

Orange
Cyberdefense



Security Navigator 2021

**Research-driven insights
to build a safer digital society**





Hugues Foulon
Executive Director of
Strategy and Cyber-
security activities at
Orange Cyberdefense



Michel Van Den Berghe
Chairman Orange
Cyberdefense France and
Group COO
Orange Cyberdefense

In 2020 our 17 SOC's and 11 CyberSOC's analyzed more than 50 billion security events daily, solved over 45,000 security incidents, and led in excess of 195 incident response missions.

Our world-class experts have digested all this unique information and synthesized our key findings in this report, to the benefit of our clients and of the broader cybersecurity community.

We are very pleased to release this edition of the Orange Cyberdefense Security Navigator. Thanks to our position as one of the largest telecom operators in the world as Orange, and as a European leader in cybersecurity services as Orange Cyberdefense, we have a unique view of the cybersecurity landscape.

The COVID-19 pandemic has disrupted the physical and digital society and economy on an unprecedented scale. It has fundamentally shifted the way in which we work and do business. We already see how a lot of these changes take shape as lasting improvements and mind-shifts. Boosted demands for secure cloud services, reliable remote network connections via SSL and videoconferencing – the new home office world is here to stay.

This crisis also proves that digital freedom is not a given. Malicious players increasingly use new and old spaces of connection and progress as opportunities for harm and disruption. Anyone can be a victim on an individual or collective level. This can lead to a breach in digital trust. At Orange Cyberdefense, we believe that the digital world can remain a trusted means of leisure, professional opportunities and services that make everyday life easier, more prosperous and fulfilling.

Never has it been more important to get out of a reaction-driven crisis mode back into the driver's seat. We need to protect freedom and safety in the digital space, not only in crisis, but on our way into the future. Our purpose is to build a safer digital society.

In the past year our 17 SOC's and 11 CyberSOC's, analyzed over 50 billion security events daily, solved in excess 45,000 security incidents, and led more than 195 incident response missions to date.

Our world-class experts have digested all this unique information and synthesized our key findings in this report, to the benefit of our clients and of the broader cybersecurity community.

We are proud and humbled everyday to be trusted with the security of our clients' most important assets, and are deploying the best expertise and technology in all domains to protect their business.

Thanks for your trust!

Hugues Foulon
Michel Van Den Berghe

Table of contents

- Introduction: What you need to know 6**
- CyberSOC Statistics: This is what happened 9**
 - Funnel: Alert to incident.....10
 - Types of incidents, Totals 11
 - The COVID-19 year 13
 - Patterns during lockdown.....14
 - A day at the office: patterns based on local time.....16
 - In the still of the night17
 - Malware trends.....18
 - Ransomware 19
 - Incident types by size 20
 - Incidents in different verticals..... 22
 - Conclusion..... 26
- Special: Pentesting the IoT – Bluetooth-LE connected padlock 28**
- World Watch: Stories about stories 31**
 - Signals 32
 - Vulnerabilities 33
 - CVE research cascade: Vulnerabilities discovered in security products..... 34
 - Time to patch..... 36
 - Threat actors 37
 - CIS advice vs. actual breaches..... 38
 - Security controls and failures..... 39
 - Conclusion..... 40
- What disrupted this year: Hidden impact of COVID 43**
 - What did we observe about attacker behavior? 44
 - State actors are people too 45
 - Ransomware perspective 46
 - What did we observe about user behavior?.....47
 - Press coverage & interest..... 48
 - What did we observe about security technology? 49
 - Managing the crisis..... 50
 - Our proposed list of priorities..... 53
 - Conclusion..... 54

- Technology insight: A dummie's guide to cybercrime 57**
 - The new realities..... 58
 - Marketplaces..... 58
 - Malwaertising, Malware, Exploits, Infrastructure 60
 - Spam & Phishing, Stolen Information, Hackers 61
 - Botnets, Money laundering 62
 - Criminal networks: a ransomware story 63
 - Conclusion..... 64
- Pentesting stories & CSIRT stories 67**
 - CSIRT story: I love the smell of ransomware in the morning!..... 68
 - Story 1: Hi I'm AD\steve-admin, please let me access VLAN2 70
 - Story 2: Red[team] alert 72
- Technology insight: Video killed the conferencing star 75**
 - Videoconferencing: Thinking about security76
 - Zoom.....76
 - Teams, Webex..... 77
 - Google Meet, BlueJeans 78
 - Tixeo, BigBlueButton, Skype for business, Jitsi Meet..... 79
 - Overview table..... 80
 - Conclusion.....81
- Security predictions: There is no bad weather 83**
 - Part 1: Cybersecurity vs. The Threat 84
 - Part 2: Cybersecurity vs. Data Security..... 85
 - Part 3: Cybersecurity vs. post-COVID 86
 - Part 4: Cybersecurity vs. Safety..... 87
- Summary: What have we learned?..... 90**
- Contributors, sources & links..... 92**



Introduction:

What you need to know



Laurent Célérier
EVP Marketing & Technology
Orange Cyberdefense

Why the term Navigator? The choice of this word is inspired by the maritime world. Before setting out to sea, every sailor needs statistical data, practical advice and weather forecasts to adapt his trajectory.

Our objective through this Navigator, dedicated to security teams, but also to IT teams in general, as well as management, is to share our analysis of this year's data, provide practical advice but also forecasts in the cyber domain. We sincerely hope to aid you in defining your security strategy.

Our general cyber ecosystem analysis, supplemented by data from our security operations centers shows that threats and vulnerabilities only declined briefly last April when containment was widespread. Since then, attacks have restarted and, in some cases, we suffered a painful increase in criminal hacking activity. Ransomware is undoubtedly one of the most frequent and dangerous attacks today, given its high level of sophistication and growing availability in the dark net. You will find a quite comprehensive deep-dive into the complex criminal ecosystems in this report.

During this particular year, 2020, we were able to measure the opportunistic nature of the attackers. Some equipment that could be thought of as an accessory, like videoconferencing or remote access, have become absolutely strategic for the global economy. This has led researchers as well as attackers to take a keen interest in these new key areas of IT. We assessed remote access technology in the last Security Navigator. This time we share with you our analysis of videoconferencing solutions in regards to security.

Another major change in recent months is the acceleration of the transition to the cloud. The flexibility, lack of up-front investment, and suitability for remote working led to cloud adoption much faster than expected. By 2023 more than half of IT will be in the cloud and 75% of companies are now switched to a "cloud first" strategy. This transformation, like all transformations, this comes with its gains but also risks, particularly in terms of security. At Orange Cyberdefense we have also stepped up in this area.

Finally, one more lesson we learn from this COVID-19 crisis relates to the value of proximity. Although technological, cybersecurity remains above all, an activity of trust, and at the heart of trust is the notion of being close to you, our customer. The global distribution of our operations centers helps us to be where you need us.

This need is all the more important in times of crisis. In this Security Navigator we share with you some experiences where we have helped our clients facing crisis abroad.

Cyber threats will quite assuredly stay. From what we see, there might even be more troubled waters ahead. Economic crisis and geopolitical tensions are following the health crisis. These destabilizations can only lead to an increase in cybercrime and state-sponsored attacks.

In this environment, the pressure on cybersecurity budgets will certainly increase for everyone who is taking security seriously. We see it as our role to offer guidance to those who seek to strengthen their resilience and help limit their vulnerabilities, so they can direct investments to areas where they will have the most impact.

Let us take advantage of this exceptional period to consider a different, more balanced security strategy. The approach of stacking layers of protection without optimizing them, or managing them properly generates a false sense of security – and a very real cost. Robust and optimized security relies on a fine balance in the knowledge of the threat and its vulnerabilities; protective measures adjusted and above all leveraged to the maximum of their capacities; detection capabilities to monitor all IT and continuously adjust its protection; effective rapid response to contain breaches and recover quickly.

This balanced approach will make it possible to focus efforts on critical risks and threats, but also to save resources, both financial and human.

At Orange Cyberdefense, we are convinced that digital security cannot be achieved without the commitment and skills of the women and men who imagine, deploy and operate cybersecurity on a daily basis. This is essential for both our customers and us. Let's take care of them, develop their talents. They have a fundamental role in our society. Above all, the Security Navigator 2021 is dedicated to them.



Hit by ransomware on New Year's Eve

On the verge from 2019 to 2020, the international currency exchange company Travelex was struck by a ransomware attack. The attackers asked for \$3 millions of ransom to unlock the company's critical systems while threatening to release personal customer data. The company paid \$2.3 millions to recover their files. ^[1]



Diana Selck-Paulsson
Threat Research Analyst
Orange Cyberdefense

Charl van der Walt
Head of Security Research
Orange Cyberdefense

CyberSOC statistics

This is what happened

To know what is going on, you sometimes have to take a step back and look at the big picture.

And we are talking about a very big picture indeed: a continuous stream of data passes through our 11 CyberSOCs and 17 SOC. We process incident data from four continents and draw additional intelligence from the internet backbone of a major global telecommunications provider, 500 public and private sources and 20 law enforcement agencies worldwide.

So as part of the Security Navigator 2021, we can again share with you a very real, first-hand picture of the events and trends over the past year.

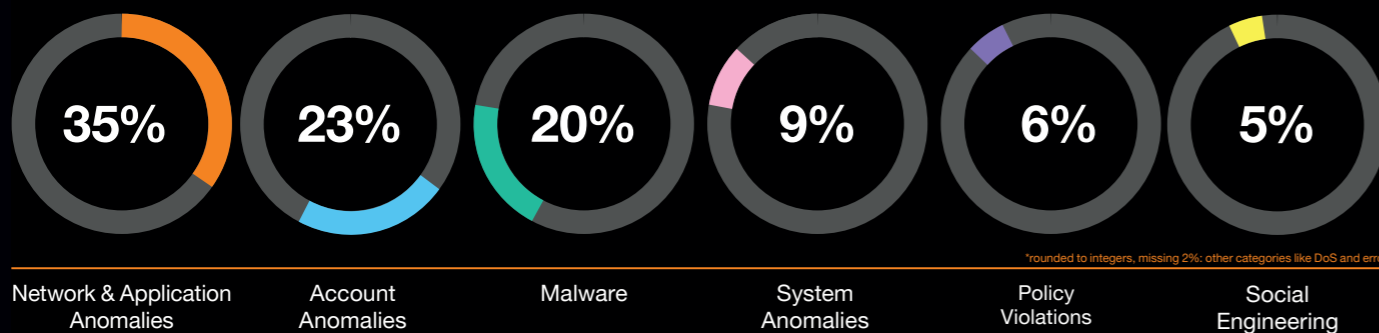
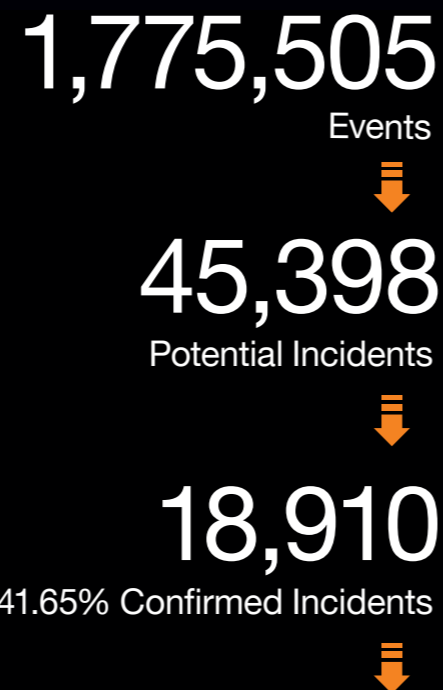
This is a very special year. The COVID pandemic has impacted the whole world in an unprecedented way. So how does this reflect on the numbers we observed in our security operation centers? And what other trends and tendencies did we see?

About the data

- Grand total of events analyzed: 1,775,505
- Total of incidents: 45,398
- Out of these incidents, 41.65% (18,910) could be confirmed as security incidents
- Period analyzed: January to October 2020.
- Data sources: firewalls , directory services, proxy, endpoint, EDR, IPS, DNS, DHCP, SIEM and our managed threat detection platform.



Funnel: Alert to incident



Types of incidents

In 2020, we detected the following incident types:

- Network & Application Anomalies**, such as tunneling, IDS/IPS alerts and other attacks related to network traffic and applications.
- Account Anomalies**, such as brute force attacks, reusing credentials, lateral movement, elevation of privileges or similar kinds of incidents.
- Malware** is malicious software such as ransomware.
- System Anomalies** are events directly related to the OS and the components around it like drivers that stop working or services that are terminated unexpectedly.
- Policy Violations**, such as installing unsupported software or connecting an unauthorized device to the network.
- Social Engineering** is any attempt to fool users; including, but not limited to, phishing and spoofing.

A global view

This year we look at a more global picture. The number of customers in our data has doubled and thus we're examining 55% more Incidents. Last year's data covered 29,391 Confirmed Incidents from 263,901 Events. This year, we've processed 1,775,505 Events that resulted in 45,398 Incidents. After analysis and communication with our customers, 18,910 were labelled true Confirmed Incidents.

Events, incidents, confirmed incidents

A note on terminology: we log an event that has met certain conditions and is thus considered an Indicator of Compromise, Attack or Vulnerability. An Incident is when this logged Event, or several Events, are correlated or flagged for investigation by a human – our security analysts. An Incident is considered 'Confirmed' when, with help of the customer or at the discretion of the analyst, we can determine that security was indeed compromised.

Totals

This year is special for our Security Navigator. Not only have we gained more customers who provide data for us to work with, but we can also report on a much broader set of operations from within Orange Cyberdefense serving customers worldwide.

Our previous dataset grew organically by 14.11% since last year to 33,540 Incidents. Our new dataset includes 45,398 Incidents from our CyberSOCs.

This unique dataset gives us the opportunity to explore several interesting questions. This report explores the following:

- What major changes have we seen since last year?
- What impact did COVID-19 and lockdowns have on Security Incidents?
- What does that say about attacker behaviors?
- What is happening on your systems while your security team is sleeping?
- Why are we detecting less ransomware, and not more?
- Why did we see so much more Adware in March?
- How do patterns vary between small organizations and large, and across industries?

Of the 45,398 Incidents in our dataset between January and October 2020, our analysts labelled 18,910 Incidents as confirmed 'True Positives'. This does not mean that the rest of the incidents were all False Positives. Some of the Incidents we process are determined to be accurate but benign and labelled 'True Legitimate'. Some Incidents can not be properly categorised.

In this year's report 41.65% of all incidents were 'confirmed' True Positives. 35% of Incidents were False Positives, 20% True Legitimates and the rest remain unknown (4%).

Securing backdoors for future access

An unknown threat actor was discovered by researchers to scan and secure vulnerable Citrix ADC servers for future access. The Citrix vulnerability CVE-2019-19781, which was disclosed just in December describes the exploitation of the Citrix Application Delivery Controller (ADC), previously known as NetScaler ADC and Citrix Gateway (previously NetScaler Gateway), which would allow an unauthenticated attacker to perform arbitrary code execution. ^[12]



General trends in detection

Network and Application Anomalies (35%) are the number one Incident type detected in 2020, followed by Account Anomalies with 23% and Malware with 20%.

While Account Anomalies (2019: 22%) and Malware (2019: 20%) seem to follow a similar trend to what we've seen in our old dataset, Network and Application Anomalies (2020: 35%) seem to have declined quite significantly compared to last year's share of 46%. We have observed more Incidents classified as Social Engineering - constituting 5% (2019: 1%) - and Policy Violations constituting 6% (2019: 3%). Both figures are considerably higher than previously tracked in 2019. While this may be due in part to the fact that a larger dataset has been used this year, there are also perceptible shifts within the dataset.

Across regions we have observed a higher volume of Social Engineering Incidents, which have seen a significant increase over the last two years (2018: 2%, 2019: 1%, 2020: 5%). This includes phishing campaigns either distributed through mass e-mail or more targeted attacks through spear phishing, as well as spam e-mails and extortion.

Policy violations are detected in large organizations more often simply because they tend to have more policies in place to begin with. This year we've seen that 2% of all Incidents were confirmed as Policy Violations amongst small businesses, compared to 3% for medium-sized organizations and 13% for our large customers.

The distribution changes slightly when we zoom into only Confirmed Incidents. Network and Application Anomaly would still be number one with a share of 34%, followed by Malware with 23% and then Account Anomalies. In other words, we observe more confirmed Malware Incidents than Account Anomalies (18%), despite Account Anomalies being raised for triage more often.

Overall, the number of Incidents processed by our CyberSOCs globally has trended upwards slightly over the year.

And so it begins ... COVID themed campaigns

Coronavirus spreading across the globe has inspired many malware authors to make use of the uncertainty and fear. In Japan, a variant of Emotet was seen attempting to scare victims into opening malicious e-mail attachments, which will infect the recipient with Emotet if macros are enabled. Similar campaigns have been observed globally. [3]

FEB

The COVID-19 year

Available data suggests that at the peak of the crisis in March there were 17 different countries under lockdown in area of operations. We note that the total volume of Incidents we processed dropped by 12% by the time the lockdowns started getting lifted significantly in May. As businesses in Europe returned to 'normal' again in June, Incidents increased by 15%, only to fall again as the European holiday period had an impact in July and August.

The impact of the pandemic on business activity is notable. According to data from the UK's Office for National Statistics¹, for example, only 66% of UK businesses were trading during one period in June and 30% of the UK workforce was on furlough leave during the same period. These two figures had reduced to 47% and 9% respectively by September.

In France, for example, where lockdown was in effect from mid-March to mid-April, Incident volumes decreased by an astounding 30% between March and May. In Sweden, however, where there was no general lockdown, volumes only decreased by a total of 3%, after dipping by 8% in April.

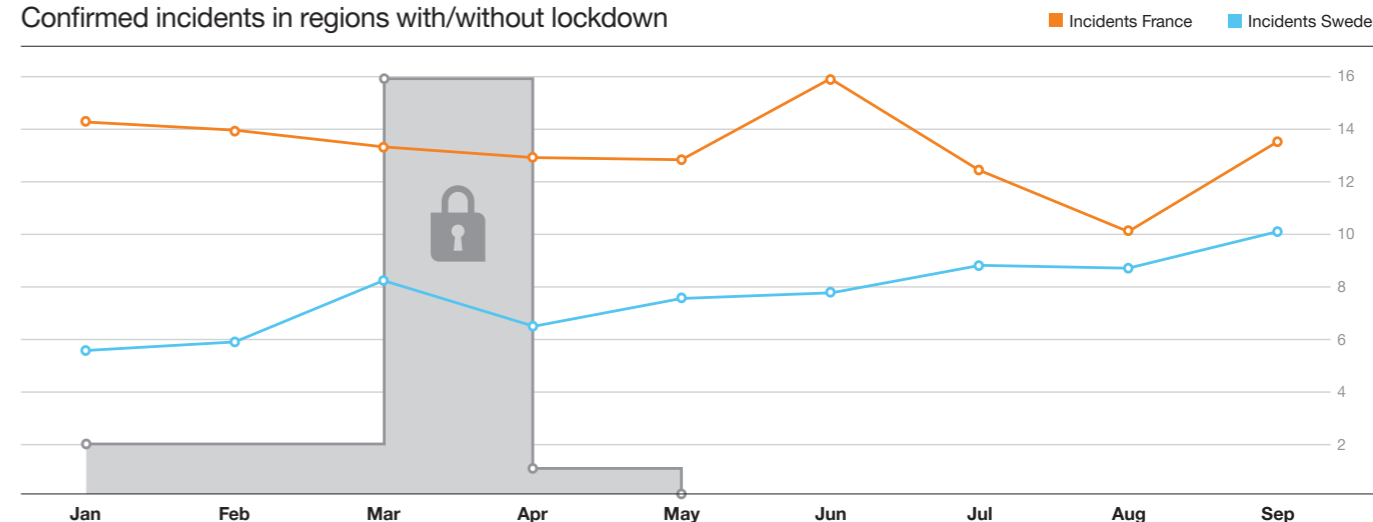
The impact of these meta factors on Incident volumes is not always immediately obvious, however. For example, after a period of leave we see an increase in failed login activity that may appear malicious, but then actually isn't. We also observed a reduced appetite to make changes during lockdown, resulting in significantly fewer AD changes or privilege escalation Incidents.

When business returned to normal again in September the number of Incidents across all our operations had increased by 18% from the lowest level in May.

The question raised by this pattern is whether verified attacker behavior was also impacted by lockdowns and the general slow-down caused by the pandemic. We can assess this question by once again looking at the difference in volumes between our customers headquartered in France and in Sweden, but this time only for confirmed malicious events.

Lockdown effects on incident count

Confirmed incidents in regions with/without lockdown



For confirmed Incidents in France we now see that the net impact of the lockdown from March to May was only 4%, much more in line with the 9% decrease observed in Sweden over the same period.

We can conclude therefore that the lockdowns had a significant impact on the total volume of security 'alerts', but no significant impact on the actual number of verified 'Incidents'.

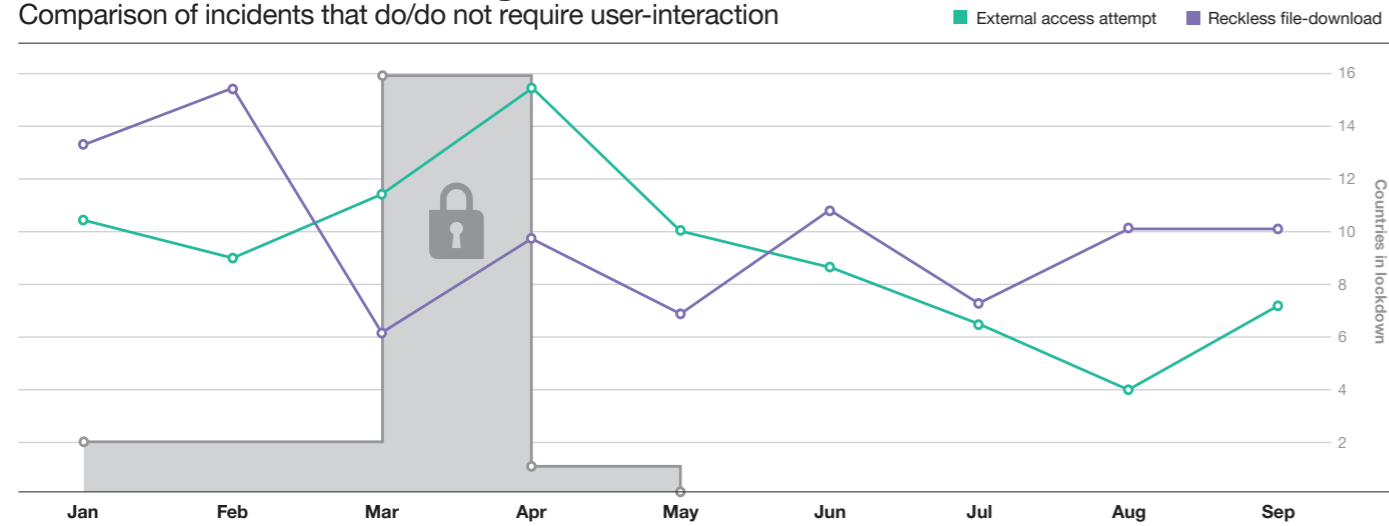
What then was the impact of COVID-19 on attacker behavior?

We will examine the question of the overall impact of the pandemic on the Security landscape in a later chapter of this report – the **Hidden Impact of COVID** – but for now we can glean some insight by examining Incidents where the attacker requires user interaction versus Incidents where the attacker can act completely alone.

From this we can conclude that the general slowdown caused by COVID-19 had a marked impact on the volume of Incidents processed by our CyberSOCs before, during and after lockdown periods, but a less significant impact on the behavior of attackers.

Incident count by user-interaction

Comparison of incidents that do/do not require user-interaction



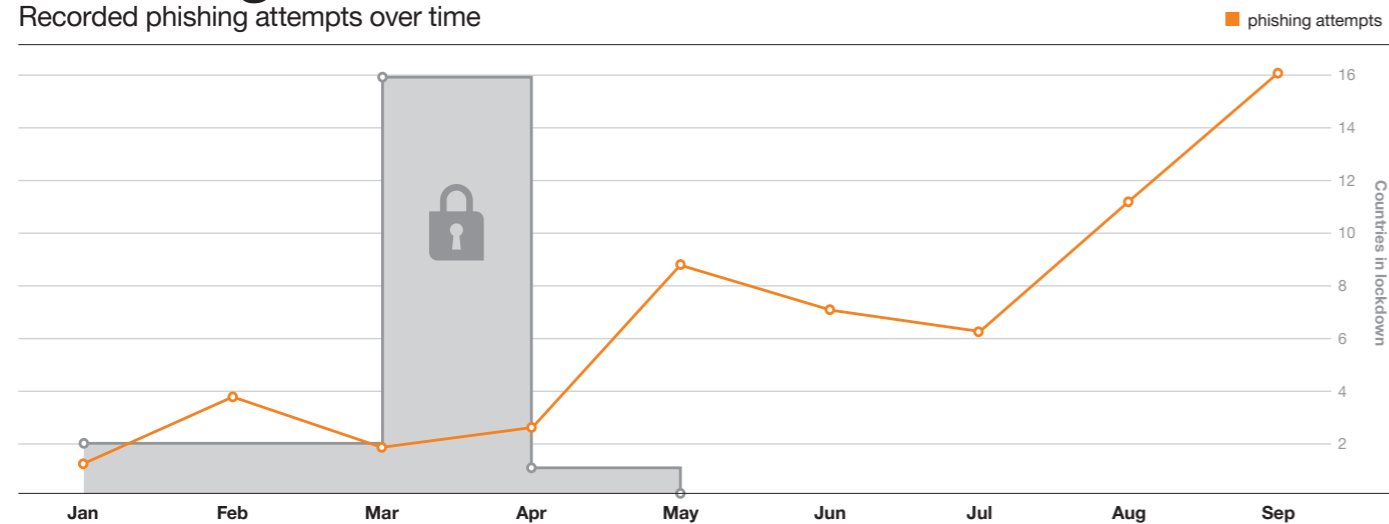
By comparing confirmed malicious Incidents that involve a user (file downloads) to Incidents where the attacker acts independently (attempts to access an external server) we note that the volume of detected Incidents of Social Engineering predictably tracks the overall level of business activity. Independent activity by attackers over the lockdown period followed a completely different pattern, however, increasing dramatically over the lockdown period before resuming to more 'normal' levels again from June.

Apart from the obvious marked increase in detected Phishing attacks over the course of the year, we note again a pattern that is consistently emerging from our examination of the COVID-19 lockdown period, namely that there was a short but pronounced spike in attacker activity at the peak of the pandemic, but that activity 'normalised' again very quickly after that. It's interesting to note that phishing activity slowed somewhat during the European summer holiday season.

This same pattern can be noted by observing patterns in confirmed Phishing Incidents in the chart below.

Phishing incidents over time

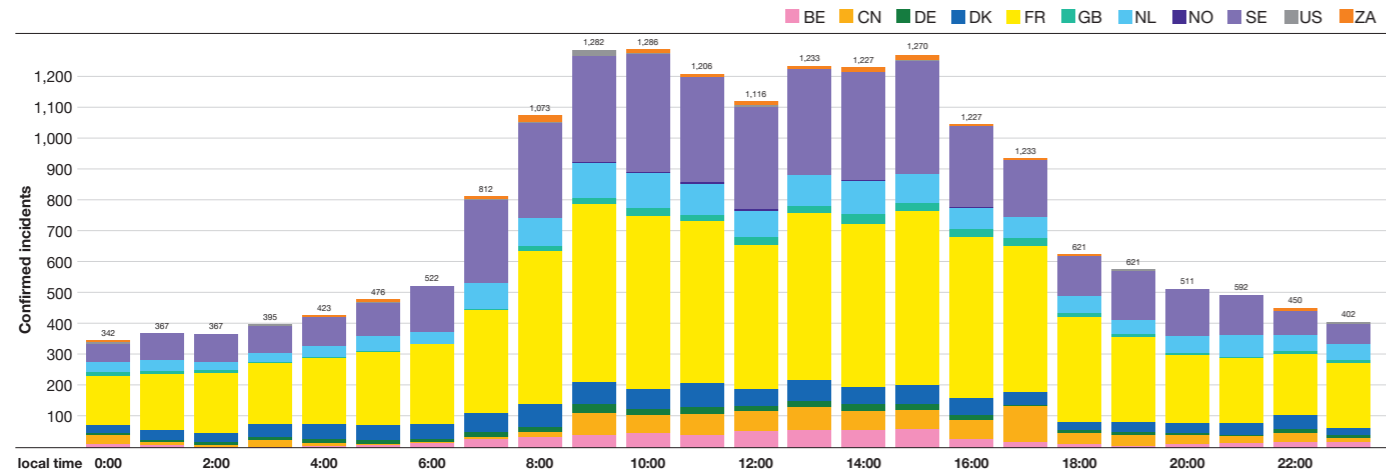
Recorded phishing attempts over time



Sextortion e-mails sent via Emotet botnet

Scammers are sending sextortion spam mails to their target's work e-mail via the Emotet botnet to reach a wider "audience". This particular sextortion scam is already around since July 2018, claiming to have recorded victims that have browsed adult sites. To increase the pressure, scammers would include leaked passwords and e-mails of the targets. [14]

Incident count over local time



A day at the office

Noting that Incident volumes were shaped by events that impact user behavior, we examine shifting patterns in Incidents over the course of the day. For this purpose, we adjust all timestamps of all Incident tickets to reflect the time of day in the customer's primary time zone.

Despite slight and predictable variations due to local working patterns, we can see that the volume of Incidents perfectly tracks the target's normal working hours. This is not simply due to 'noise' in the detection systems either, the data above depicts only verified Incidents. We confirm this thesis by examining the split across different Incident closure codes over the course of a day – noting that there is no visible decrease in the volume of False Positives after office hours.

It stands to reason that there are much fewer Incidents in total at this time (meaning fewer false positives) but it may also suggest that users who are awake and online at this time may be tired and more prone to falling for scams.

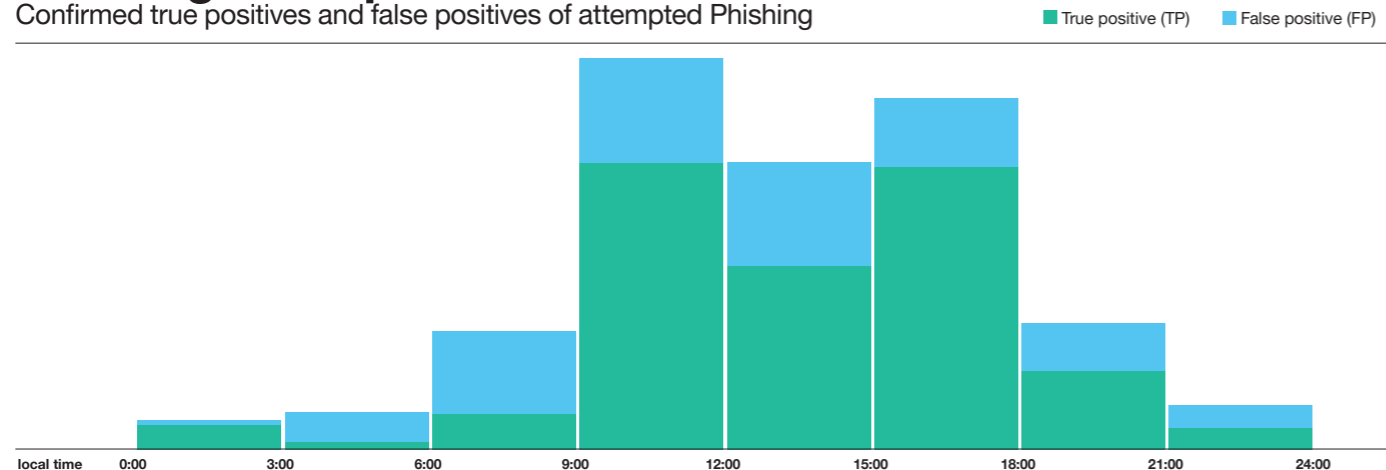
Stepping to examining the main 'periods' of a day – before work, morning, lunch, afternoon and after work – we can clearly see that Phishing False positive volumes are purely a function of user activity. The more users are busy, the more of them we'll have. True positives follow a slightly different pattern, however. One logical observation is that they occur most frequently at the start and the end of the workday (rather than over lunch time).

The data suggests that the 'volume' of Incidents is primarily a factor of user behavior. In other words, most attacks are 'carried' on the swell of user activity. Some attack categories can be executed independent of user activity, though. This connection is perhaps not surprising, but we do find it interesting to note just how acutely this is the case.

If the volume of Incidents is primarily correlated with levels of user activity, what then determines the 'shape' of these Incidents, that is the mix between the various categories of Incident? Is this mix consistent across all hours of the day, or does it change as users log off from the network?

Phishing attempts over time

Confirmed true positives and false positives of attempted Phishing



In the still of the night

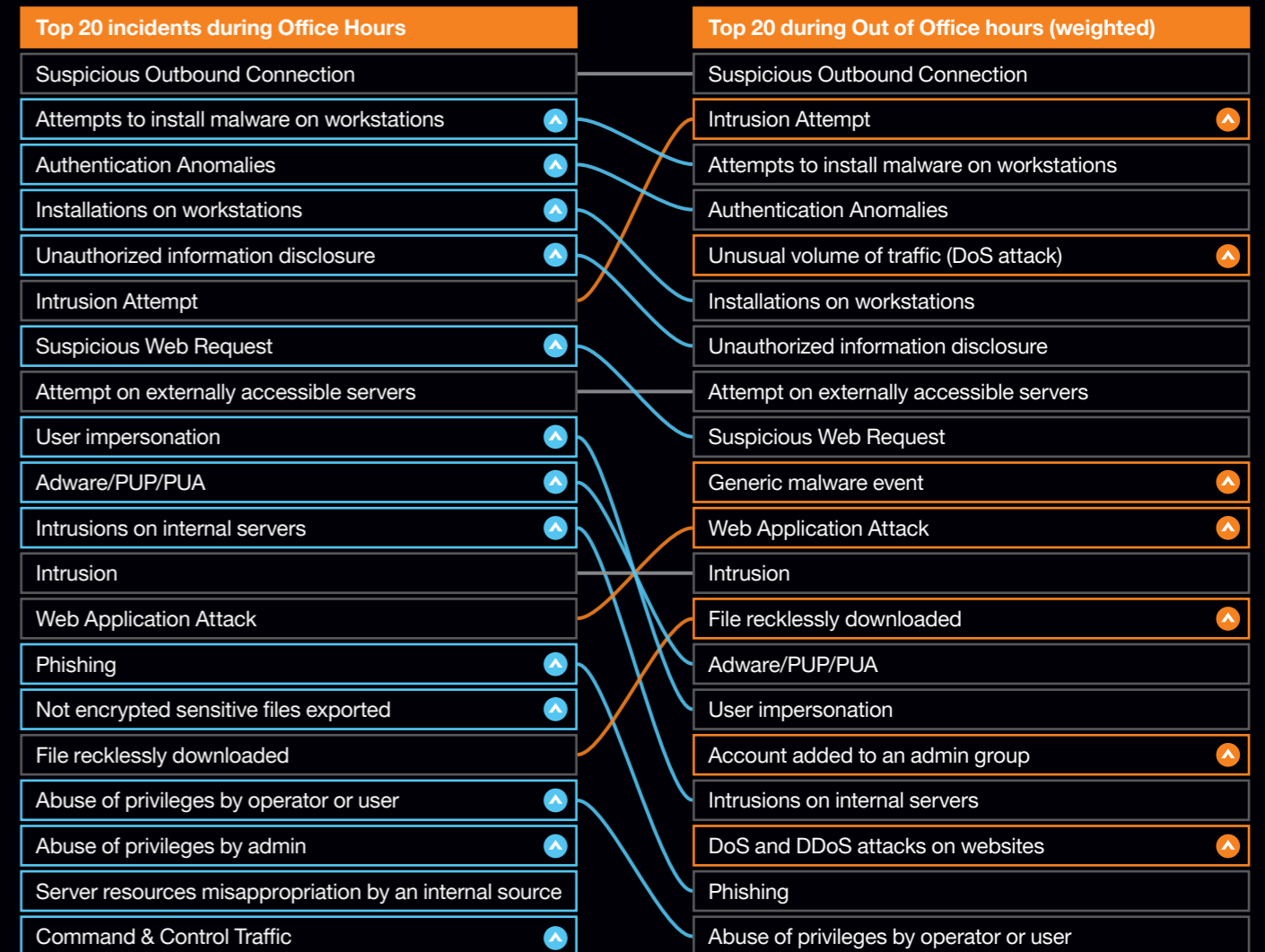
Given the additional 'noise' introduced by the higher levels of user activity, we would expect to see a higher level of False Positives during working hours. Apparently that is not the case. We find the proportion of False Positives is actually marginally higher outside working hours. However, 'True Legitimate' Incidents, which are verified Events for which there is a benign explanation, are more common during working hours. There are therefore higher levels of user activity and user error during office hours, but besides that the distribution across Incident statuses remains essentially constant through the course of the day.

Our data tells a similar story about the distribution of Incident Categories. When comparing Office Hours to Out of Office Hours distributions we note the patterns are very similar in shape, with only slight variations from place to place. Malware Incidents, for example are more highly represented after hours (22%) than during hours (19%).

Considering an 'Impact Weighted' perspective, which provides clearer insight into what an Incident means for the organization, we note some interesting patterns:

1. Malware Incidents are more highly represented after hours (22%) than during hours (19%).
2. The top 5 most common Incidents occurring during Office Hours also occur frequently (within the top six most common issues) after hours.
3. Denial of Service incidents only appear in the top 20 rankings when we consider an impact weighted ranking of the out of office hours Incidents.

Examination of the chart below shows clearly that the top 5 Incident categories that are confirmed during Office Hours are also amongst the top 6 categories during Out of Office Hours, but on average they occur 45% less often.



We can conclude that the **volume** of Incidents we deal with is primarily a function of user patterns, while the **mix** reflects attacker behavior. Attackers might have working hours, routines and patterns too. But, for the most part, attacker behaviors only manifest when they overlap with the victims' connectivity and activity. We also see that there are attacks that occur after working hours, and some that even occur predominantly after working hours.

It is clear therefore that no business can afford to let its guard down while its people are sleeping.

Malware trends

We have seen a slight increase of Malware incidents from January to October.

A clear trend in the overall threat landscape is ransomware, which has disrupted businesses across all verticals in the past year. Threat actors, that traditionally dedicated themselves to other forms of cybercrime, have seen the potential for profit in ransomware and have adapted. One such example is Emotet, which started out as a banking trojan but in recent times, has evolved its business model and focuses almost exclusively on distribution and infection through malware-related spam. Emotet is typically classified as either Trojan, Downloader or Dropper in our dataset, which means it aims to secure illicit access through infections. The access is then sold to third parties, such as ransomware operators, which then monetize the access. This model is known as Malware-as-a-Service (MaaS) and actors such as Emotet make up an important part of the supply chain, which has ensured success for ransomware operators. More about the agile business models of malware operator can be found in the [cybercrime chapter](#).

Peculiarities in ransomware detection

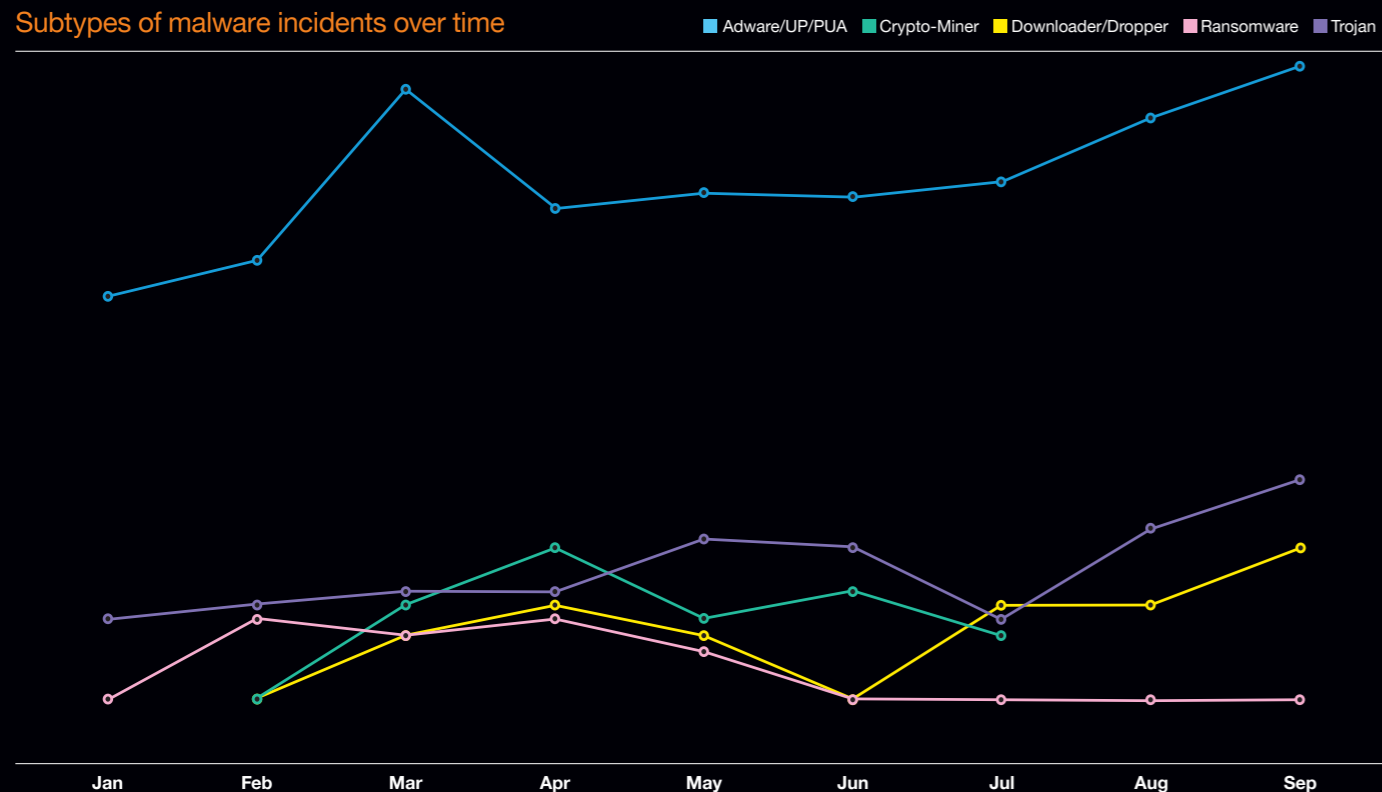
Over the past year we have recorded very few confirmed ransomware Incidents across our customers. But why is this? Well, ransomware is generally the 'final-stage' strategy for a malware infection - the last action of a compromise that has already progressed through several other phases of exploitation.

Malware operators will extract every possible bit of value from a compromised endpoint before initiating encryption and revealing their presence. The more successfully we detect malware activity in the earlier phases and disrupt it, the less likely it is to progress to a ransomware Incident. Our data suggests that an increase in early-stage detection correlates with a decrease in ransomware detection.

As we can see, we detected and confirmed more ransomware incidents during the first quarter of this year, which we believe is a function of poor levels of security team responsiveness during the peak of COVID-19. After April, we see a steady increase of detections related to Downloader and Droppers as well as Trojans (including Emotet) while at the same time we observe a decrease in confirmed ransomware incidents. We hypothesize that when security teams turned back to 'business as usual' in Q2, there were better levels of responsiveness to malware campaigns earlier in the attack cycle and therefore fewer ransomware attacks that succeeded. The significant peak in downloaders, droppers and trojans in September is in line with the increased ransomware activity seen in the wild. However, with improved focus, we seem to have managed to detect and respond to attacks during the early stage of exploitation, and thus confirmed ransomware incidents actually decreased despite the increase in campaign volumes.

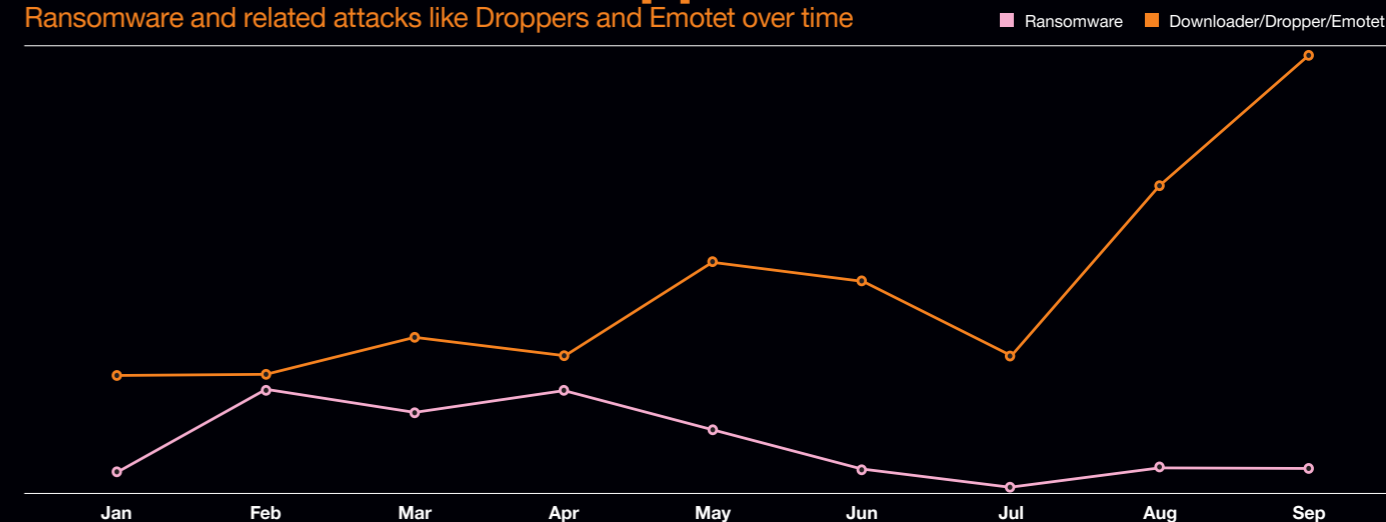
Malware trends

Subtypes of malware incidents over time



Ransomware vs. Droppers

Ransomware and related attacks like Droppers and Emotet over time



Organization size

Incidents observed at our customers are categorized by organizational size:

- Small (Employee Count = 101-1000),
- Medium (Employee Count 1001-10000) and
- Large (Employee Count = 10000 – 200000+).

The share of Incidents detected for Small businesses has grown with a share of 14% in comparison to 10% in 2019. Medium-sized claim the same share as before (2019: 31%), while Large organizations' portion of detected Incidents has continued to decrease to 55% (2019: 58%, 2018: 73%).

It is not surprising that we observe Large organizations to have the highest number of Incidents when it comes to sheer volume, followed by Medium-sized and then Small organizations. If we normalize our view and give every single Incident a weight reflecting its proportion of all Incidents for that customer, we observe that it is actually Medium-sized businesses have the highest weight in the overall Incident statistics, followed by Small and then Large organizations. This can be explained with the fact that we have more customers within the Medium-sized group than we have in the other organizational groups.

Malware big and small

Malware trends differ for organizations of different sizes. We see for example that malware Incidents among small and medium-sized businesses have increased over time, while large organizations have shown a slight decrease after a peak in March and April this year.

People Under Pressure

This year we are observing a high number of confirmed Incidents involving the installation of Adware and Potentially Unwanted Programs or Applications (PUP). These Incidents represent 60% of all confirmed classified Malware detections. Most Incidents involve users installing unwanted programs or extensions such as zip unpackers, browser add-ons that send user data to external entities, torrent clients, etc.

We noted a particular increase in confirmed Adware and PUP Incidents in March this year. This is in line with an overall trend we are seeing, which is a small peak of malware activity in March that is only reached again in late summer, where we also see an increase in Security Incidents and Confirmed Incidents overall. One explanation of the March peak could be that many employees started working from home at this time and felt they needed to install free but unapproved applications as they tried to adjust to the new reality keep up with their normal work activities. This trend was especially noticeable amongst our small and large organizations.

Chinese Military Hackers charged for Equifax Breach

The U.S. has charged four individuals belonging to the hacker group Chinese People's Liberation Army (PLA) 54th Research Institute for hacking the credit card reporting company Equifax. After hacking Equifax's digital portal, they moved around the network for weeks, obtaining personal identifiable information (PII) of nearly half all Americans, making this breach one of the biggest in history to that date. ^[5]

Incident types by size

Like last year, we observed that Medium-sized businesses have a greater amount of Network and Application Anomalies than Small and Large business organizations. Almost half (49%) of all detected Incidents were classified as Network and Application Anomalies among Medium-sized businesses. While Small and Large organizations have seen a shift in distribution, Network and Application Anomalies are still the most detected Incidents.

We consider the following observations on this data quite interesting.

We detected an increase of 13% in confirmed Malware Incidents (2020: 24%) at Small organizations from the previous year (2019: 10%), and a 9% increase in confirmed Malware cases at Medium-sized businesses to a proportion of 22% this year (2019: 13%). It would appear that Small and Medium sized businesses have "caught up" with the volume trends of Malware cases of Large businesses.

This makes Malware the second most prevalent Incident type for all organizational sizes when looking at Confirmed Incidents in 2020. While in 2019, we rated Account Anomalies in this position for Small and Medium businesses.

Also interesting to note is that the smaller the organization, the fewer Malware False Positives we see proportionally. Small organizations have a slightly lower volume of Malware detections overall than Medium and Large businesses, but proportionally far fewer False Positives. One theory on this is as follows: Large organizations implement more diverse detection capabilities than small organizations to stop the gaps they may perceive in Malware detection. These extra capabilities improve the effectiveness of the detection program - i.e. we detected more bad stuff - but some of the capabilities have lower efficiency - i.e. they produce more False Positives relative to what they find. Thus, as bigger organizations add more diverse detection capabilities to their malware detection stacks, their 'efficiency' decreases and the less incremental benefit they might have.

Another theory is that larger organizations have a larger attack surface, for example for receiving phishing and spam campaigns through mass e-mails. The likelihood that someone might click on a malicious link is therefore higher simply due to the higher number of employees. Why large organizations see higher numbers of False Positives could then be explained by the higher probability that a user might click on a suspicious link. With more users, there is more potential on clicking either on malicious or suspicious links. We thus see a higher amount of potential malicious sites that after raising upon investigation turn out to be non-malicious, thus False Positive.

The reality is, however, that with Malware the cost of an infestation far outweighs the cost of investigating a False Positive. This is especially true in the new 'Extortionware' world. Thus, the cost of a False Negative is infinitely higher than the cost of a False Positive.

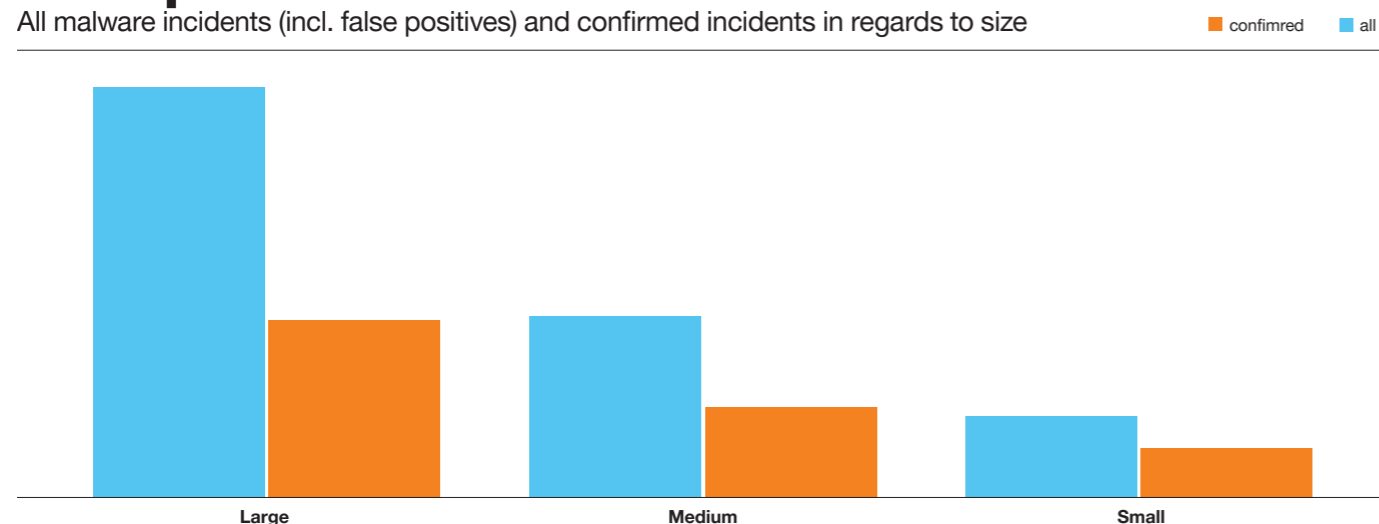
Volume per business related to size

We registered approximately 101 (2019: 63) Confirmed Incidents (median) per business for Small organizations during the 9-month reporting period. Medium sized organizations had 77 (2019: 266) and Large organizations had a median of 278 (2019: 463). That Large organizations have the highest number of Incidents is not surprising, but that Small organizations deal with more Incidents than Medium ones is a bit unexpected.

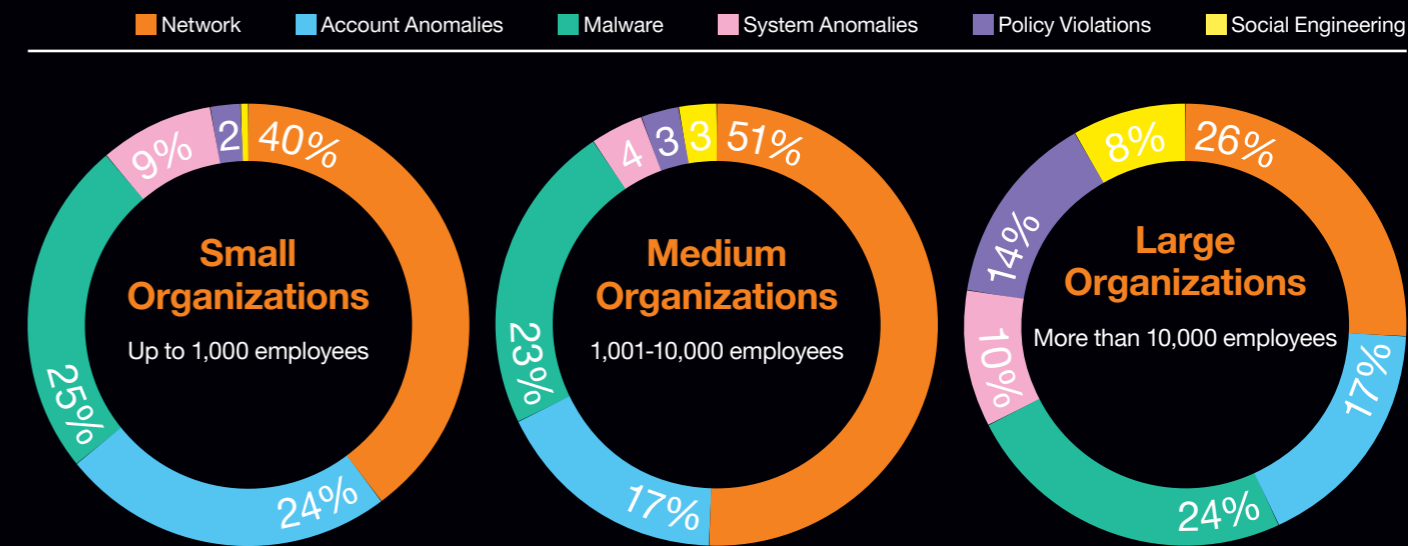
Some of our Medium sized businesses have dealt with a very low number of Confirmed Incidents this year, which in the end is a good sign, and this has led to an overall decrease in Confirmed Incidents per business since last year.

True positives vs. all malware incidents

All malware incidents (incl. false positives) and confirmed incidents in regards to size



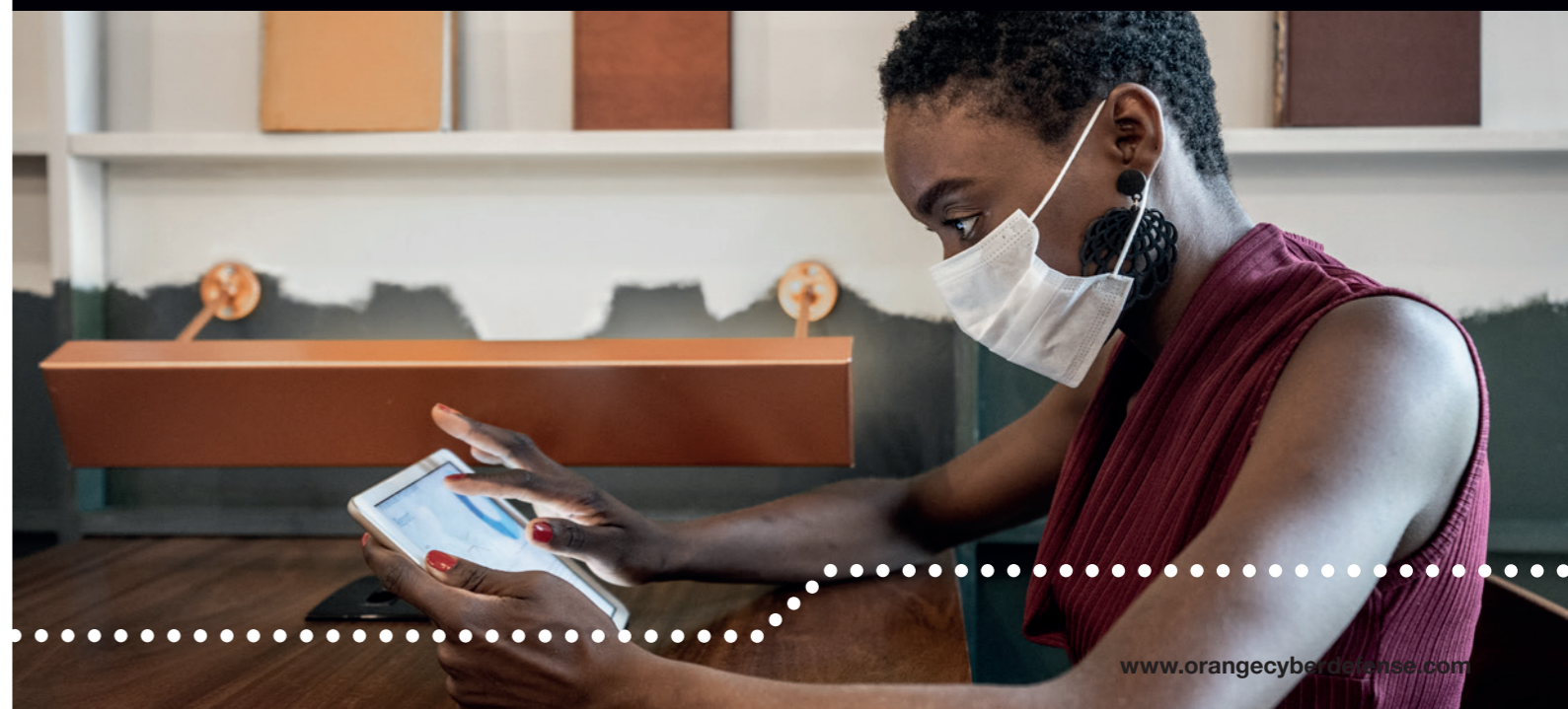
Incident distribution by size



Incident count per business

Median number of attacks per organization in each size

Some of our Medium sized businesses have dealt with a very low number of Confirmed Incidents this year. In the end that is a good sign, and this has led to an overall decrease in Confirmed Incidents per business since last year.










Incidents in different verticals

How are the incidents distributed within different verticals? We analyzed seven industries and were surprised by the differences we spotted.

Higher percentages in these graphs do not just mean that incidents are occurring more frequently, and that the industry is more 'vulnerable'. In fact, they can indicate quite the opposite. The ability to identify an incident may indicate a high security maturity. For example, in finance there are high volumes of social engineering for fraudulent purposes because financial organizations are more mature in dealing with these incidents and are able to detect and report more of them.

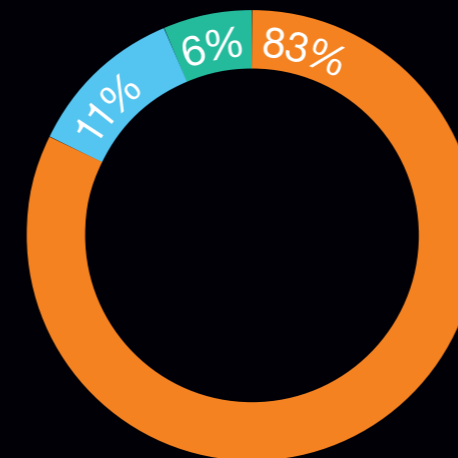
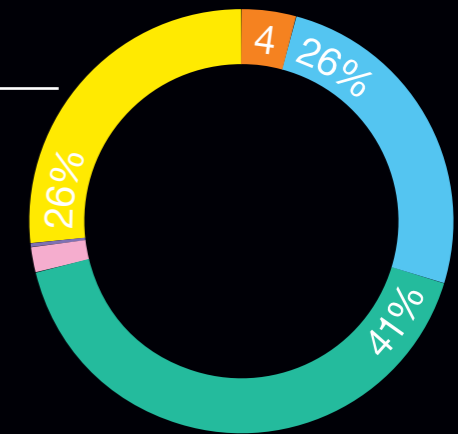
Incident distribution: Verticals

Confirmed, true-positives only

	 Network	 Account	 Malware	 System	 Policy	 Social	 DoS
Accommodation & Food	4.20%	25.61%	41.19%	1.76%	0.27%	26.42%	0.00%
Education	82.50%	11.25%	6.25%	0.00%	0.00%	0.00%	0.00%
Finance & Insurance	37.15%	19.30%	19.57%	5.07%	4.03%	10.92%	2.27%
Healthcare	81.01%	12.37%	5.52%	0.24%	0.08%	0.08%	0.00%
Manufacturing	29.10%	21.26%	26.54%	10.98%	9.50%	1.73%	0.00%
Professional, Scientific & Technical services	45.91%	23.06%	15.72%	3.46%	1.99%	7.23%	0.42%
Public Administration	38.27%	3.40%	25.31%	6.79%	24.69%	0.00%	0.00%
Real-estate, rental & leasing	11.24%	23.34%	27.95%	30.84%	6.05%	0.00%	0.58%
Retail & Trade	29.97%	12.86%	23.33%	6.20%	13.20%	6.89%	0.35%
Transportation & Warehousing	40.28%	20.83%	19.64%	15.67%	3.17%	0.00%	0.00%

Accommodation and Food Services

This vertical sticks out with having 41% of all incidents to be confirmed as malware, followed by the highest amount of social engineering (26%). One reason could be that these two often go together, social engineering as initial attack vector via phishing, vishing etc. which after several other steps leads to malware infections.

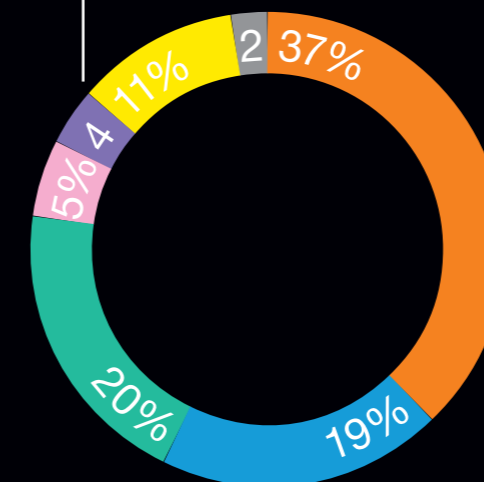
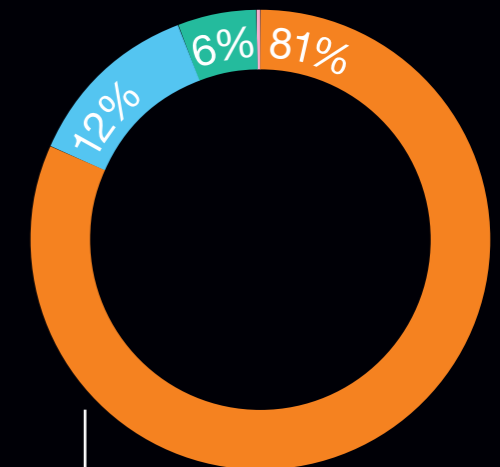


Educational services

We see a high amount of confirmed Network & Application Anomalies within the vertical Educational Services. This sector sees mostly Suspicious Outbound connections. We recorded most confirmed incidents in March and June, while otherwise the incident volume remained relatively low, possibly due to lockdowns and their impact on digital activity.

Finance and Insurance

Finance continues to have a higher amount of confirmed Social Engineering Incidents than the majority of other sectors, in particular confirmed Phishing Incidents. This year, we have also detected Denial of Service attacks against this sector. No other vertical had as many confirmed DoS attacks than this one. To put this into perspective, the absolute number is still relatively low. Finance and Insurance Incident trends follow the overall trend we have seen. A higher volume of Incidents has occurred during Q1, followed by quite a decrease in April and especially in May, while Incidents increased again in June and July.

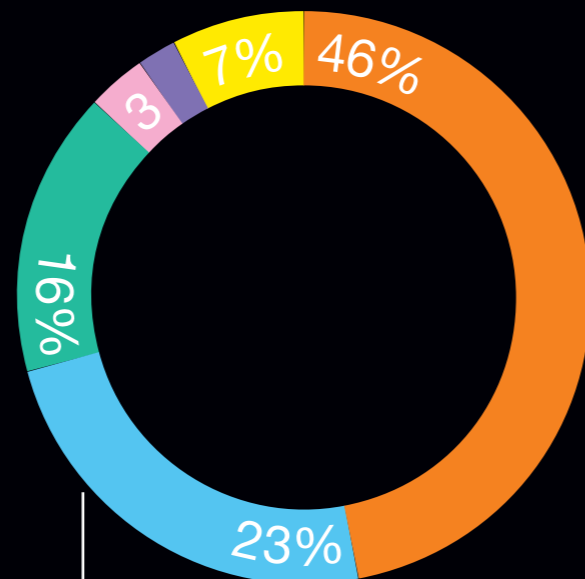
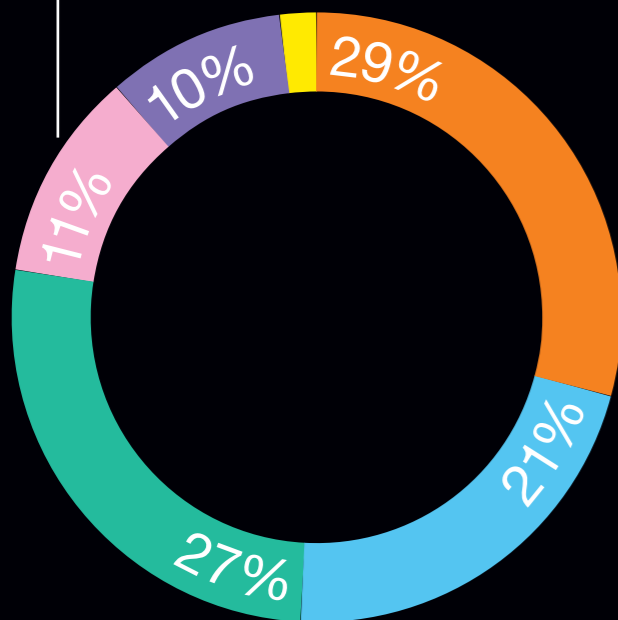


Healthcare & Social Assistance

What sticks out is the high number of Network & Application Anomaly Incidents. Especially the Healthcare sector seems to have high amounts of Confirmed Incidents regarding Unauthorized Information Disclosure (scan activities, unsuccessful SQL injection attempts, etc.), Suspicious Outbound Connection and Intrusion Attempts. When looking at Incidents overtime, Healthcare and Social Assistance had the most incidents during January this year, which decreased after that with a small exception in April, incidents continued the decreasing trend into Q3.

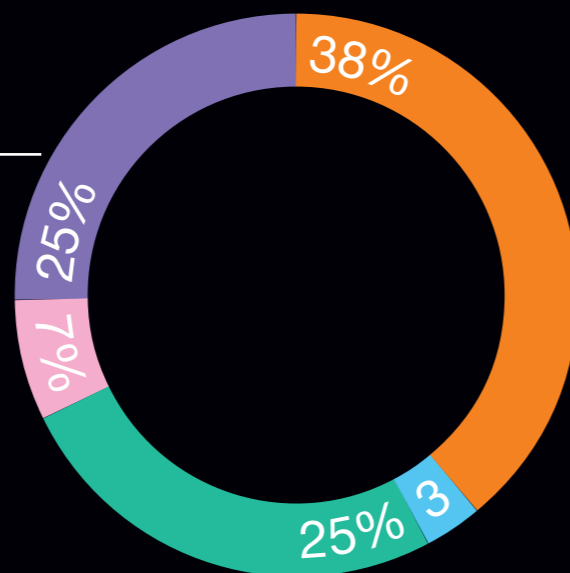
Manufacturing

This industry has seen a high volume of malware incidents with 27%, which puts it in the top 3 when looking across all verticals. As with malware, Manufacturing observes an over average occurrence of System Anomalies, and thus incidents related to OS and its components. Manufacturing sticks out with 10% of Policy Violations, making it top 3 of all industries.



Professional, Scientific, & Technical Services

Most remarkable is that we see the highest number of Account Anomalies and this vertical is one of the top 3 that observed confirmed Social Engineering Incidents, predominantly Phishing and Spam. Professional, Scientific, and Technical Services see the highest volume of incidents in August, unlike any other vertical.

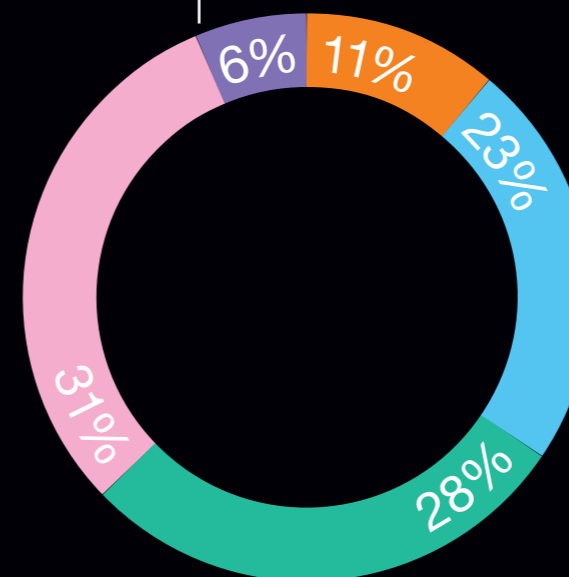


Public Administration

The highest amount of Policy Violations we see is in the Public Administration vertical. This comes as no surprise as this sector might be under more regulations than other verticals. This sector experiences 1/4 of all confirmed incidents to be classified as Malware, which means Public Administration is in Top 4 in this Incident Type in comparison to other verticals.

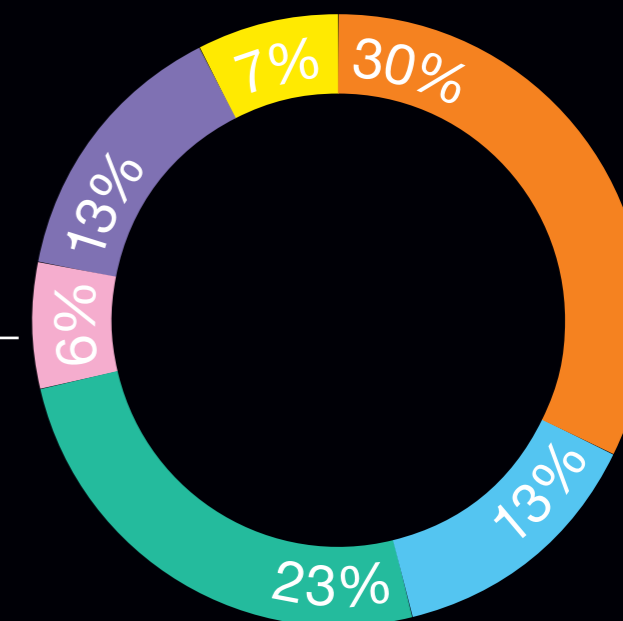
Real Estate, Rental & Leasing

Here we observe the highest amount of detected system-related incidents across industries taking 31% of all incidents. The top second incident type experienced by this industry is Malware with 28%, followed by Account Anomalies with 23%. Real Estate and Rental and Leasing is also the only sector with the least Network and Application Anomalies against the fact that this is the most seen across most other verticals.



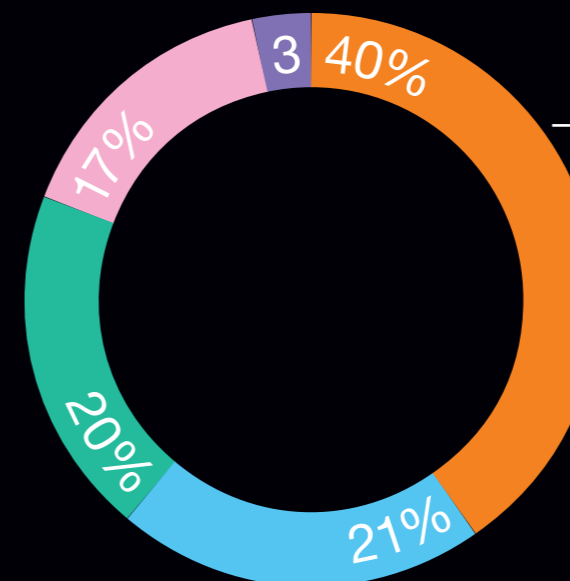
Retail & Trade

This industry is following the overall trend of the top 2 Incident types, namely Network and Application Anomalies (30%) and Malware (23%) Incidents. Besides a high number of Incidents classified as Error, the Retail sector experiences a lot of Policy Violations and Social Engineering Incidents. Retail has had a steady increase of incident volume over the year, with a small dip in August. September has seen the highest amount of incidents for this sector.



Transportation & Warehousing

Here we find the most System Anomalies registered when looking across all industries. 16% of all the incidents are confirmed to be related to anomalies in either operating systems or connected components to it. Besides System Anomalies, this sector suffers the "normal" top 3 incident types, Network, Application Anomaly, Account Anomaly and Malware. Against the overall trend, this sector has registered its most incident during April and May.



PR is everything – increasing the pressure for victims

Three more Ransomware operator groups follow Maze and create their own leak sites on the dark web. The groups, Nefilim, CLOP and Sehkmnet have created similar onion sites than the Ransomware operators of Maze. The sites publishes data leaks after the victims have chosen not to pay. [6]

Conclusion

Our detection data provides several unique insights that improve our understanding of the cybersecurity landscape.

The patterns of security Incidents over the year were markedly impacted by the business slowdown caused by the COVID-19 pandemic. Incident patterns therefore track the patterns and behaviors of users in our businesses, independently of the level of effort of the attacker, and most Incidents are detected when people are working, and computers are connected. Some types of Incident occur predominantly after working hours, however, and it is therefore clear that no business can afford to let its guard down while its people are sleeping.

We noted a particular increase in confirmed Adware and PUP Incidents during the lockdown period. Many employees started working from home at this time and appeared to install free but unapproved applications as they tried to adjust to the new remote work reality.

Ransomware has been a key theme this year and an important part of this study. We detected more ransomware incidents during the lockdowns than after they eased, which we believe is a function of poor levels of security team responsiveness during that time. After April, we see a steady increase in downloaders and droppers (including Emotet) but a decrease in confirmed ransomware. This could be because there were better levels of responsiveness to malware earlier in the kill chain after business returned to 'normal'. With focus, we can detect and respond to attacks during the early stages, preventing them from escalating to the encryption stage. This is good news for our battle against the ransomware scourge.

Customer size and industry vertical are also of interest. Here the most striking findings have to do with the intensity of Incidents dealt with by our smaller clients, which frequently match the levels experienced by larger businesses. It would also appear that Small and Medium businesses have "caught up" with the Malware trends of Large businesses.

Our data also leads us to contemplate the value of adding more detection technology, given that better detection appears to also increase the volume of 'noise'. The data suggests that more detection is more effective, but can also be noisier, leading to a higher proportion of False Positives. We believe, however, that the cost of a False Negative is infinitely higher than the cost of a False Positive. This is especially true in the new Extortionware world where the cost of an infestation far outweighs the cost of investigating a false positive.

Each industry across our client base has their own mix of Incidents. For all of them, however, the clear trend is that the volume of attacks and Incidents is relentless and growing. No business, large or small, in any vertical, can afford to let its guard down.



MAR

SMBGhost

Also referred to as SMBleedingGhost or CoronaBlue is the vulnerability CVE-2020-0796 that was given the highest CVV severity level of 10. CoronaBlue is caused by a flaw in the SMBv3 protocol. An (authenticated) attacker could target a SMBv3 server and execute code on the victim using a specially crafted packet. This is particularly dangerous because SMB services exposed to the Internet could lead to scenarios similar to WannaCry and NotPetya attacks. ^[7]

ZoomBombing

As many employees started working from home and turned towards video chats such as Zoom, a practice later termed as ZoomBombing started to surface. ZoomBombing is when meetings get interrupted by uninvited guests, which would then share inappropriate video material or just "troll" the rest of the audience. ^[8]

The website you are visiting is insecure

Four of the major browser developers have given an over one-year heads-up about starting to implement warnings whenever websites are browsed that use obsolete encryption protocols such as TLS 1.0 and TLS 1.1. This was done already back in October 2018. Now in March, it has started, Firefox 74 is now greeting users with a warning before continuing to an insecure site. Google, Microsoft and Apple will delay their implementation due to the pandemic. ^[9]

Simple but effective

A scammer has come up with a simple but efficient method to steal people's Bitcoin – operating a network of fake bitcoin QR generators. Apparently, the scammer had set up a website claiming to generate QR codes for people's Bitcoin addresses. The generator created a handful of QR codes that pointed to the scammer's bitcoin address instead. By the time of discovery, the address had generated 4.9 bitcoins (a little over £25,000) through 473 transactions. ^[12]

Stop sending GIFs on Teams

Researchers from CyberArk found a vulnerability in Microsoft Teams that allows attackers to take over accounts by simply sending a regular GIF. When communicating through Teams, authentication is done through two tokens. If an attacker has access to both tokens, they will be able to read/send messages, create groups, add or remove users and change permissions. ^[11]

APR

Popular Hacker platform shutdown by FBI

The Russian-based hacker platform Deer.io was taken down by the FBI. The platform existed since 2013, hosting approx. 24,000 shops selling illicit goods such as hacked accounts, credentials, financial and corporate data as well as personal identifiable information (PII). ^[10]

Pentesting the IoT: Bluetooth-LE connected padlock

The Internet of Things is an upcoming industry, with 'smart' devices becoming more widespread. However, this expansion could be disastrous if security isn't a priority.

Nowadays, cycling is becoming more and more common, with bike rental services gaining in popularity. That's why a customer asked us to audit a Bluetooth-LE connected padlock used for their public bicycles. Coffee arrived and so did the Breton crepes, so testing conditions were ideal.

Thomas Bygodt, Managing Consultant, Orange Cyberdefense



Step 1: Android Application

We decided to start off with a static analysis of the mobile application used to lock/unlock the padlock, so the apk-file of the app was downloaded and decompressed.

Step 2: Focusing on SSL certificate verification

A Java file we found contains a function that controls the SSL exchanges. Bingo! If you force the return value of this function, it will bypass the certificate verification and we can intercept messages.

We're going to have a coffee before moving on to the next one.

Step 3: Getting to the Heart of Things

After playing around with the assembly language (smali) of the application, we recompiled it. Result: more logs and no more SSL check!

Step 4: Bluetooth and Crypto

The elements exchanged with the server are the BLE key, the BLE password, and the MAC address of the IoT device. The weakly protected BLE key, decrypted in the application, is easily discovered.

All that remains is to take care of the AES/CBC encryption of communications.

Step 5: My best friend Python

With a Bluetooth token adapter and a Python script, we can lock and unlock the padlock... Game over! We drank too much coffee, the Breton crepes were delicious.

Having thoroughly pwned the system, we can use the extra energy and go for a free bike ride ;-)

Breton crepes:

250 g wheat flour, 70 g brown sugar, 2 eggs, 1 tablespoon of butter, 1 pinch of salt, 1/2 l milk, Rum and a little vanilla sugar.

Put the flour in a bowl and mix with the eggs and sugar and add some water. Now add "petit à petit" the milk while stirring constantly. Finally add the melted butter and rum and stir in enough water until the batter is liquid enough.

Let the dough rest for about 4 hours so that it can swell properly. Stir vigorously again before baking. Melt some butter on a crepe pan and thinly spread a spoonful of batter on the pan. Bake until golden on both sides.

Lessons learned:

The assessment of an IoT device allows to search for vulnerabilities on its whole environment: hardware, embedded software, communication protocols, servers, mobile applications, APIs, web interfaces, etc.

- Design and develop with security in mind
- Secure every component, from hardware/electronics to mobile applications and cloud-based web management tools
- Secure communications between every component
- Never trust users or their devices



Charl van der Walt
Head of Security Research
Orange Cyberdefense

World Watch

Stories about stories

Orange Cyberdefense's World Watch Service works on behalf of the customer to collect, analyse, prioritise, contextualise and summarise global, geographical and vertical threats as well as vulnerability intelligence to provide actionable security intelligence relevant to the business, its infrastructure, processes and applications.

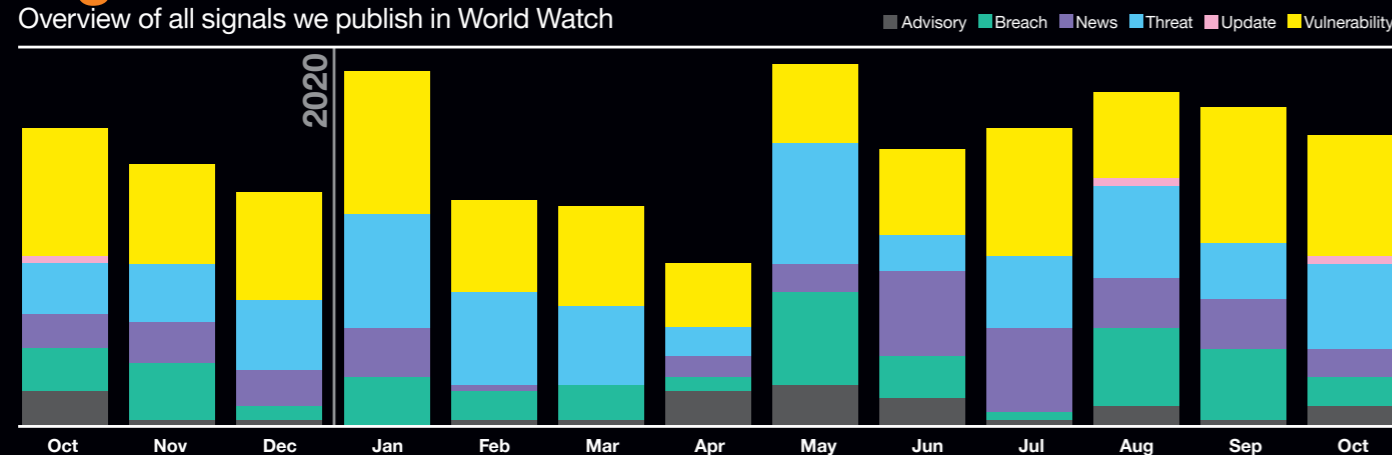
We release between 30 and 50 'Signals' a month discussing Vulnerabilities, Breaches, Threats and News we consider 'significant' and of importance to our customers globally. In the 12 months ending 30 September 2020 we produced 474 of these Signals.

Each Signal gets described using a system of standard tags that allows us to track the technologies, actors and threats discussed in the Signal. We also track specific trend factors related to the 'State of the Threat' model we use to build and observe our view of the threat landscape. We have 5,206 of these tags for this year so far. We can use them to form of a view of the significant events that are shaping our industry.

Although this is not an enormous dataset, it does provide a fresh and interesting perspective. Combined with other internal and external data sources we can use it to form a view of what's really happening in the security space.

Signals

Overview of all signals we publish in World Watch



COVID-19 Fatigue

The first thing one notices in the chart above is the obvious slow-down that occurred during April, followed by a dramatic increase in news volumes in May. This significant 'dip' reflects the extent of how the industry overall got distracted at the start of the various global lockdown periods. This level of distraction will be examined in more detail in its own chapter, but it's important to note in order to properly understand the other data we will share in this report.

The data above suggests that the volume of Signals published by our World Watch team decreased from January down to April, then spike dramatically in May, despite the low volume of overall news.

After a slump in activity in April there was a pronounced increase in May as business and the industry found its feet again after the shock of lockdown.

Attackers no doubt were also impacted by the lockdowns in one way or another, but we believe the slump in April reflects industry activity, not attacker activity. As other parts of this Navigator report will disclose, we observed a similar 'fatigue' within the volumes of Security Incidents our various global CyberSOC teams dealt with during that time.

As with the security 'news' data we presented earlier, April, May and June were clearly anomalous months as far as Security Incidents were concerned. Our analysis of the causes behind this truly 'unprecedented' period in world history will be explored elsewhere in this report.

For this section of our Security Navigator, however, we will focus on some of the broader trends we've observed from this data this year.

Critical Signals

The table below is a summary of the Signals published during this report period that were classified as 'Critical':

Category	Date	Summary
Vulnerability	15/10/2020	Critical SonicWall VPN Portal Bug Allows DoS, Worming RCE
Vulnerability	14/10/2020	October Patch Tuesday: Microsoft Patches Critical, Wormable RCE Bug
Vulnerability	15/09/2020	Zerologon Attack Against Windows
Vulnerability	15/07/2020	Microsoft patches wormable SIGRed bug in Windows DNS Server
Vulnerability	14/07/2020	RECON bug lets hackers create admin accounts on SAP servers
Vulnerability	02/07/2020	F5 TMUI Remote Code Execution Vulnerability
Vulnerability	10/03/2020	Microsoft SMBv3 Vulnerability
Vulnerability	14/01/2020	Microsoft January 2020 Security Update

Vulnerabilities

All eight Signals that were classified 'Critical' in the past year were vulnerabilities. Five of those impact Microsoft Windows, which continues to be a source of severe vulnerabilities and a frequent target for attacks. A relatively unusual vulnerability in SAP systems would allow an unauthenticated attacker to gain full access to the affected SAP system.

The last two issues in this list involved perimeter security technologies – A Critical SonicWall VPN Portal Bug and a Remote Code Execution Vulnerability in F5 TMUI.

These two critical vulnerabilities in security technologies are acute examples of what we would consider to be one of the dominant themes of this year in security, namely vulnerabilities and attacks involving the security technologies we deploy to protect our network perimeters and particularly to allow for secure remote access to our internal systems.

The technologies that featured in 2020

Let's take a look at some technology vendors that stood out in our Signals across the various categories this year.

Microsoft (Windows)

A significant number of vulnerabilities we covered this year were found among Microsoft products. Microsoft featured most prominently in our Threat and News categories also, indicating just how frequently Microsoft products contribute to active and meaningful threats and attacks.

Microsoft (and Windows) vulnerabilities continue to present us with an ongoing patching challenge. The volume of serious vulnerabilities in Windows ebbs and flows independently of the volume of issues being reported across technologies generally, but has risen sharply over the course of the last 18 months, as the chart below shows.

As can be seen in the chart below, vulnerabilities in Windows have seen a massive increase in the first three quarters of 2020. CVEs which were classified 'high' or 'critical' have in fact doubled comparing Q4 of 2019 to Q1 2020.

A critical Signal we published in September this year involved a Windows vulnerability referred to as 'ZeroLogon' - CVE-2020-1472. This CVE describes a bug in Windows Server Active Directory service that was patched in the Microsoft August 2020 Patch Tuesday. It is described as an elevation of privilege in Netlogon, the protocol that authenticates users against domain controllers and has subsequently been weaponised and is being actively used in attacks, for instance by ransomware actors.

Security Products

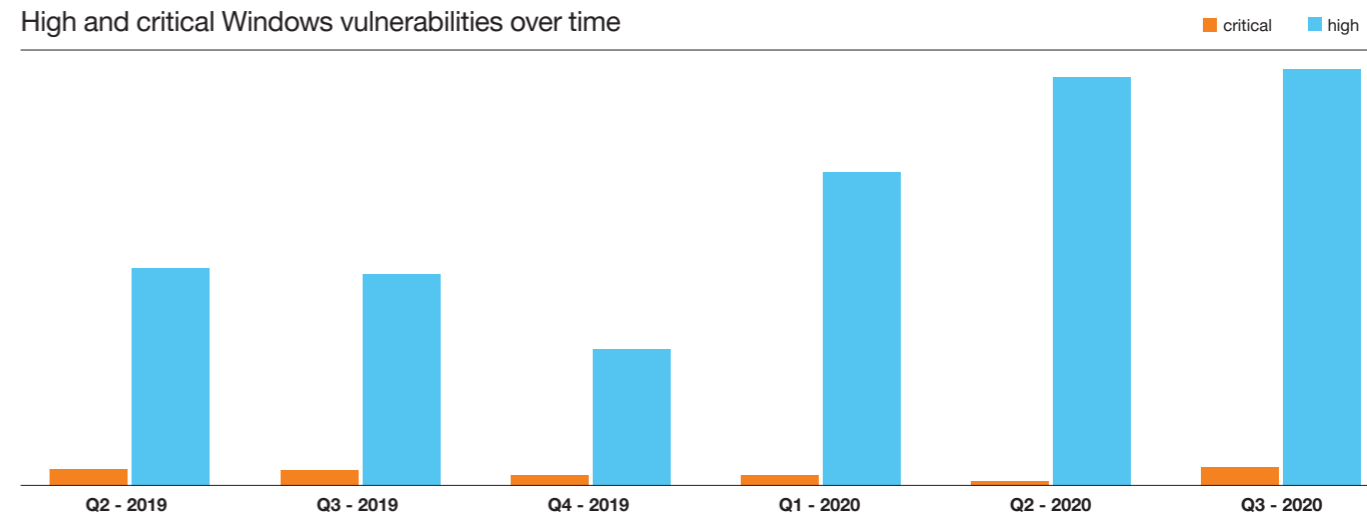
Big brands like Microsoft will always feature highly, but noteworthy over the last twelve months is also the visibility of several leading security product vendors in the very short list of technology vendors who featured multiple times in our Signals this year.

We noticed a distinctive 'bump' that occurred in May this year, where an unusually high number of vulnerabilities was reported in these security technologies. Indeed, there was a four-fold increase in vulnerabilities reported in selected security technologies between March and May 2020.

On the following page we have extracted what could be described as a "research cascade", showing how related CVEs have been researched which led to more research and subsequently to the discovery of more CVEs in similar product families.

Windows vulnerabilities

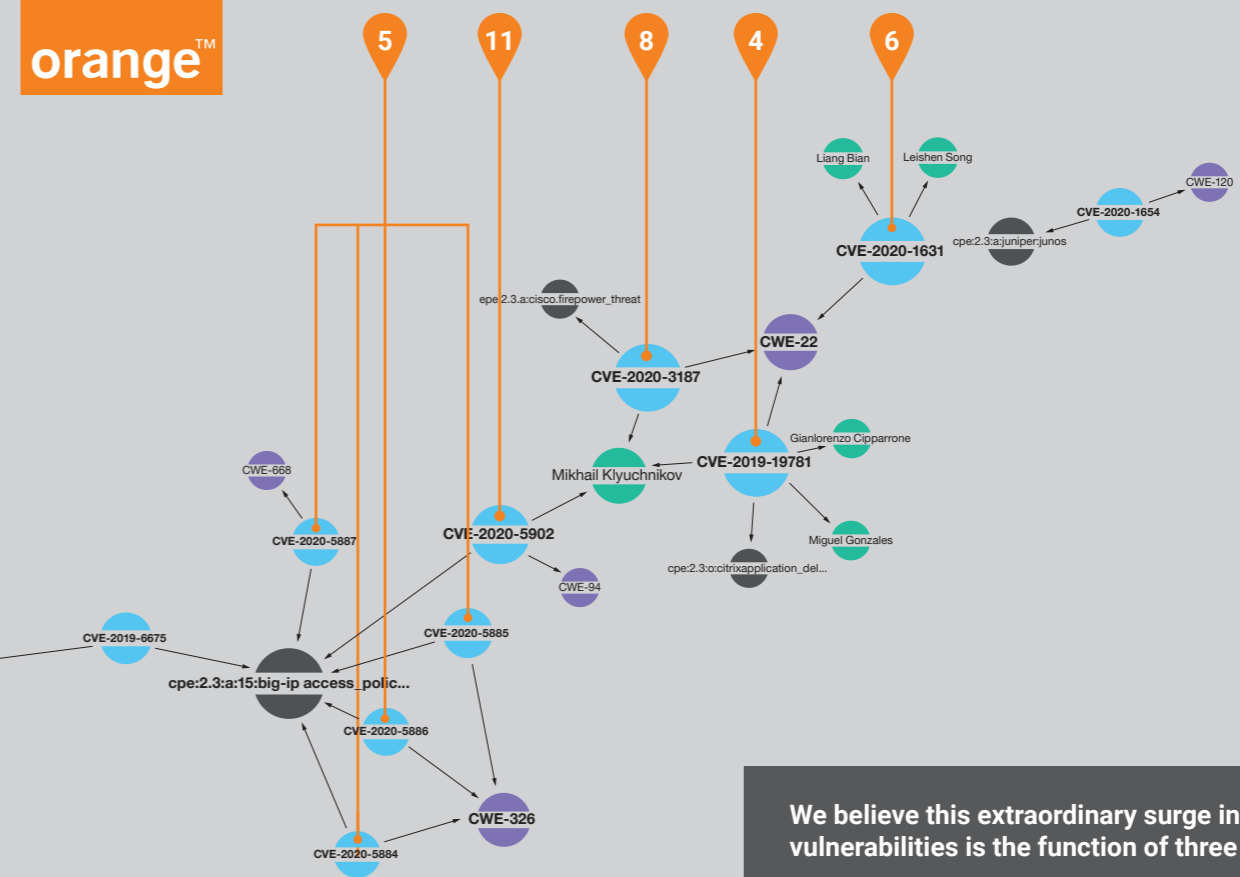
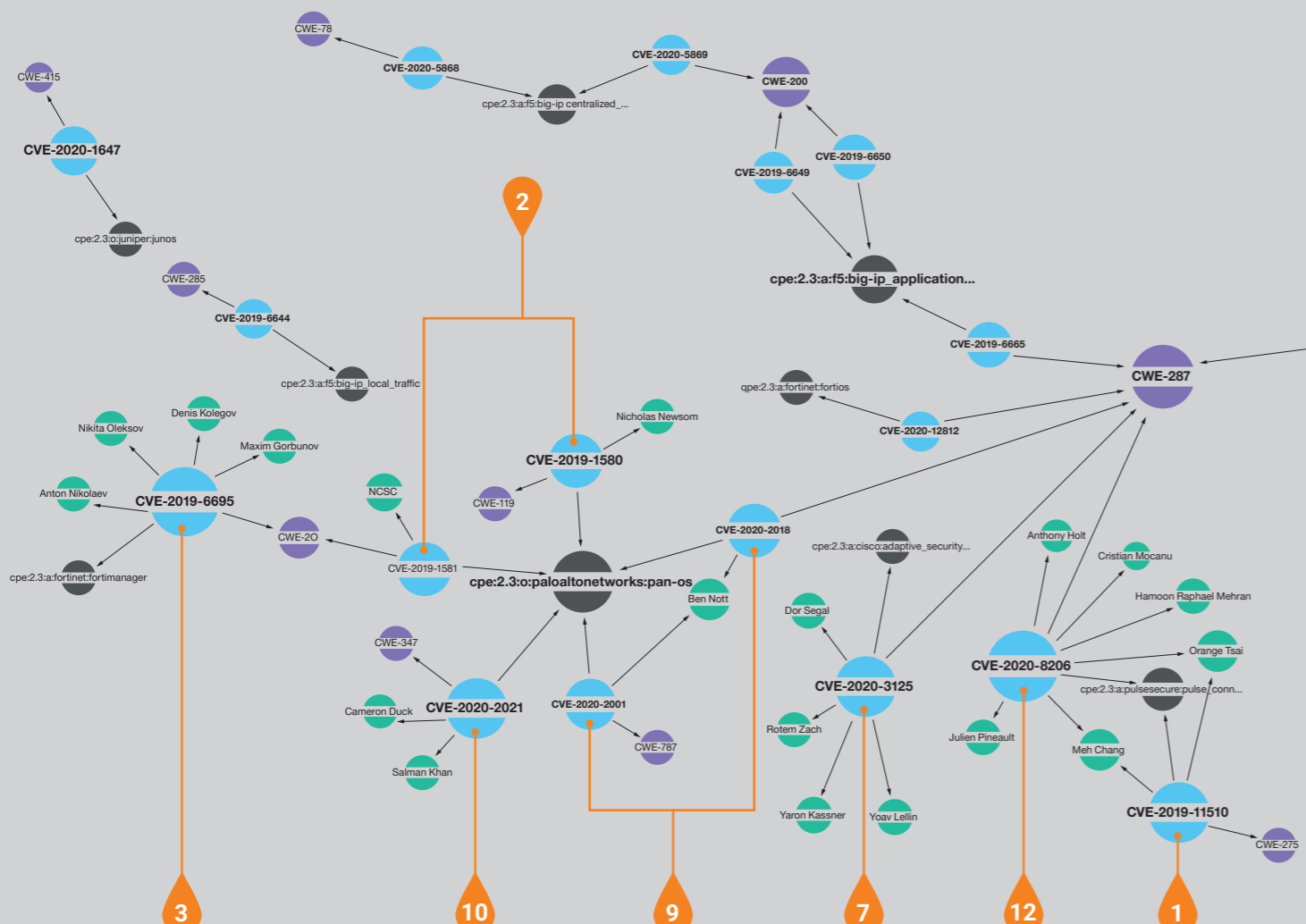
High and critical Windows vulnerabilities over time



CVE research cascade

Vulnerabilities discovered in security products

■ vulnerability ■ vulnerability class ■ researcher ■ platform



We believe this extraordinary surge in security product vulnerabilities is the function of three factors:

- The notable 'success' of Pulse Vulnerability, CVE-2019-11510, from May last year, which has been exploited in several high-profile attacks.
- The rapid and sometimes reckless adoption or expansion of secure remote access capabilities to accommodate remote workers, which made these technologies a very attractive target.
- A cascade effect in which the discovery of one vulnerability creates knowledge, experience and ideas, and thus leads to the discovery of different vulnerabilities in the same product, or similar vulnerabilities in different products.

1 May 08, 2019: CVE-2019-11510
 Orange Tsai & Meh Chang discovered a critical vulnerability affecting Pulse Connect Secure which would allow arbitrary file reading due to Permission Issues.

2 Aug 23, 2019: CVE-2019-1580/1
 Nicholas Newsom discovered a critical memory corruption vulnerability affecting PAN-OS SSHD. The UK's NCSC reported an RCE vulnerability in the PAN-OS SSH device management interface.

7 May 06, 2020: CVE-2020-3125
 Four researchers were credited with the discovery of a vulnerability in the Kerberos authentication feature of Cisco Adaptive Security Appliance (ASA) Software. The flaw was due to improper authentication which could allow an attacker to bypass Kerberos authentication.

8 May 06, 2020: CVE-2020-3187
 Mikhail Klyuchnikov again found another critical directory traversal vulnerability affecting Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software.

3 Aug 23, 2019: CVE-2019-6695
 Also due to improper input validation another critical vulnerability was reported in Fortinet FortiManager by an independent research team.

4 Dec 27, 2019: CVE-2019-19781
 A directory traversal vulnerability in Citrix Application Delivery Controller & Citrix Gateway which could lead to arbitrary code execution was discovered by Mikhail Klyuchnikov, Gianlorenzo Cipparrone and Miguel Gonzalez.

9 May 13, 2020: CVE-2020-2001/18
 Ben Nott is credited with finding two vulnerabilities affecting Palo Alto Networks PAN-OS Panorama. The first is a critical flaw that could allow an unauthenticated attacker to elevate privileges. The second could allow an attacker with access to the management interface to gain privileged access.

10 Jun 29, 2020: CVE-2020-2021
 Another vulnerability affecting Palo Alto Networks PAN-OS was reported by Cameron Duck & Salman Khan. This flaw could enable an unauthenticated attacker to access protected resources.

5 Apr 30, 2020: CVE-2020-5884/5/6/7
 Four critical vulnerabilities were disclosed affecting various F5 BIG-IP products. Three were caused by an issue with Inadequate Encryption Strength with the fourth being reported as an Exposure of Resource to Wrong Sphere.

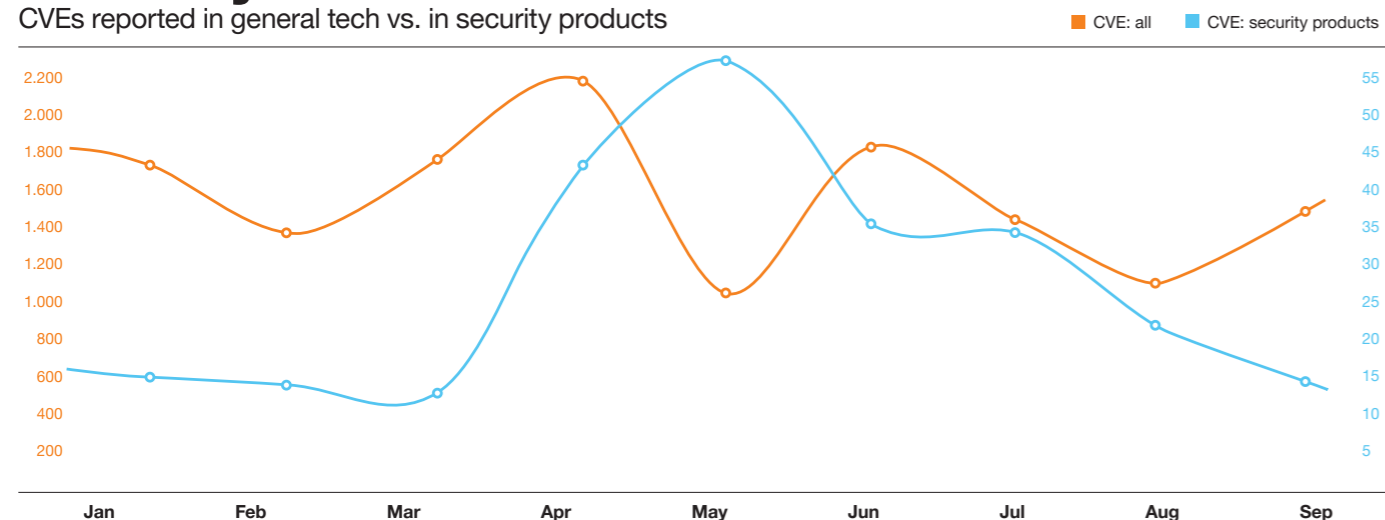
6 May 04, 2020: CVE-2020-1631
 A critical vulnerability in the HTTP/HTTPS service of Juniper Junos OS was discovered by Liang Bian and Leishen Song, this was another example of a directory traversal vulnerability.

11 Jul 01, 2020: CVE-2020-5902
 Mikhail Klyuchnikov was again credited with a vulnerability disclosure, this time impacting various F5 BIG-IP products. The critical flaw could allow an attacker to execute arbitrary commands and ultimately lead to complete system compromise.

12 Jul 30, 2020: CVE-2020-8206
 A high severity vulnerability affecting Pulse Connect Secure was disclosed as part of a security advisory. Orange Tsai & Meh Chang, who disclosed CVE-2019-11510 in May 2019, were again listed. The flaw was an improper authentication vulnerability which could allow an attacker to bypass Google TOTP (Time-based One Time Password).

Security vulnerabilities

CVEs reported in general tech vs. in security products



Vulnerabilities in security products

This chart illustrates the number of vulnerabilities in prominent perimeter security products vs vulnerabilities in technology overall. Noteworthy here is the extraordinary increase in security product vulnerabilities over the month of May 2020 – at the height of the global lockdown period.

The chart above illustrates that there was a distinctive anomaly that occurred in May this year, when reported vulnerabilities in general about halved compared to the previous month, while an unusually high number of vulnerabilities was reported in the aforementioned security technologies. Indeed, there was a four-fold increase in vulnerabilities reported in selected security technologies between March and May 2020.

In a recent advisory released by the U.S National Security Agency (NSA) titled 'State-Sponsored Actors Exploit Publicly Known Vulnerabilities'², they list the 25 known vulnerabilities in active use by state sponsored actors. Six of the 25 involve perimeter security technologies.

Given the incredible speed with which modern attackers are finding, exploiting and leveraging externally facing vulnerabilities, this extended window of exposure is significantly exacerbating the problems like ransomware, Big Game Hunting, IP theft and data leaks.

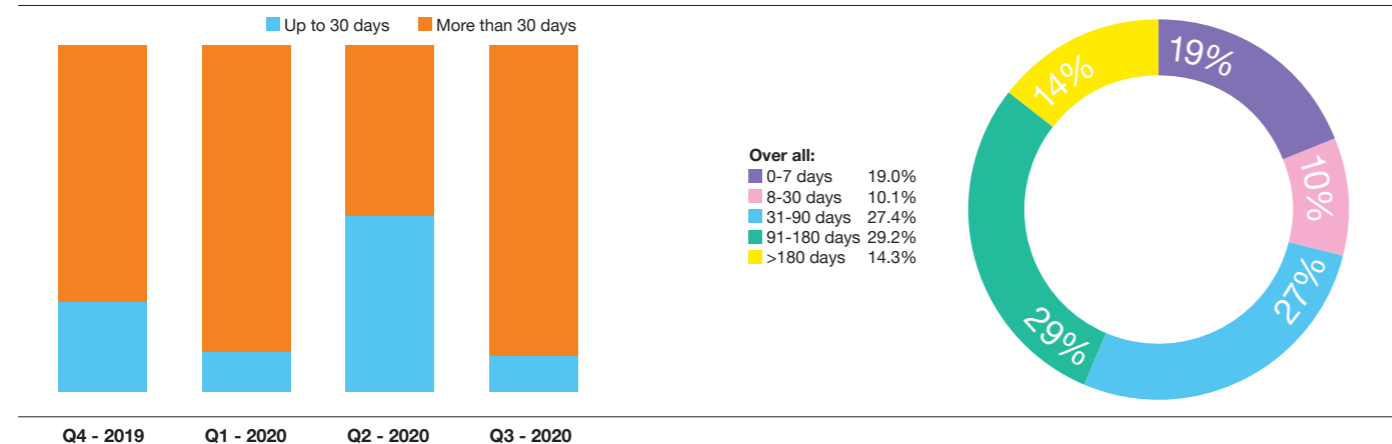
Customers are encouraged to ensure that they have the people and processes in place to respond in a timely manner to vulnerabilities in security vendor products when they're announced, or to engage with a provider that can assist with these functions. There is no doubt that there is a surge in these kinds of vulnerabilities at this time, which, when combined with the apparent rush to deploy or scale remote access capabilities, is leaving critical perimeter security exposed and contributing in a direct way to compromises and breaches.

Time to patch

A limited study we conducted across 168 security product vulnerabilities over the last 12 months reveals that, not only is the increased volume of these vulnerabilities a problem, but businesses are also taking far too long to patch them. We found that under 19% of vulnerabilities are patched within 7 days. However, the majority of 56.8% of these vulnerabilities are taking between 31 and 180 days to get resolved, and a deeply concerning 14% of vulnerabilities are still not addressed six months after notification.

Delayed patching

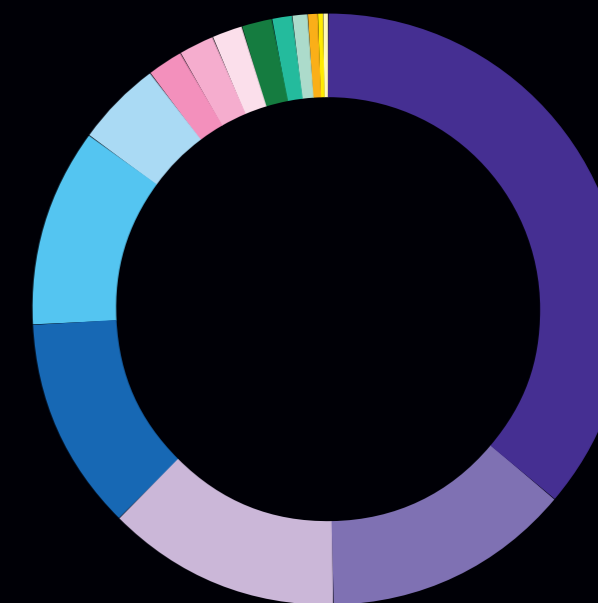
Time taken until a patch for a known CVE is applied (share per quarter over time, over all score)



Threat actors

Ransomware activity over the last 12 months (dark web monitoring)

Maze	36.31%
REvil	13.48%
Conti	12.77%
NetWalker	11.77%
Doppelpaymer	10.78%
PYSA	4.68%
CLOP	2.13%
Nefilim	1.84%
Suncrypt	1.70%
Ako	1.56%
Ragnar	1.14%
Sekhmet	0.99%
Avaddon	0.43%
Nemty	0.28%
Darkside	0.14%



Observing the dark web

The Orange Cyberdefense Malware Epidemiology Lab routinely tracks hacker portals and forums on the 'dark' web to monitor business shifts in the malware ecosystem. Through this activity we can observe new business models, changes in alliances, changes to technical infrastructure and announcements of new compromises and ransoms. The dark web is by definition 'dark' (not indexed by crawlers, search engines and other automated tools) and therefore difficult to monitor on a systemic basis, but by recording our observations of announcements and trading pages by various ransomware groups some patterns start to emerge.

Our Epidemiology Labs team tracks these shifts by observing traffic on the web forums. This allows us to comprehend shifts in the landscape at its core, rather than just at the 'edge' where variants of malware code ultimately impact the victim.

"Maze" on the rise

In our analysis of the darkweb 36.3% of published leaks were attributed to Maze. According to MITRE, 'MAZE ransomware, previously known as "ChaCha", was discovered in May 2019. In addition to encrypting files on victim machines for impact, MAZE operators conduct information stealing campaigns prior to encryption and post the information online to extort affected companies'.

Maze has exploded onto the threat scene since their emergence in 2019. It was the dominant player on the scene at that moment and promised to shape cybercrime for some time to come. REvil, Conti (which might be related to Ryuk), Doppel-paymer and Netwalker are other significant players but the landscape is constantly shifting as threat actors adjust their business models and form new alliances. The criminal ecosystem that manifests as ransomware is complex and dynamic. It consists of several diverse players that transact with one another around the various products and services that ultimately manifest as a ransomware attack and subsequent payment.

The persistent dominance of Maze over time is clear to see from this data, but so is the emergence of new players in the ecosystem, probably as the result of new or changed business alliances and practices in the underground. In a "Press release" published on their website on November 1, Maze claims to have shut down. Only time will tell if that is in fact true and what new challenges its members will seek in the future.

Tendency towards double extortion

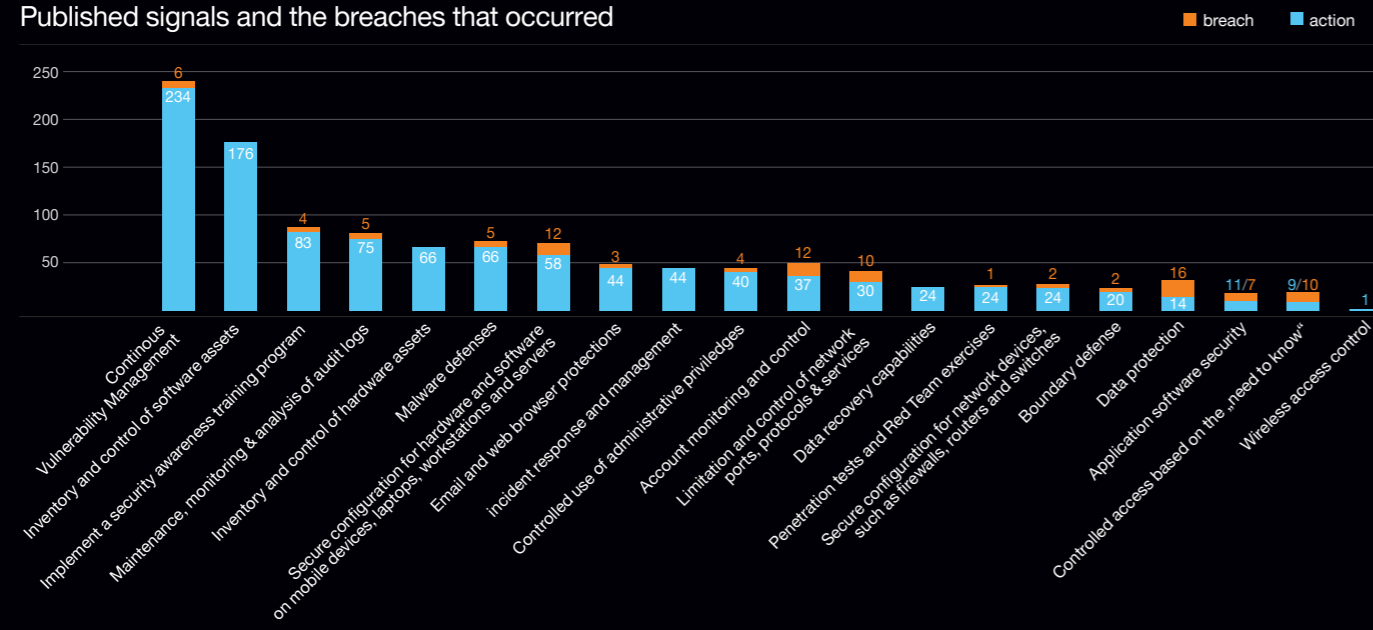
A relatively new trend amongst ransomware operators is the maintenance of 'leak' sites for the purpose of 'double extortion' in which the gang offers the decryption key if a ransom is paid but threatens to leak data if it isn't.

Most notable in the last quarter before this report was our increased visibility of the Conti ransomware group, who adopted this 'double extortion' practice in August this year and launched their own leak site. Conti overtook Maze in Q3 of this year to claim 22% of the ransomware activity we observed as a result. Most recently on October 20th, French IT services giant Sopra Steria suffered a cyberattack that reportedly encrypted portions of their network with the Ryuk ransomware, which might be connected to the Conti group. They were also credited with the Universal Health Services Ransomware Attack that impacted hospitals across the United States in September. We should expect to see more of this player over the next few months.

The key take-away for us here is that ransomware is a business, not a technology, and needs to be addressed first and foremost as a business problem. By completing the perfect triad of insatiable demand, limited supply and the smooth flow of value, cryptocurrencies have helped turn ransomware into a viable cybercrime business model. When cyber insurance policies started paying the ransom on behalf of the victim, it created the perfect storm. Ransomware is cybercrime's killer app and as far as we can see, it's here to stay.

CIS advice vs. actual breaches

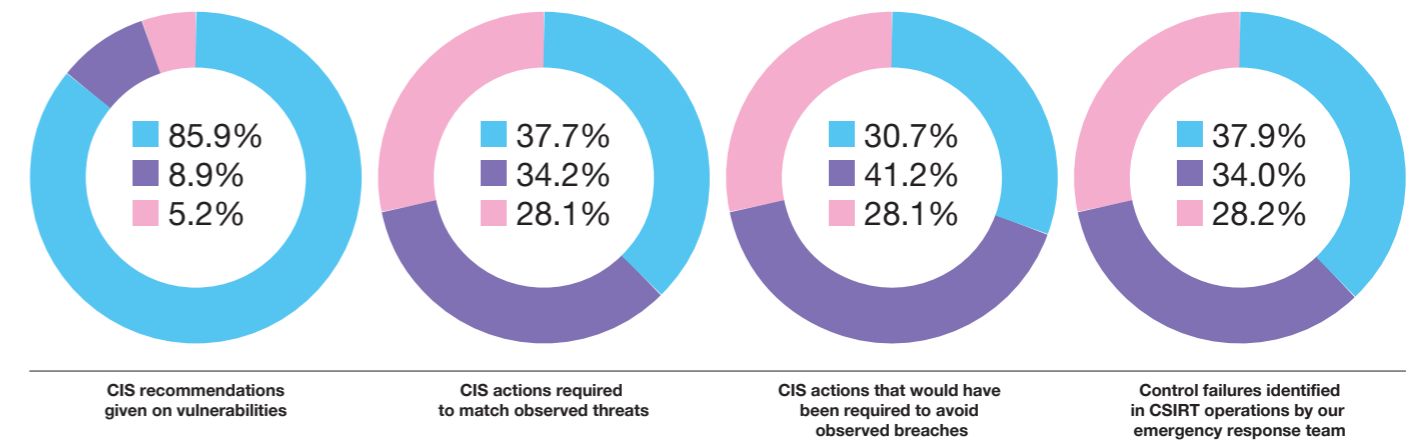
Published signals and the breaches that occurred



Control	Level	Recommended Control	Identified in breaches
Continuous vulnerability management	basic	234	6
Inventory and control of software assets	basic	176	4
Implement a security awareness and training program	organizational	83	5
Maintenance, monitoring and analysis of audit logs	basic	75	66
Inventory and control of hardware assets	basic	66	5
Malware defenses	foundational	66	58
Secure configuration for hardware and software on mobile devices, laptops, workstations and servers	basic	58	44
E-mail and web browser protections	foundational	44	44
Incident response and management	organizational	44	4
Controlled use of administrative privileges	basic	40	4
Account monitoring and control	foundational	37	12
Limitation and control of network ports, protocols and services	foundational	30	10
Data recovery capabilities	foundational	24	24
Penetration tests and red team exercises	organizational	24	1
Secure configuration for network devices, such as firewalls, routers and switches	foundational	24	2
Boundary defense	foundational	20	2
Data protection	foundational	14	16
Application software security	organizational	11	7
Controlled access based on the need to know	foundational	9	10
Wireless access control	foundational	1	1

Vulnerability, threat, breach

How does the advice requested and given match the actual requirements?



Security Controls and Failures

Examining the characteristics of breaches and incidents can easily degrade into a form of cybersecurity voyeurism. To ensure that meaningful lessons are gleaned from others' misfortunes, we need to examine more closely the mistakes that they made and consider the lessons we can learn from those.

Therefore, whenever we include a recommendation in a World Watch Signal, that recommendation is mapped to the CIS Top-20 controls framework³. This allows us to present a view on which standard security controls are occurring most frequently in our advisories.

This chart summarises the recommendations our analysts have made in our Signals, separated between Threats and Vulnerabilities on the one hand, and the control failures we recognised in breaches, on the other.

As can be seen from the list above, Continuous Vulnerability Management, Software & Hardware Inventory, Security Awareness Training and Logging are the most commonly referenced controls in our Signals. If we examine the failures noted in reported breaches, however, then Account Monitoring, Secure Configuration, Data Protection and Network Segmentation emerge as the most relevant controls. Vulnerability Management, however, appears in the top 5 controls when viewed from both perspectives.

It's interesting to note also the incongruence between the recommendations analysts make in response to Vulnerabilities and Threats vs the Control Failures we record when we examine public breaches. It seems safe to comment that while we are still called to consider and master the 'basic' controls described in the CIS framework, the breaches we analyse can be attributed to failures in the more advanced controls required by the CIS. This notion is very clearly illustrated in the set of graphs above.

As we can see from the three charts, in Signals where we comment on Vulnerabilities we are overwhelmingly likely to make recommendations that the CIS would classify as 'Basic'. Where the Signals comment on Threats we believe our customers need to respond or prepare for, the recommendations are spread much more evenly across the different levels of CIS control. Finally, where we comment on the control failures that led to breaches actually happening, we actually cite the more advanced 'foundational' and 'advanced' controls more often than the 'basics'.

In other words, while it remains clear that businesses need to master the basics of security to stay ahead of threats and vulnerabilities, this is not enough. We also need to master more advanced practices if we really want to avoid a breach and stay out of the news.

Conclusion

Breaches and compromises continue to grow, driven by strong systemic forces.

The pivot of ransomware to double-extortion and Big Game Hunting is a major theme in cybercrime this year. Ransomware is a business, not a technology, and must be countered as such.

The Maze crime group has spearheaded this new approach, making it the most noteworthy actor over the last few months. Maze is likely to fade from prominence as new alliances and business models are formed, but ransom and extortion attacks are here for the foreseeable future. The techniques being used are not new, but automation and orchestration has led to breath-taking speeds and multi-purpose malware frameworks enable the attacker to exploit a compromise in several diverse ways, before finally starting encryption.

Vulnerabilities play an equally important role in shaping the emerging threat, featuring almost twice as often in our Signals as threats. Microsoft (and especially Windows) security continues to shape the landscape, not only for the pivotal role it plays in most enterprise technology stacks, but also for the dramatic increase in serious vulnerabilities over the last 12 months.

The major security theme of 2020, however, is vulnerabilities in leading perimeter security platforms – particularly those used to facilitate secure remote access for the instant army of remote workers the COVID-19 crisis presented us with. As a result of fast implementation and scaling, patches and upgrades for these are taking far too long, and this problem appears to be getting worse.

State-backed and criminal hackers have noted this opportunity and pivoted dramatically to explore it, with devastating effect. Several major compromises and breaches exploited vulnerabilities in security products, including ransomware attacks, and these vulnerabilities are a popular constant in state-backed hackers' arsenals.

As a result, software inventory, vulnerability discovery and patching are the most frequently cited recommendations in our Signals, applying to 36% of all the Signals we published.

Mastery of these 'basic' security controls is essential for any business to stay ahead of the threat, but the basics are no longer enough. Every business is a target today, no matter how big or small. The odds still favour the attacker and compromises are therefore more common than ever.

Detection, impact limitation, response and recovery are therefore essential to reduce the duration and impact of a compromise and avoid a fully-fledged breach. Achieving this requires more than just mastering security basics. Sound architecture, segmentation, defence in depth, intelligence, detection, response, recovery and other advanced security practices must all be mastered if a business is to stay in operation and out of the news.



One of the largest European Energy providers hit by Ransomware

Attackers are using RagnarLocker Ransomware to target energy giant Energias de Portugal (EDP) and demanding \$10 million for ransom. The company is represented in 19 countries, with over 11.500 employees. The attackers claim to have extracted 10TB of sensitive data. ^[13]

MAY

New attack method by Ragnar Locker

The malware delivers Oracle VirtualBox virtualisation software and a Windows XP virtual machine to the targeted hosts. All physical and network drives from the targeted host then are mapped into the virtual machine, where the actual ransomware binary is executed and encrypts all files found in the mapped drives. ^[15]

Super Computers infected with Cryptocurrency Miners

Several supercomputers across Europe had to be shut down after Cryptocurrency mining Malware was discovered on them. This is the first known incident where external actors initiated this. Until then, only incidents where published where employees had installed cryptocurrency miners for their own personal gain. ^[14]

Never-ending story of Zeus

ZLoader banking malware, one of many forks of the infamous banking Trojan ZeuS, has been seen getting more attraction and activity in 2020. As ZLoader is used by different actors the methods and distribution varies, but e-mail with malicious attachments still seems to be used as the main entry point into victims' networks. ^[16]

Final: Misconfig of server leaks sensitive data

The French daily newspaper "Le Figaro" accidentally exposes 8TB of data due to misconfiguration of an Elasticsearch server. The exposed database contained 7.4 billion records of personable identifiable information (PII) of users and reporters. Additionally, the database also contained technical logs with information on the newspaper's backend servers, which could be leveraged by malicious threat actors. ^[17]



Charl van der Walt
Head of Security Research
Orange Cyberdefense

What disrupted this year:

Hidden impact of COVID

At the heart of the COVID-19 crisis, as its impact on IT and security was just beginning to crystalize for us, Orange Cyberdefense projected several implications of the crisis for the security ecosystem.

Many of these early predictions were universally held across the industry and many seemed self-evidently “obvious”. Several have persisted as ‘given’ truths, oblivious or even contrary to what an objective assessment of the facts in hindsight might suggest. Some have been generally ignored within the security industry and their implications for security irresponsibly understated, to our detriment we believe.

To examine the issue of what has truly and fundamentally changed in the security landscape as a consequence of COVID-19 and the subsequent rise in remote work, we consider three simple questions:

1. What did we observe about attacker behavior?
2. What did we observe about our users and their security behavior?
3. What did we observe about the resilience of technology, and particularly remote access technologies?

We answer these questions with the aid of diverse sources of data from within our business – our CyberSOC, Vulnerability Intelligence, World Watch and Managed Services operations - but also from select research performed by our contemporaries in the industry.

Finally, we also offer some practical guidance on how to handle this crisis – and similar ones if they come up.

What did we observe about attacker behavior?

Many across the globe accepted that attackers would exploit the pandemic to increase and improve attacks by leveraging three specific attributes of the crisis, namely:

1. Pandemic as perfect 'lure'; irresistible to people stressed, confused, anxious and trapped at home with limited social contact.
2. Users would be more vulnerable targets; anxious for information, eager to contribute and psychologically more vulnerable to coercion.
3. Users would be working from home and on personal IT equipment; abandoned beyond the safety of the corporate network perimeter, woefully unprotected and therefore an irresistibly juicy target for threat actors.

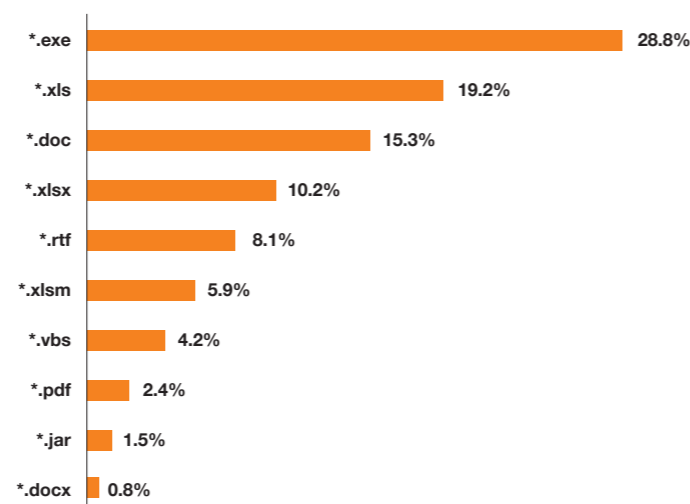
Did attackers swarm to exploit the crisis as expected? Here's what we really observed.

Attackers pivoted, but only briefly

A very thorough report from Microsoft⁴ provides one of the best sources of data regarding attacker behavior we have seen thus far. The report concludes that a momentary surge of COVID-19 themed attacks was really a repurposing from known attackers using existing infrastructure and malware, with the addition of new lures. In fact, the overall trend of malware detections worldwide did not vary significantly during this time. Moreover, COVID-themed attacks made up less than 2% of all attacks recorded over this period.

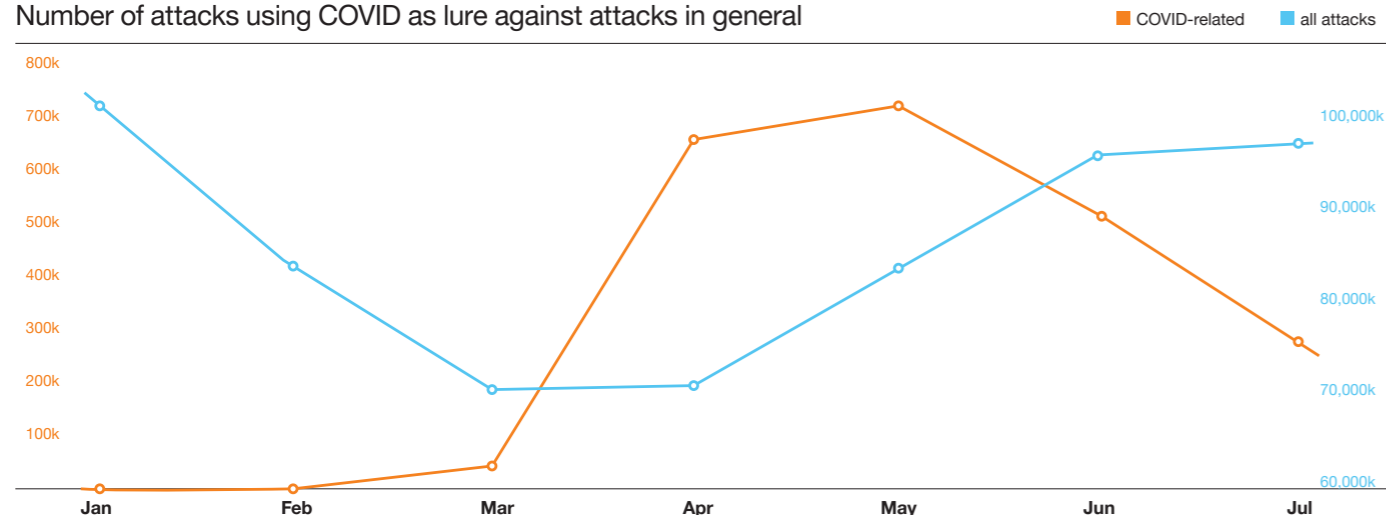
Our own data, tracking the registration of new DNS domains over time, shows that new registrations of COVID-related domains (using terms like 'covid', 'corona' and 'mask') decreased rapidly from the beginning of May to the end of June. At the same time, we observed other themes like 'Black Lives Matter' start to emerge, reflecting a change in media interest and exactly the kind of pivot that Microsoft also referred to in their report.

The charts below from Checkpoint⁵ tell a different story – the COVID 'blip' change in behavior is clearly visible. However, the majority of attachments used in malware delivery are still very old-school - .EXE, .XLS and .DOC – suggesting that attacker behavior changed only very superficially and temporarily during the crisis.



Attacks COVID-related vs. all⁶

Number of attacks using COVID as lure against attacks in general



In summary:

- Criminal attackers pivot rapidly but mostly superficially. New lures, themes and templates are common, but substantial changes to the fundamental business model are infrequent.
- We observed criminals pivoting around COVID-19 but it was short-lived. Attackers quickly move to new themes or revert to reliable old ones with alacrity. COVID-19 does not appear to be unique as a lure in this respect.
- The fundamental tactics, techniques and procedures deployed by the mainstream cybercrime ecosystem did not shift substantially because users were working from home.
- There were some indications of morality and "honour among thieves", but not enough to slow the rapid increase of ransomware and Big Game Hunting

State actors are people too

Our World Watch services reports on notable security events from Open Source Intelligence and assigns 'tracking tags' that allows us to detect trends and patterns.

One of the tracking tags we assign is used to identify major security events associated with state affiliated actors. This tag is used to track work or investment by governments, state-sponsored or supported hackers, state-developed tools or capabilities and their associated contractors, or if the story in the Signal is likely to be used by state-affiliated actors in offensive operations.

Another trend tag is used to mark scams, malware, IP theft, misinformation etc. linked to the COVID-19 outbreak. We use this tag to flag any Signal that focuses on COVID-19 research or which impacts the COVID-19 response effort or leverages the hype and hysteria about the outbreak to affect some other kind of attack, compromise or misinformation.

By comparing the prevalence of these two tags in our dataset over time, we can glean some insight into the behavior of state actors during the heart of the past COVID crisis.

We note Signals marked with the 'COVID-19' tag as orange bars, and those marked with 'State Actor' tags as a blue line.

The chart below clearly shows the emergence of 'COVID-19' as a theme in significant security news in March, peaking in May and then fading after July. This is consistent with our previous comments about the pivot to COVID-related themes by attackers.

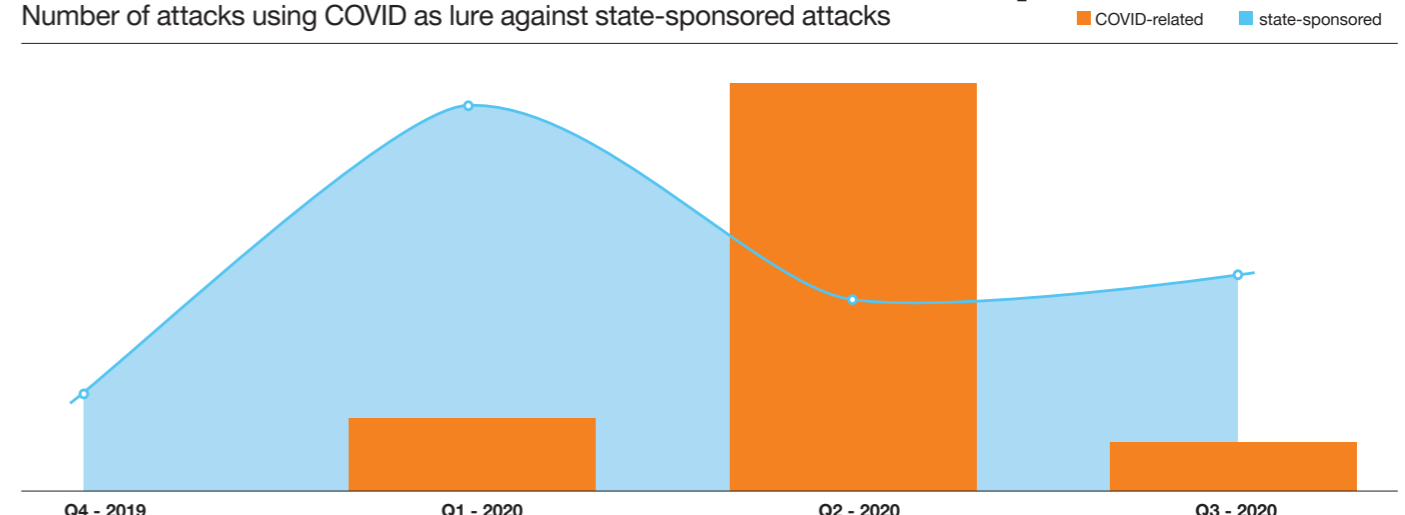
The line tracking nation-state related events follows a very different trajectory, however. Indeed, in our data, we note a slight increase in state hacking related stories in the first quarter before a slump in the second quarter when the pandemic and lockdown measures were at their peak, before increasing again slightly in the third quarter.

We believe that the apparent dip in activity during the second quarter has as much to do with a general malaise in the security industry as it does with the patterns of state hacking activities. We see no suggestion that state-backed hacking has increased due to COVID-19, or during the pandemic period.

If anything, our opinion here is that formal state actors work for governments and therefore act like most government employees – working fixed hours, taking leave and enjoying other employee constraints and benefits. Indeed, we would believe that nation-state activity may have decreased a little over the COVID period since those hackers would also have been impacted by COVID and lockdown, similar to other government departments.

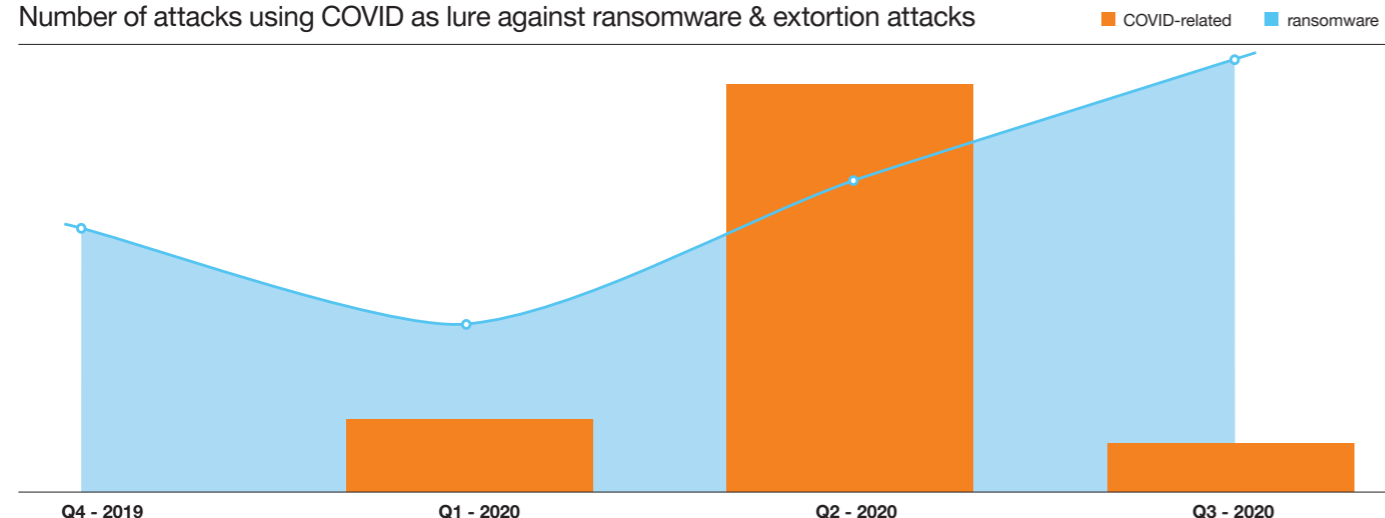
Attacks COVID-related vs. state-sponsored

Number of attacks using COVID as lure against state-sponsored attacks



Attacks COVID-related vs. ransomware

Number of attacks using COVID as lure against ransomware & extortion attacks



Ransomware perspective

The trajectory of another of our trend markers – this time ransomware – provides a telling counterpoint and valuable insight.

After a slight decrease during the first quarter of this year, significant ransomware incidents have been trending upwards in our data steadily through the course of the year. Ransomware is carried by a combination of powerful systemic drivers that include insatiable demand, limited supply and the smooth flow of value. Cryptocurrencies enable cheap, secure and reliable payment and thus turn ransomware into a viable cybercrime business model. Cyber insurance companies and their ‘negotiators’ further fuel the fire with an apparent preference for payment as the cheapest option for recovery from a breach.

The difference in trajectories between state-backed hacking (which was expected to escalate during the crisis but apparently didn’t) and ransomware (which was not given much thought in the context of the pandemic but grew steadily throughout) lies in the differences between their underlying systemic factors:

State hacking activities are fundamentally constrained by policy, budget, governance, skills limitations and other limitations. Priorities and targets may change from time to time, and the practice can be seen to be growing over time, but a state can’t suddenly produce more resources to pursue new objectives (for example corona research targets) without taking skills and resources away from other priorities. We believe this is the reason state backed activity did not change as much during the crisis as many of us expected it to.

The ransomware ecosystem is not constrained in the same way as state backed activities and will continue to grow inexorably until the systemic drivers described above are affected in some way.

The comparison between these two trends provides a valuable example to us about the importance of considering and understanding the systemic factors at the root of the security problem, rather than reacting to short-term media and vendor messages.

In summary:

- Similar to criminals, government actors may pivot to new targets or political goals.
- However, they are also resource constrained, and increasingly ‘formalised’ in their operations, so a pivot to a new target does not represent an overall increase in activity.

There are other major systemic factors and forces that have a much bigger influence on attacker behavior than the COVID-19 pandemic or the fact that people are working from home.

What did we observe about user behavior?

General predictions and even analysis of the security implications of the pandemic and lockdown speculated that people working from home would be targeted more, but also that they’d be more vulnerable to scams due to being remote and being generally under psychological strain.

Our data, again from the Signals database, suggests that attacks targeting people (e.g. phishing, water holing and scams) have been featuring more often than last year, but did not make the news more often during, or because of, the COVID-19 lockdown period. The orange bars show COVID-19-related events, while the blue line shows significant security events involving ‘the human’. Indeed, a closer examination of the data suggests that these kinds of incidents actually decreased at the start of the crisis and grew a little afterwards.

There are fluctuations in the monthly volumes not visible in the presentation below, but we don’t believe the data has the granularity to afford them much meaning. The CIRWA data shows peaks in activity in March and June 2020, separated by a deep trough in April and May. We identify the same disruptive impact of the crisis on the IT and security industry, but don’t observe any direct correlation between the scam volumes and the COVID-19 crisis.

BEC-Account compromise	2.86%
BEC-Bogus invoice	2.86%
Business e-mail compromise	2.86%
Fake software	5.71%
Phishing	52.86%
Robocall	2.86%
Spear Phishing	15.29%
Vishing	8.57%
Whaling	2.86%
Other	4.29%

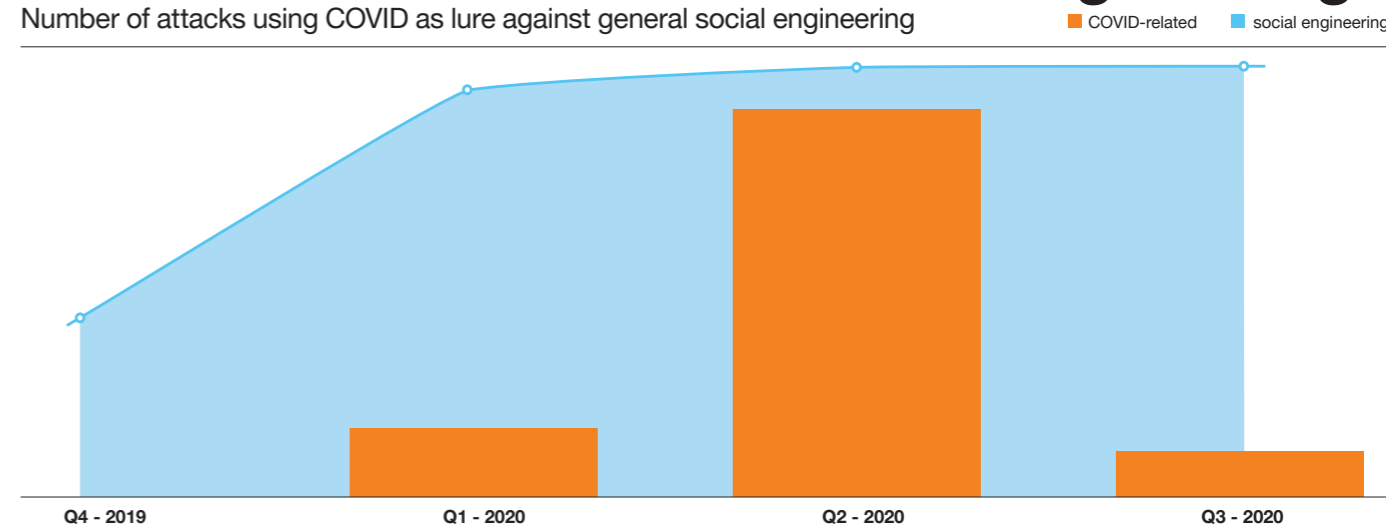
Attack is not compromise

We do not believe there is any evidence to suggest social engineering attacks were more successful during the COVID-19 period either.

A very useful open source data set from Temple University (‘Critical Infrastructures Ransomware Attacks’- CIRWA) records publicly-reported social-engineering attacks, i.e. attacks that were successful and are therefore pertinent to this discussion. There are 623 reported compromises in this dataset for the last few years. The bulk of the 70 social engineering attacks recorded for the twelve-month preceding the CIRWA report involve phishing and spear phishing. Zooming into the patterns over this time we note a similar trajectory to the volume of incidents in our own data.

Attacks COVID-related vs. social engineering

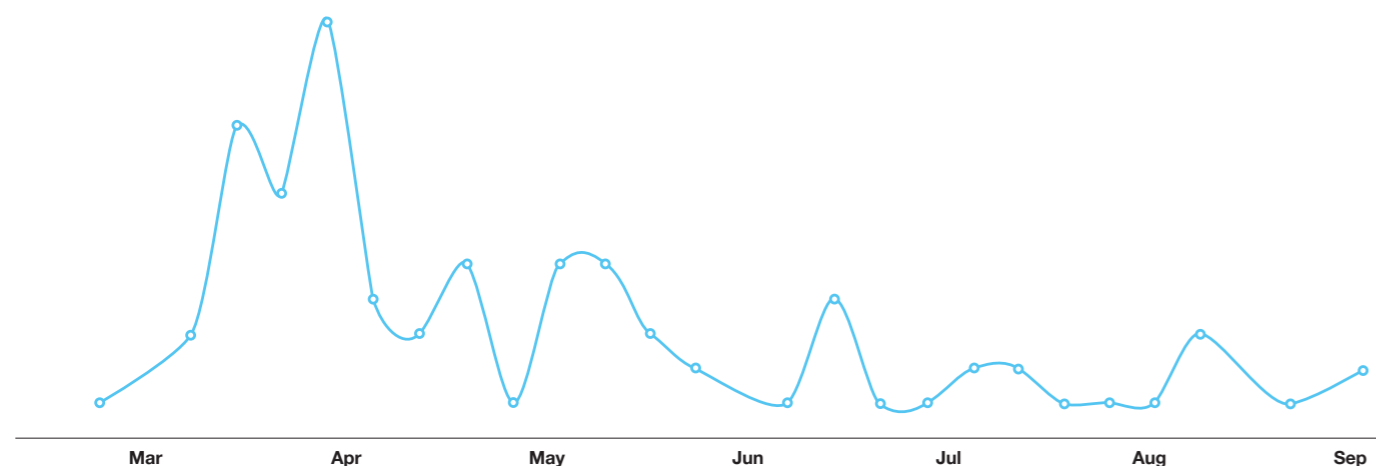
Number of attacks using COVID as lure against general social engineering



COVID-related security news

Security press articles containing the terms 'covid' or 'corona' in the title

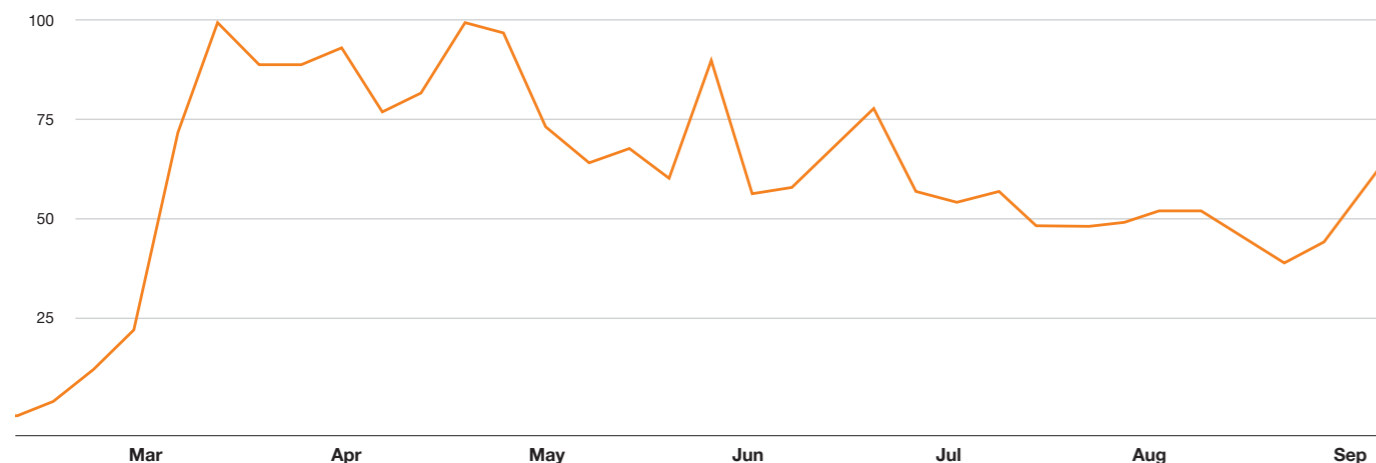
Security news stories



COVID-related Google searches

Searches containing the terms 'covid' and 'cyber'

Google searches



Press coverage & interest

A final consideration under this theme is the possible impact that proactive press coverage, corporate education and community efforts may have had on user awareness and preparedness for scams. Two data sources may shed led on this question.

The first chart from our own data tracks security press articles from a selection of major publications containing the terms 'covid' or 'corona' in the title. The second, from Google Trends shows searches containing the terms 'covid' and 'cyber'. It is clear from both datasets that interest in the issues of cybersecurity in the context of the pandemic peaked early in March and were maintained at high levels until June before it started waning.

It may well be that these extraordinary levels of media attention spawned sufficient public and corporate awareness that helped prevent far worse outcomes than we actually observed. We understand from our expert partners that many businesses adjusted their corporate security awareness training programs quickly in response to the virus and noted satisfactory levels of response from their users.

In summary:

- User vulnerability:
 - We see no evidence suggesting that users were more vulnerable to COVID-themed scams.
 - This may be because of extensive pro-active efforts.
 - A portion of users remain consistently vulnerable to phishing and scams, but this was not noticeably impacted by COVID-19.
- User responsiveness:
 - Users were actually quick to learn how to spot COVID-related scams and respond accordingly.
 - Attackers may prefer 'traditional' templates for their scams, like phishing targeting internet banking and O365.
- Attacker proceeds:
 - No noticeable increase in illicit Bitcoin transactions over the lockdown period.
 - No evidence that attackers were profiting more during lockdown.

What did we observe about security technology?

Another common theme in security predictions about the security impact of the pandemic (at least in our own predictions) was that due to the large-scale rapid rollout of remote access technologies like VPNs, these systems would be poorly configured and maintained and more frequently targeted by attackers, leading to compromise.

More access

Data from our own Managed Services Operations regarding service requests on VPN technologies demonstrates just how dramatically the adoption of secure remote access technologies increased worldwide.

The chart below shows levels of demand from our SOC over the COVID-19 period. We can clearly see the increase in demand for installations, support and service for perimeter security technologies at the beginning of the lockdown period, mirroring what the external data is telling us.

One such data source is top10vpn.com⁷, who report:

1. Global VPN demand increased 41% over the second half of March and remains 22% higher than pre-pandemic levels
2. 75 countries with significant increases in VPN demand since COVID-19 social restrictions began to be enacted
3. 21 countries where the demand for VPN more than doubled
4. Highest volume VPN demand: U.S. (41% peak increase), UK (35%) and France (80%)
5. Largest VPN demand increases were: Egypt (224%), Slovenia (169%) and Chile (149%)
6. Largest sustained increases were: Egypt (154% – over 14 days since initial peak), Peru (119% – over 28 days since peak), South Africa (105% – ongoing since mid-March)

More vulnerabilities

As we've illustrated elsewhere in this year's report, we note an anomaly in our data about vulnerability statistics over the COVID period: in conjunction with the increased deployment of security technologies, we also observe an extraordinary increase in reported vulnerabilities (not necessarily attacks) for these kinds of systems, including technologies from several leading perimeter security product vendors.

We believe this extraordinary surge in security product vulnerabilities is the function of three factors:

1. The notable 'success' of Pulse Vulnerability, CVE-2019-11510, from May last year, which has been exploited in several high-profile attacks.
2. The rapid and sometimes reckless adoption or expansion of secure remote access capabilities to accommodate remote workers, which made these technologies a very attractive target.
3. A cascade effect in which the discovery of one vulnerability creates knowledge, experience and ideas, and thus leads to the discovery of different vulnerabilities in the same product, or similar vulnerabilities in different products.

More attacks

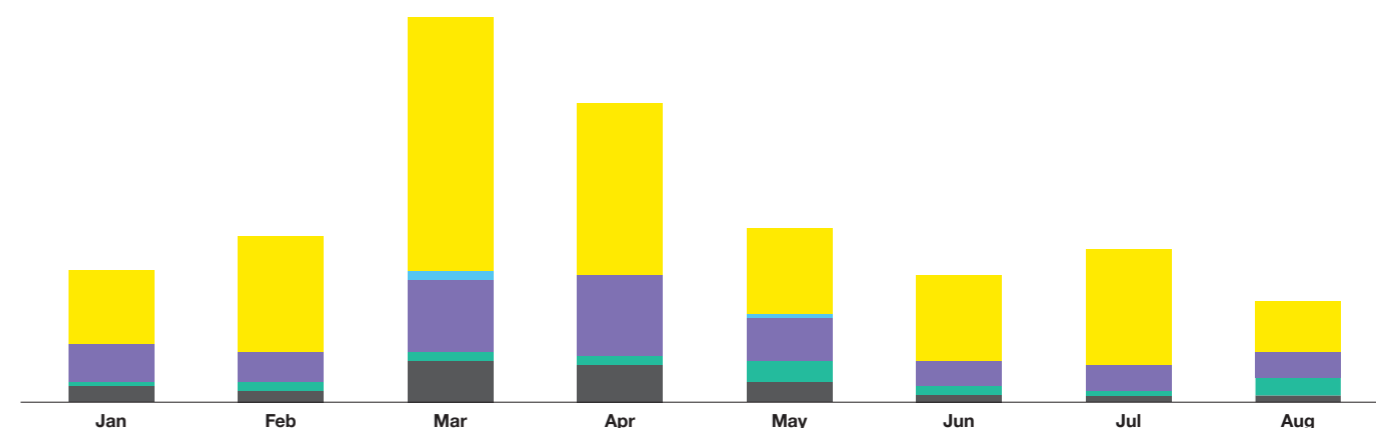
Several of the vulnerabilities recently discovered in perimeter security products have become popular targets for attack by cybercriminals like REvil and have been pivotal in some of the major breaches of the past year.

They are also popular with state-backed actors. In a recent advisory released by the U.S National Security Agency (NSA) titled 'State-Sponsored Actors Exploit Publicly Known Vulnerabilities'⁸, they list the 25 known vulnerabilities in active use by state sponsored actors. Six of the twenty-five involve perimeter security technologies.

Types of requests

Number of tickets filed by category in our service desks

Alerts Change requests Incidents Problems Service requests



Managing the crisis

In light of the threats and concerns raised, we offer the following guidance to businesses and professionals considering the cyber element of the crisis. The virus does have an impact on cybersecurity. The consequences are not unavoidable, however. Consider your cyber response strategy in this light.

Don't panic

Our guidelines for remaining rational in the crisis are as follows:

1. Understand that we are experiencing a state of **heightened threat, but only slightly increased vulnerability**. We cannot control the threat, but we can control the vulnerability, so let's focus on that.
2. **Understand what has changed and what hasn't.** Your business's threat model may be very different today than it was yesterday, but it may also not be. If it hasn't changed, then your strategy and operations don't have to either.
3. **Maintain context.** Right now, the crisis is medical and human. Don't let the hype about cybersecurity distract you from that. The internet will survive.
4. **Focus your efforts.** You will be able to achieve very little during this time of diminished capability, so spend time and energy on considering what your primary concerns are and focusing on those.
5. **Take the time to improve.** If there are elements of your infrastructure or processes that were not ready when this crisis broke, there is time now to review and improve them.

Check on your suppliers

For many businesses, there is a direct correlation between suppliers' level of security and their own, as recent incidents like the notPetya malware campaign have illustrated. At this time of elevated risk, businesses have to worry about the security of their suppliers and partners as much as their own.

Security and risk teams should consider opening and maintaining channels of communication with suppliers, providers, consultants and partners who may have access to sensitive systems and data. Discuss their responses to the elevated threat levels at this time and ensure that they remain appropriate and in line with your own.

Prioritize

As we've argued previously, we want to focus our strained resources on elements of the threat that are of most concern to us right now. Determining what the 'important threats' are is, however, very difficult. Indeed, it's a challenge that we've spoken and written about extensively in the recent past. It's our assessment that the cyber threat landscape (even without an exacerbating global crisis) is too complex and fluid to reduce to simple lists or cheat sheets. At the risk of falling into that trap, we suggest thinking about priorities during this crisis in terms of two realities – the things that have changed, and the things that haven't changed.

The things that have changed

As should be clear from reading this paper, we assess that only a small aspect of the cyber threat landscape has substantially changed as a result of the pandemic. We believe these are:

1. Your people are more vulnerable to social engineering and scams than normal.
2. You have less control and visibility over the IT systems you protect than you're used to.
3. Your users may be connecting from systems and environments that are fundamentally insecure or possibly just poorly configured.
4. You have rushed to implement remote access systems without having the time to plan and execute as well as you would like.
5. You, your team and your providers may be operating with diminished capacity.

The things that have not changed

As much as we are living through an unprecedented time in recent human history, there is really very little about the current threat landscape that is fundamentally new. As such, our priorities from a cyber point of view don't need to divert too much from what they were before the crisis:

1. Social engineering attacks like Business E-mail Compromise (BEC) are nothing new. Appropriate responses have not changed either, despite the elevated threat level.
2. Attacks against cloud-based interfaces, remote access systems and VPN gateways have been escalating for some time now. Though perhaps more acute, these attempts are not new.
3. Remote working and facilitating secure remote access for mobile workers is a very well understood problem and there are several technologies and approaches in our toolbox, suitable for almost any budget and level of technical sophistication.
4. The modern workforce has been mobile for two decades now, and vendors and IT teams can offer several methods for monitoring, maintaining and managing remote endpoints. More complex requirements, like remote isolation and triage, are easily met, even without a huge budget.

Establish emergency response procedures and systems

Preparation is essential. Take some time to facilitate a planning session with key IT and security role-players to consider your response capabilities in the event of a suspected compromise or breach. Areas to consider here include:

- How would you detect a breach? What indicators might be available to you beyond the conventional, e.g. reports from users or external service providers?
- Who needs to be informed and involved if there is a crisis?

- How might a response team communicate and collaborate, even under a worse-case scenario where trusted systems may be impacted?
- How would you communicate with other stakeholders like users, regulators, customers, board members and shareholders?
- Are you in a position to isolate an endpoint or server, whether remotely or onsite?
- Do you have access to a capable incident response team, whether in-house or via a partner?
- Do you have effective backup and a disaster recovery plan in place? When last was it tested? Could it be tested now?
- Do you have a policy position on ransomware and extortion? If you believe you would pay a ransom, do you have the funds and systems available to do so? You should also consider your negotiating strategy and appoint a negotiating team ahead of time.
- Do you understand your regulatory requirements, for example with regards to the UK ICO, and are you prepared to follow them in the event of breach?

Establish a security support hotline

Your users are feeling highly anxious right now and cyber-threats are certainly adding to anxiety levels.

Providing users and even customers with a number or address they might use to speak to someone rationally about technical and cognitive attacks they may suspect, or about their own systems and behaviors, is a powerful tool for reducing the level of anxiety and improving your security posture. If you already have a support hotline, prepare for (at least initially) a rapid increase in the volume of calls, e-mails and other available methods of communication.

Review backup and DR

Two real threats even before the crisis, which have arguably escalated due to the pandemic, are ransomware and Denial of Service.

Take some time to review the state of your backups and the readiness of your data and Disaster Recovery processes.

In this process, you need to think about home workers and the data they may be working with locally. If you don't already have a suitable backup system for remote users, then readily available public cloud solutions like Google Drive, Dropbox and Microsoft OneDrive may present a viable alternative under the circumstances.

Provide secure remote access

Secure and reliable remote access to the internet and corporate systems appears to be the biggest challenge facing our customers right now. The following principles should serve to guide the design of any remote access architecture:

1. Clearly understand your threat model. We would assert at this time that the primary challenge is to provide appropriate authentication and access control to data and corporate systems.
2. Make sure you secure DNS. Several contemporary attacks involve redirecting DNS requests in order to present phishing sites or conduct Person in the Middle attacks. Control the DNS servers that your workers use, whether by using VPN configurations or simply having them hardcode DNS resolvers on endpoints.
3. Implement multi-factor authentication. Review all your remote access systems (including web interfaces, VPN and remote access gateways) and consider how strong authentication might be implemented. A full push-to-mobile solution – as is available from Okta, Duo, Google and Microsoft – is likely going to be the best option in terms of usability, security and perhaps even ease of deployment.
4. Clarify and communicate smart password policies. We emphasize again that currently, attacks against remote access technologies is one of the key threats. If you're not able to implement strong multi-factor authentication (MFA), then consider what you can do to ensure users make strong password choices. Specifically, users should be encouraged to:
 - Change their password
 - Chose a password that they have definitely not used elsewhere, and
 - Choose a passphrase that is long but easy to remember, rather than short and complex.
5. Manage your security devices. Current campaigns are actively targeting specific corporate systems like Citrix Application Delivery Controller (NetScaler ADC) and Citrix Gateway (NetScaler Gateway) servers, Zoho ManageEngine Desktop Central and Cisco RV320 and RV325 routers. Unpatched Pulse VPN servers are another popular target. These attacks exploit known and patched vulnerabilities. In other words – they are real, but they are not difficult to fix. Ensure that you know where all your Internet-facing remote access technologies are, and that each is appropriately patched and configured.

Establish visibility over remote endpoints

With users now working remotely on a large scale, enterprises without a robust endpoint detection and protection or response capabilities may find themselves flying blind through the eye of a crisis. Businesses without any endpoint capabilities should be considering their options at this time. Two obvious routes to take for most endpoint configurations are:

1. Microsoft Sysmon: Microsoft's own free System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events using Windows Event Collection or SIEM agents and analyzing

them, you can identify malicious or anomalous activity. Sysmon is relatively safe and easy to deploy, supports most contemporary Windows versions and there are numerous commercial and open source projects that offer configuration, management, collection and reporting support.

2. Commercial EDR: Several vendors offer reputable endpoint detection, protection and response products, including CrowdStrike, Cybereason, Cylance, Palo Alto Networks TRAPS/Cortex XDR, SentinelOne and others. Many of these solutions are highly reliable and proven effective. Some also offer a variety of 'isolation' features that allow one to take an endpoint partially offline while incident triage and forensics can be performed. These solutions are available as managed services as well, speeding up the process of implementation.

Aside from these obvious solutions, other options exist to achieve the same ends. For example, VPN agents can be used to implement virtual network isolation, while open source products like Google's Remote Response (GRR) offer workable remote triage and forensics options.

Consider malicious mobile applications

We've observed a five-fold increase in the number of malicious mobile applications detected between February and March this year. We can expect that this trend will continue as the crisis stretches out.

Options available to companies in regards to malicious applications include:

- Prohibiting all installation of third-party applications.
- Implementing whitelisting to allow installation of approved applications only.
- Verifying that applications only receive the necessary permissions on the mobile device.
- Implementing a secure sandbox/secure container that isolates the organization's data and applications from all other data and applications on the mobile device.

For most businesses, the only practical technical solution is to provide their users with a mobile Anti-Virus solution or to provide company-issued mobile devices with Mobile Device Management (MDM) software installed.

Consider patching and hardening of remote endpoints, including mobile

On March 25, 2020 we published a Security Advisory about two critical zero-day flaws in Windows systems. Microsoft warned that limited, targeted attacks had been detected in the wild.⁹

Prior to that, on March 11, 2020, we warned customers about a remote code execution vulnerability in the Microsoft Server Message Block 3.1.1 (SMBv3) protocol that would give an attacker the ability to execute code on the target SMB Server or SMB Client.¹⁰

These kind of vulnerabilities on Windows servers and desktops continue to appear and are actively being exploited. The same risk exists for mobile devices, both personal and private. Although we don't believe that they represent the most likely attack vector at this time, remote endpoints cannot be ignored and failure to address them will expose your business to unnecessary risk.

Once the other priorities we discussed in this section have been addressed, effort should be invested into considering how remote user endpoints might be patched at this time. One viable option (in lieu of a viable central patching solution) may be simply to advise users of essential patches via company communications and request them to apply the patch directly.

This is far from a perfect response to the problem, but as suggested earlier: at this point every win counts.

A lesson to learn

Finally, we believe the impact of this pandemic and our collective response hold valuable lessons for security practitioners; the virus demonstrates how closely-knit our societies and economies are, and how spectacularly a catastrophe in one area spills over to the other. In responding to the crisis, we are learning to appreciate the impact that our behavior has on the whole of society, and not just on us as individuals, families and businesses. This is an essential lesson for the security community too.



Our proposed list of priorities

Proceeding from the breakdown we've modelled earlier, we would propose the following general set of priorities that businesses should be considering in light of the current threat landscape.

If your own security priorities are not already clear to you, we propose that you focus on the following responses, in order of importance:

1. Establish emergency response procedures and systems.
2. Establish a security support hotline.
3. Review backup and Disaster Recovery (DR).
4. Equip your users with the information they need to make good decisions.
5. Provide secure remote access.
6. Establish visibility over remote endpoints.
7. Consider malicious mobile applications.
8. Consider patching and hardening of remote endpoints, including mobile.
9. Review your insurance.

Conclusion

There are other massive shifts in the underlying landscape that have broad implications for security, but which we don't have the space to cover here. These include massive increases in dependencies on hitherto under-regarded technologies like videoconferencing and collaboration tools, an almost manic move to the cloud for enterprise systems and a completely unprecedented increase in online commerce.

The true impact of the COVID-19 crises and the resultant global lockdowns on cybersecurity is therefore not in the acute and obvious implications, like increased phishing or a focus by state actors on healthcare, but rather in the larger, systemic implications, which can be summarized as follows:

- Massive adoption or expansion in remote access capabilities, thereby increasing the management overhead for security teams and expanding the attack surface for adversaries.
- Increased importance of remote access technologies for businesses, making them simultaneously more attractive as targets and harder to maintain, upgrade and patch.
- Increased interest from attackers in these enterprise technologies due to their exposure to the Internet and the high levels of access they afford if compromised.

Other systemic factors, some related to COVID-19 and others independent, continue to shape the threat landscape. The systemic impact of COVID-19 on cybersecurity is not yet apparent, but the incredible move to cloud, the unprecedented acceleration of ecommerce and the sudden dependence on previously insignificant technologies like videoconferencing are sure to add to the already-visible impact that the upscaling of remote access has had, and further shape the future agendas of attackers and CISOs alike.



JUN

A shift in extortion? Increasing the pressure

The ransomware operators of REvil (Sodinokibi) group launched an auction page, which increases the pressure for the victims to pay. Besides threatening availability by encrypting files and systems; they went one step further by exfiltrating the victims' data and thus threatening confidentiality of sensitive data, if the victim chooses not to pay, data will be published on their dedicated leak site. ^[18]

A bluff, nothing else

Scammers have shifted from a sextortion bluff claiming to have recorded victims visiting adult sites towards claiming to have extracted their sensitive data. If not paid up, they would publish it. Unlike, extortion-driven ransomware attacks that make sure their victims notice them once they have reached the final stage, this scam shows no signs of it. The demand varies between \$1500 and \$2000. ^[19]

The Twitter Hack

Attackers gained control of many high-value Twitter accounts by targeting a small number of employees through a phone spear phishing attack. With the information gathered they then accessed internal systems and extended their phishing campaign towards other, higher-privilege, users. ^[22]

JUL

Feed the Devil ...

Garmin suffered from a WastedLocker ransomware attack, most likely executed by the group EvilCorp that caused a several days outage for some of Garmin's services. According to reports, the company has obtained a decryption key, indicating that they have paid the ransom in order to decrypt their systems and files. ^[21]

CVE-2020-1350: Vulnerability in Windows Domain Name System (DNS) Server

The vulnerability is "wormable", allowing malware to replicate and spread itself, it is a remote code execution vulnerability, which allows attackers to run arbitrary code in the context of the Local System Account. ^[20]



Charl van der Walt
Head of Security Research
Orange Cyberdefense

Tech insight:

A dummy's guide to cybercrime

Our business is to detect and defend against attacks. Our mission is to protect and defend customer assets. To do this we analyse attack and vulnerabilities, we try to predict the attackers moves and be a step ahead. What we rarely did up to now is to deeply assess the attackers actual situation. We ask "what does the hacker do next and how?" but never "why does he do it?"

So let us take a look at the dark side. Even in previous reports we have seen clear indications of professionalizing. Common attacks become more sophisticated, though top-notch APTs are still scarce. Attacks decrease significantly during holiday seasons. Cybercrime is a business now. But how does it work? What business models exist? How do criminals collaborate, how do they leverage and actually monetize stolen digital goods like intellectual property, credentials, credit card numbers or healthcare data?

Interactions and dependencies are complex. We have taken a closer look in this chapter, but there is more to discover in the full whitepaper you can find on orangecyberdefense.com/global/cybercrime/



The new realities

It is commonly understood that cybercrime has become a major industry. According to the World Economic Forum's (WEF) Global Risks Report 2020¹¹, by 2021 the global cybercrime damages may hit \$6 trillion. Their surveys concluded that cyberattacks were the second most concerning risk for global commerce over the next decade.

Not all cybercriminals are highly skilled or technical as these days there are offerings like Crime-as-a-Service (CaaS) that can provide non-technical criminals with the ability to conduct cybercrime operations. These types of services have most likely increased the amount of cybercrime seen today, as criminals do not need years of experience in hacking or malware to conduct an attack. This type of professionalisation has shown in the statistics. While highly critical attacks are still kind of rare, we have seen in the past few years a massive shift from low to medium criticality among the incidents we have recorded, reflecting the availability of fairly sophisticated attack tools to less skilled criminals.

Ransomware & DDoS most common

According to WEF the most popular types of services are ransomware and Distributed Denial of Service (DDoS) attacks. Cybercriminals group together to form specialist groups that collaborate and form a web of inter-connected syndicates, often also crossing over to and from conventional forms of crime.

They are organised like businesses and adopt traditional business practices, like "customer service" and "after sales support".

Such common wisdom is frequently cited and readily shared, without many of us truly comprehending the realities behind them. One critical element of cybercrime that is perhaps less understood than it should be lies at the very root of the problem, namely the flow of money and value between different players in the cybercrime ecosystem.

The cybercrime ecosystem hosts a range of players each with their own avenue of expertise and many ways to monetise products like malware, botnets and stolen information and illegal goods and services. A true understanding of this ecosystem and its systemic drivers is essential to getting to the core of the cybercrime problem and developing a strategy that will enable us to strike it at its root.

In this section we will focus on the main role players within the cybercrime ecosystem and potential links between them to paint a clearer picture of how they interact.



Marketplaces

The dark web is a part of the internet where servers use Tor, I2P, GNUNet, ZeroNet or Freenet to hide their IP addresses. The most popular dark web is accessed via the Tor browser where sites on the Tor network have domain names ending with .onion. There are several search engines that try their best at indexing these sites.

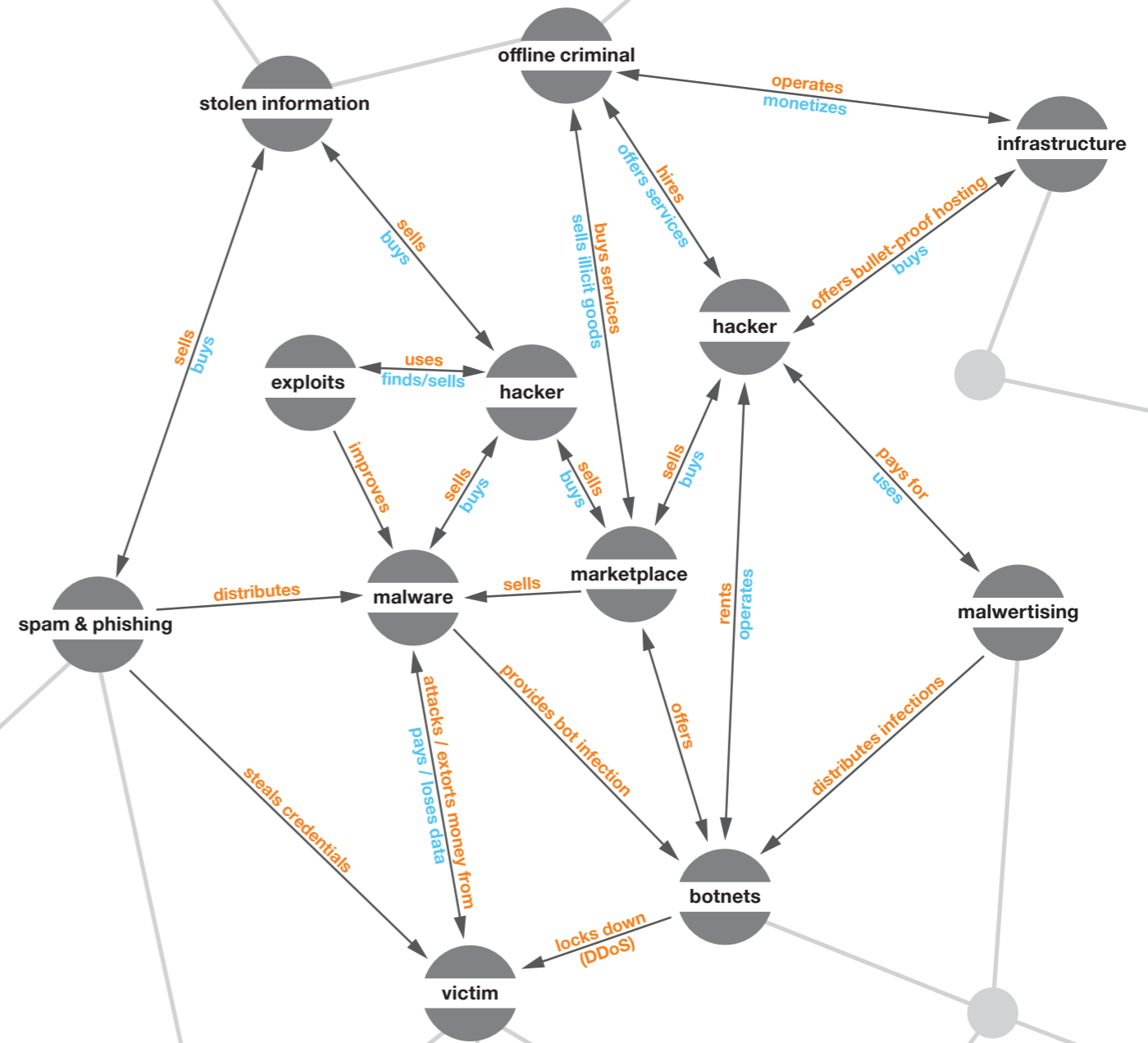
An example of some of these search engines are Torch, Kilos, Candle, notEvil and Haystak etc.¹² There are also search engines on the clearnet for Tor's hidden services, like Ahmia or webpages with links to dark web sites like Hidden Wiki.

It must be noted that the dark web is different from the deep web, which is the part of the internet that is not indexed by search engines, for example, webpages only accessible when authenticated to a site. The dark web itself makes up part of the deep web and the deep web is where the dark side of the internet flourishes.

There are also many sites on the dark web that do not have malicious intent and many legitimate sites on the Internet have a presence on the dark web too.

As for the darker side of the dark web, there are a lot of online markets, forums and Internet Relay Chat (IRC) communities that deal with illicit goods like drugs, weapons, stolen identities and of course cybercrime products and services amongst other things. Most markets provide ratings, descriptions, reviews, and even technical and customer support. They have vendors, buyers, and market administrators too, like eBay. These marketplaces have improved the customer experience of buying illicit goods and services online by providing easy access and use of escrow services. They often require a joining fee and a vetting process to ensure their spot as a vendor, or on a forum.

In Europol's 2019 cybercrime report¹³, it was suggested that the dark web is getting more fragmented, in the sense that there are more single-vendor shops and smaller fragmented markets, which even cater to specific languages. These markets and forums try to keep user identities anonymous to protect their clients from law enforcement¹⁴ and when deals are done, they commonly involve some form of cryptocurrency and third-party escrow service. This is a service that ensures that a transaction clears between two parties making a deal and is particularly useful with dark web deals when both parties may not be inherently trustworthy.





Malvertising sphere

Malvertising is the running of malicious ads on legitimate or hacked websites via third party ad networks. To simplify the online advertising industry, there are publishers (websites selling ad space), advertisers (people wanting to promote their products etc.), ad exchanges (an online platform that publishers can sell ad space on) and ad network resellers (buy ad space and connect the publishers and advertisers)¹⁷. A legitimate publisher can offer ad space on their website that an ad network can purchase and sell to a potentially malicious advertiser.

Malvertising can be sold as a service by malvertisers to be used as a distribution method for malware campaigns. From a victim's point of view a malicious ad seems legitimate, but the infrastructure in the background delivers a malicious content. Malicious advertisers inject code into ads that legitimate ad networks push to publisher websites. These ads can redirect a user to a web page running an exploit kit etc.



Exploits sphere

The exploits sphere is all about the discovery, development and selling of exploits. A vulnerability is a weakness in a software system and an exploit is an attack that leverages the vulnerability to achieve a certain outcome. Depending on the type of exploit, they can range from a line of code to a complex script and there are many types of vulnerabilities and exploits that can result in various outcomes; like crashing a server, to running code on a server to gaining full control.

Exploits depend on vulnerabilities that researchers discover and produce working exploits for¹⁸. Depending on the researcher, they may decide to responsibly disclose a vulnerability to a vendor or keep it a secret and sell the exploit for it. Alternatively, when a vendor resolves vulnerabilities in their products, a researcher may create an exploit after the vulnerability is publicly disclosed.

The sales of the exploits are generally not done directly by the researchers themselves but are carried out by suppliers that facilitate the brokering of exploits for customers. Vulnerabilities that are not known to the public yet are called zero-days and these are the most valuable. Customers for zero-day exploits can vary from white-hat security related organizations to cybercrime gangs and nation-state hacker groups.



Malware sphere

The malware sphere is all about creating, buying or selling malware and infecting computers with it. Cybercrime groups design develop and release malware themselves, sometimes with the perk of after sales support and evolutionary maintenance to meet changing customer needs. This is called a Malware-as-a-Service business, a criminal offshoot of Software-as-a-Service (SaaS), that helps to lower the bar for less-technical criminals who wish to get into running their own malware campaigns.

Malware oriented cybercrime groups include malware authors who develop the malware and must ensure that it is not detected by anti-malware software and has a good performance rate. These groups may run malware campaigns themselves or sell access to the use of their malware for other groups to use.

Malware campaigns are a set of activities carried out using various techniques with the purpose of infecting computers with malware. They require more than just purchasing or developing malware and can include factors like distribution; setting up infrastructure like command and control servers; identifying infection points; and money laundering. These different parts of a campaign may or may not be outsourced to other groups on the dark web. Malware distribution is popularly outsourced¹⁵. An example would be Pay Per Install (PPI) services, spamming, phishing, drive-by downloads, and malvertising.



Infrastructure sphere

When criminals want to host a malicious website or content for phishing, scams or carding sites or rent a server for command and control for example, they may prefer a hosting service that ignores complaints made by visitors and other hosting providers¹⁸. The types of malicious sites can include fake shopping sites, torrent and streaming sites, brute force tools and ad sites or porn.

This brings us to infrastructure. Bulletproof hosting is a profitable cybercrime business area that is often overlooked¹⁹. There are generally three types of hosting customers can buy. The first is a dedicated server, where the provider knows and is okay with hosting malicious content. The second, dedicated servers that have been compromised, are rented out, without the knowledge of the legitimate owner. The third are legitimate cloud servers being rented for malicious use. For example, an article by SpamHaus²⁰ noted that there is a recent operation renting legitimate virtual private servers (VPS) using fake identities.



Spam and phishing sphere

The spam and phishing spheres involve the creation, selling and sending of malicious e-mails with the purpose of advertising, stealing sensitive information or spreading malware. Spam e-mail campaigns can be purchased by customers who pay per e-mail sent from cybercrime groups who specialise in spamming. Once purchased, the e-mails are generally sent out from a botnet rented or run by a spammer. Emotet is a good example of malware that is primarily spread via malicious e-mails.

Spam campaigns are not always used to spread malware but are commonly also purchased to advertise websites and products. For the spam campaigners, if an e-mail recipient ends up making a purchase from their customer's website, the spammer could get a percentage of the sale. Affiliate marketing spam commonly takes place on social media platforms.

Cybercrime groups who specialise in phishing can offer a Phishing-as-a-Service rental that offers an easier way to conduct phishing attacks with monthly subscription levels. Newcomers to phishing can purchase pre-made e-mail templates, infrastructure and how-to guides on dark web forums and markets and this helps to lower the bar for entry into this type of cybercrime²¹. Similarly, phishing kits are tools that contain everything an attacker needs to launch an attack and commonly contain spoofed login webpages, phishing templates and more.



Stolen information sphere

The stolen information sphere is all about the stealing and selling of stolen information. This information can be sourced from many of the other spheres like phishing, malware and hacking. Examples of what can be sold are sensitive information like credentials for VPN, ecommerce sites, social media, Windows domain and banking or payment card information. Depending on the type of information, it can be monetised in different ways. Login credentials can be sold individually, but are usually sold in bulk and can include hashed passwords or passwords in plain text²². For banking details and payment card information, these can also be sold in bulk on carding forums, or bank accounts can be cashed out using numerous methods.

Other popular information sold ranges from a single social security number, or ID number, to a full medical record. Identity thieves, especially, like buying medical records as they usually contain a date of birth, place of birth, credit card details, social security numbers, addresses, and e-mails and even better if they include health insurance details.



Hacker sphere

The hacker sphere of the cybercrime world includes the products or services sold by hackers on the dark web. Hackers for hire advertise numerous services like stealing sensitive information, performing mobile device hacking, social media hacking, hacking courses, changing school grades, removing content from the internet, distributed denial-of-service attacks, or be hired full time, and the list goes on.

Hackers have increasingly been seen advertising access to corporate networks²³ in the form of credentials for VPNs, which may be useful to ransomware groups who want an easy way into a corporate network. In September this year, network access to organizations was seen being sold for \$500,000 on some hacker forums²⁴. The market for this type of access is now considered the 'initial access' market with VPN credentials, RDP access or access via botnets being sold.



Botnet sphere

The botnet sphere in our case is involved with the creation and monetisation of botnets - a network of infected computers/smartphones/IoT devices that can receive and run commands from their botnet operator. Creating a botnet requires developing or buying the botnet malware and finding or buying a service to distribute that malware. Botnet operators are said to be malware authors' best customers²⁵.

Botnets can be monetised in several ways. First, is to sell the botnet at a profit, and second is to rent it out for numerous services. Rental services can include spam and phishing, stealing sensitive information, proxy servers, installing other types of malware and finally, conducting DDoS attacks.

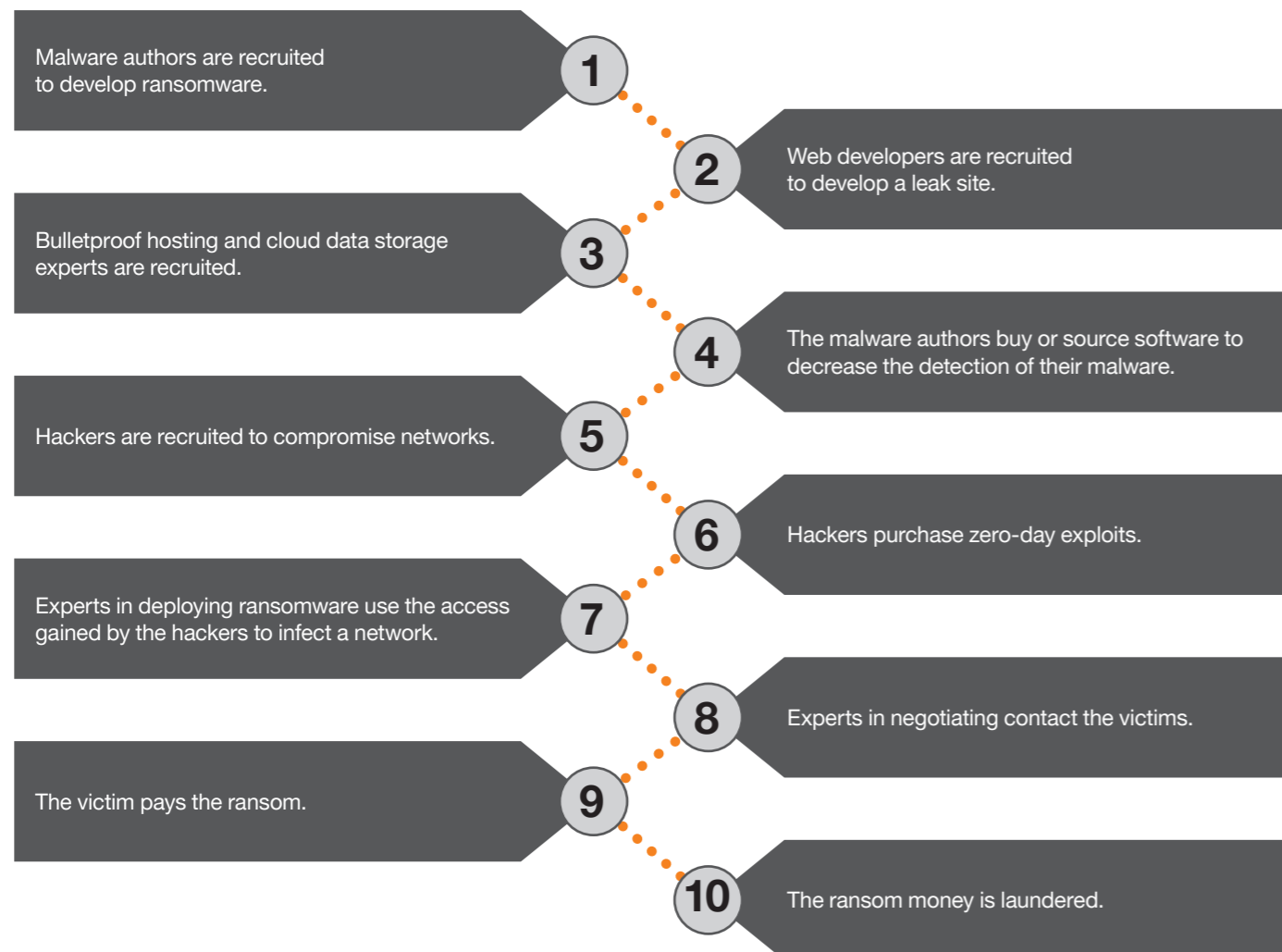


Money laundering

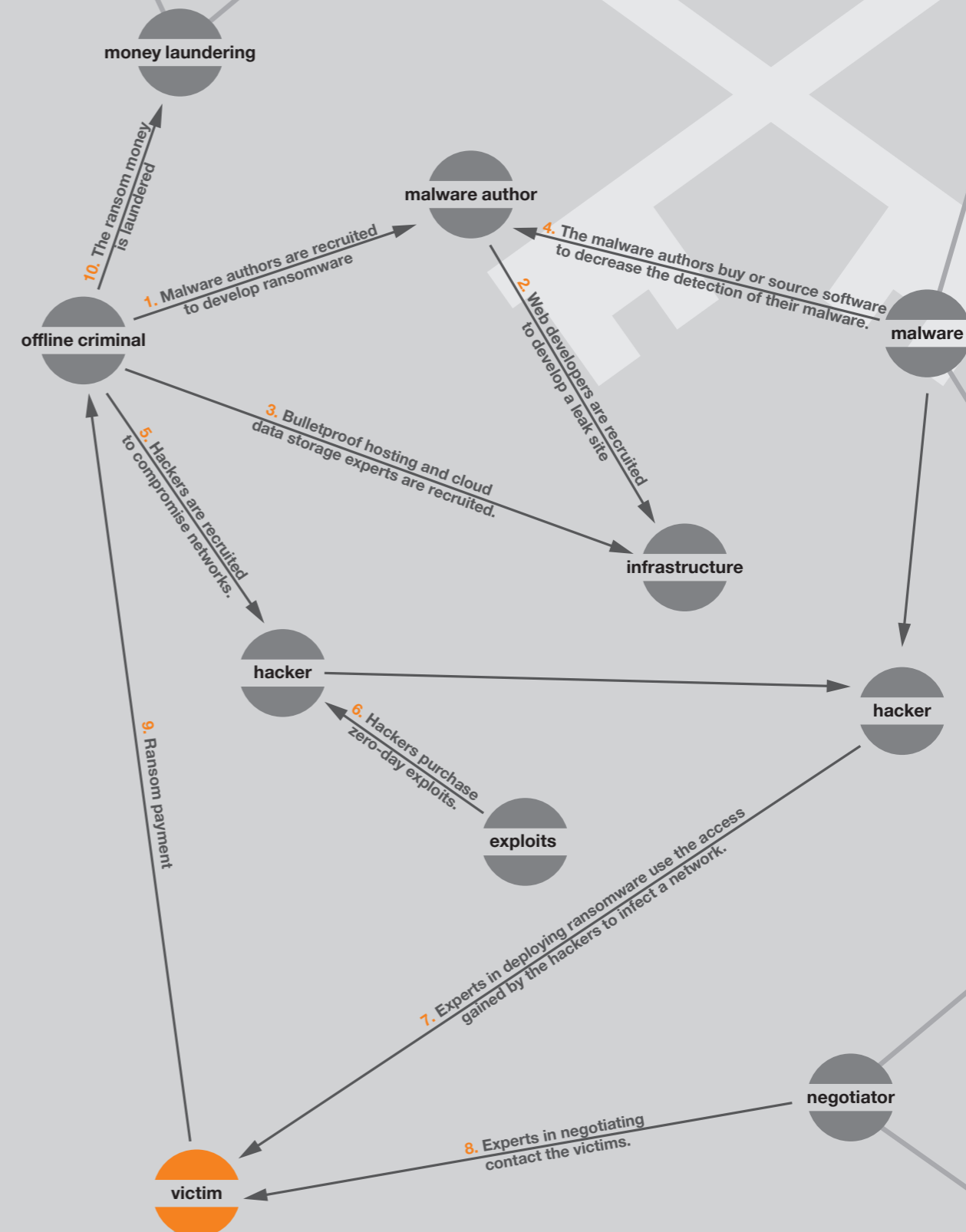
Once malware, extortion, or scams have generated money, or are looking to generate money, laundering it is an essential step in staying ahead of law enforcement. Traditional money laundering is done through a legitimate business where cash routinely flows. When the business owners deposit cash they have earned at a bank, they can also include a portion of 'dirty' money, and once the money is in their account, it looks like it is from a legitimate source.

Cybercrime groups can specialise in money laundering, like the qqaazz group who recently had several members charged with providing money laundering services to popular malware groups like Dridex, Trickbot and GozNym²⁶. Their operations consisted partly of shell companies, and money mules who helped to create bank accounts using fake identifications to receive the money and physically draw it from the bank accounts.

Example: A ransomware story



Criminal networks: A ransomware story



Conclusion

Cybercrime is more about 'crime' than it is about 'cyber'. Over the last several years we have seen interesting, yet inconsequential shifts in the tools, technologies and techniques used by criminals to conduct attacks in cyberspace. At the same time, we have seen significant shifts in the cybercrime business ecosystem which have impacted the way criminals make their money and in turn shaped the threat landscape for us in very significant ways.

A contemporary example of this kind of business shift is the recent move by ransomware actors to so-called 'double extortion' – the practice of stealing (via encryption) a victim's data in order to sell it back to them for a ransom, and threatening to leak sensitive parts of the data if they refuse to pay. This new business practice has led to the emergence of tactics referred to as 'big game hunting' - sophisticated, long-haul attacks against major companies with the goal of extracting ransoms to the tune of millions of dollars. Those millions are not once-off jackpots pocketed and splurged. Instead they are invested into a cycle of improvement and innovation that drives further, more efficient, forms of crime.

Ransomware, like most crime, is a business. Like any business, crime operates in a system. The cybercrime business ecosystem consists of diverse players, each performing a specialized role in the execution of the crime or the extraction or distribution of illicit gains. Some of the role players in this system act right at the cutting edge, recklessly crossing the boundaries of legality and putting their persons (more or less) directly at risk. Others operate in the background, perhaps even unknowingly, providing the technology, services and support the ecosystem requires to perform a crime, escape undetected or move and clean money so that the criminal proceeds can actually be used.

Pharmaspam, ransomware, DDoS extortion, carding and other forms of cybercrime are a business, not a technology challenge.

Of course a significant component of combating cybercrime is to understand and mitigate the human, organization and technology vulnerabilities criminals use to exploit their victims. But another, equally important component is to distill the business model behind a particular form of cybercrime, comprehend the various components that make it work, understand how those components interact, and seek to disrupt the business at its core.

In this section we introduced an initiative we have launched to map out the core components of the cybercrime ecosystem, in order to understand the relationships and flow of value between its various role-players. The core of this initiative is a fully interactive cybercrime network site will be online and available to our customers shortly. Our belief is that by understanding the networked nature of the cybercrime ecosystem we can begin to understand how it functions at its core, and how it can be targeted at the core to disrupt its fundamental operation, rather than just responding to its ever evolving technical tricks.

Our industry has proven in the past that we can succeed in combating cybercrime at its core. This approach needs to become the norm rather than the exception, however, and our belief is that understanding the cybercrime ecosystem network is the critical first step in this approach.



Blackbaud suffers from ransomware attack which lashed out to global data breach incidents

The service provider Blackbaud has suffered a ransomware attack in May, which led to several waves of leaked data of their customers (approx. 6 million individuals are affected) between May and August, and legal consequences for Blackbaud themselves in September. Blackbaud provides customer relationship management systems for not-for-profit organizations, healthcare entities and the higher education sector. A lot of healthcare providers suffered from ransomware attacks as a consequence. ^[25]

Fancy Bear and its backdoors

In August, the NSA and FBI released a paper describing a new malware developed by the Russian hacking group Fancy Bear (APT28) that targets Linux systems. The malware, named Drovorub, creates a backdoor on the victim's system which enables file transfer and execution of arbitrary commands as root. Drovorub uses advanced evasion techniques since it hides artifacts from common tools used for live response. ^[24]

A zero-day vulnerability

The first zero-day, CVE-2020-1380, is a remote code execution vulnerability which is actively being used in attacks. The vulnerability can exploit a weakness found in the scripting engine in Internet Explorer. Microsoft Office applications also use the same scripting engine as Internet Explorer, which means an attacker can use Office documents as well to exploit the vulnerability. ^[23]

AUG



Robinson Delaugerre
 CSIRT Investigations Manager
 Orange Cyberdefense

Pentesting & CSIRT stories

CSIRT to the rescue!

On patrol with the cyber-lifeguard

While the path of the attacker is rarely straight, it is in effect quite straight forward. You scan for a possible vulnerability, usually one you know an exploit for. If that road is blocked you check for another one. Repeat this procedure until you either get bored, run out of time or achieve success. Greetings to our marvellous pentesting teams at this point (please put down your pitch-forks, you really are doing an amazing job, as we will also see in this chapter).

The defenders life on the other hand is very complex. Torn between countless vulnerabilities, patches and attack vectors, between evaluating the latest technologies and educating the reactionary user: it is tough to stay on top of security. Generally everyone is doing a great job at it. But there is no such thing as absolute security. At some point, even the best-prepared prevention can fail. Be it by an unexpected zero-day, sheer luck, an unpatchable hardware-flaw or that one VPN box you forgot you had and didn't patch: attackers do find ways in.

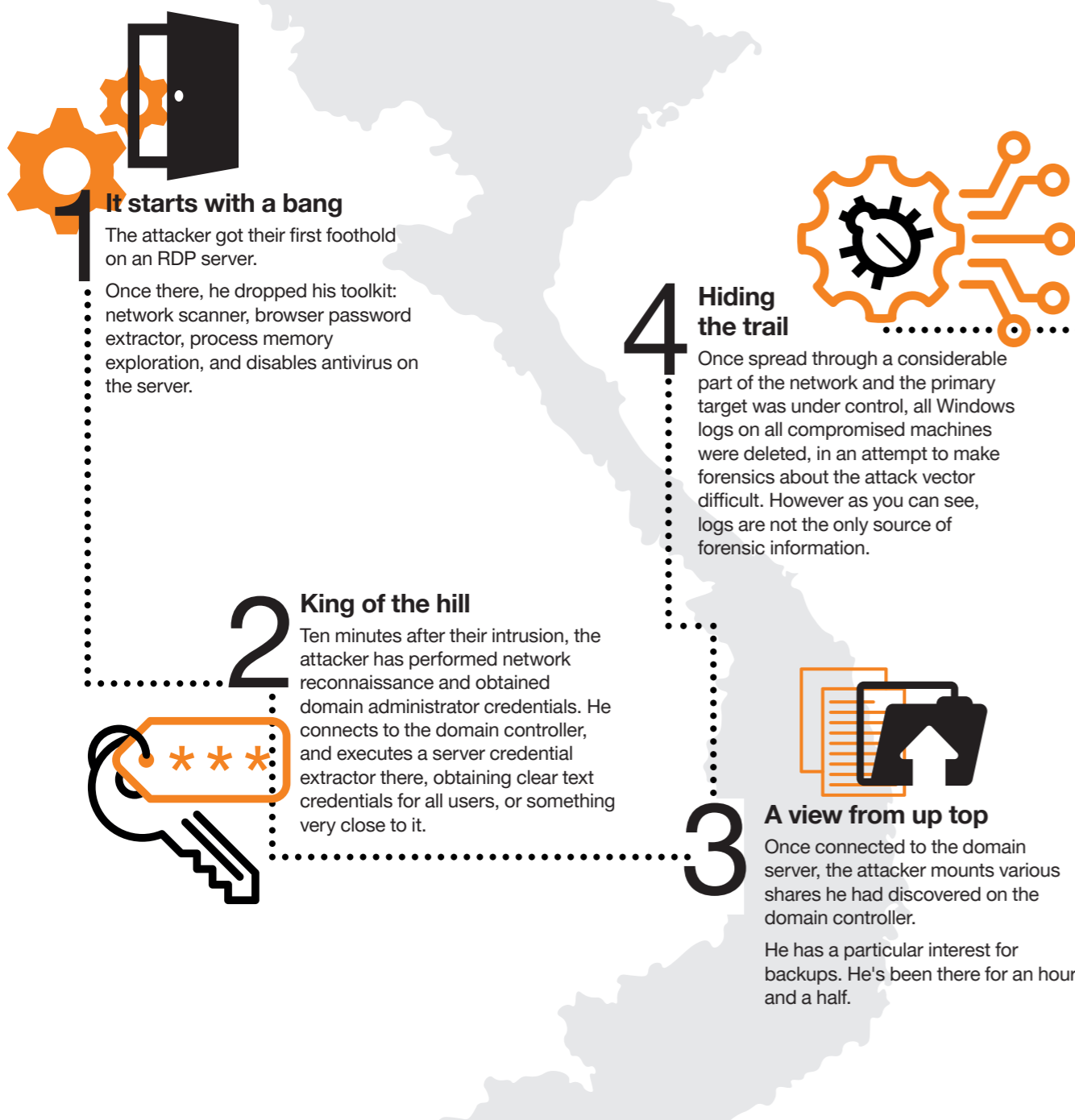
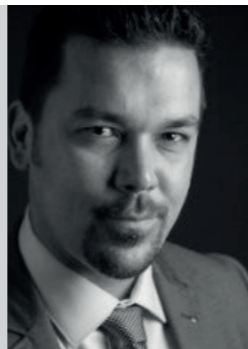
And if trouble strikes, who do you call? Exactly.

So follow us to the magnificent but often treacherous shore of the cybernetic ocean and see, how our CSIRT lifeguards saved the day.

CSIRT story 1: I love the smell of ransomware in the morning!

A client reached out to Orange Cyberdefense as one of its subsidiaries in Vietnam was suffering a ransomware attack. In collaboration with Orange Business Services providing an engineer on-site, it was possible for the CSIRT experts to get to work only few hours after the incident had been discovered.

Robinson Delaugerre, CSIRT Investigations Manager, **Orange Cyberdefense**



1 It starts with a bang

The attacker got their first foothold on an RDP server.

Once there, he dropped his toolkit: network scanner, browser password extractor, process memory exploration, and disables antivirus on the server.

2 King of the hill

Ten minutes after their intrusion, the attacker has performed network reconnaissance and obtained domain administrator credentials. He connects to the domain controller, and executes a server credential extractor there, obtaining clear text credentials for all users, or something very close to it.

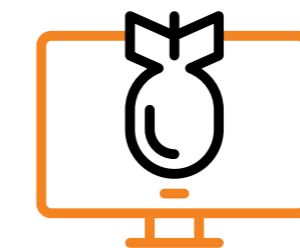
4 Hiding the trail

Once spread through a considerable part of the network and the primary target was under control, all Windows logs on all compromised machines were deleted, in an attempt to make forensics about the attack vector difficult. However as you can see, logs are not the only source of forensic information.

3 A view from up top

Once connected to the domain server, the attacker mounts various shares he had discovered on the domain controller.

He has a particular interest for backups. He's been there for an hour and a half.



5 Running ransomware

Four hours after their first login on the RDP server, the attacker deploys a variant of Phobos on all machines.



6 Restoring clean backups

Figuring out the attack history, the ransomware used and its operation mode, it was possible to restore cleaned backups of the infected systems and bring them back online. For criminal prosecution and preventing further attacks a full and detailed report was provided to the client.

Lessons learned

What lurks in the dark

We started this story with the attacker appearing on an RDP server without telling you how. With logs deleted, we'll never know for sure how the attacker got hold of the account. However, the fact that in the two hours after the deletion, more than eight thousand login attempts were logged from all over the world, brute-force seems like a pretty solid guess.

- Just like the metaphoric chain, an unsegmented network is only as strong as its weakest endpoint. Endpoint defense and endpoint detection is key in identifying attacks in an early stage and minimize the damage.
- Network segmentation can help to effectively contain an attack by restricting it to a separated part of the network. Important devices like RDP servers should be additionally protected within their segment.
- Brute-force attacks are relatively easy to detect and mitigate. Several thousand login attempts had probably failed before one was successful. Long before this, detection could have triggered an alarm and automatic countermeasures, had any protection measures or a SOC been in place, either on-premises or as a remote service.
- Lastly, hiding attack procedures and activity by deleting logs is ineffective if the logs are collected in a SIEM for analysis. Security logs are not only effectively backed up, but also enable detailed forensics to identify attack vectors and preventively remove the used vulnerabilities to avoid future attacks.

SEP

Zerologon exploited by ransomware groups

The vulnerability exploits a weakness in Netlogon's authentication process. This allows a remote attacker to create an authentication token so Netlogon sets the password for the domain controller to a known value. This can allow the attacker to take over the domain controller, escalate privileges or move laterally. Zerologon will later be widely exploited for example by the Ryuk ransomware operators. ^[26]

Pentesting story 1: Hi I'm AD\steve-admin, please let me access VLAN2

As a pentester you see a lot of different environments, some might call them little snowflakes. From a bird's-eye view they all look similar, but deep down they are all unique in their own little way. But sometimes you stumble upon a snowflake that is quite peculiar and that makes you want to poke at it with a stick to see what happens. This is a story of such a snowflake.

Justin Perdok, Security Specialist Operations, Orange Cyberdefense



1 Wait, what just happened?

During an internal assessment, we occasionally spin up services such as file servers to move stuff around in the network. After spinning up one of these services we noticed someone was trying to authenticate to us. It turned out that it was an account with Domain Admin privileges and kept authenticating on a regular basis. This allowed us to capture the passwordhash and crack the password or potentially relay these credentials and compromise systems in the network. But instead of just taking this as face value we wanted to know what was connecting to us and why.



3 "What if" questions

Seeing that this network trusted the output of a workstation to apply firewall rules, what if we told this system that we were an admin user? Could we manipulate the firewall to gain access to other systems in other networks? Would this allow us to compromise more business-critical systems that we currently did not have access to? Is there currently any public tool that allows us to do this?

Spoiler, the answers to these questions are yes, yes, yes and kinda.

2 Who was it?

After inspecting the network traffic, made by our mysterious authenticator, it looked like it was trying to gather information about the current logged on users. As it turned out, this network had a system in place that allowed the firewall to identify the current logged on user on a workstation. This information was then used to apply fine-grained firewall rules to the IP of the workstation.



The Healthcare sector is suffering ransomware attacks

Especially in the U.S. but also elsewhere, hospitals and healthcare providers are being targeted with ransomware attacks. One of many examples is the attack on the Universal Health Services (UHS) that operators over 400 healthcare facilities in the U.S. and UK. In this particular case, Ryuk ransomware has been predominantly present. [27]



5 Gathering information

Since we had previously analyzed information from sources in the internal network. We were currently operating from a network segment which we, for now, will call VLAN1. We found a system in another segmented VLAN, which will be called VLAN2. We currently could not access this system in VLAN2 presumably due to firewall rules. We also noticed that a user, let's say 'steve-admin', was able to access this system. Making 'steve-admin' an ideal target to impersonate as a logged-on user.



6 Impersonating an admin user

We fired up our tooling, supplied 'steve-admin' as our input and waited for the system to query our logged-on users while still pondering if this was going to work at all. After the system queried us, it saw that 'steve-admin' was the current logged-on user and therefore gave us his associated firewall rules. This in turn gave access to the system in VLAN2 from a network point of view. Using previously gathered credentials we were able to logon and compromise our target system.

4 Building a tool

In order to test this, we needed some tool that replicated the regular functionality. After digging into the protocol itself and other tooling, we concluded that there was no tool that fully allowed us to do this, but there were some building blocks. After extending an existing tool with these building blocks we were able to respond to these requests with arbitrary information that we fully control. Allowing us to spoof any user as if they were logged on onto our system and potentially gain their associated firewall rules.

Lessons learned

- Read and apply vendor best practices: the specific implementation of this functionality we exploited is marked as insecure by the vendor, but still supported and configurable.
- Apply Principle of Least Privilege in your Active Directory environments: service accounts should not be given the keys to the kingdom. Ensure that these accounts are only allowed to access what is truly needed for their role. For this use case, the vendor explained this in a best practice guide.
- Know what you are implementing: just because a software vendor supports some functionality, it doesn't automatically mean its secure. It can never hurt to investigate what it is doing. Ask the 'what if' questions.



Pentesting story 2: Red[team] alert

This story summarizes a Red Team operation we performed for one of our customers in 2020. The goal was to simulate an external threat in order to access a specific internal application, without being detected nor blocked by their internal security team. To do so, multiple intrusion vectors could be used.

Elias Issa, Head of Red Team France, **Orange Cyberdefense**



1 Phone probing

After finding the press office phone number (often exposed), the team called numbers following the same format, during non-working hours, looking for voice-mail boxes such as "you have reached the voice-mail of <name/surname>, please leave a message".



2 Analysis

Once a few names were gathered, an investigation was performed on each identified person, in order to define the most adapted scenario.



4 Deploying the backdoor

Once in, with a badge, an exploration of the premises has led to a room that seems perfect for hiding a physical implant.

Once the implant has been connected to the network behind a printer, a Wi-Fi access was provided to the team waiting in a car outside, allowing them to access the internal network.



3 Social Engineering

A calling platform was used in order to spoof the source telephone number. The reception desk was called by spoofing the employee's phone number, telling them that two "consultants" will be arriving in the morning and claiming that he/she will not be able to pick them up because of some problem: "Could you please make them two badges? They have been here before, they know the place".



5 Exploit the realm

A few low hanging fruits later, a valid user account allowed exploiting a misconfiguration on the domain controller in order to retrieve local admins accounts clear text password. A few jumps later, the domain admin account was compromised.



6 Access the data

The main goal was to have an authenticated access to a thick client used by some employees.

After identifying people who have access to the application, in-depth searches were carried out on their computers. This allowed direct access to the thick client while the employee was having lunch.



7 Full compromise

Once more the trophy was taken and the security had successfully been breached by the red team.

Lessons learned

Many lessons could be learned from this story:

- Train employees against Social Engineering
- Have a robust and strict procedure before allowing any person to enter the premises
- Enforce Network Access Controls (NAC)
- Perform network segmentation and filtering
- Harden the configuration of servers, workstations and Active Directory
- Never, ever store clear text passwords!





Carl Morris
Lead Security Researcher
Orange Cyberdefense

Tech insight:

Video killed the conferencing star

Videoconferencing is nothing new, but during the lockdown phase usage of the technology has seen a massive boost.

This has not only placed communication networks around the globe to an unprecedented level of stress, but it has also challenged the solutions themselves which had to cope with an exploding number of users and – following naturally – new requirements.

For many businesses, the COVID-19 epidemic has made teleworking the only feasible alternative to having their workers on site. The video call has become essential to collaborating effectively while working from home. Teams, Webex, Zoom and other collaborative platforms have become a part of our daily lives.

Videoconferencing has become the substitute for group meetings, conferences, webinars, training or even a simple conversation with colleagues. Thanks in large to these technologies, there has never been a “better” time in history to be working from home. But utilizing this incredibly useful technology is not without risks.

Videoconferencing: thinking about security

The choice of a videoconferencing solution is always a compromise between features, security and privacy. User requirements need to be weighed up against security requirements like

- encryption
- access control
- compliance
- exploit mitigation

An effective solution is a delicate balance. Using an extremely secure solution is not helpful if it doesn't fulfill the remote employee's basic communications needs. Similarly, it is not wise to select a very functional solution which does not provide an appropriate level of security. There is no single answer to the question of whether any communications platform is secure enough – it depends on who's using it and what for.

To objectively help you decide which solution suits you best, we start by presenting a 'target security model' that we believe should summarize the security needs of the 'average' corporate user. With the model in mind, we then set out to install, configure and test each of the systems we report on here. Where this was not possible, we sought to leverage insights from colleagues who were already using the platforms or (in the worst case) depended on information published by the vendor or other third-party sources. We endeavour to be clear about where our insights were gleaned in each case.

A target security model

We developed the security requirements model shown below to structure our analysis of the security attributes of the various offerings in this space:

Authentication

A robust business system must provide the ability to identify and confirm legitimate users of the platform and prevent others from entering uninvited. For businesses, this would generally also imply integration with their existing user directory, and preferably support for Single Sign-on (SSO). In the modern security climate, we would also have a strong preference for systems that support Multi-Factor Authentication (MFA).

Encryption

The confidentiality of the voice, video and text data as it traverses the local network, internet and (potentially) the providers' servers are also key. There are two models to consider here and they address different threats.

Data in transit: voice, video and text should be confidential as they traverse the LAN and public networks between the various servers and endpoints in the system. The assumption is that robust and verified encryption standards will be adopted and properly implemented, and that keys are properly managed.

End to End Encryption: The gold standard is 'End to End' encryption (E2EE), where the traffic is encrypted as it leaves the one user endpoint and only decrypted again as it arrives at the other. Crucially, "E2EE" implies that the provider cannot decrypt data that traverses their systems, even with the customer's consent or under government coercion.

Regulations and Jurisdiction

The geopolitical location and legal jurisdiction of the provider play an important role in determining the risk.

The provider of a conferencing service will be a legal entity that falls under the jurisdiction (and thus regulation) of a legal sovereign state. Not only might that impact the kinds of security standards the vendor implements, but it also has significant implications for the security of data that might be stored or processed by the vendor, in the face of possible government efforts to access that data.

Security Features and Management

Complexity is the enemy of security and so we would expect a critical system to provide administrators with clear and comprehensive tools through which the security features can be understood, implemented and monitored.

Vulnerability and Exploit History

The security features and controls that a platform lays claim to are only useful if those controls can't be subverted by hackers exploiting vulnerabilities in the technology. We therefore need to consider the track record of the vendor with regards to technical security, its level of transparency and ability to respond quickly and effectively when security bugs are reported.

Zoom

Zoom Video Communications is a company based in San Jose, California. The business has been enjoying great success since its launch in 2011, but sales have apparently rocketed with the COVID-19 epidemic.

Zoom relies on its SaaS model exclusively. It is used as a collaborative chat, audio and video solution, which allows working internally with colleagues as well as externally.

Since the beginning of the COVID-19 pandemic and the implementation of self-isolation measures around the globe, the use of Zoom has grown exponentially (+535% in the United

States alone). Several vulnerabilities and breaches, under the spotlights, have undermined trust in the company. While some concerns are justified, we feel that there has also been a fair amount of hyperbole involved, which was part of our motivation for writing this report.

Zoom 5.0 was released on April 27, 2020 and supports AES 256-bit GCM encryption. This has been enforced across the board starting May 30th, 2020 meaning only Zoom clients on version 5.0 or later will then be able to join meetings.

In-meeting security controls are now grouped under the security icon on the host meeting menu bar. These controls allow the host to enable or disable the ability for participants to: Screen share, Chat or Rename themselves. Hosts can also "Report a User" to Zoom's Trust & Safety team, enable the Waiting Room feature while already in a meeting, lock the meeting once all attendees have joined to prevent unwanted guests and remove any participants which will then prevent that individual from rejoining the meeting.

Microsoft Teams

Microsoft Teams is a proprietary collaborative communication application, operating only in SaaS mode, officially launched by Microsoft in November 2016. The service can be integrated with Microsoft Office 365 suite and Skype for Business. It is also expected to replace Skype, which will be abandoned in July 2021. The solution allows collaborative work (co-publishing and storage of documents, access to e-mails and an instant messaging system, etc.), thus offering far beyond the traditional features of videoconferencing systems. Teams also offers extensions that can be integrated into products other than Microsoft.

Microsoft Teams has been available in a free version, limited to 300 members, since July 13, 2018, although some features of Office 365 are missing. The solution now claims more than 44 million active users with an exponential acceleration since the beginning of the massive pandemic-driven teleworking migration in many countries.

The solution is available on most Microsoft Windows, MacOS, Android, iOS and GNU/Linux distributions. The product is completely usable via a browser, with no need to install a client. However, the optional rich client or a fully supported browser (like Microsoft Edge based on Chromium or Chrome itself) is required to access advanced features like content sharing, control of shared content, and background²⁷.

A free version exists for SMEs (up to 300 users) although it offers very limited functionality. We feel that the solution might be a bit heavy for very basic or occasional needs.

On April 28, 2020 researchers at Cyb0rArk created a proof-of-concept (PoC) attack that involves an inside attacker getting a victim to view a malicious GIF that allows an attacker to take

over the victim's Teams account. They reported two insecure subdomains to Microsoft, which resolved the issue in under a month. Using the bug, an attacker could gain access to an organizations' Teams accounts by making Teams API calls, which allows one to read and send messages, create groups and add and remove users.

Generally, although there is little data with which to assess this product's security heritage, it would be fair to argue that Microsoft has robust processes and has developed a strong reputation in this regard.

Cisco Webex Meetings

Cisco Webex is an American company which develops and sells web conferencing and videoconferencing applications. The Webex solution is available under several licenses including a free version (limited to 100 participants) and is available as SaaS (public cloud), on a private cloud or on-premise on a dedicated server or integrated into a Cisco telephone system.

According to Gartner, Webex is the current market leader and is considered a visionary player in video communication technologies (along with Zoom and Microsoft).

The solution is available in two forms, Webex Teams for collaborative work (addressed later) and Webex Meetings for audio and video meetings (covered here). Webex also offers a wide range of peripheral such as whiteboards, IP phones, screens and cameras for videoconferencing²⁸.

The Webex Meetings solution is used via a web browser with a plugin. It is also possible to install and use software available for Windows, Android and iOS, for access to organized meetings. Installation of the client requires administrator rights on the computer. Webex Meetings allows users to generate a unique password for every meeting. Administrators define the complexity of the password in order to comply with organizational password policies.

Webex supports role-based access, which defines the privileges of meeting attendees. This configuration also allows hosts to restrict application or desktop sharing as necessary.

Cisco Webex Teams

Cisco Webex is an American company which develops and sells web conferencing and videoconferencing applications. The Webex solution is available under several licenses including a free version (limited to 100 participants) and is available as SaaS (public cloud), on a private cloud or on-premise on a dedicated server or integrated into a Cisco telephone system.

The solution is available in two forms, Webex Teams for collaborative work (addressed here) and Webex Meetings for audio and video meetings (covered previously).

Webex Teams is an application that allows you to work in a continuous team using video meetings, group messaging, files and whiteboards sharing. Full use of the Webex Teams solution leverages a client-side application, available for Windows, iOS, Android and MacOS, but use via a browser is also possible.

Like Webex Meetings, it is possible to interconnect the solution with many services (Google Calendar, Zendesk, Trello, Twitter, etc.). Combined with the other related products and services provided by Cisco, including switches, phones and cameras, we consider this to be one of the most complete solutions currently available. As a cloud-based service, Webex enjoys the security of Cisco Datacenters which host the service.

Webex supports role-based access, which limits the privileges of meeting attendees. This configuration also allows hosts to restrict application or desktop sharing if necessary.

Cisco additionally offers the possibility of federating Webex instances, thereby eliminating the risk of confidentiality and data leaks associated with guest accounts. During internal and external collaboration, customers can therefore control the flow of sensitive content and shared confidential data can be removed.

Like other vendors, Cisco allows the administrator to manage the password criteria as required.

Cisco offers Webex Control Hub as a “web-based, intuitive, single-pane-of-glass management portal that enables you to provision, administer, and manage Cisco Webex services and Webex Hybrid Services, such as Hybrid Call Service, Hybrid Calendar Service, Hybrid Directory Service, and Video Mesh”.

Google Meet

Known as "Meet by Google Hangouts" until April 09, 2020, Google Meet is a videoconferencing platform for businesses developed by Google and established in March 2017.

The solution is integrated into the Google Suite ecosystem (Gmail, Docs, Drive, etc.).

The G Suite license requires a fee for the service used. The license level determines the maximum number of participants allowed in a video conference. However, as of April 29, 2020 Google has made Meet available for individuals, as long as they have Google accounts.

Meet allows one to organize meetings remotely (through audio and video calls), offers document sharing and an instant mailbox system. The service is accessible online through most internet browsers or via mobile applications available on Android or iOS. There is no difference between the functions offered by the client software and those offered in the web version.

The Meet application is available on most market-leading platforms: Windows, MacOS, Chrome, GNU / Linux as well as in application format on iOS and Android platforms. Meet also allows participants to join a scheduled video meeting by entering a single code. The service is only available in SaaS mode via the G Suite.

The tool is integrated into the Google Suite, making the use of other services easier. We found the product interface intuitive and easy to use, and it's possible to join meetings from any device and via mobile phones.

We found the interface with other products such as the Microsoft Office suite to be less than smooth, probably because this solution is primarily set up for Google tools users (Gmail, Chrome, Google Calendar, etc.). The system also appears to suffer from restrictions with browsers other than Google Chrome.

Google's identity and access management (IAM) service lets administrators manage all user credentials and cloud applications access in one place.

Audit logging for Meet is available within the Admin console for G Suite Enterprise, and Google offers Access Transparency²⁹, a feature which logs any Google admin access to Meet recordings stored in Drive. Access Transparency is also offered as part of G Suite Enterprise. This includes Data Loss Prevention (DLP) for Drive. Meet users can also enroll in Google's Advanced Protection Program (APP), which provides protection against phishing and account hijacking.

BlueJeans

BlueJeans provides an interoperable cloud-based video meetings service that connects many users across different devices, platforms and conference programs. Every BlueJeans member has a private “meeting room” in the BlueJeans cloud to schedule and host conference meetings. It operates with business conferencing solutions such as Cisco, Microsoft Lync, StarLeaf, Lifesize, and Polycom, as well as consumer services like Google.

Verizon communications announced on April 16th, 2020, that it had entered into an agreement to acquire BlueJeans to expand its Business portfolio offerings, particularly its unified communications offerings. The transaction is expected to close in the second quarter of 2020.

BlueJeans provides end users with interoperability to ensure frictionless videoconferencing, regardless of desktop operating system (e.g., Windows, MacOS, Linux), browser (e.g., Chrome, Firefox, Safari, Edge, Opera), mobile device (e.g., iOS, Android), or virtual desktop infrastructure (e.g., Citrix). Hardware interoperability is extensive and includes Cisco, Poly, Lifesize, Dolby and more, essentially if it is based on SIP or H.323 standards, it is interoperable with BlueJeans.

The software includes several stand-out features that will appeal to business owners and professionals. For example, meeting recordings can be broken down into chapters, with segment highlights, task assignment and smart follow-up.

On top of the fact that meetings have no time limit, hosts can create up to 20 breakout sessions and distribute participants as needed, which is great for collaborating on subtasks. You can easily share your screen, annotate with whiteboard functions, and even allow remote desktop access to an assignee. However, there is no option to blur out backgrounds for greater privacy and distraction-free meetings.

Administrators have advanced user management features and can utilize a centralized admin console to add and manage users, set access permissions and passwords as well as enable or disable features on a company-wide or group basis.

BlueJeans integrates with a number of other applications including Slack, Microsoft Teams, Microsoft Outlook, Google Calendar & Okta amongst others.

Tixeo

Based in Montpellier, France, Tixeo offers a set of secure teleconferencing solutions. The company has several references and has made security of communications a priority. Tixeo allows you to organize video conferences, share your screen and give remote control.

Tixeo's solution is commercial only and offers three operating modes:

- Shared cloud, via two offerings (standard and premium, allowing the interconnection of other traditional videoconferencing systems),
- Private cloud, operated by Tixeo,
- Server version – on-premise.

The company also offers a supply of equipment (cameras, screens, etc.) for videoconferencing.

The solution is available on the most user platforms (Android, iOS, Windows, MacOS and GNU/Linux). Users require a specific account and password which need to be provisioned beforehand. Tixeo requires the installation of a ‘thick’ client by the user, and the Tixeo server version requires the installation of a server-side application, along with the required server and network configuration. The solution does not allow for access to the conference via the telephone network.

Tixeo may not necessarily be suitable for small organizations or ad hoc needs due to its business model.

BigBlueButton

BigBlueButton is a videoconferencing solution originally developed for remote learning. It allows users to make calls, share screens, images and presentations, and provides collaborative tools such as a whiteboard, chat systems and the sharing of PDF or Microsoft documents. The platform is free of charge and published under a general limited license known as GNU.

Installation of the BigBlueButton server is only possible under the Ubuntu Linux distribution, although it can be run as a virtual machine under Windows. We found that the installation was not entirely easy as it required a dedicated server and the opening of numerous communication ports as well as the assignment of a domain name and the generation of an SSL certificate.

We found it to be a very complete solution, meeting diverse needs and use-cases. It allows for a high level of technical control and as an open-source platform is fully customizable.

Users should note, however, that the solution requires a dedicated server and that there are significant installation, security, maintenance and security management overheads.

Skype for Business

Skype for Business (previously Microsoft Lync and Office Communicator) is a proprietary instant messaging platform developed by Microsoft as part of the Microsoft Office suite. It includes audio, video, chat and file transfer functionality. Skype for Business is integrated into the Microsoft Office suite, notably with Exchange and SharePoint.

This solution initially required the installation of an on-premise Skype server, as well as the set-up of a client on the workstation, but is now integrated into the Office 2019 or 365 suite and is available in the cloud in SaaS mode via Teams. The solution is available on the most popular platforms (Android, iOS, Windows, MacOS) but not GNU / Linux.

Skype interfaces with Exchange to manage the calendar, meetings, presence indicators and document sharing.

The on-premise version requires the deployment of servers and several software components, including the .NET Framework, Microsoft Server, Microsoft SQL, etc. which are all required on each server. Along with complex network and firewall installations, deploying Skype onsite could be challenging for SME's.

In September 2017 Microsoft announced that this solution will be abandoned in favor of Microsoft Teams.

Jitsi Meet

Jitsi is a free, open-source, instant messaging, audio and video-conference application. The solution can be connected to other systems like Google Hangouts, thus allowing interactions with people on other messaging systems. It allows users to make calls on the Internet but also to landline- and mobile phones.

In our opinion, the solution offers more than satisfactory audio and video quality, with no latency observed. Jitsi Meet leverages WebRTC³⁰ and HTML5³¹, which work directly in conventional web browsers, so there is no need to install software even for iOS and Android.

Jitsi server is available as packages for Ubuntu and Debian Linux. It is also possible to install the server on Windows or MacOS devices as a virtual machine.

The solution is also highly interoperable with other messaging and communication systems.

On the downside, the solution requires a dedicated server or servers because the load rises very quickly with the number of users. Installation is within the user's own infrastructure, which means a complex configuration and continuous upkeep of the servers. Automatic installation exists under certain distributions, but not all, and we would caution that manual set up is not for everyone and might quickly become complex.

Comparison chart

- Full support
- Partial support
- No support
- Unclear

	Zoom	Teams	Webex Meetings	Webex Teams	Google Meet	BlueJeans	Tixeco	BigBlueButton	Skype f. Business	Jitsi Meet
Encryption										
Uses an appropriate encryption algorithm	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Uses a strong encryption key	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data is encrypted in transit under normal use	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data stays encrypted in transit on provider servers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Voice, video and text are all encrypted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File transfers & session recordings are encrypted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vendor technically can't decrypt the data at any point, even under regulatory pressure (full E2EE)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	N/A
Encryption implementation has withstood scrutiny over time	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Authentication										
Administrators can define password security policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Supports MFA as default	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Can integrate with Active Directory or similar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Can integrate with SSO solutions via SAML or similar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Offers Role Based Access Control (RBAC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Allows passwords to be set for meetings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Allows meeting password security policies to be set	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jurisdiction										
Headquarters address	USA	USA	USA	USA	USA	USA	FRA	N/A	USA	N/A
The vendor cannot technically access any data without the client's consent	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	N/A
A full on-prem version is available for users who don't want to trust the vendor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
For SaaS modes of deployment, the client can select which countries or political regions data is stored or processed in	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A	<input type="checkbox"/>	N/A
Complies with appropriate security certifications (e.g. ISO27002 or BSI C5)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Complies with appropriate privacy standards (e.g. GDPR)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Provides a transparency report that details information related to requests for data, records, or content.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A	<input type="checkbox"/>	<input type="checkbox"/>
Security Management										
Offers other forms of access control to meetings, e.g. waiting rooms, lockout, banning etc.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Allows granular control over in-meeting actions like screen sharing, file transfer, remote control.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Offers clear central control over all security settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitoring and maintenance of endpoint software versions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Provides compliance features like eDiscovery & Legal Hold	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auditing and reporting	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Additional content security controls like DLP, watermarking, etc.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vulnerability Management										
Percentage of NVD 2019	0.02	0.01	0.15	0.03	0.00	0.00	0.00	0.00	0.02	0.00
Percentage of NVD 2020	0.08	0.00	0.09	0.02	0.00	0.00	0.00	0.04	0.00	0.01
Vendor discloses which vulnerabilities have been addressed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Vendor runs a bug bounty	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Conclusion

Comparison is actually very hard. It depends on use cases and threat models.

When choosing a solution, organizations need to factor in both their intended use cases and their realistic threat model. Without these fundamental insights to hand, it is extremely difficult to compare the available solutions meaningfully. If certain features are required, such as meeting recordings for example, then this is likely to have a cost in terms of the security levels available. Similarly, if full end-to-end encryption is a necessity due to your threat model then this will most definitely impact on what features are available.

Other factors an enterprise may have to consider are granular Role-Based Access Control and integration with existing user directories and SSO solutions, logging and auditing and whether they can control the geographic regions of servers that their data routes through or is stored on. Most businesses also need the ability to collaborate with guest users from outside the organization and will need the ability to granularly control the use of certain features, such as file transfers, as part of their data leakage prevention strategy. The offerings of the more 'mature' players, like Cisco, Microsoft and Google are typically more advanced where features like these are concerned. Indeed we found them to be completely absent in several of the offerings we reviewed.

Even as we were putting together this review developments continue apace. A prime example of this is that despite us stating in the blog that Zoom would only offer E2EE for paid accounts, that policy was changed. Likely due to the significant public outcry when it was announced that users on the free tier would not get E2EE, Zoom announced³² that they would offer this to free users who verify their accounts by providing additional identification information such as their phone number. They stated that this verification step will ensure they can identify and prevent any abuse of the service. In a similar vein, BlueJeans have also announced³³ a number of new features and security controls, the most notable being the change from AES-128 based encryption to AES-256 instead. Other features, which should be available by the end of the summer, include virtual backgrounds, waiting room, meeting transcription, non-raise hand interactions, and enhanced integration with Slack.

Find the full in-detail analysis in our blog: orange cyberdefense.com/global/blog/video-killed-the-conferencing-star/



Stefan Lager
SVP Global Service Lines
Orange Cyberdefense

Security predictions

There is no bad weather...

...if you wear the right clothing, as the saying goes.

When predicting the future of the cybersecurity landscape you can draw parallels with the climate and weather. Climate is the long term trends that will affect us over time, and the weather is the current changes in risk that affects our business.

To be able to protect your organization you need to both protect against today's weather changes, but also plan for meeting the climate change that is going on in the cybersecurity landscape.

Since this is a big topic, I have decided to just cover four parts of it.

1



Part 1: Cybersecurity vs The Threat

Two factors that impact the risk of your company are the threat and the vulnerability. If there are no vulnerabilities, you don't need to care about the threat (=nirvana). If there are many critical vulnerabilities then even a small threat can cause a massive impact to your business. So let's look at these two components.

The Threat:

- Cyber offensive capabilities are being commoditized. This is blurring the lines between nation-state and cybercriminal actors. Advanced tools that previously were limited to a few established actors are now available broadly on the black market which is lowering the barrier of entry for cybercriminals.
- Companies are paying cybercriminals large amounts to retrieve encryption keys for locked data or to prevent data from being leaked publicly. This attracts more bad actors into the mix and funds more sophisticated attacks in the future.

Vulnerability:

- Few buyers use independent cybersecurity efficacy assessments as part of their procurement. So how do they make their decision? The bigger vendors in the cybersecurity industries can spend between 40% to 50% of their revenue on sales and marketing. That is a heavy investment in persuasion.
- Cybersecurity tooling is complex and there is a massive shortage of skills and resources to be able to deploy technology in accordance to best practices.
- Few organizations map and measure their detection abilities. A strategy for detection across the cyber-attack kill chain is a requirement and this strategy should also be verified, to see if the detection actually works.

To combat both short and long term threat evolution, investments should be mapped to the reduction in risk. To understand the reduction in risk you need to assess the efficacy of your protection solutions and not only buy what is easiest to procure. You also need to verify your detection abilities for all levels of the kill chain to make sure your detection abilities match your objectives.



2



Part 2: Cybersecurity vs Data security

Cybersecurity is evolving to be more centric around data. That is quite a natural evolution since the major costs for companies, are related to data security incidents.

Unavailability of data	Ransomware
Extortion to leak data	Extortionware
Stolen data	Intellectual Property theft
Data mismanagement	Compliance fines (e.g.: GDPR)
Fake data	Brand impact, social media attacks

We believe that organizations will need to invest more into the area of understanding their data and classifying it, to be able to apply an appropriate security strategy for its protection. This includes factors like encryption at rest, in transit and in use.

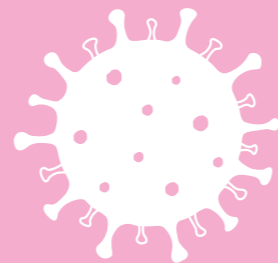
But we need to also allow access to the data in a controlled way. In the old world we would separate the good guys from the bad guys with one perimeter firewall and on the inside, there was very limited segmentation and security. In today's world, where both users and data are located anywhere, this model does no longer work. That's where the "Zero-Trust" concept comes into play. This concept includes three main components:

- **Verify:**
Identity (MFA), location, device security status...
- **Provide Least Privileged Access:**
Limit the access to the minimum and only during the time when it is required.
- **Assume breach:**
Create an infrastructure that is designed to limit the impact of a breach by segmenting access by network and users (e.g.: microsegmentation).

We predict that organization's investments in data-centric security will increase at the expense of infrastructure based security.



3



Part 3: Cybersecurity vs Post-COVID-19

COVID-19 has had a big impact on all our lives, but also on the cybersecurity industry as a whole. It has boosted many customers digital transformation journey.

When the majority of the workforce is working from home, this increases the requirements for new solutions for collaboration, access and security. We believe that while things post-COVID hopefully go back a bit more to normal, many companies have seen some of the benefits with remote working and will continue in a new hybrid mode. All employees that previously were communicating locally within the office network, protected by an enterprise grade firewall, will now connect their laptops to a cheap home ISP router and access the data over VPN connections.

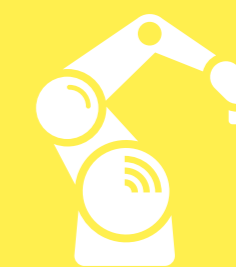
These home routers usually do not have the same cadence when it comes to software upgrades to address newly discovered vulnerabilities, and hence increase the risk of being compromised.

Once you control the router there are many ways of infecting all devices behind it, including your corporate laptops with “always-on” remote access. Orange Cyberdefense has done some interesting [research on this topic that is well worth a read](#).

To mitigate this increased risk of homeworkers we predict investments into solutions like:

- **Flexible remote access solutions.** Solutions that can scale up and down to meet current needs and that does not require a big initial investment.
- **Next generation endpoint security solutions.** Solutions that are equipped to protect against unknown advanced threats based on for example machine learning or advanced behavior analytics.
- **Endpoint Detection and Response solutions.** Since companies CyberSOCs have lost a great deal of the visibility due to all remote workers, companies need another solution that will enable visibility and detection across all endpoints, but also that fast and effective incident response work. However, there is a high likelihood that many of these solutions will fail due to one of two reasons:
 - The efficacy of the EDR technology is not good enough and analysts will suffer from alert fatigue. The challenge is not detection per se, but relevant detection
 - Companies do not have the competence nor resources to analyze the alerts that these tools generate, which will lead to increased investments in buying this as a service

We also believe that due to the uncertain times ahead, customers will prefer, to an even higher extent, OPEX based payment models vs upfront investments.



4

Part 4: Cybersecurity vs Safety

The biggest driver for investing in cybersecurity has always been financial. Customers have invested in cybersecurity to avoid ransomware, protect against IP theft, etc.

But as everything is getting connected, both directly, like for example IoT to 5G Networks, but also indirect, like factories and smart-buildings connected via internal IT networks, this introduces a whole new type of risks that does not only have financial impact, but also impacts the safety of people.

In combination with the commoditization of offensive cyber weapons also opens opportunities for new threat actors like terrorists and hacktivists that may have other goals than financial gain.

Criminals explicitly target safety locks

Triton is one example of this threat. Triton is a malware that was found back in 2017 and that was architected to disable safety systems. These protective systems were basically designed to prevent physical damage in OT/ICS environments in case of mechanical/software issues. The main objective of such a system is protecting people, environment and goods. The attack was aiming to take out these failsafes to cause physical damage and potentially harm employees. Hence this is also sometimes referred to as “the world’s most murderous malware.”

In the U.S, the Cybersecurity and Infrastructure Secure Agency (CISA) and the NSA have issued warnings that adversaries could be targeting critical infrastructure.

We predict that what is required is more cross-education of OT and IT people. Many of the security challenges in the OT environment have IT solutions that can be applied, but also due to the different protocols and also the strict priority of availability vs security, some solutions need to be adapted or uniquely designed for the OT environment.

One thing is clear though. The most common attack vector to the factories will be access via the existing IT infrastructure (e.g.: phishing e-mails, vulnerable exposed services, malicious USB-sticks...), and the Command&Control activities from OT environments also need to traverse the IT networks, in most cases.

Organizations will need to invest in solutions that can provide visibility and threat detection across both OT and IT and correlate this information, to be able to rapidly respond to the threats that could cause both a financial risk and a risk towards safety.

Death indirectly linked to a cyberattack

A ransomware attack on the Dusseldorf University Hospital lead to a death of a patient. As a consequence of the attack, the hospital in question was unable to take in new emergency patients, which meant that the woman in need of urgent care, had to be transferred to another hospital which was further away and thus lead to her death. Ironically, the hospital was not the target of the attack but the nearby university. ^[28]

Report summary:

What have we learned?



Etienne Greeff
CTO
Orange Cyberdefense

In my attempt of providing a tl;dr* I read and re-read the report a number of times.

It occurred to me how difficult the task is for defenders. There are so many data points and lessons that need to be learned and then applied to make sure that we don't become the next headline.

When trying to make sense of immense complexity it is often helpful to ask the question "Why does this matter?" We often take technology for granted whether that is remote access, cloud applications or communication technologies, including videoconferencing. At the risk of stating the obvious, it is important to realize that without dedicated defenders and our technology partners the safe use of these technologies would not have been possible.

During the current pandemic these technologies have moved from nice to have, or complementary, to absolute necessity. This is true whether we are using the technology to communicate with our grandparents, a community group or continuing our business activities, allowing our economy to function despite all the current challenges. From a defenders point of view Cybersecurity has never mattered more.

As my favourite super hero's uncle said "With great power comes great responsibility". If what we do matters greatly it is important to be able to prioritise our efforts on the areas where it has the biggest impact.

I am not going to presume to tell any individual or business what their most important priority is. My council is, however, to continuously prioritise and not to be swayed by technology vendors in applying technological band aids. Examine the threat landscape to understand what the contemporary dangers are, understand your own attack surface and vulnerabilities, understand what data and processes keeps your CEO awake at night and then apply this knowledge to prioritise your protection efforts.

* For non millennials: too long; didn't read

Above all assume that you will not get it right all the time and have the right contingency plans in place for when the worst happens.

One of the key findings in this report is that Cybercrime has become big business. The reason for this is a confluence of factors:

- Crypto currencies has made it easier to monetise Hacking and other illegal activities
- There is a lot of money to be made in specific parts of the cybercrime eco system and criminals can specialise in areas they are talented in
- Insurance companies are willing and able to make payment to threat actors creating a steady flow of money into the eco system
- The bulk of companies business is now conducted digitally even for very traditional physical activities like hairdressers
- The success of governments using cybersecurity for geopolitical aims

The reality is that when any business attracts a lot of money and success it soon follows that the business will attract a lot of very good talent. We have seen this trend within the cybercrime community. A good example of this the fact that we are seeing the use in the wild of previously undisclosed Apple vulnerabilities.

Given the fact that these vulnerabilities are worth more than \$1,000,000 dollars in the open market one has to wonder how much this was worth to the security researcher not to disclose the vulnerability and claim the bug bounty.

So how do we deal with this new world where hacking is big business and we are up against some pretty smart and well-motivated adversaries ?

As is pointed out in the report it is important to get the basics right. And as defenders we mostly do but unfortunately, the data tells us that this isn't enough. The most determined and motivated attacker will keep probing until they do discover a weakness. We have seen that commercial hackers can be as sophisticated and skilled as state sponsored adversaries.

There is one crucial difference however. A state adversary is often resource and time constrained while a commercial adversary is only constrained by economics. Economics which currently makes hacking very attractive and good business.

It is also important not just to rely on technology but also to rely on business processes. We believe that the traditional separate worlds of cybersecurity and fraud need to work together much closer as we realise that cybersecurity is not just a technical issue but a business issue. And on that note I wish you fair winds as you attempt to navigate this very complicated and treacherous seas we call cybersecurity.

» Examine the threat landscape to understand what the contemporary dangers are, understand your own attack surface and vulnerabilities, understand what data and processes keep your CEO awake at night and then apply this knowledge to prioritise your protection efforts. «

Etienne Greeff, CTO Orange Cyberdefense

Contributors, sources & links

Sources

This report could not have been created without the hard work of many researchers, journalists and organizations around the world. We've gratefully used their online publications for reference or context.

Sources/links

- [1] <https://www.ons.gov.uk/businessindustryandtrade/business/businessservices/bulletins/coronavirusandtheeconomicimpacts/8october2020>
- [2] https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_U00179811.PDF
- [3] <https://www.cisecurity.org/controls/cis-controls-list/>
- [4] <https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/>
- [5] <https://blog.checkpoint.com/2020/08/11/threat-actors-join-in-the-race-towards-a-coronavirus-vaccine/>
- [6] <https://blog.checkpoint.com/2020/08/11/threat-actors-join-in-the-race-towards-a-coronavirus-vaccine/>
- [7] <https://www.top10vpn.com/research/investigations/COVID-19-vpn-demand-statistics/>
- [8] https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_U00179811.PDF
- [9] <https://threat-advisories.secddata.com/threats/viewSignal/SIG-4618>
- [10] <https://threat-advisories.secddata.com/threats/viewSignal/SIG-4467>
- [11] http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
- [12] <https://www.hackread.com/8-best-dark-web-search-engines-for-2020/>
- [13] <https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019>
- [14] <https://www.fbi.gov/news/stories/alphabay-takedown>
- [15] https://software.imdea.org/~juanca/papers/ppi_usenixsec11.pdf
- [16] <https://www.tenable.com/blog/a-look-at-the-vulnerability-to-exploit-supply-chain>
- [17] <https://research.checkpoint.com/2018/malvertising-campaign-based-secrets-lies/>
- [18] <https://www.digitalshadows.com/blog-and-research/the-ecosystem-of-phishing/>
- [19] <https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/bulletproof-hosting-services-cybercriminal-hideouts-for-lease>
- [20] <https://www.spamhaus.org/news/article/792/bulletproof-hosting-theres-a-new-kid-in-town>
- [21] <https://www.digitalshadows.com/blog-and-research/the-ecosystem-of-phishing/>
- [22] <https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/>
- [23] <https://www.bleepingcomputer.com/news/security/network-intruders-selling-access-to-high-value-companies/>
- [24] <https://www.zdnet.com/article/network-access-sold-on-hacker-forums-estimated-at-500000-in-september-2020/>
- [25] <https://securelist.com/the-botnet-ecosystem/36279/>
- [26] <https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case>
- [27] <https://docs.microsoft.com/en-gb/MicrosoftTeams/get-clients>
- [28] <https://www.cisco.com/c/en/us/products/collaboration-endpoints/collaboration-room-endpoints/index.html?dtid=ossdc-c000283#~:explore=video-devices>
- [29] <https://cloud.google.com/access-transparency/>
- [30] <https://en.wikipedia.org/wiki/WebRTC>
- [31] <https://en.wikipedia.org/wiki/HTML5>
- [32] <https://www.bleepingcomputer.com/news/security/zoom-will-provide-end-to-end-encryption-to-all-users/>
- [33] <https://www.zdnet.com/article/bluejeans-announces-end-to-end-encryption-for-video-meetings/>

Timeline sources

- [t1] <https://www.zdnet.com/article/two-weeks-after-ransomware-attack-travelex-says-some-systems-are-now-back-online/>
<https://www.theguardian.com/business/2020/jan/13/travelex-services-begin-again-after-ransomware-cyber-attack>
<https://www.bleepingcomputer.com/news/security/travelex-reportedly-paid-23-million-ransom-to-restore-operations/>
- [t2] <https://www.bleepingcomputer.com/news/security/citrix-patches-cve-2019-19781-flaw-in-citrix-adc-111-and-120/>
<https://support.citrix.com/article/CTX267027>
<https://www.bleepingcomputer.com/news/security/hackers-are-securing-citrix-servers-backdoor-them-for-access/>
- [t3] <https://www.bleepingcomputer.com/news/security/emotet-uses-coronavirus-scare-to-infect-japanese-targets/>
<https://www.bleepingcomputer.com/news/security/as-coronavirus-spreads-so-does-COVID-19-themed-malware/>
- [t4] <https://www.bleepingcomputer.com/news/security/sextortion-e-mails-sent-by-emotet-earn-10-times-more-than-necur/>
- [t5] <https://www.bleepingcomputer.com/news/security/us-charges-chinese-military-hackers-for-equifax-breach/>
- [t6] <https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/>
- [t7] <https://blog.rapid7.com/2020/03/12/cve-2020-0796-microsoft-smbv3-remote-code-execution-vulnerability-analysis/>
<https://itcsecure.com/smbghost-cve-2020-0796-remote-code-execution-proof-of-concept/>
- [t8] <https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/?sh=136fb52b618e>
- [t9] <https://portswigger.net/daily-swig/tls-1-0-1-1-end-of-life-support-deadline-looms-for-website-encryption-laggards>
- [t10] <https://nakedsecurity.sophos.com/2020/03/27/fbi-takes-down-russia-based-hacker-platform-deer-io/>
- [t11] <https://www.bleepingcomputer.com/news/security/microsoft-teams-patched-against-image-based-account-takeover/>
- [t12] <https://nakedsecurity.sophos.com/2020/04/01/qr-code-generator-scam-steals-thousands-in-bitcoin/>
- [t13] <https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/>
- [t14] <https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/>
- [t15] <https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/>
- [t16] <https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns>
https://resources.malwarebytes.com/files/2020/05/The-Silent-Night-Zloader-Zbot_Final.pdf
- [t17] <https://www.bleepingcomputer.com/news/security/french-daily-le-figaro-database-exposes-users-personal-info/>
- [t18] <https://www.zdnet.com/article/revil-ransomware-gang-launches-auction-site-to-sell-stolen-data/>
- [t19] <https://nakedsecurity.sophos.com/2020/06/15/youve-heard-of-sextortion-now-theres-breachstortion-too/>
- [t20] <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350>
- [t21] <https://www.computerweekly.com/news/252486775/Garmin-may-have-paid-hackers-ransom-reports-suggest>
<https://www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/>
- [t22] https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html
- [t23] <https://www.zdnet.com/article/microsoft-august-2020-patch-tuesday-fixes-120-vulnerabilities-two-zero-days/>
- [t24] <https://www.nsa.gov/news-features/press-room/Article/2311407/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecu/>
- [t25] <https://healthitsecurity.com/news/blackbaud-ransomware-hack-affects-657k-maine-health-system-donors>
<https://portswigger.net/daily-swig/blackbaud-ransomware-attack-exposed-donor-data-from-two-uk-charities>
- [t26] <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hijacking-a-domain-controller-with-netlog-on-rpc-aka-zero-logon-cve-2020-1472/>
<https://ldapwiki.com/wiki/Netlogon%20service>
<https://thefirreport.com/2020/10/18/ryuk-in-5-hours/>
- [t27] <https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/>
- [t28] <https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity>
<https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies>

Disclaimer

Orange Cyberdefense makes this report available on an "as-is" basis with no guarantees of completeness, accuracy, usefulness or timeliness. The information contained in this report is general in nature. Opinions and conclusions presented reflect judgment at the time of publication and may change at any time. Orange Cyberdefense assumes no responsibility or liability for errors, omissions or for the results obtained from the use of the information. If you have specific security concerns, please contact Orange Cyberdefense for more detailed analysis and security consulting services.

**A very special thanks
to all cyber hunters,
analysts and engineers
in our SOCs.**



Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 11 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors. We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences including, Infosec, RSA, 44Con, BlackHat and DefCon.

www.orange cyberdefense.com

Twitter: @OrangeCyberDef