Skybox Security

VULNERABILITY AND THREAT

Trends Report 2018

Analysis of current vulnerabilities, exploits and threats in play

SKYBOX™ SECURITY

Contents

EXECUTIVE SUMMARY **3**

Key Findings 4

VULNERABILITIES AND EXPLOITS **5**

The Vulnerability Flood 5

OT Vulnerabilities and Attacks 6

Server–Side Vulnerability Exploitation Trending Up 7

Exploit Kits Declining but Not Dead 8

Infection Doesn't Equal Disaster 10

Social Engineering on the Rise? 11

60% Jump in Sample Exploit Code 12

Top Vulnerabilities to Follow 13

THREAT ACTORS **14**

Elite Goes Mainstream 14

Distributed Model Breeds Collateral Damage 14

MALWARE AND ATTACKS **15**

Era of Hybrids and Changelings 15

Top Malware By Category 16

CONCLUSION **17**

About This Report 18

About Skybox Security 18

EXECUTIVE SUMMARY

The old boundaries of cybersecurity and cyberattacks are disappearing — from the network perimeter, to distinct types of malware, to nation-state tactics vs. that of the cybercriminal. The attacker's advantage lies in this fluidity, exploiting endpoint vulnerabilities and inadequate security controls; reshaping attacks to evade detection; and repurposing tactics, techniques and procedures for their own use.

Cyberdefense, however, is often confined to silos stemming from disconnected processes, teams and network locations, and disparate data from various technologies and vendors. But the attacker sees no silos — only an attack surface with cracks to slip in through and press deeper into the network.

This report examines trends in vulnerabilities, exploits and threats in order to better align your security strategy with the current threat landscape. Vulnerability management programs particularly are in need of context. Prioritizing vulnerabilities by CVSS scores alone still leaves most enterprises with a laundry list of to-do's and no understanding of the threat a vulnerability poses to their organization. Adding intelligence of exploit activity in the wild, available sample exploit code and which vulnerabilities are being packaged in distributed crimeware will help organizations focus on the small subset of vulnerabilities putting them most at risk of attack.

Key Findings

Vulnerability Identification Gets a Boost

While this report is full of data on the advancements in the threat landscape, there are also signs of maturity in cybersecurity. For instance, the number of vulnerabilities published on average per month by MITRE's National Vulnerability Database (NVD) increased by 100 percent in 2017 over figures for 2016 due to organizational changes and increased vulnerability research.

Exploits Hit Hard

During 2017, there were just six new vulnerabilities exploited in the wild than in 2016. Despite the similar figures, 2017 exploits like EternalBlue were responsible for cyberattacks that stretched around the world in a matter of hours and had real impact on businesses and critical infrastructure.

Exploit Kits Down But Not Out

Since mid-2016, exploit kit activity has taken a dive mostly due to three dominant exploit kit developers going bust. However, such activity is still observed on a near-daily basis, and the storm of the next Angler may be brewing as we speak.

Server-Side Vulnerability Exploits Take the Lead

In 2017, 76 percent of all exploits affected server-side applications, including the Apache Struts vulnerability exploited in the Equifax data breach. The decline in client-side exploits reflects the trend in the decline in client-targeting exploit kits.

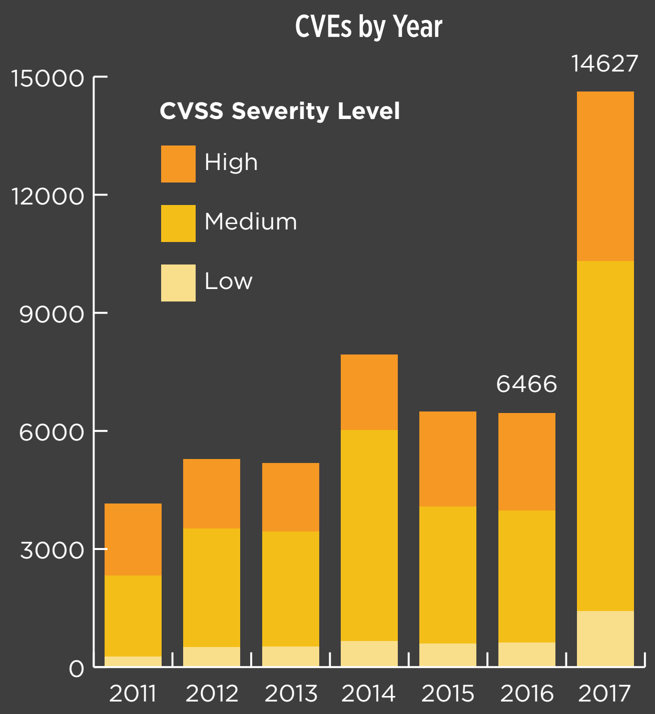
Sample Exploit Code Readily Available

New sample exploit code jumped 60 percent on average per month in 2017, making it easier to acquire vital attack components that need little adjusting to fit an attacker's objectives.

VULNERABILITIES AND EXPLOITS

The Vulnerability Flood

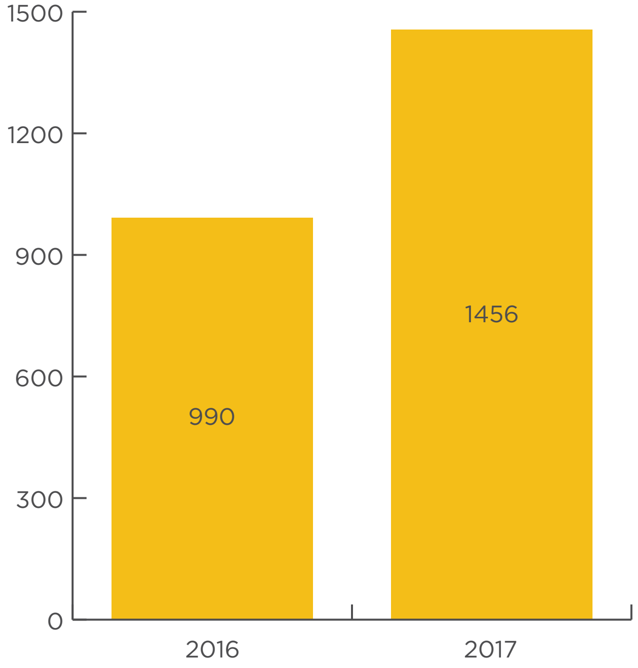
Vulnerabilities play a major role in everything from ransomware to the nation–state threat actor's playbook. So it's encouraging to see the MITRE organization increase resources to support the National Vulnerability Database (NVD). In addition to the organizational improvements, an increase in vendor and third–party vulnerability research resulted in more requests to MITRE to assign CVEs. As such, the number of vulnerabilities published in NVD in 2017 doubled compared to the previous year.



Source: https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

In terms of the types of vulnerabilities, there has been significant growth — 47 percent — in vulnerabilities in internet–connected and mobile devices.

Mobile OS Vulnerabilities



However, to deal with the influx in vulnerabilities requires better prioritization mechanisms than simply base or temporal scores of the Common Vulnerability Scoring System (CVSS). To illustrate this issue, take the many examples of browser vulnerabilities integrated into exploit kits. For instance, CVE-2017-0059 is a medium–severity vulnerability (rated just 4.3) in Microsoft Internet Explorer, but is used in both the Terror and Disdain exploit kits. On its surface, it allows "just" information disclosure, but considering that stealing banking credentials is also "just" information disclosure, it seems this vulnerability would warrant a higher severity rating. As evidenced by this example, CVSS doesn't always align with reality.

Additionally, CVSS doesn't reflect the risk posed in a unique network where certain critical vulnerabilities might be sufficiently isolated by a combination of network topology and security controls, while a medium–severity vulnerability sits exposed to potential attack. Abiding by CVSS prioritization in this instance would incorrectly reflect the risk of such issues.

OT Vulnerabilities and Attacks

Operational technology (OT) networks such as those used in energy production, manufacturing, utilities, etc. are affected by OT–specific vulnerabilities, as well as by IT vulnerabilities on systems within the OT network. Many of the human machine interfaces (HMIs) overseeing OT networks are often old, unpatched or even unsupported Windows machines sharing the same protocols like Server Message Block (SMB) and NetBios. Such HMIs could be introducing a multitude of known and exploitable Windows vulnerabilities to an environment not built to the cybersecurity standards of corporate IT networks. Even vulnerabilities within the corporate network could be used to infiltrate the OT environment, as 81 percent of organizations use wireless connections between their IT and OT networks.[1]

During 2017, almost 200 new OT–specific vulnerabilities were published, affecting Siemens products, Schneider Electric, Moxa, Rockwell and other vendors. This figure represents a 120 percent increase over that of 2016.

This rise in vulnerabilities is particularly challenging in OT environments for several reasons. OT devices are expected to maintain constant and flawless uptime and are rarely taken down for security updates or otherwise. Installing a patch could also affect performance, void vendor warranties or create safety issues for employees or communities served. Thus, patching is kept to a minimum.[2]

Additionally, about 30 percent of OT–specific vulnerabilities do not have a CVE identification, making many traditional scanning solutions ineffective (scanning is also largely prohibited due to potential disruptions).

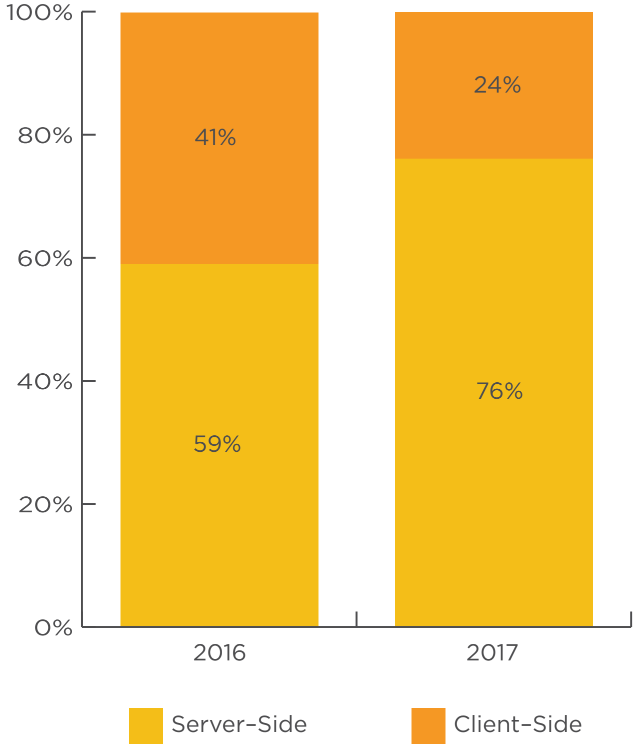
[1] Kaspersky Lab. ICS Cybersecurity: A view from the field. February 1, 2018. https://www.kaspersky.com/blog/ics-report-2017/16967/
[2] Kaspersky Lab. State of Industrial Cybersecurity 2017. https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

Server–Side Vulnerability Exploitation Trending Up

Looking at vulnerabilities exploited in the wild by the date on which they were reported, a trend is emerging: vulnerabilities affecting client–side applications are declining as those impacting server–side applications are increasing.

According to our findings, there were 49 newly exploited vulnerabilities in all of 2016. Client–side vulnerabilities accounted for 41 percent of those exploits while 59 percent were server–side vulnerabilities. Many of the client–side vulnerabilities were embedded in the popular exploit kits. During 2017, of the 55 new vulnerabilities exploited, only 24 percent were client–side vulnerabilities and 76 percent were server–side, including the Apache Struts vulnerability exploited in the Equifax data breach. The decline in client–side exploits reflects the trend in the decline in client–targeting exploit kits.

Vulnerabilities Exploited in the Wild



Analyzing which vendor's vulnerabilities have been newly exploited in the wild, Microsoft continues to hold a first–place spot. It's ubiquity among individuals and businesses alike make developing exploits for Microsoft vulnerabilities an attractive investment. It offers a huge list of potential targets — especially useful in the model of distributed cybercrime — popular in enterprises and in OT network as well.

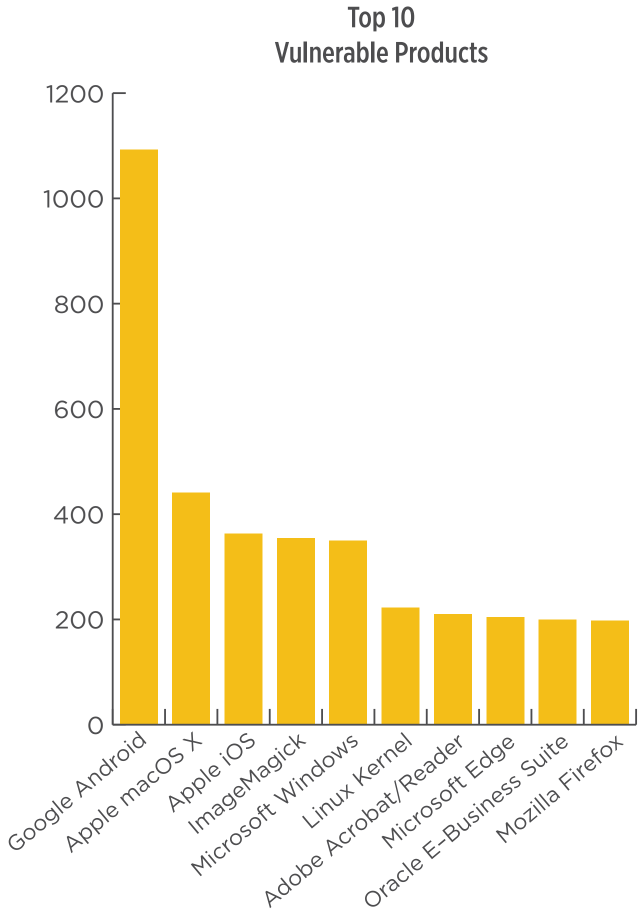
Microsoft is responsible for around a third of exploited vulnerabilities published in 2016 and 2017 that were actively used in the wild. Most infamously, the vulnerabilities included in MS17-010 played a starring role in the WannaCry attacks that exploited a Windows OS vulnerability in Server Message Block (SMB). The Shadow Brokers also released a long list of additional Microsoft exploits in 2017.

Top Exploited Vendors			
2016		**2017**	
Microsoft	**36%**	Microsoft	**39%**
Adobe	**16%**	Oracle	**14%**
Oracle	**4%**	Cisco	**7%**

During 2016, Adobe took second place, dropping to the fourth slot in 2017. Could it be a sign that the long–maligned, vulnerability–plagued Adobe Flash is finally on its way out? One can only hope.

Cisco has pushed its way into the top three in 2017, largely due to the use of vulnerable third–party applications like Apache Struts that was exploited in the Equifax data breach, and by the use of a Cisco WebEx vulnerability (CVE-2017-3823) in the Disdain and Neptune exploit kits.

Looking at purely vulnerability stats (i.e., not just exploited vulnerabilities), the most vulnerable product is Google Android, representing 10 percent of all 2017 vulnerabilities. Following behind is Apple macOS X and iOS, and ImageMagick — a graphics library embedded in Linux and, therefore, widely used.



The chart above shows the top 10 vulnerable products in 2017 accounting for roughly 3600 vulnerabilities. The other approximately 1,500 products tracked in our research were responsible for around 6,000 vulnerabilities in 2017 — less than double that of the top 10 products.

Exploit Kits Declining but Not Dead

Exploit kits have been a hallmark of the distributed cybercrime industry, putting a vital component of cyberattacks for sale (or rent) on the dark web making them available to the masses. Exploit kits are not just the handiwork of individual hackers, but of organized criminal groups, such as the famous Lurk gang behind the Angler exploit kit, intent on maximizing ROI (and evading arrest). However, their use is in decline, with attackers favoring alternative means of infection like social engineering. But just where have all the exploit kits gone?

Back in 2016, the developers of one of the top exploit kits, Angler, were arrested, following a long and concentrated effort by cybersecurity researchers. The arrests greatly shook up the exploit kit market, leaving the field without a dominant leader.

In 2017, the year began with four main exploit kits: RIG, Terror, KaiXin and Sundown, with other notable kits including Nebula, Sundown, Disdain, Magnitude and Astrum. By the end of 2017, Magnitude had replaced Sundown[1] in the major players list. However, these kits paled in comparison to the previous giants like Angler, Neutrino and Nuclear.

With the disappearance of these three kits (Angler's developers arrested, Neutrino's malvertising campaign squashed and Nuclear earning too much attention from security researchers), exploit kit activity has declined dramatically.

That being said, there is still significant activity in the exploit kit domain. And it's important to remember that exploit kits are a sort of living creature, evolving over time as they adopt new technologies to avoid detection. There's no telling when they'll rear a stronger and uglier head than before.

[1] Execute Malware. Exploit Kit Landscape Map. http://executemalware.com/?page_id=320

THE Life Cycle OF AN Exploit Kit

1 Development

Mostly occurs responding to a "market" opportunity when an old player has left the business — by their own volition or in handcuffs.

2 Blossom

Using only a small set of exploits, conversion rates of targets to victims are good. The exploit kit is usually available for purchase in this phase, sold for around $20,000-$30,000 or rented for $1,000-$2,000 per month. The idea is to keep the exploit kit effective enough to make money for the creators, but not so much so that its vulnerabilities won't be patched in a mass scale.

3 Privatization

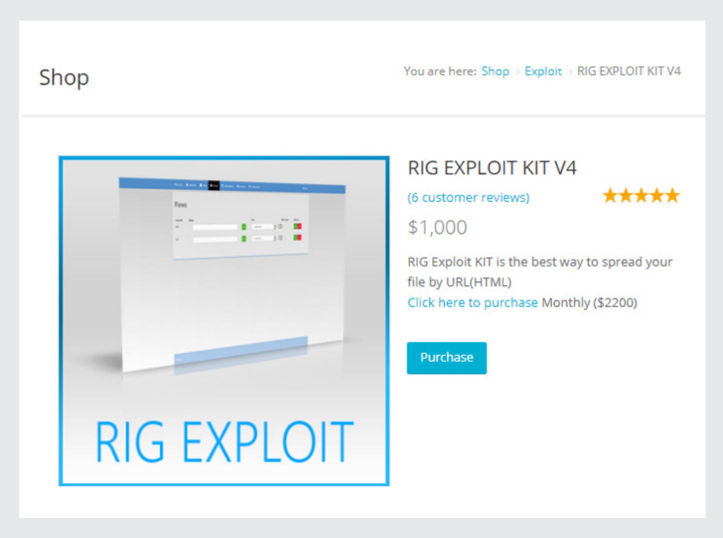
The owners behind the exploit kit still use it themselves, but it is no longer for sale. In this phase, there is a decline in the kit's distribution in hopes that the exploits will remain viable for the owners' own use.

4 Death

Possible scenarios for this phase are the exploit kit's conversion rate is below the minimal threshold, or the owners behind it have moved on to other pursuits (including prison work details).

While the exploit kit market awaits its next giant, targeted attacks are on the rise, using zero–day vulnerabilities or those with a patch readily available like Apache Struts.

The use of social engineering has also proved effective to hackers in 2017. As social engineering initially exploits weaknesses in people rather than software, it has presented a huge challenge to cyber defenders. Many are still trying to figure out what is the most effective, systematic approach for dealing with these attack vectors. In the meantime, cybercriminals are perfecting their tactics.



Shop

You are here: Shop › Exploit › RIG EXPLOIT KIT V4

RIG EXPLOIT KIT V4

(6 customer reviews) ★★★★★

$1,000

RIG Exploit KIT is the best way to spread your file by URL(HTML)

Click here to purchase Monthly ($2200)

Figure 1

Proof of the commercialization of cybercrime: the pleasantly designed, easy–to–use purchase page for the RIG exploit kit.

If any more proof was needed to show the industrial strength behind cybercrime, consider that social engineering attackers have "click through" formulas similar to many marketing programs, defining how many targets they need to touch in order to trick one into visiting a malicious site or opening a malicious file. Defense strategies, too, need to have similar, calculated insights.

One of the more notable social engineering–enabled attacks of 2017 was Bad Rabbit. The international ransomware attack began with legitimate but compromised sites that requested a fake Adobe Flash update that actually contained the malware. It required no vulnerability exploitation in the initial attack or lateral movement in the continuation.

Infection Doesn't Equal Disaster

Whether from social engineering, exploit kits or other methods of entry, infection doesn't have to equal disaster. How you prepare for and deal with infection — and limit its propagation is — what counts. Here's the top three cyber hygiene practices that can decrease the threat and damage done in cyberattacks.

Minimize Exposures

The WannaCry attack was a lesson in the importance of speedy mitigation. A key component of the attack involved vulnerabilities with an available patch and the heavily publicized EternalBlue exploit. This demonstrates that either organizations don't have effective means of prioritizing remediation or patching implementation continues to be an organizational challenge.

When patching isn't an option for reasons within or outside the organization, vulnerability management teams need fast insight to the other options at their disposal, such as IPS signatures, firewall rule changes or changes to other security controls, to cut off potential attack paths. This is especially needed for exposed vulnerabilities with known exploits.

Strengthen Internal Security Controls

One machine infected with WannaCry wasn't the biggest concern: it was the light speed with which it spread from individual machines through organizations and around the world. WannaCry propagated through open SMB ports and shows how quickly an attack can use network connectivity for its own advantage.

Proper segmentation will greatly limit the spread of an infection. Understanding how attacks can move through your network — including multi-cloud or OT environments — is crucial to effective segmentation. Attacks using stolen legitimate credentials can also be counteracted by limiting access to only required resources, minimizing the use of admin user accounts and requiring complex passwords that cannot be easily guessed in the case of brute force attacks.

Prioritize Intelligently and Track Remediation

Relying on CVSS scores alone is not enough to understand the threat vulnerabilities pose to your organization. You need to analyze vulnerabilities in the context of asset criticality, the surrounding network topology and security controls and the current threat landscape. Removing any one of these elements makes for inaccurate prioritization, and can waste remediation efforts on vulnerabilities less likely to be used in an attack.

Remediation should be focused on the small amount of vulnerabilities representing an imminent threat to your organization: those that are exposed in your network or actively exploited in the wild. The rest of your vulnerabilities pose a potential threat and should be dealt with as part of gradual risk reduction processes; these vulnerabilities, though, also need to be monitored for changes in exposure or exploitability.

Social Engineering on the Rise?

The use of social engineering has been a key page in the attacker playbook for years. But in 2017, spear phishing especially has risen as the favored delivery method,[1] tailoring the communications to each victim: for instance, HR professionals may receive a malicious file that appears to be a resume.

Social engineering attacks are delivered via email as an attachment or as a link to a specially crafted website using the following techniques:

CYBER HYGIENE 101:

A good starting point to protect against malicious spam campaigns is to enforce a strict policy of not running macros organization–wide.

Phishing Email + Vulnerability Exploit

- The Dridex banking Trojan was spread via a phishing campaign that exploited CVE–2017–0199, with an email sent to employees containing a specially crafted document. The sender? An office photocopier.
- Early reports suggested NotPetya was spread via phishing emails with malicious office document attachments exploiting CVE–2017–0199.

Running Macro Code

- Macros are used in Microsoft Office documents and, by the default protected view, are disabled. Very often, however, a user can manually enable macros (or enable editing) to see the content. In doing so, the malicious payload can be installed and infect the system.
- The TrickBot banking Trojan and Jaff ransomware were delivered as specially crafted documents in June 2017.

Malvertising

- Recent trends in malvertising pair malicious ads with legitimate applications (such as Fireball and numerous Android apps). The tech scam has unsuspecting victims download the "app," plug–in, font, etc. containing the malware.

Exploit Kits + Social Engineering

- Exploit kits can also be used in malvertising campaigns, as was the case when the Magnitude exploit kit used malvertising to deliver the Cerber ransomware in March of 2017. In this type of attack, users encounter malicious ads and are redirected to an exploit kit landing page. The user does not necessarily have to click the malvertisement; users only need the page containing the malicious ad to load in the browser.

Attacks distributed through social engineering are a challenge for every organization, as it takes advantage of human error opposed to security issues. Educating employees on best cyber practices will only go so far, but it's likely something will still fall through the cracks. Organization need broader, more systematic approaches to address the challenges of social engineering.

[1] Tech Republic. Report: Email attacks increasing, but none as much as impersonation phishing. https://www.techrepublic.com/article/report-email-attacks-increasing-but-none-as-much-as-impersonation-phishing/

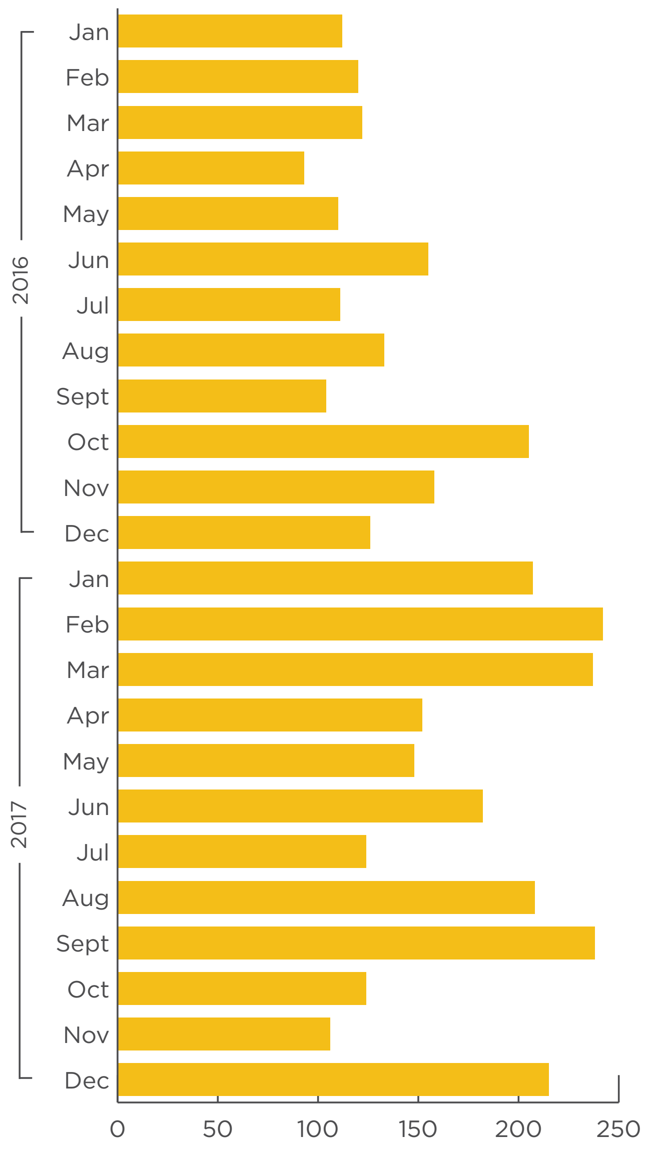
60% Jump in Sample Exploit Code

Many vulnerabilities have sample exploit code available in websites such as ExploitDB, SecurityFocus and GitHub. With minimal adjustments, if any, attackers can execute the exploit to make it fully functional.

During 2017, the number of exploit samples published per month increased at an average of 60 percent, from an average in 2016 of 121 exploit samples per month to 194.

This influx is making more and more advanced cyber weapons available to the masses of lower-skilled attackers, and the technical level of skill to make sample code fully functional is declining. Generally, exploit sample code requires minimal adjustment to fit a specific attacker's needs. Leaked exploits, as was the case with NSA-developed EternalBlue, are fully functional and need only be packaged with a delivery method.

Vulnerabilities With New Sample Exploit Code Published



SO MANY Vulnerabilities, SO FEW Exploits

Considering the thousands of vulnerabilities published in 2017 and the hundreds of vulnerabilities with available exploit code, why were only 55 exploited in the wild? It all comes back to threat resources.

Developing new exploits from scratch is no easy feat. Using them on a mass scale is even harder, requiring infrastructure (including command and control servers), QA, software update mechanisms and more. Many nation states have seen the advantage of developing (or buying) exploits that are top-secret — and attempt to keep them that way.

Considering the work that goes into exploit development, it is generally used for as long as possible; that is, until its conversion ratio dips below the acceptable threshold. At that point, it's time to develop the next zero-day.

Usually, each threat actor has its infrastructure and set of tools used for several attacks. It's generally been perceived as difficult for a threat actor to modify its tactics, techniques and procedures (TTPs); however, adoption of tools developed by other players has seemed to become easier and more popular.

Top Vulnerabilities to Follow

Oracle WebLogic Server

- Easily exploitable vulnerability via HTTP capable of compromising Oracle WebLogic, a Java EE application server
- Has been documented as downloading and executing cryptocurrency miners
- CVE-2017-10271

Apache Struts 2 Vulnerability

- RCE vulnerability
- Easy attack vector, similar to the vulnerability used in the Equifax data breach
- CVE-2017-9805

Microsoft Windows Vulnerability in Windows Search Service

- RCE vulnerability that does not require user interaction
- CVE-2017-11771

Microsoft XML Services Vulnerability

- Added to the Astrum exploit kit (aka Stegano)
- Recently used in a malvertising campaign delivering the Mole ransomware
- CVE–2017–02643

Microsoft Office Vulnerability

- RCE vulnerability which could allow for memory corruption
- Delivered by a phishing email with an RTF attachment
- A zero–day, the vulnerability was in use in actual attacks months before Microsoft's patch in October 2017
- CVE-2017-11826

Apple iAmRoot

- Allows root access with no authentication
- Not exploited in the wild (as of the publishing of this report), but attack vector is trivial
- CVE-2017-13872

THREAT ACTORS

Elite Goes Mainstream

The most significant threat trend in 2017 was the leaking of exploit tools from nation-state actors to mainstream attackers and targeting victims not usually of nation-state interest. Advanced exploits often developed for cyber espionage or cyber warfare purposes, such as the U.S. National Security Agency's EternalBlue exploit, have now been made public (in the NSA's case, thanks to The Shadow Brokers' leak in April 2017).

Now, cybercriminals can take these exploits, modify them as necessary and package them with a distribution mechanism to launch a sophisticated attack that requires minimal skills or investment in development. In the case of the MS17-010 vulnerabilities exploited by EternalBlue and other NSA cyber tools, even the existence of a patch was not enough in reality to keep organizations safe from the threat they posed. The two major attacks centering on these vulnerabilities — WannaCry and NotPetya — occurred two and three months after the patch release, respectively.

Distributed Model Breeds Collateral Damage

Attackers always have a target and a motive, whether it's financial gain, espionage, hacktivism or good-old-fashioned mayhem. Traditionally, the interests — and therefore, tools — of nation-state and mainstream attackers have been divided. But recently, retrofitting TTPs useful for a specific target or motive has gained popularity.

Ukraine appears to have been the target of the NotPetya attack, but organizations in several other countries were also hit because of factors they shared with the intended targets. The distributed model of the ransomware attack enabled NotPetya to spread rapidly across Ukraine and anywhere else it could. As cyberattackers likely have no qualms with who else is captured in the net of their attack, expect similar large-scale, collateral cyber damage in the year ahead.

While it's important to know who your enemy is, it's also important to understand that the tools of one can easily be adopted by another.

MALWARE AND ATTACKS

Era of Hybrids and Changelings

As evidenced by the chart on the following page, the two ransomware finalists at the top of our list were less than stellar at collecting ransom. Both WannaCry and NotPetya started out as ransomware attacks, but the email accounts to which a victim could use to pay the ransom were both blocked. They also weren't purely ransomware. WannaCry spread via a worm and NotPetya seemed more intent on being a wiper in ransomware's clothing.

Traditionally, malware has fallen into distinct categories: ransomware, banking Trojans, worms, etc. Now, those divisions are disappearing and attacks are using multiple elements to evade detection, spread and reach their goal.

As malware morphs into new, complex hybrids of its former self, threat intelligence has never been more vital.

Top Malware By Category

	What it Does	Why it's Important
Ransomware		
WannaCry	Ransomware	Spread to 150 countries within a matter of hours
NotPetya	Wiper (masquerading as ransomware)	No killswitch a la WannaCry Crippled a big part of Ukraine's infrastructure and some of the private sector Capable of bricking machines
Cerber	Ransomware	The leading ransomware during the first quarter of 2017 Pioneering ransomware–as–a–service schemes Distributed via different exploit kits in multiple campaigns Infected 150,000 victims in July 2016 alone
OT Malware		
Industroyer	Takes control of electricity substation switches and circuit breakers directly using industrial communication protocols present in critical infrastructure worldwide	Uses the functionality of the protocol (designed decades ago) against itself
BlackEnergy	Remote access Trojan	Attacks against Ukrainian critical infrastructure during late 2015
Banking Trojans		
TrickBot	Banking credential-stealing malware via the end user's browser	Targeting financial organizations across the globe, focusing on the U.K.
Dridex	Steals banking credentials	Active since 2014, constantly changing Estimated damage has reached the hundreds of millions of dollars[1]

[1] Slepogin, Nikita. Dridex: A History of Evolution. SecureList. May 15, 2017 https://securelist.com/dridex-a-history-of-evolution/78531/

CONCLUSION

In order to accurately prioritize remediation, organizations have to keep up with the threat landscape as it evolves. As trends in vulnerabilities, exploits and threat shift, so too must defense strategies. From WannaCry to NotPetya to the Equifax data breach, it's clear that intelligence — and taking proactive measures based on that intelligence — can make the difference between an intrusion and a damaging cyberattack or data breach.

Systematically incorporating threat intelligence in your vulnerability management and overall security management program is key to directing efforts in the right place. Correlating information of your vulnerabilities, assets, network topology and security controls with intelligence of the current threat landscape will ensure resources are focused on risks most likely to be exploited by an attacker.

About This Report

All information and data in this report without explicit reference is provided by the Skybox™ Research Lab, a team of security analysts who daily scour data from dozens of security feeds and sources as well as investigate sites in the dark web. The Research Lab validates and enhances data through automated as well as manual analysis, with analysts adding their knowledge of attack trends, cyber events and TTPs of today's attackers. Their ongoing investigations determine which vulnerabilities are being exploited in the wild and used in distributed crimeware such as ransomware, malware, exploit kits and other attacks exploiting client– and server–side vulnerabilities. This information is incorporated in the threat–centric vulnerability management (TCVM) approach of Skybox's vulnerability management solutions, which prioritize the remediation of exposed and actively exploited vulnerabilities over that of other known vulnerabilities.

For more information on the methodology behind the Skybox Research Lab and to keep up with the latest vulnerability and threat intelligence, visit www.vulnerabilitycenter.com.

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 120 networking and security technologies, the Skybox™ Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060

SKYBOX™
SECURITY