SUBEX

SecOre

THE GLOBAL THREAT LANDSCAPE REPORT

A Subex Threat Research Labs initiative

Q1 2020

www.safeandsecureiot.com

INTRODUCTION

After Subex reported the first instance of hackers using the Coronavirus pandemic to launch targeted cyberattacks in February 2020, the number of such attacks has grown exponentially since. Hackers struck in waves beginning the middle of February and intensified operations throughout March. Though we have heard of many instances of collaboration tools being hacked, it is difficult to determine the exact impact of Coronavirus related hacking on enterprises across the globe as many have not come forward and reported breaches.

But if we analyze the significant increase in cyberattacks registered by our honeypot network, it becomes clear that the hackers were highly motivated and may have been scoring success at least some of the time.

Key trends

- Coronavirus-themed phishing attacks on the rise
- Remarkable increase in cyberattacks on China
- Increasing instances of ransomware and trojans being detected
- Surveillance cameras remain the most attacked category of devices
- Most attacked regions – NA, South Asia and the Middle East
- Increase in reconnaissance (listening) attacks on critical infrastructure
- Data leakages on Dark Web increase 7 percent
- North Korean hackers switch tactics target multiple sectors
- Manufacturing, healthcare institutions, enterprises and banks among the most targeted sectors
- A rise in deceptive attacks on critical infrastructure (designed to keep national CERT teams and other cyber defense agencies occupied while the hackers chase other high-value targets)

APT watch

Advance Persistent Threat groups across the globe used the scare and anxiety generated by the Coronavirus scare to lure victims to download infected files or click on suspicious links through targeted attacks. These groups have become overactive in 47 out of 90 days of the last quarter with extensive and focused work done by their hackers and affiliated groups in targeting individuals, governments and enterprises.

Kimsuky APT: of North Korean origin, is among the oldest North Korean APT groups out there. Primary targets include South Korean institutions linked to the government, higher education and research and defense. The group has a global footprint that spans nations such as India, USA, UK and France.

Modus operandi: plant malware in documents claiming to outline South Korea's response to the Coronavirus pandemic. For its attacks outside South Korea, the group has been relying on as many as 11 emails claiming to be from the World Health Organization, Centers for Disease Control and the National Health Service, UK. In many instances the mails had PDF or word documents loaded with BabyShark malware.

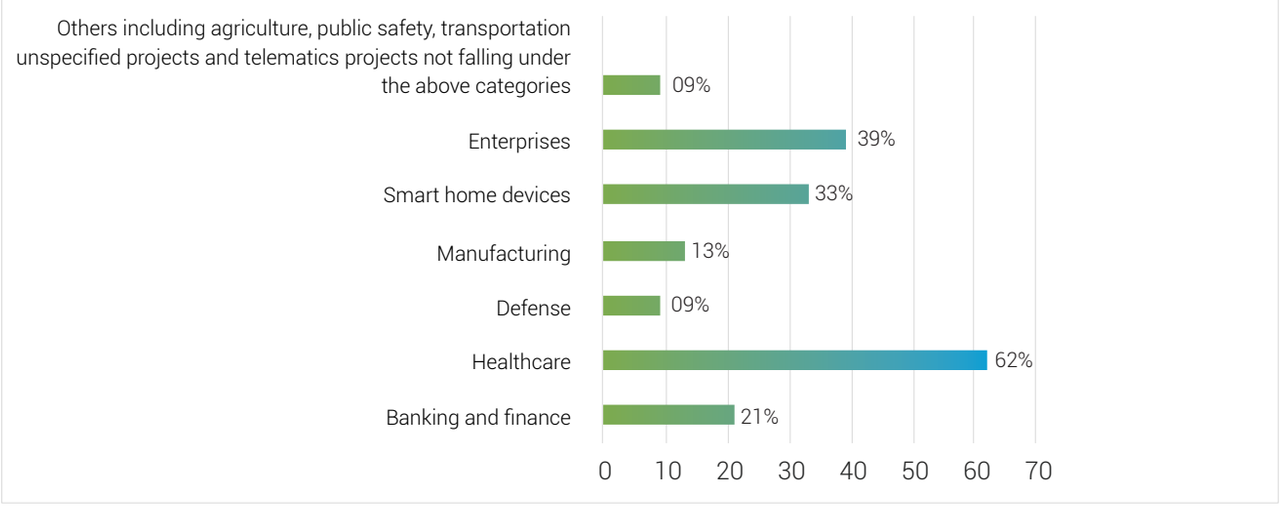
APT 36: of Pakistani origin, this group is using multiple messages related to Coronavirus to target Indian think tanks, diplomatic institutions, and defense installations.

Modus operandi: this group which used to rely on 'operational information' mails in the past is now using healthcare updates, health advisory for key personnel, diplomatic response updates and operational continuity as key themes in its effort to trick potential victims. As with its previous attempts, the targets are clearly high profile and senior serving and retired bureaucrats and defense personnel.

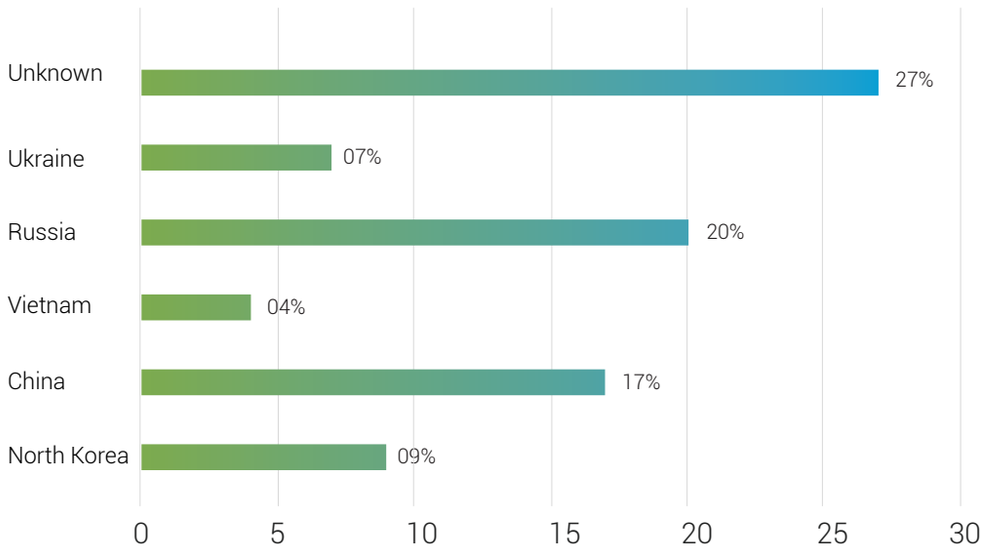
Information targets: machine configuration information, browsing patterns, passwords stored in victim's browsers and more.

Vicious Panda: of purported Chinese origin, this group has been targeting Ukraine, Mongolia, India, UAE and Vietnam.

Modus operandi: using fake diplomatic communication connected to the Coronavirus and beyond to lure people into downloading malware laden word documents. Once the document is opened, the infection is triggered with multiple processes with the machines (desktop/laptop) being targeted. Data and files are also deleted and modified without the knowledge of the victim.



Top countries of origin of cyberattacks



Cities drawing most cyberattacks

Many new cities entered the list of top 50 most attacked cities across the globe. The cyberattacks show a clear shift towards attacking cities located in remote corners of various countries. Attacks on ports, airports and other facilities in such cities witnessed a steep rise in attacks. Here are the top 10 cities that were attacked most often in 2020:


New York

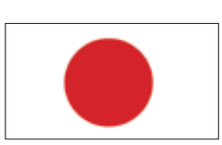

Rome


London


Kiev


Singapore


Dubai


Tokyo


Madrid


New Delhi

Focus on confusion, anxiety and less reaction time

We were tracking Coronavirus themed mails as early as Feb 23 when we were came across a sample mail. The messaging was crude and as the days went by, the hackers used more targeted messaging to play on fears of potential victims. From early March, hackers started sending emails targeting employees who were working from home. These emails had messages such as "Your official email account has been disabled by your administrator post a security assesment. Please apply a patch to your operating system to enable your device to clear the next assesment due later this week. Click here to download the patch. Failure to do so will lead to your

account being closed permanently as per our security policy".

Over 500 variants of such emails were intercepted by our threat research team. Each had a unique message and there were nearly 89 different messages that were passed on through these emails.

This clearly shows that hackers are showing a high level of interest in procuring data that can be monetized faster.

Average time to transfer data to C&C servers (lab\virtual environment)

NATURE OF DATA	AVERAGE OBSERVED TRANSFER WINDOW/ FREQUENCY OF COMMUNICATION WITH C&C
Credentials\proprietary\IP based\confidential	2-5 hours post injection of data
Network analytics info	8 hours or more
Normal/routine traffic	9 hours or more

Malware sample size for the test: 3970
Target sectors: manufacturing, telcos, defence, healthcare, shipping and utilities

In the last few weeks of March, the average time taken by malware to open communication links with command and control (C&C) servers has come down by an average of an hour globally. This means that the hackers are working to get information from infected devices and networks faster. The hackers are acting to improve their time to market with such information while exploiting the Covid-19 pandemic. They are definitely viewing this as an opportunity to expand their tactics, test strategies and also hoard and sell more information from victims.

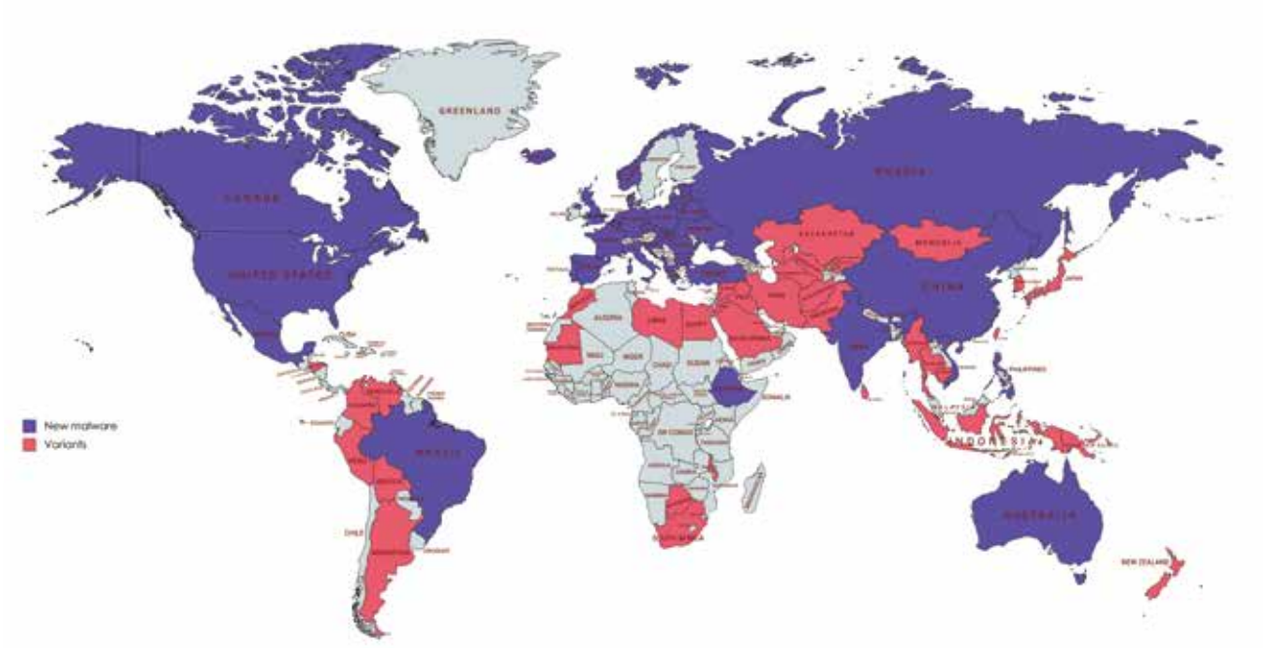
Reconnaissance activity that dipped in early February picked pace in the last two weeks of April indicating a period of testing and introducing new malware or even trying out new breach strategies. We feel that this might be an indication of these hackers getting ready to launch phase two of their plan of action.

Malware trends

In terms of malware diversity, the quarter saw the introduction of new variants of many malware including old ones such as Mirai. In March, we were able to detect multiple instances of ransomware as well including Locky and Sadogo. Though the volume of new malware registered a small dip this quarter, number of variants increased significantly.

We were expecting a significant increase in new malware between February and March 2020. We feel hackers and malware groups are holding on to the new malware developed and bought and releasing them less frequently than the same time last year. This may be because the focus has shifted from releasing new malware to using existing malware or variants in a better way using better deception strategies and tactics.

Map - global distribution of variants and new malware



As in 2019, we also recorded malware developers investing in techniques designed to prevent reverse engineering and de-bugging in order to prevent threat researchers from conducting detailed analysis and helping avoid detection thereby increasing persistence. Other than stealth and easy and rapid deployment, persistence was another key factor that malware developers were after.

Key traits in malware detected around the world (sample size 3970 unique malware)

Trait	Trait detection rates (in percentage)	Geographic distribution or focus	Verticals targeted
Persistence/ Endurance	High 79 Low 28	North America, Western Europe	Manufacturing, enterprise and critical infrastructure
High levels of stealth	66	Global	Defence, connected vehicles and manufacturing
Faster deployment	59	Global	Almost all verticals
Crypto mining	7	All except Latin America	Smart cities and manufacturing
High network mobility plus Lateral movement	33	Global	Manufacturing, smart cities, Defence, telecom

Malware sources

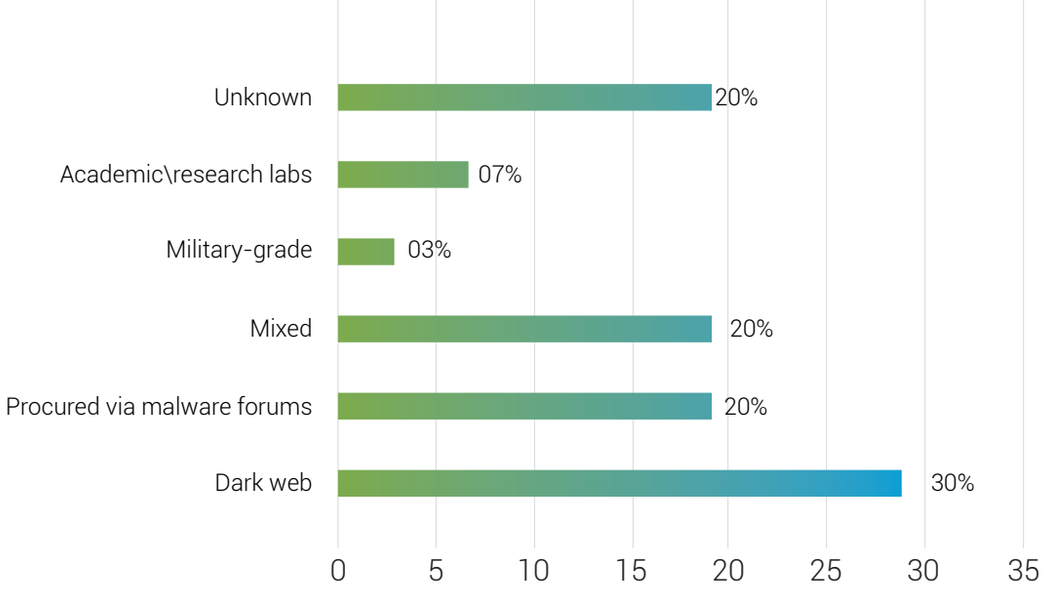
Malware authors are constantly seeking newer channels for selling malware. In the past, Darkweb was the primary source of malware trade. Today however, malware can be procured from various forums across the web. Malware market, hitherto a network of entities, agents, forums, websites and even blogs where malware can be bought or sold have morphed into one-stop shops where malware is sold, hackers and

developers and even consultants hired. There are also service based models that hackers are offering for a fee. In the first 3 months of 2020, traffic to some of these forums increased rapidly as monitored from third-party sites indicating a high level of interest. While hackers and malware users are focusing on strategies to create better communication or social engineering efforts to lure hackers, malware authors are working on releasing newer variants that evade complex malware detection mechanisms and operate with as less footprint and signature as possible.

In case of the APT actors the malware procurement patterns vary according to the country they belong to. Some actors are backed by extensive R&D facilities that churn out high grade malware to weaponize vulnerabilities. While every vulnerability out there is not exploited, the rate of discovery of new vulnerabilities has increased in the last few years. A study of the National Vulnerability Database maintained by NIST revealed that as many as 6 critical vulnerabilities have been discovered so far. The APT actors may have access to more critical vulnerabilities that are not in public domain yet.

Malware shops\markets also keep pace with changing defence tactics deployed by hackers. In 2020, we saw many exploit kits changing versions within a short period of time (as less as a fortnight in some cases). The new kits had new vulnerabilities (minus old and ineffective ones) making them more potent.

Malware origin

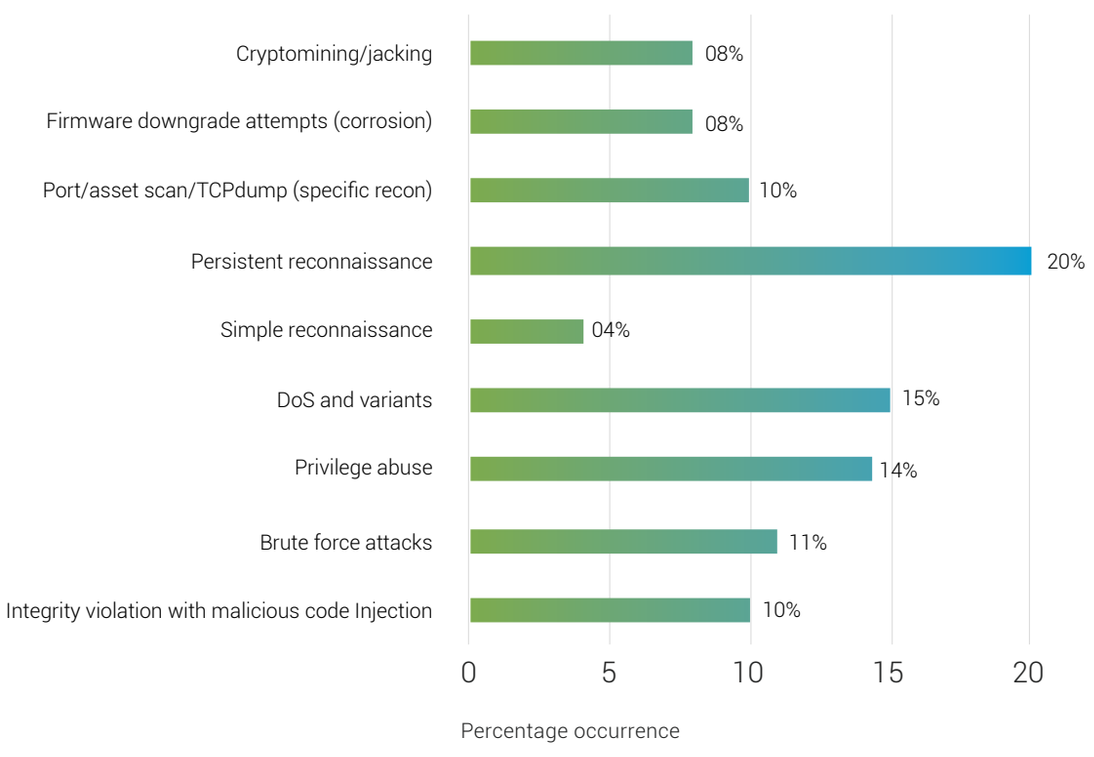


At our research lab, we were able to segregate malware based on observed traits, deep content inspection, multi-layer inspection and analysis and code slicing. Using dual sand boxing and some of our proprietary techniques, we were also able to do a behavior analysis and stealth evaluation.

Top Ports attacked

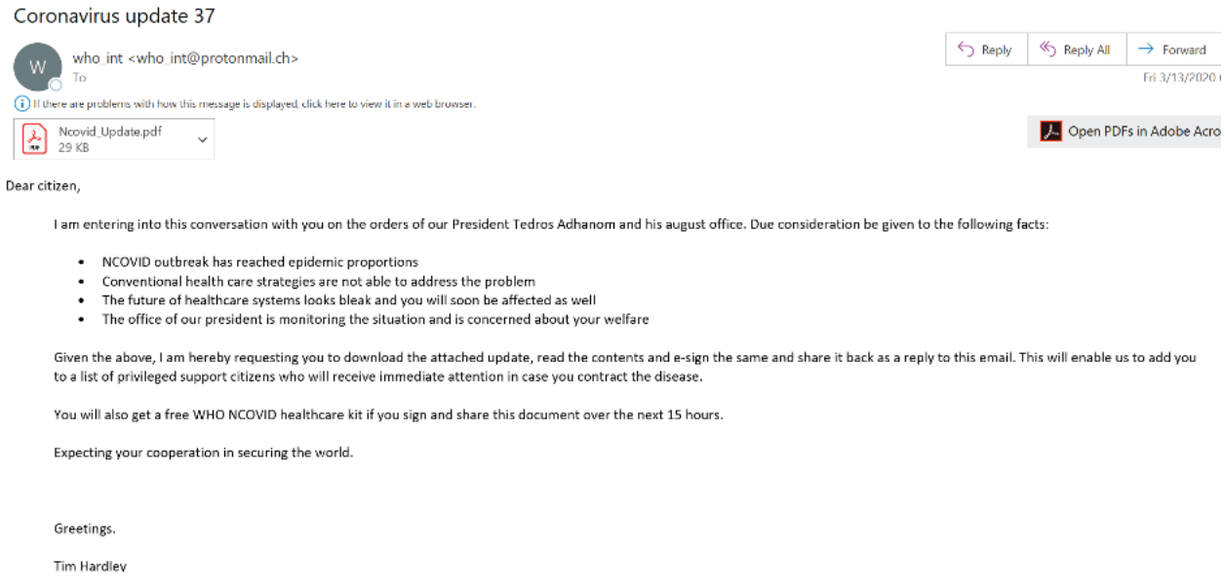
PORT	ATTACKS IN 000S
23 -Telnet	300
445 - SMB	225
22 SSH	217
1433 MSSQL	191
3306 MySQL	176
80 - HTTP	155
7547 - CWMP	97
25 - SMTP	44
20 FTP	39
Others	12

Types of attacks and frequency



Overall implications of employees working from home on cybersecurity

A sample of deceptive email attributed to the World Health Organization intercepted by Subex's threat research team.



Coronavirus update 37

W who_int <who_int@protonmail.ch>
To

Reply | Reply All | Forward
Fri 3/13/2020

If there are problems with how this message is displayed, click here to view it in a web browser.

Ncovid_Update.pdf
29 KB

Open PDFs in Adobe Acro

Dear citizen,

I am entering into this conversation with you on the orders of our President Tedros Adhanom and his august office. Due consideration be given to the following facts:

- NCOVID outbreak has reached epidemic proportions
- Conventional health care strategies are not able to address the problem
- The future of healthcare systems looks bleak and you will soon be affected as well
- The office of our president is monitoring the situation and is concerned about your welfare

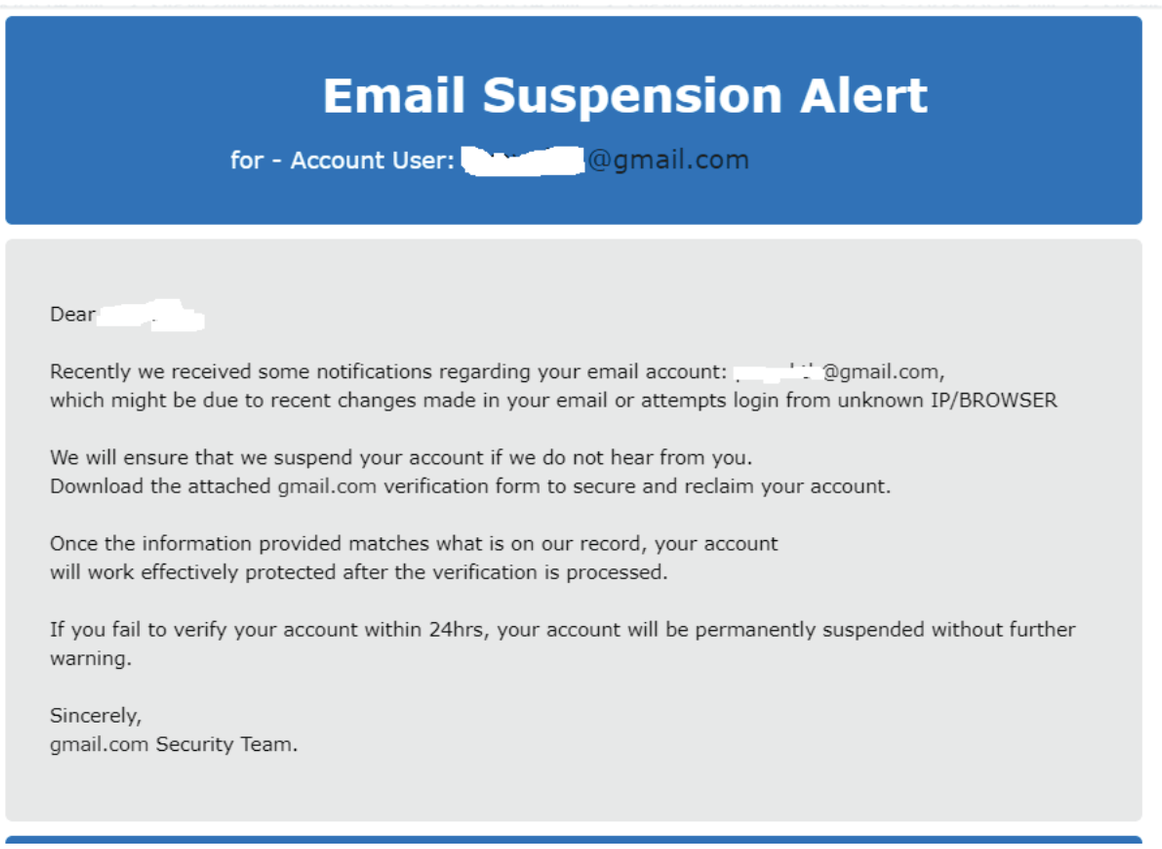
Given the above, I am hereby requesting you to download the attached update, read the contents and e-sign the same and share it back as a reply to this email. This will enable us to add you to a list of privileged support citizens who will receive immediate attention in case you contract the disease.

You will also get a free WHO NCOVID healthcare kit if you sign and share this document over the next 15 hours.

Expecting your cooperation in securing the world.

Greetings.

Tim Hardlev



Email Suspension Alert

for - Account User: [redacted]@gmail.com

Dear [redacted]

Recently we received some notifications regarding your email account: [redacted]@gmail.com,
which might be due to recent changes made in your email or attempts login from unknown IP/BROWSER

We will ensure that we suspend your account if we do not hear from you.
Download the attached gmail.com verification form to secure and reclaim your account.

Once the information provided matches what is on our record, your account
will work effectively protected after the verification is processed.

If you fail to verify your account within 24hrs, your account will be permanently suspended without further warning.

Sincerely,
gmail.com Security Team.

A phishing email intercepted by our threat research team

Devices that operate in and digital communications conducted in Unmonitored environments always pose a threat to enterprises. With many countries enforcing a lockdown, many enterprises had to make arrangements for employees to work from home. The sudden transition to a telework environment, decreased physical mobility and use of untested collaborative tools along with increased anxiety has created opportunities for hackers to exploit.

In addition, there are many employees working form home who are using a VPN to connect to the network environment. This creates a potential opening in the enterprise network through the unmonitored device operating in a network that is not protected by added layers of security.

The impact of such deterioration in the overall cybersecurity environment will not be known immediately as the gestation period for detecting such breaches is over 70 days.

Five things that changed last quarter:

- Increased threat surface with more employees working from home
- Rise in attempted fraud that preys on the anxieties stemming from the pandemic
- More DNS hijacking attacks targeting home routers: By modifying the DNS settings on the router, users are made to think that they have landed on a legitimate website. That is not the case as the page is served from a different IP address used to lure victims to share their personal information and user credentials
- Increase in malicious domains as reported by Interpol. Cybercriminals are creating thousands of fake websites every day. These sites are used to carry out spam campaigns, phishing, spreading malware or to compromise servers.
- Growing use of software-as-a-service (SaaS) and remote connectivity services that are cloud based. Attackers lure victims in order to collect credentials that allow them to access enterprise SaaS accounts and data that could be sold on the dark web or held to ransom.
- Rise in attacks carried out to deceive agencies involved in cybersecurity

These attacks are evolving and the hackers are shifting attention to newer targets every week. In the beginning of the year, the targets were oil and gas companies, manufacturing plants and large smart cities. As the pandemic showed up, healthcare institutions and welfare agencies were attacked. This followed attacks on government agencies coordinating relief work and then the hackers went after NGOs and supply chain start-ups that had received fresh funding.

The worrying trend here is the shifting tactics and targets. Hackers are not giving their targets any time to adapt and counter the growing threats.

Regional trends

North America
USA continues to be the most attacked nation in the world

Attacks on North America registered a rise in first quarter. High reconnaissance activity was registered across critical infrastructure, shipping, manufacturing and transportation sectors.

In all hackers launched all out attacks against a range of entities using modified malware. More instances of modified malware were seen this quarter than what was recorded last quarter.

Malware classes detected in the region

CLASS	PERCENTAGE DETECTION Q4, 2019)	PERCENTAGE DETECTION (Q1, 2020)
Crypto mining	11	14
Ransomware	19	22
Predatory	3	2
Defence-grade	2	7
Mission-based (uniquely engineered)	7	5
Modular malware	9	7
Reconnaissance	37	30
Others	12	13

Among the device classes in various sectors, devices connected with manufacturing registered the largest increase in attacks on them followed by healthcare, utilities and telematics. Video surveillance cameras remain the most targeted devices.

Attacks on Mexico and Canada also saw a minimal surge in the quarter.

Regional trends

Europe
Attacks on UK maintain their upward trajectory

Attacks on UK picked up in the first two months and then decline for a week before picking up again. Healthcare was the most attacked sector across whole of Europe. For some reason, hackers were also attacking non-traditional sectors like renewable energy farms. This might be a way of deceiving national cyber defense agencies and keeping them busy while they go after high value targets.

Poland, Ukraine, Spain and Germany (in that order) were the other countries in the top 5 as far as cyberattacks are concerned. Poland made its debut in the top 5 this riding on a wave of highly sophisticated attacks coming in from its immediate neighborhood targeted at critical infrastructure. Most of the cyberattacks were channeled against entities in the healthcare, financial services, defence, renewable energy and shipping sectors. Hackers were looking for vulnerabilities, gaps in defenses, OT projects in transition to IoT, remote connected assets and smart home devices for attacking.

The prevalence of high-grade malware possibly developed in state-supported labs and/or academic institutions is the highest in Europe. While in the first half of the last decade, the use of such

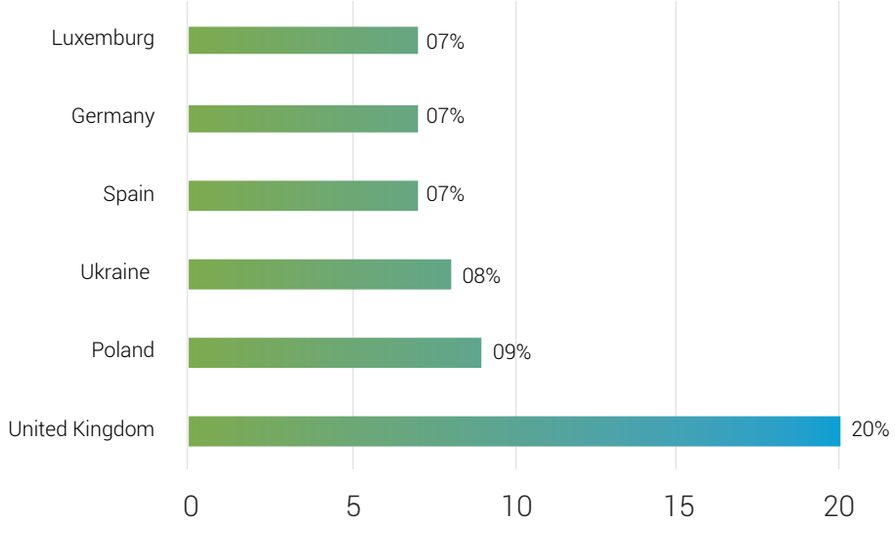
complex malware was restricted (even some nation states didn't posses such malware), today such malware and its variants are commonly detected across regions. What make the problem worse in Europe is the prevalence of bot nets that are distributing such malware through latent attacks on various establishments.

With the Covid-19 response strategies keeping many governments occupied, cybersecurity seems to have taken a back seat as collectively, Europe became the most targeted region in the world. Attacks on Poland alone rose by a whopping 79 percent this quarter.

Pattern of attacks on health-care

Attacks on healthcare institutions registered the biggest ever hike in this quarter. The attacks increased as the number of Covid-19 cases from countries like Spain, Italy and Germany increased in the month of March. In the past, most attacks were targeted against devices using legacy operating systems or unpatched firmware. But from March onwards, the attacks continued across all systems including patched ones running on updated software and firmware. This indicates that the intention was to try and manipulate the behavior of potential victims and cause a breach with help from an insider.

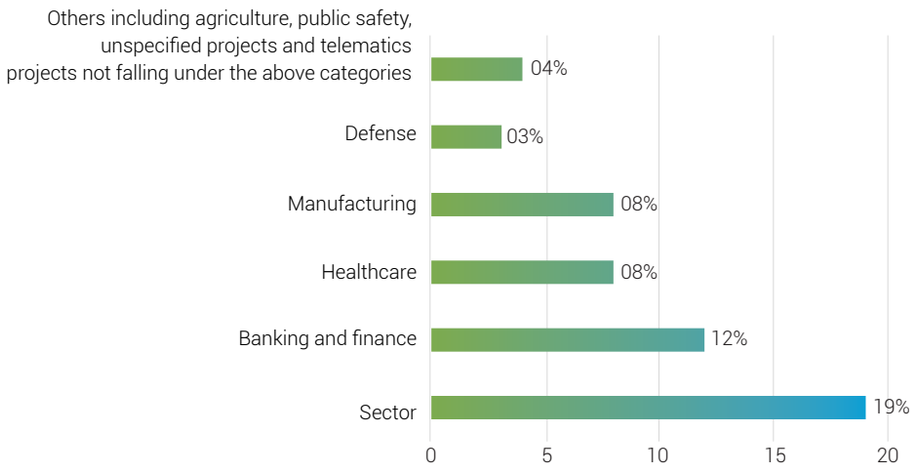
Most attacked countries



Regional trends | *Asia-Pacific*

Huge volumes of inbound attacks on China were the highlight of this quarter. Most of these attacks were connected to a group based in China's neighborhood and bear some degree of geo-political motivation. Almost all countries in the region witnessed a rise in cyberattacks with financial services and healthcare accounting for the bulk of the attacks followed by manufacturing and smart homes.

Increasing attacks on manufacturing



Attacks on healthcare institutions is inline with a trend we have seen globally. Routers for the first time replaced video surveillance camera's as the most attacked class of devices this quarter. This is despite cyberattacks on surveillance cameras registering a 7 percent increase.

Malware reported

Common ones include variants of Lockie, Mirai, Torii, Gafgyt/Lizkebab, Silex, Dingbat, Captainxolo, Shamoon, Trident, Actcraft, Mayhem, Wicked, OMG Mirai, ADB.Miner, DoubleDoor, Hide 'N Seek and many genetically new malware reported by other geographies. Our research indicates that many of these have been sourced from malware shops on the darknet and on social malware forums. Some of the variants of common malware represented a level three variation which means they were modified at least three times before being deployed to evade detection.

Over 2000 modular malware forms were also reported indicating increasing sophistication of attacks.

IP Obfuscation

Some of the samples we can across were doing port scans to detect exposed connected devices. The most common devices targeted were IP cameras. One of the samples we isolated was having access to a repository of default credentials for launching brute force attacks. The inbound attacks had a common characteristic which is IP obfuscation. We have observed patterns of IP spoofing with a clear intent to hide the geography of origin of the command and control network behind these attacks. The clear preference for manufacturing and other complex IoT deployments among these botnets is one of the reasons behind this assumption.

Persistence

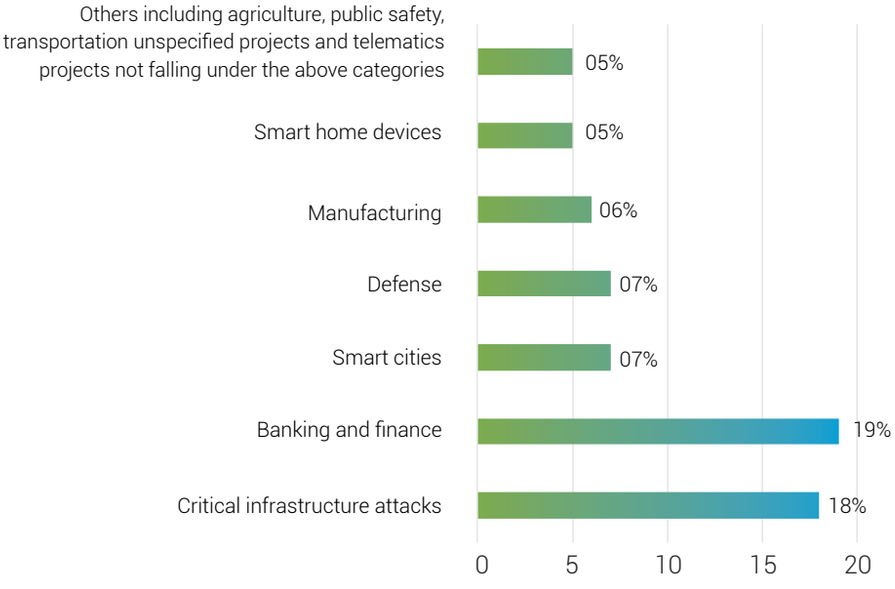
We have seen malware that has been lurking in some projects since mid-last quarter. The level of persistence varies between sectors and in some instances depending on the time of the year and the scale of the project as well. The least number of days of persistence has been seen in case of PoC projects while attacks on industrial IoT persist for the maximum length of days.

Length of persistence also depends on the response mechanisms being tested as also a need to evade detection. Highest levels of persistence were seen in the smart cities sector while agriculture reported the lowest at less than 100 days.

Regional trends | *India*

India was in the top 5 most attacked countries in the region throughout the quarter. The country attracted attacks of relatively high quality (as compared to other regions and last year). Critical infrastructure was attacked the most followed by sectors such as banking, defense and manufacturing.

Increasing attacks on key sectors



Most of the inbound attacks on India were coming from North Korea. The huge spike in attacks on banking and financial services could be attributed to attackers based in North Korea. This is largely in line with the findings of various analysts who have analyzed the increasing capabilities of North Korean hacker groups as also the increased internet bandwidth now available to them thanks to the opening of a second internet gateway in the country.

There are also reports of North Korean hackers being hired by other cybercriminals for carrying out specific attacks. Financial institutions across South East Asia. Cosmos Bank based in Pune, India lost nearly 12 million USD in a coordinated attacked traced to North Korea. The well-known Bangladesh Central Bank hacking was also traced back to a hacker in North Korea.

From attacking financial firms to siphon money to attacking nuclear power plants to getting information on various operational aspects and targeting diplomatic cables, North Korean hackers are getting more brazen and unpredictable. Financial institutions remain high on their list of targets.

Regional trends | *Middle East and Africa*

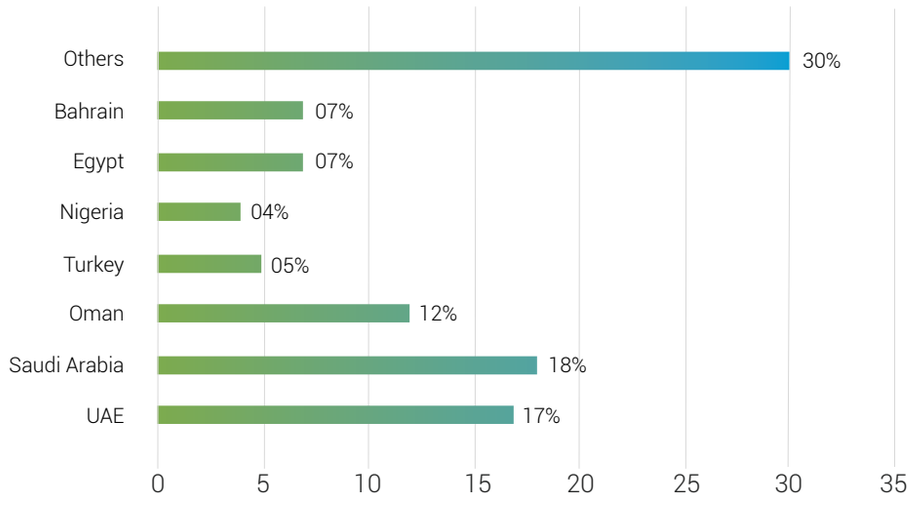
The last year saw a rise in cyberattacks on various states in the Middle East. UAE, Saudi Arabia, Oman, Jordan, and Turkey attracted the greatest number of in-bound cyberattacks. While the attack patterns remained more or less same, several of new attacks were designed to exploit the anxiety and confusion generated by the Covid-19 pandemic.

While the number of attacks registered during the quarter dipped by 3 percent, the degree of sophistication of malware and tactics improved during this period. Attacks on financial, government, energy, chemical, and telecommunications institutions continued in the quarter. Incident response strategies will be extensively tested in the days to come as the attacks rise and the probability of a breach increases.

Oil and gas and power utilities were the only sectors that witnessed a surge in cyberattacks. Such attacks are increasing in frequency and sophistication and the hackers are using newer forms of existing malware and new malware to beat cyber defense systems. Social engineering is also being used extensively in sectors such as manufacturing and financial services.

As exploratory and refining operations in the oil and has sector in the region slowed down in April, many targeted scams surfaced. Mails with messages around Covid-19 vaccines (non-existent) and personal protection equipment were being circulated across the region to lure potential victims. These were designed to get employees to reveal their credentials while they were working from home and accessing critical systems using VPN.

Percentage Geographical distribution (inbound cyberattacks)



Global forecast for Q2 2020

Here are some of the key trends that will shape the world of cybersecurity in Q2 2020

- Covid-19 themed attacks to continue
- Financial services, healthcare, smart cities and retail remain high on the list of hacker targets
- As the lock-down eases across regions, employees will return to offices and this will give the infected devices a chance to connect with larger and core networks. This could lead to more data breaches or even network security issues
- Government agencies need to be on high alert till the end of this year
- Enterprises need will experience DDoS attacks
- Deceptive attacks on not so valuable targets or those targets that are critical but are of low value to hackers will continue

Advisory

- It is advisable to conduct additional security checks and scans before such devices are allowed to connect to enterprise networks
- We advise enterprises especially financial institutions and healthcare providers to remain on high alert for the next 180 days
- Enterprises should conduct a device discovery exercise to locate and tag all devices that are part of their surveillance systems

Research Methodology

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these attributes:

01 Are landing centers for submarine cables

02 Are internet traffic hotspots

03 House multiple IoT projects with a high number of connected endpoints

04 House multiple connected critical infrastructure projects

05 Have academic and research centers focusing on IoT

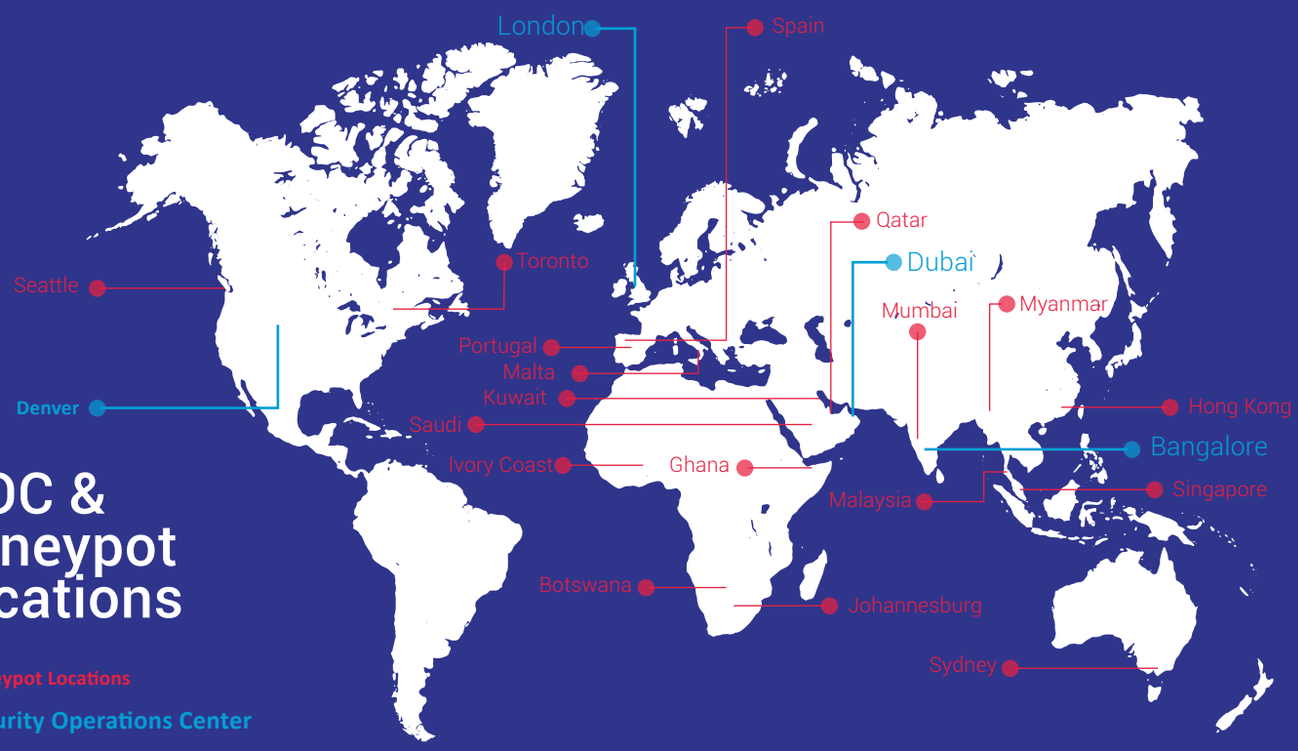
06 Have the potential to host multiple IoT projects across domains in the future

Over 6 million attacks a day registered across this network of individual honeypots are studied, analyzed, categorized and marked according to a threat rank index, a priority assessment framework, that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. Devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.

Key findings are published by us every quarter to enable businesses, decision-makers, academicians, students, CISOs and others interested in cybersecurity gain a comprehensive understanding of the evolving threat environment that envelops IoT deployments and derive appropriate responses prevent, contain and dissuade such attacks.

SUBEX

www.subex.com



ISOC & Honeypot Locations

- Honeypot Locations
- Security Operations Center

- Subex is the market leader in products Security and Fraud Management market, with over 180+ customers in total
- Recognized as the IoT security platform of the year 2018 by Compass Intelligence
- Subex is the Number 1 provider globally of Fraud Management and Security solutions in the Telecom Space, according to a Gartner report published in March 2016
- Subex runs the world's most comprehensive IoT and ICS focused honeypots of over 400 architectures across 62 locations globally.
- +700 Experts in Security/Fraud and other programs with assets, skills and innovative methods to ensure results for the operator
- Publicly listed in the National Stock Exchange (India) and Bombay Stock Exchange

Subex Limited

RMZ Ecoworld,
Devarabisanahalli,
Outer Ring Road,
Bangalore - 560103 India

Tel: +91 80 6659 8700
Fax: +91 80 6696 3333

Subex, Inc

12303 Airport Way,
Bldg. 1, Ste. 390,
Broomfield, CO 80021

Tel : +1 303 301 6200
Fax : +1 303 301 6201

Subex (UK) Ltd

1st Floor, Rama
17 St Ann's Road,
Harrow, Middlesex,
HA1 1JU

Tel: +44 0207 8265300
Fax: +44 0207 8265352

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Tel: +65 6338 1218
Fax: +65 6338 1216

For more information write to info@subex.com

Regional offices: Dubai | Ipswich