Q1 2020 Summary and Threat Assessment

Ahead of the Threat Curve

www.ClearSkysec.com - info@ClearSkysec.com

Content

Introduction

We mark the outbreak of the COVID-19 virus as a systematic change for most businesses around the world. The immense pressure felt by many companies and organizations has the potential of evolving into "The perfect storm"[1] in terms of ripe conditions for cyber-attacks, combining the following elements:

- Increased attack surface of organizations due to opening new remote access to core systems for workers and vendors.
- Mounting motivations for theft, sabotage or fraud a result of increased economic pressure.
- Bypassing or lowering security controls for user credentials and privilege management systems in order to meet business demands and remote work.
- Risk of diminishing abilities of security teams as a result of increased workload and decrease in available work power.
- HR shortage and objective difficulties of the new remote work model.

It appears that many businesses will require a lengthy recuperation period after the lockdown period ends. The short- and long-term repercussions are still unknown, and it is unclear whether additional outbreak waves will arrive, committing us to further lockdowns, specifically in the third fourth quarter of the year, when a new wave of winter-time outbreak is expected to occur.

Within this document we focus on summarizing Q1 strictly from the cybersecurity perspective and analyzing the alterations to existing cyber threats following the Covid-19 outbreak, alongside new emerging threats, in order to assist you in preparations and decision making in the cyber arena.

[1] https://en.wikipedia.org/wiki/Perfect_storm

Significant Cyber Events

Several significant events have influenced activity in cyber space vis-à-vis organizations in Q1:

Global Events:

- **The outbreak of the Coronavirus (COVID-19)** has initiated a dramatic change the way organizations operate and expose them to new set of new risks and future attacks[2]. The Covid-19 outbreak was matched by a criminal one, as we observed a sharp rise in the number of cyber-attacks by cybercrime groups around the globe exploiting the outbreak in numerous ways.
- **Numerous ransomware attacks** targeting large companies, government organizations, local authorities, as well as hospitals and medical establishments. These attacks are bolstered by exploiting the current pandemic. The result was a major disruption in service for an average time of two weeks.
- **Exposing and thwarting attack infrastructure of APT groups like "Lazarus" from North-Korea,** which specializes in attacking the financial sector, nearly bringing the group to a complete shutdown of operations[3] and decreased the number of North-Korean attacks.
- **Widescale operations to take down botnets.** The most impressive one was headed by Microsoft that disrupted one of the largest international spam botnets, **Necurs[4].** The operation brought a relative decrease in the volume of spam sent globally.
- **Focused ransomware attacks on financial companies. The most disruptive one was a ransomware attack targeting Travelex, one the world's leading foreign exchange and credit payments companies,** which did not recover from this attack for over a month[5], regardless of paying the ransom.
- **Modus operandi change in cybercrime attacks. An example is The Russian criminal group "Silence", which specializes in breaking into bank assets (specifically ATMs), that started attacking banks in Africa -** a fact that shows us that cyber-criminal groups are invading new territories.

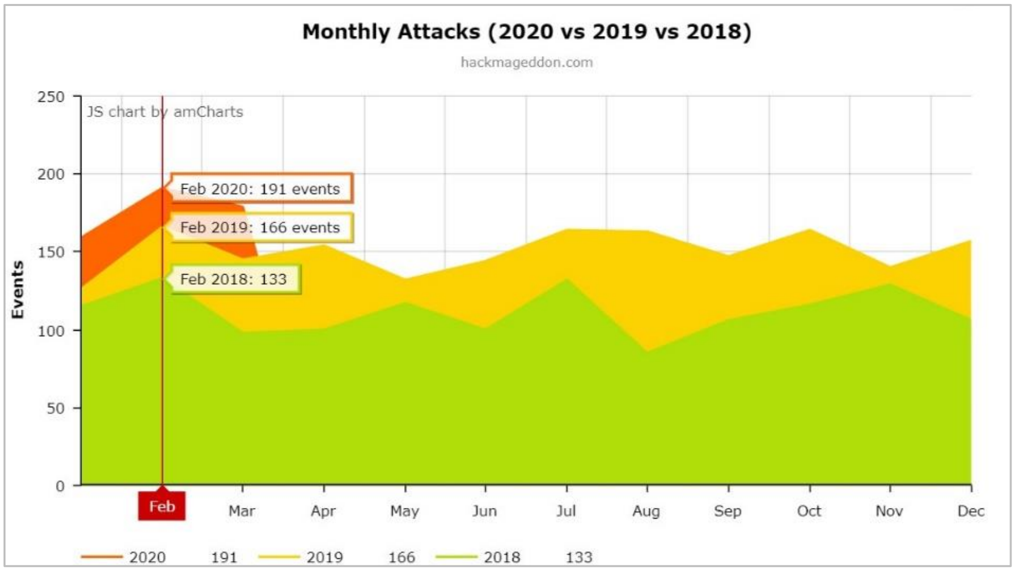
Regional related cyber events

- **The Killing of the Iranian Quds Force's commander** – Qassem Soleimani – has ushered a sharp escalation of the Iranian cyber threats in the region. To our

[2] https://www.us-cert.gov/ncas/alerts/aa20-099a
[3] https://www.us-cert.gov/northkorea
[4] https://www.wired.com/story/microsoft-necurs-botnet-takedown/
[5] https://www.zdnet.com/article/two-weeks-after-ransomware-attack-travelex-says-some-systems-are-now-back-online/

estimation, Israeli deterrence and sufficient monitoring capabilities in cyber space had prevented destructive malware attacks targeting the country[6].

- **Exposing a wide-spread Iranian "Fox Kitten" infrastructure** – which was exploiting vulnerabilities in VPN systems and infiltrated networks of many companies in Israel and several other countries using this method[7].
- **Destructive malware attacks – an Iranian attack against the Bahraini national oil company, BAPCO,** that exploited vulnerabilities in Pulse Secure's VPN to infect the company with a destructive wiper malware[8].
- **Paybox's (Israel Discount Bank payment application) database theft[9].**
- **The Israeli election data base was leaked to darknet through the "Elector" program[10].**
- **Large number of ransomware attacks targeting companies of medium and large scales (we estimate that a few dozen companies were affected).**
- **Continuous cyber-attacks and fraud attempts targeting crypto exchanges.**
- **A rise in the volume of phishing attempts aiming to steal credentials from bank and credit company customers in Israel.**



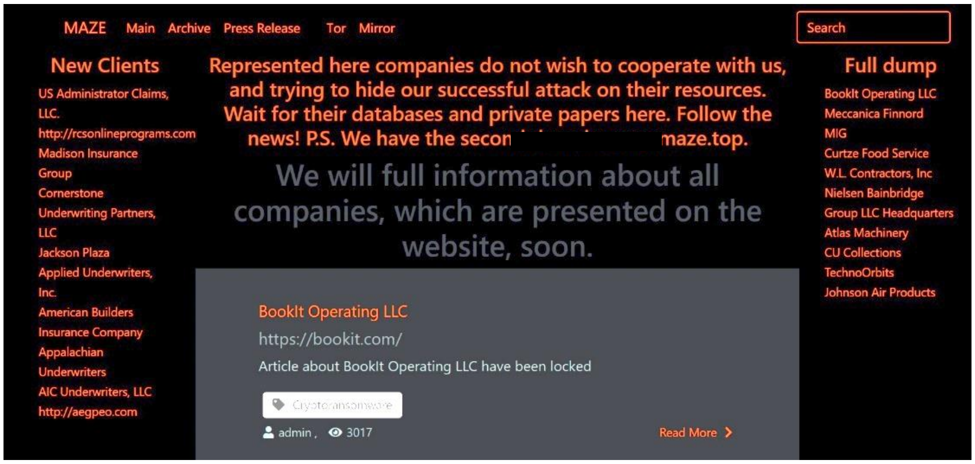
[6] https://www.buzzfeednews.com/article/meghara/qassem-soleimani-iran-cyber-attacks
[7] https://www.clearskysec.com/fox-kitten/
[8] https://www.cpomagazine.com/cyber-security/data-wiper-malware-attack-on-bahrains-national-oil-company-linked-to-iran-part-of-an-ongoing-pattern/
[9] https://tech.walla.co.il/item/3338367
[10] https://www.calcalist.co.il/internet/articles/0,7340,L-3791595,00.html

Significant and Unique Trends in Q1

Global Cyber Trends

- **A noticeable increase in the number of ransomware attacks** focusing on organizations and large companies, causing severe damage to their ability to operate. We see these attacks as the **most significant cyber threat** that exists for organizations and companies. This trend has been growing steadily since 2018, and since the outbreak of the coronavirus pandemic it has increased both in volume and level of sophistication, in addition to another extortion element, described in the next bullet.
- **An increase in the number of ransomware groups that threaten to publish sensitive information stolen from their victims in order to enforce the blackmail**

  A large quantity of Russian cybercrime organizations began to use their attained accessibility to the victim's network to force the relevant company to comply with the ransom. We observed ransomware operators threatening both publicly and discretely to not only let the affected systems remain shut down, but to release sensitive information that was gathered during infection phase. A number of groups have enacted these steps, with "Maze" standing out by publishing their victim's names and some of the gathered information on a public website in order to "encourage" them to pay the ransom. Here is the group's "home page":



New Clients

US Administrator Claims, LLC.
http://rcsonlineprograms.com
Madison Insurance Group
Cornerstone Underwriting Partners, LLC
Jackson Plaza
Applied Underwriters, Inc.
American Builders Insurance Company
Appalachian Underwriters
AIC Underwriters, LLC
http://aegpeo.com

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the secon[redacted]maze.top.

We will full information about all companies, which are presented on the website, soon.

BookIt Operating LLC
https://bookit.com/
Article about BookIt Operating LLC have been locked

Full dump

BookIt Operating LLC
Meccanica Finnord
MIG
Curtze Food Service
W.L. Contractors, Inc
Nielsen Bainbridge
Group LLC Headquarters
Atlas Machinery
CU Collections
TechnoOrbits
Johnson Air Products

Pictured: Maze's home page

- **Widespread use of the Covid-19 pandemic by all attackers** in the cyber domain. Including attacks targeting remote access systems and companies, using tailored phishing and exploiting the gaps in cyber defense that slowly widened as organizational exposure to remote access increased.
- **The rising threat to the remote access array in general and VPN systems specifically**

The trending transfer to remote-access work in times of the coronavirus pandemic increases the possibility for criminal groups and APTs abusing this medium in more encompassing and significant ways for their attacks.

- **Increase of use of cyberspace to advance political and\or financial motives**

  As this trend is less relevant to the business sector, we have seen a number of (mainly Asian) countries using their espionage units for financial and industrial espionage, sanctions evasion, and other financial gains. As part of this trend some countries, including the US at the helm, have begun to use the cyberspace to react to and directly counteract these attempts. US government officials, for instance, published indicators and research results regarding tools associated with the North-Korean "Lazarus" group, as well as attack tools belonging to the Russian FSB service.

Regional Trends

- A significant increase in the number of ransomware attacks focused on organizations and companies in Israel, including threats to publish information and damage the operational ability of these companies. The tools used by the attackers and their methods of operation are continuously becoming more sophisticated. From the information we have received we gather that most big businesses in Israel chose to restore backups and not paying the ransom.
- An increasing number of phishing attacks in Israel, targeting both employees and regular citizens, impersonating financial institutions, communication and infrastructure companies, and governmental elements. Unlike the ransomware attacks, at this point it seems that the attackers lack sophistication and that the attack tools are easy to locate.
- **A decrease in the volume of attacks emanating from Iran APT groups at the beginning of the Q1**. We estimate that the decrease is caused by two reasons: one is the termination of their central attack infrastructure (redeploying at that scale is a matter of 3-6 months), and the other is the Corona outbreak in Iran, which we asses has interrupted attack attempts originating in governmental and security organizations. Throughout the beginning of Q2 we observed signs of a resurgence in their activity, slowly returning to familiar attack patterns.

A Systematic Change – The Corona Outbreak and its Potential Influences on Cyber Space in 2020

Fundamental operational changes for companies and organizations

In this section we present several topics that may create and fuel "The perfect cyber storm". We estimate that the length of the crisis, the number of outbreak waves, and the way we exit it, will all greatly influence the probability and magnitude of future cyber-attacks.

A. Changes to hiring methods for all organizations

- Continuously downsizing the scope of employment in most businesses and shutting down unessential computing projects due to current and future decreased income, alongside downsizing in many commerce sectors.
- An accelerated shift to online work environments.
- Downsizing physical presence in offices and branches to comply with social distancing and avoid employees getting infected.
- Engaging in fields previously considered to be impossible to conduct remotely, also due to security reasons, through remote access.
- Expanding the use of untrained human resources, to take over work generated by infection, or downsizing.
- A large number of employees in the market are experiencing a significant decrease in income (unpaid vacation) and perhaps are even being laid off.

B. Hiring methods in the coming months

- Management requiring employees to conserve core business operations even when employees experience difficulties to arrive at the workplace through remote access.
- Managing employees remotely and in-office simultaneously adds difficulty to routine management.
- Management requirements to return to activity as soon as possible in order to increase diminished profits.
- A significant increase in the percent of employees who receive access to remote company computing, operation, and control systems.
- In case of an outbreak amongst employees and lack of experienced employees to operate systems, we estimate that companies will expand privileges and authorities to existing employees while recruiting less experienced workers for system maintenance, harming its level of security.

- Remote employment will decrease the ability to perform security updates in a concentrated manner both for the computing centers and the remote stations.
- Laying off employees will have an increased risk of actions driven by revenge, heightened by privileges and access to sensitive information.

C. Operational array – Core It and applications systems

- Due to the necessity of distancing and isolating employees from the company's offices, laptops and other computing devices are being handed to employees on a massive scale, in order to enable them to work remotely.
- The isolation requirements further urge enabling remote access to core systems, **including systems that were not previously remotely accessible**. Clearances are being given and sensitive operations are being performed remotely that were previously only possible while physically being present in front of the systems.
- Segmentation and network separation may be harmed by the need to allow access to all systems remotely.
- Due to isolation requirements, new online systems are activated delivering existing security and fraud limitations (for instance increasing online withdrawal ceilings or depositing large checks), suggesting we may see an increase in fraud numbers.
- The technical array is required to supply remote support for employees using company computers at home.
- The technical array is required to remotely handle operational malfunctions in the company's computing centers.
- The transfer to cloud services will be expediated and remote access may expose companies to cyber-attacks targeting their cloud services.
- **The transfer to services being supplied to customers online will be accelerated, even at the expanse of necessary security measures needed for the company's normal activity**. This acceleration may severely harm security levels. Business demands will ultimately triumph over security demands.
- Quick and alternative solutions to existing systems do not receive the control and supervision coverage usually applied.

D. Company offices

- Due to employees being distant, different areas in offices and company branches are being **abandoned** and are not as supervised by company employees as before. Attackers accessing these areas may attain physical access to the network, anonymously.

- Physically abandoned servers may enable direct access to the company's systems.
- There has been a decrease in the ability to identify and avoid fraud by physically interacting in order to conduct business.

E. Company customers

- Service customers will perform many more online activities from their home computers or cellular devices, avoiding arriving at service branches as possible.
- Due to the fact that a large number of clients will perform actions remotely, sometimes for the first time, systems that analyze purchases to prevent fraud will manufacture a lot of false positives, making actual detection more difficult.
- There is a risk that focused phishing attacks will be more effective against clients that are experiencing financial difficulties (for instance impersonating governments and requesting information in order to receive a grant as a phishing pattern).
- Due to the general social atmosphere, any service malfunction may generate unbalanced opinions amongst the public, which is much more present online than usual, leading the company's reputation being harmed.
- A certain percent of customers will experience financial difficulties and may resort to anything, including theft in every possible way.

F. Company suppliers

- Suppliers will transfer to remote work as well, including working with company systems.
- Company suppliers will also use established cloud and remote access services that may expose those services to cyber-attacks.
- Supply times will lengthen, both due to import delays and lowered physical presence in the supplier's offices.
- Software supplier will require more time to patch vulnerabilities with their products due to low employee availability.
- There is a possibility that the number of "supply chain" attacks will increase due to lessened security measure enacted following the transfer to remote access.

Possible changes to the activity of APT groups

A. Superpowers and countries (decrease in attacks)

- Some of the countries who engage in cyber-attacks experienced a massive outbreak of the Covid-19 pandemic. We estimate this will entail a further decrease in their activities in the following months. One of the biggest victims of Covid-19 in Q1 in our region is Iran, we observed a decrease in Iranian attacks in this quarter.
- Russia is continuing to do anything within its power to damage the western economy and democracies, with signs of a consciousness manipulation project designed to destabilize western democracies, specifically the US, being executed by it.
- China has resumed to near-normal activity, bolstering their campaigns with consciousness psychological campaigns as well.

B. Terrorist organizations (decrease in attacks)

- Some of the terrorist organizations that act within the cyber space are also influenced by the outbreak (Hezbollah for example), resulted in decrease of activity. we therefore estimate that attacks by these organizations will continue to decrease in the next six months, Hamas in Gaza included.

C. Cyber-crime organizations (a sharp increase of both the volume and sophistication of attacks)

- We estimate that the number of cybercrime attacks will significantly increase in the coming quarter. These organizations understand that the attack surface of companies has expanded. With companies more exposed we expect more attacks attempting to extort or steal money and information. During the passing few weeks we identified an exponential growth of the number of phishing attempts, domain establishments, extortion and ransomware attacks, and company impersonation events.

D. Lone hackers (a sharp increase in the volume of attacks)

- We estimate that the number of lone hacker attacks will increase significantly in the coming quarter. Hackers are homebound, are missing income, and can’t arrive at their workplace. The result is – additional free time to plan and execute cyber-attacks.
- We foresee an increase in the volume of demonstrative or hacktivist activity, seeing as many people will be financially harmed by the pandemic and will protest to any potentially helpful element.

Summarizing the influence of events over the threat reference

A. In continuation to the factors mentioned above, we foresee an added risk for significant cyber-attacks in the next 6 months due to the following reasons:

- It will be easier to attack and exploit vulnerabilities with the company’s new online array.
- New attacks will be executed targeting remote communication channels (various VPNs)
- Remote workstations will be attacked due to a lessened ability to supervise them.
- The company will have a lessened ability to update the company’s systems in a short time.
- The number of attacks exploiting the pandemic to bolster social engineering and fraud will increase significantly.
- We will see cyber-attacks that will be executed by abusing the relative abandonment of offices.
- The company’s suppliers similarly transferring to remote access will further increase the risk of third-party attacks, and exposure to third-party software that may not be properly maintained.
- Company customers will be more exposed to online attacks aiming to steal their credentials and currency.
- A lack of income will ease the recruitment of money mules to aid in company fraud.

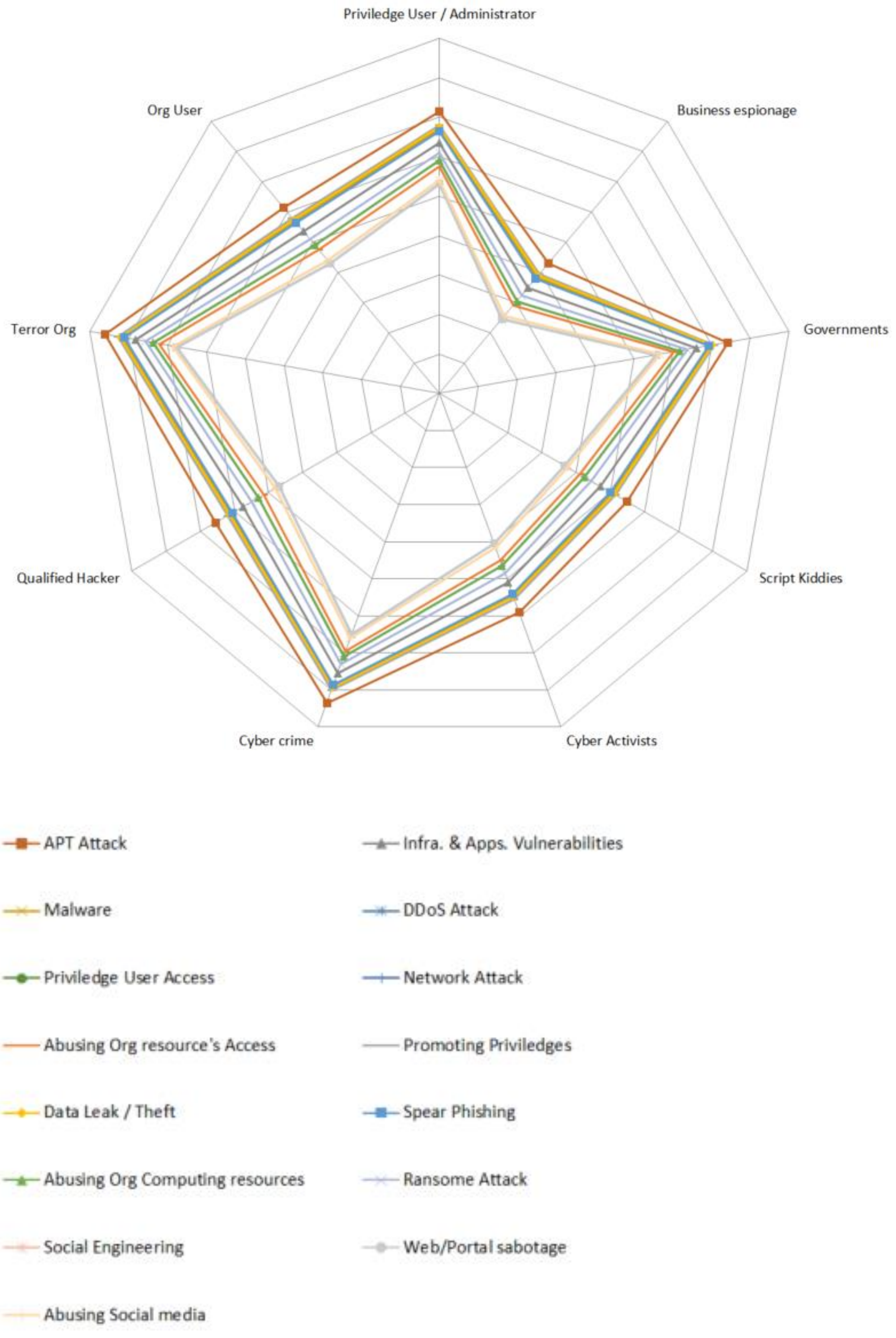
B. A graph presenting the influence of the Coronavirus outbreak

The graph is a preliminary layout based on several parameters examined to represent the cyber threat. You are welcome to receive additional information upon request. At this point the graph entails:

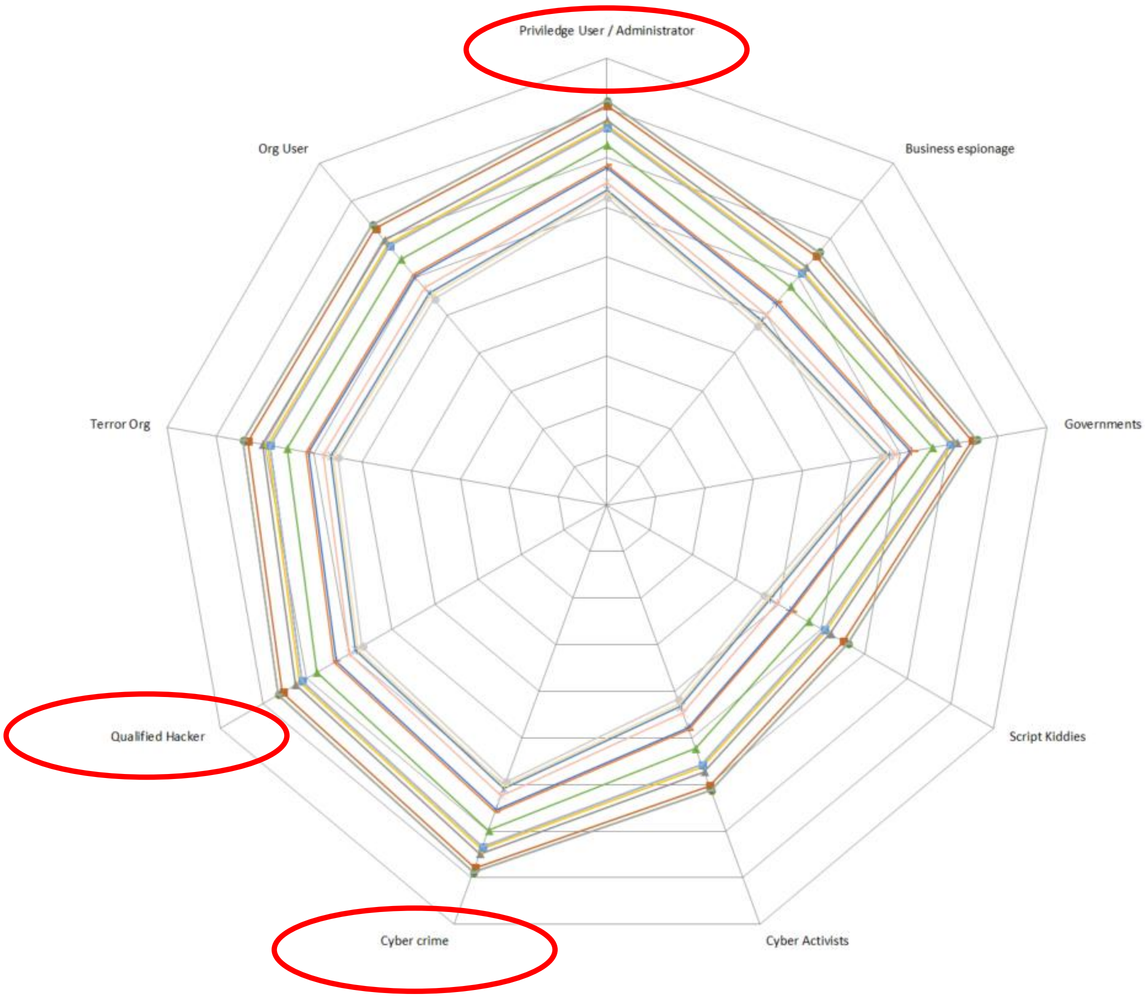
- Attack tools (from social networks to vulnerability exploitations)
- Privilege exploitation (from basic users to admin privileges)
- Kinds of attack (from ransomware to intelligence collection)

The results are thusly presented by referencing the threat by type of attacker (internal, lone hacker, criminal organizations, terrorist elements, or APTs) and suggest an increased risk of internal attacks caused by employees having escalated credentials, alongside an increase in attacks by criminal groups and lone hackers.

A graph mapping the threat reference according to attacker type, for financial organizations **before** the COVID-19 outbreak



The threat reference graph for various organizations **after** the COVID-19 outbreak (notable differences marked in red)


Priviledge User / Administrator
Business espionage
Governments
Script Kiddies
Cyber Activists
Cyber crime
Qualified Hacker
Terror Org
Org User