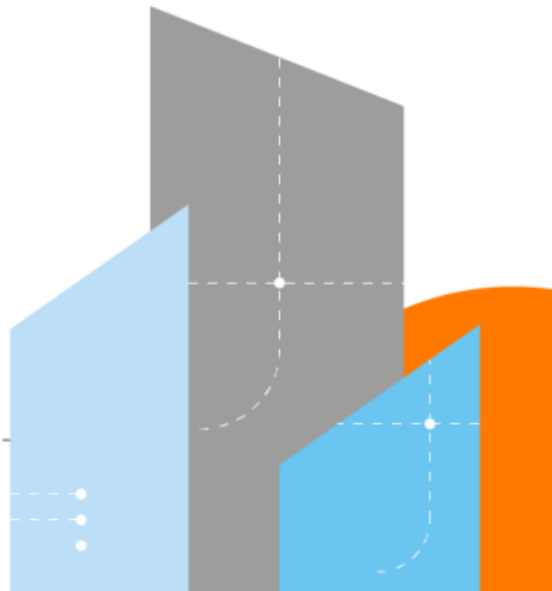
Orange
Cyberdefense

Security Intelligence

Monthly Report

May 2022



CONTENTS

INTRODUCTION

Welcome to the May monthly report. As we stated last month, some of the sections of the report have had to be deprecated due to changes in service delivery and data location. Work is still going on in the background however to introduce new sections to the report and to restore some of the statistical analysis we previously provided, there is no timeframe for when this will be available yet though.

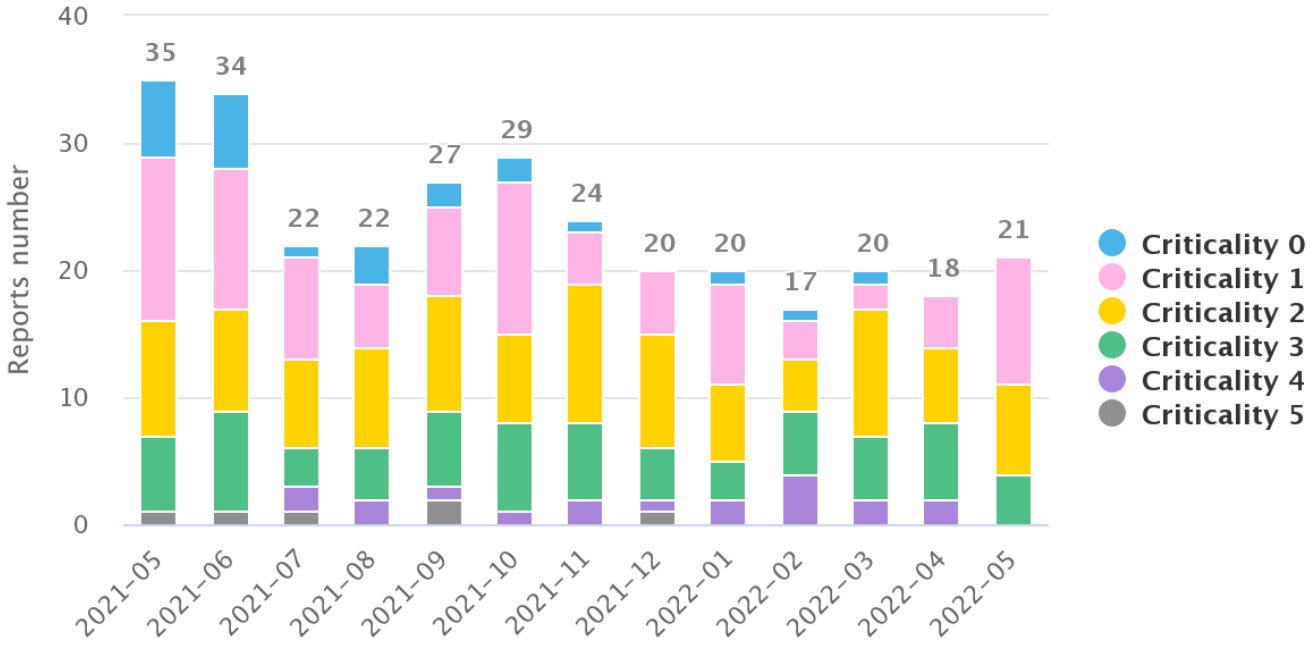
Last month in one of our Editor's Notes sections we commented on how difficult it seemed to be to disrupt the activities of the Conti cyber extortion (Cy-X) gang. Well, the truth of that particular commentary lasted less than a week, with Conti themselves deciding to do what law enforcement hadn't been able to. They supposedly have officially shut down their operations and disbanded, with their members joining smaller ransomware operations. Despite this announcement their leak site continued to operate, and is still online now, with new victims still being added. Although the last victim at the time of writing looks to have been published on June 7.

At a glance

The free access to our World Watch service, which all customers received due to the change in the service, has now expired. If you still wish to receive the advisories, please contact your Service Delivery Manager.

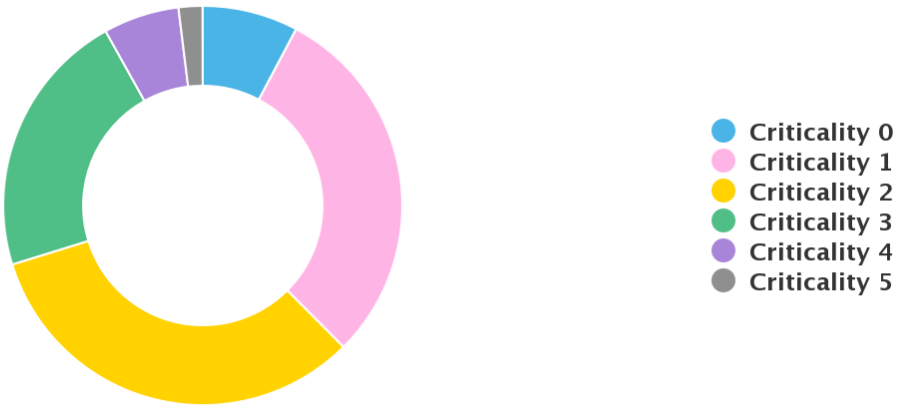
World Watch Review May 2022

The Orange Cyberdefense CERT published a total of 21 new World Watch advisories during May 2022, along with a further 18 updates being added to previously published advisories. The number of new advisories published in May is slightly above the average monthly amount so far year to date.



Breakdown of Published Advisories Previous 12 Months

The Criticality allocated to the May advisories stayed quite low with only levels 1, 2 & 3 represented, although as can be seen in the 12-month breakdown below this is in line with what we would expect as these three levels account for 84% of the previous 12 month's advisories.



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As noted above the advisories this month were all given criticality ratings of low or medium when initially published. These ratings are based on our CERT's assessment of the risk and threat levels associated with the subject of the advisory at the time of publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially be medium, if say there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase our criticality level as required if circumstances should change. Some advisories of note this month are:

SIG-613853 - New 0-day vulnerability 'Follina' in Microsoft Office recently exploited by malicious actors

- First reported by Japanese security team Nao Sec, this 0-day vulnerability allows attackers to perform a multi-stage attack to retrieve malicious code without being detected. The flaw was dubbed "Follina" by researcher Kevin Beaumont because of the maldoc sample that refers to 0438, which is the area code for Follina, Italy. The sample that uses this vulnerability was uploaded to VirusTotal from an IP address in Belarus. There is also another sample available on our Datalake platform that has a similar behavior.

SIG-609179 - F5 BIG-IP pre-auth RCE vulnerability exploited in the wild

- On May 4, 2022, security vendor F5 released a security advisory to recommend to their customers to update their products with new patches. Among these patches, one concerns a critical vulnerability that is tracked as CVE-2022-1388. This vulnerability exists because it is possible to make undisclosed requests to bypass iControl REST authentication, enabling an unauthenticated attacker with network access to the BIG-IP system via the management port and/or clean IP addresses to execute arbitrary system commands, create or delete files or disable services. F5 announced that there is no data plane exposure and that it is only a control plane issue.

SIG-608337 - New espionage APT avoids detection with QuietExit backdoor

- According to Mandiant's article, UNC3524 has been heavily targeting emails of employees working on corporate development, mergers and acquisitions, and large corporate transactions, possibly suggesting financial motivations. But as the researchers note, the group has also been able to remain undetected for a longer time than the average, which eventually reveals espionage intents. Indeed, while initial access methods remain unknown as of now, some of the intrusions conducted by UNC3524 avoided detection for at least 18 months thanks to a novel backdoor tracked as QUIETEXIT. The latter was notably deployed into the victim environment's blind spots: servers running uncommon versions of Linux or trusted network appliances which do not support security tools (such as anti-virus or endpoint protection) like wireless access point controllers, SAN arrays, and load balancers…

SIG-613535 - Exploit released for VMware critical authentication bypass vulnerability

- On May 18, VMware released security updates addressing vulnerabilities CVE-2022-22972 and CVE-2022-22973 that affect multiple VMware products, including Workspace ONE Access. In particular, CVE-2022-22972 is a critical authentication bypass vulnerability with a CVSS v3

score of 9.8. By exploiting this vulnerability, a malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate.

Editor's Notes (Beta)

This section is relatively new and was introduced in the January 2022 monthly report. Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.


Carl

Sanctioned By Association

It came as somewhat as a shock when, on the 6th of June, the LockBit Cy-X group announced on their leak site that they had breached the cybersecurity firm Mandiant and that they would be releasing the 356,841 files they claimed to have stolen. Mandiant for their part said they could find no evidence of any breach and they would monitor the situation, whilst the leak page LockBit had allocated to Mandiant remained suspiciously empty of any of the alleged stolen data.

As it soon became apparent there was a little more to this than initially met the eye. A few days prior to LockBits claim, Mandiant had published research regarding attempts by the group known as Evil Corp to change tactics in order to bypass sanctions originally imposed on them in December 2019 by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). The Mandiant research suggests that the Evil Corp group were moving away from using their own specific ransomware variants, most recently HADES, which made it easy to identify the group and therefore resulted in organisations refusing to pay because of the sanctions. Instead Mandiant reported that the group had instead begun using the LockBit Ransomware as a Service (RaaS) to conduct their operations. This meant that they could essentially hide among the other LockBit affiliates thus hindering attempts at attribution in order to evade sanctions and therefore get paid.

So, this then brings us back to the alleged breach of Mandiant by LockBit. When the stolen "files" were released, it turned out to be nothing more than a fairly farcical PR attempt by LockBit to distance themselves from Evil Corp, see screenshot below. It appears they took offence at Mandiant's report linking the two groups together and didn't want to be inadvertently sanctioned by association resulting in victims no longer agreeing to pay them….

> I was very surprised to read the news on Twitter from the yellow press.
> mandiant.com are not professional. Any scripts and tools for attacks, are
> publicly available and can be used by any hacker on the planet, most of the
> attack methods are on the forums, github and google, the fact that someone
> uses similar tools can not be proof that the attack is done by the same person.
>
> Foxconn Corporation's protection is completely absent, the admin domain was
> obtained by the oldest zerologon vulnerability. The affiliate who scrambled
> the Foxconn network works with very small companies and takes very small ransoms.
> The targets being attacked are mostly from third countries that very rarely pay.
>
> Just because FoxConn will be attacked by every ransomware affiliate in the world
> does not mean that Maxim Yakubets is hiding behind their brands. He has his own
> personal affiliate program, which is available to a narrow circle of high class
> professionals, I think the FBI agents know its name. I will not disclose the name
> of Maxim Yakubets affiliate program for ethical reasons, try to guess it yourself.
>
> Our group has nothing to do with Evil Corp. We are real underground darknet hackers,
> we have nothing to do with politics or special services like FSB, FBI and so on.
>
> We are a multinational group, our partner program includes not only Russians
> but also Americans, Chinese, Iranians, Ukrainians, and many other nations.
>
> Below you can download the proof of my words.

Charl

Cyber Extortion victimology shifting – who's next?

We've been studying trends in Cy-X (double extortion) ransomware attacks for over two years now, since January 2020. The data clearly shows that most victims (around 50%) are headquartered in the USA. This is followed by companies in Canada and United Kingdom, followed in turn by the bigger central European countries like Germany, France, Italy and Spain.

Our industry likes to speculate on the 'targeting' strategies of these cyber criminals. But our hypothesis is that the trends we see in victimology are the function a 'scattershot' approach to compromising businesses, which emerges in part from the fact that the crime of compromising victim computer systems and the subsequent crime of stealing and encrypting data and extorting the victim are frequently perpetrated by different groups.

In other words, businesses are compromised more or less randomly by one group, and those compromises are passed on to a different group that then selects which victims to extort for ransom. Any apparent 'target selection' that we observe in the victimology data is therefore the function of decisions that are made *after* the technical compromise has already occurred.

This excerpt from the leaked internal chats of the infamous Conti group, shows the two members of the group deliberating about whether a victim is a hospital, and therefore out of bounds under their own policies:

From	To	Message
reshaev	pin	Since you did not know about the ban, they did not issue

reshaev	pin	Next time I will issue
pin	reshaev	OK
pin	reshaev	but it's not a hospital
reshaev	pin	What uh
pin	reshaev	i watched a hundred times
reshaev	pin	The site looks like a hospital
pin	reshaev	they have no resuscitation, etc.
pin	reshaev	they mainly treat sports injuries
pin	reshaev	they have insurance for 3kk
pin	reshaev	that's why they screwed up
pin	reshaev	well studied them
pin	reshaev	I don't lay everything
reshaev	pin	OK
reshaev	pin	But we decided not to touch the health sector at all, even like this, so let's now bypass them.

The confusion about whether or not to extort this organisation, which has already been technically compromised, is clear to see.

The reason, America, Canada and the UK feature so highly among the Cy-X is therefore not because they are technically more vulnerable or have more data of value to steal. The real reason in our view is two-fold:

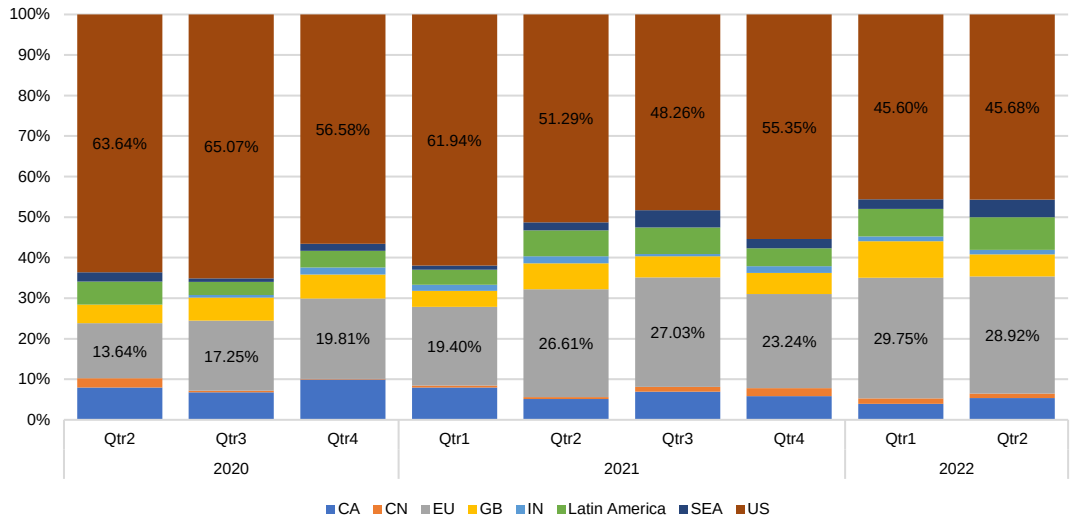
1. There are simply more businesses to target in those geographies. We think of it as akin to throwing mud at a world map on a wall. More mud sticks to the bigger countries on the map. The countries with biggest GDPs, and therefore the largest number of businesses, are hit more under this random approach to targeting.
2. For the crime of extortion to happen it is necessary for the criminal to achieve an understanding of the victim's business, study the stolen data, examine internal documents like insurance policies, and ultimately negotiate with the victim. This requires at very least finding a common language to negotiate with, but also some level of familiarity with the victims' business context.

These two reasons combined make it more likely that businesses in the large, western, English-speaking economies will fall to this crime.

Two forces are counteracting this general trend, however:

Firstly, as criminals seek out new victims and more criminals enter this space, they are being forced to seek out less 'ideal' victims – i.e. victims outside these major English-speaking geographies. Secondly, after high-profile incidents like the Colonial Pipeline compromise, western powers like the USA are increasingly making it uncomfortable for criminals who claim victims there and causing them to seek out victims in less 'charged' environments.

The net impact of these 'reverse' forces on the victimology is that the victim demographics are gradually changing. This shift can be seen in the chart below:



In the chart, we can see clearly how the proportion of victims headquartered in the USA has decreased over time, from over 63% to 45.68%. At the same time the proportion of victims located in Central Europe (EU) has increased from 13.64% to almost 29%.

The proportion of victims in Canada has similarly decreased – from a high of almost 10% to a low of 4% in the 1st quarter of 2022.

The percentage of victims from the UK has varied of the period of our study but remained more or less consistent. It remains to be seen how this trend develops.

In the meantime, the numbers in non-English economies like India, China and Japan, as well as 'developing' economies in Africa and Latin America are growing at extraordinary rates, albeit off a very low base.

This observation, if our hypothesis holds true, is important for two reasons: It suggests that efforts by the USA and her allies to counter the Cy-X threat are effective in part, but only in moving the problem elsewhere. It also suggests that the apparent barriers of language and culture, that may have served to shield businesses in Europe and elsewhere from this problem thus far, will eventually collapse.

Without the marginal impediment offered by language and culture, we see no other factors preventing the problem of Cy-X becoming as significant in Europe as it is already in the USA.

The message is clear: Europe may be enjoying a temporary reprieve where the Cy-X crime is concerned. The crime is continuing to grow, and new victims will eventually be sought out. Now is the time for us to prepare; not only technically but also in terms of our preparedness to deal with a compromise, and our broader strategies for countering the issue as crime.

Wicus

RSA Conference 2022 perspectives

I was fortunate to attend the RSA Conference 2022 in San Francisco and managed to attend a few talks. After all the conferences I've been to in the past, it is amazing to see the same messages being repeated. This makes one wonder how effective we as cyber security practitioners are and whether we are doomed to be stuck in an infinite loop of cybersecurity puppetry?

The Marie Kondo Approach to Security

On an RSA Conference panel RSA Conference Program Committee Chair, Hugh Thompson, and CISA Senior Technical Advisor, Bob Lord, recently talked about a simple approach one can use to create an effective cyber security program given budget constraints. Bob Lord was previously the CISO for the US Democratic Party's Democratic National Committee (DNC) and before that the CISO of Yahoo.

Marie Kondo has nothing to do with cybersecurity and is known for her approach to organize one's personal life by eliminating clutter and getting rid of unused personal stuff. In this context Bob applied the declutter approach to cybersecurity.

While at the DNC Bob's approach to security involved reducing the attack surface by cutting the number of applications and services that overlap in functionality. This enabled security teams to focus and not to have to protect various potential attack avenues. This approach did have its challenges as it required Bob to spend time with all stakeholders to get buy in from them as well as to educate everyone in the organization about the significance of the approach.

The reduction of overlapping services allowed Bob to use the extra budget to roll out phishing resistant multi-factor authentication across organizational structures that he oversaw. This approach reduces the risk involved with credential theft and did not introduce any additional complications. Staff knew that they were better protected through the integration of Single Sign-On authentication, and it significantly reduced the need to manage multiple passwords.

What to do when ransomware hits

A panel session that included Suzanne Spaulding, Preston Golson, Robert Huber, and moderated by Glenn Gerstell explores the value of being prepared for a ransomware incident. This was not a traditional panel discussion, but more a scripted simulation of what happens at the executive level during a ransomware incident. Each panelist played the role of CEO (Suzanne), PR (Preston), CISO (Robert), Legal Council (Glenn). The hypothetical ransomware incident impacted a company in the plastics industry.

Practicing or playing out a ransomware scenario annually is valuable as this will ensure everyone knows what is expected of them and to ensure the business can identify areas that needs improvement.

The panel highlighted a few areas to consider:

In some industries it is important to disclose cyber incidents within a short time frame as there could be regulatory penalties. Knowing which law enforcement and regulatory bodies must be contacted is important. It is strongly advised to go beyond just that. Identify people at those agencies or regulatory bodies and have

their numbers at hand. Ideally verify these contacts frequently to ensure that when needed these people are ready to lend a hand.

Having a tested communication strategy is important. Draft a boiler plate response beforehand and look at what other companies have communicated in the past. This will allow the business to quickly respond to an incident. Controlling the narrative and being as transparent as possible is a long-term strategy that will pay off, trying to hide or coverup what is happening is not feasible. Remember to include shareholders in the loop. Insider trading on publicly listed businesses must also be considered and remind executives to respect the rules.

All team members need to be empowered to execute decisions without too much red tape. For example, the legal team must provide effective assistance to the communications, security, and compliance teams without impeding their effectiveness.

Having an insurance policy that covers ransomware incidents can be beneficial as it is very likely that insurance companies have experience in dealing with such incidents. The insurance companies also have access to experts that can negotiate on behalf of the victim. It is likely that the insurance company will have an incident response team at hand. Additional budget to have an incident response contractor on retainer can be advantageous, but not everyone can afford that.

Test the resilience of your backup and recovery capabilities. This could be the difference between losing everything and starting from scratch or experiencing a painful unplanned outage.

Hacking Exposed: Next-Generation Tactics, Techniques, and Procedures

George Kurtz and Michael Sentonas of CrowdStrike demonstrated a Kubernetes container escape vulnerability (CVE-2022-0811). This vulnerability is present in specific versions of the Kubernetes CRI-O engine. The vulnerability discovered by researchers at CrowdStrike is referred to as cr8escape. An attacker can exploit this vulnerability by specifying malformed kernel parameter values in the container definition.

This vulnerability is a classic example of unsafe handling of untrusted input that allows an attacker to execute commands with elevated privileges. The exploit does require that the attacker can define a container specification with custom properties. All the attacker needs to do is use a special concatenation character (+) and combine this with the “kernel.core_pattern” property key. An attacker can then execute a desired command with root privileges due to the way the values are parsed.

The main message from the session was that old classes of vulnerabilities are present even in new software and that exhaustive testing and validation is required to ensure mistakes do not result in serious vulnerabilities. Additional monitoring of the underlying operating system responsible for hosting the container engine is a must as container escapes could go unnoticed and attacks could thus get a foothold in the container environment. Scanning of container registries for anomalous container definitions must also be performed frequently to detect malicious or unwanted activity.

Diana

The Robinhood phenomenon – how threat actors justify their actions

We are currently conducting research where we have collected over 200 unique qualitative data points from negotiation chats and cyber extortion leak site content from the dark web. What we are observing is that threat actors are including specific language on their leak sites but also during negotiation that justifies in a certain way the purpose of their criminal activities. What becomes clear is that the threat actors don't call their actions criminal but instead describe them as conducting business operations or even as a necessary action to make society aware of data mishandling and businesses' wrong doings. In very rare cases do they donate some of the extorted proceeds or claim to only conduct their attacks against certain targets (Robinhood phenomenon).

Consequently, we see that there is a strong tendency toward "rationalization" among modern extortionists. Such attempts by criminals to explain away their deviant behavior is exhibited through the theoretical concept of 'Neutralization Techniques'. Criminologists refer to the use of justifications and excuses for practicing deviant behavior as "neutralization". It is one of the most important elements explaining aberrant or criminal behavior. Psychologically, offenders must rationalize to justify their crime and make it acceptable to themselves and others. Neutralization can be accomplished in two ways: on the one hand, by denying deviant behavior ("It is not deviant"), and on the other by denying responsibility ("I am not responsible for it") (Kaptein and van Helvoort, 2019).

The former approach appears to fit cyber extortion best - denying deviant behavior. This can be done by either 'distorting the facts' or 'negating the norm'. According to Kaptein & van der Helvoort (2019: 1262-126):

"People can deny deviant behavior by changing the description of the situation so that the norm that is violated is no longer applicable and thus would appear to have not been violated at all. They can also deny deviant behavior by changing the norm so that it is no longer applicable to the situation".

It will be interesting to analyze our collected data and identify the use of Neutralization techniques that are actively applied in threat actors' communication towards the public. But also, to gain insights into other aspects such as the way they work in terms of organizational structures, their 'success rate' in extorting payments, and patterns in their negotiations as well as identifying victim variables that can provide us with valuable information on the likelihood of becoming a victim; and thus, will help develop preventive strategies to deter this form of crime.

We aim to share our first results by the end of this summer.

Good News Cyber

The good news cyber section has over the past few months celebrated the successes of law enforcement agencies across the world in clamping down on cyber criminals. This month is no exception where we highlight several stories featuring successes of various law enforcement agencies.

Business Email Compromise (BEC) is a crime where criminals trick an employee of a targeted business into transferring money to a bank account under the control of the criminal. A criminal somehow gains access to the mail account of a party associated with the victim, normally a supplier or other trusted third-party doing business with the victim. The criminal uses an existing email thread to inject the fraudulent bank details with the payment instruction and intercepts any associated response from the victim. If the email from the criminal looks legitimate, then the victim will execute the instruction. Normally the crime goes unnoticed for a while.

Interpol recently made a successful arrest of a suspect linked to a Nigerian BEC gang tracked as SilverTerrier, also known as TMT. The suspect has evaded capture but was apprehended when he attempted to reenter Nigeria. SilverTerrier is believed to have been active since 2015. In November 2020 seven members of the gang were arrested and were attributed with over 500,000 BEC cases spread over 150 countries. In a similar case, Interpol arrested three Nigerian men in possession of fraudulent documentation that could be used in BEC style crimes.

A Ukrainian was sentenced to four years in jail for selling access to hacked servers. This type of activity is normally associated with an Initial Access Broker (IAB). An IAB will compromise a host or network and advertise the access on dark markets. Cyber Extortion groups are known to utilize this type of service to buy access to potential victims. The Ukrainian is said to have compromised various types of victims, spanning sectors such as governments, hospitals, emergency services, call centers, metropolitan transit authorities, law firms, pension funds, and universities.

Cryptocurrency mixers, also known as tumblers, provide so called “privacy focused” services for persons that wish additional obfuscation of blockchain related transactions. These tumblers have a poor reputation as they are often associated with cyber-criminal activity. Blockchain transactions associated with attackers linked to the Democratic People's Republic of Korea (DPRK) were pushed through a tumbler service called Blender.io. This resulted in the U.S. Treasury Department issuing sanctions on Blender.io for their role in aiding DPRK. The U.S. Office of Foreign Assets Control (OFAC) tracked 45 Bitcoin wallets linked to DPRK and movement on some of these wallets triggered the action against Blender.io to block conversion of Bitcoin into fiat currency.

The creator of the Thanos ransomware and associated ransomware-as-a-service was charged by the U.S. Department of Justice. The person was identified as a cardiologist from Venezuela. The link to the 55-year-old was made when he used a PayPal account of a relative residing in Florida in an illicit transaction.

The FBI seized three domains associated with cybercriminal activity. The first domain was used to sell access to breach databases that could be searched to find stolen Personal Identifiable Information on more than 7 billion records. The other two domains were linked to Distributed-Denial-of-Service (DDoS) operators.

Another member of the infamous Infraud carding gang was sentenced to four years imprisonment. The convict was a very active member of Infraud and is believed to have contributed to damages totaling $568 million due to the sale of skimmed or illicitly obtained payment card details that was sold on the underground forum. This brings the total of indicted persons linked to Infraud to 36 members.

The U.S. government has managed to recover $15 million from a Swiss bank account related to the ‘3ve’ online advertising fraud scheme. The ‘3ve’ or ‘Eve’ scheme used the Kovter botnet to perpetuate click-fraud malware. The malware would run on infected hosts machines simulating users browsing advertisements.

The U.S. Department of Justice is now a signatory of the Budapest Convention. This convention has 66 member countries and helps expedite sharing of electronic evidence, especially that used to investigate cybercriminals globally