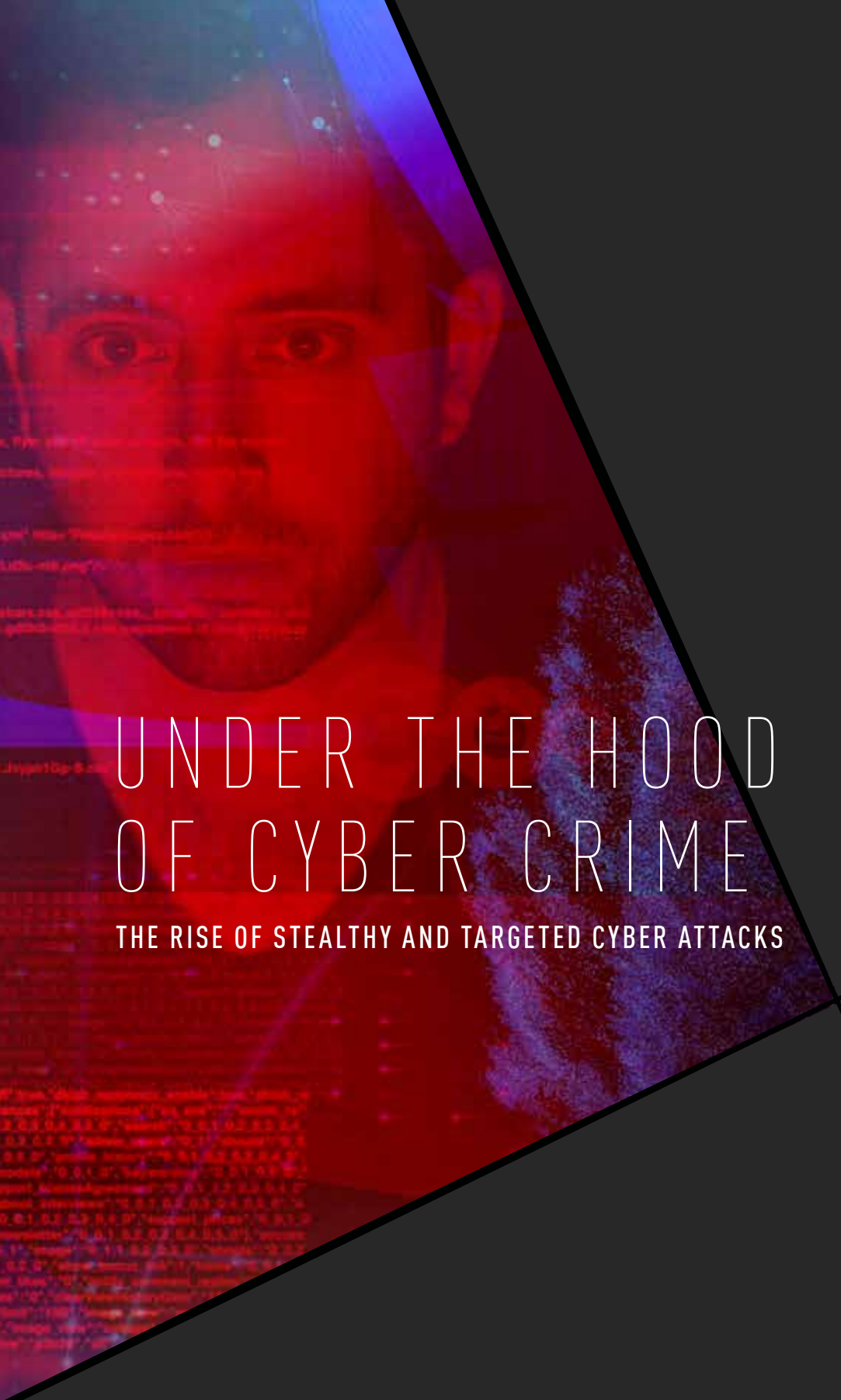


CHECK POINT RESEARCH

UNDER THE HOOD OF CYBER CRIME

THE RISE OF STEALTHY AND TARGETED CYBER ATTACKS

2019 Security Report
Volume 02

VOLUME 02

2019 SECURITY REPORT

01	INTRODUCTION	3
02	UNDER THE HOOD OF CYBER CRIME	4
03	THE DEMOCRATIZATION OF CYBER CRIME	5
04	STEALTH-LIKE MALWARE	14
05	CONCLUSION	24

INTRODUCTION

Since the dawn of the internet, a cybercriminal ecosystem has been developing right beneath our fingertips. And much like the maturing of the Internet, this ecosystem has come a long way since its inception.

In the first installmentthe 2019 Security Report, *CyberAttack Trends Analysis* we reviewed the latest trends and threats facing the IT security industry today. We assessed the major incidents that impacted organizations over the past year along with our commentary and insights regarding them. These trends fell into the categories of Cryptominers, Ransomware, Malware Methodology, Data Breaches, Mobile and Nation- State Cyber Attacks.

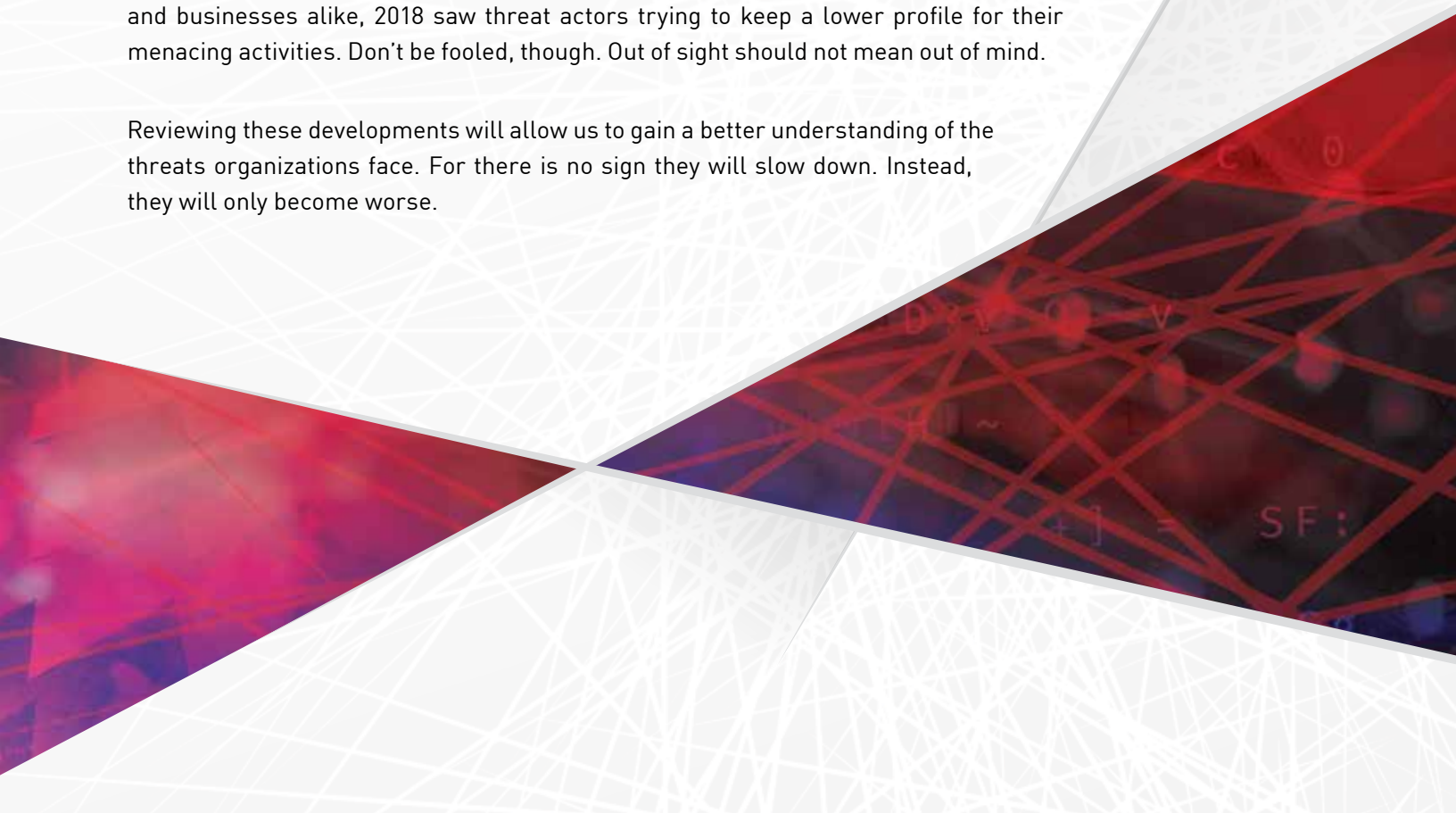
In this installment we zone in on an underlying trend that lies behind all of the above categories, the democratization of cyber crime.

While in the past cyber crime activities were the sole domain of highly technical individuals, in today's cyber underworld anyone who is willing to pay can easily obtain the suitable tools and services needed to launch any kind of cyber-attack.

While unskilled attackers have been involved in the malware distribution arena for a while now, this year we witnessed a significant growth in attacks orchestrated with cyber weapons or products that were acquired through the clandestine 'Malware-as-a-Service' industry.

We then take a deeper dive into the trend of more stealth-like malware that was silently making its way into organizations' IT infrastructure. Whereas 2017 was filled with large scale, headline grabbing attacks that served as a wakeup call to both private individuals and businesses alike, 2018 saw threat actors trying to keep a lower profile for their menacing activities. Don't be fooled, though. Out of sight should not mean out of mind.

Reviewing these developments will allow us to gain a better understanding of the threats organizations face. For there is no sign they will slow down. Instead, they will only become worse.



UNDER THE HOOD OF CYBER CRIME

Daybreak

Prior to the year 2000, hackers were primarily one-man operations exploiting weaknesses in computer operating systems or networks. In most cases, these computer enthusiasts experimented and explored this new online network and challenged themselves to 'beat the system.' In fact, despite being early cyber criminals, rarely was their behavior financially motivated. Indeed, while there was the potential for financial damage and security risks, the 'one-man-hacker' lacked the same motive and intent of the criminal gangs that were soon to follow.

After the Dawn

Not long after, once there were more people, websites and services available online, cyber criminals began to organize themselves and perfect their hacking techniques. Hardened criminal gangs soon realized that internet users saw it as safe, despite the technology being riddled with exploitable gaps and holes. Furthermore, the anonymity of the Internet served as a shield and far less risk of detection. Next, as shops and financial services moved online, vast amounts of financial data were transferred to cyber space. And where money flows, criminals are never far behind, always on the prowl to steal anything of value.

In short, gangs introduced a professional element to the world of cyber crime. Nowadays we are no longer looking at curious amateurs exploiting weaknesses in computer operation operating systems, but rather organized criminal gangs using infiltrating computer networks to infiltrate for financial gain.

THE DEMOCRATIZATION OF CYBER CRIME

Crucial to understanding the new age of cyber crime is the awareness that today's cyber crime ecosystem is one that reflects and matches the legitimate world of business, albeit completely illegal.

The main roles in this underground economy break down into the following categories:

Programmers – develop malware to extort or steal data from potential victims.

Merchants – trade and sell the victim's stolen data.

IT Technicians – build and maintain the IT infrastructure (servers, databases, etc.) for criminals.

Hackers – search and find vulnerabilities in systems, applications and networks.

Fraudsters – create and carry out new ways to scam and manipulate potential victims.

Hosting Services – provide hosting services for the criminal's fraudulent content and sites.

Management – hire and form their cybercrime teams and manage the operation.

A Programmer's Tool Box

At their disposal, programmers have a variety of malware types they can create. Named by the brilliant, late Israeli computer researcher, Yisrael Radai, malware are software programs with the purposefully malicious intent to act against the requirements of the computer user. The types of malware most commonly seen in the wild fall mainly into the following categories:

SPYWARE

Often referred to as 'keyloggers', spyware tracks and steals digital information while keeping the victim fully unaware of the situation. It is particularly interested in financial data such as credit card details and online banking login credentials.

TROJAN

Disguised as safe programs, Trojans are designed to fool users, so that they unwittingly install it on their own system, and they're later sabotaged by it. Trojans are generally used to steal both financial and personal identifiable information (PII).

> *Over **10,000** different malicious files are detected per day.*
>
> Source: ThreatCloud Map is powered by Check Point's ThreatCloud intelligence

VIRUSES

Dating back to the 1970s, a computer virus is a contagious piece of code that infects software and then spreads from file to file within a system. When infected software or files are shared between computers, or on the internetInternet, the virus spreads to new hosts.

RANSOMWARE

By locking down data on a victim's computer, typically by encryption,. Ransomware demands payment sent to an attacker in order for the encrypted files to be released and computer access restored to the victim.

BOTWARE

The purpose of Botware is to turn the victim's computer into a "zombie" and become part of a larger network of devices that await instructions from its controller to launch an attack. A distributed denial-of-service (DDoS) is a key example.

CRYPTOJACKERS

Cryptojacking is the unauthorized use of the victim's computer to mine cryptocurrency and send it back to the attacker. It feeds off the victim's CPU power and results in the victim's computer slowing or even crashing.

In today's cyber crime landscape, cyber criminals are no longer the ones with the direct technical capabilities of creating the malware that's used in attacks. Nor are they necessarily the ones who need any know-how in distributing the attack. In fact, very little knowledge is required.

Instead, all a cyber criminal needs is access to the underground communication channels that act as the main marketplace for this ecosystem. There they will manage to "order" a malware or even a direct attack against a chosen target. This is the democratization of cyber crime.

The Dark Web

Making a large chunk of the internet, the Dark Web is a hive of illicit activity. From illegal guns and drug dealing to Malware-as-a-Service (MaaS) programs, buyers and sellers use this medium to trade and exchange knowledge and products.

Hacking forums on the Dark Web have long been a popular platform and an important means of communication among cyber criminals. It allows them to publish job offers, market their products and consult with one another.

After all, large operations and campaigns cannot be carried out by one person and necessitate the recruitment of a team to share the workload. In other cases, these forums serve as places where malware and tools crafted for malignant reasons can be traded or sold to affiliates and generate revenue without the developer being directly involved in an attack.

The services offered online include malware kits, stolen data or even a package that contains a malware ready for distribution and a comprehensive management panel which allows unskilled hackers to easily track and control their infection rates and revenues. The different Malware-as-a-Services available include the infamous AZORult, File-Locker and Kraken ransomware that made headlines over the past year. The authors of GandCrab ransomware even offer technical support and tutorial videos for their product.

However, the take-down of such Dark Web market places such as the Hansa Market and Alpha Bay in 2017, spawned the next stage in the cyber game of cat and mouse. Threat actors soon shifted to new channels to evade authorities. In fact, they quickly transitioned to the increasingly popular and highly secure mobile messaging app, Telegram, to pursue their trade.

> ***57%*** *of onion sites has have illegal content.*
>
> Source: Europol "Internet Organized Crime Threat Assessment, 2017"

Communication Channels

Telegram's hosted chat groups, known as 'channels', are used to broadcast messages to an unlimited number of subscribers, and, while their entire messaging history can be viewed, any response to the public messages is held privately. The discretion these channels provide goes a long way to help conceal a cyber criminal's identity and conversations.

Any threat actor with a shady skill, service, or product to offer or buy can enjoy private, end-to-end, encrypted chats instead of exposed threads in online forums. If in the past several steps were required to ensure an anonymous connection to Tor, the Dark Web browser, today any Telegram user can easily join channels with a single tap on their phone and start to receive notifications of clandestine conversations or offers while keeping their identity completely hidden.

This has allowed for much easier completion of the first stage in organizing an attack; — connecting with those who can help put it all together.

One region in which these shady channels are flourishing is Russia and some have already attracted thousands of subscribers. Such examples are 'Dark Jobs', 'Dark Work' and 'Black Markets', to name a few. In addition, some channels, such as an Iranian channel which goes by the name of 'AmirHack', can contain up to 100,000 members.

These channels are not restricted to just recruiters and job-hunters. They also run advertisements for the sale of stolen documents or hacking tools. This is especially worrying, considering the accessibility of the channels and the promises of high salaries made to those who might otherwise refrain from carrying out such activities.

As a result, this poses a risk of growth in cyber crime rates as these positions are not only openly marketed but they are also available to inexperienced users, making dangerous tools available to anyone.

Hacking Tools and Services

"Wanted for a dark project: Cryptor running on all systems from Windows XP to 10. Bypassing the top AV especially Avast and Defender".

Example:

A cyber criminal's advertisement as posted in a Telegram channel.

The message below found in a Telegram group is a good example of how someone with no prior experience in malware development can run an entire operation by leveraging Telegram channels. In this case, whoever is behind the advertisement is outsourcing an entire project and is responsible for payment only.

DARK JOB

NAME: Виктор Тимур 18+
MEMBERS: 6,873

Description: Info (submit an advert, advert guarantees, guarantor) @dark_job_info_bot)
Main posts: Job hunting, company employees.

DARK WORK

NAME: Трофим Степан
MEMBERS: 762

Description: The Best Dark Net Message Board to Submit an Advertisement.
Main posts: Selling and creating hacking tools.

YP

NAME: Дмитрий Ефим
MEMBERS: 4,425

Description: submit an ad - @banMarket_bot Advertising / Guarantor- @deluxe_R @Rhodesk Chat - @banMarket_chat)
Main posts: Selling schemes and documents.

Other illegitimate services in some of Telegram's more crooked channels include forging legal documents such as IDs, passports, banking documents and more. As you can imagine, Photoshop experts and freelance designers are in high demand in these markets.

Next Generation Phishing Kits

One of the most advanced phishing kits, the '[A]pache Next Generation Advanced Phishing Kit', is another example of how easily accessible, and yet highly damaging, tools are promoted and sold on the Dark Web.

Allowing any aspiring cyber-criminal with very little knowledge to run a prof-essional phishing campaign, the notorious [A]pache Phishing Kit instructs those looking to steal credit card details by luring potential victims to fake shopping sites.

At $100-$300, the cost of buying this advanced Phishing Kit was higher than more standard phishing kits. Standard kits usually retail at $20-$50, though some are even free. However, those provide login pages and prompts for personal and financial information. [A]pache's next generation phishing kit, however, provided threat actors with a full suite of tools to carry out their attack. These included an entire back-office interface with which they could create convincing fake retail product pages and manage their campaign.

In order to convincingly persuade their victims that they're shopping at a genuine site, cyber criminals also need a domain that's similar to the targeted brand, for example, www.walmart-shopping.com. Those can be provided as well by illegitimate hosting services on the Dark Web. Once registered, a threat actor is ready to deploy the kit to a PHP and MySQL supported web host, log in to the kit's admin panel and begin configuring their campaign. It's really as simple as that.

To simplify this set up process further, [A]pache made a simple user interface within the admin panel where the threat actor could paste the product URL of the legitimate retailer and the product information would automatically be imported to the phishing page. Cyber criminals could then view their 'products' and change the original prices.

Example:
A fake retail site offered by next generation Phishing Kits for sale on the Dark Web.

Bots for Rent

In 2018, the Malware-as-a-Service industry offered additional services.

Some of the year's most prominent malware distributors, giant multi-purposed botnets, now offer their most valuable resources, their bots, for rent. This allows any actor to take part in high-scale global campaigns. For example, Emotet, originally a massive banking malware targeting European banking customers, has shifted its focus and now offers global packing and distribution services, leveraging its self-propagation capabilities. Ramnit, another prominent banking malware, demonstrated similar behavior with a single affiliate campaign, 'Black', which caused approximately 100,000 infections.

Ransomware Goes Agile

Due to the lack of knowledge required, as well as the ease of access and low cost of underground services, cyber criminals are more commonplace. Promoted on Dark Web hacking forums, the GandCrab Ransomware-as-a-Service affiliate program serves as a good example of how amateurs can now profit from the ransomware extortion business as well.

This model is very profitable for the malware authors and allows them to focus on malware development, while delegating the delivery stage to multiple distributors who buy or rent the product as part of an affiliation program.

As a partnership program, GandCrab lets its users keep up to 60% of the ransom revenues collected from victims, while its developers keep up to 40%. In exchange for these fees, the buyers receive the tools to initiate an attack and GandCrab's creators offer support and updates to the ransomware itself. This essentially adds another incentive for affiliates to choose their Ransomware-as-a-Service over competing suppliers. According to our research, GandCrab has dozens of active affiliates (80+), the largest of which distributes over 700 different malware during any given month. As a result, within just two months GandCrab had infected over 50,000 victims and claimed an estimated $300-600K in ransom payments.

The Accessibility of Cyber Crime

As illustrated in our journey into today's world of cyber crime, hiring services, accessing malware, and anonymously selling stolen data has never been easier. It has led to the proliferation of amateurs wanting to get in on the action. From a disgruntled employee to a bored teenager, anyone with a little capital and motivation can become a threat actor.

The convenience of encrypted channels like Telegram allows threat actors and those who wish to take part in cyber crime and communicate in a more secure manner. Sadly, although popular messaging applications have improved the security of user information over the years, they are also being abused by those fleeing from prying eyes, and the law.

In addition, Malware-as-a-Service provides everything a cyber criminal needs to get started and threatens modern organizations in two ways. It creates a demand for better, easier-to-use malicious programs, as malware developers seek to distinguish themselves from any competition. This leads to significant strides in the accessibility and sophistication of malware threats.

Furthermore, Malware-as-a-Service vastly increases the number of individual threats, as it empowers those who would not otherwise have the technical skills to create their own malicious programs. This effectively allows just about anyone to launch a cyber attack.

As a result, and together with the range of services and products now available in today's cyber crime ecosystem, there is a myriad of opportunities to carry out cyber attacks. Indeed, while the number of cyber criminals seems to be rising due to the low technical barrier to entry, the number of cyber-attacks on both organizations and individuals is growing accordingly.

Whereas 2017 was filled with large scale, headline grabbing attacks that served as a wakeup call to both private individuals and businesses alike, threat actors kept a lower profile in 2018. Don't be fooled. When it comes to cyber attacks, out of sight does not mean out of mind. Organizations are under constant attack from the ever-growing number of malware, spreading at higher rates than ever.

In 2017, cyber criminals continued to profit from ransomware attacks. It tapered off towards the end of 2017 and the beginning of 2018. In fact, this trend was so sharp that compared to its heyday just a few months before, it seemed to barely register on the radar at all.

Ransomware Gets More Targeted

Despite its decline, ransomware has not disappeared from the cyber threat landscape. Instead, cyber criminals found more lucrative payoffs with targeted ransomware attacks versus the wide-cast style of attacks seen in previous years. Distributing millions of emails with no specific victim in mind gave way to planned and researched attacks on highly targeted victims. The extra effort apparently paid off as targeted ransomware attacks have allowed criminals to earn payoffs in the millions of dollars.

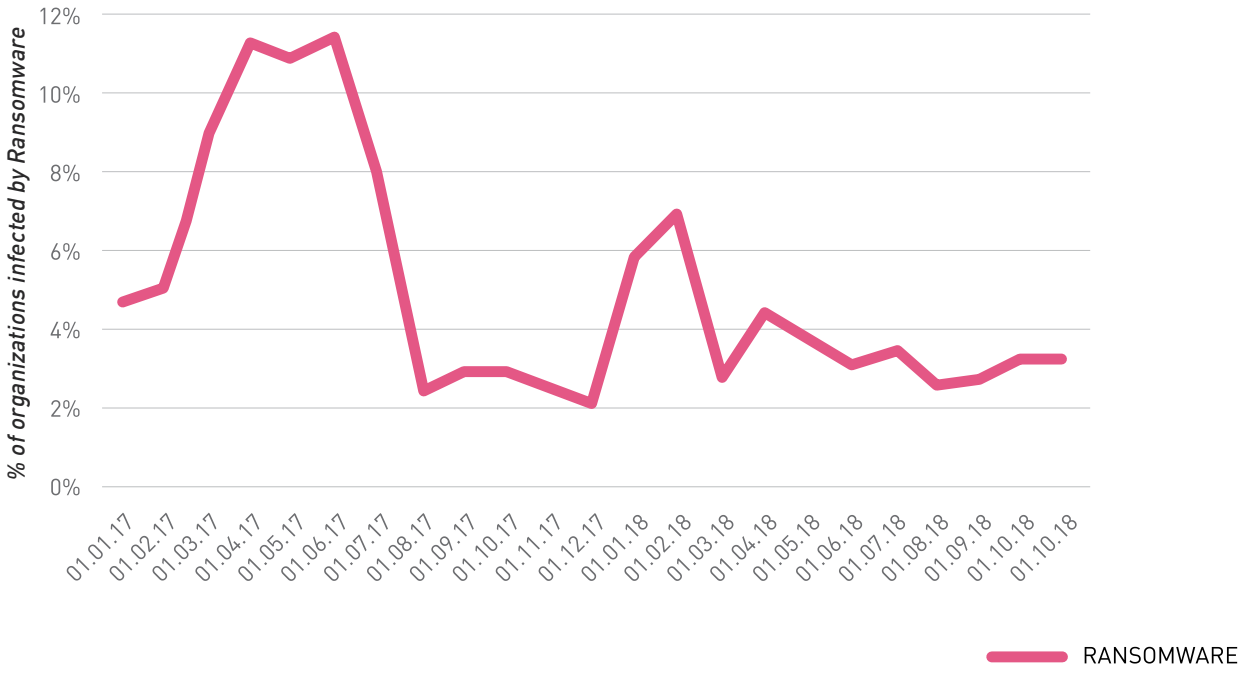
Attacks carried out against the City of Atlanta in March 2018 serve as a good example. Targeted by the SamSam ransomware, cyber criminals were able to extort much larger amounts due to the nature of the victim, the pressure it felt from its citizens, as well as the City's ability to pay the larger ransom amount. Compare this to the non-targeted GandCrab ransomware attacks, for example, where the demands maxed out at about $1,000 per victim, while the SamSam ransomware typically demands as much as $50,000 from its victims.

STEALTH-LIKE MALWARE

Whereas 2017 was filled with large scale, headline grabbing attacks that served as a wakeup call to both private individuals and businesses alike, threat actors kept a lower profile in 2018. Don't be fooled. When it comes to cyber attacks, out of sight does not mean out of mind. Organizations are under constant attack from the ever-growing number of malware, spreading at higher rates than ever.

In 2017, cyber criminals continued to profit from ransomware attacks. It tapered off towards the end of 2017 and the beginning of 2018. In fact, this trend was so sharp that compared to its heyday just a few months before, it seemed to barely register on the radar at all.

DECLINE OF RANSOMWARE ATTACKS 2017-2018



Ransomware Gets More Targeted

Despite its decline, ransomware has not disappeared from the cyber threat landscape. Instead, cyber criminals found more lucrative payoffs with targeted ransomware attacks versus the wide-cast style of attacks seen in previous years. Distributing millions of emails with no specific victim in mind gave way to planned and researched attacks on highly targeted victims. The extra effort apparently paid off as targeted ransomware attacks have allowed criminals to earn payoffs in the millions of dollars.

Attacks carried out against the City of Atlanta in March 2018 serve as a good example. Targeted by the SamSam ransomware, cyber criminals were able to extort much larger amounts due to the nature of the victim, the pressure it felt from its citizens, as well as the City's ability to pay the larger ransom amount. Compare this to the non-targeted GandCrab ransomware attacks, for example, where the demands maxed out at about $1,000 per victim, while the SamSam ransomware typically demands as much as $50,000 from its victims.

> ***46%*** *of organizations were hit by Ransomware attacks in 2018.*
>
> Source: Security Report Threat Prevention Research among IT and Security Professionals, November 2018

The prime goal is detecting the target network's crown jewel, an asset that when shut down can cripple the company's activities within minutes, leaving the victims no option but to pay the demanded ransom to avoid colossal damages which may even result in higher costs. Ransomware operators such as Ryuk even aim at neutralizing victims' backups serverss and encrypting them as well.

So far, the targeted approach has proven effective throughout 2018, generating larger revenues for the attackers, and definitely worth the greater efforts. Together with the fact that the premeditated, manual strategy assists the attackers in evading detection, it is a guarantee that this trend is going to stay with us for a while.

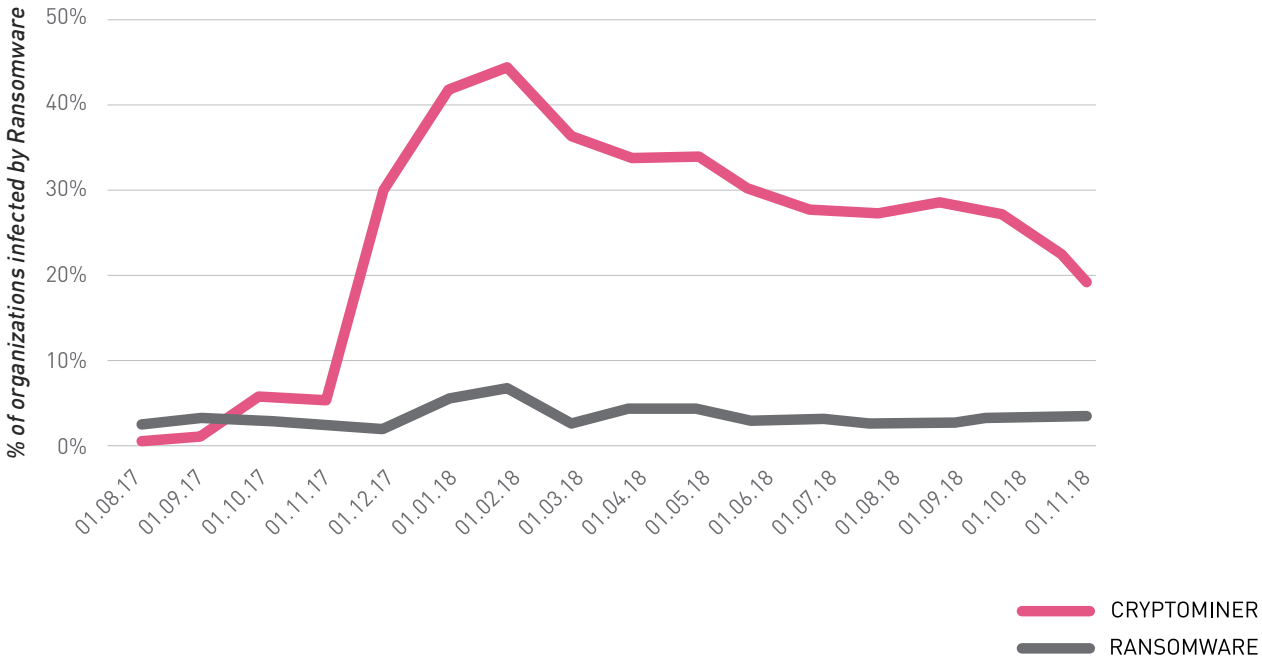
The Rise of the Cryptominers

Meanwhile, as ransomware became more targeted, a new mass-delivered malware took root. Unlike ransomware, though, it was far more stealth-like and did not alert its victims at all. In fact, in contrast to ransomware attacks, its victims were unaware of the attack until they realized the cyber criminals had already harvested their profits.

Enter the cryptominers, a far quieter and more stealth-like malware, yet no less dangerous.

As seen in the graph below, the rise in crypto-mining was dramatic. Why was this?

THE RISE OF CRYPTOMINING ATTACKS 2017-2018



> *RubyMiner attempted to exploit **30%** of all corporate networks worldwide.*
>
> Source: Check Point Research blog, "'RubyMiner affects 30% of WW Networks," January 2018

There are several reasons for the increase in crypto-mining and the decline in ransomware attacks.

1. Few victims pay the ransom. Despite the high infection rate of large scale ransomware attacks such as WannaCry, for example, only $140,000 was earned in the attack. While this may seem like a lot, it is actually a small payment rate considering that over 400,000 computers were infected.

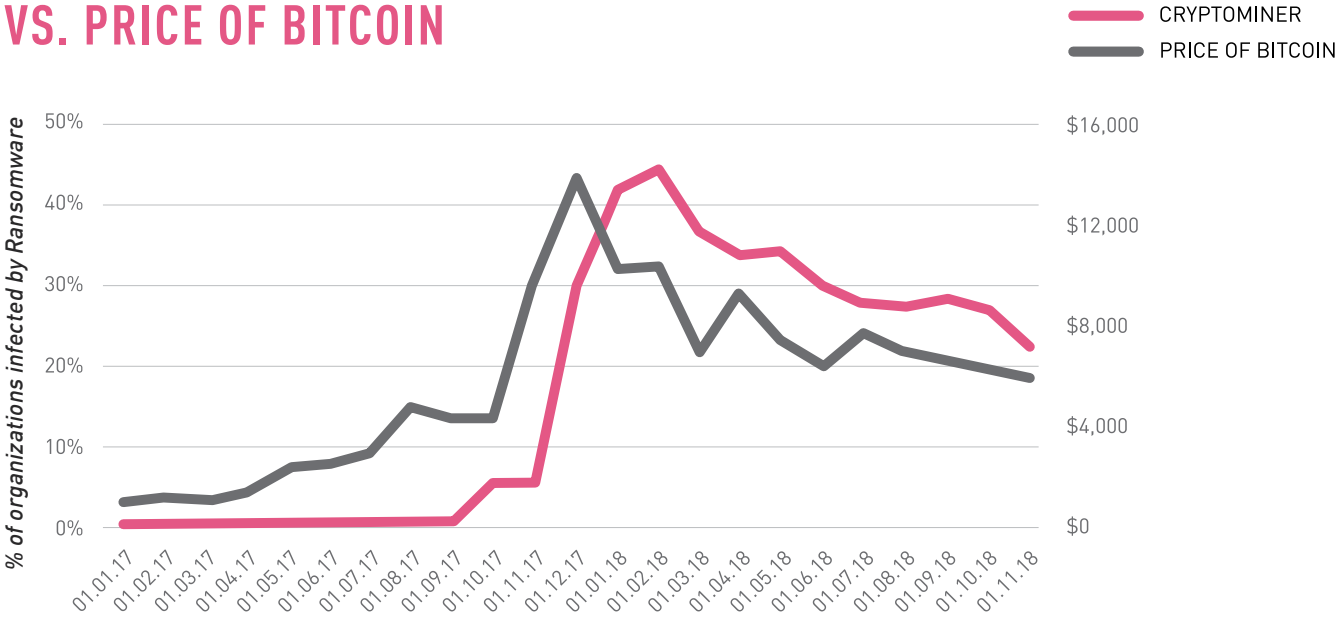
2. The volatility of cryptocurrency rates. When ransom payments are demanded in bitcoin, it is crucial for the digital currency to have a favorable exchange rate to the dollar. This means the rate has to be optimal; not too high that the victim will be unlikely to pay, and not too low that it's unprofitable for the attacker. In addition, while it is still very much a valuable currency, it has dropped hugely since mid-2017, making ransom payments, much less attractive when they're paid.

3. Cryptojacking malware is more effective. Ransomware is highly visible and triggers alerts inside an organization. They may well be infected once, pay or not pay, but then they will take measures to keep it from happening again. Cryptojackers are stealthy, flying under the radar. They do not set off alerts or alarms and often their presence is unknown, which allows the attacker to hijack their target to generate income for as long as they wish, unbeknownst to their victims.

In addition to the above, the rapid rise in crypto-currency value was a major factor in the use of cryptojackers to harvest this lucrative currency for malicious actors. Furthermore, the correlation between the rise, and subsequent drop, in cryptocurrency values and the rise of cryptomining attacks is reflected clearly in the below chart.

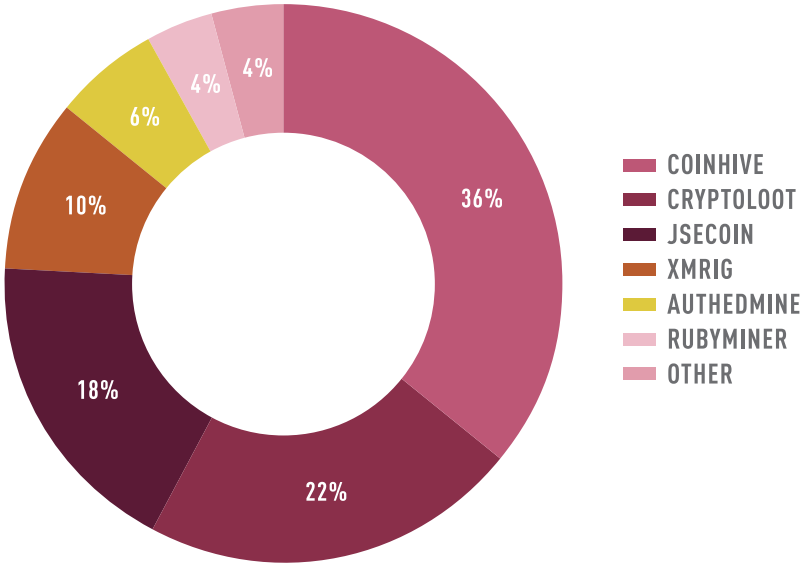
CRYPTOMINERS' IMPACT ON ORGANIZATIONS VS. PRICE OF BITCOIN

Source:
Check Point
Threat Cloud



Cryptojacking has thus allowed criminals to switch from a smash-and-grab approach, which usually turns out to be a one-hit-wonder strategy, to a prolonged clandestine operation. No longer do threat actors need to deal with uncooperative victims who do not pay up, or those who have a data back-up, rendering the attack ineffective. Instead, the change in strategy is highly effective to enable them to slip through the cracks of an organization's security posture, open a door for future attacks, and fundamentally change the nature of attacks and how organizations need to defend against them.

Chart: Top Cryptomining Malware Globally



As seen in the above chart, the most prominent cryptomining malware dominating the Global Top Cryptominers Malware list are Coinhive, CryptoLoot and JSEcoin. These malware have also kept their place at the top of the list since 2017.

These popular web-based cryptominers are easily integrated into websites, willingly by website owners as well as unknowingly by threat actors who utilize those websites' high traffic to generate cryptocurrency. Taking a different approach, the RubyMiner campaign targeted unpatched Windows and Linux servers, and maintained its high rank during the first half of 2018. As revealed by Check Point researchers last January, RubyMiner attempted to exploit 30% of all corporate networks worldwide to mobilize powerful servers into its operators' mining pool.

The Evolution of Cryptominers

Since their creation, Cryptominers have come a long way. Evolving from simple website compromise, Cryptominers have been observed this year spreading through Facebook Messenger, YouTube ads and Google Play, while infecting tens of thousands of websites, personal computers and powerful severs such as Jenkins. In 2018, though, Cryptominers upgraded and vastly improved their capabilities, becoming more sophisticated and even more destructive.

Motivated by a clear interest in increasing the percentage of computational resources leveraged, and crafted to be even more profitable, Cryptominers today target anything that could be perceived as standing in their way. As a result, we have witnessed Cryptominers targeting SQL databases, industrial systems, nuclear power plants, and, most worryingly, cloud infrastructure. Cryptominers have also evolved recently to where they can exploit high-profile vulnerabilities while evading sandboxes and security products in order to increase their infection rates.

The mobile arena was not deprived of Cryptomining attacks either. Last April, the Android Cryptominer dubbed HiddenMiner targeted numerous devices, continuously mining Monero until the devices' resources were drained. Mobile miners have even managed to penetrate Apple's App Store, with a malware that steals victims' login credentials to cryptocurrency wallets.

Adding more fuel to the fire, since the beginning of 2018 a variety of new attack methods have surfaced. One such new attack leverages the potential with cryptocurrency trading systems. Among others, these methods include virtual wallet and credential theft, cryptocurrency transaction maneuvering, as well as ICO scams (Initial Coin Offering) that lure victims to invest in a fake premature cryptocurrency.

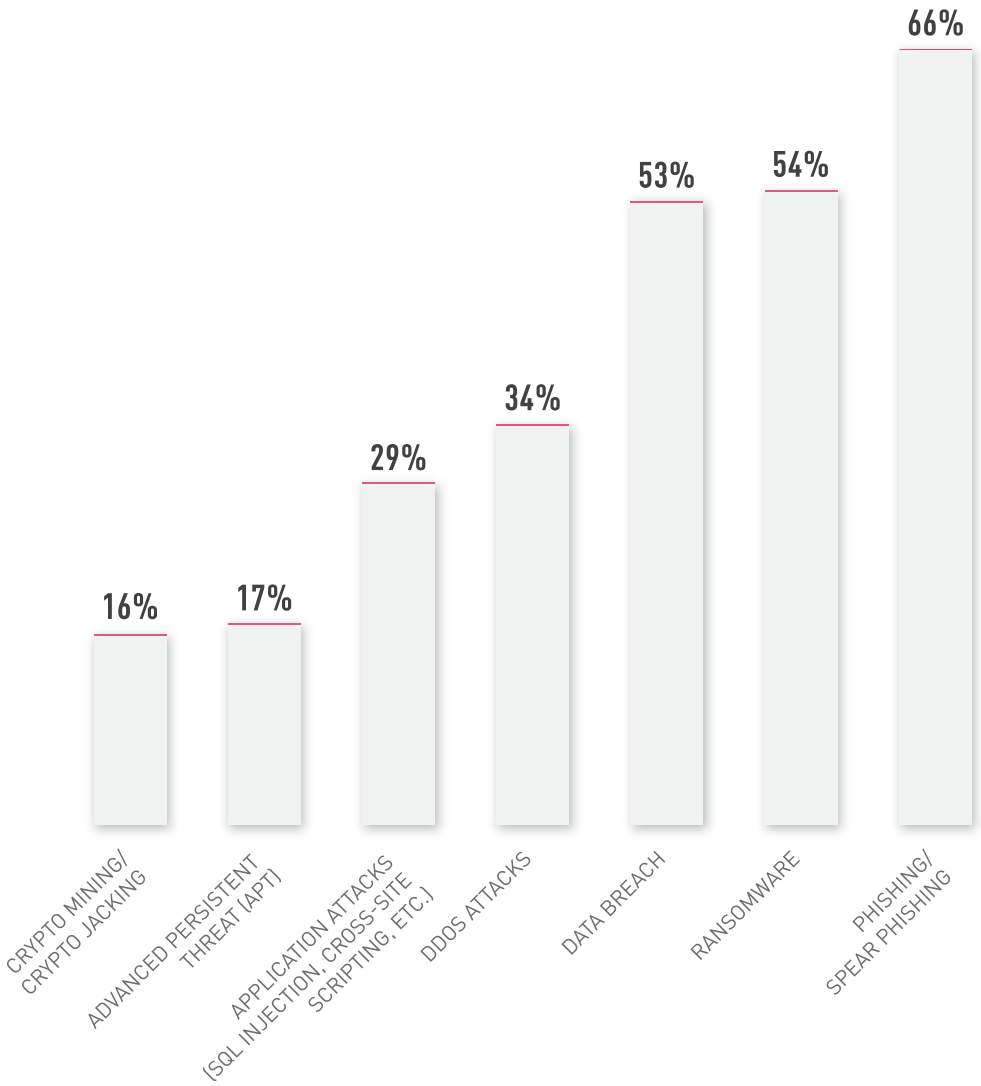
> *Cryptominers infected **10x** more organizations than ransomware but only **1 in 5** IT Security Professionals are aware they were affected.*
>
> Source: Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Moreover, other malware families have begun integrating mining capabilities into their arsenal. Ransomware, as well as prominent Banking Trojans, including Panda and TrickBot, are now targeting not only bank accounts but also cryptocurrency wallets and trading system accounts, adding features of cryptocurrency credential theft to their arsenal.

Meanwhile, the world sleeps.

Despite exposing this conspicuous threat, organizations have been less responsive in defending against covert attacks. This is concerning as cryptojackers can easily act as back doors to launch other malware types. Banking Trojans can lie undetected for months, if not years, before being detected.

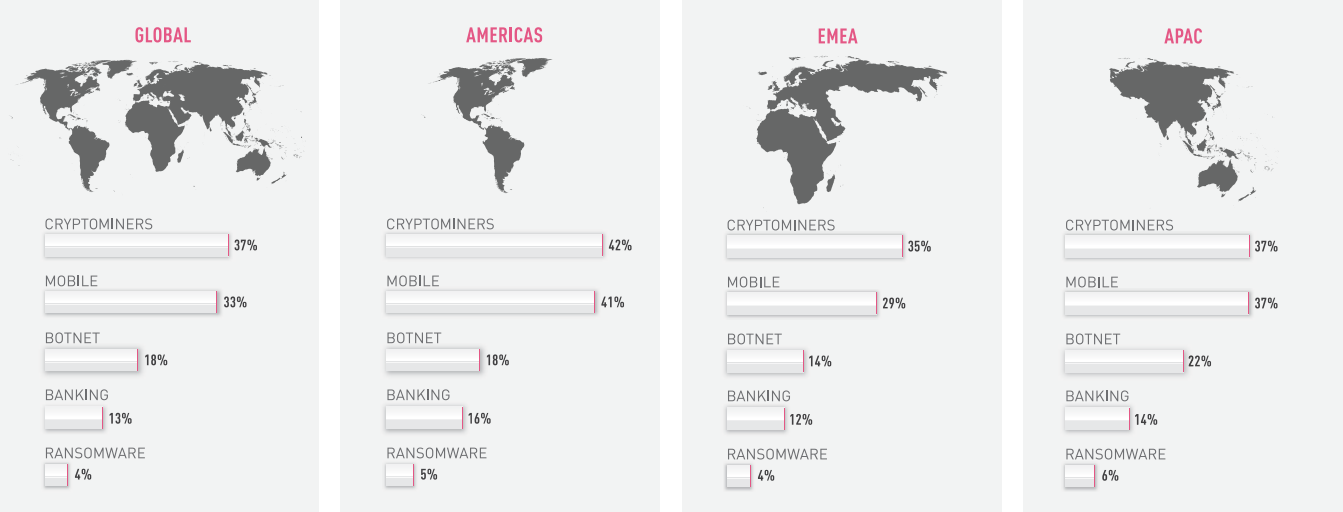
WHICH OF THE FOLLOWING TYPES OF CYBER-ATTACKS DO YOU CURRENTLY SEE AS THE GREATEST THREATS TO YOUR ORGANIZATION?



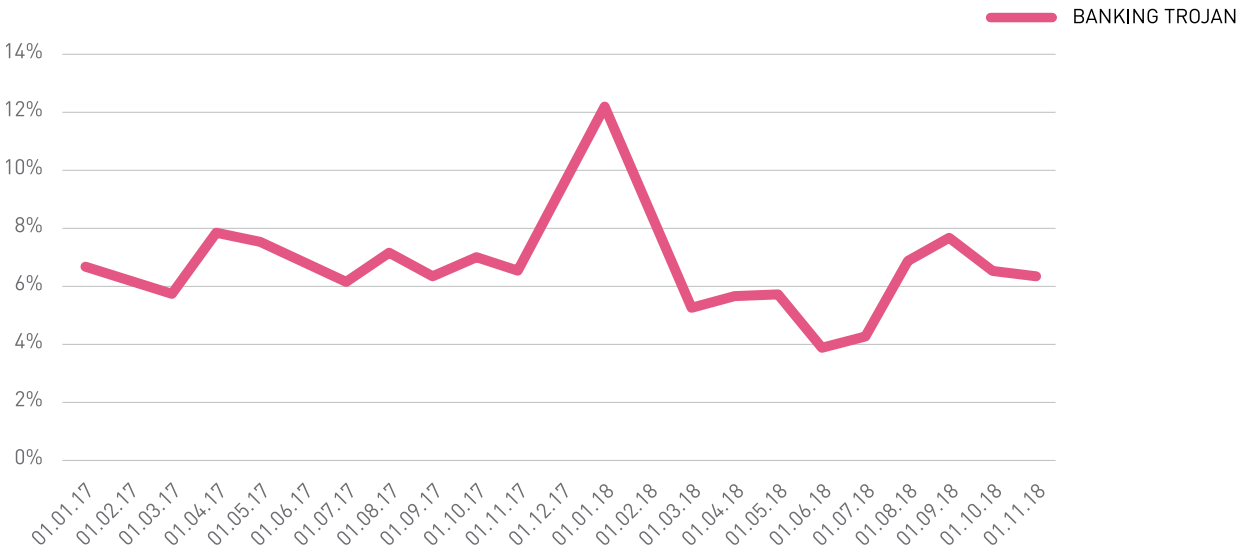
The Rise of Banking Trojans

Banking Trojans are helping cybercriminals to commit the perfect crime, stealing money from the accounts of unsuspecting victims, virtually untraceably and with minimal risk. As such it's no surprise that Banking Trojans are another prevalent type of malware. As seen in the below map, in Asia-Pacific countries they far outstripped ransomware in the number of attacks.

Map: The Most Prevalent Malware Type Across World Regions



PERCENTAGE OF ORGANIZATIONS IMPACTED BY BANKING TROJANS 2017-2018

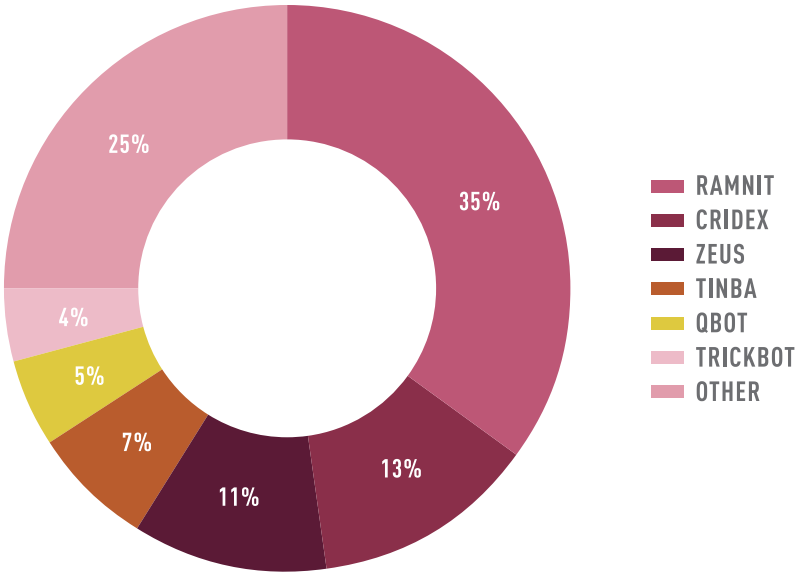


Banking Trojans are also among the stealthiest of all malware types. After a Trojan infects a user's PC or web browser, it will lie dormant and wait for the user to visit their online banking website. When the user does this, the Trojan is activated and uses keylogging to steal the victim's username and password and send it secretly to the criminals behind the attack. These criminals can then log into the user's bank account and transfer funds, usually through a complex network of transactions to cover their tracks.

Many Trojans can perform sophisticated Man-in-the-Browser (MiB) techniques such as web injections or redirection mechanisms. With this attack type, the Trojan's actions in real time are disguised, subtly changing what the user's browser displays so that it appears as if transactions are proceeding normally while the theft is happening. Other tactics include displaying fake warning pages that ask a user to re-enter their login information, or showing users a fake logout page while keeping them signed into their accounts. The aim is to conceal the Trojans' actions from users for as long as possible, to enable the criminals to continue stealing from their accounts.

In addition, Banking Trojans are transitioning to mobile. These typically involve malware which displays fake overlays on the mobile device's screen when a user tries to use an application. The overlays look the same as the login pages of banking apps, and can steal login credentials, or intercept SMS messages from the user's bank, enabling the criminal to harvest mobile transaction authentication credentials.

Chart: The Most Prevalent Banking Malware Globally
Source: Check Point Threat Cloud



Ramnit is the most prominent banking Trojan of the past year. It first appeared in 2010 and has remained active ever since. Ramnit's popularity is in line with the exposure by Check Point researchers of a massive new 'Black' campaign based on the banker. The campaign turned the victim machines into malicious proxy servers and resulted in over 100,000 infections. Shortly after the 'Black' campaign was shut down, a new Ramnit campaign emerged, distributing the AZORult info-stealer and downloader, via the RIG and GrandSoft Exploit Kits.

Trickbot is another dominant banking Trojan widely observed in 2018 that reached the top of the global, Americas and EMEA rankings. As an advanced malware based on plugins, Trickbot is constantly being updated with new capabilities, features and distribution vectors. This enables Trickbot to be a flexible and customizable malware that can be distributed as part of multi-purpose campaigns. In 2018 we witnessed Trickbot being delivered via multiple global spam campaigns, as well as creatively cooperating and sharing profits with the IcedID banking malware.

CONCLUSION

We are currently witnessing the continuous rise of the underground Malware-as-a-Service industry. This unique business model paves the way for new, unskilled attackers to enter the malware distribution arena. Anyone willing to pay can easily obtain the suitable tools and services needed to launch any kind of cyber -attack.

While this may not be a completely new phenomenon, over the past year we have witnessed a significant growth in attacks orchestrated with cyber weapons or products acquired via these underground services. When cyber crime is democratized, the number of cyber attacks increases.

As outlined in this report, mass scale ransomware attacks were much less common in 2018, though they were no less devastating. Instead, they became more targeted due to the higher profits they potentially promise when aimed against more specific targets. Indeed, 2018 saw threat actors also trying to keep a lower profile for their menacing activities.

In their place came massive cryptojacking campaigns that managed to infiltrate IT networks under the very noses of those guarding them. This is a worrying trend, for while cryptojackers infected ten times more organizations that ransomware, only one in five IT security professionals were aware that they were infected. After all, as we saw in the first installment of this report, malware such as cryptojackers and banking Trojans can easily serve many purposes and offer threat actors a back door through which more pernicious malware can be delivered.

Never does a day go by when organizations are not under constant attack from the ever growing number of malware, infiltrating IT networks from an increasing number of entry points. In the next part of this report we will investigate where the weakest entry points for these networks are and how cyber criminals exploit them to gain unauthorized access to the data stored there.