CYBER THREAT LANDSCAPE REPORT 2019 - 2020



TABLE OF CONTENTS

Executive Summary	3
Top Takeaways	4
Malware Trends in 2019	5
Top Five Malware Threats	6
Malware Infection Rates in 2019	7
Be Very Aware of Ransomware: More Targeted and Destructive	8
Top Five Ransomware	10
Sprawling Spyware Trends	11
Top Five Spyware	12
A Look at Data Breaches in 2019	13
Note-Worthy Data Breaches	14
Wipe Outs Are Moving In: The Increase in Wiper Attacks	15
MAC-OS Threats	16
Top Five MAC-OS Threats	17
Android Threats	18
Top Five Android Threats	19
Deep Instinct's Most Interesting Discoveries	20
New and Emerging Trends	22
Financially Motivated Actors Become More Professional and Serious	22
Connections Between Nation-State and Financially Motivated Attackers	23
The State of AI in Cybersecurity	24
2020 Predictions	25
About Deep Instinct	26

EXECUTIVE SUMMARY

2019 was a very eventful year for cyber security. The sophistication and daring of threat actors grew, and the financial damage caused to companies as a result of cyber attacks became apparent. Here are just a couple of examples:

Ransomware attacks became highly targeted and aimed at large enterprises. Ransomware actors preferred to perform targeted and highly lucrative attacks – with ransom demands from successful attacks reaching millions of dollars. Also, ransomware actors started threatening to leak data of attacked organizations uncooperative in paying the ransom.

Emotet becomes the most prominent threat in the landscape. After being inactive during the summer months, Emotet resurfaced in September, with a very large attack wave, and quick mutations. Throughout 2019 Emotet was seen working in collaboration with many other malware campaigns, dropping ransomware, spyware, and backdoors onto systems initially infected by Emotet.

During 2019, Deep Instinct uncovered several new and unique malware campaigns, while protecting its customers from ceaseless attacks. The campaigns uncovered include Trickbooster, an email harvesting module used by Trickbot; Legion Loader, a malware loader which can drop multiple different malware campaigns onto victims; and Separ, a credential stealer which was responsible for the credential theft of hundreds of organizations.

Deep Instinct's 2019 Threat Landscape Report represents Deep Instinct's view of the threat landscape. The report discusses trends seen during 2019, and provides concrete data on the changes in the landscape throughout the year. We hope this report will provide the reader with a better understanding of the present threat landscape and its trajectory.

3

FOREWORD

Deep Instinct is pleased to release it's 2019 Threat Landscape Report. The information presented in this report is based on D-cloud, Deep Instinct's proprietary file reputation database. The database receives data from multiple feeds, including well known threat intelligence providers, curated sources maintained by Deep Instinct's research group, and production data from Deep Instinct's customer base. The proprietary database provides real time information on threats, for the purpose of supporting Deep Instinct's research efforts and the optimal security of our customers. The analysis in this research study takes into account hundreds of millions of attempted attacks, that occurred everyday throughout 2019 within our customer environments.

Using the vast array of information that we gathered, we then started to go deep in the attempt to make sense of it all. We extrapolated on these findings to predict where the future of cybersecurity is heading, what it is that motivates attackers and most importantly, what are the steps that we can take now, in order to protect ourselves in the future.

TOP TAKEAWAYS

01

Financially Motivated Actors Ramped Up Their Game

Financially motivated actors have become more professional and widened their techniques and procedures in order to make a profit. Techniques which were once mostly deployed by nation states, such as fileless attacks, or extremely targeted attacks, are now also being carried out by cybercriminals. This was especially observed in the evolution of ransomware and spyware, where more groups are utilizing more sophisticated and evasive malware.

04

Destructive Malware – Wipers Were Back in the Game

A wiper, though simple in action, has a devastating and destructive effect on its targets. Wipers, which irreversibly damage data, were being used prolifically in the wild in the early 2010's, and have resurfaced in highly targeted attacks against industrial organizations. 2019 saw many such attacks, showing the effect of wipers on business is disastrous. With developments seen in the ransomware domain in 2019 by adding "wiping" features to its arsenal, the threat from wipers might become more serious than ever before.

02 The Rise of Targeted Ransomware Attacks

Ransomware attack tactics have evolved – and instead of focusing on "economies of scale" and statistical success through mass scale infection of end-users, ransomware operators pivoted their attack tactics to be more targeted and thereby more lucrative. Attacks on large enterprises or critical services such as health, rescue services and local authorities, any business downtime carries significant risk. Attacks at this level can yield much larger profits, by demanding higher ransom payments and improved likelihood of payout. In turn, actors have begun using more advanced attack techniques, and a wider arsenal of threats. On top of this, ransomware attackers have threatening to publish encrypted data, and also have the capability to wipe infected machines.

03 Emotet and Trickbot Dominated the Landscape

Banking Trojans and Spyware have evolved as well, spearheaded by the banker-turnedbotnet Emotet, and the financial malware Trickbot. Emotet has been the most dominant and prolific threat for most of the year. Worked and used in collaboration by multiple threat actors, dropping Trickbot, Ryuk (Ransomware), and more. The malware has continuously evolved during the year, enabling it to gain a very wide install base. Trickbot, the most prominent financial malware of the past several years, has also evolved, and ended 2019 with several large attack waves. The scope of its success and operation was demonstrated by its huge target list of more than 250M email addresses.

05

Living Off The Land Attacks Were Heavily Leveraged

This year has seen several high-profile attacks which are based on the concept of Living Off The Land (LOTL). LOTL is employed by leveraging dual-use tools, which are either already installed in the victims' environment, or are administrative, forensic or system tools which while not malware per-se, can be abused and used maliciously. The abuse by Sodinokibi ransomware of several management tools such as Webroot Management Console and Kaseya VSA RMM enabled the actors to attack dozens of organizations by only targeting a single legitimate program. This example illustrates the impact and evasive nature of such attacks, especially when it comes to achieving lateral movement, privilege escalation and persistence.

PART TWO

MALWARE TRENDS IN 2019

The past year has seen yet another rise in the amount and impact of malware attacks. Organizations and individuals are beginning to understand the possible devastating affects of malware attacks, and the risks associated with them. Meanwhile, attackers are also realizing the profits they can reap from successful and targeted attacks and are evolving their malware accordingly.

The next section will cover the main trends which were seen in malware attacks in 2019, with a focus on spyware and ransomware, which are the two threat types which had the greatest impact this year. The section will also outline the ransomware and spyware campaigns which had the highest impact in 2019.



TOP FIVE MALWARE THREATS



MOST NOTABLE ANDROID THREATS

- CAMSCANNER
- AGENTSMITH
- PEGASUS
- CERBERUS
- FINSPY

MOST NOTABLE MAC-OS THREATS

- APPLEJEUS
- COOKIEMINER
- NETWIRE
- MOKES
- LINKER

MALWARE INFECTION RATES IN 2019

The table and graph below summarize the distribution of malware by type, as collected and analyzed by Deep Instinct's D-Cloud in 2019. The data in both the graph and the table is identical, and shows that during the year, the distribution of malware types changes, however it is clear that some malware types remained dominant throughout the year. Spyware dominated the threat landscape, while droppers, which are the vehicle through which other types of malware are downloaded and executed on machines, were also very common.

The re-emergence of Emotet in September, following three months of inactivity, can also be seen clearly, as the ratio of spyware in the threat landscape significantly increased in Sep-

tember. Interestingly, though ransomware make up only a small portion of the threat landscape in terms of the total amount of unique threats, it is overly represented in terms of the impact of ransomware attacks.

In addition, we can see miners make up a very small portion of the threat landscape, and are less prominent than in 2018. This is due to two main factors. The first is the drop in the price of cryptocurrencies compared to 2018. The second is the fact that many mining malware campaigns have become more targeted, and aim to infect cloud servers, as they offer much more processing power than regular endpoints.

Month	Spyware	Dropper	Virus	Backdoor	Worm	Ransomware	Miner
Jan	79.75%	11.67%	3.32%	1.73%	1.87%	0.68%	0.98%
Feb	94.78%	2.36%	1.08%	0.56%	0.52%	0.62%	0.07%
Mar	82.54%	9.41%	1.12%	1.79%	0.74%	3.86%	0.53%
Арг	47.86%	25.55%	2.59%	10.64%	3.89%	8.43%	1.04%
May	44.64%	18.78%	3.83%	5.60%	22.42%	3.64%	1.08%
Jun	31.53%	43.99%	6.16%	8.41%	5.41%	4.20%	0.30%
Jul	24.57%	43.64%	5.20%	10.12%	7.23%	8.09%	1.16%
Aug	22.11%	30.04%	9.96%	27.58%	3.35%	6.17%	0.79%
Sep	48.09%	25.07%	4.25%	6.74%	10.70%	1.91%	3.23%
Oct	40.33%	23.89%	6.82%	17.13%	3.50%	8.28%	0.06%
Nov	67.88%	10.34%	16.84%	2.87%	1.08%	0.78%	0.20%
Dec	48.70%	14.12%	17.91%	14.59%	2.25%	2.02%	0.42%
Yearly Avg.	71.52%	12.31%	5.43%	5.21%	2.65%	2.37%	0.50%



BE VERY AWARE OF RANSOMWARE

MORE TARGETED AND DESTRUCTIVE

Ransomware has continued to be a threat in 2019. The potentially quick and very large profit gained by a successful ransomware operation has led many attack groups to develop and evolve their ransomware campaigns.

Since large-scale ransomware infections such as CryptoLocker and CryptoWall in 2013-2014, Cerber and Locky in 2016, and WannaCry in 2017, the evolution of ransomware and sophistication of attacks, gained momentum with Gandcrab and Ryuk in 2018 to Sodinokibi in 2019. Particularly as the aim shifted towards infiltrating and extorting businesses and organizations across different sectors all over the world.

The attacks involving ransomware became more targeted and focused on organizational entities rather than regular PC users. There are a couple of obvious reasons for this trend. First, organizations have more financial prospects than individuals, allowing threat actors to demand a higher ransom price. Also, it is more likely that organizations will value their data more than regular end users, where losing data might affect their operations and lead to greater financial loss, making them more willing to pay the ransom. When these organizations are in charge of critical services or infrastructure, such as hospitals or nuclear power plants, the effect of ransomware infections can be extremely critical. This year, local and state governments became one of the most popular targets of ransomware infection campaigns, more so than in previous years. Infiltrating and infecting an organization's network is not an easy task and sets a high bar for a threat actor's level of expertise. Very often, to make such operations possible and successful, requires a group of several individuals working together, making these campaigns more feasible by various well-established APT groups which are more experienced in compromising organizations' networks. This also requires advanced knowledge of lateral movement, as these targeted attacks focus on infecting only the key areas inside an organization, and this requires knowledge of the organization's network. On March 18th of 2019, Norwegian-based "Norsk Hydro", one of biggest aluminum manufacturers in the world, was affected by a devastating LockerGoga ransomware attack. The investigations are still in progress, but according to initial investigation reports, at least two threat groups worked together to issue this attack. According to other reports, this attack has links to the Russian threat group GrimSpider.

Another way of reaching key points inside an organization is the abuse of management tools used by that organization. This attack method was used by several prominent ransomware families in 2019. One such example is the Sodinokibi ransomware, which exploited several management tools, such as Webroot Management Console and Kaseya VSA RMM. Once attackers accessed these programs, they were able to perform actions on all systems managed by it.



THE MOST PROMINENT RANSOMWARE FAMILIES

BE VERY AWARE OF RANSOMWARE

MORE TARGETED AND DESTRUCTIVE

Nevertheless, spam campaigns and social engineering aimed at organization's employees remain (and probably will continue to remain) a popular attack vector. Demonstrating once again, that it is much easier to effectively "hack" a human than a computer. It only takes a single employee that will double-click and execute an emailed attachment to infect a whole network in a blink of an eye. In 2019 however, several examples of zero-day vulnerability exploitations occurred too. As an example, in April of 2019, companies from the IT sector using Oracle's Weblogic – a popular online transaction processing platform, were infected by the Sodinokibi ransomware delivered as a result of an exploited zero-day vulnerability (CVE-2019-2725) found in Weblogic. Aside from exploiting the zero-day vulnerabilities, the unpatched software is still one of the main reasons for threat actors being able to infiltrate a network. A good example for such scenarios are the attacks with RobinHood ransomware on computer systems serving Baltimore city government. In this incident it later appeared that attackers were using the EternalBlue vulnerabilities in the SMB protocol (stolen from NSA by the Shadow Brokers APT group and leaked publicly in 2017) after two years since Microsoft's patch release.

The targets have become bigger, the ransom price has increased and the financial damage to affected entities in 2019 became more conspicuous. The average cost of businesses' downtime as a result of ransomware in 2019 is estimated at \$141,000, a significant increase compared to \$46,800 from the year before. Overall, ransomware total damage cost in 2019 already exceeds the predicted \$11.5 billion and the tally is still being counted. To avoid the extremely high damage costs brought by ransomware in 2019, organizations are expected to spend more money on cybersecurity solutions in 2020.

\$141,000

The **cost of business downtime** as a result of Ransomware

Source: Datto



Source: Cybersecurityventures

TOP FIVE RANSOMWARE

Sodinokibi LockerGoga Ryuk Megacortex WannaCry

Sodinokibi

Sodinokibi, AKA REvil, is the most prominent ransomware campaign of 2019. It first appeared in the wild shortly before the end of operations of the Gandcrab ransomware, in April 2019, and has since been involved in several high-profile targeted attacks, mostly against companies and government organizations.

The attackers developing and spreading the ransomware have used several different tactics in their attacks, including use of zero-days, powershell scripts, targeting of large corporations, and in some cases, successfully conducting completely fileless attacks. Sodinokibi actors performed several notable attacks in 2019, including attacking 22 municipal governments in Texas, abusing management programs to attack dozens of organizations, demanding \$3 million from Travalex after a successful attack, and more.

This ransomware campaign best signified the trend of ransomware attackers moving towards highly targeted attacks, aimed at large enterprise networks.

LockerGoga

LockerGoga is a ransomware which first appeared in the wild at the beginning of 2019, most known for attacking major industrial firms in Europe. Its first high-profile attack was on the French company Altran Technologies, on January 24th, which was followed by another infamous attack on the Norwegian firm Norsk Hydro on March 19th. In both cases LockerGoga used a valid digital certificate signed by the companies: MIKL LIMITED, KITTY'S LTD, ALISA LTD. As a result of the attack, Norsk Hydro reported losses of up to \$70 million.

The ransomware encrypts a variety of file types and appends the .locked extension to encrypted files. Due to the fact that the ransomware spawns a new process for each file it encrypts, the encryption process tends to be slower than other ransomware families.

Ryuk

Ryuk ransomware was first seen in the wild in August 2018, and has since been involved in numerous targeted ransomware attacks, including several high profile ransomware incidents, such as attacks against Florida municipalities, which netted the criminals more than \$1.1M. As can be seen from this example, the actors behind Ryuk also target large enterprises, and demand very high ransom amounts. Several updates of Ryuk have appeared since its release, in its latest update, in September 2019, Ryuk was programmed to steal confidential military, financial, and law enforcement files. Ryuk is often distributed as a secondary payload of Emotet or Trickbot, which are spread through spam emails.

Megacortex

MegaCortex is another highly targeted ransomware campaign, which first appeared in the wild in May 2019, with attacks against large organizations. In these attacks, Megacortex used both manual and automated processes to infect a small number of victims for ransom. In its first version, the main Megacortex payload required a password in order to execute, and so could only be executed manually by the attackers. In its second version, released in August 2019, the password was hard-coded in the binary, meaning attacks are automated, and a larger number of victims can be obtained.

The ransomware was spotted attacking enterprises in the United States, Canada, and Europe, with ransom demands reaching as high as \$5.8 million.

Wannacry

WannaCry is a ransomware which was employed in a worldwide WannaCry cyber-attack which took place during March 2017. During this timeframe WannaCry managed to rapidly propagate, infect and encrypt hundreds of thousands of PCs in approximately 150 countries. Total damage estimates range from hundreds of millions to several billions of US dollars.

WannaCry's primary mode of propagation was the EternalBlue exploit, which targets a vulnerability in Microsoft's Sever Message Block (SMB) protocol. This exploit was originally developed by the US National Security Agency and was leaked online by the "Shadow Brokers" group a few months prior to the attack. While Microsoft had released patches to mitigate the exploit prior to the attack, these went unapplied by many victim organizations, leading to their compromise by the malware.

The effectiveness of the malware can still be clearly seen today, almost three years later, as the malware continues to spread and mutate in the wild. This is mainly due to the slow, and in some cases non-existent, patching routines used by companies and individuals, which enables WannaCry to continue exploiting EternalBlue. However, Cryakl activity hasn't been stopped for good and it continues to infect victims globally.

SPRAWLING SPYWARE TRENDS

EMOTET AND TRICKBOT ARE THE MOST PROMINENT MALWARE CAMPAIGNS IN 2019'S THREAT LANDSCAPE

Spyware has not remained behind in 2019. Various types of spyware, such as financial malware, banking trojans, information stealers, and the like, evolved last year, with several strains dominating the threat landscape. The next section outlines and describes the top five spyware families seen by Deep Instinct's D-Cloud in 2019.

Emotet

Emotet has been a fixture in the threat landscape since its discovery in 2014. This highly sophisticated and constantly evolving malware, which started its life as a banking malware, but has morphed into a dropper. It is distributed by means of massive, global spam campaigns targeting both home users and enterprises. It features malicious office files which are also noted for their high level of sophistication.

During recent years, 2019 included, Emotet has served mainly as a delivery mechanism for a host other malware, including Trickbot, IcedID, Gootkit, Qakbot, other malware, ransomware and spam bots.

Emotet is historically known for its "seasonal" operation, with 2019 being no different. Emotet went on hiatus for the summer months, leaving the stage open for a massive increase in TrickBot distribution during that time. However, Emotet

returned in full swing in September, in attack waves which have not ceased since.

TrickBot

Active since 2016, and constantly innovating, TrickBot is another prominent feature of 2019's threat landscape. Much like Emotet, TrickBot started its life as a banking malware but has evolved into highly modular multi-purpose malware, capable of both information theft, financial theft, lateral movement and follow-up malware download. Two such notable companions are Ryuk, a ransomware responsible for several high-profile incidents and TrickBooster, a spam bot which is responsible for the collection of a massive email address list. It is speculated that the Email list was harvested from its victim's email accounts and used to distribute TrickBot.

2019 saw multiple milestones for TrickBot, among these are the targeting of <u>RDP credentials</u>, VPN and SSH keys, bypassing windows defender, experimenting with fileless techniques, and fielding highly advanced modules intended to serve APT actors.



THE PREVALENCE OF EMOTET AND TRICKBOT IN 2019

```
DEEP INSTINCT
```

TOP FIVE SPYWARE

• Emotet • Ursnif • TrickBot • QakBot • IcedID

Emotet

Emotet is one of the most prevalent financial malware threats of the last years. It first appeared in German speaking countries in Europe around mid-2014, and after two years without significant activity, Emotet reappeared in 2017, attacking ever since, targeting the UK and the US.

From its very first version Emotet spread mainly via spam campaigns, imitating financial statements, transfers and payment invoices. Once it is dropped and run, Emotet intercepts and logs network traffic, injects into browsers and tries to access banking sites, in order to steal and store financial data. Emotet has also recently evolved into a dropper, operating a botnet, and dropping additional malware onto the infected system once initial access is achieved. Emotet has been associated with additional malware families such as Trickbot, IcedID, Ryuk, and more.

Ursnif

Ursnif, AKA Gozi, is a banking Trojan which first appeared in 2007 and has since been part of numerous attack campaigns and evolutions. Since its creation Ursnif has targeted many countries, with its main targets being Europe, Japan, Australia, the US and the UK. The malware usually spreads through targeted email phishing campaigns using malicious attachments. The main targets of Ursnif are banks and financial institutions, but the malware can also target non-financial companies, and individuals, in order to steal as much information as possible.

Ursnif steals user banking information, such as banking related credentials and credit card numbers, and can also steal other personal data, such as email and social network credentials, and contents of files from the infected computer. Ursnif's code has been leaked repeatedly over the years and has been used, modified and upgraded extensively, giving rise to many different yet similar variants.

TrickBot

TrickBot is a sophisticated banking malware that targets individuals, small-to-medium businesses and enterprise environments targeting bank account credentials, financial data and personal information in order to carry out financial fraud and identity theft.

Ny Qakbot monitors the browser on the infected machine to detect when victims interact with an online banking website, in order to steal credentials. Additionally, Qakbot collects further information from the infected machine including IP address, origin country, cookies and other system information.
s, and icedID
lcedID is a modular banking trojan active since September 2017, mainly targeting businesses in the US and the UK. It mostly

system passwords.

removable drives.

QakBot

mainly targeting businesses in the US and the UK. It mostly targets the finance industry, aiming to attack banks and credit card companies, as well as e-commerce websites. IcedID tends to be distributed as a secondary payload of Emotet, another highly active banking trojan. Once executed, it has worm-like abilities that allow it to propagate to additional machines on a network, as well as simple evasion techniques such as only operating after the machine restarts. IcedID manipulates the victim's browsers to display a correct URL address with a valid SSL in banking websites, while redirecting the traffic to a fake website, aimed at stealling credentials.

It first appeared in 2016, and became a prevalent threat,

spreading via malicious documents in mass emails. Ursnif

became known for its form rapidly with different capabilities

depending on the campaign. Its different malicious abilities and

evasion techniques are built into a module architecture which

campaign, in order to evade detection and operate a range of attack techniques. Due to its modular architecture, Trickbot

allows for easy swapping, modifying and rebuilding for each

has had several abilities throughout its different campaigns,

other than credential stealing. It could be either operating as a

backdoor, having network spreading abilities, email harvesting

features, or all the above. In some cases, Trickbot had delivered

Qakbot is a popular baking Trojan active in the wild since 2009.

Its main features are stealing online banking credentials and

other financial information. Additionally, Qakbot possesses worm features allowing it to spread through network and

ransomware-like screen lock option, which is meant to steal

A LOOK AT DATA BREACHES IN 2019

A data breach is an unauthorized collection of private or confidential data and its release to an unauthorized environment. In recent years data breaches have been on the rise, and have increased by 55% since 2012, with the number of exposed records in 2019 being 15 times more than in 2012. Since breaches can be very lucrative to hackers, who sell the leaked data, or use it to blackmail a company by threatening to release sensitive information, the increase in data breaches is expected to continue into 2020.

This type of attack can cause great damage to companies and even bring them to bankruptcy. In past events clients have filed lawsuits against a breached corporation, financially lucrative contracts with targeted organizations have been cancelled and GDPR (General Data Protection Regulation) fines have been issued. One such example was the case of AMCA (American Medical Collection Agency), which as a result of being breached in 2018, lost its biggest corporate clients. Affected individuals, whose information was compromised, sued claiming the organization failed to report the breach on time. By June 2019, the AMCA had filed for bankruptcy.

15x

Increase in the number of **Exposed Records** since 2012

Source: Wikipedia

ANNUAL NUMBERS OF DATA BREACHES AND EXPOSED RECORDS



NOTE-WORTHY DATA BREACHES

Capital One

On July 19th, 2019, Capital One Financial Corporation- one of the largest banks in the United States, found out it had been breached in March earlier that year. The breach had started with the compromise of an account, that may had been possible through a configuration vulnerability. With the compromised account in hand, the attacker was able to access Capital One's cloud infrastructure, hosted by AWS (Amazon Web Service), configure a storage gateway and download data to the threat actor's computer, with the Linux command-line utility 'dd'. The data of 100 million US users and 6 million Canadian users was compromised by the breach. This data included phone numbers, email addresses, identifiable details, self-reported income rates and in some cases, credit card balances and social security numbers. Allegedly, the breach had been conducted by Paige Thompson, who did not release any of the collected data to the public, nor tried to sell it on the dark web, their objective still remains unknown.

Continued Fallout from the Equifax Breach

Equifax, one of the three largest consumer credit reporting agencies in the world, announced in September 2017 that it was breached. Hackers were able to access records of 145 million Equifax customers, including their full names, social security numbers, birth dates, addresses, and driver license numbers. On March 2018, Equifax announced that 2.4 million additional customers were affected by the breach.

The after effects of the breach were severe, with the scale of the breach being historically unprecedented. So far, Equifax has agreed to pay at least \$575 million, and up to \$700 million, to compensate victims of the breach. There have been many investigations as a result of the breach, which in part led to the sentencing of Equifax's former CIO, and another Equifax executive, after they were found guilty of insider trading, selling their stocks before the breach was discovered.

LifeLabs

LifeLabs, Canada's leading provider of laboratory diagnostics and testing services, was hacked in October 2019. In the hack, which is considered to be the largest ever in Canada, the private data of LifeLabs 15 million customers was stolen by the hackers, who demanded a ransom from LifeLabs. To provide some perspective on the number of stolen records, 15 million customers represents around 40% of the population of Canada. The data stolen in the breach included names, home addresses, email addresses, usernames, passwords, and health card numbers. Several class lawsuits have been filed against LifeLabs as a result of the breach, with one lawsuit seeking over \$1 billion in damages.

100M

The Data of 100 million US Users was **Compromised**.

Source: <u>Reuters</u>



in **Damages** filed against LifeLabs as a result of being breached.

Source: CpoMagazine

WIPE OUTS ARE MOVING IN

THE INCREASE IN WIPER ATTACKS

2019 was a very successful year for cybercrooks operating ransomware attack campaigns. Nevertheless, the destructive attacks of a close relative of ransomware, wiper malware, could be seen in 2019 too. Reminding us that wipers are ever relevant and even more devastating.

The first wipers and ransomware attacks both began to appear in 2012, damaging victims' data. However, while ransomware is used for revenue gain, wipers are intended for pure destruction of data. Usually, the distinction between ransomware and wipers is clear, but there are instances where what would have seemed as ransomware at first, ended up being tagged as wiper under a ransomware disguise. Like NotPetya in 2017, German-Wiper was an example of such a scenario in 2019 – despite the ransom demand presented to its victims, the data on infected machines wasn't encrypted, but overwritten with zeros and couldn't be reversed to its initial state.

Furthermore, a couple of ransomware variants seen in 2019, LockerGoga and MegaCortex, were found to provide its operators with destructive features that might pose them as wipers. A new version of LockerGoga, after encrypting the files would disable the infected machine's network adapter, change the admin password and log out. This meant victims were unable to read the ransom note and the files were left encrypted for good. MegaCortex ransomware included a disk wiping feature threatening that a victim unwilling to pay the ransom will not only lose the encrypted data, but the whole system. This is an interesting development seen in ransomwares in 2019 hinting that this trend might further evolve in 2020.

Target-wise, a vast majority of wiper targets are organizations, often from the industrial sector, rather than end users which are more likely to be targeted by ransomware. Although lately the number of ransomware attacks on organizations is on the rise compared to previous years.

The threat actors choosing to attack with wiper malware tend not to be financially motivated, rather their goal is data destruction and disruption of a targeted organization's operation. This is what nation-state hacking groups usually seek to achieve, apart from their espionage operations against rival targets. Like in previous years, Iran had made headlines in the media in 2019 (and the beginning of January 2020). Two Iranian statesponsored hacking groups, xHunt and APT34 (aka Helix/OILRIG), were held responsible for attacking organizations from industrial and energy sectors in the Middle East, by ZeroCleare wiper in December and later with its derivative Dustman in January 2020. According to the initial reports, ZeroCleare and consequently Dustman have similarities with another wiper variant Shamoon v3, which is also linked to Iran and seen in attacks on oil and gas companies in the Middle East and Europe in 2018. Like Shamoon v3, ZeroCleare and Dustman have employed EldoS RawDisk driver to wipe the disk too.

A wiper, though simple in action, has a devastating and destructive effect on its targets. Although still rare, wipers are again proving to be a real and significant threat to organizations and businesses. As opposed to ransomware, where the damage can be allegedly reversed, the effect from wipers is far more disastrous, especially when a data backup strategy is weak or absent. With developments seen in the ransomware domain in 2019 by adding "wiping" features to its arsenal, the threat from wipers might become more widespread than before.



MAC-OS THREATS

Though it is often said that MacOS users do not need to worry about malware targeting the OS, every year it becomes clearer that this is not the case. In the past several years there has been a constant rise in the number and the sophistication of malware targeting MacOS systems. In addition, there has also been a rise in the numebr of potentially unwanted programs (PUA) targeting MacOS systems.

In the past year, several sophisticated APT actors targeted MacOS systems. The most notable group was the North-Korean attributed Lazarus group, which was linked to five new malware families discovered during the year. Overall, the growth in the number of malware and PUA on MacOS systems has been immense in the last several years. However that growth seems to have slowed down, with threats plateauing since 2018.

The total number of threats per month in the past three years can be seen below. Quantities have normalized, in this diagram threat numbers in January 2017 have been set to 1. The data was collected and analyzed from our Threat Intelligence infrastructure, D-Cloud.

MAC-OS THREATS PER MONTH 2017-2019



TOP FIVE MAC-OS THREATS

• AppleJeus • CookieMiner • Netwire

Linker Mokes

AppleJeus

AppleJeus is a campaign by Lazarus a North Korean-based group, which was first seen in the wild in 2018. The 2019 version of the campaign, which appeared in December 2019, had fileless attack techniques, and the ability to perform remote downloads and in-memory execution of files

CookieMiner

CookieMiner is a crypto-stealer targeting MacOS, which first appeared in January 2019. The malware collects cryptocurrency related cookies, and user credentials in its attempt to steal cryptocurrencies. In addition, the malware can not only steal other private data belonging to the victim, but can co-opt the victim's CPU for crypto mining.

NetWire

Netwire is a backdoor for MacOS, which first appeared in 2012. The malware made another appearance in June 2019, targeting Coinbase and other cryptocurrency exchanges. The malware, together with another family of malware named Mokes, made use of two Firefox zero-day vulnerabilities, CVE-2019-11707 and CVE-2019-11708, to deliver itself to its targeted list of victims.

Mokes

Mokes is a macOS spyware which first appeared in 2016. The malware appeared in June of 2019 in a targeted attack against cryptocurrency exchanges, together with NetWire (for more details see the NetWire entry). The malware can steal a variety of user data, take screenshots, log keystrokes and more. It is a cross-platform malware that has also attacked Windows and Linux systems in the past.

Linker

Linker first appeared in June 2019 and abused a GateKeeper zero-day which was disclosed in May 2019 but was left unpatched by Apple. Linker was probably developed by the same group responsible for the development of a very widespread MacOS adware, called SurfBuyer.

ANDROID THREATS

Near the end of 2019, the number of active Android devices reached the 2.5 billion mark, making it a large and attractive target for malware authors. In addition, with Android penetrating more than 76% of the Mobile OS market, naturally it is the preferred mobile operating system targeted by attackers. The main objective of attackers is obtaining profit – most commonly through adware, ransomware, selling personal data after it's stolen, or forcing devices to call expensive premium numbers owned by attackers.

The proliferation of Android malware has successfully included the largest application store, the Google Play Store. Even with improved detection rates, Google Play Protect still could not stop the entry of several hundred malicious Android applications into the store, affecting hundreds of millions of users. Examples of malicious programs with an extremely wide install base which managed to enter the Google Play Store is the CamScanner app (>100M downloads). The app had an adware component entered into it, and Agent Smith malware, which replaced installed apps with a malicious version on more than 25 million devices. Several APT actors have been acting extensively in the Android landscape. Malware written by advanced attackers such as the North-Korean attributed Lazarus Group, and the Vietnam-attributed OceanLotus group has been discovered in the wild in the past year. This is an ongoing trend that is expected to continue, as nation-state backed APT actors develop tools on any platform which is needed in order to reach their targets.

The total number of threats per month in the past three years can be seen below. Quantities have normalized, in this diagram threat numbers in January 2017 have been set to 1. The data was collected and analyzed from our Threat Intelligence infrastructure, D-Cloud.

It can be seen that total Android threat amounts in 2019 have decreased in relation to previous years. This might be due to the fact that threat actors prefer to develop malware which targets Windows systems where more profit can be gained, due to both the larger install base and the higher processing power of targeted machines.

ANDROID THREATS PER MONTH 2017-2019



TOP FIVE ANDROID THREATS

Camscanner AgentSmith

• Pegasus • Cerberus • FinSpy

CamScanner

In August 2019 it was discovered that CamScanner, an extremely popular and widespread application, present in the Google Play Store, included a dropper component. The dropper was used to drop other programs, and adware components, onto devices, however it could also be used to deliver malware.

AgentSmith

AgentSmith is malware which was found to have infected more than 25 million Android devices in July 2019. The malware attacks by replacing real applications with fake versions of them – and the fake applications then act as adware and present the user with ads. The attackers can also profit by hijacking ad events on the campaign and reporting them to an ad broker with the ID of the attacker. Though AgentSmith was used to download adware, it could have been used to download spyware and other types of malware.

Pegasus

Pegasus is a highly sophisticated spyware, created by NSO Group. Pegasus targets iOS and Android systems, and is sold by NSO Group to government and other global organizations. Since its first discovery in 2016, Pegasus was involved in several controversies. In October 2019 What's App sued NSO group, accusing the group of exploiting a vulnerability in WhatsApp in order to target more than 1,000 different targets, including human rights activists. The vulnerability, dubbed CVE-2019-3568 can lead to installing spyware on devices without any interaction from victims – all that is needed is to make a WhatsApp call to the target device.

Cerberus

Cerberus is an Android financial malware, which first appeared for sale in underground forums in the summer of 2019. In addition to having several anti-sandboxing capabilities, the malware is able to steal credentials, take screenshots, record keystrokes, and perform many other spyware activities.

FinSpy

FinSpy AKA FinFisher is a commercial surveillance program which was first sold in 2012. The spyware program re-appeared in July 2019, targeting Android users in Myanmar. Like other types of advanced spyware, the malware is able to steal credentials, take screenshots, record keystrokes, and perform many other activities.

DEEP INSTINCT'S MOST INTERESTING DISCOVERIES

THROUGHOUT 2019 DEEP INSTINCT PROTECTED ITS CUSTOMERS EXTENSIVELY, FROM A WIDE VARIETY OF THREATS

Below we summarize some of the most interesting threats we analyzed in 2019, and describe the potential damage of these threat if they would not have been prevented.

Trickbooster

Overview: <u>Trickbooster</u> is a malicious email-based infection and distribution module being used by Trickbot. From our research into the module, we uncovered a database with 250 million harvested email addresses, many of which belong to corporations and government agencies. Trickbooster harvested the email credentials and contacts from address books, and then sent malicious spam emails from the victim's compromised account. We believe this module is used by Trickbot for several purposes; propagation and infection, spreading spam for monetization purposes, and harvesting email accounts which can then be traded and used by other campaigns.

Risk: If Trickbooster would not have been prevented, it would have harvested emails from the attacked organizations and their respective business partners. It would then have targeted these email addresses with Trickbot payloads, or payloads of other malware.

Legion Loader

Overview: Legion Loader is an advanced malicious dropper, which can drop multiple types of malware as payloads. The dropper can download multiple types of info-stealers, backdoors, a fileless crypto-currency stealer built into the dropper, and occasionally a crypto-miner as well. The malware which was dropped by Legion Loader includes several well-known families, such as Vidar, Predator the Thief and Racoon stealer, in addition to an advanced Crypto-Currency stealer and an RDP backdoor.

Risk: If this dropper was not prevented in the customer environment, it would have downloaded at least one of a very large variety of malware families, which could perform a variety of actions on victims' computers. Since Legion Loader is very diverse, it could infect organizations with spyware, backdoor, and also ransomware.

Separ

Overview: <u>Separ</u> is a long-lived credential stealer, first appearing in the wild in 2013 it has continued to persist in various forms. The credential stealer is unique, as it uses a combination of very short scripts or batch files, and legitimate executables, to carry out all of its malicious business logic. Therefore, Separ is an excellent example of the advanced and evasive attack technique commonly termed as "Living Off the Land".

Risk: Several days after the attack was prevented, we managed to analyze the credentials stolen by Separ in its new attack wave. At that time, the attack affected hundreds of companies, with thousands of credentials stolen and uploaded to the attacker's severs. This shows the damage done to the hundreds of companies where Separ was not prevented.

DEEP INSTINCT'S MOST INTERESTING DISCOVERIES

Phost miner

Overview: The sophisticated <u>Phost Miner</u> was prevented at a large aviation enterprise. Investigation of the prevention events uncovered a persistent, fileless, crypto-currency (Monero) miner which uses TOR infrastructure to remain anonymous. The malware is composed of a multi-stage PowerShell command which employs reflective-PE injection and run-time code compilation to inject malicious executable content hidden in the Windows Registry directly to the victim machine's memory.

Risk: If the miner is not prevented, it will abuse the processing power of the victim machine to mine cryptocurrency. Depending on the infected machines, this could have a very serious effect on the organization, as for example the miner might infect servers which are continuously tasked, and which perform critical tasks for the infected organization.

Formbook

Overview: FormBook is an info-stealer which first appeared on the scene as early as 2016. This malware has been marketed in underground hacking forums as having elaborate evasion capabilities and a powerful credential harvesting mechanism at a relatively low price. Since its creation FormBook has been widely used in malicious spam campaigns to infect victims and steal their credentials in multiple attack waves. An attack wave of FormBook from January 2019 used a new malware-friendly file hosting service, used by threat actors as a point of distribution for their malware. The file hosting service uncovered was a new malware hosting service that could be used in other malware campaigns as well.

Risk: If FormBook would not have been prevented in customer sites, it would have started stealing user credentials, including email logins and password, financial information, and more. These credentials could then be used for a variety of uses, such as financial theft, or even deeper infiltration into the attacked organization, through theft of credentials belonging to users in the organization.

NEW AND EMERGING TRENDS

FINANCIALLY MOTIVATED ACTORS BECOME MORE PROFESSIONAL AND SERIOUS

Based on our professional insight from the past year, we found a number of trends that we identified as particularly interesting; partially because of their unique configuration and behavior, but also because of the implications that these emerging trends hold for the future of cybersecurity.

During 2019, financially motivated threat actors improved their capabilities, became more professional and escalated their actions. As these actors improved their methods, researchers took more interest, learning more about their methods and TTP's, in order to better understand their activity. These are some of the developments that we have picked up on at Deep Instinct.

Ransomware Actors Start Leaking Data

The most substantial escalations in the activity of financially motivated threat actors occurred towards the end of 2019. Two prominent ransomware distributors began leaking victims' data, instead of only holding it hostage for ransom.

In November, the operators of Maze ransomware released 700MB of data stolen from their victim, Allied Universal, after the latter did not to pay the ransom. Though ransomware distributors had threatened to leak stolen data in the past if the ransom is not paid, 2019 was the first year such a threat was carried out. This represented a turning point where a financially motivated threat actor and a ransomware attack escalated into a data breach. Following the Maze ransomware incident was the Sodinokibi ransomware group, which publicly announced they will release victims' data in order to hold them accountable to GDPR violations if the victims refuse to pay the ransom, leveraging the high penalties of GDPR, CCPA and additional privacy law violations to add pressure.

In January 2020, the <u>Sodinokibi group had lived up to their</u> <u>threat as well, publishing 337MB of data</u>, allegedly stolen from Sodinokibi victims' computers , and Maze ransomware published <u>14GB of data stolen from another victim</u>.



NEW AND EMERGING TRENDS

CONNECTIONS BETWEEN NATION-STATES AND FINANCIALLY MOTIVATED ATTACKERS

In addition to the escalation in their actions, another trend we identified in 2019 was the deepening of the connection between state sponsored actors and financially motivated actors.

In December 2019, following an investigation of the "EvilCorp" group by the US authorities, the group was accused of stealing over a 100 million USD over several years of activity, using the Dridex banking trojan. The US Department of Treasury revealed that the leader of the group, a Russian individual who had been working in collaboration since 2017 with the FSB, <u>Russia's Federal</u> <u>Security Service, provided them with sensitive data and</u> <u>confidential documents.</u>

Though it is not the first time cyber criminals had been connected to nation-state espionage, the most well known is the case of <u>GameOver Zeus</u> in which the developer collaborated with the Russian intelligence services. This revelation as well as <u>reports on an alleged connec-</u> <u>tion between the TrickBot group and North Korean APTs</u> , further demonstrate how the lines blur between financially motivated actors and state-sponsored actors. In 2019, as well as 2018, we identified an increased use of fileless attack methods. Particularly conspicuous was a spike in abusing legitimate applications and native tools such as PowerShell for lateral movement and infection. This trend has been experimented on by both nationstate and non-state actors, with new ways to employ old methods, such as creating Steganographic payloads using WAV audio files.

These trends indicate that in 2020 we are likely see other bold moves, as financially motivated actors gain more confidence, improve their relations with stronger actors in the threat landscape, and get access to more sophisticated methods.

NEW AND EMERGING TRENDS

THE STATE OF AI IN CYBERSECURITY

There have been many interesting developments and breakthroughs in AI in 2019, also specifically in cyber-security related AI.

1. Deep Learning (the most advanced form of AI) is proving to be the most effective cybersecurity solution for threat prevention

Deep learning is inspired by the brain's ability to learn new information and from that knowledge, predict accurate responses. The ability of deep learning-based network to determine quickly and accurately whether a file is malicious, enables the analysis of files pre-execution, so that malicious files can be prevented preemptively. This is critical in a threat landscape, where real-time can sometimes be too late.

2. The expansion of deep learning models

During 2019, one of the major trends in AI was the rapid growth in size of deep learning models. This was an exciting trend because it meant that larger sets of data that are comprised of greater complexity can now be processed. The result is that instead of paying attention to large data combinations as the basis of data sets, the model is now learning in more granular detail and assigning meaning to smaller combinations.

3. The ability to manipulate machine learning classifiers

In recent years, adversarial learning, the ability to fool machine learning classifiers using algorithmic techniques, has become a hot research topic. However, 2019 has seen a diffusion of such research from the limited domain of image recognition to other, more critical domains, particularly the ability to bypass cybersecurity next-generation anti-virus products.

For more details on these developments and additional developments, read the article <u>The Coolest AI Breakthroughs of 2019</u>.



DI 2020 PREDICTIONS



Increase in the scope and rate of mutation and variant changes

Mutating malware is not a new phenomenon, and malware which changes some of its characteristics has already existed for many years. However, this year malware will mutate quicker, and more effectively. New attack waves of campaigns will include previously unseen samples on a daily basis, with mutations hiding the key functionalities of malware. This will be a serious challenge to security vendors, as they will have to deal with the constant changes of prominent malware campaigns.

Strictly fileless attacks will develop

Fileless attacks have been around for several years and have become more and more common in the attack landscape. However, most attacks which are termed fileless are not truly so, since they include at least one stage in which a file is written to disk. However, the increasing sophistication of attacks, and the growing use of scripts in malware attacks will enable attackers to start performing attacks which are strictly fileless.

Multi-Purpose malware will become more common

In the past several years several key malware campaigns changed their main purpose, with the most notable example being the move of Emotet from financial malware to botnet. We predict this year will see a large increase in "multi-purpose" malware, meaning that a malware campaign will no longer limit itself to its "traditional" functionalities. For example, ransomware campaigns will no longer just encrypt files, but will also regularly have the ability to steal information, spread within networks, wipe systems, and more. This will consolidate the threat landscape to a few key malware families with multiple capabilities.

Evasion will be more focused on evading AI-based technologies

The increasing use of AI technologies in cyber security will lead threat actors to attempt to evade AI-based security solutions. The more successful malware campaigns will be those who actively seek ways to bypass detection of AI-based solutions, leading to new evasion methods and techniques.

Nation-States will further explore and implement AI in offensive operations

The use of AI in cyber security has certainly not been ignored by nation state actors. Due to the large amount of resources at their disposal, nation states will be able to explore and implement offensive uses of AI in malware attacks. This will lead sophisticated campaigns to include AI based tools in their arsenal.

ABOUT DEEP INSTINCT

Deep Instinct is changing cybersecurity by harnessing the power of Deep Learning to prevent threats in zero time. The lightweight on-device, proactive solution protects against zero-day threats, APT and ransomware attacks with unmatched accuracy and speed. The only solution providing comprehensive defense, it is designed to protect against the most evasive known and unknown malware pre-execution, across endpoints, servers, and mobile devices, likewise it can be applied to most OSs and any file types.

To learn more, visit | www.deepinstinct.com

GET A DEMO

DEEP INSTINCT'S PREVENTION IN ACTION CASE STUDIES

What does it mean to have a security product that is focused on prevention, scanning files prior to execution? In Prevention In Action, we provide a number of case studies, where customers protected by Deep Instinct were able to prevent threats from entering their enterprise. The stories demonstrate how these companies saved millions in dollars and retained resources.



JOIN THE LEARNED FEW

NEW YORK GLOBAL HEADQUARTERS

501 Madison Ave Suite 1202 NYC, NY, 10022 USA

+1-212-981-2703

www.deepinstinct.com

TEL AVIV

23 Menachem Begin Rd 28th Floor Tel Aviv, 6618356 Israel

+972-03-545-6600

SYDNEY

Level 3 100 Harris Street Pyrmont NSW Sydney 2009 Australia

+61-1800-355-015



© Deep Instinct Ltd. This document contains proprietary information. Unauthorized use, duplication, disclosure or modification of this document in whole or in part without written consent of Deep Instinct Ltd.. is strictly prohibited.

info@deepinstinct.com

DEEP INSTINCT

26