

PANDEMIC CHAOS UNLEASHES MALWARE DISASTER

2020
CYBER THREAT
LANDSCAPE REPORT



TABLE OF CONTENTS

Executive Summary	3
Foreword	3
Top Takeaways	4
The Top Malware Trends of 2020	5
Top 5: Malware Families	6
Top 5: Ransomware Families	7
Top 5: Banking Trojan Families	8
Malware Trends by OS: Documents	9
Malware Trends by OS: Mac	11
Malware Trends by OS: Android	12
Malware Trends by Campaign: Emotet	13
Malware Trends by Campaign: Ransomware	15
Malware Trends by Campaign: Financial Trojans	18
Malware Trends by Campaign: PowerShell	20
Year's Most Interesting Discoveries	21
Cyber Insights: Effect of COVID-19 on Cybersecurity	23
Cyber Insights: SolarWinds Attack	24
Cyber Insights: Risks Present at US Elections	25
Cyber Insights: Adversarial Machine Learning	26
Cyber Insights: A Look Back at Our 2020 Predictions	27
Cyber Insights: 2021 Predictions	28
Cyber Insights: The Cost of an Attack in 2020	30
About Deep Instinct	31

EXECUTIVE SUMMARY

Virtual reality always appears to mirror the reality that's on the ground, and unfortunately, the turbulent year of 2020 was no exception. From 2019 to 2020 there was a distinct rise in the amount of malware in the wild, which is all the more visible when analyzing the progression from month to month. This rise was seen across all different malware types; from ransomware and spyware, to droppers and miners. However, not only did 2020 suffer from an increase in malware attacks, but the sophistication and daring of threat actors also grew, evident by the financial damage inflicted on companies as a result of these more cunning attempts.

Like any criminal underworld, the hazards of 2020 presented numerous opportunities to cyberthreat actors. The Coronavirus pandemic caused companies around the world to abruptly switch to a work-from-home module, inadvertently widening the organization's attack surface. Employees were no longer working from behind the safe confines of the corporate network.

Moreover, the pandemic, the US Presidential elections as well as the Black Lives Matter movement, were some of the hot topics that became the "cover stories"

in many phishing campaigns. The dropper documents accompanying these phishing campaigns were used to distribute secondary malware samples, such as worms, spyware and ransomware. Their objective was often the theft of Personally Identifiable Information (PII), and their efforts proved to be successful, potentially even beyond the expectations of hackers themselves.

This report represents Deep Instinct's current view of the threat landscape. The report discusses trends seen during 2020 and provides concrete data to verify the credibility of these developments. The information was sourced from our data repositories which are routinely analyzed as part of protecting our customers from ceaseless attacks. I hope this report will provide you with a better understanding of the present threat landscape and its future trajectory.

Regards,

Shimon N Oren

VP of Research and Deep Learning

FOREWORD

Deep Instinct is pleased to release its 2020 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. This wide cumulation of data is reflective of hundreds of millions of events that occurred during 2020.

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 2020 within our customer environments. Deep Instinct's team of researchers, who combined have several decades of experience, and many of whom served in various cyber intelligence units in the Israel Defense Forces, gathered the vast array of information. They extrapolated 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

Seized Opportunity Created by the Coronavirus Pandemic

Attackers take every chance they get to spread their malware, and the pandemic gave ripe opportunities, both in terms of the hysteria it created and the forced change in working and learning conditions. Since its outbreak, plenty of COVID-19 themed malware attacks have surfaced around the globe. We address this manipulation of the pandemic as it was used in ransomware and financial malware infections.

04

Stronger Partnership between Government and the Private Sector

A developing partnership between government departments and private sector vendors provides cautious reason for optimism. In the lead up to the US 2020 presidential elections, Microsoft collaborated with government departments, such as cyber intelligence units and district courts to bring down Trickbot. This partnership proved to be fruitful as much of Trickbot's infrastructure was significantly disrupted.

02 The Growing Prevalence of Emotet

One of the most prevalent financial malware and botnet threats this year, Emotet is addressed extensively in this report. From its very first version, Emotet spread mainly via spam campaigns, imitating financial statements and payment invoices. However this past year, Emotet evolved dramatically, developing its propagation capabilities to get an initial foothold inside an organization in order to drop other malware.

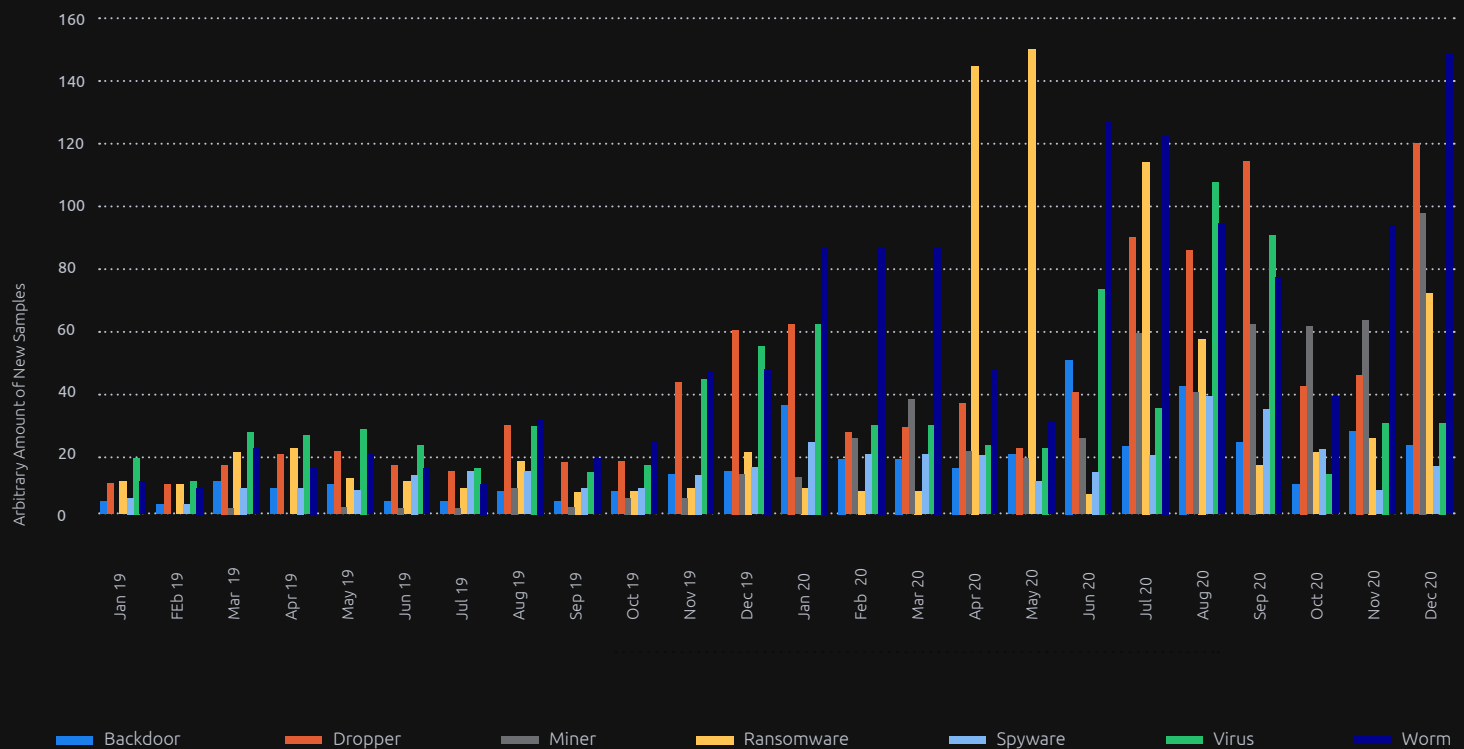
03 Double Extortion Becomes Standard in Ransomware Tactics

By the end of 2020, double extortion tactics became the new standard in ransomware, with ransomware developers even providing a warning that these steps would be taken in their ransom notes. The double extortion tactic raises the ransomware threat level and poses further risk to organizational security, because ransomware not only represents the threat of data being encrypted, but also exposed.

05 Advancing Adversarial Machine Learning Defenses

As adversarial machine learning attacks cross the inevitable line from academia into the wild, organizations need to develop their defensive capabilities against these attacks. Over the course of this year, Deep Instinct contributed to the defining and outlining of various attack vectors and methodologies used in adversarial machine learning, producing a ML threat matrix to parallel the widely used MITRE ATT&CK framework. This new addition to the MITRE framework prepares the industry for comprehending the new and advanced attack vectors of adversarial machine learning.

THE TOP MALWARE TRENDS OF 2020



The number of new samples in each month, since January 2019, grouped by malware type and shown in arbitrary units, where the amount of miner samples in January 2019 is represented by one. This data was collected from and analyzed through D-Cloud, Deep Instinct's Threat Intelligence database

As seen in the graph above, 2020 was a good year for malware, with ransomware and worm samples thriving.

From 2019 to 2020 the type of malware that had the most increase in use was miners which went up by 1061%. Ransomware went up by 435%, and the use of backdoors increased by 322%. The least utilized type of malware were viruses and spyware.

Backdoor	Dropper	Miner	Ransomware	Spyware	Virus	Worm
322%	268%	1061%	435%	191%	181%	384%

- The month that experienced the most activity was July which went up by 653% compared to July of 2019. September also saw a dramatic rise of 570%
- The quietest month relative to the previous year was November, but which still saw an increase of activity by 170%

TOP 5: MALWARE FAMILIES

Emotet

Emotet was one of the most prevalent financial malware and botnet threats this year, and is addressed extensively in this report. [See the full write up here.](#) It first appeared in German speaking countries in Europe around mid-2014, and after two years without significant activity, Emotet reappeared in 2017, targeting the UK and the US.

Agent Tesla

Agent Tesla is a spyware that is being sold online since 2014. It is advertised as a legitimate monitoring software not intended for malicious purposes. However, its password extraction functionality and features that are aimed at avoiding detection allow Agent Tesla's operators to use it for malicious purposes. Moreover, Agent Tesla's support team have been assisting users with ways to infect victims similarly to any malware campaign.

A variant of Agent Tesla was discovered by Deep Instinct, [read more details about the spyware here.](#)

Dridex

Dridex is a highly active banking trojan family, in the wild since 2011 (where it appeared as its predecessor, Cridex). The first version of Dridex appeared in mid-2014, and since then it has become one of the most high-profile financial malware families.

Dridex is most commonly spread via mass email campaigns and uses malicious email attachments that include either a word document containing a malicious macro, or a PDF that utilizes a malicious JavaScript. Following successful infection, Dridex will collect and deliver banking information, credit card data, credentials and additional sensitive data found on the victims' computer and send to its C&C servers. Other variants include a crypto-currency wallet credential stealing mechanism.

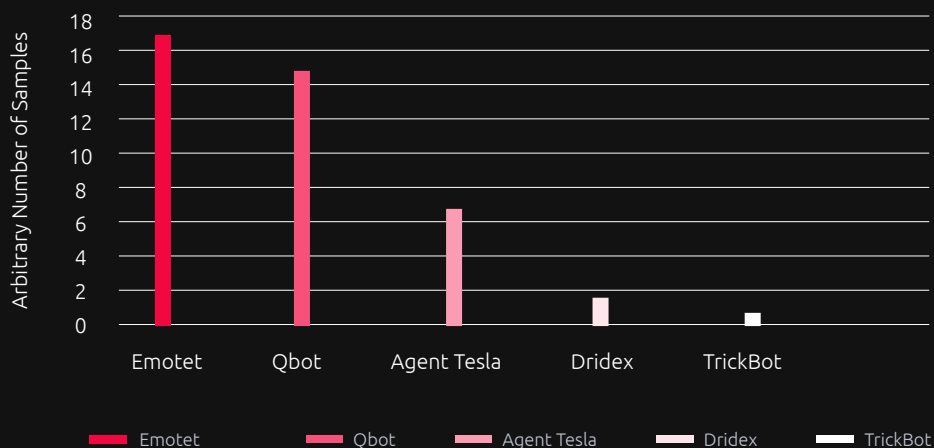
In several occasions, the Dridex infection infrastructure has also been used to spread other financial malware/spyware such as Trickbot and Emotet by either sharing the same droppers, or dropping each other as a secondary payload.

Qbot

Qbot is a popular info stealer and banking malware, active in the wild since 2009. Its main purpose is to steal online banking credentials and other financial information, though Qbot can also steal additional personal data, such as files and keystrokes. Additionally, Qbot possesses worm features allowing it to spread through network and removable drives.

Qbot monitors the browser on the infected machine to detect when victims interact with an online banking website in order to steal credentials. Additionally, Qbot collects further information from the infected machine including IP address, origin country, cookies and other system information.

Qbot's distribution methods vary and include malspam, with specially crafted document attachments triggering the infection, or exploit kits deployed on compromised websites that deliver Qbot's payload to a website's visitors.



The top 5 malware families of 2020. The number of samples, collected from Deep Instinct's D-Cloud, is shown in arbitrary units, where the number of TrickBot samples is represented by one.

TrickBot

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

A highly conspicuous player this year, a more extensive description on [TrickBot](#) can be found [here.](#)

TOP 5: RANSOMWARE FAMILIES

Sodinokibi

Sodinokibi is a ransomware which first appeared in the wild shortly before operations for Gandcrab ransomware ended in April 2019. This malware has since been involved in several high-profile targeted attacks, mostly against companies and government organizations.

The hackers 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 have also successfully conducted completely file-less attacks.

Ryuk

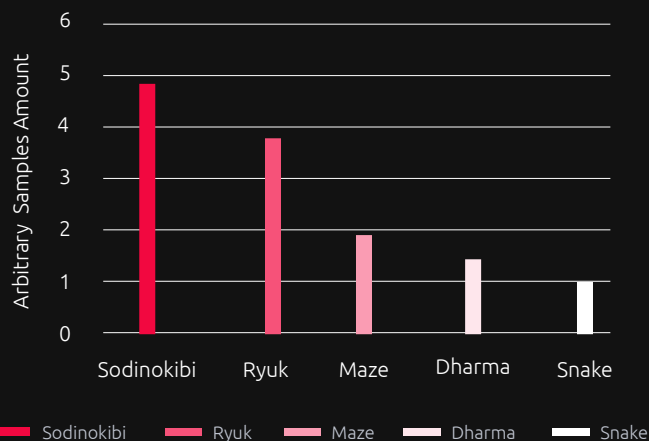
Ryuk ransomware was first seen in the wild in August 2018 and has since been involved in numerous targeted ransomware attacks. Read more about a few of Ryuk's most notorious attacks [here](#).

When Ryuk infects a system, it kills over 40 processes and stops more than 180 services, before beginning to encrypt files. Additionally, Ryuk requires Admin privileges to run and maintains persistence by writing itself to the Run registry key. Several updates of Ryuk have appeared since its release, and in its latest update in September 2019, Ryuk was programmed to steal confidential military, financial, and law enforcement files.

Maze

Maze is a ransomware active between May 2019 to November 2020, infamous for being the first ransomware to leak victims' stolen data. Maze had substantially increased its operation in October 2019, distributed in targeted attacks as well as in the 'Fallout' exploit kit. After a year of being one of the most prominent and active ransomware in the threat landscape, maze shut down its operation in November 2020.

In November 2019, the operators of Maze ransomware had contacted the cyber security news website BleepingComputer, informing them of the attack on the security staffing company Allied Universal and releasing a small sample of 700MB of stolen files, after the latter did not to pay the ransom. Afterwards, they published hundreds of Gigabytes of data stolen from different victims, in a dedicated website to victims' data dumps and leaked threats.



The number of samples from each ransomware family shown in arbitrary units, where the number of Snake samples is represented by one. The data in the graph is based on data collected from D-Cloud, combined with threat intelligence analysis.

Dharma

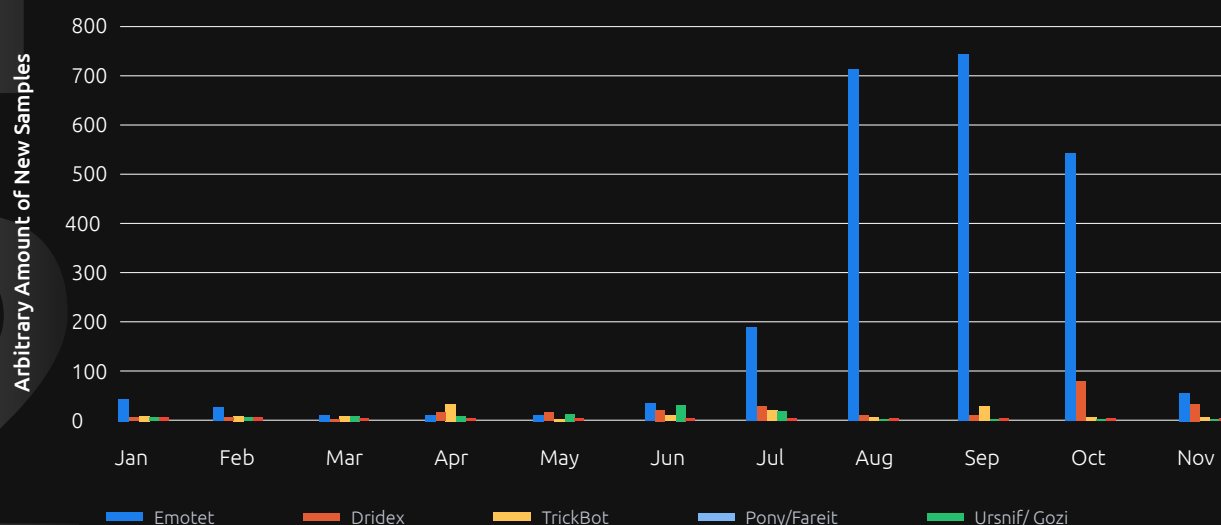
Dharma, AKA CrySis, is a ransomware family active since 2016. It is most known for targeting high profile organizations and institutions such as cities, hospital networks, parking lot systems and more, as well as private companies and small-medium businesses.

Dharma propagates via spam email, exploit kits and unsecured RDP access. After infection, Dharma encrypts all files other than system files in the affected computer, including network drives and removable devices. It then displays a ransom message, demanding a payment in bitcoin in order to provide a decryption key.

Snake

Snake is a ransomware targeting corporate networks, first discovered in January 2020. Once the ransomware, written in Go language, infects a computer, it deletes the system's shadow copies so they can't be used to restore encrypted files. It then compares its running processes against a pre-configured list, including some related to virtual machines, SCADA, remote management tools, and industrial control systems and kills those it finds. Then it starts encrypting files, each file is decrypted with a randomly generated key which Snake encrypts with its public key and stores in the encrypted file. It also stores the string 'EKANS' (Snake backwards) at the end of the file. After the malware finishes the encryption process, a ransom note called 'Fix-Your-Files.txt' is created. This file states that all the files in the corporate network were encrypted and to decrypt them, the attackers' private key is required and provides the victim with a contact email. The note along with the fact that administrator privileges are required in order to create the ransom note in the desired location, suggests that the attacker's plan is to distribute the ransomware to corporate organizations only, which aligns with the lack of infected personal computers.

TOP 5: BANKING TROJAN FAMILIES



The number of samples per malware that were seen in D-Cloud each month in 2020. The numbers are shown in arbitrary units, where the amount of Dridex samples in January is represented by one.

Emotet

For information on Emotet go to [page 13](#)

Dridex

For information on Dridex go to [page 6](#)

TrickBot

For information on TrickBot go to [page 18](#)

Pony Stealer

Pony Stealer is a spyware that has been in the wild since 2011. It is a very effective credential stealing trojan that targets popular applications including: FTP clients, cryptocurrency wallets, and browsers. Moreover, since Pony's source code was leaked in December 2012, it became much more widespread due to its availability.

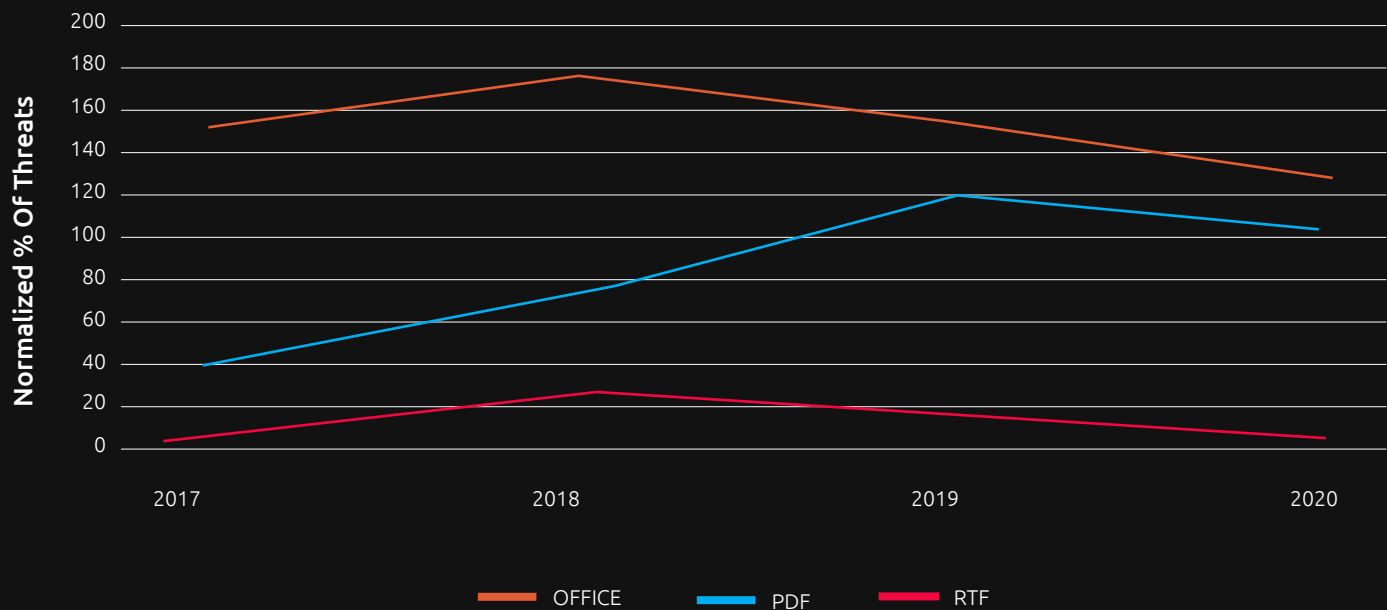
Pony is mainly distributed via phishing email campaigns as well as exploit kits and can be also used as a dropper of other malware variants, similarly to past incidents where it delivered CryptoWall.

Ursnif

Ursnif, AKA Gozi, is a sophisticated 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. This malware is usually spread through targeted email phishing campaigns.

The main targets of Ursnif are banks and financial institutions. However, the malware also targets other companies and even individuals, in order to steal as much data as possible. Ursnif mainly steals financial information such as banking site credentials and credit card numbers, as well as other personal data, such as email credentials, social network credentials, and file content from the infected computer.

MALWARE TRENDS BY OS: DOCUMENTS



Document Threat Landscape

Documents are one of the most common attack vectors used by malicious actors to spread their malware. As expected, in 2020 we observed a significant rise in the number of malware threats being distributed by documents whether they be PDF, RTF, OFFICE or other file types. Microsoft still dominates the computer market share, with 77% of the desktop market, therefore it should come as no surprise that the use of Microsoft Office Documents continues to be one of the most common attack vectors. PDF and RTF usage for malicious purposes also continued but not at the same rate.

Below we will cover some of the trends observed in 2020 regarding PDF, RTF and Office malware.

The normalized number of threats per year since 2017 can be seen above. All data was collected and analysed from our threat intelligence infrastructure, D-Cloud. As can be seen, Office malware is still the most common attack vector, while RTF is in a constant decline, and PDF is relatively unchanged compared to 2019.

MALWARE TRENDS BY OS: DOCUMENTS

PDF malware

PDF documents can be opened with a variety of tools from Adobe or Nitro PDF to any type of browser, making PDF vulnerabilities exploitable only on these platforms. Furthermore, PDF vulnerabilities are patched by Adobe and other PDF platforms by the dozens each year. The most prevalent attack vector in PDF is phishing. Luring a victim into opening a PDF file and clicking on a link, or any other form of social engineering, is much easier than exploiting a vulnerability that might act differently on different PDF viewers.

RTF malware

RTF was a common attack vector during 2016-2018 as many vulnerabilities in the format were discovered at that time. Today, RTF is the least popular format of the three, and the chances a user will encounter an RTF document in their day to day job is unlikely. The RTF format is flexible and therefore complicated, and the development of safe RTF parsers is highly complex therefore making some vulnerabilities possible while implementing the RTF parsing logic. Additionally, RTF supports embedding OLE objects and executables which allows attackers to transfer executables easily and attack using the OLE format. Despite all of this which makes RTF an attacker-friendly format, we've witnessed a steep decrease in RTF based malware since 2018. In all probability this is due to the rarity of RTF usage, which motivates hackers to use other attack vectors such as Office based malware.

Office malware

Office documents are commonly shared between organizations and individuals – therefore the chances an individual will stumble across a malware of this sort is highly likely. This makes Office documents the most prevalent document-based attack vector in 2020. Attackers constantly change their methods and take advantage of Office capabilities such as VBA and Excel4.0 Macros, OLE embedding, DDE and even XLSB in order to evade detection.

We observed several new Office threats this year, using both old and new attack techniques. In October this year, a massive Zbot campaign which used XLS files encrypted by the default password "VelvetSweatshop" was discovered. The use of this technique allowed the attackers to stay below the radar despite using a technique that is more than 10 years old.

Another highly active method is the use of Excel4.0 macros which allows an attacker to make web requests, execute shell commands, access win32 API's, and many more capabilities which are desirable for malware authors. Analyzing this kind of macros is more challenging, and as a result many malicious Excel4.0 documents have a lower detection rate.

Zloader, Qbot and Ursnif are just some of the malware families that take advantage of Excel4.0 macros. The threat actors behind Qbot took this method and combined it with the use of XLSB files. The process of transforming an excel sheet with Excel4.0 macros to XLSB is easy as it requires saving the file in the XLSB format. Furthermore, with XLSB the macros are saved as binaries rather than as OLE objects, which makes the analysis of them more difficult. The motivation behind using the capabilities of XLSB is to make the analysis of such files difficult and still be able to run Excel4.0 macros, without making any drastic changes to the malware.

MALWARE TRENDS BY OS: MAC

Apple's share of the global computer market grows every year: macOS market share in early 2019 was around 13%, while today it's about 18%. The increase of enterprises using macOS makes it an even more compelling target for opportunistic hackers and malware authors. The increase has beggotten a subsequent increase in sophisticated attacks and malware, designed specifically to target the macOS enterprise. For example, earlier this year an exploit chain was found which bypasses Microsoft's malicious macros protections to infect MacOS users. Meaning, when a user opens the document, the macro is automatically executed.

Like in 2019, in 2020 we continued to observe the sophisticated North-Korean based APT Lazarus using several new malware strains of macOS malware.

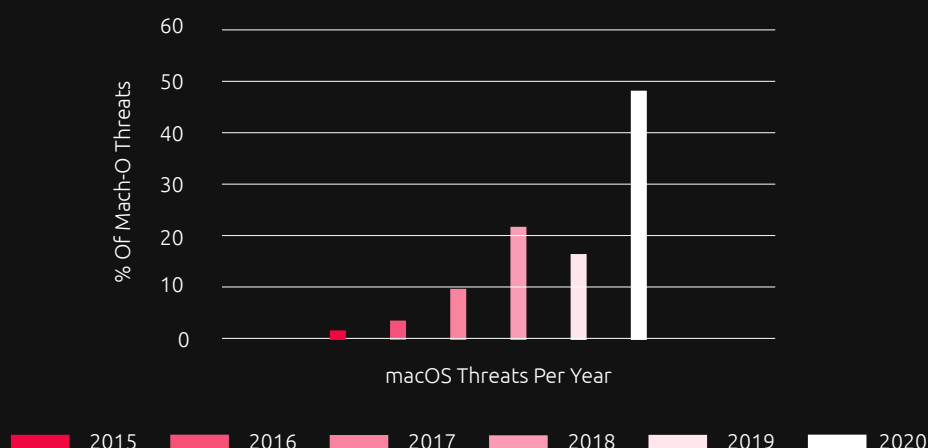
This means there are Mac-specific developers deeply invested in writing custom malware for macOS and not just transforming Windows based malware into macOS malware.

This means there are Mac-specific developers deeply invested in writing custom malware for macOS and not just transforming Windows based malware into macOS malware.

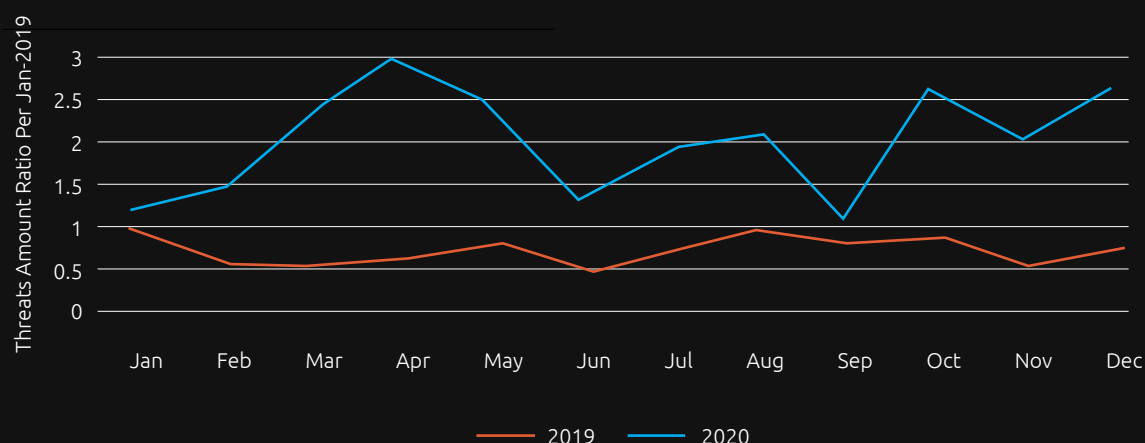
There has also been a rise in numbers of PUA (Potentially Unwanted Applications) as macOS built-in security programs do not detect PUA at the same rate as malware, leaving the door open for these borderline programs. In addition, the number of PUA developers targeting macOS systems is assumed to be significantly higher than the number of malware developers targeting them.

The total number of threats per year between 2015 to 2020 can be seen below. All data was collected and analysed from our threat intelligence infrastructure, D-Cloud. In 2020, macOS based malware was on a constant rise as can be seen from the graph below. Threats such as EvilQuest ransomware, which was discovered this year, increased dramatically in the number of macOS threats. There was a minor drop in 2019 but overall, the number of threats multiplies every year. As long as more enterprise environments use macOS, the number of threats targeting these systems will increase.

MacOS Threats



MALWARE TRENDS BY OS: ANDROID



The graph above shows the trend of malware threats targeting Android OS in 2020 compared to 2019 based on the data collected from Deep Instinct's D-Cloud. The statistics were normalized relative to the trend of January 2019.

Android Malware Threats in 2020

In 2020 the number of malware threats targeting Android OS has, as expected, considerably increased when compared with the previous year. This increase correlates with the rising popularity of Android and, unlike iOS, being a relatively open operating system that allows users to install applications from multiple sources, not just the official app-store - Google Play. The nature of Android being an operating system with open source code continues to lure malware authors due its relative ease of circumvention.

Android is significantly larger than iOS and other mobile operating systems and dominates market-share by over 70%. The significance of Android's large pool of users means that adversaries can achieve higher collateral impact on targets. This is the case without even mentioning the fact that Android is present not only in smartphones, but also drives a considerable portion of IoT enablement.

The creativity of cyber crooks is constantly challenged. To succeed, they need to adapt their social engineering skills to meet the new arena created by technological developments. Here lies the success of one of the most common attack vectors; the (spear) phishing attack. An email, SMS or even voice message with content convincing enough to persuade its reader to initiate the chain of actions that will enable their intrusion phase.

Unfortunately, the COVID-19 pandemic was widely abused and often chosen as the background story for malware delivering "Corona emergency" messages. Frequently, these misleading messages were delivered over malicious applications to smartphone users.

The graph above is clear evidence of this correlation. The examples of COVID-19-themed fake apps vary from banking malware and ransomware, to malicious RAT applications.

The tragic impact of the pandemic playing on people's fear unfortunately contributed to the widespread success of these attacks.

This year, banking trojans, ransomware and adware continued to lead the charts of top malware threats targeting Android. More and more people adopted mobile applications to conduct their finance management, which in turn, inspired cyber-criminals to develop and advance Android malware aimed at stealing personal banking information.

Similarly, due to our constant dependence on smartphones, it is easier to make victims pay a ransom for un-blocking or decrypting access to data stored on them with ransomware. For example, Android ransomware MalLocker that simply blocks the access to smartphones (as opposed to encrypting the data) has been spotted this year. Analysis found that MalLocker was found to be using a machine learning library, TinyML, that while not functional at the time, is expected to be functional in the future, and is certainly an indication of how machine learning is likely to be used in malicious activity. This example sheds light on the future development of malware, and is just another sign that malware authors never rest, but are always seeking new ways to enhance their game.

MALWARE TRENDS BY CAMPAIGN: EMOTET

The Breadth and the Power

In October, the [United States Department of Homeland Security](#) defined Emotet as one of the most prevalent cyberthreats. It is a well-deserved title for this diligent and sophisticated malware that has been terrorizing individuals, organizations and governments since 2014.

Emotet started as a banking trojan designed to steal banking credentials, but a few years later the spamming module was added, and the focus shifted to deploying Emotet as a botnet and a dropper for a myriad of infostealers, bankers and ransomware threats. Emotet loaders are usually delivered via weaponized email attachments or malicious links in the body of an email. The victim is persuaded with social engineering to open one of the “traps”. Emotet has highly effective propagation capabilities, thus in many cases it is enough for one employee to open a malicious attachment for the whole company to be infected.

New wave

Emotet entered this year continuing on from its very active last quarter of 2019, but not without a self-imposed three-week holiday. It was observed using COVID-19 themed spam emails to take advantage of the global crisis. For example, in Japan, spam written in Japanese appeared to be sent from a disability welfare service provider. The emails urged the victims to open an attached Word document to find more information regarding COVID-19 patients in several of Japan's prefectures. In February, the team added a new WiFi module to its lateral movement arsenal. The goal of the module is to discover wireless networks in the vicinity of the already infected machine so it can then infect additional networks.

It is not new for Emotet operators to take a hiatus in the middle of the year. This year, the break started in mid-February and continued until July 17th, when a new wave of dangerous spam started. One reason for botnet operators to pause their activities, is to update their infrastructure and focus resources on R&D in order to improve the effectivity and stealthiness of the bot.

Other speculation is that Emotet was slowed down as a result of a vulnerability discovered in its loader. Dubbed “EmoCrash”, the vulnerability would crash Emotet's installer and prevent any further infection. It was fixed in a new version of the installer released in July.

Deep Instinct's Ron Ben-Yizhak conducted an in-depth analysis of the loader and payloads used by Emotet in this new wave.

A large number of unique samples of the Emotet loader were collected in an attempt to find patterns in the data and understand its evasiveness. Overall, 444,000 unique samples were collected and analyzed.

The research yielded several significant findings:

- Emotet samples can be grouped according to their file size. Files with identical file sizes will have the same static information, such as the ratio between the different PE sections and their relative entropy.
- Files in each group will also have identical code.
- By following this method, 272 unique group sizes of files and 102 templates of Emotet loaders were discovered.
- By correlating the different templates with the epoch number (one of the three botnets spreading Emotet) given for each sample by the Cryptolaemus group, we were able to conclude that the operator behind each Emotet epoch has his own loader.
- Having so many templates reduces Emotet's probability of being discovered. In case a template is signed by an Anti-Virus vendor, other templates won't be affected.

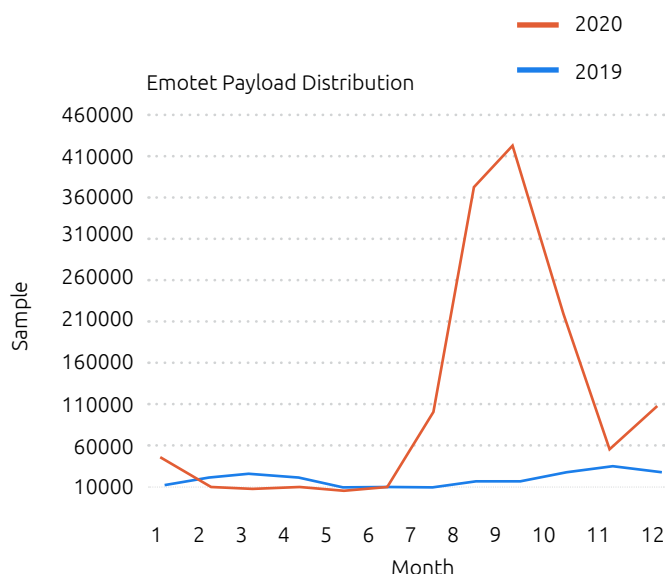
While this might be enough to make detection very hard, according to Ron's research, Emotet deploys other fascinating techniques to stay undetected:

- Emotet loaders contain heaps of benign code in order to throw off A.I. based security products.
- Most of the code inside an Emotet loader is unused. For example, in one of the analyzed samples only 16.22% of the code was executed.
- All the routines to decrypt and execute the payload are obfuscated and constructed during runtime to hide its intentions.
- The payload is loaded into memory without headers and strings that indicate a loaded executable, thus hindering forensic memory analysis.
- The payload's code is obfuscated, doesn't contain any strings and has an empty import table.

For further details please refer to the full blog on [Emotet's Latest Wave](#).

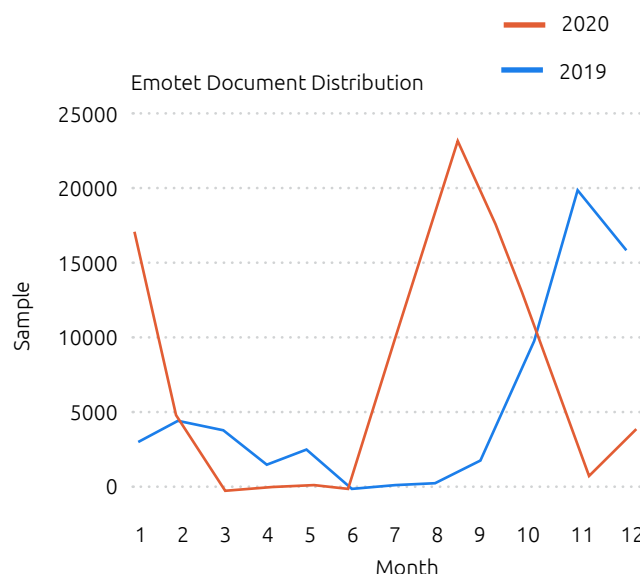
MALWARE TRENDS BY CAMPAIGN: EMOTET

Since its return in July, Emotet has been spreading in-the-wild at unprecedented numbers, as can be seen in the graphs below. The data (gathered from the [Cryptolaemus Pastedump](https://paste.cryptolaemus.com/)) shows the aforementioned drop in Emotet's presence in the spring (which also can be seen occurring in 2019 between March and August), the steep rise in Emotet distribution in July, and then a subsequent decline in November.

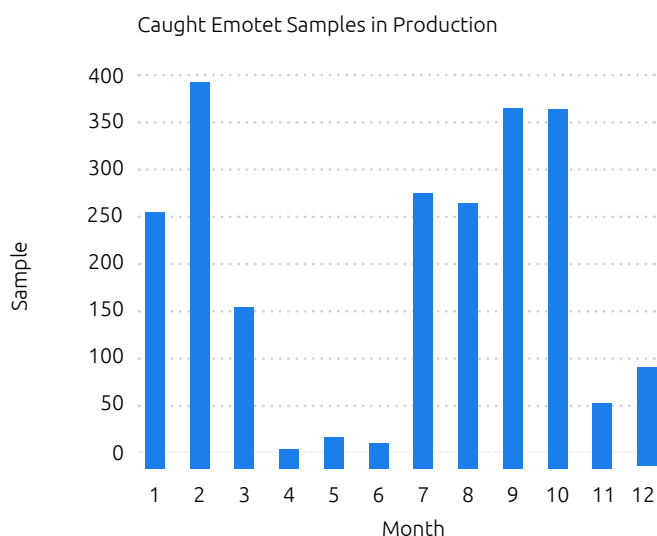


Comparison of Emotet loaders' distribution between 2019 and 2020 by month. Loaders are initial Emotet executables. It clearly shows the rapid rise in Emotet samples with the start of this year's July wave. Data was gathered from: <https://paste.cryptolaemus.com/>

The number of distributed Emotet samples are high, not only in comparison to other malware families, but also compared to its campaigns in 2019. Only this year did its numbers cross the 300k mark. This enormous wave was backed by a new spam campaign themed with fake Microsoft product updates and the US elections. An attachment stealing module was also added to build credibility to the weaponized attachments.



Comparison of Emotet droppers (that are usually Microsoft Office documents) seen in-the-wild between 2019 and 2020 by month. Naturally, we can see a correlation between the trends in distribution of Emotet's droppers and loaders distributed in 2019 and 2020. Data was gathered from: <https://paste.cryptolaemus.com/>



Comparison of Emotet samples (both loaders and droppers) prevented by Deep Instinct in customers' environment. Despite Emotet's spring break, there were still infection attempts prevented during this period. Data was gathered from Deep Instinct's D-Cloud.

Summary

6 years after its initial release, Emotet is still one of the most dangerous and innovative pieces of malware. Each year we witness the botnet gather new capabilities, reach new targets and break its own records of spam delivery. Because Emotet's infection model relies on a constant flow of new victims, each of us has a small role in stopping its spread by practicing proper "cyber hygiene", spreading awareness, and using a security product, such as [Deep Instinct™](#), that achieves a high level of efficacy.

MALWARE TRENDS BY CAMPAIGN: RANSOMWARE

If it were even possible, ransomware became an even bigger threat in 2020. The potential for a large profit, along with the success of double-extortion campaigns that combined ransomware with data leaks, led threat actors towards developing new data-stealing ransomware and adding data exfiltration features to existing malware.

Attack Vectors

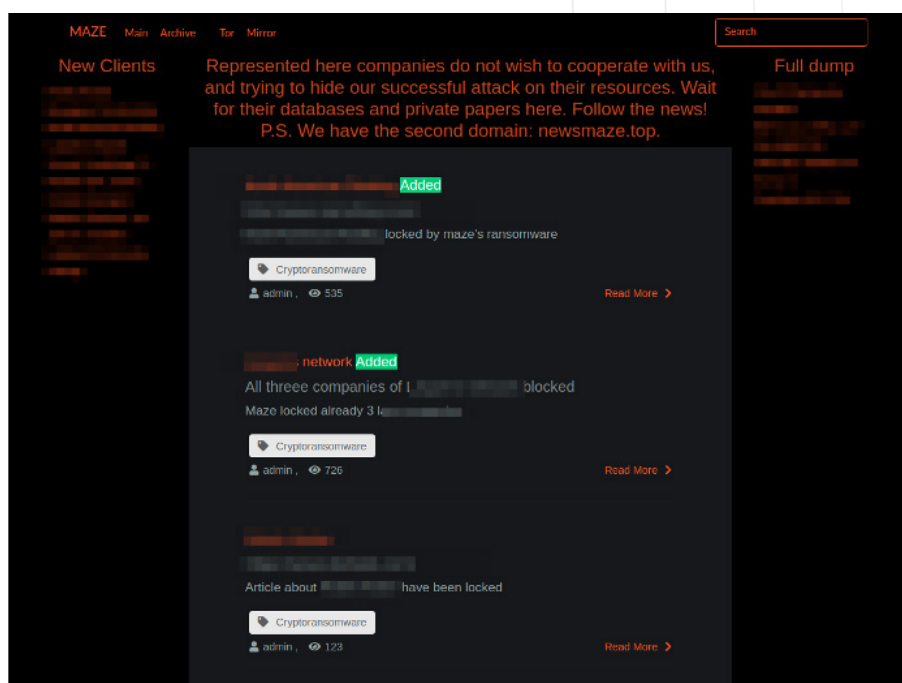
Document droppers sent in spam campaigns remained the most popular attack vector for ransomware. Establishing, once again, that the greatest vulnerability within organizations remains to be employees, who represent the best chance through which threat actors can successfully execute their malicious files. Nonetheless, Ransomware distributors also used other ways to get initial access into the victim network, like piggybacking on other malware as secondary payloads, as seen done in the wild by Egregor, dropped by Qbot and Ryuk, dropped by Emotet.

The use of poorly secured RDP connections was another common method used in 2020 performed by Sodinokibi, Dharma and Maze. Other than these methods, ransomware developers also showed-off their agility and their ability to seize an opportunity. One such example is the Ryuk ransomware gang who rapidly exploited the Zerologon privilege-escalation vulnerability (CVE-2020-1472), a massive campaign that was pulled off only one month after the technical details of the vulnerability were published.

Double-Extortion: Ransomware Leaking Data

In November 2019, the operators of Maze ransomware contacted the cyber security news website [BleepingComputer](#), informing them of an attack on the security staffing company Allied Universal and releasing a small sample of 700MB of stolen files, after the latter did not to pay the ransom.

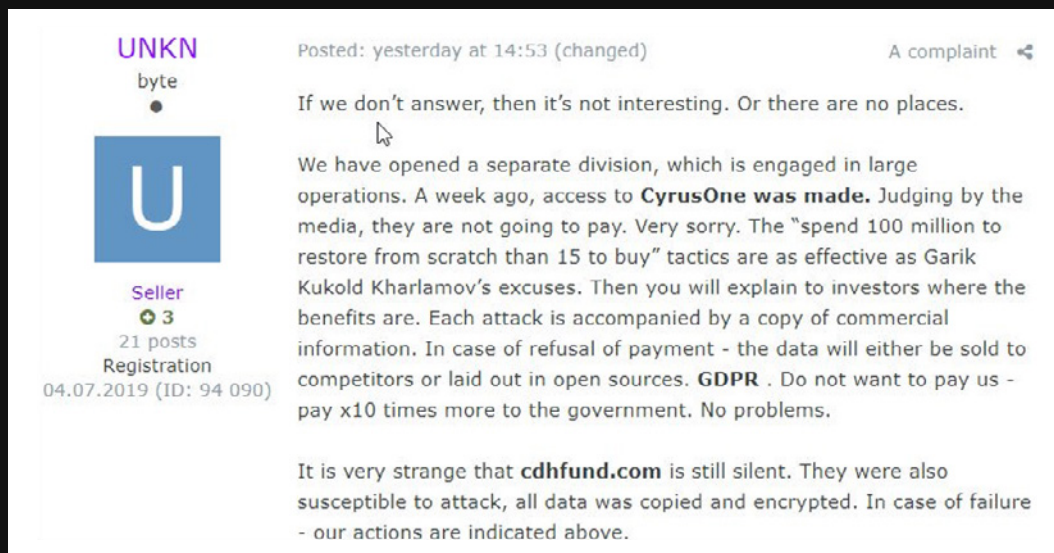
Since then, Maze operators had lived up to their threat by publishing hundreds of Gigabytes of data stolen from different victims, in a dedicated website to victims' data dumps and leak threats.



Maze Ransomware data leak site

MALWARE TRENDS BY CAMPAIGN: RANSOMWARE

Following Maze ransomware's steps was REvil, the threat group behind Sodinokibi ransomware, which in January 2020 adopted the data leakage tactic against victims unwilling to pay the ransom. In a cybercrime forum announcement, REvil group revealed an additional layer in their attack, intended to put even further pressure on the victim to pay the ransom. Aside from the risk of losing all their data, there is also the risk of trade secrets or confidential information being leaked. The victims are also exposed to penalties as a result of being in breach of privacy laws, such as GDPR.



UNKN
byte

Posted: yesterday at 14:53 (changed) A complaint

If we don't answer, then it's not interesting. Or there are no places.

We have opened a separate division, which is engaged in large operations. A week ago, access to **CyrusOne** was made. Judging by the media, they are not going to pay. Very sorry. The "spend 100 million to restore from scratch than 15 to buy" tactics are as effective as Garik Kukold Kharlamov's excuses. Then you will explain to investors where the benefits are. Each attack is accompanied by a copy of commercial information. In case of refusal of payment - the data will either be sold to competitors or laid out in open sources. **GDPR**. Do not want to pay us - pay x10 times more to the government. No problems.

It is very strange that **cdhfund.com** is still silent. They were also susceptible to attack, all data was copied and encrypted. In case of failure - our actions are indicated above.

Seller
3
21 posts
Registration
04.07.2019 (ID: 94 090)

From Tactic to 2020's Hottest Trend

Followed by Maze and Sodinokibi was Nemty, the Ransomware-as-a-Service. Its creators announced they will be hosting a blog to which stolen data will be published. Likewise, the creators of DoppelPaymer ransomware claimed they have been selling stolen data on the dark web after their victims refused to pay the ransom for almost a year. Throughout the year, new and old operations added data exfiltration abilities to their ransomware, among them was BitPyLock, Clop, Pysa, Ako, Netwalker, Nefilim, Mespinoza, Avaddon, Conti, Darkside, Snatch, Sekhmet, Ragnarlocker, and others.

By the end of 2020, double extortion tactics became the new standard in ransomware, and ransomware developers even provided warning that these steps would be taken in their ransom notes.

The double extortion tactic poses a major threat to organizational security and protection. If in the past, data-loss was the main concern, a simple backup policy could assist in recovering encrypted data following a ransomware attack, but in the case of having data leaked and exposed, remediation policies of this sort would prove to be futile.



All your files are encrypted!

If you read this message. That means we've been able to break into your network and encrypt all your machines.

All your files on all network machines, including, but not limited to:
Documents, databases, and office projects have been encrypted using strong military grade encryption algorithm **RSA-4096**.
Break it is impossible and any effort is a waste of time!

Recovery tools and other software will not help you!
Don't find your backups? because they have been successfully encrypted too or security wiped!

The only way to recover your files, are to meet our demand.

1. Create a Bitcoin wallet (we recommend you to create on [Blockchain.com](#))
2. Register on [LocalBitcoins.com](#) (or any other Bitcoin exchange), then buy **Bitcoin (BTC)**.
3. Send Bitcoins to our wallet below (in case sensitive. Make sure you copy past it):
[REDACTED]
4. Send Bitcoin Transaction ID to our e-mail address along with our wallet address you pay!
[REDACTED]
5. You will receive the tools needed to decrypt all of your machines and files!

Note: Before payment you can contact with us for 1 free small file as decryption test!

Be warned, we won't be able to recover your files if you start fiddling with them!
If you do not wish to negotiate with us. We will make your company's private papers and databases public. This's not a joke!

You have 72 hours from this moment to send us payment, or you files and the way we communicate will be lost in eternity!

BitPyLock ransom note, Source: MalwareHunterTeam

MALWARE TRENDS BY CAMPAIGN: RANSOMWARE

Ransomware and COVID-19

On March 18th 2020, Maze operators published a press release in which they committed themselves to refrain from targeting medical organization until the COVID-19 situation stabilized. They also took the unusual move of offering victims discounts on their ransom demands due to the economic crisis.

DoppelPaymer ransomware took a similar approach, replying to a query by BleepingComputer, as to whether they would refrain from targeting medical organizations. The DoppelPaymer team responded they always try to avoid hitting hospitals and nursing homes and to validate their commitment, they offered free decryption to victims in the medical industry infected by mistake.

In September, a DoppelPaymer attack on the Duesseldorf University clinic prevented the hospital from providing a patient with emergency treatment, which contributed to her death. Though the ransomware operators provided the decryption key for free, and claimed they targeted the university of Duesseldorf and not the hospital clinic, the incident remains to be the first ever reported death caused by ransomware.

The commitment taken by Maze and a few other ransomware such as NetWalker, Nefilim, and Clop, was unfortunately not shared by other ransomware operators who took advantage of the pandemic crisis to target hospitals and healthcare services providers to increase the pressure to pay their ransom.

Among these, Ryuk was the most active, attacking several hospitals in the US, UK and Canada. The most well-known victim was Universal Health Services (UHS), a major hospital chain with over 400 facilities in the United States and the United Kingdom.

...was unfortunately not shared by other ransomware operators who took advantage of the pandemic crisis to target hospitals and healthcare services providers to increase their pressure to pay the ransom.

Summary

The cyber threat landscape was anything but uneventful in 2020. With the double extortion threat tactic as the new standard, and the first death caused by ransomware, there is no doubt that ransomware is here to stay. In fact, this year has proven that organizations can no longer tolerate the risk of getting infected. Even with perfect backup systems, companies need to take a pro-active stance to shield themselves from infection by deploying solutions that focus on prevention, as this year's events have demonstrated that the damage from data leakage could be worse than data loss.

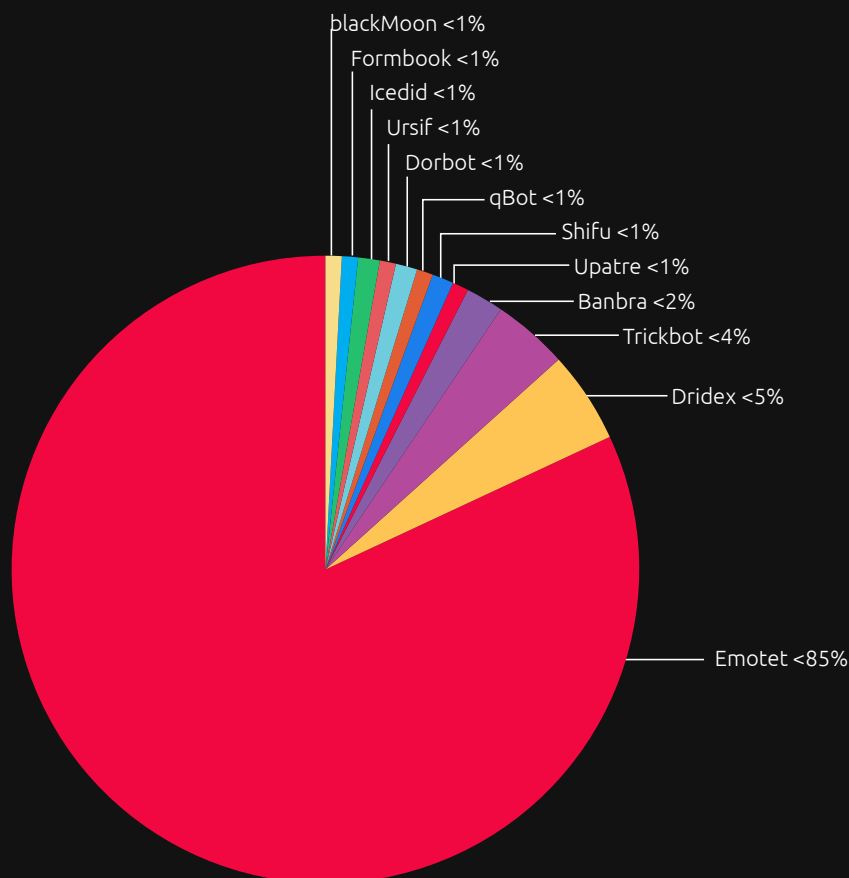
MALWARE TRENDS BY CAMPAIGN: FINANCIAL TROJANS

From the first Zeus sample in 2006 to this day, we've seen banking trojans, infostealers and RATs gaining popularity and morphing into financial weapons. The year 2020 was no exception to this trend, with veteran threat actors becoming more sophisticated and effective along with new malware strains introduced to the game.

To the right is a distribution of the most frequently seen financial malware families in 2020 collected using D-Cloud, Deep Instinct's threat intelligence database.

It can be easily seen that Emotet's numbers are unparalleled with almost 85% percent of droppers and payloads attributed to this deadly malware.

Not all doom and gloom, 2020 was also a year of restored morale following the success of massive takedown operations and the exploration of new creative ways to slow down criminal enterprises.



Trickbot

Similar to previous years, the modular banking trojan and info-stealer, Trickbot, continued to appear in headlines with its seemingly ceaseless developments and almost monthly updates to its components and infrastructure.

According to data gathered from our aforementioned D-Cloud database, Trickbot is the third most distributed malware this year, preceded by Emotet and Dridex at the top of the list.

The year started with the Trickbot gang releasing their own post-exploitation framework that was intended to allow them to move laterally and infect other devices in the victim's network. Not delivering the results they expected, the framework should've been stealthier and much more aligned with their needs than the PowerShell Empire that was used before.

The development continued with two additional new components released by the team one month apart, the BazarBackdoor and Nworm network spreading module.

The stealthy fileless backdoor allows the attackers to quietly drop other Trickbot modules or other malware while utilizing innovative technologies such as decentralized DNS services, which makes takedown operations very difficult. The Nworm module replaces the old Mworm module and its purpose is to infect the Active Directory controller with the malware. The novelties in the new module is the addition of encrypted traffic to mitigate the detection of Trickbot during transfer and fileless approach to the infection as the payload will be started from memory on the controller.

In order to broaden its scope and increase the number of potential victims, Trickbot developers created tools for Android and Linux operating systems. Towards the end of March a new Android malware named TrickMo was found. The app compliments Trickbot's ability to steal banking credentials. It would try to intercept 2FA codes sent by banks either by SMS or push notifications, to gain access to the victim's online bank account.

By the end of July, a port of Trickbot's Anchor backdoor was ported to Linux, allowing the attackers to drop Linux malware and infect Windows machines on the same network.

Additionally, two new anti-evasion techniques were added to the malware: Trickbot will now check the number of running processes and the screen resolution in order to detect if it is running inside a virtual machine.

COVID-19

The COVID-19 pandemic has provided fertile material from which to build scams, spread disinformation and malware. In the month of April alone, [Google reported](#) that it was blocking 18 million COVID-19 themed phishing and spam emails daily!

Financial malware operators didn't miss the opportunity to take advantage of the situation.

We observed Emotet used Coronavirus themed spam emails to lure targets in Japan and the United States. Trickbot and Formbook were found to have used fake emails from the World Health Organization. Zloader was spotted trying to lure victims with promises of a secret COVID cure. The Android banker Ginp was seen utilizing a fake "Coronavirus finder" app for infection. Finally, the operators of the IcedID banking trojan sent email lures that cited the Family and Medical Leave Act of the United States. A relevant piece of legislation in the case of a lockdown and even better for building the appearance of legitimacy.

Other trending topics such as the US 2020 presidential elections and the Black Lives Matter movement were abused as well.

New Faces

Several new malware strains have joined the financial trojan scene this year.

A new, simple but highly effective infostealer, RacoonaRAT was found in February on an underground Russian forum. The malware is capable of stealing credentials and cryptocurrencies from over 60 applications and digital wallets. Later this year, the malware used Google's cloud infrastructure in order to stay undetected.

RacoonaRAT was joined by the Grandoreiro banking malware in April that used overlay attacks in order to commit fraudulent money transfers from Spanish victims.

In August, the new Mekotio banking trojan was seen targeting victims in Latin America by harvesting credentials and stealing Bitcoin by replacing wallet addresses in the clipboard.

Finally, the Anubis and Abaddon infostealers were introduced, which are both equipped with credential and credit card stealing capabilities.

Other Platforms

While Windows is still the most targeted platform by financial cyberthreats, Android and MacOS were also attacked this year.

2020 brought several new banking trojans aimed at Android users. Spanish victims were lured into installing the Ginp banking trojan, by pretending to be a "Coronavirus Finder". The malware stole credit card details by promising to reveal people infected with the virus in the vicinity, for a small fee.

A month later, an additional banking trojan was found, named EventBot. The banking malware can steal information from over 200 financial and cryptocurrency applications including PayPal, Coinbase and Revolut.

Being put to rest is a known Android banker, Cerberus, that was active since 2019. The team behind it has decided that it's reached the end of its life by breaking it up and releasing the source code on a hacking forum.

In August of this year we also spotted a financial trojan on the Mac operating system called XCSSET.

The malware installed a trojanized version of the Safari browser that would try to steal credit card information, credentials and replace cryptocurrency wallets entered during transactions.

But as powerful and evasive as these crime syndicates are, they aren't perfect or bulletproof. This year we witnessed clever and unprecedented attempts to hinder these malicious empires.

A New Hope

Financial malware has been a serious threat to organizations and individuals for over a decade.

But as powerful and evasive as these crime syndicates are, they aren't perfect or bulletproof. This year we witnessed clever and unprecedented attempts to hinder these malicious empires.

Two attacks were aimed at Emotet. One dubbed "Emotehack" where payloads of the Emotet malware were replaced with images and internet memes by an unknown vigilante. The second, "EmoCrash", which exploited a buffer overflow vulnerability in the malware itself to make it crash.

The month of October was particularly hard for the operators of Trickbot with cybersecurity and hosting firms targeting its infrastructure. The takedown attempt reportedly sabotaged 94% of its infrastructure.

MALWARE TRENDS BY CAMPAIGN: POWERSHELL

PowerShell is a Microsoft Windows framework and scripting language, which has been an integral part of Windows installations for decades. In August 2016, it became cross-platform and open source.

Besides its many uses by the Windows operating system, PowerShell is a tool of great use to IT teams and system administrators, who use it to perform, and even automate, daily operations. However, as happens with everything useful, threat actors use PowerShell for malicious purposes.

PowerShell is a powerful tool that security vendors find more difficult to detect than other tools of its caliber, making it ideal for malicious actors. For this reason, the use of PowerShell for malicious purposes has increased in recent years, as well as its scripting language in major attacks. For example, in June 2016, it was reported that a Russian adversary named “Cozy Bear” had infiltrated the Democratic National Committee’s (DNC) network almost a year prior to its discovery. The group used a simple, efficient line of PowerShell code, which they stored only in the Windows Management Instrumentation (WMI) database, as a backdoor.

Dishonorable Mentions from the Past Year

01 xHunt

xHunt is a malware campaign that has been active since 2018. In September 2020, samples associated with the group were found in a Kuwaiti organization’s network and were estimated to have resided there for over a year. The campaign, which had targeted Kuwaiti organizations in the past, used two PowerShell backdoors to maintain its persistence on the organization’s Exchange server, run different commands on the system and exfiltrate data. One of the backdoors, named “TriFive”, used deleted email drafts as means for communication with the attackers. The other, dubbed “Snugy”, used the more classic approach of DNS tunneling for similar purposes. Both backdoors were run automatically, in different intervals, by two different scheduled tasks.

02 LockBit

LockBit is a ransomware family that has been active since 2019. In 2020, heavily PowerShell based LockBit attacks were observed. In these attacks, a PowerShell script had retrieved Base64 encoded PowerShell code, which in turn connected to a Command and Control (C&C) server, to retrieve additional PowerShell modules. During the attack, the malware had checked for the presence of different security products and business-related software, and only if the system was deemed as “compromise worthy” based on the software that was found, other actions were performed. These actions could vary from one attack to another and included re-configuring firewall rules to allow certain communications, password cracking, exfiltrating sensitive information and more. When the malware finished performing these tasks and establishing persistence, it turned to the main event, and ran the ransomware in memory with the use of a single WMI command.

YEAR'S MOST INTERESTING DISCOVERIES

Throughout 2020, Deep Instinct protected its customers extensively and from a wide variety of threats. This section summarizes some of the most interesting malware which was prevented by Deep Instinct in its production sites.

01 Emotet

Overview: Emotet is one of the most prevalent financial malware and botnet 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 and targeting the UK and the US.

In its later versions, Emotet has evolved into a botnet dropping other malware, such as Ryuk, Trickbot, and others onto the victim computer once initial access is generated. In its most recent attack wave, Emotet added additional evasion techniques in order to become even more evasive. These techniques are covered in depth in our blog series, '[Why Emotet's Latest Wave is Harder to Catch than Ever Before](#)'.

Risk: Emotet is one of the most prevalent and advanced malware strains in recent years, and its evolution into a botnet is a great threat for organizations. Emotet is highly effective in achieving initial access into organizations, and this access is then exploited by numerous malware campaigns which capitalize on the breached pathway – such as Ryuk ransomware, or the financial malware strains Trickbot and Qakbot.

02 Agent Tesla

Overview: Agent Tesla is infamous spyware with extensive data harvesting and keylogging capabilities. It has been active since 2014 and is marketed in dark-web forums as a commercial project, to which subscription licenses can be bought on the malware's official website. Throughout the years, tweaks and changes have been made to maintain the malware's evasiveness from new security measurements and to help it remain one of the most common malware strains in the wild.

In the last year, two innovations of this malware strain were uncovered from samples prevented in production sites: [a very complex and evasive infection flow](#), and the use of a PasteBin [service called HasteBin](#).

Risk: Agent Tesla is a highly effective strain of spyware, capable of stealing different types of private information while evading detection. Organizations which are not well protected from this threat risk the theft of private credentials and files, including sensitive information which could hurt the company financially, or be used to facilitate further attacks.

YEAR'S MOST INTERESTING DISCOVERIES

03 Formbook

Overview: FormBook is an information stealer which first appeared on the scene in 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. In February of 2020 a [highly evasive Formbook campaign](#) was uncovered, using several different filetypes, before finally injecting the main payload into memory.

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 purposes, such as financial theft, or even deeper infiltration into the attacked organization, through theft of credentials belonging to users in the organization.

04 Aggah

Overview: Aggah is a fileless multi-stage malware loader which utilizes dual-use tools along with free and open web hosting services such as Bitly and Pastebin to hold its resources. Most of these resources hold HTA scripts with embedded PowerShell scripts that run one after the other, until dropping the final payload, which usually appears to be spyware. In our analysis, the [spyware strains](#) dropped onto the victim device were Agent Tesla, Remcos RAT (Remote Access Trojan) or NanoCore RAT.

Risk: As Aggah is a highly evasive loader which is used to drop additional malware onto the victim, an Aggah attack could result in several different bad outcomes. If spyware is dropped onto the victim device, sensitive information and credentials can then be stolen, while if ransomware is deployed by the loader, the target organization will be facing encryption on some or all of its network.

05 Cryptbot

Overview: CryptBot is a relatively recent information stealer. First discovered in the spring of 2019, CryptBot steals saved browser credentials, cookies, crypto currency wallets, and text files, among other things which it then sends to its command and control server. Cryptbot combines complex evasion techniques and a [relatively simple social-engineering based distribution strategy](#) to produce an interesting method of attack that succeeds at staying relatively well hidden.

Risk: Being an information stealer, Cryptbot is able to steal user credentials, such as email logins and passwords, and financial information. This data could then be used for a variety of purposes, such as financial theft, or even deeper infiltration into the attacked organization, through theft of credentials belonging to users in the organization.

CYBER INSIGHTS: EFFECT OF COVID-19 ON CYBERSECURITY

The year 2020 will surely be remembered for the COVID-19 pandemic. The pandemic affected all areas of our daily life, and many of these changes will probably stay with us long after the pandemic itself has gone.

As digital interfaces are involved in many of our daily routines, cybersecurity has also been affected by the pandemic. The most notable impact on cybersecurity, was undoubtedly the massive transition to Working From Home (WFH), as companies strove to keep their business running while maintaining social distancing. The new arrangement of WFH, which started as a measure to combat the spread of the pandemic, is expected to become the industry norm.

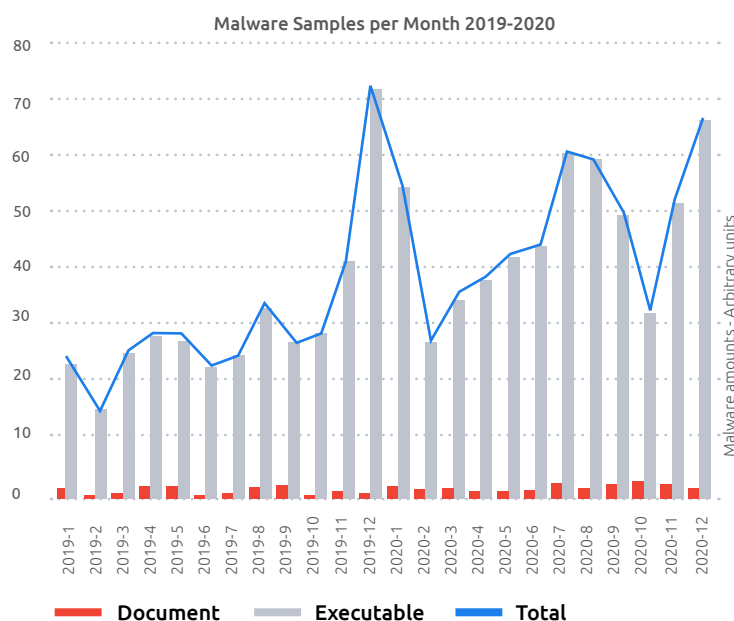
Cybersecurity-wise, there is concern that in the time that it takes companies to upscale and adapt their security to meet the change in location and form of the office network, attackers will be taking advantage of this window of exposure. Previously, an organization's network and all its data was sitting securely behind fortifications of the organizational security network. All of a sudden, the transition of moving to a wide and varied mess of different work environments made it far more complex for defenders to keep protecting the enterprise at the same level. Naturally, the organization's attack surface is amplified.

While in the past only one attempt was all a hacker could get of successfully breaking in using a new variant of malware, now they have multiple attempts, all with equally good chances. And for an attack to cause damage, it only needs to succeed once. An example of this was the Cognizant incident that hit the company early on in the work from home transition. The IT Service provider was attacked by ransomware that managed to bring business to a halt for a period of time and is alleged to have cost the company between \$50 and \$70 million.

Malicious actors are naturally aware of developments led by the pandemic, and have adapted their attacks, using COVID-19 themes in order to trick users. For example, Trickbot, the sophisticated financial malware, used fake emails from the WHO in order to lure victims into downloading a Word document attached to the email. Once the document was downloaded it then executed VBA macros and downloaded Trickbot. Unsurprisingly, Emotet also uses the Coronavirus to spread, through phishing emails and also through a different approach, adding strings related to the Coronavirus pandemic into its executable payloads.

One such example included strings from a CNN article, placed inside an Emotet executable payload and in the details section of the payload, to both fool unsuspecting users and evade detection by NGAVs.

Interestingly, the paranoia around the pandemic has been shown to correspond with a rise in malware attacks in 2020, this is especially noticeable when you compare results to 2019. Data collected from D-Cloud, Deep Instinct's threat intelligence database, shows the number of new malware samples per month, since the beginning of 2019. In the graph, Microsoft Office documents are divided between the older format- OLE and the newer format- OOXML. The numbers are shown in arbitrary units, where the number of malicious OOXML files in January 2019 is set to 1. It is clear to see that there was a rise in malware attacks in 2020, most notably in document formats.



An additional point which should be addressed is the great rise in e-commerce activity, as many businesses can only supply their products through online orders due to the pandemic. This increased digital activity widens the attack surface both of businesses and users, as more transactions are occurring online and attackers have a wider pool of targets.

Though the pandemic will hopefully soon be behind us, some of the changes caused by it are here to stay. Certainly the cybersecurity attack landscape has changed due to the transition to WFH and due to the increase in digital activity, trends which both look as if they are likely to continue. Attackers, rarely missing a beat, are going to take further advantage of these trends and the cybersecurity arena must adapt to deal with them proactively.

CYBER INSIGHTS: SOLARWINDS ATTACK

On December 8th, the security company FireEye disclosed that it had been breached by an advanced, supposedly nation state-backed, attack group, and as a result- tools developed and used by the company's red teams were stolen.

The Trojanized Orion Update

It was later disclosed that the attackers were able to infiltrate FireEye's network by infecting updates of a popular IT infrastructure management software named Orion, with their malware. Orion is a SolarWinds product, used by many organizations, including many Fortune 500 companies and numerous US Government Departments, who were all affected by the campaign. The malware is believed to have been distributed in Spring 2020, compromised Orion versions 2019.4 HF 5 to 2020.2.1, and most likely resided in breached networks for months without being detected.

...most likely resided in breached networks for months without being detected.

Techniques to Avoid Detection

The trojanized updates delivered a backdoor, dubbed "SunBurst" by FireEye and "Solorigate" by Microsoft, that allowed the attackers to steal data, which is assumed to be the attack's primary goal. To avoid detection, the attackers had limited the malware's capabilities, tracked security software installed, and put a lot of effort into making SunBurst's network activity look normal. The breadth, sophistication, and scope of the attack and [evasion techniques](#) indicate it was perpetrated by an advanced threat actor with ample, state-level resources and motivation.

Although the attackers had likely planned for their actions to be hard to attribute to any specific attack group, many in the cybersecurity and intelligence communities believe that the attack group APT 29, aka "Cozy Bear", was behind these attacks. Yet, the Russian Embassy in the USA, has since denied this accusation.

Scale of the Attack

The high profile and enormity of the attack entails the compromised data of many millions of end-customers, causing the event to be of wide public interest. Recently, more organizations confirmed that they were compromised by "SunBurst". On December 17th, the FBI, DHS-CISA, and

the Office of the Director of National Intelligence (ODNI) confirmed in a joint statement, that the backdoor had affected US federal government networks. On December 21st, VMware confirmed that its network was also compromised by the attack, but claimed that the attackers did not use their access to the network for any additional malicious purposes. Microsoft also confirmed that it found variants of the backdoor in its network, however, the company claimed that there is no evidence that attackers had accessed any customer data or compromised any of its products.

The high profile and enormity of the attack entails the compromised data of many millions of end-customers, causing the event to be of wide public interest.

Putting Out the Fire

As mentioned earlier, the attackers stole tools developed by FireEye's red team, to test their customers' security. These tools can be used dually for malicious purposes as well, so knowing that they are in the wrong hands, FireEye released rules and IoCs, that can help security vendors detect and prevent the use of the stolen tools in the networks they are entrusted with.

Moreover, SolarWinds released an update and urged its customers to install it, so it could replace the compromised versions. We call on our customers and partners to update SolarWinds software where applicable.

Deep Instinct's Customers can Rest Assured

As one of the leading cybersecurity companies today, Deep Instinct is always on the alert for new attacks of this kind and does everything in its power to ensure our customers are protected from any threat they might face. We are focused on expanding and monitoring all relevant IoCs and making sure Deep Instinct's cybersecurity product line protects against them.

CYBER INSIGHTS: RISKS PRESENT AT US ELECTIONS

The US presidential elections always draw a lot of attention from all sectors. For those who are highly invested in the results, some try to extend their influence by supporting one of the candidates or donating to their campaign, others choose a more creative way – by distributing malware.

Amid the “Special Counsel” investigation, which concluded that the 2016 presidential election had been maneuvered by Russia in favor of one of the candidates, many government organizations and private cyber security organizations were on alert for similar interference in the 2020 elections. Risks were assessed, ransomware was named one of the highest risks to the purity of the election process, and measures were taken to minimize the chances for that to happen.

Security officials strongly encouraged states to implement security measures, such as multi-factor authentication and network segmentation. States were also tasked with creating offline backups of their voter registration databases and election result reporting systems, so that any data point could be relatively easily replaced. On the offence side, security organizations took a more proactive approach to tackle potential attacks by disrupting the work of threat actors. One such example is the uncoordinated work of the US Military and Microsoft to paralyze, at least temporarily, the TrickBot malware group.

On the offence side, security organizations took a more proactive approach to tackle potential attacks by disrupting the work of threat actors.

Microsoft vs. TrickBot

TrickBot is a notorious botnet, that has been causing havoc since 2016, and is known for stealing sensitive information using various techniques and mechanisms, such as TrickBooster. It is also known for dropping and executing other malware, like the Ryuk ransomware. The botnet is estimated to have more than a million devices under its control. It is believed to be serving the objectives of both nations-states, and criminal organizations. The combination of both its adoption and widespread infection has worked to establish its status as a highly dangerous threat to democratic processes and a prime target for security organizations.

In order to tackle TrickBot, Microsoft launched an investigation, which concluded with the discovery of the servers used by the botnet to control its infected victims and their precise IP addresses. With this information in hand, Microsoft was able to get a court order from the United States District Court for the Eastern District of Virginia, allowing it and its partners to shut down the susceptible IP addresses, make the data stored on them inaccessible, and block the operators of the botnet from being able to lease or buy additional servers. Microsoft’s court case included a copyright claim against TrickBot’s use of its software code, making it the first time the company’s digital crimes unit had taken this type of legal action. The success of this approach may foreshadow an increase use of copyright claims as a means to combat malware campaigns.

Although this was just a temporary solution, it was enough to sabotage TrickBot’s effort to disrupt the election process.

A Phish with a Touch of Politics

As with any major event, malicious actors took advantage of the hype surrounding the elections to distribute phishing campaigns. The scam emails included related content, such as compelling messages that pretended to originate from one of the candidates, their parties or a different political organization, that would ask users to show their support by signing a petition, donating money, etc. Some even tried to convince potential victims that they can vote by phone, text or email, all of which are not viable options.

These attacks and others successfully provided threat actors with personal identifiable information (PII) from the many people who fell victim.

CYBER INSIGHTS: ADVERSARIAL MACHINE LEARNING

The Emerging Threat

Machine Learning (ML) has established itself in the recent years as not just a cool buzz word excessively used in cyber-security conferences and product feature lists, but also as a proven technology that has successfully delivered results across fields. Cyber-security companies like Deep Instinct utilize machine and deep learning-based technologies in their products to detect security threats more effectively, compared to classic signature-based products. These legacy products can be evaded using techniques of a relatively low level of sophistication; such as binary file packing, process injection, delayed execution, and other evasion tricks.

With the rise of ML-based security solutions, malware authors are beginning to employ adversarial machine learning to effectively evade them. Adversarial machine learning is a technique aimed at deceiving the ML model by providing specially crafted input to fool the AV into classifying the malicious input as a benign file and evade detection. A veritable cyber arms race is on, in parallel with the development of adversarial machine learning, the producers of ML-based cyber-security solutions are investing considerable effort into anticipating and researching adversarial techniques, so they can mitigate this risk. Between them they even hold open ML model evasion [challenges](#).

As one of the leading cyber-security companies applying deep learning to cybersecurity, Deep Instinct continues to play a significant role in advancing adversarial machine learning research. Over the course of this year our research group contributed to the defining and outlining of various attack vectors and methodologies used in adversarial machine learning, producing a [ML threat matrix](#) that builds on the widely used MITRE ATT&CK framework.

At Black Hat Europe 2020, Deep Instinct's researchers also demonstrated a novel methodological approach to "reverse engineer" an NGAV model without reversing the product and yet still generating a PE malware that bypasses next generation anti-virus (NGAV) products.

Not only in theory, but also in the field, Deep Instinct's research group spotted one of the first in-the-wild examples of an adversarial machine learning attack, used in the widespread malware family - Emotet. To evade the ML model that lies at the heart of an NGAV, Emotet's coders came to an extremely easy and effective technique. Since most of the classic ML-based AVs classify files based on the presence of benign and malicious features, Emotet's executable files contain a large portion of benign code that is not part of its functionality, and is never executed, but is used to obscure the malicious features. The malicious code is effectively 'camouflaged' by the inordinate amount of benign features that gets scanned without alerting any alarm.

Machine learning has led to ground-breaking innovations in cyber-security and other fields affecting our day-to-day lives. Like a classic cat and mouse race, new technology intended to deliver tangible benefits, will always spark the interest of hackers to manipulate it with never-seen-before methods. Adversarial machine learning is merely the latest attempt in that evolutionary journey.



**Deep Instinct's
research group
spotted one of the
first in-the-wild
examples of an
adversarial machine
learning attack**

CYBER INSIGHTS: A LOOK BACK AT OUR 2020 PREDICTIONS

No one could have possibly predicted what a year 2020 would be. The year that was dominated by the COVID-19 pandemic has also seen several other developments, all dwarfed by the pandemic and likely, impacted by it.

Nonetheless, we would like to take a look back at our prediction for this year, and see how they turned out.

Prediction that multi-purpose malware will become more common:

Several of our predictions turned out to be spot-on, and this was certainly one of them. Multi-purpose malware was already apparent in ransomware, but many malware variants have since added several additional functionalities, such as information theft, and the ability to propagate within target networks.

Prediction that there will be an increase in the scope and rate of mutations in malware:

This development was clearly seen in some of the most prominent malware strains in 2020, such as Emotet and Trickbot. 2020 also saw an increase in attacks that are fileless, mostly through attacks utilizing complex Powershell backdoors, which are capable of performing a completely fileless attack flow.

Prediction that malware evasion techniques will develop and be more focused on evading AI-based products:

Fortunately, this does not seem to have become a common trend in 2020. However, the increasing use of AI in cyber-security will motivate attackers to find a way to combat and bypass AI-based products.

Prediction that nation-states will further explore and implement AI in offensive operations:

Perhaps a far sighted prediction which still cannot be proved or refuted. There has been no public mention of such a development having occurred in 2020. However, as nation states have extremely evasive campaigns, the lack of publication is only an indication of this development not being found, rather than not actually occurring at all.

CYBER INSIGHTS: 2021 PREDICTIONS

With 2020 coming to an end (a wonderful thing for many of us) how is the cybersecurity landscape shaping up for 2021? With the wholesale structural shift to WFH, we look into how this rupture will continue to pan out in 2021. Cyber leaders will need to keep their proverbial 'finger on the pulse' to keep pace with the new risks, priorities and considerations that are emerging in this rapidly evolving arena.

COVID19 After Effects

While all the [COVID19 themed Mal-spam](#) that we've seen will eventually die down, the new arrangement of Working From Home (WFH) is going to become the industry norm. The concern is that in the time that it takes companies to upscale their security to meet the changing location and form of the office network, we will see hackers taking advantage of this window of exposure. Previously, an organization's network and all its data was sitting securely behind fortifications of the organizational security network. All of a sudden, the transition of moving to a wide and varied mess of different work environments made it far more complex for defenders to keep protecting the enterprise at the same level. Naturally, the organization's attack surface is amplified. While in the past only one attempt was all a hacker could get of successfully breaking in using a new variant of malware, now they have multiple attempts, all with equally good chances. And for an attack to cause damage, it only needs to succeed once.

While in the past only one attempt was all a hacker could get of successfully breaking in using a new variant of malware, now they have multiple attempts, all with equally good chances. And for an attack to cause damage, it only needs to succeed once.

An example of this was the [Cognizant incident](#) that hit the company early on in the work from home transition. The IT Service provider was attacked by ransomware that managed to bring business to a halt for a period of time and is alleged to have cost the company between \$50 and \$70 million.

Proliferation of Botnets and Access as a Service

Botnets have become one of the biggest cyber threats today, and by that nature a major cause for concern to those charged with cybersecurity. What makes botnets so dangerous is the size of their network, where the more infected online devices that a botnet has under its command, the wider its pool of malware delivery, and therefore the bigger its impact. And considering a hacker's ultimate goal is financial gain, malware infiltration or just disruption, the bigger the pool, the better. In 2021, we expect to see more malware creators sell access to their botnets, and thereby access into their network of millions of infected connected devices, an exchange that researchers at Deep Instinct coined 'Access-as-a-Service'.

The implication of this is bad. These botnets have market value in the dark web for their ability to break down the attack chain into several components, so that a smaller scale hacker can just focus their efforts on fewer components of the attack chain, and thereby become more skilled in just those limited components. For example, the botnet will provide the initial access, while the hacker will focus their effort on becoming better at information theft or the ransomware logic.

Rising Cybersecurity Company Valuations

During the recent worldwide economic downturn, cybersecurity was one of the few industries to record growth. In 2021 we expect to see cybersecurity stock prices and company valuations to continue this upward trajectory, with multiples expected to reach new heights. This development appears to reflect a changing market perception of cybersecurity products no longer seen as a discretionary item, but rather as a staple.

2021 PREDICTIONS

Organized Cybersecurity Co-operation Between Government and Private Enterprise

Combatting the growing complexity of attacks has necessitated the collaboration between private companies and government security departments. This was particularly observed in the lead up to the US elections this past November where the U.S. Cyber Command branch of the Department of Defense collaborated with multiple security companies in an effort to take down Trickbot.

The malicious botnet, which is known to be one of the most active and dangerous, had many of its infected computers liberated, as the combined effort worked to put the brakes on the attempt to interfere with electoral systems.

Furthermore, Microsoft was able to clear a legal pathway to sabotage the botnet on the basis that the writers of Trickbot malware are infringing their terms of service. Instead of writing their own code from scratch, they're abusing Microsoft code, an activity that almost every malware writer is bound to do.

We expect to see this collaboration continue and escalate as more nation-states engage in cyber warfare and support both the development and defense efforts of APTs, zero-day exploits, and machine learning-based adversarial attacks.

U.S. Cyber Command branch of the Department of Defense collaborated with multiple security companies in an effort to take down Trickbot.

Escalating Adoption of Adversarial Machine Learning Malware

As knowledge on adversarial machine learning continues to grow, that knowledge is disseminating among both sides of the cyber battle ground. 2020 saw the increased adoption of machine learning academic knowledge being used in adversarial attacks in private industry research. As this knowledge gradually makes the transition from academia to the wild, we expect to see malware campaigns attempting to evade products based on machine learning models, either by fooling the model, learning how to subvert it, or by forcing it to shut down. Since machine learning-based products are becoming the market dominant solution, it makes sense that they represent the next target for well-resourced hackers. We expect that those perpetrating the attacks will be only a select few of very sophisticated and highly capable threat actor groups who most likely will be acting as part of a nation state sponsored campaign. The bar of entry to AI based attacks is still very high, and we therefore don't expect it to become "run-of-the-mill" malware next year.

Ransomware to Target Mission Critical Organizations

2020 saw ransomware attacks increasingly amplify their leverage to coerce ransom pay-outs by not only stealing a victim's sensitive data, but also threatening to expose it. It appears that the lesson learnt for hackers is that the test of a good ransomware attack is its method of extortion. The greater the stakes, the better likelihood of a payday. For this reason, in 2021 we expect to see a move towards targeting mission critical organizations, i.e. those organizations that have minimal risk tolerance to having their digital systems shut down or their data stolen and exposed.

Hospitals and educational institutions are a good example of this, with both sectors having already suffered from a wave of ransomware infections, both schools and hospitals are under enormous pressure to keep their doors open. In the crossroads between ransomware and data privacy regulations, private companies are also more susceptible to being breached, with the added risk of being hit with large fines if found to have exposed data.

CYBER INSIGHTS: THE COST OF AN ATTACK IN 2020

In 2020, Deep Instinct commissioned the Ponemon Institute to survey over 600 IT and security practitioners on the costs that would be incurred by their organization in the event of an attack. Respondents were first asked to estimate the cost of each of the following five types of attacks: phishing, zero-day, spyware, nation-state and ransomware. They were then asked to estimate what percentage of their cybersecurity budget is spent on each phase of the security lifecycle: prevention, detection, containment, recovery and remediation.

The results were as follows:

Attack Type	Average Total Cost Of Attack (USD)
Phishing	\$832,500
Zero-day	\$1,238,000
Spyware	\$691,500
Nation-state	\$1,501,500
Ransomware	\$440,750

While these results indicate the high cost of an attack, the study also found that by preventing attacks earlier on in the lifecycle, the savings are substantial. For example, a nation-state attack is the costliest attack to respond to in the cybersecurity lifecycle (\$1.5 million). If an organization is able to effectively prevent this type of attack, the cost savings could be an average of approximately \$1.4 million per attack. Likewise, a zero-day attack can cost an average of \$1.2 million, and could save \$1.1 million if prevented.

Attack Type	Average Total Cost Of Attack (USD)	Percent of Total Cost Spent On Preventing an Attack	Average Cost Savings Resulting From The Ability To Prevent an Attack (USD)
Phishing	\$832,500	18%	\$682,650
Zero-day	\$1,238,000	12%	\$1,089,440
Spyware	\$691,500	26%	\$511,710
Nation-state	\$1,501,500	9%	\$1,366,365
Ransomware	\$440,750	10%	\$396,675

The average percent of costs related to the four phases of the cybersecurity lifecycle (detection, containment, recovery, and remediation) are as follows: phishing (82 percent of the total cost), zero-day (88 percent of total cost), spyware (74 percent of total cost), nation-state (91 percent of the total cost), ransomware (90 percent of total cost).

Every stage of the cybersecurity life-cycle has its fixed costs, even if an attack is stopped before doing any damage. This is because there are still costs associated with the prevention phase of the cybersecurity life-cycle, such as in-house expertise and investments in technology. For example, as shown in the table above, the average total cost of a phishing attack is \$832,500. And of that total cost, 82 percent is spent on detection, containment, recovery, and remediation. Respondents estimate 18 percent is spent on prevention. Thus, if the attack is effectively prevented, the total cost saved would be \$682,650 (82 percent of \$832,500). If organizations experienced all the attacks listed in the study, the average total cost is \$4.7 million and if prevented, could save the organization an average of \$4 million.

Despite these significant cost savings, the study found that up to 76% of respondents say that they focus their efforts on the detection and containment of cyberattacks because prevention is perceived to be too difficult to achieve. The resistance to re-orientating towards a preventative approach to cybersecurity, is all the more pervasive when you consider that 70% of respondents agree that their ability to prevent cyberattacks would strengthen their cybersecurity posture.

[Read the full report](#) to discover the major factors that impact an efficient cybersecurity posture, and the value of a preventative model to help organizations optimize their security budgets while building their cyber resilience.

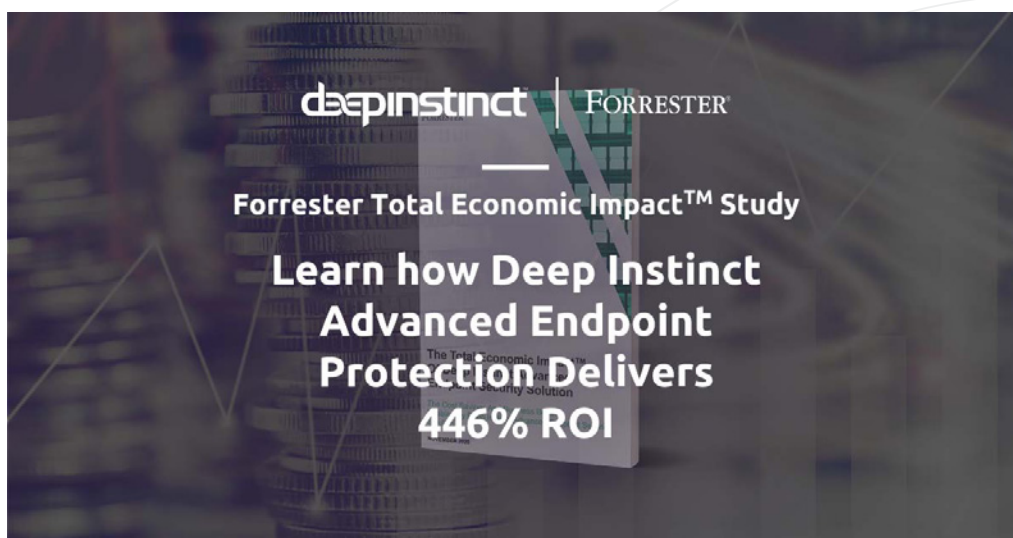
ABOUT DEEP INSTINCT



Dissatisfied with the available cybersecurity companies, Deep Instinct was born out of the desire to create a security product that would stop even the most sophisticated attacks. To achieve this, the uncharted territory of deep learning was pioneered by developing an artificial neural network brain that holds an instinctive ability to identify attacks pre-emptively. Doing so, with the highest rate of detections and minimal false-positives.

Talk about business continuity! Organizations that have adopted Deep Instinct's cybersecurity products don't even know they've been targeted! No stalling, no work interruptions, no expensive disasters.

At Deep Instinct, our customers prevent what others can't find.



www.deepinstinct.com

info@deepinstinct.com

deepinstinct
BEFORE YOU KNOW IT

© 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.