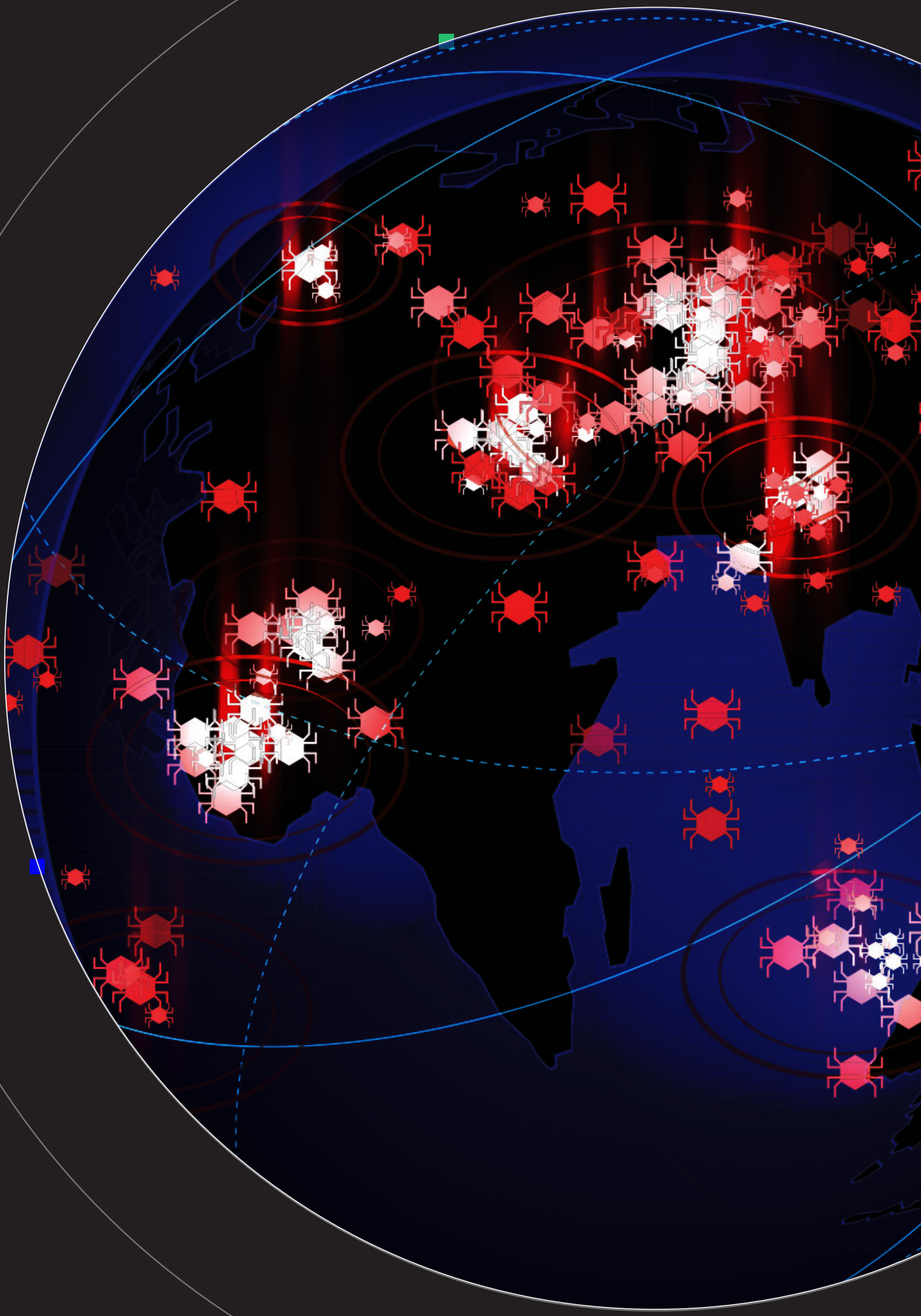
2021 Mid-year Threat Landscape Report



Trends, Takeaways, and Cybersecurity Predictions

www.deepinstinct.com

Table of Contents

Introduction 3

The Top Malware Trends of H1 2021 4

Top 5: Ransomware Campaigns 5

Top 5: Banking Trojan Campaigns 7

Top Takeaways 9

Predictions 12

Introduction

Welcome to our mid-year threat report highlighting the most significant cyber threats of the year along with trends to watch as we move through the second half of 2021. Even though this report is an interim analysis, it's worth noting that given the scope and scale of cybersecurity challenges facing organizations this year the findings could quite easily fill an annual review.

Cybersecurity attacks have continued to expand, not only in terms of threat vectors and sheer volume, but also in their damage and impact. There have also been some rays of light in the cyber community this year. The global community has begun to realize the importance of communication and cooperation in investigating and pursuing cybercriminals and their networks, and malware and ransomware are now top agenda items in strategy meetings among global leaders.

One of the more enduring developments that resulted from the COVID-19 pandemic is a lasting shift to a hybrid office model. We have not seen a significant return to the office as the vaccination rollouts progress, but are instead witnessing employees working from home several days a week with no end in sight. This trend increases the attack surface and as a result we have seen a rise in the number of phishing threats, especially with attackers posing as vaccine manufacturers or health providers, playing on their target's anxieties to gain access to personal information.

While ransomware is the top threat concern for cyber professionals according to our June 2021 study, "The Voice of SecOps," the evolving double-extortion ransomware tactic is gaining momentum around the world. Attackers are no longer content to simply encrypt the core infrastructure – they now often return weeks or months after the initial demand with a second threat. If the demand for more money is not met, these cybercriminals threaten to release sensitive company and customer information on the dark web.

We have also begun to see a significant debate on the moral, financial, and legal implications of paying a ransom. This is a highly complex topic which we will not comment on in this report, but we are confident it will remain a high-profile issue. Governments around the world will continue to both debate how to handle the scourge of ransomware, and, in parallel, collaborate to combat it as a serious local and global threat.

This report represents Deep Instinct's current view of the threat landscape and trends seen between the period January – June 2021 and provides concrete data to verify the credibility of these developments. The information was sourced from our repositories which are routinely analyzed as we continuously protect our customers from unending and varied attacks. We hope this report will provide you with a timely perspective on today's threat landscape and how it is likely to evolve through the end of this year and beyond.

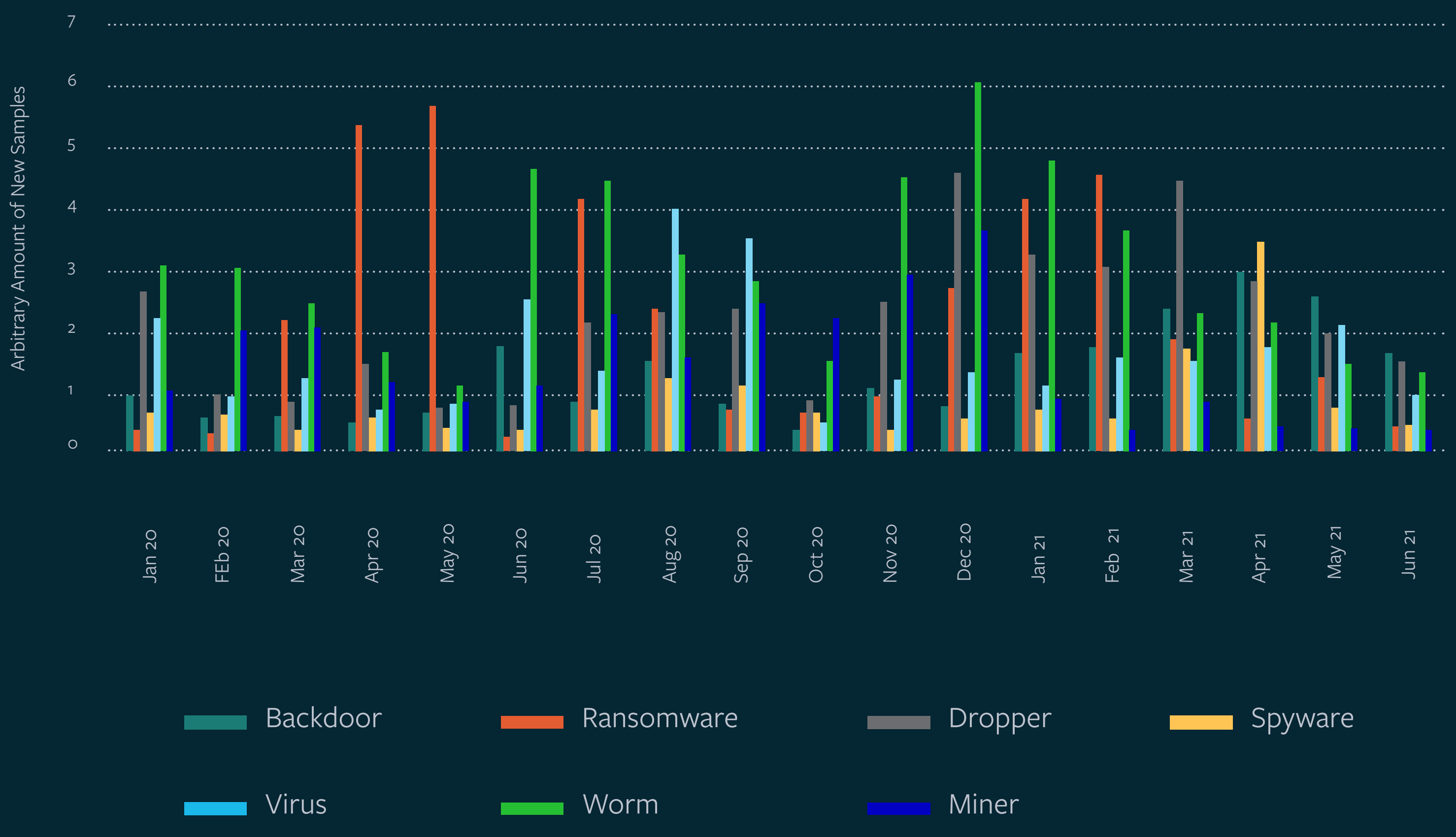
Best regards,

Shimon N. Oren

VP of Research and Deep Learning

The Top Malware Trends of H1 2021

At the midway point of 2021, the distribution of malware types per month remains relatively static over the last 18 months, with dropper, ransomware, and worm attacks constituting most significant threats. Ransomware continues to be a dominant trend. For example, we have seen an 800 percent increase in ransomware between January to June 2019 and the corresponding period in 2021.



The number of new samples in each month, since January 2020, grouped by malware type and shown in arbitrary units, where the number of backdoor samples in January 2020 is represented by one. This data was collected from and analyzed through D-Cloud, Deep Instinct's proprietary file reputation database.

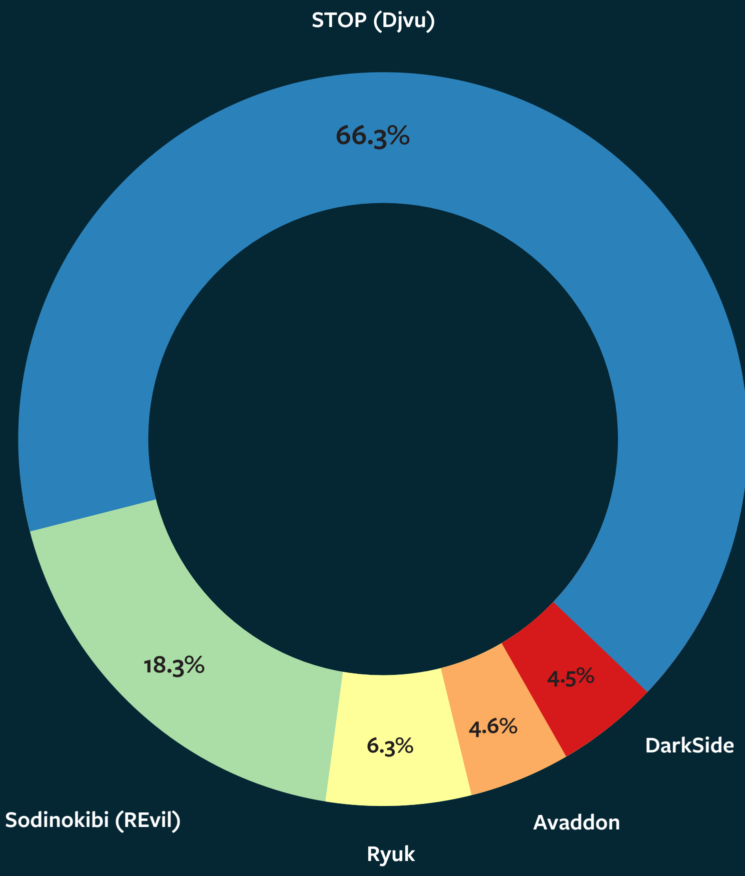
Top 5: Ransomware Campaigns in H1 2021

01 STOP (Djvu)

This ransomware campaign was first discovered in December 2018. It encrypts files on victim's machines using the AES-256 encryption algorithm; other algorithms have also been seen in newer variants. The encryption of files is partial – only the first 5 MB of data is being encrypted per file. STOP is focused on specific file types based on their file extension that include PDFs, Microsoft Office documents, databases, photos, music, videos, archives, and applications. The encrypted files are appended with various file extensions that might differ per STOP variant. Usually, the affected files will have the following file extensions: ".STOP," ".SUSPENDING," ".DATASTOP," ".djvu," ".djvuq," and many others.

One of STOP's variants, Djvu, is known for its persistence methods, which include modifying Windows functionalities. This may include disabling Windows Defender and blocking web traffic to security and downloads websites to prevent the victim from downloading security and decryption tools.

Figure 1: Top 5 Ransomware Campaigns in H1 2021 Based on Data from Deep Instinct's D-Cloud



02 Sodinokibi (REvil)

Sodinokibi, aka REvil, first appeared in the wild in April 2019 shortly before the dissolution of the Gandcrab ransomware gang. It has since been involved in several high-profile targeted attacks, predominantly against companies and government organizations. The attackers developing and spreading the ransomware have used several infection tactics, including the use of zero-days, PowerShell scripts, and human operated malware.

Sodinokibi operates as a Ransomware-as-a-Service and utilizes the "double extortion" technique in which the victim's stolen information is threatened to be released if the ransom is not paid. Sodinokibi is infamous for demanding $42 million from the former U.S. President Donald Trump and $50 million from the Taiwanese electronics giant Acer.

03 Ryuk

Ryuk ransomware was first seen in the wild in August 2018 and has since been involved in numerous targeted ransomware attacks against several high-profile targets such as municipalities, hospitals, and private companies.

Once Ryuk infects a system it gains administrator privileges, kills over 40 processes and more than 180 services, and gains persistence on the infected system before starting the encryption routine. Ryuk has been continuously developed and in March 2021 worm-like capabilities were added to the malware, enabling it to find vulnerable machines on a network and encrypt them as well.

CONTINUED ▶

Top 5: Ransomware Campaigns in H1 2021

04 Avaddon

Avaddon was first discovered in early 2020 when a forum post announced the recruitment of affiliates for this new ransomware strain, indicating that the malware would operate in a Ransomware-as-a-Service model. Two days later, the first malicious emails spreading the malware were observed.

In January 2021, Avaddon has adopted the "triple extortion" technique: In addition to stealing and encrypting the victim's data, the operators also conduct DDoS attacks against targets to force them to communicate. The Avaddon gang are infamous for attacking the insurance company AXA after the company stated that it will no longer cover damages from ransomware attacks in France. In June the group announced that they are ceasing their operations and have released all decryption keys publicly.

05 DarkSide

DarkSide first appeared in August 2020 and initially targeted organizations in English-speaking countries. The threat group behind the malware marketed it as a Ransomware-as-a-Service. The affiliates were asked to abide by the gang's code of conduct, which included avoiding the attack of organizations from several sectors, such as health and education.

Once a network was breached by DarkSide operatives, several sensitive artifacts were exfiltrated and PowerShell was used to download the DarkSide payload to several locations on the victim's computer, including a network share created by the attackers. After patient zero was fully infected, the threat actors moved laterally in the network, with the aim of reaching the Domain Controller (DC). If successful, a copy of the ransomware would be inserted into the DC to be used to infect additional targets on the same network.

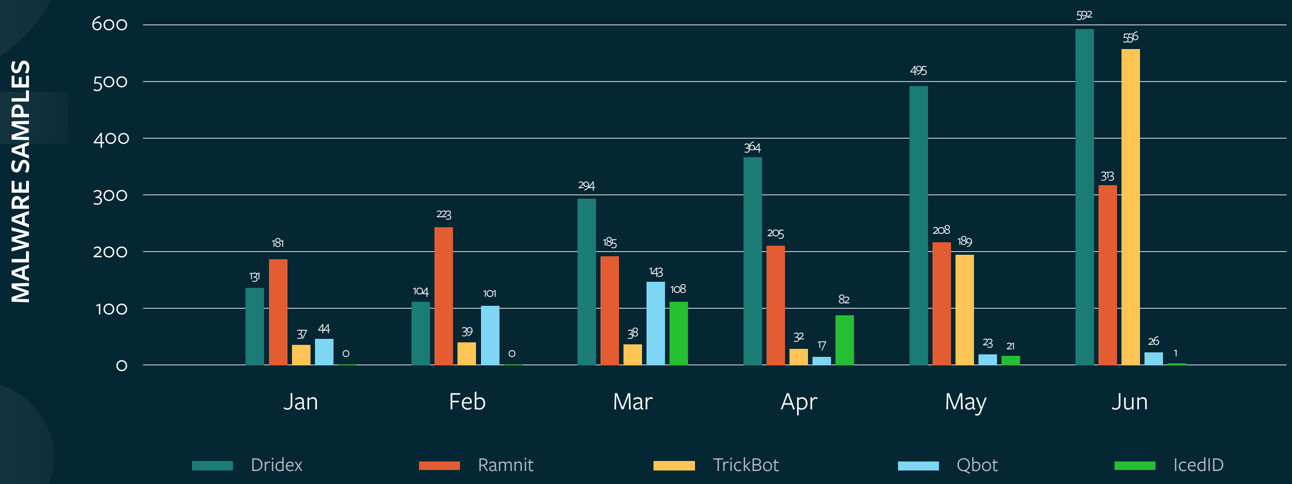
DarkSide was made infamous after its attack on the Colonial Pipeline Company on May 7, 2021. The attack caused disruptions in fuel supply, which led to fuel shortages on the East Coast of the U.S. As a consequence of this attack, DarkSide became the target of several law enforcement agencies and U.S. President Biden himself.

Following such unwanted attention DarkSide and several other ransomware gangs such as Babuk and Avaddon have discontinued their operations. But not before making ransomware a top priority for government and business leaders around the world.

Top 5: Banking Trojan Campaigns

The biggest update to our list comes from the most common banking trojan of the 2020 report, the Emotet malware; Earlier this year authorities shut down the Emotet botnet and completely terminated its operation.
But when one botnet is down, others take its place.

Dridex and Trickbot, both common botnets since 2020, are still quite active and have been joined by newer threats such as Ramnit, Qbot, and IcedID, all of which have grown in popularity among cybercriminals.



01

IcedID

IcedID is a modular banking trojan that has been active since September 2017, mainly targeting businesses in the U.S. and the UK. IcedID typically targets the finance industry, aiming to attack banks and credit card companies as well as eCommerce websites.

IcedID is distributed mostly 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. It also employs simple evasion techniques like only operating after a targeted machine restarts. IcedID manipulates the victims' browsers to display a correct URL address with a valid SSL in banking websites, but actually redirects the traffic to a fake website where credentials are stolen.

02

Ramnit

Ramnit, an active trojan since 2010, is a veteran malware which initially began its life as a Worm, spreading by infecting removeable drives. However, it quickly evolved into a fully-fledged banking malware by leveraging leaked code from ZeuS and, later, from Gozi/Ursnif.

Its evasiveness and ability to manipulate online banking sessions and steal credentials made it a formidable foe. And if that's not enough, Ramnit can also deliver other malware, turn an infected device into a remote-controlled bot, and extract sensitive information from a victim's machine.

CONTINUED ▶

Top 5: Banking Trojan Campaigns

03 Qbot

Qbot is a popular info stealer and banking malware active in the wild since 2009. Its main features are stealing 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 that allow it to spread through network and removable drives. It has been in the wild since 2009 and has been constantly updated to become more malicious.

Qbot monitors the browser on the infected machine to detect when victims interact with an online banking website and then steals credentials. 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 that trigger the infection or exploit kits that are deployed on compromised websites that deliver Qbot’s payload to the website’s visitors.

04 Dridex

Dridex is a highly active banking trojan campaign, in the wild since 2011 (initially 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.

This malware usually spreads via mass email campaigns. Dridex 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 to its C&C servers. Other variants include a crypto-currency wallet credential stealing mechanism.

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

05 TrickBot

TrickBot, which first appeared in 2016, is a sophisticated banking malware that targets bank account credentials, financial data, and personal information of individuals, small-to-medium businesses (SMBs), and enterprise environments in order to carry out financial fraud and identity theft.

Trickbot is a prevalent threat, spreading via malicious documents in mass emails and evolving over time. Its different malicious abilities and evasion techniques are built in a module architecture which allows easy swapping, modifying, and rebuilding for each campaign, allowing the malware to reduce detection rate and operate a range of attack techniques. Due to its architecture, Trickbot has several abilities in addition to credential stealing. It can operate as a backdoor, having network spreading abilities and email harvesting features depending on its deployment. In some cases, Trickbot has delivered a ransomware-like screen lock option, which is meant to steal system passwords.

Top Takeaways

In this section, we revisit the 2020 report main takeaways, and explore how these have evolved since the original report's publication.

01 Cybercriminals Seize Opportunities Created by the Coronavirus Pandemic

Although the majority of countries have already overcome the worst of the pandemic, there are some parts of the world where mass vaccination has not occurred or is lagging. The pandemic continues to play a major role as a social engineering cover story found in phishing emails, malware distribution campaigns, and other scams that focus on COVID-19 vaccines.

As the vaccination process is top-of-mind in most countries, we are seeing more attempts from attackers to lure victims by using phishing emails masquerading as one of the vaccine manufacturers.

We have seen many phishing emails disguised as Pfizer and targeting healthcare institutions. These phishing emails usually contains attachments designed to steal credentials, and in some cases, drop spyware and ransomware onto the victim's machine with the potential to cause serious damage.

02 Emotet's Demise – Is it the end?

Emotet has been one of the most significant malware threats in recent years. In January 2021, Emotet's botnet infrastructure has been dismantled in a successful and well-planned worldwide law enforcement joint operation and on April 25 of this year, Emotet was finally uninstalled from all the affected machines it infected.

Aside from its botnet expansion, Emotet has also been used as a delivery medium for other widely used malware threats such as TrickBot, Ryuk, and QakBot. Now that it is gone, these threats remain, and we are seeing less "popular" malware variants emerging.

An activity surge of BazarCall and IcedID was charted in March, which can be considered among the first signs of new malware "brands" gaining popularity among threat actors. BazarCall, is used in a similar way to Emotet in its delivery of additional malicious payload.

The malware delivers BazarBackdroor to provide threat actors with remote access to infected machines, and Ryuk ransomware (through BazarCall's BazarLoader component) that has a different destructive cause as well as TrickBot which is speculated to be linked with the BazarCall operators. We do see evidence that BazaarCall may be trying to replace Emotet's functionality. IcedID, on the other hand, is a banking Trojan seen in the wild since 2017 aimed at personal online credentials and sensitive data theft, which just became much more popular among threat actors in recent months.

Malware – like species in nature – will compete for dominance. Veteran malware threats inspire new variants that improve the well-developed techniques and common practices that have been proven to work. We must be resilient in researching and addressing emerging threats to ensure we can respond to and stay ahead of cyber threats.

Top Takeaways

03 Double Extortion – Two for the Price of One

Ransomware has been a part of our world for many years, and until late 2019, the playbook used by cybercriminals was simple: a ransomware arrives at a victim's computer, encrypts its content and possibly other data on other machines in the network, and then a ransom is demanded for the decryption. This simple concept had a straightforward safety net which many organizations chose to implement - create offline backups and use them in the unfortunate event of a ransomware attack.

Uploading the backups to all affected systems can be quite time consuming and labor intensive, leading some companies to prefer to pay the ransom instead of losing money, customer trust, and credibility while their systems are down. But since malware authors could not risk their hard work resulting in zero payments, they developed a new tactic to pressure their victims to cave in and pay - double extortion.

This adds a stage to an old tactic; before encrypting the data, the threat actors search for sensitive documents and personal information that can hurt an organization if it were to become public. They load this information to a remote server and use it as leverage to force payment. If the payment is not made, threats are issued that the sensitive information is made public, and their files will also remain encrypted. This double threat can lead to loss of reputation, loss of stock value, or GDPR and other customer lawsuits.

One of the first families to implement double extortion was Maze ransomware, which has been going strong – and interrupted - since late 2019. Since this tactic has proven to be quite affective, more and more threat actors are choosing to implement it, which means it is here to stay. The average ransom amount has gone up each year since this tactic was added to many attackers' utility belts. In 2019, the average was $115,123 and in 2020 the average escalated to $312,493. We see signs in this upward trend continuing. Just this year, we witnessed the Colonial Pipeline being targeted by DarkSide ransomware and paying $4.4 million to the attackers to get their data decrypted and keep their sensitive information unpublished. The attack ransoms will only rise until ransomware is stopped en mass.

04 Stronger Partnerships Between Government and Private Sector

Malware operations have now become complex crime organizations that consist of developers, operators, money mules, and affiliates in different countries around the world. The efforts to take them down have become more and more complex as well. It requires collaboration between several parties from both the private and the government sector to affect change and work to investigate attacks and apprehend criminals.

On January 26 of this year, we witnessed the cooperation between law enforcement agencies in seven countries and a group of private cyber researchers to bring down the Emotet empire in what was dubbed "Operation Ladybird.". For more than seven years Emotet was one of the most prevalent and sophisticated malware families. Considering its continuous development and abundant network of bots, it was a significant event in the cybersecurity world to bring such a network to heal.

Although there are only a few examples of private and government sectors openly cooperating this year, we see different law enforcement agencies from around the globe sharing intelligence and arresting those involved. For example, in February it was the cooperation between Ukraine, France, and the U.S. that brought down the Egregor ransomware gang and their infrastructure. In June, several suspected members of the Clop ransomware gang, which had infected companies in a variety of industries, were apprehended by law enforcement agencies from Ukraine, the U.S., and South Korea. These partnerships raise the stakes for malware creators and hopefully will render this crime much more risky and less popular.

Top Takeaways

05 Advancing Adversarial Machine Learning

In our 2020 Threat Landscape Report, we wrote about Deep Instinct's involvement in research to address the challenges coming from Adversarial Machine Learning (ML). Although not yet very common, we do notice signs of Adversarial ML in the threat landscape.

While not true Adversarial ML incidents, recent high profile cases like the Solarwinds/Sunburst affair and the Microsoft-signed rootkit incident can still be examined and researched through this lens. Both incidents provide a glimpse into what a potential Adversarial Machine Learning attack might look like – a small, nearly undetectable change in a large benign feature-space. Such examples also illustrate the difficulties the industry will face in the future in addressing these threats, signifying the importance of progressing research specifically of addressing the Adversarial ML attacks.

References:

https://www.cisecurity.org/solarwinds/

https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/

Predictions

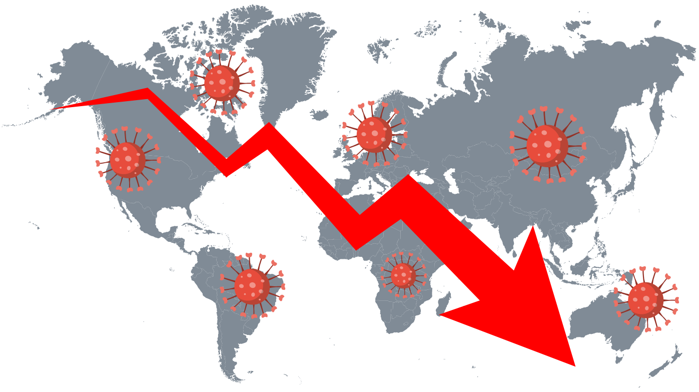
We look back at some of the major predictions we made in the 2020 report, and examine how these stand up today. Did many of these forecasts became a reality?

COVID-19 After Effects

The mass move to employees working from home, and a now dominant work-from-home culture may lead to the risks of unsecured workstations (endpoints) that are part of the organization and can provide network vulnerabilities. This will be a growing area of concern for cybersecurity professionals.

Some companies have already announced policies allowing their staff to work from home after the Covid-19 threat ends, and some even declare they will be able to work from home indefinitely.

As convenient as it may be, these kinds of decisions are having drastic impacts on the threat landscape. In the past, an attacker would have to breach the perimeter defenses to reach the victim's machine.



In our new reality, where the office is practically everywhere, the perimeter is irrelevant, and more attack attempts might reach our workstation. Securing our workstation with a good endpoint security solution is now becoming much more important.

References:

https://www.cityam.com/deloitte-tells-staff-they-can-work-from-home-forever/

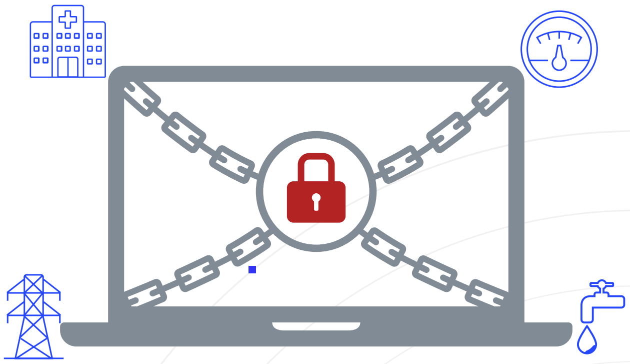
https://www.bbc.com/news/business-56759151

Ransomware to Target Mission-Critical Organizations

Cybercriminals use ransomware to steal money – plain and simple. The larger the target, the more money can be extorted. And the more important the entity, the more money will likely be paid to restore data and return to normal activity as quickly as possible. For this reason, we have seen an uptick in the targeting of mission-critical infrastructures, like healthcare organizations and electric utilities, and we predict these organizations will only continue to be targeted with greater frequency.

In 2020, in the midst of the Covid-19 pandemic, many healthcare organizations were targeted by different ransomware families- hospitals in the U.S. were attacked by Ryuk, Maze attacked Hammersmith Medicines Research (just days after it had promised not to target any healthcare organization during the fight against the pandemic), and other ransomware families took similar opportunity to exploit high-profile, highly important organizations during this time of global crisis.

In our 2020 End of Year Report, we predicted that mission-critical organizations would continue to be targeted by greedy threat actors. And, unsurprisingly, we were right. Just a few months ago, the Colonial Pipeline Company, which supplies 45 percent of the fuel to the East Coast of the U.S., had been attacked by DarkSide ransomware and paid $4.4 million in Bitcoin on the day of the attack to regain normal activity.



However, everything comes with a price – and in the case of cybercriminals overextending their attack vectors and preying on mission-critical companies, this price may come in the form of a different kind of targeting – by the U.S. government, no small adversary.

CONTINUED ▶

Predictions

Ransomware to Target Mission-Critical Organizations (cont.)

. This is what happened to the group behind the DarkSide ransomware, which was used to attack the previously mentioned energy company. Just days after the attack, U.S. President Biden announced that the U.S. would retaliate, and so it was - DarkSide's servers were shut down, the U.S. Department of Justice seized 2.3 million USD in Bitcoin paid to the threat actors, and the group announced an unceremonious early retirement. Moreover, in fear of similar retaliation, other threat actors, including the group behind the Babuk ransomware, which had attacked the Washington D.C police department about a month before, decided to retire as well.

While attacking critical infrastructures can be profitable it comes with large risks. But the rewards are potentially great, so we will likely see other ransomware families taking a chance and targeting mission-critical organizations, crossing their fingers and hoping they will not pay the price.

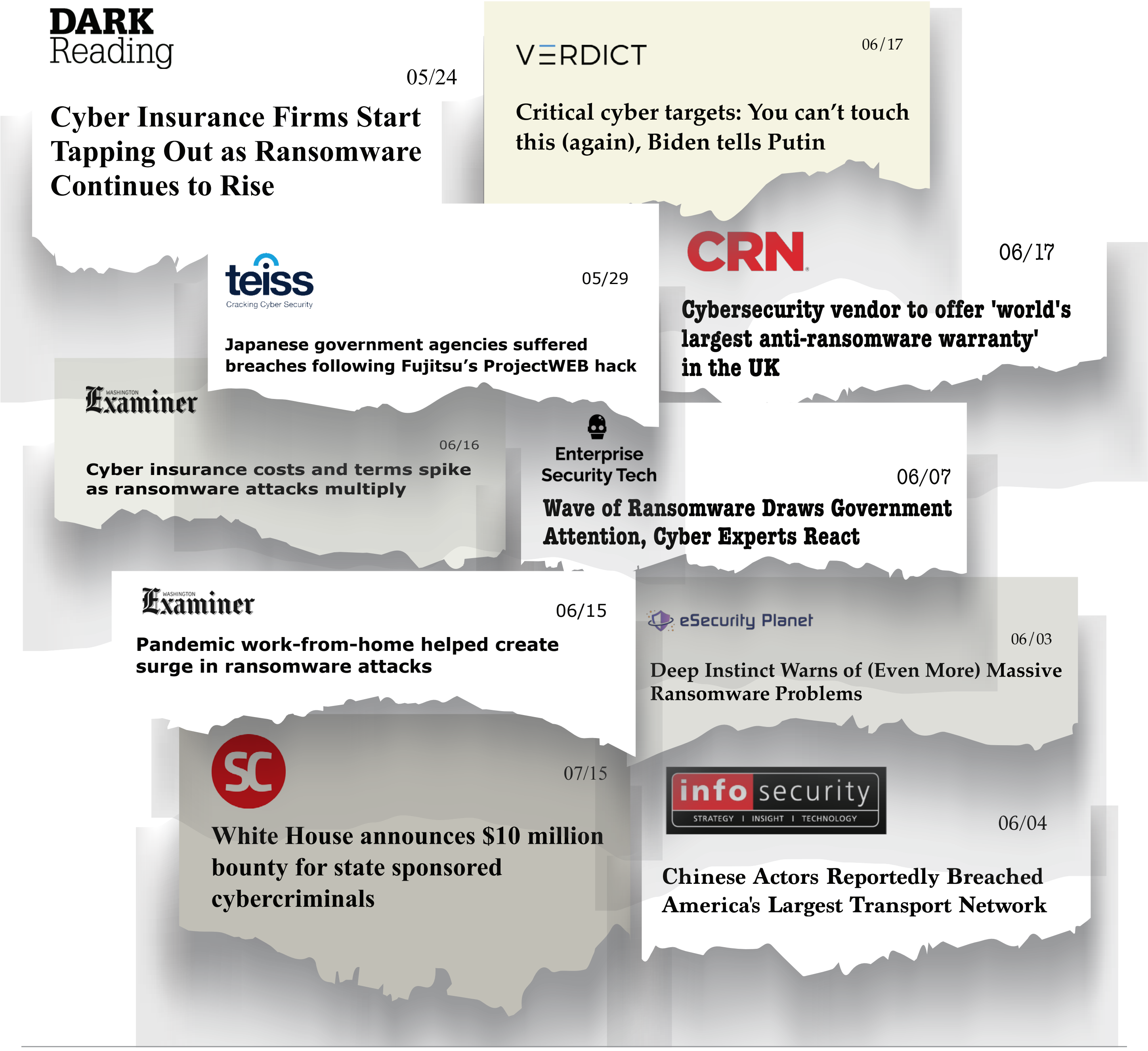
A Rise in Organized Cybersecurity Collaboration

As cybercriminals continue to develop new and sophisticated malware attacks, many governments and private companies are working tirelessly to shut down botnet operations and bring to justice the actors behind these attacks.

In our 2020 Cyber Threat Landscape Report, we discussed the cooperation between governments and private enterprises and predicted the growth in collaboration between these two sectors. Like the collaboration we saw in 2020 to take down the Trickbot botnet, this year we've seen additional partnerships between the public and the private sectors.

Botnets such as Trickbot have cost millions in damages to critical infrastructure worldwide, making them high-value targets for governments and private companies alike. Earlier this year, we also witnessed the takedown of the Emotet botnet, which many considered as one of the most infamous cybercrime services to date used to deliver ransomware, as well as other malware and cause havoc in organizational networks. This takedown was a collaborative effort between authorities in North America and Europe, with international activity coordinated by Europol. Acting Deputy Attorney General John Calrin referenced this cross-continent collaboration, *"Working with public and private partners around the world we will relentlessly pursue them while using the full arsenal of tools at our disposal to disrupt their threats and prosecute those responsible."*

With the long-lasting negative economic impact delivered by these cyberattacks, it is easy to understand why these important collaborations are already becoming common practice and why we can expect these relationships to strengthen. Partnership can only improve the health and prosperity of our global economy and, with it, the safety and security of our global citizens.



DARK Reading 05/24

Cyber Insurance Firms Start Tapping Out as Ransomware Continues to Rise

VERDICT 06/17

Critical cyber targets: You can't touch this (again), Biden tells Putin

teiss Cracking Cyber Security 05/29

Japanese government agencies suffered breaches following Fujitsu's ProjectWEB hack

CRN 06/17

Cybersecurity vendor to offer 'world's largest anti-ransomware warranty' in the UK

Washington Examiner 06/16

Cyber insurance costs and terms spike as ransomware attacks multiply

Enterprise Security Tech 06/07

Wave of Ransomware Draws Government Attention, Cyber Experts React

Washington Examiner 06/15

Pandemic work-from-home helped create surge in ransomware attacks

eSecurity Planet 06/03

Deep Instinct Warns of (Even More) Massive Ransomware Problems

SC 07/15

White House announces $10 million bounty for state sponsored cybercriminals

info security STRATEGY | INSIGHT | TECHNOLOGY 06/04

Chinese Actors Reportedly Breached America's Largest Transport Network

This report was authored by members of the Deep Instinct Threat Research team:

Shaul Vilkomir-Preisman
Bar Block
Moshe Hayun
Ido Kringel
Maxim Smoliansky
David Krivobokov

deep instinct

www.deepinstinct.com | info@deepinstinct.com

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack—providing complete, multi-layered protection against threats across hybrid environments.