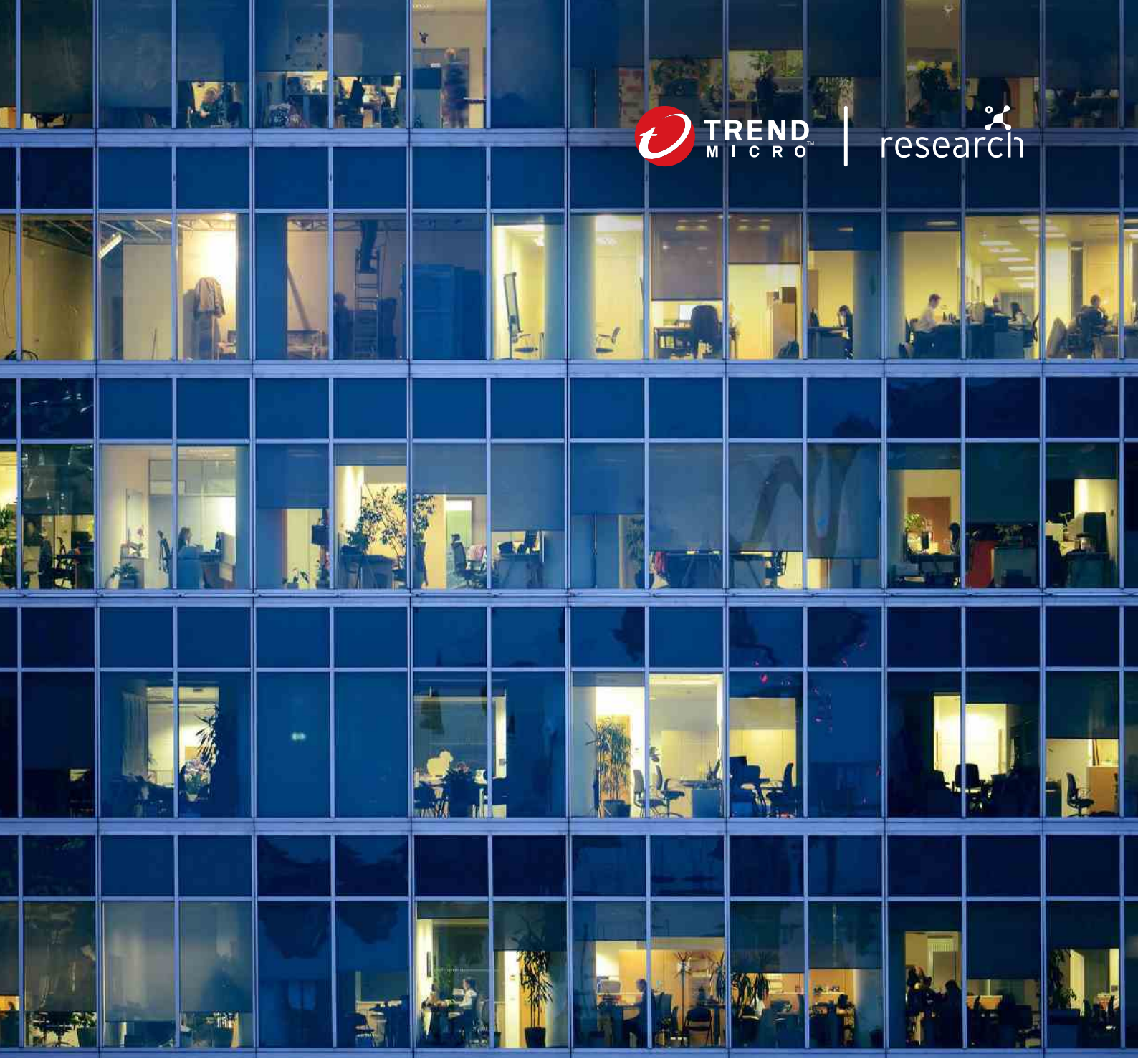

TREND MICRO | research

Attacks From All Angles

2021 Midyear Cybersecurity Report

Published by

Trend Micro Research

Stock image used under license from Shutterstock.com

Contents

Cybercriminals across the board were busy in the first half of 2021, with no signs of slowing down. Within the last six months, we saw a ransomware group shut down a major gas provider and leave half of the US East Coast without fuel. Other ransomware operators used double extortion tactics to get million-dollar payouts from enterprises. Advanced persistent threat (APT) teams compromised integral enterprise tools like Amazon Web Services (AWS) cloud servers, Kubernetes, and a popular webmail platform in Asia, all with different agendas: Some attempted to steal financial account information, while others attempted to load cryptocurrency miners. Critical bugs in major server clients and in popular printer technology were also exploited.

Our research into the first few months of the year examines dangerous vulnerabilities across different types of devices and operating systems, including the threats targeting these flaws. One example of this is our three-part investigation into the security of low-powered Long Range Wide Area Network (LoRaWAN) technology that is widely used in internet of things (IoT) configurations around the world. We also analyzed threats aimed at new Mac devices, specifically machines that use ARM64 architecture, as well as vulnerabilities in Windows operating systems and Linux machines.

Covid-19 threats continued as well, as pandemic-themed scams began revolving around a much-awaited vaccine and plans about its distribution rather than the disease-focused topics previously seen in 2020. Indeed, though the discovery of the vaccine has created a new sense of optimism, vigilance in securing the cybersecurity threshold remains indispensable.

In looking back at the threats that surfaced in the past six months, we hope that our midyear report encourages both enterprises and ordinary users to build a better and more effective defense that covers all angles of their security posture.

Modern Ransomware Attacks Prompt Multi-State Emergency Responses and Multimillion Dollar Payouts

Modern ransomware continues to be a significant threat to enterprises and government organizations. Cybercriminal groups have taken on more sophisticated business models and adopted new technologies to create efficient and stealthy ransomware attacks. These evolved attacks have certain features that separate them from traditional ransomware activities: data exfiltration rather than simple encryption, covert online collaboration, the extended use of affiliate programs, and APT-like victim targeting, among others.[1]

Most notably, in the first half of the year we saw modern ransomware actors successfully extorting companies and extracting valuable enterprise data using a double extortion technique: On top of demanding ransom in exchange for decrypting data, attackers placed increased duress on their victims by threatening to release their private data on a leak site. Enterprises that hold valuable intellectual property will view this as a serious concern, as data leaks come with regulatory penalties, lawsuits, and reputational damage. We also saw the rise of triple distributed denial-of-service (DDoS) attacks and quadruple extortion models to harass customers and increase their possibility of payment.

We researched the ransomware-as-a-service (RaaS) sites of 16 ransomware actors[2] and investigated how these actors extort money from their victims. Some keep terabytes of stolen data online for over a year and threaten to leak increasing amounts of data over time, though most keep stolen data publicly available for several months. Some of these data leak sites are on Tor-hidden servers, while others are hosted using bulletproof hosting. RaaS actors also use commercially available and free file-sharing platforms, or even host files on websites on the clear web.

How Active Were Ransomware Actors in the First Half of 2021?

Our data shows that over 7.3 million ransomware threats were detected in the first six months of 2021, which is almost half the number of detections we found in the same period in 2020. There are several factors that might have contributed to this decrease. First, it signals the shift to the more targeted modern ransomware[3] that we have been analyzing, which involves attackers moving from the less effective, quantity-focused model of ransomware to big-game hunting. We can also attribute this decrease to an improvement in the detection and blocking capabilities of security solutions. Threats were stopped and blocked before they even reached users, and so detections also dropped. It's important to note that modern ransomware uses phishing and exploits as the first step in the infection process, so when security solutions block this initial intrusion, the deployment of ransomware is prevented. Furthermore, an incident with the DarkSide ransomware brought heightened attention to ransomware operators, which might have prompted some of them to lie low. Meanwhile, law enforcement agencies across the world conducted a series of ransomware operations takedowns that might have left an impact on wide-reaching active groups.

The WannaCry and Locky families made up most of the detection count, continuing the trend we saw in our 2020 Annual Roundup.[4] WannaCry is a familiar threat that started plaguing enterprises and users since 2017; however, this year, there was a marked decrease in WannaCry detection numbers. The longevity of this family shows how long a network worm can persist if devices are not patched properly, even when the actors are not maintaining the attack.

Meanwhile, DarkSide, Nefilim, and Conti are also among the top 10 families detected in this period and stand out significantly in terms of attack scope, tools, and techniques.

In terms of targeted industries, ransomware actors focused on many of the same sectors as last year. The most affected organizations were in banking, government, and manufacturing. We saw a surge in ransomware attempts on banking groups, although RaaS is opportunistic with regard to its targeting style. This means that attackers are not likely singling out banking businesses in particular.

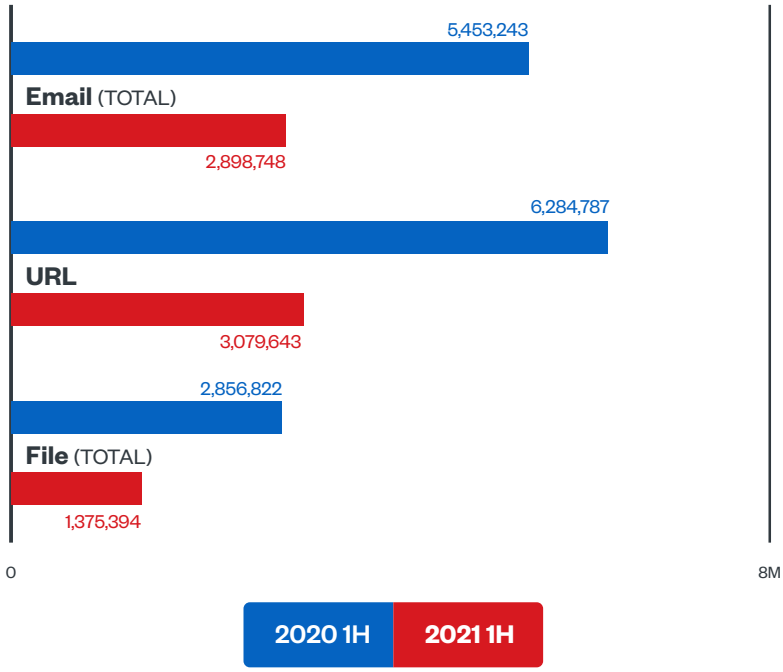

Figure 1. A half-year comparison of total detected ransomware monthly threats by layer

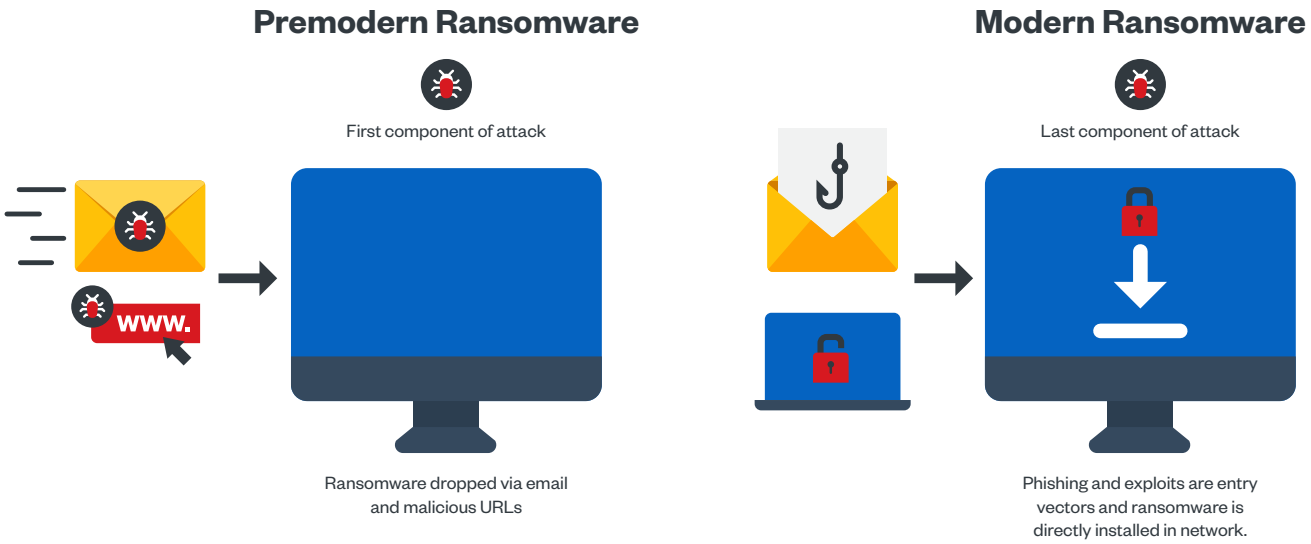

Figure 2. The differences in modern and premodern ransomware

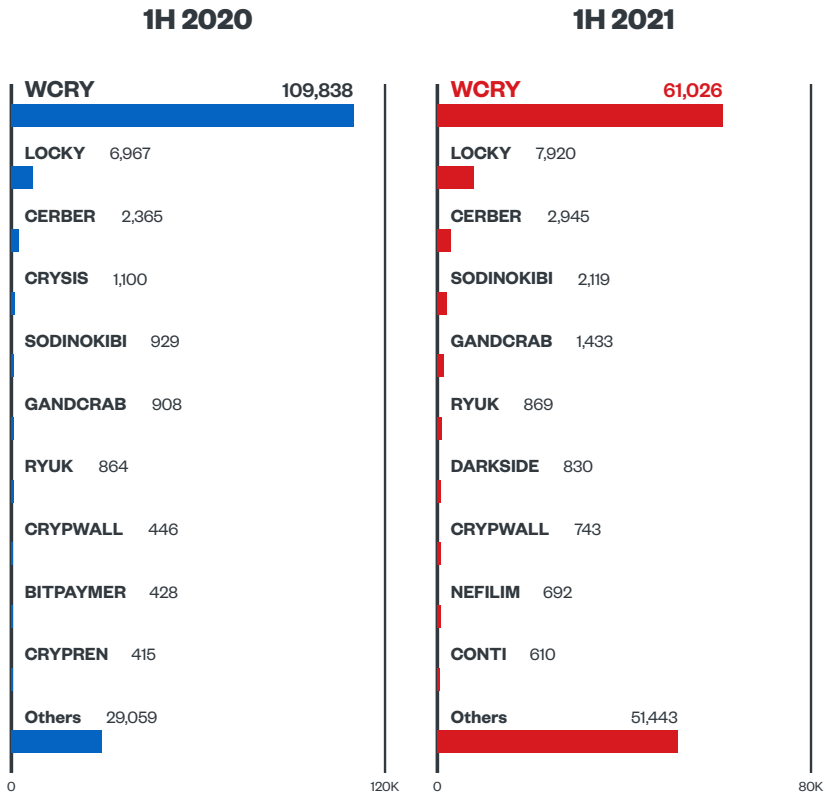

Figure 3. File-only count of ransomware family detections in the first half of 2020 compared to the first half of 2021

Source: Trend Micro™ Smart Protection Network™ infrastructure

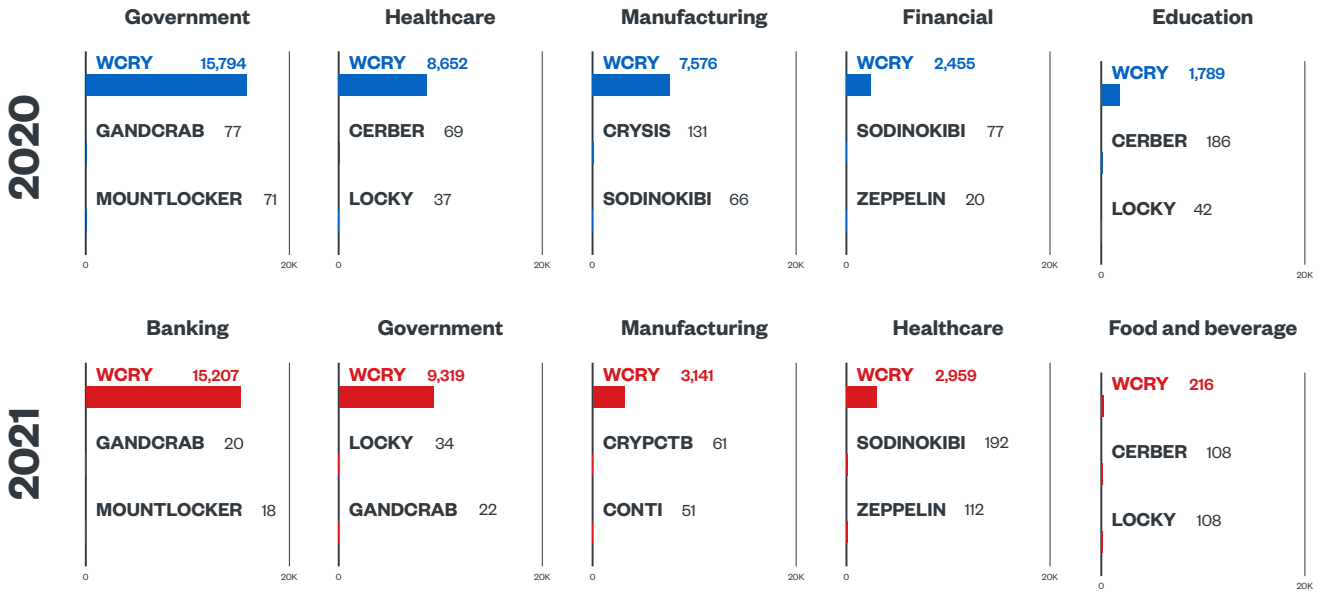

Figure 4. The top three malware families that affected the top five industries in the first half of 2020 and the first half of 2021

The Nefilim ransomware continued to target companies with billion-dollar yearly revenues, a tactic that we analyzed as the model for modern ransomware.[5] In May, the DarkSide[6] ransomware shut down Colonial Pipeline, a company responsible for providing fuel to nearly half the US East Coast. As a result, the Federal Motor Carrier Safety Administration (FMCSA) had to declare a state of emergency in 18 states to help with the shortages. The incident was so considerable that it spawned a group that posed[7] as DarkSide and sent extortionist emails to companies' generic email addresses. There was also DarkSide Linux,[8] another version of the ransomware that targets files related to virtual machines (VMs) on VMware ESXI servers. It kills VMs, encrypts files on the infected machine, collects system information, and sends it to a remote server. Meanwhile, Conti[9] is known as the successor to the popular Ryuk ransomware family, with its threat actors victimizing targets using the same methods used with Ryuk. In fact, Trickbot, Emotet, and BazarLoader are now used to distribute Conti.

In the succeeding sections, we discuss these families, as well as other ransomware attacks and developments that were significant in the first half of 2021. The tactics and tools used to conduct these malicious activities show how ransomware has evolved over the years.

How Did Modern Ransomware Spread in the First Half of 2021?

Modern ransomware attackers are now becoming more mature by using APT-level tools and techniques to access and move deeper into the victim's system, exfiltrate data, and then deliver their payloads. In May 2021, we saw that the Microsoft Exchange Server vulnerability called ProxyLogon,[10] discovered in 2020, was used to deliver three types of malware, including the BlackKingdom ransomware. One other example is the aforementioned ransomware Conti,[11] which targeted Ireland's Department of Health in May.[12] Conti has been seen compromising victims through firewall vulnerabilities CVE-2018-13379 and CVE-2018-13374, which are more sophisticated entry points than traditional ransomware. After exploiting the vulnerable firewall, the ransomware tries to move laterally within the system.

REvil or Sodinokibi[13] was yet another modern ransomware that was active throughout 2021, specifically targeting tech company Acer in March, Apple in April, and the world's largest meat processor, JBS, in June.[14] This family also used techniques that indicate a targeted approach. For example, it used the remote code execution (RCE) CVE-2019-2725 vulnerability, and we observed that it was loaded in the memory of PowerShell through reflective-load instead of binary execution. The Hello ransomware,[15] which uses *.hello* as its extension, arrives at a target system via Microsoft SharePoint vulnerability CVE-2019-0604. Our analysis revealed that after the exploit is abused for intrusion, the China Chopper web shell (detected by Trend Micro as Backdoor.ASP.WEBSHELL.SMYAAIAS) is deployed to execute PowerShell commands to facilitate the succeeding malicious actions and ultimately push the payload.

Sophisticated methods of accessing and entering an organization sometimes come from a source outside the group that actually creates or distributes the ransomware. This is where affiliate programs come in. These programs, which flourished in the first half of 2021, are basically collaborations that allow actors to share their tools, such as customizable software, new and readily available technologies for improved victim-targeting, and more. Specifically, we saw many actors with access to compromised assets (such as avenues into a victim's network) collaborate with other actors who hold ransomware. Nevertheless, while this means that certain cybercriminals can take advantage of other groups' tools and resources, there are downsides to this option.

For example, the high-profile DarkSide attacks in May had multiple victims apart from Colonial Pipeline, and it was reported that there were different affiliate groups behind the attacks. This is one of the issues that arise with affiliate programs: The ransomware group does not have oversight into the victims of its partners. For its part, the DarkSide group apologized[16] and said that it will target less controversial organizations in the future, adding that it will start checking companies that its partners want to target and encrypt.

It should be noted that these ransomware also use traditional means to gain initial access into a victim's system: malspam emails with spear-phishing links or attachments, remote desktop protocol (RDP) access that uses valid accounts, compromised websites, and others.

How Was Data Exfiltrated in 2021?

After initial access, lateral movement within a victim's system is a key phase in the modern ransomware process. Groups use this movement either to identify valuable data within the victim organization for exfiltration, or to drop malicious payloads. In the case of most modern ransomware, after gaining initial access, additional tools are downloaded. Nefilim, Conti, and Hello all use Cobalt Strike beacons. They are typically used to establish a remote connection to the environment, tag valuable data, and execute commands. We observed that Sodinokibi uses RDP and PsExec for lateral movement, dropping and executing other components and the ransomware itself. Conti operators also remotely create the scheduled tasks of the payload (which can include Cobalt Strike, KillAV scripts, and Conti) that can be remotely executed using scheduled tasks and batch files.

Predictions

In our security predictions last year, we speculated that there would be an increase in sophisticated attacker groups relying on penetration testing tools. We also predicted that Cobalt Strike, the source code for which was allegedly leaked in the second half of 2020, would be among these tools.

Data exfiltration and extortion tactics differ from the various ransomware families we saw in 2021. Typically, however, the data is used in double extortion schemes — the ransomware actors post the stolen information from non-paying victims on data leak sites as a way of pressuring them further into paying the ransom. These data leak sites are on public file-sharing platforms and sometimes on the clear web. We also noted that the exfiltration tools used by ransomware groups are usually open-source, free public resources.

For example, we found that Conti operators use the cloud storage synchronization tool Rclone to upload files to the Mega cloud storage service. Similarly, DarkSide operators use Mega client for exfiltrating files to cloud storage, 7-Zip for archiving, and PuTTY application for network file transfers.

After data is exfiltrated, the payload is dropped. Many modern ransomware actors take over networks in multiple human-supervised stages, unlike with traditional attacks that use click-on-the-link automatic events. They spend weeks or even months conquering different parts of the victim's network before they execute the ransomware payload. This is another feature that makes modern ransomware attacks seem like nation-state APT attacks. One example of this is the Nefilim[17] ransomware, which stays silently working in the victim's network for weeks to fully exfiltrate the data before executing the ransomware payload.

How Were Legitimate Tools Misused by Ransomware Gangs?

We mentioned previously that ransomware distributors sometimes use legitimate tools to perform malicious activities, but the scope of misuse is worth exploring further. On their own, most of the tools exploited by ransomware are used to help in security research or to improve efficiency. Many of them are open-source and can be used and modified by the public freely. Conversely, the features that make them good tools also make them useful for cybercriminals.[18]

Tool	Intended use	How it is used for ransomware campaigns	Ransomware campaigns that used this tool
Cobalt Strike	Threat emulation	Lateral movement, backdoor Has many other capabilities as a remote access trojan (RAT)	Clop, Conti, DoppelPaymer, Egregor, Hello (WickrMe), Nefilim, NetWalker, ProLock, RansomExx, Ryuk
PsExec	Executing processes on other systems	Arbitrary command shell execution, lateral movement	DoppelPaymer, Nefilim, NetWalker, Maze, Petya, ProLock, Ryuk, Sodinokibi
Mimikatz	Proof-of-concept code for demonstrating vulnerabilities	Credential dumping	DoppelPaymer, Nefilim, NetWalker, Maze, ProLock, RansomExx, Sodinokibi

Tool	Intended use	How it is used for ransomware campaigns	Ransomware campaigns that used this tool
Process Hacker	Monitoring system resources, debug software, and detect malware	Process/service discovery and termination (including antimalware solutions)	Crysis, Nefilim, Sodinokibi
AdFind	Active Directory (AD) search utility	AD discovery (can be a prerequisite for lateral movement)	Nefilim, NetWalker, ProLock, Sodinokibi
MegaSync	Cloud-based synchronization	Data exfiltration	Hades, LockBit, Nefilim

Table 1. Six commonly weaponized legitimate tools

Some ransomware groups use multiple tools at once in various stages of their attack. For example, Nefilim uses AdFind, Cobalt Strike, Mimikatz, Process Hacker, PsExec, and MegaSync. Primarily, ransomware operators opt for these tools for evasion. Since these tools are recognized as legitimate, they might be able to conduct malicious activity while remaining undetected by simple security software. Additionally, since they are open-source, criminals can alter their code to tweak certain parts that trigger antimalware software.

Enterprise and Government Response to Ransomware Attacks

Colonial Pipeline reportedly paid US$4.4 million in ransom to the DarkSide actors. Fortunately, in June, the US Department of Justice announced that it recovered 63.7 bitcoins[19] of the payment given. Law enforcement agencies were able to track multiple transfers of bitcoin to a specific address. However, the full ransom amount was not recovered, and the ransomware group walked away with more than half of the payment.

It seems that Colonial Pipeline was prepared for such an incident, since the company had cyber insurance with Lloyd's of London and Beazley,[20] which covered it for at least US$15 million. However, it was unclear if the company used its policy to pay. This is not an unusual scenario: In the past two years, we've seen companies involved in ransomware attacks utilize cyber insurance to deal with the ransom payments. In 2019, Norsk Hydro received US$20.2 million[21] in cyber insurance from provider AIG. In a report on cyber insurance claims made in the first half of 2021, insurance company Coalition details[22] that 41% of reported claims were made as a result of ransomware attacks. Coalition also reports that ransomware attacks are growing more severe, with the ransom demands affecting policy holders increasing 47% from the first to the second quarter of 2020.

Cyber insurance is supposed to protect enterprises from the fallout of cyberattacks; however, critics of this system argue that insurance encourages ransomware victims to simply pay the ransom and collect insurance rather than invest in security to deter hackers.

On the administrative side, the US Department of the Treasury added multiple crimeware gangs to its sanctions program.[23] This means that US entities and citizens are prohibited from conducting any sort of business with any of these gangs, including paying them ransom. The Treasury Department's Office of Foreign Assets Control (OFAC) issued advisories[24] reiterating sanctions risks associated with ransomware payments and highlighted that companies facilitating ransomware payments on behalf of a victim might violate OFAC regulations.

Legislation is also being proposed to create special funds for government ransomware payments. In New York, under proposed bill S7246,[25] state and local taxpayer funds would no longer be used to pay ransoms for ransomware attacks. Instead, a cybersecurity enhancement fund would be created to distribute grants and upgrade the cybersecurity of areas with populations of a million or less.

Although organizations hit with ransomware are tempted to simply pay the ransom to recover their data, security and government agencies are generally opposed to this idea for a couple of reasons. Firstly, there is no guarantee that the data will or can be returned by ransomware operators, and the data, even if returned, might also be corrupted. Secondly, the money will be used by these criminal gangs for further malicious activities. There has also been a historical precedent of ransomware distributors attacking paying victims again. A 2020 security report from Cybereason shows that 80%[26] of organizations that paid ransom demands experienced a second attack. Indeed, ransomware distributors could be marking their paying victims as susceptible targets that they can come back to for more ill-gained profits.

Ransomware Arrests: Egregor, Clop, Emotet

In the first few months of 2021, law enforcement agencies across the world successfully dismantled long-running cybercriminal operations and arrested key players in malicious hacking groups.

In early 2021, law enforcement teams from Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine coordinated in international activities by Europol and Eurojust and disrupted one of the most significant and long-running botnets of the past decade, Emotet,[27] dubbed by some outlets as the world's most dangerous malware.[28] Trend Micro was actually the first security service to discover and profile Emotet in 2014. Emotet evolved from spreading banking trojans to selling malware loader services and has victimized over 1.6 million machines.[29] Notably, though Emotet is not ransomware, it served as a major enabler of ransomware distribution. For example, in 2019, Emotet was used in a two-layered attack[30] where it dropped the Trickbot trojan that in turn stole information and then

loaded the Ryuk ransomware. The danger in Emotet is its resilience and evasion capabilities: It is able to spread threats laterally on victims' networks despite only having access to a few devices. Luckily, in January of this year, law enforcement teams conducted "Operation Ladybird" and took over its command-and-control (C&C) infrastructure and arrested key members of the group.

In March, a joint operation between French and Ukrainian police saw the arrest of several members of the Egregor ransomware cartel in Ukraine. The group began operations in September 2020 and operated on a RaaS business model. They also depended on other cybercriminal groups to orchestrate intrusions into victim's networks and deploy ransomware. Victims of this gang were often listed on the Egregor leak site to shame them into paying the ransom. News reports say that the arrests have made an impact on the Egregor infrastructure, contributing to the shutdown of both C&C servers and the leak site.

In June, members of the Clop ransomware gang were also arrested in Ukraine through the efforts of an international group. Like Egregor, Clop operates a leak site where, oddly enough, there has been activity even after the arrests. Aside from ransomware, the gang was also involved in money-laundering activities.

APTs Find Exploitable Cracks in Online Portals and Webmail Servers

APTs are stealthy campaigns that target specific groups and use advanced methods and malware to infiltrate and persist in their victims' systems. The goals differ for each operation, from stealing financial information and loading cryptocurrency miners to taking valuable data. In the first half of 2021, APT groups continued to broaden target bases and update their toolkits, focusing on stealthy infiltration techniques and finding new ways to abuse legitimate tools and systems to conduct malicious actions.

They also continued to search for and exploit vulnerabilities in widely used enterprise tools like Kubernetes, AWS cloud servers, and popular email platforms. Meanwhile, spear phishing remains a prevalent and successful way into a victim's system, despite the fact that attackers have also been using other accessible entry points like online e-commerce order forms.

TeamTNT

The cybercrime group TeamTNT has a reputation for being resourceful, with its loaded arsenal of hacking tools and capabilities. In 2020, the group attacked exposed Docker APIs with an XMRig cryptocurrency miner and created and distributed its own IRC (Internet Relay Chat) called TNTbotinger.

In March 2021, we found that the group was targeting AWS credentials.[31] Upon looking into the server that the group used as a repository for their stolen data, we also found Linux cryptocurrency-mining tools that they push onto compromised systems. Later in May, we also saw TeamTNT compromising Kubernetes[32] clusters in the wild and using them to mine cryptocurrency as well. We elaborate further on TeamTNT activities in our section on threats to the cloud.

Water Pamola

Water Pamola is a threat that we have been tracking since 2019. The campaign used spam emails with malicious attachments on e-commerce shops in Japan, Australia, and European countries. However, our telemetry shows that since early 2020, Water Pamola started focusing mainly on Japan. We also noted that these newer attacks are not launched via spam. Instead, malicious scripts are executed when the administrators look into customer orders on their online shop's administration panel.

Further investigations revealed that companies were fielding strange orders on their online portals. JavaScript code had been inserted into the "customer address" or "company name" fields on the order forms. The script is likely activated by exploiting a cross-site scripting (XSS) vulnerability in a shop's administration portal, and then connects to Water Pamola's server to download additional payloads.

Water Pamola has likely launched this embedded XSS script operation on many targeted online shops. If a store administrator opens the malicious order on their management panel and their site is vulnerable, the XSS attack will be loaded. One site victimized by Water Pamola disclosed a data breach and reported that customer names, credit card numbers, card expiration dates, and credit card security codes were potentially leaked. This might indicate that the overall goal of this group is financial and that they are after credit card data.

Predictions

In our previous security predictions for 2021, we anticipated that organized crime would target the logistics behind e-commerce, an industry that underwent reinforced growth during the pandemic. As a result of consumers' increased reliance on online shopping amid lockdowns around the world, we thought it likely that cybercriminals would opt for activities like sabotaging production, transporting fake goods, and trafficking.

Earth Wendigo

Trend Micro discovered an APT campaign that has been going on since May 2019. It targets government organizations, research institutions, and universities in Taiwan. Investigations reveal that the group aims to exfiltrate emails from targeted organizations by injecting JavaScript backdoors onto a webmail system that is widely used in Taiwan. The malicious script also appends itself to the victim's email signature to propagate to other contacts. Since there is no clear connection to any previous attack group, we dubbed this threat actor as Earth Wendigo.[33]

In this attack, a victim will receive a spear-phishing email with an obfuscated malicious JavaScript embedded, which will load malicious scripts from Earth Wendigo's remote server. To evade security checks, the email uses the webmail system's search suggestion function to trigger the webpage to execute the malicious script instead of directly running it.

The scripts are designed to perform malicious behaviors, including:

- Stealing browser cookies and webmail session keys and sending them to the remote server.
- Appending their malicious script to the victim's email signature to propagate the infection to the victim's contacts.
- Exploiting a webmail system's XSS vulnerability to allow their malicious JavaScript to be injected on the webmail page permanently.
- Registering a malicious JavaScript code to Service Worker, a web browser feature that allows JavaScript to intercept and manipulate HTTPS requests between client and server. The registered Service Worker script can also hijack login credentials and modify the webmail page to add malicious scripts in case the attackers are unable to inject the XSS vulnerability mentioned previously. It should be noted that this is the first time that we found an attack at large that leverages Service Worker.

At the end of the attack, Earth Wendigo delivers a JavaScript code that creates a WebSocket connection to a remote server and executes the script returned from the server. The WebSocket server instructs the backdoor on the victim's browser to read emails from the webmail server and send the content and attachments to the WebSocket server.

In a separate move from this attack, the threat actor sent malicious emails to other individuals, including politicians and activists who support movements in Tibet, the Uyghur region, and Hong Kong.

Earth Vetala

Early in 2021, Earth Vetala – MuddyWater[34] threat actors launched a campaign against organizations in the United Arab Emirates (UAE), Saudi Arabia, Israel, and Azerbaijan. The sectors that they targeted include government agencies, academia, and tourism.

The attackers used legitimate remote administration tools (RATs) to distribute their malicious payloads, specifically, the applications ScreenConnect and RemoteUtilities. These tools have broad capabilities such as file and directory browsing, downloading, and uploading files, executing and terminating processes, grabbing screenshots, and others. Earth Vetala created spear-phishing emails with embedded links to a legitimate file-sharing service to distribute archives containing these RATs. After successfully accessing the victim, attackers download post-exploitation tools to dump passwords, tunnel their C&C communication using open-source tools, and use additional C&C infrastructure to establish a persistent presence within targeted hosts and environments.

Iron Tiger

Iron Tiger is an APT threat that has historically targeted gambling and betting companies in Southeast Asia. A recent incident response investigation involving a Philippine-based gambling company prompted a closer look at the group, and over 18 months we found that they expanded their operations and were targeting governments, banks, telecommunication providers, and even the energy sector in the Middle East and Southeast Asia.

The group has also updated their toolkit with a SysUpdate malware variant that now uses five files in its infection routine instead of three.[35] The group also uses updated rootkits. One of these rootkits is used to hide files at the kernel level and has not previously been associated with this threat actor.

The SysUpdate malware was typically loaded in memory by a known method involving three files. In our recent analysis of Iron Tiger tools, we found five tools that the group now uses:

- *dlpumgr32.exe*, a legitimate signed file that belongs to the DESlock+ product
- *DLPPREM32.DLL*, a malicious DLL that is sideloaded by *dlpumgr32.exe* and that loads and decodes *DLPPREM32.bin*
- *DLPPREM32.bin*, a shellcode that decompresses and loads a launcher in memory
- *data.res*, an encrypted file that is decoded by the launcher and contains two SysUpdate versions: one for a 32-bit architecture and another for a 64-bit architecture
- *config.res*, an encrypted file that is decoded by the launcher and contains the SysUpdate configuration, including the C&C address

In summary, the launcher acts as an installer: It will copy the malware to a fixed place and ensure that it runs during the next boot of the infected host.

The Iron Tiger threat actors have updated their tools, changed their tactics, techniques, and procedures, and expanded their target base. Different active campaigns with versions of the same tools being used concurrently suggest that there might be either subgroups for this threat actor or multiple groups with access to the builders of these tools.

PlugX

Trend Micro's Apex One with Endpoint Sensor (iES) recently discovered an attacker attempting to exfiltrate sensitive information from a company with PlugX loader,[36] a remote access tool (RAT) used in attacks targeting government organizations and related industries.

Initial analysis of this PlugX variant showed that it has three parts: a normal file, a DLL loader that the normal file expects to be present, and an encrypted Binary Large Object (BLOB) file containing the malicious code.

The normal file loads a seemingly ordinary DLL named after a common Microsoft DLL. However, the hash of the DLL does not match any of the known hashes of a normal DLL. After reversing the file, we found that it was actually PlugX. We observed the process and found that PlugX decrypts, loads, and executes a DLL file (one named after another Microsoft DLL file) that is actually an encrypted BLOB.

Our investigation shows that the attacker also used other tools during the attack. The simplest way to launch these tools is to have the injected code in svchost download, drop, and execute the tools. We noted that the attacker had a unique way of launching their malicious tools: They made use of a scheduled task that runs the batch file which, in turn, executes the tool.

Evasion techniques like this, in the larger picture of the security landscape, reify the urgency of relying on security solutions that can flag anomalous events, correlate them, and associate them with known techniques that attackers previously used. With these solutions, companies can look forward to a more comprehensive view of threats to their systems.

A Look at Upgraded Criminal Campaigns and Unexplored Flaws in Unsecured Technology

Active Threats

Aside from ransomware and APT threats, the first half of 2021 also saw other criminal operations updating their tools and trying new techniques. In particular, we saw malware campaigns targeting vulnerabilities in Mac operating systems and web browsers, as well as spam emails spreading an information stealer. Cryptocurrency accounts were also a popular target, as we saw multiple malicious actors trying to collect trading account information and cryptocurrency wallet details.

XCESSET

XCSSET is a Mac malware that victimizes users by infecting Xcode projects. Although it was initially reported as a malware family, it is now classified as an ongoing campaign in light of our recent findings.

In the first half of 2021, XCSSET quickly trailed Apple as the company moved from Intel to processors that use the ARM64 architecture. It adapted to both ARM64 and x86_x64 Macs and also changed its payload. Previously, XCSSET exploited two macOS vulnerabilities, while a third exploit was found taking advantage of browsers in the operating system to implant a universal cross-site scripting (UXSS) injection. However, new samples that can run on Macs with the new M1 chip have been discovered, and these affect macOS 11 (Big Sur) as well.

The malware works by using the development version of Safari to load malicious Safari frameworks and related JavaScript backdoors from its C&C server. It hosts Safari update packages on the C&C server, then downloads and installs packages for the target's version of the operating system. To adapt to the newly released Big Sur, new packages for Safari 14 were added. Fake apps for Big Sur were also created, with modified icons that are convincingly similar to the legitimate app.

XCSSET has also been updated to steal confidential data from various websites, two of which are cryptocurrency platforms:

- 163.com
- huobi.com
- binance.com
- nncall.net
- envato.com
- login.live.com

For cryptocurrency-trading platform Huobi, the malware is not only capable of stealing account information but also of replacing the address in a user's cryptocurrency wallet, a new feature that did not exist in the previous version.

PandaStealer

In April, we found a new information stealer called Panda Stealer (a modified fork of Collector Stealer) being delivered mainly to targets in the United States, Australia, Japan, and Germany. Panda Stealer is deployed using spam emails requesting business quotes; this pushes victims to open the malicious Excel file attachments. We identified two infection chains in this case: One was an XLSM attachment containing macros that download a loader, which is responsible for downloading and executing the main stealer. The other infection chain has an XLS file containing an Excel formula that utilizes a PowerShell command to access a Pastebin alternative, paste.ee, which in turn accesses a second encrypted PowerShell command. Panda Stealer also utilizes a fileless approach in its distribution to evade detection.

Once installed, Panda Stealer can collect details like private keys and records of past transactions from its victim's various digital currency wallets, including Dash, Bytecoin, Litecoin, and Ethereum. Not only does it target cryptocurrency wallets, it also steals credentials from other applications such as NordVPN, Telegram, Discord, and Steam. It is also capable of taking screenshots of the infected computer and exfiltrating data from browsers like cookies, passwords, and cards.

Covid-19-Related Scams and Fake Products

We observed that in the first half of 2021, many users were inundated with scams that revolved around the response to Covid-19 or the effects of the pandemic. For example, we found that cybercriminals used text messages to lure people into sharing their personal information.[37] As further proof of cybercriminals' relentless tendency to exploit any situation, they also lured victims with promises of the vaccine or offers of a stimulus package for unemployed or struggling individuals.

Most of these criminal activities consisted of phishing and social-engineering plots that tried to take advantage of the constant flux of information on government pandemic response and news about regulations and lockdowns, as evidenced by the many threats that led to websites dedicated to Covid-19-focused scams and misinformation. On the other hand, some threats led to malicious mobile applications for vaccine registration or to medical response sites. Malicious apps masquerading as Covid-19 testing registrations include "V-Alert COVID-19" (detected by Trend Micro as AndroidOS_Cerberus.HRXC) and "Covid-19 Test" (detected by Trend Micro as Android OS_Anubis.GCL). Both of these apps were spotted spreading the banking malware Anubis and Cerberus.

Predictions

As part of our security predictions for 2021, we foresaw that threat actors would exploit misinformation to lure users into selecting links or downloading attachments. Considering the anticipation last year around vaccine development, we predicted that cybercriminals would resort to using the Covid-19 vaccine as a phishing lure. We also anticipated that they would turn to emails, fake apps, malicious domains, and even social media to purportedly offer health information, fake vaccines, and spots on inoculation waitlists.

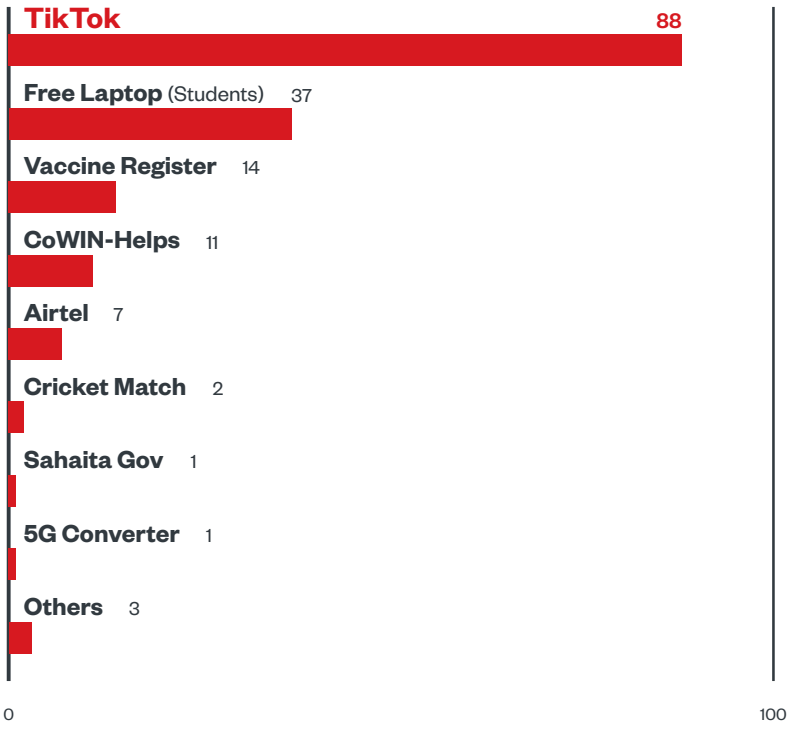

Figure 5. Breakdown of malicious apps associated with Covid-19. All fake applications here are detected by Trend Micro as AndroidOS_FakeApp.NGPF.

Subsequently, some scammers used social media websites and messaging platforms like Telegram to provide fake vaccination cards to individuals who were interested in misrepresenting their vaccination status to bypass regulations and guidelines imposed by authorities. In response, government organizations have been asking vaccinated individuals to refrain from posting pictures of their inoculation cards on social media to avoid forgeries. In a more worrying move, some sellers pushed fake vaccines on e-commerce sites. It is crucial to note that the forgery of vaccination cards, not to mention the sale of counterfeit vaccines, shows not only the willingness of some individuals to flout health guidelines but also the possibility of a prolonged pandemic and increased lockdowns.

We also saw phishing schemes targeting organizations involved in providing vaccinations, from manufacturers and logistics companies to enterprise customers.[38] We tracked malicious files, emails, and pages stealing sensitive information. The targets involved belonged to the telecommunications, banking, retail, government, and finance sectors, and were likely chosen because of their involvement in vaccination operations.

Our data on overall threats related to Covid-19 shows that there was a 50% decrease from the first half of 2020 to the first half of 2021. There are many possible factors that could have contributed to this decline, such as heightened security from both enterprises and users, improved detection and blocking from online applications and software vectors, and even a decline in cybercriminal interest in using Covid-19 as a topic for lures. We also noted that threats using this topic were found mostly in the US and Germany. Ultimately, despite the decline, scams that revolve around the pandemic and the vaccine cold chain call for sustained vigilance, as they can lead not only to the collection of private information but also to the endangerment of lives as the world continues to grapple with Covid-19.

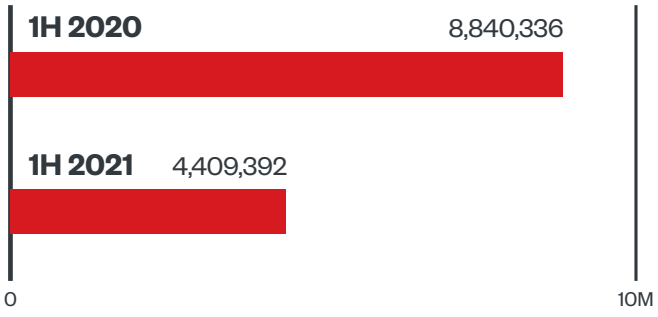

Figure 6. Comparison of Covid-19-related email threats, URLs, and malware in the first half of 2020 and the first half of 2021

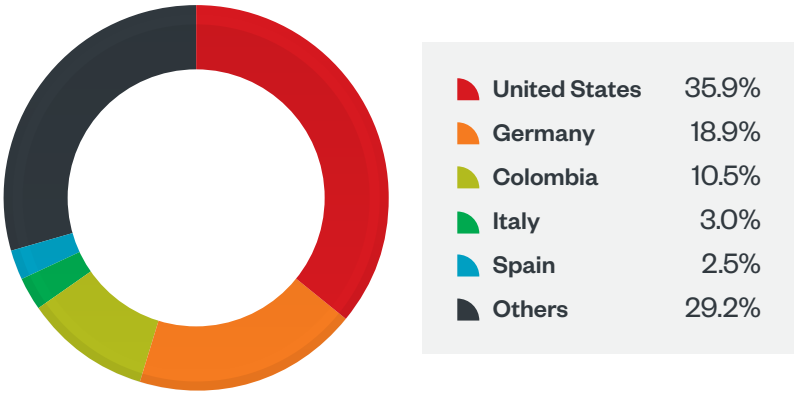

Figure 7. The top countries affected by Covid-19-related threats in the first half of 2021

Unexplored Risks and Unpatched Flaws

Apart from active malware and criminal campaigns in the first half of 2021, we also found unknown vulnerabilities that were not being exploited but still pose risks to users. It is worth emphasizing that inherent and unintended flaws can sometimes arise when security is not integrated in the development of applications and hardware. New and emerging technology also poses a risk to adopters who might not know the correct security framework that they need to apply when integrating this technology into their environments.

SHAREit flaw

We discovered several vulnerabilities in the file-sharing and gaming platform SHAREit,[39] which had previously been named as one of the most downloaded applications of 2019 and which has over 1 billion downloads in Google Play. The app markets itself as a peer-to-peer file-sharing network where users can access videos and download games.

After analyzing the app and inspecting the vulnerabilities, we first noted that the download URLs are not only from Google Play but also from other vendors. Most of the URLs use the HTTP protocol, which makes them vulnerable to tampering by a man-in-the-middle (MitM) attacker. The vulnerabilities can also be abused to leak a user's sensitive data and execute arbitrary code. They can also potentially lead to RCE. The app allows and promotes the transfer and download of various file types, such as Android Package (APK), but the vulnerabilities related to these features are most likely unintended flaws. It should be noted that since publishing our report, SHAREit has fixed these vulnerabilities.

LoRaWAN

LoRaWAN technology and devices are used in IoT systems deployed in enterprises and smart cities across the world. This technology can be scattered across large areas and wirelessly connects to the internet via radio waves. It can also be used in monitoring sensors (either for weather sensors or tracking sensors), asset management, controlled automation, climate control, and more.

New research from Trend Micro brings forward certain exploitable vulnerabilities within these devices and classifies them as low powered but high risk.[40] Our research shows that they are susceptible to denial-of-service (DoS) attacks, ACK spoofing, and bit flipping. We also learned that LoRaWaN is subject to many bugs and vulnerabilities, most of which are memory corruptions. In order to highlight the insecurities in the LoRaWAN communication environment, we created a tool that we call LoRaPWN.[41]

The fact that LoRaWAN devices are often left exposed in remote areas also leaves them vulnerable to hardware attacks like data scraping, accessing external memory, or abusing open interfaces.[42] Sensors across city blocks and weather nodes in agricultural fields are examples of vulnerable LoRaWAN devices in remote areas.

Lastly, compromised LoRaWAN devices can be used in attacks that could result in stalled operations, leaked data, or falsified information. Since these devices are used in infrastructure and smart city projects, an attack on these could cause physical consequences; for example, compromising a highway-monitoring sensor could affect motorists by causing an accident or a traffic jam.

5G Campus Networks

In our new research into campus networks,[43] we looked into risks involved in the development of a 4G/5G campus network for IT and operational technology (OT) experts who are tasked with running and maintaining factories, critical infrastructures, and other such environments. We also tested attack scenarios that were rooted from a compromised campus network and the core network within it.

For attacks conducted at the IP network, threat actors would first need to gain control over a core network's potential entry points. In our research, we identified these entry points as the server hosting network services, the VM or the containers, the network infrastructure, and the base stations. We highlighted several attacks that show how a compromised core network can also be an opening for threats that already affect industrial control systems (ICSs), such as DNS hijacking, MQTT hijacking, Modbus/TCP hijacking, downloading or resetting unprotected programmable logic controllers (PLCs), remote desktop, and SIM swapping.

Our research also led us to find cellular network-specific attacks. These attacks emphasize how relying on Access Point Name (APN), which is used for identifying the gateway between the network of a mobile device and another network, is not tantamount to having encryption. For better security when on a public network, a company should rely on its own VPN in an industrial router, rather than depend solely on its telecom provider. The use of HTTPS, MQTTS, and S7Comm-Plus, which are all secure protocols, is also recommended.

Given the number and severity of the risks involved, organizations must adapt if they are considering updating their infrastructure to include a 5G core network. Based on our research, organizations will need to consider a new trio of IT, OT, and communications technology (CT) to create a better security framework.

VPNFilter

Cybercriminals continuously target low-hanging fruit, specifically common and unsecured IoT devices such as routers, printers, and network-attached storage (NAS) devices. These devices are easy targets for many reasons: Users are less likely to patch IoT devices, operating systems have no auto-update features, and manufacturers rarely issue security updates.

In the beginning of 2021, we investigated router infections and found that one of the biggest reported malware families affecting these devices was VPNFilter,[44] an IoT botnet that was discovered in 2018 and that was active in the same year. The malware is known to compromise routers and storage devices by using backdoor accounts and exploits of several known vendors. VPNFilter operates in three stages: initial infection, C&C communications, and payload deployment.

Since it is an older threat, several mitigation tactics have already been used to essentially defang VPNFilter. In 2018, the US Department of Justice sinkholed the C&C domain (a move that involves redirecting traffic from its original destination), compelling the site Photobucket to remove user profile URLs that were being used to link to malware components.

To gather more details about the botnet, we recently partnered with the Shadowserver Foundation, a nonprofit security organization. According to Shadowserver's data, the initial spike of over 14,000 infected networks in 2018 had been reduced to 5,447. Still, it is likely that these infections will continue to be present until these devices are physically swapped out — a common trend in IoT botnets. Indeed, IoT botnets are to some degree nearly "uncleanable," and a botnet like this might be taken over by another threat actor for them to use.

We were able to inject an IP address that points back to the sinkhole owned by Shadowserver in order to check on the infected devices that are still actively looking for the download server used in the second stage of the malware operation, and more importantly, to prevent the still-infected networks from moving to the VPNFilter's next stage in the future. Unfortunately, for threats that affect routers, security solutions and remedies are not that easy. Firmware updates are encouraged, but verifying updates and applying them are not as simple as compared with doing so in PC ecosystems. It should also be noted that some users don't have access to their routers to perform upgrades because their vendor or internet service provider (ISP) provider might be responsible for setting up and updating the machine.

Widely Used and Vulnerable Technology Actively Attacked Through Critical Flaws

In March 2021, Microsoft had to manage the mass exploitation of four zero-day vulnerabilities[45] on the on-premises versions of Microsoft Exchange Server, reportedly done by Chinese hacking group Hafnium. The company released an advisory on the vulnerabilities, but in the days immediately succeeding the attack, Trend Micro reported that at least 30,000 organizations might have been attacked in the US, and 63,000 servers remained vulnerable.[46]

These vulnerabilities have collectively been dubbed ProxyLogon. Since its discovery and report, it has been exploited by threat actors to distribute the Prometei botnet, the LemonDuck coinminer, as well as ransomware families like DearCry and BlackKingdom. Vulnerable servers were easy targets since majority of Outlook Web App portals are public and indexed by search engines like Google Search, Shodan, BinaryEdge, Censys, ZoomEye, and others. According to Shodan, on March 4, a day after the patch was released, there were more than 266,000 Exchange Servers that were vulnerable to ProxyLogon.

Print Spooler, a service that runs by default on Windows, also had vulnerabilities that were actively exploited, presenting another challenge to Microsoft. At first, Microsoft addressed one vulnerability, CVE-2021-1675, with a security patch released in June. Afterward, in July, the company released a separate, out-of-band security update for PrintNightmare, this time for CVE-2021-34527, a critical bug that allowed arbitrary code execution with system privileges. However, a proof-of-concept exploit had already been released accidentally online. A successful attacker could install programs, view, change, or delete data, as well as create new accounts with full user rights. Although Microsoft was able to release an advisory for CVE-2021-34527 to fully mitigate the vulnerability, a different bug was reported in mid-July, this time an escalation-of-privilege (EOP) vulnerability revealed by researcher Benjamin Delpy.[47] Assigned as CVE-2021-34481, the vulnerability not only allowed hackers system privileges but also limited access to a network.

2021 might have started off with significant attacks exploiting critical vulnerabilities, but the number of overall reported critical vulnerabilities dipped significantly from 2020. On the other side of the spectrum, numbers for vulnerabilities classified with medium and low severity have risen.

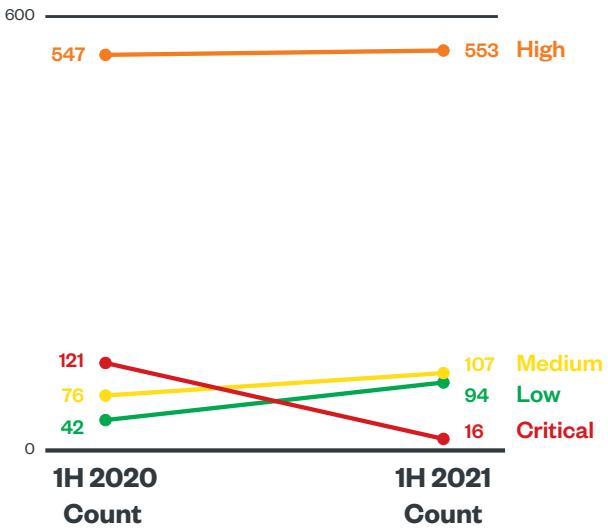

Figure 8. A comparison of the severity breakdown, based on the CVSS, of vulnerabilities in the first half of 2020 and 2021

Source: Trend Micro Zero Day Initiative program

Windows 11

On the Windows front, Microsoft announced plans to release Windows 11 in June 2021, with Windows 10 users getting a free upgrade. There have, however, been concerns about the new system requirements for Windows 11, including the fact that it will only be available on 64-bit processors. In the official announcement,[48] the security of the system is one of the major factors that pushed this decision.

According to the company's statement, "Windows 11 raises the bar for security by requiring hardware that can enable protections like Windows Hello, Device Encryption, virtualization-based security (VBS), hypervisor-protected code integrity (HVCI) and Secure Boot. The combination of these features has been shown to reduce malware by 60% on tested devices."

Our data confirms that malware is a serious concern for Windows users. Table 2 shows that Windows 10, general Windows users, and Windows 7 are most affected by malware. We detected almost 2.5 million instances of malware for Windows 10 users, which further highlights the importance of proper malware protection.

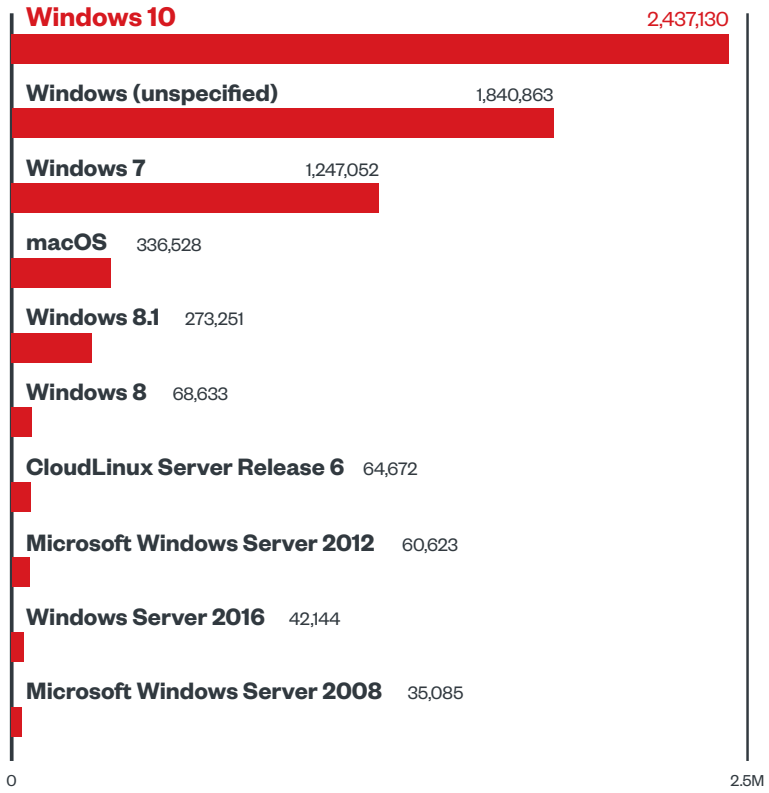

Figure 9. The top 10 operating systems according to malware detection

Microsoft SharePoint has also had several RCE vulnerabilities since the beginning of the year, which is also consistent with the number of RCE vulnerabilities from the first half of 2020.

SharePoint vulnerabilities in 1H 2020 vs. those in 1H 2021				
Microsoft SharePoint	CVE-2021-24066	Workflow Deserialization of Untrusted Data Remote Code Execution Vulnerability	ZDI-21-194	12-Feb-21
Microsoft SharePoint	CVE-2021-27076	InfoPath List Deserialization of Untrusted Data Remote Code Execution Vulnerability	ZDI-21-276	11-Mar-21
Microsoft SharePoint	CVE-2021-31181	WebPart Interpretation Conflict Remote Code Execution Vulnerability	ZDI-21-573	13-May-21
Microsoft SharePoint	CVE-2021-28474	Server-Side Control Interpretation Conflict Remote Code Execution Vulnerability	ZDI-21-574	13-May-21
Microsoft SharePoint	CVE-2021-26420	WorkflowCompilerInternal Exposed Dangerous Function Remote Code Execution Vulnerability	ZDI-21-755	23-Jun-21

SharePoint vulnerabilities in 1H 2020 vs. those in 1H 2021				
Microsoft SharePoint	CVE-2020-0931	Scorecards Deserialization of Untrusted Data Remote Code Execution Vulnerability	ZDI-20-465	15-Apr-20
Microsoft SharePoint	CVE-2020-0932	TypeConverter Deserialization of Untrusted Data Remote Code Execution Vulnerability	ZDI-20-468	15-Apr-20
Microsoft SharePoint	CVE-2020-1102	Shared Forms Incomplete Blacklist Remote Code Execution Vulnerability	ZDI-20-648	12-May-20
Microsoft SharePoint	CVE-2020-1181	Server Web Part Remote Code Execution Vulnerability	ZDI-20-694	9-Jun-20

Table 2. Half-year comparison of SharePoint vulnerabilities

VPN Vulnerabilities

As discussed in our 2020 annual security roundup,[49] virtual private networks (VPNs) have become indispensable for enterprises that are aiming to protect network connections from external threats. Many organizations and ordinary users have adopted VPNs in offices and private homes. Usage spiked in early 2020,[50] and an early 2021 study indicated that 31% of internet users worldwide have used a VPN.[51] However, although a VPN is a security tool, it can also be an entry vector for cyberthreats. In reality, VPNs can host critical vulnerabilities, and attackers can exploit these flaws to compromise targets' systems.

Our data shows the detection numbers of some of the most notable and widespread VPN vulnerabilities in 2020 and the first half of 2021. We found that there was a sudden surge in detections for CVE-2018-13379 in January 2021, and although the numbers dipped in later months, they were markedly higher than the same time last year. CVE-2018-13379 is a vulnerability in the Fortinet VPN product that allows an unauthenticated user to download system files via specially crafted HTTP resource requests.

On the other end of the spectrum, CVE-2019-11510 and CVE-2019-19781 detections numbers significantly lowered. Nevertheless, CVE-2019-11510 had already been used by actual attackers: In 2020, we saw that it was exploited to deliver the Sodinokibi ransomware.

		Fortinet	Pulse Secure			Citrix Systems	
		CVE-2018-13379	CVE-2019-11510		CVE-2019-11539	CVE-2019-19781	
2020	Jan	15,834	88,506	9		856	287
	Feb	9,864	66,164	12		52	19
	Mar	14,910	63,716	115		118	18
	Apr	18,312	62,862	69		2,703	1
	May	20,897	60,791	60		2,921	7
	Jun	27,110	39,994	123		2,783	5
2021	Jan	113,330	45,937	787		1,388	3
	Feb	77,853	15,627	488		579	761
	Mar	75,785	27,876	566	1	713	158
	Apr	68,651	21,440	956		988	5
	May	70,083	15,230	508		650	5
	Jun	61,467	9,558	301	11	418	15

Table 3. A monthly comparison of the detection counts of notable VPN vulnerabilities in the first half of 2020 and the first half of 2021

Source: Trend Micro Digital Vaccine filters

Old Cloud Threats Reemerge to Find New Targets

Data gathered from our container honeypot in the first half of 2021 shows that the tools and techniques used to target the cloud have fluctuated back to what we saw in 2019. As seen in the following graphs, in 2019 the attackers used malicious images with malware or an exploit already inside. In 2020, they moved to using base, valid, and clean images that downloaded malicious samples after deployment. But in 2021, it seems that threat actors are back to developing malicious images with malicious content.

Predictions

Last year, in our security predictions, we foresaw that hackers attempting to take over cloud servers and deploy malicious container images would be a concern for cloud adopters. As for vulnerable images in various architectures, we speculated that these images would target repositories and images as users put their unfettered trust in both container services and depositories.

Upon analyzing the data from our honeypot, we noticed some interesting behavior and found that the entry points of the malicious images are divisible into three categories.

In the first category, we saw that some actors try to lure the administrator by naming the process as a valid service. For example, we saw instances where the process is named NGINX, which is a valid web server. In reality, however, it is a piece of malware that runs under this name. The second category, which usually consists of cryptominers, doesn't even try to hide its malicious purpose; instead, the actors use well-known names of cryptocurrency miners that can be spotted easily. Lastly, in the third category, the entry point is just a script for dropping or downloading the malicious file. This is the technique that is currently most prevalent because several container image repositories now check against malicious content. To circumvent this, the attackers leave a script that is harmless at first look but actually downloads or drops the malicious content only on runtime.

TeamTNT

As we mentioned in our section on APTs, TeamTNT is a group with sophisticated tools and techniques. For example, it created and distributed its IRC bot, TNTbotinger, which is capable of DDoS. In the beginning of 2021, we found that the group was targeting cloud credentials and compromising a platform that facilitates operations for cloud applications.

In March, we investigated TeamTNT's activities and found a binary containing a hard-coded shell script designed to steal AWS credentials.[52] We discovered that after the actor compromises an instance and runs their script, it searches for any credentials deployed via the AWS metadata service. The script creates a file and then uploads it to a remote web server that is set to receive the stolen files. The web server where the malware uploads its data was actually configured (or misconfigured) to be set as open directory, which allowed us access to all the uploaded files. Alongside stolen data, the server was also a repository for Linux cryptocurrency-mining tools that the group deploys on infected systems. We detected over 4,000 infected instances in total.

Furthermore, although the script is meant to run on AWS instances, we found that it ran on any kind of Linux machine, container, and cloud instance. Based on the timestamps in the file names, we can assume that the campaign started on February 10, 2021.

In May 2021, we found that TeamTNT was also compromising Kubernetes[53] clusters that were at large and using them to mine cryptocurrency. Kubernetes is an open-source and widely used system for automating deployment, scaling, and management of containerized applications. We confirmed that close to 50,000 IP addresses were compromised across multiple clusters.

In this attack, TeamTNT installs two free, open-source tools available from GitHub: the network scanning tool Masscan, and the banner-grabbing, deprecated ZGrab. They also install their IRC bot, and used the function kube_pwn() to run the following commands to:

- Update the package index of the container.
- Install the following packages: bash, wget, and curl.
- Download a shell script called setup_xmr.sh from TeamTNT C&C server and save it on the tmp folder.
- Execute the script to start mining for the Monero cryptocurrency.

Several IP addresses were repeatedly exploited during the operation, which occurred between March and May. The identified ISP list, which had China- and US-based providers as the highest list, included some cloud service providers (CSPs). It should be noted that the numbers reflect the likelihood of significantly more clusters in operation for the US and China than in many other countries.

Linux

Apart from the vulnerabilities in the vendors that we listed, we also investigated threats to Linux systems. Although not as widely used as Windows or macOS, many large organizations, such as the National Aeronautics and Space Administration (NASA), the US Department of Defense (DoD), and Google, all use Linux.[54] In the following table, we list the top malware families that we found running on Linux servers from January 1 to June 30, 2021 based on data from Trend Micro™ Deep Security™ and Trend Micro Cloud One™ – Workload Security. In compiling this list, we identified and flagged nearly 15 million events from our sensors.

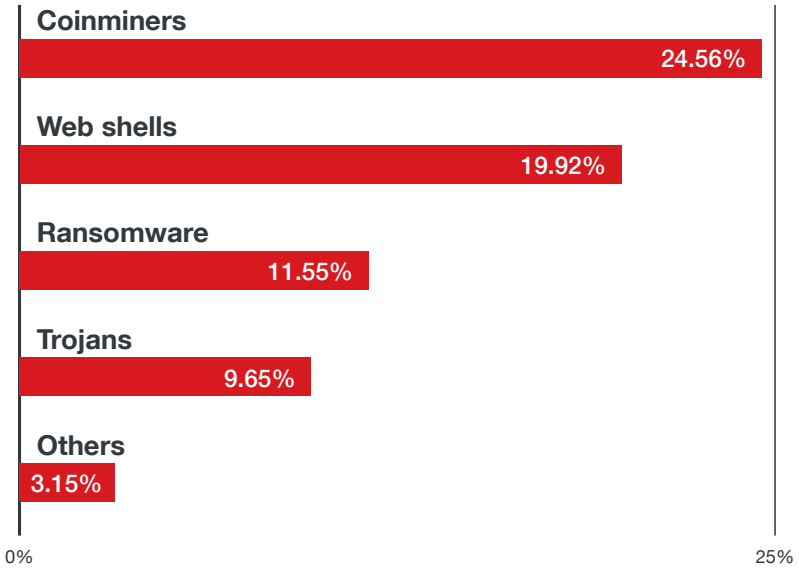

Figure 10. The top five malware families found in Linux systems from January 1 to June 30, 2021

Notably, the malware family in the top spot for Linux servers is a cryptocurrency miner. Considering that the cloud has an abundance of computing power, it makes sense that cybercriminals would steal these resources for their mining activities.

Our SPN data shows the top four Linux distributions where we found malware families:

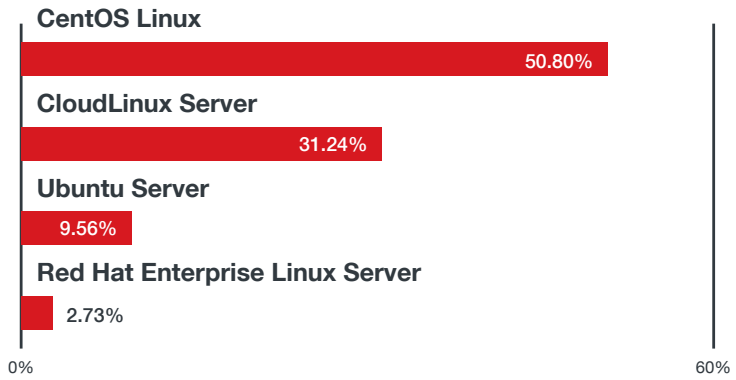

Figure 11. The top four Linux distributions and the top threat types in Linux systems for the first half of 2021

Using data from the first half of 2021 collected from Workload Security, we sorted through triggers that were deployed solely on Linux hosts. As a result, we dissected more than 50 million events, representing the following:

- More than 130,000 unique Linux hosts that reported the events
- The top 20 Linux and Unix flavors that have reported events into this dataset by volume

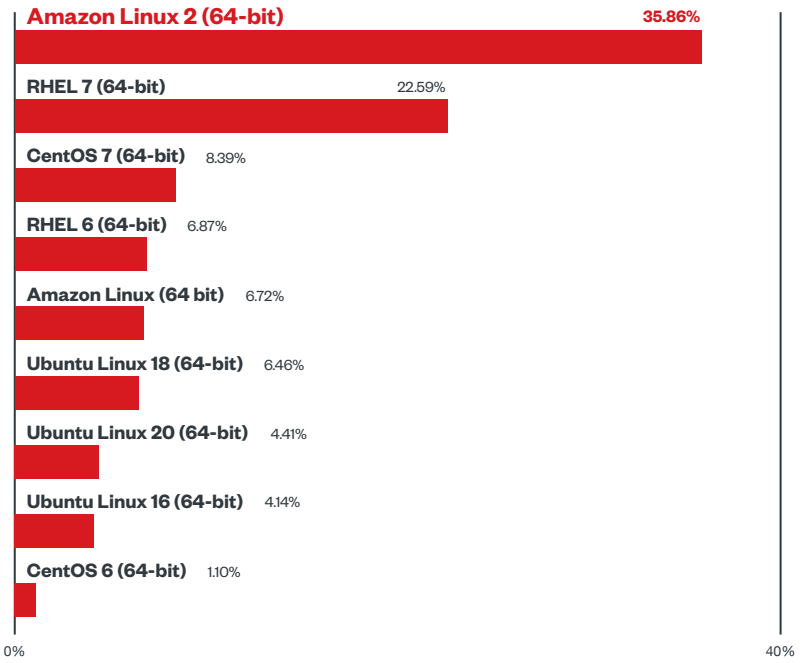

Figure 12. Volume of IPS events sorted by operating system in the first half of 2021

We also looked at data from Trend Micro Cloud One™ and found the top vulnerabilities that are at large and still being actively exploited or have existing proofs of concept.

Top vulnerabilities that have known exploits or proofs of concept	CVE
Apache Struts 2 remote code execution (RCE) vulnerability	CVE-2017-5638
Apache Struts 2 REST plug-in XStream RCE vulnerability	CVE-2017-9805
Drupal Core RCE vulnerability	CVE-2018-7600
Oracle WebLogic server RCE vulnerabilities	CVE-2020-14750
WordPress file manager plug-in RCE vulnerability	CVE-2020-25213
vBulletin 'subwidgetConfig' unauthenticated RCE vulnerability	CVE-2020-17496
SaltStack salt authorization weakness vulnerability	CVE-2020-11651
Apache Struts OGNL expression RCE vulnerability	CVE-2017-12611
Eclipse Jetty chunk length parsing integer overflow vulnerability	CVE-2017-7657
Alibaba Nacos AuthFilter authentication bypass vulnerability	CVE-2021-29441
Atlassian Jira information disclosure vulnerability	CVE-2020-14179
Nginx crafted URI string handling access restriction bypass vulnerability	CVE-2013-4547
Apache Struts 2 RCE vulnerability	CVE-2019-0230
Apache Struts OGNL expression RCE vulnerability	CVE-2018-11776
Liferay portal untrusted deserialization vulnerability	CVE-2020-7961

Table 4. A list of the top 15 vulnerabilities with exploits or proofs of concept

We saw about 200 different vulnerabilities triggered across the board. Applications targeted with these 200 vulnerabilities include popular tools and services like WordPress or Apache Struts, as well as other services like Atlassian Jira DNSmasq, and Alibaba Nacos. The top triggers are spread across the following applications (not in any order):

- Alibaba Nacos
- Apache HTTPd
- Apache Struts
- Apache Tomcat
- Atlassian Jira
- CMS – Drupal and WordPress and their plug-ins.
- DNSmasq
- ISC BIND
- Netty
- NGINX
- OpenSSL
- Oracle WebLogic Server

Attacks From All Angles Require Multifaceted Defenses

Enterprises, organizations, and ordinary users are still finding their footing in the aftermath of the Covid-19 pandemic. In 2020, cybercriminals took advantage of the abrupt move to virtual workspaces, the increase in online tools and applications, and the rise in online financial transactions. Now, in the first half of 2021, we see that threat actors are still taking advantage of any and every open avenue, whether Covid-19-related or not, and constantly searching for cracks in security to drop malicious payloads on their victims.

Old threats like ransomware are adopting more targeted and sophisticated techniques, and successful real-life attacks have proven that these modern tactics are quite effective. APT groups are working every angle, from complex exploits to simple spam mail. Our data on threats to operating systems, VPNs, IoT devices, and other technology shows that the threat landscape is varied, evolving, and persistent. Considering the different types of malicious threats and the number of active cybercriminal groups, it is vital that organizations establish a robust and multilayered security system. Now more than ever, siloed tools and single layers of protection that only cover parts of the overall infrastructure are not a sufficient defense against the advanced cybercriminal campaigns being launched.

Instead, organizations have to deploy solutions that can assess, protect, detect, respond to, and recover across multiple platforms, including emails, endpoints, servers, networks, and cloud workloads. These optimal security solutions should also provide indicators and analytics that give IT security teams a comprehensive view of risks to their organization's system without inundating them with mountains of alerts and unnecessary data.

As always, ordinary users, especially employees, are critical parts of the security posture, as they are often used to gain deeper access into organizations. As such, they should be educated on current social engineering tactics, as staying informed and alert on the latest threats will help close that entry point for attackers.

As a non-negotiable practice, patching should be prioritized by organizations, especially since many are still working remotely and using personal machines, and vulnerabilities in these endpoints could lead to more serious breaches into corporate systems. Organizations should also prioritize critical system updates and, if possible, find a way to deliver these updates to users remotely. Virtual patching is a convenient option to help businesses protect their systems and end-user machines, as well as to minimize downtime while waiting for vendors to roll out official patches.

In the first half of 2021, threats closed in from all angles for enterprises and everyday users, emphasizing the insatiable nature of cybercrime. With malicious actors relying on evolved techniques, exploiting legitimate tools, and going as far as targeting the vaccination process against Covid-19, the need for a multilayered defense strategy that can meet threats from all angles must be reified. In line with the global attempt to recover from the ongoing health crisis, enterprises must consider all facets of their security posture, not just to survive in the new work setup brought on by the pandemic but also to thrive beyond it.

The Threat Landscape in Review

In the first half of 2021, the Trend Micro™ Smart Protection Network™ (SPN) infrastructure protected users from more than 40 billion threats consisting of email threats, malicious files, and malicious URLs.

40,956,909,973

Blocked threats from January 2021 to June 2021

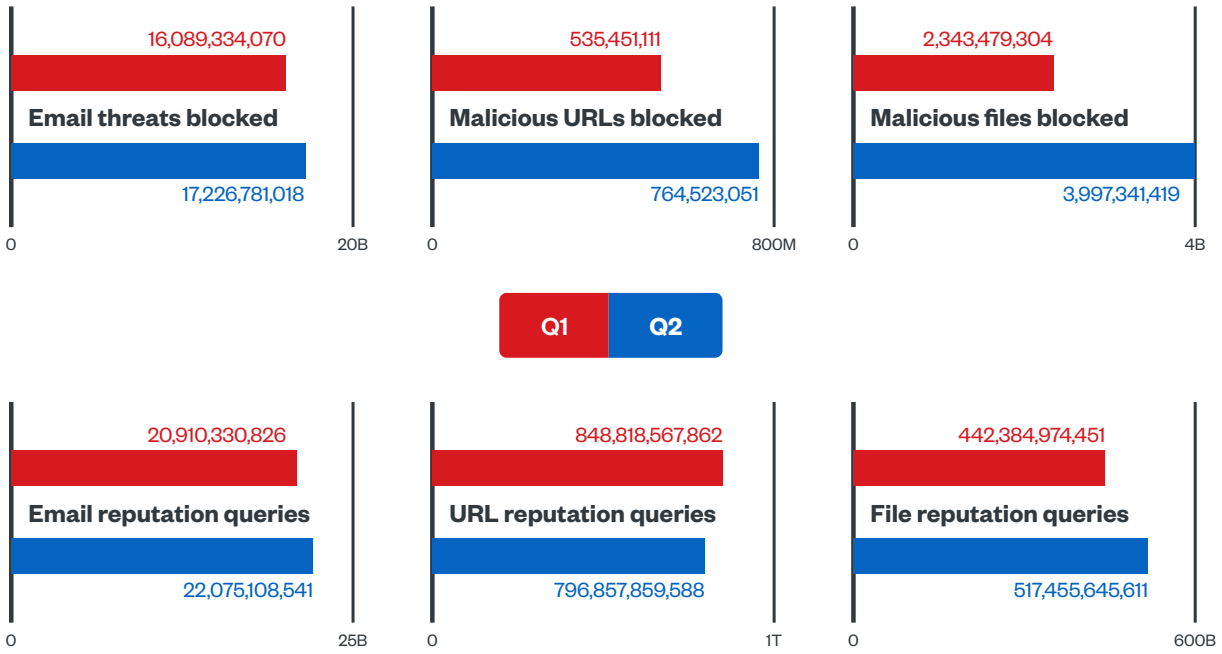

Figure 13. The number of blocked email threats, malicious files, and malicious URLs increased from the first to the second quarter of the year. Email and file queries increased while URL reputation queries decreased.

Source: Trend Micro Smart Protection Network infrastructure

Cryptocurrency miners have not only become much more prevalent over the past few months but have also become the most detected malware. WannaCry had previously been at the top of this list for a few years, but detection numbers for this family have been on a steady decline recently, causing it to move to the second spot. Webshell, which rounds out the top three, is the malware used by attackers when they successfully exploit web servers to enable them to have remote access to the affected machines.

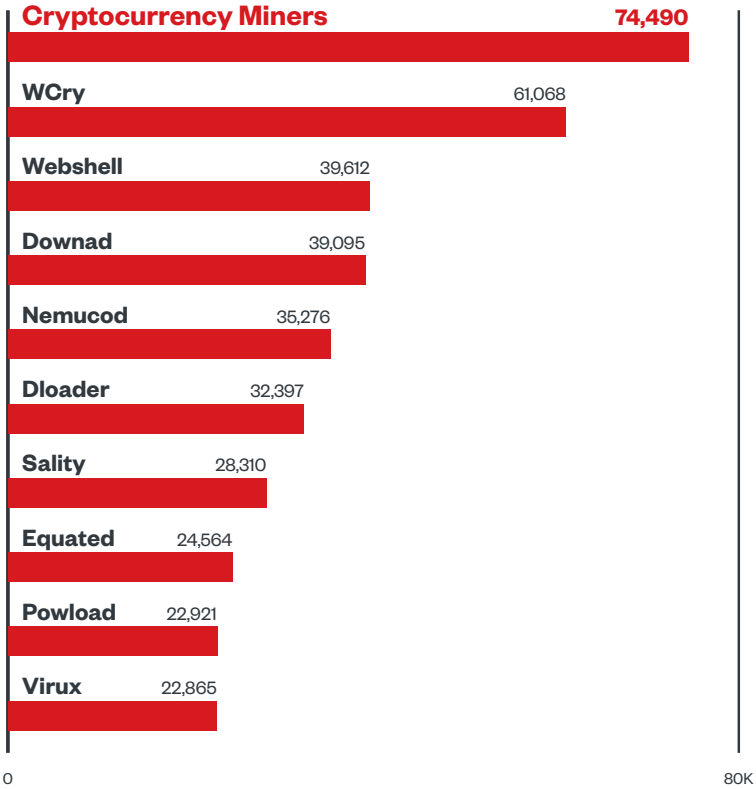

Figure 14. Cryptocurrency miners were the most detected malware, with long-running family WannaCry in the second spot: The 10 most detected malware families in the first half of 2021

Source: Trend Micro Smart Protection Network infrastructure

The most active cryptocurrency miners are mostly consistent with what we saw in 2020. MalXMR remains in the top spot, with Coinminer and ToolXMR rising in the ranks.

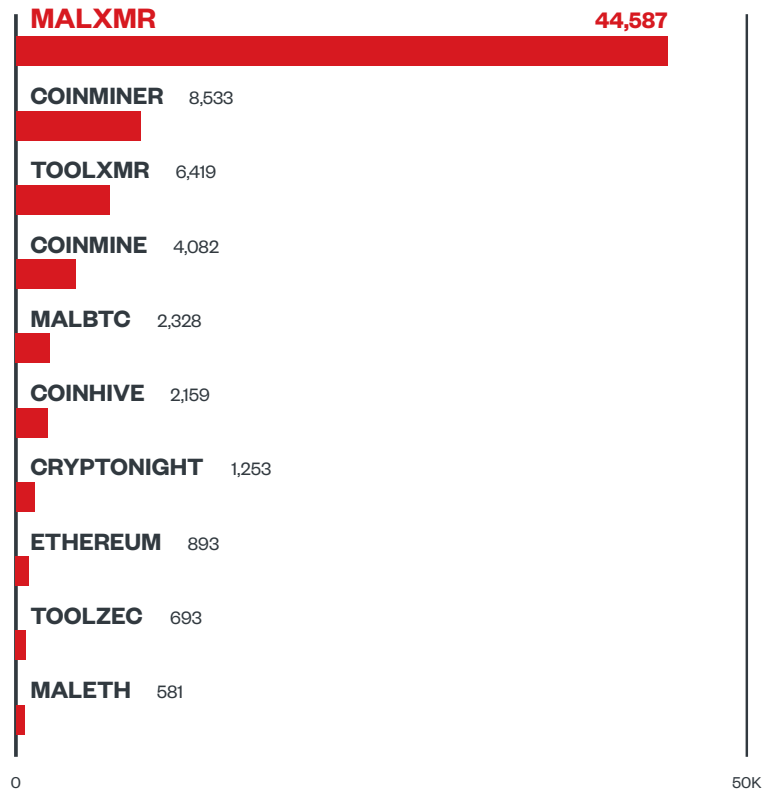

Figure 15. MalXMR, Coinminer, and ToolXMR were the most detected cryptocurrency miners: The 10 most detected cryptocurrency miners in the first half of 2021

Source: Trend Micro Smart Protection Network infrastructure

In the first half of 2021, we detected over 840,000 endpoints that connected to C&C servers and just over 22,000 C&C servers. There has been a steady decline in detections since 2020, and we see that compared to the same time last year, botnet connections decreased 36.8% and C&C servers decreased 73.1%.

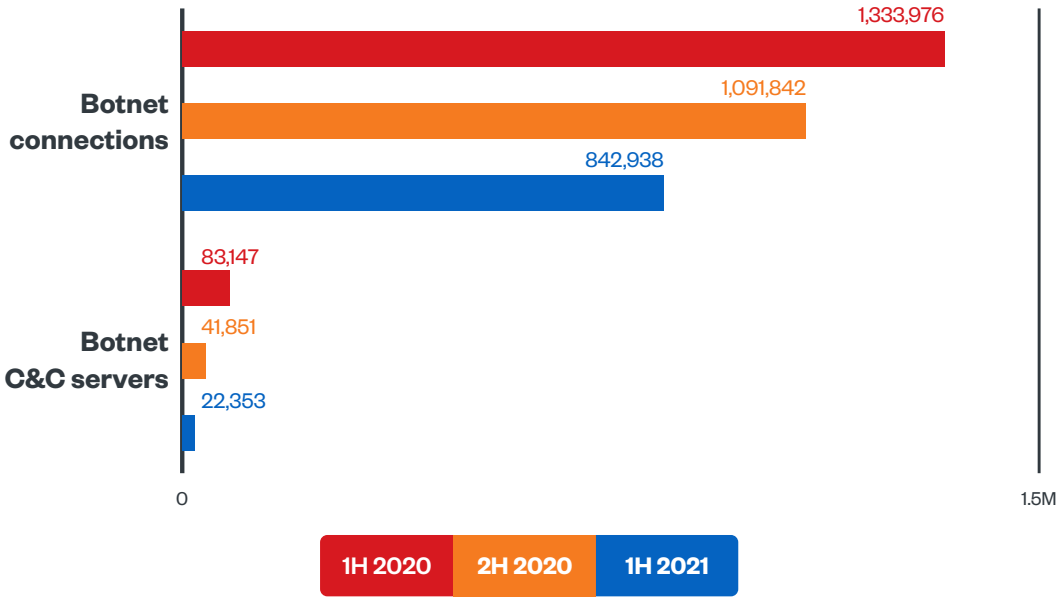

Figure 16. We detected roughly 840,000 botnet connections and over 20,000 botnet C&C servers: The numbers of detected botnet connections and botnet C&C servers in the first half of 2021

Note: Botnet connections were unique endpoints that queried or connected to C&C servers, while botnet C&C servers were unique and active C&C servers that endpoints queried or connected to.

Source: Trend Micro Smart Protection Network infrastructure

Ransomware family detections have been steadily decreasing since 2020; there were only 49 families discovered in the first half of 2021. Despite that, most of the notable cyberattacks in terms of financial impact and effect on real-world operations were ransomware attacks.

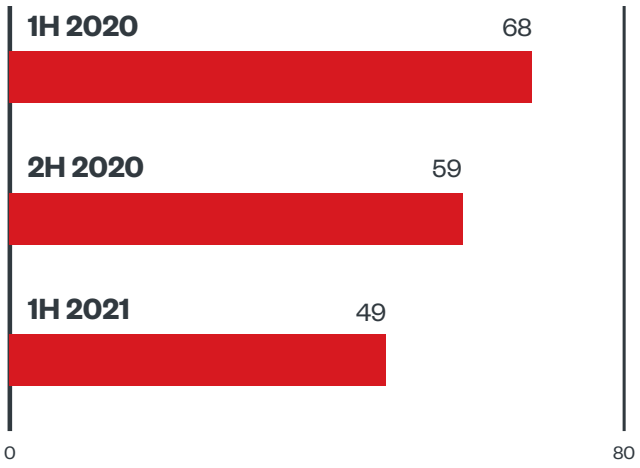

Figure 17. A comparison of the numbers of new ransomware families in 2020 and the first half of 2021 shows that new ransomware families decreased by 17%.

New ransomware families seen in 2021					
JAN	**FEB**	**MAR**	**APR**	**MAY**	**JUN**
Amjixius	IziCrypt	TrojanLock	Blackhole	Apostrius	DarkRadiation
Sophcrypt	Cryng	VoidCrypt	Nitro	Venus	Babuk
Sharpcrypter	HDLocker	HogLocker	Astro Locker	Hades	FakeRyuk
Cicada	Sickransom	OnCrypt	Hanta	Qlocker	LegionLocker
Crysis.TIBGGH	Lucifer	DadiCrypt	WhiteBlackCrypt	FiveHands	GonnaCrypt
Bluecrab	Butwo	Assist		Taihenchan	
Judge	Flamingo	HelpYou		Networm	
Mijnal	CNHCrypt	ThunderCrypt		NoCry	
Namaste		Gangbang			
Gunshot		DarkWorld			
Garytest					
Moloch					
Psixtin					

Table 5. 49 new ransomware families were discovered: New ransomware families detected in the first half of 2021

Sources: Trend Micro Smart Protection Network infrastructure and analysis of externally sourced data

There were over 5 million detections of file types used in spam email attachments, and PDF attachments made up 66.1% of that number. DOCX and EXE files were also sizeable portions of the overall count.

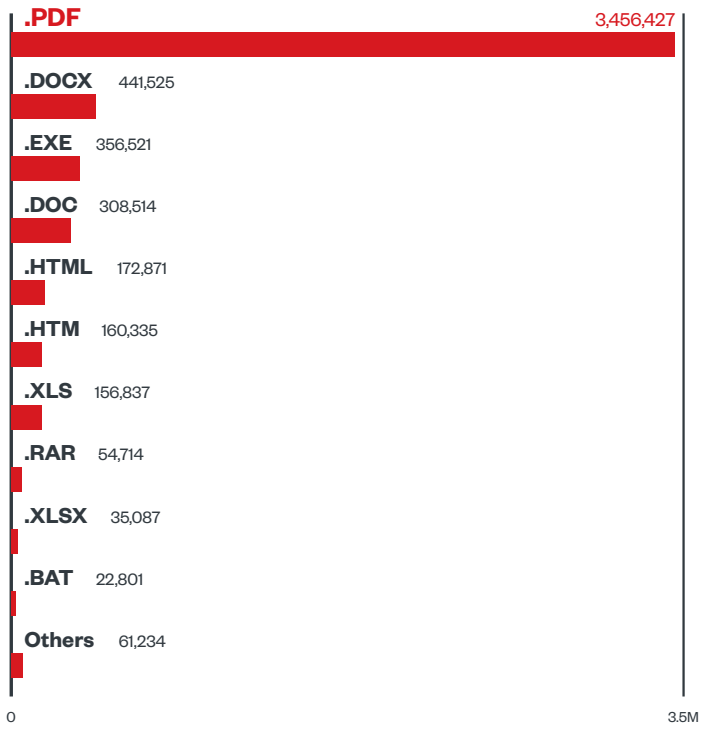

Figure 18. PDF files accounted for most spam email attachments:
The distribution of file types used in spam email attachments in the first half of 2021

Source: Trend Micro Email Reputation Services

In the first six months of 2021, we found over 3 million detections for mobile device-related malicious samples. We also saw an uptick in the number of malicious Android apps.

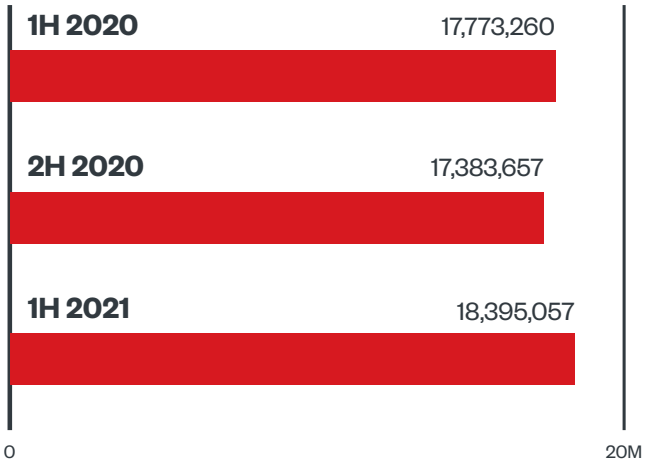

Figure 19. A half-year comparison of the number of blocked malicious Android app shows an upward trend.

Source: Trend Micro Mobile App Reputation Service

Business email compromise (BEC) scams increased slightly since 2020, rising roughly 4% from the first half of 2020. This might be due to malicious actors targeting businesses involved in Covid-19 vaccination programs, as well as attacks on the supply chain for vaccine production.

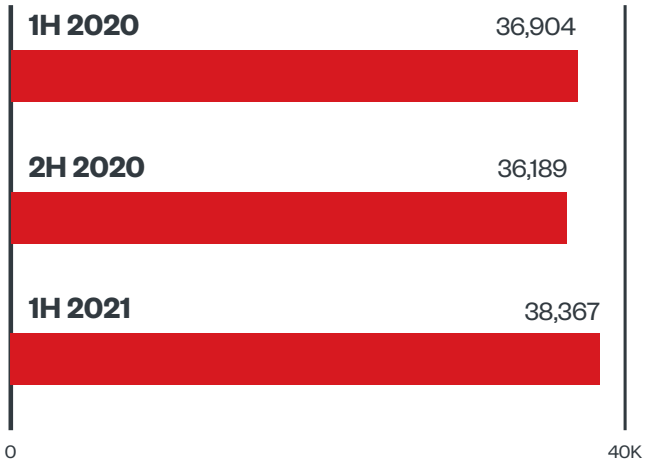

Figure 20. A half-year comparison of BEC attempts shows an increase in the first half of 2021.

Note: Data refers to the number of BEC attempts seen, which does not indicate whether the attacks were successful.

Source: Trend Micro Smart Protection Network infrastructure

References

1 Trend Micro. (June 8, 2021). *Trend Micro Security News*. "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.

2 Trend Micro. (June 8, 2021). *Trend Micro Security News*. "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.

3 Trend Micro. (June 8, 2021). *Trend Micro Security News*. "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.

4 Trend Microh. (Feb. 23, 2021). *Trend Micro*. "A Constant State Of Flux: Trend Micro 2020 Annual Cybersecurity Report." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/ph/security/research-and-analysis/threat-reports/roundup/a-constant-state-of-flux-trend-micro-2020-annual-cybersecurity-report.

5 Trend Micro. (June 8, 2021). *Trend Micro Security News*. "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.

6 Trend Micro. (May 12, 2021). *Trend Micro*. "What We Know About the DarkSide Ransomware and the US Pipeline Attack." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.

7 Cedric Pernet. (June 18, 2021). *Trend Micro*. "Fake DarkSide Campaign Targets Energy and Food Sectors." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/f/fake-darkside-campaign-targets-energy-and-food-sectors.html.

8 Mina Naiim. (May 28, 2021). *Trend Micro*. "DarkSide on Linux: Virtual Machines Targeted." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html.

9 Trend Micro. (June 15, 2021). *Trend Micro*. "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

10 Arianne Dela Cruz et al. (May 6, 2021). *Trend Micro*. "Proxylogon: A Coinminer, a Ransomware, and a Botnet Join the Party." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/e/proxylogon-a-coinminer--a-ransomware--and-a-botnet-join-the-part.html.

11 Trend Micro. (June 15, 2021). *Trend Micro*. "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

12 Sergiu Gatlan. (May 17, 2021). *Bleeping Computer*. "Conti ransomware also targeted Ireland's Department of Health." Accessed on Aug. 12, 2021, at https://www.bleepingcomputer.com/news/security/conti-ransomware-also-targeted-irelands-department-of-health/.

13 Trend Micro. (Jan. 26, 2021). *Trend Micro*. "Examining A Sodinokibi Attack." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/a/sodinokibi-ransomware.html.

14 Mitchell Clark. (June 3, 2021). *The Verge*. "FBI names REvil as the group behind meat supplier cyberattack." Accessed on Aug. 12, 2021, at https://www.theverge.com/2021/6/3/22466003/jbs-cyberattack-fbi-revil-sodinokibi-criminal-group.

15 Janus Agcaoili. (April 27, 2021). *Trend Micro*. "Hello Ransomware Uses Updated China Chopper Web Shell, SharePoint Vulnerability." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html.

16 Mitchell Clark. (May 10, 2021). *The Verge*. "Colonial Pipeline hackers apologize, promise to ransom less controversial targets in future." Accessed on Aug. 12, 2021, at https://www.theverge.com/2021/5/10/22428996/colonial-pipeline-ransomware-attack-apology-investigation.

17 Janus Agcaoili and Byron Gelera. (Feb. 23, 2021). *Trend Micro*. "An Analysis of the Nefilim Ransomware." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html.

18 Janus Agcaoili and Earle Earnshaw. (Apr. 29, 2021). *Trend Micro*. "Locked, Loaded, and in the Wrong Hands: Legitimate Tools Weaponized For Ransomware in 2021." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021.

19 Department of Justice Office of Public Affairs. (June 7, 2021). *United States Department of Justice*. "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." Accessed on Aug. 12, 2021, at https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

20 Reuters. (May 13, 2021). *Reuters*. "Colonial Pipeline has cyber insurance policy - sources." Accessed on Aug. 12, 2021, at https://www.reuters.com/business/energy/colonial-pipeline-has-cyber-insurance-policy-sources-2021-05-13/.

21 Luke Gallin. (Feb. 7, 2021). *Reinsurance News*. "Norsk Hydro claims a further $20.2mn from its cyber insurance in Q4." Accessed on Aug. 12, 2021, at https://www.reinsurancene.ws/norsk-hydro-claims-a-further-20-2mn-from-its-cyber-insurance-in-q4/.

22 Jen McPhillips. (n.d.). *Coalition Inc*. "Coalition releases new H1 2020 Cyber Insurance Claims Report." Accessed on Aug. 12, 2021, at https://www.coalitioninc.com/blog/coalition-releases-new-2020-cyber-insurance-claims-report.

23 Lindsey O'Donnell. (June 1, 2021). *Threatpost*. "Cyber-Insurance Fuels Ransomware Payment Surge." Accessed on Aug. 12, 2021, at https://threatpost.com/cyber-insurance-ransomware-payments/166580/.

24 Department of Treasury. (n.d.). *Treasury Department*. "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." Accessed on Aug. 12, 2021, at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

25 Phil Goldstein. (March 9, 2020). *Sate Tech Magazine*. "New York May Ban Ransomware Payments from Municipalities." Accessed on Aug. 12, 2021, at https://statetechmagazine.com/article/2020/03/new-york-may-ban-ransomware-payments-municipalities.

26 Arielle Waldman. (June 16, 2020). *Tech Target*. "Repeat Ransomware Attacks Hit 80% of Victims who Paid Ransoms." Accessed on Aug. 12, 2021, at https://searchsecurity.techtarget.com/news/252502519/Repeat-ransomware-attacks-hit-80-of-victims-who-paid-ransoms.

27 Erin Johnson. (March 2, 2021). *Trend Micro*. "Emotet One Month After the Takedown." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/c/emotet-one-month-after-the-takedown.html.

28 Andy Greenberg. (Jan. 27, 2021). *Wired*. "Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware.'" Accessed on Aug. 12, 2021, at https://www.wired.com/story/emotet-botnet-takedown/.

29 Department of Justice Office of Public Affairs. (Jan. 28, 2021). "Emotet Botnet Disrupted in International Cyber Operation." Accessed on Aug. 12, 2021, at https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

30 Cybereason Nocturnus. (April 2, 21019). *Cyberreason*. "A One-two Punch of Emotet, TrickBot, & Ryuk Stealing & Ransoming Data." Accessed on Aug. 12, 2021, at https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data.

31 David Fiser and Alfredo Oliveira. (March 9, 2021). *Trend Micro*. "TeamTNT Continues Attack on the Cloud, Targets AWS Credentials." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/c/teamtnt-continues-attack-on-the-cloud--targets-aws-credentials.html.

32 Magno Logan and David Fiser. (May 25, 2021). *Trend Micro*. "TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html.

33 Trend Micro. (Jan. 5, 2021). *Trend Micro*. "Earth Wendigo Injects JavaScript Backdoor for Mailbox Exfiltration." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html.

34 Adi Peretz and Erick Thek. (March. 5, 2021). *Trend Micro*. "Earth Vetala – MuddyWater Continues to Target Organizations in the Middle East." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html.

35 Daniel Lunghi and Kenney Lu. (April 9, 2021). *Trend Micro*. "Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html.

36 Gilbert Sison, Abraham Camba, and Ryan Maglaque. (Jan. 20, 2021). *Trend Micro*. "Investigation into PlugX Uncovers Unique APT Technique." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/a/xdr-investigation-uncovers-plugx-unique-technique-in-apt-attack.html.

37 Paul Pajares. (July 8, 2021). *Trend Micro*. "Threats Ride on the Covid-19 Vaccination Wave." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/g/threats-ride-on-the-covid-19-vaccination-wave.html.

38 Paul Pajares. (July 8, 2021). *Trend Micro*. "Threats Ride on the Covid-19 Vaccination Wave." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/g/threats-ride-on-the-covid-19-vaccination-wave.html.

39 Echo Duan and Jesse Chang. (Feb 15, 2021). *Trend Micro*. "SHAREit Flaw Could Lead to Remote Code Execution." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/b/shareit-flaw-could-lead-to-remote-code-execution.html.

40 Sébastien Dudek. (Jan. 26, 2021). *Trend Micro*. "Low Powered and High Risk: Possible Attacks on LoRaWAN Devices." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html.

41 Sébastien Dudek. (Feb. 18, 2021). *Trend Micro*. "Gauging LoRaWAN Communication Security with LoraPWN." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/b/gauging-lorawan-communication-security-with-lorapwn.html.

42 Sébastien Dudek. (March 30, 2021). *Trend Micro*. "Protecting LoRaWAN Hardware from Attacks in the Wild." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/c/protecting-lorawan-hardware-from-attacks-in-the-wild.html.

43 Trend Micro. (May 27, 2021). *Trend Micro*. "The Transition to 5G: Security Implications of Campus Networks." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-transition-to-5g-security-implications-of-campus-networks.

44 Stephen Hilt and Fernando Merces. (Jan. 19, 2021). *Trend Micro*. "VPNFilter Two Years Later: Routers Still Compromised." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_ph/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html.

45 Nitesh Surana. (April 14, 2021). *Trend Micro*. "Could the Microsoft Exchange breach be stopped?" Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/devops/21/d/could-the-microsoft-exchange-breach-be-stopped.html.

46 Nitesh Surana. (April 14, 2021). *Trend Micro*. "Could the Microsoft Exchange breach be stopped?" Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/devops/21/d/could-the-microsoft-exchange-breach-be-stopped.html.

47 Benjamin Delpy. (July 17, 2021). *Twitter*. "Printnightmare." Accessed on Aug. 12, 2021, at https://twitter.com/gentilkiwi/status/1416079316673339392.

48 The Windows Team. (June 28, 2021). *Windows*. "Update on Windows 11 minimum system requirements." Accessed on Aug. 12, 2021, at https://blogs.windows.com/windows-insider/2021/06/28/update-on-windows-11-minimum-system-requirements/.

49 Trend Micro. (Feb. 23, 2021). *Trend Micro*. "A Constant State Of Flux: Trend Micro 2020 Annual Cybersecurity Report." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-constant-state-of-flux-trend-micro-2020-annual-cybersecurity-report.

50 Anthony Spadafora. (Feb. 9, 2021). *Tech Radar*. "VPN usage saw major spike last year - here's why." Accessed on Aug. 12, 2021, at https://www.techradar.com/news/vpn-usage-saw-major-spike-last-year-heres-why.

51 Ivana Vojinovic. (March 21, 2021). *Data Prot*. "VPN Statistics for 2021 – Keeping Your Browsing Habits Private." Accessed on Aug. 12, 2021, at https://dataprot.net/statistics/vpn-statistics/#:~:text=The%20VPN%20industry%20is%20expected,ages%20of%2016%20and%2024.

52 David Fiser and Alfredo Oliveira. (March 9, 2021). *Trend Micro*. "TeamTNT Continues Attack on the Cloud, Targets AWS Credentials." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/c/teamtnt-continues-attack-on-the-cloud--targets-aws-credentials.html.

53 Magno Logan and David Fiser. (May 25, 2021). *Trend Micro*. "TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack." Accessed on Aug. 12, 2021, at https://www.trendmicro.com/en_us/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html.

54 Steven J. Vaughan-Nichols. (May 6, 2020). *ZDNet*. "Most popular operating systems of 2020: The more things change...." Accessed on Aug. 12, 2021, at https://www.zdnet.com/article/whats-2020s-most-popular-operating-systems/.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research