Defending the Expanding Attack Surface

Trend Micro 2022 Midyear Cybersecurity Report

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

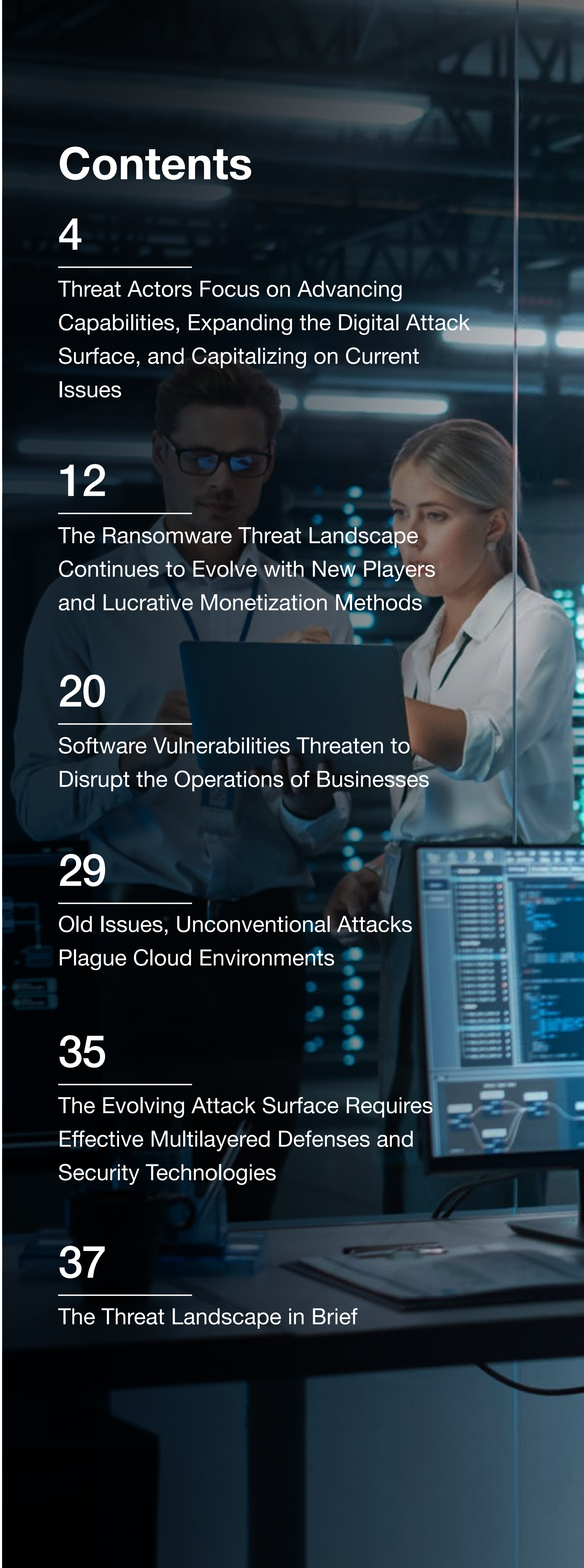
Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Stock image used under license from
Shutterstock.com



Contents

The first half of 2022 saw large sections of the workforce either returning to the physical workplace or transitioning to a hybrid setup consisting of a combination of both work-from-home (WFH) and on-site work. For many organizations that have transitioned their employees to remote working environments during the past couple of years, these changes mean facing an ever-growing attack surface in the new normal, where security teams must contend with the challenge of defending all possible sections of the IT infrastructure.

Ransomware developers continued their shift toward more lucrative and efficient monetization methods, particularly the ransomware-as-a-service (RaaS) model that has been credited as one of the key reasons for the rapid spread of ransomware attacks. In the first half of the year, three RaaS threat actors stood above the rest: Conti, LockBit, and BlackCat, each of which saw significantly higher detections in the first half of the year compared to the first half of 2021, indicating that cybercriminals are increasingly turning toward a RaaS partnership due to the benefits it provides for both parties. We also observed relatively new ransomware families such as Black Basta, Nokoyawa, and Hive being used in high-profile attacks on big-game targets.

The first half of 2022 also saw the emergence of advanced persistent threat (APT) groups that employed sophisticated toolkits and expansive infrastructure in their campaigns. At the same time, threat actors continued to turn to commodity malware, integrating older tools and malware into their attack routines for their capabilities and reliability. We have also observed that cybercriminals are seemingly looking to expand their operations beyond non-Windows operating systems, with Linux increasingly coming under fire. In their endless pursuit to benefit from any situation, malicious actors also capitalized on the Russia-Ukraine hostilities to launch cyberattacks on either side or prey on people interested in the conflict.

Based on Trend Micro™ Zero Day Initiative™ (ZDI) data, there was a rise in the number of published vulnerability advisories in general, as well as in critical- and high-severity flaws during the first half of 2022. We focused on some of the noteworthy critical vulnerabilities that targeted crucial business tools and software that are used in enterprise systems while also taking note of the vulnerabilities that affected macOS and Linux. We also delved into the Data Distribution Service Standard (DDS) and the vulnerabilities that might have a potential impact on the machines and devices that use this standard.

The cloud remains a popular target for malicious actors, with some capitalizing on old and persistent issues such as misconfiguration and others attempting to develop more novel and unconventional methods to launch attacks on cloud infrastructure.

In our 2022 midyear roundup, we examine the most significant trends and incidents that influenced the cybersecurity landscape in the first half of the year. We also review our 2022 security predictions to see which ones aligned with the trends in the first six months of the year. Through this report, we hope to enlighten users and organizations not just on the different threats that they face but also the robust security measures and policies that they need to consider to protect their environments and systems in the face of a growing attack surface that requires equally capable and extensive security measures.

Threat Actors Focus on Advancing Capabilities, Expanding the Digital Attack Surface, and Capitalizing on Current Issues

Organizations Express Concern Over the Growing Attack Surface

Over the past few years, many companies have risen to the challenge of digital transformation by adopting digital technologies to modify their existing business models, processes, and company cultures. This transformation has subsequently created a wider digital attack surface that encompasses a broader range of areas, including email inboxes, internet-of-things (IoT) devices, mobile applications, websites, public cloud services, and even the supply-chain infrastructure.

In a study we conducted in partnership with Sapio Research, we surveyed 6,297 IT security decision-makers from 29 countries about their thoughts on the risks brought about by the growing attack surface.[1] We discovered that a significant number (73%) of them were concerned about the size of their digital attack surface. 37% described their situation as constantly evolving and messy, while another 43% argued that the attack surface is spiraling out of control.

Despite these concerns, 62% of the respondents admitted to having blind spots that weaken their security posture. 37% of the organizations also claimed to have the least insight into cloud assets. 35% said the same of their insights into networks, while 32% responded that they have the least insight into their end-user assets.

It also became clear that a number of these organizations were uncertain about how to proceed given the risks that they face. 38% of respondents identified quantifying cyber risk as their primary challenge, while 33% stated that they simply lack the resources to understand and manage these risks. Another 32% cited that they have limited visibility into the areas that are at risk.

73% of IT security decision makers are concerned about the digital attack surface.

43% argue that the attack surface is spiraling out of control.

37% describe the attack surface as constantly evolving and messy.

Figure 1. A survey of 6,297 IT security decision-makers reveals that a significant number of them are concerned about the digital attack surface.

Source: Trend Micro survey in partnership with Sapio Research

Areas where organizations have the least security insight into

37% Cloud assets

34% Networks

32% End-user assets

Figure 2. IT security decision-makers name cloud assets, networks, and end-user assets as the top three areas where they have the least security insights into.

Source: Trend Micro survey in partnership with Sapio Research

Threat Actors Like Earth Lusca and Earth Berberoka Continue to Use Wide-Ranging Tools and Extensive Infrastructure in Their Attacks

The first half of 2022 saw the continuation of targeted campaigns involving APT groups that play the long game by employing large infrastructure and integrating different kinds of malware and other tools in their attacks.

One of the prominent APT groups from the first half of 2022 was the Earth Lusca, a threat actor that has been active since mid-2021[2] and which conducts cyberespionage and financially motivated campaigns targeting a wide range of organizations around the world by using spear-phishing lures and watering holes.

The group employs infrastructure that can be divided into two clusters. The first is built via rented virtual private servers (VPSs) that are used for Earth Lusca's social engineering attacks. The group also uses these as their command-and-control (C&C) servers. In particular, Earth Lusca uses the C&C server that is connected to this cluster to deploy a number of malware families such as Cobalt Strike, ShadowPad, Funny Switch, and Winnti.

The second cluster is composed of compromised servers that run older, open-source versions of Oracle GlassFish Server. This cluster is used for vulnerability scanning in public-facing servers and building traffic tunnels within the network. The group also uses it as a C&C server for Cobalt Strike.

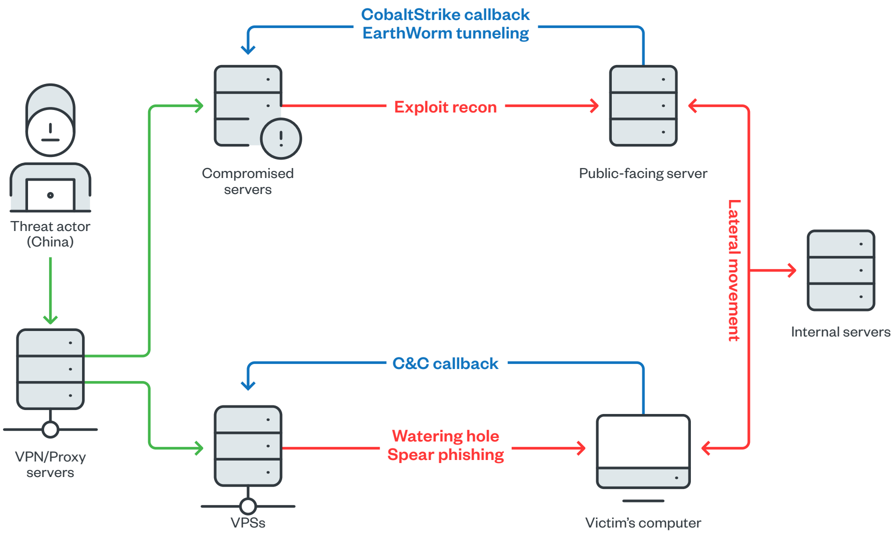


Figure 3. Earth Lusca's infection routine showing the two clusters the group employs in its attacks

A large portion of the threat actor's primary victims seem to be high-value targets such as government and educational institutions, political groups, news media, and even Covid-19 research organizations.

In April 2022, we published a research paper documenting the activities of an APT group we named Earth Berberoka that primarily targets gambling websites in China.[3] The group, which has been active since at least 2020, uses a wide range of malware families that share the same back-end infrastructure despite targeting different operating systems (Windows, Linux, and macOS).

In addition to its extensive list of malware families, Earth Berberoka employs several different infection vectors: an allegedly secure chat app called MiMi, a bogus cryptocurrency app, and a website hosting a malicious Adobe Flash Player installer.

Another notable intrusion set we encountered in the first half of 2022 is NetDooka, a multicomponent malware framework that is distributed via a pay-per-install (PPI) service.[4] The framework, which contains a loader, a dropper, a protection driver, and a remote access trojan (RAT), uses the PrivateLoader malware for distribution. According to a report from Intel471, PrivateLoader infects a user's machine through downloaded pirated software.[5]

Following infection, it installs the first NetDooka malware, a dropper component that decrypts and executes the loader. After scanning the environment, the loader then downloads another dropper component that is executed by the loader. This dropper will be used for decrypting and executing the final payload, a full-featured RAT that can perform various functions such as starting a remote shell, grabbing browser data, and taking screenshots.

The infrastructure of NetDooka makes it an attractive option for clients that want to avail of the PPI business model for their operations while also allowing their operators the opportunity to easily spread their malware.

Threat Actors Like Conti Drive Emotet Resurgence

Although new malware families often garner the lion's share of attention from both the security industry and the general public, older malware, especially those that have proven to be effective, still pose a threat to organizations. In our 2022 security predictions, we mentioned that malicious actors are increasingly turning to commodity malware and other tools to make their attacks more effective.[6] This has turned out to be an accurate prediction for Emotet, an infamous botnet that is being offered as part of a malware-as-a-service (MaaS) scheme.

Predictions

In our 2022 security predictions, we foresaw that commodity malware would grow into a formidable threat as ransomware operators continuously integrate it into their attacks.

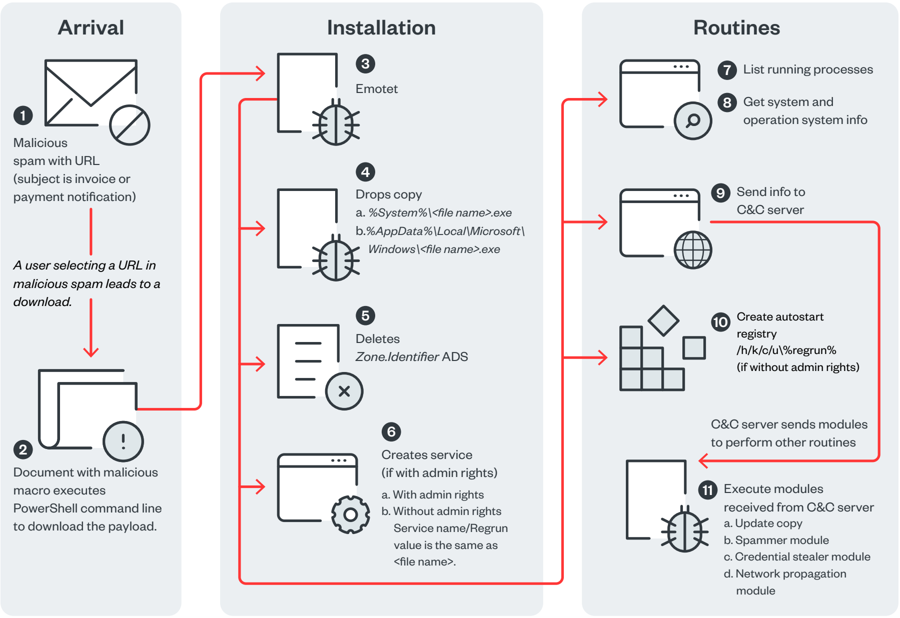

Arrival
1
Malicious spam with URL (subject is invoice or payment notification)
A user selecting a URL in malicious spam leads to a download.
2
Document with malicious macro executes PowerShell command line to download the payload.
Installation
3
Emotet
4
Drops copy
a. %System%\<file name>.exe
b.%AppData%\Local\Microsoft\Windows\<file name>.exe
5
Deletes Zone.Identifier ADS
6
Creates service (if with admin rights)
a. With admin rights
b. Without admin rights Service name/Regrun value is the same as <file name>.
Routines
7 List running processes
8 Get system and operation system info
9 Send info to C&C server
10 Create autostart registry /h/k/c/u\%regrun% (if without admin rights)
C&C server sends modules to perform other routines
11 Execute modules received from C&C server
a. Update copy
b. Spammer module
c. Credential stealer module
d. Network propagation module

Figure 4. Infection chain used in the Emotet infections we analyzed in May 2022

Emotet made its debut in 2014 and is known to have been used by operators of other malware such as Conti and Ryuk in their attacks. In 2021, its infrastructure was taken down through the collaborative effort of various law enforcement agencies from different countries.[7]

However, the dismantling of its infrastructure did not signal the end of Emotet. Just a few months later, it was observed being used in a Trickbot campaign.[8] In the first half of 2022, we saw a massive uptick in Emotet detections compared to those in the first half of 2021, proof that the botnet is thriving as a result of threat actors opting to integrate it into their operations. Indeed, researchers from Advintel named Conti operators as one of the reasons behind Emotet's recent resurgence.[9]

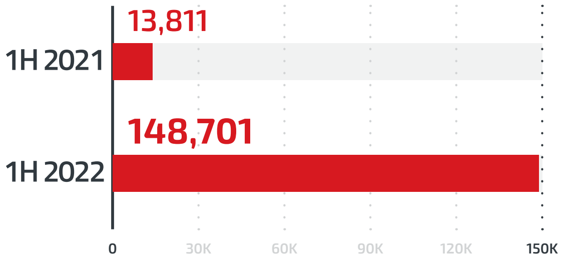


Figure 5. Emotet detections increased by over 10 times in the first half of 2022 compared to the first half of 2021, likely due to prolific threat actors using it as part of their operations.

Source: Trend Micro Smart Protection Network

Based on our Smart Protection Network (SPN) sensors, majority of the Emotet detections occurred in Japan, with the US, India, Italy, and Brazil rounding up the top five. While this does not necessarily indicate that Japan is where Emotet is most active (due to the nature of security sensors), it does show that the malware has high levels of activity in the country.

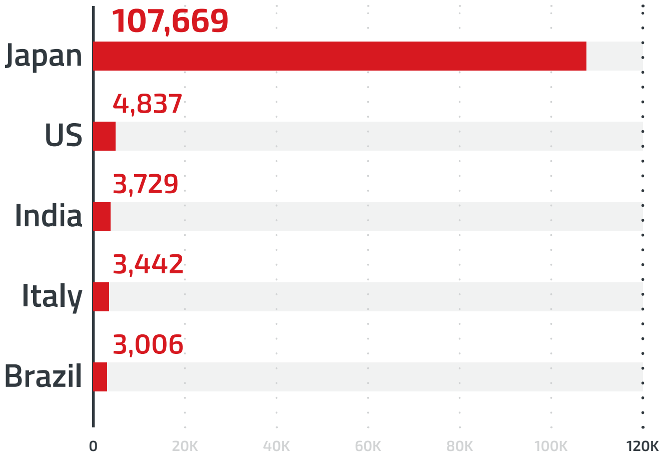


Figure 6. The countries with the highest number of Emotet detections

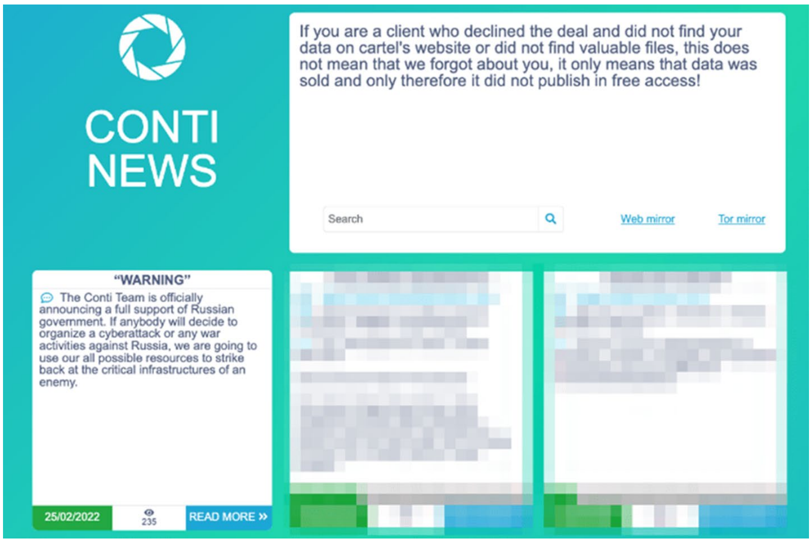
Source: Trend Micro Smart Protection Network

In May 2022, we analyzed Emotet infections across various regions and discovered that while the attacks still relied on spam campaigns, it also added small changes to its routine, such as using Excel 4.0 macros for its downloading procedure instead of using Visual Basic for Applications (VBA).[10] Other changes that were implemented in these recent Emotet infections include streamlined payloads and additional obfuscation techniques. Perhaps most importantly, the operators of Emotet have since added Cobalt Strike to their arsenal since the botnet's reappearance, making newer Emotet campaigns more dangerous.

Russia-Ukraine Conflict Extends to the Cybercrime Sphere

On February 24, 2022, the Russia-Ukraine war began. While there has been much focus on physical battles on the ground, it's important to highlight that cyberattacks targeting both sides were also launched in the ensuing chaos.[11]

One of the prominent threat actors that became involved early on was Conti, which announced its support for the Russian government just a day after the hostilities started. On its leak site, the group announced that they would strike back at groups or individuals who launched cyberattacks on Russia, although Conti would subsequently soften its stance in a succeeding post.



If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

"WARNING"

The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

Figure 7. Initial statement from the Conti group warning would-be attackers of retaliation should they target Russian infrastructure

SPN data shows a spike in BazarLoader detections in the first half of 2022 compared to the first half of the previous year — a notable shift since BazarLoader is a key enabler in Conti campaigns.

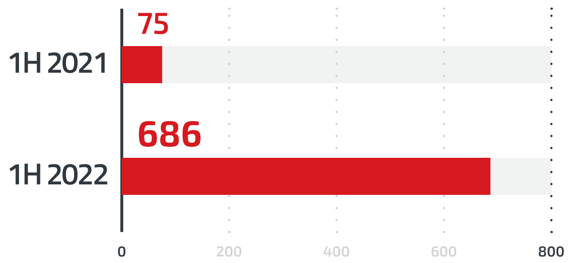


Figure 8. There were nearly 10 times as many BazarLoader detections in the first half of 2022 compared to the first half of 2021.

Source: Trend Micro Smart Protection Network

The Stormous ransomware gang, a group of Arabic-speaking cybercriminals, also announced its support for Russia[12] and declared that it would target Ukrainian government institutions as part of its plans.

Our analysis of the malware used by Stormous reveals that the group uses it to deploy different kinds of custom payloads to its victim through remote uploading and resources such as Pastebin.

Alongside ransomware groups becoming involved, security researchers observed attacks that, although not directly connected to the ongoing war, were being launched on Ukrainian organizations, websites, and infrastructure even before the conflict began.

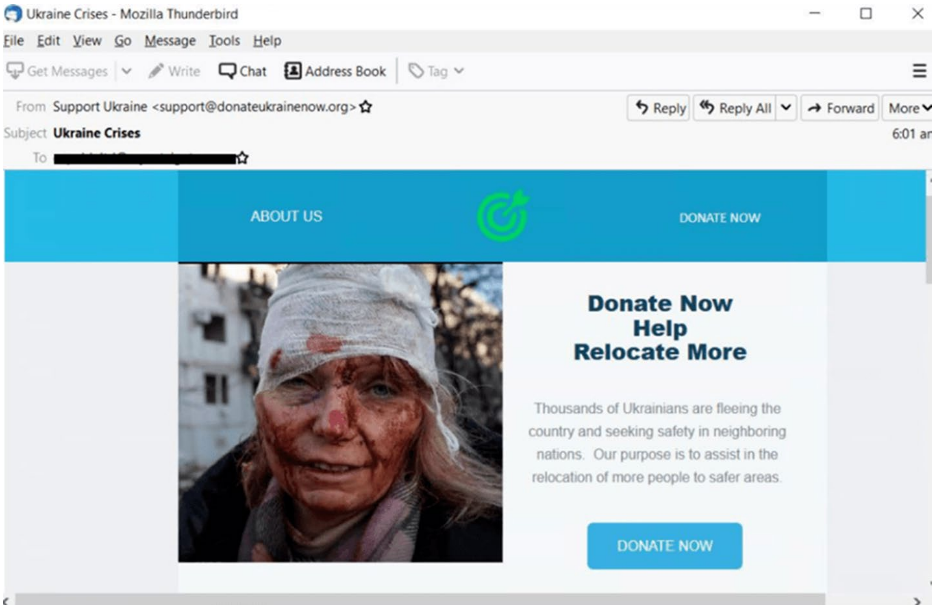
In January and February 2022, a wave of spear-phishing emails was sent to Ukrainian targets — ostensibly from Ukrainian organizations such as the National Healthcare Service and the police force — containing attachments that download and execute the OutSteel and SaintBot malware.[13] It's possible that these campaigns were carried out for information-gathering purposes as a precursor to the invasion.

On January 13 and 14, 2022, threat actors launched a direct attack on approximately 70 Ukrainian government websites, leading to the defacement of website content and system corruption via the malware WhisperGate.[14] It is suspected that these attacks were enabled via the content management system OctoberCMS, supply-chain attacks, and the exploitation of the Log4j vulnerability.[15]

At first glance, these incidents belie the complexity of the attacks launched on either side of the war. As evidenced by a March 2022 campaign that we analyzed, however, these cyberattacks are not a one-way street. In this campaign, operators used a piece of malware called RuRansom designed to infect Russian targets. Although its name implies otherwise, RuRansom is not an example of ransomware but a wiper designed to destroy its victim's data and backup files. Our discovery of numerous versions of RuRansom indicates that the malware is still under development.

Although several ransomware groups became involved, it would be a mistake to think that ransomware gangs were the only ones to take part in the Russia-Ukraine war. For example, hacktivist collective Anonymous took part in the cyber conflict by targeting Russian assets and information in attacks that included publishing confidential files from the Russian central bank, taking over state-controlled television, and leaking the personal data of Russian military personnel.[16]

Other malicious actors, while not directly targeting either side of the conflict, still attempted to capitalize on the situation. Through our honeypot, we found war-related spam emails aiming to take advantage of the situation under the guise of asking for donations and using scams to create bogus recipients of such donations. Some of these spam emails drop malware such as Ave Maria as an attachment.[17]



From Support Ukraine <support@donateukrainenow.org>

Subject **Ukraine Crises**

To [redacted]

6:01 ar

Donate Now
Help
Relocate More

Thousands of Ukrainians are fleeing the country and seeking safety in neighboring nations. Our purpose is to assist in the relocation of more people to safer areas.

Figure 9. A scam email asking recipients for donations to help with Ukrainian relocations

The Ransomware Threat Landscape Continues to Evolve with New Players and Lucrative Monetization Methods

LockBit, Conti, and BlackCat Operators Continue to Employ the Profitable RaaS Scheme

The advent of RaaS has resulted in would-be cybercriminals having access to the tools and infrastructure that would not have been available to them under ordinary circumstances.[18] One of the unique aspects of the RaaS model is the relationship between the developers and their affiliates who act as middlemen. Affiliates are also responsible for the actual infections and split ransom payment with the developers. This kind of setup provides developers additional time to evolve their malware and tools while also affording them protection from the scrutiny of security researchers and law enforcement. On the other hand, affiliates profit from ransomware attacks without the extensive legwork and infrastructure needed to initiate expansive ransomware campaigns.

Predictions

We predicted that ransomware operators would implement modern and sophisticated extortion methods while also going after more prominent targets. would grow into a formidable threat as ransomware operators continuously integrate it into their attacks.

Our telemetry data shows that over 50 active RaaS and extortion groups and more than 1,200 organizations were victimized by ransomware in the first half of the year.

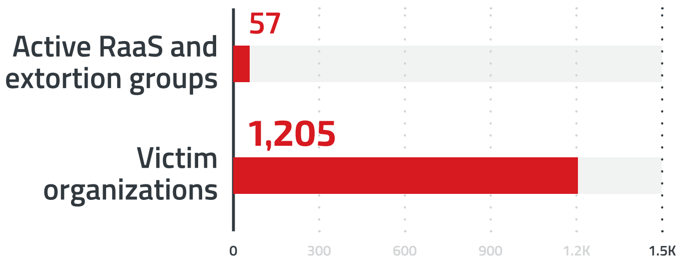


Figure 10. The number of active RaaS and extortion groups and victim organizations of successful ransomware attacks in the first half of 2022

Source: RaaS and extortion groups' leak sites

LockBit, Conti, and BlackCat were the major players in the RaaS field for the first half of 2022.[19] Based on SPN data, we observed a sharp increase in detections from each of these malware families in the first half of this year. Black Cat, a relatively new ransomware that was initially reported at the tail end of 2021, understandably saw practically nonexistent detections in 2021 before the increase in 2022. However, even older ransomware such as LockBit and Conti saw major increases, with LockBit seeing over five times and Conti nearly twice the number of detections in the first half of 2022 in contrast to the first half of the previous year.

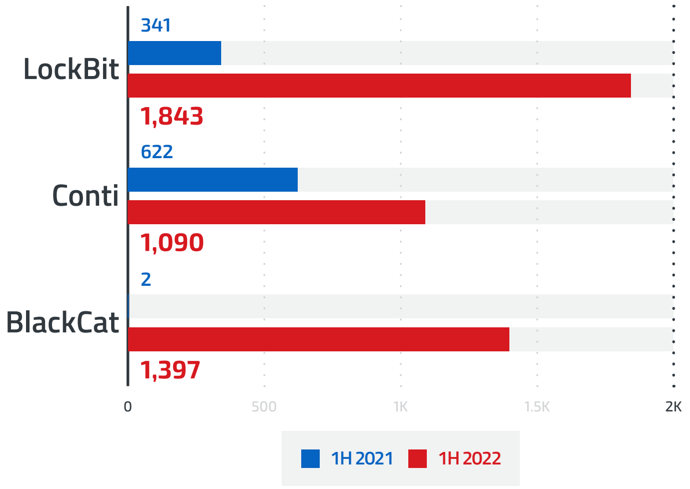


Figure 11. LockBit, Conti, and BlackCat saw a significant increase in detections in the first six months of 2022 compared to the first half of the previous year: The detection numbers for LockBit, Conti, and BlackCat

Source: Trend Micro Smart Protection Network

LockBit, which has been active since 2019 and was initially known as the ABCD ransomware, is the group with the highest number of detections.[20] In 2020, LockBit launched its RaaS affiliate program using a leak site and a few months later began using the double extortion model where the attacker threatens to publicly expose data in addition to encrypting files. In 2021, one of the prominent incidents involving LockBit occurred when it launched an attack on tech services firm Accenture, even going as far as listing the company on its leak site.[21]

LockBit has been a staple in the ransomware scene since its debut, with its operators constantly evolving its capabilities to the point where the performance of its RaaS service has become one of the group's selling points due to its speed and efficiency. LockBit's network has also garnered popularity for its capability and trustworthiness.

LockBit offers multiple options for infection routines depending on the affiliates involved in the operation, their purpose, and how they gain access to their target's system. For example, if an affiliate manages to gain access to a virtual private network (VPN) server using brute-force methods, LockBit's operators might provide an infection routine that is based on remote access service (RAS). On the other hand, the group might offer a PowerShell script to attackers that gain access to a compromised Internet Information Services (IIS) server. In addition to its encryption routines, LockBit attacks were also found to have deployed the post-exploitation tool Mimikatz to gather additional credentials.

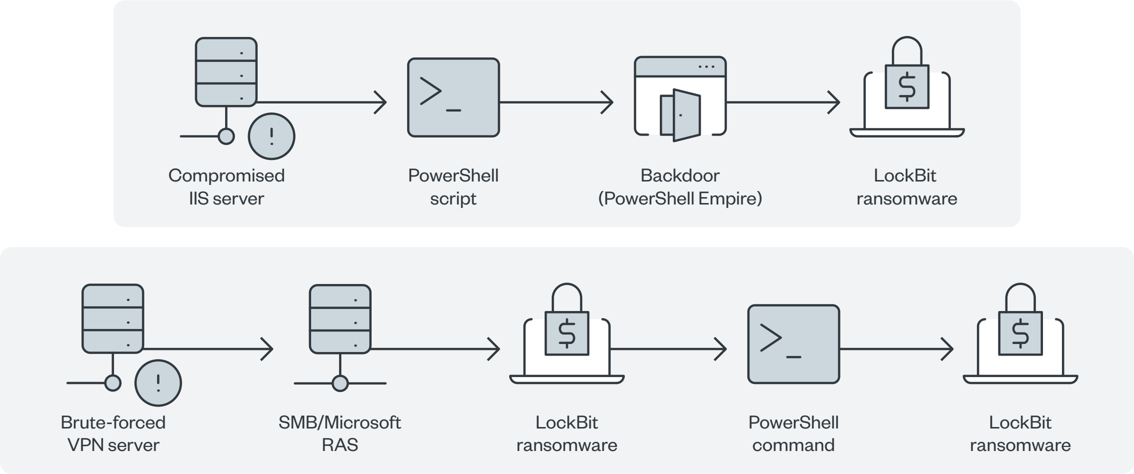


Figure 12. Two of the infection routines used by LockBit: one for when its operators manage to compromise an IIS server, and one for when they manage to compromise a VPN server via brute-force methods

Touted as the successor to the notorious Ryuk ransomware,[22] Conti hit its stride in 2021 with a number of prominent attacks, including incidents where it targeted healthcare institutions in May.[23]

Like many modern ransomware families, Conti employs more than one method to gain initial access to a victim's system. Phishing emails remain a common infiltration technique, with attackers using Google Drive links to drop BazarLoader and the attack eventually leading to an infection. Conti can also arrive on a target's machine by exploiting vulnerabilities like the FortiGate firewall vulnerabilities CVE-2018-13379[24] and CVE-2018-13374,[25] as well as various ProxyShell Microsoft Exchange vulnerabilities.[26]

Once inside the system, tools like Whoami, Nltest, and Net are used to provide the attackers some system information, such as the rights and permissions they have gained via the compromised machine. At the same time, the threat actors actively search for files that they can exfiltrate for use in their double extortion technique. If the attackers that deployed Conti find that they need to have access to greater privileges, they might also use exploits like Zerologon[27] for privilege escalation.

In February 2022, an alleged security researcher leaked some of the ransomware group's files and documents, revealing information such as the size and leadership of the group.[28] More importantly, they unearthed the code used by Conti operators for their components and infrastructure, such as the administrator panel, a decryptor, and even Conti Locker v2.

Nevertheless, the leak of such information is a double-edged sword: While it could be instrumental for researchers to use it for keeping track of and gaining insight into Conti's operation, malicious actors can use the leaked source codes to build their own startup ransomware operation.

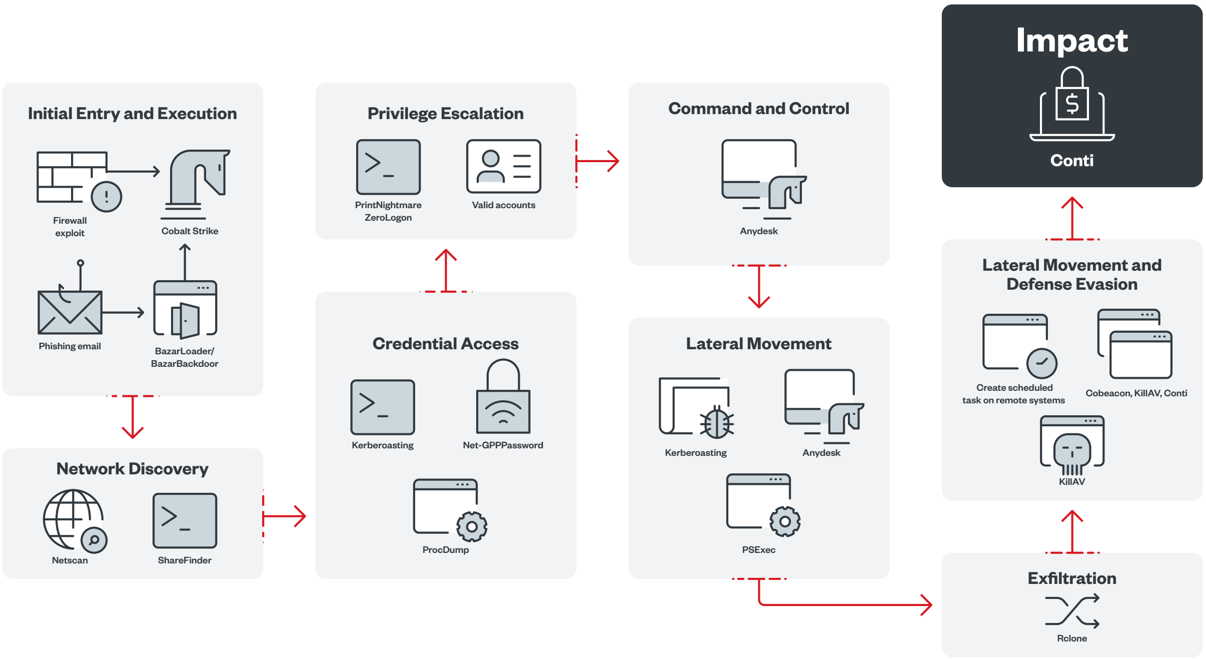


Figure 13. The infection chain used in a typical Conti attack

Although relatively new to the ransomware scene compared to LockBit and Conti, BlackCat still managed to make waves in the months that it was active by going beyond the typical double extortion scheme used by modern ransomware groups. Instead, BlackCat resorted to a "triple extortion" scheme[29] where it not only threatened to encrypt files and leak sensitive data but also warned its victims that it would launch distributed denial-of-service (DDoS) attacks on their infrastructure if the group's demands are not met.[30]

BlackCat's operators typically exploit exposed and vulnerable applications to gain entry into their target system. They then use third-party frameworks and toolsets such as Cobalt Strike to deliver the ransomware.

In April 2022, we launched an investigation into BlackCat via the Trend Micro Vision One™ platform, where we gathered information about its routine. We found that the malicious actors were actively exploiting the Microsoft Exchange Server vulnerability CVE-2021-31207[31] to insert a web shell into the victim's server for remote access. This allows the attackers the ability to remotely perform different tasks like stealing data and dropping malicious tools. The attackers then use these tools to move laterally within the system, scan the environment, and prepare it for eventual BlackCat infection.

Due to BlackCat's sophistication as the first professional ransomware family to be written in Rust, a secure programming language that has concurrent processing capabilities, as well as its unique monetization method, extensive infrastructure, and wide array of supplementary tools in its attacks, it has the potential to become a staple in the RaaS scene in the foreseeable future.

Based on both our data and data from leak sites, we were able to note that these ransomware families are used mainly to target small businesses with up to 200 employees at most as well as medium-sized businesses with up to 1,000 employees. The likely reason for this is that these types of organizations have less resources and a smaller workforce to properly deal with cyberattacks.[32]

Linux Systems Become a Prime Target for Ransomware Operators

Linux systems present an attractive target for malicious actors that are either looking to expand their reach or have decided to concentrate on specific types of infrastructure, such as servers and embedded systems where Linux is expected to see growth over the next few years.[33]

Predictions

Our 2022 security predictions anticipated that ransomware threat actors would expend more effort on targeting servers, server components, and related services.

We observed a 75% increase in ransomware attacks targeting Linux-based machines in the first half of 2022 as opposed to the first half of 2021, lending more evidence to our assumption that malicious actors are focusing more of their efforts on Linux.

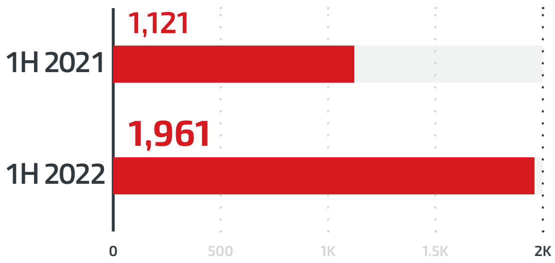


Figure 14. Linux ransomware detections grew significantly in the first half of 2022 as opposed to the first half of 2021: A comparison of ransomware detections for Linux-based machines

Source: Trend Micro Smart Protection Network

The VMware hypervisor ESXi came under heavy fire in the first half of 2022. Still, there is nothing new about cybercriminals targeting ESXi. RansomEXX[34], for example, has been exploiting ESXi vulnerabilities in its campaigns since at least 2021[35] — and it seems that other threat actors are now following suit.

In October 2021, LockBit's operators announced a Linux-based variant, LockBit Linux-ESXi Locker version 1.0, in an underground forum. This variant targets ESXi servers through a combination of Advanced Encryption Standard (AES) and elliptic-curve cryptography (ECC) algorithms to encrypt data. Since then, samples of this variant have been found in the wild.

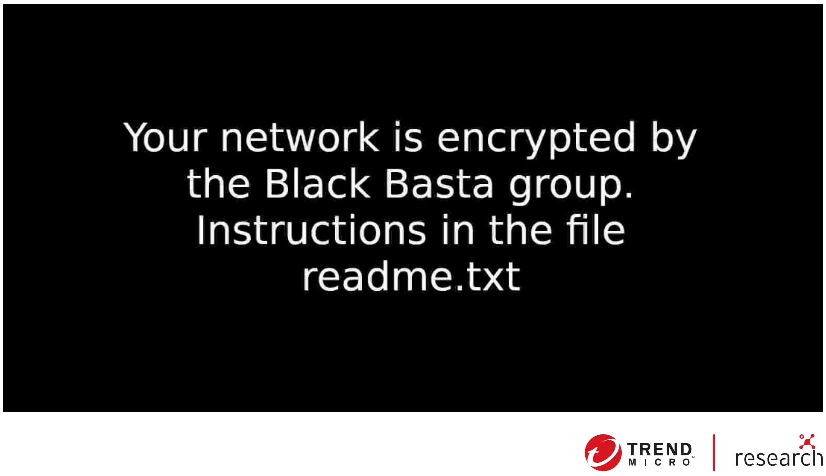
In May 2022, a new ransomware variant named Cheerscrypt was also found targeting devices using ESXi.[36] Based on the source code of the Babuk ransomware that was leaked in September 2021,[37] Cheerscrypt encrypts log files and other VMware-related files using the double extortion technique.

Although neither LockBit Linux-ESXi Locker version 1.0 nor Cheerscrypt deviates from the typical double extortion scheme used by many other ransomware variants, the potential impact of an infection is notable in this case since ESXi servers are widely used by enterprises for server virtualization. Organizations can also use these servers to host multiple virtual machines (VMs) where they keep important data. This means that they are often part of an organization's critical infrastructure, and therefore any successful attack on these components can deal great damage to an organization.

Big Game-Hunting Ransomware Families such as Black Basta and Nokoyawa Hit Organizations Across the Globe

We spotted ransomware operators setting their sights on businesses that have the capacity to pay sizeable ransom demands. Operators of the Black Basta ransomware[38] struck hard and fast, hitting nearly 50 organizations in a span of a couple of months in early 2022.[39] Black Basta originated in April 2022, when a user with the name Black Basta posted on some major underground forums that they were looking for corporate network access credentials for organizations in the United States, Canada, United Kingdom, Australia, and New Zealand. The user also mentioned that they were offering a share of the profits to any potential partners.

Currently, information on the scope and structure of the malicious actor's operation is limited. Given Black Basta's initial advertisement, however, it is likely that the group uses stolen credentials to gain access to its victim's systems. It then proceeds to perform its encryption routine, first by deleting shadow copies via *vssadmin.exe* and then booting the device in safe mode. It then deletes the service called Fax, creates a new one using the malware's path, and adds it to the registry for persistence. Finally, it shuts down and reboots the target's machine in Safe Mode with Networking using the compromised service to encrypt files. One of the notable characteristics of Black Basta is that its ransom note is hard-coded into the malware, suggesting that its operators could be using unique binaries for each of its victims.



Your network is encrypted by
the Black Basta group.
Instructions in the file
readme.txt

Figure 15. The wallpaper created by Black Basta using the .jpg file that is dropped in the %temp% folder

Security researchers also pointed out connections between Black Basta and other ransomware and APT groups. A tweet from the MalwareHunterTeam described many similarities between Black Basta and Conti,[40] while Trend Micro researchers managed to find correlations between Black Basta and QakBot.[41]

In the latter part of 2021, the Hive ransomware initiated a spate of attacks on the US healthcare sector, with some reports stating that over 300 organizations were hit in the ransomware's first hundred days of operation.[42] In 2022, we encountered Nokoyawa, a ransomware with several similarities to Hive.[43] For example, these ransomware families share common tools and techniques, including the use of Cobalt Strike during the arrival phase of the attack and the integration of tools such as the anti-rootkit scanners GMER and PC Hunter as part of defense evasion maneuvers.

However, Hive and Nokoyawa also feature different characteristics, particularly in their code (they use different languages to compile the binary) and packing method: Hive variants are packed using UPX while Nokoyawa does not use any packer whatsoever.

Most of Nokoyawa's targets were in the South American region, particularly in Argentina.

Software Vulnerabilities Threaten to Disrupt the Operations of Businesses

The Number of Critical- and High-Severity Vulnerabilities Increased During the First Half of 2022

The first half of 2022 saw a sizeable jump in the number of vulnerabilities published by CVE.org: 12,380 CVE Records, a sizeable jump from the 9,420 CVE Records that were published during the first half of 2021.[44] The same trend repeated itself in the number of vulnerabilities disclosed via the Trend Micro ZDI program, which published advisories on 944 vulnerabilities, an approximately 23% increase from the 770 vulnerabilities in the first half of 2021.

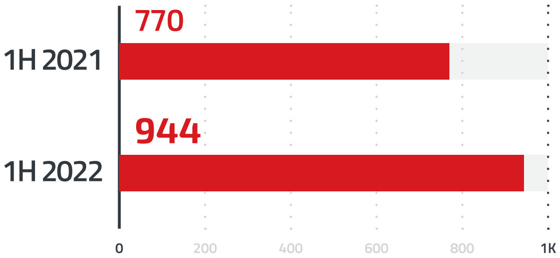


Figure 16. There was an almost 23% increase in the number of vulnerability advisories published in the first half of 2022 compared to the same period in the previous year.

Source: Trend Micro™ Zero Day Initiative™

Vulnerabilities with a high-severity rating made up the greatest portion (68%) of the published vulnerabilities. Both critical- and high-severity vulnerabilities saw large increases, while medium-severity vulnerabilities were the only ones that saw a decrease from the same period in 2021.

Given these trends, we recommend that organizations employ an efficient, risk-based approach that focuses on vulnerabilities affecting their environment, then verify whether these vulnerabilities have public proofs of concept or are being actively exploited in the wild by using resources such as the Known Exploited Vulnerabilities Catalog by the Cybersecurity and Infrastructure Security Agency (CISA).[45]

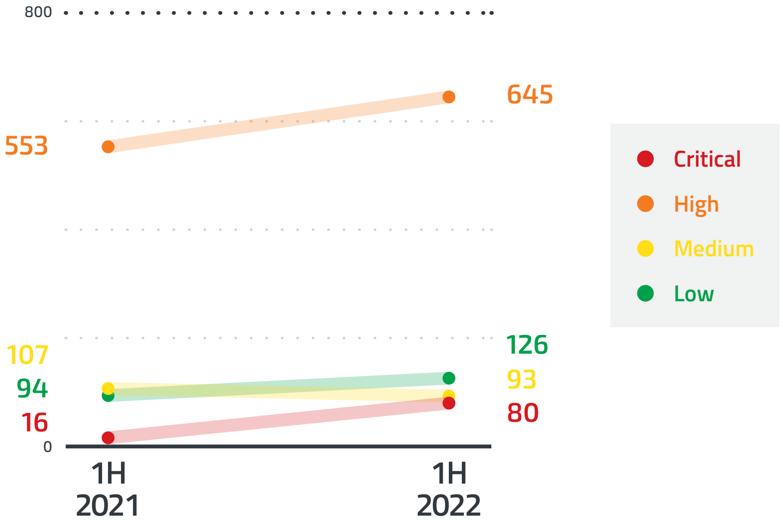


Figure 17. Critical-, high-, and low-severity vulnerabilities saw an increase in the first half of 2022, while medium-severity vulnerabilities experienced a slight dip: The severity breakdown, based on the CVSS, of disclosed vulnerabilities in the first half of 2021 and 2022

Source: Trend Micro ZDI program

CVE-2017-14100,[46] a critical-severity vulnerability that could allow shell command injections if successfully exploited and affects certain versions of Asterisk, an open-source software used to build communications applications, had the highest number of exploit detections in the first half of 2022 based on Trend Micro™ TippingPoint® Threat Protection System sensors. This was followed by the OpenSSL memory leak flaw CVE-2014-3567 and the IIS web server folder traversal vulnerability CVE-2000-0884, which had exploit detections of over 9 and 4 million, respectively. The presence of these older vulnerabilities (with exploit detections numbering in the millions in some cases) among the most exploited bugs in the first half of the year is evidence that many organizations still have difficulty implementing crucial updates to their software. Even worse, it might mean that many organizations still completely ignore such updates.

Meanwhile, CVE-2022-30190 (also known as Follina),[47] a high-severity remote code execution (RCE) vulnerability affecting Microsoft Windows Support Diagnostic Tool (MSDT), has reportedly been used in attacks on high-value targets in European countries and the US.[48] Microsoft has since patched this flaw in its June 2022 security update.[49]

Rule ID	CVE ID number	Hits	Affected products
29739	CVE-2017-14100	15,200,809	Asterisk 11.x before 11.25.2, 13.x before 13.17.1, and 14.x before 14.6.1 and Certified Asterisk 11.x before 11.6-cert17, and 13.x before 13.13-cert5
17056	CVE-2014-3567	9,107,139	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j
1095	CVE-2000-0884	4,447,190	IIS 4.0 and 5.0
3886	CVE-2010-0817	2,597,362	Microsoft SharePoint Server 2007 12.0.0.6421 and possibly earlier and SharePoint Services 3.0 SP1 and SP2.
	CVE-2011-1264		Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1
40693	CVE-2021-35394	1,166,969	Realtek Jungle SDK version v2.x up to v3.4.14B
2023	CVE-2005-1380	711,159	BEA Admin Console 8.1
	CVE-2010-0817		Microsoft SharePoint Server 2007 12.0.0.6421 and possibly earlier and SharePoint Services 3.0 SP1 and SP2
	CVE-2010-3936		Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, 2010 Update 1, and 2010 Update 2
	CVE-2017-0068		Microsoft Edge
10146	CVE-2010-2861	648,690	Adobe ColdFusion 9.0.1 and earlier
	CVE-2013-3336		Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10
31852	CVE-2014-0224	597,386	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
6161	CVE-2008-1451	580,030	Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2
31936	CVE-2018-10562	518,502	Dasan GPON home routers

Table 1. The top vulnerabilities in terms of exploit detections in the first half of 2022

Source: Trend Micro™ TippingPoint® Threat Protection System

Major Vulnerabilities Affect Important Business Tools and Software

Vulnerabilities involving critical software, tools, and components are often some of the most dangerous types of flaws due to the nature of what they affect. Furthermore, data from Vision One shows that approximately 85% of all companies subscribed to the service were exposed to highly exploitable vulnerabilities.

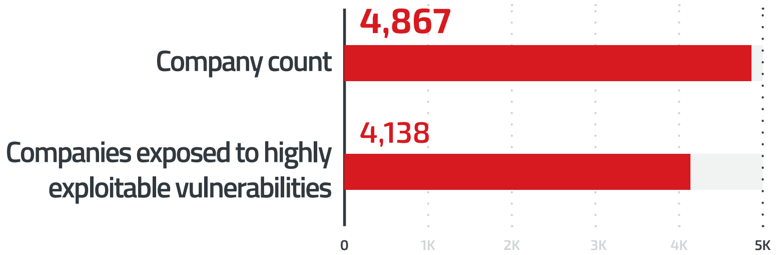


Figure 18. 4,138 out of 4,867 (85%) of all companies subscribed to Vision One were prone to highly exploitable vulnerabilities: A snapshot of Vision One data from the first week of August 2022

2021 saw the rise of CVE-2021-44228 (also known as Log4Shell),[50] a vulnerability that affected the Java-based logging library, Apache Log4j. The disclosure of Log4Shell shook the cybersecurity landscape due to the ubiquity of the software it affected and its integration into different systems, which made it difficult for organizations to determine how they were affected.[51] The first half of 2022 saw more vulnerabilities affecting critical enterprise software, with perhaps the most notable being the Spring4Shell vulnerability.

On March 31, 2022, creators of the Spring Framework, a widespread open-source Java framework commonly used in enterprise applications, published information on CVE-2022-22965,[52] a critical zero-day vulnerability (colloquially known as Spring4Shell due to its similarities to Log4Shell) that affects a number of dependencies, such as setups that run on Spring Framework versions before 5.2.20, 5.3.18, and Java Development Kit (JDK) 9 and higher.

The Spring4Shell vulnerability typically occurs when special objects or classes are exposed to certain conditions. Attackers that want to directly access an object can do so by specifying the class variable in their requests. In addition, access to the child properties of an object via class objects results in attackers being able to gain access to high-value objects in the system by following the chains of properties.[53]

We have seen Spring4Shell being used in attack attempts in the wild as early as April 2022. One of these attack attempts involved the exploitation of the vulnerability to deploy cryptocurrency-mining malware. In this scenario, an attacker first determines the operating system of the targeted machine using a string check. Once the operating system is identified, the encoded payload (a web shell that, when decoded, results in a Spring4Shell web shell) is executed. Afterward, a PowerShell command is executed. This fetches a script designed to download and execute a cryptocurrency miner on the infected machine.[54]

Predictions

In our 2022 Security predictions, we anticipated that threat actors would be able to weaponize exploits in a very short period, launching attacks even before patches can be released.

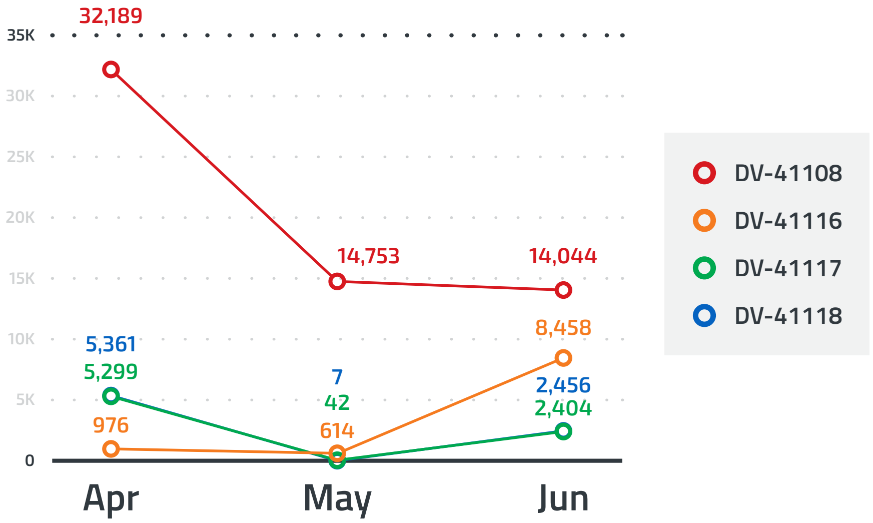


Figure 19. After the disclosure of Spring4Shell on March 31, 2022, the number of exploit detection attempts peaked in April 2022.

Source: Trend Micro TippingPoint Threat Protection System

In February 2022, Trend Micro ZDI published a blog entry that detailed CVE-2021-44142,[55] a vulnerability in Samba, the standard Windows interoperability suite of programs for Linux and Unix, specifically versions of Samba prior to 4.13.17.[56] CVE-2021-44142 exists within the parsing of EA metadata in the Samba server daemon (smbd) when opening a file. An attacker exploiting this vulnerability would thus be able to execute code in the root context even without authentication.

After an earlier version of an out-of-bounds (OOB) vulnerability in the Samba software was disclosed in Pwn2Own Austin 2021, ZDI conducted further research and discovered more variants of the bug, which they then disclosed to Samba's developers. The company subsequently released a patch addressing CVE-2021-44142 and other vulnerabilities on January 31, 2022.[57]

As a standard system service on nearly all Linux distributions, Samba is widely used. Patching CVE-2021-44142 is therefore a must for organizations that use Linux- and Unix-based systems.

Data from Trend Micro™ Deep Security™ (DS) revealed some key insights on customer environments. Log4j-related vulnerabilities (CVE-2021-44228[58] and CVE-2021-45046[59]) had high activity levels in the first half of the year, with over 5 billion combined events being detected and filtered by DS. Overall, CVE-2017-14495,[60] a flaw affecting dnsmasq — a free software that can be configured as a DNS, a DHCP (Dynamic Host Configuration Protocol), and a TFTP (Trivial File Transfer Protocol) server — had the highest number of detected events, which is unsurprising given its popularity and importance to routers and IoT gateways.[61]

The large number of detected events associated with these vulnerabilities further confirms our observation that flaws affecting ubiquitous and essential software will remain a popular choice for exploitation by malicious actors.

Filter ID	Solution	Related CVEs	Detected event counts
1009667	Deep Security	CVE-2017-14495	114,995,958,044
1000853	Deep Security	CVE-2006-4154	5,665,473,527
1011242	Deep Security	CVE-2021-44228	4,794,466,414
1003766	Apex One	CVE-2009-2524	995,700,958
1004398	Deep Security	CVE-2010-2730	967,669,441
1010971	Deep Security	CVE-2021-29441	846,824,548
1006027	Deep Security	CVE-2014-0098	417,996,287
1011456	Deep Security	CVE-2022-26134	381,361,877
1008445	Apex One	CVE-2017-8543	266,267,487
1008713	Apex One	CVE-2017-11815	188,900,588

Table 2. The number of detected vulnerability-related events based on Trend Micro™ Deep Security™ and Trend Micro Apex One™ data in the first six months of 2022

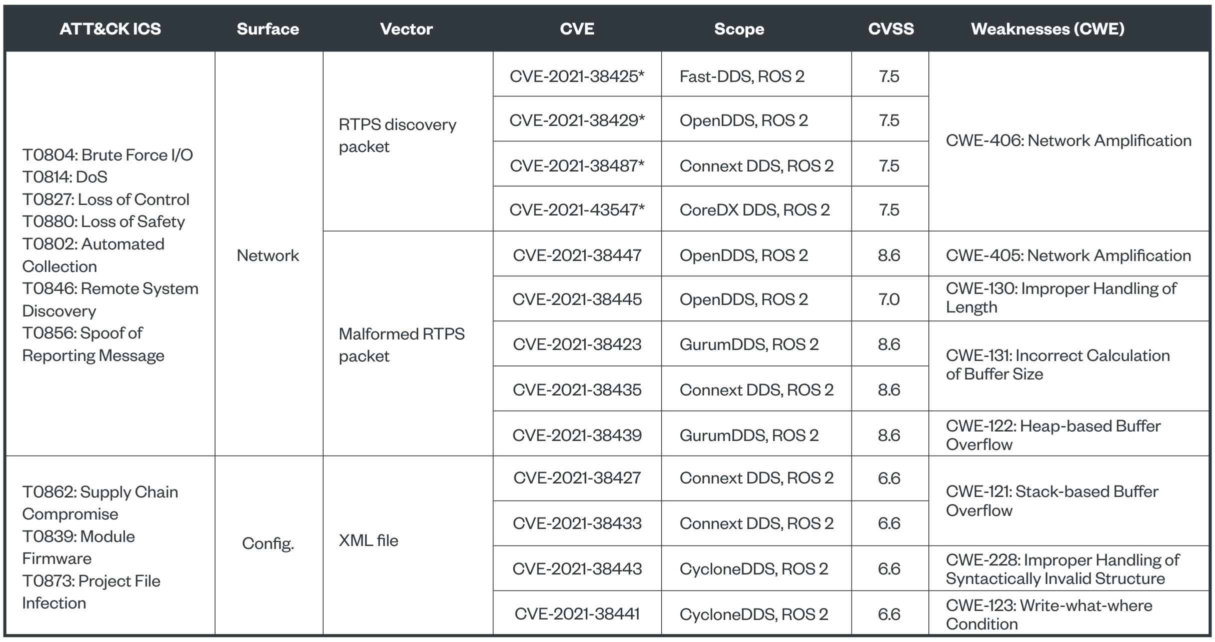
Source: Trend Micro Deep Security and Apex One

Newly Discovered Vulnerabilities Threaten the DDS Standard

The Data Distribution Service (DDS) standard is an example of middleware technology that serves as the connectivity standard for enabling secure real-time information exchange, modular application development, and rapid integration for the industrial internet of things (IIoT).[62] DDS is used to implement a reliable communication layer between sensors, controllers, and actuators in areas such as transportation, robotics, telecommunications, healthcare, and defense, making it a critical type of middleware technology despite not being widely known to the public.

In addition to the importance of DDS in the software supply chain, it's also worth noting that its location at the beginning of the chain makes it easy to lose track of. As a result, malicious actors see DDS as an attractive target. Since it serves as a security-critical building block of the system, the exploitation of a single vulnerability has the potential to leave an impact on the rest of the software stack.

In January 2022, Trend Micro Research, TXOne Networks, and ZDI in collaboration with ADLINK Labs and Alias Robotics published an entry discussing DDS from a cybersecurity perspective. The entry included information on 13 new vulnerabilities for the six most common DDS implementations.[63] These new bugs also affect Robot Operating System 2 (ROS 2), the default operating system for robotics and automation that uses DDS as middleware, meaning that the impact of each vulnerability could affect more than just DDS itself.

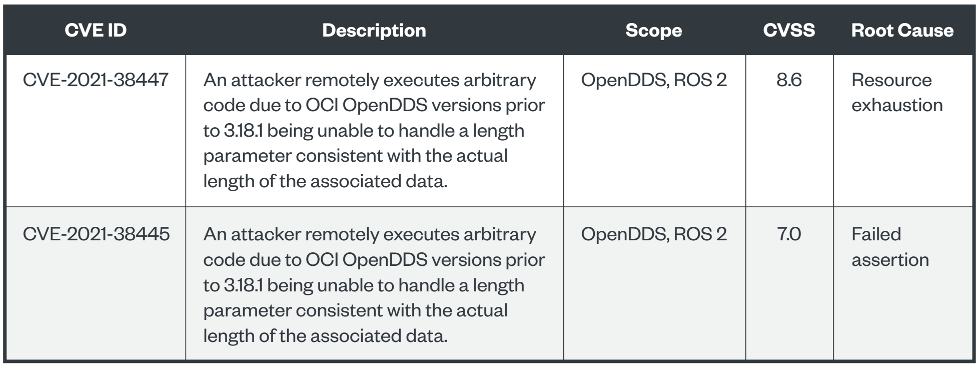


ATT&CK ICS	Surface	Vector	CVE	Scope	CVSS	Weaknesses (CWE)
T0804: Brute Force I/O T0814: DoS T0827: Loss of Control T0880: Loss of Safety T0802: Automated Collection T0846: Remote System Discovery T0856: Spoof of Reporting Message	Network	RTPS discovery packet	CVE-2021-38425*	Fast-DDS, ROS 2	7.5	CWE-406: Network Amplification
			CVE-2021-38429*	OpenDDS, ROS 2	7.5	
			CVE-2021-38487*	Connext DDS, ROS 2	7.5	
			CVE-2021-43547*	CoreDX DDS, ROS 2	7.5	
		Malformed RTPS packet	CVE-2021-38447	OpenDDS, ROS 2	8.6	CWE-405: Network Amplification
			CVE-2021-38445	OpenDDS, ROS 2	7.0	CWE-130: Improper Handling of Length
			CVE-2021-38423	GurumDDS, ROS 2	8.6	CWE-131: Incorrect Calculation of Buffer Size
			CVE-2021-38435	Connext DDS, ROS 2	8.6	
			CVE-2021-38439	GurumDDS, ROS 2	8.6	CWE-122: Heap-based Buffer Overflow
T0862: Supply Chain Compromise T0839: Module Firmware T0873: Project File Infection	Config.	XML file	CVE-2021-38427	Connext DDS, ROS 2	6.6	CWE-121: Stack-based Buffer Overflow
			CVE-2021-38433	Connext DDS, ROS 2	6.6	
			CVE-2021-38443	CycloneDDS, ROS 2	6.6	CWE-228: Improper Handling of Syntactically Invalid Structure
			CVE-2021-38441	CycloneDDS, ROS 2	6.6	CWE-123: Write-what-where Condition

Figure 20. The 13 new DDS vulnerabilities that were discovered via a collaboration between Trend Micro Research, TXOne Networks, and ZDI in partnership with ADLINK Labs and Alias Robotics; the vulnerabilities cover the network and configuration attack surfaces.

The DDS vulnerabilities can be divided into those that affect the network level and those that affect the configuration level. The former can be exploited to implement a variety of malicious techniques such as denial-of-service (DoS) attacks, spoofing, and automated collection, while the latter can be used to target DDS system developers and integrators.

To test how an actual attack might work, our researchers used the Gazebo simulator to create an environment using physics engines to mimic a real-world scenario. Using this setup, we were able to simulate an attack on an autonomous driving platform, thereby crafting a scenario where a malicious actor can exploit CVE-2021-38447[64] and CVE-2021-38445.[65] Upon exploitation, the ROS 2 nodes would either crash or allow the attacker to execute arbitrary code within the system.



CVE ID	Description	Scope	CVSS	Root Cause
CVE-2021-38447	An attacker remotely executes arbitrary code due to OCI OpenDDS versions prior to 3.18.1 being unable to handle a length parameter consistent with the actual length of the associated data.	OpenDDS, ROS 2	8.6	Resource exhaustion
CVE-2021-38445	An attacker remotely executes arbitrary code due to OCI OpenDDS versions prior to 3.18.1 being unable to handle a length parameter consistent with the actual length of the associated data.	OpenDDS, ROS 2	7.0	Failed assertion

Figure 21. Details of how CVE-2021-38447 and CVE-2021-38445 can be exploited to launch an attack on an autonomous driving platform

Notable Vulnerabilities Affecting Non-Windows Operating Systems

Some of the noteworthy vulnerabilities we discovered and analyzed in the first half of 2022 affected platforms other than Windows. In April 2022, we released a blog entry about our discovery and analysis of CVE-2022-22639,[66] a vulnerability in suhelperd, a helper daemon process for the macOS Software Update that contains the class SUHelper. This class is responsible for a critical system service via the inter-process communication (IPC) mechanism. The successful exploitation of CVE-2022-22639 can lead to an attacker gaining root privileges that they can use for malicious attacks.[67] Apple has since patched this bug via the macOS Monterey 12.3 update released in March 2022.[68]

There were also prominent vulnerabilities affecting Linux- and Unix-based operating systems. CVE-2022-0847, also known as Dirty Pipe,[69] is a bug that affects the Linux kernel from versions 5.8 and up. It exploits a flaw in the Linux kernel's memory management, specifically through how pipe page caches are merged and overwrite other page caches.[70] Dirty Pipe, which can potentially allow the elevation of an attacker to root privileges on the host, is relatively easy to exploit. It is therefore vital for organizations to check whether they are using vulnerable versions of the Linux kernel. Upon learning that these are vulnerable, they must then update their systems according to Linux kernel versions 5.16.11, 5.15.25, and 5.10.102 or later.[71]

On the other hand, CVE-2022-29464[72] is a critical RCE vulnerability that affects several products from WSO2, a technology provider that offers open-source platforms for integrating application programming interfaces (APIs), applications, and web services:

- WSO2 API Manager 2.2.0 and above
- Identity Server 5.2.0 and above
- Identity Server Analytics 5.4.0 to 5.6.0
- Identity Server as Key Manager 5.3.0 and above
- Open Banking AM 1.4.0 and above
- Enterprise Integrator 6.2.0 and above

Exploitation of this flaw, which does not require user interaction or administrative privileges, can allow attackers to infiltrate the networks of affected systems.

Since April 2022, we have been seeing CVE-2022-29464 exploit attempts in the wild. These attempts occurred after a proof of concept for the exploit was published in GitHub.[73] Shortly after this was posted, a Metasploit module for affected environments was made available.[74] These exploit attempts involve the installation of Cobalt Strike beacons and other malware as part of the attack routine.[75]

As with the other vulnerabilities discussed in this section, we encourage organizations using affected WSO2 products to update their systems or apply the temporary mitigation recommendations as suggested by their respective security advisories.[76] WSO2 has since released a patch addressing this vulnerability.[77]

Old Issues, Unconventional Attacks Plague Cloud Environments

Cloud-Based Cryptocurrency Mining Attacks From Threat Actors Like TeamTNT and Kinsing Are on the Rise

Cloud technologies have experienced explosive growth over the last decade,[78] with many organizations shifting at least part of their infrastructure to the cloud due to the benefits it provides, such as cost savings, operational resilience, business agility, and automation. This trend is expected to continue in the next few years, with Gartner forecasting that public cloud spending alone will reach nearly US$500 billion in 2022.[79]

Predictions

In our 2022 security predictions, we speculated that cloud attackers would continue to follow technology trends while still using traditional attacks on cloud users.

While widespread adoption of the cloud has made many businesses run more efficiently, it has also made cloud-based systems an attractive target for malicious actors looking to expand the regular scope of their operations.

Although cryptocurrency prices declined sharply during the first half of 2022,[80] schemes built around it do not require high investment costs since typical cryptocurrency-based attacks rely on the victim's infrastructure and resources to mine cryptocurrencies.

Traditionally, the most efficient method of cryptocurrency mining involved the use of expensive machines with powerful GPUs. Other types of cryptocurrency mining, such as CPU-based mining, can also be profitable, but only at scale where sheer numbers can make up for the difference in performance. Since most users do not have high-end graphical powerhouses at their disposal, some groups have begun focusing their efforts on quantity over quality by relying instead on compromising cloud instances for cryptocurrency-mining operations.[81]

In our research into cloud-based cryptocurrency mining, we investigated the primary threat actors that inhabit this space and determined the five most prominent groups and how they conduct their operations:

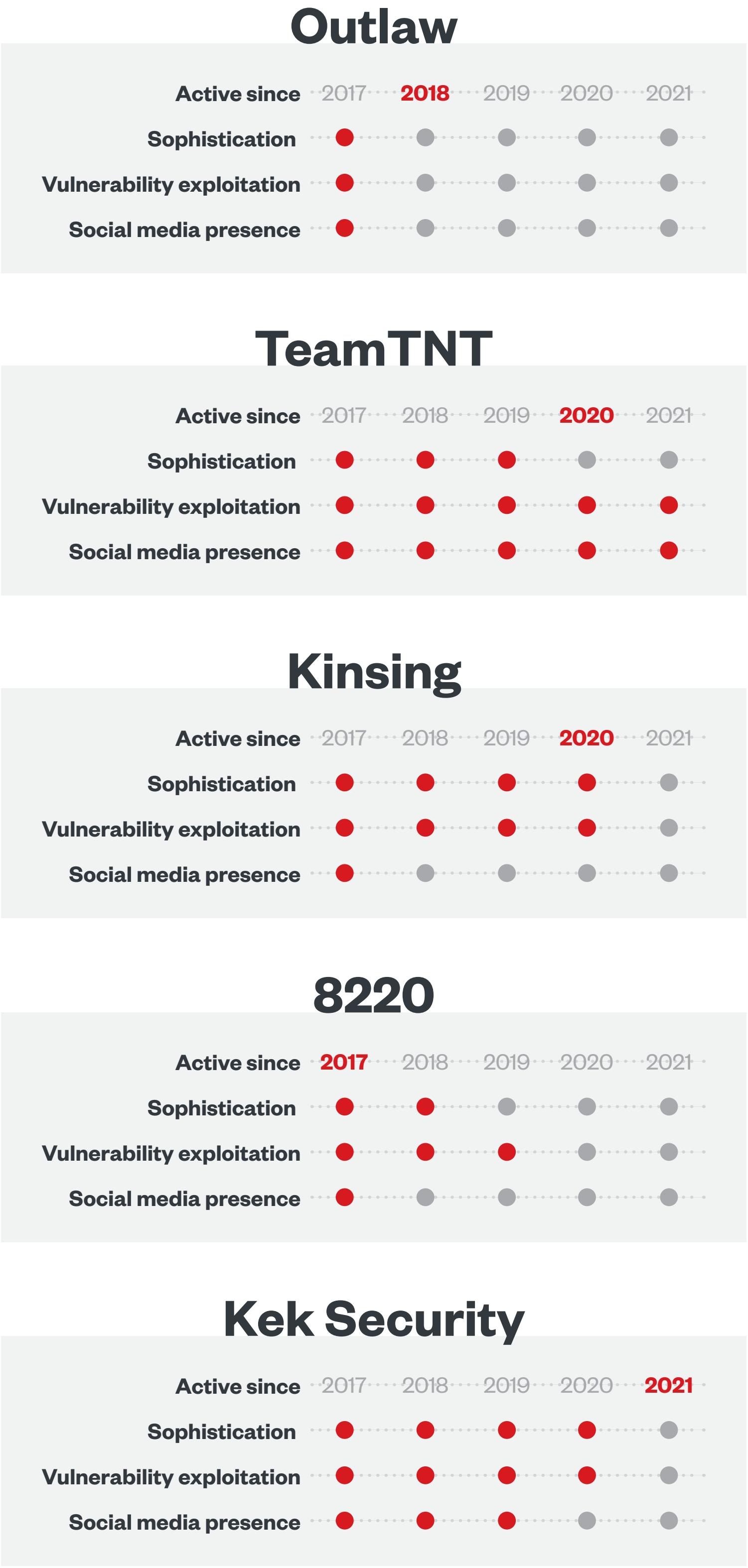
Outlaw is a threat actor that prefers to stick to the tools and techniques it knows, with relatively little change in its operations over the years.[82] Outlaw's preferred targets include IoT devices and Linux cloud servers, which it compromises by exploiting known vulnerabilities or performing brute-force Secure Shell (SSH) attacks.

TeamTNT is a group we've covered extensively over the past couple of years.[83] The threat actor is known for being active in social media, going as far as replying to researchers who have analyzed their attacks. TeamTNT has evolved quickly over a short period, making it one of the most technically proficient threat actors focused on cryptocurrency mining. The group's preferred modus operandi is to exploit vulnerable software to compromise hosts before performing credential theft as a precursor for lateral movement within the victim's system and exploiting misconfigurations.

Kinsing, at least in terms of online presence, can be considered an antithesis to TeamTNT since the group does not maintain any noticeable presence on social media or even in underground forums. However, it shares some similarities with its rival in terms of its ability to quickly adapt and evolve its operational kit.[84] The group is also known for its quick adoption of new exploits, as seen in its use of the Log4Shell vulnerability just a few days after it was first made public.[85]

8220 is a group that has been a frequent exploiter of vulnerabilities, primarily those that affect Oracle WebLogic Server. After a relatively quiet 2020, we observed that the group became much more active in 2021, with approximately 10 times the activity levels in the previous year. The threat actor has also been known to compete with Kinsing for the same resources, with the two often kicking each other out from compromised machines to install their own cryptocurrency miners.

Kek Security is a relatively new group that has been garnering attention due to its sophistication and penchant for integrating new exploits into its attacks. Kek Security is also continuously developing its malware, with some of its more recent additions providing better obfuscation capabilities to evade detection and prevent researcher analysis.



Outlaw

Active since	2017	**2018**	2019	2020	2021
Sophistication	●	○	○	○	○
Vulnerability exploitation	●	○	○	○	○
Social media presence	●	○	○	○	○

TeamTNT

Active since	2017	2018	2019	**2020**	2021
Sophistication	●	●	●	○	○
Vulnerability exploitation	●	●	●	●	●
Social media presence	●	●	●	●	●

Kinsing

Active since	2017	2018	2019	**2020**	2021
Sophistication	●	●	●	●	○
Vulnerability exploitation	●	●	●	●	○
Social media presence	●	○	○	○	○

8220

Active since	**2017**	2018	2019	2020	2021
Sophistication	●	●	○	○	○
Vulnerability exploitation	●	●	●	○	○
Social media presence	●	○	○	○	○

Kek Security

Active since	2017	2018	2019	2020	**2021**
Sophistication	●	●	●	●	○
Vulnerability exploitation	●	●	●	●	○
Social media presence	●	●	●	○	○

Figure 22. A diagram showing the five primary threat actors in the cloud-based cryptocurrency-mining space, how long they have been active, their level of sophistication, social media presence, and tendency to exploit vulnerabilities as part of their routines

Given that all these groups are targeting both common and limited resources, we witnessed multiple instances where different threat actors fought over the same machines, often using kill scripts to deal with competitors. It is this cutthroat competition that drives a large portion of the innovations implemented by the various threat actors. Primarily, these innovations involve adding capabilities that would allow them to target systems that their adversaries cannot.

Malicious Actors Abuse Cloud Tunneling Services for Cloud-Based Attacks

Some of the advantages that cloud technologies provide can likewise present security challenges for organizations. For example, the cloud's ability to swiftly deploy assets and services helps organizations be more efficient; however, it can also prevent them from having full visibility over deployed assets. Attackers can take advantage of this by launching attacks using more unconventional methods in places that IT teams and security staff are less likely to monitor.

We recently observed malicious actors abusing cloud tunnels, a service used by both individuals and businesses to expose their internal systems to the internet by relaying traffic through cloud-based infrastructure. In enterprise settings, these kinds of services are used by developers to test and deploy code, as well as to make certain services available to select users on the internet. In other words, cloud tunneling serves as a convenient tool that allows users to deploy local development services without needing to configure network firewalls and register domain names.

Due to its growing popularity, cloud tunneling services have become a prime target for malicious actors looking to expand their operations. Groups that employ cloud tunneling services normally use them for transitory purposes so that they will not need to maintain permanent infrastructures, as well as to add another layer of secrecy by masking their real locations.[86]

Cloud tunneling threats can be categorized into two distinct types: internal threats and external threats. Internal threats refer to attacks where the service is used (either purposefully or unknowingly) to expose internal services such as Server Message Block (SMB), FTP, and HTTP. On the other hand, external threats involve traditional attacks and routines such as phishing and C&C communication via the cloud tunnel.

In one blog entry in September 2020, we discuss an instance where an insider attack involved the abuse of legitimate tools and services. In particular, a malicious actor used ngrok to expose an SMB port, eventually leading to the download and execution of a keylogger.[87] In contrast, external attacks are more common and usually involve operations that integrate cloud tunneling services for the routing of malware traffic or the hosting of phishing websites.

Cloud Misconfiguration Remains an Issue for Organizations

The growth of the container market, which is estimated to reach US$8.2 billion by 2025, has made it an appealing target for cloud-focused threat actors.[88] While containers can provide organizations an increase in the speed and efficiency of their development cycles, failure to implement proper security controls could result in compromise at various stages of the pipeline, from hijacked repositories to the exploitation of weaknesses in specific components of the container software.[89]

Misconfigured container software remains a significant issue for many organizations. According to a survey from Red Hat encompassing over 300 DevOps, engineering, and security professionals, 53% of the respondents detected a misconfiguration in their container and/or Kubernetes deployment.[90]

We investigated one of the primary misconfiguration issues in Kubernetes deployments, specifically Kubernetes clusters that are publicly exposed via port 10250.[91] The kubelet is an integral part of Kubernetes, and it is responsible for ensuring that all containers are running in a pod and performing functions, such as helping nodes join the Kubernetes cluster, managing the health of containers, and keeping the control updated on node information. Port 10250, which is used by the kubelet API, is typically inaccessible to external services as it is exposed internally.

However, based on Shodan data, we were able to use IP address information and a simple script to send requests to the kubelet API to identify over 240,000 exposed Kubernetes cluster nodes. Although a significant number of these nodes returned HTTP "401 Status Code – Unauthorized," meaning that they were blocking anonymous requests, a skilled malicious actor can still compromise the kubelet authentication token or use other exploits, thereby endangering the clusters. Approximately 600 nodes returned the "200 – OK" notification, resulting in some nodes that are running a kubelet providing information on pods in that specific node. For these exposed nodes, an attacker can install and run programs via the kubelet API.

Meanwhile, Trend Micro Cloud One™ Conformity data shows the tools and services with the highest levels of service misconfiguration rates (based on total checks) from Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). In particular, Azure's activity log service had high misconfiguration rates and was associated with a high number of high-risk rules (based on Conformity risk level rating).

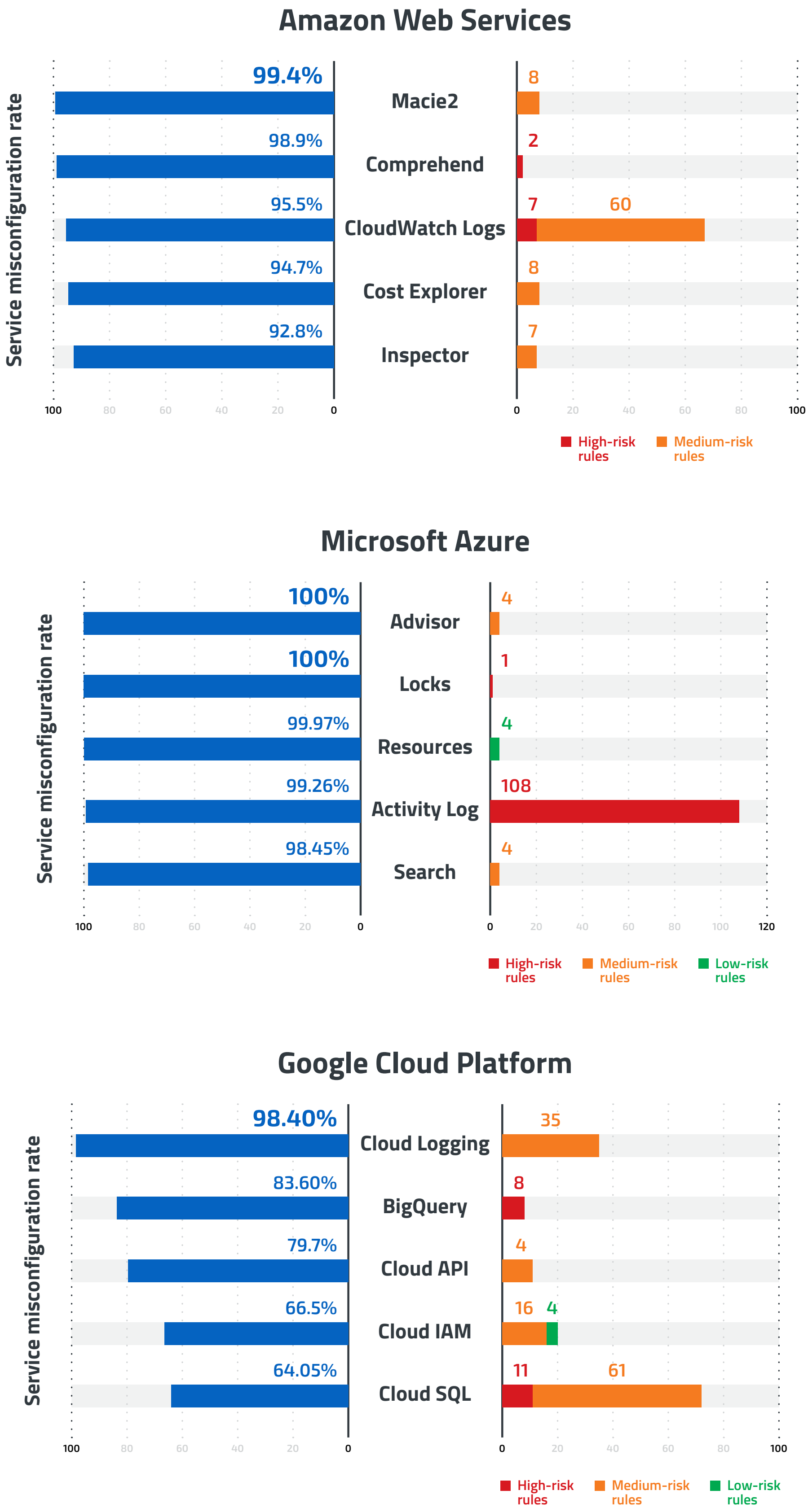


Figure 23. The top five services with the highest levels of misconfiguration rates (based on total checks) from Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)

The Evolving Attack Surface Requires Effective Multilayered Defenses and Security Technologies

If there is anything we can glean from the current state of cybersecurity, it's that the growth of the digital attack surface has organizations scrambling to fill as many security gaps as they can. After two years of remote work, some employees have started to shift back in some capacity to their on-site workplaces, while others have adopted a hybrid arrangement. These varying configurations in working environments, together with the growing number of technologies that are being integrated into business operations, are a call for organizations to allocate additional resources to cover as much of the attack surface as possible.

Over time, threat actors have become more dangerous, launching attacks that have grown in both scale and sophistication. It comes as no surprise, therefore, that threat actors now exploit multiple sections of the attack surface in a single campaign: After all, the rising popularity of service-based malware has made it easier for cybercriminals to launch attacks and for malware developers to hide their tracks.

The evolution of ransomware from the more innocuous attacks of yesteryear to the double — and even triple — extortion schemes of today means that defending systems against modern ransomware families cannot be viewed as anything less than top priority. In the same vein, widespread technologies such as cloud services, where organizations do not physically control the infrastructure, must still rely on the shared responsibility model for effective security.[92]

The first step in attack surface management (ASM) is the discovery of the attack surface itself, where organizations examine their assets and determine elements such as the critical importance of an asset, any potential vulnerabilities, the level of threat activity, and how much threat intelligence is being gathered from their assets. Assessing available security controls and how they offset risks is also an important preliminary step in planning an organization's ASM.

One integral component of ASM is visibility, as it provides valuable information on potential threats. In turn, this can help enterprises determine their risk exposure and allow them to take the necessary steps to mitigate these risks.[93]

Proper security protocols and best practices go a long way toward helping businesses protect their system from attacks. Organizations should prioritize updating their software as soon as possible to minimize the chance of attackers successfully exploiting vulnerabilities in their system. Other options, such as virtual patching, can help organizations protect their machines while they wait for vendors to provide security updates. Cloud users, meanwhile, should ensure that their cloud infrastructure is set up properly with appropriate security protocols in place to prevent attackers from capitalizing on misconfigurations. User education is also a key part of a successful security posture since end users often serve as the weakest links that malicious actors try to exploit to gain access to other parts of an organization's system.

However, the complex reality of securing infrastructure, systems, and endpoints means that even with these in place, securing each possible point of attack would still be challenging without the right security tools in place.

While there are technologies that can individually handle security for different parts of a system, these also come with their own drawbacks, such as the inability to correlate different data points from each siloed source. Security teams are thus limited to working with only pieces of the puzzle at a time when trying to determine how an attack happened and where it came from.

A single platform that can cover the entire attack surface is the ideal solution for organizations, especially those with limited resources. With a comprehensive platform, organizations stand to gain complete visibility over their attack surface, not to mention the ability to correlate different indicators so that they can focus on the bigger picture. A unified security platform can also provide multilayered protection while helping reduce expenditures that would otherwise be spent on multiple security technologies.[94] Lastly, to minimize potential security gaps, this platform must be configurable and capable of providing continuous protection of digital assets to minimize potential security gaps.

The Threat Landscape in Brief

In the first half of 2022, the Trend Micro Smart Protection Network protected users from more than 63 billion threats consisting of email threats, mobile app threats, IoT threats, network threats, malicious files, and malicious URLs.

63,789,373,773

Blocked threats

2,911,929,067,913

Overall queries

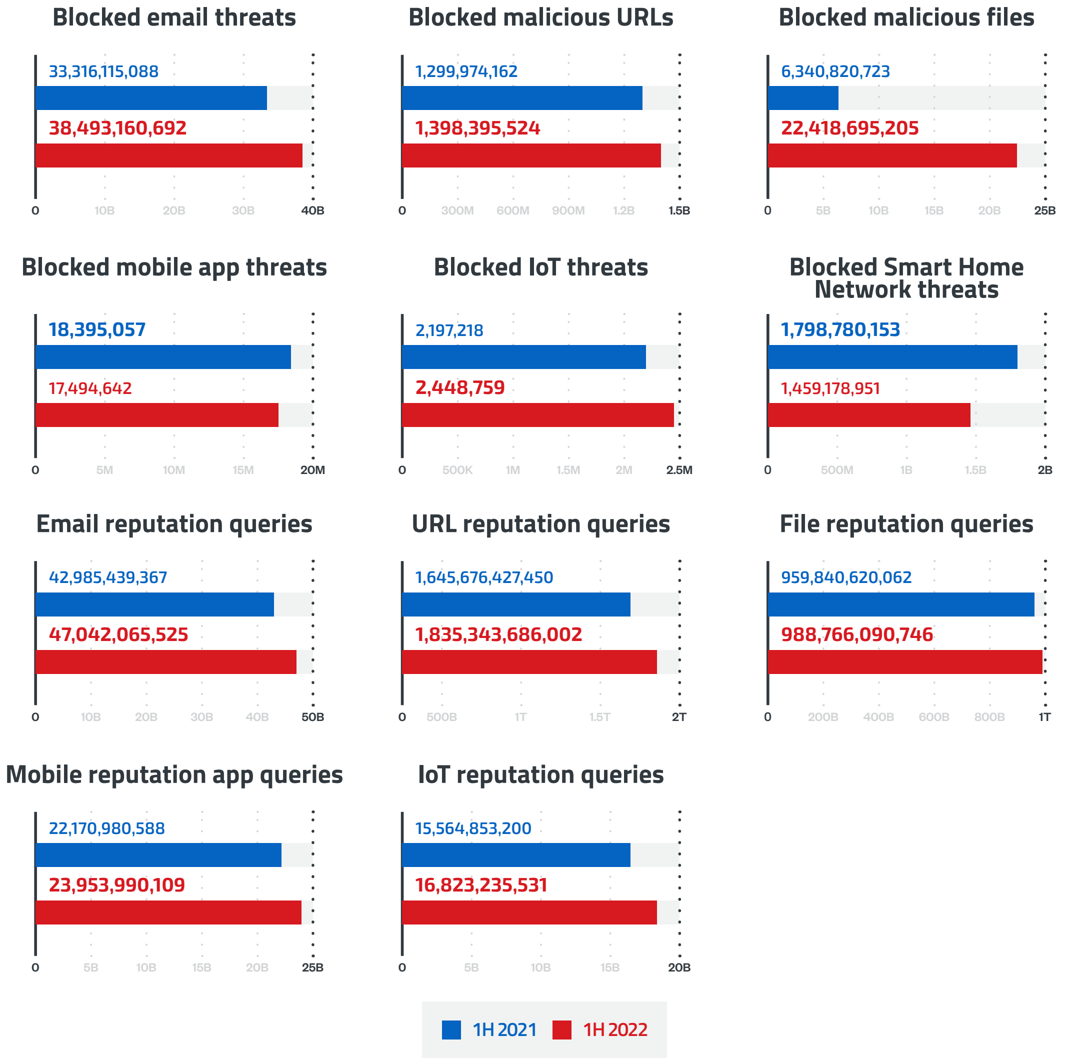


Figure 24. There was an increase in every metric for blocked threats and reputation queries in the first half of 2021 compared to the first half of 2022 based on blocked email, file, and URL threat data and queries in the first half of each year. The number of blocked malicious files also saw a significant increase.

Source: Trend Micro Smart Protection Network

The number of blocked malicious files has been seeing an upward trend since 2020: From just over 1 billion blocked files in the first half of 2020, this number has increased to over 22 billion by mid-2022. In addition to improvements in the Smart Protection Network's feedback mechanism during this period, we believe that both the pandemic and the shift to remote and hybrid work setups also contributed to this growth in detections.

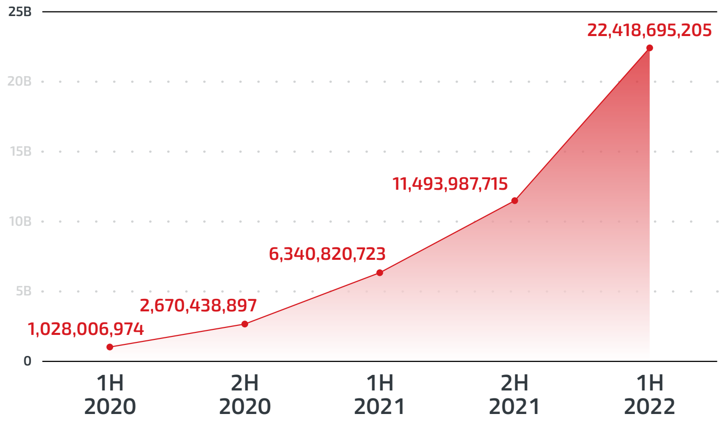


Figure 25. There has been a steady increase in the number of blocked files since the start of 2020, which has doubled approximately each half-year since.

Source: Trend Micro Smart Protection Network

Web shells were the top malware family in terms of detections in the first half of 2022, followed by Emotet, which had a resurgence this year. Cryptocurrency miners had the third highest number of detections, with the Ulise and Powload trojans rounding up the top five.

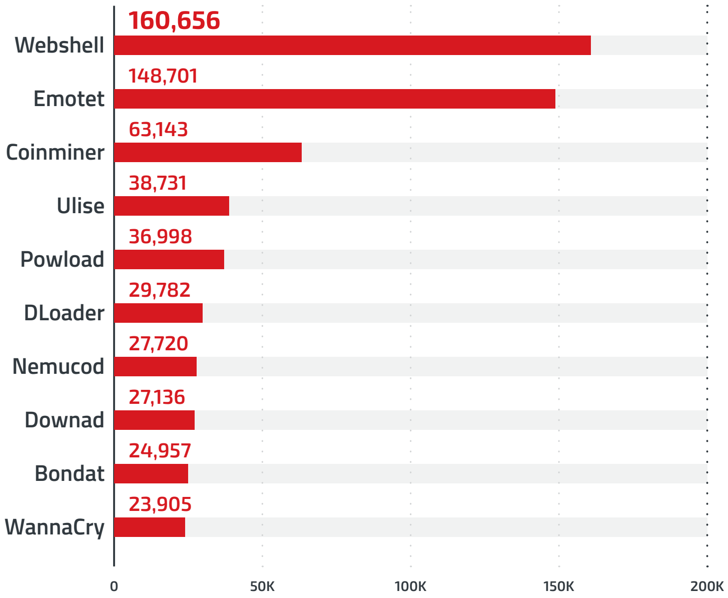


Figure 26. The top 10 malware families in terms of detections in the first half of 2022

Source: Trend Micro Smart Protection Network

Trend Micro Smart Protection Network data reveals that government, manufacturing, and healthcare remained the industries with the highest number of malware detections in the first half 2022. Still, there were some changes at the top, with government targets overtaking the manufacturing industry and the technology sector replacing banking in the top five.

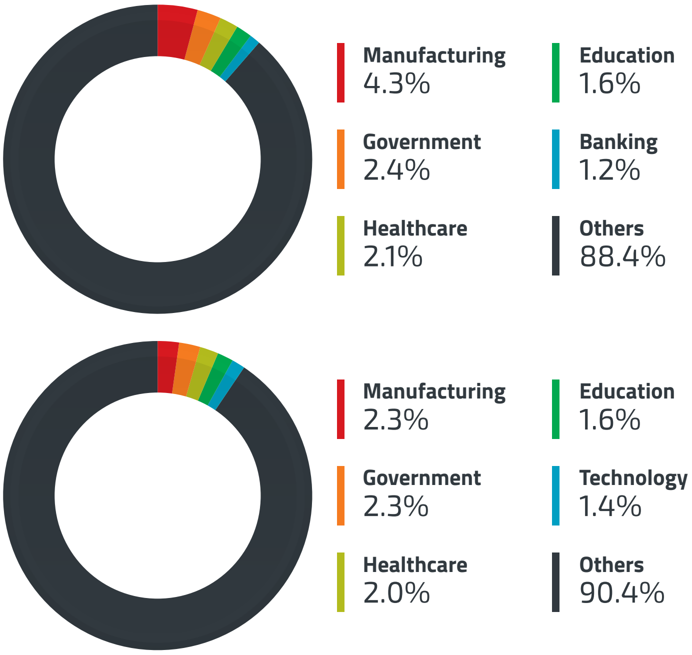


Figure 27. A comparison of the top five industries with the highest number of malware detections in the first half of 2021 and 2022

Source: Trend Micro Smart Protection Network

We detected significantly fewer new ransomware families in the first half of 2022 vis-à-vis the first half of the previous year. However, there were still some noteworthy new ransomware families, such as Cheerscrypt, that made their debut this year. It's also possible that other ransomware operators are starting to turn toward RaaS and other similar operations instead of developing their own families.

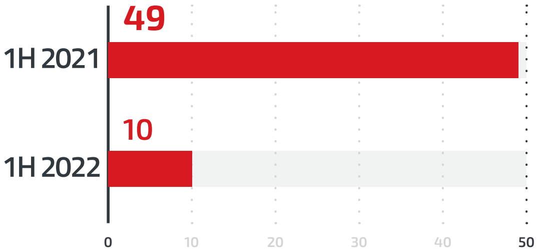


Figure 28. A half-year comparison of the detections of new ransomware families

Source: Trend Micro Smart Protection Network

Jan	Feb	Mar	Apr	May	Jun
No new families	No new families	Explus	Cheerscrypt	Keversen	ZagreuS
		NoEscape		StorageCrypt	Lorenz
				Palang	EvilNominatus
				Blaze	

Table 3. In the first half of 2022, only 10 new ransomware families were discovered, with no new ransomware families in January and February: New ransomware families in the first six months of 2022

The Fortinet path traversal vulnerability CVE-2018-13379,[95] which occurs in Fortinet's FortiGate SSL, was the top VPN flaw during the first half of the year, peaking in June with over 90,000 exploit attempts. Meanwhile, CVE-2021-22986,[96] a bug affecting the iControl REST Interface of the F5 software, had the highest individual month in terms of exploit attempts with over 100,000 detections in June 2022.

	CVE	Digital Vaccine filter	Jan	Feb	Mar	Apr	May	Jun	Total
Fortinet	CVE-2018-13379	DV-36087	21,710	21,733	26,405	25,077	32,590	90,700	218,215
Pulse Secure	CVE-2019-11510	DV-36089	8,708	8,204	10,110	14,950	16,226	48,098	106,296
		DV-36241	506	775	1,940	1,483	1,800	1,765	8,269
	CVE-2019-11539	DV-36095	0	0	0	0	30	0	30
	CVE-2021-22893	DV-39636	0	0	0	3	1	2	6
Citrix Systems	CVE-2019-19781	DV-36876	1,120	684	2,068	1,134	1,770	3,361	10,137
		DV-36927	27	15	60	67	76	43	288
Palo Alto	CVE-2019-1579	DV-38230	0	0	0	0	0	0	0
F5	CVE-2020-5902	DV-37841	19,339	17,581	34,507	24,881	36,079	62,302	194,689
		DV-38276 (Malware)	0	0	0	0	0	0	0
	CVE-2021-22986	DV-39360	1,320	2,503	1,481	91	12	39	5,446
		DV-39352	173	446	313	303	394	241	1,870
		DV-39364	3,126	3,419	3,418	3,884	54,692	105,075	173,614
SonicWall	CVE-2021-20016	DV-39727 (Malware)	0	0	0	0	0	0	0
		DV-41488	0	0	0	0	0	0	0
Cisco	CVE-2021-1609	None	0	0	0	0	0	0	0
	CVE-2021-1610	None	0	0	0	0	0	0	0

Table 4. A monthly comparison of detected attempts to exploit notable VPN vulnerabilities in the first half of 2022

Sources: Trend Micro TippingPoint Threat Protection System, Japan's Information-Technology Promotion Agency (IPA), and the Japan Computer Emergency Response Team (JPCERT) Coordination Center

There was an 11.4% increase in blocked IoT threats for the first half of 2022 compared to the first half of the previous year, indicating that malicious actors focusing on IoT were more active with their campaigns during this period.

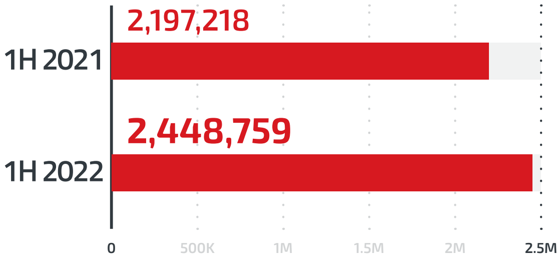


Figure 29. The number of blocked IoT threats increased by 11.4%: A comparison of blocked IoT threats in the first half of 2022 compared to the first half of 2021

Source: Trend Micro Smart Protection Network

One of the noteworthy incidents involving IoT platforms occurred when a variant of a modular botnet called Cyclops Blink, previously linked to the Sandworm APT group,[97] was found to have targeted Asus routers using a specially designed module that can access an infected device's flash memory, which allowed it to retrieve information and even survive system resets.[98] Although Cyclops Blink, which had previously attempted to launch attacks on WatchGuard Firebox,[99] is regarded as a state-sponsored botnet, our research revealed that the targeted devices were not necessarily part of critical infrastructure or industries. It is therefore likely that the attempted attacks on Asus routers were part of its operator's attempts to expand its infrastructure for future attacks on higher-value targets. Asus has since released a security bulletin that offers firmware updates for affected devices.[100]

Upon looking at trends in recent years, we have observed a steady dip in cryptocurrency miner detections, which peaked in 2018. The first half of 2022, for example, saw a noticeable decrease from the previous two half-years. One possible reason for this dip is the crash in cryptocurrency prices midyear due to various external issues.[101] It is likely that this led to cybercriminals' reduced interest in cryptocurrency-mining schemes.

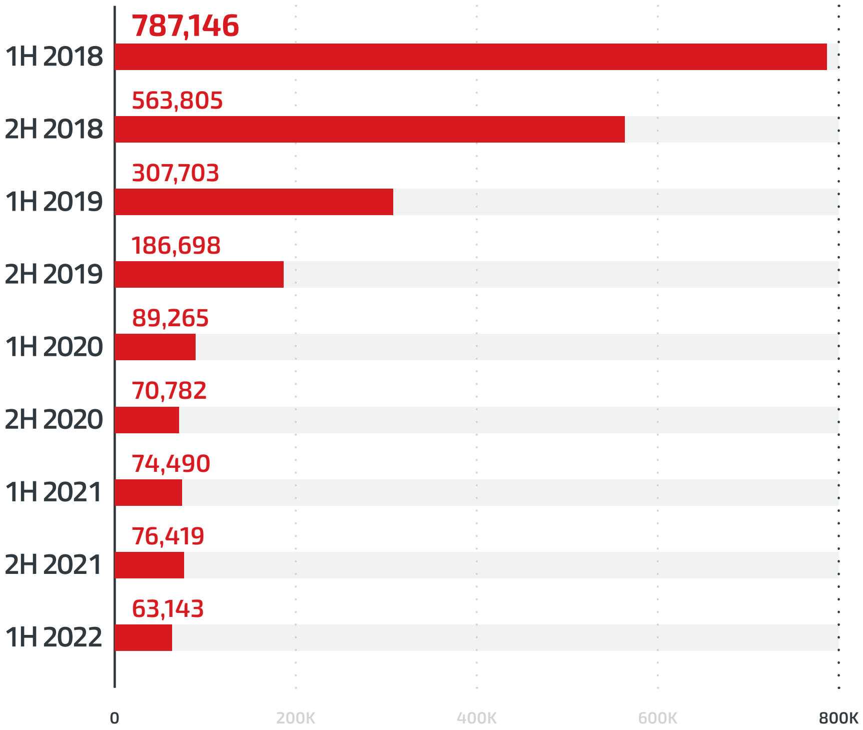


Figure 30. A comparison of cryptocurrency miner detections from the first half of 2021 to the first half of 2022

Source: Trend Micro Smart Protection Network

However, cryptocurrency-mining malware has been seeing growth in Linux operating systems. Halfway through 2022, we observed an approximately 145% increase in detections for Linux-based cryptocurrency miners as opposed to the same period in 2021.

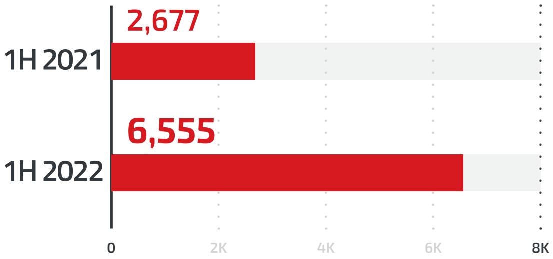


Figure 31. A half-year comparison of the number of detections for Linux-based cryptocurrency miners showing a 145% growth

Source: Trend Micro Smart Protection Network

We observed certain cryptocurrency malware-related trends during the first half of 2022.[102] For example, the rise of new technologies such as non-fungible tokens (NFTs) has made them prime targets for scammers. Some of the scams we observed involving NFTs include using fake NFT trader domains that are designed to trick users into connecting their wallets to fraudulent sites to open the way for further attacks. We also found examples of NFTs with phishing links in the description being airdropped to unwary users — again to trick them into connecting their wallets.

Another trend we recently spotted is the use of Telegram as an avenue for launching cryptocurrency scams. In one scenario, malicious actors disguised themselves as technical support representatives in a chat group, offering to help cryptocurrency users with their concerns. These fake representatives then tried to convince the victim to visit phishing sites that are designed to steal mnemonic seed phrases — a series of unrelated words that are generated when a cryptocurrency wallet is created — and private keys. We also discovered similar scenarios involving Telegram chat groups, where the group owners pretended to be legitimate chat group administrators to trick users interested in cryptocurrencies into visiting scam web pages.

Our data shows a slight decrease (4.9%) in mobile device-related malicious samples in the first half of 2022 as opposed to the first half of 2021.

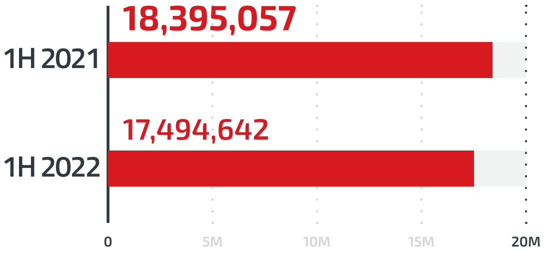


Figure 32. A half-year comparison of the detections of mobile device-related malicious samples

Source: Trend Micro Mobile App Reputation Service

As for notable mobile malware-related incidents, we discovered malicious actors publishing fake mobile apps disguised as cryptocurrency-mining software designed to lure users into either subscribing for paid services or selecting ads offering phony cryptocurrency earnings.[103] Upon further analysis, we found that one of these apps loaded a bogus website asking users to enter their private keys and mnemonic phrases, which would then be collected for future use.

References

1 Trend Micro. (2022). *Trend Micro*. "Mapping the Digital Attack Surface: Why global organisations are struggling to manage cyber risk." Accessed on July 22, 2022, at https://www.trendmicro.com/explore/trend_global_risk_research_2/the-challenge-of-man?_ga=2.73724434.1298314925.1653919723-176640189.1651078671.

2 Joseph C Chen et al. (Jan. 17, 2022). *Trend Micro*. "Delving Deep: An Analysis of Earth Lusca's Operations." Accessed on July 22, 2022, at https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf.

3 Daniel Lunghi and Jaromir Horejsi. (April 27, 2022). *Trend Micro*. "Operation Earth Berberoka: An Analysis of a Multivector and Multiplatform APT Campaign Targeting Online Gambling Sites." Accessed on July 22, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf.

4 Aliakbar Zahravi and Leandro Froes. (May 5, 2022). *Trend Micro*. "NetDooka Framework Distributed via PrivateLoader Malware as Part of Pay-Per-Install Service." Accessed on July 22, 2022, at https://www.trendmicro.com/en_us/research/22/e/netdooka-framework-distributed-via-privateloader-ppi.html.

5 Intel471. (Feb. 8, 2022). *Intel471*. "PrivateLoader: The first step in many malware schemes." Accessed on July 22, 2022, at https://intel471.com/blog/privateloader-malware.

6 Trend Micro. (Dec. 7, 2022). *Trend Micro*. "Toward a New Momentum: Trend Micro Security Predictions for 2022." Accessed on July 22, 2022, at https://documents.trendmicro.com/assets/rpt/rpt-toward-a-new-momentum-trend-micro-security-predictions-for-2022.pdf.

7 Europol. (n.d.). *Europol*. "World's most dangerous malware EMOTET disrupted through global action." Accessed on July 22, 2022, at https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

8 Trend Micro. (Dec. 7, 2021). *Trend Micro*. "Malware Awareness – EMOTET resurges with new detections." Accessed on July 22, 2022, at https://success.trendmicro.com/dcx/s/solution/1118391-malware-awareness-emotet-resurgence?language=en_US&_ga=2.30145279.1991401181.1657506653-177026311.1643353537.

9 Yelisey Boguslavskiy and Vitali Kremez. (Dec. 10, 2021). *Advintel*. "Corporate Loader 'Emotet': History of 'X' Project Return for Ransomware." Accessed on July 25, 2022, at https://www.advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware.

10 Adolph Christian Silverio et al. (May 19, 2022). *Trend Micro*. "Bruised but Not Broken: The Resurgence of the Emotet Botnet Malware." Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/e/bruised-but-not-broken--the-resurgence-of-the-emotet-botnet-malw.html.

11 Trend Micro. (March 3, 2022). *Trend Micro*. "Cyberattacks are Prominent in the Russia-Ukraine Conflict." Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html.

12 Trustwave. (April 29, 2022). *Trustwave*. "Stormous: The Pro-Russian, Clout Hungry Ransomware Gang Targets the US and Ukraine." Accessed on July 25, 2022, at https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/stormous-the-pro-russian-clout-hungry-ransomware-gang-targets-the-us-and-ukraine/.

13 Palo Alto Networks. (Feb. 25, 2022). *Unit 42*. "Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot." Accessed on July 25, 2022, at https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/.

14 Trend Micro. (March 3, 2022). *Trend Micro*. "Cyberattacks are Prominent in the Russia-Ukraine Conflict." Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html.

15 Trend Micro. (n.d.). *Trend Micro*. "Apache Log4j (Log4Shell) Vulnerability." Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/apache-log4j-vulnerability.html.

16 Carmella Chirinos. (April 12, 2022). *Trend Micro*. "Anonymous vows to continue cyber war against Putin's Russia until aggression in Ukraine stops." Accessed on July 28, 2022, at https://fortune.com/2022/04/11/anonymous-cyber-war-russia-ukraine/.

17 Miguel Carlo Ang and Earle Maui Earnshaw. (Oct. 25, 2019). *Trend Micro*. “Negasteal/Agent Tesla, Ave Maria Delivered via Malspam.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/19/j/autoit-compiled-negasteal-agent-tesla-ave-maria-delivered-via-malspam.html.

18 Trend Micro. (n.d.). *Trend Micro*. “Ransomware as a Service (RaaS).” Accessed on July 25, 2022, at https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas.

19 Trend Micro. (May 23, 2022). *Trend Micro*. “Lockbit, Conti, and BlackCat, Lead Pack Amid Rise in Active RaaS and Extortion Groups.” Accessed on July 25, 2022, at https://www.trendmicro.com/vinfo/ph/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022.

20 Trend Micro. (Feb. 8, 2022). *Trend Micro*. “Ransomware Spotlight: LockBit.” Accessed on July 25, 2022, at https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit.

21 Lisa Vaas. (Aug. 11, 2021). *Threat Post*. “Accenture Confirms LockBit Ransomware Attack.” Accessed on July 25, 2022, at https://threatpost.com/accenture-lockbit-ransomware-attack/168594/.

22 Trend Micro. (Sept. 24, 2020). *Trend Micro*. “Addressing Threats Like Ryuk via Trend Micro XDR.” Accessed on July 25, 2022, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/addressing-threats-like-ryuk-via-trend-micro-xdr.

23 Radio New Zealand. (May 18, 2021). *Radio New Zealand*. “Waikato hospitals hit by cyber security incident.” Accessed on July 25, 2022, at https://www.rnz.co.nz/news/national/442795/waikato-hospitals-hit-by-cyber-security-incident.

24 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2018-13379.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379.

25 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2018-13374.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13374.

26 Lawrence Abrams. (Sept. 21, 2021). *Bleeping Computer*. “Conti ransomware now hacking Exchange servers with ProxyShell exploits.” Accessed on July 25, 2022, at https://www.bleepingcomputer.com/news/security/conti-ransomware-now-hacking-exchange-servers-with-proxyshell-exploits/.

27 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2020-1472.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472.

28 Monica Buchanan Pitrelli. (April 13, 2022). *CNBC*. “Leaked documents show notorious ransomware group has an HR department, performance reviews and an ‘employee of the month’.” Accessed on July 25, 2022, at https://www.cnbc.com/2022/04/14/conti-ransomware-leak-shows-group-operates-like-normal-tech-company.html.

29 Pierluigi Paganini. (Dec. 10, 2021). *Security Affairs*. “BlackCat ransomware, a very sophisticated malware written in Rust.” Accessed on July 25, 2022, at https://securityaffairs.co/wordpress/125459/cyber-crime/blackcat-ransomware.html.

30 Amanda Tanner et al. (Jan. 27, 2022). *Unit 42*. “Threat Assessment: BlackCat Ransomware.” Accessed on July 25, 2022, at https://unit42.paloaltonetworks.com/blackcat-ransomware/.

31 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2021-31207.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31207.

32 Trend Micro. (May 23, 2022). *Trend Micro*. “Lockbit, Conti, and BlackCat, Lead Pack Amid Rise in Active RaaS and Extortion Groups.” Accessed on July 25, 2022, at https://www.trendmicro.com/vinfo/ph/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022.

33 Fortune Business Insights. (May 2022). *Fortune Business Insights*. “Linux Operating System Market Size, Share & COVID-19 Impact Analysis, By Distribution (Virtual Machines, Servers, and Desktops), By End-use (Commercial/Enterprise and Individual), And Regional Forecast, 2022-2029.” Accessed on July 25, 2022, at https://www.fortunebusinessinsights.com/linux-operating-system-market-103037.

34 Trend Micro. (May 17, 2022). *Trend Micro*. “Ransomware Spotlight: RansomEXX.” Accessed on July 25, 2022, at https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx.

35 Hugh Aver. (March 26, 2021). *Kaspersky*. “Ransomware in a virtual environment.” Accessed on July 25, 2022, at https://www.kaspersky.com/blog/ransomware-in-virtual-environment/39150/.

36 Arianne Dela Cruz et al. (May 25, 2022). *Trend Micro*. “New Linux-Based Ransomware Cheerscrypt Targeting ESXi Devices Linked to Leaked Babuk Source Code.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html.

37 Lawrence Abrams. (Sept. 3, 2021). *Bleeping Computer*. “Babuk ransomware’s full source code leaked on hacker forum.” Accessed on July 25, 2022, at https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/.

38 Ieriz Nicolle Gonzalez. (May 9, 2022). *Trend Micro*. “Examining the Black Basta Ransomware’s Infection Routine.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html.

39 Cybereason Nocturnus. (June 24, 2022). *Cybereason*. “Cybereason vs. Black Basta Ransomware.” Accessed on July 25, 2022, at https://www.cybereason.com/blog/cybereason-vs.-black-basta-ransomware.

40 MalwareHunterTeam. (April 27, 2022, 9:04 p.m.) *Twitter*. “So this Black Basta ransomware…” Accessed on July 25, 2022, at https://twitter.com/malwrhunterteam/status/1519301421958578177.

41 Ieriz Nicolle Gonzalez. (May 9, 2022). *Trend Micro*. “Examining the Black Basta Ransomware’s Infection Routine.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html.

42 HHS Cybersecurity Program. (April 18, 2022). *HHS Cybersecurity Program*. “Hive Ransomware.” Accessed on July 25, 2022, at https://www.hhs.gov/sites/default/files/hive-ransomware-analyst-note-tlpwhite.pdf.

43 Don Ovid Ladores et al. (March 9, 2022). *Trend Micro*. “New Nokoyawa Ransomware Possibly Related to Hive.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html.

44 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “Metrics.” Accessed on Aug. 10, 2022, at https://www.cve.org/About/Metrics#PublishedCVERecords.

45 Cybersecurity & Infrastructure Security Agency. (n.d.). *Cybersecurity & Infrastructure Security Agency*. “Known Exploited Vulnerabilities Catalog.” Accessed on July 28, 2022, at https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

46 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2017-14100.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14100.

47 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE- CVE-2022-30190.” Accessed on Aug. 23, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190.

48 Carly Page. (June 1, 2022). *Tech Crunch*. “China-backed hackers are exploiting unpatched Microsoft zero-day.” Accessed on (Aug. 23, 2022), at https://techcrunch.com/2022/06/01/china-backed-hackers-are-exploiting-unpatched-microsoft-zero-day/.

49 Dustin Childs. (June 14, 2022). *Zero Day Initiative*. “The June 2022 Security Update Review.” Accessed on (Aug. 23, 2022), at https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022-security-update-review.

50 Trend Micro. (n.d.). *Trend Micro*. “Apache Log4j (Log4Shell) Vulnerability.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/apache-log4j-vulnerability.html.

51 Brian Barrett. (Dec. 16, 2021). *Wired*. “The Next Wave of Log4J Attacks Will Be Brutal.” Accessed on July 25, 2022, at https://www.wired.com/story/log4j-log4shell-vulnerability-ransomware-second-wave/.

52 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2022-22965.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965.

53 Deep Patel et al. (April 8, 2022). *Trend Micro*. “CVE-2022-22965: Analyzing the Exploitation of Spring4Shell Vulnerability in Weaponizing and Executing the Mirai Botnet Malware.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_ph/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html.

54 Nitesh Surana and Ashish Verma. (April 20, 2022). *Trend Micro*. “Analyzing Attempts to Exploit the Spring4Shell Vulnerability CVE-2022-22965 to Deploy Cryptocurrency Miners.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/d/spring4shell-exploited-to-deploy-cryptocurrency-miners.html.

55 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2021-44142.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44142.

56 Zero Day Initiative. (Feb. 1, 2022). *Zero Day Initiative*. “CVE-2021-44142: Details on a Samba Code Execution Bug Demonstrated at PWN2OWN Austin.” Accessed on July 25, 2022, at https://www.zerodayinitiative.com/blog/2022/2/1/cve-2021-44142-details-on-a-samba-code-execution-bug-demonstrated-at-pwn2own-austin.

57 Samba. (n.d.). *Samba*. “Samba Security Releases.” Accessed on July 25, 2022, at https://www.samba.org/samba/history/security.html.

58 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2021-44228.” Accessed on Aug. 1, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228.

59 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2021-45046.” Accessed on Aug. 1, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046.

60 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2017-14495.” Accessed on Aug. 1, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14495.

61 Federico Maggi. (Oct. 9, 2017). *Trend Micro*. “Dnsmasq: A Reality Check and Remediation Practices.” Accessed on Aug. 1, 2022, at https://www.trendmicro.com/en_ph/research/17/j/dnsmasq-reality-check-remediation-practices.html.

62 Real-Time Innovations. (n.d.). *Real-Time Innovations*. “DDS: An Open Standard for Real-Time Applications.” Accessed on July 25, 2022, at https://www.rti.com/products/dds-standard#:~:text=DDS%3A%20An%20Open%20Standard%20for,meet%20real-time%20system%20requirements.

63 Federico Maggi et al. (Jan. 27, 2022). *Trend Micro*. “A Security Analysis of the Data Distribution Service (DDS) Protocol.” Accessed on July 25, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-the-data-distribution-service-dds-protocol.pdf.

64 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2021-38447.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38447#:~:text=OCI%20OpenDDS%20versions%20prior%20to,denial%2Dof%2Dservice%20condition.

65 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2021-38445.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-38445.

66 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2022-22639.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22639.

67 Mickey Jin. (April 4, 2022). *Trend Micro*. “MacOS SUHelper Root Privilege Escalation Vulnerability: A Deep Dive Into CVE-2022-22639.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/d/macos-suhelper-root-privilege-escalation-vulnerability-a-deep-di.html.

68 Apple. (March 14, 2022). *Apple*. “About the security content of macOS Monterey 12.3.” Accessed on July 25, 2022, at https://support.apple.com/en-us/HT213183.

69 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2022-0847.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847.

70 Sunil Bharti. (April 6, 2022). *Trend Micro*. “Detecting Exploitation of Local Vulnerabilities Through Trend Micro Vision One™ and Cloud One™.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/d/detecting-exploitation-of-local-vulnerabilities-through-trend-mi.html.

71 Cybersecurity & Infrastructure Security Agency. (March 10, 2022). *Cybersecurity & Infrastructure Security Agency*. “Dirty Pipe Privilege Escalation Vulnerability in Linux.” Accessed on July 25, 2022, at https://www.cisa.gov/uscert/ncas/current-activity/2022/03/10/dirty-pipe-privilege-escalation-vulnerability-linux.

72 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2022-29464.” Accessed on July 25, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-29464.

73 hakivvi. (April 25, 2022). *GitHub*. “CVE-2022-29464/exploit.py.” Accessed on July 25, 2022, at https://github.com/hakivvi/CVE-2022-29464/blob/main/exploit.py.

74 Orange Tsai et al. (May 2, 2022). *Packet Storm Security*. “WSO Arbitrary File Upload / Remote Code Execution.” Accessed on July 25, 2022, at https://packetstormsecurity.com/files/166921/WSO-Arbitrary-File-Upload-Remote-Code-Execution.html.

75 Hitomi Kimura et al. (May 31, 2022). *Trend Micro*. “Patch Your WSO2: CVE-2022-29464 Exploited to Install Linux-Compatible Cobalt Strike Beacons, Other Malware.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/22/e/patch-your-wso2-cve-2022-29464-exploited-to-install-linux-compatible-cobalt-strike-beacons-other-malware.html.

76 WSO2. (April 29, 2022). *WSO2*. “Security Advisory WSO2-2021-1738.” Accessed on July 25, 2022, at https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738.

77 WSO2. (April 29, 2022). *WSO2*. “Security Advisory WSO2-2021-1738.” Accessed on July 25, 2022, at https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738.

78 Amazon Web Services. (June 2020). *Amazon Web Services*. “Cloud Value Benchmarking Study Quantifies the Benefits of Cloud Adoption.” Accessed on July 25, 2022, at https://pages.awscloud.com/rs/112-TZM-766/images/cloud-value-benchmarking-study-quantifies-cloud-adoption-benefits.pdf.

79 Gartner. (April 19, 2022). *Gartner*. “Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $500 Billion in 2022.” Accessed on July 25, 2022, at https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022.

80 Joanna Ossinger et al. (June 19, 2022). *Fortune*. “Bitcoin has extended its record-breaking decline to below $19,000. ‘Although painful, removing the sector’s froth is likely healthy,’ one expert contends.” Accessed on July 25, 2022, at https://fortune.com/2022/06/18/bitcoin-has-extended-its-record-breaking-decline-to-below-19000-although-painful-removing-the-sectors-froth-is-likely-healthy-one-expert-contends/.

81 Mayra Rosario Fuentes et al. (March 29, 2022). *Trend Micro*. “A Floating Battleground: Navigating the Landscape of Cloud-Based Cryptocurrency Mining.” Accessed on July 25, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-navigating-the-landscape-of-cloud-based-cryptocurrency-mining.pdf.

82 Trend Micro. (Nov. 19, 2018). *Trend Micro*. “Outlaw Group Distributes Cryptocurrency-Mining Botnet.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/18/k/outlaw-group-distributes-botnet-for-cryptocurrency-mining-scanning-and-brute-force.html.

83 David Fiser and Alfredo Oliveira. (July 20, 2021). *Trend Micro*. “Tracking the Activities of TeamTNT: A Closer Look at a Cloud-Focused Malicious Actor Group.” Accessed on July 25, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf.

84 Jaromir Horejsi and David Fiser. (Nov. 24, 2020). *Trend Micro*. “Analysis of Kinsing Malware’s Use of Rootkit.” Accessed on July 25, 2022, at https://www.trendmicro.com/en_us/research/20/k/analysis-of-kinsing-malwares-use-of-rootkit.html.

85 Lawrence Abrams. (Dec. 12, 2021). *Bleeping Computer*. “Hackers start pushing malware in worldwide Log4Shell attacks.” Accessed on July 26, 2022, at https://www.bleepingcomputer.com/news/security/hackers-start-pushing-malware-in-worldwide-log4shell-attacks/.

86 Ryan Flores et al. (April 26, 2022). *Trend Micro*. “How Cybercriminals Abuse Cloud Tunneling Services.” Accessed on July 26, 2022, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services.

87 Aprilyn Borja et al. (Sept. 14, 2020). *Trend Micro*. “Analysis of a Convoluted Attack Chain Involving Ngrok.” Accessed on July 26, 2022, at https://www.trendmicro.com/en_us/research/20/i/analysis-of-a-convoluted-attack-chain-involving-ngrok.html.

88 Global News Wire. (May 6, 2020). *Trend Micro*. “Application Container Market is Expected to Reach $8.20 Billion by 2025, Says Allied Market Research.” Accessed on July 22, 2022, at https://www.globenewswire.com/news-release/2020/05/06/2028585/0/en/Application-Container-Market-is-Expected-to-Reach-8-20-Billion-by-2025-Says-Allied-Market-Research.html.

89 Trend Micro. (May 14, 2019). *Trend Micro*. “Container Security: Examining Potential Threats to the Container Environment.” Accessed on July 26, 2022, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment.

90 Red Hat. (May 18, 2022). *Red Hat*. “Kubernetes adoption, security, and market trends report 2022.” Accessed on July 26, 2022, at https://www.redhat.com/en/resources/kubernetes-adoption-security-market-trends-overview.

91 Magno Logan. (May 24, 2022). *Trend Micro*. “The Fault in Our Kubelets: Analyzing the Security of Publicly Exposed Kubernetes Clusters.” Accessed on July 26, 2022, at https://www.trendmicro.com/en_us/research/22/e/the-fault-in-our-kubelets-analyzing-the-security-of-publicly-exposed-kubernetes-clusters.html.

92 Mark Nunnikhoven. (Oct. 22, 2019). *Trend Micro*. “The Shared Responsibility Model.” Accessed on July 26, 2022, at https://www.trendmicro.com/en_us/research/19/j/the-shared-responsibility-model.html.

93 Trend Micro. (April 24, 2022). *Trend Micro*. “How to better manage your digital attack surface risk.” Accessed on July 26, 2022, at https://www.trendmicro.com/en_us/ciso/22/d/attack-surface-management.html.

94 Trend Micro. (n.d.). *Trend Micro*. “Trend Micro One.” Accessed on July 26, 2022, at https://www.trendmicro.com/en_us/business/products/one-platform.html.

95 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. “CVE-2018-13379.” Accessed on July 26, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379.

96 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. "CVE-2021-22986." Accessed on July 26, 2022, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22986.

97 Trend Micro. (Feb. 11, 2016). *Trend Micro*. "Frequently Asked Questions: BlackEnergy." Accessed on July 26, 2022, at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy.

98 Feike Hacquebord et al. (March 17, 2022). *Trend Micro*. "Cyclops Blink Sets Sights on Asus Routers." Accessed on July 26, 2022, at https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html.

99 WatchGuard. (Feb. 23, 2022). *WatchGuard*. "Important Detection and Remediation Actions for Cyclops Blink State-Sponsored Botnet." Accessed on July 26, 2022, at https://www.watchguard.com/wgrd-news/blog/important-detection-and-remediation-actions-cyclops-blink-state-sponsored-botnet.

100 Asus. (n.d.). *Asus*. "ASUS Product Security Advisory." Accessed on July 26, 2022, at https://www.asus.com/content/ASUS-Product-Security-Advisory/.

101 Zoe Kleinman. (June 14, 2022). *BBC*. "Bitcoin: Why is the largest cryptocurrency crashing?" Accessed on July 26, 2022, at https://www.bbc.com/news/technology-61796155.

102 Cifer Fang et al. (March 24, 2022). *Trend Micro*. "An Investigation of Cryptocurrency Scams and Schemes." Accessed on July 26, 2022, at https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/an-investigation-of-cryptocurrency-scams-and-schemes/03Technical%20Brief%20Keeping%20Assets%20Safe%20From%20Cryptocurrency%20Scams%20and%20Schemes.pdf.

103 Cifer Fang et al. (May 16, 2022). *Trend Micro*. "Fake Mobile Apps Steal Facebook Credentials, Cryptocurrency-Related Keys." Accessed on July 26, 2022, at https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials--crypto-related-keys.html.

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