Trend Micro
Research

TREND MICRO

Rethinking Tactics

2022 Annual Cybersecurity Report

Contents

Published by

Trend Micro Research

The year 2022 was defined by volatile political conflict and economic instability. The war in Ukraine and the escalating events surrounding the conflict sent shockwaves throughout the globe. For many governments, major enterprises, and even smaller organizations, there were disrupted supply chains, setbacks in critical multinational industries, and economic repercussions. Like many organizations operating in this unstable environment, cybercriminals groups tried to adapt and carry on as usual. In our report on the security landscape of the past year, we show how groups adjusted to modernized enterprise security, shifted to more lucrative corporate targets, and focused on new ways to access victims' networks.

In the following sections, we discuss corporate tactics that cybercriminals use to keep their business successful amid declining revenue. We dive into ransomware groups specifically and show how modern groups are taking hints from legitimate businesses when it comes to image management and corporate programs.

We also look at the state of vulnerabilities, especially how threat actors entered networks in 2022. We saw that access is key. No matter what type of malicious actor, gaining initial access into a victim's network is a necessity. These groups learn from each other, and often move in the same manner, just with different end goals. One major security move in 2022 was Microsoft's decision to block the execution of macros in their Office documents. We look at how this affected threat actor's initial access tactics, and how criminal groups have adjusted to this move.

Calling back to our mid-year security report, we saw how the attack surface continued to expand, allowing threat actors more avenues for access. We also saw how enterprise patches seemed to be less effective in 2022, an added factor to recurring cybersecurity problems plaguing businesses. Looking deeper into enterprise security, we investigated weak points in serverless computing security since many cloud service providers (CSPs) have been quick to adopt this technology. The past year also saw a rise in malicious actors targeting cloud infrastructure for their cryptocurrency mining, trying to take over more resources for more lucrative mining activities.

This is particularly critical in a time where there is a shortage of cybersecurity experts – many organizations are still seeking skilled security professionals. According to a report by consultation firm McKinsey, there were 3.5 million cybersecurity positions still open[1] in the first quarter of 2022. We hope that existing security teams, enterprise leaders, and others can use the information presented in this report to harden their cybersecurity defenses against present threats. A robust and extensive security strategy should be a priority as the attack surface continues to expand and threat actors continue to grow more sophisticated.

Cybercriminals Are Using Corporate Tactics

The current state of ransomware[2] shows how operators behind this threat have been quick to broaden their scope of attack in the face of declining returns. Recent reports say that ransomware revenue from victim payouts is waning, with a 38% decrease from 2021 to 2022.[3] But what has kept this threat alive? In recent years, it has become clear that the thriving ransomware organizations have adopted tactics from the same corporate handbook that legitimate multinational companies use.

Rebranding and Image Management

Many of these groups have structured their organizations that operate like legitimate businesses, including leveraging established networks[4] and offering technical support[5] to victims. We have been seeing an increasing level of professionalism from these groups, and the adoption of more sophisticated business tactics. This was particularly clear in 2022, when we saw one of the biggest players among ransomware groups rebrand after an image crisis.

Conti was one of the most active and prominent ransomware families in recent years[6], but after a string of high-profile attacks in 2022 and conspicuous affiliation with Russia, the brand was labeled 'toxic'.[7] Conti's operations were effectively shut down mid-2022, however, former members of the previous group emerged rebranded as several new groups: Black Basta, BlackByte, Karakurt, and Royal. This rebranding was a well-planned move, and reports[8] say Conti planned a string of public attacks as publicity for their reincarnation as smaller operations.

Diversifying Their Portfolio

In 2022 we saw ransomware groups like Agenda, BlackCat, Hive, and RansomExx develop versions of their ransomware in Rust.[9] This cross-platform language allows groups to customize malware for operating systems like Windows and Linux which are widely used by businesses.

As we mentioned in our mid-year roundup,[10] ransomware actors are now moving beyond Windows and MacOS and targeting Linux. The shift to Rust is another technique being adopted by ransomware actors to make it easier for them to target Linux machines. Rust is more difficult to analyze and has a lower detection rate by antivirus engines, making it more appealing to threat actors.

OS	2021	2022
Linux	3,790	27,602
MacOS	15,154	11,000

Table 1. Ransomware operating system (OS) comparison counts

In recent years, we saw how modern ransomware groups use the double extortion technique[11] as added pressure for victims to pay ransom. Last year, our investigations showed that ransomware groups were building up new revenue streams[12] using their existing business structure and tools. For instance, the BlackCat[13] ransomware was seen using an upgraded version of the ExMatter data exfiltration tool and Eamfo, a malware designed to steal credentials.

Shifting to monetization of exfiltrated data would be easy for ransomware groups – many of the current RaaS organizations can capitalize on the tools they already have. We expect that in the future, the groups will also adopt other criminal business models[14] that monetize initial access, such as stock fraud, business email compromise (BEC), money laundering, and cryptocurrency theft, among others.

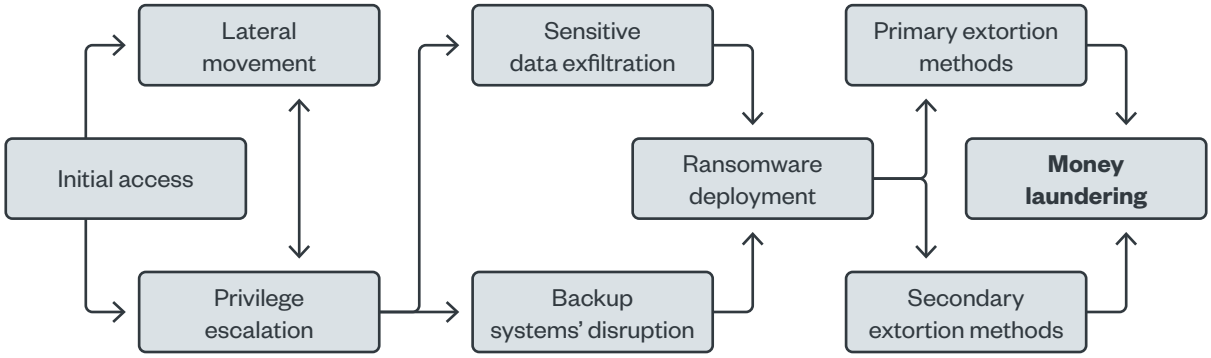

Figure 1. Example of new modern ransomware business model

These organizations are becoming jacks-of-all-trade, using their established business structure and extensive arsenal of tools to expand into new ventures. They are not tying themselves down to one method of attack, one entry vector, or one revenue stream.

> Ransomware group LockBit 3.0 introduced the first ransomware bug bounty program. Bug bounties[15] are usually set by technology companies to crowdsource vulnerabilities. Rewards are offered to researchers who report bugs, so companies can patch them. In 2022, we saw that the ransomware group was using the same tactic for their malware.

New ransomware tactics in 2022

Access is Key for Threat Actors

Regardless of the type of threat actor, they go through the same motion of gaining access to the target's environment. This is highlighted by the top three MITRE Attack techniques that we saw in 2022. These techniques show the standard operating procedure for most threat actors. No matter the type of attacker, the initial phases of their attack do not technically look different.

2022 Top Three MITRE Techniques

Remote Services, Technique T1021 – Enterprise | MITRE ATT&CK®

(Lateral Movement)

- Adversaries may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

Valid Accounts, Technique T1078 – Enterprise | MITRE ATT&CK®

(Initial Access)

- Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services.

OS Credential Dumping, Technique T1003 – Enterprise | MITRE ATT&CK®

(Credential Access)

- Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

The top three attack techniques indicate that threat actors getting access through remote services, and then they proceed to expand their footprint within the environment by utilizing valid accounts through credential dumping.

Microsoft's Major Move in 2022

The most popular initial access vector for the past seven years has been Microsoft Office documents with embedded malicious macros. These documents were usually attached to an email with a social engineering message enticing the victim to open it. If opened, the malicious macro downloads and executes malware that grants the threat actor initial access.

However, in early 2022 Microsoft decided to block the execution of macro programs on Office documents. Specifically, they blocked those downloaded from the internet, including the macros attached in emails. This single action changed everything for threat actors. No longer able to use Microsoft macros, the threat actors started searching for and using alternative vectors.

Alternatives to Microsoft Macros

Some of the alternative initial access vectors we tracked included HTML smuggling[16] and malvertising.[17] In late 2022, we identified a growing list of popular brands and applications whose keywords were hijacked to display malicious ads (a case of malvertising). For example, a Google search for "Adobe Reader" will show an advertisement that leads to a malicious site.

HTML smuggling is an initial access vector that uses email. The basic idea is to use a malicious HTML file as an attachment. When opened, the HTML file "smuggles" a ZIP file which contains an ISO file with a LNK file in it that will load the malware payload. It is a cumbersome method, but that payload will grant the threat actor initial access.

We also saw how cybercriminals were "living off the land" (abusing valid systems and tools) more in 2022. Specifically we noted that legitimate pentesting tools Cobalt Strike and Brute Ratel were used in malicious attacks.[18] A cybercriminal that uses these pentesting tools and built-in operating system tools within a short timeline is a dangerous threat.

Time	Activities
T-zero	Initial access gained through HTML smuggling
+16 minutes	CnC communication and early reconnaissance
+5 minutes	Brute Ratel is dropped
+5 minutes	Use of built-in OS tools for reconnaissance
+10 minutes	AC reconnaissance using another tool
+7 minutes	lateral movement via CobaltStrike starts

Table 2. Example of an attack timeline using legitimate pentesting tools

The Attack Surface is Expanding and Patches are Failing

Threat actors have long been learning from one another, so much so that they act and move in generally the same way. However, there are some variations in their tools and preferences (depending on availability) and perhaps how their networked environment is set up.

Top Vulnerabilities Used in 2022

In terms of top vulnerabilities seen in 2022 we saw a move from the Microsoft-focused common vulnerabilities and exposures (CVEs) to Log4J[19] CVEs. This is likely related to the major change Microsoft made, which was discussed in the previous section. Developers use Log4j as a journal to keep track or log the activity of a system or application. In 2021, several vulnerabilities were highly publicized[20] and we saw that threat actors took advantage of that in 2022.

2021 Top 3 CVEs	2022 Top 3 CVEs
NVD – CVE-2021-26855 (nist.gov) NVD – CVE-2021-27065 (nist.gov) NVD – CVE-2020-0688 (nist.gov) All of these are Microsoft Exchange vulnerabilities	NVD – CVE-2021-44228 (nist.gov) NVD – CVE-2021-45015 (nist.gov) NVD – CVE-2021-45046 (nist.gov) Three of them are Log4J vulnerabilities, one is relatively obscure

Table 3. Top three CVEs in 2021 compared to 2022

There are a few notable points when we look into the top CVEs in 2022:

- The CVEs can be exploited publicly by a threat actor. There are many dissections, write-ups, and analysis available.
- They are highly successful, with a base score of HIGH/CRITICAL. The attack vector can be performed via network, the complexity is low, and almost no existing privilege is required to exploit without user interaction (this means attacks can be automated).
- They have been reported in the news and are primed for use. There are lists of vendors (or customer bases) that have been affected. It is a known target pool that threat actors can draw from.

Threat actors are typically updated with the latest vulnerabilities and are well-aware of the CVEs that they can use for their activities. It is up to security experts and users to be ahead of the threat actors and implement fixes to vulnerabilities before they can be exploited.

As much as the vulnerabilities and weaknesses threat actors use can be similar, their motives may vary. Their end goals could be data collection and exfiltration, ransomware, cryptocurrency mining, or other malicious actions.

We also looked at data from Trend Micro™ Deep Security™ (DS) for a yearly total of vulnerability-related events, and we saw similar results to our mid-year report. A vulnerability (CVE-2017-14495) affecting dnsmasq had the highest number of detected events. This is unsurprising considering it is a popular free software that can be configured as a DNS, a DHCP (Dynamic Host Configuration Protocol), and a TFTP (Trivial File Transfer Protocol) server. It is mainly used in routers and internet of things (IoT) gateways.

The other vulnerabilities with high detection counts were varied. CVE-2021-44228 is an Apache Log4j vulnerability that we mentioned in the previous section, and CVE-2006-4154 is another vulnerability that affects Apache. Again, we see that threat actors are targeting widely used free technology essential to many businesses. Like dnsmasq, Apache is also a free software and it runs on 67% of all websites in the world.[21]

Filter ID	Solution	Related CVEs	Detection Event Counts
1009667	Deep Security	CVE-2017-14495	149,584,000,000
1011242	Deep Security	CVE-2021-44228	11,766,751,565
1000853	Deep Security	CVE-2006-4154	5,667,326,528
1004398	Deep Security	CVE-2010-2730	1,970,505,793
1010971	Deep Security	CVE-2021-29441	1,936,302,017
1011466	Deep Security	CVE-2022-30522	1,518,554,891
1006027	Deep Security	CVE-2014-0098	871,076,092
1011456	Deep Security	CVE-2022-26134	533,046,544
1011265	Deep Security	CVE-2021-45046	269,500,708
1011492	Deep Security	CVE-2022-30136	169,278,618

Table 4. The number of detected vulnerability-related events based on Trend Micro™ Deep Security™ and Trend Micro Apex One™ data in 2022

Spring4Shell CVE-2022-22965 - CVSS rating: 9.8

CVE-2022-22965 is a critical bug that affects the Spring Framework,[22] which is used to develop enterprise-level applications in Java. We first started seeing this vulnerability in April 2022 and investigations show that it allows malicious actors to weaponize and execute the Mirai botnet malware.

Log4Shell CVE-2021-44228 - CVSS rating: 10.0

CVE-2021-44228 is a critical flaw found in Apache Log4j which is a widely used Java-based logging library. National defense agencies across the world issued warnings[23] about this bug because of attacks observed in the wild. This was first reported in 2021, and the security issues continued into 2022.

Vulnerability Spotlight

Record Breaking Numbers for ZDI

Advisories from the Trend Micro™ Zero Day Initiative™ (ZDI) have kept rising, and 2022 marks their third record-breaking year. The reported 1,706 advisories are the most ever in the history of the program.

We see two reasons for the steady increase of published advisories. First, the attack surface has increased exponentially, so there are more bugs to be found. The other factor is that ZDI itself has invested in automating analysis, which has resulted in many more bugs found by researchers.

Comparing the severity of the reported common vulnerabilities and exposures (CVE), we see that from 2021 the number of critical bugs doubled in 2022, though it did not reach the heights of critical bugs in 2020.

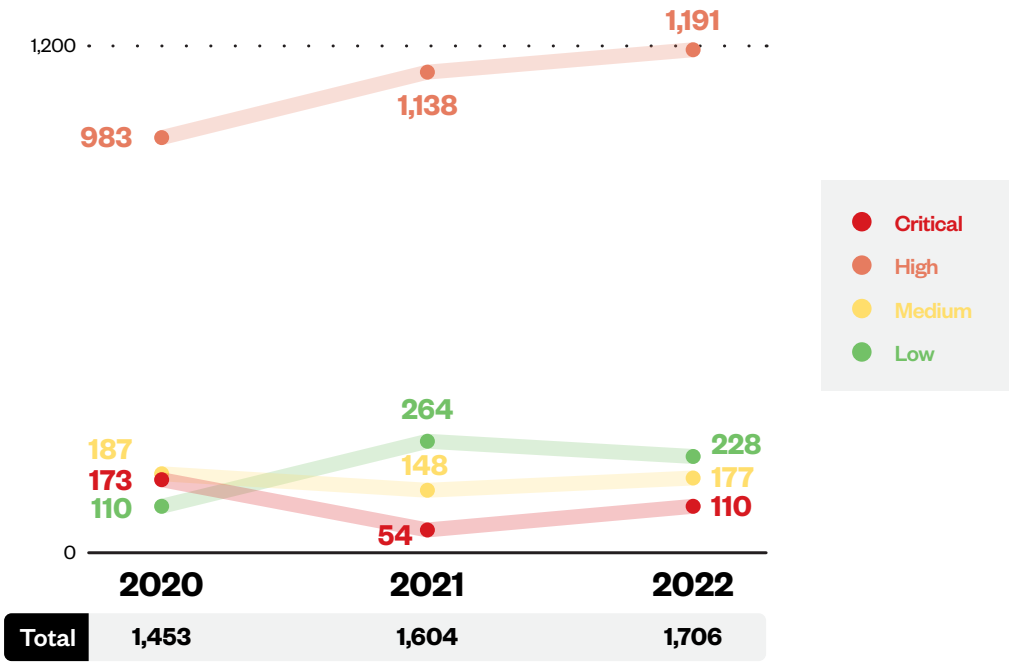

Figure 2. Comparison of number and severity of advisories across 2020, 2021, and 2022

After examining the vulnerabilities themselves, we did not see any big shifts in the types of bugs. However, we did see an increase in failed patches.[24] Organizations may not have the time or resources to create comprehensive solutions, simply pushing out quick fixes instead of addressing root issues. Not only that, but companies also seem to be disclosing less specific information in their public alerts about their vulnerabilities. This gives other businesses and security heads less information to work with when applying the patches.

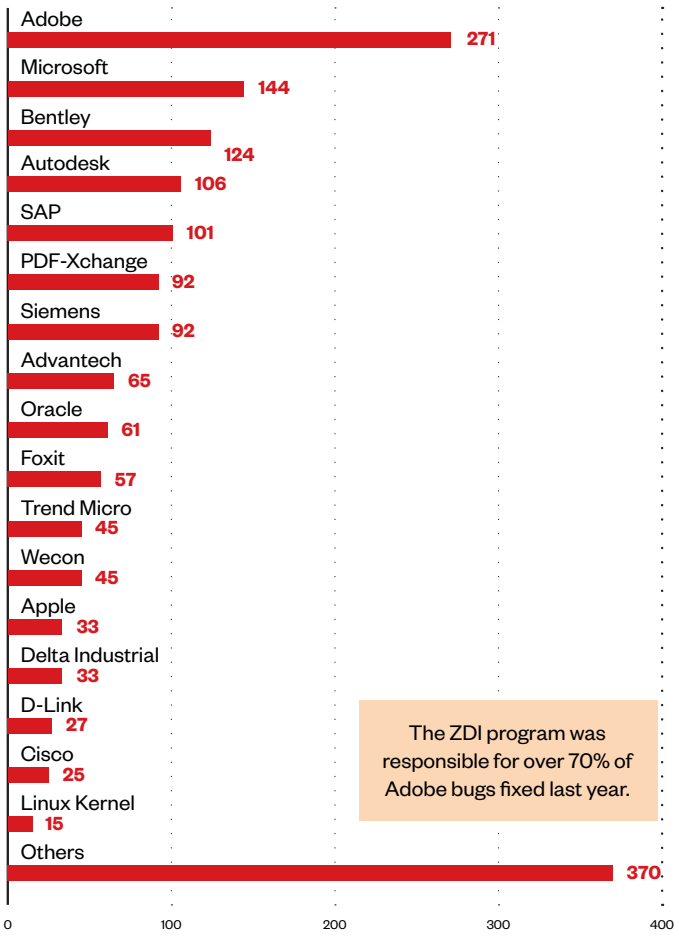

Figure 3. Published security advisories per vendor for 2022

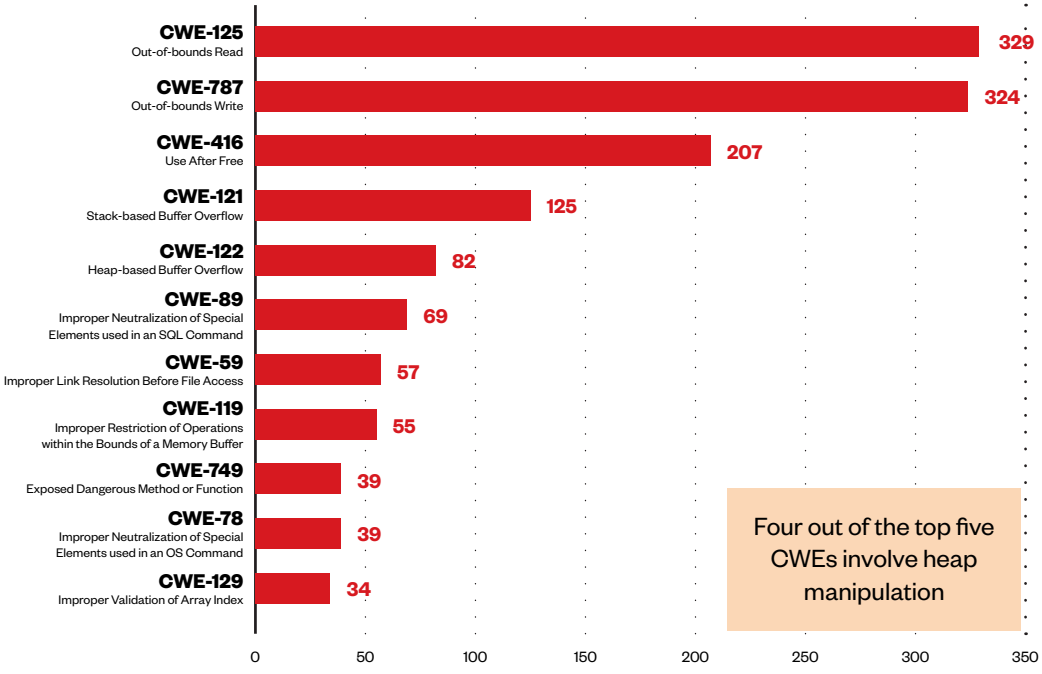

Figure 4. Top 10 CWEs from 2022 Published Advisories

Another issue with the expanding attack surface is the continuing strikes on virtual private network (VPN) vulnerabilities. The use of VPNs spiked during the pandemic,[25] and they have been integral to many business operations since. In our mid-year roundup, we reported on the detected attacks targeting certain VPN vulnerabilities, and this threat has continued through the end of 2022.

The top tracked vulnerability is still the Fortinet path traversal vulnerability CVE-2018-13379 which occurs in Fortinet's FortiGate SSL; and other highly targeted flaw was an arbitrary file reading vulnerability involving Pulse Secure Pulse Connect Secure (PCS).

	Fortinet		Pulse Secure				Citrix Systems	
	CVE-2018-13379	CVE-2022-40684	CVE-2019-11510		CVE-2019-11539	CVE-2021-22893	CVE-2019-19781	
	DV-36087	DV-41863	DV-36089	DV-36241	DV-36095	DV-39636	DV-36876	DV-36927
Jan	21,710		8,708	506			1,120	27
Feb	21,733		8,204	775			684	15
Mar	26,405		10,110	1,940			2,068	60
Apr	25,077		14,950	1,483		3	1,134	67
May	32,590		16,226	1,800	30	1	1,770	76
Jun	90,700		48,098	1,765		2	3,361	43
Jul	76,897		55,665	2,729	8		4,270	193
Aug	123,201		71,423	2,848	4		4,454	140
Sep	142,205		78,879	5,606	8	3	3,641	157
Oct	163,583	861	89,949	7,762	24	4	10,735	252
Nov	90,505	562	29,600	6,001	12	1	8,273	148
Dec	118,736	1,730	32,881	20,098	16		22,141	122

	F5					SONICWALL
	CVE-2020-5902		CVE-2021-22986			CVE-2021-20016
	DV-37841	DV-38276 (Malware)	DV-39360	DV-39352	DV-39364	DV-39727 (Malware)
Jan	19,339		1,320	173	3,126	
Feb	17,581		2,503	446	3,419	
Mar	34,507		1,481	313	3,418	
Apr	24,881		91	303	3,884	
May	36,079		12	394	54,692	
Jun	62,302		39	241	105,075	
Jul	62,756	1	2	216	91,045	1
Aug	84,159		1	178	45,099	
Sep	109,689			155	44,891	
Oct	113,307	27		168	35,872	
Nov	40,429			42	17,013	161
Dec	60,664			99	23,447	160

Table 5. A monthly record of detected attempts to exploit known VPN vulnerabilities in 2022

Weak Points Spotted in the Cloud

Cloud service providers (CSPs) have been quick to adopt serverless computing because it helps organizations run services without managing underlying infrastructure. The services are for managing business operations such as built-in scalability, operability in multiple regions, and cost manageability. Serverless technology allows developers to upload code to a specific service without worrying about infrastructure maintenance, scalability, and availability.

Weak Areas in Serverless Security

In 2022, we investigated the security of these serverless platforms and pinpointed weak areas that could potentially be abused by attackers. These serverless computing services are being used by businesses to oversee complex processes and house information integral to business operations. Handling and managing secrets, as well as sensitive data, should also be a concern for both the provider and user of services.

Figure 5. What serverless platforms can be used for

Malicious actors have started to shift focus to cloud-oriented services because misconfiguration is a prolific problem, and serverless environments are the likely next target. Since serverless technology allows users to upload code to the service, securing endpoints and writing secure code is the user's responsibility. It is vital that misconfiguration issues are not introduced into the system through the users.

We also concluded that the default configurations on cloud services are not the best options from a security perspective. Users should look to solutions involving hardening an operating system and see how the security steps should also be followed in the serverless world.

Another red flag we noted in serverless security is that both the user and the CSPs do not properly secure secrets and access tokens. Recently there have been reports of multiple hacker teams[26] that harvest CSP-specific secrets to take over the target's services or the whole account.

One incident[27] involved TeamTNT, a group known for stealing Amazon Web Services (AWS), Docker, and Linux Secure Shell (SSH) credentials. The group breached cloud environments and specifically looked for sensitive environment variables.[28] There were also reports[29] of a supply-chain attack where a Python library had its code changed to start harvesting sensitive variable content.

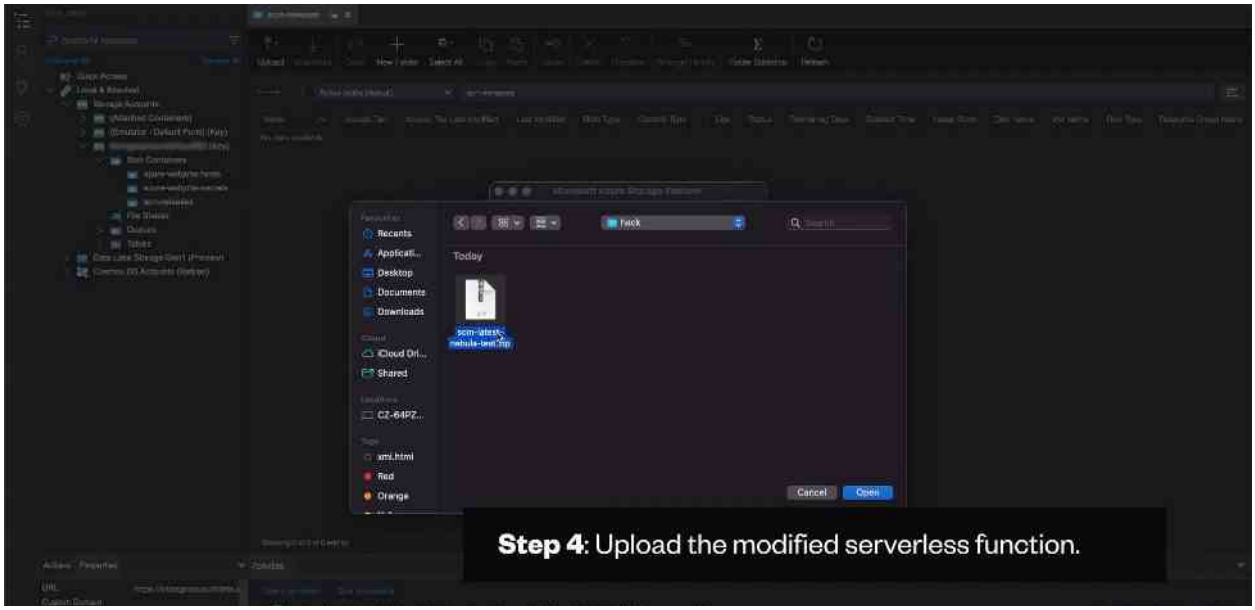

Figure 6. Trend Micro's report on what happens when secrets stored as an environmental variable are unwittingly leaked.[30]

The CSP is responsible for the execution process of the serverless service, however, the user is the one deploying code into the serverless system. In our latest report,[31] we simulated user-provided code vulnerabilities among serverless services provided by major CSPs in the market. Based on our evaluation of serverless environments, we found that the most concerning security gaps were in Microsoft Azure, for instance:

- There were sensitive environmental variables inside the Microsoft Azure environment; if these are leaked, malicious actors can fully compromise the entire serverless environment.
- There was a default runtime image using a master password that allows privilege escalation in most Azure App Service deployments.

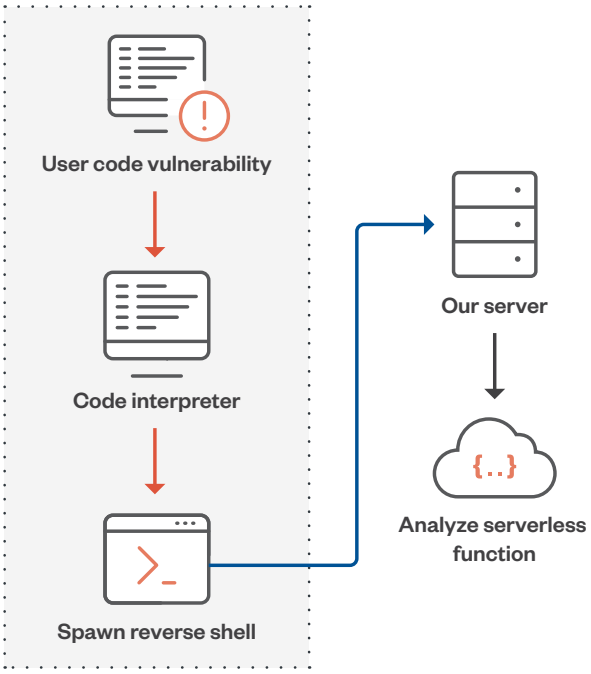

Figure 7. Attack simulation of a serverless function

One throughline we saw was that the user poses a daunting security risk. An unfamiliar user could misconfigure the cloud service and create a wider attack surface or could implement code with easily exploitable vulnerabilities.

The State of Cloud-crypto Attacks

The volatility of cryptocurrency and the seeming decline of profitability in cryptocurrency mining[32] means that miner operators needed to find alternative methods and techniques. In 2022, we saw that these malicious actors were aiming to compromise cloud infrastructure instead of relying on less lucrative CPU-based operations.

This is not a new development, but in 2022 we reported that the frequency of attacks increased,[33] keeping pace with new cloud services being created and offered for free. Some scenarios allowed malicious actors to scale their attacks so that even a few minutes or hours of compromise could generate significant profits.

This fight for resources seems to be extreme – we saw how two attackers battled for control over victim's servers[34] and that the control over a target can fluctuate within a day. These groups use kill scripts that help get rid of competing cryptocurrency miners while also strengthening their obfuscation and persistence mechanisms.

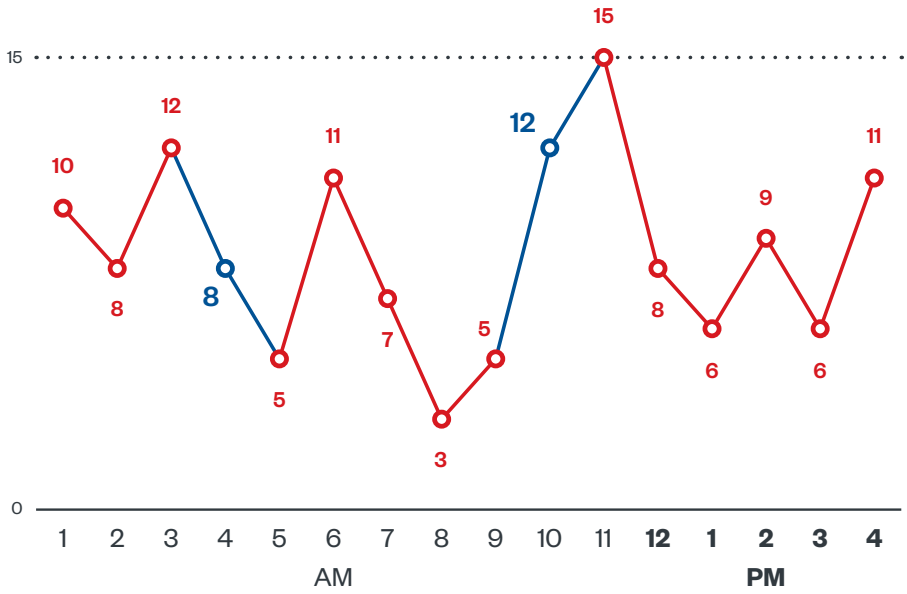

Figure 8. A typical day showing the back-and-forth control of a cloud instance by Kinsing (red) and 8220 (blue), with the numbers representing inbound control connections

Echoing the trend of ransomware actors focusing on Linux machines, we see that cryptominers are also doing the same – aiming for less protected targets with big payoffs. In November 2022, we also intercepted a cryptocurrency mining attack using an advanced remote access trojan (RAT) named the CHAOS Remote Administrative Tool[35] that was targeting Linux machines.

OS	2021	2022
Linux	8,240	13,228
MacOS	1,488	889

Table 6. Cryptominer Linux and MacOS counts in 2021 versus 2022

Companies should be aware of the hidden issues involved with cryptocurrency miners. If this threat is present in a company's system, it is usually a sign that there are deeper security issues in the cloud infrastructure. The miner may not seem as serious a threat as data exfiltration or a ransomware infection but the method with which malicious actors enter a target's system is practically the same. Most actors, regardless of their motive or endgame, first exploit a vulnerable point in the organization's security. Having a miner not only impacts an organization's cloud infrastructure, it is also an indicator of poor security hygiene.

> A spike in CPU utilization rate from an average of 13% to 100%
>
> A jump in electricity cost from US$20 to US$130 per month–a 600% increase for a single cloud instance.
>
> Closure or disruption to the online services of a business.

How will cryptomining affect cloud services?

The Business Impact of Cybersecurity Attacks

The predatory nature of cybercrime means malicious actors specifically target organizations or technologies perceived as highly vulnerable and lucrative. As mentioned in the above sections, Linux-based threats are on the rise, mainly because unsecured internet of things (IoT) devices are proliferating in enterprises and homes[36] – targets ripe for the picking. Meanwhile, cryptocurrency mining operators are actively looking for ways to sneak onto corporate cloud infrastructure and silently leech resources.

In 2022, we also saw how ransomware actors targeted small and midsize businesses operations. These are smaller organizations that can be held hostage when faced with cyberattacks since they have fewer IT security resources to avoid or respond to complex attacks.

Employees	Attack Count
Small (1-200)	1,213
Medium (201-1000)	657
Large (more than 1001)	497

Table 7. The distribution by organization size of successful ransomware attacks in terms of victim organizations in 2022

A Trend Micro global survey also showed that 52% of all organizations have a supply chain partner that has been hit with a ransomware attack.[37] Specifically, the software supply chain is where the problem is centered – the different components and tools being used within the organization can be exploited and abused by cybercriminals. And third parties may bring in new software to integrate into an organization. Cybercriminals have multiple options for entering a network, and one flaw can give them access to a whole range of systems and sensitive data.

One of the key steps in managing the security of the software supply chain is having a software bill of materials (SBOM)[38] or a formal record of the details and relationships of the software's components.

Figure 9. How supply chain partners can affect an organization's security, specifically in the case of ransomware attacks

Our data shows that cybercriminals have been focusing on certain industries. Our research shows that manufacturing targets were top of mind for threat actors in 2021. However, the threats were more evenly dispersed in 2022, when government targets were the main targets of malicious attackers.

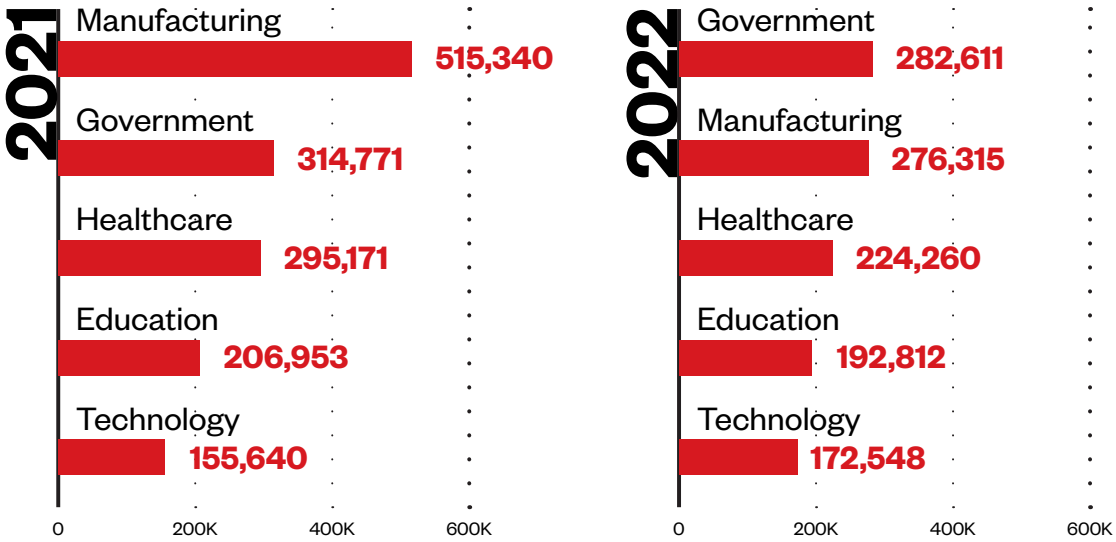

Figure 10. Top five industries affected by malicious files in 2022 compared to 2021

Note: One malware detected multiple times in one machine is counted as one unique machine

Source: Trend Micro Smart Protection Network infrastructure

Strategies for Defending Against an Increasingly Tactical Adversary

The growth of the digital attack surface is an aftereffect of enterprises navigating post-pandemic economies and trying to manage an increasingly remote workforce. Organizations continue to adopt new technology to keep up with hybrid styles of work, complex online operations and sales, burgeoning data storage needs, data protection requirements, and more. As stated in our mid-year report, this means that enterprises and organizations are scrambling to fill security gaps. Not to mention, cybersecurity experts are in increasingly short supply. This means that many organizations will require adaptable solutions and tactics that will counter threats in a more efficient way.

Meanwhile, threat actors are leaning into more legitimate business tactics and professional operations, employing the same kinds of programs and corporate strategies and their victims. Not only are they innovating in terms of tools and targets, but they are also building resilient organizations that do not rely on singular methods of attack or a particular target pool. They can exploit multiple areas of the attack surface in a single campaign.

A skills shortage means that organizations need a more efficient and holistic security solution; ideally, one that can aggregate multiple needs and actions into one platform. Here are some security practices organizations should keep in mind:

- **Asset management.** Examine assets and determine their critical importance, potential vulnerabilities, the level of threat activity, and how much threat intelligence is being gathered from the asset.
- **Cloud security setups.** Ensure that the cloud infrastructure is set up with security in mind to prevent attackers from capitalizing on known gaps and vulnerabilities.
- **Proper security protocols.** Prioritize updating software as soon as possible to minimize exploitation of vulnerabilities. Options such as virtual patching can help organizations while vendors provide their security updates.
- **Attack surface visibility.** Monitor the different technologies and networks within the organization, as well as any security system that protects them. It may be difficult to correlate different data points from siloed sources.

Organizations need a comprehensive solution that manages the entire attack surface. Visibility is key, as well as the ability to correlate different indicators so that security teams can focus on the bigger picture. A unified platform can provide multilayered protection while helping reduce expenditures that would otherwise be spent on multiple security technologies.

Threat Landscape

146,408,535,569

Overall threats blocked in 2022

In 2022, Trend Micro Smart Protection Network, including Mobile App Reputation Service, IoT Reputation Service, and Smart Home Network, protected Trend Micro customers from more than 146 billion threats. Our year-on-year data shows a 55% increase in overall blocked threats compared to 2021, there was also a substantial 242% increase in blocked malicious files. The almost 70 billion malicious files we blocked include unique and non-unique infections, meaning we count reinfections as well. This is a likely factor in the number of worms we detected (shown in Figure 16). Worms are almost impossible to get rid of since their primary function is to remain in the network and propagate. A high number of viruses or file infectors also contribute to the number of files blocked.

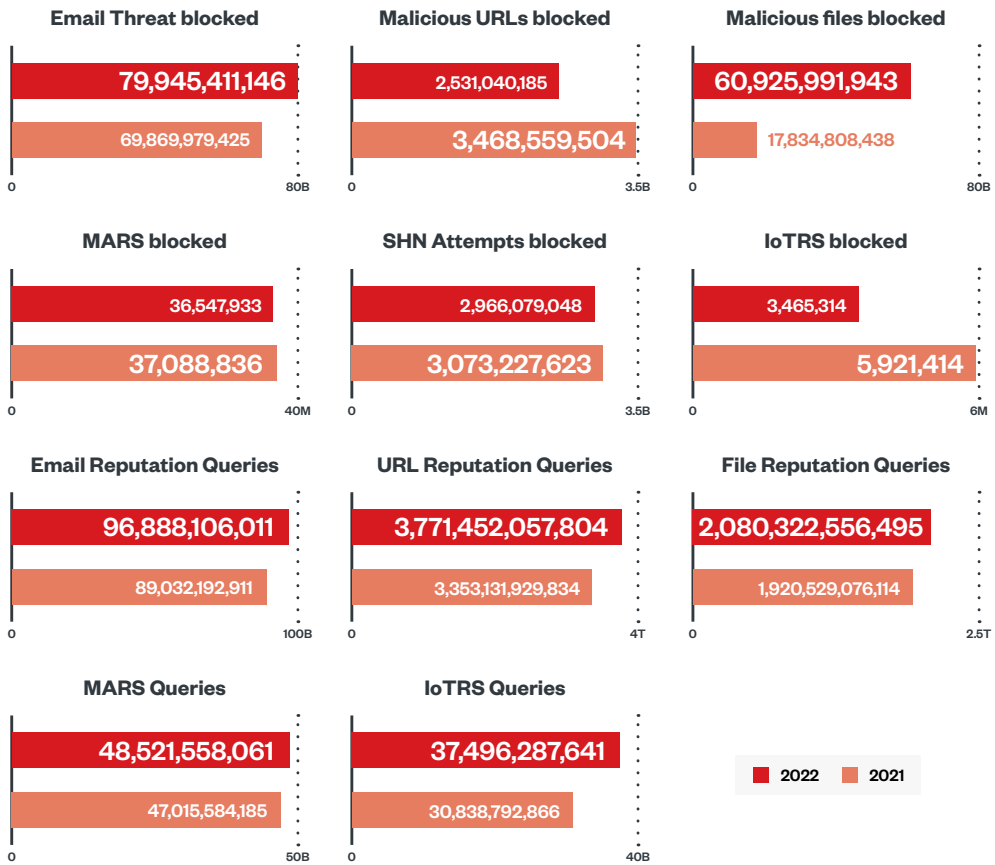

Figure 11. A comparison of the numbers of blocked email, URL, and file threats, of email, URL, and file reputation queries, and of blocked mobile app, IoT, and Smart Home Network threats in 2021 and 2022

Source: Trend Micro Smart Protection Network, including Mobile App Reputation Service, IoT Reputation Service, and Smart Home Network

The regional distribution of the threats we track shows an interesting picture of the security landscape in terms of area. Notably, we see that ransomware threats are mainly concentrated in Asia and the Americas. Business email compromise (BEC) threats were also mostly targeting victims in America, and Asia was top ranked in terms of mobile security issues.

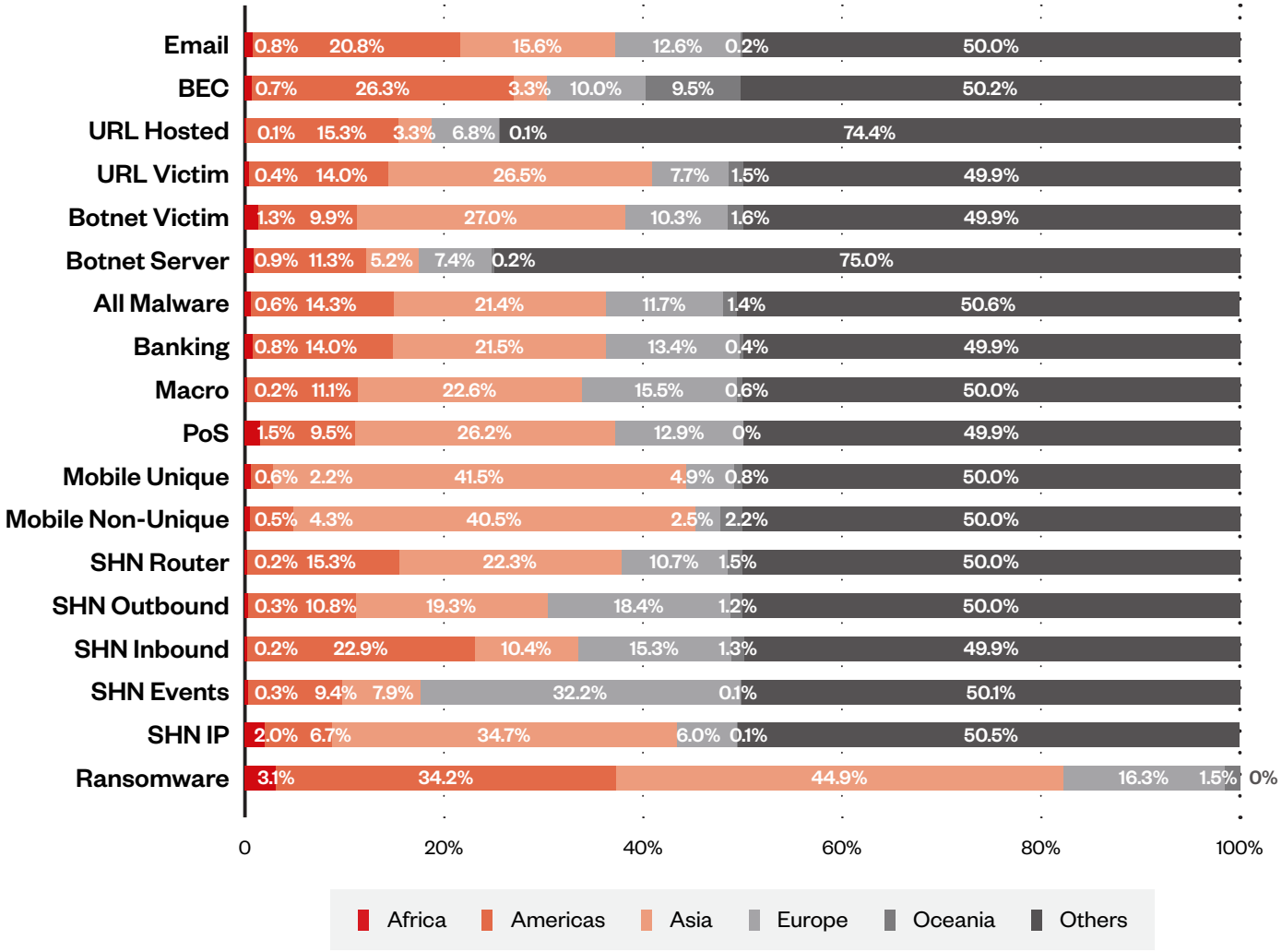

Figure 12. The regional distribution of threats tracked by Trend Micro in 2022 including: email, URL, and file threats, blocked mobile apps, IoT, and Smart Home Network threats.

Source: Trend Micro Smart Protection Network, including Mobile App Reputation Service, IoT Reputation Service, and Smart Home Network

Webshells are malicious scripts that allow threat actors to compromise web servers and launch attacks. They were the top detected malware of the year, and there was a 103% spike in web shell detections from 2021 to 2022. Emotet detections were second in our rankings – it was not in the top ten in 2021, but 2022 saw a resurgence. In terms of ransomware, LockBit and BlackCat were the top families present in 2022.

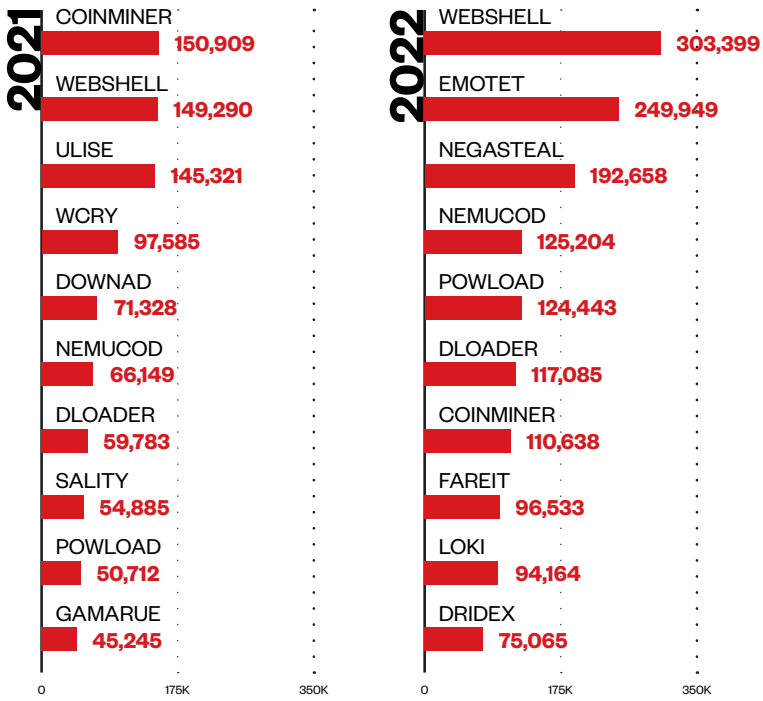

Figure 13. The top 10 malware families in terms of detections in 2021 compared to 2022

Source: Trend Micro Smart Protection Network

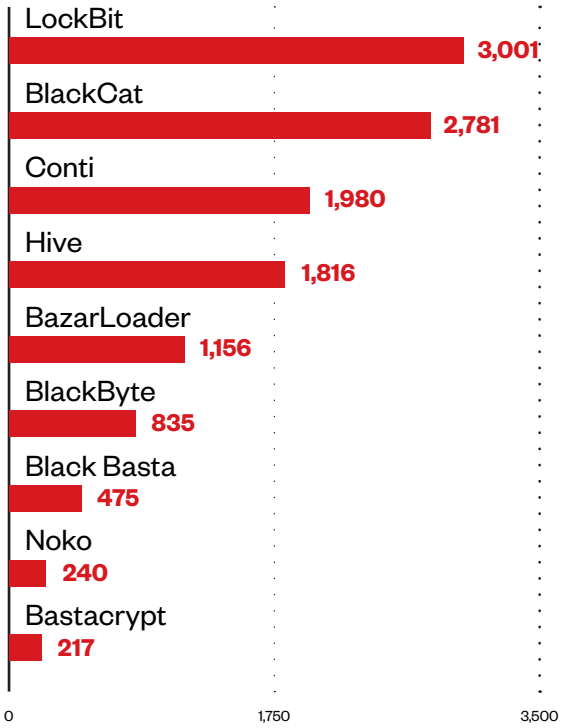

Figure 14. The top ransomware families in 2022

Source: Trend Micro Smart Protection Network

	Jan	Feb	Mar	Apr	May	Jun
1	No New Families	No New Families	Ransom.Win32.EXPLUS.A	Ransom.Linux.CHEERSCRYPT.A	Ransom.Win64.KEVERSEN.A	Ransom.MSIL.ZAGREUS.A
2			Ransom.Win32.NOESCAPE.A		Ransom.Win32.STORAGECRYPT.A	Ransom.Win32.LORENZ.A
3					Ransom.MSIL.PALANG.A	Ransom.Win32.EVILNOMINATUS.A
4					Ransom.Win32.BLAZE.A	
5						
Total			**2**	**1**	**4**	**3**

	Jul	Aug	Sep	Oct	Nov	Dec
1	No New Families	Ransom.Win32.USELESSDISK.A	Ransom.PS1.BEBACK.A	Ransom.Win32.GORF.A	Ransom.MSIL.PENTERWARE.A	Ransom.Win32.HMBRAN.A
2		Ransom.Win32.WRLDECODING.A		Ransom.Win32.MIMIKRYPT.A	Ransom.Win32.BEIJIRAN.A	Ransom.Win64.PANDORA.A
3		Ransom.Win32.PLAYDE.A		Ransom.Win32.CRYPTATO.A	Ransom.Win64.VICESOCIETY.A	Ransom.Win.32.SCHOOBOS.A
4		Ransom.MSIL.KANCRYPTER.A			Ransom.MSIL.MALLOX.A	
5					Ransom.Win64.BLOODY.A	
Total		**4**	**1**	**3**	**5**	**3**

Table 8. The new ransomware families detected in 2022

Source: Trend Micro Smart Protection Network

There was a 1.5% year-on-year decrease in blocked malicious apps in 2022.

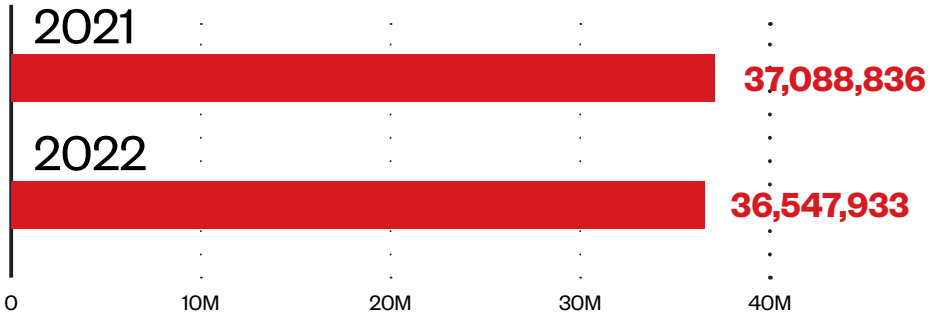

Figure 15. A comparison of blocked malicious apps in 2021 and 2022

Source: Trend Micro Mobile App Reputation Service

There was a spike in malicious file detections in 2022, and when investigating these files we were able to dissect the types of malware our products blocked. There was an 11.1% decrease of hacktool usage, it is likely that some these hack tools were used in ransomware deployment. The tool Bloodhound was most used in 2022, while Mimikatz was most used in 2021. There was a massive increase in backdoor detections, 86.2% specifically. These backdoors mostly targeted web server platform vulnerabilities.

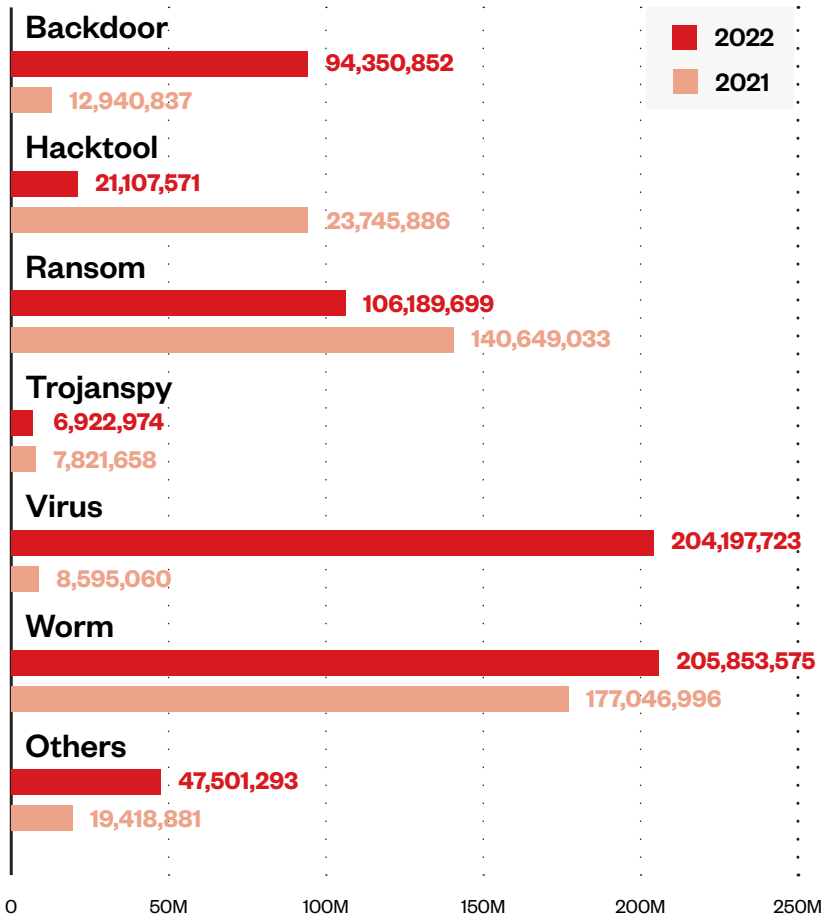

Figure 16. Comparison of malware types blocked in malicious files in 2021 and 2022

Endnotes

1 Rami Sass. (Nov. 14, 2022). *Forbes*. "A New Approach Is Needed To Close The Cybersecurity Talent Gap." Accessed on Mar. 1, 2022, at: Link.

2 Feike Hacquebord, Stephen Hilt, and David Sancho. (Dec. 15, 2022). *Trend Micro Security News*. "The Future of Ransomware." Accessed on Mar. 1, 2022, at: Link.

3 Pieter Arntz. (Jan. 23, 2023). *Malwarebytes*. "Ransomware revenue significantly down over 2022." Accessed on Mar. 1, 2022, at: Link.

4 Trend Micro Research. (Oct. 27, 2022). *Trend Micro Security News*. "Ransomware Spotlight: BlackCat." Accessed on Mar. 1, 2022, at: Link.

5 Trend Micro Research. (Dec. 7, 2022). *Trend Micro Security News*. "Ransomware Spotlight: Cuba." Accessed on Mar. 1, 2022, at: Link.

6 Trend Micro Research. (Dec. 1, 2021). *Trend Micro Security News*. "Ransomware Spotlight: Conti." Accessed on Mar. 1, 2022, at: Link.

7 Eduard Kovacs. (May 23, 2022). *Security Week*. "Conti Ransomware Operation Shut Down After Brand Becomes Toxic". Accessed on Mar. 1, 2022, at: Link.

8 Lawrence Abrams. (May 19, 2022). *Bleeping Computer*. "Conti ransomware shuts down operation, rebrands into smaller units." Accessed on Mar. 1, 2022, at: Link.

9 Nathaniel Morales et al. (Dec. 16, 2022). *Trend Micro Research*. "Agenda Ransomware Uses Rust to Target More Vital Industries." Accessed on Mar. 1, 2022, at: Link.

10 Trend Micro Research. (Aug. 31, 2022). *Trend Micro Research*. "Defending The Expanding Attack Surface: Trend Micro 2022 Midyear Cybersecurity Report." Accessed on Mar. 1, 2022, at: Link.

11 Janus Agcaoili et al. (Jun. 15, 2021). *Trend Micro Research*. "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Accessed on Mar. 1, 2022, at: Link.

12 Feike Hacquebord, Stephen Hilt, and David Sancho. (Dec. 15, 2022). *Trend Micro Security News*. "The Future of Ransomware." Accessed on Mar. 1, 2022, at: Link.

13 Trend Micro Research. (Oct. 27, 2022). *Trend Micro Security News*. "Ransomware Spotlight: BlackCat." Accessed on Mar. 1, 2022, at: Link.

14 Feike Hacquebord, Stephen Hilt, and David Sancho. (Dec. 15, 2022). *Trend Micro Research*. "Ransomware Business Models: Future Pivots and Trends." Accessed on Mar. 1, 2022, at: Link.

15 Tech Target. (July 2017). *Tech Target*. "Bug Bounty Program." Accessed on Mar. 1, 2022, at: Link.

16 Ian Kenefick, Lucas Silva, and Nicole Hernandez. (Oct. 12, 2022). *Trend Micro Research*. "Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike." Accessed on Mar. 1, 2022, at: Link.

17 Junestherry Dela Cruz. (Jan. 17, 2023). *Trend Micro Research*. "Batloader Malware Abuses Legitimate Tools, Uses Obfuscated JavaScript Files in Q4 2022 Attacks." Accessed on Mar. 1, 2022, at: Link.

18 Ian Kenefick, Lucas Silva, and Nicole Hernandez. (Oct. 12, 2022). *Trend Micro Research*. "Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike." Accessed on Mar. 1, 2022, at: Link.

19 Trend Micro Research. (n.d.). *Trend Micro Research*. "What Is Apache Log4J (Log4Shell) Vulnerability?" Accessed on Mar. 1, 2022, at: Link.

20 Trend Micro Research. (n.d.). *Trend Micro Research*. "What Is Apache Log4J (Log4Shell) Vulnerability?" Accessed on Mar. 1, 2022, at: Link.

21 WP Editorial Staff. (n.d.). *WPBeginner*. "What is: Apache." Accessed on Mar. 1, 2022, at: Link.

22 VMWare. (n.d.). *Spring*. "Spring Framework." Accessed on Mar. 1, 2022, at: Link.

23 Sean Lyngaas. (Dec. 14, 2022). *CNN Politics*. "US warns hundreds of millions of devices at risk from newly revealed software vulnerability." Accessed on Mar. 1, 2022, at: Link.

24 Lily Hay Newman. (Aug. 11, 2022). *Wired*. "Sloppy Software Patches Are a 'Disturbing Trend'." Accessed on Mar. 1, 2022, at: Link.

25 Rae Hodge. (Apr. 23, 2020). *CNET*. "VPN use surges during the coronavirus lockdown, but so do security risks." Accessed on Mar. 1, 2022, at: Link.

26 David Fiser and Alfredo Oliveira. (Aug. 17, 2022). *Trend Micro Research*. "Analyzing the Hidden Danger of Environment Variables for Keeping Secrets." Accessed on Mar. 1, 2022, at: Link.

27 David Fiser and Alfredo Oliveira. (Mar. 9, 2021). *Trend Micro Research*. "TeamTNT Continues Attack on the Cloud, Targets AWS Credentials." Accessed on Mar. 1, 2022, at: Link.

28 Trend Micro. (Feb. 2, 2023). *Trend Micro Research*. "Research Exposes Azure Serverless Security Blind Spots." Accessed on Mar. 1, 2022, at: Link.

29 28. Ax Sharma. (May 24, 2022). *Bleeping Computer*. "Popular Python and PHP libraries hijacked to steal AWS keys." Accessed on Mar. 1, 2022, at: Link.

30 Trend Micro. (Jul. 13, 2022). *YouTube*. "Proof of Concept (POC): When Secrets Stored as an Environmental Variable are (Unwittingly) Leaked." Accessed on Mar. 1, 2022, at: Link.

31 Trend Micro. (Feb. 2, 2023). *Trend Micro Research*. "Research Exposes Azure Serverless Security Blind Spots." Accessed on Mar. 1, 2022, at: Link.

32 George Kalpudis. (Jan 2, 2023). *Coin Desk*. "What Will It Take for Bitcoin Mining Companies to Survive in 2023?" Accessed on Mar. 1, 2022, at: Link.

33 Alfredo Oliveira and David Fiser. (Sept. 10, 2023). *Trend Micro Research*. "War of Linux Cryptocurrency Miners: A Battle for Resources." Accessed on Mar. 1, 2022, at: Link.

34 Alfredo Oliveira and David Fiser. (Sept. 10, 2023). *Trend Micro Research*. "War of Linux Cryptocurrency Miners: A Battle for Resources." Accessed on Mar. 1, 2022, at: Link.

35 Alfredo Oliveira and David Fiser. (Dec. 1, 2022). *Trend Micro Research*. "Linux Cryptocurrency Mining Attacks Enhanced via CHAOS RAT." Accessed on Mar. 1, 2022, at: Link.

36 Liam Tung. (Jan. 17, 2022). *ZDNet*. "Linux malware is on the rise. Here are three top threats right now." Accessed on Mar. 1, 2022, at: Link.

37 Trend Micro. (Dec. 28, 2022). *Trend Micro Research*. "Improving Software Supply Chain Security." Accessed on Mar. 1, 2022, at: Link.

38 NIST. (n.d.). *NIST*. "Software Security in Supply Chains: Software Bill of Materials (SBOM)." Accessed on Mar. 1, 2022, at: Link.

For more information visit **trendmicro.com**