CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

February 8, 2024

Patterns and Targets for Ransomware Exploitation of Vulnerabilities: 2017–2023

Executive Summary

Ransomware groups' exploitation of vulnerabilities falls into two clear categories: vulnerabilities that have only been exploited by one or two groups and those that have been widely exploited by several groups. Each of these categories requires a different approach for defense and mitigation.

Threat actor groups alone in targeting certain vulnerabilities tend to follow specific targeting and weaponization preferences, allowing companies to prioritize network defenses and vendor audits. The best defense against groups that favor unique exploitation is to build a profile of their most likely targets, both in terms of products and vulnerability types.

Widely exploited vulnerabilities are in software frequently used in major enterprises. These vulnerabilities are often easily exploited through penetration testing modules or minimal lines of code focused on devices that accept HTTP/S requests. The best defenses against widespread exploitation are patching vulnerabilities as soon as patches are available, monitoring security research for simple proof-of-concept exploits, and monitoring criminal forums for references to tech stack components (rather than specific vulnerabilities).

Key Findings

- Ransomware groups alone in exploiting three or more vulnerabilities exhibit a clear targeting focus, which defenders can use to prioritize security measures. For example, CL0P has uniquely and infamously focused on file transfer software from Accellion, SolarWinds, and MOVEit. Other ransomware groups with high levels of unique exploitation exhibit similar patterns.
- All of the vulnerabilities ransomware groups have targeted most widely are in software frequently used by major enterprises and can be easily exploited via penetration testing modules or single lines of curl code. These vulnerabilities are ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207), ZeroLogon (CVE-2020-1472), Log4Shell (CVE-2021-44228), CVE-2021-34527, and CVE-2019-19781.
- Vulnerabilities requiring unique or custom vectors to exploit (for example, malicious files using particular forms of compression) are more likely to be exploited by only one or two groups.
- Ransomware operators and affiliates are highly unlikely to discuss specific vulnerabilities, but the cybercriminal ecosystem that supports them has discussed publicly known vulnerabilities and products as targets of interest for exploitation.

Our more ambitious forecasts for 2024 are as follows:

- Improvements in generative AI are likely to lower the technical threshold for cybercriminals to identify and understand how best to exploit vulnerabilities, allowing ransomware groups to exploit more zero-day vulnerabilities in a wider set of products.

- Ransomware campaigns will affect major vendors (for example, Google and Apple) that are typically immune from such threat activity since instances of threat actors exploiting zero-day vulnerabilities in both vendors' products have risen in the past few years.
- A rebound in the value of cryptocurrency will drive extortion groups away from vulnerability research and toward crypto wallet theft.

Methodology

Vulnerability exploitation has become a primary consideration in tracking the tactics, techniques, and procedures (TTPs) associated with ransomware operations. However, while there is a high volume of excellent research on ransomware's exploitation of individual, high-profile vulnerabilities, there is less accessible research on the number of ransomware groups associated with their exploitation.

To surface such patterns, we aimed to create a list of all vulnerabilities reportedly exploited by ransomware groups and then organize this list based on the number of groups reported to have exploited these vulnerabilities. We selected vulnerabilities for this list by using the Recorded Future platform to identify any reference in which ransomware and a vulnerability were co-mentioned. Since some high-profile vulnerabilities (like Log4Shell) are mentioned in hundreds of thousands of references, we added vulnerabilities to an exclusion list every time they were identified and verified. We therefore consider the resulting list of about 90 vulnerabilities to be a high-fidelity data source that appropriately controls for "noise" in the data.

We also examined the types of vulnerabilities exploited by ransomware groups based on their Common Weakness Enumeration (CWE) identifiers. Such identifiers are product-agnostic and help categorize vulnerabilities based on similar flaws in software development, such as flaws that allow heap overflow or occur during deserialization.

Threat / Technical Analysis

Based on analysis of a list of vulnerabilities exploited by ransomware groups in the past five years, we are confident in the following assessments:

- Ransomware groups alone in exploiting three or more vulnerabilities exhibit a clear targeting focus, which defenders can use to prioritize security measures.
- All of the vulnerabilities ransomware groups targeted most widely are in software frequently used by major enterprises and can be easily exploited via penetration testing modules or single lines of curl code.
    - These vulnerabilities are ProxyShell, ZeroLogon, Log4Shell, CVE-2021-34527, and CVE-2019-19781.

- Vulnerabilities requiring unique or custom vectors to exploit (for example, malicious files using particular forms of compression) are more likely to be exploited by only one or two groups.
- Ransomware operators and affiliates are highly unlikely to reference specific vulnerabilities, but the cybercriminal ecosystem that supports them has discussed publicly known vulnerabilities and products as targets of interest for exploitation.

The full list of 87 vulnerabilities we used for this report is available in Appendix A.

Unique Exploitation is Most Common and Demonstrates Unique Focuses

Ransomware exploitation of vulnerabilities has tended to cluster at one of two ends of a spectrum: vulnerabilities that only one group has exploited or vulnerabilities that numerous groups have exploited, such as ProxyShell.

A vulnerability is more likely to be exploited by only one or two groups than by three or more groups. Out of the 87 vulnerabilities in our list, 52% (46) have reportedly been exploited by only one group, 17% (15) have been exploited by two, and the remaining 31% (27) have been exploited by three or more. These numbers indicate a high degree of diversity in ransomware groups' targets over the last several years.

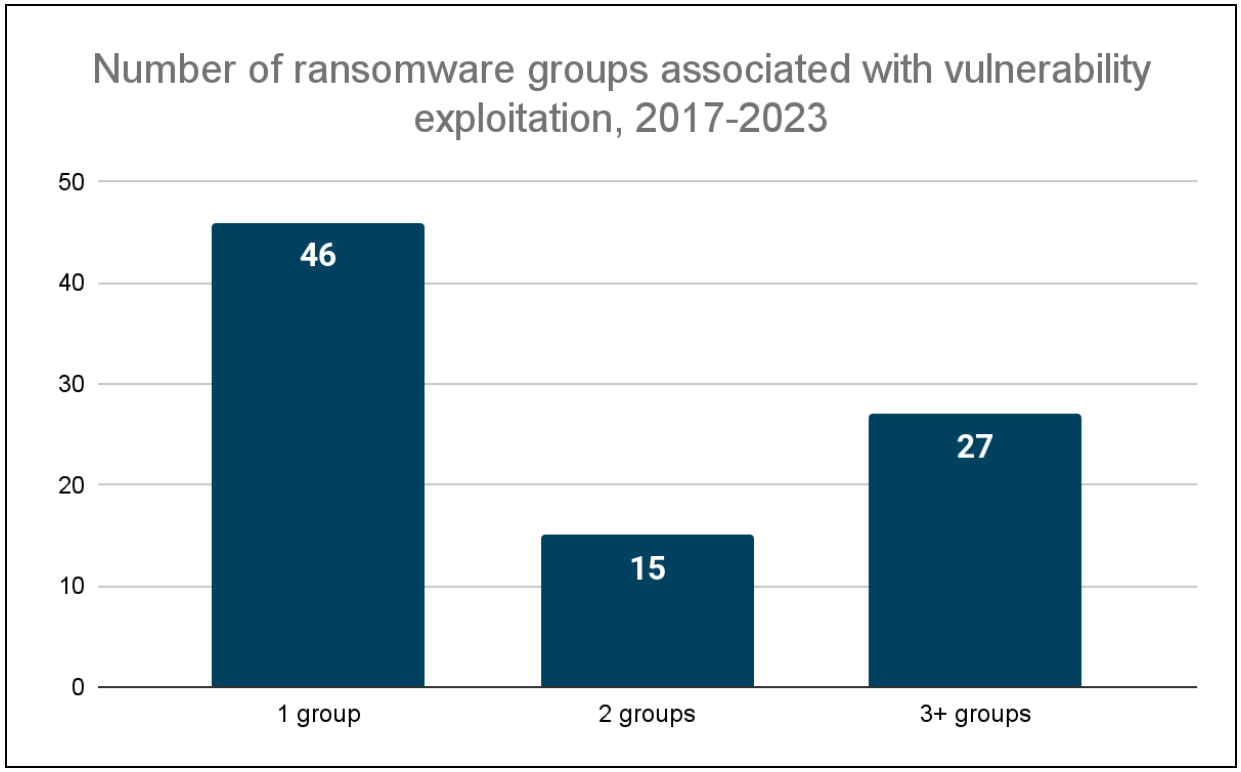

Figure 1: *Diagram showing the number of ransomware groups that have been associated with vulnerability exploitation in the last five years. By "one group", for example, we mean that only one group has been reported to have exploited a vulnerability (Source: Recorded Future)*

The ransomware variants that have been most associated with unique vulnerability exploitation are Magniber (four unique cases of exploitation), CL0P (three), ALPHV (three), and REvil (three). These unique cases demonstrate clear patterns of focus from each of these variants, as follows:

- Magniber has uniquely focused on Microsoft vulnerabilities, with half of its unique exploits focusing on Windows Smart Screen.
- CL0P has uniquely and infamously focused on file transfer software from Accellion, SolarWinds, and MOVEit.
- ALPHV has uniquely focused on data backup software from Veritas and Veeam.
- REvil has uniquely focused on server software from Oracle, Atlassian, and Kaseya.

In cyber threat research, encountering this level of consistency across a single attribute (in this case, the presence of a targeting focus) for a set of disparate threat groups is highly unusual. As a result, we can use it as a strong indicator that ransomware groups with unique targeting patterns are likely to continue these patterns. We can also use this indicator to prioritize network defenses for products most likely to fit within the targeting patterns. A compilation of the vulnerabilities uniquely exploited by these groups is available in Appendix B.

Another attribute that can help researchers understand targeting patterns is CWE identifiers given to vulnerabilities. Such identifiers are product-agnostic and categorize vulnerabilities based on similar flaws in software development, such as flaws that allow heap overflow or occur during deserialization.

The top three CWE identifications (IDs) for vulnerabilities exploited by ransomware groups are as follows:

- CWE-20 (Improper Input Validation): nine vulnerabilities
- CWE-22 (Improper Limitation of a Pathname to a Restricted Directory [“Path Traversal”]): nine vulnerabilities
- CWE-787 (Out-of-bounds Write): eight vulnerabilities

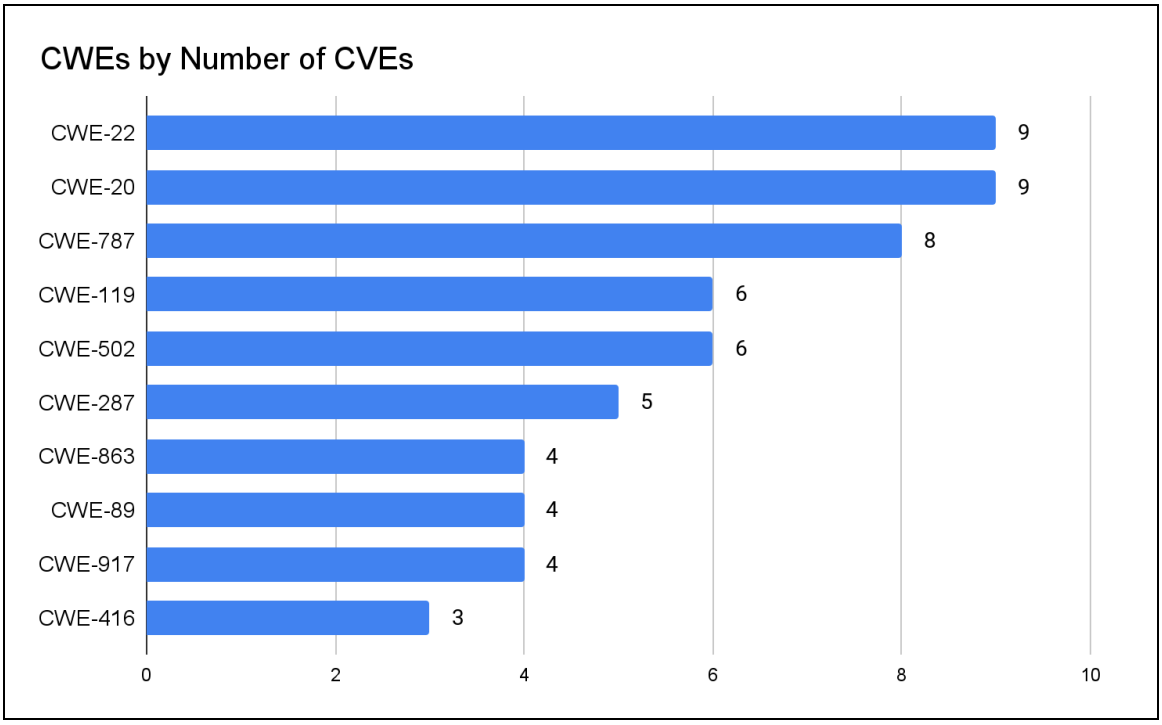

Figure 2: *Chart of the most common CWE identifiers associated with vulnerabilities exploited by ransomware groups, 2017-2023 (Source: Recorded Future)*

This result is not entirely surprising as it roughly aligns with broader patterns observed in the threat landscape. For instance, CWE-20, CWE-22, and CWE-787 all figured among the top ten CWEs on the Cybersecurity & Infrastructure Security Agency's (CISA) 2023 Top 25 Most Dangerous Software Weaknesses list, a ranking built from analyzing CVEs currently being exploited in the wild. CWE-787 took the first spot on CISA's ranking, while CWE-20 and CWE-22 took the 6th and 8th spots, respectively.

Based on a review of these CWE IDs, we are confident that if a vulnerability is only exploited by one group, it likely requires a custom-built package (a compressed file or application data, for example) and cannot simply be abused via a few lines of code.

- CVE-2019-0604 (CWE ID: 20), a vulnerability in Microsoft Sharepoint, has only been exploited in one ransomware campaign (WickrMe) per available evidence. Exploitation requires submitting malicious application package data.
- CVE-2023-47246 (CWE ID: 22), a vulnerability in Sysaid, has only been exploited in one ransomware campaign (CL0P) per available evidence. Exploitation requires a threat actor to submit a compressed WAR file webshell in a POST request to the target.
- CVE-2022-42475 (CWE ID: 787), a vulnerability in Fortinet's FortiOS, has only been exploited by one group (LockBit) per available evidence. Exploitation, per Fortinet, requires a "deep understanding of FortiOS and the underlying hardware".

Widespread Exploitation is Concentrated on Big Vendors and Easy Scripts

Across all vulnerabilities exploited by ransomware operations, five stood out as those that garnered the most threat actor attention, having been exploited by the highest number of individual ransomware threat actors. These vulnerabilities are ProxyShel, ZeroLogon, Log4Shell, CVE-2021-34527 — which affected Microsoft enterprise products such as Exchange, Netlogon, and Print Spooler — and CVE-2019-19781, which affected Citrix software. Microsoft's dominance here is unsurprising: As we have identified in previous reports, Microsoft is regularly the vendor most affected by zero-day exploitation and by ransomware overall, as about 55% of the vulnerabilities exploited by three or more groups were in Microsoft products.

The top five vulnerabilities also proved highly popular in the wider threat landscape once disclosed due to factors such as the high impact in terms of access or control over systems and the ubiquity of the affected software. For instance, nation-state groups and other non-ransomware cybercriminals were repeatedly observed targeting these vulnerabilities as part of their intrusion operations.

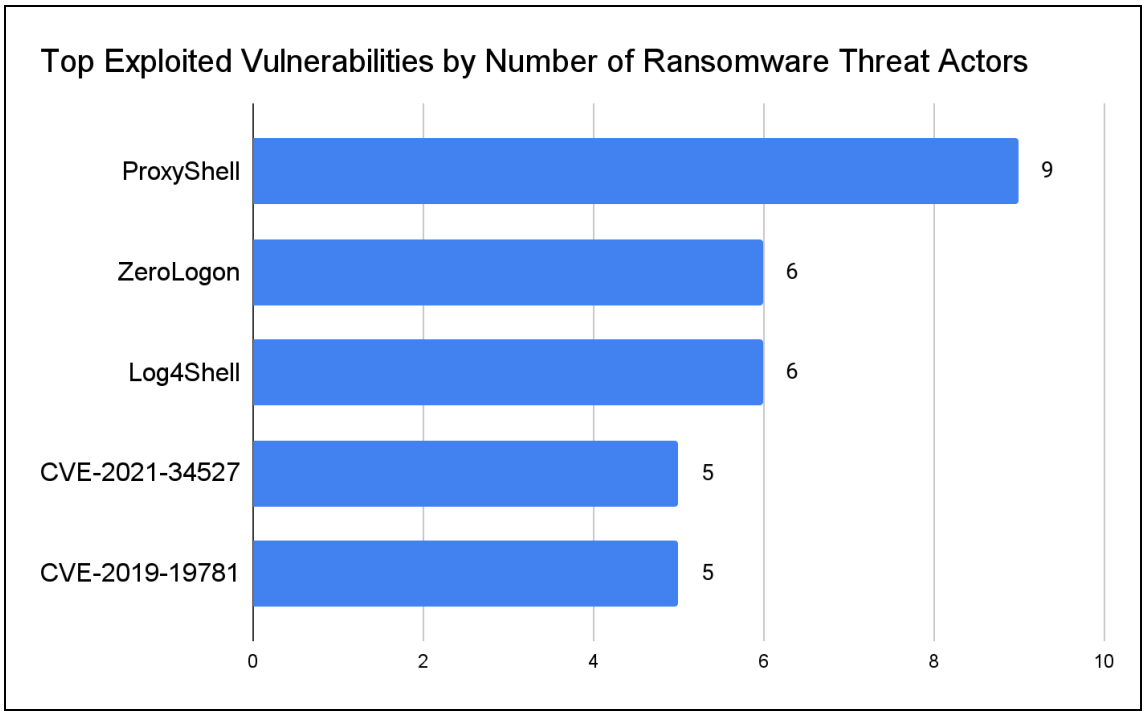

Figure 3: *Top ten vulnerabilities most exploited by ransomware threat actors (Source: Recorded Future)*

In the context of these top five, the dwell time for a vulnerability's exposure to and compromise by ransomware operators shows that organizations continue to fail at patching vulnerabilities in a timely manner. The average dwell time for the vulnerabilities above was seventeen months. The longest dwell time was for ZeroLogon, at 39 months between the vulnerability's initial disclosure (August 2020) and its most recently reported ransomware exploitation (November 2023, as an ongoing tactic reported by CISA for the Rhysida ransomware operation). In ZeroLogon's case, as is true for many other Microsoft

vulnerabilities, we suspect that the sheer market dominance of the Windows operating system (OS) means that organizations often struggle to effectively audit and patch all of their devices that run vulnerable versions of Windows.

Based on the same research approach to CWE IDs mentioned above, we also found that when many ransomware groups target a vulnerability, they do so almost always because it can be exploited with minimal lines of malicious code that can be easily implemented into mass scanning activity (through malicious HTTP requests, for example). This activity is the inverse of the previous pattern: ease of exploitation makes exploitation much more common.

While the initial discovery of these vulnerabilities can rely on an advanced understanding of a target product's syntax, configurations, and components, their exploitation by multiple ransomware groups usually relies on that initial discovery, leading to methods of target identification and compromise.

- Once leaked, ETERNALBLUE and other Server Message Block (SMB)-related vulnerabilities experienced widespread exploitation and have so far been associated with exploitation by at least seven ransomware groups. Identifying these vulnerabilities was part of advanced National Security Agency (NSA) operations, but their exposure and notoriety led them to be targeted via common penetration testing modules (for example, Metasploit).
- CVE-2019-19781, a vulnerability in Citrix ADC and Netscaler, has been exploited by up to five ransomware groups. Exploitation is possible with a few lines of curl code.
- CVE-2018-13379, a vulnerability in Fortinet's FortiOS, has been exploited by up to four ransomware groups. Exploitation is similarly possible with a few lines of curl code.

Widespread Product Targeting: Microsoft, Log4J, and Citrix Offer "Keys to the Kingdom"

The top five vulnerabilities ransomware groups exploit are in products with certain features that would make them highly attractive targets for cybercriminals. The ability to exploit any of these five allows ransomware operators to compromise millions of devices, many of them in use in enterprises. Exploits can also provide groups with immediate or easy access to accounts or platforms with administrative privileges.

Microsoft: A Huge Target Set

- Microsoft Exchange, an email and calendar server used by over 3.2 million companies worldwide, according to data from 6sense, is a notable case study as a total of eleven distinct ransomware groups proved their intent and capabilities to target vulnerabilities affecting it.
- ZeroLogon is a critical vulnerability in Windows Netlogon Remote Protocol (MS-NRPC), a key authentication component that supports user and machine account authentication in Active Directory (AD) environments. As such, ZeroLogon is particularly appealing to threat actors, especially ransomware groups, who can leverage full control over the domain controller to steal sensitive information and spread ransomware payloads across an entire network.

- Windows Print Spooler is enabled by default on all Windows-based systems, including on domain controllers and machines with system admin privileges, potentially exposing all devices on a network to compromise should these be successfully targeted.

Log4J: Another Huge Target Set

- Log4Shell affects Apache Log4j, one of the most widely adopted software logging libraries. Due to its ease of exploitation, which allows remote access, and widespread use of Log4j across networks and applications, Log4Shell attracted significant exploitation activity following its disclosure in December 2021.

Citrix: Common in Big Companies

- Citrix products are reportedly used by over 400,000 clients worldwide, including 99% of Fortune 100 companies and 98% of Fortune 500 companies. Furthermore, Citrix ADC and Gateway are "edge devices" sitting at a network's perimeter, designed to manage web traffic and ensure secure remote access. If successfully compromised, these edge devices can allow initial access to enterprise resources without any user interaction, reducing the chances of detection. Furthermore, edge devices are typically difficult to monitor and might not support endpoint detection and response (EDR) solutions or other security methods to identify malicious activity and log collection for analysis, further reducing methods to detect modifications or collect forensic images.

Ransomware Groups Avoid Discussing Vulnerabilities, but Their Criminal Ecosystems Share Vulnerability News

As much as cybersecurity professionals share intelligence on vulnerabilities, threat actors also share publicly announced vulnerabilities across criminal sources. The same websites, specifically cybersecurity-related news outlets used by professionals for awareness and alerting on cybersecurity issues, are also being perused by threat actors. Many of today's most active forums have members who readily post open-source intelligence (OSINT) articles related to vulnerabilities, zero-days, and active exploitation, such as "tabac" (on XSS Forum, with nineteen references over the last year).

When examining the activities on these monikers and their postings of publicly known vulnerabilities to forums, we identified sixteen CVEs not only referenced across criminal forums but also exploited by ransomware-as-a-service (RaaS) members (Table 1). This discovery is important because RaaS members do not declare their affiliation statuses openly, nor the number of affiliated members per RaaS variant. However, we do know that cybercriminals who are RaaS affiliates are on these criminal sources and can use these media postings to facilitate their interest in exploiting a vulnerability.

CVE Discussed on Criminal Forums	RaaS Variant Exploiting Vulnerability
CVE-2019-19781	REvil, Doppelpaymer (Grief), CL0P, Ragnarok
CVE-2020-1472 (ZeroLogon)	Ryuk, Cuba, Conti, BlackBasta (ALPHV), RansomExx, Mailto
CVE-2012-0158	Mailto, LockBit
CVE-2016-4117	Cerber
CVE-2018-8453	REvil
CVE-2021-44228 (Log4Shell)	Conti, Doppelpaymer, LockBit, AvosLocker, DEV-0401
CVE-2019-0859	N/A
CVE-2021-34527	BlackBasta, Conti, Vice Society, Cerber
CVE-2019-11510	REvil, Black Kingdom, Malito
CVE-2019-3396	REvil
CVE-2019-0604	N/A
CVE-2019-7195	eCh0raix
CVE-2021-40539	Hive
CVE-2021-26855 (ProxyLogon)	Black Kingdom
CVE-2020-0796	Conti, Malito
CVE-2020-12812	Hive
CVE-2018-13379	REvil, Conti, LockBit
CVE-2021-40444	Conti, Ryuk

Table 1: *Vulnerabilities discussed on criminal forums which have also been exploited by RaaS variants.*

There are multiple ways ransomware groups can compromise networks. They regularly obtain initial network access through the use of infostealers, botnets, purchased login credentials on the dark web, exploitation of zero-day vulnerabilities, third-party software (primarily virtual private networks [VPNs], Citrix, and Microsoft Remote Desktop), web shell attacks, and occasionally other methods, including insider access. In addition, ransomware operators often perform reconnaissance activities to acquire their own victims. Mass scanning and vulnerability assessment are widely used to identify victim networks vulnerable to exploitation or with weaknesses associated with remote access services. Operators also rely on and privately work with initial access brokers (IABs), who take a predetermined

percentage of the victim's payment as compensation and provide the operators working access to a victim's network.

Analysis of dark web forums offering ransomware-related advertisements, such as top-tier forum Ramp and low-tier forums BreachForums 2 and Ransomed Forum, indicates that representatives of ransomware operators do not list the vulnerabilities they use to target victims while hiring affiliate members. They only specify the key technical functionality of their ransomware families and the products they target. Among the most vulnerable products are Windows and Linux OSs and EXSi VMware software.

Mitigations

Based on the findings and assessments above, we consider the following to be the most effective defenses against ransomware operators' exploitation of vulnerabilities:

- Unless necessary, ensure that devices and networks cannot receive incoming requests on ports 80 (HTTP) and 443 (HTTPS). The highest-volume ransomware exploitation of vulnerabilities shows a clear preference for critical vulnerabilities that can be exploited via a few lines of code against devices that can receive HTTP/S requests. We found this to be particularly true in the case of path traversal vulnerabilities.
- Monitor security researcher articles, blogs, and code repositories for references to simple exploit syntax based on HTTP/S requests (such as curl code). This information can be used to set up detections for exploit attempts against devices that need to remain publicly accessible.
- For ransomware groups of concern, identify whether and where such groups have uniquely targeted vulnerabilities to build a profile of most likely targets, both in terms of products and vulnerability types. For example, organizations worried about CL0P should prioritize higher security measures against SQL injection in file transfer software. Alternatively, organizations worried about ALPHV should prioritize authentication hardening for data backup software.
- Patch widely exploited and critical vulnerabilities as fast as possible. The dwell time statistics above demonstrate that ransomware groups can exploit victims' vulnerable infrastructure over three years after a vulnerability's disclosure.
- Don't use criminal forum monitoring as a reliable way to identify ransomware groups' interest in specific vulnerabilities since these groups rarely discuss such vulnerabilities. Additionally, don't rely on alerts of criminal mentions of CVE identifiers, since criminals usually discuss CVE identifiers only after exploitation has occurred. Instead, monitor for criminal discussions of *vendors* and *products* of concern.

Outlook

It would be easy to summarize unsurprising predictions for the next year, such as Microsoft remaining a primary target of vulnerability exploitation or ransomware groups continuing to attempt to exploit vulnerabilities at scale. These predictions are useful for reinforcing organizations' attention to the fundamentals of network security, which do not generally change.

That said, organizations that have strong security plans to combat the most common TTPs associated with ransomware may, therefore, find value in our more ambitious forecasts for this topic, which are as follows:

- Improvements in generative AI will likely lower the technical threshold for criminals to identify and understand how best to exploit vulnerabilities. This development will lead to a criminal ecosystem in which vulnerability exploitation affects more zero-day vulnerabilities in a wider target set of products.
- Exploitation of zero-day vulnerabilities in Google and Apple products has been rising over the past few years, although typically with few details released about the threat actors involved. Based on this and other indicators of attackers' interest in these vendors, we expect that a major ransomware campaign abusing a Chrome or MacOS/iOS vulnerability is increasingly likely over the next year.
- Potentially contrasting both of the previous predictions, a rebound in the value of cryptocurrency (particularly Bitcoin) is more than likely to drive some existing ransomware and extortion groups to attempt direct theft of funds from cryptocurrency wallets rather than investing in operations that achieve cryptocurrency payments only after successful compromises and negotiations with extortion victims. This scenario would, in turn, likely direct resources away from criminal vulnerability research, stabilizing or lowering the rates of vulnerability exploitation over the year.

Appendix A: Vulnerabilities Exploited in Ransomware Campaigns, 2017-2023

CVE Identifier	Affected Vendor/Product	Ransomware Targeting
CVE-2012-0158	Microsoft Office, Microsoft SQL Server	Mailto, Estemani, Spartacus, LockBit, EDA2
ProxyShell (CVE-2021-34523)	Microsoft Exchange	Babuk, Hive, COBALT MIRAGE, Cuba, LV, LockBit, BlackByte, Conti
ProxyShell (CVE-2021-34473)	Microsoft Exchange	Babuk, Hive, COBALT MIRAGE, Cuba, LV, LockBit, BlackByte, Conti
ProxyShell (CVE-2021-31207)	Microsoft Exchange	Babuk, Hive, COBALT MIRAGE, Cuba, LV, LockBit, BlackByte, Conti
ZeroLogon (CVE-2020-1472)	Microsoft's Netlogon Remote Protocol	Cuba, Conti, Play, Mailto, RansomEXX, Black Basta, Ryuk
Log4Shell (CVE-2021-44228)	Log4j	DEV-0401, Avos Locker, COBALT MIRAGE, DoppelPaymer, LockBit, Conti
CVE-2021-34527	Windows Print Spooler	Vice, Conti, Cerber, Big Boss Horse, Black Basta, Magniber
CVE-2017-11882	Microsoft Office	REvil, Ryuk, DarkSide, Sekhmet, ALPHV, CCryptor
CVE-2019-19781	Citrix Application Delivery Controller (ADC)	DoppelPaymer, Cl0p, Ragnarok, Maze, REvil
CVE-2018-8174	Windows VBScript Engine	Buran, Gandcrab, Cuba, Magniber, Maze
CVE-2017-0143	Windows SMB	Petya, Ryuk, Satan, Conti, Wcry
CVE-2023-27350	PaperCut NG	Clop, Bl00dy, LockBit, Buhti
CVE-2018-4878	Adobe Flash Player	Paradise, GandCrab, Maze, Sodinokibi
CVE-2018-13379	Fortinet FortiOS	LockBit, REvil, Conti, Cring
CVE-2017-0145	Windows SMB	Petya, Bad Rabbit, NotPetya, Wcry
CVE-2016-4117	Adobe Flash Player	Cerber, Mole, Erebus, CryptXXX
CVE-2023-0669	GoAnywhere MFT	ALPHV, LockBit, Cl0p

CVE-2022-26134	Atlassian Confluence Server and Data Center	GandCrab, AvosLocker, Cerber
CVE-2021-40444	Microsoft MSHTML	Magniber, Ryuk, Conti
CVE-2021-27065	Microsoft Exchange Server	Kingdom Kingdom, Babuk, DearCry
CVE-2021-26411	Internet Explorer	AvosLocker, ALPHV, Magniber
CVE-2021-20016	SonicWall SSLVPN SMA100	Darkside, HelloKitty, Five Hands
CVE-2020-0796	Microsoft Server Message Block	Conti, Blue Sky, Mailto
CVE-2020-0609	Windows Remote Desktop Gateway	Egregor, Conti, REvil
CVE-2019-7481	SonicWall SMA100	ESXiArgs, LockBit, HelloKitty
CVE-2019-5544	VMware ESXi	RansomX, Babuk, Darkside
CVE-2019-11510	Pulse Connect Secure	Mailto, REvil, Black Kingdom
CVE-2017-0213	Windows COM	Nefilim, Ragnar Locker, Dharma
CVE-2016-7255	Win32k	Magniber, Cerber, GandCrab
ProxyNotShell (CVE-2022-41082)	Microsoft Exchange	Cuba, Play
ProxyNotShell (CVE-2022-41040)	Microsoft Exchange	Cuba, Play
ProxyLogon (CVE-2021-26855)	Microsoft Exchange	BlackKingdom, DearCry
ETERNALBLUE (CVE-2017-0144)	Microsoft SMBv1 server	(Not)Petya, Wcry
CVE-2022-41080	Microsoft Exchange Server	Cuba, Play
CVE-2022-24521	Windows Common Log File System Driver	Vice, Cuba
CVE-2021-28799	QNAP NAS	QLocker, eCh0raix
CVE-2021-26084	Atlassian Confluence Server and Data Center	Cerber, AtomSilo
CVE-2021-21974	VMware ESXi	RansomExx2, ESXiArgs
CVE-2021-21972	VMware vCenter Server	ESXiArgs, Memento
CVE-2019-11043	PHP	NextCry, DeadBolt
CVE-2018-8453	Win32k	REvil, Maze
CVE-2018-19320	GIGABYTE APP Center	RobbinHood, AvosLocker
CVE-2018-15982	Adobe Flash Player	Maze, Egregor
CVE-2016-0189	Microsoft JScript	NEMTY, Matrix
CVE-2023-20269	Cisco VNP	Akira, LockBit
CVE-2023-27351	PaperCut Multifunction (MF) and Next Generation (NG) software	Cl0p, LockBit, Bl00dy

CVE-2023-27532	Veeam Backup & Replication software	Cuba
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway	LockBit, ALPHV
CVE-2023-47246	SysAid	CL0P
CVE-2023-46604	Apache ActiveMQ OpenWire	HelloKitty
CVE-2023-40044	Progress WS_FTP	Reichsadler Cybercrime Group (LockBit variant, not real LockBit)
CVE-2023-36884	Windows Search	RomCom (Storm-0978)
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway	ALPHV
CVE-2023-34362	Progress MOVEit Transfer	CL0P
CVE-2023-28252	Windows Common Log File System (CLFS)	Nokoyawa
CVE-2023-24880	Windows SmartScreen	Magniber
CVE-2023-22518	Atlassian Confluence	Cerber
CVE-2023-22515	Atlassian	Cerber
CVE-2023-0669	GoAnywhere MFT	CL0P
CVE-2022-47986	IBM Aspera Faspex File Sharing	IceFire
CVE-2022-47966	Zoho ManageEngine	Bhuti
CVE-2022-44698	Windows SmartScreen	Magniber
CVE-2022-42475	FortiOS SSL-VPN	LockBit
CVE-2022-41352	Zimbra Collaboration	Rorschach
CVE-2022-29499	Mitel MiVoice Connect	Lorenz
CVE-2022-27593	QNAP NAS	Deadbolt
CVE-2022-27510	Citrix Gateway	Royal
CVE-2022-26352	ContentResource API in dotCMS	Ghost
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager	RAR1
CVE-2021-45105	Apache Log4j2	AvosLocker
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus	Hive
CVE-2021-35211	SolarWinds Serv-U	CL0P
CVE-2021-30116	Kaseya Virtual System/Server Administrator	Revil
CVE-2021-27878	Veritas Backup Exec	ALPHV

CVE-2021-27876	Veritas Backup	ALPHV
CVE-2021-27101	Accellion FTA	CL0P
CVE-2020-5135	SonicOS	Babuk
CVE-2020-36195	QNAP NAS	QLocker
CVE-2020-12812	SSL VPN in FortiOS	Hive
CVE-2019-7192	QNAP QTS and Photo Station	eCh0raix
CVE-2019-3396	Atlassian Confluence Server	Revil
CVE-2019-2725	Oracle WebLogic Server	Revil
CVE-2019-18935	Progress Telerik UI	Mailto (NetWalker)
CVE-2019-16098	MSI Afterburner	BlackByte
CVE-2019-15846	Exim	Lilocked
CVE-2019-1367	Internet Explorer	Magniber
CVE-2019-0604	Microsoft SharePoint	WickrMe
CVE-2018-8120	Win32k	GandCrab
CVE-2018-2894	Oracle WebLogic Server	Satan
CVE-2018-19943	QNAP NAS	eCh0raix (QNAPCrypt)
CVE-2017-0147	Windows SMB	Wcry
CVE-2015-2546	Microsoft Windows	Magniber
CVE-2015-1701	Win32k	Mailto (NetWalker)
CVE-2013-0213	Samba Web Administration Tool	Dharma
CVE-2009-3960	Adobe BlazeDS	Cring

Appendix B: Sets of Vulnerabilities Uniquely Exploited by Ransomware Groups

Magniber

- CVE-2015-2546
- CVE-2019-1367
- CVE-2022-44698
- CVE-2023-24880

CL0P

- CVE-2021-27101
- CVE-2021-35211
- CVE-2023-34362

ALPHV

- CVE-2021-27876
- CVE-2021-27878
- CVE-2023-27532

REvil

- CVE-2019-2725
- CVE-2019-3396
- CVE-2021-30116

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com