SPOTLIGHT

CSW Cyber SecurityWorks | CYWARE™ | ivanti

Ransomware

Through the Lens of Threat and Vulnerability Management

2022

Table of Contents

About This Report 1
Executive Summary 2
Top 10 Ransomware Findings in 2021 3
Tremendous Increase (29%) in Vulnerabilities (CVEs) Tied to Ransomware 3
Amplified Alerts and Emphasis on Cyber Hygiene 3
Zero-Day Vulnerabilities on the Target Radar 3
Increasing Incidents Compromising Supply Chains 4
Not All Ransomware Vulnerabilities Caught by Scanners 4
Critical Sectors Attacked with Devastating Impacts 4
Vulnerabilities Chained for the Maximum Impact 4
Vulnerabilities in End-of-Life Products Exploited 5
Latency Analysis—A Wake-Up Call to the Vulnerability Patching Approach 5
Software Weakness Giving Rise to Ransomware Vulnerabilities 5
Risk-Based View of Ransomware Vulnerabilities 6
Ransomware Vulnerabilities 7
Weaponization Analysis 8
CVSS Analysis 9
CWE Analysis 10
Old Vulnerabilities Tied to Ransomware 12
APT Groups Associated with Ransomware 13
Ransomware Families 13
Exploit Kits 14
Ransomware Trends and Our Analysis 15
Repeatedly Targeted Vulnerabilities 16
Top Six Disturbing Ransomware Trends 17
Zero-Day Vulnerabilities 17
Third-Party and Supply Chain Attacks 18
Vulnerability Chaining 20
Vulnerabilities in End-Of-Life Products 21
Service Offerings 22
Attack Vector Trends 23
A Latency Analysis 25
Vendors under Attack 28
Ransomware Groups That Stand Out 30
Ransomware Data Leaks 33
Vulnerable Sectors and Product Categories 35
Other Noteworthy Vulnerabilities 39
Trends to Watch Out For 40
Summary 40
Report Methodology 43
About Us 44
Appendix 46

About This Report

Since we published our 2021 Spotlight Report and index updates (1, 2, and 3) that highlighted key metrics, we have been tracking ransomware threats. We have been able to warn organizations and product vendors about ransomware threats and the specific vulnerabilities these threats are targeting through these reports.

This report brings you trends that we have noticed in the past year regarding the type of vulnerabilities that the attackers are going after, the CWEs that are churning out the most number of weaknesses, and the myriad ways in which ransomware is being used to attack organizations.

This year, we have partnered with two companies to bring forth this report—Ivanti and Cyware. This joint effort exponentially expands our efforts to provide organizations with critical insights into ransomware threats.

1 Executive Summary

Our dynamic and continued ransomware research focuses on vulnerabilities and the methods used by ransomware groups to instigate crippling attacks. In 2021, we noticed ransomware groups continue to leverage any gaps in software weaknesses, from scouting for yet-to-be recognized vulnerabilities to those that fly under the radar, weaponizing them in record time. We also observed a definitive intent to broaden their attack sphere, focusing their efforts on newer ways to compromise organizational networks and fearlessly trigger high-impact assaults.

In the wake of growing ransomware threats, a commissioned study conducted by Forrester Consulting on behalf of Cyware indicates organizations are looking to improve threat detection, incident response, and data accessibility amongst teams and automate security processes while unifying cybersecurity solutions. Furthermore, they are willing to invest in solutions that offer threat intelligence, incident response, case management, intelligence sharing, and vulnerability assessment in the coming year. Our ransomware research serves as the first step in this direction.

This Spotlight Report provides actionable insights and data that help security teams prioritize patching. This report provides high-level insights—for leaders and their organizations—that could shape future decisions and help defend their environment from crippling attacks.

Top 10 Ransomware Findings in 2021

This section highlights the key ransomware findings that we tracked in 2021. Organizations must take heed of these observations and prioritize remediation for all potential access vectors arising from these findings, directly or indirectly.

1. Tremendous Increase (29%) in Vulnerabilities (CVEs) Tied to Ransomware

Unpatched vulnerabilities are the most prominent attack vectors exploited by ransomware groups and threat actors alike. While we had 223 vulnerabilities associated with ransomware in 2020, we noticed a 29% growth in 2021, taking the total vulnerability count to 288. Alarmingly, over one-third of these 65 newly added vulnerabilities are being actively searched (therefore, trending) on the internet, adding additional emphasis on prioritizing and addressing these vulnerabilities.

2. Amplified Alerts and Emphasis on Cyber Hygiene

The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and other security agencies have been consistently warning organizations and public sector companies about fixing vulnerabilities that have become pet favorites of ransomware gangs and Advanced Persistent Threat (APT) groups. Of the 288 ransomware CVEs, security agencies have put out multiple warnings for 66 of them, restressing the importance of prioritizing patches for these vulnerabilities on an immediate basis. CISA also recently released a binding directive that forces the hand of public sector companies to patch a specific list of vulnerabilities complete with strict deadlines. This list alone features 20% of the 288 ransomware vulnerabilities.

3. Zero-Day Vulnerabilities on the Target Radar

One of the consistent trends that we noticed this year was the exploitation of zero-day vulnerabilities. QNAP vulnerability (CVE-2021-28799), Sonic Wall (CVE-2021-20016), Kaseya (CVE-2021-30116), and—more recently—Apache Log4j (CVE-2021-44228) were exploited even before they made it to the National Vulnerability Database (NVD). This dangerous trend highlights the need for agility in disclosing vulnerabilities and releasing patches based on priority.

4. Increasing Incidents Compromising Supply Chains

We have seen consistent instances of ransomware going after supply chains. Be it a third-party application (VPN in the Colonial Pipeline attack), a vendor-specific product (Kaseya VSA server), or even an open-source library (Apache Log4j), organizations are being hit where it hurts the most. A single compromise is opening up multiple avenues for threat actors to hijack complete system distributions across hundreds of victim networks and, thereby, spreading chaos and panic.

5. Not All Ransomware Vulnerabilities Caught by Scanners

We compared popular scanners—Nessus, Qualys, and Nexpose—to identify if they could detect the ransomware vulnerabilities. Here are the results of our findings:

- Only 92.7% of the 288 vulnerabilities were detected by all scanners combined.
- The number of ransomware vulnerabilities that none of the scanners could not detect stands at 21.
- All three scanners could detect 77% of the 288 vulnerabilities.

Note: The Appendix provides the list of ransomware vulnerabilities not detected by any of the three scanners. Ensure to patch them before a breach.

6. Critical Sectors Attacked with Devastating Impacts

Attacks on critical services such as oil & gas, food, pharmacy, and health care are crippling states and prompting governments to take unprecedented measures. The impact of attacks on Colonial Pipeline, JBS Meat Packers, Oldsmar's (Florida) water plant, and Springhill Medical Center was severe, and people on the streets were affected by these attacks. The unprecedented impact of these attacks compelled the US government to issue warnings that any further attack on critical sectors would be considered as "acts of war."

7. Vulnerabilities Chained for the Maximum Impact

Ransomware threat actors have been utilizing groups of vulnerabilities chained together for the maximum impact. We observed the PetitPotam CVE (CVE-2021-36942) had been chained together with the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207). We noted another chain of vulnerabilities: the set of four ProxyLogon vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065). Each of the vulnerabilities chained together seems to serve a specific purpose, from gaining initial access to allowing for deeper network penetration.

8. Vulnerabilities in End-of-Life Products Exploited

Our research also uncovered prominent instances of ransomware groups such as Cring (CVE-2009-3960 and CVE-2010-2861) and HelloKitty (CVE-2019-7481) going after vulnerabilities in products that had reached the end of their life and thus would not be updated or supported by the respective vendors. Realizing the risks involved in the continued usage of such products, CISA has marked this as one of the bad practices that could affect critical infrastructure or national critical functions.

9. Latency Analysis—A Wake-Up Call to the Vulnerability Patching Approach

Our analysis of ransomware vulnerabilities brought out some important findings.

- It is important to look beyond the NVD and keep an eye out for vulnerability trends, exploitation instances, vendor advisories, and alerts from security agencies while prioritizing the vulnerabilities to patch.
- Exploitation trends are becoming more sophisticated and impactful, with ransomware groups exploiting vulnerabilities within days of being identified.
- Vulnerabilities once associated with ransomware are perpetually just one step away from being used to launch highly impactful attacks.
- Any upgrades or patches must be applied on priority as even patched vulnerabilities can sometimes become inefficient with newer access points being identified.

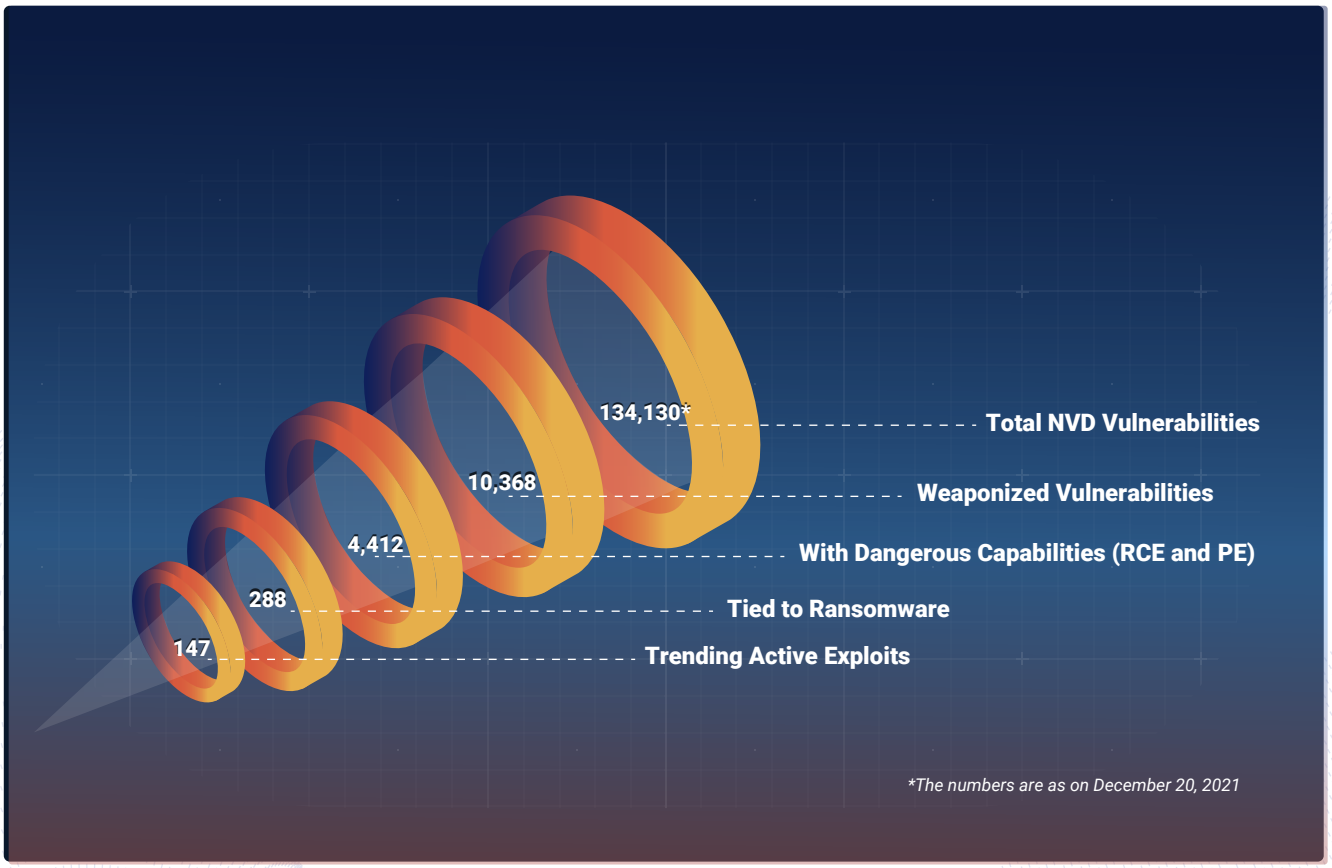
10. Software Weakness Giving Rise to Ransomware Vulnerabilities

Today, we have a total of 54 weaknesses in code that ransomware groups have exploited. This includes two new weaknesses—CWE-190 and CWE-77—added since the Ransomware Q3 Index Report 2021 was published in November 2021.

The responsibility is with code developers to ensure they do not include pieces of code that could give rise to these weaknesses, which actors with malicious motives could then exploit.

2 Risk-Based View of Ransomware Vulnerabilities

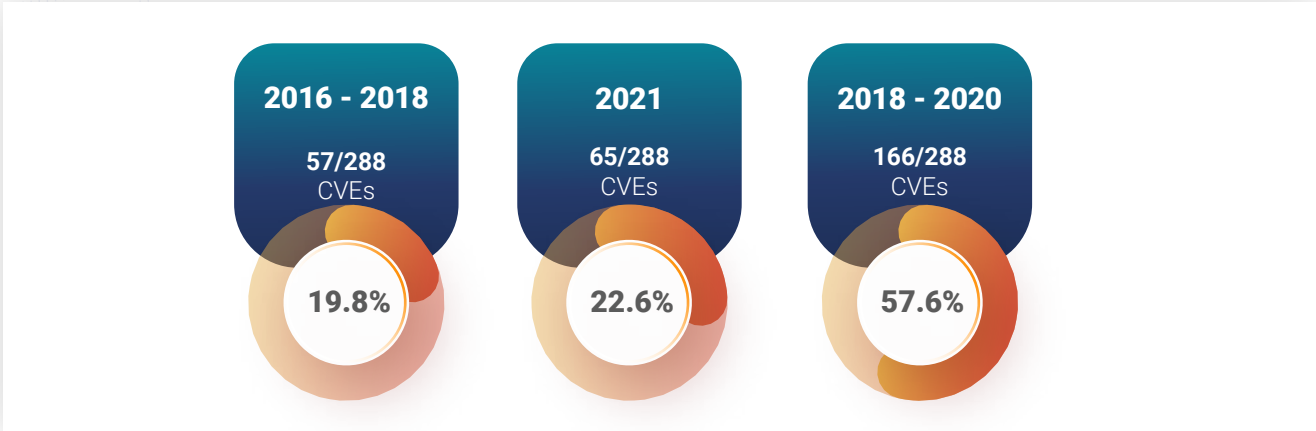
The NVD has added 22,384 vulnerabilities since 2020, and that is an average of 61 vulnerabilities disclosed every day. To wade through this sea of vulnerabilities, we adopt a risk-based approach that maps them to real-world threats. Such an approach helps security practitioners plan their patching cadence so that organizations can address weaknesses that can impact them the most. Here, we analyze the 22,834 vulnerabilities identified in 2021 and focus on the subset that has ransomware associations.



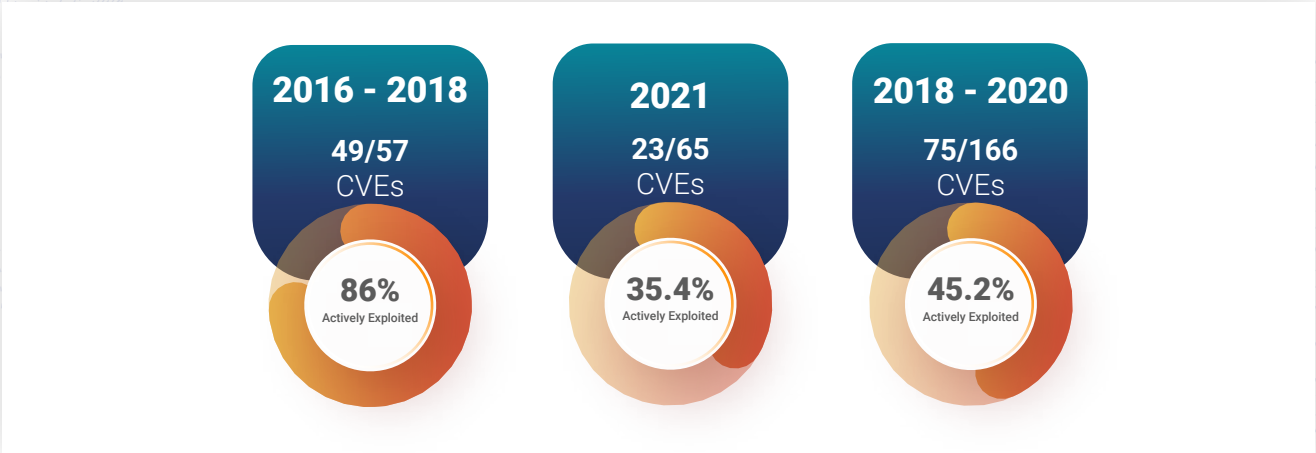
Note: Our ransomware report is updated periodically with relevant changes and highlights based on our continued research and dynamic analysis of ransomware trends and markers.

Ransomware Vulnerabilities

Our research regularly tracks vulnerabilities that are exploited by ransomware and the groups behind these exploits. While we had 223 vulnerabilities associated with ransomware in 2020, we identified 65 new ransomware vulnerabilities, a 29.1% increase in a single year in 2021. This outweighs the 26.9% increase observed between 2016 and 2018 and will most definitely cross the 39.9% that was observed between 2018 and 2020 by 2022.



Also, 36.92% of these newly added vulnerabilities have been actively trending in the dark web and have been repeatedly exploited. While this percentage increase in actively exploited vulnerabilities has reduced from 66.29% to 36.92%, the impact of the newly exploited vulnerabilities has been multifold and crippling, owing to the sophisticated methods and harmful intent of ransomware groups. Parallelly, 55.6% of the 223 vulnerabilities identified earlier continue to be actively exploited by ransomware groups.



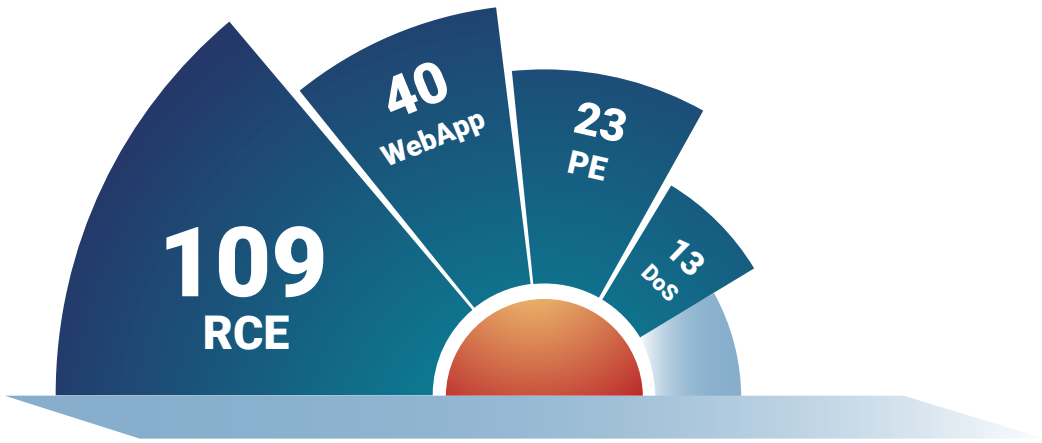
Note: While the primary focus of this year's ransomware report is the vulnerabilities between 2010 and 2021, we would like to highlight five outliers. These were published between 2007 and 2009, but we found them actively trending during our research spanning 2010–2020.

CVE-2007-1036
CVE-2009-0824
CVE-2008-2992
CVE-2009-3960
CVE-2008-3431

These are now included in our totals for CVEs tied to ransomware.

Weaponization Analysis

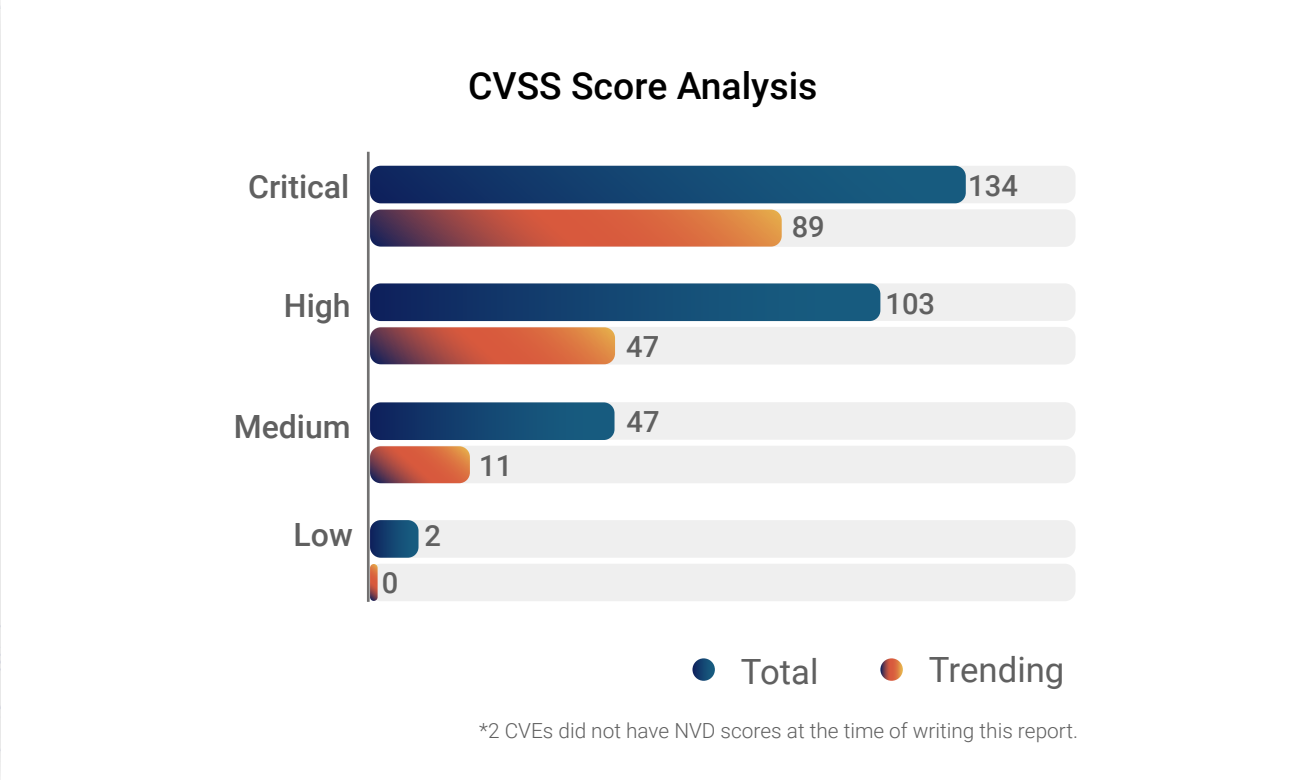
Exploit codes are built to take advantage of a vulnerability and are the deciding factor in classifying a vulnerability as weaponized. Public exploit codes are available for 57% (164) of ransomware vulnerabilities. Of these, 109 vulnerabilities can be exploited remotely (Remote Code Execution), a dangerous exploit category. The exploit vulnerabilities also include 23 vulnerabilities capable of privilege escalation, 13 vulnerabilities that can lead to denial-of-service attacks, and 40 vulnerabilities capable of exploiting web applications.



Weaponization Analysis

CVSS Analysis

Organizations worldwide follow the Common Vulnerability Scoring System (CVSS) to prioritize and patch their vulnerabilities. When we analyzed the 288 ransomware vulnerabilities from the perspective of the CVSS, we found that 26.73% belong to the critical category and 30.9% belong to the high severity category. Interestingly, we noticed that 10% of the vulnerabilities had a medium severity rating, and one vulnerability had a low score. Organizations that patch only critical vulnerabilities solely based on the CVSS v3 would miss out on addressing 73.61% of ransomware vulnerabilities, 49% of which are trending.



*2 CVEs did not have NVD scores at the time of writing this report.

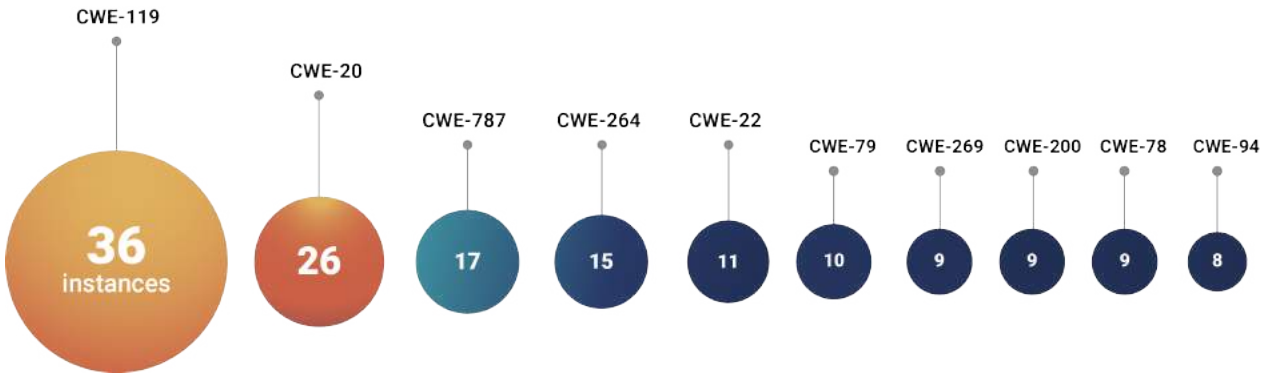
The numbers reaffirm our case for a risk-based vulnerability analysis that looks beyond the NVD CVSS alone. In addition to targeting critical vulnerabilities, ransomware groups have their eyes on those that are traditionally not recognized as severe, and this calls for a similar shift in systemic vulnerability management as well.

CWE Analysis

Our researchers studied the software weaknesses that gave rise to vulnerabilities that ransomware groups target. Here are the top five Common Weakness Enumerations (CWEs) that are contributing to ransomware vulnerabilities:

CWE	Description	Count of CVEs	OWASP 2021 Rank	MITRE 2021 Rank
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	36	NA	17
CWE-20	Improper Input Validation	26	A03	4
CWE-787	Out-of-Bounds Write	17	NA	1
CWE-264	Permissions, Privileges, and Access Controls	15	A01	NA
CWE-22	Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)	11	A01	8

The top five weaknesses listed here account for almost 40% of all vulnerabilities tied to ransomware. Of these, CWE-119 and CWE-20 continue to retain the top two spots since our analysis for 2018–2020 ransomware vulnerabilities. While CWE-264 has moved one spot below to fourth in the ranking, CWE-787 and CWE-22 have replaced CWE-94 and CWE-200 in the top five list since.



CWE analysis of Ransomware Vulnerabilities

We have also had two new weaknesses making their way to the ransomware list since our Q3 2021 Index Report.

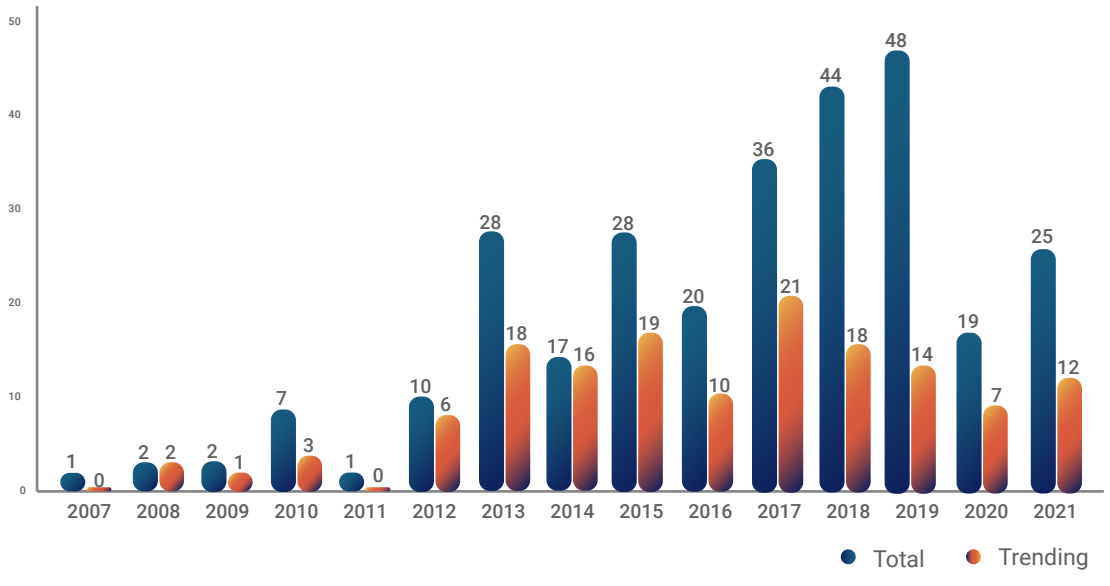
- CWE-190, an integer overflow or wraparound weakness, is related to incorrect calculation of the integer size, wrapping around to a smaller integer. When this occurs unexpectedly, it can have security consequences if used for resource management or execution control. CWE-19 ranks twelfth on MITRE's top weaknesses for 2021.
- CWE-77 is a command injection weakness that can result in improper neutralization of special elements used in a command, which could modify the intended command to a downstream component. The weakness belongs to the A03 category of OWASP 2021 and ranks twenty-fifth in MITRE's top weaknesses for 2021.

Old Vulnerabilities Tied to Ransomware

A pattern we have observed since we started our ransomware research is that ransomware groups are after newly identified vulnerabilities and also target older vulnerabilities published much earlier. For this report, we consider vulnerabilities identified before 2021 as old. In 2021 alone, we identified a total of 40 old vulnerabilities that have been associated with ransomware.

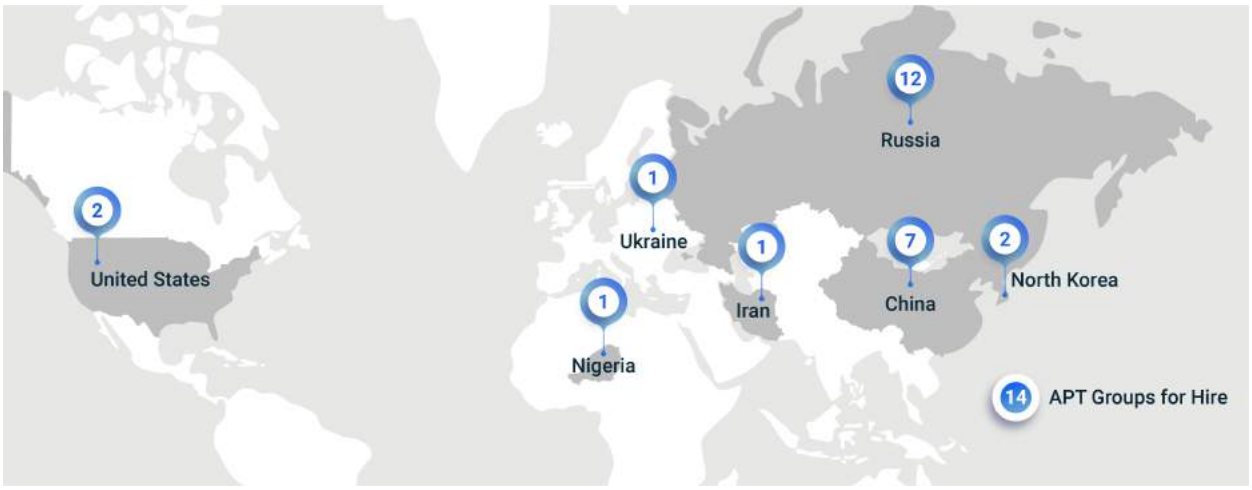
If the standard vulnerability management practice is to prioritize new vulnerabilities for remediation, 91% (263/288) of ransomware vulnerabilities remain unpatched, exposing the organizations to a huge attack window.

Vulnerabilities Tied to Ransomware and Trending by Year of NVD Publication



APT Groups Associated with Ransomware

While advanced persistent threat (APT) groups are a separate league of threat actors, we noticed ransomware being deployed by 40 APT groups overall. This marks a 7% increase since 2018–2020 and shows how state actors can create immense damage to organizations, including data leaks, data loss, disruption of organizational processes, and sensitive data compromise. The APT groups are largely from China, Russia, the USA, North Korea, Ukraine, and Iran; some of these APT groups have been around for over two decades now.



Ransomware Families

While our ransomware research uncovered 125 ransomware families during 2018–2020, we identified 32 new families in 2021, clocking a 25.6% increase in the overall family count. With 157 ransomware families exploiting the 288 vulnerabilities, ransomware groups are poised to wage rampant attacks in the coming years.

Cerber has overtaken Crypwall, 2018–2020's largest ransomware families by CVE count, with 69 vulnerabilities in its arsenal. Crypwall comes in second with 66 vulnerabilities, while Locky follows close with 64 CVEs in its bag. Cryptesla and CryptoMix finish the top five list with 56 and 54 vulnerabilities, respectively, under their belt.

CVE-2015-7645 and CVE-2015-5119 are used by 52 different ransomware families in their attacks. CVE-2013-2551, CVE-2015-0311, and CVE-2015-2419 fall next in the most used vulnerabilities list having been adapted into the arsenal of 51 different ransomware families each.

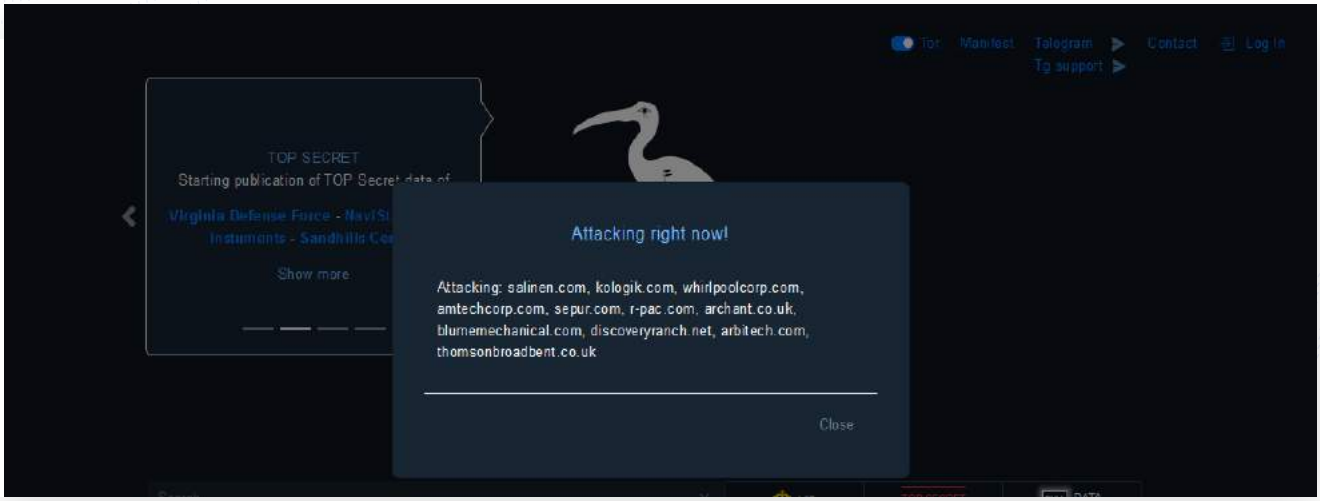
Exploit Kits

One of the trends we noticed while researching ransomware groups and their vulnerabilities is the widespread use of exploit kits by such actors. Exploit kits are automated tool kits that contain a collection of exploits that can be used to easily manipulate a variety of vulnerabilities. Once exploited, trojans, malware payloads, backdoors, or even cryptominers are added into infected entry points, which are later accessed to penetrate deeper into the compromised network. We observed 31 exploit kits being used by the identified ransomware families.

One of the prominent campaigns we noticed this year was the Indexsinas or the NSA BuffMiner campaign, where vulnerabilities linked to the EternalBlue exploit kit were exploited to gain access into vulnerable networks. While it was not conclusive if a ransomware group was involved in the campaign, our research linked the EternalBlue exploit kit to Conti, REvil, WannaCry, Satan, and Katyusha, amongst others.

3 Ransomware Trends and Our Analysis

Unpatched vulnerabilities are the main attack vectors that ransomware groups exploit to gain entry into vulnerable networks. However, our research also identified ransomware groups expanding their focus to not just single unpatched instances but to combinations of vulnerabilities, vulnerable third-party applications, technology protocols, and even insider recruiting as a means to take that first step in launching an attack.



Ransomware Attack Alerts in the Dark Web

In this section, we discuss the various trends we noted and provide our observations of the same.

Repeatedly Targeted Vulnerabilities

From our ransomware research in 2021, we noted some vulnerabilities that were repeatedly targeted by ransomware groups in multiple attacks. Here, we list these vulnerabilities and warn organizations to address them as soon as possible if they have not done so already.

Vulnerability	CVSS Severity	Vulnerability Name	Ransomware Associations
CVE-2021-26855	CRITICAL	ProxyLogon	DearCry, Black Kingdom, Epsilon Red, and Babuk
CVE-2021-26857	HIGH		
CVE-2021-26858	HIGH		
CVE-2021-27065	HIGH		
CVE-2021-31207	HIGH	ProxyShell	BlackByte, Babuk, LockFile, and Conti
CVE-2021-34473	CRITICAL		
CVE-2021-34523	CRITICAL		
CVE-2021-34527	HIGH	PrintNightmare	Vice Society, Conti, and Cerber
CVE-2021-1675	HIGH		
CVE-2020-1472	CRITICAL	ZeroLogon	Babuk, Epsilon Red, Thanos, Ryuk, Darkside, Conti, and CryptoMix

CISA recently published a list of 311 known exploited vulnerabilities and warned all federal agencies to address them within specified timelines. We took a deep dive into those 311 vulnerabilities and found that 57 vulnerabilities were associated with ransomware. VMWare, PulseSecure, F5, and Apache were the most affected vendors by these ransomware vulnerabilities, which included 18 trending vulnerabilities.

Ivanti speaks: Of note, patches for all CVEs for Pulse Secure were made available at the time the vulnerabilities were identified, and the company conducted an extensive outreach to customers, both at the time and on an ongoing basis, to help them address any risks in their environment. Ivanti, which purchased Pulse Secure in 2020, strongly encourages all customers to upgrade to the latest versions of the software to ensure they are protected against all known vulnerabilities. Ivanti remains committed to continually improving the security of all its products. In collaboration with experts such as US-CERT, Mandiant, and Stroz Friedberg, Ivanti is incorporating lessons learned and best practices to harden security measures and adding new features designed to improve the customer experience in future releases.

Top Six Disturbing Ransomware Trends

1. Zero-Day Vulnerabilities

One of the consistent trends that we noticed this year was the exploitation of zero-day vulnerabilities. A vulnerability is tagged as a zero-day vulnerability when the vulnerability has been identified by or disclosed to the vendor but is yet to be patched. In 2021, we identified many incidents, as highlighted in our Q2 2021 and Q3 2021 reports, in which zero-day vulnerabilities were exploited, sometimes even before the vendor was alerted of the existence of a flaw.

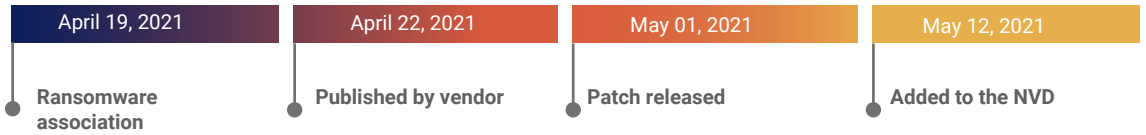
Zero-day exploits can be highly devastating to organizations, as attackers can take undue advantage before organizations even have the time to react. Incidentally, the 2021 zero-day vulnerabilities were exploited even before they made it to the NVD.

The following table lists the major 2021 zero-day ransomware targets. Interestingly, three of the four cases involved vulnerabilities without publicly available exploits.

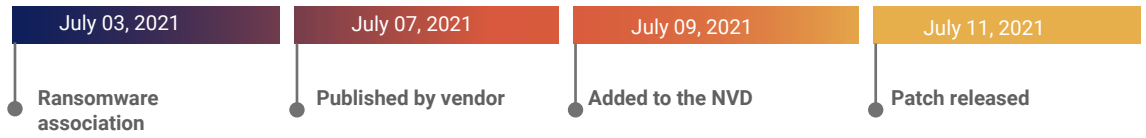
Vulnerability	CVSS Rating	Exploit Type	Vendor	Products	Ransomware Family Details	The First Wave of Attacks
CVE-2021-44228	10	RCE	Apache	Log4j	Conti, Khonsari, and TellYouThePass	Dec. 2021
CVE-2021-30116	9.8	NA	Kaseya	VSA Agent and VSA Server	Revil/Sodinokibi	July 2021
CVE-2021-20016	9.8	NA	SonicWall	SMA 100, SMA 100 Firmware, SMA 200, SMA 200 Firmware, SMA 210, SMA 210 Firmware SMA 400, SMA 400 Firmware, SMA 410, SMA 410 Firmware, and SMA 500v	Darkside and FiveHands	May 2021
CVE-2021-28799	9.8	NA	QNAP	Hybrid Backup Sync, QTS, QuTS Hero, and QuTS Cloud	Qlocker and eCh0raix	April 2021

SonicWall - CVE-2021-20016 - FiveHands Ransomware

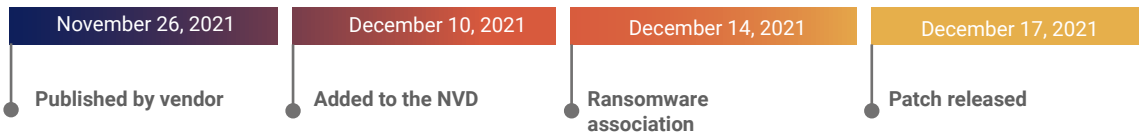
QNAP - CVE-2021-28799 - Qlocker Ransomware



Kaseya - CVE-2021-30116 - REvil Ransomware



Apache - CVE-2021-44228 - Khonsari, Conti, TellYouThePass Ransomware



Apache Log4j

CSW's experts have devised a scanner to help organizations scan for assets impacted by Apache Log4j. Get a complete suite of resources (Detection script, exploit, product list, and IOCs) to help deal with the biggest security disaster of 2021. Visit CSW Apache Log4j

2. Third-Party and Supply Chain Attacks

A supply chain attack is an insidious attack technique in which an adversary infects a trusted piece of code or hardware with a malicious component (usually malware). The malware silently propagates from this trusted supplier into the network of its customers, who all fall victim to this one-to-many supply chain compromise.

Ransomware groups look to leverage supply chain networks to maximize the impact of their attack. Here, we discuss some of the prominent supply chain attacks from 2021.

- The REvil group went after CVE-2021-30116 in the Kaseya VSA remote management service, launching a malicious update package that compromised all customers using on-site and remote versions of the VSA platform.
- The DEV-0322 APT group went after Serv-U managed file transfer software in SolarWinds in July 2021, prompting the fear of another SolarWinds supply chain attack. The TA505 APT group followed suit with another event in the latter half of 2021. This attack went one step further, deploying the Clop ransomware and compounding the magnitude of the attack.
- A similar APT supply chain ransomware link is the attack on Air India, a popular airlines establishment, which was taken to the brink of a supply chain attack by the APT41 group that is known to favor the use of the Maze ransomware.
- Another supply chain attack that shook the developing community was the Codecov software hack that hit customers from the technology to gaming sectors. While the impact of this event was curbed, it will not be long before ransomware groups leverage such methods or even work in harmony with other adversaries to destabilize high-profile organizations via insignificant supply chain components.

Most supply chain attacks also happen to be third-party attacks, wherein an organization's network is compromised due to a vulnerability in third-party software or integrations. Third-party compromise is another key cyberattack trend that is commonly seen in commercial and open-source software.

- The Colonial Pipeline attack by the DarkSide ransomware group involved the compromise of vulnerabilities in third-party VPN networks.
- The Apache Log4j vulnerability in Java logging libraries has now made hundreds of products vulnerable to attackers. The now-matured Conti group TellYouThePass that has been dormant for a while now and a new find Khonsari ransomware have been quick to exploit CVE-2021-44228.
- A ransomware attack on Elekta—a Swedish provider of radiation medical therapies and related equipment data services—impacted Jefferson Health, Northwestern Memorial Healthcare, Carle Cancer Institute Normal, and the Oklahoma Cancer Center, all suffering sensitive data breaches. While the group behind the attack has not been conclusively revealed, Elekta continues to face lawsuits as an aftermath of the attack in April 2021.

3. Vulnerability Chaining

Vulnerability chaining involves a set of unpatched vulnerabilities being combined together to launch an invasive attack. A successful attack chain allows attackers to stealthily infiltrate networks and move laterally using successive vulnerabilities at every point. The measure of the impact of such an attack is not in the individual vulnerabilities involved but in the cumulative ramifications of the chained vulnerabilities under the specific context. Let us see how ransomware groups have leveraged such chained vulnerabilities to gain initial access and penetrate deeper into organizational networks.

Interestingly, the vulnerabilities chained together are found to be of mixed severity, utilizing medium and high severity vulnerabilities that are not high on the radar of security teams. The risk here is that these vulnerabilities may not be prioritized for patching; organizations will be caught unaware if these vulnerabilities are used in a chain. This, once again, highlights the importance of the threat context in vulnerability management.

The LockFile ransomware used the heavily trending ProxyShell vulnerabilities together with the PetitPotam vulnerability to launch a series of attacks. It used the ProxyShell chain to enter into victims' networks and remotely run arbitrary code before abusing the PetitPotam flaw to gain deeper access. Although these attacks happened in mid-2021, there are 34,793 ProxyShell exposures still seen on the internet.

Vulnerability	CVSS Score	CVSS Severity	Exploit Type	Trending	Product
CVE-2021-31207	7.2	High	RCE	Yes	Microsoft Exchange Server
CVE-2021-34473	9.8	Critical	RCE	Yes	Microsoft Exchange Server
CVE-2021-34523	9.8	Medium	RCE	Yes	Microsoft Exchange Server
CVE-2021-36942	5.3	Medium	NA	No	Microsoft Windows, Windows Server 2008, 2012, 2016, and 2019

The Hafnium APT group is known to have used four ProxyLogon vulnerabilities chained together in widespread attacks in March 2021. This set the tone for ransomware groups that have followed suit; we are aware of groups that have exploited all four vulnerabilities but separately. The four Microsoft Exchange Server vulnerabilities have 8,849 unpatched instances, according to Shodan.

How long before they are chained in a single incident?

Vulnerability	CVSS Score	CVSS Severity	Exploit Type	Trending	Ransomware Families
CVE-2021-26855	9.8	Critical	WebApp	Yes	Epsilon Red, DearCry, and Black Kingdom
CVE-2021-26857	7.8	High	N	No	DearCry and Black Kingdom
CVE-2021-26858	7.8	High	N	No	DearCry and Black Kingdom
CVE-2021-27065	7.8	High	RCE/WebApp	Yes	Babuk, Epsilon Red, DearCry, and Black Kingdom

4. Vulnerabilities in End-Of-Life Products

Our research also uncovered prominent instances of ransomware groups going after vulnerabilities in products that had reached their end of life and thus would not be updated or supported by the respective vendors.

- The Cring ransomware quietly capitalized on two vulnerabilities, CVE-2009-3960 and CVE-2010-2861, in Adobe ColdFusion 9, which was left untouched since 2016 when it was tagged as "end of life." The group exploited CVE-2010-2861 to enter into the server of a services-based company and used CVE-2009-3960 to upload web shells, Cobalt Strike's Beacon payloads, and, finally, the ransomware payload.
- The HelloKitty ransomware was found targeting CVE-2019-7481 in SonicWall Secure Mobile Access (SMA) 100 series and Secure Remote Access (SRA) products with end-of-life firmware.

Even Apache Log4j that was wildly trending in December has an unsupported version, Log4j 1.x, that is being warned about by researchers. Although the version does not have any ransomware links as yet, Conti, Khonsari, and TellYouThePass ransomware groups have begun targeting Apache Log4j vulnerabilities, and it may not be long before one of the groups exploit this now-discontinued version.

5. Service Offerings

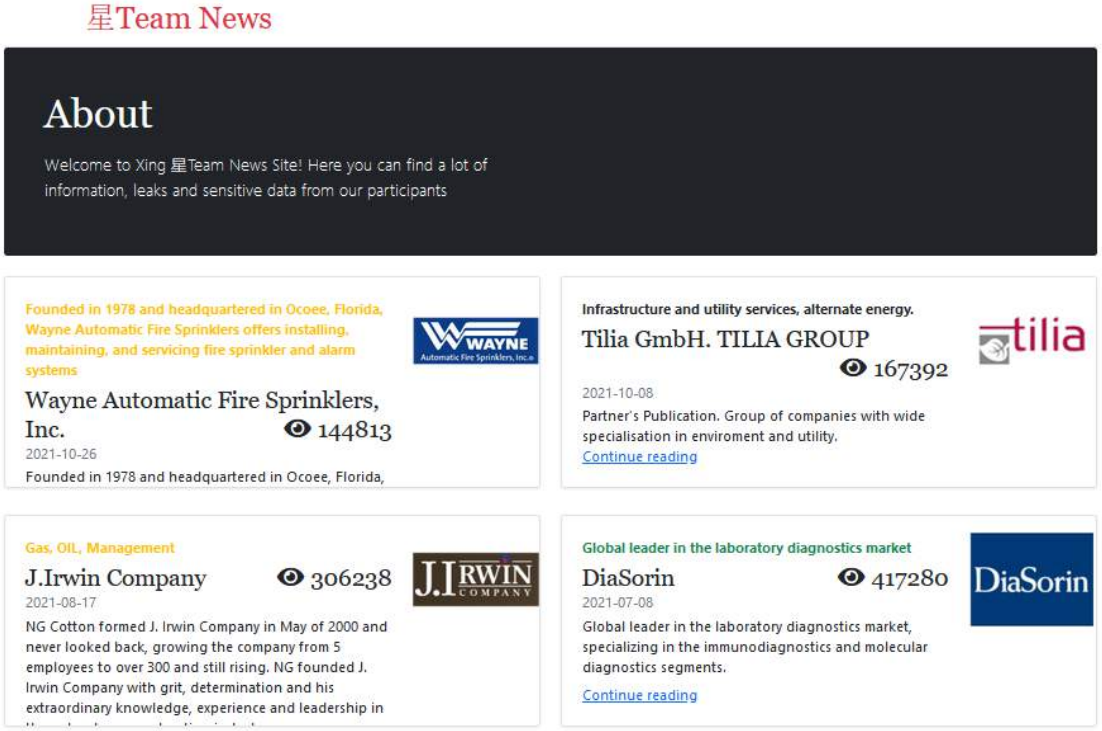
A growing ransomware practice is how groups seem to be willing to share their services with others, much like the legitimate SaaS offerings. Here are a few service trends we noticed in the past year:

- **Ransomware as a Service: Ransomware as a Service (RaaS)** is a business model wherein ransomware developers offer their services, variants, kits, or even code for use by another malicious actor in return for payment. This means that any individual or group with limited hacking knowledge can use these readily available services and deploy ransomware payloads into organizational networks. Ryuk, Conti, and DarkSide are famous for their RaaS offerings, while Nefilim, Dharma (Phobos family), and LockBit are a few recent contenders.

- **Exploit as a Service:** While buying exploit codes and zero-click RCE codes for big money has been around for a while, the latest is exploit-as-a-service solutions that allow threat actors to rent zero-day exploits from developers.

- **Dropper as a Service:** This is pure gold for newbie threat actors as they can lease dropper programs, which allow them to drop malicious payloads or malware into targeted networks.

- **Trojan as a Service:** Hackers, with a simple cloud connection, can use trojan-as-a-service offerings to obtain customized malware services for lease, without the need for installing and maintaining indiscernible software.



Groups Partnering to Launch Attacks

6. Attack Vector Trends

Cyberattacks generally start as data breaches or network intrusions and slowly develop into full-fledged ransomware attacks. Over the past year, our study of attack methods has shown malicious actors spreading their wings, looking beyond just unpatched vulnerabilities, and capitalizing on other entry points. While ransomware groups may or may not be exploiting these, we warn organizations to keep an eye out for any such abuse in their networks.

- Remote Desktop Protocol: Attackers exploit a weakness in the Remote Desktop Protocol (RDP) or how it is deployed in the network. RDP is used to control a system remotely; in turn, an attacker getting hold of an opening gets to have complete control over the system. CVE-2019-0708, a critical vulnerability in Microsoft's Remote Desktop Protocol, has two ransomware associations—DoppelPaymer and Redkeeper.
- Virtual Private Networks: Virtual Private Networks (VPNs) through which employees remotely access a company's network can have vulnerabilities that serve as an access point for network infiltration.

- XSS Vulnerabilities: Cross-site scripting attacks are injection-type attacks, wherein harmful payloads are injected into trusted websites. A universal cross-site scripting (UXSS) attack can exploit third-party vulnerabilities in browsers and their extensions to generate an XSS condition. Another emerging method is a type of side-channel attack, called the XS-Leaks, allowing attackers to collect information about their users.
- Linux Variants: From DarkSide to REvil, many ransomware groups are now adding a Linux variant of their code and codes in other languages, such as Go and Rust, to expand their attack capabilities.
- Red Teaming Tools: Cyber criminals are snowballing their impact by adopting Red Teaming tools, generally used for threat hunting and defense activities. One classic example is how Cobalt Strike has now become the go-to tool for threat actors.
- ETW Attacks: Bypass techniques that use the Event Tracing for Windows (ETW) logging mechanism can blind security products and launch cyberattacks.
- Internet Sharing Services: Proxyware platforms, which allow users to segregate a percentage of their internet bandwidth for other devices, could allow threat actors to obfuscate the source of their attack and render IP-based security checks ineffective.
- DNS Rebinding: DNS rebinding can allow attackers to abuse web-based consoles and increase the size of an organization's internal attack surface.
- SSID Stripping: SSID stripping can allow attackers to manipulate the name of a wireless network and trick users into connecting to their wireless access points, thereby leading to credential compromise.
- VoIP Attacks: We have observed a surge in the compromise of Voice over Internet Protocol (VoIP) platforms, allowing instant messaging and digital distribution. VoIP attacks help hackers gain sensitive information such as personal records.

Interestingly, we have also observed ransomware groups mimicking prominent groups like REvil to throw security practitioners off guard and ward off sanctions via similar ransom notes, website set-up, or even attack methods.

We also noticed that Threat groups have set up fake companies and reached out to company insiders, and even posted recruitment advertisements to help mount ransomware attacks. LockBit and AvosLocker are two of the prominent groups that have been known to use the insider recruitment strategy.

4 A Latency Analysis

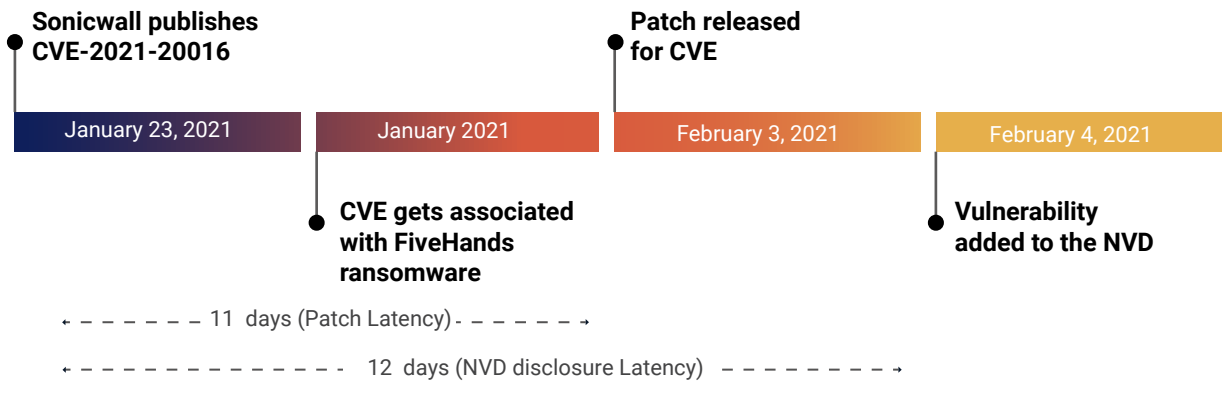
We analyzed 25 ransomware vulnerabilities from 2021 from a latency perspective, and here are our findings.

NVD Latency

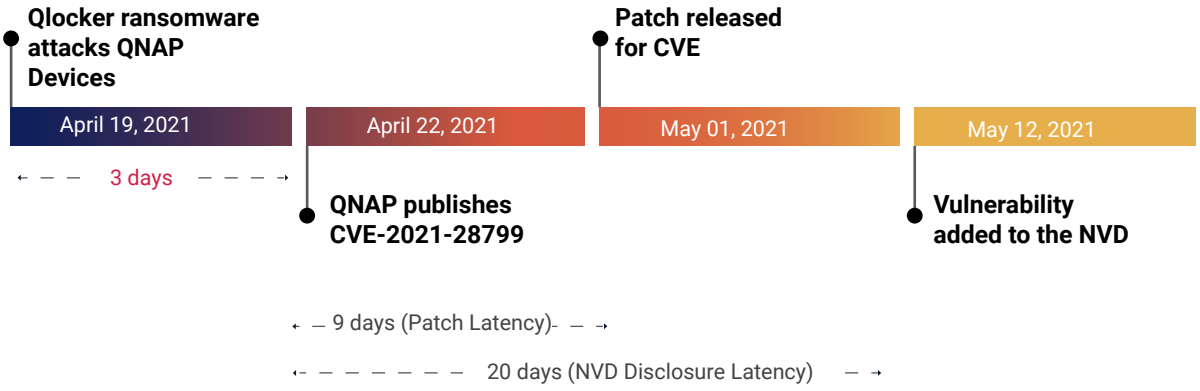
- On average, vulnerabilities from 2021 have an NVD disclosure latency of 13.7 days since the vendor published the vulnerability.
- The ProxyLogon vulnerabilities—CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065—identified in 2021 can be fixed by the Exchange Server version released in 2020 itself, an entire year before the vulnerability was added to the NVD. However, many instances still remain unpatched, highlighting a bad case of cyber hygiene.
- CVE-2021-27101 and CVE-2021-27104 were added to the NVD almost two months after the vendor called these out and provided patches.

Qlocker, FiveHands, and REvil ransomware all went after vulnerabilities in major attacks in 2021, before the vulnerabilities could be added to the NVD.

Timeline of CVE-2021-20016

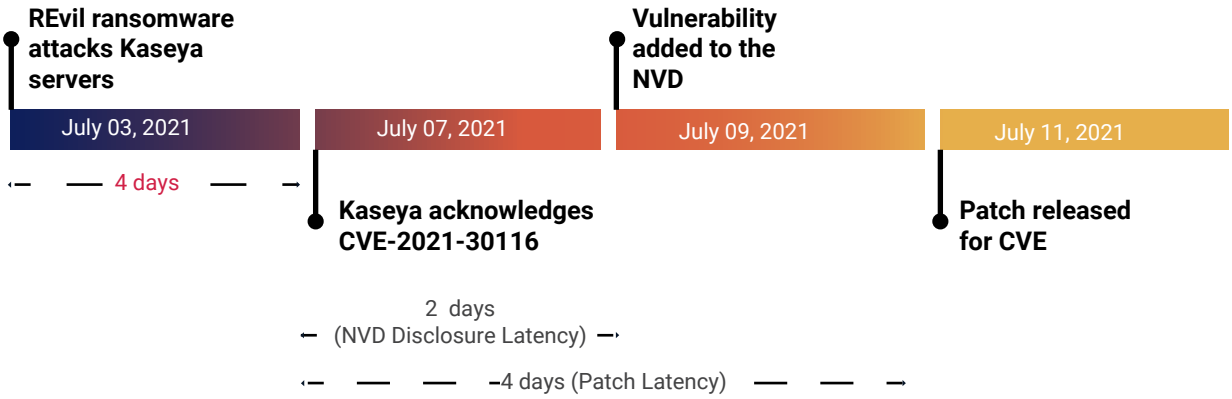


Timeline of CVE-2021-28799



*A latency in Red indicates that the attack happened before the CVE was disclosed by the vendor.

Timeline of CVE-2021-30116

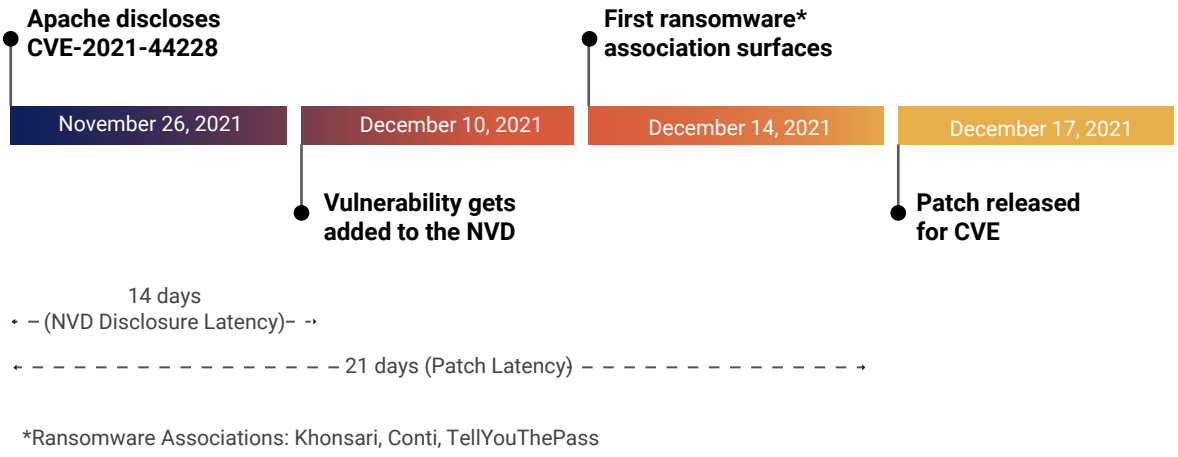


*A latency in Red indicates that the attack happened before the CVE was disclosed by the vendor.

Patch Latency

The Apache Log4j vulnerability, CVE-2021-44228, remained unpatched or partially fixed for almost a week since it was added to the NVD. Further, it was added to the NVD two weeks after the vendor's disclosure. This is a total latency of three weeks when insufficiently patched versions of the vulnerability with exposures as high as over 1,500 affected products were out in the open.

Timeline of CVE-2021-44228(Log4j)



*Ransomware Associations: Khonsari, Conti, TellYouThePass

Exploit Latency

- The first public exploits for CVE-2021-22205 were seen 209 days after the vulnerability was published by its vendor, the largest exploit gap amongst the 2021 ransomware vulnerabilities.
- Six—CVE-2021-21972, CVE-2021-26084, CVE-2021-40444, CVE-2021-44228, CVE-2021-27065, and CVE-2021-34527—of the 25 vulnerabilities were weaponized with public exploits within a week after being disclosed in the NVD. Unsurprisingly, all the CVEs have associated RCE exploits.

Zero Latency

- The vendor disclosed two vulnerabilities—CVE-2021-1675 and CVE-2021-31207—and patched and added them to the NVD, all without any latency.

In most cases, it is evident that there is a latency gap between a vulnerability being disclosed by the vendor, being published in the NVD, and a patch being released. A vulnerability can be exploited in any of these gaps and even in the gap between the vendor releasing a patch and organizations implementing the same. Thus, organizations need to be all the more vigilant and undertake all possible mitigating measures—be it a patch, an upgrade, an update, or a temporary fix—to ensure the safety of their networks and data.

5 Vendors under Attack

Our continued research over the past year brought up a few vendors whose products were repeatedly targeted by ransomware.

Vendor	Product	Vulnerability	Ransomware
Microsoft	Exchange Server	ProxyLogon and ProxyShell CVEs	Epsilon Red, DearCry, Black Kingdom, Babuk, LockFile, Conti, and BlackByte
	MSHTML	CVE-2021-40444	Cerber
	Internet Explorer/Edge	CVE-2021-26411	Cerber
VMware	vCenter	CVE-2021-21972	Memento
GitLab Inc.	GitLab	CVE-2021-22205	Cerber
Atlassian	Confluence	CVE-2021-26084	Cerber and AtomSilo
SolarWinds	Serv-U	CVE-2021-35211	Clop
Accellion	FTA	CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104	CryptoMix

Based on the analysis of vendors from a vulnerability angle, CVE-2018-3639 affects 26 different vendors and 345 of their products. Interestingly, CVE-2018-3639 is a medium severity vulnerability associated with the Stop ransomware family.

Another interesting observation is a 10% increase in the number of vulnerabilities connected to multiple vendors and products. From 102 in the 2021 Report, the number now stands at 110. If we include vulnerabilities that have multiple products belonging to a single vendor, the number goes up to 236 of the 288 vulnerabilities. This is an indication of the security dynamics today where a single vulnerability or weakness, once exposed, paves the way for many more opportunities for malicious actors. The Apache Log4j incident is enough evidence to support our claim.

End users rely on the vendor community, and it is the responsibility of vendors to ensure their offerings are strictly up to the task. Any possible attack vector must be discovered, investigated, and patched at the earliest, and the details must be immediately communicated to the user community as well to prioritize remediation.

6 Ransomware Groups That Stand Out

We have been studying ransomware groups and the vulnerabilities they are after since we published our first ransomware report in 2019. Based on the patterns and behavior of the groups, we highlight the following ransomware families that have stood out in 2021.

REvil/Sodinokibi

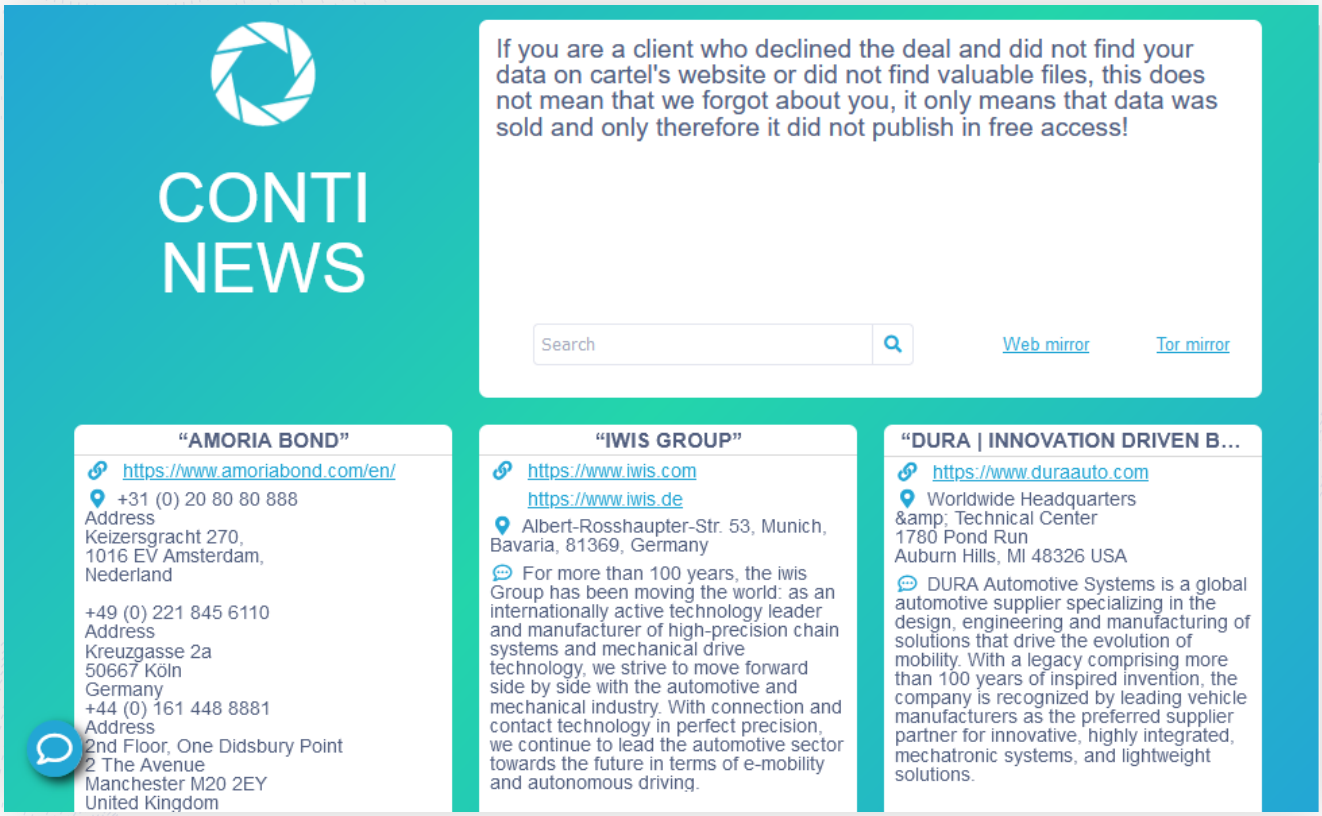
The REvil/Sodinokibi family was responsible for some of the most high-profile attacks in 2021. REvil was responsible for two significant events in 2021—for taking down JBS, the world's largest meat producer, and breaching Kaseya VSA servers—exploiting zero-day vulnerabilities resulting in a chain of third-party incidents. The REvil group was also involved in attacks on a leading Sri Lankan internet services provider; Fujifilm, a Japanese multinational conglomerate; Sol Oriens, a nuclear weapons subcontractor to the US Department of Energy; Invenergy, a renewable energy company; and Grupo Fleury, a medical diagnostic company.

The group remained dormant after the Kaseya incident and the subsequent revelation of its decryption key but came back strongly in a couple of months with newer attack methods. In the second phase, they went after two internet and telephony service providers and launched DDoS attacks on VOIP.ms and supposedly Bandwith.com.

In January 2022, Russia's Federal Security Service, at the request of US authorities, arrested several members of the REvil gang and neutralized its operations. Illicit cash, cryptocurrency, computer equipment, and luxury cars were also seized.

Conti

The Conti ransomware family was found trending without a break throughout 2021. Since its emergence, the group has added 17 vulnerabilities to exploit and launch attacks. Conti's arsenal includes vulnerabilities from 2017 onward, barring 2019. In 2021, the group went after some of the most dangerous vulnerabilities, including the ProxyShell chain, the 2017 Microsoft Windows Server Message Block server vulnerabilities, the PetitPotam, PrintNightmare, Zerologon, and the latest Apache Log4j vulnerabilities. The criticality of Conti's rampage prompted CISA to issue an exclusive advisory that urged organizations to level up their defense against this specific ransomware group.



Stop

The Stop ransomware, also called the DJVU ransomware, is one of the low-lying groups that has silently caused a constant stir. Unlike groups that go after high-profile victims, Stop ransomware targets the average home user via malicious software cracks and adware bundles. This also follows the Qlocker mode with relatively low ransom demands, most often less than a thousand dollars. While multiple tool decryptors have been released to curb the impact of the Stop group, this group is notorious for constantly releasing newer variants, which make the tools invalid.

Cuba and BlackMatter

Two groups that have kept surfacing on and off this year are the Cuba and BlackMatter ransomware groups. While our research is still ongoing about these groups, we urge organizations to diligently maintain good cyber hygiene practices to ward off such threats.

In December 2021, the FBI released an alert warning of the Cuba ransomware group that is believed to be behind the compromise of at least 49 entities in five critical infrastructure sectors—including but not limited to—the financial, government, health care, manufacturing, and information technology sectors. The group uses legitimate Windows services along with the Hancitor malware to infiltrate victim networks.

The BlackMatter ransomware is believed to be the resurgence of the DarkSide group. However, it goes against the so-called principles of the DarkSide group, which aimed to stay away from attacking critical sectors. The group has been involved in attacks against organizations in the health care, food, and agriculture sectors and has targeted companies with a revenue of $100 million and more. It was warned against by the FBI and CISA, again pointing to the importance of following security best practices.

Pysa/Mespinoza

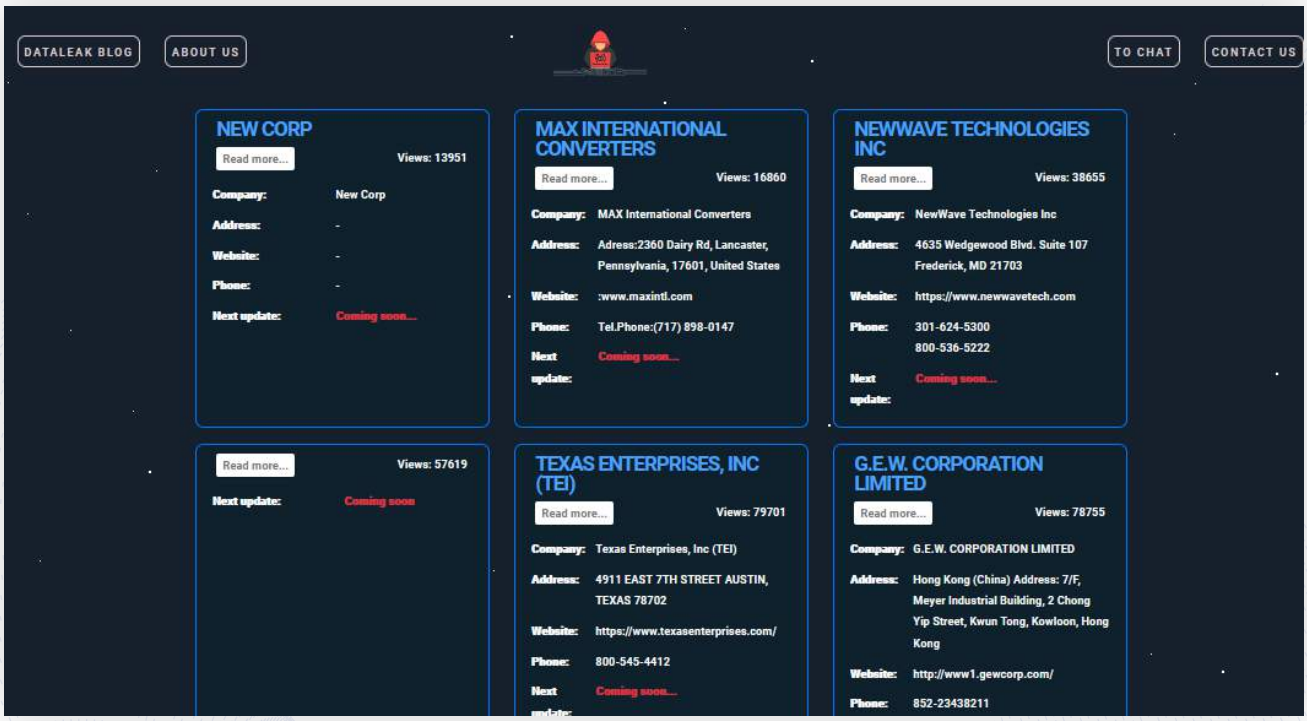
Another noteworthy mention is the Pysa/Mespinoza ransomware group, a part of the Crypsam ransomware family and one of the many ransomware groups called out by the FBI. The Pysa group is known to target government and education sectors specifically and has been observed using keyword-based scripts to scan for specific data to launch a data theft attack. The group also expanded its attack portfolio to include Linux-based systems.

7 Ransomware Data Leaks

As part of our ransomware research, we also deep dived into the dark web to understand the quantum of data leaked by ransomware groups. We identified a total of 1,285 victims and their data published across various leak sites by 35 ransomware groups combined in 2021 alone.

Unsurprisingly, Conti tops the list with 269 attack victims listed. Below is a look into other ransomware groups that have leaked data. Interestingly, groups like Pysa have also been noted as having a penchant for waiting six months or more after a breach to add victims to their leak site.

Ransomware Group	No. of victims listed in their leak sites
Conti	269
Avaddon	161
REvil	144
DarkSide	75
Pysa	68



Ransomware Victims Listed in the Dark Web

8 Vulnerable Sectors and Product Categories

This section calls out some of the sectors and product categories that were repeatedly targeted and on the radar of threat actors in 2021.

Health Care

From the Ireland health care service attack by Conti, Vice Society's attacks on Eskenazi Health, Waikato DHB and Centre Hospitalier D'Aries as featured in their leak site, Hive ransomware's attack on the Memorial Health System to REvil's supposed hack on a Brazilian health care company, the health care sector has been right on top of ransomware targets due to the magnitude of their impact. This sector has also seen several data breaches throughout the year.

The nature of the health care sector is such that an attack on any health care institution could lead to disastrous consequences. Vulnerabilities in health care services like pumps could allow for altering the dosages of medications using a simple hack. Pneumatic tubes are systems that propel cylindrical containers through networks of tubes by compressed air or by partial vacuum. While largely outdated, many hospitals still use pneumatic tubes, and vulnerabilities in such systems can lead to the entire functionality being hacked and controlled by malicious actors.

A ransomware attack on the Springhill Medical Center in the US resulted in the death of an infant when staff was cut off from fetal heartbeat monitors as a result of the network outage that followed the attack.

This calls for increased vigilance, especially by organizations that maintain the network of health care providers and medical equipment.

Critical Infrastructure

The year 2021 saw ransomware groups waging attacks on critical infrastructure, from the food industry to the utility sector, despite warnings by security advisories and governments. The DarkSide group went after Colonial Pipeline that supplies fuel to the entire US East Coast, completely disrupting the gasoline supply. REvil attacked JBS, the world's largest meat producer, forcing the organization to shut down operations across countries. The Conti ransomware took down servers in Ireland's health care services, resulting in total chaos in rendering regular health-related services. Details are still under investigation for an attack on Florida's water utility plant, where a hacker tried to change chemical levels, poisoning the potable water supply. Equally alarming is the fact that a ransomware attack could take lives, as in the case of the Springhill Medical Center attack.

Product Category Analysis

In 2021, we noticed ransomware groups targeting a wide range of products, from servers to SaaS offerings. Cumulatively, the ransomware vulnerabilities affect 2,765 unique products offered by 101 unique vendors.

Operating systems were found to be the most vulnerable product offering with the maximum vulnerabilities. Going by the number of products affected under each category, Software Development Kits (SDKs) took the first spot, followed by operating systems. We have also observed a high interest in storage, operational technology, and industrial control systems as well.

Product Category	No. of Vulnerabilities	Affected Products
Operating System	54	523
Software Application	32	501
Web Browser	29	383
Software Development Kits	15	1460
Application Framework	15	224

Although it does not appear in the top five list, an important product category we would like to highlight is the Storage. Storage or backup is the topmost recovery strategy if an organization is hit by a ransomware attack. What happens if ransomware groups target the backup? That is a scary trend that is amping up slowly.

Our research identified four vulnerabilities across 28 products in storage offerings. Network-attached storage contributed to another four ransomware vulnerabilities, with 45 affected by them. Combined, these offer eight different attack vectors making them easy targets for ransomware groups.

The following table lists the vulnerabilities in storage offerings and the ransomware groups going after them.

Vulnerability	Vendor	Product	Ransomware
CVE-2021-28799	QNAP	Hybrid Backup Sync, QTS, QUTS Hero, and QUTS Cloud	Qlocker
CVE-2018-19943 CVE-2018-19949 CVE-2018-19953 CVE-2019-7192 CVE-2019-7193 CVE-2019-7194 CVE-2019-7195 CVE-2021-28799	QNAP	Photo Station, Hybrid Backup Sync, QTS, QUTS Hero, and QUTS Cloud	eCh0raix

We have also seen many other events where the storage element has taken a hit although such hits have not been conclusively linked to a ransomware attack. NAS devices with QNAP firmware released before August 2020 were targeted by cryptocurrency malware. The StealthWorker botnet, using brute-force attacks, targeted Synology NAS devices. Western Digital's My Cloud and My Book Live devices were under active siege in mid-2021. OpenSSL vulnerabilities were used to target NAS devices, leading to application takeovers. The end of the year also brought to light vulnerabilities in ENC Security's DataVault encryption software that is being used by several major organizations, including Sony, SanDisk, and Lexar, in their storage devices.

The advanced methods that ransomware groups use today are a cause for concern. Groups are favoring double extortion techniques that include data encryption and a data leak scare and directly targeting data by terminating database processes, locking storage, or even wiping out backups.

9 Other Noteworthy Vulnerabilities

While our ransomware reports mainly focus on those vulnerabilities that have known associations to ransomware groups, we have also observed others that have the potential for ransomware exploits but are yet to be associated with known groups.

Vulnerability	CVSS Score	Vendor	Ransomware
CVE-2020-1380 CVE-2020-0878	7.5 7.5	Microsoft	Internet Explorer/Edge
CVE-2021-21985 CVE-2021-22005	9.8	VMWare	vCenter
CVE-2021-36260	9.8	Hikvision	Web Server
CVE-2021-38647 CVE-2021-38648 CVE-2021-38645 CVE-2021-38649	9.8 7.8 7.8 7.8	Microsoft	Open Management Infrastructure (OMI)
CVE-2021-40539 CVE-2021-44077	9.8 9.8	Zoho	ManageEngine
CVE-2021-42013 CVE-2021-41773	9.8 7.5	Apache	HTTP Server
CVE-2021-3064	9.8	Palo Alto Networks	VPN
CVE-2021-3711 CVE-2021-3712	9.8 7.4	NA	OpenSSL
CVE-2021-42287 CVE-2021-42278	8.8 8.8	Microsoft	Active Directory

10 Trends to Watch Out For

Our active research identified some interesting trends; here, we highlight those that could become big in 2022.

- While we are already seeing an increase in vulnerabilities in software code libraries like NPM packages (JavaScript library), we believe ransomware groups will start going after them sooner rather than later .
- We have observed APT groups going after application programming interfaces (APIs). We believe ransomware groups will not wait long to follow, with compromised APIs making it one step easier for attackers and that much harder for organizations to protect their data.
- Misconfiguration in code will change from an overlooked aspect to one of the primary attack vectors. We can already glimpse this trend from how the Apache Log4j issue is shaping up. Every other day, newer CVEs are attributed to the misconfiguration in code through versions that are released to fix earlier issues.

11 Summary

In 2020, we saw a huge spike in vulnerabilities associated with ransomware, ringing the alarm bells. This year we have seen ransomware actors moving up the stack from OS to databases, applications, and APIs. Our experts also suggest that conquering SaaS applications, IoT devices, IT and OCS offerings, and open-source software would be a prominent part of their forthcoming strategy.

We believe ransomware groups will continue to pursue all possible avenues, in combination with unpatched vulnerabilities, to expand their attack techniques and tactics. Another cause for concern is the widespread targets of ransomware, ranging from governmental organizations to storage applications.

Patches for vulnerabilities could be in the form of version updates, new software packages, or even security updates. Of the 288 ransomware vulnerabilities, we have observed ransomware groups and threat actors repeatedly scouting the web for 51% of these vulnerabilities, looking for one unpatched instance they can exploit. Thus, organizations need to be quick on the uptake and patch vulnerabilities—the ones receiving attention from attackers, exploited in the wild, or warned about in advisories—without delays.

"Ransomware is devastating to customers and employees in every sector! In 2022, we will continue to see an increase in new vulnerabilities, exploit types, APT groups, ransomware families, CWE categories, and how old vulnerabilities are leveraged to exploit organizations. Leaders need innovative and predictive help to prioritize and remediate ransomware threats."

Aaron Sandeen,
CEO,
Cyber Security Works

"Ransomware groups are becoming more sophisticated, and their attacks more impactful. Threat actors are increasingly leveraging automated tool kits to exploit vulnerabilities and penetrate deeper into compromised networks. They are also expanding their targets and waging more attacks on critical sectors, disrupting daily lives and causing unprecedented damage. Organizations need to be extra vigilant and patch weaponized vulnerabilities without delays. This requires leveraging a combination of risk-based vulnerability prioritization and automated patch intelligence to identify and prioritize vulnerability weaknesses and then accelerate remediation."

Srinivas Mukkamala,
Senior Vice President of Security Products,
Ivanti

"The substantive change we've observed across the ransomware landscape is that attackers are looking to penetrate processes, such as patch deployment, as much as they look for gaps in protection to penetrate systems. Vulnerability discovery must be met with actions that treat vulnerability data as intelligence to drive swift response decisions. As ransomware gangs operationalize their tooling, methods, and target lists, it is essential for SecOps teams to automate processes to self-heal vulnerable assets and systems and mitigate risk through real-time intelligence operationalization."

Anuj Goel,
CEO,
Cyware

The only weapon organizations have in this cyberwar is cyber hygiene. Organizations need to practice continuous vulnerability management, rigorous risk-based prioritization, and threat-aware mitigation to ensure the safety of their network and, thereby, their data at all times.

Our research is the only all-encompassing source of information about ransomware groups and the vulnerabilities they are after. We provide this information to enable organizations to stay aware and protect themselves from the menace that is ransomware.

12 Report Methodology

The information in this report is based on data gathered from various sources (including proprietary data from CSW, Cyware, and Ivanti), publicly available threat databases, and from CSW's and Ivanti's threat researchers and penetration testing teams. We hope this report can serve as a starting point for organizations that wish to take a risk-based approach to ransomware exposure to prioritize patching to secure their enterprise and reduce their attack surface. Simply put, most organizations are inundated with more vulnerabilities than they can patch, so we wanted to provide the various perspectives and details we uncovered about ransomware to shed light on the trends and key findings to help manage their vulnerability risk backed by research.

Our Focus

We focused on vulnerabilities that came into existence between 2010 and 2021 and tracked their trending dates and associations with ransomware families. Our vulnerability data is based on the NVD. We extensively analyzed the vulnerabilities that trended in 2021 and also identified CVEs and trends that are of interest.

Definitions

Throughout the report, you will notice that we use the words "trending" and "actively exploited." They are distinctly different in what we wish to convey with regards to this report:

- **Trending:** Any CVE seen within active ransomware exploit in the most recent time period, i.e., in 2021
- **Actively Exploited:** Any CVE that has been used to launch ransomware attacks in the past is defined as being tied to active ransomware exploits during the specified time period.

13 About Us

Cyber Security Works

CSW is a cybersecurity services company focused on attack surface management and penetration testing as a service. Our innovation in vulnerability and exploit research has led us to discover 50+ zero days in popular products such as Oracle, D-Link, WSO2, Thembay, and Zoho. As a CVE Numbering Authority, we hope to enable thousands of bug bounty hunters and play a critical role in the global effort of vulnerability management. As an acknowledged leader in vulnerability research and analysis, CSW is ahead of the game, helping organizations worldwide to secure their business from ever-evolving threats. For more information, visit www.cybsercurityworks.com or follow us on LinkedIn and Twitter at @CswWorks

www.cybersecurityworks.com

Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic virtual cyber fusion centers. Cyware is transforming security operations by delivering the cybersecurity industry's only Virtual Cyber Fusion Center Platform with next-generation security orchestration, automation, and response (SOAR) technology.

As a result, organizations can increase speed and accuracy while reducing costs and analysts' burnout. Cyware's Virtual Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, information sharing groups (information sharing and analysis centers and information sharing and analysis organizations), managed security services providers, and governmental agencies of all sizes and needs.

https://cyware.com/

Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they work from anywhere. The Ivanti Neurons automation platform connects the company's industry-leading unified endpoint management, cybersecurity, and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and empowers users to self-service. Ivanti manages over 200 million devices for 40,000+ customers, including 96 of the Fortune 100. Customers have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit www.ivanti.com and follow us on LinkedIn and Twitter @GoIvanti.

www.ivanti.com

14 Appendix

The list of vulnerabilities not detected by any of the scanners (Nessus, Qualys, and Nexpose) based on our research.

CVE	Ransomware Family	Patch Link	Comments
CVE-2010-1592	Robinhood	NA	
CVE-2013-0322	Paradise, GandCrab, AnteFrigus, Cryptoluck, Spora, Sodinokibi, Sage, Crypradam, Princess Locker, Philadelphia, Nemty, Mobef, Matrix, Locky, Goopic, GetCrypt, FessLeak, Globe, ERIS, Erebus, Dxh26wam, Crypwall, CryptoShield, CryptoMix, Cryp-MIC, Cry, Cerber, Buran, BartCrypt, BandarChor, ASN1, Alma Locker	Patch Now	No official patch update
CVE-2013-2618	Ryuk	Patch Now	CVE rejected By NVD
CVE-2013-3993	Petya, Locky	Patch Now	
CVE-2015-2551	TorrentLocker, Crypshed, Reveton, NanoLocker, Locky, Kovter, JuicyLemon, CTB-Locker, Waltrix, Crypwall, Crypfort, CryptoMix, CrypBoss, Cerber, Better_call_saul, Cryptesla, Cryptohasyou	NA	

CVE	Ransomware Family	Patch Link	Comments
CVE-2015-7465	Cerber	Patch Now	
CVE-2017-15302	Robinhood	NA	
CVE-2017-18362	GandCrab	NA	
CVE-2017-3197	UEFI	Patch Now	Patch available for one version of product from third party advisory
CVE-2017-3198	UEFI	Patch Now Patch Now	Patch available for one version of product from third party advisory
CVE-2017-6884	Ryuk	NA	
CVE-2018-19943	eCh0raix	Patch Now	
CVE-2018-19949	eCh0raix	Patch Now	
CVE-2018-19953	eCh0raix	Patch Now	
CVE-2019-13608	Nefilim	Patch Now	
CVE-2019-16057	Cr1ptT0r	Patch Now Patch Now	

CVE	Ransomware Family	Patch Link	Comments
CVE-2019-16647	Bitpaymer	Patch Now	Patch available from third party advisory
CVE-2019-16920	Cyborg	Patch Now	Patch available from third party advisory
CVE-2019-5039	ASN1	NA	Insufficient information
CVE-2019-9081	Satan, Mailto	Patch Now	Patch available from third party advisory
CVE-2021-28799	Qlocker, eCh0raix	Patch Now	