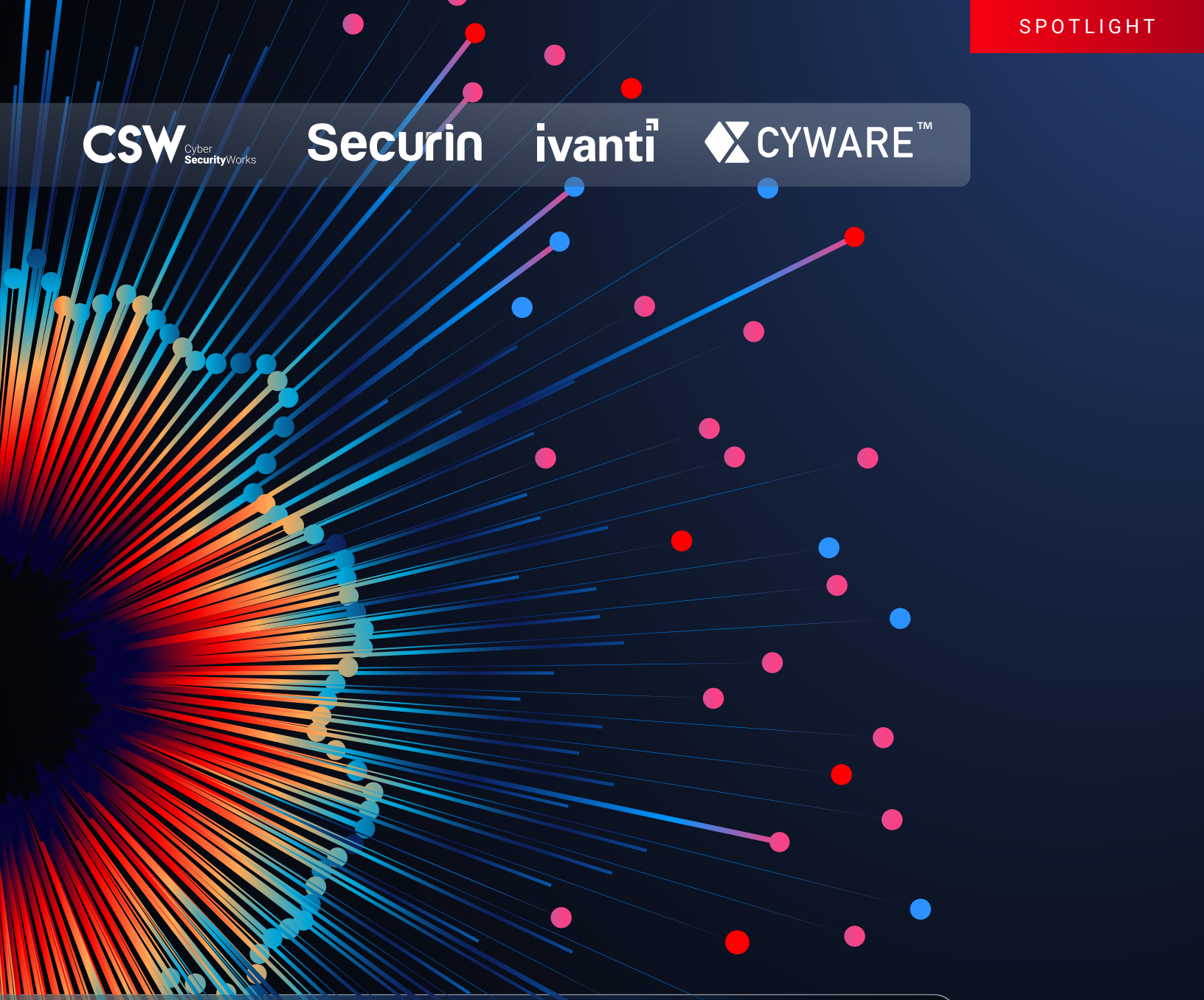
SPOTLIGHT

CSW Cyber SecurityWorks | Securin | ivanti | CYWARE™



Ransomware

Through the Lens of Threat and Vulnerability Management

2022

Index Update

Q2-Q3

Table of Contents

Message from CEO

Hi Friends,

Thank you for your continued interest in our cybersecurity research program and ransomware reports! Over the past three quarters, our research team has significantly amplified our efforts to identify key threats and trends that malicious actors use today.

The volume and complexity of attack data continue to grow. In response, we have made major investments in leveraging automation and machine learning. Now, we can better predict if a vulnerability is targeted for exploitation. We are collating our research into timely, contextual, and actionable intelligence for our customers to utilize in protecting their organizations.

No organization is safe from ransomware threats! However, we can develop risk-based strategies to protect ourselves. Threat groups are constantly evolving, adapting, and indiscriminately targeting every sector and industry. To stay one step ahead, organizations must be vigilant and tighten their cybersecurity defenses. Our research team continues to collect actionable intelligence to enable our customers to combat ransomware.

Government and federal agencies are also alert, tracking these threats and encouraging enterprises to take the ransomware crime seriously. However, the shortage of skilled cybersecurity experts and the lack of attack surface visibility in organizations are leaving gaps for threat actors to exploit. Ransomware groups are continuously finding vulnerabilities to target their victims with. There is a list of ransomware vulnerabilities that are not being detected by popular scanners, which to me as a former CIO, is a scary prospect. I am happy to see that CSW's attack surface platform, Securin, which was built to solve this very use case, gives organizations a hacker's view of their attack surface.

I hope you find this report as illuminating as it has been for me. Ransomware is a pervasive menace, and the malicious actors are going after high-impact targets that would disrupt lives and cause destruction. The only way to fight this menace is through utilizing data, intelligence, and expertise.

Yours Sincerely,
Aaron Sandeen
CEO & Co-founder, CSW

ivanti

A few years ago, ransomware was just a nuisance. Fast forward to today, the impact of ransomware is widespread. Ransomware is truly disrupting society, with threat actors capitalizing on the remote and hybrid business landscape and continuing to grow in volume and sophistication. The response to ransomware is reactive; we need organizations to be proactive and have layered defenses to be resilient.

Ransomware needs human interaction, and phishing as the only attack vector is a myth. Ransomware attack vectors have evolved and are now targeting remote access services, software weaknesses, and cloud applications. Health care, energy, critical manufacturing, and public sector (federal, state, local, education, and tribal) organizations are frequently targeted by threat actors, with unpatched vulnerabilities, coding errors, and misconfigurations being common points of infiltration.

Our goal with this report is to help organizations become proactive, realize the security risk and vulnerability exposure of their digital ecosystems, and provide actionable intelligence to proactively remediate and recover faster in the event of an incident. The combination of risk-based vulnerability prioritization and automated patch intelligence can help organizations reduce their exposure and majorly impact global cyberspace. A Binding Operational Directive (BOD) from the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) reinforces the Risk-Based Vulnerability Prioritization Approach to remediate ransomware and cyber threats.

- BOD 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks
- BOD 23-01 - Implementation Guidance
- BOD 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities
- BOD 20-01 - Develop and Publish a Vulnerability Disclosure Policy
- BOD 19-02 - Vulnerability Remediation Requirements for Internet-Accessible Systems

It is an honor to join forces with Cyber Security Works and Cyware in the global fight against ransomware and collaborate with them for this report. Together, we are committed to helping organizations drive operational efficiencies and stay ahead of sophisticated cyber threats.

Yours Sincerely,
Srinivas Mukkamala
Chief Product Officer, Ivanti

Ransomware attacks have risen to the top of the threat landscape with the introduction of new extortion techniques, strains, and cybercrime-as-a-service models. This index report uncovers a concerning trend in the ransomware landscape—the increasing weaponization of vulnerabilities by ransomware groups (466% growth from 2019) with 57 vulnerabilities, with the entire cyber kill chain mapped, making them extremely dangerous. The situation is further aggravated by blindspots in the popular vulnerability scanning platforms, making vulnerability detection a harder task.

It is now more important than ever for organizations to have direct access to vulnerability intelligence and collaborate with other organizations through threat intelligence sharing. With the growth in the number of vulnerabilities tied to ransomware exploitation, security teams must strive to gain real-time threat visibility with capabilities to execute mitigation and workarounds at machine speed. This can be accomplished through the following:

- A threat intelligence and automation-driven approach for proactive vulnerability awareness and remediation
- The resilient orchestration of security processes across cloud and on-premise environments to ensure the integrity of all vulnerable assets

Vulnerability reporting has surged annually, with thousands of new vulnerabilities being added to the National Vulnerability Database (NVD). However, not all vulnerabilities pose the same level of threat, which makes it necessary to separate the wheat from the chaff. This index aims to provide security teams with better insights into the asymmetric risks posed by different vulnerabilities to help them smartly prioritize their patching and defensive workarounds.

With this report, in partnership with Cyber Security Works and Ivanti, we are reinforcing our commitment to security collaboration efforts against the growing challenge of ransomware attacks by enabling organizations to streamline their security priorities and build mature, reliable strategies to counter ransomware threats.

Yours Sincerely,
Anuj Goel
CEO, Cyware

Introduction

Ransomware activities in 2022 continue to grow in their complexity and impact. This report continues with our traditional definitive analysis showcasing research correlating weaponized vulnerabilities with specific attack patterns. In addition, Cyber Security Works (CSW) is introducing our predictive security intelligence to provide early warnings and actionable insights to our community.

This index report covers the second and third quarters of 2022 to highlight key index numbers that have changed in the specified time frame. We have also included CSW's research on MITRE ATT&CK mapping of ransomware vulnerabilities and an analysis of how ransomware operators are orchestrating their attacks. We specifically looked at what vulnerabilities threat actors are going after and the weakness categories that help achieve their nefarious goals. Our analysis sheds light on how ransomware groups prioritize the vulnerabilities they use for exploitation and weaponization.

We dig deep into a specific industry in each quarterly report to provide key insights about their susceptibility to ransomware threats. This report focuses on the Industrial Control Systems (ICS) for the 16 critical infrastructure sectors defined by CISA.

With this Index Update, we aim to help organizations understand the actual risk posed by progressively evolving ransomware groups and provide actionable intelligence and predictive early warnings that would enable organizations to chart a proactive and defensive road map.

The 2022 Q2-Q3 ransomware report has been created in collaboration with our excellent partners at Ivanti and Cyware. We thank both of them for their expertise and intelligence to help deliver the most comprehensive Ransomware Intelligence to you.

Report Methodology

The information in this report is based on data gathered by CSW's security researchers and threat hunters, Securin's Threat and Vulnerability Intelligence platform, along with Cyware's and Ivanti's research data.

Our ransomware data is meticulously collated from multiple data sources known for their accuracy and is continuously updated by CSW's and Securin's research teams. Our security researchers and penetration testers use this data to improve our clients' security posture and keep them safe from evolving ransomware threats and risks.

The report aims to highlight key findings related to ransomware, increase ransomware literacy, and share actionable insights with our community to eliminate ransomware vulnerabilities in their environments.

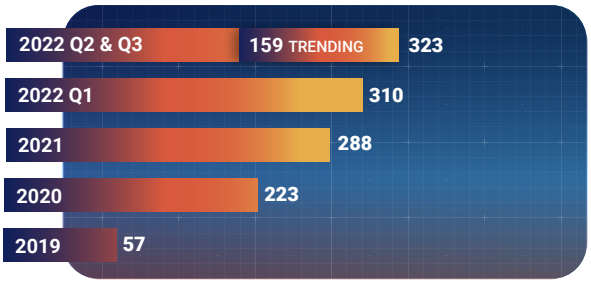
CSW's research methodology focuses on definitive and predictive data to drive our security intelligence. The definitive analysis encapsulates specific vulnerability and threat data continuously cleansed, enhanced, and validated by our researchers. Our predictive analysis leverages data from Securin's Vulnerability Intelligence (VI) platform collected from open, social, deep, and dark web sources. It then leverages more than 60 Machine Learning (ML) models to predict if a vulnerability will be exploited in the wild. This combined research approach provides comprehensive coverage and predictive intelligence to reduce ransomware risks significantly.

Our Special Snapshot section covers vulnerabilities in Industrial Control Systems deployed in critical infrastructure establishments. We analyzed CISA's advisories, conducted a MITRE analysis of the vulnerabilities that were warned about, and highlighted three sectors at great risk from ransomware threats.

Key Findings

Ransomware vulnerabilities continue to grow with 13 new additions

In this quarter, 13 new vulnerabilities have become associated with ransomware. This brings the total number of vulnerabilities tied to ransomware to 323, clocking a 466% growth from 2019. Overall, 35 vulnerabilities have become associated with ransomware this year.



CSW's experts also continuously track key ransomware vulnerabilities that are actively used by ransomware operators and have found that currently 159 vulnerabilities are trending as a point of interest for malicious actors.

More Details

The MITRE ATT&CK kill chain exists for 57 ransomware vulnerabilities

CSW's research team mapped each ransomware vulnerability to MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) kill chain to delve deep into attack patterns and enhance detection and mitigation. Through our research, we have found 57 vulnerabilities with a complete kill chain from initial access to exfiltration, making them extremely dangerous as ransomware attackers could use them to take down their victims. These vulnerabilities are found in primary vendors such as Microsoft, Oracle, VMware, Atlassian, Apache, and 15 others, spanning 74 unique products.

A MITRE ATT&CK kill chain is a model where each stage of a cyberattack can be defined, described, and tracked, visualizing each move made by the attacker. Using this framework, security teams can stop an attack and design stronger security processes to protect their assets.

More Details

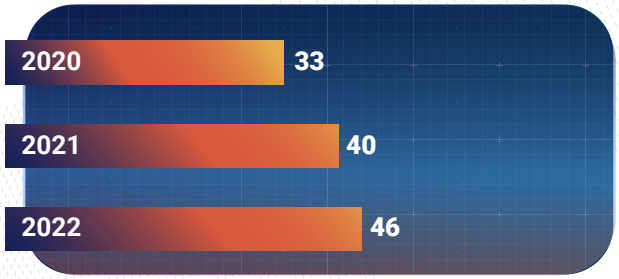
Popular scanners have blindspots

Organizations are only as secure as their ability to identify and remediate vulnerabilities. CSW continuously analyzes the abilities of top scanners to identify vulnerabilities associated with ransomware. In Q2-Q3, we identified 18 ransomware vulnerabilities for which Nessus, Nexpose, and Qualys do not have updated detection signatures.

More Details

Three more APT groups started using ransomware

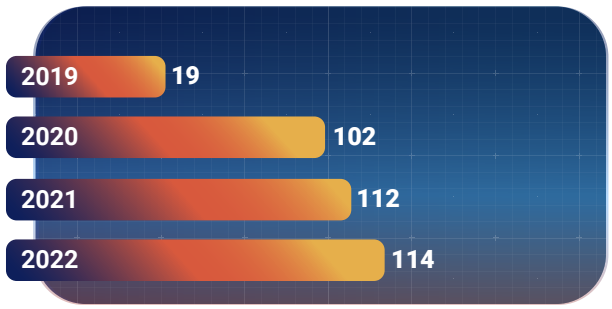
Three Advanced Persistent Threat (APT) groups—Tropical Scorpius, DEV-0530, and Andariel (also known as Lazarus)—have been recently identified as deploying ransomware as part of their attack arsenal. These APT groups use Cuba, H0lyGh0st, and Maui ransomware, respectively, to target their victims. While DEV-0530 and Andariel have been confirmed to be operating out of North Korea, we do not have details of Tropical Scopious' origin.



More Details

Ransomware vulnerabilities affecting multiple vendor products

Vulnerabilities are often found in multiple products and vendors, thanks to the reuse of software components. With this index update, 114 CVEs have been found in multiple products and vendors. Among the newly associated vulnerabilities in Q2 and Q3, CVE-2017-8046 is found in three products belonging to two vendors, Pivotal Software and VMware, while CVE-2020-0601 is found in six products affecting Microsoft and Golang.



More Details

Ransomware vulnerabilities excluded from the CISA KEV catalog

CISA continues to add vulnerabilities to the Known Exploited Vulnerabilities (KEV) catalog. At the time of this report, there are 827 vulnerabilities in the catalog; of the 323 ransomware vulnerabilities, 124 are still not listed in the CISA's KEV catalog.

More Details

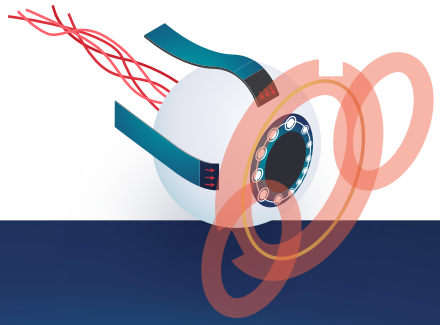
New weakness categories are contributing vulnerabilities to ransomware attackers

In the last two quarters, no less than 16 weaknesses* (CWEs) have contributed 17 vulnerabilities to ransomware, and the top three CWEs are CWE-917 (Improper Neutralization of Special Elements Used in an Expression Language Statement), CWE-943 (Improper Neutralization of Special Elements in Data Query Logic), and CWE-610 (Externally Controlled Reference to a Resource in Another Sphere). This is a vicious cycle with no way to break the wheel. Software developers consistently introduce vulnerabilities adopted by ransomware criminals to launch deadly attacks. Until testing for security is introduced early in the DevOps cycle, we will continue to see this trend.

***Note:** *MITRE describes "weaknesses" as flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture that—if left unaddressed—could result in systems, networks, or hardware being vulnerable to attacks.*

More Details

Definitive Insights

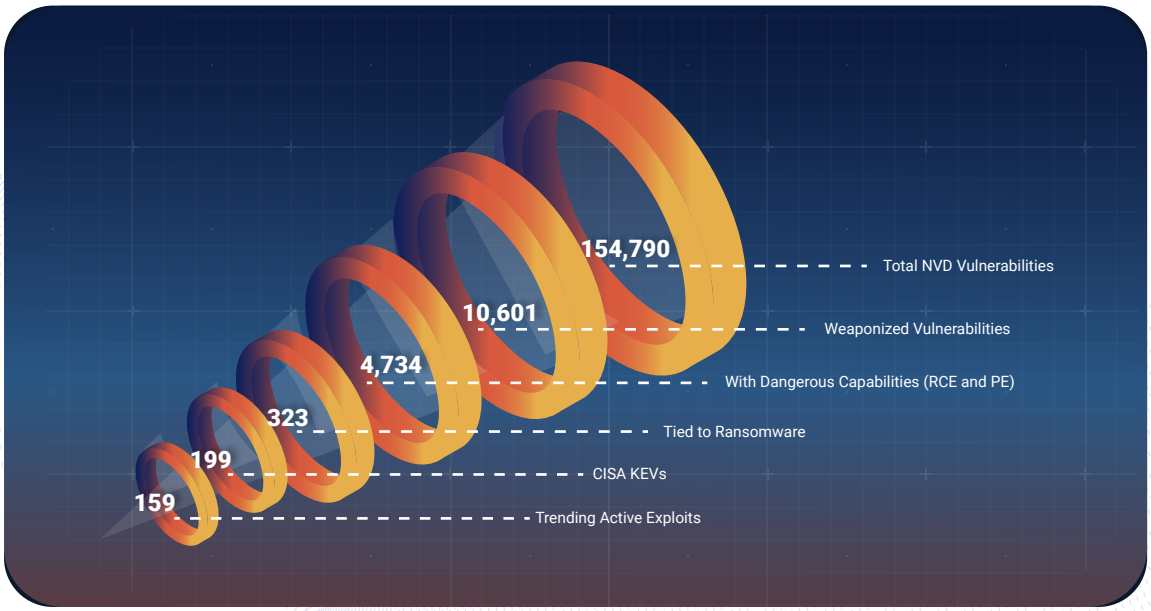


Data and intelligence collated from multiple sources and analyzed for accuracy and metrics presented in comparison with our previous reports

Ransomware index 2022 — Q2 and Q3

Focus	Q1 2022 (Total)	Q2 2022 (Total)	Q2 (Change)	Q3 2022 (Total)	Q3 2022 (Change)
CVEs associated with ransomware	310	312	2 new CVEs	323	11 new CVEs
CVEs missed by scanners	11	16	5 new CVEs	18	2 new CVEs
Ransomware vulnerabilities added to the DHS CISA KEV	141	188	47 new CVEs	199	11 new CVEs
Ransomware families that have newly emerged	161	163	3 new families* *2 families have merged into a single family	170	7 new families
Low-scoring* CVEs tied to ransomware *CVSS v2 score less than 8	193	195	2 new CVEs	202	7 new CVEs
Older* vulnerabilities associated with ransomware *Vulnerabilities from 2021 or earlier	310	311	1 new CVE	319	8 new CVEs
CWEs	63	64	1 new CWE	76	15 new CWEs* *Few CVEs have been remapped to more appropriate CWEs
Number of APT groups associated with ransomware	43	43	NA	46	3 new associations
Actively exploited* and trending vulnerabilities *Used with ransomware	157	157	NA	159	2 new CVEs
Exploit kits in use by ransomware	31	31	NA	31	NA

Ransomware vulnerabilities funnel



Here, we present a channelized view of vulnerabilities we have been tracking, specifically focusing on the ransomware segment.

CSW adopts a risk-based perspective, prioritizing vulnerabilities with threat associations. By funneling the most dangerous vulnerabilities, we help organizations focus on weaknesses that attackers find easy to exploit.

Note: *While the primary focus of this ransomware report is the vulnerabilities from 2010 onward, we would like to highlight five outliers. These were published between 2007 and 2009, but we found them actively trending during our research.*

- *CVE-2008-3431 affects xVm VirtualBox from Sun.*
- *CVE-2009-0824 and CVE-2009-3960 affect multiple products from SlySoft and Adobe, respectively.*
- *CVE-2007-1036 and CVE-2008-2992 are present in product offerings from multiple vendors.*

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

New vulnerabilities associated with ransomware

Our researchers identified 13 new vulnerabilities associated with ransomware in Q2 and Q3 of this year. From 57 vulnerabilities in 2019, there has been a 466% growth in the count of vulnerabilities associated with ransomware. As of Q3, there are 323 vulnerabilities that attackers can exploit to launch ransomware attacks; 159 of these vulnerabilities are currently trending in hacker channels.

10 of the 13 new ransomware vulnerabilities have critical severity ratings. One of the new findings, CVE-2020-36195 associated with one of QNAP's Network Attached Storage (NAS) solutions, has yet to be included in the Cybersecurity & Infrastructure Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalog.

S.No.	Vulnerability	Associated Ransomware Family	Vendor	Product	Severity
1	CVE-2021-40539	AvosLocker	Zoho Corporation	ManageEngine ADSelfService plus	Critical
2	CVE-2022-26134	AvosLocker and Cerber	Atlassian	Confluence, Confluence Data Center, and Confluence Server	Critical
3	CVE-2020-12812	Play	Fortinet	FortiOS	Critical
4	CVE-2021-35211	CryptoMix	SolarWinds	Serv-U File Server and Serv-U	Critical
5	CVE-2020-5135	Babuk	SonicWall	SonicOS	Critical
6	CVE-2021-20021	FiveHands	SonicWall	Email Security, Hosted Email Security, and Email Security Appliance	Critical
7	CVE-2021-20022	FiveHands	SonicWall	Email Security, Hosted Email Security, and Email Security Appliance	High
8	CVE-2021-20023	FiveHands	SonicWall	Email Security, Hosted Email Security, and Email Security Appliance	Medium
9	CVE-2020-2509	QNAPCrypt and Qlocker	QNAP	QTS and QuTS hero	Critical
10	CVE-2020-36195	QNAPCrypt and Qlocker	QNAP	QTS, Media Streaming Add-on, and Multimedia Console	Critical
11	CVE-2022-27593	DeadBolt	QNAP	Photo Station and QTS	Critical
12	CVE-2022-26352	H0lyGh0st	dotCMS	dotCMS	Critical
13	CVE-2022-29499	Lorenz	Mitel	MiVoice Connect	Critical

Vulnerability is trending | Vulnerability is a CISA KEV

Vulnerability Highlights

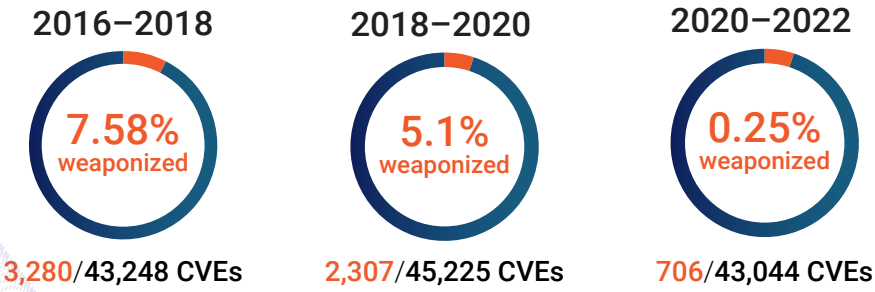
- Four of the new vulnerabilities are over a year old, going back to 2020, highlighting the importance of cyber hygiene.
- Vulnerabilities such as CVE-2022-26352 (dotCMS), CVE-2021-40539 (Zoho Corporation), and CVE-2021-20023 (SonicWall) can allow attackers to exploit web applications and remotely execute malicious code. CVE-2022-26352, additionally, can allow attackers to gain elevated privileges within exposed networks providing hackers an easy way inside organizations' networks.
- CVE-2021-20023 is the only medium severity vulnerability in this crowd of high and critical severity vulnerabilities, recently associated with the FiveHands ransomware.

We Told You So!

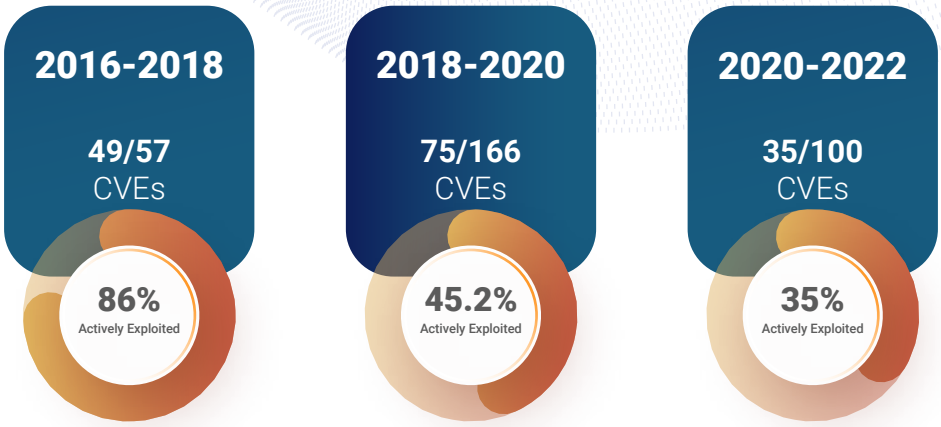
We had warned our customers about these vulnerabilities, owing to their potential impact on exploitation and increased hacker chatter, before they became conclusively associated with ransomware. Here is a look into the vulnerabilities explicitly called out in our blogs.

Vulnerability	Vendor	Product	When Did CSW Warn
CVE-2022-26134	Atlassian	3 products	Jun 2022
CVE-2020-12812	Fortinet	FortiOS	July 2021
CVE-2021-35211	SolarWinds	Serv-U File Server and Serv-U	Aug 2021
CVE-2021-40539	Zoho Corporation	ManageEngine ADSelfService Plus	Oct 2021
CVE-2022-27593	QNAP	Photo Station and QTS	July 2022
CVE-2020-2509	QNAP	QTS and QuTS hero	July 2022
CVE-2022-26352	dotCMS	dotCMS	July 2022
CVE-2022-29499	Mitel	MiVoice Connect	July 2022

A year-on-year comparison interestingly shows that the percentage of weaponized vulnerabilities with respect to the overall vulnerabilities identified in the period has reduced significantly. However, 706 vulnerabilities have become weaponized in the last two years alone.



Attackers are scouring the web regularly for unpatched instances to exploit, and 35% of the vulnerabilities associated with ransomware between 2020 and 2022 have been actively exploited. Though 35% is a slight improvement from 2018 to 2020 (45%), it is no less worrying.



"Ransomware menace continues to grow. We have seen a 466% growth in the count of ransomware vulnerabilities in the past few years. Through this data and research, we have enabled many of our customers to gain resilience through our Vulnerability Intelligence and ASM, providing them a hacker's view of their attack surface," Aaron Sandeen, CEO and Co-founder of CSW.

MITRE ATT&CK Research Findings

Security teams need an understanding of standard adversary techniques that could pose a threat to their organizations. Since it is impossible to monitor every single type of attack, MITRE created the ATT&CK framework that catalogs the exact steps and methods used by attackers to mount their attacks.

A MITRE ATT&CK kill chain is a model where each stage of the attack can be defined, described, and tracked, visualizing each move made by the attacker. Each of the tactics that are described within this kill chain has multiple techniques that will help the attacker accomplish a specific goal. This framework has detailed procedures for each technique and catalogs the tools, protocols, and malware strains that were used by attackers in real-world attacks. Security researchers consequently use these frameworks to understand attack patterns and focus their efforts on detecting exposures, evaluating current defenses, and tracking attacker groups.

As part of our research, CSW's experts mapped 323 ransomware vulnerabilities to their MITRE ATT&CK Techniques, Tactics, and Procedures (TTPs) kill chain and found that 57 ransomware vulnerabilities have an entire kill chain mapped from initial access to exfiltration, making these vulnerabilities extremely dangerous.

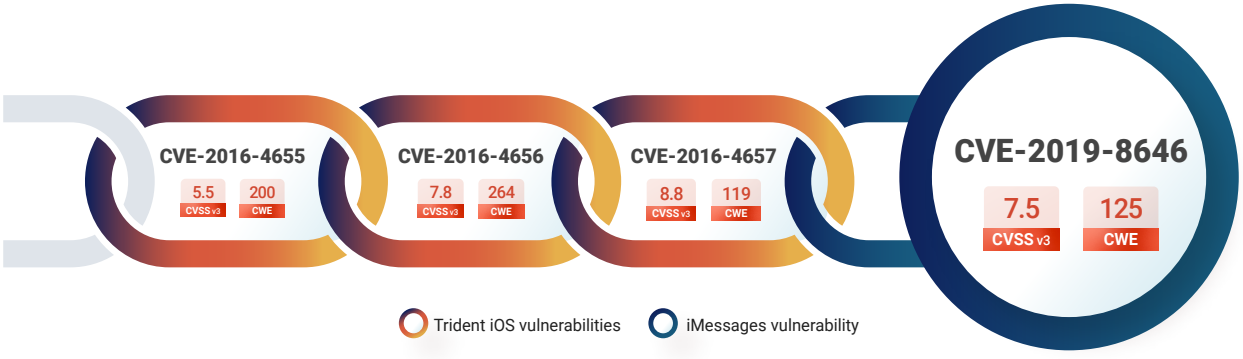
With these 57 vulnerabilities, attackers can completely take over the system from end to end, execute any code, freely move within the network, and manipulate and extract data.

Some of the primary vendors that have these 57 vulnerabilities include Microsoft, Oracle, VMware, Atlassian and Apache and 15 others. Of these, 34 vulnerabilities are Remote Code Execution (RCE) and Privilege Escalation (PE) exploits. The CISA KEV catalog has prioritized 31 of these CVEs out of which CSW experts have already warned about 11 of them. The following three vulnerabilities—CVE-2017-6884 (QNAP), CVE-2019-2729 (Oracle) and CVE-2020-16875 (Microsoft)—have not been included in CISA yet.

We have also observed attackers chaining multiple vulnerabilities to complete the kill chain to mount crippling attacks on their targets.

When operators of the FiveHands Ransomware went after four SonicWall VPN vulnerabilities (CVE-2021-20016, CVE-2021-20021, CVE-2021-20022, and CVE-2021-20023) in a single campaign, they followed the kill chain (given below) from credential access to exfiltration and impact.

In the case of the infamous Pegasus, the attackers chained Trident iOS vulnerabilities - CVE-2016-4655, CVE-2016-4656, and CVE-2016-4657—to jailbreak iPhones during an attack.

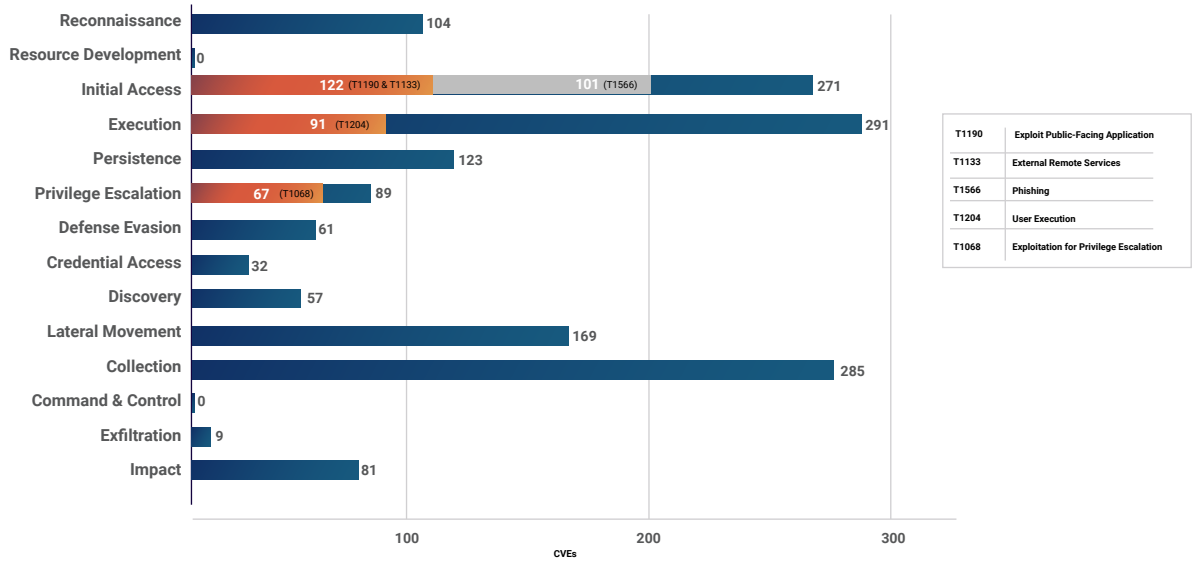


We have observed vulnerability chaining becoming a popular technique for attackers to link vulnerabilities to move deep into their target's network. Our Ransomware 2022 Spotlight Report highlighted how the LockFile ransomware group and the Hafnium APT group chained vulnerabilities in widespread attacks.

For deeper insights into how ransomware operators utilize techniques like vulnerability chaining in their attacks, check out our next annual report (scheduled to be released in January 2023), where we will be delving deep into vulnerability chaining.

Other highlights from our research

We also categorized and mapped the rest of the ransomware vulnerabilities to MITRE ATT&CK techniques, and the following are the findings:



Note: There are no vulnerability associations for Resource Development and Command & Control techniques.

Initial Access: This is a tactic wherein the attacker tries to get into your network using various entry points (also known as attack vectors) to gain a foothold within the network. The most popular technique is spear phishing, which exploits vulnerabilities on public-facing web servers.

We mapped 271 vulnerabilities to the Initial Access tactic. We found that attackers can exploit 122 ransomware-associated vulnerabilities to gain initial access by targeting external remote services (T1133) such as VPNs and other access devices that allow users in external locations to connect to the internal network and public-facing applications (T1190) like websites and database (SQL) servers.

The misconception that human interaction is required to gain initial access is wrong because attackers can easily get into your network with the help of these 122 vulnerabilities.

Vulnerabilities such as CVE-2021-44228 in Apache Log4Shell (exploited by Conti ransomware and three others) and CVE-2021-26134 in Confluence RCE (exploited by CryptoMix ransomware) are perfect examples as they help hackers gain the initial access into their target networks.

According to a report released by Palo Alto Networks, attackers take less than 15 minutes to scan for vulnerable endpoints after a new vulnerability is disclosed and announced in the NVD. Attackers are extremely agile and aggressive in exploiting zero-day vulnerabilities; for organizations, it is a race against the clock to patch and mitigate before they are attacked.

Spear Phishing - Spear phishing is a popular technique used by cyber criminals wherein the targeted victim (individual, organization, or business) receives a fake email with malicious links or attachments. These emails will coax the victims to divulge their personal details or prompt them to click on malicious links that would lead to compromise.

We found 101 CVEs mapped to the spear phishing attachment: T1566.001 and spear phishing link: T1566.002 combined.

This highlights the reliance of ransomware authors on this particular tactic to target applications and browsers and that they are not dependent only on remote access. With 101 CVEs to phish, attackers are spoilt for choice as they carefully design authentic-looking emails and messages to hoodwink their victims.

Vulnerabilities such as CVE-2017-11882 in Microsoft Office (linked to seven ransomware families) and CVE-2018-20250 in WinRAR Path Traversal (exploited by four ransomware families) are good examples.

Pegasus also makes a great example here. Attackers created a simple phishing message that, when clicked, created backdoor access to an iPhone, leading to the infiltration and compromise of iPhone devices of many worldwide figures.

User Execution - This technique relies on the user to perform specific actions that would cause them to execute a malicious code sent through a phishing email.

We found 91 ransomware-targeted vulnerabilities were mapped to T1204: User Execution. This means attackers rely on victims clicking on malicious files (T1204.002) or malicious links (T1204.001) for exploitation.

Microsoft Office RCE vulnerability CVE-2017-0199 (deployed by four ransomware families) and Internet Explorer Memory Corruption Vulnerability CVE-2021-26411 (exploited by Cerber ransomware) make great examples as they allow the attacker to execute this technique.

Privilege Escalation (PE) - This is a type of cyber attack wherein the attacker tries to gain higher privileges after infiltrating into the victim's network and moves laterally to abuse these privileges. Attackers try to exploit these types of vulnerabilities by finding weak entry points into the organization's defense.

Organizations that fail to follow the principle of least privilege, where users have more privileges than required, are at risk. We have seen many instances where attackers also exploit software vulnerabilities to gain higher privileges. CSW classifies these vulnerabilities with PE capabilities as extremely dangerous and recommends that they be patched and remediated immediately.

Our research found that ransomware actors can exploit 67 vulnerabilities to elevate privileges (T1068), easing lateral movement across organizations' domains. Microsoft Exchange Server Elevation of Privilege Vulnerability - CVE-2021-34523, which is linked to nine ransomware families (Conti, AvosLocker, BackCat, and others), makes a good example.

These findings prove that ransomware authors rely on human interaction to click on malicious links and files to launch their initial attack. That said, there are also vulnerabilities that provide them the initial access within the victim's network without any user interaction. From an attacker's point of view, vulnerabilities that can be easily exploited, providing them with easy pathways to infiltrate and mount attacks, will always be favored over others.

Organizations must level up their security strategy to stay safe from evolving ransomware threats. They must practice cyber hygiene and use robust solutions such as Attack Surface Management (ASM) to stay ahead of attackers and emerging ransomware threats.

This research also highlights the need for rigorous cybersecurity campaigns that must be used to educate the public and increase their awareness to stay safe from these threats.

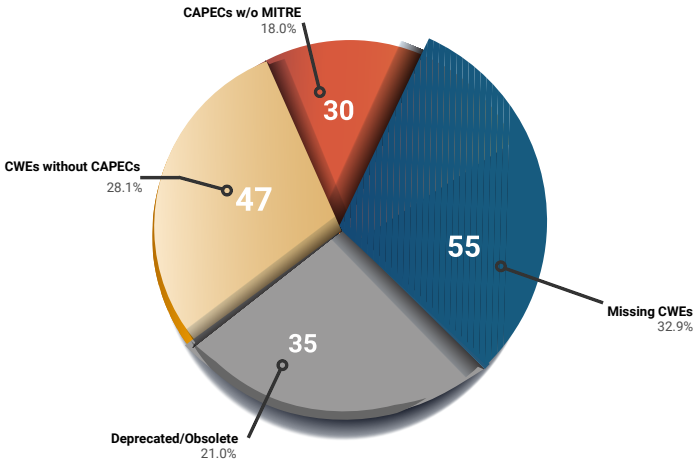
We found 57 ransomware vulnerabilities with the MITRE ATT&CK kill chain from infiltration to exfiltration. Want access to this data?

Talk To Us

Gaps in MITRE mapping are enabling ransomware criminals

Gaps in information in the NVD, MITRE ATT&CK, and CAPEC data repositories are a handicap for security researchers, inhibiting them from prioritizing vulnerabilities; consequently, this exposes organizations to ransomware attacks.

Based on our MITRE research on the CISA KEV catalog and ransomware vulnerabilities, a researcher will need to refer to around 17+ resources on average to collate accurate information.



Ransomware Vulnerabilities with Data Gaps

During this research, we found that eight weaknesses have become obsolete, suggesting that details have not been actively maintained or reviewed. This makes it difficult for researchers to map the vulnerability to the correct weakness and understand its threat context. This often results in researchers ignoring the vulnerability due to the lack of information and not prioritizing it for remediation.

Obsolete CWE	CWE_Name	Mapped CVEs
CWE-264	Permissions, Privileges, and Access Controls	18
CWE-189	Numeric Errors	6
CWE-399	Resource Management Errors	3
CWE-254	7PK Security Features	3
CWE-255	Credential Management Errors	2
CWE-16	Configuration	1
CWE-19	Data Processing Errors	1
CWE-310	Cryptographic Issues	1

Incomplete and missing data result in organizations missing the key context about how vulnerabilities can be exploited in ransomware attacks, leading to the prioritization of less significant vulnerabilities.

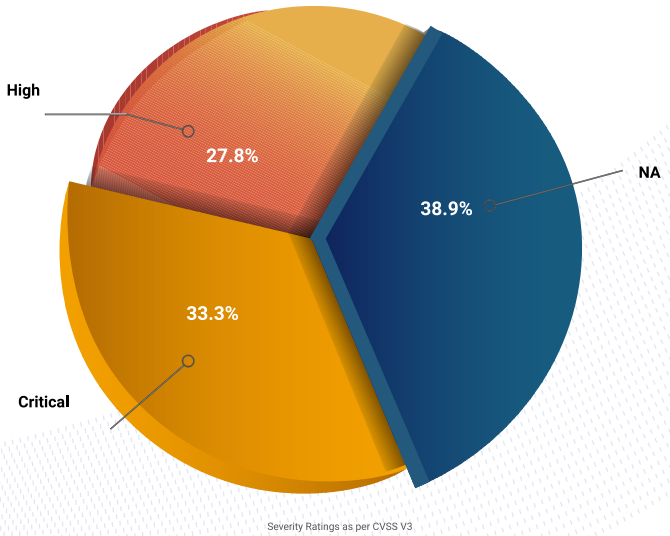
Furthermore, we analyzed 76 weaknesses overall, powering the 323 ransomware vulnerabilities. Of these, only 14 in the MITRE's top 25 most dangerous weaknesses list show up in the top 25 weaknesses powering ransomware vulnerabilities. This is yet another indication of the lack of 'threat context,' inhibiting the right prioritization of weaknesses.

MITRE and ATT&CK tactics are powerful repositories that a security researcher can use to identify and break kill chains, provided these gaps in information are fixed, and the data is continuously updated with accurate intel.

Ransomware vulnerabilities missed by popular scanners

As part of our research, CSW's experts track whether popular scanners such as Nessus, Nexpose, and Qualys detect ransomware vulnerabilities; in Q2-Q3, we found that the scanners are missing 18 of them.

Here is our analysis of these 18 vulnerabilities -



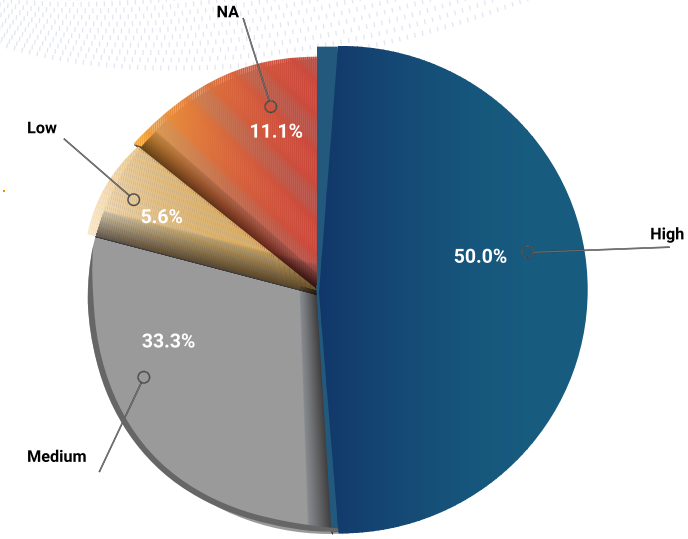
Severity Ratings as per CVSS V3

Severity Ratings as per CVSS V3

Severity ratings are calculated by the Common Vulnerability Scoring System (CVSS V3), which has been used since 2015. A drawback of this scoring system is that CVSS V3 scores for vulnerabilities discovered between 2010 and 2015 are missing.

Severity Ratings as per CVSS V2

When we compared both severity ratings, we found that the missed ratings from V3 were ranked as Medium and Low, respectively, and one of the vulnerabilities did not have a rating.



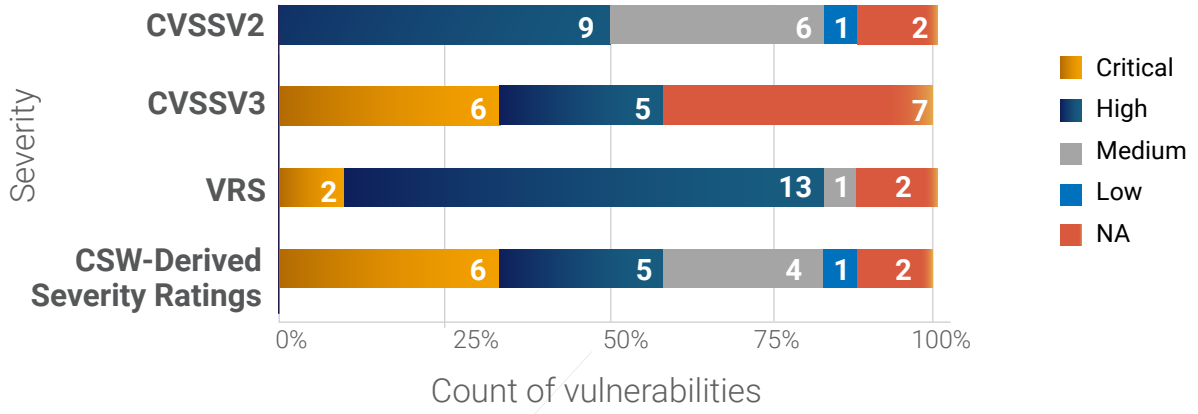
Severity Ratings as per CVSS V2

To fully understand the threat context of these undetected vulnerabilities, we applied a scoring methodology that is used in our Securin's Vulnerability Intelligence (VI) platform called the Vulnerability Risk Score (VRS). VRS is calculated based on the risk every vulnerability poses, taking into consideration looming threats, weaponized exploits, and potential impact, amongst others.

To address the issue of missing scores for the vulnerabilities in the NVD, CSW uses proprietarMachine Learning models to derive the severity score. This is equivalent to the CVSS V3 score, or the V2 scores where V3 is unavailable.

Once we derived the scores for the missing vulnerabilities, we found that 11 out of 18 vulnerabilities are rated Critical and High, and popular scanners (Nessus, Nexpose, and Qualys) do not have plugins for these vulnerabilities yet.

An interesting thing that we noted from this investigation was how ransomware operators were exploiting the NVD-rejected vulnerabilities. CVE-2019-9081, a vulnerability in the Laravel framework, and CVE-2015-2551 (product details not available) make perfect examples. CVE-2019-9081 is exploited by Satan and Mailto ransomware families, and CVE-2015-2551 by several ransomware families.



Rejected by the NVD, both these vulnerabilities do not have severity scores. With scanners lacking the plugin, we can see why ransomware operators find them interesting, as these vulnerabilities make a perfect addition to the arsenal of ransomware operators.

Other Observations:

- **Third-party integrations invite unwelcome party guests**
  - CVE-2017-18362: SQL Injection ConnectWise ManagedITSync integration through 2017 for Kaseya VSA, exploited by GandCrab ransomware, is a third-party plugin for Kaseya VSA.
  - While Kaseya products have coverage across vulnerability scanners, third-party software plugins (mentioned above) are often missed by scanners, leading to dangerous consequences.

- **Crucial data left unprotected**
    - Vulnerabilities such as CVE-2013-3993 (IBM Infosphere), CVE-2015-7465 (IBM Jazz Reporting Service), and CVE-2020-36195 (QNAP NAS) can have an impact on critical data. These vulnerabilities can allow for direct interaction with data and storage, and the fact that scanners do not detect these vulnerabilities exposes organizations to great risk.

- **Vulnerabilities in network devices are invisible**
    - Three vulnerabilities undetected by scanners belong to routers. CVE-2017-6884 impacts Zyxel routers, and CVE-2019-16057 and CVE-2019-16920 impact D-Link routers. The compromise of network devices can make it absurdly simple for attackers to gain initial access and conduct lateral movement.

On October 3, 2022, CISA issued a new Binding Operation Directive 23-01 focusing on improving asset visibility and vulnerability detection. This directive explicitly calls out that federal agencies must update vulnerability detection signatures every 24 hours starting April 2, 2023, validating the importance of this research.

Note: Scanner plugins are updated regularly. The information included here is the data available when writing this report.

Download the list of ransomware vulnerabilities that are not detected by scanners.

The need for a software bill of materials

Identifying vulnerabilities in your attack surface depends on adopted techniques, the context of scanning, and whether they are authenticated or unauthenticated approaches. Commercial scanners in the market will not be able to detect vulnerabilities in assets such as containers. One of the ways to improve this is to adopt the software bill of materials (SBOM) method to identify individual components and better identify exposures.

Vendors, developers, and consumers must focus on regularly maintaining and sharing a thorough SBOM to understand the dependencies within and outside their environment. Then, the SBOM must be cross-referenced against an accurate vulnerability database that can map the risks to organizations. A detailed SBOM analysis can not only help you identify vulnerabilities in your container, cloud, and code libraries but also help identify if you are using the latest versions of each of these offerings.

A vulnerability database that also considers the threat context, together with a detailed SBOM, must be your go-to solution to identify ransomware and other threats that could easily invade your network.

Here is a sneak preview of our SBOM analysis of the ransomware vulnerabilities. We will be delving deep into this in our next annual report (scheduled to be released in January 2023). This is what a good bill of materials integrated with a threat-aware vulnerability database can provide to you:

CVE	Package Name	Impacted Versions	Fixed Version
CVE-2015-1427	org.elasticsearch:elasticsearch	<=1.3.7 >=1.4.0,<=1.4.2	1.3.8 1.4.3
CVE-2016-3088	org.apache.activemq:activemq-client	>=5.0.0,<5.14.0	5.14.0
CVE-2017-9805	org.apache.struts:struts2-rest-plugin	<2.3.34 >=2.5.0,<2.5.13	2.3.34 2.5.13
CVE-2018-1000136	electron	>=1.7,<1.7.13 >=1.8,<1.8.4 >=2.0.0-beta.1,<2.0.0-beta.5	1.7.13 1.8.4 2.0.0-beta.5
CVE-2018-1000861	org.jenkins-ci.main:jenkins-core	<=2.138.3 >=2.140,<=2.153	2.138.4 2.154

Three more APT groups started using ransomware

We have been tracking the association of APT groups every quarter and have found them adopting ransomware as part of their arsenal. In Q1 2022, a total of 43 APT groups used ransomware as part of their arsenal to mount attacks on their victims. In the past two quarters, three more threat groups have found it effective to use ransomware, bringing the total to 46.

The following APT groups have started deploying ransomware as part of their arsenal in Q2 and Q3 2022.

APT Group	Popular Aliases	Origin Country	Ransomware Used
Andariel	Lazarus group, APT38, and TA404	North Korea	Maui
Tropical	NA	Under Research	Cuba
DEV-0530	NA	North Korea	H0lyGh0st

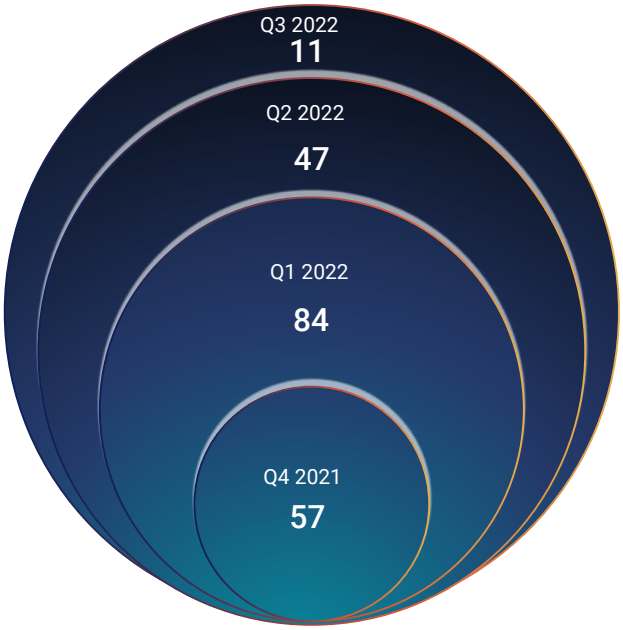
The Lazarus (Andariel) group, in particular, has been extremely active in Q2 and Q3 of 2022. The group recently forged into the cryptocurrency space, stealing currency from crypto platforms, such as Harmony Horizon Bridge and deBridge Finance, and using social engineering campaigns to target crypto experts in the fintech industry. Lazarus targets organizations in the government and private sectors, energy, aerospace, defense, engineering, finance, media, shipping and logistics, technology, and BitCoin exchanges. It is also known to target a wide range of countries, including South Korea, the United States, Thailand, France, China, Hong Kong, the United Kingdom, Guatemala, Canada, Bangladesh, Japan, India, Germany, Brazil, and Australia.

The Tropical Scorpius group was first identified in 2019 and has been recently spotted deploying new tools and tactics in its attacks. The group is known to favor the use of the Cuba ransomware, and its primary target is the USA. The group targets the government, manufacturing, transportation, logistics, health care, finance, high-tech, construction, education, energy, utilities, legal services, wholesale, retail, and real estate sectors.

DEV-0530 is a North Korean-based APT group first observed in 2021. The group is known to target organizations in the education, event management, finance, and manufacturing sectors. The actor is believed to have connections with the Andariel group and deploys the H0lyGh0st ransomware in its attacks.

From an overall perspective, when we analyze the origin countries of the APT groups, we find that Russia leads the pack with 11 APT groups, followed closely by China with eight; Iran is third in line with four APT groups. With hostile governments using state-sponsored threat groups to infiltrate, destabilize, and disrupt operations in their target countries, ransomware and malware are now being used as a precursor to physical warfare. This was amply evidenced in the recent Russia–Ukraine war.

Ransomware vulnerabilities in CISA KEVs



Note: The numbers are as on September 20, 2022

CISA's KEV catalog is a living list of vulnerabilities that hackers often exploit. This list, which began small with 287 vulnerabilities on November 03, 2021, is today an 800+ catalog and is getting updated continuously multiple times a month.

With this catalog, CISA has mandated public sector companies, federal agencies, and government entities to patch vulnerabilities often exploited by attackers and improve their security posture to safeguard their assets.

Though the KEV catalog is a valuable list for organizations to start their vulnerability management engine, the CISA website does not provide adequate threat context or explanation as to why a particular vulnerability ought to be patched on priority, and the constant updating of this list now requires prioritization within the CISA vulnerabilities to meet deadlines.

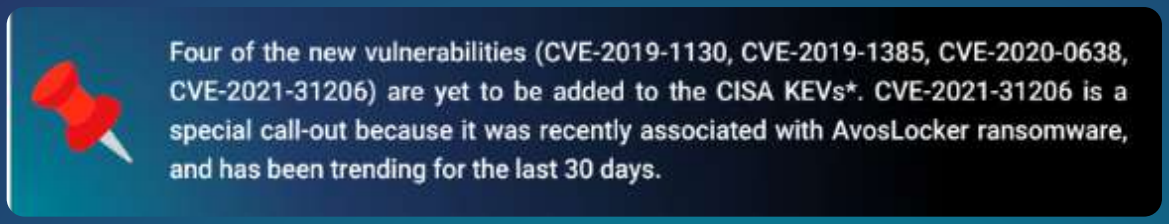
Further, a recent Binding Directive released by CISA highlights the importance of asset discovery and enumeration of the vulnerabilities in those assets to understand an organization's exposure completely. This goes hand-in-hand with our MITRE and scanner analyses that highlight the need for authenticated scans to discover the totality of vulnerabilities plaguing your network as seen from an attacker's purview.

Of the newly added vulnerabilities in Q2 and Q3 2022, CVE-2020-36195 (present in three products from QNAP) has not yet been added to the KEV catalog.

Three of the newly added ransomware vulnerabilities in Q1 2022 are now a part of CISA KEVs.

CSW's Ransomware Index Report for the first quarter of 2022, published on May 18, 2022, explicitly highlighted four vulnerabilities worthy of being added to the CISA KEVs based on our pentesters' analysis of the vulnerabilities and their capabilities.

A screenshot from CSW's Q1 2022 Ransomware Index Report published on May 18, 2022



After our warning, the following three ransomware vulnerabilities have been included in the CISA KEVs:

- CVE-2019-1130 (11 Microsoft products)
- CVE-2019-1385 (5 Microsoft products)
- CVE-2020-0638 (4 Microsoft products)

We highlight the top ransomware CVEs that are not in KEVs but have been flagged by our experts. These vulnerabilities have been red-flagged by our analysts because:

- They have been exploited by trending threats recently.
- They exist in popular products that have wide exposure.

Vulnerability	Vendor	Product	CVSS Severity	Ransomware Family Associations	Exposure
CVE-2021-31206	Microsoft	Exchange Server	High	AvosLocker	171,736 Exchange Server instances
CVE-2021-30119	Kaseya	Virtual System Administrator	Medium	Sodinokibi	29 Kaseya server instances
CVE-2021-30120	Kaseya	Virtual System Administrator	High	Sodinokibi	29 Kaseya server instances
CVE-2018-12808	3 vendors	6 products	Critical	Conti and Ryuk	Affects endpoints with Adobe Acrobat application software
CVE-2020-0609	Microsoft	Windows OS, Windows Server, and Remote Desktop Protocol	Critical	Conti and Sodinokibi	250,805 ports Also affects devices running Windows OS
CVE-2020-0610	Microsoft	Windows OS, Windows Server, and Remote Desktop Protocol	Critical	Sodinokibi	250,805 RDP ports Also affects devices running Windows OS

CSW's experts have red-flagged 124 vulnerabilities that are associated with ransomware and have not yet been added to CISA KEVs.

Note: The KEV list is continuously updated by CISA based on exploitation trends..

CWEs powering ransomware vulnerabilities

Our experts also analyze the Common Weakness Enumeration (CWE) categories of each vulnerability that exists within the ransomware vulnerabilities list. CWE is a community-developed list of weakness identification, mitigation, and prevention efforts. By mapping the vulnerabilities to CWEs, we can identify a high-level pattern of what kind of weakness is contributing the maximum number of vulnerabilities to ransomware operators and use this information to take preventive measures.

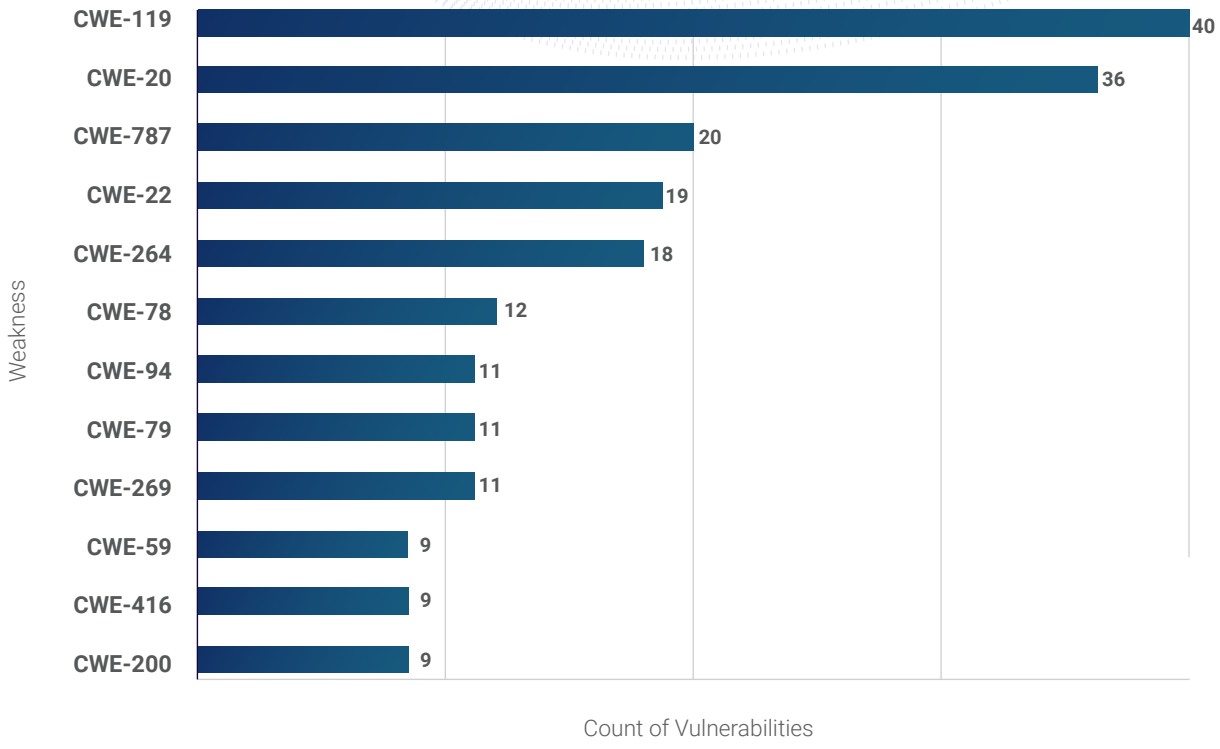
In this index report, we found that 16 new weakness categories now contribute ransomware vulnerabilities. This is a scary prospect as ransomware attackers are now looking for 16 additional drawbacks in products that they can exploit. Overall, we now have 76 CWEs giving rise to ransomware vulnerabilities.

Of the new weaknesses, we highlight the top three that could have the most impact:

- **CWE-917** arises from the improper neutralization of special elements. This is the latest weakness to be added to the popular Log4j vulnerability and can be introduced during the architecture, design, or implementation stages. The weakness has the capacity to allow unauthenticated attackers to insert executable code within existing code, leading to malicious code execution or other unexpected behavior. The weakness can also potentially lead attackers to gain initial access to external and public-facing applications.

- **CWE-943** is a weakness that directly impacts data, allowing attackers to inject additional clauses into queries. With this, attackers can modify and manipulate queries, append additional commands, and extract sensitive data.

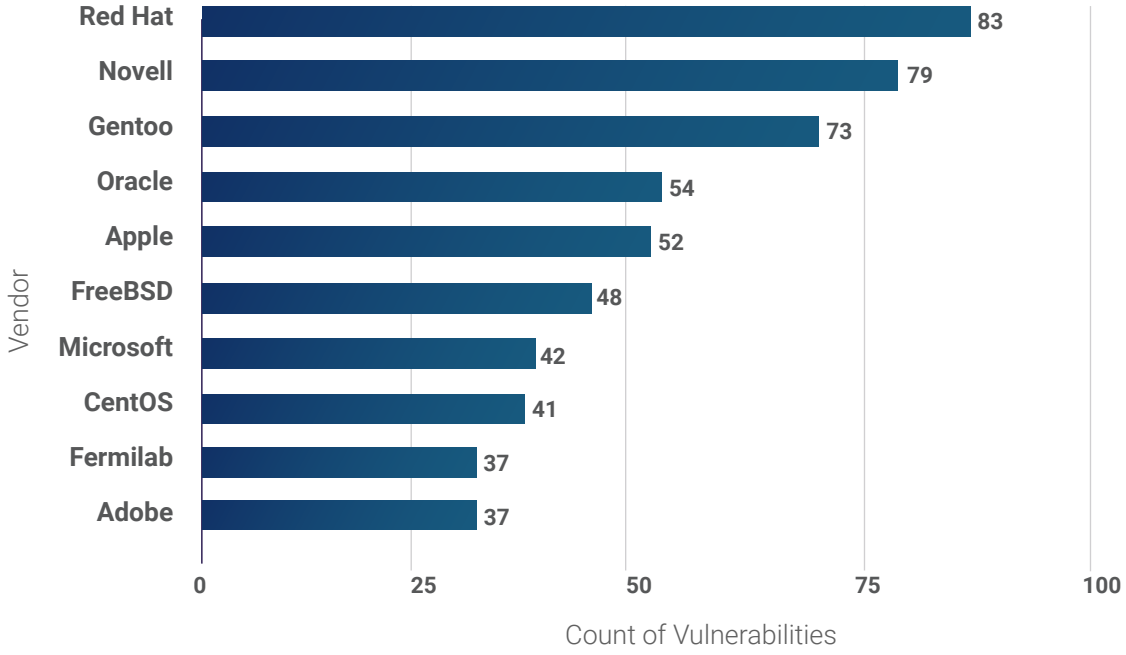
- **CWE-610** exists in products that are designed such that they can be controlled by an external resource outside of the intended control sphere. Attackers can exploit this weakness to modify files, making it dangerous. Unauthenticated access to critical functions can provide attackers with dangerous execution capabilities.



Note: Vulnerabilities are constantly assessed and remapped to more appropriate weaknesses by the MITRE, modifying the NVD data, which is dynamically reflected in our ransomware research.

Vulnerabilities affecting multiple vendor products

This is a trend that was called out in our ransomware report 2019, released by RiskSense (acquired by Ivanti). It is not uncommon to find a single vulnerability affecting multiple products and vendors, thanks to the reuse of software components. In 2020, 102 CVEs associated with ransomware had spread across multiple vendors and products. Over time, this number has increased to 114 CVEs. These 114 CVEs affect 706 unique products.



In 2022, Q2 and Q3 saw two ransomware vulnerabilities affecting multiple vendor products.

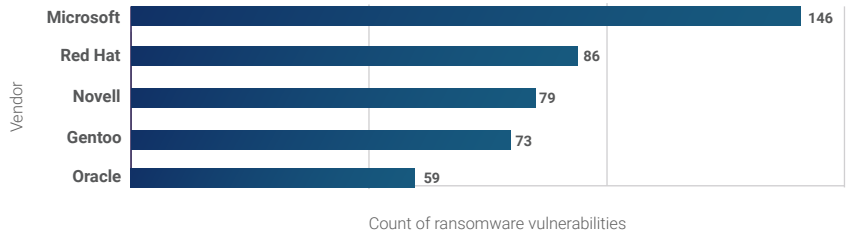
Vulnerability	Vendor	Product
CVE-2017-8046	Pivotal Software	Spring Boot
	Pivotal Software	Spring Data
	Pivotal Software	Spring Data REST
	VMware	Spring Boot
CVE-2020-0601	Microsoft	Windows 10
	Microsoft	Windows Server 2016
	Microsoft	Windows Server 2019
	Microsoft	Windows
	Microsoft	Edge
	Golang	Go

Reusing software components and open-source libraries is a hard problem to solve, as patching becomes a nightmare for security teams. Apache Log4J is a perfect example. The serious vulnerabilities that exist in this open-source library have been used in more than 273 products; ransomware groups such as Conti and others adopted these weaknesses to their fold within no time.

Vendor–product analysis of ransomware vulnerabilities

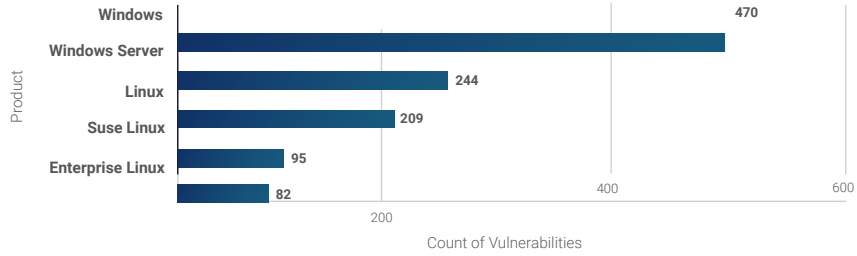
Our research has uncovered ransomware vulnerabilities in 111 unique vendors with 953 unique products. We look into the category of products affected by the new ransomware vulnerabilities identified in this index report.

Top vendors with the highest count of vulnerabilities in their products



Product Category	Vulnerability Count
REST API	1
Web Application	3
VPN	1
Operating System	4
Cloud Application	3
FTP Server	1
CMS	1
Software Application	1

Products with the most ransomware vulnerabilities



Note:

- Windows OS includes Windows, Windows 10, Windows 7, Windows 8, Windows 8.1, Windows RT 8.1, Windows Vista, Windows XP, Windows RT, and Windows 8.0.
- Windows Server includes Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2003, Windows Server 2022, Windows Server 1803, Windows Server 1709, and Windows Server.
- Linux includes Linux and Linux Kernel.

Vendors must adopt stringent security practices, address vulnerabilities before attackers can abuse them, and warn their customers well in advance. Users of third-party products must be extra vigilant in following vendor advisories to ensure they are on top of their security game.

Other significant findings

Newly identified ransomware families

CSW's research highlights 10 new ransomware families that have emerged in the past two quarters. Today, a total of 170 ransomware families are attacking their targets using 323 vulnerabilities, while the average number of vulnerabilities per family is 13.6.

Ransomware Family	Associated Vulnerability Count
Hive	7
BianLian	3
BlueSky	2
Play	2
Black Basta	1
NamPoHyu	1
Deadbolt	1
H0lyGh0st	1
Lorenz	1
Maui	1

Among the newly discovered ransomware families, PLAY and Hive groups follow many similar tactics in their attacks, leading to the assumption that the same threat actor could operate them.

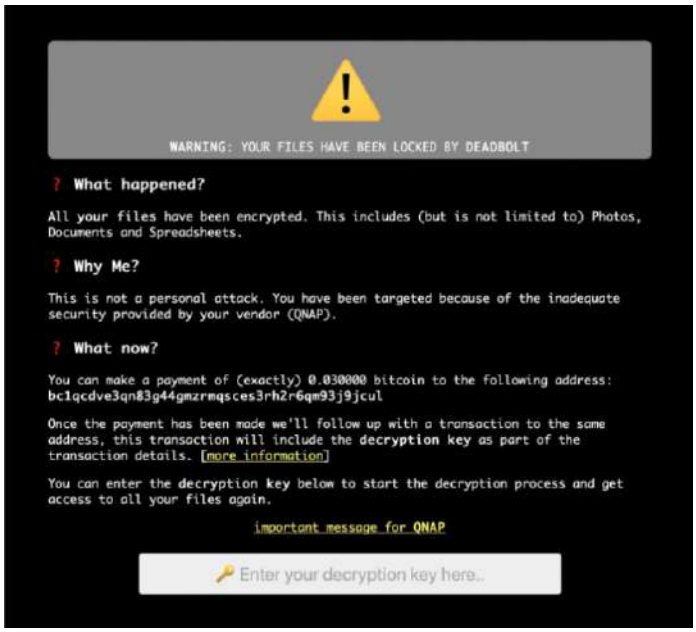
Hive ransomware has been active in the past quarter, adding seven vulnerabilities to its arsenal. It managed to cripple Costa Rica right when it was reeling under the aftermath of a Conti ransomware attack, resulting in the declaration of a national emergency. Hive ransomware, a part of the family by the same name, hit the country's public health service, completely disrupting medical aid, and was also responsible for taking down many government-run servers and user terminals, throwing the country into further disarray.

The following ransomware groups do not have a huge arsenal of vulnerabilities **yet**. Still, we call them out in this index report as they have been in the news for notorious attacks over the last two quarters.

- The FBI warned about the **Maui ransomware** being deployed by nation states against US health care and public health organizations, resulting in a ransom recovery by the feds to the tune of $500K. The ransom was recovered by following the cryptocurrency trail back to operators who deployed Maui ransomware against the victims.

"The returned ransom success story is meant to serve as a signal to other targeted organizations that working with law enforcement following a cybersecurity incident is "good business," Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division.

- The **DeadBolt** ransomware has been particularly notorious for going on a spree of attacks targeting NAS devices to the extent of hitting 3,600 devices in a single campaign, which forced the hand of QNAP to update its devices.



- The **Black Basta** group has been in the news for its possible links to the QBot malware and the Conti group while at the same time attacking the defense giant Elbit systems, the building materials giant Knauf, and the American Dental Association.

Among the 170 ransomware families, Cerber stands first with 70 vulnerabilities adopted within its fold, Crypwall comes second with 66, and Locky is third with 64 vulnerabilities. Ransomware operators are on the lookout for weaknesses that can be easily exploited, providing them with the least path of resistance to achieve their goals. The surge of new vulnerabilities and their adoption by these criminals has become a never-ending vicious cycle.

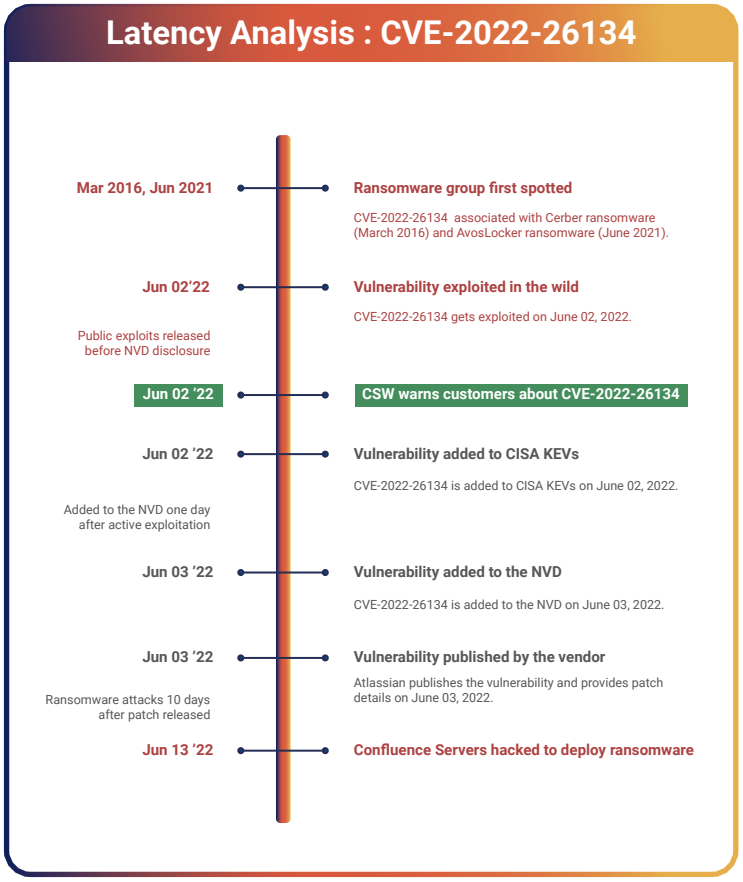
Note: *Ransomware families are constantly merging, regrouping, and reemerging from hibernation under new names and aliases. CSW's and Securin's researchers continuously update and collate information about them to provide our clients with accurate intel.*

Appendix C provides IoCs for a few of the most trending new ransomware families in Q2 and Q3 2022.

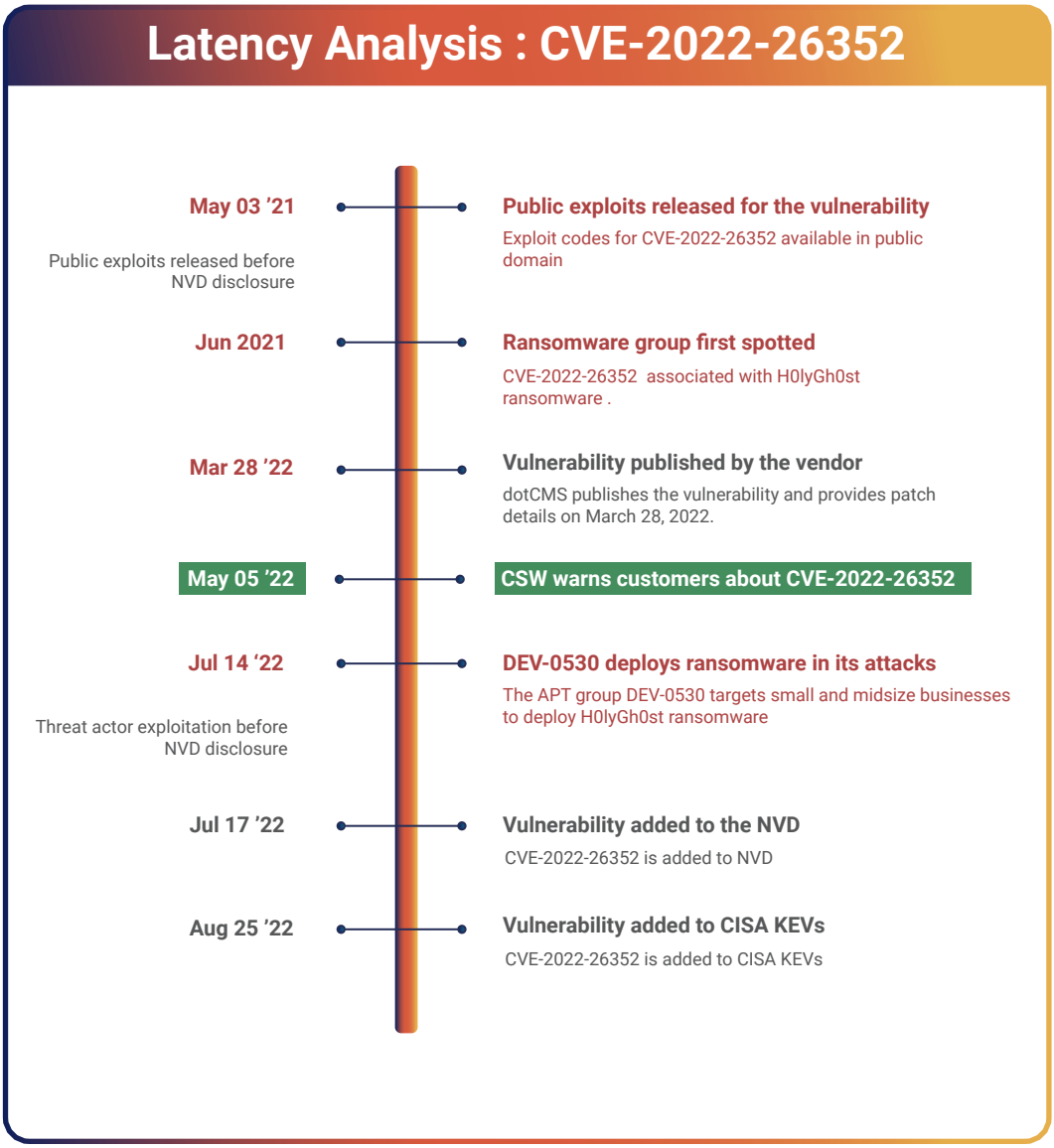
Latency analysis of new ransomware vulnerabilities

Traditional vulnerability management relied on vulnerability disclosure by sources such as the NVD or MITRE and evidence of exploitation in the wild. However, as noticed from our research thus far, attack windows are reducing at a rapid pace, with attackers going after vulnerabilities that product vendors have not yet discovered.

- Of the newly identified vulnerabilities, 54% of them were added to the NVD days after the CVE was disclosed by the vendor and provided with a patch.
- The NVD added CVE-2021-20022 even before the vulnerability was disclosed by its vendor.
- CVE-2022-26352, associated with the H0lyGh0st ransomware, is the standout of our latency analysis.
    - The vulnerability was added to the NVD 111 days after the vendor published it. Public exploits for the same were also released in the public domain in this interval.



- CVE-2022-26134, associated with AvosLocker and Cerber groups, was exploited a day before its vendor could publish it. It was added to the NVD the same day the vendor published the vulnerability.
- CVE-2021-40539 was disclosed by its vendor, added to the NVD, and had exploits released publicly, all on the same day.



This brings up the following important learnings:

- If organizations solely rely on the NVD for disclosure to patch vulnerabilities, they will be susceptible to attacks.
- Attackers are also going after vulnerabilities yet to be disclosed to the public, placing organizations at a high risk of being breached via exposures they are unaware of.
- Organizations need an accurate threat intelligence platform that can predict vulnerabilities likely to be exploited, enabling proactive patching.

Regular, cyclic patch management processes have today been overthrown by the need for agile, adhoc patching that can keep up with the changing threat landscape.

Srinivas Mukkamala, Chief Product Officer at Ivanti, says, "IT and security teams must urgently adopt a risk-based approach to vulnerability management to better defend against ransomware and other threats. This includes leveraging automation technologies that can correlate data from diverse sources (i.e., network scanners, internal and external vulnerability databases, and penetration tests), measure risk, provide early warnings of weaponization, predict attacks, and prioritize remediation activities. Organizations that continue to rely on traditional vulnerability management practices, such as solely leveraging the NVD and other public databases to prioritize and patch vulnerabilities, will remain at high risk of cyberattacks."

Importance of threat context for vulnerability prioritization

Although organizations adhere to stricter security norms today, attackers have become more sophisticated—faster, stealthier, and with a mix of old and new techniques—going after unpatched vulnerabilities. This calls to question the approach of prioritizing only critical- or high-severity vulnerabilities because 202 of the 323 ransomware CVEs have severity scores (CVSS v2) that are less than 8.

CSW's threat intelligence platform scored the ransomware vulnerabilities considering their threat context, and here are the results:

- CSW rates 45 CVEs as "critical"; these have a high or medium rating in the NVD.
- There are two low-severity CVEs (CSW gives them a medium and high rating) among the ransomware vulnerabilities.
- Our analysts mark 262 of the 323 vulnerabilities as having the highest likelihood of exploitation.

A Snapshot of Critical Infrastructure Sectors

Special Report: The impact of ransomware on industrial control systems deployed in critical infrastructure establishments

The US federal government has identified 16 critical infrastructure sectors that are vital to the ongoing functions of the country. This report provides a detailed analysis of 16 ransomware vulnerabilities targeting critical infrastructure—health care, energy, and manufacturing in particular—and the notorious ransomware operators such as Conti, Ryuk, Petya, WannaCry, and others going after the country's assets.

In this index report, our analysts and experts have added a special focus on the impact of ransomware on critical infrastructure. As defined by the DHS, critical infrastructure includes utilities—highways, bridges, tunnels, railways, and buildings—that maintain normalcy in daily life.

Such vital infrastructure's safe and efficient functioning depends on the industrial control systems that regulate the functionality of the infrastructure. Most currently deployed systems are legacy setups that include out-of-date software and, sometimes, even unsupported end-of-life components. Upgrading such infrastructure involves a huge financial overhead and technical expertise in migrating to modern technology.

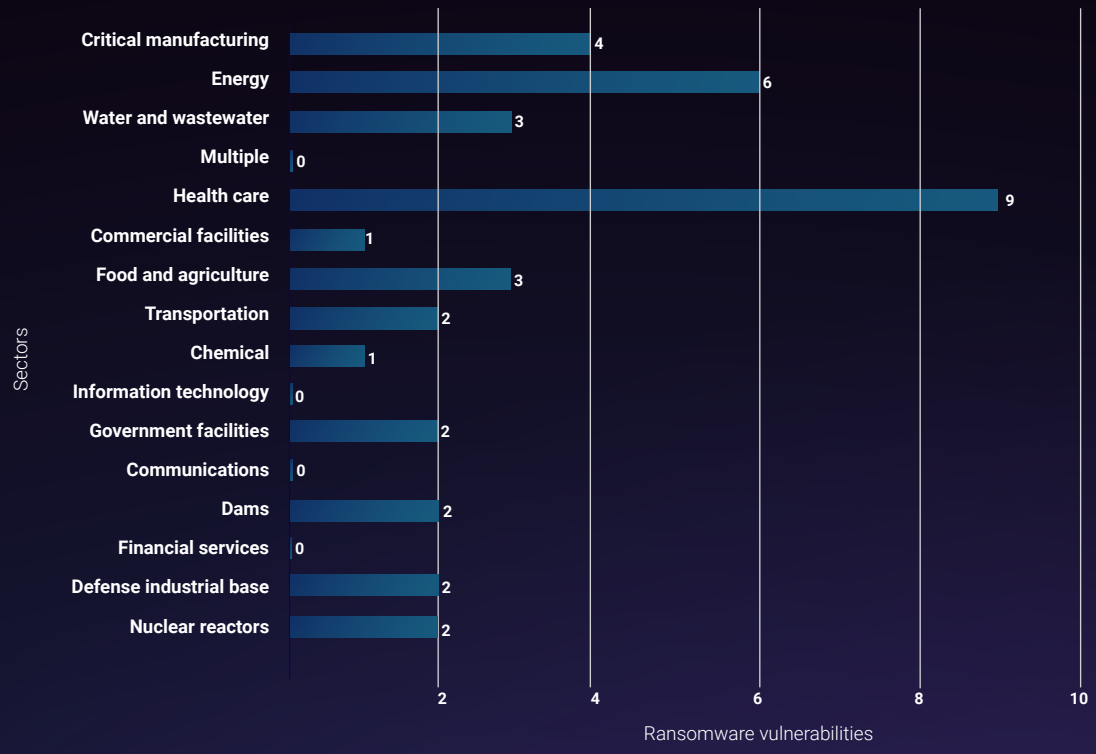
Such easily exposed attack vectors can be misused by attackers with malicious motives to cause catastrophic destruction that ranges from the loss of critical functionality and inadequate supply of basic essentials to the disruption of activities that affect the economy of the country.

The Industrial Control Systems Cyber Emergency Response Team(ICS-CERT) focuses on the security of control systems in collaboration with the US-CERT. CISA released a total of 58 ICS advisories between August 18 and September 26, 2022, emphasizing how crucial it is for critical infrastructure attack surfaces to be airtight and secure.

Our analysts investigated the control systems of critical infrastructure, and here are our key findings:

- There are 16 vulnerabilities associated with ransomware groups, such as Conti, Stop, QNAPCrypt, Ryuk, and WannaCry.
- APT groups like APT1, Hafnium, and DEV-0401 have previously exploited 20 vulnerabilities.
- Ten of the vulnerabilities have associations with both ransomware and APT groups.

ICS-CERT: Sector Focus



The organizations within the purview of three sectors–health care and public health, energy, and critical manufacturing–are plagued by vulnerabilities posing the greatest risk.

Health care and public health systems are affected by the majority of vulnerabilities, with 47.4% of the total vulnerabilities associated with ransomware groups. Since the health care sector depends heavily on other sectors for the continuity of its operations and service delivery, several of the vulnerabilities are common across other critical infrastructure sectors. The energy sector and its three interrelated segments (oil, natural gas, and electricity) clock in with 31.6% of the vulnerabilities. The critical manufacturing sector and its four subsections–primary metals manufacturing; machinery manufacturing; electrical equipment, appliance, and component manufacturing; and transportation equipment manufacturing–carry 21.1% of ransomware-affected ICS vulnerabilities.

Of the total of 16 ransomware vulnerabilities affecting ICS products, there are six vulnerabilities that do not appear in CISA's list of KEVs. Our analysts lay special emphasis on these vulnerabilities because organizations may overlook them in their patch cadence.

CVE ID	Affected Sectors	Affected Products
CVE-2018-5391	Siemens RUGGEDCOM, SCALANCE, SIMATIC, and SINEMA	Chemical, Energy, Food and Agriculture, and Water and Wastewater Systems
CVE-2018-10115	Philips Vue PACS	Health Care and Public Health
CVE-2017-6034	Schneider Electric Modicon Modbus Protocol	Critical Manufacturing, Dams, Defense Industrial Base, Energy, Food and Agriculture, Government Facilities, Nuclear Reactors, Materials and Waste, Transportation Systems, and Water and Wastewater Systems
CVE-2017-6032	Schneider Electric Modicon Modbus Protocol	Critical Manufacturing, Dams, Defense Industrial Base, Energy, Food and Agriculture, Government Facilities, Nuclear Reactors, Materials and Waste, Transportation Systems, and Water and Wastewater Systems
CVE-2017-7494	Schneider Electric U.motion Builder	Commercial Facilities, Critical Manufacturing, and Energy
CVE-2020-10713	Hitachi Energy Transformer Asset Performance Management (APM) Edge	Energy

Health Care and Public Health

CSW covered the impact of ransomware on health care systems in extreme detail in its Ransomware Report Q1 2022.

Philips Healthcare, a subsidiary of Philips, is a technology-based company specializing in developing advanced visualization software and platforms for crucial imaging equipment used in various clinical diagnoses worldwide. Philips Healthcare is the worst affected vendor in the health care sector, with eight vulnerabilities, 90% of which are five years old. The products also have the highest associations of ransomware and threat groups. CVE-2017-0144 takes the lead with 17 ransomware family associations.

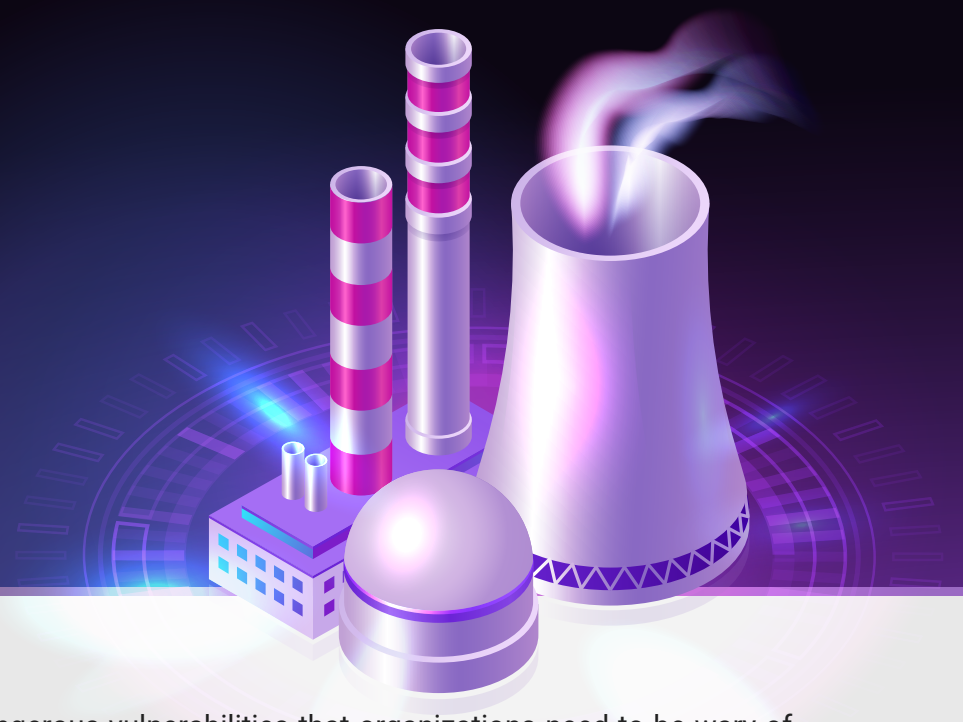
One such vulnerability, CVE-2017-0147, carries a CVSS score of a mere 5.9, but it has been at the helm of attacks and has 13 ransomware associations, emphasizing how supposedly low-scoring vulnerabilities may have a large attack footprint and overall impact.

The Philips Healthcare product in question—IntelliSpace Portal 9.0—is an advanced visualization platform most used for radiology diagnostics, apart from 70 other clinical applications in health care organizations worldwide. The product is primarily used for reading and follow-up on multifaceted cases; the critical ransomware vulnerabilities plaguing the product could have devastating impacts leading to hampered monitoring, inability to provide timely treatment, and even wrongful diagnosis or dosages of medication.

Impact: CISA's advisories to organizations in the health care sector come in the wake of continuing attacks by ransomware groups such as MountLocker, Quantum, Black Basta, and others. The impact of unpatched critical vulnerabilities could be potentially life-threatening.

Energy

Oil, Natural Gas, and Electricity



The energy sector is affected by six dangerous vulnerabilities that organizations need to be wary of. They need to adopt risk- and threat-based approaches for cyberspace management to ensure a robust attack surface.

A medium severity (CVE-2017-6032) and a critical severity vulnerability (CVE-2017-6034) affect Schneider Electric's Modicon Modbus Protocol, an Open Communications Standard utilized across critical infrastructure, which includes dams, defense, energy, food and agriculture, government facilities, transport systems, nuclear reactors, and wastewater and water systems.

With 50% of the vulnerabilities in the energy sector plaguing Schneider Electric, security teams may miss out on the importance of other equally dangerous vulnerabilities, such as CVE-2019-18935 that affects Hitachi ABB Power Grid systems and CVE-2020-10713 that affects Hitachi Energy Transformer Asset Performance Management (APM) Edge. The latter CVE, though exploited by ransomware, is yet to be added to the CISA KEV catalog, making it a vulnerability that may easily slip the eye of a seasoned security administrator.

Impact: An attack on an energy provider can result in a complete blackout or unstable energy supply. The effects of the attack could threaten health care and welfare organizations that depend on a stable power supply to maintain life-supporting equipment and hamper the functionality of all other critical sectors dependent on power, thereby having a cascading effect on the economy.

An old critical vulnerability in Baxter ExactaMix systems has the potential to compromise the critical automated pumping systems by allowing remote attackers to create denial-of-service conditions or execute arbitrary code, leading to grave industry-wide ramifications.

The recent attacks by the North Korean APT group, the Lazarus group, targeting the US energy sector, and ransomware groups like BlackCat and Ragnar Locker, highlight the importance of addressing the vulnerabilities plaguing this sector.

Critical Manufacturing

The critical manufacturing sector is subdivided into four core industries, namely, Primary Metals Manufacturing; Machinery Manufacturing; Electrical Equipment, Appliance, and Component Manufacturing; and Transportation Equipment Manufacturing.

With 25% of the vulnerabilities affecting critical manufacturing infrastructure (dams, defense industrial bases, food and agriculture, government facilities, and water and wastewater systems), it is crucial for governments and their entities to secure their systems from further attacks.

Impact: An attack on any organization in this sector could disrupt essential functions at the national level and have a supply-chain reaction across multiple industries and sectors.

Recent attacks on critical manufacturing, automation products, and network management systems have prompted CISA to release a security advisory for automation products and ICS vulnerabilities affecting other sectors.

ICS-CERT Analysis: Ransomware Products

Our experts have identified a list of top products across a wide range of sectors that are riddled with ransomware vulnerabilities.

Vendor	Products with Ransomware Vulnerabilities	Sector
Hitachi Energy	Hitachi Energy Transformer Asset Performance Management (APM) Edge	Energy
Schneider Electric	Schneider Electric U.motion Builder	Commercial Facilities, Critical Manufacturing, and Energy
Philips	Philips Vue PACS	Healthcare and Public Health
Hitachi ABB Power Grids	Hitachi ABB Power Grids eSOMS	Energy
Baxter	Baxter ExactaMix EM 2400 & EM 1200	Healthcare and Public Health
Hitachi ABB Power Grids	Hitachi ABB Power Grids eSOMS Telerik	Energy
Schneider Electric	Schneider Electric Modicon Modbus Protocol	Critical Manufacturing (Dams, Defense Industrial Bases, Energy, Food and Agriculture, Government Facilities, Nuclear Reactors, Materials and Waste, Transportation Systems, and Water and Wastewater Systems)
Siemens	Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA	Chemical, Energy, Food and Agriculture, Water and Wastewater Systems
Exacq Technologies, a subsidiary of Johnson Controls, Inc.	Exacq Enterprise Manage	Critical Manufacturing
Sensormatic Electronics, LLC, a subsidiary of Johnson Controls Inc	PowerManage	Critical Manufacturing
Spacelabs	Spacelabs Xhibit Telemetry Receiver	Healthcare and Public Health

Ransomware Vulnerabilities: A Breakdown

Here are some insights:

- Of the 16, 11 belong to the dangerous RCE/PE exploit category and can be exploited to escalate privileges or execute custom code remotely.
- Improper input validation is the most prevalent weakness powering ICS ransomware CVEs.
- Ten vulnerabilities are five years old.
- Six vulnerabilities are yet to feature on the CISA KEV list.

CSW's VRS versus CVSS

CSW considers the 'ransomware threat' context to assign higher scores to these vulnerabilities, ensuring they are given higher priority while deciding the patching cadence.

	NVD CVSS Severity	CSW VRS Severity
Critical	5	10
High	9	6
Medium	2	-

Takeaway: Be Aware of the Broader Impact of ICS Vulnerabilities

With specialized industrially aware scanners such as Claroty being the only viable option to scan for ICS vulnerabilities, organizations using regular scanners such as Qualys, Nessus, and Nexpose must make necessary changes to avert the prying eyes of threat actors looking for vulnerable endpoints.

With successful attacks on Colonial Pipeline (gas) and JBS (food), ransomware groups are now looking to wage attacks on sectors where they can cause the maximum disruption and damage and exploit the crises to demand the maximum ransom. The only option organizations have is to discover their exposures, identify the ones most critical to them, and remediate them before attackers can get a foothold. We encourage organizations to keep abreast of vendor advisories of the products they use and take necessary steps to thwart cyberattacks.

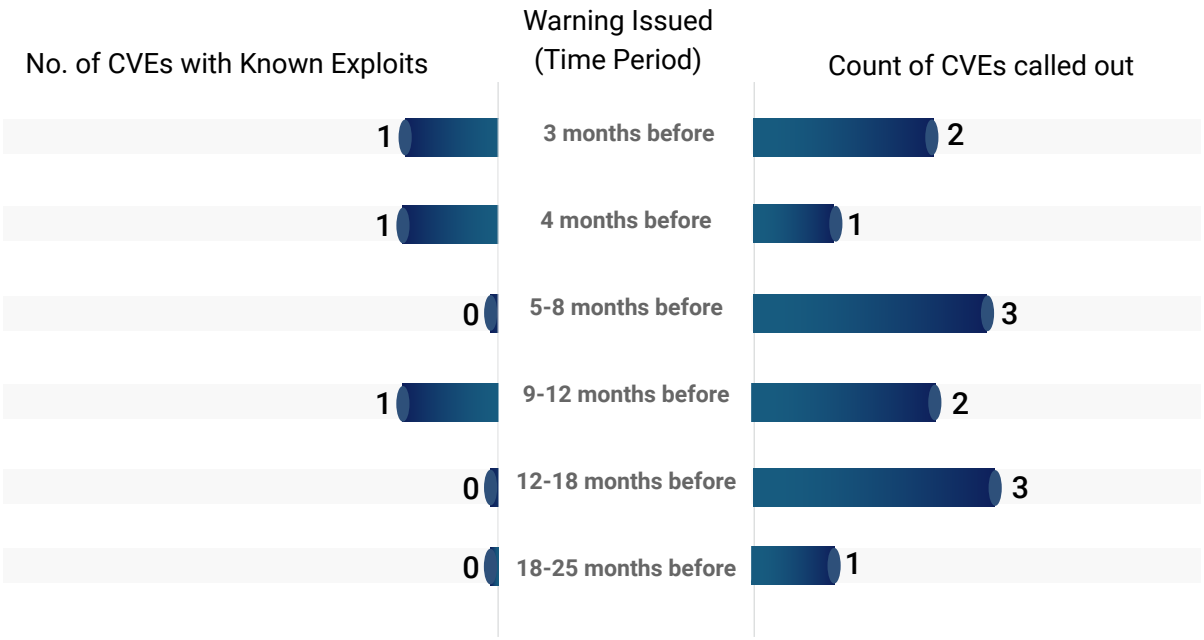
Predictive Insights

Insights on emerging threats based on trends, hackers' activity, and social media chatter, driven by Artificial Intelligence and Machine Learning (AI & ML)–based predictive analytics

Vulnerabilities with a high likelihood of exploitation

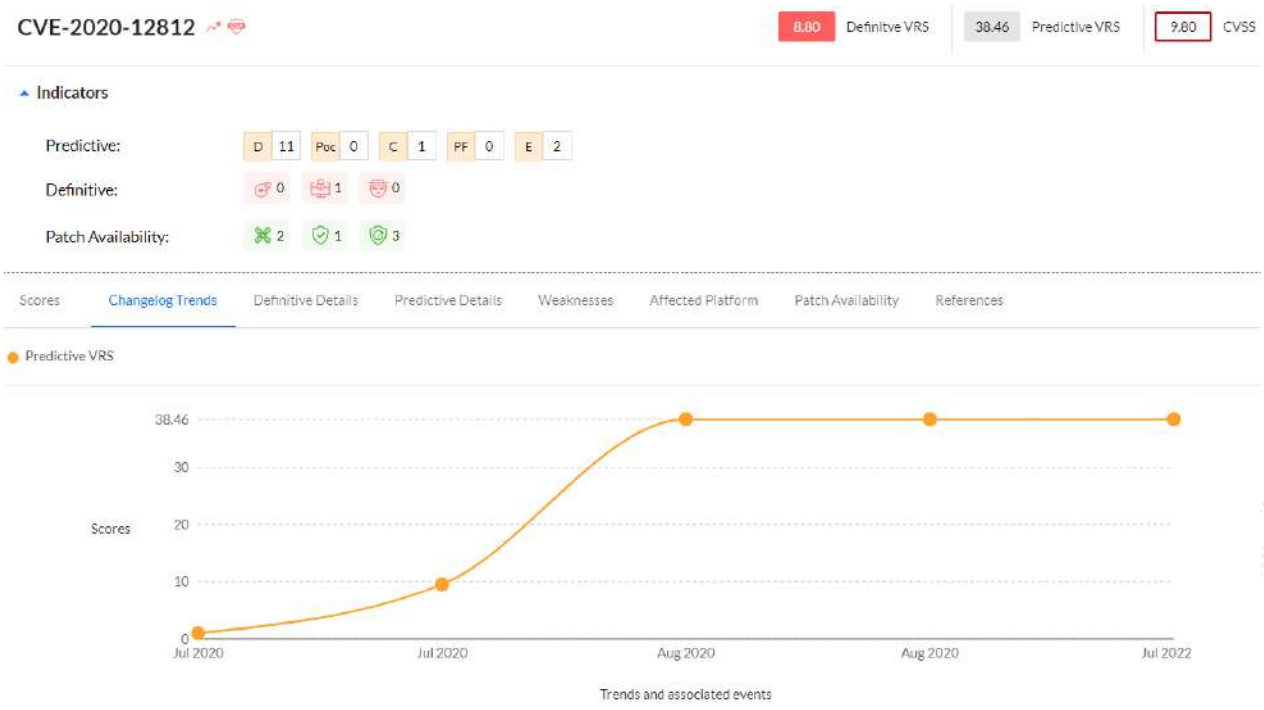
Our experts dive deep into the dark web to identify lurking threats that attackers are likely to exploit. Thus, we are able to warn our customers before threat actors can launch attacks.

All new ransomware vulnerabilities have the highest threat rating in our threat platform, except CVE-2020-36195 (a vulnerability in QNAP) that has a high rating.

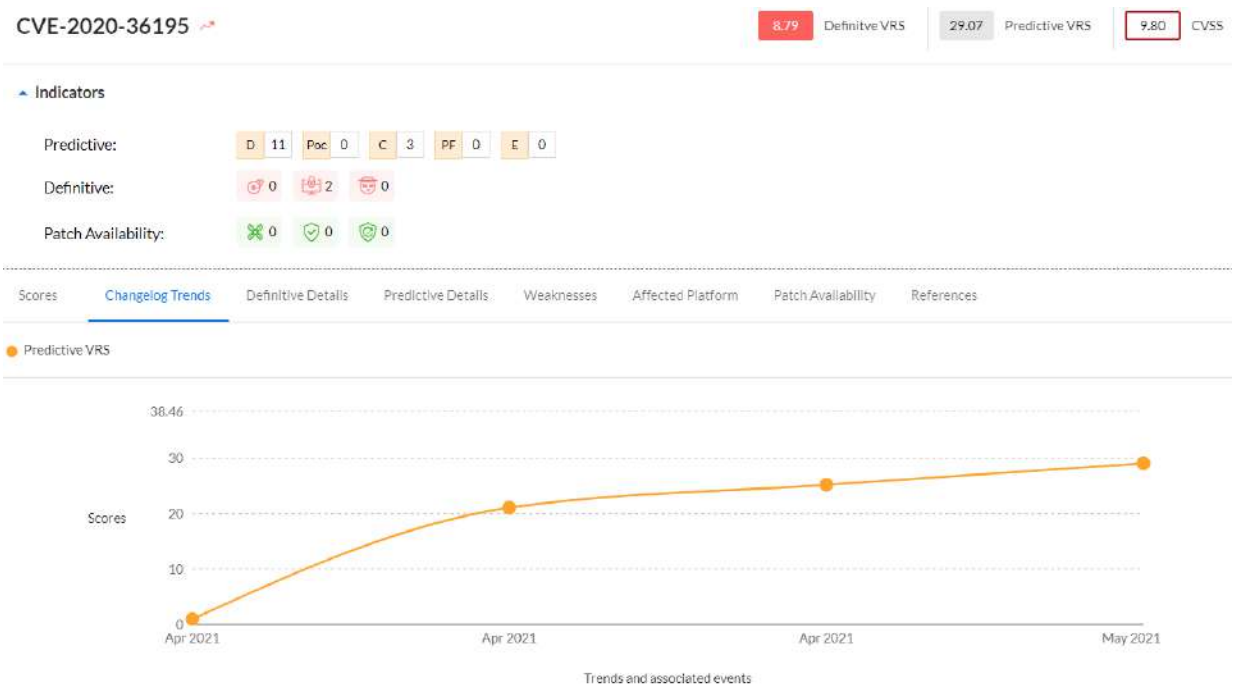


Securin VI's AI- and ML-based models predict that these new ransomware vulnerabilities have a high likelihood of being exploited by attackers. VI identifies evolving vulnerabilities by delving deep into their threat associations and the risks they pose and predicts the likelihood of an attack well in advance.

Securin VI dynamically tracks every vulnerability, with its predictive score reflecting current events and trends.



CVE-2020-12812 in Fortinet FortiOS started becoming a point of interest back in July 2020 when it was publicly disclosed by Fortinet. Our predictive VRS score slowly increased between July and August 2020 as malicious actors began to discuss extensively about the vulnerability. It reached a maximum in August 2020, and has remained so since, thanks to the multiple times CVE-2020-12812 was exploited by attackers.



CVE-2020-36195 exists in multiple QNAP products. This is an interesting vulnerability that does not feature in the CISA KEVs yet and cannot be detected by popular scanners like Nessus, Nexpose, and Qualys. The vulnerability's predictive VRS started increasing in April 2021 when massive campaigns were launched against QNAP devices. Subsequently, the score picked up momentum, reached a high value in May 2021, and continues to be a vulnerability to watch out for. Owing to exploitation by different threat actor groups, Securin's VI recently bumped up the vulnerability's definitive VRS to 8.79.

We have been ahead of the game in the past year, warning our customers about vulnerabilities way ahead of CISA. Our predictive threat intelligence platform (Securin's VI) has been able to warn customers of threats way before they were adopted by threat groups and ransomware operators." Aaron Sandeen, CEO & Co-founder of CSW

Our threat intelligence attributes the maximum ratings in our predictive VRS to 84% of ransomware vulnerabilities as they are highly sought out by ransomware operators to mount disruptive attacks.

Download the list of the top 10 ransomware vulnerabilities that have the highest possibility of being exploited in the wild.

Organizations need to adopt proactive mitigation measures to stay safe from impending and evolving threats. This demands a vulnerability prioritization approach that considers a vulnerability's realistic threat context in all its entirety. Always ensure a vulnerability's true risk is taken into account, considering its exploitability, threat associations, hacker trends, exploitation impact, and advisory warnings, while identifying evolving threats.

Anuj Goel, Co-founder and CEO of Cyware, says, "The ransomware landscape continues to witness the rise of new threat groups, along with the growing weaponization of vulnerabilities and cross-platform capabilities to infiltrate software code repositories and third-party solution providers that lead to downstream security risks. Even though post-incident recovery strategies have improved over time, the old adage of prevention being better than cure still rings true. To correctly analyze the threat context and effectively prioritize proactive mitigation actions, vulnerability intelligence for SecOps must be operationalized through resilient orchestration of security processes to ensure the integrity of vulnerable assets."

Popular threats to watch out for

Three vulnerabilities not associated with ransomware continued to dominate the threat scenario in Q2 and Q3 2022.

- Follina (CVE-2022-30190)
- VMWare (CVE-2022-22972)
- Sping4Shell (CVE-2022-22965)

We also observed multiple malware and botnets being deployed in the wild, being used to enter and invade unpatched devices. The most popular among them are Bumblebee, Rozena backdoor, and Raspberry Robin worm. Our threat analysts also warn about the QBot, SquirrelWaffle, and IcedID malware, which are primarily favored as loaders by ransomware groups.

We have observed increased threat chatter about the vulnerabilities in the **VMware ESXi** environment that attackers can exploit to compromise organizational networks. Hence, users of the **VMware ESXi** environment are advised to build up their defenses.

Future Predictions

What's next for ransomware? Having researched the threat world for decades now, CSW's researchers put forth the following predictions.

- **Source code reuse:** With prominent groups like Conti, DarkSide, and others supposedly shutting down, smaller ransomware groups are reusing their source code and building on top of it.
  E.g., Black Basta and BlackMatter
- **Shared attack methods:** Exploit methods adopted by now-defunct ransomware groups are being reused or modified and adopted by other ransomware gangs.
- **Newer, smaller gangs:** Several new and smaller ransomware groups have been identified; a few use similar tactics to those of defunct groups.
- **Sophisticated attacks:** Attackers are showcasing their expertise with advanced tactics such as encryption, exerting immense pressure on their victims with data leaks, and sometimes even deleting all their data. This trend is expected to continue.

Attack methods and patterns established by a group are here to stay, irrespective of the status of the gang that came up with the process, and are reused in other forms.

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

Conclusion

Ransomware is a pervasive threat that continues to grow in size, gathering more arsenal to target victims. Ransomware attackers have become more sophisticated as they mature in their methods to infiltrate and bring down organizations through exposures that exist in their attack surfaces. Despite concerted efforts from the FBI, CISA, and NSA and cybersecurity and vendor advisories, the number of ransomware victims is only increasing every year.

Through this report, we have adopted an attacker's viewpoint to explore attack methods used by ransomware families and threat groups. Our ransomware reports highlight the vulnerabilities exploited by these groups, in particular, with the sole intention of helping organizations identify ransomware exposures and understand why they need to be patched without delay.

One of the many things we were able to highlight in this report is how MITRE can be used to prevent attacks by researching trends and patterns and mapping these vulnerabilities to the ATT&CK kill chain. In our next annual report (scheduled to be released in January 2023), we will delve deeper into vulnerability chaining, MITRE analysis, and other related topics that would aid in understanding the ransomware threat.

Ransomware Data

Ransomware Data is proprietary information maintained by Cyber Security Works (CSW) and is used by our partner companies Securin, Ivanti, and Cyware to help customers gain resilience from ransomware threats.

Our customers use this data in myriad ways to stay safe from ransomware threats, and our experts continuously update this database with accurate information to provide them with timely information.

If you wish to access this database, drop a mail at info@cybersecurityworks.com or call us at 505-302-1113, and our experts will reach out.

Cyber Security Works

For more than a decade, CSW's vulnerability and exposure management solutions have helped clients across different geographies to secure their enterprises from emerging cyber threats. Our vulnerability and exposure management solutions have secured the IT infrastructure of diverse verticals in government entities, IT infrastructure, and private clients and have improved their security posture.
CSW is a US Department of Homeland Security–sponsored CVE Numbering Authority whose exploit research has led us to discover 54+ zero days in popular products such as Oracle, D-Link, WSO2, Thembay, and Zoho.

For more information, visit www.cybersecurityworks.com and follow us on LinkedIn and Twitter.

About Securin

Securin helps customers gain resilience against evolving threats. Powered by accurate vulnerability intelligence, human expertise, and automation, Securin's products and services have enabled organizations to make critical security decisions in managing their attack surface.

For more information, visit www.securin.io.

About 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.

About 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.

For more information, visit www.cyware.com and follow us on LinkedIn and Twitter

Appendix

Appendix A: Ransomware vulnerabilities missed by popular scanners

CVE	Vendor	Product	Ransomware Family Associations	Patch Links
CVE-2010-1592	SiSoftware	Sandra	Robinhood	Patch Now
CVE-2012-3347	EFS Technology	AutoFORM PDM Archive	Crypsam (SamSam)	1 , 2 , 3
CVE-2013-0322	2 vendors	2 products	32 groups	1 , 2
CVE-2013-2618	Network Weathermap	Network Weathermap	Ryuk	Patch Now
CVE-2013-3993	IBM	InfoSphere BigInsights	Locky and Petya	Patch Now
CVE-2015-2551	Information not available	Information not available	17 groups	Information not available
CVE-2015-7465	IBM	Jazz Reporting Service	Cerber	Patch Now
CVE-2017-15302	CPUID	CPU-Z	Robinhood	Patch Now

CVE	Vendor	Product	Ransomware Family Associations	Patch Links
CVE-2017-18362	ConnectWise	ManagedITSync	GandCrab	1 , 2 , 3
CVE-2017-3197	Gigabyte	4 products	UEFI	1 , 2 , 3 , 4
CVE-2017-3198	Gigabyte	4 products	UEFI	1 , 2 , 3
CVE-2017-6884	Zyxel	2 products	Ryuk	Information not available
CVE-2019-16057	D-Link	2 products	Cr1ptT0r	Patch Now
CVE-2019-16647	2 vendors	2 products	Bitpaymer	Patch Now
CVE-2019-16920	D-Link	8 products	Cyborg	EOL
CVE-2019-5039	OpenWeave	OpenWeave Core	ASN1	Patch Now
CVE-2019-9081	Laravel	Framework	Mailto and Satan	Patch Now
CVE-2020-36195	QNAP	3 products	QNAPCrypt and Qlocker	Patch Now

Appendix B: Top 10 ransomware vulnerabilities with a high rating on our threat intelligence platform

Vulnerability	Vendor	Product
CVE-2021-44228	22 vendors	175 products
CVE-2022-26134	Atlassian	3 products
CVE-2021-31207	Microsoft	Exchange Server
CVE-2021-34473	Microsoft	Exchange Server
CVE-2021-34523	Microsoft	Exchange Server
CVE-2020-5902	F5	16 products
CVE-2018-8174	Microsoft	10 products
CVE-2018-13379	Fortinet	FortiOS
CVE-2017-0199	Microsoft	13 products
CVE-2017-11882	Microsoft	Office

Appendix C: Indicators of compromise of newly identified ransomware families

Maui Ransomware

MD5 Hash

a452a5f693036320b580d28ee55ae2a3

c50b839f2fc3ce5a385b9ae1c05def3a

9b0e7c460a80f740d455a7521f0eada1

2d02f5499d35a8dffb4c8bc0b7fec5c2

fda3a19afa85912f6dc8452675245d6b

802e7d6e80d7a60e17f9ffbd62fcbbeb

a6e1efd70a077be032f052bb75544358

4118d9adce7350c3eedeb056a3335346

SHA-256 Hash

99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f

830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570

56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19

3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878

45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78

5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e

87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6

458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456

DeadBolt ransomware

MD5 Hash

fb2e2de57fb405512f539a1c302e2b4f

5da2297bad6924526e48e00dbfc3c27a

718ae69788dc752a8db46b0e43e42f13

cfe7e21b24b50aa442d4ca4a92cd6d6c

a76ecd6356f7a71e524c74abf2adec09

SHA-1 Hash

22e616aa3c3a512499968ffecd7d123fec6f5e96

1fcd0db29725c731681325985ff06cb90347f0cc

338c16a49899ee08b5284b9bb3b2b14d6e5bdfe3

SHA-256 Hash

444e537f86cbeeea5a4fcf94c485cc9d286de0ccd91718362cecf415bf362bcf

3058863a5a169054933f49d8fe890aa80e134f0febc912f80fc0f94578ae1bcb

4f0063bbe2e6ac096cb694a986f4369156596f0d0f63cbb5127e540feca33f68

80986541450b55c0352beb13b760bbd7f561886379096cf0ad09381c9e09fe5c

e16dc8f02d6106c012f8fef2df8674907556427d43caf5b8531e750cf3aeed77

acb3522feccc666e620a642cadd4657fdb4e9f0f8f32462933e6c447376c2178

14a13534d21d9f85a21763b0e0e86657ed69b230a47e15efc76c8a19631a8d04

2dab7013f332b465b23e912d90d84c166aefbf60689242166e399d7add1c0189

e0580f6642e93f9c476e7324d17d2f99a6989e62e67ae140f7c294056c55ad27

3c4af1963fc96856a77dbaba94e6fd5e13c938e2de3e97bdd76e1fca6a7ccb24

81f8d58931c4ecf7f0d1b02ed3f9ad0a57a0c88fb959c3c18c147b209d352ff1

653a90f92c2070b794c4d738188f172f718ae69788dc752a8db46b0e43e42f13

1ac1f9f9c519c7e141dcb1aa8157feca7943fd85db3d0a31f01e0fb44d239890

0a07c056fec72668d3f05863f103987cc1aaec92e72148bf16db6cfd58308617

184747ba1f080561ceea7f0b96dd0a8c1de2b7b2bdc2fea39954949d29aeaca9

3e30a65e6504969c05b1bed32db2a2a592da110a7d2dbda9f064f13be5390d6c

59e7573339f23c21b934fba44f04d694f67cce4f9e90982db4b6ddb3078b058c

SHA-512 Hash

81f8d58931c4ecf7f0d1b02ed3f9ad0a57a0c88fb959c3c18c147b209d352ff1444e537f86cbeeea5a4fcf

94c485cc9d286de0ccd91718362cecf415bf362bcf

Black Basta

MD5 Hash

eff424376edca5680b90ea9fedad163d

SHA-1 Hash

3c13c1e54d2d7991c1c3452ae89888a8e7a47763

SHA-256 Hash

2e890fd02c3e0d85d69c698853494c1bab381c38d5272baa2a3c2bc0387684c1

2d906ed670b24ebc3f6c54e7be5a32096058388886737b1541d793ff5d134ccb

1e7174f3d815c12562c5c1978af6abbf2d81df16a8724d2a1cf596065f3f15a2

130af6a91aa9ecbf70456a0bee87f947bf4ddc2d2775459e3feac563007e1aed

df35b45ed34eaca32cda6089acbfe638d2d1a3593d74019b6717afed90dbd5f8

2083e4c80ade0ac39365365d55b243dbac2a1b5c3a700aad383c110db073f2d9

c4683097a2615252eeddab06c54872efb14c2ee2da8997b1c73844e582081a79

8882186bace198be59147bcabae6643d2a7a490ad08298a4428a8e64e24907ad

0e2b951ae07183c44416ff6fa8d7b8924348701efa75dd3cb14c708537471d27

c9df12fbfcae3ac0894c1234e376945bc8268acdc20de72c8dd16bf1fab6bb70

01fafd51bb42f032b08b1c30130b963843fea0493500e871d6a6a87e555c7bac

433e572e880c40c7b73f9b4befbe81a5dca1185ba2b2c58b59a5a10a501d4236

72a48f8592d89eb53a18821a54fd791298fcc0b3fc6bf9397fd71498527e7c0e

f132ffc8648d38833244e612c58224285e85e863a35c872490690217c082e59c

c4fa34414fb1c199e13d7cd7def0e8f401c9649657a39224bc32310c9fd9d725

5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

5b6c3d277711d9f847be59b16fd08390fc07d3b27c7c6804e2170f456e9f1173

daa049b15bb5c1d0aef06276f9940d2fea76242f1a01ebfe299a63b7c74f7ea0

a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1

17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90

3eb22320da23748f76f2ce56f6f627e4255bc81d09ffb3a011ab067924d8013b

1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250

0d6c3de5aebbbe85939d7588150edf7b7bdc712fceb6a83d79e65b6f79bfc2ef

96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be

19c2710e498d55f2e3a3d4126064e960058e32c99dc35944b3fc09aa0eec4754

c5fcd0643823082941bc827613baf0fa574ffd9cb03a8b265d62d657367b2ea2

ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e

7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a

c532d28f9700abba1a4803c3a9d886c8c4fb26f84cf2399c533d68cfdcec4fa7

48976d7bf38cca4e952507e9ab27e3874ca01092eed53d0fde89c5966e9533bb

Hive Ransomware

SHA-256 Hash

47dbb2594cd5eb7015ef08b7fb803cd5adc1a1fbe4849dc847c0940f1ccace35

400743b945a4341559734ca144be4a96d325b9cb76169a5c43e82b21d3c59278

c1ed5916533b122bdbcb20e4a14473639f691b69f9adfc310e2d6589f3da15a7

ff3198e720eb5f3ed07c23cac434698d63e2a08647864a9d539ecb6af7aa3ffa

e1a7ddbf735d5c1cb9097d7614840c00e5c4d5107fa687c0ab2a2ec8948ef84e

12389b8af28307fd09fe080fd89802b4e616ed4c961f464f95fdb4b3f0aaf185

be1565961e123f52e54e350e0ca2666f8ffa42fdc46df18dca6f7c0ac2b43d23

25793a0764a51b38806b7dcf5f5d8df9620f090f72362aa03187c8813e054482

8a461e66ae8a53ffe98d1e2e1dc52d015c11d67bd9ed09eb4be2124efd73ccd5

2f573f7ed5d3ffc47aa0d095d3861030372074b214e2607021236c744cde6614

61fd23a73f975b2527812d14fd32ae0b929f42be3335f06401b5d324090ec9b9

56c72444a610c757a3ff81d991681a51c42e5e839dbaeaf15887f075cde83747

de03a9fcf26d9f446a362de7302e151eb3f4a90544f034a054684cc317c44742

f172f51cdb08fc31d4cc213aba90a2581f0954f4fc99a3515feead06c3257ca2

1670e8bb8065d23e1b93ed8173f079f338abef880047da21af95dd4db57e20bd

bf7bc94506eb72daec1d310ba038d9c3b115f145594fd271b80fbe911a8f3964

ea6ee7a35e964b84c59eba34384ea9dd6aa1e951a2d9424f5991b364a7d685bf

50ad0e6e9dc72d10579c20bb436f09eeaa7bfdbcb5747a2590af667823e85609

fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf

12baa6c83e6f8b059e7f14cb67bdad4e917b90bc8a139b5379a4b42a0c92a6be

104dd21cc4403680d3f2d4372c2c49cd78eee66683d89d432e8b43fad2568f85

191fd802cb6f922684cd32f51ea33b6106507c75b5baedd27a61b13cfee8a14b

9868fd95b89af8a070c45e2533bd9626d9b36f5f10419086bba5f6b337dd79a8

c29bf72d010c32acd23ca20e473dadfbe28db7d7e68971ac94cbe9d35dd3853d

612e5ffd09ca30ca9488d802594efb5d41c360f7a439df4ae09b14bce45575ec

5ae51e30817c0d08d03f120539aedc31d094b080eb70c0691bbfbaa4ec265ef3

5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968

f771389e1e67994756c3dc36278c52996b8798455fbcbb949faff3463a77dc16

97a6a4124b7a76845d65780bd44aa323532c783f008ae11a6c17bb5f7832a13a

77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618

5954558d43884da2c7902ddf89c0cf7cd5bf162d6feefe5ce7d15b16767a27e5

df7003b2f8d330b16cea1b682edddd1d85e56806a276f432e5f09091b4877a7d

7fb0391651fff5ea815395dd278986dc23af9e91036ce178dd25951758ea94c6

25f621faa29e7814e8c6d75d3e7fc3f65877d81b5dafb397526b26dcd8d3594d

bdf3d5f4f1b7c90dfc526340e917da9e188f04238e772049b2a97b4f88f711e3

6983ef6e484c0c70356d6f868ac03bc90a1055560642706743511f76aa6f28ad

3858e95bcf18c692f8321e3f8380c39684edb90bb622f37911144950602cea21

448e8d71e335cabf5c4e9e8d2d31e6b52f620dbf408d8cc9a6232a81c051441b

514cd2d5751d3bbb5a7bbf0b5733edaf3ac755b1dceb5b1e7a4155de87058983

2a6befff9aba5700d5719a998996a5aa5fe67c7ca6c763cf498a10bac099a511

7718a4f685d17423d7b8736fb1762fcbca92d2a0918fdd29b4118ac920aef517

98598eeb0a57f8c2d50a8009f060249fc45b00f564c9411e5255084e59168f73

a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749

b0508de411dec856dbf88c5f2dc4255c656a8388f00debc3eaa5d952d66ef3b7

50b2b256e60cb0fc50976b4216a28b3de8e736e2035d7c3cd59a5822c8770d2e

27cb6c7baa77bd84c21e29c75365c6990c69d0d9134e0f9272f3444aacba4488

6a0449a0b92dc1b17da219492487de824e86a25284f21e6e3af056fe3f4c4ec0

acecf1f8fc1bde7b57412e3ceb610035ef6f82bb350c22fb9e780dfa7e46e329

cba0c8e316db8c6abcdb69f03936a803d81299d9ae4c59c77839c37cda752539

d64f9742539436acba5ff9c4f1c8ca501cad86dfa823828b65418b493c8109ac

a4e6aac8e9a84886f84059e4b56ab1cfccd740690cdfb1d6860cbac02f034b21

88f7544a29a2ceb175a135d9fa221cbfd3e8c71f32dd6b09399717f85ea9afd1

1357e734118202f3277c6e9976f08d53c17d0b083992028117643eb2d465a50b

222d210e12e2fe32545af6eadfdbf0eb0638a6d132e5c9821daa04bb5b197b5a

713b699c04f21000fca981e698e1046d4595f423bd5741d712fd7e0bc358c771

c90ea27b7ea59563bb221dc694dd9cbb37994b656f9509d28413c454d0046460

f4a387624049baa6f7400ef71282ce244499be904651ee70ef145c07bee8e151

d7fe04c042782df6be1fb3e38f171631820e43b9472da93af7e5f49b550a2a33

1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff

36fe56519a798213116d5f7328fa81ef7c550f4f14c36e7f30c330bdd6d7d42e

44f8c6a7e5c8af0782cc39e1f6fc51e817ab990649da1d097f948b76d3fde442

bd9807c6e5c69f21153103703faa8067a9a883124bcfeb6b0f0645158a97d57d

9335341e54698e2a33355c0594d622828c1634557b69453b5d856211c4aa461b

98a48551e429fadc550cf8454f09c01e233aebf176bd141db57305e0ba2d0d28

8af39d53b7b9e57995003b9c22dbcad3823dd739ad8586011be57be9b9adfeb6

1ad94ad45b3c0097b9d4a69f6331c5f4f8113e8b5f5d4bcd103c690e66ca7f12

23f9744316621d583cc811663b620df5d92c3de4554a82a863c9c974c38ccaf1

ed55da207686f136205db1226c23add2bba331794de6f2c0b0861681cf344226

00dc667e31c607838c8fe69494eaa45bcaba1b737973d3842643c22477eab1f1

16d0c9651cae4ca2641f9e875be9f7b39737292eede7a7870b6081922f40b4b1

e9def82da36450f16c48af3abbba2a31f53c9c2f6fae6cf895fbf10698c04ed2

cafdc2624a909f037caeb2fb1fb89072d91ac3f2ba0b90dcfa873e01a6934c9c

cc575842398e2fec84efb9de29b230280120709aead807edc807a62072f6194d

f99eace78d92e533bf03347824fc3a16adb33b6a88f4fb3675083496a9757fa1

28518da0336e8e2e48f598dc23d6312e8567f1d088d3b20993f643a8f0e1c6ad

f7ac5830a672c6a4722050919384daaa985870d59bbbd757197de5207099cef5

b1bfc90de9dcea999dedf285c3d3d7e1901847d84ec297224a0d82720d0ed501

d5adeef0250358c54e74b012f4f7ad9f7765b2919747116870e54ff3b6340442

7cb5b1edd62718c8e42d2b56ddfc8a1152da8b3907eedc85f49d43d0ce8b44b2

c04509c1b80c129a7486119436c9ada5b0505358e97c1508b2cfb5c2a177ed11

34215cad33becc30bf2c994c2b50fd3938d6e91fdeb9dc189eb97cd036f2a223

72999cded357edf7dd8aed41942a1ea33e96004b8ab0bbc39adf86690405d16f

ec9ef903c4d23e4f10117a2c24d87d6d4bc47dc056db0d0b9178bf4e4ed30cef

a2ad0442cebe3e6abb86069a3b66b471b4a7c9d00286da4b8114d17a849128d6

dd1e4842111c38d0d24deecd6aeb830d9d90bce19df0ffd839d5cfc7a565c0ae

ff93136112316cea3f80218c5354d6e8c12cdfe449c40ab417002fe81dcf1dcb

0daac12ef83d0c5d893bb0a56ef90bf4e1c4e9938d33502b9780d67c9ad7dfad

dd1c58c48d46cce9ef92a730687f87d97bdb9d9bad51034177543e3833fa7ccb

db23ad5a44f67332cbc3d504260ec4742acb9f26373c4ef13f2ab0095a72bf6e

4fe989185c5c4c308046262f8c480d6d45224ec7e24261563c0f164b4d5f379b

da2128b5608ed39f1a4e4568e0751bd9f8cb4e8587f1a262314d13c03a6a8b9e

d0ceb8f5170972fe737ab9cbdd6f3ee472fbe62e244cccc46d137094d33f1afc

2f7d37c22e6199d1496f307c676223dda999c136ece4f2748975169b4a48afe5

aa4ffa5e1711e83d0fca382106ace09df4c55c602b8661e72f32ef5ee80c527c

20a2250d93226c25246b32f6dabbe7a876c60843e487c8e7aed76dd0aba23042

f682a4a38f7eba04b3d87a4b31d8a745f3aa6d04201ab9c3315e6c09fdc75229

44a69c3d760c8cc90e205564c9a351620a24facb504a24cffb2742061d873654

fb91cffedd7d555ca0660b992a43367817ed6bb2d202e1e9218346114d0d9bc3

25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5

d57f99908a8b4e50a1ace66ed0d84792d2765bed945247160b5d8c874fca492f

5bc8f4aa3eadc95f7235a10f6d3b257d4b3c3c6e3c0418326fd4c8f2da33d984

5edbbfd33d034b1a877cde0d2d20d3937aad7f1b6ff922168bab7bda8d6ff494

5b32ac4754bd5728cc7a68f341bf64cec4a737eb584814bb2099a5f2ff69e584

693e43e6524610a91f66f692325ff3aead9c426d587c2dcfda7c9c15773f1895

a4878bb4655f21dd34b5a8a853ebea6b9cca292190c6ca180b4afe44077002ab

ad1bcde48e755669187c9e170443d95585cb26db1f619c7f9dc57d32974471c1

a1621732042fc5b3a10ee9d31f5d92834a80668deae52c0aa5c18ea8d4c72d43

46d100b79524a1b3dfa9a98625acc0329b4b948859a397af94a97c394c7d9f74

f56b69b2ed6fb623f9e112eb9ae52a057cba260b85ef9bb789b5e4f8f7faadfd

8fb3e954a8d73eb29a7ee8a17d405b8fca0235c9e0a919e3dd0214933d89a98b

67ab2abe18b060275763e1d0c73d27c1e61b69097232ed9d048d41760a4533ef

4a7df7a500d498342804749f3a8e7c3e8711a1fcc3d8a785579d2b23d2c21686

c3732c95df41b283317330db117210bf55262d3a8f4ad2d3d2ee40626641d960

1a798bdc62d9ec900a67c72b57cd8eed2b6b6b78367e93abb08cf91f72e36f0d

6920e86a65fc94f9fd46c46c09187b802a13801904e06c6aa63c10e0c9197218

13903ef99700ab30e6f13d3579d99acaac3a9730b01720092c4e85f13152588b

bc04af5bfcd57465d938e33e13974a299062e4732298dc687baa27270a5ba60f

83f4174bf4f0bd2c6d411cf81293ccb62ce69345246938bf28a77f143ac4af40

822d89e7917d41a90f5f65bee75cad31fe13995e43f47ea9ea536862884efc25

122e397dc3a55143bd276d6ff3bc04a05601fbf390aa52a19274456ca0040a28

62d52ee299eafe3b05df8dc5110f39886073c1848aa9db02ff1bf1123f6fdfbe

30414f35f5ae50c9133017c6100b6f82dca0ca872ac6fbcf159b7b1d2303664f

3e58bda58148a39c6603954bd10e361504fd6383feef5d5f7f16cc082b78fa43

de5867fbc85c4f2cd210f60d565c99ab039f0be41c0ec6c7729d795d0ff15ecf

638cc41ca18feccf21b7ed1b71fe0b0881b592647fd286276dff6a4e48992bfa

30cdf54a171a4f4f0ce0c69b6934468bab228f5dd9f9b2a39a6b5e968f3c6565

5a991404956e8c12450424bfc0fe49600c3b7988ac0766df044f56dd93720155

efccbae3957f57bf31954261d1b13d7e985378e1ff0038cfcc2802b5a94cfa4d

e6a7d1575ad6be033d4caada4341835175e85f859d304d292ae3968dd97d682d

cac027eed3a92cd1b24745fa0b182bdc76839edf276a672ab66c311ae61de3fe

0e8e6fc94e6eb17cfd8993b3dcfd9acd11ee32f1b4e956df3097ae3259be4f9c

d5837ce670bcdf565e7648f0d43bad6232292163c3a123bfa108ee319e7df373

321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c

56c5403e2afe4df8e7f98fd89b0099d0e2f869386759f571de9a807538bad027

60cfce921a457063569553d9d43c2618f0b1a9ab364deb7e2408a325e3af2f6f

6a222453b7b3725dcf5a98e746f809e02af3a1bd42215b8a0d606c7ce34b6b2b

130c062e45d3c35ae801eb1140cbf765f350ea91f3d884b8a77ca0059d2a3c54

efbdb34f208faeaebf62ef11c026ff877fda4ab8ab31e99b29ff877beb4d4d2b

e61ecd6f2f8c4ba8c6f135505005cc867e1eea7478a1cbb1b2daf22de25f36ce

d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae3009a619e2691

e514be3e997895c7e3ece03549c8cb6b5700fe8f814948ed201ca59daa8733fb

5086cc3e871cf99066421010add9d59d321d76ca5a406860497faedbb4453c28

e452371750be3b7c88804ea5320bd6a2ac0a7d2c424b53a39a2da3169e2069e9

8f3c5f9cd657e3785d751305023cf83a7f27780d5441817614d442e28dbe3ac4

7e8dd90b84b06fabd9e5290af04c4432da86e631ab6678a8726361fb45bece58

6bdd253f408a09225dee60cc1d92498dac026793fdf2c5c332163c68d0b44efd

bd6d8f7c9e016dd7395ee7f0f8485de622a9b034b7c5d2e1af25cb762dd8d8c9

065de95947fac84003fd1fb9a74123238fdbe37d81ff4bd2bff6e9594aad6d8b

7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3

3ec89b737c5b91eb9da0a2d9c6c1f0e637087b4552e26806d959c11f8f06e96f

a586efbe8c627f9bb618341e5a1e1cb119a6feb7768be076d056abb21cc3db66

c76671a06fd6dd386af102cf2563386060f870aa8730df0b51b72e79650e5071

c367ab50c1f103963da0f0404eeda46c9e768711797d638afa1c4cf740575613

47006ed84afb1f1fd761b81f3ae7b6547c0cb4845538301035e1388693fc6f7f

6240193f7c84723278b9b5e682b0928d4faf22d222a7aa84556c8ee692b954b0

f07a3c6d9ec3aeae5d51638a1067dda23642f702a7ba86fc3df23f0397047f69

c384021f8a68462348d89f3f7251e3483a58343577e15907b5146cbd4fa4bd53

75244059f912d6d35ddda061a704ef3274aaa7fae41fdea2efc149eba2b742b3

12d2d3242dab3deca29e5b31e8a8998f2a62cea29592e3d2ab952fcc61b02088

a290ce75c6c6b37af077b72dc9c2c347a2eede4fafa6551387fa8469539409c7

baa7a6e5a093ee6be47eca86e5acbcba196c7d1d35662eecad23ec870702116a

f248488eedafbeeb91a6cfcc11f022d8c476bd53083ac26180ec5833e719b844

e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173

7667d0e90b583da8c2964ba6ca2d3f44dd46b75a434dc2b467249cd16bf439a0

9cd407ea116da2cda99f7f081c9d39de0252ecd8426e6a4c41481d9113aa523e

```
ed614cba30f26f90815c28e189340843fab0fe7ebe71bb9b4a3cb7c78ff8e3d2
e9da9b5e8ebf0b5d2ea74480e2cdbd591d82cd0bdccbdbe953a57bb5612379b0
fd3e7d0f6a31b821604707ef99da281e4fd7d11c7804e46eeed11f66b200a391
9c90c72367526c798815a9b8d58520704dc5e9052c41d30992a3eb13b6c3dd94
e9bb47f5587b68cd725ab4482ad7538e1a046dd41409661b60acc3e3f177e8c4
977b2ce598bd6518913fe216d1139c041e159a6510cd71a6a14a49570c1019be
39629dc6dc52135cad1d9d6e70e257aa0e55bd0d12da01338306fbef9a738e6b
0809e0be008cb54964e4e7bda42a845a4c618868a1e09cb0250210125c453e65
6bd3adc7e43e20ede1a82ad1469cc7ecd085b324621edbd4ec23db4e4473895f
875708f911752bef7e2ef0658d395ebeccef774d5fdb74f6e9ee60b52d86cbf0
2e29fe2ef4ed4917474ce22212fd3b1a756bd9aef176a0a6f55a3590d7c5e612
```

SHA-1 Hash

```
2aee699780f06857bb0fb9c0f73e33d1ac87a385
6e91cea0ec671cde7316df3d39ba6ea6464e60d9
27b5d056a789bcc85788dc2e0cc338ff82c57133
3477a173e2c1005a81d042802ab0f22cc12a4d55
24c862dc2f67383719460f692722ac91a4ed5a3b
d1ef9f484f10d12345c41d6b9fca8ee0efa29b60
d83df37d263fc9201aa4d98ace9ab57efbb90922
fa8795e9a9eb5040842f616119c5ab3153ad71c8
```

6b5036bd273d9bd4353905107755416e7a37c441

655979d56e874fbe7561bb1b6e512316c25cbb19

415dc50927f9cb3dcd9256aef91152bf43b59072

49fa346b81f5470e730219e9ed8ec9db8dd3a7fa

ecf794599c5a813f31f0468aecd5662c5029b5c4

763499b37aacd317e7d2f512872f9ed719aacae1

8a4408e4d78851bd6ee8d0249768c4d75c5c5f48

2ded066d20c6d64bdaf4919d42a9ac27a8e6f174

2146f04728fe93c393a74331b76799ea8fe0269f

SHA-512 Hash

fa181087df0176eb9b39d70d75d2b9d3e75a075266cc6689599217b410a79ed8583ce06f5812bbb8

3e7388b58e7498f5f2d50918efd1be9dfae1c6e049e797d8

MD5 Hash

BEE9BA70F36FF250B31A6FDF7FA8AFEB

04FB3AE7F05C8BC333125972BA907398

b5045d802394f4560280a7404af69263

d46104947d8478030e8bcfcc74f2aef7

4fdabe571b66ceec3448939bfb3ffcd1

6a58b52b184715583cda792b56a0a1ed

5e1575c221f8826ce55ac2696cf1cf0b

bb7c575e798ff5243b5014777253635d

2401f681b4722965f82a3d8199a134ed

6c9ad4e67032301a61a9897377d9cff8

6ed4f5f04d62b18d96b26d6db7c18840