SPOTLIGHT

CSW Cyber SecurityWorks | Securin | CYWARE™ | ivanti

Ransomware

Through the Lens of Threat and Vulnerability Management

Index Update Q1 2022

2022

Table of Contents

Introduction

The Ransomware Index Update Q1 2022 documents our continued investigation of ransomware groups and their weaponry of choice. In this index update, we highlight key index numbers that have changed since we published the Ransomware Spotlight Report 2022 in January 2022.

In this report, we provide a look into the current ransomware ecosystem, along with our insights and early warning predictions of highly targeted attack vectors. Our goal in publishing this Ransomware Index Update is to help organizations understand the true risk posed by rapidly evolving ransomware groups, and provide actionable learnings that organizations can use to strengthen their security posture and chart a strong defensive roadmap to counter these threats.

Top Five Findings

- 22 new vulnerabilities and 9 new weaknesses have been associated with ransomware since January 2022.
- 141 of CISA's Known Exploited Vulnerabilities (KEVs) are being used by ransomware operators including 18 newly identified this quarter.
- 11 vulnerabilities tied to ransomware are undetected by popular scanners.
- 3 new APT groups (Exotic Lily, APT 35, DEV-0401) and 4 new ransomware families (AvosLocker, Karma, BlackCat, Night Sky) are deploying ransomware to attack their targets.
- Data gaps in CWE, CAPEC, and MITRE about vulnerabilities are handicapping security researchers while enabling attackers to stealthily enter unsuspecting organizational networks.

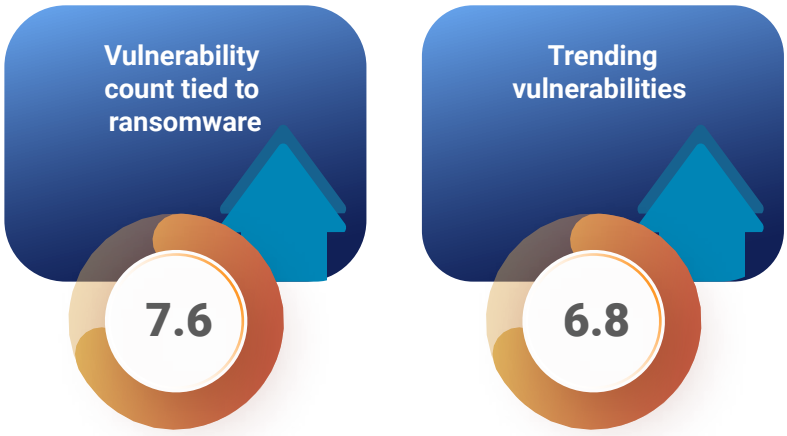
Executive Summary

Our report is based on in-depth research of ransomware incidents and the vulnerabilities targeted by ransomware groups. Our predictive ransomware-based trends and observations listed below are based on ransomware data derived from multiple threat intelligence feeds and risk analyses.

Increase in Ransomware Vulnerabilities

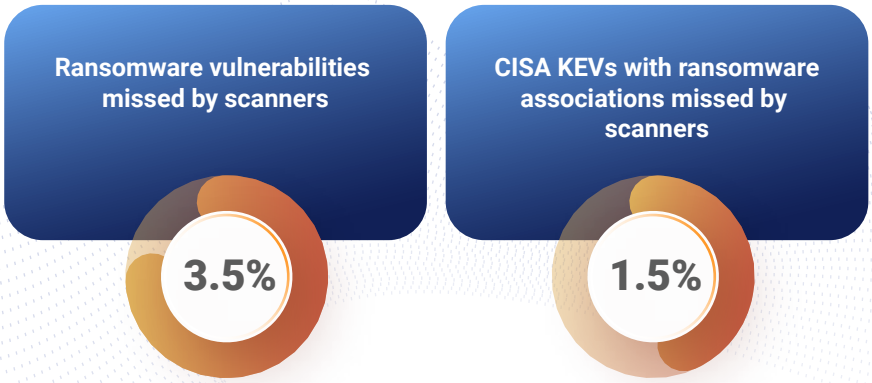
Ransomware operators have become relentless and are weaponizing vulnerabilities faster than ever to achieve their goals. Since we published the year-end ransomware report, our analysis shows a strong 7.6% increase in the number of vulnerabilities tied to ransomware in Q1 2022, with Conti dominating the list.

The new vulnerabilities include three of critical severity, and 18 of high severity, by CVSS V3 standard. The number of trending vulnerabilities also climbed 6.8% as ransomware operators continue to go after weaknesses that would create the maximum disruption and impact on their targets.



Scanners Not Detecting Ransomware Vulnerabilities

Some of the most popular scanners are not detecting several key ransomware vulnerabilities. Our research shows that over 3.5% of ransomware vulnerabilities are being missed, exposing organizations to grave risks. Our ongoing research on CISA's Known Exploited Vulnerabilities (KEVs) also revealed that scanners are missing 1.5% of vulnerabilities tied to ransomware. Besides, there is also an added risk of zero-day vulnerabilities being targeted, and a novel approach is needed to detect the same.



On a positive note, we see that the overall ransomware vulnerabilities missed by scanners has decreased from 22 (Q4 2021) to 11 (Q1 2022). This is a development in the right direction, and we hope that all scanner solutions step up in this fight against ransomware, also reducing latencies in releasing their scanner plugins.

"The fact that scanners are not detecting critical ransomware vulnerabilities is a huge problem for organizations. CSW experts are continuously tracking this as a part of our research and analysis. The good news is that in this quarter, we saw the number coming down. This means that scanner companies are taking this seriously. That said, there are still 11 ransomware vulnerabilities that the scanners are not detecting where five are rated critical and associated with notorious ransomware gangs like Ryuk, Petya, and Locky." **— Aaron Sandeen, CEO & Co-Founder CSW**

To view the list of ransomware vulnerabilities missed by scanners, please check the Appendix A.

Rapid Weaponization of Vulnerabilities

A distinct pattern that we have been noticing since 2021 is the rapidly increasing speed of vulnerabilities being weaponized.

The increased sophistication of ransomware groups has resulted in vulnerabilities being exploited within eight days of being released by their vendors.

A minor laxity in security measures by third-party vendors and organizations using their products is sufficient for ransomware groups to gain entry into vulnerable networks. We believe that next-generation vulnerability management must adopt a predictive approach that can foresee the high exploitability of vulnerabilities long before they can be compromised.

> **"Threat actors are increasingly targeting flaws in cyber hygiene, including legacy vulnerability management processes. Today, many security and IT teams struggle to identify the real-world risks that vulnerabilities pose and therefore improperly prioritize vulnerabilities for remediation. For example, many organizations only patch new vulnerabilities or those that have been disclosed in the National Vulnerability Database (NVD). Others only use the Common Vulnerability Scoring System (CVSS) to score and prioritize vulnerabilities. To better protect organizations against cyberattacks, security and IT teams need to adopt a risk-based approach to vulnerability management. This requires AI-based technology that can identify enterprise exposures and active threats, provide early warnings of vulnerability weaponization, predict attacks, and prioritize remediation activities."— Srinivas Mukkamala, Senior Vice President & General Manager of Security Products at Ivanti**

Gaps in Techniques & Tactics Adopted to Exploit CWEs

CSW experts conducted a study of the techniques and tactics used by attackers while exploiting software weaknesses. This study was conducted using 500+ vulnerabilities that were a part of the CISA KEV catalog during the time of study.

Our research brought to the forefront the various gaps that exist in sites like MITRE, NVD, and Common Attack Pattern Enumeration and Classification (CAPEC) and how these discrepancies are aiding attackers. To assess the gaps and recommend remediation for each vulnerability, our researchers had to collate information from 17 different sources apart from the NVD and MITRE. Our key findings include:

- Missing CWEs for 61 vulnerabilities in the NVD
- Deprecated/Obsolete CWEs for 33 vulnerabilities in the NVD
- CWEs without CAPEC details for 87 vulnerabilities (54 excluding deprecated ones)
- CAPECs without MITRE mapping for 30 vulnerabilities

In order to overcome such data gaps and understand how these weaknesses might be taken advantage of, organizations must look to automated sources that can map vulnerabilities with corresponding MITRE techniques.

With security researchers and IT teams handicapped by information gaps, inaccurately mapped weaknesses, and missing tactics and technique information, critical vulnerabilities tied to ransomware are not prioritized. Furthermore, overworked security teams do not have the resources or the time to look at 17+ data sources to fill in intelligence gaps and make informed decisions for remediation.

"Ransomware is now one of the most predominant attack vectors affecting the bottom line of organizations globally. This Q1 report underscores the fact with new numbers that show an increase in the number of ransomware vulnerabilities and APTs using ransomware. However, one of the major concerns that has surfaced is the lack of complete threat visibility for security teams owing to cluttered threat intelligence available across sources. If security teams have to mitigate ransomware attacks proactively, they must tie their patch and vulnerability response to a centralized threat intelligence management workflow that drives complete visibility into the shape-shifting ransomware attack vectors through multi-source intelligence ingestion, correlation, and security actioning." **— Anuj Goel, Co-founder and CEO, Cyware**

Ransomware Index 2022 Q1

Focus	Q4 2021 Total	Q1 2022 Total	Percent Change
CVEs Associated with Ransomware	288	310	7.6% ↑
Actively Exploited* and Trending Vulnerabilities *Used with Ransomware	147	157	6.8% ↑
Low-Scoring* CVEs Tied to Ransomware *CVSS v2 score less than 8	173	193	11.6% ↑
Ransomware Vulnerabilities Missed by Scanners	22	11	50% ↓
Number of Ransomware Families	157	161	2.5% ↑
Number of APT Groups Associated with Ransomware	40	43	7.5% ↑
Older* Vulnerabilities Associated with Ransomware *Vulnerabilities from 2021 or earlier	263	310	17.9% ↑
CWEs	54	63	9 new CWEs ↑
Ransomware Vulnerabilities part of CISA KEVs	57	141	84 new CVEs ↑
Exploit Kits in Use by Ransomware	31	31	-

Key Findings

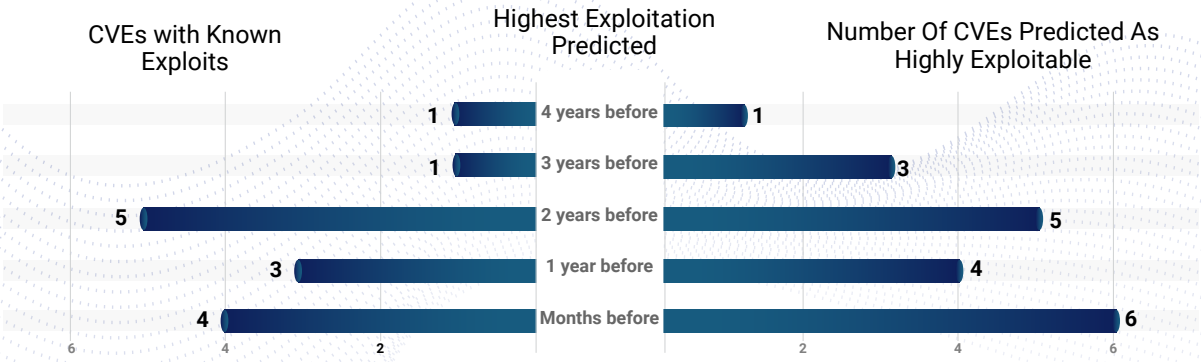
7.6% Increase in Vulnerabilities Tied to Ransomware

Our ongoing research into vulnerabilities exploited by ransomware groups has uncovered 22 new vulnerabilities in Q1 2022, marking a 7.6% increase from December 2021. Overall, 310 vulnerabilities are now tied to ransomware. All of these vulnerabilities have patches, mitigations, or workarounds available, and organizations are recommended to apply fixes before it is too late.

Vulnerability Analysis

- 11 of the 22 vulnerabilities recently linked with ransomware are from the year 2019, indicating that ransomware groups are on the hunt for vulnerabilities with pre-existing means of exploitation.
- The newly added vulnerabilities include three of critical severity, 18 tagged as high severity, and one belonging to the medium-severity category.
- 14 of the updated vulnerabilities have known public exploits (six for remote code execution (RCE), 12 for privilege escalation (PE), four for web app vulnerabilities, and one for denial-of-service (DoS)). In particular, CVE-2021-22005 and CVE-2021-22986 are linked to publicly available exploits for RCE, PE, and web app attacks.
- Seven of the 22 vulnerabilities are enumerated under the weakness category CWE-59, which leads to improper link resolution while accessing files. Popularly called the 'insecure temporary file' weakness, the software could resolve to an unintended shortcut or resource, which could allow attackers to bypass security mechanisms.
- Two notable callouts are CVE-2021-22986 (F5), which affects 73 products from F5, and CVE-2021-21985 affecting 56 VMware products.

Our ransomware and threat intelligence predicts the highest possibilities of exploitation for 19 of these vulnerabilities. For 14 of these vulnerabilities, we warned of high threat chatter more than 10 months prior to the time of publishing this report. **Our early predictions provide ample time for organizations to address these vulnerabilities and stay safe from ransomware attacks.**



Information Nuggets:

- Conti, one of the most prolific ransomware groups of 2022, is associated with 19 of the 22 new vulnerabilities.
- The remaining new vulnerabilities have been exploited by BlackCat, LockBit, and AvosLocker ransomware families.

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

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

6.8% Increase in Actively Exploited Vulnerabilities

The count of trending and heavily exploited ransomware vulnerabilities continues to grow higher. In Q1 2022, we identified 10 ransomware vulnerabilities that were actively discussed in dark web chats and were exploited in the wild, taking the total count to 157.

CVE-2021-22005 and CVE-2021-21985 were called out by CSW's experts as potential ransomware targets even before they were associated with ransomware.

2.5% Increase in the Number of Ransomware Families

Our research spotted four new ransomware families that emerged in Q1 2022, increasing the ransomware family count from 157 to 161.

New Ransomware Families	No. of CVEs Leveraged by the Family
AvosLocker	5
Karma	3
BlackCat (AlphaV)	2
Night Sky	1

The AvosLocker and Karma ransomware families have both targeted CVE-2021-31207, CVE-2021-34473, and CVE-2021-34523 in the Microsoft Exchange Server. These vulnerabilities also have associations with six recently active ransomware families including BlackByte, Conti, Babuk, and LockFile. In fact, all five vulnerabilities tied to AvosLocker are present in Exchange Servers.

The BlackCat family has adopted the capabilities to exploit a 6-year old vulnerability in older versions of Microsoft Windows. The group also takes advantage of a 2019 SQL injection flaw in SonicWall Secure Remote Access devices that have reached their end-of-life, a trend we have been calling out in our reports since 2021.

Ransomware Leader: The Conti ransomware family dominated the first quarter of 2022 with its initial declaration of support for Russia in the war against Ukraine, playbook leaks, consistent attacks, and data leaks on the dark web. Our research connects Conti to 27 vulnerabilities in Q1 2022, more than doubling its vulnerability count from 2021. As of writing this report, Conti has added 44 vulnerabilities to its arsenal!

Prolific ransomware groups like Conti are always on the lookout to add more vulnerabilities to their arsenal. As we track the trajectory of these threats, we cannot stress enough the importance of organizations adopting vulnerability intelligence, continual scanning, and attack surface management of digital ecosystems to protect their networks and data.

To view Indicators of Compromise (IOCs) of the new ransomware groups, please check the Appendix C.

7.5% Increase in the Number of APT Groups

In Q1 2022, CSW identified three new Advanced Persistent Threat (APT) groups using ransomware to invade organizational networks. We now have 43 APT groups deploying ransomware in their attacks, recording a 7.5% increase from 2021.

The adjacent table shows the newly identified ransomware groups.

The recent cyberwar sparked by the Russia-Ukraine conflict saw the use of a multitude of malware and ransomware threats from APT groups against nations supporting the warring countries. We also saw Conti ransomware operators openly pledging support to Russia and vowing to take down the critical infrastructure of Russia's "enemies."

APT Group	Country
DEV-0401	China
Exotic Lily	-
APT 35	Iran

> "If cyberwar becomes the precursor of all conflicts in the world, critical government entities and infrastructure in all countries would need better cybersecurity. Timely insights and accurate intelligence about emerging threats is the need of the hour to protect these ecosystems from incendiary attacks." — **Aaron Sandeen, CEO & Co-Founder, CSW**

9 New Weakness Categories Associated with Ransomware

Our analysis of ransomware vulnerabilities brought up nine new weaknesses giving rise to these flaws in Q1 2022. With this 17% increase, we now have 189 weaknesses powering the 310 vulnerabilities associated with ransomware groups.

With ransomware targeting specific weaknesses across multiple products and applications, organizations are going to need additional application scanning to understand and prioritize their vulnerabilities.

Based on the perspective of a penetration tester, we have spotlighted six of the most dangerous weaknesses that an attacker would hone in on as targets.

New Ransomware CWEs in Q1 2022	Weakness Category	OWASP Ranking	MITRE Ranking	Ransomware	Impact
CWE-285	Improper Authorization	A01	-	eCh0raix Qlocker	Could allow unauthorized resource access and can escalate to broken access control issues, XSS, and session replay issues
CWE-294	Authentication Bypass by Capture-Replay	A07	-	ClearEnergy	Can be escalated to perform code execution, session sidejacking, kerberoasting, remote services with stolen credentials, pass the hash, pass the ticket, and adversary-in-the-middle (AiTM) attacks
CWE-345	Insufficient Verification of Data Authenticity	A08	-	UEFI	Could result in failure to verify origin or authenticity of data, and can be used to perform code execution
CWE-36	Absolute Path Traversal	-	-	Phobos JNEC Shkolatacrypt Stop	Could give rise to path traversal and code execution vulnerabilities due to not neutralizing the absolute path
CWE-400	Uncontrolled Resource Consumption	-	27	Conti Khonsari TellYouThePass NightSky Stop	Could lead to lack of throttling for the number of allocated resources, losing all references to a resource before reaching the shutdown stage, not closing or returning a resource after processing, error conditions and other exceptional circumstances, and confusion over which part of the program is responsible for releasing the resource
CWE-693	Protection Mechanism Failure	-	-	UEFI Shkolatacrypt	Could be used to perform forceful browsing, manipulating states, directory indexing, and using unpublished interfaces

Additionally, our analysis of the techniques and tactics used by attackers exploiting vulnerabilities associated with ransomware indicated that the 310 ransomware vulnerabilities were more than enough for attackers to enter into networks, infiltrate deeper, evade detection, lock files, and demand ransoms. This makes CSW's list of 310 vulnerabilities highly dangerous and essential to safeguard against.

For a detailed MITRE analysis, please check Appendix B.

17.9% Increase in Older Vulnerabilities Tied to Ransomware

As observed from the start of our ransomware research, ransomware groups continue to leverage older vulnerabilities.

CSW noted that all the ransomware vulnerabilities newly identified in this quarter belong to this category. We now have 310 older vulnerabilities, a 17.9% increase from the previous report. The total now accounts for 100% of the ransomware vulnerabilities identified from our research—an indication of groups utilizing matured exploits and publicly available codes that can easily be customized for their needs.

CVE-2015-2546, a 7-year old medium-severity vulnerability, has been associated with ransomware in Q1 2022, along with two other vulnerabilities from 2016 and 2017.

Age of Vulnerability	Count of Vulnerabilities Used By Ransomware
More than 10 years old (Before 2013)	23
5–10 years old (2013–2017)	133 (includes 4 added in Q1 2022)
Less than 5 years old (2018–2021)	154 (includes 18 added in Q1 2022)

Note: *For the purposes of this report, we consider vulnerabilities belonging to 2021 and earlier as old.*

11.6% Increase in Low-Severity Vulnerabilities Tied to Ransomware

A pattern we have constantly observed is how ransomware groups not only go after critical vulnerabilities, but also target the low and high severity ones that often do not take precedence in an organization's patching cadence.

20 of the 22 vulnerabilities identified in this quarter are low-scoring vulnerabilities with CVSS v2 scores of less than eight. This marks an 11.6% increase in Q1 2022, contributing to 193 of all low-scoring ransomware vulnerabilities overall. At 82%, high-severity vulnerabilities dominate the list of newly added vulnerabilities this quarter, by CVSS V3 classification.

CSW's findings indicate that the true risk of vulnerabilities in an organization's attack surface is not based only on a vulnerability's severity, but on other factors such as its exploitability and associated ransomware threats, thus requiring a holistic outlook towards vulnerabilities and threats.

Vendor Products with Ransomware Vulnerabilities

Our research identified 919 unique products belonging to 103 distinct vendors as susceptible to ransomware overall. The new vulnerabilities identified in Q1 2022 affect 164 different products.

Vendor	Overall Count of Vulnerabilities	Product with Most Vulnerabilities
F5	17	Big IP products
Microsoft	143	Windows
VMware	4	Cloud Foundation and vCenter Server

The product category most affected by the new set of ransomware vulnerabilities are operating systems, followed by firewalls and web browsers.

Product Category	Count of Vulnerabilities
Operating System	125
Firewall	17
Web Browser	12
Desktop App	3
Cloud Desktop Application	2
Application Framework	2
Web Application	1
Microsoft Office Suite	1
Email Service	1

Healthcare Sector

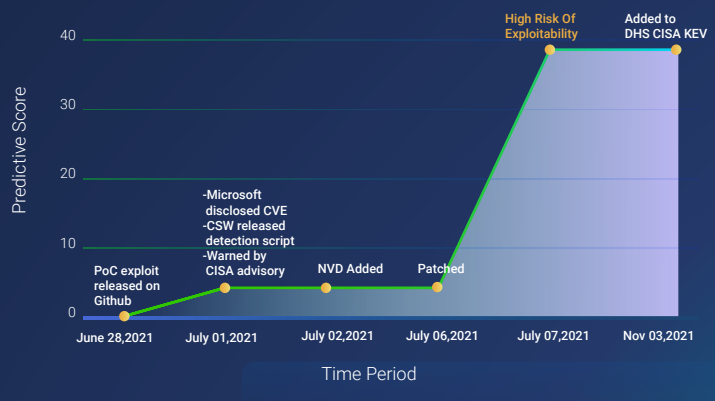
As a part of CSW's ongoing research, we analyzed 56 vendors that supply healthcare applications, medical devices, and hardware used in hospitals and healthcare centers. Here are some of our key findings for this sector.

Our Analysis

We investigated 56 vendors and 846 products and found 624 unique vulnerabilities in their products.

- 40 vulnerabilities have public exploits.
- Two vulnerabilities—CVE-2020-0601 and CVE-2021-34527—are associated with four ransomware operators: BigBossHorse, Cerber, Conti, and Vice Society.
- Four vulnerabilities in healthcare products are being used by the group APT1, a China-based threat actor.

CVE-2021-34527



Name: Windows Print Spooler Vulnerability
The vulnerability arose from an incomplete patch for CVE-2021-1675

Device Category: Surgical Equipment

Affected Healthcare Devices: Vendor - Stryker

- ADAPT Platform
- Nav3i Platform
- Nav3 Platform
- Scopis ENU

Impact: Exploitation of this vulnerability can lead to malfunctioning during critical surgeries, resulting in permanent patient disabilities or even death.

On 31 July 2021, a remote print server was developed that allows any Windows user with limited capabilities to have total control over a device simply by installing a print driver.

Exploit Type: RCE

Ransomware Associations : Conti, Cerber, Vice Society

CVE-2020-0601

Name: Windows CryptoAPI Spoofing Vulnerability
This spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates.

Device Category: Operating System

Affected Healthcare Devices:

- Biomereux

Impact: An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source

Exploit Type: Public exploit code available

Ransomware Associations : BigBossHorse

Our year-end report highlighted prominent cybersecurity attacks on the healthcare sector, such as Conti's Ireland attack, pneumatic tube exploits, dosage level adjustments, and hospital network outages, one of which resulted in the death of an infant.

CSW has analyzed some of the vulnerabilities identified in medical devices from early 2022. Although these are not associated with ransomware yet, we fear it may not be long before ransomware operators start exploiting the vulnerabilities listed below:

- **75% of network-connected medical infusion pumps were found vulnerable to security flaws from 2019–2020, which could lead to abnormal and fatal medicine dosages administered to patients.**
- **CVE-2021-43935 in Hillrom cardiac devices could be exploited to completely gain control of medical equipment that monitors cardiac stress levels, ECGs, and other cardiac-related issues.**
- **Vulnerabilities identified in the Aethon TUG smart autonomous mobile robots and JekyllBot:5 provide an easy setup for lateral movement across hospital networks and a perfect launchpad for ransomware payloads.**

> "Healthcare providers must be extremely vigilant in their cybersecurity defense posture. Unfortunately, as the pandemic calms down, the healthcare industry will likely be targeted more aggressively by ransomware attacks that cripple networks and endanger patient safety. Attackers have gotten more sophisticated, and they will likely target healthcare IoT devices like IV pumps, not just traditional devices like mobile devices and laptops."
>
> **— Srinivas Mukkamala, Senior Vice President & General Manager of Security Products at Ivanti**

Ransomware CVEs That Should be Listed Among CISA KEVs

Critical industries such as food, automotive, healthcare, finance, and government organizations have taken a big hit in this quarter, continuing the trend from 2021. In February 2022, cybersecurity advisories in the US, Australia, and UK joined hands to alert organizations of increased ransomware attacks on critical infrastructure sectors. Prior to this, CISA released a mandate directing federal agencies and public sector organizations to patch a list of KEVs within fixed timelines.

A total of 45.4% of the ransomware vulnerabilities identified in our research are part of the CISA KEVs. However, we would also like to highlight that the remaining 54.6%, which total 169 vulnerabilities with ransomware associations, are yet to be added to the CISA KEV list. Hackers worldwide are actively targeting 100 of these vulnerabilities, scouting organizations for one unpatched instance to exploit.

Four of the new vulnerabilities (CVE-2019-1130, CVE-2019-1385, CVE-2020-0638, CVE-2021-31206) are yet to be added to the CISA KEVs*. CVE-2021-31206 is a special call-out because it was recently associated with AvosLocker ransomware, and has been trending for the last 30 days.

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

Latencies in Ransomware Vulnerabilities

As part of our ransomware research, we also studied the latencies in publishing and patching newly identified vulnerabilities tied to ransomware. Here are some of our observations.

A key factor that stands out is the speed of weaponization of ransomware vulnerabilities. Some vulnerabilities were exploited within eight days of being published by their vendor!

- **All new ransomware vulnerabilities were published by their vendors together with a patch.**
- **Outlier vulnerabilities with respect to weaponization—CVE-2016-3309, CVE-2017-0101 and CVE-2019-1215—were exploited almost a year after the vulnerabilities were published and patched by their vendors and added to the NVD.**
- **Five of the vulnerabilities were exploited before they could be added to the NVD.**
- **On average, new ransomware vulnerabilities were added to the NVD a week after they were disclosed by their vendor.**

Ransomware Groups: Notable Movers and Shakers

The LockBit ransomware group joins the ranks of Conti and REvil with multiple attacks in the first quarter of 2022. It has also been actively deployed in the Ukraine-Russia cyberwar. The BlackCat/AlphaV, Lapsus$ (still under research), and Hive ransomware groups feature in the news every other day either for a data breach, a technique advancement, addition of malware to their toolkit, or even insider recruitment. This trend was called out in our Ransomware Spotlight Report 2022 released in January this year.

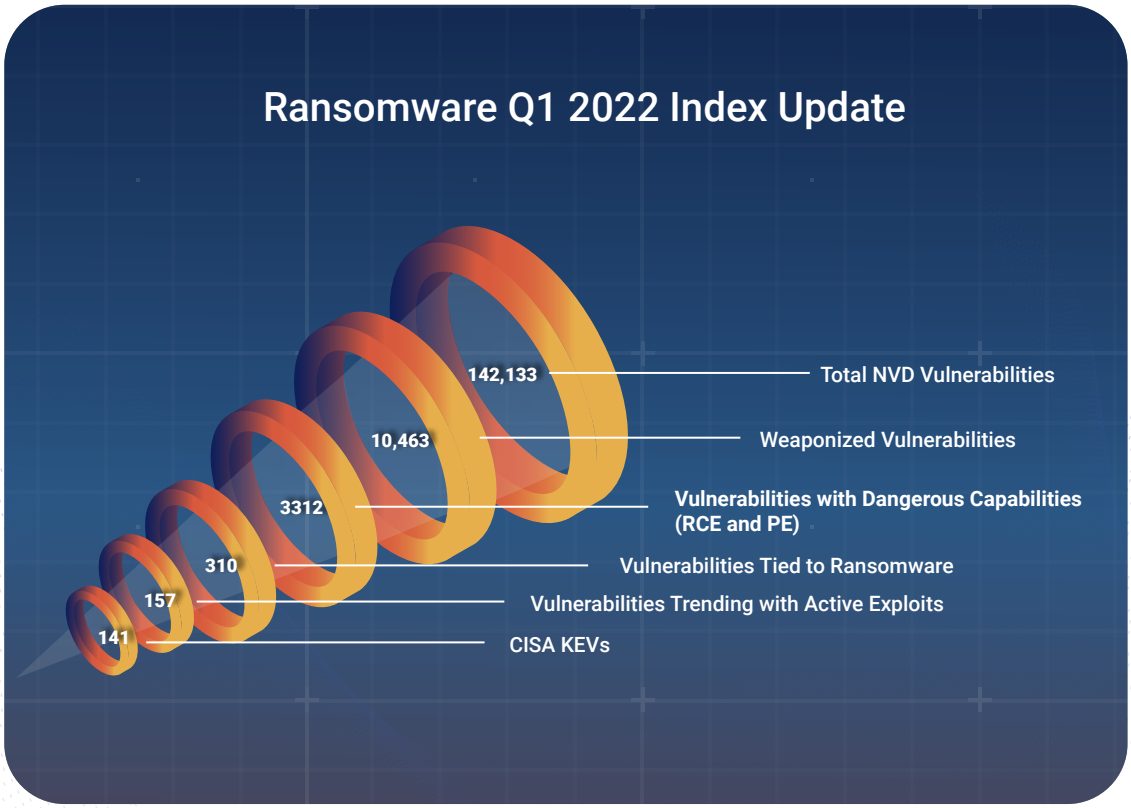
Recent news reports highlight a new Quantum ransomware group that deployed a ransomware payload within four hours of gaining access to the victim's network. Stay tuned for more on this in our upcoming reports!

Storage devices play a key role in ransomware recovery but ransomware groups, such as Qlocker and eCh0raix, are targeting them to clean out data backups and force victims to pay a ransom to release their data. In the past quarter, we have seen DeadBolt ransomware joining the trend by targeting QNAP devices.

Another menace is the Pegasus Spyware that utilized zero-click vulnerabilities to launch cyber-espionage campaigns on political figures worldwide. The spyware took advantage of the vulnerability chaining trend, and was recently spotted infecting phones of the Spanish Prime Minister and Defense Minister. Read more about vulnerability chaining in our Year End Spotlight Report.

Although not a 2022 find, the Log4j vulnerability: CVE-2021-44228, has continued to have its impact in Q1 of this year and is a worthy mention. Following our analysis in January, we now have four ransomware groups exploiting the vulnerability: Conti, Khonsari, Night Sky, and TellYouThePass. Notably, the notorious Conti group was the first to weaponize Log4j using a full attack chain.

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.



Combating Ransomware

Ransomware is a pervasive threat. Attackers and ransomware operators are constantly looking for more vulnerabilities to weaponize and increase their arsenal of tools, tactics, and techniques. The FBI's Internet Crime Report for 2021 recorded 649 ransomware attacks on critical infrastructure establishments, with nearly $50 million USD reportedly lost as a result.

All organizations are at risk from this threat, and most of them are not equipped to deal with it. Lack of cyber hygiene, budget restrictions, limited manpower, absence of talent, insufficient cybersecurity intelligence at the right time, and the lack of visibility and awareness are some of the factors that enable ransomware operators to undertake bold and crippling attacks.

We have seen this threat grow exponentially within two years from 57 to 310 vulnerabilities. We have watched affected organizations brought to their knees as they lose their reputation, trust, and brand value, resulting in the loss of business and customers.

Today, only a few organizations have access to timely knowledge and data about ransomware. Many are not cognizant about the level of threats they are facing. The overarching goal of this report is to provide the global community with a wake-up call about the threats they face.

We believe that access to accurate knowledge and data is an invaluable asset that can help organizations gain resilience against these evolving threats.

Cyber Security Works (CSW)

Security professionals need timely insights that would allow them to be agile and protect their networks from emerging and evolving threats. CSW experts have been tracking ransomware threats for a long time and we help organizations gain resilience against them even while their peers fall victim to attacks.

Continuous Vulnerability Management as a Service specifically focuses on ransomware exposure powered by our vulnerability intelligence to help stay ahead of attackers. Our recently acquired threat intelligence platform uses AI and machine learning (ML) capabilities to red-flag vulnerabilities with a high probability of exploitation. Using threat intelligence, our security experts prioritize vulnerabilities within the customer network and proactively help them remediate critical vulnerabilities.

Get proactive with your defense and get yourself a cyber intelligence team! Talk with us.

Securin

Securin's Attack Surface Management platform empowers organizations to find their true attack surface and dangerous exposures that make them susceptible to ransomware threats. Discover your known and unknown assets to get a hacker's view of your attack surface and prioritize your exposures based on the threat context.

Manage your exposures to Ransomware threats! Talk with us.

Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers. Cyware is transforming security operations by delivering the Cyber Fusion Center Platform, the next-generation SOC (NG-SOC), for its customers orchestrating the entire post-detection SecOps with automated SOC (ASOC) capabilities. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, sharing communities (ISAC/ISAO), MSSPs, and government agencies.

Ivanti

Ivanti Neurons for Risk-Based Vulnerability Management (RBVM) helps organizations measure, prioritize, and control their cybersecurity risk so they can better protect against ransomware and other dynamic cyber threats. This is critical as ransomware groups are continuing to grow in sophistication, boldness, and volume. Ivanti's proprietary Vulnerability Risk Rating (VRR) quantifies adversarial risk so customers can take risk-based prioritized action, while automation increases the efficiency and effectiveness of vulnerability management processes. Additionally, role-based access control (RBAC) plus information available in both ready-made and customizable views enable better communication and collaboration among security stakeholders.

Get a free live demo of Ivanti Neurons for RBVM

CSW Cyber SecurityWorks

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

https://www.cybersecurityworks.com/

Securin

Founded by security experts, Securin's Attack Surface Management Platform empowers organizations to discover their assets, prioritize exposures and misconfigurations that could lead to a breach.

For more information visit securin.io.

CYWARE™

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

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

https://cyware.com/

ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they work from anywhere. The Ivanti Neurons automation platform connects the company'sindustry-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.

www.ivanti.com

Appendix A: Ransomware CVEs Missed By Popular Scanners

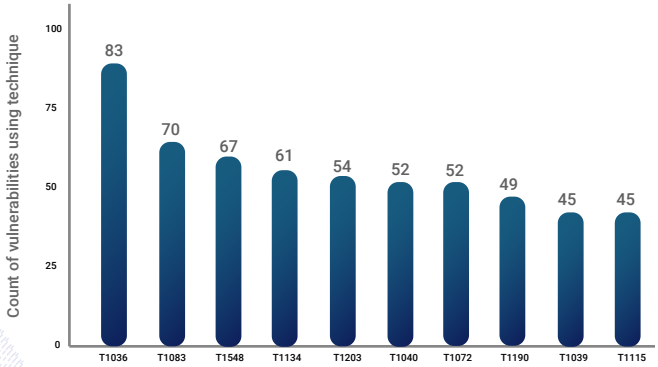
CVE	Vendor	Product	Recommended Mitigations & Patches
CVE-2010-1592	SiSoftware	Sandra	1, 2, 3, 4
CVE-2017-18362	Connectwise	Manageditsync	1, 2, 3
CVE-2017-3197	Gigabyte	gb-bsi7h-6500 Firmware	1, 2, 3, 4, 5
CVE-2017-3198	Gigabyte	gb-bsi7h-6500 Firmware	1, 2, 3
CVE-2017-6884	Zyxel	emg2926 Firmware	Patch Now
CVE-2018-19943	QNAP	QTS	Patch Now
CVE-2018-19949	QNAP	QTS	Patch Now
CVE-2018-19953	QNAP	QTS	Patch Now
CVE-2019-16920	Dlink	DIR-655 Ffirmware	1, 2, 3, 4
CVE-2019-18426	WhatsApp	WhatsApp	1, 2
CVE-2013-3993	IBM	InfoSphere BigInsights	Patch Now

Appendix B:
Mitre Mapping for Ransomware Vulnerabilities

MITRE ID	Tactic	MITRE Description of Tactic	CVE Count	Product Count	Vendor Count
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.	12	9	4
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.	31	25	21
TA0001	Initial Access	The adversary is trying to get into your network.	122	61	38
TA0002	Execution	The adversary is trying to run malicious code.	125	60	35
TA0003	Persistence	The adversary is trying to maintain their foothold.	95	47	27
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.	202	96	58
TA0005	Defense Evasion	The adversary is trying to avoid being detected.	243	107	64
TA0006	Credential Access	The adversary is trying to steal account names and passwords.	126	69	46
TA0007	Discovery	The adversary is trying to figure out your environment.	78	36	22
TA0008	Lateral Movement	The adversary is trying to move through your environment.	130	58	34

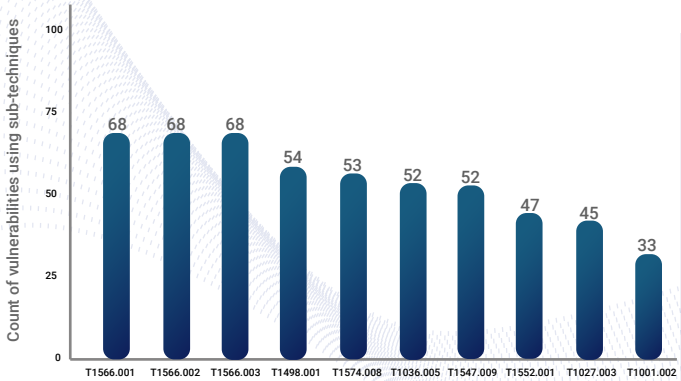
MITRE ID	Tactic	MITRE Description of Tactic	CVE Count	Product Count	Vendor Count
TA0009	Collection	The adversary is trying to gather data of interest to their goal.	70	51	36
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.	34	24	14
TA0010	Exfiltration	The adversary is trying to steal data.	30	16	11
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.	62	27	15

Most Common MITRE Techniques



T1036: Masquerading - Defense Evasion
T1083: File and Directory Discovery - Discovery
T1548: Abuse Elevation Control Mechanism - Privilege Escalation, Defense Evasion
T1134: Access Token Manipulation - Defense Evasion, Privilege Escalation
T1203: Exploitation for Client Execution - Execution
T1040: Network Sniffing - Credential Access, Discovery
T1072: Software Deployment Tools - Execution, Lateral Movement
T1190: Exploit Public-Facing Application - Initial Access
T1039: Data from Network Shared Drive - Collection
T1115: Clipboard Data - Collection

Most Common MITRE Sub-Techniques



T1566.001: Spearphishing Attachment - Initial Access
T1566.002: Spearphishing Link - Initial Access
T1566.003: Spearphishing via Service - Initial Access
T1498.001: Direct Network Flood - Impact
T1574.008: Path Interception by Search Order Hijacking - Persistence, Privilege Escalation, Defense Evasion
T1036.005: Match Legitimate Name or Location - Defense Evasion
T1547.009: Shortcut Modification - Persistence, Privilege Escalation
T1552.001: Credentials In Files - Credential Access
T1027.003: Steganography - Defense Evasion
T1001.002: Steganography - Command and Control

Appendix C: Indicators of Compromise for New Ransomware Groups

AvosLocker

Hashes

SHA 1:

05c63ce49129f768d31c4bdb62ef5fb53eb41b54
6f110f251860a7f6757853181417e19c28841eb4
9c8f5c136590a08a3103ba3e988073cfd5779519
e8c26db068914df2083512ff8b24a2cc803ea498
dab33aaf01322e88f79ffddcbc95d1ad9ad97374
e60ef891027ac1dade9562f8b1de866186338da1
67f0c8d81aefcfc5943b31d695972194ac15e9f2
2f3273e5b6739b844fe33f7310476afb971956dd
f6f94e2f49cd64a9590963ef3852e135e2b8deba

MD5:

e09183041930f37a38d0a776a63aa673
d3cafcd46dea26c39dec17ca132e5138
f659d1d15d2e0f3bd87379f8e88c6b42
afed45cd85a191fe3b2543e3ae6aa811
31f8eedc2d82f69ccc726e012416ce33
a39b4bea47c4d123f8195a3ffb638a1b
504bd1695de326bc533fde29b8a69319
eb45ff7ea2ccdcceb2e7e14f9cc01397
d285f1366d0d4fdae0b558db690497ea
cf0c2513b6e074267484d204a1653222

Karma

Hashes

SHA256:

1c41acdc2e9d8b89522ebb51d65b4c41d7fd130a14ce9d449edb05f53bbb8d59
6c98d424ab1b9bfba683eda340fef6540ffe4ec4634f4b95cf9c70fe4ab2de90
0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27
84d24a16949b5a89162411ab98ab2230128d8f01a3d3695874394733ac2a1dbd
124f3a5caf6eb464027f2865225a6a1238c3639e5b4a399f0f7f2dda7bd75aec
3ff1b90dbad5d78397fdc731c3a3c080d91fc488ac9152793b538b74a1e2d8f3
ad841882052c3f9d856ad9a393232e0a59d28e17c240d23258f1dac62f903ab8
19417c0a38a1206007a0cc82c0fc2e19db897214d27d0998bc4dbac53cc2788d
a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0
34629751d8202be456dcf149b516afefc980a9128dd6096fd6286fee530a0d20

SHA1:

08f1ef785d59b4822811efbc06a94df16b72fea3
338cff5f17663b7552fb0d687d3b67e9b47fca95
a9367f36c1d2d0eb179fd27814a7ab2deba70197

Night Sky

Hashes

2594077763e054861c086f49b8b1e9cf
9608c8b6c8d80fdc67b99edd3c53d3d2
f9481915373852640150ffe98e7218ab
37b11d3d7b7a1d18daafd6c63b33526860aaefe6
44a124b9e5894b69a1ef108d9afcdb64e3591162
682fa27b596bab8fc5b7f2a0c002447e6e2f1f6b
197d3c8a1ebf4650196e677f6b992fad1cb0f066c4d7dae32f35d24a76b1acaf
1fca1cd04992e0fcaa714d9dfa97323d81d7e3d43a024ec37d1c7a2767a17577
59c9e91ce745914985b3a0b77f6b09c9776d4746de52f02648108961063b2ddd
8c1a72991fb04dc3a8cf89605fb85150ef0e742472a0c58b8fa942a1f04877b0
93f840951fc457649fe595f8149a20be91ed742afaa90aa95759f0b29c5f5668
a077a55608ced7cea2bd92e2ce7e43bf51076304990ec7bb40c2b384ce2e5283
c30d6587fb149c117f8cebc54407abfdf2cefc6096d8a4fc9e5d2e5f890d9f64
e7e7b19c255ea052bb3c59b5597cdc92e76abe4dab72dacb92b16b7029e0d72f
6d87be9212a1a0e92e58e1ed94c589f9
9608c8b6c8d80fdc67b99edd3c53d3d2
19ce538b2597da454abf835cff676c28b8eb66f7
37b11d3d7b7a1d18daafd6c63b33526860aaefe6
8c1a72991fb04dc3a8cf89605fb85150ef0e742472a0c58b8fa942a1f04877b0
c2d46d256b8f9490c9599eea11ecef19fde7d4fdd2dea93604cee3cea8e172ac
tset123155465463213

C2C servers

service[.]trendmrcio[.]com
api[.]rogerscorp[.]org
api[.]sophosantivirus[.]ga
apicon[.]nvidialab[.]us
w2zmii7kjb81pfj0ped16kg8szyvmk.burpcollaborator[.]net
139[.]180[.]217[.]203.
139.180.217.203
45.32.125.79
45.76.188.137
87.120.36.12
207.148.122.171
http://139.180.217.203:443/LockDown[.dll]
http://45.32.125.79:443/LockDown[.dll]

nightsky[.cyou]
api.rogerscorp[.org]
api.sophosantivirus[.ga]
apicon.nvidialab[.us]
contact.nightsky[.cyou]
mail.nightsky[.cyou]
service.trendmrcio[.com]
w2zmii7kjb81pfj0ped16kg8szyvmk.burpcollaborator[.net]
suit[.md]
http://gg5ryfgogainisskdvh4y373ap3b2mxafcibeh2lvq5x7fx76ygcosad[.]onion

BlackCat

Hashes

SHA256:

59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
5121f08cf8614a65d7a86c2f462c0694c132e2877a7f54ab7fcefd7ee5235a42
f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6
0C6F444C6940A3688FFC6F8B9D5774C032E3551EBBCCB64E4280AE7FC1FAC479
2CF54942E8CF0EF6296DEAA7975618DADFF0C32535295D3F0D5F577552229FFC
CEFEA76DFDBB48CFE1A3DB2C8DF34E898E29BEC9B2C13E79EF40655C637833AE
658E07739AD0137BCEB910A351CE3FE4913F6FCC3F63E6FF2EB726E45F29E582
B588823EB5C65F36D067D496881D9C704D3BA57100C273656A56A43215F35442
3D7CF20CA6476E14E0A026F9BDD8FF1F26995CDC5854C3ADB41A6135EF11BA83
7154FDB1EF9044DA59FCFDBDD1ED9ABC1A594CACB41A0AEDDB5CD9FDAEEA5EA8
3a08e3bfec2db5dbece359ac9662e65361a8625a0122e68b56cd5ef3aedf8ce1
9802a1e8fb425ac3a7c0a7fca5a17cfcb7f3f5f0962deb29e3982f0bece95e26
e7060538ee4b48b0b975c8928c617f218703dab7aa7814ce97481596f2a78556
f7a038f9b91c40e9d67f4168997d7d8c12c2d27cd9e36c413dd021796a24e083
13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31
15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed
1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e
2587001d6599f0ec03534ea823aab0febb75e83f657fadc3a662338cc08646b0
28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169
38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1
4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf
5bdc0fb5cfbd42de726aacc40eddca034b5fa4afcc88ddfb40a3d9ae18672898
722f1c1527b2c788746fec4dd1af70b0c703644336909735f8f23f6ef265784b
7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487

7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e
9f6876762614e407d0ee6005f165dd4bbd12cb21986abc4a3a5c7dc6271fcdc3
aae77d41eba652683f3ae114fadec279d5759052d2d774f149f3055bf40c4c14
bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117
be8c5d07ab6e39db28c40db20a32f47a97b7ec9f26c9003f9101a154a5a98486
c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40
c5ad3534e1c939661b71f56144d19ff36e9ea365fdb47e4f8e2d267c39376486
c8b3b67ea4d7625f8b37ba59eed5c9406b3ef04b7a19b97e5dd5dab1bd59f283
cda37b13d1fdee1b4262b5a6146a35d8fc88fa572e55437a47a950037cc65d40
d767524e1bbb8d50129485ffa667eb1d379c745c30d4588672636998c20f857f
f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb
f2b3f1ed693021b20f456a058b86b08abfc4876c7a3ae18aea6e95567fd55b2e
40f57275721bd74cc59c0c59c9f98c8e0d1742b7ae86a46e83e985cc4039c3a5
f815f5d6c85bcbc1ec071dd39532a20f5ce910989552d980d1d4346f57b75f89
79802d6a6be8433720857d2b53b46f8011ec734a237aae1c3c1fea50ff683c13
bacedbb23254934b736a9daf6de52620c9250a49686d519ceaf0a8d25da0a97f
3c8ad2dae0b1bb536925b4e8d5a87e77c6134371eada2c7628358d6c6d3083dc
67d1f4077e929385cfd869bf279892bf10a2c8f0af4119e4bc15a2add9461fec
5a604a8f0e72f3bf7901b7b67f881031a402ab8072269c00233a554df548f54d
6660d0e87a142ab1bde4521d9c6f5e148490b05a57c71122e28280b35452e896
74464797c5d2df81db2e06f86497b2127fda6766956f1b67b0dcea9570d8b683

SHA1:

38fa2979382615bbee32d1f58295447c33ca4316
087497940a41d96e4e907b6dc92f75f4a38d861a
11203786b17bb3873d46acae32a898c8dac09850
2a53525eeb7b76b3d1bfe40ac349446f2add8784
45212fa4501ede5af428563f8043c4ae40faec76
57a6dfd2b021e5a4d4fe34a61bf3242ecee841b3
5869820f261f76eafa1ba00af582a9225d005c89
5c6ca5581a04955d8e4d1fa452621fbc922ecb7b
655c2567650d2c109fab443de4b737294994f1fd
783b2b053ef0345710cd2487e5184f29116e367c
89060eff6db13e7455fee151205e972260e9522a
9146a448463935b47e29155da74c68d16e0d7031
94f025f3be089252692d58e54e3e926e09634e40
a186c08d3d10885ebb129b1a0d8ea0da056fc362
c1187fe0eaddee995773d6c66bcb558536e9b62c
ce5540c0d2c54489737f3fefdbf72c889ac533a9
d65a131fb2bd6d80d69fe7415dc1d1fd89290394
da1e4a09a59565c5d62887e0e9a9f6f04a18b5f4
e17dc8062742878b0b5ced2145311929f6f77abd
e22436386688b5abe6780a462fd07cd12c3f3321
f466b4d686d1fa9fed064507639b9306b0d80bbf
d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
3f85f03d33b9fe25bcfac611182da4ab7f06a442
4831c1b113df21360ef68c450b5fca278d08fae2
37178dfaccbc371a04133d26a55127cf4d4382f8
fce13da5592e9e120777d82d27e06ed2b44918cf
1b2a30776df64fbd7299bd588e21573891dcecbe

MD5 Hashes:

861738dd15eb7fb50568f0e39a69e107
9f60dd752e7692a2f5c758de4eab3e6f
09bc47d7bc5e40d40d9729cec5e39d73
f5ef5142f044b94ac5010fd883c09aa7
9f2309285e8a8471fce7330fcade8619
84e3b5fe3863d25bb72e25b10760e861
6c6c46bdac6713c94debbd454d34efd9
e7ee8ea6fb7530d1d904cdb2d9745899
815bb1b0c5f0f35f064c55a1b640fca5
6c2874169fdfb30846fe7ffe34635bdb
82db4c04f5dcda3bfcd75357adf98228
20855475d20d252dda21287264a6d860
fcf3a6eeb9f836315954dae03459716d
91625f7f5d590534949ebe08cc728380

C2 IPs

89.44.9.243
142.234.157.246
45.134.20.66
185.220.102.253
37.120.238.58
152.89.247.207
198.144.121.93
89.163.252.230
45.153.160.140
23.106.223.97
139.60.161.161
146.0.77.15
94.232.41.155