SPOTLIGHT

RISKSENSE | CSW Cyber SecurityWorks

Ransomware

Through the Lens of Threat and Vulnerability Management

2021

Table of Contents

1 Executive Summary

Ransomware threats have exponentially increased. Our research uncovered 223 vulnerabilities tied to these threats; it has nearly quadrupled since our last report. Ransomware is also a compounding problem; we have seen older vulnerabilities continue to be leveraged alongside newly published vulnerabilities.

We've also seen higher adoption and utilization of these vulnerabilities across the ransomware families, increasing the overall count of trending with active exploits in the wild. It's safe to say that once a vulnerability is tied to ransomware it should be considered a high risk exposure point, regardless of its age.

Mapping vulnerabilities to real-world ransomware threats, and keeping pace with what is evolving, is a challenging cyclical process. Our research aims to bring actionable information to overworked security teams trying to cope with their never-ending list of vulnerabilities and remediation actions (applying patches, fixing misconfigurations, and addressing weakness from coding errors).

For organizations, this report brings to light the trends we've observed and provides the technical perspective of how ransomware is evolving and where an organization may have heightened ransomware risk exposure.

RiskSense this year partnered with Cyber Security Works (CSW), a leader in Attack Surface Management and an official CVE Numbering Authority (CNA). This joint effort expands beyond our previous report providing more details and trends that matter when it comes to ransomware vulnerability exposure.

Key Findings

Exponential Increase in Vulnerabilities (CVEs) tied to Ransomware

2020 has been a big year for ransomware attackers and with good reason - these threat actors had 223 vulnerable exposure points to get into your network. The number of CVEs that are being used by ransomware have nearly quadrupled since last year. However, only ten of these CVEs were published in 2020.

In our previous Spotlight Ransomware Report, we presented 57 CVEs tied to 19 ransomware families. This year, we found 223 unique vulnerabilities associated with 125 ransomware families.

Old is Gold for Ransomware

Threat actors continue to leverage older vulnerabilities. 96% of the CVEs we tracked, that's 213 out of the total 223, are vulnerabilities that were reported in the US National Vulnerability Database (NVD) before 2019.

The oldest vulnerability, CVE-2007-1036, dates from 2007 and is associated with the Crypsam (SamSam) ransomware family.

Ransomware Reigning Families, Old Lineage, & Upstarts

We identified 125 ransomware families using a mix of the 223 vulnerabilities tied to ransomware threats. Our previous report highlighted 19 ransomware families. While identifying ransomware families is a moving target, it's notable that this wild growth shows there are plenty of targets and prosperity in these threat tactics to support this type of expansion.

Even older ransomware families, such as Cobralocker (2012), Gimemo (2012), Kovter (2012), Lokibot (2012), Lyposit (2012), Reveton (2012), Urausy (2012) Crilock (2013), Cerber (2016), and Cryptomix (2016), are not showing any signs of retiring.

In fact, CryptoMix -- a family with old lineage with five well known ransomware threats (CLOP, Mole, CryptFIle2, CryptoMix, CryptoMix Revenge) -- is an example of how individual ransomware families expand their capabilities and sophistication. We found this family is utilizing 50 CVEs, the oldest from 2010, and they are also tied to CVE-2020-1472, a new vulnerability disclosed in 2020.

The upstart is Ryuk, accelerating ransomware to the adversarial masses with a ransomware-as-a-service delivery model. They have figured out how to monetize the business of ransomware, providing a code-free way for those wishing to target specific businesses or asset types.

New Horizons for Ransomware with Diversified Targets

Ransomware is cleverly looking at diverse targets to infiltrate organizations, moving up from server operating systems to weaknesses in Web and Application frameworks and applications themselves. 18 CVEs tied to ransomware are found across 6 major components in this space: WordPress, Apache Struts, Java, PHP, Drupal, and ASP.net.

We've observed popular Open Source and related projects, Jenkins, MySQL, OpenStack, TomCat, Elasticsearch, OpenShift, JBoss, and Nomad, with 19 vulnerabilities from this group being used by ransomware.

Software as a service (SaaS) as a category had the highest count of vulnerabilities that were seen trending with active exploits among ransomware families. This shift shows how these threats are moving as organizations consume more applications in this manner. The problem however is that organizations must rely on these service providers to ensure they are remediating quickly against these threats.

Foundational Code Weaknesses and Predicting Ransomware

40% of the CVEs tied to ransomware are associated with 5 Common Weakness Enumerations (CWEs):

- **CWE-119:** Improper Restriction of Operations within the Bounds of a Memory Buffer
- **CWE-20:** Improper Input Validation
- **CWE-264:** Permissions, Privileges, and Access Controls
- **CWE-94:** Improper Control of Generation of Code ('Code Injection')
- **CWE-200:** Exposure of Sensitive Information to an Unauthorized Actor

This correlation makes it easy to predict that new vulnerability disclosures with similar traits will be of interest to ransomware families. Three of these five CWEs are already found in the 2020 Top 25 Most Dangerous Software Weaknesses (CWE-119, CWE-20, and CWE-94).

By testing and fixing for these CWEs, application developers and software vendors can decrease the ease in which ransomware can attack and limit the frequency of critical security patches.

Ransomware Activity in Advanced Persistent Threat Groups

We have added a new focus in this report looking at how specific ransomware is going beyond weaponized attacks on organizations to being utilized by known adversaries with potentially broader nefarious motives. We identified 33 unique APT groups commonly using 65 ransomware exploits.

Our research uncovered ransomware association with nation state actors across the globe. Of interest is that we can link Russia to nine groups (APT28, Doppel Spider, Dungeon Spider, GOLD SOUTHFIELD, Pinchy Spider, Sandworm Team, TA505, Turla, and Zombie Spider) and China to eight APT Groups (Wizard Spider, Rocke, Naikon, Cycldek, APT41, APT40, APT10, and APT 1) respectively incorporating ransomware as part of their arsenal to launch offensive cyber attacks.

2

Taking a Risk-Based View of Ransomware Vulnerabilities

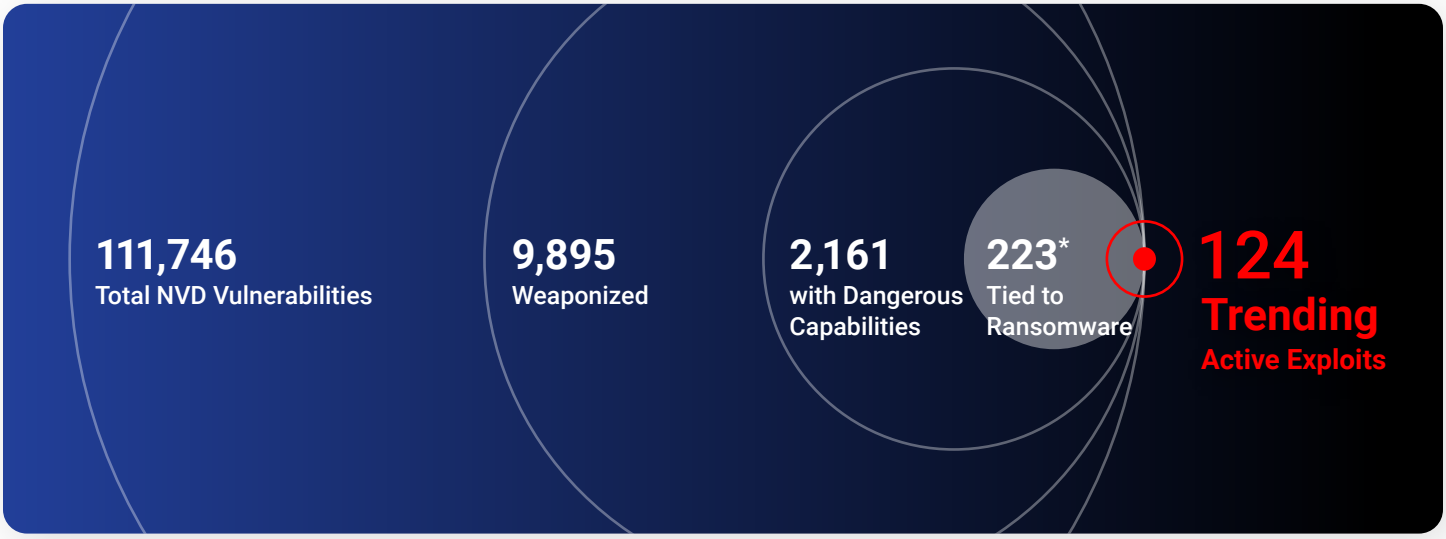
Among the thousands of vulnerabilities that are discovered every year, mapping them to real-world threat-based information helps security teams prioritize the patching for the most dangerous vulnerabilities that would cause the most damage.

This mapping is significant for two reasons. Firstly, a huge majority of vulnerabilities are not weaponized; if there is not an exploit, then the risk is minimal. Secondly, even if a vulnerability has an exploit it is only when these vulnerabilities are actively being targeted and used as part of an in-the-wild-attack do they dramatically increase an organization's risk exposure.

That's why our research begins by looking at three metrics that ultimately will help organizations prioritize and fix vulnerabilities that really matter.

- **Weaponized Vulnerabilities:** Vulnerabilities that have associated exploit code that is capable of taking advantage of the vulnerability
- **Strategic Vulnerabilities:** Vulnerabilities that have dangerous capabilities, mostly those that allow remote code execution (RCE) or privilege escalation (PE). These are highly valuable to attackers and significantly increase an organization's risk of becoming a victim
- **Trending Vulnerabilities:** These are vulnerabilities that are actively being used in-the-wild. In this report, we further refined the list by honing in on the CVEs we found that were tied to ransomware threats and families

In the past report, the strategic vulnerabilities only included those that had RCE or PE capabilities. In this report, as ransomware expands their targets, we've included two additional dangerous capabilities. These two vulnerabilities allow for distributed denial-of-service (DDoS) execution and permission changes on VPN/ remote access gateways (CVE-2017-0177, Microsoft/ DDos and CVE-2019-11510, Pulse Secure/WebApp). Here is a straightforward, yet powerful, model to prioritize vulnerabilities, especially those associated with ransomware.



One interesting data note that we would like to highlight is that four vulnerabilities presented as outliers to our dataset from last year's report. They were published between 2007-2008, but we found them active in exploits during our research spanning 2010-2020.

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

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

Weaponized, Dangerous, & Trending

Last year's Ransomware report focused on 2010-2019 looking at CVEs tied to ransomware families. This year we re-examined this data with our extended team and partnership with CSW and also added focus on 2018-2020 trends. Changes due to COVID-19 aided threat actors, allowing them to spread their wings and find vulnerabilities that could be exploited moving up the 'application stack' to remote technology and software-as-a-service applications. While 2020 saw unabated cyber attacks on all industries, we wanted to understand the opportunities attracting these threat actors.

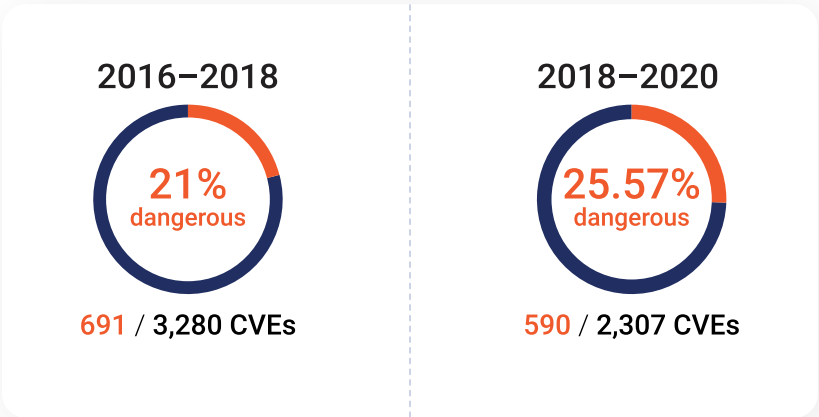
It's important to track the growth in ransomware risk by looking at the new CVEs each year, verifying if they have dangerous capabilities and mapping them to our research to understand if they are tied to ransomware families. This shows the growth in exposure points and gateways for ransomware to attack organizations. However, equally important is tracking the total number of CVEs that are trending and actively used in exploits. This number is not time bound and shows how ransomware families are leveraging a greater amount of older vulnerabilities in their arsenal year after year.

Growth in Weaponization

For the vulnerabilities that were published during 2018-2020 and comparing it to the previous two years, we saw an improvement in the percentage of vulnerabilities that became weaponized. Yet, 5% becoming weaponized is still a concern for organizations.

Growth in Dangerous Vulnerabilities (RCE/PE Capabilities)

Dangerous vulnerabilities have two characteristics, they have weaponized exploits and they have the capability of Remote Code Execution (RCE) or Privilege Escalation (PE) that significantly increases risk to an organization. While the amount of vulnerabilities that became weaponized decreased, the count of RCE/PE vulnerabilities increased. Over 25% of newly published CVEs, pose a greatly elevated risk factor due to RCE/PE capabilities.



Growth in Vulnerabilities Tied to Ransomware

While the other areas we researched looked at vulnerability capabilities, this section takes a different view, looking at our ransomware findings and the growing risk to organizations. Vulnerabilities tied to ransomware continue to grow in number. Our findings show that they will continue as along as the assets they target continue to persist. It's safe to say that once a vulnerability is tied to ransomware it should be considered an elevated risk to organizations, no matter what time frame it was first identified.

Looking at just vulnerabilities tied to ransomware, we saw growth of nearly 40%, in how families leverage the full spectrum of vulnerabilities available to them during 2018-2020 for their nefarious activities.

2016–2018

60 / 223 CVEs

2018–2020

89 / 223 CVEs

Growth in Trending/Active Exploits among Vulnerabilities Tied to Ransomware

Weaponized vulnerabilities and their dangerous exploit capabilities (RCE/PE) provide the macro-level context to evaluate increased risk to an organization. Comparing these same time periods, we see moderate growth in risk, 21% to 25.57%. However, when honing in on ransomware risk and the vulnerabilities tied to ransomware, the contribution of these two time periods shows a larger growth in risk exposure for organizations. 2018-2020 contributed to nearly 40% of the vulnerabilities we identified in this data set. **More concerning is that 66.29% of this data set are currency seen as trending with active exploits within our findings on ransomware families.**

This risk index highlights the growing ransomware exposure that cannot be addressed unless continuous ransomware threat-context can be applied to an organizations vulnerability management and prioritization program.

2016–2018

22 / 60 CVEs

2018–2020

59 / 89 CVEs

3

Analyzing Ransomware Vulnerabilities & Risk Factors

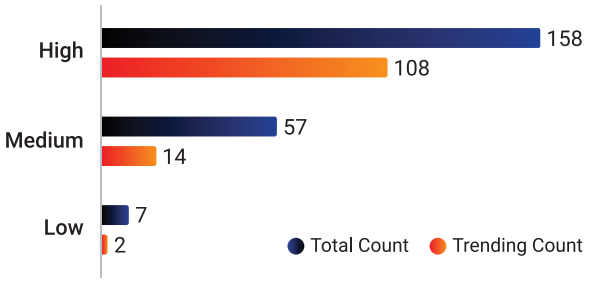
To categorize the adversarial risk of a vulnerability both CSW's database of CVE data, traits, and attack characteristics, **SecurIn Vulnerability Intelligence Quotient (VIQ) and RiskSense's Vulnerability Risk Rating (VRR)** are used. Together these analytics guided by security experts help define the most active threats. Collaborating and using threat intelligence, exploit validation, and field experience, dangerous vulnerabilities that are being actively used are discovered. This outcome provides the Trending category of vulnerabilities we reveal in this paper that elevates the risk this group poses to an organization.

Analysis of CVSS Scores & Severity Rating System

Relying only on CVSS severity scoring to prioritize vulnerabilities can be a bad idea. While CVSS is useful, its downfall is that it only looks at the individual vulnerability and has limited context on how adversaries can leverage them to infiltrate organizations or how active they are utilizing them in their threat campaigns.

Looking at the common CVSS v2 scoring across all of the 223 vulnerabilities tied to ransomware, we found 158 vulnerabilities with a CVSS v2 severity rating of High.

Vulnerabilities Tied to Ransomware with CVSS v2 Scoring (2010-2020)

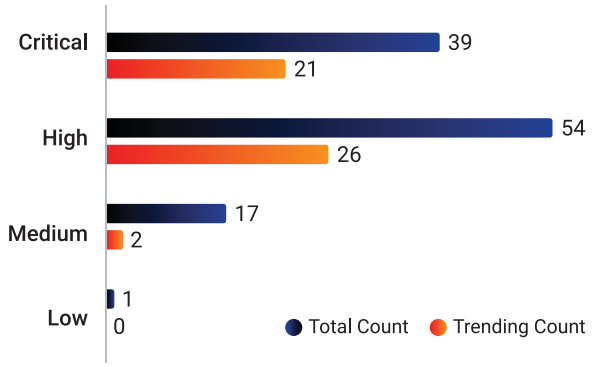


The relationship between trending and CVSS v2 scoring does not provide any direct correlation when it comes to vulnerabilities tied to ransomware. If standard practice was to prioritize remediation based on CVSS v2 High scoring CVEs during 2010-2020, only 158 out of 223 would be accounted for, leaving an exposure gap of just over 29% from unpatched vulnerabilities tied to ransomware.

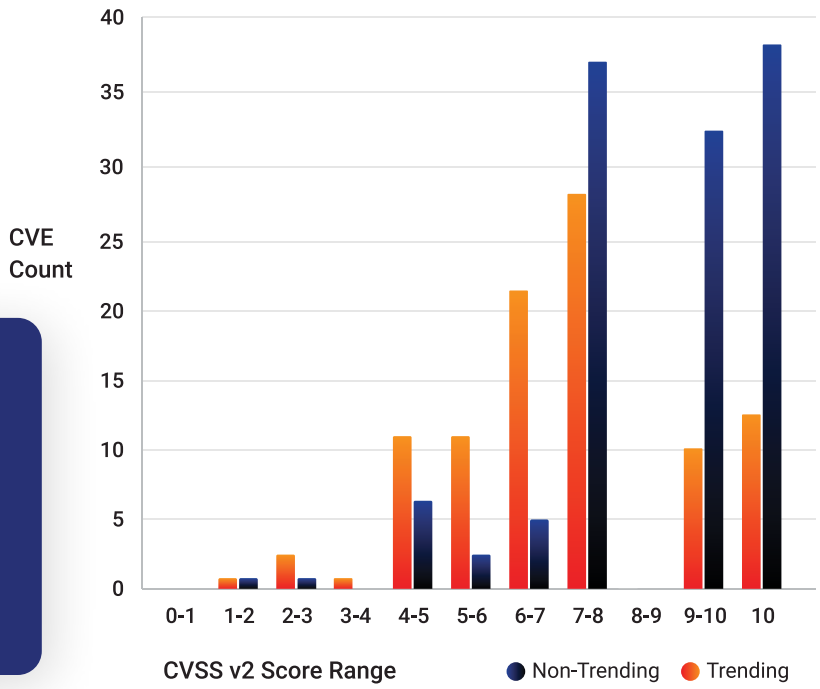
However, what's important is that from 2018-2020, using CVSS v3 scoring, if you were to patch only the Critical vulnerabilities, your coverage against ransomware would only be about 35% from the overall 111 vulnerabilities that have a CVSS v3 score. 91 CVEs tied to ransomware families trended (2018-2020) and only 21 CVEs rated Critical are a part of this list. If CVSS v3 Critical score is the benchmark for prioritization, then you would be fixing 23% of the entire trending CVEs and still be vulnerable to ransomware attack.

CVSS v2 and v3 scores can only be regarded as basic benchmarks for rating vulnerabilities, but when it comes to ransomware, they are not a good indicator for this type of threat risk. This shows that organizations need something more sophisticated that takes into account real-world threat context to help them prioritize their patching to minimize ransomware risk exposure.

Vulnerabilities Tied to Ransomware with CVSS v3 Scoring (2018-2020)



You can see the increase in CVEs tied to ransomware, all 223, and their CVSS v2 scores, yet the majority of those observed as being actively used by in-the-wild attacks and thus trending are clustered below the High scoring tier.



One CVE does not have a CVSS Score from the US NVD Listing, and interestingly, we know that it is used by ransomware families:

CVE-2019-8720

Low Scoring Vulnerabilities

Because low scoring vulnerabilities are deceptive and fly under the radar of patching priorities, we wanted to research what this means for ransomware exposure. We found 7 CVEs ranked as low looking at their CVSS v2 scores tied to ransomware. We also observed that 2 CVEs that, despite their Low scores, are in high demand among multiple ransomware families. CVE-2016-3298, with a CVSS v2 score of 3.2 and CVSS v3 score of 5.3, are tied to 36 ransomware families. CVE-2017-0213, with a CVSS v2 score of 1.9 and CVSS v3 score of 4.7, continues to be popular and is currently trending across 5 active ransomware families. Other vulnerabilities with CVSS v2 score of less than 8 are also a concern:

- There are 128 CVEs that belong in this category in our research from 2010-2020.
- 41% (53 out of 128) of these vulnerabilities had been observed and tied to active ransomware threats during the past decade.
- 35% (45 out of 128) are seen currently trending from 2018-2020.

Even though CVSS v3 altered their scoring methodology to look at impact we still find ransomware risk exposure even with this elevated scoring method:

- The number of vulnerabilities tied to ransomware, with CVSS v3 scores less than 8, is 49 in our research from 2010-2020.
- 32% (16 out of 49) of these vulnerabilities had been observed and tied to active threats during the past decade.
- 30% (15 out of 49) are trending during our current research period of 2018-2020.

Top 10 Low Scoring Vulnerabilities Tied to Ransomware (2018-2020)

CVE ID	Product Name	CVSS v2 Score	CVSS v3 Score
CVE-2017-0213	Microsoft	1.9	4.7
CVE-2016-3298	Microsoft	2.6	5.3
CVE-2013-2423	Oracle, Canonical, Fermilab, Gentoo, Red Hat, IBM, Mandriva, Amazon, Centos, Novell	4.3	N/A
CVE-2013-2618	Network-Weathermap	4.3	N/A
CVE-2013-3896	Microsoft	4.3	N/A
CVE-2013-7331	Microsoft	4.3	N/A
CVE-2017-0147	Microsoft	4.3	5.9
CVE-2009-0824	Slysoft	4.9	N/A
CVE-2010-0738	RedHat, HP, Juniper	5	N/A
CVE-2013-0431	Oracle, Novell, Fermilab, Amazon, Red Hat, IBM, Mandriva, Gentoo, Centos	5	N/A

Our data shows that ransomware risk cannot be managed by utilizing CVSS scoring. It also points to a systemic vulnerability management problem with ransomware families continuing to rely on the vulnerabilities that traditionally don't get priority when it comes to remediation.

Older Vulnerabilities

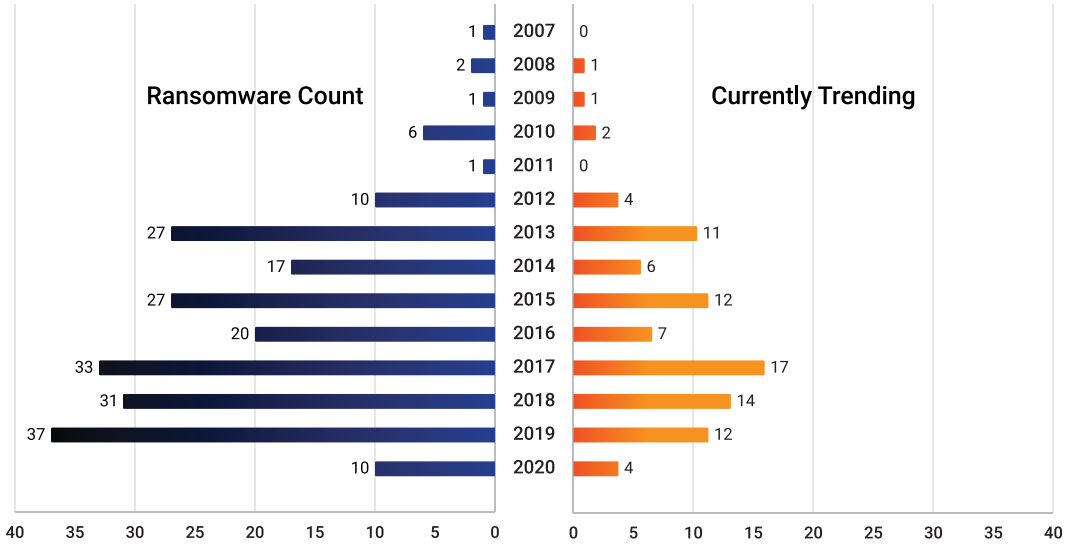
Most of the ransomware we saw found a gateway into the target network through the use of older vulnerabilities. For the purpose of this report, we have tagged any vulnerability that was discovered in 2019 or in previous years as old vulnerabilities.

The oldest trending vulnerability that we analyzed in this report was CVE-2007-1036, an RCE vulnerability associated with the Crypsam (SamSam) ransomware family. Two vulnerabilities from the year 2008 are also very active with ransomware, CVE-2008-2992 and CVE-2008-3431, with observations of them trending in 2017 and 2020, respectively.

213 CVEs (96%) out of 223 are older vulnerabilities. We also found that 120 of these vulnerabilities were actively used in ransomware threats that trended in the past decade, and 87 are currently trending (2018-2020). For those who have focused on their organizational exposure remediating only current vulnerabilities, continuing to put off older vulnerabilities, this should be a wake-up call.

Organizations that want to hone in on the vulnerabilities from 2017, 2018, and 2019 would do better with regards to ransomware exposure, as these years were the largest contributors, respectively adding 11, 8, and 10 CVEs tied to ransomware.

Vulnerabilities Tied to Ransomware and Trending by Year of NVD Publication (2018-2020)



Top 10 Older Vulnerabilities Most Active with Ransomware Families (2018-2020)

CVE ID	Ransomware Family			Ransomware Name		
CVE-2008-3431	Robinhood			Robinhood		
CVE-2009-0824	Robinhood			Robinhood		
CVE-2010-0738	Satan	Crypsam (Sam Sam)	SamSa	5ss5c DBGer	Lucky satan	SamSa SamSam
CVE-2010-0840	Reveton			Reveton		
CVE-2012-0158	Locky	Gimemo		Locky	Gimemo	
CVE-2012-0507	Cerber Crowti Crypwall Kovter Locky Reveton Sodinokibi Cryptesla Cryptohasyou Alma Locker AnteFrigus ASN1 BandarChor BartCrypt	Buran Cry CrypMIC CryptoMix Crypfort CryptoShield CTB-Locker Dxh26wam Erebus ERIS Globe FessLeak GandCrab GetCrypt	Goopic Matrix Mobef NanoLocker Nemty Paradise Philadelphia Princess Locker Crypradam Sage Spora Crypshed Cryptoluck	Cerber Crowti Crytowall Kovter Locky Reveton Sodinokibi Teslacrypt AlphaCrypt Cryptohasyou Alma Locker AnteFrigus ASN1 BandarChor	BartCrypt Buran Cry CrypMIC CryptoMix CryptoFortress CryptoShield CTB-Locker Dxh26wam Erebus ERIS Globe FessLeak GandCrab	GetCrypt Goopic Matrix Mobef NanoLocker Nemty Paradise Philadelphia Princess Locker Radamant Sage Spora Shade Troldesh YafunnLocker

Top 10 Older Vulnerabilities Most Active with Ransomware Families (2018-2020), continued

CVE ID	Ransomware Family	Ransomware Name
CVE-2012-1723	Cerber, Crypwall, NanoLocker, Urausy, CTB-Locker, Nemty, Cryptohasyou, Dxh26wam, Paradise, Alma Locker, Erebus, Philadelphia, AnteFrigus, ERIS, Princess Locker, ASN1, Globe, Crypradam, BandarChor, FessLeak, Reveton, BartCrypt, Flimrans, Sage, Buran, GandCrab, Sodinokibi, Cry, GetCrypt, Spora, CrypMIC, Goopic, Cryptesla, CryptoMix, Locky, Crypshed, Crypfort, Matrix, Cryptoluck, CryptoShield, Mobef	Cerber, CTB-Locker, Paradise, Urausy, Dxh26wam, Philadelphia, Cryptohasyou, Erebus, Princess Locker, Alma Locker, ERIS, Radamant, AnteFrigus, Globe, Reveton, ASN1, FessLeak, Sage, BandarChor, Flimrans, Sodinokibi, BartCrypt, GandCrab, Spora, Buran, GetCrypt, TeslaCrypt, Cry, Goopic, Alphacrypt, CrypMIC, Locky, Shade, CryptoMix, Matrix, Troldesh, CryptoFortress, Mobef, YafunnLocker, CryptoShield, NanoLocker, Cryptowall, Nemty
CVE-2012-4681	Lyposit, Reveton, Urausy	Lyposit, Reveton, Urausy
CVE-2013-0074	Sodinokibi, Crypwall, NanoLocker, Cryptohasyou, Waltrix, Nemty, Alma Locker, CTB-Locker, Paradise, Cryptesla, Dxh26wam, Philadelphia, AnteFrigus, Erebus, PizzaCrypts, ASN1, ERIS, Princess Locker, BandarChor, Globe, Crypradam, BartCrypt, FessLeak, Reveton, Better_call_saul, GandCrab, Sage, Buran, GetCrypt, Spora, Cerber, Goopic, TorrentLocker, Cry, CrypHydra, Crypshed, CrypBoss, JuicyLemon, UmbreCrypt, CrypMIC, Kovter, Cryptoluck, CryptoMix, Locky, Zepto, Crypfort, Matrix, CryptoShield, Mobef	Sodinokibi, CryptoShield, Mobef, Cryptohasyou, Cryptowall, NanoLocker, Alma Locker, Waltrix, Nemty, TeslaCrypt, CTB-Locker, Paradise, Alphacrypt, Dxh26wam, Philadelphia, AnteFrigus, Erebus, PizzaCrypts, ASN1, ERIS, Princess Locker, BandarChor, Globe, Radamant, BartCrypt, FessLeak, Reveton, Better_call_saul, GandCrab, Sage, Buran, GetCrypt, Spora, Cerber, Goopic, TorrentLocker, Cry, CrypHydra, Shade, CrypBoss, JuicyLemon, Troldesh, CrypMIC, Kovter, UmbreCrypt, CryptoMix, Locky, YafunnLocker, CryptoFortress, Matrix, Zepto
CVE-2013-0422	Reveton	Reveton

CWE Weaknesses Most Aligned for Ransomware Exploit

When we identified the large number of vulnerabilities tied to ransomware, we decided to investigate which Common Weakness Enumerations (CWEs) are being most abused.

We identified the top 5 CWEs by the highest count of associated CVEs (CWE-119, CWE-20, CWE-264, CWE-94, and CWE-200).

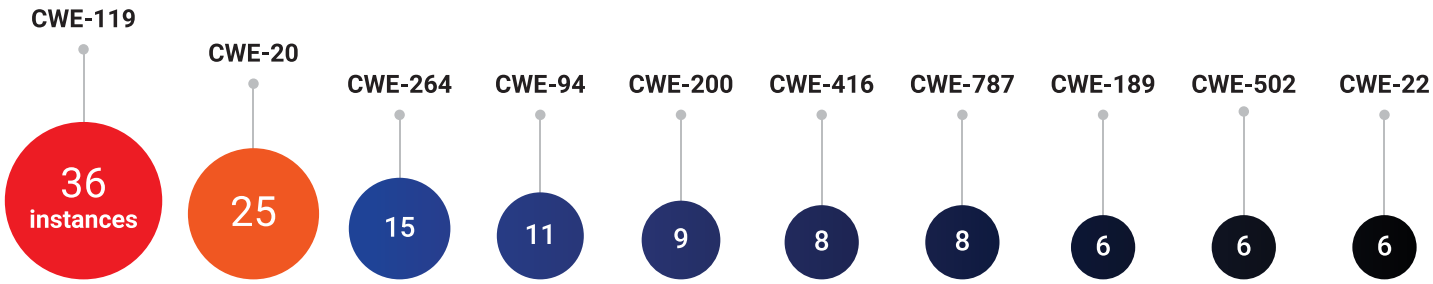
Of these, CWE-119, CWE-20, and CWE-94 are found in 2020 Top 25 Most Dangerous Software Weaknesses.

We found popular bug bounty programs offering researchers and bounty hunters huge payments to find vulnerabilities in these categories:

CWE-16	CWE-89	CWE-863
CWE-352	CWE-434	CWE-918
CWE-79	CWE-311	CWE-120
CWE-200	CWE-78	

This reinforces the fact that vulnerabilities within these weaknesses are sought out by threat actors systematically to weaponize.

Vulnerabilities Tied to Ransomware and Trending by Year of NVD Publication (2018-2020)



CWE	CWE Name	Number of instances
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	36
CWE-20	Improper Input Validation	25
CWE-264	Permissions, Privileges, and Access Controls	15
CWE-94	Improper Control of Generation of Code ('Code Injection')	11
CWE-200	Information Exposure	9
CWE-416	Use After Free	8
CWE-787	Out-of-bounds Write	8
CWE-189	Numeric Errors	6
CWE-502	Deserialization of Untrusted Data	6
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	6

4

Ransomware Families, APT Groups, & Exploit Kits

This year, we increased our research to grow our understanding about ransomware families. We identified 125 ransomware families who are delivering ransomware attacks utilizing 223 unique CVEs. The average number of CVEs per ransomware family is 17 CVEs in this year's report, while in our 2019 report the average was 4 CVEs per family.

Interestingly, we also observed that 42 ransomware families only use old vulnerabilities (2019 and earlier NVD publication dates) to target their victims, the oldest being from 2010.

A few prominent families (with their CVE count):

- **Crypwall** (66)
- **Locky** (64)
- **Cerber** (62)
- **Cryptesla** (56)
- **Reveton** (46)
- **Waltrix** (45)
- **Sodinokibi** (41)
- **Kovter** (40)
- **Cry** (37)
- **Philadelphia** (37)

Ransomware Family Details

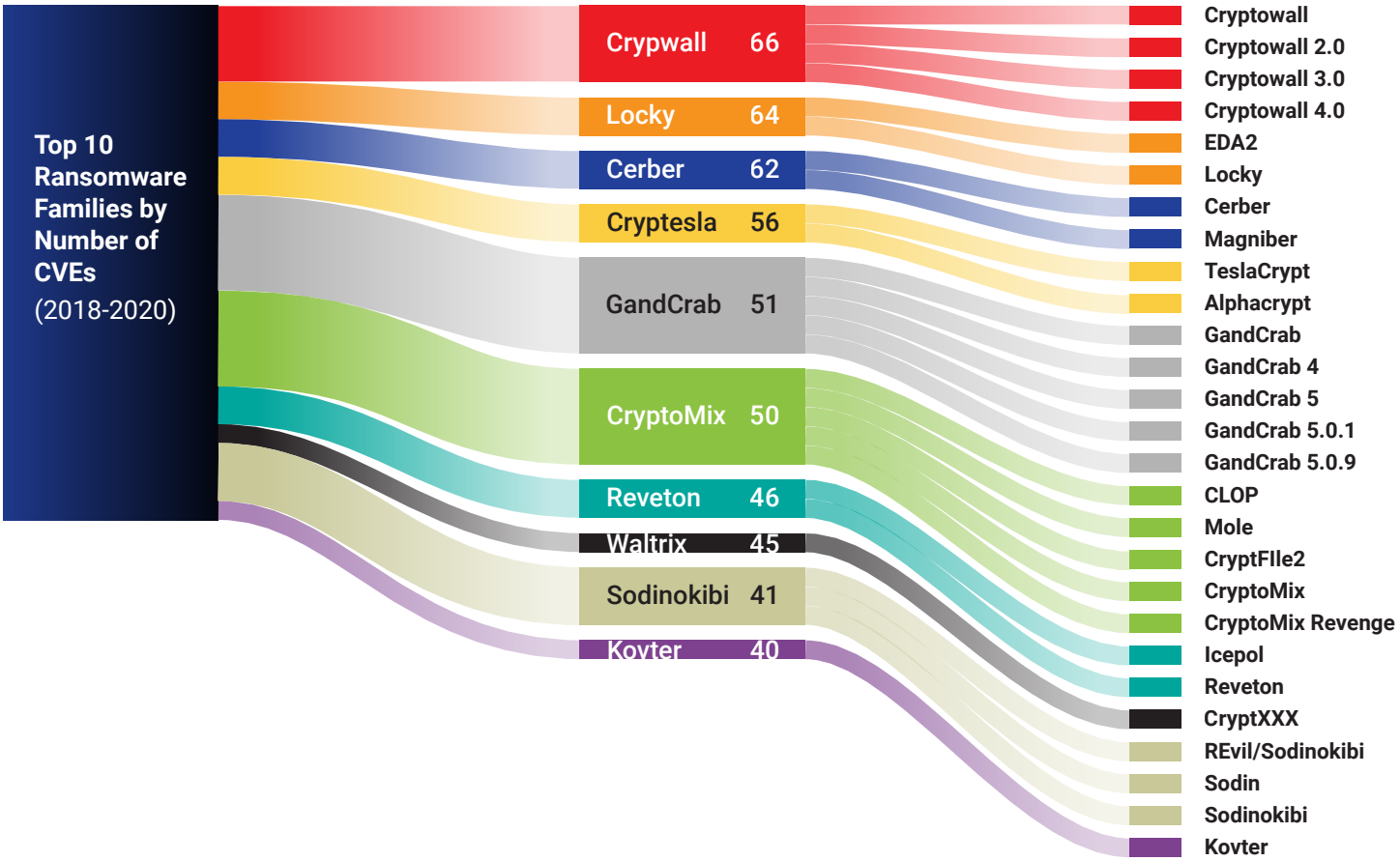
Ransomware Packages per Family

Let's take a closer look at the top three largest ransomware families based on the count of ransomware packages associated with each.

- **WannaCry:** The WannaCry ransomware family has 7 ransomware packages within its fold and targets their victims through 14 CVEs - all discovered in 2017. The WannaCry ransomware attack was a global cyberattack that took down businesses worldwide and was the first global ransomware attack that encrypted hundreds of thousands of computers in more than 150 countries within a matter of hours. It used the vulnerabilities inherent in Windows SMB protocol using NSA's classified hacking tools and the EternalBlue exploit to deliver the ransomware. Seven CVEs (CVE-2017-0146, CVE-2017-0143, CVE-2017-0213, CVE-2019-0803, CVE-2017-0145, CVE-2017-0144, and CVE-2017-0147) from this family trended from 2018-2020. Though the family is slow to update their arsenal with new vulnerabilities, they are still active and an interesting ransomware family to contend with.

- **GandCrab:** Ransomware families like GrandCrab have 6 ransomware packages using 51 CVEs within its fold. The vulnerabilities adopted by this family are mostly older CVEs but ages range from 2012 to 2019, we have not seen any additions in 2020.

- **CryptoMix:** Discovered in 2016, this ransomware family has 5 ransomware packages within its fold and 51 CVEs including CVE-2019-19781 that hit thousands of companies. This ransomware family has survived for more than four years and continues to add recent vulnerabilities into its arsenal, showing its adaptability and threat potential.



Ransomware Families and Growth in the Number of CVEs They Utilize

We observed the Crypwall ransomware family surge to the top of the list as one of the biggest ransomware families, with 4 ransomware strains tied to it and 66 CVEs within its fold. Locky is the second contender, with two ransomware packages and 64 vulnerabilities. Cerber has two ransomware strains and 62 CVEs tied to it. The 2019 report leader using the highest count of CVEs within their ransomware was Cerber with 17 CVEs. Cerber increased the number of CVEs they utilize by 27%.

Another observation is that 11 ransomware families seem to be actively adding newly discovered vulnerabilities to their fold. CryptoMix, a family with five ransomware strains is the leader in this category adopting 51 CVEs of which 19 vulnerabilities were found trending in 2018-2020.

Vulnerability Usage Across Multiple Families

In last year's report, we saw 12 ransomware families sharing 15 vulnerabilities to target their victims. This year, we observed this number greatly increase to 107 CVEs being leveraged by 113 ransomware families.

CVEs Shared Among Multiple Ransomware Families

CVE ID	Families	Vulnerable Element	CVSS v2	CVSS v3	VRR
CVE-2010-0188	Urausy Cryptohasyou Cerber CryptoMix Crypfort Crypwall CTB-Locker Locky NanoLocker Cryptesla Crypshed	Acrobat Reader Acrobat Rhel_extras Enterprise Linux Linux SUSE Linux Opensuse	9.3	N/A	10
CVE-2010-0738	satan Crypsam (SamSam) SamSa	JBoss Enterpise Application Platform Enterprise Linux Junos space Hp-ux	5	N/A	8.53
CVE-2010-1428	Crypsam (SamSam) SamSa	JBoss Enterpise Application Platform Enterprise Linux Junos space	5	N/A	6.16
CVE-2012-0158	Locky Gimemo	Office SQL Server Commerce server Visual Basic Office web components Biztalk server Visual foxpro	9.3	N/A	9.68

CVEs Shared Among Multiple Ransomware Families, continued

CVE ID	Families	Vulnerable Element	CVSS v2	CVSS v3	VRR
CVE-2012-0507	Cerber, Crowti, Crypwall, Kovter, Locky, Reveton, Sodinokibi, Cryptesla, Cryptohasyou, Alma Locker, AnteFrigus, ASN1, BandarChor, BartCrypt, Buran, Cry, CrypMIC, CryptoMix, Crypfort, CryptoShield, CTB-Locker, Dxh26wam, Erebus, ERIS, Globe, FessLeak, GandCrab, GetCrypt, Goopic, Matrix, Mobef, NanoLocker, Nemty, Paradise, Philadelphia, Princess Locker, Crypradam, Sage, Spora, Crypshed, Cryptoluck	JRE, Enterprise Linux, Rhel extras, Centos, Linux, Ubuntu Linux, Debian, Debian GNU/Linux, Debian GNU/kfreebsd, SUSE Linux, Java 1.6, Vcenter server, Debian Linux	10	N/A	10
CVE-2012-1710	Locky	Petya	Fusion middleware	7.5	N/A	7.86
CVE-2012-1723	Cerber, Urausy, Cryptohasyou, Alma Locker, AnteFrigus, ASN1, BandarChor, BartCrypt, Buran, Cry, CrypMIC, CryptoMix, Crypfort, CryptoShield, Crypwall, CTB-Locker, Dxh26wam, Erebus, ERIS, Globe, FessLeak, Flimrans, GandCrab, GetCrypt, Goopic, Locky, Matrix, Mobef, NanoLocker, Nemty, Paradise, Philadelphia, Princess Locker, Crypradam, Reveton, Sage, Sodinokibi, Spora, Cryptesla, Crypshed, Cryptoluck	JRE, Jdk, Debian, Debian GNU/Linux, Debian GNU/kfreebsd, Linux, Enterprise Linux, Centos, Ubuntu Linux, Java_1.6, SUSE Linux, Scientific Linux, Debian Linux, Opensuse, Vcenter server, Vcenter update manager	10	N/A	10
CVE-2012-4681	Lyposit, Reveton, Urausy	Jdk, Jre, Linux, Enterprise Linux, Centos, Freebsd, SUSE Linux, Opensuse, Scientific Linux	10	N/A	10
CVE-2012-5076	Reveton, Urausy	Jre, Jdk, Enterprise Linux, Linux, Centos, Ubuntu Linux, SUSE Linux, Esx, ESXi, Scientific Linux, Opensuse	10	N/A	10

APT Groups

Advanced Persistent Threats (APT) and ransomware association increases the power of this threat by several notches. These threats are called 'persistent' for a reason. The adversaries behind these threats are not solely motivated by monetary gains. APT Groups are seemingly well-funded, often by nation states who hire them to conduct deep targeted attacks. Their focus is on government, critical infrastructure, multinational organizations, and proprietary and sensitive information within pharma, key manufacturing entities, and the supply chain of their targets.

We are covering this trend because our research found ransomware also being used by APT groups. While these adversaries are not going to infect their target's network and demand ransom through bitcoins, it does show how ransomware can expedite a way into organizations.

We found 33 unique APT Groups using 65 ransomware as their arsenal to disrupt, spy, and gather intelligence from sensitive organizations. These APT Groups are largely associated with nation states such as Russia, China, Iran, North Korea, Germany, South Korea, and Nigeria.

Russian APT Groups such as APT28, Doppel Spider, Gold Southfield etc. are associated with notorious ransomware strains such as Revil, Cerber, Sodinokibi, Petya, Snake etc. Second in line are Chinese APT groups such as Wizard Spider, Rocke, Naikon, APT40, and APT41 that deploy Maze, Gimemo, Xbash, and Ryuk to disrupt critical industries.

We also noticed that certain APT groups focus exclusively on certain industries. For example groups like Wizard Spider use ransomware like Ryuk rather efficiently targeting hospitals and organizations associated with healthcare and pharma.

Most APT groups go by many aliases or by the primary ransomware strain. For example, Sandworm APT Group is also known as TeleBots, Sandworm, or BlackEnergy. While we are sharing this high-level research, there are deeper complexities of these groups that are evolving and new capabilities starting to come to light. This report only shows the trends as we begin to map these relationships.

Here is a list of APT groups, the ransomware strains they use, and their alleged nation state sponsors.

APT Groups using Ransomware Strains Grouped by Nation Association (2018-2020)

APT Group	Ransomware Name			Nation State
AnonSec	Maze			–
Anonymous	Maze			–
APT 1	Maze			China
APT10	Gimemo			China
APT28	Golang	Petya		Russia
APT29	Maze			–
APT 37	Erebus			South Korea
APT40	Gimemo			China
APT 41	Maze			China
Boss Spider	SamSam			Iran
Cycldek	Gimemo			China
Doppel Spider	DoppelPaymer			Russia
Dungeon Spider	Locky			Russia
Equation Group	NotPetya	WannaCry		United States
FIN11	CLOP			–
FIN6	LockerGoga	Maze	Ryuk	–
GOLD SOUTHFIELD	REvil/Sodinokibi	Sodin	Sodinokibi	Russia
Lazarus Group	Hermes	Hermes 2.1	WannaCry	North Korea
Naikon	Gimemo			China
PARINACOTA	Dharma			–
Pinchy Spider	GandCrab GandCrab 5 GandCrab 5.0.1	GandCrab 5.0.9 REvil/Sodinokibi	Sodin Sodinokibi	Russia
RATicate	Lokibot			–
Rocke	Xbash			China
Sandworm Team	Bad Rabbit NotPetya PetrWrap	Petya Pnyetya	WanaCrypt0r WannaCry	Russia
Shadow Brokers	Petya			–
SilverTerrier	Lokibot	Pony		Nigeria
SWEED	Lokibot			–
TA2101	Buran	Maze		Germany
TA505	Bitpaymer CLOP CryptFIle2 CryptoMix	CryptoLocker DoppelPaymer Globe Imposter	Locky Philadelphia Pony	Russia
TA530	CryptoWall			–
Turla	Snake			Russia
Wizard Spider	Ryuk			China
Zombie Spider	Cerber	Shade (Troldesh)		Russia

Exploit Kits

We also saw ransomware families leverage common exploit kits. Exploit kits are automated tools used by hackers to exploit a vulnerability and then deliver malware or ransomware payloads. Typical exploit kits today are loaded with exploits that target common software such as Adobe, Flash, Java, Microsoft Silverlight, etc. Essentially, these are packaged executables and a build of layered vulnerability attacks providing all the tools needed to target and mount an attack, or used to test the exploitability of an organization by penetration testing teams.

We found 29 exploit kits used across 84 ransomware strains. The top 5 most commonly included exploit kits in this list are:

- **RIG Exploit Kit**
- **Nuclear Exploit Kit**
- **Angler Exploit Kit**
- **Neutrino Exploit Kit**
- **Fallout Exploit Kit**
- **EternalBlue Exploit Kit**

Our research observed

Fallout and **RIG**

exploit kits available on a monthly subscription basis in many of the ransomware-as-a-service websites.

Ransomware Strains and Exploit Kits (2018-2020)

Ransomware Name	Exploit Kit Count	Exploit Kits Used		
CryptoWall	8	Infinity Nuclear Fiesta	Neutrino Himan Magnitude	RIG pseudo-Darkleech
Locky	7	Bizarro Sundown		
TeslaCrypt	6	Nuclear		
Cerber	5	Nuclear Neutrino	Magnitude Sundown	RIG
GandCrab	4	SofosFO/Stamp		
Reveton	4	Cool		
BandarChor	3	Empire Pack	Neutrino	RIG
Better_call_saul	3	Darkleech	pseudo-Darkleech	Angler
CryptFIle2	3	Nuclear	Neutrino	RIG
CryptXXX	3	Neutrino	pseudo-Darkleech	Angler

5 Ransomware as a Service

Until a few years ago, only groups with knowledge about security and with coding expertise could launch and mount complex cyber attacks. No longer is that a requirement now that ransomware as a service (RaaS) has become almost mainstream.

Ransomware as a service has enabled just about anybody to launch ransomware attacks without getting creative with code or have deep security expertise. The relative ease of this process has attracted many malicious actors. Of all the forms of cyber attacks that exist today, the ransomware attack is the most lucrative. This is a disturbing trend, monetizing the tools that enable ransomware, along with the escalating extortion tactics deployed by ransomware families.

As we previously discussed, there is a crossover with many of these sites we found in our research where exploit kits (Fallout and RIG exploit kits) are options in many ransomware-as-a-service websites. It can be reasonably assumed that the ease of subscription to these exploit kits is enabling ransomware such as Cryptowall, Locky, and TeslaCrypt to use as many as eight, seven, and six exploit kits, respectively, to mount their attacks.

Fast Enablement with No Overhead

Ransomware as a service works pretty much in the same way as any other SaaS model selling services and product subscriptions. You can pay and procure ransomware builders, malware strains, hire a way to hack popular social media sites or build custom ransomware strains. We've found these types of services brazenly describe how their package can be utilized and some even taut association with some of the biggest cyber crime attacks such as Petya or WannaCry as examples to sell their wares.

One can create an account on these sites, check subscriptions for previously bought packages, and renew them easily. Each purchase comes with detailed instructions on how to deploy the payload, making it extremely easy for anybody to launch an attack. These sites also have features such as FAQ, customer service, and quick help, making it easy for their nefarious customers every step of the way.

[PACKAGE #ELITE] - 12-MONTH C2 Dashboard (RaaS) - Price: 1900 USD

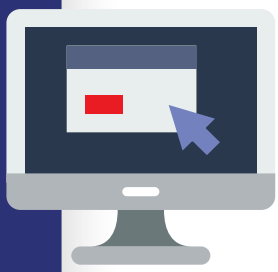
- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- Stub #: 12 x 100% private FUD stubs
- Platform: Windows (both x86 and x64)
- Duration: 12 Months access to Darknet C2 Dashboard (to receive the AES keys from Clients)
- Fees: We take NO FEES from your Clients
- Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer
- IP Tracking: Yes
- Offline Encryption: Yes
- Support: Yes
- Real-Time Client Manager: Yes
- Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (FREE)
- Paid Add-On (Clone): A fresh FUD RANION copy with the same setup information (FREE)
- Paid Add-On (Crypter): Additional Crypter/Obfuscator + unique onion address (FREE)
- Paid Add-On (Unkillable Process): Unkillable Process aka BSOD (FREE)
- Free Add-On: optional file types to encrypt (for all encrypted file types see FAQ)
- Free Add-On: optional Client's sub-banner in your language (already present en, ru, de, fr, es, it, nl, fas, za)

A typical ransomware package comes with many free add-ons and customization features, not to mention fancy names and hashtags for products.

Customizations such as changing ransom amounts based on how an attack proceeds along with access to a complete command center to monitor the attacks are common. We've even seen ransom payment pages and links providing just about anything that an attacker needs. As with anything these days, the customers of these services are encouraged to leave a rating of how well the service provided what they were looking for.

While not comprehensive, we were able to observe the following ransomware available in a sampling of Dark Web sites advertising ransomware as a service.

Ryuk	PrincessLocker
Bitpaymer	satan
Gandcrab	Thanos
Hermes	sodinokibi
Revil	Netwalker
Dharma	Cerber
egregor	Nefilim
Nempty	WannaCry



Product Categories with Expanding Ransomware Risk

Trends that we've been tracking since we released last year's report was that ransomware is moving towards targets at the application layer, and towards products heavily utilized due to COVID-19 such as VPN, access gateways, and collaboration tools. One of the largest new targets we observed is the one area that every organization relies on in case of a ransomware attack, their back-up solutions. Therefore, we cross-referenced the products into broad categories to identify the trends that are shaping up.

Application Vulnerabilities

Web & application development still is one of the most strategic activities for most organizations. It is no surprise that these web facing applications and most popular used frameworks are a target for ransomware. RiskSense research previously identified Web and Application Framework Vulnerabilities, this report looks at which ones have been seen tied to ransomware.

- We found 18 unique CVEs tied to ransomware when cross-referencing this research
- The products targeted include: WordPress, Struts, Java, PHP, Drupal, and ASP.net

SaaS Applications

We saw ransomware targeting 12 SaaS products with 47 vulnerabilities. We also found that 19 of these CVEs are trending between 2018-2020. Top products with the maximum number of vulnerabilities would be Apple's iCloud, Microsoft Outlook 365, HP's Application Lifecycle management, Oracle's Fusion Middleware, Adobe's Adobe Air, IBM's Lotus Domino, and Notes.

With the usage of SaaS products increasing, we predict that threat actors will seek out vulnerabilities inherent in these applications and weaponize them systematically.

Open Source Vulnerabilities

RiskSense research previously identified the risk from Open Source Vulnerabilities, this report looks at this list and cross references with the 223 CVEs we found tied to ransomware. 19 of these vulnerabilities exist within the Open Source category and have been tied to ransomware. These CVEs were found to exist among 7 Open Source products such as **Jenkins, MySQL, OpenStack, Tomcat, Elasticsearch, OpenShift, and JBoss**.

Of concern here is that Open Source allows developers to quickly deploy their products and it allows for quick re-use and sharing within communities with libraries. This also makes them a good target for ransomware utilization allowing these threats to have broad reaching implications.

VPN/Gateway/Collaboration Vulnerabilities

When COVID-19 pandemic induced a world-wide lock down, Cyber Security Works released a series of ten reports, Cyber Risk in Working Remotely. This research analyzed the vulnerabilities that exist in popular applications and technologies used today for remote work and collaboration. We cross referenced the CVEs listed in these reports against those found tied to ransomware and found that many devices and applications used by the world's remote workforce have vulnerabilities that open the door to ransomware attacks. Notably, Pulse Secure, Sonicwall's Secure Mobile Access, Microsoft Host Integration Server, Mitel Open Integration Gateway, Citrix Netscaler, Sophos XG Firewall, and F5's Big IP firewall have the maximum number of CVEs linked to ransomware.

We also analyzed products such as online conference tools, remote desktops, databases, and web proxies and found them vulnerable to ransomware attacks.

- Microsoft's popular online conference tool Microsoft Live Meeting has a vulnerability (CVE-2015-1671) that is linked to 14 ransomware families.
- 12 Firewall products are exposed with seven CVEs tied to ransomware:
  - Citirx: Netscaler Access Gateway Firmware
  - Citrix: Application Delivery Controller Firmware
  - Citrix: Application Delivery Controller
  - Citrix: Netscaler Gateway Firmware
  - Citrix: Netscaler Gateway
  - Citrix: Gateway Firmware
  - Citrix: Gateway
  - F5: Big IP Advanced Firewall Manager
  - F5: BIg IP Advanced Web Application Firewall
  - Mitel: Mivoice Border Gateway
  - SonicWall: Web Application Firewall
  - Sophos: XG Firewall
- Three Gateway products (Microsoft Host Integration Server, Mitel Open Integration Server, and SonicWall Secure mobile access) and one VPN, notably Pulse Secure Connect, have vulnerabilities that provide a gateway to ransomware.

Backup & Storage Vulnerabilities

We found 12 backup storage devices with 22 vulnerabilities tied to ransomware. These include popular products such as Apple's iCloud, Citrix's Xenserver, Microsoft's Sharepoint, Netapp's Cloud Backup, and RedHat's JBoss Data Grid. Five vulnerabilities (CVE-2015-1641, CVE-2017-0199, CVE-2018-15982, CVE-2018-4878, and CVE-2015-5122) that are present in these products were actively exploited between 2018-2020.

When we looked at the CWE information, we found the following weakness categories appearing multiple times: CWE-79, CWE-416, and CWE-119. Vulnerabilities that belong to these CWEs exist in these popular backup storage devices. We also looked at the CVEs that were actively exploited in 2018-2020 and found that they belong to these CWEs, CWE-39 and CWE-416.

Product Categories & CVE Count

Product Type	Product Count	CVE Count	Top Product Names		Trending (2018 - 2020)
Backup Storage	12	22	iCloud RedHat Enterprise Linux Server NetApp Storage Automation Store		5
Online Conference	2	2	Microsoft Live Meeting Selligent		2
Database	3	4	Apache ignite Elasticsearch Microsoft SQL Server		2
Gateway	3	2	Microsoft Host Integration Server		0
VPN	1	1	Pulse Secure - Pulse Connect Secure		1
Firewall	12	7	Citrix Netscaler Citrix Gateway firmware F5 Big IP - Advanced web app firewall SonicWall web application firewall Sophos XG Firewall		3
SaaS Products	12	47	Adobe-Air iCloud Outlook 365	ibm - Lotus-domino notes oracle fusion middleware	19
Open Source	8	17	JBoss MySQL Jenkins	Openstack Elasticsearch	8
Web Application	6	18	WordPress Struts	Drupal Java	11

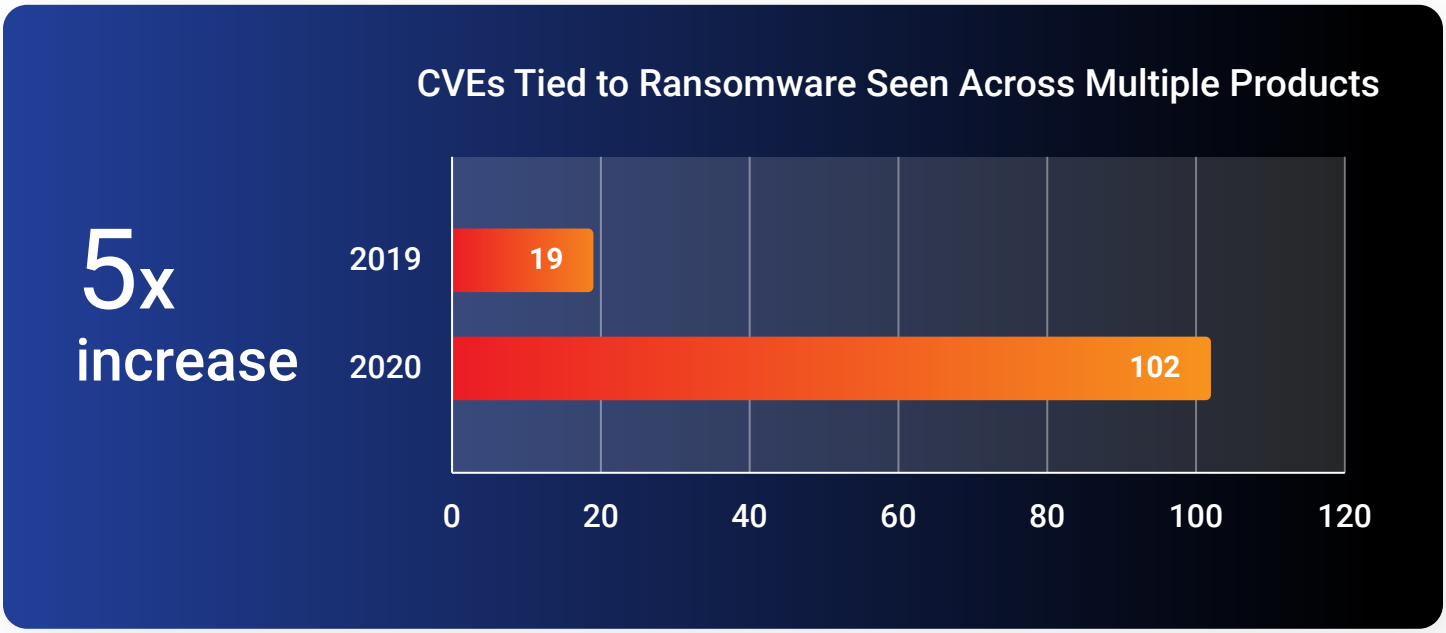
Ransomware Vulnerabilities Impacting Multiple Products

This is a trend we called out in the previous year's report. We noticed 19 CVEs, 17 of them trending vulnerabilities, found across multiple vendors and products. We showed how software components are often reused across multiple products and even vendors, making it hard to track these exposure points.

This year we found 102 CVEs tied to ransomware spread across multiple vendors and products, exacerbating this patching problem. This trend is part of the changing dynamics of today's attack surface that threat actors love to take advantage of.

A good example of this problem is Intel's AtomC processor that has a Speculative Store Bypass vulnerability (CVE-2018-3639) that is now present in 25 products & vendors (Microsoft, Canonical, Novell, Debian Gentoo, and many others).

Two vulnerabilities present in Linux language vulnerabilities CVE-2018-5391 (present in Linux kernel, versions 3.9+) and CVE-2014-3153 (Linux Kernel version 3.14) have been found affecting products such as Canonical, Novell, Huawei, Debian, RedHat, Centos, Oracle, Amazon, Fermilab, VMware, Virtuozzo, Arista, Juniper, F5, Slackware, Cisco, CPE, Palo Alto Network, Linux, Fedora Project, SUSE, Mandriva, etc.



6 Summary

Ransomware threats are no more a pesky headache as they continue to mature. The growing risk is how many ransomware attacks do not need deep technical knowledge or expertise - thanks to the emergence of ransomware as a service.

While we looked at various angles of ransomware through the lens of threat and vulnerability management the growth in vulnerabilities tied to ransomware we believe will continue. The other concerning aspect is the growth of ransomware families, the expanding strains of ransomware they are creating, and the increase in use of weaponized vulnerabilities among them.

The way to defend against this threat is elevating cyber hygiene and continuous risk-based vulnerability management that provides active threat-context about ransomware. Today this research is the only source for organizations to quickly understand their attack surface exposure and what is contributing to the growth in ransomware attacks organizations are experiencing.

> While server and operating systems were the original targets, ransomware threats are moving up the stack to applications - SaaS, Web and Application frameworks, and of course Open Source."
>
> **– Srinivas Mukkamala**
> **Founder & CEO of RiskSense**

Risk-based vulnerability management continues to evolve and we've shown that traditional ways of assessing CVE risk, using CVSS scoring and vulnerability age, when it comes to ransomware is not helpful.

> Attack Surface Management (ASM) is all about organizations reducing their exposure to ransomware. The number of vulnerabilities associated with ransomware have quadrupled in 2020 which means organizations need to view vulnerabilities from a ransomware context and patch them continuously."
>
> **– Ram Swaroop**
> **President & Co-founder,**
> **Cyber Security Works**

The landscape and tactics used by ransomware families and adversaries behind them are quickly changing and we provide this research as a way to educate and help organizations understand this evolving threat.

7 Report Methodology

The information in this report is based on data gathered from a variety of sources including RiskSense & CSW's proprietary data, publicly available threat databases, as well as RiskSense & CSW threat researchers and penetration testing teams.

We hope this research can serve as a starting point for organizations wishing to take a risk-based approach to ransomware exposure to prioritize patching to secure their enterprise and reduce their attack surface. Simply put, most organizations are inundated with more vulnerabilities than they can patch, so we wanted to provide the various perspectives and details we uncovered about ransomware to shed light on the trends and key findings to help manage their vulnerability risk backed by research.

- **Our Focus:** We focused on vulnerabilities that came into existence between 2010 to 2020 and tracked their trending dates and their associations with ransomware and families, unless there is a specific callout to older vulnerabilities. We extensively analyzed the vulnerabilities that trended in the past two years (2018-2020) and also identified those CVEs and trends that are of interest that we observed during the 2020 calendar year
- **Definitions:** All through the report, you will notice that we use the words 'trending' and 'actively exploited'. They are distinctly different in what we wish to convey with regards to this report
- **Actively Exploited:** Any CVE that has been used to launch ransomware attacks in the past is defined as being tied to active ransomware exploits during the specified time period
- **Trending:** Any CVE that is seen within active ransomware exploit in the most recent time period, mostly from (2018-2020), or when we are specifically calling out 2020 activities

RiskSense Vulnerability Risk Rating

Vulnerability Risk Rating (VRR) is designed to decipher cybersecurity risk from the widest angle possible, using an algorithm that intelligently separates and elevates the riskiest weaknesses. It takes in the highest fidelity vulnerability and threat data and leverages our deep expertise providing human validation of exploits and exploit impact.

Vulnerability exposure is more than just assessing IT and cloud infrastructure; it also includes the applications and web services critical to digital business. Across infrastructure and applications, diverse types of data are now at play from the multitude of scanners, tools, and sources that deliver vulnerability findings and weaknesses. A fundamental step in being able to express adversarial risk is to normalize this data, bringing together the impact a vulnerability poses, enriched with threat context and trending exploits to understand the likelihood of it being exploited. Doing so allows each vulnerability to be quantified with a risk rating and be prioritized accounting for its exposure potential. The outcome of VRR is that it provides a current view of adversarial risk against a CVE or CWE.

RiskSense Risk-Based Vulnerability Management platform includes the continuous VRR assessment of all CVE findings. Included with this product is our unique Ransomware risk dashboard, automatically delivering the correlation of ransomware vulnerability exposure, prioritizing which findings need immediate action and the tools to enable the fastest path toward remediation. For more information, contact info@risksense.com.

CSW's SecurIn Vulnerability Intelligence Quotient

CSW's team of threat hunters started this exercise with a goal of creating a database that would contain updated and accurate information about ransomwares and the vulnerabilities that are used as a gateway. We collated this information from a few trusted sources and used RiskSense VRR analysis to cross-reference the data that we gathered.

Our goal in building Vulnerability Intelligence Quotient (VIQ) is to be a single point of reference where ransomware is concerned and provide companies, ransomware survivors, high-value entities, and vulnerable organizations with reliable data that would help protect them from ransomware attacks.

This year, our team took into account all the CVEs that have been added to NVD from 2010 to 2020 and labeled them using an algorithm-based approach. Next, our team of threat hunters examined these weaponized CVEs and mapped their connection to ransomware, ransomware families, APT Groups, and Exploit Kits. Next, we examined how many of these vulnerabilities trended in the past two years and were abused extensively in 2020 and came up with an exhaustive list of CVEs.

96% of the vulnerabilities that we examined for this report are old vulnerabilities, and CVSS v3 scores for 112 CVEs are not available. Therefore, for most parts of the report, we have used CVSS v2 scores to assess the severity of the vulnerabilities, and wherever the ratings are available, we have added context from CVSS v3 scores.

The sheer size of the CVEs tied to ransomware families and the unabated attacks on highly vulnerable organizations tells us that ransomware research can't be an annual affair anymore. This needs to be undertaken on a month-on-month or at least on a quarterly basis. With the help of CSW's extensive ransomware database, we will release many supplemental reports that would shed more light on the ransomware attack vectors and the vulnerabilities they choose as a gateway.

SecurIn's VIQ is one among the many products that CSW will be launching in 2021. VIQ is a dynamic database of vulnerabilities mapped to threats, exploits, ransomware, exploit kits, APT groups, etc. that would be soon available on a subscription basis. If you are interested in this product, contact data@cybersecurityworks.com for more information.

RiskSense®, Inc. provides risk-based vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated penetration testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense

+1 844.234.RISK | +1 505.217.9422
www.risksense.com

CSW is a cybersecurity services company focused on attack surface management and penetration testing as a service. Our innovation in vulnerability and exploit research led us to discover 45+ zero days in popular products such as Oracle, D-Link, WSO2, Thembay, Zoho, etc., among others. We became a CVE Numbering Authority to enable thousands of bug bounty hunters and play a critical role in the global effort of vulnerability management. As an acknowledged leader in vulnerability research and analysis, CSW is ahead of the game, helping organizations worldwide to secure their business from ever-evolving threats. For more information, visit www.cybsercurityworks.com or follow us on LinkedIn and Twitter at @CswWorks

www.cybersecurityworks.com