SPOTLIGHT

RISKSENSE | CSW Cyber SecurityWorks

Ransomware

Through the Lens of Threat and Vulnerability Management

Index Update Q1 2021

2021

1 Introduction

Since the publication of the RiskSense and Cyber Security Works (CSW) Ransomware Spotlight Report in early 2021, the surge in ransomware exploits continues. This Ransomware Index compares data from our last report (published in February 2021) with new and emerging ransomware information discovered up to the end of this quarter (March 2021) to evaluate escalating threats. We aim to provide organizations with insight into the trends and growth of ransomware from the perspectives of threat and vulnerability management.

FOCUS	PREVIOUSLY REPORTED	NEW TOTALS	Q1 '21 CHANGE
CVEs Associated with Ransomware	223	260	16.6% Increase
Low Scoring CVEs Tied to Ransomware *CVSS v2 score less than 8	128	153	19.5% Increase
Active Trending Exploits Used with Ransomware	124	132	6.45% Increase
Number of Ransomware Families	125	140	12% increase
Exploit Kits Used by Ransomware	29	32	10.3% increase
Number of APT Groups Associated with Ransomware	33	34	3% increase
Old Vulnerabilities Associated with Ransomware	213* *2019 and earlier	252* *2020 and earlier	18.3% increase
CWEs	48	50	4.2% increase
Vulnerable Vendors	84	96	14.3% increase
Vulnerable Products	666	722	8.4% increase

2 Index Findings

17% Increase in CVEs Associated with Ransomware

223 vulnerabilities enabling ransomware attacks were listed in our 2019-2020 report. In one year, there has been a steady 4x increase in vulnerabilities.

Today, the total count of vulnerabilities tied to ransomware has gone up from 223 to 260 CVEs, recording a 17% increase in CVEs associated with ransomware within Q1 2021.

- 37 additional vulnerabilities were found to be used by malicious agents as attack vectors for ransomware.
- 8 of these vulnerabilities were published in 2021 and were quickly adopted into ransomware families' arsenals.

20% Increase in Low Scoring Vulnerabilities Tied to Ransomware

Low scoring vulnerabilities tend to fly under the radar and are often not prioritized for remediation. In our previous report, we identified 128 vulnerabilities with low CVSS scores*. In this quarter, we have identified 25 more vulnerabilities, increasing the count from 128 to 153.

* CVSS v2 score less than 8

18% Increase in Old Vulnerabilities Linked to Ransomware

Old still continues to be gold for ransomware. While the previous report considered CVEs identified till 2019 as old, the quarterly update extends the list to include CVEs discovered in 2020. With this, the count of old vulnerabilities tied to ransomware increases from 213 to 252, which comprises 97% of the total CVE count (as of March 2021).

Year	2020 Dec Count	Q1 2021 Count
2007	1	1
2008	2	2
2009	1	1
2010	6	6
2011	1	1
2012	10	10
2013	**27**	**28**
2014	17	17
2015	**27**	**28**
2016	20	20
2017	**33**	**35**
2018	**31**	**40**
2019	**37**	**46**
2020	**10**	**17**
2021	TBD	8
Grand Total	223	260

Greater than 6% Increase in Active Trending Exploits Used by Ransomware

In our earlier report, we identified 124 CVEs that were weaponized and trending in the wild from 2018 to 2020. Within a span of three months, there has been a 6.45% increase in active exploits used with ransomware attacks, taking the revised count to 132.

Ransomware Families Growing Dangerously Fast

Our last report recorded the growth of 18 new ransomware families between 2019 and 2020. In the past quarter, we have identified 15 new families, bringing the total count to 140 from 125. This is an alarming growth trend in a span of just three months.

- 13 of these families are connected to just one CVE each.
- DearCry is tied to 4 CVEs, all published in 2021; two of these CVEs are already on our active exploit trending list, showing how fast threat actors are adding weaponized vulnerabilities to their armory.
- BigBossHorse ransomware is tied to a newly trending 2020 vulnerability.
- The Sekhmet ransomware family uses CVEs from 2018, 2019, and 2020 and is actively adding more vulnerabilities to its arsenal.
- UIWIX is a new ransomware family that uses six CVEs from 2017. This re-emphasizes our insight that old is gold, as old vulnerabilities are still being actively used to mount ransomware attacks.
- Ryuk added five CVEs to its arsenal, bringing the total to 19 since our last report.

Darkside Ransomware - a newly identified ransomware attacked a major US fuel pipeline on May 7, 2021 using two vulnerabilities **(CVE-2019-5544 and CVE-2020-3992)** that we identified earlier this year.

Increase in Exploit Kits Used by Ransomware

We had reported the existence of 29 exploit kits in our previous report. Now, we have found three new exploit kits:

- EternalRomance Exploit Kit
- LCG Kit Exploit Kit
- Sibhost Exploit Kit

These kits were found associated with ransomware families such as Bad Rabbit, Zemblax from the Jigsaw Ransomware family, and the Urausy Ransomware family, respectively.

Increase in APT and Ransomware Association

Our research uncovered new ransomware associations to the APT group: Viking Spider in Q1 2021. Interestingly, the Viking Spider has been found exploiting an older CVE (CVE-2017-0213).

Notable Movers and Shakers (in terms of CVEs and Ransomware)

Eight newly published vulnerabilities discovered in 2021 have quickly become associated with DearCry, Black Kingdom, and CryptoMix ransomware!

> What's more interesting is that CVE-2021-26855 and CVE-2021-27065 became weaponized with an exploit that was associated with ransomware, and started to trend in the wild within eight days of their discovery!

Products, Vendor and Sectors Affected

In the first quarter of 2021, we found that 30 vendors had contributed 68 vulnerable products susceptible to ransomware. Of this, 12 vendors, namely, Accellion, Fortinet, Wordpress, Dasannetworks, Cpuid, Cpe, Asus, Mikrotik, x.org, Gnu, Openslp, and Nvidia, are new additions. A total of 111 CVEs were identified as impacting multiple vendors and products, showing a 9% increase from 2020.

When we analyzed broad product categories, we found that operating systems had the most number of ransomware associations and were linked to 10 CVEs and 86 products. Virtualization platforms landed the second spot with 17 products, followed by remote desktop apps and mail servers with 10 products each.

Product Type	CVE Count	No. of Products Affected
OS	10	86
Virtualization Platform	2	17
Remote Desktop App	5	10
Mail Server	5	10
Router	5	8
Secure File Transfer	5	5

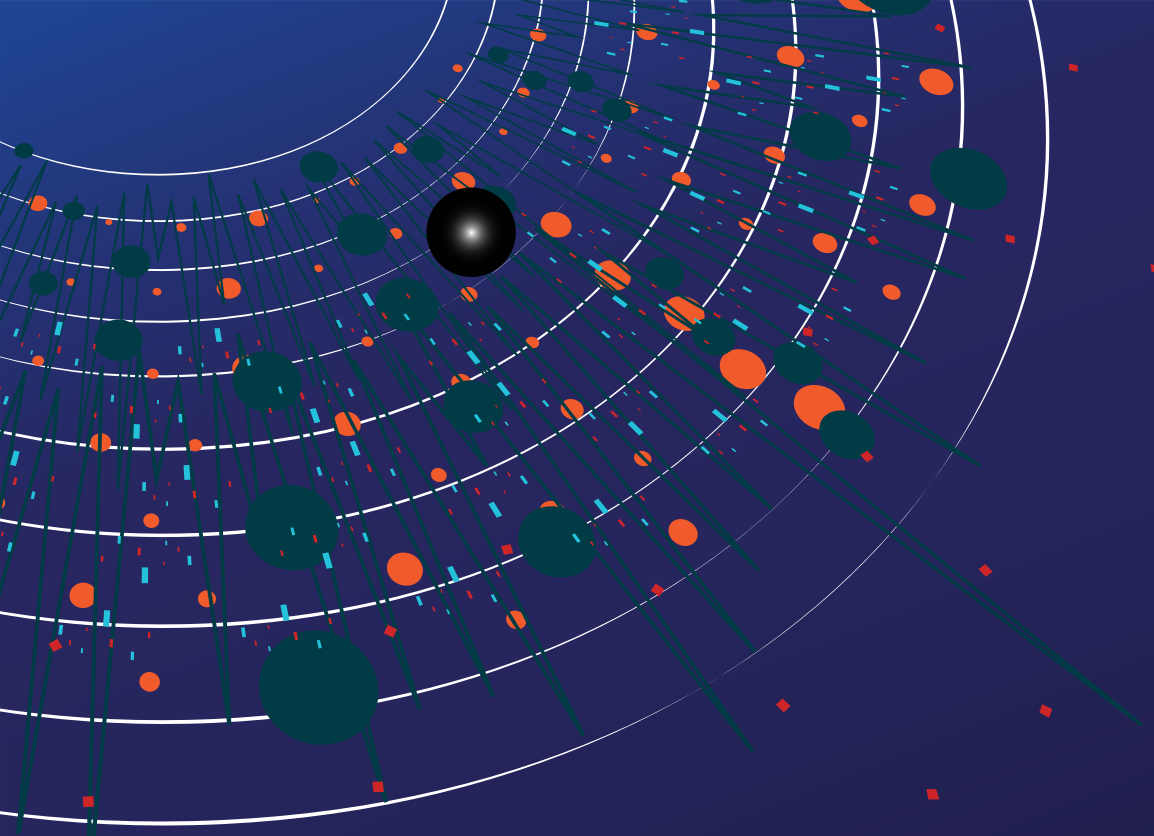
An analysis of ransomware attacks in 2021 indicates that manufacturing is the most affected sector; it is closely followed by the energy, software/IT, and education sectors.

Sector	Attack Count
Manufacturing	20
Energy	09
Software/IT	07
Education	07
Logistics	06
Government	06

4.2% Increase in CWE Categories

We identified two new entrants to the weakness category in this quarter: CWE-295 and CWE-611. CWE-295 falls under the A3 category of the Open Web Application Security Project (OWASP) Top Ten 2017 vulnerabilities, indicative of sensitive data exposure risk.

On the other hand, CWE-611 ranks nineteenth under MITRE's Top 20 weaknesses and falls under the A4-XML External Entities category of OWASP's Top Ten 2017. It has been rated 'critical' by Verizon Media's bounty rating and promises hackers a reward of $10,000-$15,000 for every vulnerability found under this weakness.



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