SPOTLIGHT

RiskSense | CSW Cyber SecurityWorks

Ransomware

Through the Lens of Threat and Vulnerability Management

Index Update Q2 2021

2021

This Quarterly Ransomware Index Spotlight Report (Q2 2021) highlights an increase in several key ransomware markers. There has been steady growth in the number of new APT groups using ransomware, an emergence of new ransomware families and Ransom as Service offerings, and an increase of Common Weakness Enumeration (CWEs) associated with researched vulnerabilities.

We also observed a slight spike in the number of vulnerabilities associated with ransomware. The long-standing trend of ransomware leveraging old vulnerabilities and low CVSS scoring CVEs is a continuing theme or trend.

Ransomware families were quick to exploit two zero-day vulnerabilities discovered in this quarter: CVE-2021-28799 (a QNAP vulnerability) and CVE-2021-20016 (a SonicWall vulnerability). These vulnerabilities were exploited prior to patch availability and publication in the US National Vulnerability Database (NVD), further establishing the unpredictability of ransomware attacks.

This Q2 Ransomware Index Spotlight Report provides organizations with important growth trends about vulnerabilities linked with ransomware. It also looks at the weaknesses that ransomware families leverage through the lens of risk and threat management.

FOCUS	PREVIOUSLY REPORTED	NEW TOTALS	Q2 '21 CHANGE
CVEs Associated with Ransomware	260	266	2.3% Increase
Low-Scoring* CVEs Tied to Ransomware * CVSS v2 score less than 8	153	159	3.9% Increase
Actively Exploited* and Trending Vulnerabilities *Used with Ransomware	132	134	1.5% Increase
Number of Ransomware Families	140	146	4.2% Increase
Exploit Kits in Use by Ransomware	31	31	-
Number of APT Groups Associated with Ransomware	34	40	17% Increase
Old Vulnerabilities Associated with Ransomware	252* *2020 and earlier	255* *2020 and earlier	1.1% Increase
CWEs	50	52	4% Increase
Vulnerable Vendors	96	96	-
Vulnerable Products	722	736	1.93% Increase

Executive Summary

In Q2 2021, ransomware attacks became more disruptive and dangerous, as they targeted organizations' supply chains and went after critical industrial sectors, such as oil and gas, food and beverages, and healthcare. Government alerts and media coverage continue to highlight ransomware as a substantial threat, throwing light on the growing concern over the new wave of cybercrime.

Q2 saw two vulnerabilities that were zero-day exploits exploited even before they were published in the NVD. Threat groups capitalized upon these zero days in QNAP and SonicWall devices before they could be patched, resulting in ransomware attacks, which in the case of QNAP became the reason for the flaw being exposed to the vendor.

Our research noted a 17% increase in the number of APT Groups adopting ransomware tactics and vulnerabilities as part of their arsenal. This is a worrying trend that needs to be monitored carefully, as it highlights attackers' growing preference for ransomware. From a defense standpoint, it presents the need for broader threat-context and risk-based vulnerability management.

Remote Code Execution and Privilege Escalation continue to be the most dangerous exploits of choice for ransomware. Today, 107 such exploits are linked to ransomware—a 15% increase from Q1 2021. As a first step towards improving their defenses against ransomware, we advise organizations to proactively prioritize remediation for these 107 vulnerabilities.

Our research discovered two new CWEs, CWE-134 and CWE-732, among the vulnerabilities tied to ransomware. One is associated with VPN and cleartext access, and the other (in conjunction with RCE) allows the attacker to take control of the entire target system. When used with other exploits, these two vulnerabilities facilitate privilege escalation and system control.

Q2 Ransomware Index Findings

Six New Vulnerabilities Tied to Ransomware

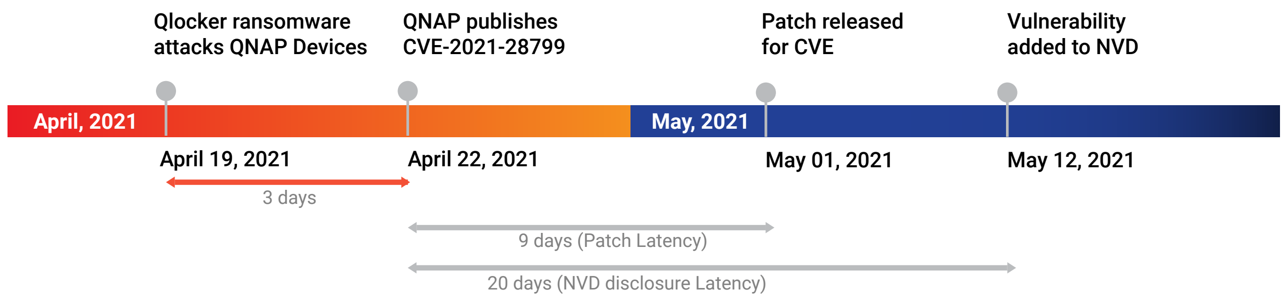
In Q2 2021, we noticed six new vulnerability associations with seven ransomware strains.

Newly-Associated Vulnerabilities	CVSS_V3 Score	CVSS_V3 Severity	Presence of Exploit	Ransomware Strains
CVE-2017-1000253	7.8	High	Yes	DarkRadiation
CVE-2018-13374	8.8	High	Yes	Conti
CVE-2019-1579	8.1	High	Yes	Pay2Key
CVE-2021-20016	9.8	Critical	Yes	Darkside and FiveHands
CVE-2021-26411	7.5	High	Yes	Cerber
CVE-2021-28799	9.8	Critical	Yes	Qlocker

While we know the adage of "old is gold" applies to attackers' preferences for ransomware, we focus on the new vulnerabilities identified in our research and highlight how they contribute to ransomware threats. Two CVEs that were zero-day exploits were strategically exploited by ransomware, even before they were published in the NVD.

- CVE-2021-28799, a QNAP vulnerability, led to ransomware attacks on April 19, 2021, compromising thousands of consumer devices and Server Message Blocks (SMBs). On April 22, 2021, QNAP discovered that the source of attack was a zero-day vulnerability and released a patch on May 1, 2021. The US NVD disclosed the vulnerability on May 12, 2021.

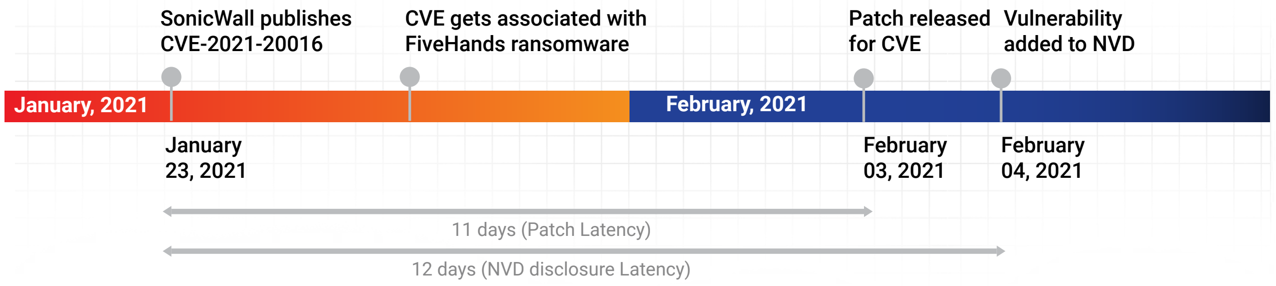
Timeline of CVE-2021-28799


Qlocker ransomware attacks QNAP Devices
QNAP publishes CVE-2021-28799
Patch released for CVE
Vulnerability added to NVD
April, 2021
May, 2021
April 19, 2021
April 22, 2021
May 01, 2021
May 12, 2021
3 days
9 days (Patch Latency)
20 days (NVD disclosure Latency)

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

- In the case of CVE-2021-20016, the SonicWall zero-day vulnerability was published on January 23, 2021. Following this, the vendor released a patch on February 3, 2021. However, before the patch was released, the vulnerability was exploited by the FiveHands ransomware group. The NVD added the vulnerability to its database on February 4, 2021, with a disclosure latency of 12 days.

Timeline of CVE-2021-20016


SonicWall publishes CVE-2021-20016
CVE gets associated with FiveHands ransomware
Patch released for CVE
Vulnerability added to NVD
January, 2021
February, 2021
January 23, 2021
February 03, 2021
February 04, 2021
11 days (Patch Latency)
12 days (NVD disclosure Latency)

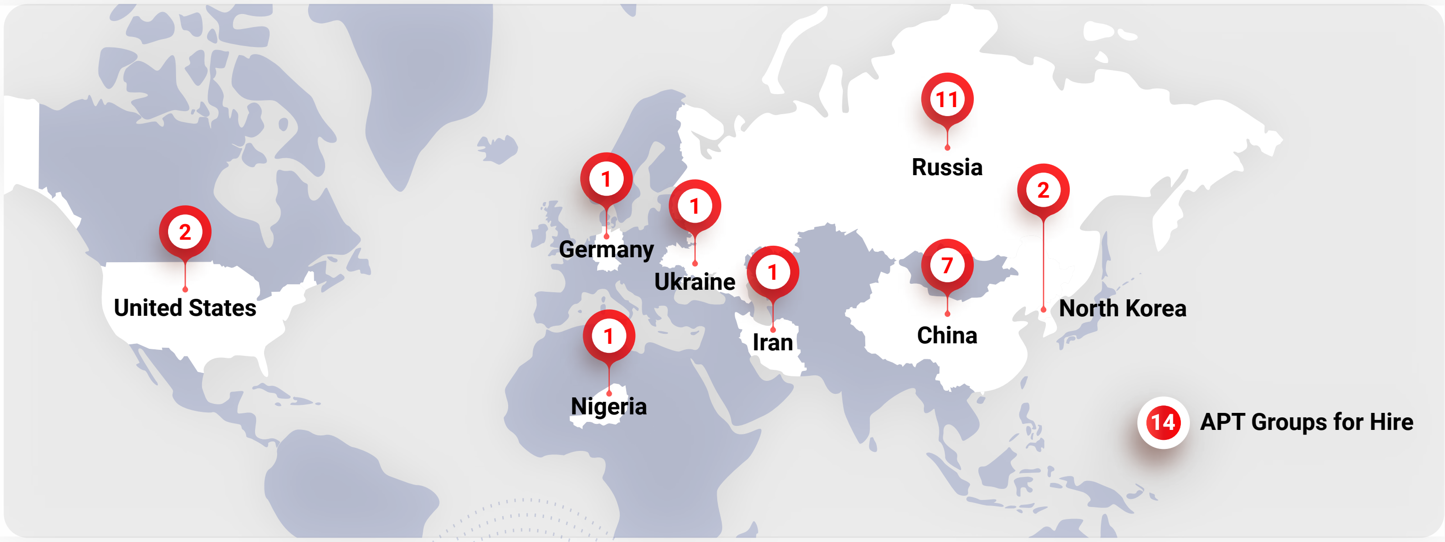
1.5% Increase in Actively Exploited Vulnerabilities

The count of trending and active vulnerabilities used by ransomware continues to increase since the last quarter. We identified two new additions: CVE-2017-1000253 and CVE-2021-20016, which were attributed to ransomware groups in Q2 2021.

APT Group	Country	CVEs Associated with Ransomware
Agrius	Iran	CVE-2018-13379
Carbanak	Ukraine	CVE-2012-0158 CVE-2017-11882 CVE-2018-8174
FIN7	Russia	CVE-2017-11882
UNC2447	-	CVE-2021-20016
UNC2465	-	-
UNC2628	-	-
UNC2659	-	CVE-2021-20016

17% Increase in the Number of APT Groups

Seven new APT groups have been identified in this quarter, further augmenting the threat faced by organizations. The significant growth in ransomware families and APT groups and their adoption of similar tactics marks a dangerous trend that organizations need to address promptly. With this Q2 2021 update, there are now 40 APT groups using ransomware as a part of their arsenal to mount crippling attacks on their targets.



4.2% Increase in the Number of Ransomware Families

An analysis of ransomware families in the second quarter of 2021 brought out six new additions to the list (see below). This takes the total number of ransomware families to 146, recording a 4.2% growth from Q1 2021.

Based on our ransomware research, the Crypwall ransomware family remains one of the biggest ransomware families in the world, with 66 CVEs within its fold. The Cerber strain has overtaken Locky with 65 CVEs tied to ransomware. By comparison, new ransomware families are focused on much smaller vulnerability packages for exploitation. For instance, we noted that Apostle, DarkRadiation, FiveHands, and Qlocker are exploiting one vulnerability each. The Epsilon Red group has three CVE associations; DarkSide has four, and Pay2Key has been exploiting five vulnerabilities in their attacks.

New Ransomware Families
Apostle
DarkRadiation
Epsilon Red
FiveHands
Pay2Key
Qlocker

Vulnerability Analysis

- All vulnerabilities acquired by the six new ransomware groups have known exploits.
- Most of the vulnerabilities being exploited are low-scoring (by CVSS v2 score). However, going by v3 scores, only the Dark Radiation and Epsilon Red groups are using two vulnerabilities with scores less than 8. The rest of the CVEs have revised v3 scores between 8.1 and 10.
- The FiveHands group is leveraging a vulnerability used by DarkSide, the group responsible for the Colonial Pipeline attack.
- Pay2Key has focused on remote access targets using a Citrix vulnerability (CVE-2019-19781) and a Pulse Secure vulnerability (CVE-2019-11510). These two CVEs are also being exploited by eleven and six ransomware groups each, respectively, including the lately notorious REvil group.

4% Increase in CWE Categories

In this update, we highlight two new CWE categories targeted by ransomware. CWE-134 (Use of Externally-Controlled Format String) and CWE-732 (Incorrect Permission Assignment for Critical Resource) are two vulnerabilities we have added to our ransomware database.

A Pentester's Perspective

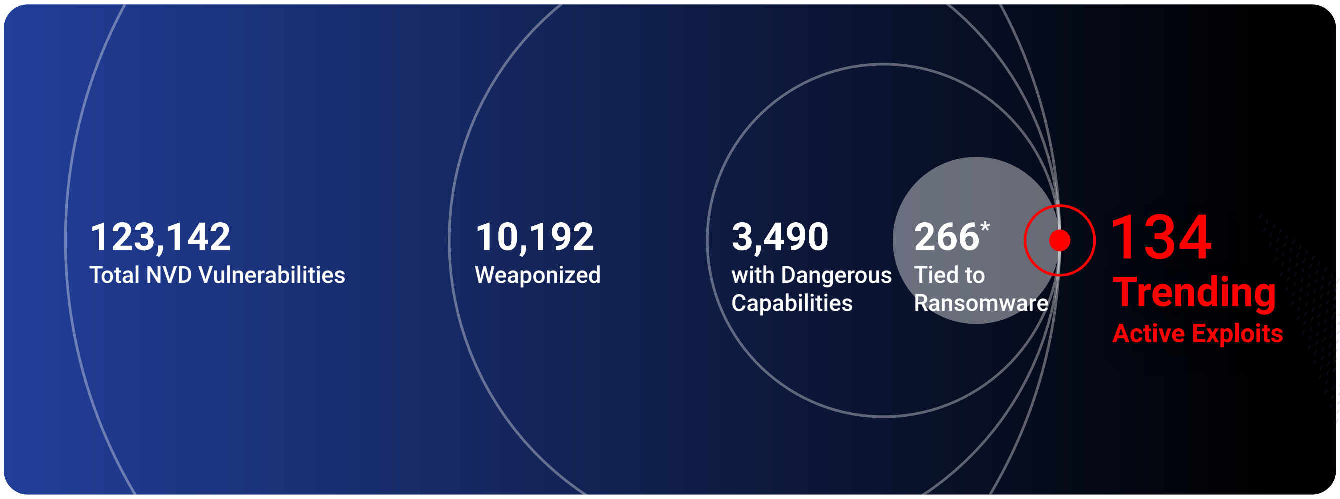
- CWE-732 leads to a new kind of attack that was recently identified. A vulnerability with this weakness exposes the credentials of VPNs in cleartext or easily readable format, thereby allowing the VPN to be easily compromised. There is also a strong possibility of attack chaining being used to infiltrate the victim's network.
- CWE-134 is a weakness that, when combined with an unauthenticated RCE vector, can directly allow hackers to access the victim's machine.
- Attackers can use these CWEs along with others in a chain to achieve their malicious motives.

1.1% Increase in Older Vulnerabilities

Three older vulnerabilities—CVE-2017-1000253, CVE-2018-13374, and CVE-2019-1579—have become associated with DarkRadiation, Conti, and Pay2Key respectively in this quarter. This brings the total count of older vulnerabilities (published in or before 2020) associated with ransomware to 255, which is 95% of the total number of ransomware vulnerabilities.

3.9% Increase in Low-Scoring Vulnerabilities

Low-scoring vulnerabilities are often missed by most scanners. For the purpose of our research, we considered vulnerabilities with CVSS v2 scores of less than 8 as low-scoring. All the new ransomware-associated vulnerabilities fall under this category, taking the count of low-scoring vulnerabilities to 159, which is a 3.9% increase from last quarter's 153.



123,142
Total NVD Vulnerabilities

10,192
Weaponized

3,490
with Dangerous Capabilities

266*
Tied to Ransomware

134
Trending
Active Exploits

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

2021 Spotlight Report

Ransomware

Download Ransomware Spotlight Report 2021 for in-depth analysis and actionable insights.

READ IT NOW

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