

UNIT 42

BY PALO ALTO NETWORKS

Threat Research Center > Trend Reports > Ransomware

RANSOMWARE

Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report

🕒 7 min read

RELATED PRODUCTS

Advanced WildFire

Cortex XDR

Cortex XSOAR

Next-Generation Firewall

By: Guang Qing He , Cecil Liu , Aiden Huang , Royce Lu

Published: July 28, 2021

Categories: Malware , Ransomware , Trend Reports

Tags: Retail , Sandbox

Download

Print

Share

This post is also available in: [日本語 \(Japanese\)](#)

Executive Summary

Ransomware is one of the top threats in cybersecurity and a focus area for Palo Alto Networks. In the current threat landscape, ransom payments are rising and organizations are seeking to protect themselves from threat actors. In the **2021 Unit 42 Ransomware Threat Report**, we detailed the observations and the trend of top ransomware families from January 2020-January 2021. This post supplements that information based on observations from the first three months of 2021, and will discuss the propagation of different ransomware families we observed in the wild and the different types of extortion used. We hope the information will help readers get a clear picture of current directions in ransomware trends.

Ransomware Trends in Early 2021

In the first quarter (Q1) of 2021, Unit 42 detected 113 different ransomware families in the wild. Based on the statistical data, the top 15 ransomware families only cover 52.3% of total ransomware cases. This demonstrates the diversity of ransomware and emphasizes how difficult it is to expand ransomware detection coverage with static profiling. Figure 1 shows the proportion of ransomware sample numbers for different families that Unit 42 detected in the wild. Among all, 6.7% of the ransomware samples are Virlock, which has been active since 2014. Virlock has the largest number of variants due to its file-infector-like behavior.

TABLE OF CONTENTS

- Executive Summary
- Ransomware Trends in Early 2021
- Ransom Payment Operations
- Ransomware Families: Low and High Profile
- Conclusion

RELATED ARTICLES

DarkGate: Dancing the Samba With Alluring Excel Files

Large-Scale StrelaStealer Campaign in Early 2024

The Art of Domain Deception: Bifrost's New Tactic to Deceive Users

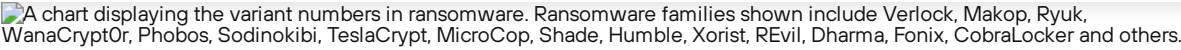
A chart displaying the variant numbers in ransomware. Ransomware families shown include Verlock, Makop, Ryuk, WanaCrypt0r, Phobos, Sodinokibi, TeslaCrypt, MicroCop, Shade, Humble, Xorist, REvil, Dharma, Fonix, CobraLocker and others.



Figure 1. Ransomware variant numbers, showing the proportion of ransomware sample numbers for different families that Unit 42 detected in the wild.

Higher malware variant numbers don't necessarily imply a higher prevalence. Some ransomware families don't deliver different variants every time, but the infection ratio per sample is high, meaning attackers delivered the same malware to huge numbers of victims. Figure 2 shows a completely different result from Figure 1 and stems from only counting ransomware samples from cases in which more than five hosts were infected with the same malware. From this lens, the top three families observed are **Ryuk** (31.7%), **Sodinokibi** (20%) and **Maze** (15%).

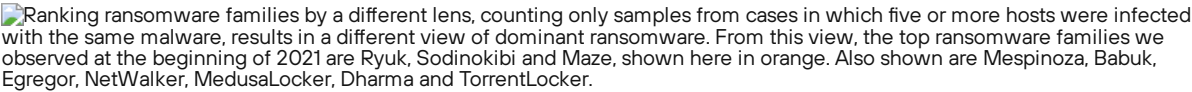
Ranking ransomware families by a different lens, counting only samples from cases in which five or more hosts were infected with the same malware, results in a different view of dominant ransomware. From this view, the top ransomware families we observed at the beginning of 2021 are Ryuk, Sodinokibi and Maze, shown here in orange. Also shown are Mespinoza, Babuk, Egregor, NetWalker, MedusaLocker, Dharma and TorrentLocker.



Figure 2. Top ransomware families based on prevalence.

Emails are still the most efficient method to deliver and propagate ransomware. Figure 3 shows ransomware arrives via different application protocols. The majority of ransomware is delivered by email. Web browsing is the second most common entry vector for ransomware infections. The process of delivering malware by a URL can include various techniques. For example, the URL links can be posted on forums or chat group software, sent by IM applications, offered via fake freeware for download or attached in emails. Web hosting ransomware can also be downloaded and successfully installed through a multi-layered infection chain among different file types. For example, **AlumniLocker** is first delivered as a phishing PDF. It leads to downloading a ZIP archive that contains an LNK downloader. This downloads and executes an obfuscated PowerShell script to finally install the ransomware.

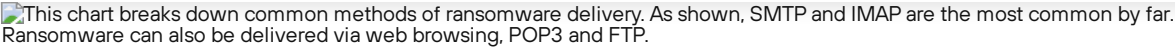
This chart breaks down common methods of ransomware delivery. As shown, SMTP and IMAP are the most common by far. Ransomware can also be delivered via web browsing, POP3 and FTP.



Figure 3. Arrival protocols used to deliver ransomware and their prevalence.

File types used to deliver ransomware in the cases we observed. Top file types are 32-bit EXE (80.8%), 64-bit EXE (5.7%), DLL (3.3%) and RAR Archive (2.8%).



Figure 4. File Type Breakdown.

Figure 4 breaks down which file types we saw in the course of ransomware detection and their prevalence. 32-bit EXE is the most common ransomware file type we observed. Other file types are often used as the first stage of infection or downloaders, such as archives, documents and scripts. Most ransomware is delivered via email with an attached archive; the ransomware is compressed in the archived files with or without password protection. “Resume” or “portfolio document” are examples of archive file names, and the archive contains one or more pieces of malware with fake document file icons. One example here is Makop, contained in a 7z archive along with an infostealer malware (SHA256: DE6DFA018773E07C218EF1DF62CE0D99A708841BF1DDFB4C6AD7E323D5D666A4). A script file is also used to download or install ransomware. For example, **GandCrab** uses JScript as a downloader, leveraging Windows Background Intelligent Transfer Service (BITS) to download the payload in the background (Figure 5). We also observed that Mailto (AKA **NetWalker**) tends to deliver ransomware in a highly obfuscated PowerShell script. Exploit documents are seldom seen for delivering ransomware. One example is an exploit RTF that led to downloading and installing Makop ransomware remotely.

GandCrab uses an HTTP BITS file transfer service to download a payload in the background.



Figure 5. GandCrab uses an HTTP BITS file transfer service to download a payload in the background.

Besides encrypting files on infected hosts, the main feature of ransomware is, of course, the demand for ransom. Since

Payment in Cryptocurrency

In these cases, the ransom note asks victims to pay a specific amount in cryptocurrency – Bitcoin (BTC), Monero (XMR), etc. – to a specific wallet address. Two ransomware families that utilize these types of ransom notes are Virlock and WanaCryptOr.

Payment Through the Darknet

Some ransomware families, including Babuk, Sodinokibi, Cerber, Mailto, Ryuk and others, seldom show the ransom amount or cryptocurrency wallet address. Instead, they instruct victims to install TOR and reach out to them on the darknet. Usually, they host a website for victims to input the identification key found in the ransom note, upload encrypted files for decryption – and pay the ransom.

Other Methods of Ransom Payment

Ransom notes from Makop, **Dharma**, Ryuk, DearCry and others, sometimes ask victims to reach out to them via email. The email addresses given are usually from untraceable email accounts. At other times, a threat actor lets the victim chat with them directly on group chat software. The victims can find the threat actor’s user name through specific group chat software or follow a chat group link in the ransom note.

Ransom Payment Operations

Ransom payment operations are complicated and highly automated processes. Attackers can create a lot of cryptocurrency wallets automatically; they can even make a unique wallet address for each victim. Once a ransom is received, the ransom will be involved in the multiple transactions that are managed to distribute and aggregate the ransom across thousands of virtual wallets. For example, the Xorist ransomware (SHA256: 4979A10B81C41ECC0FC3A0F376ADE766CE616D2301639F74E0277047CC40E3D6) demanded £1,000 for a ransom; the bitcoin wallet address was 1BFqrLCDwrrxueY7FFDn8DqeoasPJignxt. However, this wallet had not really received any ransom payments when the malware was delivered. The wallet got involved in the operation of mixing and tumbling among several other virtual wallets. This is a pretty common operation when attackers want to withdraw or disperse currency from ransom payments into other wallets. During the operation, 25.1 BTC from 538 wallets was sent to 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobuls (SHA256: CE11703DEF517306326C48A67A7C859A3DE0F18E2451DF226CE171389A5B7953), which is a wallet owned by Binance cryptocurrency exchange. (ref: **Binance on Twitter**). The 25.1 BTC amount was worth \$1.18 million at that time, and now is about \$876,000.

Ransomware Families: Low and High Profile

Since Virlock only requests a \$250 ransom, it does not draw too much public attention. Other ransomware families, however, target enterprises and ask for multimillion dollar ransoms, which garners much more media attention. Based on the way Virlock spreads the ransom amount it demands, it is likely designed to target consumers or home users.

After infection, Virlock hides the file extension through modification of the registry (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt = 1, HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden = 2). The encrypted file icon will look the same as usual, but after opening the infected file, the ransom note will pop up. Virlock uses, but isn’t limited to, PDF, DOC, PPT, JPG, BMP,GIF, RAR, 7Zip, Zip and EXE files. Figure 6 is a screenshot of a recently captured Virlock ransom note. The attacker asked for \$250 and required payment as 0.004 BTC (suggesting that at the time the ransom note was written, 1 BTC equaled approximately \$62,500). At the time of infection experiments, 1 BTC equaled approximately \$54,649, suggesting that the exchange rate in the ransom note is not updated on the fly. Some Virlock variants ask for more ransom, such as 0.771 BTC, 1.008 BTC or more.

 A warning window pops up to notify the user that an unauthorized or pirated software has been detected and your computer is blocked.



Figure 6. Virlock ransom note.

The top three samples we observed spreading in early 2021 were Ryuk, Maze, and Sodinokibi. These three contribute 7.2% out of the total infected numbers we collected.

SHA256	Ransomware name	Infection rate (vs total ransomware infection)
0e4442a40c9ffc9d8ba99be30e148c8d062a6fe5353009b4a10f040eac8aae94	Ryuk	2.6%
f4ef694c1df96910020d8b49139d406eeadb522c6ae318a4d6936a6464152dba	Maze	2.4%
6d9349a99d80e9003d3a01e0ad19c5f175e18b2dee7ef533b630772548f6c727	Sodinokibi	2.2%

Ryuk will change the infected file extension to .RYK, and leave a ransom note called `RyukReadMe.html` . One of the reasons Ryuk causes so much damage is because it will scan the local network and try to infect other machines through Server Message Block (SMB) protocols. Ryuk will even send out **Wake-on-LAN packets** to wake up systems that have been configured with this feature.

 Screenshot of Ryuk sample, showing time, source, destination and protocol.

Conclusion

In this research, we discussed ransomware family trends we observed in the first three months of 2021. First, we reviewed the trends from prevalent ransomware families, then we discussed the most common file types used as attack vectors leveraged by ransomware. Lastly, we gave an example of ransom operations and updates about top ransomware families.

Ransomware threats are a serious challenge. Employing effective backup strategies and disaster recovery procedures is important. Palo Alto Networks customers are further protected from ransomware. **Cortex XSOAR** can automatically and instantly coordinate with network security, malware analysis and threat management solutions to ensure customers remain protected. Cortex **XDR** endpoint protection stops malware, exploits and ransomware before they can compromise endpoints. With AI-powered Inline analysis, the **Next-Generation Firewall** stops exploits that lead to infection, and **WildFire**'s always up-to-date machine learning models monitor behavior to preemptively detect unknown ransomware.

If you think you may have been impacted by ransomware, please email unit42-investigations@paloaltonetworks.com or call (866) 4-UNIT42 to get in touch with the Unit 42 Incident Response team.

Additional Resources

Highlights from the 2021 Unit 42 Ransomware Threat Report

Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report

Back to top

TAGS

- Retail
- Sandbox

<

Threat Research Center

Next: THOR: Previously Unseen PlugX Variant Deployed During Microsoft Exchange Server Attacks by PKPLUG Group

>

Related Resources

C THREAT RESEARCH
IC

November 1, 2024

TA Phone Home: EDR Evasion Testing Reveals Extortion Actor's Toolkit

Extortion

Data exfiltration

Read now →

C THREAT ACTOR GROUPS
IC

October 30, 2024

Jumpy Pisces Engages in Play Ransomware

North Korea

Jumpy Pisces

Fiddling Scorpius

Read now →

C HIGH PROFILE THREATS
IC

October 10, 2024

Lynx Ransomware: A Rebranding of INC Ransomware

Leak site

Double extortion

Read now →

C THREAT RESEARCH
IC


October 9, 2024

Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Inst...

North Korea

Social engineering

Python

 Newsletter

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. Please read our [privacy statement](#) for more information.

Page 6 of 7

Your Email

Subscribe for email updates to all Unit 42 threat research.
By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).

Subscribe 

Products and services

Network Security Platform

Code to Cloud Platform

CLOUD DELIVERED SECURITY SERVICES

Prisma Cloud

Advanced Threat Prevention

Cloud-Native Application Protection Platform

DNS Security

Data Loss Prevention

IoT Security

Next-Generation Firewalls

Hardware Firewalls

Strata Cloud Manager

SECURE ACCESS SERVICE EDGE

Prisma Access

Prisma SD-WAN

Autonomous Digital Experience Management

Cloud Access Security Broker

Zero Trust Network Access

AI-Driven Security Operations Platform

Threat Intel and Incident Response Services

Cortex XDR

Proactive Assessments

Cortex XSOAR

Incident Response

Cortex Xpanse

Transform Your Security Strategy

Cortex XSIAM

Discover Threat Intelligence

External Attack Surface Protection

Security Automation

Threat Prevention, Detection & Response

Company

About Us

Careers

Contact Us

Corporate Responsibility

Customers

Investor Relations

Location

Newsroom

Popular links

Blog

Communities

Content Library

Cyberpedia

Event Center

Manage Email Preferences

Products A-Z

Product Certifications

Report a Vulnerability

Sitemap

Tech Docs

Unit 42

Do Not Sell or Share My Personal Information

Privacy Trust Center Terms of Use Documents

Copyright © 2024 Palo Alto Networks. All Rights Reserved



EN

