Understanding REvil: The Ransomware Gang Behind the Kaseya VSA Attack

unit42.paloaltonetworks.com/revil-threat-actors/

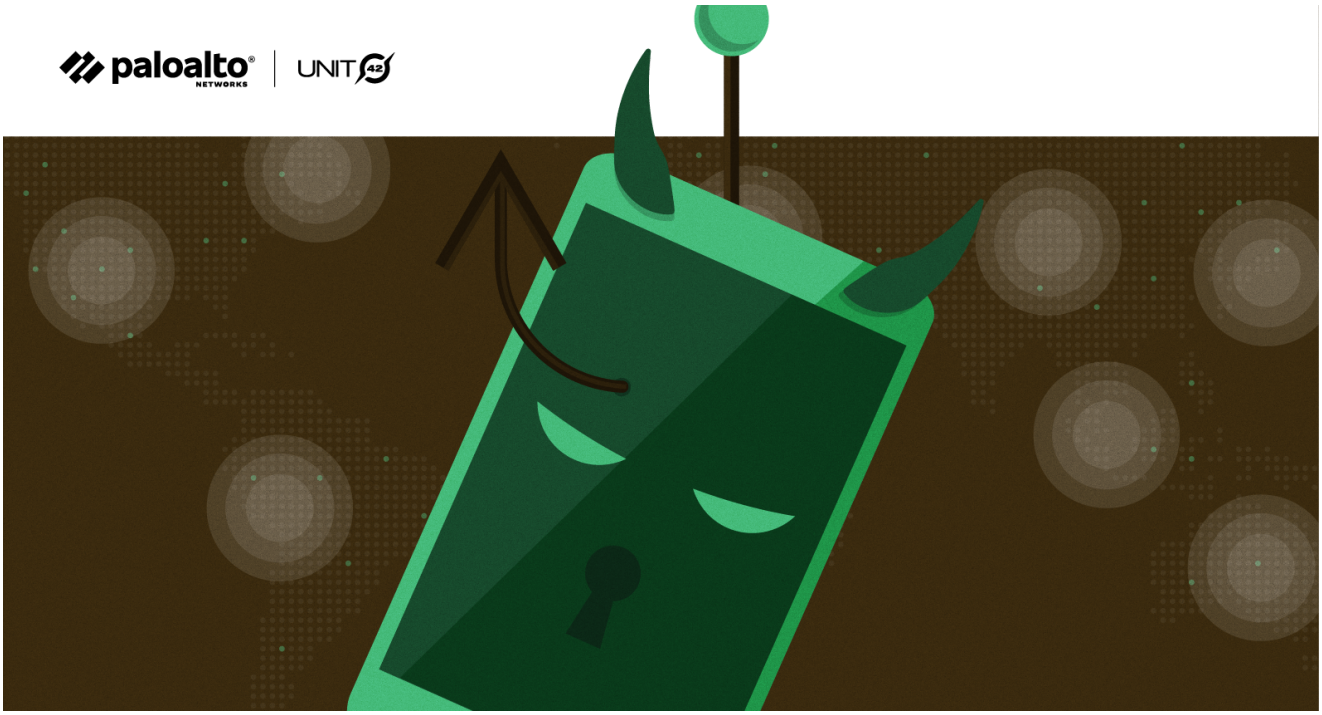
John Martineau July 6, 2021

By John Martineau

July 6, 2021 at 2:50 PM

Category: Ransomware, Unit 42

Tags: GandCrab, Kaseya, ransomware threat report, REvil, Sodinokibi



This post is also available in: 日本語 (Japanese)

Executive Summary

REvil has emerged as one of the world's most notorious ransomware operators. In just the past month, it extracted an $11 million payment from the U.S. subsidiary of the world's largest meatpacking company based in Brazil, demanded $5 million from a Brazilian medical diagnostics company and launched a large-scale attack on dozens, perhaps hundreds, of companies that use IT management software from Kaseya VSA.

While REvil (which is also known as Sodinokibi) may seem like a new player in the world of cybercrime, Unit 42 has been monitoring the threat actors tied to this group for three years. We first encountered them in 2018 when they were working with a group known as GandCrab. At the time, they were mostly focused on distributing ransomware through malvertising and exploit kits, which are malicious advertisements and malware tools that hackers use to infect victims through drive-by downloads when they visit a malicious website.

That group morphed into REvil, grew and earned a reputation for exfiltrating massive data sets and demanding multimillion dollar ransoms. It is now among an elite group of cyber extortion gangs that are responsible for the surge in debilitating attacks that have made ransomware among the most pressing security threats to businesses and nations around the globe.

Earlier this year, we released a threat assessment tying REvil/Sodinokibi to GandCrab. Here, we provide insights gleaned from Unit 42 cybersecurity consultants who worked over a dozen REvil ransomware cases in the first six months of 2021. We hope these accounts of REvil's tactics and steps taken to counter this threat will help organizations better defend against future ransomware attacks. We also encourage you to review the 2021 Unit 42 Ransomware Threat Report for further insight into REvil and other ransomware operators.

Palo Alto Networks WildFire, Threat Prevention and Cortex XDR detect and prevent REvil ransomware infections.

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

Ransomware as a Service

REvil is one of the most prominent providers of ransomware as a service (RaaS). This criminal group provides adaptable encryptors and decryptors, infrastructure and services for negotiation communications, and a leak site for publishing stolen data when victims don't pay the ransom demand. For these services, REvil takes a percentage of the negotiated ransom price as their fee. Affiliates of REvil often use two approaches to persuade victims into paying up: They encrypt data so that organizations cannot access information, use critical computer systems or restore from backups, and they also steal data and threaten to post it on a leak site (a tactic known as double extortion).

Threat actors behind REvil operations often stage and exfiltrate data followed by encryption of the environment as part of their double extortion scheme. If the victim organization does not pay, REvil threat actors typically publish the exfiltrated information. We have observed threat actors who are clients of REvil focus on attacking large organizations, which has enabled them to obtain increasingly large ransoms. REvil and its affiliates pulled in an average payment of about $2.25 million during the first six months of 2021 in the cases that

we observed. The size of specific ransoms depends on the size of the organization and type of data stolen. Further, when victims fail to meet deadlines for making payments via bitcoin, the attackers often double the demand. Eventually, they post stolen data on the leak site if the victim doesn't pay up or enter into negotiations.

2021 Trends – Something Old, Something New

Unit 42 has worked over a dozen REvil ransomware cases so far this year. While some of the tactics cited in our 2021 Unit 42 Ransomware Threat Report have remained the same, we have seen a few deviations from REvil's standard attack lifecycle. For a quick reference, we have generated Actionable Threat Objects and Mitigations (ATOMs) to display REvil's tactics, techniques, procedures and other indicators of compromise (IOCs).

How REvil Threat Actors Gain Access

REvil threat actors continue to use previously compromised credentials to remotely access externally facing assets through Remote Desktop Protocol (RDP). Another commonly observed tactic is phishing leading to a secondary payload. However, we also observed a few unique vectors that relate to the recent Microsoft Exchange Server CVEs, as well as a case that involved a SonicWall compromise. Below are the five unique entry vectors observed thus far in 2021.

- A user downloads a malicious email attachment that, when opened, initiates a payload that downloads and installs a QakBot variant of malware. In at least one case, the version of QakBot we observed collected emails stored on the local system, archived them and exfiltrated them to an attacker controlled server.
- In one instance, a malicious ZIP file attachment containing a macro-embedded Excel file that led to an Ursnif infection was used to initially compromise the victim network.
- Several actors utilized compromised credentials to access internet-facing systems via RDP. It's unclear how the actors gained access to the credentials in these instances.
- An actor exploited a vulnerability in a client SonicWall appliance categorized as CVE-2021-20016 to gain access to credentials needed to access the environment.
- An actor utilized the Exchange CVE-2021-27065 and CVE-2021-26855 vulnerabilities to gain access to an internet-facing Exchange server, which ultimately allowed the actor to create a local administrator account named "admin" that was added to the "Remote Desktop Users" group.

How REvil Threat Actors Establish Their Presence Within an Environment

Once access is obtained, REvil threat actors typically utilize Cobalt Strike BEACON to establish their presence within an environment. In several instances we observed, they used the remote connection software ScreenConnect and AnyDesk. In other cases, they chose to create their own local and domain accounts, which they added to the "Remote Desktop

Users" group. Further, the threat actors often disabled antivirus, security services and processes that would interfere with or otherwise detect their presence within the environment.

Below are specific techniques we observed thus far in 2021:

- Once the actor had access to the environment, they utilized different toolsets to establish and maintain their access, including the use of Cobalt Strike BEACON as well as local and domain account creation. In one instance, the REvil group utilized a BITS job to connect to a remote IP, download and then execute a Cobalt Strike BEACON.
- In several incidents, Unit 42 identified the use of "Total Deployment Software" by REvil threat actors to deploy ScreenConnect and AnyDesk software to maintain access within the environment.
- In many instances, the REvil actor(s) created local and domain level accounts through BEACON and NET commands even if they had access to domain-level administrative credentials.
- Unit 42 observed common evasion techniques across all engagements in which REvil threat actors used [1-3] alphanumeric batch and PowerShell scripts that stopped and disabled antivirus products, services related to Exchange, VEAAM, SQL and EDR vendors, as well as enabled terminal server connections.

How REvil Threat Actors Expand Access and Gather Intelligence

In most cases, REvil actors need to gain access to additional accounts that have a wider set of privileges in order to move further within the victim environment and carry out their mission. They often use Mimikatz to access cached credentials on the local host. However, Unit 42 also observed the SysInternals tool procdump as a means to dump the LSASS process. Unit 42 also found it common for this threat actor to access files with the name "password" within the filename. In one instance, we observed an attempt to gain access to a KeePass Password Safe.

During the reconnaissance phase of attacks, REvil threat actors often utilize various open source tools to gather intelligence on a victim environment and in some cases resort to utilizing administrative commands NETSTAT and IPCONFIG to gather information.

Below are specific observations of REvil's behavior in 2021.

- Network reconnaissance tools netscan, Advanced Port Scanner, TCP View and KPort Scanner were observed in over half the engagements Unit 42 responded to.
- The threat actors often use Bloodhound and AdFind to map out networks and gather other active directory information.
- In two engagements, Unit 42 observed the use of ProcessHacker and PCHunter in what appeared to be an attempt to gain insight into processes and services running on hosts within the environment.

How REvil Threat Actors Move Laterally Throughout Compromised Environments

In general, REvil threat actors utilize Cobalt Strike BEACON and RDP with previously compromised credentials to laterally move throughout compromised environments. Additionally, Unit 42 observed use of the ScreenConnect and AnyDesk software as methods of lateral movement. While we have seen other ransomware groups employ these tactics, we observed REvil threat actors retrieving these binaries from file sharing sites such as MEGASync and PixelDrain.

How REvil Threat Actors Complete Their Objectives

Finally, we observed REvil threat actors moving to the final stage of their attack, encrypting networks, staging and exfiltrating data, and destroying data to prevent recovery and hinder analysis.

Ransomware Deployment

- REvil threat actors typically deployed ransomware encryptors using the legitimate administrative tool PsExec with a text file list of computer names or IP addresses of the victim network obtained during the reconnaissance phase.
- In one instance, a REvil threat actor utilized BITS jobs to retrieve the ransomware from their infrastructure. In a separate instance, the REvil threat actor hosted their malware on MEGASync.
- REvil threat actors also logged into hosts individually using domain accounts and executed the ransomware manually.
- In two instances, the REvil threat actor utilized the program dontsleep.exe in order to keep hosts on during ransomware deployment.
- REvil threat actors often encrypted the environment within seven days of the initial compromise. However, in some instances, the threat actor(s) waited up to 23 days.

Exfil

- Threat actors often used MEGASync software or navigated to the MEGASync website to exfiltrate archived data.
- In one instance, the threat actor used RCLONE to exfiltrate data.

Defense Maneuvers

During the encryption phase of these attacks, the REvil threat actors utilized batch scripts and wevtutil.exe to clear 103 different event logs. Additionally, while not an uncommon tactic these days, REvil threat actors deleted Volume Shadow Copies in an apparent attempt to further prevent recovery of forensic evidence.

Conclusion: Evolve

While the REvil operational group may target large organizations, all are potentially susceptible to attack. As we draw closer to a post COVID-19 environment, IT and other defenders of networks should take time to learn what's normal in their environments and notice and question abnormalities. Investigate them. Question your defenses. Do all users need to be able to open macro-enabled documents? Do you have endpoint visibility and protections to, at minimum, alert you to secondary infections such as QakBot? If you absolutely need RDP, are you using tokenized MFA? And don't question just once – question routinely. Think like the attacker. You might be able to stop your organization from being the next victim and escape being in the headlines for the wrong reasons.

Palo Alto Networks customers are protected by:

- WildFire: All known samples are identified as malware.
- Cortex XDR with:
    - Prevention for known REvil indicators
    - Anti-Ransomware Module to prevent REvil encryption behaviors.
    - Local Analysis detection to prevent REvil binary executions.
    - Behavioral Threat Protection, Anti-exploitation modules and Suspicious Process Creation to prevent REvil techniques.
    - XDR Analytics, Analytics BIOCs and BIOCs to detect REvil techniques.
- AutoFocus: Tracking related activity using the REvil tag.
- Cortex XSOAR: "Kaseya VSA 0-day - REvil Ransomware Supply Chain Attack" playbook. Playbook includes the following tasks:
    1. Collect related known IOCs from several sources.
    2. Indicators, PS commands, Registry changes and known HTTP requests hunting using PAN-OS, Cortex XDR and SIEM products.
    3. Block IOCs automatically or manually.

Unit 42 Incident Response Services: Experts to help you respond and recover.

Additional Resources

Threat Assessment: GandCrab and REvil Ransomware

2021 Unit 42 Ransomware Threat Report

Breaking Down Ransomware Attacks

Ransomware's New Trend: Exfiltration and Extortion

Cortex XSOAR playbook documentation

Updated July 7, 2021 at 10:50 a.m. PT

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.