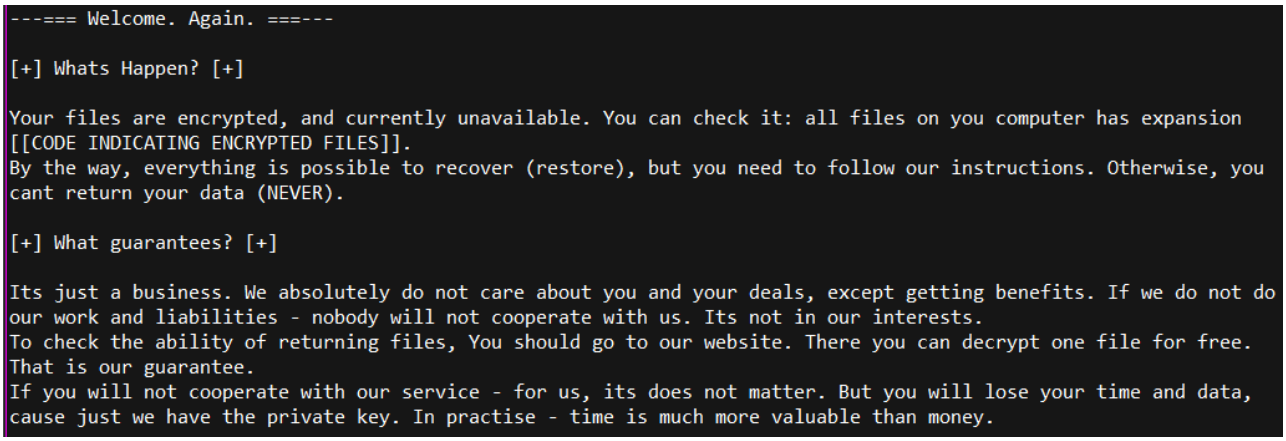
Relentless REvil, revealed: RaaS as variable as the criminals who use it

news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/

Andrew Brandt June 11, 2021

The transition to a *service model* of doing business transformed ransomware, giving its developers the ability to focus on features, and leaving the harder part – the break-in and deployment to the target's computers – to its customers, threat actors who employ a wide range of attack styles, software, and expertise to the task.

One of the ransomware-as-a-service (RaaS) we encounter most frequently, known alternately as Sodinokibi or REvil, is as conventional a ransomware as we've seen: Its routines, configuration, and behavior what we've come to expect from a mature family that's, obviously, well used in the criminal underground.



Unsurprisingly, Sophos has devoted significant effort to combat this everyday menace. In addition to tamper protection features that prevent a script from disabling endpoint protection features, we use behavioral detection rules that identify the core activities ransomware must engage in, and a feature called CryptoGuard that prevents the ransomware from encrypting data.

As attacks involving RaaS malware, including REvil, increasingly have generated public attention and news coverage, SophosLabs wanted to pull together a common body of our knowledge about the ransomware itself, and the variety we observe in attack methods employed by the criminals who lease the software and handle the break-ins.

In addition, we reviewed reports produced by Sophos Rapid Response about attacks involving Sodinokibi/REvil where the MTR team were hired to provide incident response and cleanup. From these detailed analyses, we were able to develop a picture of a common malware being deployed in myriad ways by a large base of criminal customers.

Signs of an impending attack

The deployment of ransomware usually happens at the very end of a much larger, and more elaborate, set of precursor actions that a criminal attacker will take during what might be a significantly long time before anyone in a targeted organization logs on to find a ransom note on their desktop. So while we will discuss the internals and typical characteristics of Sodinokibi/REvil, it makes more sense to describe these precursor actions first. If a defender or network owner can discover and quickly act on these behaviors while the attacker is still laying the groundwork for the final ransomware payload, it's possible to cut off the attackers' access before any harm comes to the target's computers.

Attackers themselves appear to use a combination of scripting (sometimes hosted on file repositories like Github or Pastebin) and manual control (sometimes via the console, other times through Windows Remote Desktop or commercial remote access tools).

File path and name
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/nc.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/privesc.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/SharpByeBear.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/SharpPolarbearx86.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/schedsvc.dll
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/schtasks.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/test.job
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Invoke-Sharpcradle/master/Invoke-Sharpcradle.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/cve-2020-0683.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/cve-2019-1215.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/m15-077.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/juicypotato64.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/invoke-juicypotato.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/cve-2018-8120.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/ms16-32.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/ms16-135.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/view.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/viewdevobfs.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/adpass.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/Invoke-Sharp.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/locksher.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/UpPower.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/GPpass.ps1

SOPHOSlabs

One REvil attacker used scripts taken directly from a repository of penetration tester tools on Github

We've broken a typical attack into the following phases: Penetration and initial access; Credential harvesting and privilege escalation; Tilling the field; and deployment of the ransomware. Often (but not always, because it is attacker-dependent), there's a phase where the attackers use their newfound credentials to hunt for and exfiltrate sensitive organizational data in the hours-to-weeks before delivering the payload.

Penetrating the network

Breaking in is, perhaps unsurprisingly, not all that hard to do if it's what you do, all day long. But it's possible to boil down the initial access methods employed by a variety of criminals who attacked using Sodinokibi/REvil into a few types: Brute-force attacks against known internet-facing services like VPNs, RDP, desktop remote management tools like VNC, and even some cloud-based management systems; The abuse of previously-obtained credentials or access (either retrieved from other malware or phishing) of legitimate accounts that didn't require the use of multi-factor authentication; or, in some cases, piggybacking as a payload from other malware present on the target's network.

Brute-force attacks are, unfortunately, a large part of the traffic that almost any internet-facing service sees on an hour-to-hour basis. The attacks cost so little to the attackers it pays just to throw the kitchen sink at a login screen, which is why multi-factor authentication is so incredibly important (though not necessarily a panacea). Attackers are just as able to use tools like Shodan or Censys, which reveal open ports leading to common services, as defenders.

In one of the recent attacks, the organization logged a massive volume of failed inbound RDP login attempts targeting the server which eventually became a point of access for the attackers. On a typical server, the log that stores failed attempts to login to services like RDP rolls over, overwriting the oldest data, over a period of from several days to weeks depending on how many failed attempts were made. In this attack, the volume of failed RDP login events caused the log files to completely overwrite themselves with new entries every five minutes. The data collected from that server showed approximately 35,000 failed login attempts over a five minute period, originating from 349 unique IP addresses around the world.

Username	Failed login attempts
ADMINISTRATOR	12,638
ADMIN	10,360
USER	439
SERVER	420
ADMINISTATOR1	167
TRAINING	33
CORPORATE	24
OPERATION	24
STATION	24
LIBRARY	22

Among the 35,000 brute-force login attempts made every five minutes, these were the most common usernames the attackers tried to use

RDP was implicated as one of the most common methods of breaching a network in cases we were called in to investigate, which is why shutting off the outside world's access to RDP is one of the most effective defenses an IT admin can take. But RDP was not the only culprit: attackers also gained initial access through other internet-facing services they were able to brute-force or to launch an exploit against a known vulnerability that gave them some access. In one case, the attacker targeted a bug in a specific VPN server software to gain initial access, then exploited a bug on a five-year-old version of Apache Tomcat on the same server that let the attacker create a new admin account on the server.

In at least two different cases involving different target organizations, the initial point of access was something left in place by some *other* threat actor, who we later discovered had previously struck those organizations with ransomware weeks to months prior to our involvement, victimizing them twice.

In one of those cases, we discovered a remnant of Cobalt Strike, a commercial penetration testing toolset frequently abused by criminals to provide themselves with remote access to a computer. The Cobalt Strike artifact had been left in place by a (presumably, different) threat actor who deployed a ransomware called **Le Chiffre**.

In another, the attacker appeared to have brute-forced RDP on a machine that had been previously implicated as the initial foothold of an attack by a different type of ransomware just three weeks prior to the REvil attack.

Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Command & Control	Impact
Valid accounts ID: T1078	Command and Scripting Interpreter ID: T1059	Valid accounts ID: T1078	Impair Defenses ID: T1562	T1570 - Lateral Tool Transfer ID: T1570	Application Layer Protocol ID: 1071	Data Encrypted for Impact ID: T1486
	Scheduled Task/Job ID: T1053	Create or Modify System Process ID: T1543		Remote Services: Remote Desktop Protocol ID: T1021.001		Data Destruction ID: T1485

SOPHOSlabs

The MITRE ATT&CK techniques used in one of the REvil ransomware attacks we investigated

Credential harvesting and privilege escalation

Ransomware threat actors prefer to use internal tools like Domain Controllers to deploy the payload; If they haven't bought a stolen or phished credential, they'll often quietly monitor the network where the computer on which they gained an initial foothold is located. The attackers may use freely-available, not-inherently-malicious utilities to extract saved passwords from the hard drive, and/or more advanced tools such as Mimikatz to obtain the credentials of a domain administrator account. This takes a lot of patience on the part of the attacker, because there's no guarantee they'll pick up a credential in any given set of time. But once they have what they need, they act fast.

Tilling the field: Laying the groundwork for the attack

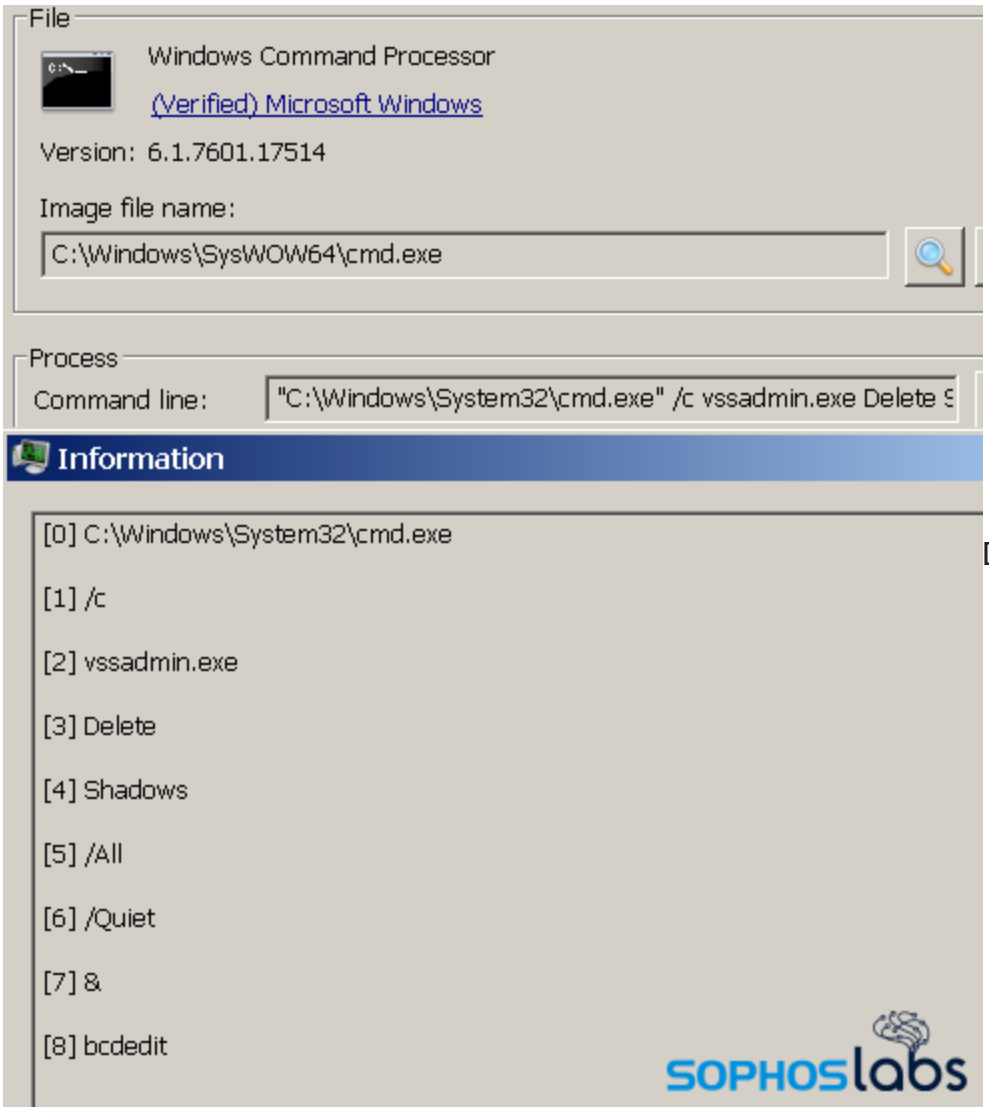
Preparing an enterprise network for a ransomware attack takes a surprising amount of work. The attackers need to establish a list of internal targets, give themselves domain admin privileges, and use those privileges to shut down or otherwise hobble anything that might impede their attack: Windows Defender is usually the first to go, but often the attackers will spend some time trying to determine what endpoint protection tools are running on the computers, and may run one or more customized scripts that combine an attempt to kill any running protection process or services, and also to remove any persistence those processes or services might have.

```
net stop "Sophos AutoUpdate Service"
net stop "Sophos Agent"
net stop "SAVService"
net stop "SAVAdminService"
net stop "Sophos Message Router"
net stop "Sophos Web Control Service"
net stop "swi_service"
net stop "SntpService"
net stop "sophossps"
net stop "swi_filter"

MsiExec.exe /X{66967E5F-43E8-4402-87A4-04685EE5C2CB} /qn
MsiExec.exe /X{1093B57D-A613-47F3-90CF-0FD5C5DCFFE6} /qn
MsiExec.exe /X{66967E5F-43E8-4402-87A4-04685EE5C2CB} /qn REBOOT=SUPPRESS
MsiExec.exe /X{1093B57D-A613-47F3-90CF-0FD5C5DCFFE6} /qn REBOOT=SUPPRESS
net stop "Sophos Anti-Virus"
net stop "Sophos AutoUpdate Service"
"C:\program files\Sophos\Sophos Endpoint Agent\uninstallcli.exe"
:Sophos AutoUpdate
MsiExec.exe /qn /X{7CD26A0C-9B59-4E84-B5EE-B386B2F7AA16} REBOOT=ReallySuppress
```

One REvil attacker built a customized script to terminate Sophos services and processes and even tries to uninstall the software. The attempt was prevented by tamper protection features in the product.

In a at least one case involving Sodinokibi, the attackers went so far as to determine that the target's network was using a Sophos firewall and managing their endpoint protection through Sophos Central. The attacker diligently worked at obtaining the credentials of IT staff and methodically tried those credentials until they found one with permissions to access the Sophos Central control panel, where they used that access to shut down any features that would have blocked the ransomware from executing.



Deleting the Volume Shadow Copy has become a time-honored ransomware tradition at this point. Routinely, we encounter PowerShell scripts, batch files, or other “laying the groundwork” code attackers deploy to disable a variety of protective features. One example is the Volume Shadow Copy, which attackers typically delete as the Volume Shadow could assist in the recovery of deleted or encrypted data.

The number of different commands they can use to execute the same tasks is somewhat limited, but the sequence and thoroughness varies greatly from threat actor to threat actor. We also discovered that some threat actors simply number their scripts sequentially, or give them benign-looking names, others have used files with profane or hateful references in the filenames, sometimes in combination with the word Sophos.

Large uploads of stolen data (exfil)

In only about half of the incidents involving Sodinokibi/REvil analyzed for this report did the attackers conduct an exfiltration of significant volumes of private, sensitive, or valuable data from the target organizations. In theory, these types of uploads should be detectable, but in practice, that never happened in the cases we investigated.

Practically speaking, once they had obtained the permissions they needed, the attackers typically spent a few days looking through file servers, collecting large amounts of documents and bundling them into one or more compressed files on a machine inside the network. Once they had collected everything they wanted to steal in one place, they would begin an upload that, depending on the network speed and the amount of data, could take from hours to more than a day to complete.

Threat actors have used a variety of cloud storage services to hold this stuff in the past, but appear to prefer a few over others. Mega.nz, the cloud storage provider, seems to be in favor among some criminals who engage in ransomware attacks we've investigated. Among the incidents where Sodinokibi was eventually deployed after a large exfiltration and an attempted extortion, roughly three-quarters used Mega.nz as a (temporary) repository for that stolen data.

Mega uses its own client application to speed uploads, which were found left behind by the attackers in cases where they didn't clean up after themselves. A small number of attackers used other methods, such as installing a portable copy of the FTP client FileZilla that they used to upload data to a staging server outside the target's network perimeter.

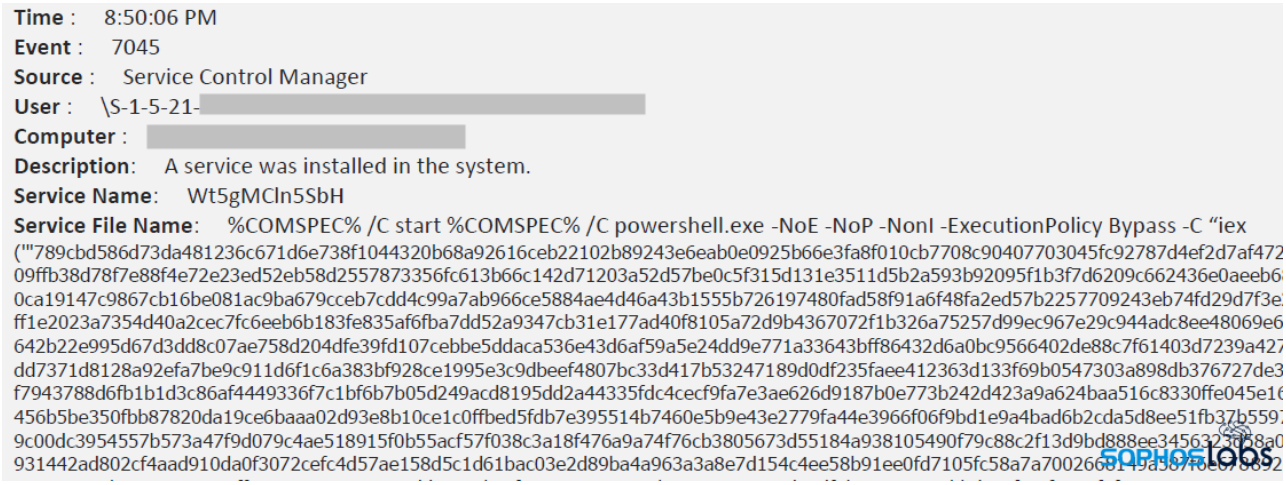
Conventional wisdom about how to respond to data leak extortion attempts has shifted away from advice to make the payment. The criminals claim they will delete their copies of the data if you pay the ransom demands, but that's widely viewed as an unreliable promise. There's no assurance other than the word of people who are extorting you that they'll hold up their end of the bargain.

The final insult: deployment

Attackers have launched the ransomware payload using a wide variety of methods. They may push out copies to individual machines from a domain controller, or use administrative commands with WMIC or PsExec to run the malware directly from another server or workstation they control over the internal network of the target organization.

Sodinokibi/REvil has a few additional options that its operators may take advantage of by launching the malware with special command flags. One of the ways we've observed ransomware attempt to work around endpoint protection tools is to reboot the computer into Safe Mode, and then begin the encryption operation. A computer in Safe Mode boots to a diagnostic form of Windows in which third-party drivers and services are not running, but the ransomware adds itself to the (very short) list of applications that run in Safe Mode. REvil has a Safe Mode flag attackers could use.

In one instance, we observed a threat actor attempt to bypass security software by delivering and installing a full copy of VirtualBox and a virtual disk file, running the ransomware within a Windows 10 virtual machine guest copied to the targeted host computer, executing the encryption commands from the guest to target the host.

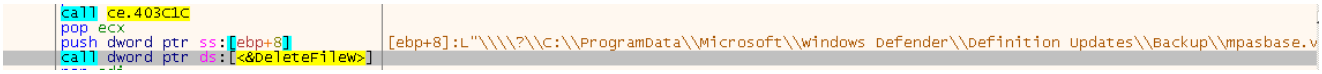


The long, encoded command string that requires you to know a lot about the machine in order to decode it

In others, we've observed the threat actor using WMI to create service entries on the machines they target for encryption. The entries contain a long, encoded command string that is impossible to decode unless you know the specific variables it was looking for. These variables included information such as the machine name, IP address, domain, and username. If you didn't know all of these for the computer the service had been installed on, then decoding the final layers was impossible.

How the ransomware, itself, works

Sodinokibi arrives as a packed, encrypted executable that has several anti-analysis features designed to frustrate researchers. The binary files are compiled with the unique configuration and ransom note text hardcoded into the application.



A subroutine for deleting the Windows Defender definitions file in REvil

When first executed, the malware profiles the target machine, enumerates a list of the running processes, and deletes the Volume Shadow Copy, the virus definition database used by Windows Defender, and temporary or backup files used by a number of different third-party programs that may be installed on the machine.

```
"fls": [ // files
    "ntuser.dat.log",
    "desktop.ini",
    "ntuser.dat",
    "iconcache.db",
    "boot.ini",
    "thumbs.db",
    "ntldr",
    "bootfont.bin",
    "ntuser.ini",
    "bootsect.bak",
    "autorun.inf"
```

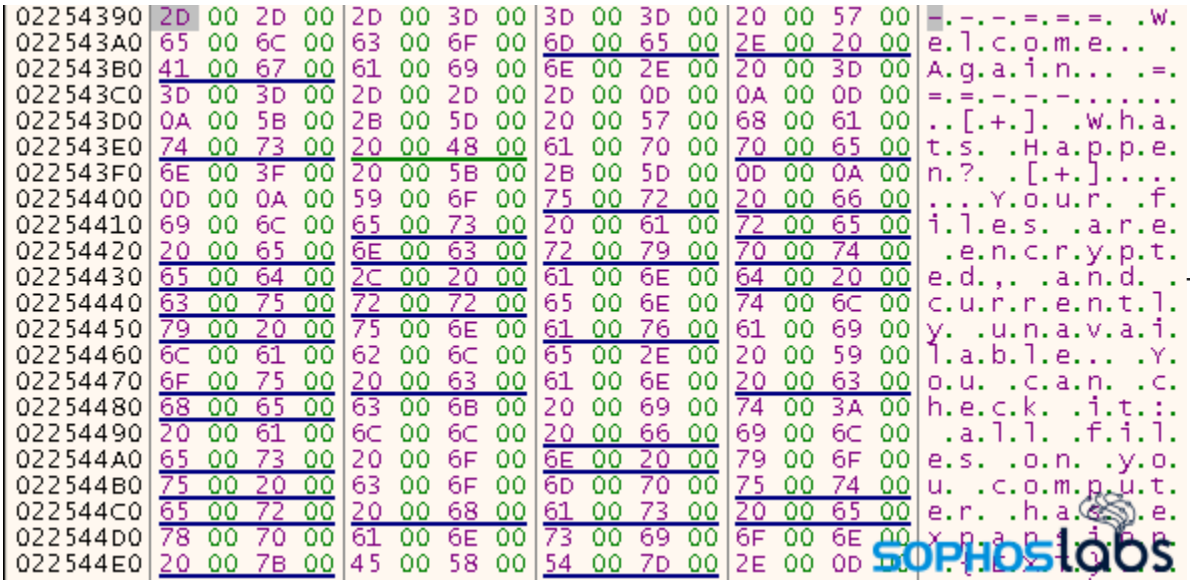
Files ignored by REvil

It searches the list of running processes for any matches to a list of process names encoded into the configuration, and then attempts to kill those processes. Among the 30-odd process names are included various database services, office applications, email clients, backup utilities, and the Firefox browser (but, oddly, no others).

```
"prc": [ // process to kill
    "tbirdconfig",
    "isqlplussvc",
    "mspub",
    "mydesktopservice",
    "xfssvccon",
    "outlook",
    "sql",
    "visio",
    "excel",
    "msaccess",
    "onenote",
    "thunderbird",
    "infopath",
    "ocomm",
    "oracle",
    "sqbcoreservice",
    "encsvc",
    "thebat",
    "steam",
    "ocssd",
    "wordpad",
    "dbeng50",
```

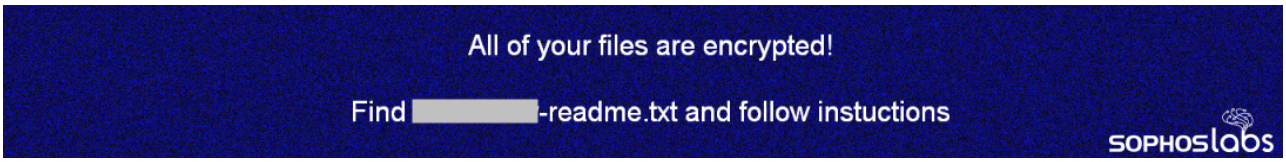
Part of the list of processes REvil tries to kill before it begins encrypting

It then enumerates the list of installed services and, at least in the case of some of the samples we received, it attempts to disable the Sophos service (these attempts routinely fail, due to tamper protection) as well as those of seven other commercial software tools.



The REvil ransom note, decrypted inside of the ransomware binary

Next, the ransomware decodes and writes out the ransom note to the root of the C: drive. The note lists a Tor website address and includes instructions on how to contact the attackers using either the Tor Browser, or with a a conventional browser on a Tor gateway website, as well as a long key that the attackers use in the decryption utility.



The ransom note notification banner

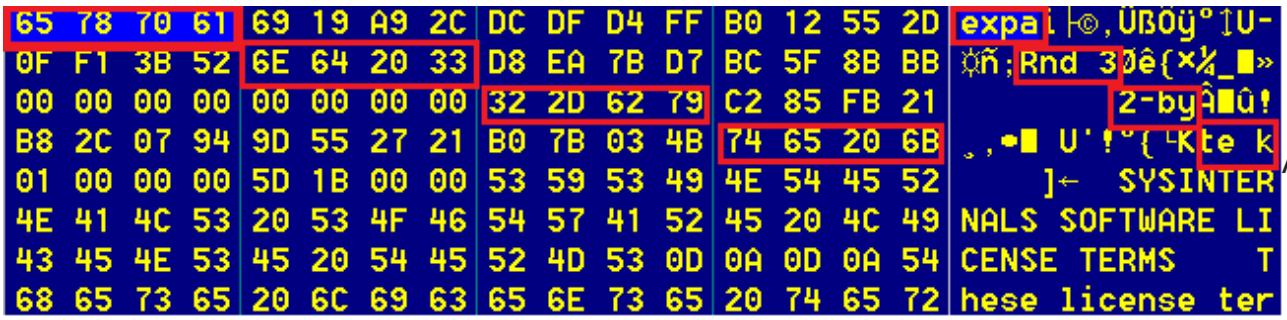
Embedded within the configuration is an encoded .bmp image file, which the ransomware writes to the *%AppData%\Local\Temp* folder and sets as the desktop image on the infected computer. The graphic says "*All of your files are encrypted! Find [name of the ransom note] for more instuctions.*" The ransom note filename starts with the same eight-random-character string the ransomware appends to the filename of every file it encrypts.

Initial state of Salsa20

"expa"	Key	Key	Key
Key	"nd 3"	Nonce	Nonce
Pos.	Pos.	"2-by"	Key
Key	Key	Key	"te k"

How the Salsa20 algorithm is used

Sodinokibi/REvil uses the curve25519/salsa20 algorithm to encrypt files. The built in configuration contains a long list of folders, file types, and specific filenames that it won't encrypt (to maintain stability of the affected computer) rather than a list of targeted filetypes.



partially encrypted file example showing how Salsa20 “steps” through a file (note the position of “expand 32-byte k”)

The ransomware does some housekeeping tasks while running. The embedded configuration contains a list of internet domain names; It sends statistics about the infection process back to the operators of the ransomware at one or more of these domains. These domains serve as strong indicators of compromise.

REvil/Sodinokibi also has switched to using the Monero cryptocurrency as its exclusive payment method. As Monero has additional privacy features that Bitcoin does not have, it’s unlikely that we’ll see a recovery of the ransom paid to a threat actor who deployed this ransomware, as the FBI was able to accomplish with the DarkSide ransomware attack against Colonial Pipeline.

Guidance for IT professionals

Sophos products detect various forms of Sodinokibi/REvil as **Troj/Sodino-***, **Mem/Sodino-***, and **HPMal/Sodino-A**.

While not an exhaustive list, these recommendations are more important than ever.

- **Monitor and respond to alerts** – Ensure the appropriate tools, processes, and resources (people) are available to monitor and respond to threats seen in the environment. It is crucial to ensure that, when a security alert or event happens, someone investigates and responds in a timely manner. Ransomware attackers may time their strike during off-peak hours, weekends, or holidays, working on the assumption that few or no staff are watching.
- **Strong passwords** – Strong passwords serve as one of the first lines of defense. As a minimum use a complex password of at least twelve characters. Password managers will help users maintain complex passwords that are unique to individual accounts. Don’t reuse passwords anywhere.

- **Multi Factor Authentication (MFA)** – Even strong passwords can be compromised. At a minimum, any form of multifactor authentication is better than none for securing access to critical resources such as e-mail, remote management tools, and network assets. TOTP MFA apps on smartphones may be safer than email or SMS-based MFA systems in the long run; In a situation where the attacker is already on the network, email may already be compromised, and SIM swapping, while rare, could compromise text message MFA codes. But don't let the perfect be the enemy of the good. MFA of any kind can save your bacon.
- **Lock down accessible services** – Perform scans of your organization's network from outside the network, and identify and lock down the ports commonly used by VNC, RDP, or other remote access tools. If a machine needs to be reachable using a remote management tool, put access to that tool behind a VPN that uses MFA as part of its login and segmented into its own VLAN away from other machines.
- **Segmentation and Zero-Trust** – At the very minimum, separate critical servers from each other and from workstations by putting them into separate VLANs as you work towards a zero-trust network model.
- **Inventory your assets and accounts** – Unprotected and unpatched devices in the network increase risk, and create a situation where malicious activities could pass unnoticed. It is vital to protect every device on your network, and the only way to do that is to have a current inventory of all connected computers and IOT devices. Use network scans and physical checks to locate and catalog them.
- **Product configuration** – Ensure that security products are configured following best practices guidance. Check policy configurations and exclusions on a regular basis. New features may not be enabled automatically.
- **Active Directory (AD)** – Conduct regular audits on all accounts in AD, ensuring that no accounts have more access than is needed for their purpose. Disable accounts for departing employees as soon as they leave the company.
- **Patch everything** – keep Windows and other software up to date. Validate that patches have been installed for critical systems like internet-facing machines or domain controllers.

Users of Sophos LiveDiscover can run SQL queries like the ones in this table to interrogate telemetry from devices on their managed network, and hunt for unusual or unexpected behavior on their managed devices.

Live Discover Query	Description
SELECT * FROM scheduled_tasks WHERE name = 'Windows Policy Update';	Check if a computer currently has the Windows Policy Update scheduled task installed on it.
SELECT * FROM scheduled_tasks WHERE name = 'Windows Autotask';	Check if a computer currently has the Windows Autotask scheduled task installed on it.
SELECT datetime, eventid, JSON_EXTRACT(data, '$.EventData.AccountName') AS AccountName, JSON_EXTRACT(data, '$.EventData.ServiceName') AS ServiceName, JSON_EXTRACT(data, '$.EventData.ImagePath') AS ImagePath, JSON_EXTRACT(data, '$.EventData.ServiceType') AS ServiceType, JSON_EXTRACT(data, '$.EventData.StartType') AS StartType FROM sophos_windows_events WHERE source = 'System' AND ImagePath LIKE '%powershell%' AND eventid = 7045 AND (ImagePath LIKE '%JABZ' OR ImagePath LIKE '%SQB%' OR ImagePath LIKE '%H4s%' OR ImagePath LIKE '%IEX%' OR ImagePath LIKE '%invoke%' OR ImagePath LIKE '%downloadstring%');	Check system event logs for the installation of services that execute suspicious PowerShell commands.
SELECT datetime, eventid, JSON_EXTRACT(data, '$.UserData.Param1') AS Name, JSON_EXTRACT(data, '$.UserData.Param2') AS Source_Machine_Network,	Check if a user has logged into a computer via RDP.

Acknowledgments

SophosLabs researchers Anand Ajjan, Hajnalka Kope, and Mark Loman and Rapid Response manager Peter Mackenzie contributed to our understanding of REvil attacks and the malware's behavior.