What to expect when you've been hit with REvil ransomware

news.sophos.com/en-us/2021/06/30/what-to-expect-when-youve-been-hit-with-revil-ransomware/

Tilly Travers June 30, 2021

REvil, also known as Sodinokibi, is a widely used, conventional ransomware-as-a-service (RaaS) offering that has been around since 2019. Criminal customers can lease the REvil ransomware from its developers, adding their own tools and resources for targeting and implementation. As a result, the approach and impact of an attack involving REvil ransomware is highly variable. This can make it hard for defenders to know what to expect and look out for.

The following information may help IT admins facing or proactively concerned with the impact of a REvil ransomware attack. The findings are based on insights from the Sophos Rapid Response team, which has investigated multiple cyberattacks involving REvil.

***Editor's note**: This article is part of a series of "What to expect" guides featuring prevalent ransomware families. Other guides cover Conti ransomware and Avaddon ransomware.*

What to do immediately: contain and neutralize

The first thing you need to do is determine whether the attack is still underway. If you suspect it is, and you don't have the tools in place to stop it, determine which devices have been impacted and isolate them immediately. The easiest option is to simply disconnect from

all networks. If the damage is more widespread than a few devices, consider doing this at the switch level and taking entire network segments offline instead of individual devices. Only shut down devices if you can't disconnect the network.

Second, you need to assess the damage. Which endpoints, servers and operating systems were affected, what has been lost? Are your backups still intact or has the attacker deleted them? If they are intact, make an offline copy immediately. Also, which machines were protected? They'll be critical in getting you back on your feet.

Third, do you have a comprehensive incident response plan in place? If not, you need to identify who should be involved in dealing with this incident. IT admins and senior management will be required, but you may also need to bring in outside security experts and consult with cyber insurance and legal counsel. Should you report the incident to law enforcement and/or inform data protection authorities? There is also the question of what information you should give to employees, many of whom are likely to find a similar ransom note on their desktop.

Last, but definitely not least: you'll need to contact these and other key people, such as customers, to let them know what's happening, but the attackers may be eavesdropping so don't use your normal channels of communication. If the intruders have been in your network for a while, they'll probably have access to email, for instance.

What to do next: investigate

Once you have managed to contain and neutralize the attack, take time to investigate what happened so you can reduce the likelihood of it happening again. If you don't feel confident about doing this yourself, there is specialist incident response and threat hunting help available 24/7 from security vendors, including Sophos.

According to the Sophos Rapid Response team, this is what you can expect from REvil/Sodinokibi ransomware activity on your network:

1. **The attackers have most likely been on your network for a few days or even weeks.**

REvil ransomware is operated by human adversaries who have leased the malware from the developers, adding their own tools and targets. They take time to prepare attacks that cause maximum disruption, which enables them to charge the multi-million-dollar ransoms REvil is known for.

Note: Malicious activity can begin before ransomware attackers arrive. Sophos experts investigating a recent REvil attack found a direct link between an inbound phishing email and a multi-million-dollar ransom attack two months later. The phishing email, which succeeded in capturing an employee's access credentials, probably came from an Initial Access Broker,

who, a few weeks later, appears to have used PowerSploit and Bloodhound to move through the breached network to locate high value domain admin credentials. The broker later sold these credentials to the REvil adversaries so they could breach the target's network.

1. **The attackers may use a variety of different methods to break in your network.**

Possible initial access methods for REvil ransomware include, but are not limited to, exploits against a known vulnerability, for example in a firewall, phishing for user credentials via spam emails as mentioned above, brute-force attacks against internet-facing services like Virtual Private Networks (VPNs), exposed remote desktop protocol (RDP), and desktop remote management tools like Virtual Network Computing (VNC), and even some cloud-based management systems.

Sites like Shodan.io provide insight into what an attacker could find out about your network; try using it to search your external IP addresses.

1. **They will have secured access to domain admin accounts as well as other user accounts.**

Attackers typically compromise multiple accounts during an attack. Their main goal is to get access to domain admin accounts that can be used to launch the ransomware. However, they also target specific admin accounts that have access to sensitive data, backup systems and security management consoles.

REvil attackers often use tools like Mimikatz, which can capture information from a running Microsoft LSASS.exe process that contains usernames/password hashes of currently logged on users. Sometimes attackers will leave this running and then deliberately break something on the machine that they've targeted, provoking an admin to log in to fix it. Attackers can then capture this admin's credentials.

If Mimikatz is blocked by security software, the attackers may instead use something like Microsoft Process Monitor to do a memory dump of LSASS.exe and take that dump file back to their machine to extract the information with Mimikatz. With Mimikatz, it doesn't matter how long or complex the passwords are because it is takes them straight out of memory.

1. **They will have scanned your network**. **They know how many servers and endpoints you have and where you keep your backups, business-critical data and applications.**

One of the first things attackers will do when they get onto a network is identify what access they have on the local machine. The next step is to find out what remote machines exist and if they can access them.

Attackers use legitimate network scanners like “Advanced Port Scanner” and “Angry IP Scanner” due to their effectiveness and the fact that they are unlikely to be blocked. These scanners will generate a list of IPs and machine names. This makes it easy for attackers to focus on critical infrastructure as most organizations helpfully give their servers descriptive names, for example NY-DC1 for the New York Domain Controller, or maybe even simpler names like “FileServer01,” “Backup_Server,” etc.

1. **The attackers are likely to have downloaded and installed backdoors that allow them to come and go on your network and install additional tools.**

They’ll have set up folders and directories to collect and store stolen information and channels for communicating with the attackers and for moving information out of your network.

The backdoors come in a variety of forms. Some just communicate back to the attackers’ IP address, allowing them to send and receive commands to the machine.

Many backdoors are classified as legitimate applications. For example, the attackers might use Remote Administration tools such as RDP to maintain access. Even if RDP is disabled by default, it is very easy for an attacker with admin access to the machine to re-enable it.

Other common legitimate tools used are Screen Connect, AnyDesk, TightVNC and PC Anywhere. This offers attackers direct control of the machine, including control over the mouse/keyboard and the ability to see the screen.

Note: In one REvil attack that Sophos investigated, the adversaries had installed the Screen Connect remote access tool onto 130 devices, roughly a third of the network, in order to maintain access if they were removed or blocked elsewhere.

Some attackers use more advanced tools such as Cobalt Strike, a post-exploitation pen-testing tool. Attackers will often try and establish a Cobalt Strike “beacon.” This allows regular communication back to the Cobalt Strike server and gives attackers complete control of the machine. It can also be used to easily deploy further beacons on other machines inside the network.

1. **In addition to the encryption of data and disruption to software and operations, some REvil operators will try to exfiltrate hundreds of gigabytes of corporate data prior to the main ransomware event.**

Sophos experts have only seen this multi-mode extortion in around half of the REvil/Sodinokibi attacks they investigated, but it is still worth being aware of the risk. The attackers will generally threaten to publish stolen sensitive data on a so-called “leak site” for anybody to download, unless they pay the ransom.

Once a file server is identified, attackers often use a tool called “Everything” that enables very fast file searching for keywords, such as “account,” “confidential,” “Social Security number.” After they identify the data, there are numerous methods the attackers can use to steal it.

For example, they could simply login to an online email service and email it somewhere or use a cloud storage provider like DropBox. Alternatively, they could install an FTP Client like FileZilla or Total Commander FTP and upload the data to their server.

Attacker often automate exfiltrating larger amounts of data. For example, they might use a tool like RClone. This is a command line tool that connects to a wide variety of cloud storage providers.

In approximately 75% of the Sophos-investigated REvil ransomware attacks that included data exfiltration used Mega.nz to temporarily store the stolen information. Mega is popular with attackers because it offers extra levels of anonymity. A few simple commands to RClone are all attackers need to exfiltrate entire directories to Mega.

Some REvil attackers use other methods, such as installing a portable copy of the FTP client FileZilla that they used to upload data to a staging server outside of the target’s network perimeter.

1. **They will have tried to encrypt, delete, reset, or uninstall your backups.**

Unless your backups are stored offline, they are within reach of the attackers. A “backup” that is online and available all the time is just a second copy of the files waiting to be encrypted.

1. **The attackers will have tried to identify what security solution is used on the network and whether they can disable it.**

It doesn’t matter how good your protection is if the attacker can turn it off or modify its policy. REvil attackers have used GMER to try to disable security software. GMER is an anti-rootkit tool that is not inherently malicious, although some security technologies will flag it as a Potentially Unwanted Application (PUA).

Sophos experts have also seen REvil ransomware attackers rebooting the computer into Safe Mode before data encryption in order to bypass endpoint protection tools.

Anyone with admin rights can instantly disable free default tools, such as Windows Defender. Most modern ransomware attempts to do this by default.

Attackers also try to find and gain access to the management consoles of more advanced security solutions in order to disable all protection just before they launch the ransomware.

Security management consoles hosted locally are especially at risk as attackers could access them with the accounts they have already compromised.

1. **The most visible part of the attack – the deployment of ransomware – probably took place when no IT admins or security professionals were online to notice and prevent the lengthy process of file encryption, possibly during the middle of the night or during the weekend.**

Note: The encryption process can take hours. An encrypted Windows endpoint will have tens or hundreds of thousands of encrypted files by the time the ransomware is done. For large fileservers this could run into the millions. This is why most targeted ransomware attacks are launched in the middle of the night, over a weekend or on a holiday, when fewer people are watching.

Up to this point, the attackers have been trying to stay hidden, but here their tactics change. They want you to know they are there and what they have done. They want you to see how much data has been lost and to understand that someone has done this maliciously and now they want a payment to decrypt the data.

This is why, in almost all ransomware attacks, encrypted files will have had a new extension name appended to the end of the file. For example, “MyReport.docx” might become “MyReport.docx.encrypted.” The ransom notes are often displayed prominently in multiple places, adding to the chaos and stress.

1. **The ransomware will have been deployed to all your endpoints and any servers that were online at the time of attack – providing that is what the attacker wanted.**

Ransomware is “deployed” like a normal application; in most attacks it doesn’t spread randomly in all directions. If your servers were encrypted, but not your endpoints, that is because the attacker chose to only target your servers.

Attackers deploy ransomware in a variety of ways. One of the most common ways that Sophos experts have seen is through a combination of batch scripts and the Microsoft PsExec tool, a great tool for executing commands on remote machines. An attacker might create a batch script that loops through a list of your IP addresses, using PsExec to copy the ransomware to each machine and then execute it.

While most security solutions (including Sophos) block PsExec by default, admins often authorize its use on their network because they find it useful too – and unfortunately the attackers know this.

Attackers could also create or edit an existing Group Policy Object (GPO) logon script. If you fail to spot this, the attack could relaunch every time a machine boots up and connects to the domain. This makes it seem like the ransomware is “spreading” when it is just caused by the GPO.

1. **The launch of the ransomware is not the end.**

Using the various access mechanisms they set up during the preparation stage, the attackers will often continue to monitor the situation and even your email communications to see how you respond. An email to the CEO stating you will be OK because they didn't encrypt the backups on Server X, could be a disaster if the attacker read it and still had access to that server.

The attacker may also wait until you recover to then launch a second attack to really emphasize that they can keep doing this until you pay.

1. **If the attackers are looking for an additional means of extortion, the time spent in your network will likely have allowed the attackers to steal business critical, sensitive and confidential information that they now threaten to publicly expose.**

Some attackers also apply emotional pressures, with direct employee or business affiliate appeals and threats over email and phone.

Most attackers will start publishing stolen data anywhere from a few days to a week after the main attack if no contact from the target is received or negotiations breakdown. However, it could be several weeks or even longer before anything gets published.

Further, while the attackers may promise to delete your information if you pay, you have no guarantees that they will.

What defenders can do

There are some proactive steps you can take to enhance your IT security for the future, including:

- Monitor your network security 24/7 and be aware of the five early indicators an attacker is present to stop ransomware attacks before they launch
- Shut down internet-facing remote desktop protocol (RDP) to deny cybercriminals access to networks. If you need access to RDP, put it behind a VPN or zero-trust network access connection and enforce the use of Multi-Factor Authentication (MFA)
- Educate employees on what to look out for in terms of phishing and malicious spam and introduce robust security policies
- Keep regular backups of your most important and current data on an offline storage device. The standard recommendation for backups is to follow the 3-2-1 method: 3 copies of the data, using 2 different systems, 1 of which is offline. Also test your ability to perform a restore
- Prevent attackers from getting access to and disabling your security: choose a solution with a cloud-hosted management console with multi-factor authentication enabled and Role Based Administration to limit access rights

- Remember, there is no single silver bullet for protection, and a layered, defense-in-depth security model is essential – extend it to all endpoints and servers and ensure they can share security-related data
- Have an effective incident response plan in place and update it as needed. If you don't feel confident you have the skills or resources in place to do this, to monitor threats or to respond to emergency incidents, consider turning to external experts for help

Further advice and technical information related to REvil ransomware can be found in MTR in Real Time: Hand-to-Hand Combat with REvil Ransomware Chasing a $2.5 Million Pay Day,and Relentless REvil, Revealed: RaaS as Variable as the Criminals Who Use It.

Conclusion

Dealing with a cyberattack is a stressful experience. It can be tempting to clear the immediate threat and close the book on the incident, but the truth is that in doing so you are unlikely to have eliminated all traces of the attack. It is important that you take time to identify how the attackers got in, learn from any mistakes and make improvements to your security. If you don't, you run the risk that the same adversary or another one might attack again in the future.