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

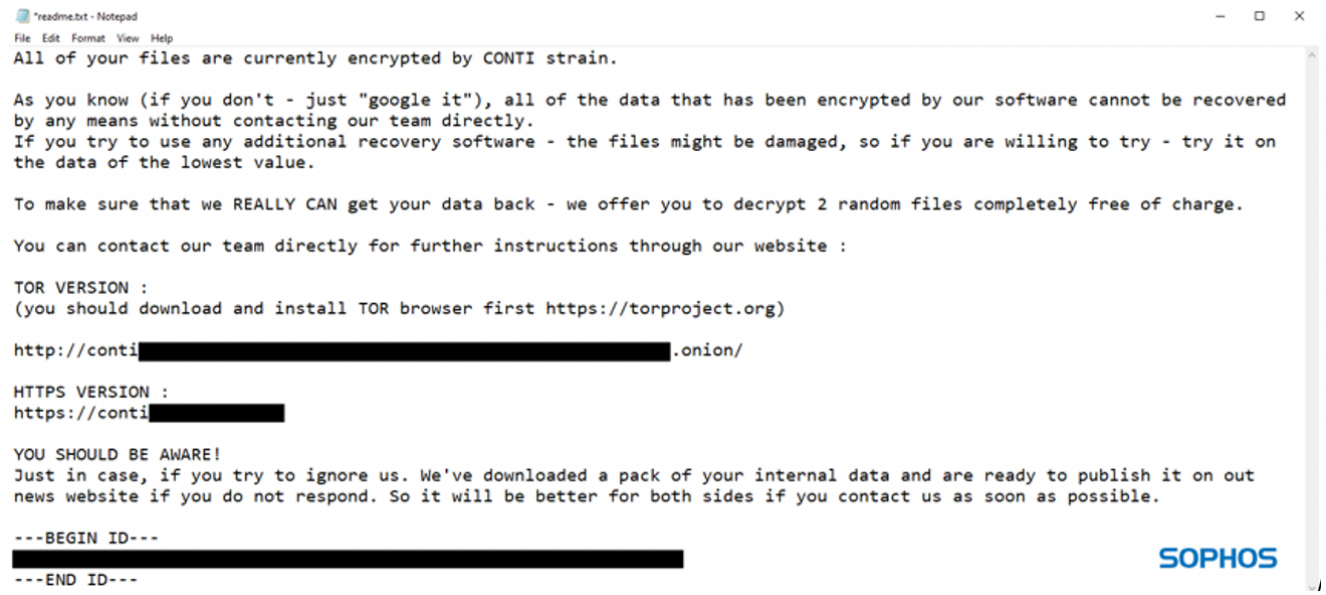
news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/

February 16, 2021

Conti ransomware appeared on the threat landscape in May 2020. It shares some similarities with other families of ransomware, but Sophos believes at this time that it is not related to them. Conti has undergone rapid development since its discovery and is known for the speed at which it encrypts and deploys across a target system. Conti is a human-operated "double extortion" ransomware that steals and threatens to expose information as well as encrypting it. The Conti News site has published data stolen from at least 180 victims thus far.

Editor's note: This is one of a series of articles focused on the Conti ransomware family, which also includes technical details of Conti ransomware, Conti Ransomware: Evasive By Nature and a detailed analysis of a Conti attack, A Conti Ransomware Attack Day-By-Day.

Imagine the scene: you're an IT admin and you turn up for work on a Monday morning to find your IT systems are down and no-one can access or run anything. On your computer screen there is a message telling you that your systems and data have been encrypted with Conti ransomware and you need to pay a ransom for the attackers to decrypt compromised files and delete stolen information.



Click the image to enlarge it

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 unplug the network cable or turn off the Wi-Fi adapter. 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.

Last, but definitely not least: you'll want to talk to people about 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 need to expect from Conti ransomware activity on your network:

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

Conti ransomware is operated by humans. They take time to prepare in order to ensure maximum disruption because this enables them to charge higher ransoms.

2. The attackers could use a variety of different methods to break in your network.

Possible initial access methods for Conti ransomware include, but are not limited to vulnerable firewalls, exposed RDP (Remote Desktop Protocol) services, and phishing user credentials via spam emails. 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.

3. 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.

Conti 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.

4. 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.

5. 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.

Another common legitimate tool used is AnyDesk. This offers attackers direct control of the machine, including control over the mouse/keyboard and the ability to see the screen.

Or they could use more advanced tools such as Cobalt Strike, a legitimate 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.

Some attackers, including Conti, also set up Tor proxies so they can send command-and-control traffic over the Tor network. Such activity is often very hard to spot.

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

Targets are threatened with the risk of their data being published on a so-called "leak site" for anybody to download, unless they pay the ransom. Some of the more valuable data is often sold to other attackers to use in further attacks.

Once a file server is identified, attackers often use a tool called "Everything" that enables very fast file searching for keywords, for example "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.

Some of the largest exfiltrations are done in a more automated way. 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. A commonly used one is MEGA as it offers extra levels of anonymity that attackers like. A few simple commands to RClone are all attackers need to exfiltrate entire directories to MEGA.

7. 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.

8. 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.

Free default tools, such as Windows Defender, can be disabled instantly by anyone with admin rights. 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.

9. The most visible part of the attack – the release 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 takes 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.

10. 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.

The ransomware can be deployed in a variety of ways. One of the most common way Sophos experts see is a combination of batch scripts and the Microsoft PsExec tool, which is 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.

11. The launch of the ransomware is not the end.

Using the backdoors 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.

12. 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 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.

Click the image to enlarge it

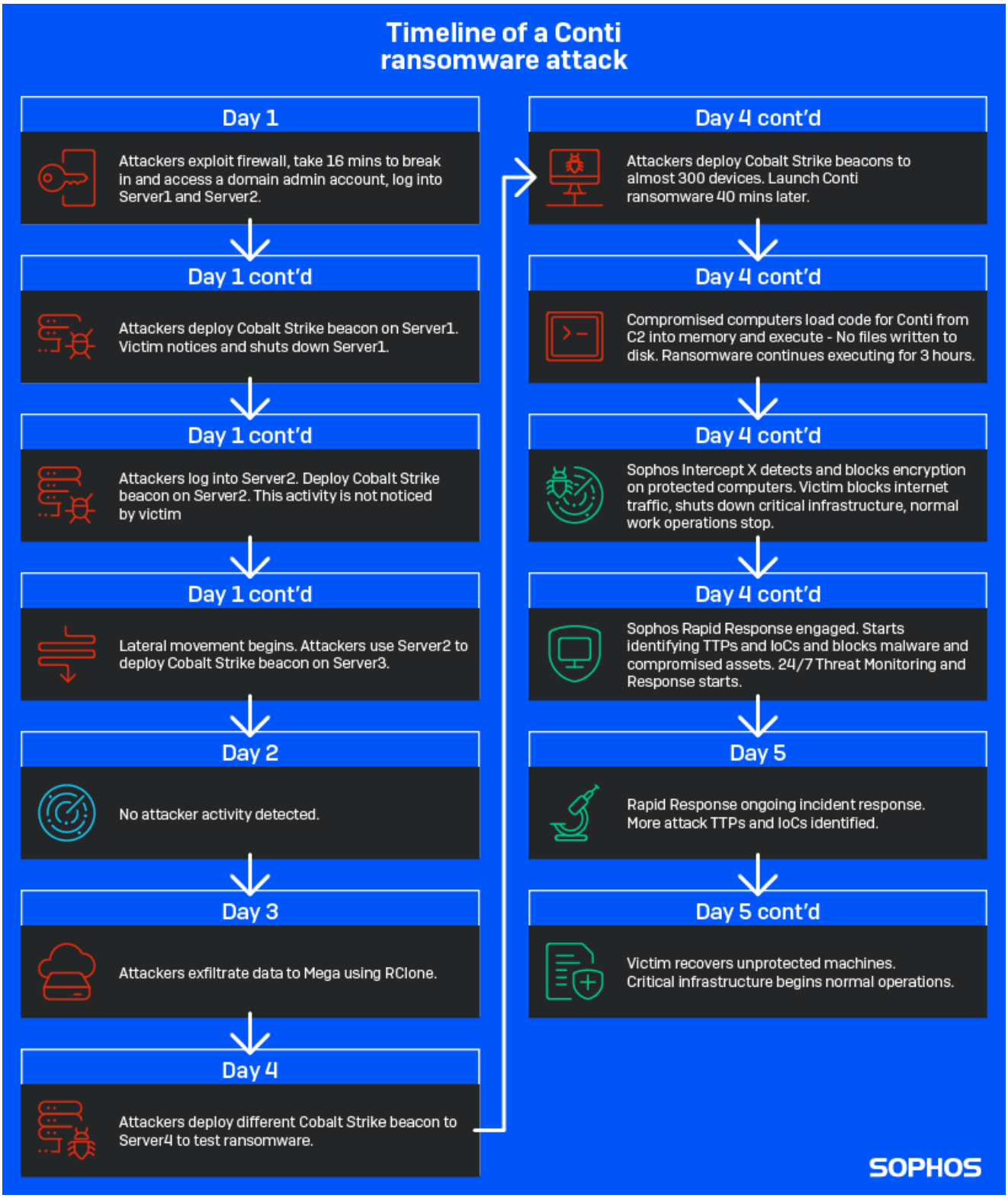
What defenders can do

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 connection and enforce the use of Multi-Factor Authentication (MFA)
- Educate employees on what to look out for in terms pf 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
- Prevent attackers from getting access to and disabling your security: choose an advanced 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, defence-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.

Conclusion



Click the image to enlarge it

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 attacker or another one might come and do this to you again next week.

Additional resources

- Technical information on Conti ransomware as well as a day-by-day analysis of a Conti attack, including indicators of compromise (IoCs) and tactics, techniques and procedures (TTPs) can be found in A Conti Ransomware Attack Day-By-Day and Conti Ransomware: Evasive By Nature.
- To help stop ransomware attacks, read the five early indicators an attacker is present
- Learn more about Sophos' Rapid Response service that contains, neutralizes and investigates attacks 24/7
- The four top tips for responding to a security incident from Sophos Rapid Response and the Managed Threat Response Team
- Learn how ransomware affects IT teams in Sophos' global survey report, Cybersecurity: The Human Challenge