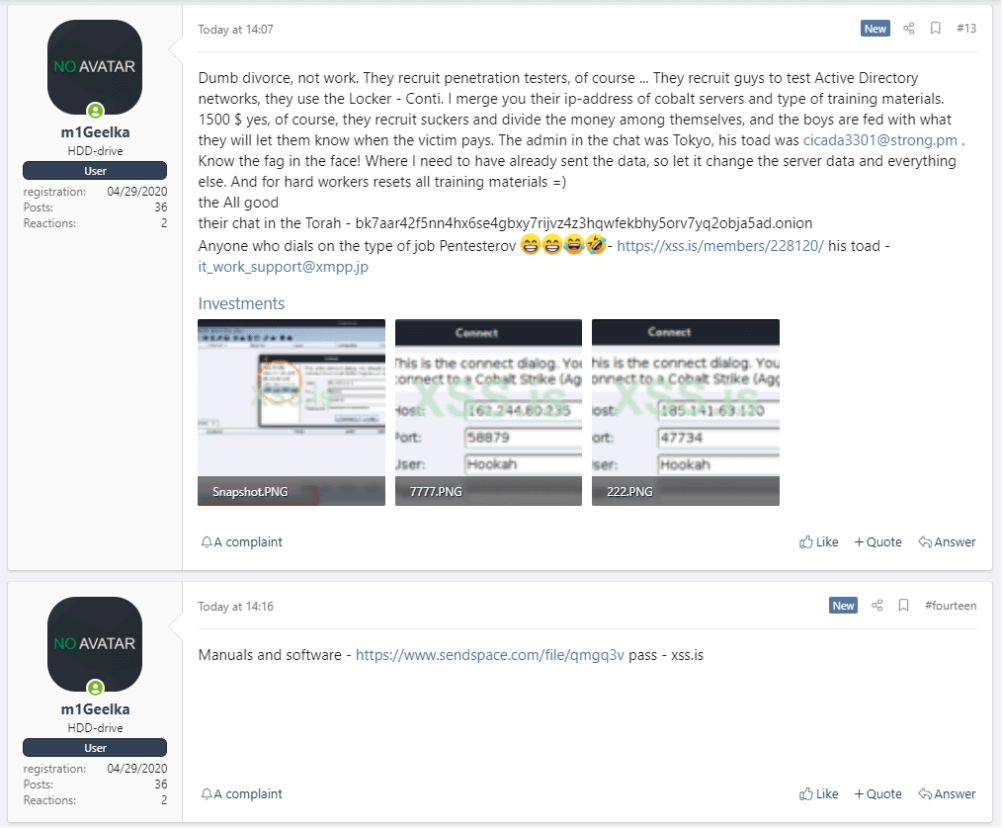
Disgruntled ransomware affiliate leaks the Conti gang's technical manuals

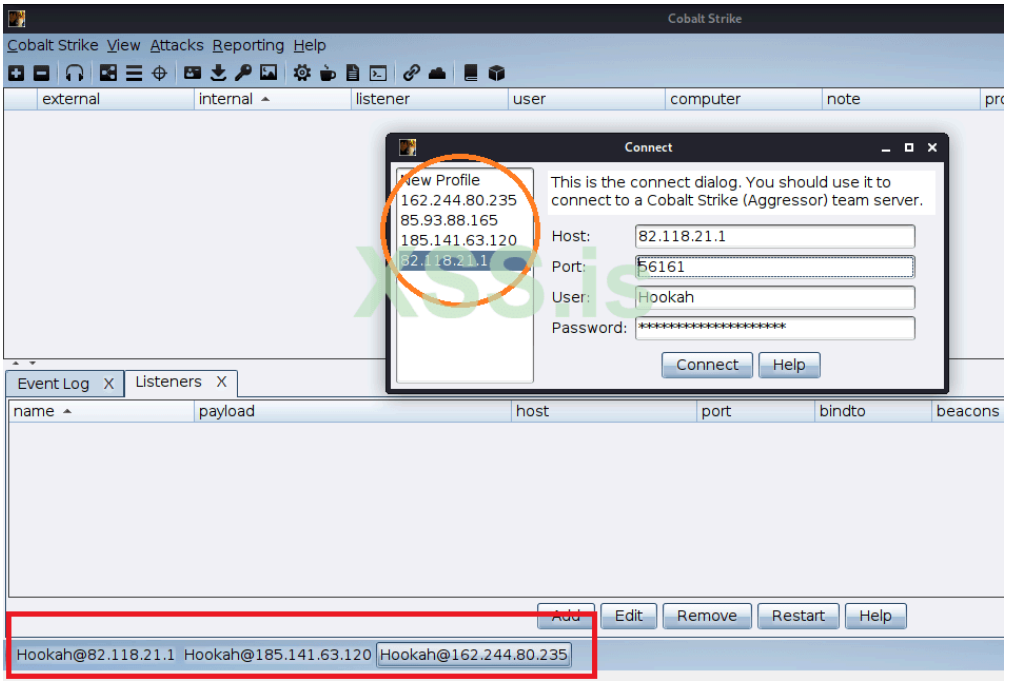
By Catalin Cimpanu

Published: 2023-01-18 · Archived: 2026-04-05 17:16:01 UTC

A disgruntled member of the Conti ransomware program has leaked today the manuals and technical guides used by the Conti gang to train affiliate members on how to access, move laterally, and escalate access inside a hacked company and then exfiltrate its data before encrypting files.

Leaked on an underground cybercrime forum named XSS earlier today, the files were shared by an individual who appears to have had an issue with the low amount of money the Conti gang was paying them to breach corporate networks.





In messages spammed across the forum, the individual shared screenshots of IP addresses where the Conti gang hosts Cobalt Strike command-and-control servers, which Conti affiliate members use to access hacked company networks.

> https://twitter.com/pancak3lullz/status/1423324601346629635

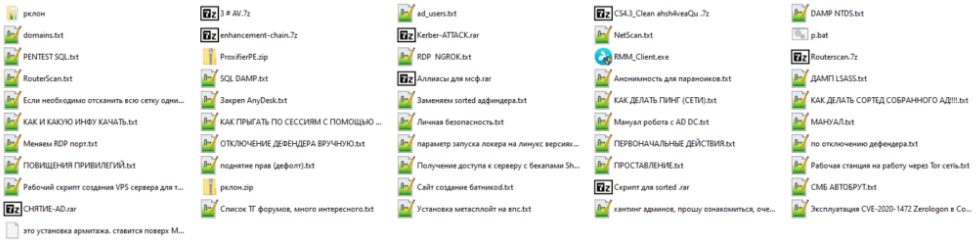
In addition, the individual also published a RAR archive named "***Мануали для работяг и софт.rar***," which roughly translates to "***Manuals for hard workers and software.rar***."

This archive contains 37 text files with instructions on how to use various hacking tools and even legitimate software during a network intrusion.

For example, the leaked manuals contain guides on how to:

- configure the Rclone software with a MEGA account for data exfiltration
- configure the AnyDesk software as a persistence and remote access solution into a victim's network [*a known Conti tactic*]
- configure and use the Cobalt Strike agent
- use the NetScan tool to scan internal networks
- install the Metasploit pen-testing framework on a virtual private server (VPS)
- connect to hacked networks via RDP using a Ngrok secure tunnel
- elevate and gain admin rights inside a company's hacked network
- take over domain controllers
- dump passwords from Active Directories (NTDS dumping)
- perform SMB brute-force attacks
- brute-force routers, NAS devices, and security cameras
- use the ZeroLogon exploit
- perform a Kerberoasting attack

- disable Windows Defender protections
- delete shadow volume copies
- how affiliates can configure their own operating systems to use the Tor anonymity network, and more



Leaks from Ransomware-as-a-Service (RaaS) operations are extremely rare; however, the data shared today isn't anything that security researchers would describe as groundbreaking.

The leaked files contain guides for basic offensive tactics and techniques that the Conti and other ransomware gangs have used during previous intrusions for years.

However, the leak will help some security firms put together stronger defensive playbooks that they can recommend to their customers in order to improve their ability to detect Conti intrusions—now knowing exactly what operations Conti affiliates might execute.

Source: https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/