Angry Conti ransomware affiliate leaks gang's attack playbook

bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/

Lawrence Abrams

By
Lawrence Abrams

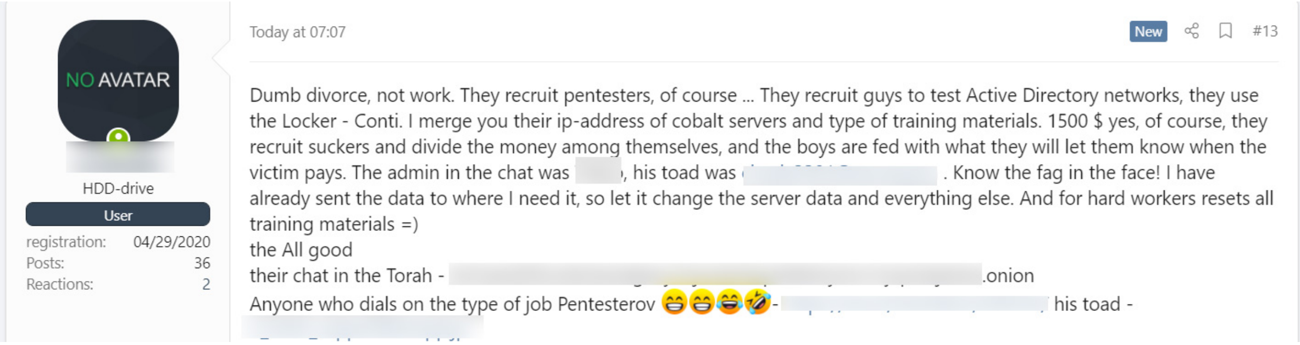
- August 5, 2021
- 02:29 PM
- 1

A disgruntled Conti affiliate has leaked the gang's training material when conducting attacks, including information about one of the ransomware's operators.

The Conti Ransomware operation is run as a ransomware-as-a-service (RaaS), where the core team manages the malware and Tor sites, while recruited affiliates perform network breaches and encrypt devices.

As part of this arrangement, the core team earns 20-30% of a ransom payment, while the affiliates earn the rest.

Today, a security researcher shared a forum post created by an angry Conti affiliate who publicly leaked information about the ransomware operation. This information includes the IP addresses for Cobalt Strike C2 servers and a 113 MB archive containing numerous tools and training material for conducting ransomware attacks.



[redacted]

HDD-drive

User

registration:	04/29/2020
Posts:	36
Reactions:	2

Today at 07:07 New #13

Dumb divorce, not work. They recruit pentesters, of course ... They recruit guys to test Active Directory networks, they use the Locker - Conti. I merge you their ip-address of cobalt servers and type of training materials. 1500 $ yes, of course, they recruit suckers and divide the money among themselves, and the boys are fed with what they will let them know when the victim pays. The admin in the chat was [redacted], his toad was [redacted] . Know the fag in the face! I have already sent the data to where I need it, so let it change the server data and everything else. And for hard workers resets all training materials =)
the All good
their chat in the Torah - [redacted].onion
Anyone who dials on the type of job Pentesterov 😁😁😂🤣- [redacted] his toad -
[redacted]

Forum post from disgruntled affiliate

The affiliate said they posted the material as he was only paid $1,500 as part of an attack, while the rest of the team are making millions and promising big payouts after a victim pays a ransom.

"I merge you their ip-address of cobalt servers and type of training materials. 1500 $ yes, of course, they recruit suckers and divide the money among themselves, and the boys are fed with what they will let them know when the victim pays," the affiliate posted to a popular Russian-speaking hacking forum.

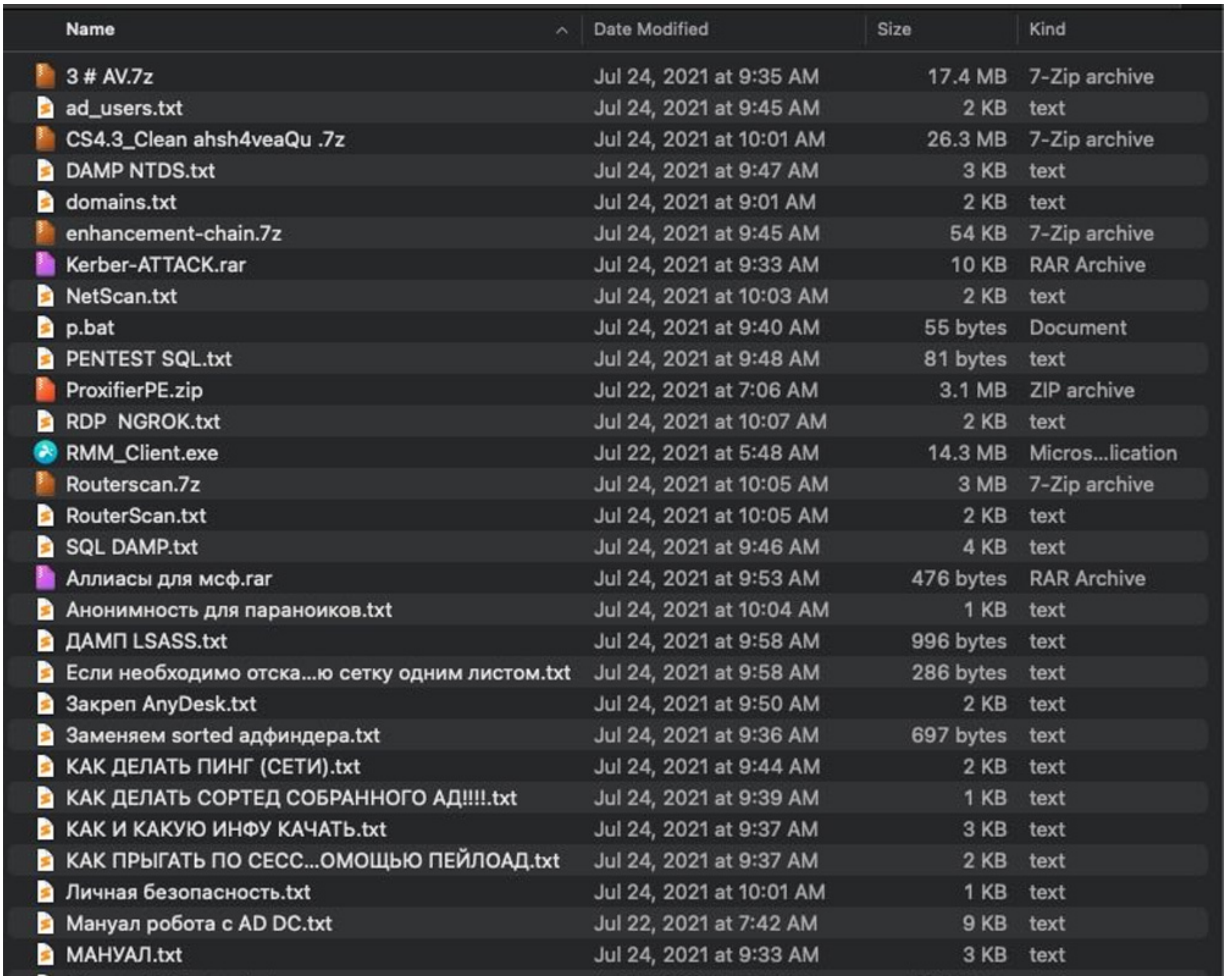
Attached to the above post are images of Cobalt Strike beacon configurations that contain the IP addresses for command and control servers used by the ransomware gang.

In a tweet by security researcher Pancak3, it is advised that everyone block those IP addresses to prevent attacks from the group.

> go block these
> 162.244.80.235
> 85.93.88.165
> 185.141.63.120
> 82.118.21.1
>
> — pancak3 (@pancak3lullz) August 5, 2021

In a subsequent post, the affiliate shared an archive containing 111 MB of files, including hacking tools, manuals written in Russian, training material, and help documents that are allegedly provided to affiliates when performing Conti ransomware attacks.

A security researcher shared a screenshot of this extracted folder with BleepingComputer. We were told it contains a manual on deploying Cobalt Strike, mimikatz to dump NTLM hashes, and numerous other text files filled with various commands.



Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал робота с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

Leaked Conti training materials

Advanced Intel's Vitali Kremez, who had already analyzed the archive, told BleepingCompter that the training material matches active Conti cases.

"We can confirm based on our active cases. This playbook matches the active cases for Conti as we see right now," Kremez told BleepingComputer in a conversation.

"By and large, it is the holy grail of the pentester operation behind the Conti ransomware "pentester" team from A-Z. The implications are huge and allow new pentester ransomware operators to level up their pentester skills for ransomware step by step."

"The leak also shows the maturity of their ransomware organization and how sophisticated, meticulous and experienced they are while targeting corporations worldwide."

"It also provides a plethora detection opportunities including the group focus on AnyDesk persistence and Atera security software agent persistence to survive detections."

This leak illustrates the vulnerability of ransomware-as-a-service operations, as a singly unhappy affiliate could lead to the exposure of carefully cultivated information and resources used in attacks.

Recently the United States government announced that its Rewards for Justice program is now accepting tips on foreign malicious cyberactivity against U.S. critical infrastructure, with a potential $10 million reward for helpful information.

Additionally, rewards through this program may be done anonymously in cryptocurrency, which could incentivize low-paid affiliates to turn on other cybercriminals.

Update 8/6/21: A source told BleepingComputer that Conti banned the pentester after learning he was poaching business away from their operation by promoting a different unidentified affiliate program.

After being banned, the affiliate leaked Conti's training material and tools as revenge.

Related Articles:

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Conti ransomware shuts down operation, rebrands into smaller units

The Week in Ransomware - May 13th 2022 - A National Emergency

Costa Rica declares national emergency after Conti ransomware attacks

US offers $15 million reward for info on Conti ransomware gang

- Affiliates
- Conti
- Playbook
- Ransomware
- Ransomware-as-a-Service

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

xrobwx71 - 9 months ago

Good info. Thanks, Grinler!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: