Angry Affiliate Leaks Conti Ransomware Gang Playbook

By Elizabeth Montalbano

Published: 2021-08-06 · Archived: 2026-04-05 14:05:14 UTC

The data includes IP addresses for Cobalt Strike C2 servers as well as an archive including numerous tools and training materials for the group, revealing how it performs attacks.

An apparently vengeful affiliate of the Conti Gang has leaked the playbook of the ransomware group after alleging that the notorious cybercriminal organization underpaid him for doing its dirty work.

A security researcher shared a comment from an online forum allegedly posted by someone who did business with Conti that included information integral to its ransomware-as-as-service (RaaS) operation, according to a report.

RaaS is a model in which an experienced ransomware developer creates and manages all the tools and infrastructure needed to perform attacks, while recruited affiliates do the actual heavy lifting. Usually they agree to be paid a percentage — typically 20 percent to 30 percent — of the ransom earned.

Apparently, the group didn't pay one disgruntled affiliate as much as expected, leading to an online rant and a leak of key data representing "the holy grail of the pen-tester operation behind the Conti ransomware 'pen-tester' team from A-Z," ethical hacker and security researcher Vitali Kremez said, according to the report.

Data revealed by the post included the IP addresses for the group's Cobalt Strike command-and-control servers (C2s) and a 113MB archive that contains numerous tools and training material for how Conti performs ransomware attacks, according to the report, which was later verified by Kremez on Twitter.

The affiliate said he received only $1,500 for his work, grumbling that "they recruit suckers and divide the money among themselves."

How to Defend Your Networks from Conti

Based on the leaked playbook, Kremez tweeted a warning for network administrators looking for Conti activity to "scan for unauthorized Atera Agent installations and Any Desk persistence:"

https://twitter.com/VK_Intel/status/1423386268990251008

Kremez also told BleepingComputer that the playbook "matches the active cases for Conti as we see right now."

Another security researcher, who goes by @Pancak3 on Twitter, advised everyone in a tweet to block several IP addresses to avoid attacks by the group, which were revealed in the data as ones being used by Conti:

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

Ransomware Rising

While the leak is a blow to the activities of the Conti operators, it also provides other threat actors tools they need to build up skills to conduct attacks of their own, Kremez told BleepingComputer.

“The implications are huge and allow new pen-tester ransomware operators to level up their pen-tester skills for ransomware, step-by-step,” he said, according to the report.

Overall, ransomware gangs have been on the run lately, with mounting pressures and crackdowns from international authorities that already have led to the shutdown of some key players, including REvil and DarkSide.

Meanwhile, new threat groups that may or may not have spawned from the previous ranks of these cybercriminal organizations are sliding in to fill the gaps they left. Haron and BlackMatter are among those that have emerged recently with intent to use ransomware to target large organizations that can pay million-dollar ransoms to fill their pockets.

Source: https://threatpost.com/affiliate-leaks-conti-ransomware-playbook/168442/