Conti Ransomware: Inside One of the World's Most Aggressive Ransomware Groups

By Flashpoint Intel Team

Published: 2022-10-04 · Archived: 2026-04-05 21:47:18 UTC

The Conti ransomware group has become one of the most notorious cybercrime collectives in the world, known for its aggressive tactics and large scale attacks against a wide range of public and private organizations. Along with other prominent ransomware groups, Conti has underlined the importance of preparing a strong response plan to mitigate the effects of what could be an incredibly damaging blow to a company's assets, personnel, and reputation.

But while it maintains its place as one of the most prolific ransomware gangs to exist in the cyber threat landscape, Conti has also gained a significant amount of attention in 2022 for activity related to potential internal divisions. Leaked private chats between Conti members and a fracture of the group have left observers questioning the future of the ransomers, prompting a look back on how it became such a fixture in the ransomware landscape.

Understanding this background is not only critical to your organization's knowledge of Conti specifically, but also gives important context to ransomware threats as a whole.

Recommended Reading: ***The Great Cyber Exit: Why the Number of Illicit Marketplaces Is Dwindling***

The formation of Conti

Led by Russia-based threat actors, the Conti ransomware variant was first observed in or around February 2020, and the collective quickly became one of the most active groups in the ransomware space. In August 2020, months after its initial debut, the threat actors distributing Conti launched a data leaks site to post confidential documents obtained by attackers. By the end of 2020 the site had leaked the data of more than 150 companies, making them the third most active ransomware leaker group that year, behind only "Maze" and "Egregor."

Conti operates using a Ransomware-as-a-Service (RaaS) attack model, paying affiliates for successfully deploying the malware into an organization's system and opening the door for the primary threat actors to further exploit and coerce the victim during the second stage of the attack. Their attack model and structure was exposed in August 2021, when a former Conti affiliate leaked Conti training documents. The threat actor claimed that Conti exploits their affiliates for cheap labor, offering only a small share of the profits.

Although not confirmed, there are several indications that the threat actors behind Conti also operate "Ryuk" ransomware—a group of Russia-based threat actors frequently referred to as "Wizard Spider." Security company CrowdStrike, which refers to the threat actors behind Ryuk as "Wizard Spider," has stated that it "is clear that WIZARD SPIDER is now running multiple [Conti and Ryuk] ransomware operations." Security researcher Brian

Krebs and news site BleepingComputer, among others, have also claimed that the two ransomware strains must be operated by the same group because of code reuse and other similarities in their operating structure.

Although the similarities between the two ransomware strains are notable and the strains may well be run by the same group, Flashpoint has not yet observed definitive proof of dual attribution.

Tactics, techniques, and procedures: A Conti attack in action

Although Conti is officially considered a RaaS variant, it differs slightly in how it structures its model and the payment of its affiliates who are responsible for gaining access to a victim's network. It is believed that rather than giving these initial deployers a percentage of whatever ransom is taken from the victim, affiliates are paid a set wage. Once the affiliates have gained access, the ransomware operators move into the execution phase of the attack using techniques that have become notoriously aggressive.

Recommended Reading:** **Ransomware-as-a-service: The new face of industrialized cybercrime

Stage 1: Gaining access to the victim's infrastructure

Several methods to infiltrate a victim's network have been observed in Conti attacks.

- **Spearphishing campaigns** target individual users with tailored emails that contain malware, either in malicious links or malicious attachments which distribute the malware onto the victim's device. Attachments, like documents, often also contain embedded scripts that download other malware, like TrickBot or Cobalt Strike, which are used in later stages of the attack and to assist with deeper network infiltration. The eventual goal is to deploy Conti ransomware.
- **Remote Desktop Protocol exploitation** uses stolen or weak RDP credentials in order to directly gain access to an organization's device, giving the malware access to data and files it can encrypt.
- **Purchasing access from "network access brokers"** allows Conti ransomers to buy their way into a network by paying other groups that have already obtained access in a previous breach or attack.

Stage 2: Lateral movement into the victim network

Once the initial malware has been deployed and the threat actors are in, the goal is to continue moving deeper into the network in order to access more data and files, giving attackers better leverage against the victim organization.

Along with the malware that is downloaded onto a victim's device, regardless of which technique is used during the first stage, backdoor malware that connects the device to Conti's command-and-control (C2) server is also downloaded. Second-stage C2 malware and file encryption tools are downloaded and penetration tools like Cobalt Strike beacon and AdFind, a command line tool to query active directory, are employed remotely, spreading through the network. It is also possible for Conti to spread via Server Message Block (SMB), and SMB exploitation is one strategy used to encrypt data on other endpoints within the same network domain.

As it spreads, Conti detects security tools and will attempt to disable them in order to protect its malware, also scanning the environment it is in to determine if it is a sandbox environment used specifically for malware analysis.

The threat actors also launch Kerberos attacks meant to obtain credentials and conduct brute force attacks, further escalating the access it has to a network and allowing for more lateral movement within the domain. They will often employ backdoors to allow them to re-enter at a later time and commit further espionage and monitor activity. This may include monitoring email correspondence that gives information about how victims are planning to address the attack, which gives them yet another advantage when it comes time to negotiate.

Stage 3: Encryption and deletion

Once attackers have located and compromised high-value data, it is exfiltrated to a server controlled by Conti, and multi-threaded encryption is used to encrypt files quickly.

Other components of Conti ransomware's encryption method and overall design make it very difficult to detect an attack. Security programs that would normally be able to automatically detect an attack are no longer able to do so, and signs of infection are minimized so that days or weeks may go by before the encryption is organically noticed by a user trying to access the affected data and files.

Stage 4: Exfiltration and extortion

It is standard for Conti attackers to delete file backups that might help victims lessen the damage done to their encrypted data. But before doing so, it is also common for these backups to be exfiltrated and saved for later, when they can be used as blackmail to threaten data leaks. As a result, victims are left with no quick way to recover their lost files and are more likely to consider complying with demands to restore access.

Conti maintains a leak site that is used to publicly reveal stolen data and sensitive information about an organization, and regularly posts about its victims as part of its extortion process. In recent times, the group has used these data leaks as a way to prevent victims from sharing private negotiation chats between Conti and its victim with any outside party.

It has stated that any victim who releases its private messages with the collective will have its opportunity to negotiate terminated, and all stolen data will be leaked automatically. It has also announced that in the event a victim chooses to release private chats after the attack has ended and its files have been deleted from Conti servers, Conti will choose another victim's data to publish as a form of collective punishment.

Excessive aggression towards victims

While Conti ransomware sets itself apart with its advanced capabilities and technical specifications, the behavior of the people behind Conti is equally challenging for its victims to deal with.

Where most ransomware groups make an effort to provide good "customer service" and hold up their end of the negotiation, Conti has been observed on multiple occasions to blatantly disregard promises made to victims and hurt them even if the victim agrees to pay. The group does not seem to care about its reputation, meaning that

victims of a Conti attack must consider the possibility that compliance may still result in leaked data or files to remain encrypted.

Notable Conti attacks

Conti has had hundreds of victims, and some have gained particularly significant widespread attention because of the tactics used or the scale of the attack.

JVCKenwood

In September 2021, Conti targeted the Japanese electronics manufacturer JVCKenwood. The company, which is headquartered in Yokohama, Japan and is known internationally for its car and home electronics, was demanded to pay $7 million for the return of approximately 1.7 terabytes of stolen and encrypted data.

During the attack, private chats between Conti and JVCKenwood were leaked to journalists, prompting Conti members to cease negotiations and leak the stolen data as a warning to future victims against publicizing communications with the ransomware group.

Ireland's Health Service

In May 2021, Ireland's Health Service was forced to shut down its IT systems after Conti attacked the nation's public healthcare system. The shutdown wreaked havoc on the entire healthcare infrastructure, limiting access to medical and diagnostics records and slowing response times.

Conti alleged that members had network access for two weeks, gathering 700GB of unencrypted data including confidential patient information and financial statements. The group asked for a ransom of $19,999,000 in order to provide a decryptor and delete the stolen data.

Costa Rican Government

In April 2022, Conti attacked the Costa Rican government's network, prompting officials to declare a national emergency on May 8. The breach spread to multiple government bodies, taking 27 government agencies offline for an extended period of time, and certain branches were unable to resume operations until early June.

Conti initially asked for a payment of $10 million, but increased its asking price to $20 million after the government refused to cooperate with the group's demands.

Shortly after the attack, Conti took part of its operation offline and announced that the Conti brand was over, signaling the beginning of the end for this famous ransomware strain as the world knew it. There is speculation that this final Conti attack against the Costa Rican government was in part a tactic to take attention away from the gradual shutdown of its operations.

The death of the Conti brand

The Russia-Ukraine war has played a major role in Conti members taking the ransomware group offline, though it is unclear if the war was the direct cause or simply a contributing factor. Signs of its impact began soon after the

war officially began in February 2022.

On February 25, one day after Russia's invasion of Ukraine started, Conti released a statement of pro-Russia support that proved to be unpopular with members and the outside world alike. "Conti" announced "full support" to the Russian government and added that cyberattacks or any kind of "war activities" would result in retaliation, including threats to critical infrastructure. The collective did not specify where the retaliation would be targeted.

A dying business

This declaration of support and the group's threat to essentially act on Russia's behalf made the group untouchable to most would-be victim companies, with almost no payments made to the group in the months after its pledge of Russian allegiance.

While potential payment to any ransomware group should be discussed with law enforcement to ensure it is legally permissible, Conti positioning itself as an extension of Russia made financial support to the group especially toxic. This cut off a significant portion of the group's income, damaging its ability to operate.

An insider scorned

Just four days after the official start of the Russia-Ukraine war, and in the wake of Conti's announcement of its support for Russia, an insider leaked tens of thousands of internal chat logs to the public. Documents revealed the group's size, its day-to-day activities, and how this cybercrime "company" was structured, showing that, in many ways, Conti operated as any normal business would.

Chats about salary structures and HR recruitment procedures divulged that the group used legitimate Russian headhunters to find new employees, and that performance reviews, training opportunities, and an "employee of the month" program were all part of the deal when working for Conti. Perhaps most surprisingly, there was evidence that some employees were unaware that they were working for cybercriminals at all—instead, they were told that it was an ad company, or that they were creating penetration testing software and needed professionals who were able to work discreetly. If one of these unknowing employees learned who they were actually working for, they were offered a bonus to stay and keep silent.

The leak also included the source code of Conti ransomware, possibly the most damaging part of this leak for the group. The whistleblower's final message via their anonymous Twitter account was a message of support for Ukraine, confirming that the leak stemmed from internal political disagreements.

There are indications from the chats that the end was near for Conti even before this leak put the final nail in the coffin. Records show that salary payments stopped in January 2022, and some users that were significant to the operation became inactive. Activity on the Conti blog did eventually resume, so it is likely that these users moved to a new chat after the leak.

The hunt for Conti

Since then, the U.S. Department of State's Transnational Organized Crime Rewards Program has put out a reward offering of $10 million USD for information leading to the identification of key members of the Conti group. This

notice is separate from events related to the group's activity during the Russia-Ukraine war, and specifically mentions the group's attack against Costa Rica, which wreaked havoc on the country's foreign trade.

The future of Conti

At this point, it is unclear whether Conti is truly gone, or if the group (or certain members) are simply taking the time to restructure and make a comeback in the future. There is doubt from many that Conti will stay closed forever, in part because of how sophisticated its technology was and how established it became.

It is possible that Conti will not return by name, but instead rebrand itself. For now, the group has stayed mostly silent.

A possible successor?

The world of ransomware is guarded by a revolving door, which means that when one group exits, a new one is never far behind. First discovered in July 2021, Diavol ransomware has been observed to use some of the same attack components as Conti. With Conti now potentially out of the ransomware race, this begs the question of whether Diavol could become the next notorious ransomware operation.

In October 2021 the FBI officially linked Diavol to WizardSpider, the malware developer also suspected to be behind Conti. Although the relationship between WizardSpider and Conti is still unconfirmed by Flashpoint, this possible connection further solidifies the theory that Diavol may come more to the forefront as Conti takes a back seat.

Identify and mitigate cyber risks with Flashpoint

Never miss a development across illicit communities and protect your assets, stakeholders, and infrastructure by identifying emerging vulnerabilities, security incidents, and ransomware attacks. Get a free trial today and see Flashpoint's extensive collections platform, deep web chatter, and dark web monitoring tools in action.
