Conti ransomware explained: What you need to know about this aggressive criminal group

By Lucian Constantin

Published: 2022-05-31 · Archived: 2026-04-05 22:44:45 UTC

Conti has been one of the most aggressive ransomware operations over the past two years and continues to victimize many large companies as well as government, law enforcement and healthcare organizations. Researchers warn that unlike other ransomware groups that generally care about their reputation, Conti doesn't always deliver on its promises to victims.

"Usually, the more successful ransomware operators put a lot of effort into establishing and maintaining some semblance of 'integrity' as a way of facilitating ransom payments from victims," researchers from Palo Alto Networks said in an analysis. "They want to establish stellar reputations for 'customer service' and for delivering on what they promise—that if you pay a ransom, your files will be decrypted (and they will not appear on a leak website). Yet in our experience helping clients remediate attacks, Conti has not demonstrated any signs that it cares about its reputation with would-be victims."

Conti first appeared in late 2019 and has slowly grown to become one of the predominant ransomware-as-a-service (RaaS) operations. It's believed to have some connections to the Ryuk ransomware, which was run by a Russian cybercrime group known as Wizard Spider. The US Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) said in a recent alert that they observed the use of Conti ransomware in over 400 attacks against US and international organizations. According to cybercrime intelligence firm Recorded Future, Conti was the ransomware strain responsible for the second largest number of victims in September 2021 after LockBit.

Conti also operates a little differently than other RaaS groups. Most groups work with partners called affiliates to compromise victims and deploy the ransomware program for a percentage of the ransom payments, but Conti is believed to pay a monthly wage to its developers.

The rebranding of Conti

In May 2022, security intelligence companies reported that the Conti infrastructure, including its official website, negotiation service, chat rooms and messengers were shut down or being reset. Researchers from security firm AdvIntel believe that the group is shutting down the Conti brand and will likely splinter off into separate teams, a process that began months ago and has accelerated recently.

It also comes after Conti launched a major ransomware and data leak extortion attack in April that impacted at least 27 Costa Rican government organizations causing disruptions in its customs and taxes platforms and impacting foreign trade and public payroll payments. This prompted the country's president Rodrigo Chaves to declare a state of national emergency on May 8.

Chaves called the Conti group terrorists and said there are indications people inside the country are collaborating with the group. In response, the Conti attackers claim to have released over 650GB of data taken from Costa Rican government systems after the government refused to pay the $10 million extortion fee. The U.S. State Department put up a reward of $10 million for information related to the identity or location of Conti's leaders as well as $5 million for information leading to the arrest of any Conti co-conspirator from any country.

"This shutdown highlights a simple truth that has been evident for the Conti leadership since early Spring 2022 – the group can no longer sufficiently support and obtain extortion," AdvIntel researchers said in a report. "The blog's key and only valid purpose are to leak new datasets, and this operation is now gone. This was not a spontaneous decision, instead, it was a calculated move, signs of which were evident since late April. Two weeks ago, on May 6, AdvIntel explained that the Conti brand, and not the organization itself, was in the process of the final shutdown. As of May 19, 2022, our exclusive source intelligence confirms that today is Conti's official date of death."

Conti also took a significant public relations hit in the cybercrime world when following Russia's invasion of Ukraine it announced its full support for the Russian government and threatened retaliatory cyber attacks against the critical infrastructure of any countries that attacked Russia. Other ransomware groups took the opportunity to distance themselves from the conflict and declare their political neutrality. Conti later tried to backtrack and said in a new message that it doesn't ally with any government and condemns the war, but the reputational damage was already done.

This was followed by a security researcher leaking tens of thousands of messages from Conti's chat communication system, giving the infosecurity industry and the whole world a deeper look into how the operation was being run.

While the Conti brand might indeed be dead, the people connected to it will likely continue to engage in cybercriminal activities as part of other teams under different names. Some of these spin-off teams have already existed inside the Conti group — for example, a data extortion group called KaraKurt or a new ransomware operation called Black Basta that's possibly related to Conti.

How Conti gains initial network access

The attackers using Conti employ many methods of obtaining access to corporate networks, including buying access from other groups that already have such access—the so-called network access brokers. Like Ryuk, Conti operators have used the TrickBot malware for access, as well as other Trojans such as IcedID. These Trojans are typically distributed through spear-phishing emails containing malicious links or Microsoft Word attachments.

Stolen or weak Remote Desktop Protocol (RDP) credentials are also a common method of entry into networks for Conti and all ransomware groups. CISA and FBI advisory also mention fake software promoted via search engine optimization, malware distribution networks like ZLoader, and the exploitation of vulnerabilities in external IT assets as other common methods of Conti affiliates gaining access. In intrusions investigated by Sophos that resulted in Conti deployment, the company observed the exploitation of FortiGate firewall appliances running vulnerable firmware.

How Conti moves laterally

Once inside a company, the hackers use a collection of tools to map the network and expand their access. Researchers have seen the use of the Cobalt Strike attack framework and a penetration testing tool called Router Scan that can scan for and brute-force web administrative credentials of routers, cameras and network-attached storage devices.

The attackers also launch Kerberos attacks with the goal of obtaining the administrator hash and conducting brute-force attacks. Many groups, including Conti, use common tools such as Windows Sysinternal or Mimikatz to obtain user hashes and plaintext credentials that enable privilege escalation and lateral movement inside the domain.

Conti affiliates have also been observed exploiting well-known Windows vulnerabilities inside networks such as SMB Server (including EternalBlue), PrintNightmare (CVE-2021-34527) in the Windows Print spooler service, or Zerologon (CVE-2020-1472) in Microsoft Active Directory Domain Controller systems.

How Conti encrypts files and deletes backups

The Conti attackers don't deploy the ransomware directly and instead rely on more lightweight loaders that can evade antivirus detection. The group has used the Cobalt Strike and the Meterpreter (Metasploit) implants, as well as a loader called getuid to inject the ransomware directly into memory.

"Because the reflective loaders deliver the ransomware payload into memory, never writing the ransomware binary to the infected computer's file system, the attackers eliminate a critical Achilles heel that affects most other ransomware families: There is no artifact of the ransomware left behind for even a diligent malware analyst to discover and study," researchers from Sophos said in an analysis earlier this year.

The ransomware also obfuscates its strings and Windows API calls by using hash values instead of API functions and adding another layer of encryption on top of it. All this is meant to make both automated detection by security programs and manual reverse-engineering hard.

Another interesting aspect of the Conti ransomware is that it supports command line execution parameters that instruct it to encrypt either the local disk, a particular network share or even a list of network shares defined in a file. "The notable effect of this capability is that it can cause targeted damage in an environment in a method that could frustrate incident response activities," researchers from VMware said in an analysis. "A successful attack may have destruction that's limited to the shares of a server that has no internet capability, but where there is no evidence of similar destruction elsewhere in the environment. This also has the effect of reducing the overall 'noise' of a ransomware attack where hundreds of systems immediately start showing signs of infection. Instead, the encryption may not even be noticeable for days, or weeks, later once the data is accessed by a user."

Conti uses the AES-256 algorithm to encrypt files with a public key that's hard-coded in the ransomware program. This means that each binary is specifically crafted for each victim to ensure that victims have a unique key pair. It also allows the program to encrypt files even if it's unable to contact a command-and-control server.

The Conti attackers also put a lot of effort into complicating restoration efforts. The malware starts by disabling and deleting the Windows Volume Shadow copies, but then also iterates through around 160 commands to disable various Windows system services including some associated with third-party backup solutions including Acronis VSS Provider, Enterprise Client Service, SQLsafe Backup Service, SQLsafe Filter Service, Veeam Backup Catalog Data Service and AcronisAgent.

Data exfiltration for double extortion

According to a report from security firm AdvIntel, Conti doesn't only delete backups, but also leverages the backup services to exfiltrate data so they can later blackmail victims with threats of data leaks. "Conti hunts for Veeam privileged users and services and leverages to access, exfiltrate, remove and encrypt backups to ensure ransomware breaches are un-backupable," the company's researchers said. "This way, Conti simultaneously exfiltrated the data for further victim blackmailing, while leaving the victim with no chances to quickly recover their files as the backups are removed."

The Conti attackers have also been observed often using the Rclone open-source utility to upload company data to cloud-based file hosting services like Mega.

Like most ransomware groups these days, Conti maintains a data leak website where it posts information about new victims. The group has recently become annoyed with the fact that its ransom negotiation chats with victims are being leaked to journalists. This happens because such negotiations happen through a victim-specific "payment sites" set up by the attackers that are usually included in the ransom notes left to the victims. If the ransom notes are uploaded to services like VirusTotal, malware researchers can find the payment sites and implicitly see the communication there between victims and the group.

In a recent blog post, the group threatened to release the data from any victim it's negotiating with if the chats are leaked during the negotiation. This has recently happened after the group compromised Japanese electronics manufacturer JVCKenwood. "For instance, yesterday, we have found that our chat with JVCKenwood whom we hit a week ago got reported to the journalists," the group wrote. "Despite what is said in the article, the negotiations were going in accordance with a normal business operation. However, since the publication happened in the middle of negotiations it resulted in our decision to terminate the negotiations and publish the data. JVCKenwood has been already informed. Moreover, this week we have once again spotted screenshots from our negotiation chats circulating over social media."

Moreover, the group warned that if the negotiation chats are leaked after the ransom is paid and the victim's files are deleted, it will publish the data stolen from another victim in a form of collective punishment.

How to mitigate Conti attacks

The joint FBI and CISA advisory contains general ransomware mitigation advice and additional resources, including recommendations such as using multi-factor authentication for accounts, implementing network segmentation and traffic filtering, scanning for software vulnerabilities and keeping software products up to date, removing unnecessary applications and applying software execution restrictions and controls, restricting remote

access such as RDP and limiting access to resources over the network, auditing and limiting the use of administrative accounts and implementing endpoint and detection response tools.

The advisory also contains a link to a list of Conti Indicators of Compromise (IOCs) and the techniques and procedures used by the group are described in the MITRE ATT&CK framework.
