In late January 2022, ThreatLabz identified an updated version of Conti ransomware as part of the global ransomware tracking efforts. This update was released prior to the massive leak of Conti source code and chat logs on Februrary 27, 2022. The leaks were published by a Ukrainian researcher after the invasion of Ukraine. However, since these leaks were published, the Conti gang has continued to attack organizations and conduct business as usual. While two versions of Conti source code have been leaked, the most recent ransomware code has not yet been leaked. This blog will highlight the most recent changes to the ransomware and how Conti improved file encryption, introduced techniques to better evade security software, and streamlined the ransom payment process.

Technical Analysis

The most recent Conti update introduced a number of new features and changes to the ransomware code. Some of these modifications include new command-line arguments that are highlighted in bold in Table 1.

Command-Line Argument	Description
-log	Previously used to log ransomware actions; this functionality has been removed, but the command-line switch remains an artifact from the previous version
-path	Start encryption using the specified path as the root directory
-size	Size parameter for large file encryption
-mode	Encryption mode local (disks) or net (network shares); the all and backups options were removed
-user	Log in to Windows Safe Mode as the specified user
-pass	Log in to Windows Safe Mode as the user with the corresponding password
-safeboot	Force reboot the system and launch Conti in Windows Safe Mode
-disablesafeboot	Disable Windows Safe Mode and reboot the system (used after file encryption occurs in Windows Safe Mode)
-nomutex	Previously used to prevent the creation of a mutex; currently unused

Table 1. Conti command-line arguments updated in January 2022

The functionality for the command-line arguments -log and -nomutex was removed. The new command-line parameters that were added are related to features that enable Conti to reboot the system in Windows Safe Mode with networking enabled and then start file encryption. By booting in Safe Mode, Conti can maximize the number of files that are encrypted, because business applications such as databases are likely not running. Therefore, those applications will not have open file handles that could prevent file encryption. In addition, many security software applications (e.g., antivirus programs) will not be loaded by default when the system is running in Safe Mode. The ability to encrypt files in Windows Safe Mode is a feature that has been observed in other ransomware families including REvil and BlackMatter.

If the -safeboot command-line argument is provided together with the -user and -pass parameters, Conti will use these values to automatically log in with the specified credentials when the system is rebooted into Safe Mode. This is performed by setting the registry values under HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon to the following:

AutoAdminLogon = 1 DefaultUserName = <username> DefaultDomainName = <computer_name or domain_name> DefaultPassword = <password>

The -user argument is expected to be in the format: <domain_name>\<username>.

If the -safeboot command-line argument is passed by itself (without the -user and -pass parameters), Conti will search for users that have administrator privileges by searching for the security identifier (SID) prefix S-1-5-21 with the relative identifier (RID) -500.

If Conti is able to locate an administrator account, Conti will execute the command cmd.exe /c net user <admin> /active:yes to make sure the account is enabled. Conti will then attempt to change the password for this account to an empty string by executing the command cmd.exe /c net user <admin> "". The corresponding registry values will then be set to automatically log in as the administrator in Safe Mode when the system is rebooted. Figure 1 shows example registry values set after an administrator account has been set up to automatically log in.

Figure 1. Example Windows registry modifications made by Conti to automatically log in as an administrator

In order to execute Conti when the system is booted into Safe Mode, a registry value is created under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce with the name *conti and the value <path_to_conti_executable> -disablesafeboot.

Conti then executes the command bcedit.exe /set {current} safeboot network and forces a system reboot by calling the Windows API function ExitWindowsEx(). This will launch Windows in Safe Mode with networking enabled as shown in Figure 2. The network mode is enabled, so that Conti can still be used to encrypt files on network shares.

Figure 2. Conti booting Windows into Safe Mode with networking enabled to encrypt files

After Conti has completed file encryption in Safe Mode, it executes the command bcedit.exe /deletevalue {current} safeboot and reboots the system. Conti's file encryption algorithms remain the same as previous versions with a per file random 256-bit ChaCha symmetric key. Each file's ChaCha key is protected by a hardcoded victim-specific 4,096-bit RSA public key.

The new Conti update also added the ability to change desktop wallpaper by writing an embedded PNG file to C:\ProgramData\conti.png. An example of the Conti wallpaper image is shown in Figure 3.

Figure 3. Conti PNG image used to set the victim's desktop wallpaper after file encryption

The feature to change the wallpaper after file encryption is very common among ransomware families to further attract the attention of victims.

In order to hinder malware analysis, Conti dynamically resolves most Windows API functions by using a hash algorithm. In the previous version of Conti, the hash algorithm was Murmur2, while the latest version now uses Murmur3. This produces different hash values for all API functions that are used by Conti, which may evade security software that searches for the corresponding hash values.

Conti also updated the encrypted file extensions to include uppercase and lowercase characters and numbers. The following file extension examples have been observed in recent Conti samples:

- .ZG7Ak
- .wjzPe
- .LvOYK
- .C5eFx
- .fgM9X

This encrypted file extension modification may be designed to bypass endpoint security software that could identify the previous Conti ransomware pattern that used five uppercase letters.

Conti also updated the ransom note and TOR hidden service URL. An example of a recent Conti ransom note is shown below:

All of your files are currently encrypted by CONTI strain. If you don't know who we are - just "Google it." As you already know, all of your data has been encrypted by our software. It cannot be recovered by any means without contacting our team directly. DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery software) can damage your files. However, if you want to try - we recommend choosing the data of the lowest value. DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond. So it will be better for both sides if you contact us as soon as possible. DON'T TRY TO CONTACT feds or any recovery companies. We have our informants in these structures, so any of your complaints will be immediately directed to us. So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and initiate the publication of whole compromised data immediately. To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge. You can contact our team directly for further instructions through our website : TOR VERSION : (you should download and install TOR browser first https://torproject[.]org) http://contirec7nchr45rx6ympez5rj...vaeywhvoj3wad[.]onion/<victim_path> YOU SHOULD

BE AWARE! We will speak only with an authorized person. It can be the CEO, top management, etc. In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company! Inform your supervisors and stay calm!

The new Conti ransom note is streamlined with a direct link to a victim-specific chat portal. Prior versions required a victim to access the portal and then upload their ransom note, which contained a unique identifier.

The latest Conti portal contains a landing page that instructs the user to follow the instructions in the README.txt file that is written to disk after file encryption. It no longer supports a victim uploading the ransom note to authenticate as shown in Figure 4.

Figure 4. Updated Conti ransom portal landing page

Conclusion

In January 2022, Conti introduced new features to bring feature parity with other ransomware families including the ability to encrypt files in Windows Safe Mode and change the desktop wallpaper. Despite the group's source code and chat logs being leaked online in February 2022, Conti continues to conduct ransomware attacks against large organizations. ThreatLabz expects the Conti gang to further update the malware and potentially rebrand as the source code leaks have damaged their reputation and may lead to other criminal groups forking the code.

Zscaler Cloud Sandbox Detection

In addition to sandbox detections, Zscaler's multilayered cloud security platform detects indicators related to the campaign at various levels with the following threat names:

Win32.Ransom.Conti

Win64.Ransom.Conti

Indicators of Compromise

SHA256	Description
fca8d48afa7e5535fb71fd22225e86602d47dcfa5a4924fcbc33aecd9c945847	Conti ransomware
16cc7519945bace49ef729e69db7d19e00252f2bd559903e1631c8878c2360f4	Conti ransomware
e6818bf8c6d20501485fc0cc644d33fcea4bd9a3b45c5d61e98317bda5c080c4	Conti ransomware
182f94d26de58b8b02ddf7223f95d153b5e907fa103c34ed76cae2c816f865f0	Conti ransomware
e950c625a94ce9e609778fcc86325530774e45572ff58ebc6549e2627941b5cc	Conti ransomware

- Security Research
- Insights and Research
-

Author

[Brett Stone-Gross](#)

Recommended for You

[Lapsus$ Attack on Okta: How to Evaluate the Impact to your Organization](#)

[Midas Ransomware : Tracing the Evolution of Thanos Ransomware Variants](#)

[Domain Fronting, Abuse and Hiding](#)

[Analysis of Adobe Acrobat Pro DC Solid Framework Heap-based Buffer Overflow Vulnerability (CVE-2021-44708)](#)