Cybereason vs. Conti Ransomware

By Cybereason Nocturnus

Archived: 2026-04-05 18:23:42 UTC

Conti is a relatively new player in the ransomware field. Since first emerging in May 2020, the ransomware operators (aka. the Conti Gang) claim more than 150 successful attacks, which equates to millions of dollars in extortion fees.

Like other ransomware syndicates that have emerged recently, the Conti gang follows the growing trend of double extortion: they steal sensitive files and information from their victims and later use it to extort their victims by threatening to publish the data unless the ransom is paid.

Key Details

Emerging Threat: In a short amount of time, Conti ransomware has caused a great deal of damage and made headlines across the world.

High Severity: The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks

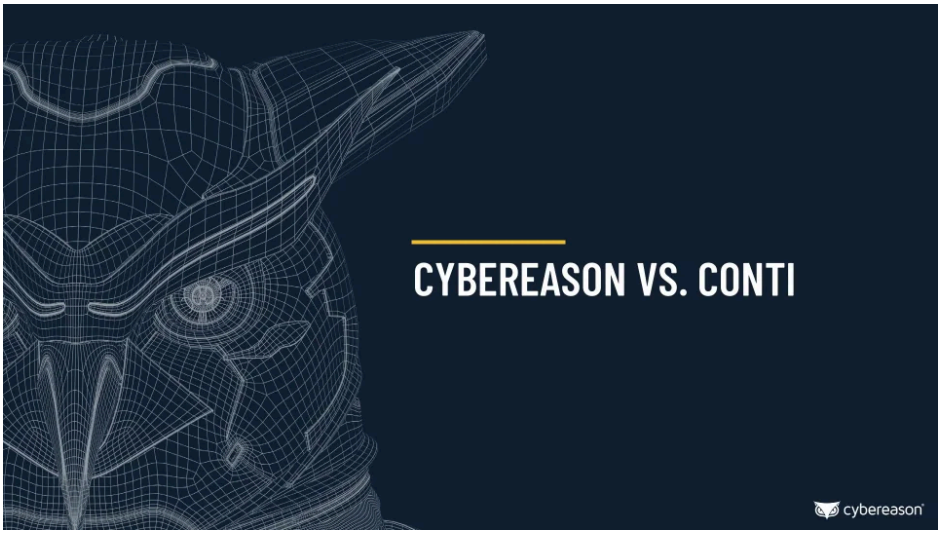
Low-and-Slow: Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-fledged hacking operation, or RansomOp.

Rapid Development Cycle: In just a few months, the Conti gang has released 3 new versions of the ransomware, improving the malware in each version.

The Successor of Ryuk: The Conti Gang collaborated with the TrickBot Gang, which are now using Conti as their ransomware of choice.

Spreading across the network: Conti is not satisfied with causing damage to just the infected machines. Instead, it spreads in the network via SMB and encrypts files on remote machines as well.

Detected and Prevented: The Cybereason Defense Platform fully detects and prevents the Conti ransomware.



Similar to ransomware such as Egregor (“Egregor News”) and Maze (“Maze News”), the Conti Gang has their own website, “Conti News,” which stores a list of their victims, and it is where they publish the stolen data:

Conti News website

Conti is a very destructive threat. Besides the double extortion that puts information and reputation at risk, the Conti operators equip it with a spreading capability, which means that Conti not only encrypts the files on the infected host but also spreads via SMB and encrypts files on different hosts, potentially compromising the entire network. The rapid encryption routine takes just a few seconds to minutes due to its use of multithreading, which also makes it very difficult to stop once the encryption routine starts.

Another major factor that contributes to the popularity of Conti is the collaboration with the TrickBot Gang. Conti is sold as a Ransomware-as-a-Service in underground forums to exclusive buyers and partners such as the TrickBot gang, which replaced Ryuk and adopted Conti as their new ransomware of choice.

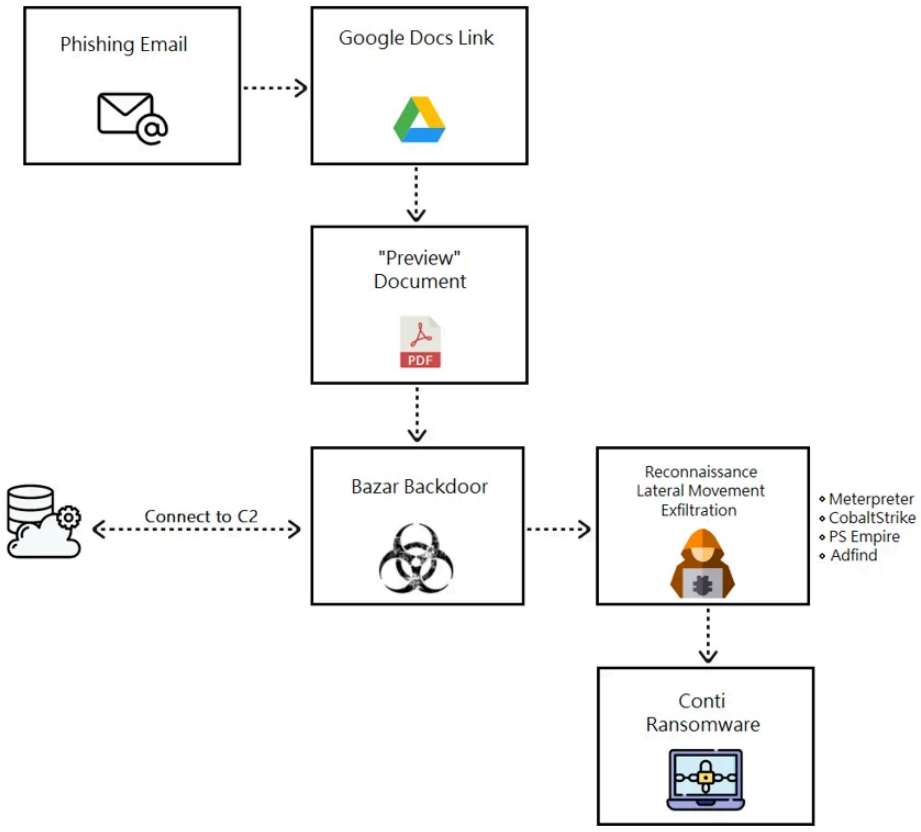
In addition to the sophisticated capabilities and the collaboration with the TrickBot gang, the increased number of Conti attacks against big companies such as Advantech, which was extorted for $13.8M, and other attacks against big North American based companies as listed in this article, contributed to Conti making its way into the news this year. With a rapid development cycle that keeps the malware up-to-date and equipped with advanced capabilities, along with the promotion done by the TrickBot gang, it is no wonder why Conti is referred to as the successor of Ryuk.

Breaking Down the Attack

From Bazar Backdoor to Ransomware

The TrickBot Gang was known to use their infamous TrickBot malware to start interactive hacking operations and deploying secondary payloads such as Ryuk and Anchor. Earlier this year, the group shifted to using the Bazar backdoor to launch an interactive attack and deploy Ryuk, and since July 2020 their new ransomware of favor has been Conti.

Although the payloads and tools of the TrickBot Gang have changed over time, the initial infection vector for the Bazar loader and backdoor has remained the same: a phishing email containing a link to Google Drive which stores the payload:



Conti attack diagram - from Bazar to ransomware

Rapid Development Cycle

Since Conti was first discovered in July 2020, three different versions have been observed. With each new version, the Conti Gang added more capabilities which make the ransomware more dangerous and destructive. The following table summarizes the main changes between the three versions:

	Version 1	**Version 2**	**Version 3**
Earliest to oldest creation times (Based on VT)	2020-05-29 2020-08-18	2020-10-09 2020-10-21	2020-11-06 2020-12-07
Ransom Note file name	Conti_readme.txt CONTI.txt	R3adm3.txt readme.txt	readme.txt
Extension	.CONTI	Changes per sample	Changes per s
Mutex	_CONTI_	lslaif8aisuuugnzxbvmdjk	Kjkbmusop9ic ojkxjfsu81209
Embedded emails / URLs	flapalinta1950@protonmail.com xersami@protonmail.com Ksarepont@protonmail.com	http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid[.]onion https://contirecovery[.]info	http://m232fd https://contire https://contire

	cokeremie@protonmail.com hawhunrocu1982@protonmail.com consfronepun1983@protonmail.com viegesobou1977@protonmail.com hardsandspikab1971@protonmail.com stargoacompte1970@protonmail.com muddkarhersmo1973@protonmail.com versmohubfast1972@protonmail.com ceslingvafi1973@protonmail.com Andrea.Davis.1989@protonmail.com forrestdane79@protonmail.com		heibeaufranin1 polzarutu1982 niggchiphoter1
Form	An independent executable	An independent executable Loader + DLL	An independe Loader + DLL
Spreading via SMB	Spreading via SMB if instructed by command line arguments.	Spreading via SMB even without command line arguments.	Spreading via
Unique	Not using a website, just an email	Observed the use of icons: 	PDB: A:\source\cont Observed the u 
Ransom Note			

Conti Ransomware Execution

This section focuses on version 2 and version 3. As mentioned in the table above, version 3 has two forms - one is an independent executable, and the other is a loader that loads a DLL from the resources section and executes it. Even before doing any static / dynamic analysis, we can use VirusTotal to determine that the resources section probably contains more data, in this case an encrypted DLL that is loaded into memory:

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	2830	3072	5.96	2b4459e441c69c2936522682e8c66420
.rdata	8192	1686	2048	4.37	fdf8d7db8046231ad829b4bd97747dda
.data	12288	2644	512	1.52	222a785276463454f91e60eaafd01e99
.rsrc	16384	208900	209408	7.97	e4ceb513f4b4da811f4d4c0264734510
.reloc	229376	3126	3584	1.11	663a632ea457fd5d1fb3eb80a2b76fa7

Screenshot of VirusTotal file's section information

The APIs for interacting with the resources are dynamically resolved using GetProcAddress:

```
push    offset ProcName ; "LdrFindResource_U"
push    esi             ; hModule
call    edi ; GetProcAddress
push    offset aLdraccessresou ; "LdrAccessResource"
push    esi             ; hModule
mov     dword_4033E4, eax
call    edi ; GetProcAddress
```

Dynamically resolved API used to interact with the resources

The loader then decrypts the payload using an hardcoded key, and loads it into memory:

```
call    ds:VirtualAlloc
mov     ecx, [esp+24h+Src]
mov     esi, eax
mov     eax, [esp+24h+dwSize]
push    eax             ; Size
push    ecx             ; Src
push    esi             ; Dst
call    memcpy
lea     edx, [esp+30h+var_1C]
push    edx
push    3Dh
push    offset a4lizzsbqJ1vCsi ; "4lIzzSbq#>J1v*CSIr#ofX3Bh%)f$3CQSdkz!vn"...
call    sub_401010
mov     ecx, [es
lea     eax, [es
push    eax
push    ecx
push    esi
call    sub_4010
add     esp, 24h
) 00000654 00401254: V
```

```
sub_401010      proc near               ; CODE XREF: WinMain(

arg_0           = dword ptr  4
arg_4           = dword ptr  8
arg_8           = dword ptr  0Ch

                push    340h            ; Size
                call    ds:malloc
```

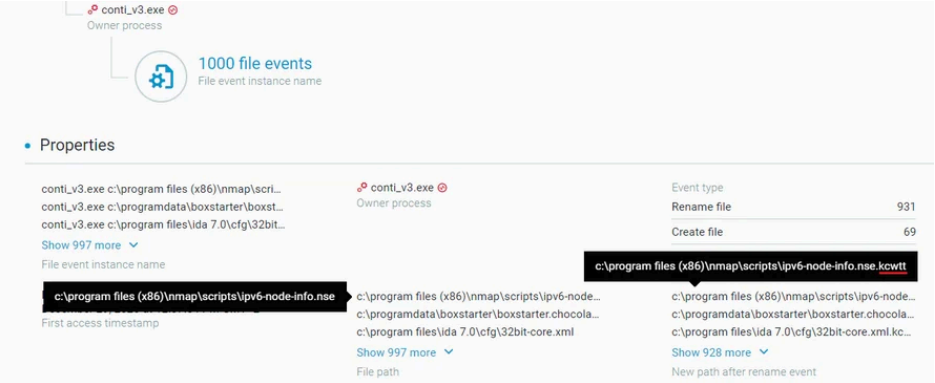
Decryption key of the Conti payload

Once the DLL is loaded, Conti starts it's encryption and spreading routines. The ransomware scans the network for SMB (port 445). If it finds any shared folders it can access, it will try to encrypt the files on the remote machines as well:

Source	Destination	Protocol	Length	Info
10.10.10.2	10.10.10.1	SMB2	182	Close Response
10.10.10.1	10.10.10.2	SMB2	208	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \10.10.10.2\C
10.10.10.2	10.10.10.1	SMB2	130	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
10.10.10.1	10.10.10.2	SMB2	158	Tree Connect Request Tree: \\10.10.10.2\C
10.10.10.2	10.10.10.1	SMB2	138	Tree Connect Response
10.10.10.1	10.10.10.2	SMB2	346	Create Request File: R3ADM3.txt
10.10.10.2	10.10.10.1	SMB2	130	Create Response, Error: STATUS_ACCESS_DENIED
10.10.10.1	10.10.10.2	SMB2	274	Create Request File:
10.10.10.2	10.10.10.1	SMB2	298	Create Response File:
10.10.10.1	10.10.10.2	SMB2	260	Find Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern:
10.10.10.2	10.10.10.1	TCP	1514	445 → 1644 [ACK] Seq=3065 Ack=3066 Win=524032 Len=1460 [TCP s
10.10.10.2	10.10.10.1	SMB2	1102	Find Response;Find Response, Error: STATUS_NO_MORE_FILES
10.10.10.1	10.10.10.2	TCP	54	1644 → 445 [ACK] Seq=3066 Ack=5573 Win=65536 Len=0

Wireshark pcap of Conti spreading via SMB

Conti uses a multithreading technique to fast encrypt all the files. This routine takes seconds to just a few minutes depending on the number of files on the machine. Each sample has a unique extension that the malware adds to the encrypted files. While using Cybereason with prevention mode off to allow investigation of the ransomware execution, it is possible to see the encryption activity and the creation of new files:

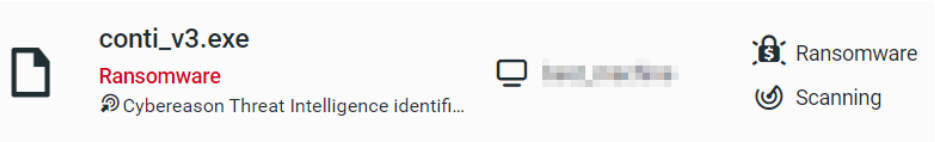


File Events feature in the Cybereason Defense Platform shows the encryption of the files

After the files are encrypted, the malware leaves the ransom note in every folder, making sure it is noticeable to the victim. The Conti Gang usually sets a deadline for the victim to pay the ransom, and if the deadline passes without payment, they leak the victim data on their website "Conti News."

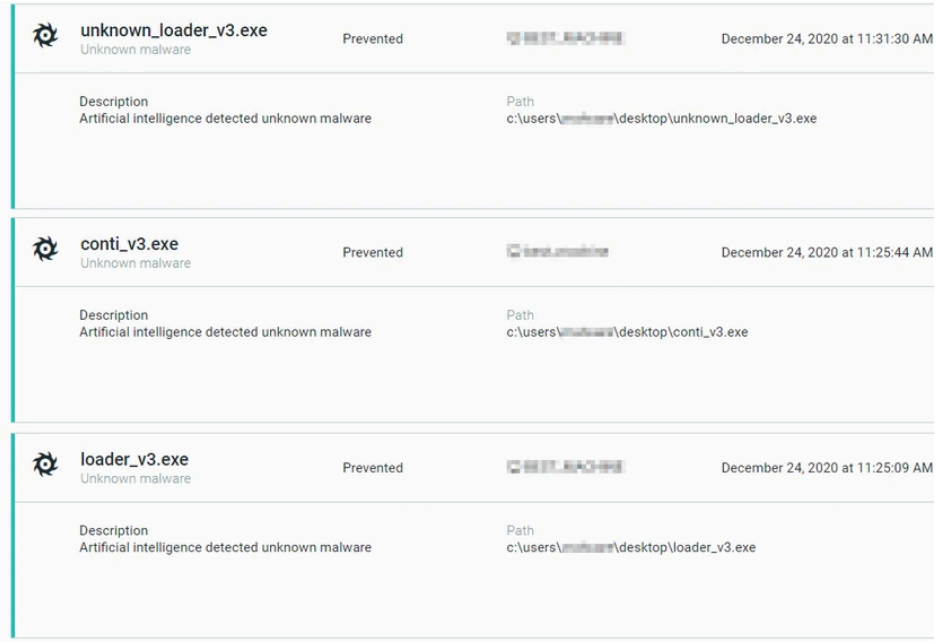
Cybereason Detection and Prevention

The Cybereason Defense Platform is able to prevent the execution of Conti Ransomware using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a Malop™ for it:

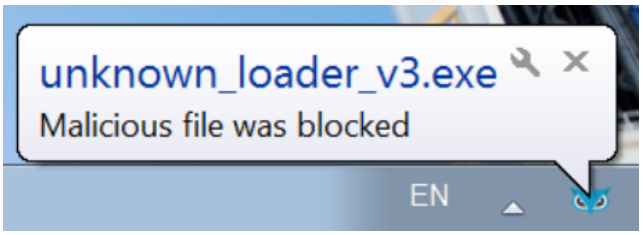


Ransomware Malop triggered due to the malicious activity

Using the Anti-Malware feature with the right configurations (listed in the recommendations below), The Cybereason Defense Platform will also detect and prevent the execution of the ransomware and ensure that it cannot encrypt targeted files. The prevention is based on machine learning, which prevents both known and unknown hashes:



Anti-Malware alert - preventing Conti ransomware



User notification, blocking the execution of the ransomware in the endpoint

Security Recommendations

• **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - more information for customers can be found here

• **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - more information can be found here

• **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities

• **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data

• **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

• **Indicator's of Compromise:** Includes C2 Domains, IP addresses, Docx files SHA-1 hashes, and Msi files. Open the chatbot on the lower right-hand side of this blog to download your copy.

MITRE ATT&CK TECHNIQUES

Initial Access	Lateral Movement	Defense Evasion	Discovery	Command and Control	Impact
Phishing	Taint Shared Content	Deobfuscate / Decode Files or Information	Account Discovery	Commonly Used Port	Data Encrypted for Impact
		Masquerading	Application Window Discovery	Remote File Copy	
		Modify Registry	File and Directory Discovery	Standard Application Layer Protocol	
		Obfuscated Files or Information	Process Discovery	Standard Cryptographic Protocol	
			System Information Discovery	Standard Non-Application Layer Protocol	

Lior Rochberger

 Lior is a senior threat researcher at Cybereason, focusing on threat hunting and malware research. Lior began her career as a team leader in the security operations center in the Israeli Air Force, where she mostly focused on incident response and malware analysis.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus
