Cybereason vs. Conti Ransomware

cybereason.com/blog/cybereason-vs.-conti-ransomware

Written By
Cybereason Nocturnus

January 12, 2021 | 5 minute read

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.

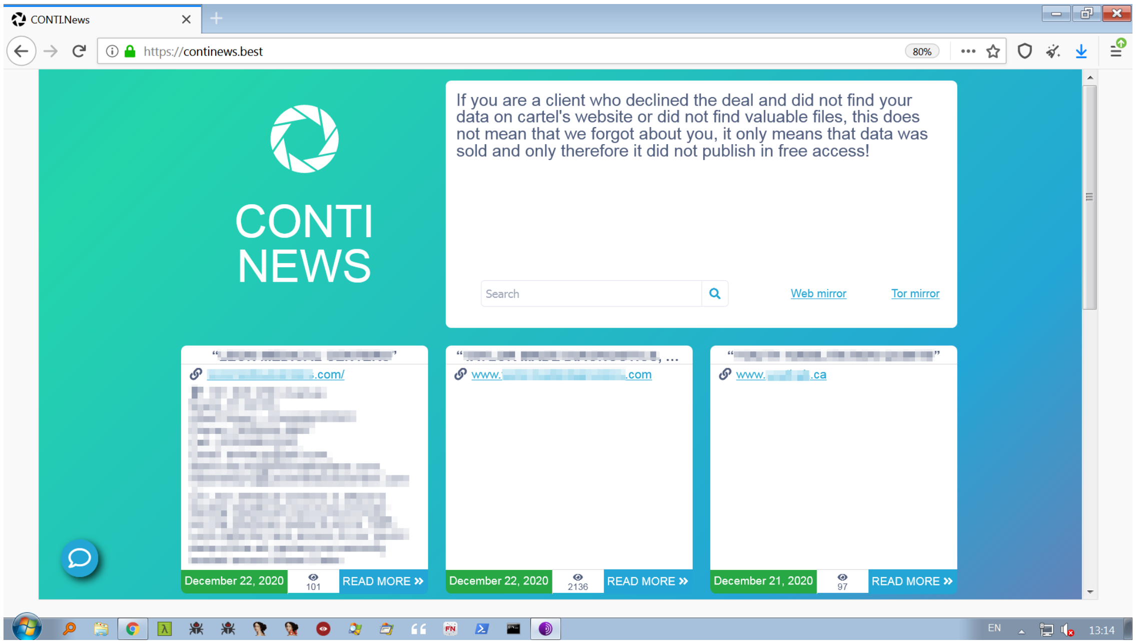
Rapid Development Cycle: In just a few months, the Conti gang has released 3 new versions of the ransomware, improving the malware in each version.

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

If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

"[redacted]"
[redacted].com/
[redacted]
December 22, 2020 · 101 · READ MORE »

"[redacted], ..."
www.[redacted].com
December 22, 2020 · 2136 · READ MORE »

"[redacted]"
www.[redacted].ca
December 21, 2020 · 97 · READ MORE »

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.

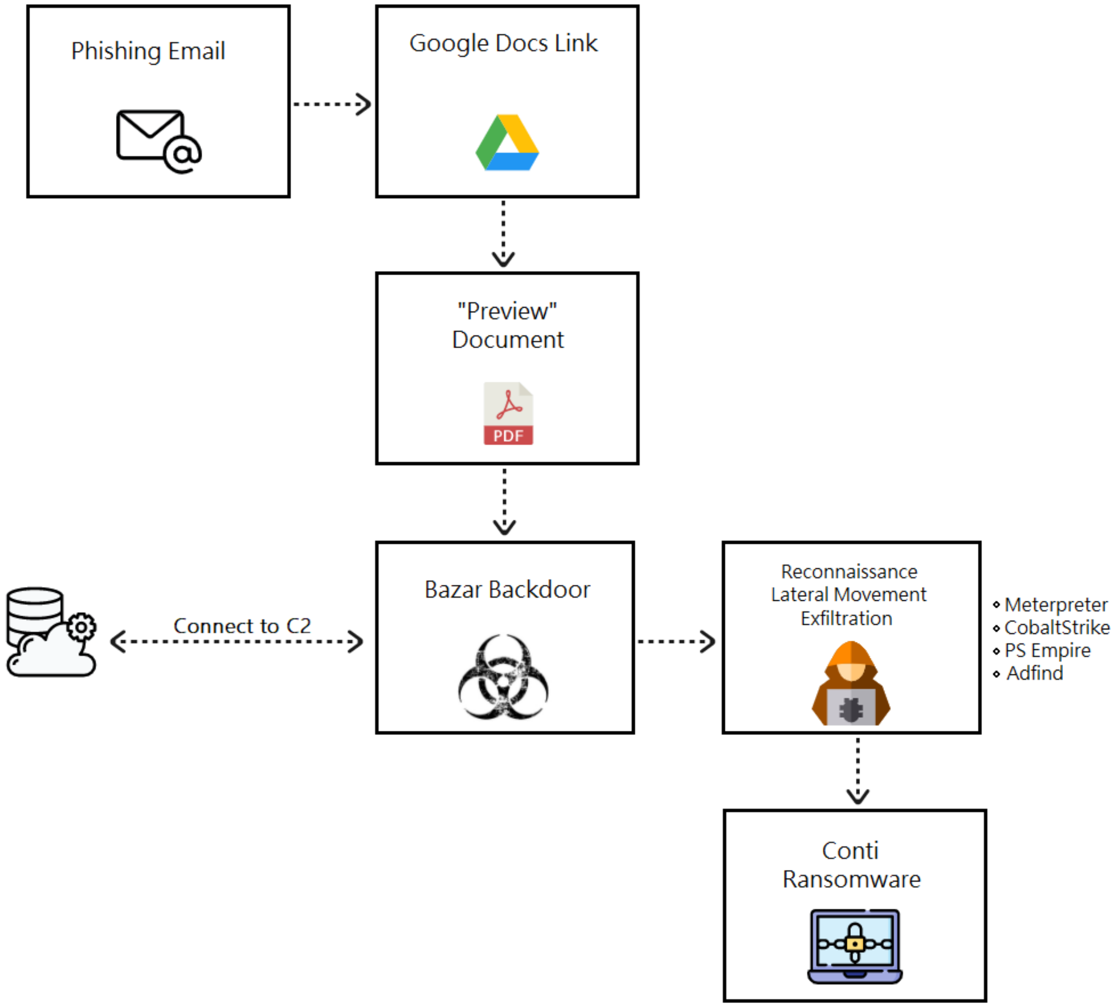
In addition to the sophisticated capabilities and the collaboration with the TrickBot gang, the increased number of Conti attacks against big companies such as Advantech, which was extorted for $13.8M, and other attacks against big North American based companies as listed in this article, contributed 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:

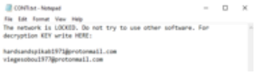
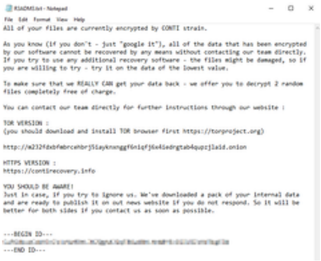
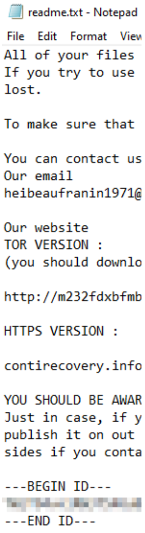


Conti attack diagram - from Bazar to ransomware

Rapid Development Cycle

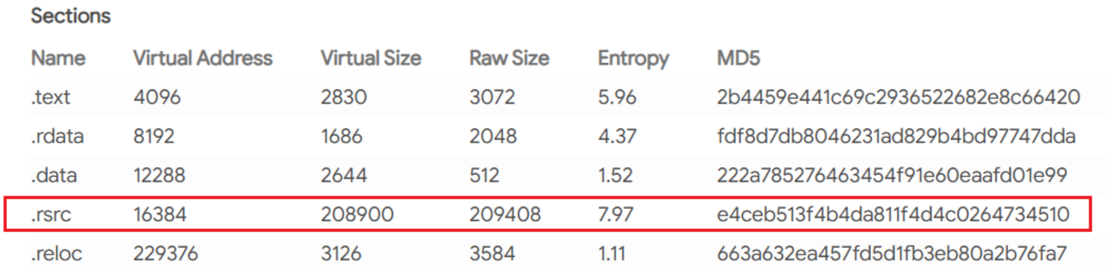
Since Conti was first discovered in July 2020, three different versions have been observed. With each new version, the Conti Gang added more capabilities which make the ransomware more dangerous and destructive. The following table summarizes the main changes between the three versions:

	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	Kjkbmusop9iqk ojkxjfsu81209C
Embedded emails / URLs	flapalinta1950@protonmail.com xersami@protonmail.com Ksarepont@protonmail.com 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	http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid[.]onion https://contirecovery[.]info	http://m232fdxb https://contirec https://contirec heibeaufranin1 polzarutu1982(niggchiphoter1
Form	An independent executable	An independent executable Loader + DLL	An independer 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\conti Observed the u
Ransom Note	 CONTI.txt - Notepad The network is LOCKED. Do not try to use other software. For decryption KEY write HERE: hardsandspikab1971@protonmail.com viegesobou1977@protonmail.com	 README.txt - Notepad All of your files are currently encrypted by CONTI strain. As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly. If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value. To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 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://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion HTTPS VERSION : https://contirecovery.info YOU SHOULD BE AWARE! Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible. ---BEGIN ID--- [redacted] ---END ID---	 readme.txt - Notepad All of your files If you try to use lost. To make sure that You can contact us Our email heibeaufranin1971@ Our website TOR VERSION : (you should downlo http://m232fdxbfmb HTTPS VERSION : contirecovery.info YOU SHOULD BE AWAR Just in case, if y publish it on out sides if you conta ---BEGIN ID--- [redacted] ---END ID---

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:

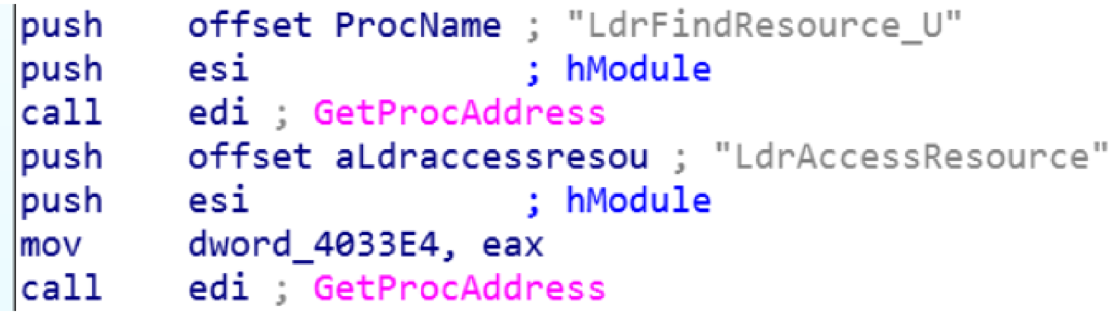


Sections

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

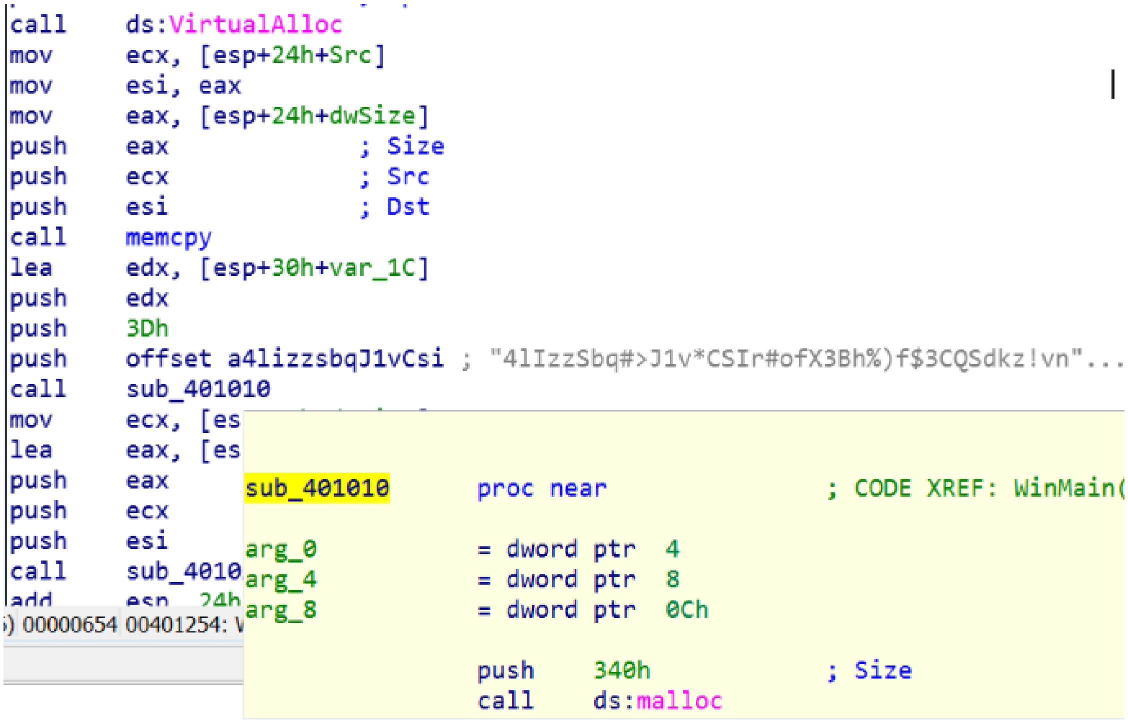
The APIs for interacting with the resources are dynamically resolved using GetProcAddress:



```
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

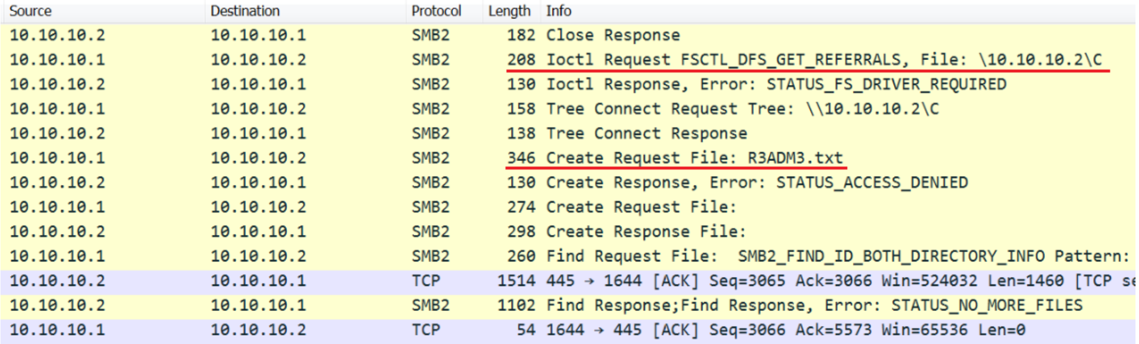
The loader then decrypts the payload using an hardcoded key, and loads it into memory:



```
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

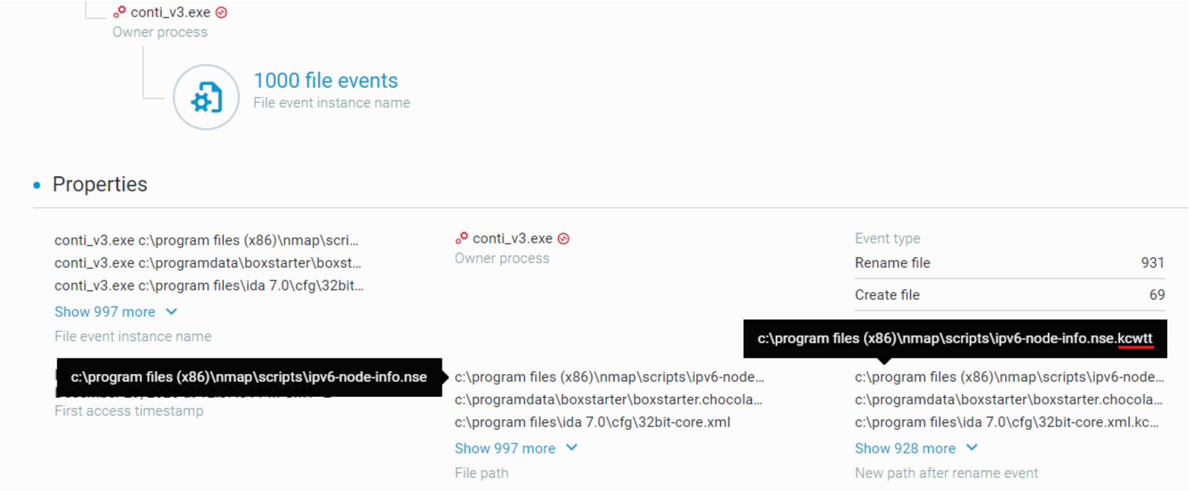
Once the DLL is loaded, Conti starts it’s encryption and spreading routines. The ransomware scans the network for SMB (port 445). If it finds any shared folders it can access, it will try to encrypt the files on the remote machines as well:



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 se
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:



conti_v3.exe
Owner process

1000 file events
File event instance name

Properties

conti_v3.exe c:\program files (x86)\nmap\scri...
conti_v3.exe c:\programdata\boxstarter\boxst...
conti_v3.exe c:\program files\ida 7.0\cfg\32bit...
Show 997 more
File event instance name

c:\program files (x86)\nmap\scripts\ipv6-node-info.nse
First access timestamp

conti_v3.exe
Owner process

c:\program files (x86)\nmap\scripts\ipv6-node...
c:\programdata\boxstarter\boxstarter.chocola...
c:\program files\ida 7.0\cfg\32bit-core.xml
Show 997 more
File path

Event type	
Rename file	931
Create file	69

c:\program files (x86)\nmap\scripts\ipv6-node-info.nse.kcwtt

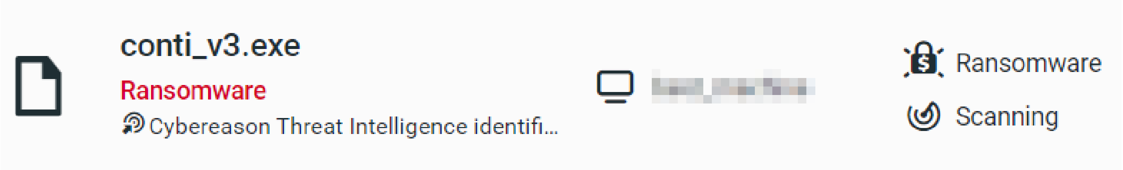
c:\program files (x86)\nmap\scripts\ipv6-node...
c:\programdata\boxstarter\boxstarter.chocola...
c:\program files\ida 7.0\cfg\32bit-core.xml.kc...
Show 928 more
New path after rename event

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^{TM} for it:



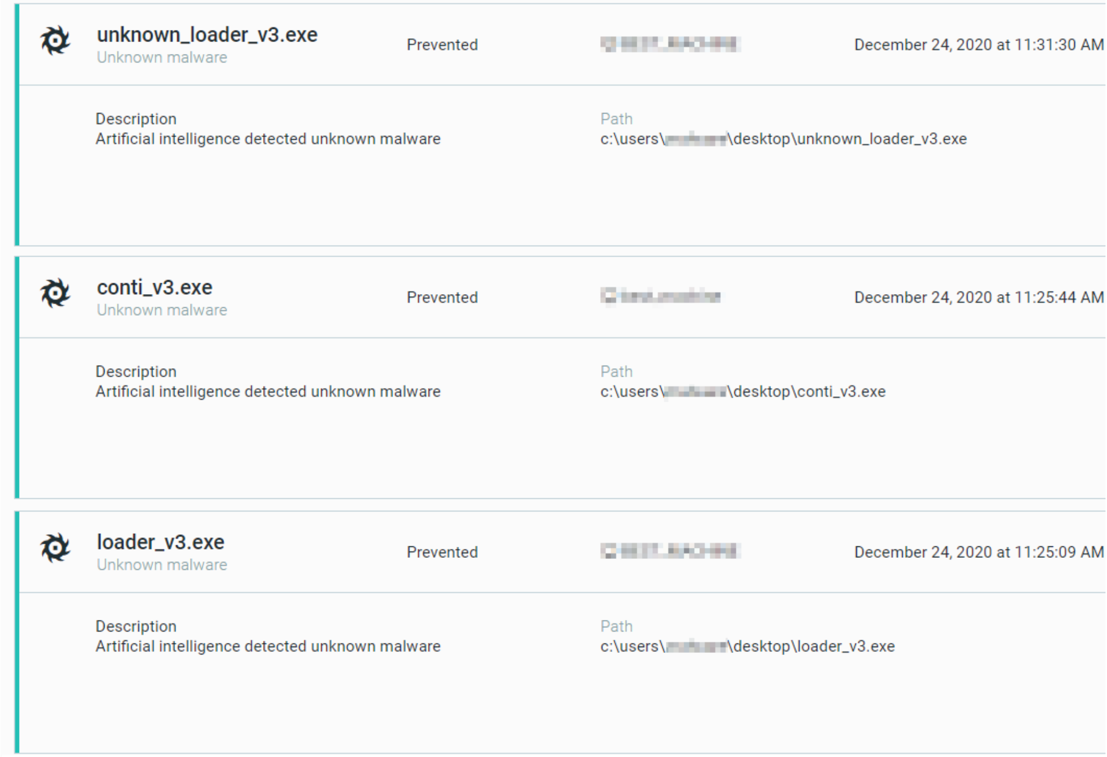
conti_v3.exe
Ransomware
Cybereason Threat Intelligence identifi...

[redacted]

Ransomware
Scanning

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:



unknown_loader_v3.exe
Unknown malware
Prevented
[redacted]
December 24, 2020 at 11:31:30 AM

Description
Artificial intelligence detected unknown malware

Path
c:\users\[redacted]\desktop\unknown_loader_v3.exe

conti_v3.exe
Unknown malware
Prevented
[redacted]
December 24, 2020 at 11:25:44 AM

Description
Artificial intelligence detected unknown malware

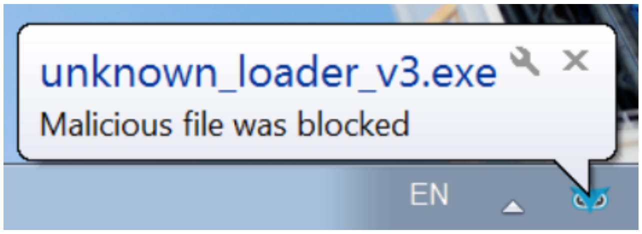
Path
c:\users\[redacted]\desktop\conti_v3.exe

loader_v3.exe
Unknown malware
Prevented
[redacted]
December 24, 2020 at 11:25:09 AM

Description
Artificial intelligence detected unknown malware

Path
c:\users\[redacted]\desktop\loader_v3.exe

Anti-Malware alert - preventing Conti ransomware



unknown_loader_v3.exe
Malicious file was blocked

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.

Conti Ransomware | Indicator's of Compromise

Indicator	Type	Comment
c14f8bc656284715516f26935afe487a1d584f56ffabbcb98f2974f6ca6cd3a4 004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf eae876886f19ba384f55778634a35a1d975414e83f22f6111e3e792f706301fe 6fce6b5f101ab504115f1251a842d55c50a046d7fd92d1fe0f42e430900bc8c5 81792fcbaad868d2e4aca1ed372f4a5abb34372d3265d5712a65cdfe05e42df8 1c4da8bf2089e82a1665f7ac350eeea291dae7509d58dbfc2037ddc1997bfd13 f52508176ff68555ba4c7b39e0d9e23a11e3ac0c3e1ef0755408ed1c0670fc21 040fcbd360c7498756519cb0e687120bd623da80784034ea89178409491b1c44 3ab3c4ffcf366dcbe660506295dcef82d058cb25b1c0b362cc62371a19a0d5f8 e16fea1b8874cc6b26e7e2df9697f03f86efa82247bb3b2922f1d05052dbcbb4 98a09f7896a7c20229e696d6e8344fe9593fd70afada5d986e04c0d6933cc4db 1490e74b93b40176975836156dc62210b7670ab5eb38f153a21cda8c72bebc76 0b0b902af452e1c949a609a3b29a9de21dac639846c77427de06e6e63c1fe904	SHA256	Conti Version1
633b9d373da7d2916f4d3b2902d4817c0f3ad5de5466ac85f34bdd37a8d3dd37 e64e350861b86d4e05668bc25e6c952880f6b39ca921496ccce1487dbf6acab6 7c6463f86027bf1d6a787f787282b5ff87bc98389c3b48181c7e84cd71684b1f ebeca2df24a55c629cf0ce0d4b703ed632819d8ac101b1b930ec666760036124 fe39822a460d96b5cd0287a371cc238933a6f7765dc165606c78bf70c4483c2a 2a6cd292fe8d850a69cc67cc417f63926896305f8eb9647a9c5aee85efd6587a 3402d9d20bc4622a87c2533484fb98889a5a85bf3191192faf4ef8431f7a4b9c 6ed577361d0db8b085c54efef19fec4055ecdaaaf65b7ec63134275d93d6f09b 1f782c00f48835beffd1cb068c1b43854b5f1542966dd5926589fece4a5058b3 9826b386065f8312a7a7ef431c735a66e85a9c144692907f5909f81f837c65f4 bbb58c0ac016bf5d8c06099b39035ccc8658c1f1630ed3fd9979ae932f67551e 0951fde8a8ea9cd45d2be14d63e6e55c8e87af0da45cf3776b495871652aa862 d236d64b7bf9510ea1746d10a4c164a2ef2c724cc62b2bca91d72bdf24821e40 dbf2380de4e4ac4ae259aa01b0a1c10ab81e246d895e290a5031709837f219eb f3ee2a9fe1aae1a566ec663969ee9e7577f790fc9ae0085620e502b680d8acd3 260709f0aad63cc84ea3e64a26b149a3b6c769697a958645b66de5137821af1e f25961cf6e019d95740c13e1b0718d6e0c8753a22106e8d61479877a31da9e18 afa77a9049000a105d744dfb9bcaeedfdc837cc93aaf045db4f819c3da445b79 0a7e7f12d79130da067fd39ede7ff4dc3dc6665d88f5278745074d77132312bf	SHA256	Conti Version2

e7ce83a1a5163487d86538344c4f37c72a795b07b03a40db7d36ec81a442d685 90cfbbe316c94611fdb48029b5302df0980395528a812404cacbc39ef1a6bde0 d3c75c5bc4ae087d547bd722bd84478ee6baf8c3355b930f26cc19777cd39d4c f092b985b75a702c784f0936ce892595b91d025b26f3387a712b76dcc3a4bc81 5cf0a6ac9786638a063eea9ab68508f31e537072bbcea27371f9121d2668a251 c67ba4c6e872dbcd2b1281c33fb033f886d8472ea021cf3974a445c4b804fec2 64a3a3ec70d20636299b8fe4f50c2b4d077f9934ee2d6ccf7d440b05b9770f56 707b752f6bd89d4f97d08602d0546a56d27acfe00e6d5df2a2cb67c5e2eeee30 c41babd8fa4fc96822f72066ba2af781e5c381a58017f72c8fec301436745b01 26b2401211769d2fa1415228b4b1305eeeed249a996d149ad83b6fc9c4f703ce 68d45d7973277c4a3095929a06c3defa40adf7bf592ede0557a89f724a290395 24347befc0663e75a848982d22f76c2b0f9dc8d26c77d6b13c78530446aa6246 73bd8c2aa71f5dcd9d2ddd79e53656c6ae3db2535e08cf9dab1cd13bdd6d5ea3 626a1863c6cb57977bf75596d78b51cb8208fadec3d68eba1dd7b5a3c88578ce 49b2c44d9a304035e586a15c1eb06101dcd64cdc17b64a0d69d253e653ff25a7	SHA256	Conti Version3
http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid[.]onion https://contirecovery[.]info https://contirecovery[.]best	Domains	Conti websites
23.106.215[.]97	IP	Site that stores a Conti payload

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