cybereason

Threat Hunting

From Solarwinds to Hafnium APT

Niv Yona

IR Practice Director
Cybereason

Eli Salem

Lead Threat Hunter
Cybereason

About Us

Niv Yona

IR Practice Director
Cybereason

- Malware Analysis, Threat Hunting
- Incident Response, Forensics
niv.yona@cybereason.com

Eli Salem

Lead Threat Hunter
Cybereason

- Malware Reverse Engineering
- Threat Hunting
eli.salem@cybereason.com

Agenda

- Threat Hunting - What & Why
- Gray Area Problem
- IOCs vs IOBs
- Data Collection
- Threat Hunting Hypothesis
- Threat Hunt Use Cases:
    1. Hunt for SolarWinds Supply Chain Attack: IOCs
    2. Hunt for ProxyLogon and Hafnium: IOBs

Threat Hunting

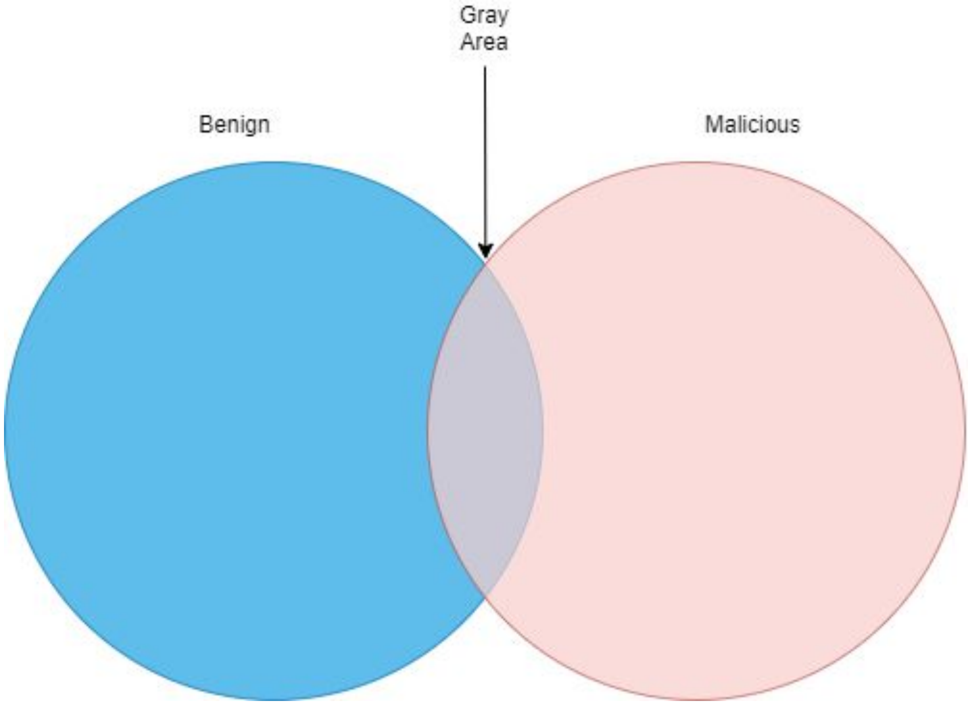
Threat hunting is the process of proactively searching for cyber threats that are undetected in an environment.

- Processes activity
- IOBs and IOCs
- Anomalies
- TTPs

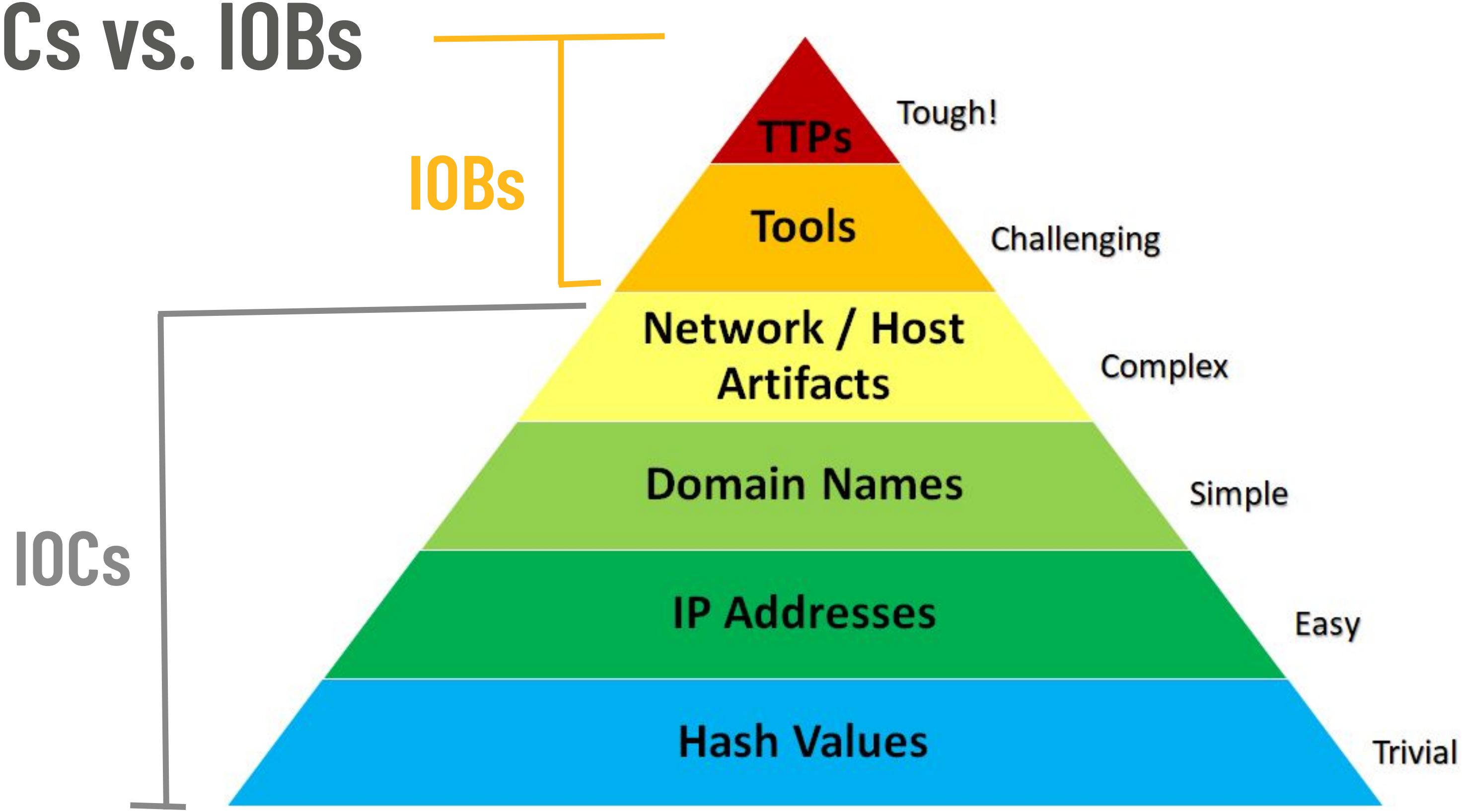
Why Threat Hunting?

- Threat actors are ever evolving
- Traditional security products leave gaps
- Attackers are already in!

Gray Area Problem



IOCs vs. IOBs


IOBs
IOCs
TTPs
Tough!
Tools
Challenging
Network / Host Artifacts
Complex
Domain Names
Simple
IP Addresses
Easy
Hash Values
Trivial

Data Collection

- EDR / EPP Products
- Telemetry Data Collection
  - Running Processes
  - Loaded Modules
  - Connections
  - File Events
  - User Activity
- Sysmon

Go Hunt!

Create Hypothesis

Research

Create Hunting Query

Detect & Analyze

Solarwinds

Solarwinds

First reported in December 2020

The campaign reportedly began in spring 2020 and affected 18K Solarwinds customers

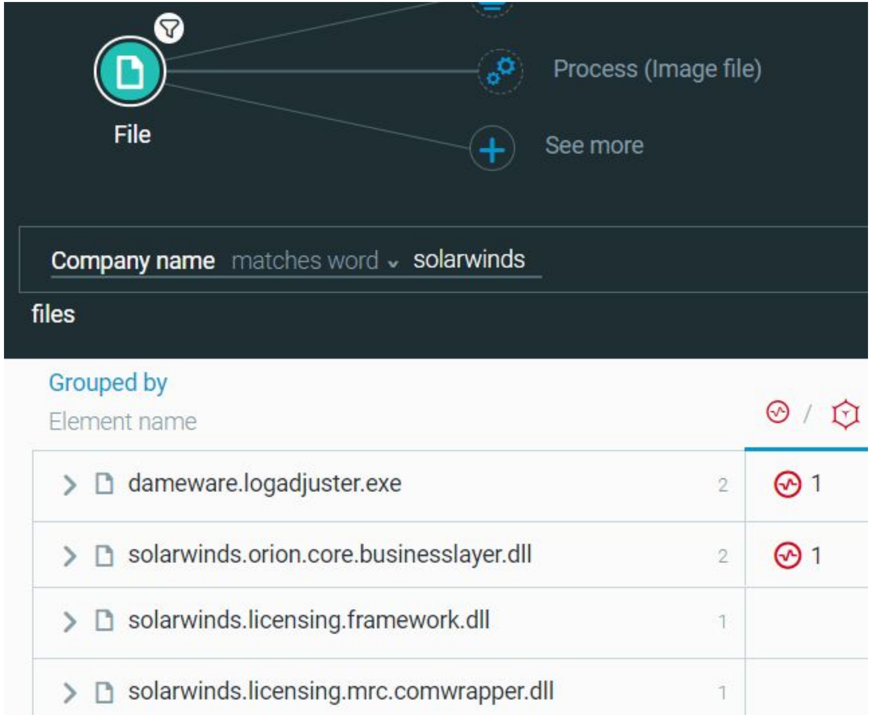
Supply Chain Attack

Threat actors inserted malicious code into legitimate updates for Solarwinds software

Multiple Backdoors

SUNBURST backdoor
TEARDROP memory dropper

Solarwinds - Scoping



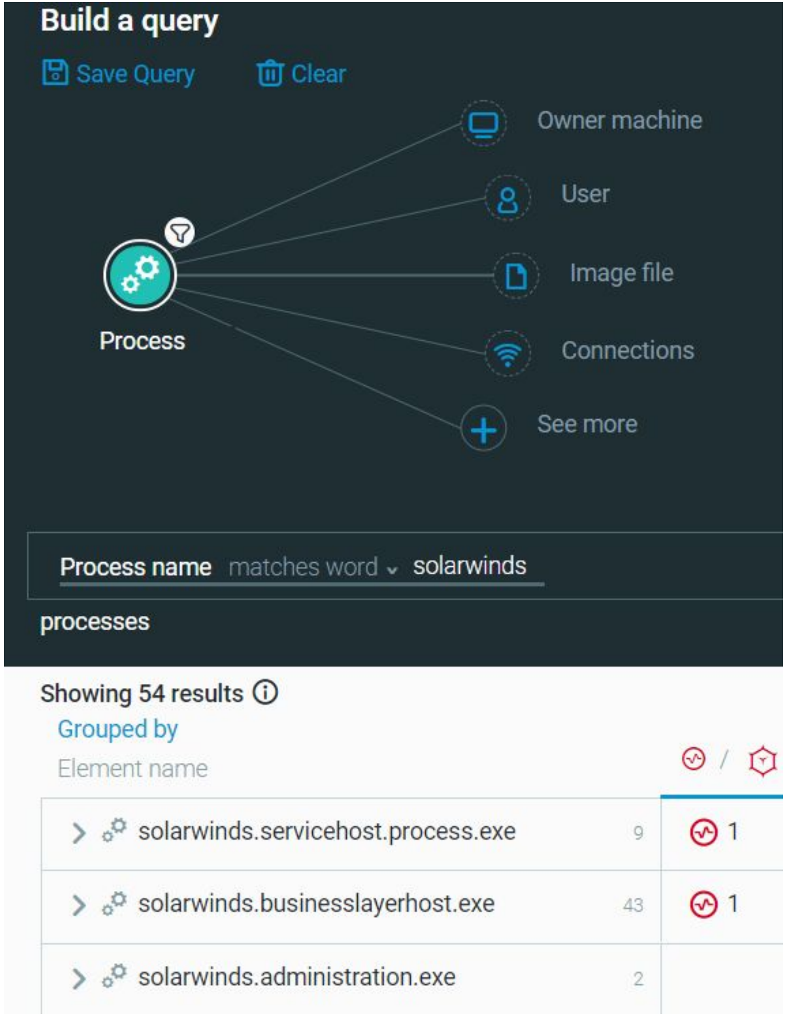
Company name matches word ⌄ solarwinds

files

Grouped by

Element name

dameware.logadjuster.exe	2	1
solarwinds.orion.core.businesslayer.dll	2	1
solarwinds.licensing.framework.dll	1	
solarwinds.licensing.mrc.comwrapper.dll	1	


Build a query

Process name matches word ⌄ solarwinds

processes

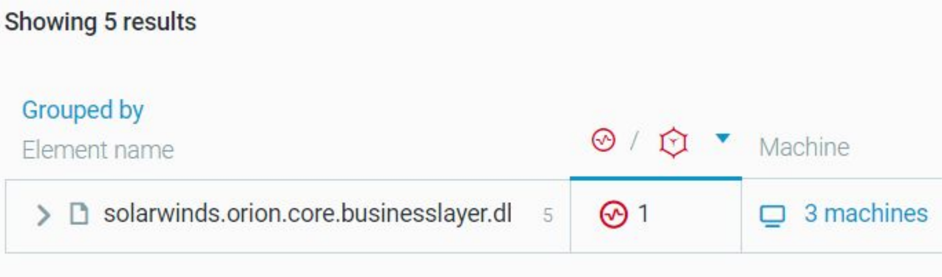
Showing 54 results ⓘ

Grouped by

Element name

solarwinds.servicehost.process.exe	9	1
solarwinds.businesslayerhost.exe	43	1
solarwinds.administration.exe	2	

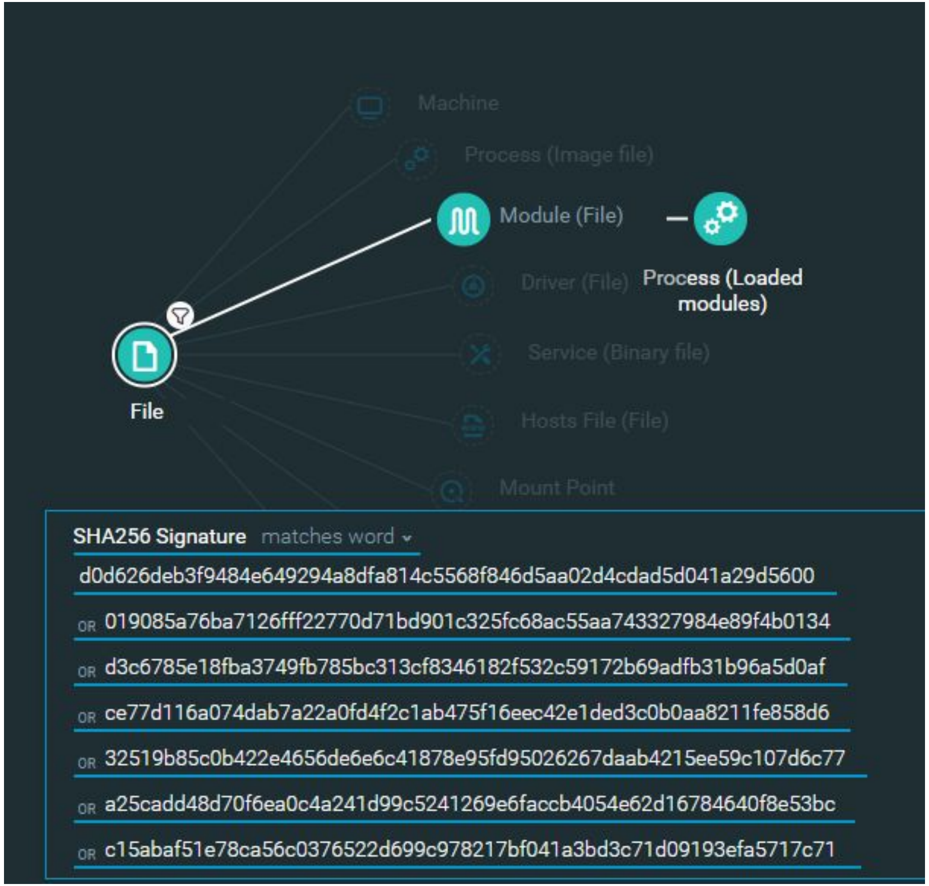
Solarwinds - IOCs Search



Showing 5 results

Grouped by
Element name

Element name	ⓘ / ⬡ ▾	Machine
> 🗋 solarwinds.orion.core.businesslayer.dl 5	1	🖵 3 machines



SHA256 Signature matches word ▾

d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600

OR 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134

OR d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af

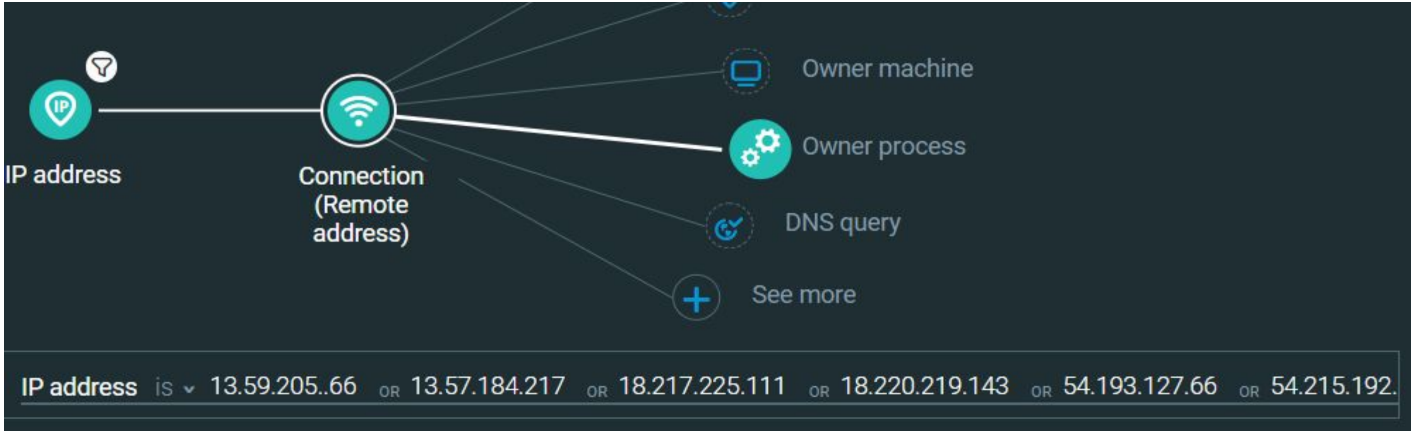
OR ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6

OR 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77

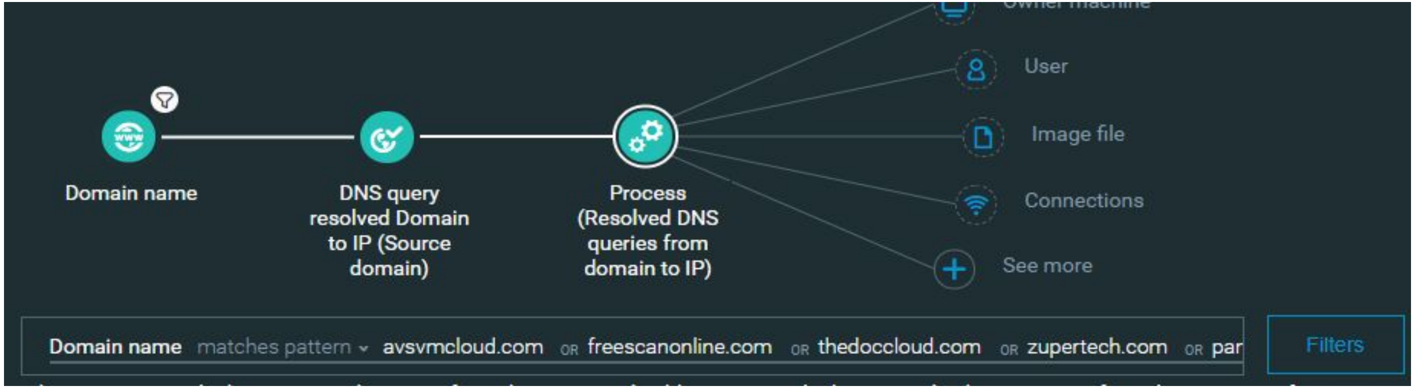
OR a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc

OR c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71

Solarwinds - IOCs Search

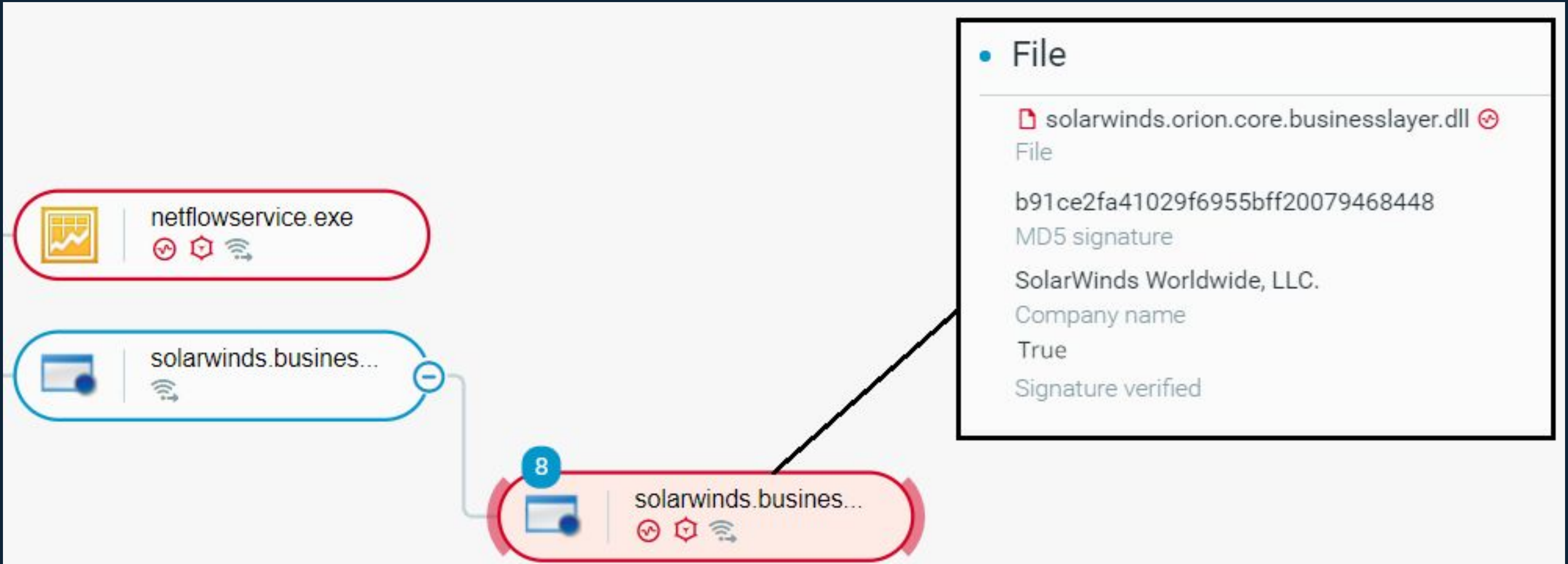


IP address is 13.59.205..66 OR 13.57.184.217 OR 18.217.225.111 OR 18.220.219.143 OR 54.193.127.66 OR 54.215.192.


Owner machine
User
Domain name
DNS query resolved Domain to IP (Source domain)
Process (Resolved DNS queries from domain to IP)
Image file
Connections
See more
Filters

Domain name matches pattern avsvmcloud.com OR freescanonline.com OR thedoccloud.com OR zupertech.com OR par

Solarwinds



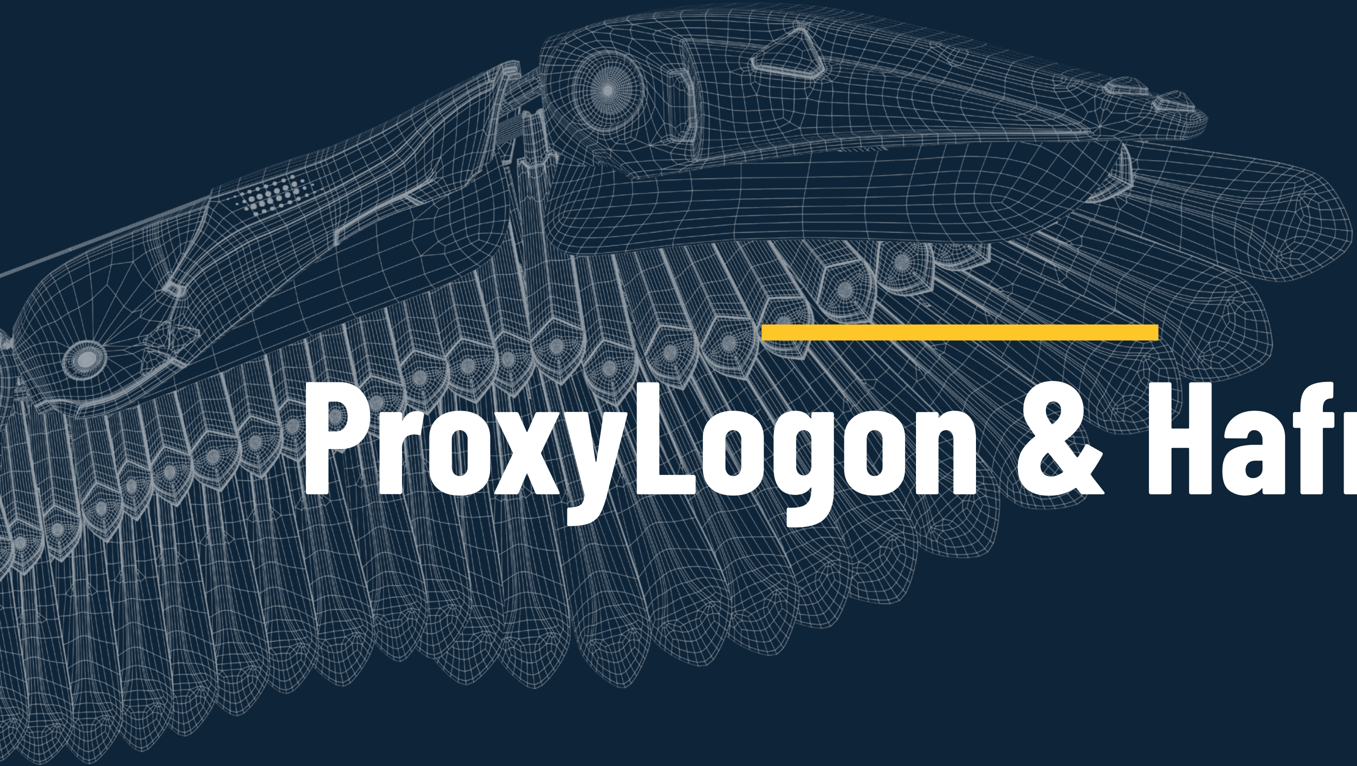
- File

solarwinds.orion.core.businesslayer.dll
File

b91ce2fa41029f6955bff20079468448
MD5 signature

SolarWinds Worldwide, LLC.
Company name

True
Signature verified



ProxyLogon & Hafnium

cybereason®

ProxyLogon & Hafnium

Several Zero Days Reported in March 2021

Microsoft announced the existence of multiple zero-day vulnerabilities in the Exchange Server on-premises product

Multiple APT Groups

HAFNIUM, APT27,APT41 and more

Thousands of organizations affected

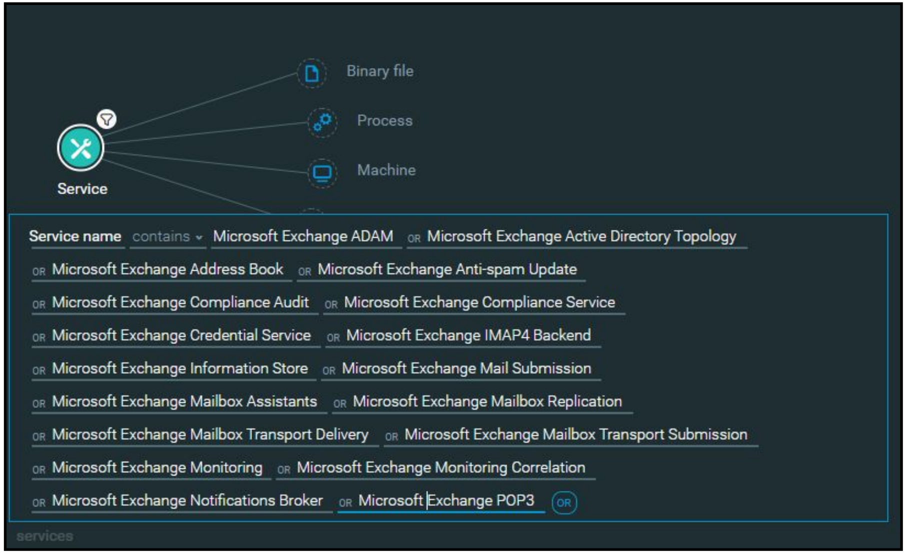
At least 30,000 organizations across the United States affected

Hunting ProxyLogon - First Hour

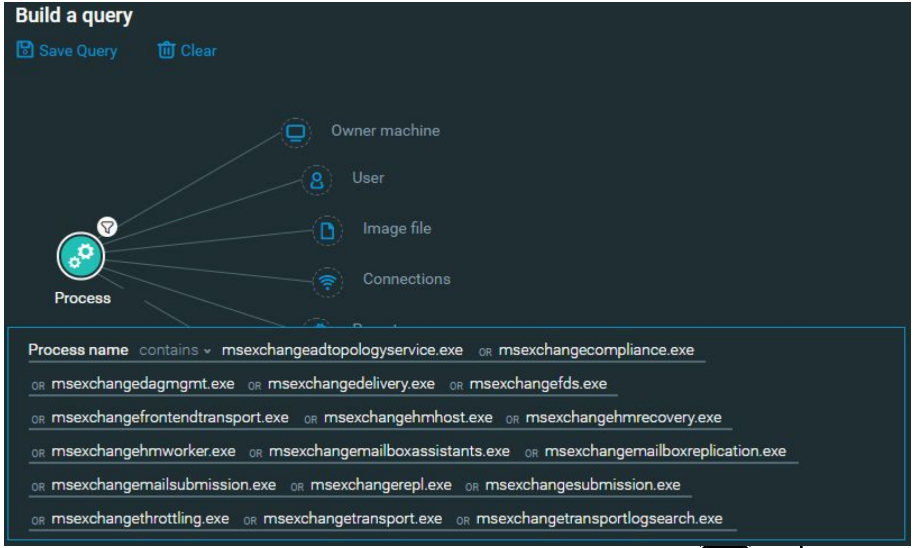
- First, scoping!
  - Exchange Server machines
  - Related processes

Hunting ProxyLogon - First Hour

Searching for MSExchange services



Service name contains Microsoft Exchange ADAM OR Microsoft Exchange Active Directory Topology
OR Microsoft Exchange Address Book OR Microsoft Exchange Anti-spam Update
OR Microsoft Exchange Compliance Audit OR Microsoft Exchange Compliance Service
OR Microsoft Exchange Credential Service OR Microsoft Exchange IMAP4 Backend
OR Microsoft Exchange Information Store OR Microsoft Exchange Mail Submission
OR Microsoft Exchange Mailbox Assistants OR Microsoft Exchange Mailbox Replication
OR Microsoft Exchange Mailbox Transport Delivery OR Microsoft Exchange Mailbox Transport Submission
OR Microsoft Exchange Monitoring OR Microsoft Exchange Monitoring Correlation
OR Microsoft Exchange Notifications Broker OR Microsoft Exchange POP3 OR



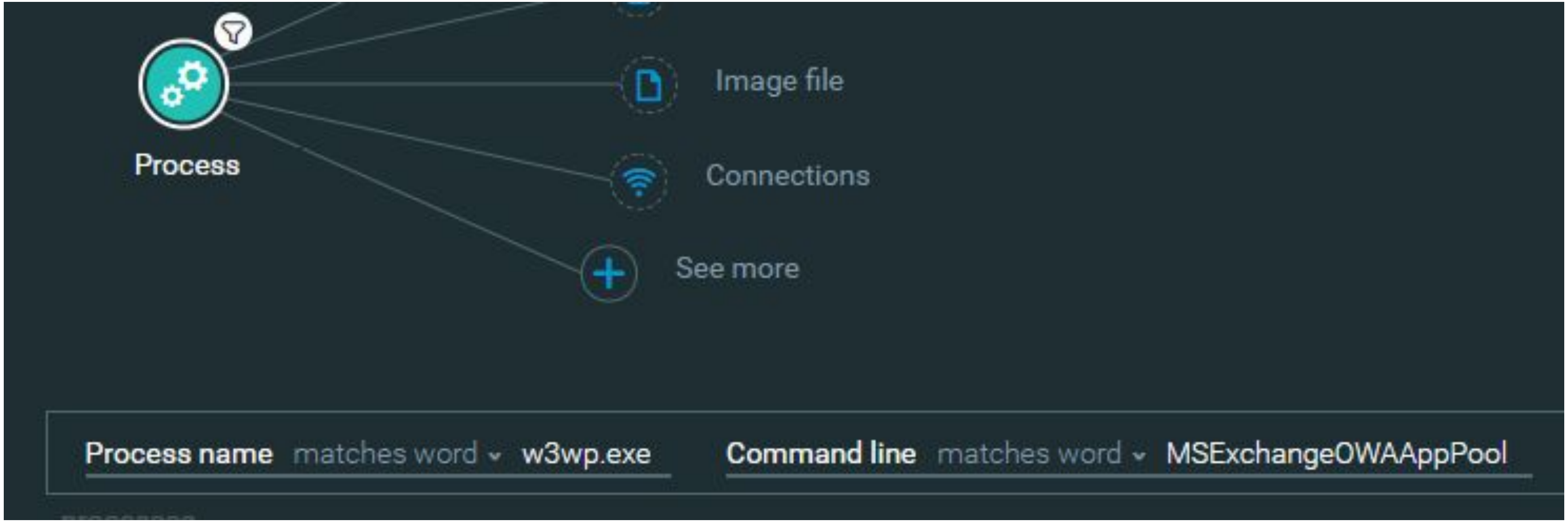
Process name contains msexchangeadtopologyservice.exe OR msexchangecompliance.exe
OR msexchangedagmgmt.exe OR msexchangedelivery.exe OR msexchangefds.exe
OR msexchangefrontendtransport.exe OR msexchangehmhost.exe OR msexchangehmrecovery.exe
OR msexchangehmworker.exe OR msexchangemailboxassistants.exe OR msexchangemailboxreplication.exe
OR msexchangemailsubmission.exe OR msexchangerepl.exe OR msexchangesubmission.exe
OR msexchangethrottling.exe OR msexchangetransport.exe OR msexchangetransportlogsearch.exe

Hunting ProxyLogon - First Hour

- Microsoft IIS worker process anomalies (W3WP.exe)
  - Command line
  - Process tree
  - File events
  - Connections

Hunting ProxyLogon

Microsoft IIS worker process + MSExchangeOWAAppPool

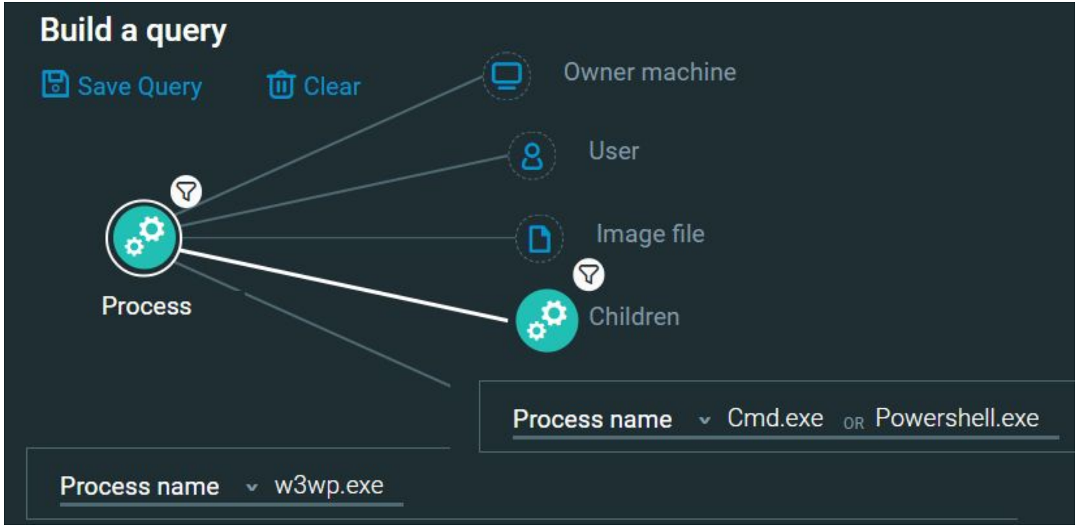


Process name matches word w3wp.exe

Command line matches word MSExchangeOWAAppPool

Hunting ProxyLogon

- Microsoft IIS worker process + MSExchangeOWAAppPool
  - Shell child processes

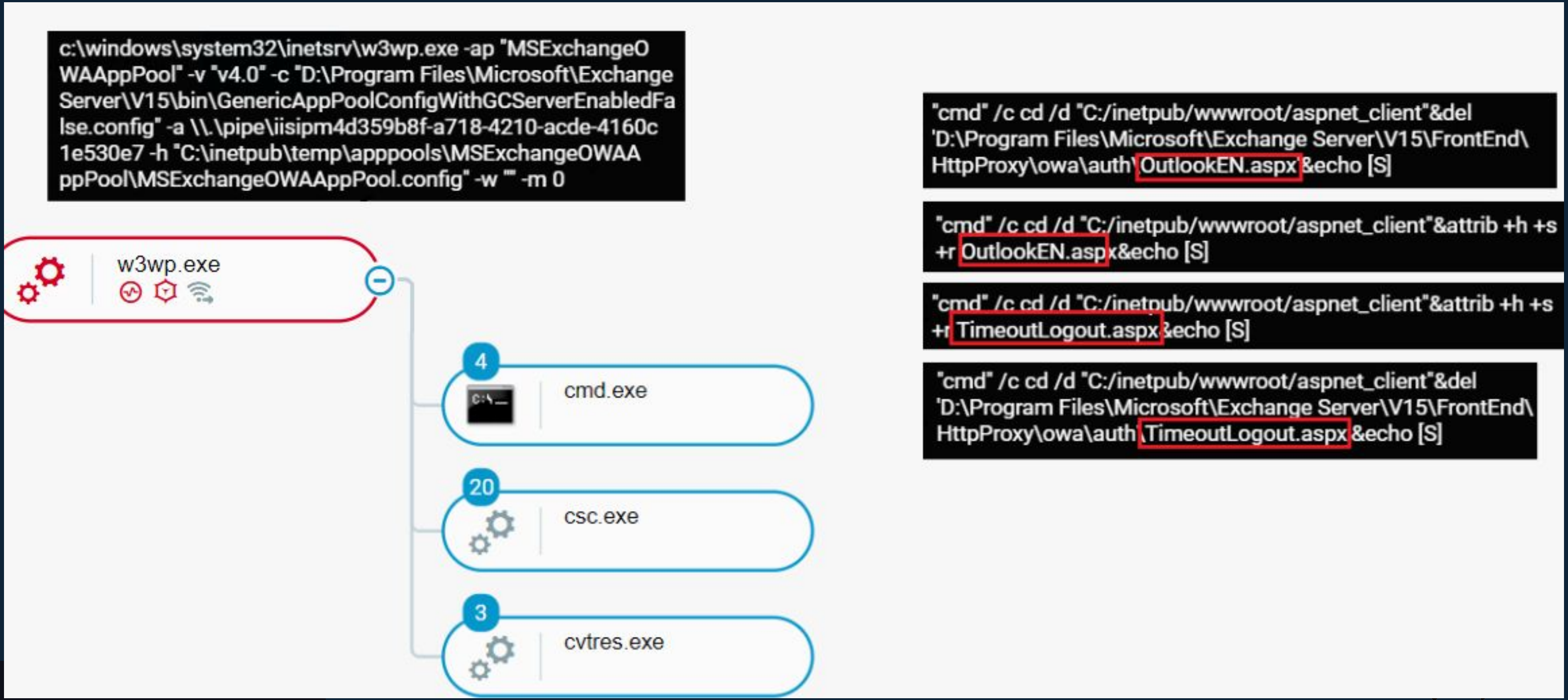


Process name w3wp.exe

Process name Cmd.exe OR Powershell.exe

cybereason

Hunting Hafnium



```
c:\windows\system32\inetsrv\w3wp.exe -ap "MSExchangeOWAAppPool" -v "v4.0" -c "D:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipm4d359b8f-a718-4210-acde-4160c1e530e7 -h "C:\inetpub\temp\apppools\MSExchangeOWAAppPool\MSExchangeOWAAppPool.config" -w "" -m 0
```

```
"cmd" /c cd /d "C:/inetpub/wwwroot/aspnet_client"&del 'D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\OutlookEN.aspx'&echo [S]
```

```
"cmd" /c cd /d "C:/inetpub/wwwroot/aspnet_client"&attrib +h +s +r OutlookEN.aspx&echo [S]
```

```
"cmd" /c cd /d "C:/inetpub/wwwroot/aspnet_client"&attrib +h +s +r TimeoutLogout.aspx&echo [S]
```

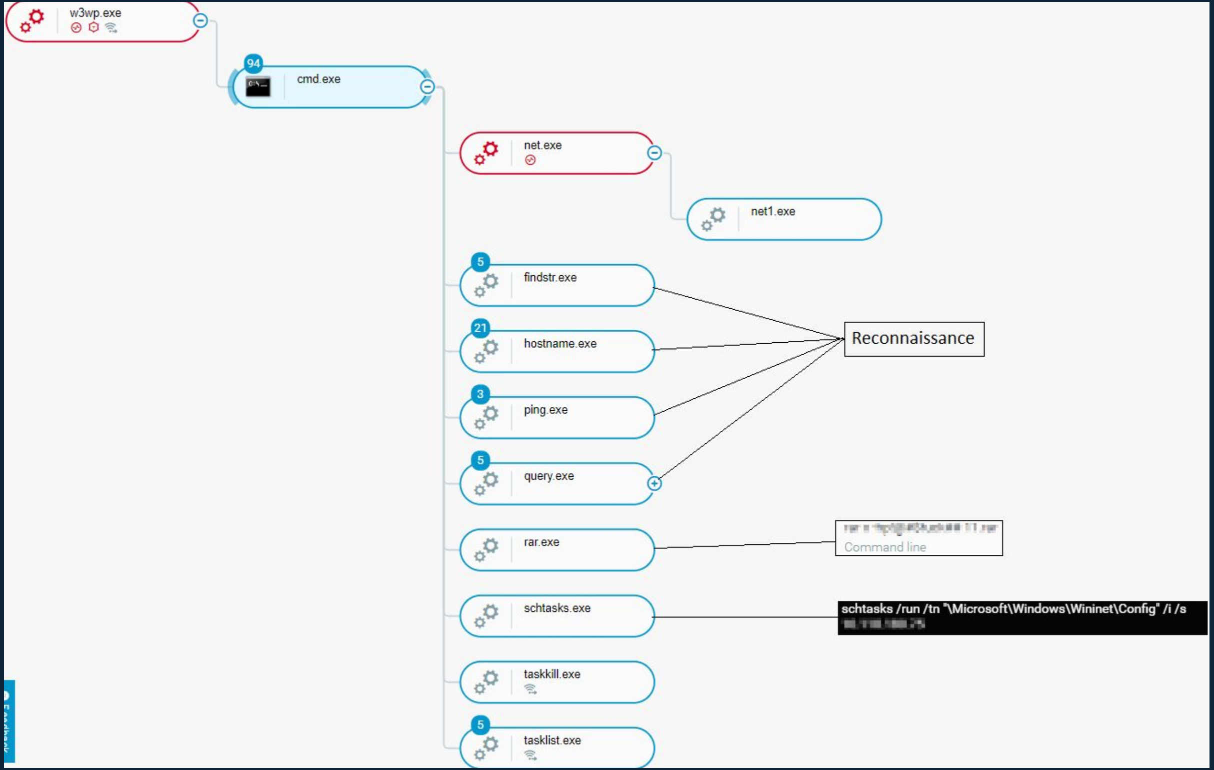
```
"cmd" /c cd /d "C:/inetpub/wwwroot/aspnet_client"&del 'D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\TimeoutLogout.aspx'&echo [S]
```

Hunting ProxyLogon - Zero Hour

Exploited directories

- C:\inetpub\wwwroot\aspnet_client - discover.aspx
- C:\inetpub\wwwroot\aspnet_client\system_web
- C:\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth - RedirSuiteServerProxy.aspx, KRYMCJ.aspx, 13DWBS.aspx, default.aspx, TimeoutLogout.aspx, OutlookEN.aspx
- C:\Microsoft\Exchange Server\FrontEnd\HttpProxy\owa\auth

Hunting Hafnium

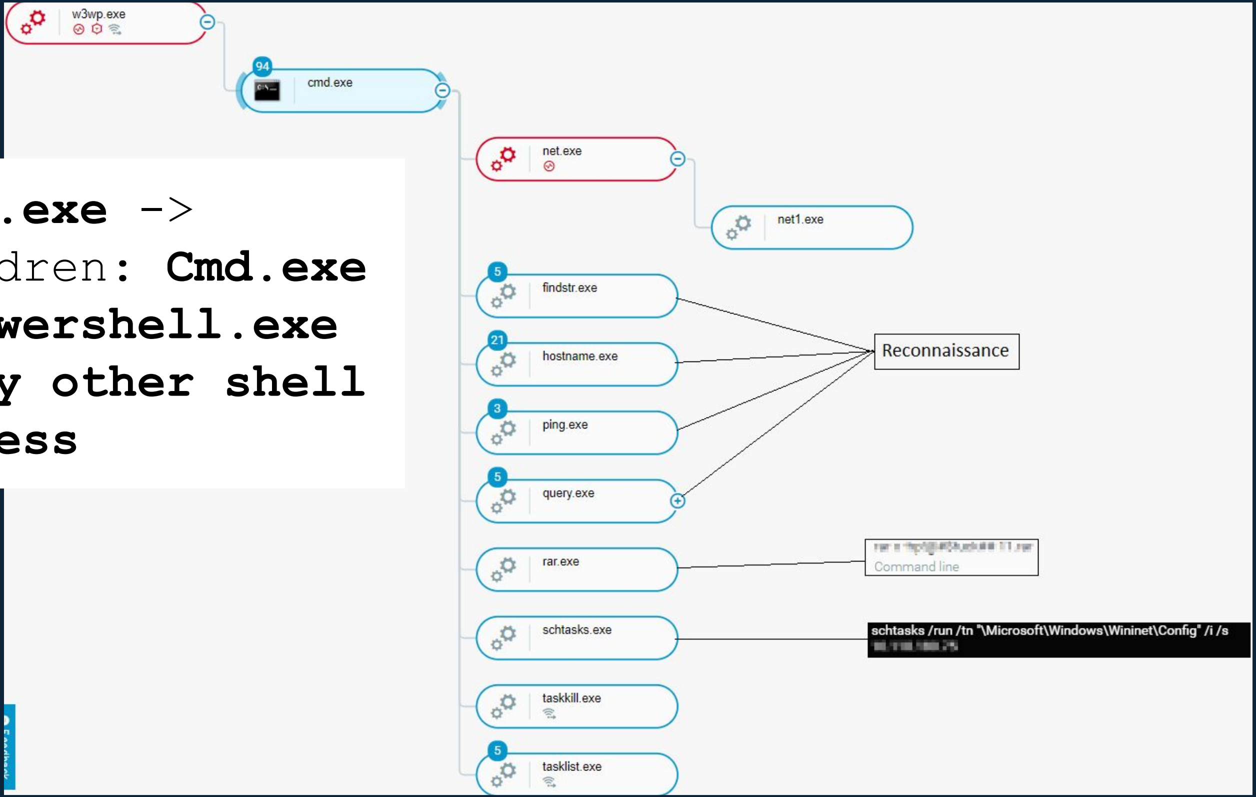


[redacted]

```
schtasks /run /tn "\Microsoft\Windows\Wininet\Config" /i /s [redacted]
```

Hunting Hafnium

w3wP.exe ->
Children: **Cmd.exe**
| Powershell.exe
| Any other shell process



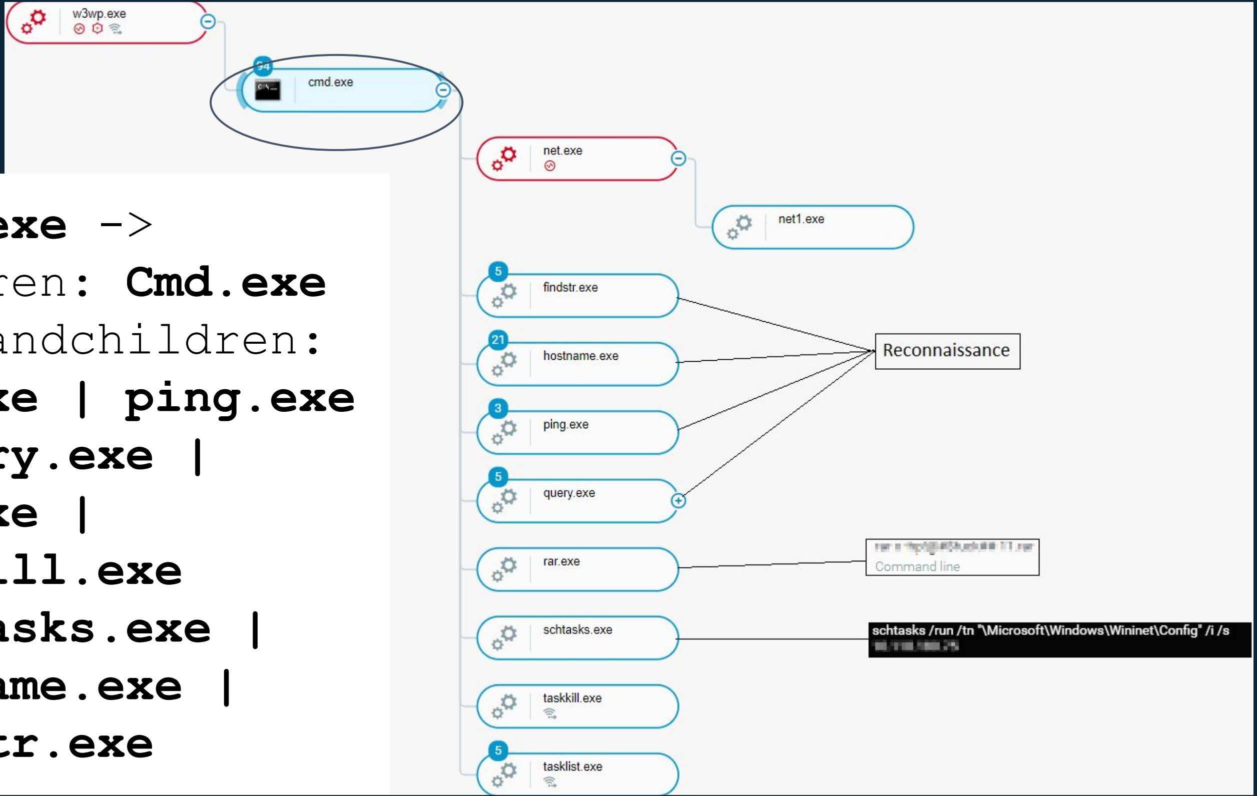
Reconnaissance

[redacted]
Command line

```
schtasks /run /tn "\Microsoft\Windows\Wininet\Config" /i /s
[redacted]
```

Hunting Hafnium

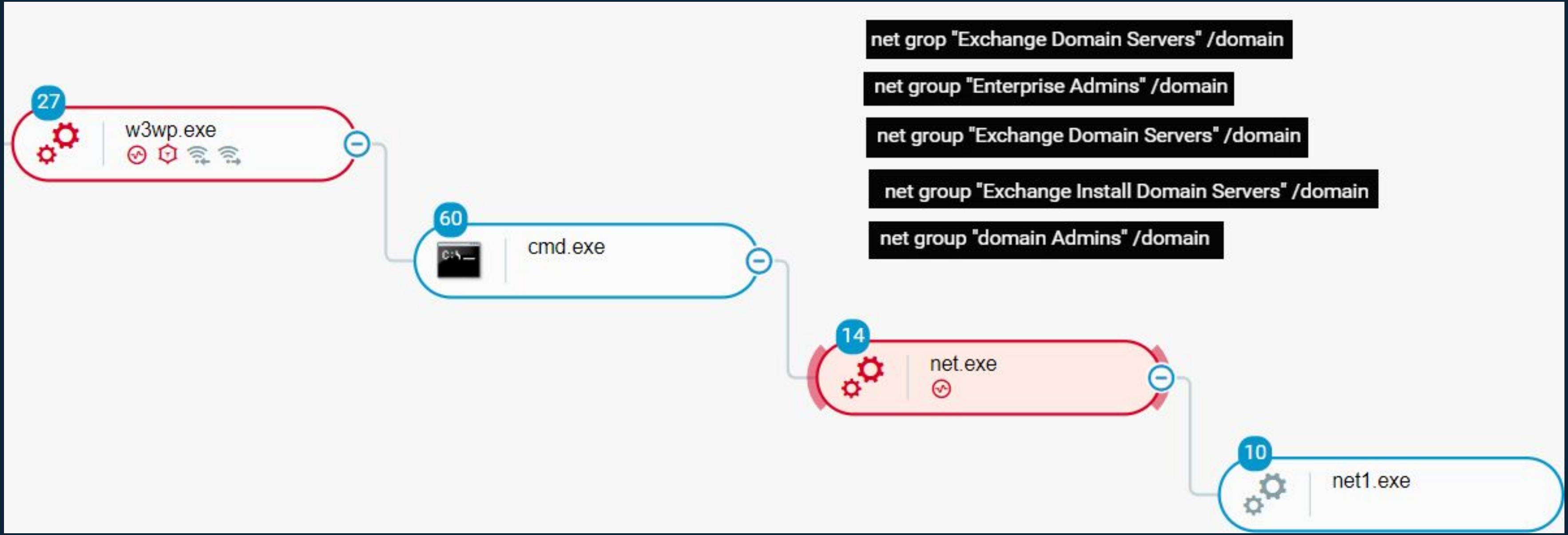
w3wP.exe -> Children: **Cmd.exe** **->** Grandchildren: **net.exe | ping.exe | query.exe | rar.exe | taskkill.exe |schtasks.exe | hostname.exe | findstr.exe**



[redacted]

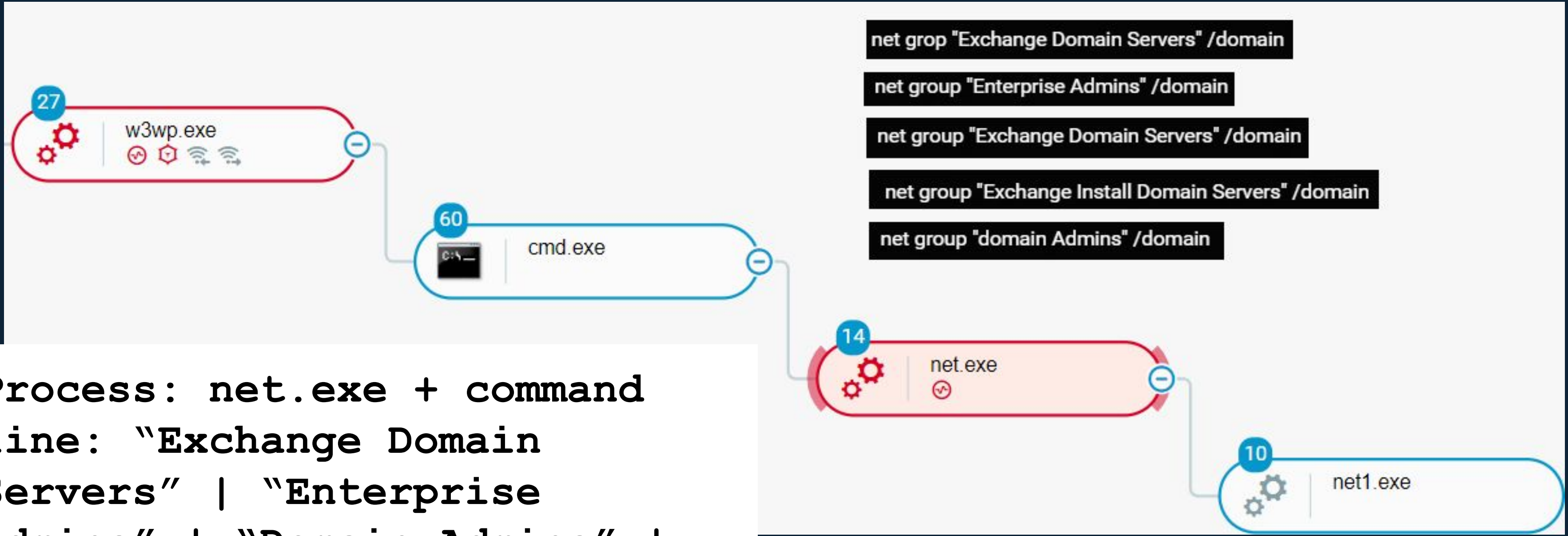
```
schtasks /run /tn "\Microsoft\Windows\Wininet\Config" /i /s [redacted]
```

Hunting Hafnium



```
net grop "Exchange Domain Servers" /domain
net group "Enterprise Admins" /domain
net group "Exchange Domain Servers" /domain
net group "Exchange Install Domain Servers" /domain
net group "domain Admins" /domain
```

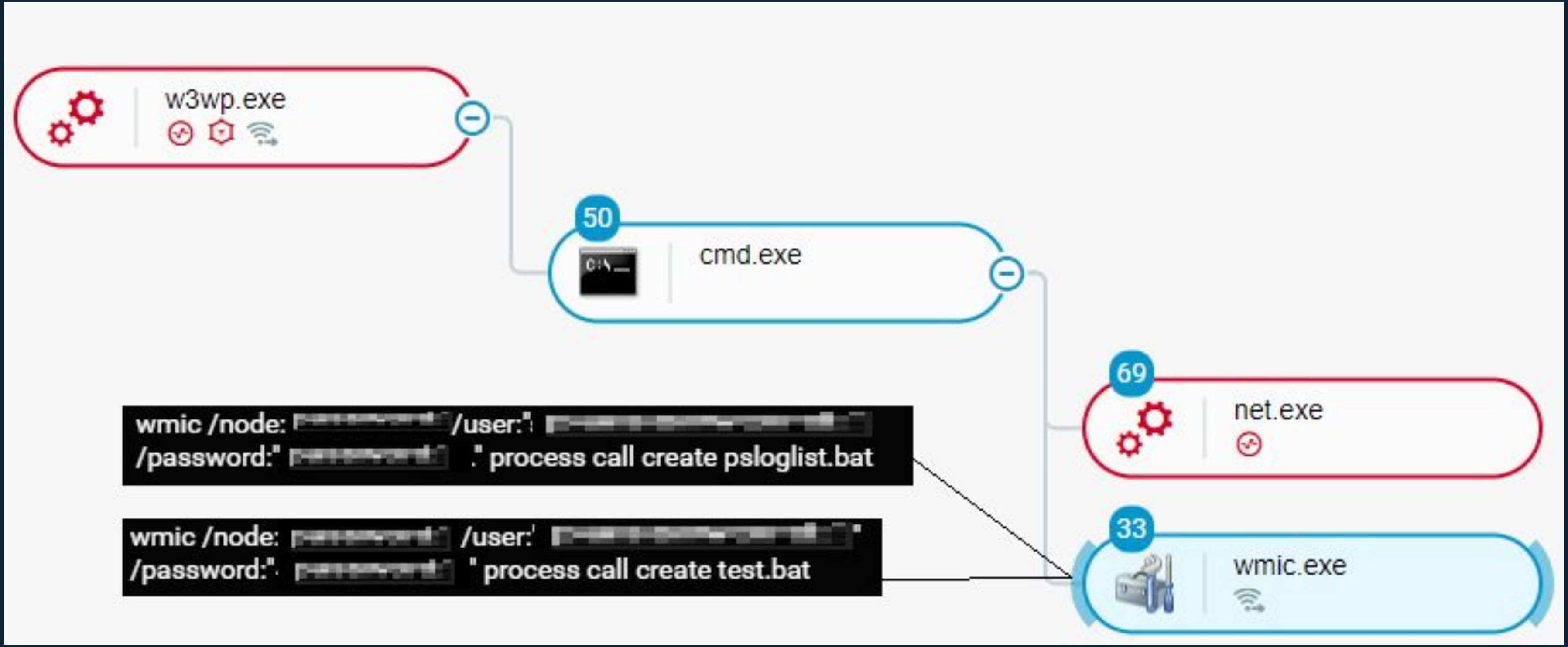
Hunting Hafnium



```
net grop "Exchange Domain Servers" /domain
net group "Enterprise Admins" /domain
net group "Exchange Domain Servers" /domain
net group "Exchange Install Domain Servers" /domain
net group "domain Admins" /domain
```

Process: net.exe + command line: “Exchange Domain Servers” | “Enterprise Admins” | “Domain Admins” | ...

Hunting Hafnium

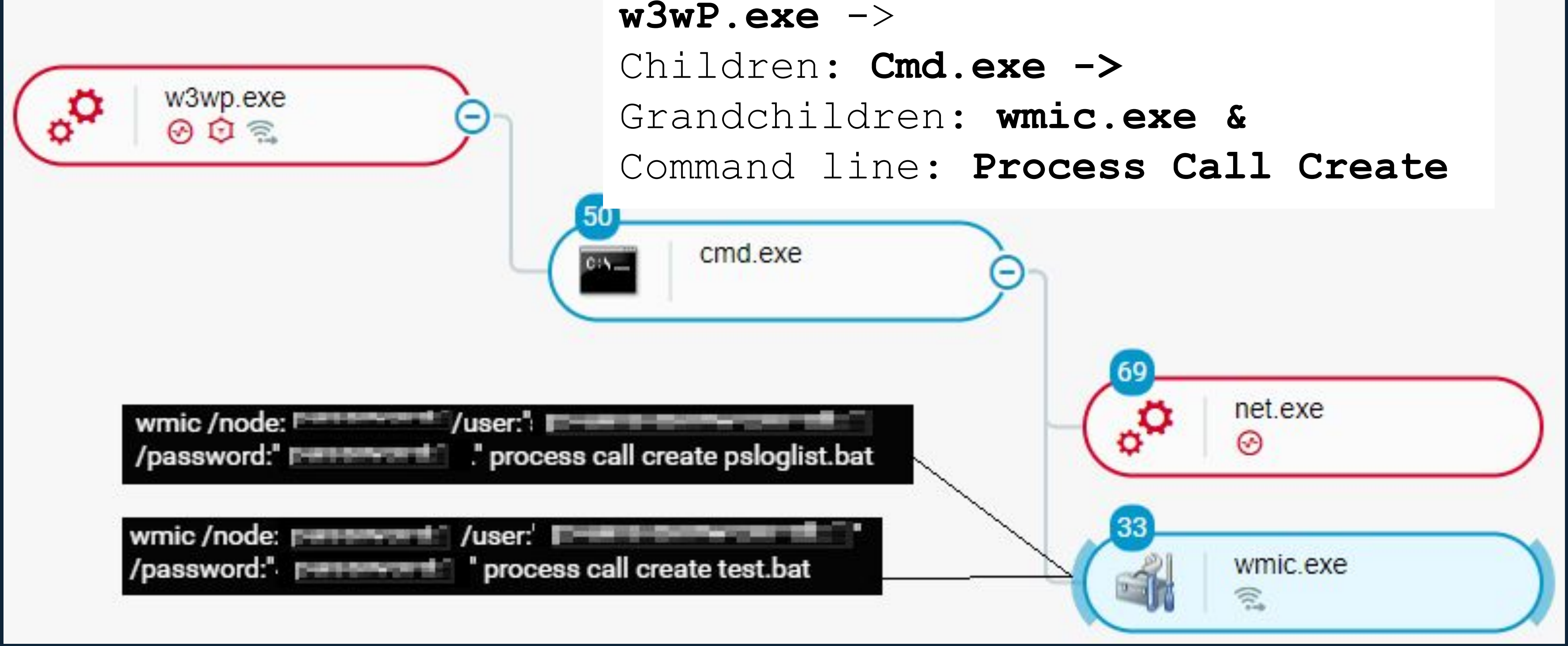


```
wmic /node: [redacted] /user:" [redacted]
/password:" [redacted] ." process call create psloglist.bat
```

```
wmic /node: [redacted] /user:' [redacted] "
/password:". [redacted] " process call create test.bat
```

Hunting Hafnium

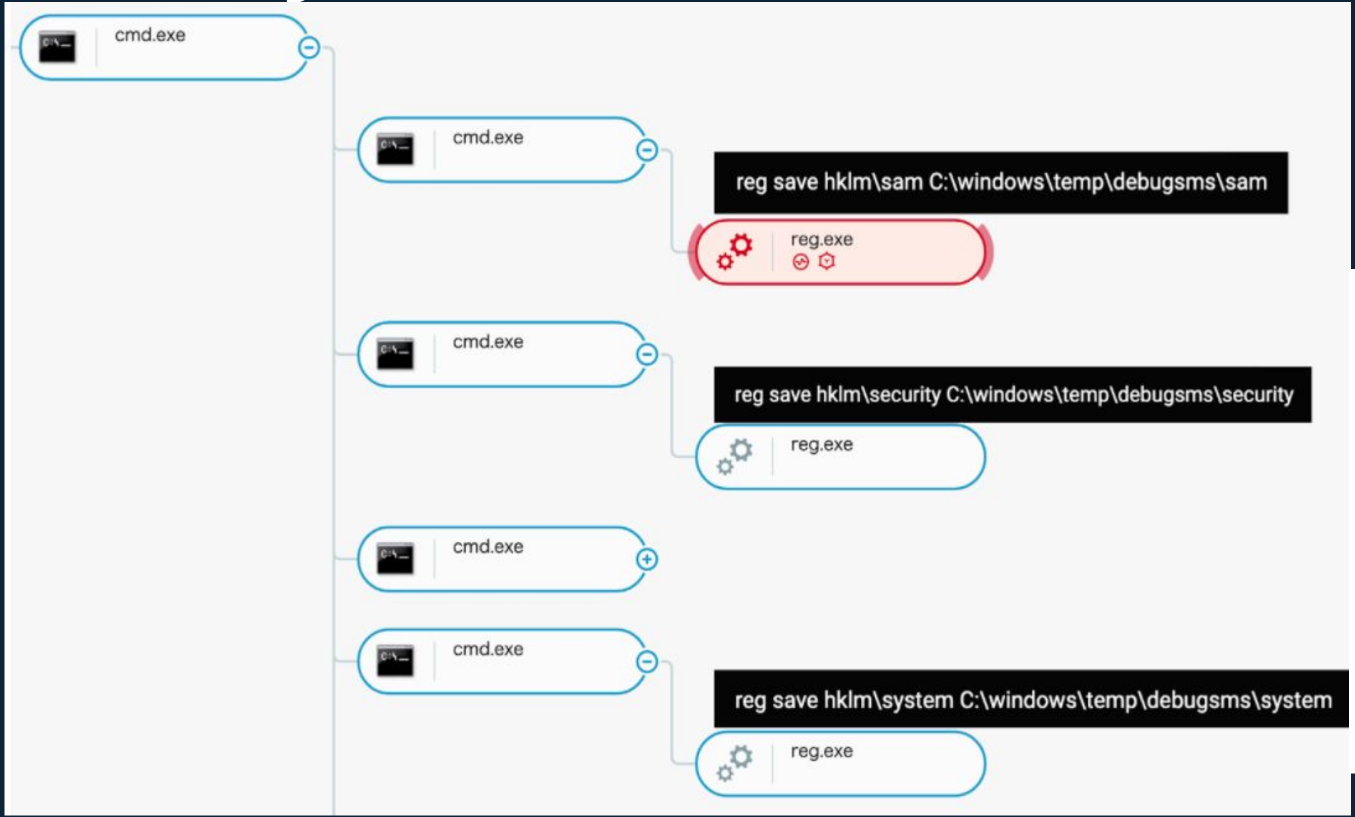
w3wP.exe ->
Children: **Cmd.exe ->**
Grandchildren: **wmic.exe &**
Command line: **Process Call Create**



```
wmic /node: [redacted] /user:' [redacted]
/password:" [redacted] ." process call create psloglist.bat
```

```
wmic /node: [redacted] /user:' [redacted] "
/password:". [redacted] " process call create test.bat
```

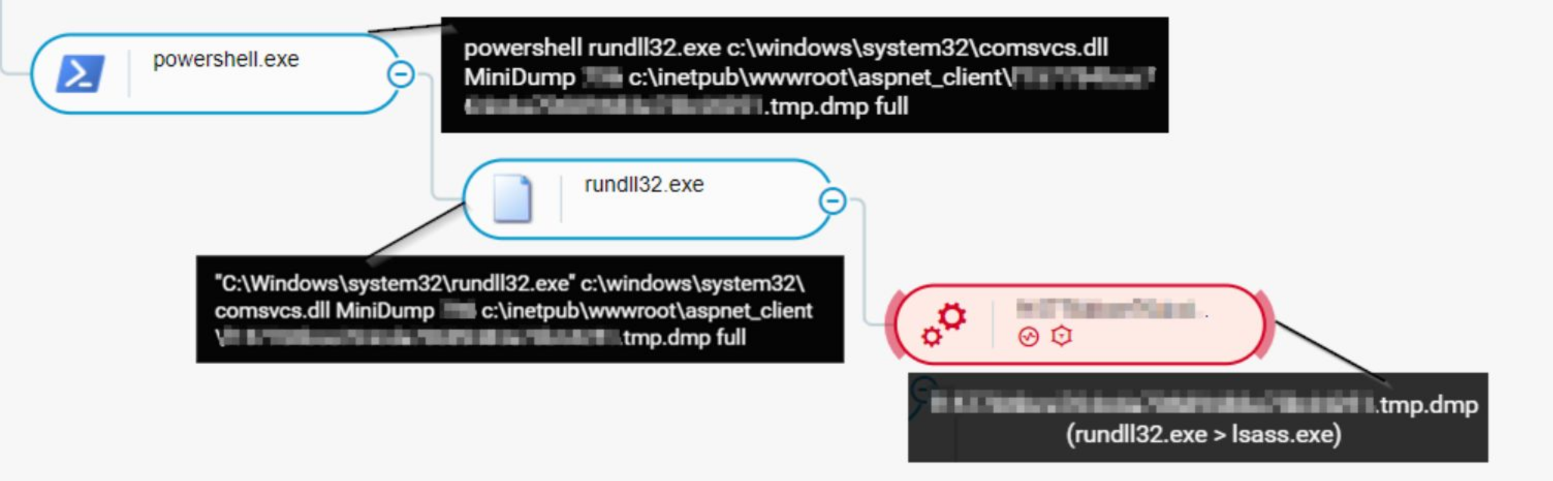
Hunting Hafnium



```
reg save hklm\sam C:\windows\temp\debugsms\sam
reg save hklm\security C:\windows\temp\debugsms\security
reg save hklm\system C:\windows\temp\debugsms\system
```

Process: Reg.exe **AND Command line:** save **AND** (hklm\sam | hklm\security | hklm\system)

Hunting Hafnium



powershell rundll32.exe c:\windows\system32\comsvcs.dll MiniDump [redacted] c:\inetpub\wwwroot\aspnet_client\[redacted].tmp.dmp full

"C:\Windows\system32\rundll32.exe" c:\windows\system32\comsvcs.dll MiniDump [redacted] c:\inetpub\wwwroot\aspnet_client\[redacted].tmp.dmp full

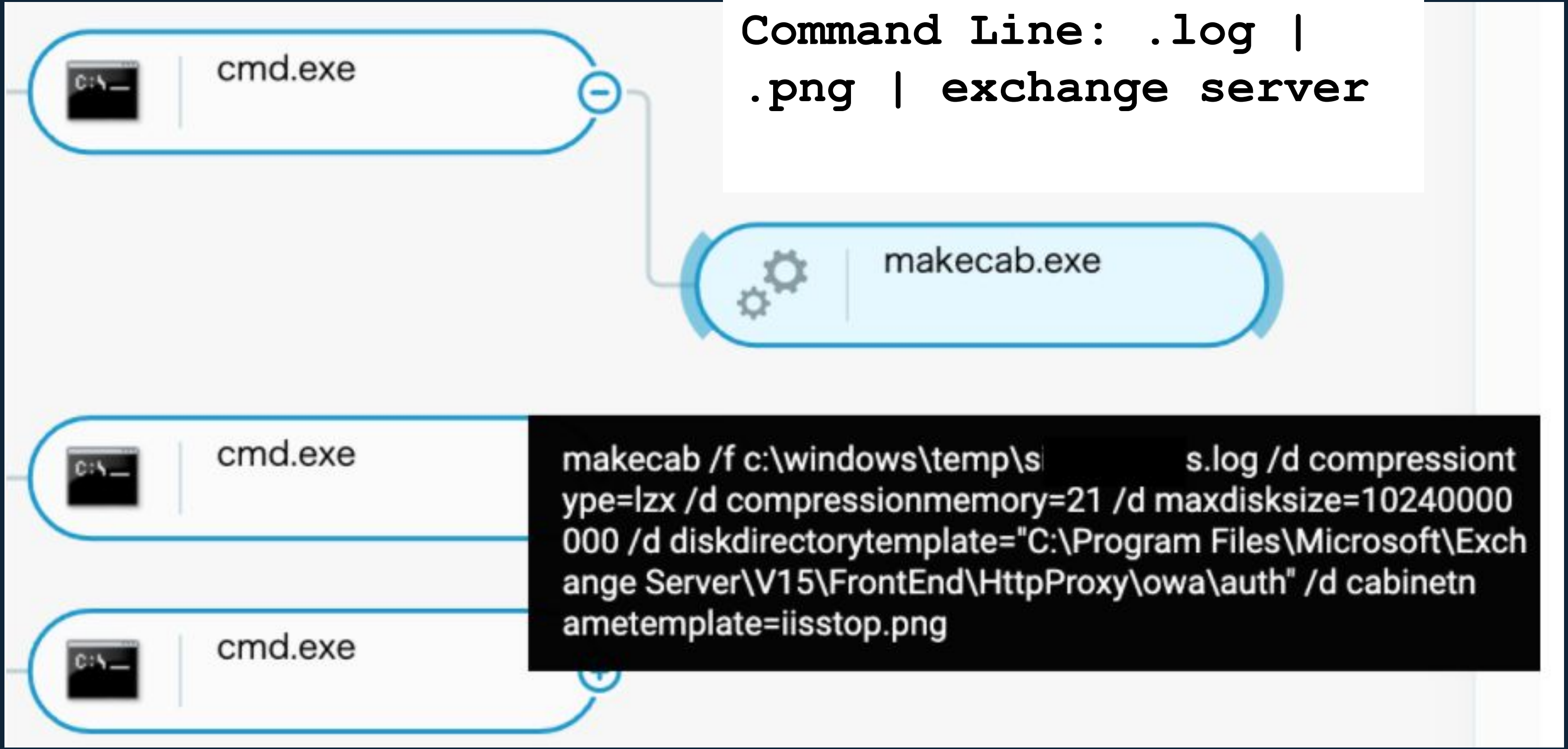
[redacted].tmp.dmp
(rundll32.exe > lsass.exe)

```
Process: Powershell.exe AND
Command line: comsvcs.dll AND
minidump
```

cybereason

Hunting Hafnium

```
Process:makecab.exe AND
Command Line: .log |
.png | exchange server
```



```
makecab /f c:\windows\temp\s[redacted]s.log /d compressiont
ype=lzx /d compressionmemory=21 /d maxdisksize=10240000
000 /d diskdirectorytemplate="C:\Program Files\Microsoft\Exch
ange Server\V15\FrontEnd\HttpProxy\owa\auth" /d cabinetn
ametemplate=iisstop.png
```

CREDIT TO OUR GREAT TEAM

- Omer Yampel
- Niamh O'connor
- Matt Hart
- Yuval Chudy
- Ilan Sokolovsky
- Mor Levi

Just do it!

- Threat hunting is a very broad and dynamic subject
- Solarwinds and ProxyLogon threats
- Happy hunting!

cybereason®