It’s ~~Maps~~ Gaps All the Way Down

Why detection and incident response are hard and what can be done to make them easier

red canary

Process spawned

`c:\windows\explorer.exe` `62022614d1d9290cd1069234f2a55cf8ef8f1572b02157ee8d4d16903c963de0d026fc1a1c565bfa6448ddc9cb0a8da1`

Process spawned by explorer.exe

`c:\windows\system32\conhost.exe` `81ca40085fc75babd2c91d18aa9ffa686651ab6c5c6d85c86b0c6c532115662e09f338fa8cc1233e1434139346f25ef6`

Process spawned by conhost.exe

`c:\windows\system32\cmd.exe` `8a2122e8162dbef04694b9c3e0b6cdeeb99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450`

Overview

Introductions

- Who are you?
- Who am I?

Why are Detection and Security Incident Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

THING ONE

Introductions

red canary

Who are you?

- Raise your hand if you do detection
- Raise your hand if you do security incident response
- Keep your hand up if you think your job is hard

Go Blue Team!

red canary

It’s not just you

“… security is quite possibly the most intellectually challenging profession on the planet… for two reasons… complexity… and rate of change [are] your enemy.”

-- Dan Geer

red canary

Who am I?

Dave Hull

Detection Engineer

RED CANARY

@davehull

- Detection engineering at Red Canary
- Former technical lead for IR in O365
- Former SANS instructor, blogger, editor
- Creator of Kansa -- a framework for collecting and analyzing endpoint data
- I pick up pennies in front of steam rollers

red canary

Overview

~~Introductions~~

- ~~Who are you?~~
- ~~Who am I?~~

Why are Detection and Security Incident Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Every pen tester’s favorite topic

What’s out of scope?

Some hard problems and some easy ones.

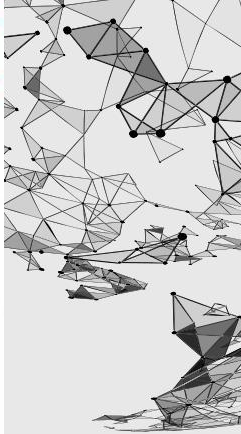
Threat occurred

File first wrote
`c:\windows\system32\[REDACTED]`

Process spawned by services.exe
`c:\windows\system32\cmd.exe` 8a2122e8162dbef04694b9c3e0b6cdee
b99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450

•••

Command Line:
```
C:\WINDOWS\system32\cmd.exe /b /c start /b /min powershell.exe -nop -w
hidden -noni -c "if([IntPtr]::Size -eq 4)
{$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}else{$b='powershell.ex
e'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni
-nop -w hidden -c $v2=(''Enabl{3''+''}Scri{2}tBloc{1}
{''+''4}n{0}''+''ocation''+''{5''+''}og''+''ging''+''''')-
f''v'',''k'',''p'',''e'',''I'',''L'');If($PSVersionTable.PSVersion.Major -ge 3){
((''{0''+''}c''+''r''+''iptB{1}ockLoggi''+''{2}g'')-f''S'',''l'',''n''); $uZr=
((''En{2}bl{0}Scri{''+''1}tBloc{''+''3}Log''+''g''+''i''+''ng'')-
```



red canary

[REDACTED] UTC [REDACTED] [REDACTED] [REDACTED]

WIN-POWERSHELL-IEX-CMDLINE-CHAR

WIN-KNOWN-POWERSHELL-MAL-CLI

WIN-POWERSHELL-BXOR

WIN-POWERSHELL-WEBPROXY

WIN-POWERSHELL-DATA-DOWNLOAD

WIN-POWERSHELL-SHORTENED-ENCODEDCOMMAND-SWITCH

WIN-POWERSHELL-BASE64-METHOD

WIN-POWERSHELL-OBF-CHAR

WIN-REMOTETHREAD-INJECTION-FROM-POWERSHELL

WIN-POWERSHELL-AMSI-BYPASS

WIN-EVENTVWR-UAC-BYPASS

Let’s talk detections

A “quick” tour of the problem space

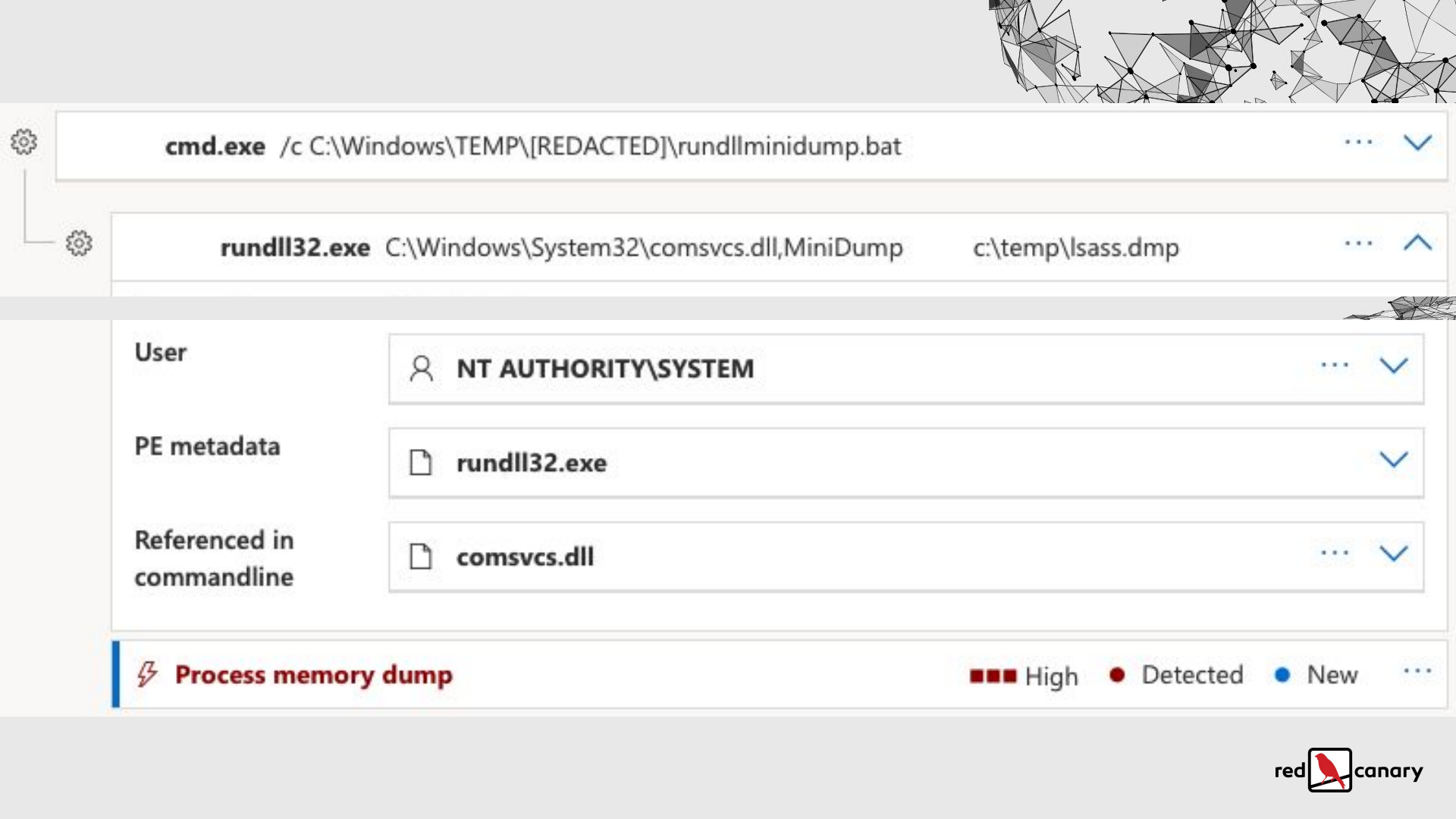
red canary

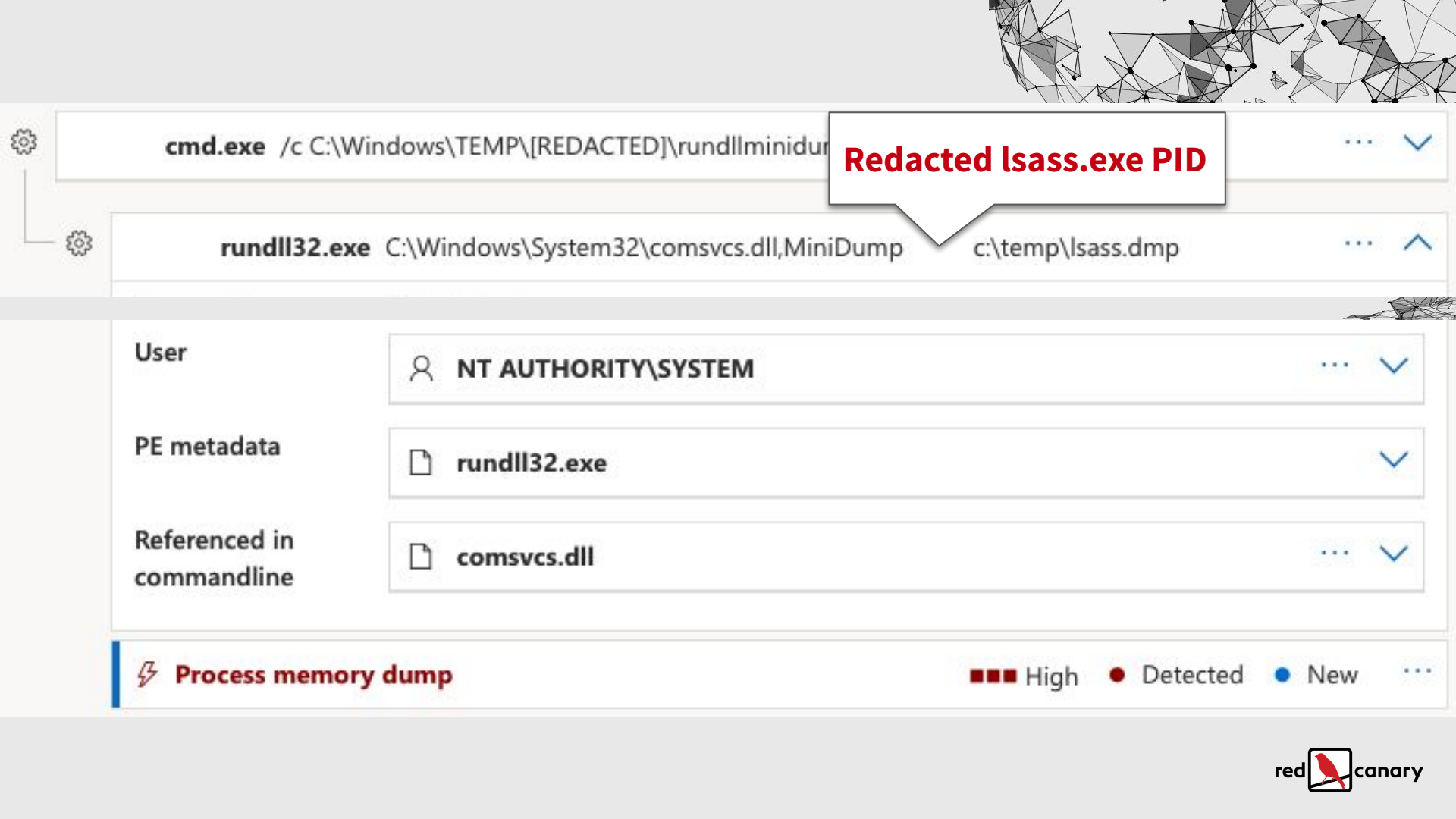
Let’s talk when something bad happens

False positives and false negatives

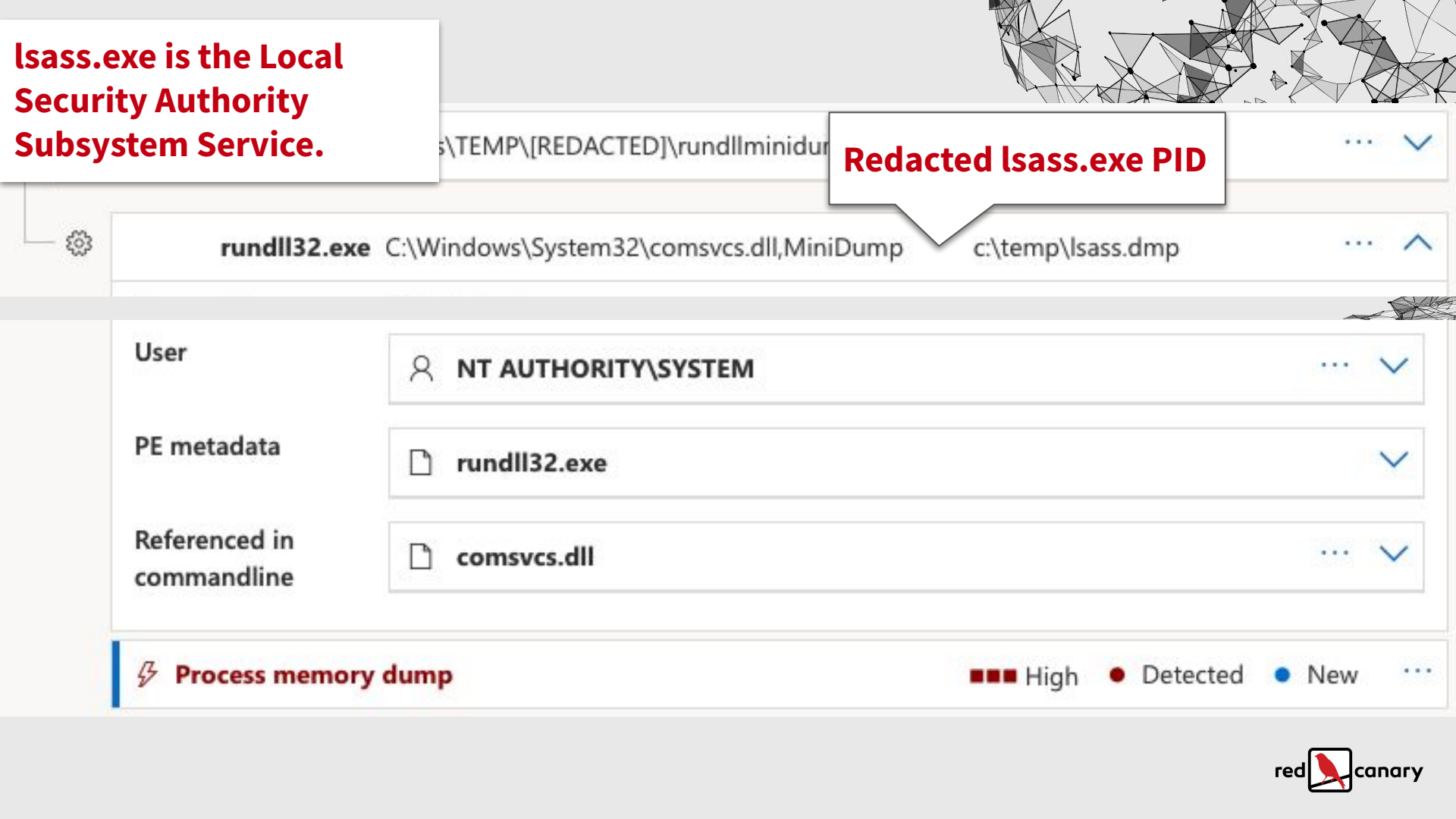
Why are you so negative about false positives?

red canary


cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidump.bat
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
User
NT AUTHORITY\SYSTEM
PE metadata
rundll32.exe
Referenced in commandline
comsvcs.dll
Process memory dump
High
Detected
New

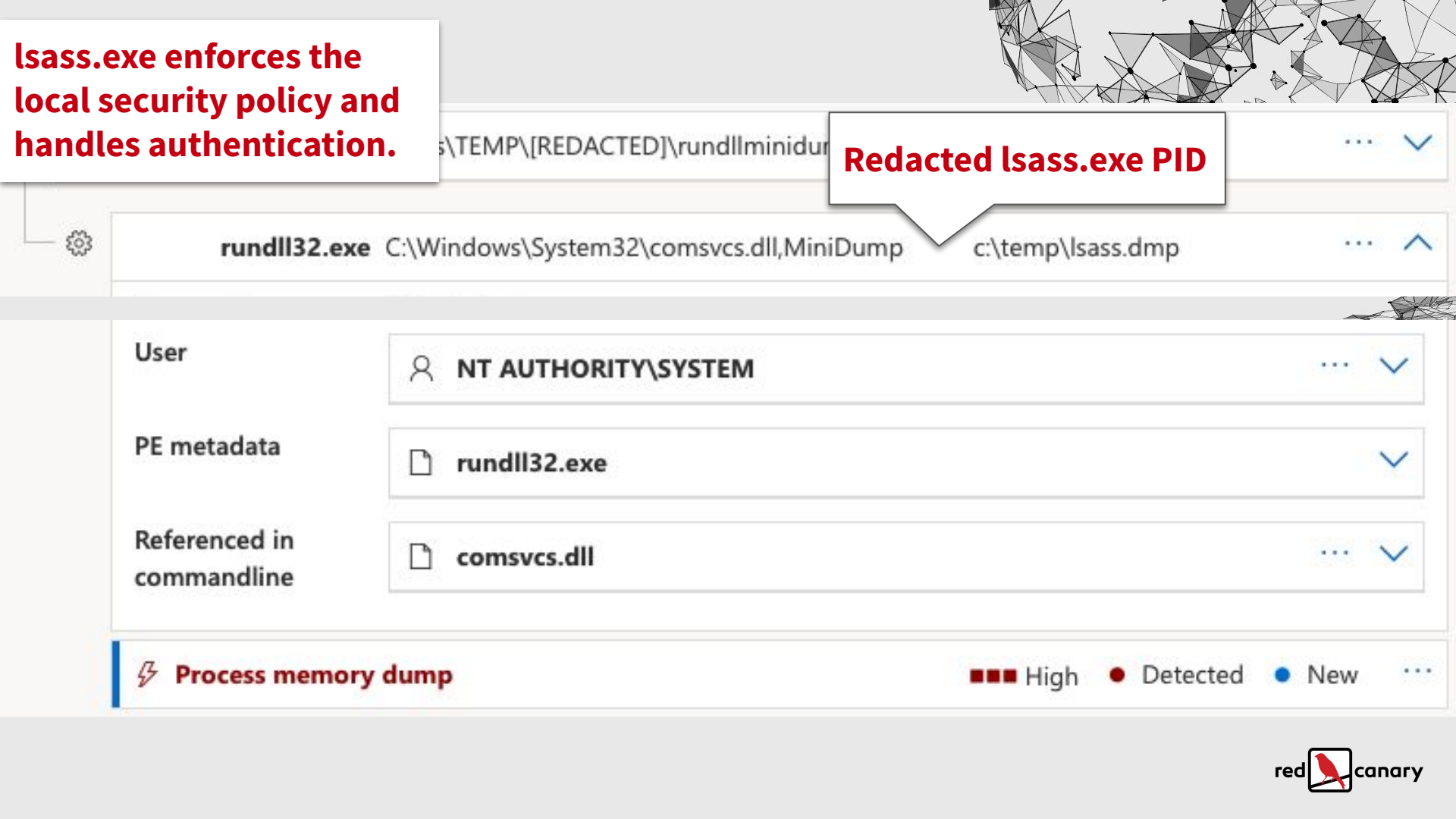

cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidu
Redacted lsass.exe PID
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
User
NT AUTHORITY\SYSTEM
PE metadata
rundll32.exe
Referenced in commandline
comsvcs.dll
Process memory dump
High
Detected
New

lsass.exe is the Local Security Authority Subsystem Service.



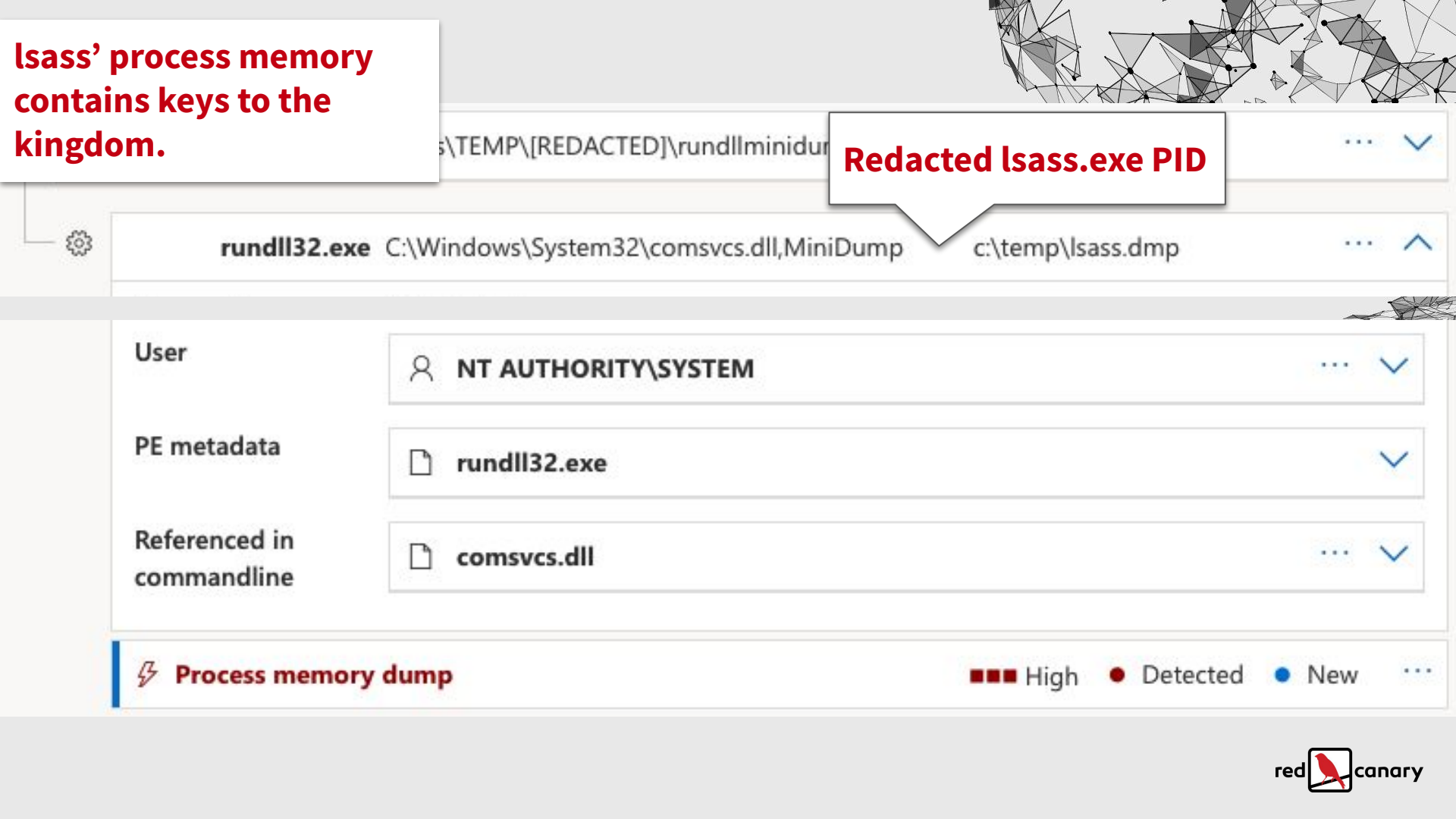
red canary

lsass.exe enforces the local security policy and handles authentication.



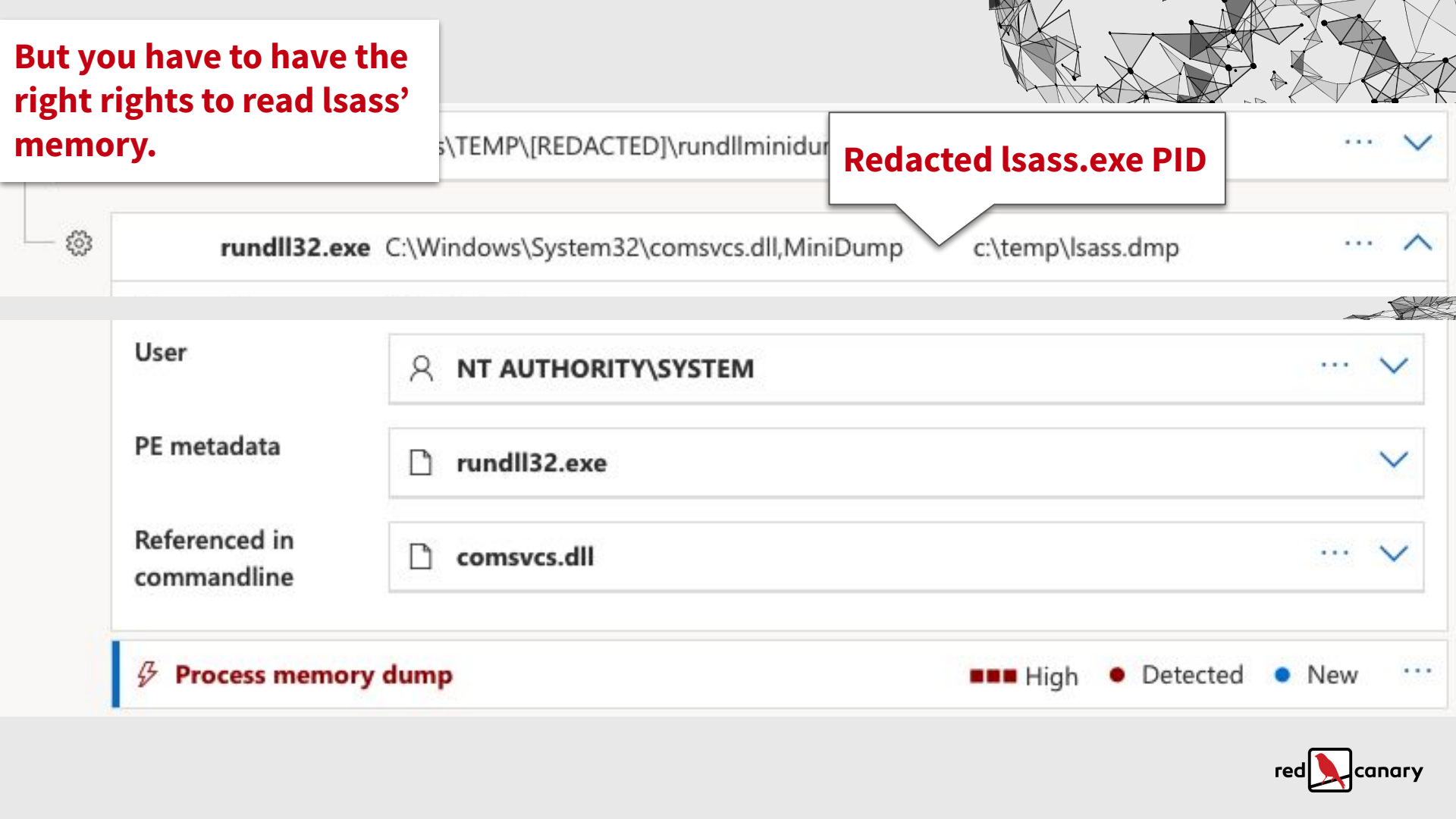
red canary

lsass' process memory contains keys to the kingdom.



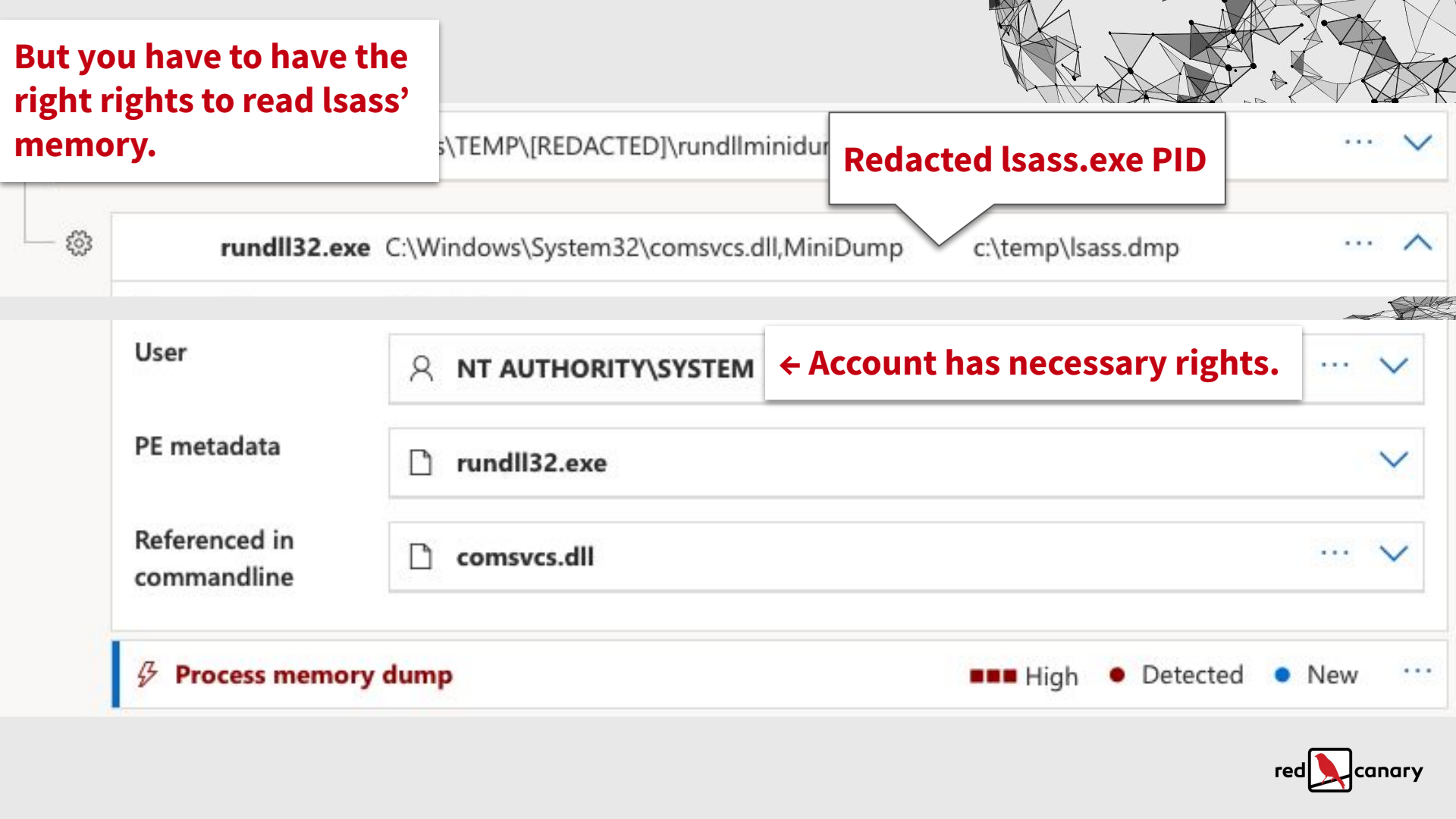
red canary

But you have to have the right rights to read lsass' memory.

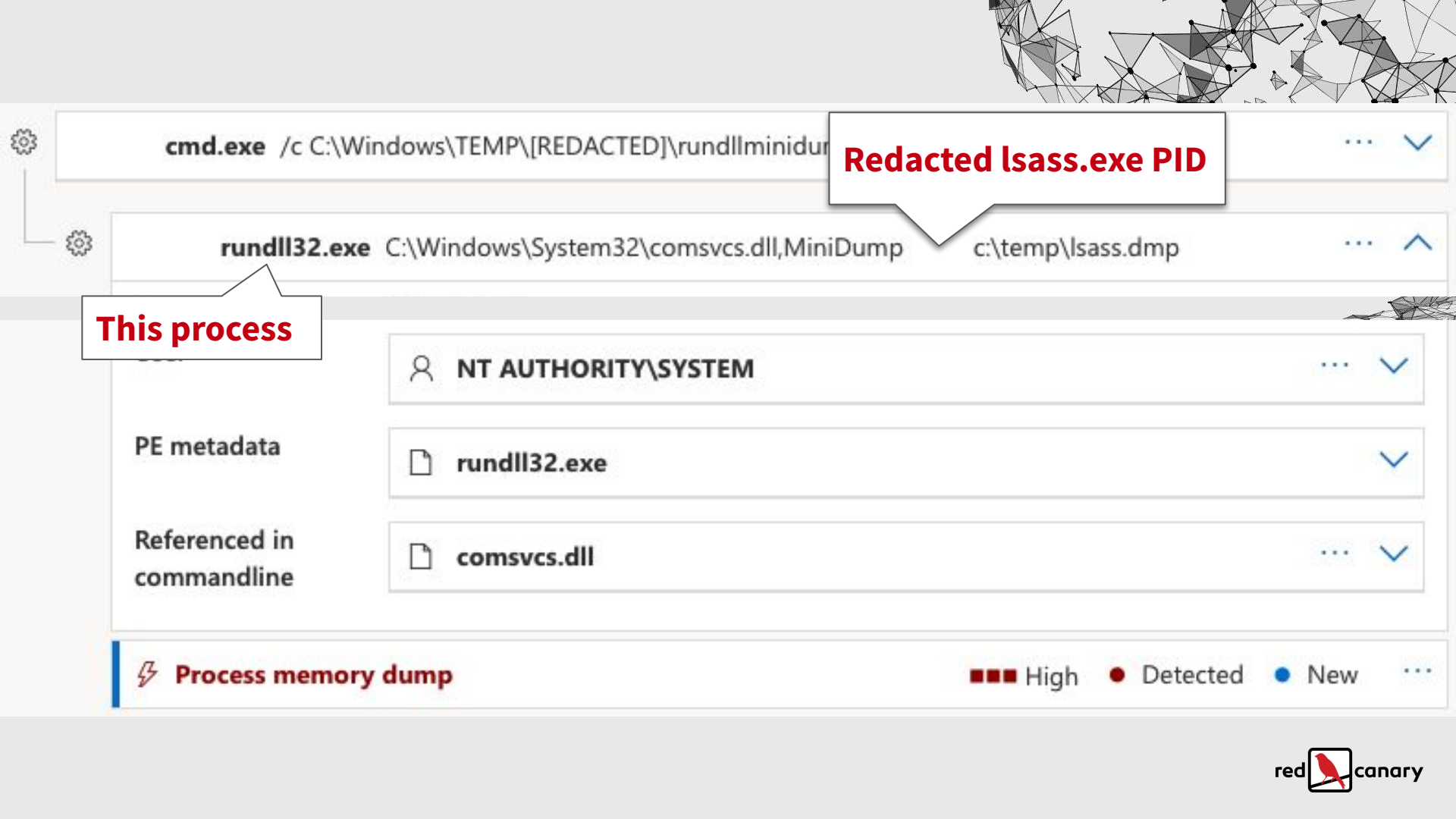


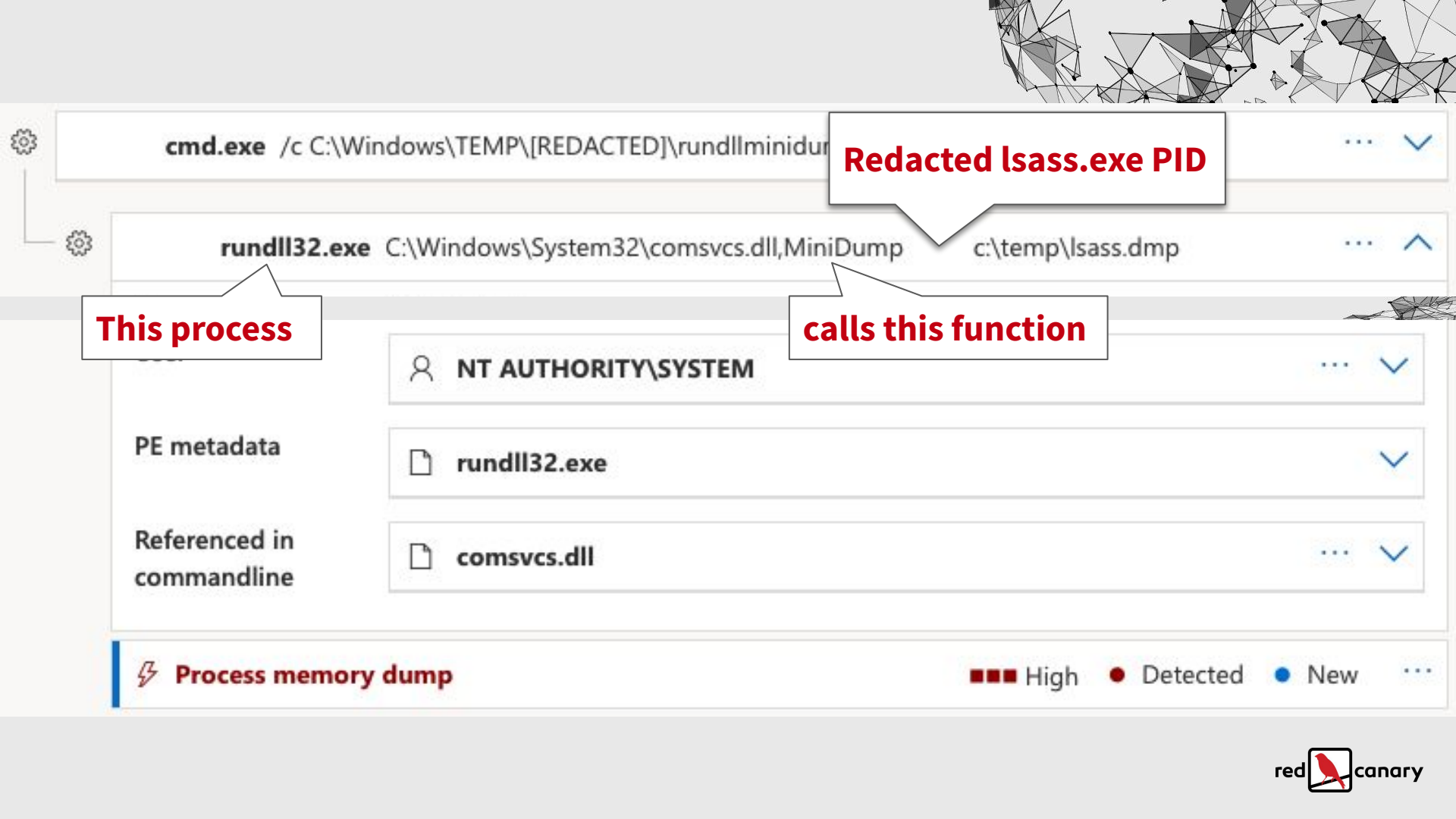
red canary

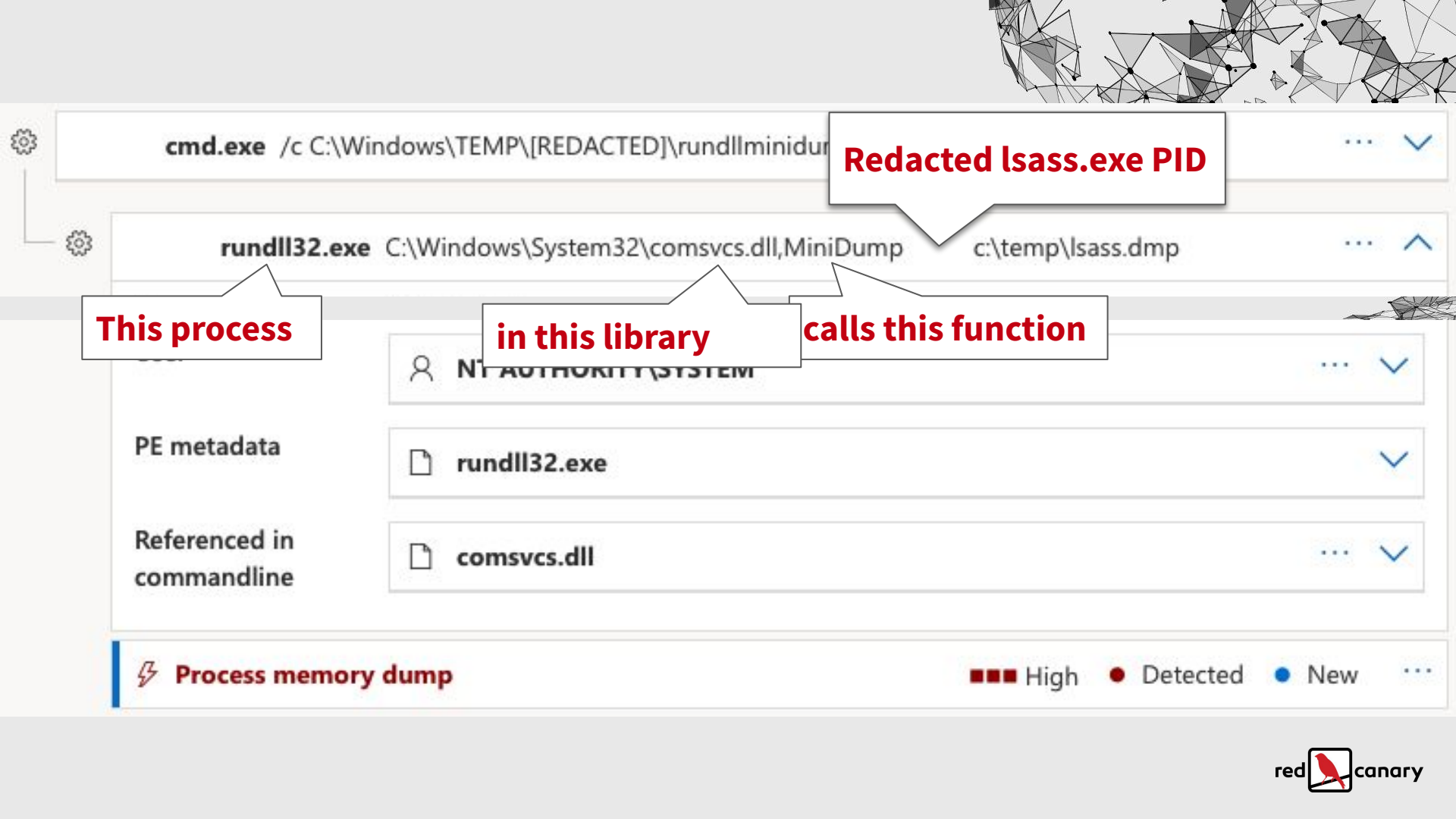
But you have to have the right rights to read lsass' memory.

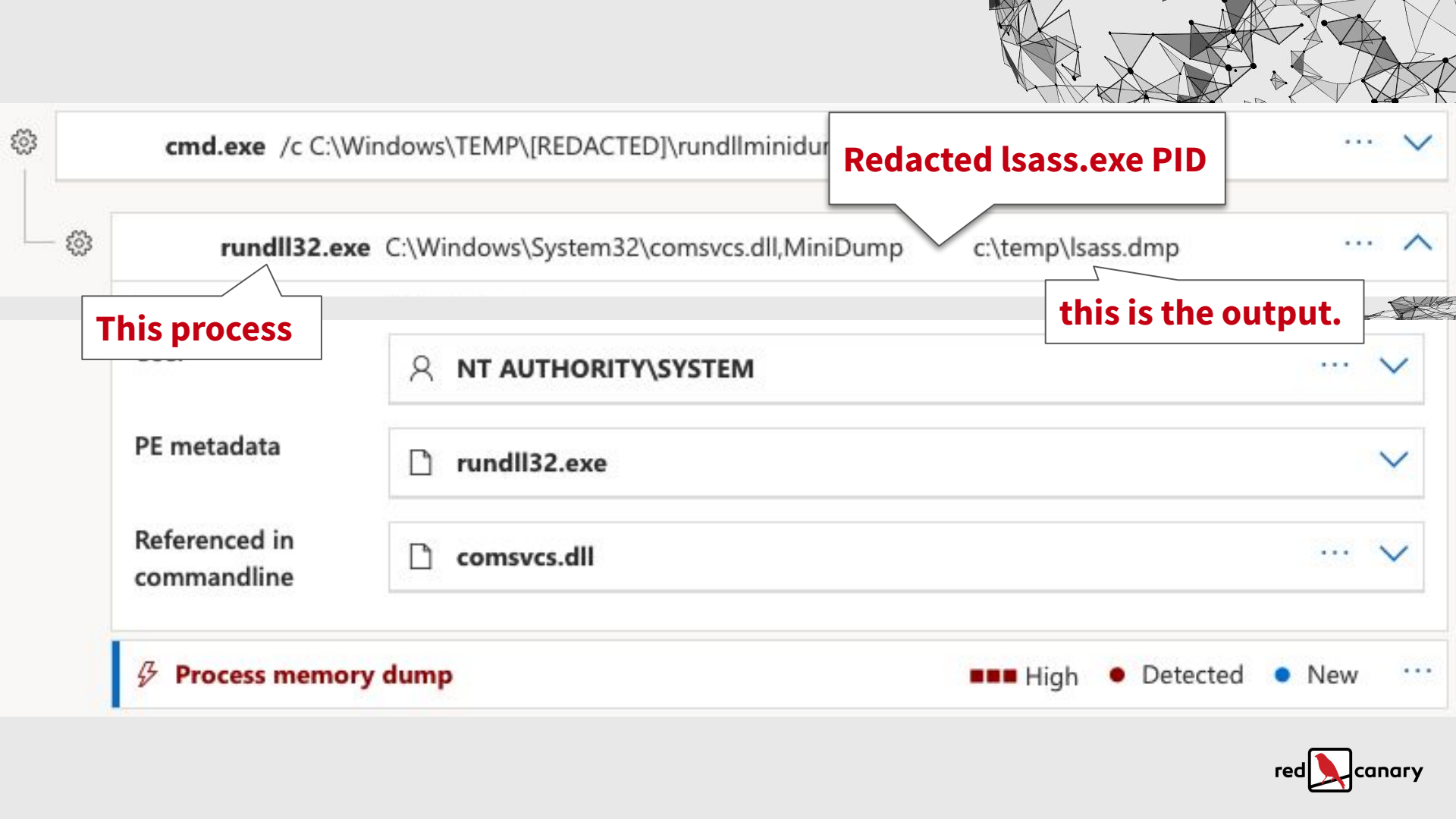


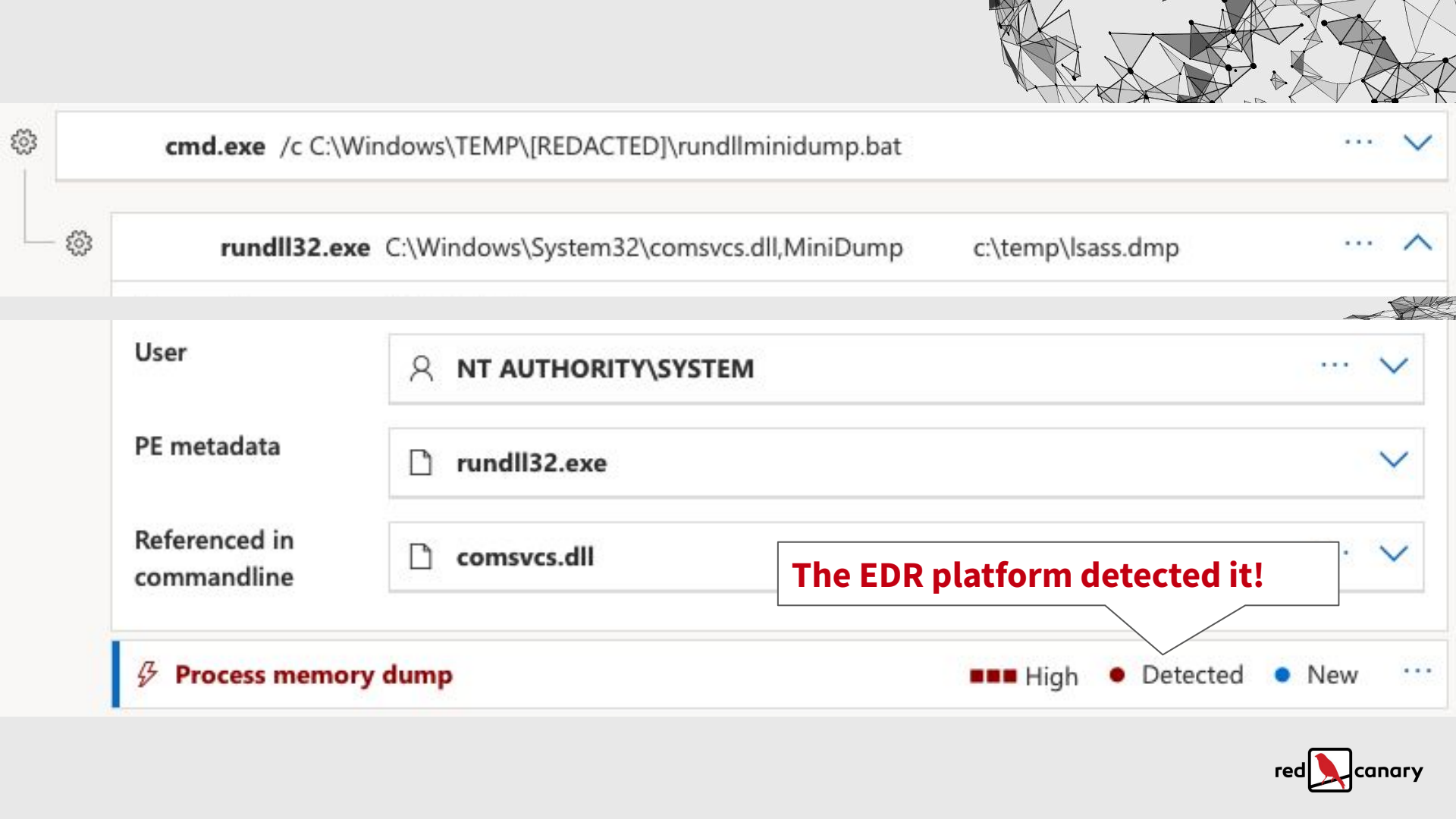
red canary


cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidu
Redacted lsass.exe PID
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
This process
NT AUTHORITY\SYSTEM
PE metadata
rundll32.exe
Referenced in commandline
comsvcs.dll
Process memory dump
High
Detected
New

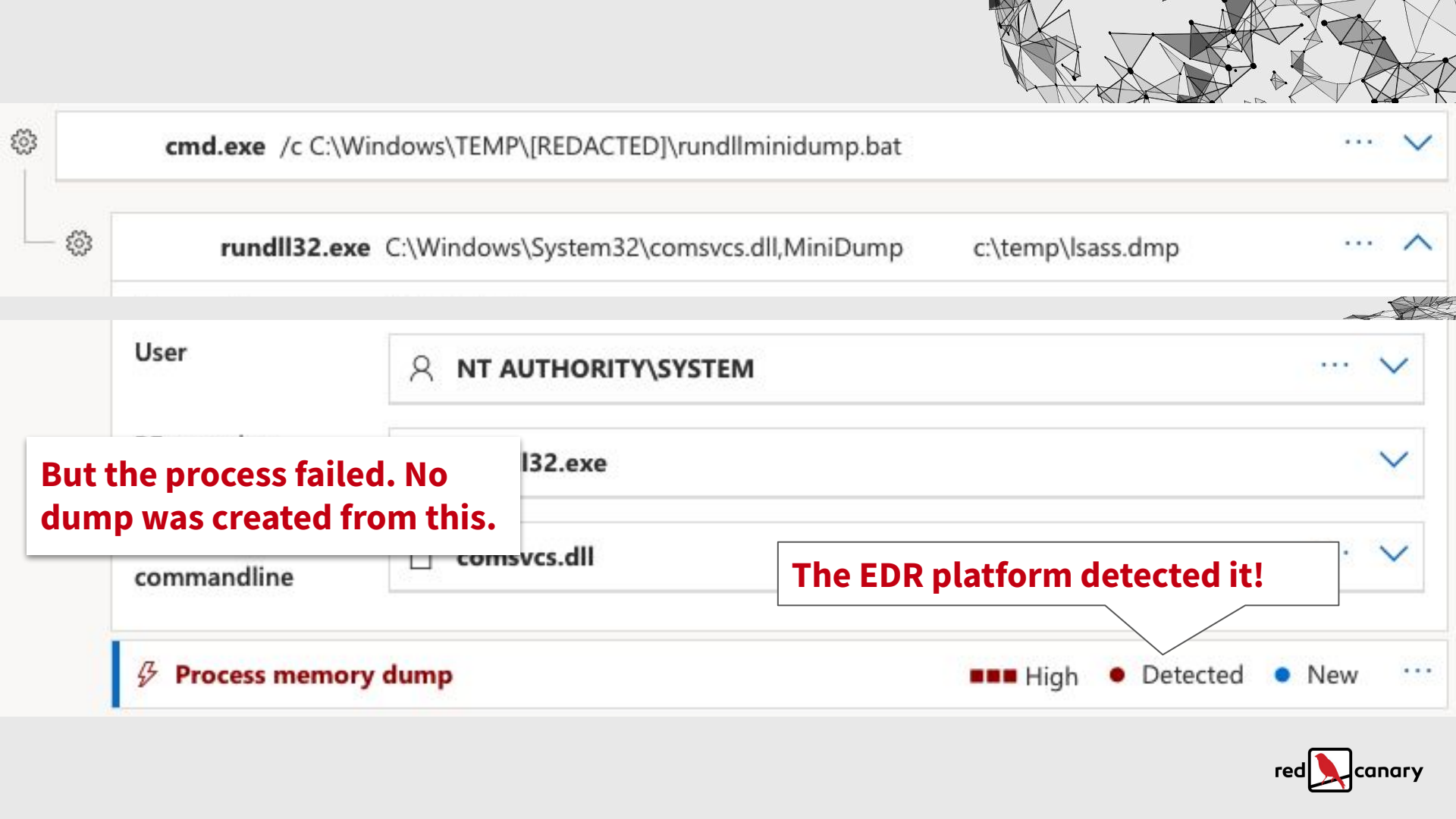

cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidu
Redacted lsass.exe PID
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
This process
calls this function
NT AUTHORITY\SYSTEM
PE metadata
rundll32.exe
Referenced in commandline
comsvcs.dll
Process memory dump
High
Detected
New

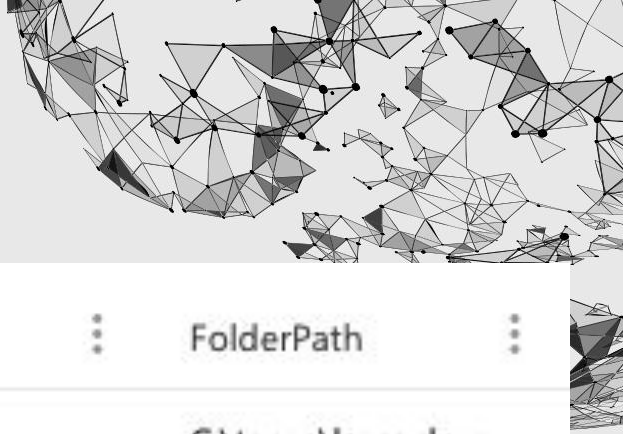

cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidu
Redacted lsass.exe PID
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
This process
in this library
calls this function
PE metadata
rundll32.exe
Referenced in commandline
comsvcs.dll
Process memory dump
High
Detected
New


cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidu
Redacted lsass.exe PID
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
This process
this is the output.
NT AUTHORITY\SYSTEM
PE metadata
rundll32.exe
Referenced in commandline
comsvcs.dll
Process memory dump
High
Detected
New


cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidump.bat
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
User
NT AUTHORITY\SYSTEM
PE metadata
rundll32.exe
Referenced in commandline
comsvcs.dll
The EDR platform detected it!
Process memory dump
High
Detected
New

red canary

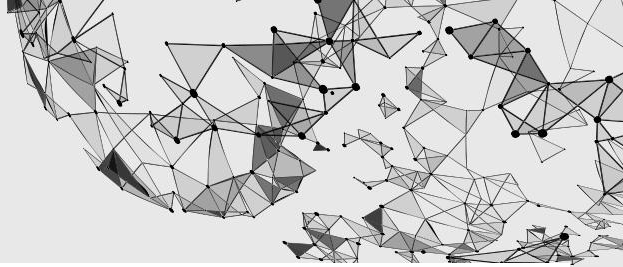

cmd.exe /c C:\Windows\TEMP\[REDACTED]\rundllminidump.bat
rundll32.exe C:\Windows\System32\comsvcs.dll,MiniDump c:\temp\lsass.dmp
User
NT AUTHORITY\SYSTEM
But the process failed. No dump was created from this.
commandline
The EDR platform detected it!
Process memory dump
High
Detected
New



InitiatingProcessFileName	InitiatingProcessParentFileName	FolderPath
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp

This process, however

red canary

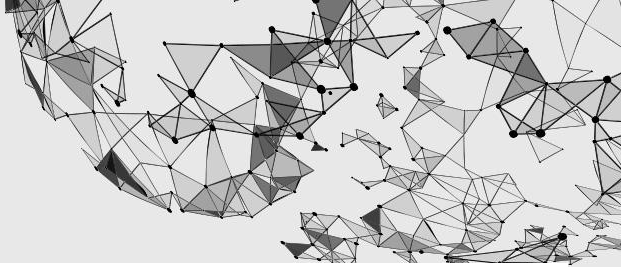


InitiatingProcessFileName	InitiatingProcessParentFileName	FolderPath
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp

This process, however,

succeeded!

red canary



InitiatingProcessFileName	InitiatingProcessParentFileName	FolderPath
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp
createdumpfromsnapshot.exe	cmd.exe	C:\temp\lsass.dmp

Zero alerts given.

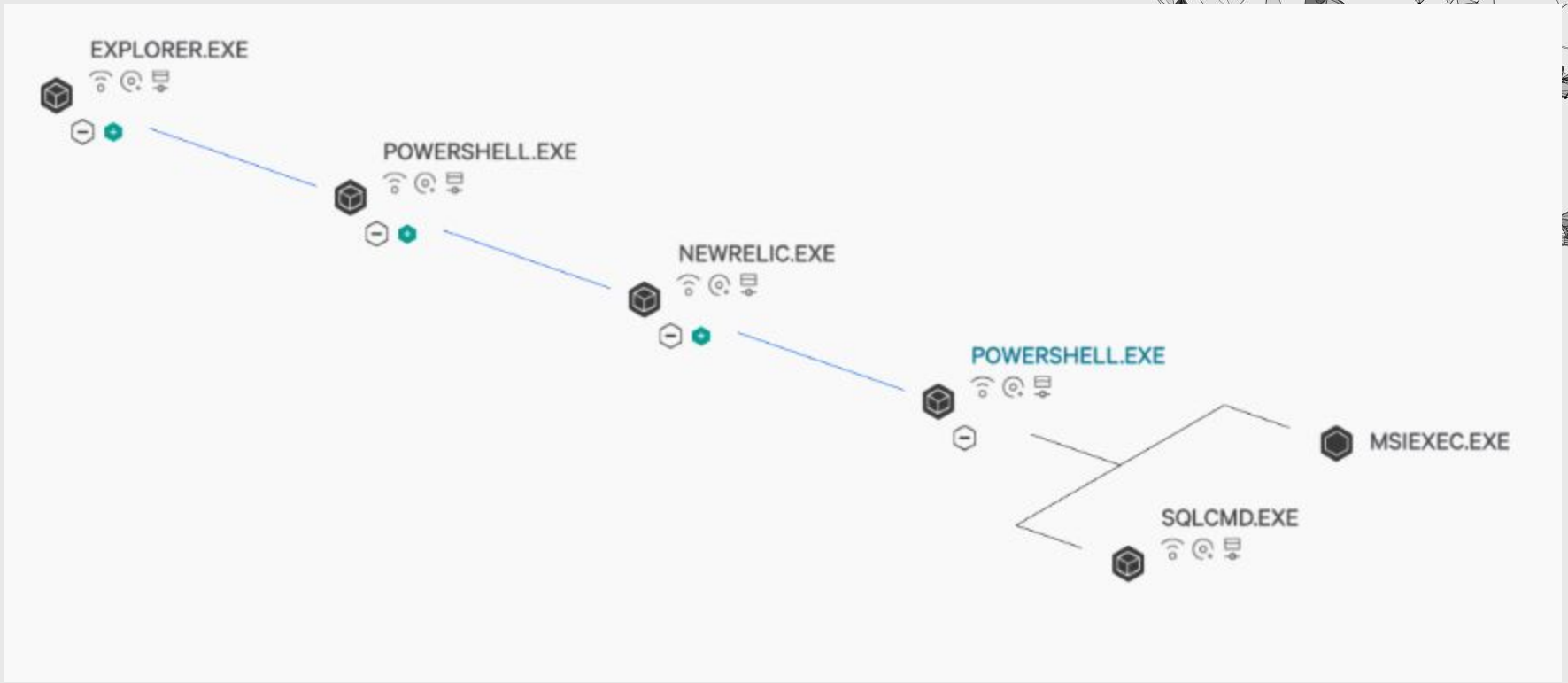
red canary

Make it easy to read

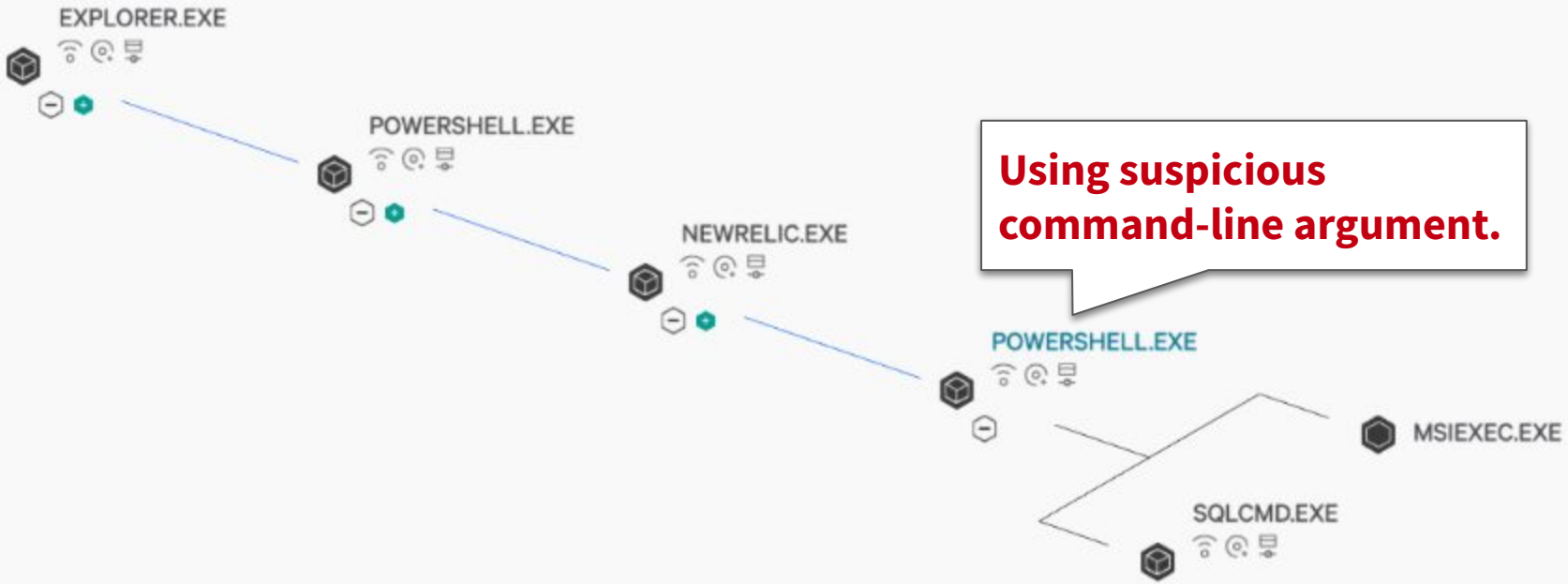
When good software goes bad?

Why are you so emo Tet?

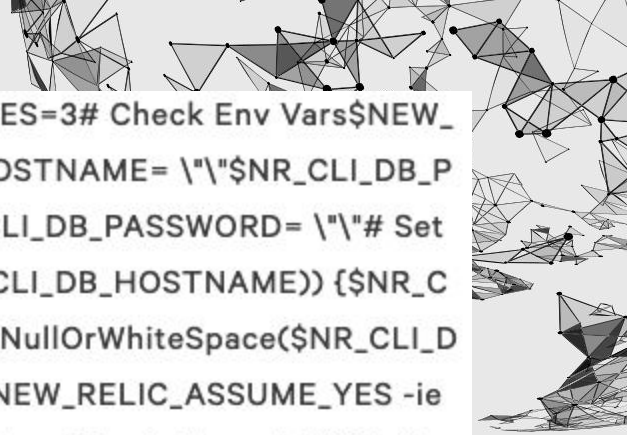
red canary


EXPLORER.EXE
POWERSHELL.EXE
NEWRELIC.EXE
POWERSHELL.EXE
MSIEXEC.EXE
SQLCMD.EXE

red canary


EXPLORER.EXE
POWERSHELL.EXE
NEWRELIC.EXE
POWERSHELL.EXE
Using suspicious command-line argument.
MSIEXEC.EXE
SQLCMD.EXE

red canary



COMMAND LINE

```
powershell -command "$TRIES=0$MAX_RETRIES=3# Check Env Vars$NEW_RELIC_ASSUME_YES= \"false\"$NR_CLI_DB_HOSTNAME= \"\"$NR_CLI_DB_PORT= \"\"$NR_CLI_DB_USERNAME= \"\"$NR_CLI_DB_PASSWORD= \"\"# Set Defaultsif ([string]::IsNullOrWhiteSpace($NR_CLI_DB_HOSTNAME)) {$NR_CLI_DB_HOSTNAME = \"127.0.0.1\"}if ([string]::IsNullOrWhiteSpace($NR_CLI_DB_PORT)) {$NR_CLI_DB_PORT = \"1433\"}if ($NEW_RELIC_ASSUME_YES -ieq \"false\") { DO { $NR_CLI_DB_HOSTNAME = Read-Host -Prompt \"SQL Server Hostname or IP (default: 127.0.0.1)\" if ([string]::IsNullOrWhiteSpace($NR_CLI_DB_HOSTNAME)) {$NR_CLI_DB_HOSTNAME = \"127.0.0.1\"} $NR_CLI_DB_PORT = Read-Host -Prompt \"SQL Server Port (default: 1433)\" if ([string]::IsNullOrWhiteSpace($NR_CLI_DB_PORT)) {$NR_CLI_DB_PORT = \"1433\"} $NR_CLI_DB_USERNAME = Read-Host -Prompt \"MSSQL Username\" $NR_CLI_DB_PASSWORD = Read-Host -Prompt \"MSSQL Password\" -AsSecureString $bstr = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($NR_CLI_DB_PASSWORD) $NR_CLI_DB_PASSWORD = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($bstr) $TRIES++ if ([string]::IsNullOr
```

COMMAND LINE

```
powershell -command "$TRIES=0$MAX_RETRIES=3# Check Env Vars$NEW_
RELIC_ASSUME_YES= \"false\"$NR_CLI_DB_HOSTNAME= \"\"$NR_CLI_DB_P
ORT= \"\"$NR_CLI_DB_USERNAME= \"\"$NR_CLI_DB_PASSWORD= \"\"# Set
Defaultsif ([string]::IsNullOrWhiteSpace($NR_CLI_DB_HOSTNAME)) {$NR_C
LI_DB_HOSTNAME = \"127.0.0.1\"}if ([string]::IsNullOrWhiteSpace($NR_CLI_D
B_PORT)) {$NR_CLI_DB_PORT = \"1433\"}if ($NEW_RELIC_ASSUME_YES -ie
q \"false\") { DO { $NR_CLI_DB_HOSTNAME = Read-Host -Prompt \"SQL Ser
ver Hostname or IP (default: 127.0.0.1)\" if ([string]::IsNullOrWhiteSpace($NR
_CLI_DB_HOSTNAME)) {$NR_CLI_DB_HOSTNAME = \"127.0.0.1\"} $NR_CLI_D
B_PORT = Read-Host -Prompt \"SQL Server Port (default: 1433)\" if ([strin
g]::IsNullOrWhiteSpace($NR_CLI_DB_PORT)) {$NR_CLI_DB_PORT = \"1433\"}
$NR_CLI_DB_USERNAME = Read-Host -Prompt \"MSSQL Username\" $NR_C
LI_DB_PASSWORD = Read-Host -Prompt \"MSSQL Password\" -AsSecureStri
) $bstr = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR
($NR_CLI_DB_PASSWORD) $NR_CLI_DB_PASSWORD = [System.Runtime.Inte
ropServices.Marshal]::PtrToStringAuto($bstr) $TRIES++ if ([string]::IsNullOr
```

Emotet does this →

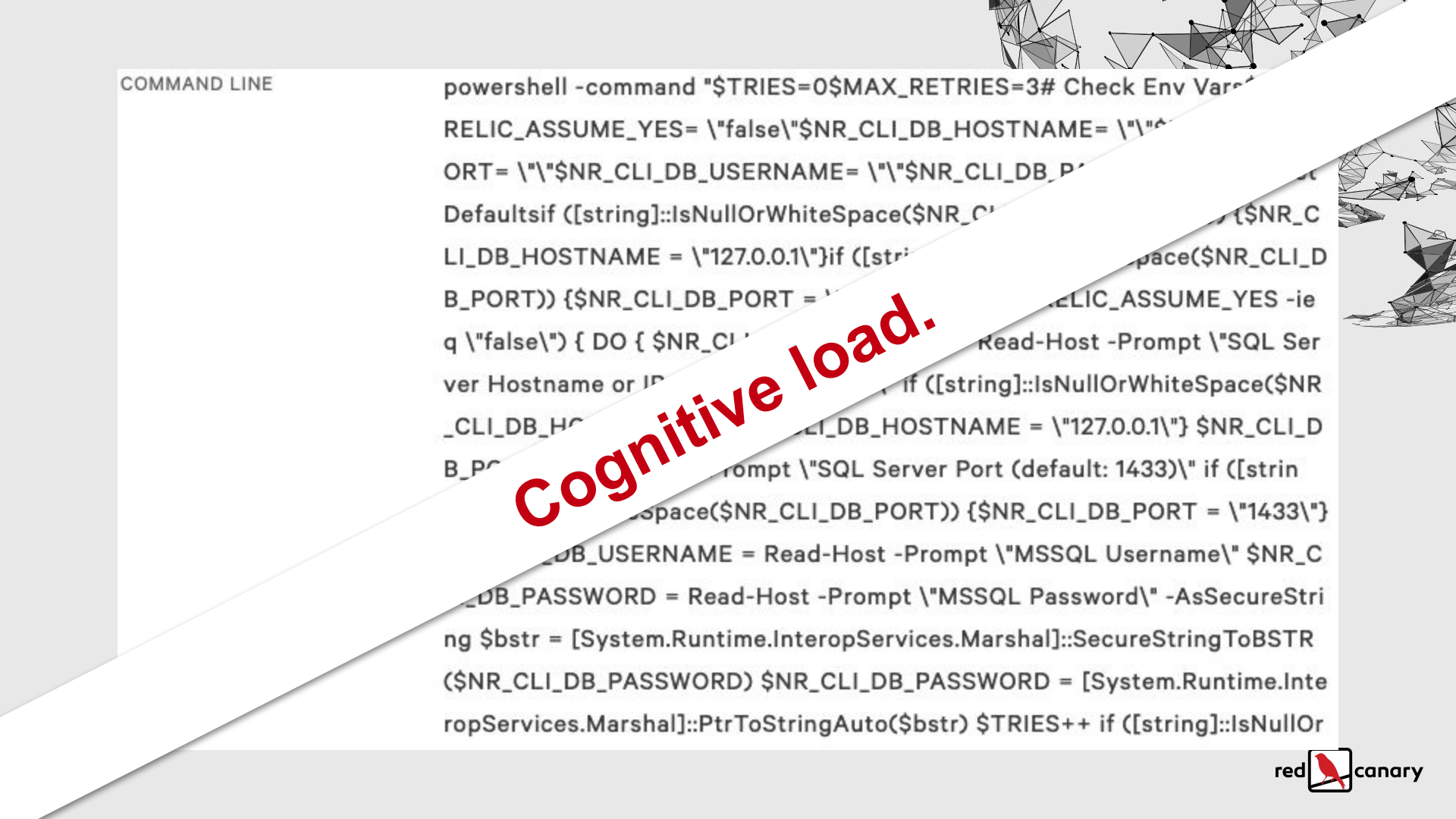
red canary

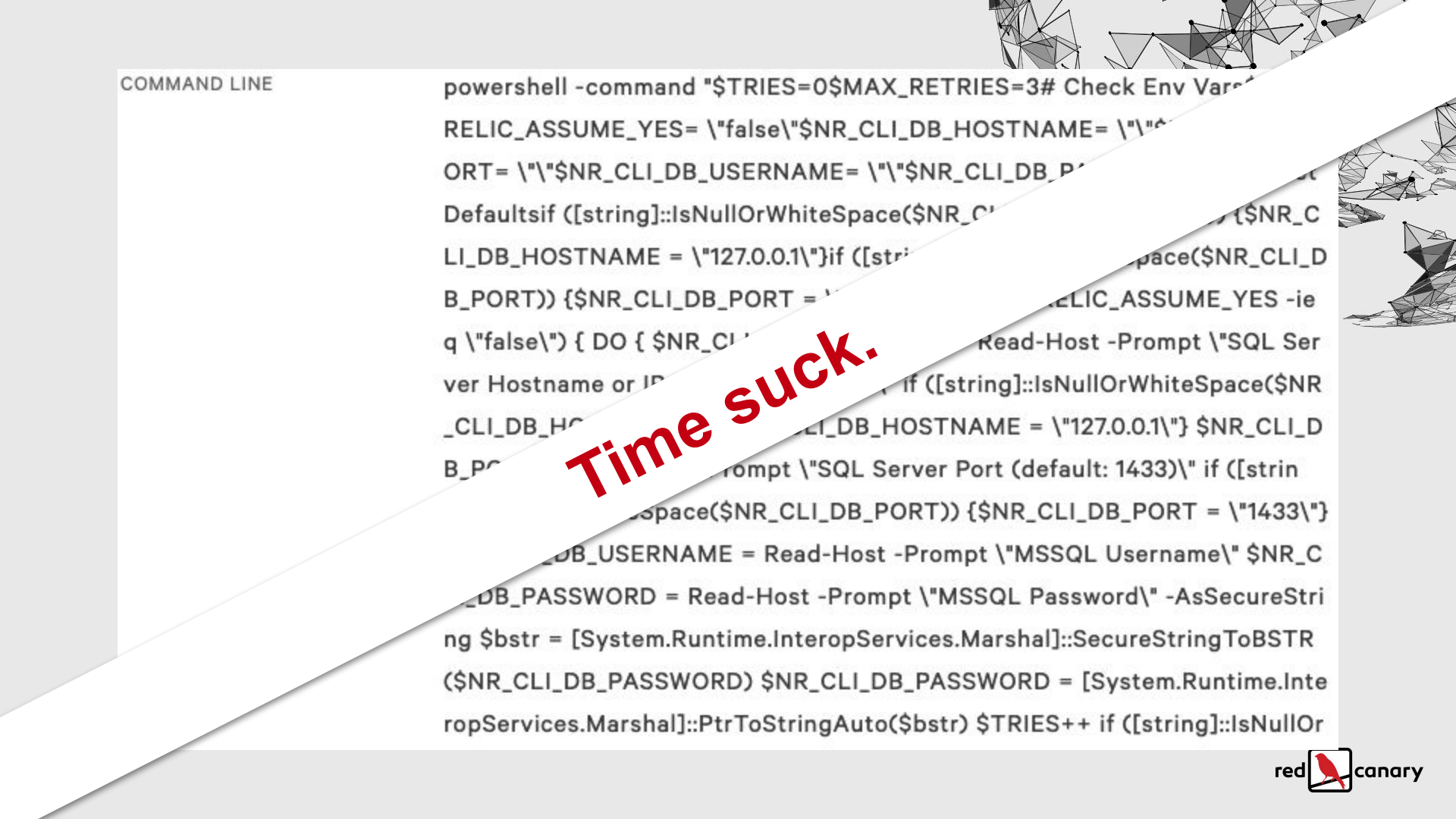
COMMAND LINE

```
powershell -command "$TRIES=0$MAX_RETRIES=3# Check Env Var
RELIC_ASSUME_YES= \"false\"$NR_CLI_DB_HOSTNAME= \"\"
ORT= \"\"$NR_CLI_DB_USERNAME= \"\"$NR_CLI_DB_P
Defaultsif ([string]::IsNullOrWhiteSpace($NR_C
LI_DB_HOSTNAME = \"127.0.0.1\"}if ([str
B_PORT)) {$NR_CLI_DB_PORT =
q \"false\") { DO { $NR_CL
ver Hostname or IP
_CLI_DB_HO
B_PO
Space($NR_CLI_DB_PORT)) {$NR_CLI_DB_PORT = \"1433\"}
DB_USERNAME = Read-Host -Prompt \"MSSQL Username\" $NR_C
DB_PASSWORD = Read-Host -Prompt \"MSSQL Password\" -AsSecureStri
ng $bstr = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR
($NR_CLI_DB_PASSWORD) $NR_CLI_DB_PASSWORD = [System.Runtime.Inte
ropServices.Marshal]::PtrToStringAuto($bstr) $TRIES++ if ([string]::IsNullOr
```

Benign.

red canary


COMMAND LINE
powershell -command "$TRIES=0$MAX_RETRIES=3# Check Env Var
RELIC_ASSUME_YES= \"false\"$NR_CLI_DB_HOSTNAME= \"\"
ORT= \"\"$NR_CLI_DB_USERNAME= \"\"$NR_CLI_DB_P
Defaultsif ([string]::IsNullOrWhiteSpace($NR_C
LI_DB_HOSTNAME = \"127.0.0.1\"}if ([str
B_PORT)) {$NR_CLI_DB_PORT =
q \"false\") { DO { $NR_C
ver Hostname or I
_CLI_DB_H
B_P
Space($NR_CLI_DB_PORT)) {$NR_CLI_DB_PORT = \"1433\"}
_DB_USERNAME = Read-Host -Prompt \"MSSQL Username\" $NR_C
_DB_PASSWORD = Read-Host -Prompt \"MSSQL Password\" -AsSecureStri
ng $bstr = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR
($NR_CLI_DB_PASSWORD) $NR_CLI_DB_PASSWORD = [System.Runtime.Inte
ropServices.Marshal]::PtrToStringAuto($bstr) $TRIES++ if ([string]::IsNullOr
Cognitive load.
red canary


COMMAND LINE
powershell -command "$TRIES=0$MAX_RETRIES=3# Check Env Var
RELIC_ASSUME_YES= \"false\"$NR_CLI_DB_HOSTNAME= \"\"
ORT= \"\"$NR_CLI_DB_USERNAME= \"\"$NR_CLI_DB_P
Defaultsif ([string]::IsNullOrWhiteSpace($NR_C
LI_DB_HOSTNAME = \"127.0.0.1\"}if ([str
B_PORT)) {$NR_CLI_DB_PORT =
q \"false\") { DO { $NR_CL
ver Hostname or IP
_CLI_DB_HO
B_PO
Space($NR_CLI_DB_PORT)) {$NR_CLI_DB_PORT = \"1433\"}
_DB_USERNAME = Read-Host -Prompt \"MSSQL Username\" $NR_C
_DB_PASSWORD = Read-Host -Prompt \"MSSQL Password\" -AsSecureStri
ng $bstr = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR
($NR_CLI_DB_PASSWORD) $NR_CLI_DB_PASSWORD = [System.Runtime.Inte
ropServices.Marshal]::PtrToStringAuto($bstr) $TRIES++ if ([string]::IsNullOr
Time suck.
red canary

When it’s 12:30 AM UTC what time is it?

Catch me (online), if you can

Can I use your PID?

red canary

Process C:\Windows\System32\svchost.exe

Command Line

```
C:\WINDOWS\system32\svchost.exe -k netsvcs -p
```

0 netconns | 0 childprocs | 3 filemods | 0 regmods | 3 modloads | 0 crossprocs | 0 scriptloads

Parent Process

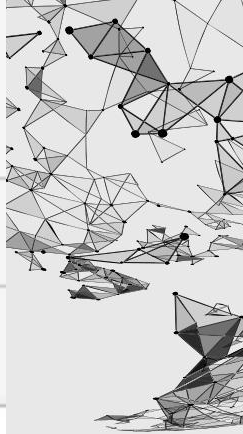
Command Line

0 netconns | 1

0 scriptloads

File Names

System.Management.Automation.ni.dll
bcrypt.dll
psapi.dll



red canary

Process C:\Windows\System32\svchost.exe

Command Line

Unmanaged code.

```
C:\WINDOWS\system32\svchost.exe -k netsvcs -p
```

0 netconns | 0 childprocs | 3 filemods | 0 regmods | 3 modloads | 0 crossprocs | 0 scriptloads

Parent Process

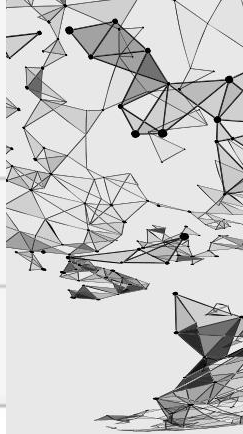
Command Line

0 netconns | 1

0 scriptloads

File Names

System.Management.Automation.ni.dll
bcrypt.dll
psapi.dll



Process C:\Windows\System32\svchost.exe

Command Line

Unmanaged code.

Note the command-line arguments.

```
C:\WINDOWS\system32\svchost.exe -k netsvcs -p
```

0 netconns | 0 childprocs | 3 filemods | 0 regmods | 3 modloads | 0 crossprocs | 0 scriptloads

Parent Process

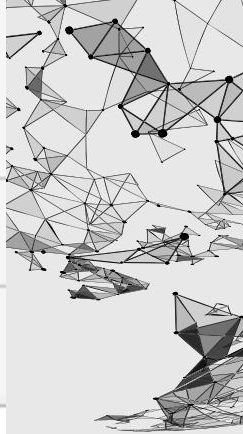
Command Line

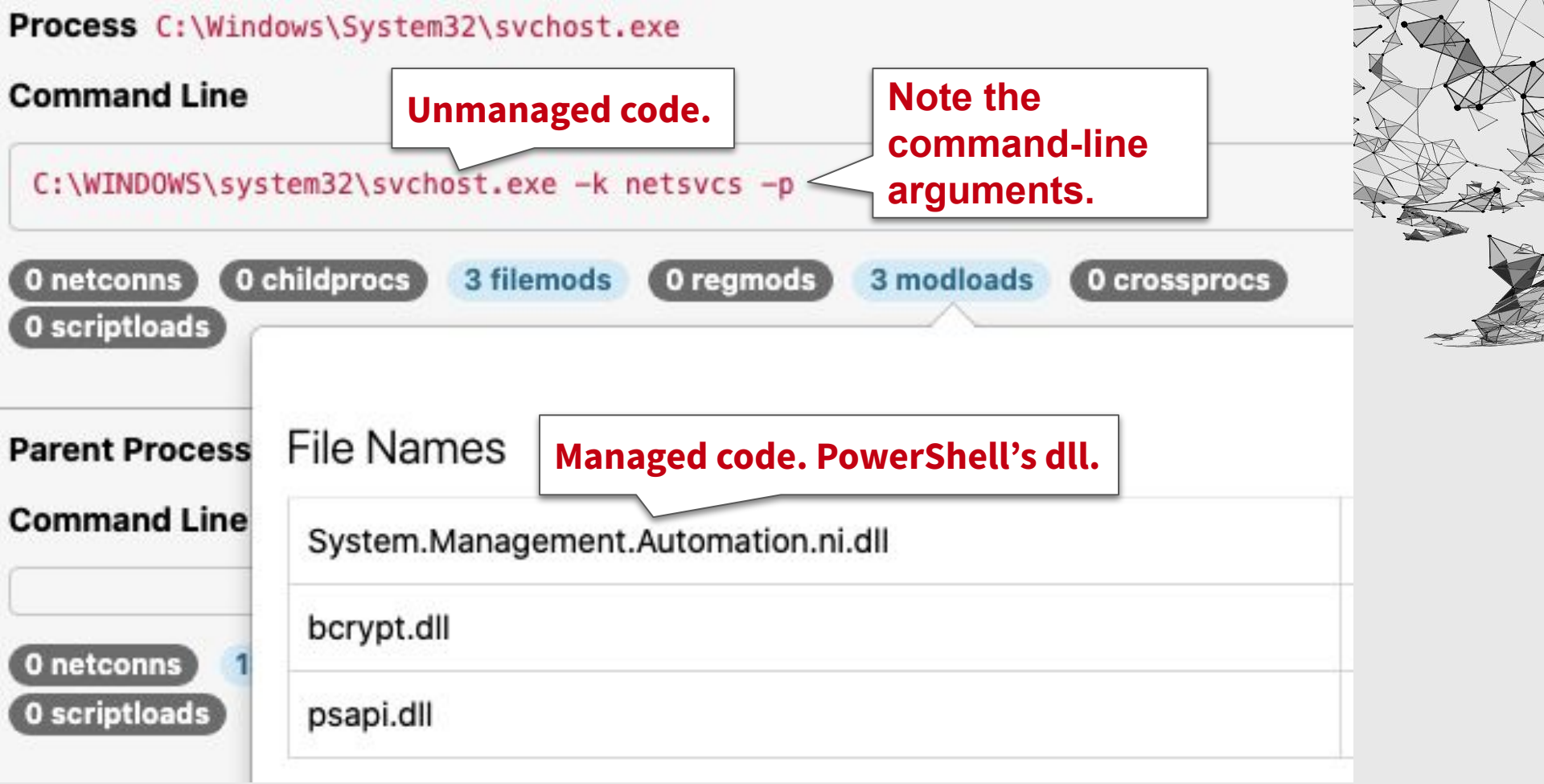
0 netconns | 1

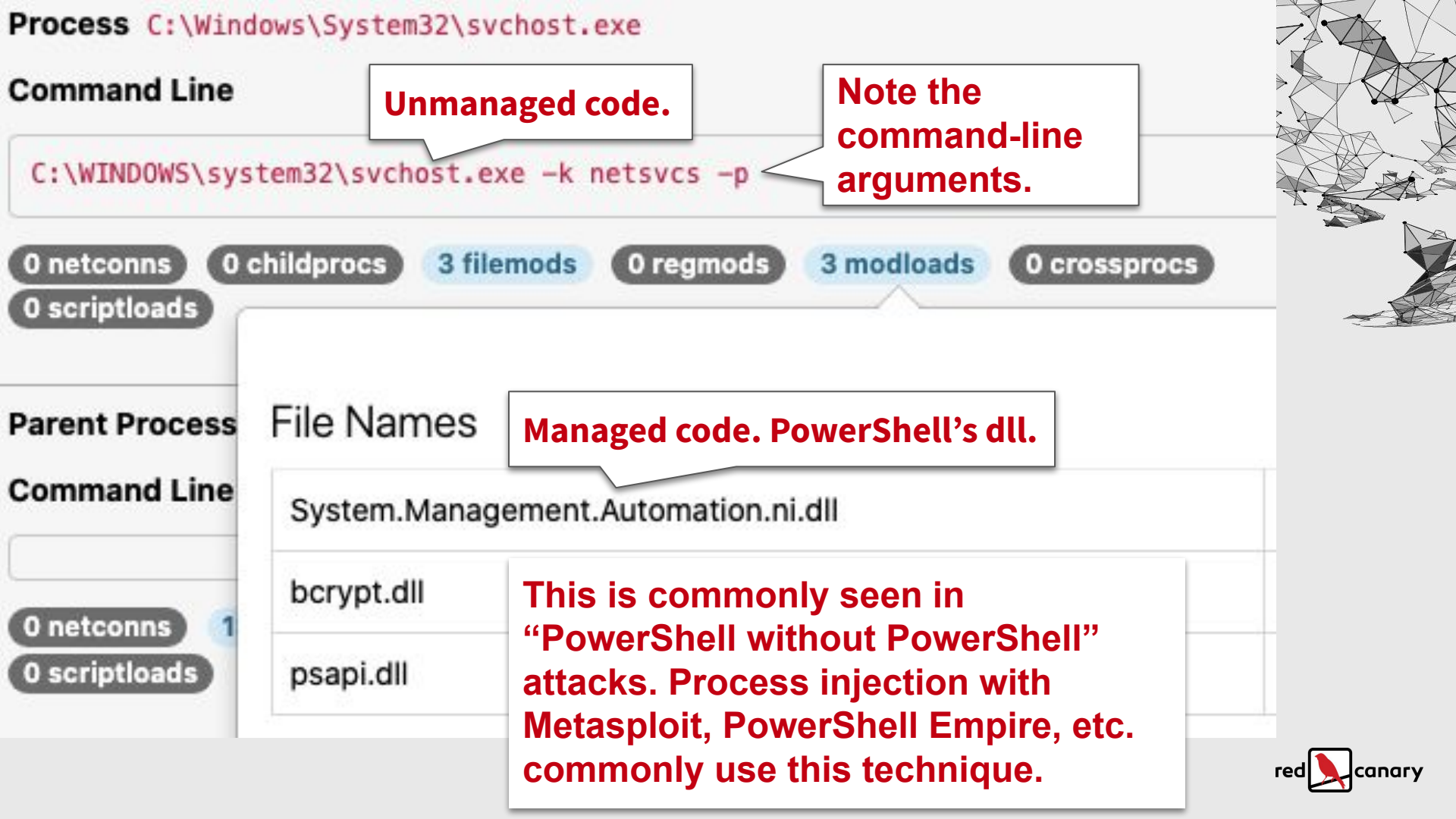
0 scriptloads

File Names

System.Management.Automation.ni.dll
bcrypt.dll
psapi.dll




Process C:\Windows\System32\svchost.exe
Command Line
Unmanaged code.
Note the command-line arguments.
C:\WINDOWS\system32\svchost.exe -k netsvcs -p
0 netconns
0 childprocs
3 filemods
0 regmods
3 modloads
0 crossprocs
0 scriptloads
Parent Process
Command Line
File Names
Managed code. PowerShell's dll.
System.Management.Automation.ni.dll
bcrypt.dll
psapi.dll
0 netconns
0 scriptloads


Process C:\Windows\System32\svchost.exe
Command Line
Unmanaged code.
Note the command-line arguments.
C:\WINDOWS\system32\svchost.exe -k netsvcs -p
0 netconns
0 childprocs
3 filemods
0 regmods
3 modloads
0 crossprocs
0 scriptloads
Parent Process
Command Line
File Names
Managed code. PowerShell's dll.
System.Management.Automation.ni.dll
bcrypt.dll
psapi.dll
0 netconns
0 scriptloads
This is commonly seen in "PowerShell without PowerShell" attacks. Process injection with Metasploit, PowerShell Empire, etc. commonly use this technique.

Query Details

Search files and processes for file svchost.exe on hostname [REDACTED]

EDR platform search.

Investigation Details

500 Total Hits

1/1 Endpoints with Hits

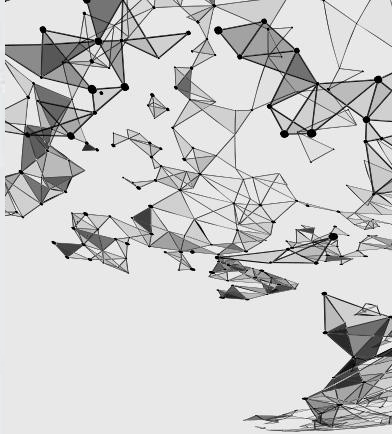
First Seen

Last Seen

⚠ Max 500 results returned per endpoint. For more results, try using the API directly.

Max results exceeded. Use the API. 😞

red canary



[REDACTED]

show me pid on hostname [REDACTED]

Redacted PID.

Are you sure you want to run:

Search process for pid [REDACTED]? on hostname

Redacted PID.

[REDACTED]

yes

No sensors match your query.

Endpoint offline.

red canary

[REDACTED]

show me data for file system.management.automation.ni.dll on hostname [REDACTED]

Are you sure you want to run:

Search files and processes for file system.management.automation.ni.dll on hostname [REDACTED]?

[REDACTED]

yes

No sensors match your query.

Endpoint offline.

[REDACTED]

show me file data for system.management.automation.ni.dll on hostname [REDACTED]

Are you sure you want to run:

Search files and processes for file system.management.automation.ni.dll on hostname [REDACTED]?

[REDACTED]

yes

Created investigation: [REDACTED]

View the Investigation

Success!

Investigation Details	0 Total Hits	0/1 Endpoints with Hits

No hits?

red canary

Success. Scoped the PID query to date and time of interest.

[REDACTED]	PM UTC	Process	Process Created

Process Name	svchost.exe	**Domain**	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe	**MD5**	f586835082f632dc8d94
User	SYSTEM	**Parent Process ID**	[REDACTED]
Process ID	[REDACTED]	**Command Line**	C:\WINDOWS\system32\svchost.exe -k netsvcs -p

Note the command-line arguments.

[REDACTED]	PM UTC	Process	Process Terminated

Process Name	svchost.exe	**Domain**	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe	**MD5**	f586835082f632dc8d9404d83bc16316
User	SYSTEM	**Parent Process ID**	[REDACTED]
Process ID	[REDACTED]	**Command Line**	C:\WINDOWS\system32\svchost.exe -k netsvcs -p

red canary

is utc 24 hour time

All Images News Shopping Maps More Tools

About 63,400,000 results (0.60 seconds)

UTC uses 24-hour (military) time notation and is based on the local standard time on the 0° longitude meridian which runs through Greenwich, England. Midnight in Greenwich corresponds to 00:00 UTC, noon corresponds to 12:00 UTC, and so on. Jan 7, 2018

UTC: Coordinated Universal Time

CDT: Central Daylight Time

PDT: Pacific Daylight Time

EDT: Eastern Daylight Time

https://www.spacearchive.info › utc

Coordinated Universal Time (UTC) - Space Archive

About featured snippets

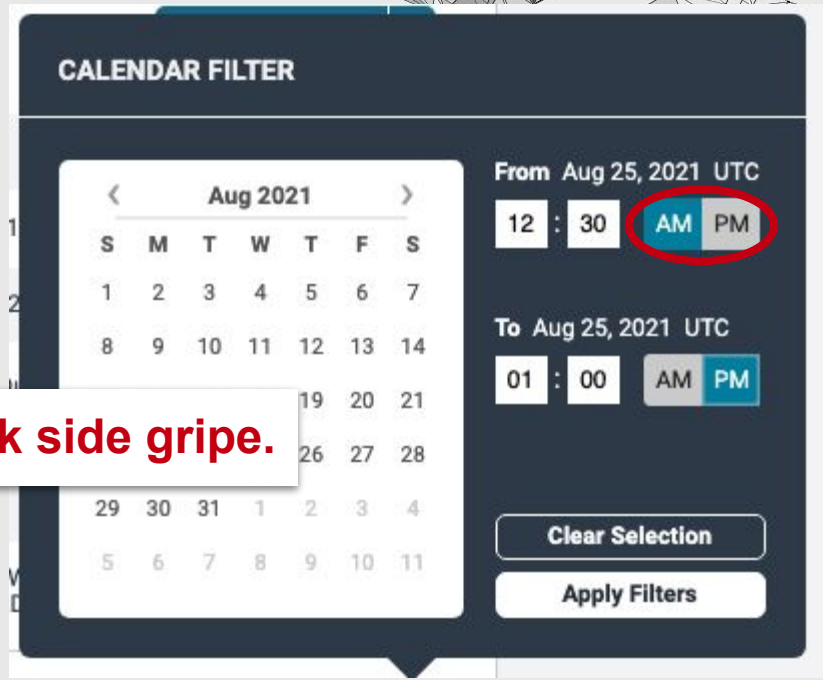
People also ask

What is UTC time now in 24-hour format?

Is UTC time AM or PM?

UTC time is the local time at Greenwich England. Time in other locations will be the UTC time hour plus or minus the local Time Zone. Daylight savings time adds 1 hour to the local standard (real) time. Twenty four hour **time does not use "am" or "pm"**, but courts hours from midnight (0 hours) to 11 pm (23 hours).

Quick side gripe.



red canary

Success. Scoped the PID query to date and time of interest.

[REDACTED]	PM UTC	Process	Process Created

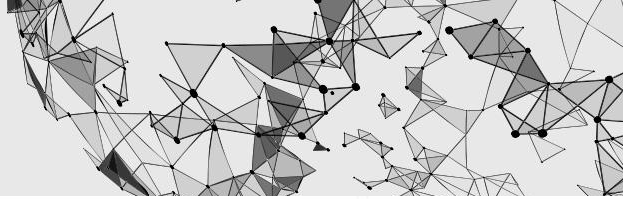
Process Name	svchost.exe	**Domain**	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe	**MD5**	f586835082f632dc8d9404d83bc16316
User	SYSTEM	**Parent Process ID**	[REDACTED]
Process ID	[REDACTED]	**Command Line**	C:\WINDOWS\system32\svchost.exe -k netsvcs -p

[REDACTED]	PM UTC	Process	Process Terminated

Process Name	svchost.exe	**Domain**	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe	**MD5**	f586835082f632dc8d9404d83bc16316
User	SYSTEM	**Parent Process ID**	[REDACTED]
Process ID	[REDACTED]	**Command Line**	C:\WINDOWS\system32\svchost.exe -k netsvcs -p

But this data provides little new information.

red canary



Start time.

[REDACTED]	PM UTC	Process	Process Created

Process Name	svchost.exe	**Domain**	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe	**MD5**	f586835082f632dc8d9404d83bc16316
User	SYSTEM	**Parent Process ID**	[REDACTED]
Process ID		**Command Line**	C:\WINDOWS\system32\svchost.exe -k netsvcs -p

Termination time.

[REDACTED]	PM UTC	Process	Process Terminated

Process Name	svchost.exe	**Domain**	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe	**MD5**	f586835082f632dc8d9404d83bc16316
User	SYSTEM	**Parent Process ID**	[REDACTED]
Process ID	[REDACTED]	**Command Line**	C:\WINDOWS\system32\svchost.exe -k netsvcs -p

But this data provides little new information. Module loads? Network connections? File, Registry changes?

red canary

2 seconds after svchost.exe terminated.

[REDACTED] **PM UTC**

Process Name	powershell.exe
Path	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User	SYSTEM
Process ID	[REDACTED][REUSED PID]
Domain	NT AUTHORITY
MD5	04029e121a0cfa5991749937dd22a1d9

2 seconds after svchost.exe terminated.

[REDACTED] **PM UTC**

New process.

Process Name	powershell.exe
Path	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User	SYSTEM
Process ID	[REDACTED][REUSED PID]
Domain	NT AUTHORITY
MD5	04029e121a0cfa5991749937dd22a1d9

2 seconds after svchost.exe terminated.

[REDACTED] **PM UTC**

New process.

Process Name powershell.exe

Path
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

User SYSTEM

Same PID as terminated svchost.exe

Process ID [REDACTED][REUSED PID]

Domain NT AUTHORITY

MD5 04029e121a0cfa5991749937dd22a1d9

red canary

2 seconds after svchost.exe terminated.

[REDACTED] **PM UTC**

New process.

Process Name powershell.exe

Path
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

User SYSTEM

Same PID as terminated svchost.exe

Process ID [REDACTED][REUSED PID]

Domain NT AUTHORITY

MD5 04029e121a0cfa5991749937dd22a1d9

Take note of the MD5 hash.

red canary

[REDACTED] **PM UTC**

Process Name powershell.exe

Path
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

User SYSTEM

Process ID [REDACTED][REUSED PID]

This is the termination event for our PowerShell process cropped for visibility purposes.

	Process	Process Terminated

Domain NT AUTHORITY

MD5 f586835082f632dc8d9404d83bc16316

Parent Process ID [REDACTED]

Command Line C:\WINDOWS\system32\svchost.exe -k netsvcs -p

red canary

[REDACTED] **PM UTC**

Process Name powershell.exe

Path
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

User SYSTEM

Process ID [REDACTED][REUSED PID]

Process

Domain NT AUTHORITY

MD5 f586835082f632dc8d9404d83bc16316

Parent Process ID [REDACTED]

Command Line C:\WINDOWS\system32\svchost.exe -k netsvcs -p

Wrong hash, process and command-line arguments.

red canary

Getting bogged down

Plenty of data, not enough information

Does this forest have any trees?

red canary

Process spawned

`c:\windows\explorer.exe` `62022614d1d9290cd1069234f2a55cf8ef8f1572b02157ee8d4d16903c963de0d026fc1a1c565bfa6448ddc9cb0a8da1`

Process spawned by explorer.exe

`c:\windows\system32\conhost.exe` `81ca40085fc75babd2c91d18aa9ffa686651ab6c5c6d85c86b0c6c532115662e09f338fa8cc1233e1434139346f25ef6`

Process spawned by conhost.exe

`c:\windows\system32\cmd.exe` `8a2122e8162dbef04694b9c3e0b6cdeeb99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450`

Quick quiz

svchost.exe spawned explorer.exe

- Common or uncommon?

Quick quiz

svchost.exe spawned explorer.exe

- Common or uncommon?
- Uncommon.

red canary

Quick quiz

svchost.exe spawned explorer.exe

- Common or uncommon?
- Uncommon.

explorer.exe spawned conhost.exe

- Common or uncommon?

Quick quiz

svchost.exe spawned explorer.exe

- Common or uncommon?
- Uncommon.

explorer.exe spawned conhost.exe

- Common or uncommon?
- Uncommon.

Quick quiz

svchost.exe spawned explorer.exe

- Common or uncommon?
- Uncommon.

explorer.exe spawned conhost.exe

- Common or uncommon?
- Uncommon.

conhost.exe spawned cmd.exe

- Common or uncommon?

Quick quiz

svchost.exe spawned explorer.exe

- Common or uncommon?
- Uncommon.

explorer.exe spawned conhost.exe

- Common or uncommon?
- Uncommon.

conhost.exe spawned cmd.exe

- Common or uncommon?
- Uncommon.

Quick quiz

svchost.exe spawned explorer.exe

- Common or uncommon?
- Uncommon.

explorer.exe spawned cor

- Common or
- Uncom

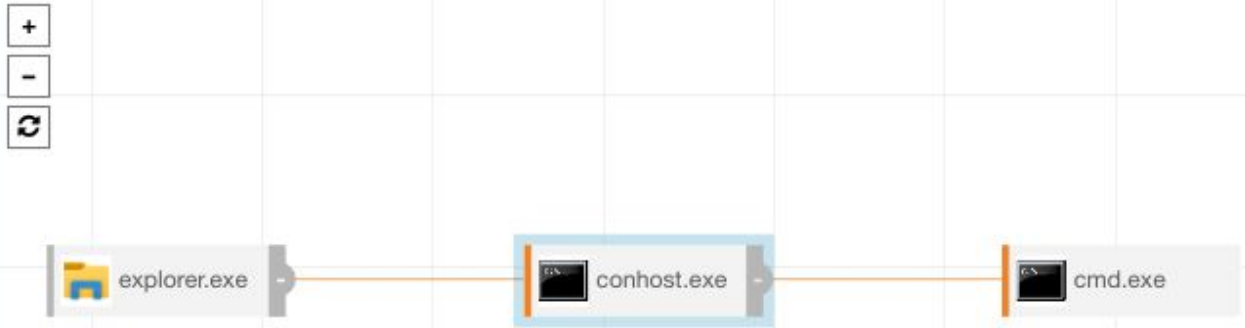
co wned cmd.exe

- mmon or uncommon?
- Uncommon.

But is it malicious?!

red canary

Process	Command Line - Copy	Host	User	Logon Type	State	Started	Duration
conhost.exe	"C:\Windows\System32\conhost.exe"	[REDACTED]	[REDACTED]	Interactive	Terminated	a day ago	a few seconds



Process: conhost.exe

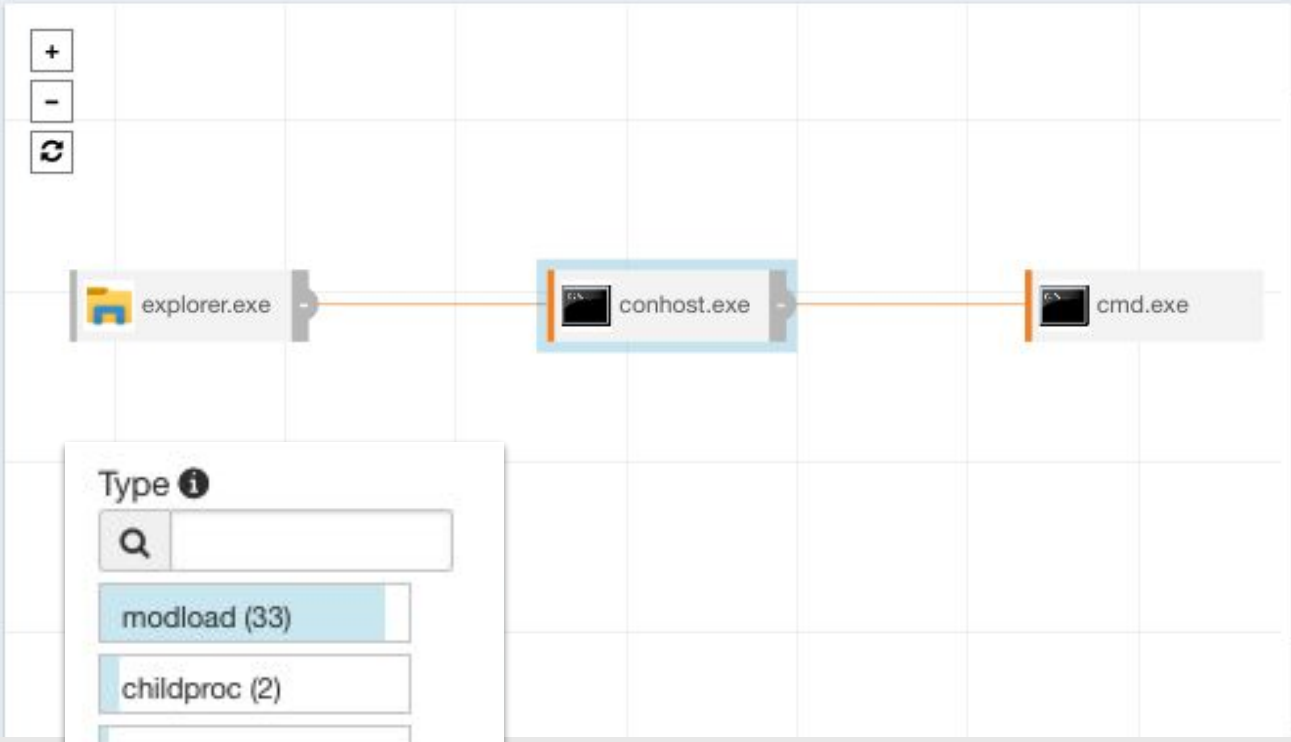
PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\conhost.exe
Username	[REDACTED]
MD5	81ca40085fc75babd2c91d18aa9ffa68
SHA-256	6651ab6c5c6d85c86b0c6c532115662e c1233e1434139346f25ef6
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

It's signed.

conhost.exe: Signed by Microsoft Corporation

red canary

Process	Command Line - Copy	Host	User	Logon Type	State	Started	Duration
conhost.exe	"C:\Windows\System32\conhost.exe"	[REDACTED]	[REDACTED]	Interactive	Terminated	a day ago	a few seconds



Process: conhost.exe

PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\conhost.exe
Username	[REDACTED]
MD5	81ca40085fc75babd2c91d18aa9ffa68
SHA-256	6651ab6c5c6d85c86b0c6c532115662e c1233e1434139346f25ef6
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

conhost.exe: Signed by Microsoft Corporation

red canary

Process	Command Line - Copy	Host	User	Logon Type	State	Started	Duration
conhost.exe	"C:\Windows\System32\conhost.exe"	[REDACTED]	[REDACTED]	Interactive	Terminated	a day ago	a few seconds

Type

modload (33)

childproc (2)

crossproc (1)

Is 33 modloads high/low for conhost.exe?

Does conhost.exe usually have chidproc and crossproc events?

Process: conhost.exe

PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\conhost.exe
Username	[REDACTED]
MD5	81ca40085fc75babd2c91d18aa9ffa68
SHA-256	6651ab6c5c6d85c86b0c6c532115662e c1233e1434139346f25ef6
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

conhost.exe: Signed by Microsoft Corporation

red canary

Description	Search
Loaded c:\windows\system32\conhost.exe **Signed** (81ca40085fc75babd2c91d18aa9ffa68)	
Loaded c:\windows\system32\ntdll.dll **Signed** (e733ce7879b76e4dfa9f78d78dc30a42)	
Loaded c:\windows\system32\kernel32.dll **Signed** (e26c1012bfe52a8e0351ed3fe7627656)	
Loaded c:\windows\system32\kernelbase.dll **Signed** (d6955652ff360c211601c669660ea05e)	
Loaded c:\windows\system32\msvcp_win.dll **Signed** (34692d0bde33641b576c32165fbaaf6d)	
Loaded c:\windows\system32\ucrtbase.dll **Signed** (2c8fe06966d5085a595ffa3c98fe3098)	
Loaded c:\windows\system32\shcore.dll **Signed** (2980aaabc9e5f254ff45d5bae51869e9)	
Loaded c:\windows\system32\msvcrt.dll **Signed** (a4f2d5942fb447cd48a5cee414983e85)	
Loaded c:\windows\system32\combase.dll **Signed** (c07af7fb8785114a9c756e6b7d219094)	
Loaded c:\windows\system32\rpcrt4.dll **Signed** (3e11203fcd5d9055c3418082cbd9edf4)	
Loaded c:\windows\system32\advapi32.dll **Signed** (e70a1568a400e71a8e644652fca4c925)	
Loaded c:\windows\system32\sechost.dll **Signed** (e127fce942c28931ded1442a1f2e84bb)	

red canary

Description	Search

Loaded c:\windows\system32\conhost.exe **Signed** (81ca40085fc75babd2c91d18aa9ffa68)

Loaded c:\windows\system32\ntdll.dll **Signed** (e733ce7879b76e4dfa9f78d78dc30a42)

Loaded c:\windows\system32\kernel32.dll **Signed** (e26c1012bfe52a8e0351ed3fe7627656)

Loaded c:\windows\system32\kernelbase.dll **Signed** (d6955652ff360c211601c669660ea05e)

Loaded c:\windows\system32\msvcp_win.dll **Signed** (34692d0bde33641b576c32165fbaaf6d

Loaded c:\windows\system32\ucrtbase.dll **Signed** (2c8fe06966d5085a595ffa3c98fe3098)

Loaded c:\windows\system32\shcore.dll **Signed** (2980aaabc9e5f254ff45d5bae51869e9)

Loaded c:\windows\system32\msvcrt.dll **Signed** (a4f2d5942fb447cd48a5cee414983e85)

Loaded c:\windows\system32\combase.dll **Signed** (c07af7fb8785114a9c756e6b7d219094)

Loaded c:\windows\system32\rpcrt4.dll **Signed** (3e11203fcd5d9055c3418082cbd9edf4)

Loaded c:\windows\system32\advapi32.dll **Signed** (e70a1568a400e71a8e644652fca4c925)

Loaded c:\windows\system32\sechost.dll **Signed** (e127fce942c28931ded1442a1f2e84bb)

Is this normal?

Are all of these modloads common for conhost.exe?

red canary

Description	Search
Loaded c:\windows\system32\conhost.exe **Signed** (81ca40085fc75babd2c91d18aa9ffa68)	
Loaded c:\windows\system32\ntdll.dll **Signed** (e733ce7879b76e4dfa9f78d78dc30a42)	
Loaded c:\windows\system32\kernel32.dll **Signed** (e26c1012bfe52a8e0351ed3fe7627656)	
Loaded c:\windows\system32\kernelbase.dll **Signed** (d6955652ff360c211601c669660ea05e)	
Loaded c:\windows\system32\msvcp_win.dll **Signed** (34692d0bde33641b576c32165fbaaf6d	
Loaded c:\windows\system32\ucrtbase.dll **Signed** (2c8fe06966d5085a595ffa3c98fe3098)	
Loaded c:\windows\system32\shcore.dll **Signed** (2980aaabc9e5f254ff45d5bae51869e9)	
Loaded c:\windows\system32\msvcrt.dll **Signed** (a4f2d5942fb447cd48a5cee414983e85)	
Loaded c:\windows\system32\combase.dll **Signed** (c07af7fb8785114a9c756e6b7d219094)	
Loaded c:\windows\system32\rpcrt4.dll **Signed** (3e11203fcd5d9055c3418082cbd9edf4)	
Loaded c:\windows\system32\advapi32.dll **Signed** (e70a1568a400e71a8e644652fca4c925)	
Loaded c:\windows\system32\sechost.dll **Signed** (e127fce942c28931ded1442a1f2e84bb)	

Is this normal?

Are all of these modloads common for conhost.exe?

What about lolbin attacks?

red canary

Description	Search
Loaded c:\windows\system32\conhost.exe **Signed** (81ca40085fc75babd2c91d18aa9ffa68)	
Loaded c:\windows\system32\ntdll.dll **Signed** (e733ce7879b76e4dfa9f78d78dc30a42)	
Loaded c:\windows\system32\kernel32.dll **Signed** (e26c1012bfe52a8e0351ed3fe7627656)	
Loaded c:\windows\system32\kernelbase.dll **Signed** (d6955652ff360c211601c669660ea05e)	
Loaded c:\windows\system32\msvcp_win.dll **Signed** (34692d0bde33641b576c32165fbaaf6d	
Loaded c:\windows\system32\ucrtbase.dll **Signed** (2c8fe06966d5085a595ffa3c98fe3098)	
Loaded c:\windows\system32\shcore.dll **Signed** (2980aaabc9e5f254ff45d5bae51869e9)	
Loaded c:\windows\system32\msvcrt.dll **Signed** (a4f2d5942fb447cd48a5cee414983e85)	
Loaded c:\windows\system32\combase.dll **Signed** (c07af7fb8785114a9c756e6b7d219094)	
Loaded c:\windows\system32\rpcrt4.dll **Signed** (3e11203fcd5d9055c3418082cbd9edf4)	
Loaded c:\windows\system32\advapi32.dll **Signed** (e70a1568a400e71a8e644652fca4c925)	
Loaded c:\windows\system32\sechost.dll **Signed** (e127fce942c28931ded1442a1f2e84bb)	

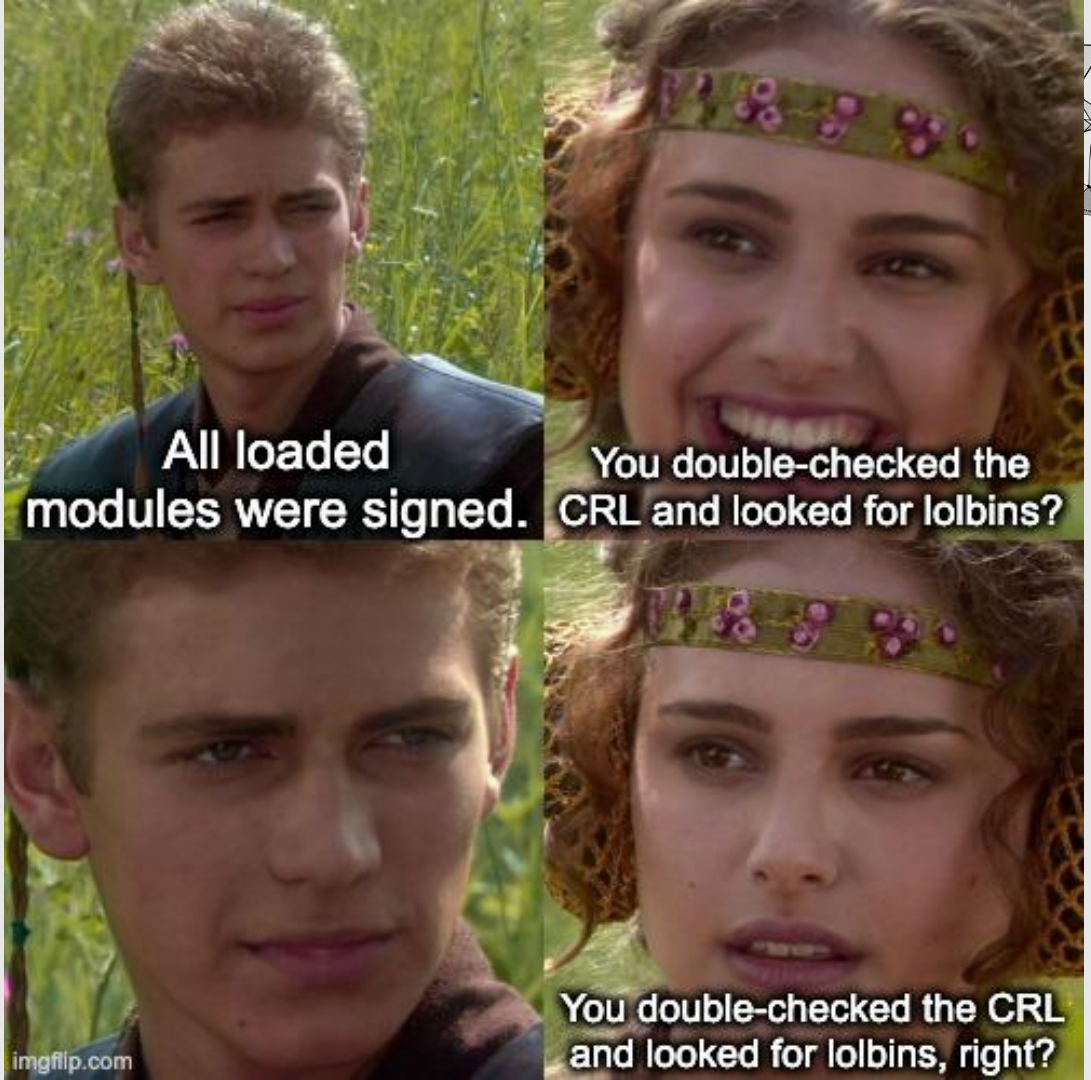
Is this normal?

Are all of these modloads common for conhost.exe?

What about lolbin attacks?

What about stolen code signing certs?

red canary


All loaded modules were signed.
You double-checked the CRL and looked for lolbins?
You double-checked the CRL and looked for lolbins, right?
imgflip.com

red canary

Description	Search
Loaded c:\windows\system32\conhost.exe **Signed** (81ca40085fc75babd2c91d18aa9ffa68)	
Loaded c:\windows\system32\ntdll.dll **Signed** (e733ce7879b76e4dfa9f78d78dc30a42)	
Loaded c:\windows\system32\kernel32.dll **Signed** (e26c1012bfe52a8e0351ed3fe7627656)	
Loaded c:\windows\system32\kernelbase.dll **Signed** (d6955652ff360c211601c669660ea05e)	
Loaded c:\windows\system32\msvcp_win.dll **Signed** (34692d0bde33641b576c32165fbaaf6d	
Loaded c:\windows\system32\ucrtbase.dll **Signed** (2c8fe06966d5085a595ffa3c98fe3098)	
Loaded c:\windows\system32\shcore.dll **Signed** (2980aaabc9e5f254ff45d5bae51869e9)	
Loaded c:\windows\system32\msvcrt.dll **Signed** (a4f2d5942fb447cd48a5cee414983e85)	
Loaded c:\windows\system32\combase.dll **Signed** (c07af7fb8785114a9c756e6b7d219094)	
Loaded c:\windows\system32\rpcrt4.dll **Signed** (3e11203fcd5d9055c3418082cbd9edf4)	
Loaded c:\windows\system32\advapi32.dll **Signed** (e70a1568a400e71a8e644652fca4c925)	
Loaded c:\windows\system32\sechost.dll **Signed** (e127fce942c28931ded1442a1f2e84bb)	

Remember we're under time pressure.

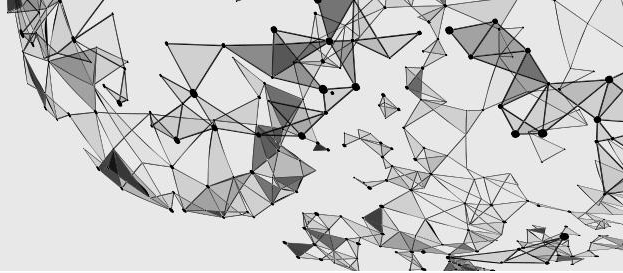
How could we determine if these module load events warrant investigating?

red canary

Description	Search
Loaded c:\windows\system32\conhost.exe **Signed** (81ca40085fc75babd2c91d18aa9ffa68)	
Loaded c:\windows\system32\ntdll.dll **Signed** (e733ce7879b76e4dfa9f78d78dc30a42)	
Loaded c:\windows\system32\kernel32.dll **Signed** (e26c1012bfe52a8e0351ed3fe7627656)	
Loaded c:\windows\system32\kernelbase.dll **Signed** (d6955652ff360c211601c669660ea05e)	
Loaded c:\windows\system32\msvcp_win.dll **Signed** (34692d0bde33641b576c32165fbaaf6d	
Loaded c:\windows\system32\ucrtbase.dll **Signed** (2c8fe06966d5085a595ffa3c98fe3098)	
Loaded c:\windows\system32\shcore.dll **Signed** (2980aaabc9e5f254ff45d5bae51869e9)	
Loaded c:\windows\system32\msvcrt.dll **Signed** (a4f2d5942fb447cd48a5cee414983e85)	
Loaded c:\windows\system32\combase.dll **Signed** (c07af7fb8785114a9c756e6b7d219094)	
Loaded c:\windows\system32\rpcrt4.dll **Signed** (3e11203fcd5d9055c3418082cbd9edf4)	
Loaded c:\windows\system32\advapi32.dll **Signed** (e70a1568a400e71a8e644652fca4c925)	
Loaded c:\windows\system32\sechost.dll **Signed** (e127fce942c28931ded1442a1f2e84bb)	

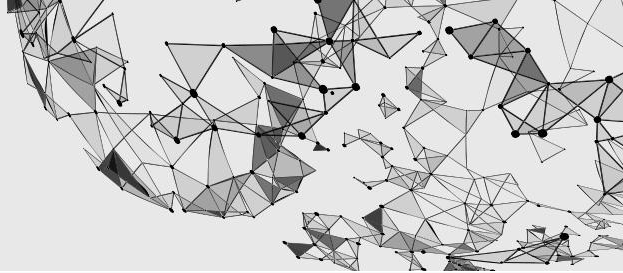
For now, let's assume they are ok and move along.

red canary



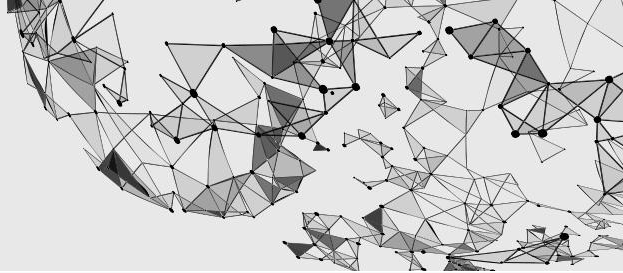
Type	Description		Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)		
childproc	PID ### ended c:\windows\system32\cmd.exe **Signed** (8a2122e8162dbef04694b9c3e0b6cdee)		

red canary



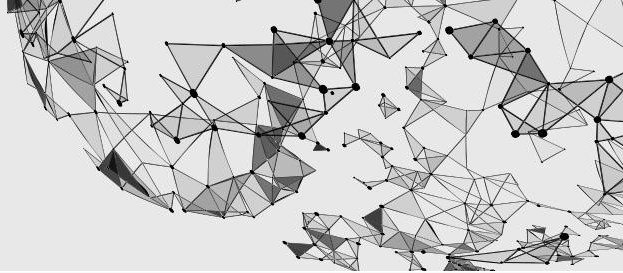
Type	Description		Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)		
childproc	PID ### ended c:\windows\system32\cmd.exe	← terminates after three seconds	

red canary



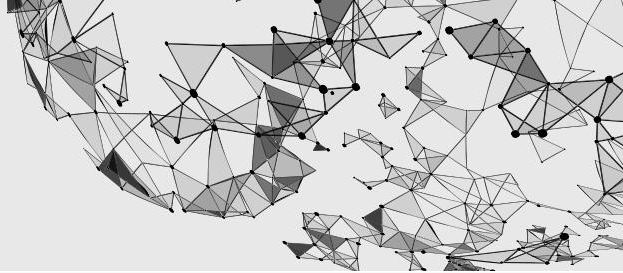
Type	Description		Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)		
childproc	PID ### ended c:\windows\system32\cmd.exe	← terminates after three seconds no command-line arguments	

red canary



Type	Description		Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)		
childproc	PID ### ended c:\windows\system32\cmd.exe	← terminates after three seconds no command-line arguments no child procs	

red canary

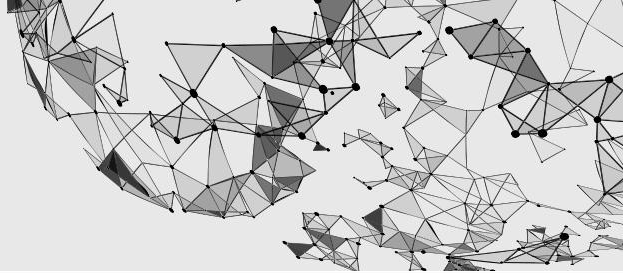


Type	Description	Search
childproc	PID ### started c:\windows\system32\cmd.exe	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)	
childproc	PID ### ended c:\windows\system32\cmd.exe	

← 14ms after conhost

← terminates after three seconds
no command-line arguments
no child procs
no file or registry writes

red canary

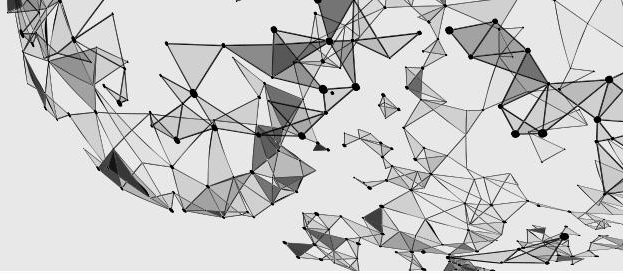


Type	Description	Search
childproc	PID ### started c:\windows\system32\cmd.exe	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)	
childproc	PID ### ended c:\windows\system32\cmd.exe	

← 14ms after conhost

← terminates after three seconds
no command-line arguments
no child procs
no file or registry writes
no netconns

red canary

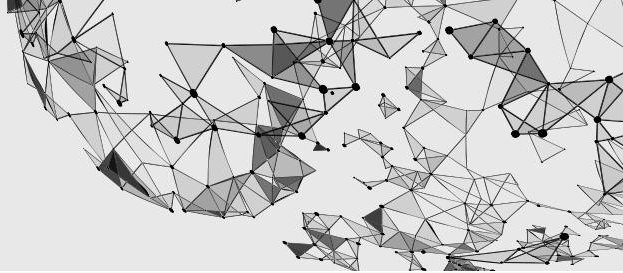


Type	Description	Search
childproc	PID ### started c:\windows\system32\cmd.exe	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)	
childproc	PID ### ended c:\windows\system32\cmd.exe	

← 14ms after conhost

← terminates after three seconds
no command-line arguments
no child procs
no file or registry writes
no netconns
one cross proc to csrss.exe

red canary

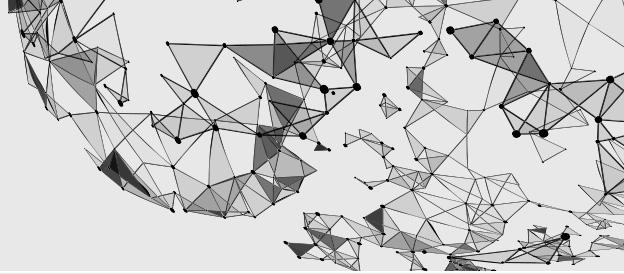


Type	Description	Search
childproc	PID ### started c:\windows\system32\cmd.exe	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)	
childproc	PID ### ended c:\windows\system32\cmd.exe	

← 14ms after conhost

← terminates after three seconds
no command-line arguments
no child procs
no file or registry writes
no netconns
one cross proc to csrss.exe
“change access rights?”

red canary

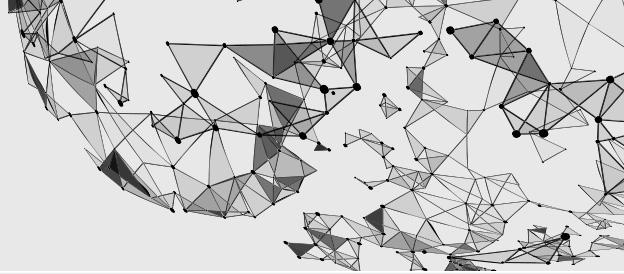


Type	Description	Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)	
childproc	PID ### ended c:\windows\system32\cmd.exe	← terminates after three seconds

PROCESS_VM_OPERATION
PROCESS_VM_WRITE

no command-line arguments
no child procs
no file or registry writes
no netconns
one cross proc to csrss.exe
“change access rights?”

red canary



Type	Description	Search
childproc	PID ### started c:\windows\system32\cmd.exe	e0b6cdee)
crossproc	Opened handle with change access rights to c:\windows\system32\svchost.exe (f586835082f632dc8d9404d83bc16316)	
childproc	PID ### ended c:\windows\system32\cmd.exe	

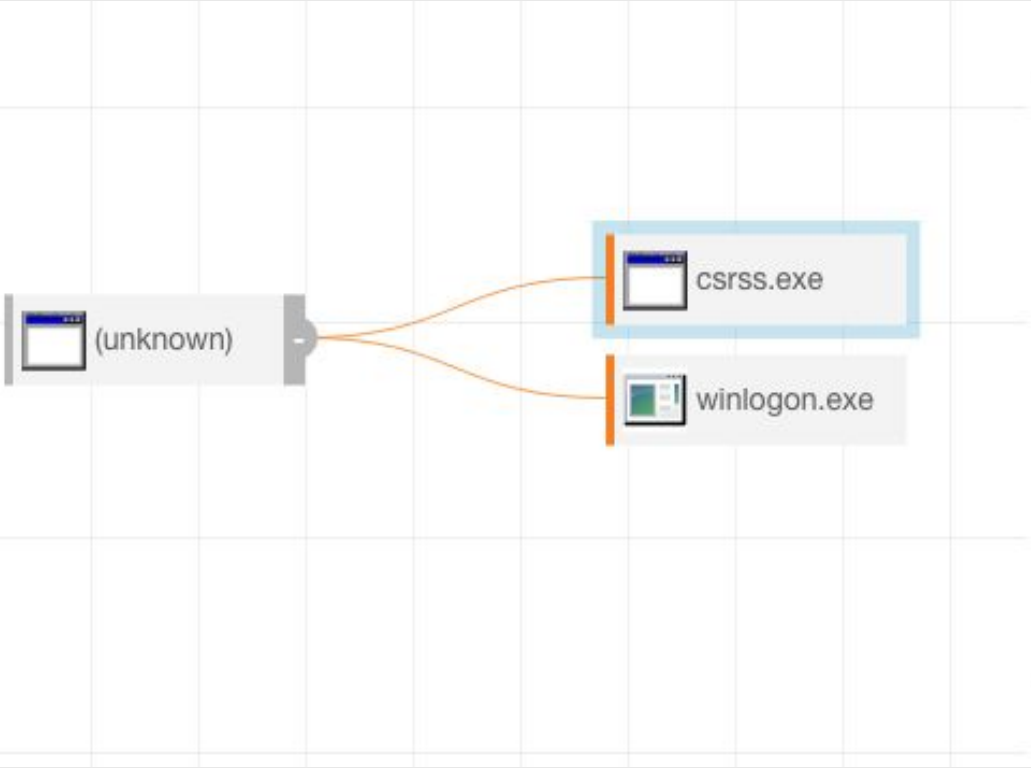
← 14ms after conhost

← terminates after three seconds
no command-line arguments
no child procs
no file or registry writes
no netconns
one cross proc to csrss.exe
"change access rights?"

PROCESS_VM_OPERATION
PROCESS_VM_WRITE

"These access rights allow this process to change the behavior of the target process."

red canary



Process: csrss.exe

PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\csrss.exe
Username	NT AUTHORITY\SYSTEM
MD5	72565e7a0145e0657e586f6cf7696dc7
SHA-256	6f1c9b4c187669bc0371260d121caf48d65f829a9104c483befbd8fc0bed24f5
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

csrss.exe: Signed by Microsoft Corporation

red canary

csrss.exe:

- **No child proc events**
- **33 reg mod events, none interesting**
- **20 modload events, all signed**
- **2 cross proc events, one from our cmd.exe, and one from its parent process**

Process: csrss.exe

PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\csrss.exe
Username	NT AUTHORITY\SYSTEM
MD5	72565e7a0145e0657e586f6cf7696dc7
SHA-256	6f1c9b4c187669bc0371260d121caf48d65f829a9104c483befbd8fc0bed24f5
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

csrss.exe: Signed by Microsoft Corporation

red canary

Process: csrss.exe

PID	[RED
OS Type	
P	ystem32\csrss.exe
	UTHORITY\SYSTEM
	72565e7a0145e0657e586f6cf7696dc7
SHA-256	6f1c9b4c187669bc0371260d121caf48d65f829a910 4c483befbd8fc0bed24f5
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

csrss.exe: Signed by Microsoft Corporation

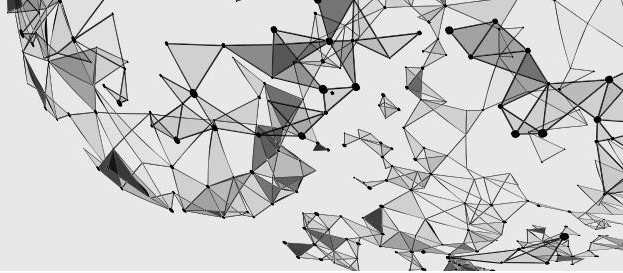
csrss.exe:

- **No child pr**
- **33 reg**
- **2**

one interesting
nts, all signed
c events, one from our
exe, and one from its parent process

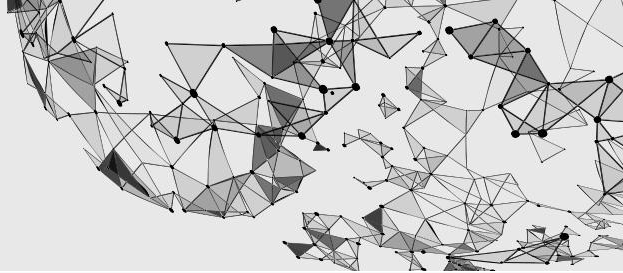
Not obviously malicious.

red canary



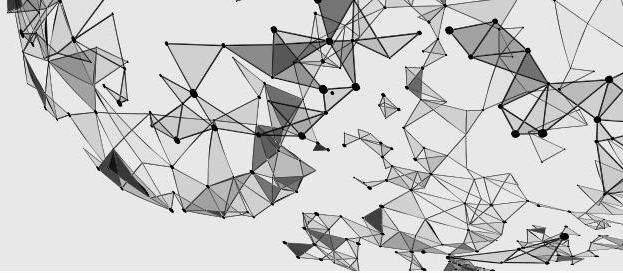
Type	Description		Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost	e0b6cdee)
crossproc	Opened handle w	17ms after conhost.exe →	2\svchost.exe (f586835082f632dc8d9404d83bc16316)
childproc	PID ### ended c:\windows\system32\cmd.exe **Signed** (8a2122e8162dbef04694b9c3e0b6cdee)		

red canary



Type	Description		Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost	e0b6cdee)
crossproc	Opened handle w	17ms after conhost.exe → "change access rights?"	2\svchost.exe (f586835082f632dc8d9404d83bc16316)
childproc	PID ### ended (		3162dbef04694b9c3e0b6cdee)

red canary



Type	Description		Search
childproc	PID ### started c:\windows\system32\cmd.exe	← 14ms after conhost	e0b6cdee)
crossproc	Opened handle w		2\svchost.exe (f586835082f632dc8d9404d83bc16316)
childproc	PID ### ended (		3162dbef04694b9c3e0b6cdee)

17ms after conhost.exe →
"change access rights?"
PROCESS_VM_OPERATION
PROCESS_VM_WRITE

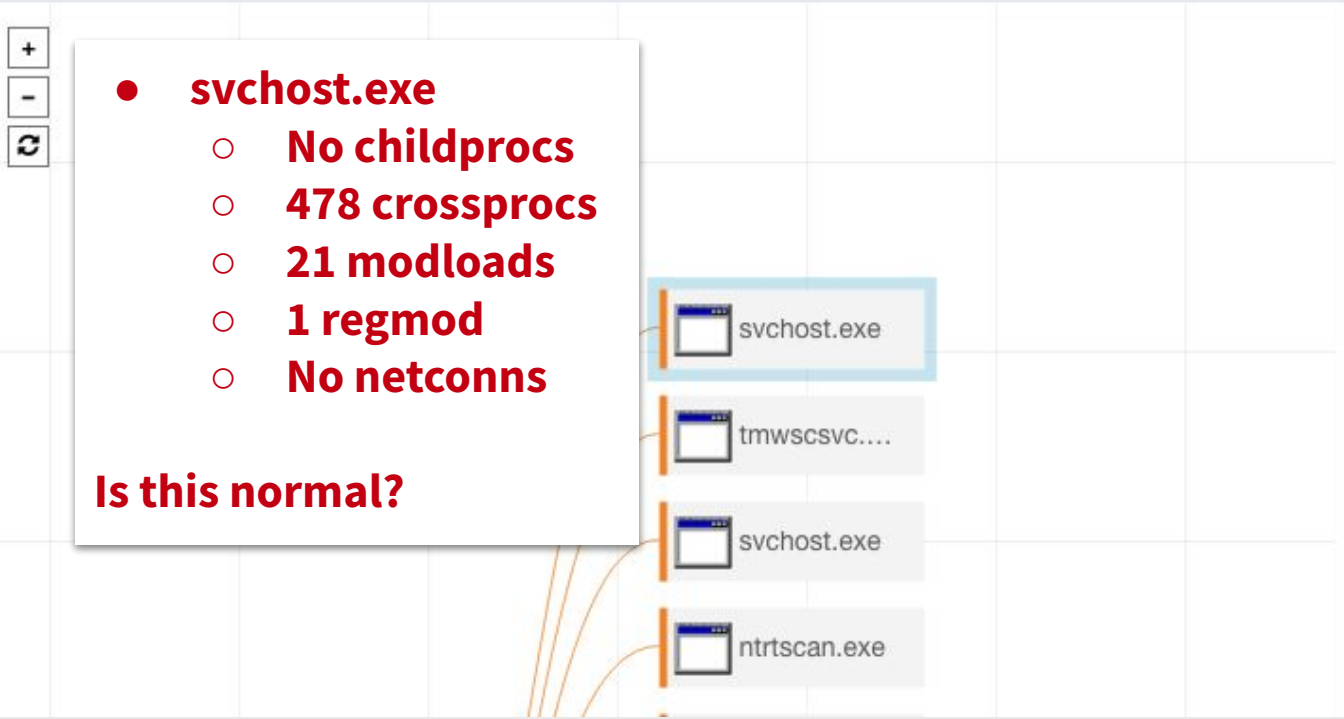
red canary

Process	Command Line - Copy	Host	User	Logon Type	State	Last Activity
svchost.exe	C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s Themes	[REDACTED]	NT AUTHORITY\SYSTEM	System	Running	2 days ago

Duration
3 days

- **svchost.exe**
  - **No childprocs**
  - **478 crossprocs**
  - **21 modloads**
  - **1 regmod**
  - **No netconns**

Is this normal?



Process: svchost.exe

PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\svchost.exe
Username	NT AUTHORITY\SYSTEM
MD5	f586835082f632dc8d9404d83bc163
SHA-256	643ec58e82e0272c97c2a59f602097 d5029db9c958c13b6558c7
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

svchost.exe: Signed by Microsoft Corporation

red canary

conhost 2/7

A handle to this process was opened with e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614d1d9290cd1069234f2a55cf8)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

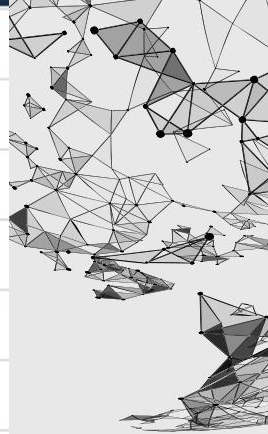
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A handle to this process was opened with change rights by c:\windows\system32\conhost.exe (81ca40085fc75babd2c91d18aa9ffa68)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)



red canary

conhost 2/7

A handle to this process was opened with e177d5beb5a6f6432ccf46fb3)
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)
A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)
A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)
A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614d1d9290cd1069234f2a55cf8)
A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)
A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)
A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)
A handle to this process was opened with change rights by c:\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)
A handle to this process was opened with change rights by c:\windows\system32\conhost.exe (81ca40085fc75babd2c
A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A handle to this process was opened with change rights by c:\windows\system32\conhost.exe (81ca40085fc75babd2c9

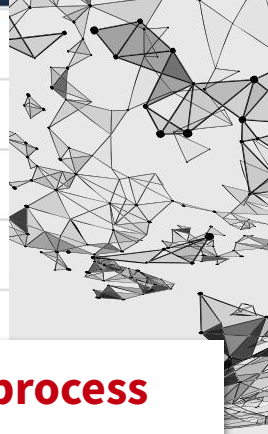
A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

← 2/7 (this page)
1 of 35 total

red canary



conhost 2/7

A handle to this process was opened with e177d5beb5a6f6432ccf46fb3)
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)
A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)
A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)
A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614
A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)
A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)
A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)
A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)
A handle to this process was opened with change rights by c:\windows\system32\conhost.exe (81ca40085fc75babd2c
A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f
A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is smartscreen.exe related? →

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is smartscreen.exe related? → Does it commonly open a handle to svchost?

← 2/7 (this page) 1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is smartscreen.exe related? →
Does it commonly open a handle to svchost?
What is it?

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is smartscreen.exe related? →
Does it commonly open a handle to svchost?
What is it?
No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is ctfmon.exe related? →

Is smartscreen.exe related? →
Does it commonly open a handle to svchost?
What is it?
No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is ctfmon.exe related? →
Is it common?

Is smartscreen.exe related? →
Does it commonly open a handle to svchost?
What is it?
No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

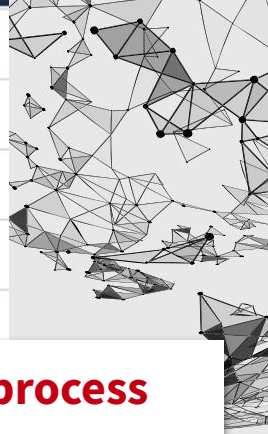
← conhost.exe's parent process

Is ctfmon.exe related? →
Is it common?
What is it?

Is s
Does it commonly open a handle to svchost?
What is it?
No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary



A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is ctfmon.exe related? →

Is werfault.exe related? →

Is s what is it?

Does it commonly open a handle to svchost?

What is it?

No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is ctfmon.exe related? →

Is werfault.exe related? →

Is it common?

Is s

Does it commonly open a handle to svchost?

What is it?

No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

← conhost.exe's parent process

Is ctfmon.exe related? →

Is werfault.exe related? →

Is it common?

What is it?

Is s

Do

handle to svchost?

What is it?

No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary

A handle to this process was opened with conhost 2/7 e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A handle to this process was opened with change rights by c:\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to this process was opened with change rights by c:\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A han :\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\explorer.exe (62022614

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to this process was opened with change rights by c:\windows\system32\rundll32.exe (ef3179d498793bf4234f708d3be28633)

A handle to :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f6432ccf46fb3)

A handle to :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

A ha :\windows\system32\smartscreen.exe (521ed922765bca8f79bd76188f879311)

A ha :\windows\system32\conhost.exe (81ca40085fc75babd2c

A ha :\windows\system32\ctfmon.exe (b625c18e177d5beb5a6f

A ha :\windows\system32\werfault.exe (5c06542fed8ee68994d43938e7326d75)

What about rundll32.exe? →

← conhost.exe's parent process

Is ctfmon.exe related? →

Is werfault.exe related? →

Is it common?

What is it?

Is s

Do

handle to svchost?

What is it?

No suspect filemods or netconns prior.

← 2/7 (this page)
1 of 35 total

red canary

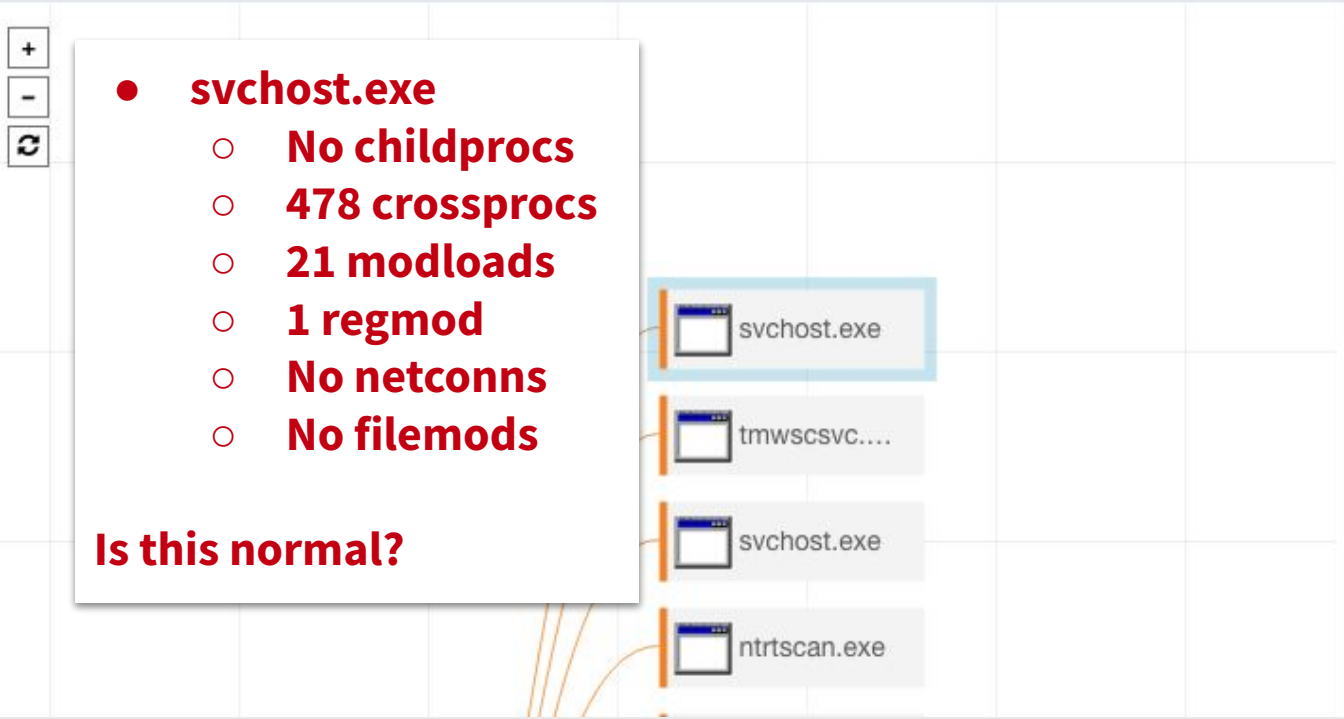
red canary

Process	Command Line - Copy	Host	User	Logon Type	State	Last Activity
svchost.exe	C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s Themes	[REDACTED]	NT AUTHORITY\SYSTEM	System	Running	2 days ago

Duration
3 days

- **svchost.exe**
  - **No childprocs**
  - **478 crossprocs**
  - **21 modloads**
  - **1 regmod**
  - **No netconns**
  - **No filemods**

Is this normal?



Process: svchost.exe

PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\svchost.exe
Username	NT AUTHORITY\SYSTEM
MD5	f586835082f632dc8d9404d83bc163
SHA-256	643ec58e82e0272c97c2a59f602097 d5029db9c958c13b6558c7
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

svchost.exe: Signed by Microsoft Corporation

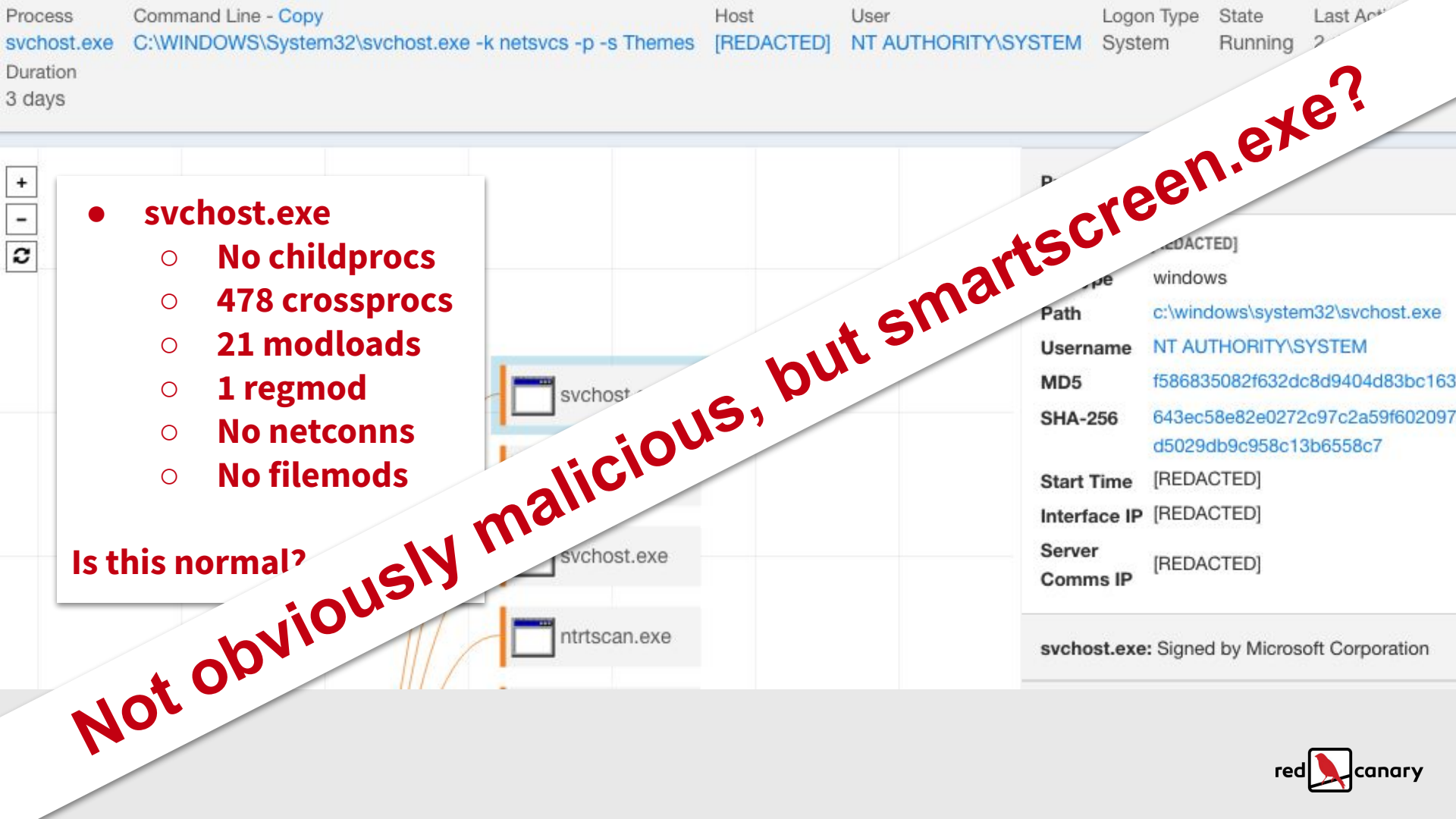
red canary

Process	Command Line - Copy	Host	User	Logon Type	State	Last Act
svchost.exe	C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s Themes	[REDACTED]	NT AUTHORITY\SYSTEM	System	Running	2

Duration
3 days

- svchost.exe
  - No childprocs
  - 478 crossprocs
  - 21 modloads
  - 1 regmod
  - No netconns
  - No filemods

Is this normal?



svchost

svchost.exe

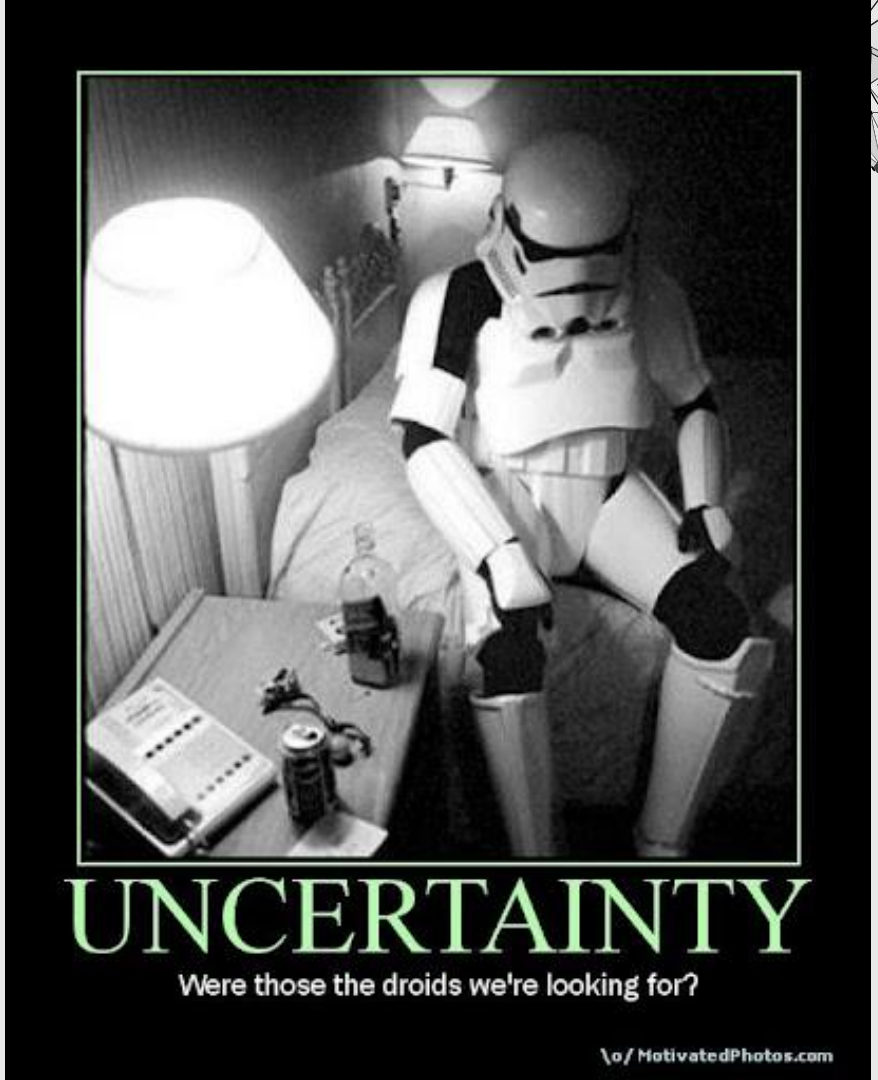
ntrtscan.exe

[REDACTED]

	windows
Path	c:\windows\system32\svchost.exe
Username	NT AUTHORITY\SYSTEM
MD5	f586835082f632dc8d9404d83bc163
SHA-256	643ec58e82e0272c97c2a59f602097 d5029db9c958c13b6558c7
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

svchost.exe: Signed by Microsoft Corporation

red canary


UNCERTAINTY
Were those the droids we're looking for?
\o/ MotivatedPhotos.com

red canary

Are you being primed?

Stop the ride, I want to get off.

Possibly.

Overview

~~Introductions~~

- ~~Who are you?~~
- ~~Who am I?~~

Why are Detection and Security Incident Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

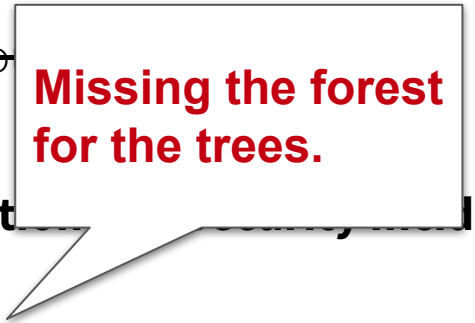
How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are yo~~
- ~~Who am I?~~



Why are Detect lent Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are yo~~
- ~~Who am I?~~

Why are Detect lent Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are yo~~
- ~~Who am I?~~

False positives.

Why are Detect lent Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are yo~~
- ~~Who am I?~~

False negatives.

Why are Detect lent Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are yo~~
- ~~Who am I?~~

Make it easier to read.

Why are Detect lent Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are yo~~
- ~~Who am I?~~

Why are Detect lent Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are yo~~
- ~~Who am I?~~

Crossing the streams on PID reuse.

Why are Detect lent Response Hard Problems(™)?

- Examples
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Overview

~~Introductions~~

- ~~Who are you?~~
- ~~Who am I?~~

Why are Detection and Security Incident Response Hard Problems(™)?

- ~~Examples~~
- Trouble with maps
- Systems of cognition

How can we make it easier?

red canary

Huh?

Maps are hard

EDR platforms are maps.

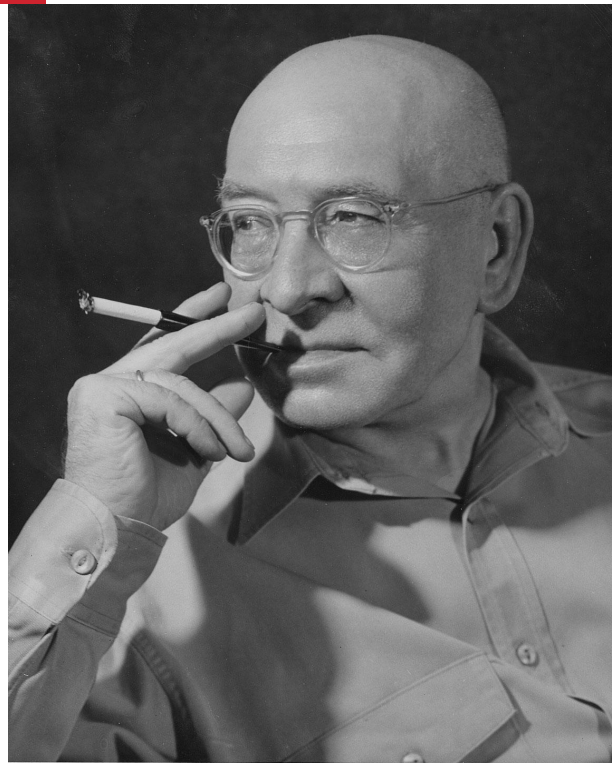
red canary

> > > > > > >
> > > > > > >
> > > > > > >
> > > > > > >
> > > >

Maps

“The map is not the territory.”

-- Alfred Korzybski



red canary

Problems with ~~maps~~ EDR tools

Maps may be incorrect

- Did conhost.exe really spawn cmd.exe?
- Did svchost.exe really modload System.Management.Automation?

Maps are lossy

- They can't tell you everything. **What did those crossproc threads do?**
- Some of what they don't tell you is **critically important**.

Maps require interpretation

- Readers of maps **may not understand** what they are looking at.
- Maps need maps, need maps, need maps...

red canary

Overview

~~Introductions~~

- ~~Who are you?~~
- ~~Who am I?~~

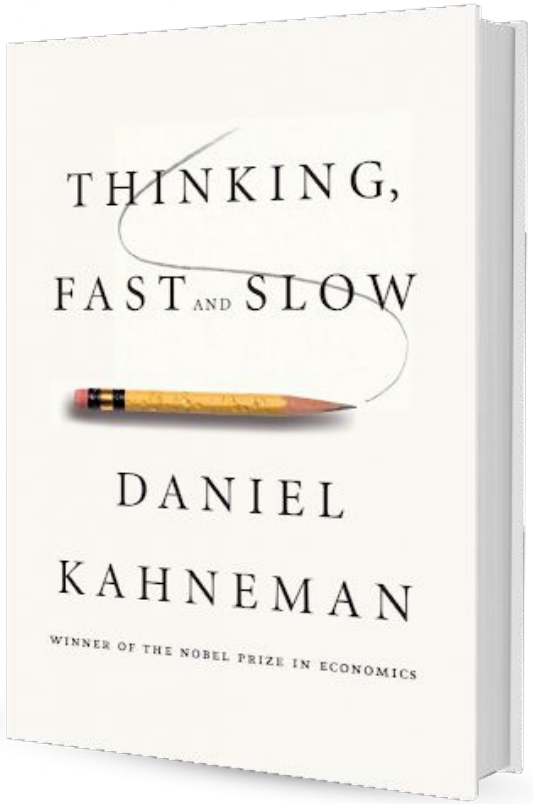
Why are Detection and Security Incident Response Hard Problems(™)?

- ~~Examples~~
- ~~Trouble with maps~~
- Systems of cognition

How can we make it easier?

red canary

Thinking systems



“... people, when engaged in a mental sprint, may become effectively blind.”

-- Daniel Kahneman

red canary

Let’s play a different game

What is this person feeling?

Let’s play a different game

What is this person feeling?

red canary

Let’s play a different game

What is this person feeling?

red canary

Let’s play a different game

What is this person feeling?

red canary

Let’s play a different game

What is this person feeling?

red canary

Let’s play a different game

What is this person feeling?

red canary

Let’s play a different game

What is this person feeling?

red canary

Let’s play a different game

What is this person feeling?

red canary

Let’s play a different game

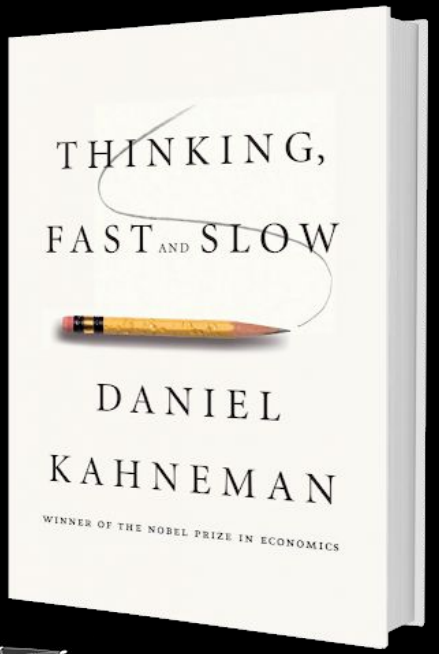
What is white’s next move?

5, 4, 3, 2, 1

red canary

What just happened?

You may have just experienced Kahneman's two systems of thinking.



red canary

	System One	System Two
Descriptions	Automatic, effortless, emotional, intuitive, perceptive, reactive	Expensive (calorically and from a risk perspective), lazy, rational, slow
Examples	Recognizing faces & expressions, dodging thrown / falling objects, chess puzzles (if you're a great chess player)	347 * 67.4, chess puzzles (if you're not a great chess player)
Implications	95% of our decisions System two tasks can become system one with enough training (chess puzzles, driving a stick-shift) Jumps to conclusions without understanding the size of the jump(s)	System two generally accepts system one's conclusions, which leads to biases (e.g. familiarity is a product of system one, system two relies on that to make judgements about truth and falsity)

Other K implications

- **Activated ideas**
- **Base rates** and **regression to the mean**

Overview

~~**Introductions**~~

- ~~Who are you?~~
- ~~Who am I?~~

Why are Detection and Security Incident Response Hard Problems(™)?

- ~~Examples~~
- ~~Trouble with maps~~
- ~~Systems of cognition~~

How can we make it easier?

red canary

So what?

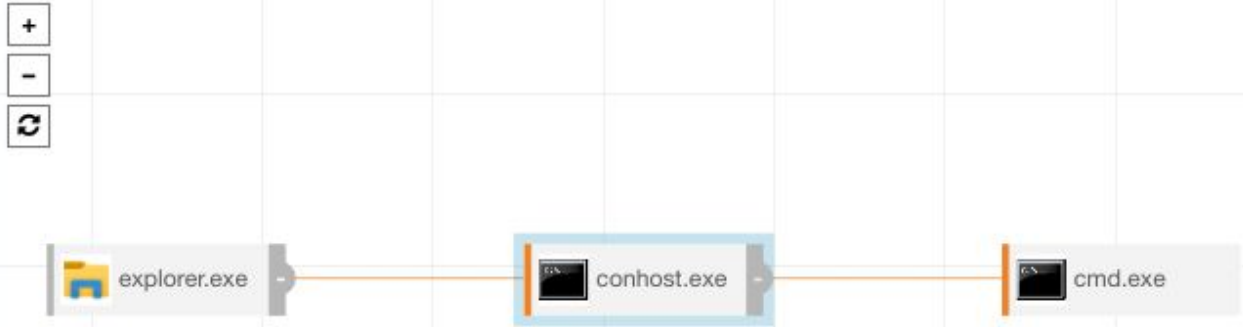
What do we do with this knowledge?

red canary

How do we make recognizing that this is good or bad...

red canary

Process	Command Line - Copy	Host	User	Logon Type	State	Started	Duration
conhost.exe	"C:\Windows\System32\conhost.exe"	[REDACTED]	[REDACTED]	Interactive	Terminated	a day ago	a few seconds



Process: conhost.exe

PID	[REDACTED]
OS Type	windows
Path	c:\windows\system32\conhost.exe
Username	[REDACTED]
MD5	81ca40085fc75babd2c91d18aa9ffa68
SHA-256	6651ab6c5c6d85c86b0c6c532115662e c1233e1434139346f25ef6
Start Time	[REDACTED]
Interface IP	[REDACTED]
Server Comms IP	[REDACTED]

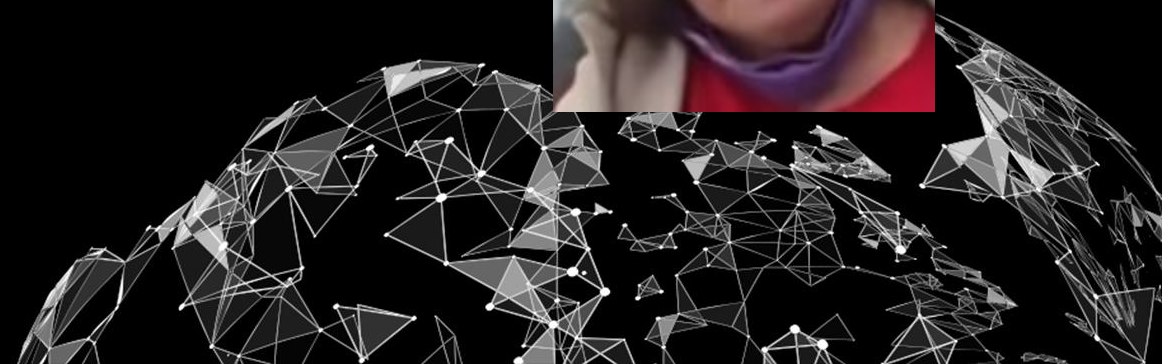
conhost.exe: Signed by Microsoft Corporation

red canary

as easy as recognizing that this kid is terrified or...

red canary

that this person is angry?



red canary

Start simple.

Here are some things we do today.

red canary

[THREAT-1372] Unwanted Software (Adware) affecting [REDACTED]

Remediated by [REDACTED] on [REDACTED].

[THREAT-151] Suspicious Activity (Dual-use and Process) affecting [REDACTED]

Acknowledged by [REDACTED] on [REDACTED].
Marked as not remediated by [REDACTED] on [REDACTED].

“ Adware was id
and home pag
additional unw
settings, netw

[THREAT-149] Malicious Software affecting [REDACTED]

Acknowledged by [REDACTED] on [REDACTED].

learn more about these classifications

“ Windows Pow
`kerberoast`

“ Windows PowerShell (`powershell.exe`) executed with an encoded command line and parameters that are indicative of malicious code execution.

red canary

[THREAT-1372] Unwanted Software (Adware) affecting [REDACTED]

Remediated by [REDACTED] on [REDACTED].

[THREAT-151] Suspicious Activity (Dual-use and Process) affecting [REDACTED]

Acknowledged by [REDACTED] on [REDACTED].
Marked as not remediated by [REDACTED] on [REDACTED].

“ Adware was id
and home pag
additional unw
settings, netw

[THREAT-149] Malicious Software affecting [REDACTED]

Acknowledged by [REDACTED] on [REDACTED].

learn more about these classifications

“ Windows Pow
`kerberoast`

“ Windows PowerShell (`powershell.exe`) executed with an encoded command line and parameters that are indicative of malicious code execution.

Use color to indicate severity.

red canary

Activated ideas

“What you see is all there is” -- maps have gaps

red canary

Threat occurred

Process spawned by explorer.exe

`c:\windows\system32\conhost.exe` 81ca40085fc75babd2c91d18aa9ffa68
6651ab6c5c6d85c86b0c6c532115662e09f338fa8cc1233e1434139346f25ef6

It's highly abnormal for the Console Window Host (`conhost.exe`) process to execute without command line arguments, and `conhost.exe` does not usually spawn child processes.

Fill in the gaps with more context.

Process spawned by conhost.exe

`c:\windows\system32\cmd.exe` 8a2122e8162dbef04694b9c3e0b6cdee
b99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450

The absence of command line parameters is indicative of an interactive session.

Process spawned by cmd.exe

`c:\windows\system32\rundll32.exe`

`ef3179d498793bf4234f708d3be28633`

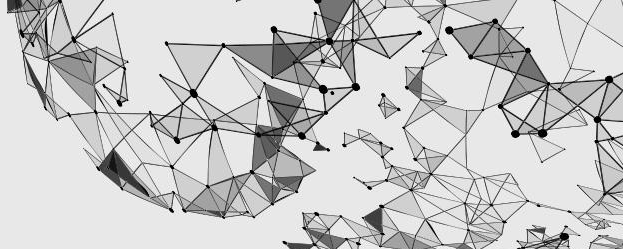
`b53f3c0cd32d7f20849850768da6431e5f876b7bfa61db0aa0700b02873393fa`

Command Line: `rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump [REDACTED] lsass.dmp full`

This command utilizes the Windows DLL Host (`rundll32.exe`) to call the MiniDump function of `comsvcs.dll` , and dump the Local Security Authority Subsystem Service (`lsass.exe`) process memory in order to retrieve credentials.

Explain why it matters.

red canary

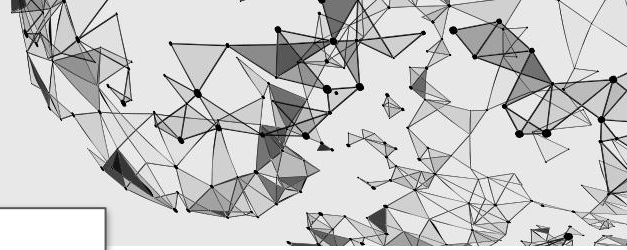


A process handle was opened by rundll32.exe to
`c:\windows\system32\lsass.exe` `15a556def233f112d127025ab51ac2d3`

This process injected into the memory of the Local Security Authority Subsystem Service (`lsass.exe`); this behavior is consistent with credential theft activity.

Explain why it matters.

red canary



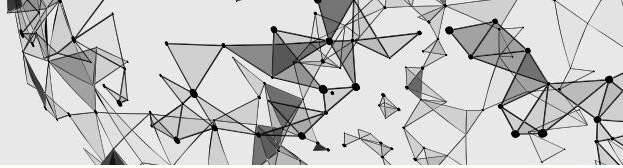
File first wrote

`c:\users\[REDACTED]\lsass.dmp`

Tell us the results, or...

The dumped process memory from the Local Security Authority Subsystem Service (`lsass.exe`) can be used to extract passwords and additional sensitive information.

red canary



Threat occurred

Process spawned

```
c:\program files (x86)\microsoft office\office16\winword.exe
ac5ecda03f8f58ed428f0a2b3713af61
99dab76e58cef2ecec369c24ae8774774ed0f76176f709b07e4b5dc0eca507a4
```

Command Line: `"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n "C:\Users\[REDACTED]\AppData\Local\Temp\Temp1_request (1).zip\WYSIATI-09.14.doc" /o ""`

The name of this `.zip` file is consistent with `A551` phishing campaigns.

In this case, the malicious macro was not executed.

lack thereof.

red canary

Base rates / regression to mean

Why intel matters...

- Direct Qbot phishing lures in early 2021 have consisted of ZIP attachments containing an macro-laden XLS dropper
    - Some campaigns followed the pattern of 1-2 words (seprated by dash or underscore), followed by 6-12 digits, followed by the date (MMDDYYYY), with the same name for both ZIP and XLS file, for example: `refusal-778578283-12072020.zip\refusal-778578283-12072020.xls`

Base rates / regression to mean

Why intel matters...

- As of June 2021, Qbot uses `regsvr32.exe` to register a randomly named DLL located in a subfolder of the `AppData\Roaming\Microsoft` directory, for example, `regsvr32.exe -s "C:\Users\[redacted]\AppData\Roaming\Microsoft\[random_a-z_chars]\[15_random_lowercase_a-z_chars].dll`.

Base rates / regression to mean

Why intel matters...

Qbot was historically seen in conjunction with other malware such as Emotet or TrickBot. These cases often begin with Emotet as the initial infection vector followed by delivery of Qbot, TrickBot, or ransomware variants as follow-on payloads. If Qbot is present in an environment, these other malware families may be present as well. In late 2020, environments impacted by Egregor ransomware have been observed to also be infected with widespread, laterally moving Qbot infections.

Base rates / regression to mean

Loaded c:\windows\assembly\nativeimages_v2.0.50727_64\system\58dbf598501f1327314c7ad2f003d5a9\system.ni.dll **Signed** (d6425a68020a5e146903cd254d4685c8)

Loaded c:\windows\assembly\nativeimages_v2.0.50727_64\system.management.a#\de5c1bef15eb922e69a3223b17c8e952\system.management.automation.ni.dll **Signed** (a48f60db9dc59396e716fc61fa9f6e69) **Highly uncommon**

Loaded c:\windows\system32\rsaenh.dll **Signed** (3c269391b3e96c30a68e0c242cc4d52e)

Give us some indication of base rates.

red canary

[REDACTED] UTC [REDACTED] [REDACTED] [REDACTED]

WIN-POWERSHELL-IEX-CMDLINE-CHAR
WIN-KNOWN-POWERSHELL-MAL-CLI
WIN-POWERSHELL-BXOR
WIN-POWERSHELL-WEBPROXY
WIN-POWERSHELL-DATA-DOWNLOAD
WIN-POWERSHELL-SHORTENED-ENCODEDCOMMAND-SWITCH
WIN-POWERSHELL-BASE64-METHOD
WIN-POWERSHELL-OBF-CHAR
WIN-REMOTETHREAD-INJECTION-FROM-POWERSHELL
WIN-POWERSHELL-AMSI-BYPASS
WIN-EVENTVWR-UAC-BYPASS

red canary

Measure the effectiveness of your detection analytics.

Show your analysts those metrics.

[REDACTED] UTC [REDACTED] [REDAC

WIN-POWERSHE	(14.99)	S
WIN-KNOWN-	(14.98)	S
W	(14.92)	S
WIN-PO	(0.31)	S
WIN-POWERSH	(14.99)	S
WIN-POWERSHELL-SHORTENED-ENCODEDCOMMAND-SWITCH	(15.00)	S
WIN-POWERSHELL-BASE64-METHOD	(13.19)	S
WIN-POWERSHELL-OBF-CHAR	(1.91)	S
WIN-REMOTETHREAD-INJECTION-FROM-POWERSHELL	(8.88)	S
WIN-POWERSHELL-AMSI-BYPASS	(14.89)	S
WIN-EVENTVWR-UAC-BYPASS	(9.07)	S

red canary

Quick recap

- Maps v territories
- Systems of cognition
- Making things easier

Maps v territories

- **EDR platforms are maps**
  - Defenders want the territory (all the data)
  - Maps **are lossy**
  - Maps **require interpretation** (maps of maps of maps)
  - Maps **may be incorrect**
  - Lossiness leads to "**what you see is all there is**"

red canary

Systems of cognition

- **System one and system two**
  - System one is automatic, **jumps to conclusions**
  - System two is expensive, **believes system one**
  - Neither system is aware of what it isn't aware of -- "**what you see is all there is**"
  - System two tasks **+ experience ~=** system one tasks

Making things easier

- **Minimize reliance on System two**
  - **Color code** and **Annotate** detections
  - **Measure** detection analytics
  - **Show** the analytic scores
  - **Study** OS internals
  - **Practice** incidents and attacker TTPs
  - Understand and present **base rates** and **regression to the mean**

red canary

What else?

- We’re really just scratching the surface.
- What are you doing?
- What else should be done?

Thank you!

Q & A

QR code for slides or visit:
https://github.com/davehull/presentations/blob/main/NolaCon_2022_Maps_Gaps.pdf

red canary