OpTC Red Team Ground Truth

Day 1

Day 1 "Plain PowerShell Empire"

Summary:
Manually connected to Sysclient0201 and downloaded malicious PowerShell Empire stager stored in a batch file. Used priv escalation methods to obtain elevated agent. Used Mimikatz to collect credentials. Attempted to inject into LSASS but it failed. Used registry edits to establish persistence. Collected screenshot of desktop. Attempted network scanning methods. Created port scan script, imported into memory and ran against /24 network. Pivoted to Sysclient0402 with WMI.

On Sysclient0402, conducted ping sweep of /24 network. Pivoted to Sysclient0660 via WMI.

On Sysclient0660, used ipconfig through powershell to obtain ip. Used mimikatz in attempt to gather logged in user's password. Attempted process migration, failed. Attempted to inject shellcode, failed. Ran scripts to get information on Domain Controller. Downloaded file from C:/. Used WMI to pivot to DC1.

Killed all other agents.

On DC1, ran mimikatz. Obtained user hashes with lsadump. Pivoted to 14 stations. Killed all agents. End of day1.

C2:
server -- news.com:80
ip -- 132.197.158.98
delay -- 5 seconds
profile -- /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Client	AgentID	ReportedIP	PID
Sysclient0201	VL8B5T3U	142.20.56.202	5452
Sysclient0201	LUAVR71T	142.20.56.202	2952
Sysclient0402	NEK5H8GX	142.20.57.147	3168
Sysclient0660	DS29HY41	142.20.58.149	880
SYSCLIENT0104	K9SW73AF	142.20.56.105	3160
SYSCLIENT0205	MX9LTPSF	142.20.56.206	5012
SYSCLIENT0321	AC5BVNRP	142.20.57.66	2980
SYSCLIENT0255	HR3PK2ZF	142.20.57.0	3472
SYSCLIENT0355	A83TU4KL	142.20.57.100	1884
SYSCLIENT0503	872METCN	142.20.57.248	1472
SYSCLIENT0462	FNP6XK89	142.20.57.207	2536
SYSCLIENT0559	ANP2E69T	142.20.58.48	1400
SYSCLIENT0419	XS3AWFB9	142.20.57.164	1700
SYSCLIENT0609	325T9FEN	142.20.58.98	3460
SYSCLIENT0771	75HYXEL3	142.20.59.4	4244
SYSCLIENT0955	98GKNAFX	142.20.59.188	4760
SYSCLIENT0874	LZFHNCES	142.20.59.107	5224
SYSCLIENT0170	UD9R6S7T	142.20.56.171	644
DC1	XH32VTK5	142.20.61.130	1852

Log:

```
09/23/19 11:23:29 -- Manually accessed console on Sysclient0201 and navigated to news.com:8000 to download runme.bat, a malicous Powershell empire stager
09/23/19 11:24:19 -- Sysclient0201, closed firefox tab and deleted runme.bat
09/23/19 11:24:54 -- Successfull checkin for Agent VL8B5T3U on Sysclient0201 ip 142.20.56.202
09/23/19 11:26:02 -- On Sysclient0201 agent VL8B5T3U, Used PowershellEmpire Module Bypasses UAC, which performs a registry modification of the "windir" value in "Environment" to bypass UAC.
09/23/19 11:26:38 -- On sysclient0201, successful checkin of elevated agent LUAVR71T
09/23/19 11:26:56 -- On Sysclient0201, killing agent VL8B5T3U
09/23/19 11:33:14 -- On Sysclient0201 agent LUAVR71T, ran mimikatz to collect clear text passwords in memory
09/23/19 11:35:26 -- On Sysclient0201 agent LUAVR71T, obtained password for user systemia.com\zleazer via mimikatz
09/23/19 11:37:15 -- On Sysclient0201 agent LUAVR71T, used psinject to inject into the LSASS process
09/23/19 11:38:09 -- On Sysclient0201 agent LUAVR71T, Process injection seems to have failed.
09/23/19 11:39:25 -- On Sysclient0201 agent LUAVR71T, established persistence by modifying HKCU:Software\Microsoft\Windows\CurrentVersion\Debug registry entry
09/23/19 11:40:41 -- On Sysclient0201 agent LUAVR71T, obtained process listing by running ps through powershell
09/23/19 11:41:50 -- On Sysclient0201 agent LUAVR71T, retried psinject into lsass
09/23/19 12:51:59 -- On Sysclient0201 agent LUAVR71T, collected data collection by obtaining a screenshot of the desktop.
09/23/19 12:58:20 -- On Sysclient0201 agent LUAVR71T, conducted ARP scan on /22 of 142.20.56.202
09/23/19 13:07:11 -- On Sysclient0201 agent LUAVR71T, ARP scan failed. Attempting to use SMB on 142.20.56.204 with credentials from Sysclient0201
09/23/19 13:08:28 -- On Sysclient0201 agent LUAVR71T, re-attempted ARP scan without setting any values.
```

```
09/23/19 13:15:48 -- On Sysclient0201 agent LUAVR71T, executed ping sweep against 142.20.56.0/24
09/23/19 13:24:36 -- On Sysclient0201 agent LUAVR71T, pivoted to Sysclient0402 using invoke_wmi
09/23/19 13:25:41 -- On sysclient0402 agent NEK5H8GX checked in as an elevated agent
09/23/19 13:29:47 -- On Sysclient0402 agent NEK5H8GX, imported and ran ping sweep script to run against 142.20.57.0/24
09/23/19 13:35:22 -- On Sysclient0402 agent NEK5H8GX, pivoted to Sysclient0660 using invoke_wmi. Agent DS29HY41 checks in.
09/23/19 13:38:31 -- On Sysclient0660 agent DS29HY41, used ipconfig to obtain IP
09/23/19 13:40:38 -- On Sysclient0660 agent DS29HY41, used mimikatz to obtain cleartext passwords from memory
09/23/19 13:44:23 -- On Sysclient0660 agent DS29HY41, attempted to migrate to local user process with psinject. Failed to inject.
09/23/19 13:49:00 -- On Sysclient0660 agent DS29HY41, obtained list of processes with ps
09/23/19 13:50:56 -- On Sysclient0660 agent DS29HY41, attempted to inject shellcode into process 4480. Injection failed.
09/23/19 13:54:11 -- On Sysclient0660 agent DS29HY41, executed script to return domain controller information.
09/23/19 13:56:48 -- On Sysclient0660 agent DS29HY41, imported and ran powershell script to find domain controllers
09/23/19 14:02:12 -- On Sysclient0660 agent DS29HY41, downloaded file zipfldr.dll
09/23/19 14:04:45 -- On Sysclient0660 agent DS29HY41, used invoke_wmi to pivto to domain controller 1. XH32VTK5 checks in on ip
142.20.58.149
09/23/19 14:06:01 -- Killed agents Sysclient0201 LUAVR71T, Sysclient0402 NEK5H8GX and Sysclient0660 DS29HY41
09/23/19 14:07:21 -- On DC1 agent XH32VTK5, ran mimikatz
09/23/19 14:09:21 -- On DC1 agent XH32VTK5, gathered user hdorka's hashes using mimikatz's lsadump capability
09/23/19 14:45:13 -- On DC1 agent XH32VTK5, used Invoke_wmi to spread to:
SYSCLIENT0104,SYSCLIENT0170,SYSCLIENT0205,SYSCLIENT0255,SYSCLIENT0321,SYSCLIENT0355,SYSCLIENT0419,SYSCLIENT0462
,SYSCLIENT0503,SYSCLIENT0559,SYSCLIENT0609,SYSCLIENT0771,SYSCLIENT0874,SYSCLIENT0955
09/23/19 15:24:33 -- On DC1 agent XH32VTK5, kill agents on:
SYSCLIENT0104,SYSCLIENT0170,SYSCLIENT0205,SYSCLIENT0255,SYSCLIENT0321,SYSCLIENT0355,SYSCLIENT0419,SYSCLIENT0462
,SYSCLIENT0503,SYSCLIENT0559,SYSCLIENT0609,SYSCLIENT0771,SYSCLIENT0874,SYSCLIENT0955
09/23/19 15:30:00 -- On Sysclient0201, removed registry persistence at HKCU:Software\Microsoft\Windows\CurrentVersion\Debug
```

Day 2

Day 2 "Custom Powershell Empire"

Summary:
Sent phishing emails to two clients containing malicious macroless_word PowerShell empire stagers. Once checked in, the agents were used to switch to a seperate PowerShell Empire server with configurations that were modified from default settings and were sent over https/443. Deathstar was used to automate enumerating the domain and obtaining an elevated shell on the doman controller.

The DC agent was used to pivot back to original target to obtain an elevated agent. Persistence was established using WMI subscriptions to call back at 10:00 or withing 5 minutes of boot. Ran modules to enumerate the local system looking for vulnerablities or important files.

Uploaded plink and created complted local port forwarding with ssh to the attacker server. Forwarded port 3389 to allow RDP into systemia through any network security devices. RDPed into target and used netcat to exfiltrate data. Used RDP to tunnel through two other hosts. On the final host, connected network share and exfilled a majority of files via netcat.

Cleaned up files and shut down RDP sessions. Used existing agent on DC to re infect five workstations for overnight C2.

Listener information:
Powershell launcher string -- "powershell -NoProfile -Sta -WindowStyle 1 -EncodedCommand"
DefaultProfile -- "/news/current.php,/login/default.php,/admin/process.jsp|Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.167 Safari/537.36"
DefaultDelay Between connections -- 30 seconds
ServerVersion -- Apache
IP: 202.6.172.98

Client,	Agent,	IP,	PID
Sysclient0501	4BW2MKUF	142.20.57.246	648
Sysclient0501	9HUGDCRL	142.20.57.246	5076
Sysclient0501	6H8SZPCW	142.20.57.246	1748
Sysclient0811	DS8V3RNH	142.20.59.44	3780
DC1.systemia.com	VUBW3KYE	142.20.61.130	3880
Sysclient0010	6FEZ8L4N	142.20.56.11	3584
Sysclient0069	EMK3VW7F	142.20.56.70	4152
Sysclient0203	UXCSTKZ9	142.20.56.204	5388
Sysclient0358	PE54DBYX	142.20.57.103	2984
Sysclient0618	73FCWS1G	142.20.58.107	4060
Sysclient0851	5BUEZALX	142.20.59.84	4652

Log:

```
09/24/19 10:28:56 -- Sent email with malicious word document to bantonio@systemia.com on Sysclient0501 and rsantilli@systemia.com on
Sysclient0811 from sgerard@ameblo.jp
09/24/19 10:36:51 -- On Sysclient0501, opened malicious attachemnt named payroll.docx. Agent K3G1U8DN checks in.
09/24/19 10:40:14 -- On Sysclient0811, opened malicious attachment named payroll.docx. Agent DS8V3RNH checks in.
```

```
09/24/19 10:46:02 -- On Sysclient0501 agent K3G1U8DN, injected powershell script to pivot to PowerShell Empire on sports.com 202.6.172.98 port 443, Agent 4BW2MKUF checks in.
09/24/19 10:51:49 -- Killed agent K3G1U8DN on Sysclient0501
09/24/19 11:03:36 -- Started DeathStar to auto find and obtain access to domain controller
09/24/19 11:04:12 -- Deathstar via Sysclient0501 agent 4BW2MKUF, obtains domain SID
09/24/19 11:04:35 -- Deathstar via Sysclient0501 agent 4BW2MKUF, obtains list of 43 Domain Admins
09/24/19 11:05:39 -- Deathstar via Sysclient0501 agent 4BW2MKUF, queried to find domain controllers
09/24/19 11:09:08 -- Deathstar via Sysclient0501 agent 4BW2MKUF, started lateral movement
09/24/19 11:09:22 -- Deathstar via Sysclient0501 agent 4BW2MKUF, started domain privesc
09/24/19 11:09:44 -- Deathstar via Sysclient0501 agent 4BW2MKUF, attempting to elevate using bypassuac_eventvwr
09/24/19 11:10:32 -- Deathstar via Sysclient0501 agent 4BW2MKUF, searched for GPOs containing credentials using GPP SYSVOL privesc
09/24/19 11:13:32 -- Deathstar via Sysclient0501 agent 4BW2MKUF, discovered current security context has admint o 1025 hosts.
09/24/19 11:20:19 -- On Sysclient0501 agent 4BW2MKUF, obtained elevated agent on domain controller. Agent VUBW3KYE on DC1.systemia.com checks in.
09/24/19 11:23:27 -- On Sysclient0501 agent 4BW2MKUF, attempted to bypassed UAC with module privesc/bypassuac_env which modifies registry entry of windir value in environment
09/24/19 11:23:45 -- On Sysclient0501 agent 4BW2MKUF, privesc failed.
09/24/19 11:25:06 -- On Sysclient0501 agent 4BW2MKUF, attempted bypassuac with privesc/bypassuac_fodhelper. Failed.
09/24/19 11:26:34 -- On Sysclient0501 agent 4BW2MKUF, used invoke wmi on localhost to obtain elevated Agent. Failed to elevated, normal agent 9HUGDCRL checked in.
09/24/19 11:31:17 -- On DC1.systemia.com agent VUBW3KYE, attempted to pivot to obtain elevated agent using WMI. Got access denied for Sysclient0501 and 0502
09/24/19 11:33:15 -- On DC1.systemia.com agent VUBW3KYE, pivoted to Sysclient0501 with an elevated agent by usign administrator credentials. Agent 6H8SZPCW checks in.
09/24/19 11:34:56 -- On Sysclient0501 agent 6H8SZPCW, set persistence using WMI subscription. Set to reach back at 10:00 everyday or within 5 minutes of boot.
09/24/19 11:35:53 -- Killed agents Sysclient0501 4BW2MKUF and Sysclient0501 9HUGDCRL
09/24/19 11:37:35 -- On Sysclient0501 agent 6H8SZPCW, used findtrusteddocuments to enumerate registry to determine any trusted documents and trusted locations.
09/24/19 11:39:38 -- On Sysclient0501 agent 6H8SZPCW, used winenum script with keywords "important,secret,classified" to search files and obtain host information
09/24/19 11:41:53 -- On Sysclient0501 agent 6H8SZPCW, ran script to check for windows privesc vectors.
09/24/19 11:45:13 -- On Sysclient0501 agent 6H8SZPCW, uploaded plink.exe
09/24/19 13:05:03 -- On Sysclient0501 agent 6H8SZPCW, validated upload worked with ls command
09/24/19 13:11:23 -- On Sysclient0501 agent 6H8SZPCW, started reverse ssh connection to port forward RDP port to attacker system. Lost contact with agent 6H8SZPCW.
09/24/19 13:19:38 -- On Sysclient0501, connected via RDP to host via forwarded port using sysadmin account.
09/24/19 13:25:46 -- Agent DS8V3RNH lost contact.
09/24/19 13:26:57 -- On Sysclient0501 via RDP session, downloaded fileTransfer1000.exe (nc.exe) from news.com:8080 via chrome.
09/24/19 13:31:29 -- On Sysclient0501 via RDP session, compressed documents in C:\documents for exfiltration.
09/24/19 13:44:34 -- On Sysclient0501 via RDP session, exfiltrated export.zip to news.com port 9999 using fileTransfer1000.exe (nc.exe)
09/24/19 13:45:12 -- On Sysclient0501 via RDP session, cleaned up fileTransfer1000.exe and export.zip
09/24/19 13:46:58 -- On Sysclient0501 via RDP session, RDPed to Sysclient0974
09/24/19 13:51:45 -- On Sysclient0974 via RDP session, browsed files in C:\documents
09/24/19 13:54:43 -- On Sysclient0974 via RDP session, RDPed to Sysclient0005
09/24/19 14:06:06 -- On Sysclient0005 via RDP session, mounted network share \\142.20.61.135\share
09/24/19 14:34:31 -- On Sysclient0005 via RDP session, added majority of share drive files to compressed folder name allgone.zip and moved to user Download folder.
09/24/19 14:37:02 -- On Sysclient0005 via RDP session, navigated to news.com:4445 and downloaded movingonup.exe (nc.exe)
09/24/19 15:04:14 -- On Sysclient0005 via RDP session, exported 3.5 gb exfil file allgona.zip
09/24/19 15:22:48 -- On Sysclient0005 via RDP session, cleaned up files in downloads folder
09/24/19 15:23:26 -- On Sysclient0005 closed RDP session.
09/24/19 15:27:32 -- On Sysclient0974 closed RDP session.
09/24/19 15:28:36 -- On Sysclient0501 closed RDP session.
09/24/19 15:42:36 -- On DC1.systemia.com agent VUBW3KYE, used invoke_wmi to spread to Sysclient0010,Sysclient0069,Sysclient0203,Sysclient0358,Sysclient0618,Sysclient0851
09/25/19 09:00:00 -- Agents ran overnight on: DC1.systemia.com VUBW3KYE, Sysclient0010 6FEZ8L4N, Sysclient0069 EMK3VW7F, Sysclient0203 UXCSTKZ9, Sysclient0358 PE54DBYX, Sysclient0618 73FCWS1G, Sysclient0851 5BUEZALX
09/25/19 10:00:00 -- Sysclinet0501 WMI Subcription persistence method activates, agent XVGHS45M checks in.
```

Day 3

Day 3 "Malicious Upgrade"

Summary:
Notepad plus was installed on hosts within Systemia but was susceptible to a malicious upgrade process. When updated, the software reached out to malicous server and downloads a binary named update.exe. The malicious binary contianed a reverse tcp meterpreter payload. It connected back to the server on port 8080. Software update was executed on two systems.

Once a connection was established, system level access was obtained. A shell was used to find local information and a network arp scan was used to identify potential targets. Built in meterpreter modules were used to enumerate local software and any shares.

The meterpreter agent was migrated from the intial one to lsass and mimikatz was used to collect clear text password and hashes. Persistence was established via an autorun registry entry. Timestomper was used to black the MAC times for files created by the persistence process. Added new admin user to attempt RDP connection.

On one client meterpereter was used to migrate to the lwabeat process.

Attacker Server DNS Names:
notepadplus-sourceforge.net
microsoft.com
IP: 53.192.68.50

Meterpreter process on Sysclient0051
PID 2712 cKfGW.exe
Migrated to lsass

Meterpreter process on Sysclient0351
PID 1932 f.exe
migrated to lwabeats

09/25/19 10:29:42 -- On Sysclient0051, updated notepad++ which download malicious binary "update.exe" which is a meterpreter payload.
09/25/19 10:31:08 -- On Sysclient0051, obtained system via meterpreters get system module. Used named pipe impersonation in memory.
09/25/19 10:32:11 -- On Sysclient0051, used meterpreter to get cmd shell. Ran commands to find out information about local system.
09/25/19 10:33:55 -- On Sysclinet0051, used arp scanner on 142.20.56.0/22
09/25/19 10:36:28 -- On Sysclient0051, used meterpreter enum modules to discover all installed applications
09/25/19 10:37:52 -- On Sysclient0051 used meterpreter enum_domain modules to identify domain controller
09/25/19 10:38:35 -- On Sysclient 0051, used meterpreter enum_shares to identify any shares on host
09/25/19 10:40:39 -- On Sysclient 0051, migrated from process 2712 cKfGW.exe to lsass 568
09/25/19 10:44:56 -- On Sysclient0051, ran mimikatz to collect cleartext passwords and hashes
09/25/19 10:48:43 -- On Sysclient0051, established persitence via meterpreter. Script written to C:\Windows\TEMP\myHbYXTpViwX.vbx. Installed Autorun at HKLM\Software\Microsoft\Windows\CurrentVersion\Run\RTqWaEHv
09/25/19 10:53:06 -- On Sysclient0051, used timestomp to edit MAC times of crated files in C:\Windows\TEMP
09/25/19 11:07:41 -- On Sysclient0051, used get_gui to add administrator "admin" to administrators and RDP group
09/25/19 11:23:31 -- On Sysclient0351, conducted update to notepadd++, which downloaded malicous update.exe binary which made connection back to attacker server
09/25/19 11:24:30 -- On Sysclient0351, migrated from process 1932 to 1256 lwabeat.
09/25/19 13:42:05 -- On Sysclient0051, RDPed to machine from attacker server.
09/25/19 14:24:03 -- Reran updated.exe on Sysclient0051