HACKTHEBOX

Real-world Incident Report Template

December 2024

Index

Real-world Incident Report

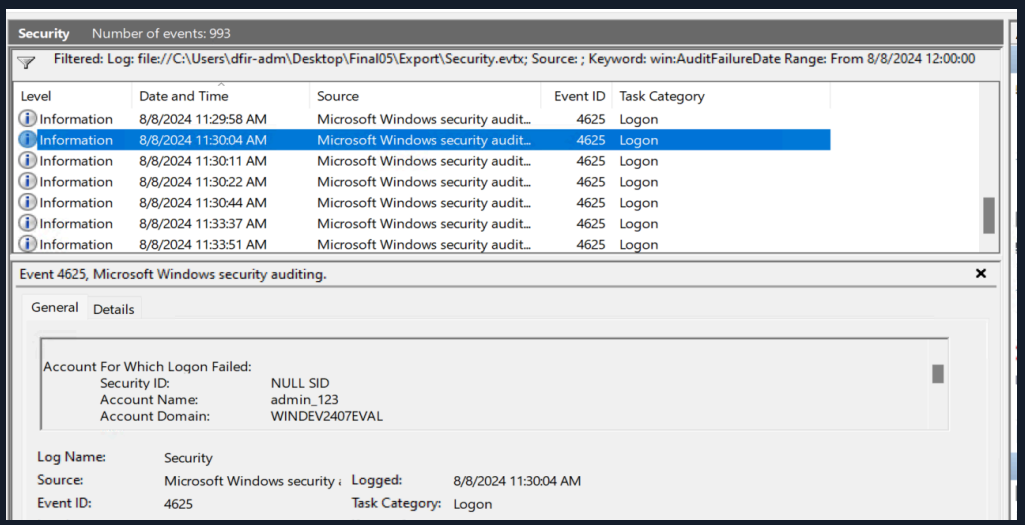
Executive Summary

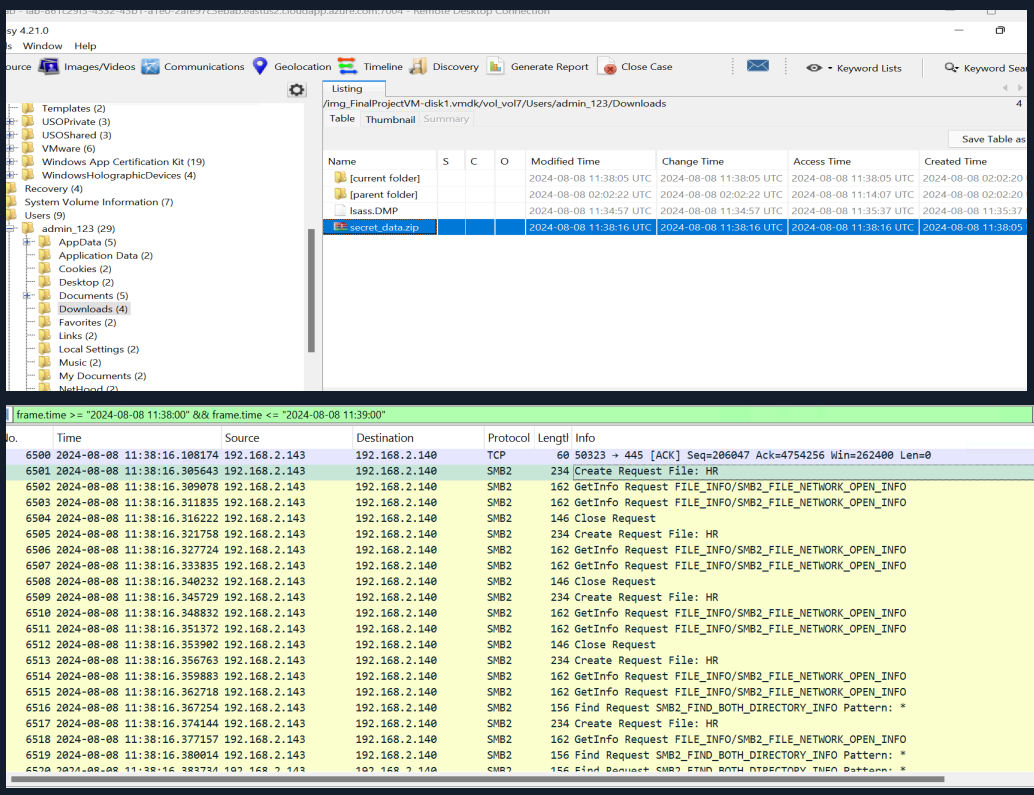
- Incident ID: INC-Final Lab
- Incident Severity: High (P2)
- Incident Status: ?
- Incident Overview: On August 8, 2024, at 11:25 UTC, SampleCorp's Security Operations Center (SOC) detected a SOCGHOLISH DRIVE-BY MALWARE DROP. The incident had many indicators of compromise to include malicious PowerShell commands initiating the download of a file, beacon.exe, followed by execution of Mimikatz.exe. The attacker used this to escalate privileges and exfiltrate sensitive data, including source code and HR-related files.

Technical Analysis:

Beacon Detected: A beacon.exe file was found in the memory dump, as well as prefetch files in Autopsy indicating that the attacker likely established a Command and Control (C2) channel to maintain persistence and execute post-exploitation tasks.

Admin Account Compromised: The attacker gained unauthorized access to the administrative account admin-123 after multiple failed logins by way of credential stealing, enabling them to exfiltrate sensitive information. Basic user had a document with credentials stored on the desktop. Time and Date stamps correlate in logs and access files of when the data was accessed.

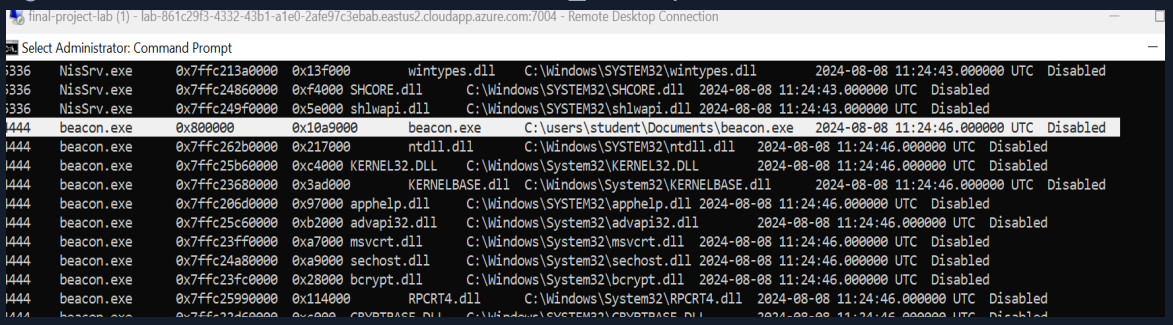




Exfiltration of Credentials: .txt files containing usernames and administrative passwords, including a file named secret_data, were located by the attacker, suggesting targeted exfiltration.

Exfiltration Activity via Network: Analysis in Wireshark and Splunk revealed multiple SMB2 requests originating from IP 192.168.2.143 to 192.168.2.140 around 2024-08-08 11:24: 49 UTC. Sensitive files, including source_code, HR data, and other proprietary information, were accessed using SMB2 commands. These acts indicate the attack was gathering data for future exfiltration.

- The first POST request occurred at 2024-08-08 11:24:49 UTC, suggesting initial communication with the C2 server to register the compromised host for further activity.
- The largest POST request was detected at 2024-08-08 11:38:54 UTC, targeted /actions/register.php?m=c27w850359 and involved 32,724 bytes of data, indicating significant file exfiltration from the file secret_data.zip located on the admin account.



- frame.time >= "2024-08-08 11:38:00" && frame.time <= "2024-08-08 11:39:00"

No.	Time	Source	Destination	Protocol	Length	Info
6500	2024-08-08 11:38:16.108174	192.168.2.143	192.168.2.140	TCP	60	50323 → 445 [ACK] Seq=206047 Ack=4754256 Win=262400 Len=0
6501	2024-08-08 11:38:16.305643	192.168.2.143	192.168.2.140	SMB2	234	Create Request File: HR
6502	2024-08-08 11:38:16.309078	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6503	2024-08-08 11:38:16.311835	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6504	2024-08-08 11:38:16.316222	192.168.2.143	192.168.2.140	SMB2	146	Close Request
6505	2024-08-08 11:38:16.321758	192.168.2.143	192.168.2.140	SMB2	234	Create Request File: HR
6506	2024-08-08 11:38:16.327724	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6507	2024-08-08 11:38:16.333835	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6508	2024-08-08 11:38:16.340232	192.168.2.143	192.168.2.140	SMB2	146	Close Request
6509	2024-08-08 11:38:16.345729	192.168.2.143	192.168.2.140	SMB2	234	Create Request File: HR
6510	2024-08-08 11:38:16.348832	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6511	2024-08-08 11:38:16.351372	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6512	2024-08-08 11:38:16.353902	192.168.2.143	192.168.2.140	SMB2	146	Close Request
6513	2024-08-08 11:38:16.356763	192.168.2.143	192.168.2.140	SMB2	234	Create Request File: HR
6514	2024-08-08 11:38:16.359883	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6515	2024-08-08 11:38:16.362718	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6516	2024-08-08 11:38:16.367254	192.168.2.143	192.168.2.140	SMB2	156	Find Request SMB2_FIND_BOTH_DIRECTORY_INFO Pattern: *
6517	2024-08-08 11:38:16.374144	192.168.2.143	192.168.2.140	SMB2	234	Create Request File: HR
6518	2024-08-08 11:38:16.377157	192.168.2.143	192.168.2.140	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
6519	2024-08-08 11:38:16.380014	192.168.2.143	192.168.2.140	SMB2	156	Find Request SMB2_FIND_BOTH_DIRECTORY_INFO Pattern: *

- Post and SMB2 protocols showing HR files being read /requested.

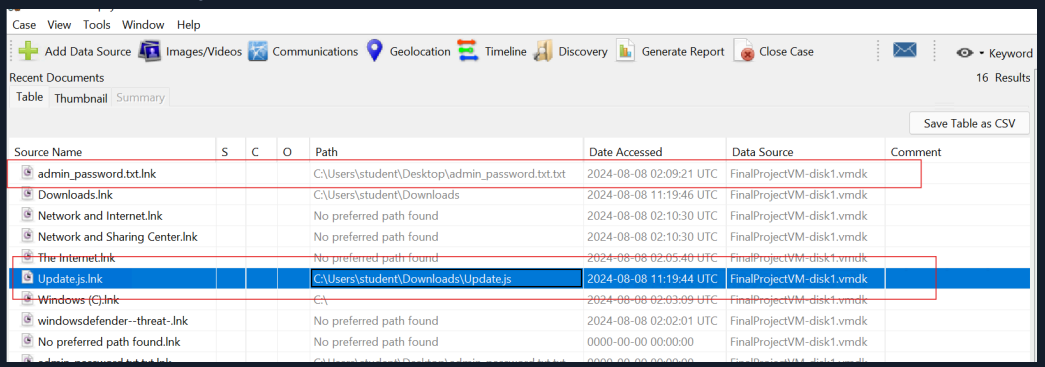
- http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
1243	2024-08-08 11:27:40.758567	192.168.2.143	192.168.2.140	HTTP	1133	POST /actions/register.php?y=26440417 HTTP/1.1
3438	2024-08-08 11:37:09.874526	192.168.2.143	192.168.2.140	HTTP	1162	POST /admin.php?_=39262064 HTTP/1.1
1266	2024-08-08 11:27:40.828214	192.168.2.143	192.168.2.140	HTTP	1163	POST /actions/register.php?z=20285x073 HTTP/1.1
3523	2024-08-08 11:37:10.499121	192.168.2.143	192.168.2.140	HTTP	1171	POST /admin.php?j=498299q10 HTTP/1.1
1280	2024-08-08 11:27:40.857466	192.168.2.143	192.168.2.140	HTTP	1182	POST /rpc.php?j=9919v2751 HTTP/1.1
3465	2024-08-08 11:37:10.305132	192.168.2.143	192.168.2.140	HTTP	1187	POST /rpc.php?z=2j5346486 HTTP/1.1
1726	2024-08-08 11:32:38.206428	192.168.2.143	192.168.2.140	HTTP	1297	POST /upload/index.php?z=33873714 HTTP/1.1
1775	2024-08-08 11:33:07.241626	192.168.2.143	192.168.2.140	HTTP	1297	POST /actions/admin.php?z=6660q4077 HTTP/1.1
3702	2024-08-08 11:38:02.898677	192.168.2.143	192.168.2.140	HTTP	1327	POST /register.php?z=25645561 HTTP/1.1
1624	2024-08-08 11:31:47.688911	192.168.2.143	192.168.2.140	HTTP	1353	POST /register.php?n=93192846 HTTP/1.1
3395	2024-08-08 11:37:00.412331	192.168.2.143	192.168.2.140	HTTP	1379	POST /upload/admin.php?v=70r321382 HTTP/1.1
3339	2024-08-08 11:36:52.658713	192.168.2.143	192.168.2.140	HTTP	1386	POST /upload/admin.php?g=18964599 HTTP/1.1
3579	2024-08-08 11:37:10.937761	192.168.2.143	192.168.2.140	HTTP	1409	POST /register.php?i=n51399941 HTTP/1.1
1223	2024-08-08 11:27:39.523791	192.168.2.143	192.168.2.140	HTTP	1426	POST /actions/rpc.php?_=45p073907 HTTP/1.1
3553	2024-08-08 11:37:10.680368	192.168.2.143	192.168.2.140	HTTP	1956	POST /register.php?j=75te693875 HTTP/1.1
1408	2024-08-08 11:29:14.824312	192.168.2.143	192.168.2.140	HTTP	1962	POST /actions/register.php?z=915j73816 HTTP/1.1
1169	2024-08-08 11:27:33.911136	192.168.2.143	192.168.2.140	HTTP	2323	POST /register.php?b=34843617 HTTP/1.1
1696	2024-08-08 11:32:20.524703	192.168.2.143	192.168.2.140	HTTP	2647	POST /rpc.php?l=151801514 HTTP/1.1
3195	2024-08-08 11:35:54.121869	192.168.2.143	192.168.2.140	HTTP	15461	POST /actions/admin.php?f=ny21502206 HTTP/1.1
6753	2024-08-08 11:38:54.224452	192.168.2.143	192.168.2.140	HTTP	32724	POST /actions/register.php?m=c27w850359 HTTP/1.1

Malware Objective: Credential theft, and proprietary/confidential information theft.

Root cause: The (insider threat) student user attempted to search for a YouTube update on the internet and ended up downloading from a malicious website. The attacker loaded credential harvesting DLLs such as samlib.dll, cryptdll.dll, sechost.dll, and vaultcli.dll to extract sensitive data from memory (as is typical with mimikatz.exe). Additionally, beacon.exe was deployed by the attacker at the beginning of the attack, likely to establish a command and control for remote access and further control of the system.

- Recently accessed files



- Mimikatz.exe timestamp 11:34 UTC

SVCHOST.EXE-D9DA307C.pf	SVCHOST.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:31:54 UTC
SVCHOST.EXE-350EF3E6.pf	SVCHOST.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:33:29 UTC
BACKGROUNDTASKHOST.EXE-CA639011.pf	BACKGROUNDTASKHOST.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:33:30 UTC
CONSENT.EXE-2D674CE4.pf	CONSENT.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:33:34 UTC
CTFMON.EXE-5E6E7DF5.pf	CTFMON.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:33:35 UTC
CONHOST.EXE-F98A1078.pf	CONHOST.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:33:38 UTC
POWERSHELL.EXE-022A1004.pf	POWERSHELL.EXE	/WINDOWS/SYSTEM32/WINDOWSPOWERSHELL/V1.0	2024-08-08 11:33:38 UTC
RUNDLL32.EXE-B7E5FEEB.pf	RUNDLL32.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:33:48 UTC
MIMIKATZ.EXE-A23B41FF.pf	MIMIKATZ.EXE	/USERS/STUDENT/DOWNLOADS	2024-08-08 11:34:03 UTC
TASKMGR.EXE-39AABA37.pf	TASKMGR.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:34:08 UTC
SYSTEMSETTINGSBROKER.EXE-4B88D329.pf	SYSTEMSETTINGSBROKER.EXE	/WINDOWS/SYSTEM32	2024-08-08 11:34:12 UTC

*Recent Web History showing access to malwaredomain.com

Web (6)
WinSxS (18015)
WUModels (8)
nallocated: 262141952-262143999)

ensions (26)
files (1)

ams (226)
tem Information (1)
ents (16)
(598)

tached (6)
ks (1)
)2)
76)
ds (2)

Web History

Table | Thumbnail | Summary

Save

Source Name	S	C	O	URL	Date Accessed	Referrer URL
History				file:///C:/	2024-08-08 02:03:09 UTC	file:///C:/
History				file:///C:/Windows/system32/oobe/FirstLogonAnim.h...	2024-08-08 01:57:59 UTC	file:///C:/Windows/system32/oobe/FirstLog
History			0	https://www.bing.com/search?q=users+and+groups&...	2024-08-08 02:06:37 UTC	https://www.bing.com/search?q=users+and
History			0	https://www.bing.com/search?q=users+and+groups&...	2024-08-08 02:06:41 UTC	https://www.bing.com/search?q=users+and
History			0	https://www.bing.com/search?q=youtube+update&cv...	2024-08-08 11:19:17 UTC	https://www.bing.com/search?q=youtube+u
History			0	https://www.bing.com/search?q=youtube+update&cv...	2024-08-08 11:19:17 UTC	https://www.bing.com/search?q=youtube+
History			0	http://www.malware-domain.com:8000/Update.js	2024-08-08 11:25:47 UTC	http://www.malware-domain.com:8000/Up
History			0	http://www.malware-domain.com:8000/Update.js	2024-08-08 11:25:47 UTC	http://www.malware-domain.com:8000/Up

- Multiple start and stops in powershell indicative of malicious activity.

Windows PowerShell Number of events: 407

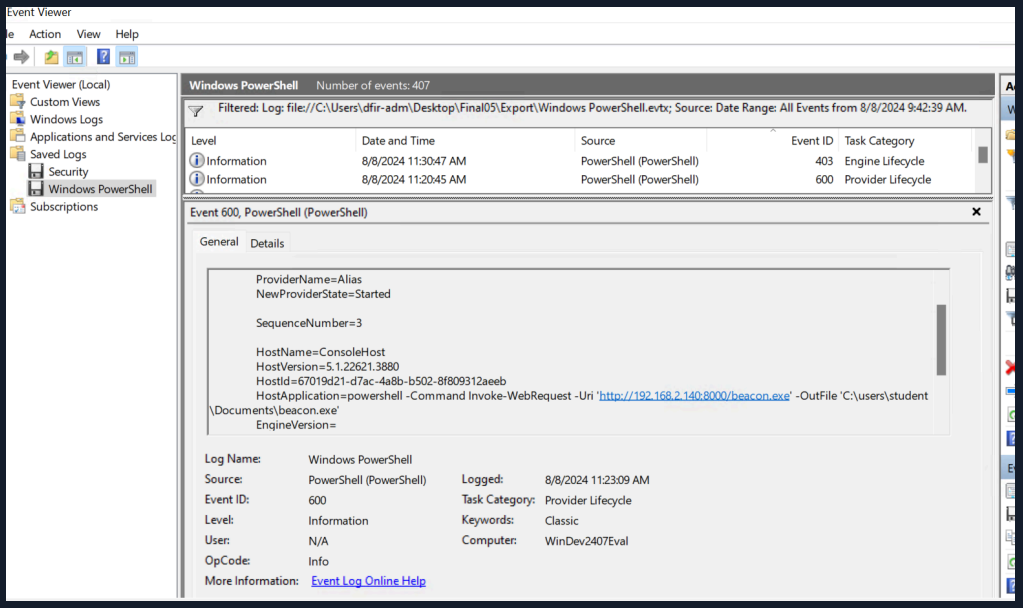
Filtered: Log: file://C:\Users\dfir-adm\Desktop\Final05\Export\Windows PowerShell.evtx; Source: Date Range: From 8/8/2024 1:00:00 AM to 8/8/2024

Level	Date and Time	Source	Event ID	Task Category
Information	8/8/2024 11:23:09 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:23:09 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:23:09 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:23:09 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:23:09 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:23:10 AM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	8/8/2024 11:24:27 AM	PowerShell (PowerShell)	403	Engine Lifecycle
Information	8/8/2024 11:26:31 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:26:31 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:26:31 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:26:31 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:26:31 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:26:31 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	8/8/2024 11:26:32 AM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	8/8/2024 11:30:47 AM	PowerShell (PowerShell)	403	Engine Lifecycle
Information	8/8/2024 11:33:41 AM	PowerShell (PowerShell)	600	Provider Lifecycle

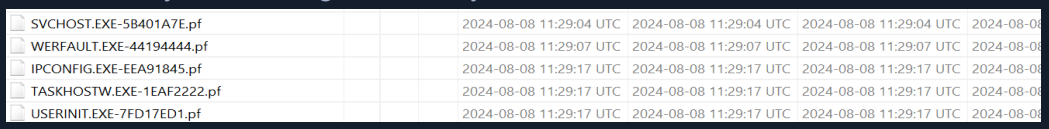
Event 600, PowerShell (PowerShell)

General Details

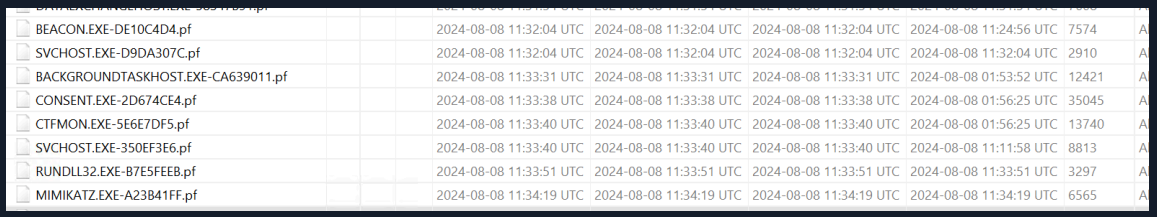
* Powershell beacon indicator



- IPConfig was run indicating the attacker may have been attempting to make lateral movement by discovering the host systems network.



- Beacon and Mimikatz timestamps



Mimikatz in wireshark as well as TCP Zerowindow indicates that too much data is going through so the connection can't keep up. Typically this indicates that the network is delivering traffic faster than the receiver can process it.

Technical Timeline

2024-08-08 11:24:49 UTC The first POST request, detected at 2024-08-08 11:24:49 UTC, targeted /actions/admin.html?h=65175566&wn=v27699923 via HTTP, suggesting initial communication with the C2 server to register the compromised host for further activity

2024-08-08 11:34:19 UTC Mimikatz.exe executed, indicating post-exploitation activity targeting credential harvesting.

2024-08-08 11:35:00 UTC POST requests to http://www.malware-domain.com:8000/Update.js detected, confirming exfiltration of .txt files containing credentials.

2024-08-08 11:38:54 UTC The largest POST request, detected, and involved 32,724 bytes of data, indicating significant file exfiltration potentially including information from secret_data.zip

2024-08-08 13:45 UTC Security Operations Personnel Review Alert.

2024-08-08 14:00 UTC Security Operations Personnel Contain the Machine.

2024-08-08 14:30 UTC Security Operations Personnel take a forensic image and collect volatile memory.

2024-08-08 15:00 UTC Security Operations Personnel request Forensic Analysis.

References:

Detailed mimikatz guide. This step-by-step guide will show you… | by CyberKid | Medium

Troubleshooting Latency by Capturing Traffic

HACKTHEBOX

Real-world Incident Report Template