Reveal Lab
Analyst: Ruslan
Date: 2026-01-25

1) Confirmed Findings

Finding	Value	Why it matters
Malicious process	powershell.exe	PowerShell is commonly used to run commands covertly and fetch/execute subsequent stages
Parent PID (PPID)	4120	The PPID helps reconstruct the execution chain: which process launched the malicious activity
Second-stage file	3435.dll	The second-stage DLL is the payload that defenders typically need to detect and block
Remote directory/share indicator	davwwwroot	Suggests access to a remote resource, often associated with WebDAV structures
User execution context	Elon	Identifies the user context under which activity ran and whose data may be impacted
Malware family	STRELASTEALER	Enables mapping to known threat behavior and selecting appropriate response actions
Execution technique (stage 2)	T1218.011	MITRE ATT&CK: abuse of rundll32.exe to execute a DLL ([MITRE ATT&CK][1])

2) What Happened

1. A suspicious process, powershell.exe, was observed and identified as malicious.
2. Its parent process was identified via PPID = 4120 (the process that launched powershell.exe).
3. PowerShell was linked to execution of a second-stage payload: 3435.dll.
4. Activity included remote resource access indicators referencing davwwwroot.
5. The activity ran under the user context Elon.
6. The overall behavior was attributed to the STRELASTEALER malware family.

3) What This Means

According to publicly available sources, Strela Stealer is described as an infostealer targeting credential theft (including email clients such as Outlook).

Given that execution occurred under user Elon, the primary risk is compromise of Elon’s data and associated services (email, corporate portals, VPN, SSO, etc.).

---

4) Recommended Actions

1. Identify the process name/type for PID 4120 that spawned the malicious powershell.exe (key to the initial vector/trigger).

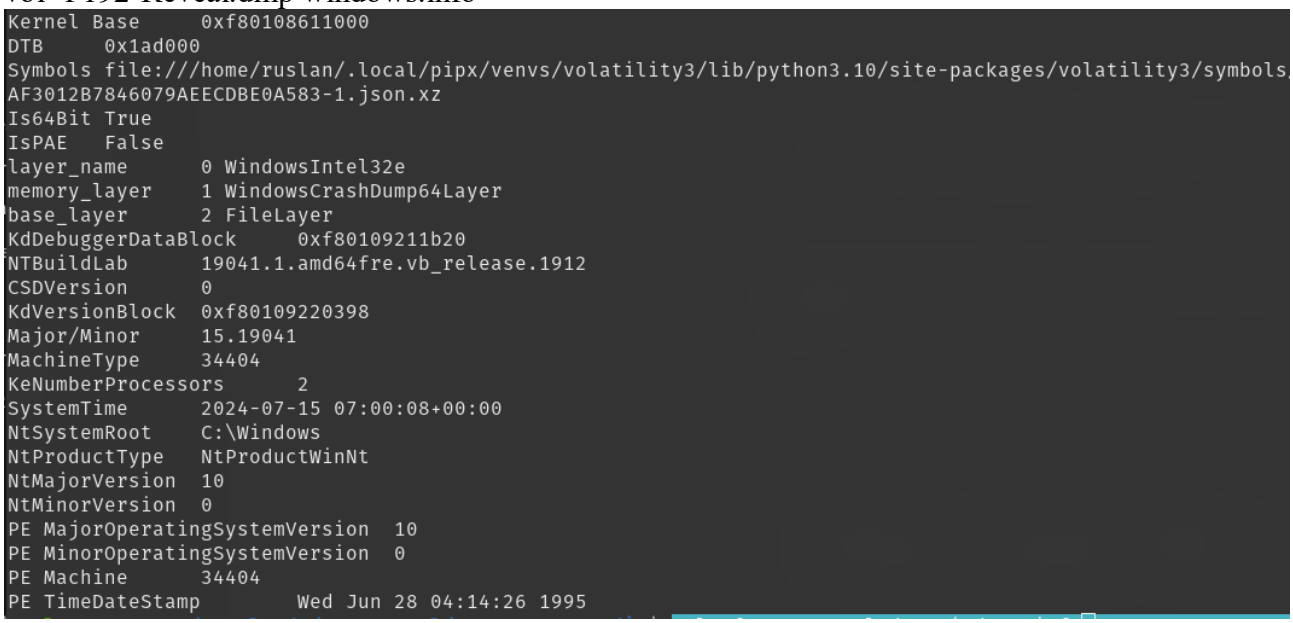
2. Hunt for 3435.dll artifacts and related DLL execution events (including rundll32.exe, technique T1218.011). (MITRE ATT&CK)
3. Secure Elon's accounts immediately: reset passwords/tokens and revoke active sessions, prioritizing email and critical systems.
4. Investigate network/host activity involving davwwwroot (potential WebDAV path) on this host and across the environment.
5. Expand evidence collection to scope the incident: Windows logs, EDR telemetry, and disk imaging (if this is a real incident rather than a lab exercise).

5) Appendix: Commands Used

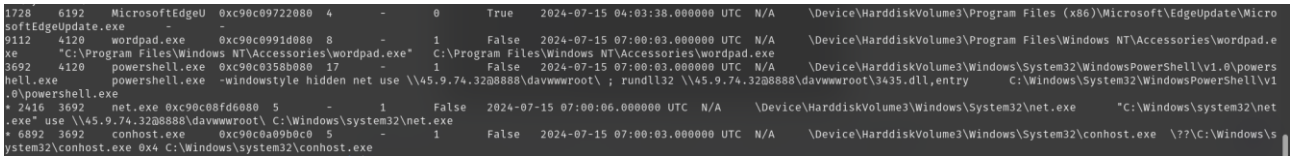
Purpose	Command
Image information	vol -f 192-Reveal.dmp windows.info
Process tree	vol -f 192-Reveal.dmp windows.pstree
Username via sessions	vol -f 192-Reveal.dmp windows.sessions | grep "3692"

1. Identifying the name of the malicious process helps in understanding the nature of the attack. What is the name of the malicious process?

vol -f 192-Reveal.dmp windows.info



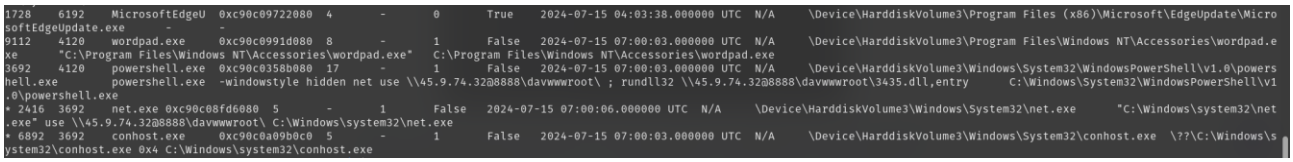
vol -f 192-Reveal.dmp windows.pstree



Answer: powershell.exe

2. Knowing the parent process ID (PPID) of the malicious process aids in tracing the process hierarchy and understanding the attack flow. What is the parent PID of the malicious process?

vol -f 192-Reveal.dmp windows.pstree



Answer: 4120

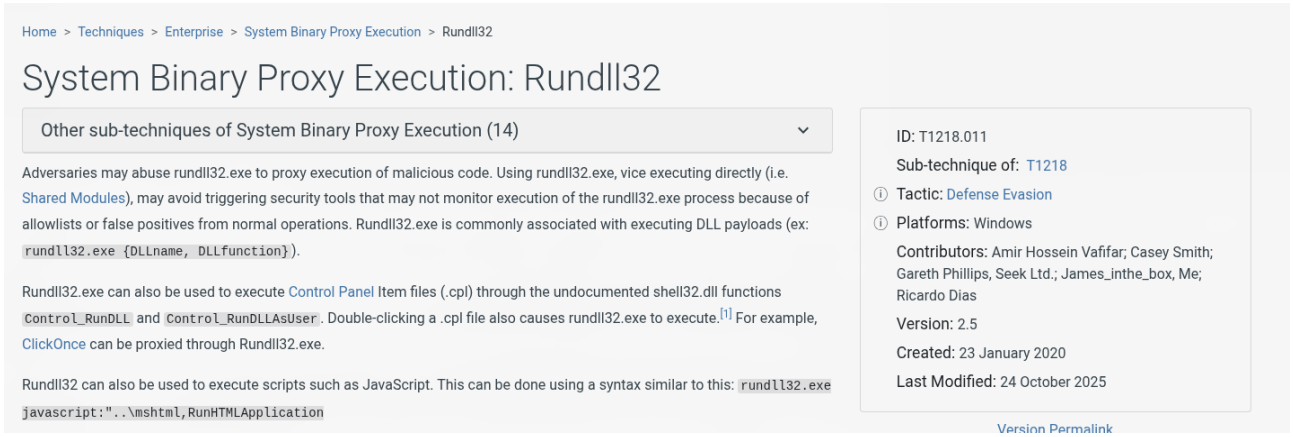
3. Determining the file name used by the malware for executing the second-stage payload is crucial for identifying subsequent malicious activities. What is the file name that the malware uses to execute the second-stage payload?

Answer: 3435.dll

4. Identifying the shared directory on the remote server helps trace the resources targeted by the attacker. What is the name of the shared directory being accessed on the remote server?

Answer: davwwwroot

5. Identifying the username under which the malicious process runs helps in assessing the compromised account and its potential impact. What is the username that the malicious process runs under?



Answer: T1218.011

6. Identifying the username under which the malicious process runs helps in assessing the compromised account and its potential impact. What is the username that the malicious process runs under?

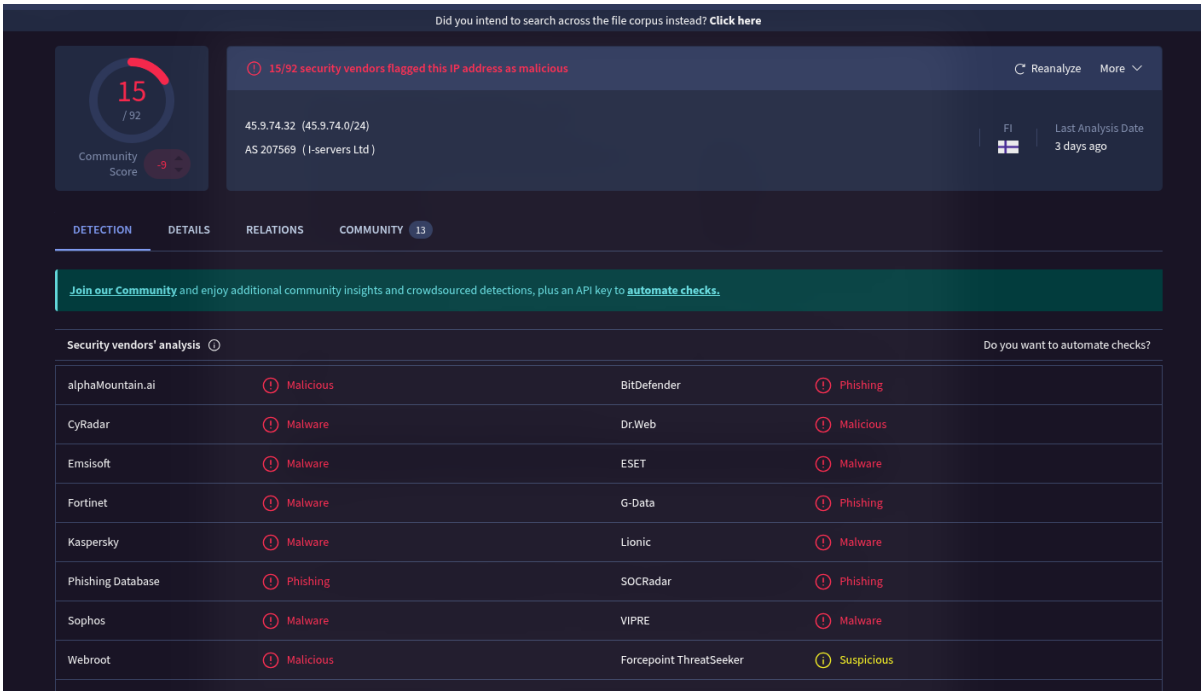
vol -f 192-Reveal.dmp windows.sessions | grep "3692"

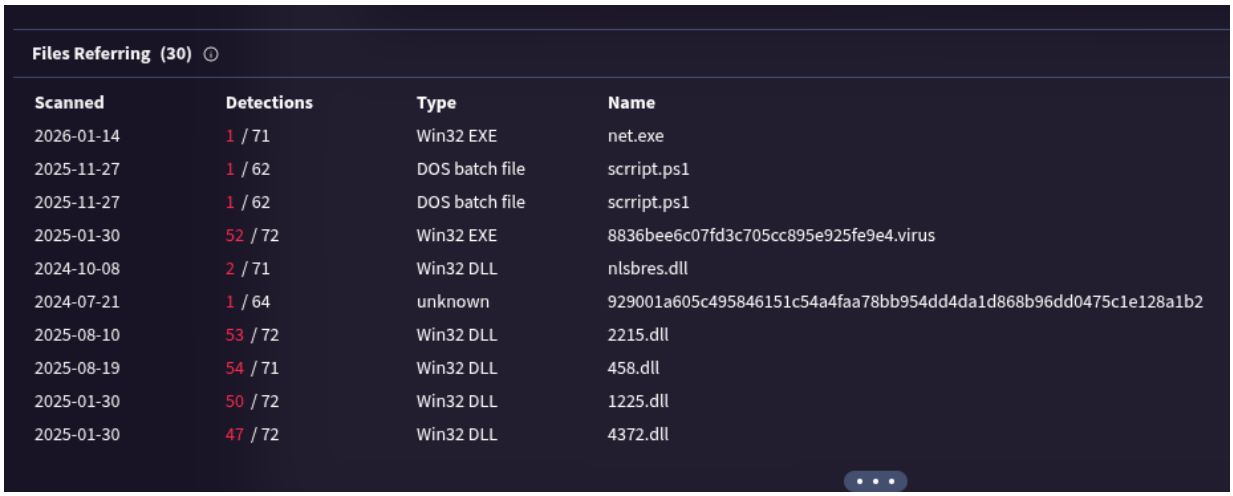
```
ruslan@pop-os:~/Downloads/192-Reveal/temp_extract_dir$ vol -f 192-Reveal.dmp windows.sessions | grep "3692"
1rogress-  100.03692    powershell.exe  DESKTOP-T51LU0E/Elon    2024-07-15 07:00:03.000000 UTC
ruslan@pop-os:~/Downloads/192-Reveal/temp_extract_dir$
```

Answer: Elon

7. Knowing the name of the malware family is essential for correlating the attack with known threats and developing appropriate defenses. What is the name of the malware family?

Answer: STRELASTEALER





Files Referring (30)

Scanned	Detections	Type	Name
2026-01-14	1 / 71	Win32 EXE	net.exe
2025-11-27	1 / 62	DOS batch file	scrript.ps1
2025-11-27	1 / 62	DOS batch file	scrript.ps1
2025-01-30	52 / 72	Win32 EXE	8836bee6c07fd3c705cc895e925fe9e4.virus
2024-10-08	2 / 71	Win32 DLL	nlsbres.dll
2024-07-21	1 / 64	unknown	929001a605c495846151c54a4faa78bb954dd4da1d868b96dd0475c1e128a1b2
2025-08-10	53 / 72	Win32 DLL	2215.dll
2025-08-19	54 / 71	Win32 DLL	458.dll
2025-01-30	50 / 72	Win32 DLL	1225.dll
2025-01-30	47 / 72	Win32 DLL	4372.dll