Analysis Summary

Analysis ID	20250722-D6KJY8
File Name	7ev3n.exe
File Size	322560
MD5	9f8bc96c96d43ecb69f883388d228754
SHA256	7d373ccb96d1dbb1856ef31afa87c2112a0c1795a796ab01cb154700288afec5
Start Time	2025-07-23 04:54:08 WIB
End Time	2025-07-23 04:56:23 WIB
Severity Score	8.4 (High)
Classification	**Malware** (Malware Probability: 100.0%)
Malware Family	Cryptominer

Detected Signatures

No.	Signature	Name	Description
1	wrote_proc_memory	A process wrote data to an area of memory in another process.	Writes directly into memory of another process.
2	executes_dropped_exe	A process was created using a dropped executable.	Executes dropped executable files to initiate payloads.
3	process_other_parent	Created a process with a different parent than the creating process.	Spawns processes with suspicious or uncommon parent process.
4	susevent_adjustprivilegetoken	A privilege for an access token was adjusted. Windows uses the token to control the ability of the user to perform various system-related operations.	Adjusts privilege tokens, often for escalation.
5	loads_driver	A driver was loaded.	Loads kernel-mode drivers, which may indicate privilege escalation.
6	files_drops_exe_user	Drops file in user directory	Drops executables in user directory for execution or persistence.
7	files_drops_exe_general	Drops executable file	Drops general executable files, likely payloads.

8	cmd_schtasks_create	Uses schtasks.exe to create a new scheduled task.	Creates scheduled tasks to ensure persistence or timed execution.
9	registry_write_runkey	Adds run entry to the registry to gain persistence across system reboots.	Uses Run key to gain persistence on reboot.
10	registry_winlogon_persistence	Modifies WinLogon for persistence	Adds persistence using Winlogon registry keys.
11	registry_bypasses_uac	Modifies registry value(s) to disable UAC checks.	Modifies registry to bypass User Account Control.
12	file_drops_windows	Drops file in Windows directory	Drops files in Windows directory for stealth or persistence.

Process Tree

No	Process Name	PID	PPID	Command Line
1	7ev3n.exe	4460	2852	"C:\Users\ADMINI~1\AppData\Local\Temp\7ev3n.exe"
2	system.exe	4860	4460	"C:\Users\Administrator\AppData\Local\system.exe"
3	cmd.exe	4888	4860	C:\Windows\system32\cmd.exe /c C:\Users\Administrator\AppData\Local\del.bat
4	SCHTASKS.exe	4896	4860	C:\Windows\System32\SCHTASKS.exe /create /SC ONLOGON /TN uac /TR "C:\Users\Administrator\AppData\Local\bcd.bat" /RL HIGHEST /f
5	cmd.exe	4972	4860	C:\windows\system32\cmd.exe /c REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Shell" /t REG_SZ /d "C:\Users\Administrator\AppData\Local\system.exe" /f /reg:64
6	cmd.exe	4980	4860	C:\windows\system32\cmd.exe /c REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "System" /t REG_SZ /d "C:\Users\Administrator\AppData\Local\system.exe" /f /reg:64

7	cmd.exe	4988	4860	C:\windows\system32\cmd.exe /c REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout" /v "Scancode Map" /t REG_BINARY /d "00000000000000001700000000003800000038e000005be000005ce00000360000001d0000001de000000f000000010000001c0000003e0000003b000000440000004500000003d0000005de000000000" /f /reg:64
8	cmd.exe	4996	4860	C:\windows\system32\cmd.exe /c REG ADD "HKEY_CURRENT_USER\Control Panel\Accessibility\StickyKeys" /v "Flags" /t REG_SZ /d 506 /f /reg:64
9	cmd.exe	5004	4860	C:\windows\system32\cmd.exe /c REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion" /v "rgd_bcd_condition" /t REG_SZ /d 1 /f /reg:64
10	cmd.exe	5012	4860	C:\windows\system32\cmd.exe /c REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v "EnableLUA" /t REG_DWORD /d 0 /f /reg:64
11	reg.exe	3172	4972	REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Shell" /t REG_SZ /d "C:\Users\Administrator\AppData\Local\system.exe" /f /reg:64
12	reg.exe	3236	4980	REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "System" /t REG_SZ /d "C:\Users\Administrator\AppData\Local\system.exe" /f /reg:64
13	reg.exe	4156	5012	REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v "EnableLUA" /t REG_DWORD /d 0 /f /reg:64
14	reg.exe	4272	4996	REG ADD "HKEY_CURRENT_USER\Control Panel\Accessibility\StickyKeys" /v "Flags" /t REG_SZ /d 506 /f /reg:64
15	reg.exe	968	5004	REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion" /v "rgd_bcd_condition" /t REG_SZ /d 1 /f /reg:64

16	reg.exe	3604	4988	REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout" /v "Scancode Map" /t REG_BINARY /d "00000000000000001700000000038000000038e000005be000005ce00000360000001d0000001de000000f000000010000001c0000003e0000003b000000440000004500000003d000000 05de000000000" /f /reg:64
17	svchost.exe	4796	580	C:\Windows\System32\svchost.exe -k WerSvcGroup
18	WerFault.exe	4360	4860	C:\Windows\SysWOW64\WerFault.exe -u -p 4860 -s 816
19	svchost.exe	2108	580	c:\windows\system32\svchost.exe -k netsvcs -s BITS
20	svchost.exe	4460	580	c:\windows\system32\svchost.exe -k localserviceandnoimpersonation -s SSDPSRV
21	svchost.exe	4956	580	c:\windows\system32\svchost.exe -k netsvcs -s wlidsvc
22	svchost.exe	5032	580	C:\Windows\System32\svchost.exe -k wsappx -s ClipSVC

Detected MITRE TTPs

No.	TTPs	Name	Description
1	T1548.002	Bypass User Account Control	Malware bypassed User Account Control (UAC) to escalate privileges.
2	T1059.003	Windows Command Shell	Malware executed shell commands using the Windows command interpreter (cmd.exe).
3	T1053.005	Scheduled Task	A scheduled task was created or manipulated by the malware to maintain persistence or execute payloads.
4	T1547.004	Winlogon Helper DLL	Malware injected DLLs into the Winlogon process to maintain persistence.
5	T1562.001	Disable or Modify Tools	Security tools were disabled or modified to avoid detection or interruption.

6	T1134.004	Parent PID Spoofing	The malware spoofed the parent process ID to disguise its origin and evade detection.
7	T1112	Modify Registry	Registry keys or values were modified by the malware to hide its presence or achieve persistence.
8	T1547.001	Registry Run Keys / Startup Folder	The malware created or modified registry keys to ensure execution at startup.

Observed DNS Queries

No	Domain IP	Domain	Description
1	8.8.8.8	blockchain.info	Public blockchain domain; may indicate crypto-related activity.
2	8.8.8.8	settings-win.data.microsoft.com	Used by Windows for telemetry and settings sync.
3	8.8.8.8	insiderppe.cloudapp.net	Commonly used by Microsoft Azure services and virtual machines.
4	8.8.8.8	sls.update.microsoft.com	Used by Windows Update service to check for and download updates.
5	8.8.4.4	blockchain.info	Public blockchain domain; may indicate crypto-related activity.
6	8.8.4.4	settings-win.data.microsoft.com	Used by Windows for telemetry and settings sync.
7	8.8.4.4	insiderppe.cloudapp.net	Commonly used by Microsoft Azure services and virtual machines.
8	8.8.4.4	sls.update.microsoft.com	Used by Windows Update service to check for and download updates.
9	8.8.8.8	ieonlinews.microsoft.com	General Microsoft domain, commonly used by Windows components.

10	8.8.4.4	ieonlinews.microsoft.com	General Microsoft domain, commonly used by Windows components.
11	8.8.8.8	dns.msftncsi.com	Unrecognized domain queried by the malware during execution.
12	8.8.4.4	dns.msftncsi.com	Unrecognized domain queried by the malware during execution.
13	8.8.8.8	jaster.in	Unrecognized domain queried by the malware during execution.
14	8.8.4.4	jaster.in	Unrecognized domain queried by the malware during execution.
15	8.8.4.4	www.msftconnecttest.com	Unrecognized domain queried by the malware during execution.
16	8.8.8.8	www.msftconnecttest.com	Unrecognized domain queried by the malware during execution.
17	8.8.4.4	ctldl.windowsupdate.com	Unrecognized domain queried by the malware during execution.
18	8.8.8.8	ctldl.windowsupdate.com	Unrecognized domain queried by the malware during execution.

Observed UDP Traffic

No	Source IP	Destination IP	Port	Description
1	192.168.30.11	192.168.30.255	137	Local broadcast/multicast traffic for device or name discovery.
2	192.168.30.11	192.168.30.255	138	Local broadcast/multicast traffic for device or name discovery.
3	192.168.30.11	8.8.8.8	53	DNS query over UDP — used to resolve domain names.
4	192.168.30.11	8.8.4.4	53	DNS query over UDP — used to resolve domain names.
5	192.168.30.11	239.255.255.250	1900	Local broadcast/multicast traffic for device or name discovery.

Summary

The malware sample initiated a total of 22 processes, suggesting moderate to high system interaction. A total of 12 behavioral signatures were triggered, indicating potential malicious actions across different categories. 8 MITRE ATT&CK; techniques were identified, covering tactics such as Bypass User Account Control, Disable or Modify Tools, Modify Registry and possibly more. All DNS queries were directed toward known and trusted domains, reducing the likelihood of C2 involvement. The network layer showed 132 UDP traffic entries, including multicast/broadcast, NetBIOS name service, DNS over UDP. Persistence techniques were observed, such as registry modifications or scheduled tasks. The presence of 'schtasks' implies that the malware schedules tasks for execution at logon.

Glossary of Terms

Term	Definition
Malware	Malicious software designed to harm, exploit, or disrupt systems or data.
Benign	A file or program that does not show harmful or suspicious behavior.
Malware Family	A group of malware that share similar behavior, structure, or purpose.
Probability	A measure of how confident the system is about its classification result (as Malware or Benign).
Signature	A rule or indicator that identifies a specific malicious behavior or pattern during execution.
Process	An instance of a running program or executable observed during the malware's behavior.
Process Tree	A hierarchical structure showing parent-child relationships of running processes.
Command Line	The arguments used when executing a program, often providing insight into its behavior.
DNS Query	A request made to resolve a domain name into an IP address, revealing possible C2 activity.
UDP Traffic	Unreliable and connectionless communication used by malware for broadcasting or stealthy data transfer.
Multicast/Broadcast	Network messages sent to multiple recipients, sometimes used for discovery or evasion.
MITRE ATT&CK;	A framework describing tactics and techniques used by threat actors, mapped from observed behavior.

TTP (Tactics, Techniques, Procedures)	Specific adversary behaviors observed during execution and mapped to MITRE IDs.
CVSS Score	Common Vulnerability Scoring System — a numerical value estimating the severity of a vulnerability or attack.
Severity Level	The corresponding threat level based on the CVSS score (e.g., Low, Medium, Critical).
Persistence Mechanism	A method used by malware to maintain access, such as scheduled tasks or registry keys.
Registry Modification	Changes made to the Windows registry, often to evade detection or maintain persistence.

Note: The CVSS score does not represent the overall danger of the malware, but rather the severity of the behavior observed.

Glosarium Istilah

Istilah	Definisi
Malware	Perangkat lunak jahat yang dirancang untuk merusak, mengeksploitasi, atau mengganggu sistem atau data.
Benign	File atau program yang tidak menunjukkan perilaku berbahaya atau mencurigakan.
Malware Family	Kelompok malware dengan perilaku, struktur, atau tujuan yang serupa.
Probabilitas	Tingkat keyakinan sistem terhadap hasil klasifikasinya (misalnya sebagai Malware atau Benign).
Signature	Aturan atau indikator yang mendeteksi pola perilaku jahat tertentu saat eksekusi.
Process	Proses program yang sedang berjalan yang diamati selama perilaku malware dianalisis.
Process Tree	Struktur hierarki yang menunjukkan hubungan induk-anak antar proses selama eksekusi.
Command Line	Argumen perintah saat menjalankan program, yang dapat mengungkapkan tujuannya.
DNS Query	Permintaan untuk menerjemahkan nama domain menjadi alamat IP, bisa menunjukkan komunikasi C2.
UDP Traffic	Komunikasi jaringan yang tidak memiliki koneksi tetap, sering digunakan untuk siaran atau komunikasi rahasia.

Multicast/Broadcast	Pengiriman pesan jaringan ke banyak penerima, kadang digunakan untuk eksplorasi atau pengelabuan.
MITRE ATT&CK;	Kerangka kerja yang mendeskripsikan taktik dan teknik penyerang berdasarkan perilaku yang teramati.
TTP (Taktik, Teknik, Prosedur)	Perilaku khas penyerang yang dipetakan dari aktivitas malware dan dikaitkan ke MITRE.
CVSS Score	Nilai standar untuk mengukur tingkat keparahan kerentanan atau serangan tertentu.
Severity Level	Level keparahan risiko berdasarkan skor CVSS (mis. Rendah, Sedang, Kritis).
Persistence Mechanism	Metode yang digunakan malware untuk bertahan hidup seperti task terjadwal atau pengubahan registry.
Registry Modification	Perubahan pada sistem registry Windows untuk menghindari deteksi atau menanamkan persistensi.

Catatan: Skor CVSS tidak menunjukkan tingkat bahaya total dari malware, melainkan tingkat keparahan dari perilaku yang terdeteksi.