Malware Analysis Report

Created on: 2025-07-19

Analysis Summary

Analysis ID	20250719-ND2H8V
File Name	7ev3n.exe
File Size	322560
MD5	9f8bc96c96d43ecb69f883388d228754
SHA256	7d373ccb96d1dbb1856ef31afa87c2112a0c1795a796ab01cb154700288afec5
Start Time	2025-07-19 18:30:35 WIB
End Time	2025-07-19 18:32:50 WIB
Severity Score	8.8 (High)
Classification	**Malware** (Malware Probability: 80.0%)
Malware Family	Rat

Detected Signatures

No.	Signature Name	Description
1	wrote_proc_memory	A process wrote data to an area of memory in another process.
2	executes_dropped_exe	A process was created using a dropped executable.
3	process_other_parent	Created a process with a different parent than the creating 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.
5	files_drops_exe_user	Drops file in user directory
6	files_drops_exe_general	Drops executable file
7	cmd_schtasks_create	Uses schtasks.exe to create a new scheduled task.
8	registry_winlogon_persistence	Modifies WinLogon for persistence
9	registry_bypasses_uac	Modifies registry value(s) to disable UAC checks.
10	registry_write_runkey	Adds run entry to the registry to gain persistence across system reboots.
11	file_drops_windows	Drops file in Windows directory

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.
Probabability	A measure of how certain the system is about its classification result.
CVSS Score	A standardized score that estimates the severity of a vulnerability or attack.
Severity Level	The level of risk posed, based on the CVSS score.
Signature	A known pattern of malicious activity detected in a file or process.
Process	A running instance of a program or executable during analysis.
Timestamp	The date and time a specific event occurred, shown in local timezone.

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.
Probabability	Tingkat keyakinan sistem terhadap hasil klasifikasinya.
CVSS Score	Skor baku yang mengukur tingkat keparahan kerentanan atau serangan.
Severity Level	Tingkat risiko berdasarkan skor CVSS.
Signature	Pola aktivitas berbahaya yang dikenali dalam sebuah file atau proses.

Process	Proses yang sedang berjalan dari program selama analisis.
Timestamp	Tanggal dan waktu suatu peristiwa terjadi, ditampilkan dalam zona waktu lokal.

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