Analisys Summary

Analysis ID	20250707-O6JS6A
File Name	7ev3n.exe
File Size	322560
MD5	9f8bc96c96d43ecb69f883388d228754
SHA256	7d373ccb96d1dbb1856ef31afa87c2112a0c1795a796ab01cb154700288afec5
Start Time	2025-07-07 15:11:54 WIB
End Time	2025-07-07 15:14:07 WIB
Severity Score	9.0 (Critical)
Classification	**Malware** (Confidence: 100.0%)
Malware Family	Ransomware

Detected Sigantures

No.	Siganture 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_write_runkey	Adds run entry to the registry to gain persistence across system reboots.
10	registry_bypasses_uac	Modifies registry value(s) to disable UAC checks.
11	file_drops_windows	Drops file in Windows directory