Analisys Summary

Analysis ID	20250707-X8H1NU
File Name	WannaCry.exe
File Size	229376
MD5	5c7fb0927db37372da25f270708103a2
SHA256	be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
Start Time	2025-07-07 15:50:15 WIB
End Time	2025-07-07 15:52:33 WIB
Severity Score	9.0 (Critical)
Classification	**Malware** (Confidence: 100.0%)
Malware Family	Coinminer

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	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.
4	files_drops_exe_user	Drops file in user directory
5	registry_write_runkey	Adds run entry to the registry to gain persistence across system reboots.
6	files_drops_exe_general	Drops executable file
7	files_creates_shortcut	Creates a shortcut link
8	cmd_taskkill_process	Kills process with taskkill.exe
9	file_drops_startup	Drops startup file
10	registry_writes_large_value	Creates or modifies a registry key with a large amount of byte data, possibly to store a binary or configuration.
11	registry_changes_wallpaper	Modifies registry value to change active wallpaper.

12	deletes_shadow_copies	Ransomware often targets backup files to inhibit system recovery.
13	file_drops_windows	Drops file in Windows directory