Analysis Summary

Analysis ID	20250710-UWMBK4
File Name	AgentTesla.exe
File Size	2932642
MD5	cce284cab135d9c0a2a64a7caec09107
SHA256	18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9
Start Time	2025-07-10 19:30:41 WIB
End Time	2025-07-10 19:32:55 WIB
Severity Score	7.3 (High)
Classification	**Benign** (Confidence: 20.0%)
Malware Family	-

Detected Signatures

No.	Signature Name	Description
1	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.
2	files_drops_exe_user	Drops file in user directory
3	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.
Confidence	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.
Confidence	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.