ZeroT, Software S0230 | MITRE ATT&CK®

Archived: 2026-04-05 12:41:57 UTC

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Many ZeroT samples can perform UAC bypass by using eventvwr.exe to execute a malicious file.[2]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	ZeroT has used HTTP for C2.[1][2]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	ZeroT can add a new service to ensure PlugX persists on the system when delivered as another payload onto the system.[2]
Enterprise	T1001	.002	Data Obfuscation: Steganography	ZeroT has retrieved stage 2 payloads as Bitmap images that use Least Significant Bit (LSB) steganography.[1][2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	ZeroT shellcode decrypts and decompresses its RC4-encrypted payload.[2]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	ZeroT has used RC4 to encrypt C2 traffic.[1][2]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	ZeroT has used DLL side-loading to load malicious payloads.[1][2]
Enterprise	T1105		Ingress Tool Transfer	ZeroT can download additional payloads onto the victim.[2]

Domain	ID		Name	Use
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Some ZeroT DLL files have been packed with UPX.[2]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	ZeroT has encrypted its payload with RC4.[2]
		.016	Obfuscated Files or Information: Junk Code Insertion	ZeroT has obfuscated DLLs and functions using dummy API calls inserted between real instructions.[2]
Enterprise	T1082		System Information Discovery	ZeroT gathers the victim's computer name, Windows version, and system language, and then sends it to its C2 server.[2]
Enterprise	T1016		System Network Configuration Discovery	ZeroT gathers the victim's IP address and domain information, and then sends it to its C2 server.[2]
