Embargo, Software S1247 | MITRE ATT&CK®

Archived: 2026-04-05 14:41:01 UTC

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Embargo has modified the Windows Registry to start a custom service named irnagentd in Safe Mode.[2]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Embargo has utilized a BAT script to disable security solutions.[2]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Embargo has created persistence through the DLL variant of the MDeployer toolkit by creating a service called irnagentd that launches after the system is rebooted in Safe Mode.[2]

Enterprise T1486 Data Encrypted for Impact

Embargo has the ability to encrypt files with the ChaCha20 and Curve25519 cryptographic algorithms.[1] Embargo also has the ability to encrypt system data and add a random six-letter extension consisting of hexadecimal characters such as ".b58eeb" or ".3d828a" to encrypted files.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Embargo has utilized MDeployer to decrypt two payloads that contain MS4Killer toolkit b.cache and the Embargo ransomware executable a.cache with a hardcoded RC4 key `wlQYLoPCil3niI7x8CvR9EtNtL/aeaHrZ23LP3fAsJogVTIzdnZ5Pi09ZVeHFkiB`.[2]

Enterprise T1480 .002 Execution Guardrails: Mutual Exclusion

Embargo has utilized a hardcoded mutex name of "LoadUpOnGunsBringYourFriends" using the `CreateMutexW()` function.[1] Embargo has also utilized a hardcoded mutex name of "IntoTheFloodAgainSameOldTrip."[2]

Enterprise T1068 Exploitation for Privilege Escalation

Embargo has leveraged MS4Killer to deliver a vulnerable driver to the victim device, sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).[2] Embargo has utilized the vulnerable driver probmon.sys version 3.0.0.4 which had a revoked certificated from "ITM System Co.,LTD."[2]

Enterprise T1083 File and Directory Discovery

Embargo has searched for folders, subfolders and other networked or mounted drives for follow on encryption actions.[1] Embargo has also iterated device volumes using `FindFirstVolumeW()` and `FindNextVolumeW()`

functions and then calls the `GetVolumePathNamesForVolumeNameW()` function to retrieve a list of drive letters and mounted folder paths for each specified volume.[1]

Enterprise T1657 Financial Theft

Embargo has been leveraged in double-extortion ransomware, exfiltrating files then encrypting them, to prompt victims to pay a ransom.[1][2]

Enterprise T1562 .009 Impair Defenses: Safe Mode Boot

Embargo has used a DLL variant of MDeployer to disable security solutions through Safe Mode.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Embargo has leveraged MDeployer to terminate the MS4Killer process, delete the decrypted payload files and a driver file dropped by MS4killer, and reboot the system.[2]

Enterprise T1490 Inhibit System Recovery

Embargo has cleared files from the recycle bin by invoking `SHEmptyRecycleBinW()` and disabled Windows recovery through `C:\Windows\System32\cmd.exe /q /c bcdedit /set {default} recoveryenabled no` .[1]

Enterprise T1112 Modify Registry

Embargo has modified and deleted Registry keys to add services, and to disable Security Solutions such as Windows Defender.[2]

Enterprise T1106 Native API

Embargo has leveraged Windows Native API functions to execute its operations.[1]

Enterprise T1135 Network Share Discovery

Embargo has searched for folders, subfolders and other networked or mounted drives for follow-on encryption actions.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Embargo has encrypted both MDeployer and MS4 Killer payloads with RC4.[2]

Enterprise T1057 Process Discovery

Embargo has utilized MS4Killer to detect running processes on the victim device.[2] Embargo has also captured a snapshot of active running processes using the Windows API `CreateToolHelp32Snapshot()` .[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Embargo has obtained persistence of the loader MDeployer by creating a scheduled task named "Perf_sys."[2]

Enterprise T1679 Selective Exclusion

Embargo has avoided encrypting specific files and directories by leveraging a regular expression within the ransomware binary.[1]

Enterprise T1489 Service Stop

Embargo has terminated active processes and services based on a hardcoded list using the `CloseServiceHandle()` function.[1] Embargo has also leveraged MS4Killer to terminate processes contained in an embedded list of security software process names that were XOR-encrypted.[2]

Enterprise T1007 System Service Discovery

Embargo has obtained active services running on the victim's system through the functions `OpenSCManagerW()` and `EnumServicesStatusExW()`.[1]

Enterprise T1569 .002 System Services: Service Execution

Embargo has created a service named irnagentd that executed the MDeployer loader after the system is rebooted in Safe Mode.[2]
