WastedLocker, Software S0612 | MITRE ATT&CK®

Archived: 2026-04-05 16:21:52 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

WastedLocker can perform a UAC bypass if it is not executed with administrator rights or if the infected host runs Windows Vista or later.[2]

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

WastedLocker has used cmd to execute commands on the system.[2]

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

WastedLocker created and established a service that runs until the encryption process is complete.[2]

Enterprise T1486 Data Encrypted for Impact

WastedLocker can encrypt data and leave a ransom note.[1][2][3]

Enterprise T1140 Deobfuscate/Decode Files or Information

WastedLocker's custom cryptor, CryptOne, used an XOR based algorithm to decrypt the payload.[2]

Enterprise T1083 File and Directory Discovery

WastedLocker can enumerate files and directories just prior to encryption.[2]

Enterprise T1222 .001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification

WastedLocker has a command to take ownership of a file and reset the ACL permissions using the `takeown.exe /F filepath` command.[2]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

WastedLocker has copied a random file from the Windows System32 folder to the `%APPDATA%` location under a different hidden filename.[2]

.004 Hide Artifacts: NTFS File Attributes

WastedLocker has the ability to save and execute files as an alternate data stream (ADS).[3]

Enterprise T1574 .001 Hijack Execution Flow: DLL

WastedLocker has performed DLL hijacking before execution.[2]

Enterprise T1490 Inhibit System Recovery

WastedLocker can delete shadow volumes.[1][2][3]

Enterprise T1112 Modify Registry

WastedLocker can modify registry values within the `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap` registry key.[2]

Enterprise T1106 Native API

WastedLocker's custom crypter, CryptOne, leveraged the VirtualAlloc() API function to help execute the payload. [2]

Enterprise T1135 Network Share Discovery

WastedLocker can identify network adjacent and accessible drives.[3]

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

The WastedLocker payload includes encrypted strings stored within the .bss section of the binary file.[2]

.016 Obfuscated Files or Information: Junk Code Insertion

WastedLocker contains junk code to increase its entropy and hide the actual code.[2]

Enterprise T1120 Peripheral Device Discovery

WastedLocker can enumerate removable drives prior to the encryption process.[3]

Enterprise T1012 Query Registry

WastedLocker checks for specific registry keys related to the `UCOMIEnumConnections` and `IActiveScriptParseProcedure32` interfaces.[2]

Enterprise T1569 .002 System Services: Service Execution

WastedLocker can execute itself as a service.[2]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

WastedLocker checked if UCOMIEnumConnections and IActiveScriptParseProcedure32 Registry keys were detected as part of its anti-analysis technique.[2]
