Winnti for Windows, Software S0141

Archived: 2026-04-05 14:19:25 UTC

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

Winnti for Windows can use a variant of the sysprep UAC bypass.[3]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Winnti for Windows has the ability to use encapsulated HTTP/S in C2 communications.[3]

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

Winnti for Windows can add a service named `wind0ws` to the Registry to achieve persistence after reboot.[3]

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

Winnti for Windows sets its DLL file as a new service in the Registry to establish persistence.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

The Winnti for Windows dropper can decrypt and decompresses a data blob.[3]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Winnti for Windows can XOR encrypt C2 traffic.[3]

Enterprise T1480 .001 Execution Guardrails: Environmental Keying

The Winnti for Windows dropper component can verify the existence of a single command line parameter and either terminate if it is not found or later use it as a decryption key.[3]

Enterprise T1083 File and Directory Discovery

Winnti for Windows can check for the presence of specific files prior to moving to the next phase of execution.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

Winnti for Windows can delete the DLLs for its various components from a compromised host.[3]

.006 Indicator Removal: Timestomp

Winnti for Windows can set the timestamps for its worker and service components to match that of cmd.exe.[3]

Enterprise T1105 Ingress Tool Transfer

The Winnti for Windows dropper can place malicious payloads on targeted systems.[3]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

A Winnti for Windows implant file was named ASPNET_FILTER.DLL, mimicking the legitimate ASP.NET ISAPI filter DLL with the same name.[2]

Enterprise T1106 Native API

Winnti for Windows can use Native API to create a new process and to start services.[3]

Enterprise T1095 Non-Application Layer Protocol

Winnti for Windows can communicate using custom TCP.[3]

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

Winnti for Windows has the ability to encrypt and compress its payload.[3]

.015 Obfuscated Files or Information: Compression

Winnti for Windows has the ability to encrypt and compress its payload.[3]

Enterprise T1057 Process Discovery

Winnti for Windows can check if the explorer.exe process is responsible for calling its install function.[3]

Enterprise T1090 .001 Proxy: Internal Proxy

The Winnti for Windows HTTP/S C2 mode can make use of a local proxy.[3]

.002 Proxy: External Proxy

The Winnti for Windows HTTP/S C2 mode can make use of an external proxy.[3]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

The Winnti for Windows installer loads a DLL using rundll32.[2][3]

Enterprise T1082 System Information Discovery

Winnti for Windows can determine if the OS on a compromised host is newer than Windows XP.[3]

Enterprise T1569 .002 System Services: Service Execution

Winnti for Windows can run as a service using svchost.exe.[3]
