Ninja, Software S1100 | MITRE ATT&CK®

Archived: 2026-04-05 14:33:46 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Ninja can use HTTP for C2 communications.[1]

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

Ninja can create the services `httpsvc` and `w3esvc` for persistence .[1]

Enterprise T1132 .002 Data Encoding: Non-Standard Encoding

Ninja can encode C2 communications with a base64 algorithm using a custom alphabet.[1]

Enterprise T1001 Data Obfuscation

Ninja has the ability to modify headers and URL paths to hide malicious traffic in HTTP requests.[1]

.003 Protocol or Service Impersonation

Ninja has the ability to mimic legitimate services with customized HTTP URL paths and headers to hide malicious traffic.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

The Ninja loader component can decrypt and decompress the payload.[1][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Ninja can XOR and AES encrypt C2 messages.[1]

Enterprise T1480 .001 Execution Guardrails: Environmental Keying

Ninja can store its final payload in the Registry under `$HKLM\SOFTWARE\Classes\Interface\` encrypted with a dynamically generated key based on the drive's serial number.[1]

Enterprise T1083 File and Directory Discovery

Ninja has the ability to enumerate directory content.[1][2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Ninja loaders can be side-loaded with legitimate and signed executables including the VLC.exe media player.[2]

Enterprise T1070 .006 Indicator Removal: Timestomp

Ninja can change or create the last access or write times.[1]

Enterprise T1559 Inter-Process Communication

Ninja can use pipes to redirect the standard input and the standard output.[1]

Enterprise T1680 Local Storage Discovery

Ninja can obtain information on physical drives from targeted hosts.[1][2]

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

Ninja has used legitimate looking filenames for its loader including update.dll and x64.dll.[2]

Enterprise T1106 Native API

The Ninja loader can call Windows APIs for discovery, process injection, and payload decryption.[1][2]

Enterprise T1095 Non-Application Layer Protocol

Ninja can forward TCP packets between the C2 and a remote host.[1][2]

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

The Ninja payload is XOR encrypted and compressed.[2] Ninja has also XORed its configuration data with a constant value of `0xAA`.[1][2]

.015 Obfuscated Files or Information: Compression

Ninja has compressed its data with the LZSS algorithm.[1][2]

Enterprise T1566 .003 Phishing: Spearphishing via Service

Ninja has been distributed to victims via the messaging app Telegram.[1]

Enterprise T1057 Process Discovery

Ninja can enumerate processes on a targeted host.[1][2]

Enterprise T1055 Process Injection

Ninja has the ability to inject an agent module into a new process and arbitrary shellcode into running processes.[1][2]

Enterprise T1090 .001 Proxy: Internal Proxy

Ninja can proxy C2 communications including to and from internal agents without internet connectivity.[1][2]

.003 Proxy: Multi-hop Proxy

Ninja has the ability to use a proxy chain with up to 255 hops when using TCP.[1]

Enterprise T1029 Scheduled Transfer

Ninja can configure its agent to work only in specific time frames.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Ninja loader components can be executed through rundll32.exe.[2]

Enterprise T1082 System Information Discovery

Ninja can obtain the computer name and information on the OS from targeted hosts.[1][2]

Enterprise T1016 System Network Configuration Discovery

Ninja can enumerate the IP address on compromised systems.[1]

Enterprise T1204 .002 User Execution: Malicious File

Ninja has gained execution through victims opening malicious executable files embedded in zip archives.[1]

Source: https://attack.mitre.org/software/S1100