KONNI, Software S0356 | MITRE ATT&CK®

Archived: 2026-04-05 14:09:28 UTC

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

KONNI has bypassed UAC by performing token impersonation as well as an RPC-based method, this included bypassing UAC set to "AlwaysNotify".[4][5]

Enterprise T1134 .002 Access Token Manipulation: Create Process with Token

KONNI has duplicated the token of a high integrity process to spawn an instance of cmd.exe under an impersonated user.[4][5]

.004 Access Token Manipulation: Parent PID Spoofing

KONNI has used parent PID spoofing to spawn a new `cmd` process using `CreateProcessW` and a handle to `Taskmgr.exe`.[5]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

KONNI has used HTTP POST for C2.[1][5]

Enterprise T1560 Archive Collected Data

KONNI has encrypted data and files prior to exfiltration.[5]

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

A version of KONNI has dropped a Windows shortcut into the Startup folder to establish persistence.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

A version of KONNI drops a Windows shortcut on the victim’s machine to establish persistence.[1]

Enterprise T1115 Clipboard Data

KONNI had a feature to steal data from the clipboard.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

KONNI used PowerShell to download and execute a specific 64-bit version of the malware.[1][5]

.003 Command and Scripting Interpreter: Windows Command Shell

KONNI has used cmd.exe to execute arbitrary commands on the infected host across different stages of the infection chain.[1][4][5]

.007 Command and Scripting Interpreter: JavaScript

KONNI has executed malicious JavaScript code.[5]

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

KONNI has registered itself as a service using its export function.[5]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

KONNI can steal profiles (containing credential information) from Firefox, Chrome, and Opera.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

KONNI has used a custom base64 key to encode stolen data before exfiltration.[4]

Enterprise T1005 Data from Local System

KONNI has stored collected information and discovered processes in a tmp file.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

KONNI has used certutil to download and decode base64 encoded strings and has also devoted a custom section to performing all the components of the deobfuscation process.[4][5]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

KONNI has used AES to encrypt C2 traffic.[6]

Enterprise T1546 .015 Event Triggered Execution: Component Object Model Hijacking

KONNI has modified ComSysApp service to load the malicious DLL payload.[4]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

KONNI has used FTP to exfiltrate reconnaissance data out.[4]

Enterprise T1041 Exfiltration Over C2 Channel

KONNI has sent data and files to its C2 server.[1][5][6]

Enterprise T1083 File and Directory Discovery

A version of KONNI searches for filenames created with a previous version of the malware, suggesting different versions targeted the same victims and the versions may work together.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

KONNI can delete files.[1]

Enterprise T1105 Ingress Tool Transfer

KONNI can download files and execute them on the victim’s machine.[1][5]

Enterprise T1056 .001 Input Capture: Keylogging

KONNI has the capability to perform keylogging.[1]

Enterprise T1680 Local Storage Discovery

KONNI can gather information on connected drives and disk space from the victim’s machine.[1][4][5]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

KONNI has pretended to be the xmlProv Network Provisioning service.[5]

.005 Masquerading: Match Legitimate Resource Name or Location

KONNI has created a shortcut called "Anti virus service.lnk" in an apparent attempt to masquerade as a legitimate file.[1]

Enterprise T1112 Modify Registry

KONNI has modified registry keys of ComSysApp, Svchost, and xmlProv on the machine to gain persistence.[4][5]

Enterprise T1106 Native API

KONNI has hardcoded API calls within its functions to use on the victim's machine.[5]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

KONNI has been packed for obfuscation.[6]

.013 Obfuscated Files or Information: Encrypted/Encoded File

KONNI is heavily obfuscated and includes encrypted configuration files.[5]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

KONNI has been delivered via spearphishing campaigns through a malicious Word document.[5]

Enterprise T1057 Process Discovery

KONNI has used the command `cmd /c tasklist` to get a snapshot of the current processes on the target machine.[4][5]

Enterprise T1113 Screen Capture

KONNI can take screenshots of the victim’s machine.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

KONNI has used Rundll32 to execute its loader for privilege escalation purposes.[4][5]

Enterprise T1082 System Information Discovery

KONNI can gather the OS version, architecture information, hostname, and RAM size information from the victim’s machine and has used `cmd /c systeminfo` command to get a snapshot of the current system state of the target machine.[1][4][5]

Enterprise T1016 System Network Configuration Discovery

KONNI can collect the IP address from the victim’s machine.[1]

Enterprise T1049 System Network Connections Discovery

KONNI has used `net session` on the victim's machine.[5]

Enterprise T1033 System Owner/User Discovery

KONNI can collect the username from the victim’s machine.[1]

Enterprise T1204 .002 User Execution: Malicious File

KONNI has relied on a victim to enable malicious macros within an attachment delivered via email.[5]
