KeyBoy, Software S0387 | MITRE ATT&CK®

Archived: 2026-04-05 17:07:56 UTC

Enterprise T1547 .004 Boot or Logon Autostart Execution: Winlogon Helper DLL

KeyBoy issues the command `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"` to achieve persistence.[2] [1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

KeyBoy uses PowerShell commands to download and execute payloads.[2]

.003 Command and Scripting Interpreter: Windows Command Shell

KeyBoy can launch interactive shells for communicating with the victim machine.[2][3]

.005 Command and Scripting Interpreter: Visual Basic

KeyBoy uses VBS scripts for installing files and performing execution.[1]

.006 Command and Scripting Interpreter: Python

KeyBoy uses Python scripts for installing files and performing execution.[1]

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

KeyBoy installs a service pointing to a malicious DLL dropped to disk.[3]

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

KeyBoy attempts to collect passwords from browsers.[3]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

KeyBoy uses custom SSL libraries to impersonate SSL in C2 traffic.[2]

Enterprise T1083 File and Directory Discovery

KeyBoy has a command to launch a file browser or explorer on the system.[2]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

KeyBoy uses `-w Hidden` to conceal a PowerShell window that downloads a payload. [2]

Enterprise T1070 .006 Indicator Removal: Timestomp

KeyBoy time-stomped its DLL in order to evade detection.[2]

Enterprise T1105 Ingress Tool Transfer

KeyBoy has a download and upload functionality.[2][3]

Enterprise T1056 .001 Input Capture: Keylogging

KeyBoy installs a keylogger for intercepting credentials and keystrokes.[3]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

KeyBoy uses the Dynamic Data Exchange (DDE) protocol to download remote payloads.[2]

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

In one version of KeyBoy, string obfuscation routines were used to hide many of the critical values referenced in the malware.[1]

Enterprise T1113 Screen Capture

KeyBoy has a command to perform screen grabbing.[2]

Enterprise T1082 System Information Discovery

KeyBoy can gather extended system information, such as information about the operating system and memory.[2] [3]

Enterprise T1016 System Network Configuration Discovery

KeyBoy can determine the public or WAN IP address for the system.[2]
