Prikormka, Software S0113 | MITRE ATT&CK®

Archived: 2026-04-05 13:01:01 UTC

Enterprise T1560 Archive Collected Data

After collecting documents from removable media, Prikormka compresses the collected files, and encrypts it with Blowfish.[1]

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

Prikormka adds itself to a Registry Run key with the name guidVGA or guidVSA.[1]

Enterprise T1555 Credentials from Password Stores

A module in Prikormka collects passwords stored in applications installed on the victim.[1]

.003 Credentials from Web Browsers

A module in Prikormka gathers logins and passwords stored in applications on the victims, including Google Chrome, Mozilla Firefox, and several other browsers.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Prikormka encodes C2 traffic with Base64.[1]

Enterprise T1025 Data from Removable Media

Prikormka contains a module that collects documents with certain extensions from removable media or fixed drives connected via USB.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Prikormka creates a directory, `%USERPROFILE%\AppData\Local\SKC\`, which is used to store collected log files.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Prikormka encrypts some C2 traffic with the Blowfish cipher.[1]

Enterprise T1083 File and Directory Discovery

A module in Prikormka collects information about the paths, size, and creation time of files with specific file extensions, but not the actual content of the file.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Prikormka uses DLL search order hijacking for persistence by saving itself as ntshrui.dll to the Windows directory so it will load before the legitimate ntshrui.dll saved in the System32 subdirectory.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

After encrypting its own log files, the log encryption module in Prikormka deletes the original, unencrypted files from the host.[1]

Enterprise T1056 .001 Input Capture: Keylogging

Prikormka contains a keylogger module that collects keystrokes and the titles of foreground windows.[1]

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

Some resources in Prikormka are encrypted with a simple XOR operation or encoded with Base64.[1]

Enterprise T1120 Peripheral Device Discovery

A module in Prikormka collects information on available printers and disk drives.[1]

Enterprise T1113 Screen Capture

Prikormka contains a module that captures screenshots of the victim's desktop.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

A module in Prikormka collects information from the victim about installed anti-virus software.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Prikormka uses rundll32.exe to load its DLL.[1]

Enterprise T1082 System Information Discovery

A module in Prikormka collects information from the victim about Windows OS version, computer name, battery info, and physical memory.[1]

Enterprise T1016 System Network Configuration Discovery

A module in Prikormka collects information from the victim about its IP addresses and MAC addresses.[1]

Enterprise T1033 System Owner/User Discovery

A module in Prikormka collects information from the victim about the current user name.[1]
