Mispadu, Software S1122 | MITRE ATT&CK®

Archived: 2026-04-02 12:24:11 UTC

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

Mispadu creates a link in the startup folder for persistence.[1] Mispadu adds persistence via the registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`.[5]

Enterprise T1217 Browser Information Discovery

Mispadu can monitor browser activity for online banking actions and display full-screen overlay images to block user access to the intended site or present additional data fields.[4][2]

Enterprise T1115 Clipboard Data

Mispadu has the ability to capture and replace Bitcoin wallet data in the clipboard on a compromised host.[1]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

Mispadu's dropper uses VBS files to install payloads and perform execution.[2][1]

Enterprise T1555 Credentials from Password Stores

Mispadu has obtained credentials from mail clients via NirSoft MailPassView.[2][4][1]

.003 Credentials from Web Browsers

Mispadu can steal credentials from Google Chrome.[2][1][5]

Enterprise T1140 Deobfuscate/Decode Files or Information

Mispadu decrypts its encrypted configuration files prior to execution.[2][1]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Mispadu contains a copy of the OpenSSL library to encrypt C2 traffic.[4]

Enterprise T1041 Exfiltration Over C2 Channel

Mispadu can sends the collected financial data to the C2 server.[1][2]

Enterprise T1083 File and Directory Discovery

Mispadu searches for various filesystem paths to determine what banking applications are installed on the victim's machine.[1]

Enterprise T1056 .001 Input Capture: Keylogging

Mispadu can log keystrokes on the victim's machine.[1][5][3]

.002 Input Capture: GUI Input Capture

Mispadu can monitor browser activity for online banking actions and display full-screen overlay images to block user access to the intended site or present additional data fields.[4][2]

Enterprise T1106 Native API

Mispadu has used a variety of Windows API calls, including ShellExecute and WriteProcessMemory.[4][2]

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

Mispadu uses a custom algorithm to obfuscate its internal strings and uses hardcoded keys.[1]

Mispadu also uses encoded configuration files and has encoded payloads using Base64.[1][2][6]

Enterprise T1566 .002 Phishing: Spearphishing Link

Mispadu has been spread via malicious links embedded in emails.[2]

Enterprise T1057 Process Discovery

Mispadu can enumerate the running processes on a compromised host.[1]

Enterprise T1055 Process Injection

Mispadu's binary is injected into memory via `WriteProcessMemory`.[4][2]

Enterprise T1113 Screen Capture

Mispadu has the ability to capture screenshots on compromised hosts.[2][3][1][5]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Mispadu can list installed security products in the victim’s environment.[1][5]

Enterprise T1176 .001 Software Extensions: Browser Extensions

Mispadu utilizes malicious Google Chrome browser extensions to steal financial data.[1]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

Mispadu has been installed via MSI installer.[2][1]

.011 System Binary Proxy Execution: Rundll32

Mispadu uses RunDLL32 for execution via its injector DLL.[1]

Enterprise T1082 System Information Discovery

Mispadu collects the OS version, computer name, and language ID.[1]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

Mispadu checks and will terminate execution if the compromised system’s language ID is not Spanish or Portuguese.[4][2]

Enterprise T1204 .002 User Execution: Malicious File

Mispadu has relied on users to execute malicious files in order to gain execution on victim machines.[1][5][2]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

Mispadu can run checks to verify if it is running within a virtualized environments including Hyper-V, VirtualBox or VMWare and will terminate execution if the computer name is "JOHN-PC."[1][2]
