menuPass, Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH, BRONZE RIVERSIDE, Group G0045

Archived: 2026-04-02 11:16:15 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[12]

Enterprise T1583 .001 Acquire Infrastructure: Domains

menuPass has registered malicious domains for use in intrusion campaigns.[1][2]

Enterprise T1560 Archive Collected Data

menuPass has encrypted files and information before exfiltration.[1][2]

.001 Archive via Utility

menuPass has compressed files before exfiltration using TAR and RAR.[6][12][8]

Enterprise T1119 Automated Collection

menuPass has used the Csvde tool to collect Active Directory files and data.[8]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

menuPass uses PowerSploit to inject shellcode into PowerShell.[12][8]

.003 Command and Scripting Interpreter: Windows Command Shell

menuPass executes commands using a command-line interface and reverse shell. The group has used a modified version of pentesting script wmiexec.vbs to execute commands.[6][12][13][10] menuPass has used malicious macros embedded inside Office documents to execute files.[9][10]

Enterprise T1005 Data from Local System

menuPass has collected various files from the compromised computers.[1][8]

Enterprise T1039 Data from Network Shared Drive

menuPass has collected data from remote systems by mounting network shares with `net use` and using Robocopy to transfer data.[6]

Enterprise T1074 .001 Data Staged: Local Data Staging

menuPass stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.[6]

.002 Data Staged: Remote Data Staging

menuPass has staged data on remote MSP systems or other victim networks prior to exfiltration.[6][8]

Enterprise T1140 Deobfuscate/Decode Files or Information

menuPass has used certutil in a macro to decode base64-encoded content contained in a dropper document attached to an email. The group has also used `certutil -decode` to decode files on the victim's machine when dropping UPPERCUT.[9][10]

Enterprise T1568 .001 Dynamic Resolution: Fast Flux DNS

menuPass has used dynamic DNS service providers to host malicious domains.[2]

Enterprise T1190 Exploit Public-Facing Application

menuPass has leveraged vulnerabilities in Pulse Secure VPNs to hijack sessions.[14]

Enterprise T1210 Exploitation of Remote Services

menuPass has used tools to exploit the ZeroLogon vulnerability (CVE-2020-1472).[8]

Enterprise T1083 File and Directory Discovery

menuPass has searched compromised systems for folders of interest including those related to HR, audit and expense, and meeting memos.[8]

Enterprise T1574 .001 Hijack Execution Flow: DLL

menuPass has used DLL side-loading to launch versions of Mimikatz and PwDump6 as well as UPPERCUT.[12][10][8] menuPass has also used DLL search order hijacking.[6]

Enterprise T1070 .003 Indicator Removal: Clear Command History

menuPass has used Wevtutil to remove PowerShell execution logs.[14]

.004 Indicator Removal: File Deletion

A menuPass macro deletes files after it has decoded and decompressed them.[9][2]

Enterprise T1105 Ingress Tool Transfer

menuPass has installed updates and new malware on victims.[6][2]

Enterprise T1056 .001 Input Capture: Keylogging

menuPass has used key loggers to steal usernames and passwords.[2]

Enterprise T1036 Masquerading

menuPass has used esentutl to change file extensions to their true type that were masquerading as .txt files.[10]

.003 Rename Legitimate Utilities

menuPass has renamed certutil and moved it to a different location on the system to avoid detection based on use of the tool.[10]

.005 Match Legitimate Resource Name or Location

menuPass has been seen changing malicious files to appear legitimate.[2]

Enterprise T1106 Native API

menuPass has used native APIs including `GetModuleFileName` , `lstrcat` , `CreateFile` , and `ReadFile` .[8]

Enterprise T1046 Network Service Discovery

menuPass has used tcping.exe, similar to Ping, to probe port status on systems of interest.[12]

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

menuPass has encoded strings in its malware with base64 as well as with a simple, single-byte XOR obfuscation using key 0x40.[9][10][8]

Enterprise T1588 .002 Obtain Capabilities: Tool

menuPass has used and modified open-source tools like Impacket, Mimikatz, and pwdump.[12]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

menuPass has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.[12][13]

.003 OS Credential Dumping: NTDS

menuPass has used Ntdsutil to dump credentials.[8]

.004 OS Credential Dumping: LSA Secrets

menuPass has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.[12][13]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

menuPass has sent malicious Office documents via email as part of spearphishing campaigns as well as executables disguised as documents.[12][7][10][2]

Enterprise T1055 .012 Process Injection: Process Hollowing

menuPass has used process hollowing in iexplore.exe to load the RedLeaves implant.[9]

Enterprise T1090 .002 Proxy: External Proxy

menuPass has used a global service provider's IP as a proxy for C2 traffic from a victim.[7][10]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

menuPass has used RDP connections to move across the victim network.[6][2]

.004 Remote Services: SSH

menuPass has used Putty Secure Copy Client (PSCP) to transfer data.[6]

Enterprise T1018 Remote System Discovery

menuPass uses scripts to enumerate IP ranges on the victim network. menuPass has also issued the command `net view /domain` to a PlugX implant to gather information about remote systems on the network.[12][7]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

menuPass has used a script (atexec.py) to execute a command on a target machine via Task Scheduler.[12]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

menuPass has resized and added data to the certificate table to enable the signing of modified files with legitimate signatures.[14]

Enterprise T1218 .004 System Binary Proxy Execution: InstallUtil

menuPass has used `InstallUtil.exe` to execute malicious software.[12]

Enterprise T1016 System Network Configuration Discovery

menuPass has used several tools to scan for open NetBIOS nameservers and enumerate NetBIOS sessions.[12]

Enterprise T1049 System Network Connections Discovery

menuPass has used `net use` to conduct connectivity checks to machines.[6]

Enterprise T1199 Trusted Relationship

menuPass has used legitimate access granted to Managed Service Providers in order to access victims of interest.[12][7][8][1][2]

Enterprise T1204 .002 User Execution: Malicious File

menuPass has attempted to get victims to open malicious files such as Windows Shortcuts (.lnk) and/or Microsoft Office documents, sent via email as part of spearphishing campaigns.[12][7][9][10][2]

Enterprise T1078 Valid Accounts

menuPass has used valid accounts including shared between Managed Service Providers and clients to move between the two environments.[6][8][2][14]

Enterprise T1047 Windows Management Instrumentation

menuPass has used a modified version of pentesting script wmiexec.vbs, which logs into a remote machine using WMI.[12][13][8]
