HotCroissant, Software S0431 | MITRE ATT&CK®

Archived: 2026-04-05 14:37:26 UTC

Enterprise T1010 Application Window Discovery

HotCroissant has the ability to list the names of all open windows on the infected host.[2]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

HotCroissant can remotely open applications on the infected host with the `ShellExecuteA` command.[2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

HotCroissant has compressed network communications and encrypted them with a custom stream cipher.[2][1]

Enterprise T1041 Exfiltration Over C2 Channel

HotCroissant has the ability to download files from the infected host to the command and control (C2) server.[2]

Enterprise T1083 File and Directory Discovery

HotCroissant has the ability to retrieve a list of files in a given directory as well as drives and drive types.[2]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

HotCroissant has the ability to hide the window for operations performed on a given file.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

HotCroissant has the ability to clean up installed files, delete files, and delete itself from the victim's machine.[2]

Enterprise T1105 Ingress Tool Transfer

HotCroissant has the ability to upload a file from the command and control (C2) server to the victim machine.[2]

Enterprise T1106 Native API

HotCroissant can perform dynamic DLL importing and API lookups using `LoadLibrary` and `GetProcAddress` on obfuscated strings.[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

HotCroissant has used the open source UPX executable packer.[2]

.013 Obfuscated Files or Information: Encrypted/Encoded File

HotCroissant has encrypted strings with single-byte XOR and base64 encoded RC4.[2]

Enterprise T1057 Process Discovery

HotCroissant has the ability to list running processes on the infected host.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

HotCroissant has attempted to install a scheduled task named "Java Maintenance64" on startup to establish persistence.[2]

Enterprise T1113 Screen Capture

HotCroissant has the ability to do real time screen viewing on an infected host.[2]

Enterprise T1489 Service Stop

HotCroissant has the ability to stop services on the infected host.[2]

Enterprise T1518 Software Discovery

HotCroissant can retrieve a list of applications from the `SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths` registry key.[2]

Enterprise T1082 System Information Discovery

HotCroissant has the ability to determine if the current user is an administrator, Windows product name, processor name, screen resolution, and physical RAM of the infected host.[1]

Enterprise T1016 System Network Configuration Discovery

HotCroissant has the ability to identify the IP address of the compromised machine.[1]

Enterprise T1033 System Owner/User Discovery

HotCroissant has the ability to collect the username on the infected host.[2]

Enterprise T1007 System Service Discovery

HotCroissant has the ability to retrieve a list of services on the infected host.[2]
