

## HotCroissant, Software S0431 | MITRE ATT&CK®

Archived: 2026-04-05 15:43:57 UTC

Enterprise [T1010 Application Window Discovery](#)

[HotCroissant](#) has the ability to list the names of all open windows on the infected host.<sup>[2]</sup>

Enterprise [T1059 .003 Command and Scripting Interpreter: Windows Command Shell](#)

[HotCroissant](#) can remotely open applications on the infected host with the `ShellExecuteA` command.<sup>[2]</sup>

Enterprise [T1573 .001 Encrypted Channel: Symmetric Cryptography](#)

[HotCroissant](#) has compressed network communications and encrypted them with a custom stream cipher.<sup>[2][1]</sup>

Enterprise [T1041 Exfiltration Over C2 Channel](#)

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

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.<sup>[2]</sup>

Enterprise [T1564 .003 Hide Artifacts: Hidden Window](#)

[HotCroissant](#) has the ability to hide the window for operations performed on a given file.<sup>[2]</sup>

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.<sup>[2]</sup>

Enterprise [T1105 Ingress Tool Transfer](#)

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

Enterprise [T1106 Native API](#)

[HotCroissant](#) can perform dynamic DLL importing and API lookups using `LoadLibrary` and `GetProcAddress` on obfuscated strings.<sup>[1]</sup>

Enterprise [T1027 .002 Obfuscated Files or Information: Software Packing](#)

[HotCroissant](#) has used the open source UPX executable packer.<sup>[2]</sup>

[.013 Obfuscated Files or Information: Encrypted/Encoded File](#)

[HotCroissant](#) has encrypted strings with single-byte XOR and base64 encoded RC4.<sup>[2]</sup>

Enterprise [T1057 Process Discovery](#)

[HotCroissant](#) has the ability to list running processes on the infected host.<sup>[2]</sup>

Enterprise [T1053 .005 Scheduled Task/Job: Scheduled Task](#)

[HotCroissant](#) has attempted to install a scheduled task named "Java Maintenance64" on startup to establish persistence.<sup>[2]</sup>

Enterprise [T1113 Screen Capture](#)

[HotCroissant](#) has the ability to do real time screen viewing on an infected host.<sup>[2]</sup>

Enterprise [T1489 Service Stop](#)

[HotCroissant](#) has the ability to stop services on the infected host.<sup>[2]</sup>

Enterprise [T1518 Software Discovery](#)

[HotCroissant](#) can retrieve a list of applications from the `SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths` registry key.<sup>[2]</sup>

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.<sup>[1]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[HotCroissant](#) has the ability to identify the IP address of the compromised machine.<sup>[1]</sup>

Enterprise [T1033 System Owner/User Discovery](#)

[HotCroissant](#) has the ability to collect the username on the infected host.<sup>[2]</sup>

Enterprise [T1007 System Service Discovery](#)

[HotCroissant](#) has the ability to retrieve a list of services on the infected host.<sup>[2]</sup>

---

Source: <https://attack.mitre.org/software/S0431/>