Black Basta, Software S1070 | MITRE ATT&CK®

Archived: 2026-04-05 13:51:34 UTC

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Black Basta has used PowerShell scripts for discovery and to execute files over the network.[7][8][5]

.003 Command and Scripting Interpreter: Windows Command Shell

Black Basta can use `cmd.exe` to enable shadow copy deletion.[2]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Black Basta can create a new service to establish persistence.[3][4]

Enterprise T1486 Data Encrypted for Impact

Black Basta can encrypt files with the ChaCha20 cypher and using a multithreaded process to increase speed.[3][9][6][5][10][2][1][8][11] Black Basta has also encrypted files while the victim system is in safe mode, appending `.basta` upon completion.[7]

Enterprise T1622 Debugger Evasion

The Black Basta dropper can check system flags, CPU registers, CPU instructions, process timing, system libraries, and APIs to determine if a debugger is present.[11]

Enterprise T1491 .001 Defacement: Internal Defacement

Black Basta has set the desktop wallpaper on victims' machines to display a ransom note.[3][9][6][7][4][5][2][1][11]

Enterprise T1480 .002 Execution Guardrails: Mutual Exclusion

Black Basta will check for the presence of a hard-coded mutex `dsajdhas.0` before executing.[2]

Enterprise T1083 File and Directory Discovery

Black Basta can enumerate specific files for encryption.[6][4][5][10][2][1][8][11]

Enterprise T1222 .002 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification

The Black Basta binary can use `chmod` to gain full permissions to targeted files.[10]

Enterprise T1562 .009 Impair Defenses: Safe Mode Boot

Black Basta can reboot victim machines in safe mode with networking via `bcdedit /set safeboot network`.[3][6][7][4][1]

Enterprise T1490 Inhibit System Recovery

Black Basta can delete shadow copies using vssadmin.exe.[3][6][7][4][5][2][1][8][8][11]

Enterprise T1680 Local Storage Discovery

Black Basta can enumerate volumes.[3][6]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Black Basta has established persistence by creating a new service named `FAX` after deleting the legitimate service by the same name.[3][6][7]

.005 Masquerading: Match Legitimate Resource Name or Location

The Black Basta dropper has mimicked an application for creating USB bootable drivers.[11]

Enterprise T1112 Modify Registry

Black Basta has modified the Registry to enable itself to run in safe mode, to change the icons and file extensions for encrypted files, and to add the malware path for persistence.[3][6][7][5][2][1]

Enterprise T1106 Native API

Black Basta has the ability to use native APIs for numerous functions including discovery and defense evasion.[3][6][4][11][7]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Black Basta had added data prior to the Portable Executable (PE) header to prevent automatic scanners from identifying the payload.[11]

Enterprise T1018 Remote System Discovery

Black Basta can use LDAP queries to connect to AD and iterate over connected workstations.[11]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

The Black Basta dropper has been digitally signed with a certificate issued by Akeo Consulting for legitimate executables used for creating bootable USB drives.[11]

Enterprise T1082 System Information Discovery

Black Basta can collect system boot configuration and CPU information.[3][6]

Enterprise T1007 System Service Discovery

Black Basta can check whether the service name `FAX` is present.[6]

Enterprise T1529 System Shutdown/Reboot

Black Basta has used `ShellExecuteA` to shut down and restart the victim system.[7]

Enterprise T1204 .002 User Execution: Malicious File

Black Basta has been downloaded and executed from malicious Excel files.[7][8]

Enterprise T1497 Virtualization/Sandbox Evasion

Black Basta can make a random number of calls to the `kernel32.beep` function to hinder log analysis.[11]

.001 System Checks

Black Basta can check system flags and libraries, process timing, and API's to detect code emulation or sandboxing.[1][11]

Enterprise T1047 Windows Management Instrumentation

Black Basta has used WMI to execute files over the network.[5]
