BlackCat, Software S1068 | MITRE ATT&CK®

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

BlackCat can bypass UAC to escalate privileges.[1]

Enterprise T1134 Access Token Manipulation

BlackCat has the ability modify access tokens.[1][2]

Enterprise T1087 .002 Account Discovery: Domain Account

BlackCat can utilize `net use` commands to identify domain users.[1]

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

BlackCat can execute commands on a compromised network with the use of `cmd.exe`.[1]

Enterprise T1486 Data Encrypted for Impact

BlackCat has the ability to encrypt Windows devices, Linux devices, and VMWare instances.[1]

Enterprise T1491 .001 Defacement: Internal Defacement

BlackCat can change the desktop wallpaper on compromised hosts.[1][2]

Enterprise T1561 .001 Disk Wipe: Disk Content Wipe

BlackCat has the ability to wipe VM snapshots on compromised networks.[1][2]

Enterprise T1083 File and Directory Discovery

BlackCat can enumerate files for encryption.[1]

Enterprise T1222 .001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification

BlackCat can use Windows commands such as `fsutil behavior set SymLinkEvaluation R2L:1` to redirect file system access to a different location after gaining access into compromised networks.[1]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

BlackCat can clear Windows event logs using `wevtutil.exe`.[1]

Enterprise T1490 Inhibit System Recovery

BlackCat can delete shadow copies using `vssadmin.exe delete shadows /all /quiet` and `wmic.exe Shadowcopy Delete` ; it can also modify the boot loader using `bcdedit /set {default} recoveryenabled No` .[1]

Enterprise T1570 Lateral Tool Transfer

BlackCat can replicate itself across connected servers via `psexec` .[1]

Enterprise T1680 Local Storage Discovery

BlackCat can enumerate local drives.[1]

Enterprise T1112 Modify Registry

BlackCat has the ability to add the following registry key on compromised networks to maintain persistence: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \LanmanServer\Paramenters` [1]

Enterprise T1135 Network Share Discovery

BlackCat has the ability to discover network shares on compromised networks.[1][2]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

BlackCat can determine if a user on a compromised host has domain admin privileges.[1]

Enterprise T1018 Remote System Discovery

BlackCat can broadcasts NetBIOS Name Service (NBNC) messages to search for servers connected to compromised networks.[1]

Enterprise T1489 Service Stop

BlackCat has the ability to stop VM services on compromised networks.[1][2]

Enterprise T1082 System Information Discovery

BlackCat can obtain the computer name and UUID.[1]

Enterprise T1033 System Owner/User Discovery

BlackCat can utilize `net use` commands to discover the user name on a compromised host.[1]

Enterprise T1047 Windows Management Instrumentation

BlackCat can use `wmic.exe` to delete shadow copies on compromised networks.[1]
