BADHATCH, Software S1081 | MITRE ATT&CK®

Archived: 2026-04-05 15:32:44 UTC

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

BADHATCH can utilize the CMSTPLUA COM interface and the SilentCleanup task to bypass UAC.[2]

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

BADHATCH can impersonate a `lsass.exe` or `vmtoolsd.exe` token.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

BADHATCH can use HTTP and HTTPS over port 443 to communicate with actor-controlled C2 servers.[1][2]

.002 Application Layer Protocol: File Transfer Protocols

BADHATCH can emulate an FTP server to connect to actor-controlled C2 servers.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

BADHATCH can utilize `powershell.exe` to execute commands on a compromised host.[1][2]

.003 Command and Scripting Interpreter: Windows Command Shell

BADHATCH can use `cmd.exe` to execute commands on a compromised host.[1][2]

Enterprise T1482 Domain Trust Discovery

BADHATCH can use `nltest.exe /domain_trusts` to discover domain trust relationships on a compromised machine.[2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

BADHATCH can beacon to a hardcoded C2 IP address using TLS encryption every 5 minutes.[1]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

BADHATCH can use WMI event subscriptions for persistence.[2]

Enterprise T1041 Exfiltration Over C2 Channel

BADHATCH can exfiltrate data over the C2 channel.[1][2]

Enterprise T1070 .004 Indicator Removal: File Deletion

BADHATCH has the ability to delete PowerShell scripts from a compromised machine.[1]

Enterprise T1105 Ingress Tool Transfer

BADHATCH has the ability to load a second stage malicious DLL file onto a compromised machine.[1]

Enterprise T1106 Native API

BADHATCH can utilize Native API functions such as, `ToolHelp32` and `Rt1AdjustPrivilege` to enable `SeDebugPrivilege` on a compromised machine.[1]

Enterprise T1046 Network Service Discovery

BADHATCH can check for open ports on a computer by establishing a TCP connection.[2]

Enterprise T1135 Network Share Discovery

BADHATCH can check a user's access to the C$ share on a compromised machine.[2]

Enterprise T1027 .009 Obfuscated Files or Information: Embedded Payloads

BADHATCH has an embedded second stage DLL payload within the first stage of the malware.[1]

.010 Obfuscated Files or Information: Command Obfuscation

BADHATCH malicious PowerShell commands can be encoded with base64.[2]

.015 Obfuscated Files or Information: Compression

BADHATCH can be compressed with the ApLib algorithm.[2]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

BADHATCH can use `net.exe group "domain admins" /domain` to identify Domain Administrators.[2]

Enterprise T1057 Process Discovery

BADHATCH can retrieve a list of running processes from a compromised machine.[2]

Enterprise T1055 Process Injection

BADHATCH can inject itself into an existing explorer.exe process by using `RtlCreateUserThread`.[1][2]

.001 Dynamic-link Library Injection

BADHATCH has the ability to execute a malicious DLL by injecting into `explorer.exe` on a compromised machine.[1]

.004 Asynchronous Procedure Call

BADHATCH can inject itself into a new `svchost.exe -k netsvcs` process using the asynchronous procedure call (APC) queue.[1][2]

Enterprise T1090 Proxy

BADHATCH can use SOCKS4 and SOCKS5 proxies to connect to actor-controlled C2 servers. BADHATCH can also emulate a reverse proxy on a compromised machine to connect with actor-controlled C2 servers.[2]

Enterprise T1620 Reflective Code Loading

BADHATCH can copy a large byte array of 64-bit shellcode into process memory and execute it with a call to `CreateThread`.[1]

Enterprise T1018 Remote System Discovery

BADHATCH can use a PowerShell object such as, `System.Net.NetworkInformation.Ping` to ping a computer.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

BADHATCH can use `schtasks.exe` to gain persistence.[2]

Enterprise T1113 Screen Capture

BADHATCH can take screenshots and send them to an actor-controlled C2 server.[2]

Enterprise T1082 System Information Discovery

BADHATCH can obtain current system information from a compromised machine such as the `SHELL PID`, `PSVERSION`, `HOSTNAME`, `LOGONSERVER`, `LASTBOOTUP`, OS type/version, bitness, and hostname.[1][2]

Enterprise T1049 System Network Connections Discovery

BADHATCH can execute `netstat.exe -f` on a compromised machine.[2]

Enterprise T1033 System Owner/User Discovery

BADHATCH can obtain logged user information from a compromised machine and can execute the command `whoami.exe`.[2]

Enterprise T1124 System Time Discovery

BADHATCH can obtain the `DATETIME` and `UPTIME` from a compromised machine.[2]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

BADHATCH can perform pass the hash on compromised machines with x64 versions.[2]

Enterprise T1102 Web Service

BADHATCH can be utilized to abuse `sslip.io`, a free IP to domain mapping service, as part of actor-controlled C2 channels.[2]

Enterprise T1047 Windows Management Instrumentation

BADHATCH can utilize WMI to collect system information, create new processes, and run malicious PowerShell scripts on a compromised machine.[1][2]
