Chimera, Group G0114 | MITRE ATT&CK®

Archived: 2026-04-05 17:50:09 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Chimera has used `net user` for account discovery.[2]

.002 Account Discovery: Domain Account

Chimera has has used `net user /dom` and `net user Administrator` to enumerate domain accounts including administrator accounts.[1][2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Chimera has used HTTPS for C2 communications.[2]

.004 Application Layer Protocol: DNS

Chimera has used Cobalt Strike to encapsulate C2 in DNS traffic.[2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Chimera has used gzip for Linux OS and a modified RAR software to archive data on Windows hosts.[1][2]

Enterprise T1119 Automated Collection

Chimera has used custom DLLs for continuous retrieval of data from memory.[2]

Enterprise T1217 Browser Information Discovery

Chimera has used `type \\c$\Users\\Favorites\Links\Bookmarks bar\Imported From IE*citrix*` for bookmark discovery.[2]

Enterprise T1110 .003 Brute Force: Password Spraying

Chimera has used multiple password spraying attacks against victim's remote services to obtain valid user and administrator accounts.[2]

.004 Brute Force: Credential Stuffing

Chimera has used credential stuffing against victim's remote services to obtain valid accounts.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Chimera has used PowerShell scripts to execute malicious payloads and the DSInternals PowerShell module to make use of Active Directory features.[1][2]

.003 Command and Scripting Interpreter: Windows Command Shell

Chimera has used the Windows Command Shell and batch scripts for execution on compromised hosts.[2]

Enterprise T1213 .002 Data from Information Repositories: Sharepoint

Chimera has collected documents from the victim's SharePoint.[2]

Enterprise T1039 Data from Network Shared Drive

Chimera has collected data of interest from network shares.[2]

Enterprise T1074 .001 Data Staged: Local Data Staging

Chimera has staged stolen data locally on compromised hosts.[2]

.002 Data Staged: Remote Data Staging

Chimera has staged stolen data on designated servers in the target environment.[2]

Enterprise T1482 Domain Trust Discovery

Chimera has `nltest /domain_trusts` to identify domain trust relationships.[2]

Enterprise T1114 .001 Email Collection: Local Email Collection

Chimera has harvested data from victim's e-mail including through execution of `wmic /node: process call create "cmd /c copy c:\Users\\\backup.pst c:\windows\temp\backup.pst" copy "i:\\\My Documents\.pst" copy` .[2]

.002 Email Collection: Remote Email Collection

Chimera has harvested data from remote mailboxes including through execution of `\\c$\Users\\AppData\Local\Microsoft\Outlook*.ost` .[2]

Enterprise T1041 Exfiltration Over C2 Channel

Chimera has used Cobalt Strike C2 beacons for data exfiltration.[2]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Chimera has exfiltrated stolen data to OneDrive accounts.[2]

Enterprise T1133 External Remote Services

Chimera has used legitimate credentials to login to an external VPN, Citrix, SSH, and other remote services.[1][2]

Enterprise T1083 File and Directory Discovery

Chimera has utilized multiple commands to identify data of interest in file and directory listings.[2]

Enterprise T1589 .001 Gather Victim Identity Information: Credentials

Chimera has collected credentials for the target organization from previous breaches for use in brute force attacks.[2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Chimera has used side loading to place malicious DLLs in memory.[2]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

Chimera has cleared event logs on compromised hosts.[2]

.004 Indicator Removal: File Deletion

Chimera has performed file deletion to evade detection.[1]

.006 Indicator Removal: Timestomp

Chimera has used a Windows version of the Linux `touch` command to modify the date and time stamp on DLLs.[2]

Enterprise T1105 Ingress Tool Transfer

Chimera has remotely copied tools and malware onto targeted systems.[1]

Enterprise T1570 Lateral Tool Transfer

Chimera has copied tools between compromised hosts using SMB.[2]

Enterprise T1680 Local Storage Discovery

Chimera has used `fsutil fsinfo drives`, `systeminfo`, and `vssadmin list shadows` for system information including shadow volumes and drive information.[2]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Chimera has renamed malware to GoogleUpdate.exe and WinRAR to jucheck.exe, RecordedTV.ms, teredo.tmp, update.exe, and msadcs1.exe.[1]

Enterprise T1556 .001 Modify Authentication Process: Domain Controller Authentication

Chimera's malware has altered the NTLM authentication program on domain controllers to allow Chimera to login without a valid credential.[1]

Enterprise T1111 Multi-Factor Authentication Interception

Chimera has registered alternate phone numbers for compromised users to intercept 2FA codes sent via SMS.[2]

Enterprise T1106 Native API

Chimera has used direct Windows system calls by leveraging Dumpert.[1]

Enterprise T1046 Network Service Discovery

Chimera has used the `get -b -e -p` command for network scanning as well as a custom Python tool packed into a Windows executable named Get.exe to scan IP ranges for HTTP.[2]

Enterprise T1135 Network Share Discovery

Chimera has used `net share` and `net view` to identify network shares of interest.[2]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Chimera has encoded PowerShell commands.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

Chimera has obtained and used tools such as BloodHound, Cobalt Strike, Mimikatz, and PsExec.[1][2]

Enterprise T1003 .003 OS Credential Dumping: NTDS

Chimera has gathered the SYSTEM registry and ntds.dit files from target systems.[1] Chimera specifically has used the NtdsAudit tool to dump the password hashes of domain users via `msadcs.exe "NTDS.dit" -s "SYSTEM" -p RecordedTV_pdmp.txt --users-csv RecordedTV_users.csv` and used ntdsutil to copy the Active Directory database.[2]

Enterprise T1201 Password Policy Discovery

Chimera has used the NtdsAudit utility to collect information related to accounts and passwords.[2]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

Chimera has used `net localgroup administrators` to identify accounts with local administrative rights.[2]

Enterprise T1057 Process Discovery

Chimera has used `tasklist` to enumerate processes.[2]

Enterprise T1572 Protocol Tunneling

Chimera has encapsulated Cobalt Strike's C2 protocol in DNS and HTTPS.[2]

Enterprise T1012 Query Registry

Chimera has queried Registry keys using `reg query \\HKU\\SOFTWARE\Microsoft\Terminal Server Client\Servers` and `reg query \\HKU\\Software\Microsoft\Windows\CurrentVersion\Internet Settings`.[2]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Chimera has used RDP to access targeted systems.[1]

.002 Remote Services: SMB/Windows Admin Shares

Chimera has used Windows admin shares to move laterally.[1][2]

.006 Remote Services: Windows Remote Management

Chimera has used WinRM for lateral movement.[2]

Enterprise T1018 Remote System Discovery

Chimera has utilized various scans and queries to find domain controllers and remote services in the target environment.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Chimera has used scheduled tasks to invoke Cobalt Strike including through batch script `schtasks /create /ru "SYSTEM" /tn "update" /tr "cmd /c c:\windows\temp\update.bat" /sc once /f /st` and to maintain persistence.[1][2]

Enterprise T1016 System Network Configuration Discovery

Chimera has used ipconfig, Ping, and `tracert` to enumerate the IP address and network environment and settings of the local host.[2]

Enterprise T1049 System Network Connections Discovery

Chimera has used `netstat -ano | findstr EST` to discover network connections.[2]

Enterprise T1033 System Owner/User Discovery

Chimera has used the `quser` command to show currently logged on users.[2]

Enterprise T1007 System Service Discovery

Chimera has used `net start` and `net use` for system service discovery.[2]

Enterprise T1569 .002 System Services: Service Execution

Chimera has used PsExec to deploy beacons on compromised systems.[2]

Enterprise T1124 System Time Discovery

Chimera has used `time /t` and `net time \ip/hostname` for system time discovery.[2]

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

Chimera has dumped password hashes for use in pass the hash authentication attacks.[2]

Enterprise T1078 Valid Accounts

Chimera has used a valid account to maintain persistence via scheduled task.[1]

.002 Domain Accounts

Chimera has used compromised domain accounts to gain access to the target environment.[2]

Enterprise T1047 Windows Management Instrumentation

Chimera has used WMIC to execute remote commands.[1][2]
