RedCurl, Group G1039 | MITRE ATT&CK®

Archived: 2026-04-05 16:06:30 UTC

Enterprise T1087 .001 Account Discovery: Local Account

RedCurl has collected information about local accounts.[1][2]

.002 Account Discovery: Domain Account

RedCurl has collected information about domain accounts using SysInternal's AdExplorer functionality .[1][2]

.003 Account Discovery: Email Account

RedCurl has collected information about email accounts.[1][2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

RedCurl has used HTTP, HTTPS and Webdav protocls for C2 communications.[1][2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

RedCurl has downloaded 7-Zip to decompress password protected archives.[3]

Enterprise T1119 Automated Collection

RedCurl has used batch scripts to collect data.[1][2]

Enterprise T1020 Automated Exfiltration

RedCurl has used batch scripts to exfiltrate data.[1][2]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

RedCurl has established persistence by creating entries in `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

RedCurl has used PowerShell to execute commands and to download malware.[1][2][3]

.003 Command and Scripting Interpreter: Windows Command Shell

RedCurl has used the Windows Command Prompt to execute commands.[1][2][3]

.005 Command and Scripting Interpreter: Visual Basic

RedCurl has used VBScript to run malicious files.[1][2]

.006 Command and Scripting Interpreter: Python

RedCurl has used a Python script to establish outbound communication and to execute commands using SMB port 445.[3]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

RedCurl used LaZagne to obtain passwords from web browsers.[1][2]

Enterprise T1005 Data from Local System

RedCurl has collected data from the local disk of compromised hosts.[1][2]

Enterprise T1039 Data from Network Shared Drive

RedCurl has collected data about network drives.[1][2]

Enterprise T1587 .001 Develop Capabilities: Malware

RedCurl has created its own tools to use during operations.[4]

Enterprise T1114 .001 Email Collection: Local Email Collection

RedCurl has collected emails to use in future phishing campaigns.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

RedCurl has used AES-128 CBC to encrypt C2 communications.[2]

.002 Encrypted Channel: Asymmetric Cryptography

RedCurl has used HTTPS for C2 communication.[1][2]

Enterprise T1083 File and Directory Discovery

RedCurl has searched for and collected files on local and network drives.[4][1][2]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

RedCurl added the "hidden" file attribute to original files, manipulating victims to click on malicious LNK files.[1][2]

Enterprise T1070 .004 Indicator Removal: File Deletion

RedCurl has deleted files after execution.[1][2][3]

Enterprise T1202 Indirect Command Execution

RedCurl has used pcalua.exe to obfuscate binary execution and remote connections.[3]

Enterprise T1056 .002 Input Capture: GUI Input Capture

RedCurl prompts the user for credentials through a Microsoft Outlook pop-up.[1][2]

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

RedCurl mimicked legitimate file names and scheduled tasks, e.g. `MicrosoftCurrentupdatesCheck` and `MdMMaintenenceTask` to mask malicious files and scheduled tasks.[1][2]

Enterprise T1046 Network Service Discovery

RedCurl has used netstat to check if port 4119 is open.[3]

Enterprise T1027 Obfuscated Files or Information

RedCurl has used malware with string encryption.[4] RedCurl has also encrypted data and has encoded PowerShell commands using Base64.[1][2] RedCurl has used `PyArmor` to obfuscate code execution of LaZagne.[1] Additionally, RedCurl has obfuscated downloaded files by renaming them as commonly used tools and has used `echo`, instead of file names themselves, to execute files.[3]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

RedCurl used LaZagne to obtain passwords from memory.[1][2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

RedCurl has used phishing emails with malicious files to gain initial access.[1][3]

.002 Phishing: Spearphishing Link

RedCurl has used phishing emails with malicious links to gain initial access.[1][2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

RedCurl has created scheduled tasks for persistence.[1][2][3]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

RedCurl has used rundll32.exe to execute malicious files.[1][2][3]

Enterprise T1082 System Information Discovery

RedCurl has collected information about the target system, such as system information and list of network connections.[1][2]

Enterprise T1080 Taint Shared Content

RedCurl has placed modified LNK files on network drives for lateral movement.[1][2]

Enterprise T1537 Transfer Data to Cloud Account

RedCurl has used cloud storage to exfiltrate data, in particular the megatools utilities were used to exfiltrate data to Mega, a file storage service.[1][2]

Enterprise T1199 Trusted Relationship

RedCurl has gained access to a contractor to pivot to the victim's infrastructure.[4]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

RedCurl used LaZagne to obtain passwords in files.[1][2]

.002 Unsecured Credentials: Credentials in Registry

RedCurl used LaZagne to obtain passwords in the Registry.[1][2]

Enterprise T1204 .001 User Execution: Malicious Link

RedCurl has used malicious links to infect the victim machines.[1][2]

.002 User Execution: Malicious File

RedCurl has used malicious files to infect the victim machines.[1][2][3]

Enterprise T1102 Web Service

RedCurl has used web services to download malicious files.[1][2]
