PUBLOAD, Software S1228 | MITRE ATT&CK®

Archived: 2026-04-05 12:46:32 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

PUBLOAD has communicated via `curl` over HTTP to identify device IP data.[3] PUBLOAD has also utilized HTTP for a command-and-control protocol through HTTP POST.[4][5][6] PUBLOAD has also leveraged HTTPS for C2.[2]

.002 Application Layer Protocol: File Transfer Protocols

PUBLOAD has used `curl` for data exfiltration over FTP.[3]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

PUBLOAD has used utilities such as `WinRAR` to archive data prior to exfiltration.[3]

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

PUBLOAD has added Registry Run keys to achieve persistence using `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`. [7][4][5][3][1]

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

PUBLOAD has used several commands executed in sequence via `cmd`. [3]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

PUBLOAD has modified HTTP POST requests to resemble legitimate communications.[5][6] PUBLOAD used FakeTLS headers in network packets to impersonate various versions of TLS protocols to blend in with legitimate network traffic. PUBLOAD has utilized FakeTLS headers with the bytes 17 03 03.[2]

Enterprise T1622 Debugger Evasion

PUBLOAD has embedded debug strings with messages to distract analysts.[7][1] PUBLOAD has leveraged `OutputDebugStringW` and `OutputDebugStringA` functions.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

PUBLOAD has decoded its payload prior to execution.[7][5][2][1][6]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

PUBLOAD has used RC4 encryption in C2 communications.[7][4][1]

Enterprise T1480 .001 Execution Guardrails: Environmental Keying

PUBLOAD has utilized environmental keying in the payload to include the victim volume serial number, computer name, username, and machine's tick count.[2]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

PUBLOAD has leveraged `curl` for data exfiltration over FTP by uploading RAR archives containing targeted files (.doc, .docx, .xls, .xlsx, .pdf, .ppt, .pptx) to an adversary-owned FTP site.[3]

Enterprise T1574 .001 Hijack Execution Flow: DLL

PUBLOAD has abused legitimate executables to side-load malicious DLLs.[7][4][5][2][1][6][8]

Enterprise T1105 Ingress Tool Transfer

PUBLOAD has acted as a stager that can download the next-stage payload from its C2 server.[5][9][2][1][6] PUBLOAD has also delivered FDMTP as a secondary control tool and PTSOCKET for exfiltration to some infected systems.[3]

Enterprise T1680 Local Storage Discovery

PUBLOAD has leveraged `wmic logicaldisk get` to map local network drives.[3]

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

PUBLOAD has renamed malicious files to mimic legitimate file names such as adobe_wf.exe.[1]

Enterprise T1106 Native API

PUBLOAD has used various Windows API calls during execution, when establishing persistence and defense evasion.[5][2] PUBLOAD stager leveraged Windows API functions with callback including `GrayStringW`, `EnumDateFormatsA`, and `LineDDA` to bypass anti-virus monitoring. [1] PUBLOAD has also utilized other native windows API functions with callback functions such as `EnumChildWindows` and `EnumSystemLanguageGroupsA`. [6]

Enterprise T1027 Obfuscated Files or Information

PUBLOAD has obfuscated DLL names using the ror13AddHash32 algorithm.[7]

.015 Compression

PUBLOAD has been delivered as compressed files within ZIP files to victims.[5][6]

Enterprise T1057 Process Discovery

PUBLOAD has used `tasklist` to gather running processes on victim host.[3] PUBLOAD has also leveraged the `OpenEventA` Windows API function to check whether the same process was already running.[1]

Enterprise T1012 Query Registry

PUBLOAD has queried Registry values to identify software using `reg query`.[3]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

PUBLOAD has created scheduled tasks to maintain persistence with the command `schtasks.exe /F /Create /TN Microsoft_Licensing /sc minute /MO 1 /TR C:\\Users\\Public\\Libraries\...` [7][5][1]

Enterprise T1518 Software Discovery

PUBLOAD has used several commands executed in sequence via `cmd` in a short interval to gather software versions including querying Registry keys.[3]

.001 Security Software Discovery

PUBLOAD has identified AV products on an infected host using the following command: `WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List`.[3]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

PUBLOAD has used valid legitimate digital signatures and certificates to evade detection.[4]

Enterprise T1082 System Information Discovery

PUBLOAD has collected and sent system information including volume serial number, computer name, and system uptime to designated C2.[7][2] PUBLOAD has also used several commands executed in sequence via `cmd` in a short interval to gather system information about the infected host including `systeminfo`.[3] PUBLOAD has decrypted shellcode that collects the computer name.[1]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

PUBLOAD has checked supported languages on the compromised system.[4]

Enterprise T1016 System Network Configuration Discovery

PUBLOAD has obtained information about local networks through the `ipconfig /all` command.[3]

.001 Internet Connection Discovery

PUBLOAD has identified internet connectivity details through commands such as `tracert -h 5 -4 google.com` and `curl http://myip.ipip.net`.[3]

.002 Wi-Fi Discovery

PUBLOAD has collected information on Wi-Fi networks from victim hosts leveraging `netsh wlan show profiles`, `netsh wlan show interface`, and `netsh wlan show`.[3]

Enterprise T1049 System Network Connections Discovery

PUBLOAD has used several commands executed in sequence via `cmd` in a short interval to gather information on network connections.[3]

Enterprise T1033 System Owner/User Discovery

PUBLOAD has obtained the username from an infected host.[7][4][2][1]

Enterprise T1007 System Service Discovery

PUBLOAD has leveraged `tasklist` to gather running services on victim host.[3]

Enterprise T1124 System Time Discovery

PUBLOAD has collected the machine's tick count through the use of `GetTickCount`.[2]

Enterprise T1205 Traffic Signaling

PUBLOAD has utilized a magic packet value in C2 communications and only executes in memory when response packets match specific values of 17 03 03.[4][9][2][1][8] PUBLOAD has also used magic bytes consisting of 46 77 4d.[4]

Enterprise T1047 Windows Management Instrumentation

PUBLOAD has used `wmic` to gather information from the victim device.[3]
