Clambling, Software S0660 | MITRE ATT&CK®

Archived: 2026-04-05 14:14:30 UTC

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

Clambling has the ability to bypass UAC using a `passuac.dll` file.[1][2]

Enterprise T1071 Application Layer Protocol

Clambling has the ability to use Telnet for communication.[1]

.001 Web Protocols

Clambling has the ability to communicate over HTTP.[1]

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

Clambling can establish persistence by adding a Registry run key.[1][2]

Enterprise T1115 Clipboard Data

Clambling has the ability to capture and store clipboard data.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

The Clambling dropper can use PowerShell to download the malware.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

Clambling can use cmd.exe for command execution.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Clambling can register itself as a system service to gain persistence.[2]

Enterprise T1005 Data from Local System

Clambling can collect information from a compromised host.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Clambling can deobfuscate its payload prior to execution.[1][2]

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

Clambling can send files from a victim's machine to Dropbox.[1][2]

Enterprise T1083 File and Directory Discovery

Clambling can browse directories on a compromised host.[1][2]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Clambling has the ability to set its file attributes to hidden.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Clambling can store a file named `mpsvc.dll`, which opens a malicious `mpsvc.mui` file, in the same folder as the legitimate Microsoft executable `MsMpEng.exe` to gain execution.[1][2]

Enterprise T1056 .001 Input Capture: Keylogging

Clambling can capture keystrokes on a compromised host.[1][2]

Enterprise T1112 Modify Registry

Clambling can set and delete Registry keys.[1]

Enterprise T1135 Network Share Discovery

Clambling has the ability to enumerate network shares.[1]

Enterprise T1095 Non-Application Layer Protocol

Clambling has the ability to use TCP and UDP for communication.[1]

Enterprise T1027 Obfuscated Files or Information

The Clambling executable has been obfuscated when dropped on a compromised host.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Clambling has been delivered to victim's machines through malicious e-mail attachments.[1]

Enterprise T1057 Process Discovery

Clambling can enumerate processes on a targeted system.[1]

Enterprise T1055 Process Injection

Clambling can inject into the `svchost.exe` process for execution.[1]

.012 Process Hollowing

Clambling can execute binaries through process hollowing.[1]

Enterprise T1012 Query Registry

Clambling has the ability to enumerate Registry keys, including `KEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt\strDataDir` to search for a bitcoin wallet.[1][2]

Enterprise T1113 Screen Capture

Clambling has the ability to capture screenshots.[1]

Enterprise T1082 System Information Discovery

Clambling can discover the hostname, computer name, and Windows version of a targeted machine.[1][2]

Enterprise T1016 System Network Configuration Discovery

Clambling can enumerate the IP address of a compromised machine.[1][2]

Enterprise T1033 System Owner/User Discovery

Clambling can identify the username on a compromised host.[1][2]

Enterprise T1569 .002 System Services: Service Execution

Clambling can create and start services on a compromised host.[1]

Enterprise T1124 System Time Discovery

Clambling can determine the current time.[1]

Enterprise T1204 .002 User Execution: Malicious File

Clambling has gained execution through luring victims into opening malicious files.[1]

Enterprise T1125 Video Capture

Clambling can record screen content in AVI format.[1][2]

Enterprise T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks

Clambling can wait 30 minutes before initiating contact with C2.[1]

Enterprise T1102 .002 Web Service: Bidirectional Communication

Clambling can use Dropbox to download malicious payloads, send commands, and receive information.[1][2]
