Troll Stealer, Software S1196 | MITRE ATT&CK®

Archived: 2026-04-05 14:54:45 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Troll Stealer uses HTTP to communicate to command and control infrastructure.[1]

Enterprise T1560 Archive Collected Data

Troll Stealer compresses stolen data prior to exfiltration.[1]

Enterprise T1217 Browser Information Discovery

Troll Stealer collects information from Chromium-based browsers and Firefox such as cookies, history, downloads, and extensions.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Troll Stealer creates and executes a PowerShell script to delete itself.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

Troll Stealer can create and execute Windows batch scripts.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Troll Stealer performs XOR encryption and Base64 encoding of data prior to sending to command and control infrastructure.[1]

Enterprise T1213 Data from Information Repositories

Troll Stealer gathers information from the Government Public Key Infrastructure (GPKI) folder, associated with South Korean government public key infrastructure, on infected systems.[1][2]

Enterprise T1005 Data from Local System

Troll Stealer gathers information from infected systems such as SSH information from the victim's `.ssh` directory.[2] Troll Stealer collects information from local FileZilla installations and Microsoft Sticky Note.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Troll Stealer encrypts gathered information on victim devices prior to exfiltrating it through command and control infrastructure.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Troll Stealer encrypts data sent to command and control infrastructure using a combination of RC4 and RSA-4096 algorithms.[1]

Enterprise T1480 .002 Execution Guardrails: Mutual Exclusion

Troll Stealer creates a mutex during installation to prevent duplicate execution.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Troll Stealer exfiltrates collected information to its command and control infrastructure.[1]

Enterprise T1083 File and Directory Discovery

Troll Stealer can enumerate and collect items from local drives and folders.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Troll Stealer creates and can execute a BAT script that will delete the malware.[1]

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

Troll Stealer is typically installed via a dropper file that masquerades as a legitimate security program installation file.[1][2]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Troll Stealer has been delivered as a VMProtect-packed binary.[1][3]

Enterprise T1113 Screen Capture

Troll Stealer can capture screenshots from victim machines.[1][2]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Troll Stealer, along with its associated dropper, utilizes legitimate, stolen code signing certificates.[1][3]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Troll Stealer is dropped as a DLL file and executed via `rundll32.exe` by its installer.[1][3]

Enterprise T1082 System Information Discovery

Troll Stealer can collect local system information.[1][2]

Enterprise T1016 System Network Configuration Discovery

Troll Stealer collects the MAC address of victim devices.[1]

Enterprise T1552 .004 Unsecured Credentials: Private Keys

Troll Stealer collects all data in victim `.ssh` folders by creating a compressed copy that is subsequently exfiltrated to command and control infrastructure. Troll Stealer also collects key information associated with the Government Public Key Infrastructure (GPKI) service for South Korean government information systems.[1][2]
