Raccoon Stealer, Software S1148 | MITRE ATT&CK®

Archived: 2026-04-05 14:56:16 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Raccoon Stealer checks the privileges of running processes to determine if the running user is equivalent to `NT Authority\System`.[3]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Raccoon Stealer uses HTTP, and particularly HTTP POST requests, for command and control actions.[1][2][3]

Enterprise T1560 Archive Collected Data

Raccoon Stealer archives collected system information in a text f ile, `System info.txt`, prior to exfiltration.[3]

Enterprise T1119 Automated Collection

Raccoon Stealer collects files and directories from victim systems based on configuration data downloaded from command and control servers.[1][2][3]

Enterprise T1020 Automated Exfiltration

Raccoon Stealer will automatically collect and exfiltrate data identified in received configuration files from command and control nodes.[1][2][3]

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

Raccoon Stealer collects passwords, cookies, and autocomplete information from various popular web browsers.[3]

Enterprise T1213 Data from Information Repositories

Raccoon Stealer gathers information from repositories associated with cryptocurrency wallets and the Telegram messaging service.[3]

Enterprise T1005 Data from Local System

Raccoon Stealer collects data from victim machines based on configuration information received from command and control nodes.[1][3]

Enterprise T1140 Deobfuscate/Decode Files or Information

Raccoon Stealer uses RC4-encrypted, base64-encoded strings to obfuscate functionality and command and control servers.[1][2]

Enterprise T1041 Exfiltration Over C2 Channel

Raccoon Stealer uses existing HTTP-based command and control channels for exfiltration.[1][2][3]

Enterprise T1083 File and Directory Discovery

Raccoon Stealer identifies target files and directories for collection based on a configuration file.[1][3]

Enterprise T1070 .004 Indicator Removal: File Deletion

Raccoon Stealer can remove files related to use and installation.[2]

Enterprise T1105 Ingress Tool Transfer

Raccoon Stealer downloads various library files enabling interaction with various data stores and structures to facilitate follow-on information theft.[1][3]

Enterprise T1027 .007 Obfuscated Files or Information: Dynamic API Resolution

Raccoon Stealer dynamically links key WinApi functions during execution.[2][3]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Raccoon Stealer uses RC4 encryption for strings and command and control addresses to evade static detection.[1][2][3]

Enterprise T1012 Query Registry

Raccoon Stealer queries the Windows Registry to fingerprint the infected host via the `HKLM:\SOFTWARE\Microsoft\Cryptography\MachineGuid` key.[2][3]

Enterprise T1113 Screen Capture

Raccoon Stealer can capture screenshots from victim systems.[1][3]

Enterprise T1518 Software Discovery

Raccoon Stealer is capable of identifying running software on victim machines.[2][3]

Enterprise T1539 Steal Web Session Cookie

Raccoon Stealer attempts to steal cookies and related information in browser history.[3]

Enterprise T1195 Supply Chain Compromise

Raccoon Stealer has been distributed through cracked software downloads.[1]

Enterprise T1082 System Information Discovery

Raccoon Stealer gathers information on infected systems such as operating system, processor information, RAM, and display information.[1][3]

Enterprise T1614 System Location Discovery

Raccoon Stealer collects the `Locale Name` of the infected device via `GetUserDefaultLocaleName` to determine whether the string `ru` is included, but in analyzed samples no action is taken if present.[1]

Enterprise T1033 System Owner/User Discovery

Raccoon Stealer gathers information on the infected system owner and user.[1][2][3]

Enterprise T1124 System Time Discovery

Raccoon Stealer gathers victim machine timezone information.[1][3]

Source: https://attack.mitre.org/software/S1148