Chaes, Software S0631 | MITRE ATT&CK®

Archived: 2026-04-05 16:42:53 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Chaes has used HTTP for C2 communications.[1]

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

Chaes has added persistence via the Registry key `software\microsoft\windows\currentversion\run\microsoft windows html help`.[1]

Enterprise T1185 Browser Session Hijacking

Chaes has used the Puppeteer module to hook and monitor the Chrome web browser to collect user information from infected hosts.[1]

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

Chaes has used cmd to execute tasks on the system.[1]

.005 Command and Scripting Interpreter: Visual Basic

Chaes has used VBscript to execute malicious code.[1]

.006 Command and Scripting Interpreter: Python

Chaes has used Python scripts for execution and the installation of additional files.[1]

.007 Command and Scripting Interpreter: JavaScript

Chaes has used JavaScript and Node.Js information stealer script that exfiltrates data using the node process.[1]

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

Chaes can steal login credentials and stored financial information from the browser.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Chaes has used Base64 to encode C2 communications.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Chaes has decrypted an AES encrypted binary file to trigger the download of other files.[1]

Enterprise T1573 Encrypted Channel

Chaes has used encryption for its C2 channel.[1]

Enterprise T1048 Exfiltration Over Alternative Protocol

Chaes has exfiltrated its collected data from the infected machine to the C2, sometimes using the MIME protocol.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Chaes has used search order hijacking to load a malicious DLL.[1]

Enterprise T1105 Ingress Tool Transfer

Chaes can download additional files onto an infected machine.[1]

Enterprise T1056 Input Capture

Chaes has a module to perform any API hooking it desires.[1]

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

Chaes has used an unsigned, crafted DLL module named `hha.dll` that was designed to look like a legitimate 32-bit Windows DLL.[1]

Enterprise T1112 Modify Registry

Chaes can modify Registry values to stored information and establish persistence.[1]

Enterprise T1106 Native API

Chaes used the `CreateFileW()` API function with read permissions to access downloaded payloads.[1]

Enterprise T1027 .011 Obfuscated Files or Information: Fileless Storage

Some versions of Chaes stored its instructions (otherwise in a `instructions.ini` file) in the Registry.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Chaes has been delivered by sending victims a phishing email containing a malicious .docx file.[1]

Enterprise T1113 Screen Capture

Chaes can capture screenshots of the infected machine.[1]

Enterprise T1539 Steal Web Session Cookie

Chaes has used a script that extracts the web session cookie and sends it to the C2 server.[1]

Enterprise T1218 .004 System Binary Proxy Execution: InstallUtil

Chaes has used Installutill to download content.[1]

.007 System Binary Proxy Execution: Msiexec

Chaes has used .MSI files as an initial way to start the infection chain.[1]

Enterprise T1082 System Information Discovery

Chaes has collected system information, including the machine name and OS version.[1]

Enterprise T1033 System Owner/User Discovery

Chaes has collected the username and UID from the infected machine.[1]

Enterprise T1221 Template Injection

Chaes changed the template target of the settings.xml file embedded in the Word document and populated that field with the downloaded URL of the next payload.[1]

Enterprise T1204 .002 User Execution: Malicious File

Chaes requires the user to click on the malicious Word document to execute the next part of the attack.[1]
