SocGholish, Software S1124 | MITRE ATT&CK®

Archived: 2026-04-05 17:15:54 UTC

Enterprise T1059 .007 Command and Scripting Interpreter: JavaScript

The SocGholish payload is executed as JavaScript.[2][1][3][4]

Enterprise T1074 .001 Data Staged: Local Data Staging

SocGholish can send output from `whoami` to a local temp file using the naming convention `rad<5-hex-chars>.tmp`.[3]

Enterprise T1482 Domain Trust Discovery

SocGholish can profile compromised systems to identify domain trust relationships.[2][3]

Enterprise T1189 Drive-by Compromise

SocGholish has been distributed through compromised websites with malicious content often masquerading as browser updates.[2]

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

SocGholish can exfiltrate data directly to its C2 domain via HTTP.[3]

Enterprise T1105 Ingress Tool Transfer

SocGholish can download additional malware to infected hosts.[3][4]

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

SocGholish has been named `AutoUpdater.js` to mimic legitimate update files.[2]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

SocGholish has single or double Base-64 encoded references to its second-stage server URLs.[1]

.015 Obfuscated Files or Information: Compression

The SocGholish JavaScript payload has been delivered within a compressed ZIP archive.[3][4]

Enterprise T1566 .002 Phishing: Spearphishing Link

SocGholish has been spread via emails containing malicious links.[2]

Enterprise T1057 Process Discovery

SocGholish can list processes on targeted hosts.[4]

Enterprise T1518 Software Discovery

SocGholish can identify the victim's browser in order to serve the correct fake update page.[4]

Enterprise T1082 System Information Discovery

SocGholish has the ability to enumerate system information including the victim computer name.[2][3][4]

Enterprise T1614 System Location Discovery

SocGholish can use IP-based geolocation to limit infections to victims in North America, Europe, and a small number of Asian-Pacific nations.[4]

Enterprise T1016 System Network Configuration Discovery

SocGholish has the ability to enumerate the domain name of a victim, as well as if the host is a member of an Active Directory domain.[2][3][4]

Enterprise T1033 System Owner/User Discovery

SocGholish can use `whoami` to obtain the username from a compromised host.[2][3][4]

Enterprise T1204 .001 User Execution: Malicious Link

SocGholish has lured victims into interacting with malicious links on compromised websites for execution.[2]

Enterprise T1102 Web Service

SocGholish has used Amazon Web Services to host second-stage servers.[1]

Enterprise T1047 Windows Management Instrumentation

SocGholish has used WMI calls for script execution and system profiling.[2]
