SMOKEDHAM, Software S0649 | MITRE ATT&CK®

Archived: 2026-04-05 16:49:14 UTC

Enterprise T1087 .001 Account Discovery: Local Account

SMOKEDHAM has used `net.exe user` and `net.exe users` to enumerate local accounts on a compromised host.[2]

Enterprise T1098 .007 Account Manipulation: Additional Local or Domain Groups

SMOKEDHAM has added user accounts to local Admin groups.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

SMOKEDHAM has communicated with its C2 servers via HTTPS and HTTP POST requests.[2]

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

SMOKEDHAM has used `reg.exe` to create a Registry Run key.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

SMOKEDHAM can execute Powershell commands sent from its C2 server.[2]

Enterprise T1136 .001 Create Account: Local Account

SMOKEDHAM has created user accounts.[2]

Enterprise T1132 .001 Data Encoding: Standard Encoding

SMOKEDHAM has encoded its C2 traffic with Base64.[2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

SMOKEDHAM has encrypted its C2 traffic with RC4.[2]

Enterprise T1041 Exfiltration Over C2 Channel

SMOKEDHAM has exfiltrated data to its C2 server.[2]

Enterprise T1564 .002 Hide Artifacts: Hidden Users

SMOKEDHAM has modified the Registry to hide created user accounts from the Windows logon screen. [2]

Enterprise T1105 Ingress Tool Transfer

SMOKEDHAM has used Powershell to download UltraVNC and ngrok from third-party file sharing sites.[2]

Enterprise T1056 .001 Input Capture: Keylogging

SMOKEDHAM can continuously capture keystrokes.[1][2]

Enterprise T1112 Modify Registry

SMOKEDHAM has modified registry keys for persistence, to enable credential caching for credential access, and to facilitate lateral movement via RDP.[2]

Enterprise T1027 .009 Obfuscated Files or Information: Embedded Payloads

The SMOKEDHAM source code is embedded in the dropper as an encrypted string.[2]

Enterprise T1598 .003 Phishing for Information: Spearphishing Link

SMOKEDHAM has been delivered via malicious links in phishing emails.[1]

Enterprise T1090 .004 Proxy: Domain Fronting

SMOKEDHAM has used a fronted domain to obfuscate its hard-coded C2 server domain.[2]

Enterprise T1113 Screen Capture

SMOKEDHAM can capture screenshots of the victim’s desktop.[1][2]

Enterprise T1082 System Information Discovery

SMOKEDHAM has used the `systeminfo` command on a compromised host.[2]

Enterprise T1033 System Owner/User Discovery

SMOKEDHAM has used `whoami` commands to identify system owners.[2]

Enterprise T1204 .001 User Execution: Malicious Link

SMOKEDHAM has relied upon users clicking on a malicious link delivered through phishing.[1]

Enterprise T1102 Web Service

SMOKEDHAM has used Google Drive and Dropbox to host files downloaded by victims via malicious links.[1]
