Ursnif, Software S0386 | MITRE ATT&CK®

Archived: 2026-04-05 12:57:30 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Ursnif has used HTTPS for C2.[3][4][2]

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

Ursnif has used Registry Run keys to establish automatic execution at system startup.[5][6]

Enterprise T1185 Browser Session Hijacking

Ursnif has injected HTML codes into banking sites to steal sensitive online banking information (ex: usernames and passwords).[6]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Ursnif droppers have used PowerShell in download cradles to download and execute the malware's full executable payload.[7]

.005 Command and Scripting Interpreter: Visual Basic

Ursnif droppers have used VBA macros to download and execute the malware's full executable payload.[7]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Ursnif has registered itself as a system service in the Registry for automatic execution at system startup.[5]

Enterprise T1132 Data Encoding

Ursnif has used encoded data in HTTP URLs for C2.[2]

Enterprise T1005 Data from Local System

Ursnif has collected files from victim machines, including certificates and cookies.[6]

Enterprise T1074 .001 Data Staged: Local Data Staging

Ursnif has used tmp files to stage gathered information.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

Ursnif has used crypto key information stored in the Registry to decrypt Tor clients dropped to disk.[2]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

Ursnif has used a DGA to generate domain names for C2.[2]

Enterprise T1041 Exfiltration Over C2 Channel

Ursnif has used HTTP POSTs to exfil gathered information.[3][4][2]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Ursnif droppers have used COM properties to execute malware in hidden windows.[7]

Enterprise T1070 .004 Indicator Removal: File Deletion

Ursnif has deleted data staged in tmp files after exfiltration.[3]

Enterprise T1105 Ingress Tool Transfer

Ursnif has dropped payload and configuration files to disk. Ursnif has also been used to download and execute additional payloads.[5][6]

Enterprise T1056 .004 Input Capture: Credential API Hooking

Ursnif has hooked APIs to perform a wide variety of information theft, such as monitoring traffic from browsers.[3]

Enterprise T1559 .001 Inter-Process Communication: Component Object Model

Ursnif droppers have used COM objects to execute the malware's full executable payload.[7]

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

Ursnif has used strings from legitimate system files and existing folders for its file, folder, and Registry entry names.[3]

Enterprise T1112 Modify Registry

Ursnif has used Registry modifications as part of its installation routine.[6][2]

Enterprise T1106 Native API

Ursnif has used `CreateProcessW` to create child processes.[4]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Ursnif droppers execute base64 encoded PowerShell commands.[7]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Ursnif has used an XOR-based algorithm to encrypt Tor clients dropped to disk.[2] Ursnif droppers have also been delivered as password-protected zip files that execute base64 encoded PowerShell commands.[7]

Enterprise T1057 Process Discovery

Ursnif has gathered information about running processes.[3][6]

Enterprise T1055 .005 Process Injection: Thread Local Storage

Ursnif has injected code into target processes via thread local storage callbacks.[3][5][4]

.012 Process Injection: Process Hollowing

Ursnif has used process hollowing to inject into child processes.[4]

Enterprise T1090 Proxy

Ursnif has used a peer-to-peer (P2P) network for C2.[1][2]

.003 Multi-hop Proxy

Ursnif has used Tor for C2.[1][2]

Enterprise T1012 Query Registry

Ursnif has used Reg to query the Registry for installed programs.[3][6]

Enterprise T1091 Replication Through Removable Media

Ursnif has copied itself to and infected removable drives for propagation.[3][8]

Enterprise T1113 Screen Capture

Ursnif has used hooked APIs to take screenshots.[3][6]

Enterprise T1082 System Information Discovery

Ursnif has used Systeminfo to gather system information.[3]

Enterprise T1007 System Service Discovery

Ursnif has gathered information about running services.[3]

Enterprise T1080 Taint Shared Content

Ursnif has copied itself to and infected files in network drives for propagation.[3][8]

Enterprise T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks

Ursnif has used a 30 minute delay after execution to evade sandbox monitoring tools.[8]

Enterprise T1047 Windows Management Instrumentation

Ursnif droppers have used WMI classes to execute PowerShell commands.[7]
