# SideCopy, Group G1008 | MITRE ATT&CK®

Archived: 2026-04-05 13:56:20 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1059 | .005 | Command and Scripting Interpreter: Visual Basic | SideCopy has sent Microsoft Office Publisher documents to victims that have embedded malicious macros that execute an hta file via calling `mshta.exe`.[1] |
| Enterprise | T1584 | .001 | Compromise Infrastructure: Domains | SideCopy has compromised domains for some of their infrastructure, including for C2 and staging malware.[1] |
| Enterprise | T1574 | .001 | Hijack Execution Flow: DLL | SideCopy has used a malicious loader DLL file to execute the `credwiz.exe` process and side-load the malicious payload `Duser.dll`.[1] |
| Enterprise | T1105 | | Ingress Tool Transfer | SideCopy has delivered trojanized executables via spearphishing emails that contacts actor-controlled servers to download malicious payloads.[1] |
| Enterprise | T1036 | .005 | Masquerading: Match Legitimate Resource Name or Location | SideCopy has used a legitimate DLL file name, `Duser.dll` to disguise a malicious remote access tool.[1] |
| Enterprise | T1106 | | Native API | SideCopy has executed malware by calling the API function `CreateProcessW`.[1] |
| Enterprise | T1566 | .001 | Phishing: Spearphishing Attachment | SideCopy has sent spearphishing emails with malicious hta file attachments.[1] |

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1598 | .002 | Phishing for Information: Spearphishing Attachment | SideCopy has crafted generic lures for spam campaigns to collect emails and credentials for targeting efforts.[1] |
| Enterprise | T1518 | | Software Discovery | SideCopy has collected browser information from a compromised host.[1] |
| | | .001 | Security Software Discovery | SideCopy uses a loader DLL file to collect AV product names from an infected host.[1] |
| Enterprise | T1608 | .001 | Stage Capabilities: Upload Malware | SideCopy has used compromised domains to host its malicious payloads.[1] |
| Enterprise | T1218 | .005 | System Binary Proxy Execution: Mshta | SideCopy has utilized `mshta.exe` to execute a malicious hta file.[1] |
| Enterprise | T1082 | | System Information Discovery | SideCopy has identified the OS version of a compromised host.[1] |
| Enterprise | T1614 | | System Location Discovery | SideCopy has identified the country location of a compromised host.[1] |
| Enterprise | T1016 | | System Network Configuration Discovery | SideCopy has identified the IP address of a compromised host.[1] |
| Enterprise | T1204 | .002 | User Execution: Malicious File | SideCopy has attempted to lure victims into clicking on malicious embedded archive files sent via spearphishing campaigns.[1] |