# Operation Sharpshooter, Campaign C0013 | MITRE ATT&CK®

Archived: 2026-04-05 14:25:26 UTC

Enterprise T1583 .006 Acquire Infrastructure: Web Services

For Operation Sharpshooter, the threat actors used Dropbox to host lure documents and their first-stage downloader.[1]

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

During Operation Sharpshooter, a first-stage downloader installed Rising Sun to `%Startup%\mssync.exe` on a compromised host.[1]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

During Operation Sharpshooter, the threat actors used a VBA macro to execute a simple downloader that installed Rising Sun.[1]

Enterprise T1584 .004 Compromise Infrastructure: Server

For Operation Sharpshooter, the threat actors compromised a server they used as part of the campaign's infrastructure.[2]

Enterprise T1587 .001 Develop Capabilities: Malware

For Operation Sharpshooter, the threat actors used the Rising Sun modular backdoor.[1]

Enterprise T1105 Ingress Tool Transfer

During Operation Sharpshooter, additional payloads were downloaded after a target was infected with a first-stage downloader.[1]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

During Operation Sharpshooter, threat actors sent malicious Word OLE documents to victims.[1]

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

During Operation Sharpshooter, threat actors installed Rising Sun in the Startup folder and disguised it as `mssync.exe`.[1]

Enterprise T1106 Native API

During Operation Sharpshooter, the first stage downloader resolved various Windows libraries and APIs, including `LoadLibraryA()`, `GetProcAddress()`, and `CreateProcessA()`.[1]

Enterprise T1055 Process Injection

During Operation Sharpshooter, threat actors leveraged embedded shellcode to inject a downloader into the memory of Word.[3]

Enterprise T1090 Proxy

For Operation Sharpshooter, the threat actors used the ExpressVPN service to hide their location.[2]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

For Operation Sharpshooter, the threat actors staged malicious files on Dropbox and other websites.[1]

Enterprise T1204 .002 User Execution: Malicious File

During Operation Sharpshooter, the threat actors relied on victims executing malicious Microsoft Word or PDF files.[1]

---