Gorgon Group, Group G0078 | MITRE ATT&CK®

Archived: 2026-04-02 10:38:23 UTC

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

Gorgon Group malware can create a .lnk file and add a Registry Run key to establish persistence.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Gorgon Group malware can create a .lnk file and add a Registry Run key to establish persistence.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Gorgon Group malware can use PowerShell commands to download and execute a payload and open a decoy document on the victim's machine.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

Gorgon Group malware can use cmd.exe to download and execute payloads and to execute commands on the system.[1]

.005 Command and Scripting Interpreter: Visual Basic

Gorgon Group has used macros in Spearphishing Attachments as well as executed VBScripts on victim machines. [1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Gorgon Group malware can decode contents from a payload that was Base64 encoded and write the contents to a file.[1]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Gorgon Group has used `-W Hidden` to conceal PowerShell windows by setting the WindowStyle parameter to hidden. [1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Gorgon Group malware can attempt to disable security features in Microsoft Office and Windows Defender using the `taskkill` command.[1]

Enterprise T1105 Ingress Tool Transfer

Gorgon Group malware can download additional files from C2 servers.[1]

Enterprise T1112 Modify Registry

Gorgon Group malware can deactivate security mechanisms in Microsoft Office by editing several keys and values under `HKCU\Software\Microsoft\Office\` .[1]

Enterprise T1106 Native API

Gorgon Group malware can leverage the Windows API call, CreateProcessA(), for execution.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

Gorgon Group has obtained and used tools such as QuasarRAT and Remcos.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Gorgon Group sent emails to victims with malicious Microsoft Office documents attached.[1]

Enterprise T1055 .002 Process Injection: Portable Executable Injection

Gorgon Group malware can download a remote access tool, ShiftyBug, and inject into another process.[1]

.012 Process Injection: Process Hollowing

Gorgon Group malware can use process hollowing to inject one of its trojans into another process.[1]

Enterprise T1204 .002 User Execution: Malicious File

Gorgon Group attempted to get users to launch malicious Microsoft Office attachments delivered via spearphishing emails.[1]

Source: https://attack.mitre.org/groups/G0078/