Confucius, Confucius APT, Group G0142

Archived: 2026-04-05 13:29:23 UTC

Enterprise T1583 .006 Acquire Infrastructure: Web Services

Confucius has obtained cloud storage service accounts to host stolen data.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Confucius has used HTTP for C2 communications.[3]

Enterprise T1119 Automated Collection

Confucius has used a file stealer to steal documents and images with the following extensions: txt, pdf, png, jpg, doc, xls, xlm, odp, ods, odt, rtf, ppt, xlsx, xlsm, docx, pptx, and jpeg.[2]

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

Confucius has dropped malicious files into the startup folder `%AppData%\Microsoft\Windows\Start Menu\Programs\Startup` on a compromised host in order to maintain persistence.[3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Confucius has used PowerShell to execute malicious files and payloads.[2]

.005 Command and Scripting Interpreter: Visual Basic

Confucius has used VBScript to execute malicious code.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Confucius has exfiltrated stolen files to its C2 server.[2]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Confucius has exfiltrated victim data to cloud storage service accounts.[1]

Enterprise T1203 Exploitation for Client Execution

Confucius has exploited Microsoft Office vulnerabilities, including CVE-2015-1641, CVE-2017-11882, and CVE-2018-0802.[3][1]

Enterprise T1083 File and Directory Discovery

Confucius has used a file stealer that checks the Document, Downloads, Desktop, and Picture folders for documents and images with specific extensions.[2]

Enterprise T1105 Ingress Tool Transfer

Confucius has downloaded additional files and payloads onto a compromised host following initial access.[3][2]

Enterprise T1680 Local Storage Discovery

Confucius has used a file stealer that can examine system drives, including those other than the C drive.[2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Confucius has crafted and sent victims malicious attachments to gain initial access.[3]

.002 Phishing: Spearphishing Link

Confucius has sent malicious links to victims through email campaigns.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Confucius has created scheduled tasks to maintain persistence on a compromised host.[2]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

Confucius has used mshta.exe to execute malicious VBScript.[1]

Enterprise T1221 Template Injection

Confucius has used a weaponized Microsoft Word document with an embedded RTF exploit.[3]

Enterprise T1204 .001 User Execution: Malicious Link

Confucius has lured victims into clicking on a malicious link sent through spearphishing.[2]

.002 User Execution: Malicious File

Confucius has lured victims to execute malicious attachments included in crafted spearphishing emails related to current topics.[3]
