Cobalt Group, GOLD KINGSWOOD, Cobalt Gang, Cobalt Spider, Group G0080

Archived: 2026-04-05 17:32:46 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

Cobalt Group has bypassed UAC.[4]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Cobalt Group has used HTTPS for C2.[1][3][4]

.004 Application Layer Protocol: DNS

Cobalt Group has used DNS tunneling for C2.[1][3][4]

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

Cobalt Group has used Registry Run keys for persistence. The group has also set a Startup path to launch the PowerShell shell command and download Cobalt Strike.[4]

Enterprise T1037 .001 Boot or Logon Initialization Scripts: Logon Script (Windows)

Cobalt Group has added persistence by registering the file name for the next stage malware under `HKCU\Environment\UserInitMprLogonScript`.[11]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Cobalt Group has used powershell.exe to download and execute scripts.[1][2][3][4][7][12]

.003 Command and Scripting Interpreter: Windows Command Shell

Cobalt Group has used a JavaScript backdoor that is capable of launching cmd.exe to execute shell commands.[11] The group has used an exploit toolkit known as Threadkit that launches .bat files.[1][2][4][11][13][12]

.005 Command and Scripting Interpreter: Visual Basic

Cobalt Group has sent Word OLE compound documents with malicious obfuscated VBA macros that will run upon user execution.[1][2][4][11][13][12]

.007 Command and Scripting Interpreter: JavaScript

Cobalt Group has executed JavaScript scriptlets on the victim's machine.[1][2][4][11][13][12]

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

Cobalt Group has created new services to establish persistence.[4]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Cobalt Group has used the Plink utility to create SSH tunnels.[4]

Enterprise T1203 Exploitation for Client Execution

Cobalt Group had exploited multiple vulnerabilities for execution, including Microsoft's Equation Editor (CVE-2017-11882), an Internet Explorer vulnerability (CVE-2018-8174), CVE-2017-8570, CVE-2017-0199, and CVE-2017-8759.[1][2][3][5][6][7][10][12]

Enterprise T1068 Exploitation for Privilege Escalation

Cobalt Group has used exploits to increase their levels of rights and privileges.[4]

Enterprise T1070 .004 Indicator Removal: File Deletion

Cobalt Group deleted the DLL dropper from the victim's machine to cover their tracks.[1]

Enterprise T1105 Ingress Tool Transfer

Cobalt Group has used public sites such as github.com and sendspace.com to upload files and then download them to victim computers.[2][3] The group's JavaScript backdoor is also capable of downloading files.[11]

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

Cobalt Group has sent malicious Word OLE compound documents to victims.[1]

Enterprise T1046 Network Service Discovery

Cobalt Group leveraged an open-source tool called SoftPerfect Network Scanner to perform network scanning.[2][3][4]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Cobalt Group obfuscated several scriptlets and code used on the victim's machine, including through use of XOR and RC4.[1][11]

Enterprise T1588 .002 Obtain Capabilities: Tool

Cobalt Group has obtained and used a variety of tools including Mimikatz, PsExec, Cobalt Strike, and SDelete.[3]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Cobalt Group has sent spearphishing emails with various attachment types to corporate and personal email accounts of victim organizations. Attachment types have included .rtf, .doc, .xls, archives containing LNK files, and password protected archives containing .exe and .scr executables.[1][2][3][4][5][6][13][12]

.002 Phishing: Spearphishing Link

Cobalt Group has sent emails with URLs pointing to malicious documents.[1][9]

Enterprise T1055 Process Injection

Cobalt Group has injected code into trusted processes.[4]

Enterprise T1572 Protocol Tunneling

Cobalt Group has used the Plink utility to create SSH tunnels.[1][3][4]

Enterprise T1219 Remote Access Tools

Cobalt Group used the Ammyy Admin tool as well as TeamViewer for remote access, including to preserve remote access if a Cobalt Strike module was lost.[2][3][4]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Cobalt Group has used Remote Desktop Protocol to conduct lateral movement.[4]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Cobalt Group has created Windows tasks to establish persistence.[4]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Cobalt Group used a JavaScript backdoor that is capable of collecting a list of the security solutions installed on the victim's machine.[11]

Enterprise T1195 .002 Supply Chain Compromise: Compromise Software Supply Chain

Cobalt Group has compromised legitimate web browser updates to deliver a backdoor. [14]

Enterprise T1218 .003 System Binary Proxy Execution: CMSTP

Cobalt Group has used the command `cmstp.exe /s /ns C:\Users\ADMINI~W\AppData\Local\Temp\XKNqbpzl.txt` to bypass AppLocker and launch a malicious script.[1][11][13]

.008 System Binary Proxy Execution: Odbcconf

Cobalt Group has used `odbcconf` to proxy the execution of malicious DLL files.[12]

.010 System Binary Proxy Execution: Regsvr32

Cobalt Group has used regsvr32.exe to execute scripts.[1][11][12]

Enterprise T1204 .001 User Execution: Malicious Link

Cobalt Group has sent emails containing malicious links that require users to execute a file or macro to infect the victim machine.[1][13][9]

.002 User Execution: Malicious File

Cobalt Group has sent emails containing malicious attachments that require users to execute a file or macro to infect the victim machine.[1][13]

Enterprise T1220 XSL Script Processing

Cobalt Group used msxsl.exe to bypass AppLocker and to invoke Jscript code from an XSL file.[1]

Source: https://attack.mitre.org/groups/G0080/