Patchwork, Hangover Group, Dropping Elephant, Chinastrats, MONSOON, Operation Hangover, Group G0040

Archived: 2026-04-02 11:34:57 UTC

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

Patchwork bypassed User Access Control (UAC).[1]

Enterprise T1560 Archive Collected Data

Patchwork encrypted the collected files' path with AES and then encoded them with base64.[3]

Enterprise T1119 Automated Collection

Patchwork developed a file stealer to search C:\ and collect files with certain extensions. Patchwork also executed a script to enumerate all drives, store them as a list, and upload generated files to the C2 server.[3]

Enterprise T1197 BITS Jobs

Patchwork has used BITS jobs to download malicious payloads.[6]

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

Patchwork has added the path of its second-stage malware to the startup folder to achieve persistence. One of its file stealers has also persisted by adding a Registry Run key.[1][3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Patchwork used PowerSploit to download payloads, run a reverse shell, and execute malware on the victim's machine.[1][3]

.003 Command and Scripting Interpreter: Windows Command Shell

Patchwork ran a reverse shell with Meterpreter.[1] Patchwork used JavaScript code and .SCT files on victim machines.[3][4]

.005 Command and Scripting Interpreter: Visual Basic

Patchwork used Visual Basic Scripts (VBS) on victim machines.[3][4]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Patchwork dumped the login data database from `\AppData\Local\Google\Chrome\User Data\Default\Login Data`.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Patchwork used Base64 to encode C2 traffic.[1]

Enterprise T1005 Data from Local System

Patchwork collected and exfiltrated files from the infected system.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Patchwork copied all targeted files to a directory called index that was eventually uploaded to the C&C server.[3]

Enterprise T1587 .002 Develop Capabilities: Code Signing Certificates

Patchwork has created self-signed certificates from fictitious and spoofed legitimate software companies that were later used to sign malware.[6]

Enterprise T1189 Drive-by Compromise

Patchwork has used watering holes to deliver files with exploits to initial victims.[2][4]

Enterprise T1203 Exploitation for Client Execution

Patchwork uses malicious documents to deliver remote execution exploits as part of. The group has previously exploited CVE-2017-8570, CVE-2012-1856, CVE-2014-4114, CVE-2017-0199, CVE-2017-11882, and CVE-2015-1641.[1][8][2][5][3][4][6]

Enterprise T1083 File and Directory Discovery

A Patchwork payload has searched all fixed drives on the victim for files matching a specified list of extensions.[1][3]

Enterprise T1574 .001 Hijack Execution Flow: DLL

A Patchwork .dll that contains BADNEWS is loaded and executed using DLL side-loading.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

Patchwork removed certain files and replaced them so they could not be retrieved.[3]

Enterprise T1105 Ingress Tool Transfer

Patchwork payloads download additional files from the C2 server.[8][3]

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

Patchwork leveraged the DDE protocol to deliver their malware.[3]

Enterprise T1680 Local Storage Discovery

Patchwork enumerated all available drives on the victim's machine.[1][3]

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

Patchwork installed its payload in the startup programs folder as "Baidu Software Update." The group also adds its second stage payload to the startup programs as "Net Monitor."[1] They have also dropped QuasarRAT binaries as files named microsoft_network.exe and crome.exe.[4]

Enterprise T1112 Modify Registry

A Patchwork payload deletes Resiliency Registry keys created by Microsoft Office applications in an apparent effort to trick users into thinking there were no issues during application runs.[3]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Patchwork apparently altered NDiskMonitor samples by adding four bytes of random letters in a likely attempt to change the file hashes.[3]

.002 Obfuscated Files or Information: Software Packing

A Patchwork payload was packed with UPX.[8]

.005 Obfuscated Files or Information: Indicator Removal from Tools

Patchwork apparently altered NDiskMonitor samples by adding four bytes of random letters in a likely attempt to change the file hashes.[3]

.010 Obfuscated Files or Information: Command Obfuscation

Patchwork has obfuscated a script with Crypto Obfuscator.[3]

Enterprise T1588 .002 Obtain Capabilities: Tool

Patchwork has obtained and used open-source tools such as QuasarRAT.[4]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Patchwork has used spearphishing with an attachment to deliver files with exploits to initial victims.[1][8][3][4]

.002 Phishing: Spearphishing Link

Patchwork has used spearphishing with links to deliver files with exploits to initial victims.[2][3][6]

Enterprise T1598 .003 Phishing for Information: Spearphishing Link

Patchwork has used embedded image tags (known as web bugs) with unique, per-recipient tracking links in their emails for the purpose of identifying which recipients opened messages.[4]

Enterprise T1055 .012 Process Injection: Process Hollowing

A Patchwork payload uses process hollowing to hide the UAC bypass vulnerability exploitation inside svchost.exe.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Patchwork attempted to use RDP to move laterally.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

A Patchwork file stealer can run a TaskScheduler DLL to add persistence.[3]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Patchwork scanned the "Program Files" directories for a directory with the string "Total Security" (the installation path of the "360 Total Security" antivirus tool).[1]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Patchwork has signed malware with self-signed certificates from fictitious and spoofed legitimate software companies.[6]

Enterprise T1082 System Information Discovery

Patchwork collected the victim computer name, OS version, and architecture type and sent the information to its C2 server.[1][3]

Enterprise T1033 System Owner/User Discovery

Patchwork collected the victim username and whether it was running as admin, then sent the information to its C2 server.[1][3]

Enterprise T1204 .001 User Execution: Malicious Link

Patchwork has used spearphishing with links to try to get users to click, download and open malicious files.[2][3][4][6]

.002 User Execution: Malicious File

Patchwork embedded a malicious macro in a Word document and lured the victim to click on an icon to execute the malware.[3][4]

Enterprise T1102 .001 Web Service: Dead Drop Resolver

Patchwork hides base64-encoded and encrypted C2 server locations in comments on legitimate websites.[8]
