APT37, InkySquid, ScarCruft, Reaper, Group123, TEMP.Reaper, Ricochet Chollima, Group G0067

Archived: 2026-04-02 12:26:21 UTC

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

APT37 has a function in the initial dropper to bypass Windows UAC in order to execute the next payload with higher privileges.[5]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

APT37 uses HTTPS to conceal C2 communications.[3]

Enterprise T1123 Audio Capture

APT37 has used an audio capturing utility known as SOUNDWAVE that captures microphone input.[1]

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

APT37's has added persistence via the Registry key `HKCU\Software\Microsoft\CurrentVersion\Run\` .[1][3]

Enterprise T1059 Command and Scripting Interpreter

APT37 has used Ruby scripts to execute payloads.[7]

.003 Windows Command Shell

APT37 has used the command-line interface.[1][3]

.005 Visual Basic

APT37 executes shellcode and a VBA script to decode Base64 strings.[3]

.006 Python

APT37 has used Python scripts to execute payloads.[7]

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

APT37 has used a credential stealer known as ZUMKONG that can harvest usernames and passwords stored in browsers.[1]

Enterprise T1005 Data from Local System

APT37 has collected data from victims' local systems.[1]

Enterprise T1561 .002 Disk Wipe: Disk Structure Wipe

APT37 has access to destructive malware that is capable of overwriting a machine's Master Boot Record (MBR).[1][3]

Enterprise T1189 Drive-by Compromise

APT37 has used strategic web compromises, particularly of South Korean websites, to distribute malware. The group has also used torrent file-sharing sites to more indiscriminately disseminate malware to victims. As part of their compromises, the group has used a Javascript based profiler called RICECURRY to profile a victim's web browser and deliver malicious code accordingly.[2][1][4]

Enterprise T1203 Exploitation for Client Execution

APT37 has used exploits for Flash Player (CVE-2016-4117, CVE-2018-4878), Word (CVE-2017-0199), Internet Explorer (CVE-2020-1380 and CVE-2020-26411), and Microsoft Edge (CVE-2021-26411) for execution.[2][1][3][4]

Enterprise T1105 Ingress Tool Transfer

APT37 has downloaded second stage malware from compromised websites.[1][5][4][7]

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

APT37 has used Windows DDE for execution of commands and a malicious VBS.[2]

Enterprise T1036 .001 Masquerading: Invalid Code Signature

APT37 has signed its malware with an invalid digital certificates listed as "Tencent Technology (Shenzhen) Company Limited."[2]

Enterprise T1106 Native API

APT37 leverages the Windows API calls: VirtualAlloc(), WriteProcessMemory(), and CreateRemoteThread() for process injection.[3]

Enterprise T1027 Obfuscated Files or Information

APT37 obfuscates strings and payloads.[3][5][7]

.003 Steganography

APT37 uses steganography to send images to users that are embedded with shellcode.[3][5]

Enterprise T1120 Peripheral Device Discovery

APT37 has a Bluetooth device harvester, which uses Windows Bluetooth APIs to find information on connected Bluetooth devices. [5]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

APT37 delivers malware using spearphishing emails with malicious HWP attachments.[1][3][5]

Enterprise T1057 Process Discovery

APT37's Freenki malware lists running processes using the Microsoft Windows API.[3]

Enterprise T1055 Process Injection

APT37 injects its malware variant, ROKRAT, into the cmd.exe process.[3]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

APT37 has created scheduled tasks to run malicious scripts on a compromised host.[7]

Enterprise T1082 System Information Discovery

APT37 collects the computer name, the BIOS model, and execution path.[3]

Enterprise T1033 System Owner/User Discovery

APT37 identifies the victim username.[3]

Enterprise T1529 System Shutdown/Reboot

APT37 has used malware that will issue the command `shutdown /r /t 1` to reboot a system after wiping its MBR.[3]

Enterprise T1204 .002 User Execution: Malicious File

APT37 has sent spearphishing attachments attempting to get a user to open them.[1]

Enterprise T1102 .002 Web Service: Bidirectional Communication

APT37 leverages social networking sites and cloud platforms (AOL, Twitter, Yandex, Mediafire, pCloud, Dropbox, and Box) for C2.[1][3]
