Darkhotel, DUBNIUM, Zigzag Hail, Group G0012

Archived: 2026-04-05 12:37:00 UTC

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

Darkhotel has been known to establish persistence by adding programs to the Run Registry key.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Darkhotel has dropped an mspaint.lnk shortcut to disk which launches a shell script that downloads and executes a file.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Darkhotel has decrypted strings and imports using RC4 during execution.[2][6]

Enterprise T1189 Drive-by Compromise

Darkhotel used embedded iframes on hotel login portals to redirect selected victims to download malware.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Darkhotel has used AES-256 and 3DES for C2 communications.[6]

Enterprise T1203 Exploitation for Client Execution

Darkhotel has exploited Adobe Flash vulnerability CVE-2015-8651 for execution.[4]

Enterprise T1083 File and Directory Discovery

Darkhotel has used malware that searched for files with specific patterns.[6]

Enterprise T1105 Ingress Tool Transfer

Darkhotel has used first-stage payloads that download additional malware from C2 servers.[4]

Enterprise T1056 .001 Input Capture: Keylogging

Darkhotel has used a keylogger.[1]

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

Darkhotel has used malware that is disguised as a Secure Shell (SSH) tool.[4]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Darkhotel has obfuscated code using RC4, XOR, and RSA.[2][6]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Darkhotel has sent spearphishing emails with malicious RAR and .LNK attachments.[2][6]

Enterprise T1057 Process Discovery

Darkhotel malware can collect a list of running processes on a system.[2]

Enterprise T1091 Replication Through Removable Media

Darkhotel's selective infector modifies executables stored on removable media as a method of spreading across computers.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Darkhotel has searched for anti-malware strings and anti-virus processes running on the system.[2][4]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Darkhotel has used code-signing certificates on its malware that are either forged due to weak keys or stolen. Darkhotel has also stolen certificates and signed backdoors and downloaders with them.[1][2]

Enterprise T1082 System Information Discovery

Darkhotel has collected the hostname, OS version, service pack version, and the processor architecture from the victim’s machine.[2][6]

Enterprise T1016 System Network Configuration Discovery

Darkhotel has collected the IP address and network adapter information from the victim’s machine.[2][6]

Enterprise T1124 System Time Discovery

Darkhotel malware can obtain system time from a compromised host.[8]

Enterprise T1080 Taint Shared Content

Darkhotel used a virus that propagates by infecting executables stored on shared drives.[1]

Enterprise T1204 .002 User Execution: Malicious File

Darkhotel has sent spearphishing emails in an attempt to lure users into clicking on a malicious attachments.[2][6]

Enterprise T1497 Virtualization/Sandbox Evasion

Darkhotel malware has employed just-in-time decryption of strings to evade sandbox detection.[8]

.001 System Checks

Darkhotel malware has used a series of checks to determine if it's being analyzed; checks include the length of executable names, if a filename ends with `.Md5.exe`, and if the program is executed from the root of the C:\ drive, as well as checks for sandbox-related libraries.[8][4]

.002 User Activity Based Checks

Darkhotel has used malware that repeatedly checks the mouse cursor position to determine if a real user is on the system.[8]
