Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:38:18 UTC

APT group: DarkHotel

Names	DarkHotel *(Kaspersky)* APT-C-06 *(Qihoo 360)* SIG25 *(NSA)* Dubnium *(Microsoft)* Fallout Team *(FireEye)* Shadow Crane *(CrowdStrike)* CTG-1948 *(SecureWorks)* Tungsten Bridge *(SecureWorks)* ATK 52 *(Thales)* Higaisa *(Tencent)* T-APT-02 *(Tencent)* Luder *(?)* Zigzag Hail *(Microsoft)* TieOnJoe *(?)* Purple Pygmy *(PWC)* G0012 *(MITRE)* G0126 *(MITRE)*
Country	South Korea
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2007
Description	(SecurityWeek) The activities of the DarkHotel advanced persistent threat (APT) actor came to light in November 2014, when Kaspersky published a report detailing a sophisticated cyberespionage campaign targeting business travelers in the Asia-Pacific region. The group has been around for nearly a decade and some researchers believe its members are Korean speakers. The attackers targeted their victims using several methods, including through their hotel's Wi-Fi, zero-day exploits and peer-to-peer (P2P) file sharing websites. Nearly one year later, the threat group was observed using new attack techniques and an exploit leaked from Italian spyware maker Hacking Team. DarkHotel victims have been spotted in several countries, including North Korea, Russia, South Korea, Japan, Bangladesh, Thailand, Taiwan, China, the United States, India, Mozambique, Indonesia and Germany. Up until recently, the attacks appeared to focus on company executives, researchers and development personnel from sectors such as defense industrial base, military, energy, government, NGOs, electronics manufacturing, pharmaceutical, and medical.

	In more recent DarkHotel attacks it has dubbed “Inexsmar,” security firm Bitdefender said the hackers targeted political figures, and they appeared to be using some new methods.	
Observed	Sectors: Defense, Energy, Government, Healthcare, Hospitality, NGOs, Pharmaceutical, Research, Technology and Chinese institutions abroad. Countries: Afghanistan, Armenia, Bangladesh, Belgium, China, Ethiopia, Germany, Greece, Hong Kong, India, Indonesia, Malaysia, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Lebanon, Malaysia, Mexico, Mozambique, North Korea, Pakistan, Philippines, Russia, Saudi Arabia, Serbia, Singapore, South Korea, Taiwan, Tajikistan, Thailand, Turkey, UAE, UK, USA, Vietnam and others.	
Tools used	Asruex, DarkHotel, DmaUp3.exe, GreezeBackdoor, Karba, msieckc.exe, Nemim, Pioneer, Ramsay, Retro, Tapaoux and various 0-days from the Hacking Team breach.	
Operations performed	2010	Operation “DarkHotel” Target: The travelers are often top executives from a variety of industries doing business and outsourcing in the APAC region. Targets have included CEOs, senior vice presidents, sales and marketing directors and top R&D staff. Method: spear-phishing targets with highly advanced Flash zero-day exploits that effectively evade the latest Windows and Adobe defenses, and yet they also imprecisely spread among large numbers of vague targets with peer-to-peer spreading tactics. Moreover, this crew’s most unusual characteristic is that for several years the Darkhotel APT has maintained a capability to use hotel networks to follow and hit selected targets as they travel around the world. <https://securelist.com/the-darkhotel-apt/66779/> <https://www.recordedfuture.com/dark-hotel-malware/>
	2015	Darkhotel’s attacks in 2015 <https://securelist.com/darkhotels-attacks-in-2015/71713/>
	Dec 2015	Operation “Daybreak” Method: Uses Flash zero-day exploit for CVE-2015-8651. Note: not the same operation as Reaper, APT 37, Ricochet Chollima, ScarCruft’s Operation “Daybreak”.
	Sep 2016	Operation “Inexsmar” Target: seems to be used in a campaign that targets political figures rather than the usual corporate research and development personnel, CEOs and other senior corporate officials. Method: This attack uses a new payload delivery mechanism rather than the consecrated zero-day exploitation techniques, blending social engineering with a relatively complex Trojan to infect its selected pool of victims. <https://labs.bitdefender.com/2017/07/inexsmar-an-unusual-darkhotel-campaign/>
	Apr 2018	Analysis of CVE-2018-8174 VBScript 0day and APT actor related to Office targeted attack <https://blog.360totalsecurity.com/en/analysis-cve-2018-8174-vbscript-0day-apt-actor-related-office-targeted-attack/>
	Aug 2018	Darkhotel APT is back: Zero-day vulnerability in Microsoft VBScript is exploited <https://blog.360totalsecurity.com/en/darkhotel-apt-is-back-zero-day-vulnerability-in-

	microsoft-vbscript-is-exploited/>
Jan 2020	Darkhotel uses a new Zero-day vulnerability in the Internet Explorer scripting engine <http://www.geekpark.net/news/254734>
Mar 2020	On March 15, 2020, ATR identified a malicious .lnk file that utilizes an infection chain similar to other known APT groups. This campaign was found to use C2 infrastructure that overlaps with the Korea-based APT group, Higaisia. The lure document, dropped by the .lnk file, was downloaded from the World Health Organization website, and is likely being used to target English-speaking individuals and entities. <https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication#When:14:00:00Z>
Mar 2020	Since March this year, more than 200 VPN servers have been compromised and many Chinese institutions abroad were under attack. In early April, the attack spread to government agencies in Beijing and Shanghai. <http://blogs.360.cn/post/APT_Darkhotel_attacks_during_coronavirus_pandemic.html>
May 2020	Ramsay: A cyber-spionage toolkit tailored for air-apped networks <https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/>
May 2020	In this latest incident, Higaisa used a malicious shortcut file ultimately responsible for creating a multi-stage attack that consists of several malicious scripts, payloads and decoy PDF documents. <https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/>
May 2020	Operation “The Gh0st Remains the Same” In this engagement, the victims received a compressed RAR folder that contained trojanized files. If the malicious files were engaged, they displayed decoy web pages associated with the software company “Zeplin”. <https://blog.prevailion.com/2020/06/the-gh0st-remains-same8.html>
May 2020	Operation “PowerFall” In May 2020, Kaspersky technologies prevented an attack on a South Korean company by a malicious script for Internet Explorer. Closer analysis revealed that the attack used a previously unknown full chain that consisted of two zero-day exploits: a remote code execution exploit for Internet Explorer and an elevation of privilege exploit for Windows. <https://securelist.com/ie-and-windows-zero-day-operation-powerfall/97976/> <https://securelist.com/operation-powerfall-cve-2020-0986-and-variants/98329/>
Nov 2021	New DarkHotel APT attack chain identified <https://www.zscaler.com/blogs/security-research/new-darkhotel-apt-attack-chain-identified>
Dec 2021	Suspected DarkHotel APT activity update <https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/suspected-darkhotel-apt-activity-update.html>

	2023	Attack Upgraded: Disclosure of DarkHotel Organization's Latest RPC Attack Components <https://paper.seebug.org/3315/>
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070903/darkhotel_kl_07.11.pdf> <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070901/darkhotelappendixindicators_kl.pdf> <https://www.securityweek.com/darkhotel-apt-uses-new-methods-target-politicians>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0012/> <https://attack.mitre.org/groups/G0126/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
