Deep-dive: The DarkHotel APT


blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html

BushidoToken

PART 1: DARKHOTEL

DarkHotel is a sophisticated and active advanced persistent threat (APT) group. It's highly capable and is known for finding and taking advantage of previously unknown vulnerabilities in common software also known as a 0day. It is a well-established group that has been active since 2007, are known Korean-speakers, and are working on behalf of a nation state.

DarkHotel was first disclosed in 2014 and is also known as DUBNIUM, Black Shop, Fallout Team, Karba, Luder, Nemim, Nemain, Tapaoux, Pioneer, Shadow Crane, APT-C-06, and TUNGSTEN BRIDGE. From the NSA's sigs.py script (also known as Territorial Dispute or TeDi) DarkHotel is signature number 25 (SIG25). Malware associated with DarkHotel includes Asruex, Parastic Beast, Inexsmar, Retro backdoor, Gh0st RAT, and the new Ramsay toolkit. Vulnerabilities leveraged in its 0day exploits include CVE-2018-8174, CVE-

2018-8373, CVE-2019-1458, CVE-2019-13720, CVE-2019-17026, and CVE-2020-0674. DarkHotel also often exploits CVE-2017-8570 and CVE-2017-11882, high-risk well-known issues in Microsoft Office.

DarkHotel appropriately earned its name infecting the **WiFi networks (WLANs)** of hotels typically used by business executives. This was in effort to compromise their devices such as smartphones and laptops that may potentially contain **intellectual property** and the individual's emails or contact lists. The WLAN of the hotels are compromised via leveraging stolen certificates, deploying .HTA files that masquerades as software updates containing the malware. The WiFi routers themselves are taken over either by remotely exploiting vulnerabilities or by gaining physical access inside the targeted hotels. As DarkHotel is state-sponsored it more than likely has capable human operators to deploy during its campaign.

This APT has targeted a wide array of countries in Asia, Europe, North America, and Africa. It primarily focuses on North Korea, South Korea, Japan, and China. Organisations in sectors such as telecommunications, manufacturing, finance, pharmaceutical, chemicals, automotive, defence, law enforcement, militaries, and NGOs have all been compromised by DarkHotel.

DarkHotel has repeatedly demonstrated its capabilities of **developing exploits for 0day vulnerabilities** in software such as Google Chrome, Mozilla Firefox, Internet Explorer, and Windows Kernel. The exploits are leveraged to deliver malware that can provide backdoor access and remote control over the target device. DarkHotel hides its malware behind layers of encryption, obfuscation, and only deploys it in singular attacks so as not to expose its

stolen certificates or 0day vulnerabilities. This group is a well-established expert at spear-phishing where it has researched its targets using **OSINT** and potentially **HUMINT**. Its lures have included political news, changes in legislation, and other business news.

In November 2014, we saw the first details of the specific activities of the DarkHotel APT. Kaspersky published a report detailing a sophisticated cyber-espionage 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. In 2015, it was found that DarkHotel was more than likely exploiting a leaked 0day vulnerability from the Italian offensive security firm, Hacking Team. DarkHotel used spear-phishing emails with .RAR archives that appear to hold a harmless-looking .jpg file. If opened, MS paint is launched and its malware is executed in the background.

In May 2018, DarkHotel was found to be responsible for distributing a 0day for **CVE-2018-8174**. This attack used URLMoniker to invoke Internet Explorer via Microsoft Word while ignoring the victim's default browser settings - a previously unknown technique. The group also leveraged **CVE-2018-8373** later that same year.

In November 2019, a threat campaign was discovered, dubbed **'Operation WizardOpium'**, which exploited a vulnerability in Google's Chrome Browser, tracked as **CVE-2019-13720**. The exploit was deployed on a Korean-language news portal, the site's main page had malicious JavaScript injected into it. No threat group has been linked directly to Operation WizardOpium, but similarities in code samples have been correlated with both the Lazarus and DarkHotel APTs. Part of the attacks included a Microsoft Windows privilege escalation 0day exploit - which was later assigned **CVE-2019-1458** - that utilised the win32k component of the Windows kernel. This bug, CVE-2019-1458, meant that the attackers could bypass detection systems on Google Chrome's sandbox to deploy the other 0day exploit for CVE-2019-13720. [1]

More recently, ESET uncovered a previously unreported cyber-espionage toolkit, dubbed **Ramsa**y, that is tailored for collection and exfiltration of sensitive documents and is capable of operating within air-gapped networks. It shares similarities with the **Retro backdoor** and is linked to DarkHotel. [2]

Tencent has further analysed the **Ramsay** attacks and cross-analysed the IOCs with campaigns it has tracked in the past. Interestingly, these attacks and those related to the Retro backdoor go as far back as 18 years ago and later incorporated the Asruex backdoor

to attack isolated networks since 2015. Tencent has linked these attacks to DarkHotel, a threat group that it claims is allegedly working for the **National Intelligence Service of the South Korean government**. [3]

The DarkHotel threat group has launched a large campaign targeting Chinese government agencies and their employees. The attacks began in March, and are thought to be using coronavirus-themed lures. The threat actors are using a 0day vulnerability (tracked as SRC-2020-281) in **Sangfor SSL VPN** servers to provide remote access to enterprise and government networks. [4]

Security research group RedDrip also found that the DarkHotel threat group developed a new exploit for another Internet Explorer (IE) vulnerability, **CVE-2019-1367**, to target China. At the time of reporting, the malicious file being used to exploit this flaw is currently detected by 18 out of 57 engines on VirusTotal. [5, 6]

In April 2020, JPCERT found that an APT group was exploiting two vulnerabilities patched earlier this year in Firefox and Internet Explorer (IE). These attacks have mostly been aimed at China and Japan. The first flaw affects the Firefox browser and is tracked as **CVE-2019-17026**. The second, designated **CVE-2020-0674**, is a remote code execution (RCE) flaw in Internet Explorer. Both bugs were patched in January and February 2020. Both vulnerabilities were used as part of a campaign aimed at Chinese government agencies and attributed to the DarkHotel APT. This campaign delivered the **Gh0st RAT** malware onto compromised devices. [7]

Threat actors recently attempted to break into the systems of the **World Health Organization (WHO)**. The organisation reported a significant increase in attacks against it since the start of the coronavirus pandemic. The most recent activity was observed around 13 March, when a group of malicious actors launched a fake site impersonating the WHO's internal email system. It has not be confirmed who is exactly responsible for the attack but researchers believe that it was the DarkHotel threat group. Further, Kaspersky researchers found that the same infrastructure was also used in targeting other healthcare and humanitarian organisations. [8]

PART 2: STARCRUFT

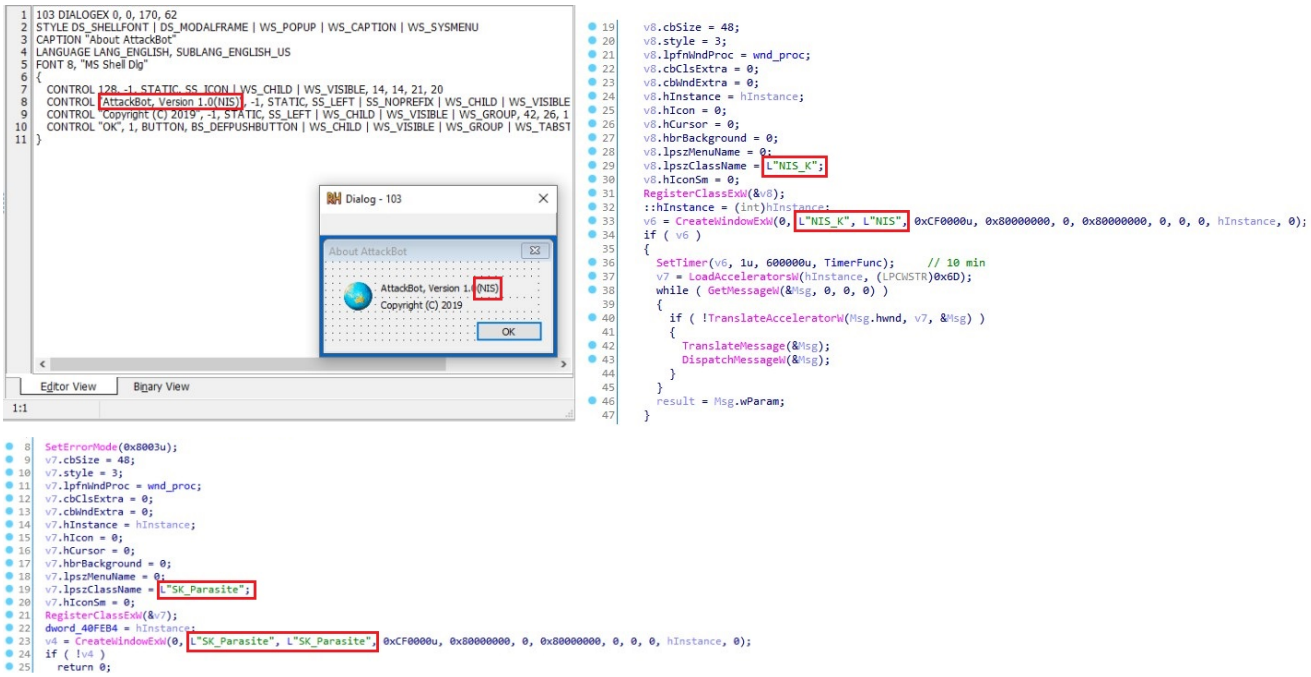
In mid-2019 ScarCruft APT was also dislcosed by Kaspersky researchers. Their investigation led to uncovering that it's another Korean-speaking threat actor with several connections to DarkHotel. StarCruft became known for creating **new tools and techniques to identify Bluetooth devices**. These are used for information gathering campaigns and finding targets.

StarCruft also developed a new method to steal data from smartphones and created malware that could **fingerprint Bluetooth devices** using the **Windows Bluetooth API**. Interestingly, the group's targets include investment and trading companies in Vietnam and Russia that have links to North Korea, along with organisations based in Hong Kong and North Korea. [1, 2]

PART 3: HIGAISA

Late last year, a new APT was publicly disclosed by Tencent, dubbed Higaisa. It was initially thought that the group was North Korean, but researchers concluded that Higaisa instead **originated from South Korea**. The Higaisa APT's main targets have been government, diplomatic, and trade organisations with links to North Korea. It has carried out attacks in China, Japan, Russia, Poland, and other nation states. Higaisa is an evolving threat as it began by distributing executable files in an unsophisticated way. Now, however, the group leverages exploits and complex multi-stage infection chains with advanced defence evasion techniques.

More recently **COVID-19-themed phishing lures** have been linked to Higaisa. The decoy document used in the attacks, an LNK file disguised as a PDF, contains a **World Health Organisation (WHO)** situation report regarding the spread of COVID-19. If opened, arbitrary commands are executed to download an encrypted payload to initiate the infection chain. After several stages of obfuscated payloads, the compromised device is connected to Higaisa’s C&C server. Other malware observed in the attacks includes **Gh0st RAT** that provides backdoor access and remote control for further post-exploitation activities. A simple infostealer is used to collect system information that also facilitates the execution of console commands and relays the responses to the C&C server. Newer Higaisa attacks now leverage the **Zeplin collaborative platform** in more decoy **PDFs disguised as LNK files** that also deliver Gh0st RAT.



Interestingly, PT Security researchers found that two of the classes in Higaisa APT's malware code were named **“SK_Parasite”** and **“NIS_K”**. The researchers speculate that these could reference the South Korean film Parasite and the National Intelligence Service (NIS) of the Republic of Korea. Alone, these are insufficient to draw firm conclusions; however, they can be seen as circumstantial evidence of a connection with South Korea.[1, 2, 3]

CONCLUSION:

Little is known about South Korea’s cyber capabilities and nothing has been confirmed. However, DarkHotel has been linked to both Higaisa and StarCruft, all of them have some connection to South Korea in one way or another. All share similar targets, strategies, and campaigns have led security researchers to conclude that the three groups either work alongside one another or are the same group using new tactics.

DarkHotel is one of the most dangerous and active APT actors on the current threat landscape. There is currently not enough evidence to confidently say DarkHotel belongs to the NIS of the ROK, as APT actors often purposely scatter false flags in their code to lead researchers down a rabbit hole.

Nonetheless, DarkHotel's ability to consistently find 0day vulnerabilities and develop exploits for them is a major security concern for governments and businesses worldwide. All organisations, specifically those with business or diplomatic relationships with South Korea must remain cautious of this sophisticated APT, along with the well-established APTs from North Korea such as Lazarus, Kimsuky, Konni, and Reaper.

Kaspersky video on Dark Hotel (2014)

Watch Video At:

https://youtu.be/HQpGzivvtqg

IOCs: https://otx.alienvault.com/browse/pulses?q=DarkHotel

Sources:

https://malpedia.caad.fkie.fraunhofer.de/actor/darkhotel

https://securelist.com/the-darkhotel-apt/66779/

https://securelist.com/the-zero-day-exploits-of-operation-wizardopium/97086/

https://s.tencent.com/research/report/1000.html

https://s.tencent.com/research/report/741.html

https://twitter.com/RedDrip7/status/1247737928953946112

https://twitter.com/RedDrip7/status/1222887262234394624

https://www.securityweek.com/darkhotel-apt-uses-hacking-team-exploit-target-specific-systems

https://www.securityweek.com/darkhotel-apt-uses-new-methods-target-politicians

https://www.microsoft.com/security/blog/2016/06/09/reverse-engineering-dubnium-2/3/?source=mmpc

https://teamt5.org/newsroom/2020/05/27/teamt5-and-macnica-networks-release-joint-project-on-2019-s-apt-attacks-in-japan.html

https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

http://blogs.360.cn/post/APT_Darkhotel_attacks_during_coronavirus_pandemic.html

https://www.virustotal.com/gui/file/be8fdfce55ea701e19ab5dd90ce4104ff11ee3b4890b292c46567d9670b63b82/detection

https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/

https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/

https://www.zscaler.com/blogs/research/return-higaisa-apt

https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication

Lessons from the Conti Leaks

How Do You Run A Cybercrime Gang?

Ransomware Decryption Intelligence