DarkHotel hackers are back targeting Chinese Telecom

March 2, 2016 By Pierluigi Paganini

The DarkHotel APT group is back and it is targeting executives at telecommunications companies in China and North Korea.

According to threat intelligence start-up ThreatBook, the DarkHotel APT group is targeting executives at telecommunications companies in China and North Korea.

The Darkhotel espionage campaign was first uncovered by security experts at Kaspersky Lab in November 2014. The experts discovered that the hacking campaign was ongoing for at least four years while targeting selected corporate executives traveling abroad. According to the experts, threat actors behind the Darkhotel campaign aimed to steal sensitive data from executives while they are staying in luxury hotels, the worrying news is that the hacking crew is still active.

The attackers appeared as highly skilled professionals that exfiltrate data of interest with a surgical precision and deleting any trace of their activity. The researchers noticed that the gangs never go after the same target twice. The list of targets includes CEOs, senior vice presidents, top R&D engineers, sales and marketing directors from the USA and Asia traveling for business in the APAC region.

Experts at ThreatBook dubbed the new campaign DarkHotel Operation 8651, the hackers have already compromised at least one organization by using spear phishing emails.

The spear phishing messages came with malicious documents attached, typically a crafted SWF file embedded as a downloadable link in a Word document.

The DarkHotel hackers exploited the Adobe Flash vulnerability CVE-2015-8651, patched by Adobe on Dec. 28 with an out-of-band patch.

The attackers disguise the malicious code a component of the OpenSSL library. Experts noticed that the malware implements a number of anti-detection measures, including anti-sandbox and just-in-time decryption.

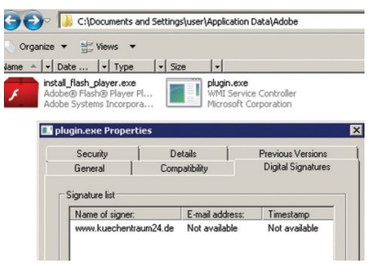
To better understand the DarkHotel group, let me provide you further details emerged by an update provided by Kaspersky Lab in August 2015. Kaspersky confirmed that the organizations targeted by the DarkHotel APT in 2015 were located in North Korea, Russia, South Korea, Japan, Bangladesh, Thailand, India, Mozambique and Germany.

Darkhotel relied on phishing emails containing links to Flash Player exploits disclosed following the data breach suffered by the Hacking Team surveillance firm.

"...at the beginning of July, it began to distribute what is reported to be a leaked Hacking Team Flash 0day. It looks like the Darkhotel *APT may have been using the leaked HackingTeam Flash 0day to target specific systems. We can pivot from "tisone360.com" to identify some of this activity. " Kaspersky wrote in a blog post.*

The DarkHotel APT used obfuscated HTML Application (HTA) files to serve backdoor and downloader code on infected systems since 2010, in August security experts discovered new variants of the malicious HTA files.

"It's somewhat strange to see such heavy reliance on older Windows-specific technology like HTML applications, introduced by Microsoft in 1999," experts noted.



The hackers also improved the obfuscation techniques using more efficient evasion methods, in one case the attackers used a signed downloaders developed to detect known antivirus solutions.

The spear-phishing emails used by the Darkhotel group in the past contain .rar archives that appeared to include a harmless .jpg file. In reality, the file is a .scr executable that appears like a JPEG using a technique known as right-to-left override (RTLO). When the file is opened, an image is displayed in the Paint application, while the malicious code is executed in the background.

Another novelty for the espionage campaign run by the Darkhotel APT group is the use of stolen digital certificates that are used to sign malware.

According to the experts at Kaspersky, the APT group appears to be Korean speaker.

Pierluigi Paganini

Security Affairs – (Darkhotel, cyber espionage)

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Brazilian police arrested Facebook Vice President for Latin America

NEXT ARTICLE
US DoD invites a restricted number of hackers to Hack the Pentagon