'DarkHotel' APT Uses New Methods to Target Politicians

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

By Eduard Kovacs on July 19, 2017

Tweet

RSS

The DarkHotel threat group has been using some new methods in attacks aimed at government employees with an interest in North Korea, according to a report published this week by security firm Bitdefender.

The activities of the DarkHotel advanced persistent threat (APT) actor came to light in November 2014, when 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.

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.

Bitdefender's analysis is based on samples from September 2016. The initial Trojan downloader, delivered via phishing emails, collects information on the infected device and sends it back to its command and control (C&C) server. If the compromised system meets requirements (i.e. it belongs to an individual who is of interest), the first stage DarkHotel downloader, disguised as a component of OpenSSL, is fetched.

In the meantime, in an effort to avoid raising suspicion, the malware opens a document titled "Pyongyang e-mail lists - September 2016," which provides a list of email contacts for various organizations in North Korea's capital city.

If the system profile does not match what the attackers are looking for, the C&C server returns a “fail” string and the attack stops. If the attack continues, a second payload is retrieved.

When Bitdefender analyzed the malware samples, the C&C server was offline, making it impossible to know exactly who the victims were and how much damage was caused. However, Bitdefender’s Bogdan Botezatu told *SecurityWeek* that, based on the structure of the phishing message, the intended targets are most likely individuals working for governments or state institutions who have an interest in the political situation in North Korea.

Experts believe that the use of social engineering and a multi-stage downloader is an improvement compared to the direct use of exploits as it gives the attackers more flexibility in malware distribution and ensures that the Trojan remains up to date.

Related: Jaku Botnet - Active Operation With Possible Links to Darkhotel APT Group

Tweet

RSS

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’s security news reporter. Eduard holds a bachelor’s degree in industrial informatics and a master’s degree in computer techniques applied in electrical engineering.
Previous Columns by Eduard Kovacs:
Exploitation of VMware Vulnerability Imminent Following Release of PoC
FBI: Higher Education Credentials Sold on Cybercrime Forums
Google Announces New Chrome and Chrome OS Security Features for Enterprises
Cloud Security Firm Lacework Lays Off 20% of Workforce
VMware to Absorb Broadcom Security Solutions Following $61 Billion Deal
2022 CISO Forum: September 13-14 - A Virtual Event

2022 Singapore/APAC ICS Cyber Security Conference]

Virtual Event Series - Security Summit Online Events by SecurityWeek

2022 ICS Cyber Security Conference | USA [Hybrid: Oct. 24-27]

Tags:

- Cyberwarfare
- NEWS & INDUSTRY
- Virus & Threats
- Virus & Malware
- Malware