DarkHotel

Presentation by Jimmy Tang, Samrat Shah, Slava Yarchak

What is DarkHotel?

- DarkHotel drives its campaigns by spear-phishing targets with highly advanced zero-day exploits, while maintaining an effective toolset and a long-running operation behind the host's machine.
- An advance persistant threat (ADT) which are a stealthy and continuous computer hacking processes orchestrated by humans targeting a specific entity.
- The threat actor usually targets hotels and business center Wi-Fi and physical connections.
- Targets have included CEOs, senior vice presidents, sales and marketing directors and top Research & Department staff
- When high-end corporate executives and entrepreneurs travel to a variety of hotels and connect to the internet, they are infected with a rare APT Trojan posing as any one of major software releases.

How Does it Attack?

- Visitors coming to Hotel's Wi-fi were prompted to install software updates to popular software packages which included that of Google Toolbar, Adobe Flash, Windows Messenger
- Added to these packeges were the installers for DarkHotel's backdoors which were installed alongside the legitimate packages.
- The backdoors are typically signed with forged digital certificates which share the same Root Certificate Authority and were originally encrypted with weak MD5 keys (RSA 512 bits).
- The weak keys took at most two week to break and cost as little as $75.
- Additionally, the backdoors installed a sophisticated digitally-signed advanced keylogger.
- It buffered, and communicated logged user data to the DarkHotel servers and its actor.

Malware Components

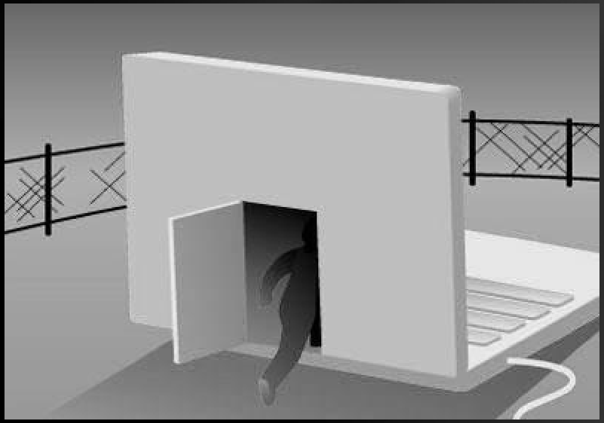
- Specific malware components were dropped by hotel installers spoofing legitimate software installers through backdoors.
- The tools included that of:

  1. Small downloader
  2. Information Stealer
  3. Trojan
  4. Dropper and Self-injector
  5. Selective Infector.

- The malware spreading is also done by peer-to-peer sharing sites, where it is delivered as a part of a large rar archive.

Damages Caused by DarkHotel

- The DarkHotel malware damages the confidentiality portion of the CIA triangle.
- Since the malware is sniffing the data because of the backdoor created, the collection of data occurs.
- Information ranging from company secrets to personal life is being sniffed.
- Hackers can sniff out login information for the executive’s company website or their personal/company social media account.
- They can then greatly benefit from this information.



Damages Caused by DarkHotel

- With the data that has been collected by the DarkHotel malware, the hacker can do a few things with the data.
- The hacker can sell a company secret in the black market or sell the login credentials for a company's website to other malicious individuals.
- The information stolen can be exposed to the public and potentially ruin a company's intellectual property or properties.
- With the login credentials the hacker can disrupt the company's website and can do major damage to the company, especially if it is a web-based one.

Prevention

- Abstinence – do not use web connection at all
- Delegation – delegate the task (and responsibility) of security to professionals
  - Company IT security team is more likely to be knowledgeable about securing remote access
  - You will be advised by the security team on company communication network procedures
  - Security team may be capable of assisting you remotely
  - Eliminates the necessity of having to put your own equipment at risk
- VPN use – in case of breach may protect the company networks from unauthorized access
- Personal systems – avoid use due to unnecessary risks
- Security software – Make use of antivirus and firewalls

Recap

- DarkHotel is malware that targets hotels and business center Wi-Fi to collect information from executives and CEOs.
- The malware disguises itself as legitimate software that needs to be updated.
- Installing the fake update, the malware creates a back door so the hacker can snoop information.
- It can cause damage to a company by sniffing from a range of login credentials to a company's top secret information. To prevent the malware from infecting the computer, the individual must have good security software, practice good security measures, or to abstain from the internet altogether.

Questions

Q: How does the DarkHotel malware infect a machine?

A: By masking itself as a legitimate software update (Adobe flash, Java, etc), the malware is installed onto the system by the user and creates a back door for the hacker to sniff information.

Q: What can the hackers gain by collecting information from executives/CEOs?

A: By having the information, the hacker can do many things like the extortion of information, the spread of a company’s top secret information to the public, to ruin a company’s website using login credentials and more.