Darkhotel: a spy campaign in luxury Asian hotels

By Alex Drozhzhin

Published: 2014-11-10 · Archived: 2026-04-05 16:29:36 UTC

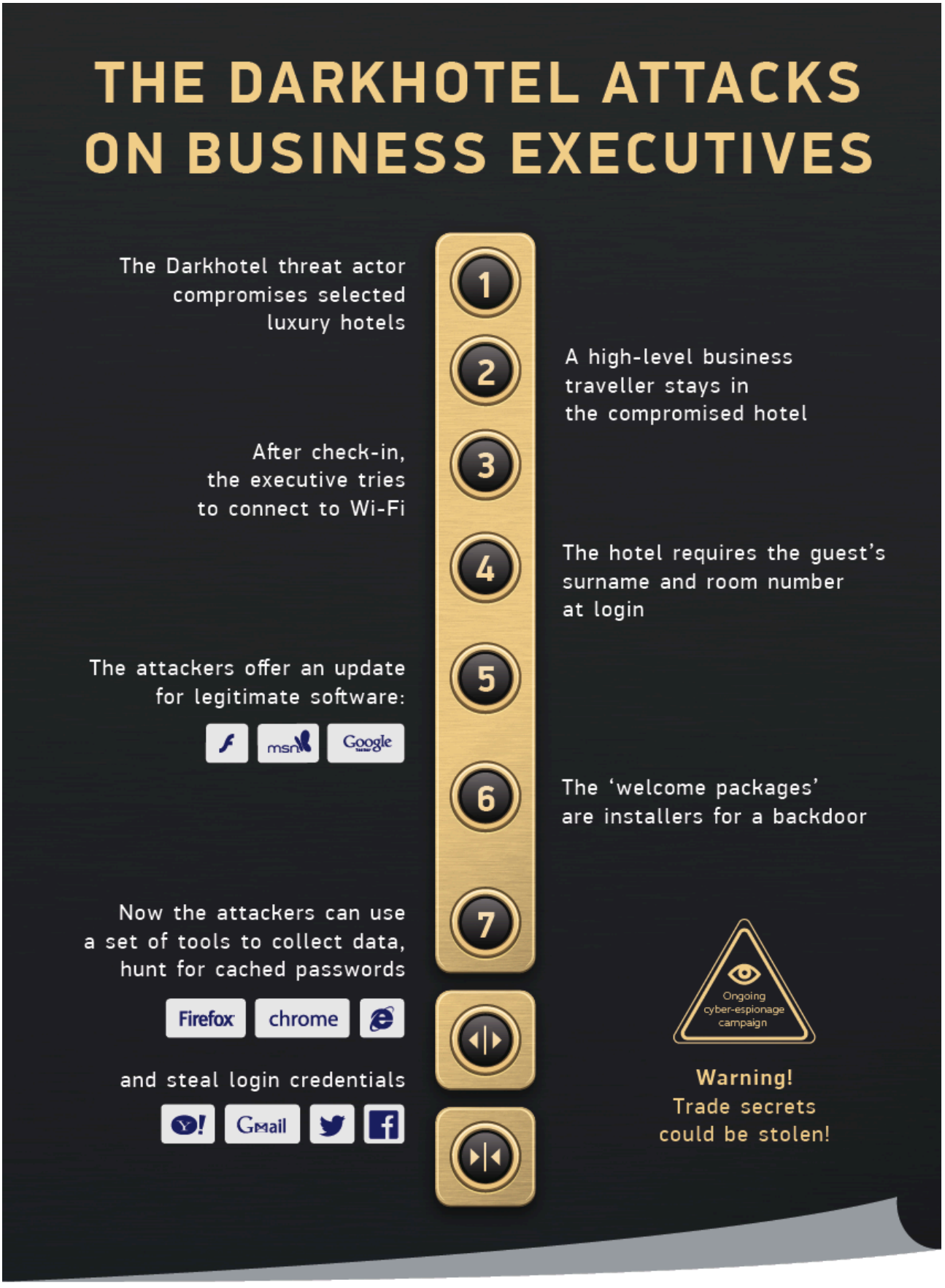
Cyberespionage is the weapon of choice in the 21st century. Even a seemingly harmless mobile app is able to find out quite a few secrets that a careless user might reveal, let alone full-scale surveillance campaigns specifically targeted at representatives of major businesses and government organizations.

This autumn's newest revelation is Kaspersky Lab's discovery of a spy network, dubbed 'Darkhotel', which had been active for seven years in a number of Asian hotels. Furthermore, smart and professional spies involved in this long-running operation created a comprehensive toolkit consisting of various methods that can be used to break into victims' computers.

The FBI first mentioned the attacks on guests that were staying in the hotels in question in 2012. However, the malware used over the course of Darkhotel's activity (a.k.a. Tapaoux) have been popping up here and there as early as 2007. Having studied the logs of C&C servers used to manage the campaign, security researchers discovered connections dating back to January 1, 2009. With all of the above in mind, the campaign appears to have been active for quite awhile.

> The #Darkhotel campaign appears to have been active for seven years.
>
> Tweet

The main method of infiltration into the victim's PC was through Wi-Fi networks in a number of luxury Asian hotels. Cybercriminals used zero-day exploits in Adobe Flash and other popular products by renowned vendors. Such vulnerabilities are not easy to find, which proves the fact that either rich sponsors, who can afford to purchase quite an expensive cyber weapon, were behind the operation, or the high level of professionalism of the agents that were involved in the campaign. Likely both.



The aforementioned method of dropping spyware was the most frequently used, yet not the only, way for the criminals to handle the operation, which suggests that they were employed by hotels. The alternative involves a Trojan, distributed through torrent clients, as part of a compromised archive of adult-rated comics in Chinese.

Also the cyberspies used targeted phishing, sending compromised emails to employees of state and non-profit organizations.

Criminals used a sophisticated keylogger. The spyware employed an integrated module to snatch passwords saved in popular browsers.

Many facts, besides the use of zero-day vulnerabilities, prove the high level of awareness of the cybercriminals. They went as far as to succeed in forging digital security certificates they used for their malware. To spy on communication channels used by their victims, criminals used a sophisticated keylogger. The spyware employed an integrated module to snatch passwords saved in popular browsers.

Strangely, the culprits were extremely cautious and designed a number of measures to prevent the detection of the malware. Firstly, they ensured the virus had a very long ‘incubation period’: the first time the Trojan connected to the C&C servers was 180 days after it had infiltrated the systems. Secondly, the spyware program had a self-destruction protocol if the language of the system changed to Korean.

The criminals were mainly operating in Japan, as well as in neighboring Taiwan and China. However, Kaspersky Lab managed to detect attacks in other countries, including those very far from the territories, which were an interest for the culprits.

Commenting on Darkhotel, Kurt Baumgartner, Principal Security Researcher at Kaspersky Lab, said: “For the past few years, a strong actor named Darkhotel has performed a number of successful attacks against high-profile

individuals, employing methods and techniques that go well beyond typical cybercriminal behavior. This threat actor has operational competence, mathematical and crypto-analytical offensive capabilities, and other resources that are sufficient to abuse trusted commercial networks and target specific victim categories with strategic precision."

At last we can say that Kaspersky Lab's products detect and neutralize the malicious programs and their variants used by the Darkhotel toolkit. You can read the full story of Darkhotel APT at Securelist.com

---