The Darkhotel APT

By GReAT

Published: 2014-11-10 · Archived: 2026-04-05 13:27:18 UTC

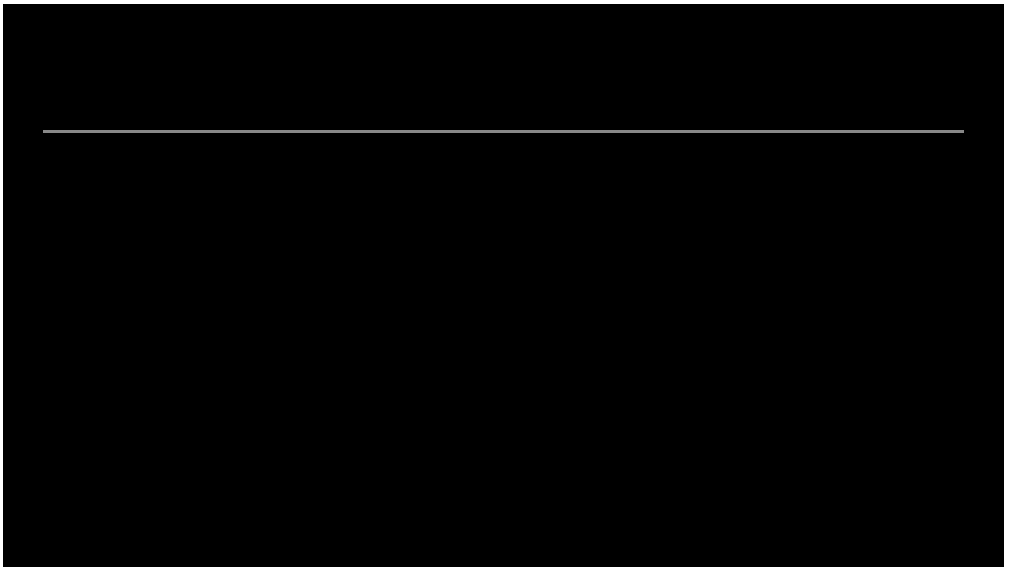
APT reports

APT reports

10 Nov 2014

2 minute read

A Story of Unusual Hospitality



The Darkhotel APT – Kaspersky Lab Research
Technical Appendix

Much like Crouching Yeti, the Darkhotel APT is an unusually murky, long standing and well-resourced threat actor exhibiting a strange combination of characteristics.

This APT precisely drives its campaigns by spear-phishing targets with highly advanced Flash zero-day exploits that effectively evade the latest Windows and Adobe defenses, and yet they also imprecisely spread among large numbers of vague targets with peer-to-peer spreading tactics. Moreover, this crew's most unusual characteristic is that for several years the Darkhotel APT has maintained a capability to use hotel networks to follow and hit

selected targets as they travel around the world. These travelers are often top executives from a variety of industries doing business and outsourcing in the APAC region. Targets have included CEOs, senior vice presidents, sales and marketing directors and top R&D staff. This hotel network intrusion set provides the attackers with precise global scale access to high value targets. From our observations, the highest volume of offensive activity on hotel networks started in August 2010 and continued through 2013, and we are investigating some 2014 hotel network events.

In addition to polluting p2p networks to infect the masses, they delegitimize Certificate Authorities to further their attacks. They abuse weakly implemented digital certificates to sign their malcode. The actor abused the trust of at least ten CAs in this manner. Currently they are stealing and re-using other legitimate certificates to sign their mostly static backdoor and infostealer toolset. Their infrastructure grows and shrinks over time, with no consistent pattern to the setup. It is both protected with flexible data encryption and poorly defended with weak functionality.

Victim categories include the following verticals:

- Very large electronics manufacturing
- Investment capital and private equity
- Pharmaceuticals
- Cosmetics and chemicals manufacturing offshoring and sales
- Automotive manufacturer offshoring services
- Automotive assembly, distribution, sales, and services
- Defense industrial base
- Law enforcement and military services
- Non-governmental organizations

About 90 percent of the infections appear to be located in Japan, Taiwan, China, Russia and South Korea, partly because of the group’s indiscriminate spread of malware. Overall, since 2008, the infection count numbers in the thousands. The more interesting travelling targets include top executives from the US and Asia doing business and investment in the APAC region. A combination of Kaspersky Security Network (KSN) detections and command and control data recorded infections in the United States, the United Arab Emirates, Singapore, Kazakhstan, South Korea, the Philippines, Hong Kong, India, Indonesia, Germany, Ireland, Mexico, Belgium, Serbia, Lebanon, Pakistan, Greece, Italy and others. This actor’s victim geolocation distribution has a long tail, and multiple significant targets and victims travel frequently throughout many of these countries. So, victim geolocation changes while they are travelling frequently.

When Kaspersky Lab researchers visited Darkhotel incident destinations with honeypot machines they did not attract Darkhotel attacks, which suggests the APT acts selectively.. Further work demonstrated just how careful these attackers were to hide their activity – as soon as a target was effectively infected, they deleted their tools from the hotel network staging point, maintaining a hidden status.

Darkhotel activity and objects have leaked out in bits and pieces over the past few years, but we have identified Darkhotel tools dating back to 2007. Considering their well-resourced, advanced exploit development efforts and large, dynamic infrastructure, we expect more Darkhotel activity in the coming years. Our Darkhotel report and appendices of indicators and technical details collects and organizes this APT’s activity to date.

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
