Application Security , Fraud Management & Cybercrime , Governance & Risk Management

Darkhotel APT Gang Taps Flash Flaw

Attacks Tied to South Korea Aim to Trick Potential Victims

Mathew J. Schwartz (euroinfosec) • August 11, 2015

Twitter | Facebook | LinkedIn | Credit Eligible | Get Permission

The advanced persistent threat gang behind a long-running series of cyberespionage-focused campaigns quickly tapped a zero-day exploit for a flaw in Adobe Flash after it was leaked in July, as part of the 400 GB dump of data stolen from hacked spyware vendor Hacking Team. But the APT gang has long employed trickery to exploit a number of high-profile targets, suggesting that potential victims will need to do more than just update their version of Flash Player to counter these types of attacks in the future.

See Also: 451 Research Report: Tackling the Visibility Gap in Information Security

That warning is being sounded by security firm Kaspersky Lab, which says that the long-active group, known as "Darkhotel," continues to favor diplomatic targets, as well as organizations that have "strategic commercial interests" - ranging from electronics and pharmaceuticals firms to private equity institutions and automotive manufacturers - in the Asia-Pacific region.

The APT group's use of Flash exploits is not new. In February 2014, Kaspersky Lab reported tracing back to the group a zero-day Flash attack used successfully against both Mac OS X and Windows 7 machines. Adobe quickly patched the related vulnerability. "Darkhotel seems to have burned through a pile of Flash zero-day and half-day exploits over the past few years, and it may have stockpiled more to perform precise attacks on high-level individuals globally," writes Kurt Baumgartner, principal security researcher at Kaspersky Lab, in a research report. "From previous attacks we know that Darkhotel spies on CEOs, senior vice presidents, sales and marketing directors and top R&D staff."

Other security firms have been tracking the same group - also known as Fallout Team, as well as Tapaoux - and report that since at least 2007, the APT gang has relied on targeted spear-phishing attacks to infect victims, but may also sometimes have gained physical access to targeted systems. The gang has also been tied to attacks involving peer-to-peer networks that infect large numbers of PCs at once, after which the attackers then exfiltrate data from targets of interest.

New Flash Flaw Targeted Fast

The new Kaspersky Lab report builds on a July 8 warning from Weimin Wu, a malware researcher at security firm Trend Micro, who reported that an exploit for an Adobe Flash zero-day flaw - CVE-2015-5119 - leaked via the July 5 dump of data stolen from Hacking Team had been used in spear-phishing attack against a target in South Korea. While the Darkhotel group was not named, Wu added that systems from both South Korea and Japan appeared to have visited an attack site being run by the attackers, which attempted to exploit visiting PCs with drive-by attacks based on Hacking Team's Flash flaw (see *Hacking Team Zero-Day Attack Hits Flash*).

"Fallout Team - publicly referred to as Darkhotel - has been using this Hacking Team exploit since July," threat-intelligence firm iSight Partners says in an Aug. 11 research note. "Fallout Team is a sophisticated espionage operation that we believe has a nexus to South Korea. The team has demonstrated access to significant operational resources and has also previously exploited zero-day vulnerabilities to compromise targets with a vested interest in security issues oriented around the Korean peninsula."

Exploits Launched Via Hotel WiFi

The Darkhotel moniker dates from November 2014, when Kaspersky Lab warned that the APT group had been using hotel networks across Asia and the United States to infect and track thousands of targets as they moved around the globe. "The more interesting travelling targets include top executives from the U.S. and Asia doing business and investment in the APAC region," Kaspersky Lab said. It added that the targets appeared to be carefully selected, and that after a hotel network was used to infect a victim, the related attack tools then appeared to be quickly deleted from the network, to help disguise the attack.

Since then, the Darkhotel group has reportedly continued to employ many of the same attack techniques. For example, Kaspersky Lab says that the zero-day Flash exploit obtained from the Hacking Team dump was launched from a website that the group had previously used to target an older Flash flaw. The group has also continued to sign some of its malware with digital certificates that have been stolen from Chinese-based firm Xuchang Hongguang Technology, and also still relies in large part on executable HTML - .hta - files in its attacks.

Spear-Phishing Continues

The group's attacks have continued throughout 2015, with Kaspersky Lab reporting that it has seen the attackers hit targets and victims located in at least nine countries: Bangladesh, Germany, India, Japan, Mozambique, North Korea, Russia, South Korea and Thailand. Meanwhile, systems from Amazon Web Services, as well as from France, Germany, Ireland and Ukraine also visited the attack infrastructure, but Kaspersky Lab says it believes those systems were associated with researchers.

Darkhotel also continues to target victims with spear-phishing attacks that send files to targets that are stored in the .rar WinRAR archiver format, with such names as "schedule(2.11~16).rar" and "schedule(6.1~6).rar" as well as "letter.rar," and will often keep attacking targets until they are successfully infected, Kaspersky Lab says. "For example, the attachment 'schedule(2.11~16).rar' could be sent on February 10th, with Darkhotel returning to the same targets in late May for a second attempt with attachment 'schedule(6.1~6).rar.'"

Many of the group's attacks rely on the right-to-left override technique, or RTLO, which attackers can abuse to spoof file extension names, Kaspersky Lab says. In the case of the Darkhotel attacks, RTLO has been used in some cases to disguise executable .scr files as .jpg files. If a target opens the supposed image file, however, it instead drops a link onto their desktop and executes it, which launches a "target shell script" that initiates an AJAX-based download of a 1.2 MB executable, which then "injects malicious code and spawns remote threads into legitimate processes" - thus fully compromising the system - Kaspersky Lab says.

It adds that the most recent versions of the attackers' malware downloader includes defenses against 27 different types of antivirus software, ranging from Avast and Intel/McAfee to Kaspersky Lab and F-Secure.

Despite the technical moves, however, Martijn Grooten, who edits malware research site Virus Bulletin, notes that related attacks still rely largely on tricking would-be victims.

Exploit Kits at Work Too

Of course, Darkhotel is not the only group that used the Flash exploits that were leaked from Hacking Team. In fact, the Hacking Team breach "has facilitated multiple operations by known operators, particularly in the short term after the breach," iSight Partners says (see *Zero-Day Exploit Alert: Flash, Java*). Indeed, in the days and weeks following the data dump, the French malware researcher Kafeine reported that related exploits had been added not only to the open source Metasploit penetration-testing framework, but also to six separate exploit kits that are sold - and employed - by cybercriminals for in-the-wild attacks.

Application Security | Fraud Management & Cybercrime | Governance & Risk Management | Next-Generation Technologies & Secure Development

Twitter | Facebook | LinkedIn | Credit Eligible | Get Permission

‹ Previous
Wire Fraud Just Got More Challenging

Next ›
Feds Charge 9 with $30M Insider Trading, Hacking Scheme

About the Author

Mathew J. Schwartz

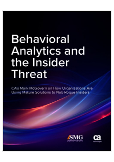
Executive Editor, DataBreachToday & Europe

Schwartz is an award-winning journalist with two decades of experience in magazines, newspapers and electronic media. He has covered the information security and privacy sector throughout his career. Before joining Information Security Media Group in 2014, where he now serves as the executive editor, DataBreachToday and for European news coverage, Schwartz was the information security beat reporter for InformationWeek and a frequent contributor to DarkReading, among other publications. He lives in Scotland.

You might also be interested in ...

The Need For A Business-Driven Security Posture

Tenable Research: How Lucrative Are Vulnerabilities?



Behavioral Analytics and the Insider Threat

GET DAILY EMAIL UPDATES

Covering topics in risk management, compliance, fraud, and information security.

Email address | Submit

By submitting this form you agree to our Privacy & GDPR Statement

RESOURCES

Three Steps to Securing Enterprise Data on Cloud Platforms

Container Security Best Practices: A How-To Guide

5 Best Practices For Application Security: A How-To Guide

Container Security Best Practices: A How-To Guide

Deception Technology: Making the Case

LATEST NEWS

Digital Identity
Data Governance: How to Tackle Three Key Issues

Cloud Security
Uncertain Markets May Drive Cybersecurity Consolidation

Application Security
Security Firm Checkmarx Getting New Owner

Artificial Intelligence & Machine Learning
ACLU Files Lawsuit Over Facial Recognition at US Airports

Endpoint Security
COVID-19 Response: 5 Tips for Securing Remote Workplace

LATEST TWEETS AND MENTIONS

MyersEH
Check out this video interview w/ @LNSundra @Forescout where she addresses tough questions such as enterprise… https://t.co/NjzqC5jAsn
about a minute ago. Retweet

andynorton27000
Data Governance: How to Tackle Three Key Issues https://t.co/cvH1V5IH4y https://t.co/9P2J99jxlo
about a minute ago. Retweet

vishne0
RT @ArrakisConsult: Contact Arrakis for your confidential needs. Security Firm Checkmarx Getting New Owner https://t.co/039Z4uGkmO sales…
8 minutes ago. Retweet

nickster2407
Some great cybersecurity tips on WFH from Phil Reitinger of Global Cyber Alliance https://t.co/iNMrxP8N6n
11 minutes ago. Retweet

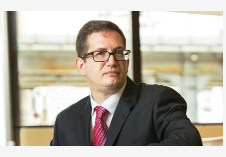
healthinfosec
#HHS #OCR Issues Limited #HIPAA Waivers Amid #Coronavirus Pandemic: Includes Moves to Facilitate #Telehealth; Drops… https://t.co/vtWtvQAH6Y
12 minutes ago. Retweet

Follow us on Twitter

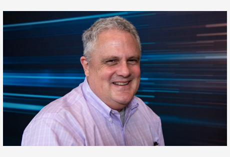
Around the Network

The New Insider Risk: When Creativity Goes Bad

Making the Healthcare Supply Chain 'Smarter'



COVID-19: How to Adjust Business Continuity Plans



COVID-19 Response: 5 Tips for Securing Remote Workplace