Darkhotel APT is back: Zero-day vulnerability in Microsoft VBScript is exploited | 360 Total Security Blog

Published: 2018-08-21 · Archived: 2026-04-05 23:13:09 UTC

Aug 21, 2018Elley

Choose a language

Learn more about 360 Total Security

VBScript is available in the latest versions of Windows and Internet Explorer 11. However, Microsoft disabled VBScript execution in the latest version of Windows in the browser's default configuration, which makes it immune to the vulnerability. There are still other ways to load scripts. For example, applications in the Office suite rely on the IE engine to load and render web content.

The researchers of Trend Micro noticed that the VBScript vulnerability being exploited after Microsoft delivered its regular Windows update in July. The vulnerability is named as CVE-2018-8373, which was addressed in this month's patch delivery. It is a use-after-free memory corruption that allows attackers to run shellcode on the compromised computer.

After analyzing the exploit code, the researchers found that it used the same obfuscation technique as an older VBScript vulnerability CVE-2018-8174 which is fixed in May. The older vulnerability is known as "Double Kill", which was reported by Qihoo 360. The researchers of Qihoo 360 pointed out that Trend Micro's analysis of CVE-2018-8373 referenced the same domain name embedded in Office documents to download "Double Kill" exploit code.

In May, the researches of Qihoo 360 analyzed "Double Kill" and confirmed its association with the Darkhotel group (APT-C-06). The researchers drew this conclusion from the tools and methods that Darkhotel group used. It is considered that the decryption algorithm used by "Double Kill" is similar with APT-C-06, and China is one of its main targets.

Kaspersky Lab found Darkhotel in 2014 and has traced its activity since 2007. The experts believe that the group chronically targeted corporate executives and representatives of government organizations who stay in Asian luxury hotels.

We can conclude that Darkhotel is a highly sophisticated group or has strong financial support through its use of zero-day exploit in renown products.

Earlier this month, McAfee and Intezer claimed that Darkhotel has a strong connection with North Korea. They analyzed the malware used in multiple attacks related to North Korea. After analyzing the code used between 2008 and 2017, the researchers associated these malware families together.

Based on the research, Darkhotel is directly related to the Dark Seoul malware, which has the strong connection with “Operation Blockbuster” (an attack against Sony Pictures, which FBI believes that this is launched by North Korea).

Note: This article is from Bleeping Computer.

Learn more about 360 Total Security
