# North Korea-linked Dark Hotel APT leverages CVE-2018-8373 exploit

August 19, 2018 By Pierluigi Paganini

## The North Korea-linked Dark Hotel APT group is leveraging the recently patched CVE-2018-8373 vulnerability in the VBScript engine in attacks in the wild.

The vulnerability affects Internet Explorer 9, 10 and 11, it was first disclosed last month by Trend Micro and affected all supported versions of Windows.

The flaw could be exploited by remote attackers to take control of the vulnerable systems by tricking victims into viewing a specially crafted website through Internet Explorer. The attacker could also embed an ActiveX control marked 'safe for initialization' in an application or Microsoft Office document that hosts the IE rendering engine.

*"A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user." reads the security advisory published by Microsoft.*

*"An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights."*

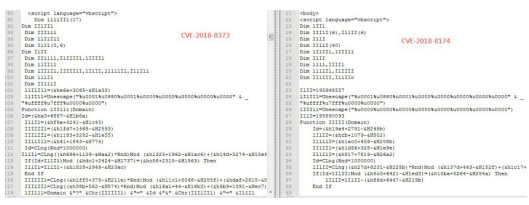
The analysis of the exploit code for the CVE-2018-8373 revealed it shared the obfuscation technique implemented for another exploit triggering the CVE-2018-8174 flaw.

The CVE-2018-8174 was first discovered by experts at Chinese security company Qihoo 360 and it was fixed in May by Microsoft.

The similarities in the exploits suggest that were developed by the same threat actor.

*"We found this exploit using heuristics, which led to a more in-depth analysis. Interestingly, we found that this exploit sample uses the same obfuscation technique as exploits for CVE-2018-8174, a VBScript engine remote code execution vulnerability patched back in May" wrote Trend Micro.*

*"We suspect that this exploit sample came from the same creator. Our analysis revealed that it used a new use-after-free (UAF) vulnerability in vbscript.dll, which remained unpatched in the latest VBScript engine."*




A similar theory was proposed by experts from Qihoo that collected evidence that linked the use of the CVE-2018-8373 exploit to Dark Hotel.

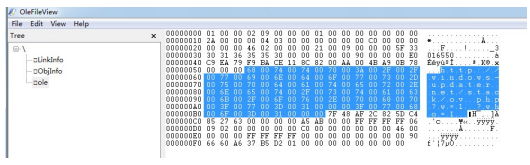
The experts discovered that domain name embedded in Office documents in latest attacks is the same used to download Double Kill exploit code in previous attacks linked to the North Korea-linked APT group.

*"The 360 Threat Intelligence Center first obtained the IOC address after Trend Micro coding through the big data analysis association:*

> *http://windows-updater[.]net/realmuto/wood[.]php?who=1??????*

***Associated homologous 0day attack sample" states Qihoo***

*"And found an attack time and trend technology found in the wild "double kill" 0day attack on the same day suspected of using the 0day attack of the office document sample, the domain name embedded in the Offce document sample and the domain name format given by Trend Micro (http ://windows-updater[.]net/stack/ov[.]php?w= 1\x00who =1)"*



In the analysis published in May by Qihoo 360 the researchers associated the CVE-2018-8373 exploit with Dark Hotel based on TTPs associated with the threat actor (e.g. the decryption algorithm that malware used is identical to Dark Hotel's one).
Experts speculated that the CVE-2018-8373 was used in a cyber espionage campaign aimed at China.

Pierluigi Paganini

(Security Affairs – Dark Hotel, APT)

Share this...

APT CVE-2018-8174 Dark Hotel APT Hacking North Korea Pierluigi Paganini Security Affairs

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
China's Belt and Road project (BRI) is a driver of regional cyber threat activity

NEXT ARTICLE
Security Affairs newsletter Round 176 – News of the week

YOU MIGHT ALSO LIKE

Adobe releases out-of-band patches for critical issues in Acrobat Reader, Photoshop, Bridge, ColdFusion

March 18, 2020 By Pierluigi Paganini

Trend Micro addresses two issues exploited by hackers in the wild

March 18, 2020 By Pierluigi Paganini


Yoroi Blog