INCIDENTS

The rush for CVE-2013-3906 – a Hot Commodity

By Dmitry Tarakanov on November 14, 2013. 4:58 pm

Two days ago FireEye reported that the recent CVE-2013-3906 exploit has begun to be used by new threat actors other than the original ones. The new infected documents share similarities with previously detected exploits but carry a different payload. This time these exploits are being used to deliver Taidoor and PlugX backdoors, according to FireEye.

At Kaspersky Lab we have also detected that yet another APT group has just started spreading malicious MS Word documents exploiting CVE-2013-3906. This APT actor is the Winnti group, which we described in detail here. They have sent spear-phishing emails with an attached document containing the exploit. As usual the Winnti perpetrators are trying to use this technique to deliver 1st stage malware – PlugX.

We became aware of an attack against one gaming company which constantly undergoes attacks from the Winnti group. The MS Word document containing the exploit shows the same TIFF "picture" –**7dd89c99ed7cec0ebc4afa8cd010f1f1** – that triggers the exploitation of the vulnerability, as in the Hangover attacks. If the exploitation is successful, the PlugX backdoor is downloaded from a remote URL:
hxxp://**211.78.90.113/music/cover/as/update.exe**.

According to the PE header, this PlugX sample was compiled on **November 4, 2013**. The internal functional PlugX Dynamic Link Library that is decrypted and allocated in memory during malware execution is a little bit older – it dates from **October 30, 2013**. In terms of its development branches, the version of PlugX which is downloaded is slightly different from the conventional PlugX but the same type as the one discovered by FireEye when the malware sends CnC HTTP POST packets with noticeable additional headers:

FireEye sample	Winnti's variant
FireEye sample POST /<random [0-9A-F]{24}> HTTP/1.1 Accept: */* FZLK1: 0 FZLK2: 0 FZLK3: 61456 FZLK4: 1	Winnti's variant POST /<random [0-9A-F]{24}> HTTP/1.1 Accept: */* HHV1: 0 HHV2: 0 HHV3: 61456 HHV4: 1

Winnti's PlugX is connecting to a new, previously unknown C2, **av4.microsoftsp3.com**. This domain points to the IP-address **163.43.32.4**. Other Winnti-related domains have been pointing here starting with October 3, 2013:

ad.msnupdate.bz	**ap.msnupdate.bz**	
book.playncs.com	**data.msftncsl.com**	**ns3.oprea.biz**

Once again, we are witnessing a rapid spread of the usage of a recently discovered vulnerability by different APT actors. Due to the high level of competition, we have already seen how quickly new exploits are added to different Exploit Packs when cybercriminals get involved. It's not yet clear how the new APT actors have come into possession of the CVE-2013-3906 – perhaps they obtained the same "builder" as the Hangover attackers, or acquired just a few samples of poisoned MS Word documents and adapted them for own needs. Anyway, we can conclude that just as regular cybercriminals under competition pressure, APT actors too will not rest on their laurels but aim to constantly evolve, perfecting their everyday processes and working more closely together becoming an ever more dangerous threat.

Discovered samples

Exploit.MSOffice.CVE-2013-3906.a
MS Word document: Questionnaire.docx, 63ffbe83dccc954f6a9ee4a2a6a93058

Backdoor.Win32.Gulpix.tu
PlugX backdoor: update.exe, 4dd49174d6bc559105383bdf8bf0e234

Backdoor.Win32.Gulpix.tt
PlugX internal library: 6982f0125b4f28a0add2038edc5f038a

TARGETED ATTACKS VULNERABILITIES AND EXPLOITS

Share post on:

Related Posts

Mokes and Buerak distributed under the guise of security certificates

Operation AppleJeus Sequel

Kaspersky Security Bulletin 2019. Statistics

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Enter your comment here

Name *

Email *

□ Save my name, email, and website in this browser for the next time I comment.

□ Notify me when new comments are added.

SUBMIT

□ I'm not a robot reCAPTCHA Privacy - Terms

IN THE SAME CATEGORY

An advertising dropper in Google Play

New FinSpy iOS and Android implants revealed ITW

DNS Manipulation in Venezuela in regards to the Humanitarian Aid Campaign

DarkVishnya: Banks attacked through direct connection to local network

KoffeyMaker: notebook vs. ATM

kaspersky

Email

□ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

SUBSCRIBE