Wekby APT attacks leverage Hacking Team exploits

July 11, 2015 By Pierluigi Paganini

According to the experts at Volexity the Flash Player exploit has been leveraged in spear phishing campaign launched by the Wekby APT.

As anticipated, several criminal gangs included the code for the exploitation of CVE-2015-5119 vulnerability in their exploit kits, let's remember that the exploits code was disclosed as the result of the attack against the Hacking Team.

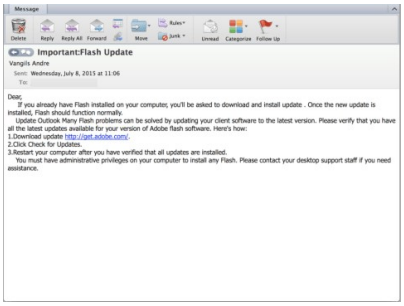
Adobe promptly patched the flaw, but according to security solutions provider Volexity, the Adobe Flash Player exploit has been leveraged by advanced persistent threat (APT) groups, including the Chinese Wekby APT (aka APT 18, Dynamite Panda and TG-0416).

Experts at Volexity confirmed that the Flash Player exploit has been leveraged in a number of cyber attacks run by APTs and also by common criminal groups.

> *"The exploit has since been added into the Angler Exploit Kit and integrated into Metasploit. However, not to be* out done, *APT attackers have also started leveraging the exploit in targeted spear phishing attacks as well." reports the blog post published by the company.*

Experts speculate that the Wekby group is the APT that hacked the Community Health Systems and compromised 4.5 million patient records from the target by exploiting the Heartbleed vulnerability.

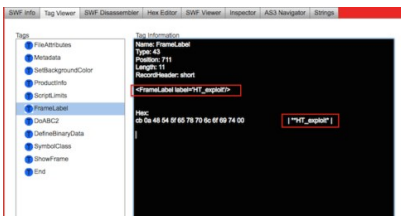
The Wekby APT sent spear phishing messages to the victims titled "Important: Flash update" trying to exploit the news of the release of the patch for Flash Player zero-day.



The campaign was lauched to compromise victims systems and serve the Gh0st RAT. Experts noticed that the C&C used by the Wekby group is located in Singapore and was already used in the past by the same threat actor.

The Wekby were sent out the malicious messages by using a spoofed Adobe email address and they included a link apparently pointing to the official Adobe download domain that was referring a domain set up to serve the SWF file crafted to exploit the CVE-2015-5119.

The Labels found by the experts in the SWF file suggest that the code for the Adobe exploits is the same leaked in the Hacking Team hack.



Bad story ... and it is just the beginning!

Pierluigi Paganini

(**Security Affairs** – Wekby , APT)

Share this...

Adobe | Adobe Flash | APT | CVE-2015-5119 | Hacking | Hacking Team | Wekby | zero-Day

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
A review of the Kofer Ransomware Campaign

NEXT ARTICLE
UK to ban messaging applications under a new law

YOU MIGHT ALSO LIKE

Noooo, now Ancient Tortoise BEC scammers are launching Coronavirus-Themed attacks

March 15, 2020 By Pierluigi Paganini

Slack bugs allowed take over victims' accounts

March 14, 2020 By Pierluigi Paganini