May 25, 2016

Danti and Co.: Cyberespionage Groups Use a Single Vulnerability to Target Organizations Around the World

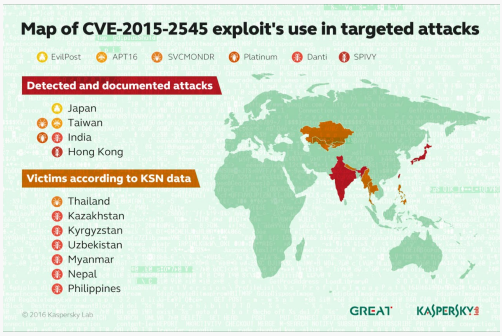
Kaspersky Lab's Global Research and Analysis Team has spent the last few months observing a wave of cyberespionage attacks conducted by different groups across the Asia-Pacific (APAC) and Far East regions, all of which share one common feature: in order to infect their victims with malware, the attackers use an exploit for the CVE-2015-2545 vulnerability

Kaspersky Lab's Global Research and Analysis Team has spent the last few months observing a wave of cyberespionage attacks conducted by different groups across the Asia-Pacific (APAC) and Far East regions, all of which share one common feature: in order to infect their victims with malware, the attackers use an exploit for the CVE-2015-2545 vulnerability. This weakness in Microsoft Office software was patched at the end of 2015, but still appears to be of use to these threat actors. The Platinum, APT16, EvilPost, and SPIVY groups were already known to use the exploit, and they are now joined by a fairly new and previously unknown group called Danti.

An exploit is a malicious tool widely utilized by cyberespionage groups and cybercriminals to silently infect targeted machines with malware. Several years ago, the use of so-called zero-day vulnerabilities (those that are used in the wild before the vendor of the affected software releases the patch) was the defining characteristic of sophisticated threat actors, but things have changed: nowadays cyberespionage groups are more likely to use exploits for known vulnerabilities, just because it is cheaper and seems to deliver an acceptable rate of infection.

The CVE-2015-2545 error enables an attacker to execute arbitrary code using a specially crafted EPS image file. The severity of the exploit for this vulnerability is high because it uses PostScript technique and can evade Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) protection methods embedded in Windows. Danti is the latest group to have been spotted using this vulnerability.

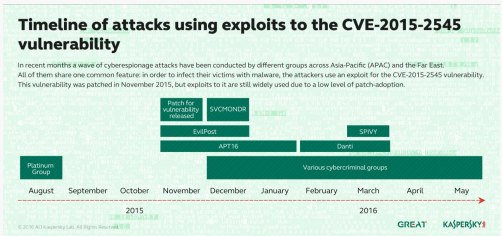
Danti is highly focused on diplomatic entities. It may already have full access to internal networks in Indian government organizations. According to Kaspersky Security Network, some Danti Trojans have also been detected in Kazakhstan, Kyrgyzstan, Uzbekistan, Myanmar, Nepal and the Philippines. Its activity was first spotted at the beginning of February and continued through March to the present day.



The exploit is delivered through spear-phishing emails. In order to attract the attention of potential victims, the threat actors behind Danti have created emails in the names of several high-ranking Indian government officials. Once the exploitation of the vulnerability takes place, the Danti backdoor is installed and this subsequently provides the threat actor with access to the infected machine so they can withdraw sensitive data.

The origin of Danti is unknown, but Kaspersky Lab researchers have reason to suspect that the group is somehow connected to the Nettraveler and DragonOK groups. It is believed that Chinese-speaking hackers are behind these groups.

Also, Kaspersky Lab researchers have spotted CVE-2015-2545-attacks of unknown origin against some organizations in Taiwan and Thailand. These attacks have been given the internal name SVCMONDR after the name of the Trojan that is downloaded after exploitation of the vulnerability. The Trojan is different to the one used by the Danti group, but it shares some common features with Danti as well as with APT16 – a known cyberespionage group presumed to be of Chinese origin.



"We expect to see more incidents with this exploit, and we continue to monitor new waves of attacks and the potential relationship with other attacks in the region. Waves of attacks conducted with the help of just one vulnerability suggests two things: firstly, that threat actors tend not to invest many resources into the development of sophisticated tools, like zero-day exploits, when 1-day exploits will work almost as well. Secondly, that the patch-adoption rate in the target companies and government organizations is low. We urge companies to pay closer attention to patch-management in their IT infrastructure in order to protect themselves from known vulnerabilities at the very least," - said Alex Gostev, Chief Security Expert at Kaspersky Lab Research Center in APAC.

Read more about targeted attacks utilizing CVE-2015-2545 at Securelist.com

More information on how Kaspersky Lab technologies protect against cyberattacks that make use of vulnerabilities is available on Kaspersky Business blog.

Related Articles Virus News

Hidden threat: criminals conceal miners under the guise of legitimate thematic applications

Kaspersky Lab's researchers have discovered that more and more cyber criminals are turning their attention to malicious software that is mining cryptocurrencies at the expense of users' mobile devices.

Read More >

Kaspersky Lab DDoS Intelligence quarterly report: amplification attacks and old botnets make a comeback

Kaspersky Lab has published its report looking at botnet-assisted DDoS attacks for the first quarter of 2018

Read More >

New variant of SynAck ransomware uses sophisticated Doppelgänging technique to evade security

Kaspersky Lab researchers have discovered a new variant of the SynAck ransomware Trojan using the Doppelgänging technique to bypass anti-virus security by hiding in legitimate processes.

Read More >