For Immediate Release

Kaspersky Lab Expert Analyses Icefog, A New Advanced Persistent Threat That Attacks The Supply Chain

PETALING JAYA, October 18, 2013 - Kaspersky Lab, a leading developer of secure content and threat management solutions through its Global Research & Analysis Team (GReAT) expert, Michael Molsner analyzed and dissected a new cyber-espionage campaign codenamed 'Icefog' exclusively for Malaysian media, here, today.

Kaspersky Lab's security research team recently published a research paper on the discovery of the Icefog cyber-espionage campaign which is described as a small yet energetic Advanced Persistent Threat (APT) group that focuses on hitting the supply chain of Western companies in South Korea and Japan. **Sinkhole connection in Malaysia and Singapore were also observed.** The operation started in 2011 and has increased in size and scope over the last few years.

"For the past few years, we've seen a number of APTs hitting pretty much all types of victims and sectors. In most cases, attackers maintain a foothold in corporate and governmental networks for years, smuggling out terabytes of sensitive information," said Mr. Michael Molsner, a member of the Global Research & Analysis Team who is based in Japan, and who is part of the team credited with discovering and analyzing the Icefog APT.

"Icefog is different. The 'hit and run' nature of the Icefog attacks demonstrate a new emerging trend, of smaller hit-and-run gangs that go after information with surgical precision. The attack usually lasts for a few days or weeks rather than the months or years of more traditional APTs. After obtaining what they were looking for, the Icefog attackers clean up and leave. In the future, we predict the number of small, focused '[1]APT-to-hire' groups to grow, specializing in hit-and-run operations; a kind of 'cyber mercenary' team for the modern world," Mr. Molsner explained.

[1] APT: Advanced Persistent Threat

In total, Kaspersky Lab observed more than 4,000 unique infected IPs and several hundred victims (a few dozen Windows victims and more than 350 Mac OS X victims).

In addition to Japan and South Korea, many sinkhole connections in several other countries were observed, including Taiwan, Hong Kong, China, the USA, Australia, Canada, the UK, Italy, Germany, Austria, **Singapore,** Belarus and **Malaysia**.

"Based on the list of IPs used to monitor and control the infrastructure, Kaspersky Lab's experts assume some of the players behind this threat operation are based in at least three countries: **China, South Korea and Japan,"** he said.

The Key Findings of Icefog Attacks

» The attackers rely on **spear-phishing and exploits for known vulnerabilities** (eg. CVE-2012-0158, CVE-2012-1856, CVE-2013-0422 and CVE-2012-1723). The lure documents used in the attacks are specific to the target's interest; for instance, an attack against a media company in Japan used the lure

» Based on the profiles of known targets, the attackers appear to have an interest in the following sectors: **military, shipbuilding** and **maritime** operations, **research companies, telecom** operators, **satellite** operators, **mass media** and **television**.

» Research indicates the attackers were interested in targeting defense industry contractors such as **Lig Nex1** and **Selectron Industrial Company**, ship-building companies such as **DSME Tech, Hanjin Heavy Industries** or telecom operators such as **Korea Telecom**.

» The attackers are hijacking sensitive documents and company plans, e-mail account credentials, and passwords to access various resources inside and outside the victim's network.

» During the operation, the attackers are using the "Icefog" backdoor set (also known as "Fucobha"). Kaspersky Lab identified versions of Icefog for both **Microsoft Windows** and **Mac OS X**.

» While in most other APT campaigns, victims remain infected for months or even years and attackers are continuously exfiltrating data, Icefog operators are processing victims **swiftly and in a surgical manner** -- locating and copying only specific, targeted

information. Once the desired information is obtained, they abandon the infection and move on.

» In most cases, the Icefog operators appear to already know very well what they need from the victims. **They look for specific file names**, which are identified and transferred to the Command and Control server.

The Attack & Functionality

Kaspersky researchers have sinkholed 13 of the 70+ domains used by the attackers. This provided statistics on the number of victims worldwide. In addition, the Icefog command and control servers maintain encrypted logs of their victims together with the various operations performed on them. These logs can sometimes help to identify the targets of the attacks and in some cases, the victims.

Solution

Kaspersky Lab's products detect and eliminate all variants of Icefog malware.

-ENDS-

About Kaspersky Lab
Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab is one of the top vendors of information security solutions in the world. The company's products and technologies are used by over 300 million people worldwide, its technology is licensed by leading security vendors globally. The Kaspersky Lab group of companies is headquartered in Moscow, has five regional divisions and numerous local offices throughout the world. You can learn more about Kaspersky Lab by visiting http://www.kaspersky.com.my

This press release is issued on behalf of Kaspersky Lab by About Communication Sdn Bhd. For media enquiry and exclusive interview with Kaspersky Lab representatives, kindly contact:-	
PR Contact for Malaysia **Retna Vijayan** Tel: 03.8075.6000 Mobile: 012.639.8443 E-mail: retna.vijayan@aboutcom.com.my **Faris Zakaria** Tel: 03.8075.6000 Mobile: 017.574.3840 E-mail: faris.zakaria@aboutcom.com.my	