The Icefog APT: A Tale of Cloak and Three Daggers

By GReAT

Published: 2013-09-25 · Archived: 2026-04-05 13:25:51 UTC

APT reports

APT reports

25 Sep 2013

2 minute read

The emergence of small groups of cyber-mercenaries available for hire to perform surgical hit and run operations.

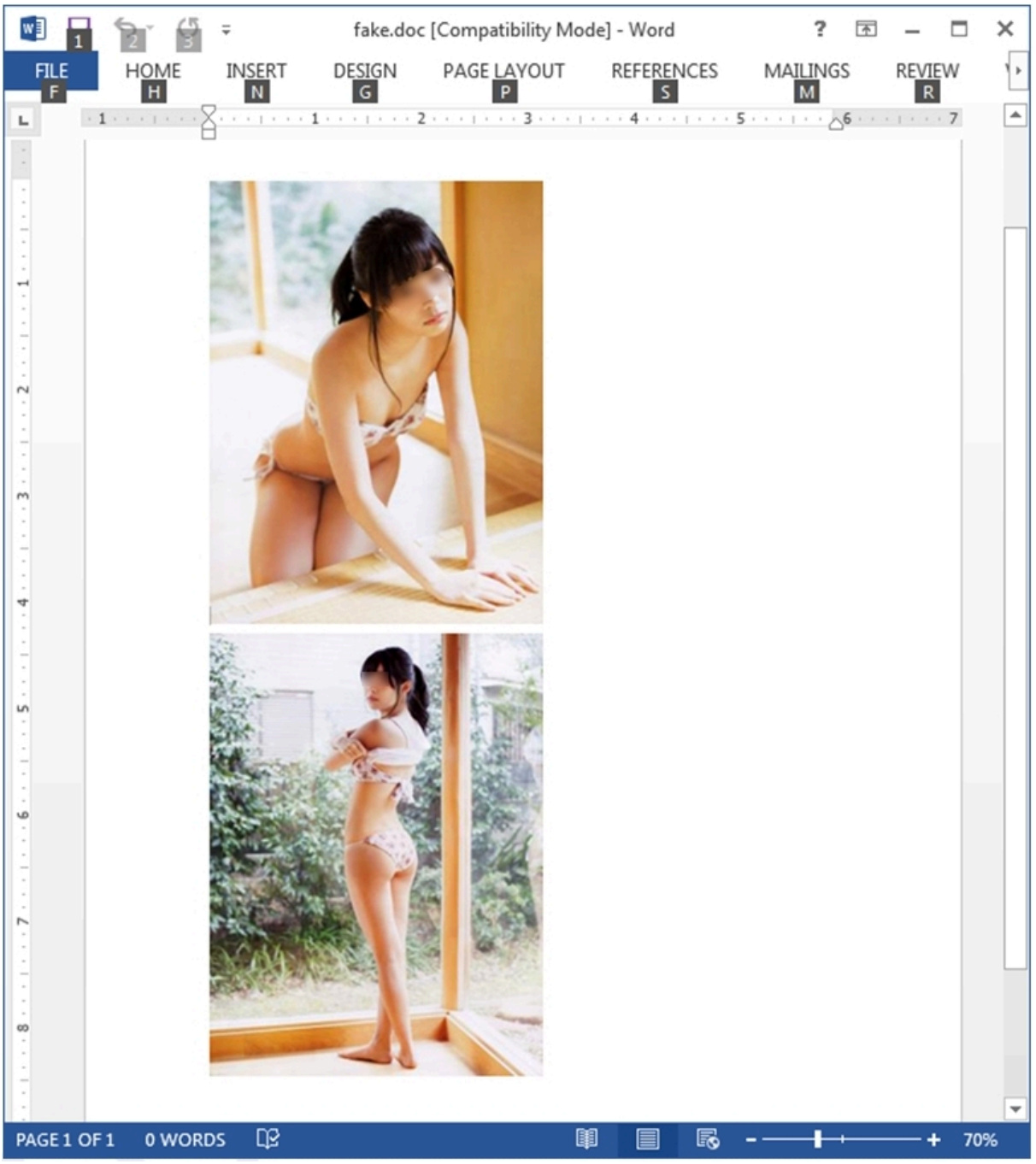
The world of Advanced Persistent Threats (APTs) is well known. Skilled adversaries compromising high-profile victims and stealthily exfiltrating valuable data over the course of many years. Such teams sometimes count tens or even hundreds of people, going through terabytes or even petabytes of exfiltrated data.

Although there has been an increasing focus on attribution and pinpointing the sources of these attacks, not much is known about a new emerging trend: the smaller hit-and-run gangs that are going after the supply chain and compromising targets with surgical precision.

Since 2011 we have been tracking a series of attacks that we link to a threat actor called ‘Icefog’. We believe this is a relatively small group of attackers that are going after the supply chain — targeting government institutions, military contractors, maritime and ship-building groups, telecom operators, satellite operators, industrial and high technology companies and mass media, mainly in South Korea and Japan. This Icefog campaigns rely on custom-made cyber-espionage tools for Microsoft Windows and Apple Mac OS X. The attackers directly control the infected machines during the attacks; in addition to Icefog, we noticed them using other malicious tools and backdoors for lateral movement and data exfiltration.

Key findings on the 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 following lure:



Lure document shown to the victim upon successful execution of the exploit

- 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 C&C.

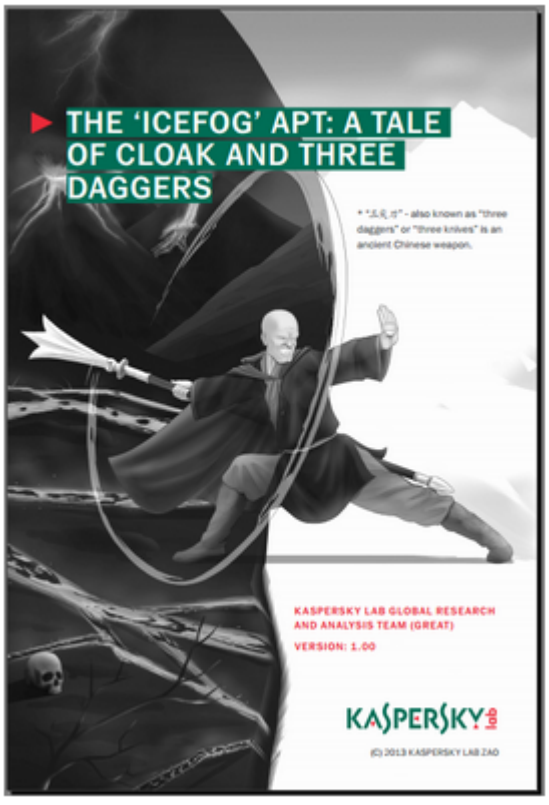
Kaspersky Lab would like to thank KISA (Korea Internet & Security Agency) and INTERPOL for their support in this investigation.

We’re sharing Indicators of Compromise based on the OpenIOC framework for Icefog. This way organizations have an alternative way of checking their network for presence of (active) Icefog infections.

You can download the IOC file (.zip) here.

A detailed FAQ on Icefog is available.

You can read our full Icefog report here:



[Click to download]

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
