The Icefog APT: A Tale of Cloak and Three Daggers

securelist.com/the-icefog-apt-a-tale-of-cloak-and-three-daggers/57331/

APT reports

APT reports

25 Sep 2013

minute read

Authors

Expert GReAT

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

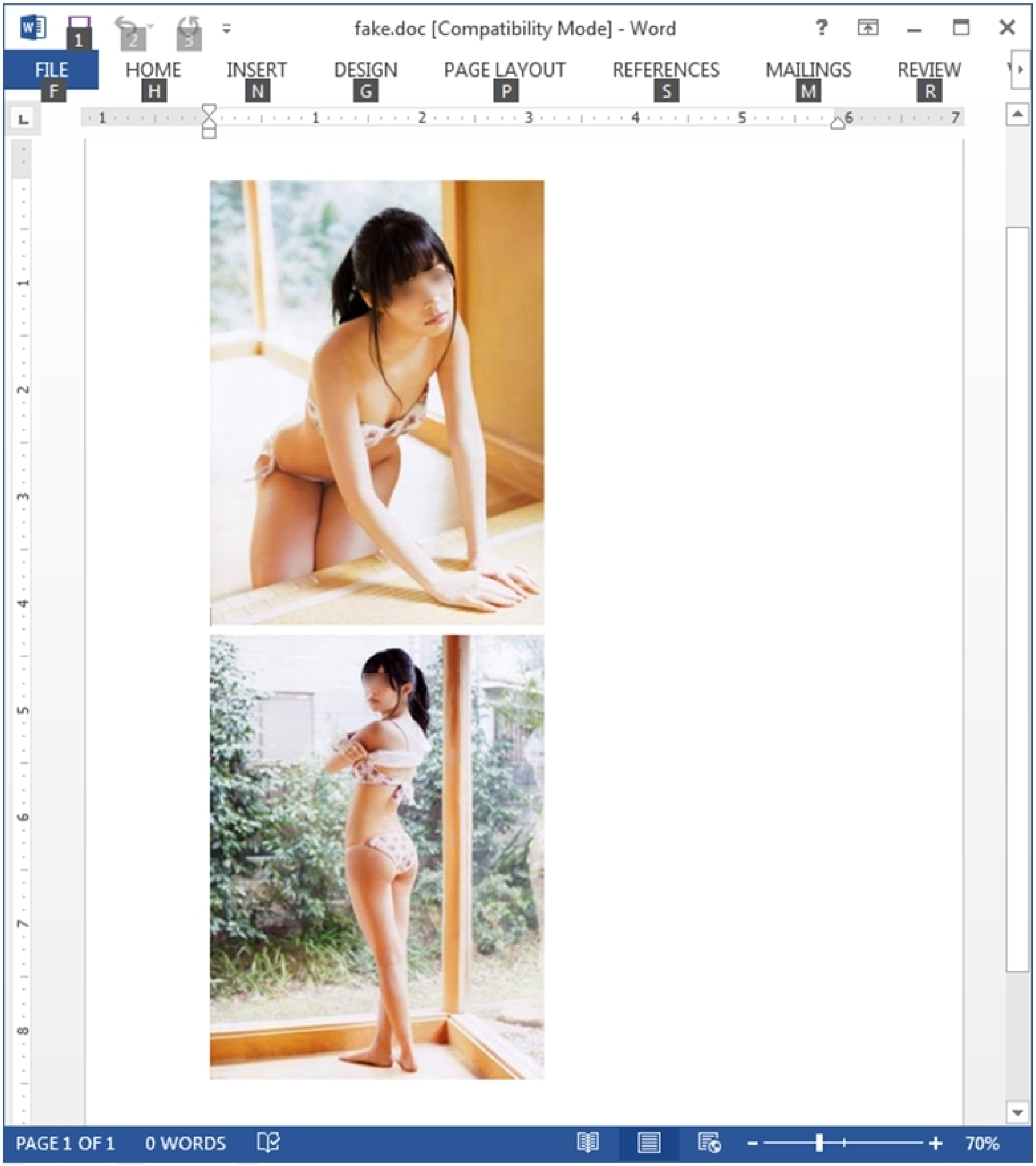
The world of Advanced Persistent Threats (APTs) is well known. Skilled adversaries compromising high-profile victims and stealthily exfiltrating valuable data over the course of many years. Such teams sometimes count tens or even hundreds of people, going through terabytes or even petabytes of exfiltrated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

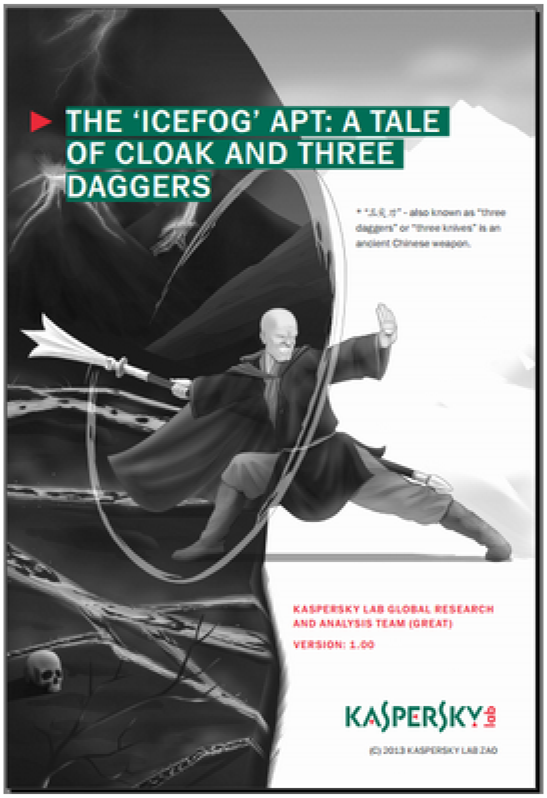
Kaspersky Lab would like to thank KISA (Korea Internet & Security Agency) and INTERPOL for their support in this investigation.

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:


THE 'ICEFOG' APT: A TALE OF CLOAK AND THREE DAGGERS

* "[illegible]" - also known as "three daggers" or "three knives" is an ancient Chinese weapon.

KASPERSKY LAB GLOBAL RESEARCH AND ANALYSIS TEAM (GREAT)

VERSION: 1.00

KASPERSKY lab

(C) 2013 KASPERSKY LAB ZAO

[Click to download]

- APT
- Cyber espionage
- Exploit Kits
- Icefog
- Malware Technologies
- Social engineering
- Spear phishing
- Targeted attacks
- Zero-day vulnerabilities

Authors

Expert GReAT

The Icefog APT: A Tale of Cloak and Three Daggers

Your email address will not be published.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

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

Ferocious Kitten: 6 years of covert surveillance in Iran

Bizarro banking Trojan expands its attacks to Europe

APT trends report Q1 2021

APT10: sophisticated multi-layered loader Ecipekac discovered in A41APT campaign

APT annual review: What the world’s threat actors got up to in 2020

Subscribe to our weekly e-mails

The hottest research right in your inbox

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

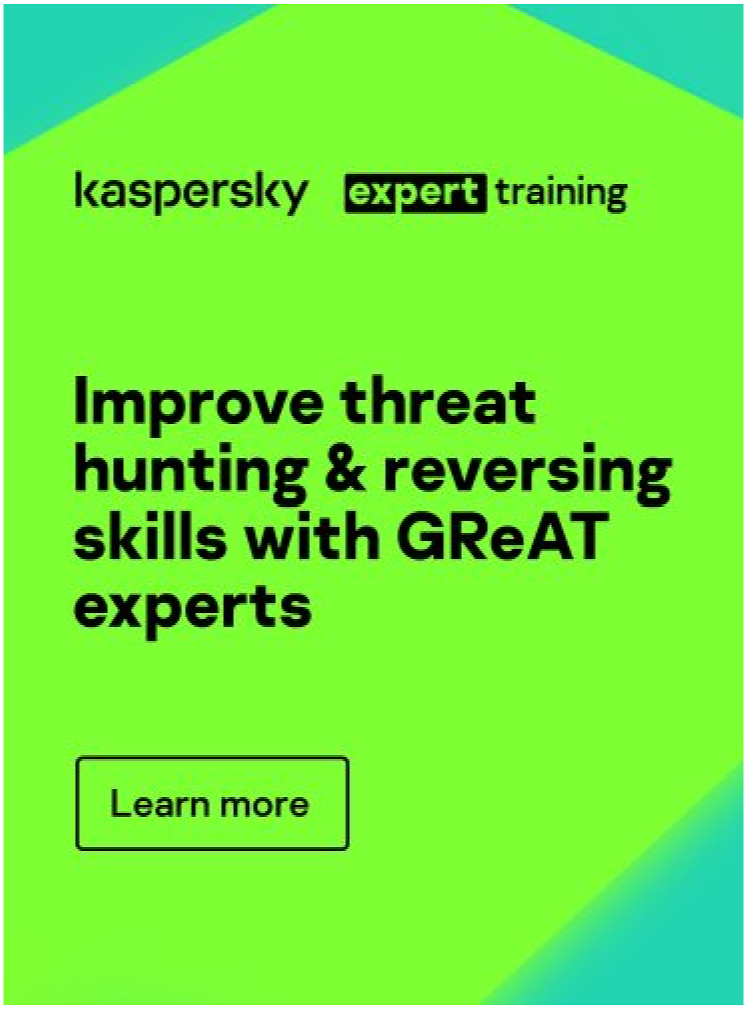
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.


kaspersky
expert training
Improve threat hunting & reversing skills with GReAT experts
Learn more