Kaspersky Lab Uncovers "The Mask": One of the Most Advanced Global Cyber-espionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers

11 Feb 2014
Virus News

New threat actor: Spanish-speaking attackers targeting government institutions, energy, oil & gas companies and other high-profile victims via cross-platform malware toolkit

Today Kaspersky Lab's security research team announced the discovery of "The Mask" (aka Careto), an advanced Spanish-language speaking threat actor that has been involved in global cyber-espionage operations since at least 2007. What makes The Mask special is the complexity of the toolset used by the attackers. This includes an extremely sophisticated malware, a rootkit, a bootkit, Mac OS X and Linux versions and possibly versions for Android and iOS (iPad/iPhone).

The primary targets are government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organizations and activists. Victims of this targeted attack have been found in 31 countries around the world – from the Middle East and Europe to Africa and the Americas.

The main objective of the attackers is to gather sensitive data from the infected systems. These include office documents, but also various encryption keys, VPN configurations, SSH keys (serving as a means of identifying a user to an SSH server) and RDP files (used by the Remote Desktop Client to automatically open a connection to the reserved computer).

"Several reasons make us believe this could be a nation-state sponsored campaign. First of all, we observed a very high degree of professionalism in the operational procedures of the group behind this attack. From infrastructure management, shutdown of the operation, avoiding curious eyes through access rules and using wiping instead of deletion of log files. These combine to put this APT ahead of Duqu in terms of sophistication, making it one of the most advanced threats at the moment," said Costin Raiu, Director of the Global Research and Analysis Team (GReAT) at Kaspersky Lab.
"This level of operational security is not normal for cyber-criminal groups."

Kaspersky Lab researchers initially became aware of Careto last year when they observed attempts to exploit a vulnerability in the company's products which was fixed five years ago. The exploit provided the malware the capability to avoid detection. Of course, this situation raised their interest and this is how the investigation started.

For the victims, an infection with Careto can be disastrous. Careto intercepts all communication channels and collects the most vital information from the victim's machine.

Detection is extremely difficult because of stealth rootkit capabilities, built-in functionalities and additional cyber-espionage modules.

Main findings:

- The authors appear to be native in the Spanish language which has been observed very rarely in APT attacks.
- The campaign was active for at least five years until January 2014 (some Careto samples were compiled in 2007). During the course of Kaspersky Lab's investigations, the command-and-control (C&C) servers were shut down.
- We counted over 380 unique victims between 1000+ IPs. Infections have been observed in: Algeria, Argentina, Belgium, Bolivia, Brazil, China, Colombia, Costa Rica, Cuba, Egypt, France, Germany, Gibraltar, Guatemala, Iran, Iraq, Libya, Malaysia, Mexico, Morocco, Norway, Pakistan, Poland, South Africa, Spain, Switzerland, Tunisia, Turkey, United Kingdom, United States and Venezuela.
- The complexity and universality of the toolset used by the attackers makes this cyber-espionage operation very special. This includes leveraging high-end exploits, an extremely sophisticated piece of malware, a rootkit, a bootkit, Mac OS X and Linux versions and possibly versions for Android and iPad/iPhone (iOS). The Mask also used a customized attack against Kaspersky Lab's products.
- Among the attack's vectors, at least one Adobe Flash Player exploit (CVE-2012-0773) was used. It was designed for Flash Player versions prior to 10.3 and 11.2. This exploit was originally discovered by VUPEN and was used in 2012 to escape the Google Chrome sandbox to win the CanSecWest Pwn2Own contest.

Infection Methods & Functionality

According to Kaspersky Lab's analysis report, The Mask campaign relies on spear-phishing e-mails with links to a malicious website. The malicious website contains a number of exploits designed to infect the visitor, depending on system configuration. Upon successful infection, the malicious website redirects the user to the benign website referenced in the e-mail, which can be a YouTube movie or a news portal.

It's important to note the exploit websites do not automatically infect visitors; instead, the attackers host the exploits at specific folders on the website, which are not directly referenced anywhere, except in malicious e-mails. Sometimes, the attackers use subdomains on the exploit websites, to make them seem more real. These subdomains simulate subsections of the main newspapers in Spain plus some international ones for instance, "The Guardian" and "Washington Post".

The malware intercepts all the communication channels and collects the most vital information from the infected system. Detection is extremely difficult because of stealth rootkit capabilities. Careto is a highly modular system; it supports plugins and configuration files, which allow it to perform a large number of functions. In addition to built-in functionalities, the operators of Careto could upload additional modules that could perform any malicious task.

Kaspersky Lab's products detect and remove all known versions of The Mask/Careto malware.

To read the full report with a detailed description of the malicious tools and stats, together with indicators of compromise, see Securelist. A complete FAQ is also available here.

