The Careto/Mask APT: Frequently Asked Questions

By GReAT on February 10, 2014. 9:03 pm

Research

-
- Tweet

CYBER ESPIONAGE KEYLOGGERS ROOTKITS. TARGETED ATTACKS ZERO-DAY VULNERABILITIES



- GReAT
- Kaspersky Labs' Global Research & Analysis Team

-



What exactly is Careto / "The Mask"?

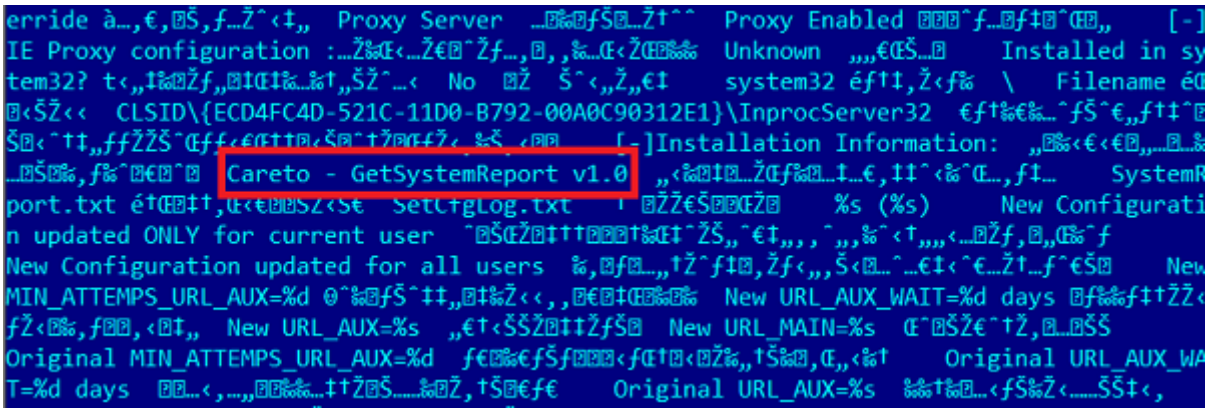
The Mask is an advanced threat actor that has been involved in cyber-espionage operations since at least 2007.

What makes The Mask special is the complexity of the toolset used by the attackers. This includes an extremely sophisticated 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 uses a customized attack against older Kaspersky Lab products in order to hide in the system. This puts it above Duqu in terms of sophistication, making The Mask one of the most advanced threats at the current time. This and several other factors make us believe this could be a state-sponsored operation.

Why do you call it The Mask?

The name "Mask" comes from the Spanish slang word "Careto" ("Mask" or "Ugly Face") that the authors included in some of the malware modules.



Who are the victims? / What can you say about the targets of the attacks?

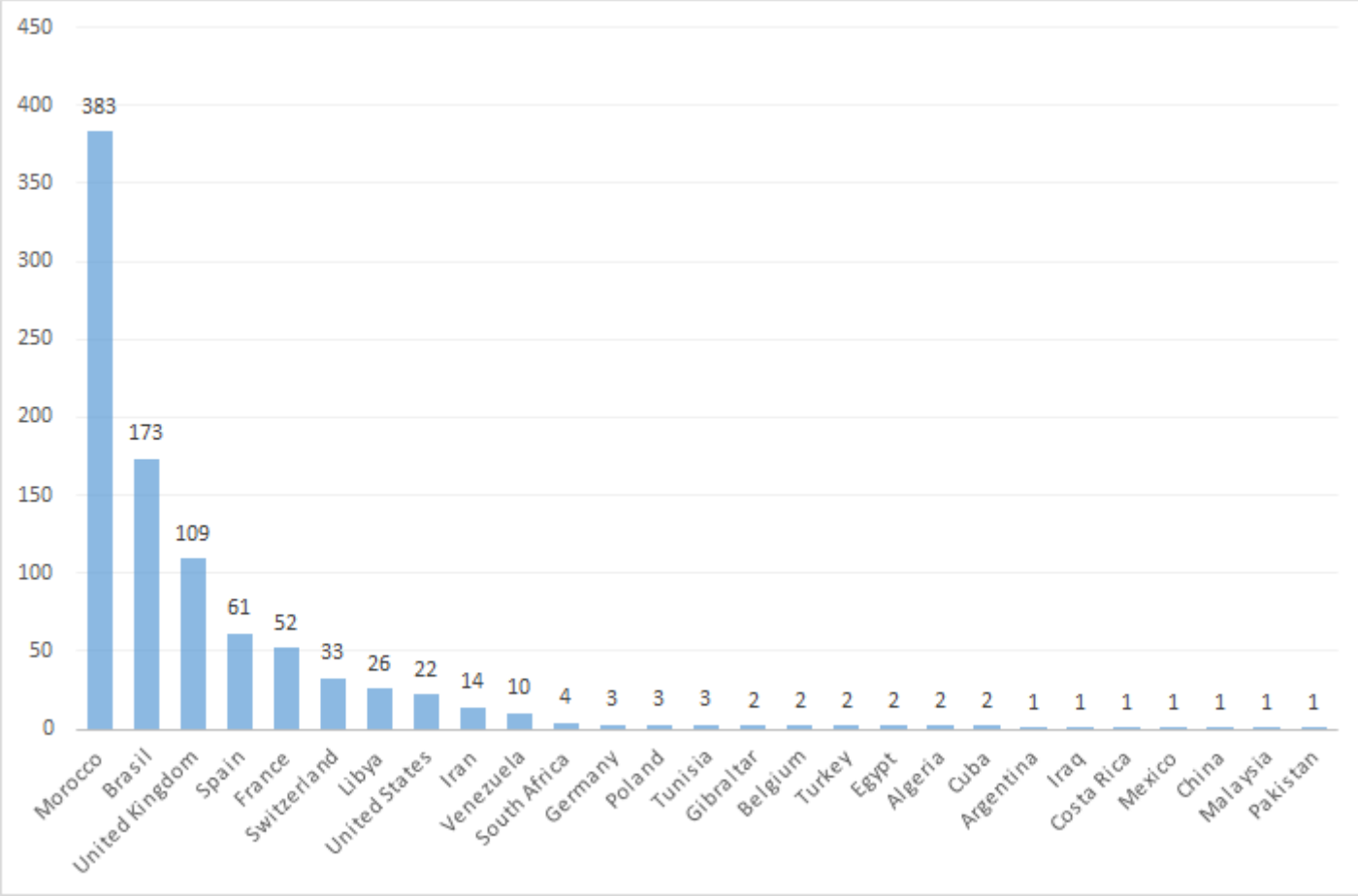
The main targets of Careto fall into the following categories:

- Government institutions
- Diplomatic offices and embassies
- Energy, oil and gas companies
- Research institutions
- Private equity firms
- Activists

Do we know the total number of victims?

Although the exact number of victims is unknown, we observed victims at more than 1000 IP addresses in 31 countries. 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.

Based on an identification algorithm we developed, we counted over 380 unique victims between over 1000+ IPs.



However, considering that victim information has been collected only for some command-and-control servers and sinkholed hosts, the total number of affected countries and unique victims can be much higher.

What does Careto do? What happens after a target machine is infected?

For the victims, an infection with Careto is disastrous. 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. In addition to built-in functionalities, the operators of Careto can upload additional modules which can perform any malicious task. Given the nature of the known victims, the impact is potentially very high.

How does Careto infect computers?

The Mask campaign we discovered 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 his 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 sub-domains on the exploit

websites, to make them seem more legitimate. These sub-domains simulate sub-sections of the main newspapers in Spain plus some international ones like the Guardian and the Washington Post.

Are the attackers using any zero-day vulnerabilities?

So far, we observed attacks using multiple vectors. These include at least one Adobe Flash Player exploit (CVE-2012-0773). The exploit was designed for Flash Player versions prior to 10.3 and 11.2.

The CVE-2012-0773 was originally discovered by VUPEN and has an interesting story. This was the first exploit to break the Chrome sandbox and was used to win the CanSecWest Pwn2Own contest in 2012. The exploit caused a bit of a controversy because the VUPEN team refused to reveal how they escaped the sandbox, claiming they were planning to sell the exploit to their customers. It is possible that the Careto threat actor purchased this exploit from VUPEN.(See story by Ryan Naraine)

Other vectors used include social engineering, asking the user to download and execute a JavaUpdate.jar file or to install a Chrome browser plugin. We suspect other exploits exist as well, but we haven-t been able to retrieve them from the attack server.

Is this a Windows-only threat? Which versions of Windows are targeted? Are there Mac OS X or Linux variants?

So far, we observed Trojans for Microsoft Windows and Mac OS X. Some of the exploit server paths contain modules that appear to have been designed to infect Linux computers, but we have not yet located the Linux backdoor. Additionally, some of the C&C artifacts (logs) indicate that backdoors for Android and Apple iOS may also exist.

Have you seen any evidence of a mobile component - iOS, Android or BlackBerry?

We suspect an iOS backdoor exists but we haven't been able to locate it yet. The suspicion is based on a debug log from one of the C&C servers where a victim in Argentina is identified and logged as having a user agent of "Mozilla/5.0 (iPad; CPU OS 6_1_3 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Mobile/10B329". This appears to indicate it is an iPad, although without a sample, it's hard to be sure.

In addition to this, we also suspect the existence of an Android implant. This is based on a unique version identifier sent to the C&C which is "AND1.0.0.0". Communications with this unique identifier have been observed over 3G links, indicating a possible mobile device.

How is this different from any other APT attack?

What makes The Mask special is the complexity of the toolset used by the attackers. This includes extremely sophisticated malware, a rootkit, a bootkit, Mac and Linux versions and possibly versions for Android and iPad/iPhone (Apple iOS).

Also, The Mask uses a customized attack against older Kaspersky products in order to hide in the system. This puts it above Duqu in terms of sophistication, making The Mask one of the most advanced APTs at the current time. This and several other factors make us believe this could be a state-sponsored operation.

How did you become aware of this threat? Who reported it?

We initially became aware of Careto when we observed attempts to exploit a vulnerability in our products to make the malware "invisible" in the system.

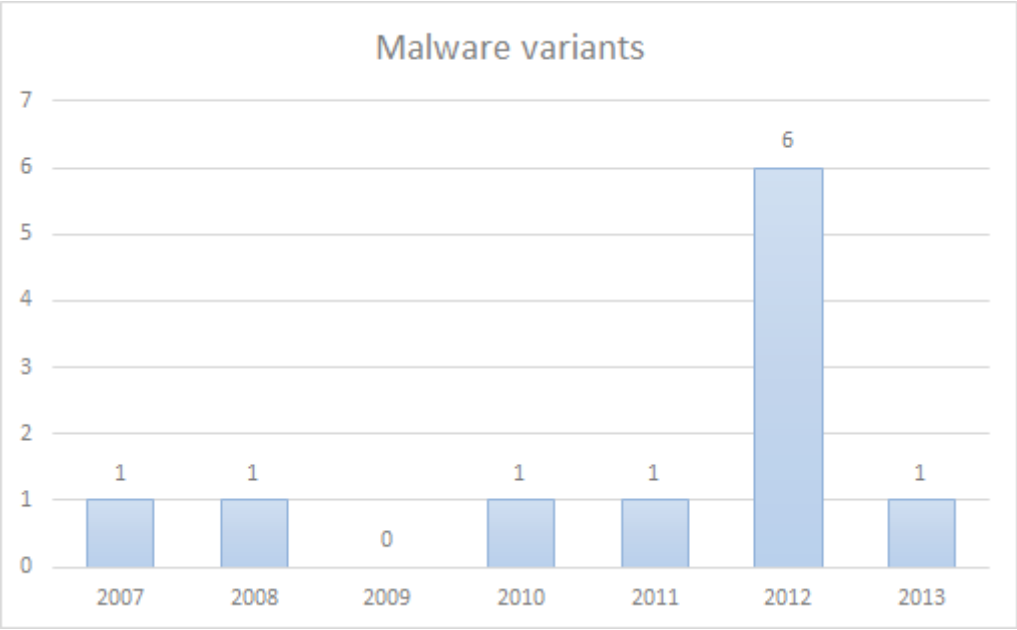
Of course, this raised our interest and our research team decided to investigate further. In other words, the attackers attracted our attention by attempting to exploit Kaspersky Lab products.

Although the vulnerability in the products was discovered and fixed five years ago, there is still a possibility that there are users out there who haven't updated the product. In such cases the exploit can still be active, although it will not prevent us from removing the malware and cleaning the system.

Are there multiple variants of Careto? Are there any major differences in the variants?

Careto is a highly modular system; it supports plugins and configuration files which allow it to perform a large number of functions.

Variants of Careto have different compilation timestamps going back to 2007. Most modules were created in 2012.



Is the command-and-control server used by Careto still active? Have you been able to sinkhole any of the C&Cs?

At the moment, all known Careto C&C servers are offline. The attackers began taking them offline in January 2014. We were also able to sinkhole several C&C servers, which allowed us to gather statistics on the operation.

What exactly is being stolen from the target machines?

The malware collects a large list of documents from the infected system, including encryption keys, VPN configurations, SSH keys and RDP files. There are also several unknown extensions being monitored that we have not been able to identify and could be related to custom military/government-level encryption tools.

Here's the full list of collected files from the configurations we analyzed:

***.AKF,*.ASC,*.AXX,*.CFD,*.CFE,*.CRT,*.DOC,*.DOCX,*.EML,*.ENC,*.GMG,*.GPG,*.HSE,*.KEY,**
***.M15,*.M2F,*.M2O,*.M2R,*.MLS,*.OCFS,*.OCU,*.ODS,*.ODT,*.OVPN,*.P7C,*.P7M,*.P7Z,*.PAB,*.PDF,**
***.PGP,*.PKR,*.PPK,*.PSW,*.PXL,*.RDP,*.RTF,*.SDC,*.SDW,*.SKR,*.SSH,*.SXC,*.SXW,*.VSD,**
***.WAB,*.WPD,*.WPS,*.WRD,*.XLS,*.XLSX**

Is this a state-sponsored attack?

The Mask uses a customized attack against older Kaspersky Lab products in order to hide in the system. In addition, it includes a rootkit, a bootkit, Linux/Mac versions and possibly a version for Apple iOS. This puts it above Dugu in terms of sophistication, making The Mask one of the most advanced APTs at the current time.

Also, we observed a very high degree of professionalism in the operational procedures of the group behind this attack, including monitoring of their infrastructure, shutdown of the operation, avoiding curious eyes through access rules, using wiping instead of deletion for log files, etc. This level of operational security is not normal for cybercriminal groups.

his and several other factors make us believe this could be a state-sponsored campaign.

Who is responsible?

Attribution is a difficult task. On the internet, it is extremely difficult to make a solid attribution due to the volatile nature of the way it was built.

Some clues such as the use of the Spanish language are weak, as it is spoken in many countries, including Latin America, Mexico or the United States (for instance in Miami, where a strong Spanish-speaking community exists).

We should also keep in mind the possibility of false flag attacks before making any solid assumption on the identity of who is responsible without very solid proof.

How long have the attackers been active?

Some Careto samples were compiled as far back as 2007. The campaign was active until January 2014, but during our investigations the C&C servers were shut down.

That's at least five years. We cannot rule out the possibility of the attackers resurrecting the campaign at some point in the future.

Did the attackers use any interesting/advanced technologies?

The Windows backdoor is extremely sophisticated, and the attackers used a number of techniques in order to try to make the attack stealthier. These include injection into system libraries and attempting to exploit older Kaspersky Lab products to avoid detection.

Additionally, the exploits cover all potential target systems, including Mac OS X and Linux. Also, the communication between different exploit shellcode modules is done through cookies, which is quite an unusual technique.

Does Kaspersky Lab detect all variants of this malware?

Yes. Our products detect and remove all known versions of the malware used by the attackers. Detection names:

- Trojan.Win32/Win64.Careto.*
- Trojan.OSX.Careto

Are there Indicators of Compromise (IOCs) to help victims identify the intrusion?

Yes, IOC information has been included in our detailed technical research paper.

You can read our full report here.



[Click to download] https://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/