A Scary “Mask”: Tag, You’re It!

by Sharon D. Nelson, Esq. and John W. Simek

Remember the childhood game of chasing all of your friends in an attempt to merely lay a finger on them so they could assume the role of the “it” person? It doesn’t feel much different these days when dealing with technology. There are a ton of “bad guys” trying to compromise your technology for a variety of reasons. Once your computer is infected it may be a long time before you are even aware of the compromise.

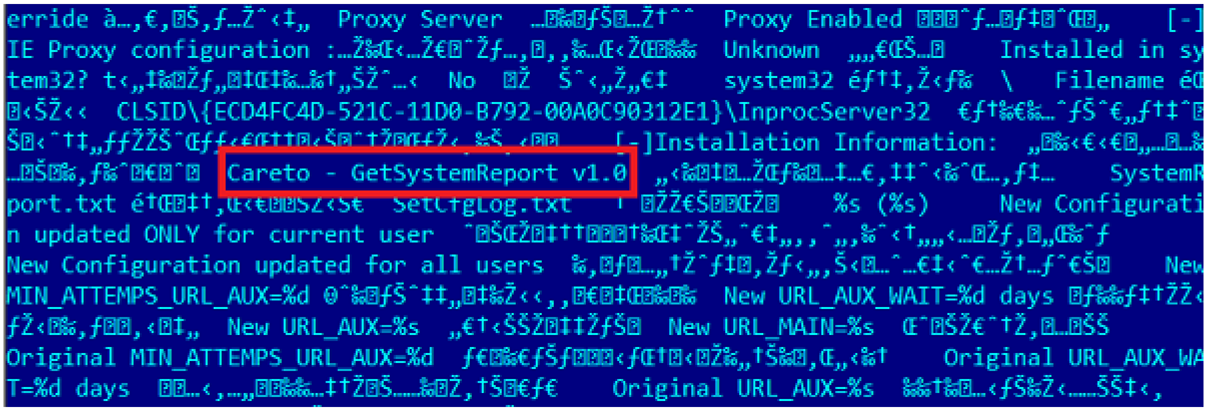
Advanced Persistent Threat (APT)

There are so many definitions of APT that it can make your head spin. It can refer to an advanced attack on a network. But today, an advanced persistent threat is more often defined as a body (e.g. a government) that has the ability and intent to target a specific entity with sophisticated intrusion techniques. Further, we describe an APT as dealing with a cyberthreat. Malware is installed on a computer or network device to gather intelligence and information about the selected target. Probably one of the more famous APTs is the Stuxnet worm, which targeted the computers for Iran’s nuclear program. Usage of APTs has grown tremendously over the last several years and we anticipate an even steeper growth given the recent revelations of spying activity by the NSA, Australian Signals Directorate and the British Government Communications Headquarters.

Mask

This is not the kind of mask that you wear on Halloween (or perhaps every night in New Orleans), but a recently discovered APT that has been around infecting computers for at least the last seven years. It is really a tribute to the programmers that they developed software that has been in hiding for so long. In fact, several researchers have said that the attack, dubbed The Mask or “Careto” (Spanish for “Ugly Face” or “Mask”) is the most sophisticated APT operation they have ever seen.

Kaspersky Labs discovered the campaign while investigating attacks on a patched vulnerability for some of their older products and wrote a blog post describing it. “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).” That’s some pretty scary stuff. They also found the word “Careto” contained within some of the software modules as shown in the included graphic.



```
erride à…,€,□Š,ƒ…Ž˜‹‡„  Proxy Server  …□‰□ƒŠ□…Ž†˜˜  Proxy Enabled □□□˜ƒ…□ƒ‡□˜Œ□„    [-]
IE Proxy configuration :…Ž‰Œ‹…Ž€□˜Žƒ…,□,,‰…Œ‹ŽŒ□‰□‰  Unknown  „„€ŒŠ…□    Installed in sy
tem32? t‹„‡‰□Žƒ„□‡Œ‡‰…‰†„ŠŽ˜…‹  No  □Ž  Š˜‹„Ž„€‡    system32 éƒ†‡,Ž‹ƒ‰  \   Filename é□
□‹ŠŽ‹‹  CLSID\{ECD4FC4D-521C-11D0-B792-00A0C90312E1}\InprocServer32  €ƒ†‰€‰…˜ƒŠ˜€„ƒ†‡˜□
Š□‹˜†‡„ƒƒŽŽŠ˜Œƒƒ‹€Œ‡‡□‹Š□˜‡Ž□Œƒ Ž‹ ‰Š ‹□□     [-]Installation Information:  „□‰‹€‹€□„…□…‰
…□Š□‰,ƒ‰˜□€□˜□  Careto - GetSystemReport v1.0  „‹‰□‡□…ŽŒƒ‰□…‡…€,‡‡˜‹‰˜Œ…,ƒ‡…     SystemR
port.txt é†Œ□‡†,Œ‹€□□ŠŽ‹Š€  SetCfgLog.txt  ‡ □ŽŽ€Š□□ŒŽ□    %s (%s)     New Configurati
n updated ONLY for current user  ˜□ŠŒŽ□‡††□□□†‰Œ‡˜ŽŠ„˜€‡„„,˜„„‰˜‹†„„‹…□Žƒ,□„Œ‰˜ƒ
New Configuration updated for all users  ‰,□ƒ□…„†Ž˜ƒ‡□,Žƒ‹„„Š‹□…˜…€‡‹˜€…Ž†…ƒ˜€Š□    New
MIN_ATTEMPS_URL_AUX=%d 0˜‰□ƒŠ˜‡‡„□‡‰Ž‹‹,,□€□‡Œ□‰□‰  New URL_AUX_WAIT=%d days □ƒ‰‰ƒ‡†ŽŽ‹
ƒŽ‹□‰,ƒ□□,‹□‡„  New URL_AUX=%s  „€†‹ŠŠŽ□‡‡ŽƒŠ□  New URL_MAIN=%s  Œ˜□ŠŽ€˜†Ž,□…□ŠŠ
Original MIN_ATTEMPS_URL_AUX=%d  ƒ€□‰€ƒŠƒ□□□‹ƒŒ†□‹□Ž‰„†Š‰□,Œ„‹‰†    Original URL_AUX_WA
T=%d days  □□…‹,…„□□‰‰…‡†Ž□Š……‰□Ž,†Š□€ƒ€    Original URL_AUX=%s  ‰‰†‰□…‹ƒŠ‰Ž‹……ŠŠ‡‹,
```

Targets

Where did Kaspersky discover the malware? Researchers were able to identify 380 unique victims at more than 1000 IP addresses in 31 countries. The targets included government institutions, diplomatic offices and embassies, research institutions, private equity firms, activists, and energy, oil and gas companies. Many but not all of the victims were in Spanish speaking countries.

What does it do?

Once your machine is infected, the malware intercepts all the communication channels and collects the most vital information from the infected system. It is very hard to detect it since it has stealth rootkit capabilities. Besides the functions programmed into the malware, additional modules can be transferred to the infected computer from the command-and-control (C&C) servers. Since the malware is intercepting the communications, it can steal sensitive information such as encryption and SSH keys.

Safety first

Like so many malware infections, The Mask gets delivered through spear phishing e-mail. The e-mail campaign contains links to malicious websites containing a number of exploits designed to infect the user. If the infection is successful, you are redirected to a benign website that was referenced in the spear phishing e-mail.

The primary lesson is not to be stupid. Be wary of spear phishing e-mail and certainly don't click on links that may appear in the messages or attachments. The good news is that the C&C network is shut down and no longer functioning. Kaspersky thinks the attackers shut down the campaign once they noticed they were being monitored. That's not to say that it won't come back in some other form so be careful out there.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com.