South Korean Financial Companies Targeted by Castov

Created: 29 May 2013 01:05:48 GMT | Updated: 29 May 2013 13:35:18 GMT | Translations available: 日本語

Lionel Payet Symantec Employee

The financial malware landscape is constantly evolving, cybercriminals are becoming more knowledgeable about the financial sector, and attacks are becoming more sophisticated. We've recently released a report, "The World of Financial Trojans," describing the different features and techniques used by banking malware. It would seem that the choices made by the malware authors concerning these techniques and features depend on the cybercriminals' financial resources and market knowledge.

In most cases financial malware favors exploit kits as their infection vector. In the past few months we have been actively monitoring an exploit kit, called Gongda, which is mainly targeting South Korea. Interestingly, we have come across a piece of malware, known as Castov, being delivered by this exploit kit that targets specific South Korean financial companies and their customers. The cybercriminals in this case have done their research on the South Korean online financial landscape.

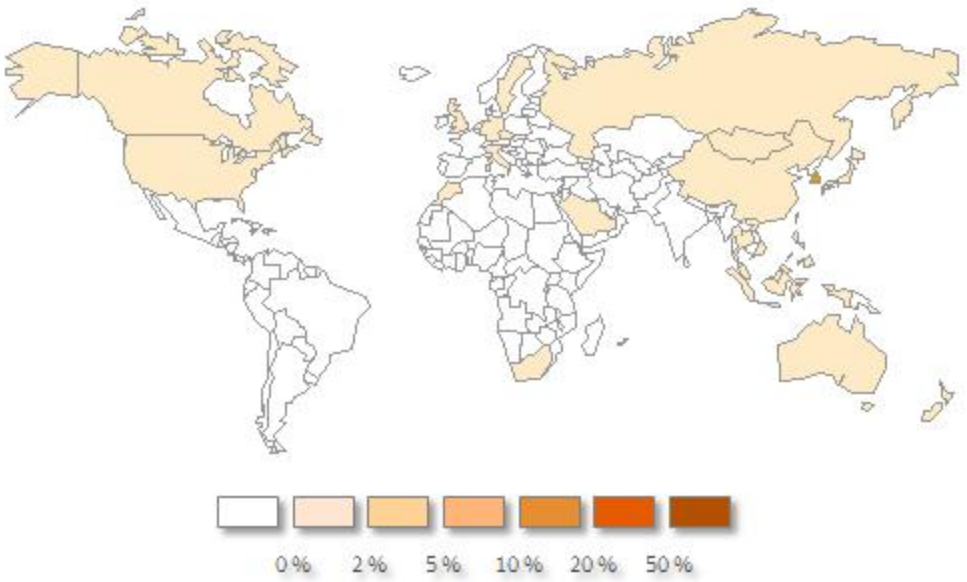

Figure 1. *Heatmap of Gongda IPS detections for May 2013 (98% of hits are in South Korea)*

The initial stage of this threat is Downloader.Castov and is compiled in Delphi with the ability to stop antivrius software which, once inside a computer, will report the infection to its command-and-control (C&C) server and download an encrypted file that is the second stage.

The second stage is Infostealer.Castov. The infostealer checks at specific offsets in a list of clean DLLs (all related to Korean online banking software and security) for opcode instructions and then patches those instructions. The injected code checks strings that appear to be passwords, account details, and transactions. Once the data is found and collected, it will be sent to a remote server.

Combo	Hooked DLLs	Screenshot	Password	Account details	Transaction	Certificate
1	*BaseAddres + 0x618A5* in BankPayEFT.ocx	X	X	X		
	cs_get_pwd in y7csel.dll		X			X
2	*BaseAddr+0x0CEC1* in INIdirectbankUI60.dll		X	X	X	X
3	*ICL_COM_Check_Password* in inicore_v2.3.16.dll	X				
	BG_SSACnK_Load in ssa_LG_UPLUS.dll		X			X

Table 1. *Targeted DLLs and actions taken*

Additionally, the infostealer collects the digital certificates stored in the compromised computer's NPKI directory (%ProgramFiles%\NPKI). Those digital certificates are widely used in South Korea and are issued for financial general purposes (individual/corporate)

such as banking, credit card, insurance etc. They are unique to each user and are valid for one year.

The combination of screenshots, passwords, and digital certificates will allow the cybercriminals to access users' financial accounts.

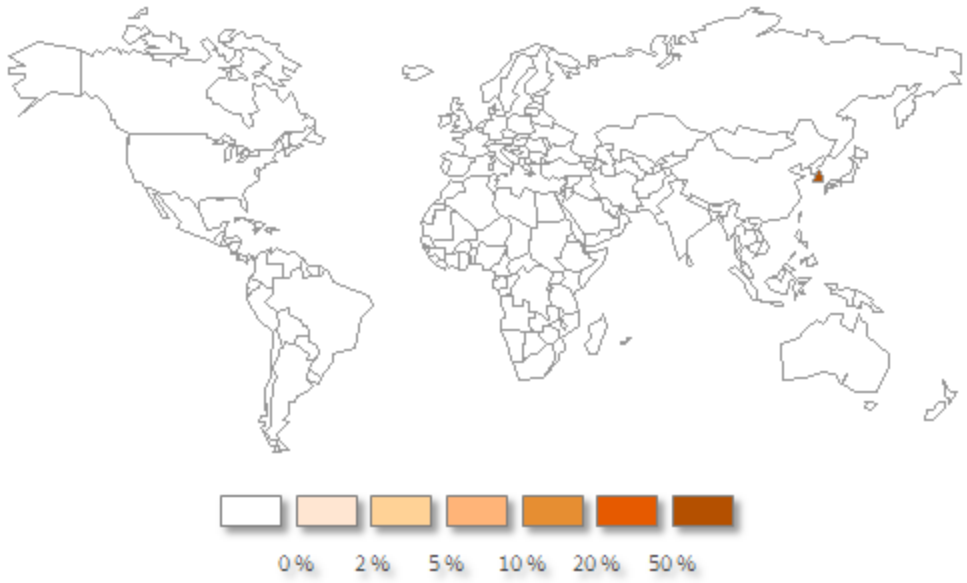

Figure 2. *Heatmap of Castov antivirus detection from January to May 2013*

Symantec has the following protection in place for both Castov and Gongda:

Antivirus protection:

- Downloader.Castov
- Infostealer.Castov

Intrusion prevention protection:

- Web Attack: Gongda Exploit Kit Website
- Web Attack: Gongda Exploit Kit Website 2

To ensure the best protection, we recommend you use the latest Symantec Technologies and up to date antivirus definitions.

Blog Entry Filed Under: