TrendLabs
SECURITY INTELLIGENCE BLOG
Threat News and Information Direct from the Experts
TREND MICRO

Bad Sites | Botnets | CTO Insights | Exploits | Internet of Things | Mac | Malware | Mobile | Social | Spam | Targeted Attacks | Vulnerabilities

blog.trendmicro.com Sites > TrendLabs Security Intelligence Blog > Bad Sites > Banking Trojan Targets South Korean Banks; Uses Pinterest as C&C Channel

Dec15 **Banking Trojan Targets South Korean Banks; Uses Pinterest as C&C Channel**

9:53 am (UTC-7) | by Joseph C Chen (Fraud Researcher)

Share

We recently found a new banking Trojan which targeted several banks in South Korea. This isn't the first, though: in June last year, we saw that several online banking threats widened their range and targeted South Korean banks using various techniques.

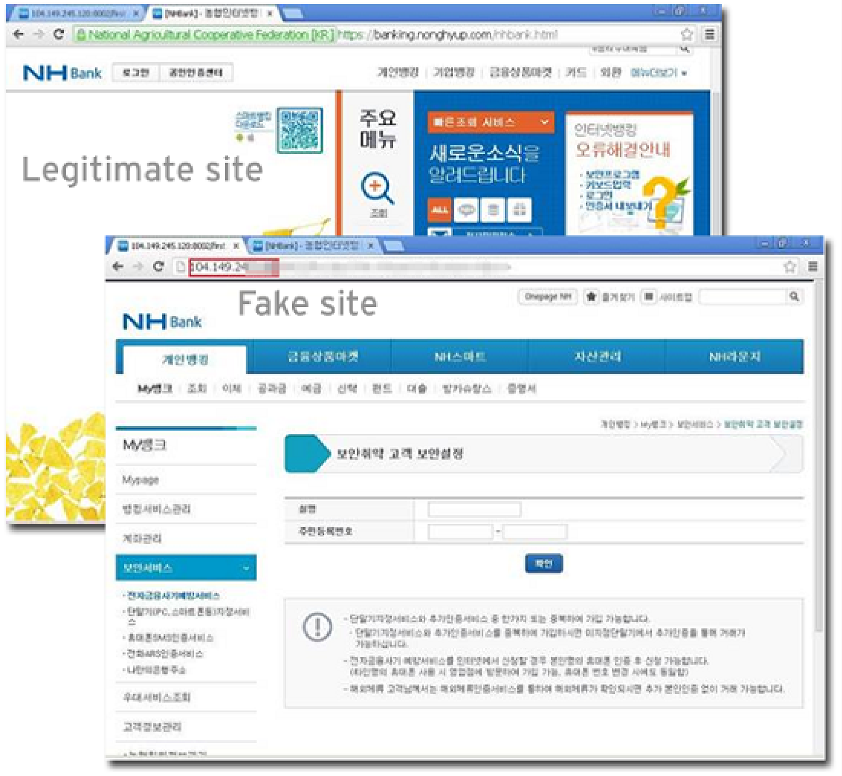
Throughout the course of monitoring similar threats, we noticed a new wave of banking Trojans targeting South Korean banks that show unusual behavior, including the use of Pinterest as their command and control (C&C) channel.

Infection Via Malicious Iframe Injection

This threat is currently affecting users in South Korea via compromised sites leading to exploit kits. In mid-November, we found an infection chain that involved multiple malicious websites in a single infection.

To deliver this threat to the user, legitimate sites are first compromised and an iframe tag is injected. This tag redirects users to a second compromised site which hosts an exploit kit, which delivers the banking Trojan to the user. We detect this as TSPY_BANKER.YYSI.

Once this malware is present on an affected system, users who access certain banking websites using Internet Explorer are automatically redirected to a malicious site. The site contains a phishing page that asks users to input their banking credentials. Users who access the website with other browsers are not affected. (Due to South Korean regulations, users in South Korea generally use Internet Explorer to access local banking sites.)



Search our blog:
Go

Targeted Attacks

- Joke or Blunder: Carbanak C&C Leads to Russia Federal Security Service
- Attack Gains Foothold Against East Asian Government Through "Auto Start"
- Operation Tropic Trooper: Old Vulnerabilities Still Pack a Punch

Bookmark the Threat Intelligence Resources site to stay updated on valuable information you can use in your APT defense strategy

Recent Posts

- Joke or Blunder: Carbanak C&C Leads to Russia Federal Security Service
- Exploring CVE-2015-1701 — A Win32k Elevation of Privilege Vulnerability Used in Targeted Attacks
- Attack Gains Foothold Against East Asian Government Through "Auto Start"

Calendar

May 2015

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

« Apr

Email Subscription

Email Subscription

Your email here

Subscribe

Figure 1. Comparison between legitimate banking site and fake banking site

Below is a list of targeted banking websites that are targeted for information theft:

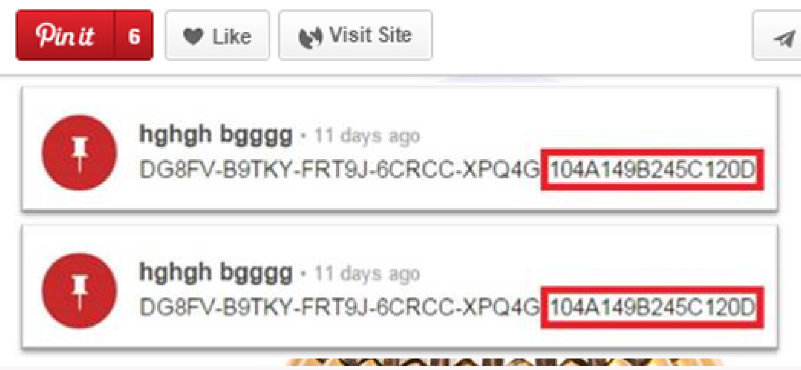
- *hxxp://kbstar.com*
- *hxxp://wooribank.com*
- *hxxp://banking.nonghyup.com*
- *hxxp://v3clinic.ahnlab.com*
- *hxxp://hanabank.com*
- *hxxp://mybank.ibk.co.kr*
- *hxxp://www.ibk.co.kr*
- *hxxp://banking.shinhan.com*
- *hxxp://www.fcsc.kr*

How is this redirection done? If the user visits one of the above sites, the malware will instead cause Internet Explorer to load an iframe that loads various phishing pages. The URL of this banking site will vary, depending on the URL of the original site.

The malware will also spoof the URL in the address bar to make the user believe they are at the legitimate banking site. Upon entering their personal information, they will then be redirected to the fake banking site. In addition to the listed banks, the website of a popular South Korean search engine is similarly modified to open a pop-up window with links to the monitored banks.

The command-and-control (C&C) routines of this malware are interesting. *How* does it know which fake site to redirect users to?

This is normally done by contacting a C&C server, but in this case the attackers didn't do that. Instead, they used the social networking site Pinterest. Cybercriminals can customize redirect victims to different fake servers using comments on certain Pinterest pins:



hghgh bgggg · 11 days ago
DG8FV-B9TKY-FRT9J-6CRCC-XPQ4G104A149B245C120D

hghgh bgggg · 11 days ago
DG8FV-B9TKY-FRT9J-6CRCC-XPQ4G104A149B245C120D

Figure 2. Comments left on the Pinterest pin

We can see above how the comments above include the text *104A149B245C120D*. This is decoded as 104.149.245.120; similarly 70A39B104C109D decodes to 70.39.104.109. The letters are replaced with a dot. This allows the attackers to quickly change their server locations in order to avoid being detected.

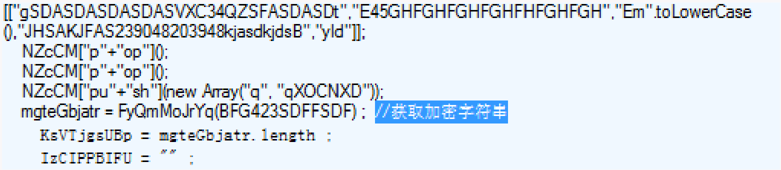
Code Reused From SweetOrange Exploit Kit?

We mentioned earlier that a compromised site was used to host the exploit code which plants malware onto the site's visitors.

Vulnerabilities in Internet Explorer are used to deliver malware in these cases – specifically, CVE-2013-2551 and CVE-2014-0322. Both of these vulnerabilities have long been patched, the former in May 2013 and the latter in September 2014. Javascript obfuscation is heavily used to prevent code analysis. However, we were still able to find that the exploit is similar to that used by the SweetOrange exploit kit, which we discussed earlier this year.

In this month, they are now using the Gongda exploit kit to deliver malware but still targeting users redirected from Korean websites. The CVE-2014-6332 vulnerability in Windows was used in this attack, which was only patched in November.

Additionally, we observed that the deobfuscated exploit code contained comments written in Chinese that described how the vulnerability works.



```
[["gSDASDASDASDASVXC34QZSFASDASDt","E45GHFGHFGHFGHFHFGHFGH","Em".toLowerCase
(),"JHSAKJFAS239048203948kjasdkjdsB","yld"]];
   NZcCM["p"+"op"]();
   NZcCM["p"+"op"]();
   NZcCM["pu"+"sh"](new Array("q", "qXOCNXD"));
   mgteGbjatr = FyQmMoJrYq(BFG423SDFFSDF) ;  //获取加密字符串
     KsVTjgsUBp = mgteGbjatr.length ;
     IzCIPPBIFU = "" ;
```

Figure 3. Chinese comment in exploit code

The malware also communicates to various servers to the URL *hxxp://{various IP addresses}:9000/tongji.html*. (The word *tongji* is the Romanized form of the Chinese word for *statistic*.)

About us

The cybercriminals also used a Chinese web analytics/tracking service named *51yes.com* to generate statistics both for the compromised websites and the C&C servers.

The diagram below shows the entire attack scenario.

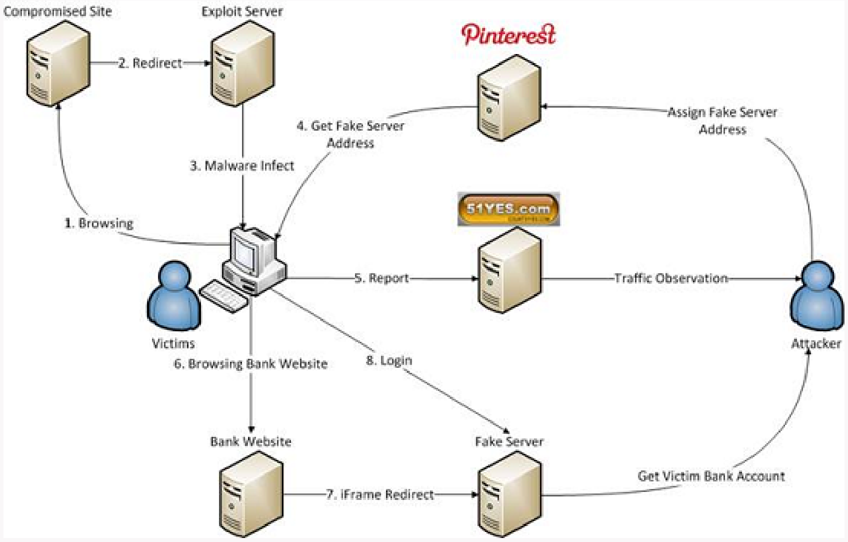


Figure 4. Overview of Attack Scenario

The following hashes are related to this attack:

- 1c0c82b6e53d6d2a6d7c1d2d0e3ccce2
- 6c8791edb12cdb08bee9c567a6d7904c
- bfb00d3f4b94542c5f1f3d1ce6718c7b
- c4e2c9006b9cbc70ede643f6ae623084
- e9d3661aaa4845464a08268e138ae8a4

Vulnerability analysis by Brooks Li
Malware analysis by Marilyn Melliang and Ronnie Giagone

Share this article

This entry was posted on Monday, December 15th, 2014 at 9:53 am and is filed under Bad Sites, Exploits, Malware . Both comments and pings are currently closed.

Comments are closed.

Evaluating the Security of Cyber-Physical Systems: AIS (Paper and Source Code Now Available)
Cross-Signed Certificates Crash Android

- Internet Safety for Kids & Families
- Simply Security News
- Trend Micro Blog [German]
- TrendLabs Security Blog [Japan]
- Cloud Security APAC

Do you have a product-rela question? Visit our eSupport