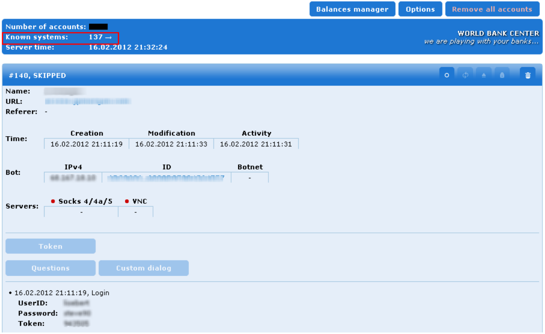
Cridex Trojan Virus

Jaimie Sauls

March 5, 2012

What is the target?

- A plug-in for the virus includes a database of 137 financial institutions.
- The database holds the structure of the bank websites.
- Only 10 out of 43 virus scanners were able to detect the virus.



Number of accounts: [redacted]
Known systems: 137 →
Server time: 16.02.2012 21:32:24

WORLD BANK CENTER
we are playing with your banks...

#140, SKIPPED

Name: [redacted]
URL: [redacted]
Referer: -

Time:

Creation	Modification	Activity
16.02.2012 21:11:19	16.02.2012 21:11:33	16.02.2012 21:11:31

Bot:

IPv4	ID	Botnet
[redacted]	[redacted]	-

Servers:

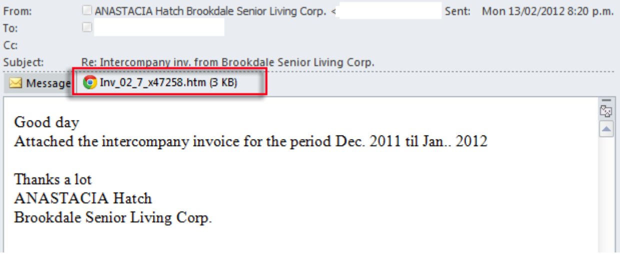
● Socks 4/4a/5	● VNC
-	-

- 16.02.2012 21:11:19, Login
  UserID: [redacted]
  Password: [redacted]
  Token: [redacted]

Figure: Attacker Interface

How does it spread?

- Hundreds of WordPress-based websites were altered
- Email spam containing an 'invoice'



From: □ ANASTACIA Hatch Brookdale Senior Living Corp. < [redacted] Sent: Mon 13/02/2012 8:20 p.m.

To: □ [redacted]

Cc:

Subject: Re: Intercompany inv. from Brookdale Senior Living Corp.

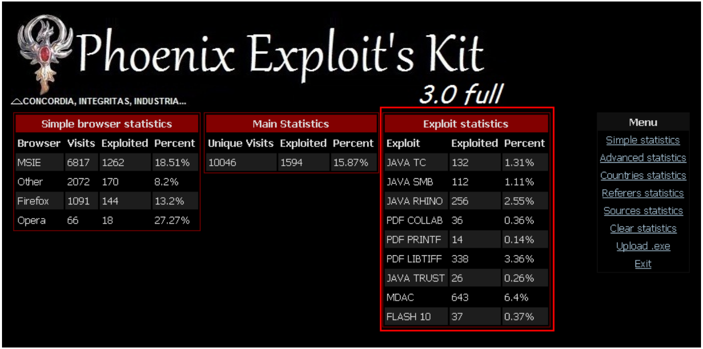
Inv_02_7_x47258.htm (3 KB)

Good day
Attached the intercompany invoice for the period Dec. 2011 til Jan.. 2012

Thanks a lot
ANASTACIA Hatch
Brookdale Senior Living Corp.

What is the Phoenix Exploit Kit?

Don't worry, they have their own blog!



Simple browser statistics

Browser	Visits	Exploited	Percent
MSIE	6817	1262	18.51%
Other	2072	170	8.2%
Firefox	1091	144	13.2%
Opera	66	18	27.27%

Main Statistics

Unique Visits	Exploited	Percent
10046	1594	15.87%

Exploit statistics

Exploit	Exploited	Percent
JAVA TC	132	1.31%
JAVA SMB	112	1.11%
JAVA RHINO	256	2.55%
PDF COLLAB	36	0.36%
PDF PRINTF	14	0.14%
PDF LIBTIFF	338	3.36%
JAVA TRUST	26	0.26%
MDAC	643	6.4%
FLASH 10	37	0.37%

Fun fact: It specifically does not download the virus if you are using Chrome.

Next Steps

- Virus copies information to C drive as an unassuming executable that creates necessary files
- Removes the original malware
- Tries to communicate with its Command and Control servers
  - Becomes part of a botnet
- Downloads customized configuration from the main server

Goal of the Virus

Once set-up is complete, the virus begins to collect information from your computer, such as:

- Cookies
- FTP credentials
- Email accounts
- Visited websites

With this information, the attacker may be able to make fraudulent transactions on your behalf.

How do I protect my computer?

Sources

- http://www.securityweek.com/trojan-targets-nearly-140-financial-institutions-worldwide
- http://labs.m86security.com/2012/03/the-cridex-trojan-targets-137-financial-organizations-in-one-go/
- http://labs.m86security.com/2012/01/massive-compromise-of-wordpress-based-sites-but-'everything-will-be-fine'
- http://labs.m86security.com/2012/02/cutwail-drives-spike-in-malicious-html-attachment-spam/