EXHIBIT 11

Threatpost | The first stop for security news

- Categories
  - Category List
    - Apple
    - Cloud Security
    - Compliance
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Microsoft
    - Mobile Security
    - Privacy
  - Category List
    - SMB Security
    - Social Engineering
    - Virtualization
    - Vulnerabilities
    - Web Security
  - Authors
    - Dennis Fisher
    - Michael Mimoso
    - Christopher Brook
    - Brian Donohue
    - Anne Saita
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Dennis Fisher
    - Michael Mimoso
    - Christopher Brook
    - Brian Donohue
    - Anne Saita
    - Guest Posts
  - The Kaspersky Lab News Service

Featured Posts

All


How a $10 USB Charger Can...


President Proposes National Breach Notification Standard


Microsoft Censures Google For Publishing Windows...

- Podcasts

Latest Podcasts

All


2014 Year in Review


How I Got Here: Andrew Jaquith


Dave Aitel on the Sony Hack


Ryan Olson on the CoolReaper Backdoor

Mike Mimoso on the Sony Breach


Costin Raiu on the Regin APT...

Recommended

- Robert Hansen on Aviator, Search Revenue and the $250,000 Security Guarantee
- Threatpost News Wrap, February 21, 2014
- How I Got Here: Jeremiah Grossman
- Chris Soghoian on the NSA Surveillance and Government Hacking

The Kaspersky Lab Security News Service

- Videos

Latest Videos

All


Twitter Security and Privacy Settings You...


The Biggest Security Stories of 2013


Jeff Forristal on the Android Master-Key...


Researchers Discover Dozens of Gaming Client...


Mozilla Drops Second Beta of Persona...


Vulnerabilities Continue to Weigh Down Samsung...

Recommended

- Twitter Security and Privacy Settings You Need to Know
- Lock Screen Bypass Flaw Found in Samsung Androids
- Facebook Patches OAuth Authentication Vulnerability
- Video: Locking Down iOS

The Kaspersky Lab Security News Service

Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

01/13/15 10:45
There are so many problems with what Cameron said that it's hard to know where to begin. http://t.co/FyQPgf0gBO

Ramnit Variant Targets UK Banks with OTP Attack

Follow @mike_mimoso by Michael Mimoso April 30, 2013 , 2:01 pm

Nowhere is the cat-and-mouse game between attackers and the security of users more evident than with social engineering schemes. Users' awareness of phishing campaigns, for example, may be improving, but that's just forcing attackers bent on identity theft and stealing payment card information to up their games.

Researchers at security company Trusteer report today the last salvo in this back-and-forth, this time with a variant of the Ramnit malware family. Ramnit's authors have been prolific in moving the malware in many new directions. Variants have been tuned to steal social media credentials, banking credentials, and avoid detection by security companies with rootkit functionality.

Related Posts

Dridex Banking Trojan Spreading Via Office Macros

January 7, 2015 , 12:15 pm

New Emomet Variant Targets Banking, Email Credentials

January 7, 2015 , 10:35 am

Microsoft Reports Massive Increase in Macros-Enabled Threats

January 5, 2015 , 2:46 pm

The latest variant to be discovered is targeting a number of UK banks with a one-time password SMS attack, Trusteer fraud prevention solutions manager Etay Maor said. Once the malware infects a victim's computer, it waits for the user to log in to their online bank account to conduct a man-in-the-browser attack, injecting convincing screens into the victim's browser asking them to configure a new one-time password service.

The service is a legitimate one already in place at the banks in question to initiate transactions. This one differs, however, in that it's purporting to the user that the bank now requires a one-time password for all operations related to their online accounts. The attackers even went so far as to soothe the potential concerns of any security conscious users by altering the banking site's FAQ page to reflect the changes implemented by the malware.

"The fact that they've changed the FAQ section to support this fake new process is astonishing to me in terms of details," Moar said. "The attackers are exploiting the trust relationship the user has with the bank. They have no idea the malware is in the middle and injecting new screens. It's amazing how much effort they put into making sure someone falls victim; it's a new level of social engineering."

Once the user logs into their bank account, the malware kicks in and injects a screen with instructions on how to configure a new one-time password service. The user is told that a new single-use destination number will be generated and that they are to enter their one-time password into the input field.

In the background, the Ramnit variant is connecting to the attacker's server which is sending back details of a money mule account, Maor said. Once that's complete, a wire transfer is initiated to the mule, but in order to complete the robbery, the user must be tricked into entering the one-time password and sending it to the temporary receiver number, which is the mule's account number.

"By entering the OTP, the user unknowingly enables the malware to complete the fraudulent transaction and finalize the payment to the mule account," Maor wrote in a blogpost. "This is yet another example of how well designed social engineering techniques help streamline the fraud process."

Maor said that in past attacks he's studied, attackers have built in pre-defined mule accounts, but that tactic isn't feasible because those are easier to block and trace than the dynamic list that seems to be integrated into this particular attack.

"Mules are an important part of the process; you cannot cash out without one," Maor said. "Usually criminals won't re-use the mule in other attacks; they won't last too often. Now it's more dynamic."

Categories: Malware

Recommended Reads

January 7, 2015 , 12:15 pm
Categories: Malware, Social Engineering, Web Security

Dridex Banking Trojan Spreading Via Office Macros

by Michael Mimoso

Spam campaigns in the U.K. are using Office macros to spread the Dridex banking Trojan, researchers at Trustwave report.

Read more...

68 23 6 44 0 1

January 7, 2015 , 10:35 am
Categories: Hacks, Malware, Microsoft, Social Engineering, Web Security

New Emomet Variant Targets Banking, Email Credentials

by Dennis Fisher

Security researchers are tracking a new version of the Emomet malware that is targeting users'

Read more...

149 33 34 123 0 5

January 5, 2015 , 2:46 pm
Categories: Malware, Microsoft, Social Engineering

Microsoft Reports Massive Increase in Macros-Enabled Threats

by Brian Donohue

Microsoft is warning of a significant uptick in threats tricking users to enable macros and then infecting them with malicious macros files.

Read more...

Top Stories

Encryption is Not the Enemy

January 13, 2015 , 11:30 am

Google Passes on Older Android Patches; 930 Million Devices Vulnerable

January 12, 2015 , 12:44 pm

12 Million Home Routers Vulnerable to Takeover

December 18, 2014 , 12:23 pm

President Proposes National Breach Notification Standard

January 12, 2015 , 1:55 pm

WordPress 4.0.1 Update Patches Critical XSS Vulnerability

November 21, 2014 , 9:52 am

Exploits Circulating for Remote Code Execution Flaws in NTP Protocol

December 19, 2014 , 1:33 pm

How a $10 USB Charger Can Record Your Keystrokes Over the Air

January 13, 2015 , 7:03 am

0-Days Exposed in Several Corel Applications

January 12, 2015 , 1:18 pm

Most Targeted Attacks Exploit Privileged Accounts

November 20, 2014 , 4:51 pm

The Final Say

From Kaspersky Blogs

My 2014: A rush and a push and the land is ours an...

There are just a few days left of this year, so I'd better rush and push and go over 2014 in review, before I get on to congratulating everyone for having a super year and wishing all the best f...

Read more...

Bitcoin value plunges following $5M Bitstamp Heist

The new year has started rather badly for the Bitcoin world.

Read more...

Tip of the Week: What is My Kaspersky and how to u...

We have a special solution for multi-device users. If you are using our products on many devices, we recommend you register on the My Kaspersky web portal....

Read more...

Year 2014 in security: looking back over one's sho...

2014 is over, as are the holidays. Time to look back at the business security highlights of past the year....

Read more...

The creator's path ... A student's guide to software...

Victor Yablokov continues his story: 'The creator's path... A student's guide to software development', in which Victor shares his experience of becoming an expert. Don't r...

Read more...

Threatpost | The first stop for security news The Kaspersky Lab Security News Service
CategoriesApple | Cloud Security | Compliance | Critical Infrastructure | Cryptography | Data Breaches | Featured | Featured Podcast | Featured Video | Government | Hacks | Malware | Microsoft | Mobile Security | Podcasts | Privacy | Scams | Slideshow | SMB Security | Social Engineering | Uncategorized | Videos | Virtualization | Vulnerabilities | Web Security

- RSS Feeds
- Home
- About Us
- Contact Us

Authors

Dennis Fisher

Michael Mimoso
Christopher Brook
Brian Donohue
Anne Saita