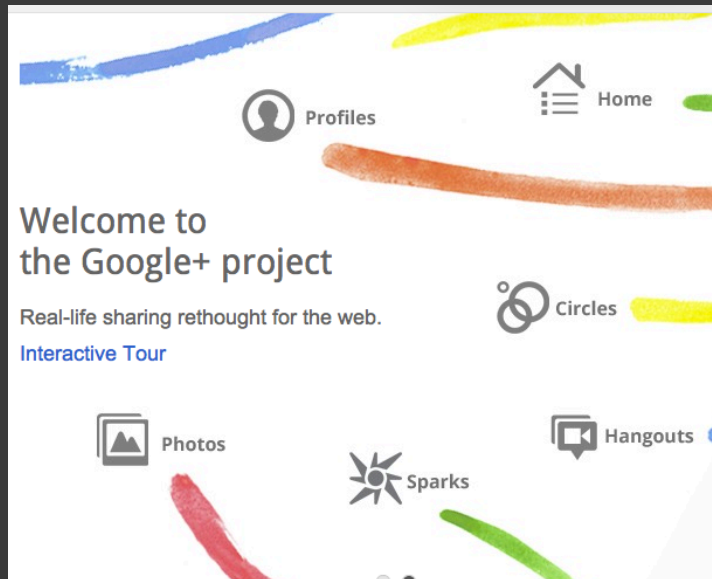
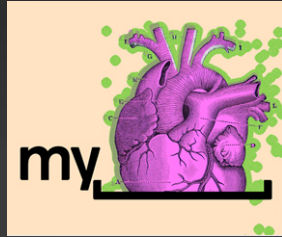


SOCIAL ENGINEERING

The clever manipulation
of the natural human
tendency to trust.

Social Networks - a place to discover old and new friends



Facebook Virus Turns Your Computer into a Zombie

Brennon Slattery, PC World

Dec 5, 2008 10:02 am



"If you really want to hack someone, the easiest place to start is a fake Facebook profile -- it's so simple, it's stupid," Feinberg told *The New York Times*.

Zeus Bank Malware Surges On Facebook

News



Mathew J. Schwartz

Old threat makes a comeback, targeting Facebook users' bank credentials and more.

Bankers Beware Fast-Spreading Facebook Malware

by SEAN SPOSITO
JUN 12, 2013 12:24pm ET

Print
Email
Reprints

Comment

Tweet 43

Share 37

Crooks long ago began ensnaring social network users to infect their computers with the Zeus Trojan virus. Evidence suggests hackers are using the malware to target bank customers via Facebook in larger numbers.

Internet security company Trend

Email Still Effective Marketing Tool?

JUNE 05, 2013 · BY MARCIA KAPLAN



2 Comments



Tweet

119



Share

27



+1

7



Like

23

At a time when social media seems to be the only thing people talk about, email is still an effective ecommerce marketing tool. But merchants will have to alter how they use it if they wish to keep up with changes in how people access email messages.

Are People Still Reading Email?

The research is positive. Several brands reported an increase of five percent in open, click, and conversion rates from 2011 to 2013. The Direct Marketing Association's 2012 Email Tracking Study reported consumers are still signing up to receive marketing related emails.



Social Engineering
Framework

navigation

- GENERAL DISCUSSION >
- INFORMATION GATHERING >
- ELICITATION >
- PRETEXTING >
- PSYCHOLOGICAL PRINCIPLES >
- INFLUENCING OTHERS >
- SE TOOLS >
- SE EXTRAS / RESOURCES >

search

Search

toolbox

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link

page language

Computer Based Social Engineering Tools: Social Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the <http://www.social-engineer.org> launch and has quickly become a standard tool in a penetration testers arsenal. SET was written by David Kennedy (ReL1K) and with a lot of help from the community it has incorporated attacks never before seen in an exploitation toolset. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Contents [hide]

- 1 Beginning with the Social Engineer Toolkit
- 2 SET's Menu
- 3 Attack Vectors
 - 3.1 Spear-Phishing Attack Vector
 - 3.2 Java Applet Attack Vector
 - 3.3 Metasploit Browser Exploit Method
 - 3.4 Credential Harvester Attack Method
 - 3.5 Tabnabbing Attack Method
 - 3.6 Man Left in the Middle Attack Method
 - 3.7 Web Jacking Attack Method
 - 3.8 Multi-Attack Web Vector
 - 3.9 Infectious Media Generator
 - 3.10 Teensy USB HID Attack Vector
- 4 Frequently Asked Questions
 - 4.1 Q. I'm using NAT/Port forwarding, how can I
 - 4.2 Q. My Java Applet isn't working correctly and



HOME SOLUTIONS TRAINING DOWNLOADS BLOG ABOUT US CAREERS CONTACT

Social-Engineer Toolkit

The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community.

The Social-Engineer Toolkit has over 2 million downloads and is aimed at leveraging advanced technological attacks in a social-engineering type environment. TrustedSec believes that social-engineering is one of the hardest attacks to protect against and now one of the most prevalent. The toolkit has been featured in a number of books including the number one best seller in security books for 9 months since its release, "Metasploit: The Penetrations Testers Guide" written by TrustedSec's founder as well as Devon Kearns, Jim O'Gorman, and Mati Aharoni.

SET is included in the latest version of the most popular Linux distribution focused on security, Back|Track. It can also be downloaded through github using the following command:

```
git clone https://github.com/trustedsec/social-engineer-toolkit/ set/
```



Strategy

Recover username and password

Use your account to spread to your friends

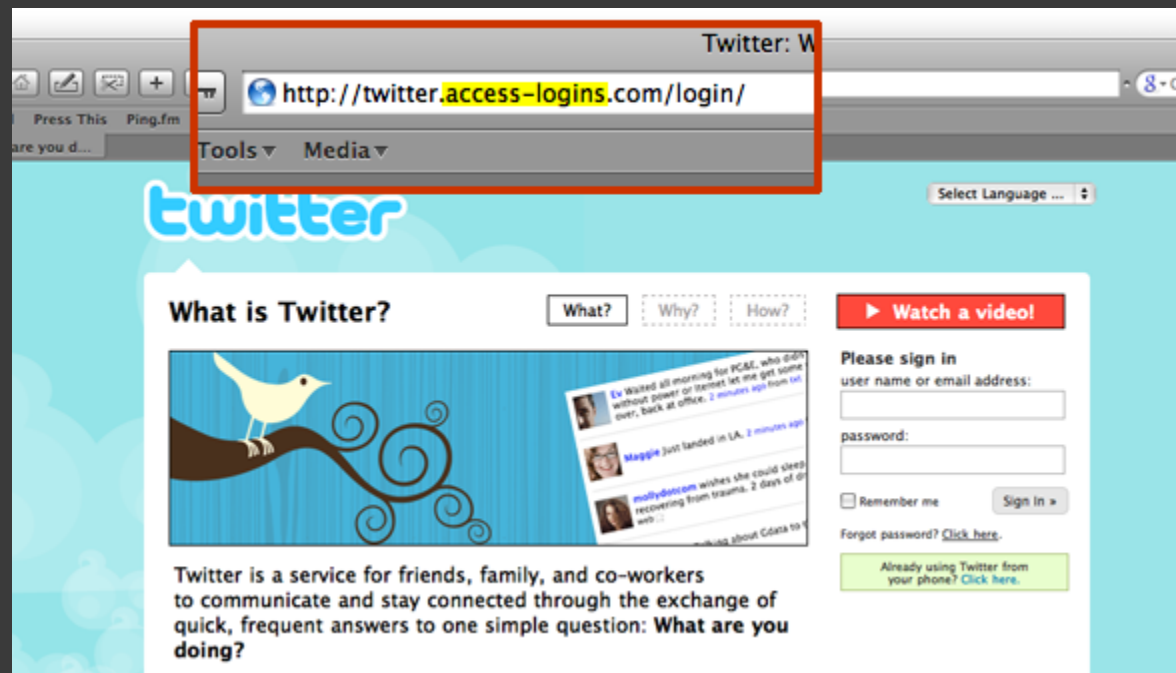
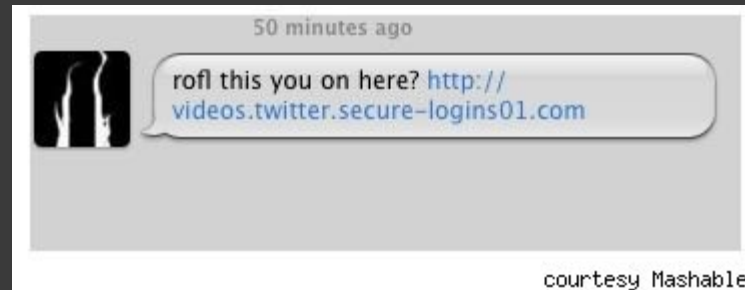
<http://youtu.be/K8lWLwuiDwk>

- Dear user:

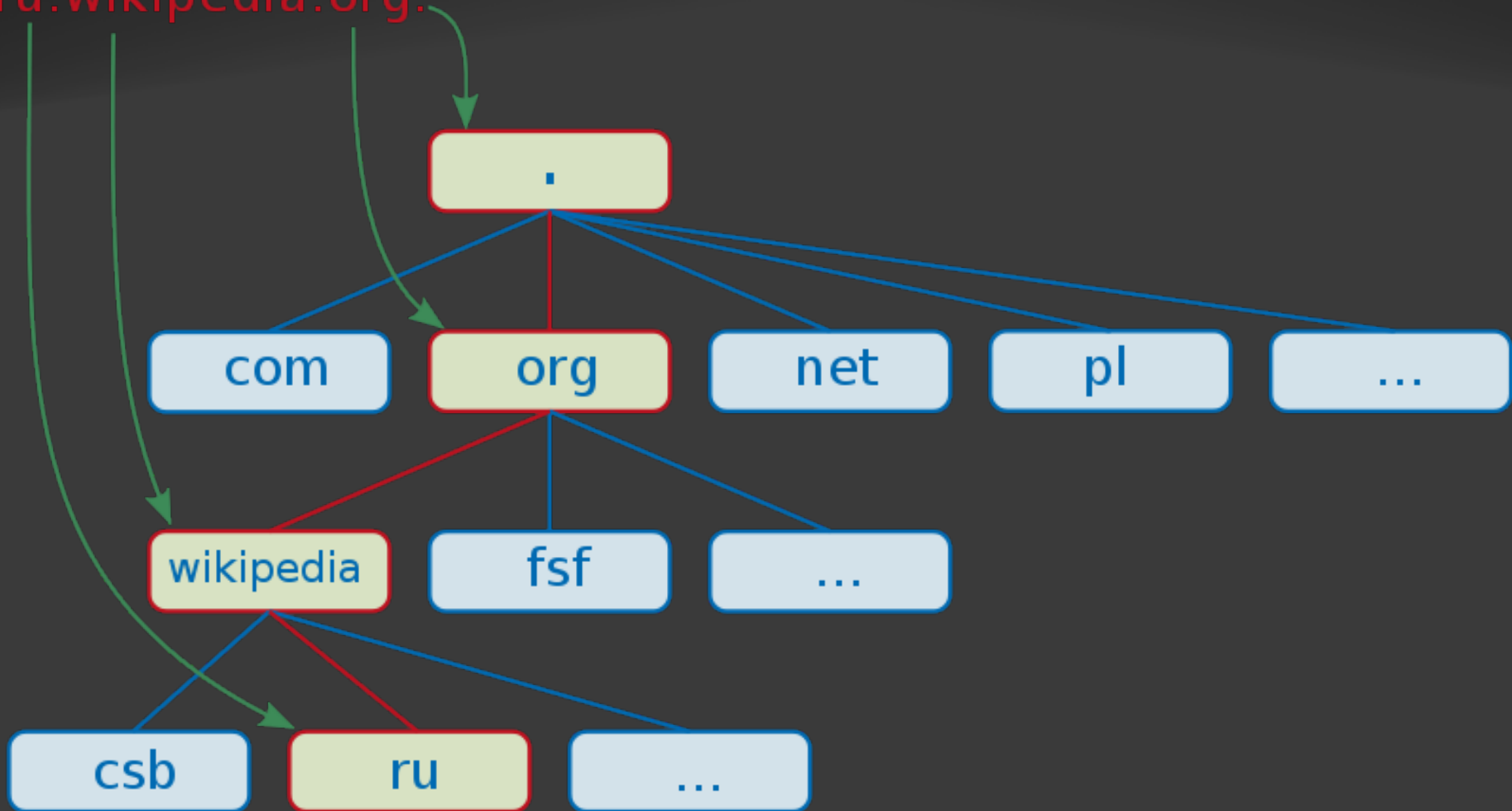
Your facebook account has been locked out due to inactivity. To re-activate your account please click below and enter your account information.

[http://
activate.facebook.uareowned.net/
88adbao798283o8298398?login.asp](http://activate.facebook.uareowned.net/88adbao798283o8298398?login.asp)

- Twitter Phishing scam:



ru.wikipedia.org.



<http://en.wikipedia.org/wiki/File:DNS-names-ru.svg>

protocol://computer.domain.name/pathname/filename.ext

http: // www.cnn.com / tiger-woods / story.html

http: // www.buy.com.money.ru

Which software program would you like to download?

1. ftp://ftp.microsoft.com/software/patches/fixit.exe
2. http://www.micosoft.com/software/patches/fixit.exe

Source: <http://navigators.com/url.html>

Example: [Checkout these links](#)

URL hiding techniques

Encoding

HTML obfuscation


Frames

What happens when these links appear to come from your friend?

URL shortening and obfuscation
are a problem

URL examination services
www.longurl.org

Browsers maintain a “bad websites list”
Hard to keep it updated



Buying more email storage
made me go Google.
www.google.com/postini

[About](#) [Expand](#) [Services](#) [Tools](#)

[Ads by Google](#) [Tinyurl URL](#) [Kral FM Canli](#) [Submit URL Site](#) [DNS Lookup](#)

Browse with Confidence and Increased Security!

Avoid phishing, malware, and viruses by examining short URLs before visiting them. Find out where links *really* take you.

http://is.gd/w

Expand

Stay Safe Online !

When in doubt, don't click it !

This message is brought to you
by NUCIA