SECURE360 Conference

Aditya K Sood (IoActive Inc.)
Emerging Trends in Online Social Network (OSN) Malware
Tuesday 14th, 11:00 AM
Aditya K Sood

- Senior Consultant at IOActive: [http://ioactive.com/](http://ioactive.com/)
- Others
  - Worked previously for Armorize, Coseinc and KPMG
  - Active Speaker at Security conferences
- Personal Website:
  - LinkedIn: [http://www.linkedin.com/in/adityaks](http://www.linkedin.com/in/adityaks)
  - Website: [http://www.secniche.org](http://www.secniche.org)
  - Blog: [http://secniche.blogspot.com](http://secniche.blogspot.com)

Coordinated Research

- Rohit Bansal, Cyber Security Division, PMO INDIA
- Dr. Richard J Enbody, Associate Professor, Michigan State University

About IOActive

Established in 1998, IOActive is an industry leader that offers comprehensive computer security services with specializations in smart grid technologies, software assurance, and compliance. Boasting a well-rounded and diverse clientele, IOActive works with a majority of Global 500 companies including power and utility, game, hardware, retail, financial, media, travel, aerospace, healthcare, high-tech, social networking, and software development organizations.
Disclaimer

- The points presented in this talk is completely based on the independent research and does not relate to any of my previous or present employer.

- A number of images have been taken from different resources (Sophos, etc.) and others collected during real time analysis
  - Phishing emails, spam messages, rogue tweets, etc.
  - Reverse engineering snippets of malware

- The demos (videos) are built using compromised malware and real time analysis of different attacks
Social Networks – Malware Paradigm!

- A malicious link is served on OSNs
- Users follow that link and gets infected with malware

Question – Who is responsible?
- OSN Vendors for serving that link
- Users for following that link
- Browsers for getting exploited
- Third-party plugins (Java, Adobe, etc.) for inherent vulnerabilities
- Anti-virus vendors for not detecting the malware
- IPS/IDS for failing to detect the data exfiltration
The Reality!

40% of Social Network Users Attacked by Malware

Global Malware Hackers Use Social Media to Escape Cyber Sleuths

Social-media malware hurting small businesses

Malware stemming from social networks like Facebook and Twitter infected 33 percent of small firms recently surveyed by Panda Security, causing financial losses.

Malware and spam rise 70% on social networks, security report reveals
OSN Malware : Features

- Conduct operations in a deceptive manner
- Steal identities and sensitive information
- Breach privacy
- Harness the power of inherent design of OSNs
- Exploit the built-in design model to trigger attacks
- Automated in nature
Emerging Trends: History to Now…

- Phishing/Spams
- OSN Scams
- LikeJacking/ClickJacking
- Rogue Applications and Profiles (Facebook, Twitter etc.)
- Sponsored Advertisements and Malvertisements
- Worms
- Socioware
Users are the Assets!

- OSNs User Base
- Facebook
  - 1.05 Billion

Refer: Facebook quarterly earning – Q-4
http://www.scribd.com/doc/123034877/Facebook-Q4-2012-Investor-Slide-Deck
Users are the Assets!

OSNs User Base
Twitter – 465 Million and reached 500 Million recently
Refer: http://blog.sironaconsulting.com
43% of fake profiles have never updated their Facebook status...
...compared to 15% of real people who have never updated their Facebook status.

Claim to have attended college

40% REAL PEOPLE

68% FAKE PROFILES

Average number of friends

REAL PEOPLE 130 FRIENDS

FAKE PROFILES 726 FRIENDS

Average number of tags per photo

REAL PEOPLE 1 TAG FOR EVERY FOUR PHOTOS

FAKE PROFILES 136 TAGS FOR EVERY FOUR PHOTOS

Barracuda Study (2012)
- http://www.barracudalabs.com/fbinfographic/
OSN Chain Infection!

Chain Exploitation — Social Networks Malware
Online Social Network Malware - Trends
Trend (1) – Phishing (Facebook)

Phishing

- Old school tactic but amazingly, it still works
- Brand name manipulation and social engineering
- Exploits ignorance and doubt among OSN users
- Extensively used for conducting drive-by-download attacks
Trend (1) – Phishing (Twitter)
Trend (1) – Spamming (Twitter)

- Used in Surveys Scams
- URL shortener services are very fruitful
  - Hiding targets
  - Serving exploits
  - Redirections on the fly
Trend (2) – Scams

- Illegitimate surveys and polls
- Spreading malware
- Stealing users information
Note: A number of fake facebook profiles even exist for more than a year.
Trend (4) – Malicious Applications

Opening picture190962329_profile12790917.zip

You have chosen to open
picture190962329_profile12790917.zip
which is a: WinRAR ZIP archive (73.9 KB)
from: http://www.smaonline.ro

What should Firefox do with this file?

- Open with WinRAR.ZIP (default)
- Save File
- Do this automatically for files like this from now on.

OK Cancel

Photo has been moved.

This photo has been moved to other location. To view this photo click View Photo.
Trend (5) – Malvertisement
Trend (6) – Worms

Koobface (2009-2010)
- Inject malicious content in wall posts. Hoax warnings
- Sending emails to inboxes of the registered Facebook’s users
- Chain infection to distribute koobface malware to a large set of users
- Also used stolen Facebook credentials for malicious purposes

Likejacking Worm (2010 -2012)
- Injecting malicious links
- To raise ratings by triggering unauthorized likes
Trend (6) – Worms (cont…)

Lily Jade (2012)
- Exploits Crossrider web API to build plugin to attack different browsers
- Uses jQuery to send malicious messages

Ramnit Worm (2010 - 2012)
- Stolen Facebook accounts’ credentials are used to deliver malicious messages through compromised accounts
Trend (7) – Likejacking/ Clickjacking

- Injecting malicious links with likes
  - Manipulating the implementation of like functionality
  - Very effective in tricking users to follow the likes
- Earlier, used to spread malware but now:
  - It has become a legitimate business model. Amazing!
  - For $5, one can get a number of likes!
LikeJacking/Clickjacking Demo (Facebook)

- This demo shows how LikeJacking was conducted earlier to trigger infections in Facebook.
- It worked when Facebook did not implement any confirmation button.
- The newly deployed code actually restricts the active implementation of this attack, but it is not the complete solution.
- A new variant of LikeJacking code can be expected in the near future.
Trend (8) – Identity Stealing (Grabbers)

- Stealing OSN specific user credentials
- Hooks browser to capture all the POST request used for submitting forms
- HTTP POST requests carry accounts credentials
- OSN specific account credentials are used earlier for building worms
  - Example: Koobface

- Details on Form-grabbing technique:
OSN Grabber (Demo)

- A bot having built-in functionality to capture OSN data is installed in the testing environment
- Facebook website is opened and credentials are provided
- The bot steals the user credentials
Trend (9) - Socioware

- Malware targeting OSN from end user machines
- Malware exploiting OSNs functionality in an automated manner
- Virtually, turns your friends into frenemies
- Exploit users by compromising
  - Identity
  - Privacy
- Completely deceptive in nature
Trend (9) – Inside Socioware

Socioware

- A class of malware explicitly use to spread infections across different OSNs (Facebook, Twitter, etc.)
- Primarily developed as built-in components of bots.
  - Named as SPREADERS in the underground economy
- Explicitly used for building OSN worms
- Subverts capabilities of OSNs to distribute malware to a large sections of users

How?

- Based on Man-in-the-Browser (MitB) paradigm
- Triggering infections from already infected machines
- Browsers are hooked and OSN web pages are injected
- Exploit trust model that exists between users
Understanding Socioware – Targeting Facebook Online Chat
Facebook Chat – Infections!

Sophos: Facebook Chat is Attacked by Hackers to Spread Malware

Facebook Chat Feature Exploited for Spreading Malware

Beware of Facebook chats bearing hidden malware

MUST READ: Facebook chat spreading the Dorifel malware

Facebook chat worm continues to spread

Latest Facebook Chat System Dorkbot Malware

Dangerous Malware Link Spreading Through Facebook Chat System

Facebook virus spreads via photo album chat messages
Spreadsers – Distribution!

- Creating malicious Facebook application and embedding Java applet that triggers drive-by-download to install spreader
- Using exiting botnet to upload infected machines with spreaders
- Pay-per infection (PPI) with Browser exploit Packs (BEPs) to infect websites to distribute spreaders
- Using USB devices to distribute spreaders physically
Spreaders – Components!

- Executable (Injection Engine): The primary logic file that spreads malicious messages
- Status Notification Component: The executable updates about the status of the injection (success/failure)
- Link Storage Component: It stores the different injection (URLs) to be injected by the executable
- Time Interval Component: A logic which decides when to inject the malicious link based on the timing
Spreaders – Internal Design

- **Step 1** - Installed in the end users’ machines
- **Step 2** – Hooks browser libraries and controls HTTP communication channel
- **Step 3** – Remains dormant and starts monitoring engine to detect OSN surfing through browsers
- **Step 4** - On successful detection, triggers internal logic to find pattern in the web page
- **Step 5** – Read the malicious message from file (or internally) for injection
- **Step 6** – Triggers injection and notify the state (success or failure to C&C)
- **Step 7** – Deactivates itself for a few minutes and starts infecting again
Spreader Demo

- Spreader is installed in the controlled virtual environment
- Facebook website is opened and credentials are provided
- Facebook chat is activated to send messages to friends
- Spreader injects malicious messages after a given time interval
Socioware - Universal Web Injests

- Automated way to inject unauthorized content in HTTP responses
- Technique works as:
  - Hijacking the communication channel of browsers
  - Manipulating the low level HTTP protocol libraries used by browsers
- Primarily aimed for:
  - Stealing information from banking websites on end user machines
Socioware - Universal Web Injects

- **set_url [target webpage URL] * GP**
  - Setting the target web page to inject
  - For all HTTP requests $G = GET \& P=POST$

- **data_before/ data_end tag**
  - Setting the required data in the web page before injected content

- **data_inject/ data_end tag**
  - Data to inject in the web page

- **data_before/ data_end tag**
  - Setting the required data in the web page after the injected content
Your Facebook account is temporary locked!
To continue using your account please answer few questions:

First Name: 
Last Name: 
E-mail: 
Year of birth: 
Password: 
Ukash 20 euro voucher #: 

To confirm verification you have to enter 20 euro Ukash voucher. Ukash vouchers are sold by ukash.com website and Ukash.com is not affiliated with Facebook company. 20 euro will be added to your Facebook main account balance. This verification is used to confirm your age and country of origin.
The Ukash voucher consists of 19 numbers and face value (sum), begins on "633". For example 6337180116517630998
Facebook Built-in Protection

Immune System
- Users feedback on the channel that is used by malware as a launchpad
- Based on message classifier which identify users as infected with malware when the classifier marked messages as shady in collaboration with feedback provided by the users' friends
- User marking in conjunction with URL characteristics and features

Traffic Analyzer
- Crawling every possible URL
- Resolving DNS entries and checking against blacklists
- It requires resolving of URL shorteners too
Point to Ponder!

Why end users and client side software are still the priority targets?
Future!

- OSN will remain the centralized target for distributing malware
- Trend of automated infections against OSN will continue
- Significant increase in socioware based crimeware services
- Possibility of advanced likejacking attacks
- Socioware attacking mobile platforms
Questions!
Thanks!

- To all my team members
- IOActive for its continuous support
- Secure 360 team for giving me an opportunity to speak