Social Engineering Countermeasures

Phishing

Prepared By: M. Georgia Gibson Henlin, Andrew Nooks

Presented by: Andrew A. Nooks

About Us

Andrew A. Nooks

- BSc. Computer Science
- Certs: CISSP, CISM, CISA, CRISC
- Core IT Experience: 14+ yrs
- IT Security: 8+ yrs
- Consultant
- Director

M. Georgia Gibson Henlin

- Masters in Innovation Law & Policy U of T;
- Certs: CCFE; CHFI.
- Technology and Cybersecurity Practice

Definition

- **Social engineering** is the act of manipulating people into performing actions or divulging confidential information.

- **Phishing** is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Web sites

Social Engineers

- Hackers
- Penetration Testers
- Spies or Espionage
- **Identity Thieves**
- Disgruntled Employees
- Information Brokers
- **Scam Artists**
- Executive Recruiters
- Sales People
- Governments
- Everyday People

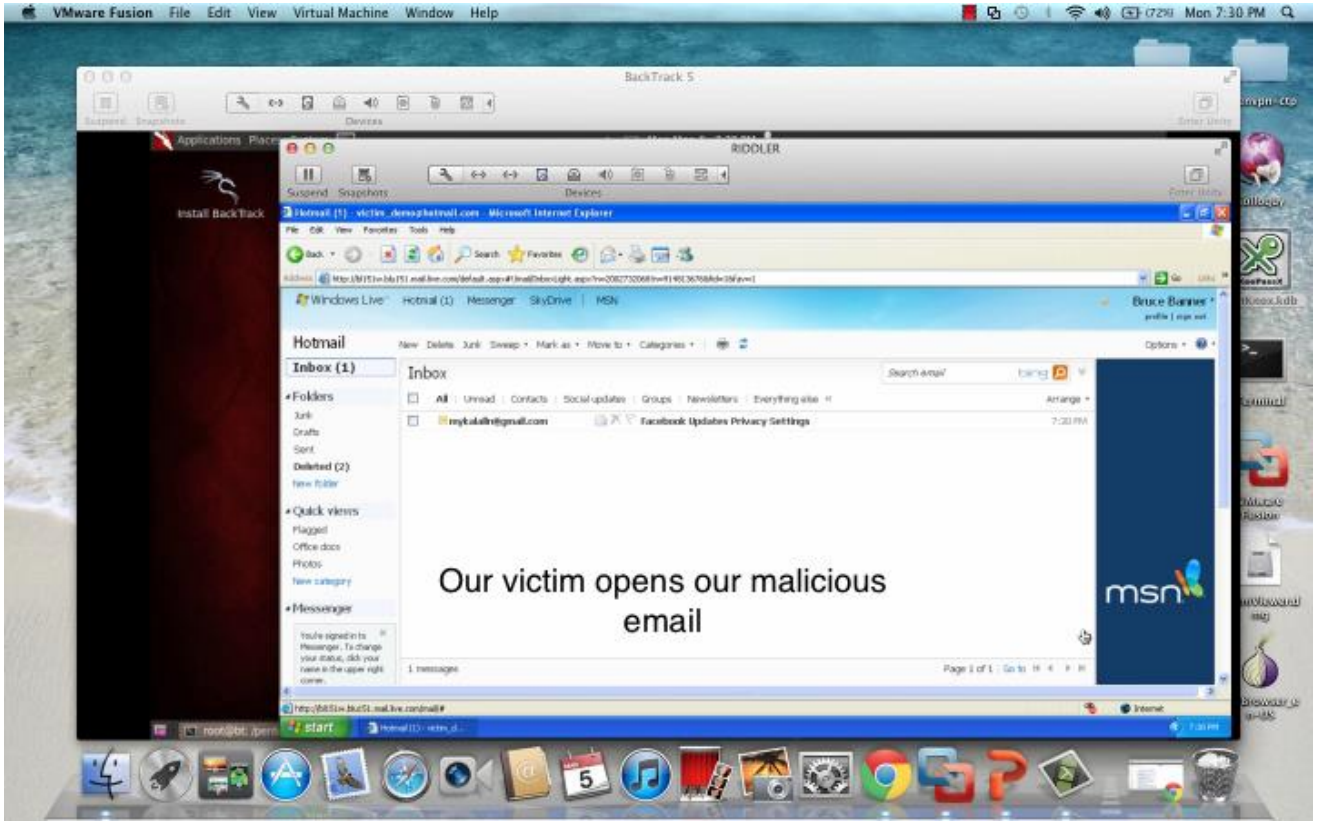
Purpose

- Intelligence gathering
- Espionage (Business or Government)
  - Trade Secrets or Security
- **Financial Fraud**
- **Personal Gain**

Approach

- **Impersonation by telephone**
  - IT department
  - Phone company
  - Senior Management
- Physical Impersonation
  - Co-worker
  - Phone Company
  - Ancillary Staff
- **Electronic Communications**
  - **Internet**
  - **Social networks**
  - **Email**
- Other Methods
  - Mail theft
  - Garbage surfing
  - Shoulder surfing

DEMO – Video (Lab Created)



DEMO – SCREENSHOTS FROM ACTUAL PHISHING INCIDENT

Phishing Email: Could also be invitation to view a pic or video

Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.
This message was marked as spam using the Outlook Junk E-mail filter.
This message was converted to plain text.

rom: RealDatingSystem <afRcDpn35@agipiberia.es> Sent: Tue 1/15/2013 6:31 AM
o: Andrew [redacted]
c:
ubject: New messages. Check your inbox

Dear andrew [redacted]

You've got 11 new messages from girls.

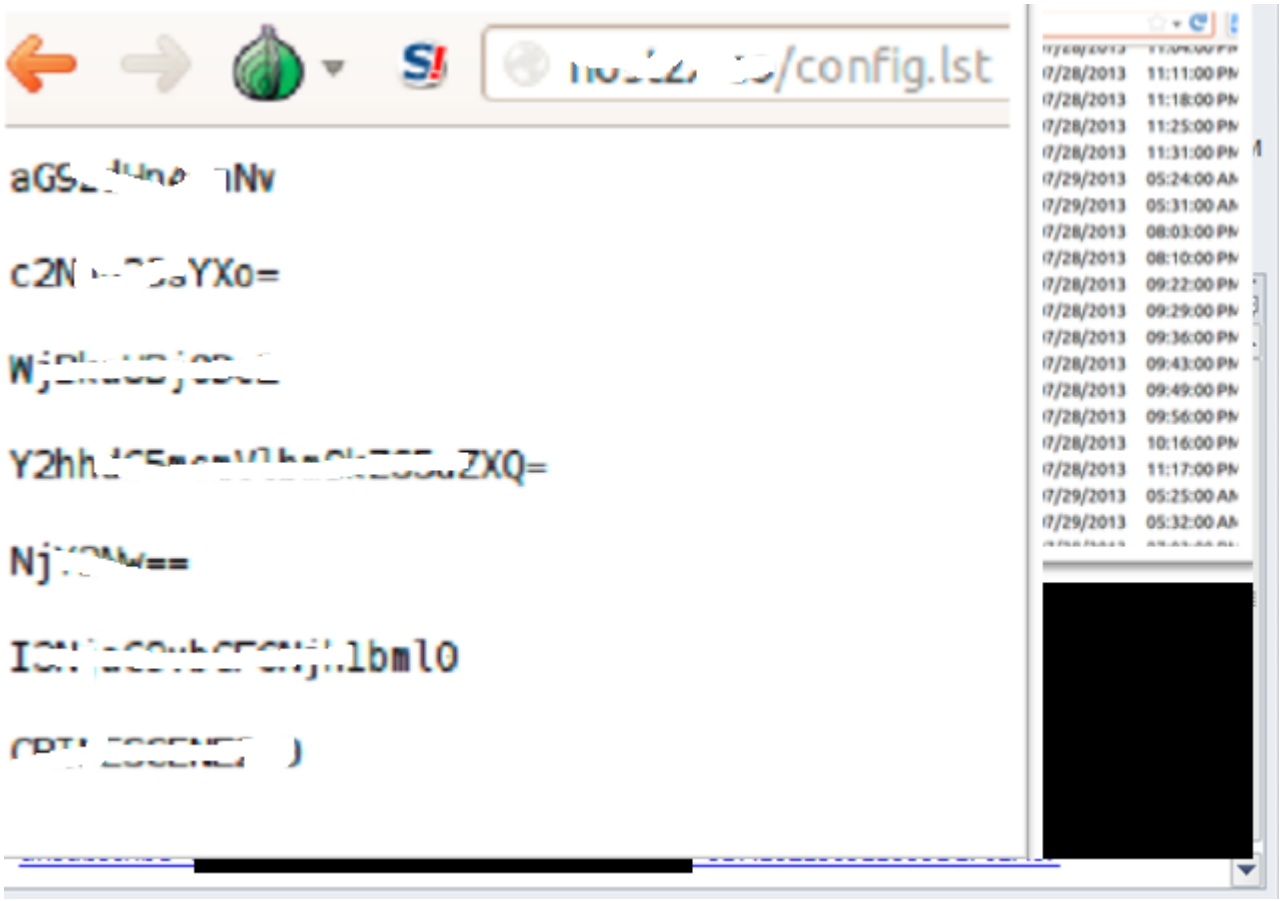
Please follow link below to check your inbox:

https://w[redacted]ru/read_msg?id=[redacted]<http://www.dating2008.ru/>

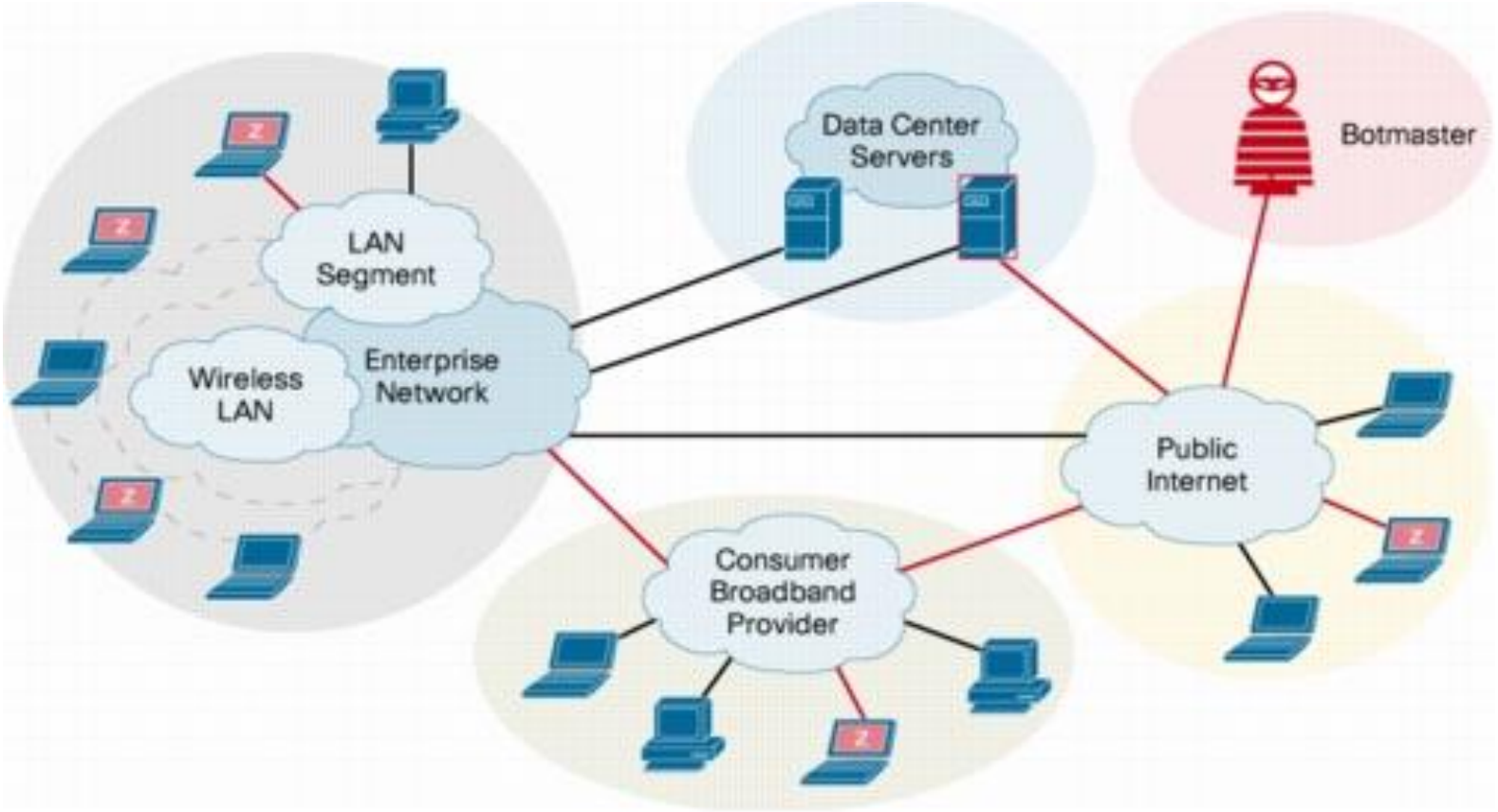
(c) 2013. RealDiatingSystem.
All rights reserved.

About us <http://w[redacted]/#about> | Legal notice
<http://w[redacted]/legal> | Unsubscribe <http://www.da[redacted]u/?
unsubscribe=[redacted]=8DAE62E369EB[redacted]EF01A8F>

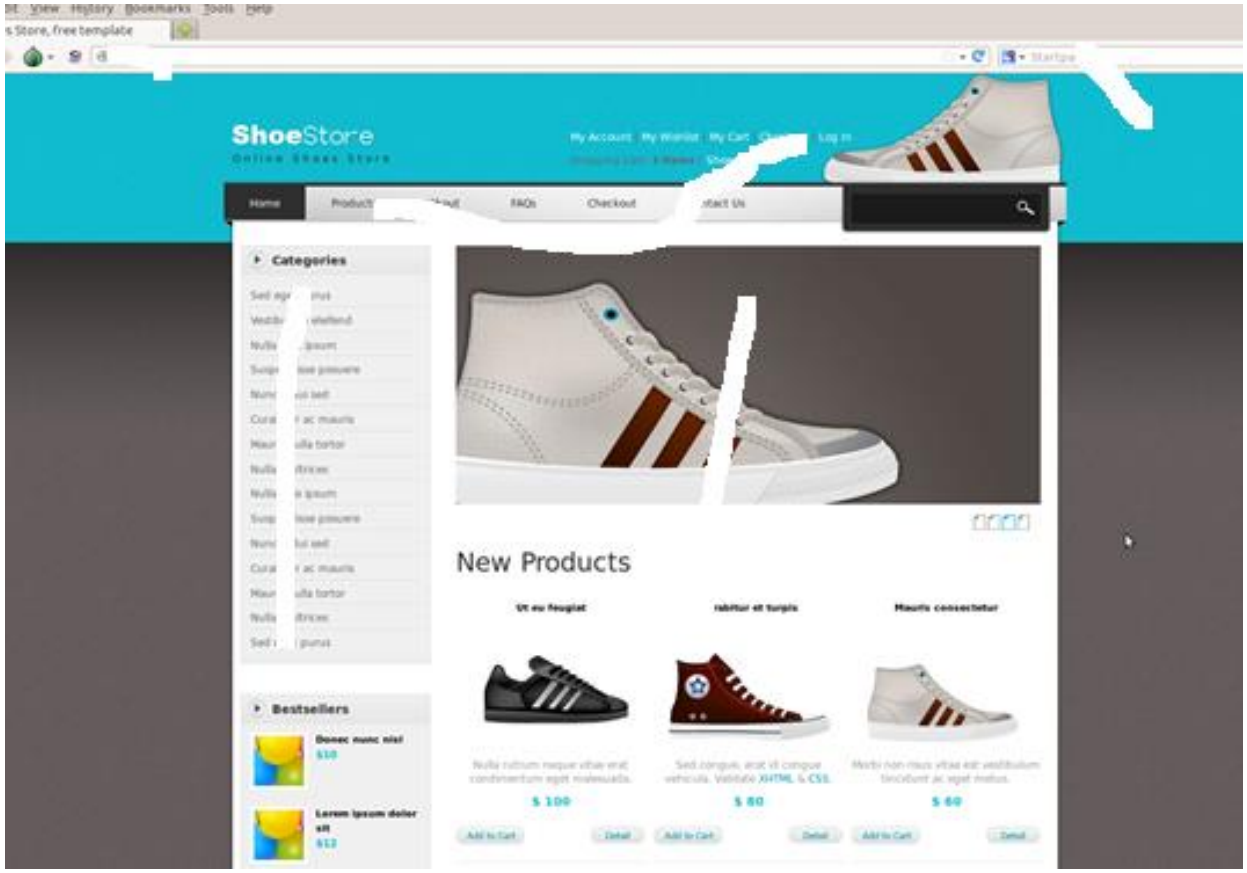
Malicious content Downloaded: Include this encoded Config File



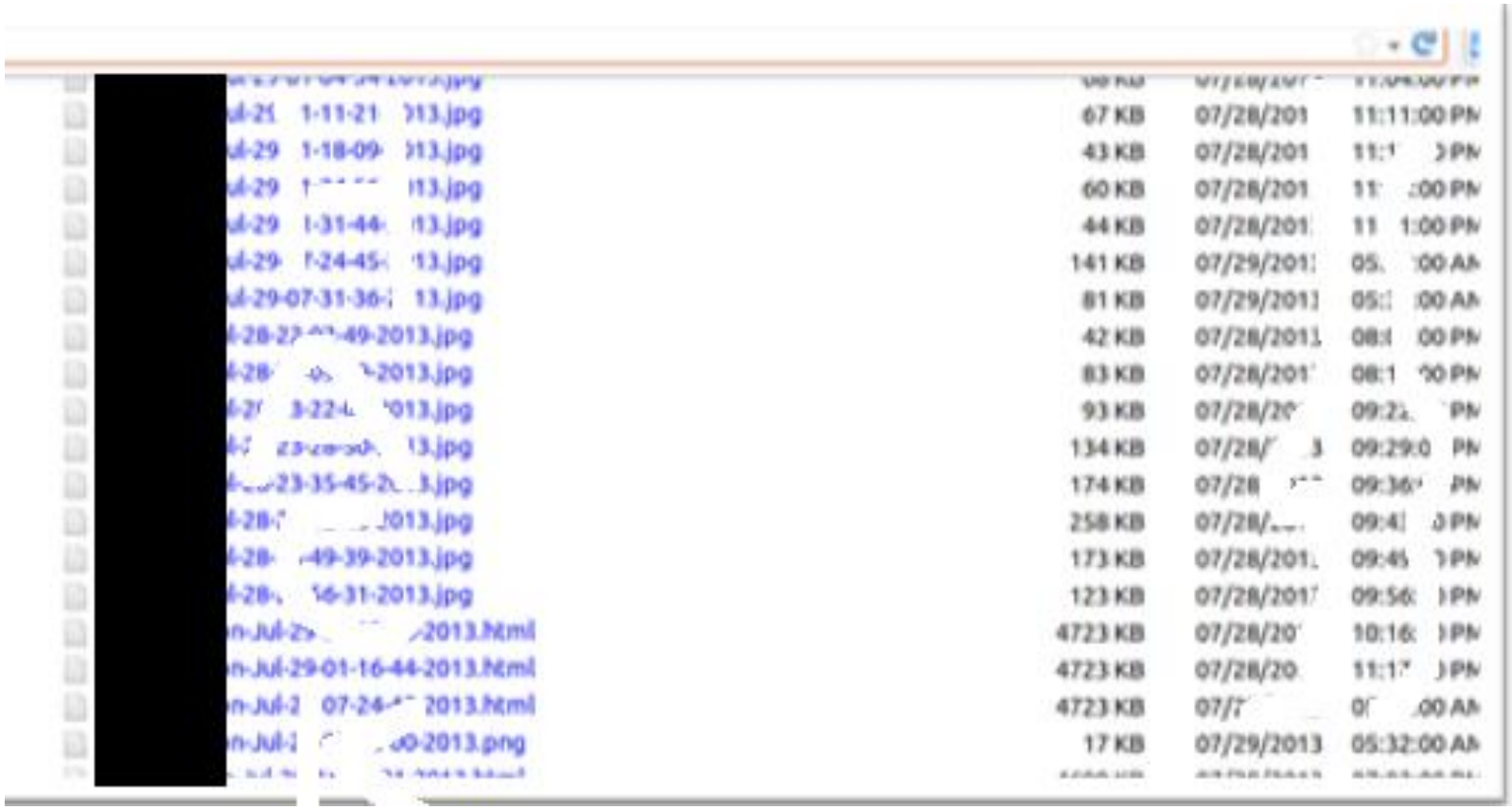
Computer now a member of Robot Network (BotNet)



Malware Uploaded information to Fraudsters Site



Uploaded Infromation



Why it works!

- **Desperation**
- Worthy Cause
- To belong
- Entertainment
- To Compete
- Consequences
- **Trust**
- Curiosity

Be Aware: Did you expect a parcel?

From: **FedEx 2Day A.M.** <support@zapchasti-plus.ru>
Date: Wed, Nov 19, 2014 at 1:55 PM
Subject: Ship Notification
To: mhenlin.....

FedEx

Dear Customer,

Your parcel has arrived at November 17. Courier was unable to deliver the parcel to you.

To receive your parcel, print this label and go to the nearest office.

Get Shipment Label [click here]

FedEx 1995-2014

Identifying Scams

- Unusual Requests to click
- Unbelievable offer or Unsolicited call, email or assistance
- Service Offering
- Request for assistance
- Payment of Advance Fee

Impact

Business

- Reputation
- Competition
- Brand Damage
- Data theft/leakage
- Financial Losses

Personal

- Financial Losses
- Imprisonment

Governance Measures

- Provide Awareness Training and Guidelines
- Implement a Incident Management Framework
  - Policy
  - Procedures:
    - Prepare, Identify, Contain, Eradicate, Recover, Review

Non Technical Countermeasures

- Just hang up
- Do not open emails from unknown sources
- Verify with sender from known sources
- Prevent Emails from loading images
- Pay attention to certificate errors
- Prevent application from leaking information
- Due Diligence
- Do not click on links in emails asking for personal information esp. Banks or utility companies

Technical Countermeasures

- Use license software
- Update with vendor patches
- Use anti-malware applications
- Use virtual systems for research
- Data Loss Prevention
- Multi-factor or “Out” of Band authentication
- System Assessment

Legal Deterrent

- Legal procedures for procedures and conviction “Lotto Scam” Act, 2013.
- Up to 20 years imprisonment on conviction.
- Proposed amendment to the Evidence Act to allow for evidence by video link;

Legal Countermeasures

- Evidence Amendment Bill, also proposes to expand definitions:

“document” means, in addition to a document in writing, anything in which information of any description is recorded;”

Legal Countermeasures

- Evidence Amendment Bill, 2014 makes proposal that presumes that the Computer is working. Burden therefore on accused to prove otherwise:
  - Easier to secure conviction.
    - Increased likelihood of conviction – big deterrence.

Thank you!

References

- http://isaca.org
- http://en.wikipedia.org/wiki/Social_engineering_%28security%29
- http://www.social-engineer.org/
- http://kingston.usembassy.gov/service/scams.html
- http://searchsecurity.techtarget.com/definition/phishing