CE 817 - Advanced Network Security
Phishing I

Lecture 15

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.

What is Phishing?

- "Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials”

  Anti-phishing Working Group

What is Phishing?

- Social engineering aspect:
  - Sending “spoofed” e-mails
  - Building confidence between a phisher and a victim

- Technical aspect:
  - Spyware
  - Pharming - DNS poisoning

Key Characteristics

- Upsetting or exciting statements – must react immediately
- Ask for information such as username, passwords, credit card numbers, social security numbers, etc.
- Emails are typically NOT personalized

- “Masked” links

How Phishing Works

- “Legitimate” emails seem to originate from trusted sources – banks or online retailers
- Social engineering tactics convince the reader that their information is needed
  - Fear is the #1 tactic
  - Solicitation of help
- Links and email look very real
  - Account Update
  - http://www.ebay.com/myaccount/update.asp
    - actually links to http://187.34.123.231

How Phishing Works

- Techniques
  - Mispelled URLs (http://www.welllsfargo.com/account)
  - Spoofing URLs (http://www.google.com@members.tripod.com)
  - Javascript
  - International Domain Names

How Phishing Works

- The Stolen Results
  - Voluntary! Remember you gave it to them.
  - Login
    - Username
    - Password
  - Update Information
    - Social Security Number
    - Address
    - Bank Account Number
    - Credit Card Number

Phishing Example

Subj:	**Your Bank of Oklahoma Account could be Suspended**
Date:	10/31/2005 9:17:23 PM W. Europe Standard Time
From:	department@bankofoklahoma.com
To:	rsutton603@aol.com

Sent from the Internet (Details)

BANK OF OKLAHOMA
You're Better Off At BOk!

Security Alert

Please note that Your B
there is a problem with y
your information,please use the
our Account:

http://secure.bankofoklah oma.com/cgi-bin/dll87443/update/default.asp

Bank of Oklahoma Security Department
Thank you.

Please Note: Bank of Oklahoma always contacts its costumers about acount expiration.That is how we show our *quality* and *respect* to our clients.However your information are 100% safe in our 128-ssl dabatase.

Actually links to
http://212.45.13.185/bank/index.php

Phishing Example

SouthTrust

Dear SouthTrust customer,

We recently reviewed your account, and we suspect an unauthorized ATM and/or PIN- based point of sale transaction on your account. Protecting your account is our primary concern.Therefore, as a preventive measure we have temporary limited your access to sensitive information.
SouthTrust Bank features.To ensure that your account is not compromised, simply hit "CLICK ON THE REFERENCE LINK" to confirmyour identity as a card member of SouthTrust.

Login to your SouthTrust Online Banking with your SouthTrust username and password.

Confirm your identity as a card memeber of SouthTrust.

View your transaction history and report suspicious activity or any unauthorized change.

https://southtrustonlinebanking.com/retail/

If you are not enrolled for SouthTrust Online Banking get started today! Complete the steps below and takeadvantage of our online services today!

Select your account: Personal Accounts, Business Acounts, Credit Card Premiere Line or Credit Line Only.
It`s that easy. If you still need assistance, just click the "Help" button within Internet Banking, or contact us. We`re here to help you 24 hours a day, 7 days a week.

*Please do not reply to this message. Mail sent to this address cannot be answered.

*For assistance, log to your SouthTrust Bank Account and chose th

Thomas D. B. Graff, Member FDIC

Another false link!

VeriSign Secure Site Click to verify

Wachovia Bank, N.A. d/b/a SouthTrust Bank, Member FDIC

Phishing Example

Subject: **Sharif University of Technology (WEBMAIL ACCOUNT SUPPORT)**
From: Support Team <supportteam@sharif.ir>
Reply-To: sharifmail@Alum.com
Date: 9/16/08 1:04 AM
To: undisclosed-recipients:;

Dear Subscriber,
Due to the incessant rate of Scam we are currently upgrading our webmail with a hard spam protector as such all web mail users must respond to
this Email immediately by entering your password here (**********)

USER NAME:
PASSWORD:

Failure to comply with the above instruction will immediately render your email ACCOUNT deactivated from our database. You can also confirm your email address by logging into your web mail account.Thank you for using our web mail!

THE SUPPORT TEAM
(http://www.sharif.ir)
WEBMAIL ACCOUNT SUPPORT.
Sharif University of Technology

2008, Sharif University of Technology, Tehran, Iran

This message was sent using IMP, the Internet Messaging Program.

--
Este mensaje ha sido analizado por **MailScanner**
en busca de virus y otros contenidos peligrosos,
y se considera que está limpio.

Consequences

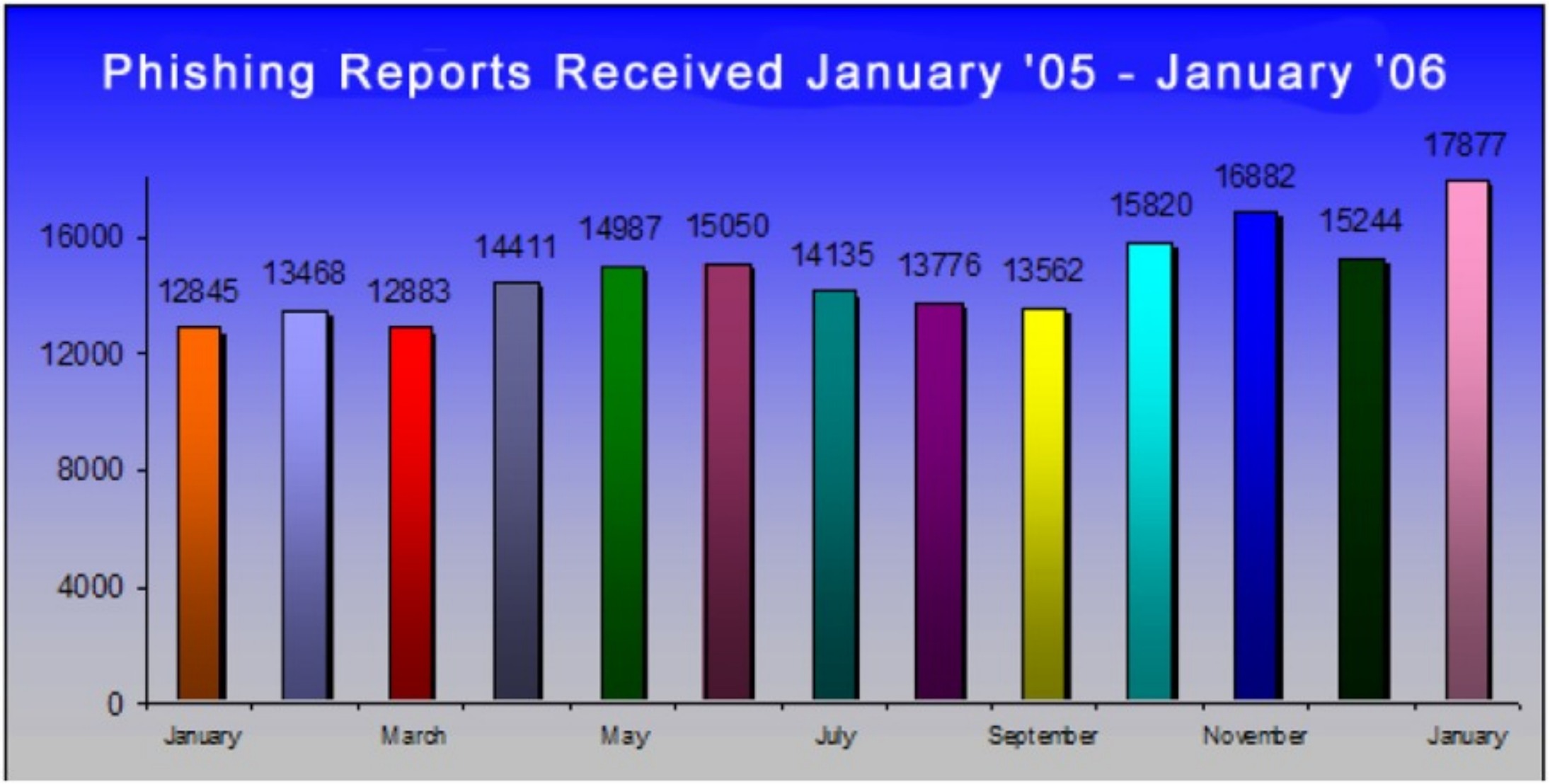
- Customers:
  - Financial consequences – stolen financial information
  - Trust and effective communication can suffer

- Service providers (banks, retailers...)
  - Diminishes value of a brand
  - Customer loss
  - Could affect stakeholders

Phishing is a Plague on the Internet

- Estimated 3.5 million people have fallen for phishing
- Estimated to cost $1-2.8 billion a year (and growing)
- 9255 unique phishing sites reported in June 2006
- 40621 unique phishing sites reported in August 2009
- 26402 unique phishing sites reported in March 2011
- 44407 unique phishing sites reported in May 2014
- The number of phished brands was 339 in January 2011
- The number of phished brands was 531 in 2014Q2
- Easier (and safer) to phish than rob a bank

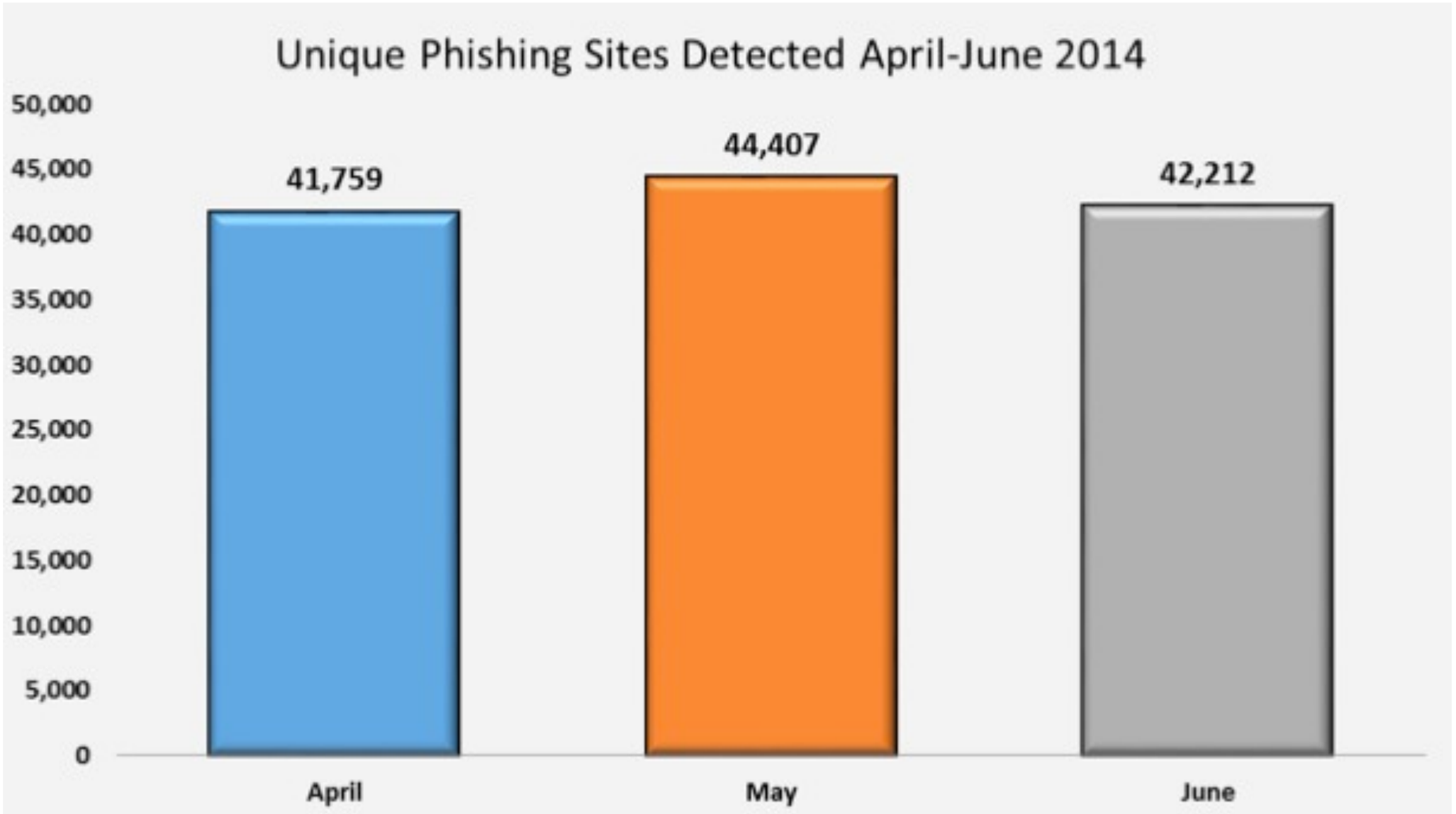
Phishing Damage

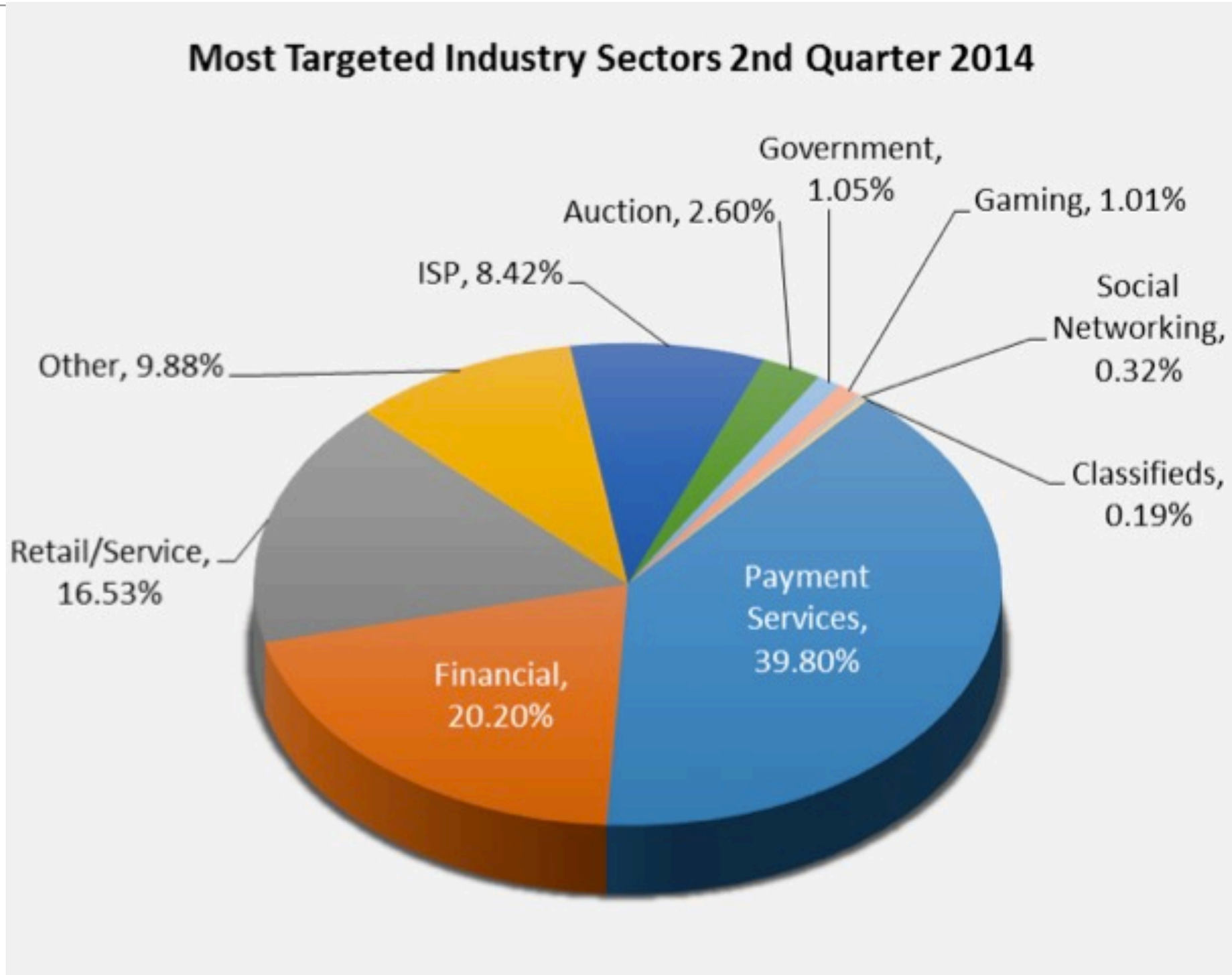


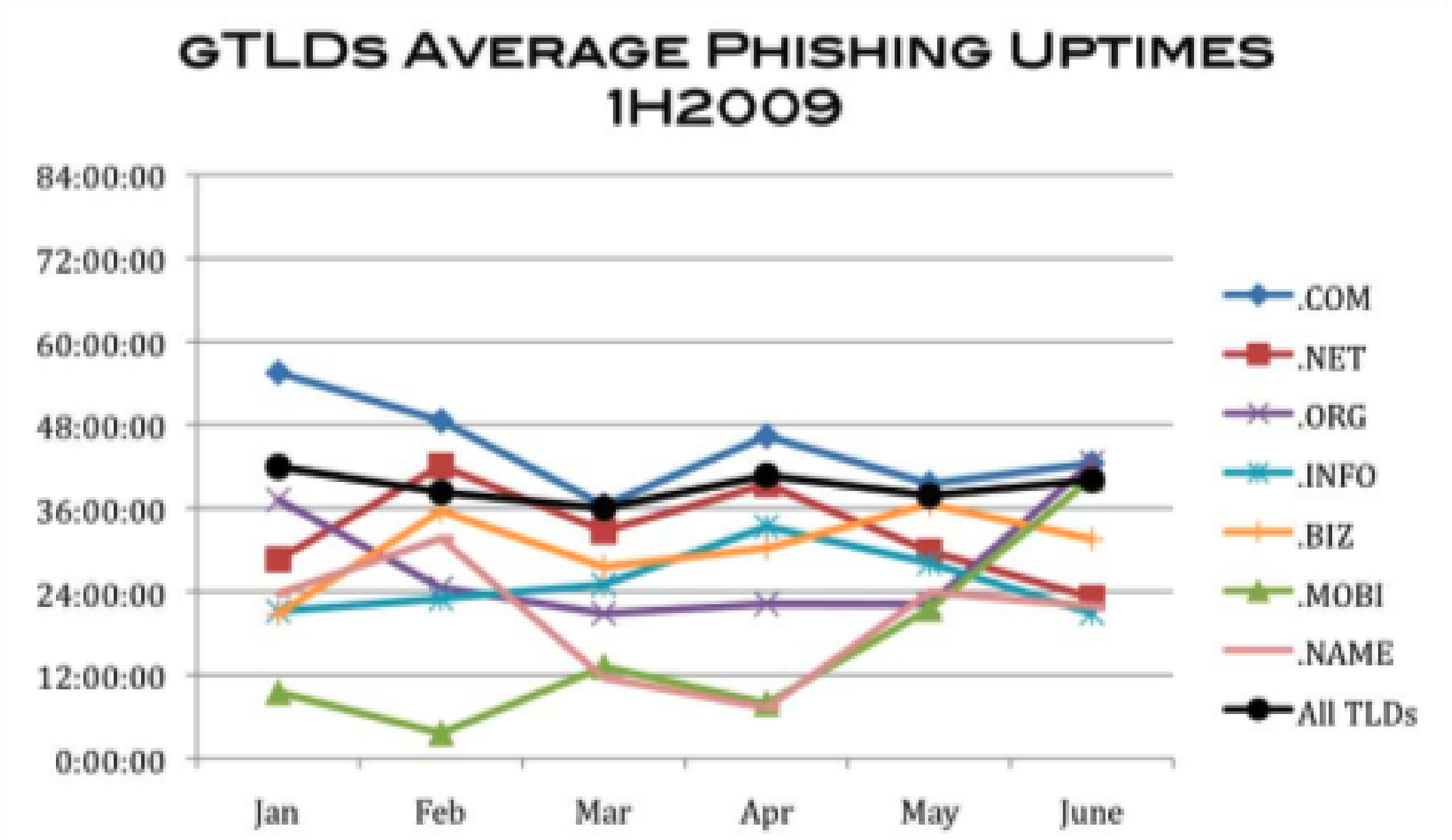
Courtesy of: The Anti-Phishing Working Group

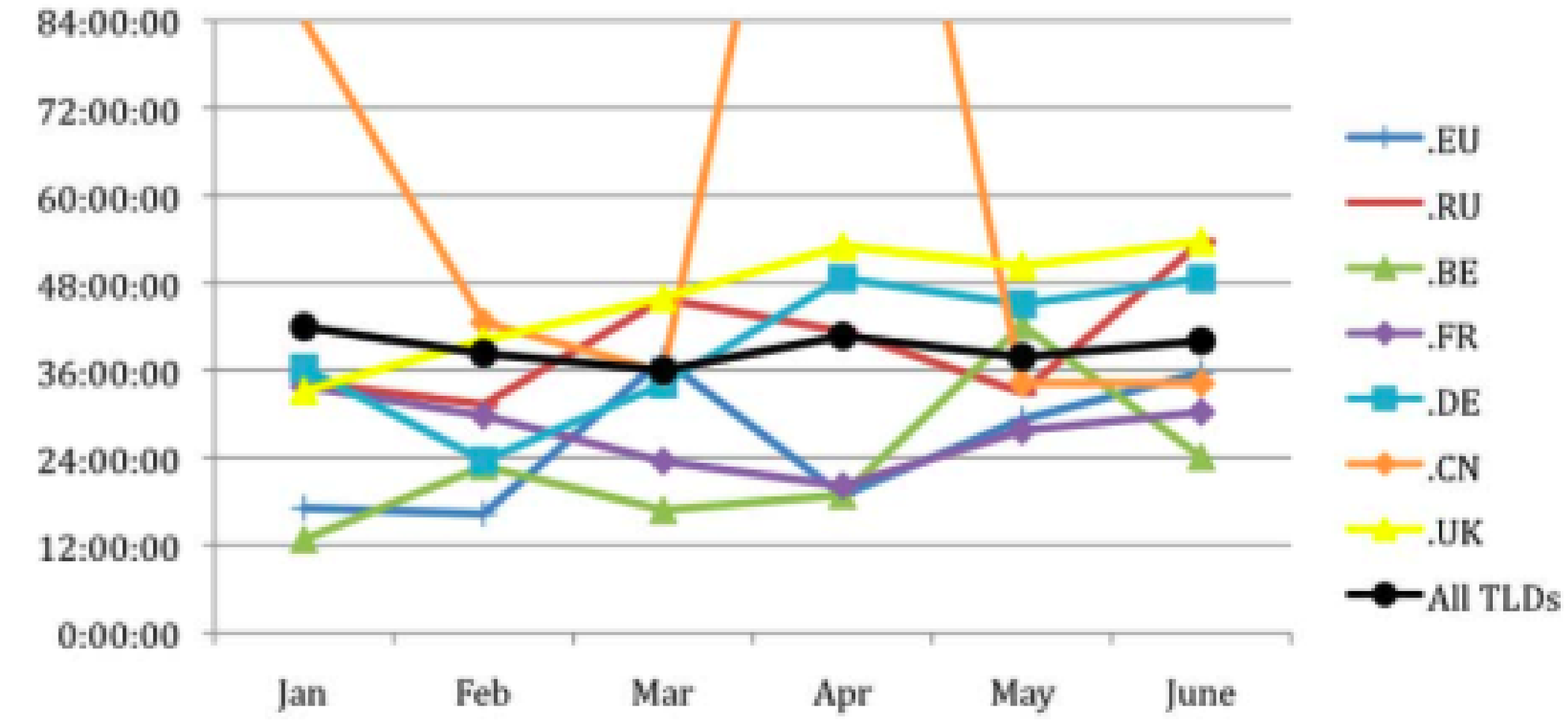
Phishing Targets

Courtesy of: The Anti-Phishing Working Group


Unique Phishing Sites Detected April-June 2014
50,000
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
41,759
44,407
42,212
April
May
June


Most Targeted Industry Sectors 2nd Quarter 2014
Government, 1.05%
Auction, 2.60%
Gaming, 1.01%
ISP, 8.42%
Social Networking, 0.32%
Other, 9.88%
Classifieds, 0.19%
Retail/Service, 16.53%
Payment Services, 39.80%
Financial, 20.20%

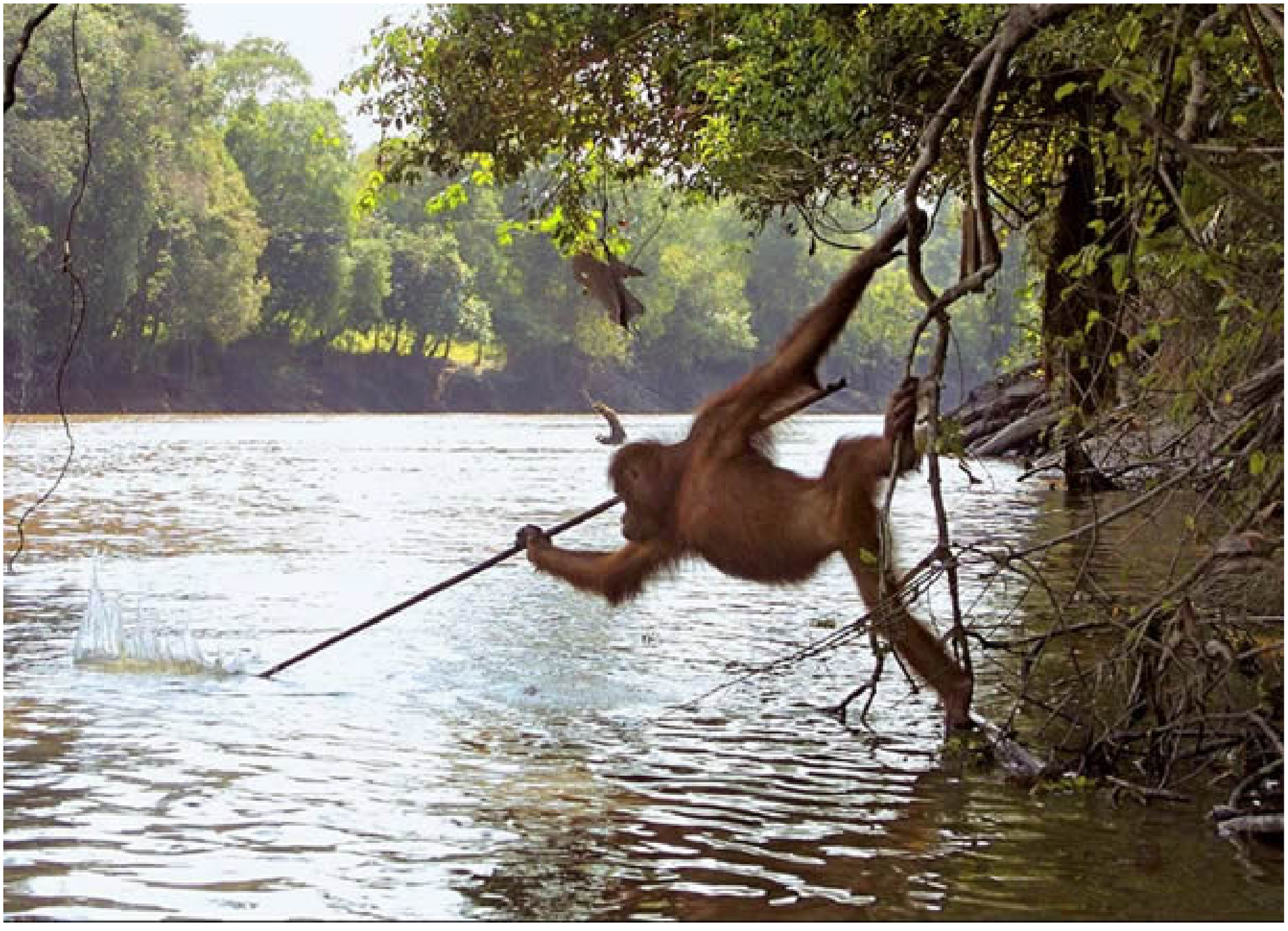

gTLDs Average Phishing Uptimes
1H2009
84:00:00
72:00:00
60:00:00
48:00:00
36:00:00
24:00:00
12:00:00
0:00:00
Jan
Feb
Mar
Apr
May
June
.COM
.NET
.ORG
.INFO
.BIZ
.MOBI
.NAME
All TLDs


ccTLDs Average Phishing Uptimes
1H2009
84:00:00
72:00:00
60:00:00
48:00:00
36:00:00
24:00:00
12:00:00
0:00:00
Jan
Feb
Mar
Apr
May
June
.EU
.RU
.BE
.FR
.DE
.CN
.UK
All TLDs

Phishing Targets

- Users lack computer knowledge
  - Elderly
- Users lack security knowledge
  - Elderly
  - Teens
  - New Computer Users
  - Infrequent Computer Users

Spear Phishing



[Daily Mail]

Spear Phishing

- Targeted at a specific company, government agency, organization, or group
- Phisher gets an e-mail address of an administrator/colleague
- Spoofed e-mail asks employees to log on to a corporate network
- A key-logger application records passwords
- Phisher can access corporate information

Whaling Attacks

- Phishing attack directed at high profile executives
- From “The Register” 16th April 2008:
  - Highly targeted email scam that singled out as many as 20,000 senior corporate executives
  - Messages masquerade as an official subpoena requiring the recipient to appear before a federal grand jury
  - The emails correctly address their full name and include their phone number and company name
  - Recipients who click on a link that offers a more detailed copy of the subpoena are taken to a website that informs them they must install a browser add-on in order to read the document
  - a backdoor is installed and key logging software that steals log-in credentials used on websites for banks and other sensitive organizations.
  - About 2,000 executives took the bait on the first day

Phishing Techniques

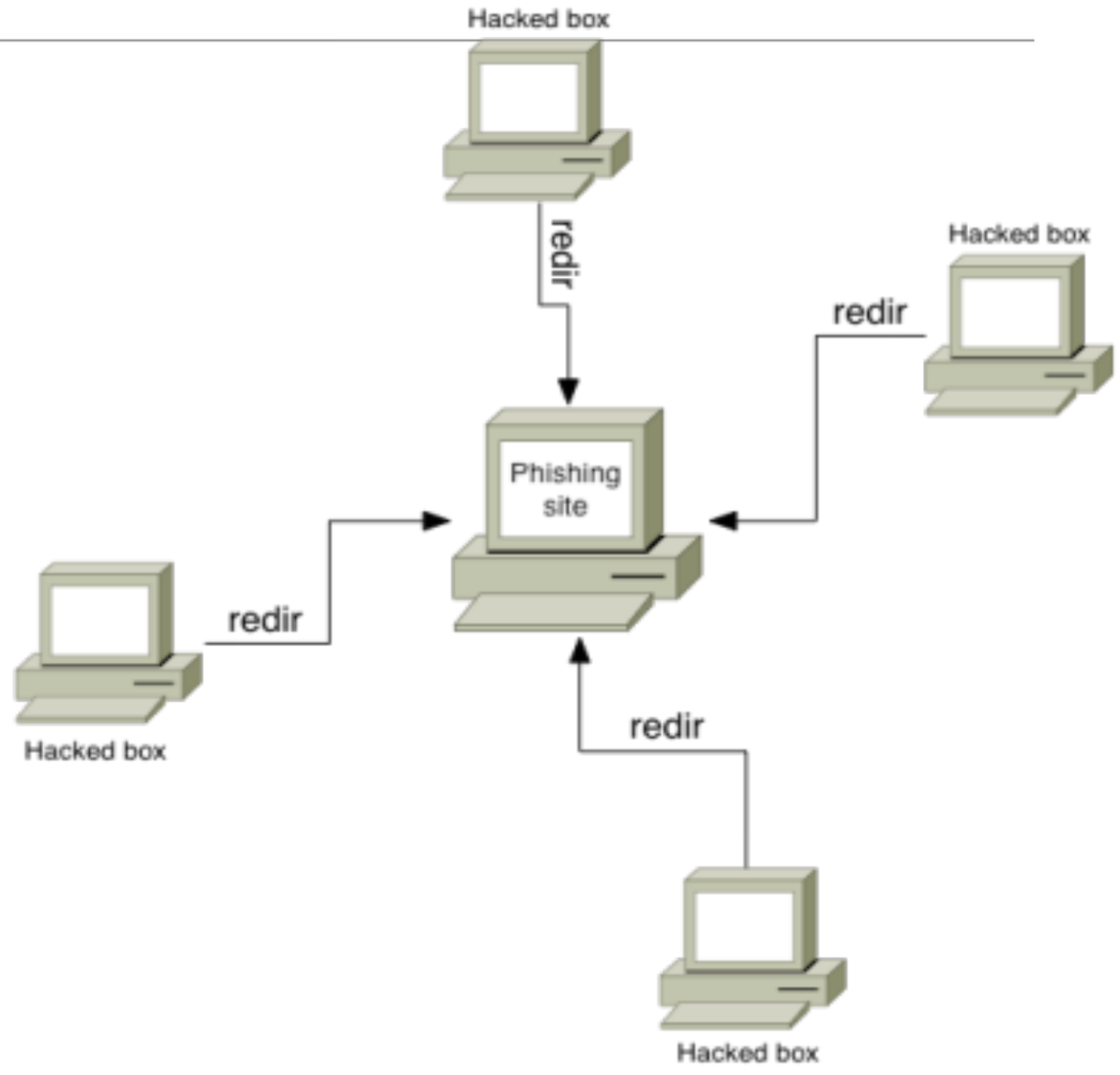
- Phishing through compromised web servers
  - Find vulnerable servers
  - Gain access to the server
  - Pre-built phishing web sites are up
  - Mass emailing tools are downloaded and used to advertise the fake web site via spam email
  - Web traffic begins to arrive at the phishing web site and potential victims access the malicious content

Phishing Techniques

- Phishing through port redirection
  - Find vulnerable servers
  - Install software that will forward port 80 traffic to a remote server
  - Make sure that it is running even after a reboot
  - Try not to get detected
  - Web traffic begins to arrive at the phishing web site and potential victims access the malicious content

Phishing Techniques

- Combined technique
  - If a remote host is lost other will continue to phish
  - If the central phishing site is lost, compromise another and update redirections
  - Faster configuration setup, concurrent adjustments can be made



Phishing Techniques

- Additional approaches
  - Register similar sounding DNS domains and setting up fake web sites, e.g. www.paypa1.com www.welsfargo.com
  - Configure the fake phishing web site to record any input data that the user submits silently log them and then forward the user to the real web site

Phishing Techniques

- Transfer of funds
  - International transfers are monitored, find an intermediate person to send the money
  - “Hello! We finding Europe persons, who can Send/Receive bank wires from our sellings, from our European clients. To not pay TAXES from international transfers in Russia. We offer 10% percent from amount u receive and pay all fees, for sending funds back. Amount from 1000 euro per day. All this activity are legal in Europe, Thank you, FINANCIE LTD.”

Pharming

- Typing URL e.g. www.newegg.com Translates to IP address 216.52.208.185
- DNS – a dictionary with pairs URL - IP
- What happens if somebody hacks the DNS?
  - Instead of 216.52.208.185 , www.newegg.com might take us to 192.168.10.103
  - Usually, a false web page is there

Pharming

- How hard is it to perform DNS poisoning?
  - Local DNS cache
  - Local DNS
  - Wireless routers

Statistical Highlights for 2nd Quarter 2014

	April	May	June
Number of unique phishing websites detected	41,759	44,407	42,212
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	57,733	60,809	53,259
Number of brands targeted by phishing campaigns	332	357	345
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	56.76%	54.31%	64.47%
Percentage of sites not using port 80	0.85%	0.42%	0.56%

Countries Hosting Phishing Sites – 2nd Quarter 2014

April		May		June	
United States	35.64%	United States	48.22%	United States	35.79%
Ukraine	17.29%	Germany	7.61%	China	4.32%
Hong Kong	10.36%	Russian Federation	4.86%	Germany	4.19%
United Kingdom	7.25%	United Kingdom	3.49%	Turkey	3.92%
Canada	3.03%	France	2.79%	Russian Federation	3.30%
Netherlands	0.54%	Hong Kong	2.53%	United Kingdom	2.80%
Russian Federation	0.43%	Turkey	2.36%	France	2.03%
France	0.39%	Canada	2.25%	Netherlands	1.85%
Germany	0.39%	Netherlands	2.07%	Poland	1.71%
Japan	0.24%	Poland	1.96%	Canada	1.67%

Phishing Prevention

- Public Education:
- Do not believe anyone addressing you as a 'Dear Customer' 'Dear business partner', etc.
- Do not respond to an e-mail requesting username, password, bank account number, etc.
- Do not click on the link provided in an e-mail message

Acknowledgments/References

- [Guthrie] Phishing and Pharming, Jason Guthrie, Accounting Fraud Class, April 2006.
- [Pejović] "Phishing: Read Behind the Lines, Veljko Pejovic, CompSci595N/ PolSci595N/Engl593: The Technology and Society Seminar Series, University of California at Santa Barbara, Fall 2006.
- [APWG] GlobalPhishingSurvey 1H2009. http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf (April 21, 2012)