Threats Without Frontiers

Dave Jevans
Chairman, APWG

Reviewing Predictions

- Globalization of infections and attacks

Global Malware Infection Rates

Ranking	Country	Infection Rate
1	South Korea	57.30%
2	China	51.94%
3	Taiwan	42.88%
4	Bolivia	42.28%
5	Honduras	40.80%
6	Turkey	39.29%
7	Ecuador	37.59%
8	Russia	36.78%
9	Slovakia	36.09%
10	Poland	35.74%

Ranking	Country	Infection ratio
23	Holland	24.74%
24	Hungry	24.54%
25	Finland	24.02%
26	Ireland	23.64%
27	Germany	22.61%
28	Uruguay	21.94%
29	United Kingdom	21.01%
30	Norway	20.50%
31	Sweden	19.07%
32	Switzerland	18.40%

Reviewing Predictions

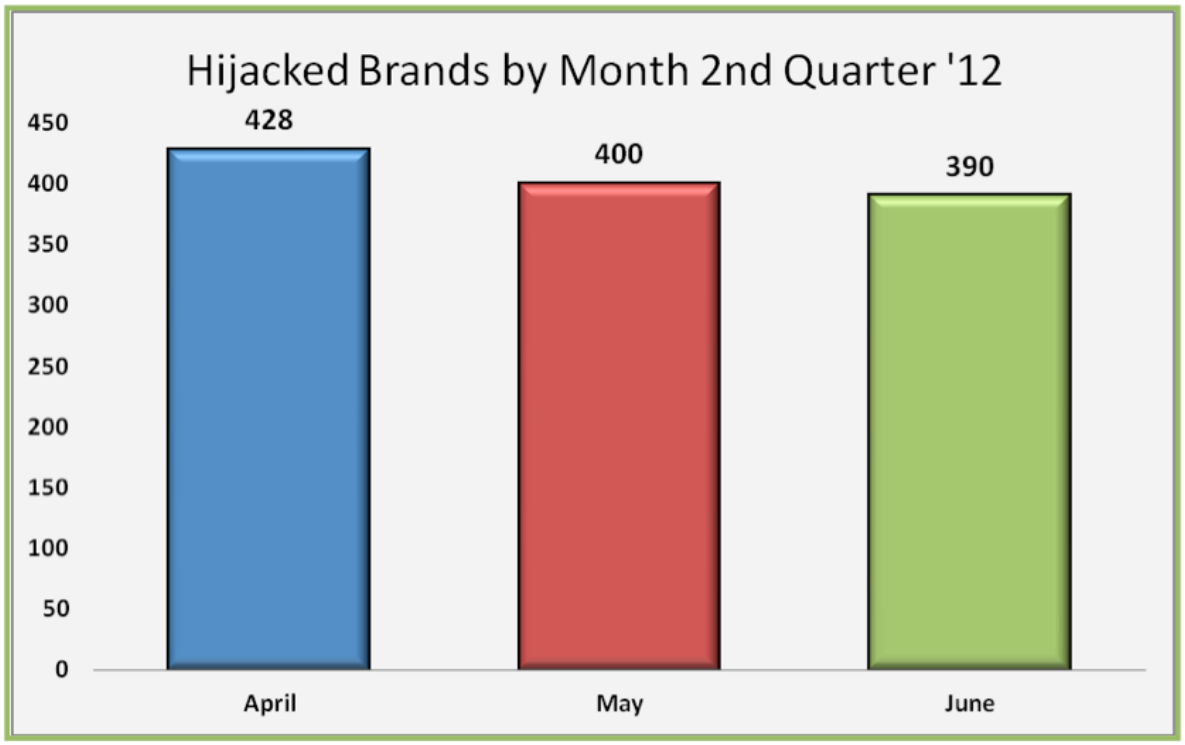
- Globalization of infections and attacks
- Creates an attack fabric that lends itself to global joe jobs

Reviewing Predictions

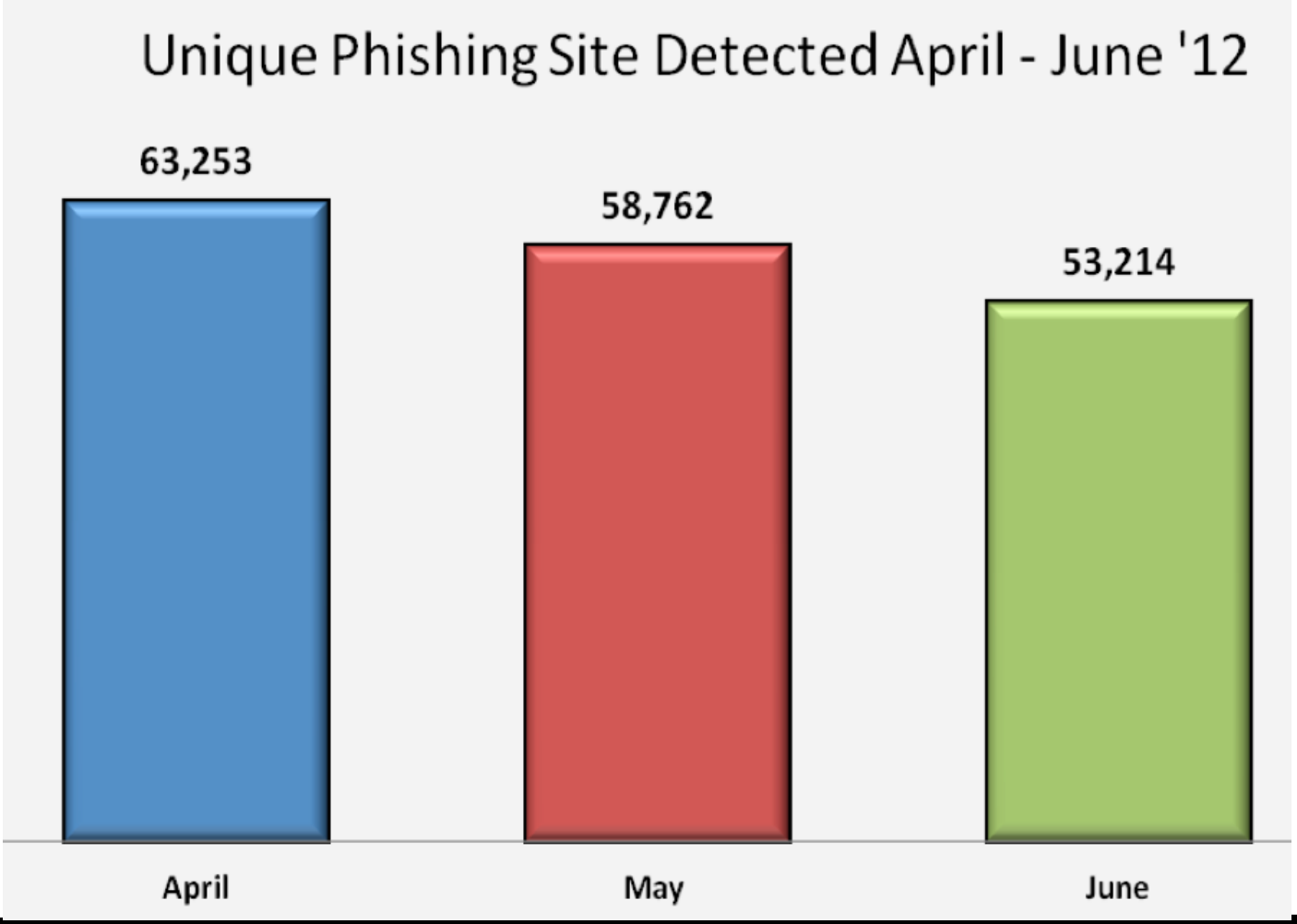
- More phishing

More Phishing

Brands Targeted by Cybercrime Gangs Reach All-Time High in April



April 2012 - Highest Levels Ever



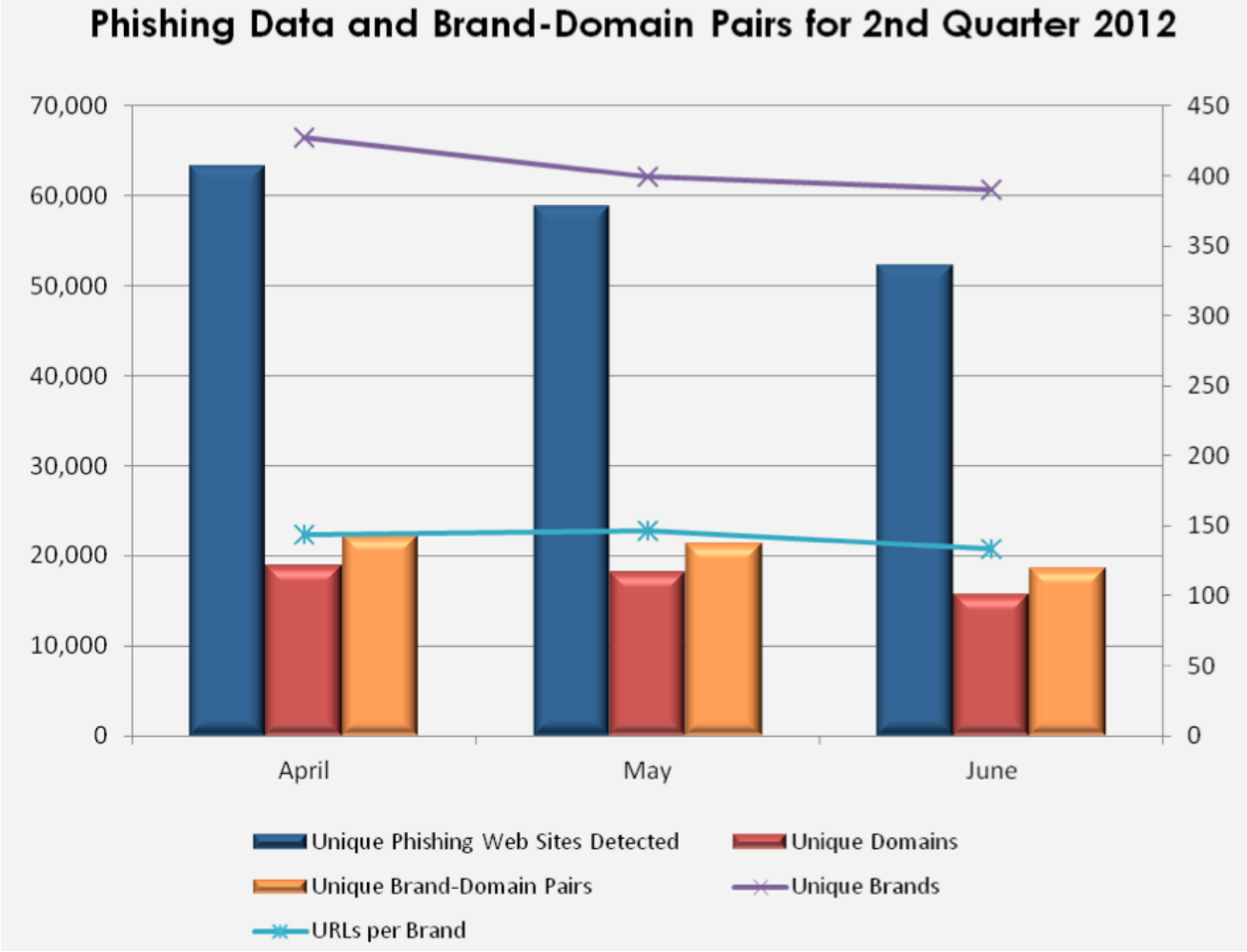
Hack One Shared Server, Phish From All Its Sites

- "Even excluding the thousands of phishing sites created by this tactic, phishing in the second quarter of 2012 was up significantly over the first quarter."
  - Rod Rasmussen, President and CTO of Internet Identity

More 2012 Stats

	April	May	June
Number of Unique Phishing Web Sites Detected	63,253	58,762	52,214
Unique Domains	18,878	18,191	15,637
Unique Brand-Domain Pairs	22,247	21,425	18,532
Unique Brands	428	400	390
URLs Per Brand	143.85	146.90	133.88

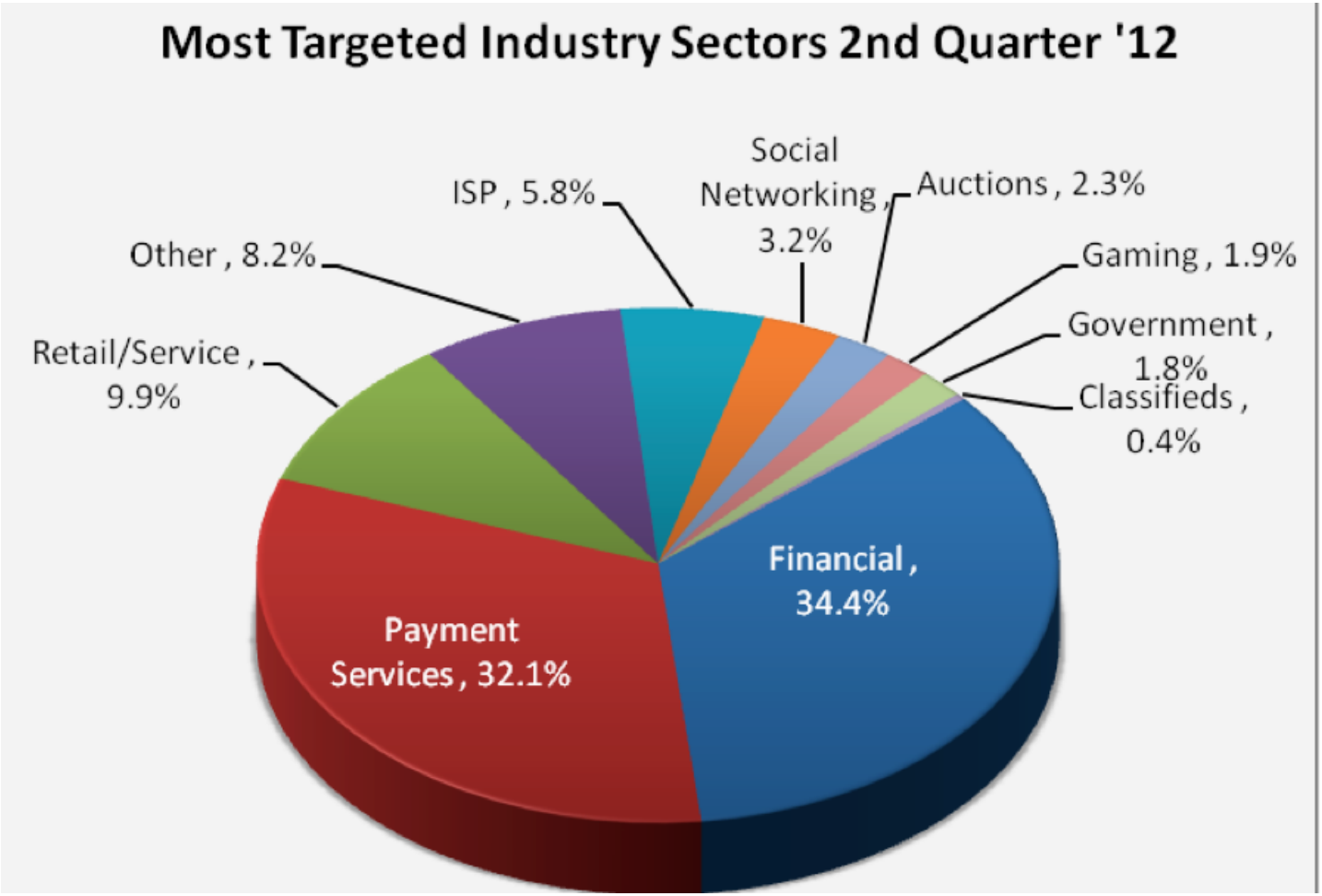
More 2012 Stats



Phishing Increases

- "Targeted attacks remain the favorite attack vector used to launch phishing attacks, as the number of unique brands during the entire quarter rose to 601 in Q2 2012 from 587 in Q1 2012"
  - Ihab Shraim, chief information security officer, MarkMonitor

Industry Focus of Attacks



Countries Hosting Phishing Sites

April		May		June	
USA	58.45%	USA	87.91%	USA	71.55%
Egypt	6.28%	Bahamas	5.55%	Germany	3.36%
Brazil	4.54%	Germany	0.53%	UK	3.08%
Canada	3.93%	Canada	0.47%	Canada	2.71%
Germany	3.91%	Rep. Korea	0.46%	France	2.17%
UK	2.45%	Switzerland	0.45%	Brazil	1.61%
Netherlands	1.67%	UK	0.44%	Netherlands	1.52%
France	1.56%	Netherlands	0.42%	Czech Rep.	1.34%
Russia	1.14%	Egypt	0.36%	Japan	1.19%
Turkey	1.12%	Belgium	0.34%	Russia	0.94%

Countries Hosting Keyloggers & Trojan Downloaders

April		May		June	
USA	46.44%	USA	78.13%	USA	55.17%
Russia	11.55%	UK	3.77%	France	11.17%
France	7.81%	France	3.64%	China	7.00%
China	4.15%	China	1.75%	Russia	3.73%
Brazil	3.77%	Russia	1.48%	Rep of Korea	2.85%
Netherlands	3.68%	Germany	1.34%	Netherlands	2.63%
Rep of Korea	3.33%	Hong Kong	1.07%	Germany	2.56%
Germany	2.94%	Netherlands	0.80%	Ukraine	1.83%
UK	2.25%	Iceland	0.67%	UK	1.70%
Poland	1.40%	Canada	0.67%	Brazil	1.33%

Reviewing Predictions

- Spear-phishing for APT

U.S. warns of cyberattacks on gas pipeline companies

The Department of Homeland Security wants the gas sector to monitor malware planted via cyberattacks as part of an investigation.

by Elinor Mills | May 7, 2012 6:27 PM PDT

Follow

7 68 6 +1 0 More + Comments 0

U.S. gas pipeline operators have been targeted in sophisticated phishing attacks since at least December, with the Department of Homeland Security helping firms deal with the incidents since March, the DHS and an industry expert said.

"DHS's Industrial Control Systems Cyber Emergency Response Team has been working since March 2012 with critical infrastructure owners and operators in the oil and natural gas sector to address a series of cyber intrusions targeting natural gas pipeline companies," DHS spokesman Peter Boogaard said in an e-mail sent to CNET today.

"The cyber intrusion involves sophisticated spear-phishing activities targeting personnel within the private companies. DHS is coordinating with the FBI and appropriate federal agencies, and ICS-CERT is working with affected organizations to prepare mitigation plans customized to their current network and security configurations to detect, mitigate and prevent such threats."

The agency has been meeting with companies in private about the matter and late last week issued the first public advisory, which was first reported on by The Christian Science Monitor. It's unclear who is behind the attacks and whether they have led to pilfering of data or other negative consequences. Boogaard did not respond to follow up questions seeking more

Scammers Want Access To The Freshest & Most Juicy Information

From LexisNexis <support@accurint.com>
Subject **Accurint Product Support**
Reply to support@accurint.com
Cc recipient list not shown:;

LexisNexis®
Accurint®

During our regular scheduled maintenance of our systems, your account was flagged for having a long period of inactivity.

For security reasons, inactive accounts are disabled after a long period of time.
To prevent this from occurring, you are required to immediately login to your account with the link provided below

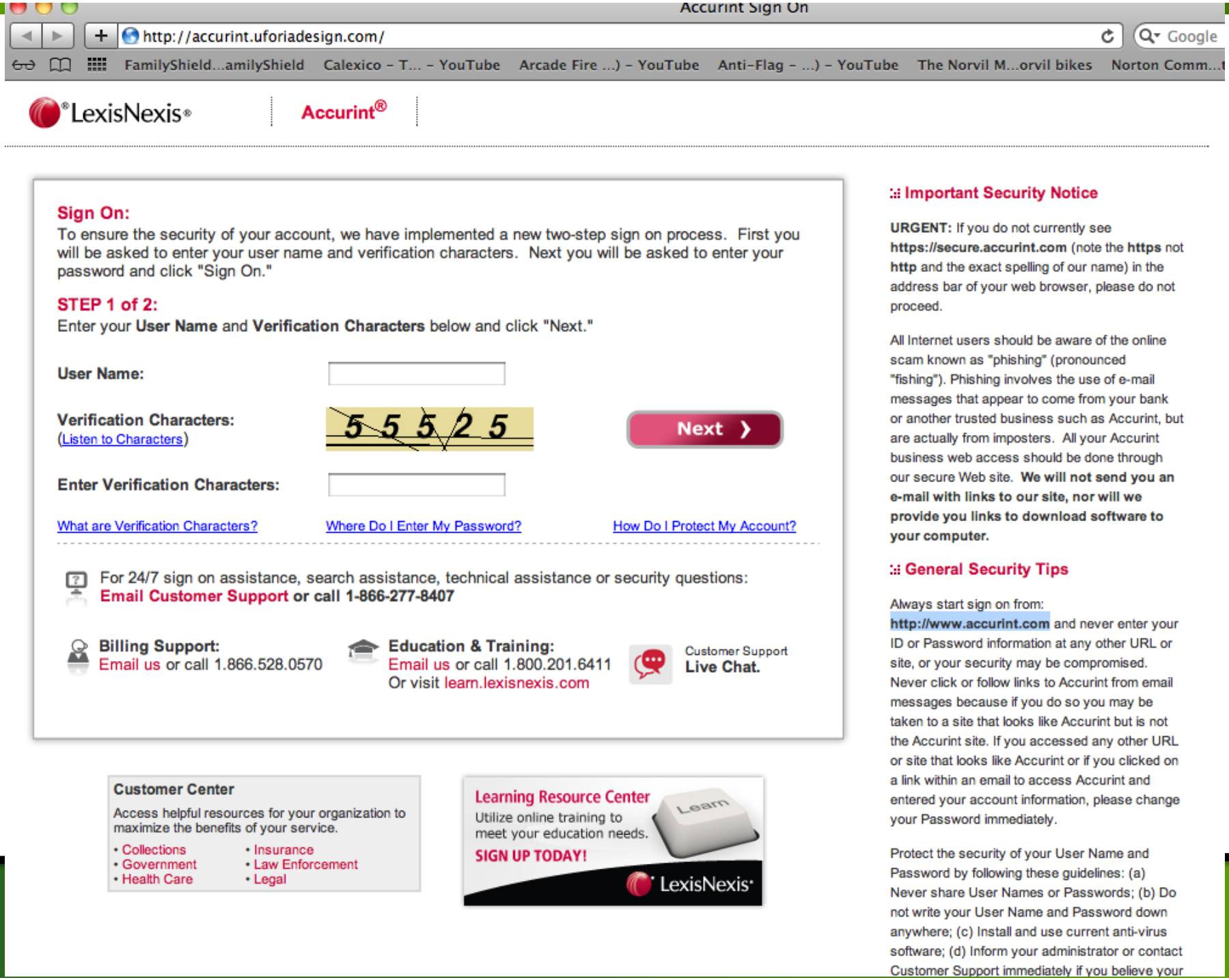
To access your account please click here

Please Note:
You are not required to perform any transaction or activity after login. If your account is indeed active, you are still required to log in with the link provided above to take your account off the flag list. You are required to login to your account once every three months to indicate use of your LexisNexis Accurint online service.

Protecting the security of your account is our primary concern, and we apologize for any inconvenience this may have caused you.

N.B: You will receive one more notification from us before your account is disabled. If you don't receive this notification, it indicates your account has been unflagged and is fully active.

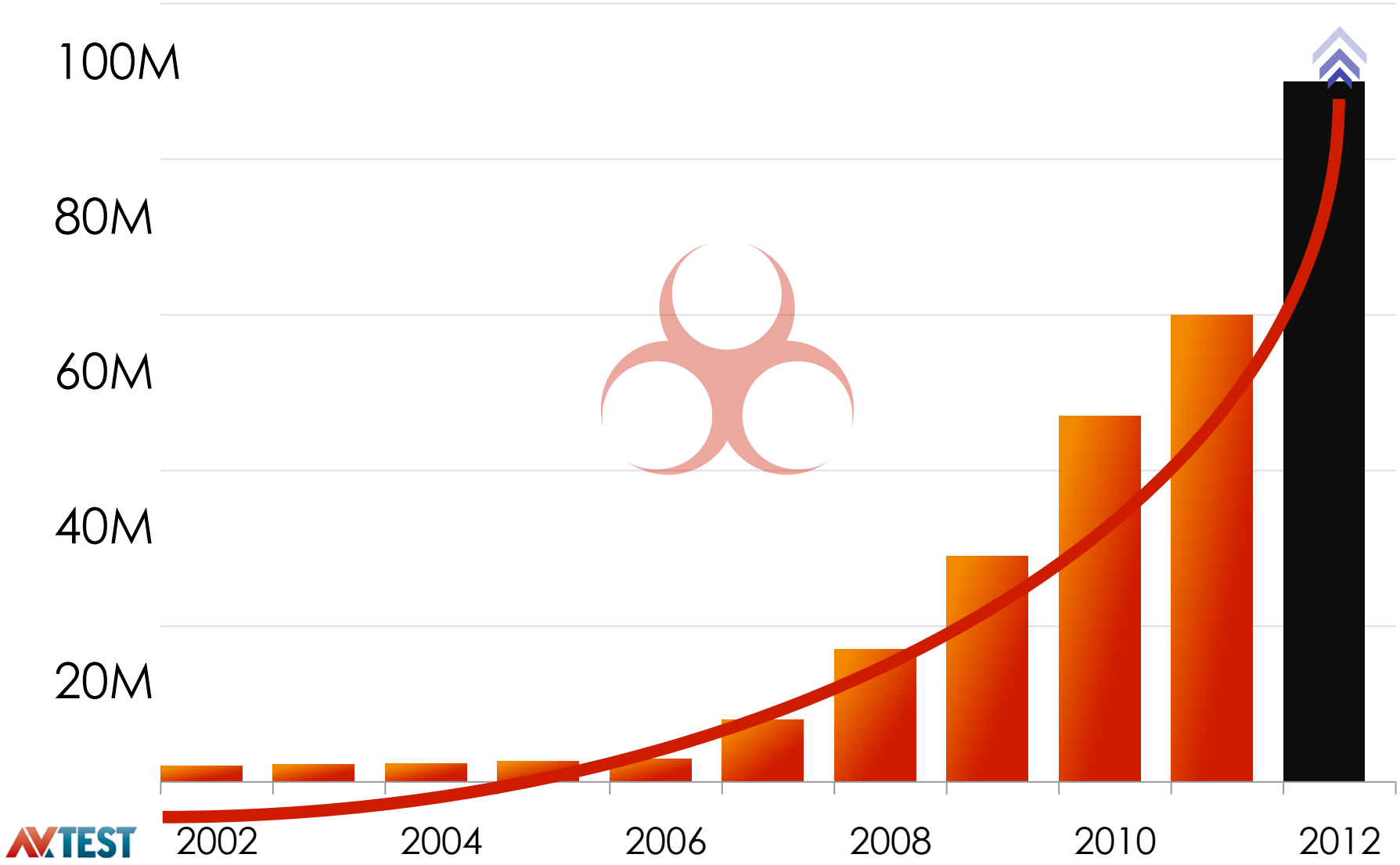
Sincerely.
Account Review Department
LexisNexis Accurint


Accurint Sign On
http://accurint.uforiadesign.com/
Google
FamilyShield...amilyShield
Calexico - T... - YouTube
Arcade Fire ...) - YouTube
Anti-Flag - ...) - YouTube
The Norvil M...orvil bikes
Norton Comm...
LexisNexis®
Accurint®
Sign On:
To ensure the security of your account, we have implemented a new two-step sign on process. First you will be asked to enter your user name and verification characters. Next you will be asked to enter your password and click "Sign On."
STEP 1 of 2:
Enter your User Name and Verification Characters below and click "Next."
User Name:
Verification Characters:
(Listen to Characters)
5 5 5 2 5
Next
Enter Verification Characters:
What are Verification Characters?
Where Do I Enter My Password?
How Do I Protect My Account?
For 24/7 sign on assistance, search assistance, technical assistance or security questions:
Email Customer Support or call 1-866-277-8407
Billing Support:
Email us or call 1.866.528.0570
Education & Training:
Email us or call 1.800.201.6411
Or visit learn.lexisnexis.com
Customer Support
Live Chat.
Customer Center
Access helpful resources for your organization to maximize the benefits of your service.
• Collections
• Government
• Health Care
• Insurance
• Law Enforcement
• Legal
Learning Resource Center
Utilize online training to meet your education needs.
SIGN UP TODAY!
Learn
LexisNexis
:: Important Security Notice
URGENT: If you do not currently see https://secure.accurint.com (note the https not http and the exact spelling of our name) in the address bar of your web browser, please do not proceed.
All Internet users should be aware of the online scam known as "phishing" (pronounced "fishing"). Phishing involves the use of e-mail messages that appear to come from your bank or another trusted business such as Accurint, but are actually from imposters. All your Accurint business web access should be done through our secure Web site. We will not send you an e-mail with links to our site, nor will we provide you links to download software to your computer.
:: General Security Tips
Always start sign on from: http://www.accurint.com and never enter your ID or Password information at any other URL or site, or your security may be compromised. Never click or follow links to Accurint from email messages because if you do so you may be taken to a site that looks like Accurint but is not the Accurint site. If you accessed any other URL or site that looks like Accurint or if you clicked on a link within an email to access Accurint and entered your account information, please change your Password immediately.
Protect the security of your User Name and Password by following these guidelines: (a) Never share User Names or Passwords; (b) Do not write your User Name and Password down anywhere; (c) Install and use current anti-virus software; (d) Inform your administrator or contact Customer Support immediately if you believe your

Reviewing Predictions

- More Malware
  - Primarily trojans / crimeware

Booming Malware Economy



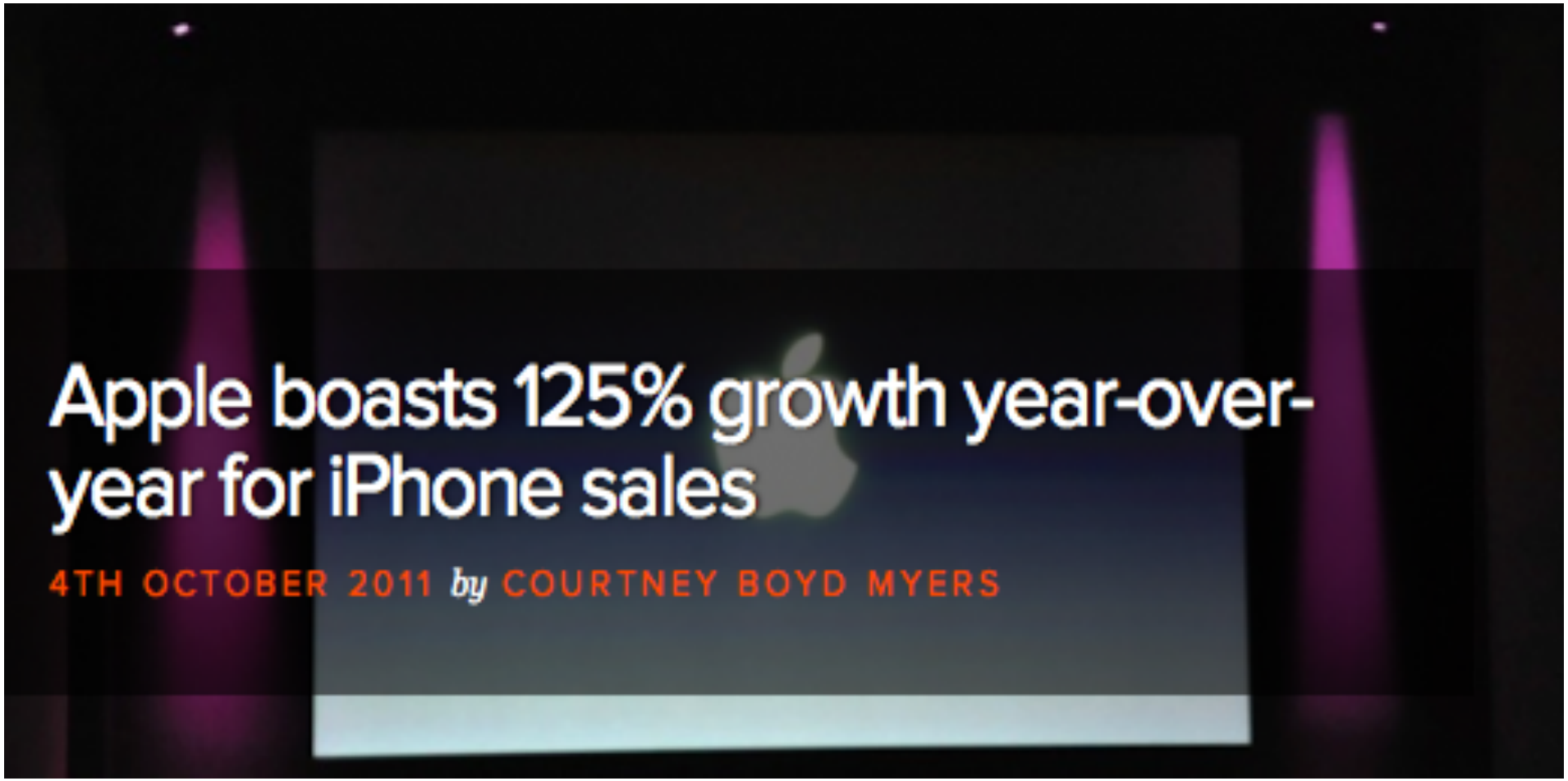
Trojans Dominate Malware

Type of Malware Identified	% of malware samples
Trojans	78.92%
Worms	10.78%
Virus	7.44%
Rogueware	2.96%
Other	.17%

Reviewing Predictions

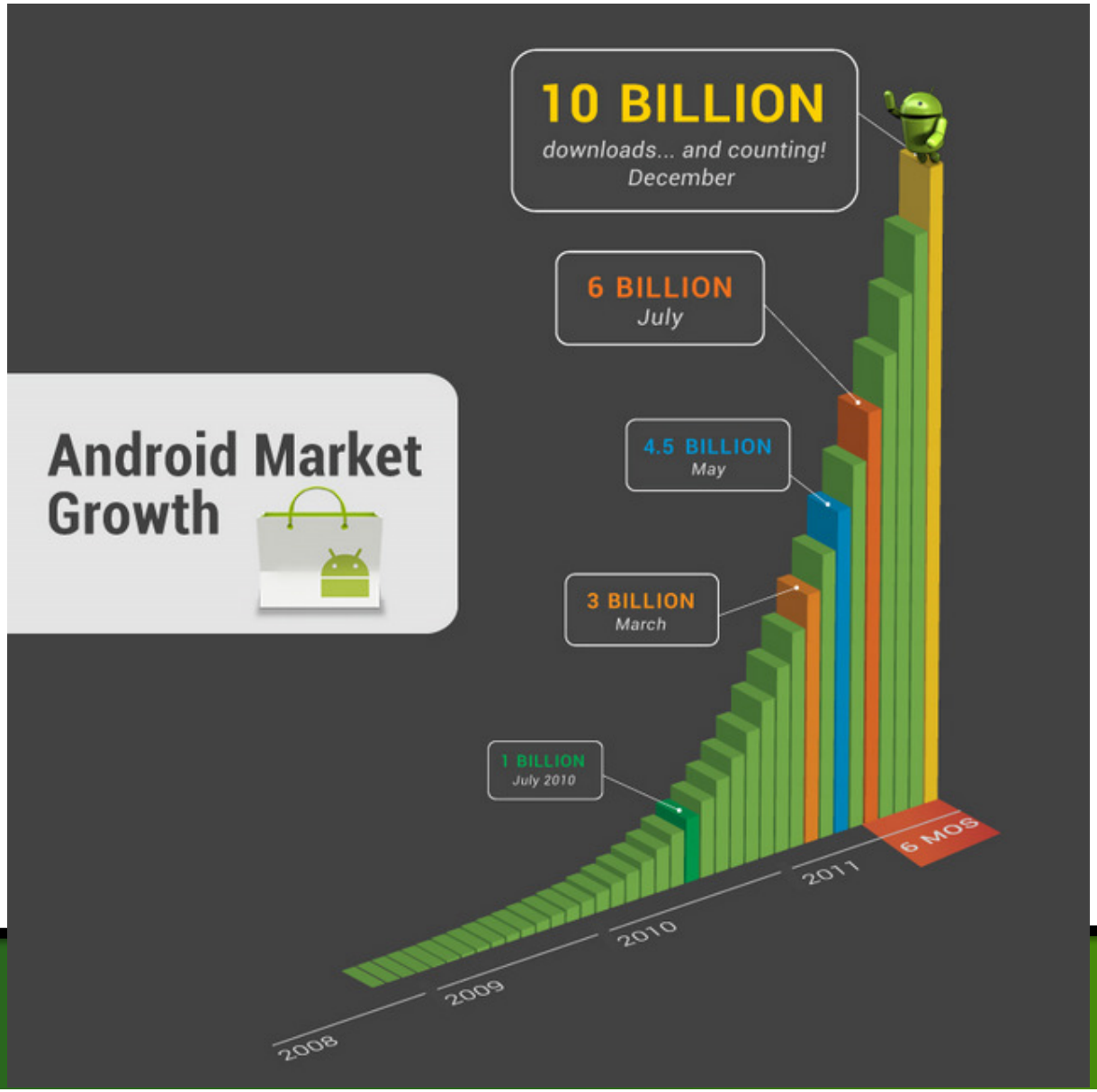
- Mobile malware and malicious apps

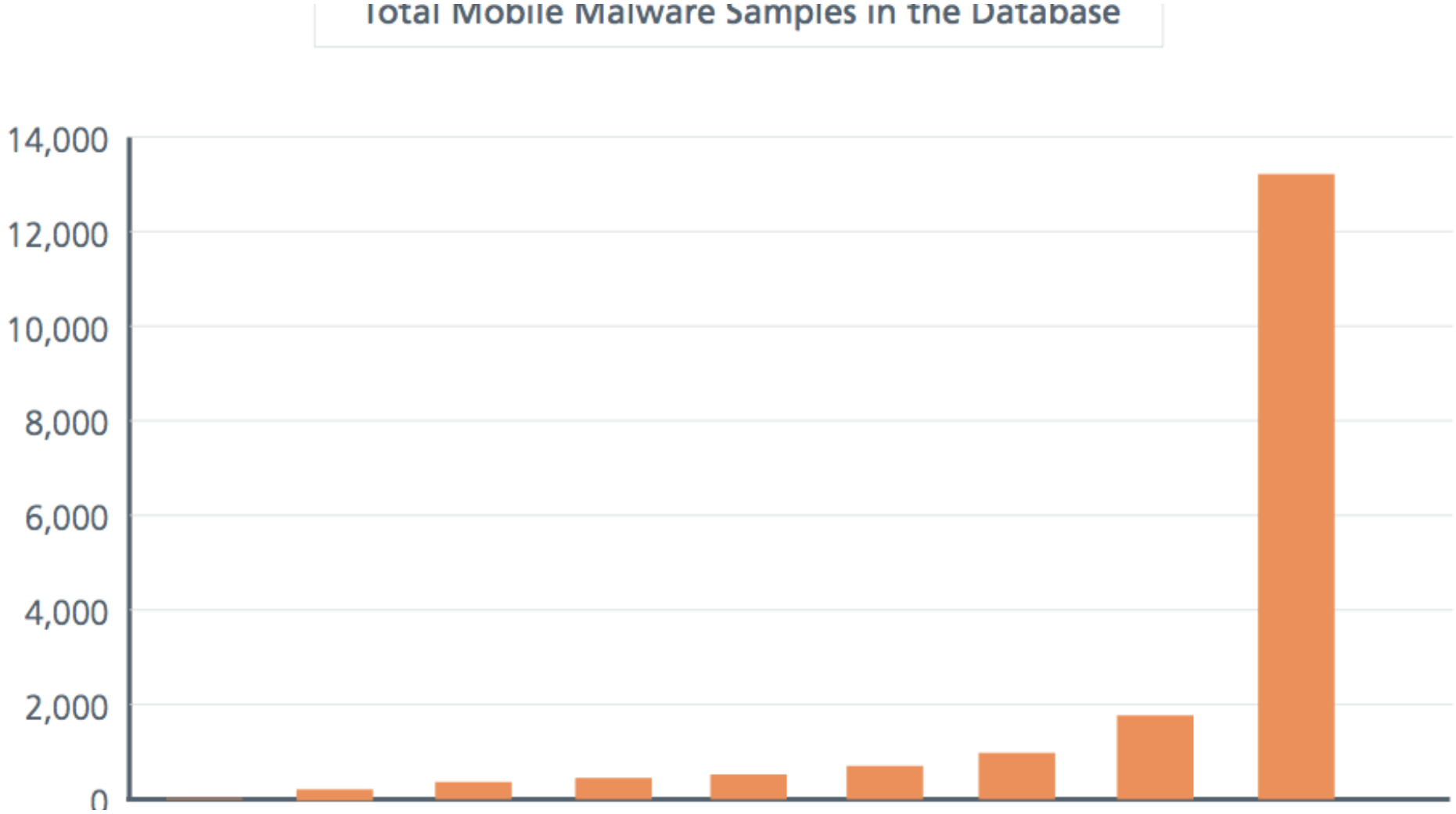
300M iPhones Sold



850,000 New Droids per Day

IRONKEY™

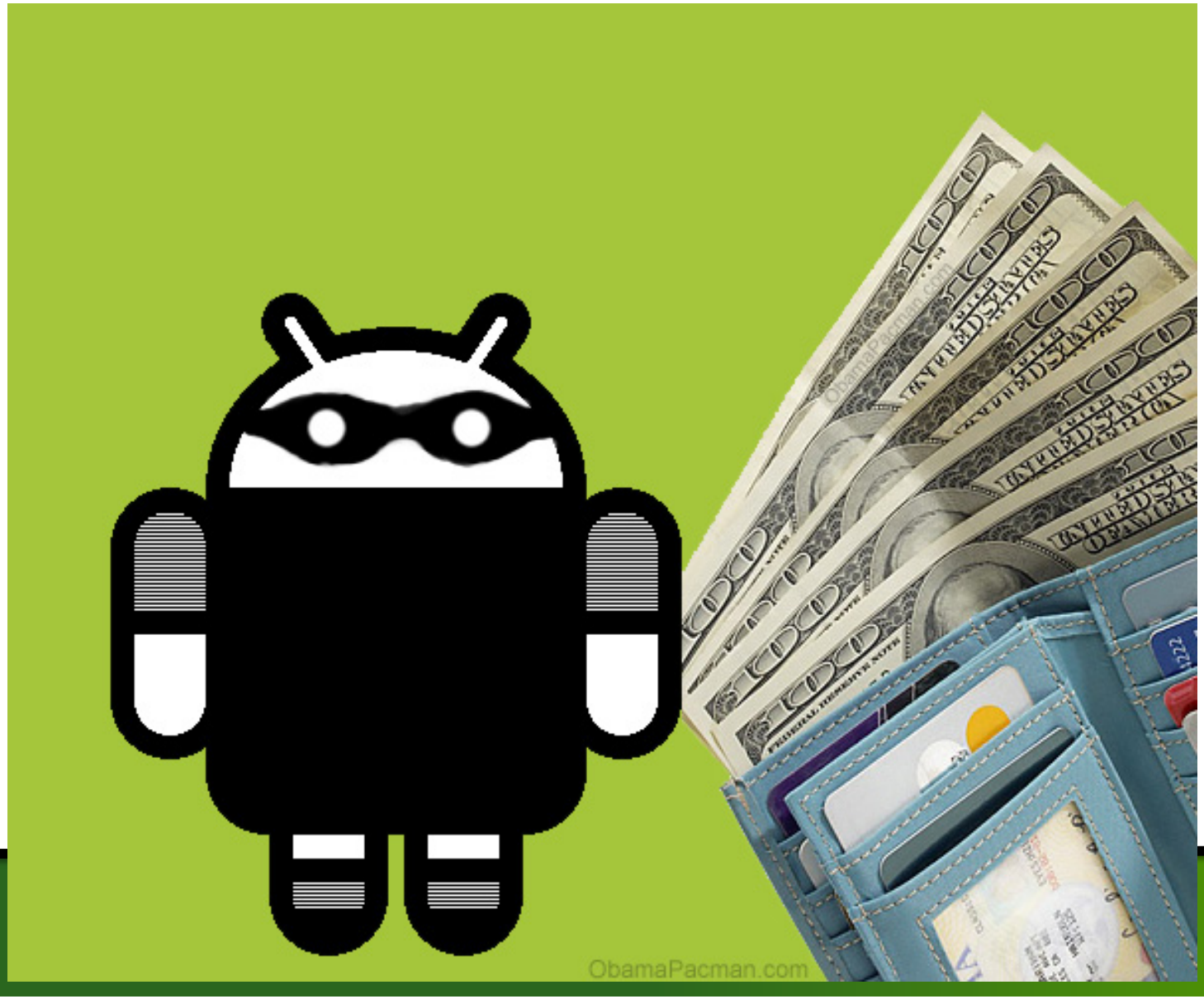



Total Mobile Malware Samples in the Database
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0

2012 Mobile Smartphone Threats

Smishing and Phishing on Mobile Phones

Fake Banking Apps



Hacked Apps Posted To Markets

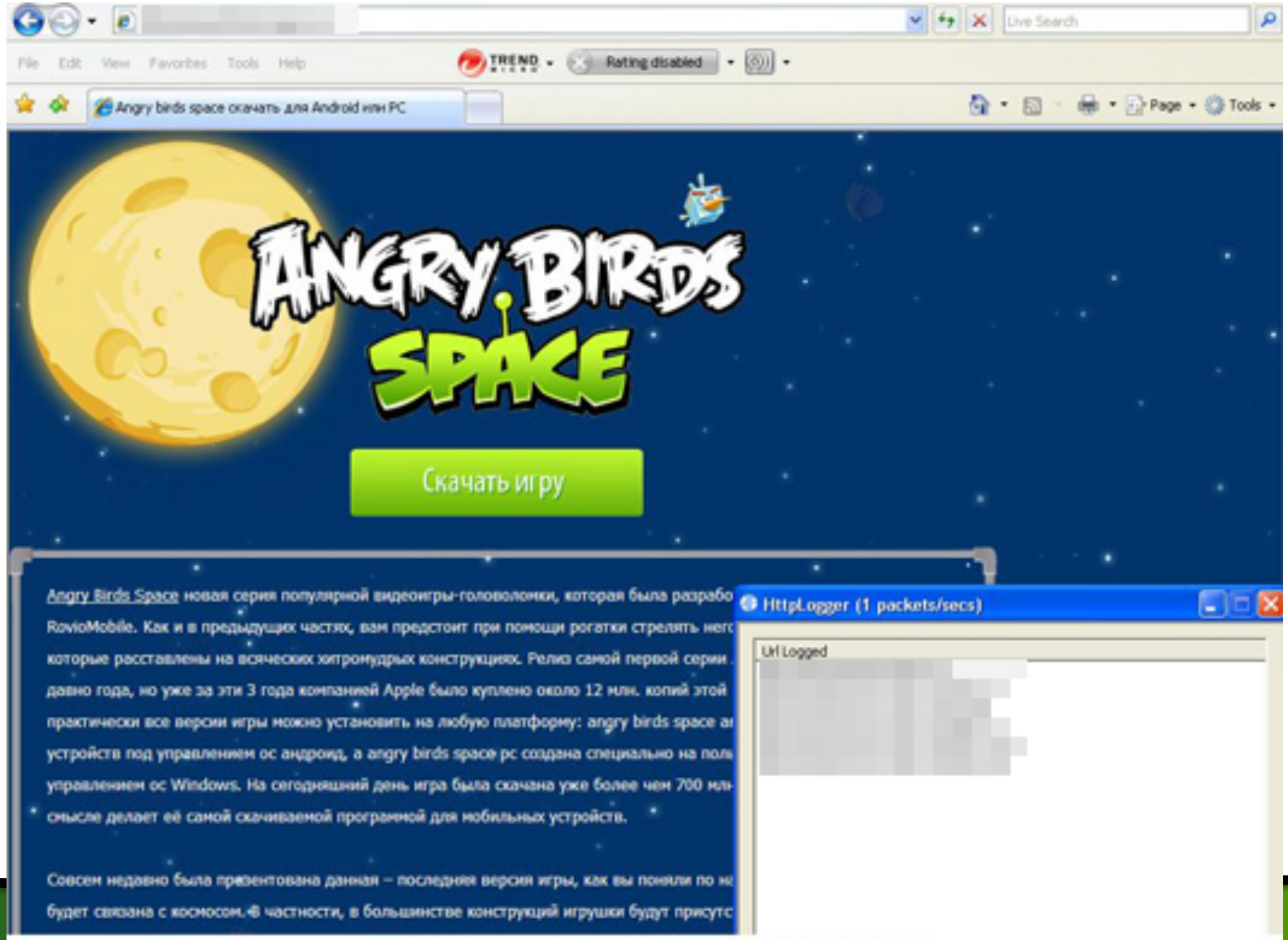
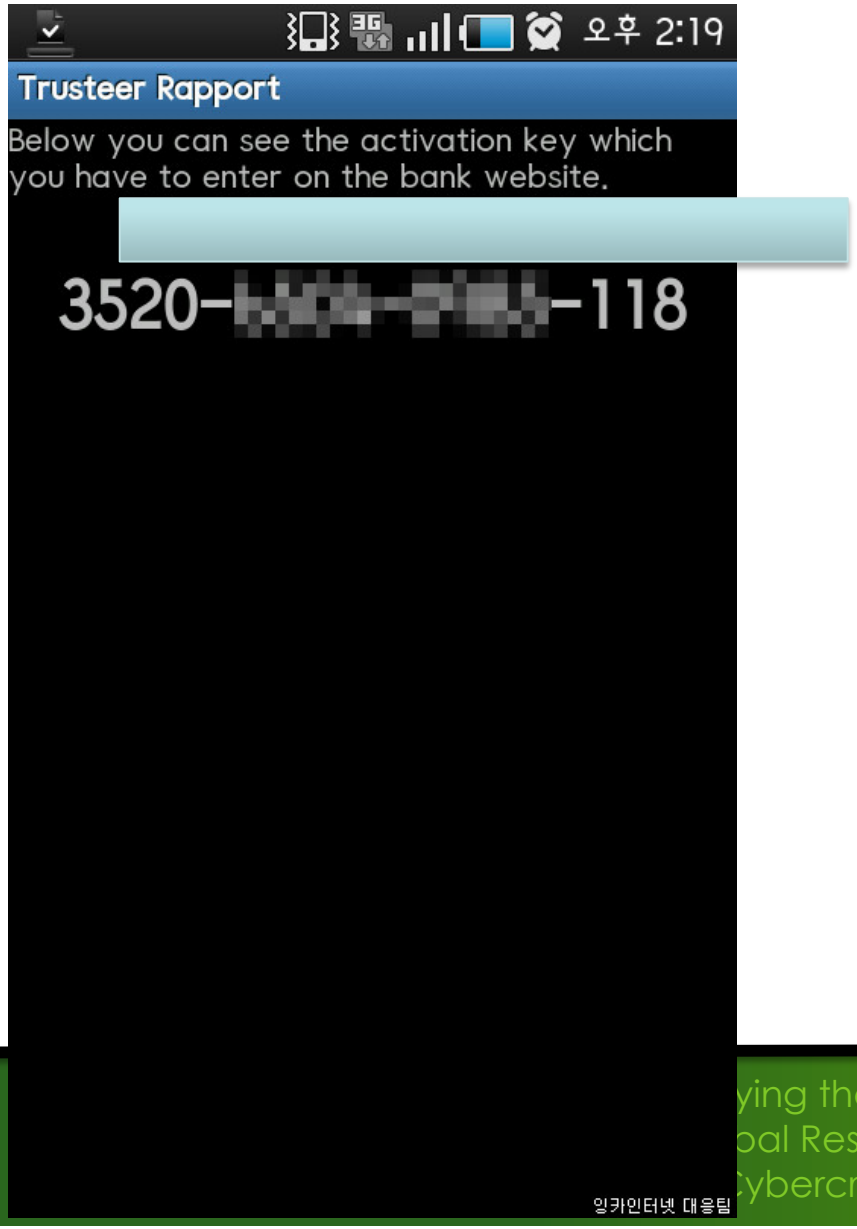


Figure 4. Site hosting rogue *Angry Birds Space*

Figure 1. Website showing free *Instagram* download lure

Fake OTP Apps Install Android Malware

Fake Security Apps



TECH | 5/04/2012 @ 1:22PM | 583 views

Android Hit By Drive-By Malware

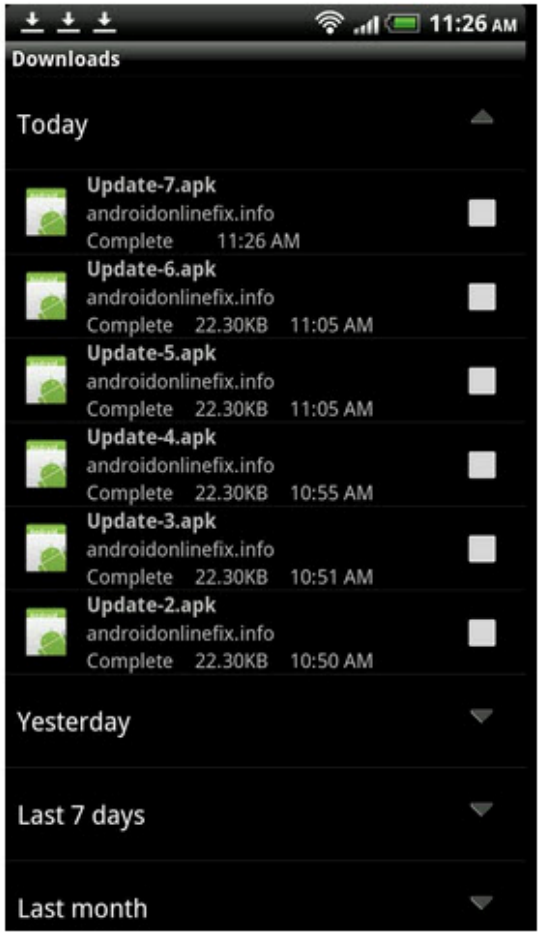
+ Comment now

New drive-by malware that attacks Android users visiting compromised websites has been discovered by Reddit users georgiabiker.

Sites distributing the malware have themselves been compromised and injected with malicious code called Troj/Iframe-HX. The malicious code examines the *User Agent* string sent by the browser to see if it contains the string "Android" and if it does a malicious Android package called *Update.apk* is sent to the browser.

Hacked websites are commonly used to infect PCs with malware, but this is the first example of Android users being targeted by this technique.

The good news about this malware is that is it only downloaded automatically, and relies on the user to do the job of installing it. For this to work the "Unknown sources" setting *enabled* (a feature commonly referred to as "sideloading").



- Sites infected with bad iFrame
- Checks User-Agent
- Update.apk sent to browser
- Installed if device allows apps from unknown sources

com.Security.Update

By Charlie Osborne for Zero Day | October 22, 2012 -- 07:58 GMT (00:58 PDT)

Follow @ZDNetCharlie

Research has shown that thousands of popular apps in the Google Play store may leave sensitive information exposed.

A paper (.pdf) released by researchers from Leibniz University in Hannover and Philipps University of Marburg, found that 17 percent of the Secure Sockets Layer (SSL)-using apps analyzed in a study -- biased towards free, popular applications -- were vulnerable to man-in-the-middle MITM attacks.

Man-in-the-middle attacks are similar to eavesdropping -- when an attacker intercepts messages, fakes authentication and may inject new information while impersonating a different source.

1,074 apps in a sample of 13,500 contained flaws in their SSL implementation, the researchers stating that these apps contained "SSL specific code that either accepts all certificates or all hostnames for a certificate and thus are potentially vulnerable to MITM attacks". From this sample, the teams manually created MITM attacks against 100 out of the set.

Through the attacks, data was fraudulently captured including "credentials for American Express, Diners Club, Paypal, Facebook, Twitter, Google, Yahoo,Microsoft Live ID, Box, WordPress, IBM Sametime, remote servers, bank accounts and email accounts." In addition, the team wrote:

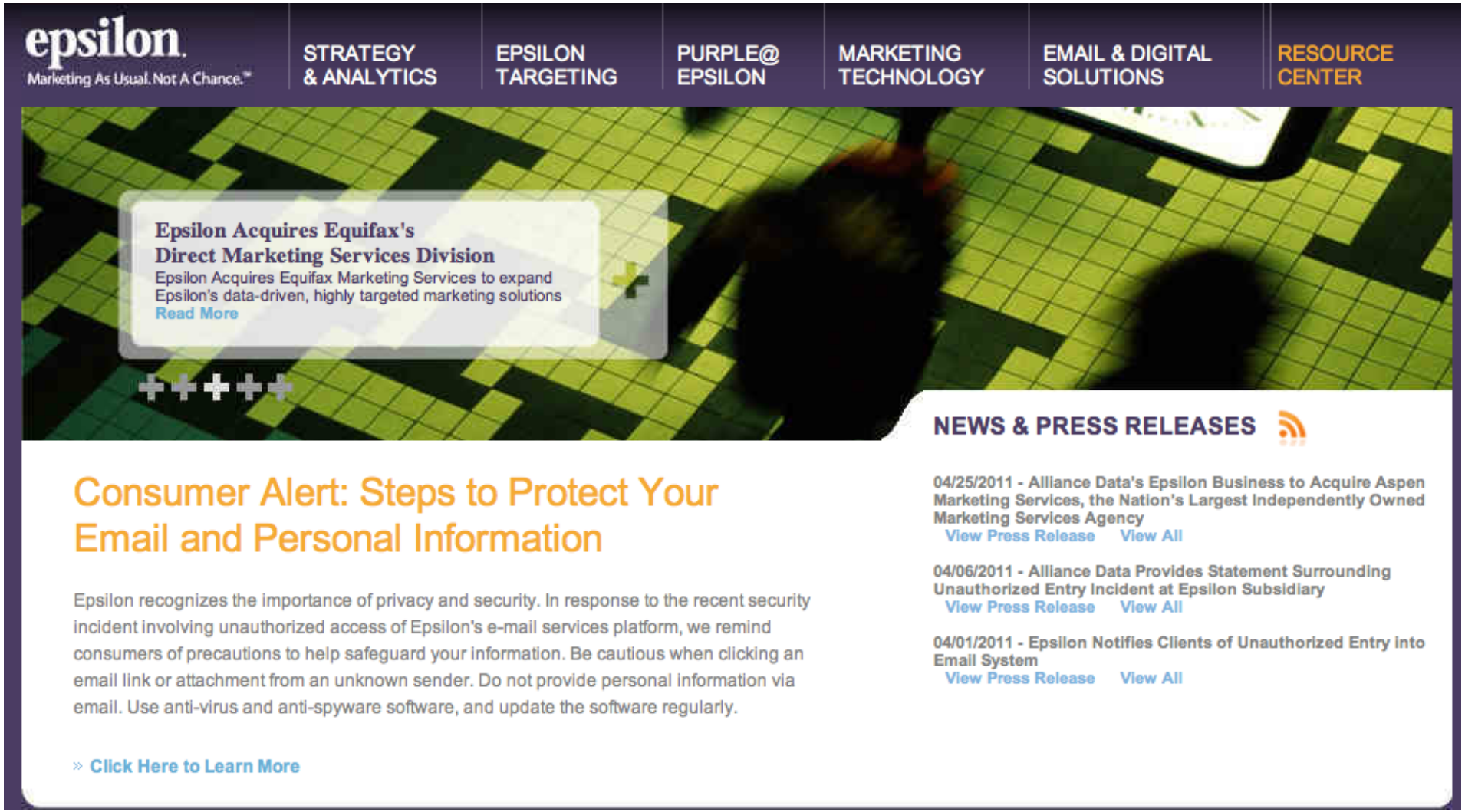
> "Facebook, email and cloud storage credentials and messages were leaked, access to IP cameras was gained and control channels for apps and remote servers could be subverted."

This wasn't the end of such vulnerabilities. By creating a proof-of-concept tool called MalloDroid which finds potentially exploitable SSL programming, the researchers were able to manipulate virus signatures to update the functionality of an anti-virus app to kill off mobile device protection or even remove applications.

Reviewing Predictions

- Using compromised infrastructure to mount attacks

Email Service Providers Are An Important Attack Vector



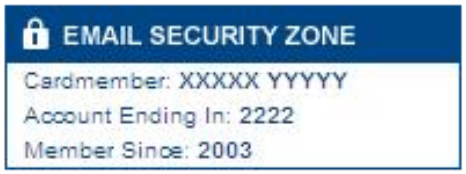
fication

Dear David Jevans,

Recently, Citi was notified of a system breach at Epsilon, a third-party vendor that provides marketing services to a number of companies, including Citi. The information obtained was limited to the customer name and email address of some credit card customers. No account information or other information was compromised and therefore there is no reason to re-issue a new card.

Because e-mail addresses can be used for "phishing" attacks, we want to remind our customers of the following:

- Citi Cards uses an Email Security Zone in
  email to help you recognize that the email
  us. Customers should check the Email Sec
  verify that the email you received is from C
  reduce the risk of personal information beir
  To help you recognize that the email was s
  we will always include the following in the E
  Security Zone in the top headline portion o
  emails:
  - Your first name and last name
  - Last four digits of your Citi card acc
  - *And recently to increase security, w*
    added your "member since" date loc
    front of your card, where available.



- ThankYou(SM) Rewards always includes y
  name, last name, last four digits of your Th

on our behalf to our customers, that files containing your first and
o their computer system. MoneyGram was one of a number of companies
ion that was compromised does not include any customer financial

ils that contain links containing computer viruses or other types of
l information. You should be extremely cautious before opening links or
ion in response to any email. If you receive an email that appears to be
t to TransactionSecurity@moneygram.com. It did not come from MoneyGram.

your personal ID, password, social security number, PIN or account
tion in response to an email request at any time.*

Sent: Monday, April 04, 2011 10:04 AM
Subject: Please read important message about your e-mail address

Note: This is a service message with information related to your e-ma

CHASE

Chase is letting our customers know that we have been informed by
send e-mails, that an unauthorized person outside Epsilon accessed f
addresses of some Chase customers. We have a team at Epsilon inve
confident that the information that was retrieved included some Chas
addresses, but did **not** include any customer account or financial info
everything we know, your accounts and confidential information rema
are advising our customers of everything we know as we know it, and
what impact, if any, this will have on you.

We apologize if this causes you any inconvenience. We want to remin
ask for your personal information or login credentials in an e-mail. As
receive e-mails asking for your personal information and be on the lo
It is **not** Chase's practice to request personal information by e-mail.

As a reminder, we recommend that you:

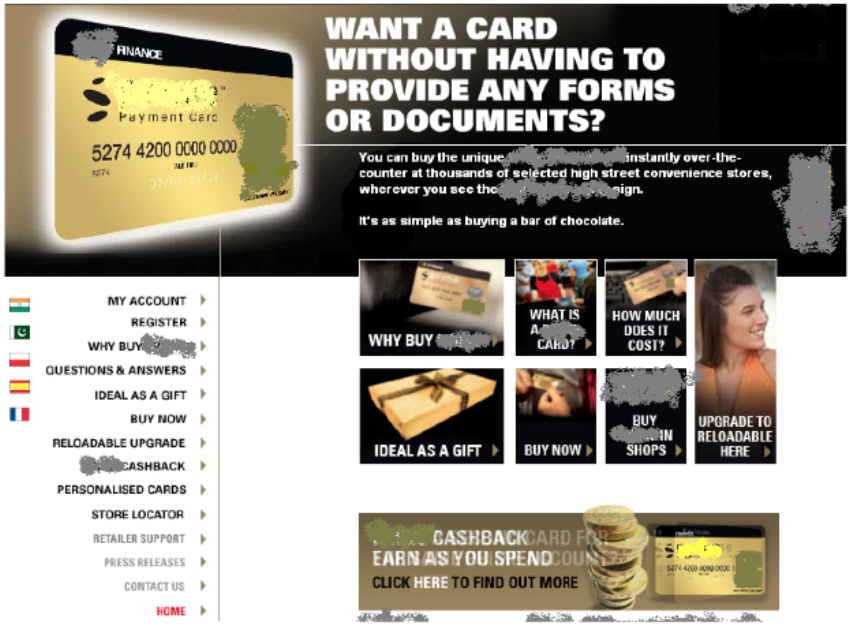
- Don't give your Chase Online[SM] User ID or password in e-mail

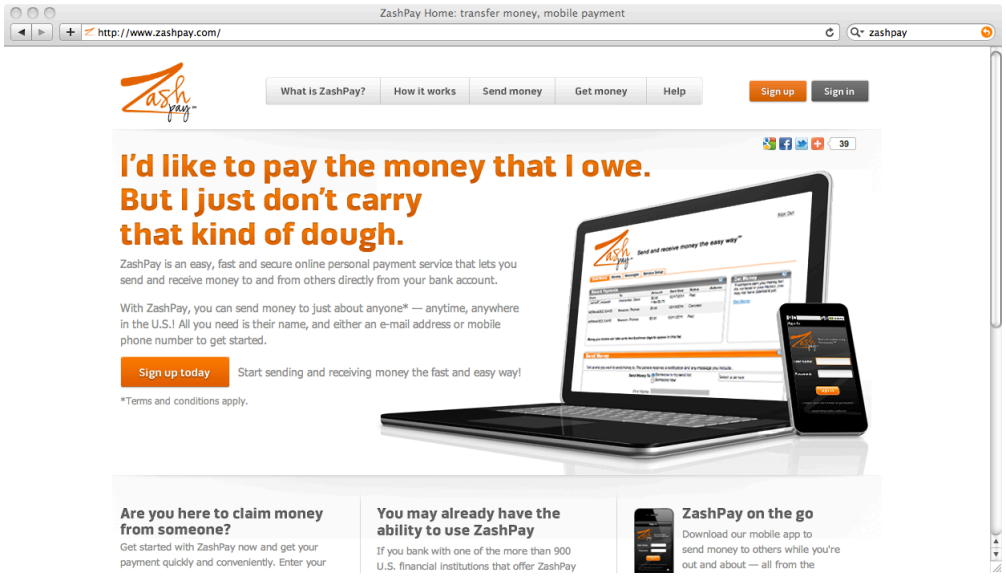
A Lack of Money Mules Will No Longer Slow Fraud Losses

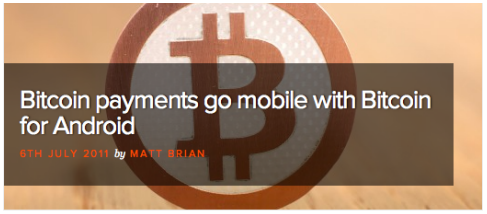
Card-to-Card Transfer

With RushCard Card-To-Card Transfer, you can send money to anyone with a RushCard or transfer money between your own personal cards. Send birthday money to your sister, emergency cash to your son in college, or stash away some savings on your secondary card. Whatever your reason, you'll enjoy:

- The flexibility to send money instantly or schedule a future transfer
- An affordable rate that is a fraction of the cost of wiring money
- Quick instant transfers – done in just 15 minutes time
- The convenience of completing a transfer online, from your mobile phone, or over the phone with a live agent





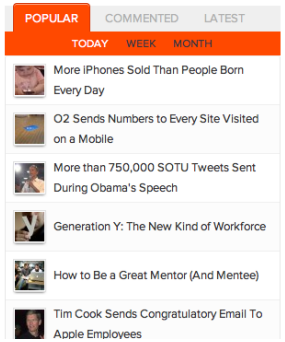


If you have invested in the virtual currency Bitcoin, the chances are that you want to be able to send and receive Bitcoin payments on your smartphone device.

Whilst there are a number of options available to Bitcoin investors, a dedicated Android app that could facilitate the sending and receiving of Bitcoins and support additional Bitcoin features had not been forthcoming – until today.

Bitcoin for Android is a new application which operates as a fully functional Bitcoin wallet. Available on the Android Market, the app supports the scanning of QR codes to initiate transactions, allows users to email invoices from their device to request money and can even process payments without an Internet connection by waiting to send transactions when a connection is restored.

The application natively supports the Bitcoin URI format and backs up a user's wallet file to the Cloud by synchronising it to a user's Google account – useful if a user loses their phone.



North Miami Beach, Florida (CNN) -- Criminals across the country are raking in billions of dollars in tax refunds through a new and brazen form
returns, law

Using characteristics of tax returns that the IRS has identified and confirmed as fraudulent filings involving identity theft, we analyzed Tax Year 2010 tax returns to identify additional tax returns that met the characteristics of these confirmed cases. Our analysis found that, although the IRS detects and prevents a large number of fraudulent refunds based on false income documents, there is much fraud that it does not detect. We identified approximately 1.5 million additional undetected tax returns with potentially fraudulent tax refunds totaling in excess of $5.2 billion. If not addressed, we estimate the IRS could issue approximately $26 billion in fraudulent tax refunds resulting from identity theft over the next five years.

can issue th
gotten their returns on actual Treasury checks.

The thieves know that the IRS does not verify the employer W-2s sent with the return until after the refund is issued.

Reviewing Predictions

- Death of Bitcoin exaggerated


Market Price (USD)
Source: blockchain.info
Market Price (USD)
16
14
12
10
8
6
4
2
Nov '11
Dec '11
Jan '12
Feb '12
Mar '12
Apr '12
May '12
June '12
Jul '12
Aug '12
Sep '12
Oct '12

2	Linode Hacks	March 2012	46700 ฿ a. 46653.47830495 ฿
3	July 2012 Bitcoinica Theft	July 2012	40000.00000000 ฿
4	Allinvain Theft	June 2011	25000.01000000 ฿
5	Bitfloor Theft	September 2012	u.b. 24086.17219307 ฿
6	Tony Silk Road Scam	April 2012	est. 20000 ฿
7	May 2012 Bitcoinica Hack	May 2012	18547.66867623 ฿
8	*Bitomat.pl Loss*	August 2011	est. 17000 ฿
9	Bitcoin7 Hack	October 2011	est. 11000 ฿ u.b. 15000 ฿

Major (≥1000 ฿)

Rank	Name	Time	Severity
10	*Stefan Thomas Loss*	June 2011	est. 7000 ฿
11	BTC-E Hack	July 2012	est. 4500 ฿
12	Mooncoin Theft	September 2011	est. 4000 ฿
12	Kronos Hack	Unknown	est. 4000 ฿
14	Betcoin Theft	April 2012	3171.50195016 ฿
15	February 2012 Bitcoinica Theft	February 2012	est. 3000 ฿
16	June 2011 Mt. Gox Incident	June 2011	2600 ฿ l.b. 2643.27 ฿
17	*October 2011 Mt. Gox Loss*	October 2011	2609.36304319 ฿

Reviewing Predictions

- Cyber Warfare

Panetta Warns of Dire Threat of Cyberattack on U.S.

By ELISABETH BUMILLER and THOM SHANKER
Published: October 11, 2012 | 192 Comments

Defense Secretary Leon E. Panetta warned Thursday that the United States was facing the possibility of a "cyber-Pearl Harbor" and was increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government.

Francois Lenoir/Reuters

Defense Secretary Leon Panetta seeks new standards to protect vital infrastructure.

Related

Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials (September 27, 2012)

In a speech at the Intrepid Sea, Air and Space Museum in New York, Mr. Panetta painted a dire picture of how such an attack on the United States might unfold. He said he was reacting to increasing aggressiveness and technological advances by the nation's adversaries, which officials identified as China, Russia, Iran and militant groups.

"An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches," Mr. Panetta said. "They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."

Defense officials insisted that Mr. Panetta's words were not hyperbole, and that he was responding to a recent wave of

Market Responses

- 18 months ago only 3 Android anti-malware products
- Now over 40

Market Responses

- Censorship
  - TOR
  - AnchorFree, 10M users
  - 225 VPN services

Market Responses

- Web fraud skyrockets
  - Silvertail, Guardian Analytics, etc

Market Responses

- Advanced Persistent Threats detection
  - Damballa, FireEye, Netwitness

Emerging Threats

- Javascript methods to attack internal machines
- Javascript monitoring of all activities
- Javascript sending webforms for other sites

Emerging Threats

- Passwords are still the biggest security problem on the Internet

Emerging Threats

- Spear-phishing

Emerging Threats

- Spear-phishing/Malware to bank employees

Emerging Threats

- Using mobile devices as entry points for cybercrime
  - Spear-phishing to phones
  - Malicious apps on phones
  - Capturing 2FA
  - Exploiting the coming phone-to-car rich interfaces

Emerging Threats

- Encrypted communities
  - The bad buys will take up this technology much faster than the good guys
    - Wikr, etc
  - What percentage of the people that you email do it encrypted?

Emerging Threats

- CyberWar hype stimulates crazy responses
  - Banning Chinese firewall vendors
    - Good, bad?
  - Billions spent by multiple conflicting agencies

A flame from a Saudi Aramco oil installion is seen near the oil-rich area of Khouris, Saudi Arabia, in 2008. Middle Eastern oil and gas companies have been targeted in

Emerging Threats

- Darknets
  - Silk Road was only the beginning
  - There are thousands of Tor hidden services
  - Once they get strong end-to-end encryption easy to use, it will be unstoppable
  - Even the US government is paying for steganography development

What Can We Do?

- Conferences like this are crucial
- Private and pubic sector must share information and wisdom
- Data sharing standards need to be activated and implemented

How Does a World of Localities Engage a Problem of Global Dimensions Like Cybercrime and Respond with Consolidated Effort?

Unified Data Logistics

- Too many stakeholders to let Tower of Babel be the operational model.
- Time to:
  - Rationalize data structures
  - Standardize cybercrime file formats
  - Standardize data exchange and communications protocols
  - Coordinate efforts through (technically) unimpeded data sharing
  - Data policy impedances another matter
    - But we're working on it

Thank You To Our Sponsors

ILLUMINTEL

Illumintel Inc. provides advising and security services to top-level-domain registry operators and other Internet companies.

IID

Internet Identity (IID) is a US-based provider of technology and services that help organizations secure their Internet presence.

MarkMonitor®

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

PANDA SECURITY

Panda Security's mission is to keep our customers' information and IT assets safe from security threats, providing the most effective protection with minimum resource consumption.

Yes! websense®
ESSENTIAL INFORMATION PROTECTION™

Websense, Inc. is a global leader in secure Web gateway, data loss prevention, and e-mail security solutions, protecting more than 43 million employees at organizations worldwide.