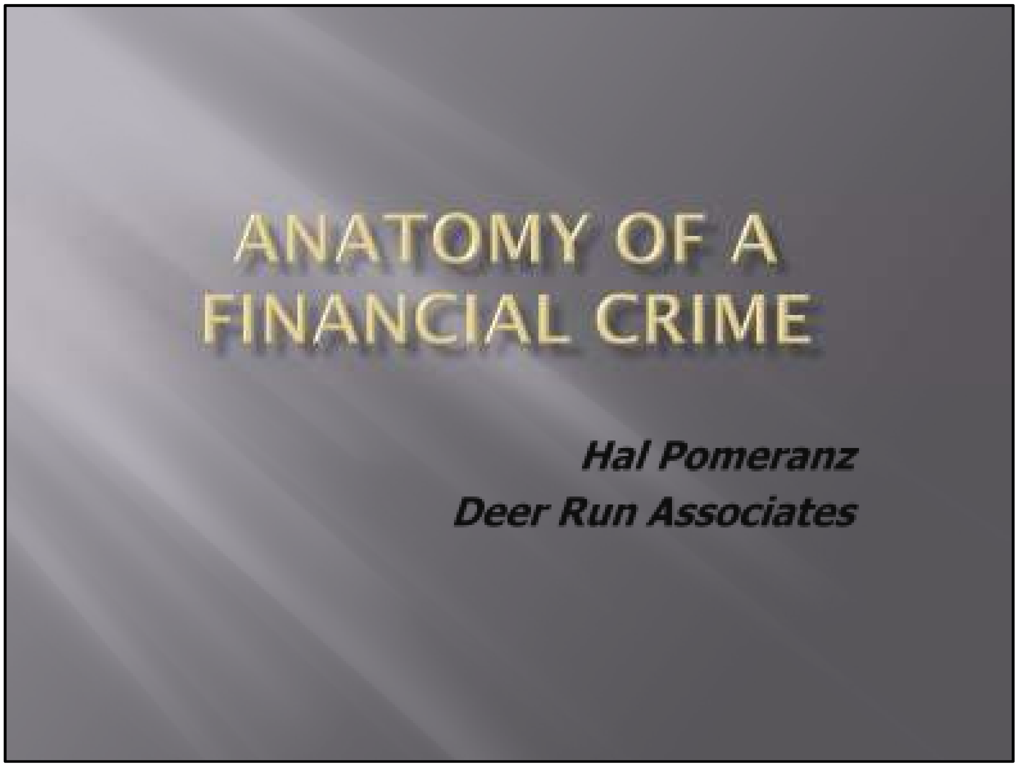
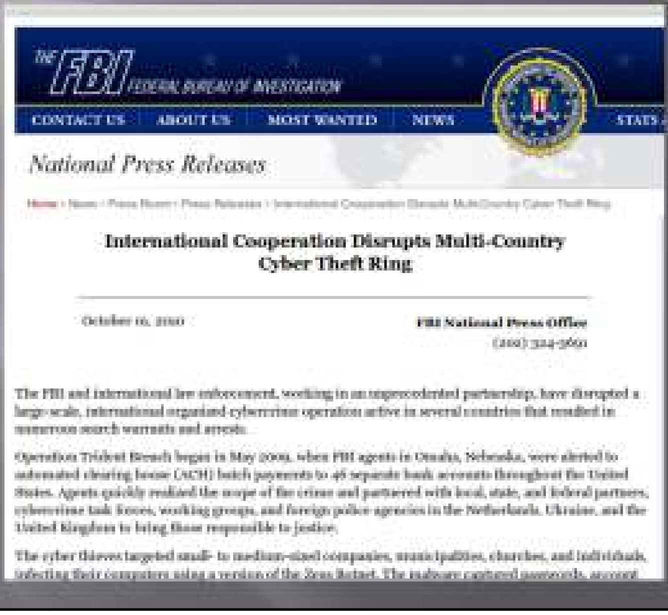


ANATOMY OF A FINANCIAL CRIME

Hal Pomeranz
Deer Run Associates

Where Has Hal Been?



National Press Releases

Home › News › Press Room › Press Releases › International Cooperation Disrupts Multi-Country Cyber Theft Ring

International Cooperation Disrupts Multi-Country Cyber Theft Ring

October 01, 2010

FBI National Press Office
(202) 324-3691

The FBI and international law enforcement, working in an unprecedented partnership, have disrupted a large-scale, international organized cybercrime operation active in several countries that resulted in numerous search warrants and arrests.

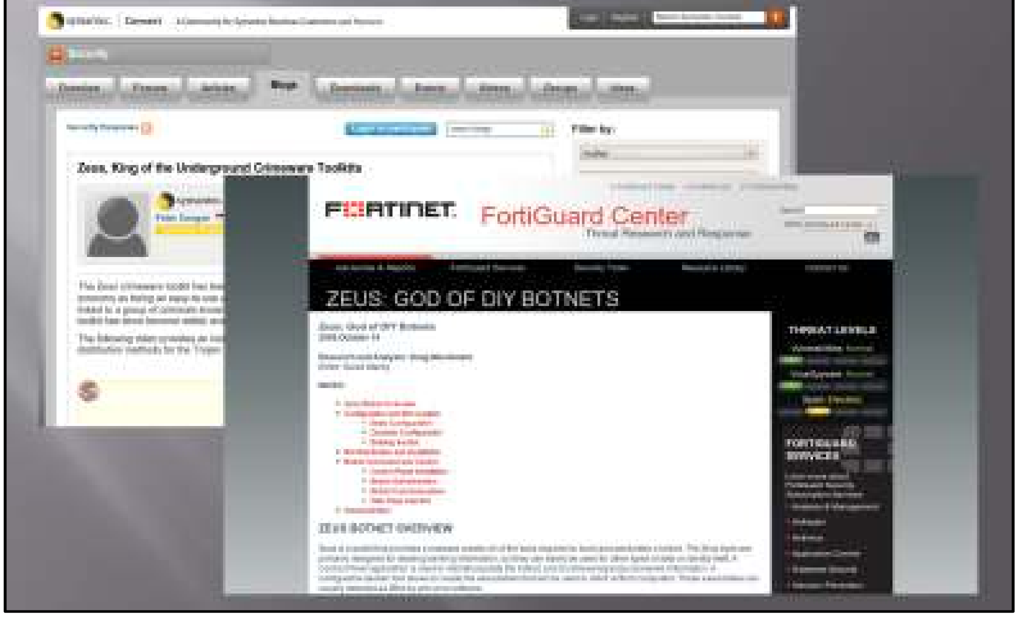
Operation Trident Breach began in May 2009, when FBI agents in Omaha, Nebraska, were alerted to automated clearing house (ACH) batch payments to 46 separate bank accounts throughout the United States. Agents quickly realized the scope of the crime and partnered with local, state, and federal partners, cybercrime task forces, working groups, and foreign police agencies in the Netherlands, Ukraine, and the United Kingdom to bring those responsible to justice.

The cyber thieves targeted small- to medium-sized companies, municipalities, churches, and individuals, infecting their computers using a version of the Zeus Botnet. The malware captured passwords, account

http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring

]

Lot's of Publicly Available Info



Filter by:

Zeus, King of the Underground Crimeware Toolkits

FortiGuard Center

Threat Research and Response

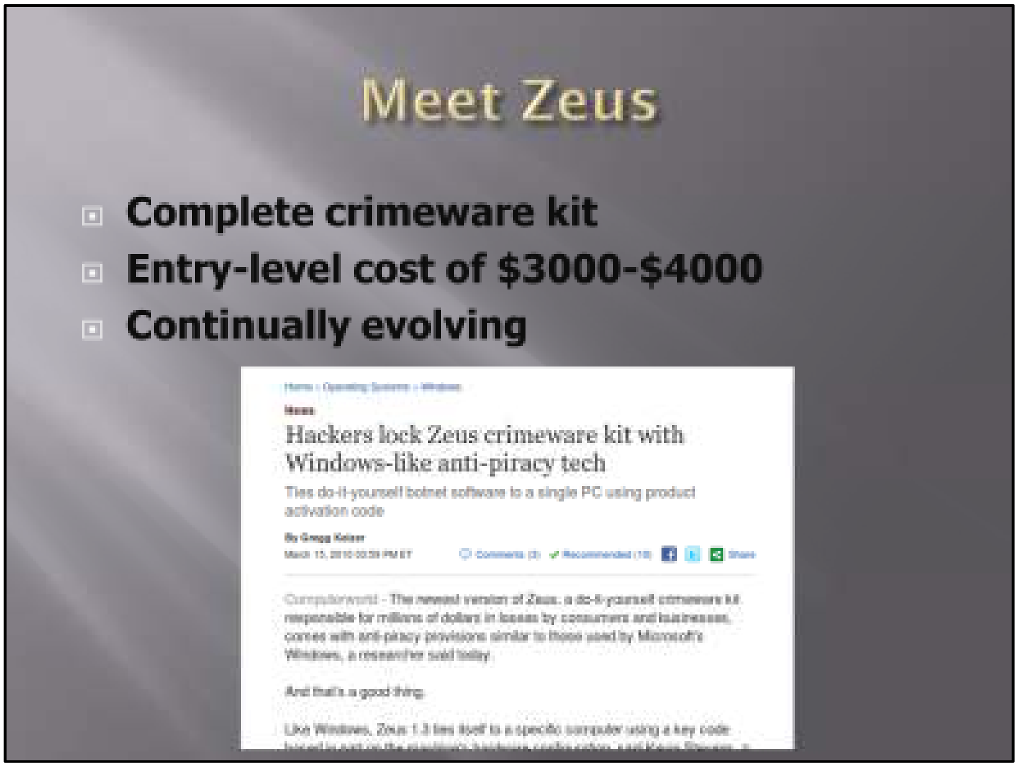
ZEUS: GOD OF DIY BOTNETS

Zeus: God of DIY Botnets

2009 October 14

ZEUS BOTNET OVERVIEW

http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits
http://www.youtube.com/watch?v=CzdBCDPETxk
http://www.fortiguard.com/analysis/zeusanalysis.html



Meet Zeus

- Complete crimeware kit
- Entry-level cost of $3000-$4000
- Continually evolving

Home › Operating Systems › Windows

News

Hackers lock Zeus crimeware kit with Windows-like anti-piracy tech

Ties do-it-yourself botnet software to a single PC using product activation code

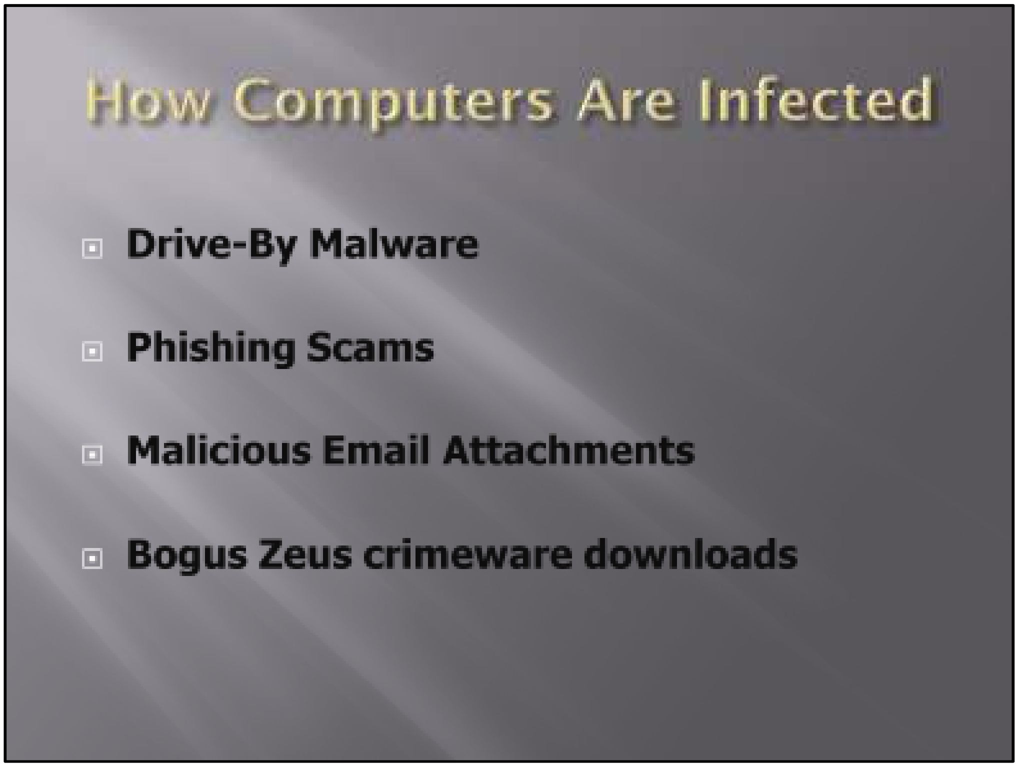
By Gregg Keizer
March 15, 2010 03:39 PM ET

Computerworld - The newest version of Zeus, a do-it-yourself crimeware kit responsible for millions of dollars in losses by consumers and businesses, comes with anti-piracy provisions similar to those used by Microsoft's Windows, a researcher said today.

And that's a good thing.

Like Windows, Zeus 1.3 ties itself to a specific computer using a key code

http://www.computerworld.com/s/article/9170978/Hackers_lock_Zeus_crimeware_kit_with_Windows_like_anti_piracy_tech



How Computers Are Infected

- Drive-By Malware
- Phishing Scams
- Malicious Email Attachments
- Bogus Zeus crimeware downloads

Does This Really Work?

› Security Fix

Security Fix

Brian Krebs on Computer Security

About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Brian Krebs

SEARCH THIS BLOG

Go

RECENT POSTS

- Bit.ly to scour shortened links for badness
- DC bookkeeper loses thousands after clicking on wrong e-mail

Zeus Trojan Infiltrates Bank Security Firm

On Sept. 1, security industry sta in-depth online seminar for its b examined the stealth and sophi horse program that organized t cyber heists this year.

A week later, Silver Tail learned network defenses.

Silver Tail founder **Laura Mathe** targeted by criminals wielding Z webinar, which spotlighted the r

cnet news

InSecurity Complex

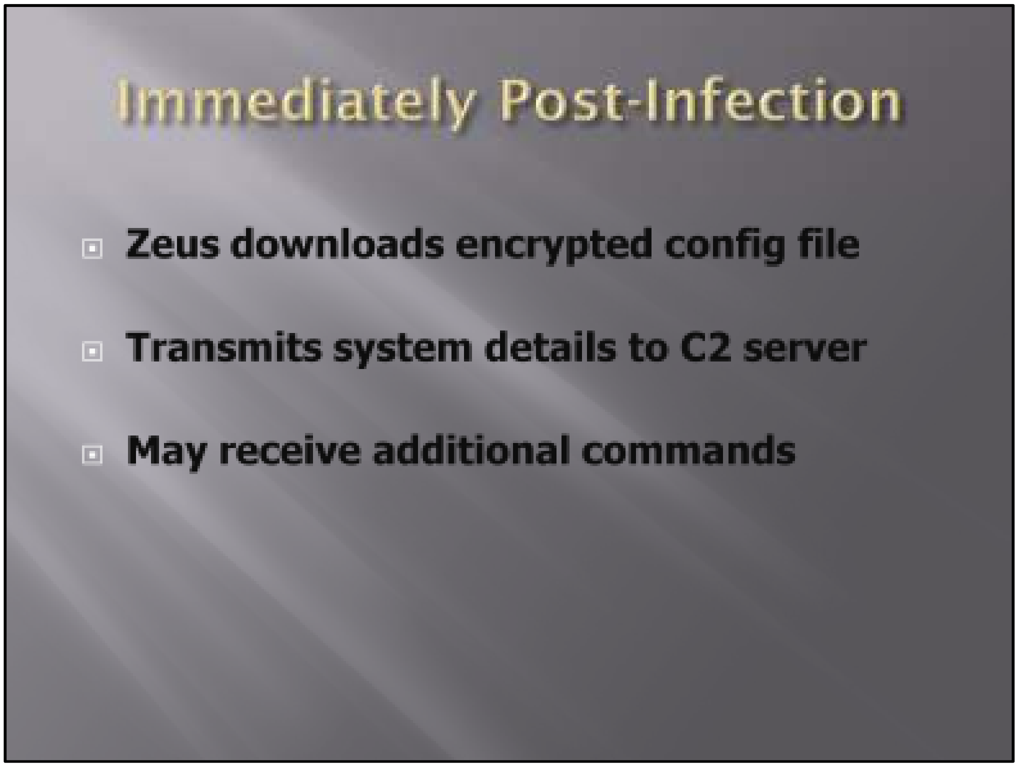
88 percent of firms show Zeus botnet activity

179

[illegible]

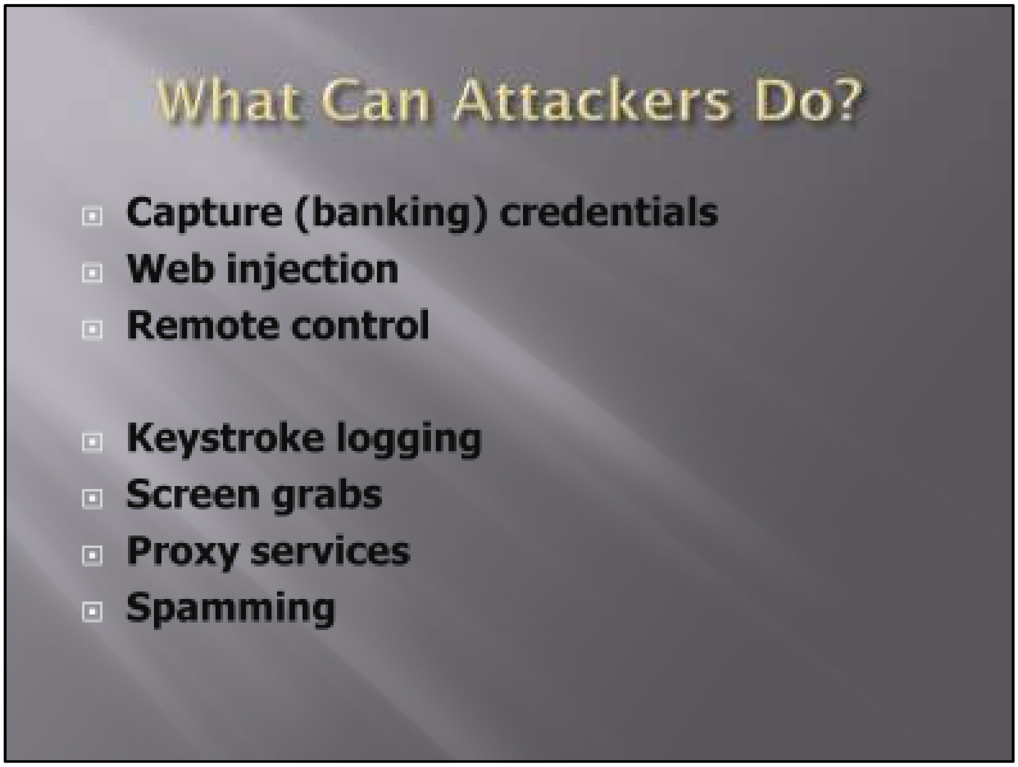
RSA's FraudAction [illegible]

http://voices.washingtonpost.com/securityfix/2009/10/ubiquitous_zeus_trojan_targets.html
http://news.cnet.com/8301-27080_3-20002425-245.html



Immediately Post-Infection

- Zeus downloads encrypted config file
- Transmits system details to C2 server
- May receive additional commands

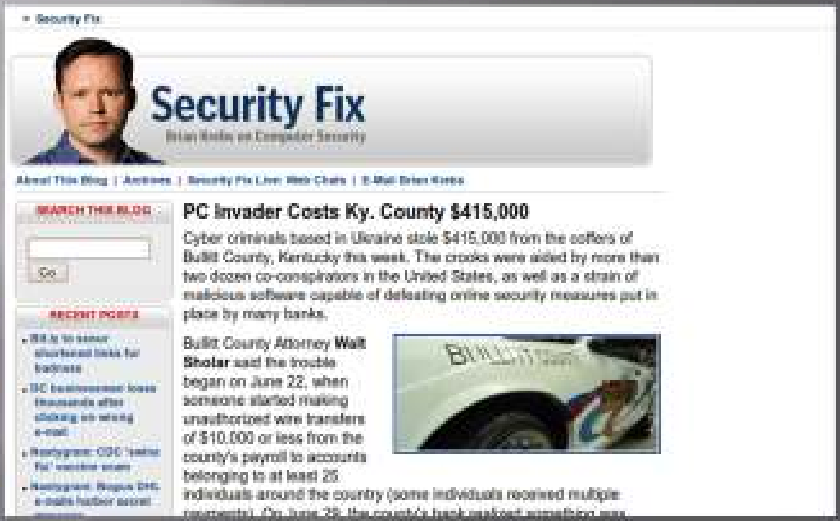


What Can Attackers Do?

- Capture (banking) credentials
- Web injection
- Remote control

- Keystroke logging
- Screen grabs
- Proxy services
- Spamming

A Typical Theft



▾ Security Fix

Security Fix

Brian Krebs on Computer Security

About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Brian Krebs

SEARCH THIS BLOG

Go

RECENT POSTS

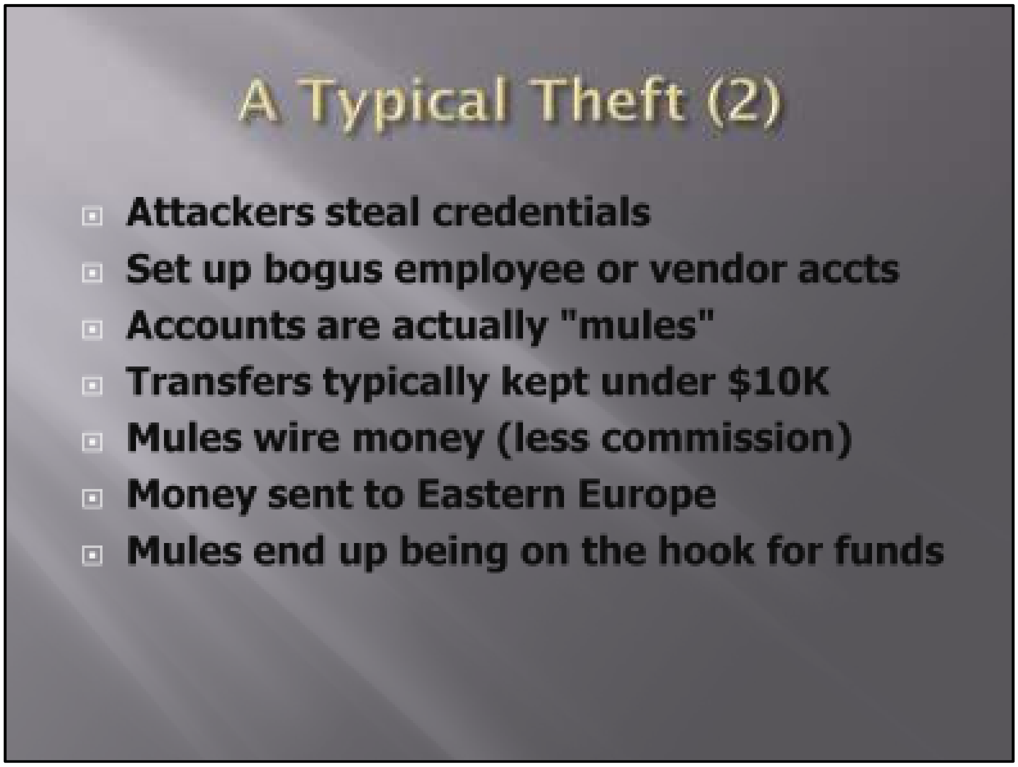
- Bit.ly to scour shortened links for badness
- DC businessman loses thousands after clicking on wrong e-mail
- Realygram: CDC 'swine flu' vaccine scam
- Realygram: Bogus DHL e-mails harbor secret

PC Invader Costs Ky. County $415,000

Cyber criminals based in Ukraine stole $415,000 from the coffers of Bullitt County, Kentucky this week. The crooks were aided by more than two dozen co-conspirators in the United States, as well as a strain of malicious software capable of defeating online security measures put in place by many banks.

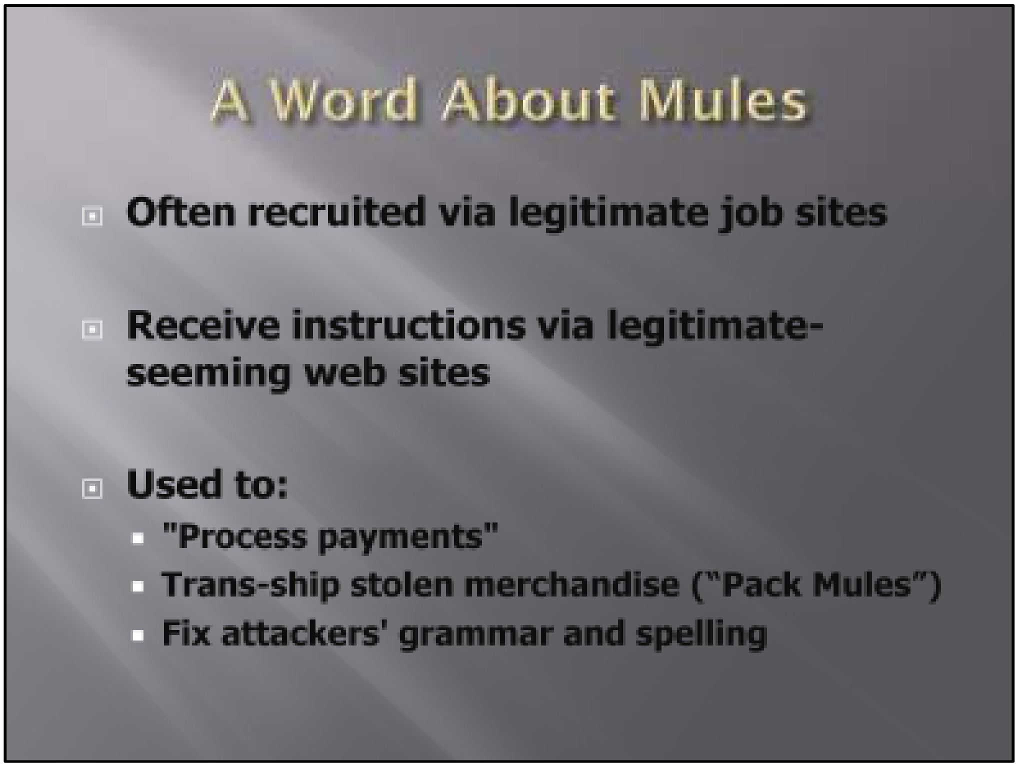
Bullitt County Attorney **Walt Sholar** said the trouble began on June 22, when someone started making unauthorized wire transfers of $10,000 or less from the county's payroll to accounts belonging to at least 25 individuals around the country (some individuals received multiple payments). On June 29, the county's bank realized something was

http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html



A Typical Theft (2)

- Attackers steal credentials
- Set up bogus employee or vendor accts
- Accounts are actually "mules"
- Transfers typically kept under $10K
- Mules wire money (less commission)
- Money sent to Eastern Europe
- Mules end up being on the hook for funds

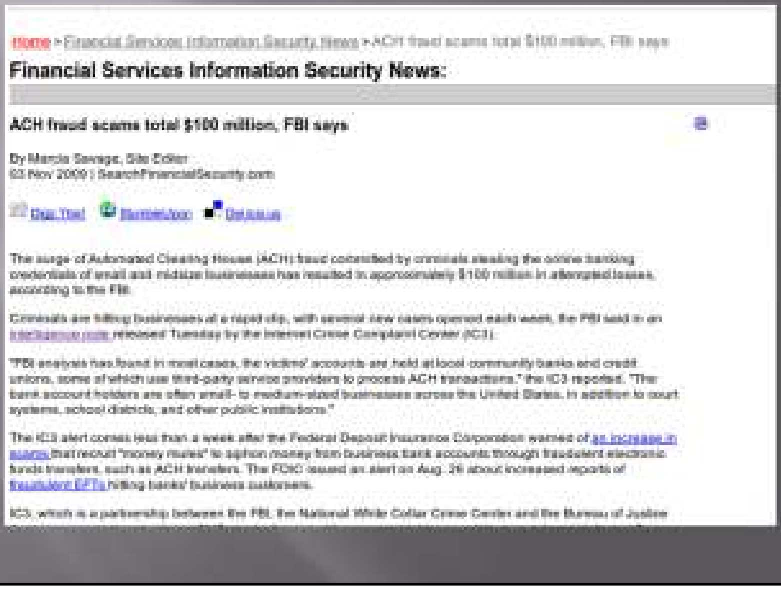


A Word About Mules

- Often recruited via legitimate job sites
- Receive instructions via legitimate-seeming web sites
- Used to:
  - "Process payments"
  - Trans-ship stolen merchandise ("Pack Mules")
  - Fix attackers' grammar and spelling

http://www.nartv.org/2010/12/16/pack-mules-the-re-shipping-fraud-malware-connection/

Bad News for Small Business



Home > Financial Services Information Security News > ACH fraud scams total $100 million, FBI says

Financial Services Information Security News:

ACH fraud scams total $100 million, FBI says

By Marcia Savage, Site Editor
03 Nov 2009 | SearchFinancialSecurity.com

Digg This! StumbleUpon Del.icio.us

The surge of Automated Clearing House (ACH) fraud committed by criminals stealing the online banking credentials of small and midsize businesses has resulted in approximately $100 million in attempted losses, according to the FBI.

Criminals are hitting businesses at a rapid clip, with several new cases opened each week, the FBI said in an intelligence note released Tuesday by the Internet Crime Complaint Center (IC3).

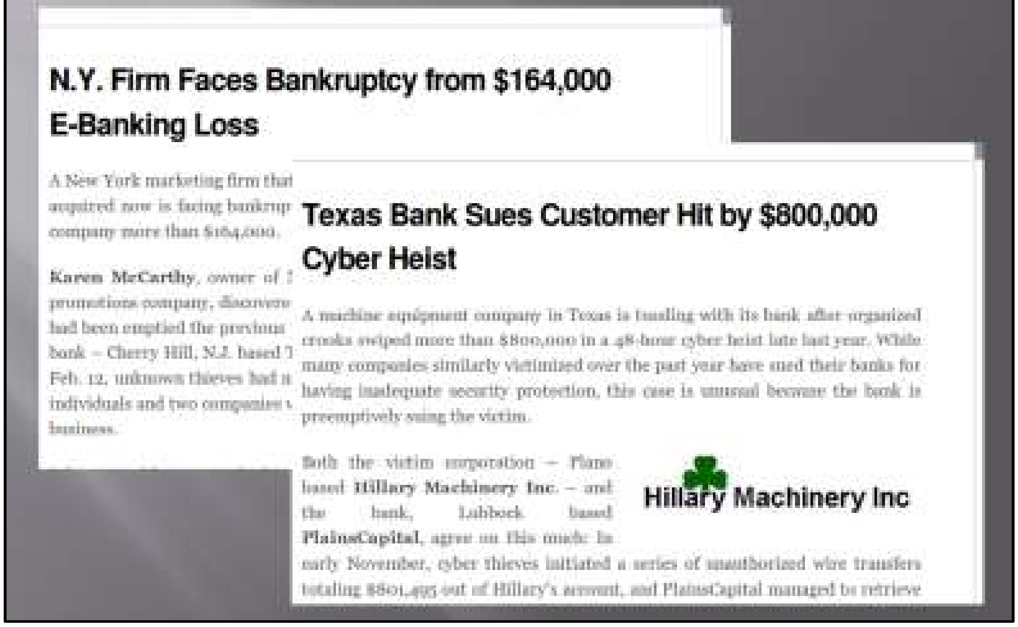
"FBI analysis has found in most cases, the victims' accounts are held at local community banks and credit unions, some of which use third-party service providers to process ACH transactions," the IC3 reported. "The bank account holders are often small- to medium-sized businesses across the United States, in addition to court systems, school districts, and other public institutions."

The IC3 alert comes less than a week after the Federal Deposit Insurance Corporation warned of an increase in scams that recruit "money mules" to siphon money from business bank accounts through fraudulent electronic funds transfers, such as ACH transfers. The FDIC issued an alert on Aug. 26 about increased reports of fraudulent EFTs hitting banks' business customers.

IC3, which is a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice

http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1373452,00.html

Downstream Effects…



N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

A New York marketing firm that
acquired now is facing bankrup
company more than $164,000.

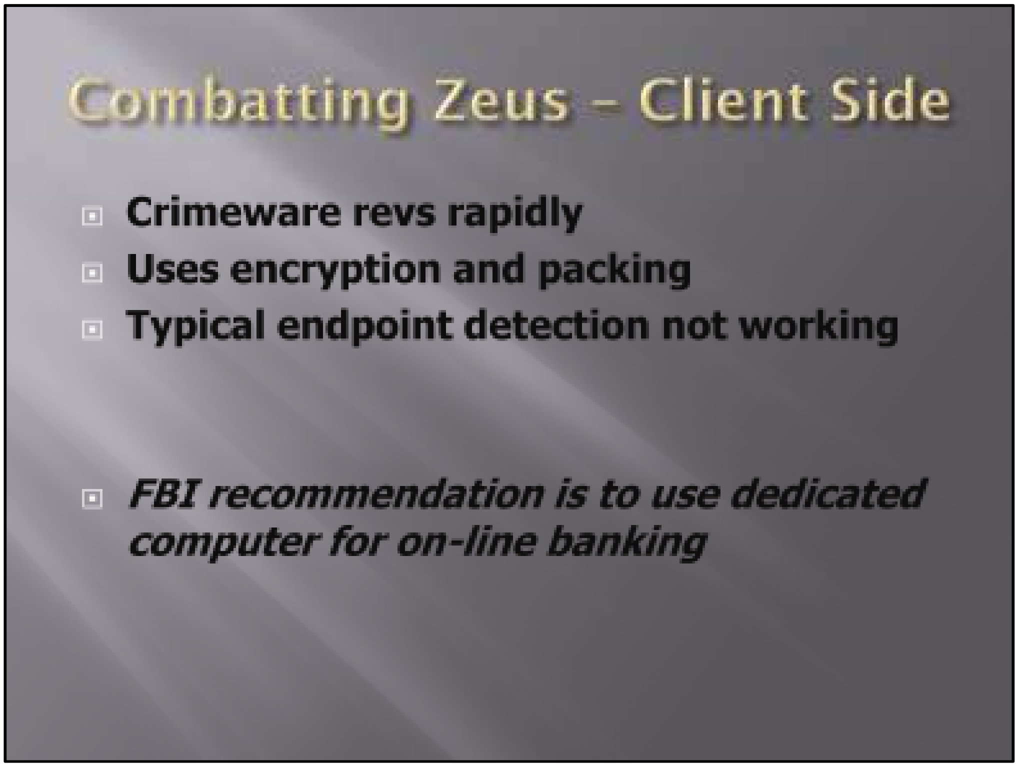
Karen McCarthy, owner of
promotions company, discovere
had been emptied the previous
bank – Cherry Hill, N.J. based T
Feb. 12, unknown thieves had n
individuals and two companies w
business.

Texas Bank Sues Customer Hit by $800,000 Cyber Heist

A machine equipment company in Texas is tussling with its bank after organized crooks swiped more than $800,000 in a 48-hour cyber heist late last year. While many companies similarly victimized over the past year have sued their banks for having inadequate security protection, this case is unusual because the bank is preemptively suing the victim.

Both the victim corporation – Plano based **Hillary Machinery Inc.** – and the bank, Lubbock based **PlainsCapital**, agree on this much: In early November, cyber thieves initiated a series of unauthorized wire transfers totaling $801,495 out of Hillary's account, and PlainsCapital managed to retrieve

http://krebsonsecurity.com/2010/02/n-y-firm-faces-bankruptcy-from-164000-e-banking-loss/
http://krebsonsecurity.com/2010/01/texas-bank-sues-customer-hit-by-800000-cyber-heist/



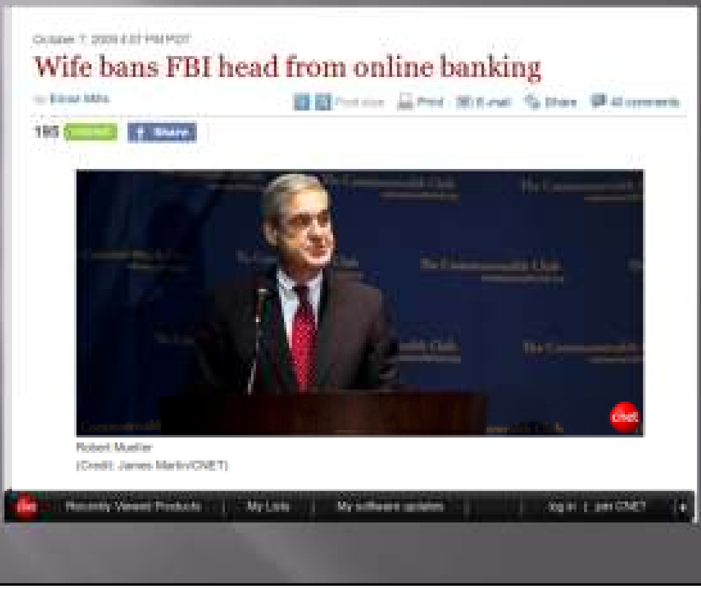
Combatting Zeus – Client Side

- Crimeware revs rapidly
- Uses encryption and packing
- Typical endpoint detection not working

- *FBI recommendation is to use dedicated computer for on-line banking*

http://www.usatoday.com/tech/news/computersecurity/2009-12-30-cybercrime-small-business-online-banking_N.htm

Or Perhaps…



October 7, 2009 4:07 PM PDT

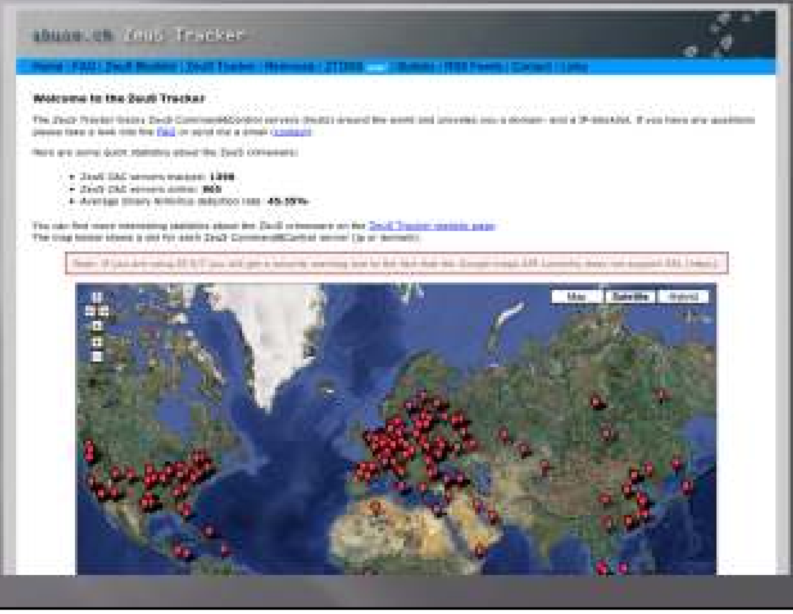
Wife bans FBI head from online banking

by Elinor Mills

Robert Mueller
(Credit: James Martin/CNET)

http://news.cnet.com/8301-27080_3-10370164-245.html

Combatting Zeus – C2 Servers



abuse.ch ZeuS Tracker

Home | FAQ | ZeuS Monitor | ZeuS Tracker | Removal | ZTDNS | ... | Rulesets | RSS Feeds | Contact | Links

Welcome to the ZeuS Tracker

The ZeuS Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have any questions please take a look into the FAQ or send me a email (contact).

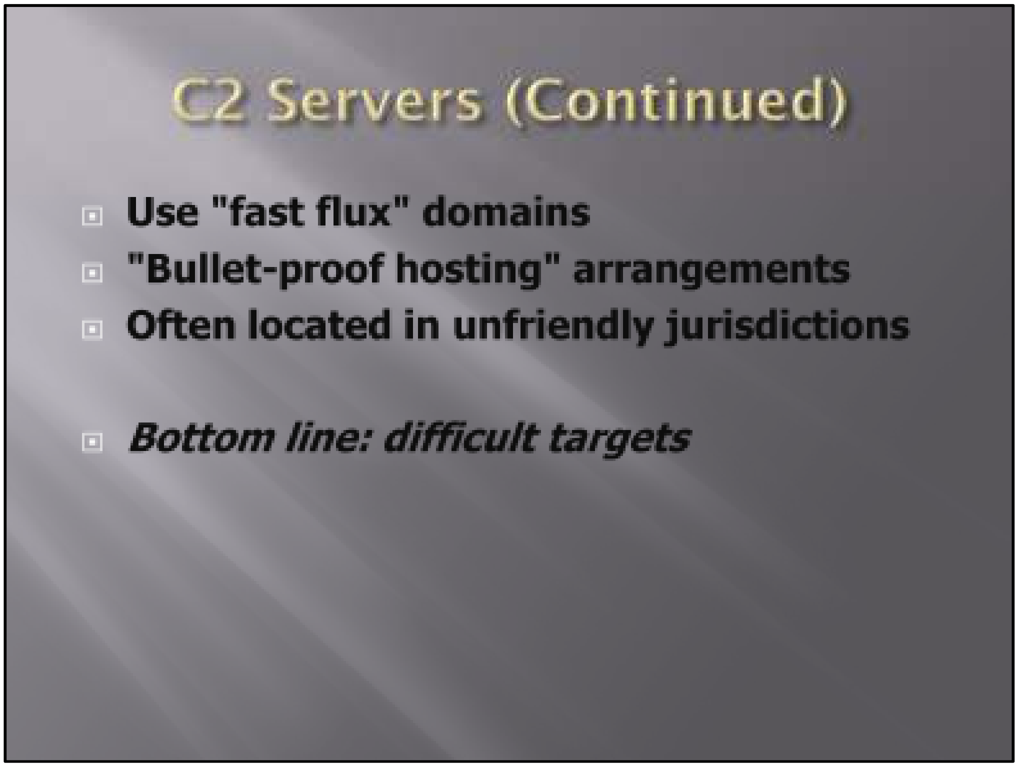
Here are some quick statistics about the ZeuS crimeware:

- ZeuS C&C servers tracked: **1898**
- ZeuS C&C servers online: **865**
- Average binary Antivirus detection rate: **45.35%**

You can find more interesting statistics about the ZeuS crimeware on the ZeuS Tracker statistic page.
The map below shows a dot for each ZeuS Command&Control server (ip or domain).

Note: If you are using IE 6/7 you will get a security warning due to the fact that the Google maps API currently does not support SSL (https).

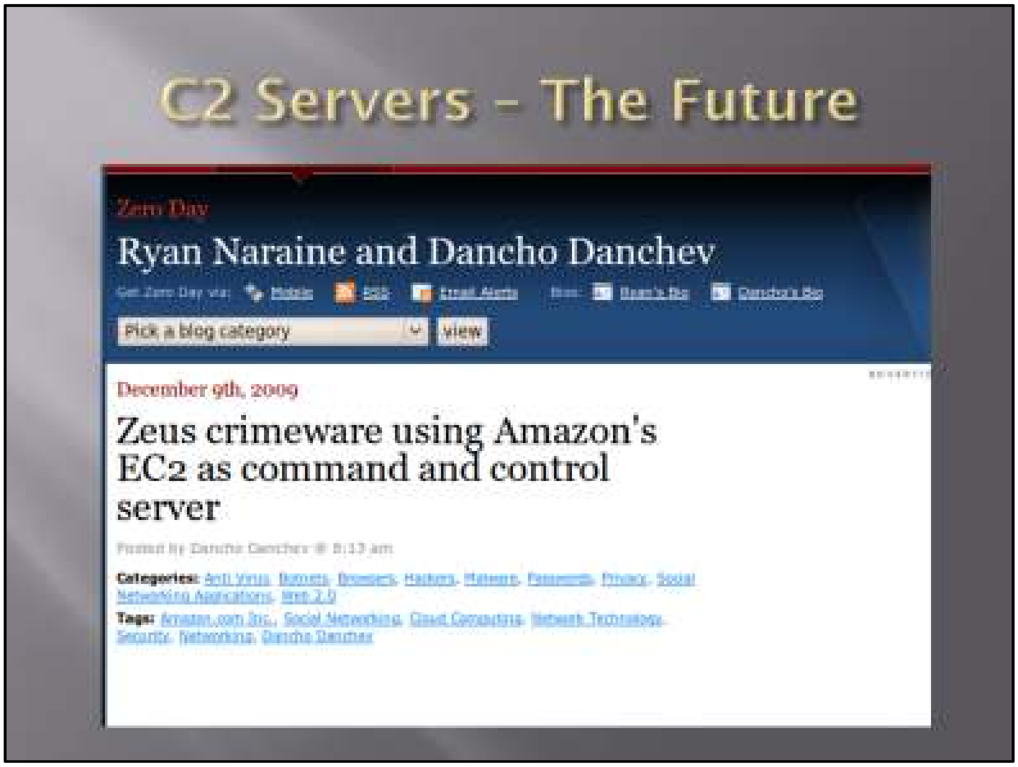
https://zeustracker.abuse.ch/index.php



C2 Servers (Continued)

- Use "fast flux" domains
- "Bullet-proof hosting" arrangements
- Often located in unfriendly jurisdictions

- *Bottom line: difficult targets*



C2 Servers – The Future

Zero Day

Ryan Naraine and Dancho Danchev

Get Zero Day via: Mobile RSS Email Alerts
Bios: Ryan's Bio Dancho's Bio
Pick a blog category
view

December 9th, 2009

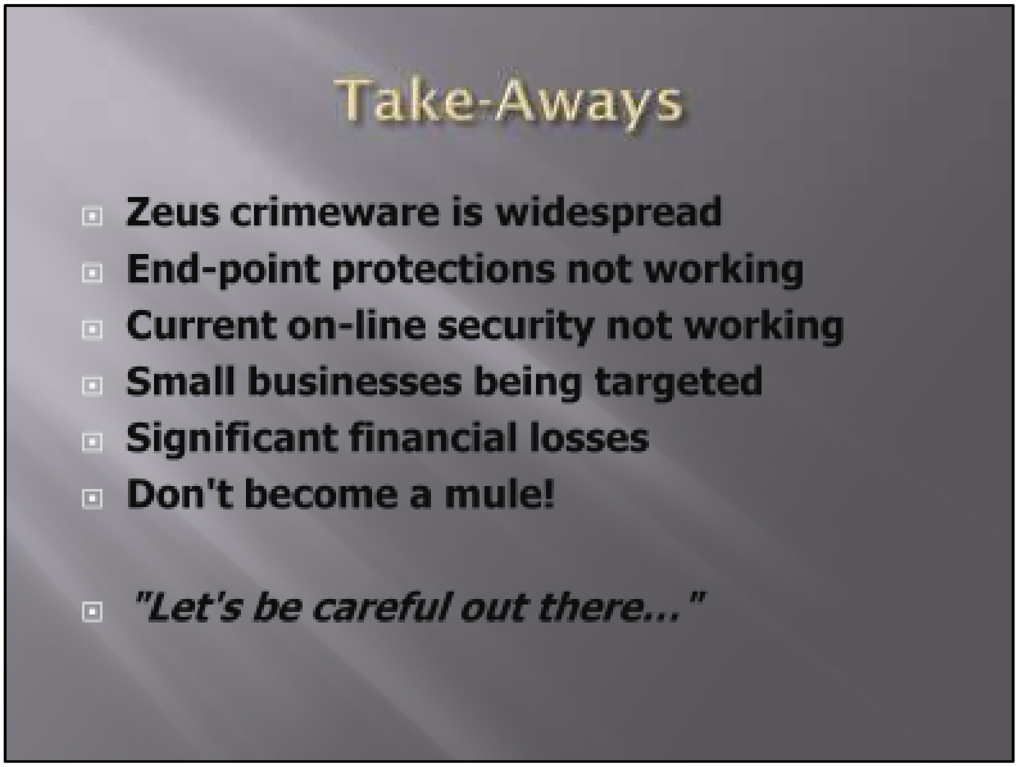
Zeus crimeware using Amazon's EC2 as command and control server

Posted by Dancho Danchev @ 8:13 am

Categories: Anti Virus, Botnets, Browsers, Hackers, Malware, Passwords, Privacy, Social Networking Applications, Web 2.0

Tags: Amazon.com Inc., Social Networking, Cloud Computing, Network Technology, Security, Networking, Dancho Danchev

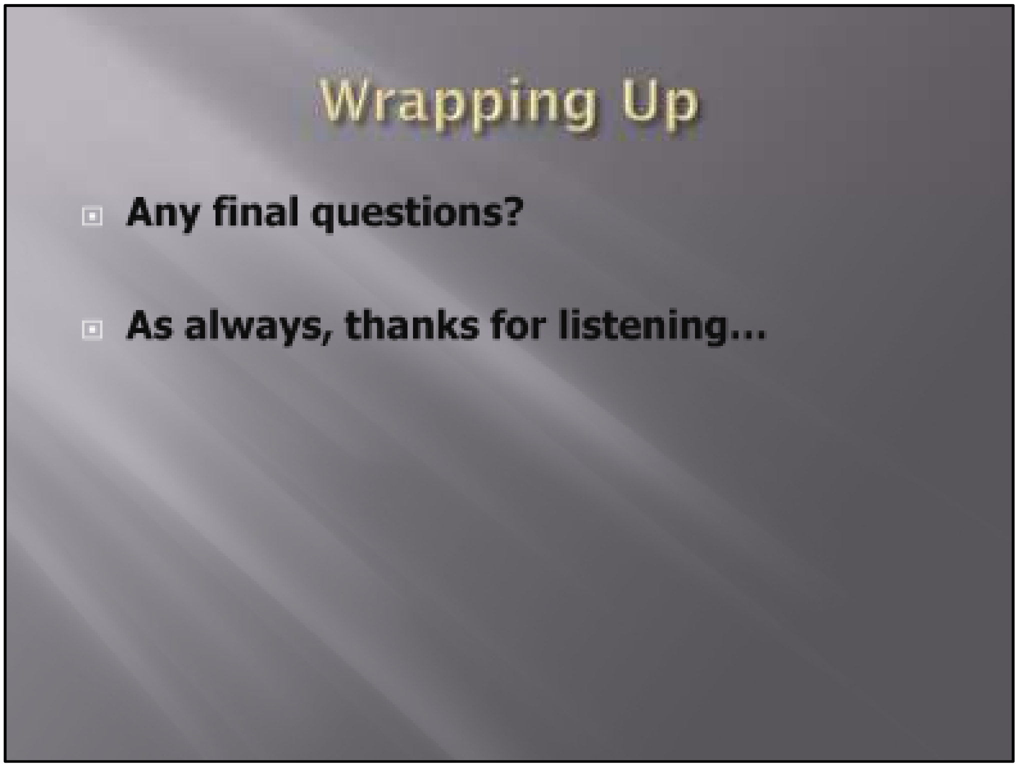
http://blogs.zdnet.com/security/?p=5110



Take-Aways

- Zeus crimeware is widespread
- End-point protections not working
- Current on-line security not working
- Small businesses being targeted
- Significant financial losses
- Don't become a mule!

- *"Let's be careful out there..."*



Wrapping Up

- Any final questions?
- As always, thanks for listening…