

Computer Security at Home

Internet and E-mail

Self-Defense

Office of Information Security
City of Seattle



Roadmap for this Presentation

- Introductions
- Who Are the Bad Guys?
- What Are They After?
- How Do They Do It?
- Self-Defense
- Summary and Discussion



Today You Will Learn...

- The Who, What, Why and How of Attacks Against:
 - Your Computer
 - Your Money
 - Your Privacy
- Techniques and Habits to Protect Yourself and Your Family
- How To Fight Back



Importance of This Workshop

- *To Your Employer*
 - Protecting Secrets and Brand Value; Avoiding Cost of Breach Reporting
- *To You, the Government Employee*
 - You Are The Final Control
- *To You, the Consumer, the Parent*
 - Your Financial Data, Your Family
- *To People Like Me*
 - We'd like to keep our jobs, thanks.



At The End of this Workshop

You Will Be Able To

- Identify Attempts to Deploy Malware Onto Your Home Computer
- Recognize Phishing, Pump-n-Dump, and “419” Scams
- Avoid Signing Yourself and Your Friends Up For Even More SPAM!
- Report Incidents and Save Others!



Handy Definitions

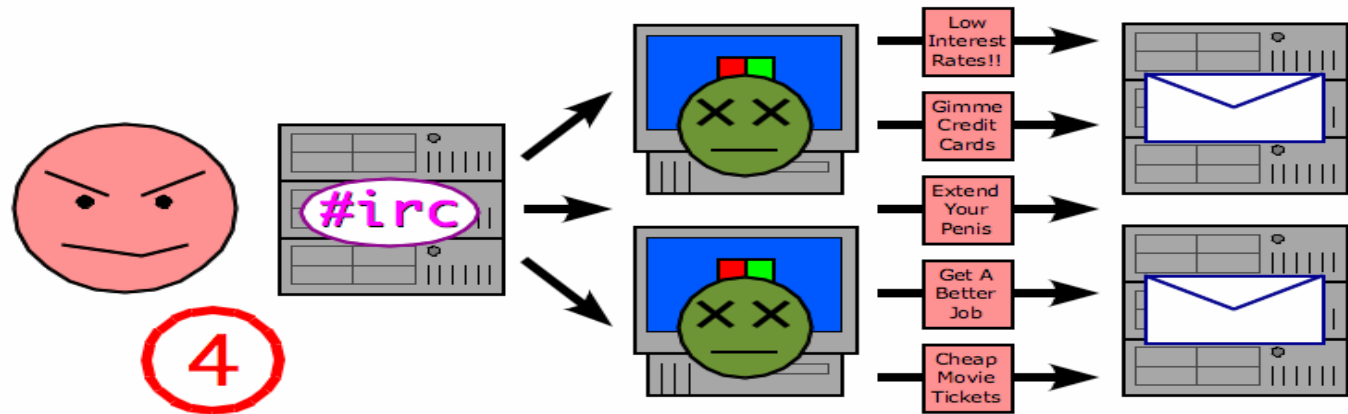
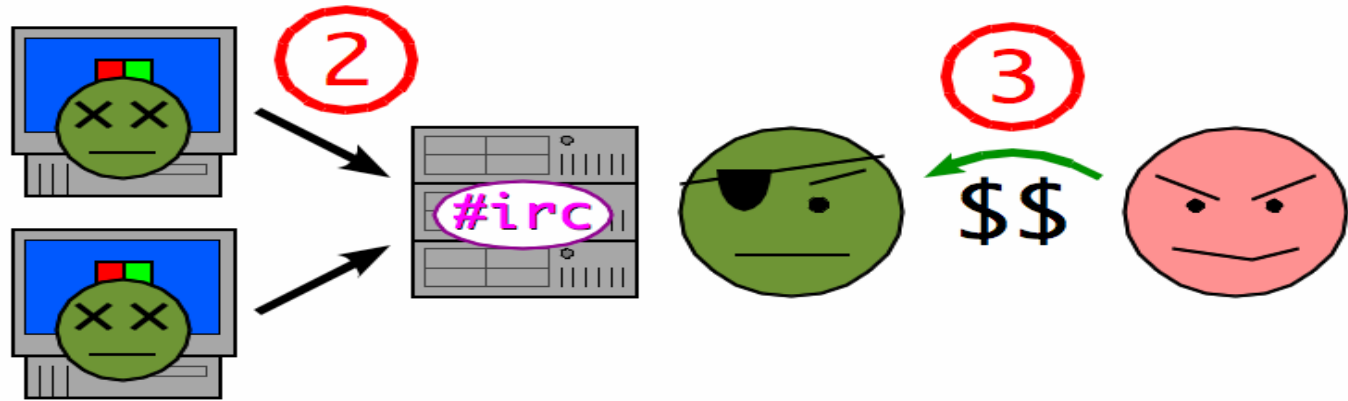
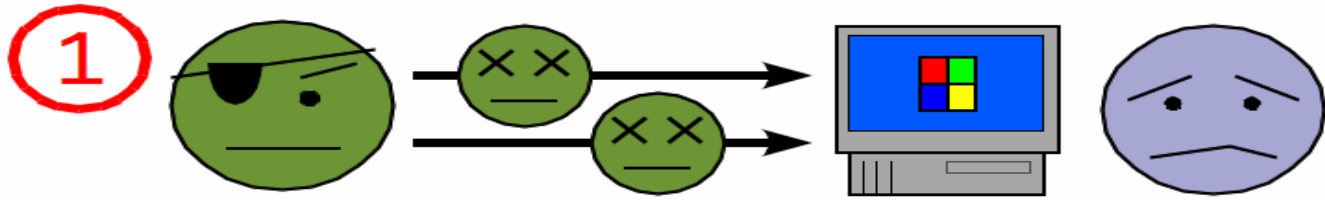
- **Threat** – The danger of attack on a computer system
- **Vulnerability** – Susceptibility to attack
- **Impact** – What bad thing will happen?
- **Risk** – Probability of Threat Multiplied by Potential Impact.



A Few More Definitions

- **Adware** – Generates Advertising Msgs
- **Spyware** – Tracks Online Habits
- **Malware** – General Term
- **Trojan** – Program that Lies in Wait to Perform some Insidious Function
- **Rootkit** – Method of Hiding Malware
- **Botnet** – Collection of Compromised Computers Under Central Command and Control





What's The Motive?

- “Willie Sutton used to say he robbed banks because that’s where the money is. The same applies today to crooks and the Internet.”



Willie Sutton

Keith Lordeau
FBI, Special Agent



Organized Crime and CyberCrime

- This is a BUSINESS
 - Profit Maximization
 - Reduced Risk
 - E-Commerce is a Natural Extension and Gives GLOBAL Market Access
- Home Base in Weak States
 - Safe Haven for International Ops
 - Added Degree of Protection Against Law Enforcement (aka “jurisdictional arbitrage”)
- The Internet is Anonymous
 - Secrecy is Assured



How Big Is The Problem?

- FBI - \$62B in CyberCrime
 - ...but, most crimes are not reported or are not detected
- Gartner - \$2B in Phishing Losses in 12 months
- Symantec – detected 157,477 unique phishing messages – an increase of 81%
- Stolen data is costing US and UK businesses \$150,000 per hour!



Today's Landscape

- Email threats decline while malicious web content grows
- Trojans taking over from spyware
- Malware types differ according to location
 - 30% of all malware is now written in China, most of it taking the form of Trojans used for gaining a backdoor into users' computers.



Annoyances

- Smart Young People
 - Will Always Be a Low-Level Threat
 - 21st Century: Viruses Out, “Botnets” In
 - Mostly Individuals or Small Groups
- Low-Level Organized Crime
 - Constant Threat
 - Partnered with SYP
 - Mostly SPAM Distribution



Real Threats

- Serious Organized Crime
 - Increasing and Very Serious Threat
 - After Your Personal and Financial Information
 - Extortion
 - Well-Funded and Highly Organized Groups
 - Increasingly Using Social Engineering



Who's Not a Threat?

- Industrial Espionage
 - Theft of Intellectual Property
- Terrorists and Nation-States
 - Generally Not a Threat to Home Users
 - Interested in Military and Critical Systems
 - Focused on Intelligence, Disruption
 - Government Networks are a Target



What *Are* They After?

- Your E-Mail Address
- Your Browsing Habits
- Your Computer
- Your Personal and Financial Information
- Your Kids
- Your [City | County | State]



How Do They Do It?

- Vulnerable Computers + Bad Habits = Worms, Trojans and Worse!
- Chain E-Mail, Bogus “Reward” Sites
- Phishing
- Nigerian “419”, European Lottery and Other “Trust” Scams
- Pump-n-Dump Stock Hyping



Today's Vulnerability

- **Secunia Advisory:** SA23769 **Release Date:** 2007-05-08 **Last Update:** 2007-05-11

Critical:

Highly critical **Impact:** System access

Where: From remote

Solution Status: Vendor Patch

Software: [Microsoft Internet Explorer 5.01](#)

[Microsoft Internet Explorer 6.x](#)

[Microsoft Internet Explorer 7.x](#)

Description:

Multiple vulnerabilities have been reported in Internet Explorer, which can be exploited by an attacker to compromise a user's system.



Today's Threat

By Paul Hales: Monday 21 May 2007, 15:56

A NEWER AND DECIDEDLY more dastardly version of the Russian Gozi virus, which uses key stroke logging capabilities to steal bank account details, has been loosed onto the Interweb, insecurity experts have warned.

The program is an updated version of the Gozi Trojan horse program which uses advanced Winsock2 functionality to hack into encrypted SSL (Secure Sockets Layer) streams and send the data back to a server in Russia.



Potential Impacts

- Nuisance: SPAM, Adware, Slow Computer
- Cost: Computer Cleaning Software, Technician Time, New Disk (or Computer!)
- Disclosure of Passwords and/or Financial or Personally Identifiable Information => Fraud
- Loss of Privacy; Threat to Safety



Be Informed

- Know What's Happening IN GENERAL:
 - Computer Security web sites
 - Computer Magazines
 - Software websites (Microsoft, Adobe)
 - Government sites (FCC, NIST, DHS, FBI)
 - Children's Safety sites
 - Classes like this one!



Be Aware

- Know What's Happening TODAY!
 - Phishing, Nigerian 419 scams, Trojan du jour, social engineering, e-mail address harvesting
 - Learn to Recognize Attacks in Progress
 - Learn Reporting Organizations and Use Them
- Educate Your Kids
 - MySpace and Other Online Communities
 - Teach Suspicion



Be Suspicious

- If you get an email that seems too good to be true – it is!
- Be very cautious about unexpected email, especially if it has an attachment
- Don't follow links that you aren't sure about – or surf dangerous sites
- Don't open executable attachments (.exe, .com, .scr) or any attachment you weren't expecting (even if it's from a friend)



Be Alert

- Know the types of activities to avoid
- Check for the lock symbol if you are disclosing confidential information
- Know what your kids are doing online – make rules
- Watch for symptoms
 - Computer slow to start
 - Applications run slowly or lock up
 - Computer runs slow or won't shut down



Be Prepared

Reduce Your “Attack Surface”

- Use Throwaway E-Mail Account Information When Posting Publicly
- Hold Information Tightly
- Use “Tiered” Passwords on Websites and *change them regularly!*



Examples



E-Mail Scams

- You have received a card from an admirer!
- Yassar Arafat's Wife: Nigerian 419 scams
- You have won the EU Lottery!
- Little Girl Saved: Six Degrees of Separation
- Become an EBay Powerseller!
- Your card was used in Bulgaria
- Saddam Hussein Found Alive!



Example: Pump-n-Dump

- Carnegie Cooke & Company, Inc. (CGKY)
A Huge PR campaign is expected starting Wednesday and all next week so grab as much as you can up to \$0.25 range.
- Infinex Ventures Inc. (IFNX) = OTC: IFNX.OB
This One is Strong UP 0.50 (28.57%) Jan 9th Alone
Huge PR Campaign Running for Tuesday Jan 10th
We expect explosive growth thru Friday



Examples: Bogus “Polls”



National Opinion Poll ConsumerSavingCenter.com

Do you like President Bush?

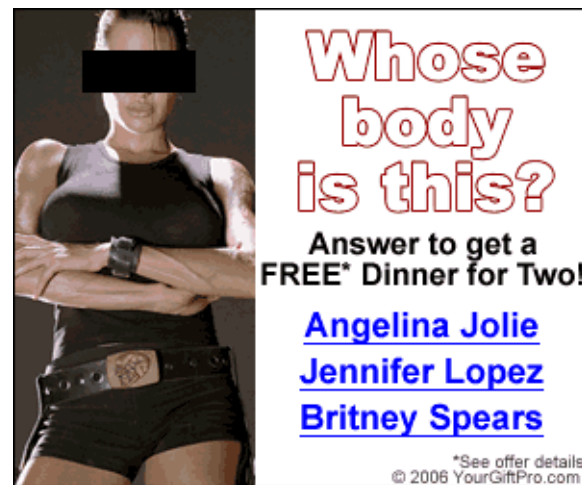
Answer and get a FREE* Laptop!

*see details



Fun quiz for fun moms

GO



Whose body is this?

Answer to get a FREE* Dinner for Two!

[Angelina Jolie](#)
[Jennifer Lopez](#)
[Britney Spears](#)

*See offer details.
© 2006 YourGiftPro.com



Examples: 419 Scam

Dearest,

How are you today? It is my pleasure to contact you for a business venture which I and my junior sister (Sandra) intend to establish in your country. Though I have not met with you before but I believe, one has to risk confiding in succeed sometimes in life. There is this huge amount of eight million U.S dollars(\$8,000,000.00) which my late Father kept for us with a Fiduciary Fund Holder in Abidjan before his sudden death during this war in Cote d'ivoire.

Now I and my sister have decided to invest these money in your country or anywhere safe enough outside Africa for security and political reasons. We want you to help us claim and retrieve these fund from the Fiduciary Fund Holders and transfer it into your personal account in your country for investment purposes.

If you can be of an assistance to us we will be pleased to offer to you 15% Of the total fund. You can call me on this line for more detail: [*real #*].

I await your soonest response.



Hostile or “Poisoned” Websites

- Can Exploit Vulnerabilities on Your Computer Without Your Knowledge
- Usually Deploy Adware and Spyware
- Russian (and other) Kits Available to Equip Websites with Deployment Functionality: \$999.00
- 285,000,000 clicks to hostile websites every month (5 search engines studied)
- Newer Payloads are Keystroke Loggers



Example: Drive-By Download



LyricsDomain

Discover the songs you love...

Tell a Friend!

Browse: [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Y] [Z] [#]

- Lyrics Search
- Add Lyrics
- New Lyrics
- Request Lyrics
- Screen Savers
- Contact
- Webmasters
- Cheap Hosting
- Sick T-shirts

Partner sites

- Absolute Lyric
- @Lyrics
- Lyrics XP
- Lyrics Planet

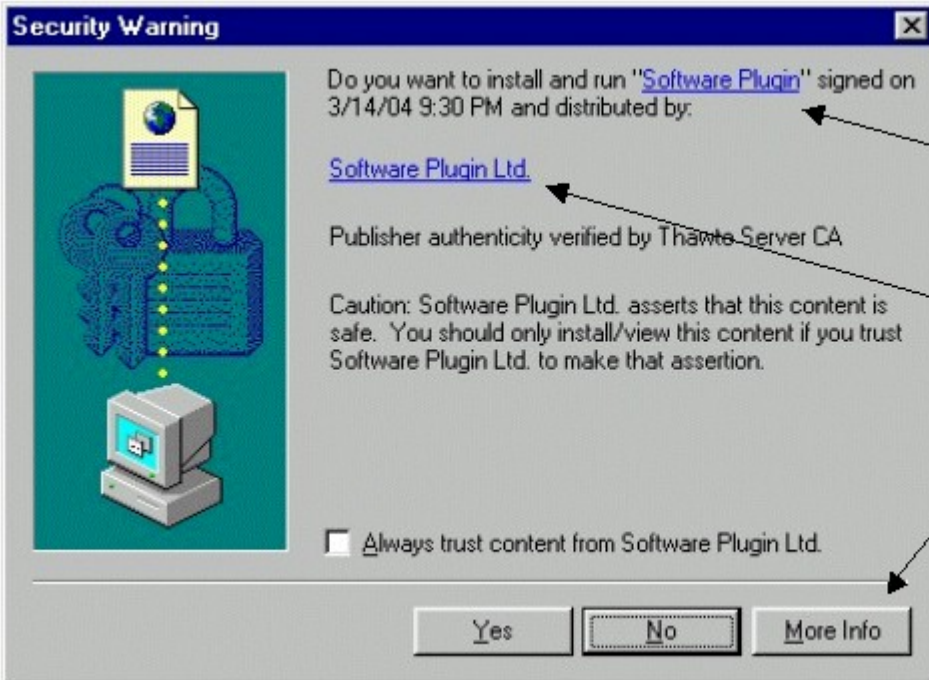
Song Lyrics Domain - Welcome!

Everyday we hear songs... new songs... you don't want to miss a single word... our site: helping you discover the songs you love.

Site News

March 14, 2004

NORAH JONES LYRICS: "Sunrise", "Thing", "Don't Miss You At All", "KE Harder The Fall)", "All I Need To Know", "Midnight And Daylight", "Paris, Tennessee", "I Will Stand", "Steamy Windows", "Lonely, Needin' Lovin'", "When I'm Good", "Everywhere We Go", "Calif Feel That Way Again", "Live Those Goes Down", "The Woman With You", "I Think About Leaving" and more.



Link to more information

Link to digital certificate

Help for digital certificates



Example: Phishing

Subject: Your Checking Account at Citibank.



Dear Citibank customer,

We are letting you know, that you, as a Citibank checking account holder, must become acquainted with our new Terms & Conditions and agree to it.

Please, carefully read all the parts of our new Terms & Conditions and post your consent.

Otherwise, we will have to suspend your Citibank checking account.

This measure is to prevent misunderstanding between us and our valued customers.

We are sorry for any inconvenience it may cause.

[Click here to access our Terms & Conditions page and not allow your Citibank checking account suspension.](#)

© 2003 Citibank. Citibank (West), FSB. Member FDIC. Citibank with Arc Design is a registered service mark of Citicorp.




Citi.com

A member of  Citigroup
[Citigroup Privacy Promise](#)
[Terms & Conditions](#)
Copyright © 2003 Citicorp

Password Management: Financial Sites

- Use ***at least*** 8 characters
- Think of a “Pass Phrase”
- Use mix of numbers, letters (upper and lower case) and non-alphanumeric characters: \$ # @ ! * &

Example: The pass phrase, “I hate to be late” would look like: lh82BL8!



Password Management: Occasional Shopping Sites

- On First Login, Set up a Password So Complex You Will Never Remember
- Each Time You Return, Have Your Password E-Mailed To You
- On Login, Change it to Something You Will Never Remember



Password Management: E-Mail Sites

- Lower Risk than Financial or Shopping
- Substitute 2-3 Numbers for Letters
Inserted Into a Word: N0v3mb3r
- Change Routinely



Technical Controls

- Anti-Virus
- Personal Firewall
- Hardware Firewall
- Spyware Sweeper
- Automatic Updates



Striking Back

- ***NEVER*** Contact Scammers
- Report Phishing Immediately; For Example phishing@paypal.com
- Also use abuse@....
- Teach Your Aunt to Forward Stories Using BCC:
- Routinely Review Your Credit Records



Summary

- Bad People Want Your Money
- They Get it Using a Combination of Computer Vulnerability, Exploit Delivery, and Bad User Choices
- The Problem is Getting Worse
- Your Awareness and Behaviour Is The Best Control
- Avoid Sketchy Websites; Treat All E-Mail with Suspicion
- Educate Yourself and Fight Back!

