Cyber Crime and Payment Fraud Trends

Key Threats to All Businesses

CliftonLarsonAllen

CLAconnect.com

What do the following have in common?

- Catholic church parish
- Hospice
- Collection agency
- Main Street newspaper stand
- Electrical contractor
- Health care trade association
- Rural hospital
- Mining company

- On and on and on and on…….

Three Reasons Why We Should Care

- Organized Crime
  - Wholesale theft of personal financial information
- Payment Fraud – Corporate Account Takeover
  - Use of online credentials for ACH, CC and wire fraud
- Hackers are targeting you!
  - WSJ front page: “Hackers Turn to Small Business”

The Cost?

Norton/Symantec Corp:

- Cost of global cybercrime: $388 billion

- Global black market in marijuana, cocaine and heroin combined: $288 billion

- Hackers are lazy - go for the “easy money”
- Bank customers are much easier targets than the banks themselves

Banks vs. Customers – In the Courts

Bank Sues Customer

- **$800,000** fraudulent ACH transfer - Bank retrieves $600,000 = $200,000 lost
- Both bank and customer have responsibilities, who is at fault?

Customer Sues Bank

- **$560,000** fraudulent ACH transfer
- ***Funds wired to*** **accounts in Russia, Estonia,** ***Scotland, Finland, China*** and the US and were withdrawn soon after deposits were made.
- Multiple wires = unusual activity so bank notifies client, but how quickly and what actions were taken to prevent additional fraud?
- What are the bank's obligations versus the client's?
- *U*pdated regulatory guidance should improve consistency of controls.

Court Cases Will Eventually Set Standard - Both parties accountable for risks

Network Security – Doing Business Safely

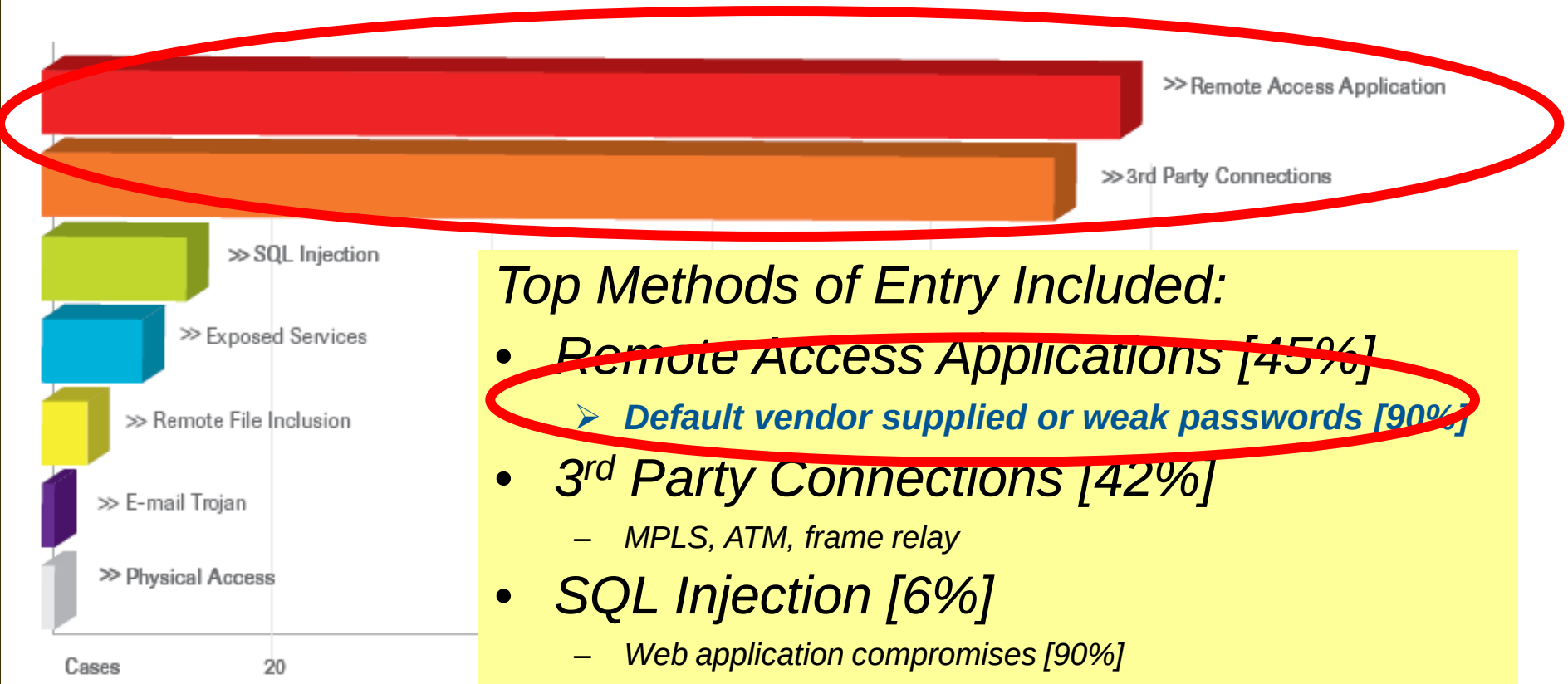
- Emerging & Continuing Trends
  - Intrusion Analysis Reports
  - "Blocking and Tackling"
- Common attack vectors
- 10 Key defensive measures

Two Security Threat Reports

- Intrusion Analysis: TrustWave
  - January 2010 and April 2011
  - https://www.trustwave.com/GSR
- Intrusion Analysis: Verizon Business Services
  - July 2010 and April 2011
  - http://securityblog.verizonbusiness.com/2011/04/19/2011-data-breach-investigations-report-released/

TrustWave – Intrusion Analysis Report

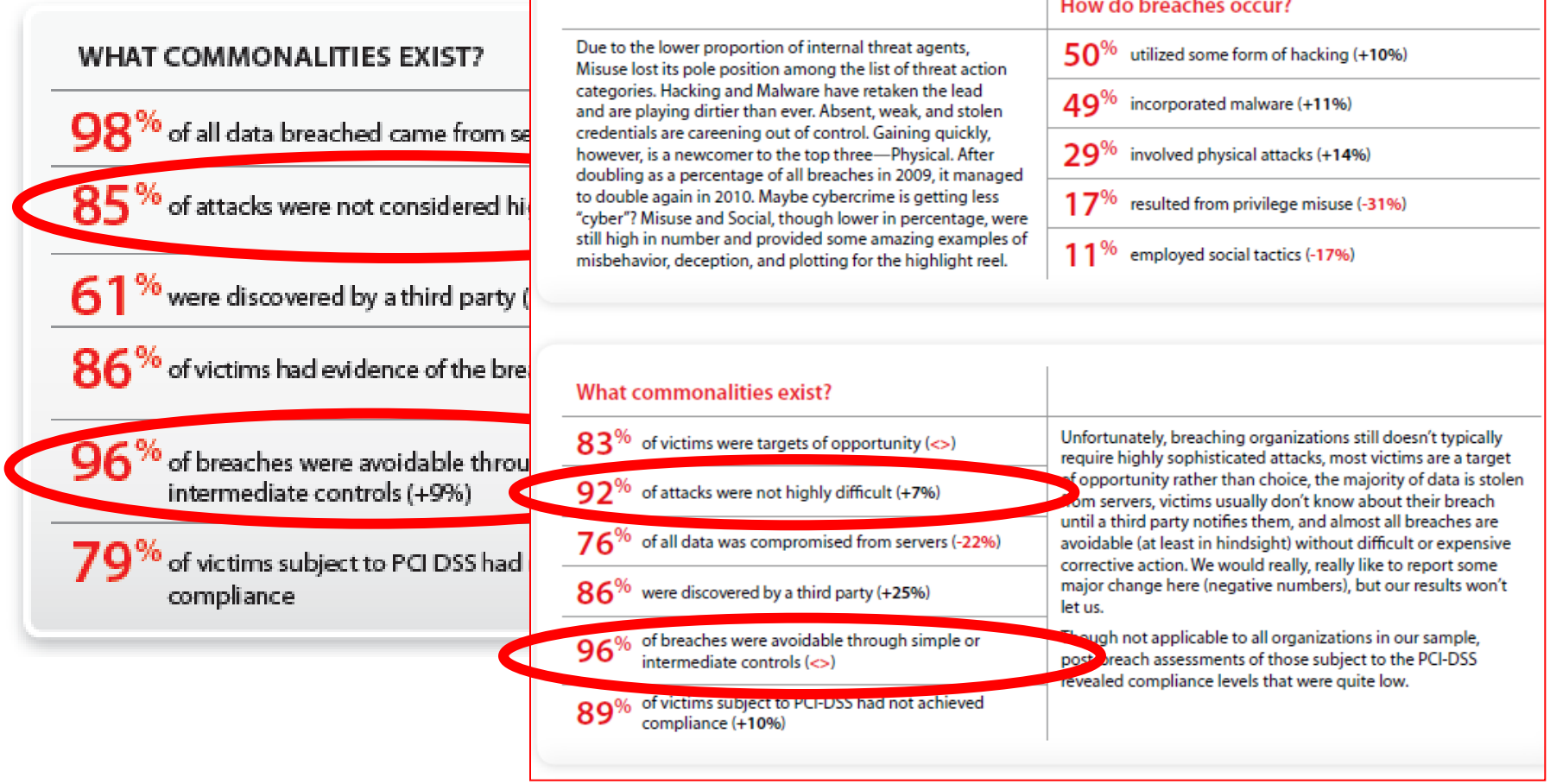
Top Methods of Entry Included:



Top Methods of Entry Included:

- *Remote Access Applications [45%]*
  - ***Default vendor supplied or weak passwords [90%]***
- *3rd Party Connections [42%]*
  - *MPLS, ATM, frame relay*
- *SQL Injection [6%]*
  - *Web application compromises [90%]*
- *Exposed Services [4%]*

Verizon Data Breach Analysis



WHAT COMMONALITIES EXIST?

98% of all data breached came from se

85% of attacks were not considered hi

61% were discovered by a third party (

86% of victims had evidence of the bre

96% of breaches were avoidable throu intermediate controls (+9%)

79% of victims subject to PCI DSS had compliance

How do breaches occur?

Due to the lower proportion of internal threat agents, Misuse lost its pole position among the list of threat action categories. Hacking and Malware have retaken the lead and are playing dirtier than ever. Absent, weak, and stolen credentials are careening out of control. Gaining quickly, however, is a newcomer to the top three—Physical. After doubling as a percentage of all breaches in 2009, it managed to double again in 2010. Maybe cybercrime is getting less "cyber"? Misuse and Social, though lower in percentage, were still high in number and provided some amazing examples of misbehavior, deception, and plotting for the highlight reel.

50% utilized some form of hacking (+10%)

49% incorporated malware (+11%)

29% involved physical attacks (+14%)

17% resulted from privilege misuse (-31%)

11% employed social tactics (-17%)

What commonalities exist?

83% of victims were targets of opportunity (<>)

92% of attacks were not highly difficult (+7%)

76% of all data was compromised from servers (-22%)

86% were discovered by a third party (+25%)

96% of breaches were avoidable through simple or intermediate controls (<>)

89% of victims subject to PCI-DSS had not achieved compliance (+10%)

Unfortunately, breaching organizations still doesn't typically require highly sophisticated attacks, most victims are a target of opportunity rather than choice, the majority of data is stolen from servers, victims usually don't know about their breach until a third party notifies them, and almost all breaches are avoidable (at least in hindsight) without difficult or expensive corrective action. We would really, really like to report some major change here (negative numbers), but our results won't let us.

Though not applicable to all organizations in our sample, post-breach assessments of those subject to the PCI-DSS revealed compliance levels that were quite low.

Hackers, Fraudsters, and Victims

- Opportunistic Attacks

- Targeted Attacks

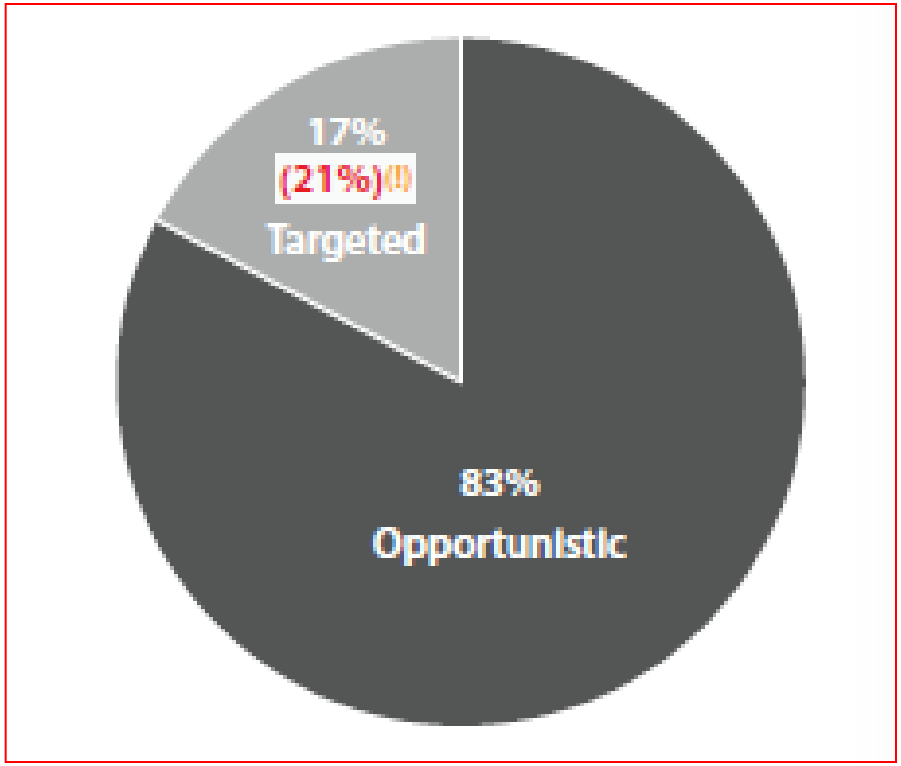


Table 6. Types of external agents by percent of breaches within External

Organized criminal group	58%
Unaffiliated person(s)	40%
Former employee (no longer had access)	2%
Competitor	1%
Unknown	14%
Other	<1%

How do hackers and fraudsters break in?

- Social Engineering
- Email Phishing
  - "Spear Phishing"
- On-line banking trojans

The Fine Art of "People Hacking"

"Amateurs hack systems, professionals hack people."

Bruce Schneier

- Social Engineering uses non-technical attacks to gain information or access to technical systems
  - Pre-text telephone calls
  - Building penetration
    - Seeding
  - Email attacks

Pre-text Phone Calls

- "Hi, this is Randy from Comcast. I am working with Mike, and I need your help…"
  - Name dropping
  - Establish a rapport
  - Ask for help
  - Inject some techno-babble
  - **People want to avoid inconvenience**
  - **Timing, timing, timing…**

Physical (Facility) Security

Compromise the site:

- "Hi, Joe said he would let you know I was coming to fix the printers…"

Plant devices:

- Keystroke loggers
- Wireless access point
- Thumb drives ("Switch Blade")

Examples…
Steal hardware (laptops)

http://www.sptimes.com/2007/10/28/Business/Here_s_how_a_slick_la.shtml
http://www.privacyrights.org/ar/ChronDataBreaches.htm

Risk Assessment Theory

- Inherent Risk – Likelihood vs Impact
- Control Risk
- Total Risk

IR X CR = TR

Spear Phishing

"Second Generation" phishing

Goal is to "root the network"

Install malware

- Log system activity to harvest passwords
- Use automated tools to execute fraudulent payments

Trick users into supplying credentials (passwords)

SANS – Client Side Vulnerabilities

- Client side vulnerabilities
  - Missing operating system patches
  - Missing application patches
    - Apple QuickTime
    - Java Vulnerabilities
    - MS Office Applications
    - Adobe Vulnerabilities (PDF, Flash, etc…)
- Objective is to get the users to “Open the door”

Spear Phishing Success Factors

- With so much money at stake hackers are putting in more effort to increase the likelihood that the emailed link will be followed:
  - "Spoof" the email to appear that it comes from someone in authority
  - Create a customized text that combines with the spoofing to create pressure to act quickly (without thinking)

FW: Microsoft Security Update - Message (HTML)

File Edit View Insert Format PGP Tools Actions Help

Fr: **Randall J. Romes [rromes@larsonallen.com]**

To: 'rromes'

Cc:

Su:

Microsoft has provided an update this morning that needs to be applied to all PCs as soon as possible. This needs to be installed on ou

Thanks,

Randall J. Romes

From: Microsoft Security Info [mailto:security@microsoft.com]
Sent: Tuesday, February 19, 2008 8:57 AM
To: Romes, Randall J.
Subject: Strong Password Checking Tool

Two or Three tell-tale signs
Can you find them?

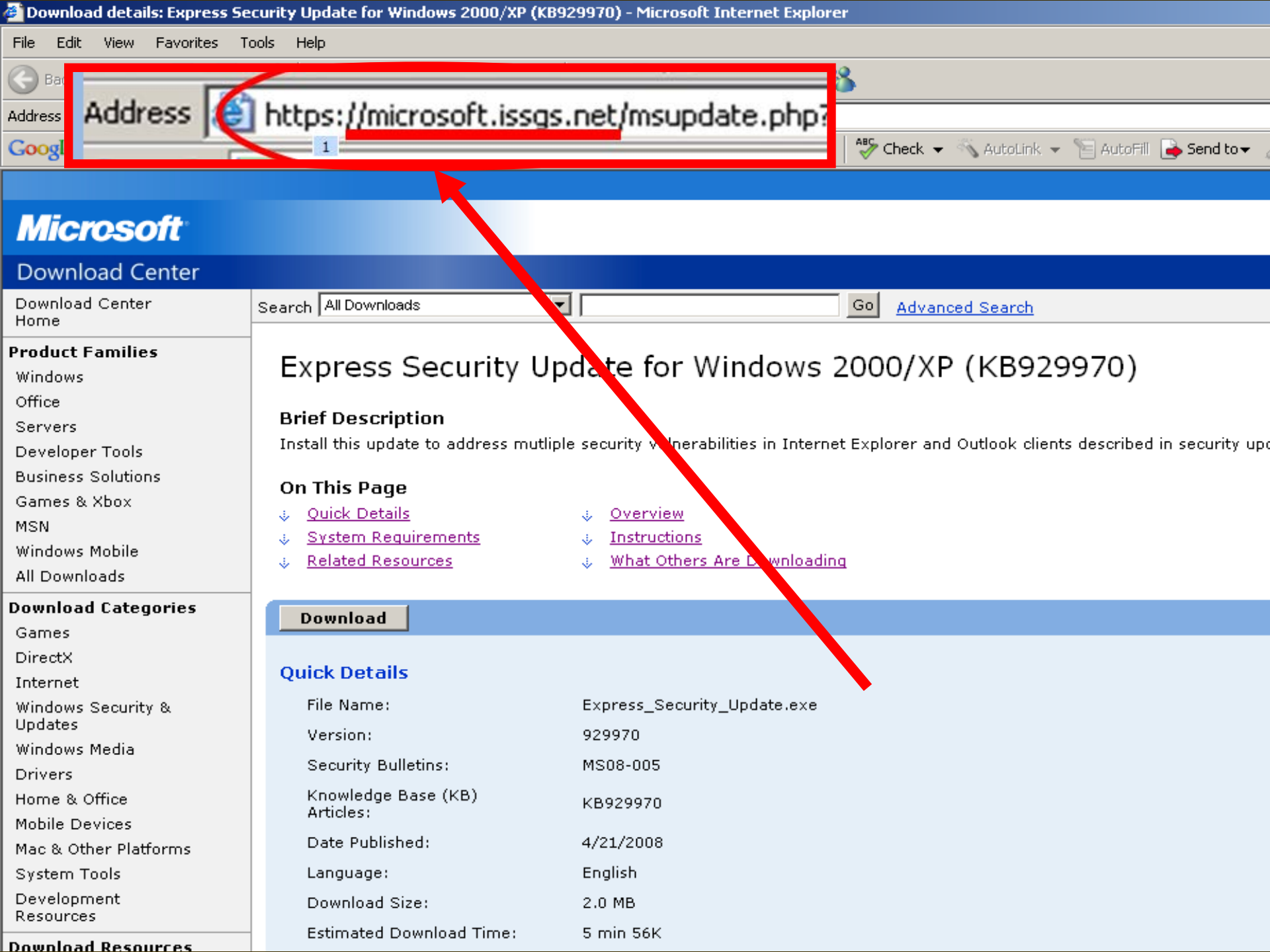
Greetings,

A recent group of viruses have been released which put systems at risk. These viruses exploit vulnerabilities in Internet Explorer an personal information. The viruses targeting Microsoft Outlook are particularly dangerous because they only require the recipient to

Anyone running Microsoft Windows 2000 or XP should download the following patch and install it immediately, to patch the vuln

1. Click on this link https://microsoft.isgs.net/msu[illegible]4uY29tCg==

3. A dialog box will pop up (you may need pop-ups enabled). Start the installation immediately by clicking the "Run" button. The i


Download details: Express Security Update for Windows 2000/XP (KB929970) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
https://microsoft.issqs.net/msupdate.php?
Check AutoLink AutoFill Send to
Microsoft
Download Center
Download Center Home
Product Families
Windows
Office
Servers
Developer Tools
Business Solutions
Games & Xbox
MSN
Windows Mobile
All Downloads
Download Categories
Games
DirectX
Internet
Windows Security & Updates
Windows Media
Drivers
Home & Office
Mobile Devices
Mac & Other Platforms
System Tools
Development Resources
Search All Downloads Go Advanced Search
Express Security Update for Windows 2000/XP (KB929970)
Brief Description
Install this update to address mutliple security vulnerabilities in Internet Explorer and Outlook clients described in security upd
On This Page
Quick Details
System Requirements
Related Resources
Overview
Instructions
What Others Are Downloading
Download
Quick Details
File Name: Express_Security_Update.exe
Version: 929970
Security Bulletins: MS08-005
Knowledge Base (KB) Articles: KB929970
Date Published: 4/21/2008
Language: English
Download Size: 2.0 MB
Estimated Download Time: 5 min 56K

Zues, Citadel, Gozi, Spyeye, Sinowal…

- **$72 million** stolen by international cybercrime gang
- Install back doors or use “Man-in-the-Browser” attack
- Bypass tokens and secret questions
- Display expected info to user – conduct fraud in background
- Intelligent malware and criminals avoid triggering detection

Money Mules

- “Work at Home”
- Re-shipper, insurance settlements processing, etc.
- Sometimes mule is co-conspirator, sometimes victim
- Move money out of the country without triggering alerts

Multi-Factor Authentication Solutions

- MFA is critical

- Silver bullet?

10 Key Defensive Measures

Training Your Employees is Critical

(but not easy)

CliftonLarsonAllen

CLAconnect.com

Strategies

Our information security strategy should have the following objectives:

- Users who are more aware and savvy
- Networks that are resistant to malware
- Relationship with our banks is maximized

Ten Keys to Mitigate Risk

1. **Strong Policies -**

   - Email use
   - Website links
   - Removable media
   - **Users vs Admin**
   - **Insurance**

Ten Keys to Mitigate Risk

2. Defined user access roles and permissions

- Principal of minimum access and least privilege
- **Users should NOT have system administrator rights**
  - **"Local Admin" in Windows should be removed (if practical)**

Ten Keys to Mitigate Risk

3. **Hardened internal systems (end points)**
   - Hardening checklists
   - Turn off unneeded services
   - **Change default password**
   - **Use Strong Passwords (see tip next slide)**
4. **Encryption strategy – data centered**
   - Email
   - Laptops and desktops
   - Thumb drives
   - **Email enabled cell phones**
   - Mobile media

Tip: Build a password from a phrase.

I like to eat Oreo cookies
at night.

ilteocan

or, even better:

Il2eOc@n

Ten Keys to Mitigate Risk

5. Vulnerability management process

- Operating system patches
- **Application patches**
- Testing to validate effectiveness –
  - "belt and suspenders"

Ten Keys to Mitigate Risk

6. **Well defined perimeter security layers:**
   - **Network segments**
   - Email gateway/filter
   - Firewall – “Proxy” integration for traffic in AND out
   - Intrusion Detection/Prevention for network traffic, Internet facing hosts, AND workstations (end points)
7. **Centralized audit logging, analysis, and automated alerting capabilities**
   - Routing infrastructure
   - Network authentication
   - Servers
   - Applications

Ten Keys to Mitigate Risk

8. Defined incident response plan and procedures

- **Be prepared**
- Including data leakage prevention and monitoring
- Forensic preparedness

Ten Keys to Mitigate Risk

9. Know / use Bank Tools

- Multi-factor authentication
- Dual control / verification
- Out of band verification / call back thresholds
- ACH positive pay
- ACH blocks and filters
- Review bank contracts relative to all these
- Monitor account activity ***daily***
- **Isolate the PC used for wires/ACH**

Ten Keys to Mitigate Risk

10. Test, Test, Test
    - "Belt and suspenders" approach
    - Penetration testing
        - Internal and external
    - Social engineering testing
        - Simulate spear phishing
    - Application testing
        - Test the tools with your bank
        - Test internal processes

Questions?

Hang on, it's going to be a wild ride!!

Mark Eich, Principal

Information Security Services Group

mark.eich@claconnect.com

***

(612)397-3128