Protecting Your Business from Phishing and Internet Attacks

Senior Security Consultant ISS

INTERNET | SECURITY | SYSTEMS®

Agenda

- ***Overview of Phishing***
- ***Best Practices for Policy & Education***
- ***Internet Attacks***
- ***Technology Solutions***

INTERNET | SECURITY | SYSTEMS®

What is Phishing?

- (v) phish-ing (a.k.a. brand spoofing) - creating a replica of an existing Web page and sending a fake email to fool a user into sharing personal, financial or password data.

- It’s an identity theft attack that attempts to steal sensitive information using social engineering.

- The term phishing comes from the fact that Internet scammers are using sophisticated lures as they "fish" for users' financial information and password data.

INTERNET | SECURITY | SYSTEMS®

Is Phishing a Serious Threat?

"[Phishing is the] hottest & most troubling, new scam on the Internet."

Jana Monroe, FBI (July '03)

INTERNET | SECURITY | SYSTEMS®

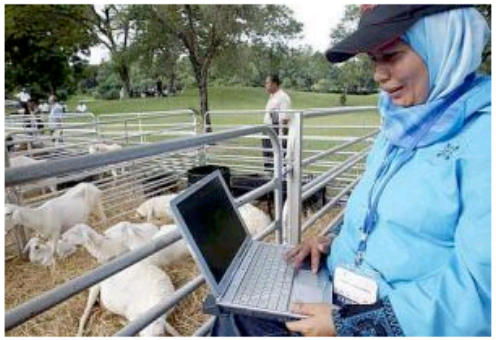
Thursday October 7, 2004

Rearing goats helps Basniar overcome major setback

BY ZANI SALLEH

KUALA LUMPUR: Six years ago, a woman suffered a big setback when her clothes shop in Sungai Besar near Sekinchan burnt down.

But she has turned the disastrous incident into an opportunity for success by rearing goats instead.



KEEPING UP TO DATE: Basniar using her laptop computer while her goats are on display at the exhibition in Kuala Lumpur Wednesday.

Today, Basniar Masni, 37, has a thriving family business selling goats and sheep to farms, markets and butchers throughout the country.

Armed with RM40,000, she started with 14 goats, and is now rearing no fewer than eight types of goats, including *kibas* from the Middle East, the Indian-breed *Jannapari*, sheep and the local *kampung* goat on a 1.2ha farm.

She said her success came through hard work and perseverance.

"It is a 24-hour job, just like raising children, where full commitment is needed," she said at the Malaysian Agriculture, Horticulture and

Is Phishing a Serious Threat?

"Identity theft undermines the basic trust on which our economy depends."

President Bush (July '04, while signing ITPEA)
Identity Theft Penalty Enhancement Act,

INTERNET | SECURITY | SYSTEMS®

Identity Theft Penalty Enhancement Act

It says that anyone who, while engaged in any of a long list of crimes, knowingly "transfers, possesses, or uses, without lawful authority" someone else's identification will be sentenced to an extra prison term of two years with no possibility of probation. Committing identity fraud while engaged in *certain major crimes* sometimes associated with terrorism--such as aircraft destruction, arson, airport violence or kidnapping top government officials--gets an automatic extra five years.

INTERNET | SECURITY | SYSTEMS®

Is Phishing a Serious Threat?

95% of phishing exploits reported originate from forged addresses.

5 New phishing exploits are reported every month.

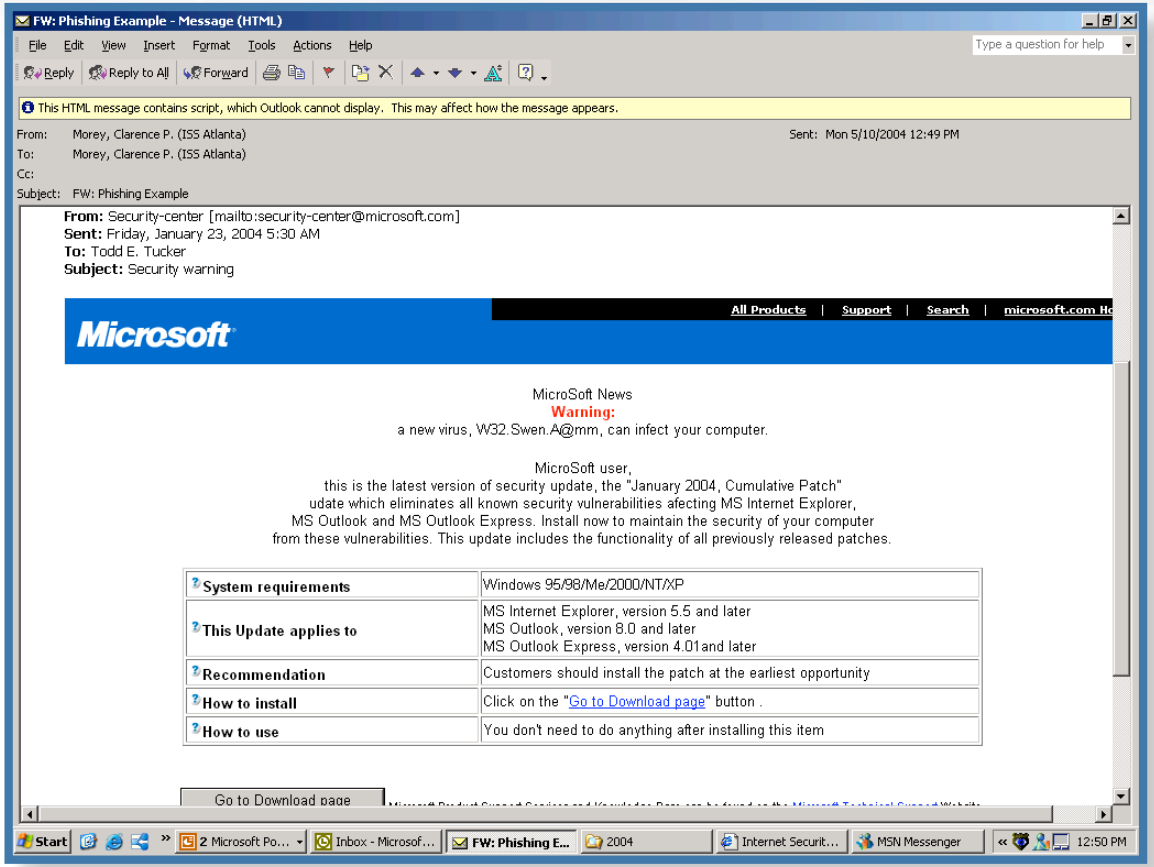
5% of all recipients actually respond to phishing exploits.

INTERNET | SECURITY | SYSTEMS®

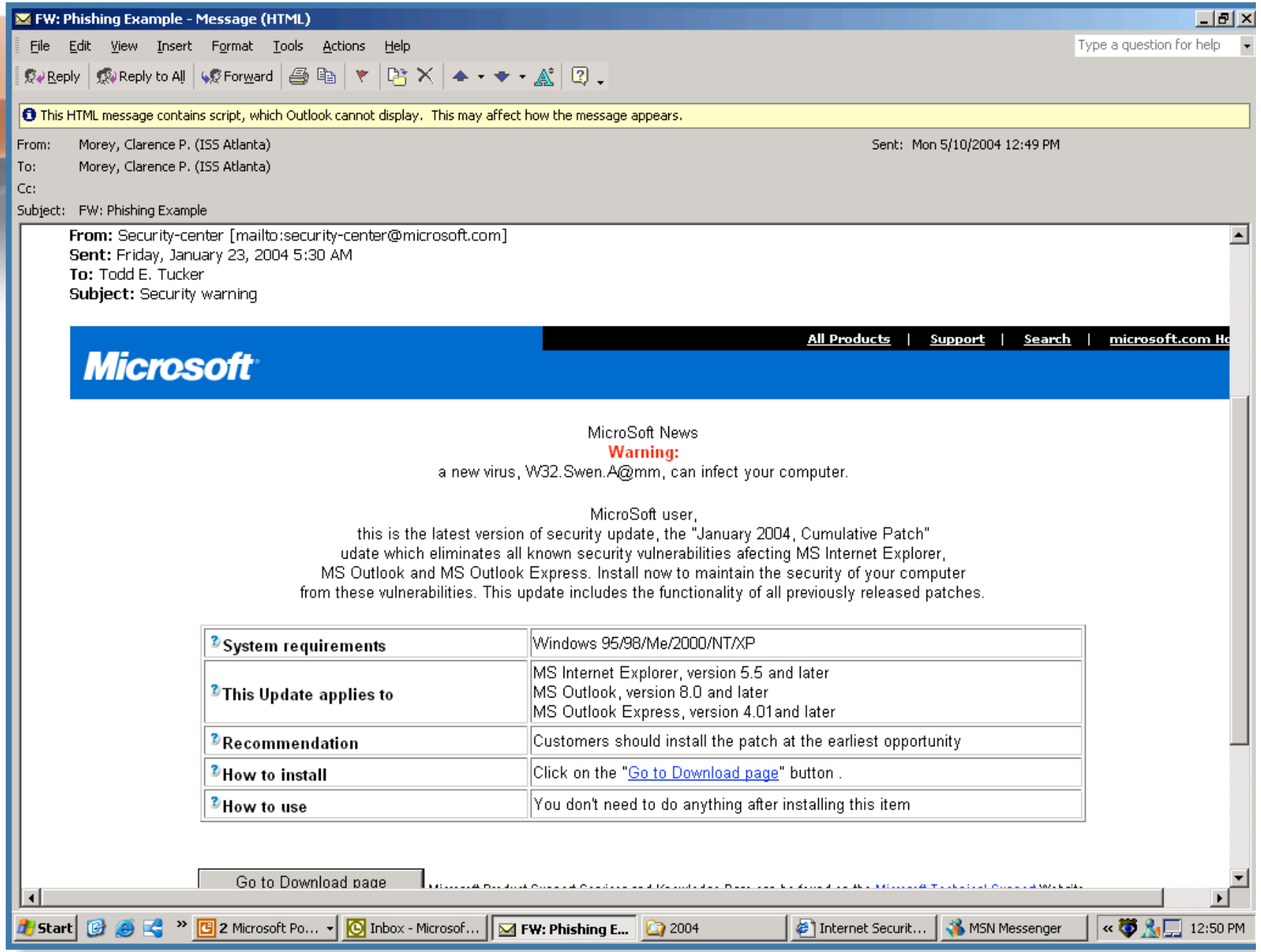
Source: APWG (July '04)

Is Phishing a Serious Threat?

- Traditionally a consumer issue, but changing…



INTERNET SECURITY SYSTEMS®



INTERNET SECURITY SYSTEMS®

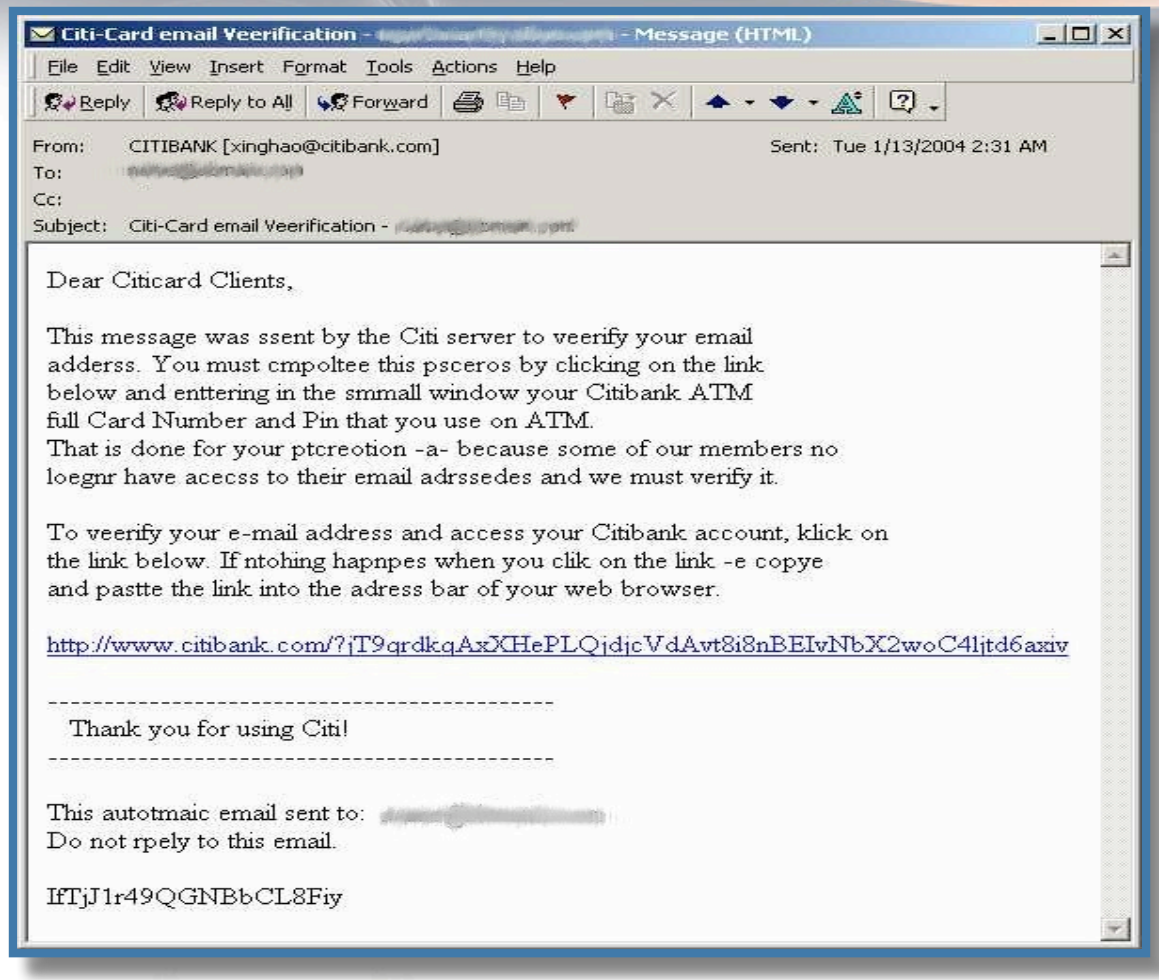
How do Phishers do it?

- Good Link
- Link
- Form
- Frames
- Reply

Note: in descending order of sophistication

INTERNET | SECURITY | SYSTEMS®

Anatomy of an Exploit…

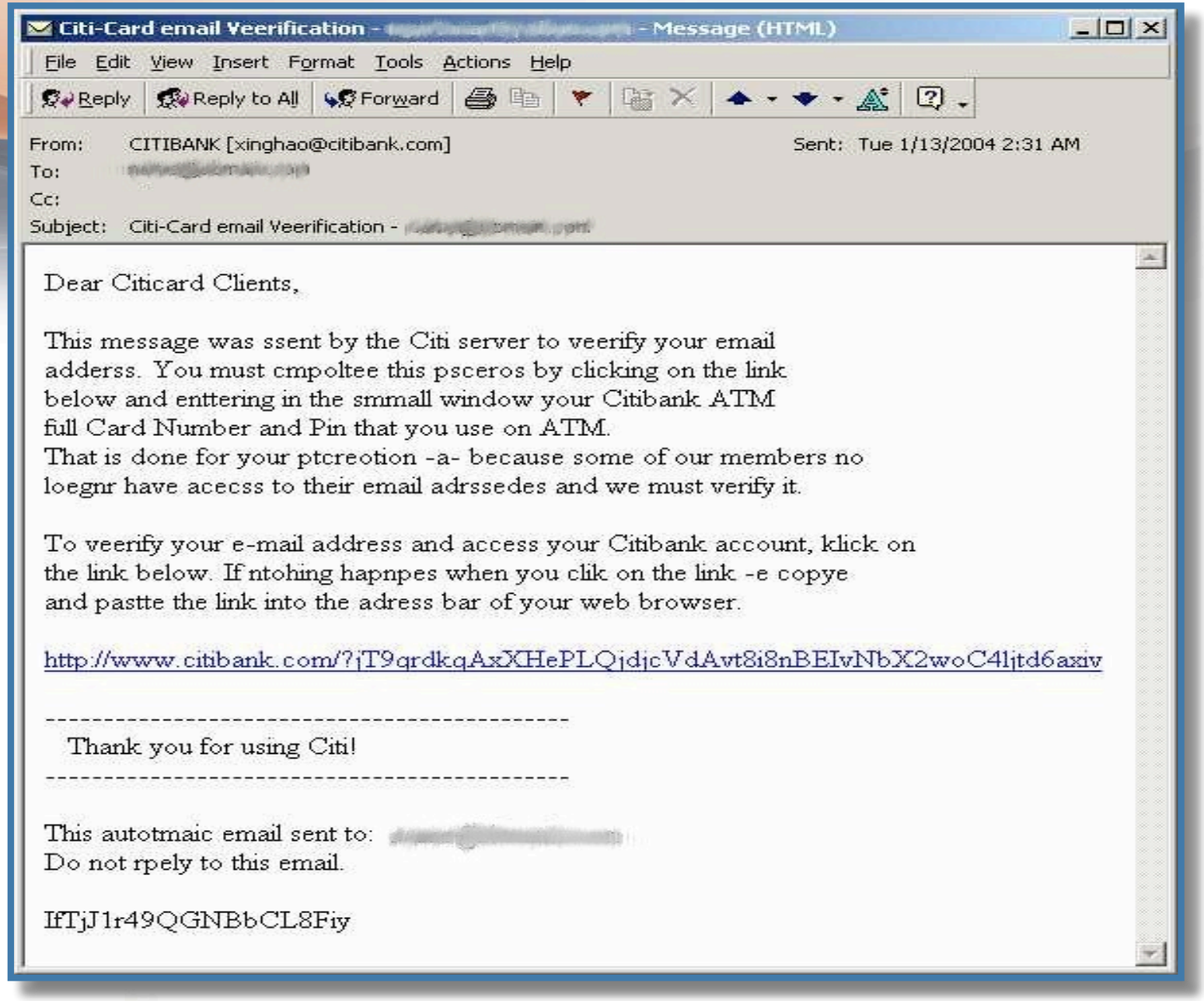


Step 1

"The Bait"

Building credibility

INTERNET SECURITY SYSTEMS®



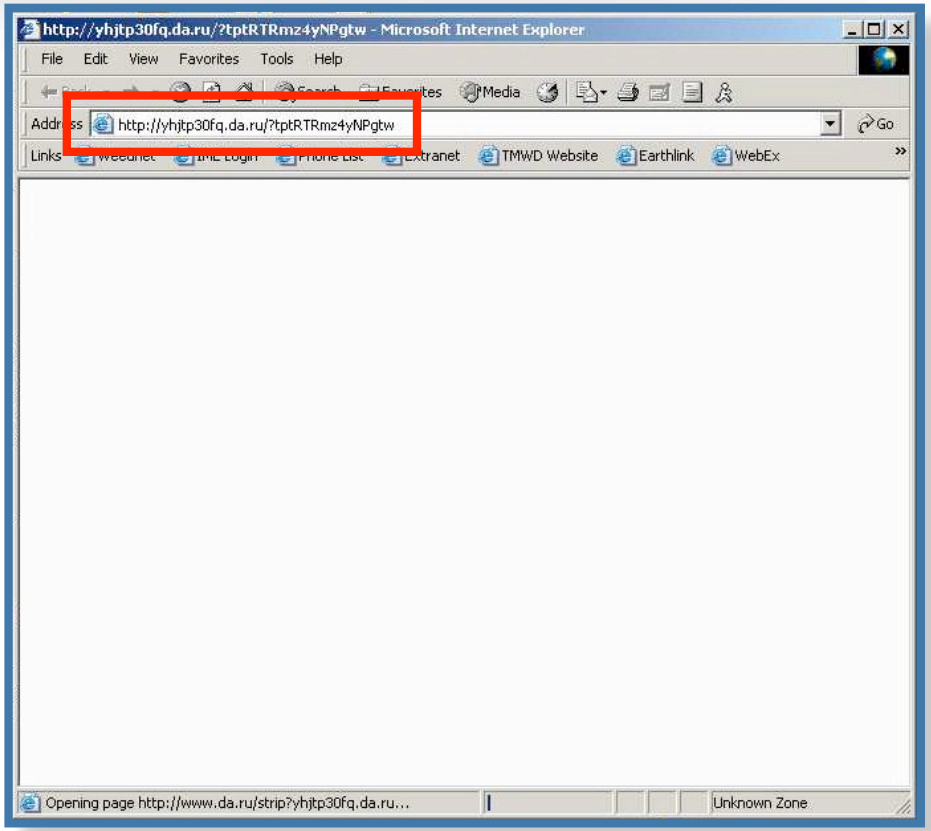
INTERNET SECURITY SYSTEMS®

Anatomy of an Exploit…

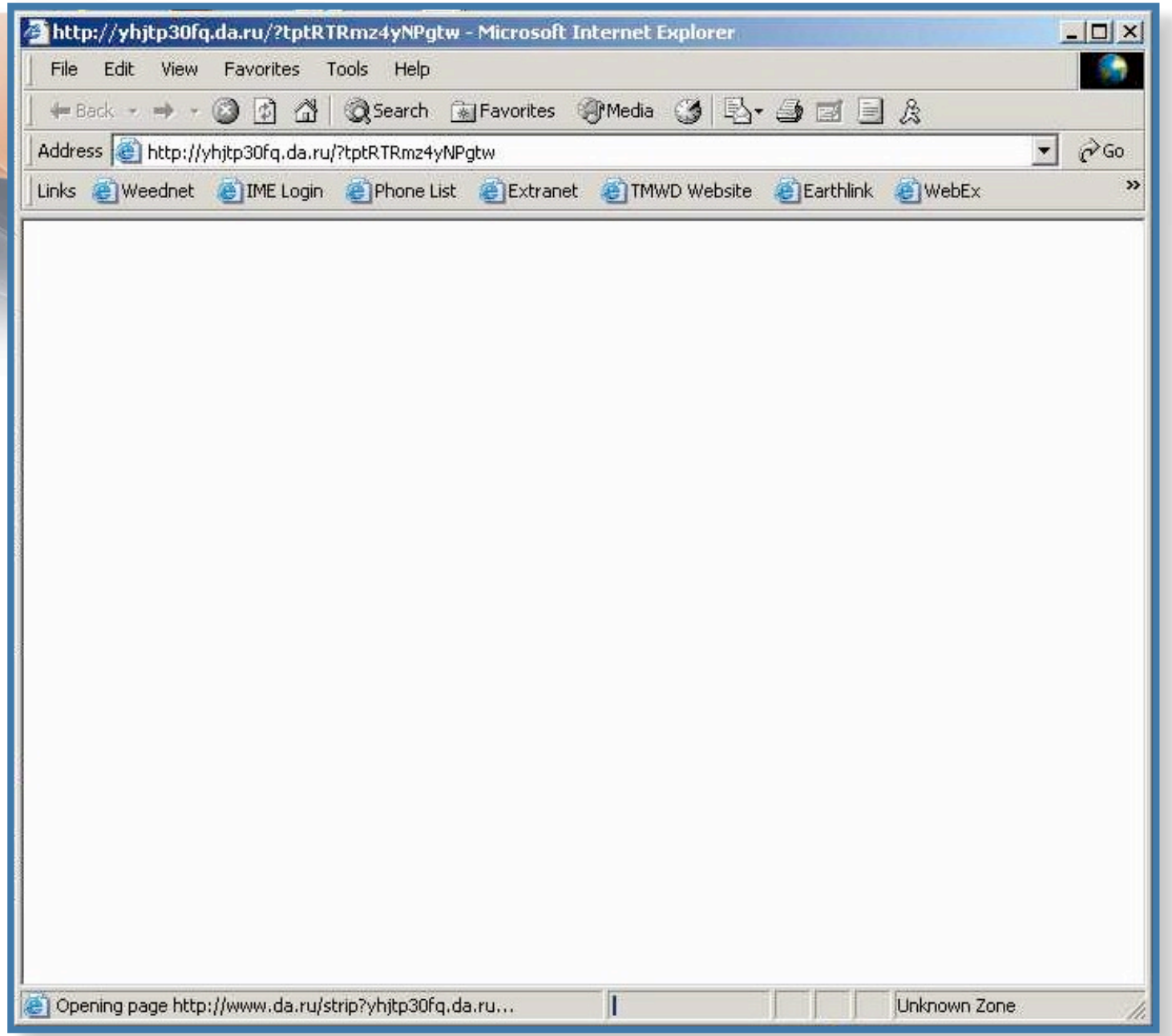
Step 2

"The Hook"

Redirecting



INTERNET | SECURITY | SYSTEMS®

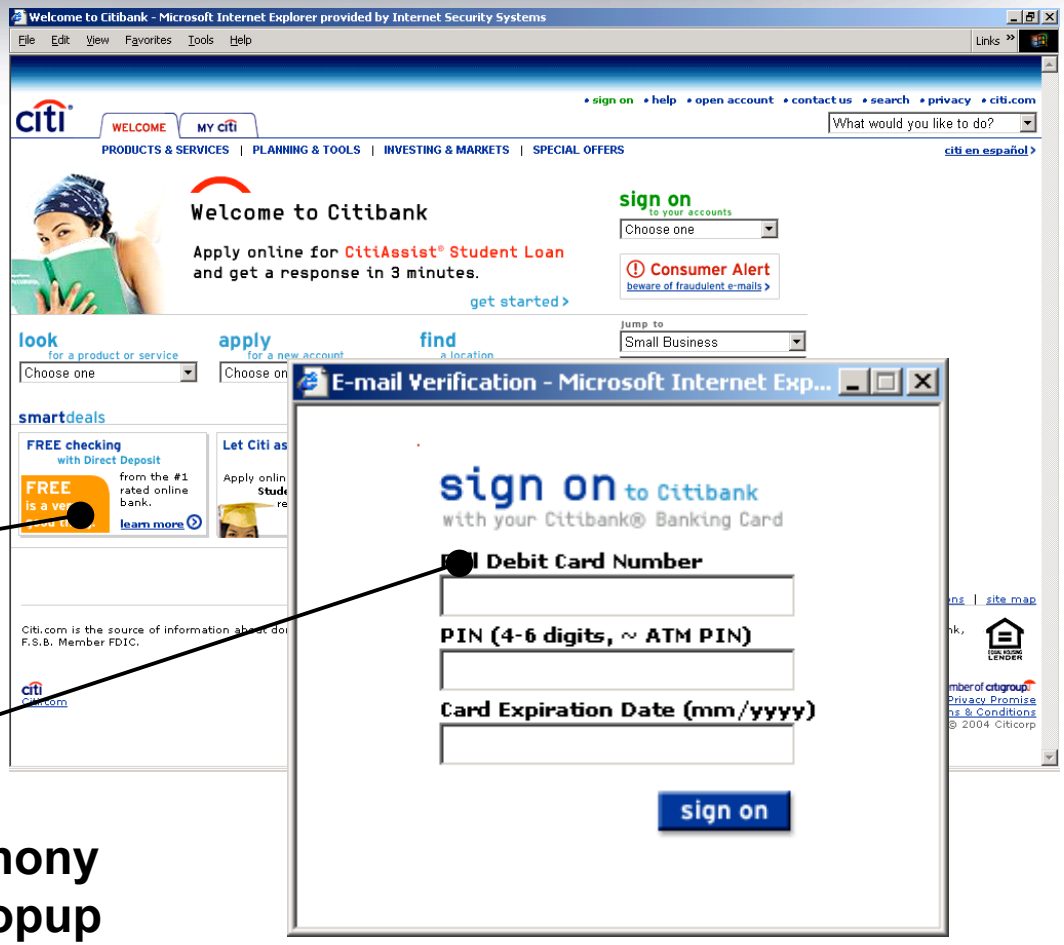


INTERNET SECURITY SYSTEMS®

Anatomy of an Exploit…

Step 3

"Reeling in"



Actual Citibank Homepage

Phony Popup

INTERNET SECURITY SYSTEMS®

Example

- Per RFC 2396, the URL scheme for HTTP is represented as <userinfo>@<host>:<port>
  - So a url like…

    http://**www.citibankonline.com**:acKTtF4BD6y4TZlcv6GT5D@**yhjtp30fq.da.rU**/*?tptRTRmz4yNPgtw*

    …actually takes you to http://**yhjtp30fq.da.rU**

- Not WYSIWYG… reinforces the need for end user security awareness & education

INTERNET | SECURITY | SYSTEMS®

Link Tricks

- **Links**

-IP address

:http://202.111.23.1/siafrequentflyer/now.php

-Long Status line

:*http://www.mandarin.com/$%%^#%%%%#$$$$$#@fakesite.com……*

-Similar Names

:http://www.hackinthbox.org/verify

INTERNET SECURITY SYSTEMS®

More Tricks

- **Mouse over**

-Javascript to show false mouse over message

- **URL as a button**

-You see text displayed thinking its url, actually it's a text description of a Form Button, button is white blending into background

- **Url Encoding**

:http://www.scv.com@%32%31%332E%32%32%30%2E%36%38%, which translates into 213.220.68.214

INTERNET | SECURITY | SYSTEMS®

Web Site Tricks

- Pop ups

----------*→Real Site with pop-up window*

- Floating Address Bar

----------*→javascipt opens a second window with fake url*

- Replacement Address Bar

----------*→Javascript uses a table in Web page to show fake*

Address bar but you can type inside it {greyed out Back button/ no history}

- Fake Secure site

----------*→how often do we check the Cert ?*

INTERNET | SECURITY | SYSTEMS®

So what are we to do?

Sample FTC recommendations

- Don’t click on links in an email
- Don’t Email personal or confidential information
- Review credit card/bank statements as soon as you receive them
- Use anti-virus software and keep it up to date
- Be cautious about opening any attachment or downloading any files

INTERNET | SECURITY | SYSTEMS®

Best Practice Defenses -Policy and Education

- Risk Assessment – people element is ignored
- Security policies, standards and procedures
- Security organization
- Employee education

INTERNET | SECURITY | SYSTEMS®

Understanding Risk

- To get management support… **AND**
- To organize funding, your must recognize and understand the risks.
  - *Why should I spend money on this versus upgrade my firewall?*
- Phishing presents two categories of risk:
  - Personal/individual risk
  - Corporate Risk

INTERNET | SECURITY | SYSTEMS®

Risks of Email Fraud

- Individual Risk
  - Individual's privacy compromised
  - Financial or reputation loss

- Corporate Risk
  - Revealing critical data
  - Possible reputation damage (AOL)
  - Reporting issues (CA SB 1386, HIPAA, etc.)

INTERNET | SECURITY | SYSTEMS®

Policies, Standards and Procedures

- Create Company-wide policies and practices regarding the specific form and content of all outbound customer emails.
- Make sure enforcement is covered in your policies.
- Have clear data classification policies that protect corporate data that may get divulged in phishing scams.

INTERNET | SECURITY | SYSTEMS®

Source: Information Security Policies Made Easy

The Security Organization

- Ensure clear ownership and sponsorship of security policies.
- Clearly identify ownership of technical controls for enforcement of standards and procedures.
- Get user buy in to improve awareness of their security role within the organization
- Incident Response -*Be prepared*

INTERNET SECURITY SYSTEMS®

***Source: Information Security Roles & Responsibilities**

Policy Education

- Like most email attacks, user education is by far the most important factor!
- How can policy education be a success?
  - Provide specific education on phishing to Internal and Customers
  - Make security education a part of the culture
  - Reinforce that policies are for their protection, not just the companies
  - Use a variety of educational techniques
  - Make it a game
  - Use automated policy tools

INTERNET | SECURITY | SYSTEMS®

The Market Need

Protecting Users

Protecting Brands

MTA Authorization Records in DNS working group, otherwise known as MARID, has been shut down.

INTERNET | SECURITY | SYSTEMS®

Protecting Users

Authentication-based Approaches

1. Website Client Authentication

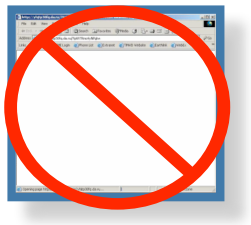
-Implementation

2.Mail Server Authentication

-Competing standards

3.Mail Authentication

-Implementation



URL-based Approaches

INTERNET | SECURITY | SYSTEMS®

Protecting Brands

Monitoring-based Approaches

1. ***DNS Registrations***
2. ***Hacker Chat Rooms***
3. ***Spam Honey Pots***

Logo/Image Recognition

INTERNET | SECURITY | SYSTEMS®

Internet Attacks

INTERNET | SECURITY | SYSTEMS®

Internet Attacks and Phishing

"The phishing problem has a lot of intersection with other problems we look at, such as malicious code & spam."

Department of Justice (May '04)

INTERNET | SECURITY | SYSTEMS®

Net Strategy

Inbound & Outbound

- Spam
- Security Exploits
- Confidential Information
- Personal & Inappropriate Content
- Dangerous & Unknown Attachments
- Web Abuse

INTERNET | SECURITY | SYSTEMS®

Hackers get Serious

- Pre 2004
  - Hackers were kids
  - Not very many good ones
    - Less than 100 could “write shellcode”
  - Intention was to play
    - Damage was accidental
- Post 2004
  - Hackers are grown up
  - Many of them
    - More than 10,000 can “write shellcode”
  - Intention is to profit
    - Damage is intentional

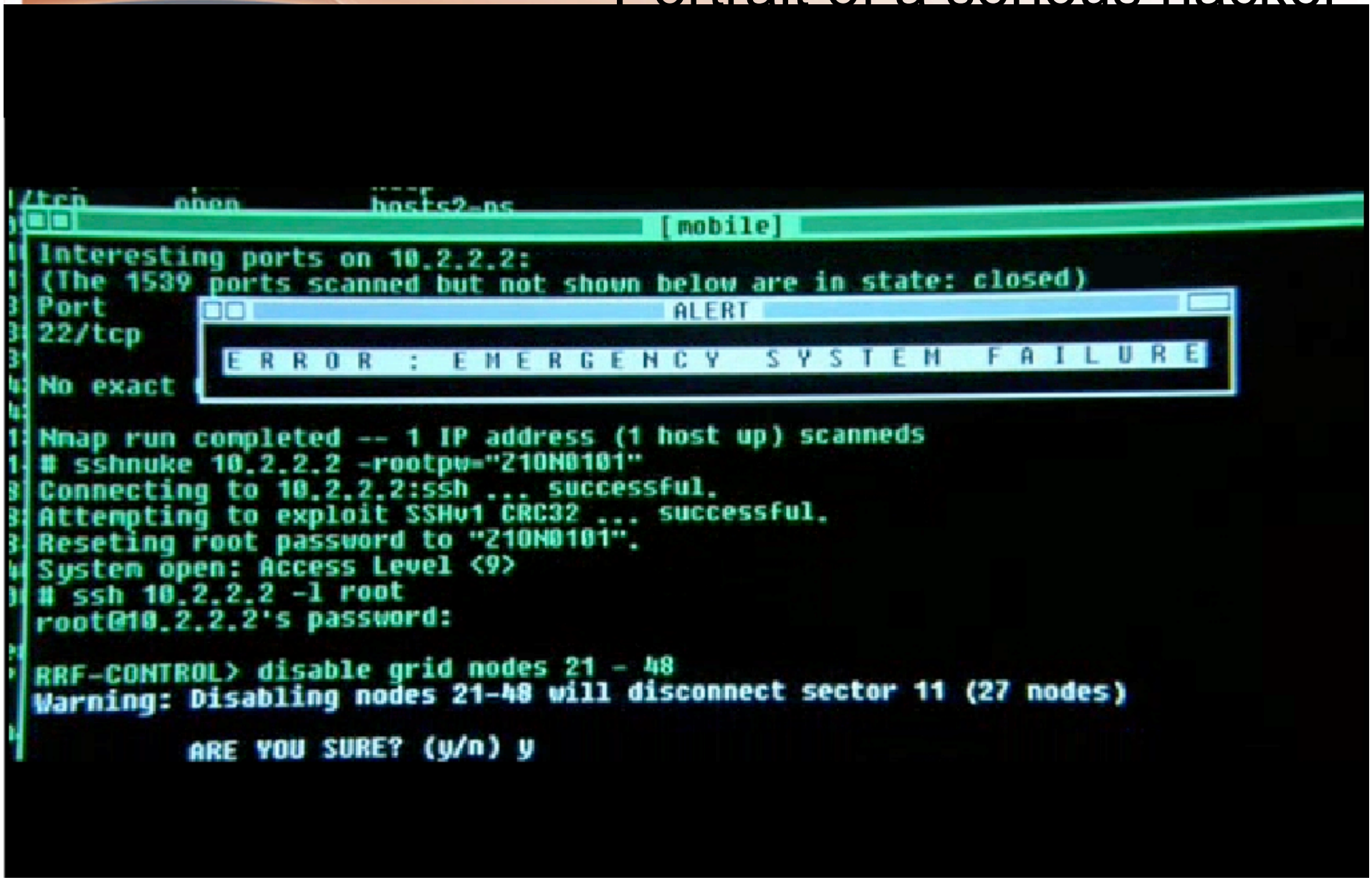
INTERNET | SECURITY | SYSTEMS®

Need smarter protection

- Pre 2004
  - Simple measures stopped hackers
  - Anti-virus products worked
    - Rushed to respond to latest virus
  - Script-kiddies only ran exploits downloaded from public forums
- Post 2004
  - Hackers bypassing simple measures
    - Rush to respond to latest anti-virus update
  - Anti-virus is cleanup
    - Not prevention
  - Hackers write their own exploits

INTERNET | SECURITY | SYSTEMS®

“Matrix Reloaded”
Portrait of a serious hacker



In Depth Protection

- Anti Spam / URL Filtering /IPS / VPS
- New Vulnerability research
  - Discover new threats before hackers do
  - Provide prevention in advance of hacker discovery
- Existing vulnerability research
  - Find out the details before hackers write exploits
    - Don’t wait for hackers to figure things out for Vendors
  - Create comprehensive, proactive defense
    - Details posted to public forums not enough

INTERNET | SECURITY | SYSTEMS®

*What's the **Difference?***

Protecting against *exploits* is reactive

- Too late for many
- Variants undo previous updates
- Typical of AV and most IDS/IPS vendors

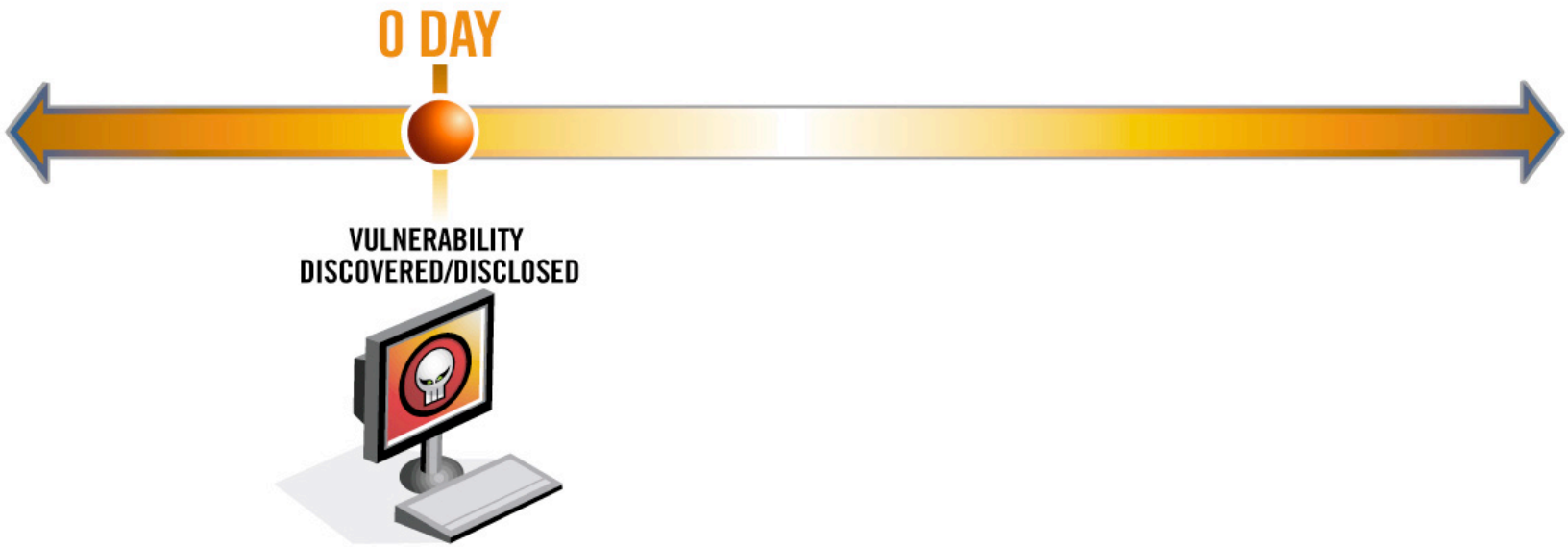
Protecting against *vulnerabilities* is proactive

- Stops threat at source
- Requires advanced R&D

INTERNET | SECURITY | SYSTEMS®

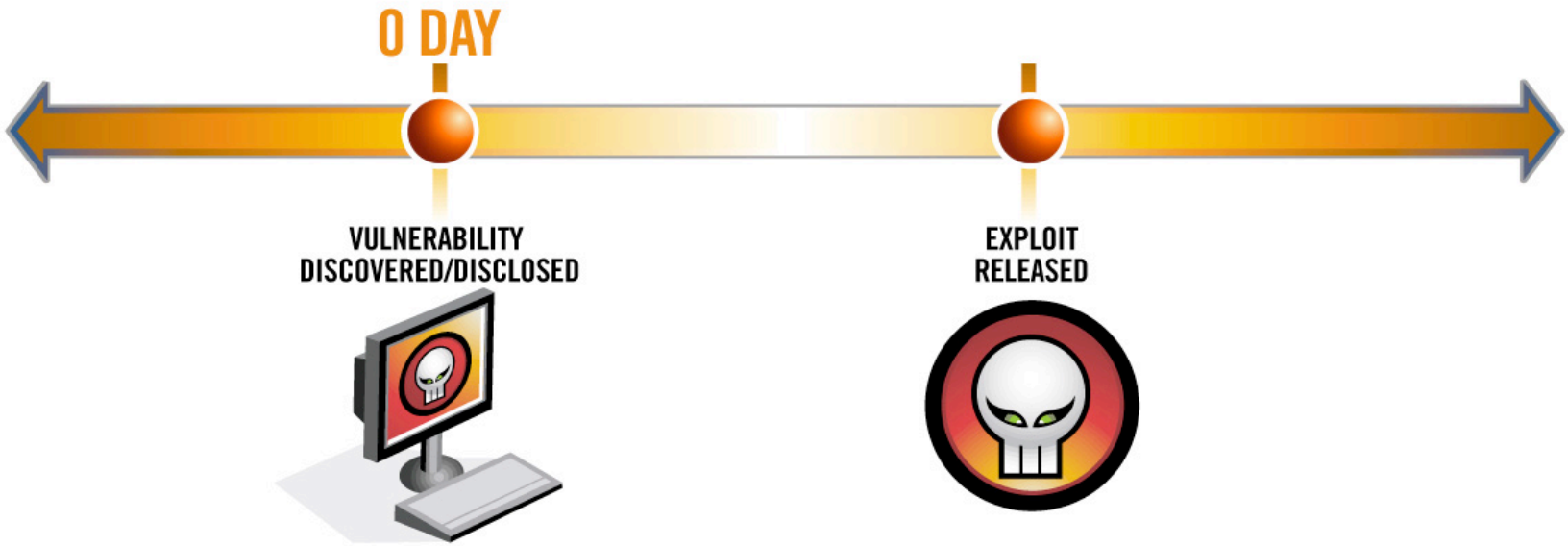
Vulnerabilities & Exploits

Zero-Day Protection - Zero-Day Threats



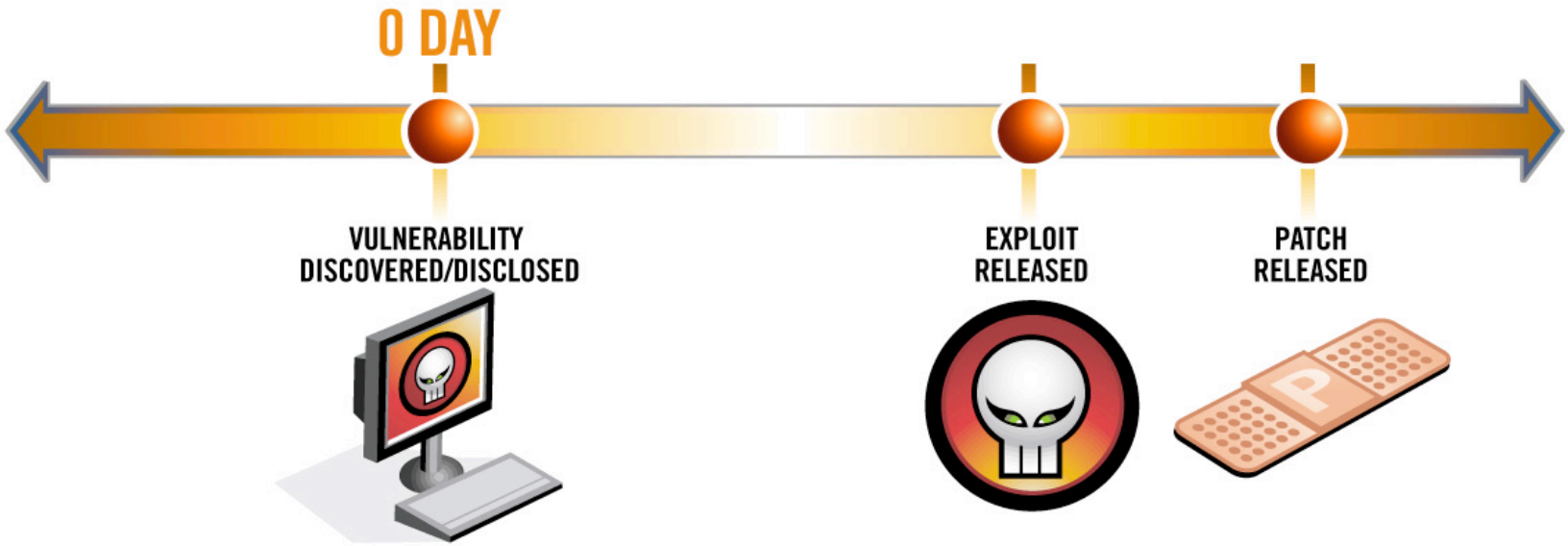
INTERNET | SECURITY | SYSTEMS®

Zero-Day Protection - Zero-Day Threats



INTERNET | SECURITY | SYSTEMS®

Zero-Day Protection - Zero-Day Threats



INTERNET | SECURITY | SYSTEMS®

Zero-Day Protection - Zero-Day Threats

INTERNET | SECURITY | SYSTEMS®

Zero-Day Protection - Zero-Day Threats

INTERNET | SECURITY | SYSTEMS®

Zero-Day Protection - Zero-Day Threats

INTERNET | SECURITY | SYSTEMS®

Zero-Day Protection - Zero-Day Threats

INTERNET | SECURITY | SYSTEMS®

Blaster Chronology

- July 1999: X Froce researches MS-RPC, adds NamedPipes and RPC analysis
- July 16 2003, 1:00pm EDT: Bulletin published
- July 16, 3:30pm: Vulnerability identified by X Force
- July 16, 8:30pm: “Exploit” engineered
- July 17, 1:00 AM: ISS products updated and protected
- July 25, 9:00am: Chinese hacker exploit
- July 25, 12:00pm: Functional exploit released
- July 27: Competitive Vendors’ updates begin to appear
  - Their customers were open to attack for two days
- August 11 2003: Blaster worm appears
- August 24 2003: Agobot worm appears
  - Competitive products update signature for variant

INTERNET | SECURITY | SYSTEMS®

“Protocol-analysis”

- A “protocol” is just the “structure” or “format” of network traffic
  - Data has structure
    - Example: book structure
      - Chapters, titles, paragraphs, words, etc.
    - Example: presentation structure
      - Slides, heading, point, sub-points, etc.
    - Example: Blaster structure
      - Ethernet, IP, TCP, SMB, NamedPipes, MS-RPC, ISystemActivator
- What does it mean to “analyze” protocols?
  - To consider the structure, rather than just the raw data, when detecting intrusion

Protocol-analysis and “buffer-overflows”

- What is a “buffer-overflow”?
  - One of the most common types of hacker attacks
    - CodeRed, Slammer, Blaster, Sasser were buffer-overflows
    - Nimbda was not
  - Sends more data than can fit within buffer
    - Hackers can figure out something clever to do with that extra data
- How to detect with “protocol-analysis”?
  - Find buffer in network traffic
  - Measure length of buffer
  - Trigger when buffer exceeds length

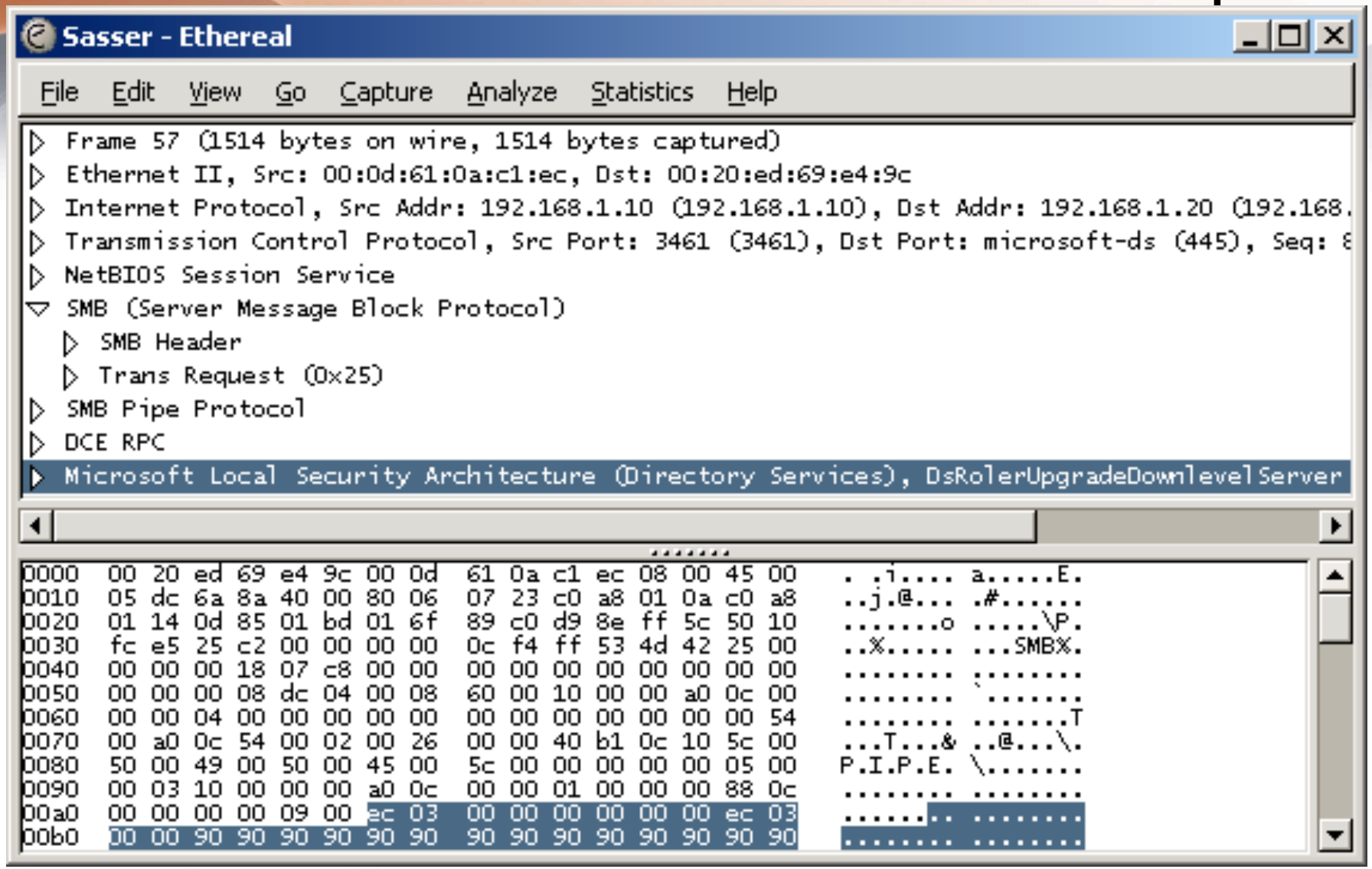
Pattern-matching and buffer-overflows

- What is “pattern-matching”?
  - Traditional way of doing intrusion-detection
  - The basis for most intrusion-detection systems
- How to detect buffer-overflow with pattern-matching?
  - Wait for hackers to publish exploits
  - Search network traffic for patterns unique to exploit
    - It’s “signature”
  - Trigger whenever pattern found

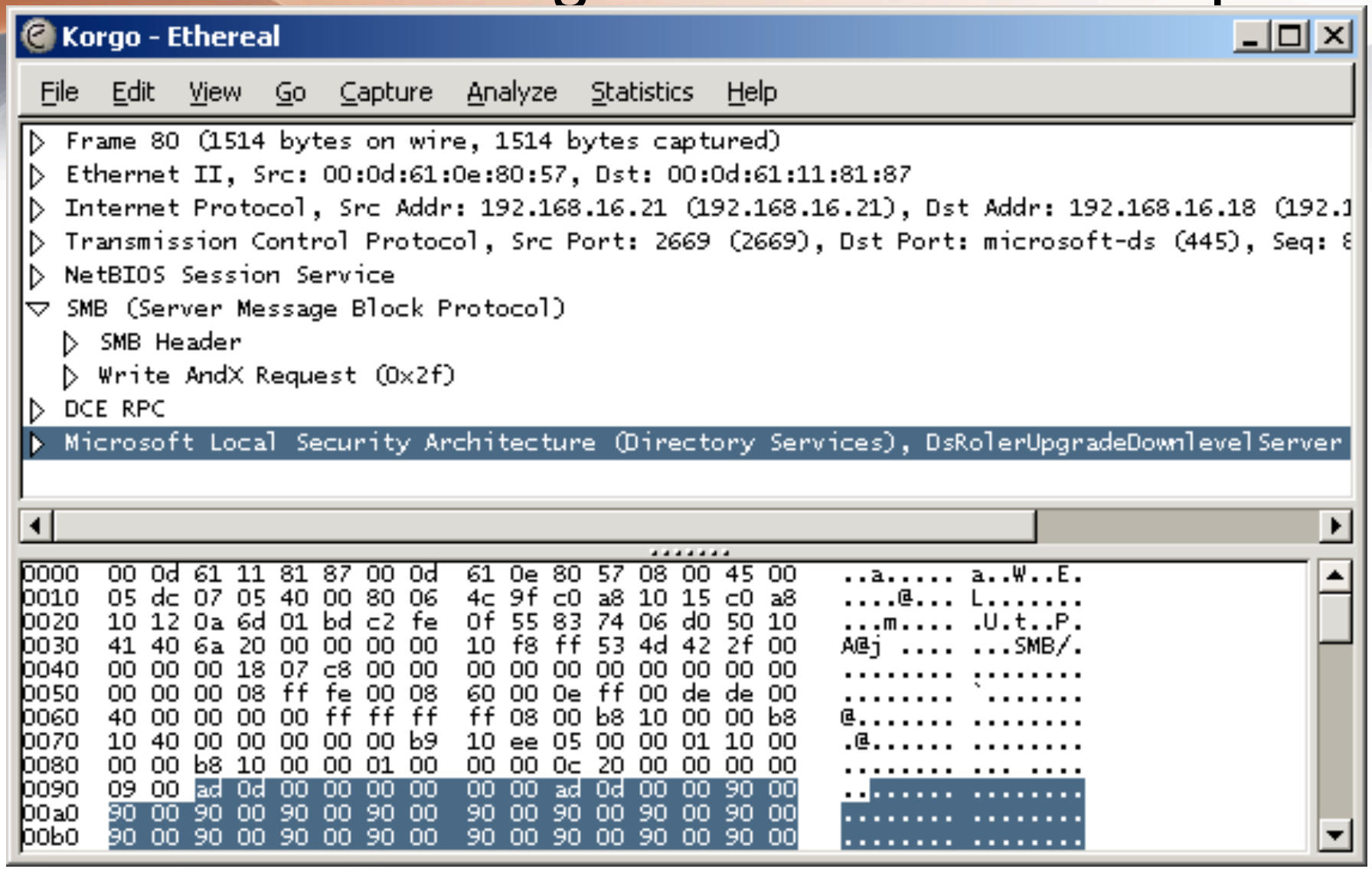
Contrast

- Protocol-analysis
  - Signatures are written to the vulnerability (“vulnerability-signatures”)
  - Signatures written BEFORE hackers release exploits
  - Signatures require vulnerability-analysis in order to write
    - (takes more effort)
  - Detects unknown exploits
- Pattern-matching
  - Signatures written AFTER hackers release exploits
  - Signature do not require vulnerability-analysis
    - Only exploit analysis
  - Only detect the exploits they were written for
  - New signatures must be written each time new exploit appears
    - …and hackers can create new signatures designed to bypass IDS/IPS

Sasser: “Trans Request”



Korgo: “Write AndX Request”



Recap: Buffer-overflow detection

- Protocol-analysis Signatures
  - Finds buffer in packet
  - Measures length
  - Tests length against threshold
- Sasser detection
  - Finds buffer in “Trans” request
  - Measures length of 1004 characters
- Korgo detection
  - Finds buffer in “Write” request
  - Measures length of 3501 characters

In Depth Protection

1) Stop unnecessary mails to your system – Anti Spam
2) Stop you from going to the illegitimate sites – URL filtering
3) Protect against malicious programs - IPS
4) Stop malicious programs in their execution phase – VPS
5) Regular Scanning – Vulnerability Assessment

INTERNET | SECURITY | SYSTEMS®

Market Leadership

1994 – First vulnerability analysis tool

1996 – First commercial vulnerability assessment product

1997 – ISS X-Force team first to provide primary vulnerability and threat research

1997 – First commercial intrusion detection system

1999 – #1 worldwide market share leader IDnA

2001 – First gigabit Intrusion protection product

2001 – First inline intrusion prevention system

2002 – First protection platform covering networks, servers, desktops & laptops

2002 – First and only unified enterprise protection system

2003 – First Guaranteed Protection services

2003 – Developed world's first Smart Firewall

INTERNET | SECURITY | SYSTEMS®

For More Information

- **www.iss.net**
- **Proventia Products that fight phishing**
  - www.iss.net/resources/phishing.php
- **Free 30-day download of ISS products**
  - www.iss.net/antispam

INTERNET | SECURITY | SYSTEMS®

Thank you !

INTERNET | SECURITY | SYSTEMS®