



# 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***

# 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.



# *Is Phishing a Serious Threat?*

*“[Phishing is the] hottest & most troubling, new scam on the Internet.”*

Jana Monroe, FBI (July '03)



Rearing goats helps Basniar overcome major setback - Microsoft Internet Explorer provided by Internet Security Systems

File Edit View Favorites Tools Help

Address <http://thestar.com.my/news/story.asp?file=/2004/10/7/nation/9067746&sec=nation>

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

**More Channels** [The Star Online](#) > [News](#)

**Business**

**Sports**

**Entertainment**

**Lifestyle**

**Health**

**Technology**

**Education**

**Classifieds**

**Directory**

**e-Cards**

**Member**

**30-Day Archives**

**Contests**

**Games**

**Extras**

**Property**

**Motoring**

**Purple Sofa**

**Comics**

**AudioFile**

**Maritime**

**Jobs**

**Kuali**

**Clove**

**Weather**

**Specials**

**Online exclusives**

**Columnists**

**Honours lists**

Awarded Superbrands

Start Rearing goats helps B...

11:23 AM

# *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](#),

# *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.

## *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.

# Is Phishing a Serious Threat?

- Traditionally a consumer issue, but changing...

FW: Phishing Example - Message (HTML)

This HTML message contains script, which Outlook cannot display. This may affect how the message appears.

From: Morey, Clarence P. (ISS Atlanta) Sent: Mon 5/10/2004 12:49 PM  
To: Morey, Clarence P. (ISS Atlanta)  
Cc:  
Subject: FW: Phishing Example

From: Security-center [mailto:security-center@microsoft.com]  
Sent: Friday, January 23, 2004 5:30 AM  
To: Todd E. Tucker  
Subject: Security warning

**Microsoft** All Products | Support | Search | microsoft.com

MicroSoft News  
**Warning:**  
a new virus, W32.Swen.A@mm, can infect your computer.

MicroSoft user,  
this is the latest version of security update, the "January 2004, Cumulative Patch"  
update which eliminates all known security vulnerabilities affecting MS Internet Explorer,  
MS Outlook and MS Outlook Express. Install now to maintain the security of your computer  
from these vulnerabilities. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This Update applies to	MS Internet Explorer, version 5.5 and later MS Outlook, version 8.0 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportunity
How to install	Click on the "Go to Download page" button.
How to use	You don't need to do anything after installing this item

Go to Download page

**FW: Phishing Example - Message (HTML)**

File Edit View Insert Format Tools Actions Help

Type a question for help

Reply Reply to All Forward Print Forward Stop X Undo Redo ?

**i** This HTML message contains script, which Outlook cannot display. This may affect how the message appears.

From: Morey, Clarence P. (ISS Atlanta) Sent: Mon 5/10/2004 12:49 PM  
 To: Morey, Clarence P. (ISS Atlanta)  
 Cc:  
 Subject: FW: Phishing Example

**From:** Security-center [mailto:security-center@microsoft.com]  
**Sent:** Friday, January 23, 2004 5:30 AM  
**To:** Todd E. Tucker  
**Subject:** Security warning

**Microsoft** All Products | Support | Search | microsoft.com Home

MicroSoft News  
**Warning:**  
 a new virus, W32.Swen.A@mm, can infect your computer.

MicroSoft user,  
 this is the latest version of security update, the "January 2004, Cumulative Patch"  
 update which eliminates all known security vulnerabilities affecting MS Internet Explorer,  
 MS Outlook and MS Outlook Express. Install now to maintain the security of your computer  
 from these vulnerabilities. This update includes the functionality of all previously released patches.

<b>System requirements</b>	Windows 95/98/Me/2000/NT/XP
<b>This Update applies to</b>	MS Internet Explorer, version 5.5 and later MS Outlook, version 8.0 and later MS Outlook Express, version 4.01 and later
<b>Recommendation</b>	Customers should install the patch at the earliest opportunity
<b>How to install</b>	Click on the " <a href="#">Go to Download page</a> " button .
<b>How to use</b>	You don't need to do anything after installing this item

Go to Download page

Start | 2 Microsoft Po... | Inbox - Microsof... | FW: Phishing E... | 2004 | Internet Securit... | MSN Messenger | 12:50 PM

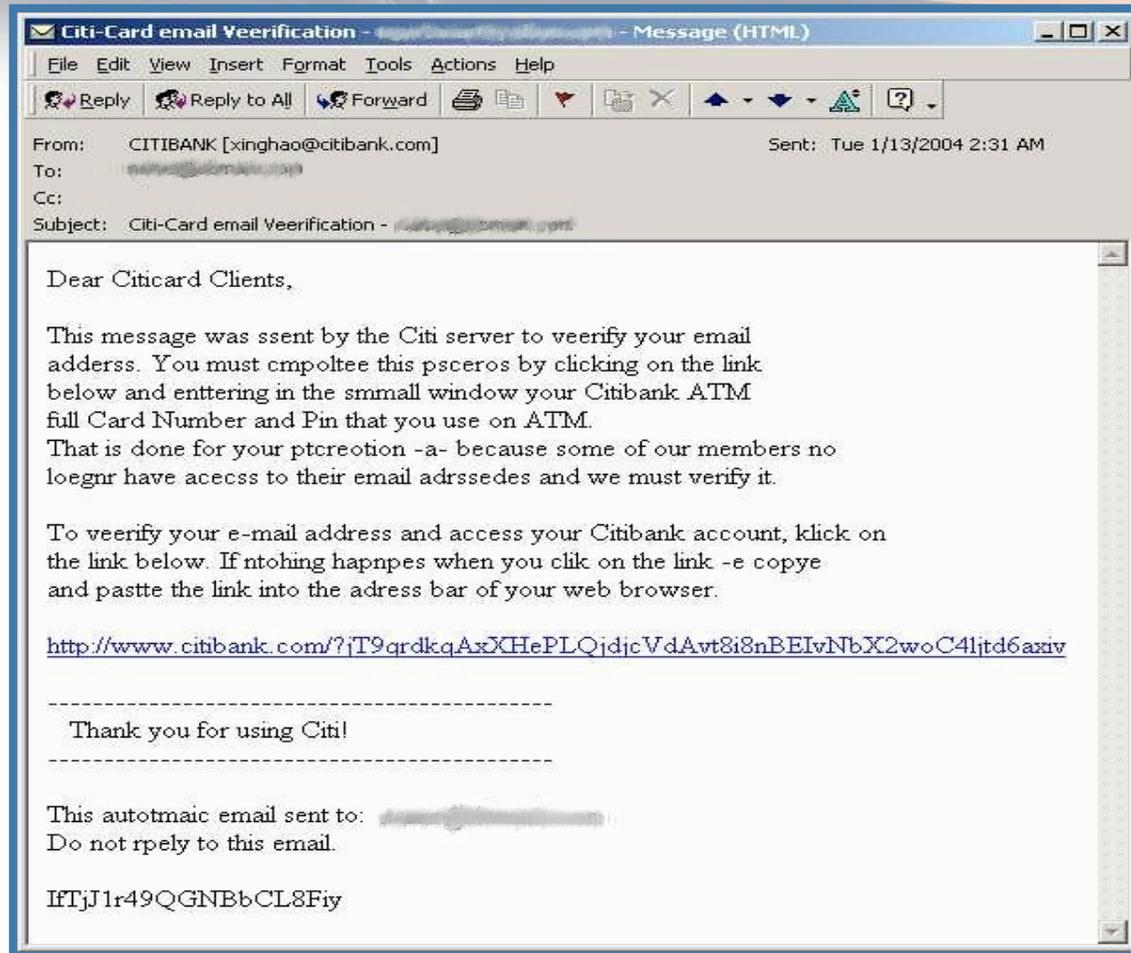
# How do Phishers do it?



- *Good Link*
- *Link*
- *Form*
- *Frames*
- *Reply*

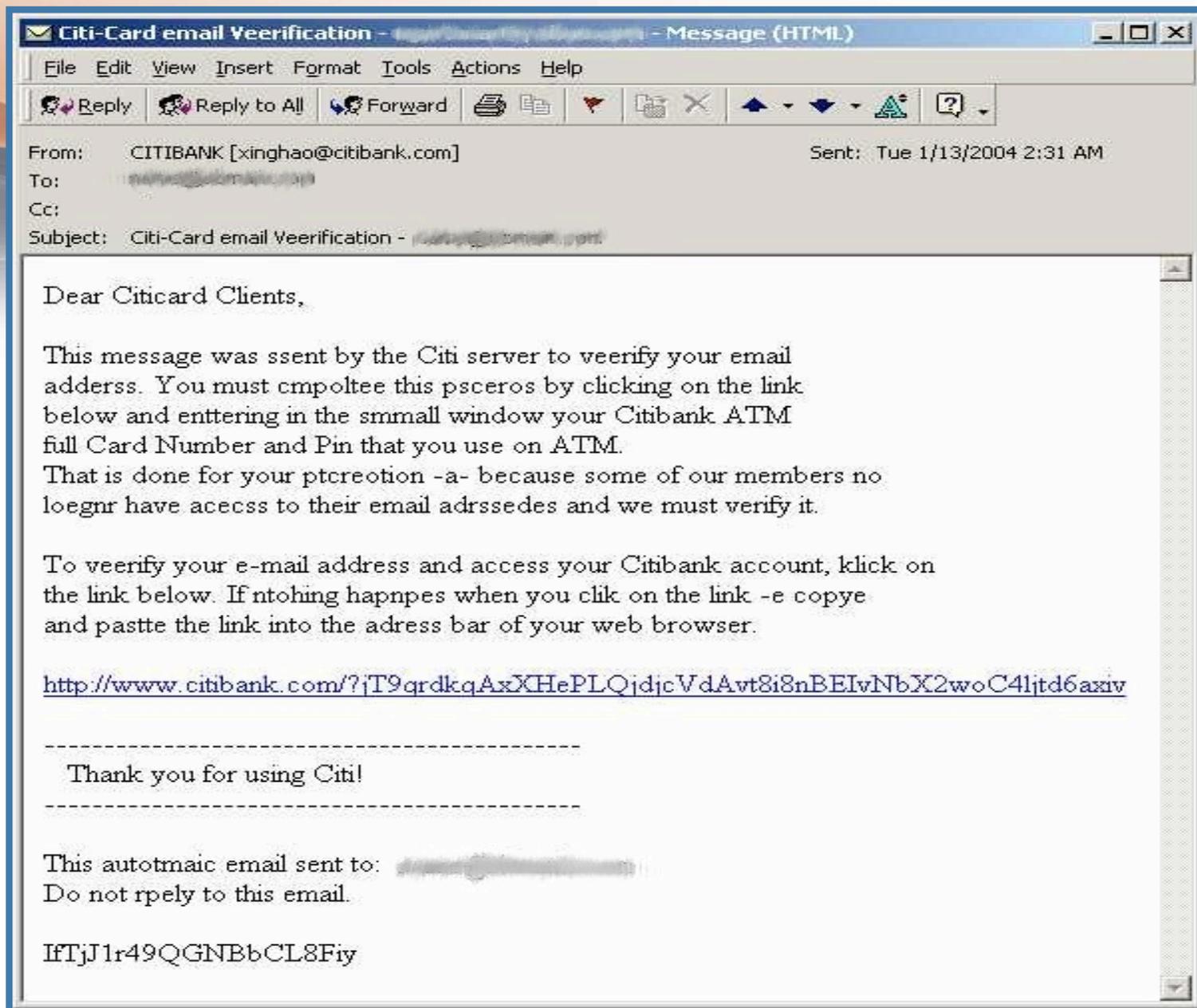
**Note: in descending order of sophistication**

# Anatomy of an Exploit...



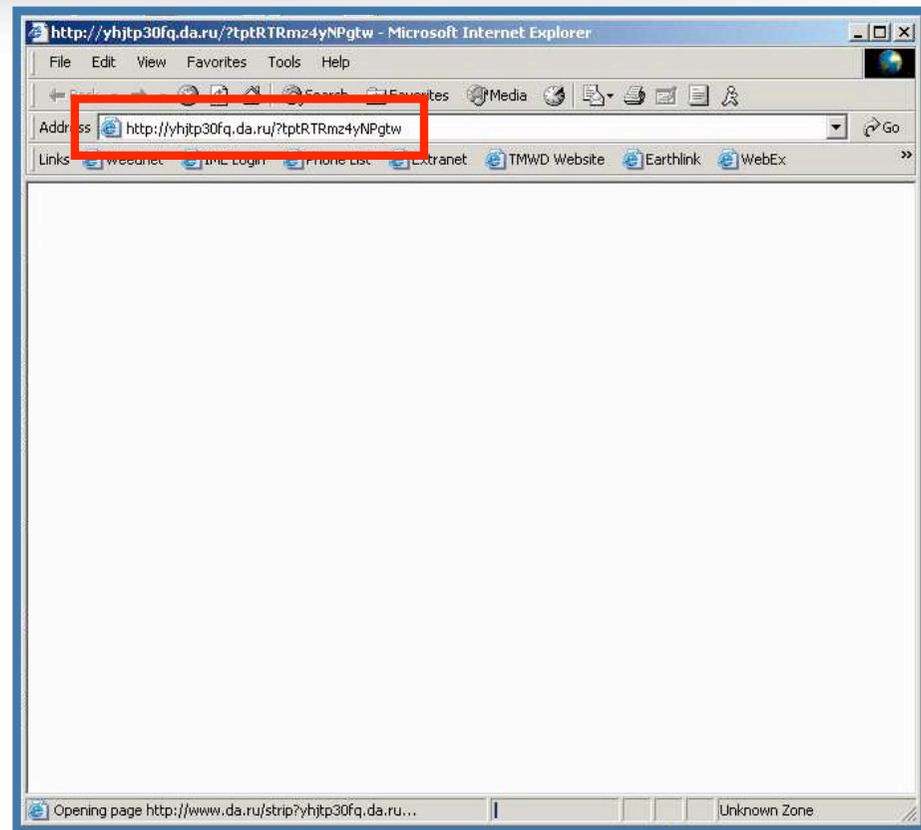
## Step 1 "The Bait"

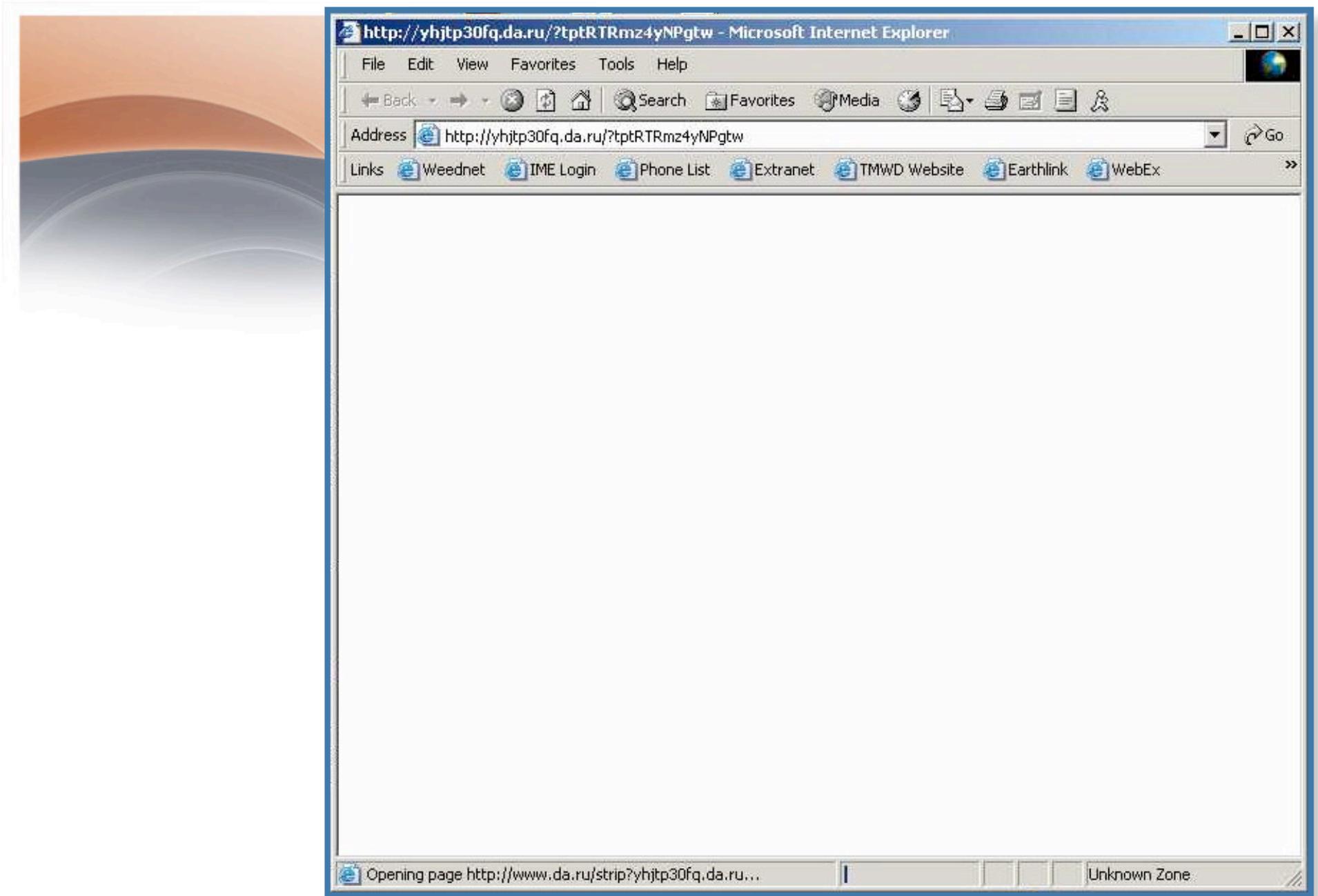
*Building credibility*



# Anatomy of an Exploit...

## Step 2 “The Hook” Redirecting





# Anatomy of an Exploit...

## Step 3 "Reeling in"

The image shows a screenshot of a Microsoft Internet Explorer browser window displaying the Citibank homepage. The browser title is "Welcome to Citibank - Microsoft Internet Explorer provided by Internet Security Systems". The homepage features the Citibank logo, navigation links, and a "sign on" button. A "Consumer Alert" banner is visible. A "Phony Popup" window is overlaid on the homepage, titled "E-mail Verification - Microsoft Internet Exp...". The popup contains a "sign on to Citibank" header and a form with the following fields: "Debit Card Number", "PIN (4-6 digits, ~ ATM PIN)", and "Card Expiration Date (mm/yyyy)". A "sign on" button is located at the bottom of the popup. Lines connect the labels "Actual Citibank Homepage" and "Phony Popup" to their respective elements in the screenshot.

## 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

# Link Tricks

- **Links**

- IP address**

- :<http://202.111.23.1/siafrequentflyer/now.php>

- Long Status line**

- :[http://www.mandarin.com/\\$%^#%#\\$\\$\\$\\$#@fakesite.com.....](http://www.mandarin.com/$%^#%#$$$$#@fakesite.com.....)

- Similar Names**

- :<http://www.hackinthbox.org/verify>



# Web Site Tricks

- Pop ups

-----→*Real Site with pop-up window*

- Floating Address Bar

-----→*javascript 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 ?*

*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

# *Best Practice Defenses -Policy and Education*

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

# Understanding Risk

- To get management support... **AND**
- To organize funding, you 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



# *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.)



# *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.

# 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*

# *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

# The Market Need

## Protecting Users



## Protecting Brands

MTA Authorization Records in DNS working group, otherwise known as MARID, has been [shut down](#).

# Protecting Users

## Authentication-based Approaches



### **1. Website Client Authentication**

*-Implementation*

### **2. Mail Server Authentication**

*-Competing standards*

### **3. Mail Authentication**

*-Implementation*



## URL-based Approaches

# Protecting Brands

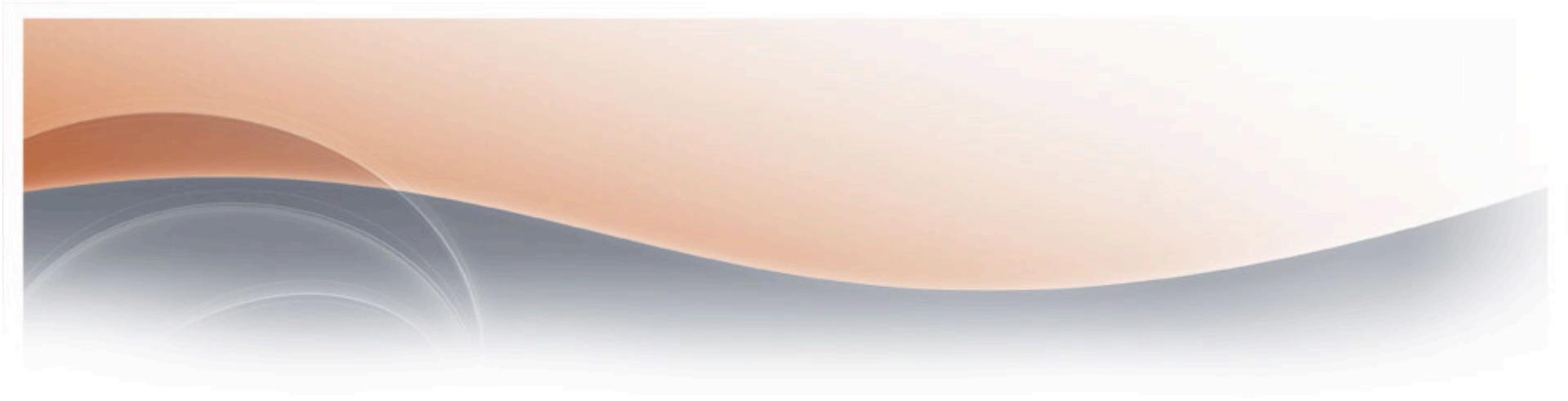
## Monitoring-based Approaches

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



## Logo/Image Recognition





# ***Internet Attacks***

# *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)



# Net Strategy

## Inbound & Outbound

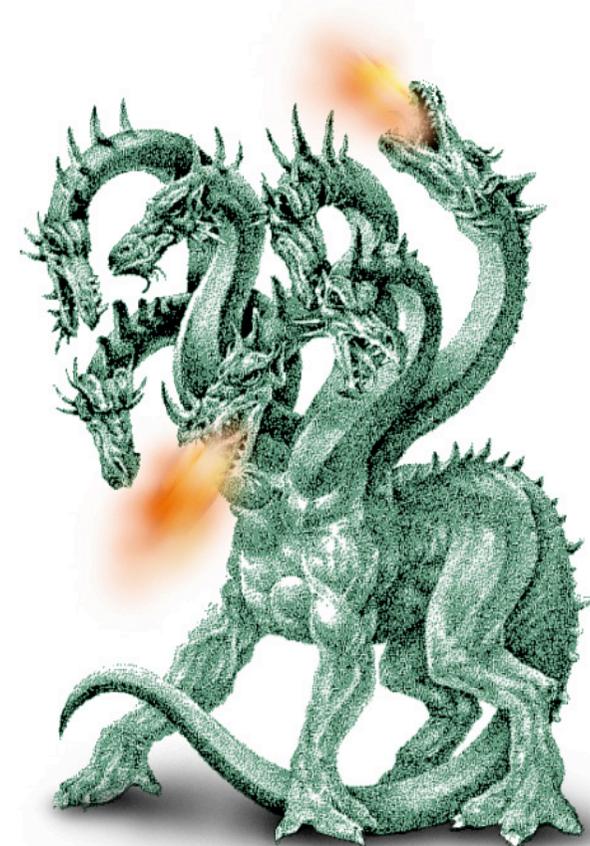
- Spam
- Security Exploits
- Confidential Information
- Personal & Inappropriate Content
- Dangerous & Unknown Attachments
- Web Abuse



*“Casting a Wider Net”*

# 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

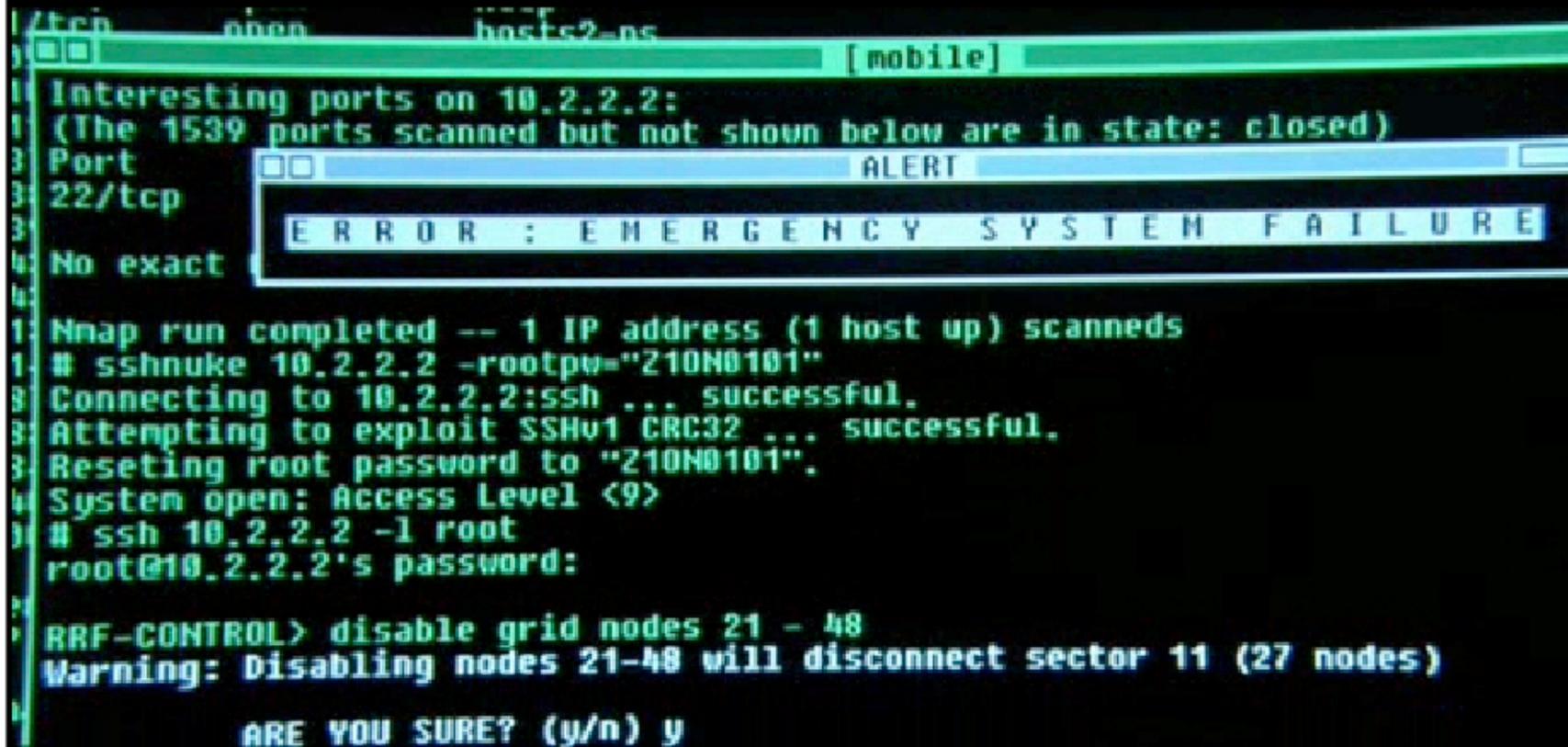


# *Need smarter protection*

- 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

# “Matrix Reloaded” Portrait of a serious hacker

```
1 /tcp      open      hosts2-ns
2 [mobile]
3 Interesting ports on 10.2.2.2:
4 (The 1539 ports scanned but not shown below are in state: closed)
5 Port      State
6 22/tcp    open
7 No exact
8
9 Nmap run completed -- 1 IP address (1 host up) scanned
10 # sshnuke 10.2.2.2 -rootpw="210N0101"
11 Connecting to 10.2.2.2:ssh ... successful.
12 Attempting to exploit SSHv1 CRC32 ... successful.
13 Reseting root password to "210N0101".
14 System open: Access Level <9>
15 # ssh 10.2.2.2 -l root
16 root@10.2.2.2's password:
17
18 RRF-CONTROL> disable grid nodes 21 - 48
19 Warning: Disabling nodes 21-48 will disconnect sector 11 (27 nodes)
20
21 ARE YOU SURE? (y/n) y
```



# *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

# 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

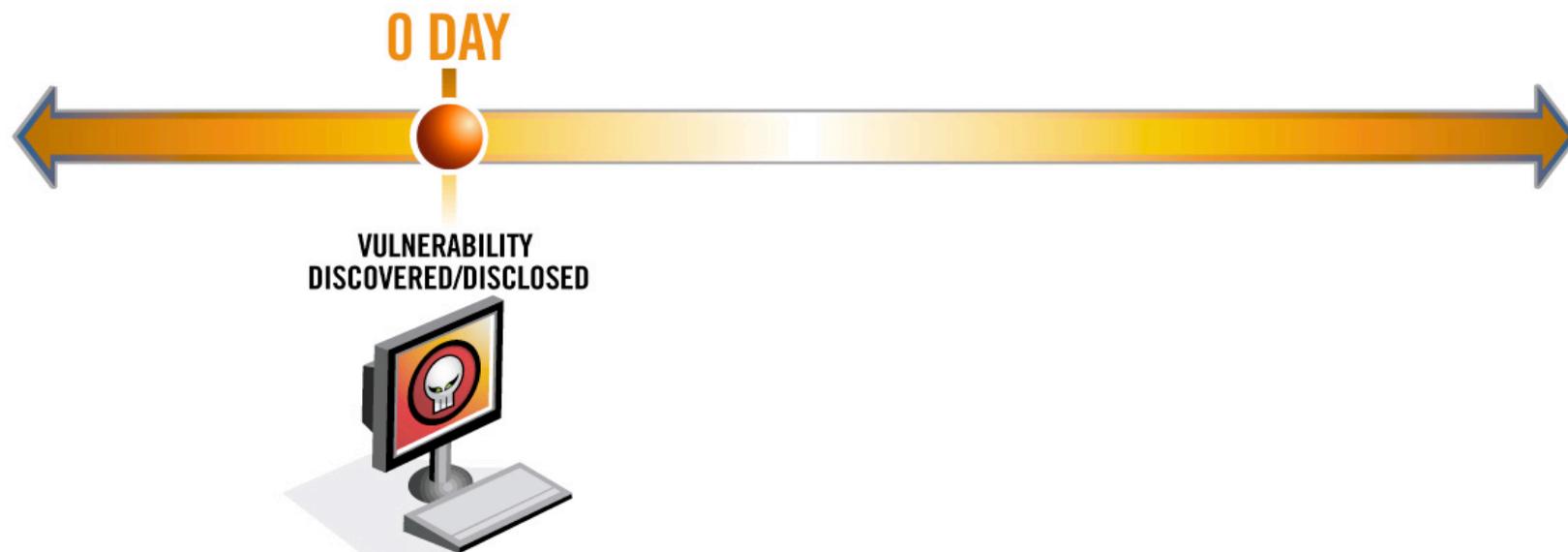
- Stops threat at source
- Requires advanced R&D



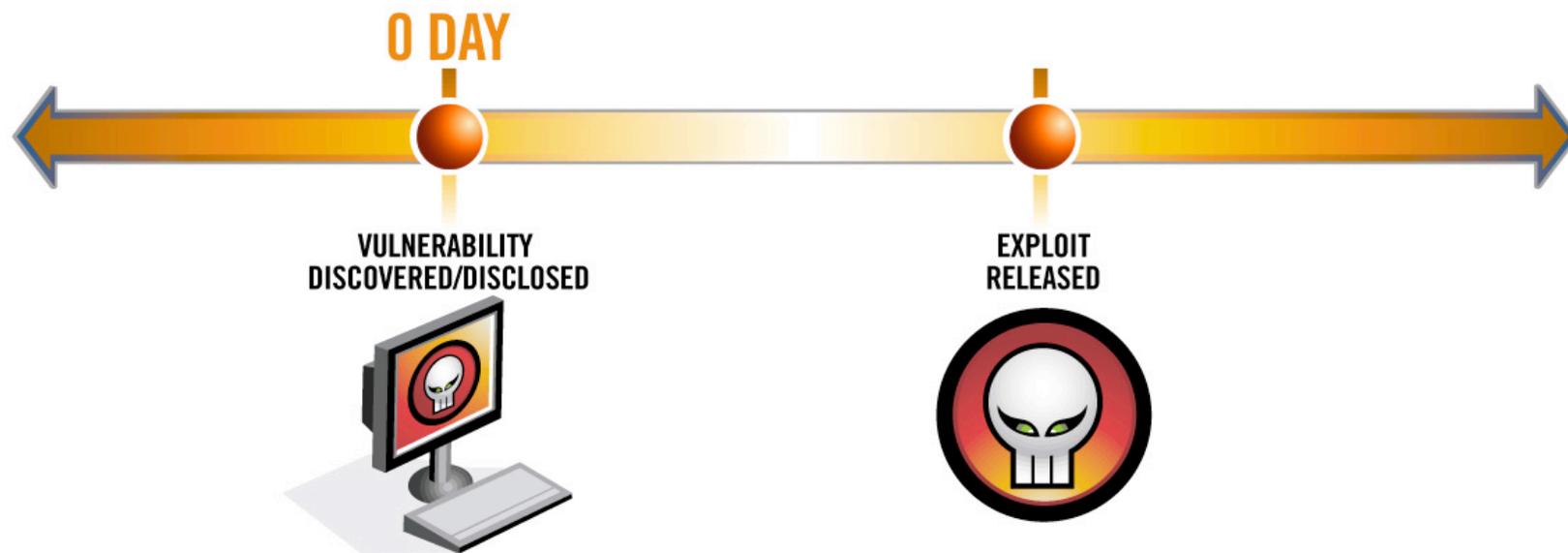
# Vulnerabilities & Exploits



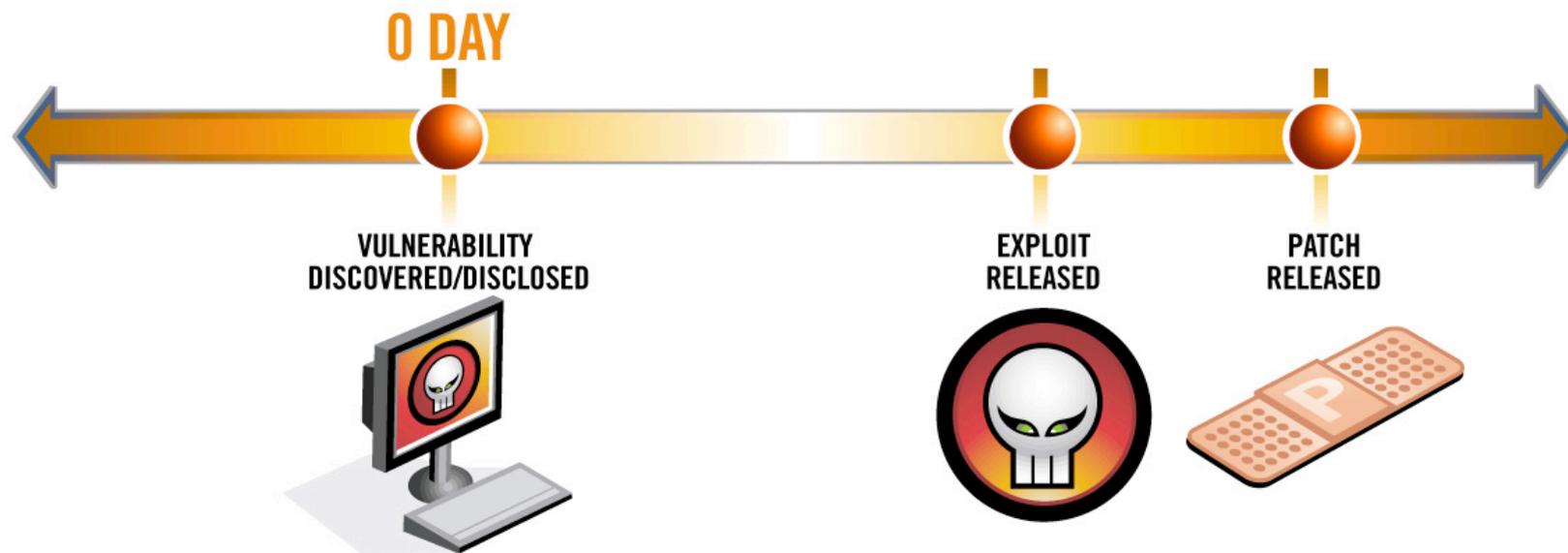
# Zero-Day Protection - Zero-Day Threats



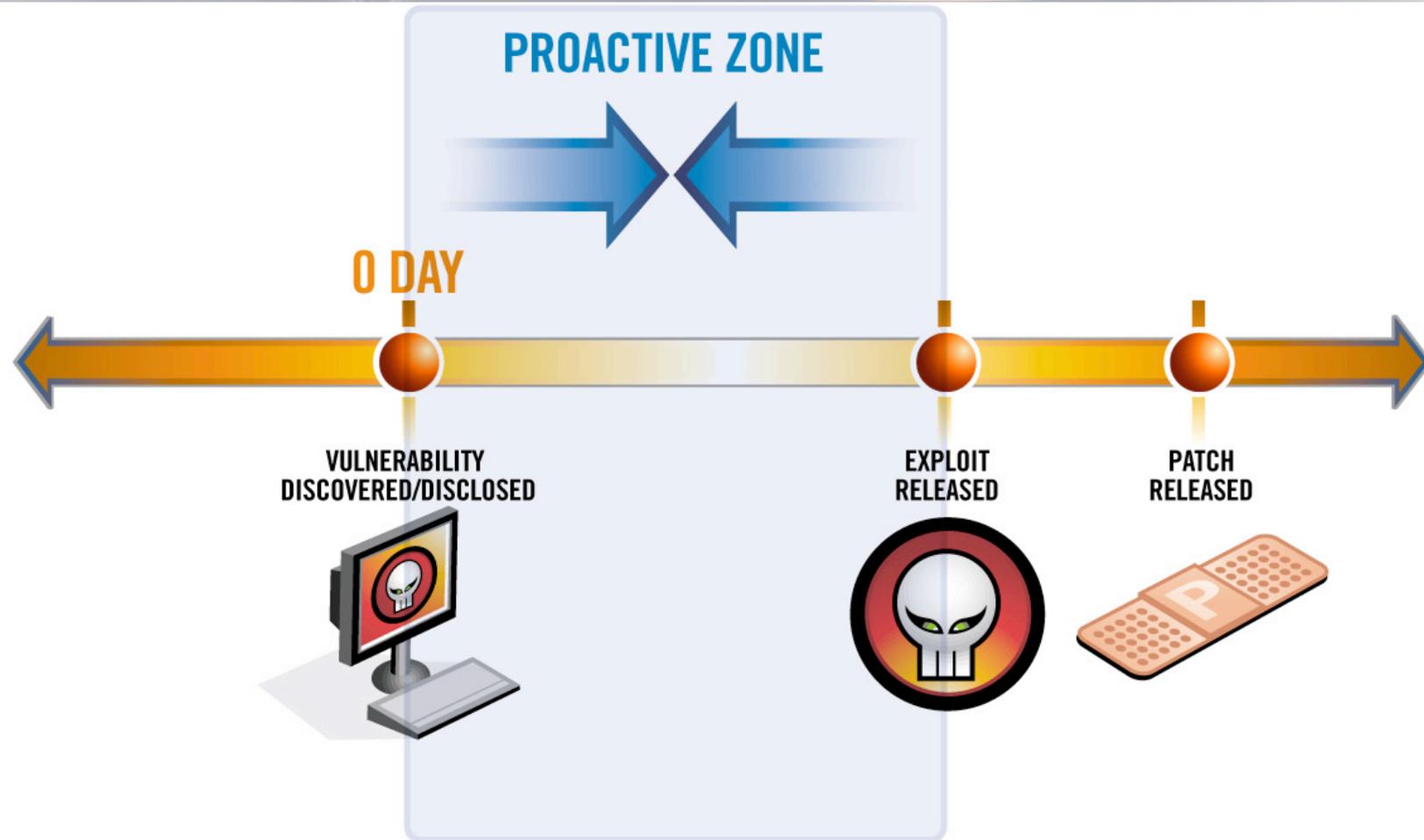
# Zero-Day Protection - Zero-Day Threats



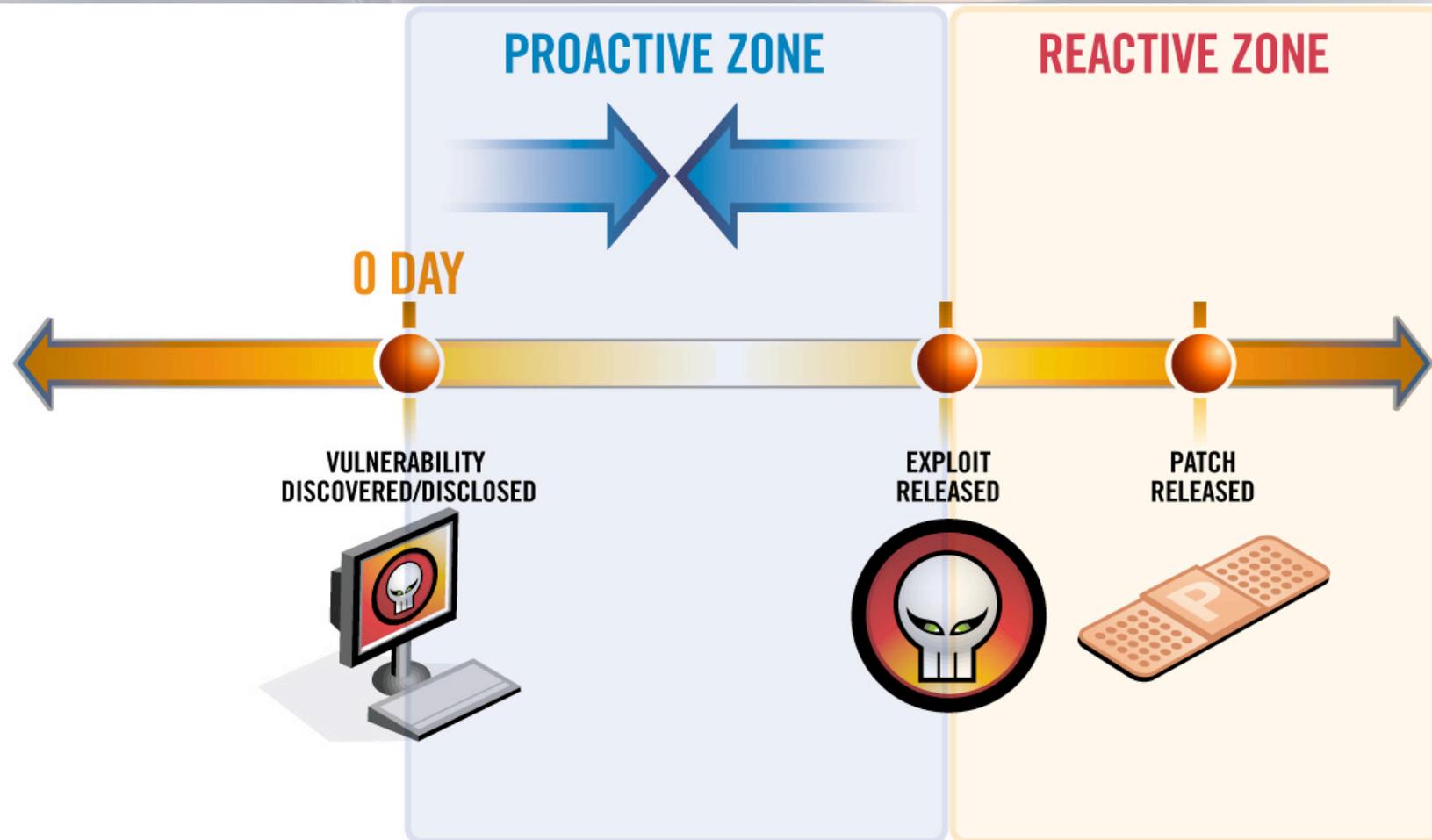
# Zero-Day Protection - Zero-Day Threats



# Zero-Day Protection - Zero-Day Threats



# Zero-Day Protection - Zero-Day Threats



# Zero-Day Protection - Zero-Day Threats



# Zero-Day Protection - Zero-Day Threats



# Blaster Chronology

- **July 1999:** X Force 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

# “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

# Sasser: "Trans Request"

The screenshot shows the Sasser - Ethereal application window. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The main pane displays a tree view of network layers for Frame 57 (1514 bytes on wire, 1514 bytes captured):

- ▶ Ethernet II, Src: 00:0d:61:0a:c1:ec, Dst: 00:20:ed:69:e4:9c
- ▶ Internet Protocol, Src Addr: 192.168.1.10 (192.168.1.10), Dst Addr: 192.168.1.20 (192.168.1.20)
- ▶ Transmission Control Protocol, Src Port: 3461 (3461), Dst Port: microsoft-ds (445), Seq: 8
- ▶ NetBIOS Session Service
- ▼ SMB (Server Message Block Protocol)
  - ▶ SMB Header
  - ▶ Trans Request (0x25)
- ▶ SMB Pipe Protocol
- ▶ DCE RPC
- ▶ Microsoft Local Security Architecture (Directory Services), DsRolerUpgradeDownlevelServer

Below the tree view is a hex dump of the packet data. The highlighted row (00a0) shows the following hex values: 00 00 00 00 09 00 ec 03 00 00 00 00 00 00 ec 03. The corresponding ASCII representation is: ..... . . . . .

0000	00	20	ed	69	e4	9c	00	0d	61	0a	c1	ec	08	00	45	00	. . .i . . . . .	a . . . . . E .
0010	05	dc	6a	8a	40	00	80	06	07	23	c0	a8	01	0a	c0	a8	..j.@. . . . # . . . . .	
0020	01	14	0d	85	01	bd	01	6f	89	c0	d9	8e	ff	5c	50	10	.....o . . . . . \P .	
0030	fc	e5	25	c2	00	00	00	00	0c	f4	ff	53	4d	42	25	00	..%. . . . . . . . . . SMB%. . . . .	
0040	00	00	00	18	07	c8	00	00	00	00	00	00	00	00	00	00	..... . . . . . . . . . .	
0050	00	00	00	08	dc	04	00	08	60	00	10	00	00	a0	0c	00	..... . . . . . . . . . .	
0060	00	00	04	00	00	00	00	00	00	00	00	00	00	00	00	54	..... . . . . . . . . . . T . . . . .	
0070	00	a0	0c	54	00	02	00	26	00	00	40	b1	0c	10	5c	00	...T...& ..@... \ . . . . .	
0080	50	00	49	00	50	00	45	00	5c	00	00	00	00	00	05	00	P.I.P.E. \ . . . . .	
0090	00	03	10	00	00	00	a0	0c	00	00	01	00	00	00	88	0c	..... . . . . . . . . . .	
00a0	00	00	00	00	09	00	ec	03	00	00	00	00	00	00	ec	03	..... . . . . . . . . . .	
00b0	00	00	90	90	90	90	90	90	90	90	90	90	90	90	90	90	..... . . . . . . . . . .	

# Korgo: "Write AndX Request"

The screenshot shows the Korgo - Ethereal interface. The packet list pane displays the following details for Frame 80:

- Frame 80 (1514 bytes on wire, 1514 bytes captured)
- Ethernet II, Src: 00:0d:61:0e:80:57, Dst: 00:0d:61:11:81:87
- Internet Protocol, Src Addr: 192.168.16.21 (192.168.16.21), Dst Addr: 192.168.16.18 (192.168.16.18)
- Transmission Control Protocol, Src Port: 2669 (2669), Dst Port: microsoft-ds (445), Seq: 8
- NetBIOS Session Service
- SMB (Server Message Block Protocol)
  - SMB Header
  - Write AndX Request (0x2f)
- DCE RPC
- Microsoft Local Security Architecture (Directory Services), DsRolerUpgradeDownlevelServer

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column contains the text: ..a..... a..W..E. ....@... L..... .m.... .U.t..P. A@j .... ...SMB/. .....

# 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

# 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



*For More Information*

- **www.iss.net**
- **Proventia Products that fight phishing**
  - [www.iss.net/resources/phishing.php](http://www.iss.net/resources/phishing.php)
- **Free 30-day download of ISS products**
  - [www.iss.net/antispam](http://www.iss.net/antispam)



*Thank you !*

