Crime On The Internet

Dealing With Spyware, Botnets And Other Cyber Attacks

David Aucsmith
Senior Director
Institute for Advanced Technology in Governments
Microsoft Corporation
awk@microsoft.com

On The Front Line

Our Products

- 80% of world's critical infrastructures
- Determined, resourceful, global adversaries

msn

Our Business

- Subject to Phishing, Bots, Root-kits, …

Our Resources

- Attacked > 4,000 times a day
- At least one DDoS a day
- Logged attacks from every country


Hacking

Short History of “Hacking”

Short History of "Hacking"

Mainframes

80s

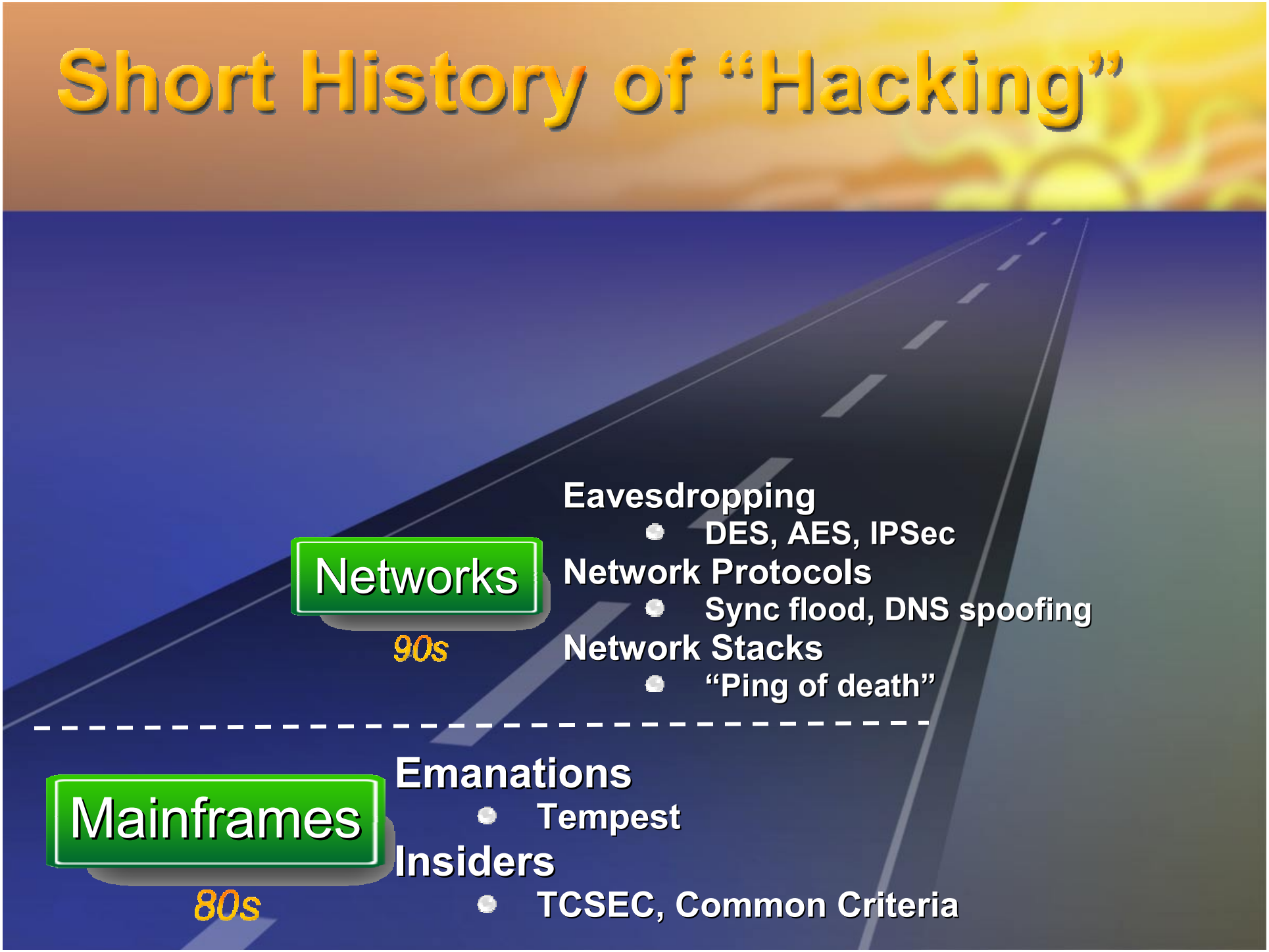
Emanations

- Tempest

Insiders

- TCSEC, Common Criteria

Short History of "Hacking"



Networks

90s

Eavesdropping
- DES, AES, IPSec

Network Protocols
- Sync flood, DNS spoofing

Network Stacks
- "Ping of death"

Mainframes

80s

Emanations
- Tempest

Insiders
- TCSEC, Common Criteria

Short History of "Hacking"

Services — *00s*

- **Operating System Services**
  - Buffer overruns, XSS
  - Web spoofs, worms
- **Application Services**
  - SQL injection, SQL Slammer
  - Media players

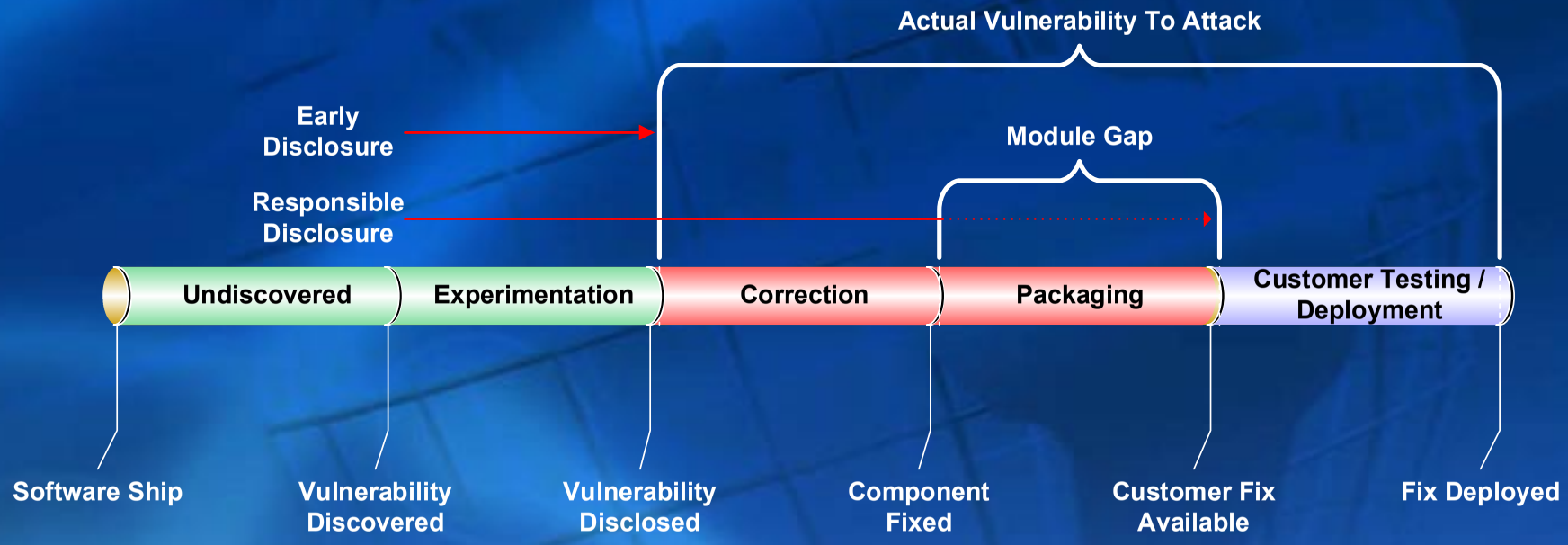
Networks — *90s*

- **Eavesdropping**
  - DES, AES, IPSec
- **Network Protocols**
  - Sync flood, DNS spoofing
- **Network Stacks**
  - "Ping of death"

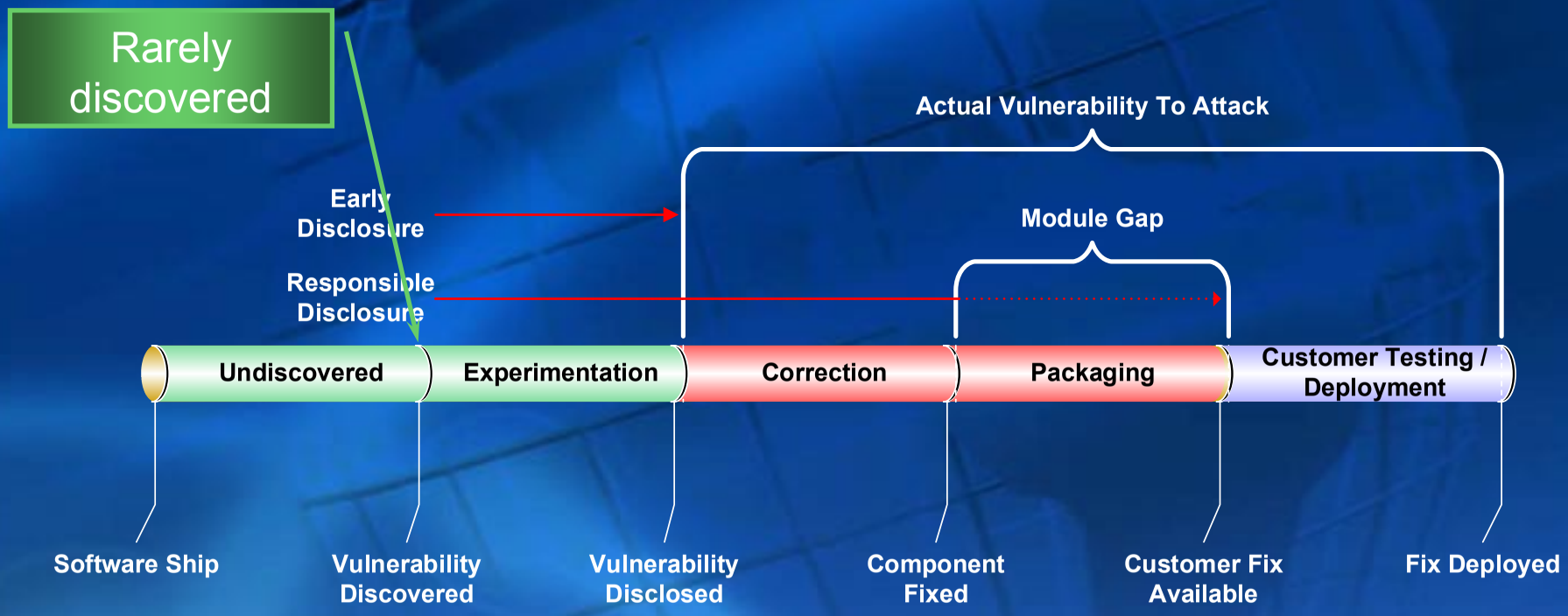
Mainframes — *80s*

- **Emanations**
  - Tempest
- **Insiders**
  - TCSEC, Common Criteria

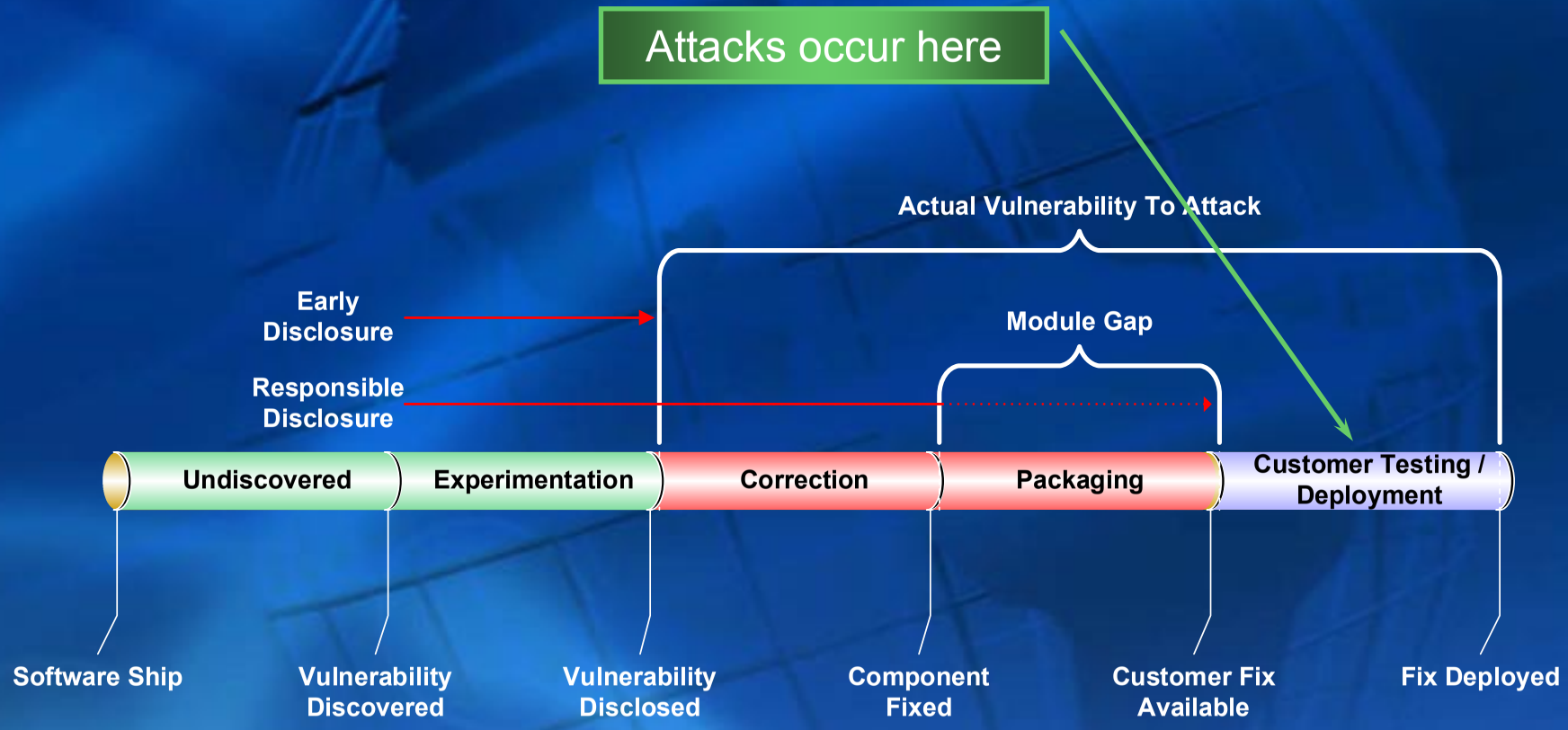
Vulnerability Timeline



Vulnerability Timeline

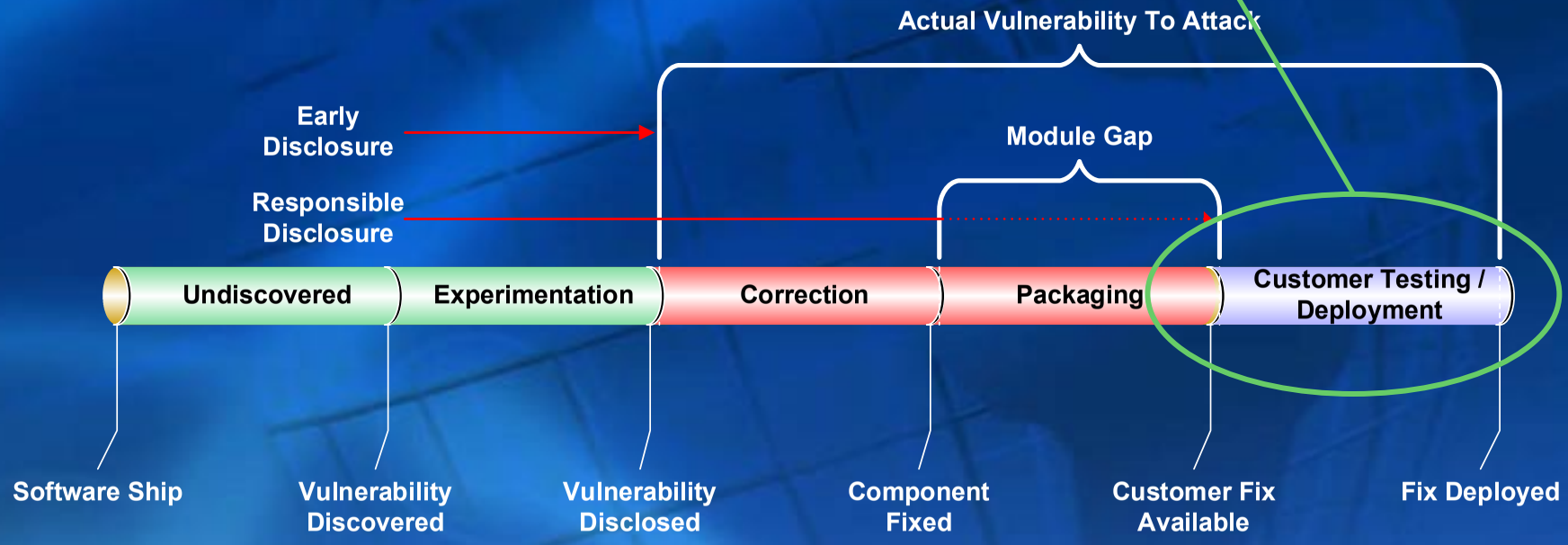


Vulnerability Timeline

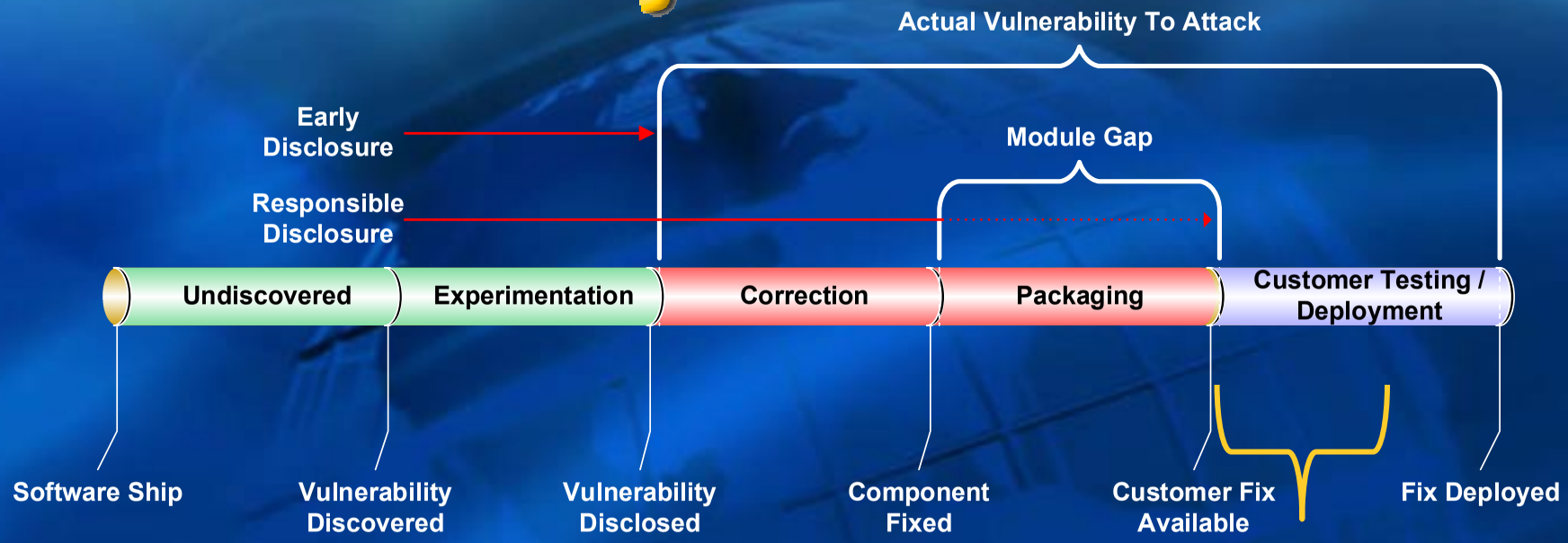


Vulnerability Timeline

Why does this gap exist?

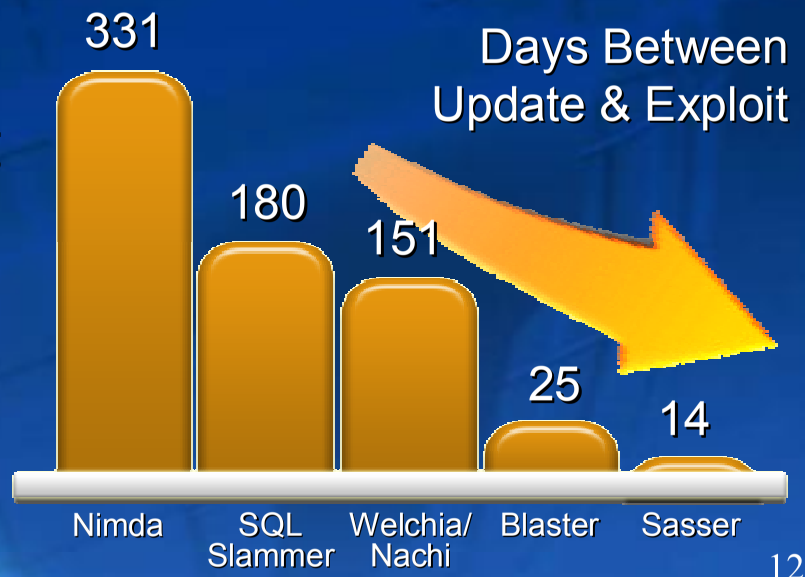


Vulnerability Timeline



- Days From Patch To Exploit
  - Have decreased so that patching is not a defense in large organizations
  - Average 6 days for patch to be reverse engineered to identify vulnerability

Source: Microsoft



The Forensics of a Virus

July 1	July 16	July 25	Aug 11
Vulnerability reported to us / Patch in progress	**Bulletin & patch available No exploit**	**Exploit code in public**	**Worm in the world**

Report

- Vulnerability in RPC/DDOM reported
- MS activated highest level emergency response process

Bulletin

- MS03-026 delivered to customers (7/16/03)
- Continued outreach to analysts, press, community, partners, government agencies

Exploit

- X-focus (Chinese group) published exploit tool
- MS heightened efforts to get information to customers

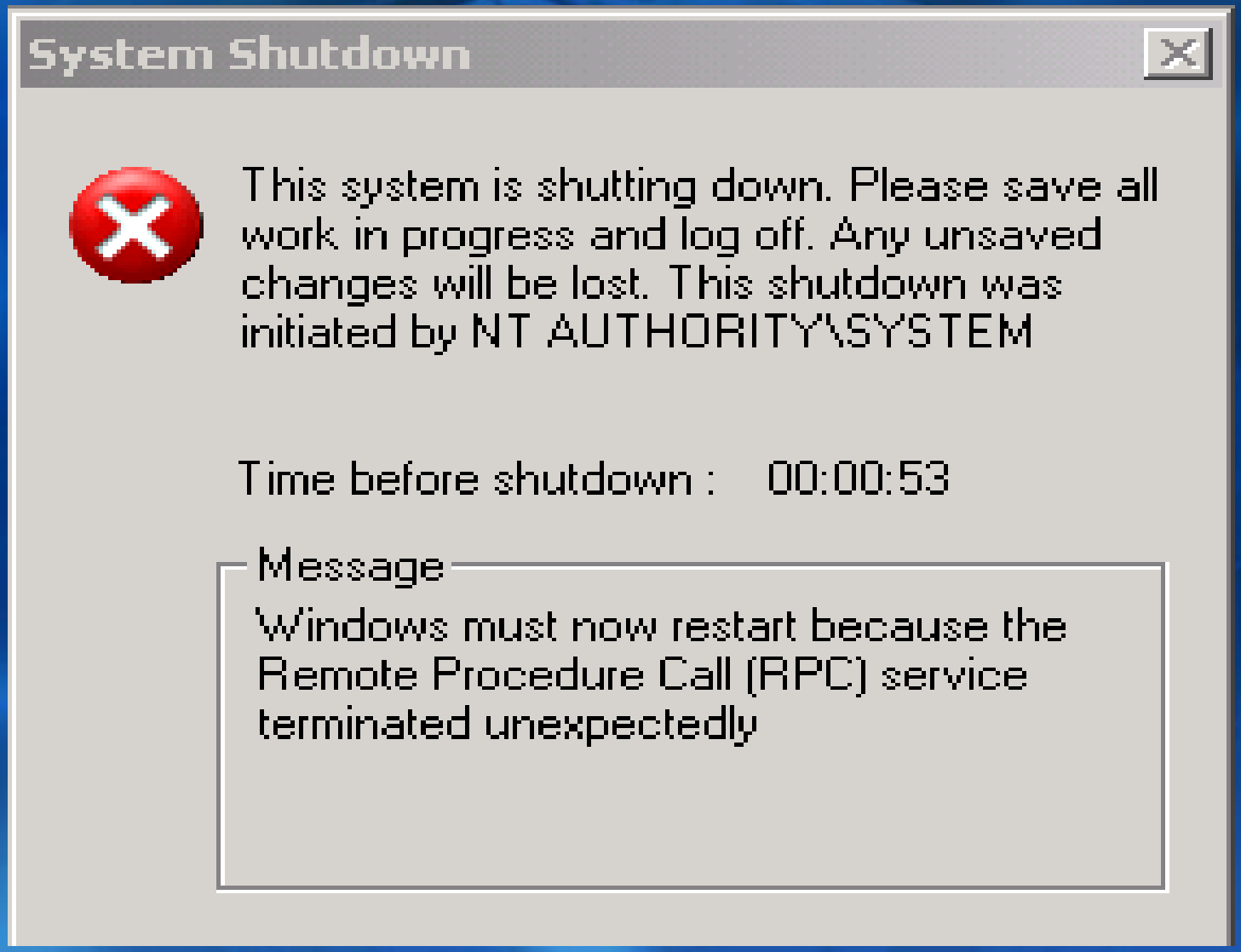
Worm

- Blaster worm discovered –; variants and other viruses hit simultaneously (i.e. "SoBig")

Blaster shows the complex interplay between security researchers, software companies, and hackers

Source: Microsoft

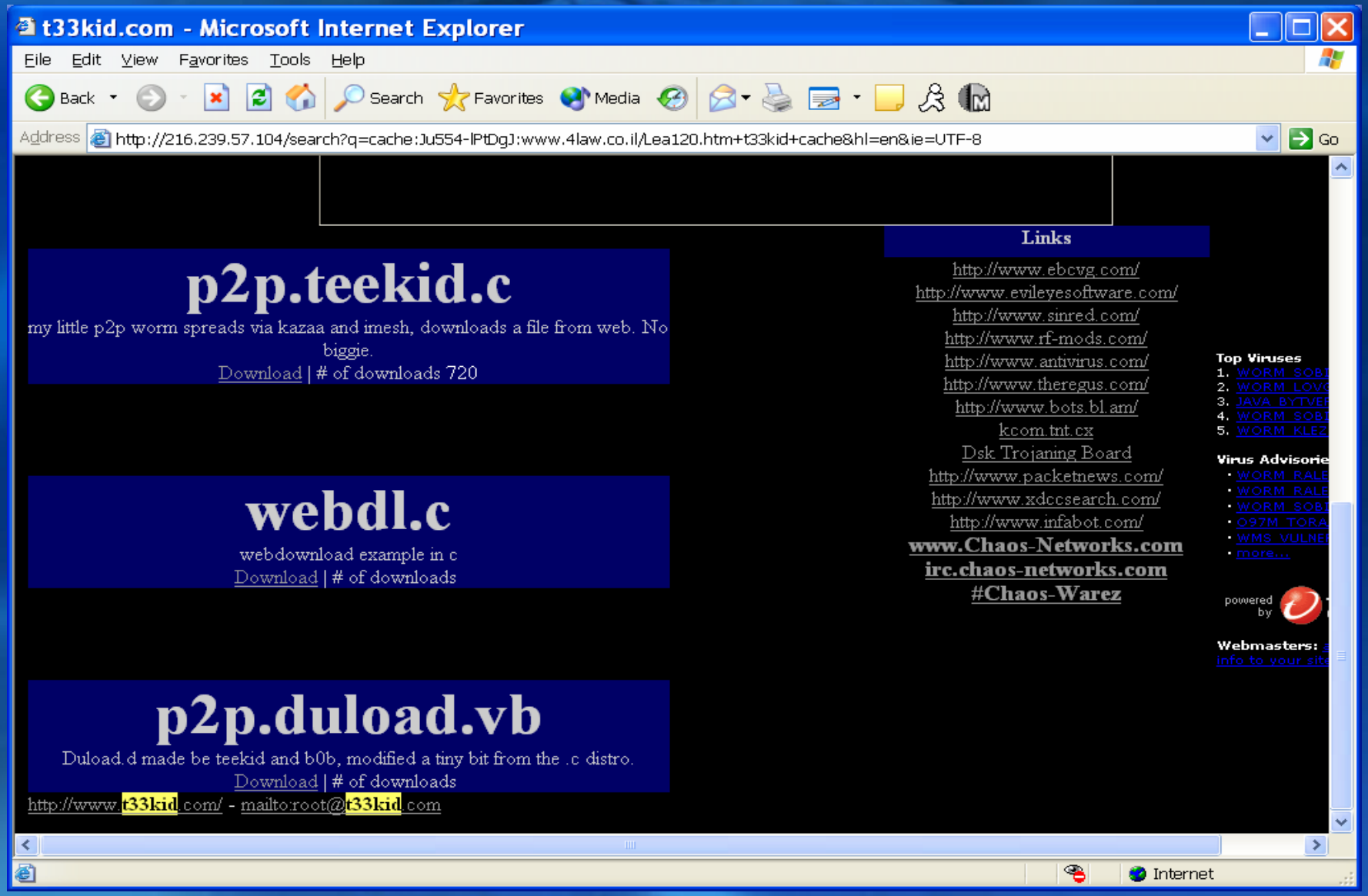
OCA


System Shutdown
This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM
Time before shutdown : 00:00:53
Message
Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly

Investigation

- Analysis of code led us to t33kid.com
  - FBI/USSS watched and gathered intelligence
- Real-time Subpoena
  - ISP Cari.net in San Diego (issued by on call AUSA)
- Virtual host led to Texas
- Owner of site in Texas
  - Had criminal record
  - Was potential suspect
- T33kid.com leased space from Texas owner
- Investigative work led us to Jeffrey Lee Parson
  - Seven computers seized

Investigation



The Forensics of Exploits

"Less than 24 hours after Microsoft released its Security Bulletins for August, exploit code was made publicly available for the vulnerabilities addressed in Microsoft Security Bulletin MS05-038 and MS05-041. The postings, titled 'Microsoft Internet Explorer COM Objects Instantiation Exploit (MS05-038)' and 'Microsoft Windows Remote Desktop Protocol DoS Exploit (MS05-041),' were published by the French security firm FrSIRT. A second piece of code was published on August 11th for MS05-038."

"Three pieces of exploit code targeting the Windows Plug and Play issue (MS05-039) have been made publicly available. These are listed as the 'Microsoft Windows Plug and Play Remote Buffer Overflow Exploit (MS05-039)', 'Microsoft Windows 2000 Plug and Play Universal Remote Exploit (MS05-039)' and 'Microsoft Windows 2000 Plug and Play Universal Remote Exploit #2 (MS05-039)' on the FrSIRT Web site. One of which has also been included as an exploit module in the Metasploit Framework."

"Authorities in Morocco and Turkey have arrested two people believed to be responsible for unleashing a computer worm that infected networks at U.S. companies and government agencies earlier this month, the FBI said Friday.

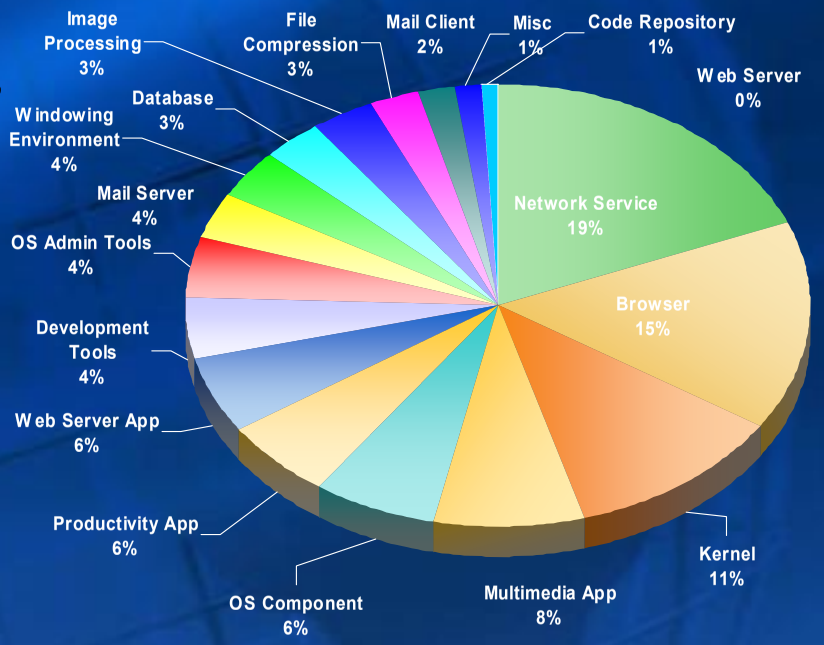
…

Microsoft played a role in locating the suspects, the FBI said." http://www.msnbc.msn.com/id/9086742/

Exploit Statistics - 2005 (YTD)

- Answers "Where are the greatest risks?"
- Exploits written in 2005 for 6 popular Operating Systems
  - Win32
  - Linux (4 distributions)

Exploits written 2005 YTD - all platforms



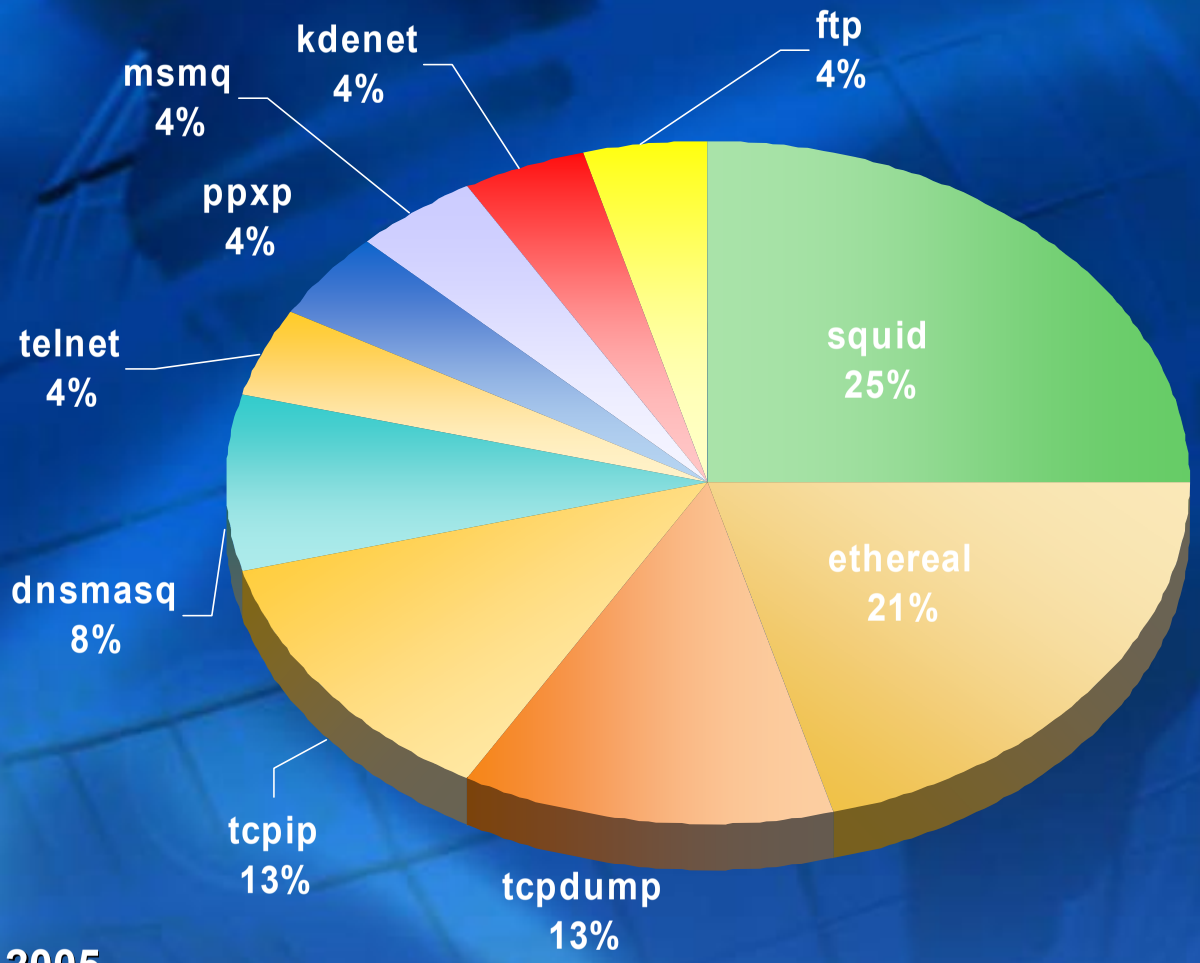
2005 Vulns and Exploits (YTD)

	Vulns	Exploitable	Trivial
Total	344	96	61

Thru May 31, 2005

Exploit Statistics - 2005 (YTD)

Network service

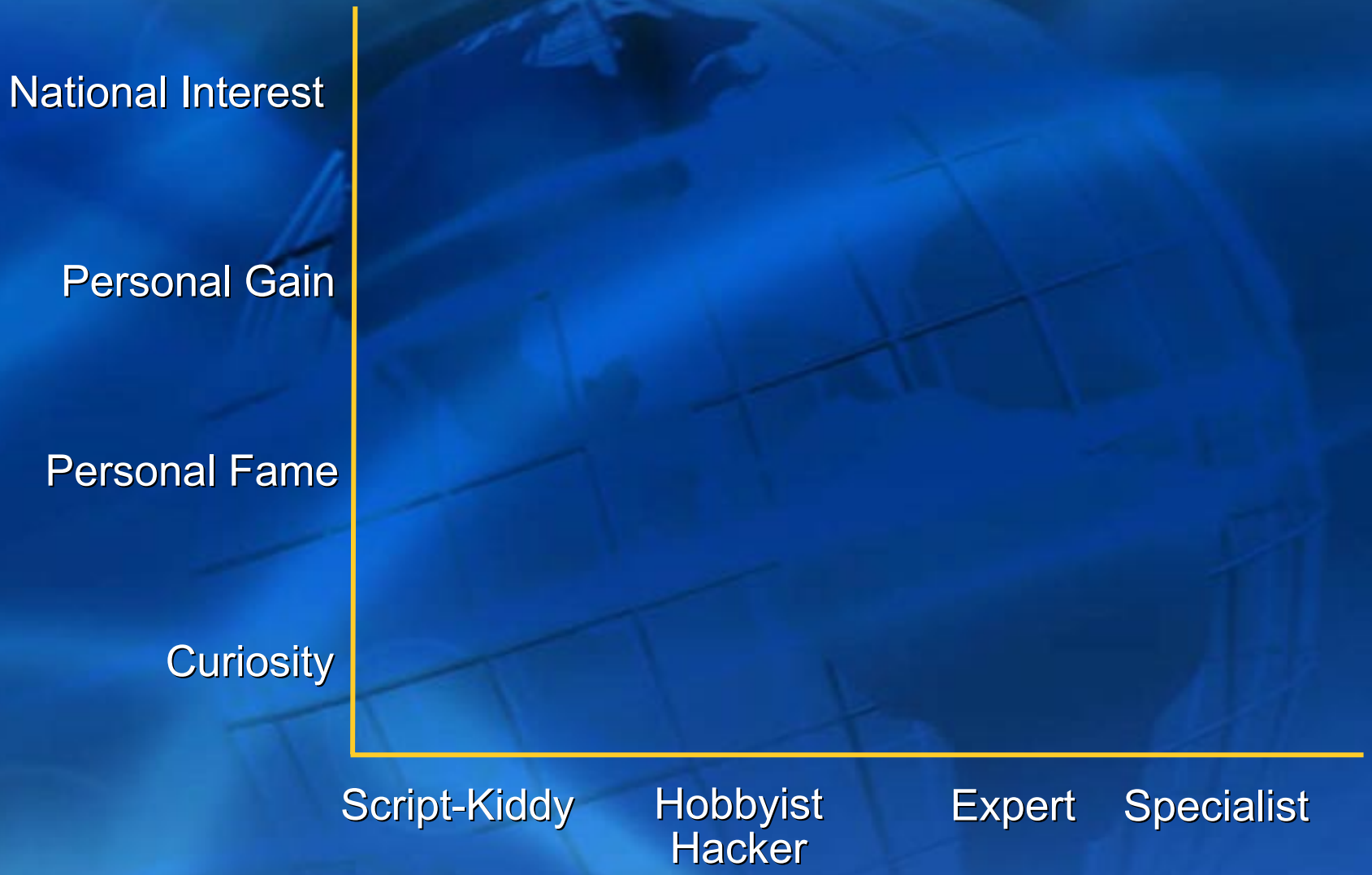


Thru May 31, 2005

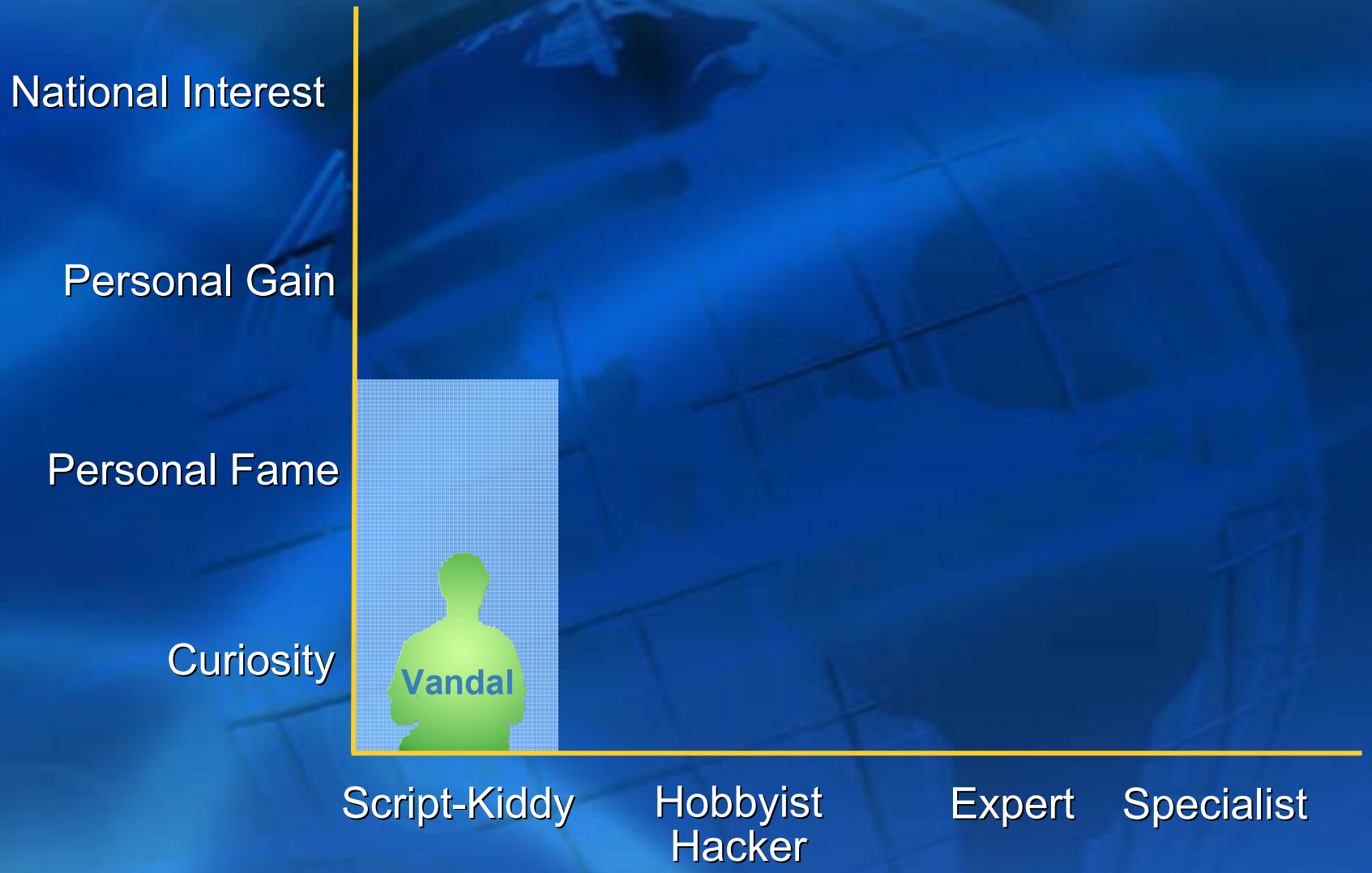
Understanding the Landscape

Understanding the Landscape

Understanding the Landscape



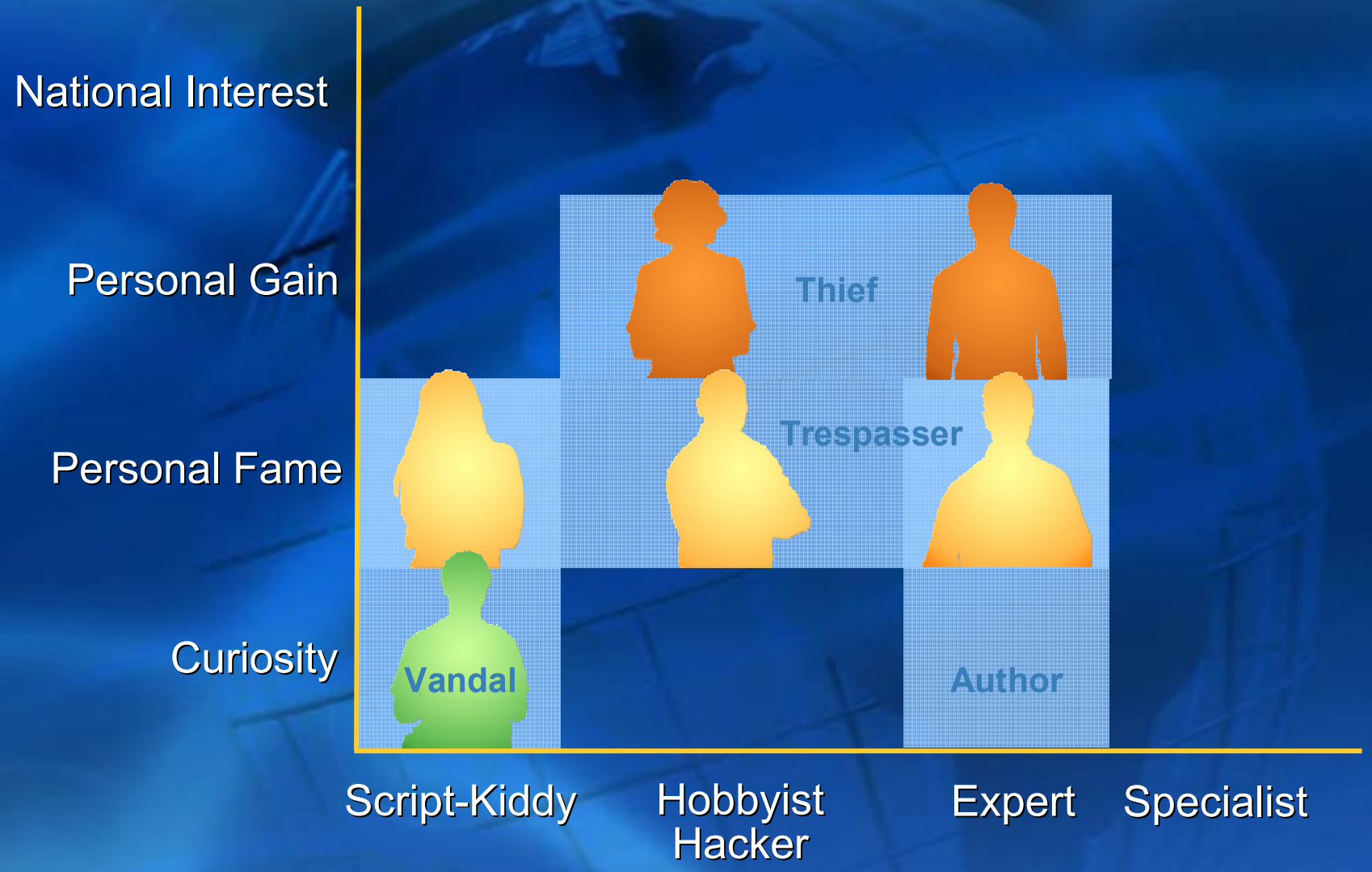
Understanding the Landscape



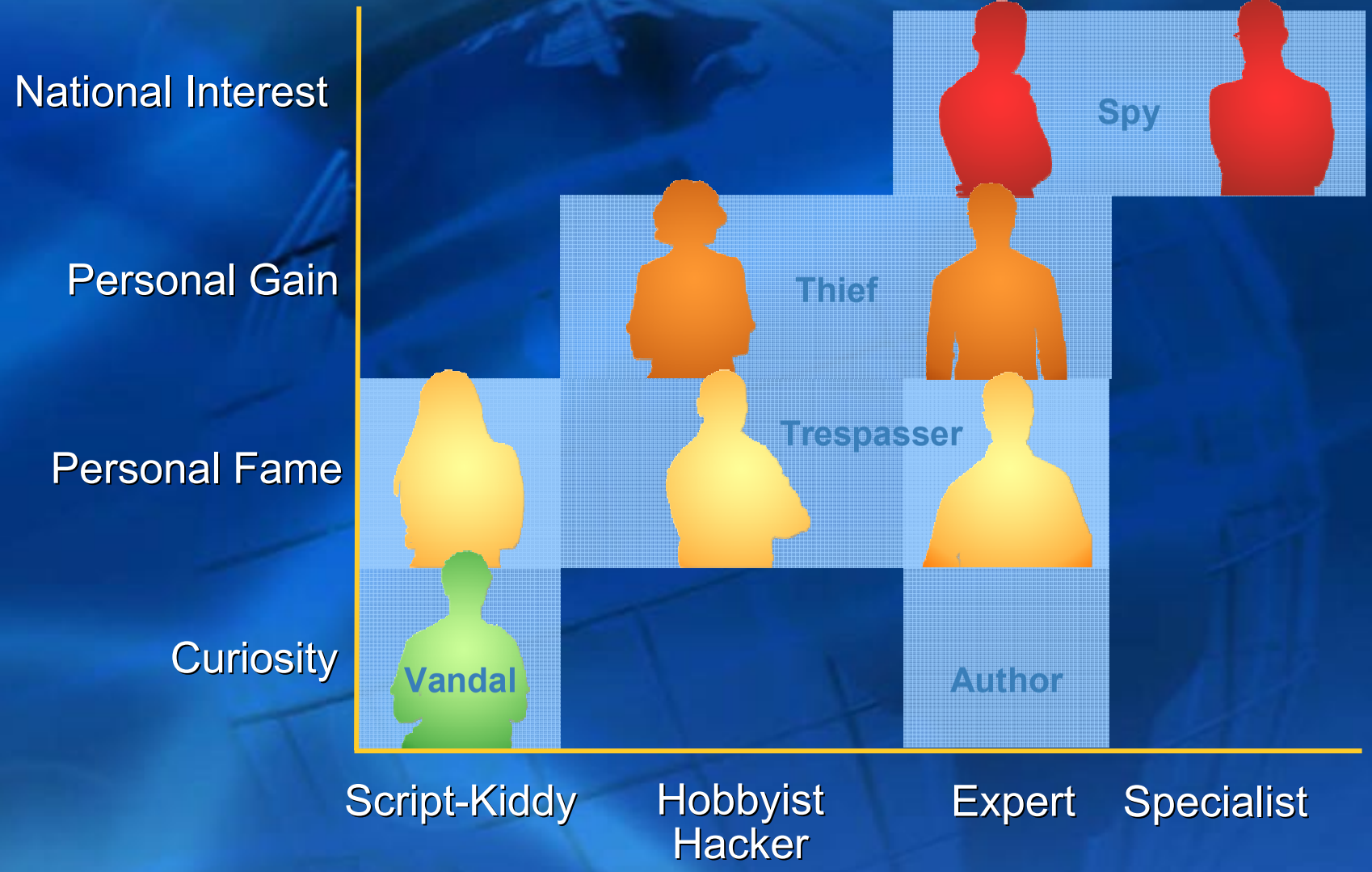
Understanding the Landscape

Understanding the Landscape

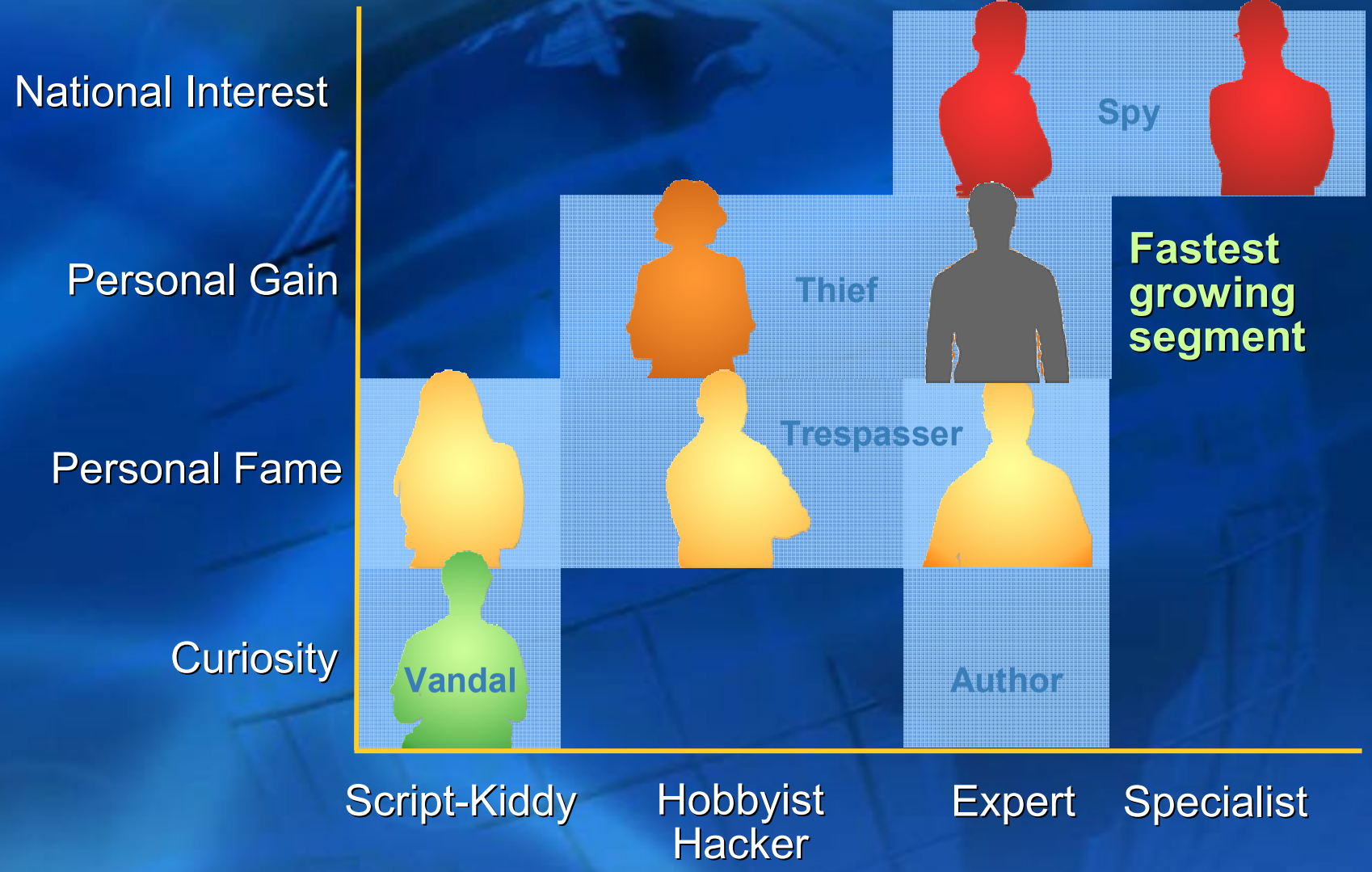
Understanding the Landscape



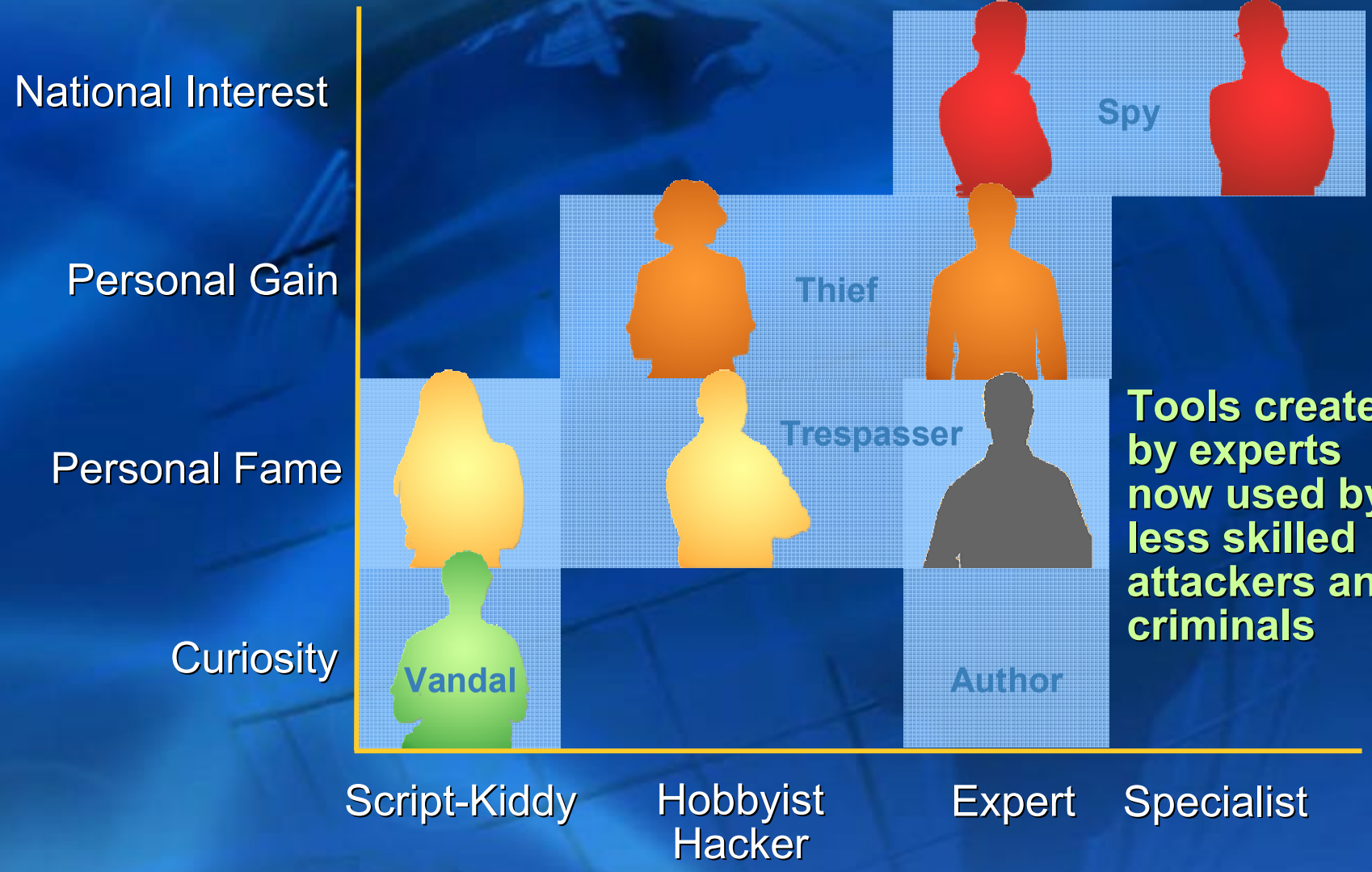
Understanding the Landscape



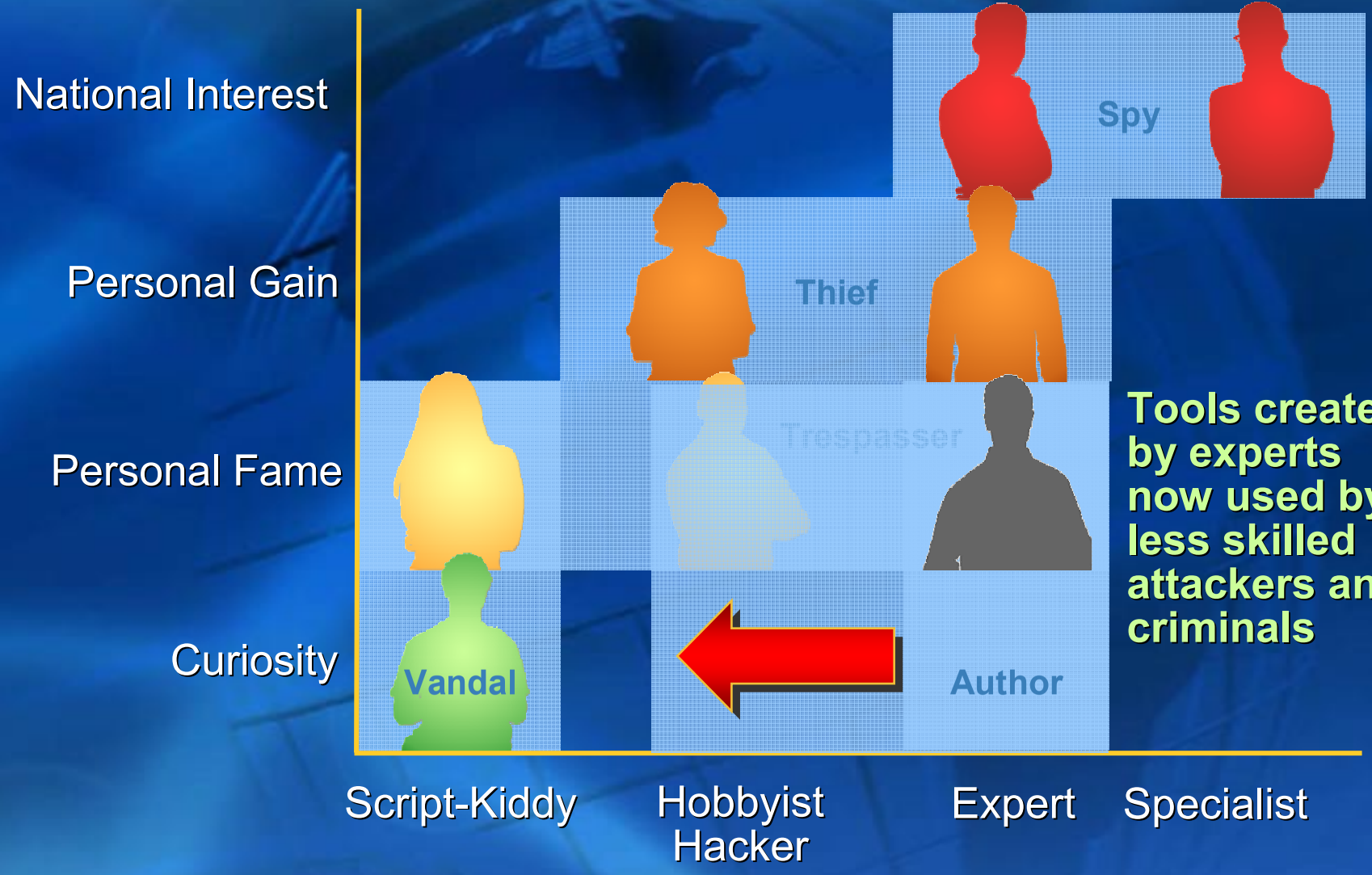
Understanding the Landscape



Understanding the Landscape



Understanding the Landscape



Understanding the Landscape

Legacy

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

1990

2005

Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004

1990

2005

Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

32-bit 2.5 GHz processor
250 GByte disk
3 GByte ram
DVD R/W drive
21” digital monitor

1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004

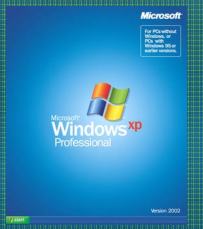
1990

2005

Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

Windows XP SP2
ICF
USB
UPnP
Windows Update



16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

32-bit 2.5 GHz processor
250 GByte disk
3 GByte ram
DVD R/W drive
21” digital monitor

1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004

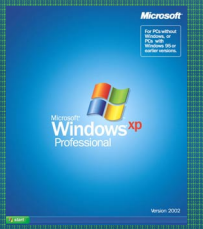
1990

2005

Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

Windows XP SP2
ICF
USB
UPnP
Windows Update



Legacy creates security issues

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

32-bit 2.5 GHz processor
250 GByte disk
3 GByte ram
DVD R/W drive
21” digital monitor

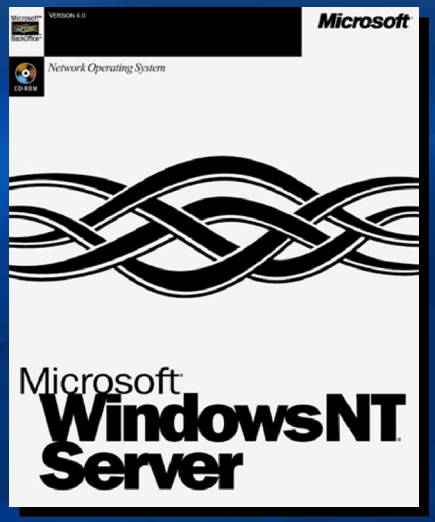
1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004

1990

2005

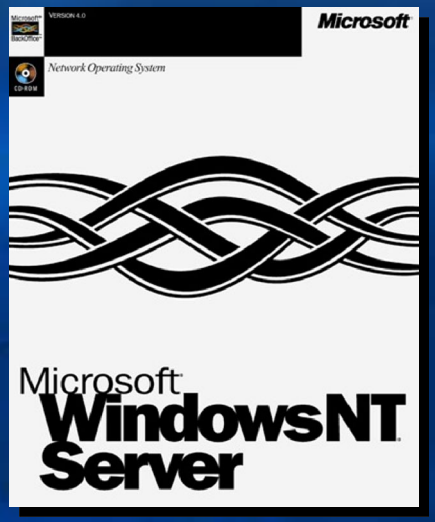
Keeping It In Perspective

- The security kernel of Windows NT was written:
  - Before there was a World Wide Web
  - Before TCP/IP was the default communications protocol

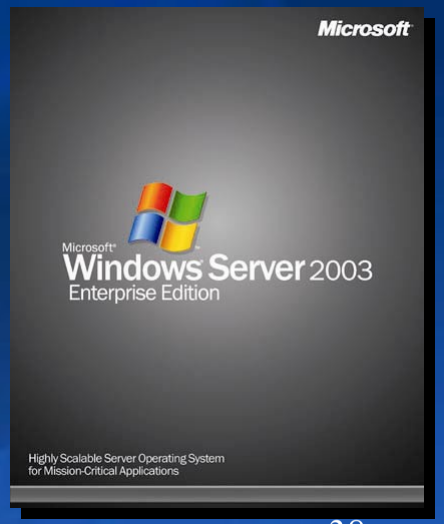


Keeping It In Perspective

- The security kernel of Windows NT was written:
  - Before there was a World Wide Web
  - Before TCP/IP was the default communications protocol



- The security kernel of Windows Server 2003 was written:
  - Before buffer overflow tool kits were available
  - Before Web Services were widely deployed



Honey Pot Projects

- Six computers attached to Internet
  - Different versions of Windows, Linux and Mac OS

Honey Pot Projects

- Six computers attached to Internet
  - Different versions of Windows, Linux and Mac OS
- Over the course of one week
  - Machines were scanned 46,255 times
  - 4,892 direct attacks

Honey Pot Projects

- Six computers attached to Internet
  - Different versions of Windows, Linux and Mac OS
- Over the course of one week
  - Machines were scanned 46,255 times
  - 4,892 direct attacks
- No up-to-date, patched operating systems succumbed to a single attack

Honey Pot Projects

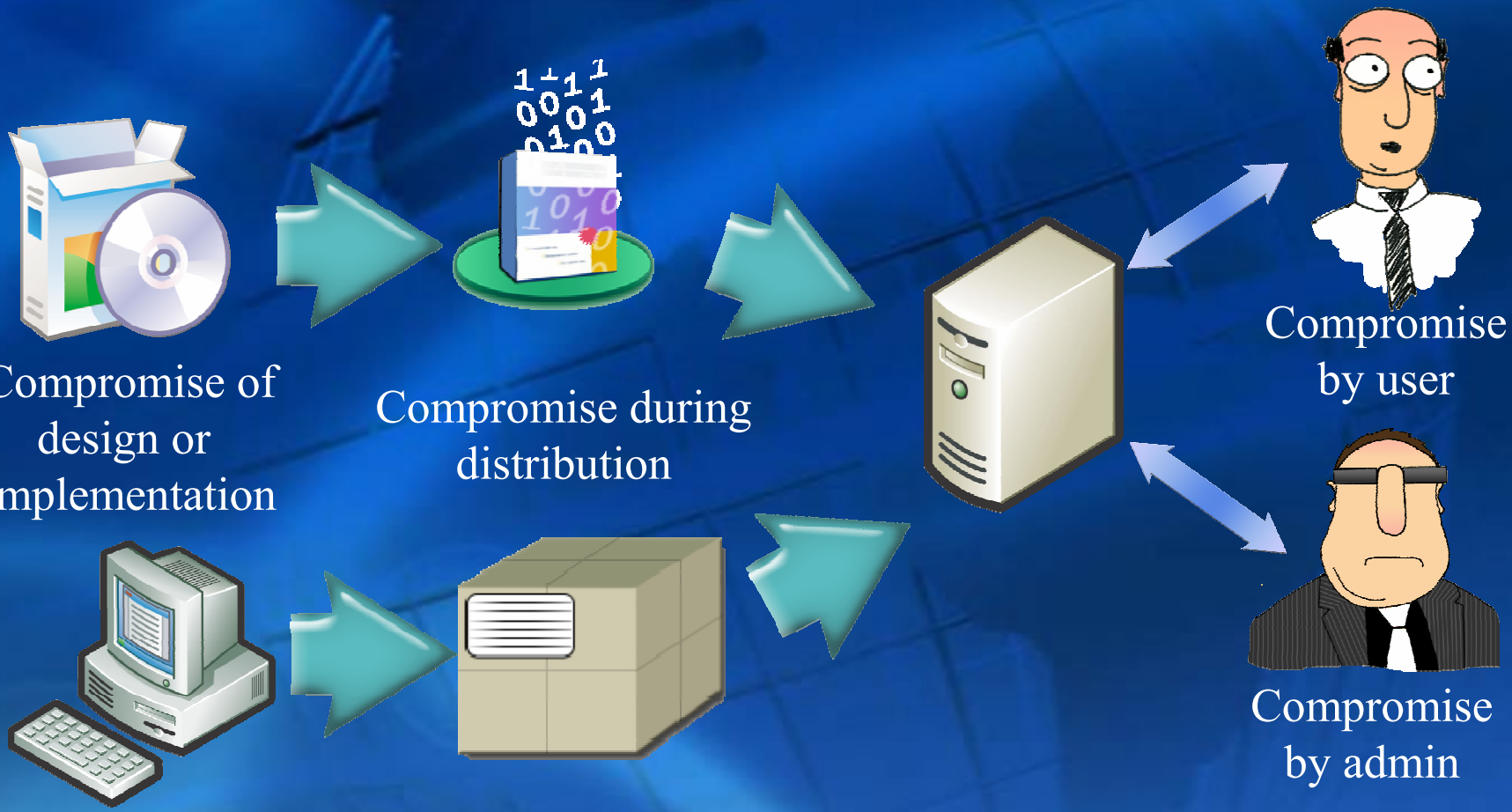
- Six computers attached to Internet
  - Different versions of Windows, Linux and Mac OS
- Over the course of one week
  - Machines were scanned 46,255 times
  - 4,892 direct attacks
- No up-to-date, patched operating systems succumbed to a single attack
- All down rev systems were compromised
  - Windows XP with no patches
  - Infested in 18 minutes by Blaster and Sasser
  - Within an hour it became a "bot"

Source: StillSecure,
see http://www.denverpost.com/Stories/0,1413,36~33~2735094,00.html

Insiders and Outsiders

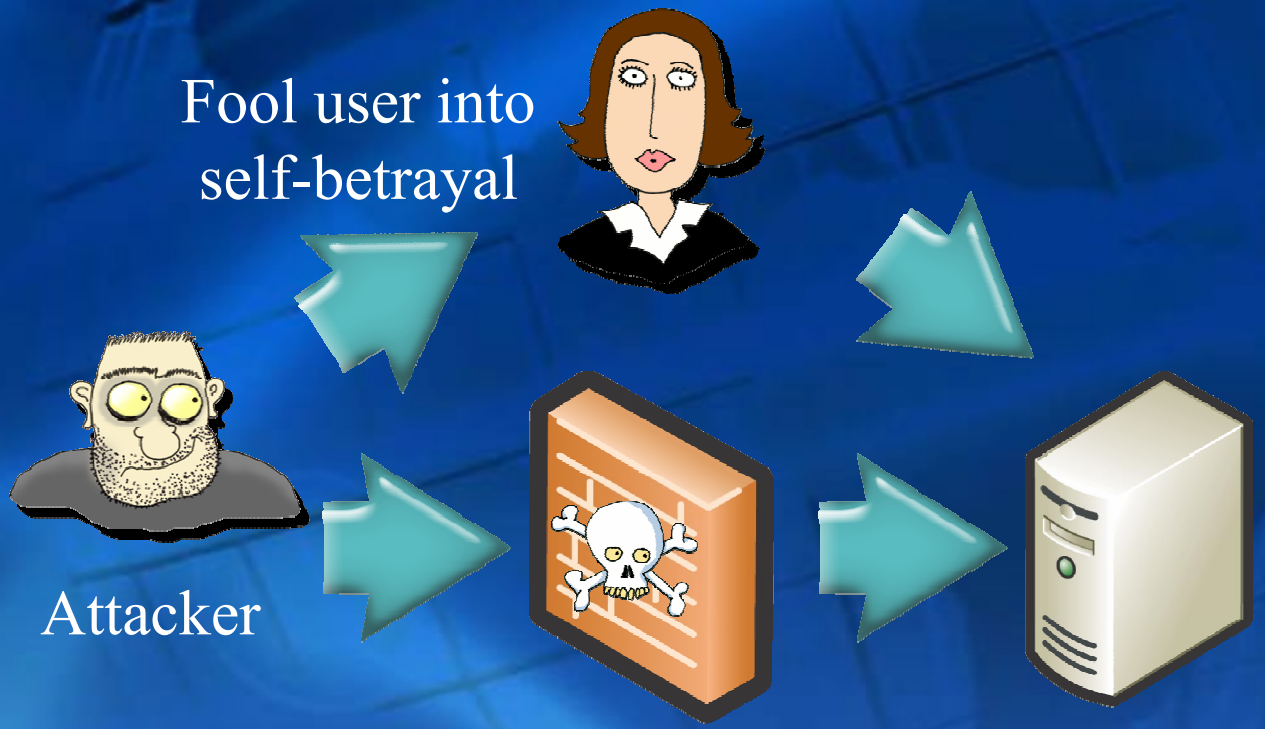
Trusted Insider

- Compromise of security by trusted party
  - Traditional domain of TCSEC and Common Criteria



Un-trusted Outsider

- Traditional “hacker”
  - Asynchronous network attack via vulnerability
  - User self-betrayal



Attack Automation

- Malware
  - Spam, phishing, worms, bots, …
- Asymmetric
  - Attacker need only find one victim
  - Defender needs to protect all
- Force multiplier
  - Write once, attack all
- Harvest
  - Harvest the “interesting” successes


Spam

Spam

- Mass unsolicited email
- For commerce
  - Direct mail advertisement
- For Web traffic
  - Artificially generated Web traffic
  - Harassment
- For fraud
  - Phishing
  - Identity theft
  - Credential theft

An Affiliates Program

- “Our first program pays you $0.50 for every validated free-trial registrant your website sends to [bleep]. Commissions are quick and easy because we pay you when people sign up for our three-day free-trial. Since [bleep] doesn't require a credit card number or outside verification service to use the free trial, generating revenue is a snap.

  The second program we offer is our pay per sign-up plan. This program allows you to earn a percentage on every converted (paying) member who joins [bleep]. You could make up to 60% of each membership fee from people you direct to join the site.

  Lastly, [bleep] offers a two tier program in addition to our other plans. If you successfully refer another webmaster to our site and they open an affiliate account, you begin earning money from their traffic as well! The second tier pays $0.02 per free-trial registrant or up to 3% of their sign-ups.”

An Affiliates Program

- "Our first program pays you $0.50 for every validated free-trial registrant your website sends to [bleep]. Commissions are quick and easy because we pay you when people sign up for our three-day free-trial. Since [bleep] doesn't require a credit card number or outside verification service to use the free trial, generating revenue is a snap.

  The second program we offer is our pay per sign-up plan. This program allows you to earn a percentage on every converted (paying) member who joins [bleep]. You could make up to 60% of each membership fee from people you direct to join the site.

  Lastly, [bleep] offers a two tier program in addition to our other plans. If you successfully refer another webmaster to our site and they open an affiliate account, you begin earning money from their traffic as well! The second tier pays $0.02 per free-trial registrant or up to 3% of their sign-ups."

Key Points

- $0.50 for every validated free-trial registrant
- 60% of each membership fee

Do the Math

- SoBig spammed over 100 million inboxes

Do the Math

- SoBig spammed over 100 million inboxes
- If 10% read the mail and clicked the link
  - = 10 million people

Do the Math

- SoBig spammed over 100 million inboxes
- If 10% read the mail and clicked the link
  - = 10 million people
- If 1% of people who went to site signed up for 3-days free trial
  - = (100,000 people) x ($0.50) = $50,000

Do the Math

- SoBig spammed over 100 million inboxes
- If 10% read the mail and clicked the link
  - = 10 million people
- If 1% of people who went to site signed up for 3-days free trial
  - = (100,000 people) x ($0.50) = $50,000
- If 1% of free trials sign up for 1 year
  - = (1,000 people) x ($144/yr) = $144,000/yr

An Affiliates Program

California Man Charged with Botnet Offenses
November 3, 2005

Botnets are big business ... U.S. case against an alleged computer hacker, who authorities believe netted $60,000 in cash and a BMW from a personal army of zombie computers.

Federal authorities arrested a 20-year-old California man Thursday and charged him with running a network of 400,000 compromised computers called a "botnet," including computers used by the U.S. government for national defense.

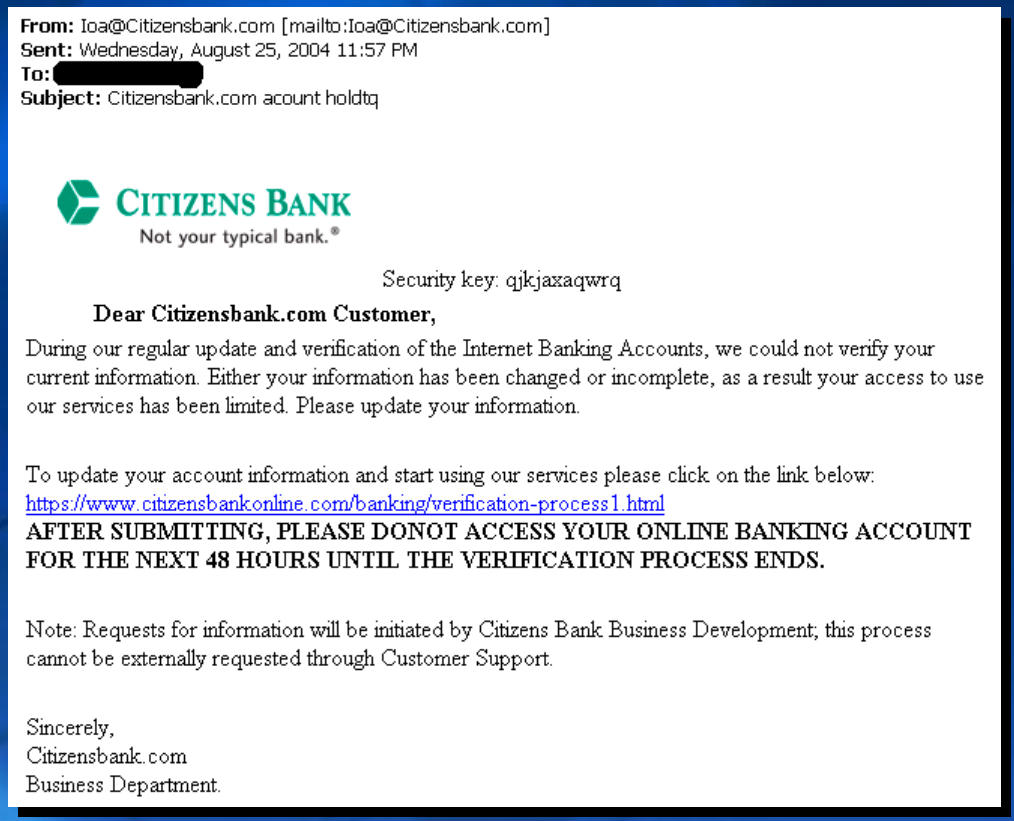
Ancheta was a member of affiliate networks used by unnamed "advertising service companies," who paid him around $60,000 to install their advertising software on the machines he controlled, the statement alleges.

Ancheta allegedly distributed software for Gammacash, of Quebec, and LoudCash, part of CDT of Montreal, which was purchased by 180 Solutions Inc. in April.


Phishing

Phishing

- **Faking**
  - An e-mail that seems to be from a legitimate source
- **Spoofing**
  - A Web site that appears to be "official"
- **Phishing**
  - Luring users to provide sensitive data



From: Ioa@Citizensbank.com [mailto:Ioa@Citizensbank.com]
Sent: Wednesday, August 25, 2004 11:57 PM
To: [redacted]
Subject: Citizensbank.com acount holdtq

CITIZENS BANK
Not your typical bank.®

Security key: qjkjaxaqwrq

Dear Citizensbank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

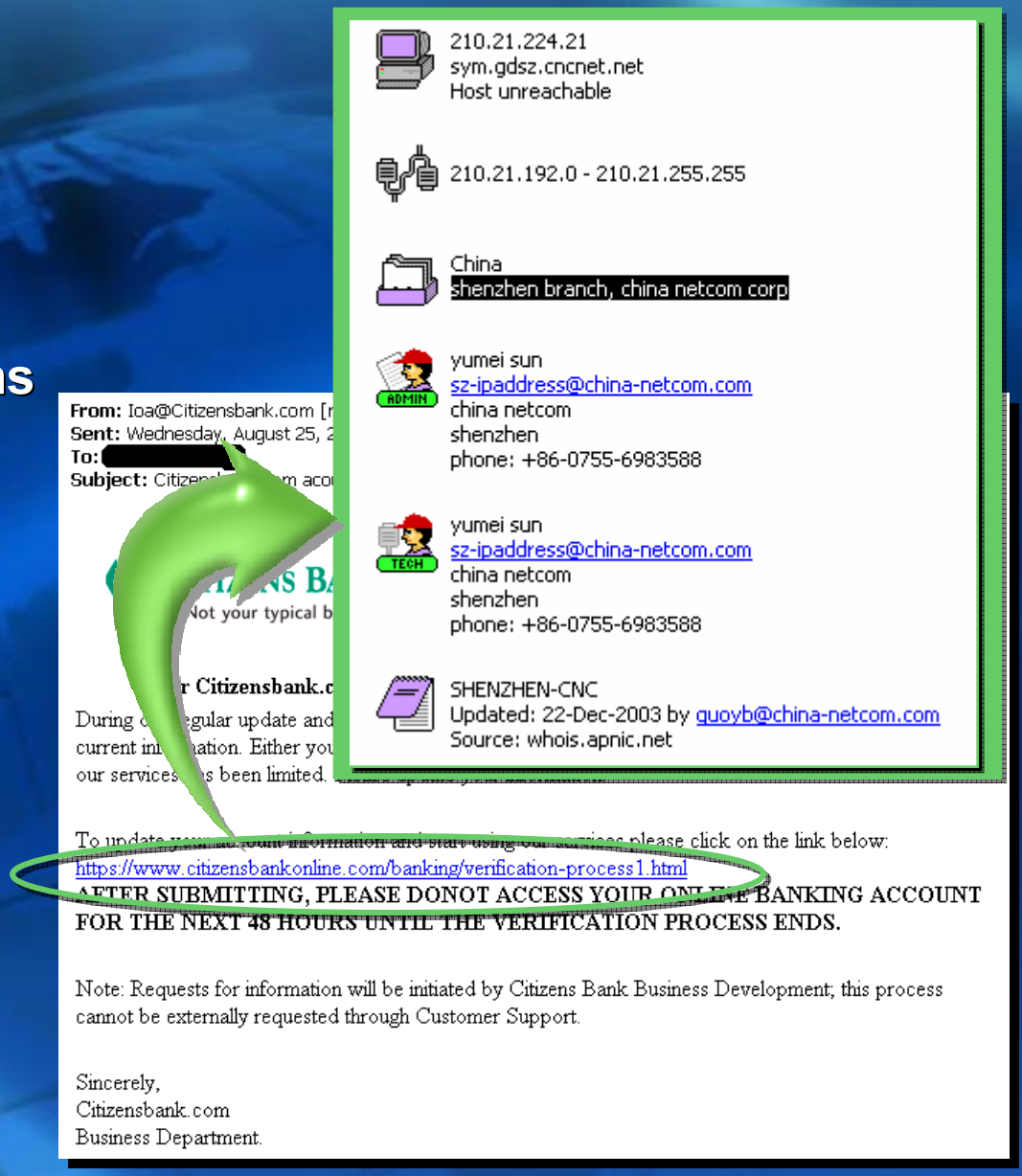
To update your account information and start using our services please click on the link below:
https://www.citizensbankonline.com/banking/verification-process1.html
AFTER SUBMITTING, PLEASE DONOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.

Note: Requests for information will be initiated by Citizens Bank Business Development; this process cannot be externally requested through Customer Support.

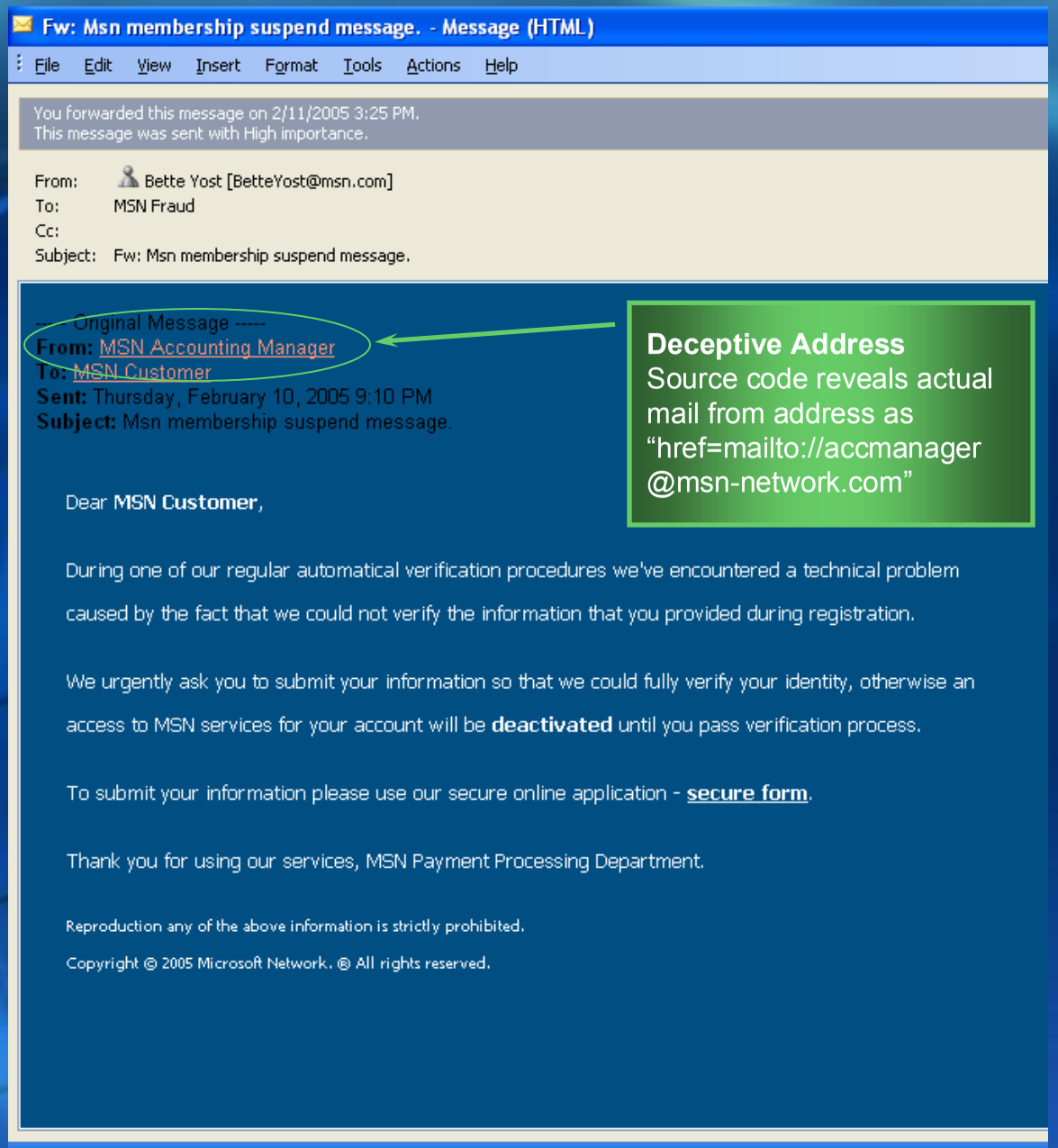
Sincerely,
Citizensbank.com
Business Department.

Phishing

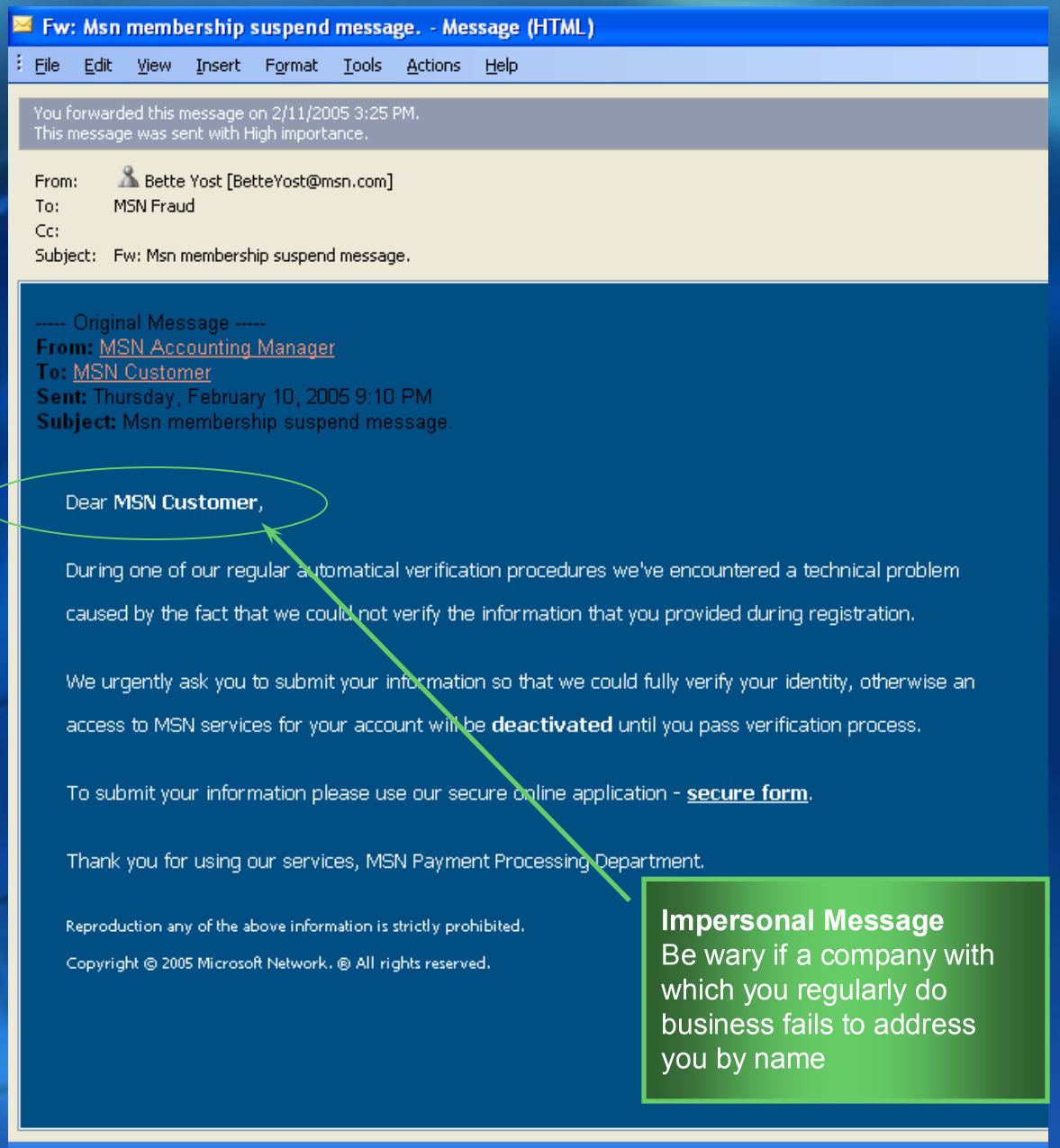
- **Faking**
  - An e-mail that seems to be from a legitimate source
- **Spoofing**
  - A Web site that appears to be "official"
- **Phishing**
  - Luring users to provide sensitive data



Phishing

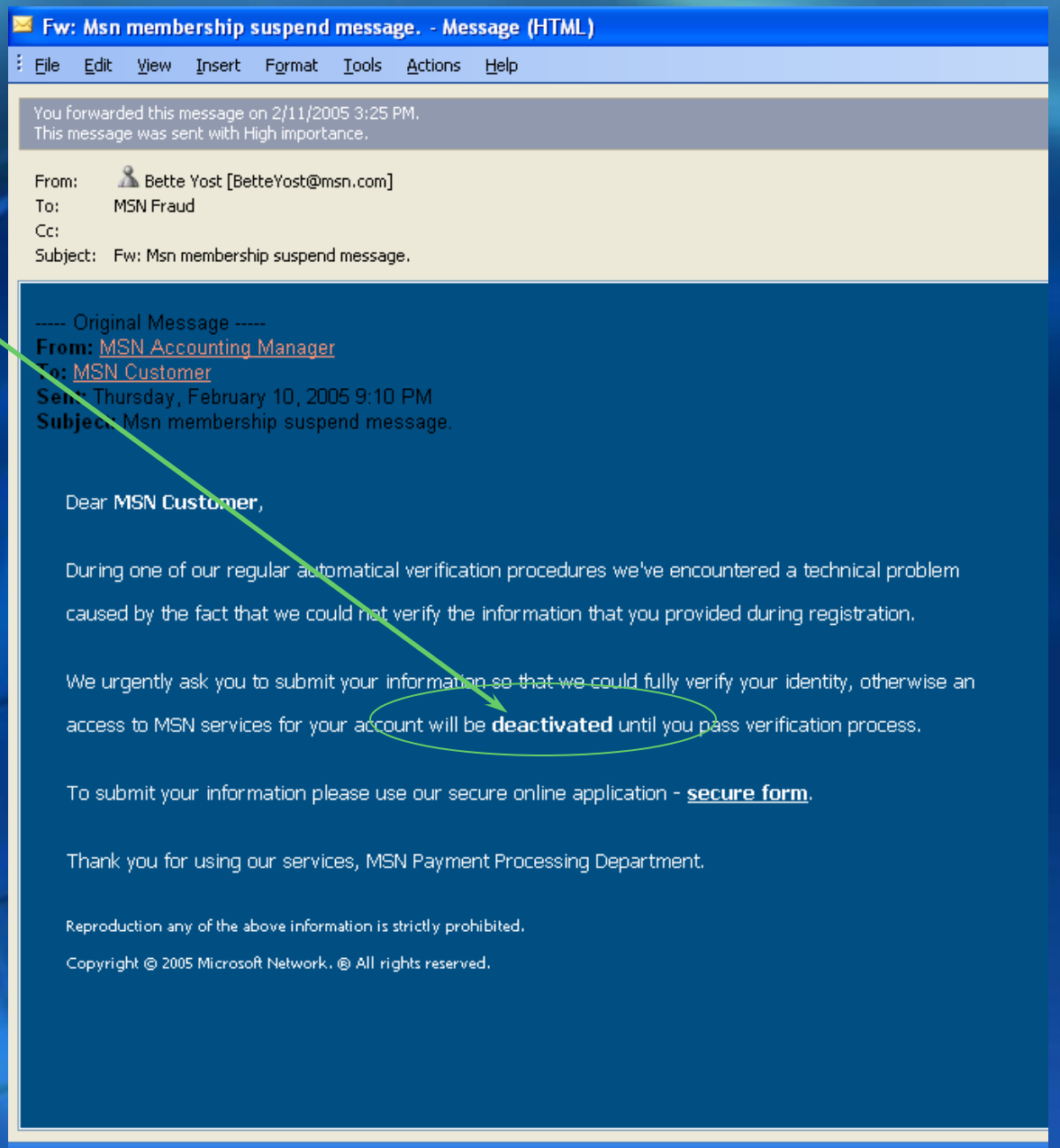

Fw: Msn membership suspend message. - Message (HTML)
File Edit View Insert Format Tools Actions Help
You forwarded this message on 2/11/2005 3:25 PM.
This message was sent with High importance.
From: Bette Yost [BetteYost@msn.com]
To: MSN Fraud
Cc:
Subject: Fw: Msn membership suspend message.
----- Original Message -----
From: MSN Accounting Manager
To: MSN Customer
Sent: Thursday, February 10, 2005 9:10 PM
Subject: Msn membership suspend message.
Dear MSN Customer,
During one of our regular automatical verification procedures we've encountered a technical problem caused by the fact that we could not verify the information that you provided during registration.
We urgently ask you to submit your information so that we could fully verify your identity, otherwise an access to MSN services for your account will be deactivated until you pass verification process.
To submit your information please use our secure online application - secure form.
Thank you for using our services, MSN Payment Processing Department.
Reproduction any of the above information is strictly prohibited.
Copyright © 2005 Microsoft Network. ® All rights reserved.
Deceptive Address
Source code reveals actual mail from address as "href=mailto://accmanager @msn-network.com"

Phishing


Fw: Msn membership suspend message. - Message (HTML)
File Edit View Insert Format Tools Actions Help
You forwarded this message on 2/11/2005 3:25 PM.
This message was sent with High importance.
From: Bette Yost [BetteYost@msn.com]
To: MSN Fraud
Cc:
Subject: Fw: Msn membership suspend message.
----- Original Message -----
From: MSN Accounting Manager
To: MSN Customer
Sent: Thursday, February 10, 2005 9:10 PM
Subject: Msn membership suspend message.
Dear MSN Customer,
During one of our regular automatical verification procedures we've encountered a technical problem caused by the fact that we could not verify the information that you provided during registration.
We urgently ask you to submit your information so that we could fully verify your identity, otherwise an access to MSN services for your account will be deactivated until you pass verification process.
To submit your information please use our secure online application - secure form.
Thank you for using our services, MSN Payment Processing Department.
Reproduction any of the above information is strictly prohibited.
Copyright © 2005 Microsoft Network. ® All rights reserved.
Impersonal Message
Be wary if a company with which you regularly do business fails to address you by name

Phishing

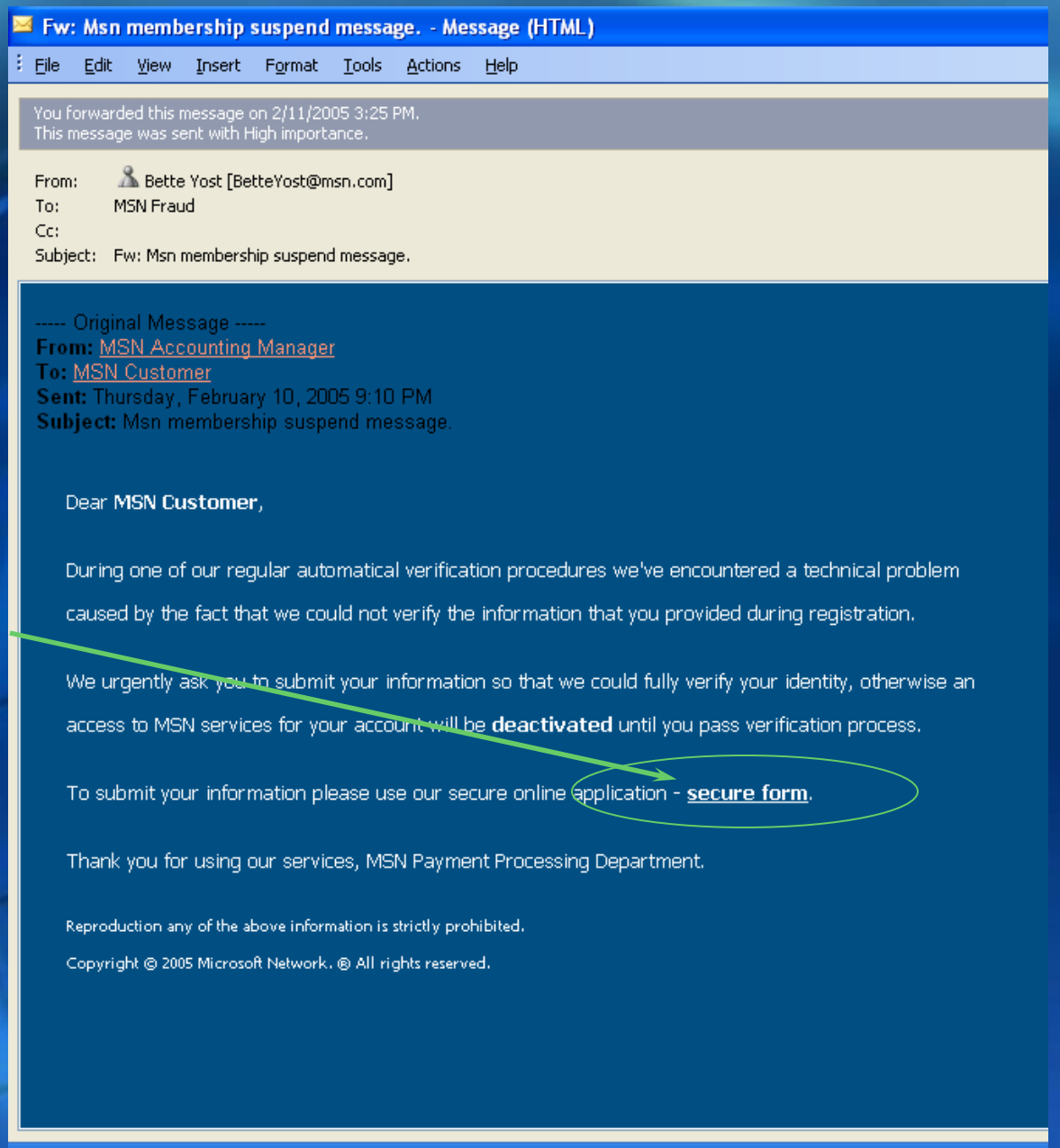
Alarmist Message
Criminals try their best to create a sense of urgency so you'll respond without thinking. Also, look for misspellings, grammatical errors, and typos--such as "…an access to MSN services for your account…"



Phishing

Deceptive Link
Source code reveals that the actual address linked to is "href=http://www.online-msnupdate.com/?sess=qCKWmHUBPPZwT8n4GEMNn70wHDEG140IHKG5tAGiqGOINeov&amp:cid=bettevost@msn.com"

The difference between these two URLs could be a sign that the message is fake. (However, even if the URLs are the same, don't let down your guard, because the pop-up could be a trick, too.)



Fw: Msn membership suspend message. - Message (HTML)

File Edit View Insert Format Tools Actions Help

You forwarded this message on 2/11/2005 3:25 PM.
This message was sent with High importance.

From: Bette Yost [BetteYost@msn.com]
To: MSN Fraud
Cc:
Subject: Fw: Msn membership suspend message.

----- Original Message -----
From: MSN Accounting Manager
To: MSN Customer
Sent: Thursday, February 10, 2005 9:10 PM
Subject: Msn membership suspend message.

Dear **MSN Customer**,

During one of our regular automatical verification procedures we've encountered a technical problem caused by the fact that we could not verify the information that you provided during registration.

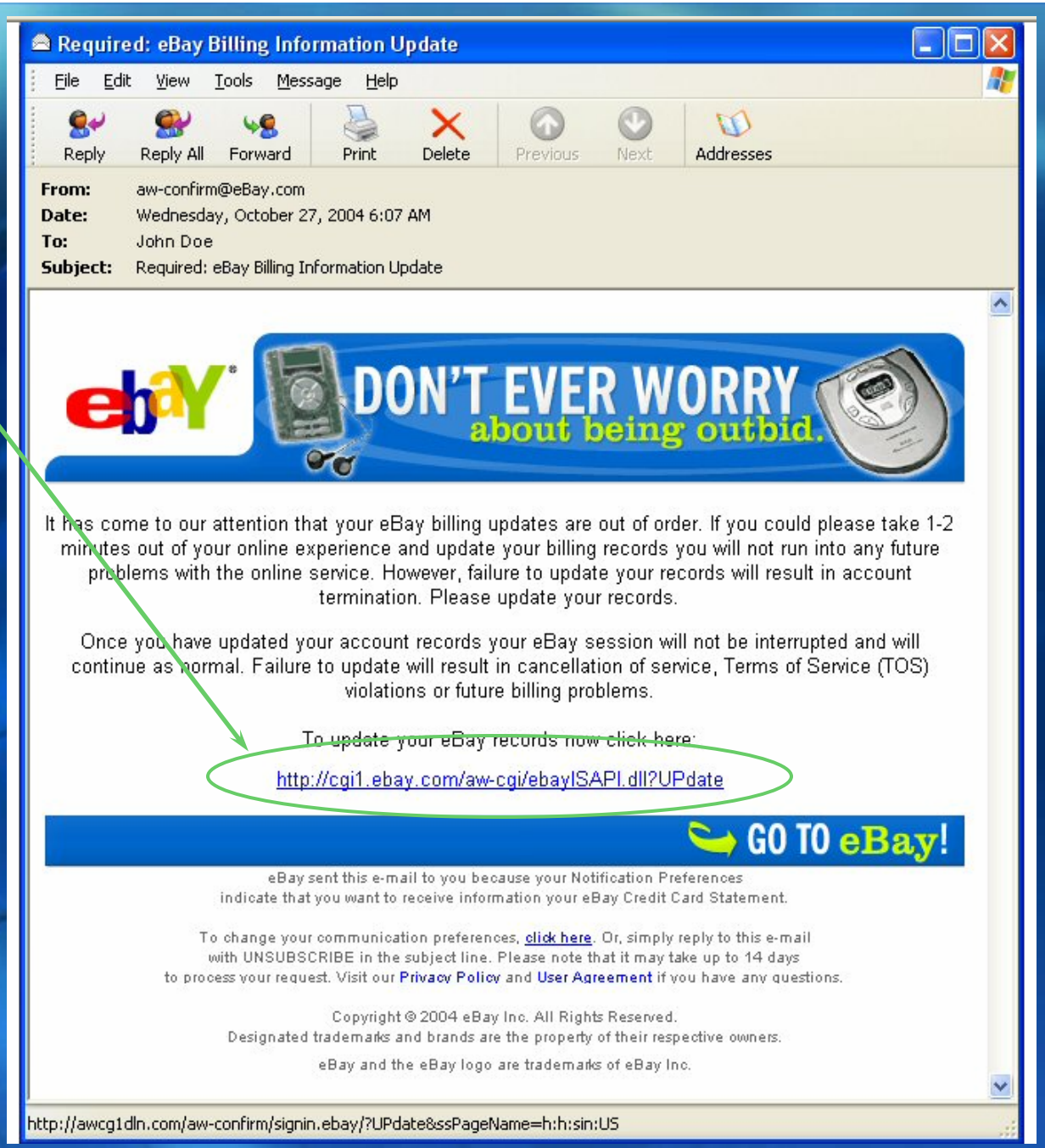
We urgently ask you to submit your information so that we could fully verify your identity, otherwise an access to MSN services for your account will be **deactivated** until you pass verification process.

To submit your information please use our secure online application - **secure form**.

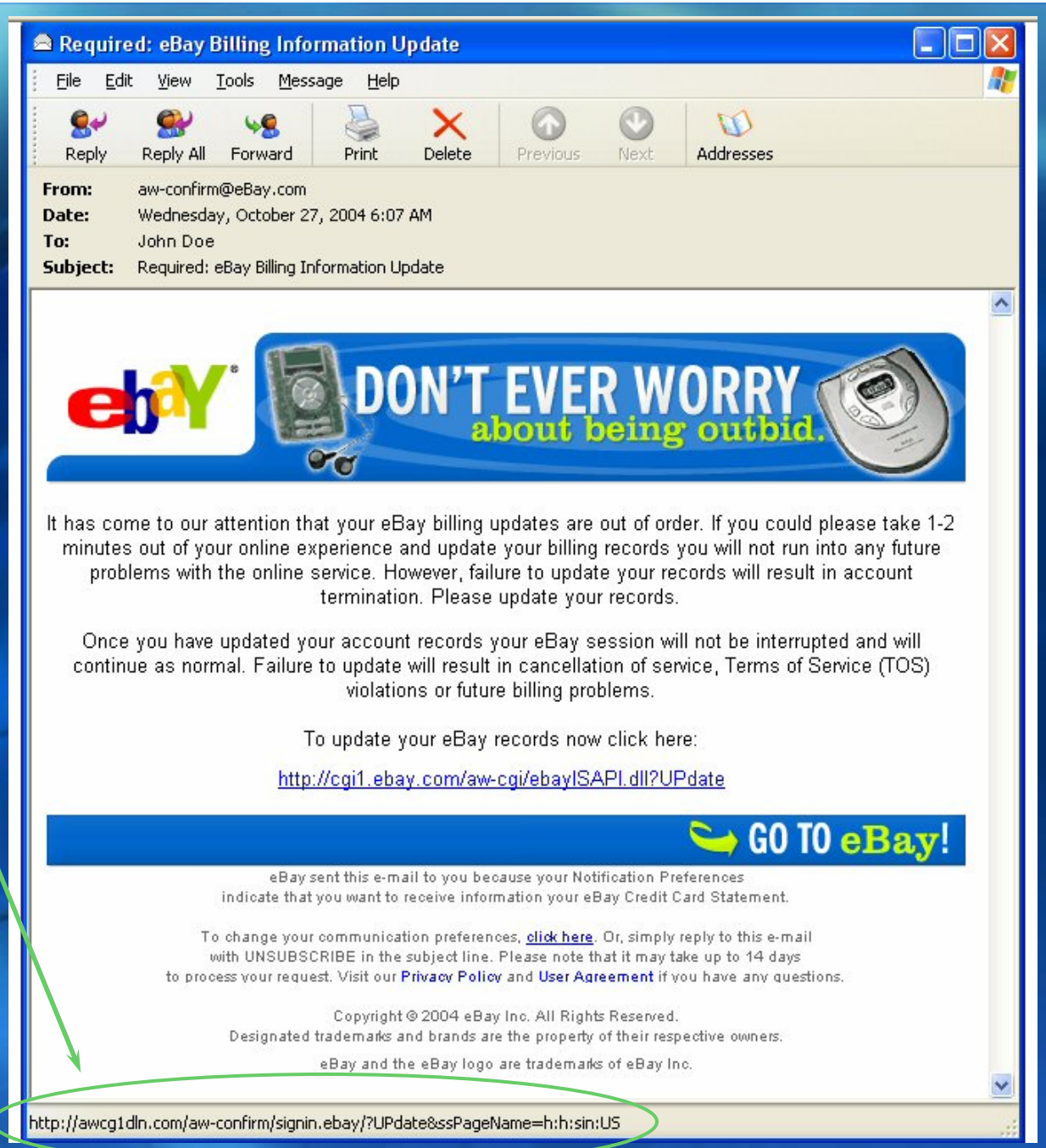
Thank you for using our services, MSN Payment Processing Department.

Phishing

Know the Company
eBay generally does not send out emails to customers containing login links. Look carefully at the status bar for all links and URLs—the URL in the status bar for the login link is not eBay.com.

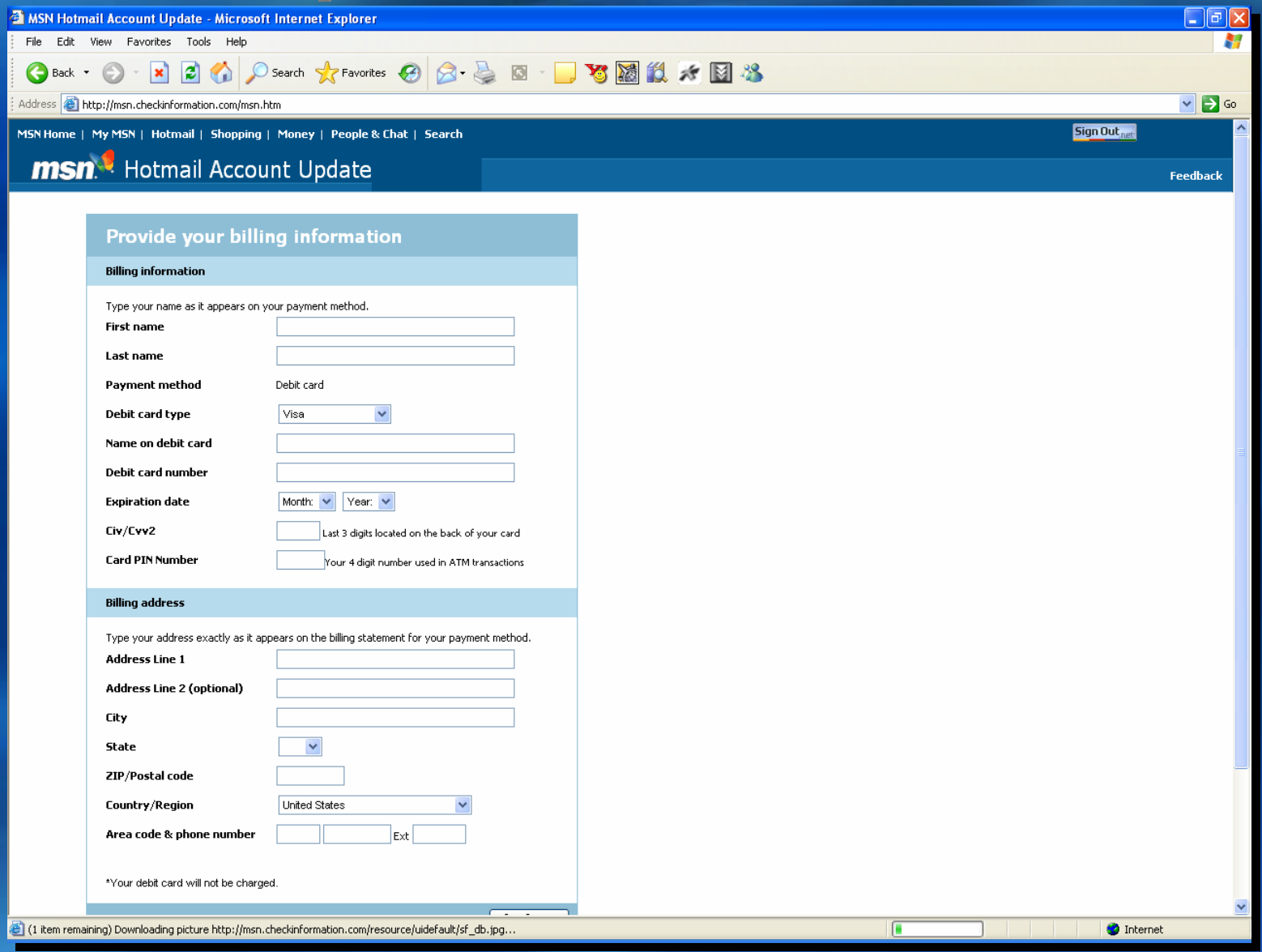


Phishing



Differences between links or URLs in an email and the status bar should make you suspicious.
If you receive an e-mail like this one, open a new browser window, type in the URL yourself and login into your account to see if there are any real account problems.

Phishing


MSN Hotmail Account Update - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://msn.checkinformation.com/msn.htm
Go
MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search
Sign Out
msn Hotmail Account Update
Feedback
Provide your billing information
Billing information
Type your name as it appears on your payment method.
First name
Last name
Payment method
Debit card
Debit card type
Visa
Name on debit card
Debit card number
Expiration date
Month:
Year:
Civ/Cvv2
Last 3 digits located on the back of your card
Card PIN Number
Your 4 digit number used in ATM transactions
Billing address
Type your address exactly as it appears on the billing statement for your payment method.
Address Line 1
Address Line 2 (optional)
City
State
ZIP/Postal code
Country/Region
United States
Area code & phone number
Ext
*Your debit card will not be charged.
(1 item remaining) Downloading picture http://msn.checkinformation.com/resource/uidefault/sf_db.jpg...
Internet

MSN Billing Phishing Case

MSN Billing Phishing Case

1 **MS filed John Doe lawsuit in WA**

MSN Billing Phishing Case

1 MS filed John Doe lawsuit in WA

2 Issued subpoenas to web hosts in CA

MSN Billing Phishing Case

1 MS filed John Doe lawsuit in WA

2 Issued subpoenas to web hosts in CA

3 Subpoenas identified ISP in Austria

MSN Billing Phishing Case

1 MS filed John Doe lawsuit in WA

2 Issued subpoenas to web hosts in CA

3 Subpoenas identified ISP in Austria

4 Austrian ISP identified IP address registered to Qwest in the US

MSN Billing Phishing Case

1 MS filed John Doe lawsuit in WA

2 Issued subpoenas to web hosts in CA

3 Subpoenas identified ISP in Austria

4 Austrian ISP identified IP address registered to Qwest in the US

5 Subpoena to Qwest and investigations identified Jayson Harris in Iowa, US

6 Referred to FBI and obtained $3 million Default Judgment

Phishing Impact

- Most people are spoofed
  - Over 60% have visited a fake or spoofed site
- People are tricked
  - Over 15% admit to having provided personal data
- Target for spoofing attacks
  - Banks, credit card companies, Web retailers, online auctions (E-bay) and mortgage companies.
- Economic loss
  - 1.2 million U.S. adults have lost money
  - The total dollar impact: $929 million

Source: TRUSTe & Gartner

Spyware

Spyware

- Software that:
  - Collects personal information from you
  - Without your knowledge or permission

Spyware

- Software that:
  - Collects personal information from you
  - Without your knowledge or permission
- Privacy
  - 15 percent of enterprise PCs have a keylogger
    Source: Webroot's SpyAudit
  - Number of keyloggers jumped three-fold in 12 months
    Source: Sophos

Spyware

- Software that:
  - Collects personal information from you
  - Without your knowledge or permission
- Privacy
  - 15 percent of enterprise PCs have a keylogger
    Source: Webroot's SpyAudit
  - Number of keyloggers jumped three-fold in 12 months
    Source: Sophos
- Reliability
  - Microsoft Watson
    - ~50% of crashes caused by spyware

Spyware

- Software that:
  - Collects personal information from you
  - Without your knowledge or permission
- Privacy
  - 15 percent of enterprise PCs have a keylogger
    Source: Webroot's SpyAudit
  - Number of keyloggers jumped three-fold in 12 months
    Source: Sophos
- Reliability
  - Microsoft Watson
    - ~50% of crashes caused by spyware
- Support Costs
  - Dell, HP, IBM: Spyware causes ~30% of calls
  - Estimated support costs at $2.5m+ / year

Spyware as Espionage

Israel Spyware

"Dubbed "Trojangate," the incident resulted in nearly 20 arrests, with some reports indicating that there were hundreds -- perhaps thousands -- of documents stolen from multiple Israeli firms. About 100 servers containing stolen data have been seized and are being investigated." *BBC*

Spyware as Espionage

Israel Spyware

"Dubbed "Trojangate," the incident resulted in nearly 20 arrests, with some reports indicating that there were hundreds -- perhaps thousands -- of documents stolen from multiple Israeli firms. About 100 servers containing stolen data have been seized and are being investigated." *BBC*

"In 2004, MessageLabs came upon a Trojan horse created for the purpose of attacking a type of software used in airplane design." *AP*

Spyware as Espionage

Israel Spyware

"Dubbed "Trojangate," the incident resulted in nearly 20 arrests, with some reports indicating that there were hundreds -- perhaps thousands -- of documents stolen from multiple Israeli firms. About 100 servers containing stolen data have been seized and are being investigated." *BBC*

"In 2004, MessageLabs came upon a Trojan horse created for the purpose of attacking a type of software used in airplane design." *AP*

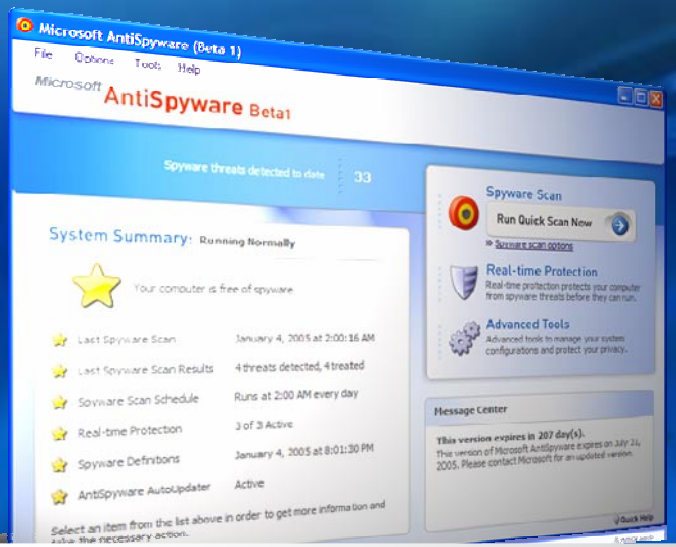
"Someone placed surveillance software on sheriff's office computers, apparently enabling unauthorized access to sensitive information about prisoner movements, confidential homeland security updates and private personnel files." *AP*

Criminal Spyware

UK police foil massive bank theft

"Police in London say they have foiled one of the biggest attempted bank thefts in Britain. The plan was to steal £220m ($423m) from the London offices of the Japanese bank Sumitomo Mitsui. Computer experts are believed to have tried to transfer the money electronically after hacking into the bank's systems. A man has been arrested by police in Israel after the plot was uncovered by the National Hi-Tech Crime Unit. Unit members worked closely with Israeli police …" *Story from BBC NEWS: http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk/4356661.stm*

Combating Spyware Threats



Microsoft Windows AntiSpyware

Helps protect Windows users from spyware and other potentially unwanted software

Detect and remove spyware

- 17 million downloads, 23 million spyware packages cleaned
- Scheduled scans help maintain PC security and privacy

Improve Internet browsing safety

- Continuous protection guards 50+ ways spyware gets on a PC
- Intelligent alerts handle spyware based on your preferences

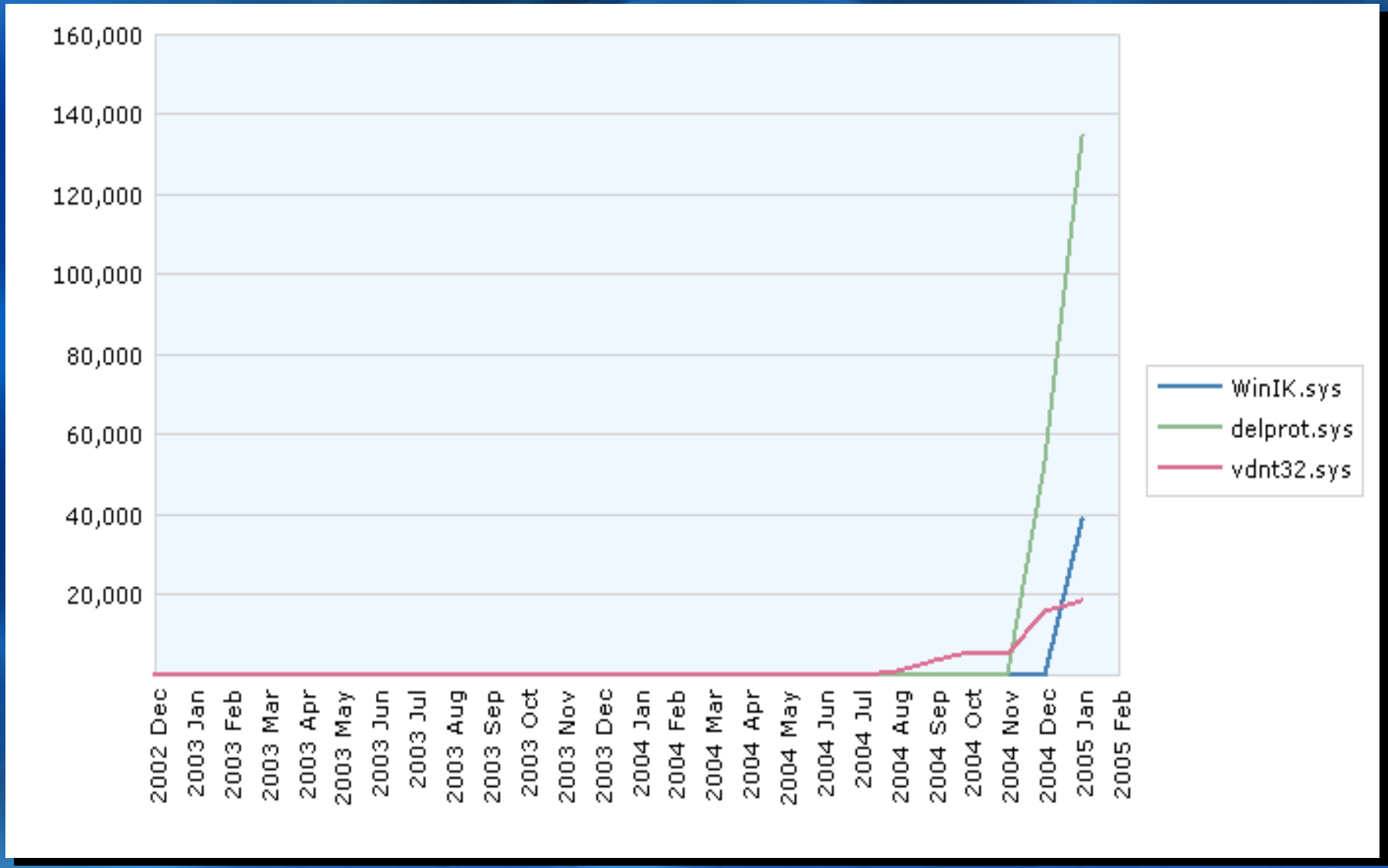
Stop the latest threats

- Global SpyNet™ community helps identify new spyware
- Automatic signature downloads keep you up-to-date

Feb. 2005 OCA Snapshot

Driver	Characteristic	Instance count
Delprot.sys	Deletion protection for iSearch adware/spyware.	81870 1.03%
"LoadMeDude" TROJ_LODMEDUD_A	Randomly named driver that hides processes, registry, files. Auto-update capability. Bundled with Comedy Central adware/spyware.	25496 0.32%
winik.sys	Protects CommonName adware/spyware.	13583 0.17%
iesprt.sys TROJ_BANKER.W	Steals banking passwords.	2386 0.03%
Hxdefdrv.sys "Hacker Defender"	Public domain source rootkit. Resource hiding and backdoor capability.	1323 0.02%

OCA: Spyware Drivers




Bots

Bots

- Bot Ecosystem
  - Bots
  - Botnets
  - Control channels
  - Herders

Bots

- Bot Ecosystem
  - Bots
  - Botnets
  - Control channels
  - Herders
- It began in mass with MyDoom.A
  - Eight days after MyDoom.A hit the Internet
  - Scanned for the back door left by the worm
  - Installed Trojan horse called Mitglieder
  - Then used those systems as their spam engines
  - Millions of computers across the Internet were now for sale to the underground spam community

Bot-Nets Tracked (3 Sept. 2004)

Age (days)	Name	Server	MaxSize
02.00	nubela.net	dns.nubela.net	10725
10.94	winnt.bigmoney.biz (randex)	winnt.bigmoney.biz	2393
09.66	PS 7835 - y.eliteirc.co.uk	y.eliteirc.co.uk	2061
09.13	y.stefanjagger.co.uk (#y)	y.stefanjagger.co.uk	1832
03.10	ganjahaze.com	ganjahaze.com	1507
01.04	PS 8049 - 1.j00g0t0wn3d.net	1.j00g0t0wn3d.net	3689
10.93	pub.isonert.net	pub.isonert.net	537
08.07	irc.brokenirc.net	irc.brokenirc.net	649
01.02	PS 8048 - grabit.zapto.org	grabit.zapto.org	62
10.34	dark.naksha.net	dark.naksha.net	UNK
08.96	PS 7865 - lsd.25u.com	lsd.25u.com	UNK
UNK	PS ? - 69.64.38.221	69.64.38.221	UNK

Bot-Nets Tracked (3 Sept. 2004)

Age (days)	Name	Server	MaxSize
02.00	nubela.net	dns.nubela.net	10725
10.94	winnt.bigmoney.biz (randex)	winnt.bigmoney.biz	2393
09.66	PS 7835 - y.eliteirc.co.uk	y.eliteirc.co.uk	2061
09.13	y.stefanjagger.co.uk (#y)	y.stefanjagger.co.uk	1832
03.10	ganjahaze.com	ganjahaze.com	1507
01.04	PS 8049 - 1.j00g0t0wn3d.net	1.j00g0t0wn3d.net	3689
10.93	pub.isonert.net	pub.isonert.net	537
08.07	irc.brokenirc.net	irc.brokenirc.net	649
01.02	PS 8048 - grabit.zapto.org	grabit.zapto.org	62
10.34	dark.naksha.net	dark.naksha.net	UNK
08.96	PS 7865 - lsd.25u.com	lsd.25u.com	UNK
UNK	PS ? - 69.64.38.221	69.64.38.221	UNK

Bot-Nets Tracked (3 Sept. 2004)

Age (days)	Name	Server	MaxSize
02.00	nubela.net	dns.nubela.net	10725
10.94	winnt.bigmoney.biz (randex)	winnt.bigmoney.biz	2393
09.66	PS 7835 - y.eliteirc.co.uk	y.eliteirc.co.uk	2061
09.13	y.stefanjagger.co.uk (#y)	y.stefanjagger.co.uk	1832
03.10	ganjahaze.com	ganjahaze.com	1507
01.04	PS 8049 - 1.j00g0t0wn3d.net	1.j00g0t0wn3d.net	3689
10.93	pub.isonert.net	pub.isonert.net	537
08.07	irc.brokenirc.net	irc.brokenirc.net	649
01.02	PS 8048 - grabit.zapto.org	grabit.zapto.org	62
10.34	dark.naksha.net	dark.naksha.net	UNK
08.96	PS 7865 - lsd.25u.com	lsd.25u.com	UNK
UNK	PS ? - 69.64.38.221	69.64.38.221	UNK

As of 12 August 2005:
Tracking 3523 bot-nets of which 700 are active
Average size is 80,000 computers

In The News

Botnet with 10,000 Machines Shut Down

Sept 8, 2004

"A huge IRC "botnet" controlling more than 10,000 machines has been shut down by the security staff of Norwegian provider Telenor, according to the Internet Storm Center. The discovery confirms beliefs about the growth of botnets, which were cited in the recent distributed denial of service (DDoS) attack upon Akamai and DoubleClick that sparked broader web site outages. […]"

http://news.netcraft.com/archives/2004/09/08/botnet_with_10000_machines_shut_down.html

In The News

Botnet with 10,000 Machines Shut Down

Sept 8, 2004

"A huge IRC "botnet" controlling more than 10,000 machines has been shut down by the security staff of Norwegian provider Telenor, according to the Internet Storm Center. The discovery confirms beliefs about the growth of botnets, which were cited in the recent distributed denial of service (DDoS) attack upon Akamai and DoubleClick that sparked broader web site outages. […]"

http://news.netcraft.com/archives/2004/09/08/botnet_with_10000_machines_shut_down.html

FBI busts alleged DDoS Mafia

Aug 26, 2004

"A Massachusetts businessman allegedly paid members of the computer underground to launch organized, crippling distributed denial of service (DDoS) attacks against three of his competitors [...]"

http://www.securityfocus.com/news/9411

Payloads

- Keystroke loggers for stealing CC, PII
- SYN or application flooding code
  - Used for DDoS
  - DDoS has been used many times
  - Including public attacks against Microsoft.com
- Spam relays – 70-80% of all spam

  Source SpecialHam.com, Spamforum.biz
- Piracy
- Future features

Botnet Damage Potential

10,000-member botnet

Attack	Requests/bot	Botnet Total	Resource exhausted
Bandwidth flood (uplink)	186 kbps	1.86 Gbps	T1, T3, OC-3, OC-12
Bandwidth flood (downlink)	450 kbps	4.5 Gbps	T1, T3, OC-3, OC-12, OC-48 (2.488Gbps) 50% of Taiwan/US backbone
Syn flood	450 SYNs/sec	4.5M SYN/sec	4 Dedicated Cisco Guard (@$90k) OR 20 tuned servers
Static http get (cached)	93/sec	929,000/sec	15 servers
Dynamic http get	93/sec	929,000/sec	310 servers
SSL handshake	10/sec	100,000/sec	167 servers

Botnet Damage Potential

10,000-member botnet

Attack	Requests/bot	Botnet Total	Resource exhausted
Bandwidth flood (uplink)	186 kbps	1.86 Gbps	T1, T3, OC-3, OC-12
Bandwidth flood (downlink)	450 kbps	4.5 Gbps	T1, T3, OC-3, OC-12, OC-48 (2.488Gbps) 50% of Taiwan/US backbone
Syn flood	450 SYNs/sec	4.5M SYN/sec	4 Dedicated Cisco Guard (@$90k) OR 20 tuned servers
Static http get (cached)	93/sec	929,000/sec	15 servers
Dynamic http get	93/sec	929,000/sec	310 servers
SSL handshake	10/sec	100,000/sec	167 servers

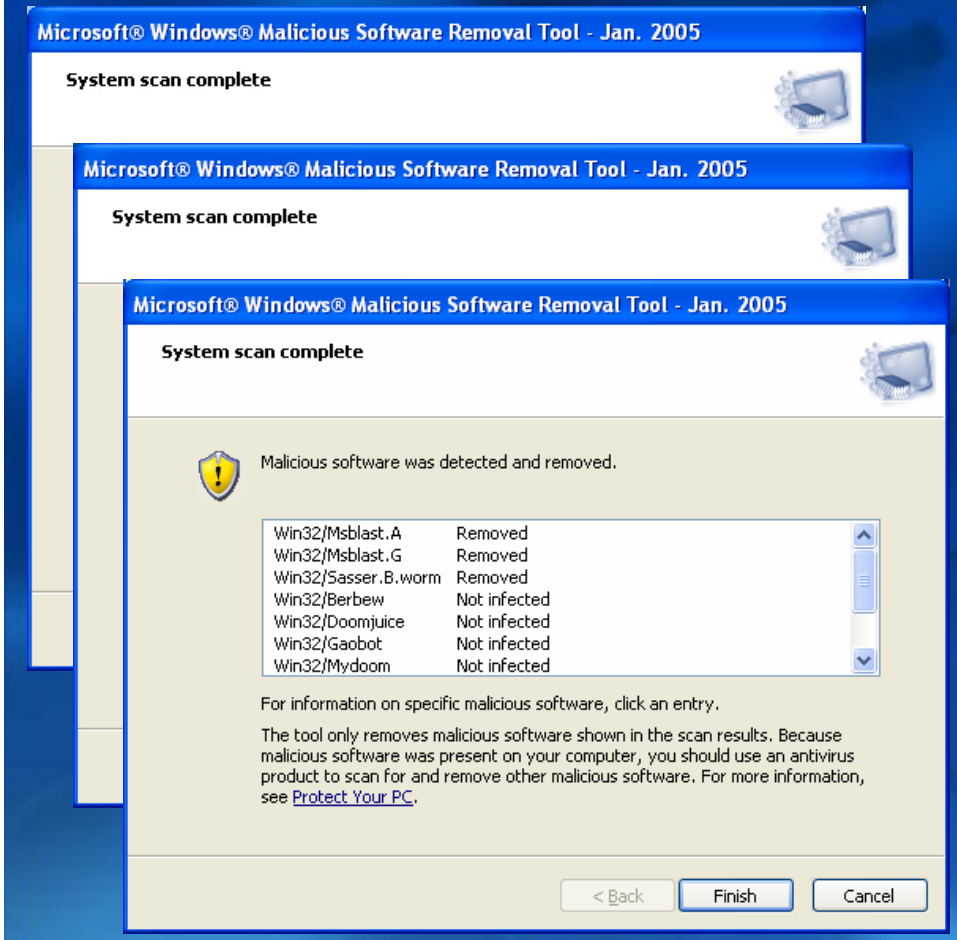
```
>$350.00/weekly - $1,000/monthly (USD)
>Type of service: Exclusive (One slot only)
>Always Online: 5,000 - 6,000
>Updated every: 10 minutes
```

```
>$220.00/weekly - $800.00/monthly (USD)
>Type of service: Shared (4 slots)
>Always Online: 9,000 - 10,000
>Updated every: 5 minutes
```

September 2004 postings to SpecialHam.com, Spamforum.biz

Malicious Software Removal

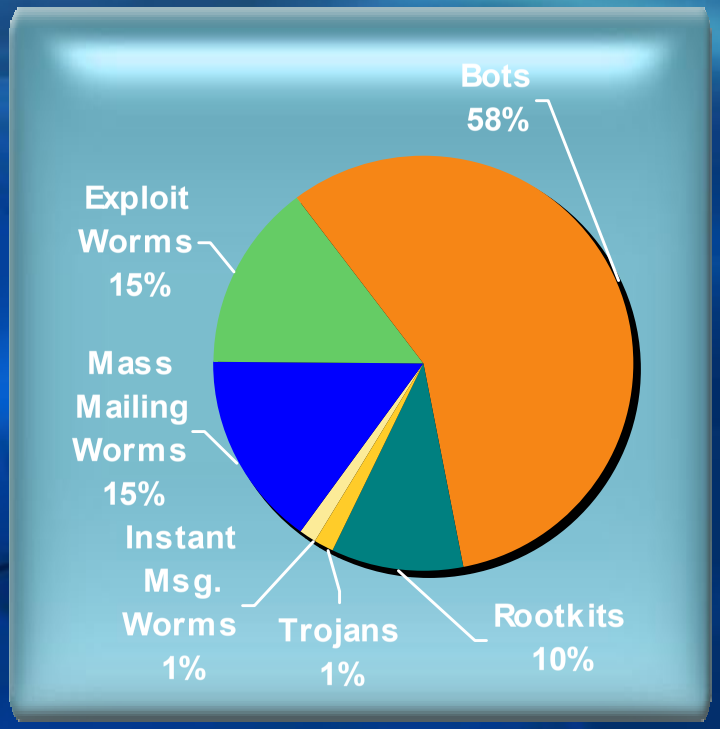
Complements traditional Antivirus technologies by providing one tool that removes prevalent viruses and worms from a PC

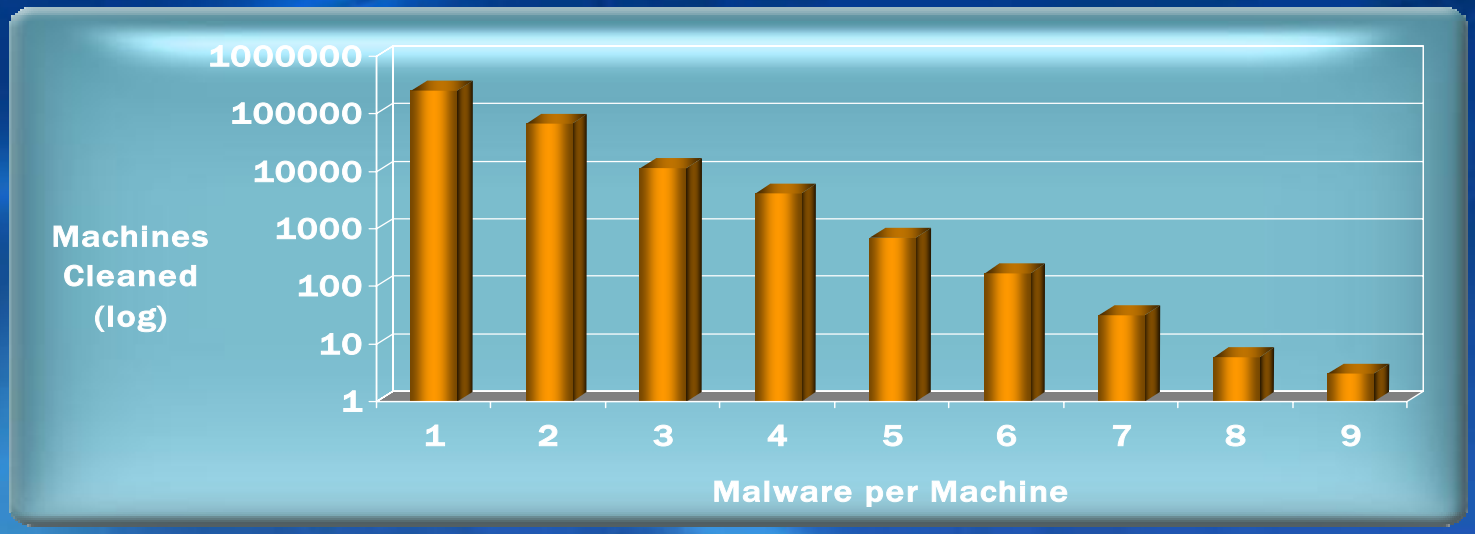


- **Updated monthly to remove prevalent malware**
- **Targeted at consumers without antivirus**
- **Enterprise deployable as part of a defense-in-depth strategy**
- **Available through:**
  - ⇨ **Windows Update**
  - ⇨ **Auto Update**
  - ⇨ **Online interface**
  - ⇨ **MS Download Center**

Cleaner Statistics (as of 27 July 2005)

Release	Days Live	Executions	Disinfections	
			Value	%
January	28	124,613,632	239,197	0.1920%
February	28	118,209,670	351,135	0.2970%
March	35	145,502,003	443,661	0.3049%
April	28	125,150,400	590,714	0.4720%
May	35	164,283,730	1,154,345	0.7027%
June	28	162,763,946	642,955	0.3950%
July	18	156,379,734	627,414	0.4090%
Total	200	1,001,824,331	4,093,531	0.4106%





Source: Microsoft

The Economics of Crime

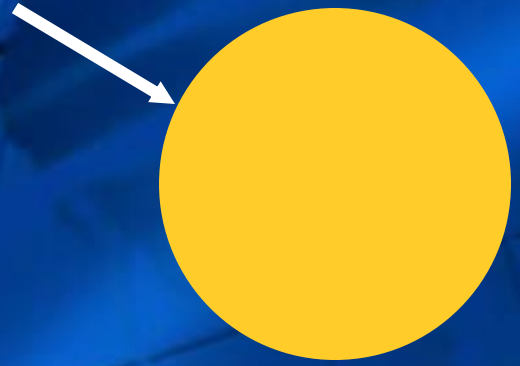
- Increase the value of an enterprise by damaging a competing enterprise
- Manipulate the value of a futures contract
- Divert delivery of value, to someone to whom it was not intended
- Make a coercive threat credible
- Stop by direct intervention an activity perceived as destroying value
- Reduce an opponent's defensive or destructive capabilities

Source: Scott Borg, an economist at Dartmouth

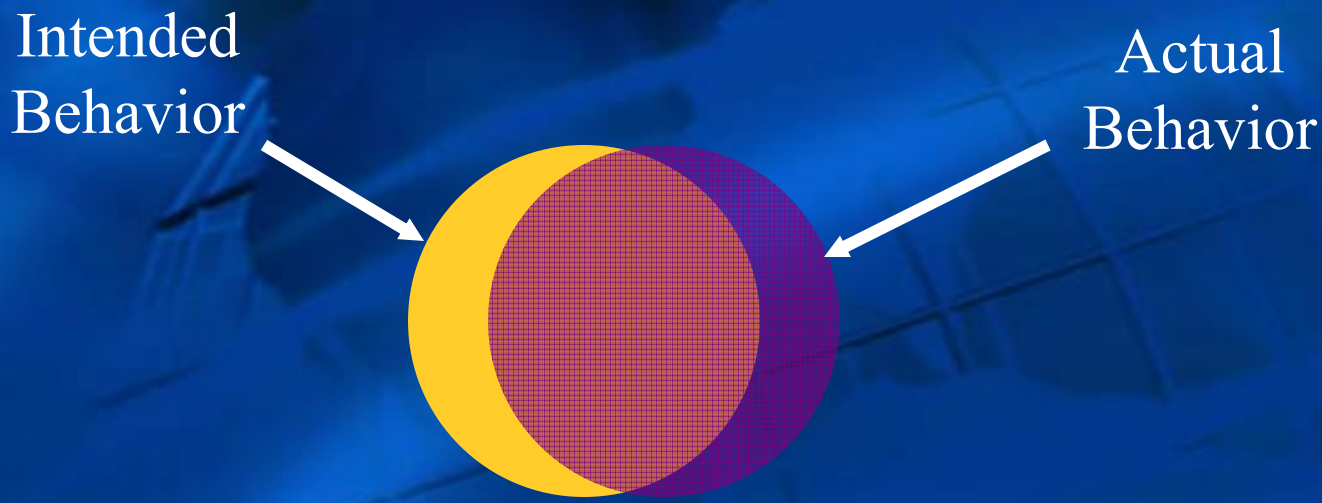
The Fundamental Problem

The Fundamental Problem

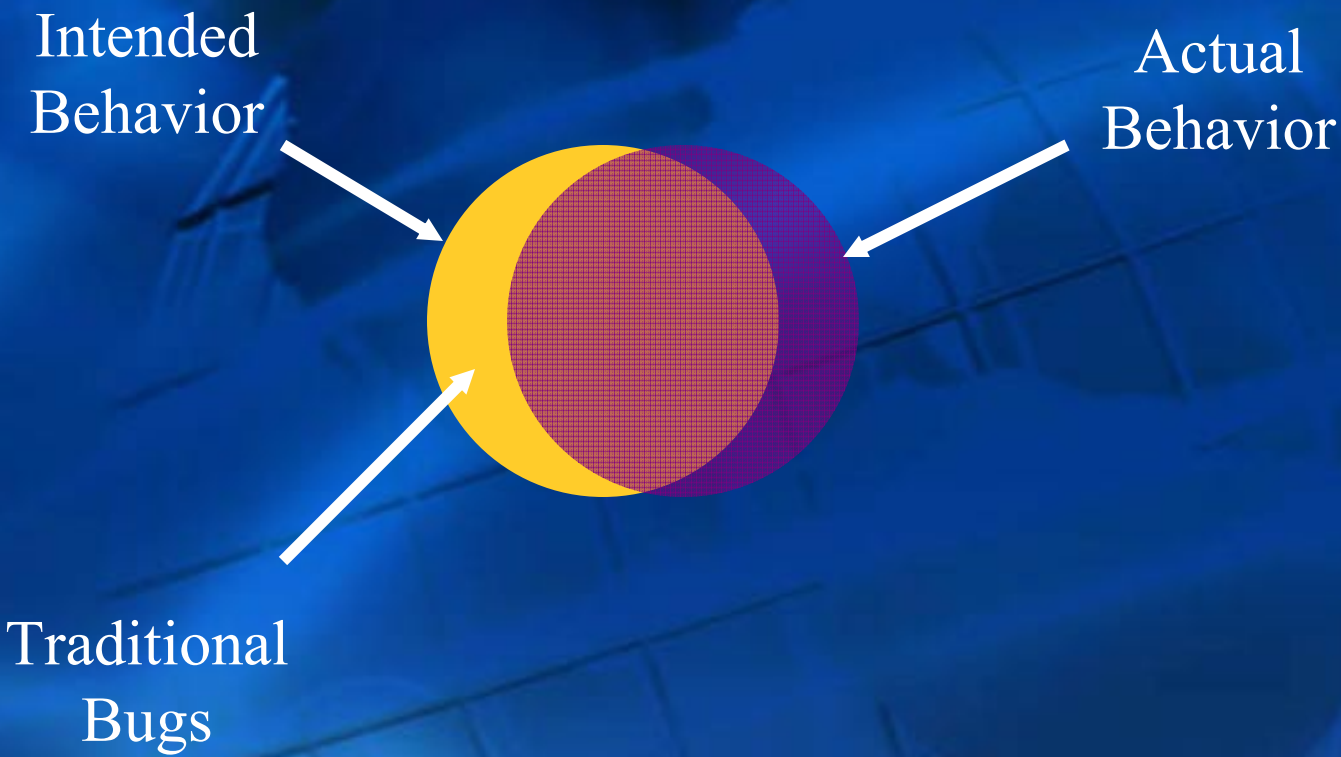
Intended
Behavior



The Fundamental Problem



The Fundamental Problem

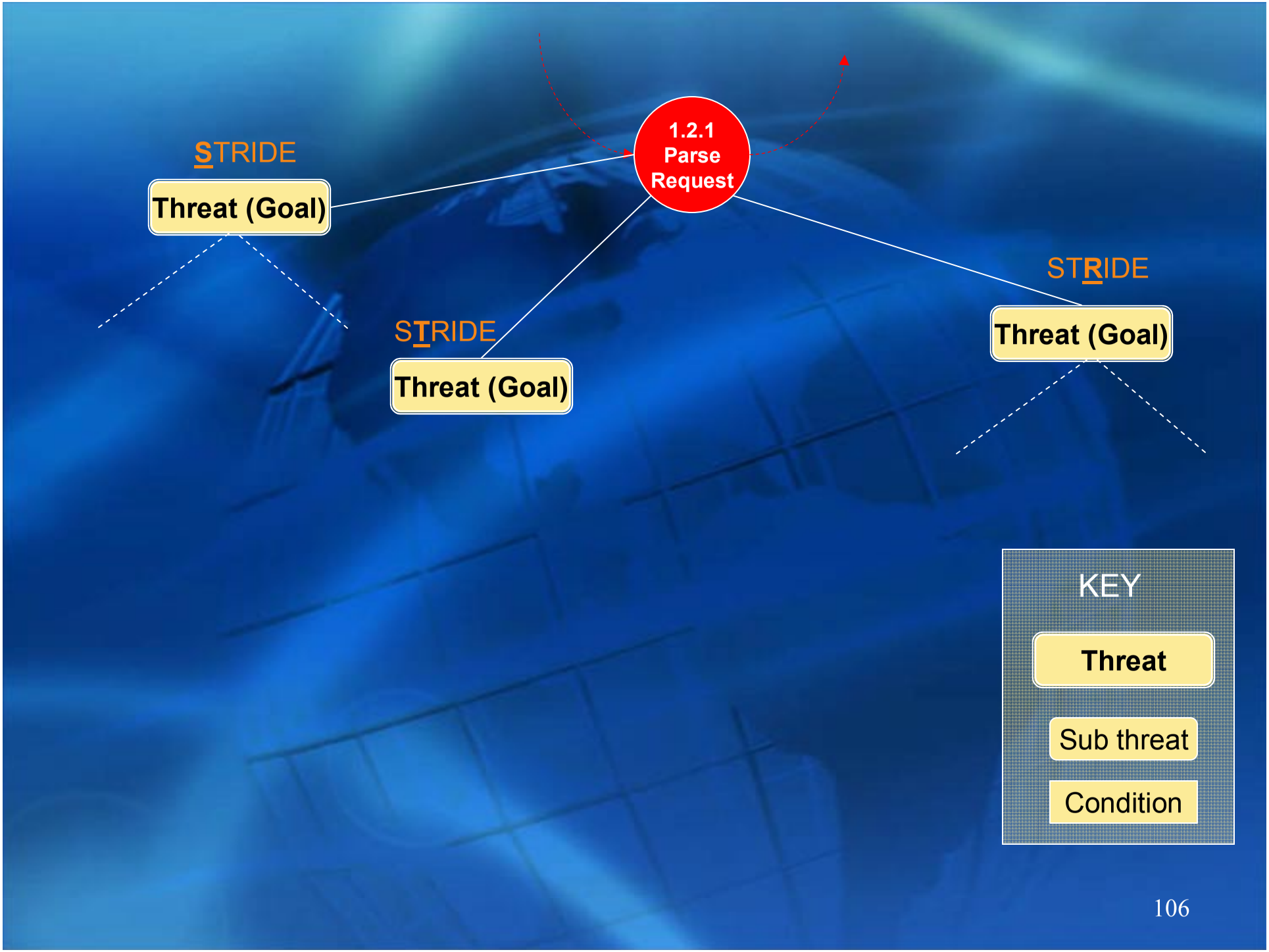


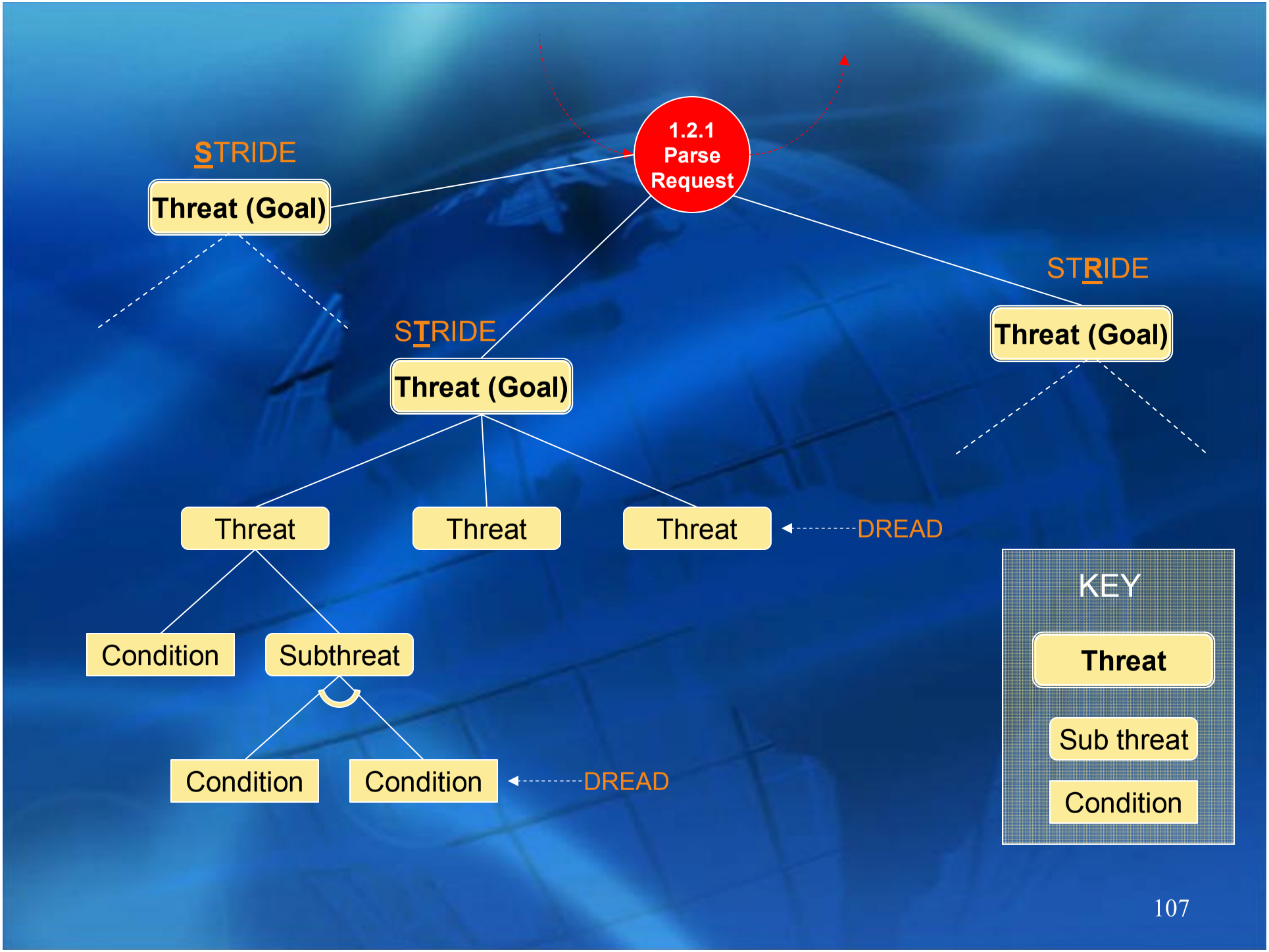
The Fundamental Problem

Threat Modeling Process

- Create model of app (DFD, UML etc)
- Categorize threats with STRIDE
  - Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Elevation of Privilege
- Build threat tree
- Rank threats with DREAD
  - Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability


1.2.1
Parse
Request


1.2.1
Parse
Request
STRIDE
Threat (Goal)
STRIDE
Threat (Goal)
STRIDE
Threat (Goal)
KEY
Threat
Sub threat
Condition


1.2.1
Parse
Request
STRIDE
Threat (Goal)
STRIDE
Threat (Goal)
STRIDE
Threat (Goal)
Threat
Threat
Threat
DREAD
Condition
Subthreat
Condition
Condition
DREAD
KEY
Threat
Sub threat
Condition

SD3 At Work – MS03-007

SD3 At Work – MS03-007

The underlying DLL (NTDLL.DLL) not vulnerable

Code made more conservative during Security Push

SD3 At Work – MS03-007

The underlying DLL (NTDLL.DLL) not vulnerable

Code made more conservative during Security Push

Even if it was vulnerable

IIS 6.0 not running by default on Windows Server 2003

SD3 At Work – MS03-007

The underlying DLL (NTDLL.DLL) not vulnerable

Code made more conservative during Security Push

Even if it was vulnerable

IIS 6.0 not running by default on Windows Server 2003

Even if it was running

IIS 6.0 doesn't have WebDAV enabled by default

SD3 At Work – MS03-007

The underlying DLL (NTDLL.DLL) not vulnerable

Code made more conservative during Security Push

Even if it was vulnerable

IIS 6.0 not running by default on Windows Server 2003

Even if it was running

IIS 6.0 doesn't have WebDAV enabled by default

Even if it did have WebDAV enabled

Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)

SD3 At Work – MS03-007

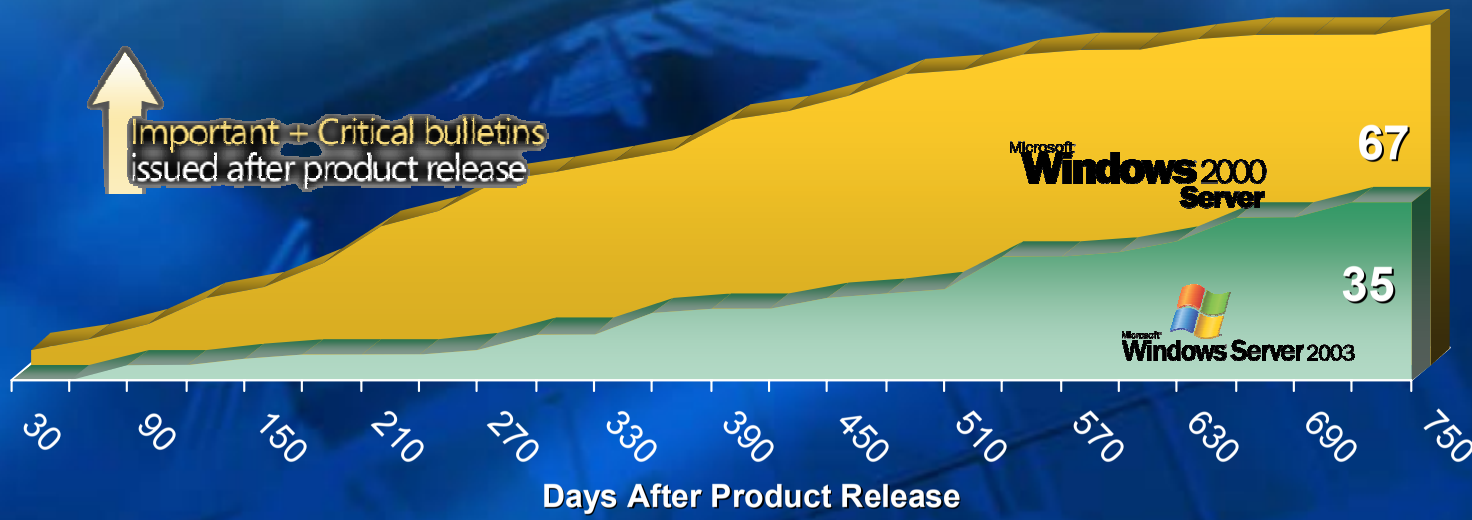
The underlying DLL (NTDLL.DLL) not vulnerable	Code made more conservative during Security Push
Even if it was vulnerable	IIS 6.0 not running by default on Windows Server 2003
Even if it was running	IIS 6.0 doesn't have WebDAV enabled by default
Even if it did have WebDAV enabled	Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)
Even if the buffer was large enough	Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)

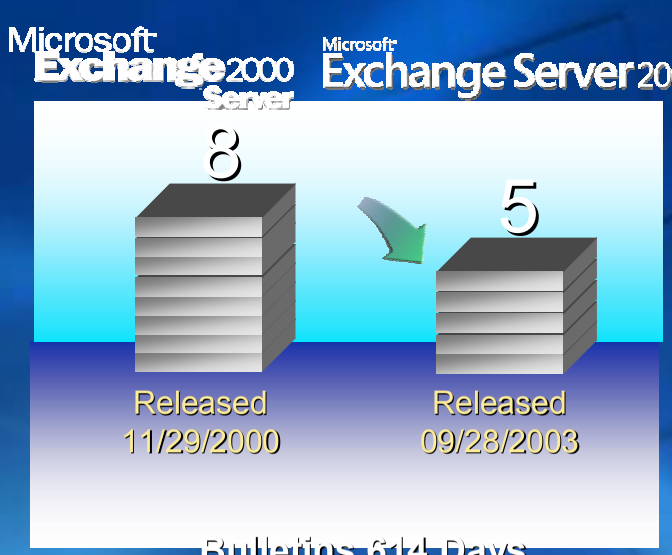
SD3 At Work – MS03-007

The underlying DLL (NTDLL.DLL) not vulnerable	Code made more conservative during Security Push
Even if it was vulnerable	IIS 6.0 not running by default on Windows Server 2003
Even if it was running	IIS 6.0 doesn't have WebDAV enabled by default
Even if it did have WebDAV enabled	Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)
Even if the buffer was large enough	Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)
Even if it there was an exploitable buffer overrun	Would have occurred in *w3wp.exe* which is now running as 'network service'

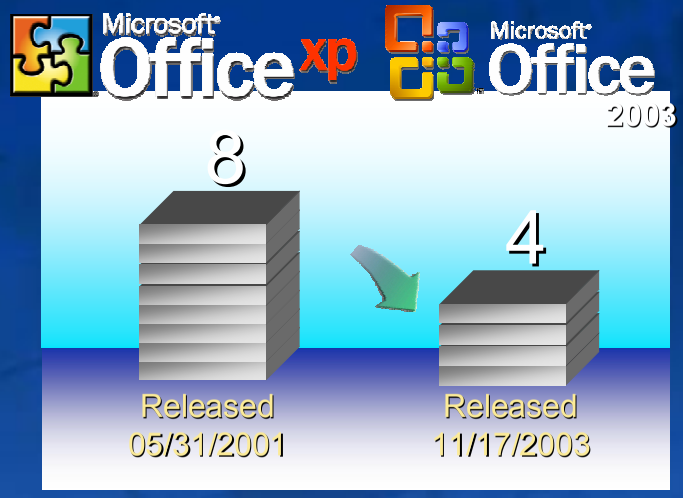
Focus Yields Results

As of June 2, 2005





Bulletins 614 Days After Product Release



Bulletins 564 Days After Product Release