

Evolution of Cyber Threats

William Billings, CISSP, ITIL

Chief Security Officer

Microsoft Federal

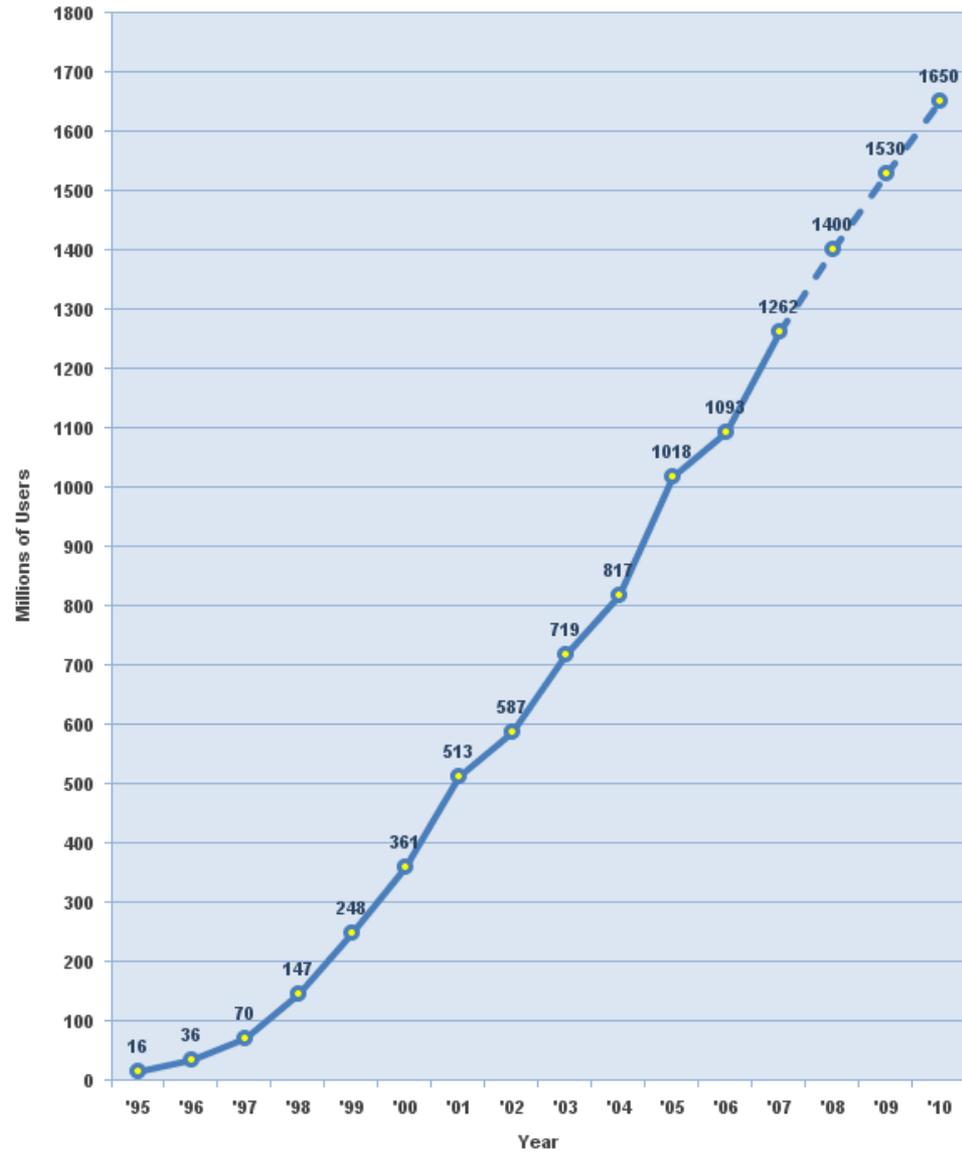
Microsoft Corporation

William.Billings@Microsoft.com



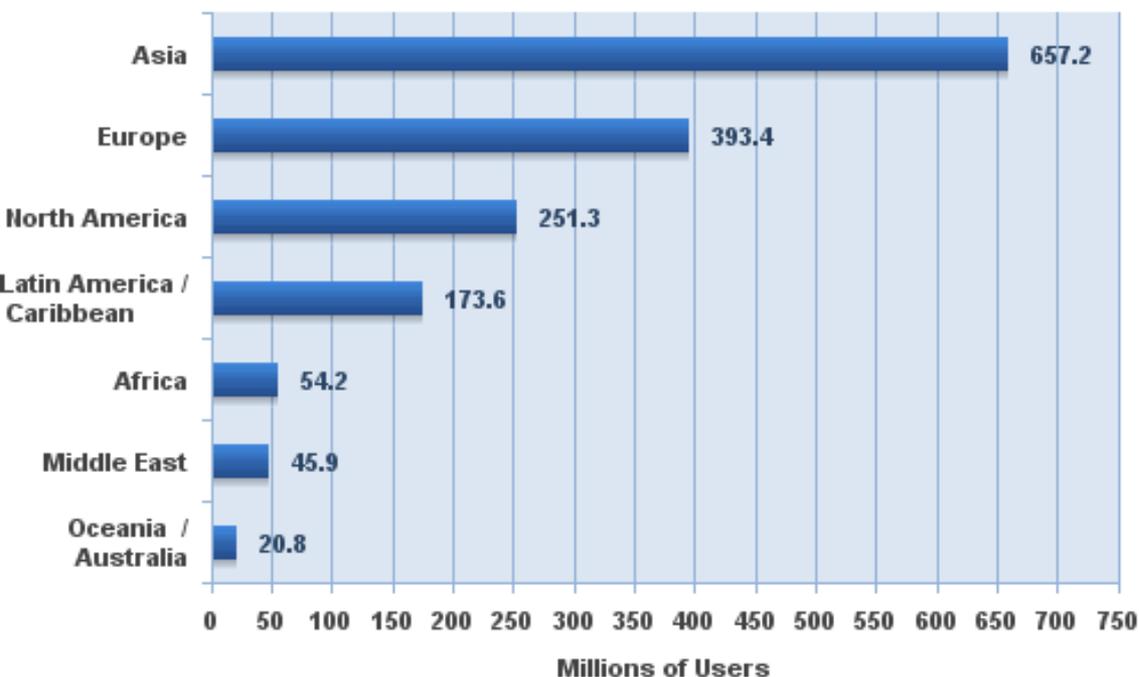
The medium . . .

Internet Users in the World Growth 1995 - 2010



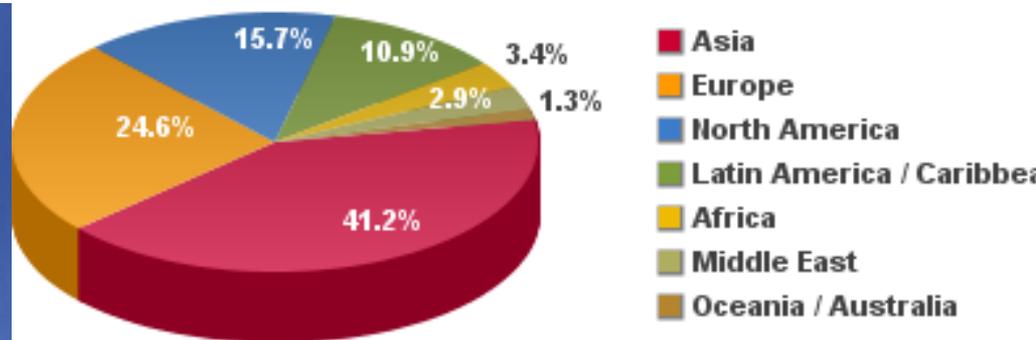
Source: www.internetworldstats.com - January, 2008
Copyright © 2008, Miniwatts Marketing Group

Internet Users in the World by Geographic Regions



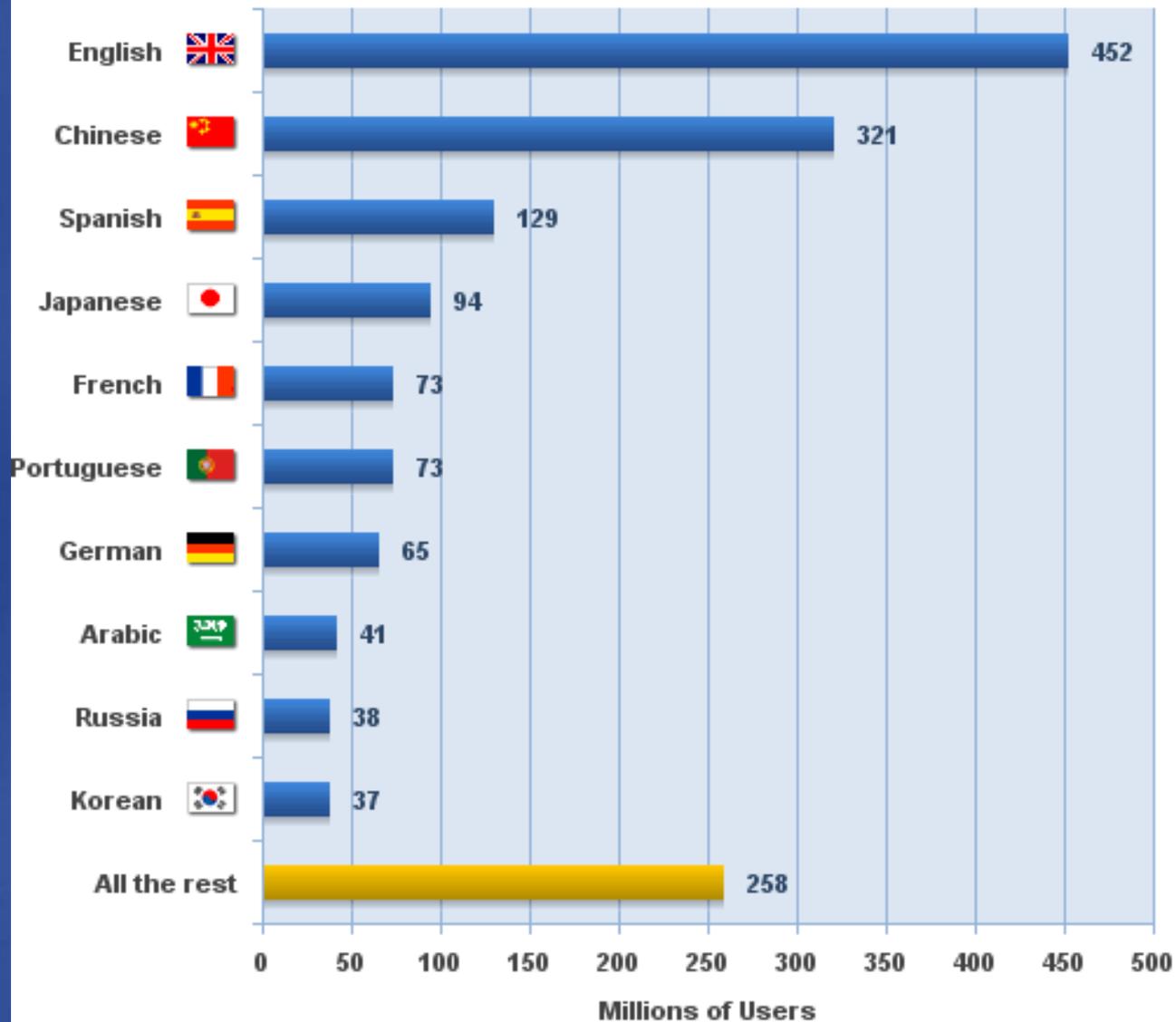
Source: Internet World Stats - www.internetworldstats.com/stats.htm
 Estimated Internet users are 1,596,270,108 for March 31, 2009
 Copyright © 2009, Miniwatts Marketing Group

World Internet Users by World Regions



Source: Internet World Stats - www.internetworldstats.com/stats.htm
 1,596,270,108 Internet users for March 31, 2009
 Copyright © 2009, Miniwatts Marketing Group

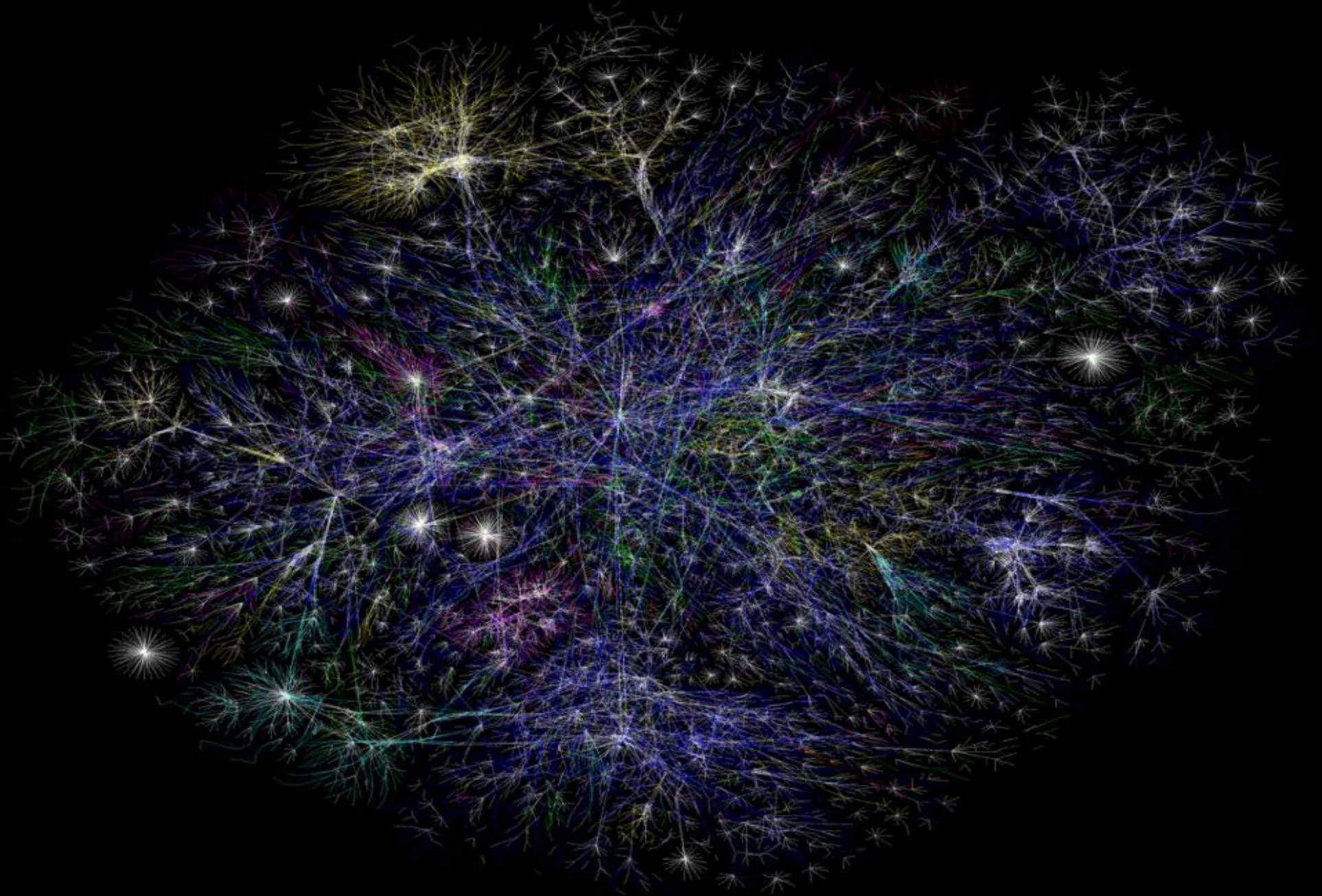
Top 10 Languages in the Internet millions of users



Source: Internet World Stats - www.internetworldstats.com/stats7.htm

Estimated Internet users is 1,581,571,589 for 2008

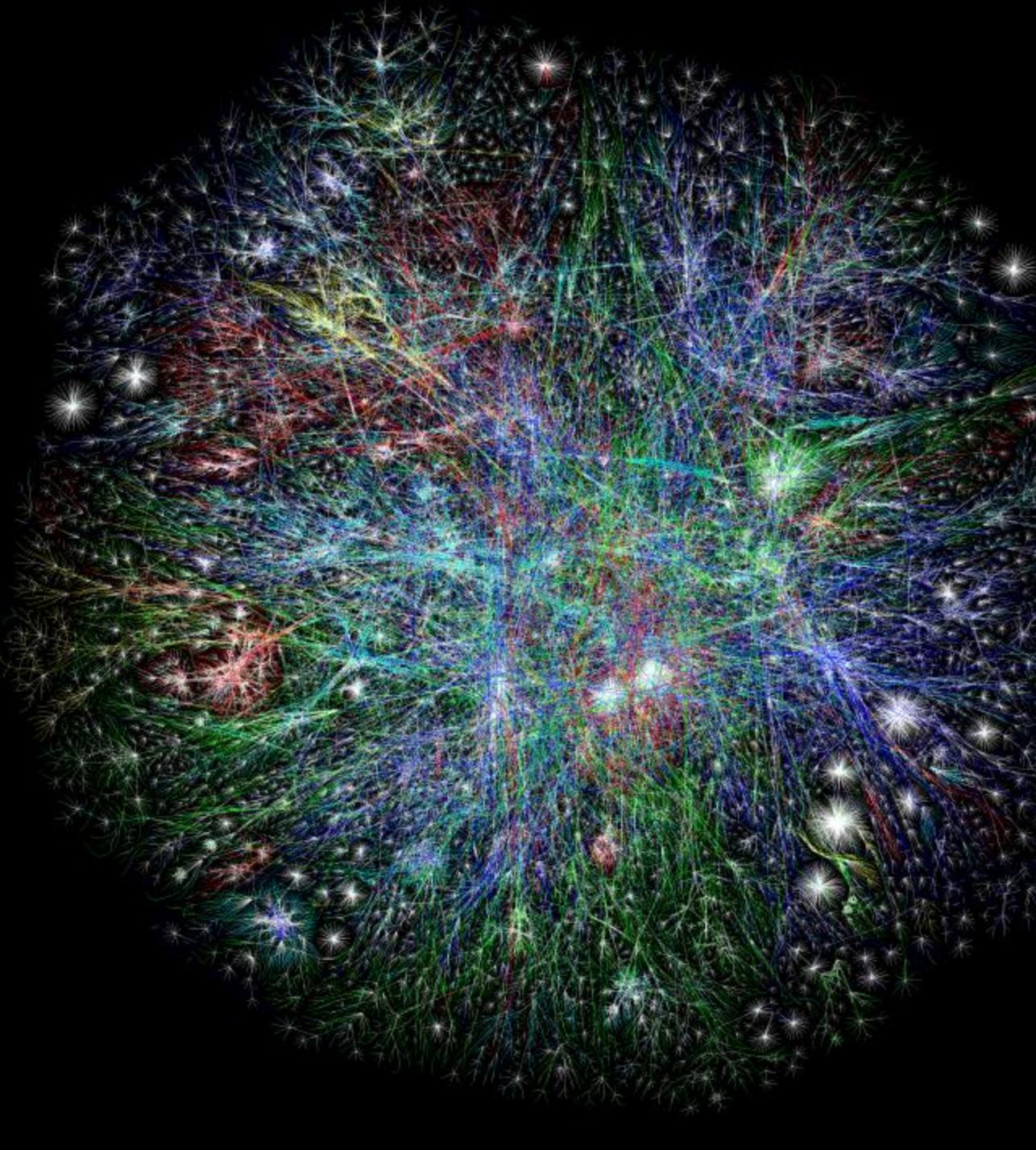
Copyright © 2009, Miniwatts Marketing Group



Number of Hosts advertised in the DNS

Date	Survey Host Count	Adjusted Host Count	Replied To Ping*
Jan 2009	625,226,456		-
Jul 2008	570,937,778		-
Jan 2008	541,677,360		-
Jul 2007	489,774,269		-
Jan 2007	433,193,199		-
Jul 2006	439,286,364		-
Jan 2006	394,991,609		-
Jul 2005	353,284,187		-
Jan 2005	317,646,084		-
Jul 2004	285,139,107		-
Jan 2004	233,101,481		-
Jan 2003	171,638,297		-
Jul 2002	162,128,493		-
Jan 2002	147,344,723		-
Jul 2001	125,888,197		-
Jan 2001	109,574,429		-
Jul 2000	93,047,785		-
Jan 2000	72,398,092		-
Jul 1999	56,218,000		-
Jan 1999	43,230,000		8,426,000
Jul 1998	36,739,000		6,529,000
Jan 1998	29,670,000		5,331,640
Jul 1997	19,540,000	26,053,000	4,314,410
Jan 1997	16,146,000	21,819,000	3,392,000
Jul 1996	12,881,000	16,729,000	2,569,000
Jan 1996	9,472,000	14,352,000	1,682,000
Jul 1995	6,642,000	8,200,000	1,149,000
Jan 1995	4,852,000	5,846,000	970,000
Jul 1994	3,212,000		707,000
Jan 1994	2,217,000		576,000
Jul 1993	1,776,000		464,000
Jan 1993	1,313,000		

[* estimated by pinging a sample of all hosts]



The Machine . . .

- 100 billion clicks per day
- 55 trillion links
- 1 billion PC chips on the internet
- 2 million emails per second
- 1 million IM messages per second
- 8 terabytes per second traffic
- 65 billion phone calls per year
- 255 exabytes of magnetic storage
- 1 million voice queries per hour
- 2 billion location nodes activated
- 600 billion RFID tabs used
- Uses 5% of global electricity

Moore's law indicates that this is doubling in power every 2 years. You do the math . . .

The Flattening of the World

Beneficial change

- Social: Enabling a global village
- Economic: Easier, faster commerce
- Political: Freer exchange of ideas

Undesirable change

- Increase in online crime, lack of traceability
- Bulk identity theft
- Targeted attacks against businesses & governments

Cyber threats . . .

A short quiz

Joe the drug dealer



Steve the cyber criminal



Who makes more money?

*Cost of U.S.
cybercrime:
More than \$100B*



Personal information
(credit cards, bank
account numbers) are
commoditized and
traded

Cyber-Espionage . . .

April 2007: The Department of Commerce had to take the Bureau of Industrial Security's networks off line for several months. This Commerce Bureau reviews high tech exports and its networks were hacked by unknown foreign intruders.

April 2007/August 2008: Estonia and Georgia had their cyber networks attacked by unknown foreign intruders, most likely at the behest of the Russian government.

June 2007: The Secretary of Defense's unclassified email was hacked by unknown foreign intruders.

July 2007: Reports surface about the State Department recovering from a large-scale network attack affecting operations worldwide, where the hackers appeared to target the department headquarters and offices dealing with China and North Korea.

September 2007: Contractors at DHS and DOD had their networks hacked, as a back door into agency systems

January 2008: A CIA official said the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities.

June 2008: The networks of several Congressional offices were hacked by unknown foreign intruders. Some incidents involved offices with an interest in human rights or Tibet.

November 2008: *BusinessWeek* reported that in April 2005, hackers gained access to a computer network in NASA's Kennedy Space Center, and launched a malignant software program that gathered data about Space Shuttle Discovery and sent it to a computer system in Taiwan. Much of the data came from a computer server connected to a network that tracks malfunctions that could threaten the International Space Station.

November/December 2008: Classified networks at the Defense Department and U.S. Central Command were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and secure the networks.

February 2009: FAA computer systems were hacked, increasing the risk of an intentional disruption of commercial air traffic.

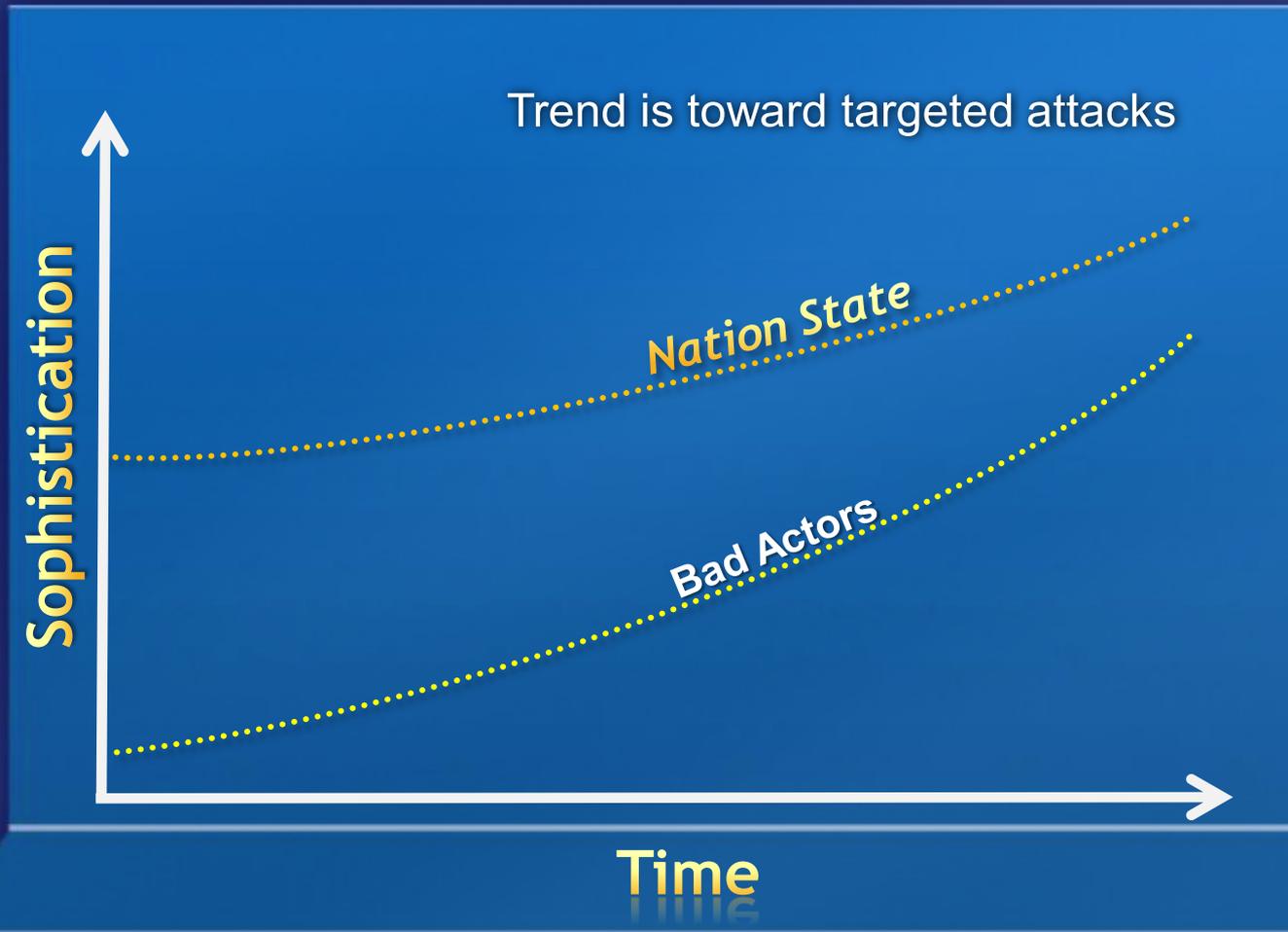
March 2009: Canadian researchers found a computer espionage system that they attributed to China implanted on the government networks of 103 countries..

March 2009: Reports in the press suggest that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran.

April 2009: Reports circulate about malicious software discovered on computers that control the U.S. power grid.

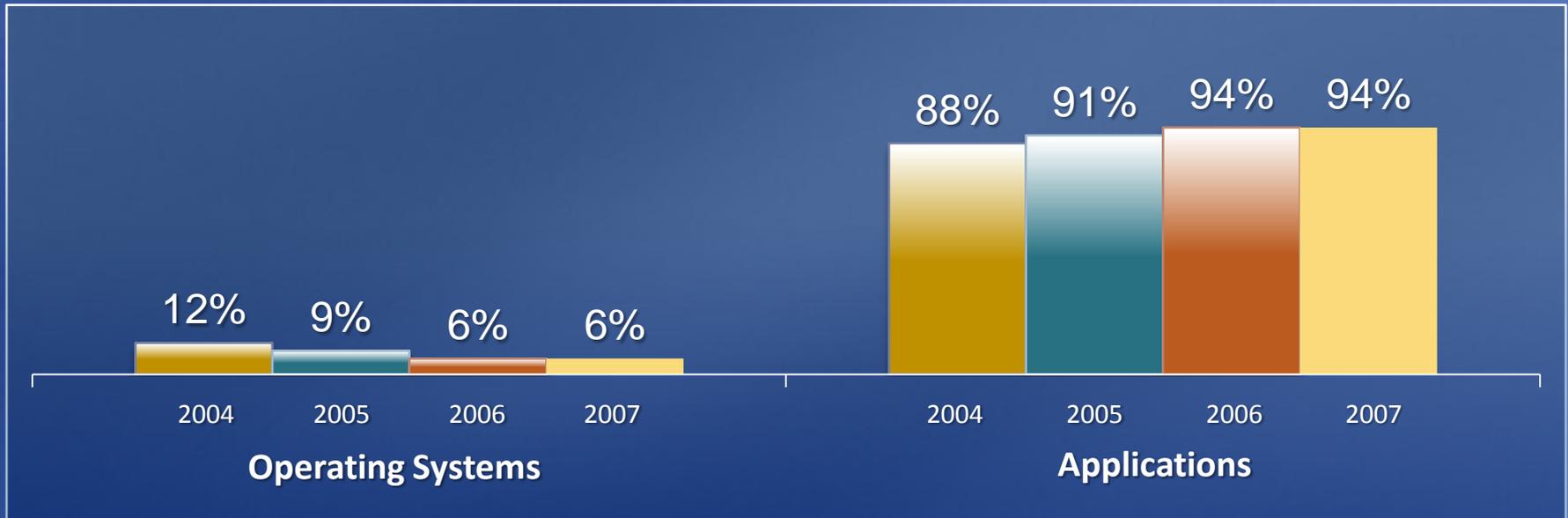
April 2009: Reports reveal that hackers downloaded data about the Joint Strike Fighter, a multibillion-dollar high-tech fighter jet known as the F-35, by exploiting vulnerabilities in the computer networks used to design and build the aircraft's weapon systems.

Attack Sophistication



Attacks focusing on applications

% of Vulnerabilities: Major Operating Systems versus Applications



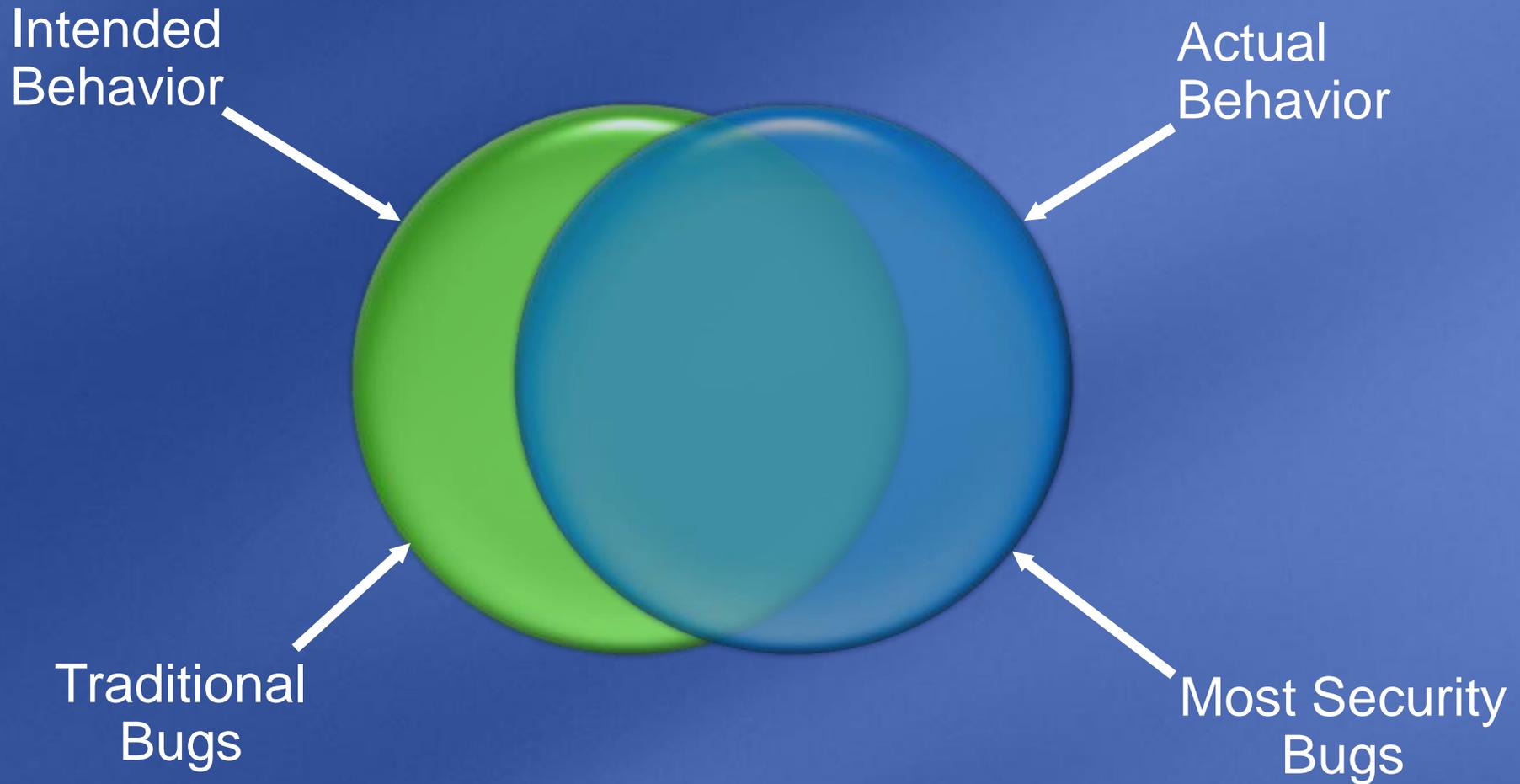
Calculated from the Microsoft Security Intelligence Report 2008

~90% of vulnerabilities are remotely exploitable

Sources: IBM X-Force,

The problem . . .

The Fundamental Problem



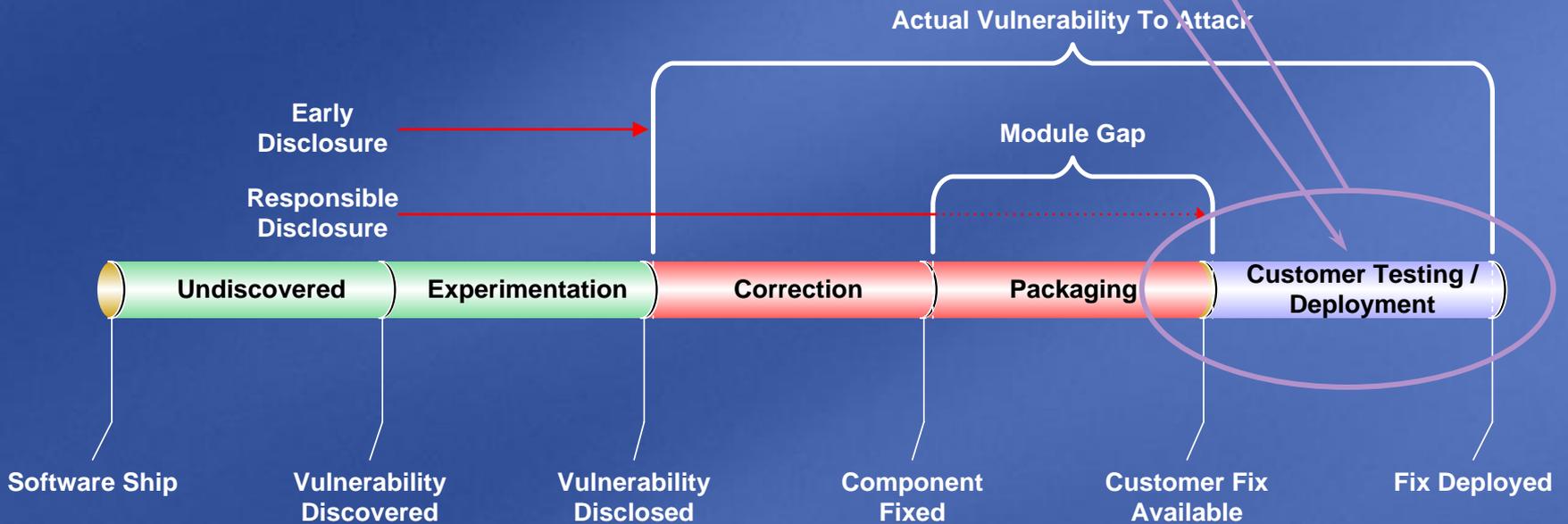


The problem part deux . . .

Vulnerability Timeline

Why does this gap exist?

Attacks occur here



Vulnerability Timeline

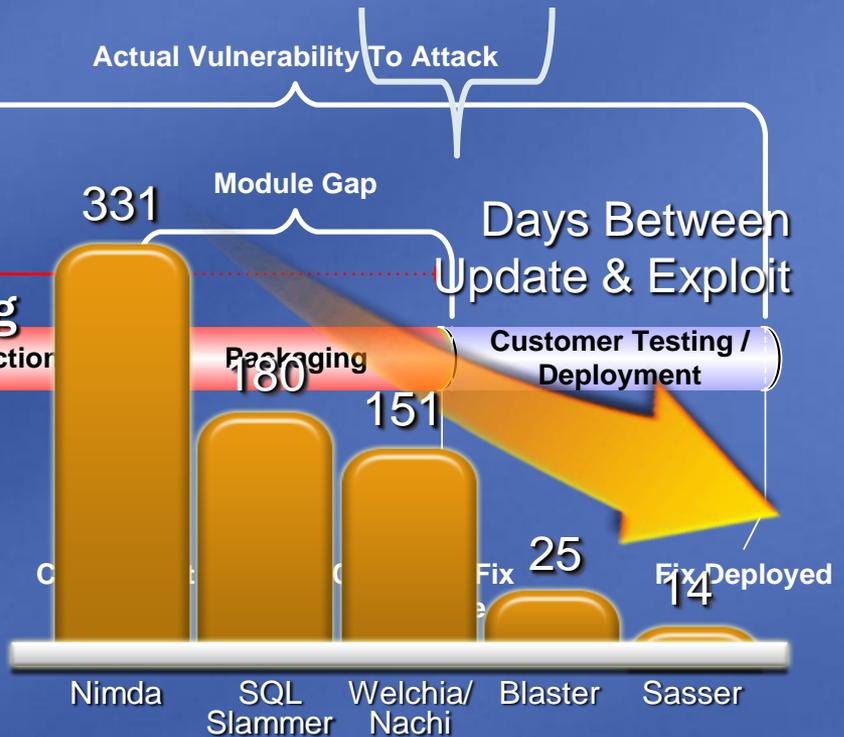
- **Days From Patch To Exploit**
 - Have decreased so that patching is not a defense in large organizations

Average 2 days for patch to be reverse engineered to identify vulnerability

Software Ship

Vulnerability Identified

Vulnerability Disclosed



Source: Microsoft

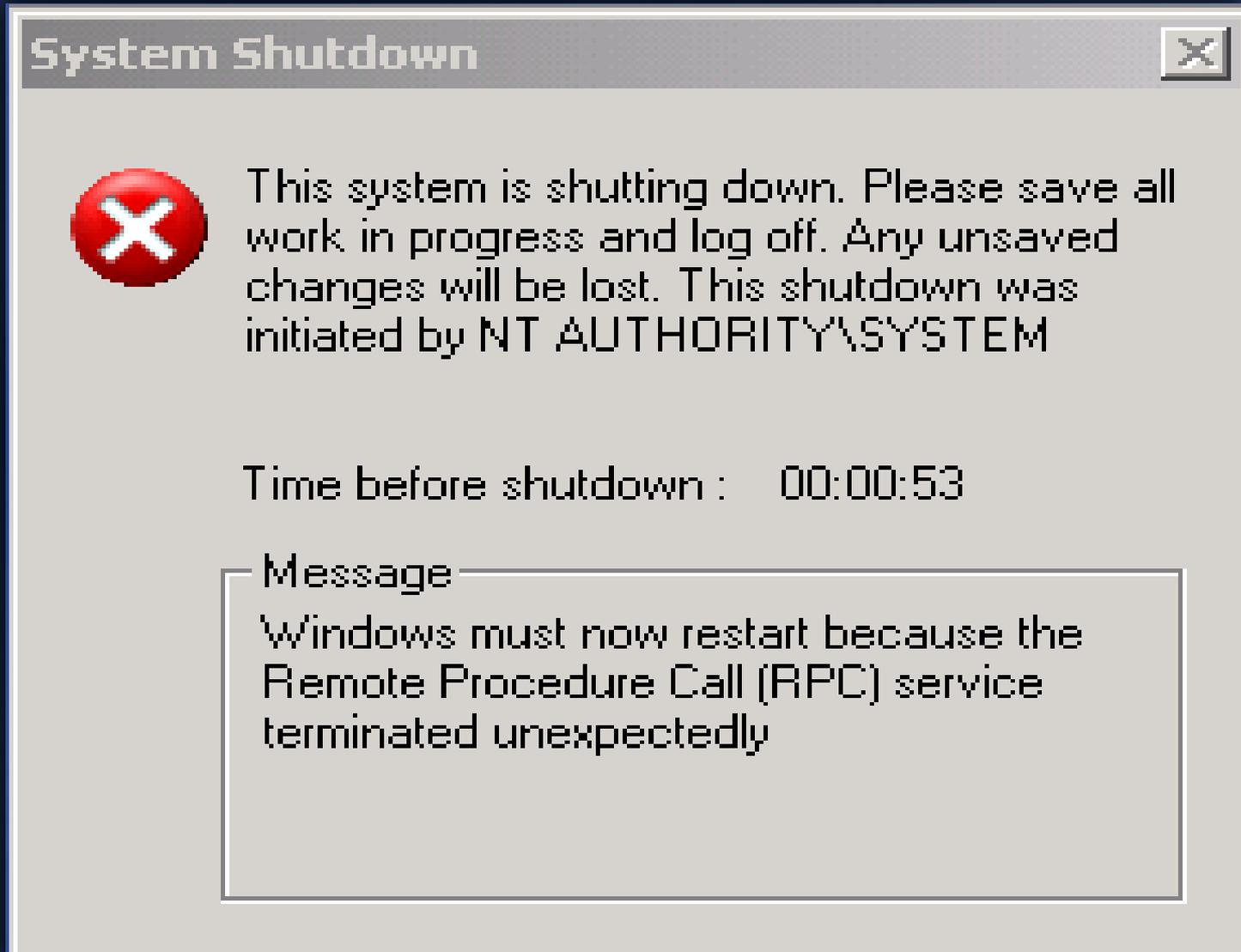
Focusing on the problem . . .

Online Crash Analysis

- 500 million PCs are capable of reporting system crashes
- 600,000 kernel reports a day



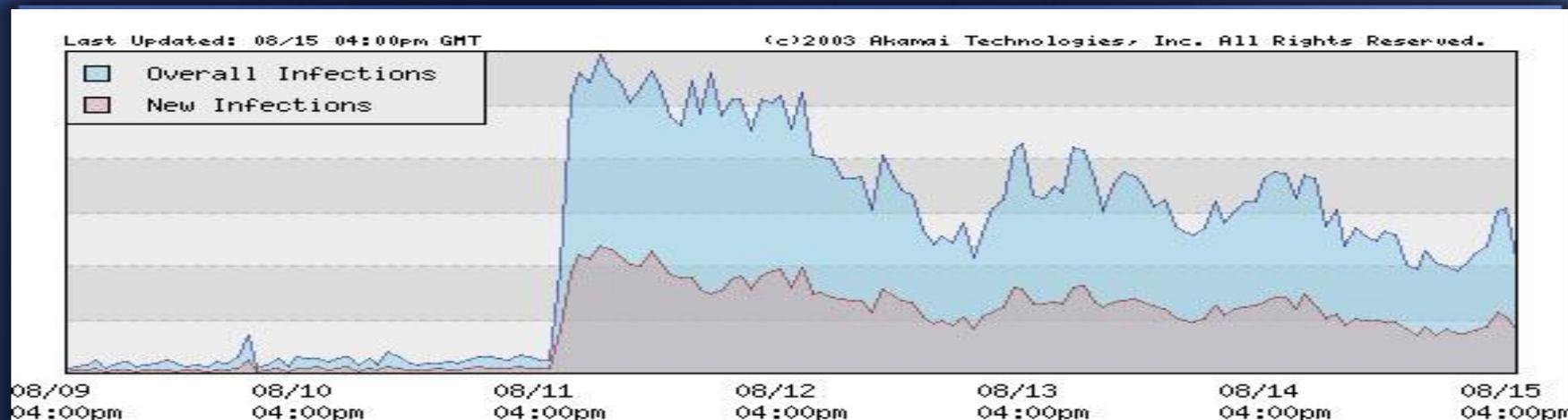
Online Crash Analysis



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

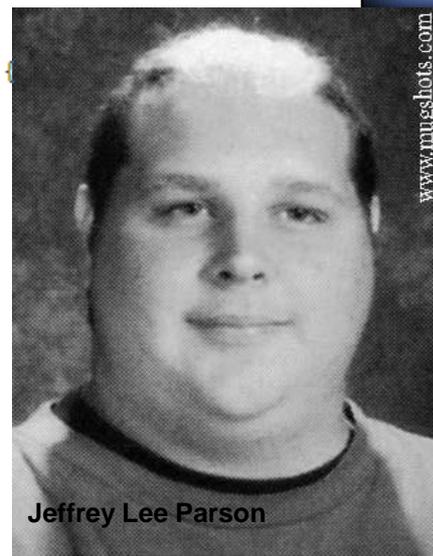
Investigation



Port 135 (i.e. The Internet)

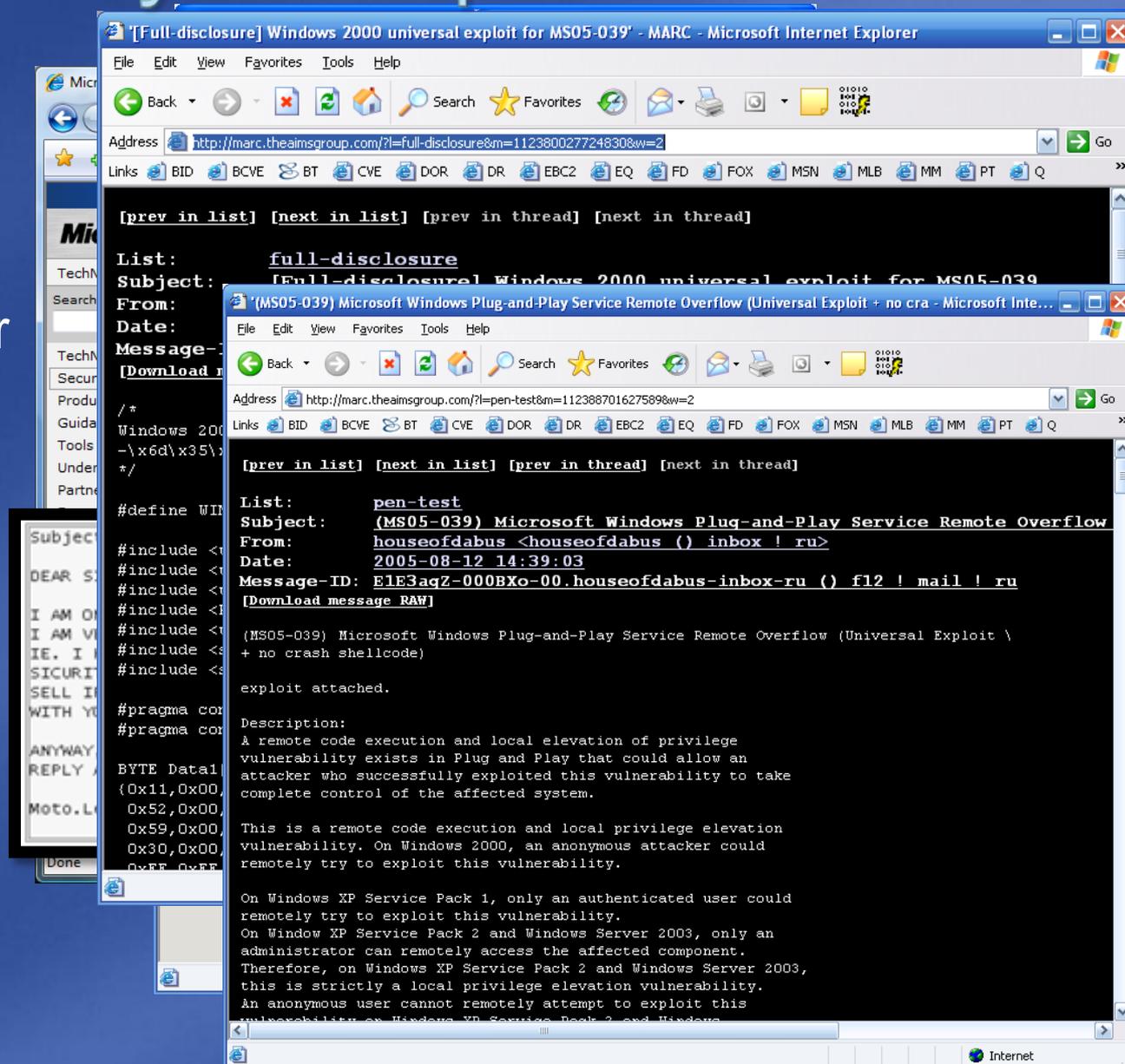
```
error_status_t _RemoteActivation(WCHAR *pwszObjectName, ... ) {
    *pshr = GetServerPath( pwszObjectName, &pwszObjectName);
    ...
}

// GetServerPath calls GetMachineName directly w/ pwszObjectName...
HRESULT GetMachineName(
    WCHAR * pwszPath,
    WCHAR wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN + 1]) {
    pwszServerName = wszMachineName;
    LPWSTR pwszTemp = pwszPath + 2;
    while ( *pwszTemp != L'\\' )
        *pwszServerName++ = *pwszTemp++;
    ...
}
```

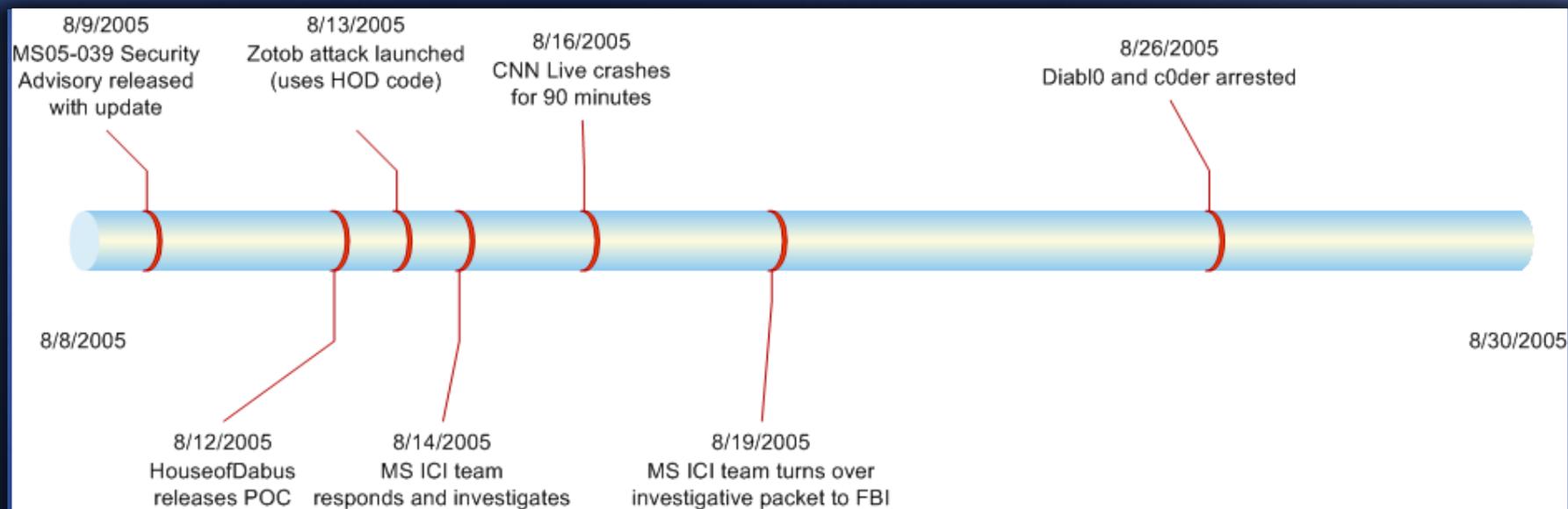


From Advisory to Exploit

1. Original Advisory
2. Newsgroup chatter
3. Private offers
4. 1st Exploit
5. 2nd exploit
6. 3rd exploit (which became Zotob)



Zotob



```
PNP_QueryResConfList (  
    [in]                handle_t    hBinding,  
    [in, string, ref]   LPWSTR      pDeviceID,  
    [in]                RESOURCEID  ResourceID,  
    [in, size_is(ResourceLen)] LPBYTE ResourceData,    <<---- cast to CS_STRUCTURE* pCsData  
    [...]  
    // copy the legacy and class-specific signature data  
    //  
    ptr = (LPBYTE) ((LPBYTE)pResDes +  
                  sizeof(CM_PARTIAL_RESOURCE_DESCRIPTOR));  
  
    memcpy(ptr,  
           pCsData->CS_Header.CSD_Signature +  
           pCsData->CS_Header.CSD_LegacyDataOffset,  
           pCsData->CS_Header.CSD_LegacyDataSize);  
  
    ptr += pCsData->CS_Header.CSD_LegacyDataSize;  
  
    memcpy(ptr,  
           pCsData->CS_Header.CSD_Signature,  
           pCsData->CS_Header.CSD_SignatureLength);
```

Zotob

- C0der

- Atilla Ekici

- 21 Years Old

- Sakarya, Turkey

- Member of Turkcoders, a 10 member financial crime ring

- Buys a worm with a botnet payload Credit Card numbers from “diabl0”

- Diabl0

- Farrid Essebar

- 18 years old

- Moroccan

- Member of 0x90 hacking crew

- Sells botnet exploit to c0der



Additional perspective . . .

MS07-029

Article ID: 935966 - Last Review: December 3, 2007 - Revision: 3.5

MS07-029: Vulnerability in Windows DNS RPC interface could allow remote code execution

View products that this article applies to.

On This Page

Expand all | Collapse all

INTRODUCTION

Microsoft has released security bulletin MS07-029. The security bulletin contains all the relevant information about the security update. This information includes file manifest information and deployment options. To view the complete security bulletin, visit one of the following Microsoft Web sites:

- Home users:
<http://www.microsoft.com/protect/computer/updates/bulletins/200705.msp>
- IT professionals:
<http://www.microsoft.com/technet/security/bulletin/ms07-029.msp>

[↑ Back to the top](#)

Known issue with this security update

After you install security update 935966, the workaround that is described in the following Microsoft Knowledge Base article should be removed:

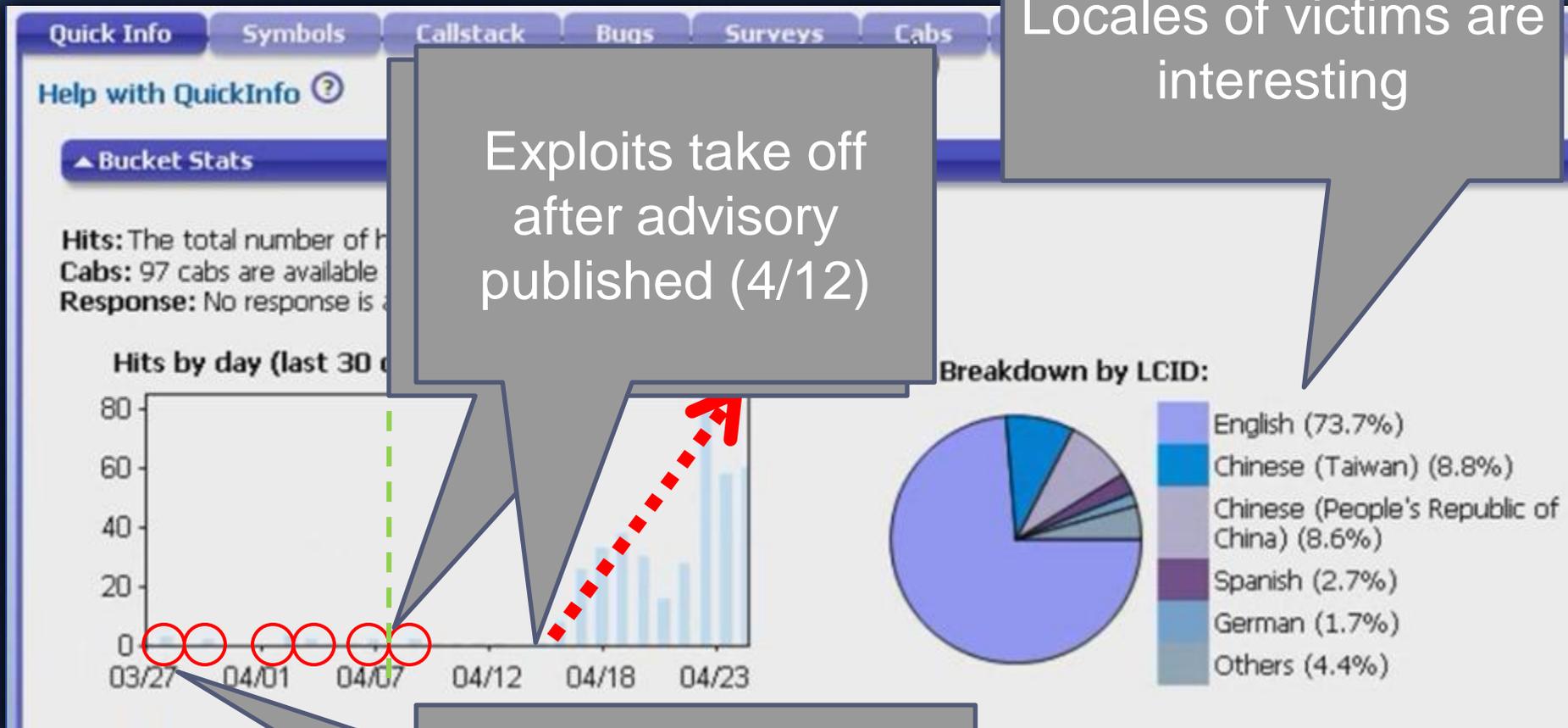
[936263](#) How to disable remote administration of the DNS Server service in Windows Server 2003 and in Windows 2000 Server

Otherwise, Remote Management of the DNS server by using Microsoft Management Console may fail.

[↑ Back to the top](#)

[↓ Back to the top](#)

MS07-029



Exploits take off after advisory published (4/12)

Locales of victims are interesting

But what are these crashes (going back to 3/8)

Opportunity

January						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

February						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

March						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

April						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

May						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

June						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

July						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

August						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

September						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

October						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

November						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

December						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

January						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

February						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

March						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

April						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

May						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

June						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

July						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

August						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

September						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

October						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

November						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

December						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

January						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

February						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

March						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

April						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

May						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

June						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

July						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

August						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

September						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

October						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

November						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

December						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

2005

2006

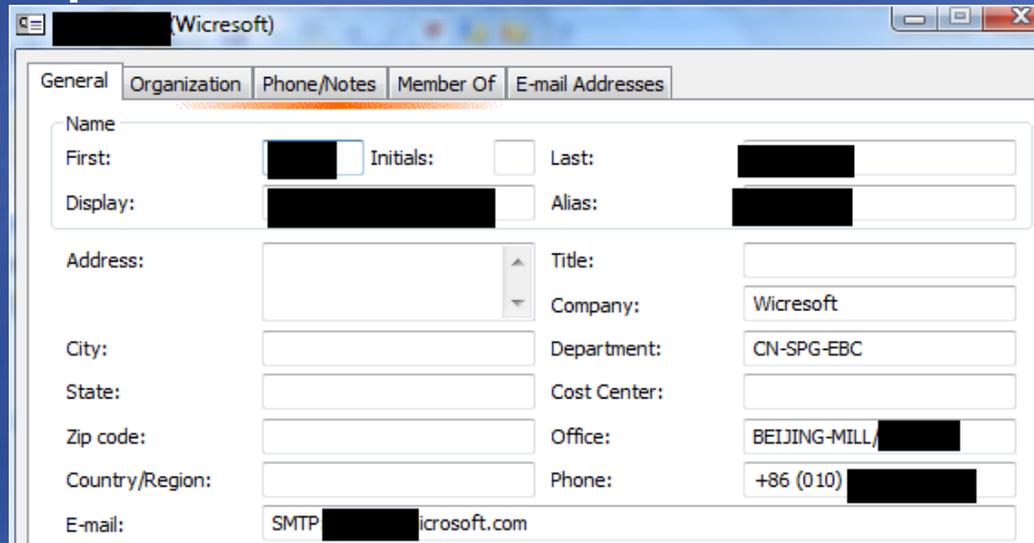
2007

CAB	Date Created	Size	OS Info	Exception	Symbol	Problem Class
256424826	12/13/2005	296,033	Win2003 SP1	stack buffer overrun	DNS.EXE! Lookup_ZoneTreeNodeFromDottedName	GS_FALSE_POSITIVE_EBP_ESP_CORRUPT
297414667	8/1/2006	523,309	Win2003 SP1	stack buffer overrun	DNS.EXE! Lookup_ZoneTreeNodeFromDottedName	STACK_OVERRUN
298064488	8/4/2006	562,465	Win2003 SP1	stack buffer overrun	DNS.EXE! Lookup_ZoneTreeNodeFromDottedName	STACK_OVERRUN
331396577	3/8/2007	335,317	Win2003 SP1	stack buffer overrun	DNS.EXE! Lookup_ZoneTreeNodeFromDottedName	STACK_BUFFER_OVERRUN

On the front lines . . .

November 2007 Attack

- Found machine on corporate network that pinged out at regular intervals to an interesting IP address
- Machine reported AV software installed and running but no detections/cleaning
- Routine process kicks in



The image shows a screenshot of a Microsoft Exchange Global Address List (GAL) entry for a user at Wicresoft. The window title is "[Redacted] (Wicresoft)". The "General" tab is selected, showing the following information:

Name	
First:	[Redacted] Initials: [Redacted] Last: [Redacted]
Display:	[Redacted] Alias: [Redacted]

Address:	
[Redacted]	Title: [Redacted]
City:	Company: Wicresoft
State:	Department: CN-SPG-EBC
Zip code:	Cost Center: [Redacted]
Country/Region:	Office: BEIJING-MILL/[Redacted]
E-mail:	Phone: +86 (010) [Redacted]
SMTP [Redacted]@wicresoft.com	

Now Things Get Interesting

- Image of machine image piped back to our labs
- Tasks – evaluate risk to MS
 - Reverse engineer the malware
 - Determine original infection vector
 - Spread mechanism & spread rate
 - Identify data exfiltration method
 - Any secondary infections
 - Possible inside involvement
- Initial infection appeared Oct 17, 2007

Infection Log

19:19:01 29.11.2007 Log begin:

Response Reason: Start

Ch 1.0 ID:-1 CHNV-HUAZ

NetAdapter(00):Intel(R) PRO/Wireless 2200BG Network Connection - Packet Scheduler Miniport
MAC 00:15:00:39:44:95 Type:6

GatewayList: ;

DHCP Server: 157.60.74.5;



19:19:21(+5 hour) 29.11.2007

WIN DIR=C:\WINDOWS; WORK DIR=C:\WINDOWS\system32; TEMP DIR=C:\DOCUME~1\v-huaz\LOCALS~1\Temp\; USER=v-huaz;

5.1.2600 Service Pack 2

19:20:01 Enumerating list:

19:20:01 id: C2F8E4F2

19:20:01 id: 38EA4802

19:20:01 id: F2DA6F38

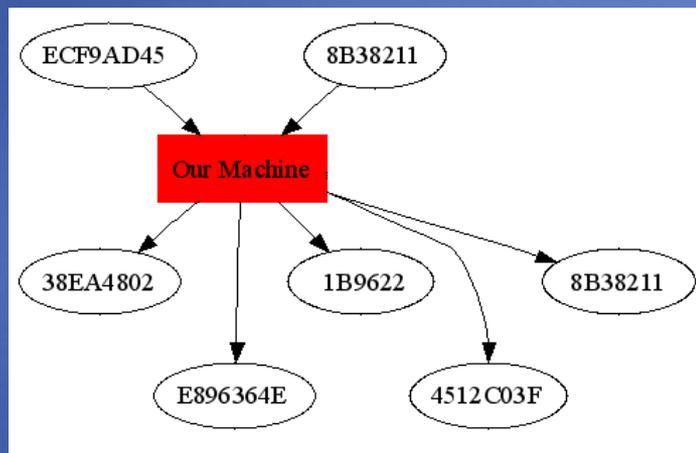
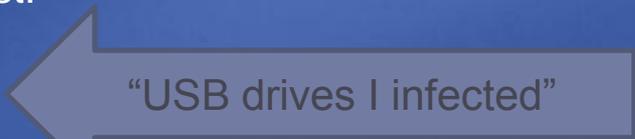
19:20:01 id: 1FCA7015

19:20:01 Enumerating Nlist:

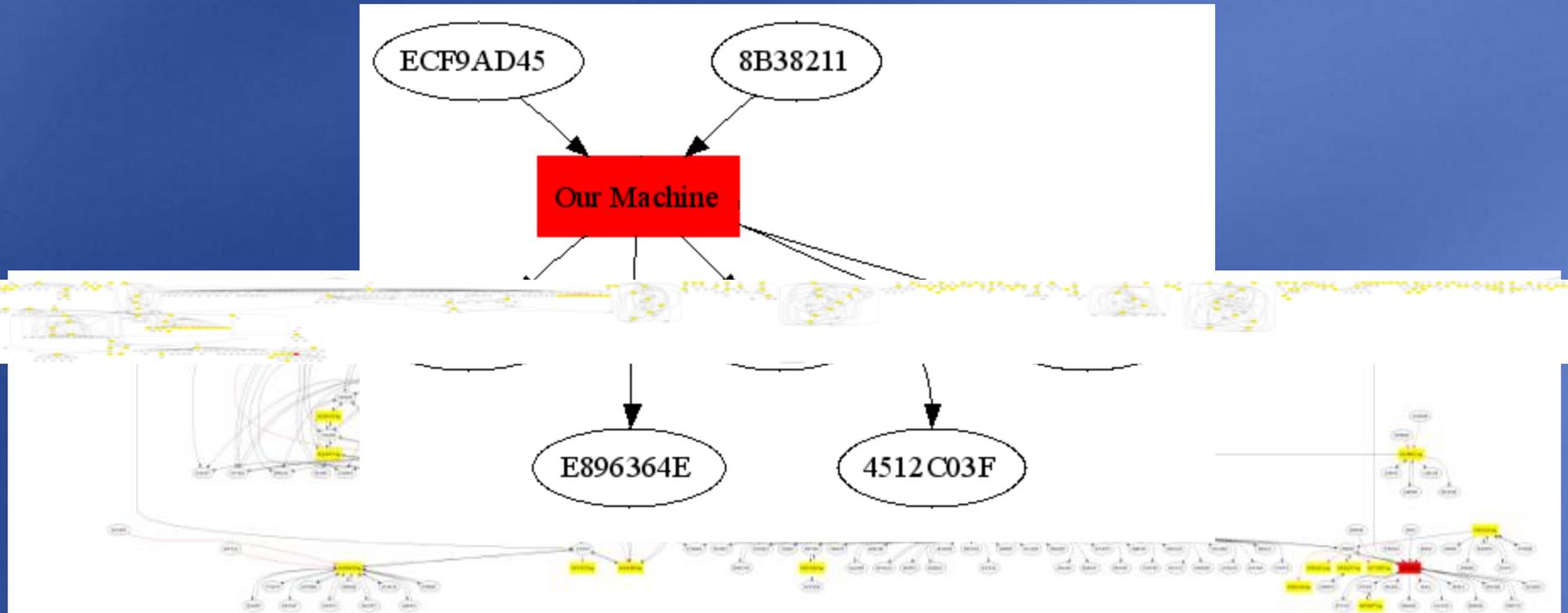
19:20:01 id: 8B38211

19:20:01 id: ECF9AD45

19:20:01 Log end.



Collect and Build The Graph

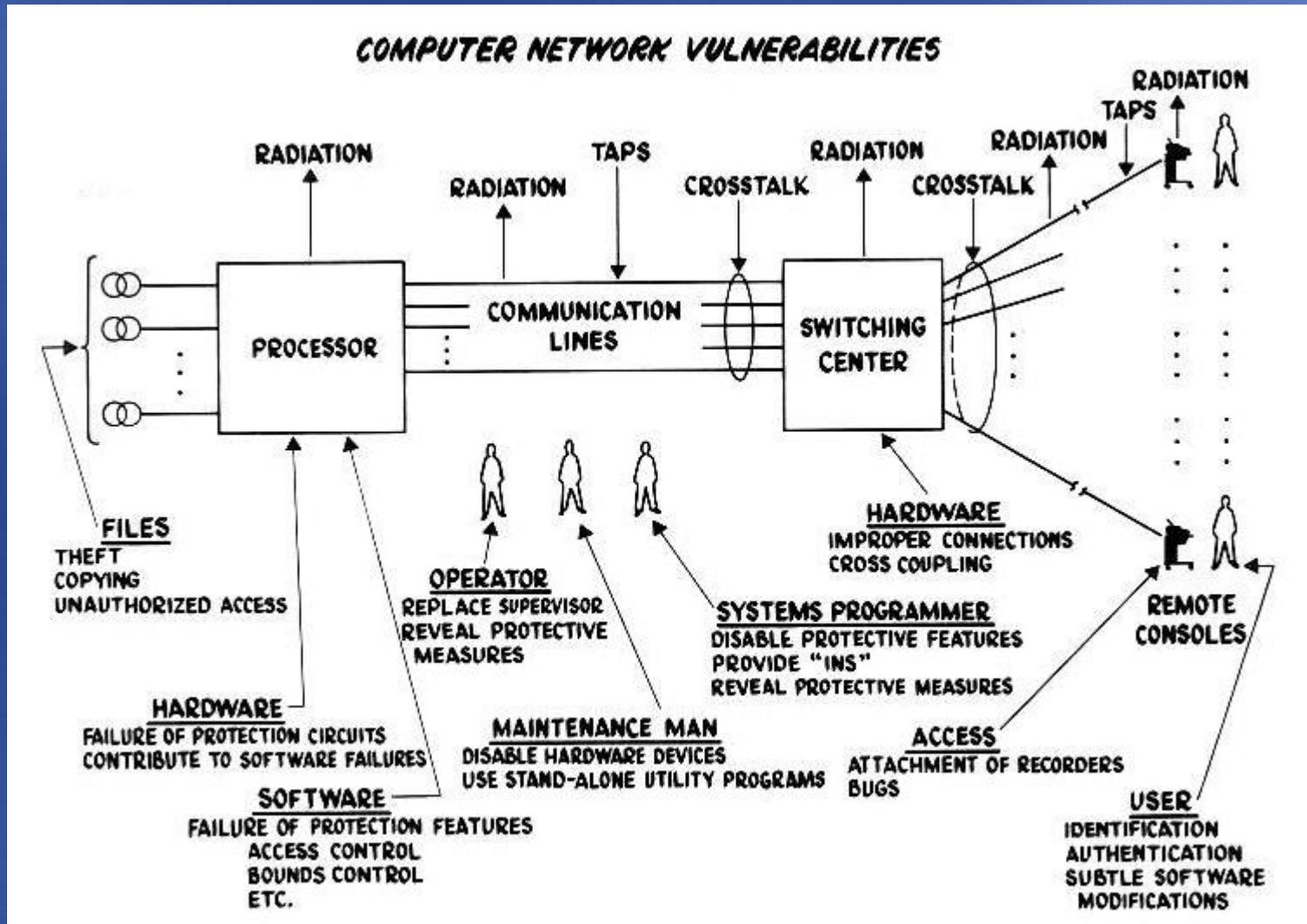


Collaboration

- Discussion with US/UK indicate this is indeed interesting software, and we have the very first sample
- January briefings in UK & US
- Discussions/trading samples & analysis
- Ongoing work to understand spread – OCA
 - How can crash reporting be used?
 - What are OCA strengths?
 - What can it tell us about this threat?

Sometimes old is new . . .

A long term problem



Our World is Flat ...

- Growth of the internet
- Societal & Cultural Environment
- Cyber Threat Business Models
- Macroeconomic Environment
- Sophistication of Attacks
- A long term problem . . .



Microsoft[®]

Your potential. Our passion.[™]