Reducing Risks from Cyber Attacks

Presented for Cyber Security Awareness Month 2012

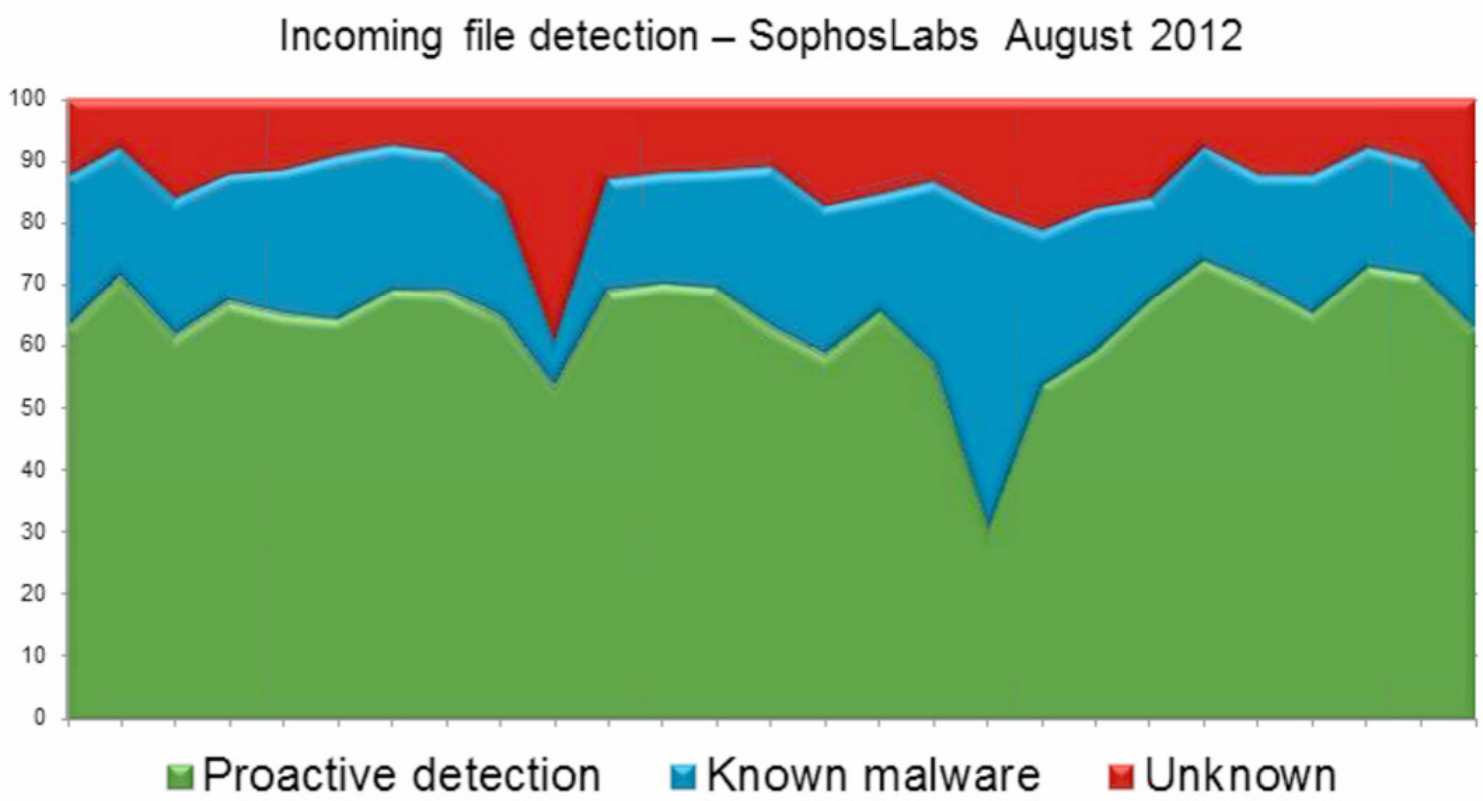
Tim Gurganus
tim_gurganus@ncsu.edu

History of Malware at NC State University

- 100K to 200K samples submitted everyday to antivirus companies
- Analysis done by automation

- 25 years ago – manual analysis, figure out how it spreads, create fingerprint/pattern for detection

Detection is half the story



SOPHOS

History of Malware at NC State University

- 1986 – Brain.A spread via 5 1/4” floppy
  - Written by two brothers in Pakistan as a POC to prove PC-DOS was not as secure as Unix
  - Now running Brain Telecommunications
  - Stone and Cascade were basically same as Brain
  - Spread when an infected floppy was left in the floppy drive and DOS restarted – BIOS was set to boot from any floppy
  - Every floppy put into the infected PC got infected
  - Yankee Doodle was a .COM infector that infected all .COM files on the floppy to spread

History of Malware at NC State University

- 1990 Joshi virus
- Did nothing until one day a year
- PC wouldn’t boot until you typed:
  - Happy Birthday Joshi

History of Malware at NC State University

- 1991 – viruses spread via 5 1/4” floppy and had a visual component
  - Viruses like Form and Dark Avenger had a visual component
  - You would know you were infected by the sound played or the graphics shown
  - Omega – displayed Omega character on the screen if 13th of the month was a Friday
  - Later viruses opened and closed the CD tray to indicate infection

History of Malware at NC State University

- 1992 Michelangelo virus
- Destroyed files on infected PC
- Overwrote the first 100 sectors of the infected disk so files were lost and the PC wouldn’t boot

History of Malware at NC State University

- 1993 Disk Destroyer
- Copied FAT into RAM and overwrote the copy on disk
- Displayed slot machine game on screen and let you have 5 turns
- If you happened to win the jackpot, it copied the FAT back to disk, if not you lost your FAT and files were no longer accessible

History of Malware at NC State University

History of Malware at NC State University

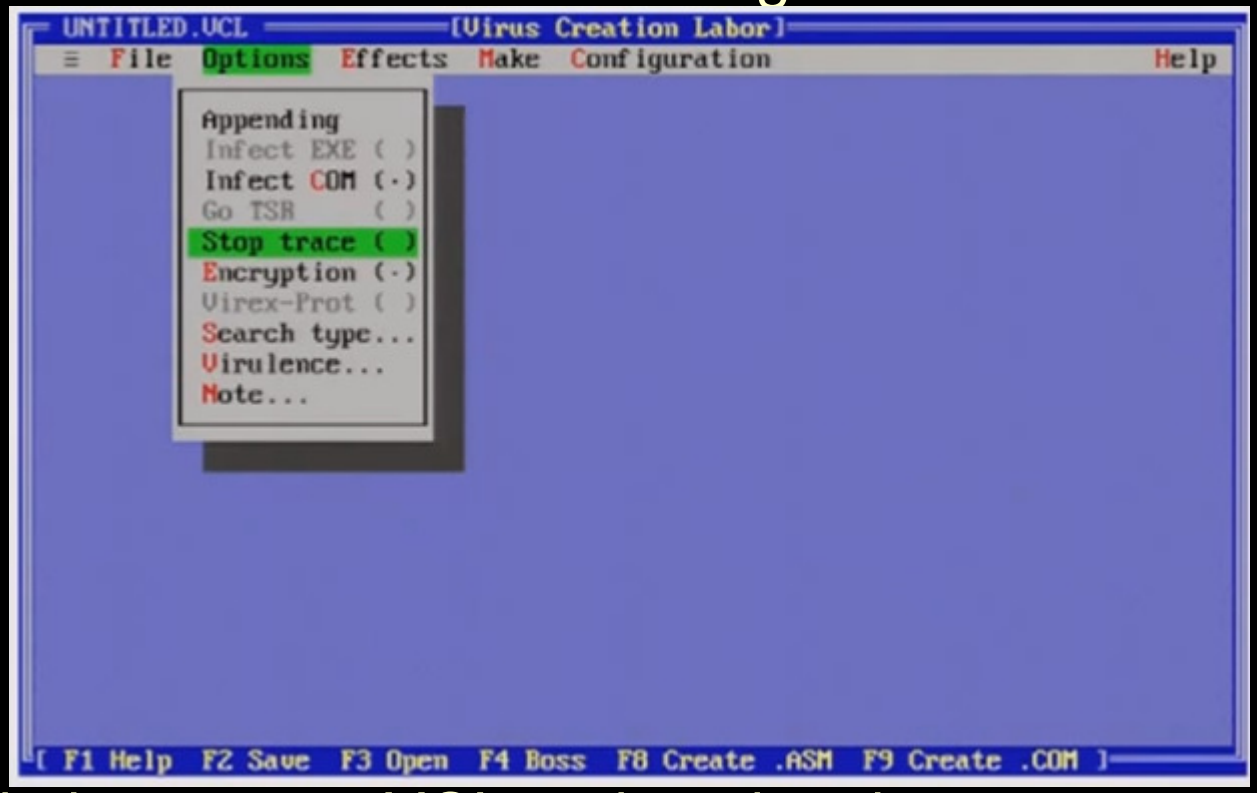
- Today's malware is different
- You will not know you are infected when malware like ZeroAccess rootkit or Zeus is installed
- Older malware could crash the system
  – that rarely happens today

History of Malware at NC State University

- 1992 MtE – First virus mutation engine
- Written by Bulgarian virus writer known as Dark Avenger
- A kit for making any virus a polymorphic virus

History of Malware at NC State University

- 1992 VCL - First Virus creation lab
- A kit with a text GUI for creating viruses



- Click the menus, VCL makes the virus

History of Malware at NC State University

- 1992 Windows viruses appeared
- WinVir – written for Windows 3.0
- Infected the Windows PE file structure which was different from MS-DOS .exe and .com infectors

- 1993 Monkey virus - encrypts and moves the partition table
- 1994 OneHalf virus – encrypted ½ of the hard drive (by XORing sector data with a random key)
  - Encrypted a little of the drive every boot
  - When half of the drive was encrypted, decryptor stopped working and drive data was lost unless you knew how to reverse the encryption

History of Malware at NC State University

- 1995 Concept virus – first Office document infector
- Infected documents instead of boot sector or programs
- Written in VBA (Visual Basic for Applications) scripting language
- Virus code ran when Word document was opened (init) or saved (infected other documents when saved)
- Became the most common virus in the world within 30 days

History of Malware at NC State University

- 1996 Laroux virus – first Excel document infector
- Infected documents instead of boot sector or programs
- Written in VBA (Visual Basic for Applications) scripting language
- Virus code ran when Excel document was opened (init) or saved (infected other documents when saved)
- ***Variant of Laroux randomly changed spreadsheet values by rounding them up or down by 0.001% once a day***
- Took a long time to notice infection and by then usually all copies were corrupt

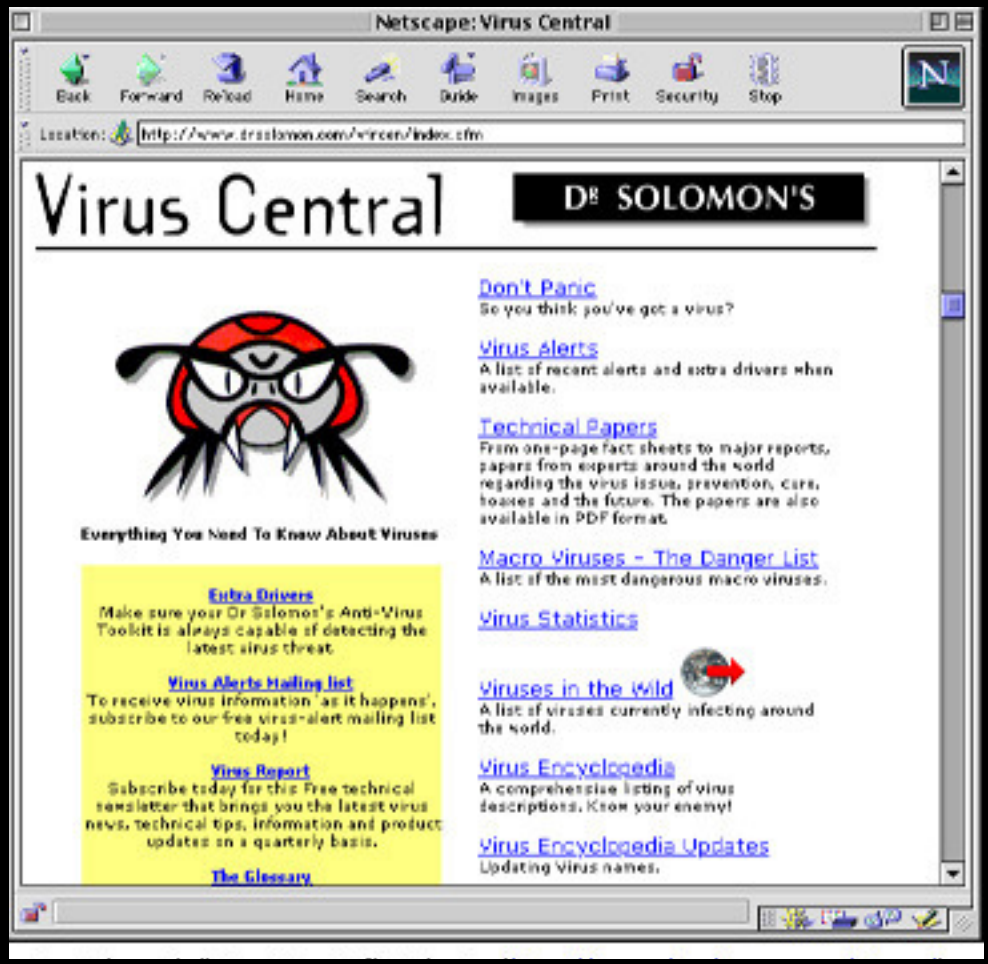
History of Malware at NC State University

- 1996 Boza virus – First Windows 95 virus

- Virus writers were seeking fame and notoriety

History of Malware at NC State University

- 1997 NCSU purchases Dr. Solomon Antivirus Toolkit

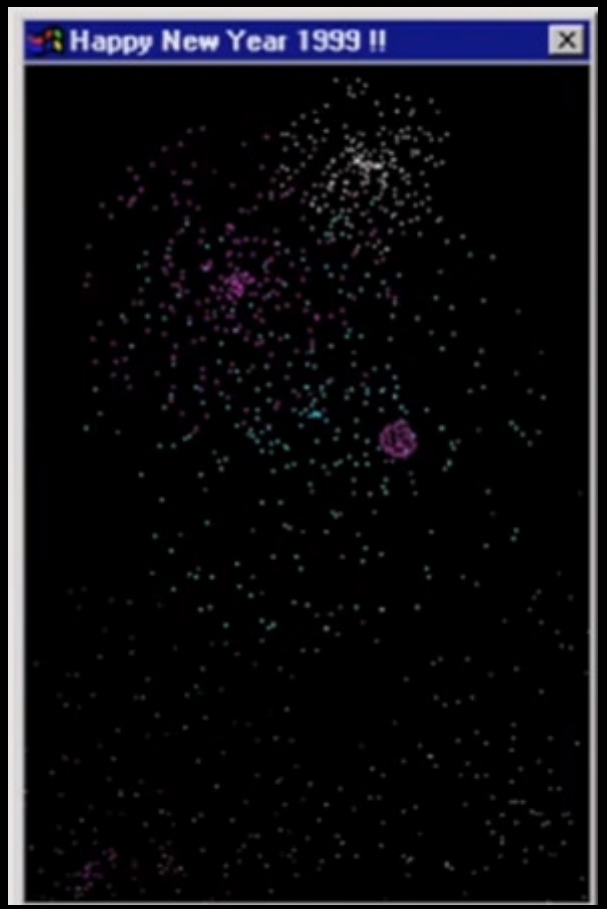


- Detects and removes viruses from DOS, Windows, Windows 95, Windows NT and Macintosh systems

- Could recognize more than 1,400 different types of viruses, including macro viruses

History of Malware at NC State University

- 1998 RemoteExplorer malware
- 1998 Happy99 virus – first **Email worm**



Email claimed to be a 'Happy New Year' card for 1999

As it displayed animation, it emailed a copy of itself to everyone in your Outlook address book (message appeared to come from the infected user)

Virus attached to message named happy99.exe

These kind of email worms quickly became a big problem

History of Malware at NC State University

1999 First email viruses in .zip file format

Melissa – First Macro virus spread via Email

- one of the largest out breaks on campus

- Used Outlook for sending email
- Infected Word documents
- Sent copy of itself as attachment in Word document
- Document was randomly selected from the hard drive of the infected user's PC (great for data leakage)

History of Malware at NC State University

2000 Loveletter virus

Sent emails with subject: I love you

Used email addresses from Outlook Address book

Also one of the largest email virus outbreaks on campus

Sent network passwords back to its author in the Philippines

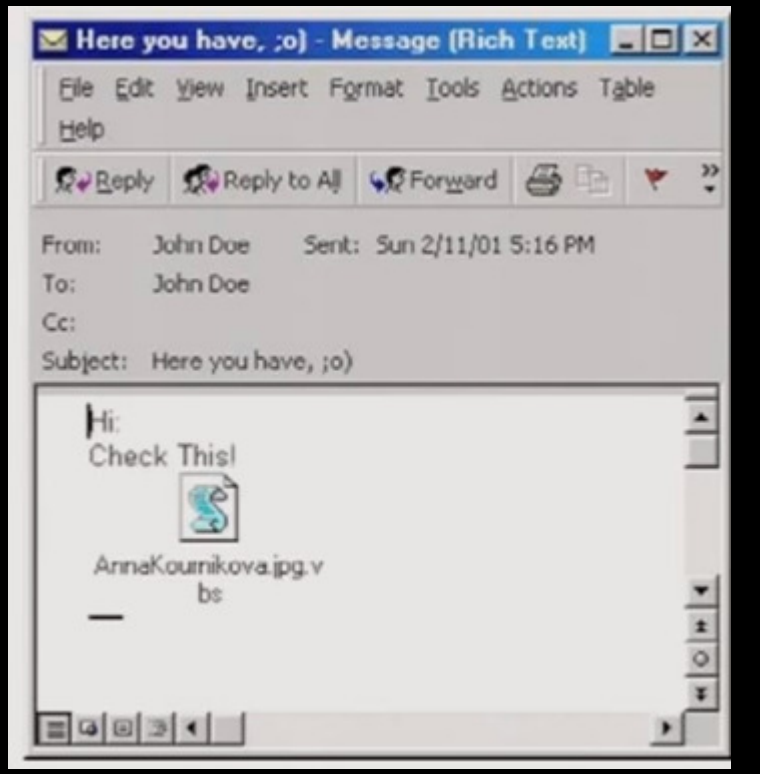
Also in 2000, **NCSU purchases a site license for Norton Antivirus** for home and campus computers

History of Malware at NC State University

2001 Annakournikova virus

Also spread via email

Used popular tennis player for social engineering to get you to open the email attachment



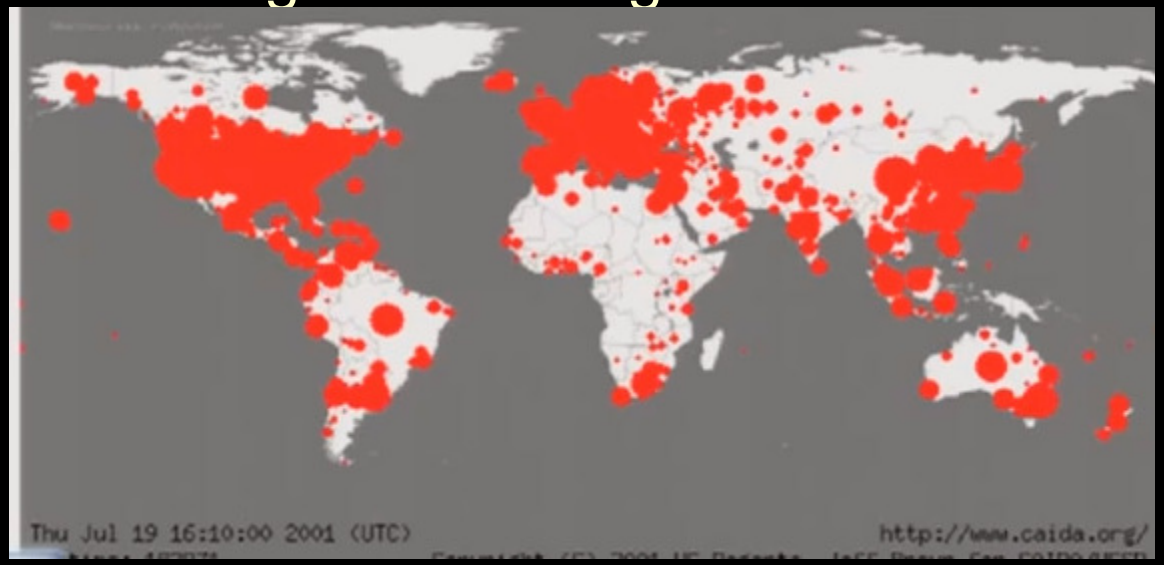
History of Malware at NC State University

2001 Code Red – Worm infected Windows IIS Servers

Released one week after US spy plane made an emergency landing in China

Code Red program had the phrase “Hacked by Chinese” at the end of the file

Code Red targeted the English version of Windows



Map of Infections in first 24 hours

Included DDOS Code targeting whitehouse.gov by IP address

History of Malware at NC State University

2001 Sircam also spread via email

2001 Nimda - First virus to spread via Windows File sharing

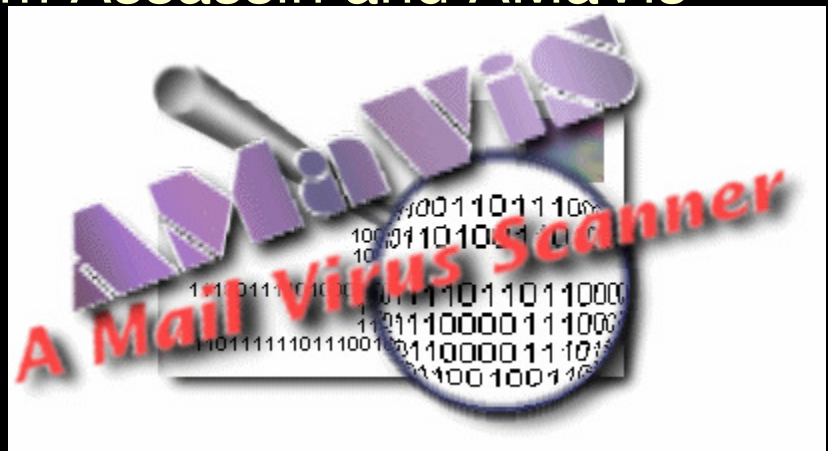
Found 1 week after September 11, 2001 terrorist attacks

2002 Klez – Overloaded NCSU campus email servers

2002 Bugbear – Email worm

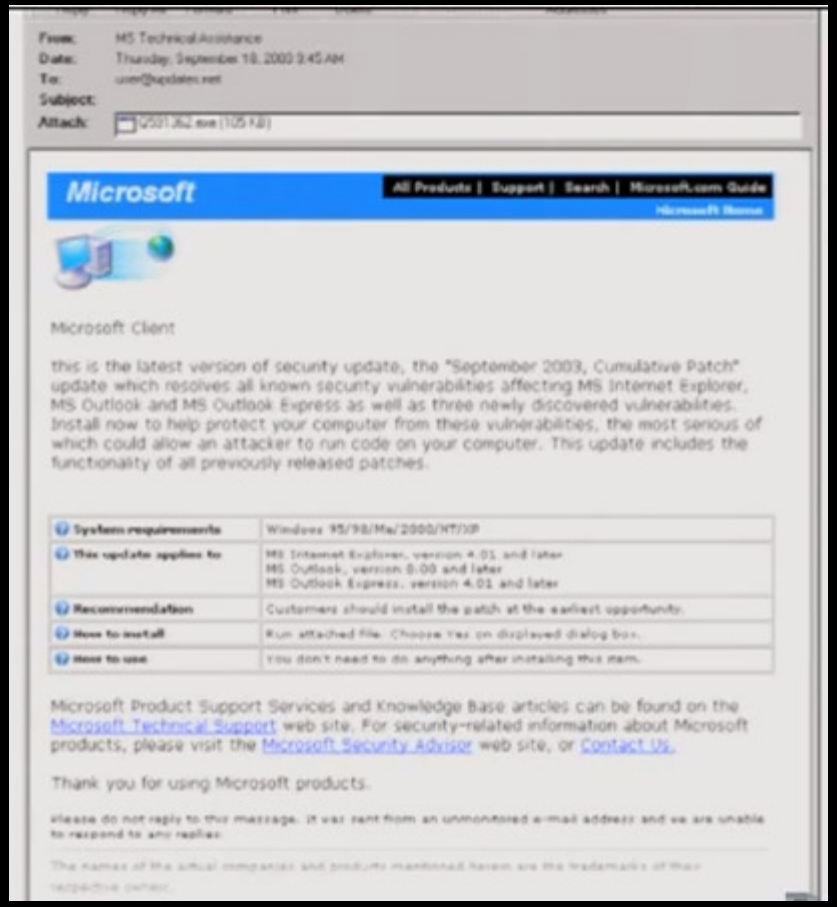
2002 Slapper worm – infected Linux Apache servers

2003 NCSU starts running Spam Assassin and AMaVis antivirus on mail servers



History of Malware at NC State University

2003 Swen - fake Microsoft update arrived in email



Email had same wording, Graphics and links as a real Bulletin from Microsoft at the time

Spoofed sender was MS Technical Assistance

History of Malware at NC State University

2003 Swen - fake Microsoft update arrived in email

Microsoft Client

this is the latest version of security update, the "September 2003, Cumulativ
update which resolves all known security vulnerabilities affecting MS Internet
MS Outlook and MS Outlook Express as well as three newly discovered vulner
Install now to help protect your computer from these vulnerabilities, the mos
which could allow an attacker to run code on your computer. This update inc
functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportuni
How to install	Run attached file. Choose Yes on displayed dialog box.

Message dynamically included the current month and year

At this time, there was no Microsoft Update

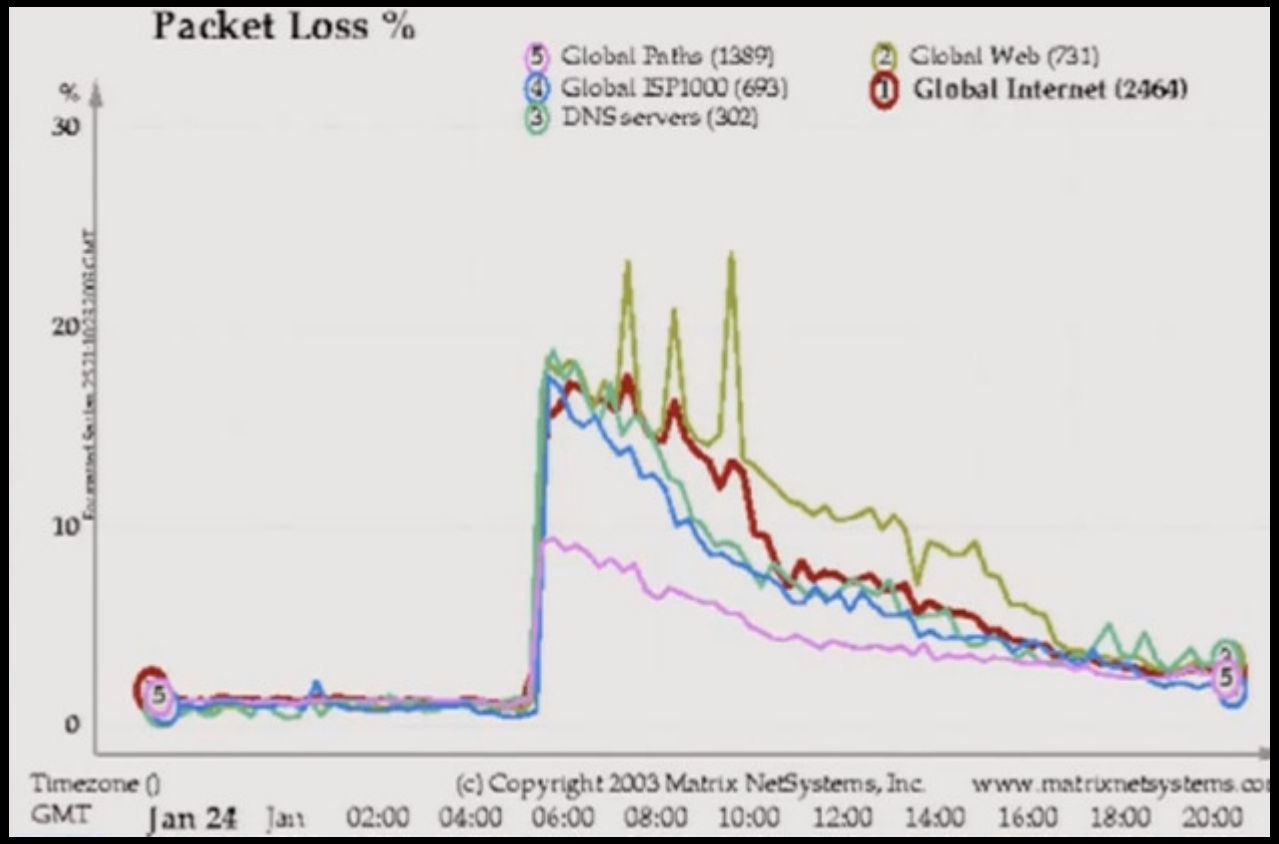
Attachment was named:

Q591362.exe

History of Malware at NC State University

2003 Slammer worm – infected Microsoft SQL servers

Spread world wide scanned all IPs in 20 minutes



Was memory resident - infection went away on restart

History of Malware at NC State University

8/13/2003 MS Blaster – used MS03-026 Exploit to spread

- Had code to DDOS Microsoft Windows update site
- Significant incident for NCSU campus
- Somewhat mitigated by Stealther outbreak 8/3/2003 before

History of Malware at NC State University

2003 Fizzer virus – First mass mailing malware used for sending spam

Prior to Fizzer, email worms spread themselves via email

Fizzer infected hosts ran a SMTP mail relay service

Access to infected hosts was sold to spammers **for profit**

This continues today as a way for virus writers to make money

Fizzer hijacked network bandwidth

Today's malware steals bandwidth, usernames and passwords

History of Malware at NC State University

2004 Sasser worm - Exploited MS04-011 vulnerability

Significant incident for NCSU campus

At this time, most Windows users were not running a firewall

Gateway port blocks were not effective in preventing these worms from spreading to campus

Computers infected with Blaster and Sasser displayed this window and rebooted after each infection

Often while trying to download the patch from Microsoft, the PC would be infected again and reboot again and again.

History of Malware at NC State University

Where Malware was developed:

History of Malware at NC State University

Where Malware is developed now:

History of Malware at NC State University

2003 Sobig virus – money making virus sent spam

2003 SDBot - Open source botnet controller and agent

2004 Mydoom – also used for sending spam

- One of the biggest outbreaks on campus
- Spread via email and P2P network Kazaa
- Had DDos functions as well as mass mailing

2004 Bagle – mass mailing malware

2004 Netsky – spam generating malware

2005 Mytob, Zotob – botnets used for spamming, scanning, Spreading malware, DDos, Installing Rootkits

History of Malware at NC State University

2005 Haxdoor rootkit used to hide botnet or any other malware

2006 Warezov – malware used for file trading XDCC type networks

2007 Storm worm – used email with link to a website

Emails had many themes/stories

Infected hosts communicated using encrypted Peer-to-Peer network

Significant event for NCSU campus due to large number of variants

Email and Antivirus struggled to keep up with malware changing

2008 Mebroot – root kit used to hide other malware like torpig

Still have a few infections each year on campus now

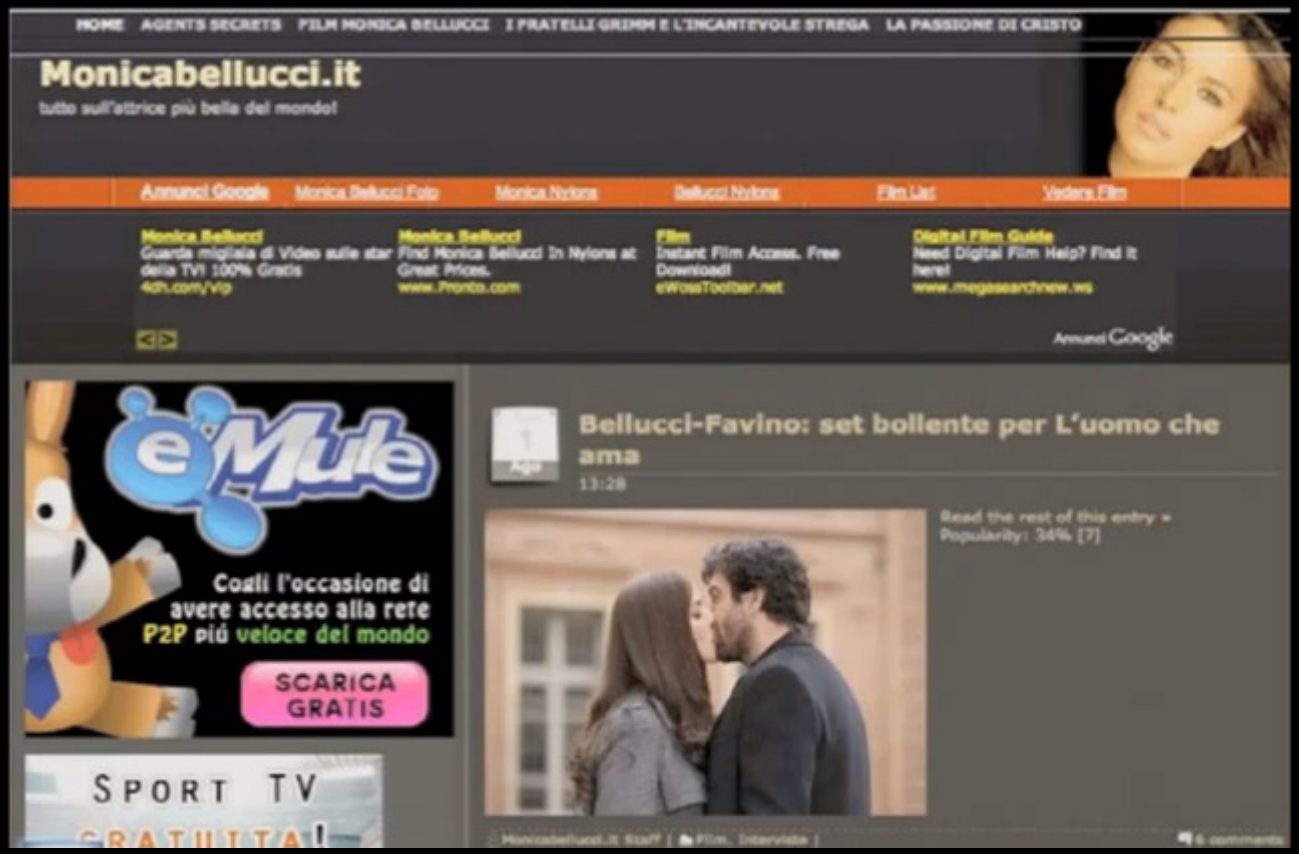
One of the most advanced malware seen

Infection came from viewing compromised website

monicabellucci.it was the first

History of Malware at NC State University

2008 Mebroot – root kit used to hide other malware like torpig



Mebroot infects MBR of PC hard drive

If PC bluescreened Mebroot sent debug Information back to the virus writers

1000s of Infections on campus

This is the main way infections occur up to the present time

Brief History of Malware

Economic Cost of Malware Worldwide:

Bugbear:	$ 3.9 billion
Love Bug:	$ 8.8 billion
Swen:	$ 10.4 billion
Yaha:	$ 11.5 billion
Mimail:	$ 11.5 billion
Klez:	$ 19.8 billion
MyDoom:	$ 22.6 billion
SoBig:	$ 37.1 billion

History of Malware at NC State University

2009 Conficker / Waledac

- Created large botnet – 12 million machines
- Update site changed everyday using complex algorithm
- Spread via network exploit, network share, flash drives and dictionary attack

2009 TDSS / TDL3 / TDL4 rootkits

- Even more advanced than Mebroot
- Rootkit supports 32 and 64-bit Windows 7
- 4.5 million infections worldwide
- 1000 infections on campus

Modern Malware Threats

Symantec Global Internet Security Threat Report

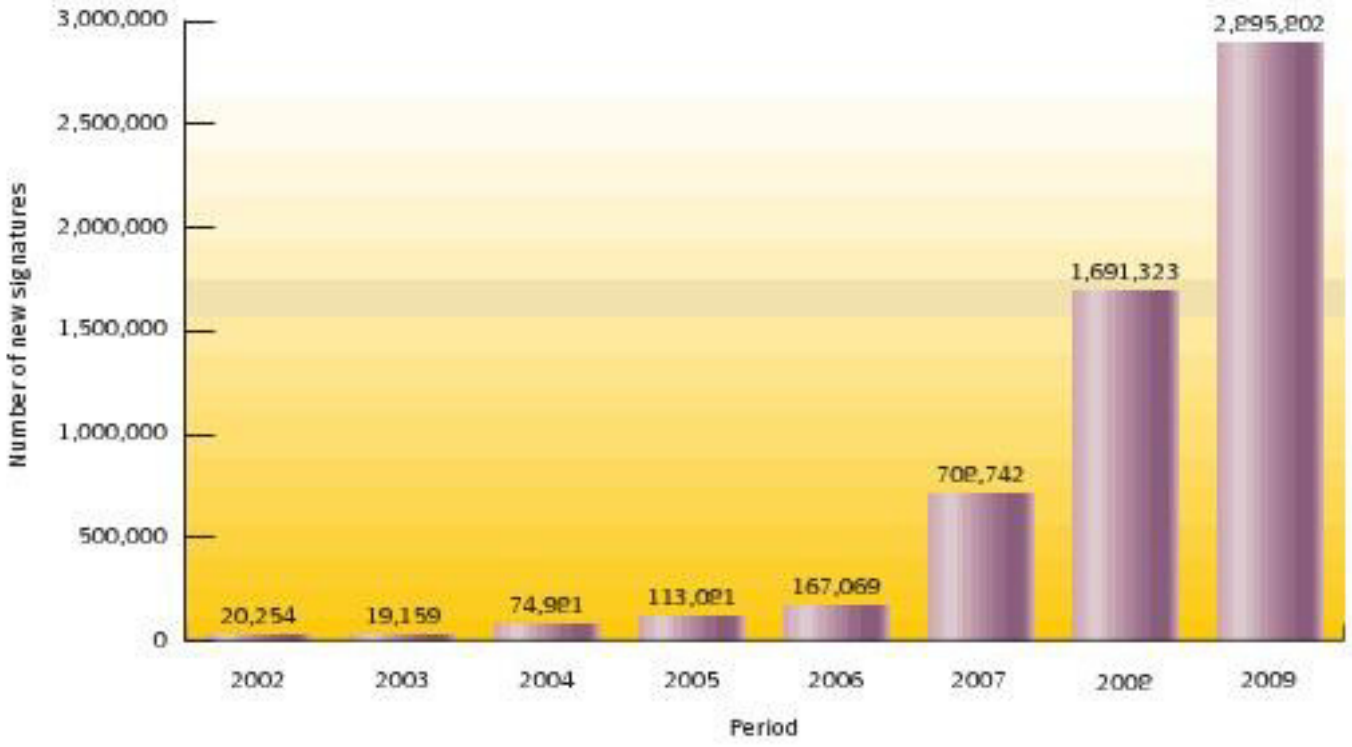


Figure 10. New malicious code signatures

Source: Symantec.

Malware Threats

- The number of crimeware application suites has grown in the last year making it easier to produce malicious code, build botnets, create phishing attacks, etc.

Example Crimeware applications are:

- Blackhole Exploit Kit
- Crimepack
- Eleonore
- Icepack
- Mpack
- Zombie Infection Kit
- SEO Sploit Pack
- Redkit Exploit Pack

CrimeWare Threats

Zombie Infection Kit:

Итого	100 %	1333	320	24.01 %
Iexplore 8	41.41 %	552	143	25.91 %
Iexplore 7	21.68 %	289	76	26.3 %
Firefox	18.9 %	252	42	16.67 %
Iexplore 6	12.45 %	166	52	31.33 %
Chrome	2.93 %	39	4	10.26 %
Unknown	1.43 %	19	1	5.26 %
Opera	1.2 %	16	2	12.5 %

This screen shot from Zombie Infection Kit Shows the real-time Browser exploitation Statistics.

Note the support for Firefox and Google Chrome.

CrimeWare Threats

SEO Sploit Pack:

This screen shot from the SEO Sploit Pack shows the Effectiveness of various exploits targeting Java, PDF and Windows.

Note the number of Java exploits.

CrimeWare Threats

SEO Sploit Pack:

This screen shot from the SEO Sploit Pack shows the Effectiveness of various exploits targeting Java, PDF and Windows.

Note the number of Java exploits.

Out of date Java clients are very common.

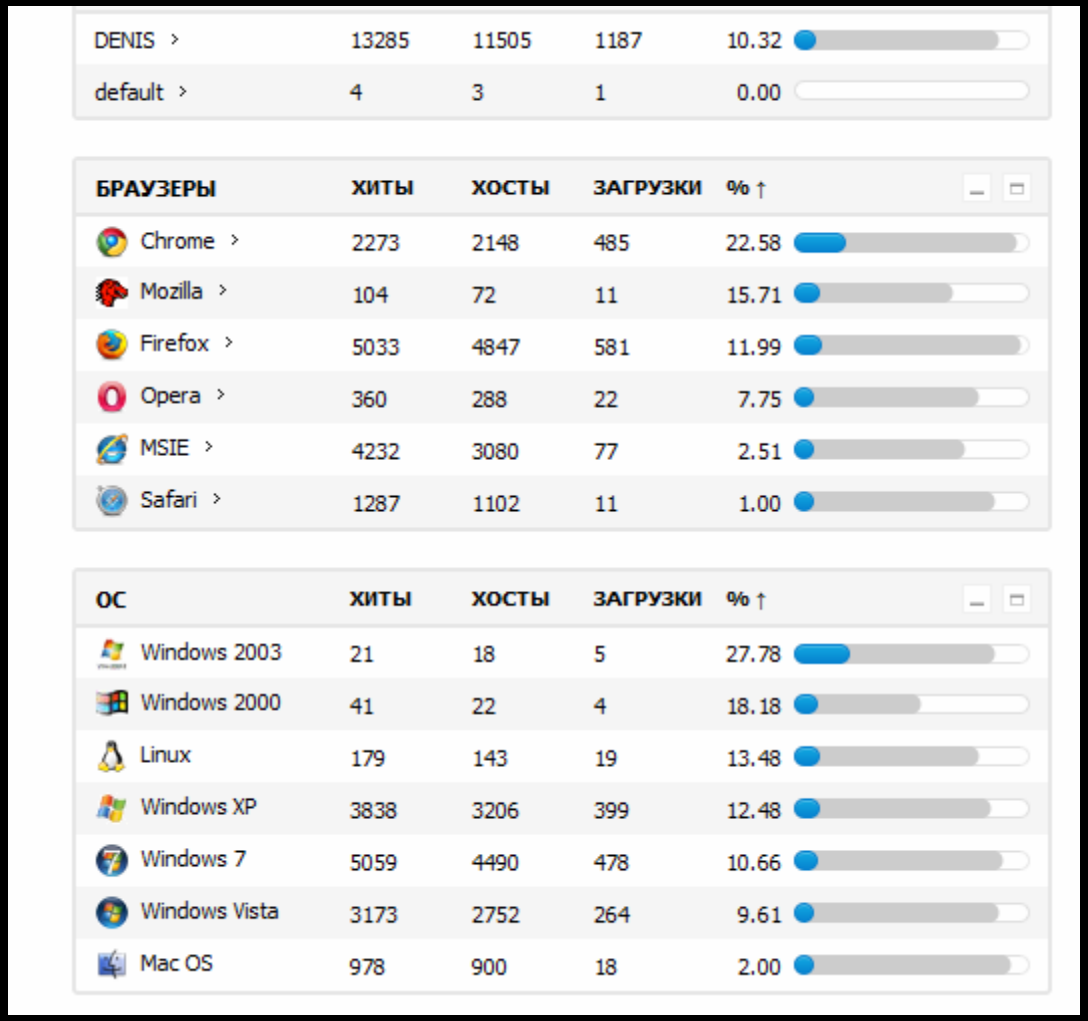
CrimeWare Threats

Blackhole Infection Kit:

This screen shot from Blackhole Infection Kit shows the efficiency of various exploits available in the kit.

CrimeWare Threats

Blackhole Infection Kit:



DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58
Mozilla ›	104	72	11	15.71
Firefox ›	5033	4847	581	11.99
Opera ›	360	288	22	7.75
MSIE ›	4232	3080	77	2.51
Safari ›	1287	1102	11	1.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78
Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48
Windows 7	5059	4490	478	10.66
Windows Vista	3173	2752	264	9.61
Mac OS	978	900	18	2.00

This screen shot from Blackhole Infection Kit shows the percentage of browsers and Operating Systems Infected.

Note the support for Opera, Safari and Google Chrome.

Some bots are Linux and OS X computers.

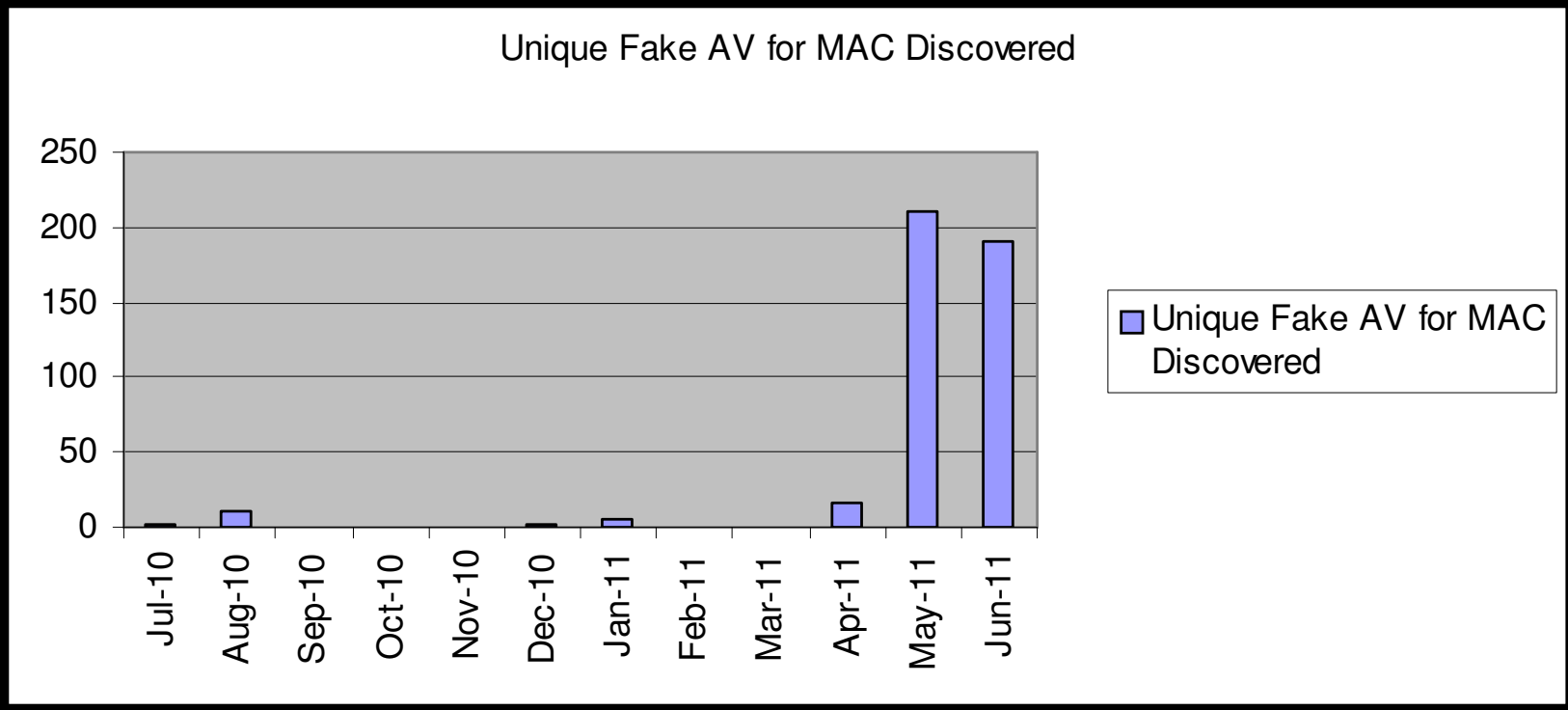
Over 500 Flashback Infections on Campus in 2012

Day	UUID	Kaspersky	Dr. Web	IP Address	Remedy ID
13	02093A70-4D79-550E-9560-48ED50ED0898	Yes	Yes	152.7.40.120	01654853
14	132A2A3C-4161-5A81-94C3-FE6CF9A50328	Yes	No	152.7.54.120	01654878
12	17AEA21E-D596-53BF-B4F1-57CCDEE4F1A7	Yes	Yes	152.7.57.85	01655174
12	1FE2B0C7-191F-5326-9B07-5068114A2B0F	Yes	No	152.7.33.40	01654760
14	282117E2-55E0-5B1B-A849-9BC0F748AD83	Yes	No	152.7.20.138	01654885
10	2C1919D9-CF5E-560A-B8E1-30F91981DB36	Yes	No	152.7.10.101	01655180
13	3ACD33AD-EDFD-51B3-A21C-F3941B877C25	Yes	Yes	152.7.24.168	01654860
13	542CA267-F2AB-5302-B3CE-CA364F8D93A5	Yes	Yes	152.7.46.169	01654861
12	557DA90A-31C7-5A35-996A-426B17823755	Yes	Yes	152.7.12.59	01654882
13	5D7D1B46-561B-5F09-AFD6-D6E37A602E84	Yes	Yes	152.7.31.148	01654857
12	5E8B9110-E2D1-59C7-93C4-718C8FA165D1	Yes	Yes	152.7.41.224	01654876
12	64C656AB-712E-5F6D-B52E-DB4D9FA66E48	Yes	Yes	152.7.59.141	01654931
12	64E2D992-83A5-5D3A-9787-2A23A1A4830E	Yes	Yes	152.7.16.58	01654873
14	65D2456A-63F7-5935-9E9C-A2F9A82835E9	Yes	Yes	152.7.56.219	01654890
12	66EDDC01-3A31-512E-A4EF-33A02664A190	Yes	No	152.7.56.187	01654765
12	69EFA529-78FB-5742-A0C4-926841AABD8F	Yes	Yes	152.7.32.110	01654871
14	79BD82F8-CFE7-5F18-BB24-6B6382ACB79F	No	Yes	152.7.65.91	1654883
12	7C244548-78FF-550B-B2B4-12F0176F7DD7	Yes	No	152.7.18.117	01654753

Viruses & Trojans At NCSU

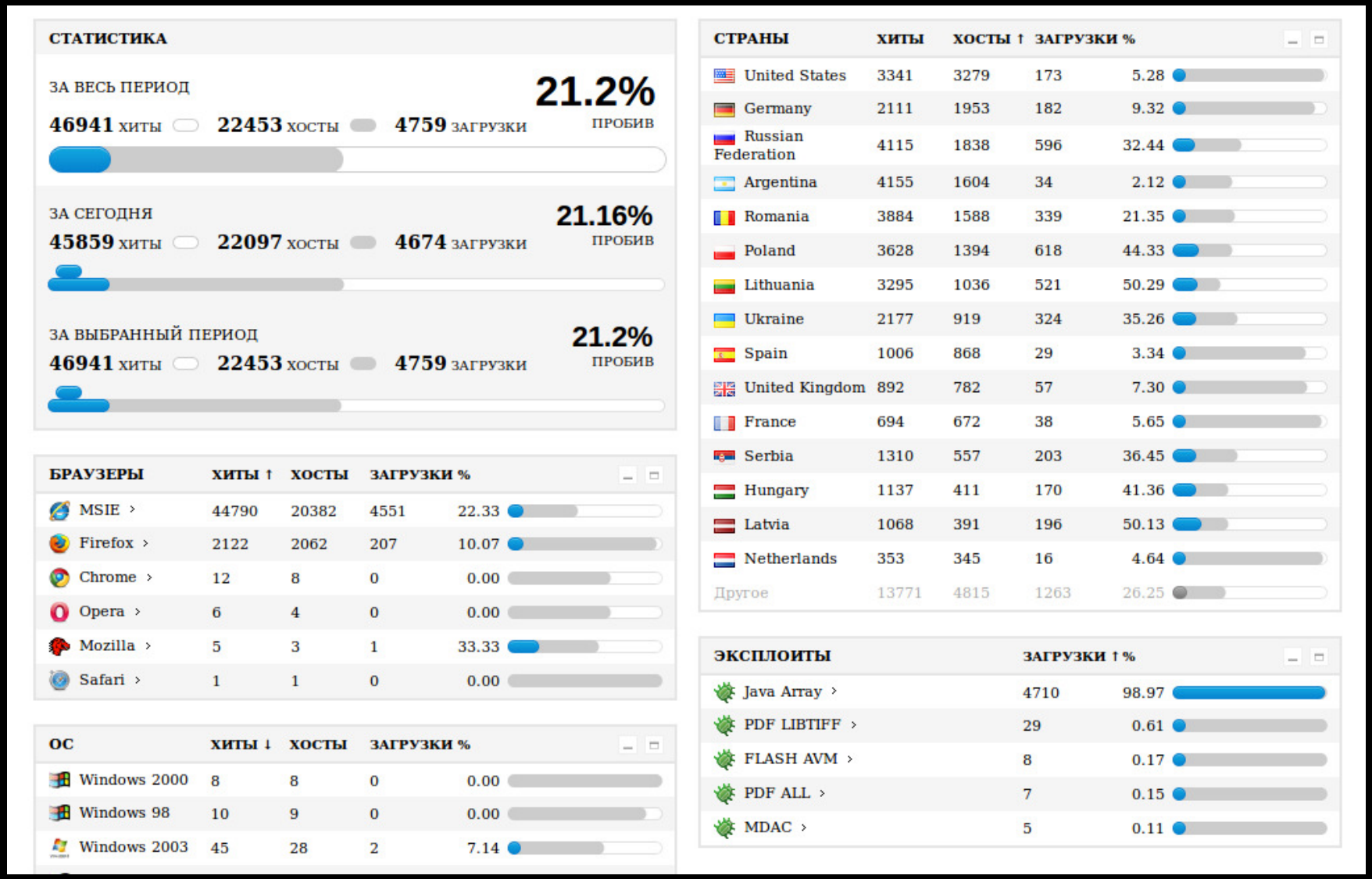
Fake Antivirus Software

In 2011, Fake Antivirus trojans for the Mac appeared:



* From McAfee Quarterly Threat Report Q2 2011

BlackHole Exploit kit Console



СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД
46941 ХИТЫ **22453** ХОСТЫ **4759** ЗАГРУЗКИ
21.2% ПРОБИВ

ЗА СЕГОДНЯ
45859 ХИТЫ **22097** ХОСТЫ **4674** ЗАГРУЗКИ
21.16% ПРОБИВ

ЗА ВЫБРАННЫЙ ПЕРИОД
46941 ХИТЫ **22453** ХОСТЫ **4759** ЗАГРУЗКИ
21.2% ПРОБИВ

БРАУЗЕРЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
MSIE ›	44790	20382	4551	22.33
Firefox ›	2122	2062	207	10.07
Chrome ›	12	8	0	0.00
Opera ›	6	4	0	0.00
Mozilla ›	5	3	1	33.33
Safari ›	1	1	0	0.00

ОС	ХИТЫ ↓	ХОСТЫ	ЗАГРУЗКИ	%
Windows 2000	8	8	0	0.00
Windows 98	10	9	0	0.00
Windows 2003	45	28	2	7.14

СТРАНЫ	ХИТЫ	ХОСТЫ ↑	ЗАГРУЗКИ	%
United States	3341	3279	173	5.28
Germany	2111	1953	182	9.32
Russian Federation	4115	1838	596	32.44
Argentina	4155	1604	34	2.12
Romania	3884	1588	339	21.35
Poland	3628	1394	618	44.33
Lithuania	3295	1036	521	50.29
Ukraine	2177	919	324	35.26
Spain	1006	868	29	3.34
United Kingdom	892	782	57	7.30
France	694	672	38	5.65
Serbia	1310	557	203	36.45
Hungary	1137	411	170	41.36
Latvia	1068	391	196	50.13
Netherlands	353	345	16	4.64
Другое	13771	4815	1263	26.25

ЭКСПЛОИТЫ	ЗАГРУЗКИ ↑	%
Java Array ›	4710	98.97
PDF LIBTIFF ›	29	0.61
FLASH AVM ›	8	0.17
PDF ALL ›	7	0.15
MDAC ›	5	0.11

Blackhole Exploit Kit

Over 85 percent of the infected servers which are using exploit kits are serving exploits by BlackHole. Recently, a new 0-day vulnerability in Java (CVE-2012-4681) was discovered in the wild. It didn't take more than a day for the BlackHole malware author to add this exploit to the BlackHole arsenal.

BlackHole exploit toolkit: after the integration of the newest exploit, the Java exploits achieved a success rate of between 75 and 99 per cent.

Overall, BlackHole managed to infect every fourth computer – the usual success rate was one in ten.

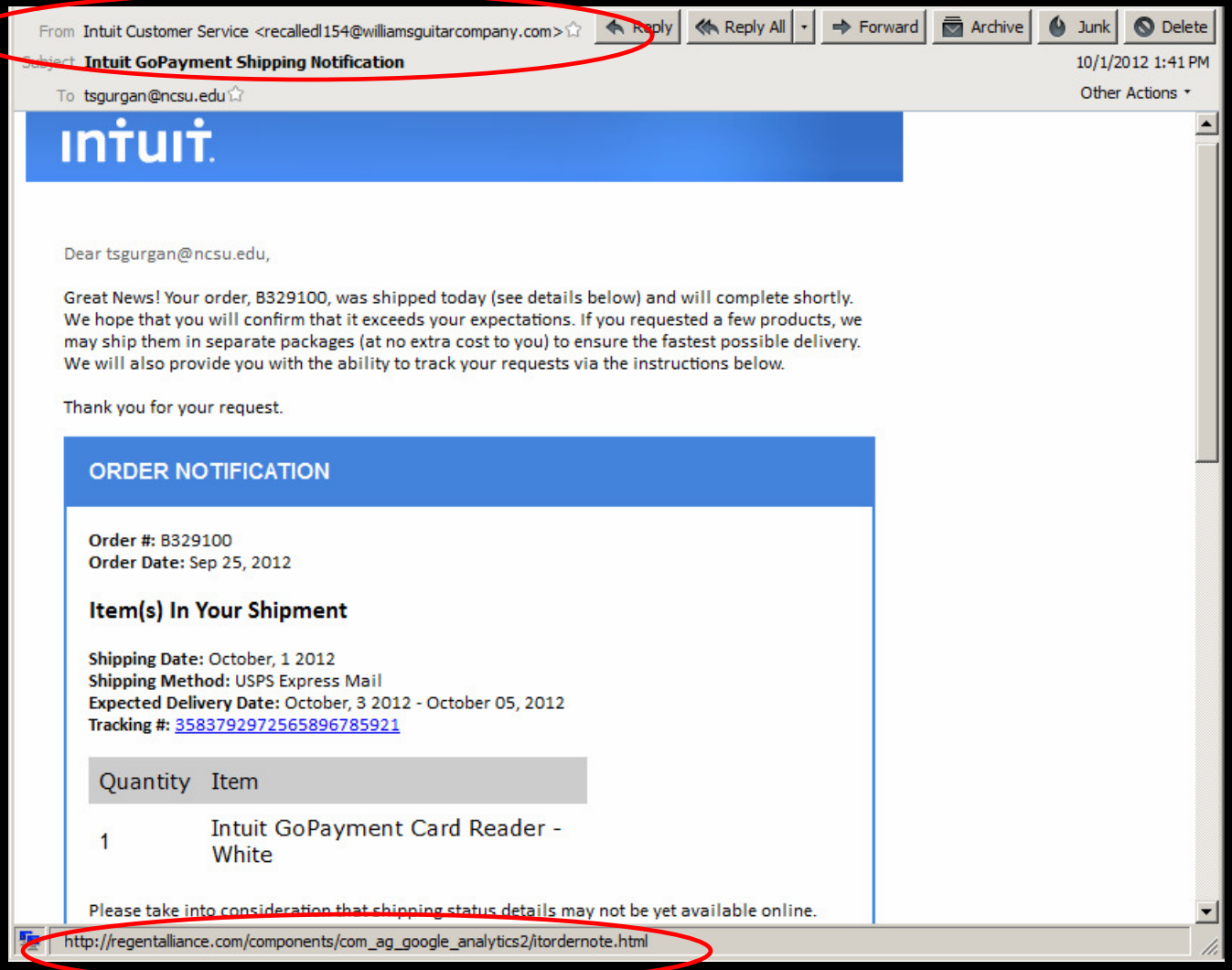
Usually, a good exploit kit, like BlackHole, has a success rate of around 10 percent for infecting machines visiting the servers. In the new version of BlackHole infection servers, we have seen up to a 25 percent success rate!

Furthermore, statistics show that Java exploits in BlackHole servers are 75 to 99 percent successful

Used in Intuit Order malicious email attack Monday, Oct. 1st, 2012:

http://blog.dynamoo.com/2012/10/intuit-shipment-spam-art-londonnet.html

Malware in Your Inbox



Links in the messages lead to websites hosting the Blackhole Exploit Kit which attempts to install a Zeus variant onto victims' systems.

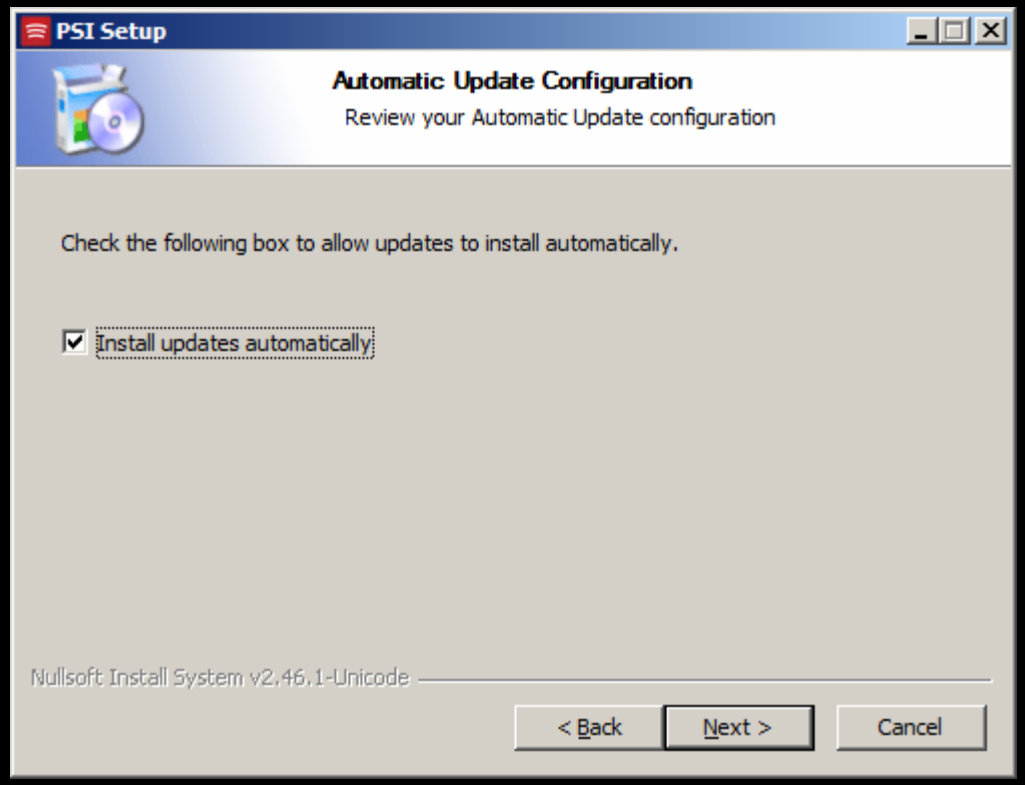
The observant user would notice that none of the links lead back to intuit.com

Vulnerability Analysis

- Most Exploited Applications on Campus:
  - Java runtime environment
  - Adobe Reader
  - Flash Player
    - flash for Devices is going away
  - Internet Explorer
  - Media Player
  - A survey found that only 2 percent of Windows systems had no out-of-date programs
- Utilities to Reduce Risk
  - Secunia PSI 3.0
    - http://secunia.com/products/consumer/psi/
  - BrowserCheck and Plugin-Check
    - http://browsercheck.qualys.com

Patching Vulnerable Applications

- Secunia PSI 3.0
  - http://secunia.com/products/consumer/psi/



Patching Vulnerable Applications

- Secunia PSI 3.0
  - http://secunia.com/products/consumer/psi/

Patching Vulnerable Applications

- Secunia PSI 3.0
  - http://secunia.com/products/consumer/psi/

Patching Vulnerable Applications

Qualys BrowserCheck

http://browsercheck.qualys.com

Checks common players, viewers, OS patches

Plugin-Check

https://www.mozilla.org/en-US/plugincheck/

Checks common players and viewers

Reducing Risks from Cyber Attacks

Running Antivirus Alone is not a Winning Strategy:

- Only 38% of Zeus malware is detected by antivirus software
- A recent study by University of Alabama at Birmingham found that antivirus detection rates averaged around 25% for malware arriving in email.
- European Network and Information Security Agency recently had this *frank* response after the “High Roller” financial theft of millions of Euros from online bank accounts: “Banks should consider all PCs infected and take steps to protect customers from fraudulent transactions.”

Why Antivirus Alone is not a Winning Strategy:

DATE	SPOOFED BRAND	ATTACK TYPE	INITIAL VT DETECTION RATE	LATEST VT RATE
6/20/2012	Verizon Wireless	BlackHole Exploit Kit > Generic Bad thing	3 out of 42	4 out of 40
6/20/2012	UPS + DHL	Zipped .EXE > Generic Bad Thing	4 out of 42	6 out of 42
6/19/2012	USPS	Zipped .EXE > SpyEye/Cridex/Bredolab	5 out of 42	10 out of 42
6/18/2012	Verizon Wireless	BlackHole Exploit Kit > Ransom/Birele/ZeuS	0 out of 42	20 out of 42
6/15/2012	Verizon Wireless	BlackHole Exploit Kit > ZeuS/Cridex	4 out of 42	28 out of 42
6/15/2012	Habbo.com	BlackHole Exploit Kit > ZeuS/Cridex	20 out of 35	29 out of 42
6/14/2012	Tax Payment Failed/IRS	BlackHole Exploit Kit > Zeus	4 out of 35	29 out of 42
6/14/2012	DHL	Zipped .EXE > Andromeda	27 out of 42	35 out of 42
6/12/2012	Twitter.com	BlackHole Exploit Kit > ZeuS	14 out of 42	29 out of 42
6/12/2012	LinkedIn.com	BlackHole Exploit Kit > ZeuS	12 out of 42	29 out of 42
6/12/2012	Amazon.com	BlackHole Exploit Kit > Cridex/Carberp/Dapato	5 out of 42	24 out of 41
6/11/2012	Paypal.com/eBay.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	5 out of 42	24 out of 41
6/11/2012	Amazon.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	4 out of 42	
6/11/2012	Myspace.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	4 out of 42	27 out of 41
6/8/2012	Xanga.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	5 out of 38	30 out of 42
6/6/2012	Craigslist.com	BlackHole Exploit Kit > Cridex/ZeuS	5 out of 42	32 out of 42
6/6/2012	American Express	BlackHole Exploit Kit > ZeuS	10 out of 42	30 out of 42
6/6/2012	DHL	Zipped .EXE > ZeuS/Andromeda	25 out of 42	38 out of 42
6/5/2012	DHL	Zipped .EXE > Andromeda	25 out of 41	32 out of 40
6/5/2012	Hewlett-Packard	LINK or HTML > Javascript > ZeuS	16 out of 42	27 out of 41
6/4/2012	Paypal.com/eBay.com	Exploit Kit > ZeuS/Cridex	0 out of 42	31 out of 42
6/4/2012	Hewlett-Packard	HTM attachment >	3 out of 42	27 out of 42
6/1/2012	Bank of America	BlackHole Exploit Kit > ZeuS	13 out of 41	28 out of 42
5/31/2012	Windstream	BlackHole Exploit Kit > ZeuS	14 out of 42	27 out of 42
5/30/2012	Citi Credit Card	BlackHole Exploit Kit > ZeuS	8 out of 42	N/A
5/30/2012	Citibank.com	BlackHole Exploit Kit > ZeuS	8 out of 42	25 out of 42
5/29/2012	Bancorp	BlackHole Exploit Kit > ZeuS	15 out of 42	N/A
5/29/2012	Facebook	Zipped .EXE > ZeuS/Andromeda	14 out of 42	36 out of 41
5/28/2012	Facebook	Zipped .EXE > ZeuS/Andromeda	9 out of 42	36 out of 42
5/23/2012	PayPal.com	BlackHole Exploit Kit > ?	N/A	N/A
5/23/2012	DHL	Zipped .EXE > Andromeda	13 out of 42	37 out of 42
5/22/2012	Better Business Bureau	Zipped .EXE > Andromeda	4 out of 42	36 out of 42
5/21/2012	Better Business Bureau	Zipped .EXE > ZeuS/Andromeda	16 out of 41	37 out of 42

Microsoft EMET: A Windows Hardening Tool

- Modifies the way Windows runs so as to break common exploits such as those used by Blackhole Exploit kit including:
  - Buffer overflow exploits
  - Heap overflow exploits
  - SEH (structure exception handler) exploits
  - ROP (return oriented programming) exploits
  - DLL injection exploits
- "Microsoft's Enhanced Mitigation Experience Toolkit" (EMET) protects against many 0-day exploits and halts execution of common exploits even when applications are not patched.
- Hardening effect is greatest for Windows XP, but EMET adds protection to Windows 7 where applications are not patched
- Version 3.5 now notifies users when a process has been stopped (crashed) because a protective mechanism was activated by the hardening tool
- Administrators can now deploy the tool across a network using Group policies or the System Center Configuration Manager (SCCM).
- EMET 3.0 can import and export 'Protection Profiles' with customized settings or common Microsoft and third-party applications, and three default configuration profiles are included. The company says that EMET has also been tested under the Windows 8 Consumer Preview."
- Download link: http://www.microsoft.com/en-us/download/details.aspx?id=30424

Other ways to Harden Your Computer

Use AutoUpdate features of Java, Flash Player and Adobe Reader

Use a browser plugin to block Ads and scripts like NoScript ,
Updated Adblocker or AdBlock Plus

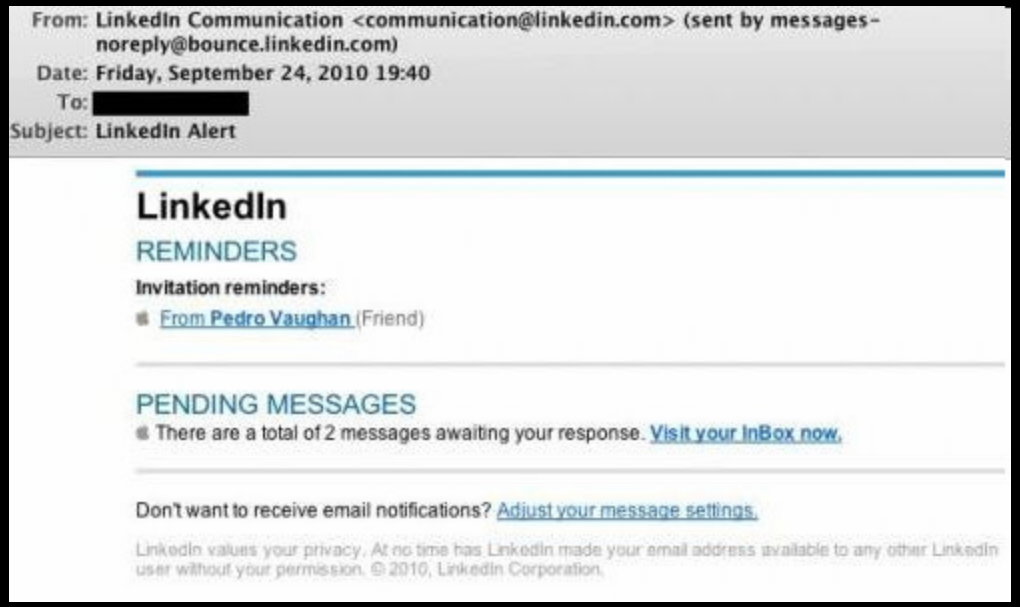
Exploit Shield browser addition:

http://download.cnet.com/ExploitShield-Browser-Edition/3000-18510_4-75780388.html

Blocks exploits similar to EMET when launched from Web Browsers

Viruses & Trojans on Social Networks

Fake LinkedIn Invite Leads to ZeuS Trojan


From: LinkedIn Communication <communication@linkedin.com> (sent by messages-noreply@bounce.linkedin.com)
Date: Friday, September 24, 2010 19:40
To: [redacted]
Subject: LinkedIn Alert

LinkedIn

REMINDERS

Invitation reminders:

- From Pedro Vaughan (Friend)

PENDING MESSAGES

- There are a total of 2 messages awaiting your response. Visit your InBox now.

Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010, LinkedIn Corporation.

Links in the messages lead to websites hosting the SEO Exploit Pack which attempts to drop a Zeus variant onto victims' systems.

The observant user would notice that none of the links lead back to linkedin.com

Botnets Are Collecting Data On You and Your PCs

Three or more years ago, botnet operators focused on stealing email and password credentials, which were useful to spammers.

Now botnet controllers are building massive profiles on their users, including:

- Name
- Address
- Age
- Sex
- Financial worth
- Relationships
- Where they visit online – this information comes from history and cookies

They sell this information, where it ultimately finds its way into legitimate lead generation channels

Sites will buy the information stolen via botnets in bulk. In some cases, a company might pay $20 -$30 for a qualified lead.

Alternatively, Botnets can be used to sign up individuals for all kinds of pay for registration schemes since they have all the data needed.

Why are You a target?

- University students and staff computers or poorly maintained
- We tend to have many computers per person, not manage patching them
- We have excess bandwidth, email accounts and storage
- We have few security personnel or security tools.
  Not nearly enough to watch everything
- Our network has a good reputation – something worth stealing
- We have intellectual property and research data that is worth stealing

Common Scams sent via e-mail to @ncsu.edu users

The Rise in Social Engineering attacks:

While not technically sophisticated, hackers have studied what emails you normally open and created malicious fakes to spread viruses and steal passwords.

Viruses sent to Campus email users included:

- Fake UPS, Fedex, DHL shipment notices in malicious PDFs
- Fake I.R.S. Notices (tax payment due or denied)
- Fake Denied Electronic Fund transfers (ACH)
- Fake Credit Card notices (card blocked, charge denied)
- Fake NYC traffic/parking tickets (speeding or illegal parking)
- Infected Office Documents and PDFs sent as *"Scans"* from Hewlett-Packard Officejet
- Fake trojan security updates from your bank in .zip file
  Trojan application update programs
  Security Certificate Trojans
- Fake Facebook messages waiting notices that were really led to Facebook viruses

https://s3.amazonaws.com/knowbe4.cdn/SocialEngineeringRedFlags.pdf

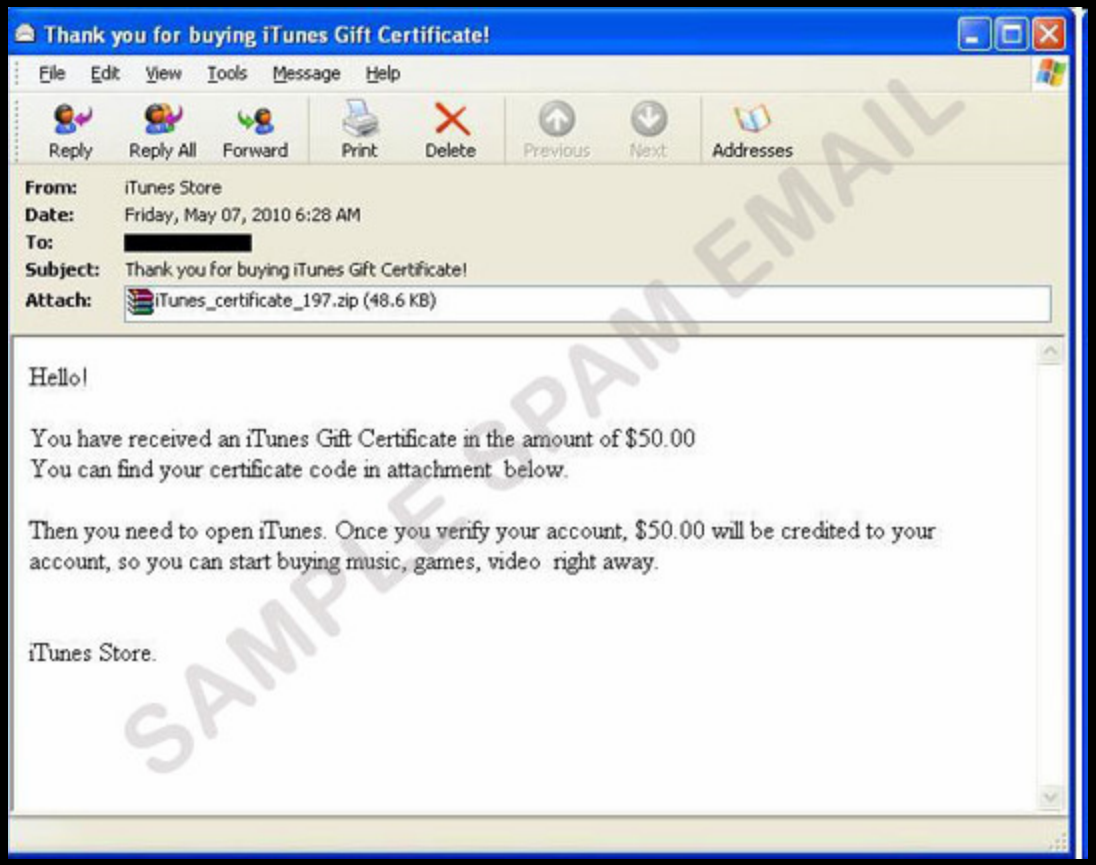
Avoiding Phishing Attacks

Phishers and the lies they tell:

- Your email is over quota
- We are Upgrading the email system and need your password
- You have sent too much spam
- There is a virus in the email system
- You need to upgrade your antivirus software
- We have too many accounts and are removing inactive ones
- You can get more email storage if you send your password in
- We're sorry, but we made a mistake and now we need your password to finish our email upgrade
- Someone logged in from a suspicious IP, we think your account is hacked, send us your password to show it is OK.

Phishing attack summary

Malware in your Inbox



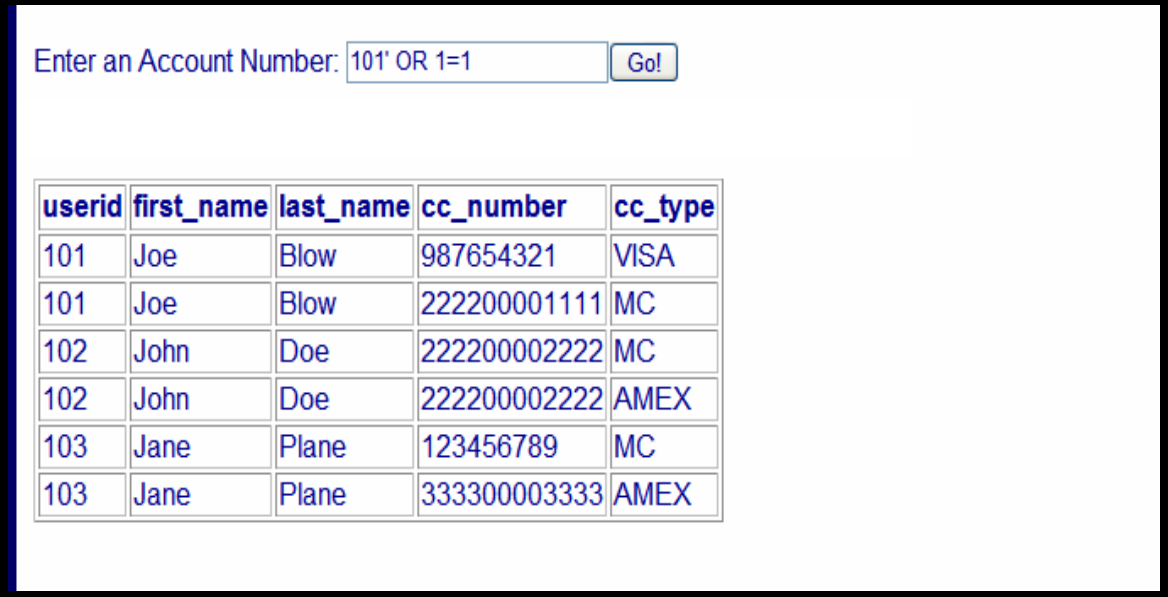
A spam sending botnet was used to send thousands of messages like this to users on campus.

The attachment is actually the SASFIS trojan for Windows

Reducing Risks from Cyber Attacks

In 2012, Millions of accounts on popular and not-so-popular websites have been compromised and posted to the internet using SQL Injection

What happens if you enter ‘OR 1=1 as the username or account number?



userid	first_name	last_name	cc_number	cc_type
101	Joe	Blow	987654321	VISA
101	Joe	Blow	222200001111	MC
102	John	Doe	222200002222	MC
102	John	Doe	222200002222	AMEX
103	Jane	Plane	123456789	MC
103	Jane	Plane	333300003333	AMEX

Reducing Risks from Cyber Attacks

Enter ‘ OR 1=1 into username

All usernames and passwords get displayed

See if your accounts are some of the ones compromised:

https://shouldichangemypassword.com/

Tracking over 13,000,000 email addresses of compromised accounts in 2012

Try: margot.noel5@hotmail.fr

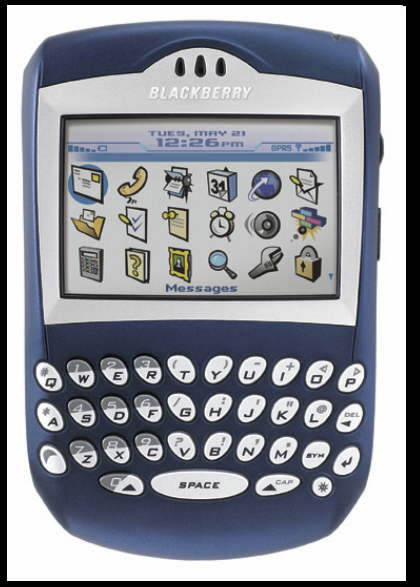
https://passfault.appspot.com/password_strength.html#menu

Securing Your Mobile Device

Blackberry Security Tips

To Encrypt your Blackberry:

- *Enable* password from Options | Security Options | General Settings
- *Enable* content protection to encrypt the data (email, memos, tasks, addresses, notes, calendar and cache) on the device
- When password is enabled, the Blackberry will erase the data on it if the wrong password is entered 10 times
- These settings can be made mandatory via Security Policy from the Blackberry Enterprise Server
- Blackberry App Password Keeper can encrypt your password lists



iPhone Security Tips

iPhone 3GS and greater – encryption on device

- iTunes backup encrypted with your password
- iPhone 4 encrypted on device and iTunes

Set passcode to lock device from Settings | General menu

- Set device to auto-lock when not in use
- iPhone passcode can be 4 digit PIN number
  OR passphrase entered with onscreen keyboard
- After you set a PIN or passcode, data encryption is enabled

To secure the data on your iPhone:

- Use a free App like KeePass to:
  - Encrypt notes files
  - Store an encrypted password lists
  - Enter passwords and import/export passwords
- Use an App like Lockbox or 1Password
  - Encrypt passwords, credit cards, and .CSV files
  - Notes interface in 1Password is much better
- Use free Qualys browser check to see if your device needs an update:
  - http://browsercheck.qualys.com

Android Security Tips

Android memory is not encrypted, but you can:

To secure the data on your Android:

- Use an App like LastPass or free KeePassDroid to:
  - Store encrypted passwords
- Use an App protector like Android Protector
  - Require a PIN code to launch an App such as Gmail, Market or Calendar
- Use an App like B-Folders to:
  - Store encrypted files of any kind using AES-256 bit encryption
- The Noscript plugin to Firefox is now available for Android:
  - This plug-in blocks javascript except where specifically allowed

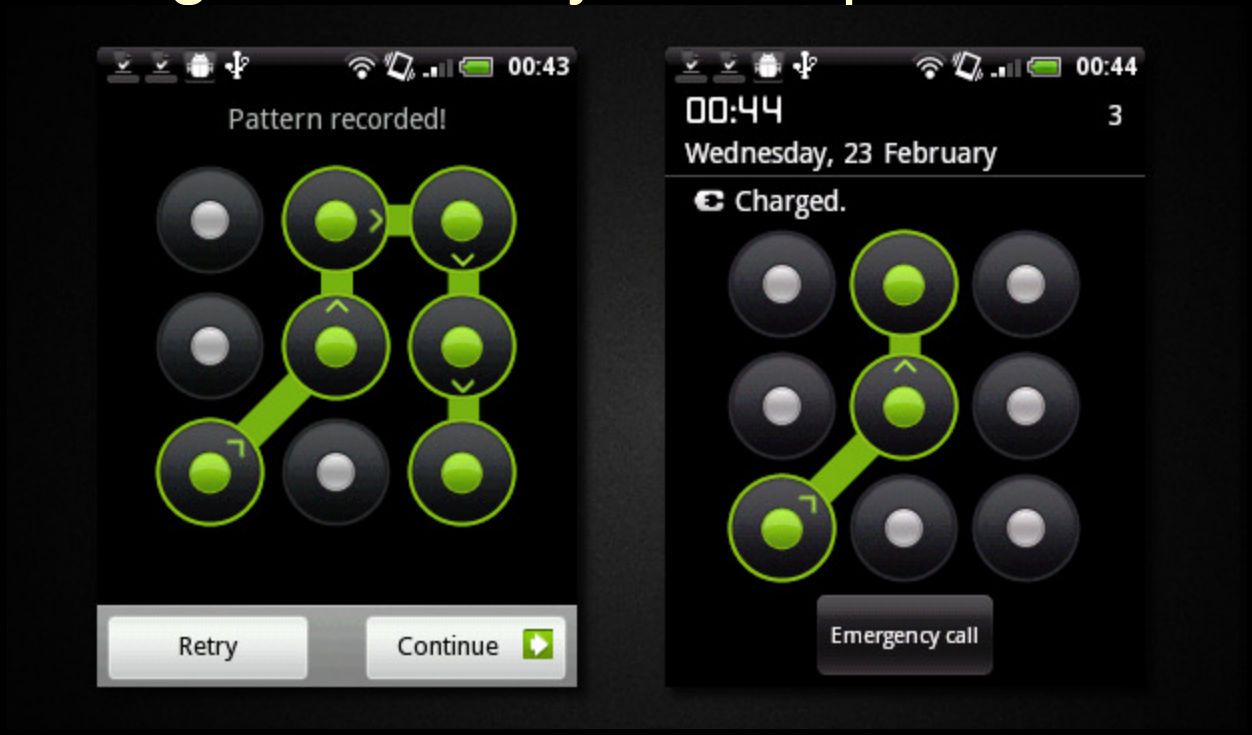
Securing Your Mobile Device

Use a screenlock

Android password can be a PIN code or gesture

To set the screen lock:

Settings > Security > Setup screen lock



If you select pattern,

A 3x3 grid pattern is displayed for creating your gesture Pattern

Due to design, *shoulder surfing passwords is a greater concern with mobile computers*

Avoiding Computer Theft

Device Tracking Software

- 5% of enterprise mobile devices are lost
- If you lose your mobile you were using for online banking, report it to your bank
- If your laptop or mobile phone is stolen, having tracking software installed makes it possible to find it.
- Install a tiny agent in your PC or phone, which silently waits for a remote signal to wake up and contact you with the devices location.
- This signal is sent from the Internet or via Text message and allows you to gather information regarding the device's location, hardware and network status, what is on the screen and a picture of the room in front of the device.
- If you give this information to the Police, they can find your missing mobile device.

Avoiding Computer Theft

Device Tracking Software

- If your laptop or mobile phone is stolen, have tracking software installed makes it possible to find it.

- Download from http://preyproject.com

Available for Windows 2000/XP/Vista/7 (32 and 64 bit available)
OS X and Linux
Android, iOS too.

For Android:

- Choose Control Panel Mode
- Create an account by entering an email address and password.
- Activate the client using link in email and an SMS text message

For Laptops:

- Choose Stand Alone Mode
- Enter your website information
- Enter your email address and SMTP server address

Avoiding Computer Theft

Prey Device Tracking Software

In Stand Alone mode, you have complete control of how software works

In Control Panel mode, you use the preyproject website to control the program

In Stand Alone mode, the program checks every 10-20 minutes for a web page on your website

If your laptop or device is stolen, erase the page from your website and Prey will start sending reports when it is online.

Avoiding Computer Theft

Device Tracking Software

The Prey report emailed to your account will show the approximate location of your laptop:

lat=35.7885825 :: lng=-78.6708385 :: accuracy=52.0

Public network IP and gateway IP:

public ip=75.200.169.17 :: internal ip=75.200.169.17 :: gateway ip=75.200.169.17 ::
mac address=00-50-56-C0-00-08

The current logged in username and uptime:

logged user=tsgurgan ::
uptime=\SECURITY-LAPTOP has been up for: 6 day(s), 6 hour(s), 52 minute(s), 10 second(s)

As well as a screen shot of the desktop and a photo from the webcam if possible.

Avoiding Computer Theft

Device Tracking Software

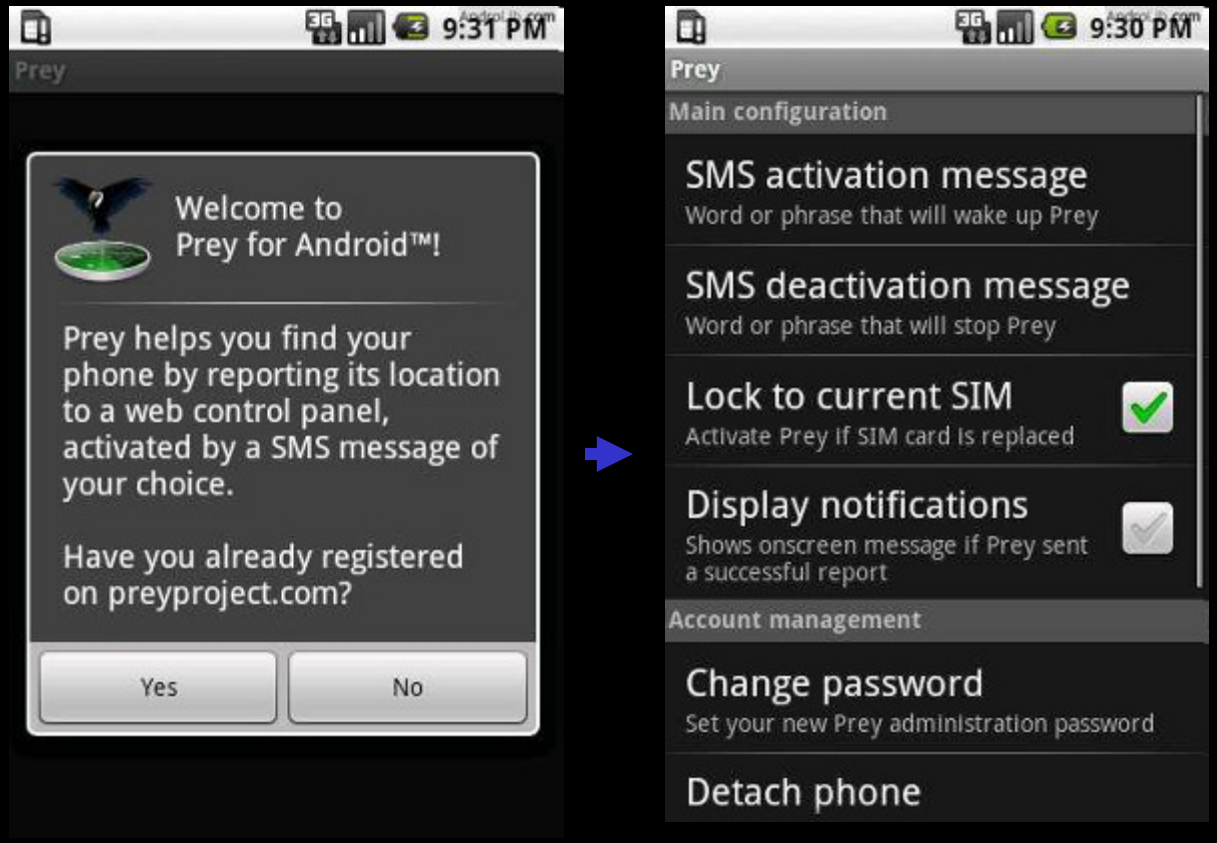
Prey Phone Tracker Android features:

- GPS + Wifi geo-location.
- SIM change detection.
- SMS or Cloud To Device activation (2.2+).
- Lock phone/tablet for privacy (2.2+).
- Uninstall protection (2.2+).
- Loud alarm sound.
- Alert messages to user.

Avoiding Computer Theft

Device Tracking Software

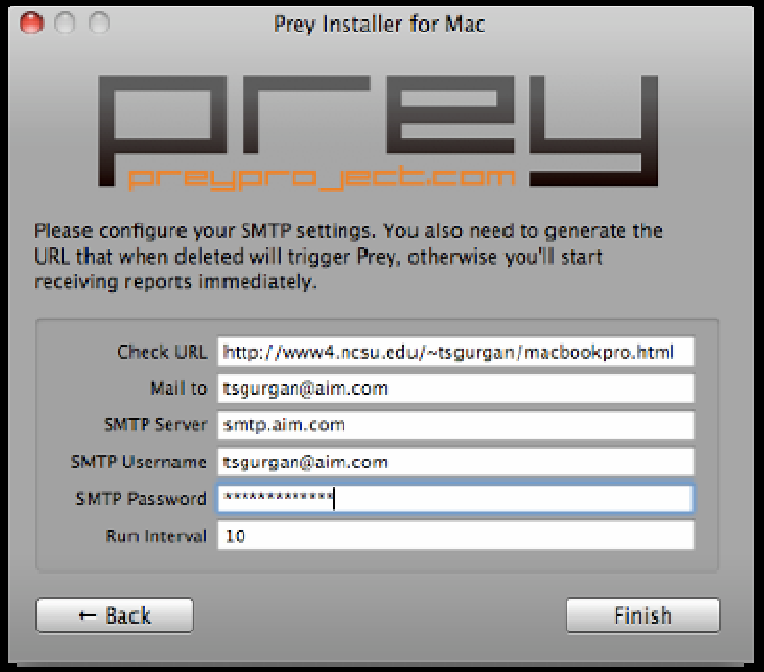
With the information in the report, Police can track down the street address of your device.



Avoiding Computer Theft

Laptop Tracking Software

Installing Prey on OS X:

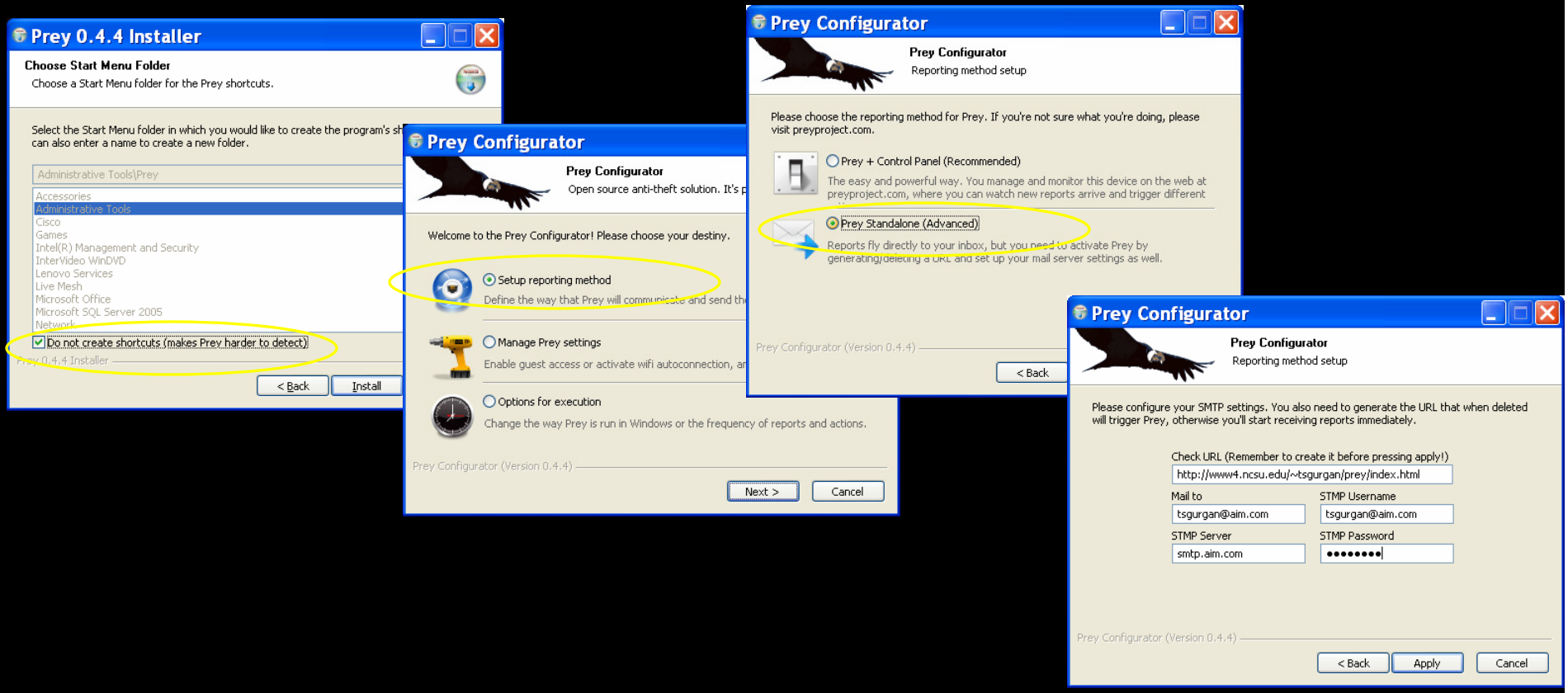


Mac Install

Avoiding Computer Theft

Laptop Tracking Software

Installing Prey on Windows:



Reducing Risks from Cyber Attacks

1) Patch your systems
   Desktops, laptops and mobiles OS
   Java
   Adobe Acrobat Reader
   Flash Player
   Other browsers, players and viewers

Reducing Risks from Cyber Attacks

2) Use OS hardening utilities

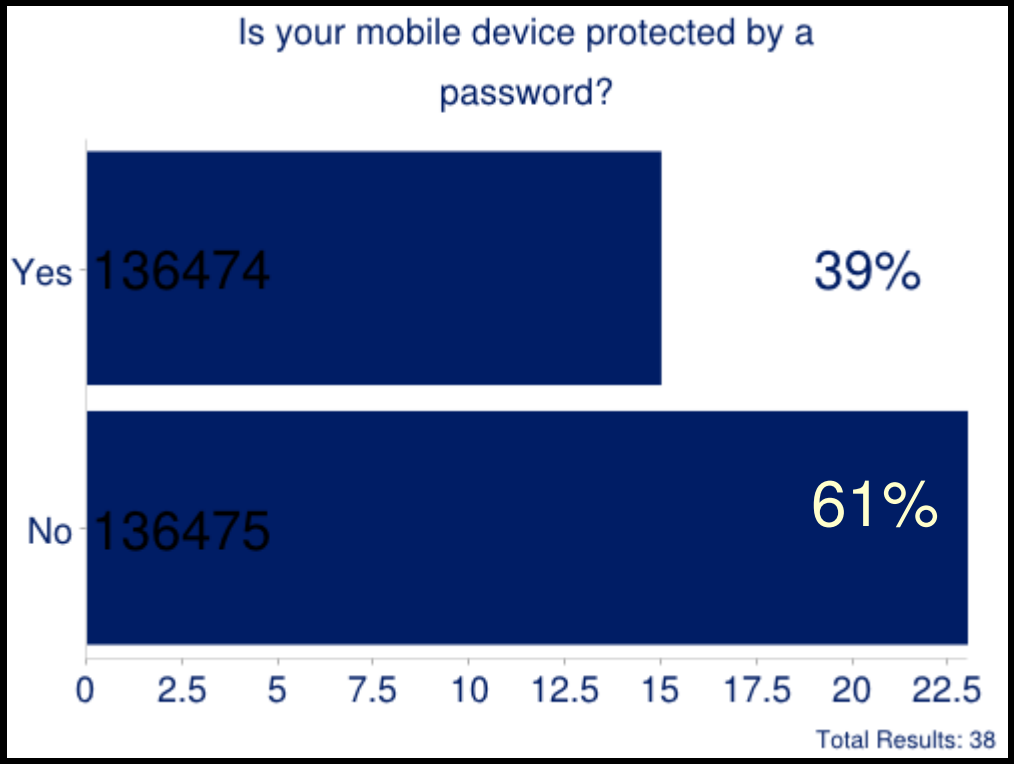
Microsoft EMET
ExploitShield Browser Edition utility
Auto Update browsers, players and viewers
NoScript or Add Blocker browser plug-in

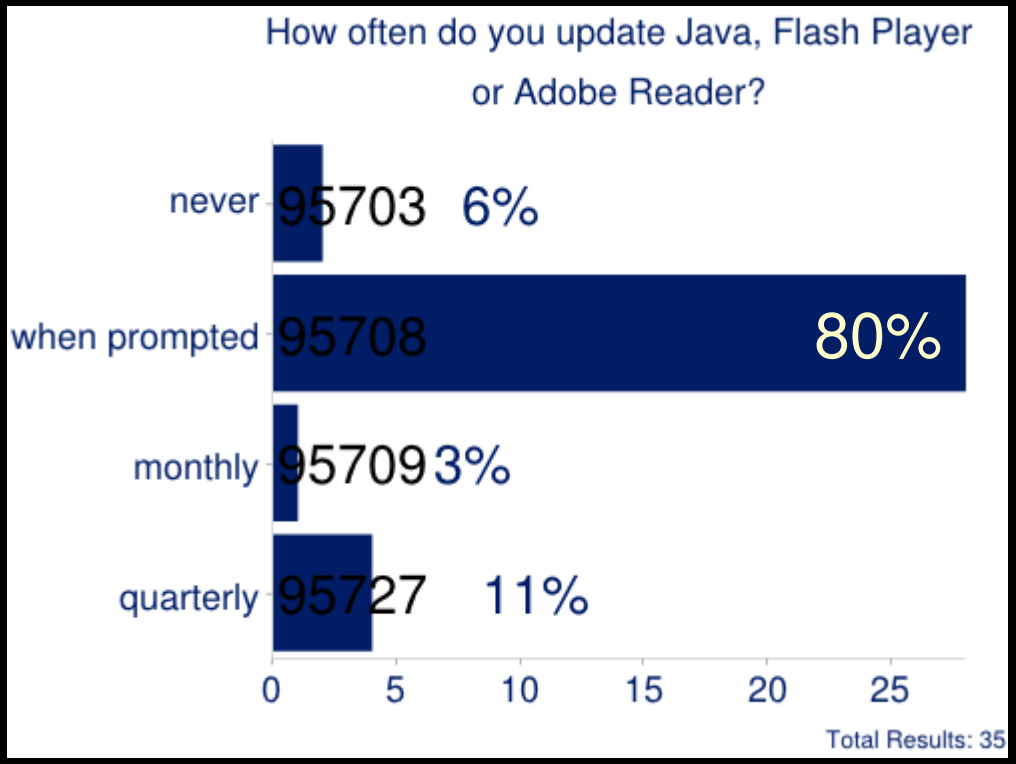
Reducing Risks from Cyber Attacks

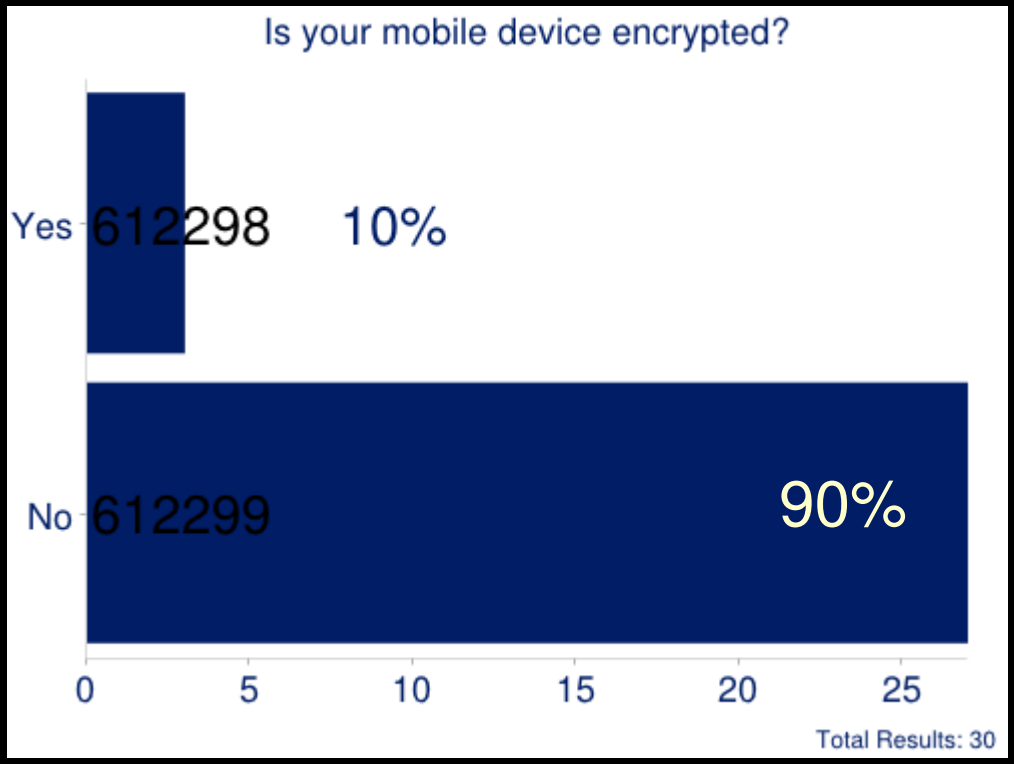
3) Know the social engineering Red Flags

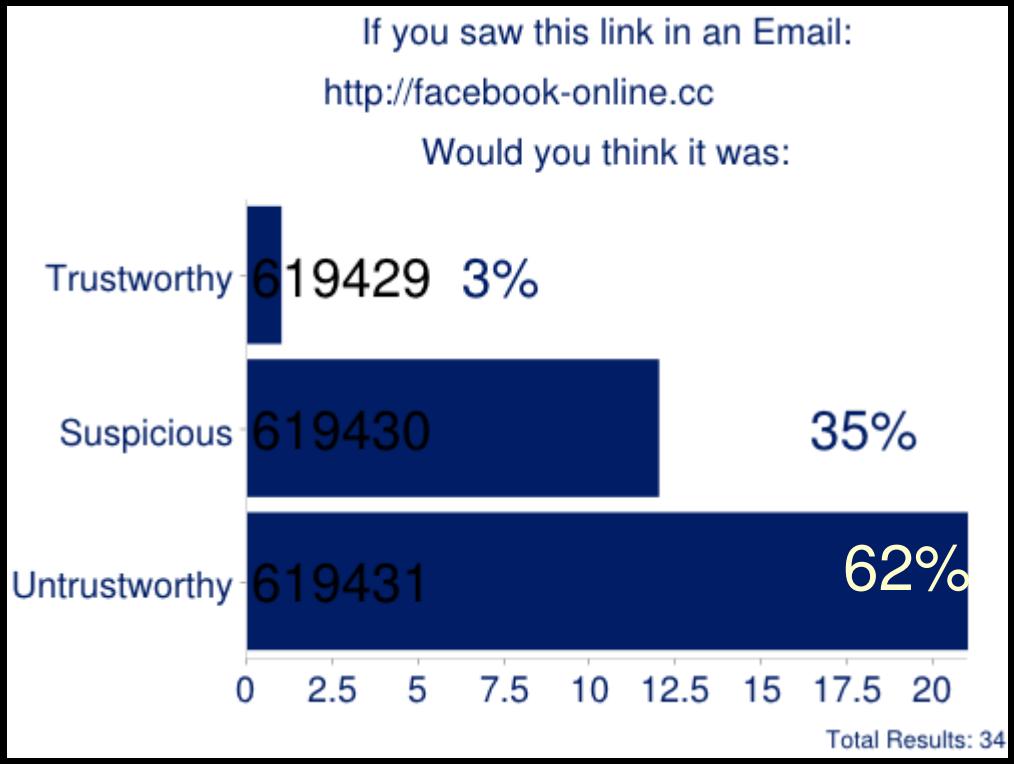
4) Secure your mobile device:
   - Use a screen lock password
   - Turn on encryption
   - Install antivirus program
   - Install and Configure device location/remote wipe software

5) Manage your accounts –
   - Avoid Phishing Attacks
   - Use Keepass or other password manager

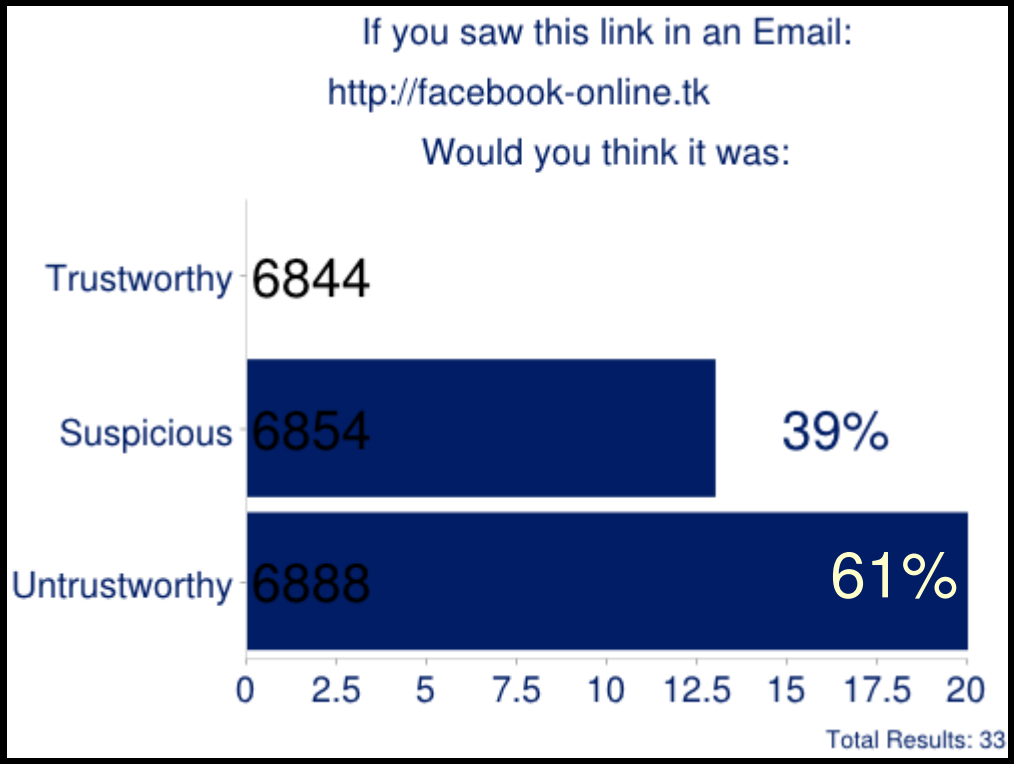

Is your mobile device protected by a password?
Yes
136474
39%
No
136475
61%
0
2.5
5
7.5
10
12.5
15
17.5
20
22.5
Total Results: 38


How often do you update Java, Flash Player or Adobe Reader?
never
95703
6%
when prompted
95708
80%
monthly
95709
3%
quarterly
95727
11%
0
5
10
15
20
25
Total Results: 35

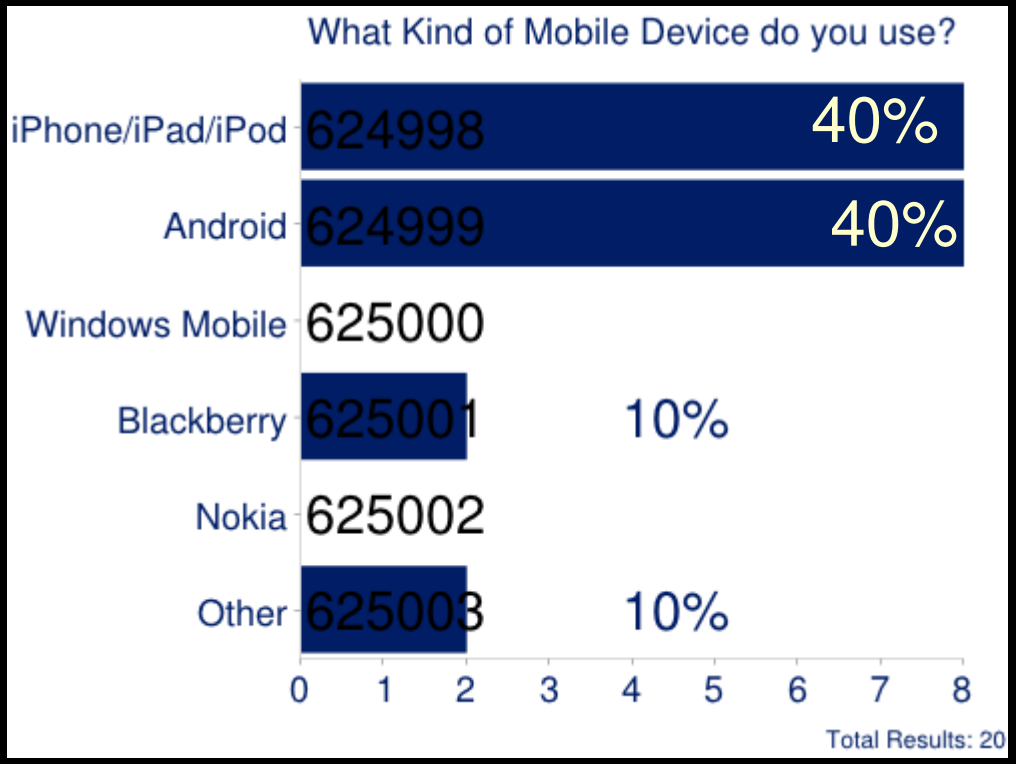

Is your mobile device encrypted?
Yes
612298
10%
No
612299
90%
0
5
10
15
20
25
Total Results: 30



The .cc domain has a poor reputation. Google made the decision in 2012 to remove all .cc and .co pages from search results.



The .tk domain has a poor reputation and is most commonly used for phishing attacks and malware websites.


What Kind of Mobile Device do you use?
iPhone/iPad/iPod
624998
40%
Android
624999
40%
Windows Mobile
625000
Blackberry
625001
10%
Nokia
625002
Other
625003
10%
0
1
2
3
4
5
6
7
8
Total Results: 20