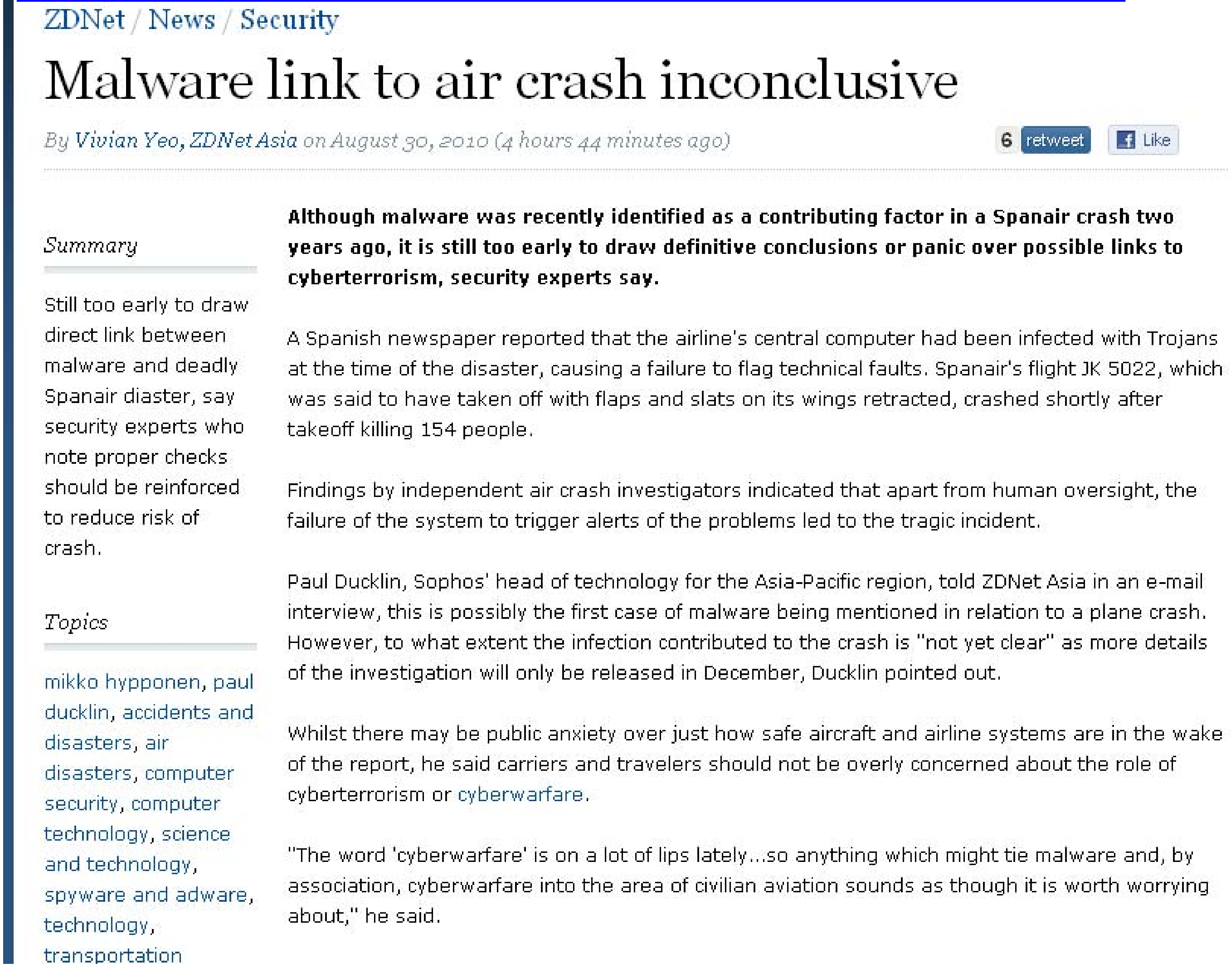
Introduction to Malicious Code (Malware)

EDA 263 – Computer Security

Original Slides: Erland Jonsson
Changes by Magnus Almgren

http://www.zdnetasia.com/malware-link-to-air-crash-inconclusive-62202513.htm



ZDNet / News / Security

Malware link to air crash inconclusive

By Vivian Yeo, ZDNet Asia on August 30, 2010 (4 hours 44 minutes ago)

Summary

Still too early to draw direct link between malware and deadly Spanair diaster, say security experts who note proper checks should be reinforced to reduce risk of crash.

Topics

mikko hypponen, paul ducklin, accidents and disasters, air disasters, computer security, computer technology, science and technology, spyware and adware, technology, transportation

Although malware was recently identified as a contributing factor in a Spanair crash two years ago, it is still too early to draw definitive conclusions or panic over possible links to cyberterrorism, security experts say.

A Spanish newspaper reported that the airline's central computer had been infected with Trojans at the time of the disaster, causing a failure to flag technical faults. Spanair's flight JK 5022, which was said to have taken off with flaps and slats on its wings retracted, crashed shortly after takeoff killing 154 people.

Findings by independent air crash investigators indicated that apart from human oversight, the failure of the system to trigger alerts of the problems led to the tragic incident.

Paul Ducklin, Sophos' head of technology for the Asia-Pacific region, told ZDNet Asia in an e-mail interview, this is possibly the first case of malware being mentioned in relation to a plane crash. However, to what extent the infection contributed to the crash is "not yet clear" as more details of the investigation will only be released in December, Ducklin pointed out.

Whilst there may be public anxiety over just how safe aircraft and airline systems are in the wake of the report, he said carriers and travelers should not be overly concerned about the role of cyberterrorism or cyberwarfare.

"The word 'cyberwarfare' is on a lot of lips lately...so anything which might tie malware and, by association, cyberwarfare into the area of civilian aviation sounds as though it is worth worrying about," he said.

Malicious code - some observations

Malicious code is any code ***added***, ***changed*** or ***removed*** from a software system in order to intentionally cause harm or subvert the intended function of the system.

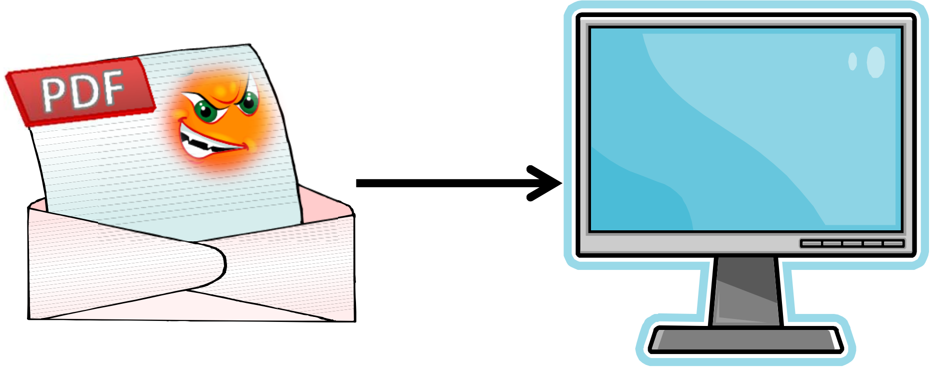
- "If you let somebody else execute code on your computer, then it is not your own computer"
  - User convinced of running a program, maybe done indirectly by just inserting a USB memory (CD/DVD) into computer,
  - User/system running a program (e.g. web browser) with a vulnerability that can be taken advantage of,
  - …
- Malicious code can be many things: viruses, worms, Trojan horses, rabbits, etc.
- Note that from a technical/scientific viewpoint:

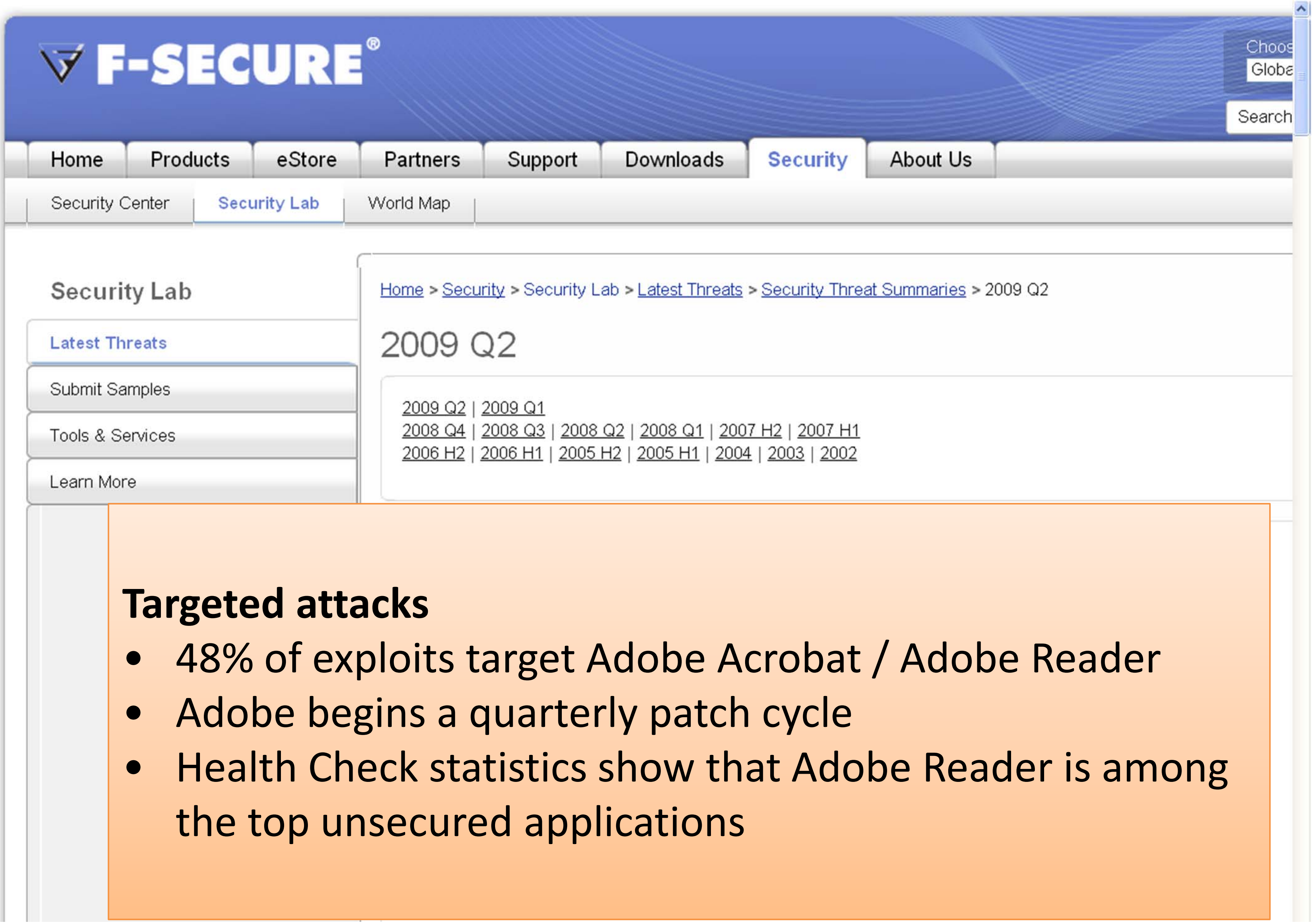
  malicious code is "normal" code!!
- Thus: the malware problem is a software problem.

Malicious Code (2)

- **Many users say:**

  I would never download unsecure content!
- But what type of content is safe?





Home > Security > Security Lab > Latest Threats > Security Threat Summaries > 2009 Q2

2009 Q2

2009 Q2 | 2009 Q1
2008 Q4 | 2008 Q3 | 2008 Q2 | 2008 Q1 | 2007 H2 | 2007 H1
2006 H2 | 2006 H1 | 2005 H2 | 2005 H1 | 2004 | 2003 | 2002

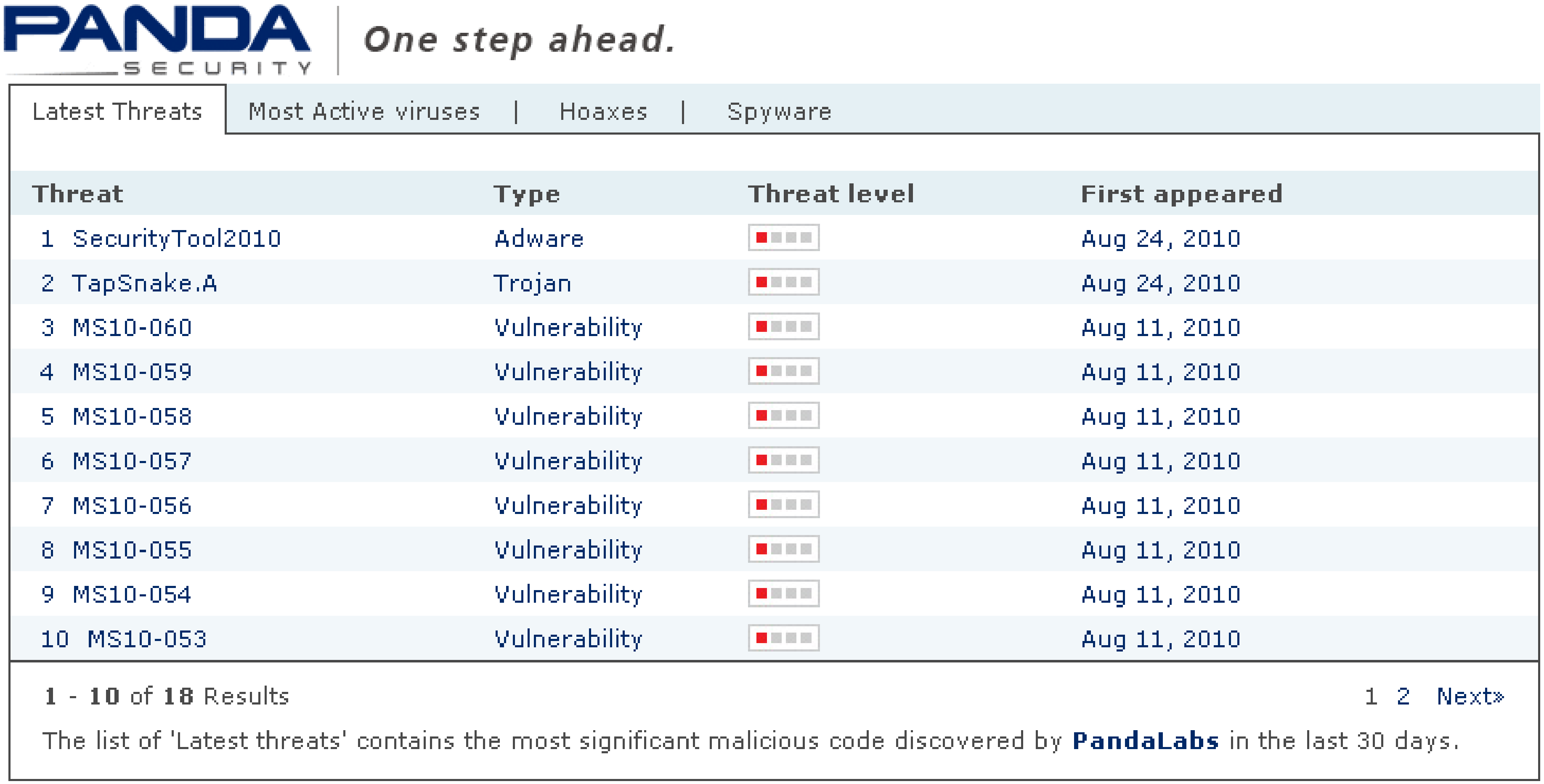
Targeted attacks

- 48% of exploits target Adobe Acrobat / Adobe Reader
- Adobe begins a quarterly patch cycle
- Health Check statistics show that Adobe Reader is among the top unsecured applications

Malicious code - some recent trends

- Previously malware was normally of one specific kind. Nowadays, it is “multifunctional” and complicated.
  - Malware is **targeting end users** through Web-based attacks *(Symantec Internet Security Report xiv)*
- Most viruses today are non-destructive. Rather, they try to take control over your computer to
  - **collect financial information** or
  - using it for malicious purposes, becoming a **zombie,** e.g. to **distribute spam.** (claim is that 70% of all email is spam)
- All kinds of malware tend to be called “virus”.
  - Bagle, Mydoom, Netsky, Sasser, Kargo and Sober (2004)
  - Conficker (2009)

Latest Threats



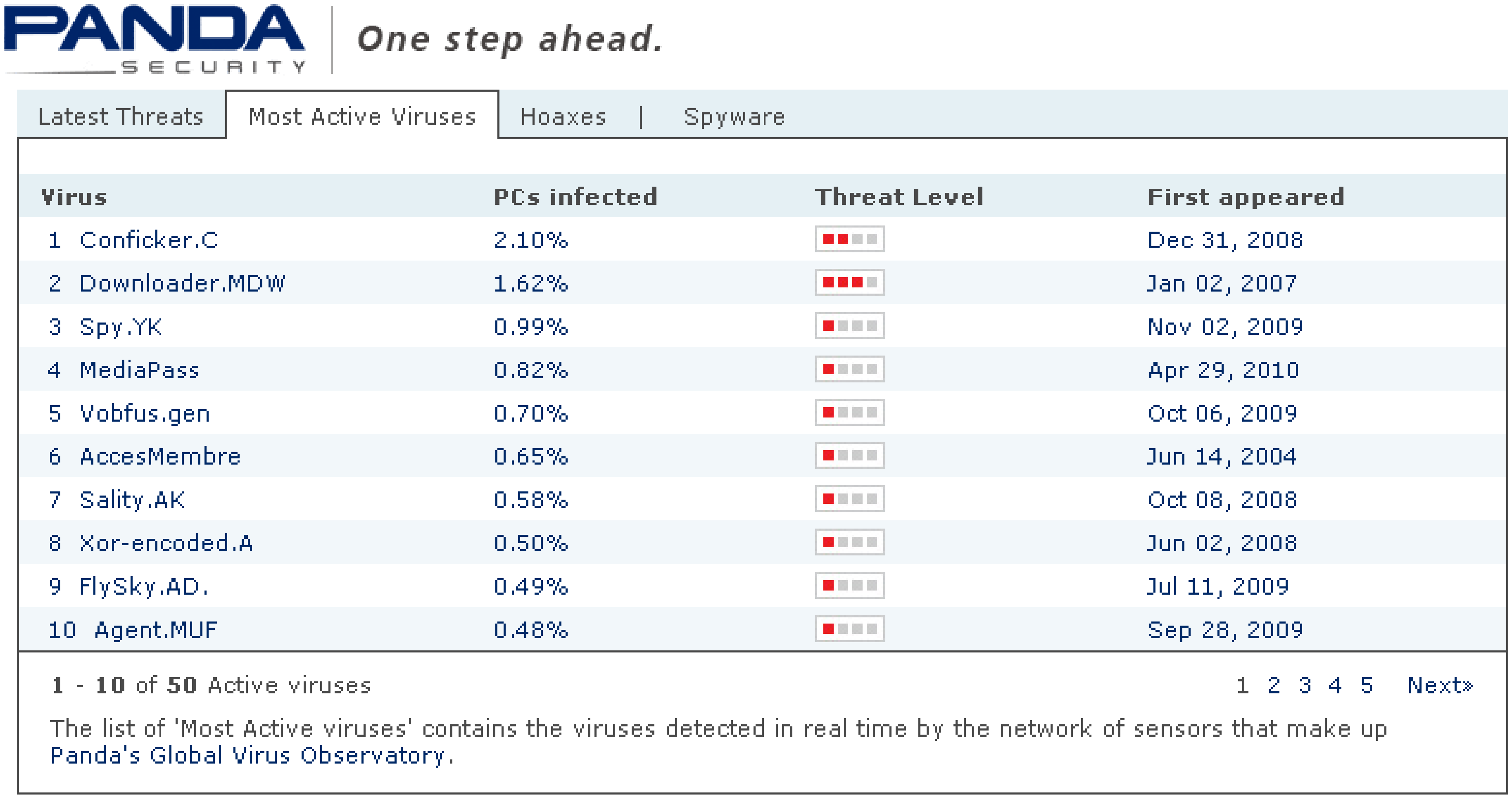
Threat	Type	Threat level	First appeared
1 SecurityTool2010	Adware	🟥⬜⬜⬜	Aug 24, 2010
2 TapSnake.A	Trojan	🟥⬜⬜⬜	Aug 24, 2010
3 MS10-060	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010
4 MS10-059	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010
5 MS10-058	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010
6 MS10-057	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010
7 MS10-056	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010
8 MS10-055	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010
9 MS10-054	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010
10 MS10-053	Vulnerability	🟥⬜⬜⬜	Aug 11, 2010

1 - **10** of **18** Results 1 2 Next»

The list of 'Latest threats' contains the most significant malicious code discovered by **PandaLabs** in the last 30 days.

http://www.pandasecurity.com/homeusers/security-info/default.aspx?lst=ul (100831)

Most Active Viruses

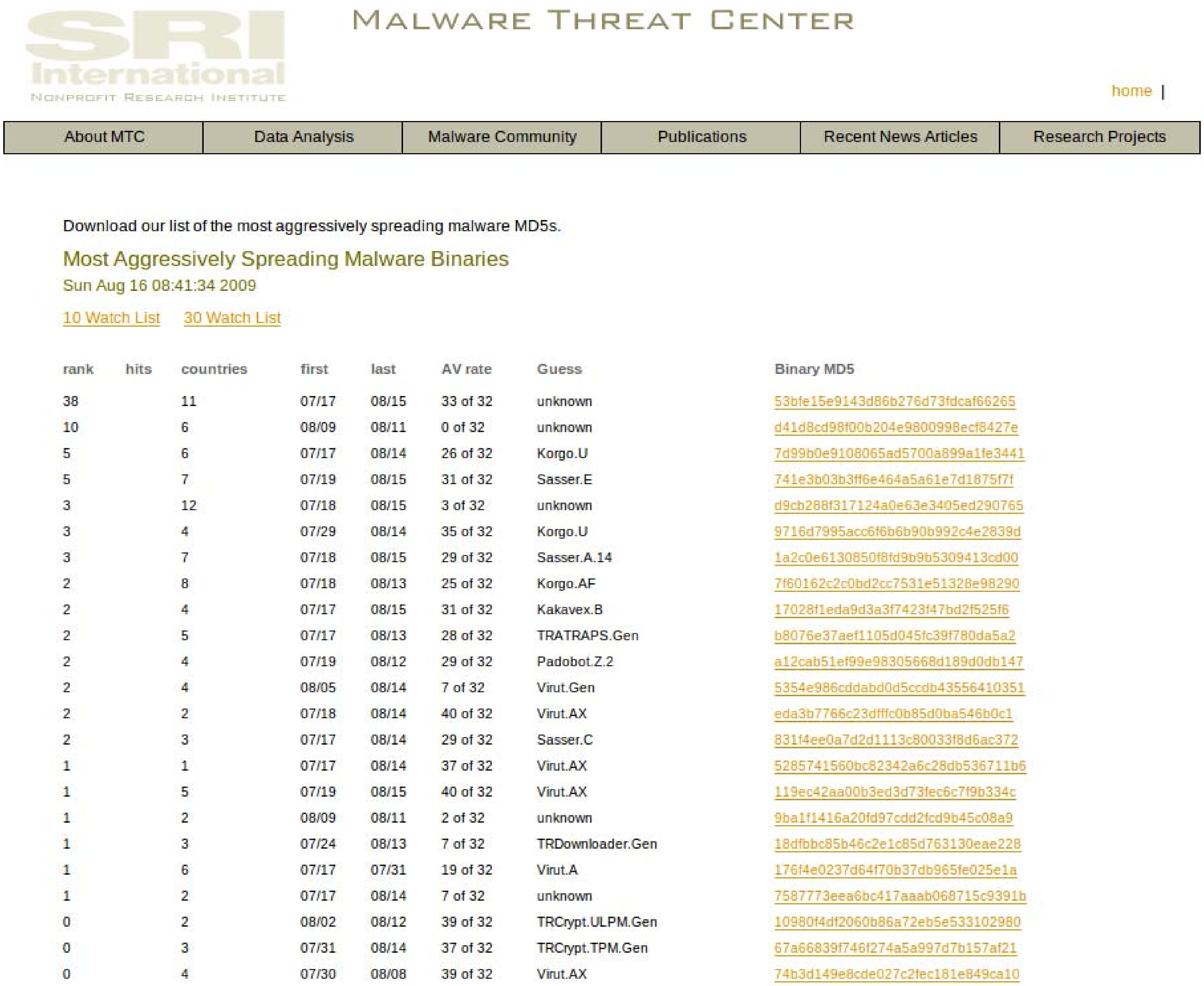


Virus	PCs infected	Threat Level	First appeared
1 Conficker.C	2.10%	🟥🟥⬜⬜	Dec 31, 2008
2 Downloader.MDW	1.62%	🟥🟥🟥⬜	Jan 02, 2007
3 Spy.YK	0.99%	🟥⬜⬜⬜	Nov 02, 2009
4 MediaPass	0.82%	🟥⬜⬜⬜	Apr 29, 2010
5 Vobfus.gen	0.70%	🟥⬜⬜⬜	Oct 06, 2009
6 AccesMembre	0.65%	🟥⬜⬜⬜	Jun 14, 2004
7 Sality.AK	0.58%	🟥⬜⬜⬜	Oct 08, 2008
8 Xor-encoded.A	0.50%	🟥⬜⬜⬜	Jun 02, 2008
9 FlySky.AD.	0.49%	🟥⬜⬜⬜	Jul 11, 2009
10 Agent.MUF	0.48%	🟥⬜⬜⬜	Sep 28, 2009

1 - **10** of **50** Active viruses 1 2 3 4 5 Next»

The list of 'Most Active viruses' contains the viruses detected in real time by the network of sensors that make up Panda's Global Virus Observatory.

http://www.pandasecurity.com/homeusers/security-info/default.aspx?lst=ac (100831)



MALWARE THREAT CENTER

Download our list of the most aggressively spreading malware MD5s.

Most Aggressively Spreading Malware Binaries

Sun Aug 16 08:41:34 2009

10 Watch List 30 Watch List

rank	hits	countries	first	last	AV rate	Guess	Binary MD5
38		11	07/17	08/15	33 of 32	unknown	53bfe15e9143d86b276d73fdcaf66265
10		6	08/09	08/11	0 of 32	unknown	d41d8cd98f00b204e9800998ecf8427e
5		6	07/17	08/14	26 of 32	Korgo.U	7d99b0e9108065ad5700a899a1fe3441
5		7	07/19	08/15	31 of 32	Sasser.E	741e3b03b3ff6e464a5a61e7d1875f7f
3		12	07/18	08/15	3 of 32	unknown	d9cb288f317124a0e63e3405ed290765
3		4	07/29	08/14	35 of 32	Korgo.U	9716d7995acc6f6b6b90b992c4e2839d
3		7	07/18	08/15	29 of 32	Sasser.A.14	1a2c0e6130850f8fd9b9b5309413cd00
2		8	07/18	08/13	25 of 32	Korgo.AF	7f60162c2c0bd2cc7531e51328e98290
2		4	07/17	08/15	31 of 32	Kakavex.B	17028f1eda9d3a3f7423f47bd2f525f6
2		5	07/17	08/13	28 of 32	TRATRAPS.Gen	b8076e37aef1105d045fc39f780da5a2
2		4	07/19	08/12	29 of 32	Padobot.Z.2	a12cab51ef99e98305668d189d0db147
2		4	08/05	08/14	7 of 32	Virut.Gen	5354e986cddabd0d5ccdb43556410351
2		2	07/18	08/14	40 of 32	Virut.AX	eda3b7766c23dfffc0b85d0ba546b0c1
2		3	07/17	08/14	29 of 32	Sasser.C	831f4ee0a7d2d1113c80033f8d6ac372
1		1	07/17	08/14	37 of 32	Virut.AX	5285741560bc82342a6c28db536711b6
1		5	07/19	08/15	40 of 32	Virut.AX	119ec42aa00b3ed3d73fec6c7f9b334c
1		2	08/09	08/11	2 of 32	unknown	9ba1f1416a20fd97cdd2fcd9b45c08a9
1		3	07/24	08/13	7 of 32	TRDownloader.Gen	18dfbbc85b46c2e1c85d763130eae228
1		6	07/17	07/31	19 of 32	Virut.A	176f4e0237d64f70b37db965fe025e1a
1		2	07/17	08/14	7 of 32	unknown	7587773eea6bc417aaab068715c9391b
0		2	08/02	08/12	39 of 32	TRCrypt.ULPM.Gen	10980f4df2060b86a72eb5e533102980
0		3	07/31	08/14	37 of 32	TRCrypt.TPM.Gen	67a66839f746f274a5a997d7b157af21
0		4	07/30	08/08	39 of 32	Virut.AX	74b3d149e8cde027c2fec181e849ca10

http://mtc.sri.com/live_data/binaries/

Malicious code - reasons for increase

A few trends that largely influence the wide spread of malicious code:

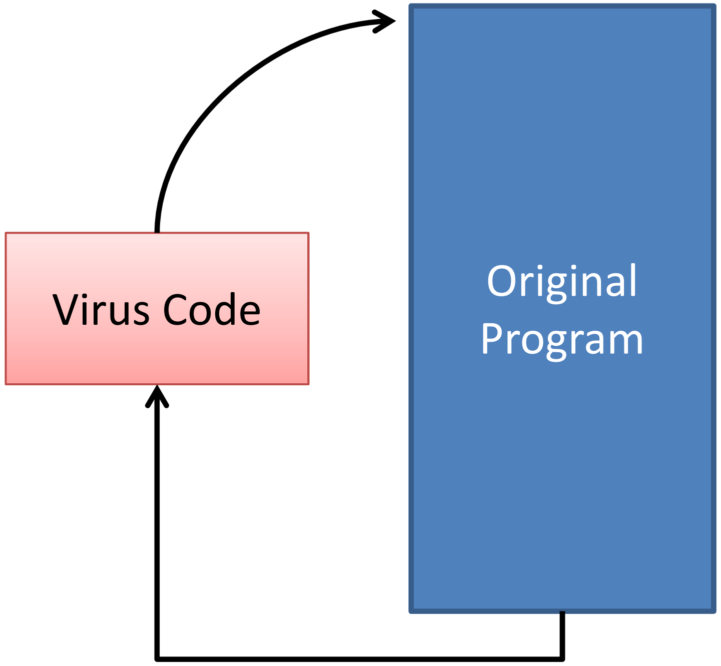
- **Growing number and connectivity of computers**
  - “everybody” is connected and dependant on computers
  - the number of attacks increases
  - attacks can be launched easily (automated attacks)
- **Growing system complexity**
  - unsafe programming languages
  - heterogeneity
  - hiding code is easy
  - verification and validation is impossible (let alone proofs)
- **Systems are easily extensible**
  - mobile code, dynamically loadable modules
  - incremental evolution of systems

Types of Malicious code (1)

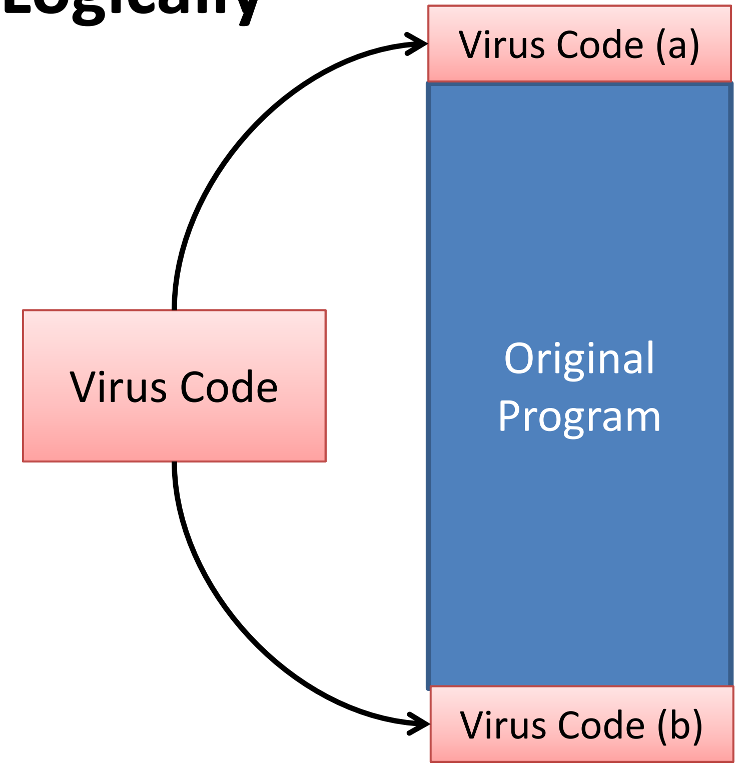
- **Traditional virus (1982)**
  - attaches to existing program code
  - intervenes in normal execution
  - replicates and propagates
- **Document virus (macro virus)**
  - highly formatted documents include commands (+data)
- **Stealth virus (and rootkits)**
  - hides the modifications it has made in the system, normally by monitoring system calls and forging the results of such calls
- **Polymorphic virus**
  - avoids virus scanners by producing multiple variant of itself or encrypting itself.

Virus Surrounding a Program

Physically

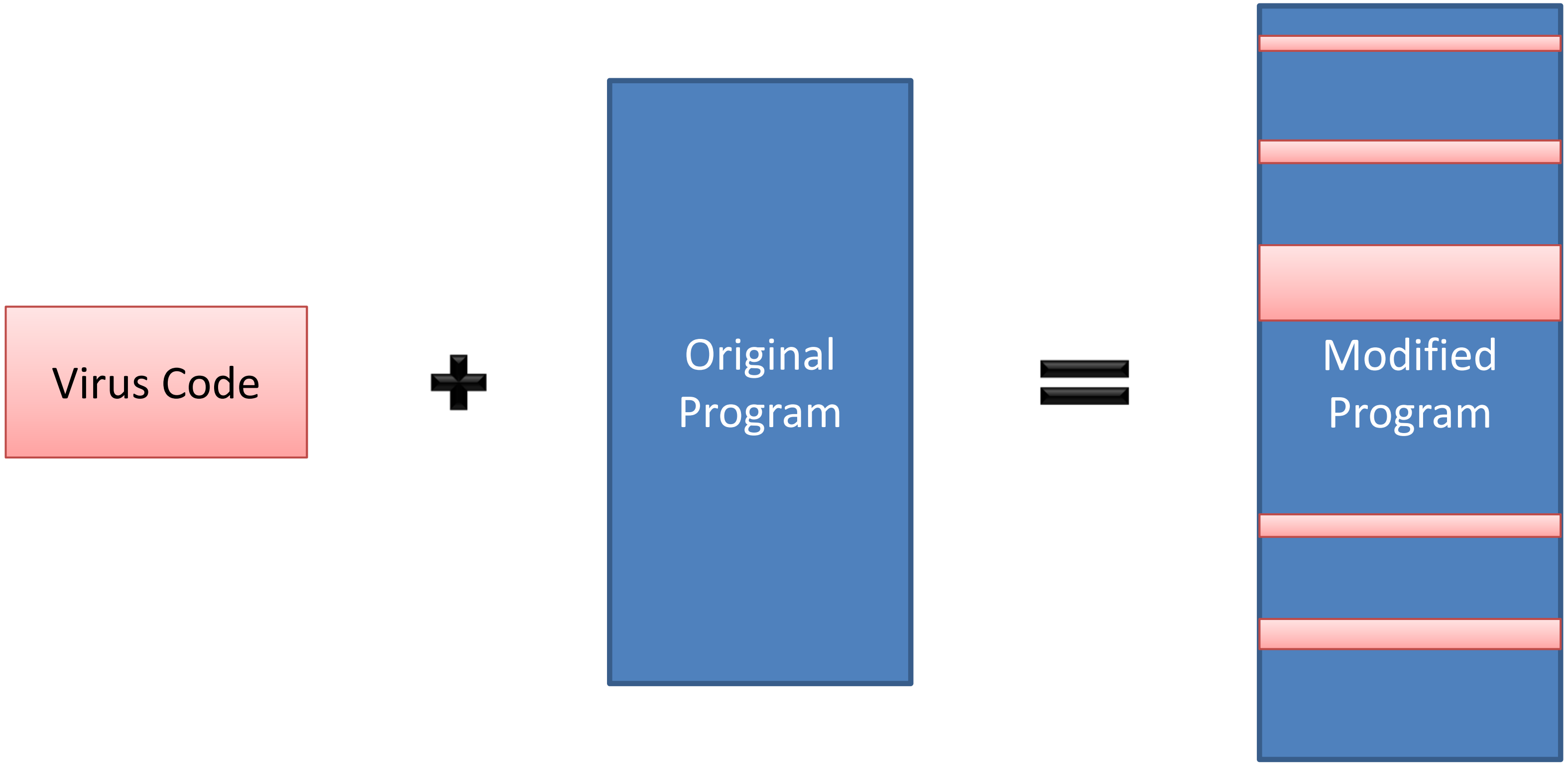


Logically



Pfleeger: p. 115 (119)

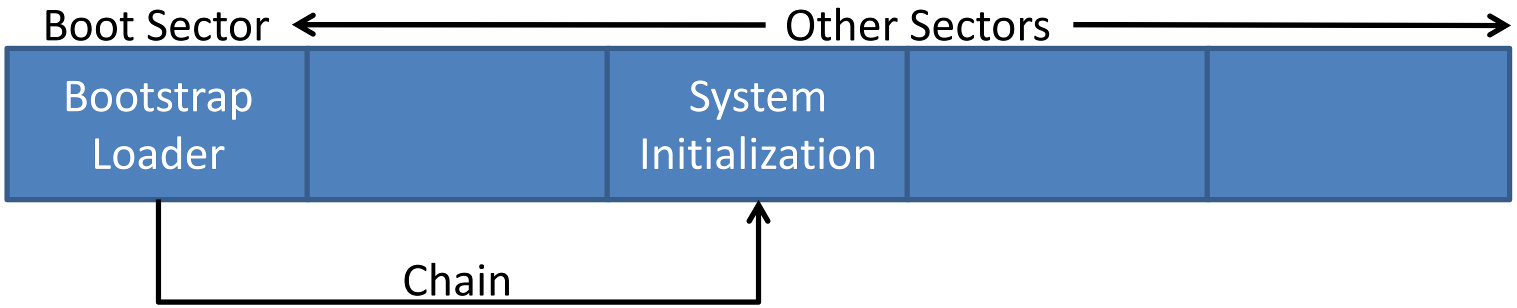
Virus Integrated into a Program



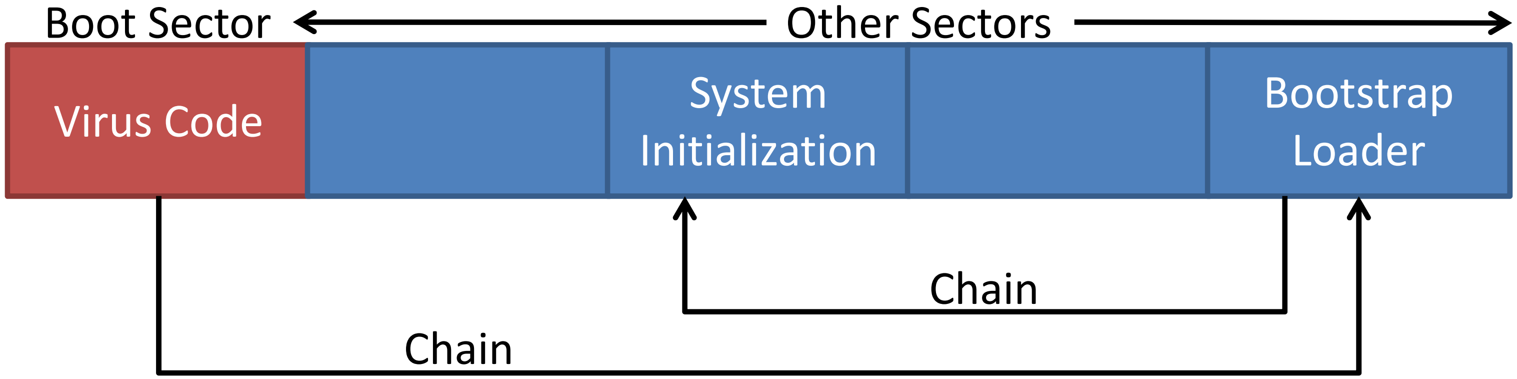
Pfleeger : p. 115 (120)

Boot Sector Virus Relocating Code

Before Infection

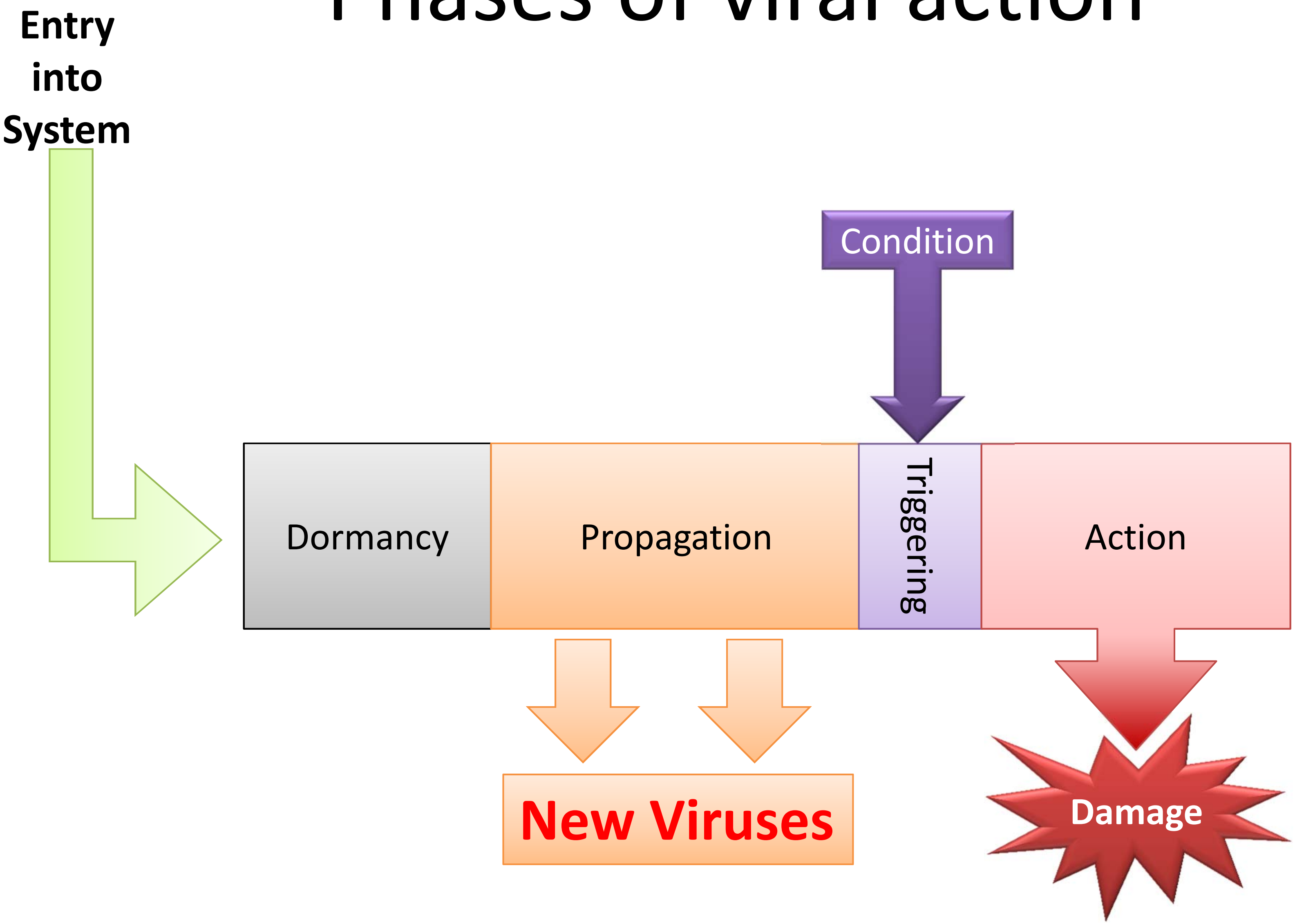


After Infection



Pfleeger: p. 119 (123)

Phases of viral action



Types of Malicious code (2)

- **Hoax virus**
  - is no virus at all. It is an email with a bogus warning
- **Rabbit** (or bacteria, greedy programs)
  - is a virus (or worm) that replicates without bounds, thus exhausting some computing resource. Does not spread to other systems (thus attacking *availability* only).
- **Worm** (1975, 1982)
  - is a stand-alone program that replicates and spreads copies of itself via the network. Non-trivial to make.
- **Trojan Horse**
  - is a “normal” program that contains some hidden functionality, that is unwanted by the user.

Hoax virus

----- Original Message -----
From: *** ********* <***@**.*****.***>
To: ***** ********* <**********@*****.***>
Sent: Wednesday, October 25, 2008 5:12 PM
Subject: Virus Warning

IMPORTANT, URGENT - ALL SEEING EYE VIRUS !
PASS THIS ON TO ANYONE YOU HAVE AN E-MAIL ADDRESS FOR.

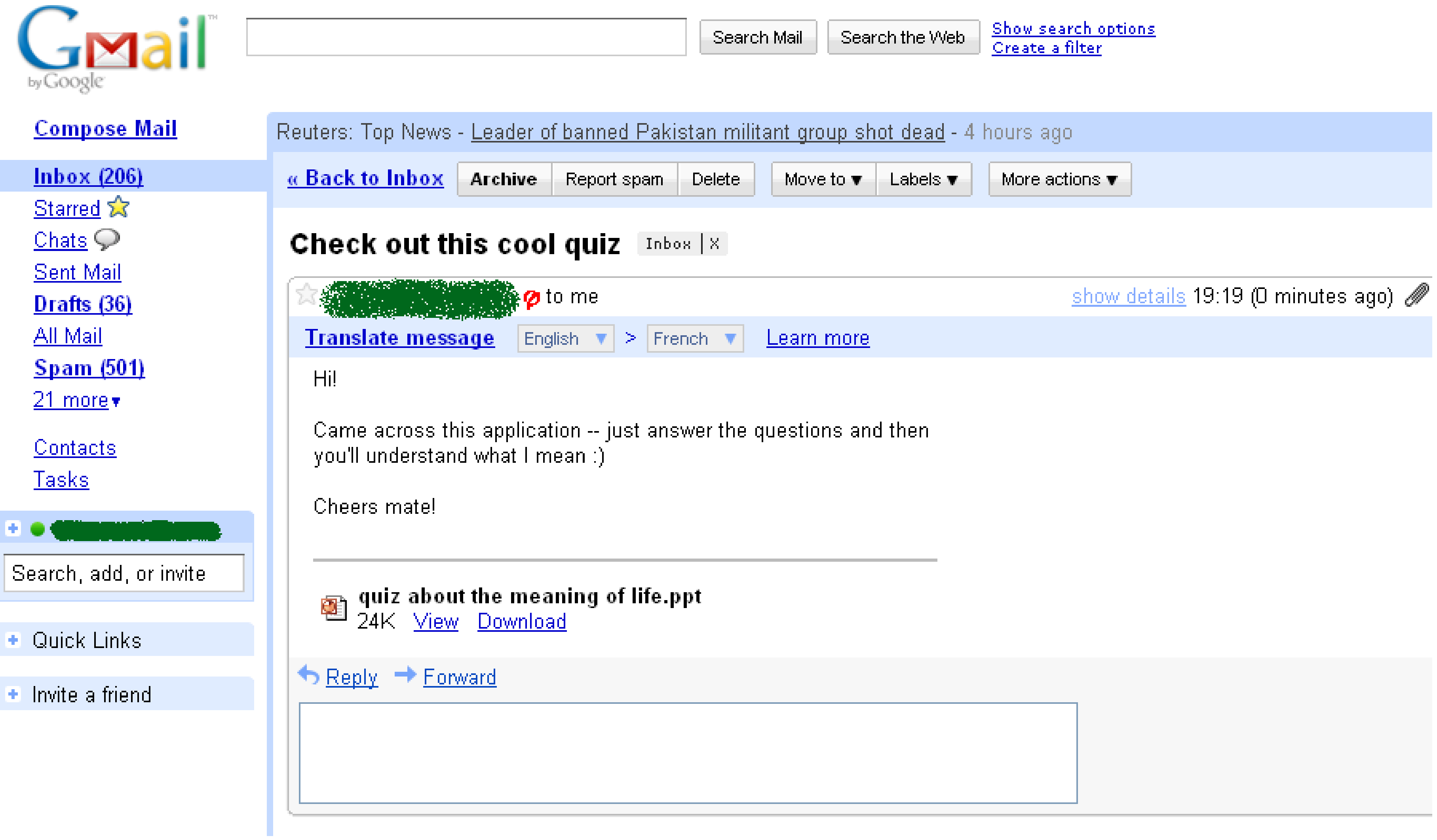
If you receive an email titled "*********" DO NOT OPEN IT ! It will erase everything on your hard drive. This information was announced yesterday morning from IBM, FBI and Microsoft states that this is a very dangerous and malicious virus, much worse than the "I Love You," virus and that there is NO remedy for at this time. Some very sick individual has succeeded in using the reformat function from Norton Utilities causing it to completely erase all documents on the hard drive. It has been designed to work with Netscape Navigator and Microsoft Internet Explorer. It destroys Macintosh and IBM compatible computers. This is a new, very malicious virus and not many people know about it. Pass this warning along to EVERYONE in your address book and please share it with all your online friends ASAP so that this threat may be stopped. Please practice cautionary measures and tell anyone that may have access to your computer. Forward this warning to everyone that might access the Internet.

Signature (Code Red Worm)

- Uses an **unchecked buffer** in a section of code that handles the input of the URLs:
- GET/default.ida?NNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

Sans: http://www.sans.org/resources/malwarefaq/code-red.php ; Pfleeger: p. 120 (124)

Trojan Horse Example



Reuters: Top News - Leader of banned Pakistan militant group shot dead - 4 hours ago

[redacted]

Check out this cool quiz Inbox | X

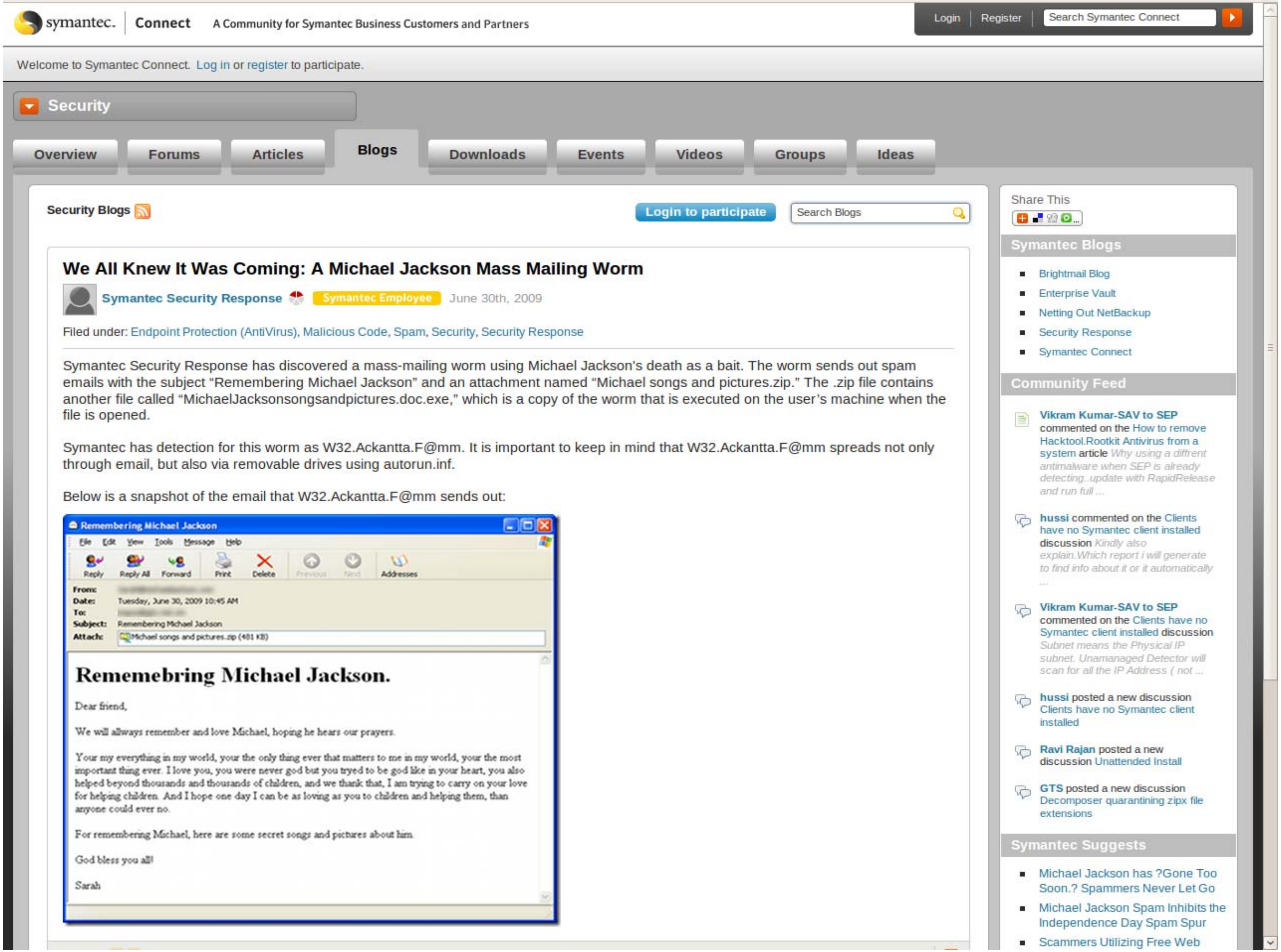
[redacted] to me show details 19:19 (0 minutes ago)

Hi!

Came across this application -- just answer the questions and then you'll understand what I mean :)

Cheers mate!

quiz about the meaning of life.ppt
24K View Download



symantec. Connect A Community for Symantec Business Customers and Partners
Login | Register | Search Symantec Connect

Welcome to Symantec Connect. Log in or register to participate.

Security
Overview Forums Articles Blogs Downloads Events Videos Groups Ideas

Security Blogs

Login to participate
Search Blogs

We All Knew It Was Coming: A Michael Jackson Mass Mailing Worm

Symantec Security Response Symantec Employee June 30th, 2009

Filed under: Endpoint Protection (AntiVirus), Malicious Code, Spam, Security, Security Response

Symantec Security Response has discovered a mass-mailing worm using Michael Jackson's death as a bait. The worm sends out spam emails with the subject "Remembering Michael Jackson" and an attachment named "Michael songs and pictures.zip." The .zip file contains another file called "MichaelJacksonsongsandpictures.doc.exe," which is a copy of the worm that is executed on the user's machine when the file is opened.

Symantec has detection for this worm as W32.Ackantta.F@mm. It is important to keep in mind that W32.Ackantta.F@mm spreads not only through email, but also via removable drives using autorun.inf.

Below is a snapshot of the email that W32.Ackantta.F@mm sends out:

Remembering Michael Jackson
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: [redacted]
Date: Tuesday, June 30, 2009 10:45 AM
To: [redacted]
Subject: Remembering Michael Jackson
Attach: Michael songs and pictures.zip (481 KB)

Rememebring Michael Jackson.

Dear friend,

We will allways remember and love Michael, hoping he hears our prayers.

Your my everything in my world, your the only thing ever that matters to me in my world, your the most important thing ever. I love you, you were never god but you tryed to be god like in your heart, you also helped beyond thousands and thousands of children, and we thank that, I am trying to carry on your love for helping children. And I hope one day I can be as loving as you to children and helping them, than anyone could ever no.

For remembering Michael, here are some secret songs and pictures about him.

God bless you all!

Sarah

Share This

Symantec Blogs

- Brightmail Blog
- Enterprise Vault
- Netting Out NetBackup
- Security Response
- Symantec Connect

Community Feed

Vikram Kumar-SAV to SEP commented on the How to remove Hacktool.Rootkit Antivirus from a system article *Why using a diffrent antimalware when SEP is already detecting..update with RapidRelease and run full ...*

hussi commented on the Clients have no Symantec client installed discussion *Kindly also explain.Which report i will generate to find info about it or it automatically ...*

Vikram Kumar-SAV to SEP commented on the Clients have no Symantec client installed discussion *Subnet means the Physical IP subnet. Unamanaged Detector will scan for all the IP Address (not ...*

hussi posted a new discussion Clients have no Symantec client installed

Ravi Rajan posted a new discussion Unattended Install

GTS posted a new discussion Decomposer quarantining zipx file extensions

Symantec Suggests

- Michael Jackson has ?Gone Too Soon.? Spammers Never Let Go
- Michael Jackson Spam Inhibits the Independence Day Spam Spur
- Scammers Utilizing Free Web

http://home.mcafee.com/AdviceCenter/most-dangerous-celebrities

Dangerous People (!!!)

"Cameron Diaz"-searches yield ten percent risk of landing on a malicious site

Types of Malicious code (3)

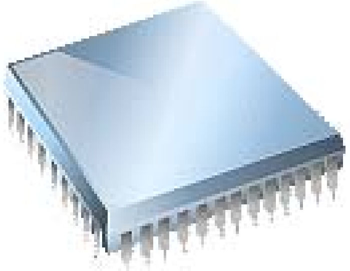
- **Logic bomb**
  - malware that triggers on a condition and “detonates”
- **Time bomb**
  - malware that triggers on a time condition and “detonates
- **Trap door (Back door)**
  - is an undocumented and unknown (to the user) entry point to a system,
  - normally inserted during the system design phase, and
  - could be put there for a useful purpose (trouble shooting, testing, maintenance, but left by mistake.
- **Salami attack**
  - achieving some economic benefit but making a large number of insignificant changes, e.g. rounding errors.

Types of Malicious Code

Code Type	Characteristics
Virus	**Attaches** itself to a program and propagates copies of itself to other programs (1980:ies)
Trojan horse	Contains unexpected, additional functionality
Logic bomb	Triggers action when condition occurs
Time bomb	Triggers action when specified time occurs
Trapdoor, backdoor	Allows unauthorized access to functionality
Worm	Propagates copies of itself through a network, replicating, stand-alone (1975, 1982)
Rabbit, Bacteria, Greedy program	Replicates itself without limit to exhaust resource (cmp flooding Denial-of-service attack)
Salami attack	Uses seemingly inconsequential data; Example: fractions of cents when calculating interests for bank accounts → accumulated into hacker's account. Each account owner would not notice ***but*** ∑ many small pieces = significant amount.

Stallings: p. 217;Pfleeger: p. 112 (117)

Hardware Tampering



- So far, only discussed problems in software.
- Tampering can also happen in the hardware, where the vulnerability or the Trojan horse is permanently etched in the component.
- Supply chain is becoming global, and the very complex components are made all over the world, which makes it difficult to control the process.
- Can you really trust your computer?

Mobile code
Examples

- **Attack script**
  - – Javascript, VisualBasic scripts, **…**
- **Java applets**
- **ActiveX control**
    - is a Microsoft version of a Java applet, and
    - is much more powerful that the Java applet.
    - ActiveX controls are extremely dangerous if used for malicious purposes.

Stallings: p. 219

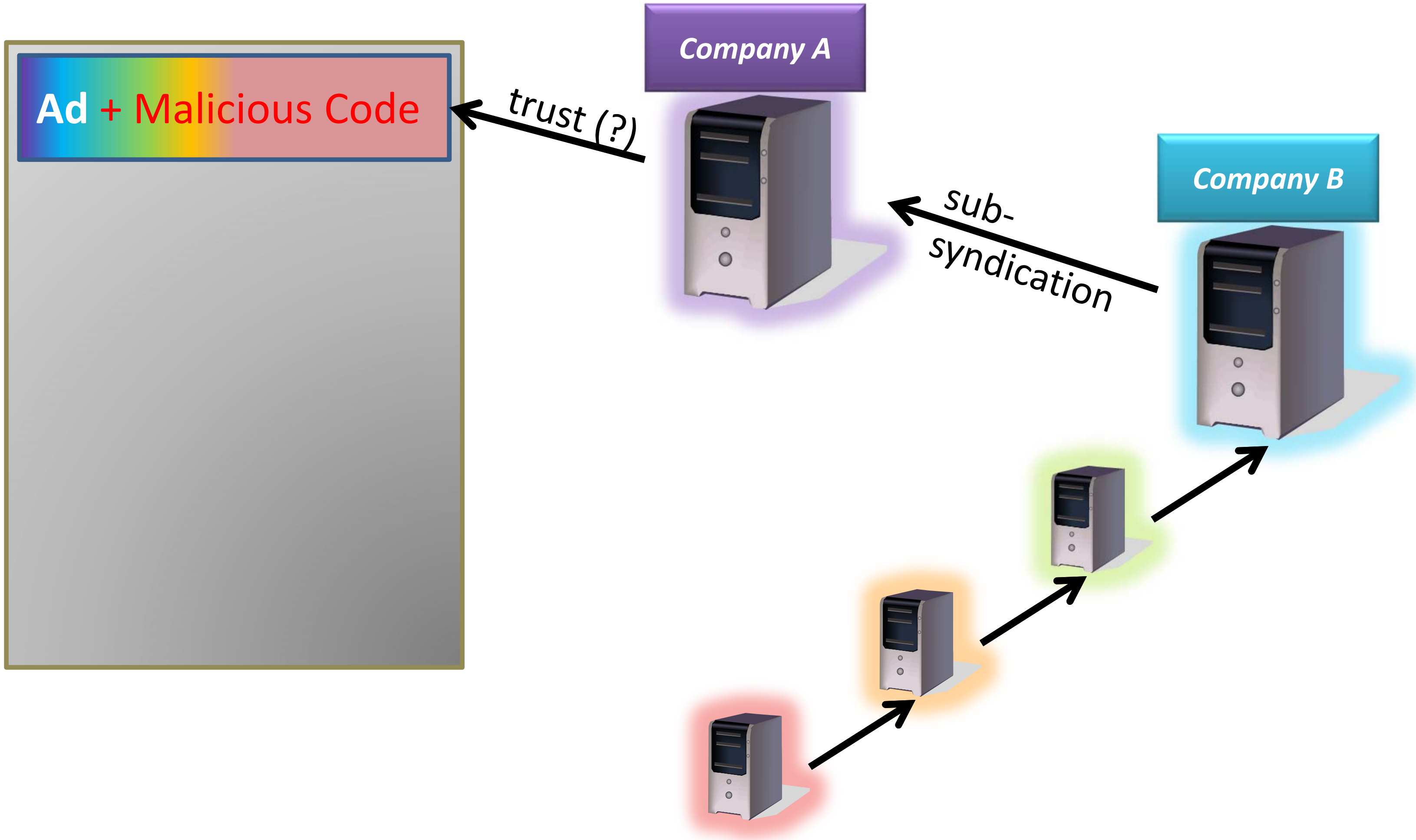
Drive-by Downloads

- Download of **malware** through exploitation of a web browser, e-mail client or operating system bug, **without any user intervention** whatsoever. (Wikipedia)
- Pwn2Own 2009: Hacking contest targeting browsers
  - Firefox, Safari, Internet Explorer hacked immediately.
  - Google Chrome had problem but could not be hacked.

http://research.google.com/archive/provos-2008a.pdf

http://arstechnica.com/security/news/2009/03/chrome-is-the-only-browser-left-standing-in-pwn2own-contest.ars

Drive-by Downloads
An Example (6)


Ad + Malicious Code
trust (?)
Company A
sub-syndication
Company B