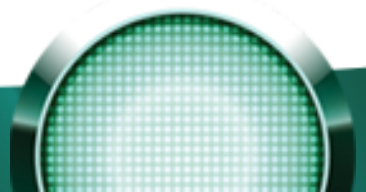
Run silent, run deep: today's threat landscape

David Emm

Senior Technology Consultant

david.emm@kaspersky.co.uk

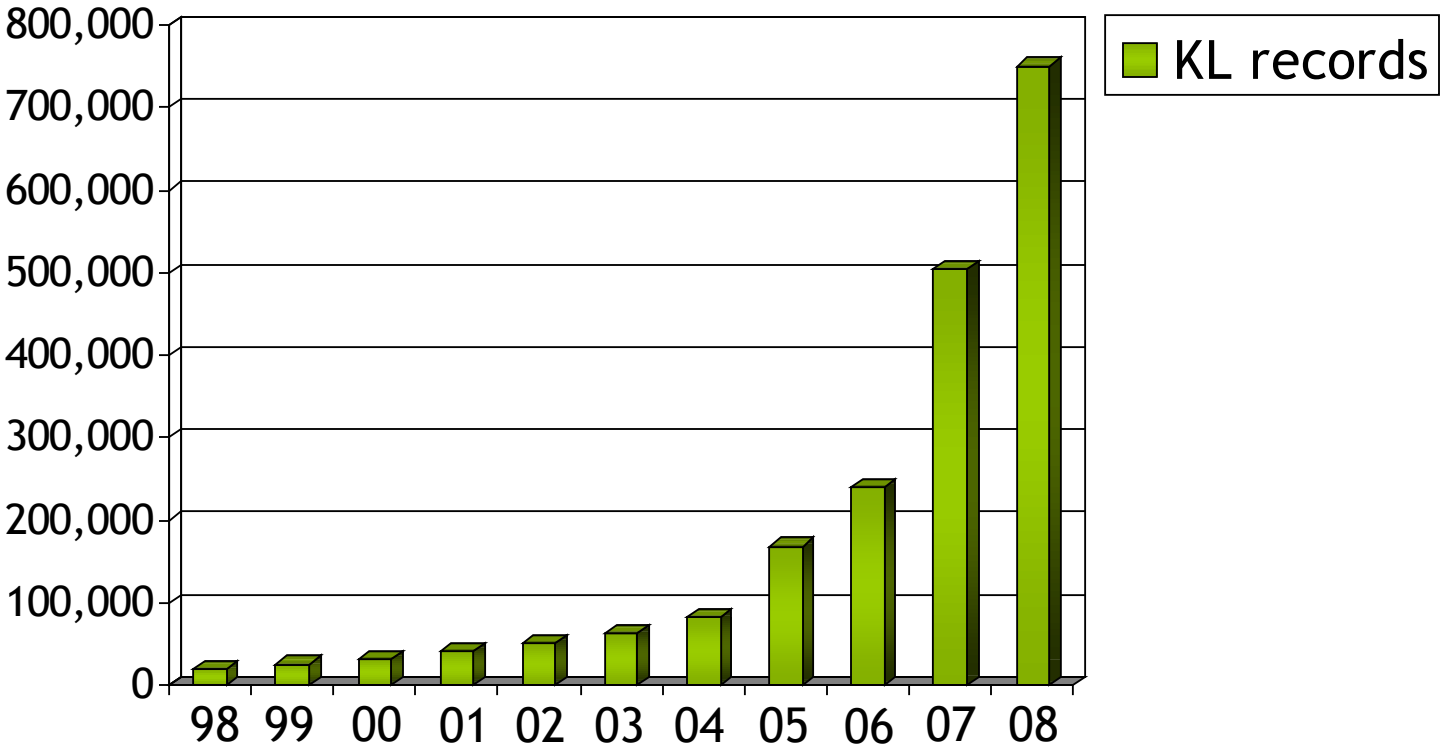


KASPERSKY lab

Agenda

- Today's threat landscape
- Trojans & botnets
- Banking malware
- Ransomware
- Web-based attacks
- Stealth
- Polymorphism
- Sabotage
- Future prospects
- 'Upping the Anti-'

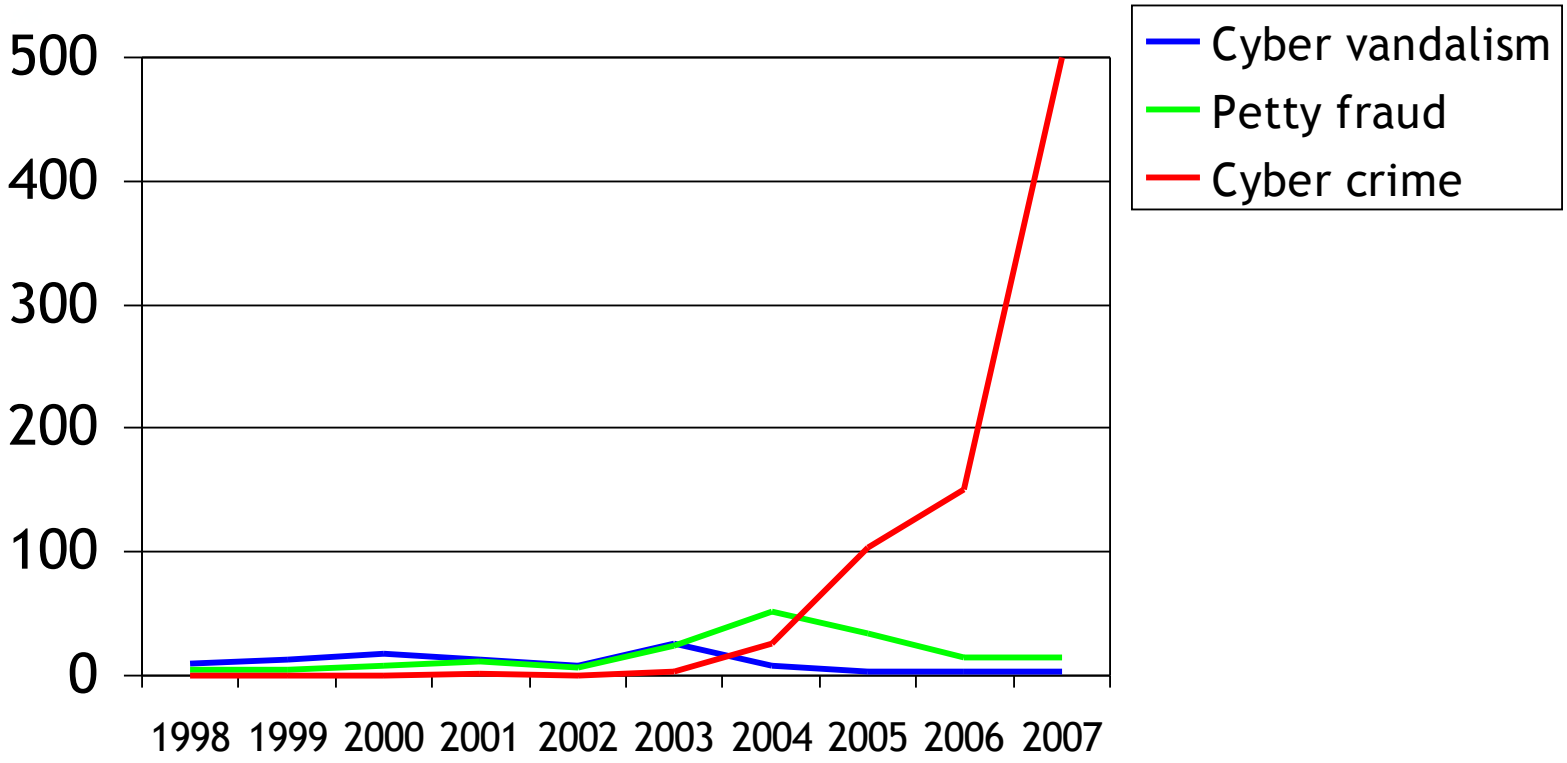
Increasing numbers



Source: Kaspersky Lab

Who & why?

- Types of malware in daily updates



Source: Kaspersky Lab

Who & why?

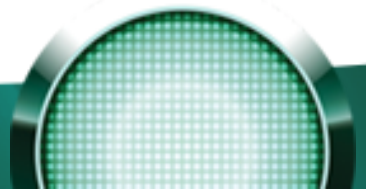
- In the 1990s
  - Acts of computer vandalism or petty crime
  - Many written by teenagers
- Today's malware
  - 'Crimeware'
  - Tailored for Illegal commercial activity
    - Fraud
    - Unwanted advertising
    - Extortion & data destruction
    - Other purposes . . . dialers, virtual property theft

Latest threats

- The ‘virus’ threat today

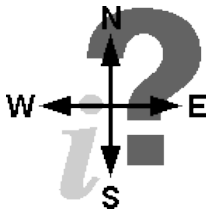
LATEST VIRUSES	Detection time
7 May 2008	
Trojan-PSW.Win32.Magania.nxq	11:43
Trojan-PSW.Win32.Magania.nxp	11:43
Backdoor.Win32.Hupigon.btya	11:40
Backdoor.Win32.Hupigon.btxz	11:40
Trojan.Win32.Agent.lqu	11:38
Trojan-Downloader.Win32.Zlob.mqf	11:38
not-a-virus:AdWare.Win32.Virtumonde.qvw	11:38
Trojan.Win32.Dialer.baa	11:38
Trojan-Dropper.Win32.Pincher.ao	11:38
Trojan-Spy.Win32.Delf.byy	11:37

Source: Kaspersky Lab Virus Watch



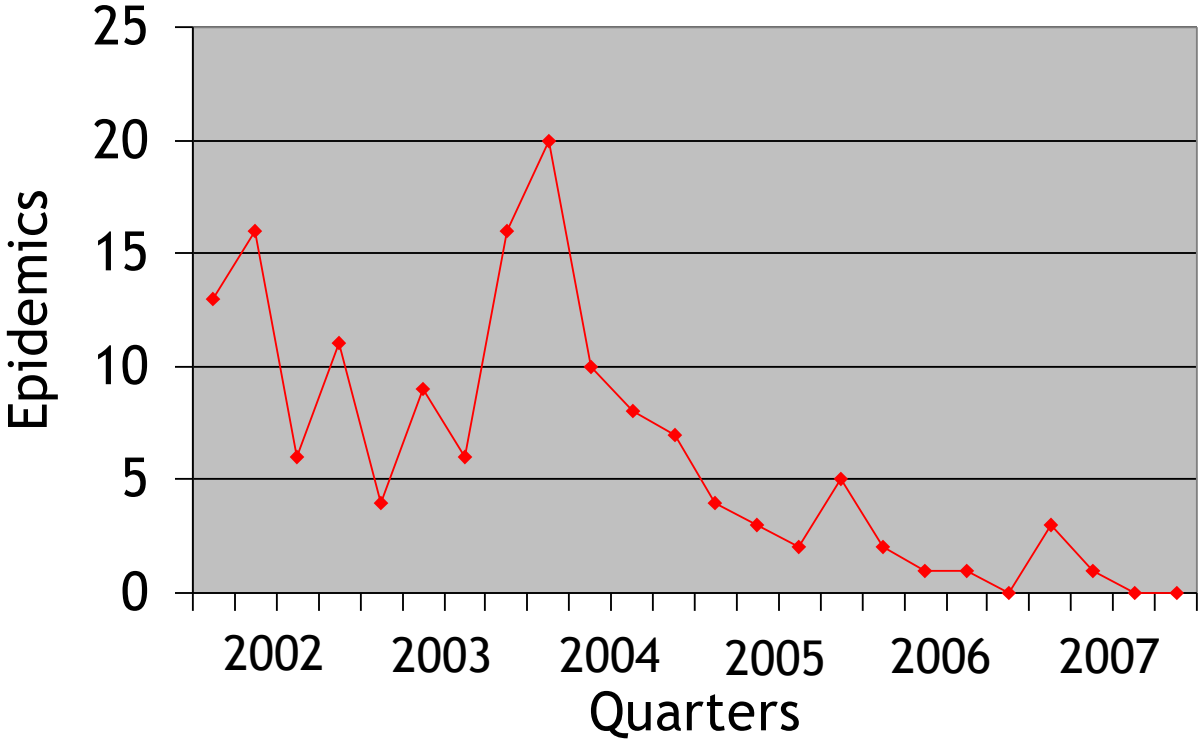
KASPERSKY lab

Where?



- Top sources of malicious code
  - China
  - Latin America
  - Russia & eastern Europe
- Malware ‘division of labour’
  - Online games in China
  - Banking Trojans in Latin America
  - Botnets in Russia & eastern Europe
- Cyber crime mirrors the legitimate economy
  - i.e. interdependence of different activities

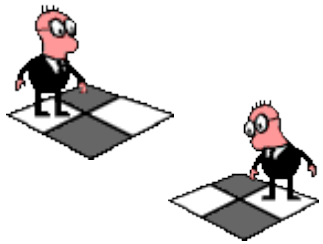
The end of *global* epidemics



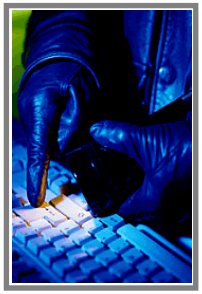
Source: Kaspersky Lab

Today's tactics

- Low-key, localised outbreaks
  - Less visible to AV 'early warning radar'
  - Less visible to law enforcement agencies
  - Infected PC population more 'manageable'
    - i.e. easier to process stolen data
  - Sabotage security defences
  - & compete to 'own' victims



Today's attack methods



- Spam mailing
  - Instead of self-replication
- Trojans
  - Spyware
  - ID theft
  - Botnets
- Exploits
  - 'Drive-by downloads'
- Phishing & other banking threats

Trojans

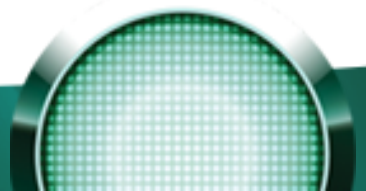
- 90% of threats are Trojans
  - Today's 'weapon of choice'
- But what is a Trojan?
- Think Greek myth … Trojan *Horse*
  - Looks like it's good
  - But does something bad

Today's Trojans

- Different types of Trojan
- Tailored for specific purposes
  - Backdoor Trojans
  - PSW Trojans
  - Trojan Spies
  - Trojan Droppers
  - Trojan Downloaders
  - Trojan Proxies
  - Trojan Notifiers
  - Trojan Clickers
  - ArcBombs

Spyware

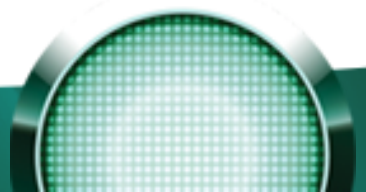
- Programs that ‘spy’ on the user
  - Without the user’s knowledge or consent
- Track activity & gather information
- Examples
  - Key strokes
  - Confidential information
    - Login & password
    - CC & PIN numbers
  - E-mail addresses
  - Browsing habits



KASPERSKY lab

Spyware

- No industry standard definition
- Catch-all term for different threats
  - Trojans
  - Adware
  - Dialers & other ‘pornware’ programs
  - Other ‘potentially unwanted’ programs
    - ‘Riskware’

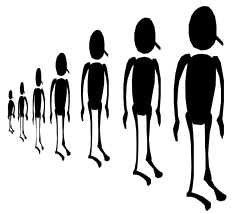


KASPERSKY lab

Spyware

- Potential impact
  - Data loss
  - Privacy issues
  - Legal issues
    - Unwanted things done ‘on your behalf’
  - Bandwidth loss
  - System instability
    - Reduce performance
    - Web browser problems

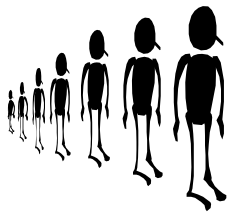
Botnets



- Some backdoors include a scanner
  - To locate all victims
  - & co-ordinate their actions
    - Using IRC channels, IM or WWW
- The result is a ‘bot network’
  - Network of remotely-controlled victims
  - Sometimes referred to as a ‘zombie army’
  - Used for spam distribution
  - Or DDoS attacks

Botnets

- Command-and-control
  - Through a central server
- Or distributed
  - Using P2P model
    - Zhelatin
    - Mayday



Attacked hosts (total - uniq)	
IE XP ALL	114721 - 96104
QuickTime	2175 - 2048
Win2000	7033 - 6260
Firefox	12885 - 12514
Opera7	1271 - 1264

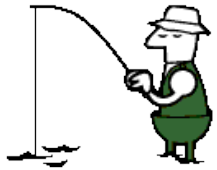
Traffic (total - uniq)	
Total traff	159073 - 129089
Exploited	44804 - 35574
Loads count	17408 - 15968
Loader's response	38.85% - 44.89%
Efficiency 10.94% - 12.37%	

Browser stats (total)	
MSIE	4 0%
Opera	1 0%

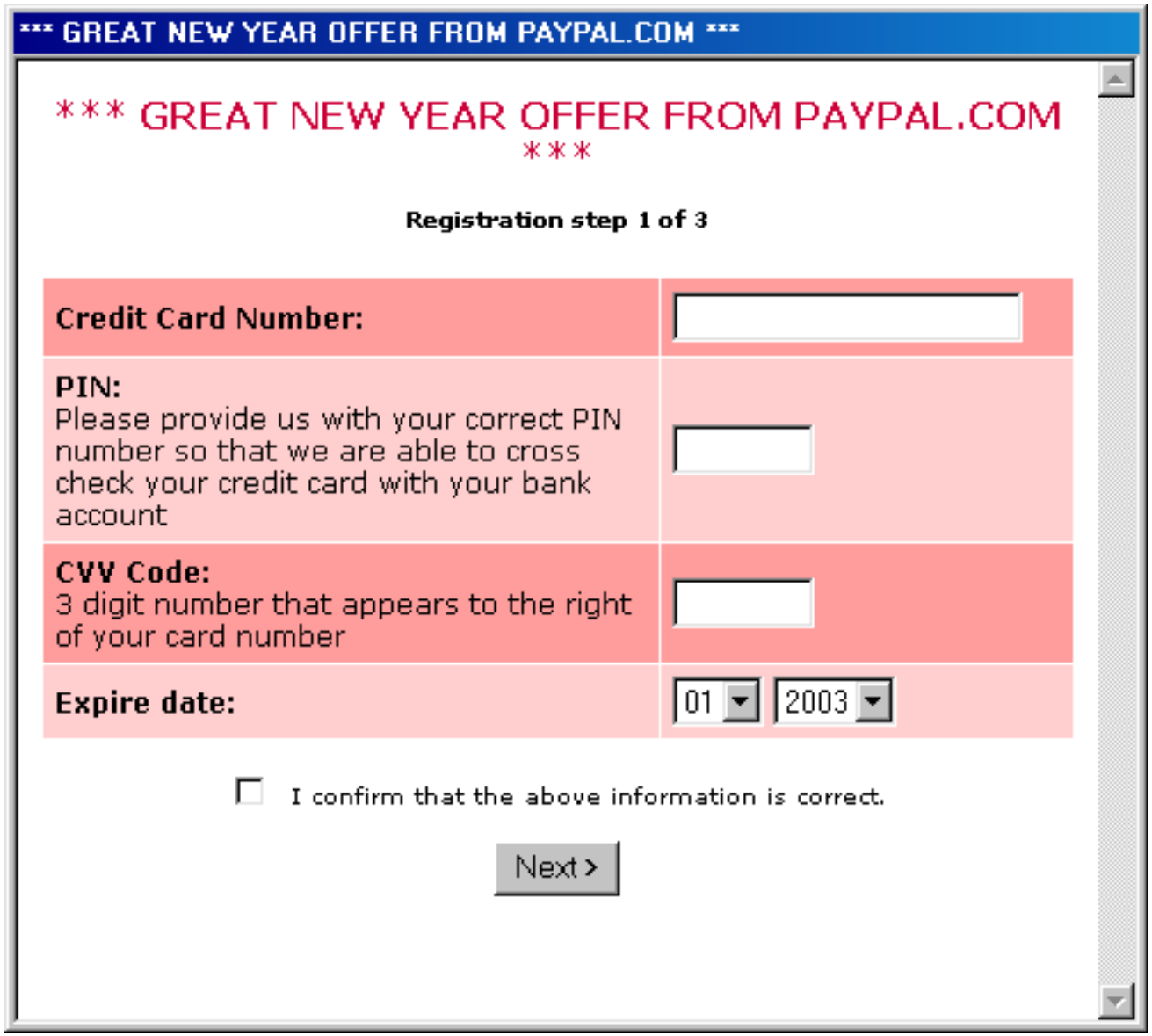
Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

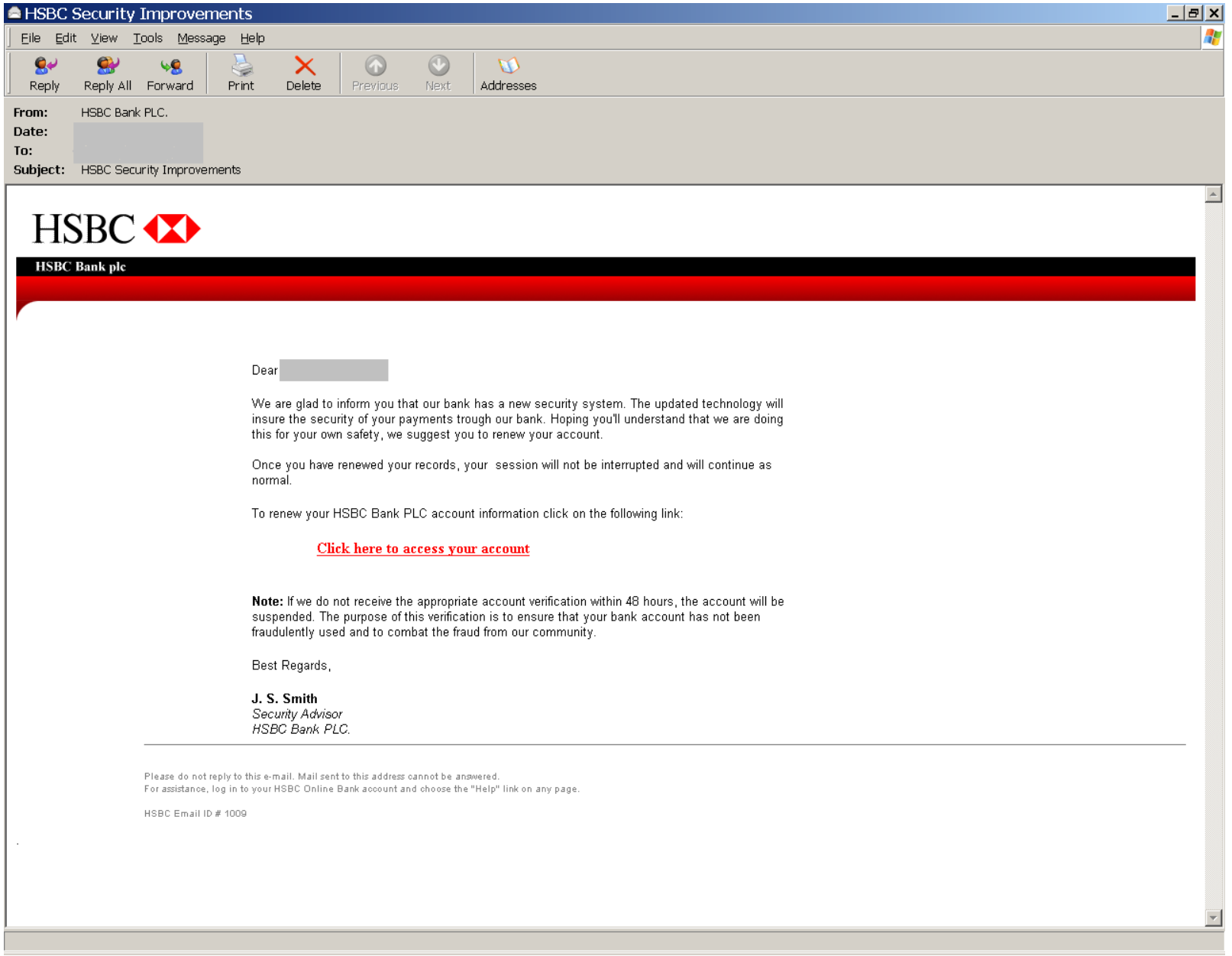
Country	Traff	Loads	Efficiency
RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
IT - Italy	7045 4.4%	593 3.4%	8.42%
GE - Georgia	5775 3.6%	673 3.9%	11.65%
BY - Belarus	5419 3.4%	657 3.8%	12.12%
KZ - Kazakstan	3098 1.9%	376 2.2%	12.14%
US - United states	1117 0.7%	50 0.3%	4.48%
AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%

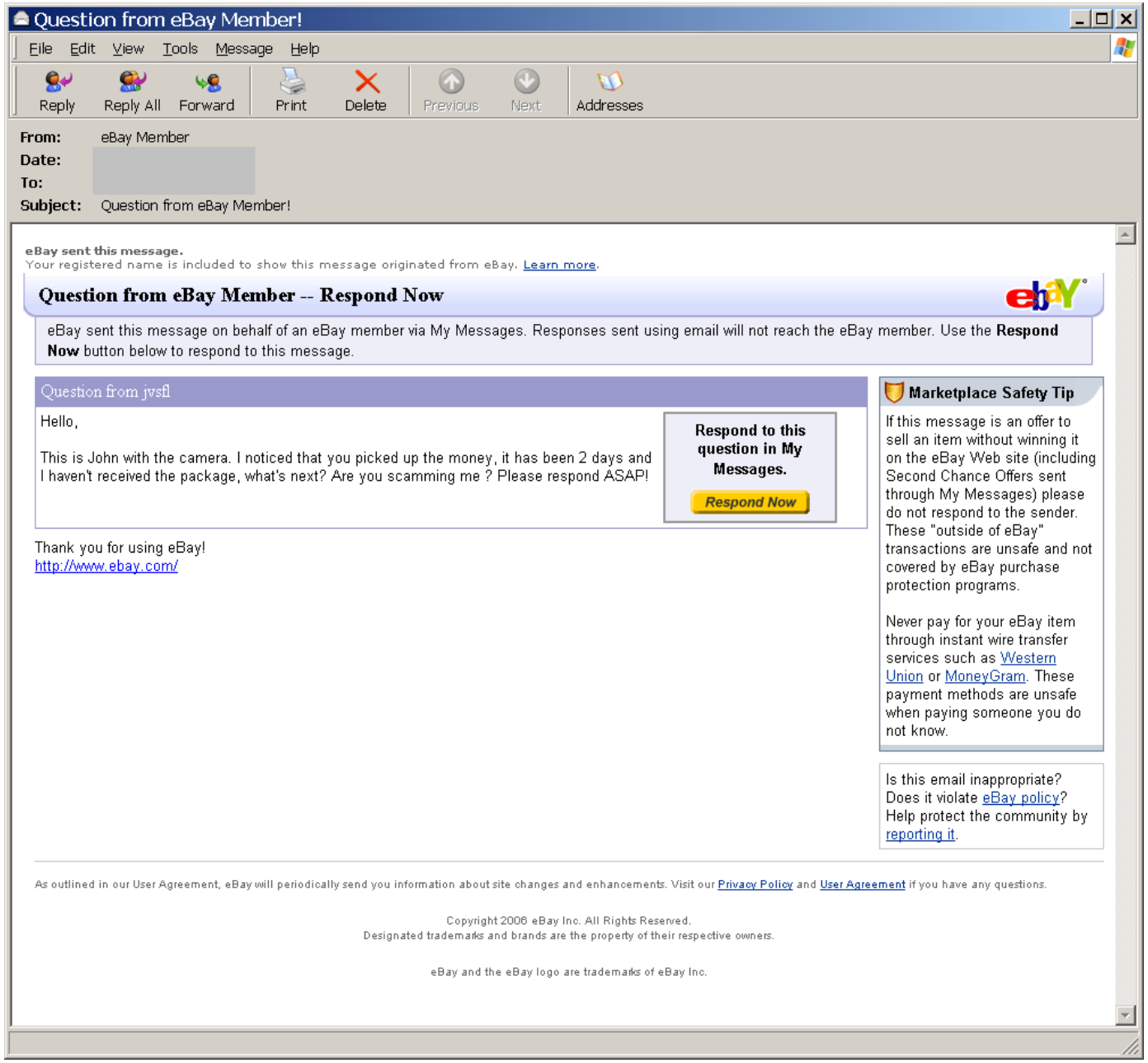
Banking malware [1]



- Phishing
- Typically starts with a spam e-mail
  - Spoofed ‘From’ address
  - Same style & logo as bank
    - Or other organization handling online financial transactions
  - E-mail message contains a link
    - Directs victim to a fake web-site
    - That looks like the bank’s web-site
    - Used to capture confidential data
      - Login, password, PIN


*** GREAT NEW YEAR OFFER FROM PAYPAL.COM ***
*** GREAT NEW YEAR OFFER FROM PAYPAL.COM ***
Registration step 1 of 3
Credit Card Number:
PIN:
Please provide us with your correct PIN number so that we are able to cross check your credit card with your bank account
CVV Code:
3 digit number that appears to the right of your card number
Expire date:
01
2003
I confirm that the above information is correct.
Next >


HSBC Security Improvements
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: HSBC Bank PLC.
Date:
To:
Subject: HSBC Security Improvements
HSBC
HSBC Bank plc
Dear
We are glad to inform you that our bank has a new security system. The updated technology will insure the security of your payments trough our bank. Hoping you'll understand that we are doing this for your own safety, we suggest you to renew your account.
Once you have renewed your records, your session will not be interrupted and will continue as normal.
To renew your HSBC Bank PLC account information click on the following link:
Click here to access your account
Note: If we do not receive the appropriate account verification within 48 hours, the account will be suspended. The purpose of this verification is to ensure that your bank account has not been fraudulently used and to combat the fraud from our community.
Best Regards,
J. S. Smith
Security Advisor
HSBC Bank PLC.
Please do not reply to this e-mail. Mail sent to this address cannot be answered.
For assistance, log in to your HSBC Online Bank account and choose the "Help" link on any page.
HSBC Email ID # 1009


Question from eBay Member!
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: eBay Member
Date:
To:
Subject: Question from eBay Member!
eBay sent this message.
Your registered name is included to show this message originated from eBay. Learn more.
Question from eBay Member -- Respond Now
eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will not reach the eBay member. Use the Respond Now button below to respond to this message.
Question from jvsfl
Hello,
This is John with the camera. I noticed that you picked up the money, it has been 2 days and I haven't received the package, what's next? Are you scamming me ? Please respond ASAP!
Respond to this question in My Messages.
Respond Now
Thank you for using eBay!
http://www.ebay.com/
Marketplace Safety Tip
If this message is an offer to sell an item without winning it on the eBay Web site (including Second Chance Offers sent through My Messages) please do not respond to the sender. These "outside of eBay" transactions are unsafe and not covered by eBay purchase protection programs.
Never pay for your eBay item through instant wire transfer services such as Western Union or MoneyGram. These payment methods are unsafe when paying someone you do not know.
Is this email inappropriate? Does it violate eBay policy? Help protect the community by reporting it.
As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.
Copyright 2006 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are trademarks of eBay Inc.

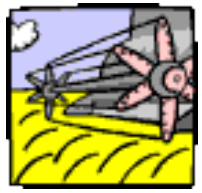
Banking malware [2]

- Technical engineering
- Re-direct victim's web traffic
  - Change host DNS server
  - Change gateway DNS server
  - Use a DLL [i.e. BHO] to re-direct traffic
  - Modify 'hosts' file

Banking malware [3]

- Technical engineering
- ‘Man-in-the-middle’
  - Re-direct traffic through proxy ‘go-between’ server
  - & leave SSL ‘intact’
- Patch Windows files
- ‘Man-in-the endpoint’
  - HTML insertion
  - Undetectable for bank
  - Even using one- or two-factor authentication

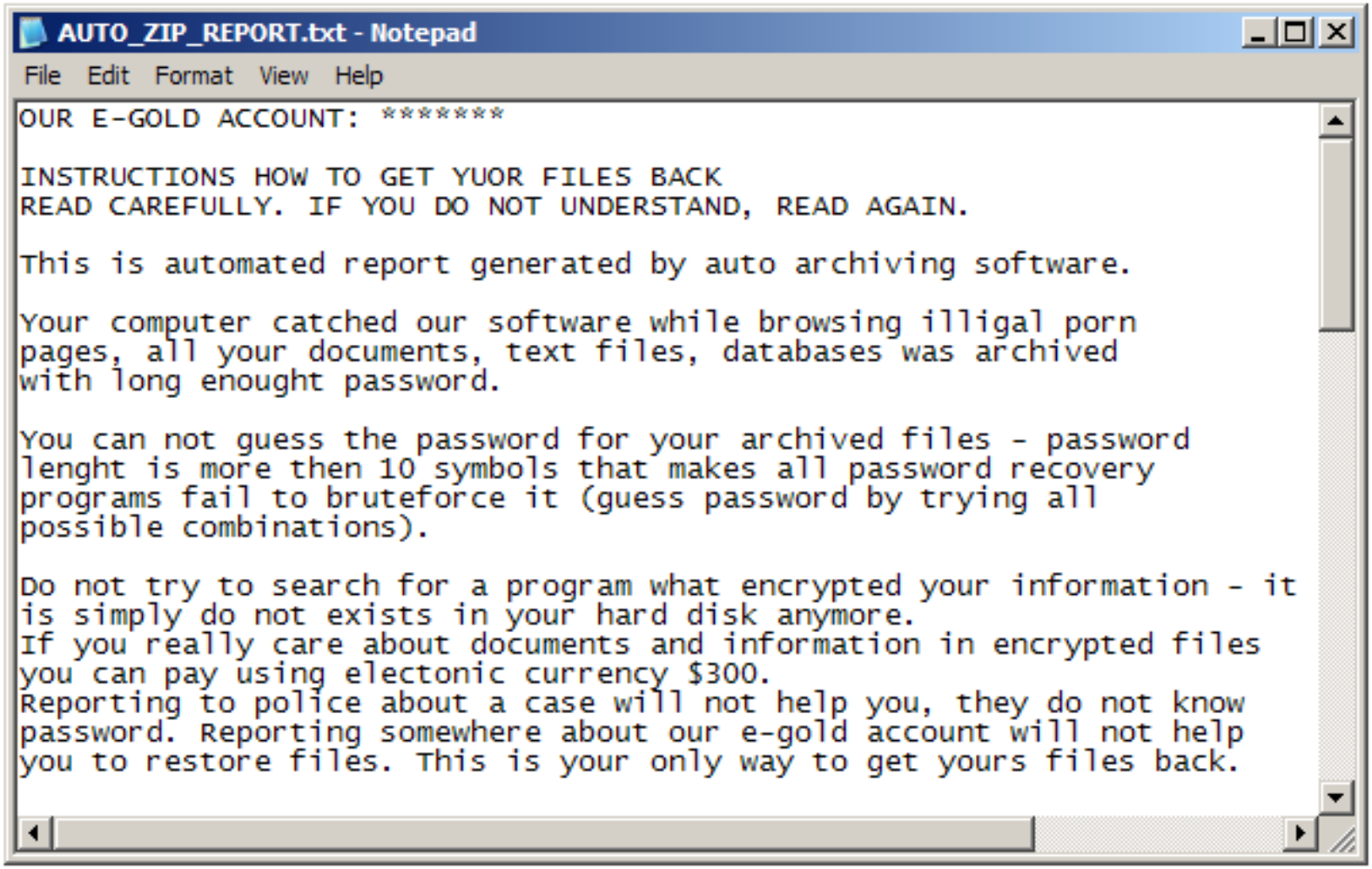
Banking malware [4]



- DNS cache poisoning
- aka ‘pharming’
- Exploit vulnerability in DNS server
  - Spoof entries in the cache
  - To return a fake IP address for the domain requested by user

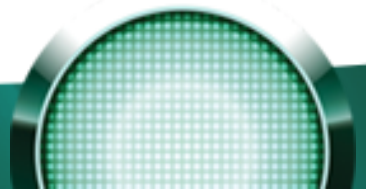
Ransomware

- Cyber blackmail
- Virus, worm or Trojan
- Encrypt user's data
- Create a text file
  - The ransom demand
  - Instructions on how to restore data
  - e-payment
- Examples
  - Gpcode, Krotten, JuNy, Cryzip, Skowor


AUTO_ZIP_REPORT.txt - Notepad
File Edit Format View Help
OUR E-GOLD ACCOUNT: *******
INSTRUCTIONS HOW TO GET YUOR FILES BACK
READ CAREFULLY. IF YOU DO NOT UNDERSTAND, READ AGAIN.
This is automated report generated by auto archiving software.
Your computer catched our software while browsing illigal porn pages, all your documents, text files, databases was archived with long enought password.
You can not guess the password for your archived files - password lenght is more then 10 symbols that makes all password recovery programs fail to bruteforce it (guess password by trying all possible combinations).
Do not try to search for a program what encrypted your information - it is simply do not exists in your hard disk anymore.
If you really care about documents and information in encrypted files you can pay using electonic currency $300.
Reporting to police about a case will not help you, they do not know password. Reporting somewhere about our e-gold account will not help you to restore files. This is your only way to get yours files back.

Web-based attacks

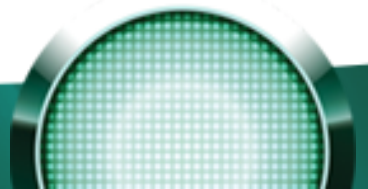
- Find a host web server
  - Exploit a vulnerability
  - Upload ‘user’ content or third-party script
- Inject malicious HTML into web page
  - Either self-contained
  - Or as link to external web server
- ‘Drive-by download’
  - As victim visits web site
  - Through application vulnerability
  - Or social engineering



KASPERSKY lab

Web-based attacks

- MPack
  - Exploit bundle created by Russian hackers
    - & sold to other hackers
  - PHP, JavaScript or VBS
  - Encrypted
    - To evade web AV programs
    - & make it hard to analyse
  - Browser & other vulnerabilities
  - Malicious script built into compromised web page
  - & executed automatically when victim visits page
- IcePack & WebAttacker



KASPERSKY lab

Stealth

- Packers
  - Utilities for encoding a program
  - Create a malicious program
  - Pack it
    - To conceal the code
  - Pack it several times
    - To make it even harder to find
  - Re-pack it
    - To create new variant(s)

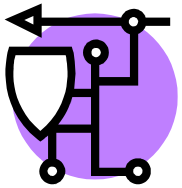
Stealth

- Rootkits
  - Replace legitimate libraries
  - Or install kernel module
  - Intercept system calls
  - & conceal Trojan [or spyware] activity
    - Installed files
    - Registry edits
    - Running processes
    - Network activity

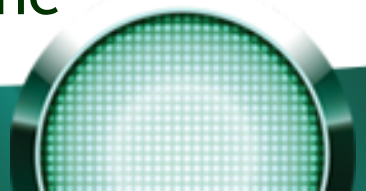
Polymorphism

- Hand-in-hand with web-based attacks
- Server-side polymorphism
- Code obfuscation
  - Multi-layer scripts
  - Periodically re-compile the code
    - Include junk instructions
    - At variable locations

Anti-anti-virus



- Malicious code self-defence techniques
  - Stop security processes
  - Delete security files
  - Block anti-virus updates
  - Lock files to prevent a scan
  - Suppress error messages
    - Or even auto-click ‘OK’
  - Sabotage sandbox analysis
- & even remove competing malware
  - Look for other malicious code & remove it
  - To ‘own’ the victim’s machine



Damage

- Subtle & insidious
  - No threat to computer up-time
  - Programs designed to make money illegally
    - Compromise security
    - Steal data
    - Hijack computer
  - It often goes undetected
  - So it’s harder to quantify

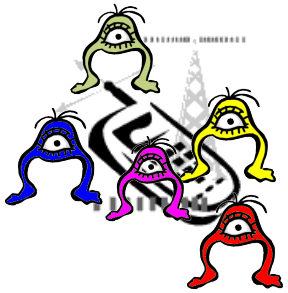
Future prospects

- Auto-generation of malware
  - & increase in volume of threats
- ‘Malware 2.0’
  - Hybrid threats
  - P2P botnets
    - Widespread distribution
    - Over a short period
    - Multiple variants with short ‘shelf-life’
  - Multiple distribution methods
  - ‘Anti-anti-virus’ self-protection techniques
  - Server-side polymorphism

Future prospects

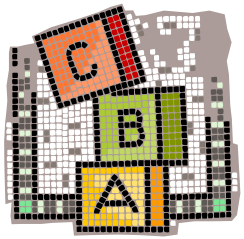
- Rootkits & ‘bootkits’
- Return of file viruses
  - Specifically targetting online games
- Continued use of exploits
  - ‘Drive-by downloads’
- Social networking attacks
  - Theft of login and passwords
  - ‘Web 2.0’ exploits

Future prospects



- Mobile threats
  - All the technical elements exist for mobile malware
    - Viruses, worms, Trojans, dialers
  - But not a major problem ... yet
  - Not yet a target for professional cyber criminals
  - ‘Critical mass’
    - Use for banking and other financial transactions
    - Connectivity
    - OS developments

‘upping the Anti-’



- From AV to Internet security
  - Signatures
    - First on-demand, then real-time
  - Statistical analysis & emulation
  - Heuristic analysis
  - Generic detection
  - Firewall & IDS
  - HIPS
  - Whitelisting
  - …

& finally ...

- Thank you for listening!
- If you need further information
  - david.emm@kasperskylab.co.uk
  - info@kasperskylab.co.uk
  - 0871 789 1631
  - http://www.kaspersky.co.uk/
  - http://www.viruslist.com/