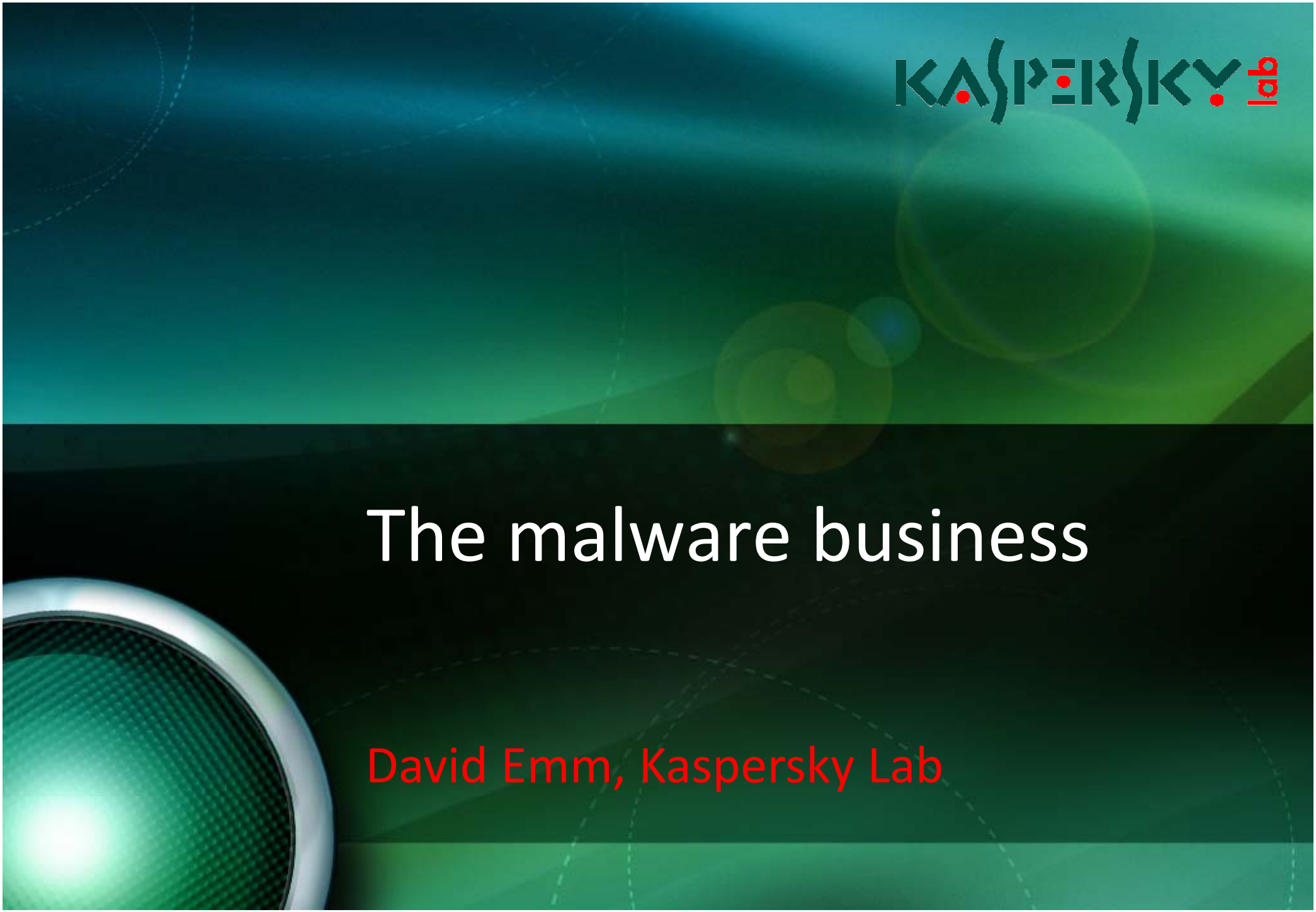



# The malware business

David Emm, Kaspersky Lab

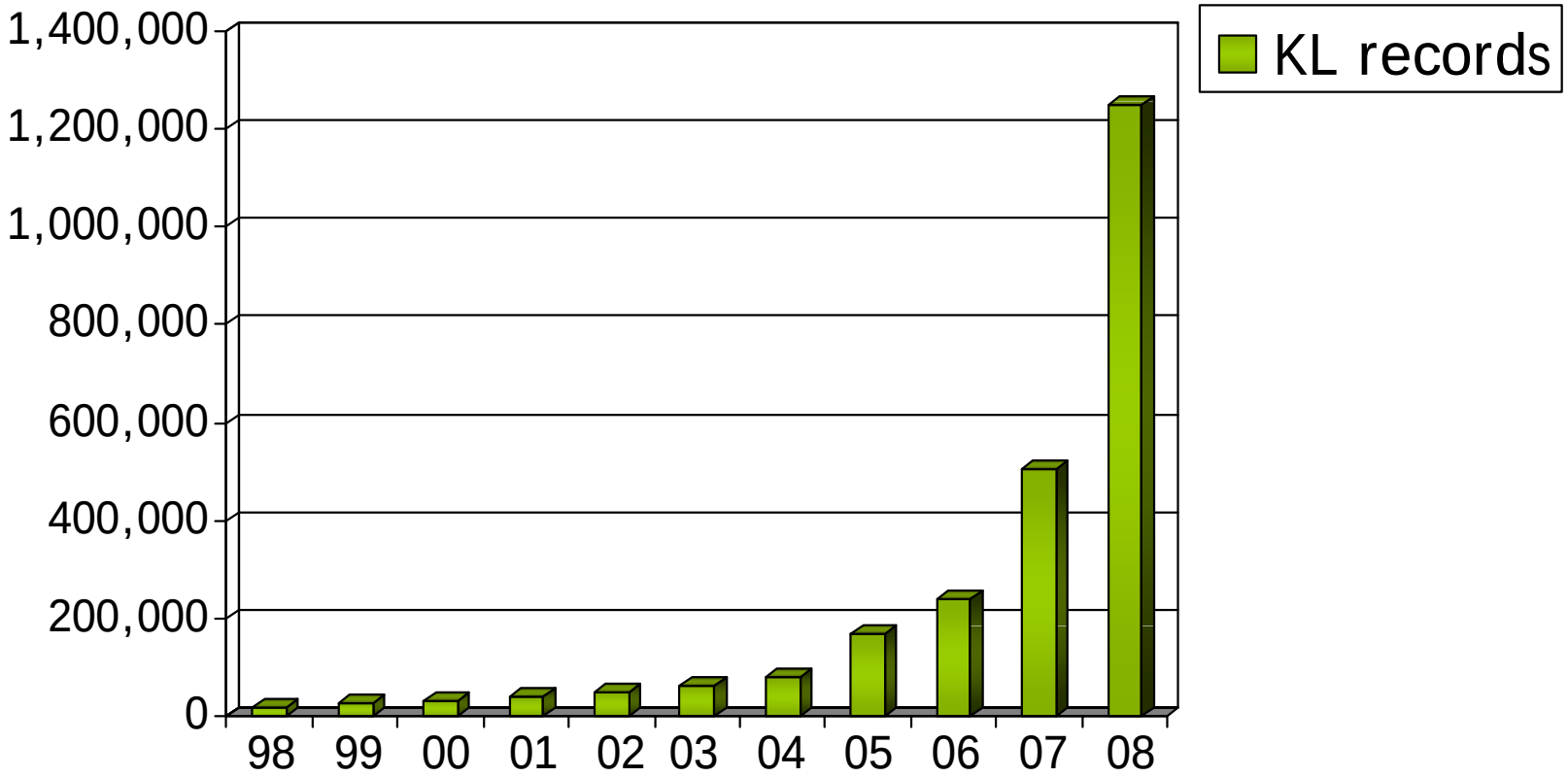
# From cyber vandalism to cyber crime

- Malware is profit-driven
  - ID theft & fraud
  - Extortion
  - Unsolicited advertising
  - Theft of virtual property
- Relies on computer up-time
  - ‘Own’ the victim’s machine
  - Capture the data

# The nature of the malware business

- It’s organised
  - i.e. crime that is organised
  - Rather than ‘organised crime’
- Economic interdependence
- Competition
- No centralised control by a ‘Dr No’ character
  - It mirrors the legitimate economy

# The scale of the problem




Source: Kaspersky Lab

# The scale of the problem

- It’s global
  - The Internet transcends geo-political borders
  - So do the cyber criminals
  - Unfortunately law enforcement doesn’t!
  - So cyber criminals can ‘hide between the cracks’

# ‘Operation Bot Roast’

Home | Site Map | FAQs

FEDERAL BUREAU OF INVESTIGATION

Celebrating a Century 1908-2008

SEARCH

**Contact Us**
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

**Learn About Us**
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

**Get Our News**
- Press Room
- E-mail Updates
- News Feeds

**Be Crime Smart**
- Wanted by the FBI
- More Protections

## Headline Archives

### OPERATION: BOT ROAST
### ‘Bot-herders’ Charged as Part of Initiative

06/13//07

They’re called “bot-herders:” hackers who install malicious software on computers through the Internet without the owners’ knowledge. Once the software is loaded, they can control the computer remotely. And once they’ve compromised enough computers, they have a robot network or botnet.

Some botnets are huge: tens of thousands of infected computers. Or more. As a result of Operation Bot Roast, an ongoing and coordinated initiative to disrupt and dismantle these bot-herders, we’ve identified about 1 million computers across the country that have been compromised.

The FBI has also charged numerous individuals with cyber crimes around the nation as a direct result of the coordinated operation, including:

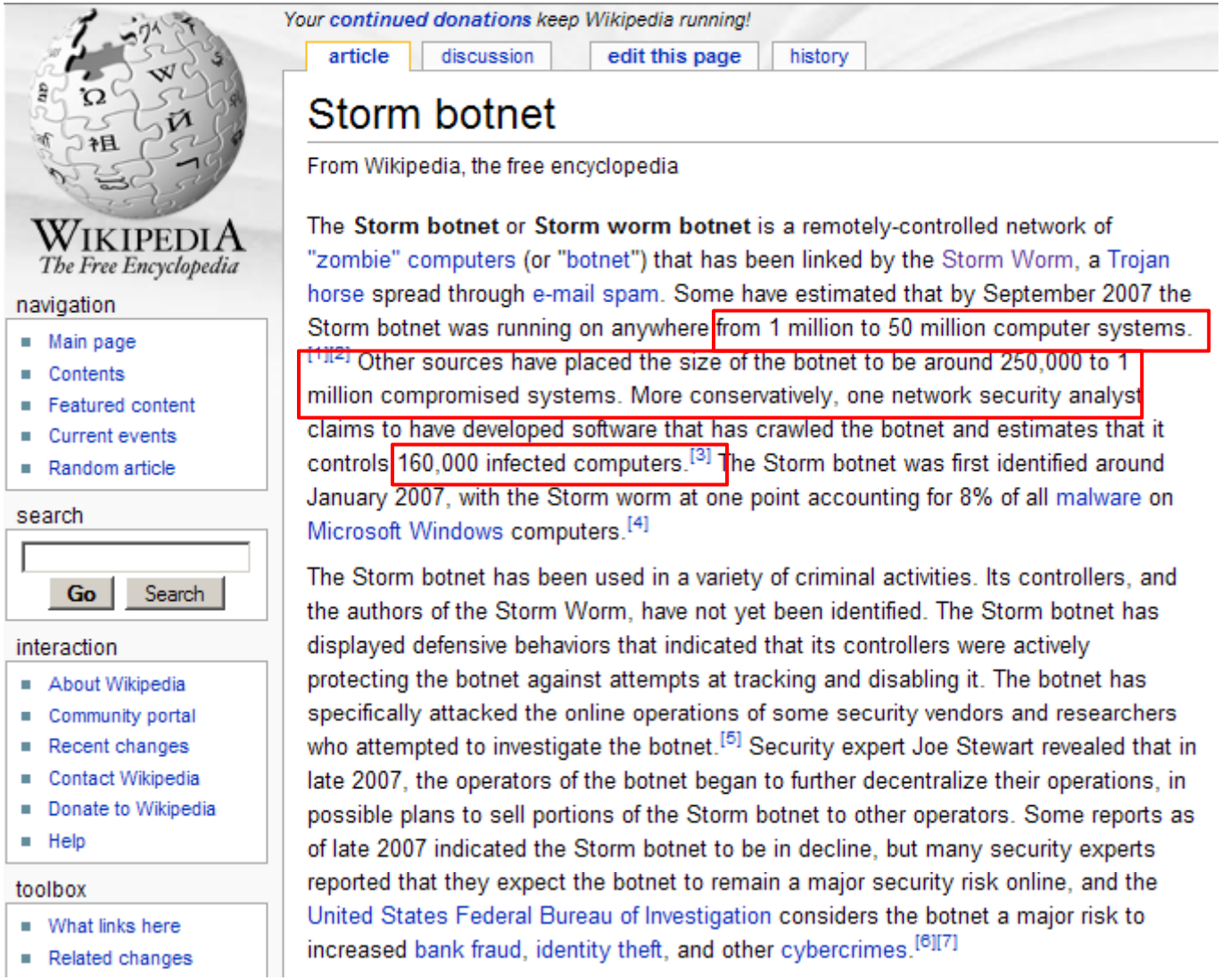
Headline Archives

Headline Story Index

**2008**
- September
- August
- July
- June
- May
- April
- March
- February
- January

**2007**
- December
- November
- October
- September
- August
- July
- June
- May
- April
- March
- February
- January

# Storm Worm



Your **continued donations** keep Wikipedia running!

article | discussion | edit this page | history

WIKIPEDIA
The Free Encyclopedia

navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

search
Go Search

interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

toolbox
- What links here
- Related changes

## Storm botnet

From Wikipedia, the free encyclopedia

The **Storm botnet** or **Storm worm botnet** is a remotely-controlled network of "zombie" computers (or "botnet") that has been linked by the Storm Worm, a Trojan horse spread through e-mail spam. Some have estimated that by September 2007 the Storm botnet was running on anywhere from 1 million to 50 million computer systems.[1][2] Other sources have placed the size of the botnet to be around 250,000 to 1 million compromised systems. More conservatively, one network security analyst claims to have developed software that has crawled the botnet and estimates that it controls 160,000 infected computers.[3] The Storm botnet was first identified around January 2007, with the Storm worm at one point accounting for 8% of all malware on Microsoft Windows computers.[4]

The Storm botnet has been used in a variety of criminal activities. Its controllers, and the authors of the Storm Worm, have not yet been identified. The Storm botnet has displayed defensive behaviors that indicated that its controllers were actively protecting the botnet against attempts at tracking and disabling it. The botnet has specifically attacked the online operations of some security vendors and researchers who attempted to investigate the botnet.[5] Security expert Joe Stewart revealed that in late 2007, the operators of the botnet began to further decentralize their operations, in possible plans to sell portions of the Storm botnet to other operators. Some reports as of late 2007 indicated the Storm botnet to be in decline, but many security experts reported that they expect the botnet to remain a major security risk online, and the United States Federal Bureau of Investigation considers the botnet a major risk to increased bank fraud, identity theft, and other cybercrimes.[6][7]

# Shadow botnet

## Analyst's Diary

### Taking down botnets

Roel August 06, 2008 | 19:57 GMT comment

Let's start with a few facts. Last week the Dutch police arrested a 19 year old Dutch man for selling a botnet to a Brazilian, who was also arrested. The 'Shadow' botnet is made up of around 100 000 infected machines.

However, the arrest isn't the end of the story. The Dutch police are working to help the victims. One of the steps they're taking is informing users that Kaspersky Lab websites include removal instructions (created at the request of the Dutch High Tech Crime Team) on how to get rid of the malware which transformed machines into bots.

The case raises a number of security questions which need to be discussed once the botnet has been dismantled. But in the meantime, if you think your computer might be part of the Shadow botnet, check it with an online scanner such as Kaspersky Online Scanner, and read the removal instructions we've posted here. The botnet does include machines from around the world, so you're not automatically safe just because you don't live in the Netherlands.

Do remember that the removal instructions only apply to the malware which has been used to create the botnet. These programs may have downloaded additonal malware to your machine, so make sure you also scan your computer with an up-to-date antivirus solution.

# Division of labour

- China
- Latin America
- Russia
- & there's specialisation
  - Gaming malware in China
  - Banking Trojans in Latin America
  - Botnets in Russia

# The nature of the threat

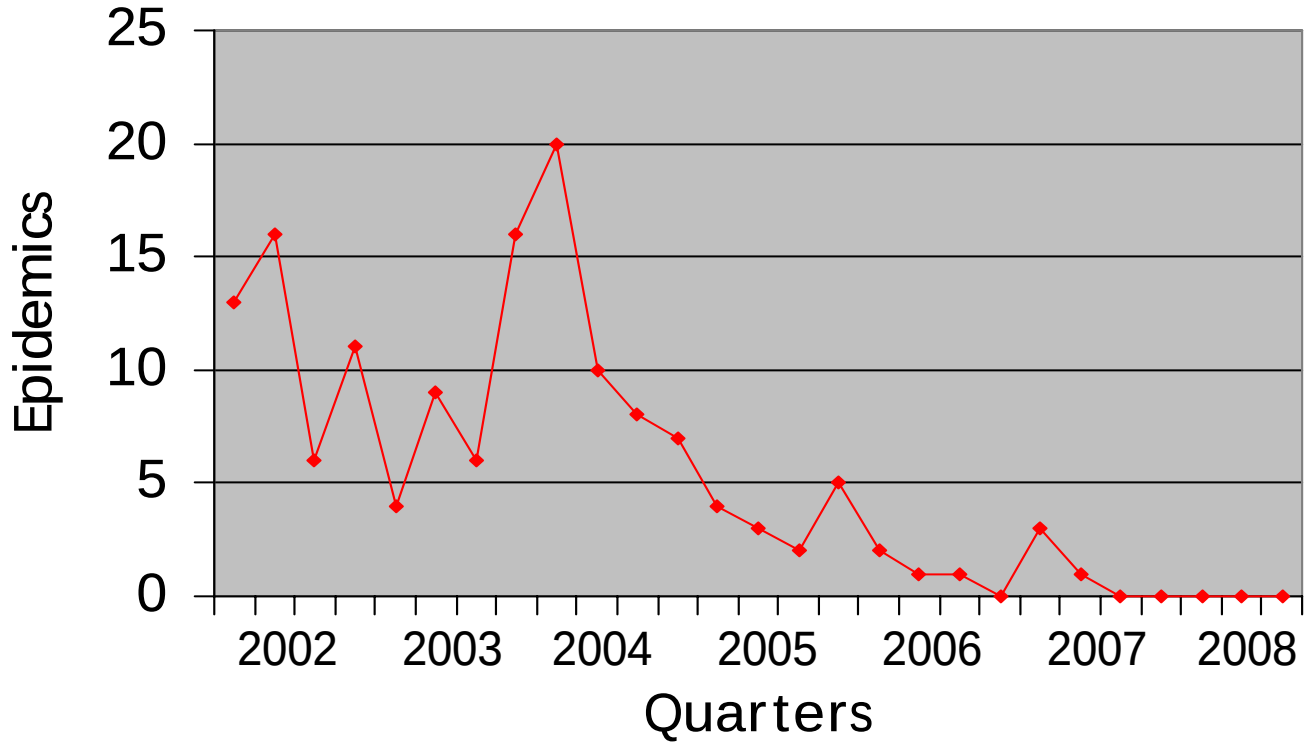
- Trojans, Trojans and more Trojans

| LATEST VIRUSES | Detection time |
|---|---|
| **24 September 2008** | |
| Backdoor.Win32.Rbot.ups | 09:50 |
| Backdoor.Win32.Hupigon.eani | 09:49 |
| Trojan-GameThief.Win32.OnLineGames.tkiw | 09:49 |
| Trojan-Downloader.Win32.Zlob.zow | 09:49 |
| Trojan.Win32.Buzus.yzi | 09:49 |
| Trojan.Win32.Sadenav.pj | 09:49 |
| Trojan.Win32.Monder.qdm | 09:48 |
| Backdoor.Win32.Hupigon.eanh | 09:48 |
| Trojan-GameThief.Win32.Magania.aeig | 09:48 |
| Backdoor.Win32.Hupigon.eang | 09:48 |

Source: Kaspersky Lab

# The nature of the threat

- Decline in global epidemics

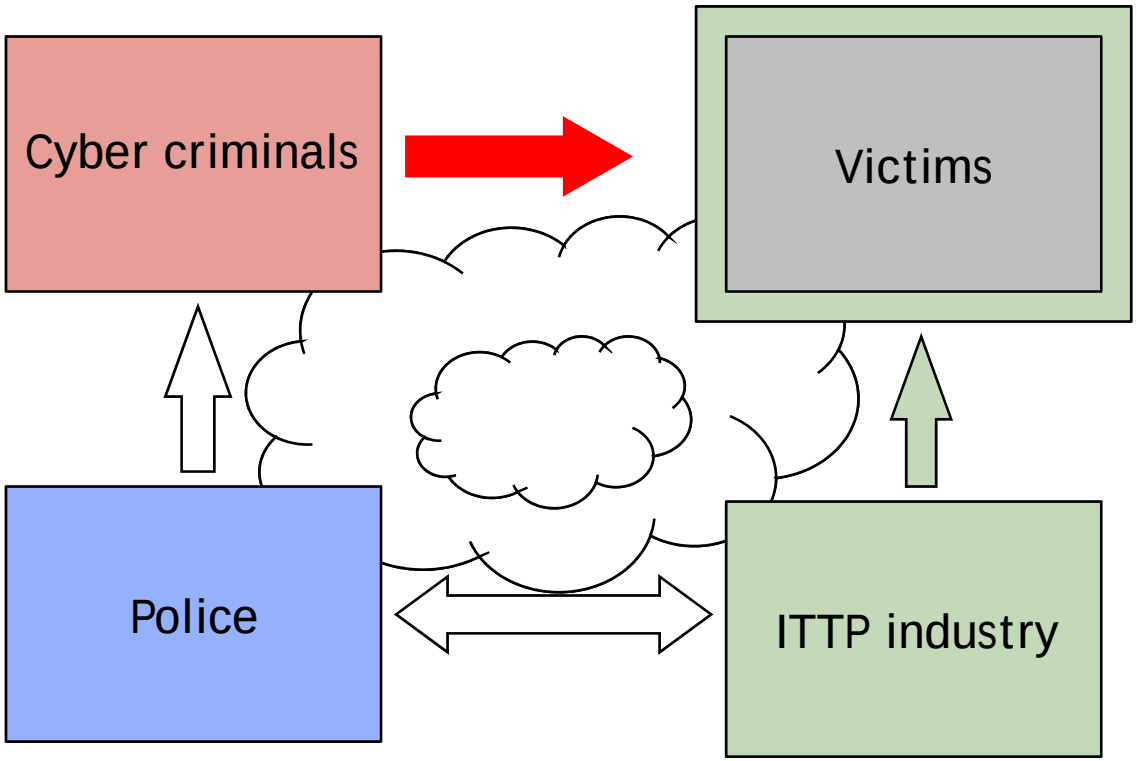



Source: Kaspersky Lab

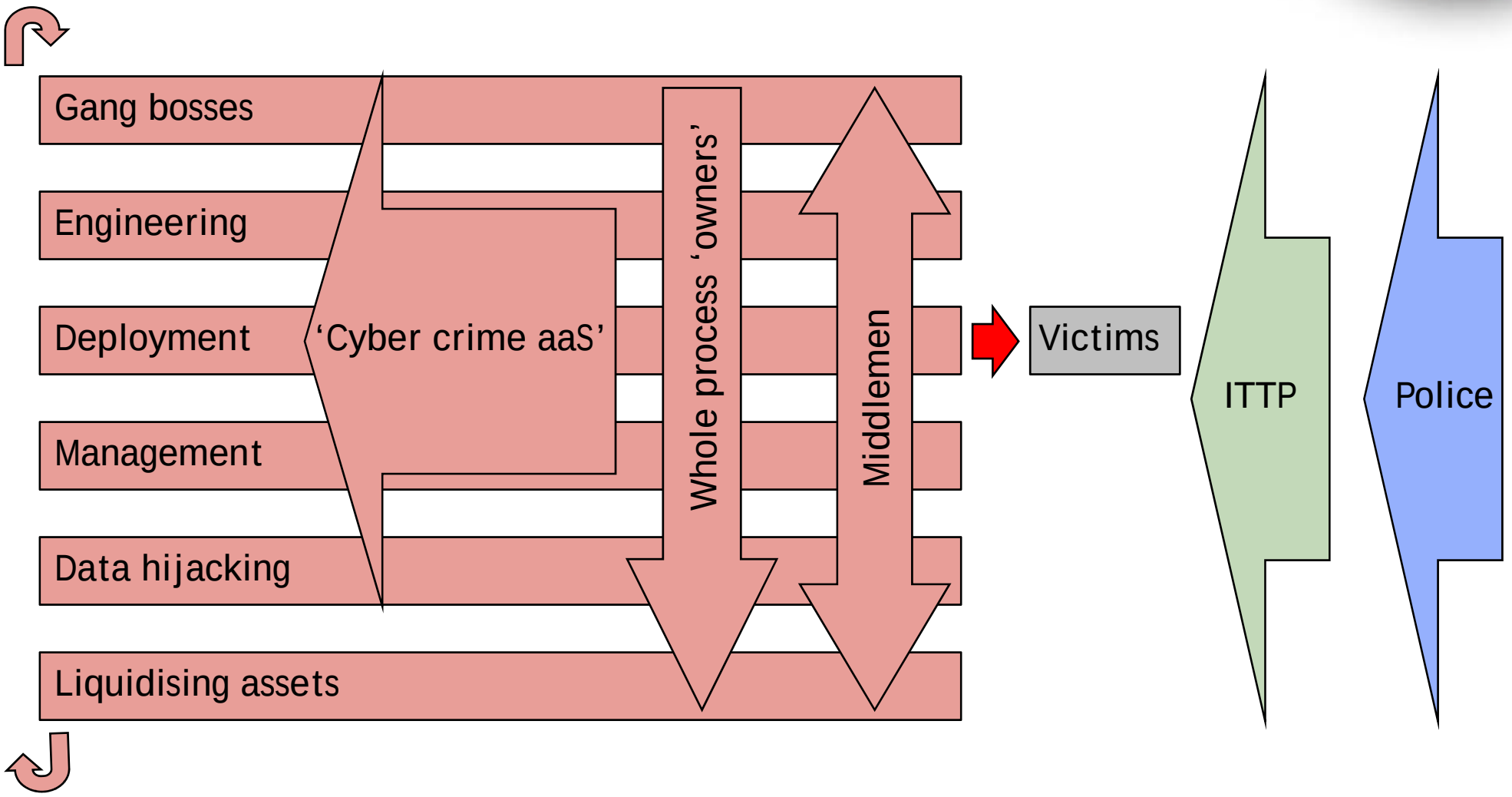
# The nature of the threat

- Cyber criminals:
- Use low-key small-scale attacks
  - Less visible to AV ‘early warning radar’
  - Less visible to law enforcement agencies
  - Easier to manage compromised computers
- Sabotage security defences
- & compete to ‘own’ victims

# The malware eco$ystem



# The malware eco$ystem



# Cyber criminals & their business

- Data theft
  - Bank account login credentials
  - Online game login credentials & virtual property
  - E-mail addresses
  - Personal data [e.g. credit card numbers]
  - Other data [e.g. IM accounts, software licences]
- Misuse of computer resources
  - Botnets
  - Client-server injection
  - SMS and telephone calls to premium services

# Malware engineering

- Development
  - Modern compilers [e.g. C++] and Assembler
    - To build executable files
  - Scripts, macro & other software
  - Simple & complex applications
  - Automatic code generation tools
- Self-defence
  - Compression & encryption
  - Obfuscation
  - Stealth
  - In-process injection

# Deployment & injection

- Deployment
  - E-mail attachments
  - Links
  - Auto-run worms
  - Direct attacks [insiders, removable media]
  - Trojan-Droppers & Trojan-Downloaders
- Injection
  - Click-and-execute
  - Software vulnerabilities

# Managing compromised computers

- Direct
  - Hacker connects to infected machine
  - Through a proxy or chain of proxies
- Indirect
  - Hacker uploads data to a server
  - Sends instructions to IRC
  - Initiates P2P data transfer
  - Infected machine connects to the server
  - Listens to IRC
  - Calls P2P ‘brothers’ for instructions

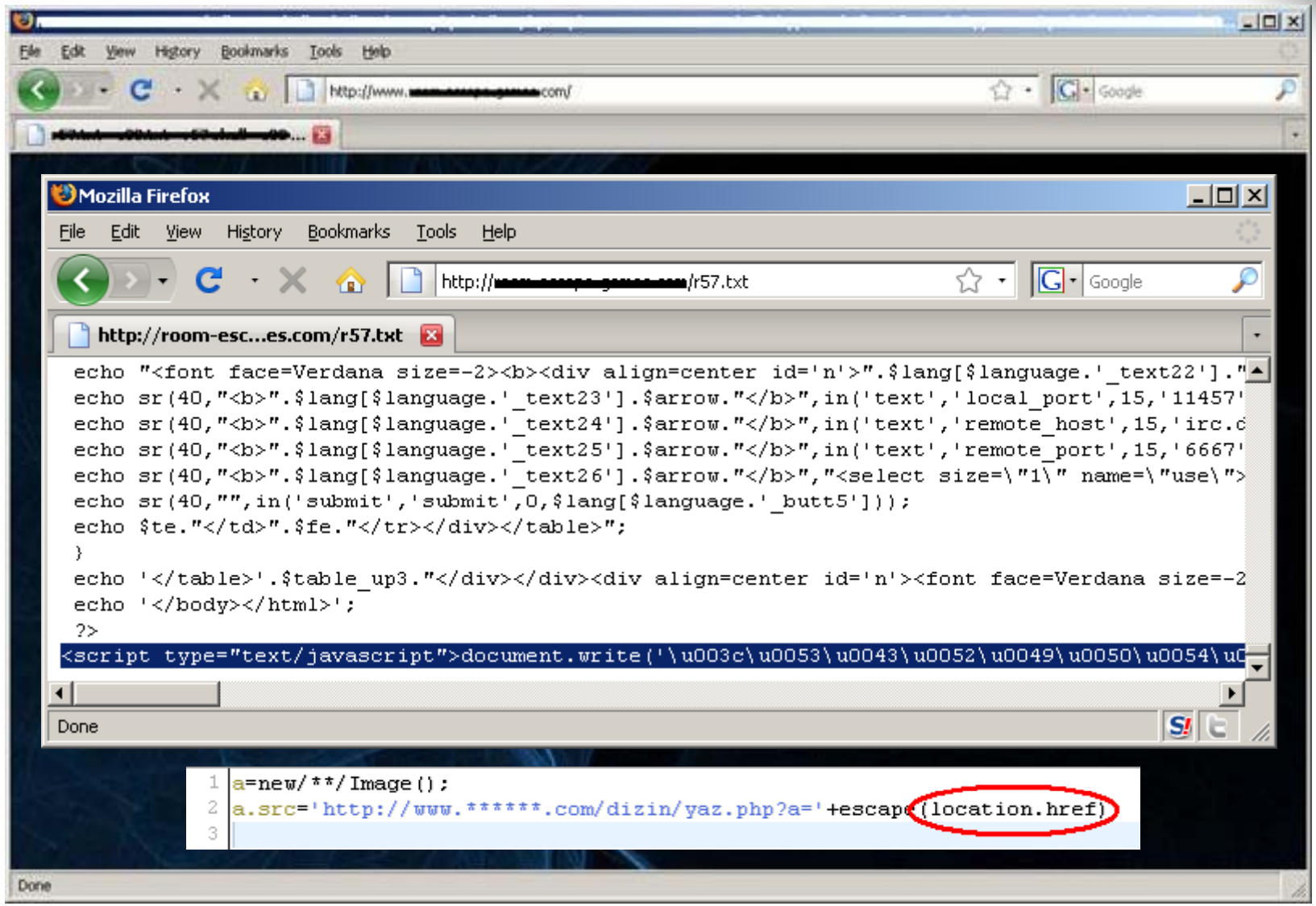
# Data hijacking

- Stored data
  - Parsing files on disk & extracting data
  - Extracting data from known files
  - Reading data from the registry
- Real-time data
  - Keylogging
  - Browsing history
- Phishing
- Extortion
  - Trojan-Ransom programs

# Victims

- Individuals
  - Stolen personal data
  - System overload
  - Internet capacity
- Businesses
  - Stolen money
  - Information leakage
  - DDoS
  - Reputation
- Government & military
  - Information leakage

# Hackers hacking hackers



# No honour among thieves

- Hackers hacking hackers
  - Web site hosting PHP shells
    - For breaking into vulnerable web sites
  - They contain obfuscated script
  - To capture URLs of vulnerable sites
- Phishers phishing phishers
  - Phishing kits
  - With scripts that also send them the captured data

# Liquidising assets

- Converting virtual assets into real money
- Direct theft
  - Cash from victim account into cyber criminal's account
    - Unsophisticated
    - Easy to investigate
- Use of money mules
  - Human proxies
- Sale of stolen assets
  - Credit cards, stolen e-mail addresses, etc.

# Wanted: money mules

**We are currently looking for freelance financial representatives in Europe and USA.**

We sell Apple products and supporting accessories in Europe and USA,
you have a possibility to become a freelance financial representative of our company in your country.

**Candidate requirements:**
- Location in **USA** or country of the **EUROPEAN UNION (Switzerland also accepted)**.
- **free 2-3 hours a day**;
- 21+ years old;
- Honest, responsible and prompt in operations;
- Have an adaptable, flexible and professional attitude;
- Polite, tactful;
- Have constant internet access for communication with our company via e-mail.

**This job will give you:**
- part-time employment;
- work from home;
- communication and business skills for working in other spheres of activity;
- possibility to combine this job with your full-time employment and own schedule;
- additionally, you will receive awards and bonuses for high-quality and accurate work.

So we hire people for **freelance work**. You can combine it with your full-time work.
The salary for private persons is 300 - 2500 EUR per week.
We have special offer for the companies also (earnings are 2000 - 5500 EUR per week ) .

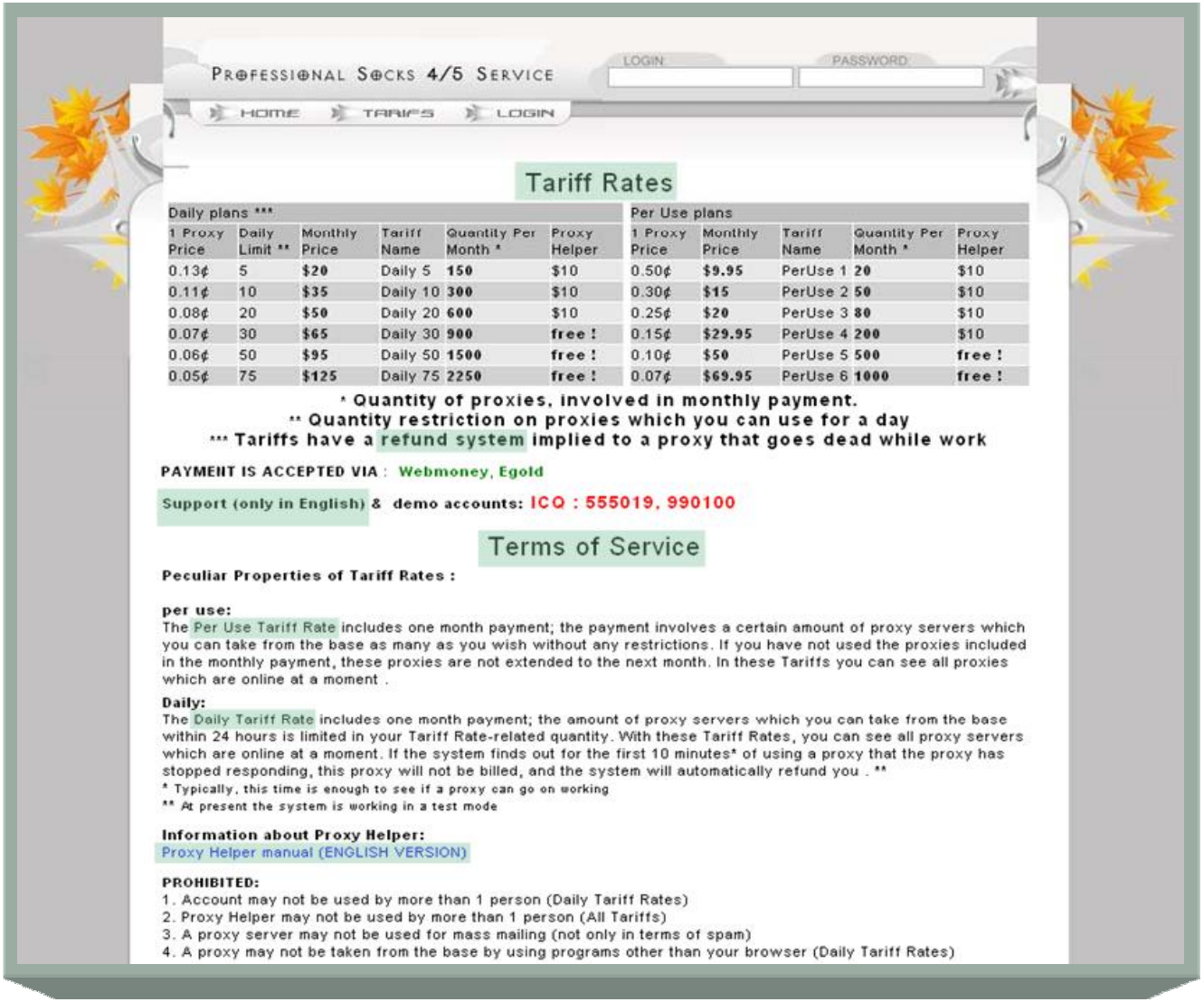
**If you have an interest to our proposition fill out this form please:**

FIRST NAME:
LAST NAME:
COUNTRY:
CITY:
AGE:
E-MAIL:
You are: private
Send

# Cyber Crime as a Service

- Malware development
  - Trojans & development kits
  - Obfuscation tools
  - Exploits
- Botnets
  - E-mail spam
  - Proxy networks
- Other features
  - Market in stolen data
  - Bullet-proof hosting
  - Cyber crime community forums

# Cyber Crime as a Service



PROFESSIONAL SOCKS 4/5 SERVICE

LOGIN PASSWORD

HOME TARIFS LOGIN

## Tariff Rates

| Daily plans *** | | | | | | Per Use plans | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 Proxy Price | Daily Limit ** | Monthly Price | Tariff Name | Quantity Per Month * | Proxy Helper | 1 Proxy Price | Monthly Price | Tariff Name | Quantity Per Month * | Proxy Helper |
| 0.13¢ | 5 | $20 | Daily 5 | 150 | $10 | 0.50¢ | $9.95 | PerUse 1 | 20 | $10 |
| 0.11¢ | 10 | $35 | Daily 10 | 300 | $10 | 0.30¢ | $15 | PerUse 2 | 50 | $10 |
| 0.08¢ | 20 | $50 | Daily 20 | 600 | $10 | 0.25¢ | $20 | PerUse 3 | 80 | $10 |
| 0.07¢ | 30 | $65 | Daily 30 | 900 | free ! | 0.15¢ | $29.95 | PerUse 4 | 200 | $10 |
| 0.06¢ | 50 | $95 | Daily 50 | 1500 | free ! | 0.10¢ | $50 | PerUse 5 | 500 | free ! |
| 0.05¢ | 75 | $125 | Daily 75 | 2250 | free ! | 0.07¢ | $69.95 | PerUse 6 | 1000 | free ! |

* Quantity of proxies, involved in monthly payment.
** Quantity restriction on proxies which you can use for a day
*** Tariffs have a refund system implied to a proxy that goes dead while work

PAYMENT IS ACCEPTED VIA : Webmoney, Egold

Support (only in English) & demo accounts: ICQ : 555019, 990100

## Terms of Service

**Peculiar Properties of Tariff Rates :**

**per use:**
The Per Use Tariff Rate includes one month payment; the payment involves a certain amount of proxy servers which you can take from the base as many as you wish without any restrictions. If you have not used the proxies included in the monthly payment, these proxies are not extended to the next month. In these Tariffs you can see all proxies which are online at a moment .

**Daily:**
The Daily Tariff Rate includes one month payment; the amount of proxy servers which you can take from the base within 24 hours is limited in your Tariff Rate-related quantity. With these Tariff Rates, you can see all proxy servers which are online at a moment. If the system finds out for the first 10 minutes* of using a proxy that the proxy has stopped responding, this proxy will not be billed, and the system will automatically refund you . **
* Typically, this time is enough to see if a proxy can go on working
** At present the system is working in a test mode

**Information about Proxy Helper:**
Proxy Helper manual (ENGLISH VERSION)

**PROHIBITED:**
1. Account may not be used by more than 1 person (Daily Tariff Rates)
2. Proxy Helper may not be used by more than 1 person (All Tariffs)
3. A proxy server may not be used for mass mailing (not only in terms of spam)
4. A proxy may not be taken from the base by using programs other than your browser (Daily Tariff Rates)

# Cyber Crime as a Service

| 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<br>0% |
| Opera | 1<br>0% |

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

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

# Politically motivated attacks

- Estonia
  - May 2007
- Astrakhan & Krasnodar
  - Summer 2007
- Marshall Islands
  - June 2008
- Georgia
  - August 2008

# Addressing the problem

- Crime isn’t going away
  - Nor is cyber crime
- Mitigating the risks
  - Security technologies
  - Law enforcement
  - The human factor


KASPERSKY lab
Thank you !
david.emm@kaspersky.co.uk