ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Cybercrime Operations + Web 2.0 Threats

Kaderforum des Polizeidepartements der Stadt Zürich

Dr. sc. ETH Stefan Frei
Andreas Reichmuth

# About

- Stefan Frei, Dr. sc. ETH
  - Dozent & Senior Research Associate, ETH Zurich

- Brief Bio
  - been in IT security for more than a decade
  - worked for international penetration testing and R&D teams in industry and academia
  - member of the IBM ISS X-Force attack team
  - frequent speaker at security conferences like BlackHat, DefCon
  - recognized cybercrime expert in industry and media

# Outline

- Cybercrime - from amateurs to organized crime
- Tools and services of the trade
- Life Malware Demonstration

- Web 2.0 - Understanding the threat
- How Web 2.0 change things
- Cyber Protesting

- Defense

Acknowledgments to Gunter Ollmann, Damballa

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Evolution of Cybercrime

There is no security on this earth, only opportunity
*Douglas MacArthur (1880-1964)*

# The Environment

- world Internet usage has grown 362% to an estimated 1.6 billion users since 2000
- networking has evolved from dedicated point to point connections to ubiquitous communication between people, platforms, and applications
- vulnerabilities in applications and devices are now exposed and accessible globally
- number of targets, revenue per target and type of exploitation has also evolved rapidly

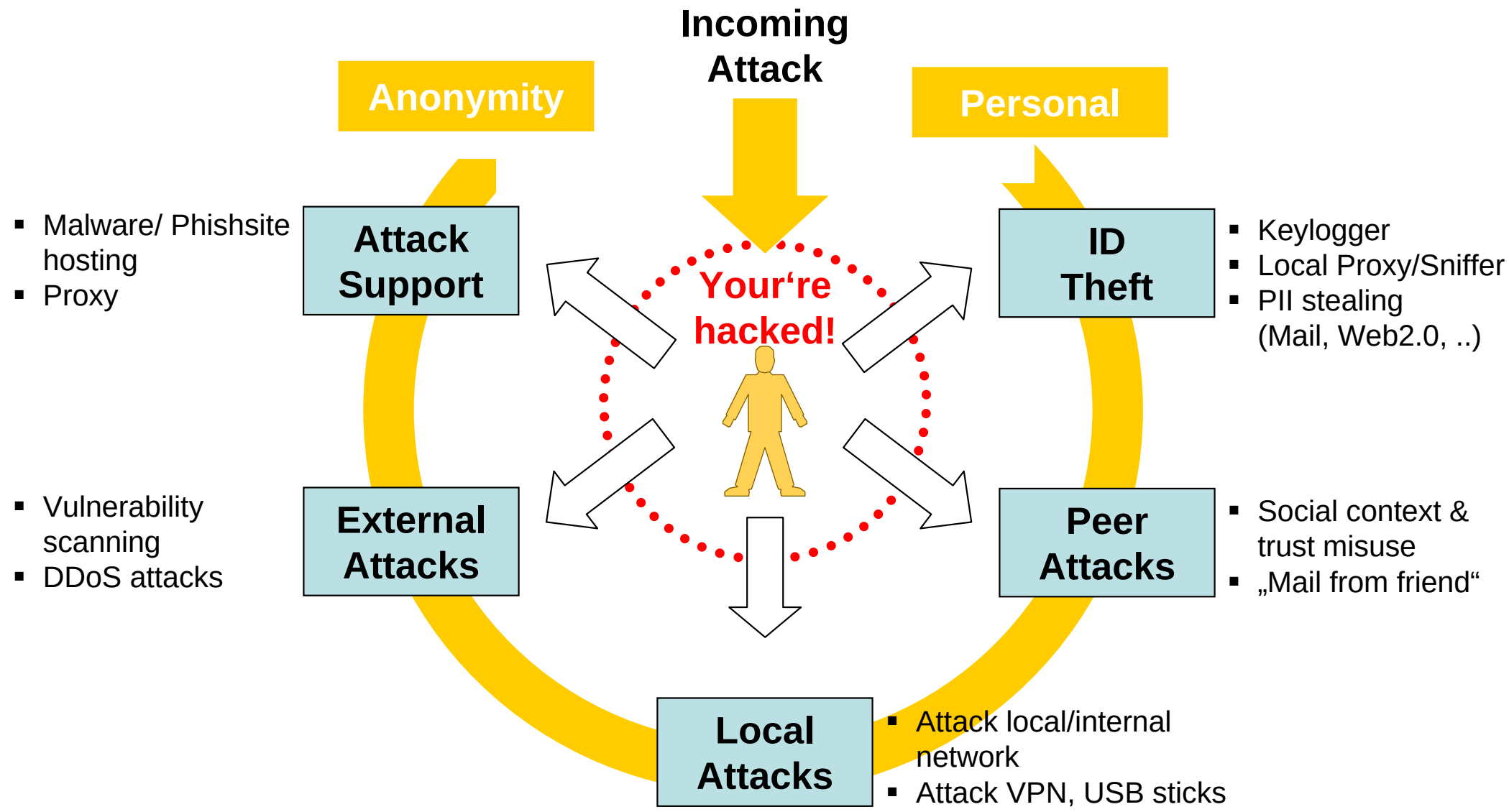
# Cybercrime

- Organized crime
  - .. is primarily about the pursuit of profit
  - .. the continuation of business by criminal means
  - .. tend to be exceptionally good at identifying and seizing opportunities for new illegal enterprises and activities
- The Internet and the continuing growth of electronic commerce offer enormous new prospects for illicit profits

# Cybercrime - a professional endeavor

- Specialization of the development
  - .. of malware & tools, acquisition of targets, localization, distribution, controlling of botnets, laundering the money
  - by experts in the respective field
- Division of Labor
  - leads to the availability of formidable tools and services in support of the criminals
  - competition among actors has contributed to a considerable drop in the price of malware, and in the availability of advanced customer care and services

# You‘re 0wned - what‘s next?




**PII** = Personally identifiable information

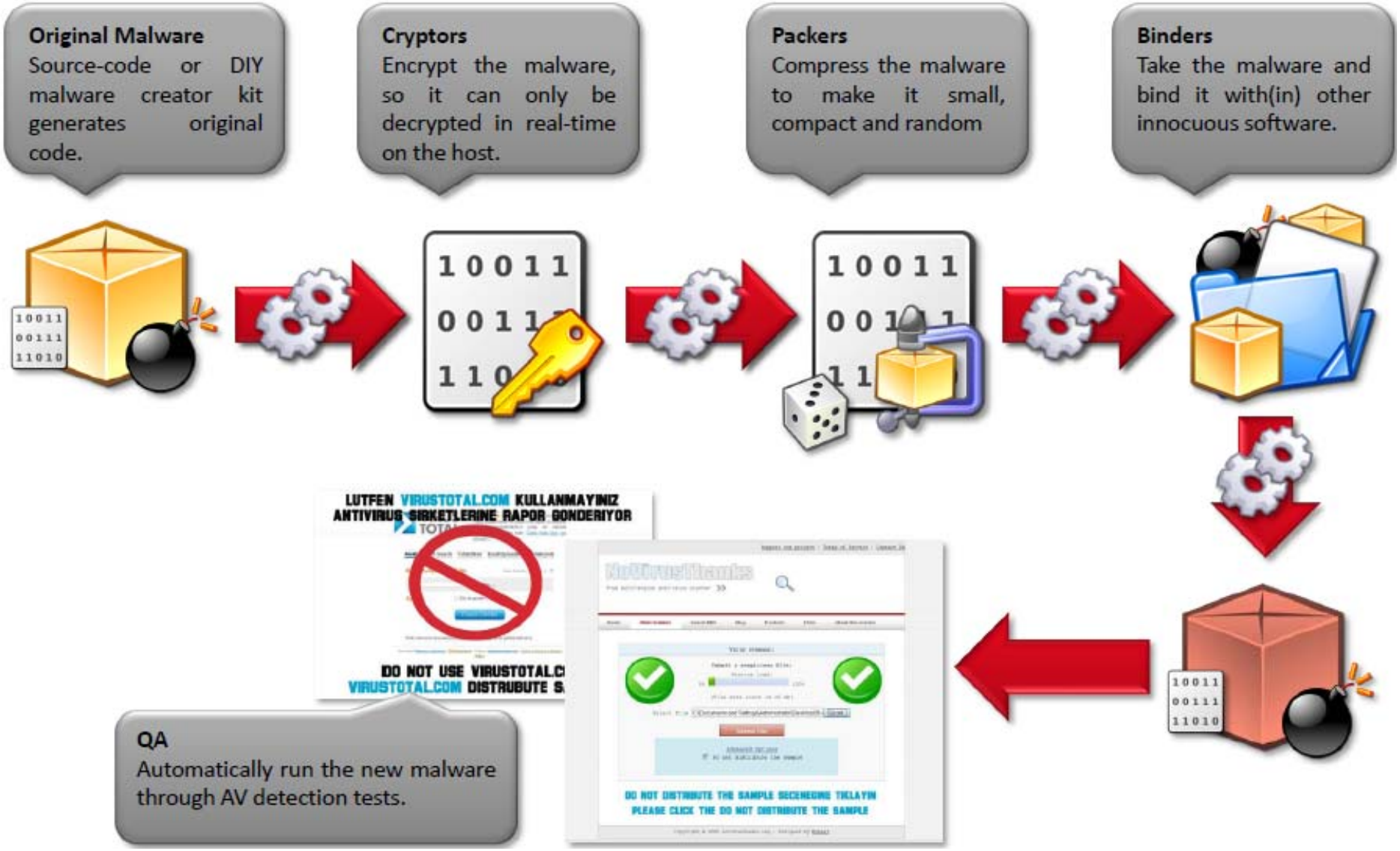
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# The right tools for the job

# Malware Development Lifecycle

1. Malware construction
   - source code or do-it-yourself malware kits
2. Malware distribution
   - turn malware into self-spreading worm
3. Malware reverse engineering protection
   - protect your investment - against analysis and copycats
4. Malware detection evasion
   - ensure your malware bypassed antivirus et al.

# Malware Development Lifecycle




Source: http://www.damballa.com/downloads/r_pubs/WP_SerialVariantEvasionTactics.pdf

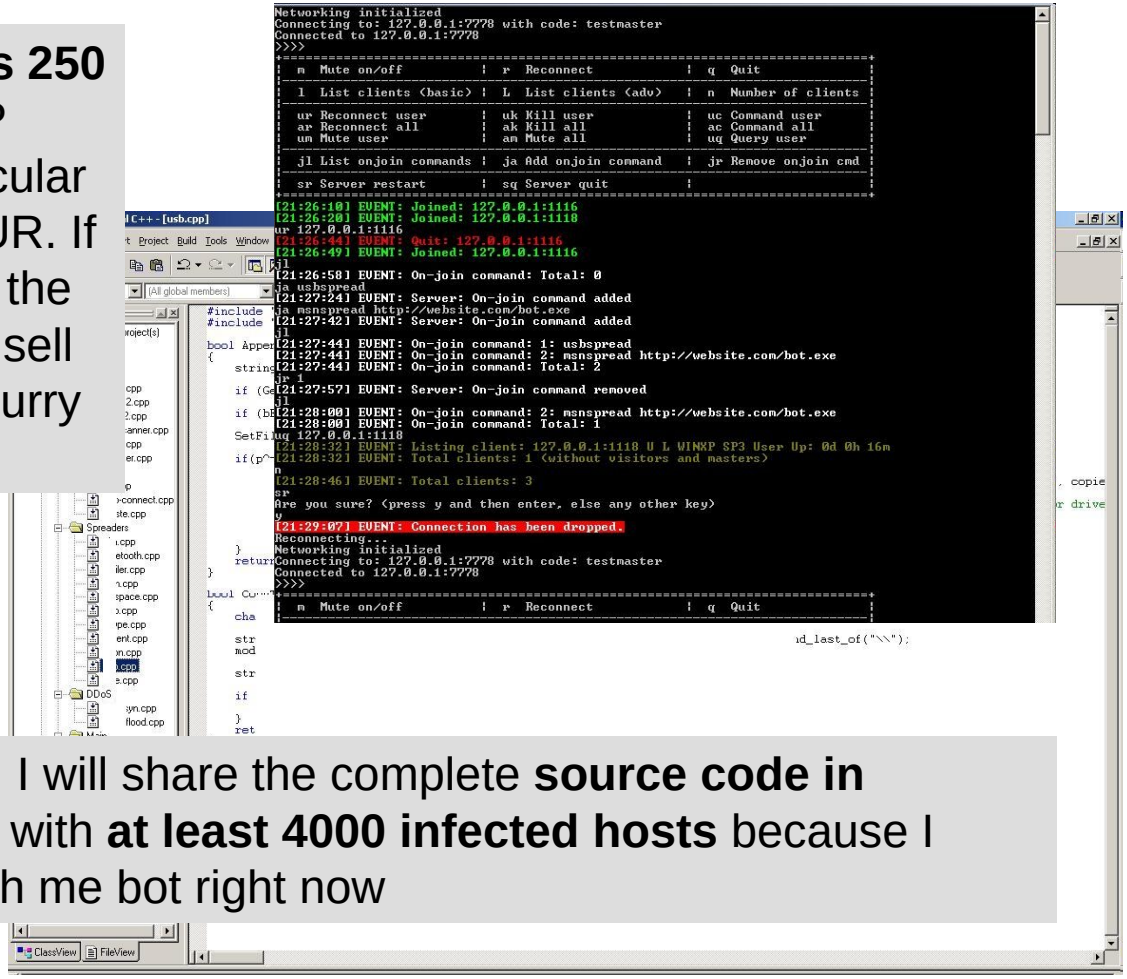
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# 1. Malware Construction

# Will code malware for financial incentives

- “Malware coding for hire" propositions

**Starting price for my malware is 250 EUR.** Additional modules like P2P features, **source code** for a particular module go for an additional 50 EUR. If you're paying in another currency the price is 200 GBP or 395 dollars. I sell only ten copies of the builder so hurry up




I can also offer you **another deal**, I will share the complete **source code in exchange to access to a botnet** with **at least 4000 infected hosts** because I don't have time to play around with me bot right now

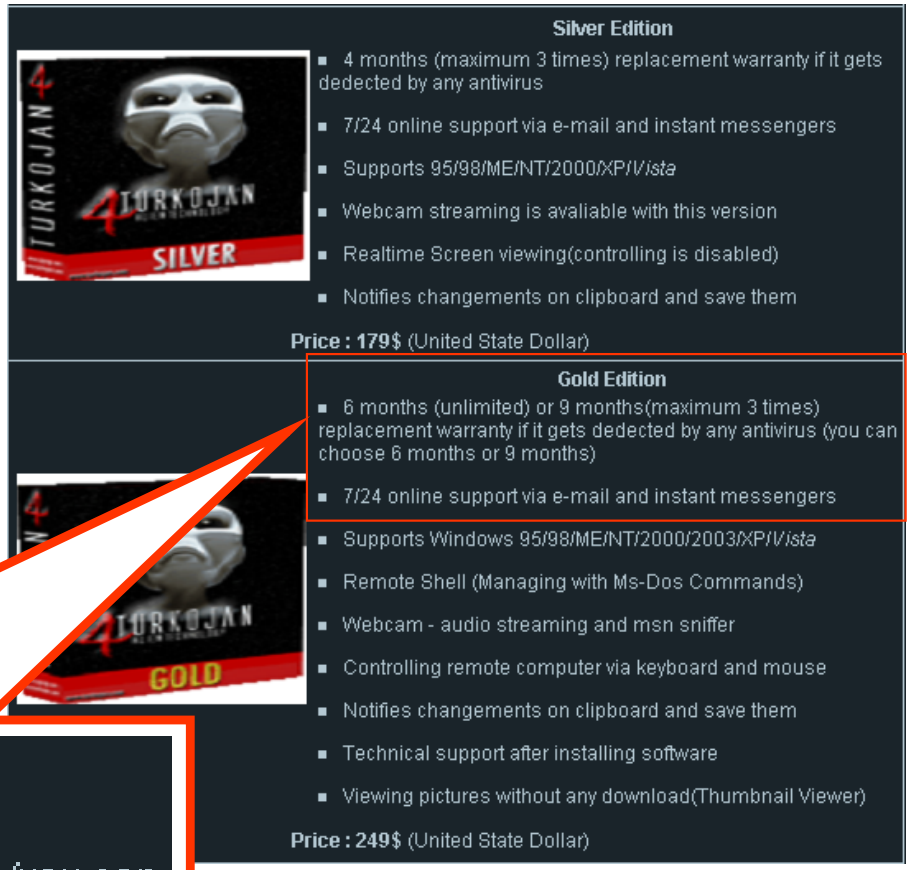
Source: http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html

# Do-It-Yourself Malware Kits

- Constructor kit features
  - Trojan constructor
  - remote desktop
  - webcam & audio streaming
  - remote password & registration key retrieval
  - remote shell
  - advanced file manager
  - online / offline key logger
  - updates by plug-in uploads
  - etc..

# Remote Administration Kit (RAT)

- Gold Edition
  - 7/24 online support
  - replacement warranty if tool gets detected by any antivirus
  - for USD 249.-




**Gold Edition**

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

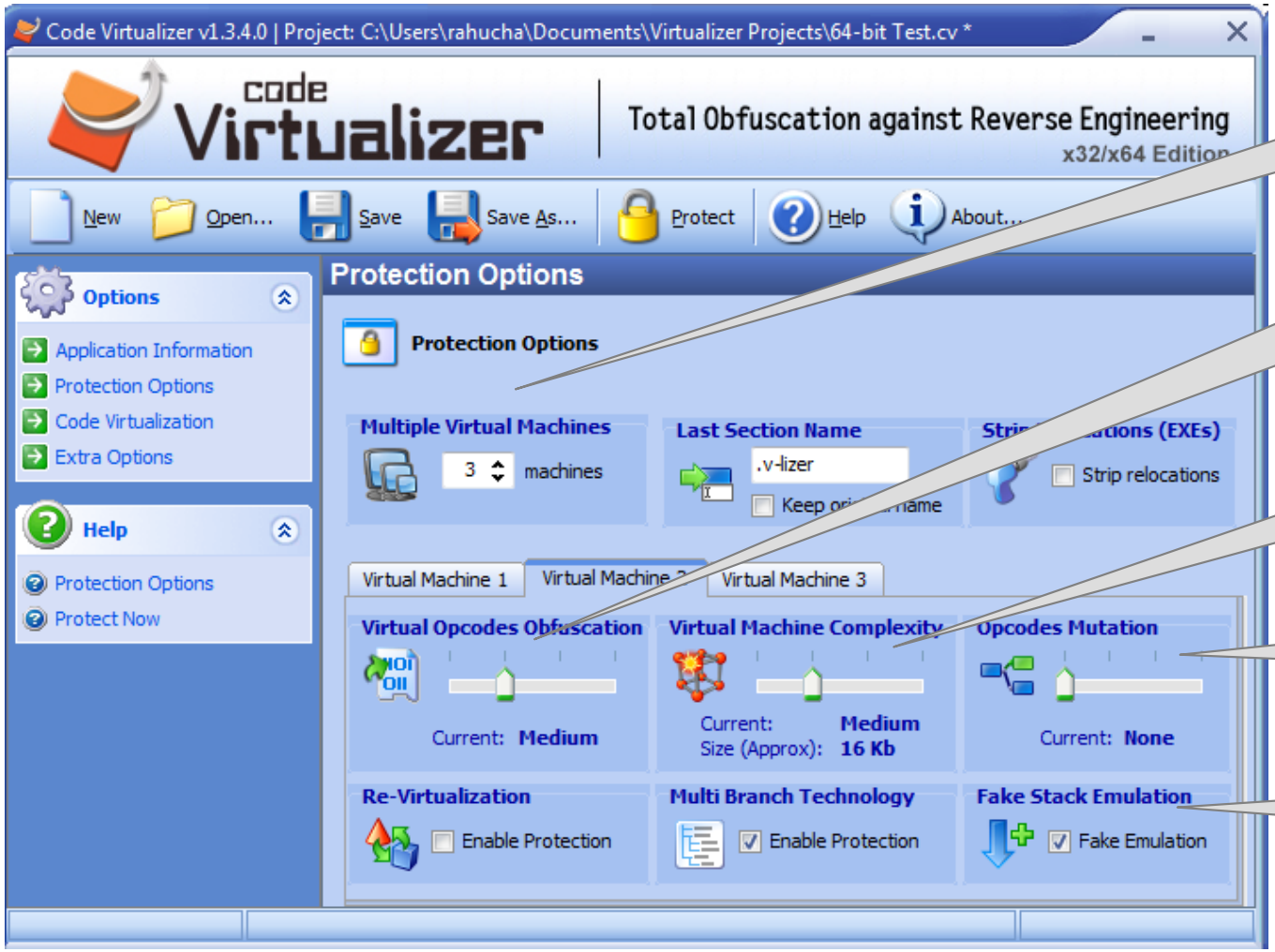
# 2. Malware Protection

# Protect your investment

- Anti debugging tools
  - powerful code-obfuscation systems help developers protect their sensitive code areas against reverse engineering

- Code Virtualizer
  - protects your sensitive code areas in any x32 and x64 native PE files
  - protects executable files/EXEs, system services, DLLs, OCXs , ActiveX controls, screen savers and device drivers)
  - commercial tool

# Obfuscation options




# of virtual machines

Level of obfuscation

Complexity of virtual machines

Number of mutations

Fake stack emulation

Source: http://www.oreans.com/index.php

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# 3. Malware Distribution

# Turn any executable into a worm

- TrojanToWorm T2W
  - gives programmers an easy user interface to turn any executable file into a worm
  - let's you turn `notepad.exe` into a self spreading worm
  - design a worm with different functionalities by just checking different flags
    - as compress it with UPX
    - select expiration time and spreading methods

# Do-it-yourself Worm

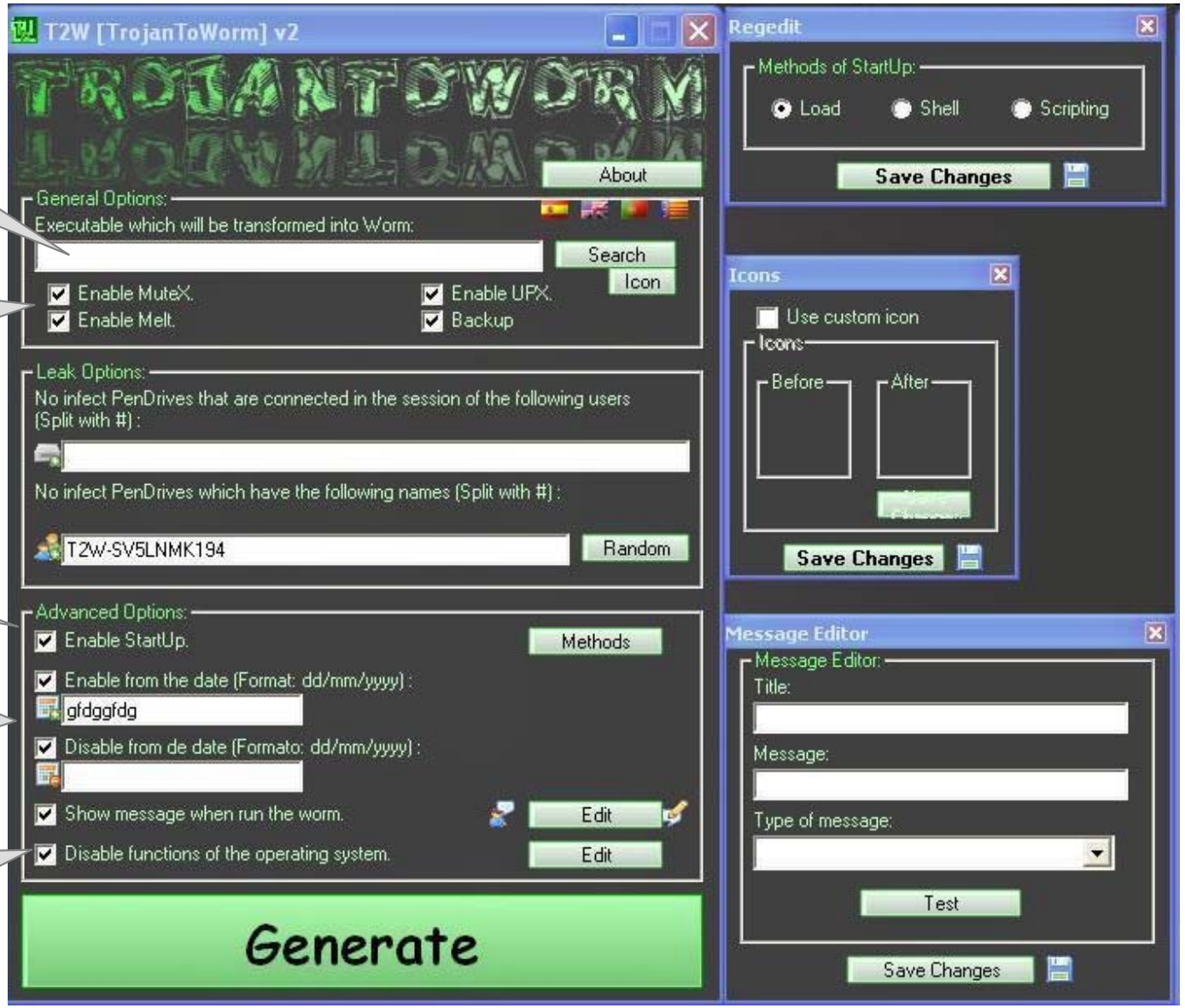
Executable to be turned into a worm

Flags to compress it, create mutex, ..

Enable auto-start?

Activity start- and end-date

Disable unwanted OS functions



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# 4. Antivirus Evasion

# Underground antivirus testing tools

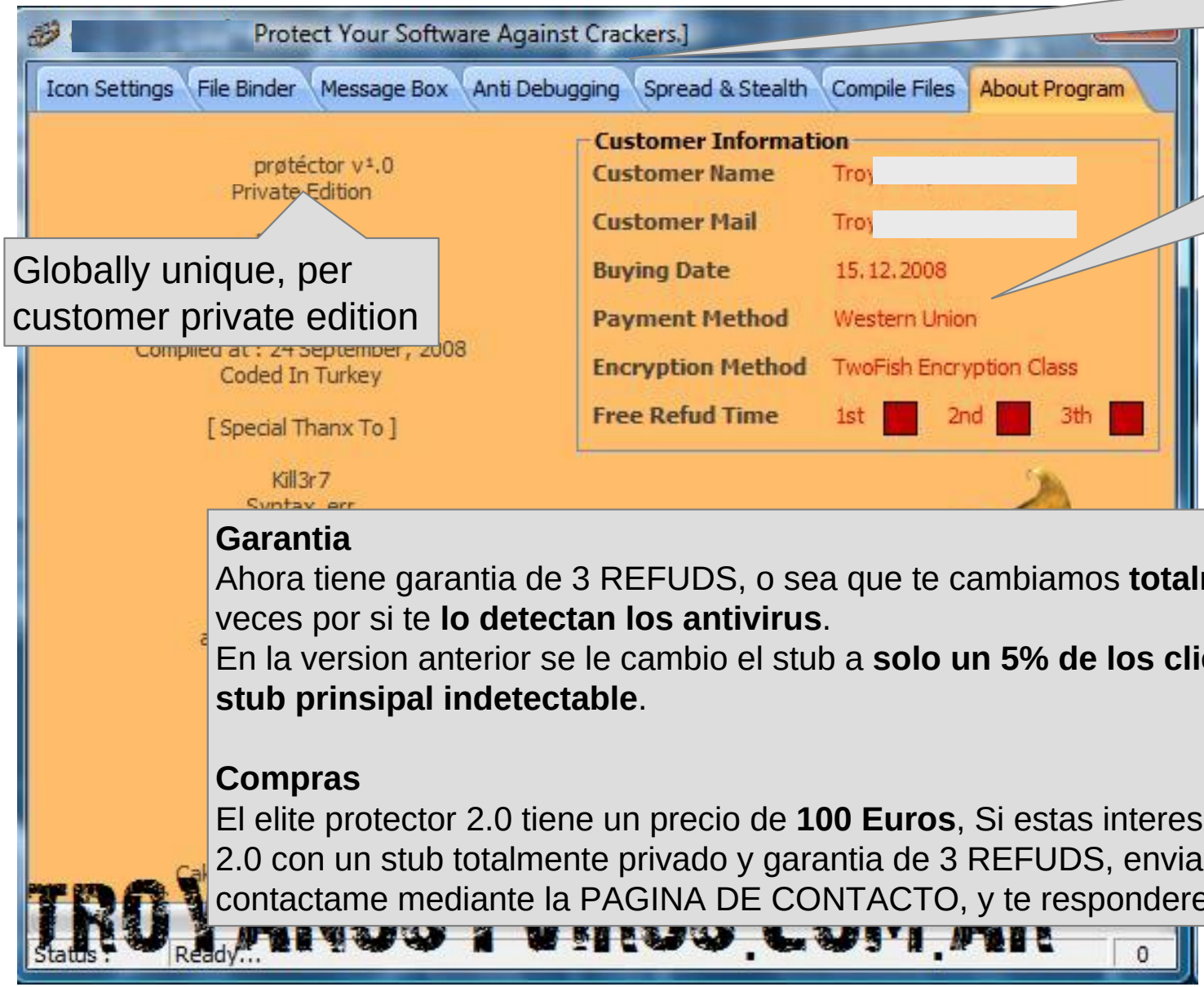

Source: http://pandalabs.pandasecurity.com/archive/Multi-AVs-Scanners.aspx

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# All-In-One
# Malware Construction Kits

# Handy All-In-One Tools

All you need, Binder, Anti Debugging, Spread & Stealth, ...



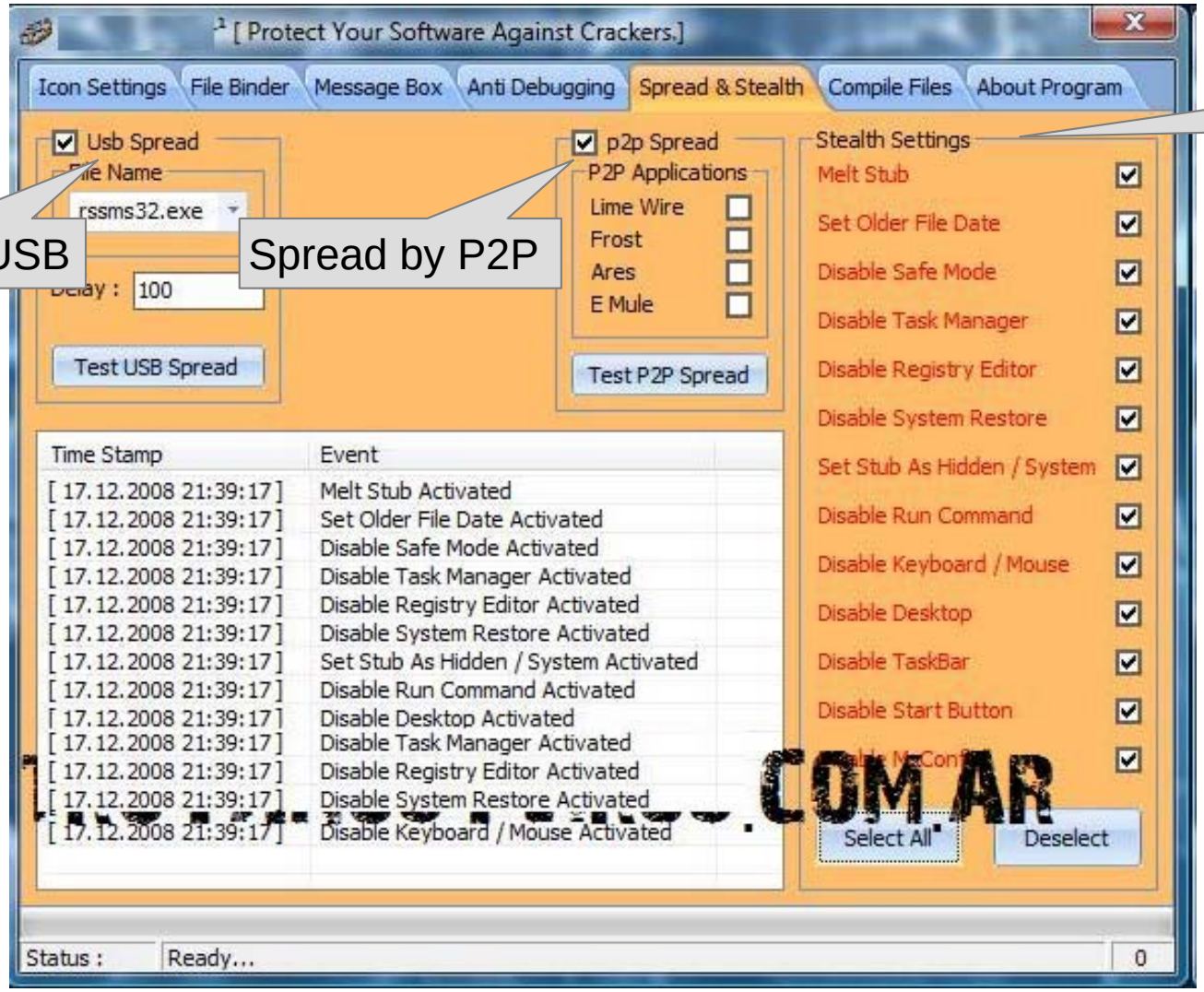

Globally unique, per customer private edition

Customer information, payment method, number of refunds, ...

**Garantia**
Ahora tiene garantia de 3 REFUDS, o sea que te cambiamos **totalmente gratis** tu stub hasta 3 veces por si te **lo detectan los antivirus**.
En la version anterior se le cambio el stub a **solo un 5% de los clientes**, El resto siguen con su **stub prinsipal indetectable**.

**Compras**
El elite protector 2.0 tiene un precio de **100 Euros**, Si estas interesado en comprar ### Protector 2.0 con un stub totalmente privado y garantia de 3 REFUDS, envia un mail a ####@gmail.com o contactame mediante la PAGINA DE CONTACTO, y te respondere a la brevedad.

# Spread and Stealth



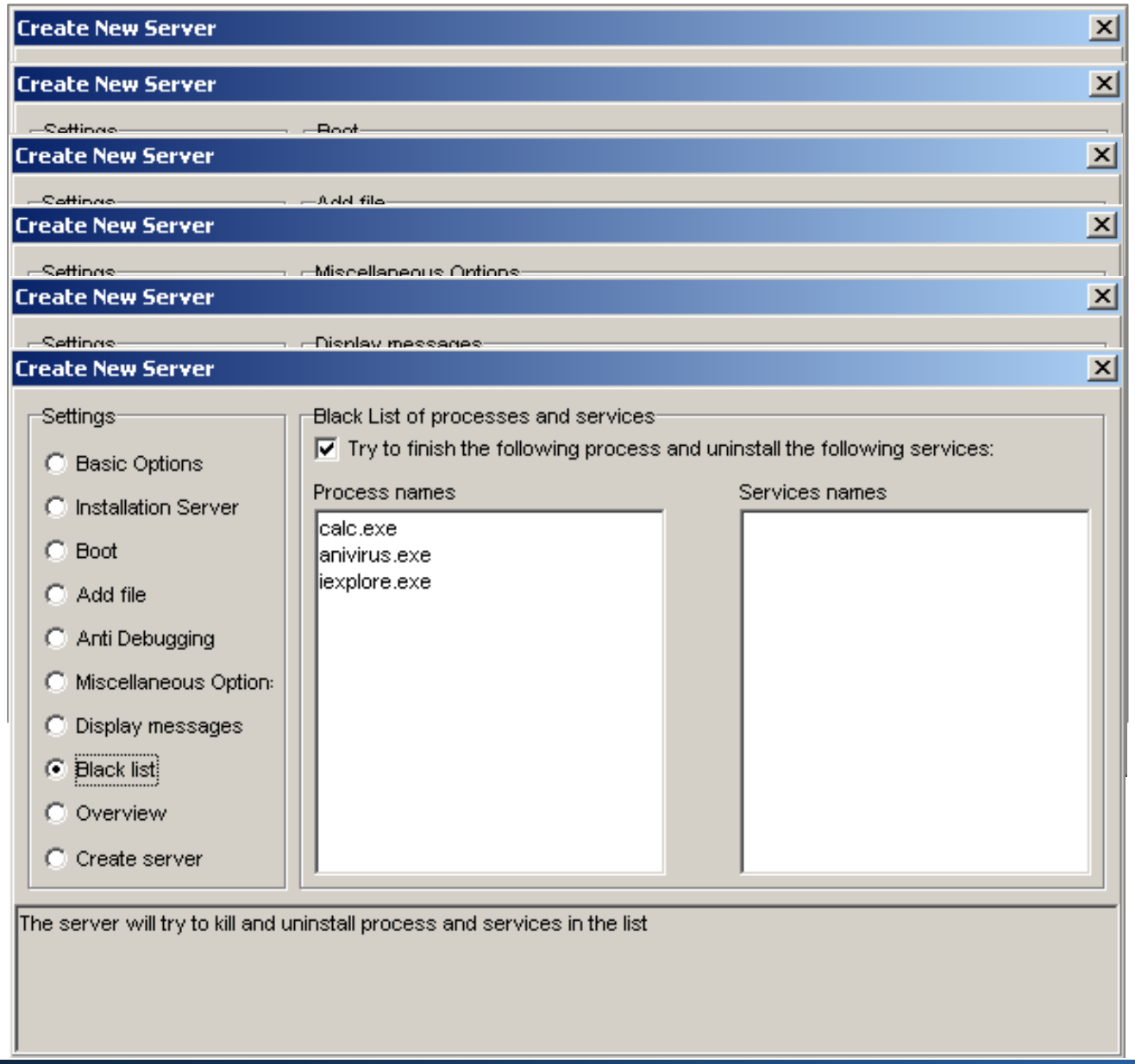
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Live Demonstration
# Trojan DIY Construction Kit

# Demonstration - Menu du jour

- Build trojan
  - build trojan with customized functionality
  - hide it in the Minesweeper game
  - remotely control infected host(s)
- Code Crypter
  - obfuscate/crypt Minesweeper worm
  - check antivirus detection rate

# Create a new trojan/server




where to find the command & control host

define startup options

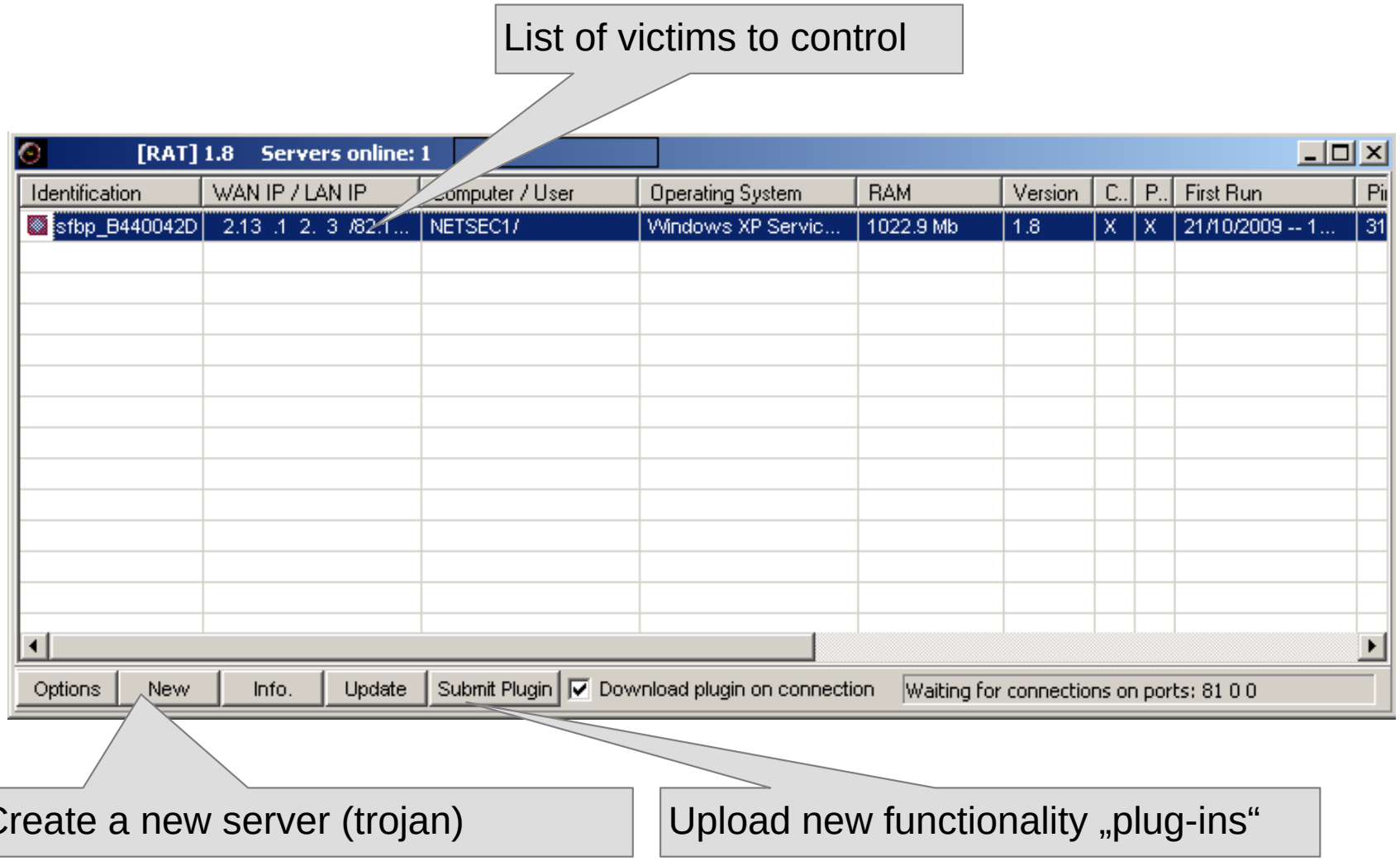
select program(s) to hide the Trojan in

key logger - yes please

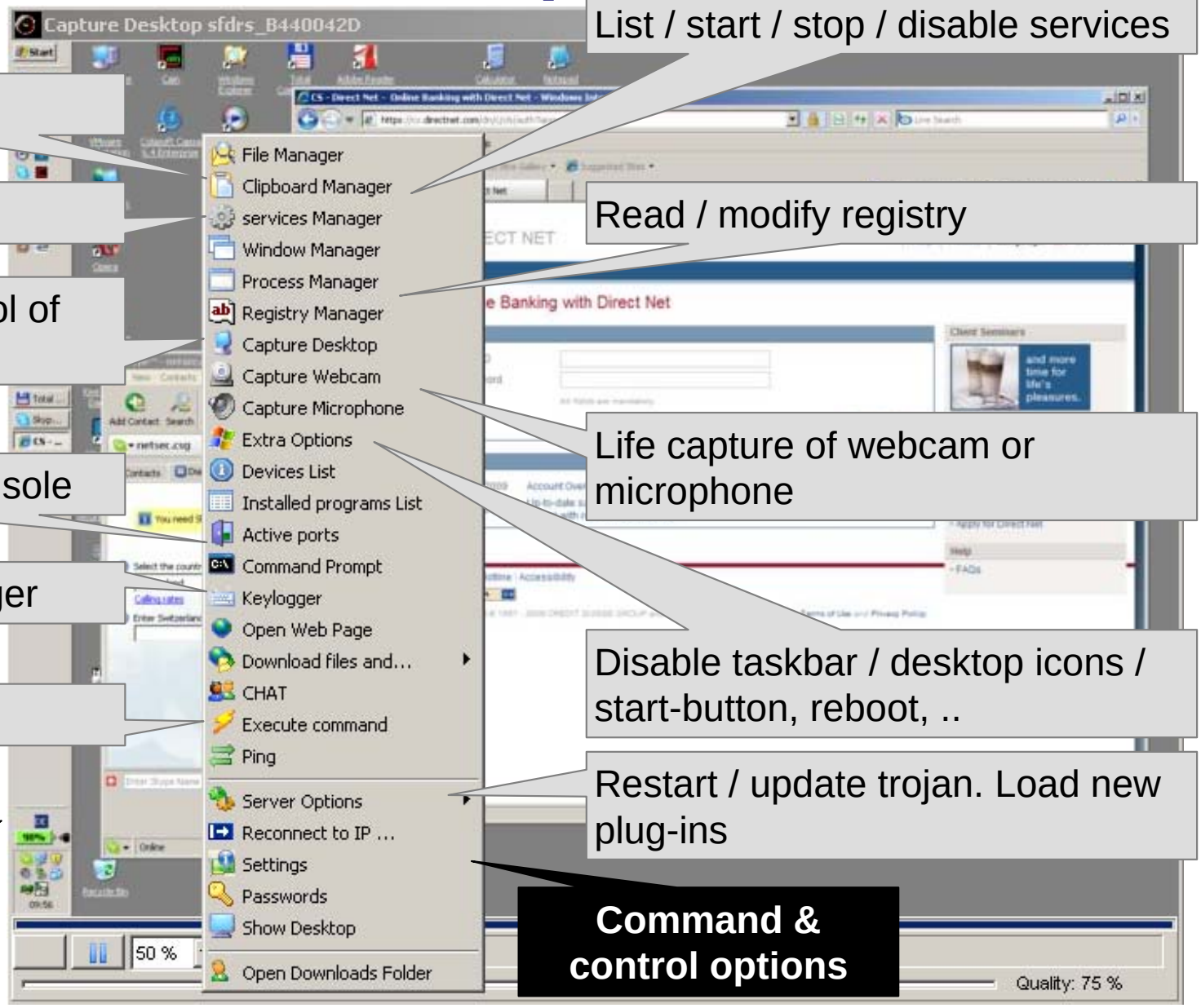
startup message to deceive victim (if needed)

disable/kill unwanted processes on target machine

# Command and Control



# Command and Control Options




Read clipboard

List and kill processes

Life capture and control of desktop

Remote command console

Online / offline keylogger

Execute commands

List / start / stop / disable services

Read / modify registry

Life capture of webcam or microphone

Disable taskbar / desktop icons / start-button, reboot, ..

Restart / update trojan. Load new plug-ins

**Life remote target session**

**Command & control options**

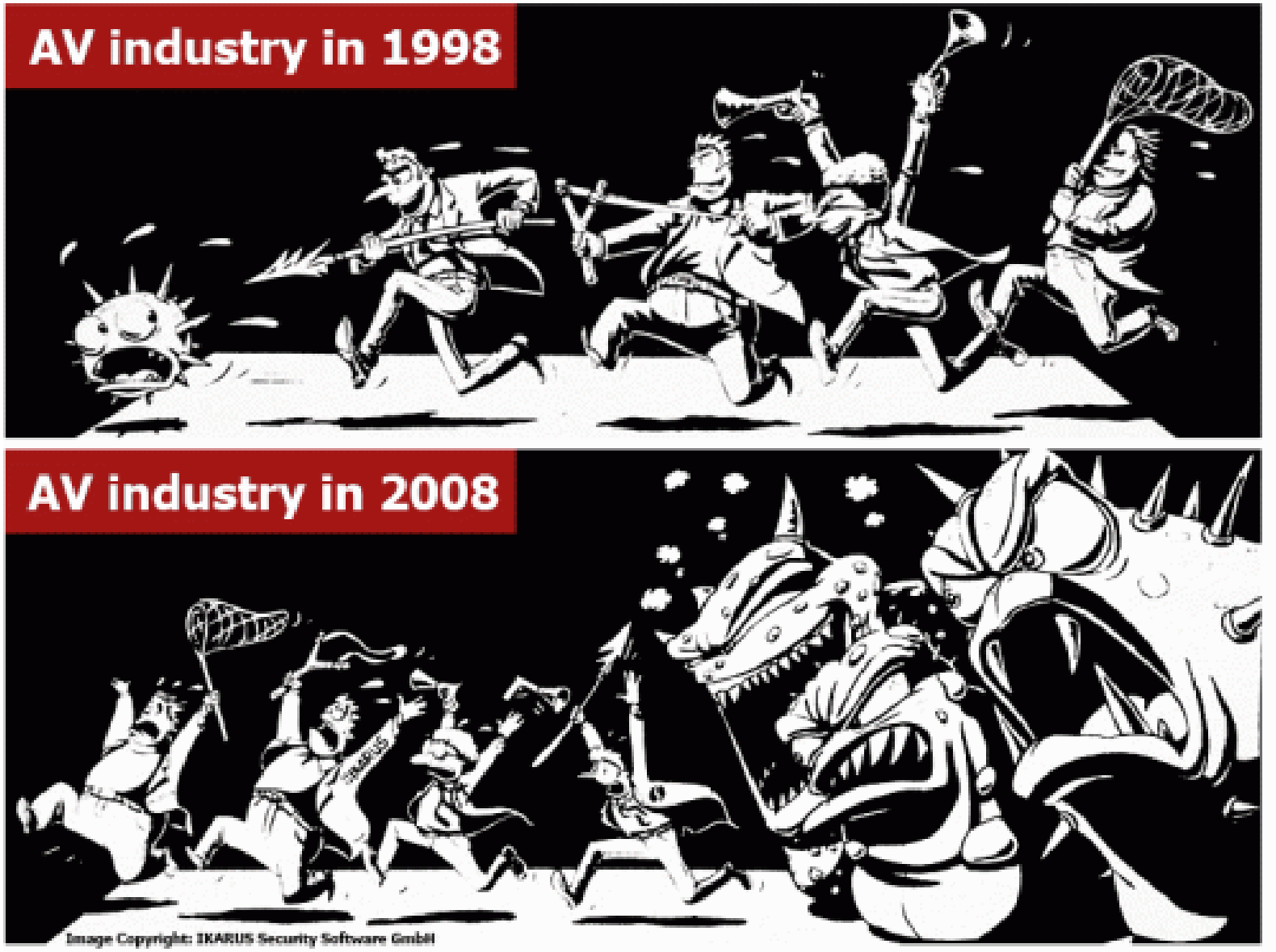
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Antivirus Evasion

# Antivirus Evasion Summary

- Experiment
  - Trojan built with a freely available DIY kit
  - Trojan obfuscated using a freely available crypter
  - both tools are more than 6 month old
- 03-Dec-2009
  - Trojan: detected by 77% of 40 AV products
  - Trojan after crypter: detected by 35% of 40 AV products
- 21-Dec-2009
  - Trojan after crypter: detected by 61% of 40 AV products
- Failed to detect
  - many of the major AV vendors failed to detect the Trojan more than 18 days after the sample was made available ..

# Antivirus is playing catch-up



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Cyberwarfare Web 2.0

# Web 2.0 - Social Networking Sites

- Social Network phenomenon creating new forums for mass communication and event coordination
- Virtual community “groups” can be created to address passionate topics, political ideals, and social injustices
- Groups tend to attract like-minded communities of interest and can swell their ranks rapidly
- Members of a group with targeted agenda’s can promote calls to action and facilitate “mob” responses
- Distribution of cyber arms and coordinated attacks possible

# Social networks on the rise

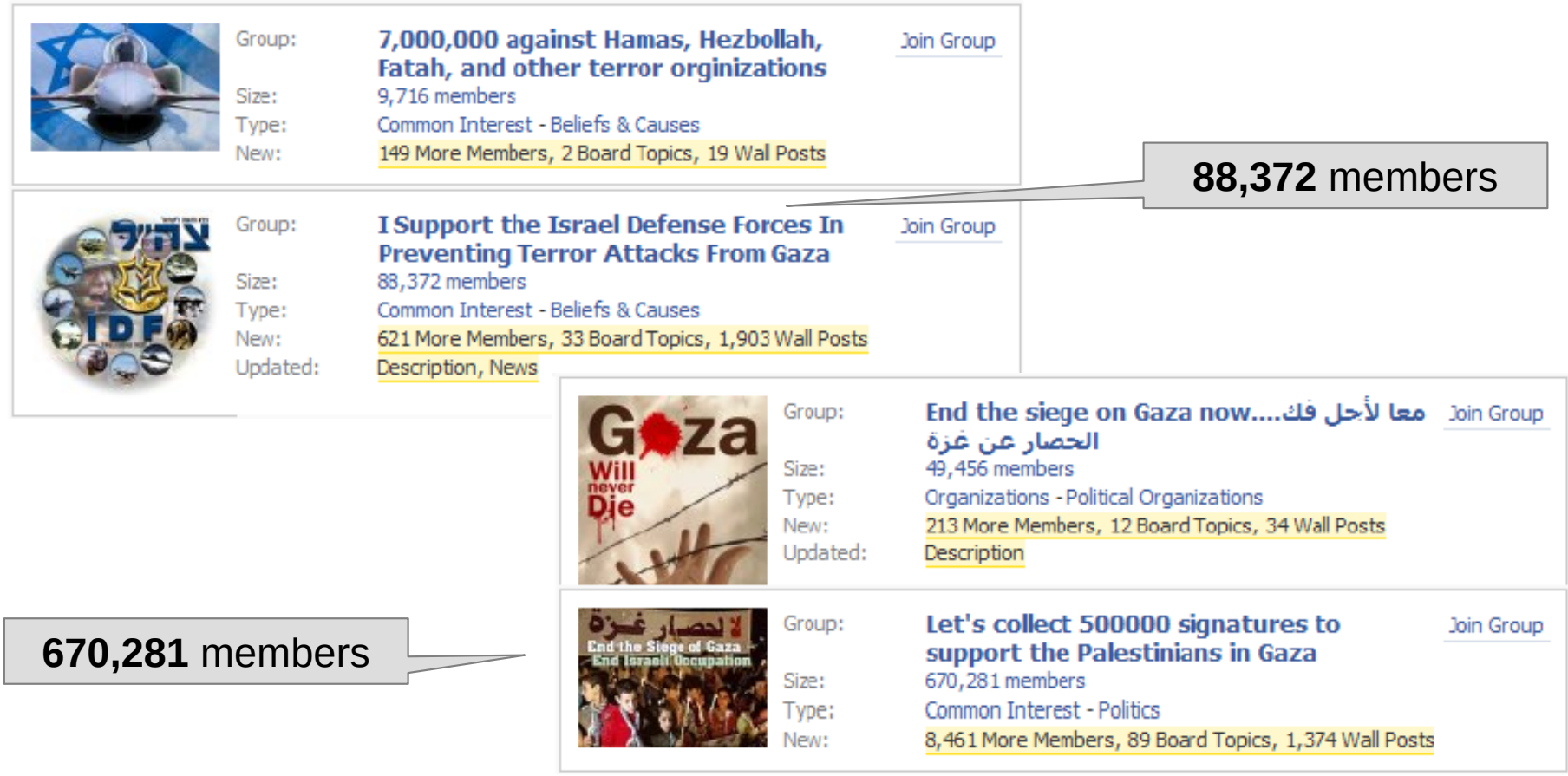
- Social networking sites on the increase
- Huge numbers of online members
- Almost all sites have the ability to create new “groups” or “forums” for discussion and information sharing

| Site | Members |
|---|---|
| Facebook | 300,000,000 |
| MySpace | 263,000,000 |
| Skyrock | 22,000,000 |
| LinkedIn | 43,000,000 |
| Orkut | 67,000,000 |
| Bebo | 40,000,000 |
| Hi5 | 80,000,000 |
| Nexopia | 1,500,000 |
| Mixi | 21,000,000 |
| Vkontakte | 25,000,000 |
| Netlog | 36,000,000 |
| Habbo | 117,000,000 |
| Friendster | 90,000,000 |

Wikipedia

# Common Interest Groups

- Military actions in the Gaza territory led to new social network groups supporting the opposing sides



# Moving beyond discussion

- popular movements and causes within a social network may stretch beyond joining an online group and participation in group discussions
- online groups are an ideal vehicle for organizing more influential or disrupting mass protests
  - physical
    - "here's the private phone number of the ambassador. tell her what you really think."
    - "meet outside the French embassy on Sunday with your plaque"
  - cyber
    - "everyone email staff@embassy.fr with your photos"
    - "their Web site reboots if you type ####### in to the visa request page. if we all do this, no one will be able to get a visa!"

# Cyber-Jihad Communities

- Numerous external web sites already exist specifically for the coordination of cyber attacks
  - most sites are organized along religious and political views
  - independent of social network sites – but often referred to from them
- Several web sites also offer tools that community members can download and target a mutual adversary
  - often referred to as a “Cyber-Jihad”

# Cyber-Jihad Coordination

- External Web sites promoting tools and tactics to target adversaries
- Social network forums and groups often link to external tool distribution sites

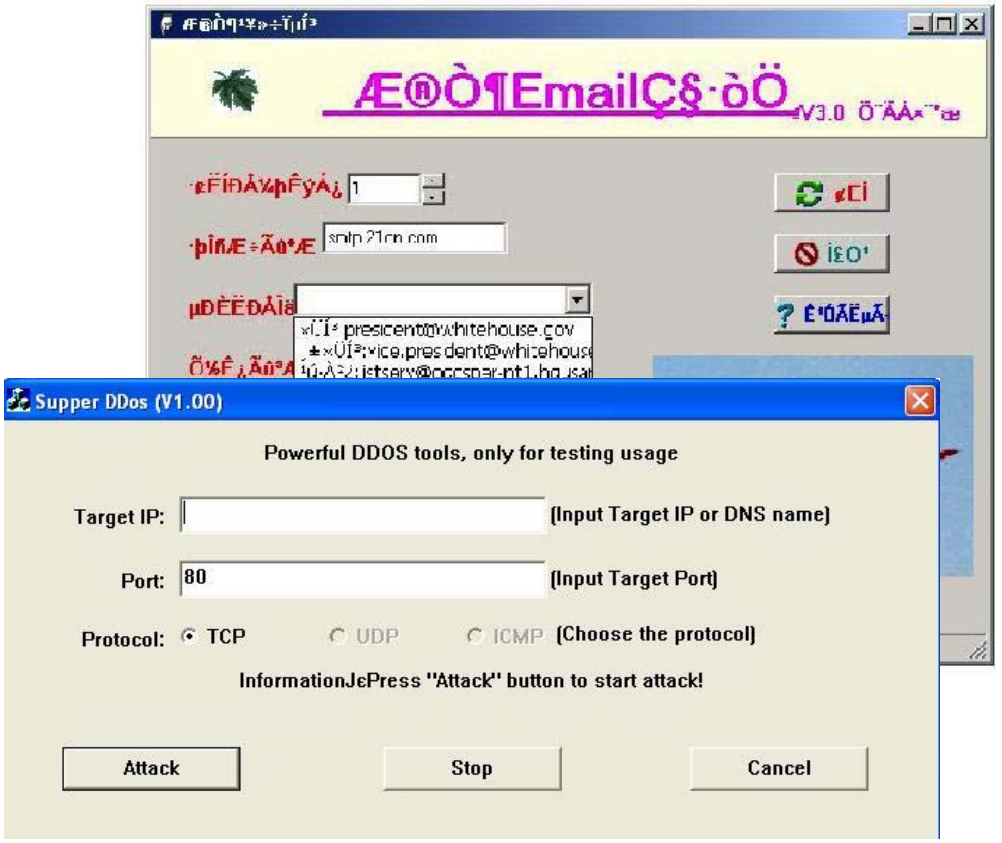

http://www.helpisraelwin.com

# Tools

- Tools used for community targeted attacks are typically of the distributed denial of service (DDoS) variety
- Target lists normally agreed in advance

  - Mail bombers
    - hundreds of mails per minute to specific mail address

  - Network flooders
    - saturate network connections
    - Exhaust system resources
    - ICMP flooding




http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cncom.html

# DDoS Attack

- DDOS = Distributed Denial of Service

- Community members download the attack tool
- At a specified date & time they launch their attack
- Combined volume of attack traffic caused target to stop functioning

- Example: 5,000 home DSL users can create
  - 1.3 Gbps of traffic volume
  - 150m e-mails per hour
  - 250,000 transactions per second

# Combined attack tool

- Social Network Coordinated DDoS
  - download software package, install, and participate
  - social network group provides command and control instructions
  - built-in DDoS functionality (mail, web, ..)
- Ease of participation
  - “Donate the unused power of your computer to the cause…”
  - “Use your spare Internet bandwidth while you’re asleep…”
  - “Automatically further the cause just by installing this tool…”

# Who are likely targets?

- Group creation and “mob” attacks
  - **Political** - “oppose the military junta in ..”
  - **Ideological** - “eating meat is bad, close down XXX turkey farm ..”
  - **Theological** - “Jedi is not a legitimate religion, don’t let them recruit ..”
  - **Local** - “stop the invasion of XXX within our community ..”
  - **Commercial** - “don’t let them sell toys with lead paint ..”
  - **Sporting** - “we’ll teach them for taking our trophy ..”

# Attack Ramifications

- Economic Exhaustion
  - prevent customers/clients from accessing Internet services
  - swamp internal systems and disrupt business processes
  - drive up hosting and cloud costs
- Public disinformation
  - defamatory information and brand erosion
- Flooding of non-Internet systems
  - harassment of business executives
  - unreachable telephony systems and emergency services

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Defense Strategies

# Defense strategies

- The threat is as complex as it is broad
  - no single protection solution will curtail the threat

- Instead, measures need to be taken within:
  - the Social Network site
  - the targeted organization
  - organizations whose employees can contribute to attacks
  - the ISP/Telco infrastructure routing the attack traffic
  - the abused intermediary sites that may host defamatory material

# Social Networking Sites

- Social Network sites bear the greatest burden in protecting organizations from being targeted by their members
- Most sites already have exhaustive user agreements that prohibit the discussion and participation of these attacks
  - Unfortunately, they appear to be rarely enforced…
- Monitoring Group Discussion Content
  - identification of malicious code, attack coordination, and breach of site usage agreements
- Removal or Sanitization of Content
  - filtering of offending content and discussions

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Conclusions

# Malware Economics

- cybercrime is a business that makes money at every level
- follow the money if you want to understand the root cause
- division of labor and specialization provides advanced and easy to use tools at low cost with extensive service provision
- new services and degrees of sophistication are appearing daily - no end in sight

# Defense

- Cybercrime
  - we have to deal with the threat one piece at a time
  - the end target is the user, customer centric

- The is no silver-bullet
  - no single technology can provide 100% protection
  - we need antivirus despite its limitations
  - keep your machine fully patched at any time:
    OS, all applications/plug-ins & antivirus

# Cyber Protesting

- Cyber-protesting, get used to it…
- Are you a victim or an enabler?
  - receiving end of an attack
  - facilitating an attack on others
- Tools are growing in sophistication
  - easier to become involved in a protest
  - ramifications are fuzzy…
- Collaboration
  - international and interdisciplinary collaboration needed

# Recommendation: Tools

- Online Virus Check
  - check every downloaded or received file for viruses using many diverse antivirus products
  - Recommended tool: Virus Total
    http://www.virustotal.com
- Check for pending updates
  - install all pending patches prior to use your machine
  - check your OS and all applications/plug-ins of your machine for pending updates
  - Recommended tool: Secunia PSI
    http://secunia.com/vulnerability_scanning/personal

# Further Reading

- Reading
  - Gunter Ollmann, Damballa
    http://www.damballa.com/downloads/r_pubs/CSI2009_CyberProtesting.pdf

# Thank you

- Contact: Dr. Stefan Frei
- http://www.techzoom.net