Rolf Schulz
CEO

Global Network Security GmbH

Technical Evolution of Cyber crime

Just a few thoughts…

Traditional (Industrial) Espionage

- The cooperation of insiders is necessary
- So why should they do this ?
  - financial gain , revenge, dissatis-faction with company management , culture, religion ….
- Problem : The mole
  - recruitment is a big risk for the attacker, can report to security or friends
- Break-ins and extortions are also common.
  - All these techniques are quite risky for the attacker as they require a lot of preparation and control.

Electronic devices

- electronic attacks are becoming more and more typical.
  - Wiretapping
  - ISDN D-Channel Attacks etc.
- concept behind this is trend-setting
  - Place a bug and go – low risk, automatic system
  - data is delivered to a central device (like a tape recorder) which is positioned in a safe area
  - BUT: Only spoken word
- Next : key logger devices
  - Collecting keystrokes, placed between keyboard and computer
  - Static RAM or wireless technologies (even Burst Mode available)

Worms and Viruses

- Today most of the interesting data is stored on computer systems …

Some Cases ...

- A virus caused data on Japanese nuclear power plants to leak on to the internet through a file-sharing platform, a report in the *Yomiuri Shimbun* says. The computer of an employee who was in charge of nuclear inspections was infected by a virus that reveals data through the Winny file-sharing (a Japanese only version) software. According to a report in the *Yomiuri Shimbun*, maintenance data equivalent to 31 floppy disks was leaked.
- The newspaper also said that this not the first time that information had leaked in this manner. Data on a police investigation in Hokkaido had been transmitted from an officer's PC last year while in March this year, private data about 50 patients who had undergone checks at Tokyo Medical and Dental University Hospital in Bunkyo Ward, Tokyo, were discovered to have leaked.

What happened ?

- The private computer of an employee who was in charge of nuclear inspections was infected by a virus that revealed data through the Winny file-sharing software (a very popular system primarily used in Japan)
- The software (Winny) is responsible for other information leakages on government systems and it was earlier recommended by official sources, to uninstall this product
  - So lessons learned? Not really. The last report of a data leakage is from March 2006: “Ehime prefectural police have announced that confidential personal information on 4,400 people was included in files accidentally uploaded to the Internet via Winny file-sharing software

Some Cases ...

- According to a Reuters media report, a married couple accused of developing a Trojan horse to spy on top Israeli companies have been placed in custody by the Israeli police.
- Michael Haephrati, and his wife Ruth Brier-Haephrati, were arrested in May 2005 in London, accused of writing malicious spyware software which was bought by private investigators to help top Israeli businesses spy on their competitors.
- Companies probed by the Israeli authorities in connection with the case include mobile phone operators, Cellcom and Pelephone, and satellite television provider YES.

Customised Trojan Horses

- The incident in Israel was a perfect example for a custemized Trojan attack.
- The malware was brought to the customer on demo disks
- Trojan monitored keystrokes and collected different types of documents. All this data were send to several “Collector-Systems” – so called *drop zones*
- antivirus software was not able to detect the malware

Spear Phishing

- NISCC Briefing 08/2005 Issued 16 June 2005” reported targeted Trojan email attacks against MoP
- Example: Golf…
- the attacker spied on the private behaviour and hobbies of his target. Once his passion is identified, it is easy for the attacker, to customise an email that the target will trust.
- Spear Phishing is THE new Risk for Top Management or Politicians…or just for people like us ☺

Hiding the tracks

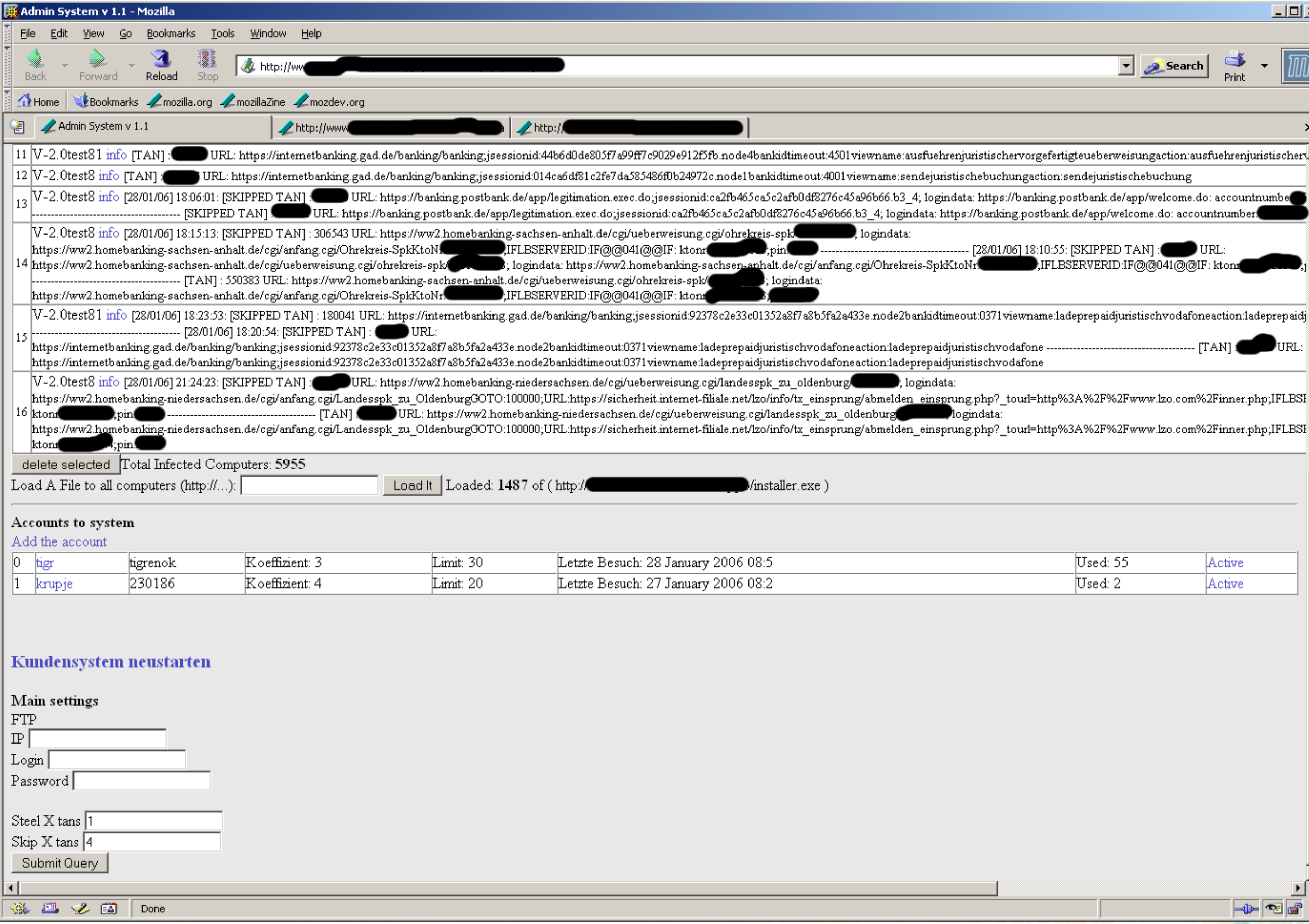
- AV Tools are signature based...
  - This is something like a fingerprint of the software. A signature is created by disassembling the virus, analyzing it and then identifying those sections of code that seem to be unique to the malware. The binary bits of those sections become the signature of the virus
- What does “unique to the malware” mean?
  - snapshot from one existing Binary
  - each variant is different
- Packer...
  - a tool, to compress and / or encrypt EXE Files – or parts of them

Bots and More …

- Modern Trojans are hard to find – Anti Virus Software needs more then 5 days to identify them.
  - hiding processes, files, connections
  - preventing anti-virus and operating system updates
  - kill running anti-virus processes and change personal firewall settings
  - anti debugging features
  - update functionality
  - Web based command & control (c&c) mechanism

Bots and More …

- Command and Control Bot Nets
- More and more Bots are using encrypted communication (SSL, Peer2Peer via Waiste)
  - Avoid detection from IDS Systems
  - Prevent Botnet Jacking, this is the „unfriendly“ takeover through enemy Bots
  - Payload also more and more encrypted
- Payload is getting bigger, rootkits are common today.
- Activities become more professional, business oriented
  - Exchange market for trojans / bots
    - Rent a Botnet for less then 3000 $US
  - Customization of trojans / bots
  - Global data collection and selling


Admin System v 1.1 - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://ww[redacted]
Search
Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
Admin System v 1.1
http://www[redacted]
http://[redacted]
Done

```
11 V-2.0test81 info [TAN] : [redacted] URL: https://internetbanking.gad.de/banking/banking;jsessionid:44b6d0de805f7a99ff7c9029e912f5fb.node4bankidtimeout:4501viewname:ausfuehrenjuristischervorgefertigteueberweisungaction:ausfuehrenjuristischer
12 V-2.0test8 info [TAN] : [redacted] URL: https://internetbanking.gad.de/banking/banking;jsessionid:014ca6df81c2fe7da585486f0b24972c.node1bankidtimeout:4001viewname:sendejuristischebuchungaction:sendejuristischebuchung
13 V-2.0test8 info [28/01/06] 18:06:01: [SKIPPED TAN] : [redacted] URL: https://banking.postbank.de/app/legitimation.exec.do;jsessionid:ca2fb465ca5c2afb0df8276c45a96b66.b3_4; logindata: https://banking.postbank.de/app/welcome.do: accountnumbe[redacted]
   ------------------------------------ [SKIPPED TAN] [redacted] URL: https://banking.postbank.de/app/legitimation.exec.do;jsessionid:ca2fb465ca5c2afb0df8276c45a96b66.b3_4; logindata: https://banking.postbank.de/app/welcome.do: accountnumber[redacted]
14 V-2.0test8 info [28/01/06] 18:15:13: [SKIPPED TAN] : 306543 URL: https://ww2.homebanking-sachsen-anhalt.de/cgi/ueberweisung.cgi/ohrekreis-spk[redacted], logindata:
   https://ww2.homebanking-sachsen-anhalt.de/cgi/anfang.cgi/Ohrekreis-SpkKtoN[redacted];IFLBSERVERID:IF@@041@@IF: kton[redacted];pin[redacted] ------------------------------------ [28/01/06] 18:10:55: [SKIPPED TAN] : [redacted] URL:
   https://ww2.homebanking-sachsen-anhalt.de/cgi/ueberweisung.cgi/ohrekreis-spk/[redacted]; logindata: https://ww2.homebanking-sachsen-anhalt.de/cgi/anfang.cgi/Ohrekreis-SpkKtoNr[redacted];IFLBSERVERID:IF@@041@@IF: kton[redacted];
   ------------------------------------ [TAN] : 550383 URL: https://ww2.homebanking-sachsen-anhalt.de/cgi/ueberweisung.cgi/ohrekreis-spk/[redacted]; logindata:
   https://ww2.homebanking-sachsen-anhalt.de/cgi/anfang.cgi/Ohrekreis-SpkKtoNr[redacted];IFLBSERVERID:IF@@041@@IF: kton[redacted];[redacted]
15 V-2.0test81 info [28/01/06] 18:23:53: [SKIPPED TAN] : 180041 URL: https://internetbanking.gad.de/banking/banking;jsessionid:92378c2e33c01352a8f7a8b5fa2a433e.node2bankidtimeout:0371viewname:ladeprepaidjuristischvodafoneaction:ladeprepaidj
   ------------------------------------ [28/01/06] 18:20:54: [SKIPPED TAN] : [redacted] URL:
   https://internetbanking.gad.de/banking/banking;jsessionid:92378c2e33c01352a8f7a8b5fa2a433e.node2bankidtimeout:0371viewname:ladeprepaidjuristischvodafoneaction:ladeprepaidjuristischvodafone ------------------------------------ [TAN] [redacted] URL:
   https://internetbanking.gad.de/banking/banking;jsessionid:92378c2e33c01352a8f7a8b5fa2a433e.node2bankidtimeout:0371viewname:ladeprepaidjuristischvodafoneaction:ladeprepaidjuristischvodafone
16 V-2.0test8 info [28/01/06] 21:24:23: [SKIPPED TAN] : [redacted] URL: https://ww2.homebanking-niedersachsen.de/cgi/ueberweisung.cgi/landesspk_zu_oldenburg/[redacted]; logindata:
   https://ww2.homebanking-niedersachsen.de/cgi/anfang.cgi/Landesspk_zu_OldenburgGOTO:100000;URL:https://sicherheit.internet-filiale.net/lzo/info/tx_einsprung/abmelden_einsprung.php?_tourl=http%3A%2F%2Fwww.lzo.com%2Finner.php;IFLBSI
   kton[redacted];pin[redacted] ------------------------------------ [TAN] [redacted] URL: https://ww2.homebanking-niedersachsen.de/cgi/ueberweisung.cgi/landesspk_zu_oldenburg[redacted]logindata:
   https://ww2.homebanking-niedersachsen.de/cgi/anfang.cgi/Landesspk_zu_OldenburgGOTO:100000;URL:https://sicherheit.internet-filiale.net/lzo/info/tx_einsprung/abmelden_einsprung.php?_tourl=http%3A%2F%2Fwww.lzo.com%2Finner.php;IFLBSI
   kton[redacted];pin[redacted]
```

delete selected Total Infected Computers: **5955**

Load A File to all computers (http://...): Load It Loaded: **1487** of (http:/[redacted]/installer.exe)

Accounts to system

Add the account

0	tigr	tigrenok	Koeffizient: 3	Limit: 30	Letzte Besuch: 28 January 2006 08:5	Used: 55	Active
1	krupje	230186	Koeffizient: 4	Limit: 20	Letzte Besuch: 27 January 2006 08:2	Used: 2	Active

Kundensystem neustarten

Main settings

FTP

IP

Login

Password

Steel X tans 1

Skip X tans 4

Submit Query

Example : TorPig

- The next step in worm technology evolution was TorPig., first seen in early 2006.
- The Trojan attempts to steal passwords, as well as logging key presses and open window titles to text files and periodically sends the collected information to a remote user via HTTP.
- The Trojan downloads and executes additional files from a remote site. Configuration files may also be downloaded which define further behaviors.
- Troj/Torpig-C automatically closes security warning messages displayed by common anti-virus and security related applications

Torpig - Overview

- How does it work ?
  - The infected System connects to c&c Server
  - The trojan recieves a list (encrypted) of Triggerstrings (or Softwareupdates or a new c&c Server list
- Triggerstrings example:
  - *.inetbank.net.au
  - DE|SPK.de Kontodetails homebanking*.de*
  - DE|izb.de Kontoart portal*.izb.de*
  - DE|volks.de Konto-Nr *vr-*ebanking.de*
  - but also: COM|gov.sg type SINGPASS* psi*.gov* singpass*.gov*

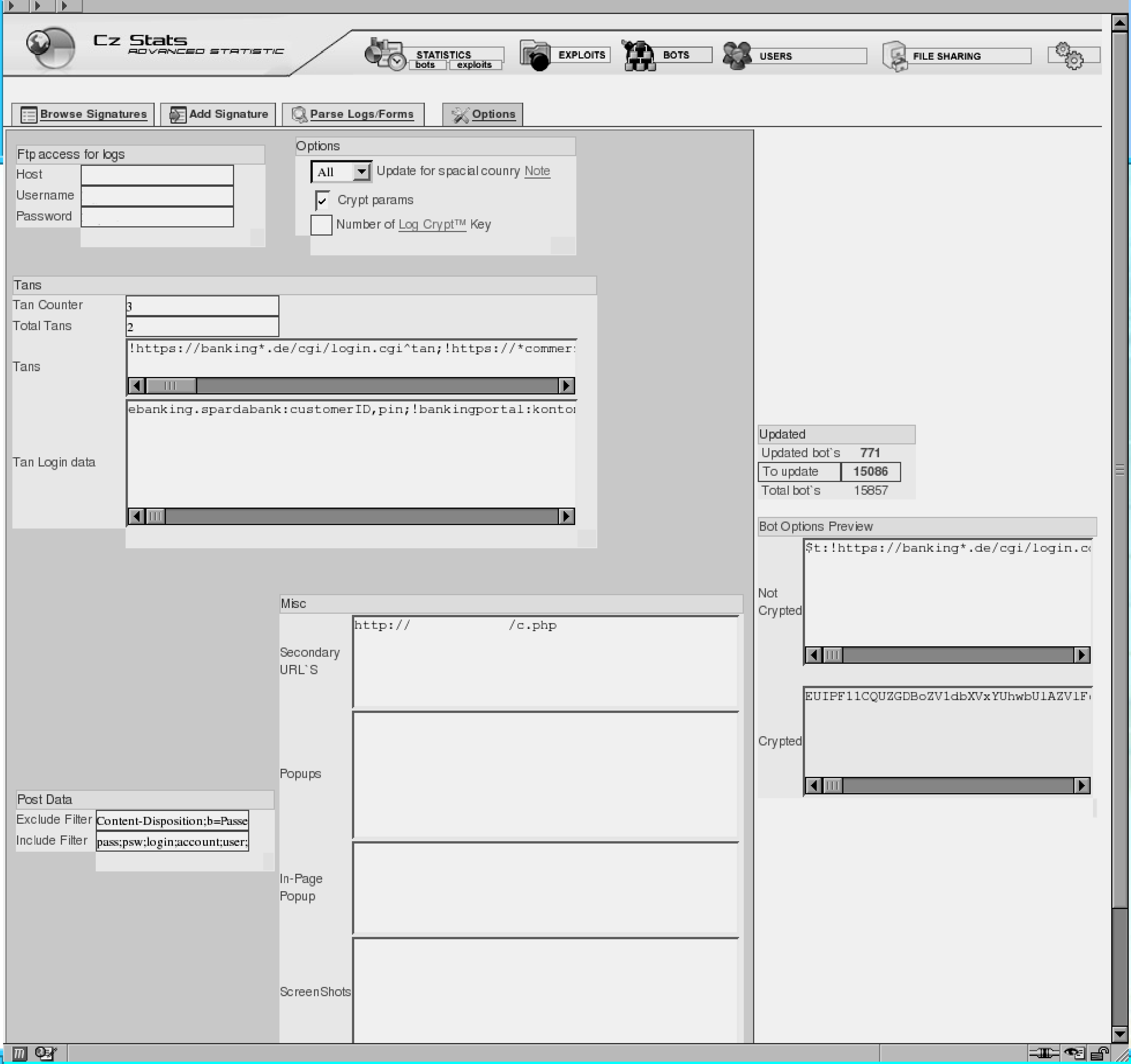
TorPig Function

- If visiting a website which is under observation, the Trigger ibank.communityfirst.com.au /xxx/yyy will be passed to a c&c System.
- GETconfig/check_domain.php?p1=2&p2= ibank.communityfirst.com.au
- [...]
- and returns as an answer the URL of a phishing site.
- ibank.communityfirst.com.au _corp.php
- After visiting the website. Using I-Frames and helper objects, (simple: writing directly to the render engine of the browser) the SSL Certificate of the original Site remains intact!!!

Ideas with TorPig

- Lets have a look on the following trigger strings:
  - 1. COM|abc.com secret|confidentialinternal*.abc.com*
  - 2. DE|pharma*.de .mdb *target-*internal.de*
  - 3. COM|intranettype Document target.company*.com
- In (1) the Trojan collects classified data, triggered by the keyword Secret or Confidential from the internal server,
- in (2) a MS Access Database from the intranet of target.com is transferred to a collector system.
- The attacker can also manipulate the intranet web server.

mbH



Ftp access for logs

Host

Username

Password

Options

All ▾ Update for spacial counry Note

☑ Crypt params

□ Number of Log Crypt™ Key

Tans

Tan Counter: 3

Total Tans: 2

Tans: !https://banking*.de/cgi/login.cgi^tan;!https://*commer

Tan Login data: ebanking.spardabank:customerID,pin;!bankingportal:kontoı

Updated

Updated bot`s	771
To update	15086
Total bot`s	15857

Bot Options Preview

Not Crypted: $t:!https://banking*.de/cgi/login.c

Crypted: EUIPF11CQUZGDBoZV1dbXVxYUhwbU1AZV1F

Misc

Secondary URL`S: http://   /c.php

Popups

In-Page Popup

ScreenShots

Post Data

Exclude Filter: Content-Disposition;b=Passe

Include Filter: pass;psw;login;account;user;

Garbage Collection...

- All the Trojans around not only manipulate systems, they also collect randomly data from infected systems which has to do with credit cards, accounts, personal information, passwords, University Accounts etc
- Portal Accounts, Company VPN Data, Govermental Sites...
- Data is sold via BBs or P2P

Trojaner collecting Data...

- 00003: [IP:200.87.50.200 18.04.2006 01:19:50 nt]
- 00005: destination=https%3A%2F%2Fwebmail.ntu.edu.sg%2Fexchange%2F&flags=2&username=STAFF%5Cmzxiao&password=pattyxxxxx&domain=STAFF&forcedownlevel=0&trusted=0
- 00006: NTU Webmail - http://www.xg6hc.cn
- https://webmail.ntu.edu.sg/exchweb/bin/auth/owalogon.asp?url=https://webmail.ntu.edu.sg/exchange/&reason=0
- 00008: [-- webmail.ntu.edu.sg/exchweb/bin/auth/owaauth.dll --]

Trojaner collecting Data...

- Destination=https%3A%2F%2Fexchange.nus.edu.sg%2Fexchange&flags=0&username=nusxxx%5Cu0306879&password=h3xxxx2g&forcedownlevel=0&trusted=0
- [IP:61.111.221.51 06.06.2006 06:08:00 nt]
- 00002: REMOTE IP: 202.156.6.4
- 00003: TIMESTAMP: 10\6 7:35:18-------------------------------

- URL:https://www.singpass.gov.sg/npin/redirectLogin.do?npin_data1=483643A6D479505CB8BC29B687C36E91AC40F11967DFC565B706BF425876A4D1724C8758BBF0850803FF3D070C3F087C7F24143F9DFCFECA078F49F02E89F700B1D98C46C1C06A443238729BA8E2AB3239A8CEBABB4585947FB9C1D43BAF9E80A8F098309B24EDE0BEF3E269DFCE9A72CFED97EB984F6F72B039BB482087243F&npin_data2=7CC59ED4642DF0D111E20ED2E5A585A77F892F428336C2F124EAA87D460B6F323FE72E3ABBB8EB4893B7B869470C14BF97398B79EEC136A8E4A3D7DBC410ABB575070021F4955CEC86995C204CB2D5247AC39A8B73D6D834A17726
- 00005: action=submitLoginSingPassID
- 00006: firstSingPassIDChar=S
- 00007: partialSingPassID=1000075z

- txt_access_id=S1234256J&txt_password=S1234256J&action=PROCESS&page=CNELOGIN&app=SNBLOGIN&version=v12&cmd_ok.x=0&cmd_ok.y=0
- [-- psi.gov.sg/NASApp/tmf/TMFServlet --]

Collecting Data – WHY?

- Collect and sell
  - Customers are org. Crime Scene
  - Customers are Terrorist
  - and also : articles of exchange...
- RISK : False identity
  - set up some social Background
  - to pretend to be an “old boy” at University...
  - faking IDs, Credit Cards etc.

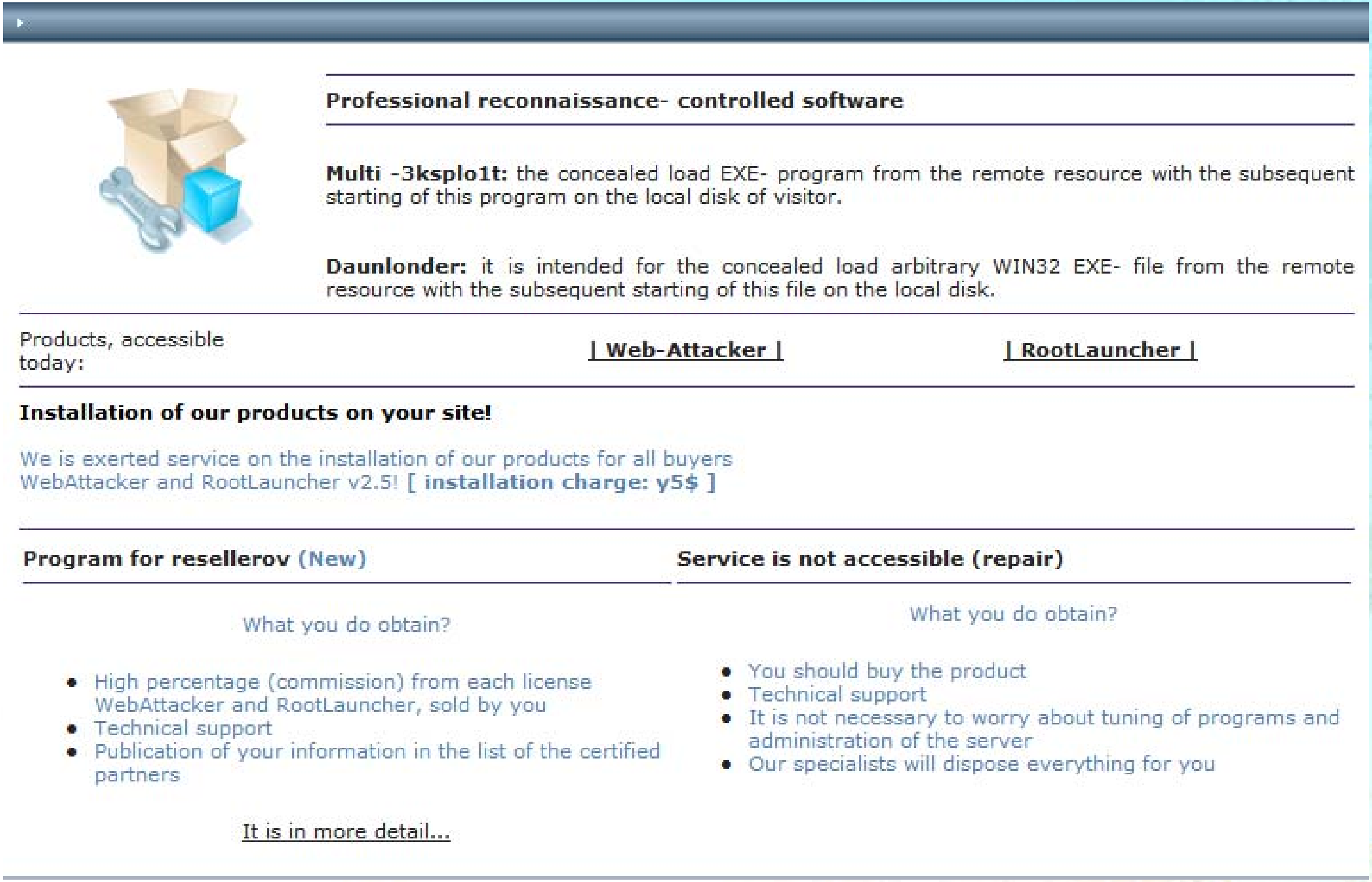
MyFib

- MyFip
  - Myfip is a network worm discovered in August of 2004.
  - designed solely for the purpose of intellectual property theft.
  - Collects the following Data
    - .pdf - Adobe Portable Document Format
    - .doc - Microsoft Word Document
    - .dwg - AutoCAD drawing
    - .sch - CirCAD schematic
    - .pcb - CirCAD circuit board layout
    - .dwt - AutoCAD template
    - .dwf - AutoCAD drawing
    - .max - ORCAD layout
    - .mdb - Microsoft Database

MyFib

- Mainwebsite : net918.com, registered to a user in Tianjin.
- **Sample source IP addresses:**
- 60.26.0.0/24 CNCGROUP Tianjin province network
- 221.198.15.10 CNCGROUP Tianjin province network
- 218.69.195.108 CNCGROUP Tianjin province network
- **Sample collector IP addresses used:**
- 202.104.237.179 CHINANET Guangdong province network
- 221.196.118.219 CNCGROUP Tianjin Province Network

Bot Net Shopping & Marketing



Professional reconnaissance- controlled software

Multi -3ksplo1t: the concealed load EXE- program from the remote resource with the subsequent starting of this program on the local disk of visitor.

Daunlonder: it is intended for the concealed load arbitrary WIN32 EXE- file from the remote resource with the subsequent starting of this file on the local disk.

Products, accessible today: **| Web-Attacker |** **| RootLauncher |**

Installation of our products on your site!

We is exerted service on the installation of our products for all buyers WebAttacker and RootLauncher v2.5! **[installation charge: y5$]**

Program for resellerov (New)

What you do obtain?

- High percentage (commission) from each license WebAttacker and RootLauncher, sold by you
- Technical support
- Publication of your information in the list of the certified partners

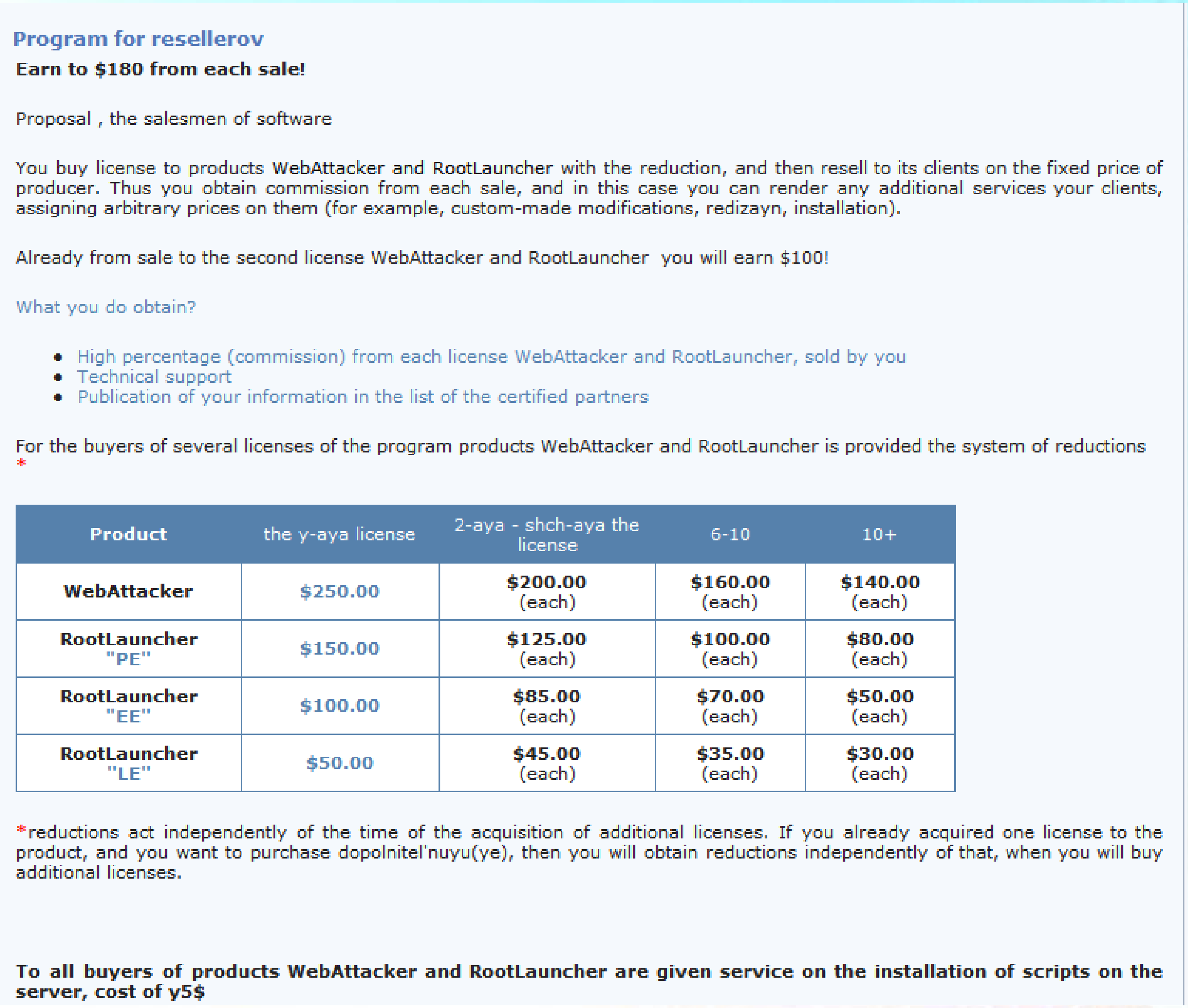
It is in more detail...

Service is not accessible (repair)

What you do obtain?

- You should buy the product
- Technical support
- It is not necessary to worry about tuning of programs and administration of the server
- Our specialists will dispose everything for you

Bot Net Shopping…



Program for resellerov

Earn to $180 from each sale!

Proposal , the salesmen of software

You buy license to products WebAttacker and RootLauncher with the reduction, and then resell to its clients on the fixed price of producer. Thus you obtain commission from each sale, and in this case you can render any additional services your clients, assigning arbitrary prices on them (for example, custom-made modifications, redizayn, installation).

Already from sale to the second license WebAttacker and RootLauncher you will earn $100!

What you do obtain?

- High percentage (commission) from each license WebAttacker and RootLauncher, sold by you
- Technical support
- Publication of your information in the list of the certified partners

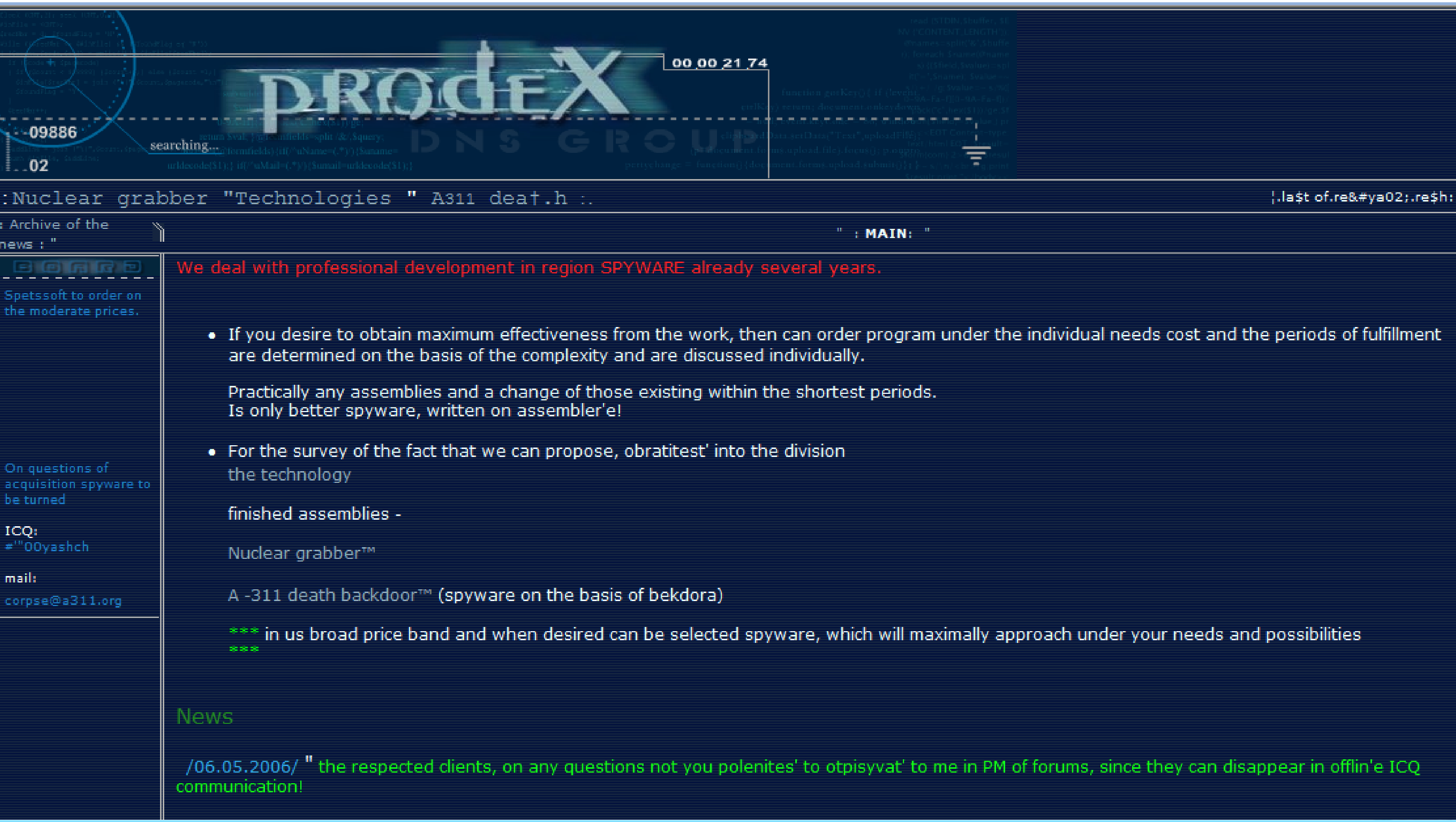
For the buyers of several licenses of the program products WebAttacker and RootLauncher is provided the system of reductions *

Product	the y-aya license	2-aya - shch-aya the license	6-10	10+
WebAttacker	**$250.00**	**$200.00** (each)	**$160.00** (each)	**$140.00** (each)
RootLauncher "PE"	**$150.00**	**$125.00** (each)	**$100.00** (each)	**$80.00** (each)
RootLauncher "EE"	**$100.00**	**$85.00** (each)	**$70.00** (each)	**$50.00** (each)
RootLauncher "LE"	**$50.00**	**$45.00** (each)	**$35.00** (each)	**$30.00** (each)

*reductions act independently of the time of the acquisition of additional licenses. If you already acquired one license to the product, and you want to purchase dopolnitel'nuyu(ye), then you will obtain reductions independently of that, when you will buy additional licenses.

To all buyers of products WebAttacker and RootLauncher are given service on the installation of scripts on the server, cost of y5$

Bot Net Shopping



:Nuclear grabber "Technologies " A311 deat.h :.

¦.la$t of.re&#ya02;.re$h:

: Archive of the news : "

" : MAIN: "

Spetssoft to order on the moderate prices.

On questions of acquisition spyware to be turned

ICQ:
#'"00yashch

mail:
corpse@a311.org

We deal with professional development in region SPYWARE already several years.

- If you desire to obtain maximum effectiveness from the work, then can order program under the individual needs cost and the periods of fulfillment are determined on the basis of the complexity and are discussed individually.

  Practically any assemblies and a change of those existing within the shortest periods.
  Is only better spyware, written on assembler'e!

- For the survey of the fact that we can propose, obratitest' into the division

  the technology

  finished assemblies -

  Nuclear grabber™

  A -311 death backdoor™ (spyware on the basis of bekdora)

  *** in us broad price band and when desired can be selected spyware, which will maximally approach under your needs and possibilities ***

News

/06.05.2006/ " the respected clients, on any questions not you polenites' to otpisyvat' to me in PM of forums, since they can disappear in offlin'e ICQ communication!

A little SpyHoTo...

- First : You need a good Trojan, something like TorPig
  - It’s flexible and gives an excellent return on malware investment (ROMI)
- We only want to spy, not to manipulate. So we don’t need any sophisticated tool to capture sessions or extract forms
- To be on the safe side, we order all of this from our Russian Solutions Provider. Investment is between 200US$ and 3000 US$. Delivery is fast and secure, and we will also receive a bill.

A little SpyHoTo...

- Dropzone: Use internal test systems in the company, nobody will recognize them...
- How to infect the targets ?
  - Setup an internal Website with some nice pics from the last social event, party, Lisa’s Baby, Jacks Puppies... etc. Don’t forget Webattacker or something similar.
  - prepare some fancy USB Sticks with some presentations and the Trojan
- WAIT
- At the end of the Week, use your IPod to copy the Payload from the Drop Zones

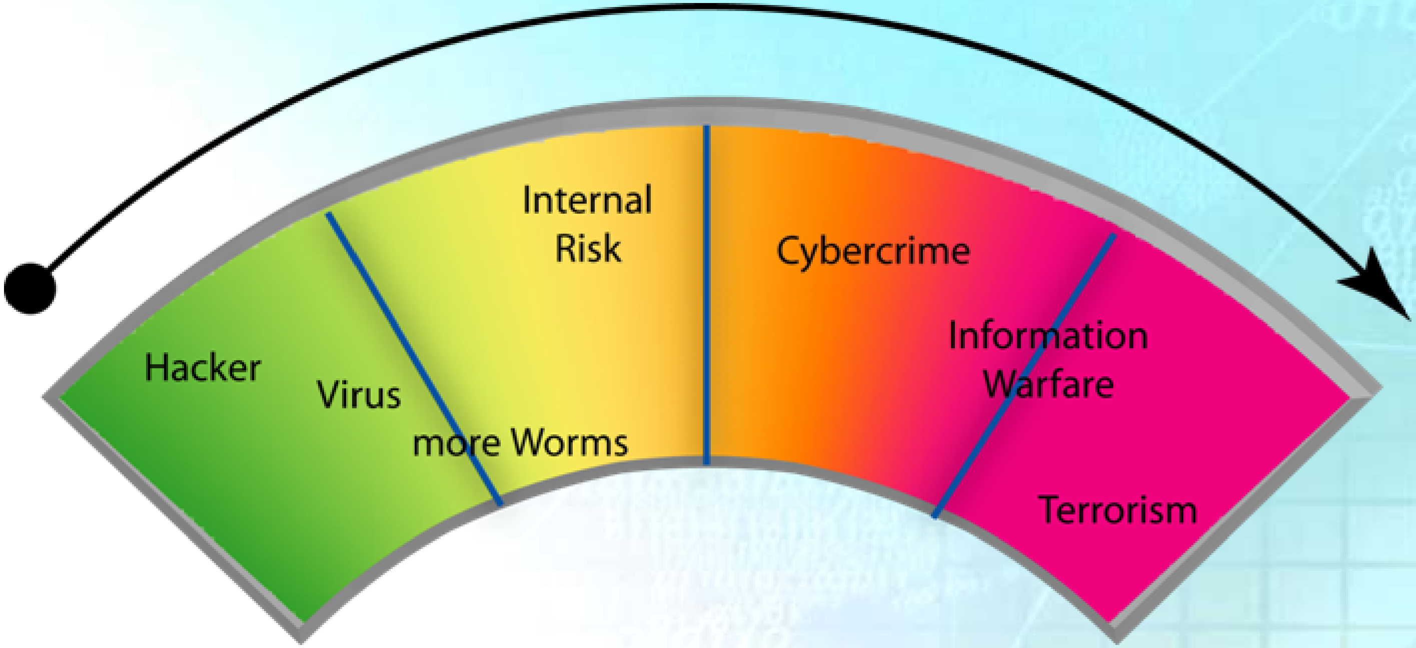
Upcoming Trends

- Mobile Attacks
- Localization Attacks
  - Abusing the momentum and localizing the attack to target specific users only
- Rise in encryption and use of packers
- Virtualization
- Intellectual property theft worms
- Use of new transport protocols
  - Latest : ICMP
  - Latest : P2P Encryption

Situation

- There is a convergence of increasing threats, growing global regulatory pressure, cost constraints, and evolving security tools challenging IT departments.
- There is a paradigm shift on the attackers side. Professional criminals, not bored teenage hackers, are now the source of the most serious security threats.
- Attackers no longer follow obscure idealistic goals, they simply follow the money .
- Beside all this, terrorists discovered the potentials of the worldwide networks, misusing private and corporate resources for their political goals
- At last, Security becomes more and more a cost center, and there's renewed pressure to provide high levels of security with as few money as possible.

Security – Quo vadis



Hacker	-- calculable and – mostly- predictable, prevention possible
Internal risk	– hard to guess, best to cover with organizational measures
Cyber crime	– prevention not really easy...
InfoWar	– no prevention without support from the government
Terrorism	- same situation as as InfoWar

More News ...

D&B Israel launches industrial espionage system

- (Israel Business Arena Via Thomson Dialog NewsEdge) D&B Israel has won a license from the Ministry of Justice to launch an industrial espionage system that will provide the business sector with new war tools against competitors.
- The D4 system will combine knowledge and alerts about customers both inside and outside the enterprise system, knowledge on movement of customers to competitors, and tools for reducing bad debts and focused marketing, including cross-referencing of customer data.
- The system will provide an alternative to non-segmented knowledge or knowledge from many sources, which was previously collected through surveillance companies but not received in real time nor cross-referenced.

Do not trust...

- MessageLabs and Counterpane reported in April this year, that 61% of computers have “some type” of spy ware or ad ware installed, and that the use of Trojans for spying on competitors is quite common.
- **INDIA ACCUSES US OF SPYING**
  - *By Konstantin Kornakov Jul 31 2006*
- *After several high profile arrests within the Indian security forces, the country’s government has decided to lodge an official protest with the US embassy in New Delhi. Indian authorities accuse the US of using a joint Indian-US cyber security forum as cover for spying activities in which several senior national security officials were involved.*