



# 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?**



# Web AppSec vs. Malware



- 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

A photograph of a diver in a metal cage underwater, surrounded by a large school of blue fish with yellow tails. A great white shark is swimming towards the cage from the right side of the frame.

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



# Learning from Online Banking



- 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 photograph of a large, intricate wooden roller coaster. The track is a complex network of dark brown wooden beams forming loops, turns, and a tall tower. A train of red and white cars is visible on one of the tracks. The surrounding area is a mix of green grass and sandy ground.

#1 Vector

Application  
Complexity

# 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?

# Commercial Web defacement



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

**Zone-H.org Notifications**      For New Zone-H

List Of Sites That Hacked and U Want to Report it	List Of Site That Reported Successfully
List Of Failed , Before Reported in Last 6 Month	
About Defacer and Deface Method Defacer Name Access credentials through Man In the Middle Patriotism	
Load List From File   Start Reporting   Clear All   On Hold   Save   OK  First Load List Of Site That Hacked and then Click Start Reporting	

**Limited Version**

PHP File URL   Address That U Upload	PHP File , ONLY Use It , No Use Another PHP Shell
PHP File Address :	<input type="text" value="http://www.target.com/test/idf.php"/> Ex: http:// /test/idf.php
Deface Page Address   Must Be Upload in The Folder That PHP File Uploaded	Deface Page Name :
	<input type="text" value="http://www.target.com/test/deface.htm"/> Ex: http:// /test/deface.htm
Deface Name That above Deface Address Will Be Copy By This Name in Defaced Sites	Deface Name :
	<input type="text" value="def.htm"/> Ex: def.htm
List Of Site in Server   Click it and wait	List Perm Folder Of Site That U Click It , Click it To Be Defaced
Choose Attack Method <input checked="" type="radio"/> Manual Mode <input type="radio"/> Automatic Mode Max Perm Folder Number : 10 Find Shortest in First 10 Perm Folder That Show in Manual Mode ; Deface It , go next site	
Get Site List  Clear Site List To Start New Project  Help      About	
List Of site That Hacked , Click To Open Site in Browser For Check  Other Tools U Need   U Can Get a Connect Back And Try To Root Access Get Connect back   Zone-h Reporter   Save Defaced List	



# SQL Injection Attack Tools

A screenshot of a web application interface, likely a penetration testing tool, demonstrating a SQL injection attack on a database named 'TestDB'. The URL in the address bar is 'http://localhost/sqlinject/news.asp?id=1'. The main window shows a list of users in the 'admin' table of the 'TestDB' database. The query used is 'select top 3 id,username,password from TestDB..admin order by id'. The results show three rows: (1, testUserzjs, 123456), (25, test, password), and (26, ff, aa). On the left side, there's a sidebar with various tools and links, including '安全漏洞' (Security Vulnerabilities) and '完整URL' (Full URL). The bottom status bar shows the IP as '5' and the status as 'XoR 8=3 + XoR 8=8 XOR 数字型 未探测'.



Getting Started  
with Malware...



# Keylogger Creators



## The Rat! 7.0XP Configuration ...

Version <input type="text" value="The Rat! 7.0XP"/>	The Rat! Files & Registry Names EXE <input type="text" value="socketme.exe"/>	Registry Value Name <input type="text" value="Explorer"/>	Encryption <input type="checkbox"/> Encrypt spy dump	ClipBoard <input checked="" type="checkbox"/> Watch ClipBoard ( Max Buffer Size 1-131070 bytes) : <input type="text" value="131070"/>
Enter the Directory and the File name the spy Dump shall be writed in <input type="text" value="c:\rat.log"/>		Send mail <input checked="" type="checkbox"/> Send spy dump on e-mail Authentification SMTP (RFC-2554) <input checked="" type="checkbox"/> Use Authentification		
Hide your Dump file in System Directory <input checked="" type="checkbox"/> Write Dump into System Directory\filename.ext		Login : <input type="text" value="mybestbox@mail.ru"/> Existing Server (16 chars) : <input type="text" value="therat.h15.ru"/> Pass : <input type="text" value="XXXXXXXX"/>		
Enter Dump file name (8.3 format) : <input type="text" value="32therat.log"/>		Delay between successful sendings : <input type="text" value="2"/> (min.) SMTP server for mail sending : <input type="text" value="smtp.mail.ru"/> SMTP Port : <input type="text" value="2525"/> Field SUBJECT in e-mail as user ID (8 char) : <input type="text" value="user_one"/>		
Invisibility & Fire Wall Bypassing <input checked="" type="checkbox"/> Invisible in Process Delay Before Invisibility Start (msec.) : <input type="text" value="1000"/> <input checked="" type="checkbox"/> Invisible in Registry		Field FROM (For mail.ru server this field and Login field is one and the same) : <input type="text" value="mybestbox @ mail.ru"/>		
Phantom Mode <input checked="" type="checkbox"/> Phantom Mode Bypass FireWall As... : <input type="text" value="C:\Program Files\Internet Explorer\EXPLORE.EXE"/>		Field TO (Enter E-mail adress, the Spy Dumps will be sended to) : <input type="text" value="mybestbox @ mail.ru"/>		
The Rat!'s Life : <input checked="" type="checkbox"/> Start Monitoring : <input type="text" value="11.04.2006"/> <input type="text" value="20:27:00"/> <input checked="" type="checkbox"/> Stop & Delete : <input type="text" value="11.04.2007"/> <input type="text" value="21:00:00"/>		Notification <input checked="" type="checkbox"/> Display Notification Message on startup		
Hot Keys to Stop The Rat! <input checked="" type="checkbox"/> Ctrl+ <input type="checkbox"/> Shift+ <input checked="" type="checkbox"/> Alt+ <input type="checkbox"/> Win+ <input type="checkbox"/> Disable <input type="button" value="Default"/> <input type="button" value="Apply"/> <input type="button" value="Save"/> <input type="button" value="Exit"/>				



# Malware creator kits – Shark 3

## (Jan '08)



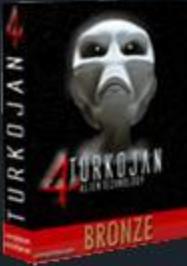
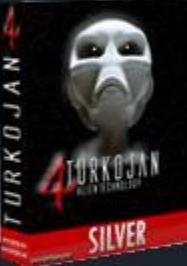
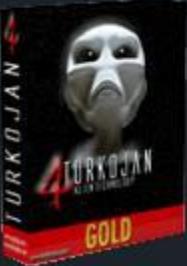
- “Remote Administration Tool” – RAT
- Added anti-debugger capabilities
  - VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box etc.

The screenshot shows the 'New Server' configuration dialog in the Shark 3 software. The dialog is divided into several sections:

- Left Sidebar:** A tree view of configuration options: Basic Settings, Server Installation, Start Up, Install Events, Bind Files, Blacklist, Anti Debugging, **Stealth** (selected), Firewall Bypass, Advanced, Summary, and Compile.
- Right Sidebar:** Another tree view of configuration options: Basic Settings, Server Installation, Start Up, Install Events, Bind Files, Blacklist, Anti Debugging, Stealth, Firewall Bypass, **Advanced** (selected), Summary, and Compile.
- Main Content Area:**
  - Compression ratio:** Traffic compression ratio (0 to 9): **9**
  - Transfer compression ratio:** Transfer compression ratio (0 to 9): **9**
  - Tolerance:**
    - Cpr-Tolerance Limit: **2** %
    - Ping-Tolerance in seconds: **20**
  - Key Stuff:**
    - Server Mutex: **sharK6WVHZZQ2H7**
    - Primary Key: **bHQqK1LG][i^s@guWwqeud2NbKfT6Q[8eAjB>HCsF61]Jq1oCGX5QJdu:iFmbfsnKc>JXURk4a:OO9L9@=1zXbO**
    - Secondary Key: **aZguw3Tzc=Kff\_VQ`1Cx<54?Ifvr44PplSQKxCSJ7p1pMalB?eKY20cK:\E\_GIVva\yxXPO:un][eKfOsuk80u9@pX7IiCsHskYdy<v0Us:hq**
    - Random Seed: **7t0bw4fk98y18z6tgzi3**

At the bottom of the dialog are buttons for **Load Settings**, **Save Settings**, and **Cancel**.

- Construction
- V.4 New
- Remote
- Webcam
- Audio
- Remote
- MSN
- Remote
- Advertising
- Online
- Information
- Computer
- Etc..

	<p><b>Bronze Edition</b></p> <ul style="list-style-type: none"> <li>■ 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)</li> <li>■ 1 month replacement warranty if it gets deducted by any antivirus</li> <li>■ 7/24 online support via e-mail</li> <li>■ Supports only Windows 95/98/ME/NT/2000/XP</li> <li>■ Realtime Screen viewing(controlling is disabled)</li> </ul> <p>Price : 99\$ (United State Dollar)</p>
	<p><b>Silver Edition</b></p> <ul style="list-style-type: none"> <li>■ 4 months (maximum 3 times) replacement warranty if it gets deducted by any antivirus</li> <li>■ 7/24 online support via e-mail and instant messengers</li> <li>■ Supports 95/98/ME/NT/2000/XP/Vista</li> <li>■ Webcam streaming is available with this version</li> <li>■ Realtime Screen viewing(controlling is disabled)</li> <li>■ Notifies changes on clipboard and save them</li> </ul> <p>Price : 179\$ (United State Dollar)</p>
	<p><b>Gold Edition</b></p> <ul style="list-style-type: none"> <li>■ 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets deducted by any antivirus (you can choose 6 months or 9 months)</li> <li>■ 7/24 online support via e-mail and instant messengers</li> <li>■ Supports Windows 95/98/ME/NT/2000/2003/XP/Vista</li> <li>■ Remote Shell (Managing with Ms-Dos Commands)</li> <li>■ Webcam - audio streaming and msn sniffer</li> <li>■ Controlling remote computer via keyboard and mouse</li> <li>■ Notifies changes on clipboard and save them</li> <li>■ Technical support after installing software</li> <li>■ Viewing pictures without any download(Thumbnail Viewer)</li> </ul> <p>Price : 249\$ (United State Dollar)</p>

[Online: 0] \_ X



Port : 15963



JAN v.4

TURKOJAN  
giCigi Online  
rights reserved.  
Turkey

me :	OS :
[REDACTED]	WinXP
Status : Passive	



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



The screenshot shows a Microsoft Visual Studio interface with a solution named 'bot'. The Solution Explorer lists files like msns.h, helpfuncs.h, helpfuncs.c, funcs.h, bot.c, and structs.h. The Botnet Control window displays a command-line interface with various commands (m, r, l, ur, ar, um, jl, sr) and their descriptions. The Output window shows log entries from the botnet, including client connections and events. The Properties window is visible on the right.

**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.

# Hire-a-malware-coder Pricing



- 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"



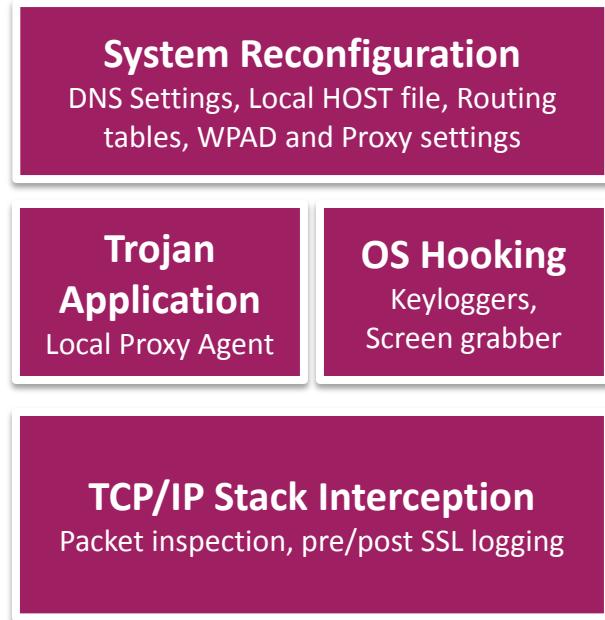
Looking for a soft target?



# Intercepting Traffic – Man-in-the-browser



**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



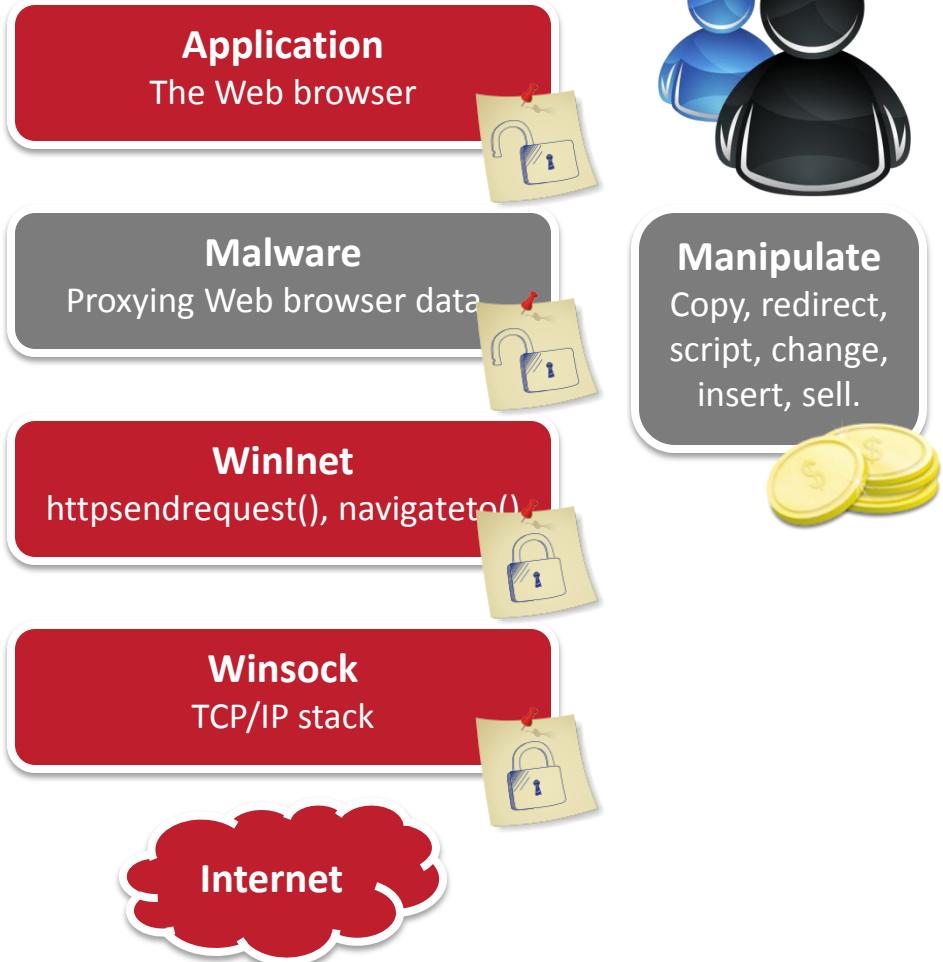
# API Hooking Malware



## 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**



A photograph of a large, arched opening in a heavy metal vault door. The door is made of thick, polished metal with a circular frame and a handle on the left. The archway leads to a bright, metallic interior of the vault.

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)

