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
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
#1 Vector

Application Complexiy
• 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

5/14/2009
OWASP 2009 Europe - Factoring Malware and Organized Crime into Webapp Security
SQL Injection Attack Tools

- Automatic page rank verification
- Search engine integration for finding “vulnerable” sites
- Prioritization of results based on probability for successful injection
- Reverse domain name resolution
- etc.

OWASP 2009 Europe - Factoring Malware and Organized Crime in to Webapp Security
Getting Started with Malware...
### Keylogger Creators

**The Rat!** popular keylogger creator kit – "Keylogger on demand" or "zero-day keylogger"

- **Prices in WebMoney (WMZ)**
  - The Rat! 7.0XP - 29 WMZ
  - The Rat! 6.0XP/6.1 - 22 WMZ
  - The Rat! 5.8XP - 15 WMZ
  - The Rat! 5.5XP - 13 WMZ
  - The Rat! 5.0XP - 9 WMZ
  - The Rat! 4.0XP - 8 WMZ
  - The Rat! 3.xx - 7 WMZ
  - The Rat! 2.xx - 6 WMZ

---

**The Rat! 7.0XP Configuration**

<table>
<thead>
<tr>
<th>Version</th>
<th>The Rat! Files &amp; Registry Names</th>
<th>Registry Value Name</th>
<th>Encryption</th>
<th>Clipboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Rat! 7.0XP</td>
<td>EXE socketme.exe</td>
<td>Explorer</td>
<td>Encrypt spy dump</td>
<td>Watch ClipBoard (Max Buffer Size 1-131070 bytes): 131070</td>
</tr>
</tbody>
</table>

**Enter the Directory and the File name**
- c:\rat.log

**Hide your Dump file in System Directory**
- Write Dump into System Directory\Filename.ext
- Enter Dump file name (8.3 format): 32therat.log

**Invisibility & Fire Wall Bypassing**
- Invisible in Process: Delay Before Invisibility Start (msec.): 1000
- Invisible in Registry

**Phantom Mode**
- Phantom Mode: Bypass FireWall As...:
- C:\Program Files\Internet Explorer\EXPLORE.EXE

**The Rat!’s Life**:
- Start Monitoring: 11.04.2006 20:27:00
- Stop & Delete: 11.04.2007 21:00:00

**Hot Keys to Stop The Rat!**
- Ctrl+Shift+Alt+Win+Disable
- Ctrl+Alt+F12

---

5/14/2009

OWASP 2009 Europe - Factoring Malware and Organized Crime into Webapp Security
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.

5/14/2009
OWASP 2009 Europe - Factoring Malware and Organized Crime in to Webapp Security 17
• Constructor/Turkojan
• V.4 New features:
  – Remote Desktop
  – Webcam Streaming
  – Audio Streaming
  – Remote passwords
  – MSN Sniffer
  – Remote Shell
  – Advanced File Manager
  – Online & Offline keylogger
  – Information about remote computer
  – 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 deducted 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 deducted 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 changements 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 deducted 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 changements 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)

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

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

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
API Hooking Malware

Clean System

Application
The Web browser

WinInet
httpsendrequest(), navigateto()

Winsock
TCP/IP stack

Internet

Infected System

Application
The Web browser

Malware
Proxying Web browser data

WinInet
httpsendrequest(), navigateto()

Winsock
TCP/IP stack

Internet

Manipulate
Copy, redirect, script, change, insert, sell.
• 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, mother's 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
Traditional Banking Malware

• 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)