The Threat of Banking Trojans: Detection, Forensics, and Response

(Insights from a Bank CSIRT)

Marc Vilanova, e-la Caixa CSIRT
July 2nd, 2009
Agenda

• Who am I?
• What is a Banking Trojan?
• Sensitive Information Hijacking Attacks
• Incident Response life cycle
• Torpig: An example of HTML Injection Trojan
• Trojans’ detection parameters
• Conclusions
• Q&A
Who am I?

- My name is Marc Vilanova
- e-Crime Intelligence Analyst for e-la Caixa CSIRT
- Incident Response
  - Phishing and its variants
  - Banking Trojans
  - 419 or Nigerian Scams
  - Trade Mark Abuse
  - Mobile Malware ...
- Memberships
  - FIRST (Forum of Incident Response and Security Teams)
  - APWG (Anti-Phishing Working Group)
  - Various Security Mailing Lists ...
- You can reach me at mvilanova@lacaixa.es
What is a Banking Trojan?

“A piece of malware that seats waiting for the user to access its online bank account in order to steal its sensitive information such as login credentials, debit/credit card numbers or modify its money transactions on-the-fly.”

Well-known banking Trojans:
- Anserin / Torpig / Sinowal / Mebroot
- WSNPoem / Zbot / ZeuS
- Bancos / Banker / Infostealer
- SilentBanker
Sensitive Information Hijacking Attacks

Keylogging

“Attack which intercepts the user's keystrokes when entering a password, credit card number, or other information that may be exploited.”

Not directly implemented on all banking Trojans
**Sensitive Information Hijacking Attacks**

**HTML Injection**

“Attack where the Trojan uses HTML injection to add new form fields or entirely Phishing websites in the users’ browser in order to convince them to provide personal information, additional user credentials or financial account information.”

Usually, HTML code/templates are held on another server distinct from the C&C.

Source: ThreatExpert
Sensitive Information Hijacking Attacks

Man-in-the-Browser

“A MiTM similar approach where the Trojan has the ability to modify pages, transaction content or insert additional transactions on-the-fly, all in a completely covert fashion invisible to both the user and host application.”

- Common facilities provided to enhance Browser capabilities such as Browser helper Objects (IE), Extensions (Firefox), API-Hooking (MiTM between the executable and its libraries) and UserScripts (Javascript) are used.

- No matter what mechanisms such as SSL/PKI and/or Two or Three Factor Authentication solutions are in place. None of them can defend the user.

- Attacks are working on the transaction level, not on the authentication level.
Incident Response life cycle

Detection

Response

Forensics
Incident Response life-cycle

Detection

- **Bank**
  - 24/7 Customer Service
  - Web Servers Logs
  - Malware Laboratory

- **Third Party Companies**
  - Malware and Forensic Analysis
  - Anti-Virus

- **Others**
  - Financial Institution, CERT/CSIRT, and Malware Research and Analysis Communities
Incident Response life-cycle

Forensics

**Static**
- Disassembler and analysis of assembly language code, packer detection, interesting strings, etc.
- Safer, but limited compared with dynamic analysis

**Dynamic**
- File system, the registry, other processes, and network monitoring
- C&C domains names and IP addresses
- Trojans’ detection parameters
Incident Response life-cycle

Response

Bank

- Timely-alerts based on Trojans’ detection parameters
- Trojan-infected customer detection during session process

Third Party Companies

- Domain name blackholing and IP egress-traffic blocking
- Anti-Virus signatures
Torpig: An example of HTML Injection Trojan

User visits the bank website
**Torpig: An example of HTML Injection Trojan**

Trojan contacts the HTML injection server
Torpig: An example of HTML Injection Trojan

The Injection server responds with the HTML Phishing content
Torpig: An example of HTML Injection Trojan

The Phishing content is injected into the user’s web browser
Torpig: An example of HTML Injection Trojan

The stolen information is sent to the C&C server

Note: New fields - “bonificpwdXX” and “ourpin” - are added in the POST content request
# Trojans’ detection parameters

<table>
<thead>
<tr>
<th>Trojan Name</th>
<th>Detection Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anserin/Torpig/Sinowal</td>
<td>&amp;bonificpwd= &amp;ourpin= &amp;login=Login</td>
</tr>
<tr>
<td>ZeuS</td>
<td>&amp;t= &amp;p= &amp;u= &amp;non= &amp;notredirect=</td>
</tr>
<tr>
<td>SilentBanker</td>
<td>&amp;pin=</td>
</tr>
<tr>
<td>MiTB (Unknown name)</td>
<td>_holder</td>
</tr>
<tr>
<td>Others</td>
<td>&amp;fuck= &amp;npass= &amp;n_coordinates= &amp;y=</td>
</tr>
</tbody>
</table>
Conclusions

• Even before 2005 Banking Trojans have been generating fraud to the financial institutions around the world through different kinds of attacks.

• The continuous evolution and development of techniques and methodologies used by malware creators leaves the common detection and protection systems still one step behind.

• As long as gangs are able to operate in Internet hosting their creations, the “Wack a Mole” game will continue. More efforts on prosecute them should be done.

• Malware creators use additional parameters that allow financial institutions to recognize them and to create Trojan-infected customers timely-alerts.

• Taking advantage of these additional parameters could lead financial institutions to prevent potential looses generated by these kinds of threats.
Q & A
Thank you!
ありがとうございました