Cert-Lexsi
Dead angle (Torpig vs PRG)
Agenda

- Cert-Lexsi Presentation
- Torpig vs PRG: Introduction
- Ecosystems
- Propagation
- Clients code
- Infrastructure
- Targets
- Comparison and efficiency
- News
Cert-Lexsi is a French CSIRT Team:

- Established in 2001
- 25 dedicated people
- Paris, Geneva, Montreal, Singapore

Our direct CSIRT-related activities for our constituency:

- Vulnerability Surveillance Service (Vulnerability Database and alerting)
- Cybercrime Surveillance and Analysis (Phishing, Malware, Studies)
- Emergency Response for Incidents
Introduction

**PRG** / **NTOS** / **WSNPoem** / **Zbot** / **Zeus**

Anserin / **Torpig** / Sinowal / **Torpig Mebroot (MBR)**
Ecosystems

**Torpig ecosystem**
- Malware as a service (MaaS)
- Piloted by a few coders/administrators
- Selected clients (cooptation) that ensure propagation (15-20)
- Centralized data collection and dispatch to clients
- All private > no public offering

**PRG ecosystem**
- Malware kit is sold on black markets (Official price: 3000 USD)
- Probably 100+
- Bad support
- Models such as a311, haxdoor, Pinch...
PRG (ZeuS) Control Panel
Propagation

**Torpig propagation**
- Drive-bys mainly, exploits kits (Neosploit)
- Today about 250k infections

**PRG propagation**
- Mail attachments, drive-bys, exploits kits (el fiesta)
- About 100-200k infections
**Clients Code**

**Torpig / Mebroot Code**

- Big evolutions: MBR Rootkit
- Strong skills, core injection, updated dlls
- Form-grabbing and injection
- Not for sell (service)
- Hard to Detect for Avs

**PRG Code**

- No real evolution
- Userland, inject in processes
- Capacity for RT MitM
- For sell everywhere, kits disclosed
- Good AV coverage

```assembly
cli
xor bx,bx
mov ss,bx
mov WORD PTR ss:0x7bfe,sp
mov sp,0x7bfe
push ds
data32
pusha
cld
mov ds,bx
mov si,0x413
sub WORD PTR [si],0x2
lods ax,WORD PTR ds:[si]
shl ax,0x5
mov 03,ax
```
**Infrastructure**

**Torpig infrastructure**
- One single c&c, rotating frequently
- c&c shutdown prevention
- Major variants now with MBR
- Multiple builds (clients)
- No bullet-proof hosting anymore
- Infrastructure strategy: be stealth, feed the beast.

**PRG infrastructure**
- Each client has its own infra
- Multiple variants as the kit is spread
- Some at bullet-proof hosting
- Infrastructure strategy: none
One unique Targets configuration file:

- 2,000+ targets
  (now around 250)
### PRG Targets

**Analyzing 243 PRG unique configuration files**

- 982 targeted domains
- Very small overlap / never the exact same configuration files

<table>
<thead>
<tr>
<th>Domain</th>
<th>Count</th>
<th>Targeted Domain</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>fiducia.de</td>
<td>225</td>
<td>barclays.co.uk</td>
<td>145</td>
</tr>
<tr>
<td>internetbanking.gad.de</td>
<td>219</td>
<td>cbonline.co.uk</td>
<td>143</td>
</tr>
<tr>
<td>vr-networld-ebanking.de</td>
<td>218</td>
<td>caja-granada.es</td>
<td>143</td>
</tr>
<tr>
<td>gruposantander.es</td>
<td>198</td>
<td>clavenet.net</td>
<td>143</td>
</tr>
<tr>
<td>norisbank.de</td>
<td>197</td>
<td><a href="http://www.ccm.es">www.ccm.es</a></td>
<td>142</td>
</tr>
<tr>
<td>comdirect.de</td>
<td>190</td>
<td>ccm.es</td>
<td>142</td>
</tr>
<tr>
<td>dresdner-privat.de</td>
<td>188</td>
<td>cajamadridempresas.es</td>
<td>137</td>
</tr>
<tr>
<td>citibank.de</td>
<td>185</td>
<td>cajabadajoz.es</td>
<td>136</td>
</tr>
<tr>
<td>e-gold.com</td>
<td>182</td>
<td>nationalcity.com</td>
<td>136</td>
</tr>
<tr>
<td>bancacajaproximaempresas.com</td>
<td>175</td>
<td>unicaja.es</td>
<td>135</td>
</tr>
<tr>
<td>bankofamerica.com</td>
<td>174</td>
<td>53.com</td>
<td>135</td>
</tr>
<tr>
<td>chase.com</td>
<td>174</td>
<td>tdcanadatrust.com</td>
<td>134</td>
</tr>
<tr>
<td>wellsfargo.com</td>
<td>171</td>
<td>citizensbankonline.com</td>
<td>134</td>
</tr>
<tr>
<td>paypal.com</td>
<td>165</td>
<td>usbank.com</td>
<td>133</td>
</tr>
<tr>
<td>banesto.es</td>
<td>164</td>
<td>suntrust.com</td>
<td>132</td>
</tr>
<tr>
<td>osmp.ru</td>
<td>162</td>
<td>cajadeavila.es</td>
<td>131</td>
</tr>
<tr>
<td>citibank.com</td>
<td>161</td>
<td>quibui.it</td>
<td>130</td>
</tr>
<tr>
<td>openbank.es</td>
<td>156</td>
<td>yandex.ru</td>
<td>130</td>
</tr>
<tr>
<td>wamu.com</td>
<td>153</td>
<td>isideonline.it</td>
<td>129</td>
</tr>
<tr>
<td>wachovia.com</td>
<td>153</td>
<td>secservizi.it</td>
<td>128</td>
</tr>
<tr>
<td>lloydtsb.co.uk</td>
<td>150</td>
<td>lwbank.it</td>
<td>127</td>
</tr>
<tr>
<td>ybonline.co.uk</td>
<td>150</td>
<td>cajamadrid.es</td>
<td>127</td>
</tr>
<tr>
<td>halifax-online.co.uk</td>
<td>150</td>
<td>bancopastor.es</td>
<td>127</td>
</tr>
<tr>
<td>bancopopular.es</td>
<td>147</td>
<td>rupay.com</td>
<td>127</td>
</tr>
<tr>
<td>hsbc.co.uk</td>
<td>147</td>
<td>poste.it</td>
<td>127</td>
</tr>
<tr>
<td>cajacanarias.es</td>
<td>146</td>
<td>nwbol.com</td>
<td>127</td>
</tr>
<tr>
<td>lloydtsb.com</td>
<td>146</td>
<td>cajamurcia.es</td>
<td>127</td>
</tr>
</tbody>
</table>
Cybercriminal’s Torpig short analysis

<table>
<thead>
<tr>
<th>Positives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard to catch (private ring)</td>
</tr>
<tr>
<td>Money goes to coders</td>
</tr>
<tr>
<td>Understand payment interfaces</td>
</tr>
<tr>
<td>Find channels for monetizing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Negatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of opportunities</td>
</tr>
<tr>
<td>Centralized head</td>
</tr>
<tr>
<td>Predictable C&amp;C</td>
</tr>
</tbody>
</table>
# Cybercriminal’s PRG short analysis

<table>
<thead>
<tr>
<th>+</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Less expensive</strong></td>
<td><strong>Easy to catch (public ring)</strong></td>
</tr>
<tr>
<td><strong>No predictable c&amp;c</strong></td>
<td><strong>Not a really “malware as a service”</strong></td>
</tr>
</tbody>
</table>
Comparison and efficiency

Look-a-likes

- Similar objectives: money
- Similar interception methods
- Both Russian-speaking ring

Differences

- in code skills
- in infrastructure protection
- in private/public market approach
Thank you

Any questions?

- Thomas GAYET - Speaker
- Vincent HINDERER

- cert@lexsi.com
- http://cert.lexsi.com/