50 SHADES OF CRIMEWARE
Frank Ruiz - Threat Intelligence Analyst at Fox IT y miembro de la organización sin ánimo de lucro mlw.re.

Manu Quintans - Threat Intelligence Manager at Buguroo / Deloitte, miembro fundador de la organización sin ánimo de lucro mlw.re focalizada en combatir amenazas en Internet.
What we know about Cyber-Crime?

It's Time Back To Reality

Understand Cyber-Crime activities

Previously on… 2013

Reality Bites

New trends at Cyber-Crime

Examples (We have a Target) :

Intelligence

DEMO TIME!

Bye bye!
WHAT WE KNOW ABOUT CYBER-CRIME?
ciber-. 1. Elemento compositivo prefijo, creado por acortamiento del adjetivo *cibernético*, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la realidad virtual.

SEÑORA! Soy un T800, he venido del futuro a robarle la tarjeta monedero....
WHAT WE KNOW ABOUT CYBER-CRIME?

ARAB WINTER
27,000 SMS INTERCEPTADOS
WHAT WE KNOW ABOUT CYBER-CRIME?

- 1.580,00 WEBSITE LOGIN CREDENTIALS
- 320,000 EMAIL ACCOUNTS
- 41,000 FTP ACCOUNT CREDENTIALS
- 3.000 RDP
- 3.000 SSH ACCESS

MOAR PONY!

In our last episode of "Look What I Found" we talked about a fairly large instance of the Pony Botnet Controller. With the source code of Pony leaked and in the wild, we continue to see new instances and forks of Pony 1.9. One of the latest instances we’ve run into is larger than the last with stolen credentials for approximately two million compromised accounts.

With so much data in our hands, we thought it would be interesting to look into some statistics regarding this particular attack.

We’ll start off with the final numbers, and then break it down:

- 1,580,000 website login credentials stolen
- 320,000 email account credentials stolen
- 41,000 FTP account credentials stolen
- 3,000 Remote Desktop credentials stolen
- 3,000 Secure Shell account credentials stolen
WHAT WE KNOW ABOUT CYBER-CRIME?

APT1

- Obama runs first law about cybersecurity.
- CISPA (Cyber Intelligence Sharing and Protection Act) is running again
- Mandiant, presents at RSA Conference new SOC.

Securestate talk at 2005 about this group and there tools...
WHAT WE KNOW ABOUT CYBER-CRIME?

visiting the SpyEye/ZeuS Merger

In 2010, I discovered that the authors of the SpyEye and Zbot Trojans — once competitors in the market for botnet and management kits — were planning to kill further development of ZeuS and fuse the two malware families into one. Initially, I heard some skepticism from folks in the community about this. But three months later, security researchers are starting to catch glimpses of this new hybrid Trojan in the wild with the author(s) shipping a series of beta releases that...
A New Trojan in Town: Meet Zberp

Trusteer researchers recently discovered a new Trojan that has been targeting more than 450 financial institutions around the world, mainly in the U.S., U.K. and Australia. The new Trojan, which seems to be a variant of the well-known Zeus Trojan (a.k.a. Zbot), also demonstrates behaviors associated with the Carberp Trojan family. Therefore, we named it the Zberp Trojan.

According to an analysis conducted by Trusteer researchers Martin G. Korman and Tal Darsan, the Trojan seems to have been assembled from the leaked source code of two well-known Trojans: Zeus and Carberp. The Zeus source code was exposed to the public in 2011, and it is already used by some criminal groups that customize its behavior and develop new features. The Carberp source code was offered for sale last...
It’s time back to “reality”
It’s time back to “reality”
It’s time back to “reality”

NOS HACEMOS UN ARTICULILLO?

PERO SIN MARICONADAS...
It’s time back to “reality”

DOC! TENEMOS QUE VOLVER AL PASADO!

Y EVITAR QUE LOS PADRES DE BRIAN KREBS SE CONOZCAN!
Understand Cyber-Crime activities
Understand Cyber-Crime activities

Layer #1

- Indetectables
- DamageLabs
- HackForums
- ExploitIN
- DarkCode
- Antichat

The Undercoat
Just for kiddies
Understand Cyber-Crime activities
Understand Cyber-Crime activities
Understand Cyber-Crime activities
Understand Cyber-Crime activities
Understand Cyber-Crime activities

The Limbo
Semi Pro

- Pustota
- Verified
- Infraud
- CCPRO
Understand Cyber-Crime activities
Understand Cyber-Crime activities
LAYER #3

Understand Cyber-Crime activities

The Heaven’s door

Maza
TopSecurity
Korovka
Commuizn

Gang’s tha!
Understand Cyber-Crime activities
### Understand Cyber-Crime activities

**SERVERS, VPS, VIRTUALS, DOMAINS**

<table>
<thead>
<tr>
<th>Правила форума</th>
<th>Фонд форума</th>
<th>Статус &quot;Vendor&quot;</th>
<th>Статус &quot;Seller&quot;</th>
<th>Jabber @korovka.pro</th>
<th>Раздача инвайтов</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korovka.CC &gt; Другое</td>
<td>Халява</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Корневой каталог:**

- My cabinet
- New thread

**Темы раздела:** Халява

<table>
<thead>
<tr>
<th>Тема / Автор</th>
<th>Рейтинг</th>
<th>Последнее сообщение</th>
<th>Ответов</th>
<th>Просмотров</th>
</tr>
</thead>
<tbody>
<tr>
<td>Халявные CC / FREE CC (1 2 3 4 5 ... Последняя страница)</td>
<td></td>
<td>01.12.2013 15:57</td>
<td>618</td>
<td>17,436</td>
</tr>
<tr>
<td>lolita</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Раздача раюал (1 2 3 4 5 ... Последняя страница)</td>
<td></td>
<td>28.11.2013 17:45</td>
<td>58</td>
<td>2,101</td>
</tr>
<tr>
<td>Lomik</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Инвайты] Спрос / предложение инвайтов (1 2 3 4 5 ... Последняя страница)</td>
<td></td>
<td>26.10.2013 09:01</td>
<td>97</td>
<td>2,793</td>
</tr>
<tr>
<td>MrArs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Поделитесь дедиком) (1 2 3 4 5 ... Последняя страница)</td>
<td></td>
<td>28.09.2013 22:29</td>
<td>191</td>
<td>6,100</td>
</tr>
</tbody>
</table>
Understand Cyber-Crime activities

- Cryptolocker
- Sinowall
- Gozi
- ZeusP2P
- Private
  - From Russia with love!
Previously on...
Previously on…

- First year, without new Banking Trojans. (Except’s KINS aka Kasper)
- Symlink Arrested (January)
- Paunch Arrested (BlackHole Exploit Kit) (OCTOBER)
- FBI shut down SilkRoad and they arrest Ross William Ulbrich. (OCTOBER)
- Target Breach. :-| – (NOVEMBER/DECEMBER)
- FBI With Spanish Police Cooperation take’s down Liberty Reserver and arrest CEO.– (MAY 2013)
- ZeusP2P (Game Over) and CryptoLocker Take down. - (MAY/JUN 2014)
Has been a special year in the volition of the industry of cyber-Crime

• The feeling of impunity begins to disappear.
• Groups midlevel begin to close and professionalize their assets.
• Ironically, the vetted gang’s start to show some gaps.
Previously

These Changes are due to

• Detentions.
• Proliferation of bloggers / twitters 'investigating' cybercrime scene. *(Pr0n stars)*
• Insider Researchers.
•Leaks (Pasties, services... )
The “industry” of Cyber-Crime, now are more than closed than ever.
New trends
New Trends at Cyber-Crime Industry

01 POS Malware - POINT OF SALES SYSTEM

02 TOR BASED NEW MOBILE MALWARE (EG: TOR BASED)

03 CRYPTOCURRENCIES
   Bitcoin, Litecoin, DogeCoin just Crypto Malware Miners!
The lack of a Banking Trojan for sale and the large increase in demand for cards has moved many players in this business.

Citadel users move their business to this new system.

Grows offer POS malware sales.
POS POINT OF SALE, What we found on markets?

The Beauty, the Bad, the Ugly and Guest start

01 Alina Malware
02 Dexter Malware
03 BlackPos
04 Soraya
OUR SERVICES

POS POINT OF SALE,
Software as Service? of course!
OUR SERVICES

Mobile Malware

Uses new resources like TOR. Increase of injections with support for mobile malware.

Mobile malware for sale:

• iBanking (as Service).
• Perkele
OUR SERVICES

IBanking Malware

---

**My projects** | **Phone list** | **SMS list** | **All SMS list** | **All Call list** | **Sounds** | **Contact list** | **Url report**
---|---|---|---|---|---|---|---

<table>
<thead>
<tr>
<th>Telephone number</th>
<th>ICCID</th>
<th>Model</th>
<th>OS</th>
<th>IMEI</th>
<th>Last command send</th>
<th>Last command</th>
<th>Control number</th>
<th>Phone status</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>42320543984</td>
<td>800945324205923803200</td>
<td>Unknown std</td>
<td>Android 4.4</td>
<td>947647817285271</td>
<td>26-02-2014 14:32:48</td>
<td>contact list (pending)</td>
<td>+863332040295</td>
<td>SMS OFF, Call OFF, Rev. OFF, Admin OFF</td>
<td>Select command 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project ID</th>
<th>Phone count</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0</td>
</tr>
<tr>
<td>500</td>
<td>1</td>
</tr>
<tr>
<td>600</td>
<td>0</td>
</tr>
<tr>
<td>111</td>
<td>2</td>
</tr>
<tr>
<td>id</td>
<td>phone number</td>
</tr>
<tr>
<td>----</td>
<td>--------------</td>
</tr>
<tr>
<td>59</td>
<td>4016</td>
</tr>
<tr>
<td>58</td>
<td>4018</td>
</tr>
<tr>
<td>57</td>
<td>(N)</td>
</tr>
<tr>
<td>56</td>
<td>(N)</td>
</tr>
<tr>
<td>55</td>
<td>(N)</td>
</tr>
<tr>
<td>54</td>
<td>(N)</td>
</tr>
<tr>
<td>53</td>
<td>4013</td>
</tr>
<tr>
<td>52</td>
<td>(N)</td>
</tr>
<tr>
<td>51</td>
<td>(N)</td>
</tr>
<tr>
<td>50</td>
<td>(N)</td>
</tr>
<tr>
<td>49</td>
<td>(N)</td>
</tr>
<tr>
<td>48</td>
<td>(N)</td>
</tr>
<tr>
<td>47</td>
<td>(N)</td>
</tr>
<tr>
<td>46</td>
<td>(N)</td>
</tr>
<tr>
<td>45</td>
<td>4015</td>
</tr>
<tr>
<td>44</td>
<td>(N)</td>
</tr>
<tr>
<td>43</td>
<td>(N)</td>
</tr>
<tr>
<td>42</td>
<td>(N)</td>
</tr>
<tr>
<td>41</td>
<td>(N)</td>
</tr>
<tr>
<td>40</td>
<td>(N)</td>
</tr>
<tr>
<td>39</td>
<td>41</td>
</tr>
<tr>
<td>38</td>
<td>(N)</td>
</tr>
</tbody>
</table>

**Perkele Malware**
## CryptoCurrencies

### Statistic

<table>
<thead>
<tr>
<th>Clients</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>147679</td>
</tr>
<tr>
<td>Activity last Week:</td>
<td>119982</td>
</tr>
<tr>
<td>Activity last 24 h:</td>
<td>71749 (48%)</td>
</tr>
<tr>
<td>Activity last 30 m:</td>
<td>20307 (13%)</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash rate total:</td>
<td>344124.15</td>
</tr>
<tr>
<td>Average Hash rate:</td>
<td>2.33</td>
</tr>
<tr>
<td>Hash rate 24 hrs:</td>
<td>176008.80</td>
</tr>
<tr>
<td>Hash rate 30 min:</td>
<td>51362.38</td>
</tr>
<tr>
<td>Countries</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----</td>
</tr>
<tr>
<td>India</td>
<td>15975 (10%)</td>
</tr>
<tr>
<td>Spain</td>
<td>9677 (6%)</td>
</tr>
<tr>
<td>Thailand</td>
<td>9167 (6%)</td>
</tr>
<tr>
<td>Brazil</td>
<td>9093 (6%)</td>
</tr>
<tr>
<td>United States</td>
<td>8811 (5%)</td>
</tr>
<tr>
<td>Mexico</td>
<td>6700 (4%)</td>
</tr>
<tr>
<td>Vietnam</td>
<td>5906 (3%)</td>
</tr>
<tr>
<td>Argentina</td>
<td>5014 (3%)</td>
</tr>
<tr>
<td>Romania</td>
<td>5006 (3%)</td>
</tr>
<tr>
<td>Egypt</td>
<td>4601 (3%)</td>
</tr>
<tr>
<td>Italy</td>
<td>4227 (2%)</td>
</tr>
<tr>
<td>Turkey</td>
<td>3503 (2%)</td>
</tr>
<tr>
<td>Peru</td>
<td>3428 (2%)</td>
</tr>
<tr>
<td>Colombia</td>
<td>3267 (2%)</td>
</tr>
</tbody>
</table>
## TOTAL HASH RATE

<table>
<thead>
<tr>
<th>Expected Rewards</th>
<th>24H HASH RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>24 hours</strong></td>
<td><strong>24 hours</strong></td>
</tr>
<tr>
<td>124.24818819 LTC</td>
<td>63.54593438 LTC</td>
</tr>
<tr>
<td>1279.26 EUR</td>
<td>654.52 EUR</td>
</tr>
<tr>
<td><strong>7 days</strong></td>
<td><strong>7 days</strong></td>
</tr>
<tr>
<td>869.73731731 LTC</td>
<td>444.82154063 LTC</td>
</tr>
<tr>
<td>8954.82 EUR</td>
<td>4581.66 EUR</td>
</tr>
<tr>
<td><strong>30 days</strong></td>
<td><strong>30 days</strong></td>
</tr>
<tr>
<td>3727.44564560 LTC</td>
<td>1906.37803125 LTC</td>
</tr>
<tr>
<td>38377.78 EUR</td>
<td>19635.69 EUR</td>
</tr>
</tbody>
</table>
Brian Krebs

18/Dec/2013: Sources: Target Investigating Data Breach
20/Dec/2013: Cards Stolen in Target Breach Flood Underground Markets
22/Dec/2013: Non-US Cards Used At Target Fetch Premium
24/Dec/2013: Who’s Selling Credit Cards from Target?
10/Jan/2014: Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen
15/Jan/2014: A First Look at the Target Intrusion, Malware
16/Jan/2014: A Closer Look at the Target Malware, Part II
29/Jan/2014: New Clues in the Target Breach
04/Feb/2014: These Guys Battled BlackPOS at a Retailer
05/Feb/2014: Target Hackers Broke in Via HVAC Company
12/Feb/2014: Email Attack on Vendor Set Up Breach at Target
19/Feb/2014: Fire Sale on Cards Stolen in Target Breach
25/Feb/2014: Card Backlog Extends Pain from Target Breach
About the breach

What happened?

Has the issue been resolved?

Does that information include social security numbers?

Do you think you will find anything else?

How could Target let all this credit and debit card information get accessed?

How can I be assured you are taking the steps to protect my information in the future?
UN MALWARE!!!
UN MALWARE!!!
UN MALWARE!!!
INTELLIGENCE

- Emerging threat research
- Strategic partnerships to share intelligence
- Tailored threat focus areas
- Live, dynamic intelligence feeds with advanced
- Actively tracking of cybercrime element
- Daily emerging threat reviews
- Awareness of the changing technology and business environment
- Metrics and rending data for multiple key threat indicators
- Recommendations on improved and refined processes

- Botnet monitoring and analysis
- Malware reverse engineering
- Social media monitor
- Reputation scans
- Deep web monitoring
- Social engineering threats
- Spoofed websites
- All Source Intelligence

- Emerging tech review
- Loss management
- Vendor management
- Executive identity monitoring

... and remember
INFRASTRUCTURES
OUR SERVICES

Simple Botnet

INTERNET

BOTNET
Simple Botnet With Proxy
Botnet With Double Proxy

OUR SERVICES

VICTIMS

INTERNET

PROXY - 1

PROXY - 2

BOTNET
OUR SERVICES

FAST FLUX + C&C

VICTIM

HTTP GET

FASTFLUX

GET REDIRECT

RESPONSE CONTENT

RESPONSE CONTENT
OUR SERVICES

FAST FLUX + PROXY + C&C

VICTIM

HTTP GET

FASTFLUX

GET REDIRECT

RESPONSE CONTENT

RESPONSE CONTENT
OUR SERVICES

TOR INFRASTRUCTURES

VICTIMS

INTERNET

TOR Network
DEMO Concept

BUILD POS ENVIRONMENT

SWIPE OUR CREDIT CARD

BREATHE DEEPLY

INFECT OUR POS

CALM DOWN

PWN THE BOTNET AND GET OUR MONEY BACK!

OH MY GOD!!!

IT'S BEAUTIFUL!
Me robo mi tarjeta...

Yo quemé su botnet...
THANKS!
WARNING!

SPAM IS COMING!

SAVE 20% when you order online and enter Promo Code AVN99
FREE standard shipping when you order online.
THANKS!!