LAC payments week, Lima, September 11-14, 2017. Session on “Cybersecurity: a shared responsibility”

Giovanni Pichling Zolezzi
ASBANC - COO
Social Engineering
Phishing anatomy

1. Upload phishing kit
2. Send phishing email
3. Visit phishing page
4. Mail stolen credentials
5. Fetch email

Phisher

Email server

Hacked site

Victim
El método **black box**, que aumentó un 287%, 58 bancos de 10 países europeos sufrieron ataques de este tipo.

Although the Ploutus Team began by targeting Latin American countries, it now runs in multiple ATM vendors making it a worldwide issue and becoming the greatest ATM malware risk. Below is a list of countries that submitted a variant of Ploutus-D to VirusTotal:

- Mexico
- Peru
- Dominican Republic
- Ukraine
- Taiwan
- United States
Ransomware - Wannacry

Oschadbank ATM in Kyiv
IoT Microcontrollers

Arduino

Cubie Track

Raspberry
Already has 7,000 viruses that attack your devices

- Half of the viruses for these smart devices are dated 2017. That is, they are circulating for the first time.

- These malicious codes have been designed by cybercriminals to pirate devices, this serves to spy, extort and even involve people in blackmail.

Fuente: http://www.cioal.com/2017/06/23/iot-ya-cuenta-con-7-000-virus-que-atacan-sus-dispositivos//
Cybersecurity not only refers to protecting itself as an entity, but also assessing the risks to which it is exposed. An entity does not work alone, it interacts with other institutions and that is where risk is transferred.
Vulnerabilities Market

ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJS: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape

*All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.
Strategy to combat computer crime

Stakeholders

- Asociations (ASBANC, Confiep, FELABAN, OEA)
- Financial institutions (Banks, Financial others)
- Law enforcement authorities
- Government authorities (local - national)
- Critical Service Providers
- Regulation authorities & Consumer protection authorities
- Armed forces (National defense – Strategic sectors)
- Embassies & Consulates
- Global iniciatives (Budapest agreement)

Educación

- Clients
- Employees
- Law Enforcement Officials

- Use the same tools that criminals use
- Hire Specialized Services

Tecnología

- Autoregulation
- Legislation
- Sharing computer crime information

Normatividad
Promote operation of comprehensive Security observatories
Global cyberattacks monitoring
Global cyberattacks monitoring

#OpNoLeyLaboral  #LeyPulpin
Social network monitoring
Monitoreo Páginas Web
(Home Banking)
Deepweb operations
Deepweb - identity theft

Order Process:

After buying an ID or passport send us a message with your age and gender so we can find a matching dataset, alternatively you can provide a dataset (name, age, gender, size etc.). We will also need a biometric photo in high quality and signature scanned, we will give more instructions after your purchase.

Passports

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
<th>Buy now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lithuanian Passport</td>
<td>2650 EUR</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>Netherlands Passport</td>
<td>3150 EUR</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>Denmark Passport</td>
<td>3150 EUR</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>Great Britain Passport</td>
<td>4000 EUR</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>Canada Passport</td>
<td>2500 EUR</td>
<td>1</td>
<td>Buy now</td>
</tr>
</tbody>
</table>
Deepweb – Rent a hacker, dDoS

DDoS Attack

Our Pricing

<table>
<thead>
<tr>
<th>Plan</th>
<th>Bronze Lifetime</th>
<th>Gold Lifetime</th>
<th>Green Lifetime</th>
<th>Business Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price per month</td>
<td>5.00€</td>
<td>22.00€</td>
<td>50.00€</td>
<td>60.00€</td>
</tr>
<tr>
<td>1 Concurrent +</td>
<td>1 Concurrent +</td>
<td>1 Concurrent +</td>
<td>1 Concurrent +</td>
<td>1 Concurrent +</td>
</tr>
<tr>
<td>300 seconds boot time</td>
<td>600 seconds boot time</td>
<td>1200 seconds boot time</td>
<td>1800 seconds boot time</td>
<td></td>
</tr>
<tr>
<td>125Gbps total network capacity</td>
<td>125Gbps total network capacity</td>
<td>125Gbps total network capacity</td>
<td>125Gbps total network capacity</td>
<td></td>
</tr>
<tr>
<td>Resolvers &amp; Tools</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
</tr>
<tr>
<td>24/7 Dedicated Support</td>
<td>24/7 Dedicated Support</td>
<td>24/7 Dedicated Support</td>
<td>24/7 Dedicated Support</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Price</td>
<td>Quantity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small Job like Email, Facebook etc hacking</td>
<td>250 EUR = 1,344 €</td>
<td>1</td>
<td>Buy now</td>
<td></td>
</tr>
<tr>
<td>Medium-Large Job, naming people, espionage, website hacking etc</td>
<td>500 EUR = 3,299 €</td>
<td>8</td>
<td>Buy now</td>
<td></td>
</tr>
</tbody>
</table>
Deepweb - Carding
Phishing as a Service
Themes

• ¿Qué beneficios brinda usar una tarjeta de débito para realizar transacciones con sumas altas dinero?

• ¿Cómo opera la delincuencia informática?

• Consejos de seguridad para las compras por el Día de la Madre.

• Recomendaciones para evitar ser víctima de suplantación.

• Recomendaciones de Seguridad para Fiestas Patrias.

• ¿Qué es el phishing y cómo evitar enlaces maliciosos?

• Dinero en efectivo, llama peligro.

• Seguridad durante las fiestas de fin de año
Lack of understanding of the ecosystem in which we live
We do what everyone else does and we expect different results
Massive global attacks will continue. Impersonation will increase. User Profile admin must be assigned responsibly
Buying zero-day vulnerabilities encourages search for new attack vectors
  - It was paid $1,000,000 for an iOS9 exploit. Exists an offer of $1'500,000 for an exploit of iOS10
The increase in the incidence of collateral type attacks is anticipated
There is a lot to do and it requires tools that allow you to be at the level that demonstrate the crime of the current attacks
 Networks must be segmented and verify that we have control of the backup
Criminal organizations attack the financial system, do not focus on an entity. The need for IT security specialists is increasing day by day and the gap continues to increase, hence the need to form alliances for information exchange and collaborative monitoring
Legacy systems prove to be a valuable target for crime because of the greater facility to attack them
If we base our defense system on computer security programs and equipment; when something happens, it will be too late to react, we should orient our information searches and strategies in their origin