CEBOLLA CHAN 3.0: A WINDOW INTO THE CHAOTIC SPANISH-LANGUAGE UNDERGROUND

Liv Rowley
Intelligence Analyst
Flashpoint
PLOUTUS.D MALWARE VARIANT USED IN U.S.-BASED ATM JACKPOTTING ATTACKS

Ecuador Bank Says It Lost $12 Million in Swift 2015 Cyber Hack

U.S. Man Residing in Costa Rica Pleads Guilty for Role in Two Separate Multi-Million Dollar Fraud Schemes
UNDERSTANDING THE SPANISH-LANGUAGE UNDERGROUND
State of Cybercrime in LATAM

- Growing cybercriminal communities
- Increased internet penetration in LATAM
- Low security awareness
- Weak or nonexistent cybercrime legislation
The Spanish-Speaking World
What is the “Underground”? 

- Forums & marketplaces on Tor 
- Password protected sites 
- Private communications groups
  - Messaging applications
  - Social platforms
Spanish-Language Underground

The obvious...
- Security
- Anonymity

And the less apparent...
- Exchange of ideas
- Supply chains
- Partnerships & mentorships
- Sense of community
Spanish-Language Cybercrime

- Malicious insiders
- Call centers
- Phishing
- Online carding
## Comparisons to Other Linguistic Communities

<table>
<thead>
<tr>
<th>Spanish-Language</th>
<th>Russian-Language</th>
<th>English-Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious insiders</td>
<td>Malware</td>
<td>Malicious insiders</td>
</tr>
<tr>
<td>Call centers</td>
<td>Network compromises</td>
<td>DDoS Booter for hire</td>
</tr>
<tr>
<td>Phishing</td>
<td>Account takeover</td>
<td>Refund fraud</td>
</tr>
<tr>
<td>Online carding</td>
<td>Online carding</td>
<td>In-store carding</td>
</tr>
</tbody>
</table>

**FLASHPOINT**
Cebolla Chan 3.0
Cebolla Chan 3.0 Stats

- October 2014 – September 2016; March 2018 – Present
- 135,000 posts
- 22,000 active members
Cebolla Chan 3.0

Chatter on Cebolla Chan

- High-level activity
  - Tutorials on cybercrime
  - Recruitment of insiders
  - Sale of compromised information

- Low-level activity
  - Conspiracy theories

Tutorial on compromising RDP servers

Seeking technicians to compromise ATMs
Timeline of Activity

CEBOLLA CHAN 3.0

October 2014

September 2016

March 2018

“Adding Security Improvements”
THE INTER-CEBOLLA CHAN 3.0 PERIOD
Inter-Cebolla Chan 3.0 Period

Migration of Users to Other Forums

- Former members of Cebolla Chan 3.0 discuss what happened
- Use status from Cebolla Chan 3.0 to establish reputation in new communities
- Links are shared to new forums
Inter-Cebolla Chan 3.0 Period

New “Cebolla Chans”

- Emergence of new “Cebolla Chans”
- At least five Cebolla Chan spin-offs
- Gain many followers very quickly
Inter-Cebolla Chan 3.0 Period

New Platforms

- Other communications platforms continue to gain popularity
- Better for mobile communications
Instability is rampant

- A carding forum has gone offline and changed domain three times in one year
- New iteration of Cebolla Chan run by scammers
- Major darkweb forum loses all user information
- Cebolla Chan 3.0 reemerges after 1.5 years
The Underground as a Hydra

- Spanish-language underground is unstable and unpredictable
- Multiple forums and communication platforms keep it alive
- To seriously disrupt this arena, multiple platforms must disappear at once
Persistence

ACTOR MIGRATION AS COMMUNITIES DISAPPEAR & APPEAR

- Cebolla Chan 3.0
- Cebolla Chan 4.0
- Libertor
- Cebolla Cafe

Year:
- 2016
- 2017
- 2018
Key Takeaways

- Understand your exposure to Spanish-language cybercrime
  - Review threat exposure to partners and subsidiaries in the region
  - Take inventory of servers and other infrastructure
  - Monitor web traffic from Spanish-speaking countries

- Combat low security awareness
  - Implement rigorous security training for all employees
  - Embed security analysts with your partners in the region

- Gain visibility into Spanish-language underground
  - Monitor and respond to changes in the underground
  - Identify the threat actors targeting your organization
  - Hire Spanish-speakers to ensure accurate understanding of threats
QUESTIONS?

Liv Rowley

olivia@flashpoint-intel.com