

# RSA® Conference 2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: HT-F01

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

**Liv Rowley**

Intelligence Analyst  
Flashpoint





# Latin America in the News

**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**

RSA® Conference 2018



# UNDERSTANDING THE SPANISH-LANGUAGE UNDERGROUND

# Spanish-Language Underground

## State of Cybercrime in LATAM

- Growing cybercriminal communities
- Increased internet penetration in LATAM
- Low security awareness
- Weak or nonexistent cybercrime legislation





# Spanish-Language Underground

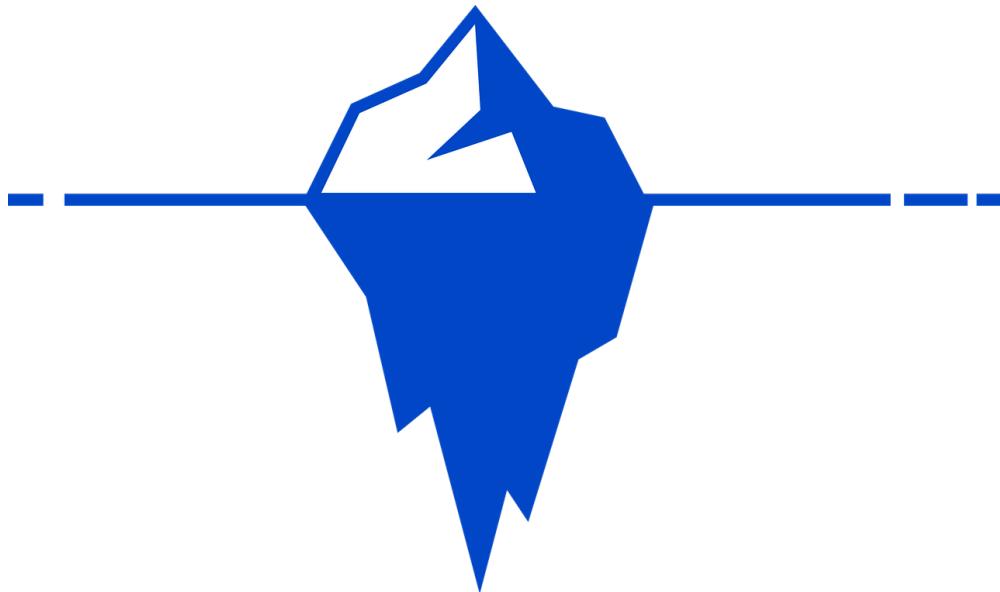
## The Spanish-Speaking World



# Spanish-Language Underground

## What is the “Underground”?

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





# Spanish-Language Underground

## The obvious...

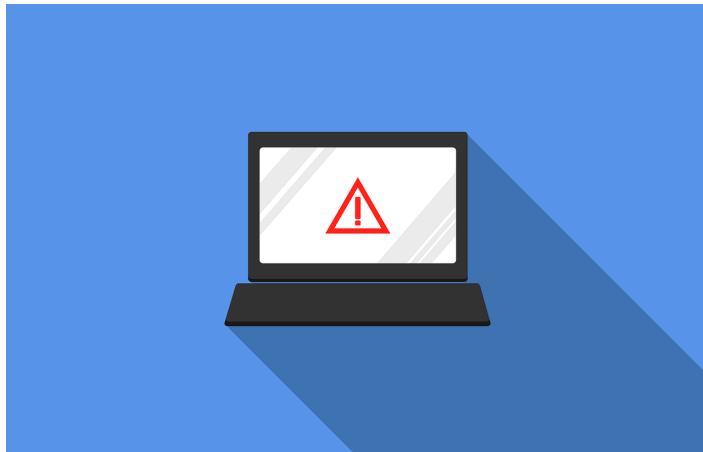
- Security
- Anonymity

## 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

## Spanish-Language

- Malicious insiders
- Call centers
- Phishing
- Online carding

## Russian-Language

- Malware
- Network compromises
- Account takeover
- Online carding

## English-Language

- Malicious insiders
- DDoS Booter for hire
- Refund fraud
- In-store carding

RSA® Conference 2018



**CEBOLLA CHAN 3.0**



# Cebolla Chan 3.0

Facebook.com/DuckVideos

Hola, Invitado! [Iniciar sesión](#) [Registrarse](#)

Cebolla Chan 3.0

DUCKVIDEOS

Temas Mensajes

Bienvenid@s a Cebolla Chan v.3.0 (Páginas: 1 2 3 4 ... 9)

SystOp

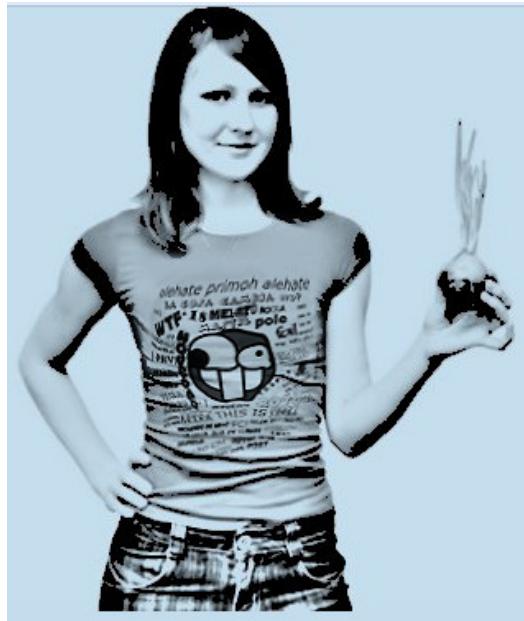
Tema / Autor	Resuestas	Vistas	Puntuación
<b>Temas importantes</b>			
↳ <a href="#">Bienvenid@s a Cebolla Chan v.3.0 (Páginas: 1 2 3 4 ... 9)</a> <small>SystOp</small>	85	86,884	★★★★★
<b>Temas normales</b>			
↳ <a href="#">Encierro metete me urge mucho ayudame</a> <small>Anonymous The Hacker</small>	0	163	★★★★★
↳ <a href="#">Necesito una pagina que de numeros de tarjetas de credito Colombia</a> <small>rachinaro258</small>	1	255	★★★★★
↳ <a href="#">consejos y links utiles para novatos y personas en general, que disfruten la deep web</a> <small>quoldime</small>	44	64,700	★★★★★
↳ <a href="#">link usa citizenship</a> <small>chachalaco</small>	0	112	★★★★★
↳ <a href="#">Liberar telefonos android</a> <small>AlbaCumbidebre</small>	2	592	★★★★★
↳ <a href="#">Iphone y samsung bloqueados</a> <small>modd</small>	1	159	★★★★★
↳ <a href="#">Ayuda en el tema mecumbe</a> <small>AnonymousTheHacker</small>	0	234	★★★★★
↳ <a href="#">Ayuda para novatos sobre BTC</a>	1	1,997	★★★★★



# 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

[REDACTED] on May 17, 2016 13:03 UTC

Hola! Soy [REDACTED]... ([REDACTED] en la cleanweb) para los que no me conocen llevo 9 años en el carding y en el hacking.. recien termine de hacerles un video donde muestro paso a paso de principio a final como hackear escritorios remotos.

Tutorial on compromising RDP servers

[REDACTED] on September 10, 2016 16:58 UTC

Buscamos tecnicos para montar dispositivos y montar vacios... Solo gente seria que sea o conozca un tecnico ... para toda america latina menos Colombia... pueden dejarme MP o agregararme a mi icq [REDACTED].. saludos...

Seeking technicians to compromise ATMs



## Timeline of Activity

### CEBOLLA CHAN 3.0



RSA® Conference 2018

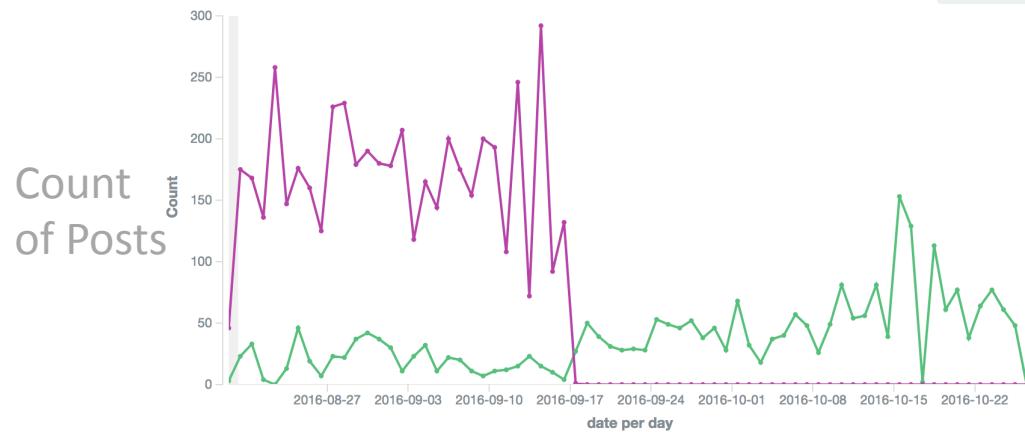


## THE INTER-CEBOLLA CHAN 3.0 PERIOD

# 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



Date per day

# Inter-Cebolla Chan 3.0 Period

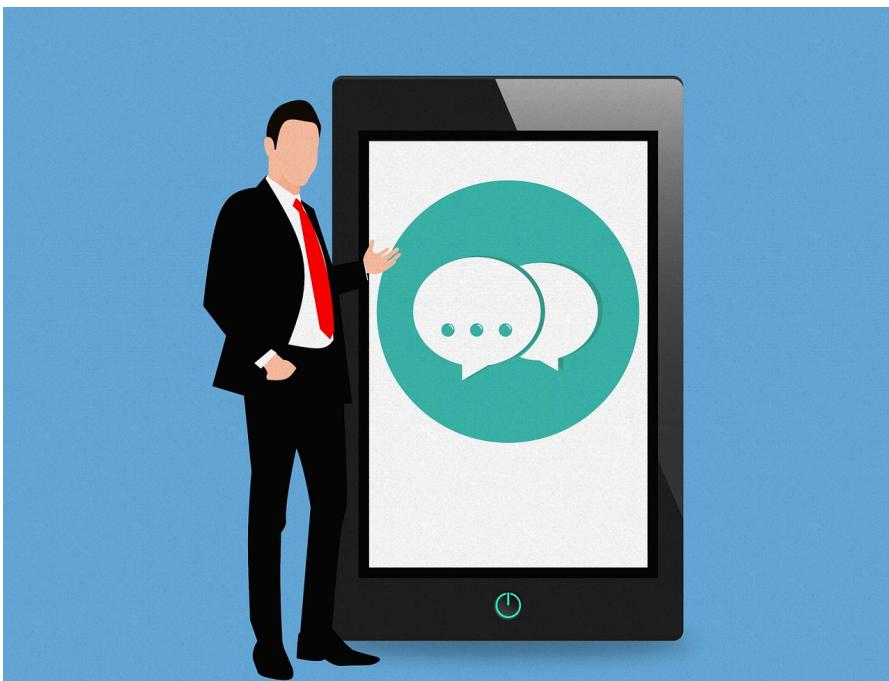
## New “Cebolla Chans”

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



## New Platforms

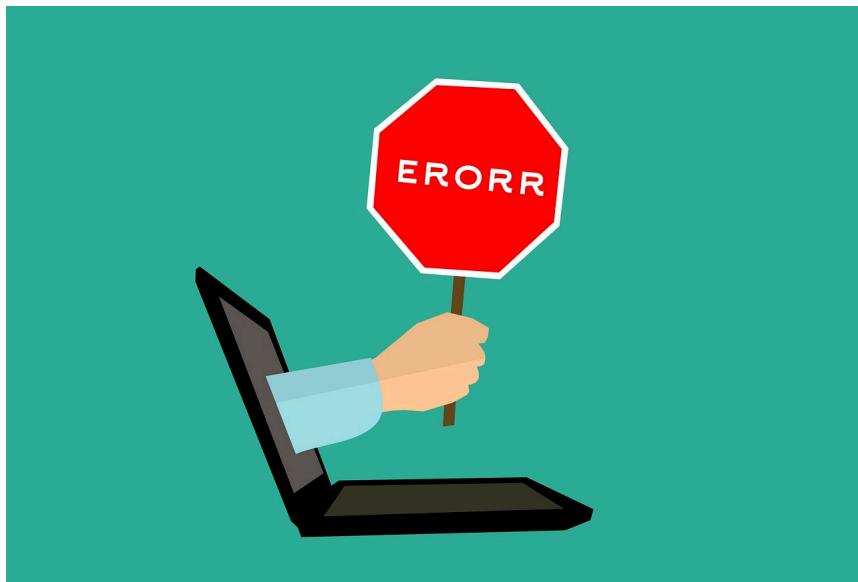
- Other communications platforms continue to gain popularity
- Better for mobile communications



# Spanish-Language Underground

## 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



# Spanish-Language Underground



## 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





# 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

RSA® Conference 2018



## QUESTIONS?

Liv Rowley

[olivia@flashpoint-intel.com](mailto:olivia@flashpoint-intel.com)