

El valor de la información: desafíos frente al Ransomware

Fabián Zambrano Smith
Director Regional SOC Digiware

[El valor de la información]

TECH
JAN 9 2017, 11:51 AM ET

Ransomware: Now a Billion Dollar a Year Crime and Growing

by HERB WEISBAUM

Security experts say hackers deploying ransomware have been extorting money from computer users of all stripes.  Patrick Lux / Getty Images

SHARE

 Share

 Tweet

 Email

 Print

Ransomware payments for 2016 are expected to hit a billion dollars, according to the FBI. That compares to just \$24 million paid in 2015.

And it's expected to get even worse this year — with more victims and more money lost.

Experts even predict that the cloud could come under attack this year because it's such a lucrative target and could result in ransom payments in the millions of dollars.

Ransomware is a family of malware that blocks access to a PC, server or mobile device, or encrypts all the data stored on that machine. It's typically

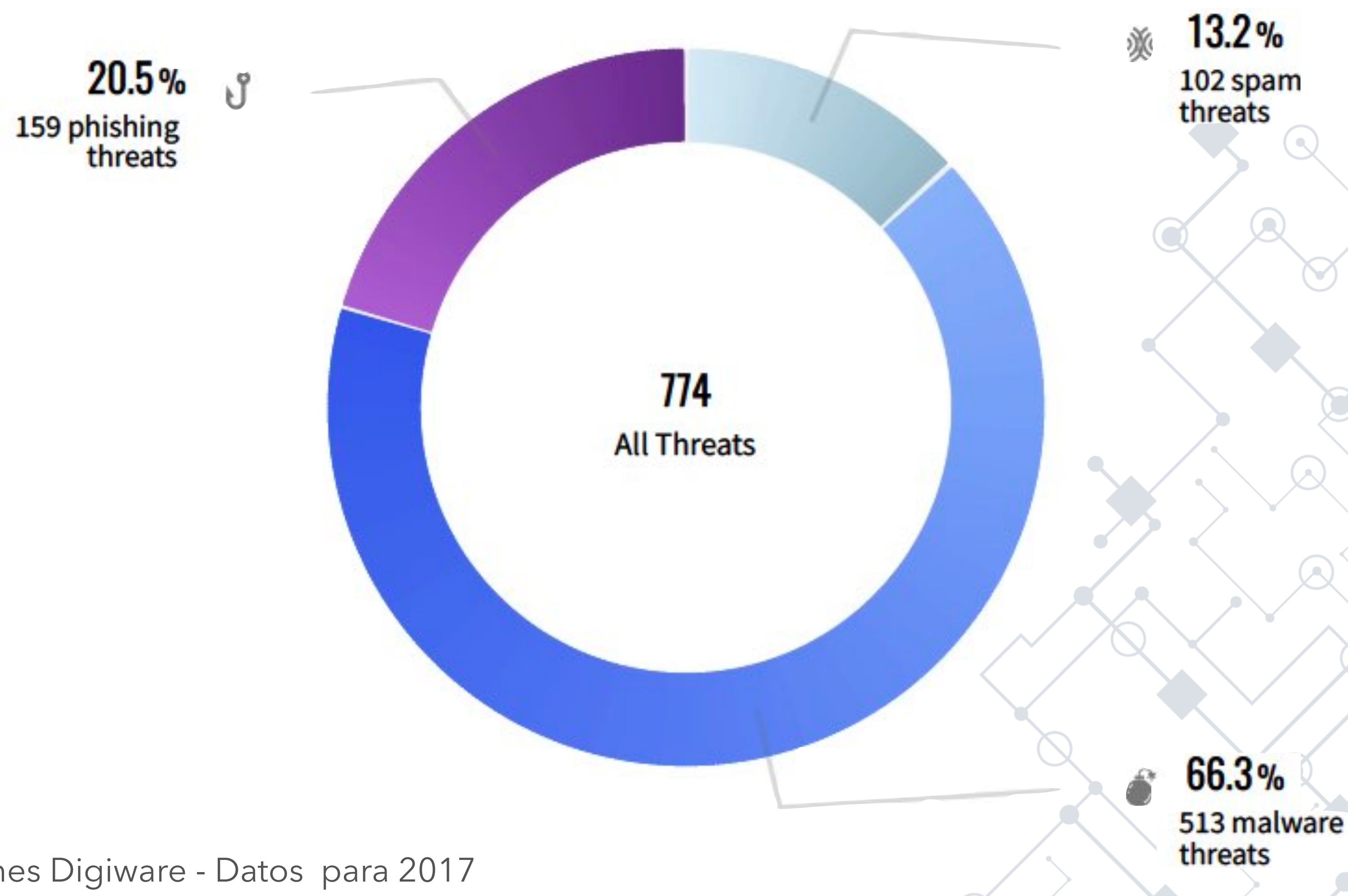
From the Web

Sponsored Links



McDonald's sales top forecasts after promotions push

Distribución de tipos de amenazas - participación promedio/mes 2017



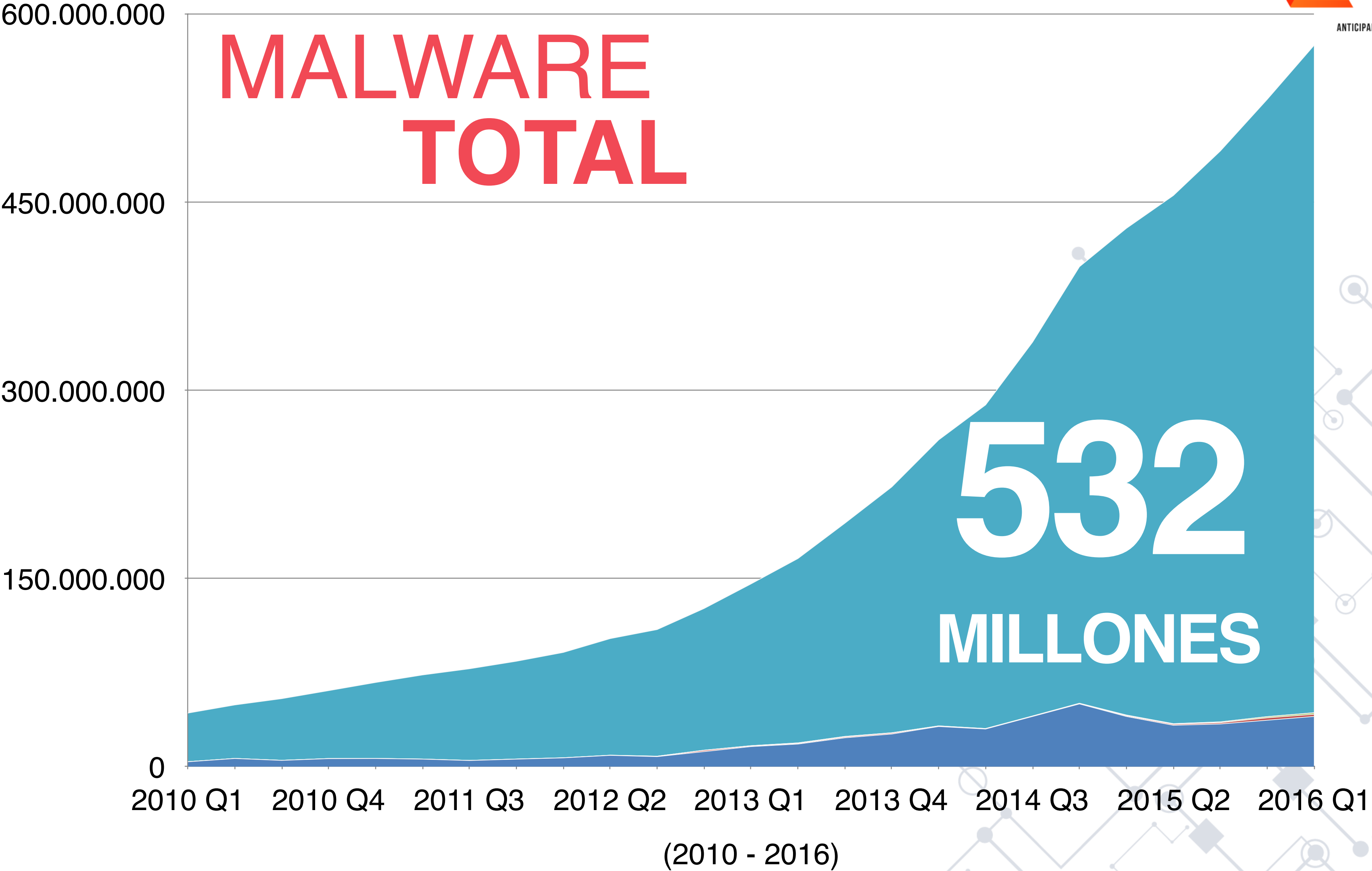
[La problemática del Malware

“No puede existir un **antivirus** que detecte todas los posibles **virus** de computador”

Fred Cohen sobre el
Antivirus - 1987.

Fuente McAfee.

MALWARE TOTAL



[

60.000.000

■ Malware

■ Mobile

■ Ransomware

■ Macros

MALWARE

6,000!!

NUEVAS CEPAS

3000
por min.

45.000.000

30.000.000

15.000.000

0
2010 Q1 2010 Q4 2011 Q3 2012 Q2 2013 Q1 2013 Q4 2014 Q3 2015 Q2 2016 Q1

[

FIRMAS = HASH

MD5/SHA1/SHA256

5d0ffbc8389f27b0649696f0ef5b3cfe

32B x 530M = **16.9G**

COMPRESION!

100:1

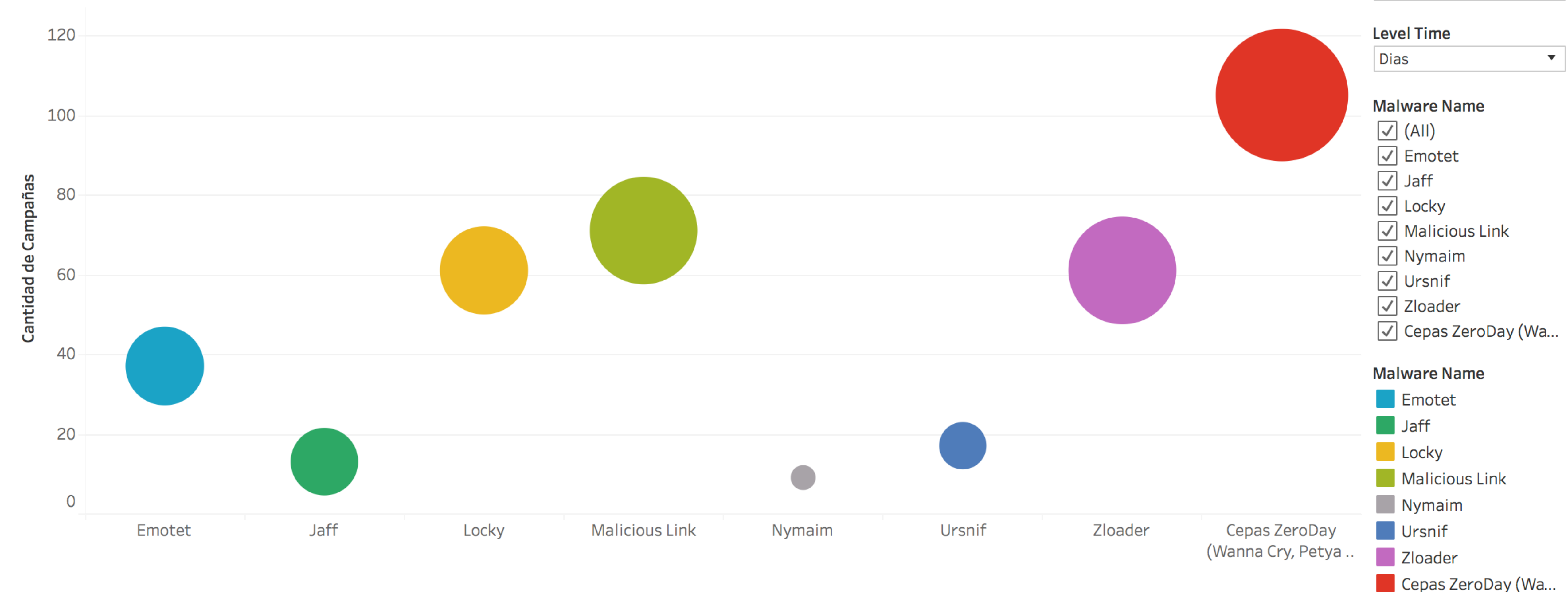
16.9Gb = 169Mb

100Gb = 1Gb

1Tb = 10Gb!

Detalle de Campañas

Camapañas por Malware



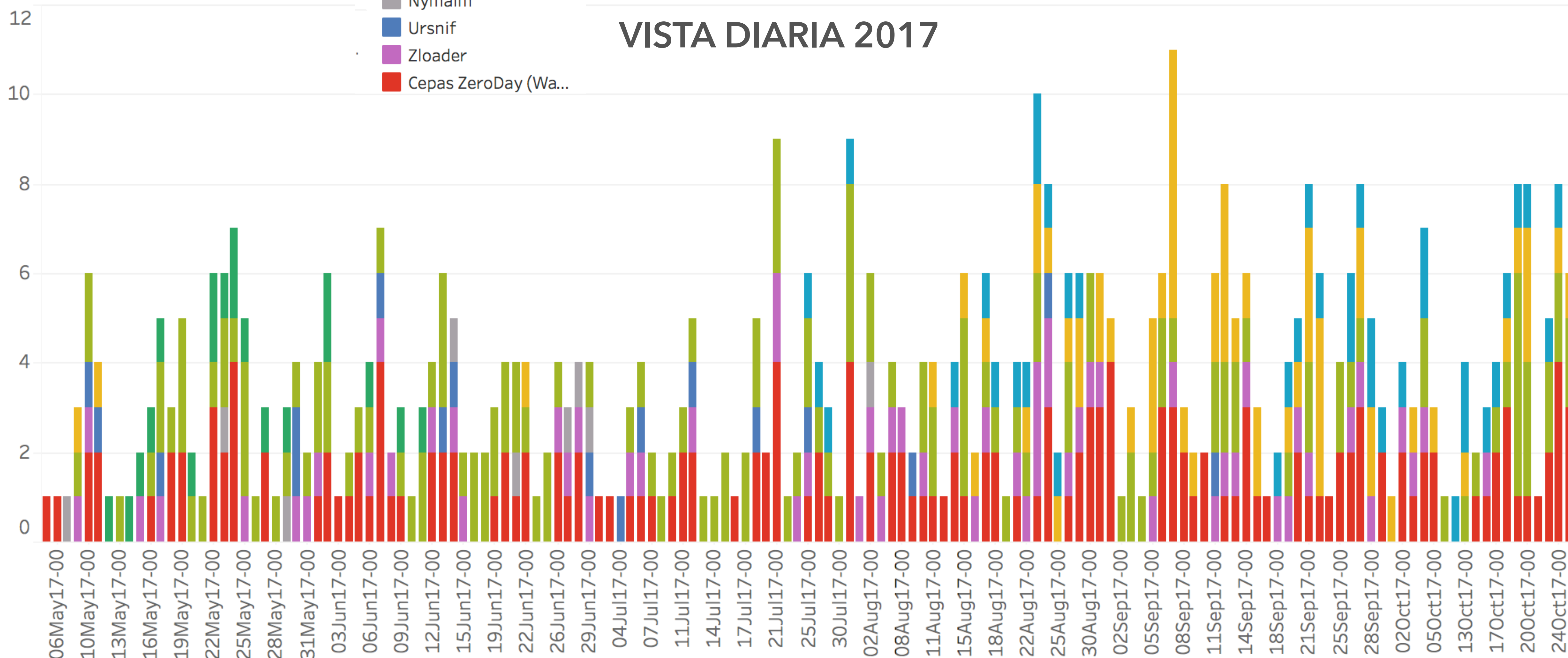
Camapañas pór Periodo

Malware Name

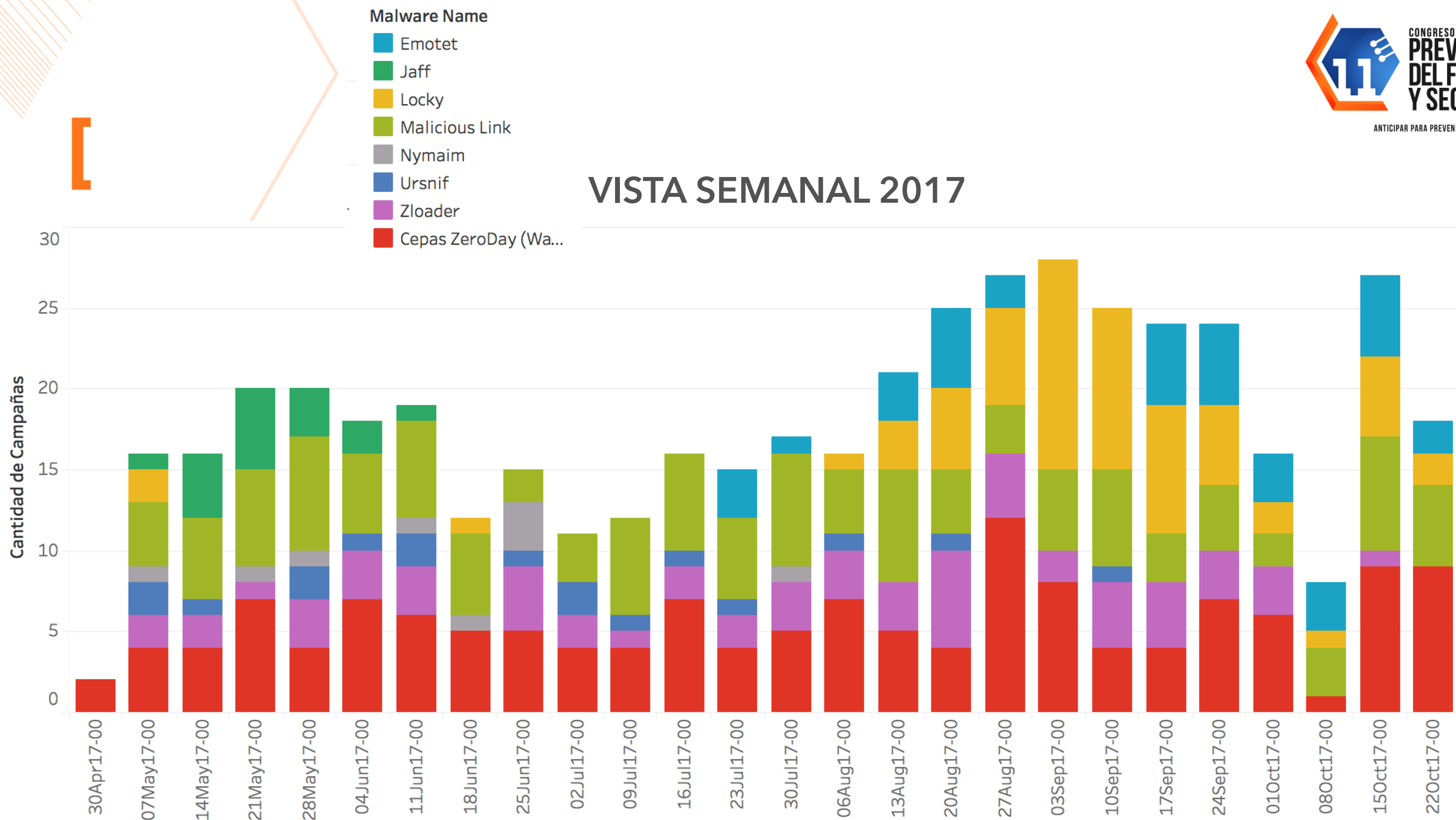
- Emotet
- Jaff
- Locky
- Malicious Link
- Nymaim
- Ursnif
- Zloader
- Cepas ZeroDay (Wa...)

VISTA DIARIA 2017

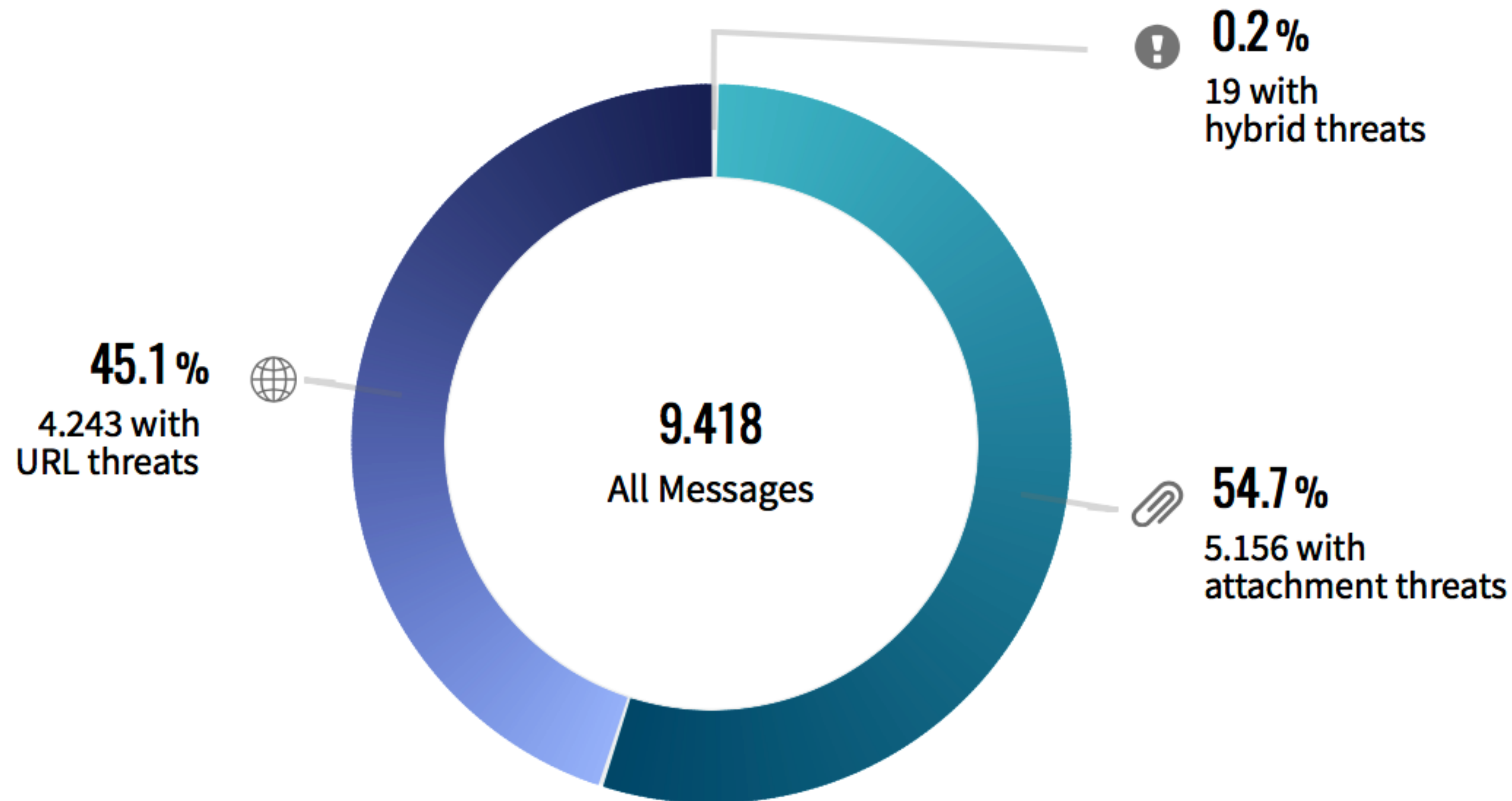
Cantidad de Campañas



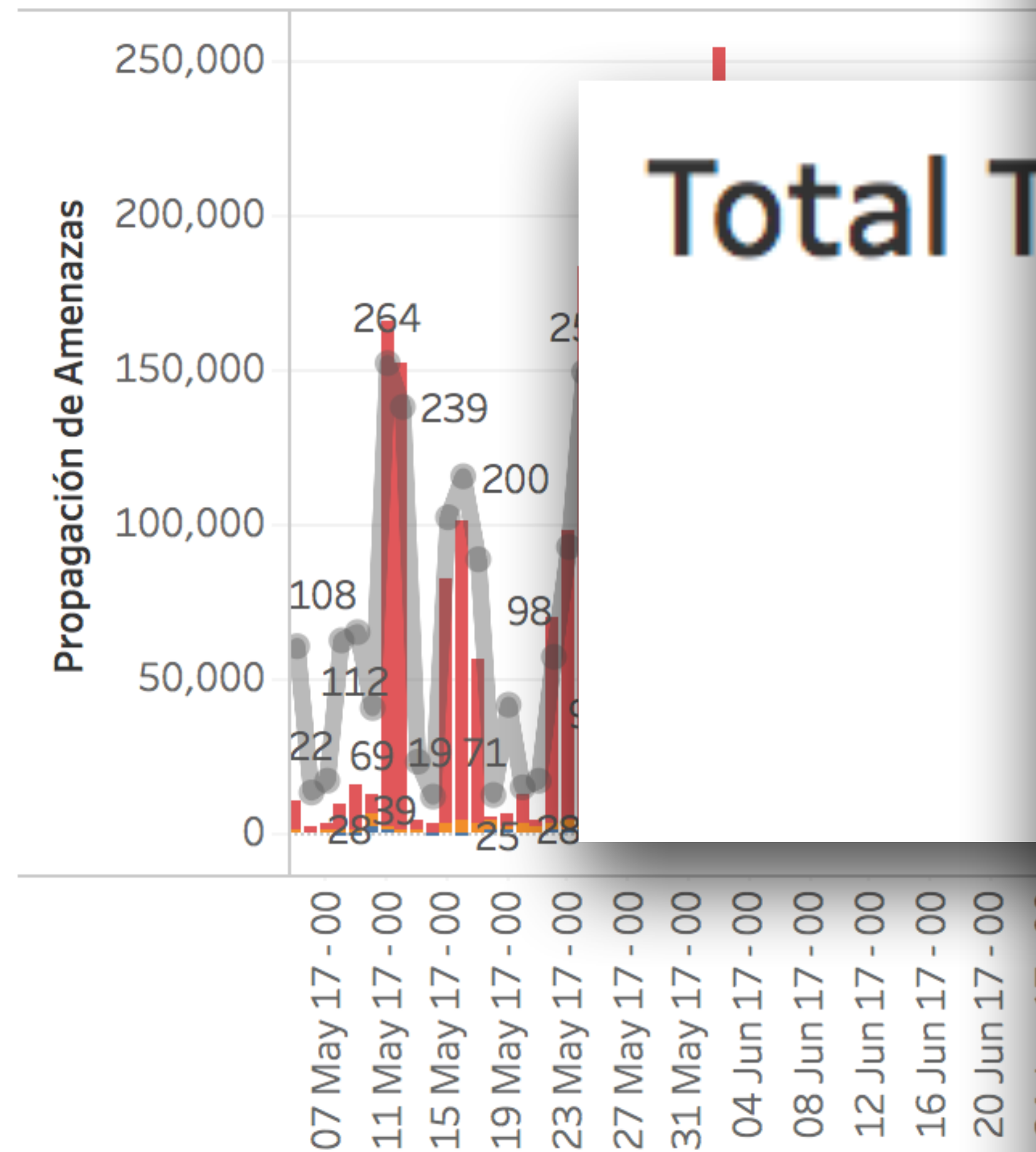
VISTA SEMANAL 2017



Familias de ataque por día



TimeLine Activity



Messages

Blocked

Delivered

% Messages Block..

Delivered Message

Not Rewritten

Rewritten

Clicks

Clicks Blocked

Clicks Permitted

Users

Intended Use

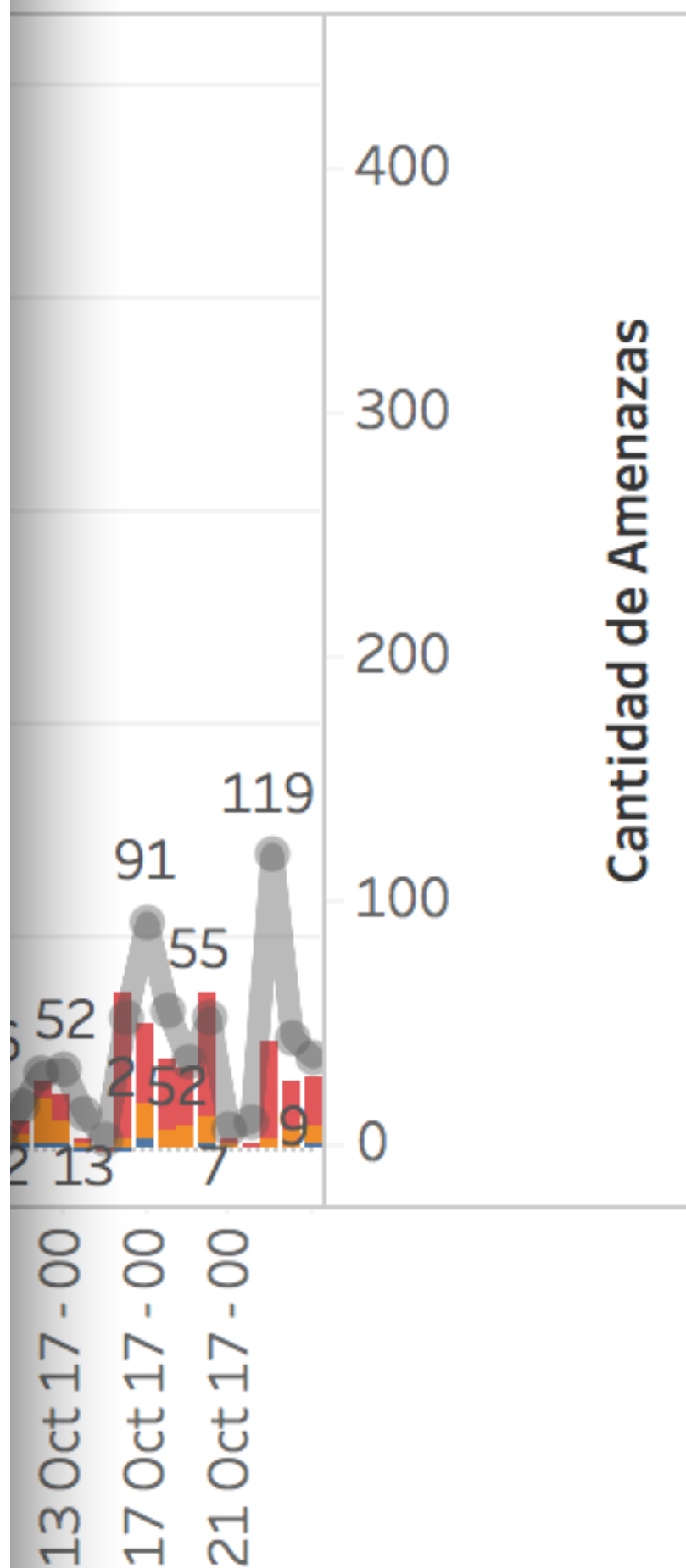
Impacte Users

At Risk Users

**Se recibe un
ataque por
usuario al día**

**5.1% del total de
usuarios son
objetivo de ataque
persistente**

**Al menos cada 27
días un usuario
será impactado**



[x

- **Seguridad basada en DNS**
- **Aislamiento de entornos Endpoint (VDI)**
- **EndPoint Detection and Response (EDR)**
- **Parchado Virtual**
- **Reescritura URL dentro de los correos (URL Messages Rewritten)**