Panorama de las amenazas informáticas en México y Latinoamérica

Camilo Gutiérrez Amaya

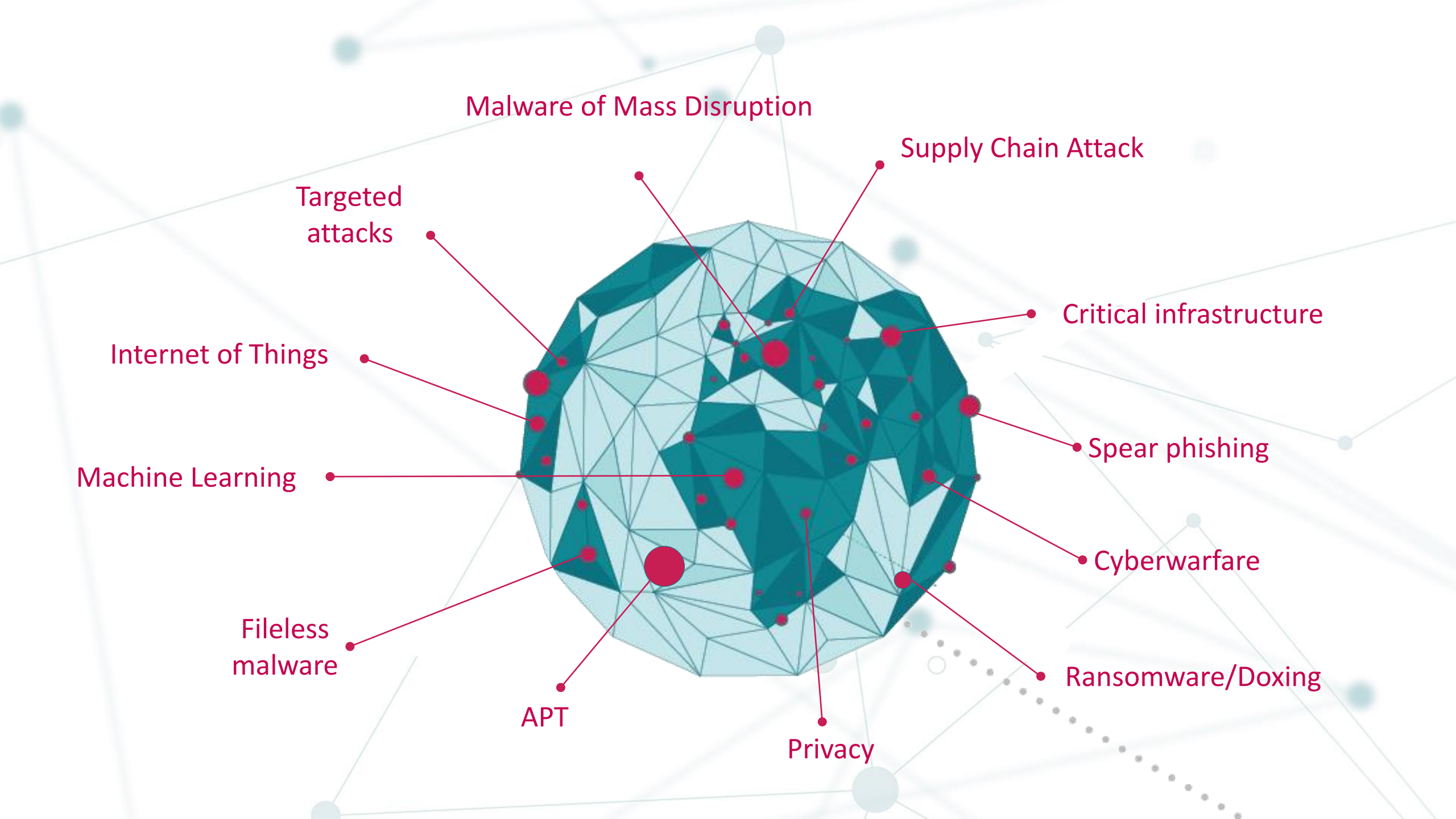
Jefe del Laboratorio de Investigación ESET

Miguel Ángel Mendoza

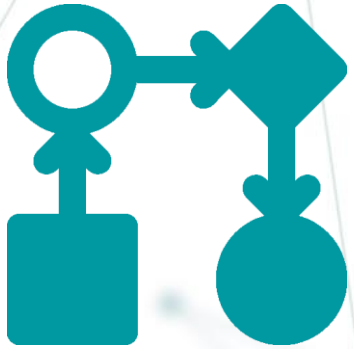
Investigador de Seguridad ESET

UNAM CERT

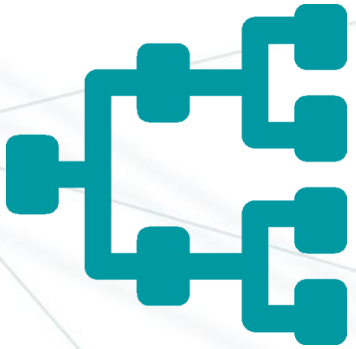
DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN


Malware of Mass Disruption
Supply Chain Attack
Targeted attacks
Critical infrastructure
Internet of Things
Spear phishing
Machine Learning
Cyberwarfare
Fileless malware
Ransomware/Doxing
APT
Privacy

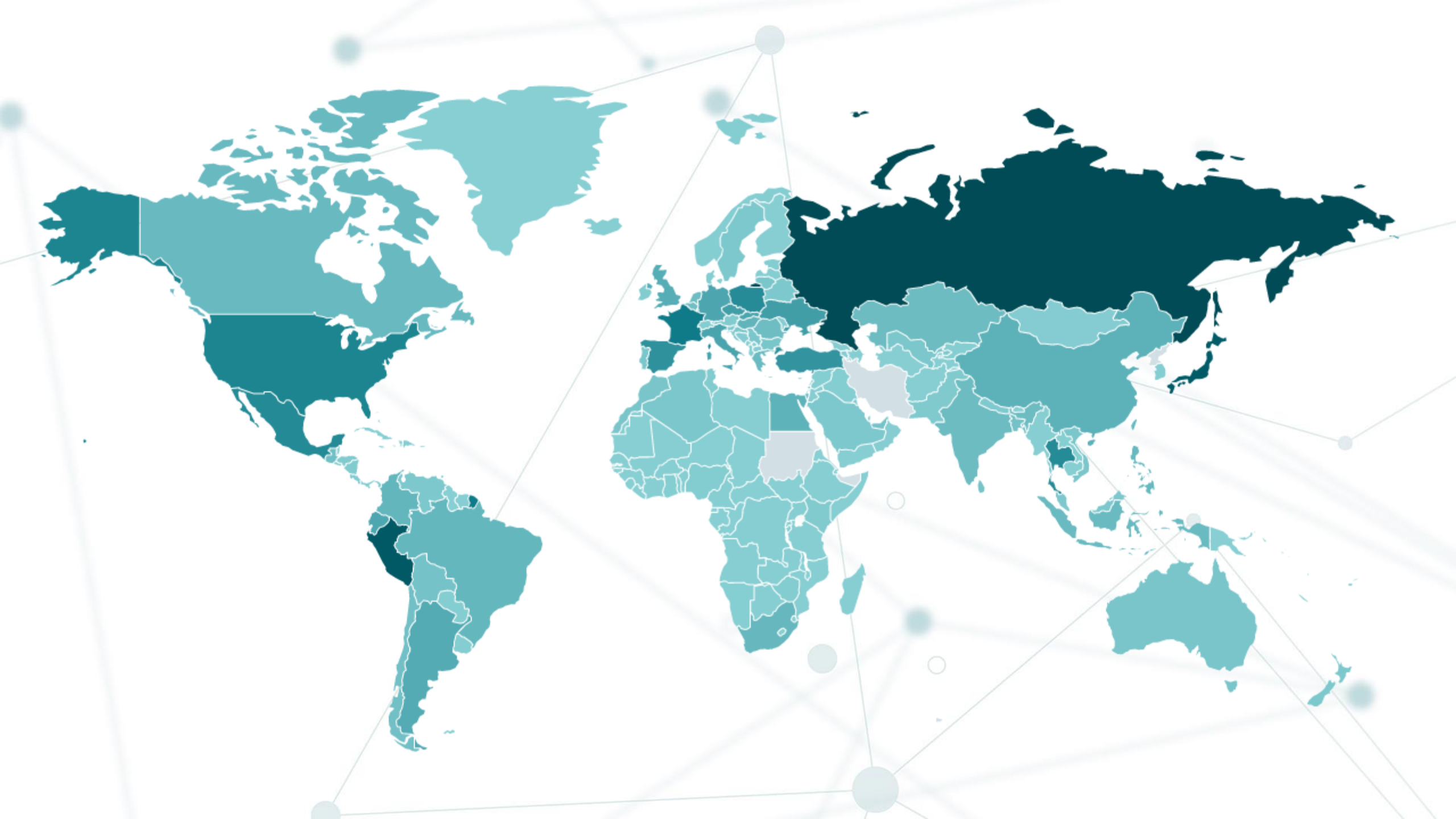
Cantidad



Complejidad



Diversidad

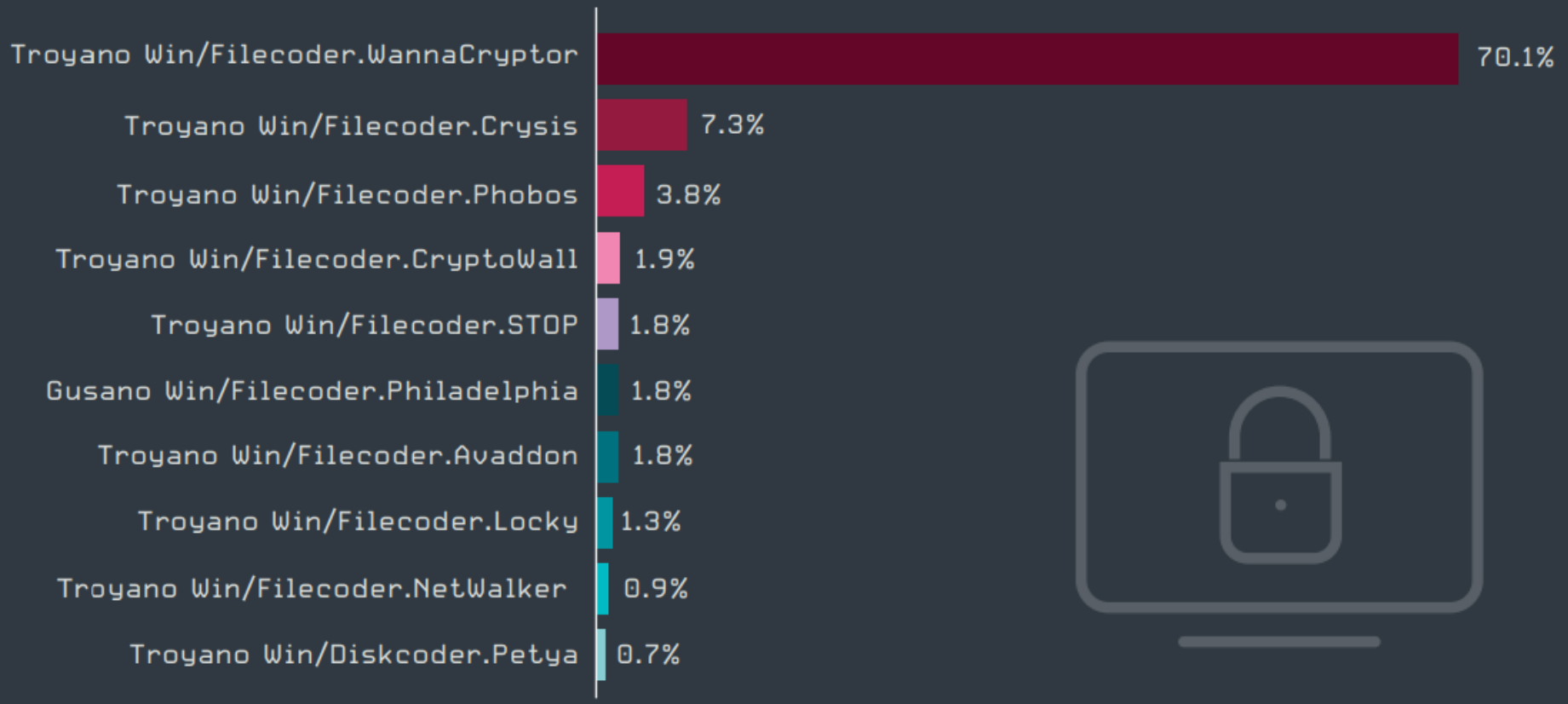



INFORME DE AMENAZAS
2020

Ransomware

Los desarrolladores de ransomware pertenecen a grupos organizados y combinan el secuestro de información con doxing.

Ransomware en Latinoamérica (Q3 2020)



welivesecurity BY ESET

Ransomware y filtración de información: una tendencia que se consolidó en 2020

La práctica extorsiva de filtrar la información secuestrada en caso de no realizar el pago del rescate comenzó a verse en la en la última parte del 2019 y se consolidó en los primeros meses del 2020 como una modalidad adoptada por varias familias de ransomware.

Instituciones de gobierno

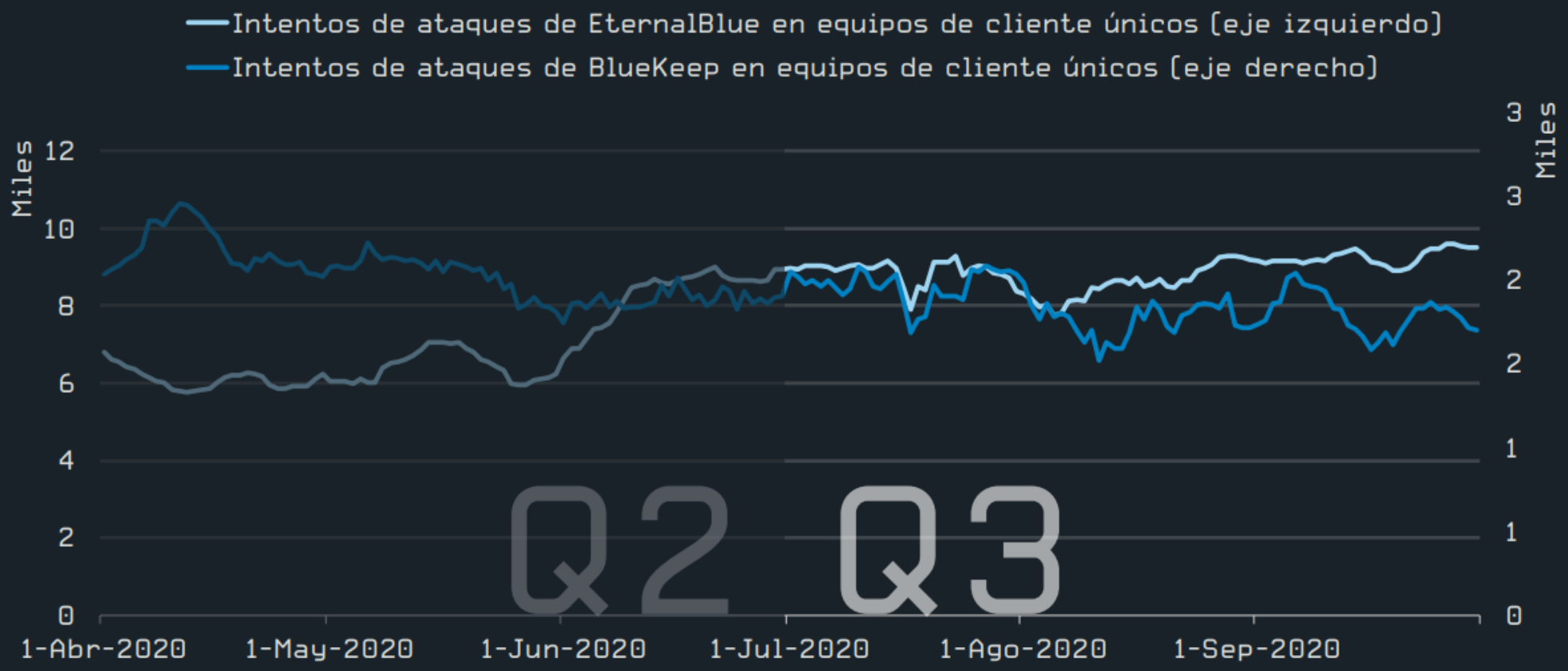
Instituciones educativas

Instituciones de salud

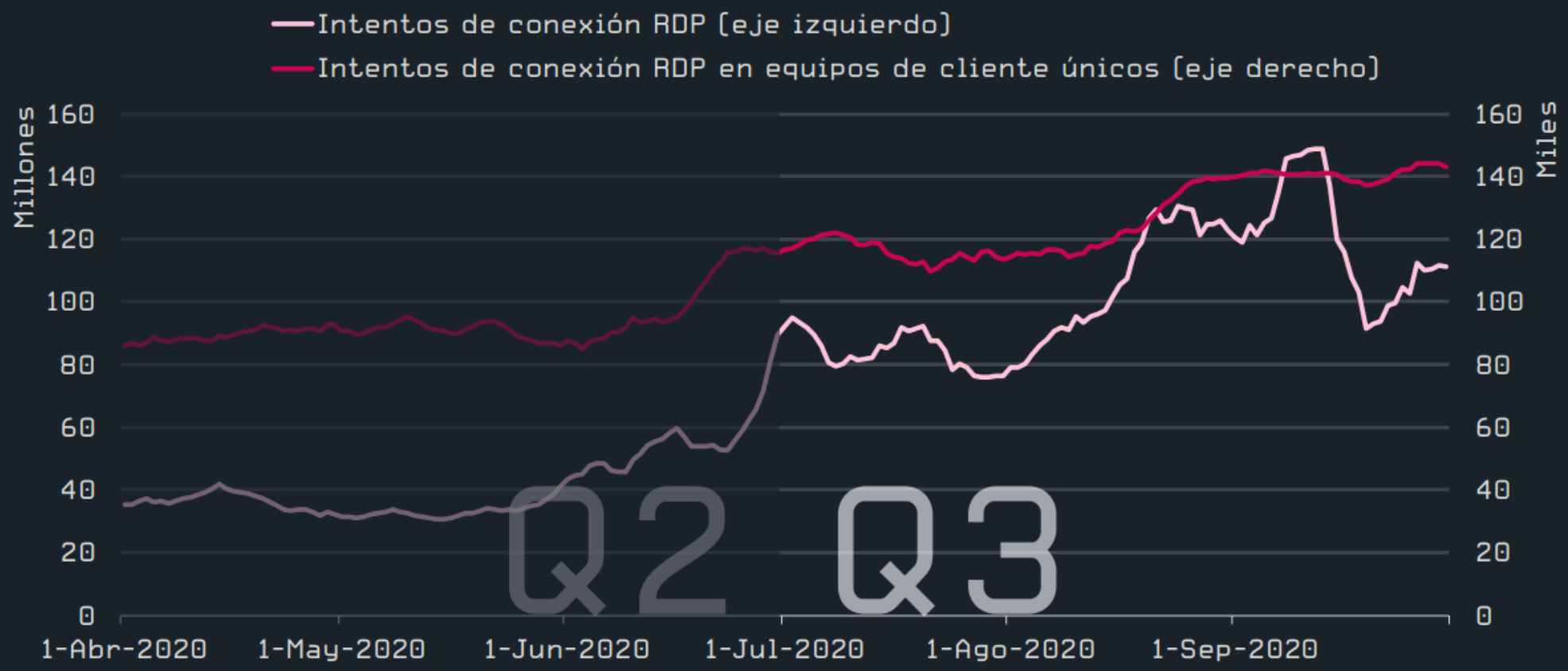
Exploits

La explotación de vulnerabilidades está representada principalmente por EternalBlue y BlueKeep.

Detecciones de EternalBlue y BlueKeep

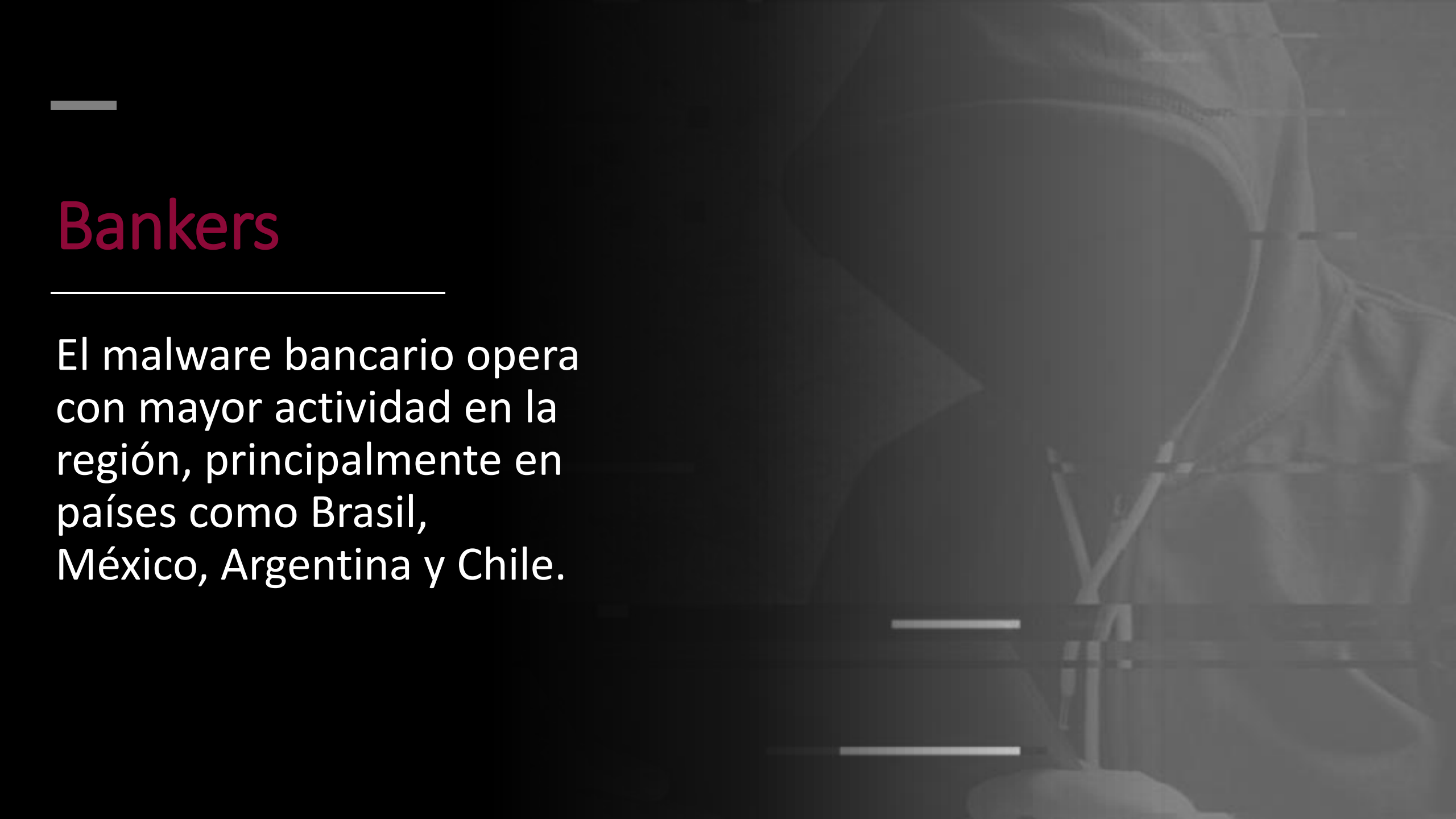


Ataques de fuerza bruta a RDP

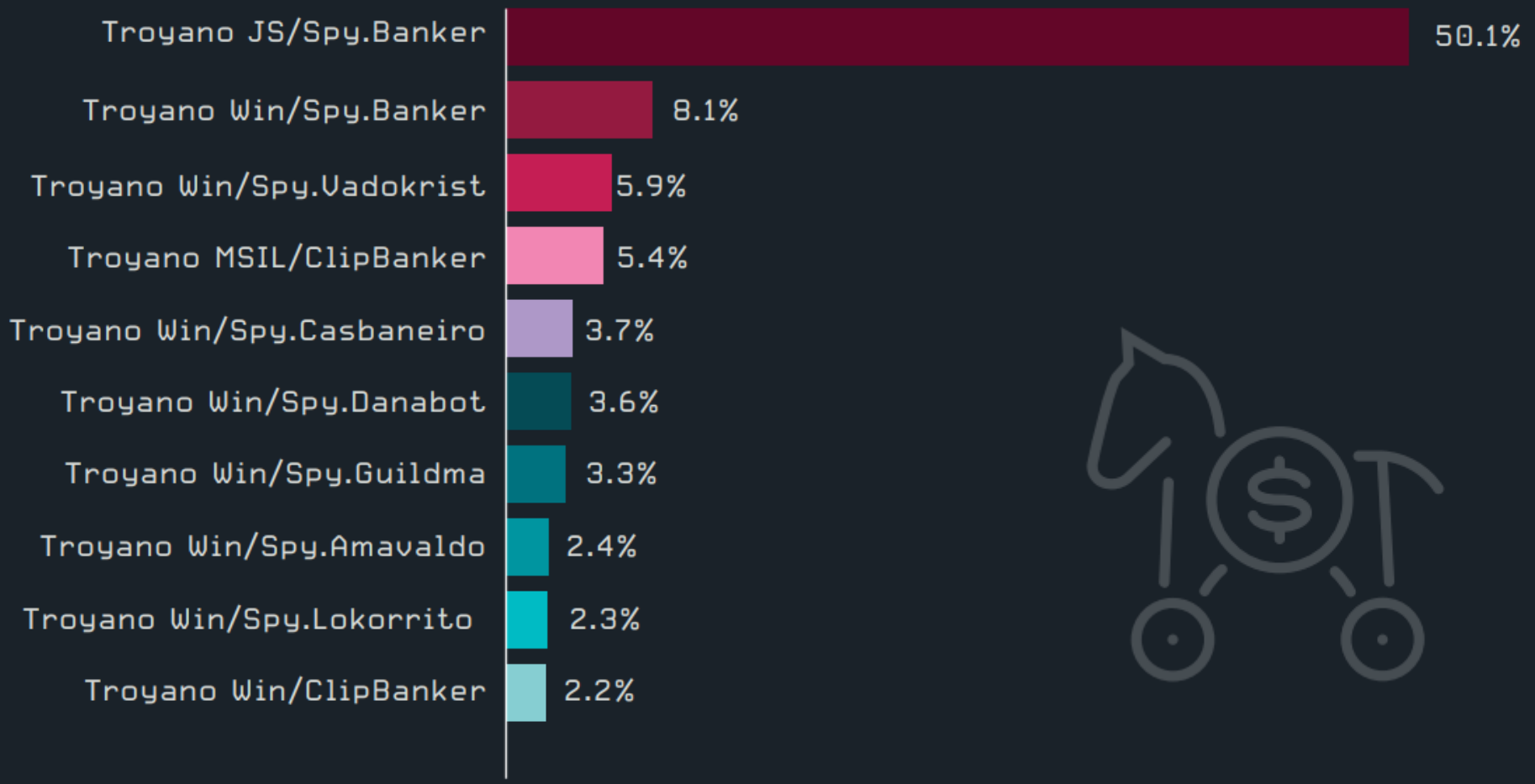


Bankers

El malware bancario opera con mayor actividad en la región, principalmente en países como Brasil, México, Argentina y Chile.



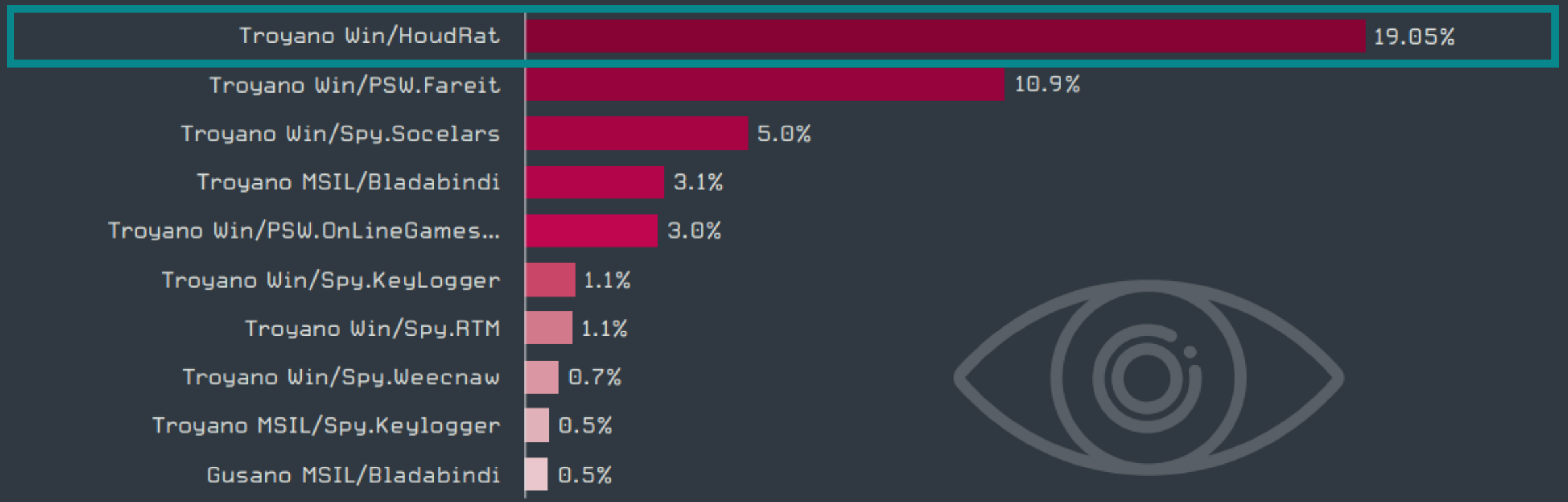
Malware bancario en LATAM (Q3 2020)



Spyware

Las “herramientas clásicas” de los cibercriminales para la extracción de información mantiene actividad constante en Latinoamérica.

Detecciones de Spyware (Q3 2020)

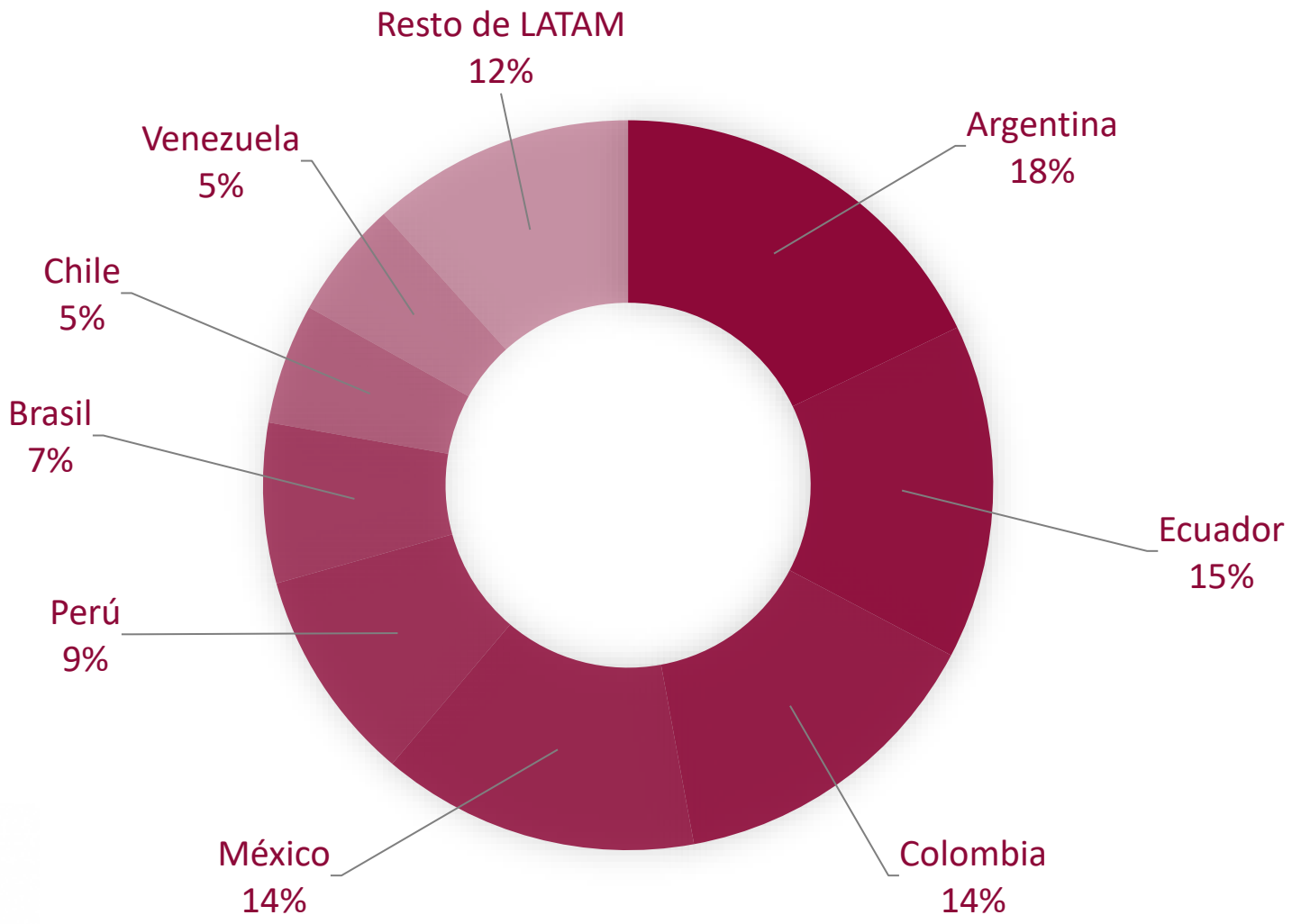


ESET participa en operación global para interrumpir Trickbot

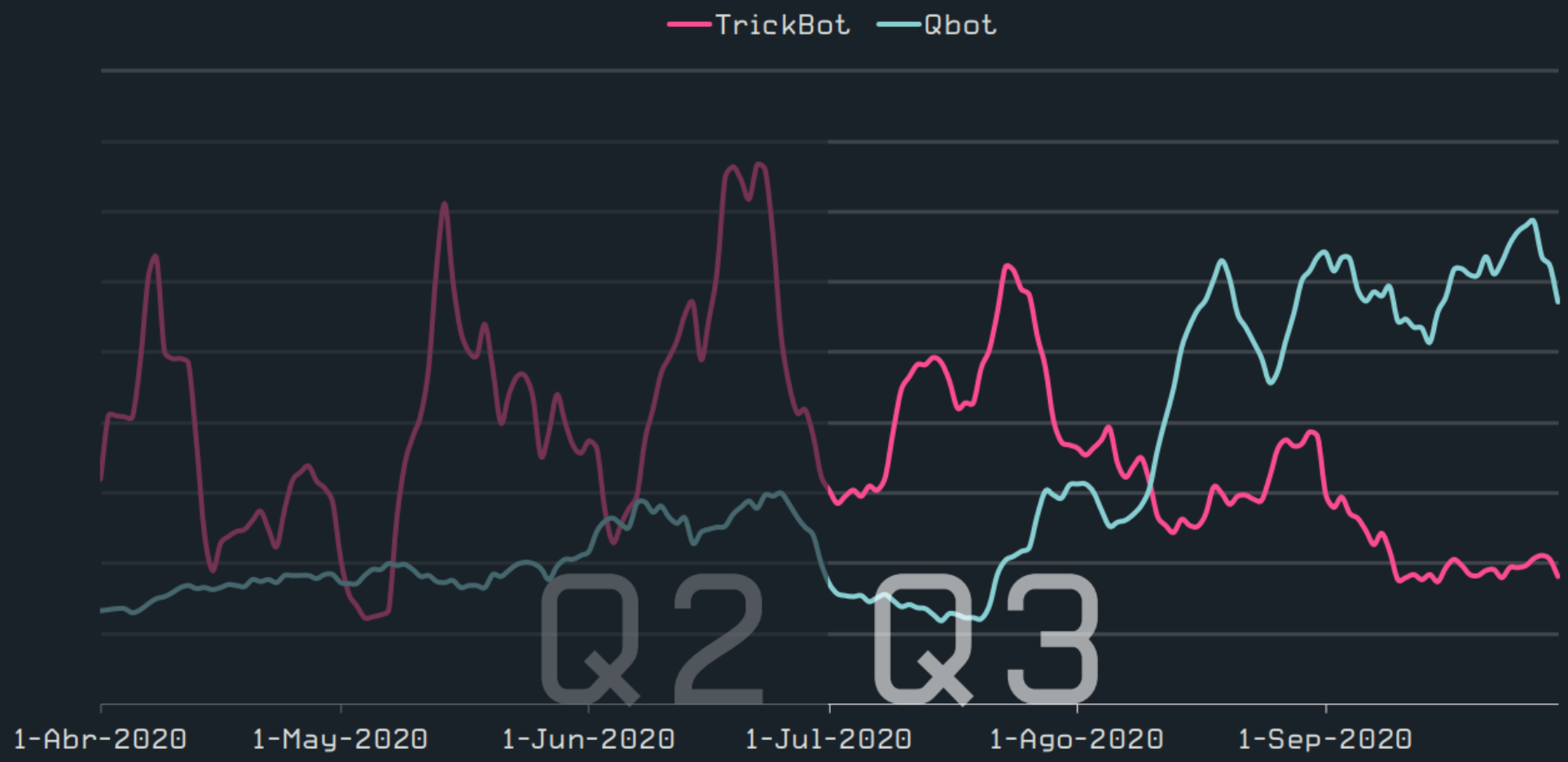
A lo largo de su monitoreo, ESET analizó miles de muestras maliciosas cada mes para ayudar en este esfuerzo por interrumpir Trickbot.

Detecciones de Trickbot en el mundo (octubre 2019 - octubre 2020)

Detecciones de Trickbot en Latinoamérica (2020)



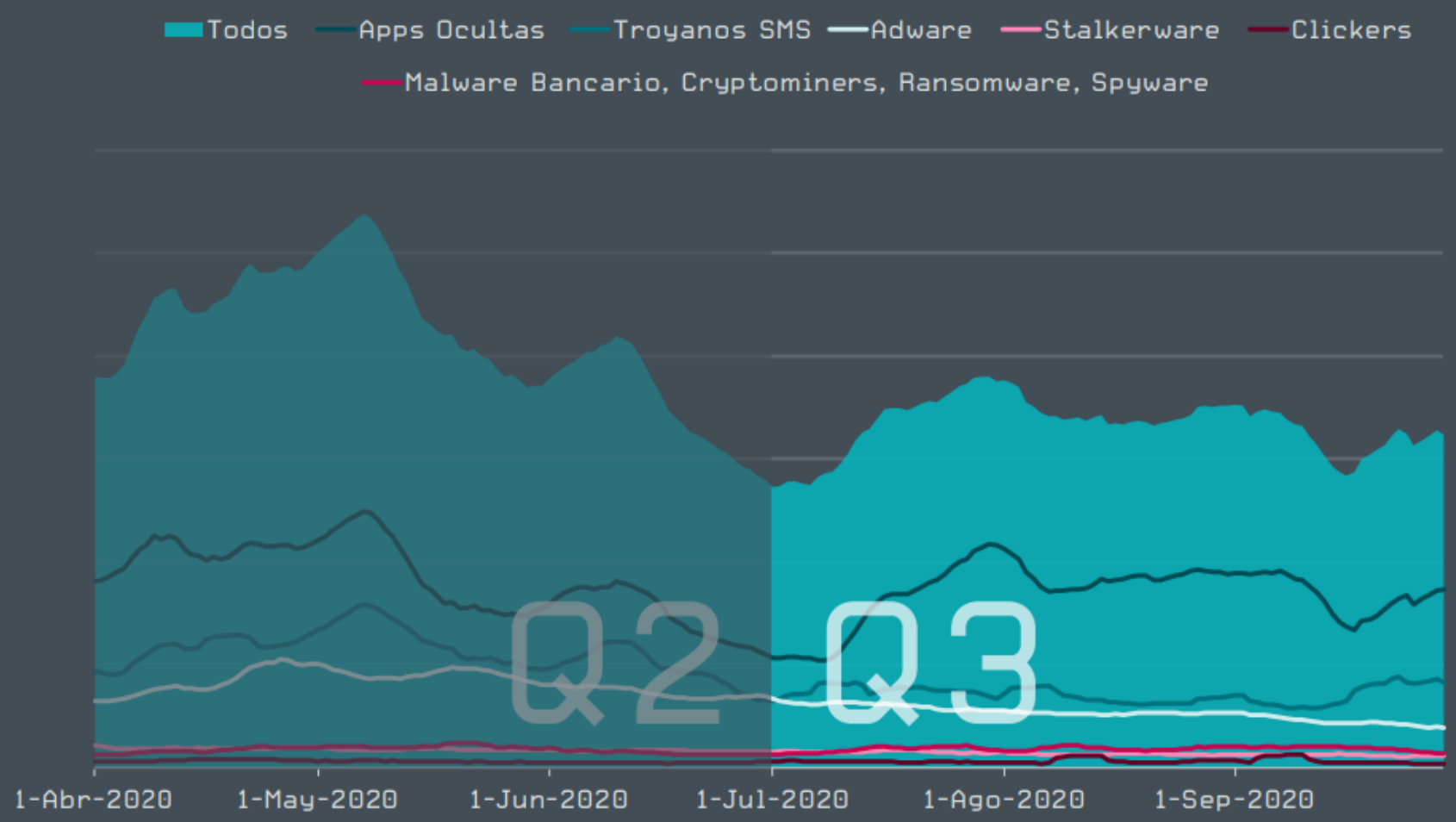
Detecciones de TrickBot y Qbot



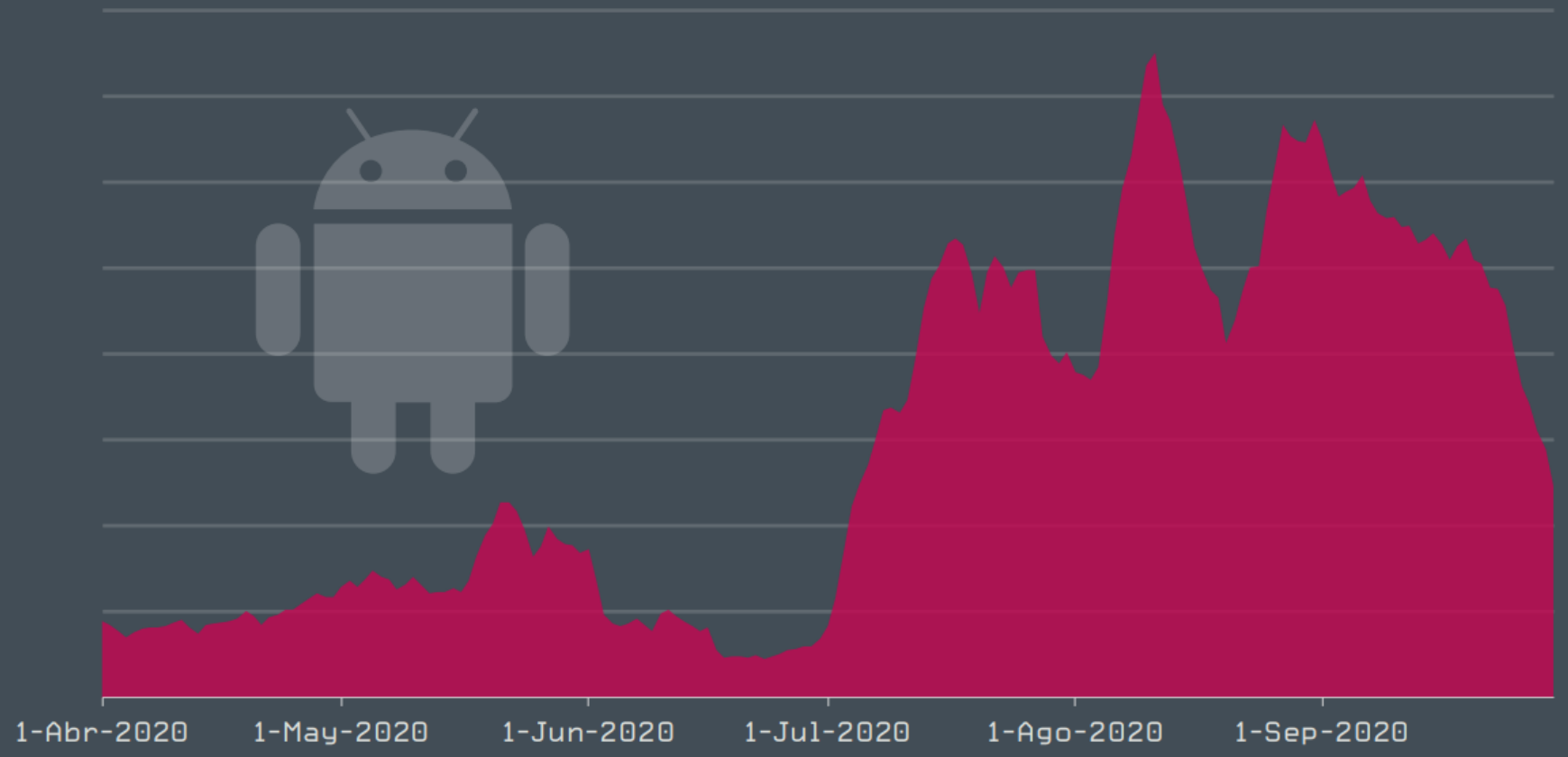
Amenazas en Android

Los dispositivos móviles se encuentran en la mira de los atacantes desde hace años; el malware bancario para Android va en aumento.

Detección de amenazas para Android



Detección de malware bancario para Android

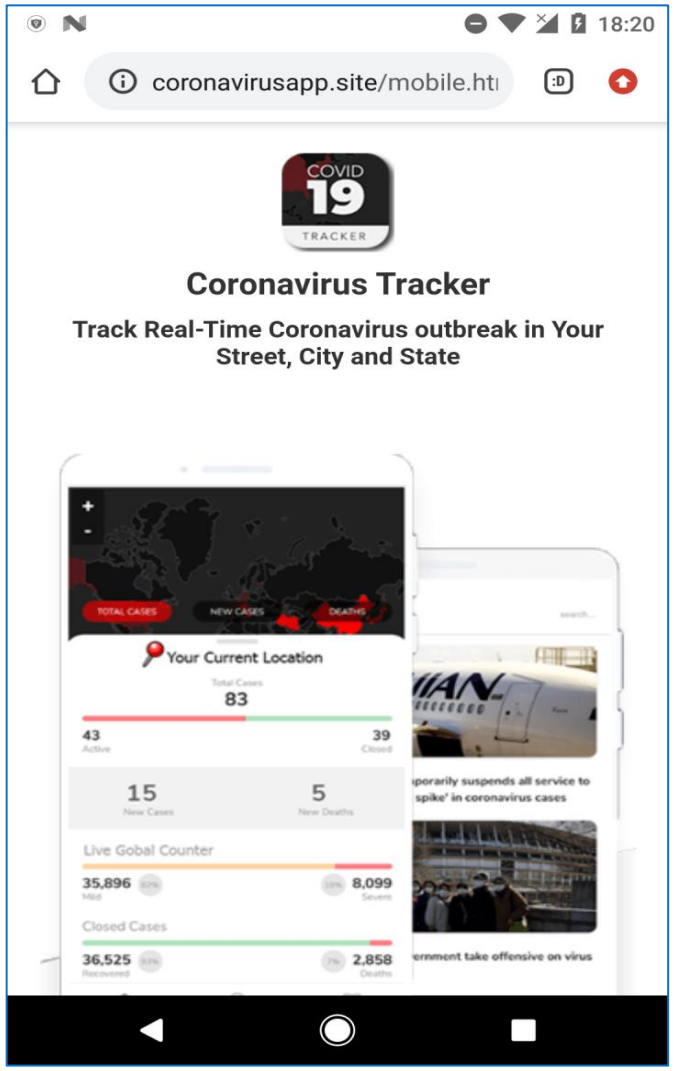


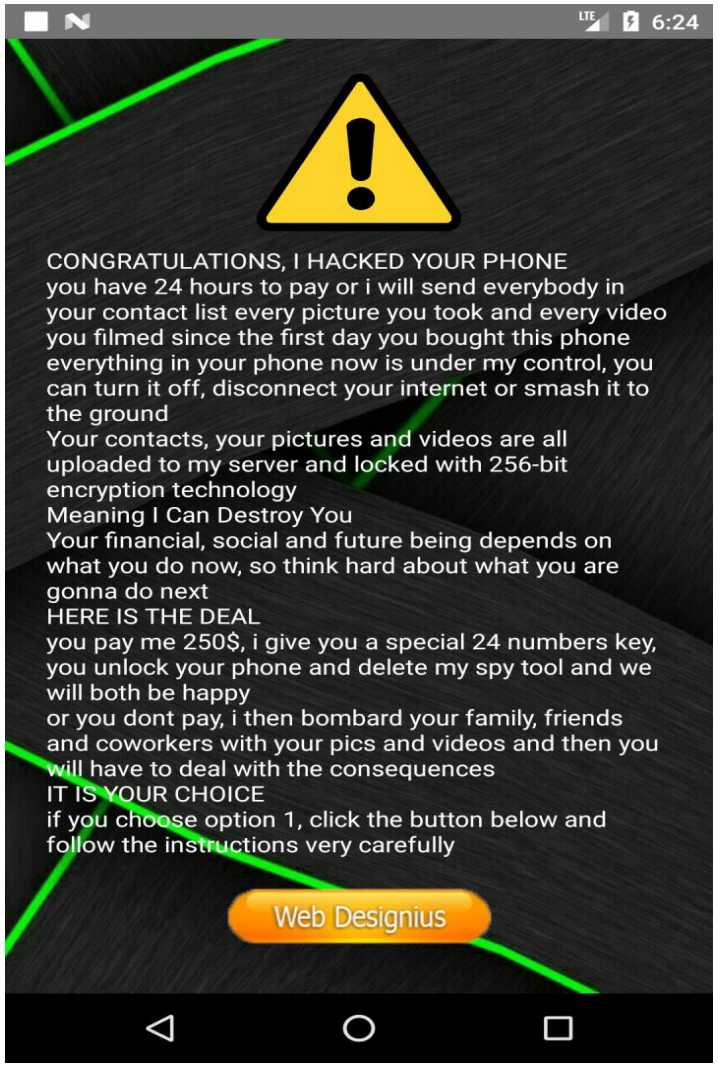
welivesecurity BY ESET

Fallos de seguridad en apps de rastreo de COVID-19 que utilizan Firebase

Tras haber identificado apps de rastreo de COVID-19 que utilizaban bases de datos Firebase y que exponían datos privados de los usuarios, compartimos algunas recomendaciones para configurarlas de manera segura.

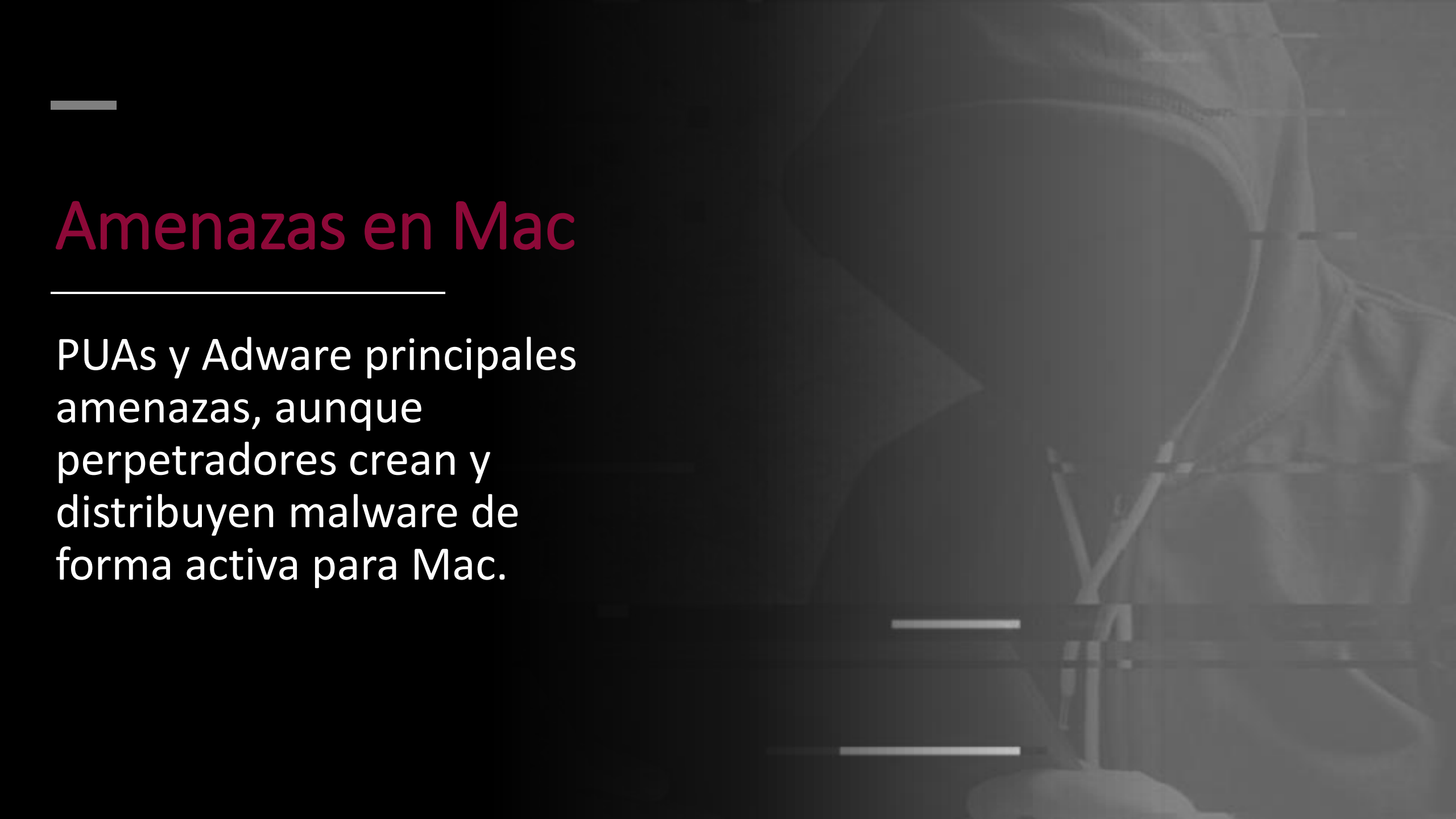
Falsas apps utilizan distribuyen malware para Android



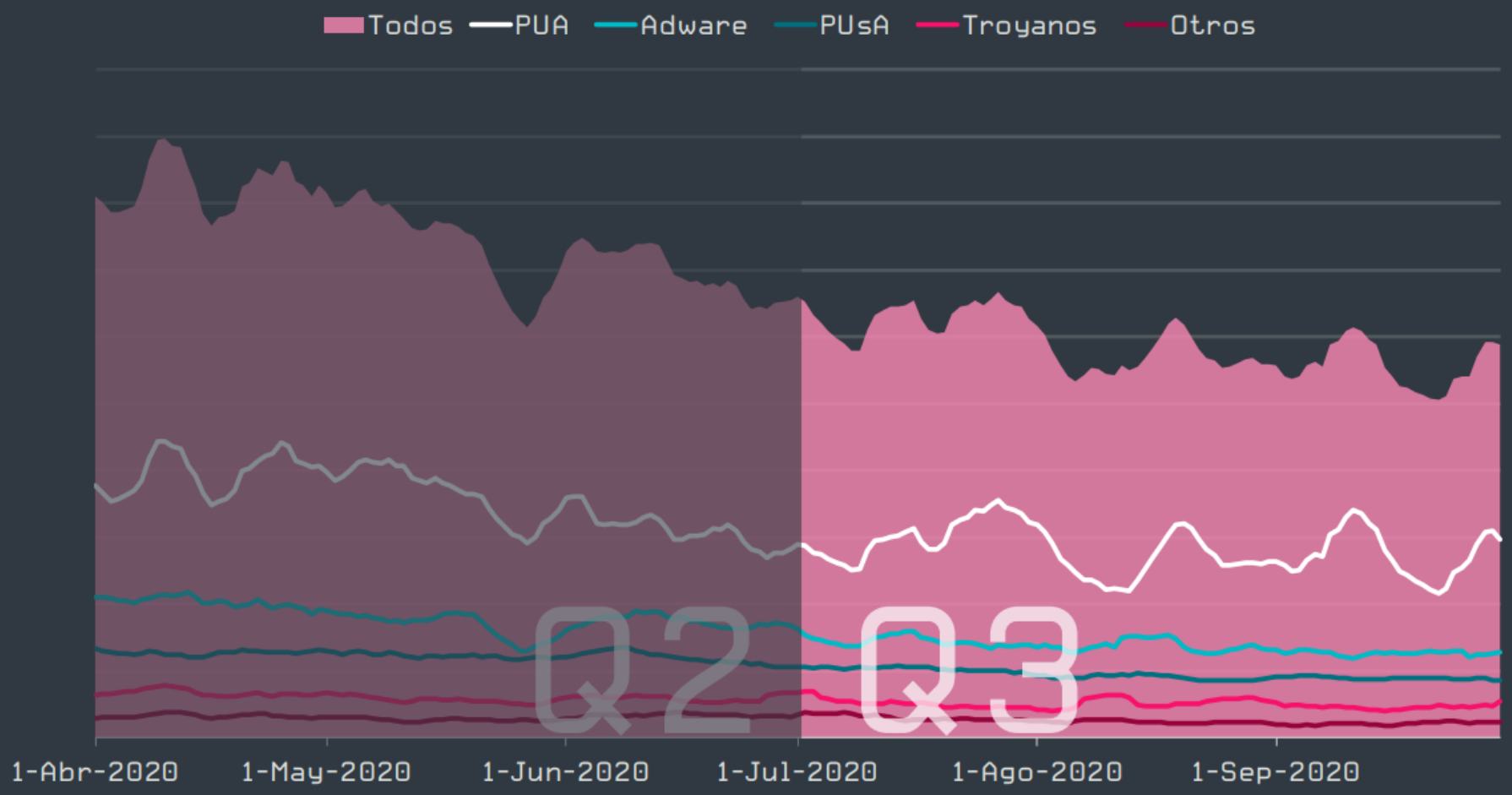


Amenazas en Mac

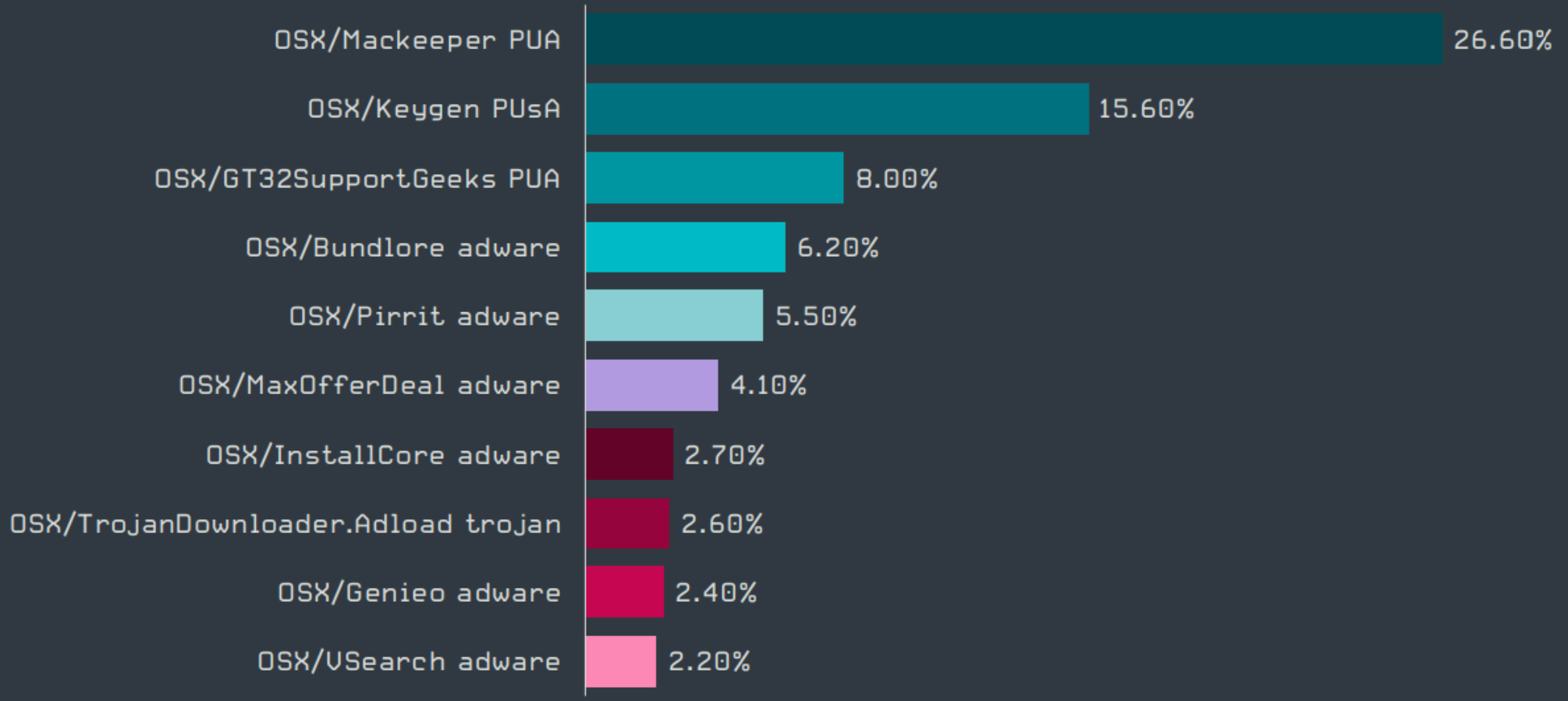
PUAs y Adware principales amenazas, aunque perpetradores crean y distribuyen malware de forma activa para Mac.



Detección de amenazas para Mac



Principales amenazas para Mac



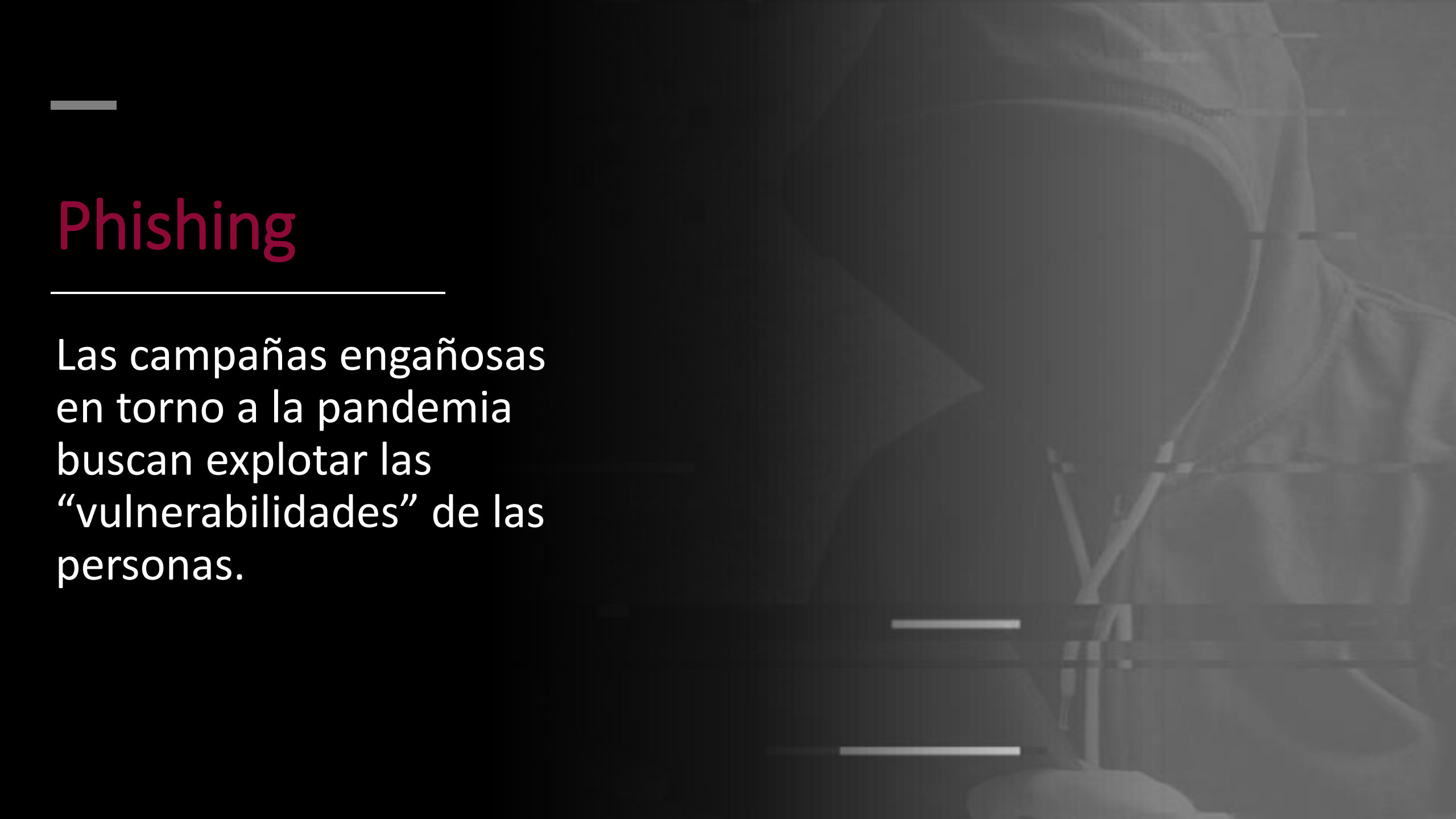
welivesecurity BY ESET

App de trading de criptomonedas para Mac es utilizada para distribuir malware

Análisis del malware GMERA y cómo a través de aplicaciones para la compra y venta de criptomonedas dirigidas a usuarios de Mac busca robar información.

Phishing

Las campañas engañosas en torno a la pandemia buscan explotar las “vulnerabilidades” de las personas.



COVID-19

ENGAÑOS

Engaño vía WhatsApp pretende hacer creer que Adidas está regalando tapabocas

El engaño suplanta la identidad de Adidas e intenta hacer creer que la marca está regalando tapabocas reutilizables. El objetivo es instalar aplicaciones no deseadas en el dispositivo de las víctimas.

Luis Lubeck 29 Sep 2020 - 02:38PM

COVID-19

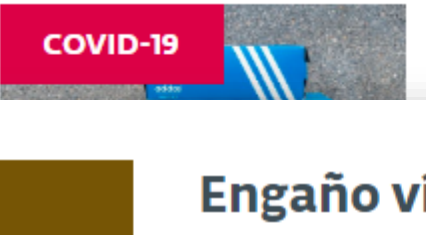
COVID-19

Ataques de DNS hijacking en routers es utilizado para descargar app maliciosa sobre COVID-19

Comprometen routers para redirigir a los usuarios a una página que ofrece una falsa app de información sobre el COVID-19 que en realidad descarga un troyano.

Juan Manuel Harán 25 Mar 2020 - 01:00PM

COVID-19



Engaño a través de WhatsApp hace creer que

9 para
patillas como
demia.

-19

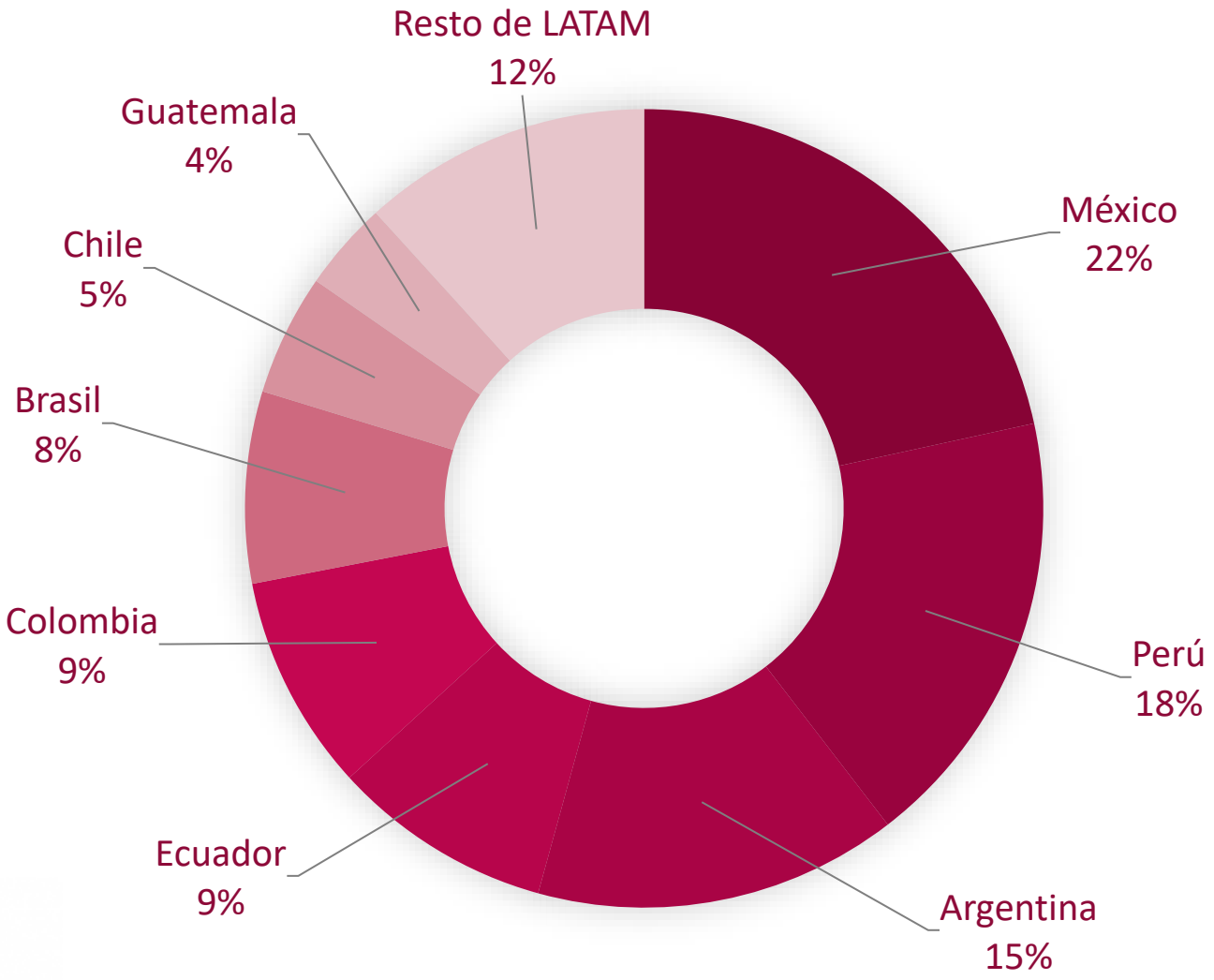
que se
ara

: nuevo engaño

vecha de la situación
plan ta la identidad de
cidad invasiva.

Luis Lubeck 24 Jun 2020 - 01:00PM

Distribución de detección en Latinoamérica (2020)



Otros recursos de información

ESET VIRUS RADAR BETA

HOME > Statistics > Top Threats

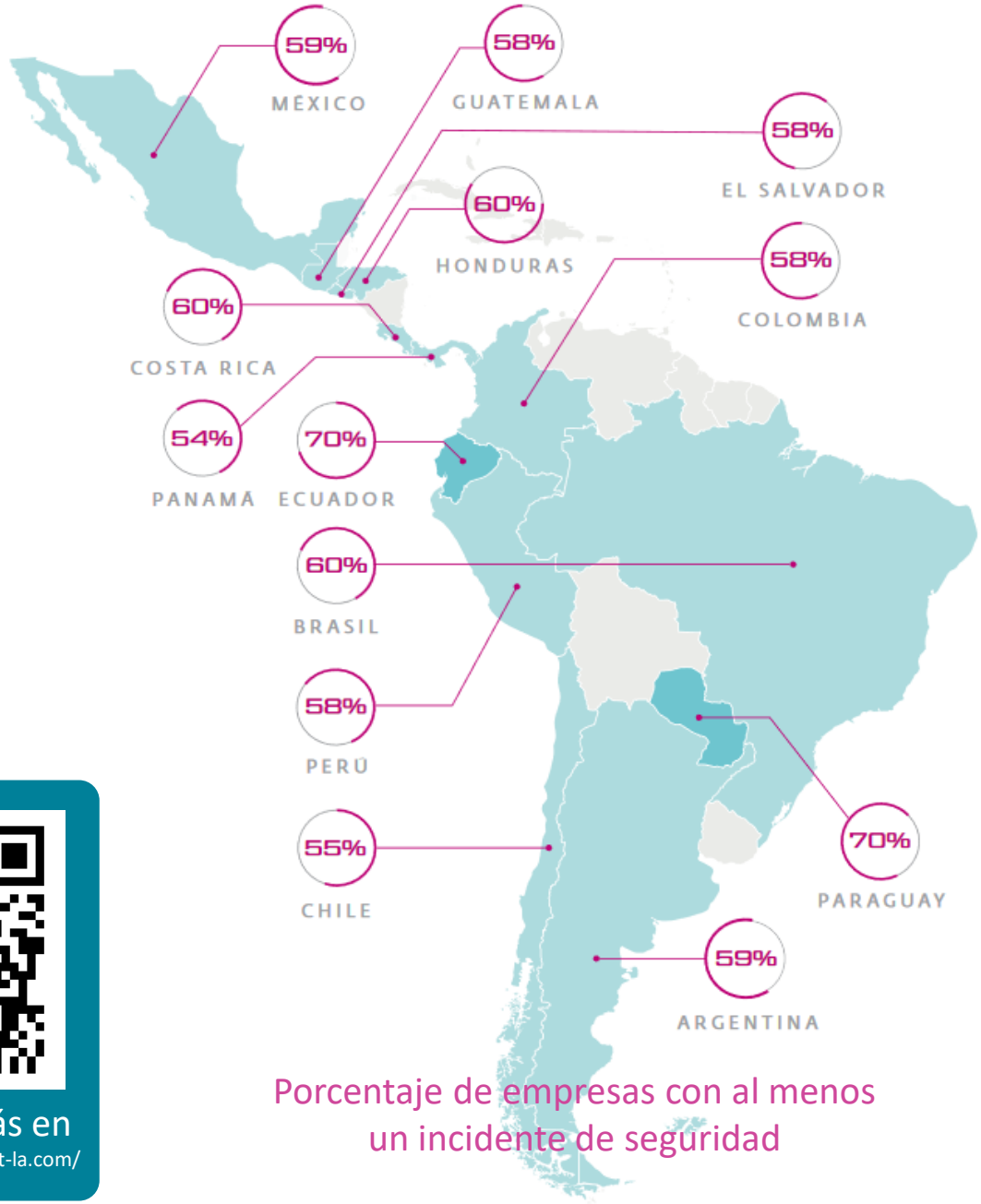
Top Threats

Top Threats

Mexico | Month | Less | JSON / XML / DOC

	Threat Name	Change	Prevalence Level		
1	JS/Adware.Subprop	▲		11.87 %	Map-Timeline
2	JS/Adware.Atocari	▼		10.78 %	Map-Timeline
3	Incoming.Attack.Generic	▲		9.58 %	Map-Timeline
4	RDP.Attack.Generic	▲		9.43 %	Map-Timeline
5	JS/PopunderJS	▼		6.56 %	Map-Timeline
6	HTML/ScrInject	▲		5.43 %	Map-Timeline
7	JS/ExAds	▼		5.37 %	Map-Timeline
8	JS/Adware.Adport	▲		4.78 %	Map-Timeline
9	JS/Adware.AdFly	▼		4.49 %	Map-Timeline
10	SMB.Attack.Generic	▲		3.86 %	Map-Timeline
11	JS/Adware.Popcash	▲		3.37 %	Map-Timeline
12	JS/Mybestdc	▼		3.31 %	Map-Timeline
13	JS/Adware.Revizer	▲		2.51 %	Map-Timeline
14	SMB/Exploit.DoublePulsar	▲		2.3 %	Map-Timeline
15	JS/Adware.PopAds	▼		2.28 %	Map-Timeline

Puedes ver más en
https://www.virusradar.com



Porcentaje de empresas con al menos un incidente de seguridad

Puedes ver más en
https://security-report.eset-la.com/

BID Mejorando vidas | OEA Más derechos para más gente

English
Español

Niveles de madurez
Inicial
Formativo
Establecido
Estratégico
Dinámico

Capacidad de seguridad cibernética
Los datos utilizados se recogieron a través de una encuesta en línea desarrollada en colaboración con el Centro Global de Capacidad sobre Seguridad Ciberneutica (GCSCC) sobre la base del Modelo de Madurez de Capacidad de Seguridad Cibernetica (CMM), por sus siglas en inglés. Los valores de 2016 utilizados se actualizaron para reflejar el Modelo de madurez de la capacidad de ciberseguridad para la edición revisada de las naciones (CMM). Todas las evaluaciones realizadas en la publicación de 2016 siguen siendo las mismas, excepto la inclusión de nuevos indicadores.

Descargue el XLS de todo lo seleccionado
Descargar

Volver al mapa

Volver al mapa

País a comparar por años
México

	México 2020	México 2016
Política y Estrategia de Seguridad Cibernética		
Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
Protección de la Infraestructura Crítica (IC)		
Identificación de Incidentes		
Organización		
Gestión de Riesgos y Respuesta		
Manejo de Crisis		
Manejo de Crisis		
Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

Puedes ver más en
https://observatoriociberseguridad.org

#safeandconnected

¡GRACIAS!

Camilo Gutiérrez Amaya

Jefe del Laboratorio de Investigación ESET

hcamiloga

Miguel Ángel Mendoza

Investigador de Seguridad ESET

angel_mendoza