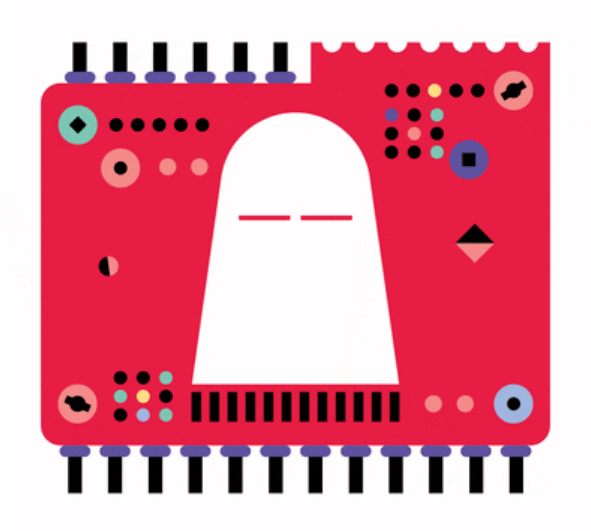


Aumento interanual de más de **70%** en los **ataques de Ransomware a nivel mundial.**

República Dominicana | Crecen los ataques informáticos

Los ciberataques reportados y resueltos aumentaron en más de un 50%

Ataque
Hackers piden US$600 mil para devolver datos al IAD

Un ciberataque masivo en Costa Rica aflige a la ciudadanía

Las pérdidas económicas eclipsan la extorsión de $15 millones que el gobierno se negó a pagar a cibercriminales, y el caos solo está empeorando.

ATAQUES INFORMÁTICOS >

E Los hackeos a instituciones públicas asedian al Gobierno de López Obrador

El Ejército, la Lotería Nacional, Pemex y la Secretaría de Comunicaciones han sido objeto de ataques cibernéticos en los que el Gobierno ha perdido información sensible

CIBERATAQUES >

Un ciberataque pone en alerta al Poder Judicial de Chile

La infección de una parte minúscula del sistema informático ocurre a una semana de la masiva filtración de correos electrónicos de las Fuerzas Armadas producto de un 'hackeo'

Durante la primera mitad del 2023 el Ransomware fue una amenaza creciente para el sector financiero.

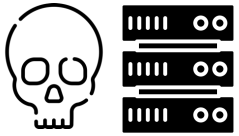
Aumento de un 30% a los eventos relacionados con Ransomware en comparación con el 2022.

El valor total de la actividades reportadas en la primera mitad del 2023 es de 570 millones. La cantidad mensual promedio de transacciones fue de 66.4 millones de dólares.

AMÉRICA LATINA BAJO ASEDIO: “SE REGISTRARON 4 MIL ATAQUES DE RANSOMWARE AL DÍA EN AMÉRICA LATINA EN 2023”

KASPERSKY lab

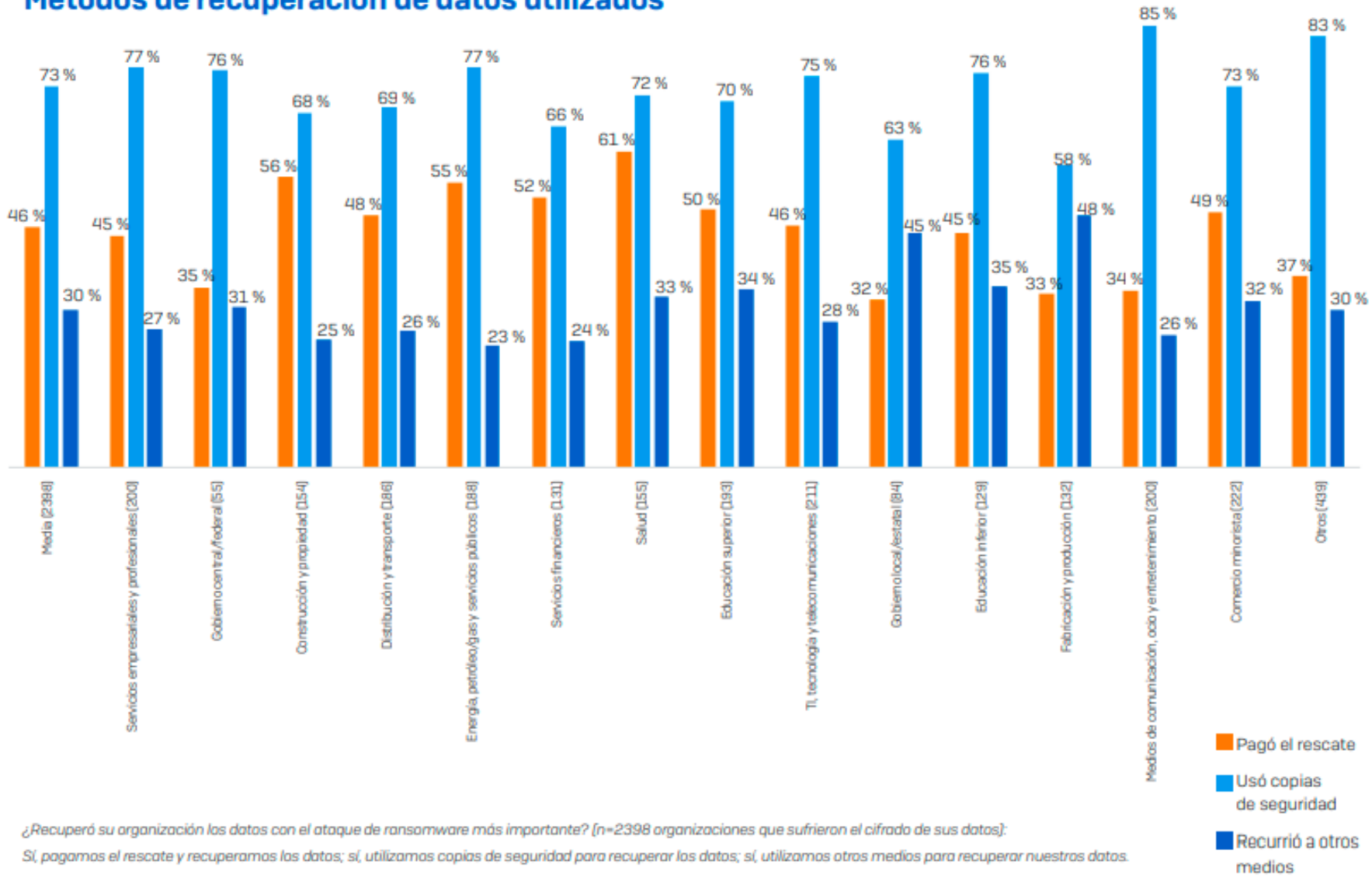
Aumento de la frecuencia y la gravedad de los ataques de Ransomware 2020 – H12022



	2020	2021	2022
Número de Ataques de Ransomware	118 MM	305 MM **+62%**	609 MM **+100%** Estimado basado de H1
Rescate Promedio Pagado	USD$ 115,123	$312,493 **+171%**	$570,000 **+82%** A partir del H1 2021
Rescate Más Alto Pagado	$ 5 MM	$10 MM **+50%**	$40 MM **+300%** A partir del H1 2021

Fuente: Unidad 42 Ransomware Threat 2022 (Palo Alto), SonicWall Cyber Threat Report 2022.

Métodos de recuperación de datos utilizados



¿Recuperó su organización los datos con el ataque de ransomware más importante? (n=2398 organizaciones que sufrieron el cifrado de sus datos):

Sí, pagamos el rescate y recuperamos los datos; sí, utilizamos copias de seguridad para recuperar los datos; sí, utilizamos otros medios para recuperar nuestros datos.

Los Pagos de Rescates han Aumentado

3x
Aumento de la proporción que pagó
Rescates de más de USD$ 1 MM

21%
Pagaron rescates de menos
De USD$ 10,000

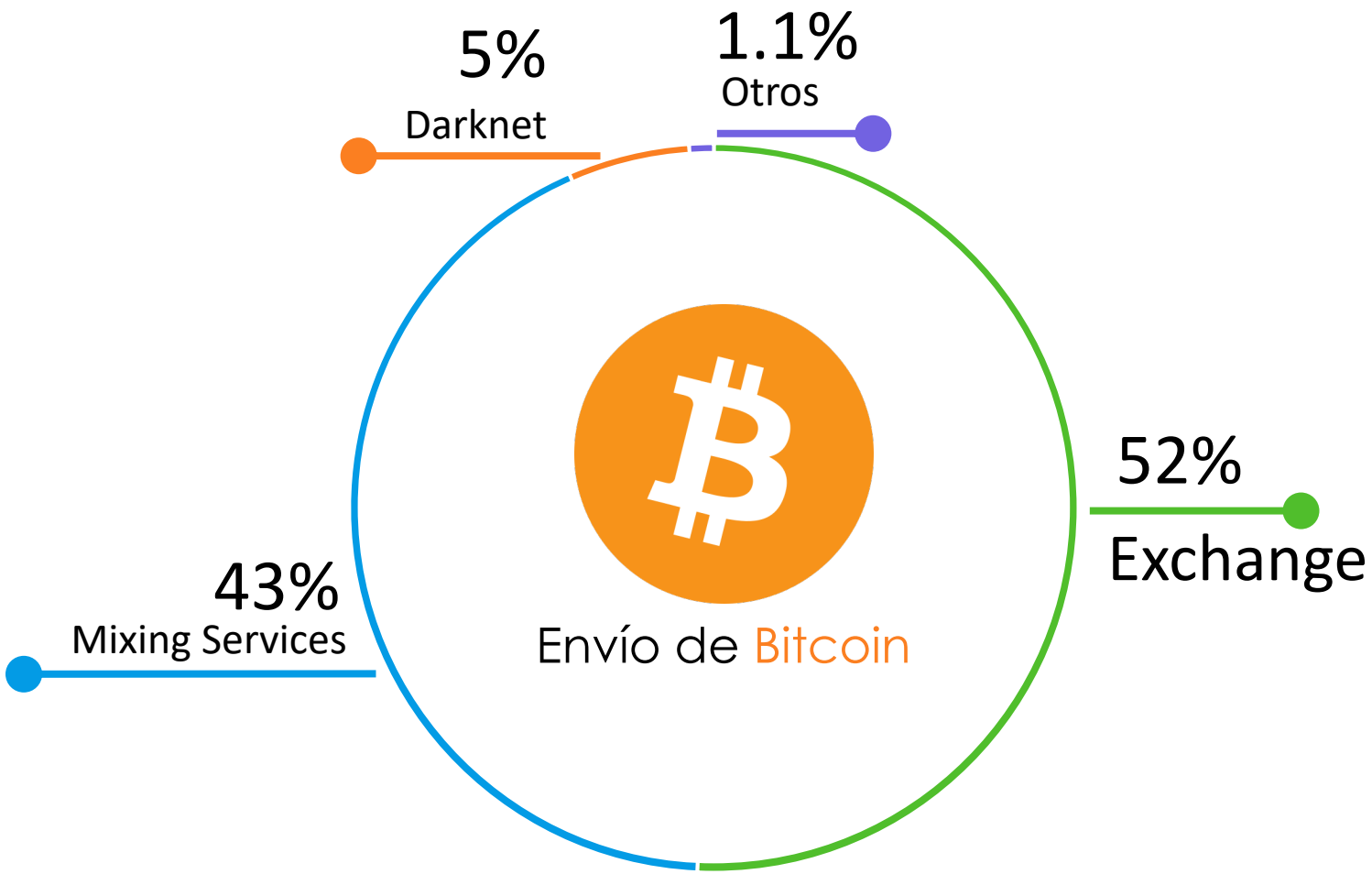
USD$ 812 360
Media de los rescates

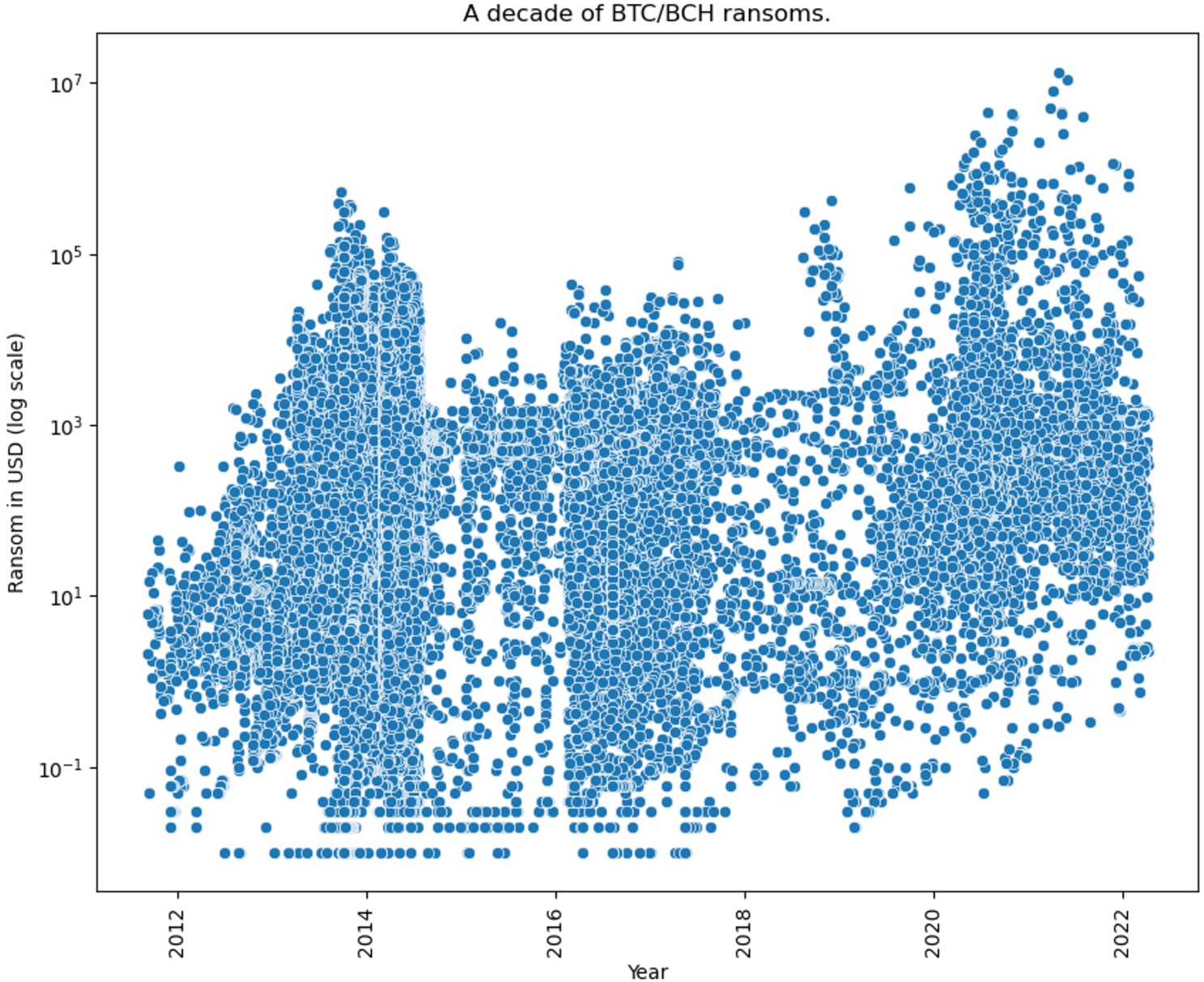
FABRICANTES, SERVICIOS PÚBLICOS
Pago de rescate medio más alto
(USD$ 2 Millones)

SALUD
Pago de rescate medio
Más bajo (USD$ 197,000)

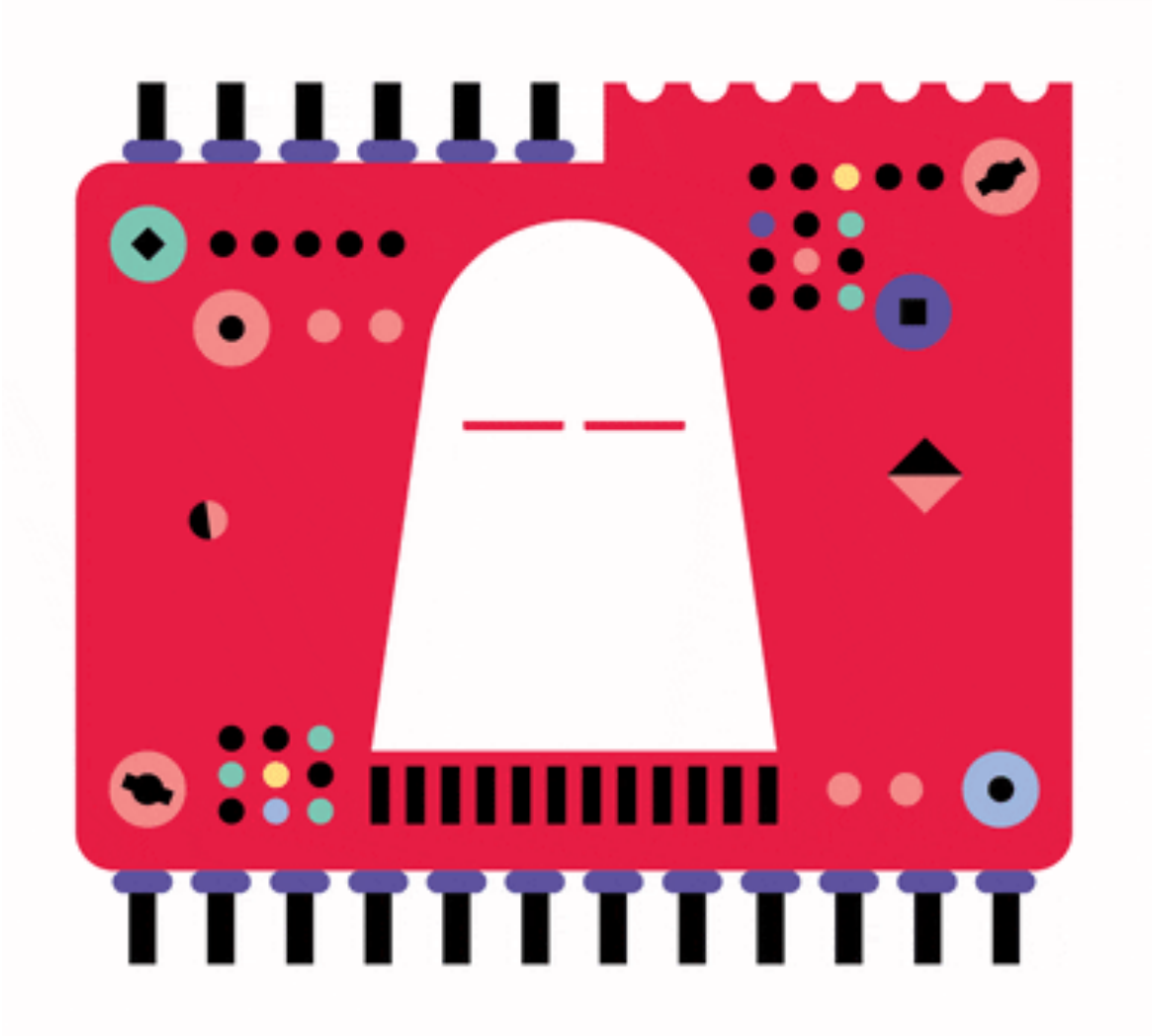
110 direcciones de billeteras únicas.

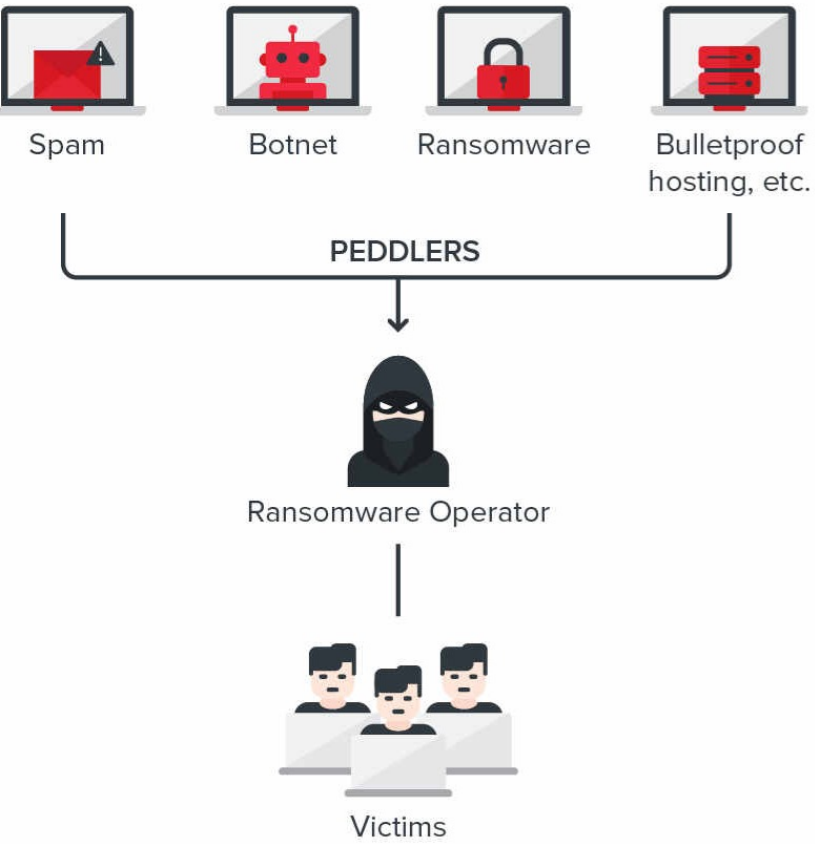
34 millones de dólares registrados a billeteras proporcionadas por los ciberatacantes.

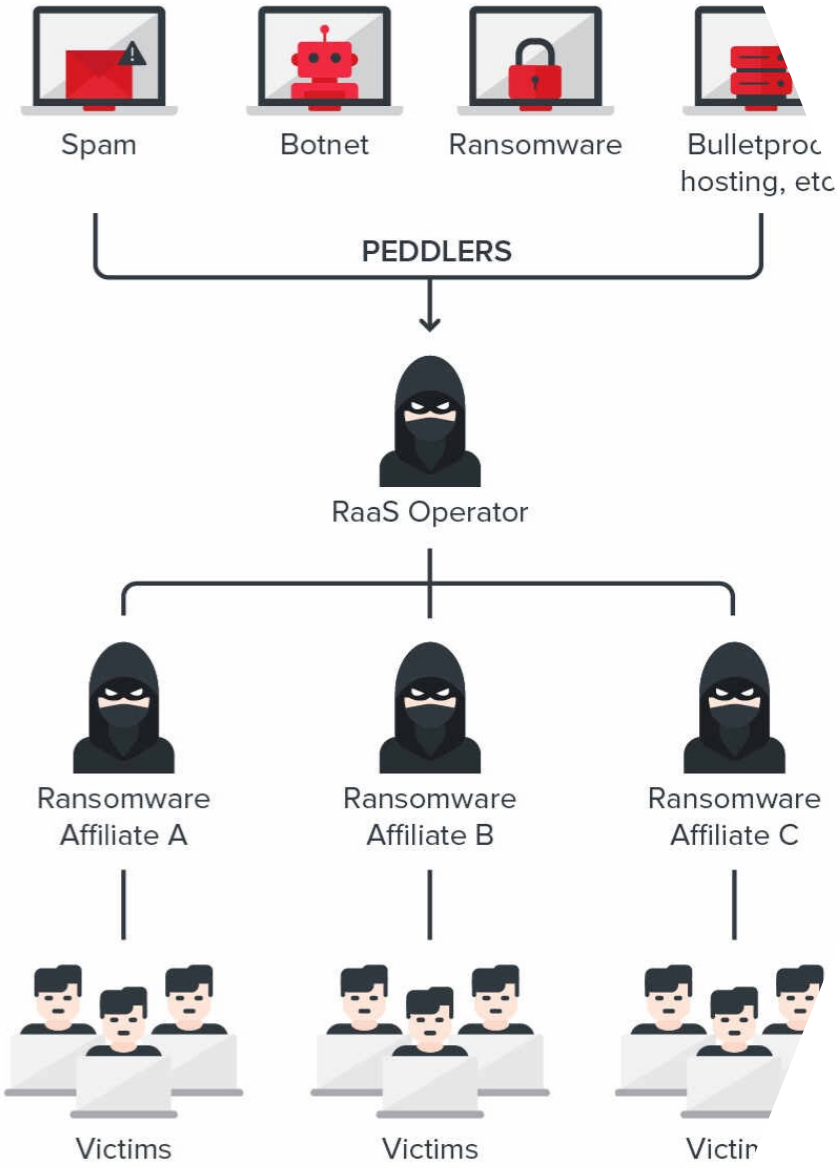


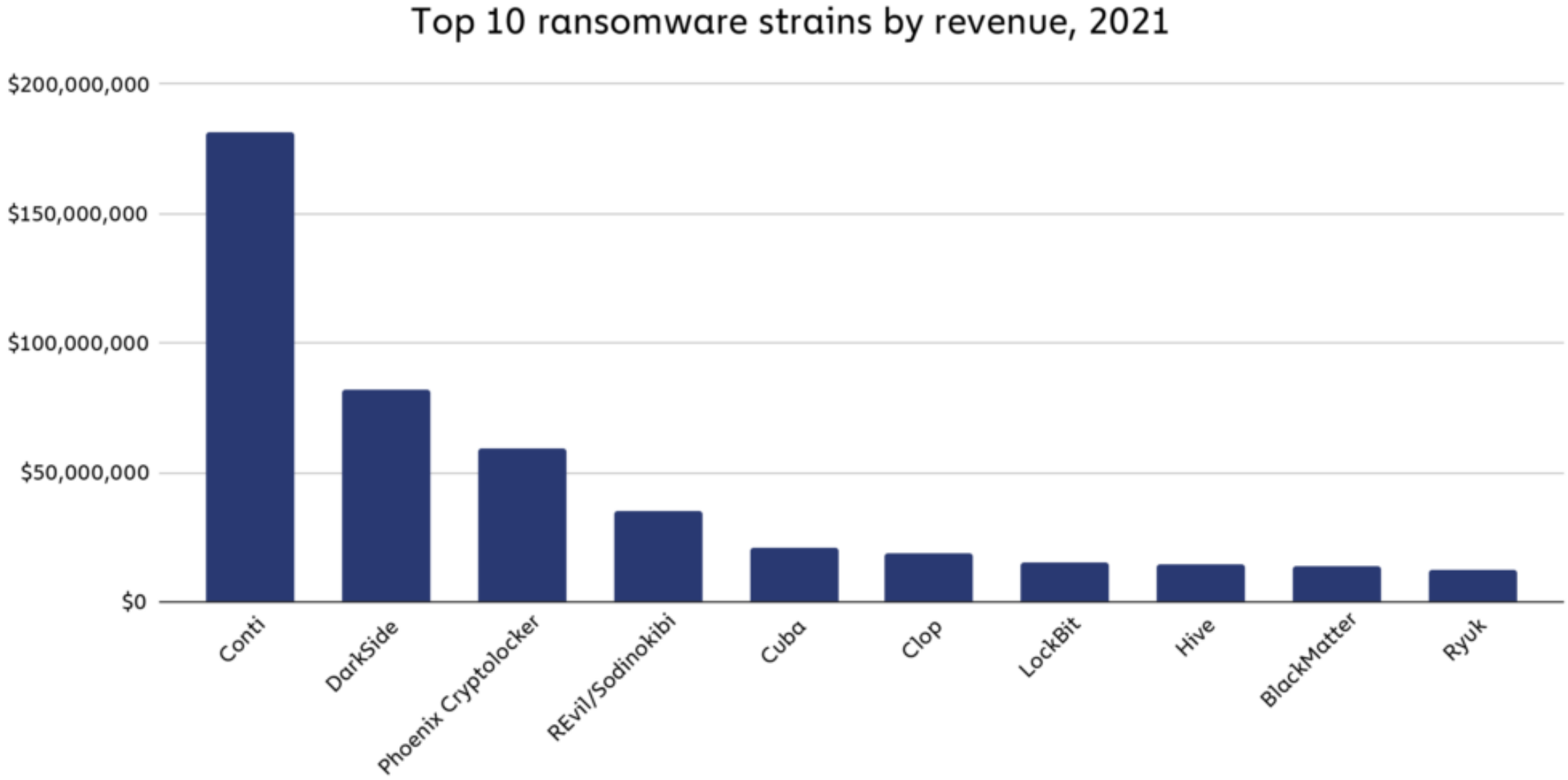

A decade of BTC/BCH ransoms.
Ransom in USD (log scale)
10^{7}
10^{5}
10^{3}
10^{1}
10^{-1}
2012
2014
2016
2018
2020
2022
Year

Acceso como Servicio (AaaS) como ventaja para la detección temprana.

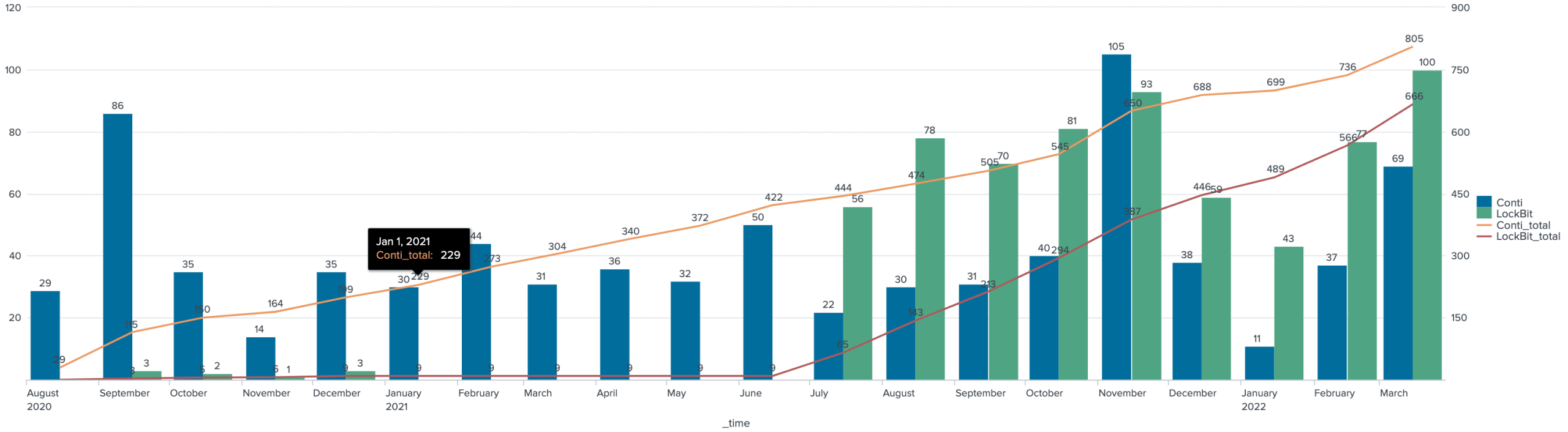



Spam
Botnet
Ransomware
Bulletproof hosting, etc.
PEDDLERS
Ransomware Operator
Victims

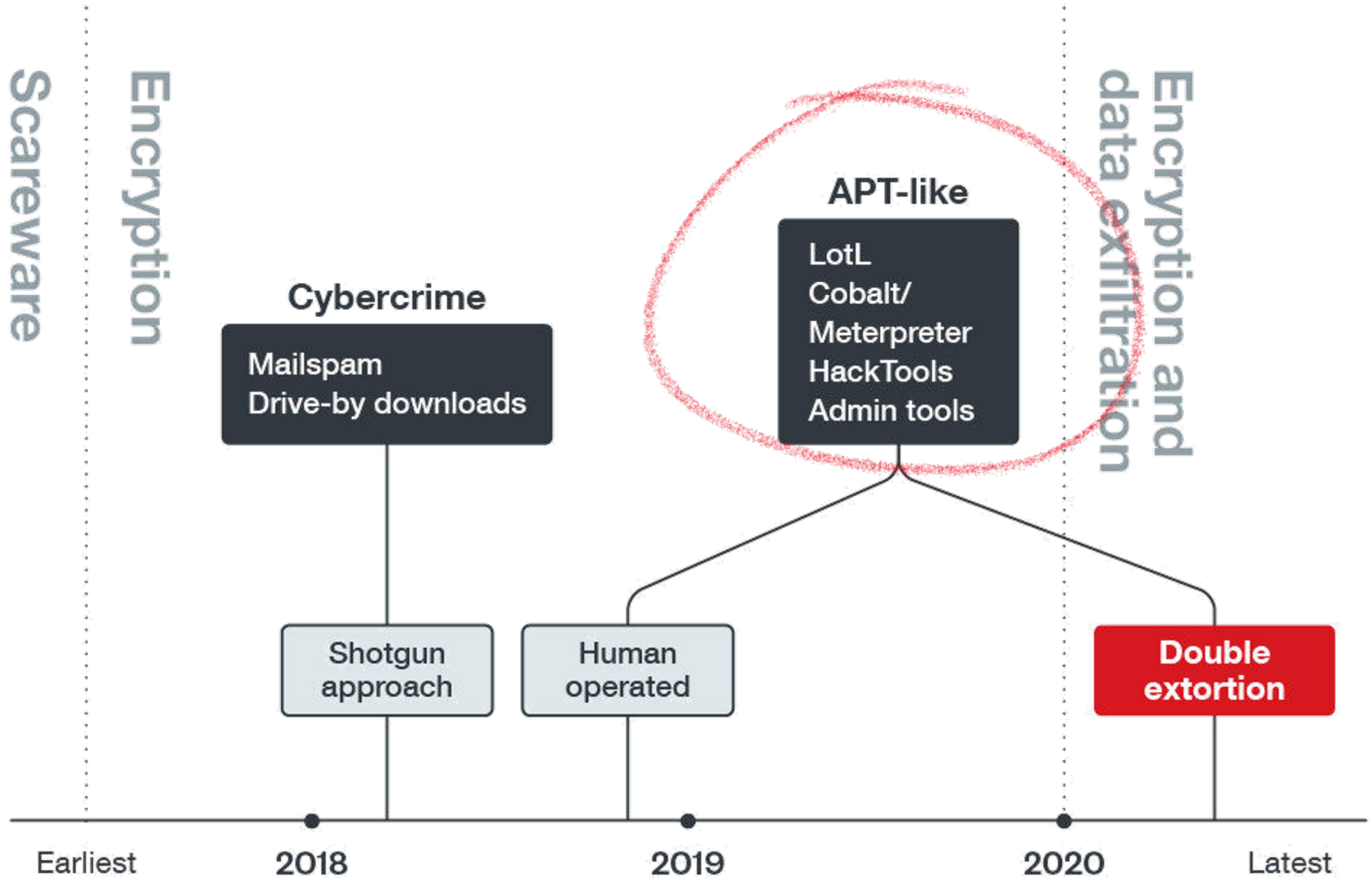

Spam
Botnet
Ransomware
Bulletproc hosting, etc
PEDDLERS
RaaS Operator
Ransomware Affiliate A
Ransomware Affiliate B
Ransomware Affiliate C
Victims
Victims
Victir


Top 10 ransomware strains by revenue, 2021
$200,000,000
$150,000,000
$100,000,000
$50,000,000
$0
Conti
DarkSide
Phoenix Cryptolocker
REvil/Sodinokibi
Cuba
Clop
LockBit
Hive
BlackMatter
Ryuk

Números mensuales y acumulados de organizaciones víctimas de Conti y LockBit desde agosto de 2020 hasta marzo de 2022



Fuente: https://www.trendmicro.com/es_es/research/22/f/conti-vs-lockbit-a-comparative-analysis-of-ransomware-groups.html


Scareware
Encryption
Encryption and data exfiltration
Cybercrime
Mailspam
Drive-by downloads
APT-like
LotL
Cobalt/
Meterpreter
HackTools
Admin tools
Shotgun approach
Human operated
Double extortion
Earliest
2018
2019
2020
Latest

El informe revela tres tipos principales de proveedores de acceso (AaaS):

- **Vendedores oportunistas**
  - Se centran en obtener una ganancia rápida y no dedican todo su tiempo al acceso.
- **Los proveedores de acceso dedicados**
  - Son hackers sofisticados y hábiles que ofrecen acceso a una variedad de empresas diferentes. Sus servicios suelen ser utilizados por afiliados y grupos de ransomware más pequeños.
- **Tiendas online que ofrecen credenciales RDP y VPN**
  - Estas tiendas dedicadas solo garantizan el acceso a una sola máquina en lugar de a toda una red u organización. Sin embargo, representan una forma simple y automatizada para que los ciberdelincuentes con habilidades más bajas compren acceso. Incluso pueden buscar por ubicación, ISP, sistema operativo, número de puerto, derechos de administrador o nombre de la empresa.

Fuente: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market

EUROPOL

OPERATION CRONOS

10
< COUNTRIES IN TASKFORCE CRONOS />

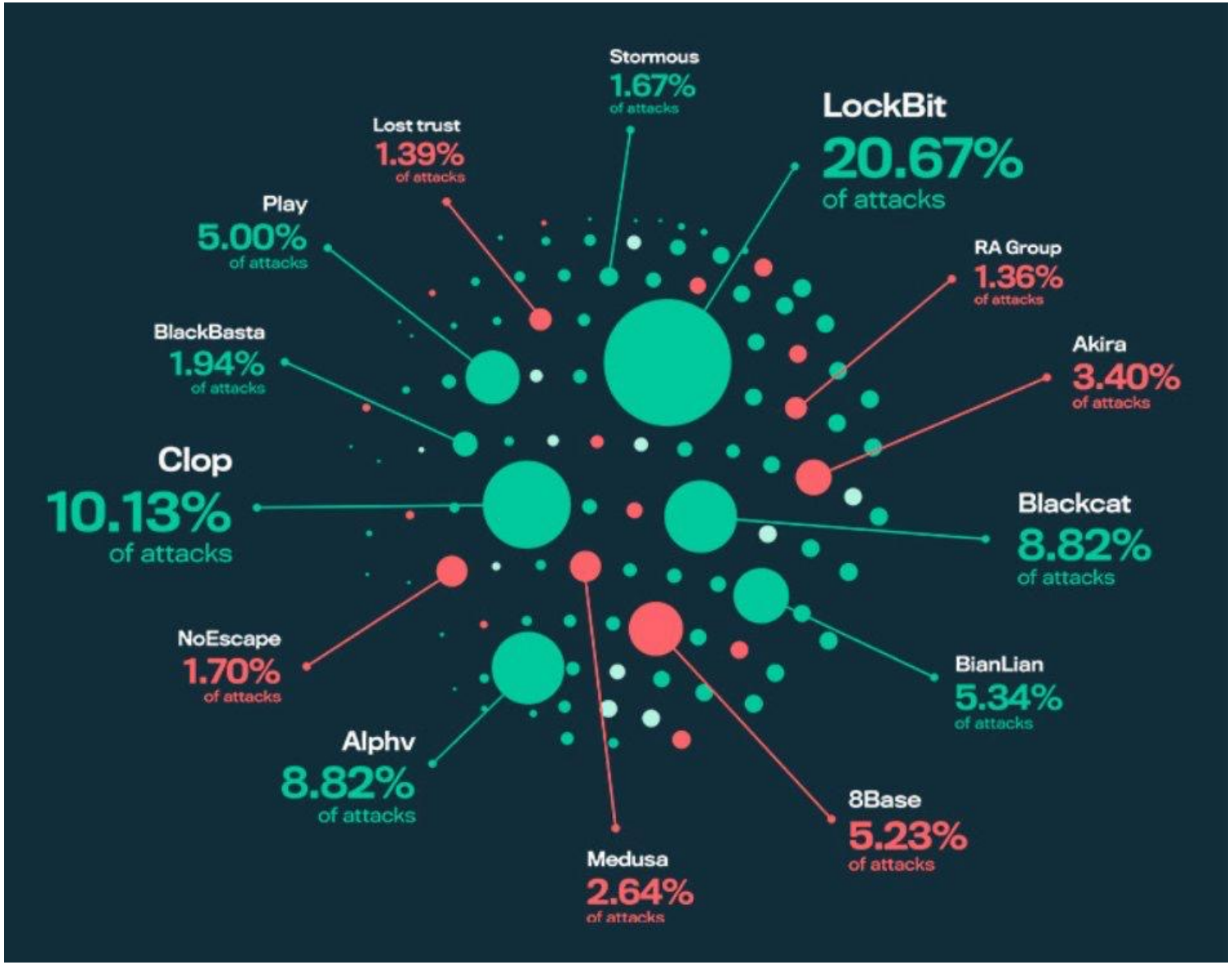
2
< ARRESTS />

MORE THAN
200
< CRYPTOCURRENCY ACCOUNTS FROZEN />

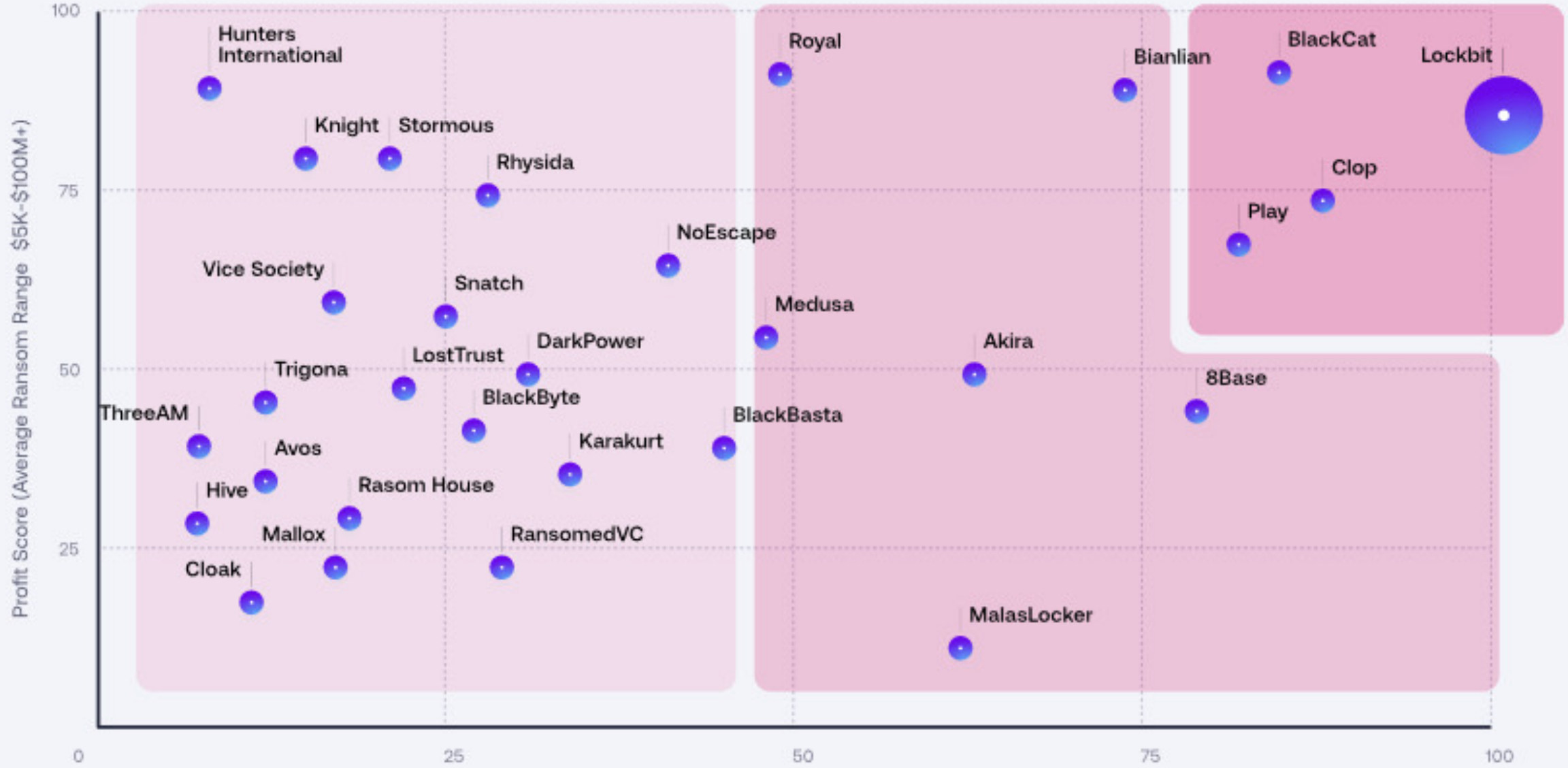
34
< SERVERS TAKEN DOWN />

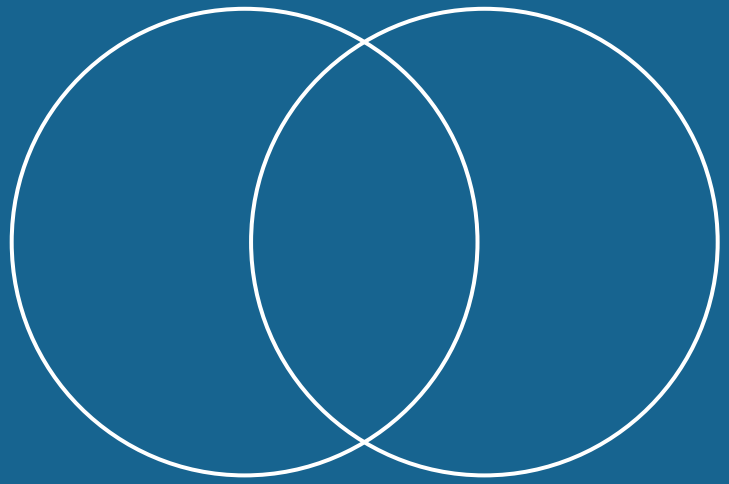
14 000
< ROGUE ACCOUNTS CLOSED />

< LAW ENFORCEMENT HAS TAKEN CONTROL OF THE TECHNICAL INFRASTRUCTURE AND LEAK SITE />


Stormous
1.67%
of attacks
LockBit
20.67%
of attacks
Lost trust
1.39%
of attacks
Play
5.00%
of attacks
RA Group
1.36%
of attacks
BlackBasta
1.94%
of attacks
Akira
3.40%
of attacks
Clop
10.13%
of attacks
Blackcat
8.82%
of attacks
NoEscape
1.70%
of attacks
BianLian
5.34%
of attacks
Alphv
8.82%
of attacks
8Base
5.23%
of attacks
Medusa
2.64%
of attacks

2023 Ransomware Group Risk Matrix

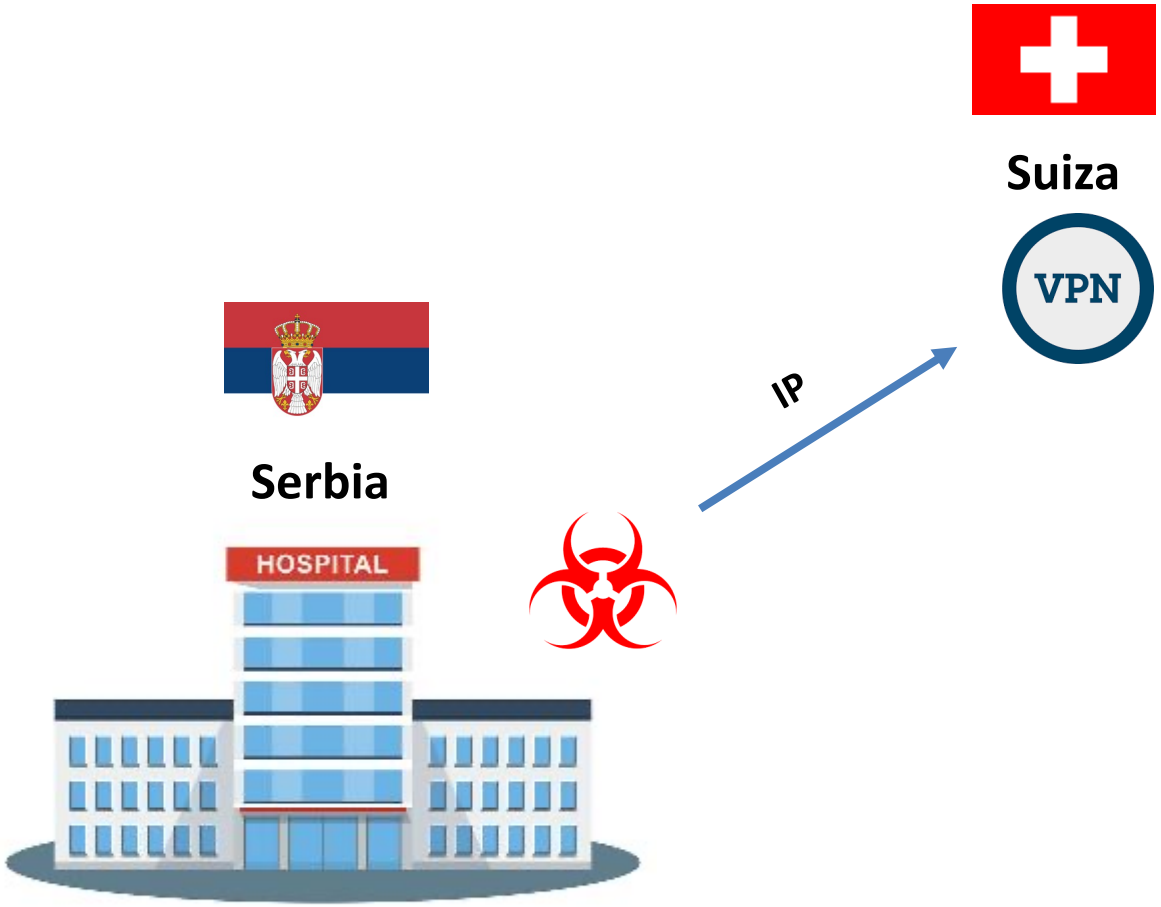




Cooperación

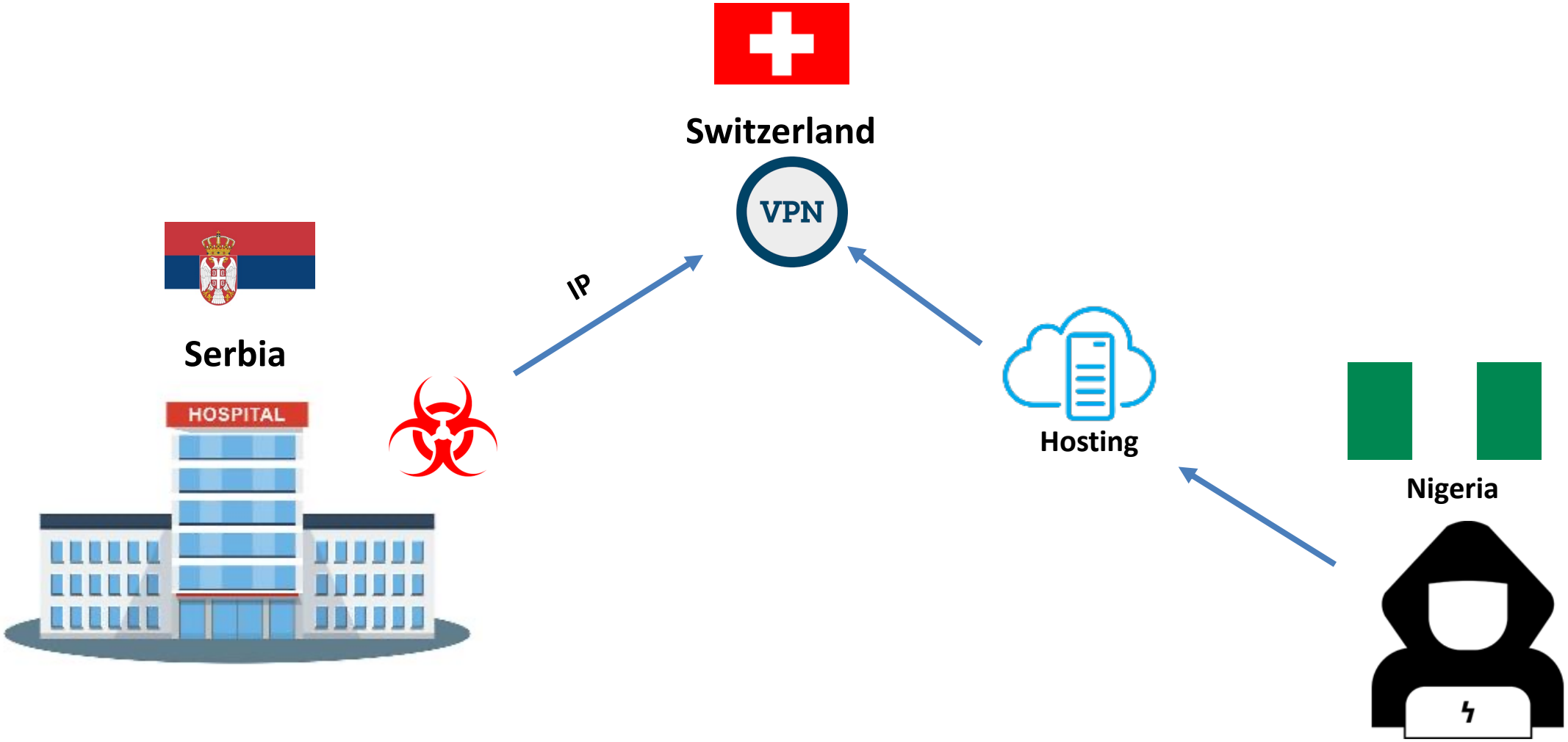
Escenario No. 1

Hospital víctima de ransomware



Escenario No. 1

Hospital víctima de ransomware



Escenario No. 1

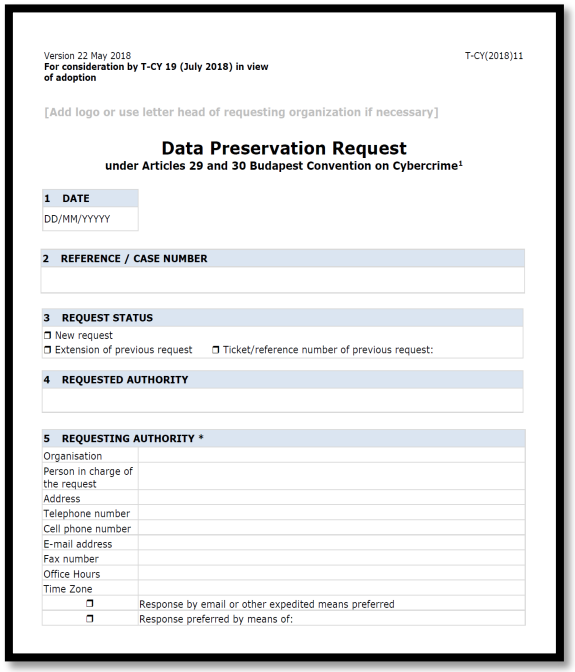
Hospital víctima de ransomware

Preguntas:

- Qué debemos hacer?
- Qué unidad hace la solicitud? (Policia o fiscalia?)
- Cuales son los mecanismos disponibles?
- Quién escribe la solicitud?
- Quién la envia y hace seguimiento?
- Quién recibe la información de divulgación?

Herramientas

Formulario de Preservación



Version 22 May 2018
For consideration by T-CY 19 (July 2018) in view of adoption

T-CY(2018)11

[Add logo or use letter head of requesting organization if necessary]

Data Preservation Request
under Articles 29 and 30 Budapest Convention on Cybercrime[1]

1 DATE
DD/MM/YYYYY

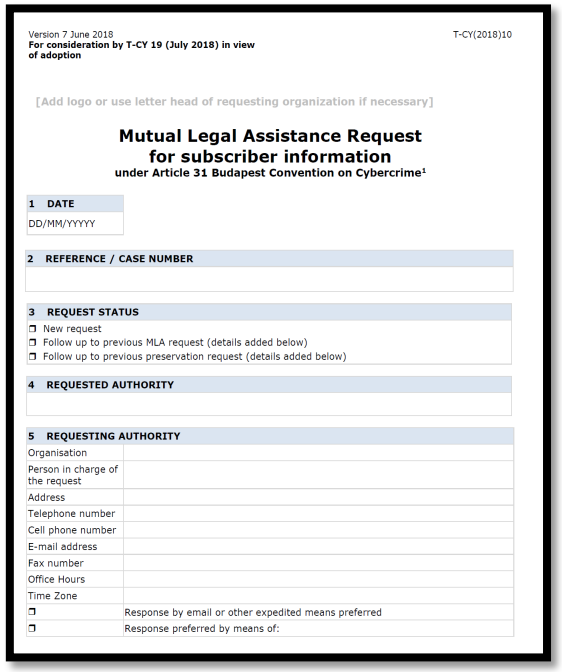
2 REFERENCE / CASE NUMBER

3 REQUEST STATUS
❒ New request
❒ Extension of previous request ❒ Ticket/reference number of previous request:

4 REQUESTED AUTHORITY

5 REQUESTING AUTHORITY *	
Organisation	
Person in charge of the request	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	
❒	Response by email or other expedited means preferred
❒	Response preferred by means of:

Formulario de divulgación



Version 7 June 2018
For consideration by T-CY 19 (July 2018) in view of adoption

T-CY(2018)10

[Add logo or use letter head of requesting organization if necessary]

Mutual Legal Assistance Request for subscriber information
under Article 31 Budapest Convention on Cybercrime[1]

1 DATE
DD/MM/YYYYY

2 REFERENCE / CASE NUMBER

3 REQUEST STATUS
❒ New request
❒ Follow up to previous MLA request (details added below)
❒ Follow up to previous preservation request (details added below)

4 REQUESTED AUTHORITY

5 REQUESTING AUTHORITY	
Organisation	
Person in charge of the request	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	
❒	Response by email or other expedited means preferred
❒	Response preferred by means of:

Directorio de PoC's

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Restricted
Version 1 September 2020

Budapest Convention on Cybercrime

Directory of

24/7 Points of Contact

Signatarios de la Convención de Budapest

No signatarios de la Convención de Budapest

Recomendaciones

- Mantener repositorio seguro actualizado:
  - Información actualizada de los PoC 24x7
  - Información de las autoridades competentes
  - Procedimientos requeridos
  - Capacidades
  - Herramientas disponibles
  - Canal de comunicación seguro
- Crear instrumentos legales que habiliten la operación de los PoC 24x7