



ESCOLA GALEGA
DE ADMINISTRACIÓN
PÚBLICA



Protegiéndonos
de los
HACKERS



EL PAÍS ECONOMÍA

MERCADOS MIS FINANZAS VIVIENDA FORMACIÓN MIS DERECHOS NEGOCIOS CINCO DÍAS RETINA ÚLTIMAS NOTICIAS

Te quedan 6 artículos gratis este mes SUSCRÍBETE

SEPE >

El SEPE sigue paralizado por el ciberataque: “Rellenamos expedientes con formularios antiguos a mano”

El director de la institución asegura que ya están dados de alta

Un bebé muere después de que unos hackers atacaran un hospital

Un bebé en Alabama ha fallecido a consecuencia de un ataque *hacker*. El bebé, que nació con una lesión cerebral, no pudo ser atendido por un ataque *ransomware*.

1 octubre, 2021 - 11:25

GUARDAR

The Colonial Pipeline Cyberattack

Ciberataque al oleoducto Colonial Pipeline: esto sabemos

La dependencia en el oleoducto ha crecido a medida que el aumento de la producción de petróleo y gas de EE. UU. ha nevado

Un ciberataque paraliza las webs del Ministerio de Justicia, Educación, Economía y el INE

Ya no hay respeto: Ciberataque interrumpe las operaciones de varias fábricas de cerveza

La firma cervecera Molson Coors ha reportado ser víctima de un **ciberataque** perpetrado contra sus instalaciones que “ha producido una demora en las operaciones y el envío de cerveza”.

CincoDías

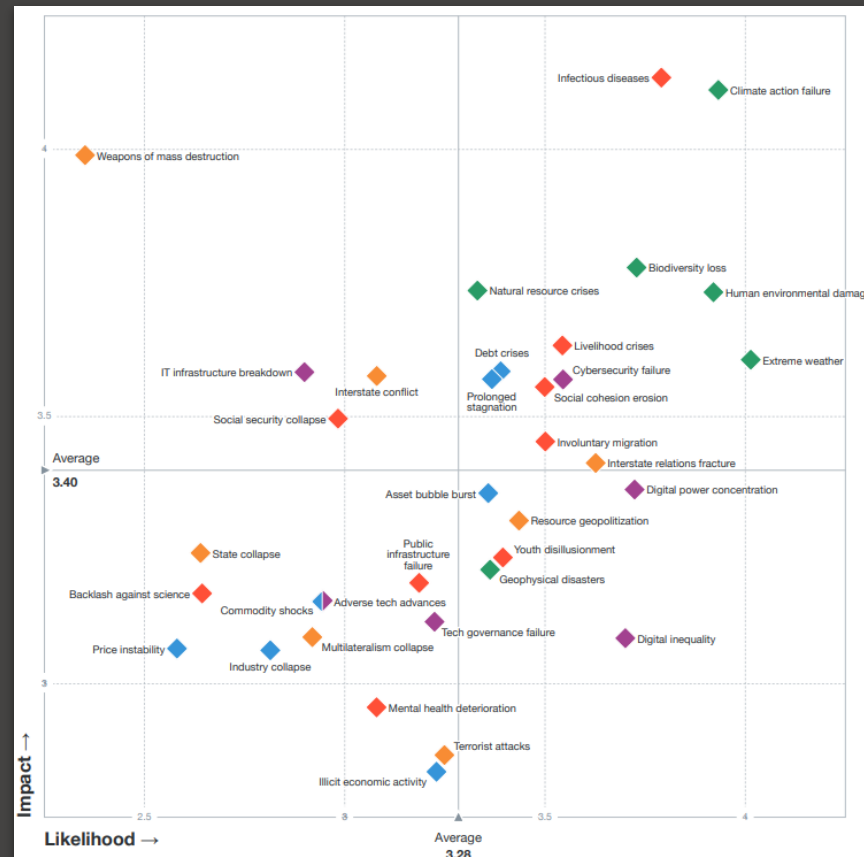
Compañías Mercados Economía Mi Dinero Fortuna / Cotizaciones

Compañías

SEGURIDAD

Un nuevo ciberataque se extiende a más de 350 organizaciones... los 'hackers' han robado 70 millones

Las empresas afectadas están en EE UU, Alemania y Canadá; la española, según ESET. La cadena sueca de supermercados ha cerrado 800 tiendas



Global Risks 2021 - World Economic Forum

Antonio Fernandes



Cultura de la Ciberseguridad

Gestor

Mentor

Divulgador



ISACA
Madrid Chapter



AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

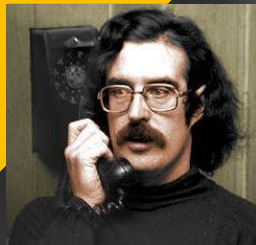


Tech Model Railroad Club (TMRC)

Artificial Intelligence Laboratory

ARPANET





John Draper



Steve Wozniak



Robert Morris



Kevin Mitnick





Un HACKER
NO
es un
CIBERDELINCUENTE



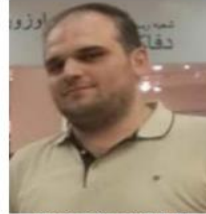
MOSTAFA SADEGHI



SAJJAD TAHMASEBI



MOHAMMED REZA
SABAH



SAID POURKARIM
ARABI



MOHAMMAD REZA
ESPARGHAM



Cyber Most Wanted



DANIAL JELOUDAR



ARASH AMIRI ABEDIAN



MOHAMMAD SAEED
AJILY



MARWAN ABUSROUR



BEHZAD
MOHAMMAZADEH



PARK JIN HYOK



KIM IL



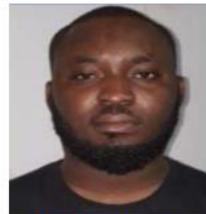
DMITRY
ALEKSANDROVICH
DOKUCHAEV



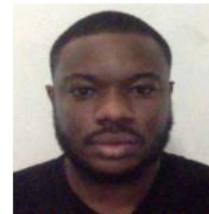
IGOR ANATOLYEVICH
SUSHCHIN



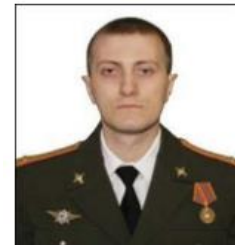
EVGENIY
MIKHAILOVICH
BOGACHEV



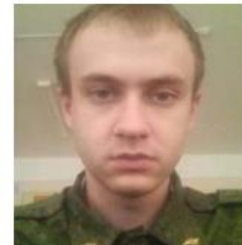
FELIX OSILAMA OKPOH



ABIOLA AYORINDE
KAYODE



SERGEY
VLADIMIROVICH
DETISTOV



PAVEL VALERYEVICH
FROLOV

Principales Motivos

Hacktivismo

Espionaje (APT)

Dinero

GUERRA CIBERNÉTICA

El CNI advierte que España es objetivo inminente de grupos de hackers rusos



• El CCN-CERT, el departamento de ciberamenazas del CNI, ha compartido un artículo que anticipa que instituciones y empresas españolas podrían ser víctimas de los próximos ataques cibernéticos rusos

Los tres ciberataques de Rusia que más teme occidente

20MINUTOS / NOTICIA / 27.03.2022 - 12:26H



— Los servicios secretos rusos po

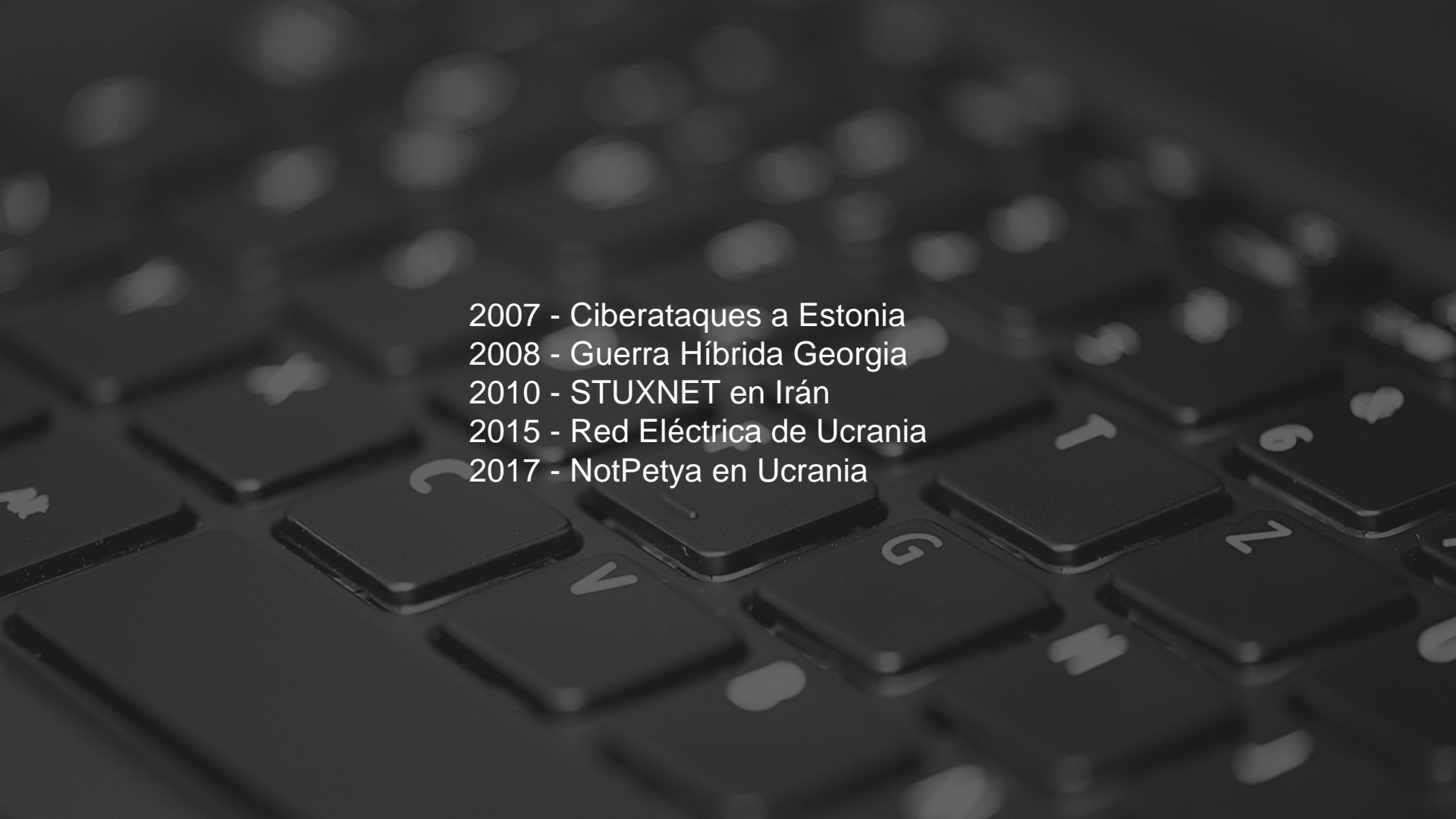
en plena guerra, según 'The Times'.

DE MOMENTO, TODO ESTABLE

El Gobierno llama a las empresas críticas a reforzar su ciberseguridad ante la guerra

El CNPIC comunicó el viernes a las compañías de los sectores estratégicos la necesidad de reforzar los protocolos de seguridad. De momento, no se ha detectado actividad fuera de lo habitual

Por **Carla Raffin**



2007 - Ciberataques a Estonia
2008 - Guerra Híbrida Georgia
2010 - STUXNET en Irán
2015 - Red Eléctrica de Ucrania
2017 - NotPetya en Ucrania

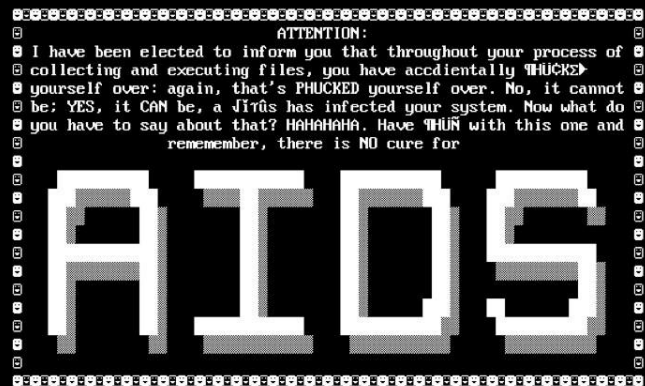
Principales Motivos

Hacktivismo

Espionaje (APT)

Dinero

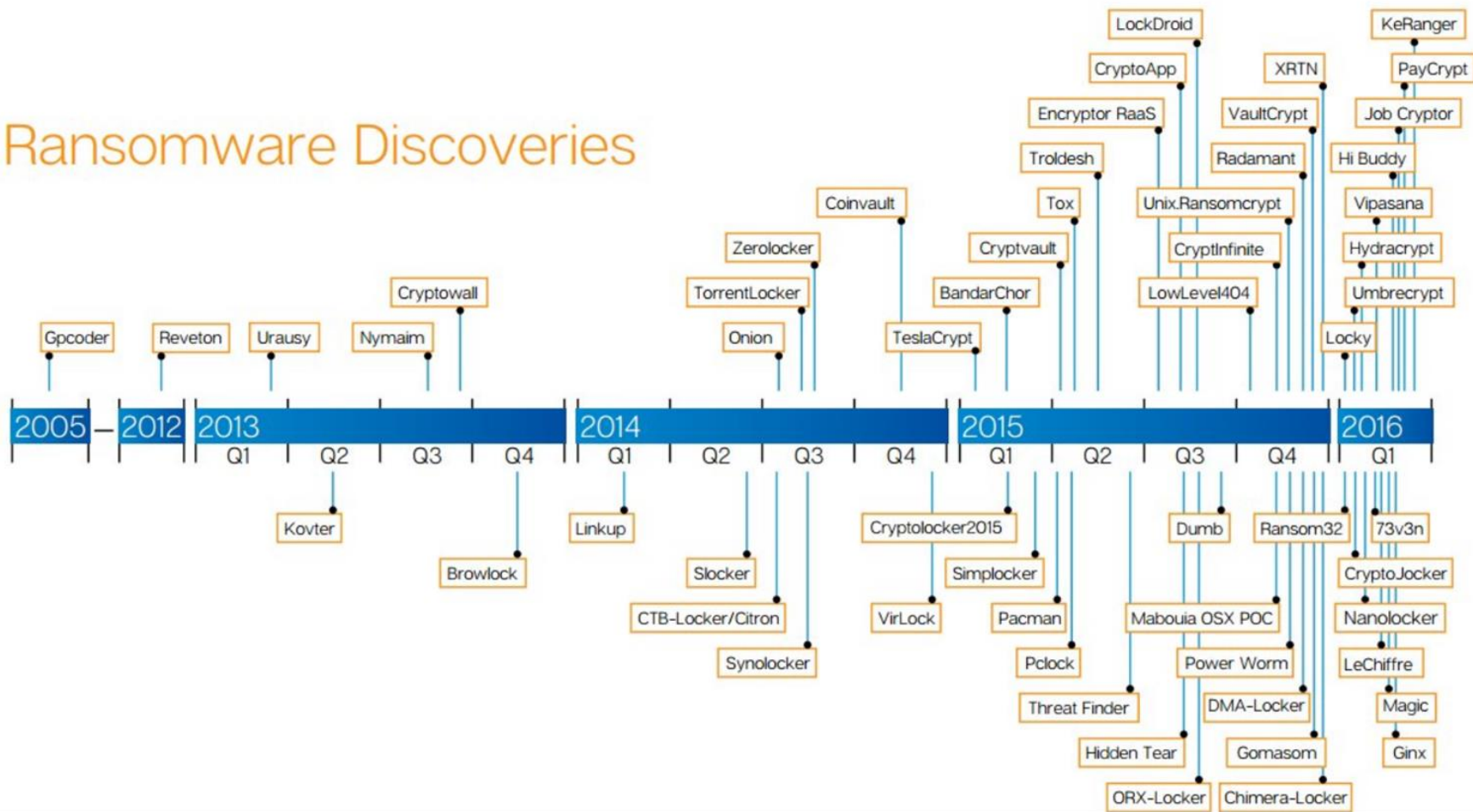
Ransomware



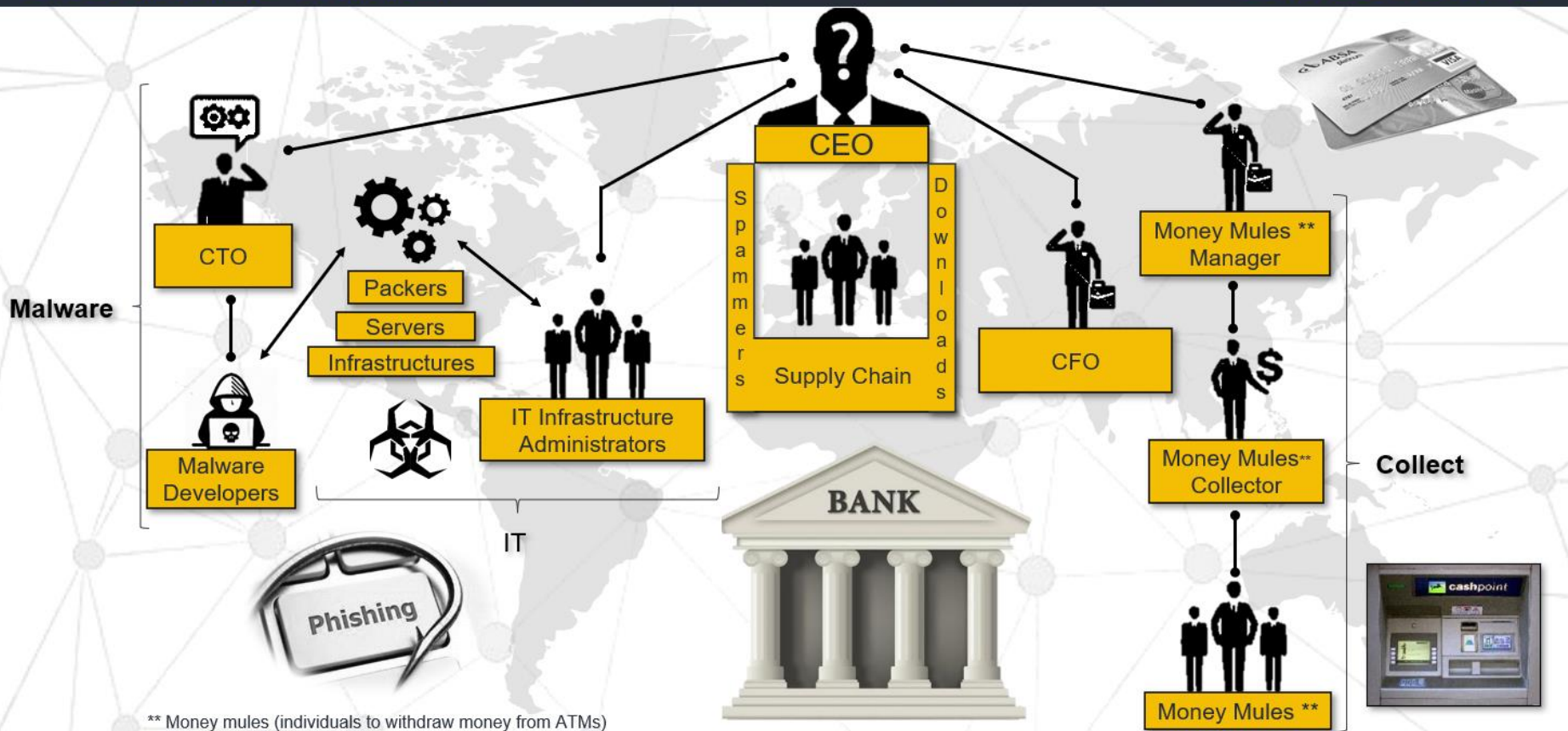
ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accidentally PHUCKED
yourself over: again, that's PHUCKED yourself over. No, it cannot
be: YES, it CAN be, a VIRUS has infected your system. Now what do
you have to say about that? HAHAAHAHA. Have THUN with this one and
remember, there is NO cure for
AIDS

1989

Ransomware Discoveries

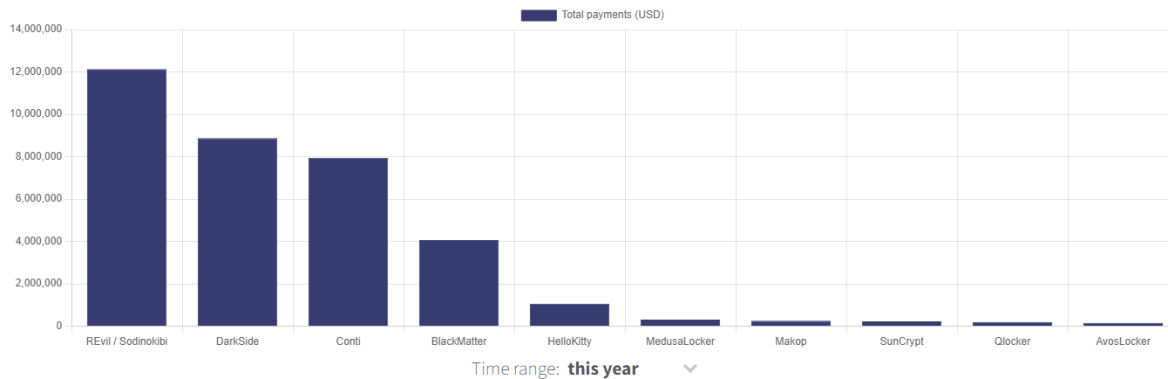


ORGANIZED CRIME: HIERARCHICAL AND DISTRIBUTED STRUCTURES



- (2006) - Zeus
- (2009) - Jabber Zeus
- (2010) - Retiro de Slavik
- (2011) - GameOver Zeus
- (2013) - Cryptolocker
- (2015) - Recompensa de 3M\$





CYBER EXPERTOS MARIBEL POYATO

El cibercrimen ya mueve más dinero que el narcotráfico

Vicente Ramírez
4 octubre, 2019

21 Compartido 5,265 Visualizaciones 1

Compartir artículo

Compartido en twitter

+

Análisis del panorama de amenazas



Sector

Macro-Inteligencia

Threat Intelligence (T.I.)

Objetivo

Micro-Inteligencia

Perfilado del Objetivo

Los atacantes seleccionan un objetivo, lo investigan e identifican cualquier punto débil que pueda ser clave para avanzar.

Personas

Procesos

Tecnología



Desarrollado por:

Mildrey Carbonell Castro,
Francisco Luis de Andrés Pérez.

Red Team (R.T.)

CAT, Cyber Attack Taxonomy

Movimientos Laterales

Identificados los nuevos objetivos dentro de la red, se procede a saltar de un equipo a otro hasta alcanzarlos.

Reconocimiento Interno

Una vez dentro de las instalaciones del objetivo, es necesario analizar toda la infraestructura para ver si existen medidas de seguridad avanzadas, u otros objetivos más valiosos

7º

Ejecución del Objetivo

Dstrucción de datos, la ocultación, o la exfiltración de los mismos

Compromiso

En esta fase se ejecutan las técnicas necesarias con el propósito de lograr generar brechas de seguridad en las infraestructuras del objetivo

Infiltración

Aprovechando las brechas de seguridad de la fase anterior, se cargan herramientas más dañinas y orientadas a allanar el camino hacia nuevas fases

Persistencia

En esta fase se ejecutan todas las tácticas y técnicas que aseguran la continuidad del ataque en cualquier evento que se produzca, así como la ocultación de cualquier rastro que pueda suponer la detección.

¿ Triple Extorsión ?

SERGAS: 7557

[REDACTED]@sergas.es

Sourced from Collections data

[Request entry removal ?](#)



[REDACTED]@sergas.es

Sourced from Collections data

[Request entry removal ?](#)



[REDACTED]@sergas.es

Sourced from geyseco.es (Cit0day) data

[Request entry removal ?](#)



[REDACTED]@sergas.es

Sourced from UnknownSite (Cit0day) data

[Request entry removal ?](#)



[REDACTED]@sergas.es

Sourced from clubcocinafacil.com (Cit0day) data

[Request entry removal ?](#)



Result #71118543

Email

[REDACTED]@sergas.es

Password

Espa?a.

Registros por Administración Gallega

Xunta: 3329

Deputación Ourense: 80

Deputación Pontevedra: 293

Deputación A Coruña: 24

Deputación Lugo: 420

Concello de Vigo: 519

Concello da Coruña: 270

Concello de Ourense: 37

Concello de Lugo: ¡0! <- ¿SIN SSL?

¿EMOTET?

¿REDES SOCIALES?

¿MAILS PERSONALES?

¿OTROS PORTALES DE ADMINISTRACIÓN SIN SSO?



Recursos Humanos en Deputación de Pontevedra Bueu

Current: Recursos Humanos at Deputación de Pontevedra



Gabinete de prensa · Deputación de Pontevedra Puenteareas

Current: Gabinete de prensa at Deputación de Pontevedra



Director de Comunicación en Deputación de Pontevedra Greater Vigo Metropolitan Area

Current: Director de Comunicación at Deputación de Pontevedra



Jefe de servicio cultura · Deputación de Pontevedra Greater Vigo Metropolitan Area

Current: Jefe de servicio cultura at Diputación de Pontevedra



Ingeniera de mantenimiento en Deputación de Pontevedra Greater Vigo Metropolitan Area

Current: Ingeniera de mantenimiento at Deputación de Pontevedra



Técnica de gestión en Deputación de Pontevedra Greater Vigo Metropolitan Area

Current: Técnica de gestión at Deputación de Pontevedra




Gestión de programas en Deputación de Pontevedra Bueu

Current: Gestión de programas at Deputación de Pontevedra




Legal Counsel at Deputación de Pontevedra Albeancos

Past: Legal Counsel (asistencia técnica) at Xunta de Galicia




Ingeniero Informático en Diputación Provincial de Ourens...

Connect




Técnico Superior Desenvolvemento Local...




Técnica de gestión y ejecución de Proyectos Europeos

Connect




Agente de empleo y desarrollo local. Administración local

Connect




--




Director Area Medio Ambiente en Diputación Provincial de Ourense

Connect




Computer Science and New Technologies Manager

Message




Técnico Desarrollo Local y Fondos Europeos en Diputación...




Jefa de Negociado en Diputación de Ourense


Message



Ingeniero de Caminos, Canales y Puertos



Técnico de desarrollo de aplicaciones en Deputación...



Arquitecto en Diputación Provincial de Ourense

¿ Formato de Correo Electrónico?
¿ Cruce con otras Redes Sociales?
¿ Ingeniería Social?

• [Redacted] Compliant [Redacted] Entorno [Redacted]

Está orientado a albergar aplicaciones JEE más críticas, o de cierta criticidad, que requieren niveles de servicio más elevados. De igual modo, también está destinado a aplicaciones en donde se requieran capacidades JEE que no están incluidas en un simple contenedor web. La selección de esta plataforma en lugar de la plataforma Tomcat para nuevos proyectos, se debe decidir en base a criterios como complejidad de la arquitectura, criticidad, afinidad de: negocio, tecnológica, de administración, de soporte, etc.

Nota: la plataforma [Redacted] también es corporativa, pero no se recomienda para nuevos desarrollos.

• [Redacted] con [Redacted] Entorno UNIX.

Su uso quedará reducido a los entornos ya existentes y, de ser necesario, en proyectos en los que no encajen las soluciones estándar [Redacted], su uso deberá ser correctamente argumentado y consensuado con el equipo de Arquitecturas Tecnológicas. Esta plataforma seguirá manteniendo el soporte de fabricante.

Nota: la plataforma [Redacted] también es corporativa, pero no se recomienda para nuevos desarrollos. Es importante que los proyectos empiecen a migrar a la nueva versión.

• [Redacted] Para aplicaciones .NET bajo entorno [Redacted] (con soporte a versiones inferiores).

Su uso está reservado a proyectos existentes y nuevas aplicaciones que deban utilizar plataforma Windows: en estos casos, su uso deberá ser correctamente argumentado y consensuado con el equipo de Arquitecturas Tecnológicas.

Nota: la plataforma [Redacted] también es corporativa, pero no se recomienda para nuevos desarrollos.

2.5. Generador de informes/documentos

• [Redacted] Plataforma de reporting para la generación de informes (listados) en varios formatos de salida: pdf, html, xml, etc.

• [Redacted] Servidor para la generación de documentos y conversión de formatos, en base a plantillas, por parte de las aplicaciones. El acceso a este servidor debe ser a través de los servicios existentes para este propósito.

2.6. Servidores de bases de datos

• [Redacted] (codificación ALCOA) Es la opción corporativa a utilizar en nuevos proyectos. Por defecto se utiliza el modo de clúster Oracle RAC. Si en alguna aplicación no encaja el uso de Oracle RAC por algún motivo, se podrán usar servicios [Redacted] para simular el comportamiento de una base de datos Single Instance. Este aspecto deberá ser argumentado y consensuado con el equipo de Arquitecturas Tecnológicas.

• [Redacted] La selección de esta plataforma en lugar de la de Oracle para nuevos proyectos, se debe decidir en base a criterios como la afinidad de negocio, tecnología, administración, soporte, etc., previa

• [Redacted] Es una solución disponible para ámbitos reducidos, por lo que su uso debe argumentarse y consensuarse con el equipo de Arquitecturas Tecnológicas en cada caso

• **Correo**

Servicio de correo en el ámbito Xunta basado en Microsoft:

• [Redacted]

Nota: está prevista una próxima instalación de la versión [Redacted]

• [Redacted] Servicio de archivado de correo para [Redacted]

Servidor de correo actual en los ámbitos de Educación y Justicia basado en:

• [Redacted]

• **Vulnerabilidades**

• [Redacted] Para el análisis de vulnerabilidades en aplicaciones web.

• [Redacted] Servicio online en la Amtega para la detección de virus

[83] Plataforma de empleo

Los componentes de la arquitectura actual son:

- Base de datos: [Redacted]
- Back-end: [Redacted]
- ESB: [Redacted] en versión standalone.
- Front-end: [Redacted]
- Sistema de SSO: [Redacted]
- Repositorio de identidades: [Redacted]

Base de datos

El motor de base de datos en el momento de la redacción del pliego es un [Redacted] con la posibilidad de que durante el proceso de licitación y tramitación del presente procedimiento el motor de base de datos sea migrado a versiones más recientes

Está prohibido el desarrollo de procedimientos almacenados que sean procesos de negocio.

Back-end

El back-end está formado por un conjunto de clases java que realizan el acceso a datos y realizan las comprobaciones y transformación de datos antes de escribirlos o leerlos.

En este elemento de arquitectura están construidas las primitivas de los procesos de negocio.

El back-end ofrece al ESB un conjunto de webservices que en sí, o son procesos de negocio atómicos, o son

- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8243
- CVE-2019-11539
- CVE-2019-11510

Pulse
Secure VPN



- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-19781
- CVE-2019-11634

Citrix



Microsoft
Exchange



- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855

- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

Fortinet



- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

SonicWall



- CVE-2021-22986
- CVE-2020-5902

F5



- CVE-2020-2021
- CVE-2019-1579

Palo Alto



QNAP



- CVE-2021-28799
- CVE-2020-36198

- CVE-2020-12271

Sophos



- CVE-2019-0604

SharePoint



- CVE-2019-0708

RDP



- CVE-2017-0199

Microsoft
Office



- CVE-2021-21985

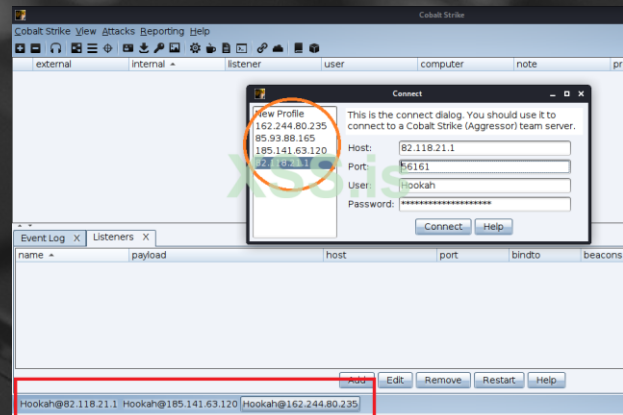
vCenter



Conti Affiliate Leak

For example, the leaked manuals contain guides on how to:

- configure the **Rclone** software with a MEGA account for data exfiltration
- configure the **AnyDesk** software as a persistence and remote access solution into a victim's network [a *known Conti tactic*]
- configure and use the **Cobalt Strike** agent
- use the NetScan tool to scan internal networks
- install the **Metasploit** pen-testing framework on a virtual private server (VPS)
- connect to hacked networks via RDP using a **Ngrok** secure tunnel
- elevate and gain admin rights inside a company's hacked network
- take over domain controllers
- dump passwords from Active Directories (NTDS dumping)
- perform SMB brute-force attacks
- brute-force routers, NAS devices, and security cameras
- use the **ZeroLogon** exploit
- perform a **Kerberoasting** attack
- disable Windows Defender protections
- delete shadow volume copies
- how affiliates can configure their own operating systems to use the Tor anonymity network, and more





¡ Gracias !

¿ Preguntas ?



/afernandesvigo