Uruguay ciber SEGURO 2021

Del 22 al 26 de noviembre

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento

CCN / CCN-CERT

Ciberamenazas y Tendencias 2021

Javier Candau
Jefe Departamento Ciberseguridad
Centro Criptológico Nacional
ccn@cni.es
jdciber@ccn.cni.es

CCN centro criptológico nacional

Código dañino (malware)

- Es un programa pequeño que se ejecuta sin el conocimiento o el permiso del usuario, teniendo como objetivo infiltrarse o alterar el normal funcionamiento del Sistema.

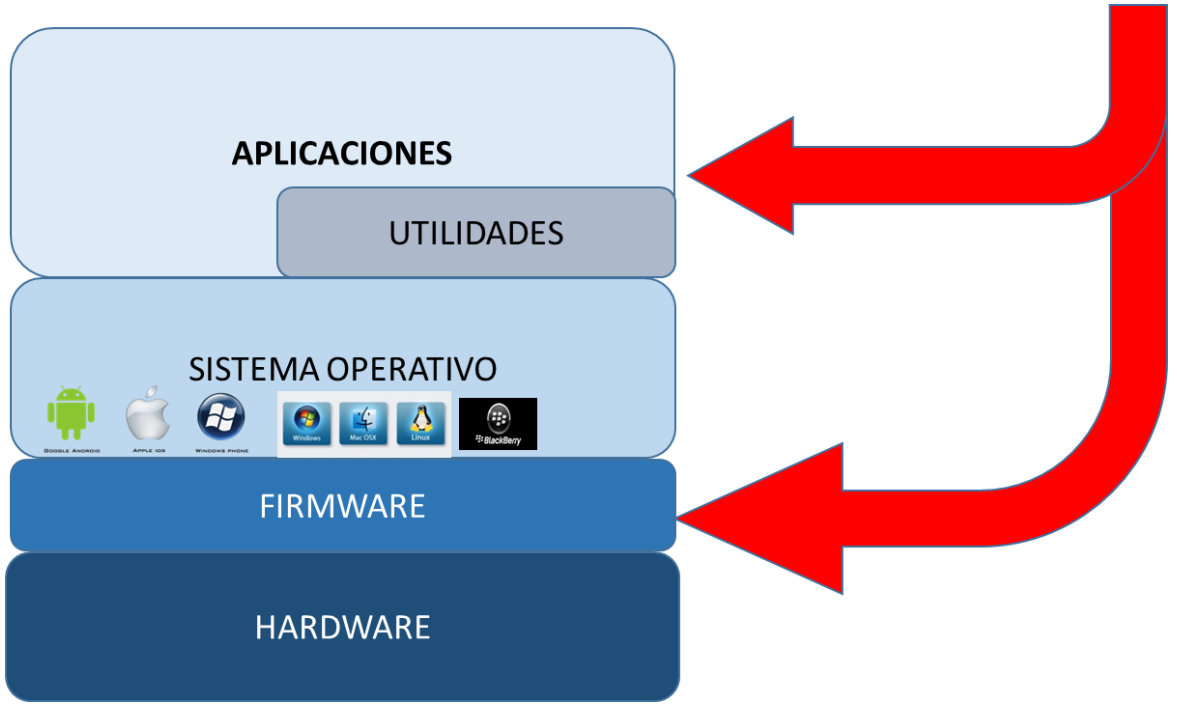
¿Qué se necesita para que un Ciberataque tenga éxito?

- **Vulnerabilidad** + explotar esa vulnerabilidad creando un “arma” **(exploit) + ingeniería social** =

Vector de infección

Vulnerabilidades de la tecnología:

- Vulnerabilidades públicas (CVE)
- Vulnerabilidades Día 0
- Vulnerabilidades Día 1



Índice

1. Conceptos
2. Centro Criptológico Nacional / CCN-CERT.
3. Normativa Servicios esenciales
4. Agentes de la amenaza
5. Casos 2017-2021
6. Defensa vs Ataque. CONCLUSIONES

2020
2030

NIS 1.0 / NIS 2.0

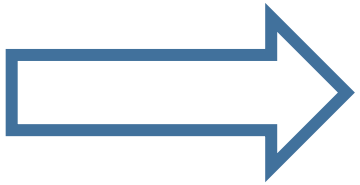
RDL 12/2018 / RD 43/2021

TD + Ciberseguridad
Defensa activa
Ciberinteligencia

- Accesos remotos / Uso de la nube
- **Auditoria / vigilancia continua**
- Respuesta integrada
- Zero Trust
- Seguridad por defecto (CERTIFICACIÓN)
- **Intercambiar ciberincidentes**

ens Esquema Nacional de Seguridad

2010



ens Esquema Nacional de Seguridad 2021

CCN centro criptológico nacional

SECTOR PÚBLICO. Esquema Nacional de CiberSeguridad

5

6 Principios básicos

a) Seguridad integral
b) Gestión de riesgos
c) Prevención, reacción y recuperación
d) Líneas de defensa
e) Reevaluación periódica
f) La seguridad como función diferenciada

75 Medidas de seguridad

a) Marco organizativo
b) Marco operacional
c) Medidas de protección

15 Requisitos mínimos

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de riesgos
c) Gestión del personal
d) Profesionalidad
e) Autorización y control de accesos
f) Protección de las instalaciones
g) Adquisición de productos
h) Seguridad por defecto
i) Integridad y actualización del sistema
j) Protección de la información almacenada y en tránsito
k) Prevención ante otros sistemas de información interconectados
l) Registro de actividad
m) Incidentes de Seguridad
n) Continuidad de la actividad
o) Mejora continua del proceso de seguridad

ens Esquema Nacional de Seguridad

1. Los **Principios básicos**, que sirven de guía.
2. Los **Requisitos mínimos**, de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS. **Sellos de conformidad.**
5. La **respuesta a incidentes de seguridad**. Papel del CCN- CERT. **Notificación**
6. El uso de **productos certificados**. Papel del Organismo de Certificación (CCN).
7. La **formación y concienciación**.
8. Serie 800 Guías CCN-STIC (**57 documentos**)

Categoría BÁSICA: 45 controles (60%)
Categoría MEDIA: 63 controles (84%)
Categoría ALTA: 75 controles (100%)

CCN centro criptológico nacional

CCN / CCN-CERT

- Ley 11/2002 reguladora **del Centro Nacional de Inteligencia.**
- RD 421/2004, 12 de Marzo, que regula y define el ámbito y funciones del **CCN**.

- RD 3/2010, 8 de Enero, que define el **Esquema Nacional de Seguridad** para la Administración Electrónica, modificado por el RD 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, las tecnologías de la información y experiencia de implantación.

- RDL 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información. **Coordinación incidentes.**
- RDL 14/2019, de 31 de octubre, Medidas urgentes. **Coordinación CSIRT públicos y enlace con exterior**
- RD 43/2021, de 28 de enero, Desarrollo RDL 12/2018. **Plataforma Nacional**

MISIÓN

Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al **Sector Público** a afrontar de forma activa las nuevas ciberamenazas.

COMUNIDAD

Responsabilidad en ciberataques sobre:

- **sistemas clasificados**,
- sistemas del **Sector Público**,
- empresas y organizaciones de **sectores estratégicos** para el país en coordinación con el CNPIC.

PREVENCIÓN

Reducir la superficie de exposición

- Proporcionar guías y estándares de seguridad
- Avisos y vulnerabilidades
  - Amenazas | Malware | Mejores prácticas
- Auditorías | Inspecciones
  - Implantación ENS
- Formación

DETECCIÓN

Vigilancia Continua

- Detección y Respuesta ante ciberataques
  - Despliegue de RRT
- Intercambio de información
  - ciberincidentes y ciberamenazas
  - Plataforma Nacional

RESPUESTA

Eficiente e integrada

- Centro de Operaciones de Ciberseguridad
  - Red Nacional de SOC,s
- Coordinación técnica de CERTs / SOC,s

CCN
centro criptológico nacional

SOLUCIONES CCN-CERT

Auditoría

- </inés>
- </pilar>
- </amparo>
- </clara>
- </rocío>
- </emma> — EMMA-VAR
- </ana>
- </carla>

Detección

- </sat-inet>
- </sat-sara>
- </sat-ics>
- Sonda distribuida

Soluciones basadas en IA

Análisis

- </gloria>
- </ada> MARTA y MARIA
- </maría>
- </marta>

Vigilancia

- </carmen>
- </claudia>
- </μclaudia>
- ALICIA

Soluciones basadas en IA

Intercambio

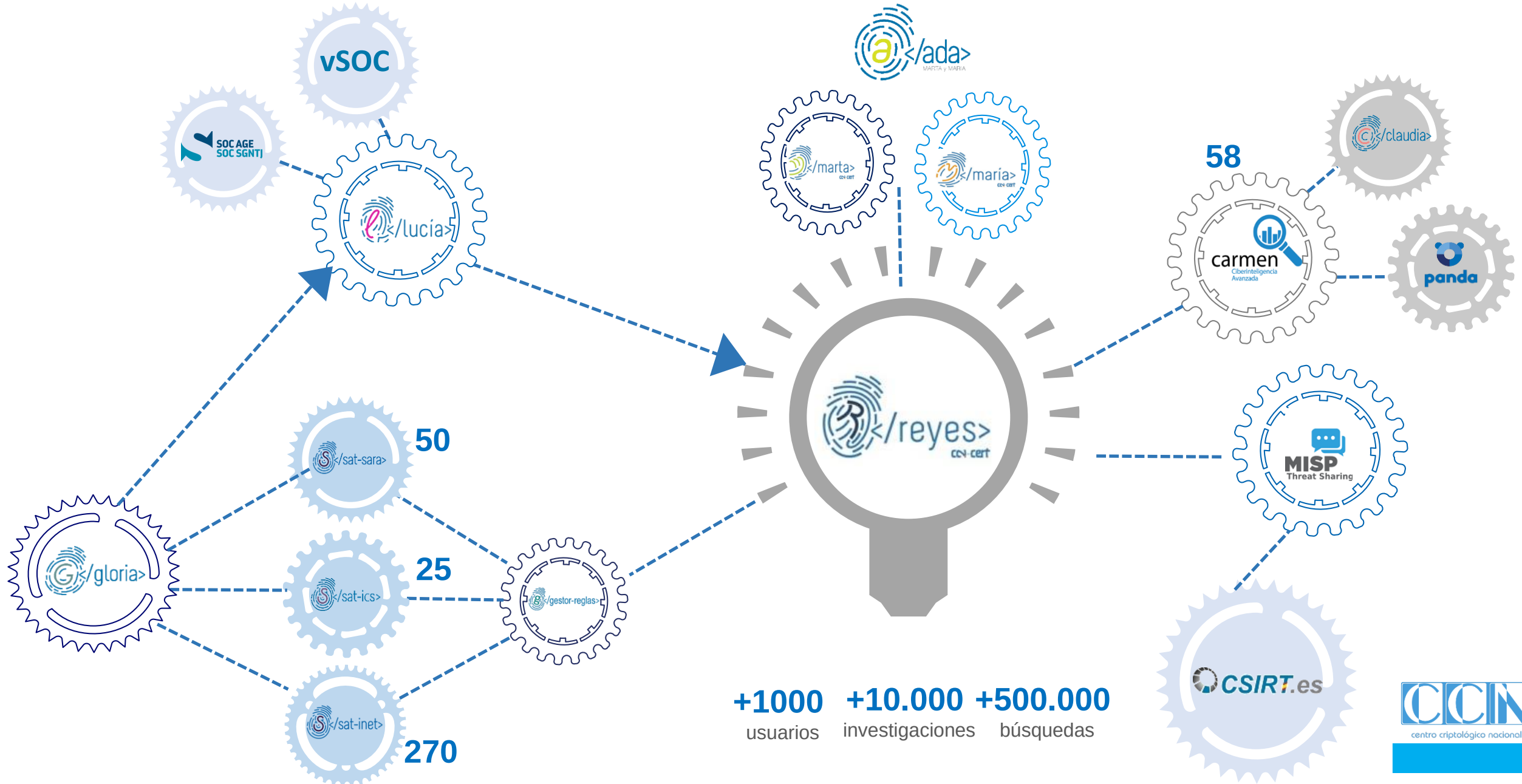
- </lucía>
- </loreto>
- </reyes>

Formación

- </vanesa>
- ATENEA — Plataforma de desafíos de seguridad — CCN-CERT
- ángeles — Formación y Talento en Ciberseguridad
- </elena> — Simulador de Cibervigilancia

CCN centro criptológico nacional

1 Vigilancia Continua. Ciberinteligencia

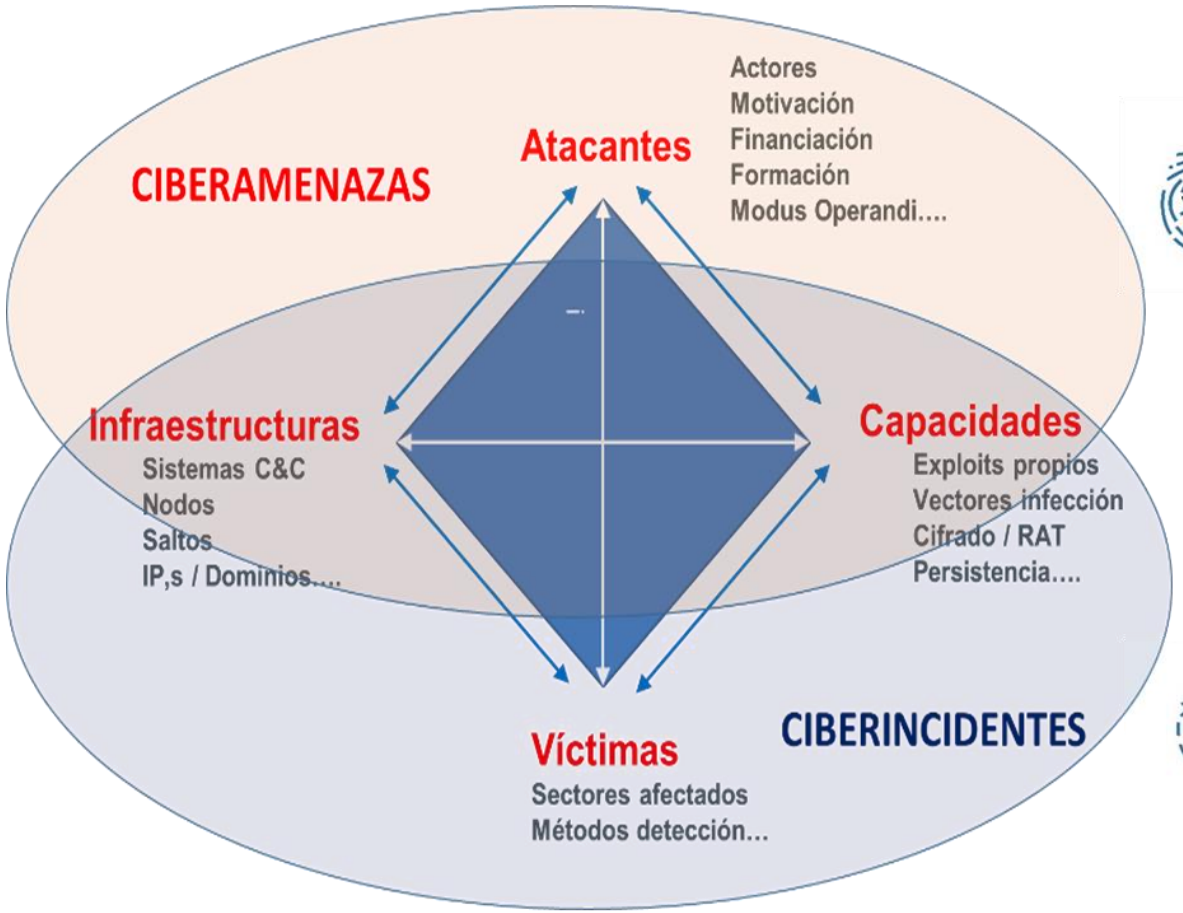


+1000 usuarios

+10.000 investigaciones

+500.000 búsquedas

CCN centro criptológico nacional



CERT/CSIRT

</reyes>

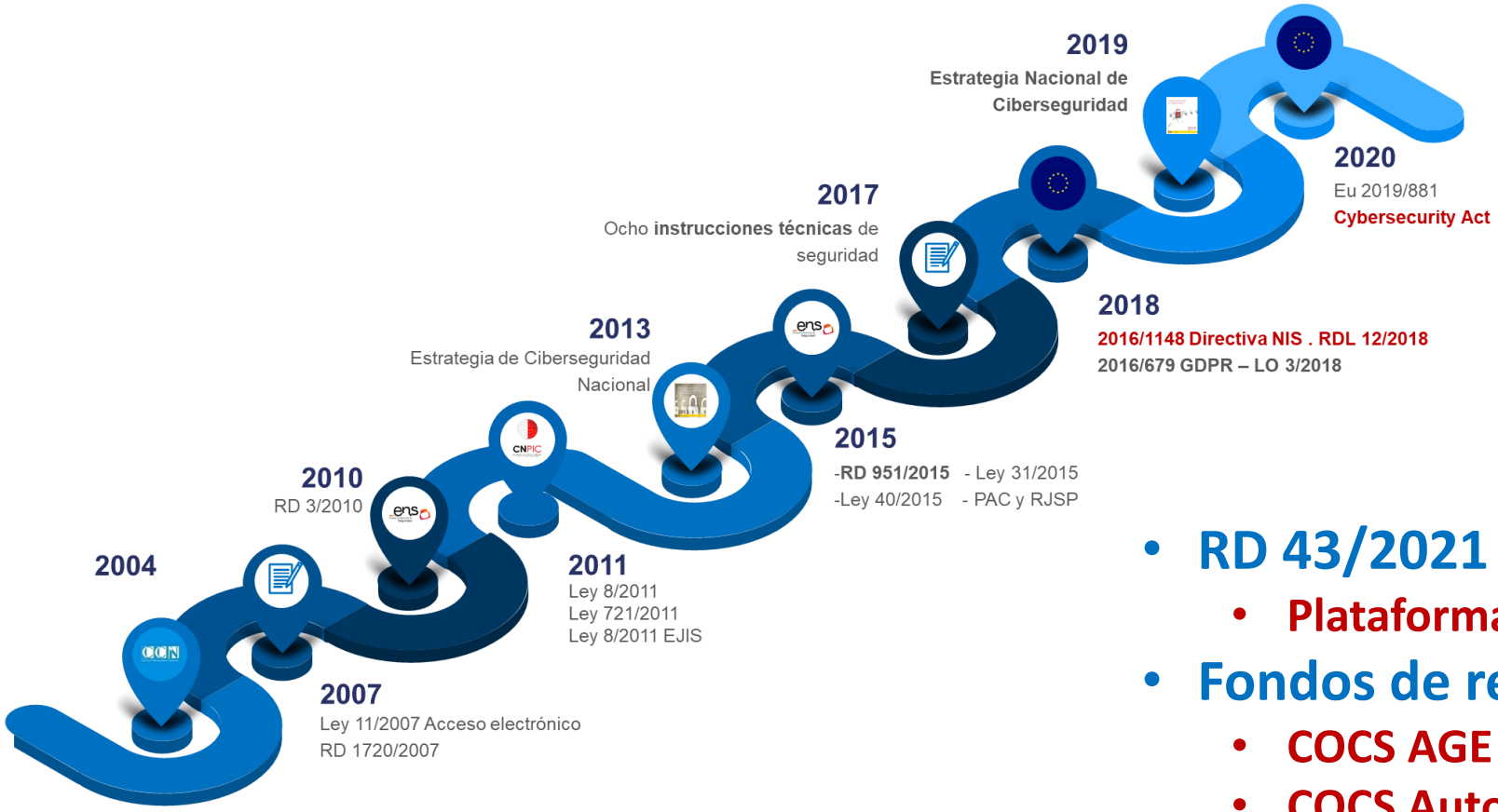
Comunidad

CERT/CSIRT

</lucía>

Comunidad

3 Actualización Normativa



- RD 43/2021 Desarrollo RDL 12/2018 (NIS)
  - Plataforma común
- Fondos de reconstrucción
  - COCS AGE
  - COCS Autonómicos / provinciales
- Autoridad Nacional de certificación
- NIS 2.0 Estrategia Ciberseguridad UE
- ENS 2021 ???

CCN centro criptológico nacional

Ley 8/2011 IC - 2016/1148 Directiva NIS – RDL 12/2018

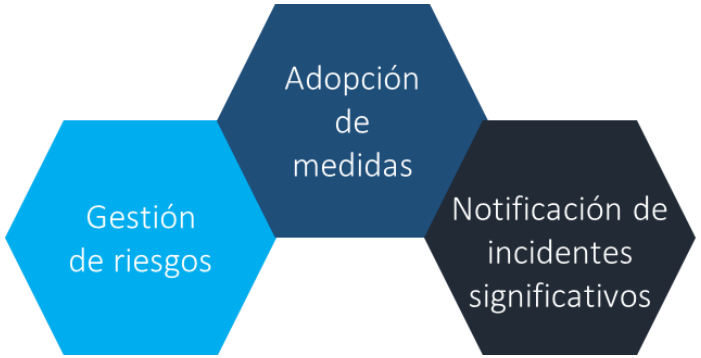
NIS 1.0

Industria nuclear	Administración	Espacio
Alimentación	Industria Química	Inst. Investigación
Hídrico	Sanidad	Transportes
Banca y mercados financieros	Infraestructuras y Serv Digitales (TIC)	Energético

Infraestructuras críticas

Servicios esenciales

Mayoría operadores Públicos



LECCIONES APRENDIDAS DE NIS 1.0

- **Criterios de Designación OSE /PSD**
  - Mucha diferencia entre estados / Criterios muy diferentes
- **No hay conjunto de medidas de seguridad**
  - Autoridades competentes deben supervisar
- **Notificación de incidentes**
  - No hay criterios para incidentes transfronterizos
- **Informe de estado de seguridad (ENISA)**
  - Similar al informe INES

Impacto directiva NIS 2.0

MÁS SECTORES

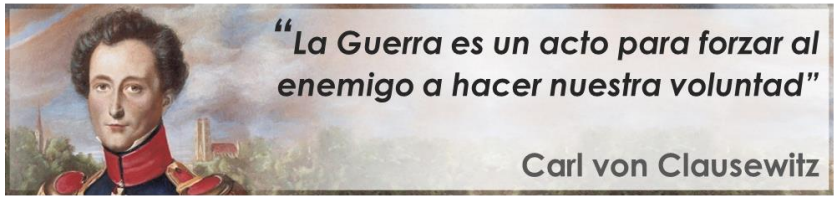
2 REGIMENES DE REGULACIÓN

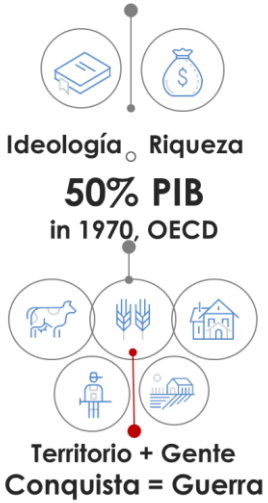
Essential entities	Important entities
Energy (electricity*, district heating, oil, gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)	
Public administrations	
Space	

AUTORIDADES COMPETENTES DEBEN SUPERVISAR MEDIDAS DE SEGURIDAD ARMONIZADAS

* New types of entities in electricity: electricity markets, production, aggregation, demand response and energy storage

2 Agentes de la amenaza





Estas compañías significan

18%

Del Mercado de valores USA

Y USA significa

25%

Del PIB global

Microsoft Google amazon

Insignificante

Gente & Territorio

CCN centro criptológico nacional

Ciberguerra: Las nuevas armas.

Robo:	*"Tomar la propiedad de otro, con la intención de privarlo permanentemente de la misma."*	2017.08 Equifax Ransomware
Extorsión:	*"Practica de obtener algo, especialmente dinero a través de FUERZA o AMENAZA."*	2017.05 WannaCry 2017.06 Bad Rabbit
Propaganda Desinformación:	"Influenciar los votantes de un país para beneficiar a una potencia extranjera."	2015 Brexit 2016 Elecciones USA 2017 Cataluña 2018 Brasil
Espionaje:	*"Acto de manera secreta adquirir información sensible o clasificada."*	2013.10 Teléfonos móviles de líderes europeos. 2014 SNAKE 2015 Snowden
Sabotaje:	*"Intento deliberado de debilitar / deshabilitar los servicios esenciales, sistemas económicos o de defensa."*	2010.07 Stuxnet 2012.08 Shamoon infectó 30,000 equipos de Aramco Interrumpió las operaciones más de 2 semanas. 2015 Blackenergy 2017 NotPetya

Resultado final ● **Transferencia de Riqueza**

Incidentes 2021

82.530 ciberincidentes en 2020

+70.000 ciberincidentes en 2021

+ 12000 ciberincidentes de LUCIA

11.000 en 2020

+ 100 ciberincidentes CRÍTICOS

64 en 2020

+ 3.500 muy alto o crítico

CCN centro criptológico nacional

Definiciones

CIBERSEGURIDAD

La habilidad de proteger y defender las redes o sistemas de los **ciberataques.** Estos según su motivación pueden ser:

CIBERESPIONAJE

Ciberataques realizados para obtener secretos de estado, propiedad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal.

CIBERDELITO / CIBERCRIMEN

Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito.

CIBERACTIVISMO

Activismo digital antisocial. Sus practicantes persiguen el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social.

CIBERTERRORISMO

Actividades dirigidas a causar pánico o catástrofes realizadas en las redes y sistemas o utilizando éstas como medio.

CIBERCONFLICTO / CIBERGUERRA / GUERRA HÍBRIDA

Operación dirigida por un Estado que utiliza tácticas abiertas y encubiertas con el objetivo de desestabilizar otros Estados y polarizar a la población civil. Incluye una gran variedad de herramientas como diplomacia y acciones de inteligencia tradicional, actos subversivos y de sabotaje, influencia política y económica, instrumentalización del crimen organizado, operaciones psicológicas, propaganda y desinformación y ciberataques

CIBERATAQUE

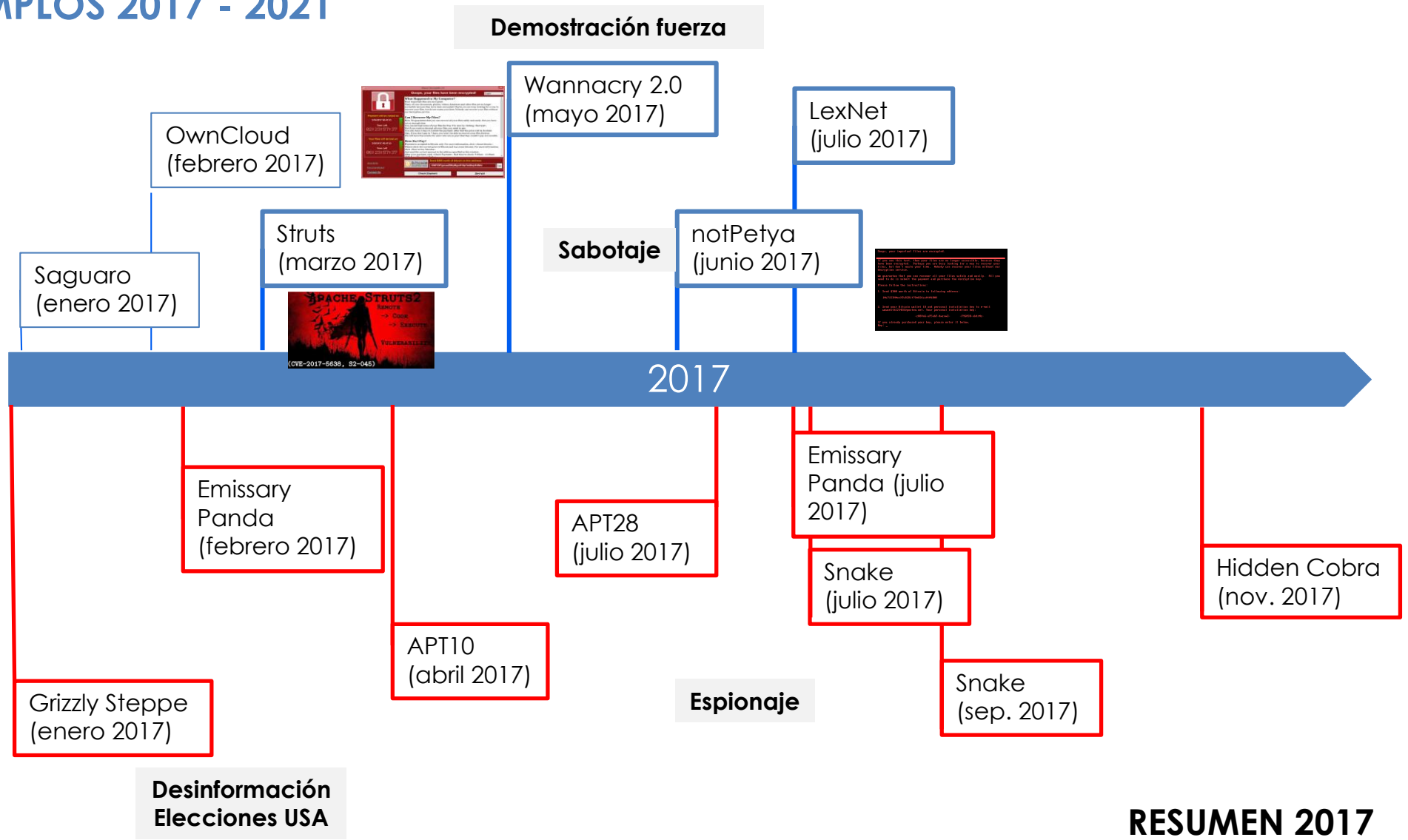
Uso de redes y comunicaciones para acceder a información y servicios sin autorización con el ánimo de robar, abusar o destruir.

Agentes de la amenaza

1. Ciberespionaje / Robo patrimonio tecnológico, propiedad intelectual
   - China, Rusia, Irán, otros…
     - Servicios de Inteligencia / Fuerzas Armadas / Otras empresas
2. Ciberdelito / cibercrimen
   - HACKERS y crimen organizado
3. Ciberguerra / ciberconflicto / Guerra híbrida
   - Ataque a Infraestructuras críticas y otros servicios
4. Hacktivismo
   - ANONYMOUS y otros grupos
5. Uso de INTERNET por terroristas
   - Objetivo : Comunicaciones , obtención de información, propaganda, radicalización o financiación
6. Ciberterrorismo
   - Ataque a Infraestructuras críticas y otros servicios

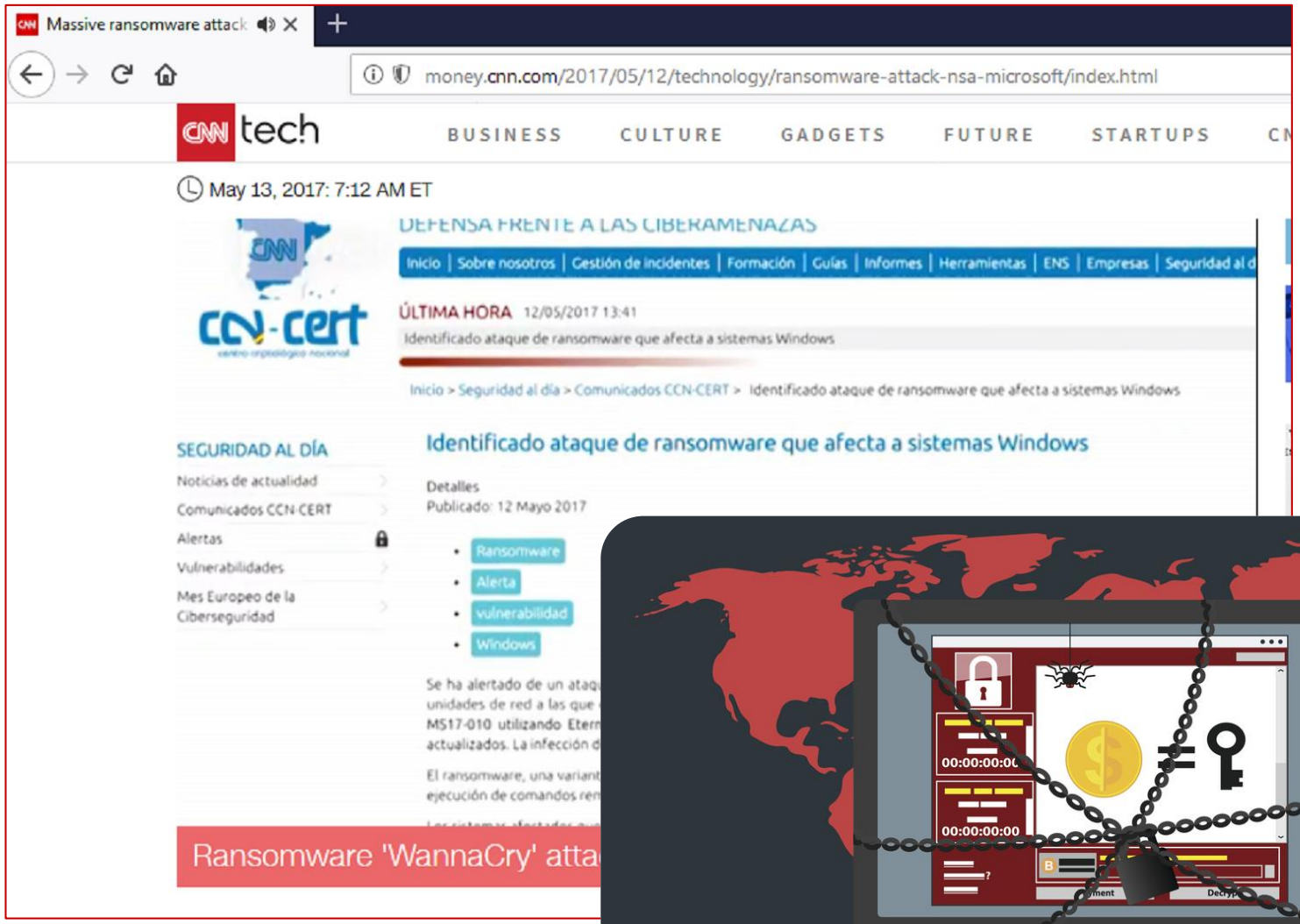
Usuarios internos

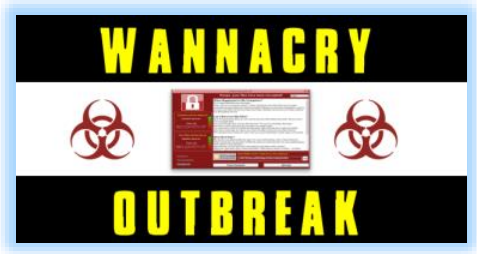
5 EJEMPLOS 2017 - 2021



RESUMEN 2017

Ransomware





El "*ransomware*" está contribuyendo a hacer la **ciberamenaza REAL**

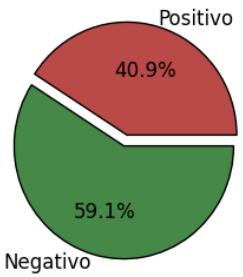
¿Qué puedo hacer?

CCN centro criptológico nacional

WannaCry como caso de estudio para futuros ciberataques

Análisis solicitado por info@ccn-cert.cni.es
Fecha: 2017-05-12 17:00:36
Nombre: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin
Tamaño: 3514368 bytes
Tipo de fichero: PE32 executable (GUI) Intel 80386, for MS Windows
Tipo MIME: application/x-dosexec
MD5: 84c82835a5d21bbcf75a61706d8ab549
SHA1: 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

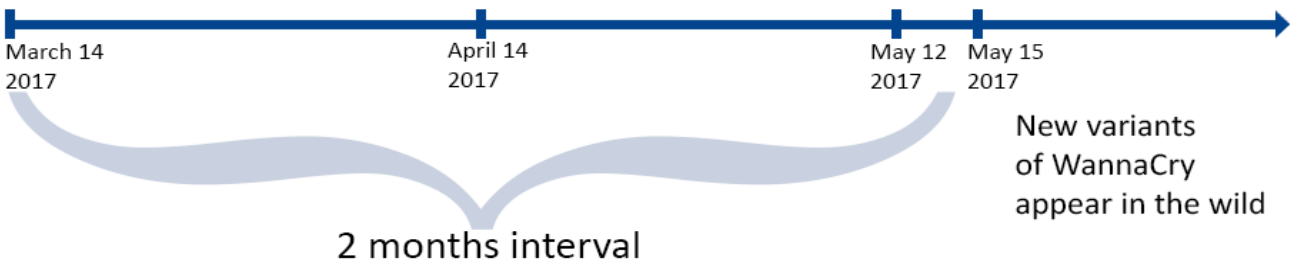
Resultado: POSITIVO

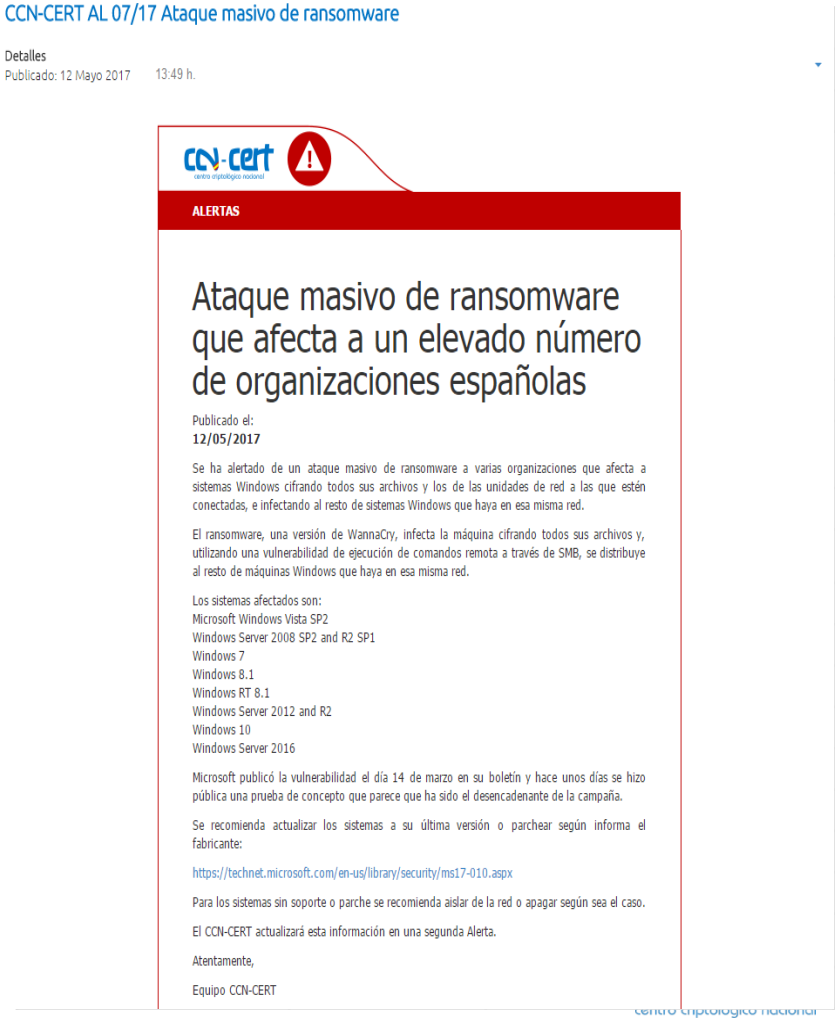


Microsoft Security Bulletin MS17-010 - Critical

ShadowBrokers leak

WannaCry 2.0 ransomeware outbreak started appearing in the wild.




CCN-CERT AL 07/17 Ataque masivo de ransomware

Detalles
Publicado: 12 Mayo 2017 13:49 h.

ALERTAS

Ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas

Publicado el:
12/05/2017

Se ha alertado de un ataque masivo de ransomware a varias organizaciones que afecta a sistemas Windows cifrando todos sus archivos y los de las unidades de red a las que estén conectadas, e infectando al resto de sistemas Windows que haya en esa misma red.

El ransomware, una versión de WannaCry, infecta la máquina cifrando todos sus archivos y, utilizando una vulnerabilidad de ejecución de comandos remota a través de SMB, se distribuye al resto de máquinas Windows que haya en esa misma red.

Los sistemas afectados son:
Microsoft Windows Vista SP2
Windows Server 2008 SP2 and R2 SP1
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2012 and R2
Windows 10
Windows Server 2016

Microsoft publicó la vulnerabilidad el día 14 de marzo en su boletín y hace unos días se hizo pública una prueba de concepto que parece que ha sido el desencadenante de la campaña.

Se recomienda actualizar los sistemas a su última versión o parchear según informa el fabricante:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Para los sistemas sin soporte o parche se recomienda aislar de la red o apagar según sea el caso.

El CCN-CERT actualizará esta información en una segunda Alerta.

Atentamente,

Equipo CCN-CERT

NotPetya Ransomware Attack Cost Shipping Giant

https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-

Maersk CEO now sees the good side of the incident

"It was an important wake-up call," he said. "We were basically average when it comes to cyber-security, like many companies. And this was a wake-up call to become not just good —we actually have a plan to come in a situation where our ability to manage cyber-security becomes a competitive advantage."

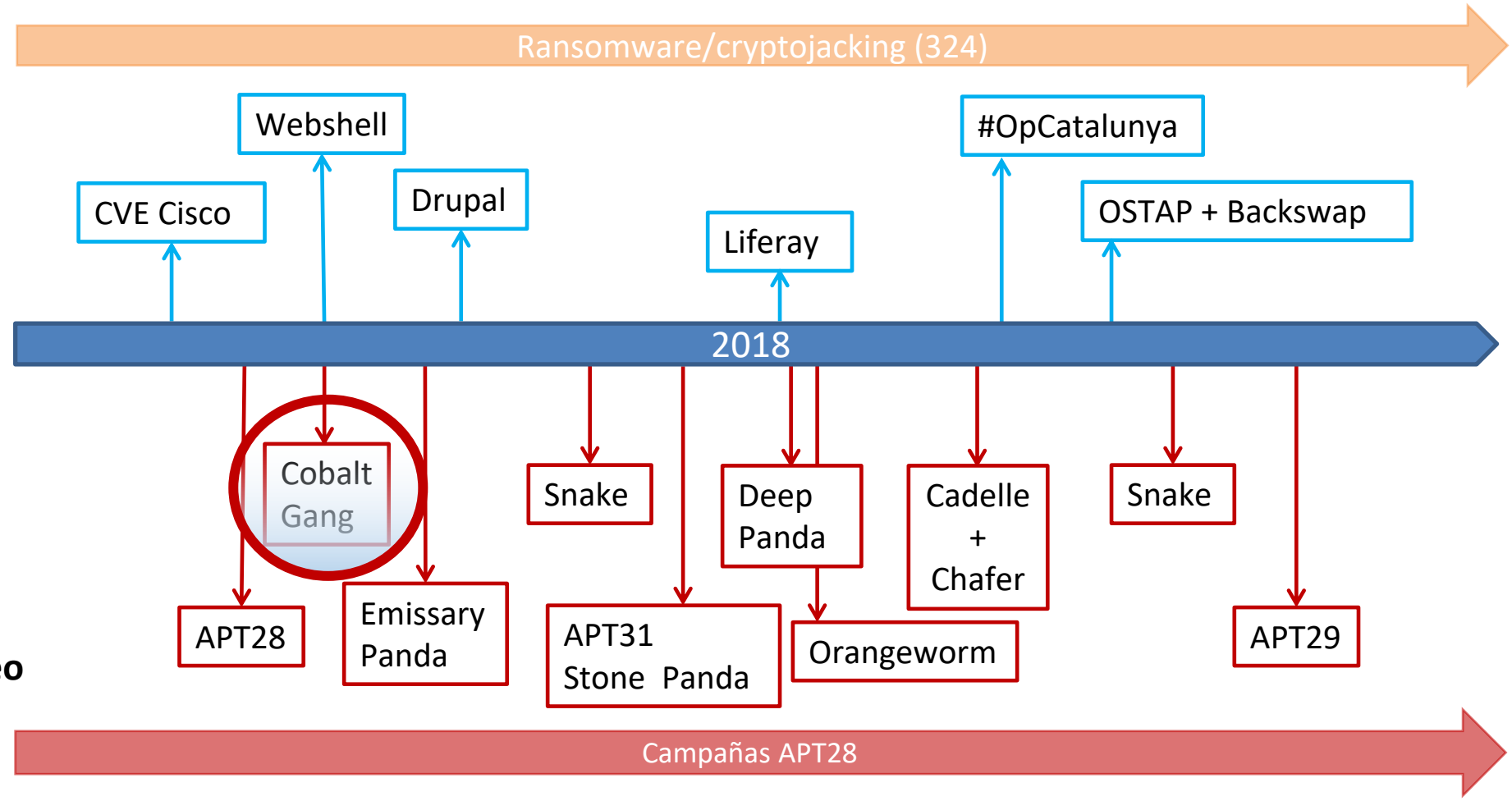
In the subsequent discussions, Snabe also urged fellow Davos World Economic Forum participants to focus on securing cyberspace.

A video of Snabe's comments regarding Maersk's NotPetya recovery efforts, and more, is embedded below. The discussion is right at the beginning, following the 02:20 mark.

revenues rising from $8.7 billion to $9.6 billion year-over-year.

CCN
centro criptológico nacional

INCIDENTES 2018



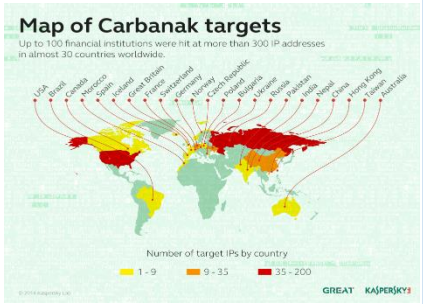
AAPP
Aeronáutico
Bancario
Energía
Salud
Transporte Aereo
TIC

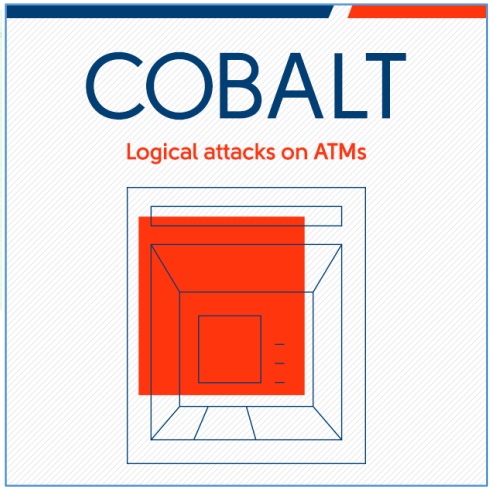
RESUMEN 2018

CIBERCRIMEN: CARBANAK / COBALT GANG

Cibercrimen usando técnicas APT:

- “Spear phishing” simulando comunicaciones bancarias.
- Movimientos laterales: Ammyy RAT y comprometimiento de servidores SSH.
- Grabaciones vídeo de empleados (particularmente administradores).
- Uso de red SWIFT, actualización balances y mecanismos de desembolso (ATM).
- Fondos transferidos a cuentas bancarias de USA y China.





CCN
centro criptológico nacional

Cae en España el 'hacker' de los 10.000 millones, el ciberladrón más importante del mundo: Carbanak

PABLO HERRAIZ QUICO ALSEDO 27 MAR. 2018 | 10:11

Una de las 'mulas' de la banda Carbanak, robando dinero de un cajero. / Vídeo: EL MUNDO

ALERTAS

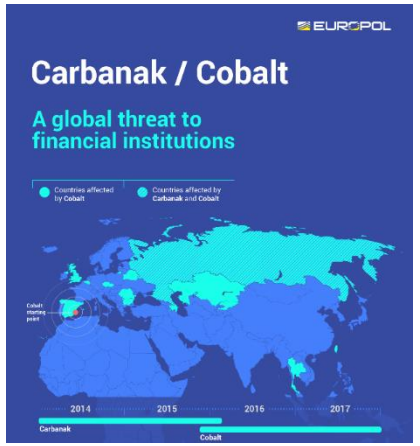
Detectada una campaña del Grupo Cobalt Gang contra el sector bancario

Publicado el: **23/03/2018**

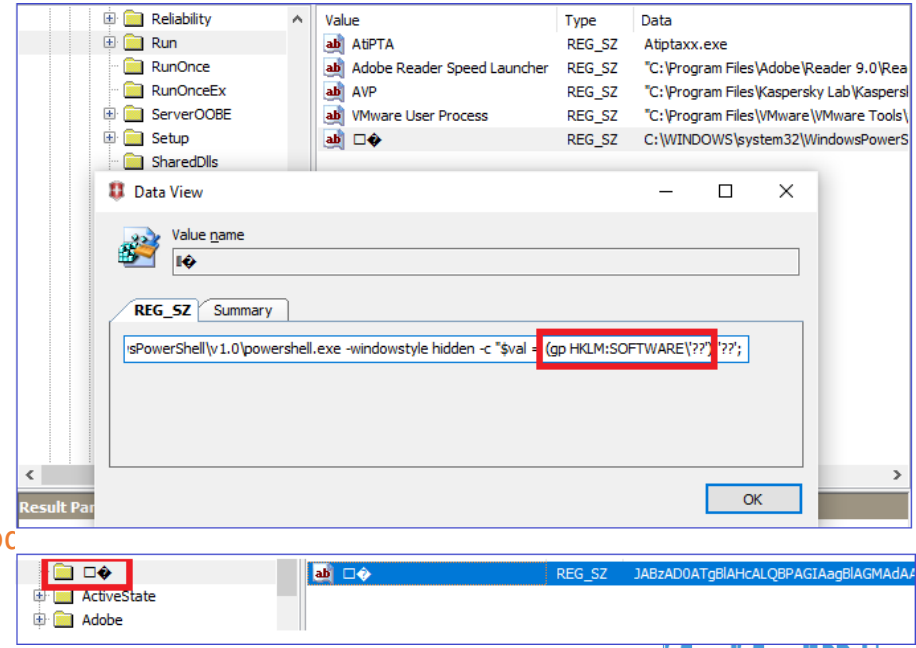
Nivel de criticidad: **Crítico**

El Equipo de Respuesta a incidentes del Centro Criptológico Nacional, CCN-CERT, alerta sobre la existencia de una campaña muy agresiva contra el sector bancario, por parte del grupo Cobalt Gang. Este grupo, relacionado con el cibercrimen, inició su actividad en el año 2016 y, desde entonces, ha realizado numerosas campañas en las que ha sustraído importantes cantidades de dinero a las entidades afectadas.

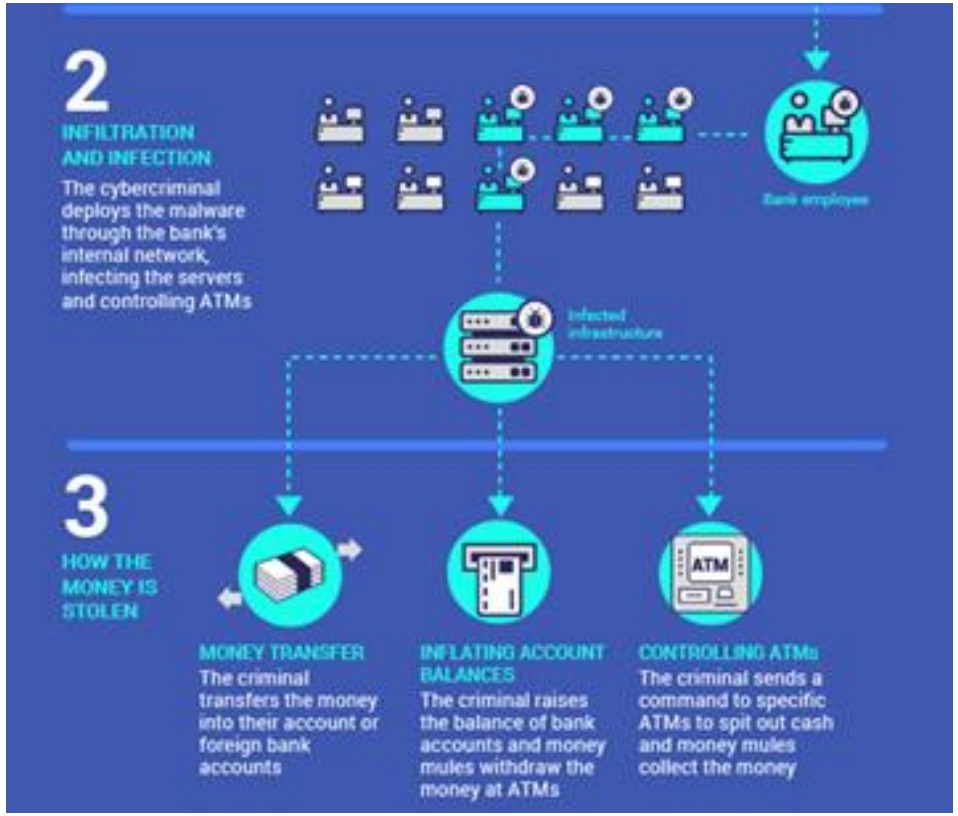
El grupo utiliza, entre otras herramientas, la denominada Cobalt Strike y su primera incursión suele realizarse a través de las técnicas de *Spear-phising* y explotando las vulnerabilidades del sistema.



- **Modus operandi & malware:**
  - Obtención de credenciales de usuarios privilegiados, creación de nuevos.
  - Reconocimiento de red → servidores de interés.
  - Cobalt Strike Beacon en modo SMB/*named pipe* **(14.03.2018)**.
  - Uso y abuso de Powershell: como servicio o ejecutado via CSB.
  - Despliegue por etapas, con ofuscación:
    - 1ª etapa: servicio Powershell + script ofuscado
    - 2ª etapa decodifica y descomprime (Gzip) otro script PS
    - 3ª etapa: script (OSINT) que inyecta *shellcode* (espacio de memoria proceso legítimo) → mod
      named pipe (interno) o modo HTTP (hacia los C2)

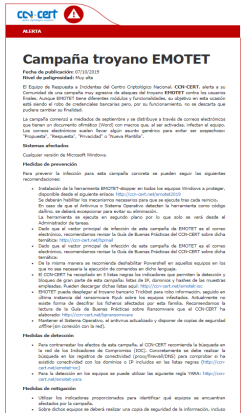


centro criptológico nacional



CCN
centro criptológico nacional

Ciberincidentes relevantes 2019



Emotet #23

Emotet #24

Enero | Febrero | Marzo | Abril | Mayo | Junio | Julio | Agosto | Septiembre | Octubre | Noviembre | Diciembre

2019

???

APT39

Snake

APT39

APT33

Cobalt Gang

Snake

+30

Organismos afectados

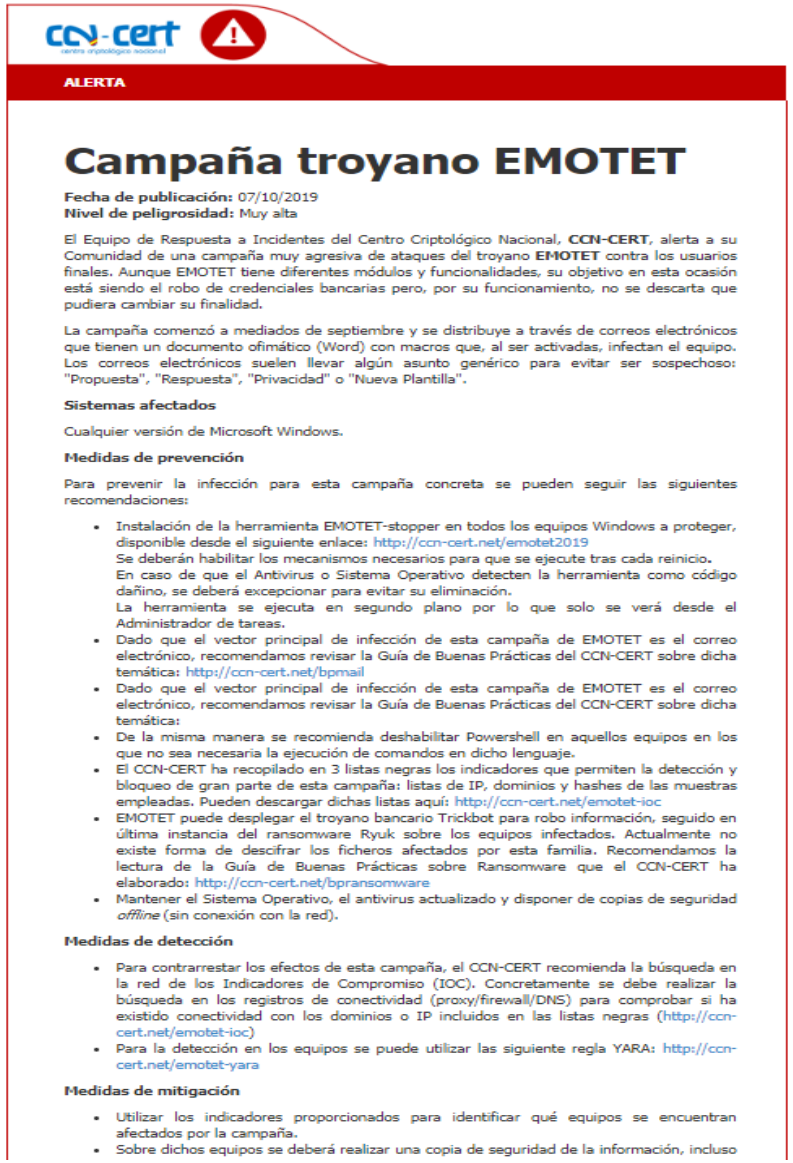
Campañas APT

CCN centro criptológico nacional

Lecciones aprendidas. Ransomware

+30

Organismos afectados



ALERTA

Campaña troyano EMOTET

Fecha de publicación: 07/10/2019
Nivel de peligrosidad: Muy alta

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, **CCN-CERT**, alerta a su Comunidad de una campaña muy agresiva de ataques del troyano **EMOTET** contra los usuarios finales. Aunque EMOTET tiene diferentes módulos y funcionalidades, su objetivo en esta ocasión está siendo el robo de credenciales bancarias pero, por su funcionamiento, no se descarta que pudiera cambiar su finalidad.

La campaña comenzó a mediados de septiembre y se distribuye a través de correos electrónicos que tienen un documento ofimático (Word) con macros que, al ser activadas, infectan el equipo. Los correos electrónicos suelen llevar algún asunto genérico para evitar ser sospechoso: "Propuesta", "Respuesta", "Privacidad" o "Nueva Plantilla".

Sistemas afectados

Cualquier versión de Microsoft Windows.

Medidas de prevención

Para prevenir la infección para esta campaña concreta se pueden seguir las siguientes recomendaciones:

- Instalación de la herramienta EMOTET-stopper en todos los equipos Windows a proteger, disponible desde el siguiente enlace: http://ccn-cert.net/emotet2019
  Se deberán habilitar los mecanismos necesarios para que se ejecute tras cada reinicio.
  En caso de que el Antivirus o Sistema Operativo detecten la herramienta como código dañino, se deberá excepcionar para evitar su eliminación.
  La herramienta se ejecuta en segundo plano por lo que solo se verá desde el Administrador de tareas.
- Dado que el vector principal de infección de esta campaña de EMOTET es el correo electrónico, recomendamos revisar la Guía de Buenas Prácticas del CCN-CERT sobre dicha temática: http://ccn-cert.net/bpmail
- Dado que el vector principal de infección de esta campaña de EMOTET es el correo electrónico, recomendamos revisar la Guía de Buenas Prácticas del CCN-CERT sobre dicha temática:
- De la misma manera se recomienda deshabilitar Powershell en aquellos equipos en los que no sea necesaria la ejecución de comandos en dicho lenguaje.
- El CCN-CERT ha recopilado en 3 listas negras los indicadores que permiten la detección y bloqueo de gran parte de esta campaña: listas de IP, dominios y hashes de las muestras empleadas. Pueden descargar dichas listas aquí: http://ccn-cert.net/emotet-ioc
- EMOTET puede desplegar el troyano bancario Trickbot para robo información, seguido en última instancia del ransomware Ryuk sobre los equipos infectados. Actualmente no existe forma de descifrar los ficheros afectados por esta familia. Recomendamos la lectura de la Guía de Buenas Prácticas sobre Ransomware que el CCN-CERT ha elaborado: http://ccn-cert.net/bpransomware
- Mantener el Sistema Operativo, el antivirus actualizado y disponer de copias de seguridad *offline* (sin conexión con la red).

Medidas de detección

- Para contrarrestar los efectos de esta campaña, el CCN-CERT recomienda la búsqueda en la red de los Indicadores de Compromiso (IOC). Concretamente se debe realizar la búsqueda en los registros de conectividad (proxy/firewall/DNS) para comprobar si ha existido conectividad con los dominios o IP incluidos en las listas negras (http://ccn-cert.net/emotet-ioc)
- Para la detección en los equipos se puede utilizar las siguiente regla YARA: http://ccn-cert.net/emotet-yara

Medidas de mitigación

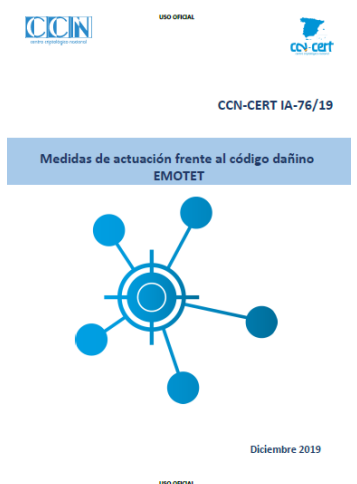
- Utilizar los indicadores proporcionados para identificar qué equipos se encuentran afectados por la campaña.
- Sobre dichos equipos se deberá realizar una copia de seguridad de la información, incluso

Deficiencias encontradas

- Redes NO segmentadas
- Red interna sin vigilancia
- Reutilización de contraseñas
- Sistemas obsoletos
- Sin actualizaciones de seguridad
- Poco/Nulo personal de seguridad TIC
- Todo el back-up conectado a la red

Plan de recuperación

- **Vacuna (EMOTET STOPPER)**
- Punto final
- Segmentar la red
- SAT INTERNET
- Servicio de seguridad gestionada

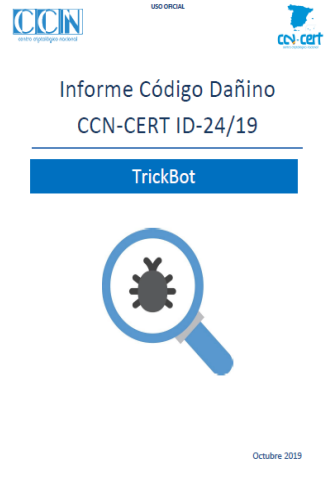


USO OFICIAL

CCN-CERT IA-76/19

Medidas de actuación frente al código dañino EMOTET

Diciembre 2019



USO OFICIAL

Informe Código Dañino
CCN-CERT ID-24/19

TrickBot

Octubre 2019

USO OFICIAL

Informe Código Dañino
CCN-CERT ID-25/19

"Ryuk"

Noviembre 2019

centro criptológico nacional

2 Ciberincidentes 2021

RRT desplegado

Ransomware Ministerio

Ransomware EELL

Estafa Ayto.

Ransomware Universidad

Intrusión Conf Hidrogra

ZeroLogon (Exchange) **(x14)**

Ransomware Agencia Gub.

Ransomware **(x5)**

Compromisos EELL/CCAA **(x9)**

Ransomware SEPE

Venta Accesos DarkWeb **(x7)**

Cobalt-Strike Ministerios

Ransomware EELL+Universidad **(x9)**

Ransomware ASAC **(~70)**

Ransomware 2 Ministerios

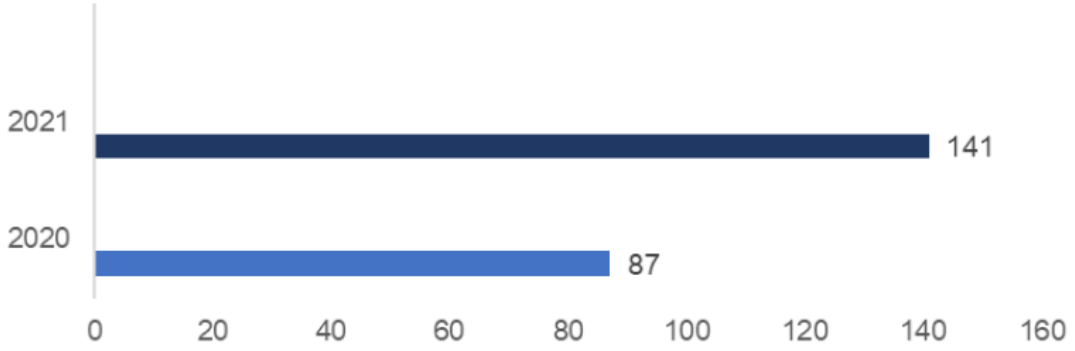
Ransomware Hospital

Enero | Febrero | Marzo | Abril | Mayo | Junio

2021

AYTO
(APT) – Sin impacto

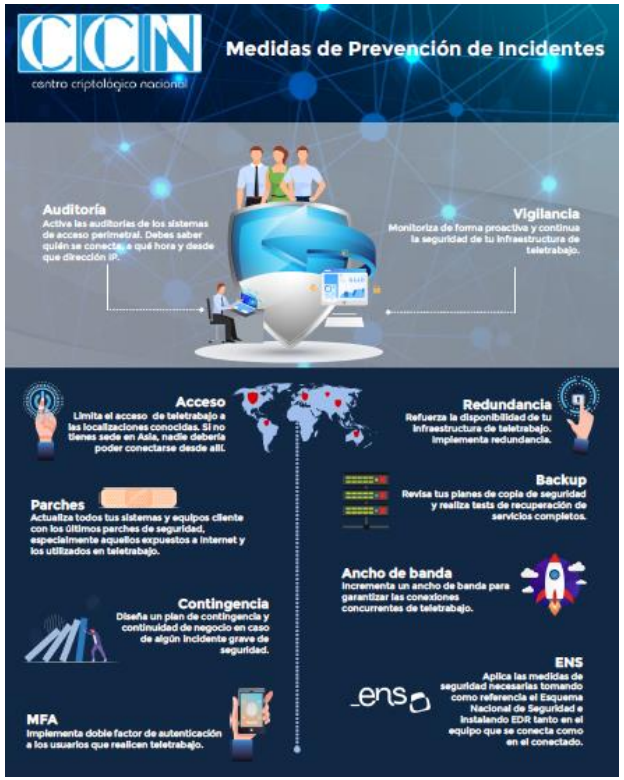
AGE
(APT Desconocido



Número de incidentes de tipo ransomware gestionados por el CCN. Fuente: LUCÍA

Campañas APT

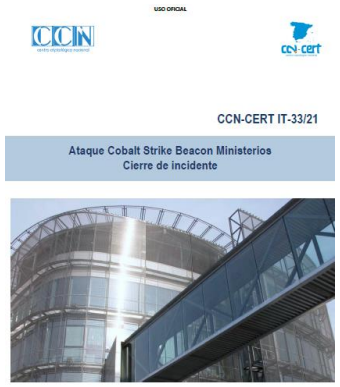
Medidas de prevención de incidentes

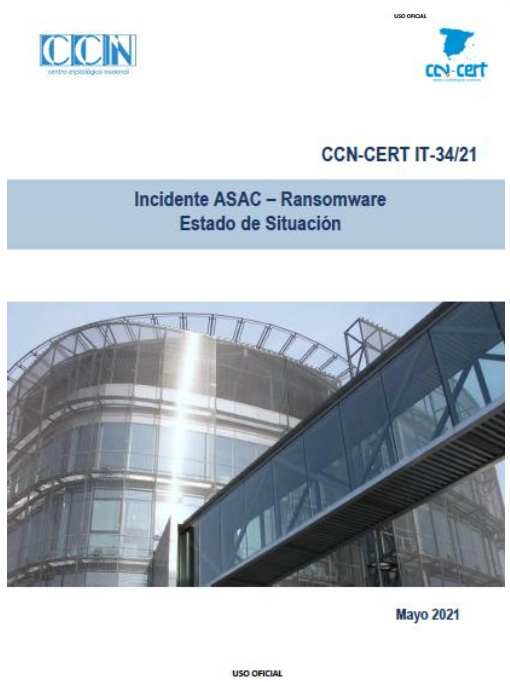


Abril 2020
En plena pandemia

1. **Auditoría.** Activa las auditorías de los sistemas de acceso perimetral. Debes saber quién se conecta, a qué hora y desde que dirección IP.
2. **Vigilancia.** Monitoriza de forma proactiva y continua la seguridad de tu infraestructura de teletrabajo.
   - **CARMEN / SAT INTERNET / EMMA-VAR**
3. **Acceso. Limita el acceso de teletrabajo a las localizaciones conocidas**. Si no tienes sede en Asia, nadie debería poder conectarse desde allí.
4. **Redundancia.** Refuerza la disponibilidad de tu infraestructura de teletrabajo. Implementa redundancia.
5. **Parches.** Actualiza todos tus sistemas y equipos cliente con los últimos parches de seguridad, especialmente aquellos expuestos a Internet y los utilizados en teletrabajo.
6. **Backup.** Revisa tus planes de copia de seguridad y realiza tests de recuperación de servicios completos.
7. **Ancho de banda.** Incrementa un ancho de banda para garantizar las conexiones concurrentes de teletrabajo.
8. **Contingencia.** Diseña un plan de contingencia y continuidad de negocio en caso de algún incidente grave de seguridad.
9. **MFA.** Implementa **doble factor de autenticación** a los usuarios que realicen teletrabajo. También conocido por 2FA
10. **ENS.** Aplica las medidas de seguridad necesarias tomando como referencia el Esquema Nacional de Seguridad e instalando EDR (capacidad de detección y respuesta. Evolución del antivirus) tanto en el equipo que se conecta como en el conectado.

CCN
centro criptológico nacional





Mayo 2021
En plena pandemia

Ataques Cobalt Strike + Ransomware. ¿Qué esta pasando?

1. **Compra de credenciales** de acceso remoto a la organización en el mercado negro.
2. Entrada en la red por un acceso remoto a la misma y **elevación de privilegios** a administrador en un servidor.
3. Instalación de **herramientas de control remoto** (ej. COBALT STRIKE) y movimiento lateral para controlar toda la red.
4. **Robo de información de la organización** (datos personales o propiedad industrial) que le permita la extorsión y fuerce el pago del rescate
5. **Cifrado de datos de la organización y solicitud de rescate**.

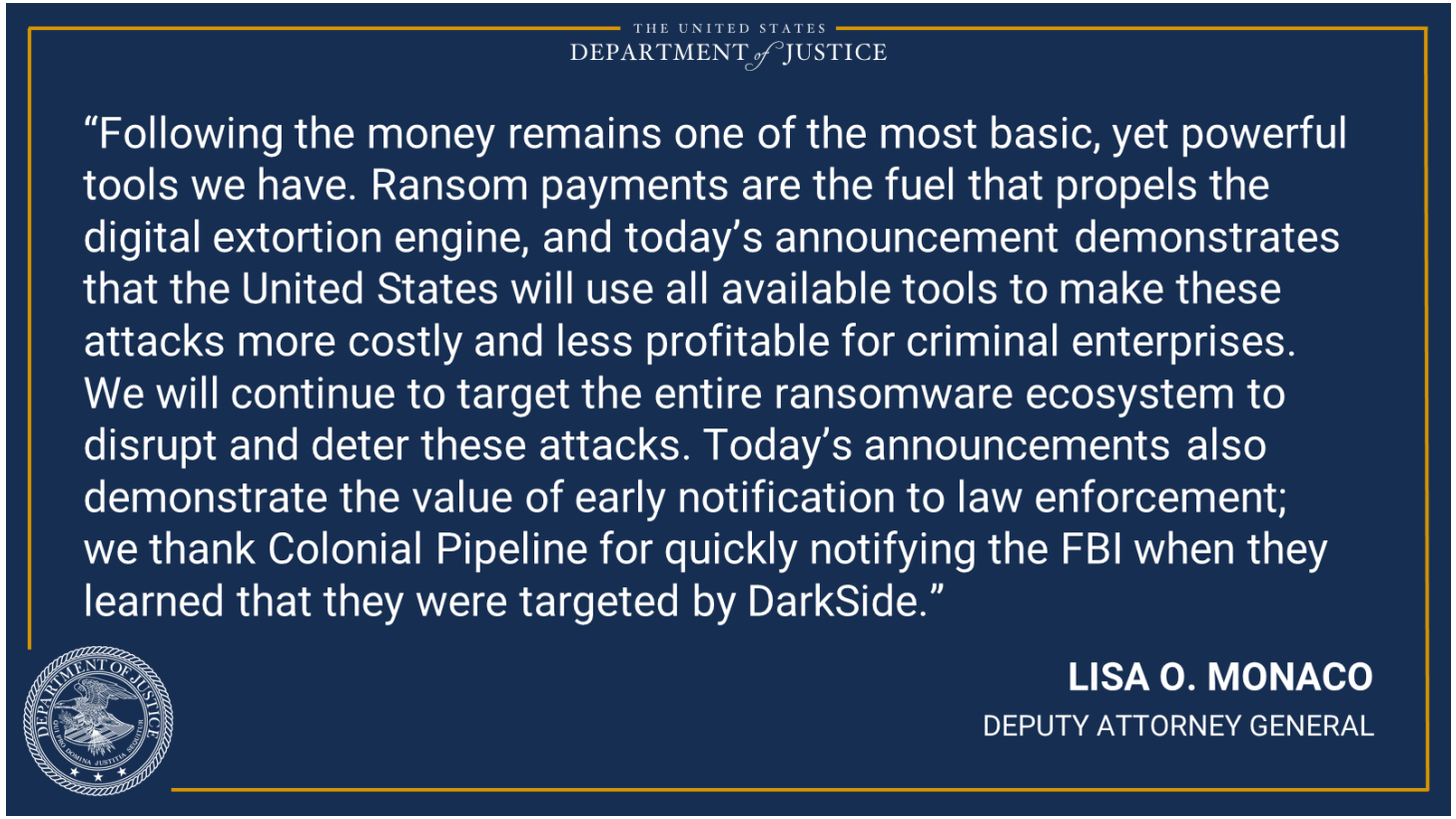
CCN centro criptológico nacional

Lecciones no aprendidas

- **Backups en línea (o incluso sin backup).**
- **Accesos remotos (VDI, VPN, RDP) sin 2FA**
- Redes ‘planas’ –> Necesidad de segmentación.
- Usuarios como administradores locales.
- Logs muy limitados.
- Falta de monitorización fuera de horas (horario habitual del despliegue dañino)
- **Redes de confianzas (unidades compartidas)**
- **Ausencia de EDR / microCLAUDIA**

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-buenas-practicas-bp/5864-ccn-cert-bp-21-gestion-de-incidentes-de-ransomware/file.html

Incidente Colonial. Distribución Hidrocarburos



- Inicio del incidente: **07.05.2021**
- Fin del incidente: **14.05.2021**
- **Impacto:**
  - Interrupción de operación en oleoducto de 8.000 km. 45% combustible de la Costa Este
  - Temor a desabastecimiento en 50M personas
  - Pago rescate: 5.000.000 $
- **Grupo de Ataque:**
  - DARKSIDE

- USA vincula a cibercriminales ubicados en Rusia e insta a acciones por parte del gobierno Ruso
- **12.05.2021** Presidente BIDEN firma la orden ejecutiva **PARA MEJORA DE LA CIBERSEGURIDAD DE LA NACIÓN**
  - Plan de mejora en 100 días

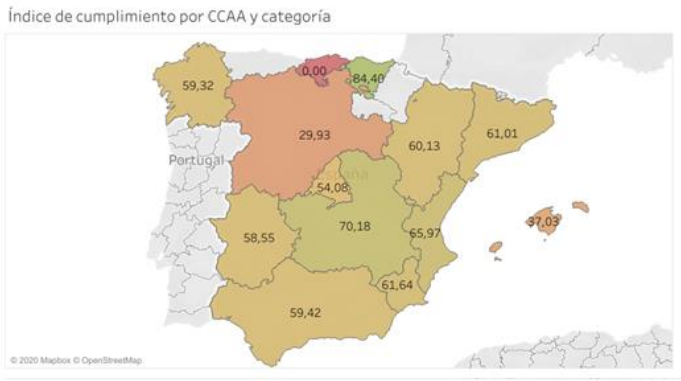
Defensa vs Ataque

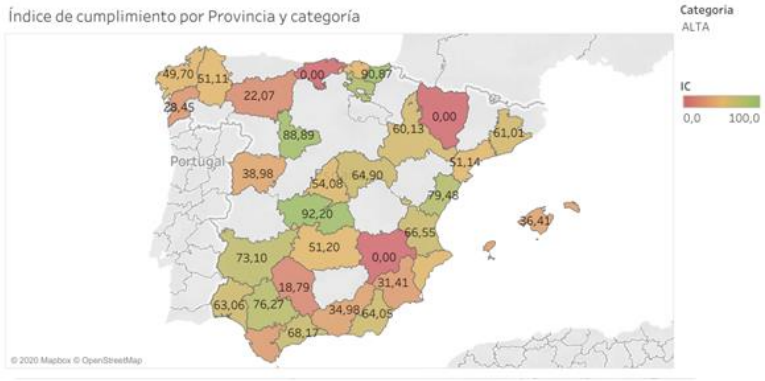
Necesidad de implementar ciberseguridad

- Privilegios de usuarios
- Autenticación de usuario / administración
- Redes sociales / Telefonía móvil
- Servicios en nube
- Unidades de memoria
- Sistemas NO actualizados ni configurados
- Redes no controladas ni vigiladas
- Antivirus tradicional obsoleto
- Atacantes especializados
- No sabemos nuestro nivel de seguridad
- Y ahora….. Teletrabajo

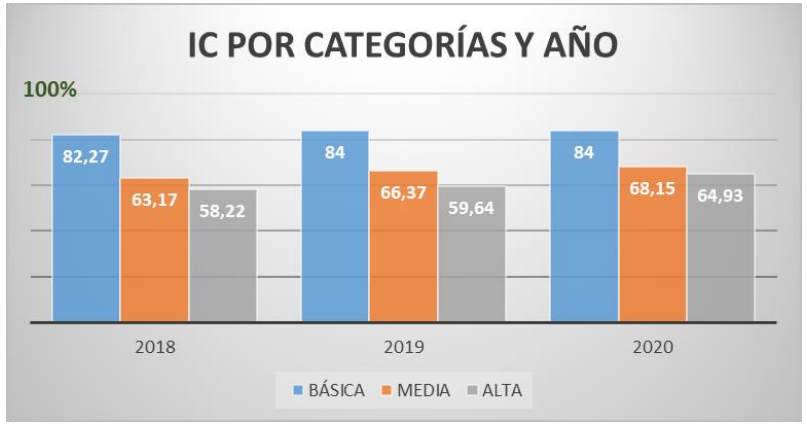
El nivel de madurez sigue siendo **BAJO**

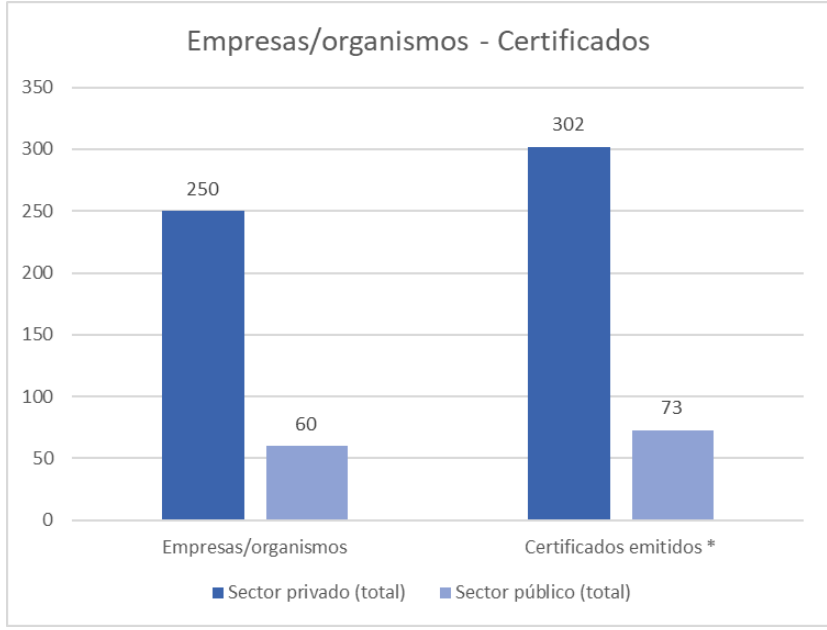
Índice de cumplimiento por CCAA y provincia para sistemas de Categoría ALTA

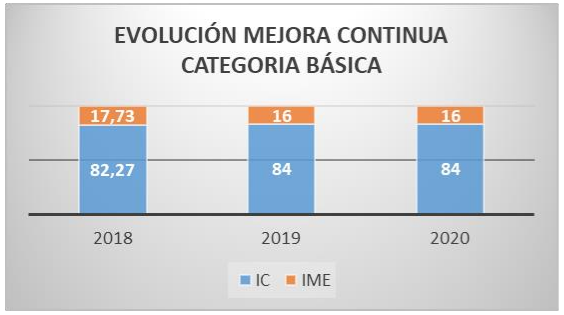


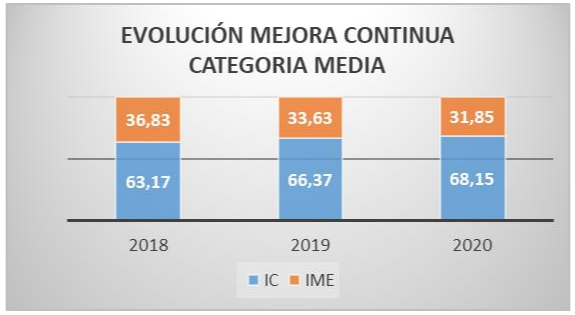


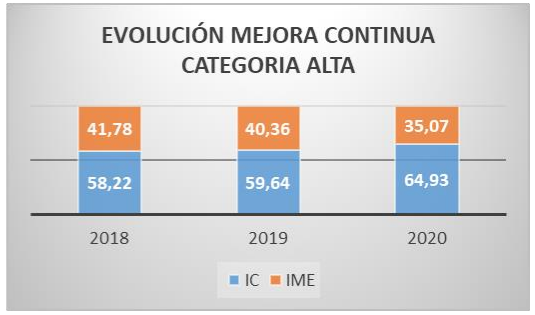
Prevención











centro criptológico nacional

Situación actual y amenazas

VERIZON rp_data-breach-investigations

CONCLUSIONES

- **Antivirus es insuficiente. Disponer capacidad reacción en equipos / servidores.**

- **<u>Disponer de un SOC / CERT no es una opción</u>.**
  Mejor servicio compartido. Revisión centralizada de LOG,s. *La ciberseguridad no es el negocio principal de muchas empresas / organismos….*
  - **Vigilar Perímetro y Red interna….24*7**
  - **Basados en reglas y anomalías**
  - **Procedimientos gestión incidentes / gestión crisis**

- **<u>Necesidad de realizar auditorias</u>. Vigilar el desempeño de los departamento TIC**

- **<u>Necesidad de Unidad de ciberseguridad separada de TIC</u> o con suficiente independencia, sin conflictos de interés.**

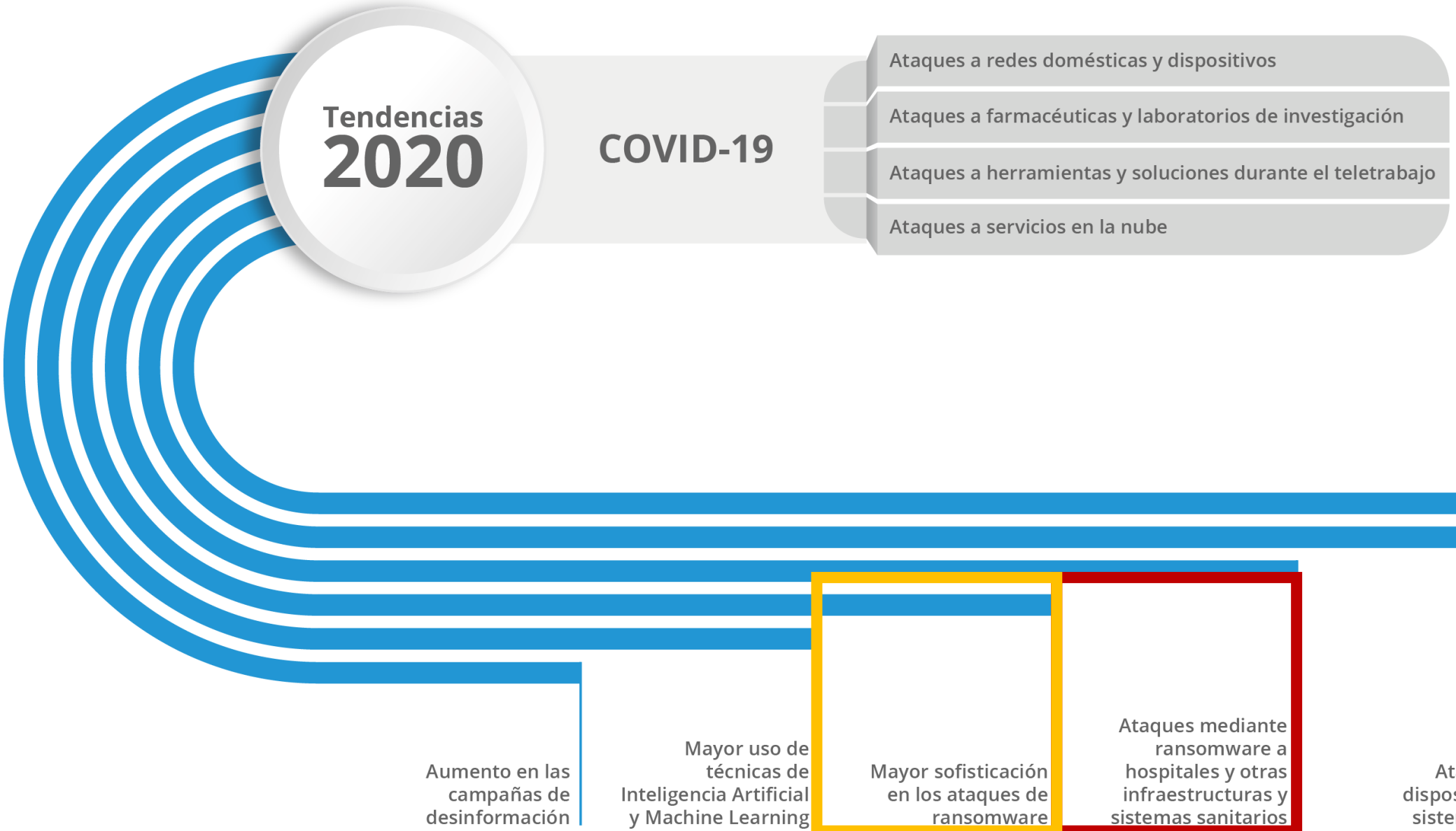
- **NO NOTIFICAR ----- COMPARTIR y COLABORAR**

SOC AGE
SOC SGNTJ

SOC

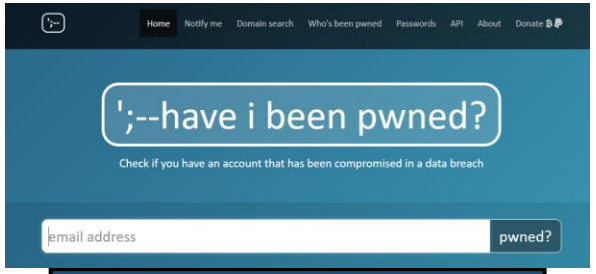
CCN
centro criptológico nacional

TENDENCIAS 2020



CIBERATAQUES QUE MAS PREOCUPAN

- **Ciberespionaje**: incremento actividad ataques patrocinados por estados.
  - Posibles ciberataques para realizar demostración de fuerza en el entorno internacional.
  - Ataques a la cadena de suministro
  - Sofisticación del código. Umbral de detección muy bajo. Ofuscación.
  - **Se han adaptado a las nuevas condiciones de teletrabajo ocasionadas por COVID19. Ataque VPN**
- ***Cibercrimen***: incremento en la actividad y selectividad sobre objetivos más rentables.
  - Ransomware como instrumento de financiación pero no la principal amenaza,
  - Miners como beneficio económico más estable y directo frente ransomware.
  - Ataques complejos al sector financiero y salud.
  - Venta de servicios a terceros (botnets IoT, vulnerabilidades 0-day, malware fileless, …).
- **La Nube como objetivo.** Migración de grandes empresas. El COVID19 ha acelerado la implantación de estas soluciones. Necesidad de configuración adecuada.
- **Accesos remotos.** Migración de todos durante el COVID19. Suplantación usuarios remotos. ¡ Cuidado con las credenciales ¡.



Muchas

Gracias

E-mails

ccn@cni.es

info@ccn-cert.cni.es

sat-inet@ccn-cert.cni.es

sat-sara@ccn-cert.cni.es

sat-ics@ccn-cert.cni.es

organismo.certificacion@cni.es

Páginas web:

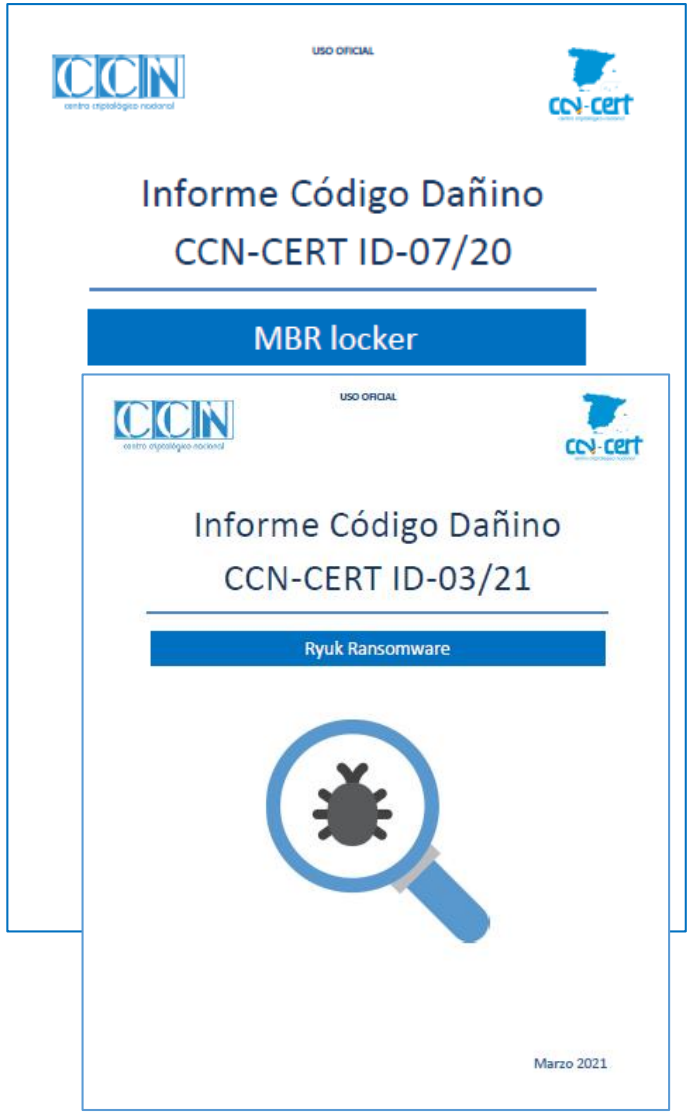
www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

angeles.ccn-cert.cni.es

Crisis debida a ataques con malware. ¿Qué necesitamos?



En la crisis del COVID19 necesitamos:

- **TEST,s** que nos mida impacto / nº infectados
- **TRATAMIENTO** que cure al enfermo
- **VACUNA** que evite nuevas infecciones

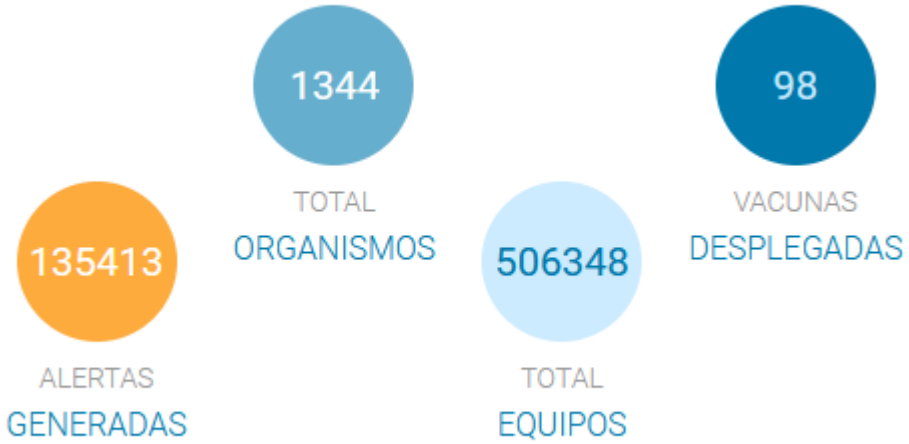
- Proceso de infección
- Procedimiento de Desinfección
- Reglas de Detección (IOC,s)
- Vacuna
  - Rescate

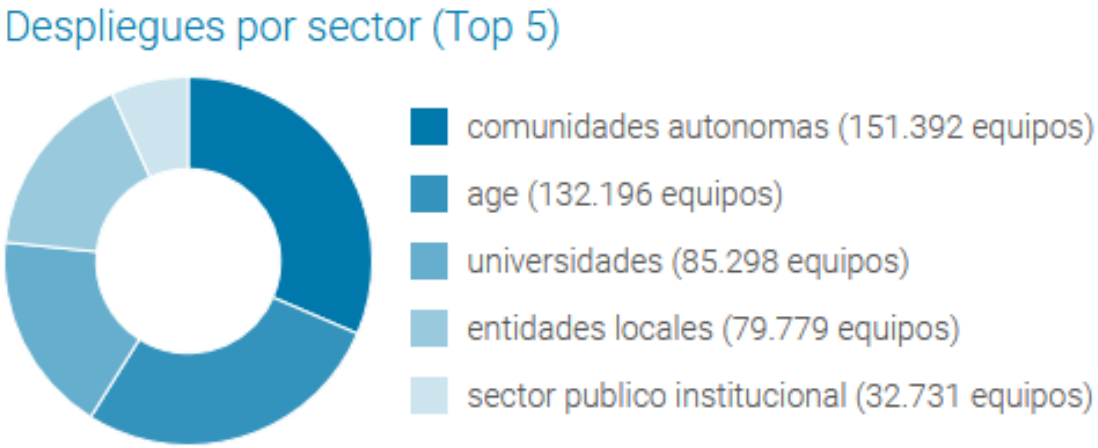
Centro de Vacunación

En una crisis con un malware necesitamos:

- **REGLAS DETECCIÓN** que nos alerte infección y mida impacto / nº equipos infectados
- **PROCD DESINFECCIÓN / RECUPERACIÓN** que cure a la víctima
- **VACUNA** que evite nuevas infecciones

</µCLAUDIA>. Centro de vacunación





OBJETIVOS 2021

- Mayor esfuerzo en vacunas. Vacunas genéricas que paran TTP,s de grupos de ataques
- **Mejor visibilidad de alertas**. Mejora en los informes y en la información a proporcionar en los equipos donde se instale.
- Arquitectura Federada. **Visibilidad a SOC,s / CERT autonómicos**
- Integración con SIEM GLORIA / CARMEN / Otros SIEM. **Mejorar la visibilidad del organismo**
- **Certificación LINCE**