CCN / CCN-CERT

Importancia de la ciberseguridad en la Transformación Digital de una Ciudad

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

centro criptológico nacional

FEMP. Iniciativas

Grupo de trabajo 1

01	**Estrategia de sostenibilidad turística Valencia 2030** Ayuntamiento de Valencia
02	**A Coruña – Ciudad abierta: participación, datos abiertos y transparencia** Ayuntamiento de A Coruña
03	**Smart Pamplona Lab** Ayuntamiento de Pamplona
04	**Tarjeta Ciudadana (Valladolid)** Ayuntamiento de Valladolid
05	**Visión y estrategia de los ecosistemas de datos del ayuntamiento de Valencia** Ayuntamiento de Valencia

Aplicaciones Turísticas
Movilidad / aparcamientos
Gestión del tráfico
Gestión aguas / residuos
IA en trámites
…//…

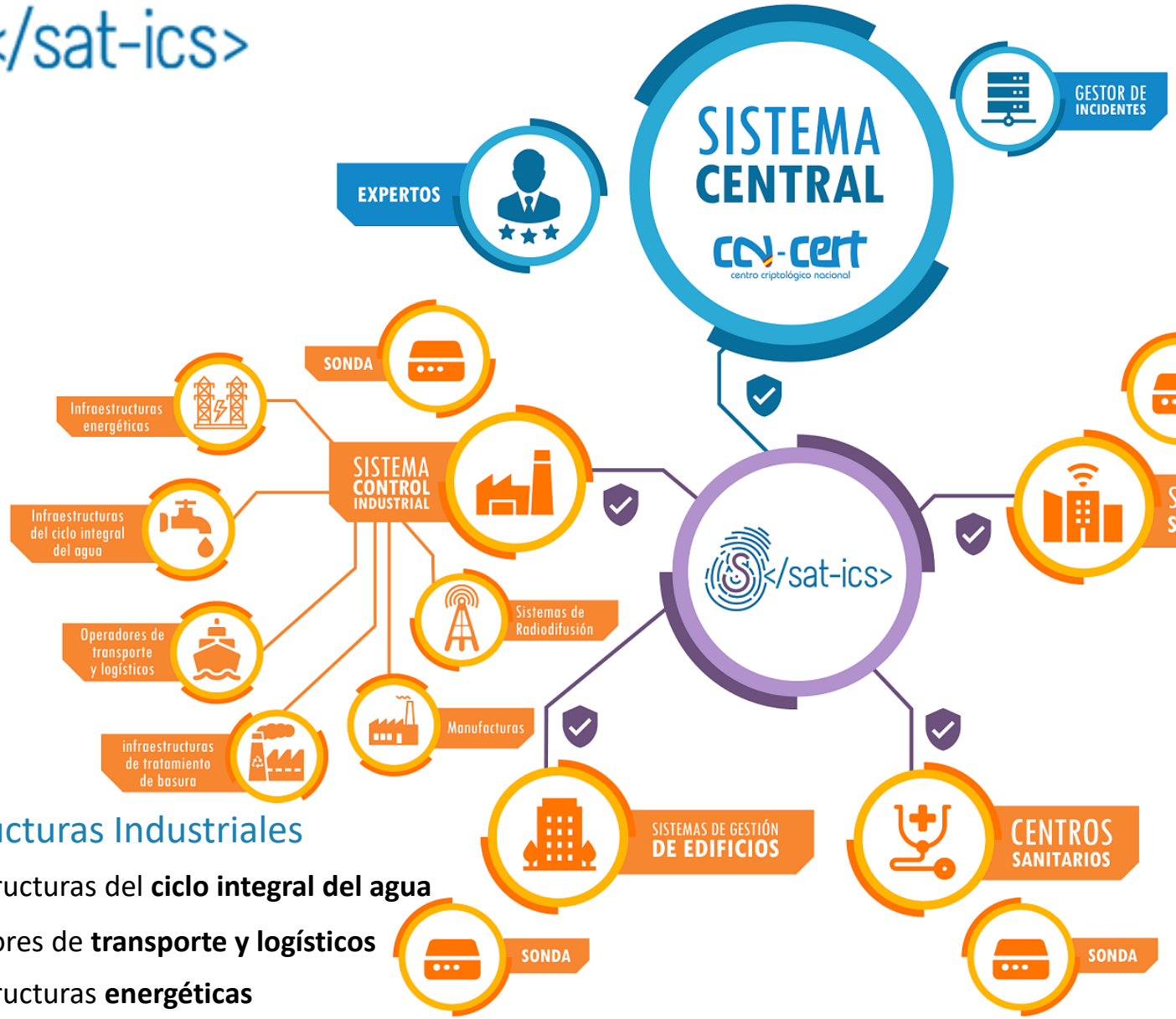
Grupo de trabajo 2

06	**Bilbao - Movilidad Conectada, proyecto europeo C-Mobile** Ayuntamiento de Bilbao
07	**Victoria-Gasteiz - VGBIZIZ: La red de aparcamientos seguros para bicicleta** Ayuntamiento de Vitoria
08	**Valencia: Introducción a la certificación ITU** Ayuntamiento de Valencia
09	**Rivas-vaciamadrid: implantación bono de la iniciativa Wifi4EU** Ayuntamiento de Rivas-Vaciamadrid

Grupo de trabajo 3

10	**Cáceres – La información geográfica en tu mano. Extensión de la IDE al área metropolitana** Ayuntamiento de Cáceres
11	**Diputación de Valencia – Connecta Valencia Territorio Turístico Inteligente y Sostenible: Soluciones de trazabilidad territorial** Diputación de Valencia
12	**Villanueva del Pardillo - Registro de Entrada Asistido con IA** Ayuntamiento del Pardillo

- **GOBERNANZA DE LA CIBERSEGURIDAD**
- **PREVENCIÓN**
- **DETECCIÓN**
- **RESPUESTA**



Sistemas de Smart Cities

- Sistemas de gestión de **alumbrado público**
- **Control de tráfico**
- Gestión de **residuos urbanos**

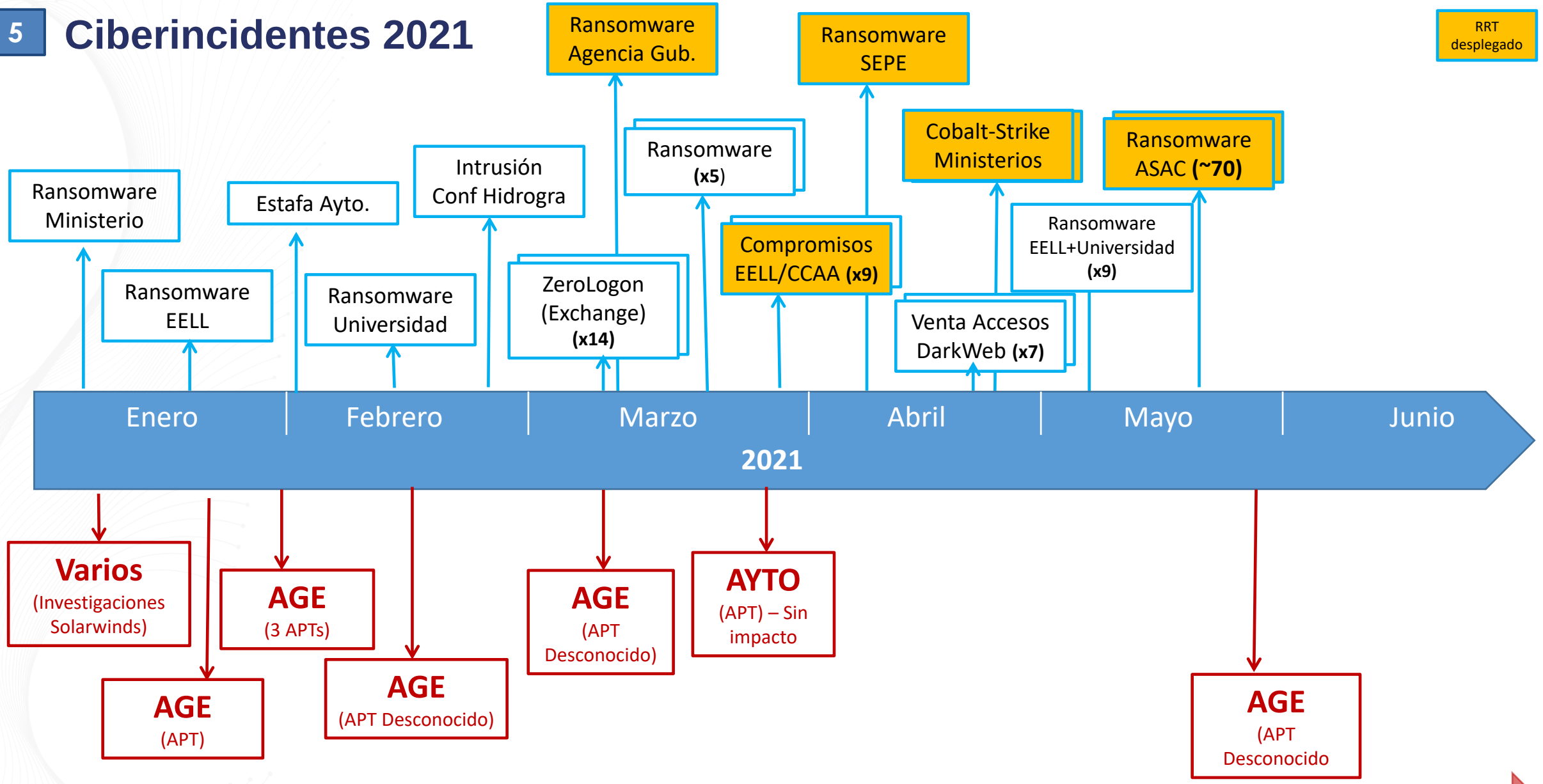
Infraestructuras Industriales

- Infraestructuras del **ciclo integral del agua**
- Operadores de **transporte y logísticos**
- Infraestructuras **energéticas**
- Infraestructuras de **tratamiento de residuos**
- Sistemas de **radiodifusión / Manufactura /** Institutos y centros de **investigación**

Centros sanitarios y Sist. Gestión de Edificios

- Redes de **Diagnóstico por imagen** (**DICOM**)
- Redes de **seguridad y control de accesos**
- **BMS**
- Sistemas **HVAC**

5 Ciberincidentes 2021



LA OTRA PANDEMIA

El SEPE sufre un ataque
informá
sus ser
gestión
miles d

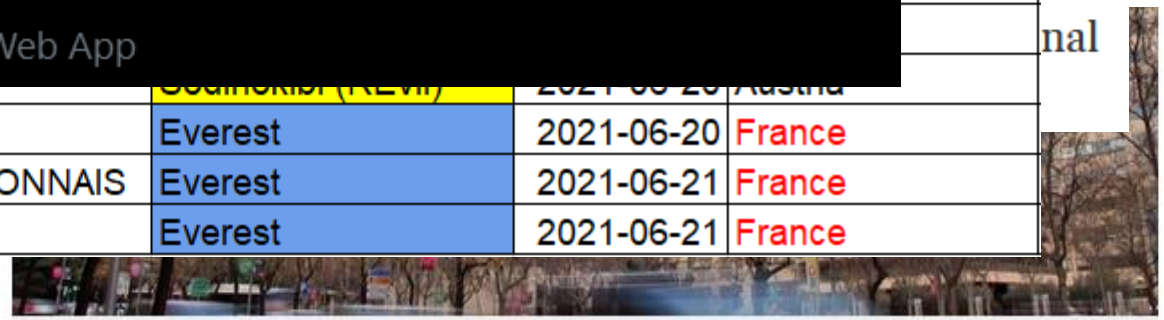
El sindicato CSIF
actividad en todo
afectado al sistem
prestaciones por

ATAQUE
El M
cib
Los re
trabaj

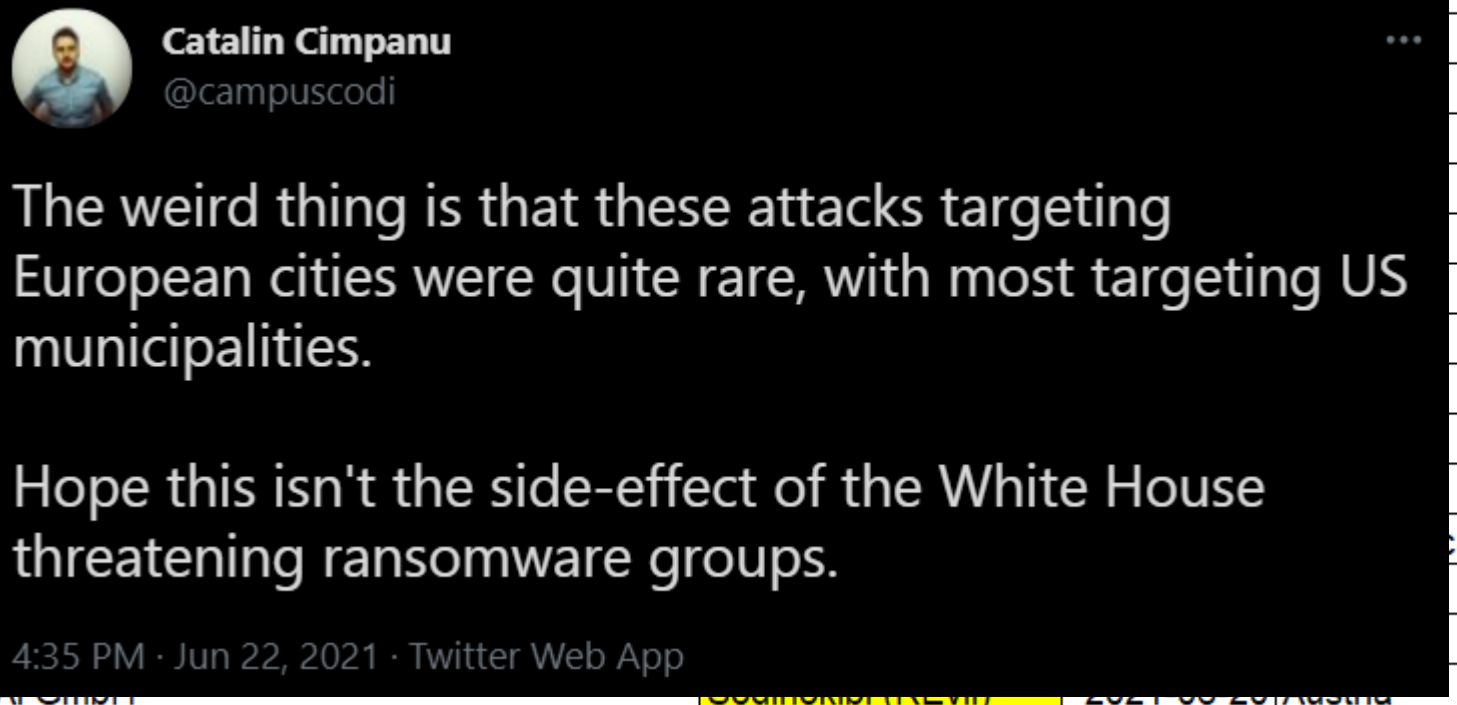
Un ciberataque obliga a Economía,
a
emas para

mes de la Ville de
ibles suite à une
mment le cas des

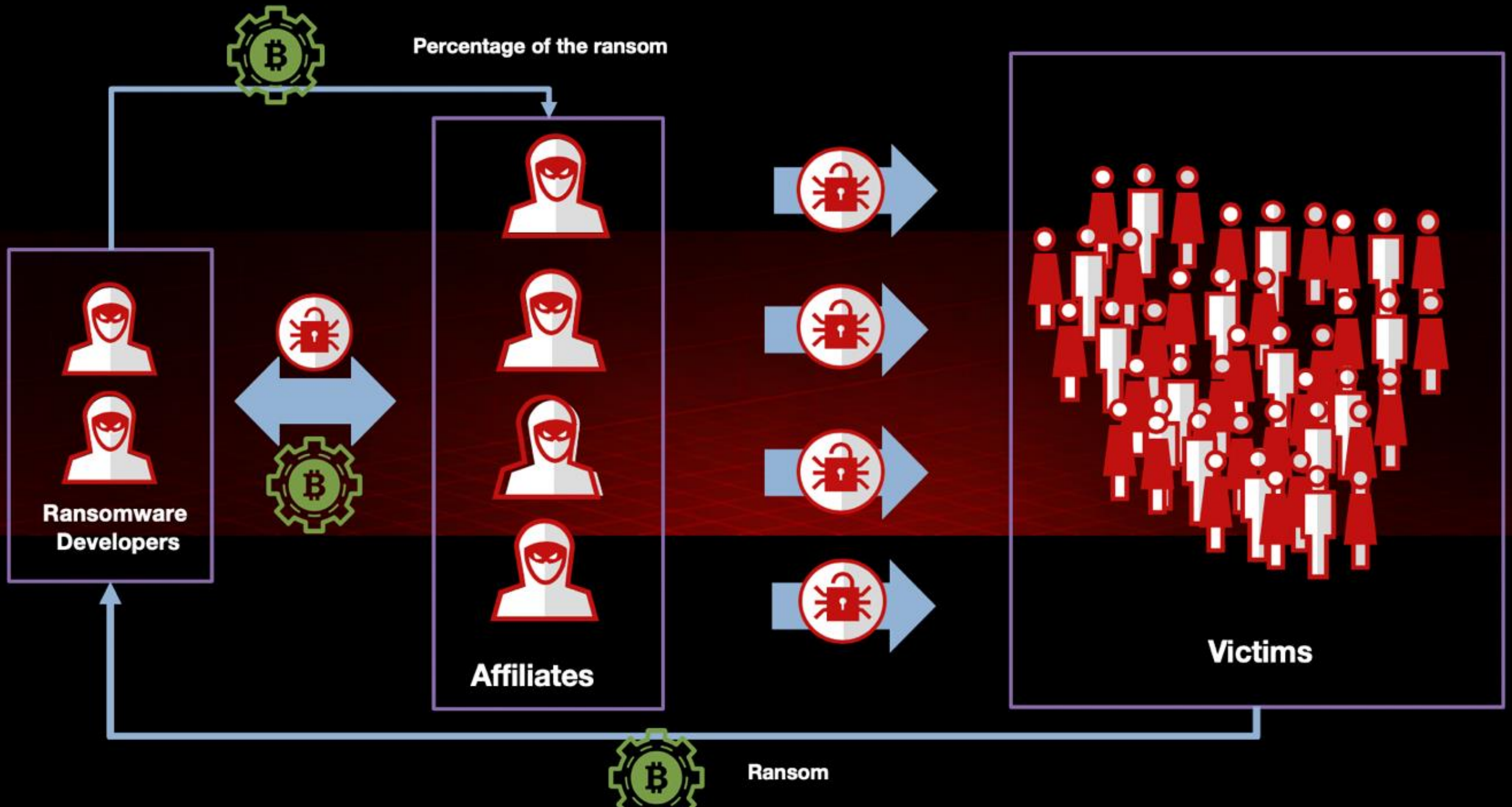
nal



No	Victim	Ransomware Gang	Date	Victim Country
2484	ENE TECHNOLOGY, Inc	SynACK	2021-06-16	Taiwan
2485	American Cotton Coop Association	Grief	2021-06-16	USA
2486	Vogel Heating & Cooling	Conti	2021-06-17	USA
2487	Sunsations Inc.	Conti	2021-06-17	USA
2488	Performance Award Center	Marketo	2021-06-17	USA
2489	Co	Co	2021-06-17	Canada
2490	BF			
2491	As			
2492	Au			
2493	Gr			
2494	Ce			
2495	Vo			
2496	Ur			
2497	Ma			
2498	Gr			
2499	Wi			
2500	Mc			ca
2501	La			
2502	Ep			
2503	HA	Sodinokibi (REvil)	2021-06-20	Austria
2504	Always Group	Everest	2021-06-20	France
2505	ASSURANCES ET COURTAGES LYONNAIS	Everest	2021-06-21	France
2506	Alltech France	Everest	2021-06-21	France

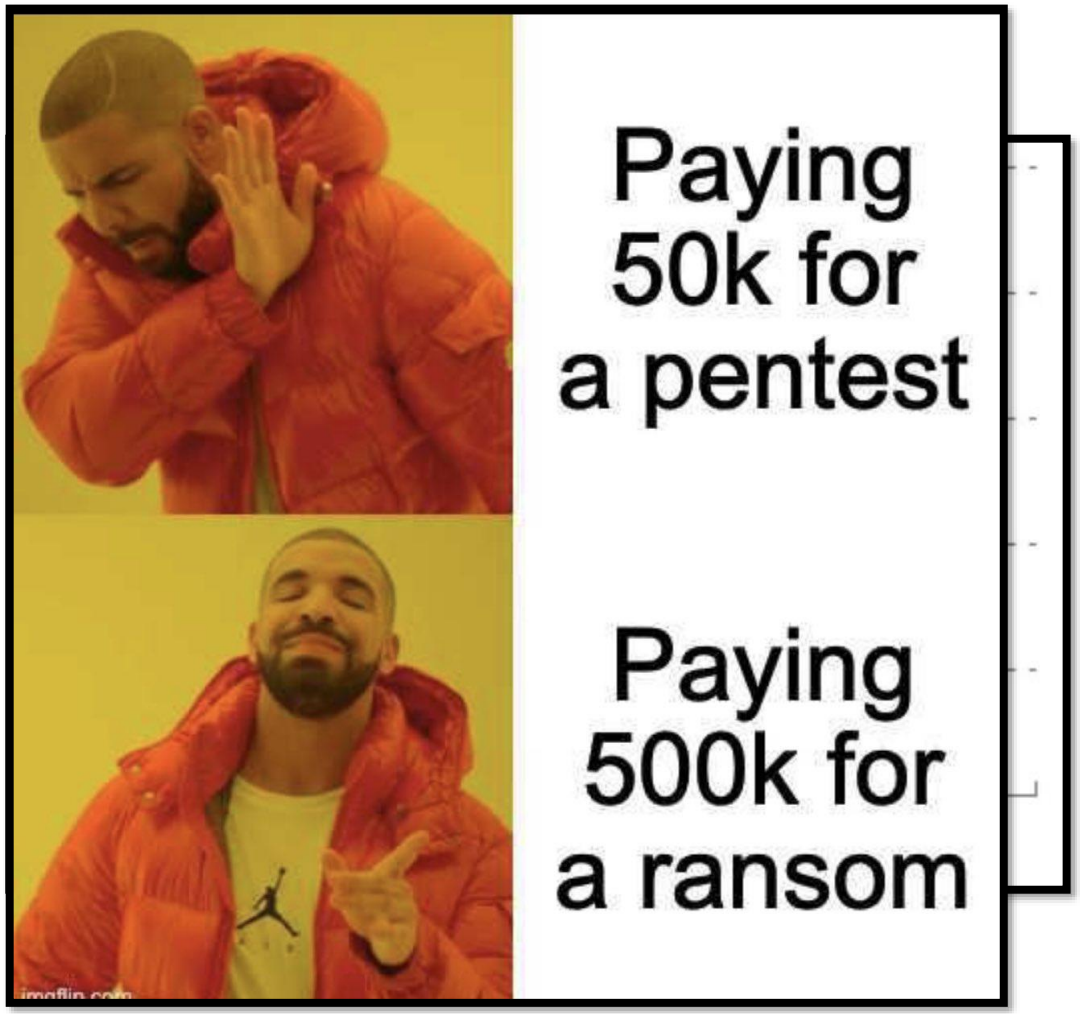


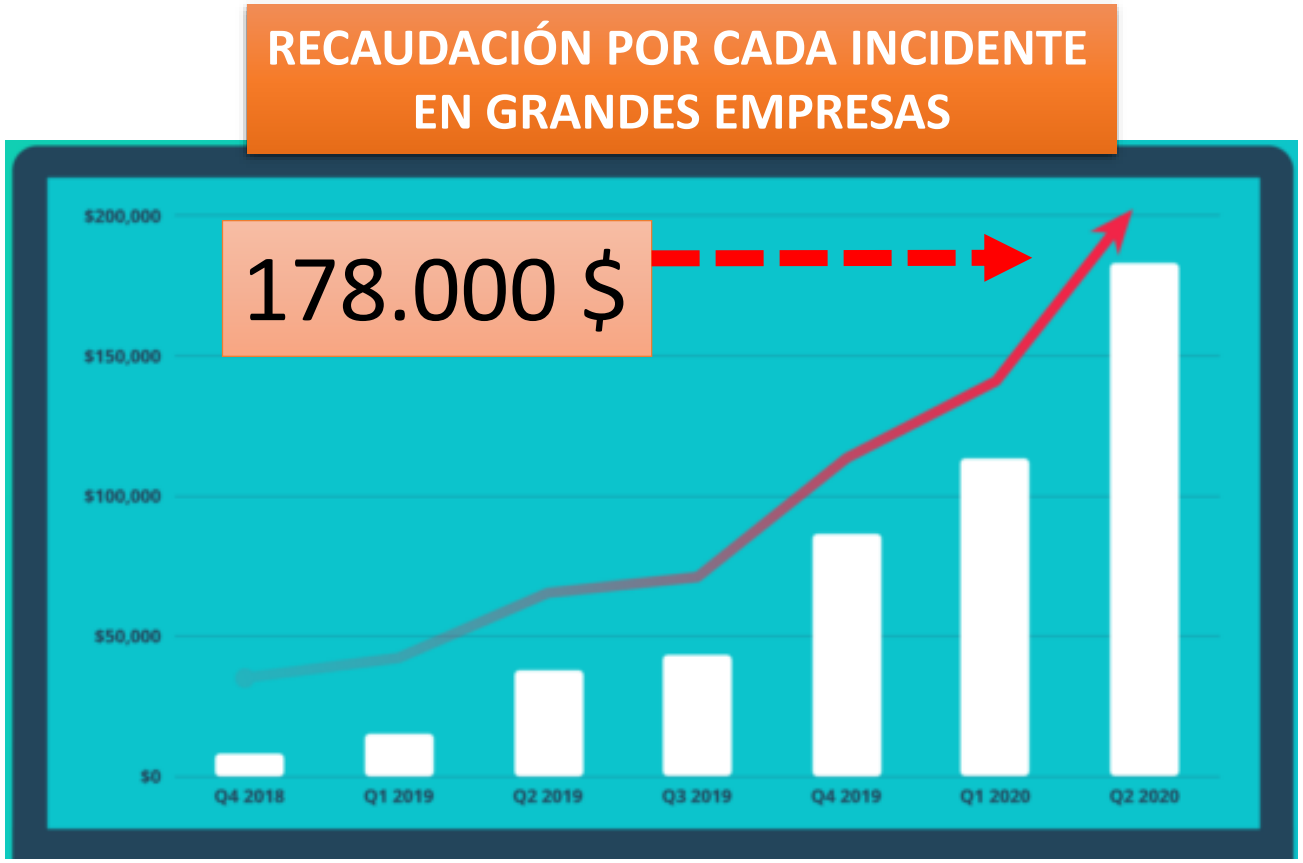
Ransomware-as-a-Service (RaaS) Model



Recaudación anual del Ransomware

- Año tras año el auge del Ransomware sigue creciendo exponencialmente:





EN 2021 EL COSTE SERÁ DE 20.000 MILLONES DE $

CCN centro criptológico nacional

¿CÓMO ENTRAN EN NUESTRAS REDES?

1. CREDENCIALES DÉBILES EN SISTEMAS DE ACCESO REMOTO (VPN/CITRIX/..)

2. COMPRA DE CREDENCIALES LEGÍTIMAS EN MERCADO NEGRO

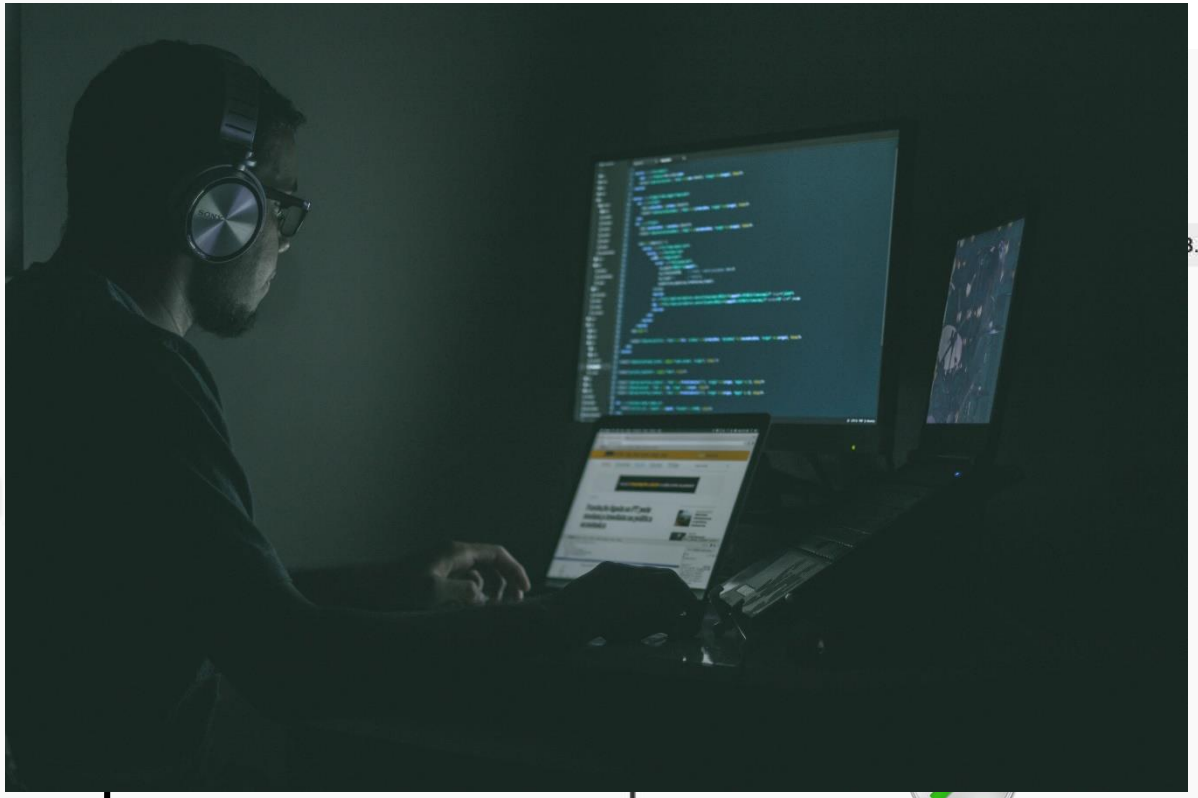
3. EXPLOTACIÓN DE VULNERABILIDADES EN PERÍMETRO

TELETRABAJO

4. ATAQUES DE PHISHING

ESQUEMA TRADICIONAL DE ATAQUE

Ryuk Speed Run, 2 Hours to Ransom



20:57 UTC Bazar malware

exploited against primary domain controller

CVE-2020-1472

21: 54 First lateral movement to domain controller using RDP

22:58 First system ransomed.

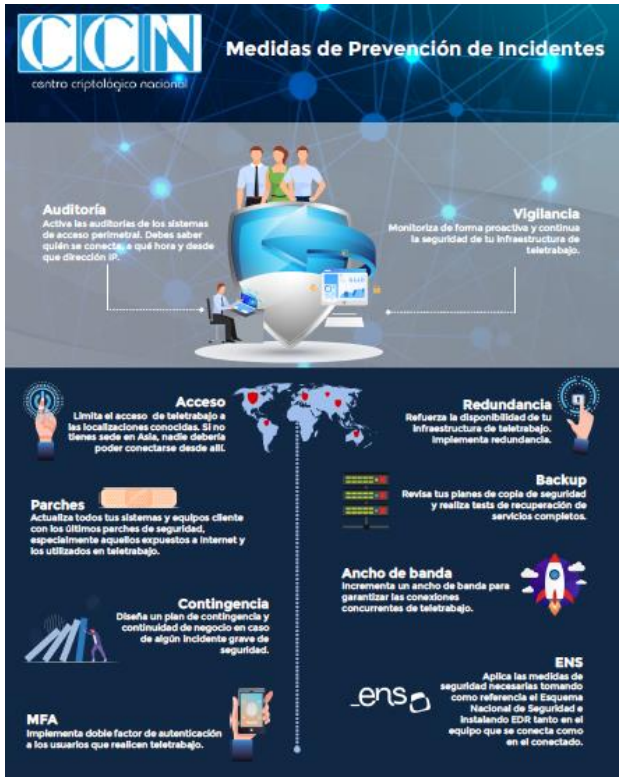
23:41 All systems ransomed.

¿TIEMPO DE RECUPERACIÓN?

- Depende de :
  - **El tamaño de la organización** → Parque de 10 equipos Vs. 100.000
  - **El alcance de la infección**
    - **¿Se ha cifrado todo?** → Recuperación parcial Vs. Total
    - **¿Se tienen copias de seguridad?** → Que no se hayan cifrado
    - **¿Se ha robado información?** → Identificar activos / Poner denuncia / LOPD
  - **Los recursos humanos y HW disponible** → Equipo cualificado y organizado

2 semanas en casos más leves → Más de 4 semanas en casos severos

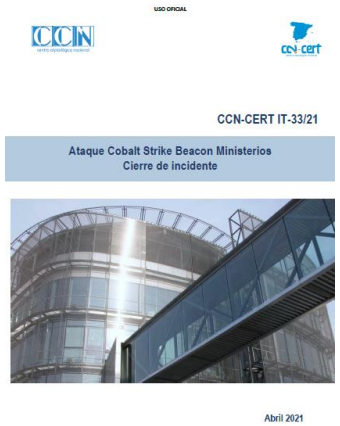
Medidas de prevención de incidentes

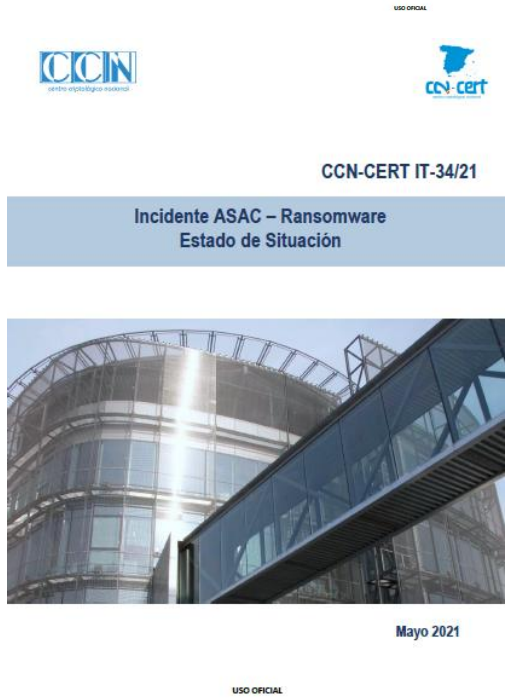


Abril 2020
En plena pandemia

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

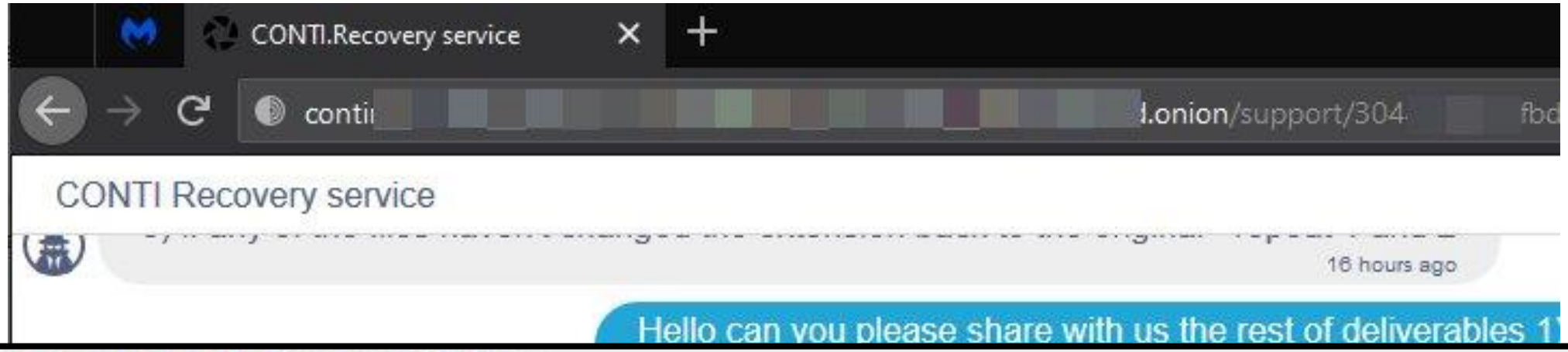
Lecciones no aprendidas

- **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

Lecciones no aprendidas

CONSEJOS DEL ATACANTE…

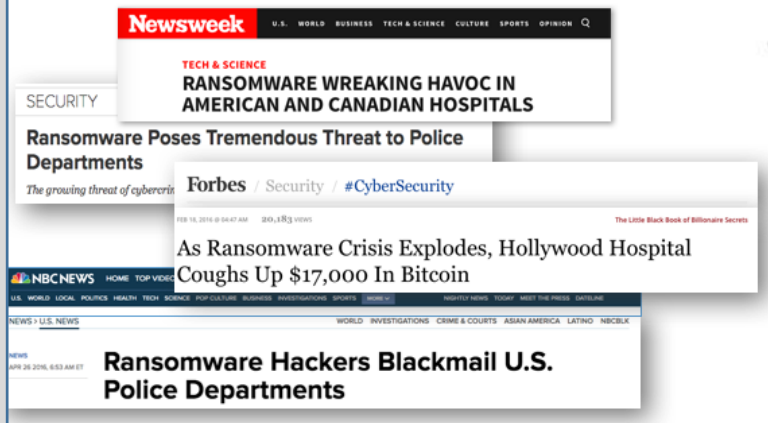


Our recommendations will be :

1. Implement better email filtering policies
2. Implement tape-based backup hardware
3. Audit account access policies network wide
4. Rebuild the network using segmentation procedures
5. Implement better password policies
6. Block pass-the-hash and kerberoast attacks
7. Notify all your employees and security policies inside the company (opening email attachments, changing passwords, etc)
8. Buying better AV/EDR software

CONSECUENCIAS DE UN INCIDENTE DE RANSOMWARE

- Servicios de la organización parados ✓
- Empleados no pueden trabajar ✓
- Exposición pública en medios ✓
- Presión social y política ✓
- Robo de información ✓



- INVERTIR EN SEGURIDAD → FORMACIÓN, PERSONAS Y EQUIPOS

Defensa vs Ataque

No hay Transformación Digital sin 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**

CONCLUSIONES

- **Antivirus es insuficiente. Disponer capacidad reacción en equipos / servidores (EDR / Microclaudia).**

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

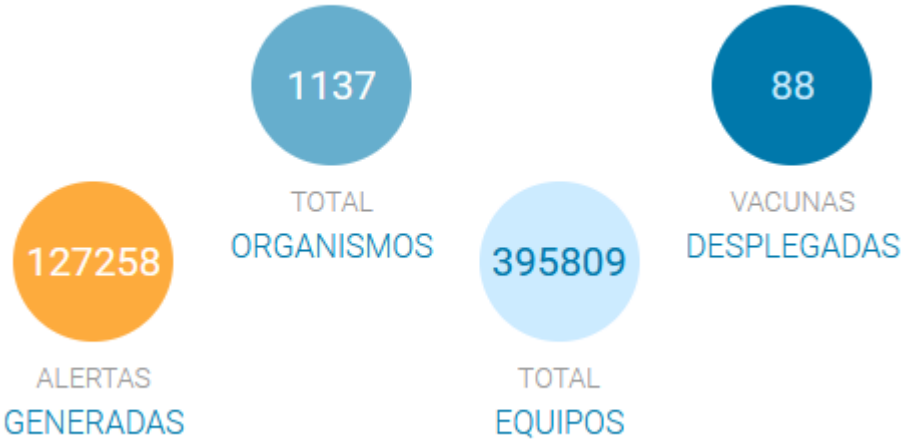
- **Necesidad de realizar auditorias. Vigilar el desempeño de los departamento TIC**

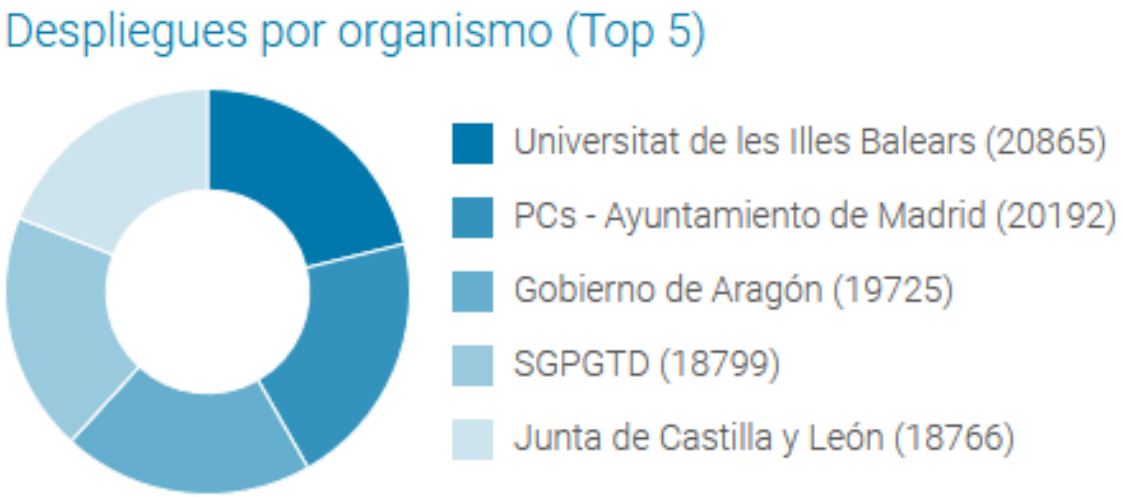
- **Necesidad de Unidad de ciberseguridad separada de TIC o con suficiente independencia, sin conflictos de interés.**

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

SOC

</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**

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