
SOFISTIC
CYBERSECURITY


Juan Carlos García
SOC Manager & Country Manager Spain

Ciberseguridad, una moda no pasajera

Tech Xplore — Topics — Week's top — Latest news

Home / Security

OCTOBER 15, 2021

$590 mn in ransomware payments reported to US in 2021 as attacks surge

by Joshua Melvin

New data s

New data o
payments w
setting a pa
extortion bo

LA VANGUARDIA

CIBERATAQUE

La mayor red de oleoductos de EE.UU. paralizada por un ataque de "ransomware"

- Se sospecha que "DarkSide", un grupo de piratas informáticos del este de Europa, ha bloqueado el acceso a los ordenadores de la compañía y pide dinero para liberarlos
- Se trata de uno de los mayores ciberataques que se han hecho públicos en Estados Unidos

Un ciberataque deja sin servicio a los sistemas informáticos del SEPE y provoca la caída de la web

El Ministerio de Trabajo investiga el origen de la brecha de seguridad en los sistemas informáticos del servicio público de empleo que ha afectado también a los ordenadores de empleados del organismo, que han tenido que apagarlos a la espera de conocerse el alcance

— "Nos están midiendo": los ataques contra Defensa, hospitales y grandes empresas preocupan a la ciberseguridad española

BUSINESS INSIDER — Economía — Tecnología — Estrategia — Política — Más temas — Suscríbete

Los atacantes del Ayuntamiento de Castellón reivindican la filtración de 119 gigas en datos robados: el 'ransomware' hace su agosto en las administraciones españolas

Alberto R. Aguilar 13 abr. 2021 7:30h

BBC NEWS | MUNDO

Noticias — América Latina — Internacional — Medio ambiente — Coronavirus — Hay Festival

Tecnología — Video — Centroamérica Cuenta — BBC Extra

Corea del Norte: el informe de la ONU que acusa a Pyongyang de "robar US$2.000 millones a través de ciberataques" para fabricar armas

europapress / internacional

Actualizado 11/04/2021 19:43 CET

Irán denuncia el ataque de "terrorismo nuclear" de este domingo contra la central de Natanz

Israel ya ha atacado en anteriores ocasiones el programa nuclear iraní

MADRID, 11 (EUROPA PRESS)

El director de la Organización de la Energía atómica iraní, Ali Akbar Salehi, ha achacado al "terrorismo nuclear" el incidente ocurrido este domingo en la central nuclear de Natanz, la más importante del programa de enriquecimiento de uranio iraní.

Menú — El Confidencial

SE TRATA DEL 'RANSOMWARE' RYUK

El Ministerio de Trabajo sufre un segundo ciberataque con el virus que tumbó el SEPE

El organismo ha vuelto a sufrir un ciberataque con el 'ransomware' Ryuk, el mismo que tumbó el SEPE varias semanas. El alcance es importante y se ha calificado internamente como "crítico"

Sede del Ministerio de Trabajo en Madrid. (EFE)

Por Manuel Ángel Méndez

09/06/2021 - 12:26 Actualizado: 09/06/2021 - 16:05

EL PAÍS — Internacional — SUSCRÍBETE — INICIAR SESIÓN

CIBERSEGURIDAD >

Biden convoca a 30 países a una reunión para combatir los ciberataques en la que no está Rusia

Estados Unidos asegura que mantiene una vía abierta para tratar las amenazas de ciberseguridad con Moscú

europapress / portaltic / ciberseguridad

Publicado 18/09/2020 10:08 CET

Muere una mujer durante un ataque de 'ransomware' a un hospital de Dusseldorf (Alemania)

¿Por qué está tan de moda la ciberseguridad?

Impacto empresarial de los ataques

280

Días tardan las empresas en identificar y contener las brechas

* Fuente: informe Deloitte Global

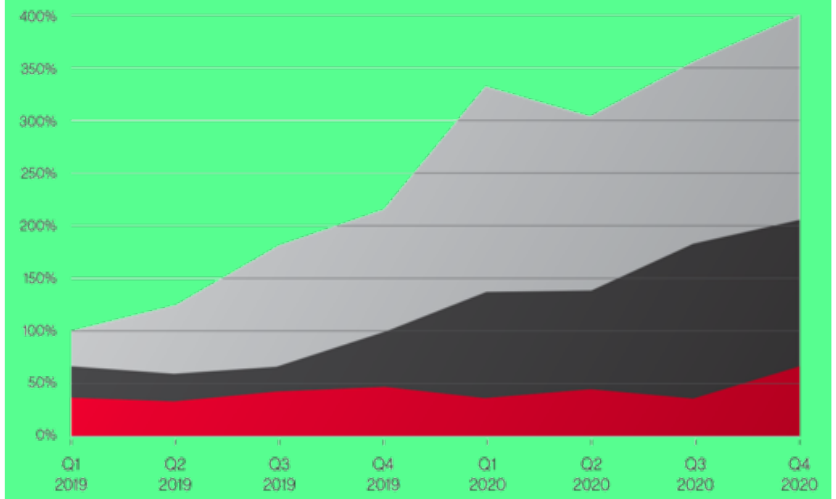
Impacto ataques en ciberseguridad 2021

$6 trillones

$11 trillones se predicen para 2025

*Fuente: Cybercrime Magazine

Crimen organizado en ciberseguridad



* Fuente: 2021 CROWDSTRIKE GLOBAL THREAT REPORT

¿De dónde proceden las amenazas?

Ciberdelincuentes contratados (eCrime as a Service)

Organizaciones criminales

Organizaciones financiadas por estados

Hacktivistas

SOFISTIC CYBERSECURITY

Errores que las empresas suelen cometer

Alta complejidad tecnológica

Mercado de ciberseguridad fragmentado

Tener a empleados como primera línea de defensa

SOFISTIC CYBERSECURITY

¿Cuál es el coste real de un ciberataque?

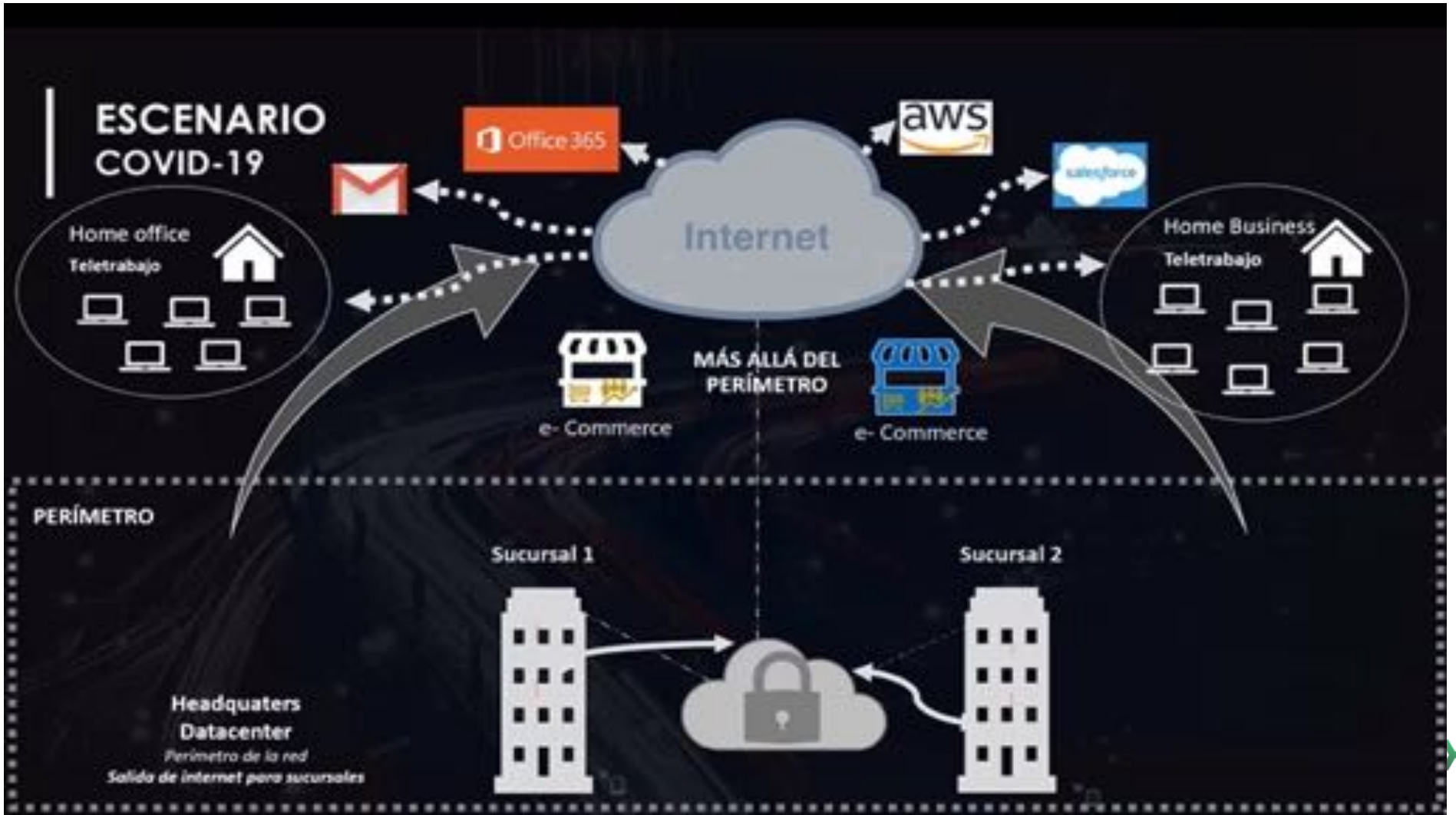
Robo de dinero y datos

Afectación en la reputación de marca y de liderazgo

Responsabilidad empresarial y legal

SOFISTIC CYBERSECURITY

Cambio en el perímetro de la empresa



SOFISTIC CYBERSECURITY

9 principales amenazas 2021/22

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

- Ransomware
- Malware
- Cryptojacking
- Phishing Email
- Brechas de datos
- DDoS y phishing / ataques web
- Desinformación / Bulos
- Amenazas no maliciosas
- Ataques a la cadena de suministro

SOFISTIC CYBERSECURITY

Tendencias ransomware

Supply chain attacks

Double extortion

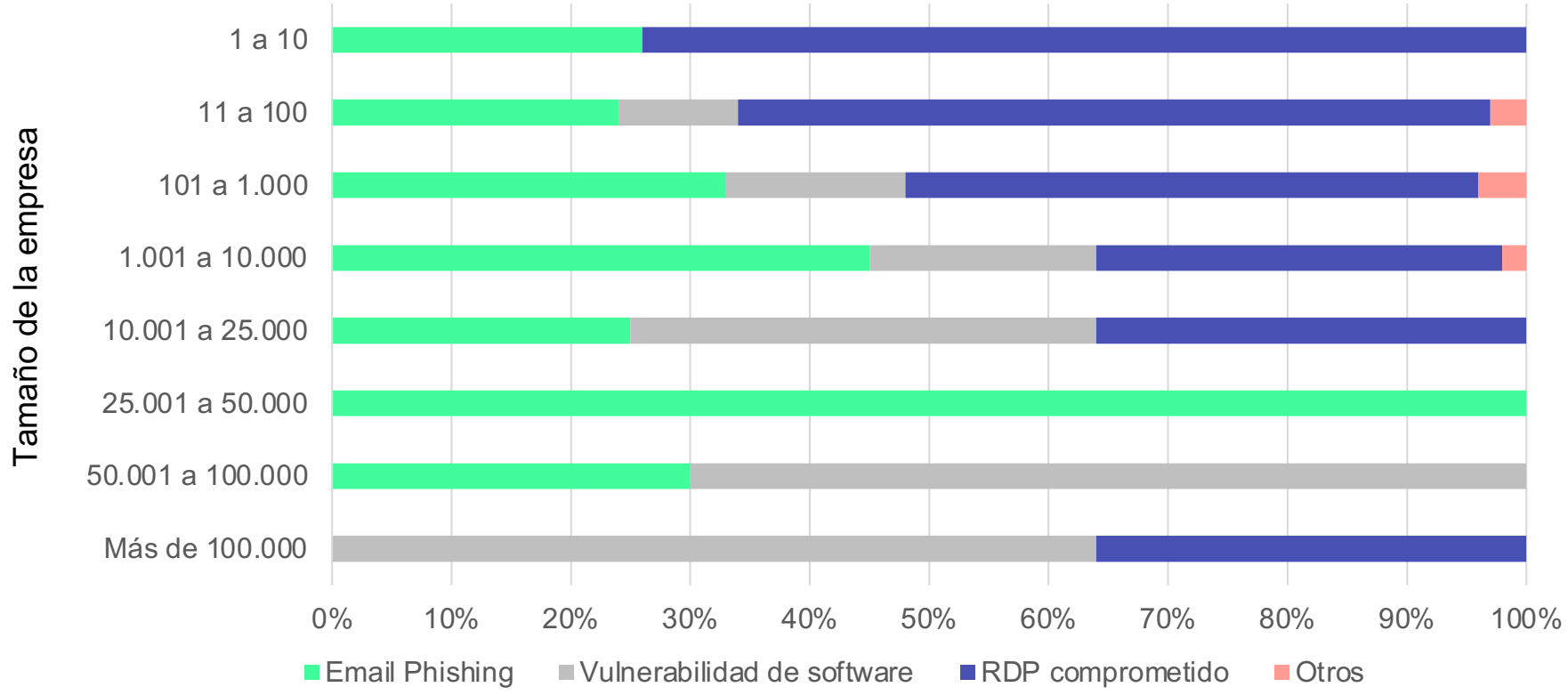
Ransomware as a service

Attacking unpatched systems

Phishing

SOFISTIC CYBERSECURITY

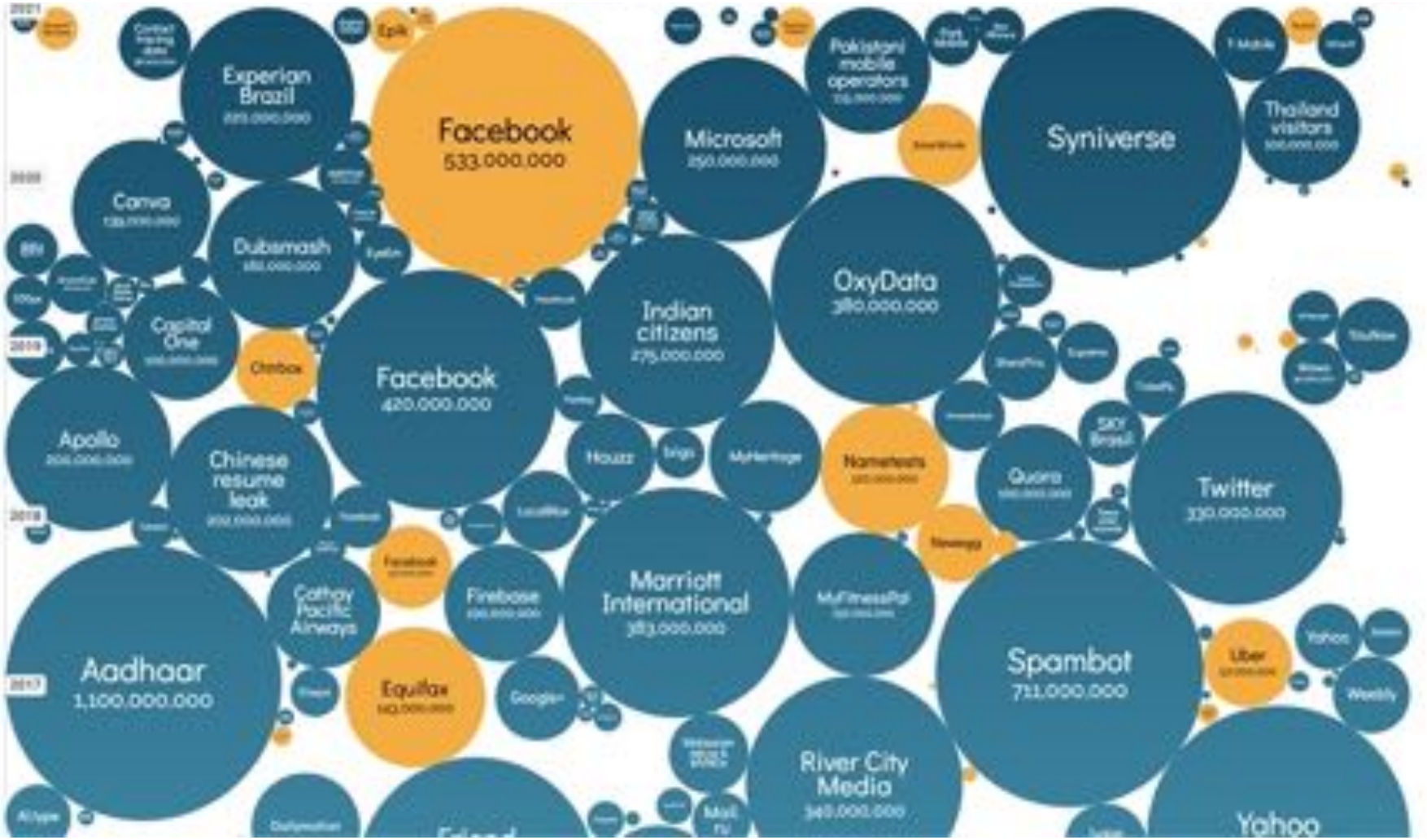
¿Vectores de entrada de los ransomware?



Fuente: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

SOFISTIC CYBERSECURITY

¿Cómo afectan las brechas de seguridad?



SOFISTIC CYBERSECURITY

IA ofensiva

(p.e. ingeniería social)

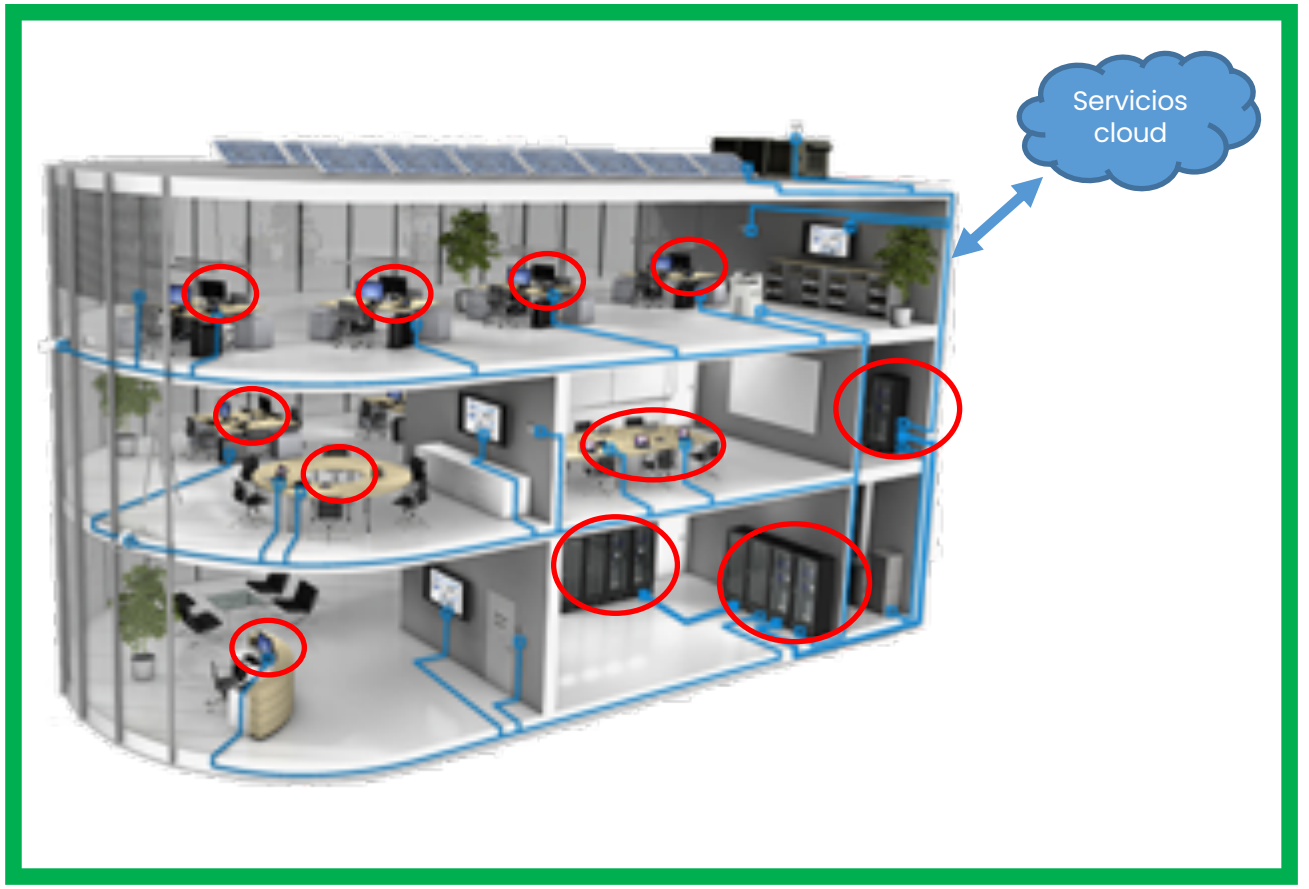
SOFISTIC CYBERSECURITY

IA defensiva

CROWDSTRIKE

DARKTRACE

exabeam



SOFISTIC
CYBERSECURITY

Enfoque actual

SOC + XDR

Extended Detection and Response

Enfocamos al analista en:

Conocimiento

Visibilidad

Prevención

Protegiendo mediante:

Analítica de comportamiento

Centrado en amenazas

Automatización

DARKTRACE CROWDSTRIKE UareSAFE Microsoft exabeam

Ejemplos de incidentes y casos de éxito

SOFISTIC CYBERSECURITY

Ejemplo real incidente: ataque ransomware

¿Qué ha pasado?

- La empresa dispone de diversos sistemas de seguridad (EDR + IDS/IPS).
- El EDR no estaba protegido contra desinstalación y está basado en firmas.
- No hay una correcta gestión de las alertas.
- Además del cifrado, se ha publicado:
  - Base de datos del CRM.
  - Inventariado de equipos, users, hashes.

¿Cómo se podría haber evitado?

- CrowdStrike como EDR basado en comportamiento y con protección anti-desinstalación.
- Darktrace buscando anomalías a nivel de red.
- Gestión eficiente de alertas.

Ejemplo real incidente: fallo segmentación de red

¿Qué ha pasado?

- La empresa tiene “supuestamente” la red segmentada por operaciones.
- Si un equipo usa la conexión para la TV de la sala de descanso, se puede acceder a: impresoras, controlador de dominio, NAS...

¿Cómo se podría haber evitado?

- Darktrace buscando anomalías a nivel de red.
- Realizando ejercicios de test de intrusión externo e interno de forma periódica.

Ejemplo real incidente: malware para minar criptomonedas

¿Qué ha pasado?

- La empresa tiene un AV centralizado, en local y basado en firmas.
- Supuestamente se estaba gestionando el AV de forma correcta.

¿Cómo se solucionó?

- Con CrowdStrike se detectaron los procesos relacionados con el minador.
- Los servidores estaban infectados desde hace más de 2 años.

Caso de éxito: detección de malware polimórfico

¿Qué ha pasado?

- Darktrace detecta incidentes y anomalías a nivel de red, neutralizando las conexiones al exterior.
- Tanto el AV inicial como otro instalado posteriormente, no detectaban nada en los equipos.

- En la POC de CrowdStrike se detectaron los procesos que generaban las alertas. Tras la investigación posterior, se determinó el origen de las alertas y se neutralizó el malware.

Caso de éxito: protocolos obsoletos y conexiones TOR

¿Qué ha pasado?

- Ciertas máquinas OT están un segmento de red específico, con salida a Internet limitada.

- Darktrace detectó:
  - Escaneos de red y movimientos laterales en un equipo industrial.
  - Equipos obsoletos con el protocolo SAMBA v1 activo.
  - Un empleado del departamento I+D+i navegaba por red TOR.

Caso de éxito: trabajador exfiltrando información

¿Qué ha pasado?

- El trabajador finaliza el contrato el viernes.
- A lo largo de la semana, accede a diversos repositorios para descargar información general.
- El último día, realiza una conexión a Sharepoint para descargar información confidencial y moverla a una cuenta de Dropbox personal.

- Darktrace bloquea el equipo para evitar la fuga de información.

Caso de éxito: robo de credenciales

¿Qué ha pasado?

- El EDR bloquea un robo de credenciales en el servidor.
- Los ejercicios de pentest externo/interno evidencian malas prácticas que no se mitigan.
- Las contraseñas utilizadas no se consideran robustas.

- Exabeam detecta, previa a la detección del EDR:
  - Conexiones anómalas de un usuario, y uso de sistema operativo-navegador no habitual.
  - Movimientos laterales en la red.
  - Accesos a diferentes servidores por primera vez.

¿Dudas?

SOFISTIC
CYBERSECURITY

¡Muchas gracias por vuestra atención!

Juan Carlos García
jcgarcia@sofistic.com

SOFISTIC
CYBERSECURITY