V-Valley

enhancing your business

Ciberseguridad: como proteger nuestros datos, seguridad en internet, la importancia de la ciberseguridad a nivel empresarial y el papel relevante que está adoptando hoy en día. Herramientas a nivel usuario.

V-Valley

enhancing your business

Nociones no aburridas de seguridad

David Sánchez

V-Valley Presales

El ponente: (vamos, yo, David Sánchez)

- Preventa de soluciones de seguridad en V-Valley
- Formador oficial para SonicWALL, WatchGuard, Sophos, Trellix (Antiguo McAfee), Check Point, Cloudflare…
- He trabajado como soporte de varios niveles, instalador, formador, preventa técnico, y hasta como desarrollador de negocio ligado a marcas de seguridad
- Nivel de Inglés Medio

- FALSO: Mi inglés es la caña

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Seguridad Informática

- Sirve para proteger una organización
- Peligros de fuera
- Peligros de dentro
- Un ataque informatico no contagia el COVID (eso sí es un virus)
- **… pero puede hacer que cierre una empresa destruyendo la información de la compañía**

Nociones no aburridas de seguridad

Luchamos contra el Lado Oscuro, pero…
¿Quiénes son?

- La gente ve una ataque informático como un delito sin víctimas. Falso, cuestan millones, y tienen consecuencias como pérdida de puestos de trabajo, encarecimiento del coste de la vida…
- Pensadlo, si no robaríais un coche aparcado en la calle, por muy fácil que fuese, ¿Por qué entrarías en la red de una empresa para robar su información y después extorsionarles para recuperarla?

Nociones no aburridas de seguridad

Luchamos contra el Lado Oscuro, pero…
¿Quiénes son?

- A menudo son bandas criminales que delinquen en muchas otras “ramas”: drogas, armas, trata…
- Estados Nación como Rusia, Korea del Norte y otros tienen sus equipos de ataque
- Atacar en solitario es una receta para el fracaso, las Fuerzas de Seguridad son expertos con años de experiencia y presupuesto. Vamos, que te van a pillar fijo.
- Pasad de la cárcel. No es interesante.

Nociones no aburridas de seguridad

- A grandes rasgos, antes había sólo 2 tipos de entrada para atacar:

1. El perímetro, la puerta de entrada de la empresa (FIREWALLS)
2. El endpoint, ordenadores de los usuarios (ANTIVIRUS, ejem)

- Desde la pandemia, como podéis suponer, todo ha cambiado
  - El perímetro casi ha desaparecido
  - Empresas enormes han quedado muy tocadas, otras se han convertido en gigantes, con nuevos modelos de negocio que defender de manera distinta
  - Antiguos fabricantes de seguridad han muerto. ¡Larga vida a los nuevos!
  - Nuevos atacantes, nuevas tácticas de ataque. Nuevos Objetivos
  - Por no hablar de la guerra…

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Espera, entonces, si todo ha cambiado, ¿Cuáles son los ataques que son más efectivos? ¿Con qué podríamos hacer más daño?

Nociones no aburridas de seguridad

V-Valley
enhancing your business

1980 — 2000 — 2010 — 2018

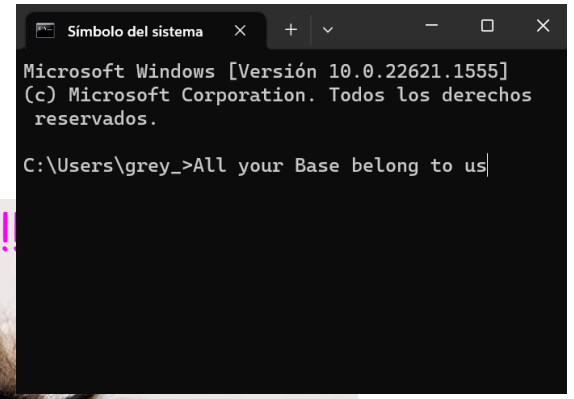
A m e n a z a s

Gen I	Gen II	Gen III	Gen IV	Gen V
Últimos 1980s – Ataques a PCs – Sin conexión	Mediados 1990s – Ataques desde internet	Primeros 2000s - Explotando vulnerabilidades de aplicaciones	2010 - Contenido Polimórfico	2018- Mega ataques multi-vector
Anti Virus	**Firewall**	**Intrusion Prevention (IPS)**	**Sandbox y Anti-Bot**	**Tecnologías Antimalware multicapa en tiempo real**
100%	100%	50%	7%	?%

Nociones no aburridas de seguridad

V-Valley
enhancing your business

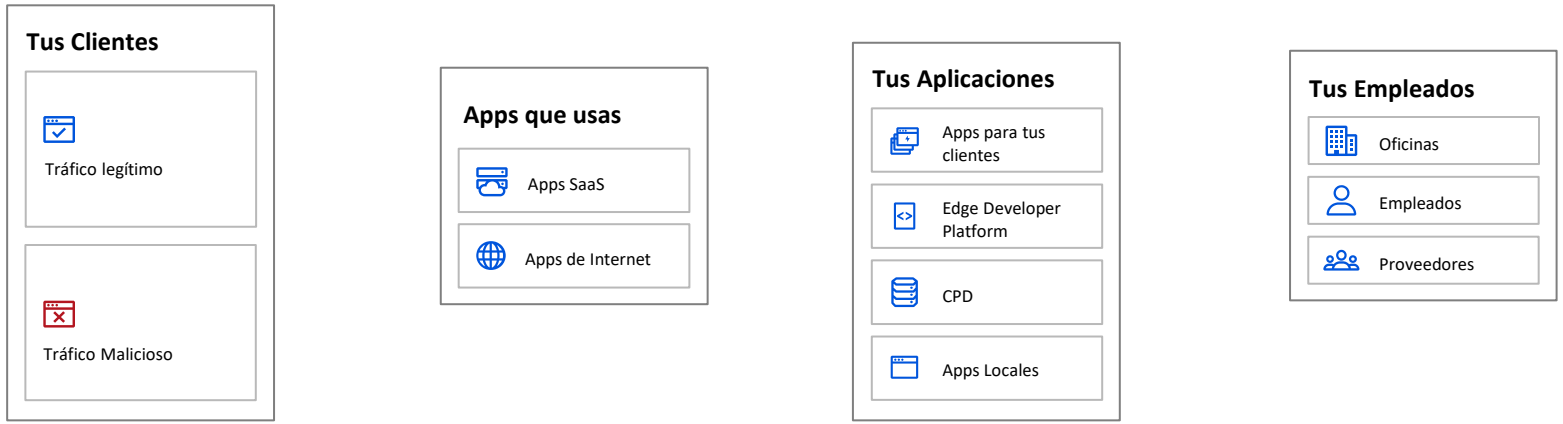
- **Tipos de Ataque**
  - Vector de ataque, generalmente el usuario por ingeniería social, aunque puede muy bien ser phishing, spear phishing, spam, robo de credenciales, malware, exploits…
  - Un ataque Zero Day es un ataque para el que aún no existe protección.
  - Un hacker suele ser creativo, no sabemos cual es el siguiente método, y generalmente, un ataque va a usar varias estrategias para garantizarse el éxito.
  - El sentido común es la mejor defensa.
  - **El 99% de los usuarios carecemos de sentido común**



Nociones no aburridas de seguridad

Superficies de contacto: qué son, y cómo defenderlas

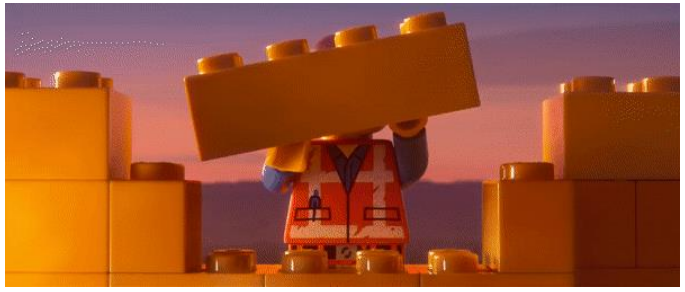
- Una superficie de contacto es cualquier dispositivo, servicio, aplicación o comportamiento de usuarios que está expuesto a un ataque.
- Ojo, el ataque no tiene por qué venir de internet, también hay ataques realizados “desde dentro”.
- Normalmente, ninguna empresa intenta cubrir todas sus superficies de contacto a la vez, siempre intentamos solucionar las más críticas primero.



Nociones no aburridas de seguridad

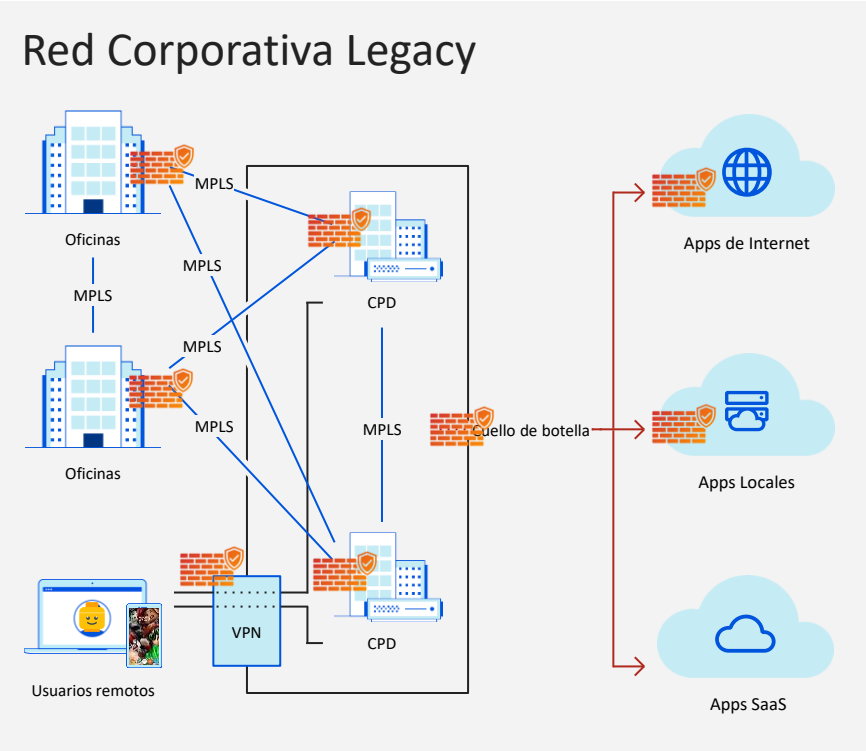
Superficie de contacto: Perímetro

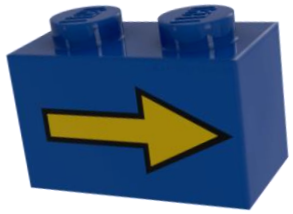
- El Perímetro es lo que rodea una o varias redes corporativas (De ahora en adelante las denominaremos LAN)
- Está protegido por uno o más puntos de entrada. Estas protecciones pueden ser de diverso tipo, las más habituales son Firewalls, pero también existen IPS, Proxies, WAFs, SWG, Email Security…
- Durante la pandemia, el perímetro se ha difuminado totalmente, la movilidad ha ganado presencia, y ahora mismo hay que buscar soluciones nuevas.



Nociones no aburridas de seguridad

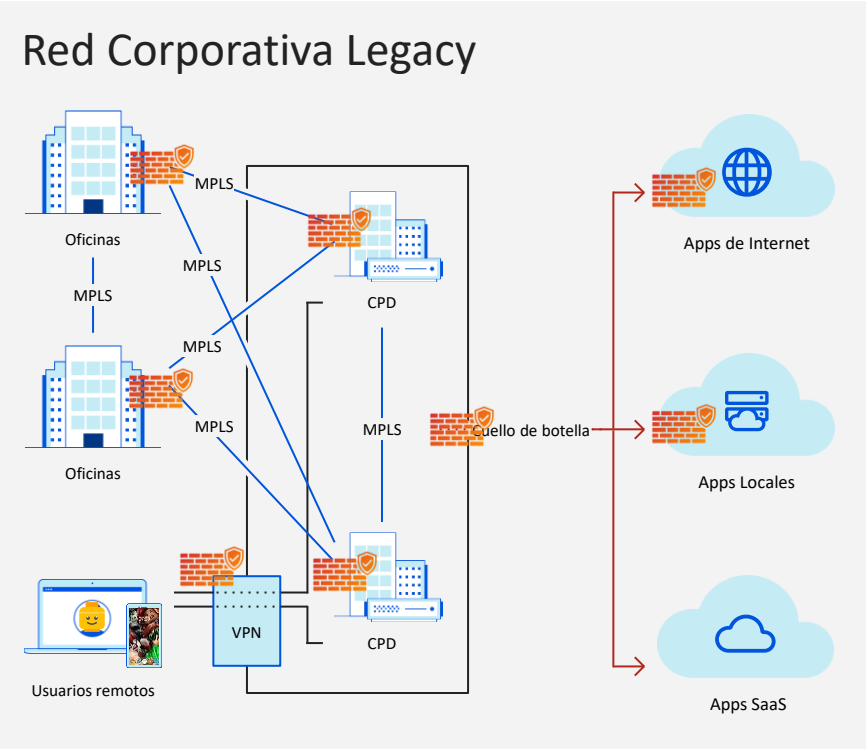
Superficie de contacto: Perímetro

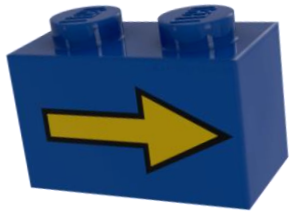




Nociones no aburridas de seguridad

Superficie de contacto: Perímetro

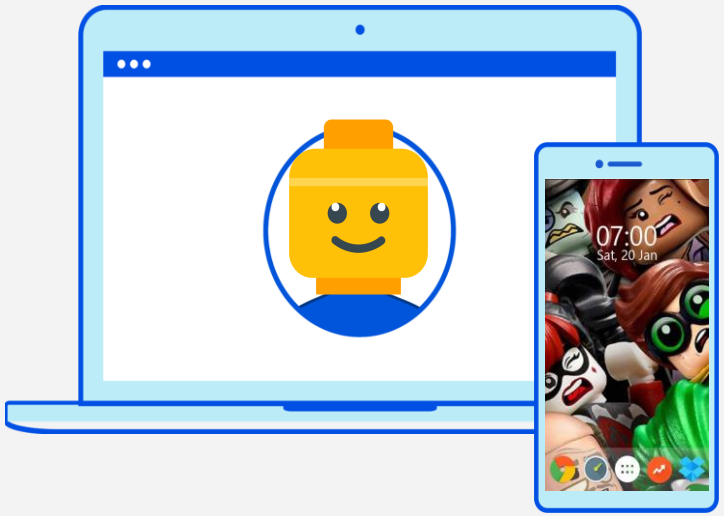




Nociones no aburridas de seguridad

Superficie de contacto: Endpoint

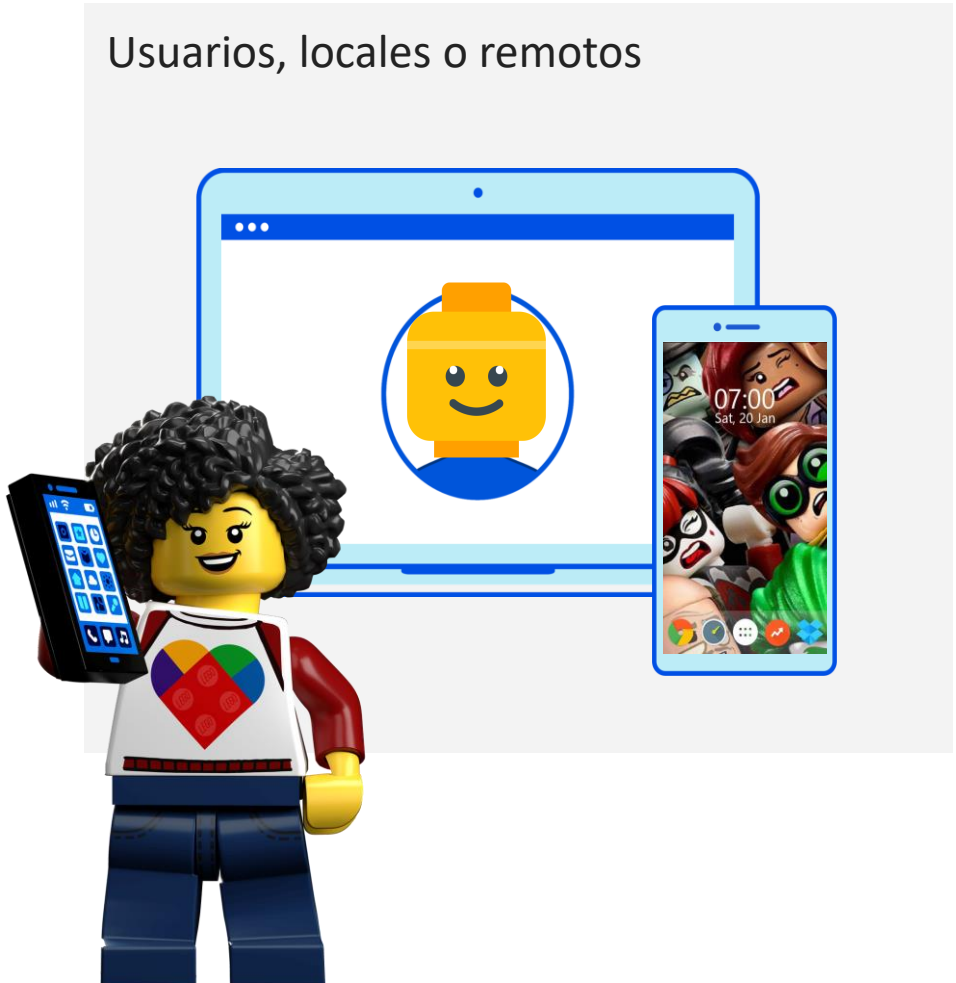
Usuarios, locales o remotos



- El Endpoint está ya habitualmente fuera del perímetro, y por tanto, desprotegido
- Las soluciones Endpoint Security (ENS) son cada vez más sofisticadas, y ya no dependen de firmas para detener ataques
- Disponen de gestión centralizada (preferiblemente SaaS), Firewall, Host IPS, Control de URLs, control de aplicaciones, y algunas soluciones hasta cliente VPN.
- Hay pocas empresas sin ENS, pero si hablamos de los móviles…

Nociones no aburridas de seguridad

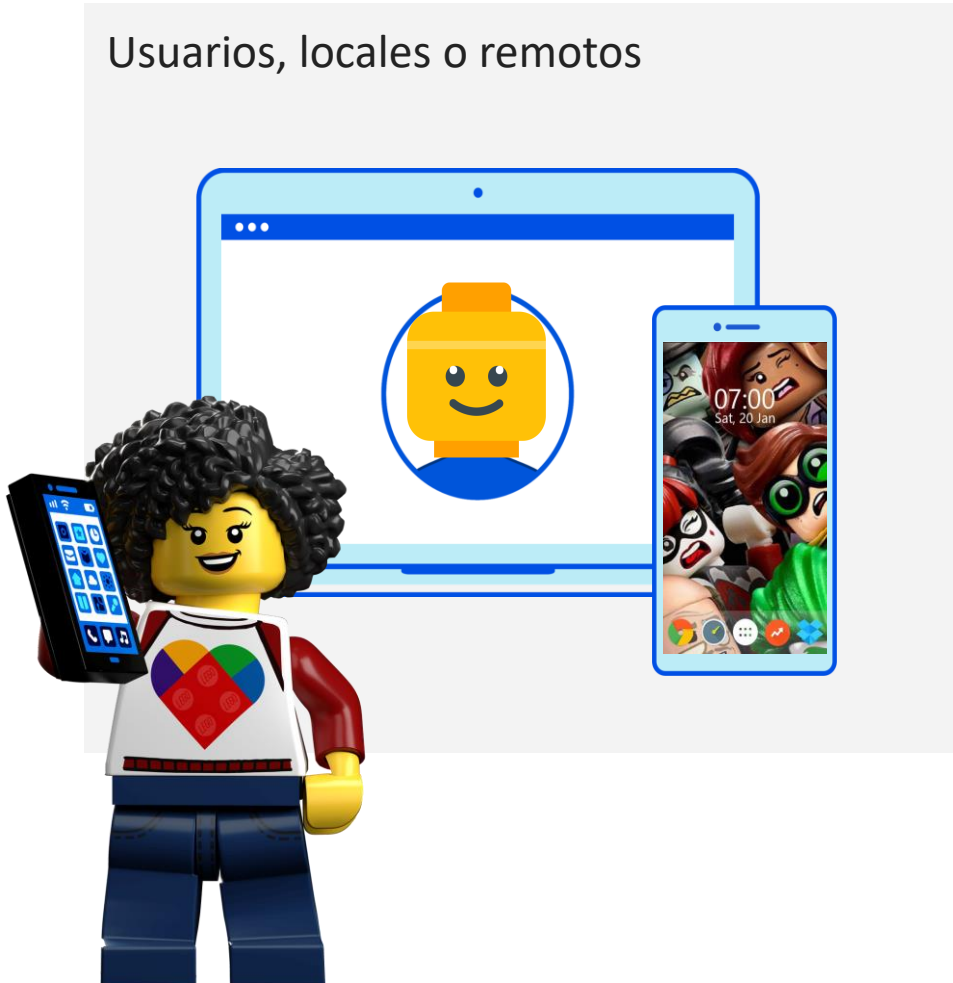
Superficie de contacto: Endpoint



- Hablemos de los móviles:
  - Actualmente, son uno de los principales puntos débiles de cualquier organización
  - Sistema Operativo muy restringido, a menudo un ENS no puede ni borrar un archivo malicioso después de detectarlos
  - Los ENS avanzados para SO móvil se denominan MTD, y no todos los ENS son MTD. Un MTD habla con un UEM (Universal Endpoint Manager, el antiguo MDM) para realizar las acciones de seguridad solicitadas
  - Permiten un control total del parque móvil

Nociones no aburridas de seguridad

Superficie de contacto: Endpoint

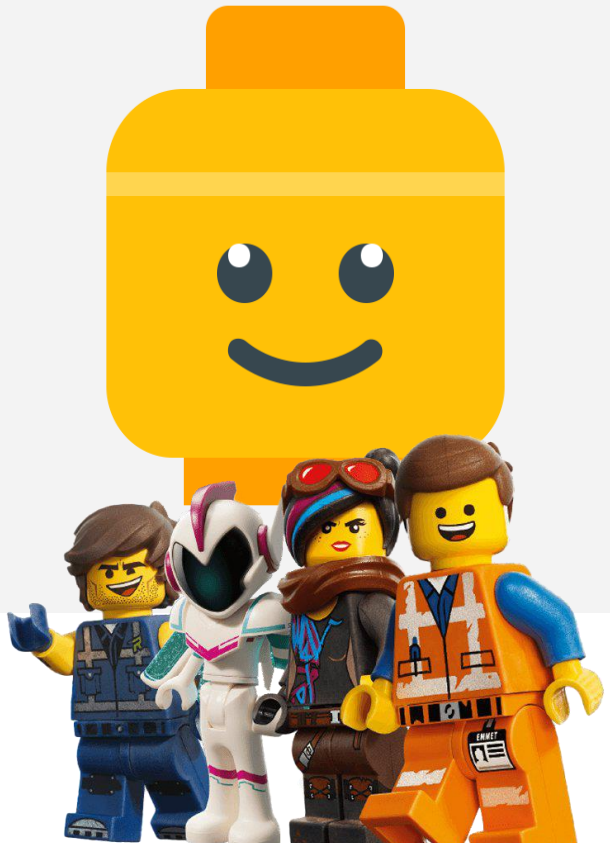


- Hablemos de los móviles:
  - Actualmente, son uno de los principales puntos débiles de cualquier organización
  - Sistema Operativo muy restringido, a menudo un ENS no puede ni borrar un archivo malicioso después de detectarlos
  - Los ENS avanzados para SO móvil se denominan MTD, y no todos los ENS son MTD. Un MTD habla con un UEM (Universal Endpoint Manager, el antiguo MDM) para realizar las acciones de seguridad solicitadas
  - Permiten un control total del parque móvil

Nociones no aburridas de seguridad

Superficie de contacto: Usuarios

Usuarios, locales o remotos

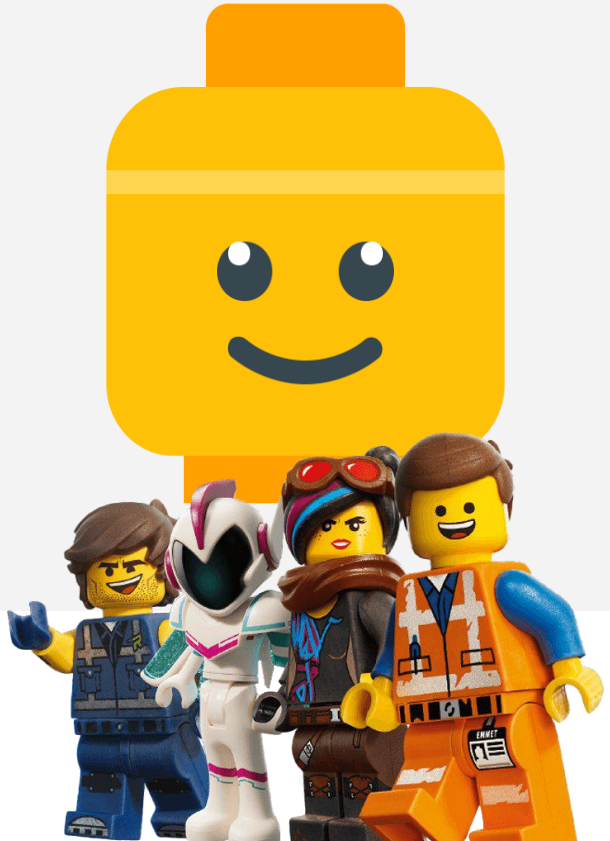


- El usuario es probablemente el primer “culpable” de que los atacantes consigan sus objetivos
- La concienciación, la formación, son indispensables. Pero siempre va a existir ese usuario “que lo sabe todo”, o “que le gusta hacer click”…
- Actualmente, existen varios tipos de defensa para asegurarnos de que esto no ocurre: NAC, UEBA, ZTNA, IAM, Control de URL…
- Os sorprendería saber la cantidad de empresas que aún no disponen de un dominio…

V-Valley
enhancing your business

Superficie de contacto: Usuarios

Usuarios, locales o remotos



- La idea aquí es huir de proteger máquinas, y empezar a proteger usuarios.
- Lo primero es identificarlo, asegurarnos de que es quien dice ser. Además, hay que establecer qué privilegios tiene ese usuario, y cuál es su comportamiento “aceptable”.
- En base a esos permisos, y a ese comportamiento habitual, el usuario tendrá acceso o no a los recursos corporativos, o de internet. Además, podemos regular, o prohibir el uso de BYOD. En cualquier plataforma y SO.

Nociones no aburridas de seguridad

Superficie de contacto: La Nube

- Las nubes, públicas, privadas, IaaS o SaaS son ya una parte normal de nuestras vidas. Ya no es “cuando migremos a la nube”, las empresas usan la nube cuando es necesario, y las situaciones híbridas son el escenario común.
- Las nubes, por defecto, requieren identificación, con lo que los siguientes pasos, IAM, UEBA, son bastante sencillos siempre que dispongamos de servicios SSE, SASE, o incluso un simple CASB.

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Superficie de contacto: La Nube

- Sin embargo, las nubes a menudo asumen la “responsabilidad compartida”, hay partes de la infraestructura que es protegida por el proveedor, y partes que son responsabilidad nuestra. Nuestros datos, habitualmente, caen en este último caso.
- Así, “XXXX no se ocupa de la seguridad”, a no ser que la contratemos expresamente, y hay muchas empresas que prefieren la seguridad del fabricante que ya conocen sus técnicos, que la seguridad de AWS, Azure o GCloud, por ejemplo.

Nociones no aburridas de seguridad

Superficie de contacto: La Nube

- Las nubes de todo tipo, como ya han demostrado las apps para móviles, van a tener cada vez más importancia en la foto. Los servicios locales están ya en muchos casos sólo en nichos de seguridad extrema, con niveles de paranoia y desconfianza altísimos, como la Defensa Nacional.
- SASE, WAFaaS, SWG, FWaaS, IPSaaS, los servicios de Postura de Seguridad e Inventariado, además del boom de servicios de identificación SAML, nos permiten asegurar un uso racional y controlado de los recursos de las nubes.

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Nociones no aburridas de seguridad

V-Valley
enhancing your business

El Email es, sin duda, el mayor problema hoy en día

- La mayor parte de ataque van a venir por ahí
- **Está en todas partes. Móvil. IoT. Tu PC. El PC de la Oficina.**
- Hay mil oportunidades de liarla, y con liarla una vez, es suficiente.

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Bienvenidos a Técnicas, Tácticas y Procedimientos 101

- Un ataque tipo sucedería así:
  - Varias personas de la organización reciben un email, suplantando a una entidad que envía emails habitualmente al equipo.
  - El email en sí no tiene contenido malicioso, pero si contiene un “botón”, que incluye un enlace que redirige a quien lo pulsa a una página HTTPS, que simula ser el servicio del email (Por ejemplo, DHL).
  - Muy pocas compañías tienen activado el análisis del tráfico SSL, con lo que la página “entra”.
  - Una vez que estás en esa página, pueden cargar contenido activo malicioso, intentar un robo de credenciales para llevar a cabo un ataque a una escala mayor, o simplemente ganar acceso. El cielo es el límite a partir de entonces.

V-Valley
enhancing your business

Bienvenidos a Técnicas, Tácticas y Procedimientos 101

- A simple vista el atacante ha usado una ausencia de Email Security, y una baja seguridad en el firewall del perímetro para llevar a cabo su ataque, sin embargo, el trabajo del atacante ha podido ser mucho más elaborado
  - Trabajo previo de investigación y recolección de direcciones válidas de email, perfil de la empresa, acudir a la sede para ver qué servicio de mensajería usan, o incluso hablar con algún usuario de la empresa en un descanso, durante el almuerzo… Cuanto más profunda la investigación, más oportunidades de éxito.

V-Valley
enhancing your business

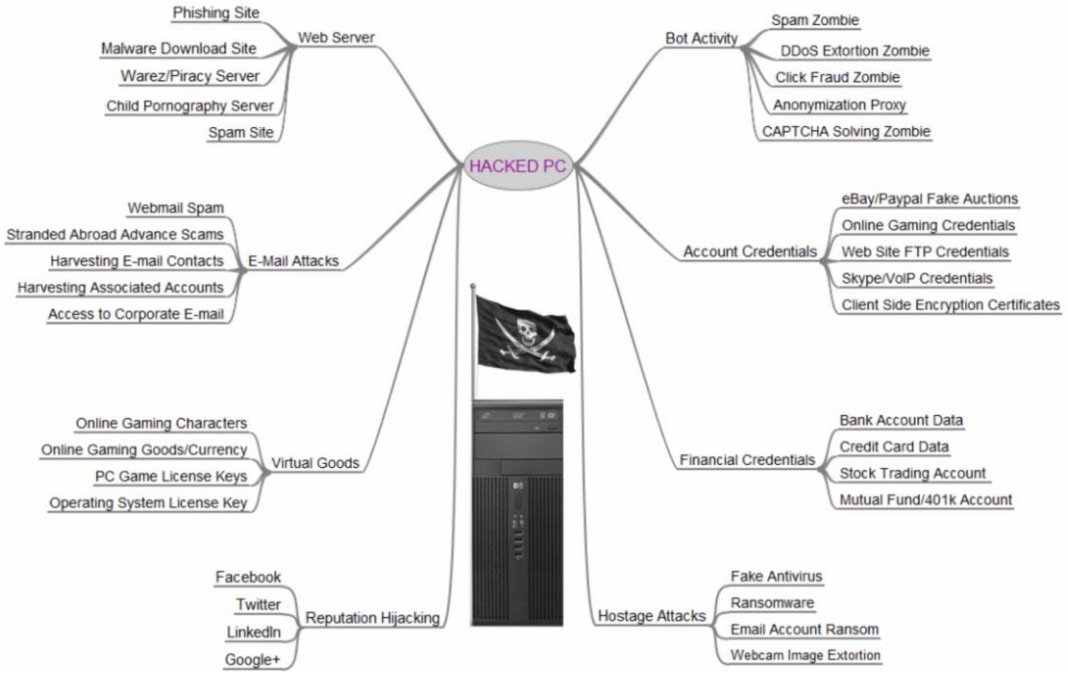
Bienvenidos a Técnicas, Tácticas y Procedimientos 101

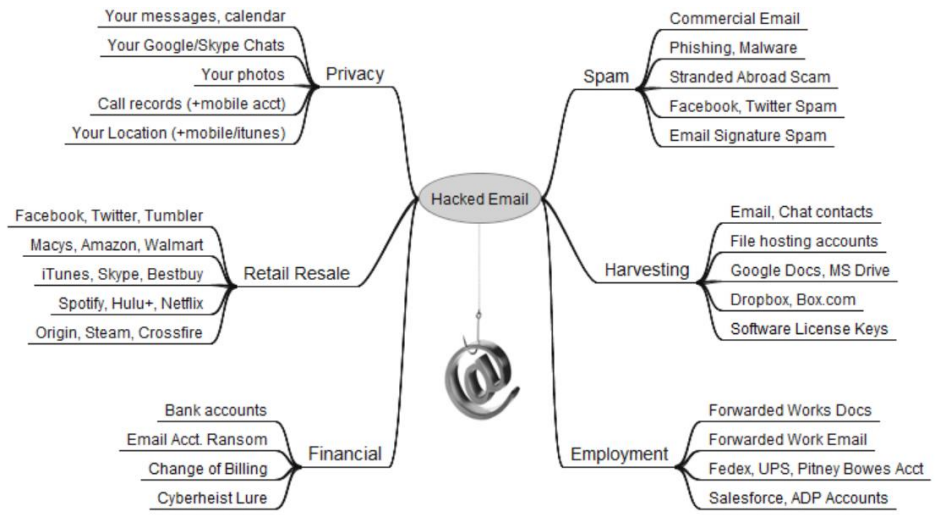
- A simple vista el atacante ha usado una ausencia de Email Security, y una baja seguridad en el firewall del perímetro para llevar a cabo su ataque, sin embargo, el trabajo del atacante ha podido ser mucho más elaborado
  - El atacante ha tenido que confeccionar un email que se parezca realmente al servicio a suplantar, y crear la landpage que después insertará la amenaza en el visitante. El resto de “infraestructura” para la realización del ataque es bastante sencilla de conseguir para un atacante profesional.

Nociones no aburridas de seguridad

Bienvenidos a Técnicas, Tácticas y Procedimientos 101

- A simple vista el atacante ha usado una ausencia de Email Security, y una baja seguridad en el firewall del perímetro para llevar a cabo su ataque, sin embargo, el trabajo del atacante ha podido ser mucho más elaborado





Nociones no aburridas de seguridad

V-Valley
enhancing your business

Bienvenidos a Técnicas, Tácticas y Procedimientos 101

- Sólo queda esperar, y recoger los frutos del “duro” trabajo…
- Todas estas técnicas están detalladas en el Mitre Att&ck Framework

- Muchos fabricantes de seguridad hacen uso de este framework para desarrollar defensas específicas para apartados concretos del framework, y para la posterior visualización de los eventos recogidos.
- La idea es, además de ser más precisos al crear las herramientas, entender después mejor qué es lo que ha pasado

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Sí. Jo.

Nociones no aburridas de seguridad

El elefante en la habitación, la visualización

- Cualquier fabricante de seguridad que se precie, dispone de una herramienta de visualización para entender lo que ha pasado durante el tiempo que ha estado defendiéndolo.
- Además, muchas organizaciones necesitan almacenamiento normativo de logs durante años, para cumplir con la legislación vigente. Para esto, existen soluciones como los SIEM, o los agregadores de logs, que pueden ofrecer visualización especializada en seguridad, además de ese almacenamiento.

Nociones no aburridas de seguridad

El elefante en la habitación, la visualización

- Las herramientas de visualización pueden ayudarnos a descubrir nuestros puntos débiles, y a subsanarlos después de remediar un ataque. Mediante Mitre y la correlación de eventos, podemos ver no sólo el punto de inicio y el punto final, sino toda la cadena de eventos producidos.
- Una vez que tengamos nuestra lista de la compra, podemos ir punto por punto solucionando problemas.

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Visualizar, remediar, pero ¿Qué más podríamos hacer después del ataque?

- Automatizar, claro.
- Existen soluciones multifabricante que mediante la API de los distintos fabricantes, que incluyen playbooks, orquestaciones de diversos elementos para que, una vez detectado el comienzo del próximo ataque, se tomen medidas automáticas e inmediatas, que reduzcan al mínimo la exposición. Los SOAR son herramientas, que junto a un SIEM, permiten mejorar sensiblemente la postura de seguridad de la organización.

Nociones no aburridas de seguridad

Herramientas Gratuitas

- Las herramientas para cubrir cada superficie de contacto, pueden ser gratuitas hasta cierto punto. Obviamente, el nivel de protección no es igual que el que tienen soluciones comerciales con equipos de I+D, y tampoco están tan “terminadas”, pero muchas veces el objetivo no es ese. Ojo, tampoco hay soporte…

Nociones no aburridas de seguridad

Por superficie de contacto:

- Perímetro: PFSense sin duda. Da para jugar y configurar bastante
- Endpoint Security: Avast, Avira, Microsoft Defender
- Defensa de Aplicación: WAF y AntiDDoS de Cloudflare
- Conoce a tu enemigo: Kali, Nmap, Metasploit, Aircrack-NG, Shodan
- Visualización: Wireshark, por supuesto.
- Investigación: ZimmermanTools

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Herramientas Comerciales:

- Las herramientas no gratuitas suponen un coste, pero vienen con muchas ventajas obvias, facilidad de uso, soporte, solución rápida de bugs, canal de venta, desarrollo continuo de I+D con miles de personas involucradas…
- La mayor parte de empresas de tamaño medio ve valor en este tipo de propuesta, y las prefiere a soluciones gratuitas

A10 · BACKBOX · Bitdefender · CLOUDFLARE
CHECK POINT · ca technologies A Broadcom Company · CounterCraft · ENTRUST
kaspersky · MICRO FOCUS · SONICWALL · TREND MICRO
Trellix · Skyhigh Security · VU · WatchGuard

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Herramientas Comerciales:

- Perímetro: Check Point, Cloudflare, Sonicwall
- Endpoint Security: Trellix, Check Point, Trend Micro
- Defensa de Aplicación: Cloudflare, A10
- Identidad: Entrust
- Visualización: Trellix, XMCyber
- Investigación: Trellix

A10 BACKBOX Bitdefender CLOUDFLARE
CHECK POINT ca technologies A Broadcom Company CounterCraft ENTRUST
kaspersky MICRO FOCUS SONICWALL TREND MICRO
Trellix Skyhigh Security VU WatchGuard

Nociones no aburridas de seguridad

Trabajar en ciberseguridad:

- Es bueno tener un título universitario en el ramo informático, pero no es imprescindible. Esto es más de saber que de títulos (aún).
- Trabajar en el sector es fácil una vez que consigues tu puerta de entrada (y te matas a aprender y a turnos complicados durante unos años). Después, no falta trabajo.
- Mantenerte en el sector es a partir de ahí una combinación de trabajo, actualizarte, buenas decisiones al cambiar de empresa, y ser una persona normal. De las que saludan, se despiden, y son amables con la gente.

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Trabajar en ciberseguridad:

- E inglés. Creo que lo he mencionado al principio, pero no puedo deciros lo importante que ha sido para mi carrera en seguridad poder entenderme con la gente que sabe y que viene a compartir conocimiento (y oportunidades) desde otras latitudes. Ya sea China, Korea, Francia, Alemania, UK o USA. Todo es en inglés.
- Si flojeas, dale toda la caña que puedas.

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Nociones no aburridas de seguridad

V-Valley
enhancing your business

Haber estudiado inglés...

Thank you

GRAZIE • GRACIAS • OBRIGADO • DANKE • MERCI • 감사 • 謝謝 • 感謝

V-Valley is the Advanced Solutions Distributor of the Esprinet Group

V-Valley | esprinet®