Personas: La Primera Linea de Ciberdefensa

David F. Pereira Q.

David F. Pereira Q.
@davidpereiracib

- Fundador y Director Ejecutivo de SecPro
- CEH, ECSA/LPT, CHFI, ENSA, ECSS, ECVP, CEI, QGSS, ECIH, EDRP, NFS, OPSEC, CICP, CCISO.
- +24 Años de experiencia en Ciberseguridad y DFIR
- Consultor Internacional - Hacker Ético en diversas entidades en el mundo, de ámbitos como el Financiero, Energético, Militar, Inteligencia, Diplomático, Minero, entre otros.
- Instructor / Consultor de Fuerzas de Ciberdefensa, Fuerzas Militares y Policía, en varios Países. (Homeland Security – Servicio Secreto entre otras)

SecPro
SECURITY PROFESSIONALS

Personas: La Primera Línea de Ciberdefensa

@davidpereiracib

Preguntas Complejas de Responder para las áreas de Seguridad TI:

- Que tan efectivas son mis defensas?
- Que tan útiles son los datos que capturan mis dispositivos?
- Podría detectar una APT dentro de mi red?
- Tengo cubrimiento traslapado de herramientas? (2 o mas herramientas que hagan lo mismo)
- La tecnología que me ofrece el mercado es la solución a mis necesidades?

Personas: La Primera Línea de Ciberdefensa

@davidpereiracib

La Pirámide del Dolor: Hagamos sufrir al atacante

"Todas las operaciones en el Ciberespacio, comienzan con un Ser Humano"

David F. Pereira Q.
@davidpereiracib

El accionar del Ciberdelincuente: (Kill Chain)

@davidpreiracib

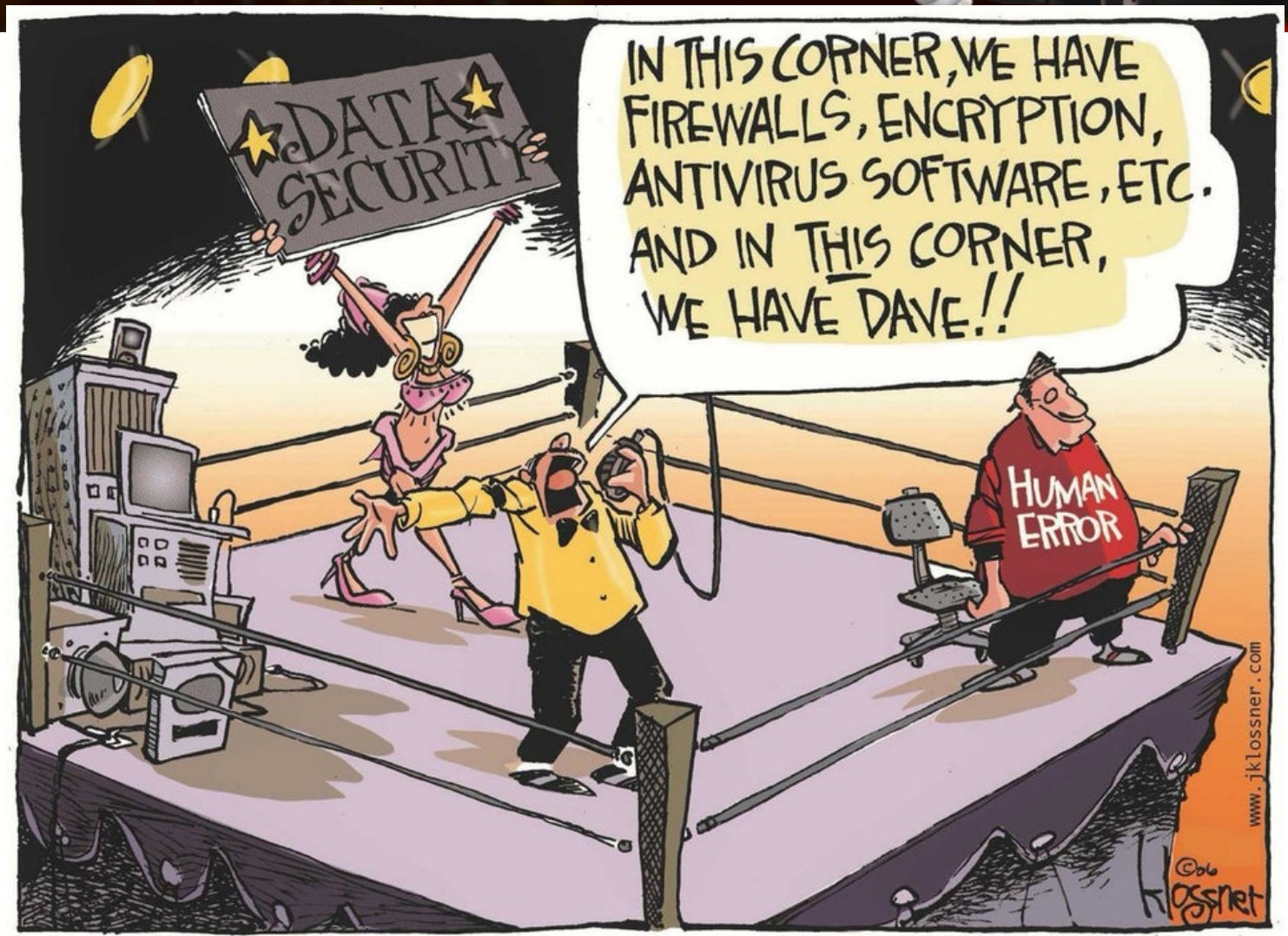
En donde Interviene el error humano?

Ciberataque

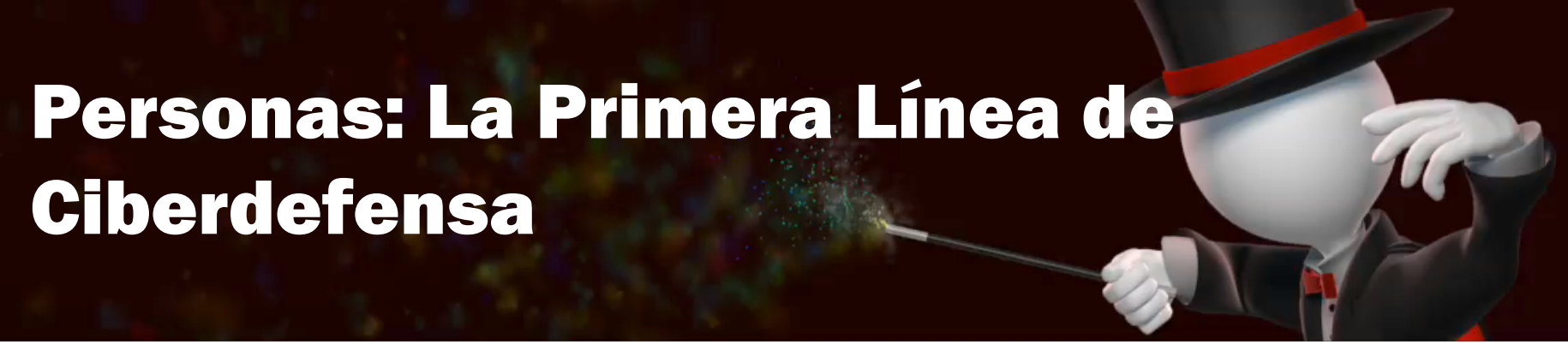
1. Reconocimiento	Info de: Servidores, Infraestructura, Proveedores , Software, emails, usuarios, etc. Teléfonos, etc. (OSINT)	Preparación
2. Weaponization	Crear archivo con el exploit o malware para entrega, o definir tipo de ataque	
3. Entrega	Enviar Mail, Enlace de Internet, Memoria USB o Similar, usar ingeniería social	Intrusión
4. Explotación	Explotar vulnerabilidad para ejecutar código en la infraestructura victima	
5. Instalación	Instalar Malware, Backdoor o extraer información de la infraestructura victima	
6. Comando y Control – C2	Controlar a la Víctima remotamente por canal cifrado oculto tipo I2P, Tor, VPN	Intrusión Activa
7 Acción sobre el Objetivo	Generar el acto hostil sobre la infraestructura de la Víctima	

SecPro
SECURITY PROFESSIONALS

@davidpereiracib



Personas: La Primera Línea de Ciberdefensa



“La identidad del Usuario es el nuevo perímetro”

@davidpereiracib

F3EAD

@davidpereiracib

Es un sistema que permite estimar y prever las operaciones enemigas, visibilizar, localizar y atacar las fuerzas contrarias, realizar inteligencia, explotación y análisis del personal y del material enemigo capturado

F3EAD en Ciber

@davidpereiracib

- Find

  Cuáles son las prioridades de nuestra operación?

  Cuáles son los problemas que debemos resolver?

- Fix

  En donde podemos encontrar la información que requerimos?

  En donde están localizados los problemas identificados?

- Finish

  Cual es la respuesta al problema?

  Como podemos resolverlo?

  Como lo consideramos solucionado?

SecPro
SECURITY PROFESSIONALS

F3EAD en Ciber

@davidpereiracib

- Exploit
  - Dónde reposa la información sobre la Operación?
  - Qué información es crítica para su análisis?
- Analyze
  - Qué aprendimos de esta operación?
  - Que información debemos compartir con las partes interesadas?
  - Cómo vamos a presentar estos datos?
- Disseminate
  - Quién necesita conocer esta información y cuando?

SecPro
SECURITY PROFESSIONALS

OPSEC para contrarrestar Kill Chain

@davidpereiracib

Reconocimiento | Armamento | Entrega | Explotación | Instalación | Comando y Control | Ataque

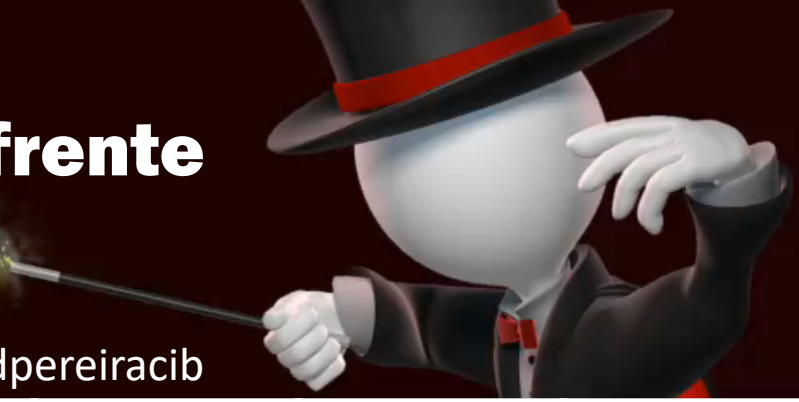
Fase 1: Preparación | Fase 2: Intrusión | Fase 3: Brecha

Medidas Proactivas

Medidas Reactivas

Limitar la exposición de información Crítica	Detectar vulnerabilidades en nuestros sistemas	Concientización Detección Monitoreo Vigilancia Digital UEBA Control de Privilegios	Detecc. Escalación de Privilegios Detecc. Exfiltración de datos Respuesta a Incidentes

Ciclo de Ciberinteligencia frente a Kill Chain



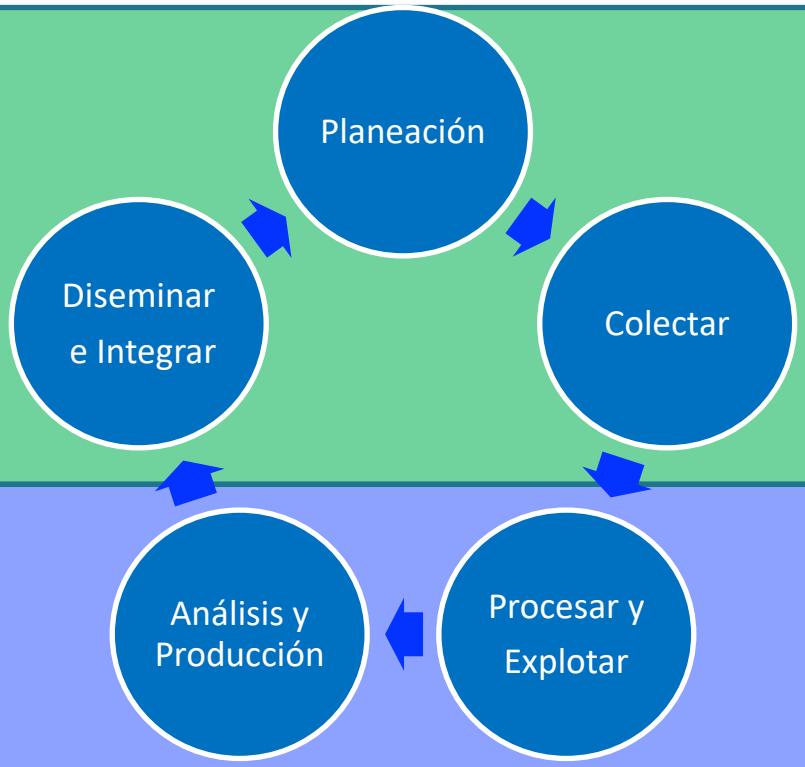
@davidpereiracib

Reconocimiento → Armamento → Entrega → Explotación → Instalación → Comando y Control → Ataque

Fase 1: Preparación | Fase 2: Intrusión | Fase 3: Brecha

Nivel Estratégico

Nivel Táctico



Personas: La Primera Linea de Ciberdefensa

@davidpereiracib

Ingeniería Social:

Técnica que el ciberdelincuente usa para engañar a las personas, buscando que:

- Hagan Algo
- Crean Algo
- Digan Algo
- Entreguen Algo

Personas: La Primera Linea de Ciberdefensa

@davidpereiracib

Por qué somos susceptibles a estos ataques?

R./Porque somos Humanos

- Tendemos a confiar
- Queremos ser de ayuda o utilidad
- Deseamos obtener reconocimiento
- Somos curiosos
- Nos da miedo perder algo
- No sabemos que existe la Ingeniería Social
- Pensamos que no vamos a ser víctimas

Personas: La Primera Línea de Ciberdefensa

@davidpereiracib

Cómo logran engañarnos los ciberdelincuentes?

1. Aprovechan toda la información que puedan buscar de nosotros

- OSINT: Open Source Intelligence
- (Búsqueda en Fuentes Abiertas)
  - Redes Sociales
  - Internet
  - Redes Profesionales
  - Blogs
  - Etc.

Personas: La Primera Línea de Ciberdefensa

@davidpereiracib

¿Con una imagen mia… Qué pueden hacer?

Tracking (En donde Estamos, Quienes Somos), Detección de Sistema Operativo, Reconocimiento Facial, Aplicaciones Instaladas en mi máquina y más….

Veamos…..

Personas: La Primera Línea de Ciberdefensa

@davidpereiracib

Cómo logran engañarnos los ciberdelincuentes?

2. Establecen un vínculo o relación

- Chats
- Imágenes
- Emojis
- Llamadas
- Encuentros
- Detección de Emociones
- Generación de Confianza

Nada es lo que parece …

@davidpereiracib

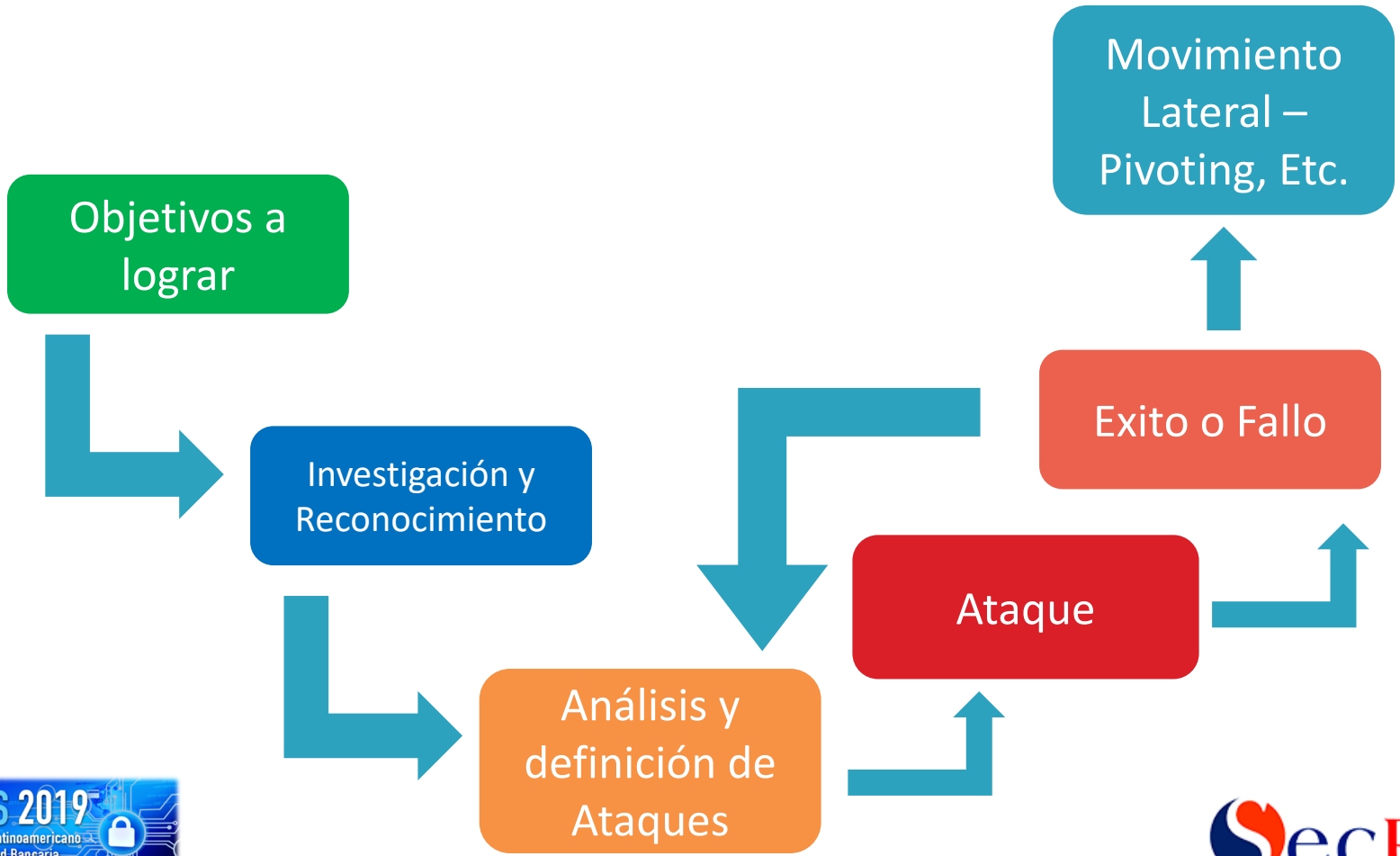
Cómo logran engañarnos los ciberdelincuentes?

3. Nos Influencian

- Nos Convencen de algo
- Nos hacen sentir obligados a algo
- Implantan una idea
- Crean una necesidad
- La Explotan

El Flujograma de la Ingeniería Social

@davidpereiracib



Constantes en el hacking humano

@davidpereiracib

En un ataque normalmente encontramos:

- Manipulación de emociones
- Formas de presionar con el tiempo
- Usurpación de Identidad de funcionarios, autoridades, etc.
- Algún tipo de carnada u oferta
- Dar una falsa sensación de tranquilidad Ej. 2FA

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Laser Phishing

El Laser Phishing es una técnica de phishing que utiliza Inteligencia Artificial. De esta manera cada correo falso se crea customizado y configurado de acuerdo a la información que se logra recabar de forma automática por parte del atacante. Se tienen en cuenta factores como:

- Intereses
- Actitudes
- Preferencias

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Baiting

El Atacante deja abandonados en distintos lugares, memorias USB,o dispositivos llamativos, con el objetivo de que alguien caiga en la trampa y las introduzca en un Computador: normalmente vienen infectadas con algún tipo de malware o realizan acciones automáticas en la máquina en donde se introducen generalmente a fin de tomar control del equipo victima;

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Piggybacking - Tailgating

El atacante camina detrás de la víctima e incluso podría entablar una breve conversación a fin de que la víctima lo deje pasar o los celadores o vigilantes asuman que vienen juntos y le permitan el ingreso.

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Piggybacking - Tailgating

En otro tipo de ataque piggybacking, el ingeniero social pretenderá ser una persona que entrega un paquete o mercancía, probablemente con algún tipo de uniforme. Él o ella se acercarán a la puerta justo detrás de otros empleados, cargados con un paquete y solicitará a alguien ayuda para abrir la puerta.

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Vishing - Swatting

Técnica que utiliza llamadas telefónicas para engañar a la víctima; ej.: Felicitarlo por haber sido favorecido en un sorteo, o el crédito pre-aprobado en el banco X.

Pero existe una modalidad más peligrosa: el Swatting:

Consiste en hacer una llamada telefónica a las autoridades (Policía) haciendo creer que una persona (esposo, esposa, etc.) está armada y que la vida de quien llama está en peligro en ese momento.

Se orquesta un pretexting completo para generar una respuesta armada letal a esta llamada.

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Pretexting

El atacante crea y utiliza un escenario falso, tratando de hacerlo creíble con el objetivo de convencer a la víctima de que revele información o realice una acción.

Normalmente el ciberdelincuente ha recabado información previamente, la cual le es útil para fijar puntos de confianza.

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Fuzzing

Consiste en sobrecargar a la víctima con información, de manera tal que le resulte más fácil aceptar términos que normalmente no aceptaría, con tal de evitar la pérdida de tiempo o el leer 40 paginas de ”acuerdos de uso” de determinado servicio o aplicación.

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Smishing

Phishing por medio de mensajes SMS que se complementan con una url en el mensaje para hacer click sobre ella, solicitar una llamada Telefónica, etc.

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Fake News – Noticias Falsas

La creación de noticias falsas que comienzan a circular como rumores y luego el imaginario colectivo les da valor de ciertas;

Ej. Código de Transito-> Extintor

De otra forma, algunas empresas o personas sin escrúpulos se prestan para hablar bien o mal de algún tema en específico; las personas leen estas reseñas y se va generando el efecto ”bola de nieve” de forma positiva o negativa.

Ej. “Ex agente de la CIA anuncia una debacle económica en Colombia”

https://www.google.com/search?client=firefox-b-d&q=agente+cia+predice

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Ingeniería Social Inversa

El Atacante crea un desperfecto o lo simula y luego aparece para brindar “ayuda”

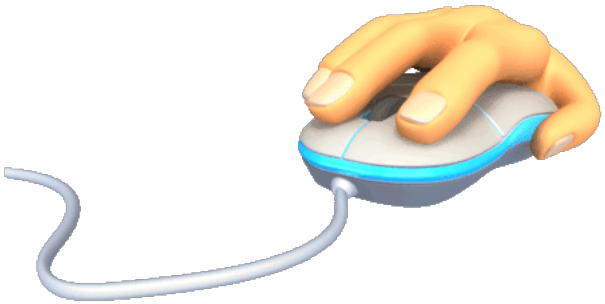
Ej: Persona uniformada con una planilla en la mano, diciendo que viene a “reparar”
El Internet;

O la llamada telefónica de “Soporte” ofreciendo mejorar la velocidad de nuestro computador.

Ataques Avanzados de Hoy y Mañana

@davidpereiracib

Click Sintético



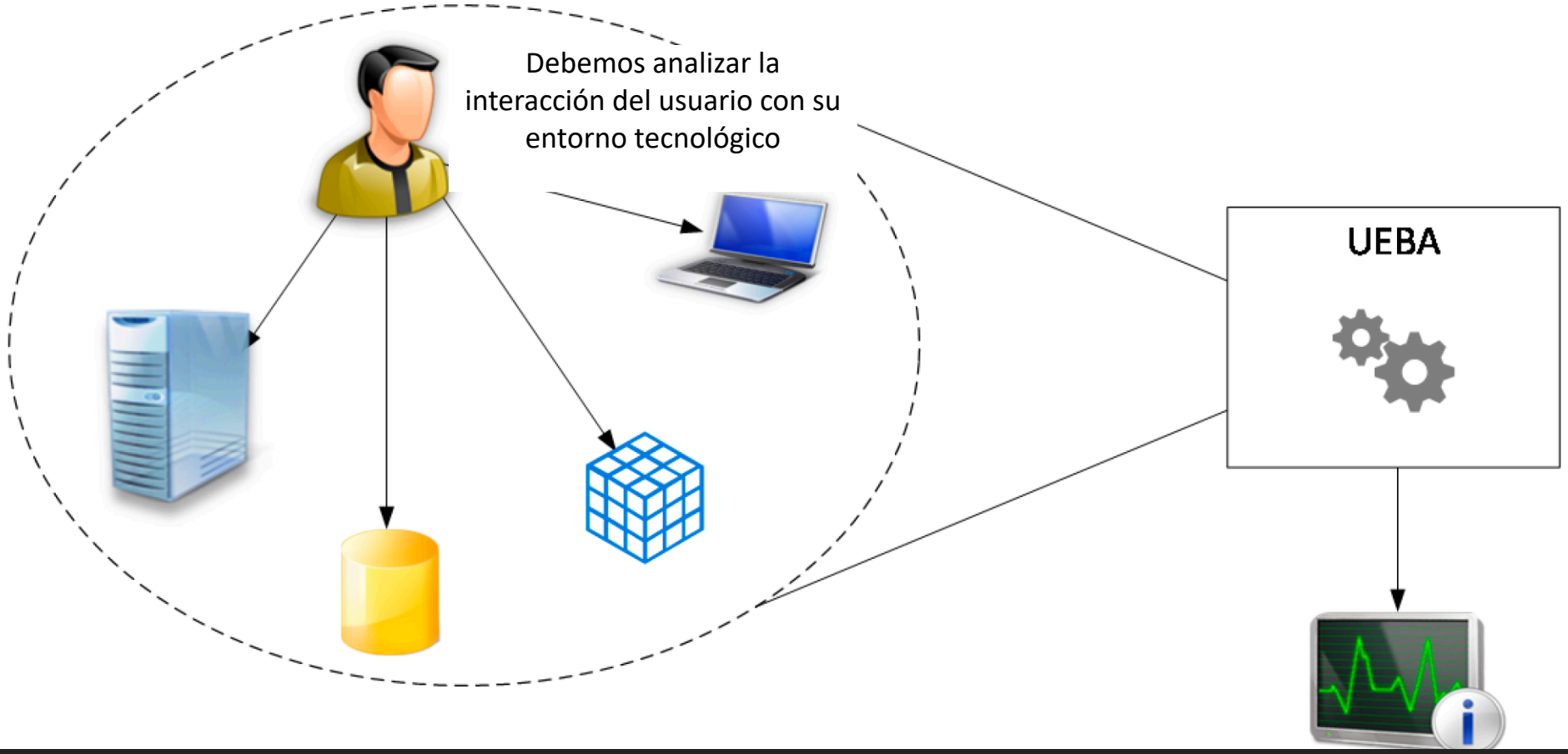
El atacante ejecuta un código en un sitio web con el objetivo de obligar al mouse a realizar click en algún lugar en específico sin la intervención del usuario;

Utilizado para desactivar alertas, aceptar instalaciones, etc.

Si el Usuario cayó.....

@davidpereiracib

Alternativa: UEBA – User Entity Behavior Analytics / BIOC – Behavior indicator of compromise



Cómo Defendernos?

@davidpereiracib

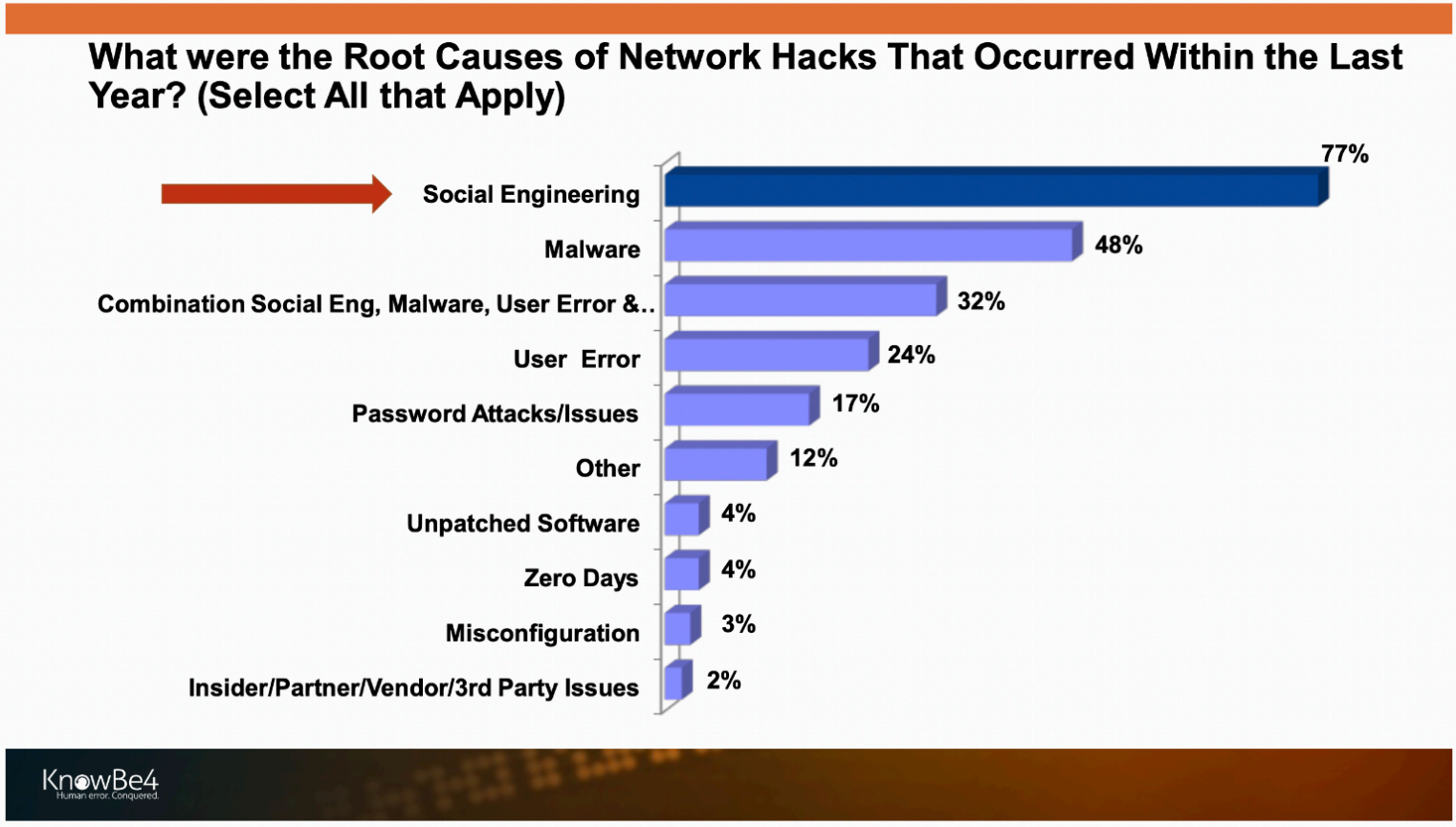
Meta:

RECONOCER LO QUE OCURRE, o las INTENCIONES de nuestro CiberInterlocutor

Personas: La Primera Línea de Ciberdefensa

@davidpereiracib

Exhibit 1. **A 77% Majority of Firms Cite Social Engineering as Top Cause of Security Breaches**



Source: KnowBe4 October 2018

Recomendación:

@davidpereiracib

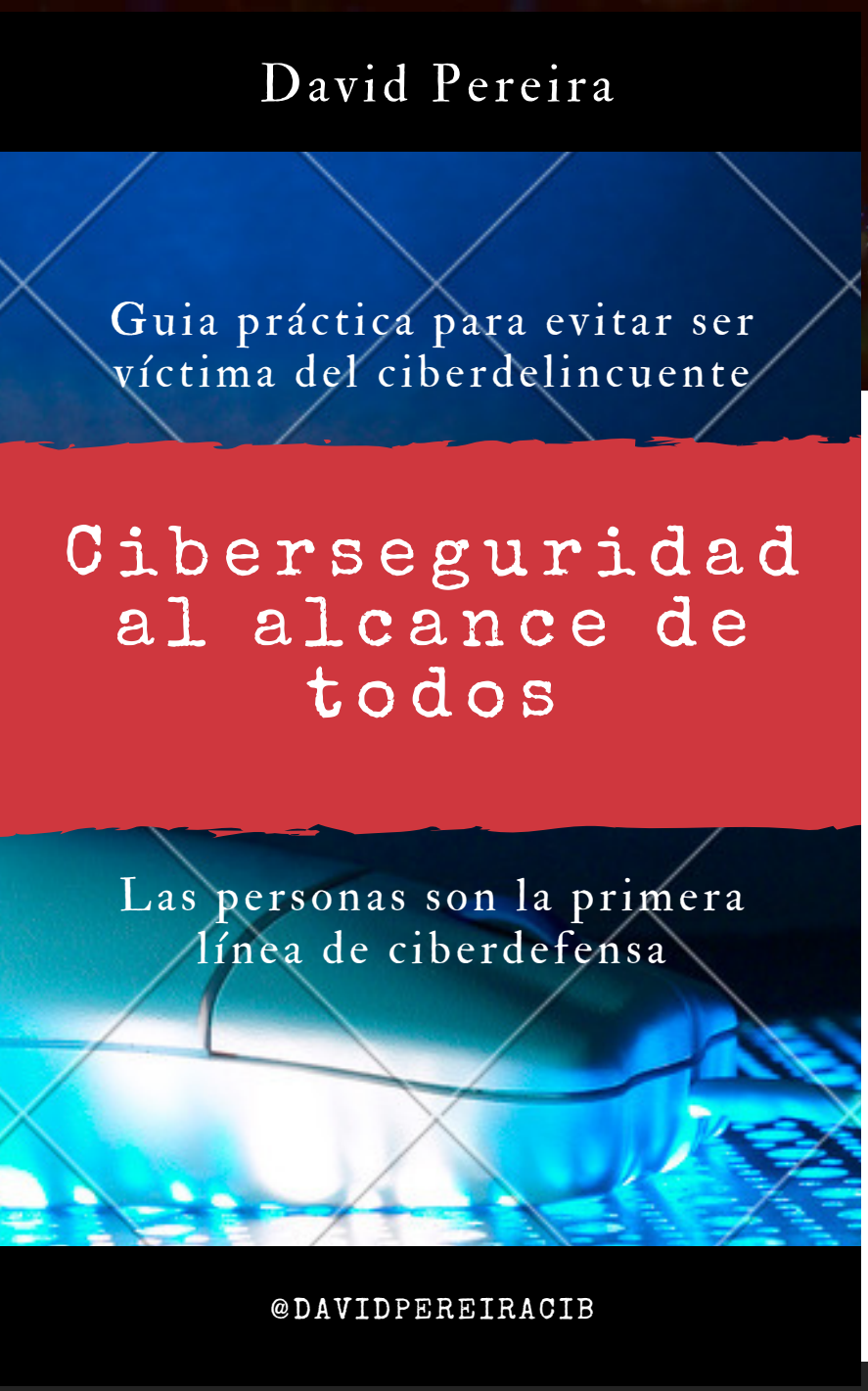
Concientizar y Capacitar:

”Un usuario concientizado es un eslabón que se vuelve fuerte en la cadena de ciberseguridad de la compañía o entidad”

“Un usuario capacitado, es la primera línea de ciberdefensa que deberíamos tener en nuestras organizaciones”

David F. Pereira Q.
@davidpreiracib

SecPro
SECURITY PROFESSIONALS



Próximamente en Ebook;

SecPro
SECURITY PROFESSIONALS

Muchas Gracias!!

David Pereira

david.pereira@secpro.org

@davidpereiracib

https://www.youtube.com/user/dfpluc2