PROYECTO FINAL - INFORMATION SECURITY

THE HUMAN ELEMENT AND DEFENSE STRATEGY

A CASE STUDY OF NOTPETYA

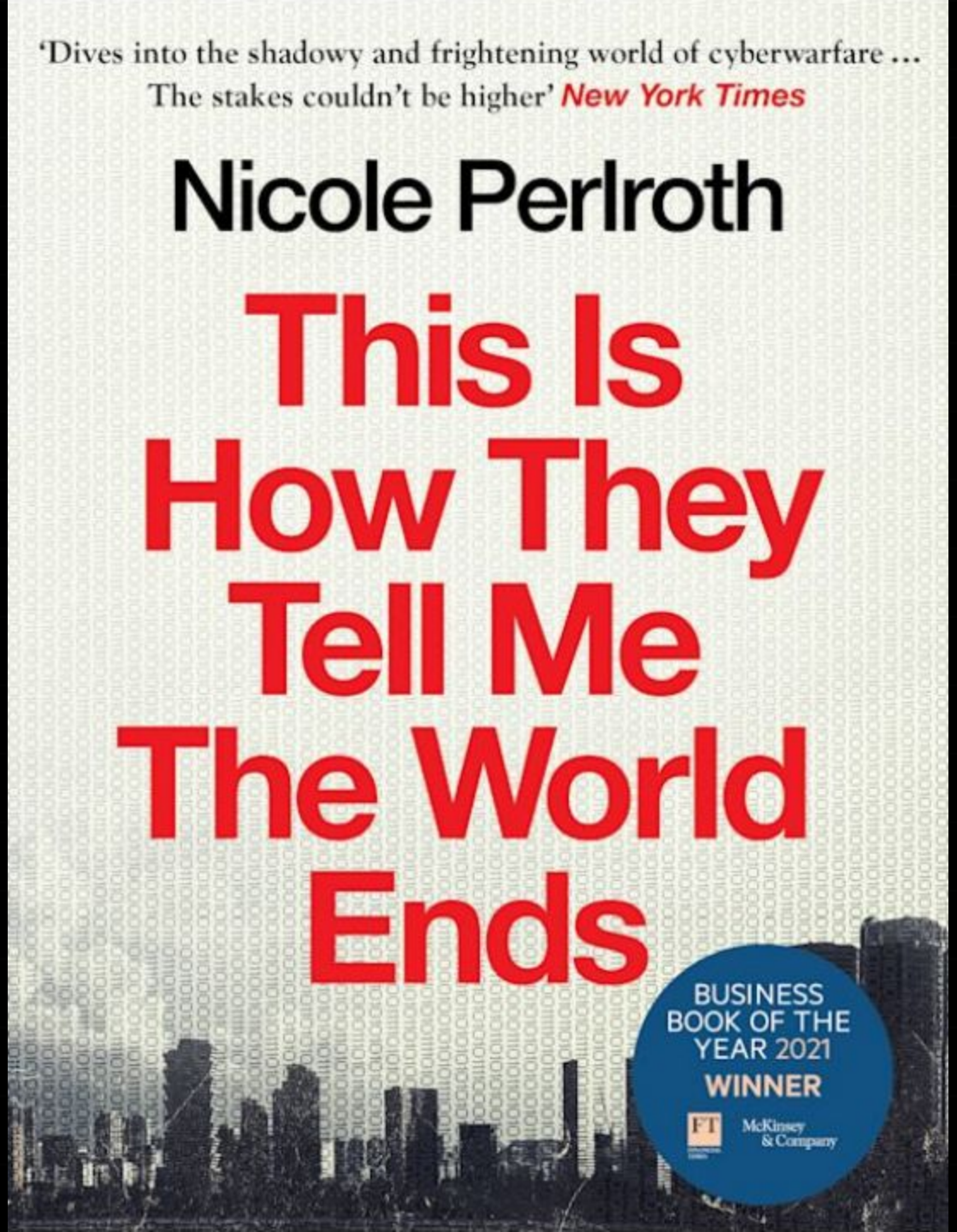
EL NUEVO PODER: DATOS

En tiempos pasados, el poder de un imperio se medía por la cantidad de soldados o misiles. **Hoy, ese poder se mide en datos.**

Quienes tienen acceso a información crítica pueden adelantarse, espiar o sabotear sin ser detectados. El verdadero peligro no es solo perder datos, sino no saber que han sido robados.

Este informe analiza tres ejes centrales del libro *"This Is How They Tell Me the World Ends"* de Nicole Perlroth:

- El ataque **NotPetya** como caso de estudio central.
- La crítica **escasez de talento** en ciberseguridad defensiva.
- La urgente necesidad de priorizar la **defensa digital** sobre la ofensiva.



1. INTRODUCCIÓN

El factor humano y la interconexión digital.

EL ELEMENTO HUMANO

EL ESLABÓN MÁS DÉBIL

La autora subraya que el factor humano es el punto crítico de la cadena de seguridad. Errores mínimos, clics indebidos y negligencia pueden tener consecuencias globales.

CULTURA DE INMEDIATEZ

Una cultura organizacional que favorece la rapidez y la comodidad sobre la seguridad suele dejar la protección en segundo plano, abriendo puertas invisibles al enemigo.

LA DISPARIDAD ESTRUCTURAL

Mientras la defensa ha sido dejada atrás, la **ofensiva** ha recibido fondos, incentivos y prestigio.

Esta dinámica ha generado vulnerabilidades estructurales que actores como Rusia, China o Irán han sabido aprovechar para desestabilizar infraestructuras críticas globales.

> *"No basta con saber atacar: hay que aprender a resistir."*

2. MARCO TEÓRICO

Conceptos clave para entender la ciberguerra moderna.

ZERO-DAYS Y CIBERARMAS

Zero-day: Fallo de software desconocido por el fabricante. No existe parche para corregirlo.

Su alto valor radica en que permiten acceder a sistemas altamente protegidos sin dejar rastro, convirtiéndose en herramientas estratégicas de espionaje y guerra.

EL MERCADO GRIS

DE AFICIONADOS A MERCENARIOS

Perlroth describe un mercado global multimillonario donde gobiernos y actores privados compran y venden estas vulnerabilidades.

La acumulación de estas ciberarmas representa un riesgo enorme si se filtran, como ocurrió con los exploits de la NSA usados en NotPetya.

TTPS (TACTICS, TECHNIQUES & PROCEDURES)

Las TTPs explican cómo se ejecuta un ataque, desde la intrusión hasta el impacto. Comprenderlas es clave para modelos de defensa como `MITRE ATT&CK`.

INTRUSIÓN

Explotación de vulnerabilidades o credenciales robadas.

MOVIMIENTO LATERAL

Uso de herramientas como PsExec y WMI para expandirse.

IMPACTO

Destrucción de datos, encriptación o exfiltración.

INFRAESTRUCTURA CRÍTICA

FRAGILIDAD SISTÉMICA

Servicios esenciales como energía, salud y logística dependen de sistemas digitales con fallas históricas y escasa inversión en defensa.

La interconexión agrava los riesgos: una falla local en un proveedor menor puede escalar a una crisis internacional en minutos.

FACTORES HUMANOS

Muchas de las fallas críticas no son técnicas, sino humanas:

- Malas prácticas operativas (reutilización de contraseñas).
- Falta de segmentación de redes.
- Políticas como NOBUS ("Nobody But Us") que retienen vulnerabilidades en lugar de reportarlas para su corrección.
- Entornos corporativos donde se privilegia la velocidad.

3. CASO DE ESTUDIO: NOTPETYA

El ciberataque más destructivo de la historia.

CONTEXTO GEOPOLÍTICO

NotPetya surgió en un momento de alta tensión entre Ucrania y Rusia. Ucrania se convirtió en un "paisaje infernal de pruebas digital" para el Kremlin.

Antes de NotPetya, Rusia ya había ejecutado ataques contra la red eléctrica ucraniana (2015, 2016) como parte de una estrategia de guerra híbrida.

EL VECTOR: M.E.DOC

EL CABALLO DE TROYA

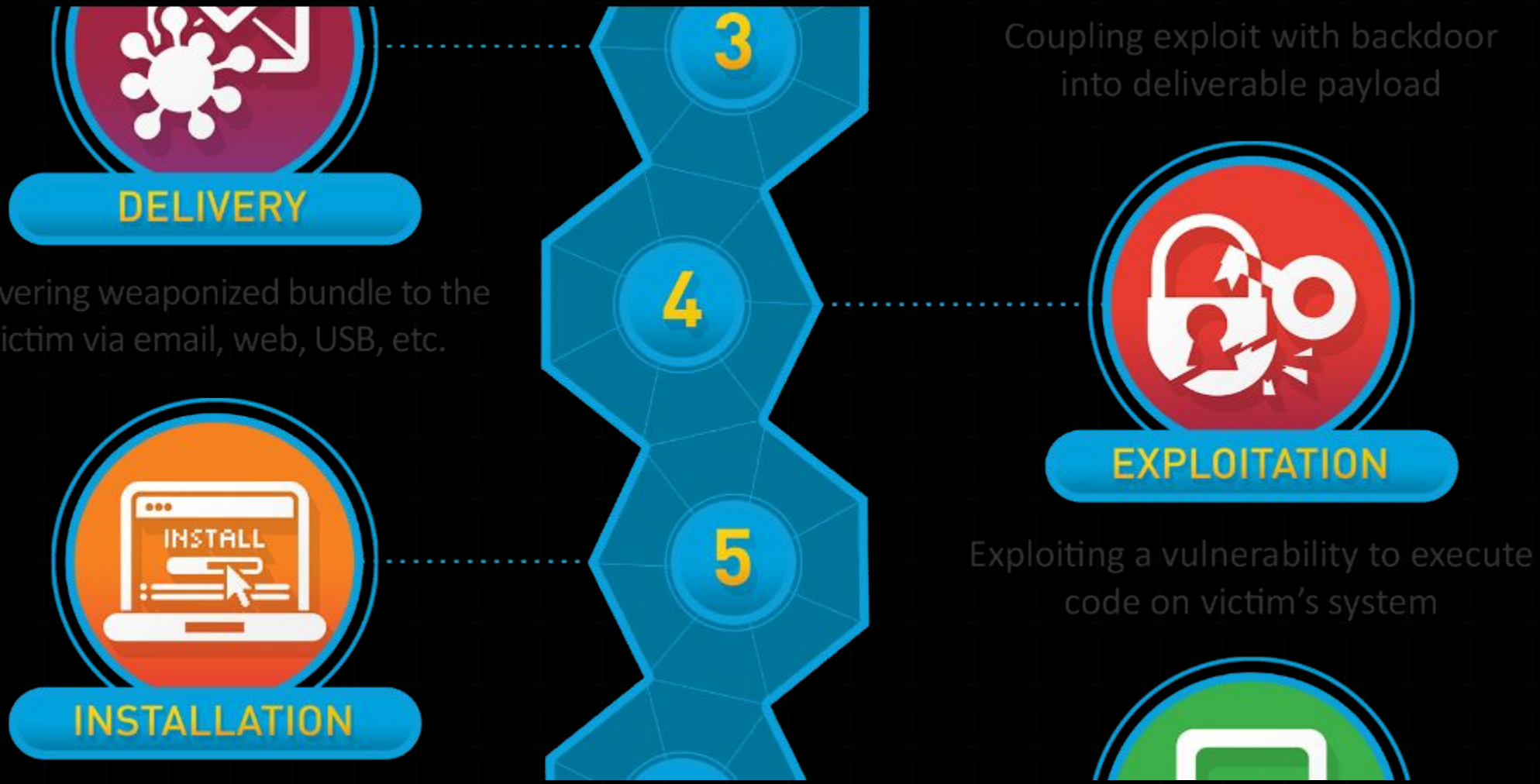
M.E.Doc era el software tributario estándar en Ucrania, utilizado por casi todas las empresas.

Los atacantes comprometieron los servidores de actualización de Linkos Group (creador de M.E.Doc) para distribuir una actualización maliciosa.

CONFIANZA COMPROMETIDA

Bastó con que un solo empleado instalara la actualización legítima para abrir las puertas. La confianza en un proveedor esencial convirtió una debilidad puntual en un desastre nacional.

CADENA DE ATAQUE (KILL CHAIN)



Acceso Inicial (M.E.Doc) → Ejecución → Movimiento Lateral (EternalBlue/Mimikatz) → Impacto (Wiper)

TTP: ETERNALBLUE & ETERNALROMANCE

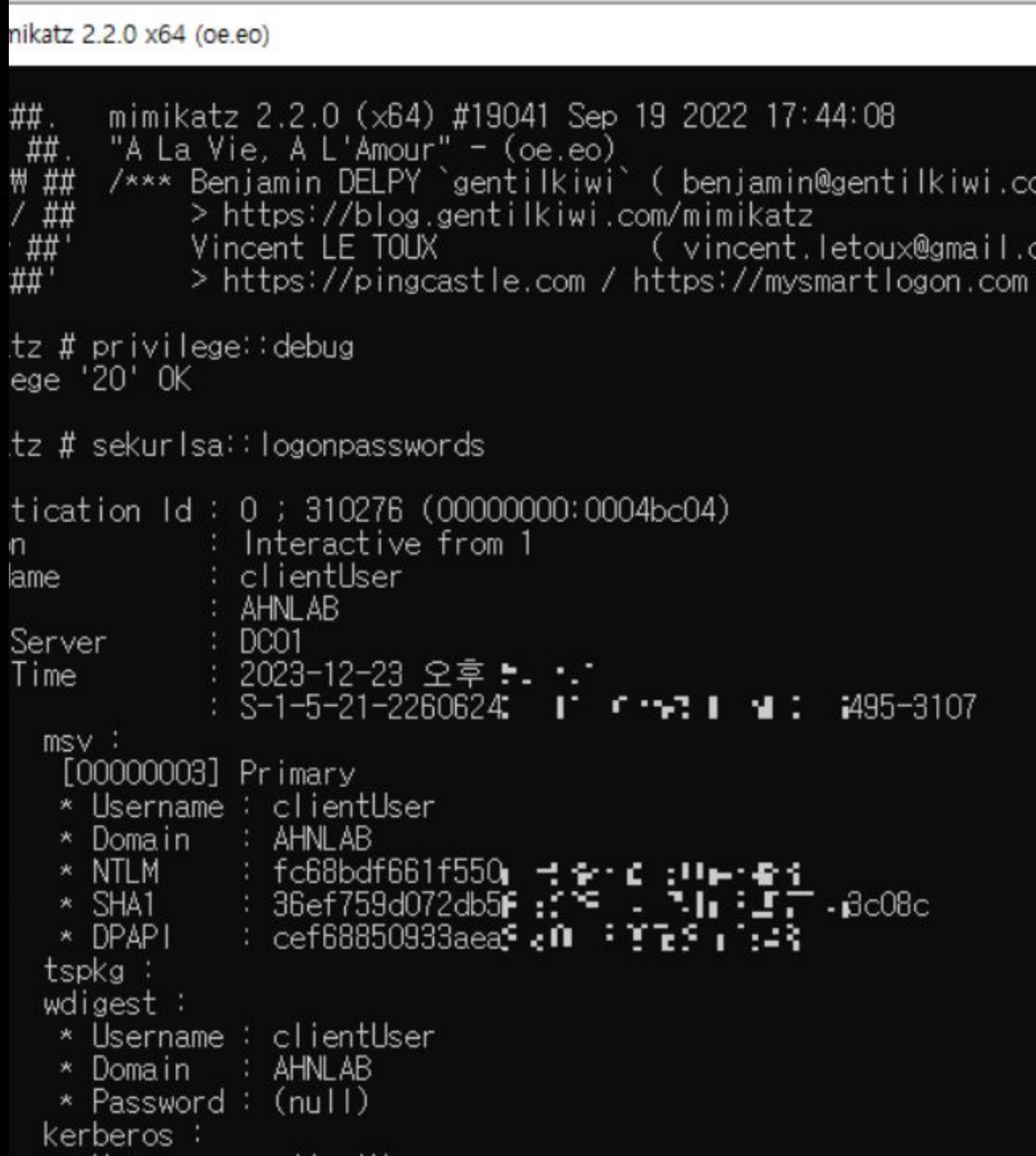
ARMAS DE LA NSA

Estos exploits aprovechaban vulnerabilidades en el protocolo SMB de Windows. Fueron desarrollados por la NSA y robados/filtrados por el grupo *Shadow Brokers*. Permitían la ejecución remota de código sin necesidad de que el usuario hiciera clic en nada, facilitando una propagación automática y veloz.

TTP: MIMIKATZ

Herramienta utilizada para extraer credenciales en texto claro directamente de la memoria del sistema.

Una vez que NotPetya infectaba una máquina de administrador, usaba Mimikatz para robar sus contraseñas y acceder a cualquier otro equipo de la red, incluso aquellos que ya estaban parchados contra EternalBlue.



WIPER, NO RANSOMWARE

> *La nota de rescate era solo una fachada; el verdadero objetivo era borrar datos.*

Análisis Forense

Aunque simulaba pedir un rescate, la encriptación dañaba la Tabla Maestra de Archivos (MFT) de forma irreversible. El propósito no era el dinero, sino la destrucción total y la parálisis de la infraestructura ucraniana.

IMPACTO EN UCRANIA

Los efectos fueron inmediatos y devastadores, paralizando sectores críticos:

BANCA

Cajeros automáticos y transferencias fuera de línea.

TRANSPORTE

Trenes, aeropuertos y servicio postal detenidos.

ENERGÍA

Sistemas de monitoreo de radiación en Chernóbil afectados.

IMPACTO GLOBAL: MAERSK

El gigante naviero, responsable de casi el 20% del comercio mundial, quedó paralizado.

Sus sistemas portuarios y logísticos se apagaron. Camiones hicieron filas kilométricas en los puertos y barcos quedaron varados sin saber qué carga llevaban. La reconstrucción de su red fue una hazaña titánica.

OTRAS VÍCTIMAS GLOBALES

MERCK & PFIZER

Interrupción masiva en la producción y distribución de medicamentos. Merck reportó pérdidas de cientos de millones debido a la detención de la fabricación.

FEDEX (TNT EXPRESS)

La subsidiaria europea TNT Express vio sus operaciones logísticas congeladas, resultando en pérdidas millonarias y retrasos globales en envíos.

COSTO FINANCIERO TOTAL

$10 Mil Millones

Estimación de pérdidas económicas globales

NotPetya demostró cómo un ataque dirigido a una nación puede causar daños colaterales masivos a la economía mundial.

FALLAS ESTRUCTURALES

- **Monocultivo Tecnológico**: Dependencia total de un solo software (M.E.Doc).
- **Parches no aplicados**: Microsoft tenía parches para EternalBlue meses antes.
- **Redes Planas**: Falta de segmentación permitió el movimiento lateral sin restricciones.
- **Doctrina NOBUS**: La decisión de la NSA de no reportar EternalBlue permitió que fuera robado y usado en contra de Occidente.

4. BRECHA DE TALENTO

La asimetría entre ataque y defensa.

INCENTIVOS OFENSIVOS

EL DINERO ESTÁ EN EL ATAQUE

- Zero Day Charlie: vendió vulnerabilidad de Linux por $50000 en lugar de regalarla.
- Charlie Miller reveló públicamente la compra de exploits por la NSA.
- "No More Free Bugs": dejar de regalar el trabajo de hackers.
- Brokers como Zerodium: llegaron a ofrecer millones de dólares exploits para iPhone.
- Vulnerabilidades para explotar > Vulnerabilidad para reportar/corregir

FUGA DE CEREBROS

La NSA pierden talento ante contratistas privados y gobiernos extranjeros.

Un exploit de millones de dólares no se compara al salario mensual de un trabajador por buscar apasionadamente fallos.

FORMACIÓN PÚBLICA

Expertos formados con impuestos y recursos estatales.

RECLUTAMIENTO

Atraídos por salarios libres de impuestos en lugares como Abu Dabi (Project Raven).

SERVICIO PRIVADO

Terminan trabajando para intereses extranjeros

CASO: PROJECT RAVEN

Ex-operadores de la NSA fueron contratados por la empresa **DarkMatter** en EAU bajo la premisa de defensa.

"Purple briefing" fachada de defender a EAU de ciberataques

La realidad operativa ("black briefing") implicaba usar sus habilidades para espiar a desertores, rivales geopolíticos y hasta ciudadanos estadounidenses.

CRISIS EN LA CONTRATACIÓN DEFENSIVA

AGENCIAS CIVILES

Luchan por captar talento para proteger infraestructura crítica. No pueden competir con los salarios ni con la "mística" de las agencias de espionaje.

EL ATRACTIVO DE LA OFENSA

Es más tentador ir a donde están los "juguetes nuevos" (exploits ofensivos) en lugar de trabajos donde deben parchear sistemas obsoletos y lidiar con burocracia.

MERCADO GRIS

La venta de exploits y zero days se encuentra en la delgada franja entre lo legal e ilegal, técnicamente no es ético realizarlo pero tampoco existen normativas ni leyes que prohíban esta divulgación de información.

La monetización de vulnerabilidades ha permitido que actores no estatales o países con menos recursos accedan a capacidades ofensivas de alto nivel (NSO Group y Pegasus).

La necesidad apremia actividades ilegales y poco éticas (armas, drogas) -> Ejemplo en ciberseguridad "Cyber Gauchos" en Argentina tiene fuertes incentivos para vender sus hallazgos al mercado gris internacional en lugar de fortalecer la industria local.

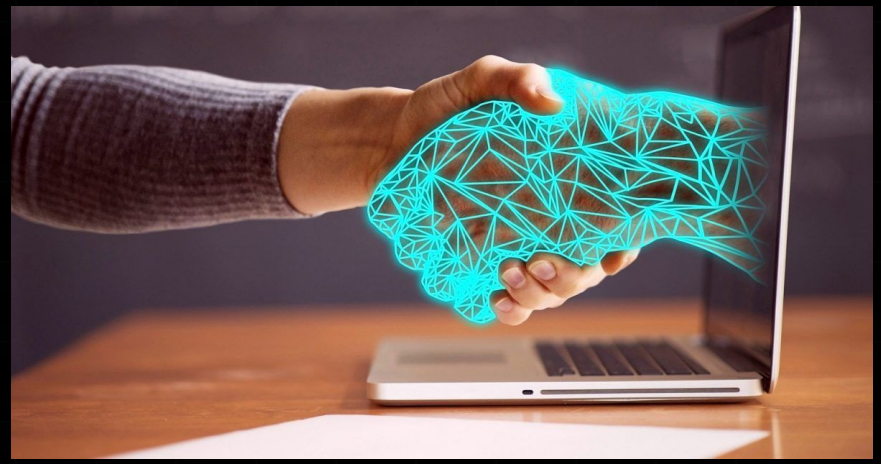
NO HAY SOLUCIÓN FINAL PERO SI PARCIALES...

Hay que combatir fuego con fuego

No todos tienen precio económico

Legalizar el hacking

Ética y normativas



5. ESTRATEGIAS DE MITIGACIÓN

Cómo defenderse ante lo inevitable.

1. PARCHEO MS17-010

La mitigación más básica y efectiva.

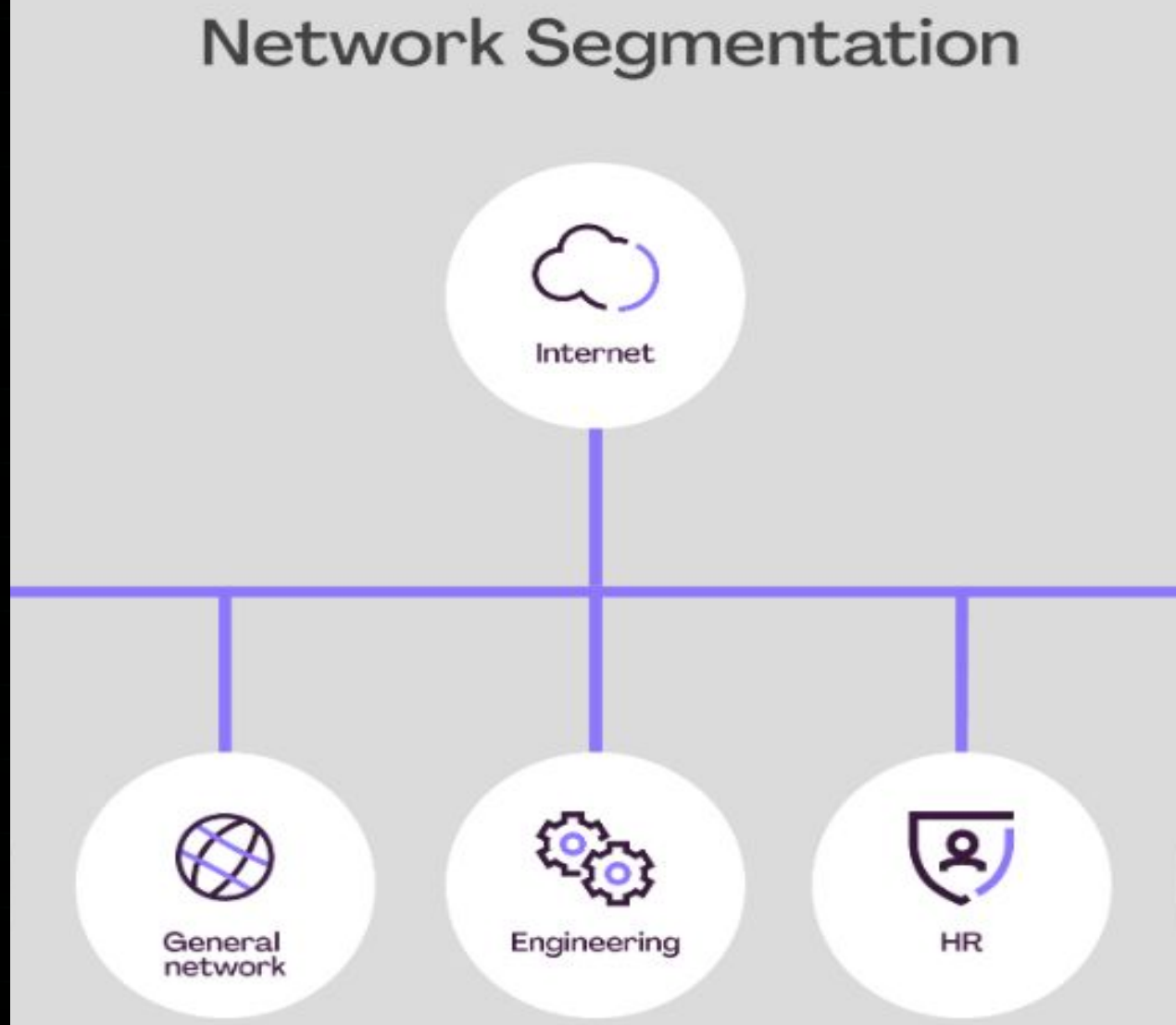
El exploit EternalBlue ya había sido parchado por Microsoft tres meses antes de NotPetya. La presencia de sistemas heredados y la falta de procesos de actualización rigurosos permitieron el desastre.

```
> Update-Mgmt: Critical Priority
```

2. SEGMENTACIÓN DE RED

La arquitectura plana es el mejor amigo del ransomware.

Firewalls internos y microsegmentación habrían limitado la catástrofe a un dominio local, impidiendo que una infección en Ucrania apagara servidores en Estados Unidos o Dinamarca.



3. MFA & HIGIENE DE CREDENCIALES

CONTRA MIMIKATZ

Mimikatz fue devastador porque muchas cuentas administrativas residían en memoria. Restringir privilegios y evitar logins de administradores de dominio en equipos inseguros es vital.

AUTENTICACIÓN ROBUSTA

El uso de MFA para accesos privilegiados y movimientos laterales habría frenado la expansión automática.

4. RESPALDOS "AIR-GAPPED"

La única defensa real contra un "wiper" destructivo.

Maersk se salvó gracias a un controlador de dominio en Ghana que estaba **apagado por accidente** durante el ataque.

Las organizaciones deben tener copias de seguridad fuera de línea, inalcanzables para el malware que recorre la red.

RESILIENCIA: LA LECCIÓN DE MAERSK

EL PEOR CASO

Las arquitecturas deben diseñarse asumiendo el fallo catastrófico total. La posibilidad de perder todos los controladores de dominio simultáneamente debe ser parte del modelo de amenazas.

INDEPENDENCIA

Operaciones críticas (facturación, logística) deben poder funcionar temporalmente de forma aislada sin depender de la infraestructura central global.

PLANES ALTERNOS (ANALÓGICOS)

Cuando la tecnología falla, lo humano prevalece.

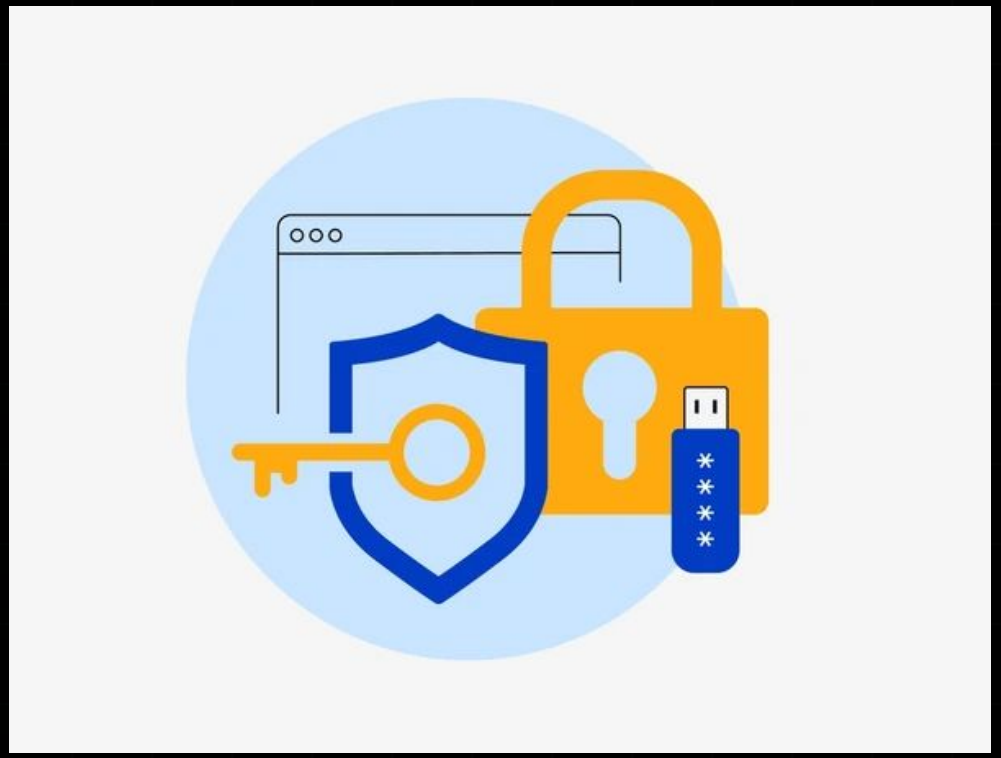
Durante el apagón de Maersk, el uso de WhatsApp personal, pizarras físicas y procesos manuales permitieron mover algo de carga.

Es vital tener canales de comunicación preestablecidos para coordinar cuando la red corporativa está muerta.

SEGURIDAD ES GOBERNANZA

La lección final es que la seguridad no es solo un problema de TI.

- Incentivos alineados con la seguridad, no solo la velocidad.
- Responsabilidad a nivel directivo (C-Level).
- Auditorías reales, no solo de cumplimiento ("Check-box").
- Cultura interna que reporte errores sin miedo.



6. PRIORIDAD DEFENSIVA CRÍTICA

EL PROBLEMA DE FONDO: NOBUS

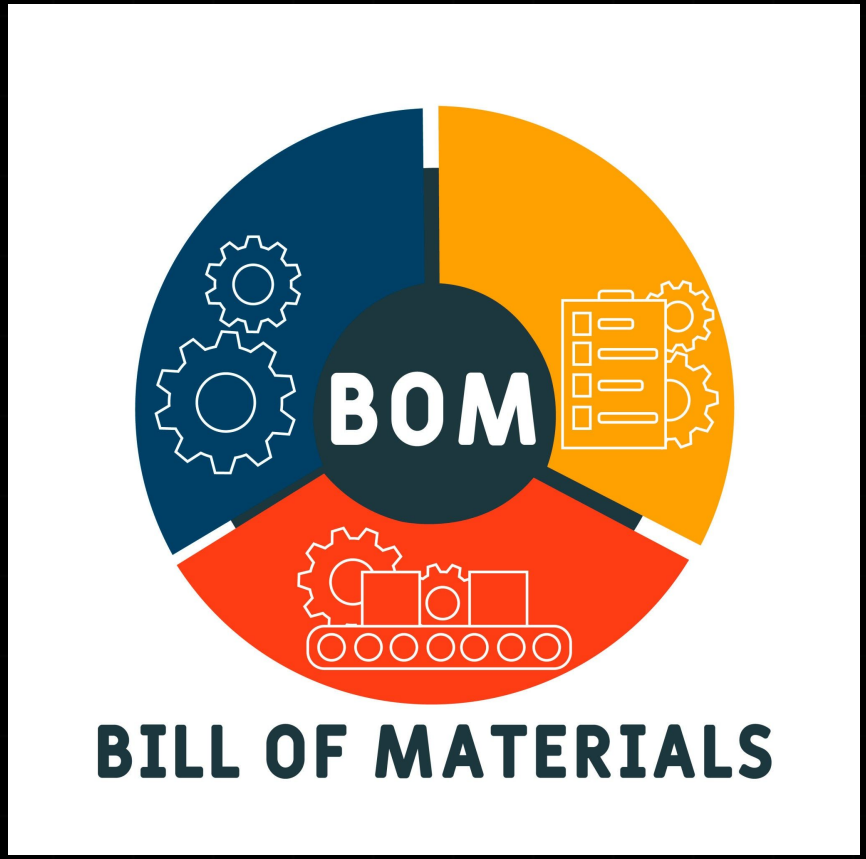
- ¿Qué era NOBUS? La política de la NSA ("Nobody But Us") asumía que EE.UU. podía acaparar vulnerabilidades porque nadie más era lo suficientemente sofisticado para encontrarlas.
- La Realidad Actual: Perlroth demuestra que esta premisa es falsa y peligrosa.
  - Adversarios (Rusia, China) y cibercriminales ahora tienen acceso a las mismas herramientas.
  - El mercado de exploits se ha democratizado; ya no es un monopolio estadounidense.
- El Resultado: Acaparar un zero-day para atacar a un enemigo deja esa misma puerta abierta para que ataquen a nuestros hospitales y redes eléctricas.

PRIORIDAD #1: REFORMA DEL VEP

- Vulnerabilities Equities Process
- El Cambio Necesario: El gobierno debe priorizar la divulgación inmediata de fallos a los fabricantes (Microsoft, Apple, etc.) para que los parcheen, en lugar de guardarlos para espionaje.
- El Caso EternalBlue (NotPetya):
  - La NSA conocía la falla en Windows por 5 años.
  - Si la hubieran reportado antes, NotPetya no habría tenido el vehículo de transmisión para paralizar el comercio global.
- Conclusión: La defensa de la infraestructura propia debe estar por encima de la capacidad ofensiva de inteligencia.

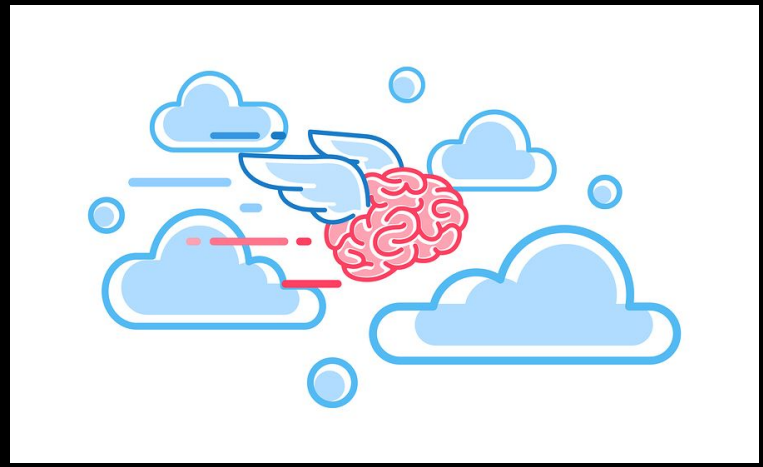
TRANSPARENCIA RADICAL

- El Problema: No sabemos qué código hay dentro de nuestra infraestructura crítica. Usamos software como una "caja negra".
- La Propuesta: Exigir una Lista de Materiales de Ciberseguridad (SBOM).
  - Igual que los alimentos tienen etiquetas nutricionales, el software crítico debe listar sus componentes.
- El Objetivo: Permitir auditorías rápidas. Cuando se descubre una vulnerabilidad, saber exactamente qué hospitales o plantas de energía están en riesgo para protegerlos de inmediato.



LA CRISIS DE TALENTO: FUGA DE CEREBROS Y ÉTICA

- El Problema Económico: La defensa paga menos. Los mejores hackers de la NSA abandonan el servicio público por sueldos millonarios en el sector privado o gobiernos extranjeros (como DarkMatter en los Emiratos Árabes).
- Desensibilización Ética: Se entrena a los ingenieros para ver el código como un "puzzle" matemático, ignorando las consecuencias humanas. Esto crea mercenarios digitales dispuestos a espiar a disidentes o activistas por dinero.
- La Solución:
  - Incentivos: Crear bug bounties nacionales competitivos para que reportar fallos sea rentable.
  - Cultura: Dignificar la defensa y hacer obligatoria la formación ética para evitar la creación de "ciber-mercenarios".



CONCLUSIÓN: EL EFECTO BUMERÁN

- Lección de NotPetya: En un mundo interconectado, las ciberarmas regresan para golpearnos.
- La ciberseguridad no es abstracta; son ambulancias desviadas, puertos cerrados y datos médicos perdidos.
- Debemos cambiar la mentalidad de "Atacar Primero" a "Resistir Mejor". La seguridad debe ser parte del diseño (Code Security), no un parche posterior.

¿PREGUNTAS?

Gracias por su atención.

Grupo 3

GRUPO 3 - INTEGRANTES

TANDAZO COBO, XAVIER

0021243

1

HERRERA CARRIÓN, PABLO ANDRÉS

00326431

CANTOS RIERA, PAULO SEBASTIAN

00326682

LÓPEZ ORTIZ, ERICSON DANIEL

00326945

Universidad San Francisco de Quito

4/12/2025