

GROUP 1:

THE ECONOMICS AND ETHICS

OF THE ZERO-DAY MARKET

INTEGRANTES:

Anahí Andrade, Andrez De La Cruz, Roberth Lara y Mateo Salgado.

¿QUÉ ES UN ZERO-DAY?



Un **zero-day** es una vulnerabilidad desconocida por el fabricante y sin parche disponible. Su nombre proviene del día cero, indicando que no hay defensa posible.

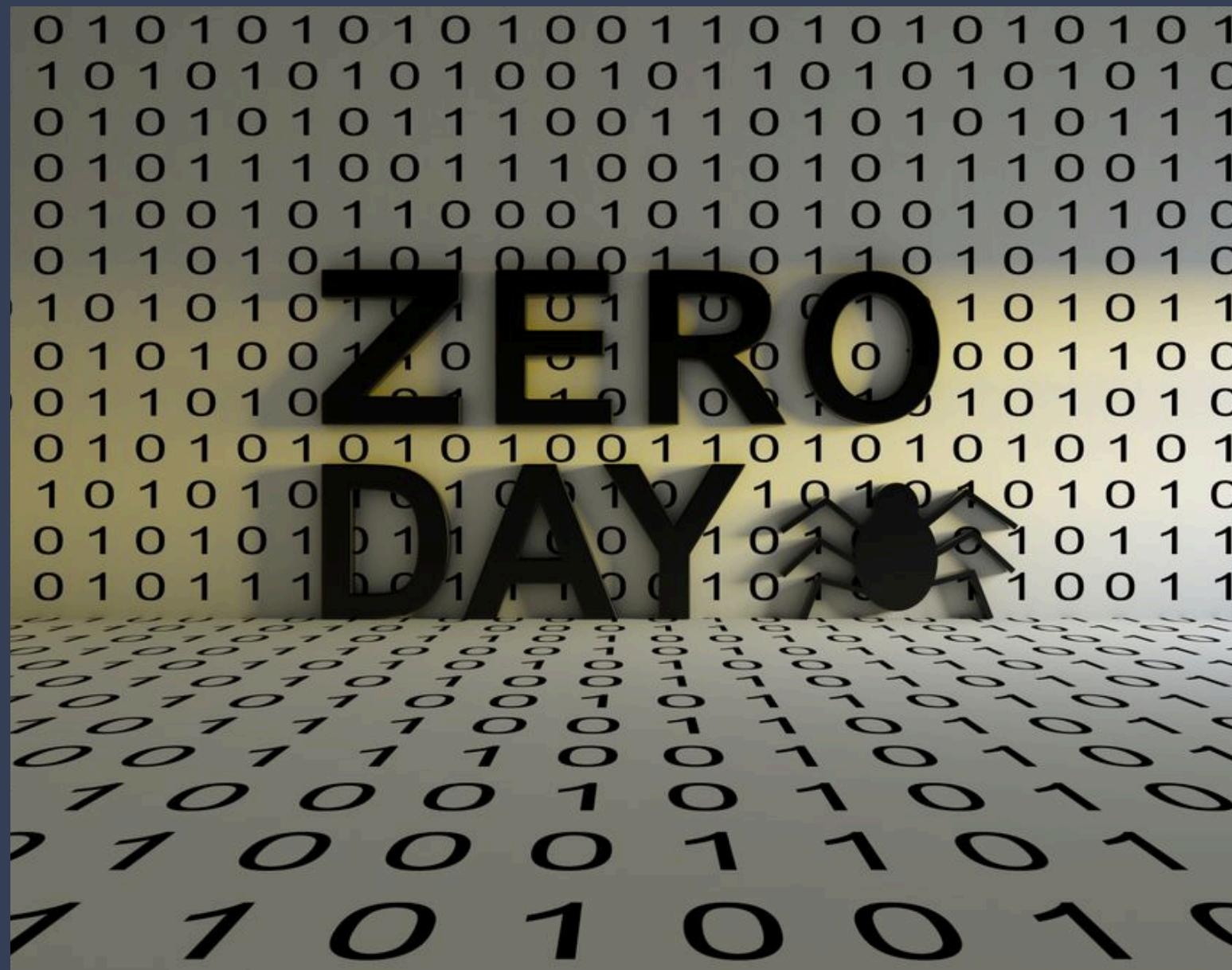
Características:

- Permite intrusión silenciosa.
- Evade antivirus y defensas.
- Alto valor ofensivo.
- Se explota antes de que el público lo conozca.

Nicole Perlroth investigó durante años el mercado global de zero-days, revelando:

- Un ecosistema dominado por gobiernos, empresas privadas y mercenarios.
- Ausencia total de regulación.
- Incentivos económicos enormes para la compra clandestina.
- Riesgos globales producto del almacenamiento stockpile.

¿QUÉ ES UN ZERO-DAY?



- Los zero-days dejaron de ser fallos técnicos aislados.
- Hoy forman parte de una industria armamentista global, opaca y altamente lucrativa.
- Participan hackers independientes, brokers, empresas de spyware, contratistas de defensa y agencias de inteligencia como la NSA y el BSI alemán.
- El libro muestra cómo estas vulnerabilidades se transforman en armas para espionaje, vigilancia y operaciones encubiertas.

FASE 1: EL DESPERTAR - EL ORIGEN DE LA CARRERA ARMAMENTISTA

- Tras el ataque Operation Aurora contra Google, quedó claro que los ataques ya no eran de aficionados, sino de estados nacionales. Por lo que google reforzó su infraestructura, desarrolló fuzzing masivo e incrementó sus bug bounties. Al mismo tiempo, agencias de inteligencia comenzaron a acumular zero-days en lugar de reportarlos.
- Este choque entre parchear vs acumular impulsa la carrera de ciberarmas.



FASE 2: EL DILEMA ECONÓMICO DE LOS INVESTIGADORES

IDEFENSE: PAGABA ~100 USD POR VULNERABILIDAD.

MERCADO OFENSIVO: PAGABA MILES O DECENAS DE MILES POR EL MISMO FALLO.

GOOGLE ESCALÓ RECOMPENSAS DESDE CAMISETAS A 1,5 MILLONES USD (ANDROID).

AUN ASÍ, LOS INVESTIGADORES MIGRARON AL MERCADO OFENSIVO POR PRECIOS 10–50 VECES MAYORES.

FASE 3: DE LA ÉTICA AL MERCADO GRIS - EL CASO NETRAGARD



Adriel Desautels / "Cyanide" - Netragard:

- Descubrió un fallo en software de HP en 2002 y tras disputas legales (y apoyo de la EFF), entró al mercado de exploits.
- Vendió su primer zero-day en formato MP3 por \$16.000
- Luego vendió otros por > \$90.000
- iDefense seguía pagando \$100 con un diferencial de precios gigante.
- Netragard exigía:
 - 98 a 99% de éxito,
 - “clean fail” sin rastros,
 - exclusividad pagada al triple.
- Solo vendía a entidades estadounidenses.
- Este modelo sentó las bases para brokers globales más agresivos.

TRANSICIÓN CRUCIAL DEL MERCADO DEFENSIVO AL OFENSIVO

PEN TESTING REALISTA (NETRAGARD)

Primer tramo claro:

Investigador - Broker con filtros éticos - Agencias/contratistas de EE.UU.

- Falsificación de documentos.
- Intrusión física.
- Llaves, tarjetas, acceso a ascensores.
- Infiltración en bancos, casinos, laboratorios.
- “We protect you from people like us”.



FASE 4: GLOBALIZACIÓN DEL MERCADO

Chaouki Bekrar / Vupen:

- Rompió la seguridad de Google Chrome en Pwn2Own (2012), y rechazó el premio porque debía revelar el exploit, declarando que no compartiría su zero-day “ni por 1 millón de dólares”.
- Vendía a:
 - NSA (Estados Unidos)
 - BSI (Alemania)
- Pagos:
 - Bekrar vendía a gobiernos y a la NSA por cifras muy superiores a las recompensas corporativas.



LA CADENA DE SUMINISTRO - INTERMEDIARIOS

Zerodium Offers
\$1.5 Million
Bounty For iOS
Zero Day Exploits



PROBLEM

Este movimiento disparó la carrera de precios.

FASE 5: TRANSPARENCIA DE PRECIOS Y EXPLOSIÓN DEL MERCADO

- Tras la revocación de su licencia de exportación en Europa, Bekrar movió operaciones a Washington D.C.
 - Fundó Zerodium, ubicada en el corazón del mercado ofensivo.
 - Publicó listas de precios, rompiendo la regla de silencio:
 - \$80.000 - Chrome
 - \$100.000 - Android
 - \$500.000 - iPhone (jailbreak remoto)
 - \$1.000.000 (2015) jailbreak remoto iPhone
 - \$1,5 – \$2,5 millones (2020) para exploits zero-click móviles.



FASE 6: WEAPONIZATION - EL CASO HACKING TEAM

"Hacking Team representa el siguiente eslabón: empresas que integran zero-days de brokers en productos de vigilancia llave en mano"

Empresa italiana de spyware.

➤ En 2015, el hacker Phineas Fisher filtró 420 GB de emails, contratos, y código.

➤ Clientes revelados:

- Sudán, Arabia Saudita, EAU, Marruecos, Etiopía, Nigeria, Uzbekistán, Kazajistán, Azerbaiyán, entre otros.

➤ Utilizaban spyware contra periodistas, opositores y activistas.

➤ Hacking Team integraba:

- Zero-days comprados a Vupen.
- Un zero-day de Adobe Flash vendido por Adriel Desautels.

SE FORMÓ UNA CADENA

Investigadores → Brokers (Vupen/Zerodium) → Hacking Team → Gobiernos → Víctimas

CONSECUENCIAS DEL ESCÁNDALO

» **REGULADORES EUROPEOS
RETIRARON:**

- La licencia de exportación de Hacking Team.
- Posteriormente, la licencia de Vupen.

» Descubrir que un exploit de Desautels terminó en un régimen represivo, el cual llevó al cierre voluntario de su negocio.

INCLUSO LOS BROKERS “ÉTICOS” PERDIERON CONTROL SOBRE EL USO FINAL.

FASE 7: EL MERCADO MADURO - NSO COMO ESTÁNDAR

EL PUNTO FINAL DE LA CADENA

VENTA

En 2014, vendido parcialmente a Francisco Partners (~\$120 millones).

PRODUCTO PRINCIPAL: PEGASUS

- Infecta iPhone, Android, BlackBerry, Symbian.
- Versiones modernas: zero-click (sin interacción).

Uso por autoridades mexicanas para espiar periodistas, activistas anticorrupción y defensores de DD.HH.

FUNDADORES: SHALEV HULIO Y OMRI LAVIE, CON VÍNCULOS A UNIDAD 8200.

CADENA DE SUMINISTRO COMPLETA

Ahora que hemos visto los actores individuales, veamos cómo se conecta todo el sistema:

DESCUBRIMIENTO

- INVESTIGADORES INDEPENDIENTES O EQUIPOS INTERNOS (NETRAGARD, VUPEN, NSO).

VALUACIÓN

- FIABILIDAD, ALCANCE, PERSISTENCIA, INTERACCIÓN, DETECTABILIDAD.

INTERMEDIACIÓN

- BROKERS (VUPEN/ZERODIUM, NETRAGARD, ETC).
- COMISIONES DE 3 % A 60 %.
- REVENTA A AGENCIAS COMO NSA, BSI, CIA.

WEAPONIZATION

- INTEGRACIÓN EN PLATAFORMAS OFENSIVAS O SPYWARE (HACKING TEAM, PEGASUS).

OPERACIÓN

- DESPLIEGUE POR GOBIERNOS: EEUU, EUROPA, MÉXICO, EAU, SUDÁN, ETIOPÍA, ETC.

RIESGO SISTÉMICO

- TODO EL MUNDO QUEDA VULNERABLE MIENTRAS NO EXISTA UN PARCHE.

Esta cadena tiene múltiples puntos de fallo, como veremos a continuación.

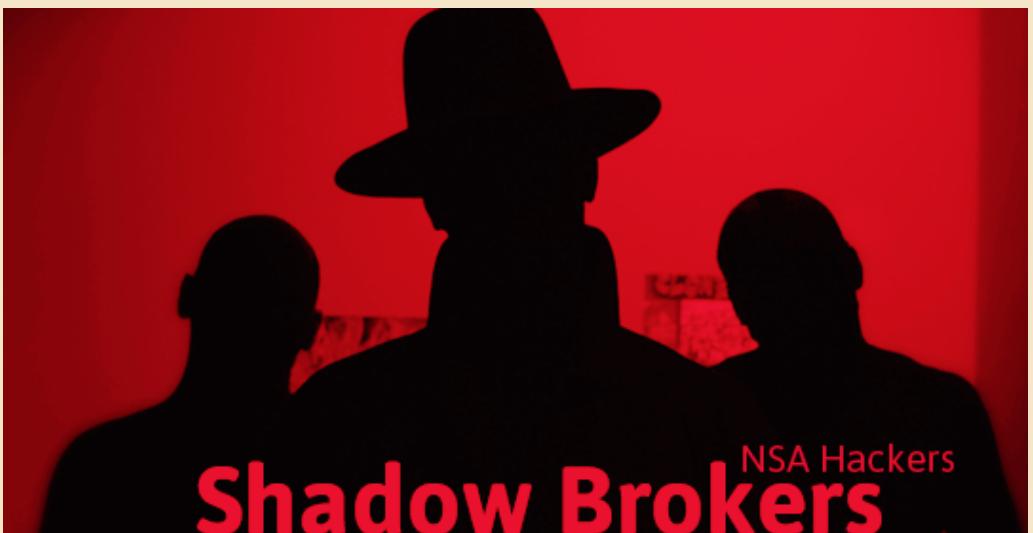
FALLO TIPO 1: CORRUPCIÓN INTERNA

Ejemplo de corrupción en la cadena (Ejemplo de cyber shatner)

➤ HACKERS VETERANOS DENUNCIARON:

- Contratistas que revendían exploits con márgenes x10.
- Empresas que rechazaban exploits, luego los usaban sin pagar.
- Sustitución de personal en defensa por programadores rusos más baratos.
- Resultado: Puertas traseras rusas infiltradas en sistemas críticos del Pentágono.

LA CADENA COMPLETA Y SUS FALLAS



El caso más grave de pérdida de control

FALLO TIPO 2: COLAPSO SISTÉMICO

- WannaCry, basado en EternalBlue, una herramienta robada de la NSA.
- NotPetya, considerado el ciberataque más destructivo de la historia, daños por > \$10.000 millones que afectó a:
 - Maersk
 - FedEx
 - Merck (farmacéutica)
 - Bancos ucranianos
 - Ministerios de gobierno

No solo los dictadores o empresas corruptas pierden control de su spyware.

Incluso la agencia más avanzada del mundo siendo la NSA perdió el control de sus propias armas. El almacenamiento o “hoarding” de vulnerabilidades sin reportarlas creó una bomba que terminó explotando sobre el planeta entero.

CASO “SHADOW BROKERS”

Cuando las armas digitales de la NSA se volvieron contra el mundo.

➤ ¿Qué pasó en 2016?

- Un grupo misterioso llamado “The Shadow Brokers” robó y filtró parte del arsenal de ciberarmas de la NSA, incluyendo las herramientas de Equation Group, la unidad más secreta “Tailored Access Operations” (TAO).

➤ ¿Qué filtraron?

- Exploits y zero-days extremadamente poderosos, usados durante años en operaciones de inteligencia.
- Incluidos ataques contra:
 - Windows
 - routers Cisco
 - sistemas bancarios
 - infraestructura global

➤ Consecuencia inmediata:

- Grupos criminales y estados hostiles reutilizaron esos mismos zero-days contra:
 - hospitales
 - sistemas de emergencia
 - empresas
 - gobiernos enteros



¿PARCHAR O EXPLOTAR? UN MODELO ECONÓMICO DEL DILEMA ZERO-DAY

EL DILEMA “PATCH VS HOARD”

- Gobiernos compran y desarrollan zero-days en programas ultra secretOS.
- Para que un zero-day sea valioso, debe mantenerse en secreto.
- Parchar → se pierde la capacidad ofensiva
- Acumular → se deja a todo el mundo vulnerable

VARIABLES DEL MODELO

- **V**: valor operativo del exploit para el gobierno
- **P**: probabilidad de que otro actor descubra la vulnerabilidad
- **D**: daño económico esperado si la vulnerabilidad es explotada masivamente
- **C**: costo de parchear para el fabricante
- **R**: costo reputacional/político si se descubre que se acumuló el zero-day

2 ESTRATEGIAS 2 ECUACIONES

PARCHAR:

$$B_{\text{patch}} = -C$$

ACUMULAR:

$$B_{\text{hoard}} = V - (P \cdot D) - R$$

REGLA DE DECISIÓN y COSTO DE OPORTUNIDAD

DECISIÓN SOCIAL:

$$B_{\text{patch}} > B_{\text{hoard}}$$

REORDENANDO:

$$P \cdot D > V + C - R$$

COSTO DE OPORTUNIDAD DE NO PARCHAR:

$$CO_{\text{nopatch}} = P \cdot D + R$$

EJEMPLO RÁPIDO CON NOTPETYA

- **Del libro:**
 - Daños totales de NotPetya > 10 mil millones USD
- **Supongamos:**
 - $D=10\ 000$ D millones
 - $P=5\%$ (probabilidad de que explote algo así en 1–2 años)
 - Daño esperado: $P \cdot D = 500P \cdot D=500$ millones

CONCLUSIÓN DEL MODELO

- El libro muestra que la acumulación de zero-days no es gratis.
- El costo de oportunidad de no parchear puede ser de miles de millones.
- Un modelo simple ayuda a ver que la decisión no es sólo técnica, sino económica y ética

ÉTICA, REGULACIÓN Y POLÍTICA PÚBLICA EN EL MERCADO ZERO-DAY



EL DILEMA ÉTICO: PATCH VS HOARD

Opción 1: HOARD (acumular)

- Se guarda la vulnerabilidad en secreto para operaciones ofensivas.
- Otorga ventaja estratégica temporal.
- Mantiene desprotegidos a todos los usuarios del software afectado.

Opción 2: PATCH (divulgar)

- Se reporta al fabricante.
- Se parchea la vulnerabilidad y se protege a millones de personas.
- Se pierde la ventaja ofensiva inmediata.

¿Qué deben hacer los gobiernos cuando encuentran una vulnerabilidad crítica?

Conflicto Ético

¿Debe un Estado priorizar su capacidad de ataque o la seguridad colectiva?

Mantener en secreto una vulnerabilidad expone a civiles, empresas y servicios esenciales sin su consentimiento.

SHADOW BROKERS Y ETERNALBLUE: UNA LECCIÓN GLOBAL

CÓMO LA ACUMULACIÓN (“HOARD”) PUEDE CONVERTIRSE EN UNA CATÁSTROFE

- La NSA guardó en secreto la vulnerabilidad EternalBlue durante años.
- Fue filtrada por el grupo Shadow Brokers.
- Corea del Norte y Rusia la reutilizaron sin modificar.

SHADOW BROKERS Y ETERNALBLUE: UNA LECCIÓN GLOBAL

CONCLUSIÓN ÉTICA Y TÉCNICA

- La idea de que un Estado puede “controlar” un arsenal digital es falsa.
- Una sola filtración tuvo un impacto global similar al de un desastre natural.

IMPLICACIONES ÉTICAS, SOCIALES Y GEOPOLÍTICAS

› 1. RIESGO SISTÉMICO

- Una vulnerabilidad retenida afecta a toda la infraestructura digital del planeta.
- No distingue entre enemigos, aliados o civiles.

› 2. INCENTIVO PERVERSO

- El mercado premia no reportar vulnerabilidades.
- Se prioriza el espionaje sobre la seguridad ciudadana.

IMPLICACIONES ÉTICAS, SOCIALES Y GEOPOLÍTICAS

› 3. AFECTACIÓN A LA POBLACIÓN CIVIL

- Los mayores perjudicados no son los objetivos militares.
- Son hospitales, servicios básicos, empresas de logística, gobiernos locales.

› 4. ESCALADA SILENCIOSA

- Los estados compiten por arsenales digitales, sin mecanismos de control.
- Se crea una especie de “Guerra Fría cibernética” sin tratados de contención.

POLÍTICA PÚBLICA: LO QUE DEBE CAMBIAR

1. Regulación internacional estricta del mercado zero-day

- Control real de exportaciones de spyware.
- Listas negras globales para jugadores reincidentes.
- Auditorías y trazabilidad obligatoria.

2. Estándar global de divulgación responsable

- Obligación de reportar vulnerabilidades críticas dentro de un plazo definido.
- Comités multilaterales para evaluar riesgos y decidir si se retiene o no.
- Transparencia mínima para evitar abusos.

3. Priorizar defensa sobre ofensiva

- Invertir más en protección que en acumulación de exploits.
- Programas globales de bug bounty.
- Cooperación entre gobiernos y empresas tecnológicas.
- Reforzar infraestructura crítica con parches tempranos.

CONCLUSIÓN: UNA AMENAZA GLOBAL

Un mercado sin regulación es una bomba de tiempo.

- El enfoque de acumular vulnerabilidades sin parcharlas genera riesgos mayores que los beneficios estratégicos.
- Los ataques recientes (WannaCry, NotPetya) demuestran que una sola filtración puede paralizar al mundo.
- La seguridad digital global depende más del parche oportuno que de cualquier capacidad ofensiva.



MENSAJE FINAL

- Regular, divulgar y priorizar la defensa no es idealismo.
- Es la única forma de evitar que el próximo “EternalBlue” cause un daño aún mayor.
- El libro de Perlroth demuestra que la humanidad ya no puede darse el lujo de permitir un mercado zero-day sin supervisión.

GRACIAS

Fuente:

- Perlroth Nicole, This Is How They Tell Me the World Ends: The Cyberweapons Arms Race
<https://owasp.org/www-project-top-ten/>