CLONER

TECNOLOGÍAS EMERGENTES

usadas para el mal: cómo cambió el arsenal del atacante

IA Ofensiva · Identidad Digital · Cadena de Suministro · IoT/OT · Cibercrimen como Servicio · Computación Cuántica

EL NUEVO ARSENAL DEL ATACANTE

6 tecnologías que redefinieron el cibercrimen — y un caso real en cada una

01

IA, Deepfakes y Fraude de Confianza

Caso Arup — $25.6M

02

Robo de Identidad Digital y Abuso de Accesos

Caso Midnight Blizzard vs Microsoft

03

Cadena de Suministro de Software

Caso SolarWinds — 18,000 víctimas

04

IoT, OT y Tecnologías con Impacto Físico

Caso Colonial Pipeline

05

Cibercrimen como industria

Caso LockBit — Operation Cronos

06

Computación Cuántica y Criptografía

Harvest Now, Decrypt Later

01

IA, DEEPFAKES Y FRAUDE DE CONFIANZA

La IA no solo nos hace más productivos a nosotros, sino también a los atacantes

Phishing hiperpersonalizado

Emails multilingües, sin errores, con contexto real del objetivo.

Herramientas maliciosas

WormGPT, FraudGPT: LLMs sin restricciones éticas vendidos como servicio desde $110/mes en la dark web.

Deepfakes de video y voz

Clonación de voz con solo 3 segundos de audio. Videollamadas completas con participantes generados por IA.

+89% de aumento en ataques con IA habilitada (CrowdStrike 2026).

CASO: ARUP (2024) — DEEPFAKE EN VIDEOLLAMADA

U$25.6M

PERDIDOS EN UNA SOLA VIDEOLLAMADA

Arup — Firma de ingeniería británica
Hong Kong, Enero 2024

15 transferencias bancarias
a 5 cuentas controladas
por los atacantes

Fraude descubierto
una semana después

ANATOMÍA DEL ATAQUE

1. **Email del "CFO"**

   Solicita transacción secreta. El empleado sospecha phishing.

2. **Videollamada deepfake**

   Todos los participantes eran recreaciones IA del CFO y colegas reales.

3. **Confianza artificial**

   Caras y voces familiares eliminaron toda sospecha del empleado.

4. **Transferencia ejecutada**

Lección: No se comprometió ningún sistema. El ataque fue 100% ingeniería social potenciada por IA.

02

ROBO DE IDENTIDAD DIGITAL, ABUSO DE ACCESOS Y PERMISOS

El atacante ya no necesita vulnerar sistemas por fuerza. Le basta con abusar de identidades válidas, permisos concedidos y flujos legítimos de autenticación.

Robo de sesiones y tokens

Los tokens OAuth permiten acceso persistente incluso si se cambia la contraseña.

La identidad se convierte en el nuevo perímetro de ataque.

Apps maliciosas con permisos legítimos

Aplicaciones OAuth con consentimiento engañoso obtienen acceso completo a buzones, archivos y directorios.

Movimiento lateral silencioso

El atacante se mueve como un usuario legítimo, invisible para herramientas de detección tradicionales.

CASO: MIDNIGHT BLIZZARD vs MICROSOFT

Enero 2024 — Grupo APT29 (Inteligencia rusa) compromete correos de altos ejecutivos de Microsoft

1	**Password spray**	Comprometen cuenta de prueba sin MFA en tenant legacy de Microsoft.
2	**App OAuth olvidada**	Encuentran app OAuth abandonada con permisos elevados al entorno corporativo.
3	**Escalamiento de privilegios**	Crean apps OAuth maliciosas y asignan rol full_access_as_app a Exchange Online.
4	**Exfiltración silenciosa**	Acceden a buzones de correo de liderazgo senior, equipos legales y de ciberseguridad.

La cuenta comprometida era de prueba, sin MFA y olvidada. Los proxies residenciales ocultaron el origen del ataque durante meses.

03

CADENA DE SUMINISTRO SOFTWARE

Bibliotecas abiertas, paquetes comprometidos, proveedores vulnerables y pipelines de desarrollo expuestos transforman al software en vehículo de ataque.

Software como vehículo

Una sola brecha en un proveedor puede comprometer a miles de organizaciones downstream a través de actualizaciones legítimas.

Confianza como arma

Los atacantes no atacan directamente: penetran al proveedor y viajan dentro de actualizaciones firmadas digitalmente.

Ecosistema expandido

La seguridad ya no termina en los muros de la organización. Cada dependencia de terceros es una superficie de ataque.

CASO: SOLARWINDS — EL ATAQUE MÁS SOFISTICADO DE LA HISTORIA

18,000

empresas descargaron
el malware SUNBURST

14 meses

sin ser detectado

APT29 (Cozy Bear)

Inteligencia rusa (SVR)
Confirmado por EE.UU. y Reino Unido

LÍNEA DE TIEMPO

Sep 2019 — Atacantes acceden al entorno de desarrollo de SolarWinds

Feb 2020 — Inyectan SUNSPOT y SUNBURST en el código fuente de Orion

Mar 2020 — SolarWinds distribuye actualizaciones con el código malicioso

Dic 2020 — FireEye detecta la brecha investigando un incidente propio

Dic 2020 — CISA ordena desconexión inmediata a todas las agencias federales

Víctimas: Departamentos del Tesoro, Estado, Defensa y Seguridad Nacional de EE.UU., más empresas Fortune 500.

04

IoT, OT Y TECNOLOGÍAS CON IMPACTO FÍSICO

La convergencia entre tecnología conectada y operación real exige una visión de ciber resiliencia que va más allá de la seguridad informática tradicional.

Superficie expandida

Sensores, PLC, SCADA, redes industriales y dispositivos edge conectados amplían exponencialmente los vectores de entrada.

De bits a átomos

Un ataque cibernético a sistemas OT/IoT puede detener fábricas, interrumpir servicios esenciales y generar impacto físico real.

IT + OT convergentes

La interconexión entre sistemas informáticos y sistemas operacionales hace que una brecha de ciberseguridad pueda paralizar la operación física.

CASO: COLONIAL PIPELINE (2021) — CUANDO EL MUNDO FÍSICO SE DETIENE

45%

del combustible de la costa este de EE.UU.

$4.4M

pagados en rescate (75 Bitcoin)

5,500

millas de oleoducto paralizado por 6 días

17

estados con declaración de emergencia

¿QUÉ PASÓ?

Vector de entrada

Robo de contraseña sin MFA.

El grupo DarkSide robó 100 GB de datos en 2 horas y desplegó ransomware en los sistemas de facturación.

Impacto en el mundo real

Filas kilométricas en gasolineras. Compras de pánico. Precio de la gasolina al máximo en 6 años. Biden declaró estado de emergencia nacional. 10,600 estaciones sin combustible.

05

CIBERCRIMEN COMO INDUSTRIA

El cibercrimen profesionalizó su modelo: herramientas, accesos, malware y servicios completos pueden comprarse como si fueran parte de una industria.

Ransomware-as-a-Service

El desarrollador crea el malware e infraestructura. Los afiliados ejecutan ataques a cambio de un porcentaje. Un modelo franquicia del crimen.

Barrera técnica eliminada

Ya no se necesita expertise. Herramientas point-and-click, soporte técnico y hasta comunidades para mejorar el malware.

Especialización criminal

Brokers de acceso inicial, lavadores de cripto, negociadores de rescate: cada rol está profesionalizado en el ecosistema.

CASO: LOCKBIT — EL IMPERIO RANSOMWARE

25-30%

de todo el ransomware global en 2023

2,000+

víctimas en todo el mundo

U$ 120M+

extorsionados en pagos de rescate

OPERATION CRONOS — FEBRERO 2024

El takedown

10 países coordinados por NCA (UK) y FBI. 34 servidores incautados. 14,000 cuentas de afiliados bloqueadas. 200+ billeteras crypto congeladas. Claves de descifrado liberadas gratis.

La resurrección

Una semana después, LockBit relanzó operaciones desde nuevos servidores. En 2025 emergió LockBit 5.0 con payloads para Windows, Linux y VMware. El modelo RaaS es resiliente por diseño.

06

COMPUTACIÓN CUÁNTICA Y AMENAZA A LA CRIPTOGRAFÍA

La computación cuántica podría quebrar los esquemas criptográficos actuales, comprometiendo datos, comunicaciones, identidades y firmas digitales.

RSA, ECC y Diffie-Hellman

El algoritmo de Shor factorizaría en horas lo que hoy toma miles de años. Toda la infraestructura de clave pública actual quedaría obsoleta.

Q-Day: ~2030

Expertos estiman que computadoras cuánticas podrán romper la encriptación actual en la próxima década. NIST ya publicó estándares de criptografía post-cuántica.

Solo 4% preparado

Apenas el 4% de las organizaciones tiene una estrategia cuántica definida (ISACA 2025).

CASO: HARVEST NOW, DECRYPT LATER

La amenaza cuántica que ya está ocurriendo hoy

HOY

Recolectar

Intercepción y almacenamiento de tráfico cifrado: datos diplomáticos, financieros, propiedad intelectual, registros médicos. Sin señales de intrusión.

ESPERAR

Almacenar

Los datos se guardan pacientemente durante años o décadas. No hay rescates, no hay disrupciones. El ataque es invisible.

Q-DAY

Descifrar

Con computadores cuánticos suficientemente poderosos, todo lo almacenado se descifra. Datos sensibles quedan expuestos. El daño ya está hecho.

Casos observados: 2016 tráfico canadiense redirigido a China · 2019 tráfico móvil europeo interceptado · 2020 datos de Google, Amazon y 200+ redes redirigidos por Rusia

CONSTRUYENDO CIBER RESILIENCIA

Construir ciber resiliencia no significa sólo poner más seguridad, sino prepararse para resistir, responder y recuperarse cuando ocurra un ataque.

Respaldo inmutable

Copias offline e inmutables como última línea de defensa contra ransomware.

Zero Trust + MFA

Eliminar cuentas legacy, auditar OAuth, verificación continua de identidad.

Seguridad en cadenas de suministros de software

Auditar proveedores, librerías y componentes, monitoreo continuo de dependencias de terceros.

Convergencia IT/OT

Segmentar redes OT, monitorear dispositivos IoT, planes de respuesta específicos ante incidentes.

Detección con IA

Combatir IA con IA: sistemas ML para anomalías, simulacros de deepfake y phishing.

Cripto-agilidad (PQC)

Inventario criptográfico, preparar migración a criptografía post-cuántica.

CLONER

Comprender la evolución del atacante

es clave para diseñar una estrategia de

ciber resiliencia capaz de responder al presente

sin perder de vista las amenazas del futuro.

El respaldo no es solo una copia de datos.

Es la capacidad de volver a levantarse.

Cloner.cl

Líderes en respaldo de información en la nube