Creando una Trayectoria Profesional en Seguridad Digital: Fundamentos de la Ciberseguridad (sesión teórica)

Agosto, 2021

Tabla de contenidos

Capacitación en Ciberseguridad OEA

Fundamentos de la Ciberseguridad

¿Qué es la Seguridad de la Información?

Objetivos de la seguridad de la información

Modelos de Seguridad de la Información

Actores en escenarios de Ciberseguridad

Privacidad en el siglo XXI

Escenarios de ciber-seguridad: delitos informáticos

Datos estadísticos del panorama de ciber-seguridad durante la pandemia

Frameworks de Seguridad de la información

La combinación de espacio, tiempo y fuerza, que deben considerarse como los elementos básicos de esta teoría de la defensa, hace de esta una cuestión complicada, Por consiguiente , no es fácil encontrar un punto fijo de partida.

-**De la guerra**, *Carl Von Clausewitz*

Fundamentos de la Ciberseguridad

Se presentará una introducción a los conceptos básicos de la Seguridad de la Información y la Ciberseguridad, además de una breve introducción a los escenarios y retos asociados a dichas disciplinas. Se realizará la presentación de definiciones técnicas fundamentales para abordar los siguientes módulos.

El módulo contiene una práctica (laboratorio) y un examen en linea.

Fundamentos de la Ciberseguridad (1/2)

- ¿Qué es la Seguridad de la Información/Ciberseguridad?
- Conceptos básicos: Integridad, Disponibilidad, Confidencialidad
- Seguridad vs Facilidad de Uso
- Actores en escenarios de Ciberseguridad: Hacker/Cracker/CISO/Ethical hacker/investigador forense/Custodio/Dueño de la información/usuario final
- Privacidad en el siglo XXI
- Escenarios de ciber-seguridad: delitos informáticos, hacktivismo, retribución económica
- Frameworks y referencias relevantes para la seguridad de la información

Fundamentos técnicos

Fundamentos de la Ciberseguridad (2/2)

- Arquitectura del nivel OSI
- El modelo cliente servidor
- Arquitectura de sistemas
- Arquitectura de aplicaciones
- Breve introducción al protocolo IP
- Breve introducción a protocolos de transporte (TCP, UDP)
- Breve introducción al sistema de resolución de nombres (DNS)
- Breve introducción a protocolos de aplicación (HTTP, SSH)
- Resumen de Ciber-amenazas

¿Qué es la Seguridad de la Información? (1/2)

Seguridad de la Información

La seguridad de la información puede definirse como el conjunto de **medidas preventivas** y **reactivas** en una organización para proteger la información y los sistemas de información de posibles accesos, divulgaciones, interrupciones, modificaciones o destrucción por parte de **entes no autorizados**, con el objetivo de mantener la integridad, disponibilidad y confidencialidad de los mismos.

¿Qué es la Seguridad de la Información? (2/2)

¿Qué es la ciber-seguridad?

La ciber-seguridad son una serie de mecanismos, controles y estrategias para proteger los activos que se encuentran de forma electrónica (computadoras, servidores, redes, dispositivos móviles etc.) de un **posible comprometimiento** o **ataque**.

Objetivos de la seguridad de la información (1/3)

- **Disponibilidad** (Availability)
- **Integridad** (Integrity)
- **Confidencialidad** (Confidentiality)

Figura 1: Triada de la seguridad.

Objetivos de la seguridad de la información (2/3)

- **Disponibilidad**: se debe asegurar que los accesos a la información y a los sistemas sean **confiables** y **oportunos** por parte de los individuos autorizados
- **Integridad**: la información procesada debe ser **confiable** y **exacta**, se deben prevenir todas las modificaciones no autorizadas
- **Confidencialidad**: se debe asegurar un **nivel de secrecía necesaria** en cada paso del procesamiento de datos y prevenir la divulgación no autorizada de información

Objetivos de la seguridad de la información (3/3)

Analizar

- **Requerimientos Funcionales:** ¿La solución ejecuta las tareas requeridas?
- **Requerimientos de aseguramiento (CIA)** ¿Estamos seguros del nivel de protección que provee esta solución?

Figura 2: Análisis de la funcionalidad de la seguridad.

Modelos de Seguridad de la Información (1/4)

¿Qué son los Modelos de Seguridad de la Información?

Los modelos de seguridad de la información son plantillas que describen como la seguridad de la información debe de ser trazada y gobernada. Es decir, es una estructura de procesos de seguridad.

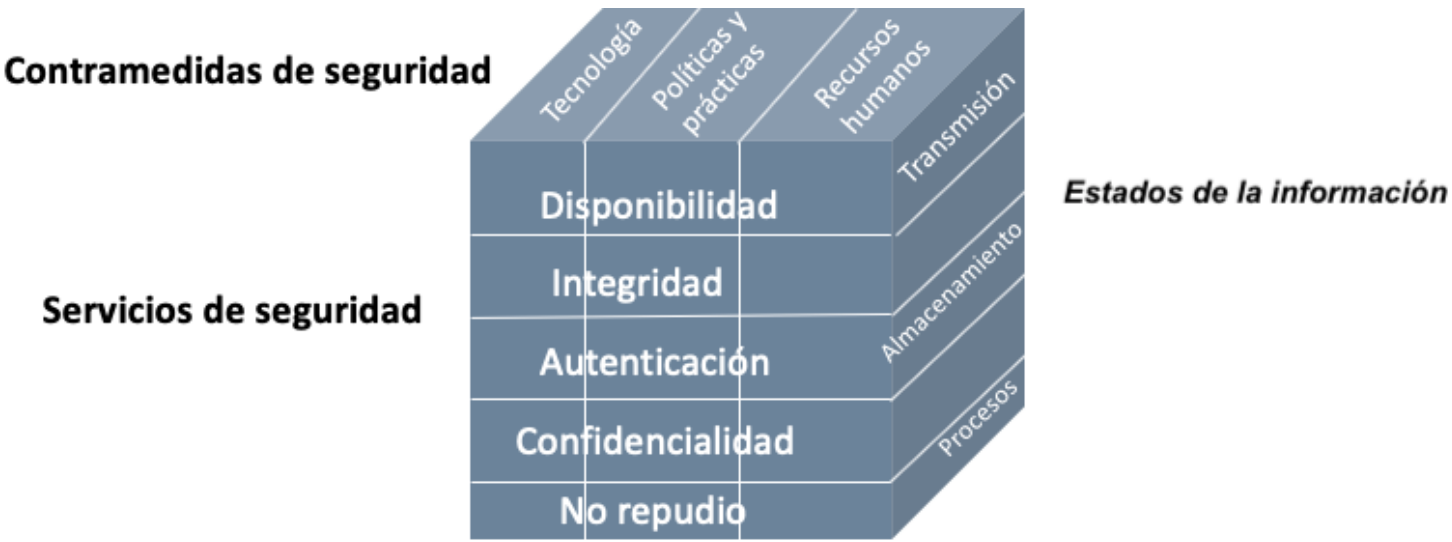


Figura 3: Modelo de McCumber.

Modelos de Seguridad de la Información (2/4)

- **No repudio**: es el nivel de garantía de que una entidad no pueda negar la validez de un artefacto en un canal de comunicación seguro
- **Autenticación**: proceso de identificar a una entidad, determinando de hecho quién se declara ser
- **Seguridad por oscuridad**: principio que intenta utilizar el secreto (de diseño, implementación, etc.) para garantizar la seguridad. Este principio se puede plasmar en distintos aspectos, como por ejemplo:
  - *Mantener el secreto del código fuente del software*
  - *Mantener el secreto de algoritmos y protocolos utilizados*
  - *Adopción de políticas de no revelación pública de la información sobre vulnerabilidades*

Modelos de Seguridad de la Información (3/4)

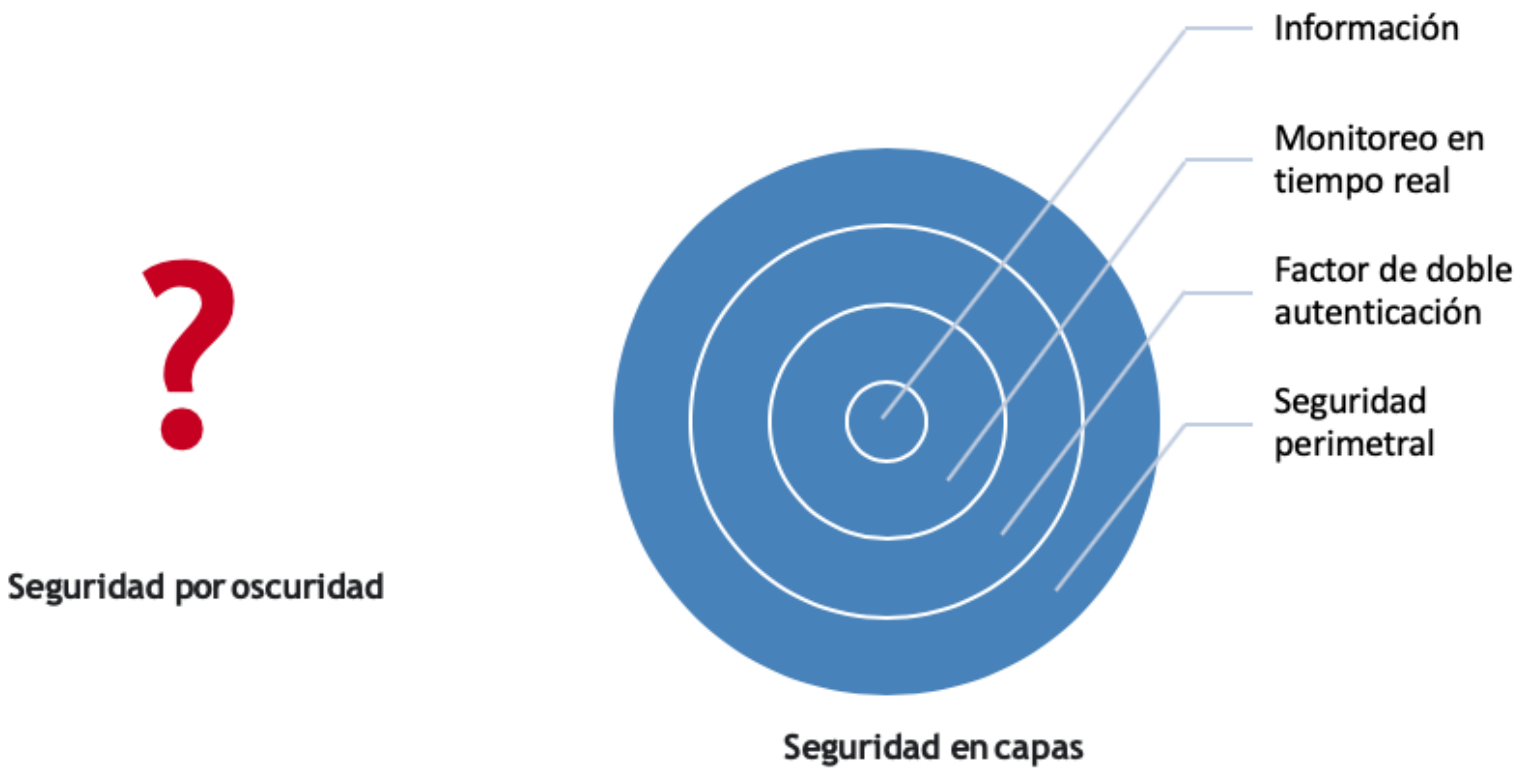


Figura 4: Seguridad por oscuridad vs seguridad en capas.

Modelos de Seguridad de la Información (4/4)

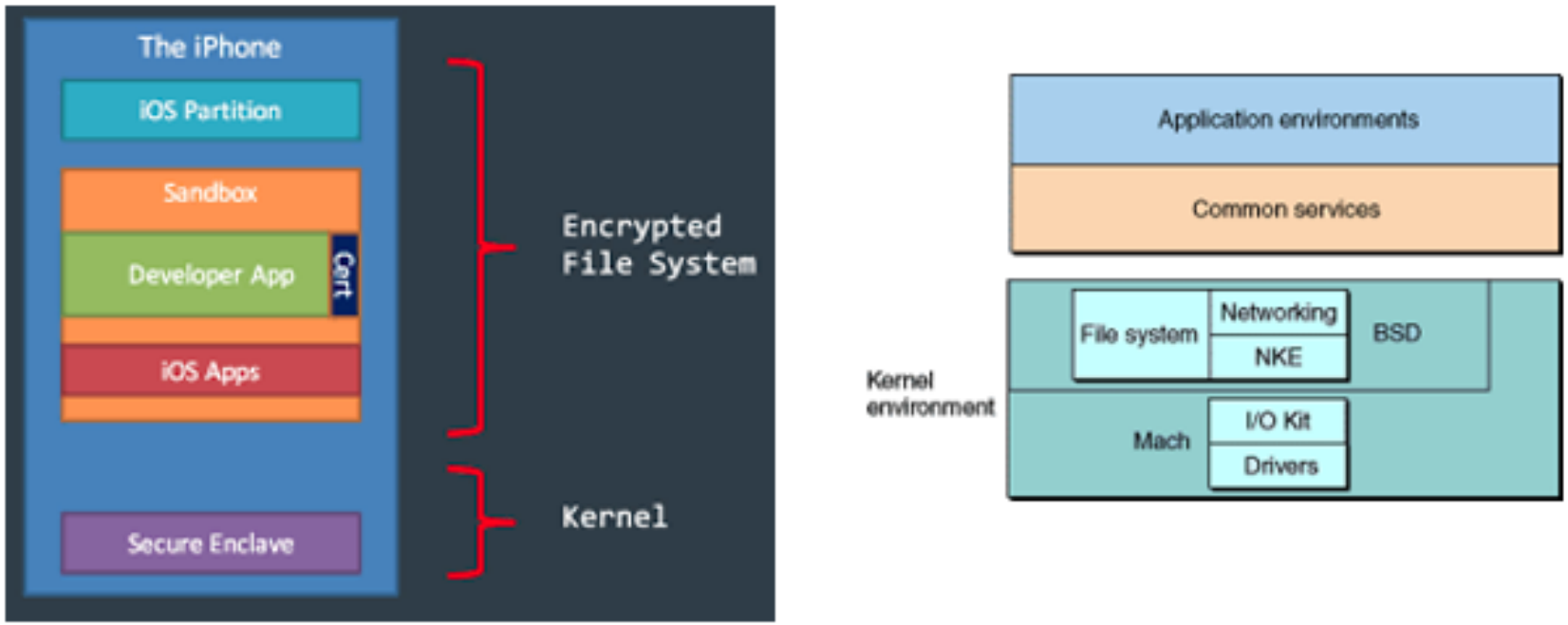


Figura 5: El kernel del sistema operativo de iOS ha sido objeto de especulación por utilizar el principio de seguridad por oscuridad.

Actores en escenarios de Ciberseguridad (1/2)

- **Cracker**: delincuente informático, que accede a sistemas informáticos sin autorización y en la mayoría de los casos con intenciones maliciosas. Es a veces denominado **black hat hacker**
- **Hacker**: persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora

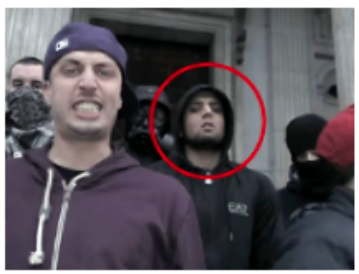


Figura 6: Hunaid Hussain fue hacker de sombrero negro (**black hat hacker**) que formó parte del grupo terrorista ISIS.

Actores en escenarios de Ciberseguridad (2/2)

- **CISO: Chief Information Security Officer**: oficial de seguridad de la información. Es el responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información
- **Ethical Hacker**: Consultor en seguridad de la información que sistemáticamente intenta penetrar sistemas, redes o aplicaciones con autorización de sus custodios y/o propietarios. Es también conocido como *white hat hacker*
- **Propietarios/Dueños**: es de facto la persona responsable de un conjunto particular de datos. Ejemplo: *CEO, Gerentes/Líderes de área, etc.*
- **Custodio**: personal encargado de operar y entregar protección técnica a los activos de información. Ejemplo: *backup y restauración de datos*

Privacidad en el siglo XXI (1/2)

Acerca de la privacidad

La privacidad puede ser definida como el ámbito de la vida personal de un individuo, que se desarrolla en un espacio reservado, teniendo como propósito principal mantenerse **confidencial**.

La privacidad en Internet

- Se refiere al control de la información que posee un determinado usuario que se conecta a la red interactuando con diversos servicios en línea, en los que intercambia datos durante la navegación
- Implica el derecho o el mandato a la privacidad personal con respecto al almacenamiento, la re-utilización, la provisión a terceros y la exhibición de información a través de Internet

Privacidad en el siglo XXI (2/2)

Algunos de los métodos de espionaje por Internet y que afectan la privacidad son:

- Rastreo
- Observadores intermediarios ¿Mediante Proxies?
- Espionaje
- Retención de datos
- Análisis de tráfico

Escenarios de ciber-seguridad: delitos informáticos (1/11)

Hacktivismo

- Protesta o desobediencia civil relacionada con el uso de tecnologías informáticas. Los ciber-ataques son dirigidos para popularizar ideas **orientadas socialmente**
- Generalmente, los hacktivistas no pertenecen a ninguna organización o asociación formal
  Tienen su propia interpretación de lo que constituye un comportamiento aceptable

Escenarios de ciber-seguridad: delitos informáticos (2/11)

Figura 7: El colectivo de hackers activistas Anonymous utiliza ataques de Denegación de Servicio (DoS), como herramienta primordial para comprometer la disponibilidad de servicios.

Escenarios de ciber-seguridad: delitos informáticos (3/11)

Empleados de Huawei habrían ayudado a gobiernos de África a espiar a sus oponentes políticos

Gobierno sueco concede a la policía el uso de spyware contra sospechosos de crímenes violentos

Figura 8: Ejemplos de riesgos en la privacidad mediante herramientas de software para espionaje (*spyware*).

Escenarios de ciber-seguridad: delitos informáticos (4/11)

Apple registra la localización de los iPhone aunque lo desactives

Apple ha confirmado a un investigador de seguridad que los nuevos iPhone registran la localización, incluso si lo hemos deshabilitado en la configuración.

Figura 9: Las compañías establecen mecanismos de privacidad que difícilmente los usuarios pueden administrar.

Escenarios de ciber-seguridad: delitos informáticos (5/11)

En la siguiente lista se muestran algunos campos de los cuales se pueden observar y obtener datos confidenciales:

- Proveedores de Internet
- Motores de búsqueda
- Redes compartidas (*redes corporativas*, *hotspot*)
- Redes sociales
- Geo-localización

Escenarios de ciber-seguridad: delitos informáticos (6/11)

Figura 10: La Dark Web ,una parte de la Deep Web, contiene sitios dinámicos para fomentar el mercado negro. La mayoría son transacciones descentralizadas en monederos tipo bitcoin (BTC).

Escenarios de ciber-seguridad: delitos informáticos (7/11)

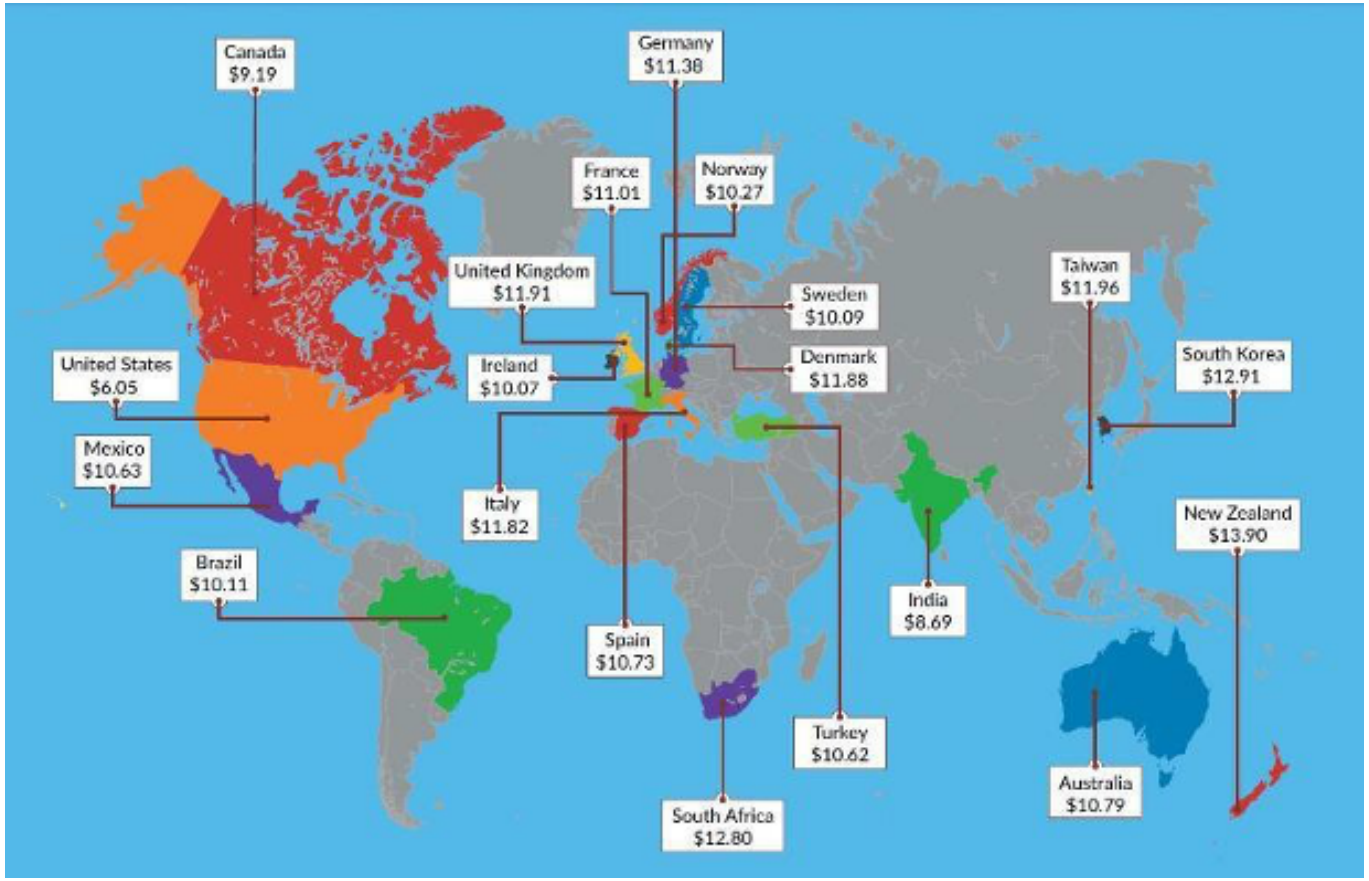


Figura 11: Precio promedio de venta tarjetas de crédito en el mercado negro (Top 20 por precio).

Escenarios de ciber-seguridad: delitos informáticos (8/11)

La ciudad de Torrance en California todavía se enfrenta a una demanda de ransomware de 100 BTC después de restarle importancia a la cantidad de datos privados que se habían perdido en el ataque

Figura 12: Los *ransomware* y *crypto-lockers* son mecanismos de extorsión comunes y con blancos dirigidos como gobiernos o empresas. Generalmente los ciber-delincuentes exigen una alta suma en BTC por la recuperación de la información.

Escenarios de ciber-seguridad: delitos informáticos (9/11)

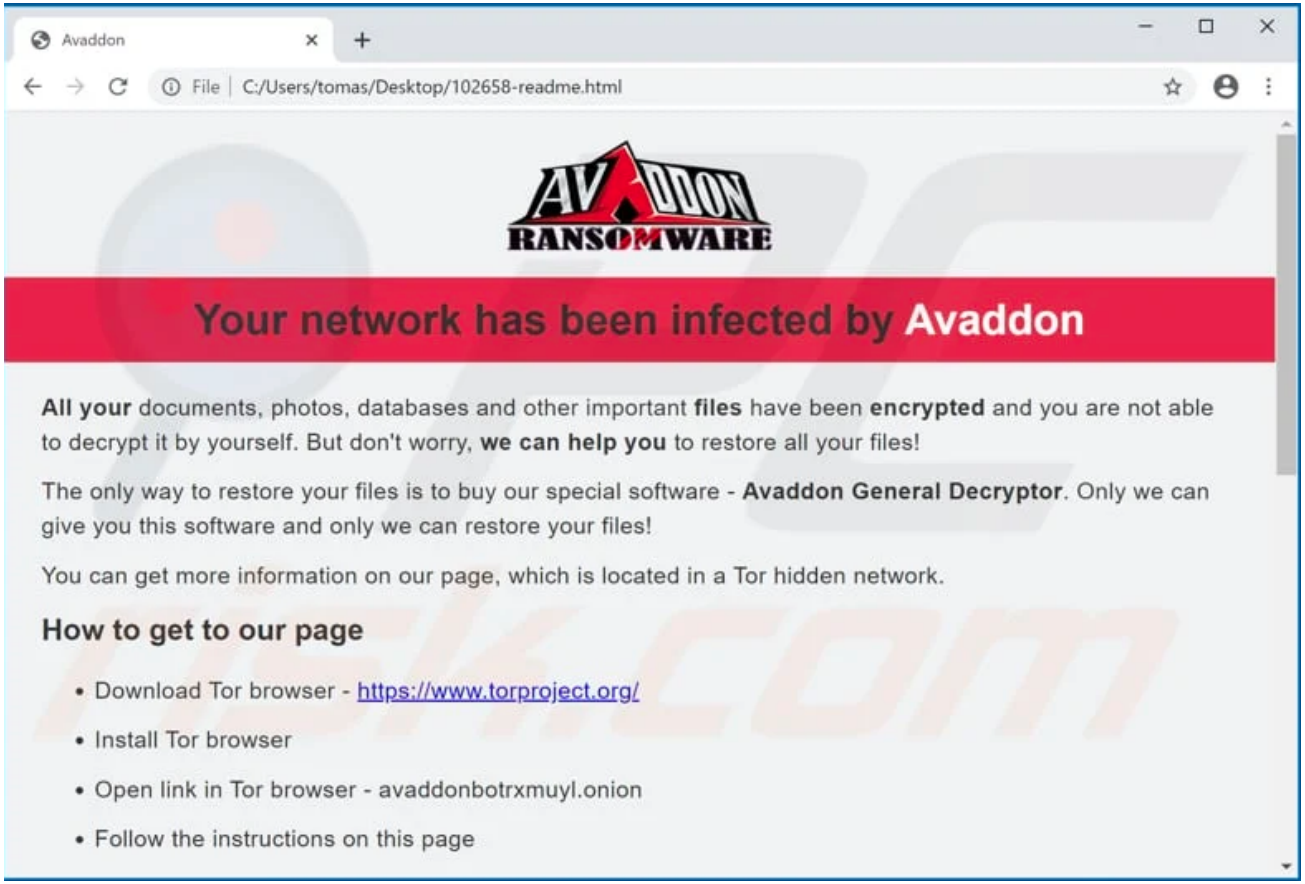


Figura 13: Ejemplo del *ransomware Avaddon*, que se ha popularizado por diferentes ataques en el año 2021

Escenarios de ciber-seguridad: delitos informáticos (10/11)

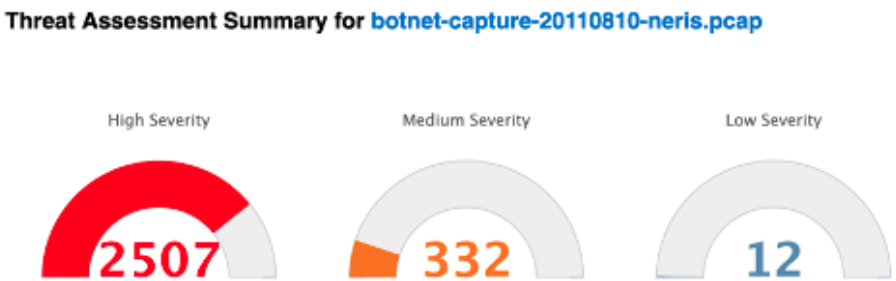
Figura 14: La suplantación de identidad mediante *phishing* o *spear phishing* afecta en gran parte a los productos financieros.

Entre las herramientas más comunes utilizadas por los ciber criminales se encuentran:

- Remote Access Trojans (RATs)
- Webshells (mediante ataques de bind/reverse shell)
- Programas de robo de credenciales
- Ataques de movimiento lateral

Escenarios de ciber-seguridad: delitos informáticos (11/11)

- Centros de control y comando (C & C)



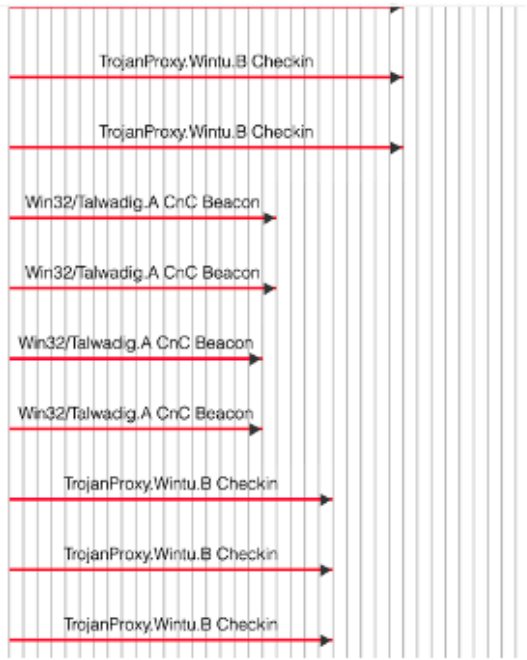


Figura 15: Ejemplo del análisis de una *botent* con sus respectivas cargas útiles (*payloads*) maliciosas.

Datos estadísticos del panorama de ciber-seguridad durante la pandemia (1/2)

- 47 % de los empleados se pueden distraer fácilmente con mensajes de phishing, mientras trabajan desde casa (**Tessian**)
- Ha aumentado en un 43 % el número de amenazas a aplicaciones de trabajo remoto (**Verizon**)
- 52 % de las compañías analizadas tiene preocupación por el uso de plataformas de trabajo remoto, desde el inicio de la pandemia (**Gartner**)
- El trabajo remoto puede ser un negocio lucrativo para los ciber-criminales, se estima que en promedio una vulnerabilidad puede costarle $\$137,000$ dólares a la empresa(**IBM**)
- 81 % de los profesionales en ciber-seguridad han reportado incidentes desde el inicio de la pandemia (**ISC**)

Datos estadísticos del panorama de ciber-seguridad durante la pandemia (2/2)

- 83 % de las compañías de telecomunicaciones han reportado fallas por sus clientes, de las cuales, 36 % son relacionadas a fallas de seguridad (**CompTIA**)
- La consulta *cómo quitar un virus* ha incrementado en un 42 % (**Google Trends**)
- Ha aumentado en un 8 % el uso de soluciones mediante VPNs (**WatchGuard**)
- 76 % de los trabajadores por vía remota coinciden que trabajar desde casa incrementa el riesgo de que su información sea expuesta mediante una vulnerabilidad (**IBM**)

Frameworks de Seguridad de la información (1/4)

La serie ISO/IEC 27000

- Comprende estándares de seguridad de la información publicados conjuntamente por la *Organización Internacional de Normalización (ISO)* y la *Comisión Electrotécnica Internacional (IEC)*
- La serie proporciona recomendaciones de mejores prácticas sobre la gestión de la seguridad de la información (la gestión de los riesgos de la información a través de controles) en el contexto de un Sistema de gestión de la Seguridad de la Información (SGSI), similar en diseño a los sistemas de gestión para el aseguramiento de la calidad (la serie *ISO 9000*) y protección del medio ambiente (serie *ISO 14000*)

Frameworks de Seguridad de la información (2/4)

Control Objectives for Information and Related Technology (COBIT)

COBIT es un marco de alto nivel centrado en la identificación y mitigación de riesgos. Se ha desarrollado principalmente para el gobierno de TI. Se usa principalmente en la industria para cumplir con los estándares de Sarbanes-Oxley.

US National Institute of Standards and Technology (NIST)

El marco NIST ha evolucionado durante 20 años y contiene una amplia gama de estándares de seguridad de la información y mejores prácticas.

En el siguiente listado se muestran estándares específicos de la industria:

Frameworks de Seguridad de la información (3/4)

- **PCI DSS (Payment Card Industry Data Security Standard)**: para el manejo de tarjetas de crédito
- **HIPAA (Health Insurance Portability and Accountability Act, US)**: marco de seguridad de la información de salud
- **GDPR (General Data Protection Regulation, EU)**: regulación al tratamiento de datos personales su libre circulación
- **NIST Cybersecurity Framework**: El NIST (The National Institute of Standards and Technology) propone un framework orientado a la protección de sistemas de información en la industria, el cual se basa en cinco procesos fundamentales: *identificación*, *protección*, *detección*, *respuesta* y *recuperación*

Frameworks de Seguridad de la información (4/4)

¿Qué es una certificación de seguridad de la información o de ciber-seguridad?

Es un tipo de certificación que valida las habilidades necesarias para poder realizar funciones relacionadas a la seguridad de la información o ciber-seguridad. En su mayoría establecen un conocimiento especializado para poder ejecutar un rol o nivel en un puesto relacionado al área.

Algunas de las certificaciones más populares son:

- CEH: *Certified Ethical Hacker*
- CISSP: *Certified Information Systems Security Professional*
- CCSP: *Certified Cloud Security Professional*
- CISA: *Certified Information Systems Auditor*
- *COBIT 5 Certification Training*
- *CompTIA+ Security+*