CORRIENTES Ministerio de Educación Dirección de Nivel Superior	**INSTITUTO SUPERIOR DE FORMACIÓN DOCENTE** **ITUZAINGÓ- CORRIENTES** **BUENOS AIRES Y APIPE** **CUE:1801768-00** **Correo Electrónico 1801768-00@mec.gob.ar**	

Informe de Investigacion de Malwares Famosos a Nivel Mundial y Recomendacion de Antivirus.

Apellido y Nombre de Estudiantes:

Ayala Lucila, Ojeda Itati

fecha: 28/08

CORRIENTES Ministerio de Educación Dirección de Nivel Superior	**INSTITUTO SUPERIOR DE FORMACIÓN DOCENTE** **ITUZAINGÓ- CORRIENTES** **BUENOS AIRES Y APIPE** **CUE:1801768-00** **Correo Electrónico 1801768-00@mec.gob.ar**	

Introduccion:

En la era digital actual, la seguridad en linea es un tema cada vez mas importante. Los Malwares y Virus Informaticos representa una amenaza constante, para nuestras computadoras , datos y privacidad.

A lo largo de los años hemos, vista como Malwares famosos como I Love You (2000), Stuxnet (2010) WannaCry (2017), NotPeya(2017), Emotet(2014-2021) han causado daños significativos a individuos y Organizaciones a nivel Mundial. Por eso es que es fundamental estar informados sobre estos peligros y tomar medidas para protegerse.

En este informe, exploraremos algunos de los malwares mas notorios y revisaremos las opciones de antivirus disponibles para garantizar la seguridad de nuestros sistemas de datos.

CORRIENTES Ministerio de Educación Dirección de Nivel Superior	**INSTITUTO SUPERIOR DE FORMACIÓN DOCENTE** **ITUZAINGÓ- CORRIENTES** **BUENOS AIRES Y APIPE** **CUE:1801768-00** **Correo Electrónico 1801768-00@mec.gob.ar**	I.S.F.D.I

Malwares:

ILOVEYOU (2000) : fue un gusano informático, uno de los primeros y más notorios virus de correo electrónico.

1.**Origen**:

- Dónde: Apareció en Filipinas.

- Cuándo: Fue descubierto por primera vez el 4 de mayo de 2000.

Creadores:

- Se cree que fue creado por Onel de Guzmán, un programador filipino.

2. **Propagación**:

- Métodos de infección: Se propagó principalmente a través de correos electrónicos con el asunto “ILOVEYOU” y un archivo adjunto llamado “LOVE-LETTER-FOR-YOU.txt.vbs”. El archivo estaba disfrazado como un mensaje de texto, pero en realidad contenía un script de Visual Basic que ejecutaba el gusano.

- Método de infección: Al abrir el archivo adjunto, el gusano se autoejecutaba, enviando copias de sí mismo a todos los contactos del usuario en su libreta de direcciones de Outlook.

3. **Impacto:**

- Tipos de daño: El gusano sobrescribió archivos de ciertos tipos (como archivos de imágenes y documentos) con su propio código, causando

pérdida de datos. También alteró la configuración del sistema y dejó notas de rescate.

- Número de usuarios afectados: Se estima que afectó a millones de usuarios en todo el mundo, causando daño a sistemas en empresas y gobiernos.

Impacto económico y social:

- Económico: El daño económico se estima en alrededor de 10 mil millones de dólares debido a la pérdida de datos, interrupciones en el trabajo y costos de recuperación.

- Social: Generó una gran preocupación sobre la seguridad en las comunicaciones electrónicas y la vulnerabilidad de los sistemas informáticos.

4. Funcionamiento:

- Operación: ILOVEYOU utilizaba ingeniería social para engañar a los usuarios y provocar que abrieran el archivo adjunto. Una vez abierto, el gusano se replicaba y enviaba copias a todos los contactos del usuario.

- Eficacia: La eficacia del gusano se debió a su capacidad para aprovechar la confianza de los usuarios en los correos electrónicos y la facilidad con que se propagaba a través de listas de contactos.

5. **Mitigacion**:

- Medidas: Se implementaron parches de seguridad, se mejoró el filtrado de correos electrónicos y se fortalecieron las políticas de seguridad informática. Las empresas también comenzaron a educar a los usuarios sobre los riesgos del phishing y la ingeniería social.

- Lecciones aprendidas: El ataque subrayó la importancia de la seguridad en el correo electrónico, la necesidad de mantener software actualizado y la efectividad de educar a los usuarios para reconocer amenazas de seguridad.

NotPetya (**2017**) :

fue un ataque cibernético que se presentó como un ransomware pero en realidad estaba diseñado para causar daño y destrucción a gran escala.

1. **Origen**:

- Dónde: El ataque se originó en Ucrania, pero se extendió rápidamente a nivel global.

- Cuándo: Fue descubierto el 27 de junio de 2017.

Creadores:

- Se sospecha que fue desarrollado por un grupo de hackers con vínculos con el gobierno ruso, aunque el grupo específico detrás del ataque no se ha confirmado oficialmente.

2. Propagación:

- Métodos de infección: NotPetya se propagó a través de un exploit de Windows llamado EternalBlue, que también se usó en el ataque

WannaCry. Utilizaba una vulnerabilidad en el protocolo SMB (Server Message Block) para moverse lateralmente a través de redes.

- Método de infección: El malware se distribuyó inicialmente a través de una actualización de software comprometida para una empresa de contabilidad ucraniana, que luego se propagó a otras redes.

3. Impacto:

- Tipos de daño: NotPetya cifraba archivos en los sistemas infectados y luego sobrescribía el registro de arranque del sistema (MBR), haciendo que el sistema no pudiera arrancar. A diferencia de otros ransomware, NotPetya no tenía una funcionalidad de recuperación de archivos y estaba diseñado para causar daños irreparables.

- Número de sistemas afectados: Afectó a miles de sistemas en más de 60 países, con un impacto significativo en grandes empresas y organizaciones gubernamentales.

-Impacto económico y social:

- Económico: El impacto económico se estimó en más de 10 mil millones de dólares debido a la pérdida de datos, interrupciones en el negocio y costos de recuperación.

- Social: El ataque generó una gran preocupación sobre la seguridad cibernética y la vulnerabilidad de las infraestructuras críticas, destacando la necesidad de una mejor protección y preparación para ataques cibernéticos.

5. Funcionamiento:

- Operación: NotPetya actuaba cifrando archivos y dañando el MBR, lo que hacía que los sistemas afectados fueran inutilizables. La combinación de cifrado y sobrescritura del MBR garantizaba que los datos fueran irrecuperables.

- Eficacia: La eficacia del ataque se debió a su rápida propagación a través de redes comprometidas y su capacidad para evadir las medidas de seguridad tradicionales. La utilización del exploit EternalBlue permitió una expansión rápida y efectiva.

6. Mitigación:

- Medidas: Las organizaciones reforzaron sus prácticas de seguridad, aplicaron parches de emergencia, y se centraron en mejorar la detección y respuesta ante amenazas cibernéticas. Se hicieron esfuerzos para compartir información sobre vulnerabilidades y ataques a nivel global.

- Lecciones aprendidas: El ataque subrayó la importancia de mantener sistemas actualizados, la necesidad de proteger las redes contra amenazas internas y externas, y la importancia de tener un plan de respuesta a incidentes para mitigar el impacto de ataques cibernéticos.

NotPetya demostró la capacidad de los ataques cibernéticos para causar daños masivos y resaltó la necesidad de una ciberseguridad robusta para proteger infraestructuras críticas y datos sensibles.comprometidas, aprovechando vulnerabilidades en el sistema y credenciales robadas para moverse a otros sistemas en la misma red.

3. Impacto:

- Tipos de daño: Emotet inicialmente robaba credenciales y datos bancarios, pero con el tiempo se convirtió en una plataforma para distribuir otros tipos de malware, como ransomware y troyanos de acceso remoto. El daño incluía pérdida de datos, interrupción de operaciones y daños financieros.

- Número de sistemas afectados: Emotet afectó a miles de organizaciones en todo el mundo, desde pequeñas empresas hasta grandes corporaciones y organismos gubernamentales.

Impacto económico y social:

- Económico: El impacto económico fue significativo debido al costo de la limpieza de sistemas, recuperación de datos y pérdida de productividad. Las estimaciones varían, pero se calculó que el costo de los ataques relacionados con Emotet alcanzó millones de dólares.

- Social: Generó una mayor conciencia sobre la necesidad de educación en ciberseguridad, así como sobre la importancia de proteger la infraestructura de TI contra ataques sofisticados.

4. Funcionamiento:

- Operación: Emotet operaba como un troyano modular, que permitía a los operadores del malware descargar y ejecutar otros tipos de malware en los sistemas comprometidos. Su diseño modular lo hacía muy flexible y difícil de detectar.

- Eficacia: Su eficacia se debió a la combinación de técnicas avanzadas de ingeniería social para la infección inicial y su capacidad para adaptarse y distribuir otros malware, aumentando su impacto.

5. Mitigaciones:

- Medidas: Las autoridades internacionales, incluyendo Europol y el FBI, realizaron operaciones coordinadas para desmantelar la infraestructura de Emotet en enero de 2021, que incluyó el apagado de servidores de comando y control. Las organizaciones también mejoraron

sus prácticas de seguridad, como el entrenamiento en detección de phishing y la implementación de políticas de seguridad más estrictas.

- Lecciones aprendidas: El caso de Emotet subrayó la importancia de la cooperación internacional en la lucha contra el crimen cibernético, necesidad de mantener sistemas actualizados y la eficacia de educar a los usuarios para detectar y evitar ataques de phishing. También demostró la importancia de tener una estrategia de respuesta a incidentes bien establecida.

Antivirus Norton:

1.Historia y Desarrollo

Creación:

Norton Antivirus fue creado por Peter Norton, un conocido autor y experto en software, a través de su empresa Norton Computing. El primer lanzamiento del antivirus fue en 1990. En 1990, Norton Antivirus era una de las primeras soluciones de software diseñadas para combatir virus informáticos.

Evolución:

A lo largo de los años, Norton Antivirus ha evolucionado significativamente. Inicialmente centrado en la detección y eliminación de virus, ha expandido sus capacidades para incluir protección contra malware, spyware, ransomware y amenazas de phishing. Norton ha integrado funciones avanzadas como firewall, protección en tiempo real, y herramientas de optimización del sistema. La compañía ha lanzado versiones actualizadas anualmente, con mejoras en la detección y en el rendimiento del software.

2 Funciones Principales:

- Protección en Tiempo Real: Ofrece protección continua contra amenazas en tiempo real, evitando que malware y otras amenazas infecten el sistema.

- Escaneo de Malware: Realiza escaneos completos del sistema y archivos en busca de virus, spyware y otros tipos de malware.

- Firewall: Incluye un firewall avanzado para bloquear accesos no autorizados y proteger contra intrusiones externas.

- Protección Contra Ransomware: Proporciona herramientas específicas para detectar y bloquear ataques de ransomware.

- Optimización del Sistema: Incluye herramientas para mejorar el rendimiento del sistema, como la eliminación de archivos temporales y la gestión del inicio del sistema.

3 Efectividad:

La efectividad de Norton Antivirus en la detección y eliminación de malware se ha mantenido alta en comparación con otros antivirus. En pruebas recientes realizadas por laboratorios independientes como AV-Test y AV-Comparatives, Norton ha obtenido calificaciones generalmente altas por su capacidad para detectar y eliminar amenazas. Sin embargo, es importante revisar las pruebas más recientes para obtener la información más actualizada, ya que la eficacia puede variar con el tiempo y las actualizaciones de software.

4. Compatibilidad

Norton Antivirus es compatible con los principales sistemas operativos, incluyendo:

- Windows:Desde Windows 7 hasta las versiones más recientes.

- macOS:Las versiones más recientes de macOS.

- Android: Compatible con versiones recientes del sistema operativo Android.

- iOS: Aunque la protección en iOS es más limitada, ofrece ciertas funcionalidades de seguridad como la protección web y la privacidad.

5.Costo y Licencias

- Costo: Norton Antivirus ofrece varias opciones de suscripción. Los precios pueden variar dependiendo de la región y de las ofertas promocionales. En general, los precios anuales oscilan entre $30 y $100 USD.

- Licencias: Ofrece opciones de licencia que pueden cubrir desde un solo dispositivo hasta múltiples dispositivos. Las opciones incluyen:

- Norton Antivirus Plus: Protección básica para un solo dispositivo.

- Norton 360 Standard: Incluye protección para varios dispositivos y almacenamiento en la nube.

- Norton 360 Deluxe: Amplía la protección a más dispositivos y agrega herramientas de VPN y protección de identidad.

- Norton 360 Premium:Ofrece funciones adicionales como copias de seguridad en la nube y protección para más dispositivos.

Las opciones de licencia y precios están sujetas a cambios y pueden variar según la oferta del momento.

INSTITUTO SUPERIOR DE FORMACIÓN DOCENTE
ITUZAINGÓ- CORRIENTES
BUENOS AIRES Y APIPE
CUE:1801768-00
Correo Electrónico 1801768-00@mec.gob.ar

McAfee Antivirus

1.Historia y Desarrollo:

- Creación: Fundado por John McAfee en 1987. McAfee ha evolucionado desde su enfoque inicial en la detección de virus a una suite completa de seguridad.

- Evolución: Ha integrado protección contra malware avanzado, ransomware, y herramientas de optimización del sistema. También ha añadido funciones como protección en tiempo real, firewall y herramientas de privacidad.

2.Funciones Principales:

- Protección en Tiempo Real: Sí.

- Escaneo de Malware: Sí, incluye escaneo completo y personalizado.

- Firewall:Incluye firewall bidireccional.

- Protección Contra Ransomware: Sí, con herramientas dedicadas.

- Optimización del Sistema: Incluye herramientas para mejorar el rendimiento del sistema.

3.Efectividad:

- Desempeño:McAfee tiene un historial sólido en detección y eliminación de malware. Resultados de pruebas recientes por AV-

Test y AV-Comparatives suelen ser positivos, pero puede haber variación en la eficacia en comparación con otras soluciones.

4.Compatibilidad:

- Sistemas Operativos: Windows, macOS, Android, iOS.

5.Costo y Licencias:

- Costo:Varía entre $30 y $100 USD anuales dependiendo del nivel de protección y el número de dispositivos.

- Licencias: Opciones para uno o varios dispositivos, con productos como McAfee Total Protection y McAfee LiveSafe.

Bitdefender Antivirus

1.Historia y Desarrollo:

- Creación:Fundado en 2001 en Rumania. Bitdefender ha crecido para ofrecer una amplia gama de productos de seguridad cibernética.

- Evolución: Ha evolucionado para incluir protección avanzada contra malware, ransomware, y amenazas emergentes, y ha integrado tecnologías como el aprendizaje automático y la inteligencia artificial.

2.Funciones Principales:

- Protección en Tiempo Real: Sí.

- Escaneo de Malware: Sí, con escaneo en la nube y análisis avanzado.

- Firewall: Sí, en versiones completas.

- Protección Contra Ransomware: Sí, con funcionalidades avanzadas.

- Optimización del Sistema: Opcional en algunos paquetes.

3.Efectividad:

- Desempeño: Bitdefender ha obtenido altas calificaciones en pruebas de AV-Test y AV-Comparatives, con una sólida reputación en detección y eliminación de amenazas.

4.Compatibilidad:

- Sistemas Operativos: Windows, macOS, Android, iOS.

5.Costo y Licencias:

- Costo: Entre $40 y $100 USD anuales dependiendo del paquete y el número de dispositivos.

- Licencias:Ofrece opciones como Bitdefender Antivirus Plus, Bitdefender Internet Security, y Bitdefender Total Security.

Kaspersky Antivirus

1.Historia y Desarrollo:

- Creación: Fundado por Eugene Kaspersky en 1997. Kaspersky ha evolucionado para ser una de las soluciones más completas en el mercado.

- Evolución: Se ha expandido para incluir protección contra una amplia gama de amenazas, desde virus hasta ataques dirigidos y ransomware.

2 Funciones Principales:

- Protección en Tiempo Real: Sí.

- Escaneo de Malware:Sí, con escaneo rápido y completo.

- Firewall: Sí, en versiones completas.

- Protección Contra Ransomware: Sí, con herramientas avanzadas.

- Optimización del Sistema:Opcional en algunos paquetes.

3.Efectividad:

- Desempeño: Kaspersky ha obtenido excelentes resultados en pruebas de AV-Test y AV-Comparatives. Su tecnología es conocida por su alta tasa de detección y bajo impacto en el rendimiento del sistema.

4 Compatibilidad:

- Sistemas Operativos: Windows, macOS, Android, iOS.

5.Costo y Licencias:

- Costo:Varía entre $30 y $100 USD anuales, dependiendo del paquete y el número de dispositivos.

- Licencias: Incluye opciones como Kaspersky Antivirus, Kaspersky Internet Security, y Kaspersky Total Security.

Aquí tienes una descripción de cada uno de los malwares mencionados:

1. **ILOVEYOU (2000)**

- **Definición:** ILOVEYOU es un gusano informático que se propagó por primera vez en mayo de 2000. Fue enviado como un archivo adjunto a un correo electrónico con el asunto "ILOVEYOU".

- **Características:** Este gusano, escrito en VBScript, se replicaba a sí mismo enviando copias a todos los contactos del usuario infectado. Modificaba archivos en el sistema, sobrescribiéndolos con su código, lo que provocaba la pérdida de datos.

- **Impacto:** Se estima que infectó alrededor de 45 millones de sistemas en todo el mundo y causó daños económicos que ascienden a miles de millones de dólares.

2. **Stuxnet (2010)**

- **Definición:** Stuxnet es un gusano informático altamente sofisticado descubierto en 2010, diseñado específicamente para atacar sistemas de control industrial.

- **Características:** Este malware estaba dirigido a software SCADA utilizado para controlar y monitorear procesos industriales. Stuxnet fue

programado para alterar el funcionamiento de las centrifugadoras en las instalaciones nucleares de Irán, dañándolas en secreto.

- Impacto: Considerado uno de los primeros ciberataques que tuvo un impacto físico directo. Se cree que retrasó el programa nuclear iraní y es un ejemplo de ciberarma.

3. WannaCry (2017)

- Definición:WannaCry es un ransomware que se propagó rápidamente en mayo de 2017, afectando a cientos de miles de computadoras en más de 150 países.

- Características: Explotaba una vulnerabilidad en sistemas Windows utilizando la herramienta de la NSA llamada EternalBlue. El malware encriptaba los archivos del usuario y exigía un rescate en Bitcoin para desbloquearlos.

- Impacto: El ataque causó interrupciones en servicios de salud, telecomunicaciones y otras infraestructuras críticas, con daños estimados en miles de millones de dólares.

4. NotPetya (2017)

- Definición: NotPetya es un ransomware que se propagó en junio de 2017, inicialmente identificado como una variante de Petya, pero luego se descubrió que su principal objetivo era destruir datos en lugar de obtener un rescate.

- Características: Utilizaba vulnerabilidades similares a WannaCry (como EternalBlue) para propagarse y cifrar las tablas de archivos, haciendo los

sistemas inoperables. El propósito parecía ser la destrucción masiva más que el beneficio económico.

- Impacto: Afectó a empresas en todo el mundo, causando interrupciones significativas y pérdidas financieras, especialmente en Ucrania, donde se originó el ataque.

5. Emotet (2014-2021)

- Definición: Emotet es un malware originalmente diseñado como un troyano bancario que evolucionó para convertirse en una plataforma de distribución para otros tipos de malware, incluyendo ransomware.

- Características: Se propagaba principalmente a través de campañas de correo electrónico de phishing con archivos adjuntos maliciosos o enlaces. Emotet era notable por su capacidad de evadir la detección y actualizarse constantemente.

- Impacto: Fue responsable de numerosos ataques a nivel global, afectando a organizaciones y gobiernos