UNIVERSIDAD DE GUAYAQUIL

INGENIERIA INDUSTRIAL

INGENIERÍA EN SISTEMAS DE INFORMACIÓN

TAREA 2

TÍTULO

VIRUS INFORMATICO LETAL CONOCIDO

ALUMNO:

MADELINE MUÑOZ VILLEGAS

MATERIA:

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

DOCENTE:

ING. OTTO GONZALES MENDOZA

CURSO:

8VO SEMESTRE NOCTURNO

AÑO LECTIVO:

CICLO I

2023-2024

DESARROLLO

Uno de los virus informáticos más notorios es el gusano "Conficker" (también conocido como "Downup", "Downadup" o "Kido"), que se propagó a nivel mundial en 2008. Este gusano infectó millones de computadoras en todo el mundo y fue especialmente efectivo al explotar vulnerabilidades en sistemas operativos sin parches. Aunque no se considera el virus más letal en términos de daño físico o pérdida de vidas, tuvo un impacto significativo en el mundo digital.

El virus Conficker se propagó explotando vulnerabilidades en sistemas operativos de Windows y aprovechando contraseñas débiles o predeterminadas. Desactivaba las defensas de seguridad, bloqueaba el acceso a sitios web de seguridad y permitía a los atacantes tomar control remoto de los sistemas infectados.

Según Demurtas (2020) en su articulo explica que durante el periodo comprendido entre finales de 2008 y todo el año 2009, se produjo una extensa propagación del virus Conficker, también conocido como Downup, que logró infectar una cantidad significativa de computadoras con el sistema operativo Microsoft Windows. Esta infección generó problemas en el rendimiento de diversos sistemas, llegando incluso a afectar el funcionamiento de buques pertenecientes a la Marina británica y del Parlamento de Londres.

Entonces en respuesta a las amenazas de este ataque cibernético, las organizaciones y los gobiernos han implementado diversas estrategias y planes de contingencia. Estos pueden incluir:

Mantenimiento de sistemas actualizados: Las organizaciones y los gobiernos suelen priorizar la aplicación de parches y actualizaciones de seguridad en sus sistemas operativos y software para mitigar vulnerabilidades conocidas.

Implementación de soluciones de seguridad: Se utilizan firewalls, sistemas de detección de intrusiones, software antivirus y otras herramientas de seguridad para prevenir y detectar posibles amenazas.

Educación y concienciación: Se realizan campañas de sensibilización y capacitación para que los empleados y usuarios finales estén al tanto de las mejores prácticas de seguridad cibernética, como la importancia de no abrir archivos adjuntos sospechosos o hacer clic en enlaces no verificados.

Respuesta y recuperación ante incidentes: Las organizaciones y los gobiernos establecen planes de respuesta ante incidentes cibernéticos, que incluyen la identificación temprana de amenazas, la contención de los ataques, la recuperación de sistemas y la investigación forense para identificar a los responsables.

Para protegerse contra Conficker y otros virus informáticos similares, es fundamental mantener actualizado el sistema operativo y el software con los últimos parches de seguridad, utilizar contraseñas fuertes y únicas, contar con una solución antivirus actualizada y evitar la ejecución de archivos adjuntos o enlaces de fuentes no confiables.

Referencias

Demurtas, A. (2020). *La Evolución normativa de la ciberseguridad en la Unión Europea y su impacto político a nivel de actores, objetivos y recursos.* Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=8696947