Universidad de Oviedo

Estudio Caso Ético

Caso 2: Anti-Worm

Omar Teixeira González

UO281847

Pelayo Reguera García

UO282348

ASLEPI

Tabla de contenidos

Introducción

En el caso asignado, se describe la propagación de un gusano informático a través de Internet que aprovecha una vulnerabilidad de seguridad en un sistema operativo, comúnmente utilizado en PCs, para el que Chris Smart desarrolla un *anti-gusano* que explota la misma vulnerabilidad en estas máquinas con el objetivo de ejecutarse y propagarse, pero con la particularidad de descargar un parche que protege el sistema contra el gusano original.

De esta forma, Chris lanza su *anti-gusano* tomando precauciones, con el objetivo de que no sea rastreable, se propaga por Internet consumiendo grandes cantidades de ancho de banda e instalándose en millones de computadoras. Sin embargo, los administradores de sistemas lo perciben simplemente como otro gusano más y acaban por bloquearlo de la misma manera con la que se hacía con el gusano original.

Artículos relevantes

1.01. Aceptar completa responsabilidad por su trabajo.

En la elaboración de su programa antimalware concebido como no rastreable, Chris incurre en un incumplimiento de esta disposición del código, al llevar a cabo dicha tarea de manera anónima. En virtud de esta circunstancia, en caso de presentarse una denuncia, carecería de identificación personal o entidad específica a la cual atribuir la responsabilidad correspondiente.

1.03. Dar el visto bueno al software sólo si se tiene fundada creencia de que es seguro, cumple las especificaciones, ha pasado las pruebas pertinentes y no disminuye la calidad de la vida, disminuye la confidencialidad o daña al medio ambiente. El efecto último del trabajo debiera ser el bienestar público.

La divulgación del programa de manera anónima e independiente sugiere implícitamente que no se han llevado a cabo pruebas exhaustivas. Además, al persistir en su propagación mediante el mismo método que el gusano original, se incumplen los requisitos fundamentales de confidencialidad y seguridad. Este enfoque podría potencialmente dar lugar a futuras vulnerabilidades adicionales para el usuario destinatario.

1.04. Mostrar a las personas o autoridades correspondientes cualquier peligro real o potencial para el usuario, la sociedad o el medio ambiente, que consideren, de manera razonable, que esté asociado con el software, o documentos relacionados.

La omisión por parte de Chris de proporcionar información detallada sobre el funcionamiento del software, al seguir la estructura del gusano original, conlleva la falta de divulgación de la vulnerabilidad explotada. Este vacío informativo constituye un riesgo potencial para el usuario y obstruye la posibilidad de abordar y corregir la vulnerabilidad de otras maneras. La transparencia en cuanto a la naturaleza de la amenaza sería esencial para implementar medidas efectivas de seguridad y mitigación.

1.05. Cooperar en las materias relacionadas con las preocupaciones graves causadas por el software, su instalación, mantenimiento, soporte o documentación.

Una vez más, la ejecución anónima y la explotación de la vulnerabilidad en lugar de abordar su corrección representan una transgresión al código ético. La ausencia de informes sobre la instalación del programa antimalware repercute negativamente en el mantenimiento y soporte del software instalado. Además, la carencia de cualquier referencia a la documentación pertinente obstaculiza la comprensión adecuada y el manejo eficaz de la herramienta por parte de los usuarios, contribuyendo así a una falta de claridad y transparencia en el proceso.

3.06. Trabajar para seguir los estándares de la industria, si disponibles, que sean los más adecuados para las tareas, desviándose de los mismos sólo cuando esté justificado ética o técnicamente.

La omisión de seguir los estándares éticos se evidencia al llevar a cabo la instalación mediante la explotación de la vulnerabilidad, sin esperar la confirmación del usuario afectado por dicha vulnerabilidad. A pesar de que la intención original sea corregir los problemas ocasionados por el gusano original, es importante reconocer que estas prácticas podrían variar en el futuro. Además, es crucial destacar que la vulnerabilidad en cuestión aún no ha sido abordada, lo que plantea preocupaciones adicionales en términos de seguridad y estabilidad del sistema.

3.11. Garantizar una adecuada documentación, incluyendo problemas significativos descubiertos y las soluciones adoptadas, para cualquier proyecto en el que trabajen.

La ausencia de referencia a la documentación en el desarrollo del programa antimalware, sumada al hecho de que dicho desarrollo se llevó a cabo de manera individual y sin comunicación previa, sugiere la posibilidad de que la documentación sea inexistente o limitada. Este aspecto plantea inquietudes significativas en cuanto a la capacidad de comprensión y manejo del software, así como a la transferencia de conocimientos a otros posibles colaboradores o usuarios. La elaboración de una documentación exhaustiva se revela como un componente esencial para garantizar la eficacia, la transparencia y la continuidad del proyecto.

6.06. Obedecer todas las leyes que gobiernen su trabajo, a menos que, en circunstancias excepcionales, tal cumplimiento sea inconsistente con el interés general.

El incumplimiento de las leyes se manifiesta al obviar la decisión del usuario en lo que respecta a la instalación, agravado por las prácticas previamente mencionadas de llevar a cabo la implementación de manera anónima y aprovechando la vulnerabilidad inherente al gusano original. Esta falta de respeto hacia la autonomía del usuario representa una violación de los principios legales que rigen la privacidad y el control del individuo sobre su sistema. Es imperativo que las acciones emprendidas respeten y se ajusten a las normativas vigentes para preservar la legalidad y la integridad del proceso.

Conclusión

En lugar de realizar un *anti-gusano* que explotase esa vulnerabilidad, se deberían de haber realizado las siguientes acciones.

- Informar de la vulnerabilidad encontrada.
- Solucionarla o proponer una solución en la medida de lo posible.
- En caso de seguir con el método del *anti-gusano* (no sería lo óptimo), informar al usuario de la instalación y los correspondientes "beneficios" que esto conllevaría.
- Ofrecer una documentación y soporte con respecto a lo desarrollado.

Bibliografía

1. Dolado, J. (s. f.). El Código de Ética de Ingeniería del software. (13 de febrero de 2019). http://www.sc.ehu.es/jiwdocoj/elcodigo.htm
2. CCII. (s. f.). Código ético y deontológico de la Ingeniería Informática. Consejo de Colegios de Ingeniería Informática. (13 de febrero de 2019). https://ccii.es/CodigoDeontologico