UNA UNIVERSIDAD NACIONAL COSTA RICA
DTIC Dirección de Tecnologías de Información y Comunicación

BOLETÍN DTIC

21 de julio de 2022
Boletín 7
dtic@una.cr

Noticias, comentarios y anuncios tecnológicos

En esta edición:

¿Qué es un Hacker?

La Real Academia Española indica que la palabra "hacker" corresponde a una definición de "pirata informático". Un "pirata informático" es definido como una "persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta".

Adicionalmente, se refiere al mismo término como una "persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora."

Por lo anterior, podemos observar que el término "hacker" no siempre se refiere a una "persona mala o un bandido", tal como se detalla a continuación:

Un hacker de "**sombrero blanco**" o "**hacker ético**" es un experto en seguridad informática, que se especializa en buscar vulnerabilidades o fallas de seguridad en sistemas y plataformas de comunicación.

Un hacker de "**sombrero negro**" son generalmente ciberdelincuentes, que atacan sistemas informáticos con el fin de causar daños, provocando la interrupción de los servicios tecnológicos, así como el robo de información.

Un hacker de **"sombrero gris"** es una persona que ataca sin permiso sistemas informáticos con el fin de detectar problemas de seguridad en estos, ofreciendo posteriormente sus servicios para solventar estas debilidades. Se considera como un punto medio de los dos términos anteriores.

Malware – Parte 4

Malware de criptominado

Este software malicioso se instala en un dispositivo tipo "endpoint" sin autorización del usuario, y se dedica sin su conocimiento a llevar actividades de criptominado.

El criptominado aparece en el año 2017, y es el proceso mediante el cual se utiliza el poder de procesamiento de un computador a través de su CPU, para poder llevar a cabo miles de operaciones dirigidas a resolver un reto o ecuación matemática, que recompensa este esfuerzo con la asignación de una criptomoneda.

Un solo computador portátil o de escritorio no puede llevar a cabo por sí misma este tipo de procesos, pero cientos o miles de computadores infectadas trabajando de forma coordinada podrían lograrlo.

Bombas lógicas

Una bomba lógica es un malware que permanece "dormido" en nuestro computador, y llega a ejecutarse o a "explotar" una vez que se cumplan una serie de condiciones predeterminadas o programadas con antelación.

En términos generales: evite la instalación de software desconocido, utilice herramientas antimalware, y ponga atención a cualquier comportamiento anómalo de su computador.

¿Qué es un XDR?

Un XDR (Extended Detection and Response) o software de Detección y Respuesta Extendidas, es una nueva solución de protección para "endpoints" o dispositivos informáticos de usuario final, tales como computadores, teléfonos inteligentes, tabletas, etc.

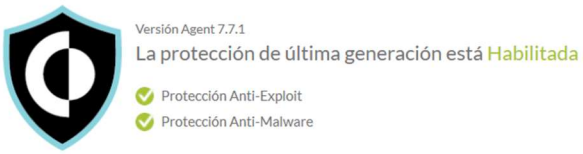
El XDR es la evolución del software del tipo EDR (Endpoint Detection and Response).

Consulte el Boletín 5 para retomar los conceptos de Endpoint y EDR.

El software de protección tipo EDR trabaja en muchas ocasiones con bases de datos que reconocen miles de patrones de malware conocidos, tales como virus, troyanos, gusanos, etc.

Sin embargo, las amenazas informáticas son cada vez más complejas y difíciles de detectar, por lo que los EDR a pesar de ser bastante funcionales, pueden fallar o dejar de detectar algún comportamiento anómalo en algún momento.

Por lo anterior, un software XDR es una solución avanzada para la detección de amenazas de seguridad; que recoge y correlaciona actividad de riesgos informáticos de varas capas, a saber: computadores en general, servidores, servicios en la nube, correo electrónico, redes de datos y otras.



Representación de software XDR para Windows

Las soluciones XDR comparten sus hallazgos en infraestructuras de nube, lo cual hace posible informar de patrones de actividad maliciosa detectadas a nivel mundial.

Por su complejidad, la utilización de soluciones XDR tiene un costo económico mayor para las organizaciones en general.