PROYECTO: Sistema de Detección de Código malicioso - ransomware

Resumen Técnico

Recientemente un tipo particular de software malicioso está afectando a muchos usuarios en todo el mundo, éste es denominado ransomware (del inglés ransom, "rescate", y ware, por "software"). Se trata de un malware que cifra todos o gran parte de los archivos del sistema de archivos de la computadora infectada y luego ofrece la clave para desencriptar los datos sólo si el usuario realiza una transferencia de dinero a la cuenta de los atacantes. Generalmente esta cuenta, es una billetera digital de Bitcoin. Para lograr su objetivo, el ransomware se instala en las víctimas generalmente mediante un archivo infectado enviado a través de correo electrónico, un sitio web comprometido o aprovechando vulnerabilidades del sistema operativo. Luego abre cada archivo (o algunos de ellos), los encripta, los guarda y por último borra los archivos originales. Normalmente, los ransomware usan cifrado simétrico para encriptar los archivos con una clave generada aleatoriamente y luego cifra esta clave usando cifrado asimétrico. Existen diferentes técnicas y herramientas para mitigar este tipo de ataques tanto en forma proactiva como reactiva. Una de las mejores maneras (y la más recomendada por los especialistas en seguridad informática) es la generación de backups y mantenerlos en un sitio donde no sean alcanzables a través de este tipo de malware (por ejemplo, apartados de la red de trabajo diaria). Ésta es una práctica proactiva que lamentablemente no suele ser tan frecuente entre las organizaciones y menos aun de usuarios independientes. Otra medida proactiva es tener usuarios con mínimos privilegios logrando así que el ransomware afecte solo a los archivos que tenga permisos para ser modificados. En este proyecto se busca desarrollar un sistema que se acople con el sistema operativo para detectar la ejecución de un ransomware y poder bloquearlo. Esta técnica es reactiva pero permite mitigar el problema en casos que los atacantes hayan logrado ingresar como usuario con elevados privilegios como administrador. Este estilo de malwares se está ejecutando permanentemente generando un consumo alto de recursos, dando como resultados una actividad del procesador excesiva debido a la ejecución de algoritmos de cifrado y también la escritura/lectura a disco. Es posible definir estos indicadores como patrones en los procesos del sistema para tenerlos en cuenta para la detección. De esta manera, el ransomware sólo afectaría unos cuantos archivos y no todo el sistema de archivo permitiendo salvar la mayor cantidad de archivos posibles.

Autores:

Gastañaga, Iris
Gibellini, Fabián Alejandro
Frias, Pablo Sebastián; Ruhl, Analía Lorena; Ciceri, Leonardo Ramón; Parisi, Germán Nicolás; Zea Cardenas, Milagros; Bertola, Federico; Olmedo, Paula Beatriz

Duración: Inicio: 01/01/2018 - Fin: 31/12/2019