Módulo de cifrado para un ramsomware

Objetivo

Que el alumno ponga en práctica los conocimientos de cifrado simétrico y asimétrico, y conozca el proceso que lleva a cabo un ransomware para “secuestrar” la información de un objetivo.

Actividades a desarrollar

1. El sistema deberá de funcionar en un sistema Windows 10. No es necesario escalar privilegios, es decir, se podrá ejecutar con permisos de administrador.
2. Se realizará un *Dropper* que al momento en que el usuario ejecute el señuelo, se inicien las acciones maliciosas. El *Dropper* podrá contener todos los archivos necesarios (programa, la llave pública con la que se cifrará la llave AES, bibliotecas, etc.) para que el módulo de cifrado funcione correctamente, o sólo tendrá una instrucción para descargar esos archivos, es decir, hará las funciones de un *Downloader*.
3. Se deberá instalar automáticamente en el sistema objetivo todas las bibliotecas y programas necesarios para la correcta ejecución del módulo.
4. El módulo contendrá como mínimo, el archivo ejecutable que llevará a cabo las acciones maliciosas.
5. Una vez que el usuario ejecute el módulo, el ejecutable se copiara en la ruta %WINDIR%\system32.
6. El módulo cifrará los archivos que tengan las siguientes extensiones .docx, .xlsx, .pdf, .jpeg y .jpg. Y que se encuentren en el directorio %UserProfile%\Documents. Una vez cifrados, se borrarán de forma segura los archivos originales.
7. Los archivos serán cifrados con una llave aleatoria AES-256 en un modo de operación seguro
8. La llave AES-256 se cifrará con la llave pública RSA-2048, y para este proyecto se guardará en un archivo dentro del mismo sistema. Una vez cifrada, se sobreescribirá en la RAM la llave AES-256.
9. Mostrar en el escritorio del sistema objetivo una imagen en donde indique que los archivos han sido cifrados, y que se requiere un pago para poder “rescatarlos”, así como una *wallet* de una criptomoneda para que se realice el depósito.
10. Crear un programa independiente que realice el descifrado de los archivos, simulando que se pagó el rescate por ellos.
11. 2 puntos extra sobre el proyecto si además se instala un minador de una criptomoneda. Elegir una criptomoneda a usar, generar una *wallet* y conectarse a una *pool*. Configurar los parámetros del software de minado con esos datos.
12. Se realizarán las pruebas de funcionamiento del módulo en una máquina virtual con Windows 10, si así lo consideran, el equipo podrá proporcionarla.
13. Elaborar una memoria técnica detallada sobre el proceso.

Indicaciones adicionales

1. El proyecto se podrá realizar en equipo de máximo 3 integrantes.
2. La fecha de entrega será para el 29 de mayo.
3. Se entregará tanto el código fuente, como el ejecutable para Windows.
4. El ejecutable deberá de estar comprimido en zip con la contraseña `1nf3ct3d`.

Referencias

- Cryptocurrency Wallet Guide: A Step-By-Step Tutorial
  https://blockgeeks.com/guides/cryptocurrency-wallet-guide/
- Bitcoin Wallet
  https://en.bitcoin.it/wiki/Wallet
- CPUMiner-Multi
  https://github.com/tpruvot/cpuminer-multi
- Operacion Groundbait: Análisis de un kit de herramientas para espionaje cibernético
  https://www.welivesecurity.com/wp-content/uploads/2016/05/Operacion-Groundbait.pdf

Facultad de Ciencias UNAM

Universidad Nacional Autónoma de México

Paulo Contreras Flores
paulo.contreras.flores@ciencias.unam.mx