Exemple de ransomware

Ransomware

Una Visió General

Ransomware és un tipus de **malware** (software maliciós) dissenyat per bloquejar o restringir l'accés als arxius o sistemes d'un usuari, generalment mitjançant la **xifrat** de les dades, per després exigir un pagament o rescat (ransom) a canvi de restaurar-ne l'accés. Aquest pagament sol sol·licitar-se en criptomonedes, com Bitcoin, per dificultar el rastreig.

Funcionament del Ransomware

El ransomware típicament segueix un cicle d'atac que involucra diverses fases:

1. **Infecció inicial**: El ransomware ingressa al sistema, generalment a través de vectors com **phishing** (correus electrònics maliciosos amb enllaços o arxius adjunts), descàrregues no segures, vulnerabilitats en sistemes o xarxes, o mitjançant atacs enginyeria social.
2. **Xifratge de dades**: Un cop dins del sistema, el ransomware xifra arxius importants al disc de l'usuari usant algoritmes de xifrat forts com **AES** o **RSA**. Això impedeix que l'usuari accedeixi a les vostres dades, ja que només l'atacant té la clau per desxifrar la informació.
3. **Missatge de rescat**: Apareix una notificació exigint un pagament a canvi de la clau de desxifrat. L'atacant sovint imposa un límit de temps per generar una sensació d'urgència, amenaçant de destruir les dades si el pagament no es fa.
4. **Possible doble extorsió**: En atacs més recents, a més de xifrar les dades, els atacants també amenacen de **publicar la informació robada** si no es paga el rescat, afegint-hi una segona capa d'extorsió.

Ransomware i C2 (Command and Control)

Els atacs de ransomware sovint depenen de servidors **C2 (Command and Control)**, que són utilitzats pels atacants per controlar el malware remotament i rebre instruccions.

C2 al Context del Ransomware

1. **Comunicacions**: El ransomware es pot connectar a un servidor C2 per rebre instruccions específiques, com ara el moment en què s'ha d'activar, quins fitxers ha de xifrar, o quines

criptomonedes enviar els pagaments.

2. **Distribució de claus**: En alguns casos, les claus de xifratge són generades al servidor C2, i el ransomware les sol·licita quan infecta un sistema. Això assegura que només el servidor C2 i els atacants tinguin la clau de desxifrat, fent impossible que la víctima desxifre els fitxers sense pagar.
3. **Exfiltració de dades**: Si el ransomware inclou la doble extorsió (robatori de dades a més de xifratge), el C2 també és responsable de rebre les dades exfiltrades abans que el ransomware les xifre localment.
4. **Actualització o control dinàmic**: Alguns ransomware poden estar programats per rebre actualitzacions des del servidor C2, cosa que permet als atacants modificar el comportament del malware segons sigui necessari (per exemple, per evitar detecció).

Corolari

El **ransomware** és una de les amenaces més destructives dins de l'ecosistema del malware**. La seva capacitat per inutilitzar dades crítiques, combinada amb l'ús de sistemes de** C2** per al control remot, el fa molt efectiu i difícil de combatre. Els atacants utilitzen tècniques avançades de xifratge per segrestar informació i utilitzen mètodes sofisticats de distribució a través de servidors C2, cosa que els permet mantenir el control i maximitzar l'impacte dels seus atacs.

Simulació d'un escenari real d'un atac de Ransomware

Objectiu

Volem simular en primera persona un atac de ransomware a una empresa i observar el procés. Per a aquest comès utilitzarem com a màquina atacant ***Kali***, que també farà de servidor C2.

Simularem un escenari amb una víctima Windows 10 i un altre amb una víctima Linux (Rocky). Utilitzarem un senzill software que xifrarà tot el contingut d'un directori, deixant-lo il·legible. De la mateixa forma, enviarà la clau per a desxifrar i els arxius sense xifrar al nostre server C2.

Per a prevenir execucions d'aquesta eina per error, també es genera en la víctima un `readme.txt` que conté els logs de la execució i la clau de desxiframent. Està clar que en un escenari real això no pasaría mai sinò que es demanaría un rescat.

1. Primer escenari: Atacant (Kali) + Víctima (Windows 10)

La eina que utilitzarem està escrita en Powershell que, encara que és multiplataforma, haurem d'instalar-lo en Kali:

```
sudo apt update && sudo apt upgrade

# Instal·lem dependències
sudo apt install -y wget apt-transport-https software-properties-common

# Importem les claus de Microsoft
wget -q "https://packages.microsoft.com/keys/microsoft.asc" -O- | sudo tee
/etc/apt/trusted.gpg.d/microsoft.asc

# Afegim el repository de powershell a Kali
sudo sh -c 'echo "deb [arch=amd64]
https://packages.microsoft.com/repos/microsoft-debian-buster-prod buster main"
> /etc/apt/sources.list.d/microsoft.list'

#Actualitzem i instal·lem powershell
sudo apt update

sudo apt install -y powershell
```

Per a iniciar un terminal de Powershell no cal més que: `pwsh`

En la màquina atacant clonem el repositori de l'eina que farem servir

```
git clone https://github.com/JoelGMSec/PSRansom
```

El mateix repositori ho clonarem en la víctima Windows. Podeu fer-lo instal·lat **Git** en Windows o simplement descarregant un zip amb el contigut del repositori i descomprimint-lo en la màquina.

> **Atenció**
>
> És més que probable que hàgiu de desactivar la protecció antimalware de Windows per a fer servir els scripts de Powershell d'aquesta eina.

Ara que ja teniu el *setup* comencem amb l'acció:

- En un terminal de Powershell en l'atacant, posa a l'escolta en el port 80 el servidor C2. Per a saber com fer-lo, utilitza l'ajuda de la eina: `./C2Server.ps1 -h`

  > **Tip**
  >
  > Utilitza permisos de `sudo` o no et deixarà

- En la màquina víctima crea un directori que es cride SAD i fica una imatge, un arxiu de text **amb contingut** i qualsevol altre arxiu.
- En un terminal de Powershell (executant-se com Administrador), inicia el Ransomware.

  Hauràs d'indicar-li el directori, l'adreça del servidor C2 i el port en el que està escoltant. A més, hauràs d'utilitzar la opció per a exfiltrar arxius, de tal forma que se transmetin a l'atacant i es guarden sense xifrar allà.

  Per a saber com fer-lo, utilitza l'ajuda de la eina: `./PSRansom.ps1 -h`

  > ✗ **Failure**
  >
  > Aquest pas et donarà un error que t'informarà de l'execució de scripts està deshabilitada en el sistema. PowerShell té diverses polítiques d'execució, quatre de les més utilitzades són:
  >
  > - **Restricted**: cap script no serà executat. Com es comentava anteriorment, aquesta és la configuració predeterminada.
  > - **RemoteSigned**: permeten executar els scripts creats localment amb signatura remota. Els scripts que es van crear en una altra màquina no s'executaran a no ser que estiguin signats per un editor de confiança.
  > - **AllSigned**: els scripts només s'executaran si està signat per un editor de confiança. Aquí també s'hi inclouen els scripts creats localment.
  > - **Unrestricted**: tots els scripts s'executaran, tant se val qui els hagi creat i si estan signats o no.
  >
  > **Decideix quina és la política adequada per al nostre cas i busca en Internet el comandament adequat de Powershell per a establir-la.**

- Una vegada executat exitosament `PSRansom.ps1`, començarà la simulació de la infecció i es conectarà amb el C2, xifrarà els arxius del directori i exfiltrarà la informació.
- En la víctima s'informarà de la conexió, es rebrà la clau de desxifrat i es rebran els arxius desxifrats per, a continuació, desxifrar-los i guardarlos.

> **Task**
>
> - Comprova que tots els arxius del directori han sigut xifrats. Tots tenen extensió `.psr` i no es poden obrir.
> - Trobaràs un arxiu `readme.txt` informant-te de l'atac, amb els logs de què ha sigut xifrat i amb la clau de desxifrat (per si ha sigut una simulació accidental)
> - Comprova quen el servidor C2 s'ha rebut la clau i els arxius.
> - Utilitzant una altra vegada l'ajuda de la eina, desxifra els arxius xifrats en la màquina víctima.

2. Segon escenari: Atacant (Kali) + Víctima (Rocky)

En aquest cas, haurem d'instal·lar Powershell en Rocky també:

```
sudo dnf update

sudo dnf install -y https://packages.microsoft.com/config/rhel/8/packages-microsoft-prod.rpm

sudo dnf install -y powershell

pwsh
```

Y després repeteix exactament el mateix procés que en el cas anterior.

Per a treure nota

Imagina en aquest últim cas que no contem amb la clau de desxifrat, lo qual s'apropa bastant a la realitat. En aquestos casos és esencial una cosa que ja vam vore amb anterioritat; una bona política de backups.

> **Tasca**
>
> Repeteix el segon escenari pero abans fes un backup del contingut del directori amb *rsync* a una altra màquina qualsevol. Simula l'atac y restaura aquesta còpia. D'aquesta forma simulem tant l'atac com la resposta mateixa.

Forma de lliurament

Haureu de lliurar els següents vídeos, un per a cada escenari:

- Un vídeo a on s'observe tot el procediment del primer escenari
- Un vídeo a on s'observe tot el procediment del segon escenari
- Si feu la part Per a treure nota podeu incloure-la directament en el primer vídeo. Es a dir, en el primer vídeo haureu de restaurar el backup però també desxifrar els arxius xifrats.