Universitat Oberta de Catalunya

uoc.edu

Cibercrimen: Ransomwares

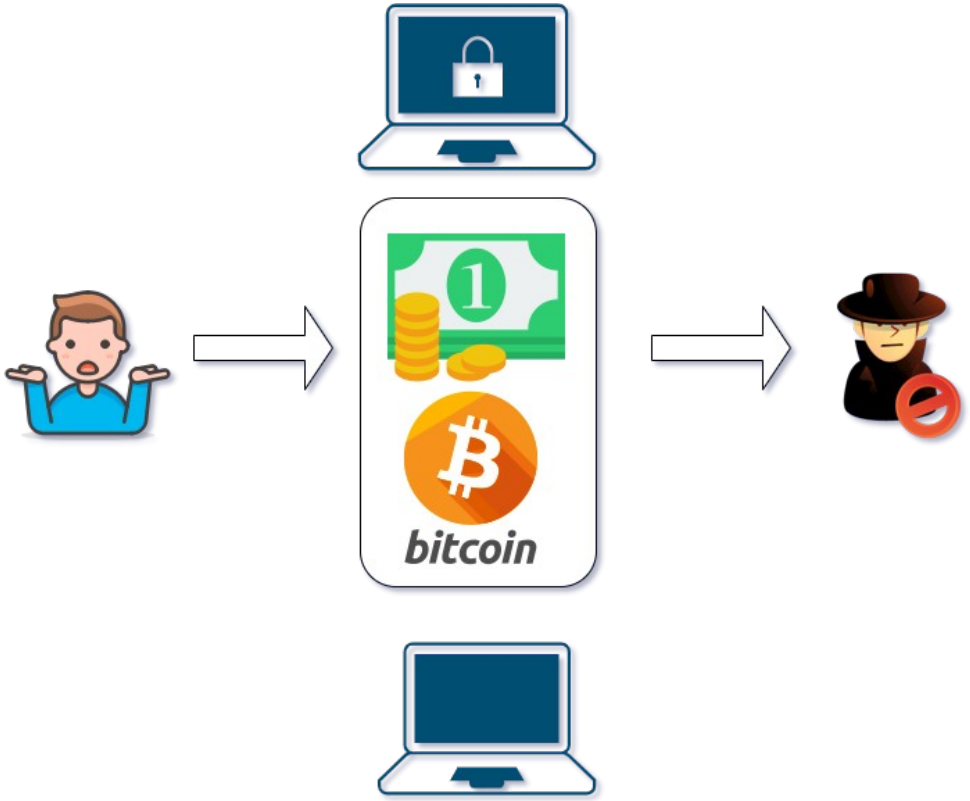
Máster Interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones (MISTIC)

Presentado por: Armando Antonio Nieto Hernández

Universitat Oberta
de Catalunya

Contenido

Ransomware: Definición



Ransomware: Características

Es un tipo de Malware

Por lo que hereda mucho de sus características principales

Persistencia

Se mantiene en el equipo, a pesar de reiniciarlo.

Canales de infección

E-mail, sitios web comprometidos, aplicaciones maliciosas, entre otros.

Se expande

Infectado un equipo, ésta busca expandirse a otros en de la misma red.

Secuestro de datos

Cifra los datos para exigir un rescate a cambio de desbloquearlos.

Ransomware: Tipos

1. ScreenLocker.
2. Browser ransomware.
3. Crypto ransomware.
4. Ransomware orientado a una infraestructura específica.
5. Boot ransomware.
6. Ransomware para la nube.
7. Ransomware para smartphones.
8. Ransomware para IoT (RoT).

Vectores de Infección

1. Adjuntos en correo electrónico.
2. Enlaces embebidos en documentos.
3. Enlaces en el cuerpo del correo electrónico.
4. Descarga de archivos.
5. Sitios web comprometidos.
6. Unidades de almacenamiento externas.
7. Exploit Kits
8. Equipos débilmente protegidos.

Modelo de Negocios

1. Satan
2. Philadelphia
3. MacRansom
4. Stampado
5. RaaSberry

Estrategias de Prevención

Nivel 1

Establecer una política de seguridad a nivel de TI

Nivel 2

Seguridad física y del entorno

Nivel 3

Defesan perimetral

Nivel 4

Protección de la red Interna

Nivel 5

Protección de aplicaciones

Nivel 6

Protección de datos

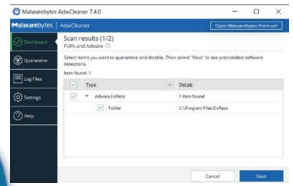
Nivel 7

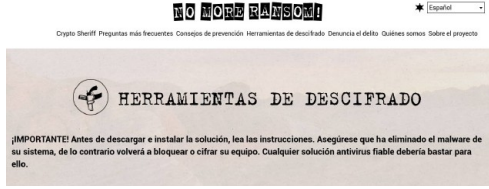
Protección de equipos

Recuperación de Desastres

1. Copia de respaldo

2. Tratar de descifrar la información

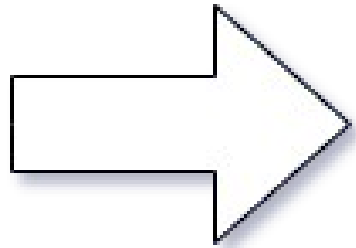




IoT

Impactos Legales

Acciones de Empresas Antivirus



Campaña notable: Ryuk Ransomware

RyukReadMe.txt - Notepad

File Edit Format View Help

```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvu1zjg67wt86dhYqNj

Ryuk
No system is safe
```

Campaña notable: Ryuk Ransomware

Wizard Spider

Controlan el malware Trickbot.

Emotet + TrickBot + Ryuk

Grim Spider

Controlan el ransomware Ryuk.

Campaña notable: Ryuk Ransomware

1. Se detiene software de seguridad instalado (antimalware).
2. Instala una versión adecuada según la arquitectura objetivo.
3. Depende de una infección primaria para desplazarse en la red.
4. Enumera los recursos de red compartidos.
5. Cifra los recursos a los que logra tener acceso.

Conclusiones

1. Una amenaza real y de las más peligrosas hoy en día, a la vez muy rentable para ciberdelincuentes.
2. Las soluciones Antivirus no son suficientes.
3. Todos estamos expuestos, independientemente del sistema operativo o dispositivo que utilicemos.
4. Es necesario homologar diferentes legislaciones para un combate más efectivo contra toda clase de delitos cibernéticos.

¡Muchas Gracias!