Crypto-Refuse
La venganza del Sysadmin

Security Consultant

MVP Enterprise Security

https://www.nccgroup.trust

Juan.garrido@nccgroup.trust

Twitter: @tr1ana

Índice

Crypto-Malware

Descripción

- Software malicioso
  - Restringe el acceso al equipo
  - Restringe acceso a los datos almacenados en el OS
  - Restringe el acceso al código fuente
- Cifrado
  - Desde sus inicios, este tipo de variantes destaca por hacer uso de avanzados sistemas criptográficos como RSA y AES
- Exige un pago a modo de rescate para desbloquear el acceso

Crypto-Malware

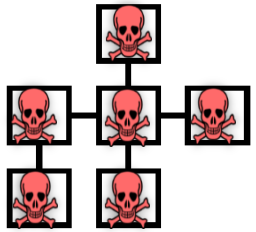
Crypto-Malware

Variantes

- En la actualidad existen decenas de variantes, entre las que se incluyen:

Dirty decrypt	Chimera
CryptoLocker	TeslaCrypt
Cryptowall	Shade
Citroni	CoinVault
Cryptographic Locker	Rannoh
Wildfire	Rakhni
TorrentLocker	Locky
Samas	Etc..

Crypto-Malware



- Que a una organización le cifren datos puede no ser “casual”

- El número y el tipo de ficheros objetivo continúa en aumento
  - Las últimas muestras analizadas cifran
    - Ficheros de tipo CAD (Diseño)
    - Ficheros de BBDD (MDB)
    - Ficheros ofimáticos (DOCX, XLSX, PDF…)
    - Ficheros de tipo FIN (Financieros?)

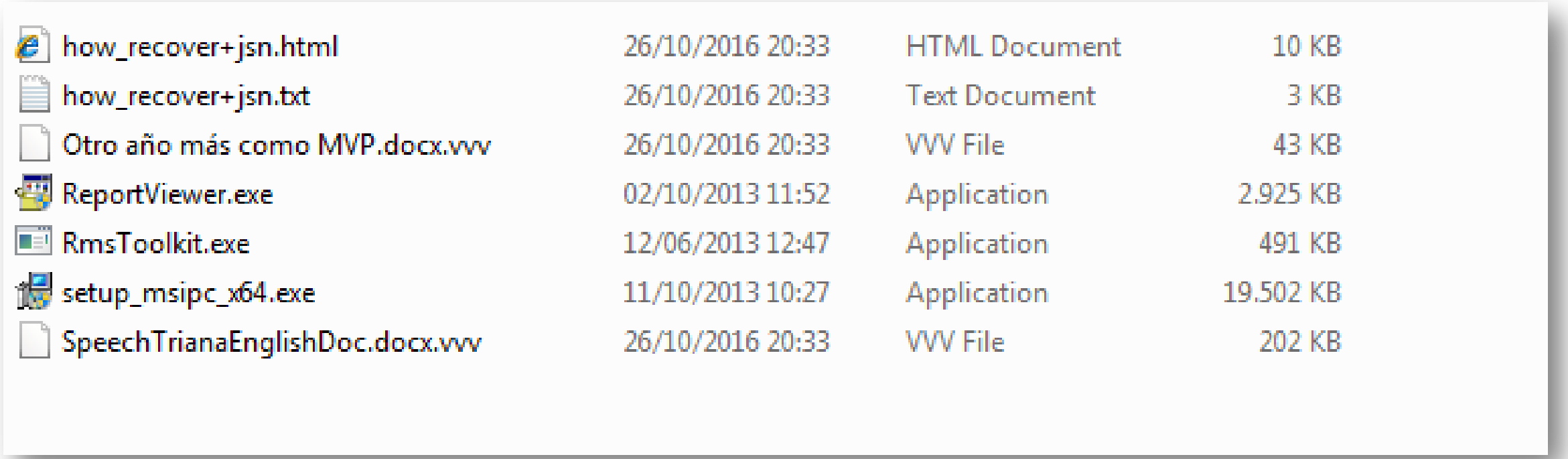
Crypto-Malware

Extensiones

- Primeras versiones no cifraban las extensiones de los ficheros
- Últimas versiones cifran las extensiones de los ficheros
- En función de la versión se cifrará con una extensión u otra
  - ZZZ
  - YYY
  - VVV
  - Etc..

Crypto-Malware

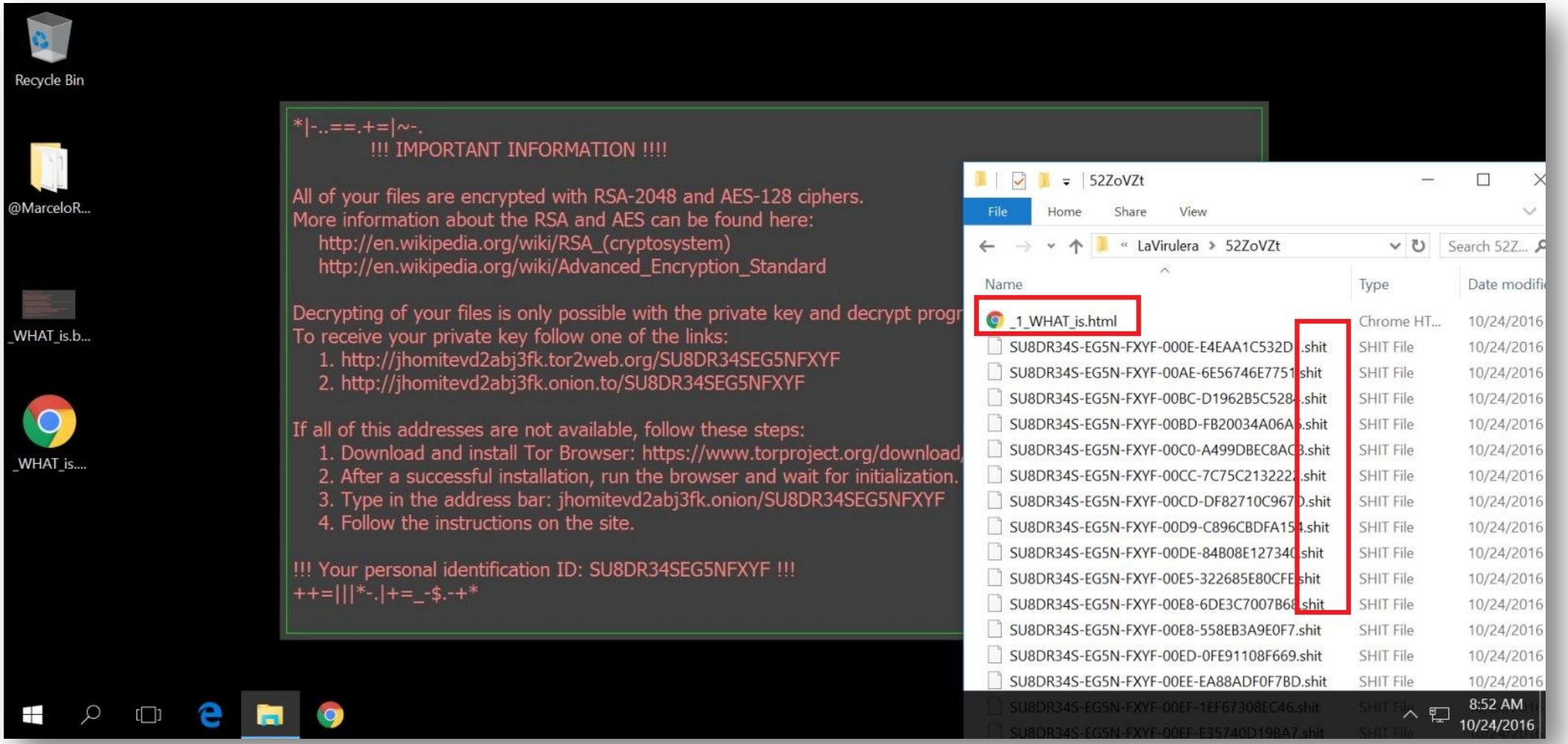
Extensiones



how_recover+jsn.html	26/10/2016 20:33	HTML Document	10 KB
how_recover+jsn.txt	26/10/2016 20:33	Text Document	3 KB
Otro año más como MVP.docx.vvv	26/10/2016 20:33	VVV File	43 KB
ReportViewer.exe	02/10/2013 11:52	Application	2.925 KB
RmsToolkit.exe	12/06/2013 12:47	Application	491 KB
setup_msipc_x64.exe	11/10/2013 10:27	Application	19.502 KB
SpeechTrianaEnglishDoc.docx.vvv	26/10/2016 20:33	VVV File	202 KB

Crypto-Malware

Y por supuesto….



Crypto-Malware

Algunas notas

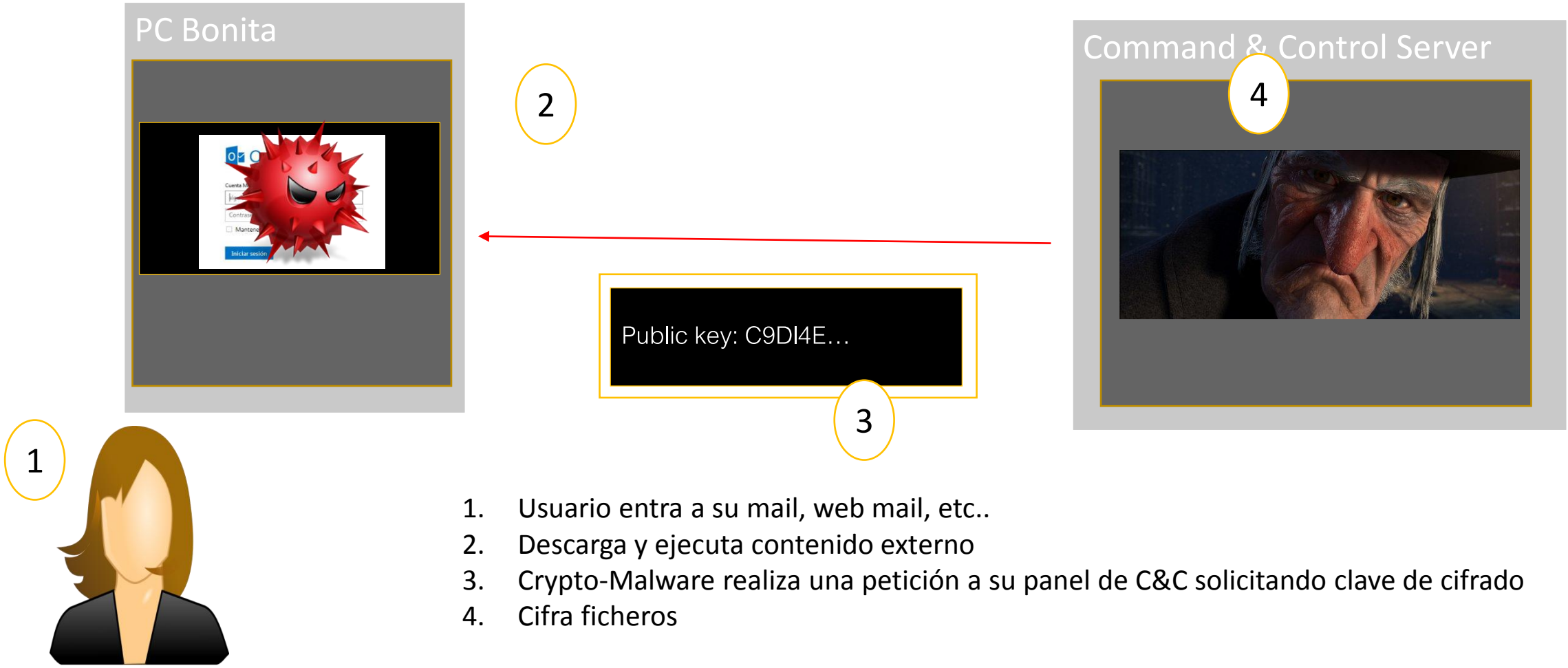
- Diferente frente a otro tipo de amenazas
  - No oculta sus acciones, tal y como lo haría un Troyano o Rootkit
  - En casi todos los casos el Malware hace imposible al usuario el acceso a sus datos
  - Fácil para el desarrollador
    - Implementación de cifrado en todos los lenguajes de programación
    - Muy bien documentadas
    - De fácil implantación

Crypto-Malware

Métodos de infección

- Este tipo de versiones se caracteriza por infectar sistemas mediante las siguientes metodologías:
  - SPAM
  - Ingeniería social
  - Malvertising
  - Botnets

How it works?



1. Usuario entra a su mail, web mail, etc..
2. Descarga y ejecuta contenido externo
3. Crypto-Malware realiza una petición a su panel de C&C solicitando clave de cifrado
4. Cifra ficheros

Crypto-Malware

Primera ejecución

- Versiones modernas de este tipo de amenazas realizan varias tareas en el equipo antes de infectarlo:
  - Destruyen todo tipo de copias de seguridad
    - vssadmin.exe Delete Shadows /All /Quiet
  - Deshabilitan la recuperación del sistema
    - Reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v DisableSR /t REG_DWORD /d 1 /f
  - Deshabilitan el “modo de recuperación”
    - bcdedit /set {default} recoveryenabled No
  - Determinadas versiones cifran el MBR (Master Boot Record)

You had bad luck.There was crypting of all your files in a FS bootkit virus
<!SATANA!>
To decrypt you need send on this E-mail: orjovaja@mail.com
your private code: C98F4DEC6A78B1A714D0FD416A61248B and pay on
a Bitcoin Wallet: Xqz5WKhkQJBub7XABd4TJANXtQXGCacNUG total 0,5 btc
After that during 1 - 2 days the software will be sent to you - decryptor -
and the necessary instructions. All changes in hardware configurations of
your computer can make the decryption of your files absolutely impossible!
Decryption of your files is possible only on your PC!
Recovery is possible during 7 days, after which the program - decryptor -
can not ask for the necessary signature from a public certificate server.
Please contact via e-mail, which you can find as yet in the form of a text
document in a folder with encrypted files, as well as in the name of all
encrypted files.If you do not appreciate your files we recommend you format
all your disks and reinstall the system. Read carefully this warning as it is
no longer able to see at startup of the computer. We remind once again- it is
all serious! Do not touch the configuration of your computer!
E-mail: orjovaja@mail.com - this is our mail
CODE: C98F4DEC6A78B1A714D0FD416A61248B this is code; you must send
BTC: Xqz5WKhkQJBub7XABd4TJANXtQXGCacNUG here need to pay 0,5 bitcoins
How to pay on the Bitcoin wallet you can easily find on the Internet.
Enter your unlock code, obtained by E-mail here and press "ENTER" to
continue the normal download on your computer. Good luck! May God help you!
<!SATANA!>

Crypto-Malware

Versiones y sabores

- Ningún OS se libra de este tipo de amenazas. En la actualidad existen versiones y variantes para todos los OS más comunes
  - Todas las versiones de Windows
  - Linux
    - https://blogs.msmvps.com/harrywaldron/2016/08/30/linux-malware-fairware-ransomware-deletes-web-server-files/
  - MAC OS
    - http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/


Infección

Crypto-Malware

Defensa

- Necesitamos proteger tanto a equipos cliente como a equipos de tipo servidor
- En muchos escenarios equipos cliente tienen más criticidad que equipos de tipo servidor
  - P.ej.- Usuarios que no hacen backup
- Defensa frente a determinados ataques:
  - Web Browser
    - Phishing, SPAM, etc..
  - Mail
    - Una de las principales puertas de entrada de software malicioso

Crypto-Malware

Defensa

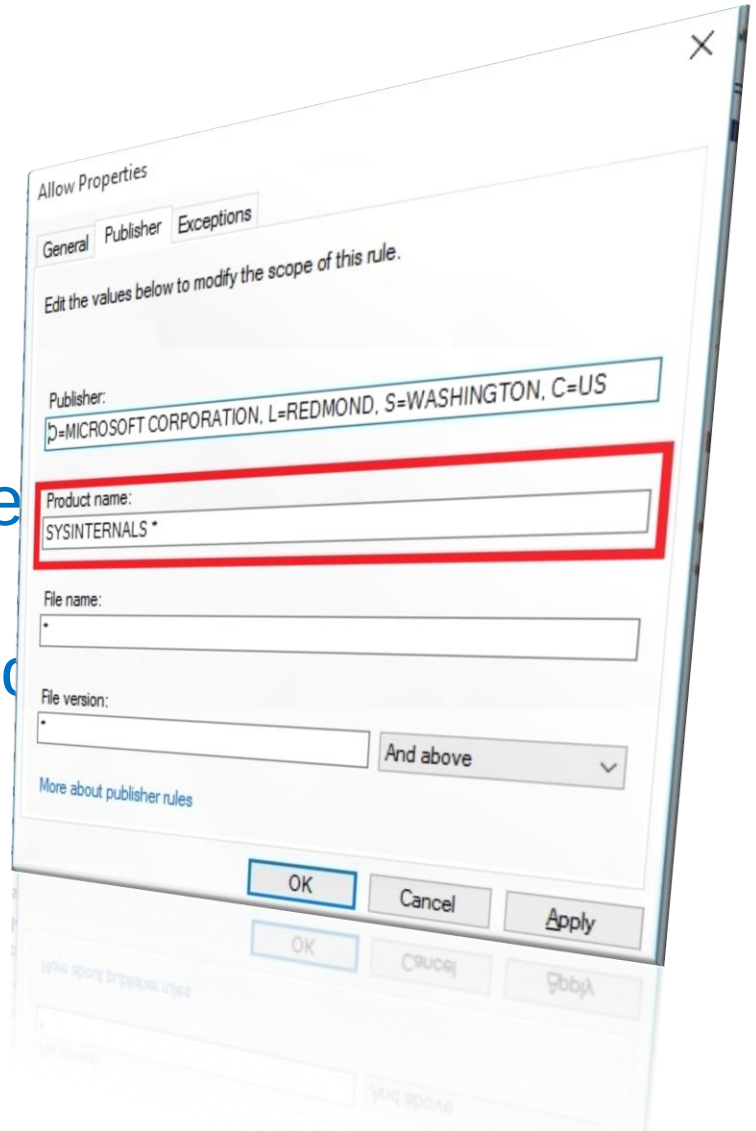
- Desplegar defensas adicionales basadas en GPO y APPLocker
  - Restricción de acceso a determinados PATH como %APPDATA% o ·%TEMP%
  - Útil para escenarios de correo y Web
- No es 100% eficiente
  - Basado en BlackList
  - Hay que hacer esfuerzos adicionales con ciertas aplicaciones que se instalan en estos PATH (P.ej.- Chrome)

Crypto-Malware

Defensa

APPLocker:

- Se pueden implementar reglas en base al emisor de un binario
- Ejemplo
  - Bloquear a cualquier aplicación que intente ejecutarse dentro del PATH %APPDATA% excepción de las firmadas con el certificado de Chrome, Microsoft, etc..




Protegiendo al cliente

Crypto-Malware

Servidor de Ficheros

- Los servidores de ficheros también pueden ser protegidos mediante políticas adicionales
- File Server Resource Manager
  - Suite de herramientas para ficheros incluida en Windows Server
  - Administra los tipos de datos almacenados en un servidor de ficheros
  - Con FSRM
    - Establecere quotas de almacenamiento
    - Organizar y clasificar los documentos
    - Generar reglas

Crypto-Malware

Reglas FSRM

- Controlar el tipo de ficheros que un usuario puede almacenar
  - Basados en reglas
    - Por nombre, RegEXP, etc..
    - Extender la regla con excepciones, acciones a tomar, etc..
  - Podemos aplicar la regla tanto a un directorio como a un volumen de disco
  - Ejemplos
    - Fuerza a que no se almacenen ficheros de tipo EXE en este volumen de datos
    - Clasifica todos los documentos que almacenen números de cuenta corriente como CONFIDENCIALES

Crypto-Malware

Crear regla

- Se podría implementar una regla que:
  - Permitiese almacenar todo de datos dentro del servidor de ficheros
    - No queremos empleados furiosos! ☺
  - Única excepción
    - Intentaremos prevenir cualquier tipo de cambio sobre un fichero base
  - Aplicaremos esta regla en un volumen de datos o directorio objeto de análisis y protección

Crypto-Malware

Señuelo

- El directorio señuelo tendrá que ser el primero que elija el Crypto-Malware para ser cifrado
- Cómo hacemos esto?
  - Nombrar directorio con caracteres especiales ($, _, etc..)
  - Sigue sin ser perfecto pero:
    - Mayoría de Malware utilizan la biblioteca Kernel32.lib para usar funciones de búsqueda de ficheros
    - Uso de la función FindNextFile o de la estructura de datos WIN32_FIND_DATA
    - Todas las muestras analizadas utilizan esta función
- https://msdn.microsoft.com/en-us/library/windows/desktop/aa364418(v=vs.85).aspx

Protegiendo el servidor de ficheros

Crypto-Malware

Monitorización y alertas

- Configurar las reglas con las opciones especiales para:
  - Añadir alertas al visor de eventos de Windows
    - Útil para monitorización, equipos de respuesta a incidentes, etc..
    - Se pueden re-enviar los logs a servicios como Kibana, SCOM, etc..
  - Envío de correo electrónico a responsables de seguridad
    - Ayuda a coordinar un intento de infección enviando un email por cada intento de acceso

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en