sepian

Seguridad Digital
de Andalucía

WEBINAR

Prevención de ataques ransomware en entornos reales

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

Contenidos

Qué vamos a tratar

Contenidos

1. Introducción al ransomware
2. Vías de infección:
   Principales campañas de ransomware en España
3. Medidas preventivas:
   Tipos de eventos
   Ficheros de configuración
4. Medidas reactivas:
   Filtrando las entradas
   Extrayendo logs con powershell
5. Ejemplos de uso:
   Infección de equipo
   Protección contra infección
   Restauración de ficheros

Objetivos

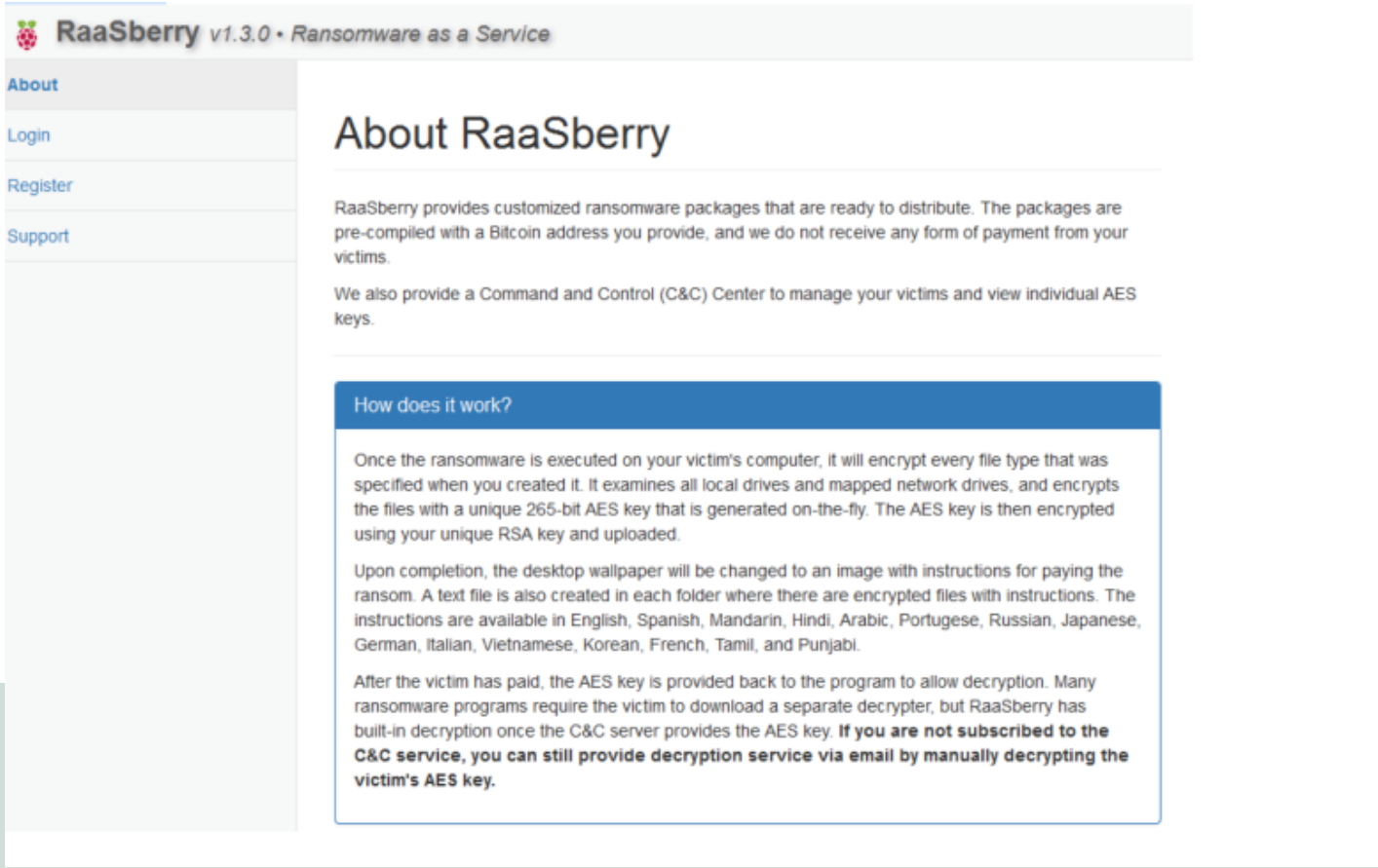
- Analizar e identificar la amenaza al igual que las vías de infección.
- Conocer las posibles medidas para intentar evitar los incidentes.
- Identificar las diferentes herramientas y procedimientos a tomar si el incidente se ha producido.

Introducción al ransomware

sedian Seguridad Digital de Andalucía

- El ransomware es una extorsión que se realiza a través de un malware que se introduce en los equipos. Ha sido el más destructivo en la última década.
- Es tan conocido, que no es misión de esta charla dar una descripción exhaustiva ni mucha teoría sobre ello, pero sÍ algunos datos, para entender su trayectoria.
- El ransomware ha sido una de las técnicas más lucrativas para los delincuentes y no sólo en la parte ciber. Por ello se ha expandido tanto.
- Como muestra: WannaCry en 2017, donde se produjeron 400.000 ataques en 150 países diferentes.

La extensión de este tipo de malware, así como el crecimiento de variantes, se debe también en parte a lo que se conoce como RaaS (Ransomware as a Service), un servicio por el cual los cibercriminales facilitan la creación de Ransomware a cualquier persona que lo desee a cambio de un porcentaje de las ganancias que su campaña pudiera ganar.

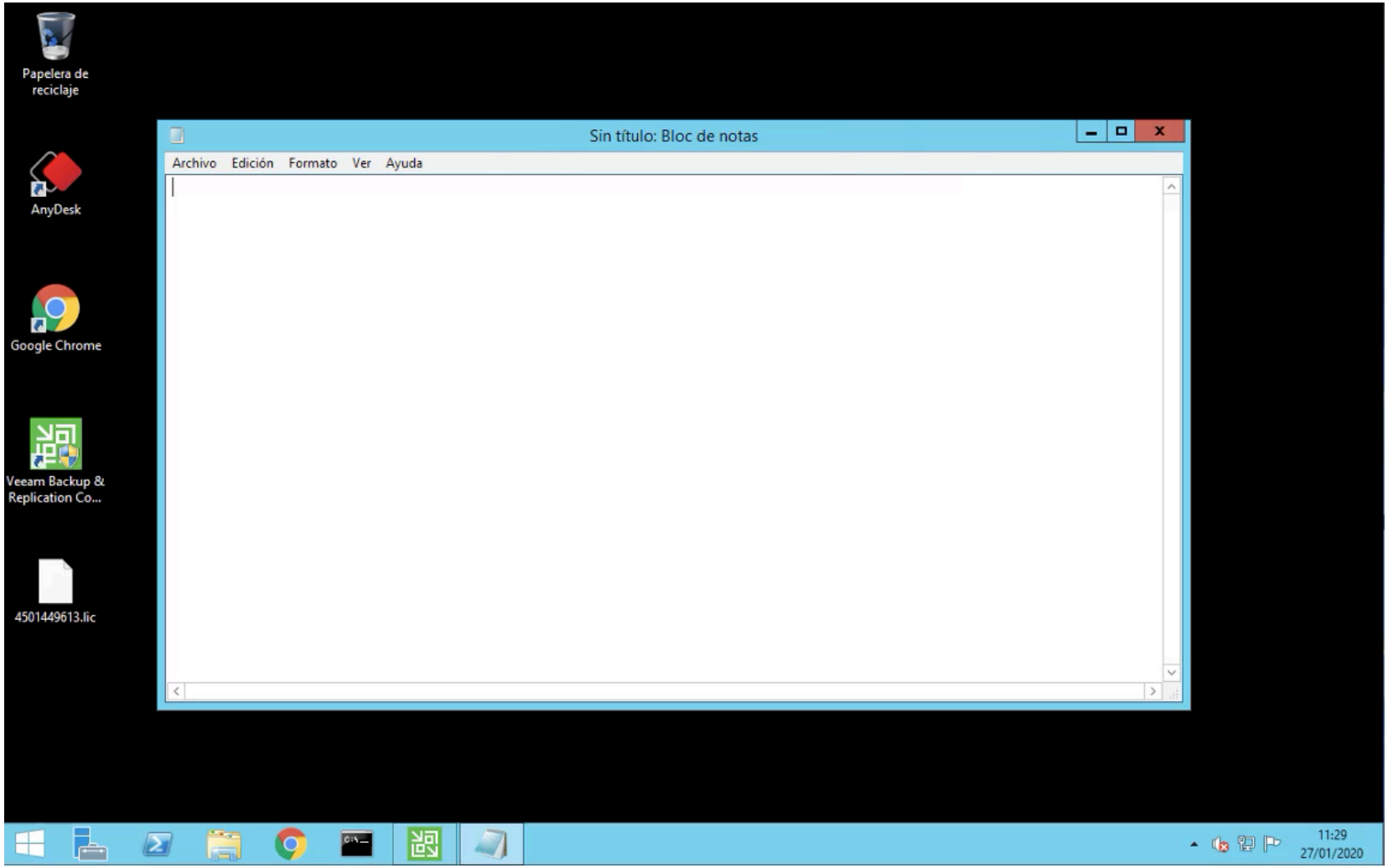


Vías de infección

- Uso de mensajes de Spam/phishing: a pesar de que otros métodos de infección están cobrando cada vez más relevancia, el uso de correos electrónicos como medio de propagación sigue siendo el más utilizado.
- Web Exploit Kits: que se aprovechan de vulnerabilidades en el navegador o en los plugins instalados.
- Servicios RDP en Windows: con contraseñas predecibles o vulnerables a ataques por diccionario. Suelen ser atacados aquellos servidores que están publicados directamente en Internet y que sus responsables tienen la errónea creencia que poner un puerto distinto (Ej: 3390,3391) al de por defecto (3389), evita el ataque.
- Métodos que dependen cada vez menos de la iteración del usuario.

Medidas preventivas

- **Mantener copias de seguridad periódicas de todos los datos importantes.**
- Existe la “norma” del 3-2-1, que determina que se deberían realizar al menos tres copias de seguridad de los datos, dos de las cuales deberán estar en soportes diferentes (por ejemplo, un DVD o un disco duro externo, un USB o incluso en la nube) y una última en formato físico en un lugar distinto a donde se almacenan las dos primeras, evitando así posibles catástrofes.
- La mejor forma actualmente de realizar copias sin que ningún ransomware afecte a ellas, es tener “Service Providers” donde alojar nuestras copias, lejos de nuestra infraestructura y sobre todo, sin acceso directo por los sistemas operativos.
- Ejemplo:


Papelera de reciclaje
AnyDesk
Google Chrome
Veeam Backup & Replication Co...
4501449613.lic
Sin título: Bloc de notas
Archivo Edición Formato Ver Ayuda
11:29
27/01/2020

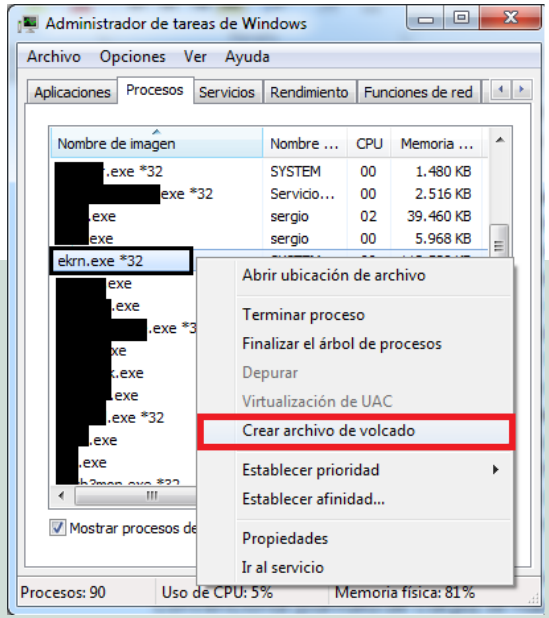
- **Utilizar VPN:** como método de acceso remoto a determinados servicios. Parte de las infecciones por ransomware se producen a través de servicios de escritorio remoto.
- Utilizar herramientas como **CryptoLocker Prevention Kit**, las cuales permiten crear políticas de grupo para impedir la ejecución de ficheros desde directorios como App Data, Local App Data o directorios temporales (comúnmente utilizados por gran variedad de ransomware).
- No utilizar cuentas con permisos de administrador a no ser que sea estrictamente necesario. La ejecución de cierto código dañino, bajo una cuenta de administrador, permite llevar a cabo todo tipo de acciones dañinas en el sistema. Considérese el uso de cuentas limitadas para la gran mayoría de usuarios.

- Utilizar un sistema antivirus correctamente actualizado, pero con medidas anti-ransomware y un firewall de aplicación en el sistema operativo con reglas de filtrado restrictivas. Dichas contramedidas servirán como refuerzo adicional a otros sistemas de protección basados en red tales como IDS/IPS, etc.
- Los anti-ransomware utilizan herramientas de prevención por comportamiento, no por firmas, detectando y cortando un comportamiento atribuido a una técnica de infección.

Medidas reactivas

- En la mayoría de los casos, se es consciente de que hemos tenido un ataque de ransomware, una vez han sido cifrados los archivos del equipo. Aun así, en todos los casos se aconseja seguir una serie de pasos.
- **Desconectar las unidades de red**: esto supone “tirar del cable” de red (o desactivar las interfaces inalámbricas). De este modo se podría llegar a evitar el cifrado de ficheros en unidades de red accesibles, en el caso de que el ransomware aún no hubiera finalizado su ejecución.

- **Comprobar si el proceso dañino aún sigue ejecutándose**. Esta tarea no es sencilla en muchos casos, ya que podría haberse inyectado en otro legítimo o simplemente podría haber finalizado su ejecución.
- Sin embargo, en caso de identificarse el proceso en cuestión (usando herramientas como Process Explorer de Sysinternals), desde el Administrador de Tareas de Windows (Taskmanager) se realizará un dump (volcado de la memoria) del proceso dañino. Para ello, hay que hacer clic derecho sobre el proceso y seleccionar la opción “Crear archivo de volcado” (se guardará en %TMP%). Una vez volcado el fichero, hay que guardarlo a buen recaudo en un sistema aislado.



- **Finalizar la ejecución del proceso dañino.** Para ello existen dos alternativas:

    - En caso de haberse identificado el proceso simplemente bastará con parar su ejecución desde el Administrador de Tareas de Windows: clic derecho sobre el proceso y seleccionar la opción “Finalizar el árbol de procesos”.
    - Si no se ha podido identificar el proceso, se recomienda apagar el equipo de manera manual e inmediata.

- **Arrancar el equipo en Modo Seguro**. Antes de que arranque Windows de manera convencional (pantalla de carga) se habrá de pulsar la tecla F8 para acceder al menú de arranque avanzado, desde el que se seleccionará iniciar desde “Modo Seguro”. De este modo evitaremos que el ransomware vuelva a arrancar de nuevo en caso de que este fuera persistente.
- **Realizar una copia de seguridad del equipo**. Esta copia contendrá todos los ficheros cifrados y no cifrados, y deberá realizarse en un dispositivo de almacenamiento externo aislado de la red. En caso de que no pudieran descifrarse los ficheros es importante conservarlos, ya que en un futuro puede que se rompa el cifrado o se liberen las claves del C&C.

Descifrado del ransomware: es posible en algunos casos, el descifrado del ransomware con algunas herramientas. El CCN CERT publicó una tabla en la que se muestran las posibilidades y el tipo de recuperación.

RANSOMWARE	POSIBILIDAD DE RECUPERACIÓN DE LOS DATOS	
BANDARCHOR	Dependiendo de la muestra y su similitud con el Ransomware llamado RAKHNI se puede intentar usar la herramienta de descifrado realizada por Kaspersky. En caso de que la muestra no tenga similitud, solo a partir de backup.	○
BAT_CRYPTOR	A partir de backup.	✗
CERBER	A partir de backup. En las versiones 1 y 2 mediante herramienta de Check Point.	✗
CRITONY (variante del CTB-LOCKER)	A partir de backup.	✗
CRYPTEAR	Al ser una prueba de concepto y tener su código fuente, su autor publicó una herramienta de descifrado en el mismo repositorio del código.	✔
CRYPTODEFENSE (2ª versión de CRYPTOWALL)	Mediante herramienta de Emsisoft.	✔
CRYPTOFORTRESS	A partir de backup.	✗
CRYPTOGRAPHIC LOCKER	Mediante herramientas forenses de recuperación de ficheros.	○
CRYPTOLOCKER	Consultar en www.decryptcryptolocker.com	○
CTB-LOCKER / CRITONI	A partir de backup.	○
CRYPTOWALL	A partir de backup. En la tercera versión a través de herramientas de recuperación de archivos. La cuarta y quinta versión sólo si se puede obtener la clave RSA.	✗
CRYPTXXX	Mediante herramienta de Kaspersky.	✔
DMALOCKER	Para las dos primeras versiones se puede usar la herramienta de Emsisoft. En el caso de las dos últimas versiones solo se puede a partir de backups.	○
LOCKY	Comprobar mediante herramienta de Emsisoft Autolocky.	○
PETYA	En la primera versión se puede utilizar la herramienta realizada por bleepingcomputer, en el caso de la segunda se ha publicado la clave privada de descifrado.	✔
MISCHA	Se ha publicado la clave privada de descifrado.	✔
SATANA	Solo a partir de backup. El sector de arranque no se recupera.	✗
TESLACRYPT	Mediante la herramienta de descifrado realizada por ESET.	✔
TORRENTLOCKER	Mediante herramienta TorrentUnlocker de BleepingComputer. La última versión no puede ser descifrada (desde mayo 2016 aproximadamente).	○
ZEROLOCKER	Mediante herramienta UnlockZeroLocker de Vínsula.	✔
JAZZ	Mediante herramienta RakhniDecryptor de Kaspersky Labs.	✔
WANNACRY	Solo a partir de backup. Existe herramienta de prevención del CCN, NoMoreCry.	○
CRYSIS	Consultar herramienta RakhniDecryptor de Kaspersky Labs. Solo algunas variantes.	○
NONPetya	Actualmente no existe una solución automatizada, y la solución manual es costosa.	○

✔ Sí existe solución ○ Existe solución parcial ✗ No existe solución

Medidas reactivas
Descifrado del ransomware

Podemos actualizar esto a través de publicaciones en la propia página del CNN-CERT:

Medidas reactivas
Descifrado del ransomware

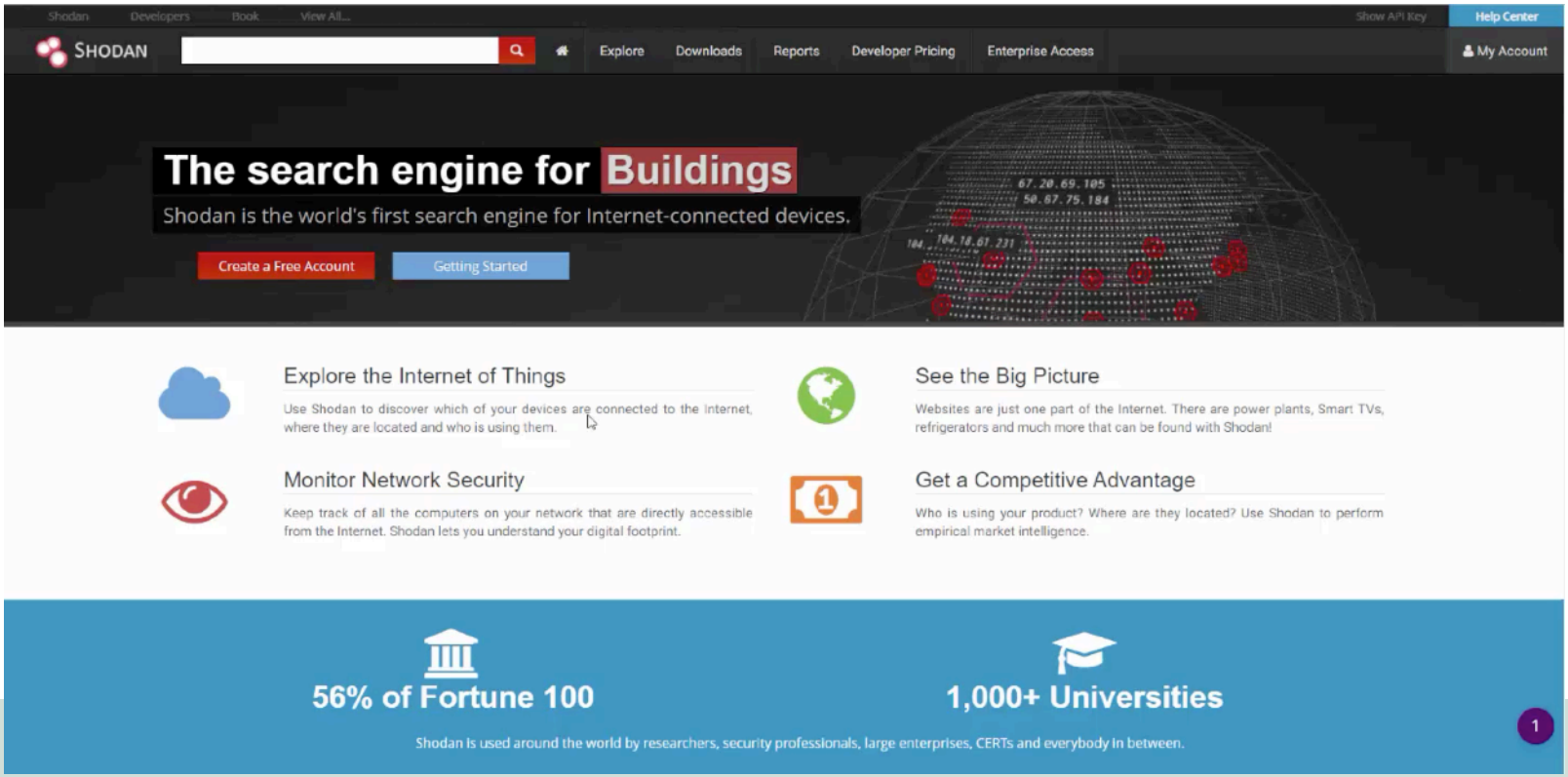
O a través de otras páginas como puede ser https://www.nomoreransom.org/es:

Ejemplos de uso

Ejemplo 1 – Descubrimiento de servidores RDP

- En este ejemplo. Utilizaremos Shodan para descubrir equipos en una determinada región geográfica.
- Veremos como no es necesario que estén en el puerto 3389 para su descubrimiento.

Ejemplo 1 – Descubrimiento de servidores RDP

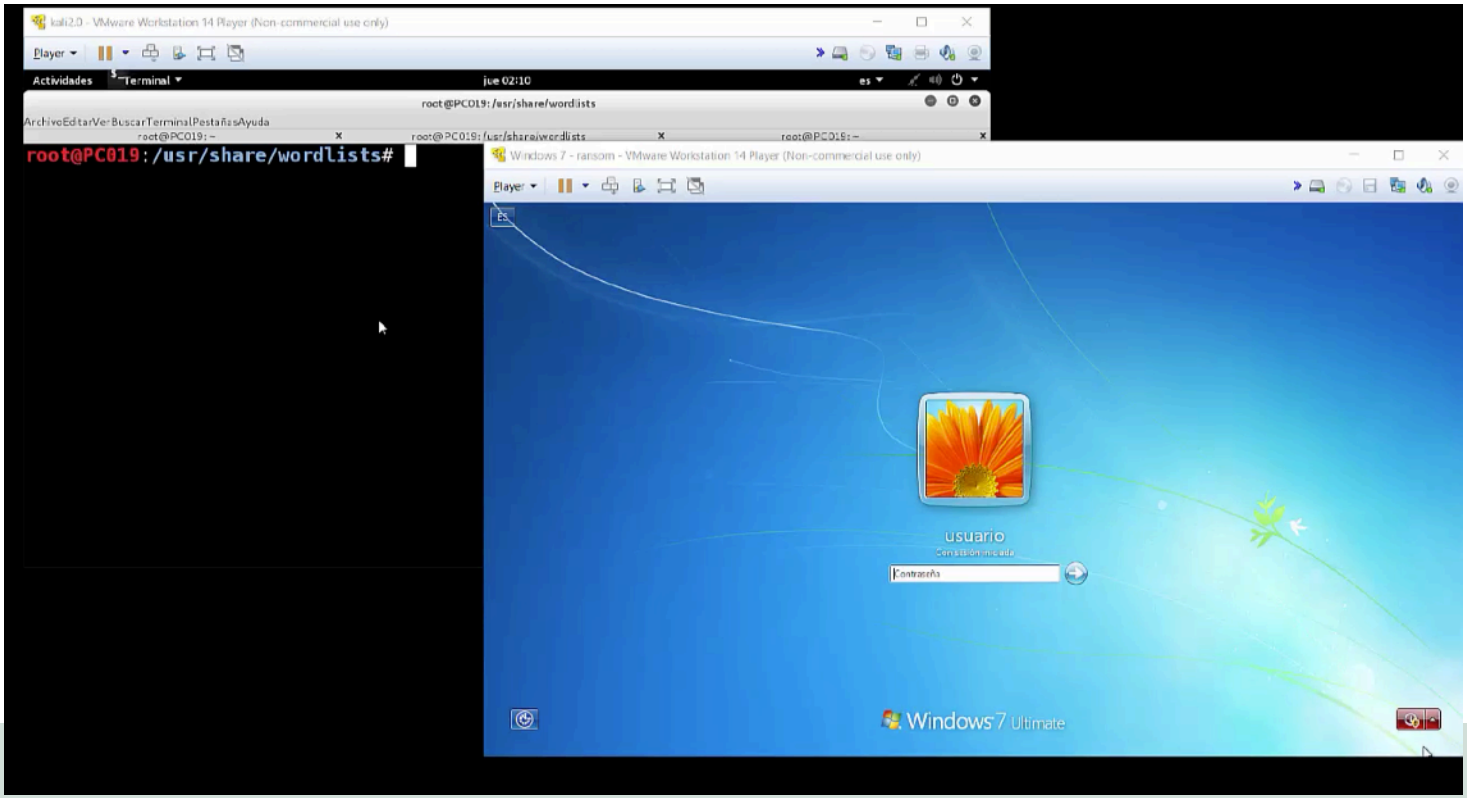


Ejemplo 2 – Infección del equipo

En este ejemplo, veremos cómo infectamos un equipo con el malware GandCrab. Para ello:

- Encontramos un equipo al que podemos conectar por escritorio remoto.
- Atacamos ese equipo por diccionario hasta poder acceder a él.
- Ejecutamos el malware que copiamos en el equipo.
- Al tratarse de un malware que tiene herramienta de descifrado, utilizamos dicha herramienta.

Ejemplo 2 – Infección del equipo

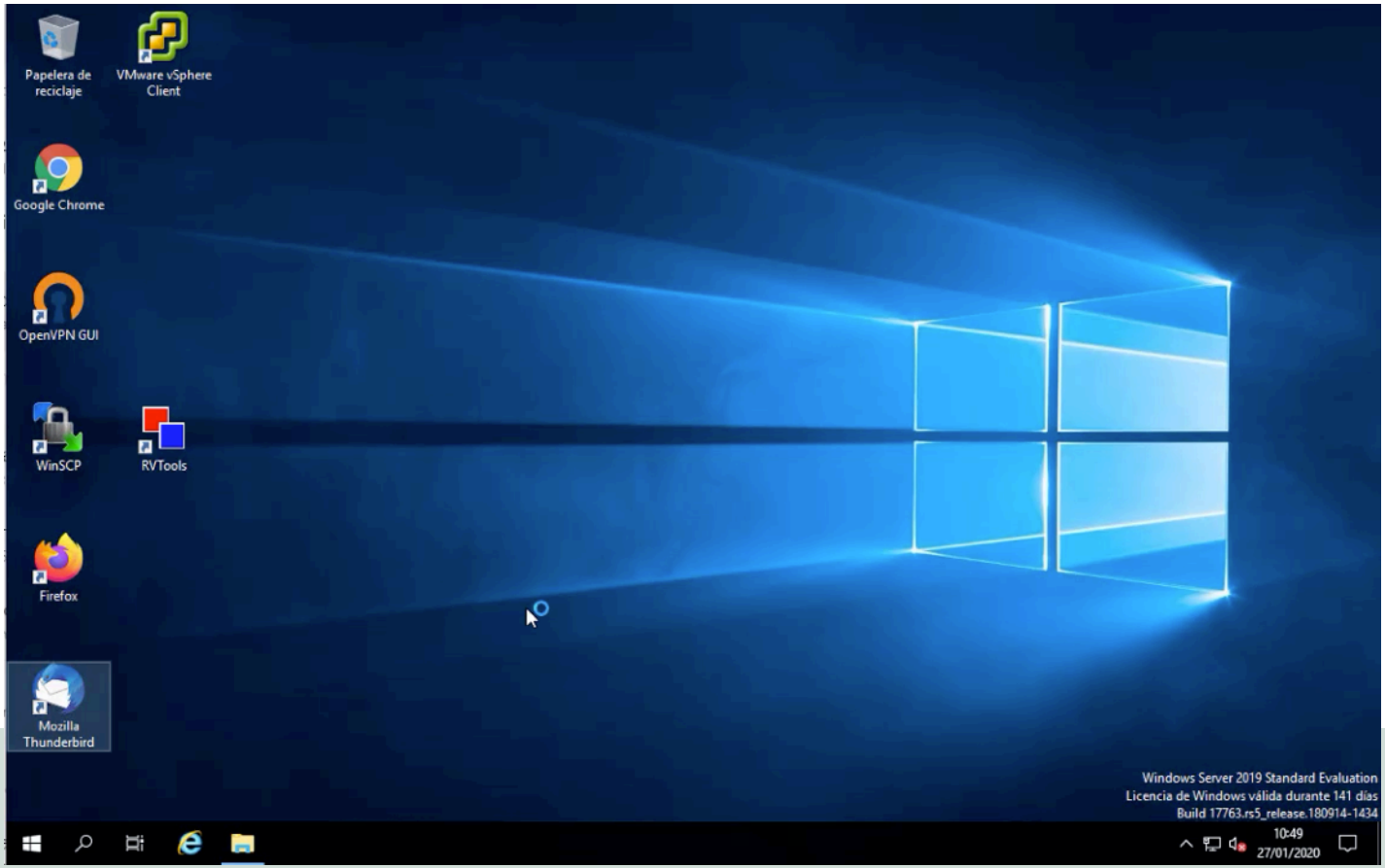


Ejemplo 3 – Restauración de ficheros con Instantáneas de Volumen Windows

Cómo crear y cómo restaurar carpetas de Windows, a través de VSS de Windows:

- Este método es eficaz cuando:
  - La ejecución del malware se coge a tiempo.
  - Las carpetas atacadas no tienen un tiempo de modificación alto.
  - Tenemos carpetas compartidas a través de Windows y el servidor no se ha visto afectado.
- Tenemos un volumen creado y asignado a esta máquina.
- Formateamos el disco y lo ponemos a disposición del sistema.
- En el vídeo forzaremos la ejecución de las instantáneas, para no esperar a su ejecución programada.

Ejemplo 3 – Restauración de ficheros con Instantáneas de Volumen Windows



sedian Seguridad Digital de Andalucía