Vault7 WikiLeaks y Wannacry

28 de mayo de 2017

Ingeniería de Servidores 2017
Universidad de Granada

Contenidos

Releases Vault-7

WikiLeaks y Vault 7

WikiLeaks y Vault 7

WikiLeaks y Vault 7

- ¿Qué es WikiLeaks?

WikiLeaks y Vault 7

- ¿Qué es WikiLeaks?
- ¿Qué es Vault 7?

WikiLeaks y Vault 7

- ¿Qué es WikiLeaks?
- ¿Qué es Vault 7?
- ¿Por qué nos interesa tanto a los usuarios como a los administradores de sistemas?

Dark Matter

Dark Matter

Dark Matter

- 23 de Marzo de 2017

Dark Matter

- 23 de Marzo de 2017
- Infección permanente del firmware de dispositivos y ordenadores de Apple.

Dark Matter

- 23 de Marzo de 2017
- Infección permanente del firmware de dispositivos y ordenadores de Apple.
- Permite inyección de código malicioso a través del firmware y persistentes al reinicio.

Dark Matter

- 23 de Marzo de 2017
- Infección permanente del firmware de dispositivos y ordenadores de Apple.
- Permite inyección de código malicioso a través del firmware y persistentes al reinicio.
- Se pueden infectar dispositivos de arranque EFI/UEFI para ejecutar código malicioso al inicio de la máquina.

Marble Framework

Marble Framework

Marble Framework

- 31 de Marzo de 2017

Marble Framework

- 31 de Marzo de 2017
- Herramienta para ocultar datos ante un análisis forense informático.

Marble Framework

- 31 de Marzo de 2017
- Herramienta para ocultar datos ante un análisis forense informático.
- Hace esto escondiendo el malware creado por la CIA e introduciendo idiomas variados y con distintas codificaciones con la intención de confundir a analistas y antivirus.

Grasshopper

Grasshopper

Grasshopper

- 7 de Abril de 2017

Grasshopper

- 7 de Abril de 2017
- Plataforma de creación de malware para Windows.

Grasshopper

- 7 de Abril de 2017
- Plataforma de creación de malware para Windows.
- Crea un lenguaje de módulos sencillos para confeccionar malware aprovechando vulnerabilidades conocidas.

Hive

Hive

Hive

- 14 de Abril de 2017

Hive

- 14 de Abril de 2017
- Monitorización de usuarios y obtención de información gracias a una plataforma back-end

Hive

- 14 de Abril de 2017
- Monitorización de usuarios y obtención de información gracias a una plataforma back-end
- Utiliza HTTPS con una interfaz y consola interactiva.

Hive

- 14 de Abril de 2017
- Monitorización de usuarios y obtención de información gracias a una plataforma back-end
- Utiliza HTTPS con una interfaz y consola interactiva.
- Emplea dominios e IPs específicas para cada usuario que quiera ser monitorizado.

Weeping Angel

Weeping Angel

Weeping Angel

- 21 de Abril de 2017

Weeping Angel

- 21 de Abril de 2017
- Herramienta para espiar a usuarios a través de vulnerabilidades y puertas traseras de la serie F de televisores de Samsung.

Weeping Angel

- 21 de Abril de 2017
- Herramienta para espiar a usuarios a través de vulnerabilidades y puertas traseras de la serie F de televisores de Samsung.
- Esta serie de televisiones tienen micrófono, usado en los espionajes.

Scribbles

Scribbles

Scribbles

- 28 de Abril de 2017

Scribbles

- 28 de Abril de 2017
- Se aprovecha de marcas de agua que monitorizan quién está leyendo un documento.

Scribbles

- 28 de Abril de 2017
- Se aprovecha de marcas de agua que monitorizan quién está leyendo un documento.
- Se comunican con servidores preparados para recibir datos de este tipo.

Scribbles

- 28 de Abril de 2017
- Se aprovecha de marcas de agua que monitorizan quién está leyendo un documento.
- Se comunican con servidores preparados para recibir datos de este tipo.
- Afecta a documentos generados con las versiones de Microsoft Office 1997-2016.

Wannacry

¿Qué es Wannacry?

¿Qué es Wannacry?

¿Qué es Wannacry?

- Wannacry es un ransomware.

¿Qué es Wannacry?

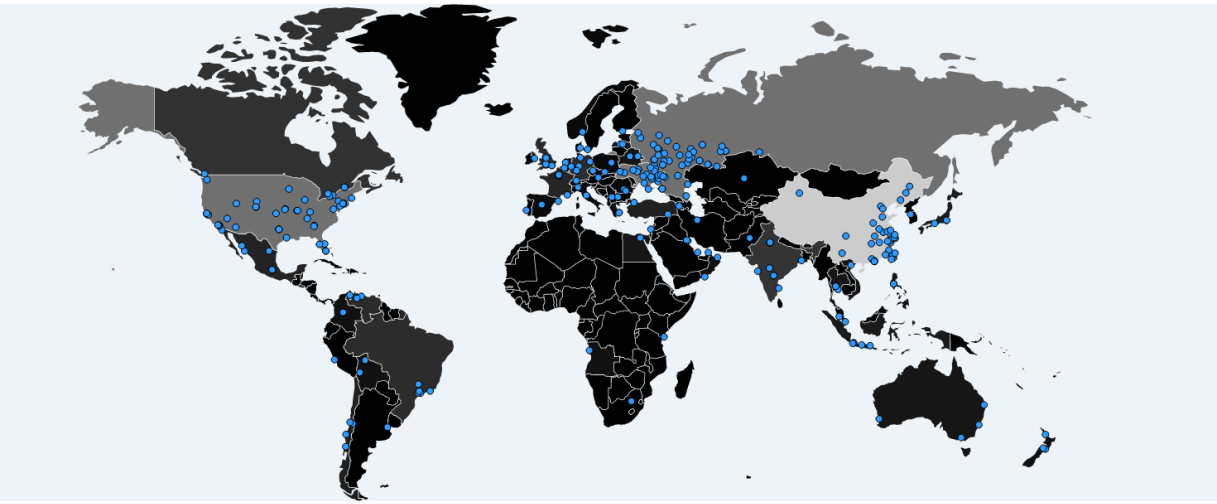
- Wannacry es un ransomware.
- ¿Cómo se ha infectado por primera vez?

¿Qué es Wannacry?

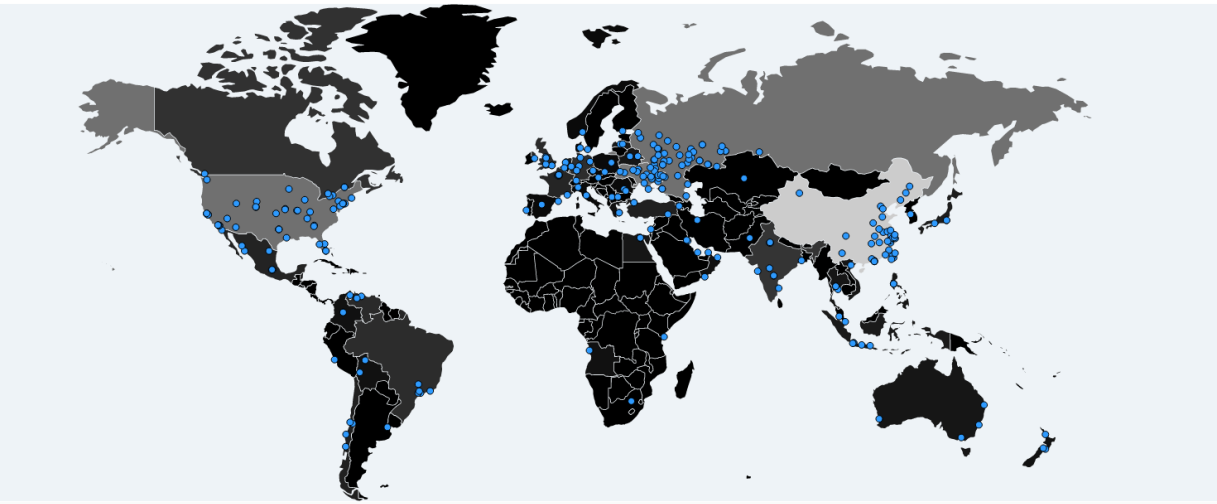
- Wannacry es un ransomware.
- ¿Cómo se ha infectado por primera vez?
- Las plataformas afectadas son las máquinas Windows en sus diferentes versiones.

¿Cómo funciona?

¿Cómo funciona?

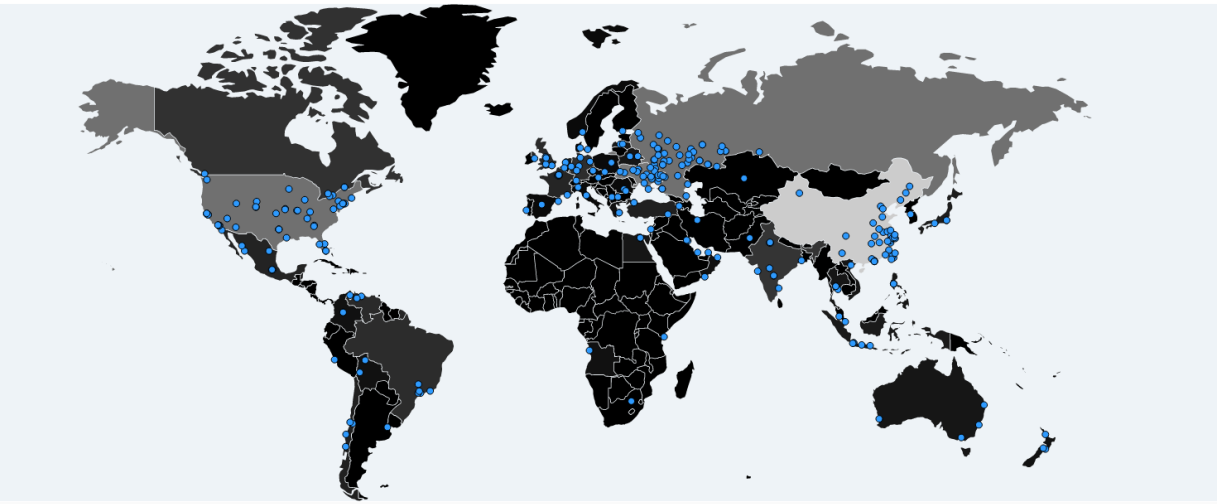


¿Cómo funciona?



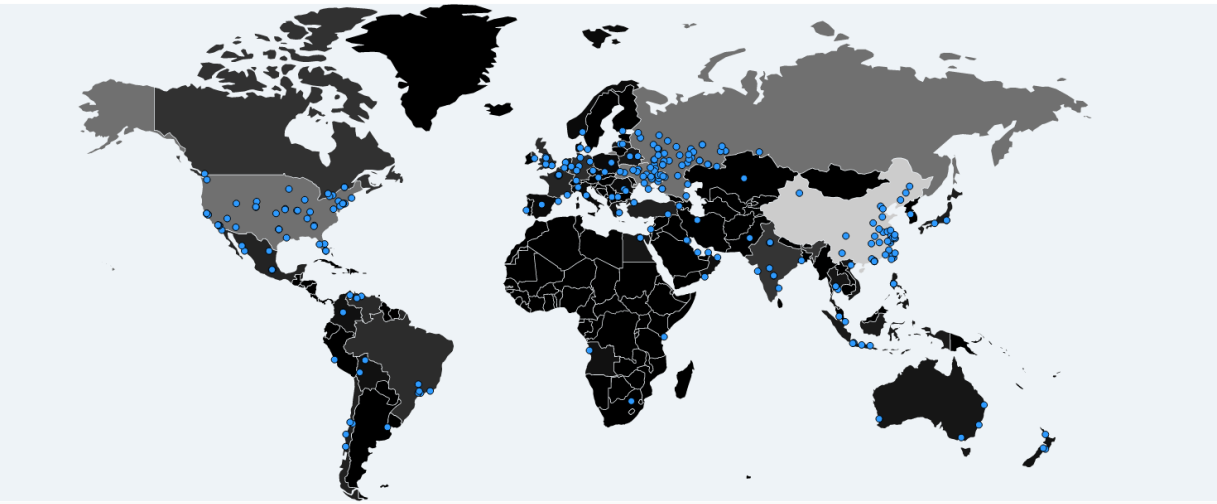
- ¿Qué medidas de seguridad hemos tomado para probar el malware?

¿Cómo funciona?



- ¿Qué medidas de seguridad hemos tomado para probar el malware?
- ¿Como infecta usando SMB?

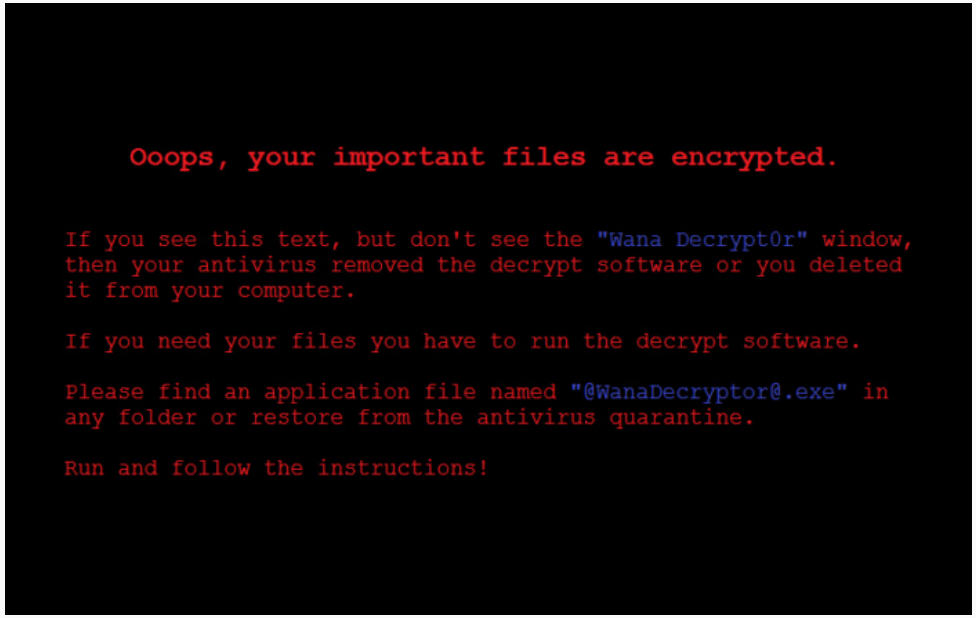
¿Cómo funciona?



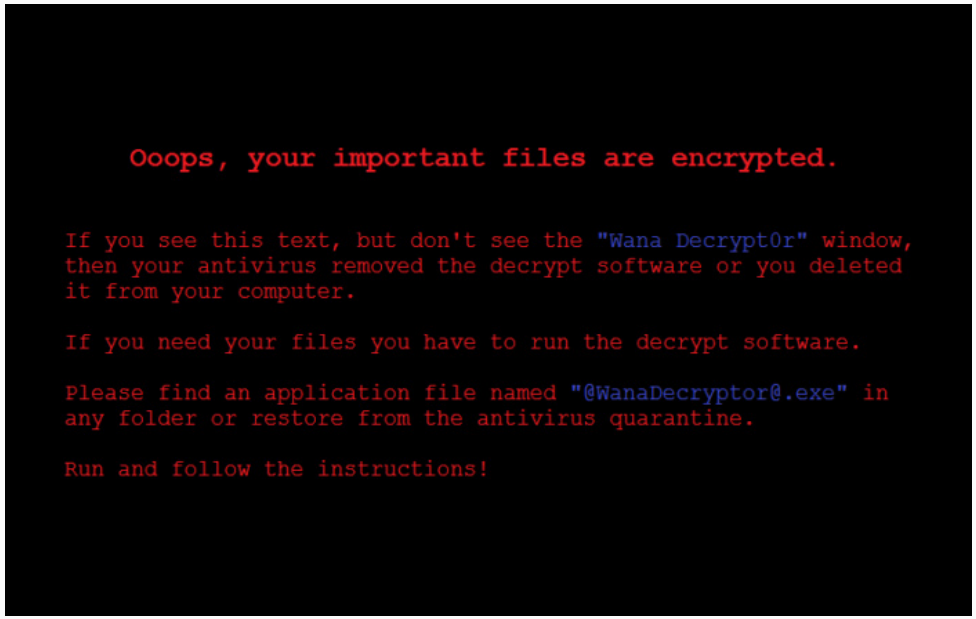
- ¿Qué medidas de seguridad hemos tomado para probar el malware?
- ¿Como infecta usando SMB?
- ¿Cómo encripta los archivos y cómo se recuperan si pagas?

Análisis forense del malware

Análisis forense del malware

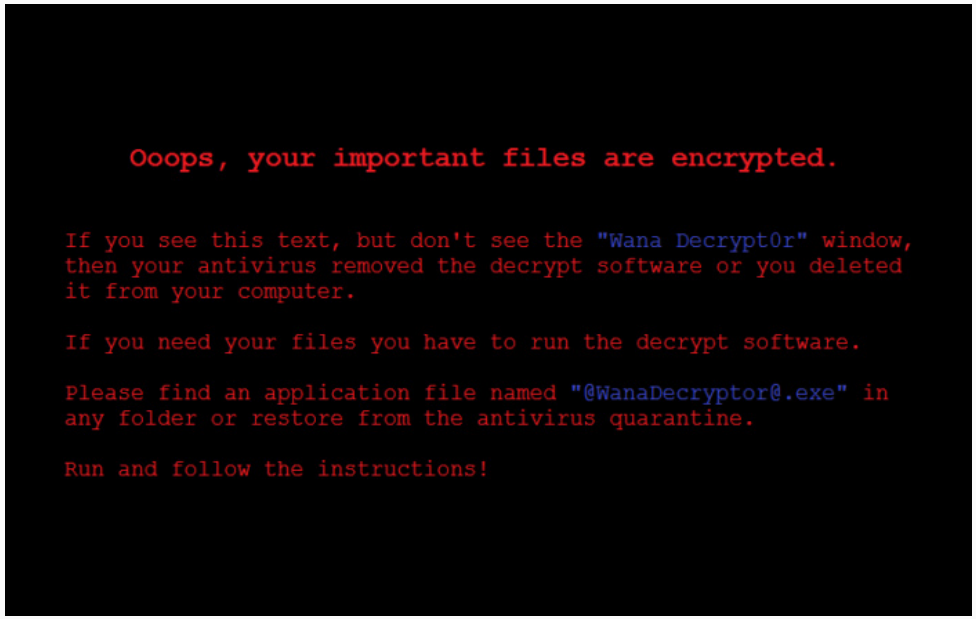


Análisis forense del malware



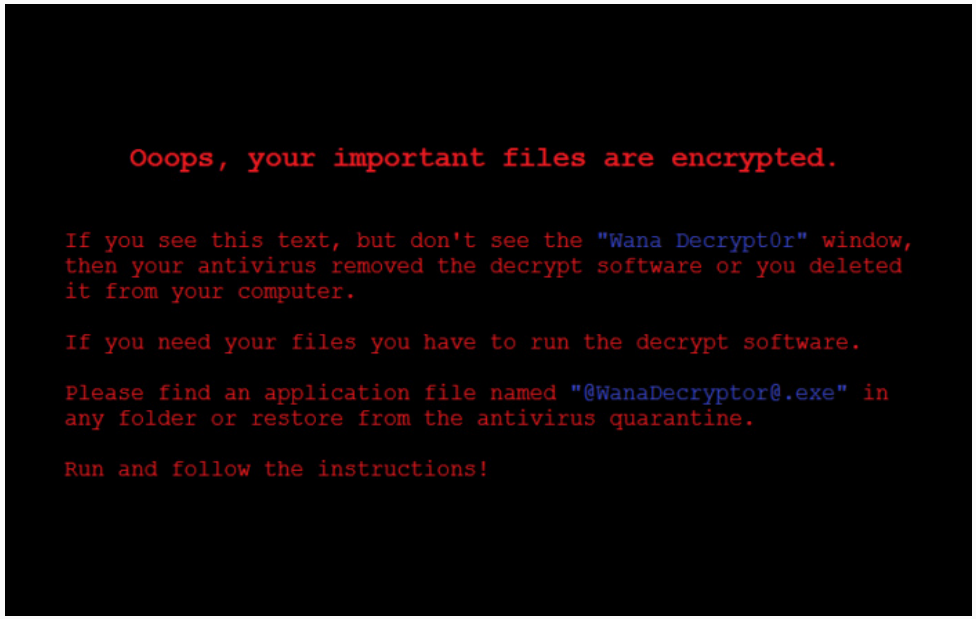
- Strings sobre el ejecutable.

Análisis forense del malware



- Strings sobre el ejecutable.
- KillSwitch del malware.

Análisis forense del malware



- Strings sobre el ejecutable.
- KillSwitch del malware.
- Estudio del malware sobre una máquina virtual.

Preguntas


Alai
@alaisierra
Seguir
“No sé lo qué ha podido pasar, yo puse una tirita en todas las webcams de los ordenadores de Telefónica”.
13:21 - 12 May 2017
378
387