Agencia de Regulación y Control de las Telecomunicaciones	**SEGURIDAD DE LA INFORMACIÓN**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
	INCIDENTE BEAGLE	

ÍNCIDE

INCIDENTE BEAGLE

1. INTRODUCCIÓN

Beagle o también conocido como Bagle es un gusano (malware) escrito en distintos lenguajes de programación, comprimido y/o encriptado, se propaga a través de correo electrónico y redes P2P. Si el gusano llega por correo electrónico, el asunto del mensaje varía con cada versión, su remitente siempre es falso y contiene adjuntos. Este gusano es capaz de actualizarse desde diferentes sitios de Internet y de desactivar muchos de los programas de seguridad instalados.

A través de los años, los autores del gusano Bagle o Beagle han demostrado una gran habilidad para lograr cambios técnicos y de distribución en el código del malware, Bagle ha evolucionado incorporando nuevas técnicas de infección, de reproducción y de ingeniería social, logrando una gran efectividad en su reproducción y cantidad de infecciones. Cada una de las distintas versiones que han aparecido, es capaz de cosechar distintos tipos de información.

2. CARACTERÍSTICAS

2.1. Funcionalidad.- Si bien durante sus cientos de versiones el mismo ha ido cambiando la forma de beneficiarse, sus funcionalidades pueden resumirse en:

- Envío de SPAM: su principal medio de distribución.
- Robo de direcciones de correo electrónico: le permite realizar ataques de Phishing y favorecer el SPAM, así como la venta, por parte de sus autores de las direcciones obtenidas.
- Robo de información confidencial: su principal beneficio.
- Instalación de Backdoors: le permite establecer futuros puntos bases de ataques.

2.2. Componentes.- La información que las distintas versiones recolectan a través de sus componentes es:

- IP, NAT, Nombre de la computadora infectada y su dominio
- Nombres de usuario y contraseña de POP3/IMAP
- Captura de datos de Usuario grabados por el navegador
- Configuración de cuentas FTP, navegadores web y clientes de correo.
- Contraseñas de administradores de passwords.
- Usuario y contraseña de aplicaciones de mensajería instantánea
- Usuario y contraseñas de dispositivos de acceso remoto RAS
- Usuario y contraseñas de sitios de Home-Banking

- Hashing de contraseñas.

2.3. Tareas.- Gracias a sus múltiples funcionalidades es capaz de realizar las siguientes tareas:

- Instalación de troyanos y backdoors que permiten el control remoto de las maquinas infectadas y la creación de redes de bots (zombies).
- Manipulación de DNS y archivos de host del sistema.
- Auto-actualización y descarga de otros malwares como el troyano Mitglieder.
- Inyección de distintas funcionalidades del sistema operativo.
- Finalización de procesos y servicios de aplicaciones de seguridad (antivirus, firewalls, IDS) y del sistema operativo.
- Residencia camuflada en memoria.
- Cambio de íconos de sus adjuntos para pasar desapercibido.
- Utilización de ingeniería social en el cuerpo y asunto del mensaje.
- Generación de nombres de archivos aleatorios (o conocidos por el usuario) para facilitar el engaño.
- Generación de ID para cada computadora infectada.
- Catalogación de equipos infectados.
- Rápida modificación de su código que obliga a los antivirus a su actualización excepto a aquellos que lo detectan con capacidades proactivas.
- Explotación de vulnerabilidades solucionadas o sin solución así como 0-days.
- Capturas y envió de pantallas.
- Capturas de teclas Keylogger.
- Auto-caducidad luego de un período de tiempo.
- Recolección y robo de contraseñas para muchas aplicaciones.
- Falsear direcciones de mails de origen.
- Motor propio de envío de correo (SMTP).
- Conexión de sitios remotos para la realización de distintas acciones.
- Encriptación y compresión de distintas partes de su código mediante diferentes técnicas.
- Aprovechamiento de las botnets creadas mediante su componente de backdoor.
- Evita actualizaciones de programas de seguridad.
- Evita el envío de correos electrónicos a empresas de seguridad.
- Prevención contra ataques de otros malware como NetSky.

3. TIPOS

Como ya se mencionó, Beagle se vale de diferentes componentes para realizar sus tareas. Los programas (en su mayoría otros malware) de los que se vale para realizar sus funciones son:

- **Gusano Beagle:** es el encargado de instalar los otros componentes, llevar registro de lo realizado, eliminar "competidores", controlar las redes de bots y mantenerse actualizado desde distintos sitios de Internet.
- **Mitglieder/Beagooz:** troyano encargado de realizar el envío masivo de mail, vulnerar todo el software de seguridad, robar datos y actualizarse.
- **Tooso/Tango:** troyano que vulnera y desactiva los componentes de seguridad del sistema y detiene procesos y servicios de actualización de software. Ambos son detectados como variantes de Beagle.
- **Lodear/Lodeight:** troyanos desarrollados para buscar, obtener y actualizar distintos miembros de la familia desde Internet. Son detectados como variantes de Beagle.
- **Monikey:** gusano desarrollado para facilitar la propagación mediante el envío masivo de correo y la utilización de redes P2P. También es detectado como variante de Beagle.
- **LDPinch, Tarno y Vipgsm:** permiten el robo de contraseñas de distintos programas.
- **Formglieder:** utilizado para obtener información confidencial como datos bancarios y financieros. Es detectado como variante de Beagle.

4. REFERENCIAS

- Borghello C. La historia sin fin: Virus Bagle. Recuperado 03 de mayo de 2021. Obtenido de http://www.eset-la.com/pdf/prensa/informe/historiasinfinvirusbagle.pdf.
- MASHEVSKY Y. The Bagle botnet. Recuperado 03 de mayo de 2021. Obtenido de https://securelist.com/analysis/36046/the-bagle-botnet/.