¿Qué es un gusano informático y cuáles son sus características?

n gusano informático, también conocido como “worm”, es un tipo de malware que tiene la capacidad de propagarse de forma automatizada para infectar la mayor cantidad de computadoras posibles de manera rápida, tanto sobre una red hogareña como corporativa. Pueden llegar a ralentizar la máquina víctima o la red en la que se encuentra, ya sea por un alto consumo de los recursos del equipo o por un alto consumo de la red. Debido a su gran alcance y potencial riesgo, ESET explica de qué se trata, cómo identificarlos y consejos para mantener los dispositivos protegidos.

Desde la aparición del primer worm en 1998, quedó en evidencia la efectividad de este tipo de malware para propagarse, ya que logró infectar alrededor de 6.000 equipos de los 60.000 que aproximadamente conformaban ARPANET, la red que dio origen a Internet.

Al día de hoy, los worms evolucionaron y cuentan con payloads para realizar otro tipo de actividades maliciosas; por ejemplo, el gusano VjWorm que puede propagarse a través de dispositivos USB y tiene capacidades de RAT (Troyano de Acceso Remoto) que le permite obtener información personal de un usuario víctima.

¿Cómo se propagan los gusanos informáticos?

Los gusanos buscan auto propagarse para afectar a la mayor cantidad de equipos posible. Esta propagación automática puede optar por una o más técnicas, algunas de estas pueden ser:

- **Correo electrónico:** En este caso los worms son capaces de generar automáticamente un correo copiándose como archivos adjuntos, o poniendo un enlace donde se encuentra el código malicioso, el mismo puede estar acortado con alguna herramienta o no. Este se envía hacia los contactos de la víctima. Una posible victima puede ser una cuenta comprometida o la cuenta del usuario en la maquina infectada.

- **Mensajería instantánea:** Similar al correo electrónico, en este caso los worms se distribuyen por redes de mensajería instantánea, WhatsApp, Skype, etc. A veces utilizan enlaces acortados acompañados de frases engañosas como “Mira este video, es muy gracioso”, “Aprovecha esta oferta por tiempo limitado”, entre otros.

- **Sitios comprometidos:** En este caso se trata de infectar un sitio web que presente vulnerabilidades. En caso de haberlo conseguido, la víctima se infectará con el worm cuando visite el sitio en cuestión.

- **Dispositivos USB:** En este caso los worms detectan unidades extraíbles conectadas a la maquina infectada y se replican sobre estas. En algunos casos, son capaces de crear accesos directos sobre los archivos alojados en estas unidades con la intención de confundir al usuario para que ejecute alguno de estos accesos directos, que terminan ejecutando el malware además del archivo original.

- **Explotación de vulnerabilidades:** En este caso el gusano puede contar con un set de exploits de una o más vulnerabilidades, sean conocidas o no, para poder propagarse sobre distintos equipos que puedan estar tanto en una red hogareña como corporativa. La explotación puede ser por errores de configuración en la red o problemas de seguridad en el sistema operativo o aplicaciones.

- **Chats IRC:** Similar a la mensajería instantánea, este tipo de malware puede utilizar redes de Internet Relay Chat (IRC) para enviarse sobre otras máquinas utilizando mensajes que pueden contener algún enlace o archivo adjunto.

- **Redes P2P:** En este caso los worms pueden distribuirse a través de redes peer-to-peer (P2P), utilizando conexiones establecidas para enviar copias de sí mismo.

Teniendo en cuenta que la forma de auto propagación que tienen los worms hacen que sean amenazas muy efectiva, ESET menciona que existen distintos códigos maliciosos pertenecientes a otras familias, ya sean RAT, botnets, ransomware, etc., que optan por tener un módulo de auto propagación similar a los worms para hacer más dañina la amenaza. Algunos ejemplos de familias de malware con características de gusano de estos pueden ser: Lemon Duck, un malware para minar criptomonedas que cuenta con un módulo para propagar automáticamente el malware enviando correos con contenido malicioso abusando de Microsoft Outlook en la maquina víctima, y Bondat, un malware para minar criptomonedas capaz de auto propagarse a través de dispositivo USB conectados en la maquina víctima.

ESET comparte los siguientes consejos para minimizar los riesgos de ser víctima:

- Tener los equipos y aplicaciones actualizados a la versión más reciente.

- Mantener actualizadas las soluciones de seguridad instaladas en el equipo.

- En el caso de correos electrónicos o mensajes recibidos a través de alguna aplicación, prestar atención a:

- La dirección de correo y el nombre de la persona que envía el mensaje.

- Si el mensaje contiene faltas de ortografía u otro tipo de error.

- Quién envía el correo, y si se expresa de una forma extraña o de una manera que no suele expresarse normalmente.

- No abrir ningún correo si hay motivos para dudar, ya sea del contenido o de la persona que lo envió.

- Ser prudentes al descargar y extraer archivos comprimidos .zip, .rar, etc. más allá de que la fuente que envía el correo sea legitima.

- No descargar archivos adjuntos de correos si se duda de su recepción o de cualquier otra cosa.

- Si un correo o mensaje tiene un enlace que nos lleva a una página que solicita las credenciales para poder acceder, es importante ¡no hacerlo! En su lugar se recomienda abrir la página oficial del sitio de forma manual y desde otro navegador u otra pestaña, e ingresar desde ahí.