INFOPAPER:
EMOTET - EL MALWARE MÁS PELIGROSO DEL MUNDO

Contenido

Introducción

++++ Incremento masivo de la actividad de Emotet ++++

++++ Emotet: daños informáticos en el Tribunal de Apelación de Berlín ++++

++++ Emotet todavía tiene países bajo control ++++

El nombre "Emotet" aparece repetidamente en las noticias en relación con ataques de hackers extremadamente graves contra empresas, administraciones, hospitales y universidades. En 2019, el BSI calificó el malware Emotet como el más peligroso del mundo porque ha causado un daño que asciende a millones.

¿Qué hace que Emotet sea tan peligroso y cómo puedes protegerte de él? Hornetsecurity te dará el punto de vistas de sus expertos en ciberseguridad.

¿Qué es Emotet?

Emotet **apareció por primera vez como un troyano bancario en 2014.** El ataque tenía como objetivo interceptar datos de acceso de clientes de bancos alemanes y austriacos. Mientras tanto, Emotet puede recargar y ejecutar una variedad de otros módulos con otras funciones maliciosas. Emotet ataca **principalmente a través de correos electrónicos no deseados** y afecta tanto a usuarios privados como a empresas, hospitales, instituciones gubernamentales e infraestructuras críticas.

Adapta y automatiza métodos de ataques altamente profesionales de amenazas persistentes avanzadas. **Los ciberdelincuentes actúan** de manera muy perseverante para seguir siendo capaces de actuar en el sistema infectado durante el mayor tiempo posible.

Un aspecto que hace que Emotet sea particularmente peligroso: Desde finales de 2018, el malware ha podido leer las relaciones de contacto y el contenido del correo de los buzones de los sistemas infectados utilizando la llamada" Outlook harvesting" para lanzar nuevos ataques sobre dicha base. La propagación es extremadamente rápida. Otros destinatarios pueden recibir correos de aspecto real de personas con las que estuvieron en contacto recientemente. Los archivos adjuntos maliciosos o las URL contenidas en el mensaje se abren descuidadamente.

Además de este módulo de correo no deseado, Emotet también puede cargar un módulo de gusano, que le permite propagarse de forma independiente en la red de la empresa. Esto le permite **propagarse a otros ordenadores sin requerir que los usuarios hagan clic y activen un archivo adjunto.**

En este contexto, Emotet también realiza ataques de fuerza bruta con el objetivo de hackear contraseñas. Esto puede tener graves consecuencias. Una vez que el ordenador está infectado, Emotet descarga malware adicional a través de servidores C&C, dependiendo del objetivo.

Existe el riesgo de robo de datos, pérdida de control sobre los sistemas, falla de toda la infraestructura de TI y restricciones en los procesos comerciales críticos. En casos extremos, las redes de toda una empresa deben reconstruirse después de la infección. **Los daños a menudo ascienden a millones en pérdidas.**

Maestro del disfraz: ¿Por qué es tan difícil luchar contra Emotet?

Emotet no es fácil de identificar e interceptar, ya que engaña a los productos antivirus tradicionales: **como un virus polimórfico.** El código cambia ligeramente con cada nueva recuperación para evitar la detección por parte de escáneres de virus basados en firma.

Además, el virus detecta cuándo se está ejecutando en una máquina virtual. Tan pronto como se registra en el entorno de sandbox, el **programa entra en una especie de modo de espera y deja de funcionar** cualquier acción maliciosa durante ese momento.

Una alianza peligrosa: Emotet, TrickBot y el ransomware Ryuk

Como se mencionó anteriormente, Emotet carga malware adicional después de una infección. Se crea una alianza particularmente peligrosa cuando se usa en **conjunto con TrickBot y Ryuk:** disfrazado en un documento de Word, Emotet penetra y espía la red corporativa cuando se ejecuta el archivo.

Como un "abridor de puerta", recarga el troyano bancario TrickBot, que entre otras cosas copia los datos de acceso a la cuenta. Transmite esta información al ransomware Ryuk, que es el último en cargarse. **Ryuk ahora cifra todos los archivos en el sistema que TrickBot y Emotet han clasificado previamente como sensibles** o importantes.

Lo más curioso de Ryuk es que, además de cifrar datos importantes, **también elimina todas las copias de seguridad existentes de esos datos al mismo tiempo,** haciendo la recuperación mucho más difícil. Según los expertos de Hornetsecurity, está surgiendo una nueva tendencia en el desarrollo de software de chantaje con esta función de eliminación. Además, la cantidad solicitada se basa en el valor que TrickBot podría proporcionar como la disponibilidad financiera actual de la compañía.

El ataque es extremadamente selectivo y afecta principalmente a las empresas, que pueden pagar grandes sumas de dinero para recuperar el acceso a sus datos. Ryuk apareció por primera vez en agosto de 2018 y desde entonces ha generado varios millones de dólares. Todavía no está claro qué grupo de hackers está detrás.

¿Cómo protegerte?

Para protegerte eficazmente de Emotet, debes centrarse en el punto de entrada principal del malware: la comunicación por correo electrónico. **Hornetsecurity Advanced Threat Protection detecta fácilmente Emotet y Ryuk** en correos electrónicos y cuarentenas de ambos programas de malware. La primera instancia del análisis identifica el troyano Emotet. Los troyanos posteriores Ryuk y TrickBot se pueden desenmascarar utilizando el análisis de comportamiento dinámico en el entorno limitado ATP. **Los correos electrónicos que contienen el malware pérfido no se entregan a los destinatarios.**

Comportamiento básico y relevante de seguridad

Debido a que Emotet a menudo **se esconde en archivos de Microsoft Office** y necesita macros para instalar malware, tiene sentido no permitirlos. Tampoco son necesarios en áreas privadas y de negocios. Sin embargo, si no puedes prescindir de ellos, es posible permitir solo macros firmadas.

Una vez desplegado **las actualizaciones de seguridad deben instalarse inmediatamente** para sistemas operativos, programas antivirus, navegadores web, clientes de correo electrónico y programas de oficina. **Se recomienda hacer copias de seguridad.**

La vigilancia es primordial: incluso con remitentes supuestamente conocidos, se debe tener cuidado con los archivos adjuntos de correos electrónicos, especialmente con documentos de Office y enlaces contenidos. En caso de duda, es aconsejable contactar directamente con el remitente de un correo sospechoso y verificar la credibilidad del contenido.

Accesos a la **propia red de la compañía debe ser monitoreada continuamente.** De esta manera, se puede determinar de manera oportuna si se ha producido una infección por Emotet.

Checklist: ¿Qué debe suceder en el caso de una infección de Emotet?

Si las medidas de seguridad tomadas han fallado y ocurre una infección, se deben tomar las siguientes medidas de inmediato:

Para evitar una mayor propagación, **se debe informar, lo antes posible, al departamento de TI de la empresa y a todas las personas de nuestro entorno** . Los contactos de correo tienen un gran riesgo de infección.

Las IP de C&C de Emotet deben ser bloqueadas inmediatamente. Como resultado, el malware no recibirá ningún comando nuevo y no podrá descargar más módulos.

El malware realiza profundos cambios de seguridad en el sistema infectado y no se elimina fácilmente de los ordenadores. Por lo tanto, es esencial **que reinstales los componentes de TI afectados.**

Debes tener en cuenta todo lo que has usado previamente: **cambiar la contraseña** ya que es probable que los hackers se hayan aprovechado y tengan acceso a otras áreas sensibles.

Es necesario **cuestionar los conceptos de ciberseguridad existentes e identificar puntos de entrada** para protegerse mejor de nuevos ataques.

- ☑ **Informar al departamento de TI y a todas las personas de nuestro entorno**
- ☑ **Bloquear IP de C&C de Emotet**
- ☑ **Vuelve a instalar los componentes de TI afectados**
- ☑ **Cambia las contraseñas usadas anteriormente**
- ☑ **Pregúntate sobre los conceptos de seguridad**
- ☑ **Identifica puntos de entrada**