Publicado en Madrid el 16/12/2021

El malware más buscado de noviembre de 2021: Emotet vuelve al Top 10

La vuelta de Emotet como séptimo malware más prevalente es "extremadamente preocupante" , según Check Point Research. Trickbot vuelve a ocupar el primer puesto y el sector de la educación y la investigación siguen encabezando la lista de objetivos de los ciberdelincuentes

Check Point Research, la división de Inteligencia de Amenazas Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, ha publicado su Índice Global de Amenazas del mes de noviembre. Los investigadores informan que, mientras Trickbot sigue encabezando la lista de malware más predominante, afectando al 5% de las empresas a nivel mundial, Emotet vuelve a aparecer en el índice en séptima posición. Asimismo, Check Point Research también revela que los sectores que más se ha visto atacado son los de la educación y la investigación.

A pesar de los grandes esfuerzos a principios de este año de la Europol y de numerosos organismos policiales para acabar con Emotet, se ha confirmado que la famosa red de bots ha vuelto a la acción en noviembre y ya es el séptimo malware más utilizado. Trickbot encabeza el índice por sexta vez, e incluso está implicado en la nueva variante de Emotet, que se está instalando en máquinas infectadas utilizando la infraestructura de Trickbot.

Emotet se propaga a través de correos electrónicos de phishing que contienen archivos Word, Excel y Zip infectados que despliegan este malware en el host de la víctima. Los emails contienen líneas de asunto intrigantes como noticias de actualidad, facturas y falsos memorándums corporativos para atraer a las víctimas a abrirlos. Recientemente, Emotet también comenzó a propagarse a través de paquetes maliciosos de Windows App Installer que simulan ser software de Adobe.

"Emotet es una de las redes de bots más exitosas de la historia de la cibernética y es responsable de la explosión de ataques de ransomware dirigidos que hemos presenciado en los últimos años", explica Maya Horowitz, VP de Investigación de Check Point Software. "La reaparición de la botnet en noviembre es extremadamente preocupante, ya que puede conducir a un aumento de este tipo de ataques. El hecho de que esté utilizando la infraestructura de Trickbot significa que está acortando el tiempo que le llevaría a Emotet construir un punto de apoyo suficientemente significativo en las redes de todo el mundo. Dado que se está propagando a través de correos electrónicos de phishing con archivos adjuntos maliciosos, es crucial que la concienciación y la formación de los usuarios estén en lo más alto de la lista de prioridades de las empresas cuando se trata de ciberseguridad. Y cualquiera que quiera descargar el software de Adobe debe recordar, como con cualquier aplicación, que sólo debe hacerlo a través de los sites oficiales".

Check Point Research también ha revelado este mes quelos sectores de la educación y la investigación son el más atacado a nivel mundial, seguido por el de las comunicaciones y el gubernamental/militar. Asimismo, los expertos de la compañía señalan que “Servidores web con URL

maliciosas de directorio transversal”, es la vulnerabilidad explotada más común - que ha afectado 44% de las empresas a nivel mundial-, seguida de “La revelación de información del servidor web Git” que impactó a más del 43.7%. "La ejecución de código remoto en encabezados HTTP" se sitúa en tercer lugar, afectando al 42% de los negocios en el mundo.

Los 3 malware más buscados en España en noviembre:

*Las flechas muestran el cambio de posición en el ranking en comparación con el mes anterior.

? Formbook - Detectado por primera vez en 2016, FormBook es un InfoStealer que apunta al sistema operativo Windows. Se comercializa como MaaS en los foros underground de hacking por sus fuertes técnicas de evasión y su precio relativamente bajo. FormBook cosecha credenciales de varios navegadores web, recoge capturas de pantalla, monitoriza y registra las secuencias de teclas, pudiendo descargar y ejecutar archivos según las órdenes de su C&C. Ha atacado al 7,10% de las compañías en españolas.

? Trickbot - Trickbot es un troyano bancario dominante que se actualiza constantemente con nuevas capacidades, características y vectores de distribución. Esto permite que sea un malware flexible y personalizable que puede distribuirse como parte de campañas multipropósito. Ha afectado a un 5,03% de las empresas españolas.

? Agent Tesla – Es un RAT avanzad que funciona como un keylogger y un usurpador de contraseñas que ha estado infectando ordenadores desde 2014. AgentTesla es capaz de monitorizar y registrar las teclas marcadas pulsadas por la víctima, el portapapeles del sistema toma capturas de pantalla y extrae credenciales pertenecientes a una variedad de software instalado en la unidad de la víctima (incluyendo Google Chrome, Mozilla Firefox y el cliente de correo electrónico Microsoft Outlook). Esta RAT ha atacado al 3,48% de las empresas en España.

Los sectores más atacados en Europa

Este mes, la educación/investigación es la industria más atacada a nivel mundial, seguida de las comunicaciones y el gobierno/militar.

Educación/investigación
Servicios públicos
Comunicaciones

Top 3 vulnerabilidades más explotadas en noviembre:

? Servidores web con URL maliciosas con directorio transversal (CVE-2010-4598,CVE-2011-2474,CVE-2014-0130,CVE-2014-0780,CVE-2015-0666,CVE-2015-4068,CVE-2015-7254,CVE-2016-4523,CVE-2016-8530,CVE-2017-11512,CVE-2018-3948,CVE-2018-3949,CVE-2019-18952,CVE-2020-5410,CVE-2020-8260) – Existe una vulnerabilidad de cruce de directorios en diferentes servidores web. La debilidad se debe a un error de validación de entrada en un servidor web que no sanea adecuadamente la URL para los patrones de recorrido de directorios. El éxito de la explotación permite a los ciberdelincuentes remotos no autentificados revelar o acceder a archivos arbitrarios en el servidor vulnerable.

? Revelación de información del servidor web Git - La explotación exitosa de la vulnerabilidad de divulgación de información en el Repositorio Git. permite compartir de forma involuntaria información de la cuenta.

? Ejecución remota de código en encabezados HTTP – Las cabeceras HTTP permiten que el cliente y el servidor pasen información adicional con una petición HTTP. Un ciberdelincuente remoto puede usar un encabezado HTTP vulnerable para ejecutar código arbitrario en el equipo infectado.

Top 3 del malware móvil mundial en noviembre:

AlienBot - Esta familia de malware es un Malware-as-a-Service (MaaS) para dispositivos Android que permite a un atacante remoto, como primer paso, inyectar código malicioso en aplicaciones financieras legítimas. El ciberdelincuente obtiene acceso a las cuentas de las víctimas, y finalmente controla completamente su dispositivo.

xHelper - aplicación Android maliciosa que fue descubierta por primera vez en marzo de 2019. Se utiliza para descargar otras aplicaciones maliciosas y mostrar anuncios. Es capaz de esquivar los antivirus móviles, así como reinstalarse por sí misma en caso de que el usuario la elimine.

FluBot – FluBot es un malware botnet para Android que se distribuye a través de SMS de phishing, la mayoría de las veces haciéndose pasar por marcas de reparto de logística. Una vez que el usuario hace clic en el enlace dentro del mensaje, FluBot se instala y obtiene acceso a toda la información sensible del teléfono.

El Índice Global de Impacto de Amenazas de Check Point y su Mapa ThreatCloud están impulsados por la inteligencia ThreatCloud de Check Point Software. ThreatCloud proporciona inteligencia de amenazas en tiempo real derivada de cientos de millones de sensores en todo el mundo, sobre redes, endpoints y móviles. La inteligencia se enriquece con motores basados en IA y datos de investigación exclusivos de Check Point Research, la rama de inteligencia e investigación de Check Point Software Technologies.

La lista completa de las 10 familias principales de malware en octubre está disponible en el blog de Check Point Software.

Datos de contacto:
EverythinkPR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Hardware Software Ciberseguridad Dispositivos móviles