Publicado en Madrid el 13/07/2022

El malware más peligroso del momento: Snake Keylogger escala al podium por primera vez

Check Point Research informa que Emotet ha aumentado su incidencia y además sigue siendo el malware que más impacto tiene alrededor del mundo, mientras que Snake Keylogger ha conseguido escalar hasta el podium

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 junio de 2022. Los investigadores han encontrado que Emotet sigue siendo el malware número uno y además ha aumentado alrededor de un 6% su incidencia global, pero lo ha hecho menos de un 1% en nuestro país. Siguiendo con su escalada del último mes, Snake Keylogger se cuela en los tres primeros puestos, empatando a Formbook con un 4,38% cada uno, lejos ambos aún de Emotet.

Emotet, ha afectado al 14% de las organizaciones de todo el mundo en junio, un aumento que supone prácticamente el doble con respecto al mes anterior. Este malware es muy rentable gracias a su capacidad para pasar desapercibido. Su persistencia también hace que sea difícil de eliminar una vez que un dispositivo se infecta, lo que lo convierte en la herramienta perfecta en el arsenal de un ciberdelincuente. Concebido como un troyano bancario, suele distribuirse a través de correos electrónicos de phishing y tiene la capacidad de incorporar otros malwares, lo que aumenta su habilidad para causar daños generalizados.

Hay otros malwares que tienen más incidencia en España como Raspaberry Robin, GuLoader y Wacatac. El primero se descubrió hace unos meses (septiembre de 2021) y se distribuye a través de unidades USB infectadas, además de utilizar varias funcionalidades legítimas de Windows para comunicarse con sus servidores de C&C y ejecutar cargas útiles maliciosas. GuLoader apareció por primera vez en diciembre de 2019 y se utilizaba para descargar Parallax RAT, pero se ha aplicado a otros troyanos de acceso remoto como Netwire, FormBook y Agent Tesla. Wacatac por último, es una amenaza troyana que bloquea los archivos pero no los cifra como el típico ransomware. Cuando Wactac se infiltra en el sistema del usuario, cambia los nombres de los archivos de destino añadiendo una extensión ''''.wctw''''.La falta de capacidad para cifrar los datos hace que esta amenaza sea reversible. Normalmente, Wactac se propaga mediante campañas de correo electrónico de spam y software falso.

“Snake Keylogger sigue ascendiendo en la escala de malware con más incidencia gracias a su facilidad para infectar información sensible”, afirma Eusebio Nieva, director técnico de Check Point Software para España y Portugal. “Junto al ascenso de Keylogger, también es importante notificar la subida de Emotet, que sigue reinando y con más presencia que en meses anteriores, gracias a su persistencia y técnicas de evasión. El hecho de que Emotet sea autopropagable y que Keylogger puede infectar cualquier tipo de archivo, hacen que estén tan arriba en la lista y hay que tener mucho cuidado con ellos.”, concluye Nieva.

Los 3 malware más buscados en España en junio:

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

1.? Emotet – Emotet es un troyano avanzado, autopropagable y modular que en su día se utilizó como troyano bancario y que actualmente distribuye otro tipo de malware o campañas maliciosas. Emotet utiliza múltiples métodos para mantener la persistencia y técnicas de evasión para evitar ser detectado y puede propagarse a través de correos electrónicos spam de phishing que contienen adjuntos o enlaces maliciosos.

? Formbook – FormBook es un Infostealer dirigido al sistema operativo Windows y fue detectado por primera vez en 2016. Se comercializa como Malware as a Service (MaaS) en foros clandestinos de hacking por sus potentes técnicas de evasión y su precio relativamente bajo. FormBook recolecta credenciales de varios navegadores web, recoge capturas de pantalla, monitoriza y registra las pulsaciones del teclado, y puede descargar y ejecutar archivos según las órdenes de su C&C.
? Snake Keylogger – Snake es un keylogger .NET modular y un ladrón de credenciales que se detectó por primera vez a finales de noviembre de 2020; su funcionalidad principal es registrar las pulsaciones de los usuarios y transmitir los datos recopilados a los actores de la amenaza. Las infecciones de Snake suponen una gran amenaza para la privacidad y la seguridad en línea de los usuarios, ya que el malware puede robar prácticamente todo tipo de información sensible y es un keylogger especialmente evasivo y persistente.

El Índice Global de Impacto de Amenazas de Check Point Software 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 mayo está disponible en el blog de Check Point Software.

Datos de contacto:
Ramón
633510672

Nota de prensa publicada en: Madrid

Categorías: Nacional E-Commerce Software Ciberseguridad Consumo Dispositivos móviles