Los actores de amenazas confían cada vez más en la técnica del contrabando de HTML en las campañas de phishing como un medio para obtener acceso inicial y desplegar una variedad de amenazas, incluido el malware bancario, los troyanos de administración remota (RAT) y las cargas útiles de ransomware.

Microsoft 365 Defender Threat Intelligence Team, en un nuevo informe publicado este jueves, reveló que identificó infiltraciones que distribuían el troyano bancario Mekotio, puertas traseras como AsyncRAT y NjRAT, y el malware TrickBot. Los ataques en varias etapas, denominados ISOMorph, también fueron documentados públicamente por Menlo Security en julio de 2021.

El contrabando de HTML es un enfoque que permite a un atacante *«contrabandear»* droppers de primera etapa, a menudo scripts maliciosos decodificados incrustados en archivos adjuntos HTML especialmente diseñados o páginas web, en una máquina víctima aprovechando las funciones básicas de HTML5 y JavaScript en lugar de explotar una vulnerabilidad o un defecto de diseño en los navegadores web modernos.

Al hacerlo, permite al actor de amenazas construir las cargas útiles de forma programática en la página HTML utilizando JavaScript, en lugar de tener que realizar una solicitud HTTP para buscar un recurso en un servidor web, al mismo tiempo que evita las soluciones de seguridad perimetral. Luego, los droppers HTML se utilizan para buscar el malware principal que se ejecutará en los puntos finales comprometidos.

> *«Cuando un usuario objetivo abre el HTML en su navegador web, el navegador decodifica el script malicioso, que a su vez, ensambla la carga útil en el dispositivo host. Por lo tanto, en lugar de que un ejecutable malicioso pase directamente a través de una red, el atacante crea el malware localmente detrás de un firewall»*, dijeron los investigadores.

La capacidad de HTTP Smuggling para eludir los proxies web y las puertas de enlace de correo electrónico, lo ha convertido en un método lucrativo entre los hackers patrocinados

por el estado y los grupos de ciberdelincuentes para distribuir malware en ataques del mundo real, según informó Microsoft.

Nobelio, el grupo de amenazas detrás del corte de la cadena de suministro de SolarWinds, se encuentra en el aprovechamiento de esta misma técnica para entregar Cobalt Beacon como parte de un ataque basado en correo electrónico sofisticado dirigido a agencias gubernamentales, grupos de expertos, consultores y organizaciones no gubernamentales situados frente a 24 países, incluyendo Estados Unidos.

Más allá de las operaciones de espionaje, el contrabando de HTML también se ha adoptado para los ataques de malware bancario que involucran al troyano Mekotio, y los atacantes envían correos electrónicos no deseados que contienen un enlace malicioso que, cuando se hace clic en él, desencadena la descarga de un archivo ZIP que, a su vez, contiene un Descargador de archivos JavaScript para recuperar binarios capaces de robo de credenciales y registro de teclas.

Pero en una señal de que otros actores están tomando nota e incorporando el contrabando de HTML en su arsenal, se descubrió una campaña de correo electrónico realizada en septiembre por DEV-0193, abusando del mismo método para entregar TrickBot. Los ataques implican un HTML malicioso adjunto que, al abrirlo en el navegador web, crea un archivo JavaScript protegido con contraseña en el sistema del destinatario, lo que solicita a la víctima que proporcione la contraseña del archivo HTML adjunto original.

Al hacerlo, se inicia la ejecución del código JavaScrit, que posteriormente lanza un comando de PowerShell codificado en Base64 para ponerse en contacto con un servidor controlado por un atacante para desplegar el malware TrickBot, lo que finalmente allana el camino para los siguientes ataques de ransomware.

> *«El aumento en el uso de contrabando de HTML en campañas de correo electrónico es otro ejemplo de cómo los atacantes siguen perfeccionando componentes específicos de sus ataques mediante la integración de técnicas altamente evasivas.*

> *Esta adopción muestra cómo las tácticas, técnicas y procedimientos (TTP) se filtran desde las bandas de delitos cibernéticos a los actores de amenazas maliciosas y viceversa. También refuerza el estado actual de la economía sumergida, donde tales TTP se mercantilizan cuando se consideran efectivos»,* dijo Microsoft.