Los expertos en ciberseguridad han delineado una versión actualizada de una avanzada herramienta de identificación y redireccionamiento denominada WoofLocker, diseñada con el propósito de llevar a cabo estafas de soporte técnico.

El elaborado esquema de redireccionamiento de tráfico fue inicialmente documentado por Malwarebytes en enero de 2020. Se vale de código JavaScript embebido en sitios web comprometidos para realizar comprobaciones de filtrado de tráfico web y detección de bots, con el fin de proporcionar código JavaScript de la siguiente fase que redirige a los usuarios hacia un bloqueador de navegadores (también conocido como browlock).

Esta estrategia de redirección, a su vez, utiliza artimañas esteganográficas para ocultar el código JavaScript dentro de una imagen en formato PNG que solo se entrega si la fase de validación tiene éxito. Si se identifica a un usuario como un bot o como tráfico no relevante, se utiliza un archivo PNG falso que carece del código malicioso.

WoofLocker es también llamado 404Browlock debido a que intentar acceder directamente a la URL del browlock sin la redirección adecuada o el token de sesión de un solo uso resulta en una página de error 404. El análisis más reciente de la firma de ciberseguridad indica que la campaña aún está en curso.

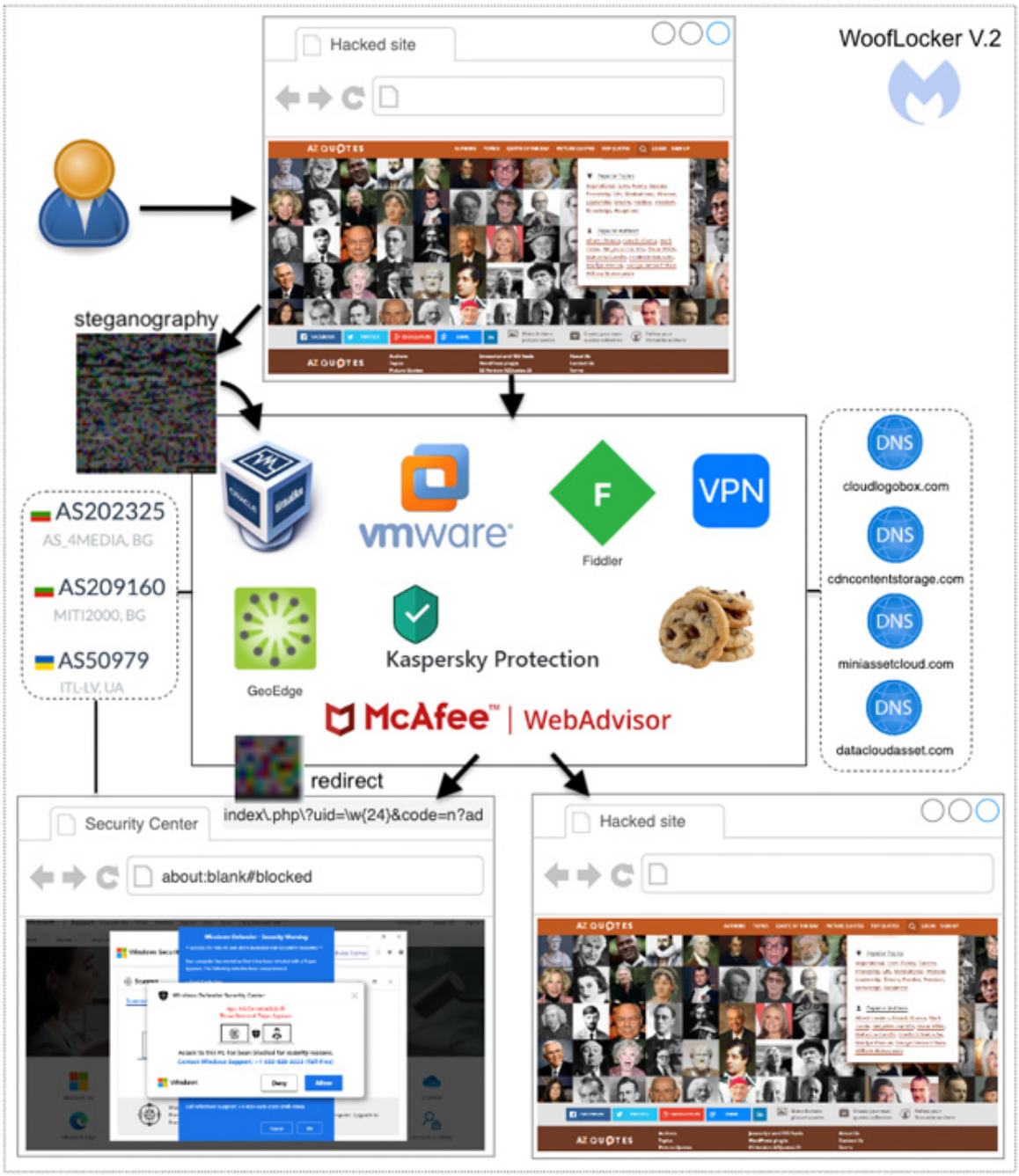
> *«Las tácticas y técnicas son muy parecidas, pero la infraestructura es ahora más resistente que antes para frustrar posibles intentos de eliminación»*, comentó Jérôme Segura, director de inteligencia de amenazas en Malwarebytes.

> *«Resulta igualmente complicado reproducir y estudiar el mecanismo de redirección en la actualidad que en aquel entonces, sobre todo a la luz de nuevas comprobaciones de identificación para detectar la presencia de máquinas virtuales, ciertas extensiones de navegador y herramientas de seguridad».*

La mayoría de los sitios que cargan WoofLocker son sitios web dirigidos a un público adulto, y la infraestructura utiliza proveedores de alojamiento en Bulgaria y Ucrania que otorgan a los actores de amenazas una mayor protección contra intentos de eliminación.

El objetivo principal de los bloqueadores de navegadores es persuadir a las víctimas seleccionadas a solicitar asistencia para resolver problemas informáticos (que en realidad no existen) y obtener control remoto sobre la computadora para elaborar una factura que recomienda a las personas afectadas que adquieran una solución de seguridad para abordar el problema.

> *«Esto es gestionado por terceros a través de centros de llamadas fraudulentos. El actor de amenazas detrás de la redirección de tráfico y el browlock recibirá pago por cada cliente potencial que resulte exitoso»,* mencionó Segura en 2020.



La identidad precisa del autor de la amenaza sigue siendo un misterio, y existen pruebas de que los preparativos para la campaña comenzaron tan temprano como en 2017.

> *«A diferencia de otras campañas que confían en la compra de anuncios y en la constante persecución de proveedores de alojamiento y registradores, WoofLocker es un negocio muy estable y requiere poco mantenimiento. Los sitios web que alojan el código malicioso han estado comprometidos durante años, mientras que la infraestructura de identificación de huellas digitales y bloqueo de navegadores parece estar respaldada por registradores y proveedores de alojamiento sólidos»*, señaló Segura.

Esta revelación coincide con la descripción de una nueva cadena de infección por malvertising que implica el uso de anuncios falsos en motores de búsqueda para dirigir a usuarios que buscan programas de acceso remoto y escáneres hacia sitios web trampa que conducen a la instalación de malware ladrón.

Lo que distingue a esta campaña es su capacidad para identificar a los visitantes mediante la API WEBGL_debug_renderer_info para recopilar las propiedades del controlador de gráficos de la víctima y distinguir entre navegadores legítimos, rastreadores y máquinas virtuales, para luego exfiltrar los datos a un servidor remoto con el fin de determinar el siguiente paso.

> *«Al utilizar un filtrado más efectivo antes de redirigir a posibles víctimas hacia el malware, los actores de amenazas aseguran que sus anuncios maliciosos y su infraestructura permanezcan en línea durante más tiempo. Esto no solo dificulta que los defensores identifiquen y denuncien tales eventos, sino que también probablemente tiene un impacto en las acciones de eliminación»*, explicó Segura.

Este desarrollo también sigue a una nueva investigación que descubrió que sitios web pertenecientes a agencias gubernamentales de los Estados Unidos, destacadas universidades y organizaciones profesionales han sido secuestrados durante los últimos cinco años y se han utilizado para promocionar ofertas y promociones fraudulentas a través de archivos *«PDF envenenados»* cargados en los portales.

Muchas de estas estafas están dirigidas a niños y pretenden engañarlos para que descarguen aplicaciones, malware o proporcionen datos personales a cambio de recompensas inexistentes en plataformas de juegos en línea como Fortnite y Roblox.