R0BL0CH0N TDS: A deep dive into the infrastructure of an affiliate marketing scam

orangecyberdefense.com/global/blog/cert-news/r0bl0ch0n-tds-a-deep-dive-into-the-infrastructure-of-an-affiliate-marketing-scam

Author: Simon Vernin, CERT Analyst (World Watch Team)

Executive Summary

- Affiliate marketing is a marketing strategy in which businesses reward affiliates for driving traffic or sales to their website. While being a legitimate and widely used marketing technique to boost traffic and sales for a product or service, affiliate marketing is also used in numerous malicious schemes promoting sweepstakes, home improvement services, casinos, or dating sites.
- Hundreds of small affiliate networks promote **primarily dubious affiliation offers** that lead to well-known scams.
- Affiliates are specialists in traffic generation and use their skills to **distribute various types of content, ranging from legal advertising to direct malware distribution.**
- The World Watch team has identified a previously undocumented Traffic Distribution System (TDS) linked to affiliate marketing being used in scams that **impacted around 110 million of Internet users**. We have named it **R0bl0ch0n TDS** based on specific patterns in the URL redirections: "0/0/0".
- This TDS infrastructure consists of numerous domains and dedicated servers protected behind Cloudflare. Even if the threat actor includes legitimate features such as unsubscribe and contact forms, steps are taken to hide the real entity behind these campaigns.
- IOCs can be found on our GitHub page here.

Note: The analysis cut-off date for this report was end of May, 2024

Introduction to affiliate marketing

Key concepts and stakeholders

Affiliate marketing is a marketing strategy in which businesses reward affiliates (partners or “partnerka" in Russian) for driving traffic or sales to their website. Here’s a breakdown of the key concepts:

1. **Merchant or advertiser:** The business or brand that wants to promote its products or services.
2. **Affiliate marketer (also called publisher):** An individual or company that promotes the merchant’s products or services in exchange for a commission on leads or sales generated.
3. **Affiliate network:** An interface (website, tool) that connects merchants with affiliates, offering tracking, reporting, and payment features. Not all affiliate programs use a network; some are run directly by the merchant.
4. **Customer:** The end-user who interacts with the affiliate’s marketing efforts and completes the desired action (e.g., providing his data, making a purchase…).

5. **Commission:** The payment made to the affiliate, typically a percentage of the sale or a fixed amount per action.

You've certainly already come across affiliate marketing on numerous occasions. When 50 different YouTube content creators promote the same product (a video game, an online bank, etc.) to drive up sales for a brand, they're engaging in affiliate marketing! In this case, the content creators serve as the affiliate marketers,while the brand they're promoting corresponds to the merchant.

Content creators are indeed one type of affiliate marketers, though prehaps not the most representative example. Most affiliate marketing campaigns are more abstract and typically leverage:

- Direct offer dissemination
- Sites that display ads or coupon
- Personal blogs
- Cashback portal

Usually, affiliate marketers tend to be specialized in specific **verticals** (including crypto, gambling, dating sites, sweepstakes) and rely on specific delivery means, such as social networks, SEO, SMS, or email.

Through an affiliation code or link, the merchant keeps track of the earnings made thanks to the affiliate marketer and compensate them through a cashback for each effective sell or download. In this case, the fact that a partnership established between the merchant and an affiliate marketer is generally clearly stated.

Affiliate networks

The merchant often lets a third-party handle tracking and payment to the affiliate marketers. This third-party intermediary is known as an **affiliate network.** Affiliate networks consist of interfaces or hubs that centralize offers for various products or services and connect merchants to marketers. For instance, if you own a blog of computer reviews, you can apply to a dedicated affiliate program that will generate a unique affiliate link for you to mention in your articles. Merchants will reward you for any product (let's say a computer!) bought by your readers.

Existing affiliate hubs are extremely diverse. Some hubs have strict requirements and KYC measures to verify affiliates' ID, while others offer quick signups with dubious levels of transparency. **Importantly, in many of these affiliate networks, advertising offers for legitimate products systematically coexist with shady deals or even malicious scams**, ranging from free gift cards or dating and crypto mobile applications to "miracle" traditional medicine offers.

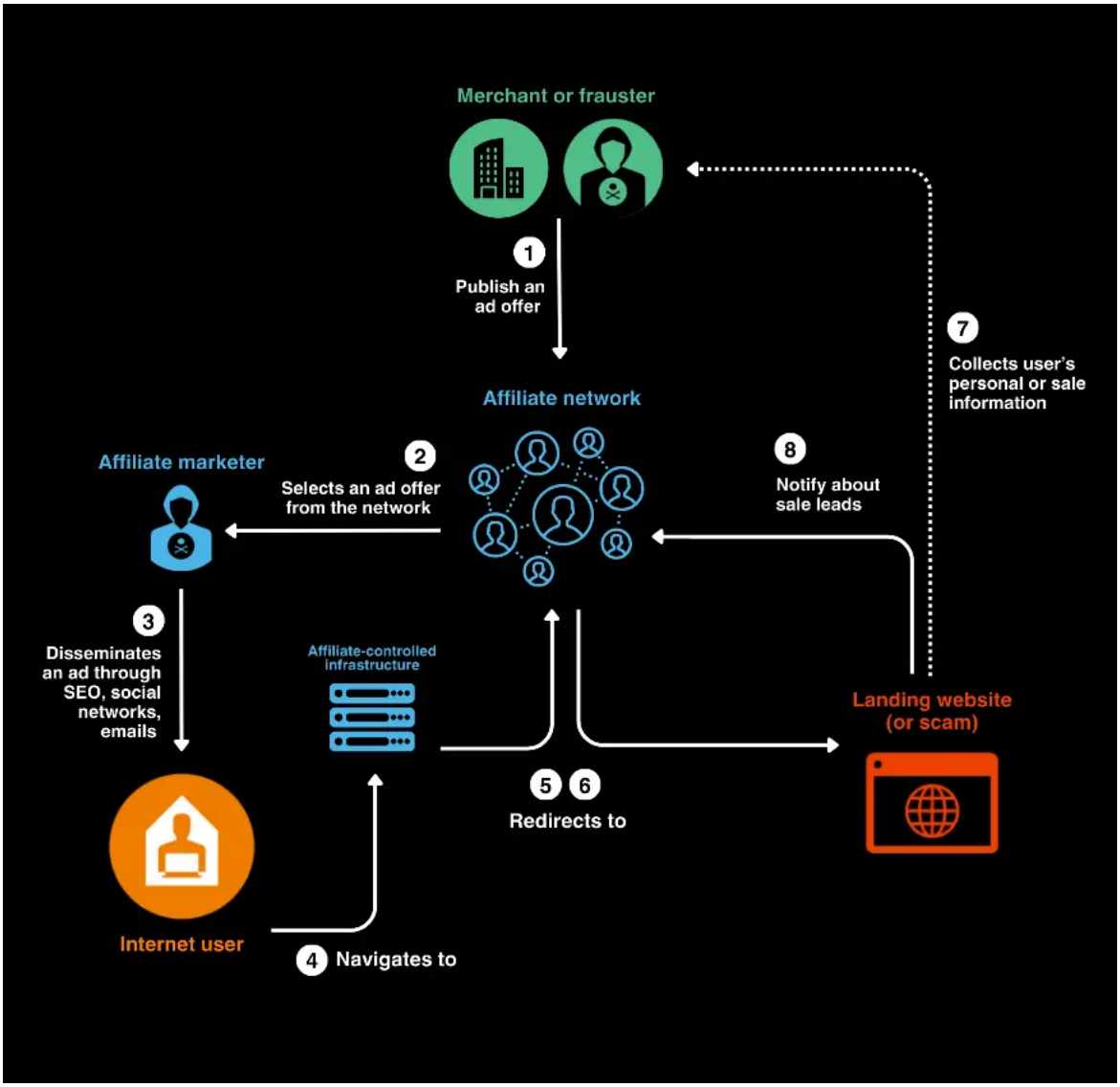

Figure 1: Lifecycle of an affiliate offer

Affiliate networks aggregators

Alongside traditional affiliate networks, some platforms such as Affplus or OfferVault aggregate offers from numerous affiliate networks into one centralized interface. On these platforms, the offers are classified by verticals, by **geos** (the countries where the offer should be advertised), and by affiliate network entities. Often, the offers contain:

- The preview of the landing page (i.e., the final scam page)
- Restrictions on the ad distribution such as “No SEO”, “Only emails”
- Commission rates (i.e., the price paid by the “Merchant” for reaching a specific number of users, either clients or victims)

Examples of widespread fraud scheme

Upon analysis of these marketing hubs, we have distinguished two types of offers of particular interest, as they are associated with well-known scams:

> **Sweepstakesoffers**. Consisting of attractive lottery winning messages such as “CONGRATULATIONS, you won an iPhone,” these ads are often disseminated by affiliate marketers via email. After filling out a small online survey, users are then asked to pay a small shipping fee, which in fact signs them up to a recurring payment (between 20-45€ every two weeks). The Federal Trade Commission has published a consumer advisory on this type of scam, pointing out that they have received complaints amounting to more than $300 million in loses with an average of $900 per victim. This figure is way below our own estimates, considering the sheer number of campaigns sent daily.

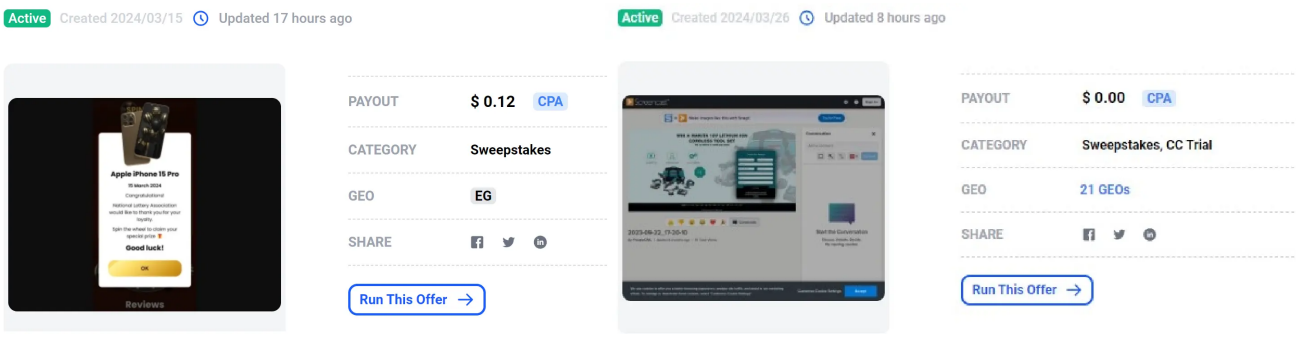

Figure 2: Sweepstake offers for an iPhone 15 and a Makita tool set

Home improvement offers. This category of ads offers overpriced gutter filters installations, solar panels, heat pumps, or showers for the elderly. These scams are often sent via emails and/or promoted through SEO. Each time a user fills a contact form for these home installations, the affiliates earn a commission from the merchant, who then calls the potential customer back. Often, these domestic works are offered by merchants who falsely inflate the government subsidies the customer is eligible to.

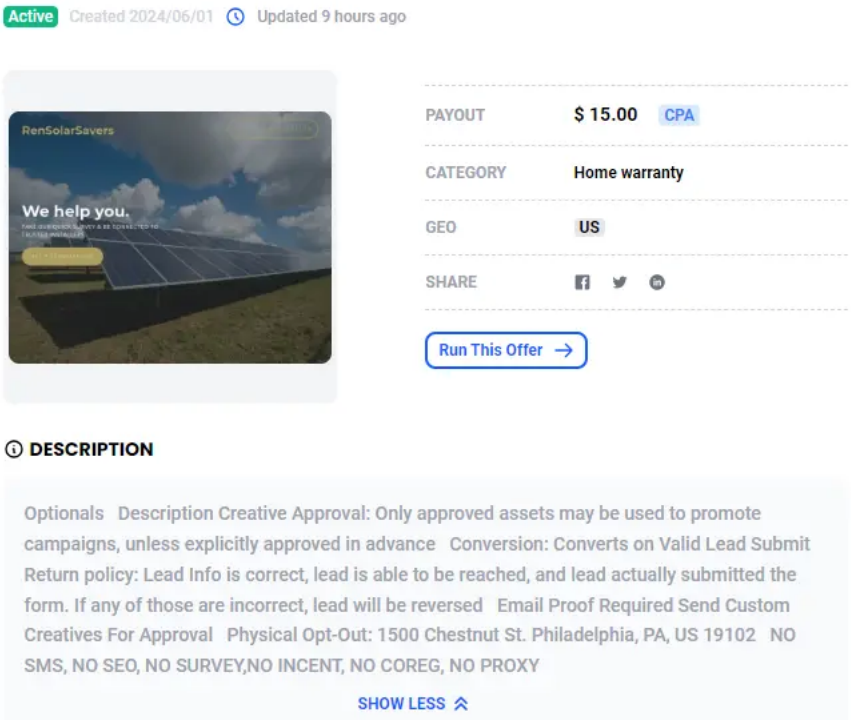

Figure 3: Solar panel offer with details on what is a valid lead

R0bl0ch0n technical analysis

Context

On May 15, 2024, Palo Alto Networks's Unit 42 published a thread on GitHub about a credit card infostealing campaign that used deceptive emails redirecting to enticing fake shops or surveys, overlapping with those observed in this investigation on affiliate marketing.

The goal of our report is to describe and document the redirection chain that occurs in this campaign, including the TDS that we have dubbed **R0bl0ch0n** (because we are cheese loversc!) and its associated tracking infrastructure.

Traffic distribution system

Building on the key indicators of the campaigns detailed by Palo Alto Networks, we noticed that the URLs embedded in the emails all follow the same patterns (**<domain>/bb/[0-9]{18}**). These URLs have several automatic redirects leading users to either fake shops or fake surveys. Similar URLs are easily found on URLScan; however, they are not properly crawled since user interaction is required on the page to bypass a fake captcha.

Upon analysis, we noticed some of these redirections seem to go through a **Traffic Distribution System (TDS),** which filters and redirects users to scam sites based on their fingerprints. The TDS presence is recognizable by the pattern "**0/0/0"**, which led us to dub this TDS **R0bl0ch0n**. As a reminder, TDS are systems that analyze incoming web traffic and redirect in accordance with the rules set by the operator.

The traffic generated for the fake shops is stamped with special tracking parameters, designed to identify the affiliate from which the traffic originates (affId, c1, c2, c3 parameters). These affiliate parameters are likely related to Konnektive CRM, a sales and affiliate management CRM tool developed by a small Puerto Rican company. In the case of fake surveys, similar tracking parameters are also added to the URL, but only once the user fills out the survey and reaches the final landing page.

Bellow, is a complete redirection chain from the initial URL contained within the spam to the final survey page.

Status Code	URL	IP	P
200	www.connected.chance-impression.com/bb/620218704269530479	45.145.179.198	Ir
302	www.connected.chance-impression.com/bb/decrypt2NEW.aspx	45.145.179.198	s
200	www.connected.chance-impression.com/EmailValidator.aspx client>&cn=<string>&uid=<uuid>	45.145.179.198	cl
200	atlilacstreet.com/0/0/0/7e0d2470daabd2fa4d3beca1824bd1b8/A6B16CB5E4AE4692C997B0274BA8DF1A/<same uuid>	94.154.173.187	cl
200	edictpage.lat/004/f650b42b3bc7abf8f2611610ea45d6ebx/118801820302/35093201/ow/194903	104.21.1.165	n
200	edictpage.lat/14f7234c42f0f9d327d8577097f03015	104.21.1.165	fi

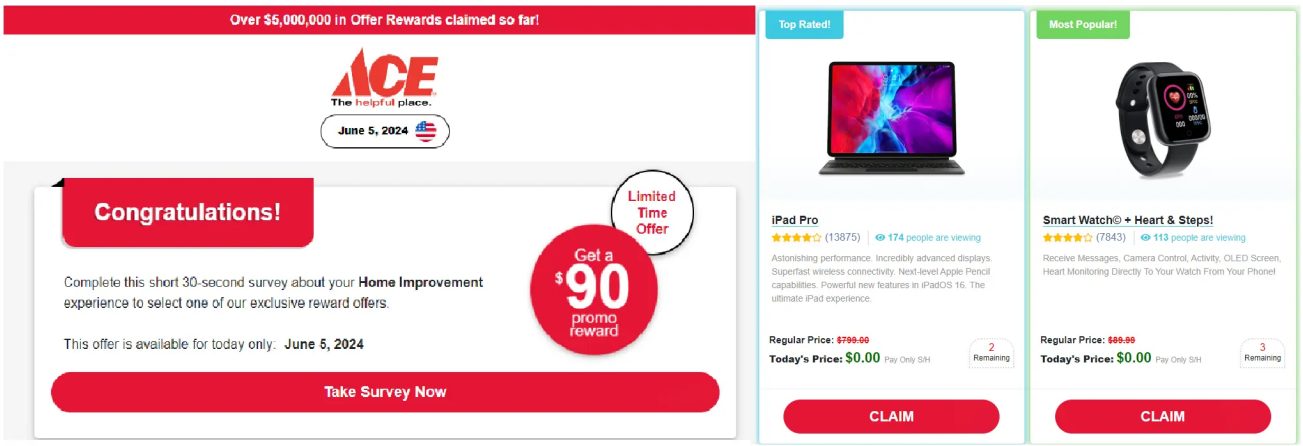

Figure 5: Final page of the campaign: ACE sweepstake survey and gifts

This redirect chain is quite interesting:

- The **chance-impression.com** domain seems to perform several checks on the server side, in particular a check to see if the user IP has already accessed this page. Trying to access the same URL twice in a row will redirect the internet user to legitimate websites such as Yahoo or YouTube. Accessing the same URL with a new IP address may result in a similar redirect chain with a different final page. This infrastructure is **likely operated by an affiliate.**
- The final URL shares the same fake survey pattern as the one in the Palo Alto Networks report (**<domain>/[a-f0-9]{32}**). Upon completing the survey and choosing a reward, the user is redirected through another series of pages, the final one resembling the fake shop URLs shared by Palo Alto Networks (with an **affId=** parameter). Themes and advertised products are also similar. These URLs, which include all the affiliation-related parameters, indicate that this part of the infrastructureis **likely operated by an advertiser**.
- The user goes through the R0bl0ch0n TDS domain recognizable by the **0/0/0** pattern, as will be detailed later. This infrastructure is used for tracking purposes and is **likely operated by an affiliate network**.

By searching for URLs matching this pattern in Urlscan and in our Orange telemetry, we were able to identify more than 250 domains used in May 2024 (see Appendix for the full list). These domains have a short lifespan and are mainly hosted on shared servers under Quadranet and Baxet AS.

Number of domains	AS	AS number
50	Quadranet (US)	AS8100

Number of domains	AS	AS number
57	Baxet (RU/US)	AS49392/AS398343
17	Cogent (US)	AS174
14	Eurocrypt (BG)	AS25211
13	Madgen (US)	AS55154
10	SEDO (DE)	AS47846

Some URLs associated with this **0/0/0** TDS lead to an unsubscribe form. It is possible to reuse a valid URL path leading to the unsubscribe form to ensure that the detected domains are part of this TDS, as the same logic is shared among all the TDS nodes.

Because TDS domains are hosted on shared infrastructure with a short lifespan and do not seem to follow an obvious naming pattern, the discovery of new domains is difficult. The same conclusion applies to fakes surveys domains such as **edictpage.lat**, which are protected by Cloudflare and are heavily rotated. However, these domains communicate with another cluster of domains that are used as tracking domains and provide some insights into the scale of this infrastructure.

Tracking infrastructure

Domains hosting fake survey webpages share user data with third-party websites. For instance, the domain **facileparking.sbs** shares data with **event.trk-adulvion.com**. This domain is hosted behind Cloudflare; however, the **event.trk-** pattern is quite unique, and pDNS databases allow the discovery of about 30 similar domains hosted behind Cloudflare. The complete pattern of exchanged data is as follows:

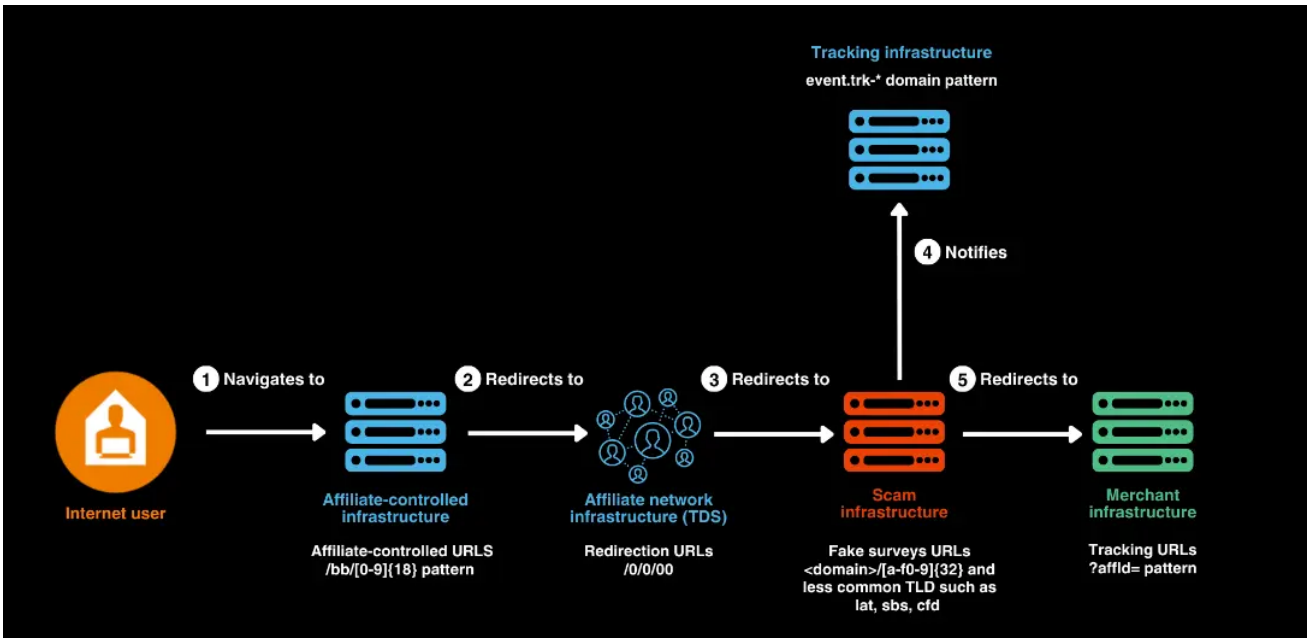

Figure 6: Complete overview of a redirection chain including TDS and tracking infrastructure

This domain cluster became active in the summer of 2021, according to pDNS databases. All these domains host the same content, so it is possible to uncover the real IP of these domains thanks to a Censys query. The latter reveals more than 300 dedicated AWS IP addresses hosting this specific page.

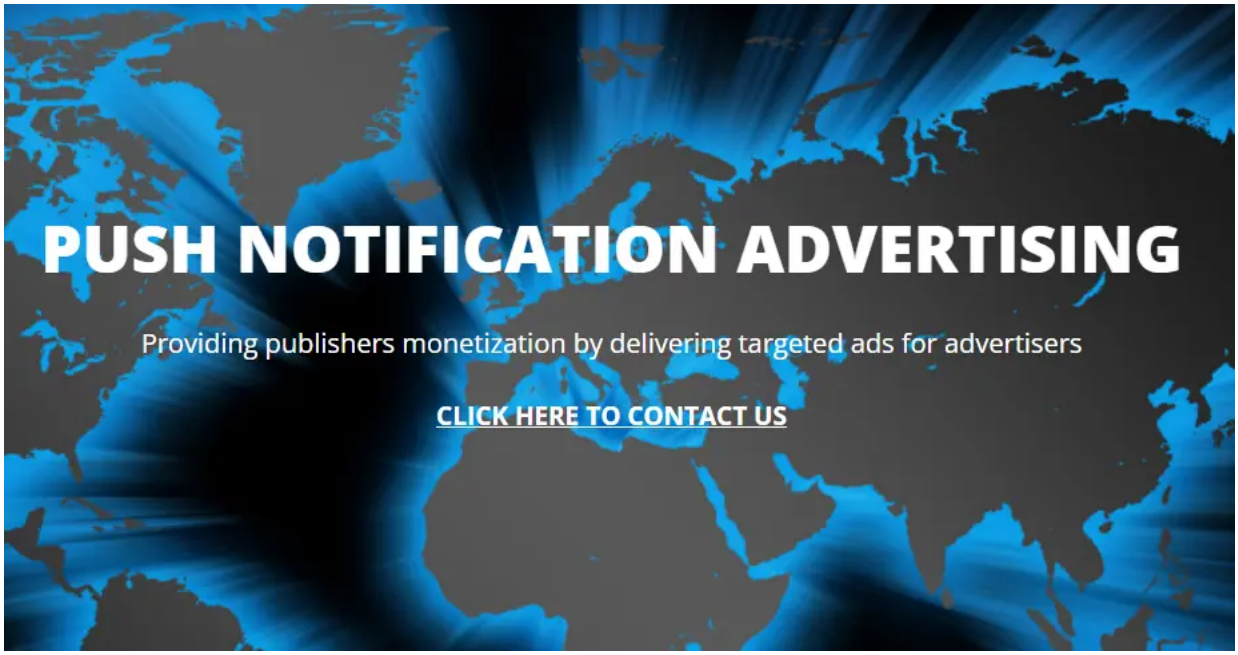

Figure 7: Page shared among all the tracking domains

The website, titled “Push Ads,” features visuals that suggest it is part of an affiliate network infrastructure. The presence of a “Work with us” form link further supports this hypothesis. However, at the time of writing, World Watch has not been able to identify the specific affiliate network operating this TDS.

According to DomainTools, the cumulative total of DNS A queries for these **event.*** subdomains since 2021 is around 110 million. User fingerprinting ensures that only one DNS query is registered per user, making this figure a good indicator of the total number of people targeted by the scams propagated through this affiliate network. Furthermore, all the domains are linked to **subscription.*** subdomains (in addition to the event ones). Together, these subdomains account for more than 3 million DNS queries. No direct query to this endpoint was identified during our analysis, suggesting it is likely requested only after a user successfully subscribes to the advertised services.

Some words on affiliates

Several distinct vectors are used for the initial dissemination of the URLs that redirect through the R0bl0ch0n TDS, indicating that these campaigns are likely carried out by different affiliates. For instance, in the Palo Alto Networks report, we noted that the affiliate used the same domain to send the email (From field) and in the scam URL. These domains are hosted by a provider called BADGER-BV (AS42881), based in Moldova, and the associated IP addresses have SMTP port opened with a unique banner.

Additional patterns that suggest the involvement of different affiliates include:

- Use of random AWS subdomains with data in the URL fragment part that are passed to R0bl0ch0n TDS and are likely to be related to affiliation parameters. (cf UrlScan)
- Use of random Azure subdomains with URLs matching this pattern **<random_subdomain>.blob.core.windows.net/<random_subdomain>/1.html**. Data in the URL fragment is also passed to R0bl0ch0n TDS. (cf. UrlScan)
- Use of URL shorteners (cf. UrlScan)

Leveraging legitimate services such as AWS, Azure infrastructure, or URL shorteners allows the affiliates to easily modify and deploy new infrastructure to bypass detection and countermeasures implemented by Google Safe Browsing or anti-spam filters.

Wrap-Up

Although it is unclear whether this infrastructure is exclusively used for malicious purposes, it openly supports such activities. We therefore recommend blocking this infrastructure as it could potentially be used at any time to deliver malware or phishing, in addition to the usual scams.

Orange Cyberdefense’s Datalake platform provides access to Indicators of Compromise (IoCs) related to this threat, which are automatically fed into our Managed Threat Detection services. This enables proactive hunting for IoCs if you subscribe to our Managed Threat Detection service that includes Threat Hunting. If you would like us to prioritize addressing these IoCs in your next hunt, please make a request through your MTD customer portal or contact your representative.Orange Cyberdefense’s Managed Threat Intelligence [Protect] service offers the ability to automatically feed network-related IoCs into your security solutions. To learn more about this service and to find out which firewall, proxy, and other vendor solutions are supported, please get in touch with your Orange Cyberdefense Trusted Solutions representative.