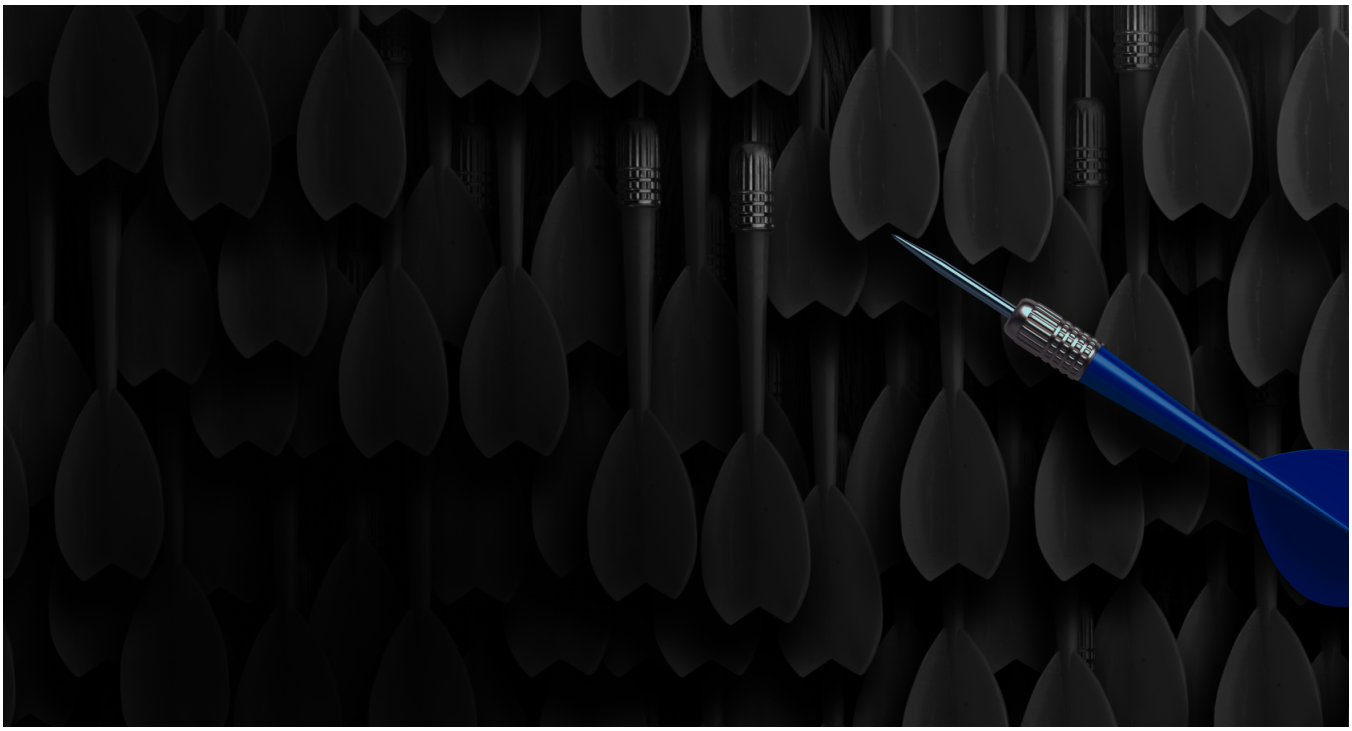
Ready-made fraud

blog.group-ib.com/target



21.12.2021

Behind the scenes of targeted scams

Yakov Kravtsov

Head of Special Projects Department

Yvgeny Egorov

Lead Analyst at Special Projects Department

Dear customer! Congratulations! You are one of the 100 users that we selected to receive the chance to win an [sic] Samsung Galaxy S10, Samsung Galaxy S9 or Apple iPhone 12. You have 4 minutes and 27 seconds to answer the following questions before we give your gift to another happy user! Good luck!

Some of those "lucky ones" who bought the story that they were a winner and rushed to answer the questions eventually lost their money. Messages about lotteries and surveys are one of the most popular scamming schemes, and they have recently increased in scope, their technological sophistication, personalization scale, and last but not least, severity.

One of the major success factors behind this scheme is the use of special targeted links, customized for a specific victim. Group-IB Digital Risk Protection analysts have recorded the presence of this targeted scam in over 90 countries worldwide, with over 120 international brands exploited in the fraudulent campaign. To learn why this scam is so hazardous and how exactly the targeted scam works, read our new blog post.

Personal approach ensured

Just a couple of years ago — in 2017-2019 — online scams were focused on the mass character: by indiscriminately targeting users, cybercriminals tried to ensure that at least someone would take the bite.

Link redirecting user to the targeted link, placed on an adult site

This idea formed the basis of popular scams with fake giveaways, surveys and reimbursement of non-existent benefits. Over time, fewer and fewer people fell prey to such schemes. This made it much more difficult for cybercriminals to make money, which was further exaggerated by the frequent blocks of the fraudulent infrastructure. Those events pushed scammers to search for more sophisticated ways of fulfilling their financial ambitions.

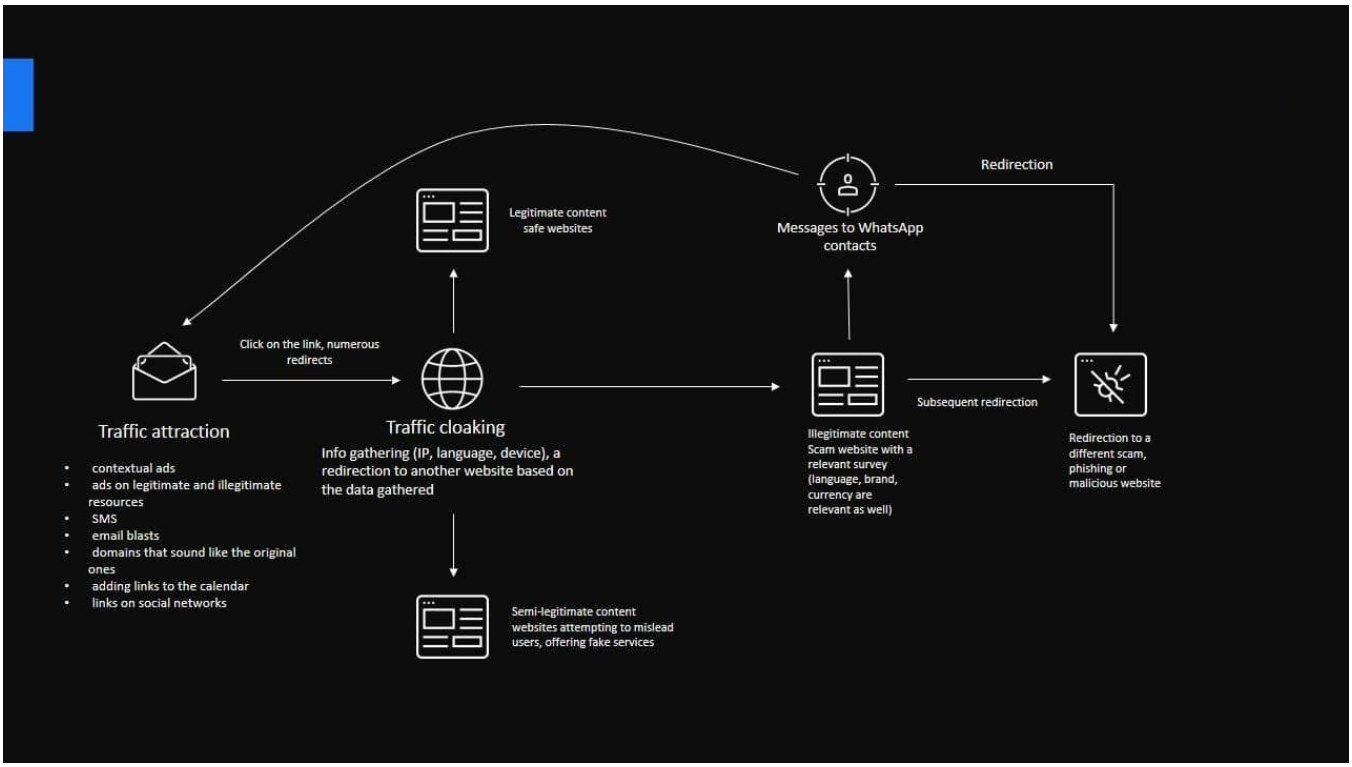
The mass SMS sending, and the waves of messages in messengers and emails were replaced by the so-called personal approach. Now, threat actors generate a unique **targeted link** customized for their victim, which utilizes the potential victim's unique parameters (country, time zone, language, IP, browser, and etc.) to display the relevant content on the scam page.

The targeted link most frequently leads to the website with the notorious surveys, which, however, now are tailored for the user. Even if a user suspects anything wrong in time, the targeted link cannot be blocked, as it's customized. Scammers create a targeted link customized for a specific user so that it doesn't display any content to those who attempt to follow it without specific cookies. But first things first, let's check how the fraudulent scheme works, what risks it entails and how one can protect against it.
Targeted links: how do they work?

We once received a request from one of our customers to analyze a fraudulent link. The customer informed us that they were not able to open the link and see the content. We examined the link and found out that scammers exploited over a hundred brands.

In Singapore, visitors to the thepiratebay.cc torrent tracker received a personal link leading to the fake site allegedly belonging to a Singaporean mobile network operator (traffic: 13,500 people per day)

Judging from Group-IB DRP team's experience, this is quite a common case; this kind of content does not live long. Nevertheless, the resource was sent for analysis. It turned out that the problem was much deeper, and the mechanism to create targeted links had considerably changed.



The scheme illustrating how targeted links work

The analysis showed that the scammers used all the available tools to distribute the malicious link: contextual advertising, advertising on legal and completely illegal sites, SMS, mailouts, and buying domains that sound like the original ones. Adding links to the calendar and posts on social networks, which were trendy at that time, were less common. The mail outs and SMS almost always contained a short link, which had information about a customer motivation program, where the user could win an expensive device.

Next, the scammers resorted to the so-called **traffic cloaking**. This is a popular way of distributing traffic, where one user sees legitimate content and the other semi-legitimate or illegal content depending on the redirection conditions (IP, language, device). Legitimate content is completely unremarkable and does not pose any threat. It does not raise any questions from advertisers or providers. Semi-legitimate and illegal content, on the other hand, violate advertising distribution rules and pose a great threat to users, especially the inattentive ones.

Cloaking is prohibited by all ad networks, but the scamming is often not immediately recognized, even with the help of special software. Advertising can "live" on the site for a very long time. In addition, this type of fraud is spread by more than one person and not even one group of people. This is a massive network. When part of the fraudulent accounts that spread illegal traffic is blocked, new ones instantly appear; this is one of the reasons why this scheme is very difficult to eliminate.

When following the link, the user was sent into a chain of redirections, after which they received something like this:

https://y****s.site/s10xs/***/?
osv=Windows%2010.0&isp=G***S%20T***m&ip=***.***.***.111&key=eyJ0aW1lc3RhbXAiOiIxNTU0Mzg4MjYzIiwiaGFzaCI6IjIwZGQwM2I2Y2
UxMDI1NzJhZWY1NDM0MTZhNzZjODY2ZjIyYzZmZDgifQ%3D%3D&td=7ktpj.b***k.com&bemobdata=c%3D227bad15-b386-42e0-911b-
674575ed6cd8..a%3D0..b%3D0..e%3D1554388262666418..c1%3D9627..c2%3D9254..c3%3D1554388262666418..r%3Dhttps%253A%252F
%252F***t.ru%252Fgoto%252F9254%252F44db6ebf9c%252F#

01

After a while, the links began to change their form, removing the referrer (the site from which the user came), making the link less informative for analysis:

https://ca****k/pr/i12/brand/m***o/
?osv=Windows%2010.0&isp=Chrome&tid=1aa56077-f400-4910-92c6-
bb249266438d&key=eyJ0aW1lc3RhbXAiOiIxNjA3OTQzODExIiwiaGFzaCI6IjUzZGExNmE3YWU5NzJmMTEyMTMyMDc2YzZiOGMyNTU4NDdl
NDI3YjUifQ%3D%3D&td=t.w***k.click&bemobdata=c%3Df84cec94-089f-4dbd-8b13-2f9ddea20bb4..a%3D0..b%3D1#

02

Now the URLs have become short, which makes it very difficult to analyze and respond to these violations, because when you receive this kind of link, it becomes very difficult and sometimes impossible to reach the regulator with explanations.

https://e***.click/cz/i12/brand/m***l/

03

The next problem in eliminating this type of fraud is the modus operandi of the link the user follows.

When a user clicks on a banner, contextual ad, a malicious link from an email, or even an SMS, they are not immediately redirected to a static site. Firstly, the user is redirected many times, with data being collected from them each time: geolocation, language, browser, provider name.

Based on this information, a final fraudulent link is automatically generated; this includes a timestamp — the information about the date and time. This specific link is unique and will work only once and only for a specific user.
When eliminating such schemes, a specialist usually faces the following difficulties:

such links are very difficult to detect

the scam is very difficult to respond to promptly

the time of resource operation is significant

The most interesting part is the content on the fake website. It can be absolutely different, and the scammer may attempt to exploit random brands or the brand the victim frequently uses.

On these sites, surveys are conducted, allegedly on behalf of a large company. Very often scammers promise a large prize for completing the poll. But after completing this survey, the user will be asked to fill out a form with their personal data in order to receive the prize. As a rule, the system requires the user to provide the following information:

Scammers may use different templates for the phishing sites:

Using this data, the attackers can easily make online purchases on your behalf, sell this data on the black market, or create accounts anywhere on the Internet, using your personal data.

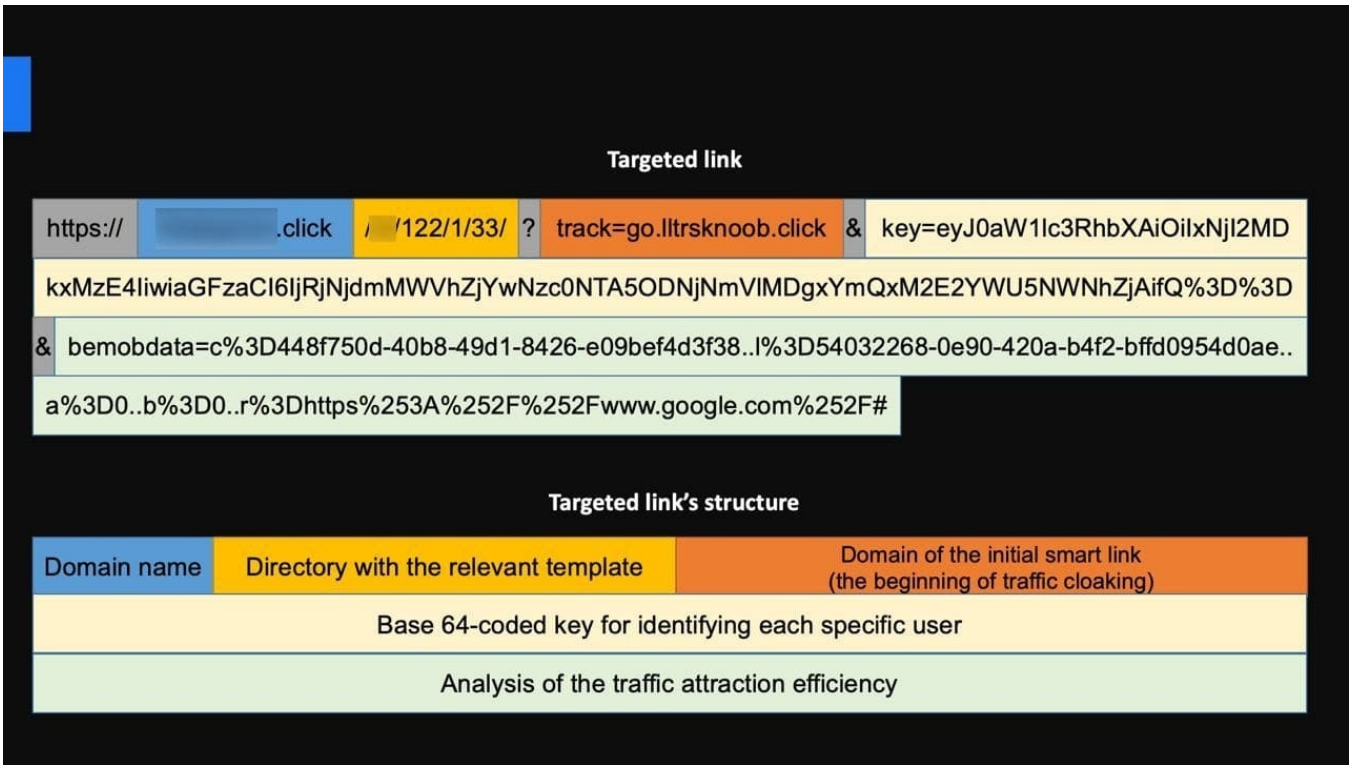
The scammers can also immediately ask the user to transfer an amount of money. For example, as a test payment or tax, which is allegedly imposed on the prizes.

It should be noted that besides phishing, the link can pose other threats. There are also other options for monetization such as malware, direct debiting of funds, or the purchase of subscriptions using your personal data.

Examining the targeted link: what's inside?

The structure of a targeted URL varies to a certain extent, but can be divided into several parts.

The first part redirects the user to a directory on a website, which stores material selected for particular users based on information available about them: country, location, brand, etc.



The structure of a targeted link

Examples of URLs with different directories:

1

https://f****n.click/***/122/1/33/?
track=go.l***b.click&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDkxMzE4IiwiaGFzaCI6IjRjNjdmMWVhZjYwNzc
0NTA5ODNjNmVlMDgxYmQxM2E2YWU5NWNhZjAifQ%3D%3D&bemobdata=c%3D448f750d-40b8-
49d1-8426-e09bef4d3f38..l%3D54032268-0e90-420a-b4f2-
bffd0954d0ae..a%3D0..b%3D0..r%3Dhttps%253A%252F%252Fwww.google.com%252F#

2

https://s***r.click/kr/i12/****/a***n/?
ts=08e29a07-b84a-41cf-a9c0-1cb114072fbc&camp=&zone=&landid=22b8a4d3-9ef6-496e-bf40-a48c
5e1fff2d&osv=Windows%2010.0&isp=G***S%20T***m&tid=08e29a07-b84a-41cf-a9c0-
1cb114072fbc&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDk2MTUwIiwiaGFzaCI6IjJhNjllZWU1YmI1ZjViZTJiODgw
ODJmMDA4NDk3YjRjMGQwODE3M2MifQ%3D%3D&td=t.w***k.click&bemobdata=c%3D9265ab6c-
bff5-4bf2-85fc-7bc1dbb4daa9..l%3D22b8a4d3-9ef6-496e-bf40-a48c5e1fff2d..a%3D0..b%3D1#

Moreover, the link may contain:

1

the user's provider

2

OS version

3

a key consisting of two variables (to be described in detail later in the text)

3

a type of website to which the user is redirected (the name of the directory to which the user is redirected)

Track: most often, this is the domain of the initial smartlink, and it is the starting point for cloaking. Usually, it is a legal platform.

Then comes the base64-encoded key. It contains a timestamp and a hash. These parameters are used to identify each specific user and label them as unique.

Examples of links with a different hash:

1

https://l***v.click/it/s20i11/w***d/?
osv=Windows%2010.0&isp=G***S%20T***m&tid=1aa56077-f400-4910-92c6-
bb249266438d&key=eyJ0aW1lc3RhbXAiOiIxNjA4MTA2MDg3IiwiaGFzaCI6IjdiNGY3YmJkMzhkMzVkMDg4ODd
jYzdlMWY2Mzk5NWZjZGNlZmQxMzEifQ%3D%3D&td=t.w***k.click&bemobdata=c%3D23150be1-e444-
4aa1-b631-33e989cb3f2d..a%3D0..b%3D0#

key = {"timestamp":"1608106087","hash":"7b4f7bbd38d35d08887cc7e1f63995fcdcefd131"} - base64 encode
2

https://n****n[.]click/au/20/1/2/?
track=go.lltrsknoob.click&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDkwNTk2IiwiaGFzaCI6IjJhYjY5ZmU2ZDU0ZjE0MG
JmYzI3YjMyN2I1NzdlMTdhYWFlMjc1MDUifQ%3D%3D&bemobdata=c%3Dbecb4768-3b61-47b9-8dd8-
a6633197096b..l%3D2b5bb6f7-cd86-49e5-afb6-
013d10a5ea16..a%3D0..b%3D0..r%3Dhttps%253A%252F%252Fwww.google.com%252F#

The last element in the URL is the blob link, which is added to further analyze the effectiveness of the traffic attracted.

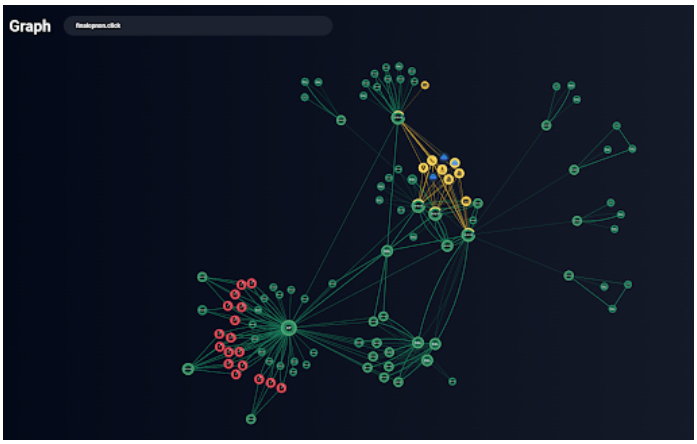
Targeted link infrastructure: domain networks

We found at least **60 different domain name networks** that generate targeted links. On average, each of them contains over **70 domain names**.

The largest detected network in terms of the number of domain names includes **232** domain names. It is possible that not all the sites are currently active. Such a large number of domains is created to make it possible to redirect the traffic to a related resource as soon as possible if an active one is blocked. This way, the fraudsters ensure continuous operation of their scamming scheme.

Very often, a large number of domain names on the network does not mean that this network is the most visited.

The next screen shows a network of resources that contains **51 domain names** with targeted links. This is one of the largest networks in terms of traffic found by Group-IB experts.

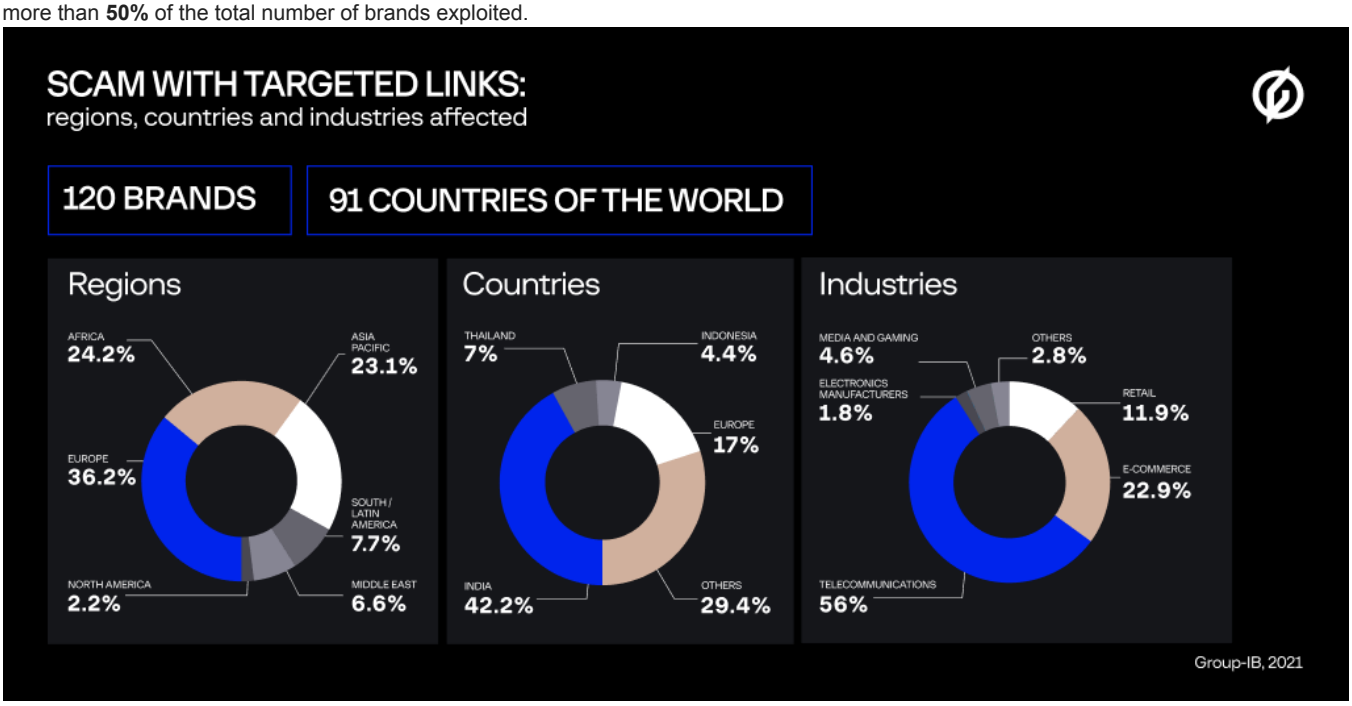


The average number of users following targeted links located on the finalopnon.click domain is about **4,640** people per day. We can conclude that scammers are actively attracting traffic here and making sure that the operation does not stop due when the site is blocked.

The domain names of this network are visited by **330,993** people per day (on average, 6,620 people visit each domain name). Almost **10 million people** can fall victim to the scamming scheme per month on the abovementioned network alone.
Scam's scale: geography and victims

Like many successful large-scale Internet scams, targeted fraud first appeared in Russia, but over time spread all over the world. Today, this type of fraud has been spotted in **more than 90 countries**, with cybercriminals exploiting **more than 120 brands** as bait.

Criminals mostly try to exploit the brands of leading telecommunications companies, which enjoy special "love" in this scheme, and make up more than **50%** of the total number of brands exploited.



The number of potential victims is huge, since on average, more than **5,000** people per day visit these websites. Group-IB experts estimate the damage at **$80 million** per month*. In addition, users lose personal data and risk infecting their devices with malware.

Analyzing the server infrastructure, which hosted these websites, we found out numerous targeted link templates sorted by country. Each template is stored in a special directory related to a country. One brand could be used many times, with the language being changed based on the country. Thus, we managed to evaluate the geographical scope of the Target Scam.

For each specific website with fraudulent content, traffic source information was collected and sorted by country. Based on this division, the main sources of traffic for such resources are India (42.2%), Thailand (7%), and Indonesia (4.4%), among others. Based on the pattern identified, the target regions for the scamming scheme are: Europe (36.3%), Africa (24.2%), and Asia (23.1%).

* The calculation formula was as follows: the number of sites * the site's minimum conversion * an average money loss on a phishing website.

Each country was taken into account only once.

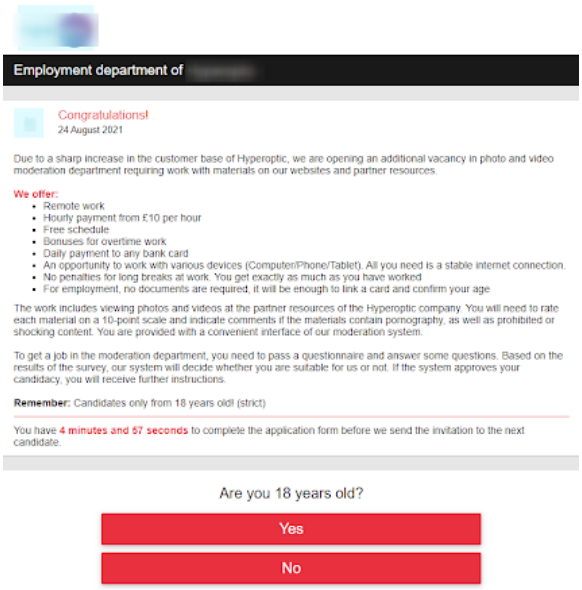
In general, the geography and number of brands used in this scamming scheme are incredibly broad. Among the companies, there are many well-known global brands; the list contains **at least half** of all the world's countries.

For each country there is at least one template and on average, at least three well-known brands are used.

Sometimes brands are used more than once, and of course, the language of the template also changes; overall, there are **more than 120** unique brands involved in the scheme.

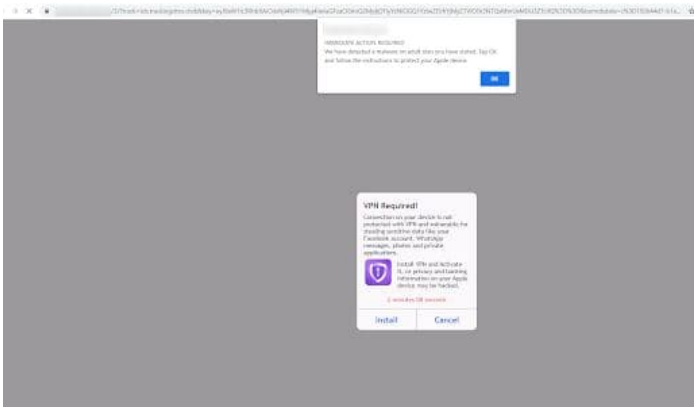
The most common fraud template is a promise to give away a MacBook, Sony PlayStation 5, iPad Pro or the latest smartphones from Apple and Samsung in return for the user's participation in a survey.

And even job offers:

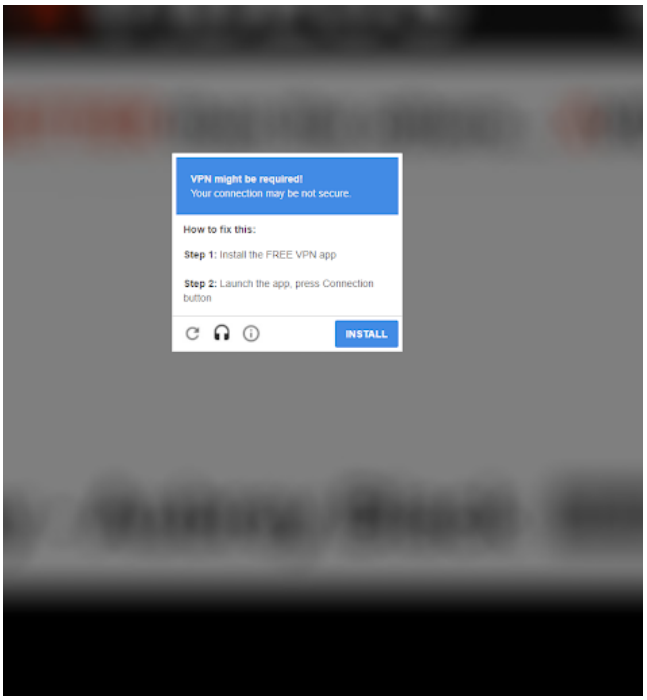


There's also a scam requesting that users download a fake VPN upgrade and offering an app as bait, and so on:

Eliminating a vulnerability:



And just a free VPN:



Risks

Targeted fraud carries risks not only for users, but also for the brands that the scammers abuse. Companies incur both reputational and financial losses; if a user loses money because of a brand, then they are likely to abandon it.

There are also many unpredictable risks. For example, accounts are stolen on the site on an enormous scale, and then money is laundered through these accounts.

If it comes to litigation, the company can receive a severe blow to its reputation, along with a fine from the regulatory authorities.

When buying or selling bad traffic, ad networks risk their reputation, customers, and money. Such behavior usually entails financial loss.
Recommendations for users

Do not send money to anyone for a "prize". Companies that organize these competitions do not use this practice.

Always pay attention to the domain name of the site.

Do not trust promotions with a quick countdown timer, as in most cases these promotions are fraudulent.

Only enter your bank card details on trusted sites.

Do not open links sent to you, even if they come from a good friend or a relative, as their account could be compromised.

Use a special virtual card for online shopping and set a limit for this card.

Recommendations for rights holders

Carefully process user messages and implement a system that will process all incidents related to the security of the company and its users.

Track messages from users outside the company. This will not only help your security service, but also your PR and marketing departments.

Conduct independent monitoring not only for phishing, but for all threat vectors, which may come from unexpected sources.

Hire DRP vendors whose experience and technologies make it possible to detect and block not only fraudulent sites, but the entire infrastructure of attackers. This method allows you to quickly eliminate violations on all Internet resources involved in the scheme, as well as to monitor the emergence of domain names that might host illegitimate content.