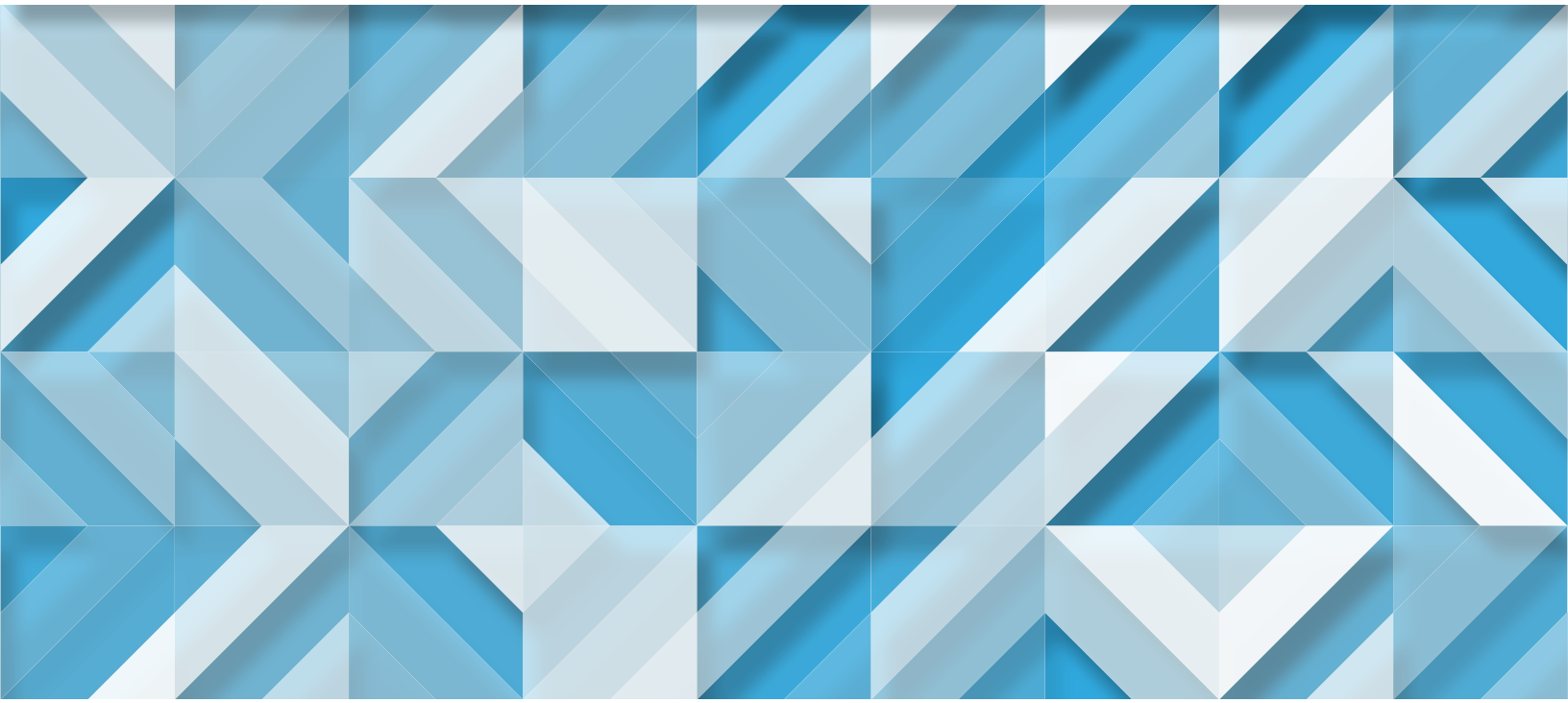
NoTrove:

The Threat Actor Ruling a Scam Empire



APRIL 2017

RISKIQ®

EXECUTIVE SUMMARY

When it comes to threats delivered through the digital advertising ecosystem, malware is usually what keeps folks up at night. However, while the infosec world laser-focuses on hunting and neutralizing exploit kits, a different type of threat is left to grow unimpeded, often to enormous sizes: scams. Scam campaigns grow quickly and silently in the shadows by acquiring cheap infrastructure. Over the years, these campaigns have become pervasive to the point of badly degrading the overall quality of the internet.

If you've ever seen a digital ad offering free electronics or "fabulous prizes" in return for taking a quick survey, you know what scams are. Essentially, scams are undesirable advertising, which fly under the radar because of the "gray" nature of their payload. In other words, while scams aren't classified as crimeware, they are intentionally misleading and disingenuous, and compromising the integrity of digital advertising.

By utilizing machine learning to enhance our ability to identify scams, RiskIQ detected 845% more scam incidents[1] in 2016 than 2015, a number we expect to increase again this year. With this new approach to scams, we're also able to closely examine their infrastructure to determine what makes them effective and lucrative to operate. What we find alarming about our research on a threat actors we've come to call "NoTrove" is the sheer scale of these scam networks' infrastructure and the traffic they command.

THE TARGET: *WEB TRAFFIC*

The main goal of scammers is often to accrue as much web traffic as possible. Essentially, web traffic is the result of a computer connecting with a web browser and an actual human connecting with digital content sitting on a hosting server. It's comprised of visitors to websites, with each single click and background request counting as a minuscule but significant drop in a vast pool of monitored, tracked, and often commoditized data points. Ecosystems and economies form to buy, sell, and trade this traffic; products and services are designed to aid in analyzing and classifying it. Traffic is redirected and shuffled around the web as part of partnerships and business contracts.

Traffic is critical to the giant exchanges in the online advertising space and to the very many niche affiliate network programs that exist, with organizations of all kinds tasked with monetizing and, ultimately, squeezing every last fraction of a penny of indirect marginal profit of each URL visited. To monetize their traffic collecting, scammers like the one outlined in this report may participate in shady traffic affiliate programs or sell traffic to traffic buyers (brokers).

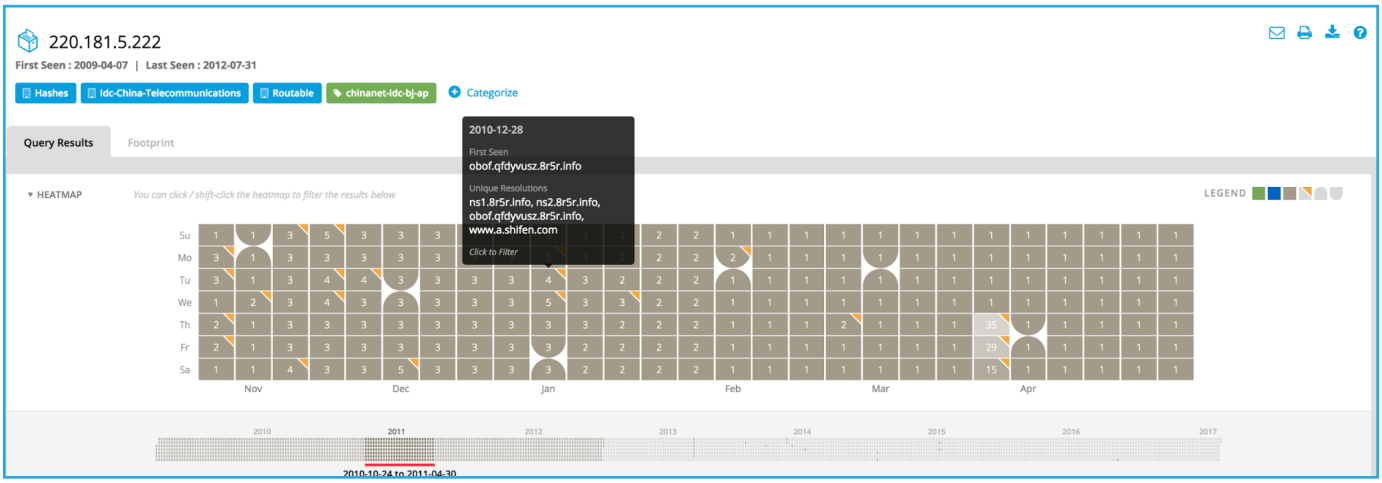
Traffic is an essential commodity for legitimate web companies and criminal underground economy alike. Everyone wants a piece of the traffic pie, and NoTrove is feasting.

[1] RiskIQ's 2016 Malvertising Report, RiskIQ Research, 1/30/2017

THE CULPRIT: *WHO (WHAT) IS NOTROVE?*

One of these scam networks, by the prolific actor "NoTrove," is particularly successful in capturing traffic. NoTrove's peculiar name comes from a common theme observed in the URI pattern. This actor's URLs almost always come with the parameters /tov= or /rov=, and are most commonly associated with fake rewards scams. Therefore, the name came together as No (Treasure) (T/R)ove,or NoTrove for short.

We first observed NoTrove a year ago when we began expanding our focus on scams, but Passive DNS (PDNS) results inside PassiveTotal indicate this group has been operating as far back as December of 2010:



(Fig 1. Earliest observed instance of NoTrove) https://passivetotal.org/search/220.181.5.222

In Fig-1 above you'll see an older version of a NoTrove host, but today, NoTrove builds its infrastructure in a very particular way:

- A typical NoTrove fully qualified domain name (FQDN) will use a high-entropy (i.e., highly random) host, shown in blue. High-entropy hosts indicate that they are created by automation, which threat actors will employ to quickly build infrastructure with which to launch attacks.
- Following these high-entropy hosts are campaign-specific middle hosts (shown medium blue) we think are used to label the type of scam (e.g., survey, promo, prize, etc.). With so much infrastructure constantly in rotation, this is how NoTrove keeps it all organized. So far, we've observed 78 variants representing NoTrove's different payloads.
- Following the "label" hosts are a high-entropy or randomly worded domains (shown in light blue), again indicating they were created by automation.

Here are some more examples of typical contemporary NoTrove FQDNs:

bogzz.bestprizeland.8702.ws
uchzz.pcloadletter.footbaths.xyz
rjkzz.super-promo.7891223.com
tcfzz.stream.7891223.com

THE MODUS OPERANDI: *WITH SCAMS, SIZE MATTERS*

With high-entropy domains and constantly shifting hosting, we've seen NoTrove burn through just under 2,000 domains and over 3,000 IPs. Combined with the 78 variations of campaign-specific middle-word variants and randomized hostnames, we've seen NoTrove operate across millions of FQDNs. Typically, one IP used by NoTrove will house a set of domains, but each campaign-specific *.domain.tld campaign variant will be hosted on its own IP, usually a Choopa or Linode droplet. These IPs and domains can be found in this PassiveTotal public project here:

https://passivetotal.org/projects/7ee582dc-c792-e635-ce78-0396e1e00bf4

But, to see just how prevalent this actor is, we can look at the Alexa rankings of its domains. Usually, each domain will only be active for a couple of weeks, but during that period it is not uncommon for the domain to shoot up into the Alexa top ten thousand based purely on scam ad deliveries. In fact, the highest rank we've seen historically for a NoTrove domain was 517, making it one of the most visited pages on the entire internet for that day.

THE MUG SHOT: *WHAT VICTIMS SEE*

So what does NoTrove look like? Well, with the 78 variants of tracked middle-phrase campaigns, there are many different payloads. However, the most common versions seen are scam survey rewards, fake software downloads, and redirections to potentially unwanted programs (PUPs).

Seen Here:

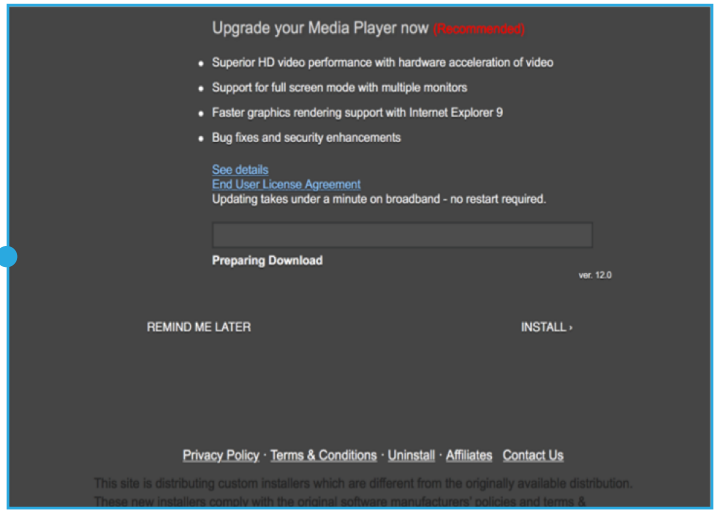


Fig 2. Fake Media Player

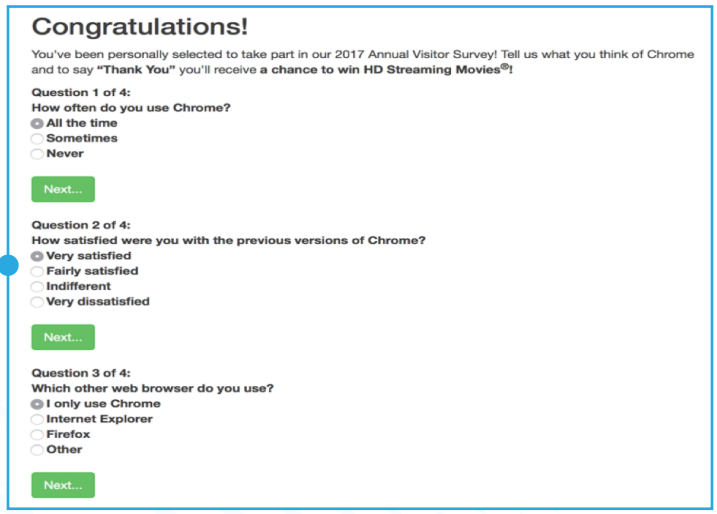


Fig 3. Fake Rewards

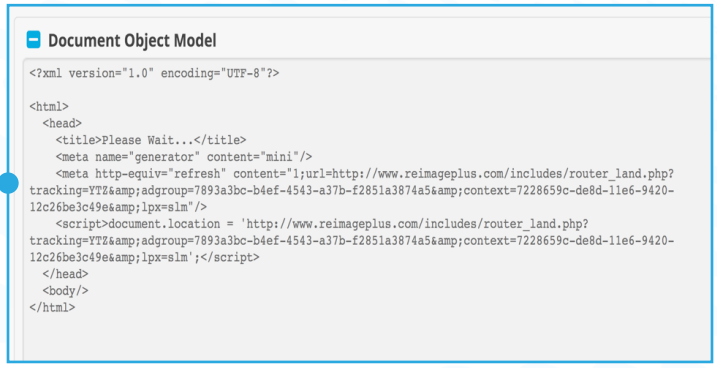


Fig 4. Redirection to PUP

THE DELIVERY: *HOW THE TRAFFIC COMES AND GOES*

Below, we'll journey through a sequence overview from a RiskIQ crawl that ended up on a commonly advertised PUP from NoTrove to examine how NoTrove sends users to one of its scam pages.

Sequence Overview

Sequence	URL	Cause	Response Code	Frame	Window	Parent Window	Lost Referrer	Referrer
1	http://a.diretrak.com/c/a1b4cfa80d8ca9d3?siteid=%5Bzone%5D&a...	topLevelRedirect	302	-	-	: TopLevelWindow@3e5dd993	-	
2	http://ugzk9.6136878.com/?s1=158bd986fea17b253093547	redirect	302	-	-	: TopLevelWindow@3e5dd993	-	
3	http://5rbzz.ddldownload-now.cenb.gdn/?sov=3870563&hid=c...	redirect	200	true	true	: TopLevelWindow@3e5dd993	-	
4	http://5rbzz.ddldownload-now.cenb.gdn/MOB413downloadaudiorot...	location.refresh	200	true	true	: TopLevelWindow@3e5dd993	true	http://5rbzz.ddldownload-now.c...
5	http://play.leadzupc.com/?m=0AEHUSROTATIVE&a=M129K13JFPS...	location.refresh	302	-	-	: TopLevelWindow@3e5dd993	true	http://5rbzz.ddldownload-now.c...
6	http://adperience.afftrack.com/click?aid=6&linkid=T464&a...	redirect	302	-	-	: TopLevelWindow@3e5dd993	-	
7	http://ts46j.2yq.xyz/?s1=89be5438a202ff347ac8df99c8371fca&am...	redirect	302	-	-	: TopLevelWindow@3e5dd993	-	
8	http://tz4zz.detect.cenb.gdn/?sov=358894285&hid=btdrrdfb...	redirect	200	true	true	: TopLevelWindow@3e5dd993	-	
9	http://tz4zz.detect.cenb.gdn/REI495slmAE.html	location.refresh	200	true	true	: TopLevelWindow@3e5dd993	true	http://tz4zz.detect.cenb.gdn/?...
10	http://www.reimageplus.com/includes/router_land.php?tracking...	location.refresh	301	-	-	: TopLevelWindow@3e5dd993	true	http://tz4zz.detect.cenb.gdn/R...
11	http://www.reimageplus.com/land/sqh/index.php?tracking=YTZ&a...	redirect	200	true	true	: TopLevelWindow@3e5dd993	-	

We begin our trek with a request for an ad from a(.)diretrak(.)com, where we are immediately shunted off to a rotator (dedicated infrastructure for redirecting the user based off of various parameters) that then kicks us over to the first stage of a NoTrove delivery. You can see here that NoTrove typically comes in two stages:

1. An internal redirection based on the type of campaign
2. The scam payload, a redirection to a PUP, or, if there is nothing to serve for that requested campaign, it will fallback to delivering another ad through a second network

3	http://5rbzz.ddldownload-now.cenb.gdn/?sov=3870563&hid=c...	redirect	200	true	true	: TopLevelWindow@3e5dd993	-	
4	http://5rbzz.ddldownload-now.cenb.gdn/MOB413downloadaudiorot...	location.refresh	200	true	true	: TopLevelWindow@3e5dd993	true	http://5rbzz.ddldownload-now.c...

In this example, there was nothing to deliver for the given parameters on that particular campaign, so NoTrove used the fallback of delivering an ad pulled through play(.)leadzupc(.)com, which is the Mobusi mobile-based ad network.

Page http://5rbzz.ddldownload-now.cenb.gdn/MOB413downloadaudiorotatorwebALL.html

Status | Messages (0) | Dependent Requests (0) | Cookies (10) | Links (0) | Headers | Response & DOM | DOM Changes | Causes | Sequence To Parent

Document Object Model

```
<?xml version="1.0" encoding="UTF-8"?>

<html>
  <head>
    <title>Please Wait...</title>
    <meta name="generator" content="mini"/>
    <meta http-equiv="refresh" content="1;url=http://play.leadzupc.com/?m=0AEHUSROTATIVE&amp;a=M129K13JFPSIITT2&amp;pubid=3870563&amp;PC=1"/>
    <script>document.location = 'http://play.leadzupc.com/?m=0AEHUSROTATIVE&amp;a=M129K13JFPSIITT2&amp;pubid=3870563&amp;PC=1';</script>
  </head>
  <body/>
</html>
```

From Mobusi, the sequence passes through Afftrack for affiliate traffic tracking, and then off to the same rotator we saw before. Once again, that rotator spits us back out to NoTrove. This time, however, we're hitting a different campaign.

8	http://tz4zz.detect.cenb.gdn/?sov=358894285&hid=btdrrdfb...	redirect	200	true	true	: TopLevelWindow@3e5dd993	-		
9	http://tz4zz.detect.cenb.gdn/REI495slmAE.html	location.refresh	200	true	true	: TopLevelWindow@3e5dd993	true	http://tz4zz.detect.cenb.gdn/?...	

With this campaign, we were given an actual result when we hit the second stage of NoTrove. We received a redirection out to ReimagePlus, a PUP commonly associated with low-quality affiliates, aggressive, misleading advertising, and software bundlers.

THE CONSEQUENCES:
WHY IT MATTERS

NoTrove is far from the only actor operating enormous swaths of scam infrastructure, which pollutes digital advertising networks and degrades the overall effectiveness of the digital ad ecosystem. Redirecting users through layers and layers of what amounts to digital junk may be incredibly lucrative for NoTrove operators, but adversely affects those reliant on the credibility of the digital advertising ecosystem.

More and more users are becoming attuned to the undesirability and potential dangers of scams and are turning to ad blocking as a solution. Unfortunately, ad blockers block all ads, so publishers don't get paid. Ad blockers eat away at digital advertising revenue and sharply curtail the growth of the industry. In 2016, 69.8 million Americans were expected to use an ad blocker, an increase of 34.4% over last year[2]. In 2017, that figure is projected to grow by another 24%, or 86.6 million people. This practice, according to Juniper Research, will cost the digital media industry over $27 billion by 2020.[3]

The problem for those in charge of the security of ad networks is that constantly shifting infrastructure means simply blocking domains and IPs isn't enough. NoTrove is spread so far and wide that blocking one piece of its infrastructure is akin to playing whack-a-mole—no matter how many you hit, another will pop up. Also, the scale at which NoTrove and groups like it operate means identifying scams in time to block their impact is no longer possible for humans alone.

THE RESPONSE:
MACHINE-LEARNING AUTOMATION

If left unchecked, NoTrove and threat actors like it will continue to balloon to even greater size, encompassing more domains, IPs, and other infrastructure. Until we can commit to stopping those accruing scam empires across the web, these threat actors will cause more problems for the digital advertising space and the internet as a whole.

Fortunately, you should now have enough information to identify a NoTrove scam. Unfortunately, mere humans lack the computing power to identify NoTrove's rotating infrastructure quickly enough to do much about it.

However, with machine learning, human security professionals can enjoy accurate, automated detection and confirmation of NoTrove scams. Just like this report taught you how to know a piece of NoTrove infrastructure when you see it, machine learning can detect what the NoTrove page looks like down to the document object model (DOM) and learn what makes a NoTrove page a NoTrove page. Eventually, it will even understand small variances in the payload without the need for any human intervention, so it can continue to detect NoTrove, even as this threat actor evolves.

[2] US Ad Blocking to Jump by Double Digits This Year, eMarketer, 6/30/2016

[3] Worldwide Digital Advertising: 2016-2020, Juniper Research, 11/5/2016 by Sam Barker