

Investigate proxyware attack vectors and its potential problems

Rasmus Karlsson, Ellen Brunnström
{*raska119, ellro412*}@student.liu.se

Supervisor: Niklas Carlsson
niklas.carlsson@liu.se

Project Report for Information Security Course
Linköpings universitet, Sweden

May 11, 2022

Abstract

As new trends are introduced on the internet, so are the new threats. Proxyware is a software that lends your unused bandwidth to other users who may use it to access content using your IP address. The problem with this is that what someone else does while using your IP address might be brought back to you if they for example do something illegal online. Another problem is that web sites might start to see you as a proxy or just another mindless bot as a consequence of using proxyware. Proxywares have increased in popularity over the last couple of years and an increasing amount of people have begun using it, seeing a way to earn extra money without doing much. With this incentive to use proxywares, most people might not think twice about what is actually going on when lending your IP address to someone else. The risk of something bad happening to you is low, but since there is not actually much money to be made, the risk might not be worth it. In this report we investigate how easy it is for an unknowing user to be tricked into downloading a corrupt version of a proxyware. We also investigate the proxyware Honeygain by looking at the traffic going through our network as we use the software. We reach the conclusion that if you want to use proxyware you have to make sure you download it from an official web page since there are fake web pages around. If you go ahead and use an official proxyware, you will most

likely be safe from harm, but it is still not completely risk free.

1 Introduction

A proxyware is a software client that enables you to lend your bandwidth to others in return for money. The business model is based on a person acting as an internet proxy by providing your unused bandwidth to other individuals and organisations. Since you get compensated for allowing others to use your bandwidth, this business model allows you to earn a passive income. This is the lucrative aspect of proxywares, the honey if you will. *Honeygain* [1], one of the bigger organisations organising this, began in 2018 and has been growing ever since.

But with success comes also those trying to ride the same wave for their own benefit. According to Cisco [2], there has been a growing number of malicious actors that try to benefit from this as well with several different methods of exploiting the rising hype around proxyware.

One approach [2] is to trick a user into downloading a correct copy of a well known proxyware, for example Honeygain, but with a twist - hiding other installations from the user in the same package, letting them unknowingly also generate a passive income for the attacker. This can be done by installing a crypto mining program that silently installs and remains hidden

on the computer while continuously running, unbeknownst to the user. Another approach is to infect the victim's computer with a hidden copy of a proxyware - effectively using their bandwidth without the host knowing of it and generating a passive income for the attacker. In most scenarios when the attacker installs a program on the victim's computer, they disable the notifications for that program and moves it to an obscure location in the computer [2]. This makes it difficult to notice, if at all, that it is running or even exists. To look closer into how likely you are to reach a suspicious web page, which might be hosting malware, this paper will investigate the search results of common proxyware terms on different search engines (Google, Bing and Yahoo).

Another potentially dangerous aspect of proxyware comes not from malicious actors trying to install programs on your computer, but who wants to use your IP address [2]. As mentioned previously, when you lend your bandwidth using a proxyware, you share your IP address with the service which lets others use you as a proxy. This means that for every activity the borrower of your IP address generates, it will look like you did it. This is investigated in this paper by looking at the communication going through a device which has proxyware installed.

Previous research have been made looking into Residential IP proxies [3] [4], which is what your IP address becomes when joining with a proxyware. They have also looked into how to detect that a proxy is running on your device. More of this can be read in Section 6.

The rest of the paper is structured by first displaying the background needed for understanding the rest of the paper. It starts with the method explaining how the search engine study was to be conducted and then the analysing of Honeygain (a proxyware). The results of utilising these methods are then presented. We then analyse the results from the search engine results and the network data gained from Honeygain before we conclude the paper.

2 Background

Proxyware - Proxyware is a software that shares your network connection with an central organisation in exchange for other benefits, e.g. money. The organisation may then use the provided network connection to pose as a user at your location in order for other organisations to benefit and use it for research and testing of products, among others. Another common use for proxies is content delivery; making content available in a place where it usually is not.

Honeygain - Honeygain is one of several different providers of these kinds of proxyware services, started 2018 [1] and claims to be familiar with the industry and that they have created a safe and sound environment and an easy way of earning money.

Attack vector - An attack vector is the path that leads to a vulnerability in a system. This includes a certain number of steps an attacker has to use to reach vulnerable code, which might includes typing malicious code in the comments section of a web page, and then gaining access to the host's terminal. There might be several different paths to a given vulnerability and if you block one of them, the others still exist. You have to fix the underlying cause of the vulnerability to truly block all attack vectors.

Proxy Server - A proxy server is a server that acts as a middle man between you and the internet. It can be used to bypass IP restrictions, obfuscate yourself, and increase anonymity while surfing on the internet.

Residential IP - An IP address given to a user by an internet service provider (ISP) and is associated with a single user and location. Short: RESIP. See Section 2.1 for its usage here.

Virtual Machine - A virtual machine is a piece of software that emulates a computer. Its memory and storage is separated from the host machine's, which means that programs inside the virtual machine cannot reach the data outside of it, making a safe environment for testing new or untrustworthy software.

2.1 Residential IP

According to Tosun et al. [3] proxy providers who began using residential IP as data-centers are too easy to detect and block. Residential IP addresses (RE-

SIP) are instead tied to a person, controlled by an ISP and can be used for many purposes. Including deluding advertising traffic or history, or for making an identity theft look more valid. But, it can also be used to confirm that, for example, an advertising campaign works as it should [5], or the more gray area of accessing content locked to a specific area.

3 Method

This section will describe the methods used to learn more about proxyware and the situations described in the introduction.

3.1 Theoretical methods

There are articles and blogs that cover materials related to proxyware which will be the basis of the literature study, and one experiment will be conducted using different search engines.

3.1.1 Literature Study

Initially, to begin the work in understanding proxyware, a literature study will be conducted. The topic of proxyware is quite new and to our knowledge not many peer-reviewed articles have been published on this matter. Therefore, much of the information regarding proxyware will come from official proxyware sources, blogs, and forums. One example of this is the Honeygain subreddit¹. The majority of the related reading will be conducted on aspects that relate to proxyware, for example residential IP.

3.1.2 Analysing search results

It is also interesting to look closer on what the search results are when a user wants to download software for proxyware. We want to analyse the web pages that pop up when searching for key terms related to proxyware. We will use the search terms *proxyware*, *Honeygain*, and *Peer2Profit* when analysing web pages related to *proxyware*. We will also be using the different search engines *Google*, *Bing*, and *Yahoo*.

¹<https://www.reddit.com/r/Honeygain/>

From this we expect to find a some sort of metric by looking at how much of the results were malicious, and how *easy* it is to get infected by a malware when trying to install a proxyware.

We define safe web pages which include the following traits

- Official page for related software
- Well known and moderated forum
- Articles
- Blogs

And we define web pages with the following traits unsafe

- Domain name similar to official web page, offering the same software
- Same domain name but with another top-level domain
- Third party web pages offering the same software

A user is able to post links to unsafe web pages on forums, such as Reddit, but we believe that those relatively large subreddits are moderated enough to remove malicious content when posted. A domain with similar name but different top-level domain can be, for example, *honeygain.org* which is a different web page than *honeygain.com*, the official web page for Honeygain.

3.2 Analysing Honeygain

One interesting aspect of selling your bandwidth is to look at what other users actually use it for. Therefore, the approach here is that we download and look at the traffic that is going through our bandwidth as we use Honeygain. One of the most important aspects of this method is to protect your computer, which is why we will install Honeygain on a virtual machine using VirtualBox with the operative system being Linux Ubuntu (64 bit). VirtualBox has its own network engine which uses NAT to hide the host machine's IP address from the guest software, making

sure our own IP address will not be the one used by Honeygain.

When other people use our bandwidth via Honeygain, their traffic will go through our machine and we can monitor it in two ways, among others. We can install a filter, like a user in reddit did to monitor their internet traffic², and we can use *Wireshark* to monitor our internet traffic.

From this monitoring, we will try to find patterns of Honeygain use, for example if it is possible to look closer at the data, just like A.Tosun et al. [3] did, and provide some answers and look at similarities to the RESIP papers [3][4]. As being the proxy may differ from relaying data through a proxy, we will have a different perspective from the papers mentioned above, which can give further understanding on the matter.

4 Result

In this section, we provide the results gained from our research. We also provide some further insight to one of the found suspicious domains.

4.1 Literature study

According to E. Root [6], potential issues that might occur when using proxyware includes the risk of downloading fake or malicious copies of proxyware. There is also the risk that the IP address one chooses to utilize for the proxyware get blocked, or at least flagged by others for being spam, or for participating in attacks. This might be bad for one user, and worse for a company relying on their IP addresses being accessible [6]. Others using your IP address might also give you other problems than a contaminated IP address. E. Brumaghin points out that an IP address doing bad things while connected to you can lead to legal involvement [2].

Another potential misuse of your IP address is for geographical spoofing in order to display a relevant location when buying something online with stolen

²https://www.reddit.com/r/Honeygain/comments/kadza9/just_looked_at_my_adguard_home_logs_interesting/

identity and credentials [3], or trying to access an geoblocked content on a streaming service.

One common problem [7] that might occur when using Honeygain or other proxywares is that you might encounter more CAPTCHAs³, Cloudflare checks, and other measures against bots. This is due to the proxyware service might favour your IP address over others in certain cases, and therefore your IP address will generate a lot of traffic to a certain website. This might look like suspicious activity, or like a bot, from the other end, and they will therefore deploy some anti-bot measures against you, even though you did not personally visit their site.

For example, one user [8] reported to having their IP address blacklisted for being a VPN after using Honeygain. This is most likely due to the problems stated previously. Likewise, another user [9] also reports being blacklisted for being VPN, and need to do CAPTCHA and are receiving messages about "unusual activities" when accessing Google. Yet another user [10] reports that their ISP have started noticing and reacting to malicious traffic. On the other hand, Honeygain claims that they monitor every client's activity all the time to prevent any damage to the user's network or system [11]. In tandem with this, they also claim they prohibit buyers from using your data for illegal or malicious means.

4.2 Search results

Provided in Table 1 are the results from different search engines and search terms showing the amount of suspicious results out of 100 viewed results given from the criteria presented in Section 3.

	Proxyware	Honeygain	Peer2profit
Google	2%	5%	10%
Yahoo	2%	8%	10%
Bing	-	8%	14%

Table 1: Table displaying the percentage of suspicious search results. The uppermost row represents the search terms, while the left most column represents the search engines used.

³Acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart"

The results from the search term "Proxyware" consisted mostly of articles and blogs discussing the dangers of proxyware. A quick glance at the same search term on Bing gave the same result, so we did not do any further study on Bing regarding proxyware. In the next step, when we searched for actual proxywares, Honeygain and Peer2profit, the results were much more interesting. This time not only blogs and articles showed up, but more download links as well. Most of them were official domains, but some were not and claimed to provide either the official Honeygain/Peer2profit client or some addition to it. Those were flagged suspicious, as you do not know what they have included in that package. When comparing the other two search terms on Google and Bing, the latter yielded more suspicious web pages.

While looking at the search results on Google for "Honeygain" a notice appeared about search results being removed because of DMCA infringements.

4.2.1 Further investigation of a suspicious domain

One interesting result was found by looking closer at one of the results which was flagged as a DMCA infringement [12]. This result was not found as a result on Google but found in other search engines. At first glance there are a lot of similarities to the "real" page from 2020⁴ [13], see Figure 1, compared to the "fake" page, see Figure 2. Besides the differences in the buttons for different installers, and the missing Honeygain logo to the upper left on the real Honeygain, there is not much that differ. Some of these differences may also stem from the real page having updated their design since the imposter page was created. Looking further into the web page, the HTML meta-data also looks realistic for this page.

If you instead look at the outgoing links from the imposter, Figure 3, you get some clues; Yllix (an online advertising network) and a GitHub link pointing to a private user messi06. Is that something the real Honeygain would have? Another clue is to look at the URL; it is actually the subdomain that is called "honeygain", and the domain name (Second Level

⁴From 14 March 2020, using Wayback Machine

Domain) is "neocities.org".

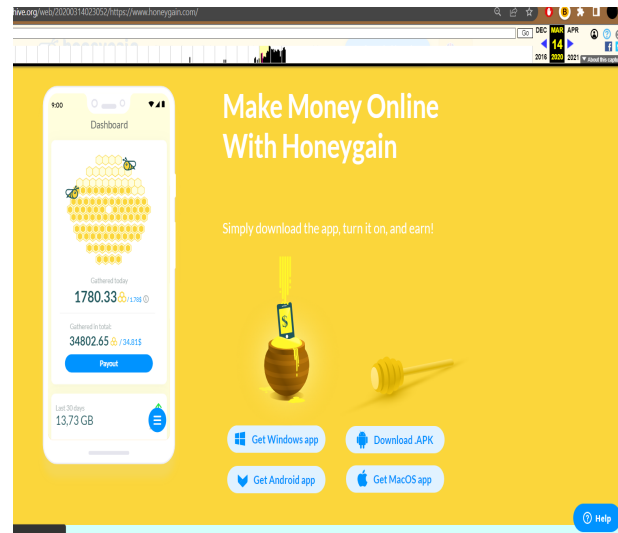


Figure 1: Image of real Honeygain home page 2020 via Wayback Machine

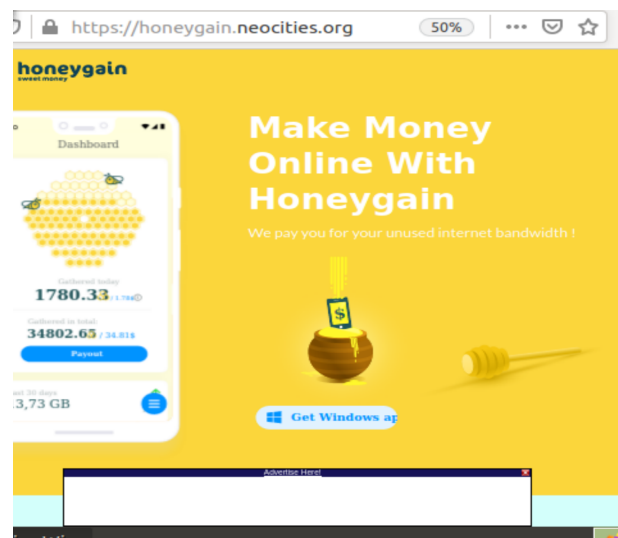



Figure 2: Home page of probable fraudulent copy of Honeygain

Outgoing Links 

- https://download.honeygain.com/android-app/honeygain_app.apk
- <https://www.facebook.com/honeygainapp/>
- https://www.instagram.com/honeygain_app/
- <https://yflilx.com/publishers/495451>
- https://twitter.com/Honeygain_App
- <https://honeygain.en.aptoide.com/>
- https://galaxystore.samsung.com/detail/com.honeygain.make.money?session_id=W_7ec69f8aaa862c7c95537878f72b2a3
- <https://github.com/messi06/honeygain/raw/master/HgSetup.zip>
- <https://appgallery.cloud.huawei.com/marketshare/app/C101337001>
- <https://apps.apple.com/us/app/honeygain-make-money-online/id1479049768>

Figure 3: Outgoing links from above mentioned page, collected from Virustotal.com

4.3 Using Honeygain

As mentioned in Section 3, we set up a virtual machine using *VirtualBox* and installed Honeygain on it. Here we encountered problems. Given that we did not want to use our own IP address, in the case of it becoming compromised, we had decided to use a Virtual Private Network (VPN) over our regular connection. As Honeygain are interested in your correct ISP-provided address, rather than a data center IP address [14], this was not appreciated. Honeygain are using services like ip2location⁵ in order to investigate the source of the IP address.

To circumvent this, we used the network Eduroam, which gave us the IP address 130.236.1.9. After starting Honeygain, we used *Wireshark*⁶ to monitor the traffic to and from our computer and we noticed almost immediate activity. One activity we noticed was the Honeygain API call which occurred quite frequently, probably to reestablish an existing connection or to establish a new one. If we filter the results to our IP address, we see that every type of protocol that relates to our IP address is DNS. Every DNS call was either to Honeygain’s API or to Cloudflare.

The most frequent IP address which used our connection was 172.17.0.2, which in turn connected to a whole bunch of different IP addresses. The other end of the connection was either us, when 172.17.0.2 communicated with us, or another IP address, which indicates that we are used as a middle hand - the

⁵<https://www.ip2location.com/>

⁶<https://www.wireshark.org>

proxy in the communication.

Most IP address used the standard ports used for internet connection DNS(53 and 5353), HTTP(80) and HTTPs(443), but the 172.17.0.2 address opened a lot of different ports both for TCP and UDP communication. They were in the range 33404-59954 for TCP, and in the range 33051-60698 for UDP connection. These ports fall under both the User ports and the Dynamic ports [15].

Most of the network traffic was encrypted and unreadable to us, but some was sent over http, for example see Figure 4, and we could see at least which domains the foreign connections wanted to visit. We encountered the following domains:

- www.msftconnecttest.com
- api.geoedge.com
- ocsip.digicert.com
- ocsip.pki.goog
- tkdeu.welldnn.com
- clk.tradedoubler.com
- redir.tradedoubler.com

```

172.17.0.2 13.107.4.53 HTTP 150 GET /connecttest.txt HTTP/1.1
172.17.0.2 172.17.0.2 HTTP 572 HTTP/1.1 200 OK (text/plain)
172.17.0.2 13.107.4.53 HTTP 150 GET /connecttest.txt HTTP/1.1
172.17.0.2 172.17.0.2 HTTP 572 HTTP/1.1 200 OK (text/plain)
172.17.0.2 52.28.24.72 HTTP/2. 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
52.28.24.72 172.17.0.2 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 52.28.24.72 HTTP 609 HTTP/1.1 200 OK (text/html)
52.28.24.72 172.17.0.2 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
172.17.0.2 52.28.24.72 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
172.17.0.2 52.28.24.72 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
172.17.0.2 52.28.24.72 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
172.17.0.2 35.186.231.97 HTTP 407 GET /clickId=249284a3004031&df= HTTP/1.1
35.186.231.97 172.17.0.2 HTTP 520 HTTP/1.1 302 Moved Temporarily (text/html)
172.17.0.2 52.51.92.242 HTTP 507 GET /projetcr?rid_query_id=200" HTTP/1.1
172.17.0.2 172.17.0.2 HTTP 200 HTTP/1.1 200 Found (text/html)
172.17.0.2 52.28.24.72 HTTP/2. 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
52.28.24.72 172.17.0.2 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
52.28.24.72 172.17.0.2 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 59 HTTP/1.1 200 , JavaScript Object Notation (application/json)
52.28.24.72 172.17.0.2 HTTP 217 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 604 HTTP/1.1 200 OK (text/html)
172.17.0.2 52.28.24.72 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
52.28.24.72 172.17.0.2 HTTP 172 GET /ip HTTP/1.1
52.28.24.72 172.17.0.2 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
172.17.0.2 52.28.24.72 HTTP 172 GET /ip HTTP/1.1
172.17.0.2 52.28.24.72 HTTP 301 HTTP/1.1 200 , JavaScript Object Notation (application/json)
93.184.220.29 172.17.0.2 OCSP 444 Request
93.184.220.29 172.17.0.2 OCSP 452 Response
172.17.0.2 142.250.74.35 OCSP 446 Request

```

Figure 4: Picture of the HTTP activity collected by *Wireshark*

After running Honeygain for about 30 minutes, we could see how much of our network we had shared through Honeygain, Figure 5. The amount of data that we shared through our network was not a lot and as the dashboard indicates, it did not amount to a single dollar earned.

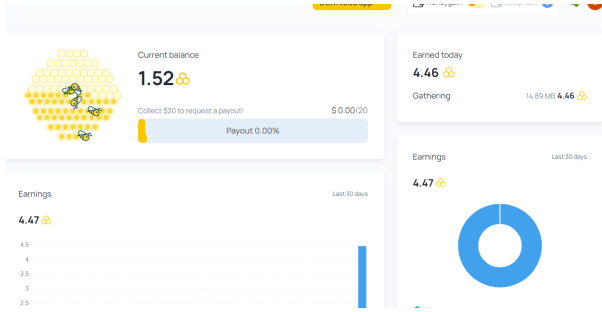


Figure 5: Picture of the dashboard after 30 minutes of running Honeygain

5 Analysis

Here we discuss the results previously obtained. We analyse why the results might be the way they are, and discuss some interesting findings from our investigation.

5.1 Search results

As seen in Table 1, searches on Honeygain generated less potentially malicious results than Peer2Profit, and Google displayed less potentially malicious results than the other search engines used. This might stem from that organisations, on behalf of Honeygain, petitioned to remove imposter links from Google regarding the DMCA (Digital Millennium Copyright Act) [16].

The fact that Yahoo and Bing displayed more malicious result probably is because they, unlike Google, have not been told to exclude those. Or at least not to the best of our knowledge. For example, the page mentioned in one of the DMCA claims [12] were found in the search results here. We investigated this further in Section 4.2.1.

Proxyware is a more official term used by entities such as Talos intelligence [2] - a user interested in using a proxyware would probably search on a provider rather than that term itself, and that may be the reason that that search term did not generate more suspicious result. But, as our search was conducted without properly examining the website

of every result there might be search results of a malicious nature that was unintentionally flagged as proper and vice versa. Third party installers that offers a valid and safe version of Honeygain/Peer2Profit might have might have been flagged as suspicious. Also, the numbers will probably change over time, as pages get taken down or new malicious results are spawned.

To increase this research we can continue looking at other search queries, for example adding a "download honeygain/proxyware/peer2profit" search. As E. Root [6] mentions, those may yield more potentially malicious results, and is also a reasonable search query for a user wanting to download a proxyware.

5.2 Running Honeygain

Honeygain obviously is aware of the fact that VPN:s exists, and does not want those in their network. One reason that Honeygain does not allow users to use the service while connected to a VPN might be that it hinders their collection of residential IP addresses. They want these kinds of private IP addresses in order to be more "free" on the internet, and to be able to act as normal users. Instead, using a VPN makes it look like your data is coming from a data center, which in many cases is unwanted, and you are prohibited from receiving the same services as using a residential IP would.

They also potentially get a more diverse group of IP addresses, coming from different locations, if they do not allow VPN. But why would they want a diverse group of IP addresses? Maybe because a group of IP addresses is harder to block in bulk if they for example are used in a botnet rather than if a proportion of them came from different VPN services. Web pages may also be more unwilling to block a residential IP address as they are presumed to be innocent users. Another reasonable explanation is just that they need different locations to be able to verify for example ads, or test that location-specific content work.

Honeygain claims that their system is secure to use due to them monitoring the traffic all the time. They have a lot of people using their software, so to moni-

tor all the traffic they must have automatic systems implemented to scan the traffic. It is difficult, but not impossible, to bypass automatic scans. In a scenario like this one where there are an endless amount of possible outcomes in the traffic, there might be a slight possibility a malevolent user will get away with using a residential IP for illegal activities.

5.3 Using Honeygain

The IP address that occurs in the communication with Honeygain, 172.17.0.2, is interesting to note. 172.16.0.0 to 172.31.255.255 is an allocated private IP address range [17], which means that we are now talking to/within a private network, which further acknowledges that we are a part of the internal Honeygain network.

Among the visible HTTP results presented in Section 4.3 are services made for checking/evaluating our connection, as well as some commercial domain names. Among these, for example *Tradedoubler* is an advertising company [18], which can correlate with the "Ad Verification" Honeygain claims [5] they are using the residential proxy for.

The Cisco Talos article [2] reported a potential problem with people using proxyware. The problem was that from the outside it looks as if the user itself is generating all the observed activity, which might be potentially illegal, and that it was hard to discern whether it was the user or someone behind the curtains abusing the proxyware service who was actually doing it. From the data we got using Honeygain, we noticed that we could see which IP address sent data, and where it was going, by observing the packets captured by Wireshark. This may give an indication that, if you're inside the system, you may be able to see more of where the actual attacker is coming from.

5.3.1 Honeygain business model

According to Honeygain [19], if you share data using the standard model, the payout rate is 3\$ for every 10 GB shared through your network. When we ran Honeygain for about 30 minutes, we amounted to about 15 MB of data shared, which is roughly 0.015% of

the needed amount of 10 GB. If we continued with the rate of 15 MB every 30 minutes, we would reach our payout goal of 3\$ in 330 hours, which is a very bad hourly rate. But, we have to consider the fact that this is a passive income with you doing nothing but sharing unused bandwidth. That said, you don't earn a lot by using Honeygain's standard model. Is it worth it?

6 Related Work

Since this study is quite new, and a lot of work has not been done in this area before, there may not be much to compare to. If any studies of similar work is found, it will be discussed here.

6.1 Residential IP

Several previous articles have investigated residential IP proxy where users, either knowingly or unknowingly, share their bandwidth to be used as node in the proxy network. Mi et al. [4] investigates several RESIP services by subscribing to them, and then communicating with their own servers in order to collect the IP addresses used by the proxies, gathering over 6 million IPs. Out of those, they find that 2.20% was either blacklisted or in other way reported, with 11.57% becoming blacklisted first after they were added to the collection. Some was also indicated to be used for fast fluxing.

Tosun et al. [3] proposes a RESIP host detection algorithm to identify malicious proxy flows, this is conducted by investigating 1) the network traffic flow 2) the amount of data sent 3) looking for an expected DNS check. Mi et al. [4] also gives some insight into the infrastructure of RESIP services, for example the opening of (unusual) ports to operate as gateways for TCP connection. We also saw this when looking at Honeygain network traffic in Section 4.3. Both Tosun et al. [3] and Mi et al. [4] also investigate commercial RESIP providers, and provide insight into their recruitment practices.

7 Conclusions

In this paper we have investigated the amount of suspicious search result on Bing, Google and Yahoo, finding out that Google generally shows fewer suspicious results than the other search engines, and that the search term "Honeygain" displays fewer suspicious results than "Peer2Profit" does, regarding results from both Google and other search engines. Some of this can be traced back to others on behalf of Honeygain submitting DMCA claims to Google to remove search results.

We could not find something inherently malicious in the data we collected from running Honeygain. However, if this was due to Honeygain's security measures or if we connected to a benevolent or at least neutral user is hard to tell. We can still see the potential for using residential IP addresses to shift blame onto another when committing crimes across the internet with the proxyware system, as it seems difficult, and maybe impossible, to fully prevent it regarding proxyware. So apart from risking your own IP address getting flagged as a bot, you should also be aware of the risk of it being used for something you did not intend which might lead back to you. The risk is most likely tiny, but it is definitely still there.

From looking at the communication going through our device, we can see that running Honeygain opens up many ports on the high numbers of User- and Dynamic ports, and that most communication is made with the private network IP address 172.17.0.2 as either the destination or the source. The only time our IP address is visible used is when communicating with the DNS protocol.

There are still more things here that can be further studied, for example a more comprehensive and longitudinal study of the communication going through our connection when being a part of the Honeygain network. One could also compare that with other providers of proxyware and look closer at differences in between, both in regards to if they follow their own policies, but also looking closer at what traffic patterns exists in order to create a way of finding hidden proxyware on a device.

References

- [1] Honeygain. *About Honeygain*. URL: <https://www.honeygain.com/about-us/> (visited on 05/03/2022).
- [2] Edmund Brumaghin. *Attracting flies with Honey(gain): Adversarial abuse of proxyware*. <https://blog.talosintelligence.com/2021/08/proxyware-abuse.html>. Aug. 2021.
- [3] Altug Tosun et al. "RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows". In: *2021 IEEE International Conference on Consumer Electronics (ICCE)*. 2021, pp. 1–6. DOI: 10.1109/ICCE50685.2021.9427688.
- [4] Xianghang Mi et al. "Resident Evil: Understanding Residential IP Proxy as a Dark Service". In: *2019 IEEE Symposium on Security and Privacy (SP)*. 2019, pp. 1185–1201. DOI: 10.1109/SP.2019.00011.
- [5] Honeygain. *How your network is used: business cases*. URL: <https://www.honeygain.com/business-cases/> (visited on 04/21/2022).
- [6] Enoch Root. *Businesses' proxyware headache*. URL: <https://www.kaspersky.com/blog/proxyware/42947/> (visited on 04/28/2022).
- [7] Adam Dubois. *Comparing Popular Proxyware Bandwidth Sharing Apps*. URL: <https://proxyway.com/research/proxyware-passive-income-apps> (visited on 05/06/2022).
- [8] NoFaithlessness1325. *Honeygain got my residential IP blacklisted as a VPN*. URL: https://www.reddit.com/r/Honeygain/comments/m8nuyp/honeygain_got_my_residential_ip_blacklisted_as_a (visited on 05/06/2022).
- [9] Jazzlikepatient33. *HoneyGain is a Scam!* URL: https://www.reddit.com/r/Honeygain/comments/p095yq/honeygain_is_a_scam (visited on 05/06/2022).

- [10] [deleted user]. *Did sharing IP with honeygain cause it? I am not using anything else to cause this.* URL: https://www.reddit.com/r/Honeygain/comments/11c31e/did_sharing_ip_with_honeygain_cause_it_i_am_not (visited on 05/06/2022).
- [11] Honeygain Support. *Honeygain respects your data & privacy.* URL: <https://www.honeygain.com/security> (visited on 05/05/2022).
- [12] Lumendatabase.org. *DMCA (Copyright) Complaint to Google.* URL: <https://www.lumendatabase.org/notices/27003010> (visited on 04/21/2022).
- [13] Wayback Machine. *Honeygain 14 March 2020.* URL: <http://web.archive.org/web/20200314023052/https://www.honeygain.com/> (visited on 04/27/2022).
- [14] Honeygain Helpdesk. *Error: Unusable network.* URL: <https://support.honeygain.com/hc/en-us/articles/360011078760-Error-Unusable-network> (visited on 04/28/2022).
- [15] Internet Engineering Task Force (IETF). *RFC 6335.* URL: <https://datatracker.ietf.org/doc/html/rfc6335> (visited on 05/08/2022).
- [16] Lumendatabase.org. *Search results.* URL: https://www.lumendatabase.org/notices/search?utf8=%5C%E2%5C%9C%5C%93%5C&term=honeygain%5C&sort_by= (visited on 04/21/2022).
- [17] Keenetic. *What is the difference between a public and private IP address?* URL: <https://help.keenetic.com/hc/en-us/articles/213965789-What-is-the-difference-between-a-public-and-private-IP-address-> (visited on 05/05/2022).
- [18] Tradedoubler. *Om oss.* URL: <https://www.tradedoubler.com/sv/om-oss> (visited on 05/04/2022).
- [19] Honeygain Helpdesk. *Payout Rate.* URL: <https://support.honeygain.com/hc/en-us/articles/360013231420-What-is-the-current-payout-rate-> (visited on 05/05/2022).