Investigation of attack vectors and protection against abuse of proxyware

Henrik Träff
hentr783@student.liu.se

Lucia Choura
lucch716@student.liu.se

Supervisor:
Niklas Carlsson, niklas.carlsson@liu.se

Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

The aim of this project was to outline the types of different attack vectors associated with proxyware applications and how these can be detected and protected against. Documented and possible attack vectors were collected and explained. A method for analysis was created but ultimately not executed due to constraints relating to running these types of applications on the university computers and lack of experience in cyber security. The results show that the range of attack vectors that can be staged against proxyware applications are many. Further investigation is needed to better define the attack vectors that more relate to proxyware applications, such as when the IP address of an infected device is masked on this network.

1. Introduction

With new technology comes new opportunities. The opportunities that present themselves are not only for the user of the technology, but also for potential attackers. The concept of proxyware is one example of a new technology and one that has grown in popularity in the past years. Proxyware or proxy applications are platforms marketed as a way for users to generate revenue by selling unused internet bandwidth. This opens the door for abuse of proxyware platforms. Some types of possible and observed attacks are information stealing, cryptojacking and Man-in-the-Middle attacks [1], [2].

This can lead to serious costs for both individuals and companies that decide to use these applications. That is why it is important to investigate different types of attack vectors on these platforms. To avoid these attacks, it is also important to investigate ways people can protect themselves. The purpose of the report was to study different attack vectors, how to detect them and protect against them. To gain further knowledge, the following research questions are answered:

- What type of attack vectors are there against proxyware, that may or may not be specific for these kinds of applications?
- How can each different attack vector be detected and/or protected against.
- To what extent can these attacks be simulated, measured and characterized?

2. Background

This section describes some concepts and definitions that will be used in the report.

2.1 Attack vector

Attack vector is a term used to describe possible methods or paths an attacker can make use of to exploit vulnerabilities in a system and gain access to said system [3].

2.2 Proxyware

Proxyware refers to a platform or application where the users are connected to each other in a network of clients. By joining a network, users can either sell unused bandwidth to other clients or pay a fee to get their traffic routed to the internet connection provided by other users on the network. There are several platforms that host these services. Honeygain, EarnApp, Peer2Profit, IPRoyal Pawns and PacketStream are examples of active platforms [4], [5].

Each one of these use different implementations to achieve the functionality that is associated with proxyware. However, one thing that is constant for all of them is that the actions executed by a bandwidth-buyer will be associated with the IP address of the bandwidth seller [5].

2.3 Wireshark

A network protocol analyzer that is open source and free of charge to use when wanting to capture network traffic on a computer. The wide range of features and applicable filters' allows for a flexible tool to analyze packets passing through the user's network [6].

2.4 VirtualBox

VirtualBox is a virtualization software (also called hypervisor or virtual machine) which allows the user to run different operating systems on their machine. This could for example be Linux, Mac OS and Microsoft Windows. There are several reasons as to why someone would use VirtualBox. It could be to try a different operating system, develop a program for a certain operating system or take additional precautions when handling potential malware since it isolates the malware from the host system [7].

2.5 IPRoyal Pawns

IPRoyal Pawns is an app or proxyware which is used to earn a passive income by selling internet bandwidth. The income is based on how much bandwidth is sold and how long the proxyware is active or running. For example, if a person sells 8 GB and has the app running for 16 hours daily, the total income would be 43 dollar/month. IPRoyal Pawns is available on Windows and Android. In regard to how a user's device is used, IPRoyal Pawns has an internal proxy service that is a Peer-to-Peer network that provides the client network with the IP addresses. The proxyware service is stated to have a team of security experts that monitor traffic and only allow legitimate traffic [8].

2.6 Peer-to-Peer networks

A Peer-to-Peer network is a set of peers or computers, where each one of them is linked to other peers within the network to share resources. This can be done with no physical connection. In a Peer-to-Peer network, each peer is equally privileged in terms of permissions and capabilities. Every peer acts as client and server, so the client-server architecture is removed. Skype and Bitcoin are two examples of the usage of Peer-to-Peer networks [9].

2.7 Virtual Private Network

A virtual private network (VPN) is used to establish a protected network connection between the user and the internet by creating a so-called tunnel. The data traffic that goes through the VPN or tunnel is encrypted and anonymized. It also disguises the user's actual IP address by substituting it with a different one in another location [10].

3. Solution and Analysis

3.1 Documented and possible attack vectors

This section presents a collection of attack vectors that can be linked to proxyware applications or that, theoretically, can be staged against a proxyware application.

3.1.1 Trojanized installers

As with any downloadable application, proxyware also has its fair share of trojan installers associated with them. By pretending to be an installer to the actual application, trojanized installers trick users to download malicious executables, allowing for malware attacks to be staged. With their own investigation [1], Cisco Talos Intelligence Group found multiple trojanized installers targeting users of Honeygain. Once executed, these trojans have different infection methods and stage different attacks. These trojanized installers, packaged as droppers, contain a legitimate Honeygain installer while also containing malicious executables that are run in silence next to the legitimate installer. One infection process of a trojanized installer, installs a legitimate Honeygain client while also trying to register the attacker's proxyware account on the victim's client. This serves as a means to monetize victims' internet bandwidth which could have consequences, such as: severely decreased internet connection speed, unhinged selling of bandwidth ultimately being costly for users on a tight internet plan. Besides the installer, there are other processes executing in the background. For a more detailed explanation of the infection process and its execution flow, please see the following source [1].

3.1.2 Cryptojacking and crypto mining

A perfect example of a malware attack that can be staged through a trojan horse is a cryptocurrency mining

malware. Crypto mining malware runs on the victim's processor and as a result occupies computing resources, ultimately making the victim's computer slower for other uses. These kinds of malware have been found in some trojans and are highly likely to be found in other trojans. In the case of proxyware, these can be staged together with trojans imitating proxyware installers [1], [11].

3.1.3 Information stealers

An information stealer is a Trojan malware used by attackers whose motive is to collect information from a person's device without the person's consent. A frequently used type of information stealer is one that collects login information, such as usernames and passwords. These are sent to another device through email or the network. Another commonly used information stealer are keyloggers. These intend to track the user's keystrokes to potentially obtain sensitive information [12]. This technique is also used by attackers when a person installs a proxyware infected with malware [1].

3.1.4 Referral codes

Another technique found to be associated with proxyware, is the monetization through distribution of Honeygain referral codes to victims. The victim is presented with a Honeygain landing page with a referral code (presumably) connected to the malicious actor's account, and then registers an Honeygain account, resulting in revenue being generated for the attacker.

A referral code is not an attack vector per se, but can still be used in conjunction with a trojanized installer [1].

3.1.5 Botnets

A botnet is a network of devices which have been hijacked and infected with malicious code. This network is controlled by an attacker or attackers remotely. Botnets are mostly used to perform a mass attack [13]. In the case of proxyware, a botnet can be used to generate revenue. What happens is that when the victim has installed the proxyware (together with the malware), the malware tries to use the attacker's login information to register a new client. Some proxyware applications have constraints on the maximum number of devices that can be registered under one account, Honeygain is one example. In this case, nothing prevents the attacker from creating several accounts [1]. Other proxyware applications might limit the number of devices registered on an IP address or network, and an example of this is IPRoyal Pawns [14].

3.1.6 Others

The concept of proxyware, selling internet to other users and ultimately becoming a node in a network that may or may not have already infected devices on it, allows for other types of attacks to be staged on the hosted network. Regular scanning and port attacks such as, syn flood attacks and Null scans can be performed on the network against other nodes than that of the infected.
Man-in-the-Middle attacks can be carried out on non-encrypted HTTP requests being sent over a shared internet connection. In [15], the authors discovered security risks on the relay system of VPN Gate. These risks would allow for Man-in-the-Middle attacks to be staged against nodes on the network. VPN Gate is operated on a distributed network of nodes relaying traffic, similar to a Peer-to-Peer network. This further shows that Man-in-the-Middle attacks potentially could be staged against nodes on the networks belonging to proxyware applications.

A more interesting aspect of these networks is that whoever is selling their internet, is also lending their IP address for others' activity to be associated with. In the case of suspicious activity, the host's IP address can end up being banned or registered on block lists for certain sites, limiting what the host can do on the internet. Also, legal aspects of such activities can also be of relevance, since it is hard to prove one's innocence, because the activity is connected to the host IP address. For organizations, this is of equal importance, if not more important. A blockage of an organization's IP address could really affect an organization's ability to carry out their business operation [1].

3.2 Protection against attack vectors

This section covers some methods that can be used to avoid possible attack vectors and how to detect malware in proxyware.

3.2.1 Education

A system is as secure as its weakest link, and usually these are the humans [16]. That is why it is of great importance to have knowledge regarding attack vectors. One way a person can gain knowledge is by doing some research and try to stay updated about what attack vectors are currently existing and protection against them. This can be done by reading magazines or websites with the focus on technology [17].

From an organization's perspective, it is of value to train the employees so that they can distinguish between malicious and non-malicious activity. It is also important to raise awareness of what kind of malware exists and continue to educate [18].

3.2.2 Antivirus

Although education is of importance, accidents can happen where a person might download infected software. Whether it regards an individual or organization, an antivirus software is another way to protect against attack vectors [18]. An antivirus software is designed to scan, detect, prevent and remove viruses from a device. It protects the devices' files and hardware from malware, for instance, this could be Trojan horses, worms, etc. [19].

3.2.3 Principle of least privilege

From an organizational aspect, the Principle of Least Privilege can be applied to minimize the risk of an employee exposing the organization to malware. This is because the principle gives the employees the lowest level of user right to perform their work [18].

3.2.4 Network traffic accounting

To protect against malicious, illegal and suspicious network traffic being sent through a user's device, the internet-sharing applications could allow the user to decide on what traffic to be allowed. In [20], by implementing a so-called, "allowlist", a node in their distributed VPN (dVPN) system, VPN-Zero, could then decide which traffic to be tunneled through it. This could potentially be applied to proxyware systems, so that unwanted traffic would not be allowed on nodes that do not allow it. This could however lead to nodes not being used and as a consequence, not generate revenue.

3.2.5 Detection of proxyware malware

Cisco Talos Intelligence Group concluded some indicators of compromise they had noted during their investigation [1]. The indicators include a mutex, a file hash, domains and URLs. The mutex found was, "LIJKMERGL32D23890NUFEWOIHJ". The following domains are related to the malware campaigns they analyzed:

- ariesbee[.]com
- bootesbee[.]com
- aurigabee[.]xyz
- analytics[.]honeygain[.]com

The mutex was for example in the initial malware loader and this loader starts creating the mutex and if it fails it exits. Another example is the URLs that can be found in different places in the malware. One case is about referral code where the malware used the initial installer process to run a file which redirected the person to the attackers (presumably) Honeygain referral code page. For more in-depth description and examples visit Cisco Talos Intelligence Groups website [1].

Malware can be detected by using machine learning. There are different techniques within machine learning that can be used. Some examples are support vector machines, Naïve Bayes and neural networks [21]. An example of machine learning detection is presented in [22], where network traffic relating to cryptojacking is classified with a machine learning algorithm. The algorithm was based on an analysis of traffic generated by cryptocurrencies. Their algorithm consisted of feature extraction, k-Fold Cross-Validation, Random Forest and statistics.

3.3 Proxyware network analysis

An additional investigation of the network traffic associated with one of the proxyware applications, IPRoyal Pawns, did not come to fruition as we would have hoped. Preparations for said investigation were planned, but ultimately did not get executed due to constraints regarding authorization and available resources. Running a IPRoyal Pawns client on the Linköping University internet would entail allowing other devices connected to the client to use the internet of the university while also generating revenue. This requires authorization, which would not be acquired. Secondly, running these kinds of applications comes with a risk of malicious traffic reaching the network of the university, which also adds to it not being allowed to do.

The approach switched to doing the analysis from a personally owned laptop with our own internet connection. On the laptop, VirtualBox was installed and set up so that the host IP network was hidden through the use of a NAT on the virtual machine. Due to the risk and uncertainty associated with doing this analysis, the laptop was chosen on the basis that the cost of using the laptop was not large. After a virtual machine with Windows 10 as the operating system was set up, Wireshark and IPRoyal Pawns were downloaded. However, the analysis was not performed due to uncertainty with second hand selling of internet connection. Both the internet provider and the landlord have to sign off/allow for internet bandwidth to be sold, especially since the internet agreement in place concerns both parties.

3.3.1 Packets of interest

Identifying malicious activity and/or infected nodes in a proxyware application is a rather broad task that includes analyzing for either well-known attacks and

scans or a general investigation of the data contained in the packets. In a proxyware network, where the user is a node hosting the internet connection, interesting packets include HTTP and HTTPS requests being made from the user's own IP address. In this regard, looking at a packet's source IP address would be redundant. Wireshark filters could be implemented to catch ICMP packets relating to scanning or DDoS attacks.

The result of running IPRoyal Pawns while simultaneously capturing HTTP and HTTPS packets would yield many more requests made from the host's IP address. From this, one could distinguish requests being made by others by looking at the associated server name, compare with traffic generated before running the application, and the type of request that was being made. See Fig. 1 and 2.

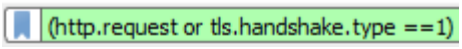

Figure 1. Wireshark filter for HTTP and HTTPS handshake packets.

Figure 2. Interesting information relating to HTTP and HTTPS packets in Wireshark.

3.4 Evaluation and Comparison

This section will cover the methods used while also evaluating them. Comparison to other methods will be made. There will be discussion about how to further the research.

3.4.1 Hands-on investigation

As previously described, an investigation of the network traffic on the proxyware could not be done. This was due to the potential security risks and opaque guidelines regarding if we are allowed to run and investigate proxyware even though it would involve monetizing the university's network for the sake of the investigation. We considered running the proxyware using our own internet, but this would require us to check with our landlord since they are providing the internet. Our assessment was that this would be time-consuming since we would probably need to speak to a manager who might or might not give us an approval. In this case, our resources to do the analysis were limited.

After consulting with our supervisor about how we could proceed further, we concluded that we would not continue the investigation. Since the project was time-limited, we might have not been able to do a thorough analysis, which in return might not be useful for the report. On the other hand, it would be interesting to analyze and gain further knowledge about the tools we were using and the different ways these can be used.

In hindsight, better foresight would have helped us understand the necessary boxes to tick off before an analysis could be made. This would have provided us with a time buffer so that we might have been able to solve the unforeseen obstacles and do the traffic analysis. To set up a workplace where malicious activities can be examined, requires experience in working with cyber security. We believe that if we had experience with the different tools we used and how to perform an analysis, it would have made it feasible for us to do the intended investigation.

3.4.2 Literature

Besides the intended traffic analysis, we did research on secondary sources. The sources we found consisted mostly of blogs, tech, websites and company websites. The information written in them were very similar to each other and many other websites we found, but one of our references stood out. This was, as mentioned before, the investigation made by Cisco Talos Intelligence Group. Their investigation was thorough, and their work has therefore been essential for this report [1]. In other optimal circumstances, we would have liked to do a similar investigation to get a more in-depth understanding and experience about the different attack vectors directed at proxyware.

Other than literature directly relating to proxyware applications, a couple of published papers that somewhat relate to this subject were found. The authors in [20], presented a Distributed Virtual Private Network (dVPN), that would preserve privacy and implement traffic accounting. This seemed relevant given that dVPNs and most proxyware applications make use of Peer-to-Peer networks in their services. In regard to detection of malicious activity through network traffic analysis, [22] proved to be relevant in suggesting approaches to detect suspicious activity. Using machine learning to detect network traffic associated with crypto mining on a local network, could potentially be applied to detect cryptojacking on a proxyware network.

3.4.3 Further research

There are a number of things that can be done in future research. One would be to do an investigation and analysis to not only get more insight but to see if the already existing attack vectors have advanced and if completely different attack vectors can be detected. In addition, it would be of interest to explore new tools that can be useful to do such investigations. It is also engaging to explore new and different ways to protect against attack vectors and see if/how they differ from these available today.

4. Related work

4.1 Analysis of trojanized installers

Cisco Talos Intelligence Group, one of the largest commercial threat intelligence teams, have investigated and documented attacks against proxyware applications. Specifically, the intelligence group investigated possible attacks against the Honeygain platform. Their result covers a detailed explanation of multiple infection processes of found trojanized installers associated with Honeygain, while also more generally discussing possible attacks against proxyware applications. Analyzing attack vectors, such as trojanized installers, would only be feasible if the ones carrying out the analysis are experienced in the field of cyber security and have access to needed equipment and hardware. Therefore, their analysis of these kinds of attack vectors would have to be sufficient for the sake of the report. We implore you to read their post for a detailed coverage of proxyware associated trojanized installers [1].

4.2 Strong privacy guarantees with dVPNs

In [20], the authors talk about requirements related to a successful dVPN and present their own dVPN with strong privacy guarantees, minimal impact on performance and a way to account for the traffic tunneled through a user's device. The network traffic of VPN-users might not preserve privacy. There are no guarantees that the commercial VPN providers will not log or tamper with the personal traffic. With distributed VPNs, the VPN service is decentralized. For the users of dVPNs, in addition to being VPN clients, they are also a part of a peer-to-peer network, as relay nodes. In conjunction with the improved privacy of these networks, other risks are introduced.

In a Peer-to-Peer network, users may need to facilitate illegal or harmful traffic through their device. There is also, similarly to VPN, not a guarantee regarding personal traffic privacy. The solution presented in [20], VPN-Zero, is a dVPN that preserves privacy and implements traffic accounting. The idea behind this solution is that the nodes of the network should be able to control what traffic is tunneled through them. One caveat with this solution is that strong privacy guarantees can only be achieved through the usage of private traffic such as TLS [23] and DOH [24]. The presented solution seems promising, but future work is needed when it comes to traffic forwarded to Content Delivery Networks (CDNs).

As many of the internet-sharing applications are implemented using a Peer-to-Peer network, VPN-Zero might prove to be relevant in making proxyware users account for traffic tunneled through their devices. The introduction of an "allowlist" could serve as a prevention mechanism against harmful or illegal traffic. Users would then no longer run the risk of allowing these types of traffic to be tunneled through their device and be associated with illegal or harmful traffic. Privacy concerns regarding the proxyware service providers is also something to look into, and the design of VPN-Zero could also help with making proxyware preserve privacy.

4.3 Machine learning to detect cryptojacking

Another related work is by Caprolu et al. [22], where they used machine learning to analyze a network to find out if there was any activity of malicious mining, also called cryptojacking. What they did was analyze network traffic of three cryptocurrencies, Bitcoin, Monero and Bytecoin. This was done using normal traffic and traffic shaped by VPN (NordVPN and ExpressVPN). Both ingoing and outgoing network flows were studied. They found that depending on what cryptocurrency was used, the interarrival time and packet size could vary when using VPN. Caprolu et al. [22], presents the Crypto-Aegis Framework (a machine learning framework) which they designed based on the analysis. The purpose of the framework was to detect and identify activities linked to cryptocurrencies. According to the authors, their solution was "superior to competing solutions in the literature" basing the statement of their results' on viability and quality [22]. Their work could be extended so that it can be applied for several uses or attacks. This detection technique could allow proxyware applications to better detect misusages of the application and increase the cyber security of these platforms.

5. Conclusions

Even though the project was met with difficulties in order to be properly executed, there are still takeaways in regard to the stated research questions. When it comes to

the types of attack vectors against proxyware, the range of them is quite substantial. As with any trojan, a multitude of different malware attacks can be staged, and it is no different to proxyware applications. More specific to proxyware, instances of malware attacks trying to hijack proxyware clients in the installation phase, have been found. Secondly, referral codes associated with presumably an attacker's account, have been recorded in instances where the attackers try to get the victim to register through their referral code, ultimately gaining a profit.

When it comes to what a connection to one of these services entails for a client's device, the answer is not certain. Like with any network that has infected nodes on it, malicious traffic to the other nodes can range from a plethora of attack vectors. In this regard, one might hope that the service provider has a system in place to stop malicious actors from being on their networks. We had hoped to gain more clarity on this subject than what was gained, and there is certainly a need for investigation in this area of proxyware applications.

Lastly, a host node selling an internet connection also involves associating the host IP address with all internet traffic being made. This would mean that other malicious activity on the internet would be associated with the host, masking the malicious actor. Also, this would lead to consequences such as IP address blocks or even legal conflicts. Users and companies need to be aware of these risks, and take necessary precautions if ever a proxyware service is to be used. Antivirus programs might even be circumvented by the traffic generated on this network, which in turn sparks the idea of organizations implementing the principle of least privilege. Proxyware applications are a fascinating concept with many possible pitfalls. With more services of this type launching, the more sophisticated attack vectors against proxyware are employed and the need for investigation grows.

References

[1] E. Brumaghin, Cisco Talos Intelligence Group, https://blog.talosintelligence.com/2021/08/proxyware-abuse.html , 2021

[2] CywareLabs, https://cyware.com/news/attackers-sell-your-internet-bandwidth-for-passive-income-f385f4ea, 2021

[3] Sumo Logic, https://www.sumologic.com/glossary/attack-vector/, 2019

[4] C. Osborne, ZDNet, https://www.zdnet.com/article/cyberattackers-are-now-quietly-selling-off-their-victims-internet-bandwidth/, 2021

[5] J. Grimes, BestProxyReviews https://www.bestproxyreviews.com/honeygain-vs-iproyal-pawns-vs-packetstream-vs-peer2profit/, 2022

[6] Wireshark, https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

[7] J. Wallen, TechRepublic, https://www.techrepublic.com/article/virtualbox-everything-the-pros-need-to-know/, 2017

[8] IPRoyal Pawns, https://iproyal.com/pawns/

[9] N. Jafari Navimipour, F. Sharifi Milani, "A comprehensive study of the resource discovery techniques in Peer-to-Peer networks", *Peer-to-Peer Netw. Appl.*, Volume 8, 2016, pages 474–492. Available online at: https://doi.org/10.1007/s12083-014-0271-5

[10] H. Sawalmeh, M. Malayshi, S. Ahmad and A. Awad, "VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements", *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2021, pages 236-241. Available online at: https://www.doi.org/10.1109/3ICT53449.2021.9581512

[11] Kaspersky, https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking, 2022

[12] Trend Micro, https://www.trendmicro.com/vinfo/us/security/definition/Info-stealer, 2022

[13] Trend Micro, https://www.trendmicro.com/vinfo/us/security/definition/botnet#:~:text=A%20botnet%20%5Bshort%20for%20bot,rented%20out%20to%20other%20cybercriminals, 2022

[14] IPRoyal Pawns, https://iproyal.com/pawns/terms-of-use/

[15] Y. Sun, B. Wang, C. Wang, Y. Wei, "On Man-in-the-Middle Attack Risk of the VPN Gate Relay System", *Security and Communication Network*s, 2021. Available online at: https://doi.org/10.1155/2021/9091675

[16] E. Kost, UpGuard, https://www.upguard.com/blog/what-is-an-attack-vector, 2022

[17] Tech-blog, gbadvisors, https://www.gb-advisors.com/attack-vectors-in-cybersecurity/, 2018

[18] B. Soare, Heimdal, https://heimdalsecurity.com/blog/attack-vectors/, 2022

[19] Verizon, https://www.verizon.com/info/definitions/antivirus/

[20] M. Varvello, I. Querjeta Azurmendi, A. Nappa, P. Papadopoulus, G. Pestana, B. Livshits, “VPN-Zero: A Privacy-Preserving Decentralized Virtual Network”, *2021 IFIP Networking Conference*, 2021, pages 1-6. Available online at: https://doi-org.e.bibl.liu.se/10.23919/IFIPNetworking52078.2021.9472843

[21] R. Sinha, S. Lal, “STUDY OF MALWARE DETECTION USING MACHINE LEARNING”, 2021. Available online at: http://doi.org/10.13140/RG.2.2.11478.16963

[22] M. Caprolu, S. Raponi, G. Oligeri, R. Di Pietro, “Cryptomining makes noise: Detecting cryptojacking via Machine Learning”, *Computer Communications*, Volume 171, 2021, pages 126-139. Available online at: https://doi.org/10.1016/j.comcom.2021.02.016.

[23] E. Rescoria, Tls 1.3 rfc, https://datatracker.ietf.org/doc/html/rfc8446, 2018

[24] P. Hoffman, Dns queries over https (doh), https://datatracker.ietf.org/doc/html/rfc8484, 2018