Illuminating HolaVPN and the Dangers It Poses
TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by:
Trend Micro Research

Stock images used under license from Shutterstock.com

For Raimund Genes (1963-2017)
This paper is about free software called HolaVPN that has been installed on millions of computing devices around the world. HolaVPN is being marketed as a community Virtual Private Network (VPN): Internet users are told they can help each other to access websites freely and without censorship by sharing their internet connections. This may sound like a noble initiative, but in reality the HolaVPN service poses severe risks to the internet community in a number of ways.

First of all, the HolaVPN software does not use encryption and it leaks client IP addresses. This makes it dangerous to use for internet users who wish to use VPN services to avoid surveillance or censorship. The community aspect of HolaVPN is seemingly absent. As our research showed, users of HolaVPN don’t really share their internet connections with each other; instead, their web traffic is routed through a list of about a thousand exit nodes hosted in data centers. Each computing device with free HolaVPN version installed is turned into an exit node that is monetized by a commercial service called Luminati. This commercial service, which is also owned by Hola Networks Ltd., is selling the bandwidth of HolaVPN users to third parties by offering a residential proxy network. This has been a known issue since 2015; however, it has not been apparent so far for what purposes the Luminati network is being used. A residential proxy network with millions of exit nodes can be abused in various ways as it gives a high degree of anonymity. Cybercriminals have a great interest in such a network to commit their crimes illicitly. In this paper we will explain in detail how the Luminati proxy network works and how it is being abused by malicious actors.

To understand what Luminati is being used for, we analyzed 100 million URLs that were scanned anonymously for security purposes through Trend Micro software installed on about 7,000 computers that had been used as exit nodes of the Luminati residential proxy network in 2017 and 2018. We made an explicit breakdown and thus got a good understanding of the nature of Luminati traffic. It appears that more than 85 percent of all Luminati traffic in our dataset was directed to mobile advertisements, mobile app domains and affiliate programs that pay for referrals and installation of apps. Millions of clicks on advertisements and advertisement impressions are loaded via Luminati each day — a potentially very profitable business. The market of mobile advertisements is huge and growing rapidly, and fraudsters will try to get their share of the revenue. During our investigation, we collected explicit evidence that the former actors who were involved in the infamous KlikVip gang (also related to a now-defunct Ukrainian company called Innovative Marketing) are now using Luminati to send traffic from their mobile advertisement sites to third-party landing pages. Given the past activities of KlikVip, it is likely that these actors found a new way to commit click fraud on a large scale. This is one of the obvious ways how a proxy network like Luminati can be abused.

We also found that a substantial part of the Luminati traffic was related to the scraping of online content such as subscription-based scientific magazines, private contact details of physicians and attorneys, data on inmates, court documents in the U.S. and China, credit information, and even the Interpol's most wanted list. Airline reservation systems and websites that sell concert tickets were being accessed frequently via Luminati as well. Boarding passes, online check-in portals and Passenger Name Records (PNR) were accessed via Luminati in significant numbers. Limited edition sports shoes and other popular but hard-to-get items were bought by scripts using Luminati. To evade botnet detection, some users of Luminati are likely using captcha solving services offered by sweatshops.

Aside from finding data scraping activity on Luminati, we also saw it being used by hackers for their illicit activities. We have collected evidence that hackers have attempted to verify leaked webmail credentials via Luminati and have even tried to access the webmail of companies through the proxy network for an extended time period. Mobile payment systems were accessed via the Luminati network as well.

In this paper, we will provide a detailed look into HolaVPN and Luminati. We will compare traffic going through Luminati with traffic that is coming from computers that have known adware installed. There appears to be a significant overlap in traffic patterns that are related to adware and Luminati. We will explain why HolaVPN and Luminati are major risks to our customers and internet users in general.

To protect our customers, we have decided to detect the HolaVPN software as unwanted, high-risk software. We recommend all corporations and organizations not to allow HolaVPN in their network.
Overview of HolaVPN

We started our research into HolaVPN and Luminati in 2017 when we were approached by Swedish investigative journalist Mattias Carlsson of Dagens Nyheter, one of Sweden’s more popular newspapers. He had information on the current activities of the infamous KlikVip actors. From 2006 to 2010, the KlikVip actors were notorious for promoting click fraud scams and spreading fake antivirus software. He told us that the former KlikVip actors now own a company based in Berlin, Germany, that sells car parts and has numerous international websites. This company received the attention of the journalist as it was advertising on a couple of extremist websites in Sweden.

We looked into the company identified by the journalist and found that it was using internet infrastructure of a size that is unusual for a car parts company. We found that as of September 2018, the company has more than 240 IP addresses being used in about 20 different IP ranges. The company’s name is also used in the SSL certificates of mobile advertisement domain names, and the mail servers of these sites are hosted in the company’s IP space. After further research, we soon found out that the former KlikVip actors have registered more than 50 mobile advertisement domains.

After a closer look into these mobile advertisement service providers, we found that the vast majority of the traffic related to these sites is routed through the Luminati proxy network. We estimate that up to 4 percent of all traffic that was sent through Luminati (with millions of exit nodes) in 2017 was related to domains that are owned by the former KlikVip actors. This sparked our interest in Luminati and its sister service HolaVPN. Given the past activities of KlikVip, we suspected that the mobile ads traffic might be fraudulent and we started to systematically collect information on Luminati.

![Figure 1. One of the websites related to mobile advertisements linked to the former KlikVip actors](https://example.com/image.png)

---


History of HolaVPN

Hola Networks Ltd. initially started as a stealth startup company called Zon Networks Ltd. in 2008. On its website, Zon Network wrote in 2009, “ZON is developing the next quantum leap in communications for consumers, based on technology which is extremely advanced, yet super-simple to use. We plan to launch ZON 1.0 soon.”

The company, which is based in Netanya, Israel, changed its name to Hola Networks Limited in October 2010. It was in stealth mode for several years and, from what we understand, Hola Networks had ambitions as great as Zon Network had in 2009. After about four years in stealth mode, it finally launched an alpha version for software that it claimed will make the internet 10 times faster. In 2012, the company posted on its website that Hola “is building an overlay network for HTTP, DNS, TCP and IP, which will change the way the Internet works - for the first time in 40 years...”

Note: In 2012, Hola Networks claimed it was working on a new project that would change the internet “for the first time in 40 years.”

Figure 2. Screenshot of the hola.org website from 2012

The project sounded very ambitious and was probably way too ambitious. We don’t know what happened to Hola Networks’ initial plans, but we do know that in 2012 the first versions of HolaVPN software were offered as a free peer-to-peer (P2P) VPN network. The software of HolaVPN was far from a new overlay network of HTTP, DNS, TCP and IP, and later, there appeared to be some serious security issues with the software. As we will show in our analysis, today, HolaVPN still isn’t a secure VPN solution like many other companies are offering. In 2015 it became evident that HolaVPN is selling the bandwidth of its millions of users via another company called Luminati. Luminati is also owned by Hola Networks Ltd. This was in the news in 2015 and back then it wasn’t obvious and it wasn’t mentioned in the terms and conditions of HolaVPN explicitly.

---

In the next section, we will first look into the HolaVPN software and explain why it isn’t software that can be called a VPN. We will show for what purposes the Luminati network is being used in succeeding sections.

**Analysis of HolaVPN software**

We started our analysis by looking at the browser extensions of HolaVPN that are offered on the hola.org website and on the Google Chrome™ Store. Upon installing the browser extension, which was originally marketed as a peer-to-peer network, we quickly realized that HolaVPN is not similar to other VPN services that route all of the client’s network traffic through an encrypted tunnel. Rather, it only routes HTTP and HTTPS traffic of the browser through the HolaVPN network with no encryption. The absence of encryption alone already makes HolaVPN a dangerous tool for internet users who are looking for online security and privacy.

![Hola's browser extension asks for all kinds of permissions to access users’ data](image)

Figure 3. Hola’s browser extension asks for all kinds of permissions to access users’ data

After installing HolaVPN's browser extension, a user will be asked to download the HolaVPN setup package that will install additional components.
The Hola installer package contains multiple binaries but there are two important binaries needed for it to function well: a Chromium™ browser with a HolaVPN browser extension pre-installed and a Hola service (hola_svc.exe) that handles exit node traffic and communication with the command-and-control server (C&C) of Luminati. We noticed that the version of the Chromium browser that was installed was a two-year-old version (49.0.2623.110) at the time we tested the Hola installer package in 2018. Of course, installing two-year-old software is an additional risk for HolaVPN users. We retested this on October 28, 2018 and discovered that the Chromium version has been updated to 68.0.3440.75. Despite this update, the Chromium version HolaVPN uses is still not the latest stable Chromium build, possibly putting users at risk.

We analyzed the network traffic of HolaVPN to check how its P2P connection works. HolaVPN is advertised as a P2P network where users can use idle resources of each other’s computing devices. However, we found that traffic is mostly routed through roughly 1,000 super nodes in data centers. Upon installing HolaVPN, we chose different exit nodes on the menu. Then, we checked the IP addresses of the exit nodes if they were all in the data centers. We discovered that the menu in the HolaVPN software only allows for choosing a country. In some cases, the chosen country is not available. When this occurs, another exit node (in a data center) will be chosen. We did not observe any real P2P traffic and it doesn’t seem to be possible at all to use other users’ computers as exit nodes. Also, as we will show in the next sections, the vast majority of the traffic that is routed through the residential HolaVPN exit nodes is not generated by other HolaVPN users. So there is seemingly an absence of real P2P traffic. This is in contrast to how HolaVPN is marketed as a tool to “[share …] bandwidth with the community.”

---

On October 8, 2018, HolaVPN updated its Chrome browser extension overview in the Chrome Web Store: It now states that the HolaVPN extension is not a P2P application. It also states that the extension does not link to nor does it encourage the download of other products or components, as it can fully function by itself upon download. However, when we installed and tested HolaVPN’s Chrome browser extension on October 28, 2018, we were still prompted to install additional components to run the proxy. It is hard for a regular proxy user to use the HolaVPN software without downloading additional components such as the months-old Chromium browser extension and an executable file.

We found serious risks for internet users, especially those who rely on HolaVPN to access websites that are blocked or censored in their home countries. First of all, there is no encryption between the client and super nodes. This is very unusual for software that claims to be a VPN solution, and it makes HolaVPN basically useless for anonymity purposes and dangerous to use.

Second, we discovered that client machines that have the free version of HolaVPN installed will leak the real client IP address to the websites the user is browsing. To verify this, we registered a testing domain and accessed the domain using the free version of HolaVPN. The following occurs when a user types a new domain in the HolaVPN browser after selecting the country the user wants to access the internet from:

1. Even though the icon on the browser says that HolaVPN is active, if a user opens a new tab and types a domain in the browser bar, the site will be accessed directly via the client IP address. That is a huge risk in itself.
2. The HolaVPN browser downloads a list of exit nodes for the desired domain.

```
GET /client_cgi/rule_ratings?rmt_ver=1.82.644&ext_ver=1.81.443&browser=chrome&product=www&lccgi=0&root_url=tripod.com&src_country=BR&limit=20&proxy_country=&vpn_only=true HTTP/1.1
```

3. The system verifies if the customer has a paid subscription or has the free version.

4. The browser sends a user ID (UID) and the domain he is trying to access to client.hola.org.

5. An HTTP GET request is sent to hola.org in the following format:

```
GET /access/ourtestdomain.com/using/vpn-us?go=2 HTTP/1.1\r\n```

6. Another HTTP GET is sent, this time to the website of the domain directly, thus leaking the real user’s IP and letting the domain owner know that the user is a HolaVPN user, as the referral header contains information about HolaVPN.

7. The client sends a “ping” to the exit node via HTTP.

8. The client connects to a super node of HolaVPN without encryption:

```
Authorization: Basic dXNlcj1jaWQtMTU5NDQ5NTc5LXV1aWQtNzY0Tk0ZjY1OTEyYmVkYzElZTgyZjI2ODIyZyYmQ6ZDc1MzMyZDhjMGM4
```

9. Now all HTTP(S) requests are proxied through the super node.

This behavior is very different from that of a normal VPN solution where all internet traffic is routed through an encrypted VPN tunnel. HolaVPN is not a secure VPN solution — rather, it is an unencrypted web proxy service.

The absence of encryption between client and super nodes means that somebody who is able to intercept traffic can see the websites a Hola user is visiting and can read data he is uploading or downloading on the internet. This is in contrast to how HolaVPN is marketed on its website and in recent public talks by the Hola Networks Ltd. CEO. In reality, it introduces significant risks to internet users.
The super nodes of HolaVPN block access to several websites that belong to widely used webmail services like mail.aol.com and outlook.com. Several other domains like ticketmaster.com are blacklisted too. Maybe this was an easy solution to stop abusive traffic that is being sent through the HolaVPN super nodes. Regardless, a VPN service that blocks a variety of websites is of limited use. Its marketing claims appear to be far from the actual truth.
Hola Networks Ltd. is offering a premium version of HolaVPN with a paid subscription wherein there are no blacklisted domains. Donating computing resources as an exit node is also optional for this service.

There is a critical risk to users of the free version of HolaVPN software in a corporate environment. The exit node that will be installed on the users’ computers will potentially give unknown third parties access to internal systems. Through the computing devices that have HolaVPN installed, the corporate firewall can be circumvented and reconnaissance of the internal network is possible. This alone is a good reason to not at all allow HolaVPN in a corporate environment.

Uninstalling Hola binaries can be done via the Control Panel (Control Panel > Program > Uninstall a program). However, after performing the process, we discovered that the binaries were not deleted from the system. Though we found that both the service and auto-start registries have been deleted, we saw that Hola was running during the uninstallation process itself – meaning the registries will be added right back after the uninstallation process.

**Increasing User Base Through SDKs**

Hola Networks Ltd. and Luminati are actively seeking to increase the number of exit nodes in the Luminati proxy network. To this end, Luminati offers a software development kit (SDK) for Android™ and Windows® applications. This SDK can be bundled with third-party software and apps. When an app is bundled with Luminati’s SDK, the user is prompted to install additional software that would allow Luminati to use the client computing device as an exit node. Luminati’s SDK is available for Windows and Android applications.¹¹

![Figure 8. Several Android apps are using the Luminati SDK](https://luminati.io/sdk)

In 2017 and 2018, employees of Luminati sent unsolicited email messages advertising the SDK options to several mailing lists that deal with the development of open-source software. In a typical email from Luminati employees, it states that Luminati pays US$3,000 per 100,000 active users per month. The unsolicited email messages were sent to the development community of Nmap (a free open-source security scanner tool), Pidgin (a free messaging client), SuperTux (a free open-source video game) and several other mailing lists. It is highly advisable to decline any bundling with Luminati’s SDK.

Naturally, most of the developers of free open-source applications are not interested in monetizing their software by bundling it with adware or the SDK of Luminati.


The Luminati Proxy Network

So far, a breakdown of the actual traffic that is sent through the Luminati proxy network has not been published or publicly revealed. This section will look at who is using Luminati and how. The next section will provide a detailed breakdown of the Luminati network’s traffic.

On its website, Luminati describes itself as the world’s largest proxy network, with millions of residential IP addresses. According to the company, there are various use cases for the proxy network like retail price comparison, advertisement verification, brand protection and sales intelligence. Usage of the residential proxy network of Luminati cannot easily be detected by website owners and advertisers — the exit nodes are not known publicly. IP addresses that are assigned to home users are often dynamic and not static. This means it is very hard to detect and block Luminati exit nodes.

The proxies Luminati is selling access to are computing devices of internet users who have installed HolaVPN. HolaVPN advertises itself as a free peer-to-peer VPN network. It is said that users who install HolaVPN can use the internet connections of other users as exit nodes, provided that they allow their own computer to become an exit node as well. Together with the HolaVPN software, another binary is bundled and installed that communicates with Luminati C&C servers and hence gives Luminati a way to sell the bandwidth of millions of residential computing devices to third parties.

Figure 11. Luminati advertises the use of its vast proxy network to scrape online contents
Hola Network Ltd. CEO says in public presentations and interviews that HolaVPN helps the public in countries where governments enforce censorship and that they see an uptick in HolaVPN usage whenever a country decides to block access to certain sites.14 The CEO has also given examples of how to use Luminati for companies active in advertising, travel, security, online retail, recruitment and financial services.15 As shown in the screenshot in Figure 12, he claims that one of Hola Networks’ largest customers has said that “Luminati is the absolute truth.” 16

![Figure 12. A hyperbole on Luminati's usage from a presentation of the CEO of Hola Networks Ltd.](image)

The reality is, however, that a large residential proxy network like Luminati poses a big risk to security on the internet. Because the exit nodes are hard to track and are of a dynamic nature, it is possible for users of the Luminati network to be anonymous to a high degree. Selling the bandwidth of millions of residential internet users is a very risky business as it will surely attract cybercriminals and fraudsters. It is not hard to imagine that actors committing click fraud or targeted attackers who do reconnaissance of a network have a great interest in getting access to Luminati. The advertisement business in general is exposed to a lot of attempts to commit fraud. The incentive for committing advertisement fraud is large as the total market of advertisements on the internet is estimated at many billions of dollars and is still growing each day.17

---


In the next sections, we provide a detailed look into the Luminati proxy network. We have researched the outgoing traffic of thousands of Luminati exit nodes for more than a year. We have collected more than 100 million URLs that were sent through about 7,000 exit nodes in the Luminati network and we made a detailed breakdown of these URLs. It appears that the vast majority of the traffic through Luminati is going to websites owned by companies who are active in mobile advertisements and apps for mobile devices. We also saw evidence of scraping of online content, and a significant part of Luminati traffic is going to reservation systems of airlines and concerts. We also saw some traffic related to email account hacking. A very limited percentage is related to academic research and security companies that monitor phishing sites.

Some customers of Luminati

Though the majority of the traffic that is sent via Luminati most likely comes from scripts and automated computer software, it is possible to use the Luminati network manually too. In case someone is using the Luminati proxy network on a corporate laptop or desktop computer, the user will risk leaking personal information, as standard software (like Microsoft® Outlook®) might attempt to load configuration URLs that are typical for a corporate network environment. It appears that some of the customers of Luminati most probably leak corporate URLs. By a careful analysis of the traffic that is being sent through Luminati, we were able to identify a couple of companies that are likely using Luminati manually. Among these companies we found is an India-based company that provides services in rate intelligence and price optimization for the travel and hospitality industry.

Figure 13. A Luminati customer’s website offers rate intelligence and price optimization services in the hospitality service and travel industry
Another probable Luminati customer is an Israeli company that claims to be in the ad security and verification business. According to its website, this company is offering the “world’s largest and fastest premium proxy network.” This company is possibly reselling Luminati services.

We also have evidence that a U.S.-based business that offers to bring new followers on Instagram is also using the Luminati proxy. We can easily imagine how Luminati could be used to create new (fake) followers on Instagram and how it could be used to let bots interact on social media as if they are real human users.

About 4 percent of all traffic that is routed through the Luminati proxy network is related to mobile advertisement companies that have been set up by the former KlikVip actors. These actors also offer a service that they claim can be used to check the proper functioning of a chain of redirects between different affiliate sites that eventually will lead an internet user to a landing page or an advertisement. The company website (see Figure 14) states that 100,000 URL redirect checks per day are available for almost US$1,500 per month. We don’t know whether this is a real business offering or not, but this could be used for click fraud too. We do know that the said service makes use of the Luminati proxy network to check chains of URL redirects. Thus, we were able to have actual hard evidence that the former KlikVip actors are using Luminati.

Figure 14. Former KlikVip actors offer a service that is supposed to check affiliate links
Breakdown of Luminati Traffic

Hola Networks Ltd. sells the bandwidth of millions of HolaVPN users via their Luminati website. Prices are steep and start from US$500 up to US$100,000 per month. The average user of HolaVPN will have no idea what kind of traffic Luminati is pumping through the user’s internet connection. A user might think that going for HolaVPN’s service will benefit the internet community at large and give people living in countries with censorship the freedom to access blocked websites without fear. As we have mentioned in the previous sections, we did not see any evidence for the latter. On the contrary, the vast majority of traffic generated by HolaVPN users is going through more than 1,000 proxies hosted at cheap data centers around the world. The bandwidth resources HolaVPN “shares” with the community is being used for Luminati.

So far, the traffic coming out of Luminati has not been described in a public report. In this section, we will make an explicit breakdown of the traffic that was pumped through Luminati for more than a year, starting in spring 2017 and ending in 2018. We analyzed the traffic coming out of 7,000 Luminati exit nodes on computing devices that run Windows systems. We collected more than 100 million URLs that were sent through these Luminati exit nodes.

Figure 15. Subscription plans for Luminati
Mobile Traffic

The first thing we noticed is that about 80 percent of all traffic that is sent through Luminati has a forged user agent that is set to a mobile device like an iPad®, iPhone® or Android phone. This means that about 80 percent of the traffic that is sent through the Luminati network looks to be coming from a mobile device when in reality it comes from a Windows machine. This immediately raises a question: Why is there such a large portion of forged mobile traffic being routed through Luminati?

![Chart showing OS distribution](chart1.png)

*Note: Interestingly, included in the Others category are Windows Phone (.09%) and Blackberry OS (.02%).*

Figure 16. Breakdown of OS according to user agents used in Luminati traffic

![Chart showing browser distribution](chart2.png)

Figure 17. Breakdown of browsers in the forged user agents in traffic that is routed through Luminati
After a more detailed analysis, it appears that a large percentage (up to 86 percent) of all Luminati traffic is going to domains of companies that are either developing mobile apps, are in the mobile advertisement business, or in the business of affiliate tracking. Table 1 shows the top 20 companies.

<table>
<thead>
<tr>
<th>Company</th>
<th>Country/Region</th>
<th>% of Luminati Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile app advertisement company 1</td>
<td>USA</td>
<td>5.1%</td>
</tr>
<tr>
<td>Mobile app advertisement company 2</td>
<td>China</td>
<td>4.4%</td>
</tr>
<tr>
<td>Mobile affiliate network company 1</td>
<td>India</td>
<td>4.3%</td>
</tr>
<tr>
<td>Mobile app company 1</td>
<td>China</td>
<td>3.8%</td>
</tr>
<tr>
<td>Mobile advertisement company of former KlikVip actors</td>
<td>Ukraine</td>
<td>3.5%</td>
</tr>
<tr>
<td>Mobile app advertisement company 3</td>
<td>Portugal</td>
<td>3.3%</td>
</tr>
<tr>
<td>Mobile affiliate network company 2</td>
<td>USA</td>
<td>3.2%</td>
</tr>
<tr>
<td>Mobile advertising company 1</td>
<td>China</td>
<td>2.7%</td>
</tr>
<tr>
<td>Mobile app advertisement company 4</td>
<td>India</td>
<td>2.6%</td>
</tr>
<tr>
<td>Mobile affiliate network company 3</td>
<td>China</td>
<td>2.4%</td>
</tr>
<tr>
<td>Mobile affiliate network company 4</td>
<td>Taiwan</td>
<td>1.8%</td>
</tr>
<tr>
<td>Mobile advertising company 2</td>
<td>India</td>
<td>1.6%</td>
</tr>
<tr>
<td>Mobile affiliate network company 5</td>
<td>Russia</td>
<td>1.5%</td>
</tr>
<tr>
<td>Mobile advertising company 3</td>
<td>Netherlands</td>
<td>1.4%</td>
</tr>
<tr>
<td>Mobile advertising company 4</td>
<td>Germany</td>
<td>1.4%</td>
</tr>
<tr>
<td>Mobile app advertisement company 5</td>
<td>Hong Kong</td>
<td>1.3%</td>
</tr>
<tr>
<td>Mobile app advertisement company 6</td>
<td>China</td>
<td>1.3%</td>
</tr>
<tr>
<td>Mobile affiliate network company 6</td>
<td>USA</td>
<td>1.3%</td>
</tr>
<tr>
<td>Mobile app advertisement company 7</td>
<td>China</td>
<td>1.2%</td>
</tr>
<tr>
<td>Mobile app advertisement company 8</td>
<td>Brazil</td>
<td>1.18%</td>
</tr>
</tbody>
</table>

Table 1. Breakdown of traffic that is routed through the Luminati proxy network based on Trend Micro™ Smart Protection Network™ data

The market of mobile advertisement is huge and is still growing fast. It has been estimated at US$143 billion in 2017 and will continue to grow for the coming years.\(^{18}\) It is possible that some of the Luminati traffic is legitimate and involves checking whether advertisements are displayed properly. For a tiny fraction of the traffic, we have seen some evidence for that. However, for the vast majority of the traffic, we have not seen any evidence that mobile advertisements are being loaded through the Luminati proxy network as part of an internet browser session that would imitate a web browsing session of a normal user. Mobile advertisement platforms are potentially vulnerable to fraud, especially for ad impressions (advertisements that are being shown to users, for example, in mobile applications). The exit nodes of Luminati actually belong to residential internet users. How can advertisers see that traffic coming from millions of HolaVPN exit nodes to their sites is not human generated but bot generated? The answer is that it is virtually impossible. As the incentive for fraud with mobile advertisements is so big, it is highly possible that the Luminati network is being abused by cybercriminals for click fraud at a large scale.

To make our evidence stronger, we have compared traffic coming out of the Luminati network with traffic that is coming from known adware that has a large install base on Windows computers. There appears to be a remarkable overlap with traffic that is generated by adware of a company called Adrocks.bz.

**Comparison with Adrocks.bz**

As we have indicated earlier, the market for online advertisements is huge and is expected to grow to hundreds of billions of dollars annually in the coming years. Therefore it is to be expected that bad actors will try to get their share of this huge market. One way to generate traffic makes use of phone click farms. Tens of thousands of smartphones are put in a rack and are then used to click on advertisement links and to display advertisements. This is a labor-intensive way of click fraud. A more scalable method for bad actors would be to generate a lot of traffic to mobile advertisement links that is forged in such a way that it looks to be originating from real smartphones or tablets from all over the world. One example is the traffic that is generated by adware of a Japanese company called Adrocks.bz. We have looked at Adrocks.bz adware for Windows and we have found that more than 96 percent of all Adrock traffic from Windows computers forges the user agent to a mobile platform. This means that more than 96 percent of the Adrock traffic looks to be originating from a mobile device that is displaying an advertisement, while in reality those advertisements are loaded from a Windows computer with Adrock installed.

![Pie chart showing distribution of user agents](image)

*Figure 18. More than 96% of the user agents in the traffic of Microsoft Windows adware of Adrocks.bz is forged to a mobile platform*

This clearly indicates there is a huge market for potentially fraudulent mobile advertisements. It puts up to 86 percent of traffic that is sent through Luminati in a dubious light. Is this really legitimate traffic or is it fraudulent, duping mobile advertisement and mobile app companies?
There is substantial overlap between traffic that is sent through Luminati and the traffic that is sent from the Windows-based Adrocks adware. Both networks are sending traffic to a lot of domains that host mobile advertisements or track affiliates. In total, we counted more than 31,000 hostnames to which both the Luminati network and the adware of Adrocks are sending traffic.

**Comparison with Proxygate**

Apart from HolaVPN, there is a smaller-scale “community” VPN that offers proxies of “volunteers.” Users are encouraged to make their own computer available as an exit node by giving them access to more proxies when they donate their bandwidth. Proxygate has been installed by other malware and is unwanted and risky software at the least. We have monitored outgoing traffic of about 1,400 Windows computers with Proxygate installed. Proxygate forges the user agent of about 10 percent of traffic to a mobile device. There is a significant overlap with traffic coming out of Luminati as well.

![ProxyGate](image)

**Figure 19. Proxygate's website**

In the next few sections we will discuss other potentially abusive traffic coming out of the Luminati network.

**Scraping of online content**

A small but still significant part of Luminati’s traffic is related to scraping of data that is put online by various publishers. Normally, an organization that publishes data online doesn’t allow for scraping of all the contents from its website. Controls will be put in place to stop a third party to scrape data. These controls might include rate limiting of web requests from the same IP address or IP range, and asking users to solve captchas that would block automated requests. When these don’t help stop the abuse, IP addresses that do the crawling might be added to a blacklist. It is easy to block exit nodes of Tor, which are listed publicly; however, the proxy network of Luminati is very large and dynamic. Therefore, countermeasures against scraping are very difficult when a scraper uses Luminati. In fact, scraping is one of the use cases Luminati suggests on its website. At the very least, users who have installed HolaVPN are likely unaware that their internet bandwidth is being used for data scraping purposes.
We have seen clear evidence of scraping of online data via the Luminati proxy network. Among others, we have seen scraping of content from websites hosting classified advertisements, job and recruitment websites, online journals which specialize in a certain scientific field, newspaper websites, and business listings. We have also seen attempts to scrape data from websites that have information on medical doctors and attorneys. Even the official Interpol wanted list is being scraped via Luminati. However, the total percentage of scraping is low. We estimate it at about 0.6 percent of all traffic. However, that is still a very significant amount of web traffic as Luminati is routing dozens of millions of URLs per day.

<table>
<thead>
<tr>
<th>Online Publisher</th>
<th>% of Luminati Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backpage</td>
<td>0.17%</td>
</tr>
<tr>
<td>Job listings</td>
<td>0.05%</td>
</tr>
<tr>
<td>Online science journals</td>
<td>0.04%</td>
</tr>
<tr>
<td>Inmates / Interpol wanted list</td>
<td>0.02%</td>
</tr>
<tr>
<td>Business listings</td>
<td>0.02%</td>
</tr>
<tr>
<td>Craigslist</td>
<td>0.01%</td>
</tr>
</tbody>
</table>

Table 2. Breakdown of website content being scraped via Luminati network
Airline reservation systems

In one of his public talks, the President of Luminati, who is also the Hola Networks Ltd. CEO, showed just how Luminati can be used to spot different prices for the same plane ticket when ordered from different places in the world. As Luminati has many exit nodes around the world, the price differences of plane tickets could be researched using Luminati exit nodes. We indeed saw that about 1 percent of all Luminati traffic is related to airline reservation systems. Is this traffic really meant to spot consumer discrimination? And when consumer discrimination is detected, what comes next? We have seen Luminati traffic going to the reservation systems of more than 150 different airlines and four large central airline reservation systems. The distribution of the airlines that are affected is interesting: most big airlines are missing from the list or receive a small amount of traffic from the Luminati network. The ones that have their systems accessed via Luminati are mostly budget airlines around the world and several lesser known regional airlines.

As described earlier, we have explicit evidence that an Indian company active in the hospitality business has been using the Luminati proxy network manually. We noted that this company offers services in rate intelligence and price optimization for the travel and hospitality business. So part of the traffic to airline reservation companies could come from this company. However, that doesn’t explain all of the traffic we have seen. More than 1 percent of the traffic to airline reservation systems is actually for downloading boarding passes. Web check-in URLs of airlines are accessed, as well as other URL requests that contain family names and Passenger Name Records (PNR) codes. These go well beyond collecting intelligence on airfares. Apparently, there is an actor who is sending personal information of passengers through Luminati. This raises a big red flag.

Figure 21. Distribution of URLs loaded at reservation systems aggregated by country

As described earlier, we have explicit evidence that an Indian company active in the hospitality business has been using the Luminati proxy network manually. We noted that this company offers services in rate intelligence and price optimization for the travel and hospitality business. So part of the traffic to airline reservation companies could come from this company. However, that doesn’t explain all of the traffic we have seen. More than 1 percent of the traffic to airline reservation systems is actually for downloading boarding passes. Web check-in URLs of airlines are accessed, as well as other URL requests that contain family names and Passenger Name Records (PNR) codes. These go well beyond collecting intelligence on airfares. Apparently, there is an actor who is sending personal information of passengers through Luminati. This raises a big red flag.

---

Concert tickets and limited edition sports shoes

Concerts of popular artists are often sold out within minutes after tickets go on sale. There is money to be made by speculators here. One scheme consists of hoarding concert tickets of a popular artist and selling them later at a premium to individual buyers who were not able to buy a ticket earlier. There is one problem with this scheme though. Quickly buying large numbers of tickets from one IP address can be noticed and be blocked easily by a ticket vendor. A proxy network like Luminati, however, has millions of residential exit nodes and thus makes it possible to send bursts of ticket search and ticket purchase web requests through the proxy network. It may then appear as if the requests are coming from many different users around the world, when in fact they are coming from one automated script behind the Luminati network.

Indeed, we have seen substantial traffic to large ticket vendors’ websites that is being routed through the Luminati proxy network. About 0.4 percent of all Luminati traffic goes to major websites that sell tickets. There is substantial data scraping found on concerts, artists and resale offerings of tickets. We did not find explicit evidence for online purchasing of tickets through Luminati. However, we think that the substantial scraping of ticket data may be part of a larger scheme against ticket vendors.

We have seen explicit evidence that limited edition sports shoes are being purchased through Luminati. Other exclusive goods like bags, rare dolls and sportswear are probably bought via Luminati too. In the underground forum HackForums, one user says he in fact uses Luminati to buy shoes. Access to a residential proxy network might not be enough though to buy limited edition online goods in an automated way. Though bot traffic through Luminati is hard to distinguish from real human-generated traffic, some online stores will still require solving captchas in an attempt to filter out bot traffic. We saw that traffic that very much looks like purchases of shoes from online stores is regularly combined with requests to captcha-solving services. These online services either try to solve captchas with Optical Character Recognition (OCR) techniques or have sweatshops where human workers are solving the captchas manually.

![Figure 22. A post on HackForums where an actor says he uses Luminati to purchase limited edition shoes](image)

So we can deduce that these users of Luminati use multiple methods to evade bot detection by vendors of limited edition shoes and sportswear.
MobilePay

A limited but not entirely negligible part of all Luminati traffic is related to mobile payments, in particular, to a system that is called MobilePay. This is a system meant for small payments on a phone. Payments for online purchases will be directly charged to the owner’s phone bill. Though it is only meant for micropayments, this is a payment system some bad actors might try to take advantage of. From the Luminati data we have analyzed, it is clear that threat actors are trying to take advantage of the Italian version of MobilePay by loading mobile payment URLs via the Luminati proxy network. Other mobile payment systems are accessed through Luminati too.

Academic research

The proxy network of Luminati has been used a couple of times in academic research. One research studied how transparent the internet is. To this end, the researchers looked into DNS hijacking of domain names that cannot be resolved, HTTP content modification, SSL certificate replacement and content monitoring. It is understandable that academic researchers like to use a proxy network like Luminati. It is a tool that will give unique insights into how the internet looks like from different parts of the world. However, there are some important academic issues at stake. The researchers have explicitly discussed ethics of using Luminati in their paper. They have paid for access to the Luminati proxy network and that they were careful in abiding by the terms and conditions of Luminati. We think however that the scale of the residential proxy network of Luminati raises immediate and obvious red flags for security researchers. To what end was this proxy network created in the first place and what are the main objectives? The possibilities for abuse are immense, hard to resist and hard to block. One can be certain that a service like Luminati will attract a lot of bad actors and the risk is high for the users of HolaVPN. Researchers should consider these risks before choosing Luminati as a research tool.

Later the same researchers used the Luminati network again for a second paper on the DNSSEC ecosystem. In our dataset, we saw part of the measurements that were done by the academic researchers. We estimate it at about 0.1 percent to 0.2 percent of all Luminati traffic at the time the measurements were done.

Hackers using Luminati

A large residential proxy network like Luminati is a very powerful tool for cybercriminals. Therefore, it is no surprise that we have spotted traces of criminal use of Luminati during our research. For example, we have seen dozens of attempts to access the webmail server of a Malaysian company that is active in chemicals and industrial machinery. As far as we can tell, only Malaysian exit nodes were used during these attempted accesses of webmail that were spread over a period of more than six weeks.

---

We have seen the same for a marketing company based in Cyprus. During a period of about two weeks, the webmail of this company was accessed via exit nodes of Luminati in Cyprus only.

From at least December 2017 until March 2018, threat actors have been verifying a list of leaked credentials of mail.ru accounts using Luminati. Unauthorized access to webmail is illegal in most jurisdictions. This kind of traffic can bring users of HolaVPN whose computing devices are turned into Luminati exit nodes in a difficult legal position. They might be held responsible for the traffic that is coming from their exit points.

**Luminati in China**

Luminati has a site in Chinese, apparently aimed explicitly for Chinese users of the proxy service. We indeed have seen some scraping of Chinese services that are probably of interest to Chinese users of Luminati only. Here are some examples of scraping of Chinese services through Luminati:

<table>
<thead>
<tr>
<th>Description</th>
<th>% of Luminati Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website for credit information on companies</td>
<td>0.01%</td>
</tr>
<tr>
<td>Recruitment site</td>
<td>0.05%</td>
</tr>
<tr>
<td>Chinese judicial-related website</td>
<td>0.00003%</td>
</tr>
</tbody>
</table>

Table 3. Examples of Chinese services with domains scraped through Luminati

While the total amount of Luminati traffic to a Chinese judicial-related website is relatively small, it is big enough to trigger captchas from the site. We saw that whoever is using Luminati to query this site is also solving captchas for that site. These captchas are possibly being solved either manually or via a dedicated service that uses OCR techniques and sweatshops that solve captchas manually.

China has a lot of startups that are in the mobile application business and mobile advertisement business. It appears that dozens of these Chinese companies are potentially taken advantage of by an actor or a group of actors that pump traffic to the APIs and advertisement links of these mobile companies. About 22 percent of all Luminati traffic goes to the websites of these Chinese companies. An additional 5 percent of all Luminati traffic goes to websites of mobile app developers and mobile advertisement companies in Hong Kong.
Figure 23. Chinese version of Luminati at hxxps://luminati-china.io/

Note: The total amount of this traffic is almost 86 percent of everything that was routed through the Luminati proxy network from October 2017 to March 2018.

Figure 24. Distribution of Luminati traffic routed to domain names of affiliate programs for mobile advertisement companies and mobile app companies
Conclusion and Recommendations

In this paper we have carefully reviewed the HolaVPN software and made a detailed breakdown of all traffic that was being routed through Luminati from March 2017 until May 2018. We have a dataset of more than 100 million URLs that were sent through about 7,000 exit nodes.

We found that the HolaVPN software is not a secure VPN. Not only is traffic from users’ computers to the super nodes not encrypted, the users’ IP addresses are regularly exposed to the websites they visit. This makes HolaVPN an unsafe solution to circumvent censorship and interception of internet communications. The fact that HolaVPN installs other software that will make the users’ computing device into a Luminati exit node is particularly worrisome. It is known that Hola Networks Ltd. sells access to the residential exit nodes via its Luminati business. This is particularly risky for computing devices with HolaVPN installed that are used within a corporate network. The exit nodes give an attacker who has subscribed to the Luminati service the opportunity to do reconnaissance from within the corporate network. It is also possible to use subscription services from within an organization that has exit nodes that are based on the IP range. For example, academic journals that are freely accessible from within the university network.

The detailed breakdown of Luminati traffic shows that the vast majority of all Luminati traffic is likely related to fraud with mobile advertisements and traffic from mobile apps. We found concrete evidence for massive scraping of online content. This scraping often violates the terms and conditions of the target websites and may be illegal in some jurisdictions. We also have shown that hackers have found their way to Luminati.

All of this makes the HolaVPN software of high risk to our customers. By the time of this paper’s publishing, Trend Micro solutions will detect the HolaVPN software as unwanted software with detection names PUA_HOLA.SM1 and PUA_HOLA.SM2. We advise internet users to completely remove this software from HolaNetworks Ltd. from their computers.
Appendix

We made an explicit breakdown of more than 82 percent of the traffic that is routed through Luminati.

<table>
<thead>
<tr>
<th>Company</th>
<th>Country</th>
<th>% of Luminati Traffic</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile advertisements</td>
<td>Various</td>
<td>82%</td>
<td></td>
</tr>
<tr>
<td>Mobile advertisement company of former KlikVip actors</td>
<td>Ukraine</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>Various companies</td>
<td>Various</td>
<td>2%</td>
<td>IP checks</td>
</tr>
<tr>
<td>Luminati</td>
<td>Israel</td>
<td>1%</td>
<td>C&amp;C traffic</td>
</tr>
<tr>
<td>Airlines</td>
<td>Various</td>
<td>1%</td>
<td>Access to reservation systems</td>
</tr>
<tr>
<td>Anti-fraud companies</td>
<td>Various</td>
<td>0.5%</td>
<td>Companies that claim to be in the anti-fraud business</td>
</tr>
<tr>
<td>Online stores</td>
<td>Various</td>
<td>0.5%</td>
<td>Data scraping and purchases</td>
</tr>
<tr>
<td>Concert tickets vendors</td>
<td>Various</td>
<td>0.4%</td>
<td>Access to reservation systems</td>
</tr>
<tr>
<td>Travel websites</td>
<td>Various</td>
<td>0.3%</td>
<td>Access to reservation systems</td>
</tr>
<tr>
<td>Dating sites</td>
<td>U.S., Canada</td>
<td>0.2%</td>
<td>Data scraping</td>
</tr>
<tr>
<td>Anti-captcha services</td>
<td>Various</td>
<td>0.1%</td>
<td>Bot detection evasion</td>
</tr>
<tr>
<td>Academic research</td>
<td>U.S.</td>
<td>0.1%</td>
<td>Internet measurements</td>
</tr>
<tr>
<td>Online scientific journals</td>
<td>Various</td>
<td>0.04%</td>
<td>Data scraping</td>
</tr>
<tr>
<td>Inmates / Interpol wanted list</td>
<td>Various</td>
<td>0.02%</td>
<td>Data scraping</td>
</tr>
<tr>
<td>Whols domain lookups</td>
<td>Various</td>
<td>0.02%</td>
<td>Data scraping</td>
</tr>
<tr>
<td>Others</td>
<td>Various</td>
<td>8%</td>
<td></td>
</tr>
</tbody>
</table>

Table 4. Detailed breakdown of Luminati traffic
TREND MICRO™ RESEARCH
Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com