World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(4): 1-5
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Alem Kozar
Internacionalni Univerzitet Travnik, *Bunar bb* - Dolac Travnik, Bosnia and Herzegovina

Nikola Atlagić
ITEP, Banja Luka 78000, Bosnia and Herzegovina

Mladen Radivojević
ITEP, Banja Luka, Bosnia and Herzegovina

Correspondence:
Mladen Radivojević
ITEP, Banja Luka, Bosnia and Herzegovina

Using VPN service against hacker espionage

Alem Kozar, Nikola Atlagić, Mladen Radivojević

Abstract
Interest in the topic of identity protection on the Internet is constantly gaining in importance, with progressive growth of digital communication and application of the Internet as an information and communication technology in the modern age, the increasing censorship applied by the security agencies, governments of modern states, ISP companies (the legal obligation to retain data user activity), the company operates industrial espionage and marketing companies to determine the target market. There are a number of other organizations and individuals who are motivated diverse interests looking for information that essentially interfere with the privacy of individuals or companies. This paper analyzes the identity protection on the Internet using anonymous networks. By anonymous networks means access to a global network using VPN (Virtual Private Network), web proxy and an anonymous network against hacker espionage. The focus of analysis is on the topography and security to protect the identity provided by the Tor anonymous network.

Keywords: VPN, web proxy, hacker espionage, internet, identity protection

Introduction
In short, VPN, or Virtual Private Network is defined as an interconnection of local area network that uses secure encrypted ways of mutual communication, usually via the Internet. This means that the VPN extends a private network across the public network or over the internet and it allows users to send and receive sensitive information as die in their computers directly connected to the same private LAN, though, physically, they are not in the same network.

In other words VPN is a communication system that uses the infrastructure of the Internet for flexible and cost-effective data transfer between remote or virtual office, then employees through home computers connect to a private computer network. In addition to the Internet, for the realization of a VPN connection is possible to use different technologies and communication channels such as shared ATM networks, private networks and ISPs, and others.

So this kind of network such as a VPN can be defined more as a service that provides a secure Internet connection using a private network to some remote locations. What does that mean 'private remote locations'? When someone is using VPN, his computer connects directly to the first of a number of different computers around the world deceiving so trace the original computer and its location. In this way ensures a high security when surfing, with very little chance that the user some spying.

When using the local area network to access various services on the Internet, the source of network requests, our own local area network LAN. If we are connected to a VPN Esau our traffic passes through it, then the outside world to see part of the VPN Local Network.

Source said, not more than your network to which the user is connected via VPN. This means that the website and other networks with which we communicate no longer see the IP address of the user's computer as the source of the request, but the IP address of the VPN which the user uses.

Fig 1: Schematic representation of the functioning of a VPN

However, there is a catch: if you use a VPN server which is located in our country, which also uses the same ISP, then it is quite possible that the Internet provider can see our network traffic. However it will not able to conclude that our directly, since the origin of the traffic is not a VPN server on our computer.

Connecting to a VPN

Connecting to a VPN, he can be in several ways, but the general idea is that it should confirm the user's identity. The simplest way to establish the secure connection is logging directly to the server with a username and a password. There is also the possibility of installing a certain software that will allow us to create a secure connection. This program will perform encryption and data deskriptovanje And that usually requires a username and password to confirm their identity. In any case there is a possibility of use of other forms of authentication, such as tokens or smart cards and. The advantage of using tokens is činjenicada it is very difficult to hack And, since it is nearly impossible to steal a password. Also each token is unique, which means that the server will immediately recognize its users.

The advantages of using VPN

1. Movements between the user and the VPN is encrypted, so it's impossible for anyone to see what the user is doing on the internet.
2. As long as the user is connected to the VPN, will have access to the entire Internet without censure that could have an impact on users.
3. Can be accessed servers and geographically restricted websites, if users will be using a VPN server that is located in a region where these are available server or website.
4. Servers to which the user connects will see the user's IP address, but the address of the VPN server.
5. Possibility of surfing the Internet, reading e-mails or send important information to the public networks and without risk to anyone attempting to operate espionage

VPN servers

Fig 2: NordVPN

NordVPN are continually concerned about the anonymity of users and takes all that would have been no logs of users, their IP addresses or activities. In addition, not recorded any time or dates.

Also this server has a fantastic protection about which I care, or have their own infrastructure. Any user who "comes to the Internet" pass through two of their VPN server (at least 2 knots, if not more so), and used two layers of 256 bit encryption protection. You could also use a combination of Sun + VPN. This means that the connection is going through Nord VPN servers, and then another and through the Tor network, which guarantees virtually 100% protection.

Fig 3: Private Internet Access

Of additional protection have also:

1. kill switch - if it breaks the connection, not the nikakakv traffic redirect,
2. IPv6 leak protection,
3. DNS leak protection,
4. Shared IP System.

They have excellent custom applications for Windows, OS X (Mac OS), Linux, Android, iOS and coming soon Chrome extenzion! From protocol, users can choose among other things, VPN and IPSec. They have the local log works debugging problems, but these logs regularly destroy themselves.

Fig 4: ExpressVPN

Express VPN does not use traffic logs or logs that would possibly be able to connect user activity on the Internet and the time and date of the service. In addition, their entire VPN service based on shared IP addresses so we can not even clearly identify which user is using which IP address.

Fig 5: Anonymizer

Anonymizer is one of the few VPN service that still does not offer payment by Bitcoin, but it is planned for this year. On the other hand one can pay with any credit card. Not kept any specific data unless the user has paid VPN service.

Fig 6: TorGuard

TorGuard has its own custom applications for Windows, Mac, Linux and Android using OpenVPN. They also have application for iOS, but it uses IPSec as the Alps, is limited in this regard and does not allow the use of OpenVPN. All of these applications are not saved any logs on the local device.

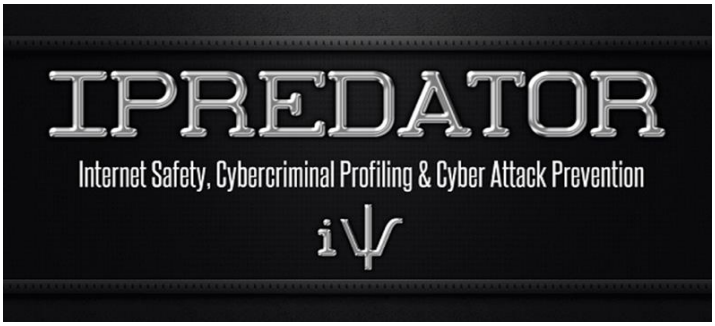

Fig 7: Ipredator

Ipredator contains no logs of users even at all possible to connect real IP address of the user and the time of service use. The only thing that is temporarily used the store IP addresses in a database until the connection is made. At this point is that data deleted from their database.
Doing business in Sweden and there are all of their servers.

Espionage through the Internet increasingly dangerous

Computer espionage directed to the state infrastructure will be the main threat on the Internet next year, rated followup manufacturing company McAfee antivirus software.

According to the study, computer crime will also jeopardize the on-line banking, and some governments and groups will use the Internet for cyber spying and for the execution of "cyber attacks".

According to the study, computer crime will also jeopardize the on-line banking, and some governments and groups will use the Internet for cyber spying and for the execution of "cyber attacks".

The objectives of the attack will be sensitive systems state of the network infrastructure, such as electrical networks, air traffic management systems, financial market and management of computer networks.

Using the Internet for Web espionage is present in about 120 countries.

From the initial individual attempted attacks have evolved into well-organized and well-financed activities aimed at the political, military, economic and technological espionage.

A new malicious programs are becoming increasingly resistant, and are constantly improved and contain highly regulated functions, for example in the field of encryption.

Nuwara worm was the first example of this type of hazardous codes and experts believe that the next year appear a number of similar.

It will also be largely occur attacks focused on calls via the Internet and the misuse of social networking sites MySpace, Facebook type. Frequent attacks aimed at banks can, according to experts, seriously undermine public confidence in the on-line banking and deter e-commerce.

You can not be totally anonymous on the internet?

After this some laws, information about what is being done on the internet providers can only be requested by the police through the courts of the state where the user or users find but again it is the legality of that lesser mortals know, there are laws that users do not know which is largely occur. The man who was part of such an apparatus which is followed all what is happening in the online waters, could no longer tolerate this violation of the right to privacy, and went public with the truth and evidence, what is working American agency NSA under the pretext of defense against terrorism . In short, the NSA, followed the boss of a company, the Prime Minister, an electrician from the distribution, the UN Secretary General, the Chancellor of Germany, a student from Sarajevo, who visit the sites, that information leave, have access to their e-mails, monitor what they are doing at social networks and the like, all under the pretext of defense against bad guys from Al Qaeda. Even if users are hidden behind a 100 proxy, VPN, firewall, TOR's again will there a site owner to know that you were at that and that page, watched it and it might succeed and that the user install a Trojan horse that will activate the user's laptop webcam or microphone and again have an insight into how that a user looks, that his tone of voice, what he says or what the story is in the room where the laptop, if someone calls you by name and they will know this information.

Even your own professional hackers can be hacked and that it does not know the same technique. Suppose Russian hacker was hacked by turning his camera by his knowledge at the same time his computer infected with a virus that he personally wrote.

In this work will be discussed how to reduce the exposure of users' privacy to a minimum and where lurking danger with a practical example and it does not mean that it should be locked in the bunker to set up around land mines to shut down everything that has power in itself, and only then make sure.

In short, all what is published on social networks, comment on other sites or Facebook, or comment on any site with a real name, mail that is sent to such and such, form or survey that was filled by the user here and there, tasks that the user has made on this and this forum, may be visible on the Internet, with all the physical location of a user if the same user is not behind the TOR, proxy-I or VPN. Each user reckless publication on social networks, comment on the site or the like can be a direct impact on user privacy.

Espionage world officials

The US National Security Agency (NSA) eavesdropped on more than 60 million phone calls in Spain between December 2012 and January 2013, said the Spanish newspaper El Mundo, the US ambassador to Madrid was summoned to the foreign ministry.

According to documents provided by the former analyst NSA Edward Snowden and that is passed on El Mundo, this agency has spied on 60.5 million phone calls in Spain between 10 December 2012 and 8 January 2013. The paper states that the NSA "is not recorded content calls, but the serial number, the place where they are located, phone number and the SIM card used and the duration of calls. "

US Ambassador James costoso was invited to give explanations of the alleged wiretapping Spanish officials which have been made public and followed after other revelations about US spying 35 world leaders.

After the discovery that Americans spy on the whole world and maybe even Angela Merkel, Germany and Brazil have begun work on the UN resolution on the protection of personal freedoms. Looking to the right of the individual and included a provision on the protection of privacy on the Internet. Both countries reacted angrily after it emerged that the information the spy Angela Merkel and Brazilian President Dilma Rousseff.

On the other hand the American eavesdropping cell phone of German Chancellor caused tension in transatlantic relations. President Obama had to give an explanation. But American experts were asked the question: Why so much excitement?

"A little eavesdrop, so what? So to summarize them briefly reactions in the United States after it was announced that the US National Security Agency NSA probably tapped and mobile phone Angela Merkel. The case reached the front pages only the few US newspapers. CNN quoted federal Chancellor to 'friends do not listen in' and that's it. "

Fifth Heokstra, who until 2007 headed the Committee for the secret services of the US Congress, also thought to be in Europe too much fuss unnecessarily. "I think that in the world of secret services means that we are good friends - the French, Germans, Israelis, Americans or come a time when each spy and that everyone can understand," said Hoekstra for Deutsche Welle, adding that European allies are spying in the US.

The importance of VPN in the system of protection

One of the biggest problems in the field of protection and security of computer networks and data are insufficient investment companies and institutions in serious protection mechanisms as well as a strong belief that the hacker

attacks will not happen just them. Statistics show that most of the decline in the company information system causes significant financial losses and to re-establish a working system requires additional investments and a specific time. On the other hand, labor mobility and centralization of applications and resources, then cloud computing and the expansion of M2M technologies have influenced the creation of all major security challenges.

Using VPN network brings benefits to both parties to telecom operators and users. Therefore, VPN network, an important part of the offer and a significant source of income for each telecom operators. As the simplest example of this network are intended as a VPN network mainly for legal entities (companies). This type of network involves linking mobile (in some cases fixed) ports in a group which is allocated to special benefits such as cheaper (or free) calls for cheaper mobile devices, a discount on the invoice and the like. Linking the connections of a company in Mobile VPN network resulting in reduced invoice that companies must pay. This often causes disbelief with the user, because they are offered services aimed at reducing their consumption. In view of the telecom operator, the terminal binding has advantages. One of the biggest advantages is that in this way they acquire a larger number of users, and thereby increase the revenues of telecom operators and to provide a proper place and role in the telecom market. In this way reduces the risk of losing market position. The presence of telecom operators in today's telecommunications market is growing as forcing telecom operators to fully orient towards the user, or put them in the focus of its business.

Conclusion

The problem of identity protection is multifaceted; is related to the information culture; habits of the individual; financial status. The challenge starts from the operating system (licensed or pirated versions), via servers that use a variety of purposes and the Internet sites you visit.

Virtual private networks, Web proxy services and Tor network certainly reduce the level of risk exposure of individual loss digital identity. Tor project there twelve years.

Third-generation applications offers the best protection. The advantage Tor network compared to other software anonymous networks is reflected in the onion routing traffic, which changes the hub method when listening to tea of choice, whenever url-ing new sites on the Internet. Additional safety is provided encoding and decoding of content on each node. The best results are achieved when all traffic under the SSL and TLS protocols, including access to the destination server on the public network.

Increasing the number of relays, which form the backbone of the private network, represents additional security for users. Relays are mostly owned by volunteers, who may use the same computer for other purposes and there is a shadow on exceptionally designed private network. The risk of attack with establishing control over a computer is very large.

Refences

1. Keith D. Watson, e Tor Network, "A Global Inquiry into the Legal Status of Anonymity Networks", 11 Wash. U. Glob. Stud. L. Rev. 715, 2012th.
2. P. Staletić, N. Staletić, "piracy of digital content on the Internet", XII International Scientific Symposium, Jahorina, 2013.
3. The hacker News, “Tor anonymizing network compromised by French researchers”, http://thehackernews. com/2011/10/tor-anonymizing-network-compromisedby.html, 3.februar 2014
4. http://mondo.rs/a83538/Mob-IT/Vesti/Spijunaza-preko-Interneta-sve-opasnija.html. 15. 3. 2017.
5. https://bs.wikipedia.org/wiki/ATM. 15. 3. 2017.
6. http://pcchip.hr/internet/sto-je-vpn-za-sto-se-koristi/ 16. 3. 2017.
7. http://www.pametnitelefoni.rs. 20. 3. 2017.
8. http://www.4dportal.com/hr. 22. 3. 2017.