Christos Beretas, MSc

http://www.christosberetas.com

chr.beretas@gmail.com

(+30) 693-890-9477

Greece

HONEYPOT PROJECTS ARE EVERYWHERE

Short Bio

I am holder of Bachelor and Master of Science degree in the field of Computer Systems from City University of Seattle, USA, also I am holding various certificates from other universities. My research areas are: **Cyber Security**, **Networks**, **Privacy**, **Software Development**, and **Social Media**. Also, I am active in the field of IT, telecommunications, and social media campaigns. I am involved in various research and other projects globally both in public and private sector, I am designed and developed various kind of software applications which are available globally and divided in 3 categories, (**1**) some of them are freeware, (**2**) some of them are for commercial purposes (organizations globally asked me to create that custom applications not available in public), and (**3**) some of my software applications are "honeypot" applications for different purposes for example for testing, feedback, evaluation, random projects, etc.

Abstract

The internet has helped considerably in improving the quality of human life, has helped release, a freedom of expression, opinion, creativity, the professional and personal relationships as well as the massive collection, storage and processing of information which is the result of all the above . There is the sense that when a user subscribes to an online service such as a dating site, although nowadays assure all online web sites that their users' personal information will not be forwarded to third parties and will only be available if requested legal by a court, often violated without the user's consent, it is true, is happened, it is not so simple and indifferent perhaps for some to listen especially if strictly involved private data.

Many scientists and researchers in recent years researching about the data collection program, processing and information storage with the distinguished name "**PRISM**" by **NSA** in the US. This program involves several companies to provide information to the **NSA** and the number of companies participating in the program is expected to increase ratio of the increasing demand of information and total control of Internet data traffic. I come as a researcher and say this is the icing on the cake. Why do I say this? There are organizations around the world which have established agreements with respective Internet web services to exchange information, such as IP address, your personal information registered for the online service, your country, your photos, even personal messages you exchanged with someone. There is a frightening your personal message addressed to a friendly face to leak and be read by a third party? And if the message contains personal information about the personal life of health, you can even think the size of the personal information breach? in fact they will have collected information that can create a full image of your self. You should not forget something very important, providing personal information to a third party, these

personal information are in the hands of others where we have not access and we do not know who is behind, whether to share to others, and if we delete them we will never know if they are deleted. You might think that someone surpasses by far even the **PRISM** and yet it is true and it happens for the following **cases**.

1. **Record user habits, perhaps targeted ads by country.**
2. **Targeted information gathering.**

Case 1: Personal information about what users are doing when visiting a website is recording the habits and preferences, then create a database for user habits even by the creator of the website or by transferring data in a third company for their further utilization. This technique is widely used today as a means of promoting products and this is the light loss of any personal information of the above two cases.

Case 2: Personal information recorded unbeknownst to the user, concerning personal information crucial for humans including personal messages, identifying locations and pretense person.

In this case, organizations and even state governments have initiated collaborations with several other companies, or by the people who provide Internet services to collect and share personal information. Many users believe that when they are registered in a web service their data will remain intact or that web service is low profile and no one will be interested to proceed to an agreement on exchange of information, this is wrong. The Internet is full of websites that collect such information and then transfer them to the companies partners or in governments, there are many smaller **PRISM** in this online world. The way to protect themselves is to follow the following rules:

- Do not use the same passwords that used in other services.
- Create an e-mail account that you will use in your online transactions, never use your regular e-mail account.
- Do not post pictures with private moments or with other people, a photo with your self is enough.
- When a web page asking for personal information, if is not official web site or web service, never entered your real personal information.
- Never respond to mails type to "**confirm your e-mail because it will be deleted**" that "**the inbox has been full with spam**", **etc**. **NEVER and NO ONE will ask you to verify your e-mail account or will ask you to login anywhere**.
- Do not indicated anywhere that is unofficial the number of your bank account, e-mail messages, for example, that "**you have won a huge amount of money**" and they are asking your personal information to give you that amount of money, **I'm sorry to say but you are not won** and instead if you give to them your personal information including your bank account they will create a "**Black Card**" and they will make transactions in your name.
- Be careful when you are connecting to websites that ask you to enter personal information usually the web address must starts with **HTTPS** for secure data transfer. Websites that invite you to enter personal information, but the web address begins with **HTTP** this means that the data transfer is done with unsafe manner and the data is transferred as **text** that is not secure.

- And remember always, opening an e-mail message is safe, but to open an attached file is **NOT** always safe.

References

Nemati, Hamid. 2010. **Security and Privacy Assurance in Advancing Technologies:** New Developments. IGI Global.

Eric Cole. 2011. **Network Security Bible**. John Wiley & Sons.