The Clarion Volume 9 Number 2 (2020) PP 61-64
The Clarion
International Multidisciplinary Journal
ISSN : 2277-1697

# The state of cyber security: the emerging threat trends.

**Laba Thakuria** and **Pranab Kumar Goswami**
Deputy Controller of Examination, Assam downtown university, Guwahati, India
Department of Engineering and Technology, Assam downtown University, Guwahati, India

## Abstract

Computer Security has become a major challenge in the present years due to the continuous global technological development and the different possibilities for the use of computer. Cyber threats are growing at an alarming rate and at the same pace with the online use of Personal Computers and mobile devices. This work surveys the state of Cyber Security emerging threats landscape, through the overview of related works reported between the various years in the literature by stakeholders and experts in Information Technology (IT) industry. Different type of Cyber emerging threats such as malicious attack, network attack and network abuse have been identified with specific interest on virus, Phishing, Spam and insider abuse to mention but a few. It has been established that these Cybercriminals tools are exhibiting common level of sophistication and advancement as the advances in Computer and mobile technologies. The available countermeasures are found to be satisfactorily effective, yet Cyber criminals are creating new measures to overcome Security mechanism. It is also envisaged that as the technologies advances, a resultant proliferation of cyber threats will be witnessed. Thus, a few government and Information Technology (IT) stakeholders' strategic policies to help in combating cyber threats were presented.

**Keywords**: Cybercrime; Attack; Deep fakes;Cloud jacking; Threat; Malware; phishing.

## 1. Introduction

The perceived benefits of Computer technology were affected greatly by the increasing concern with internet crime today. This truly presents a major challenge to Security of the internet world. Cyber Security can essentially be defined 'as the body of technologies, practice with coordinated series of actions, designed to defend Networks, Computers, System Application Programs and data from an Attack, Damage or Unauthorized Access'. Cyber Security experts classified Cyber Emerging threats as malicious attacks, network attacks, and network abuse. Malicious attack is any effort to exploit another person computer and infect the system resources through Virus, Trojan horses, Spyware etc. Network attacks are intended actions meant to damage or disturb data information flow of the Computer System on a Network Service account, which causes effects such as Denial of Service (Dos), Session Hijacking, Email Spoofing et. Network abuse is fundamentally an exploit to the point of interaction of a network, and it could be utilized by actions such as spam, phishing, pharming etc.

Cyber-attacks are widely, viewed as criminal action led by means of the Web. These exploits can incorporate taking an Organization's intelligent property, seizing online bank accounts, designing and circulating Viruses on different Computers, posting secret Business Data on the Web and destroy a nation's basic national Infrastructure. Internet threats are seen as the highest failure to business and revenue loses of all Organizations. As put on by Tatum, Cyber Attack can be defined as…"An attempt to undermine or compromise the function of a Computer-based system, or attempt to track the online movements of individuals without their permission; Attacks of this type may be undetectable to the end user... or lead to such a total disruption of the network that none of the users can perform even the most rudimentary of tasks" (Canty, D., 2012 ). This definition clearly described the manifestation of how serious of the problem with Cyber Attacks, and because of the increasing sophistication of these kinds of network attacks, a research by

Corresponding author : pranab.pkg08@gmail.com
**DOI number:** 10.5958/2277-937X.2020.00016.7

International Telecommunications Union (ITU) reveals an estimated survey report of about $1trillion was lost to Cyber related frauds globally in 2012, out of which $390billion was accounted for justification. The initial phase of this research will encompass an extensive literature review on the increasing sophistication and maliciousness of Cyber Security emerging threats that create unique challenges to federal information systems and government wide cyber security efforts. The review will critically discusses the current state and future forecast of States of cyber Security, the existence of internet threats landscape in administering government agencies. It will also put down some recommendations needed to combat the threats. An administrative and IT Stakeholder's Policies which if completely executed will work find in the fight against internet crime. These policies were recommended as a tool in fighting against the current and future risen cases of Cyber related crime.

## 2. Research methodology

The data for this research were derived from secondary sources: previous researches and analyses of scholars; books, Journals, Conference proceedings, white papers and Government publications on cyber security that are related to the current trend of cyber emerging threats. As the study involved an extensive literature review which critically analysed the present state of cyber security: emerging threats landscape. It lays down the policy to enhance cyber-Security and the critical steps to acquiring the know-how on how to deal with the emerging cyber threats; and the content analysis approach was utilized for analysis.

## 3. Developments

The two perspectiveof developments in threats landscape can be viewed as follows:

**Negatives developments**

• Development of Cyber criminal's activities has grown maturely focusing mostly on Government and Private Commercial Institutions.

• Cyber-crime goes Mobile: Cyber criminals are now experts in social engineering with attack patterns and tools targeting and compromising our mobile devices.

• The two emerging digital battle fields: big data and the internet of things a concern to Cloud Storage Security services.

**Positive developments**

• Law enforcement agent had succeeded in binding up a strong international Cyber policy as this led to the arrest of gang responsible for the spread of Police Virus.

• Because of the risen cases of Cyber-crime threat analysis was encouraged and this provides valuable information to Cyber experts. (Gerke M., (2012)

• Vendors had now constantly updates there products forsecurity patches.

• Cooperation among organisations was achieved all in an effort to fight Cyber-crime

## 4. Cyber threat trends: 15 cyber security threats for 2020

Here's a short glossary of terms and trends that could pose cyber security threats in 2020, and how they might impact businesses, governments, and individuals in the coming year and beyond.

**Deepfakes**

Deepfakes is a combination of the words "deep learning" and "fake." Deepfakes happen when artificial intelligence technology creates fake images and sounds that appear real. A deepfake might create a video in which a politician's words are manipulated, making it appear that political leader said something they never did. Other deepfakes superimpose the face of popular actors or other celebrities onto other people's bodies. (Kosutic, D 2007)

**Deepfake voice technology**

This technology allows people to spoof the voices of other people — often politicians, celebrities or CEOs — using artificial intelligence.

**AI-powered cyber attacks**

Using artificial intelligence, hackers are able to create programs that mimic known human behaviours. These hackers can then use these programs to trick people into giving up their personal or financial information.

**Synthetic identities**

Synthetic identities are a form of identity fraud in which scammers use a mix of real and fabricated credentials to create the illusion of a real person. For instance, a criminal might create a synthetic identity that includes a legitimate physical address. (Kruger,R.C.(2008). The Social Security number and birthdate associated with that address, though, might not be legitimate.

**Hackers attacking AI while it's still learning**

Artificial Intelligence evolves. It's most vulnerable to cyber-attacks, though, when it's learning a new model or system. In these attacks, known as poisoning attacks, cybercriminals can inject bad data into an AI

program. This bad data can then cause the AI system to learn something it's not supposed to.An example? Some cybercriminals have used poisoning attacks on AI systems to get around spam detectors.

**Disinformation in social media**

As we have probably heard the term "fake news." This is also known as disinformation, the deliberate spreading of news stories and information that is inaccurate and designed to persuade people — often voters — to take certain actions or hold specific beliefs. Social disinformation is often spread through social media such as Facebook and Twitter. "Fake news" became a hot topic during and after the 2016 presidential election. (Marinos, L., and Sfakianakis A., (2012)

**New cyber security challenges that 5G creates**

Tech experts worry that 5G will create additional cybersecurity challenges for businesses and governments. A 2019 study by Information Risk Management, titled Risky Business, said that survey respondents worried that 5G technology will result in a greater risk of cyberattacks on Internet of Things (IoT) networks. They also cited a lack of security in 5G hardware and firmware as a worry.

**Advances in quantum computers pose a threat to cryptographic systems**

The idea of quantum computing is still new, but at its most basic, this is a type of computing that can use certain elements of quantum mechanics. What's important for cyber security is that these computers are fast and powerful. The threat is that quantum computers can decipher cryptographic codes that would take traditional computers far longer to crack — if they ever could.

**Vehicle cyber attacks**

As more cars and trucks are connected to the Internet, the threat of vehicle-based cyber-attacksrises. The worry is that cybercriminals will be able to access vehicles to steal personal data, track the location or driving history of these vehicles, or even disable or take over safety functions.

**Cloud jacking**

Cloud jacking is a form of cyberattack in which hackers infiltrate the programs and systems of businesses, stored in the cloud, and use these resources to mine for crypto currency.

**Election security**

The U.S. government fears that hackers from other countries might target the voter-registration databases for state and local governments, with the intent to either destroy or disrupt this information. This could prevent people from being able to vote. The U.S. government, then, has boosted efforts to protect this election information from criminals. (Tatum, Malcolm (2010).

**Cyber-attacks against less-developed nations**

The residents of developing nations might be more vulnerable to cyber-attacks. People in these countries often conduct financial transactions over unsecured mobile phone lines, making them more vulnerable to attacks.

**Ransom ware attacks on the public sector** In a ransom ware attack, hackers access the computer systems of an end user, usually freezing them. These attackers will only unlock the infected systems if the victim pays a ransom. Hackers today often target the computer systems of government bodies, including municipalities, public utilities, and fire and police departments, hijacking their computer systems until these government agencies pay a ransom. (Ponemon, (2012)

**Data privacy**

Companies, medical providers and government agencies store a large amount of important data, everything from the Social Security numbers of patients to the bank account numbers of customers. Data privacy refers to a branch of security focused on how to protect this information and keep it away from hackers and cybercriminals.

**Breaches in hospitals and medical networks**

Hospitals and other medical providers are prime targets for cybercriminals. That's because these medical providers have access to the personal and financial information of so many patients. Data breaches can expose this information, which hackers can then sell on the dark web.

## 5. Conclusion

This paper has outlined the reasons for widespread of different types of threats thereby affecting the states of Cyber security. The aim of this survey is to assess and evaluate the state of Cyber security emerging threats and the best approach needed to mitigate Cyber security breaches. The accompanying conclusions might be drawn from the present study that shows governments and large cooperation all over the world should be wary of the growing danger of cybercrime in the near future. This study has reported and envisaged a dramatic increase in the amount of targeted attacks on institutions and

large government cooperation around the globe. This is based on the prediction that Cybercriminals tactics in the near future is focused to be more complicated and difficult to prevent, detect and address compared to the current known ones. However companies and state organizations at the moment are influenced by the principal attacks, because today the more Security is reactive the more Cybercriminals are keen in exploiting that weakness. As the uses of mobile devices continue to grow, the volume of attacks targeted to these devices will grow proportionately. (Justin, M. Rao (2011). The dynamic race between defenders and attacker has continued and the projection is that it will continue even far spreading beyond western Europe and the US and actually affecting Eastern Europe, the middle East and Africa. Having a better understanding of how cybercrime affects our businesses will play a greater role in addressing it; we need to know who it targets how and why? Who are the perpetrators and how much harm are they causing. Taken together, these findings suggest a role for the government take absolute countermeasures against Security threats. Unless governments adopt this measure to mitigate threats, security threats will continue to manifest unabated.

***References***

A New Circular Vision for Electronics Time for a Global Reboot. 2019. World Economic Forum.

Canty, D., 2012. Digital Danger Zone: tackling cyber security.Arabian Oil and Gas, [online] 19 January. Available at < http://www.arabianoilandgas.com/article-9868-digitaldanger-zone-tackling-cyber-security/4/ > [accessed 28 December 2013].

Gerke M., (2012) Understanding cybercrime: Phenomena, Challenges and legal response ITU Telecommunication Sector Sept, 2012. Is a new edition of a report previously entitled Publication Understanding Cybercrime: A Guide for Developing Countries? Online available at: www.itu. int/ITU-D/cyb/cybersecurity/legislation.html.

Justin, M. Rao (2011) the economics of spam email metric MAAWG report Microsoft research. Available at: http://www.maawg.org/system/_les/news/MAAWG 2013.

Kosutic, D 2007, what is Cybersecurity and how can iso 271001 help? Blog. Accessed 25 January 2014 <http:/ /blog.iso27001standard.com/2011/10/25/what-is-cybersecurityand-how-can-iso-27001-help/#.

Kruger, R. C. (2008). Investigating the possible introduction of managed broadband internet security: a pilot study (Doctoral dissertation, Stellenbosch: Stellenbosch University).

Marinos, L., and Sfakianakis A., (2012) ENISA Threat landscape responding to the Evolving Threat Environment. Report by European network and Information Security Agency, September, 2012 Available at: http://www.enisa. europa.eu

Ponemon, (2012) Cost of Cyber Crime Study: United Kingdom benchmark Study of UK Organisations, PonemonIntstitute Research Report October, 2012

Tatum, Malcolm (2010) "What Is a Cyber-attack?"Available on-line from: http://www.wisegeek.com/what-isa-cyberattack.htm (Accessed 29th January, 2014).

□□□