Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (93-95), Month: January-April 2016, Available at: www.noveltyjournals.com

Emerging Trends and Techniques: An Explorative Study of Novel Approaches Adopted by Cybercriminals to Commit Cybercrime

Dr. P.B. Pathak

Assistant Professor & Head, Department of Computer Science & Information Technology Yeshwant Mahavidyalaya
Nanded, Maharashtra, India

Abstract: **Cybercrime is spreading all over the globe very rapidly. Cybercriminals are increasingly inventing innovative ways of committing Cybercrime. The worldwide trend of certain types of Cybercrimes is much ahead other due extensive amount money they generate. The Cyberdefence need to be more perfect attempting to eliminate all sorts of vulnerabilities by adopting a risk based approach. Cyberattacks are real; they potentially impacts and so nobody can ignore increasing threat of Cyberattacks. The current research paper discusses some of the leading and severe Cybercrimes.**

Keywords: **Cyberattacks, Cybercrime, Cyberdefence, Espionage, Healthcare, Ransomware, Spam.**

I. INTRODUCTION

Cybercrime is growing very fast encompassing almost every sector of all walks of our life. Increasing number of Cybercriminals are exploiting the Internet’s features like anonymity, speed and ease to commit diverse and borderless crimes, causing serious damage and posing realistic threats to global victims. Though Cybercrime cannot be defined specifically and comprehensively; still it is sophisticated attacks against computer hardware/software and crimes against children, crimes against financial institutions, Cyberterrorism using Internet. Earlier Cybercrimes ware committed unorganized way mainly by individuals or small groups nowadays, we experience organized, highly expert cybercriminals connected globally and on very large scale.

Cybercrime ever is on the rise and for sure is here to stay. Most of the nations have ranked Cybercrime as their top national security threat. The tools in the arsenal of global Cybercriminals include Cyberattacks-Espionage-Disrupting Critical Infrastructure, Smart Spam-Release of Confidential Information, Ransomware- Holding and Destruction of Data. Stealing Data of Healthcare Companies These types of Cybercrimes are dominating the globe. [1,2]

II. CYBERATTACKS: ESPIONAGE AND DISRUPTING CRITICAL INFRASTRUCTURE SYSTEMS

The risks from Cyberattacks become increasingly daunting due to transformation of traditional data keeping practice either business or personal, in to digital form on open and globally interconnected technology platforms. A Cyberattacks is deliberate exploitation of victims Cyberinfrastructure and data. Cyberattacks use malware to modify computer program, logic or data, resulting in disruptive consequences that can compromise confidential data and lead to cybercrimes. [3]

Espionage is unauthorized spying using computer by deployment of viruses that secretly observe or destroy data in the computer systems of government agencies and large enterprises. Espionage is the practice of spying on computers to obtain information about the plans and activities of a competing company. Espionage describes the stealing of secrets stored in digital formats or on computers and computer networks.[4]

Critical Infrastructure Systems (CIS) refers to processes, systems, facilities, technologies, computer networks, assets and services essential to the health, safety, security or economic well-being of citizens of the nation. CIS can be interconnected or stand alone and interdependent of provinces, territories and national borders. CISs are easier to target. Disruptions of CIS could result in disastrous loss of life, adverse economic effects and significant harm to public confidence. [5]

III. SMART SPAM: RELEASE OF CONFIDENTIAL INFORMATION

Spam is pouring in the Internet with multiple copies of the unwanted commercial email messages, in an attempt to deliver the message to the people not intended to receive it and can be very annoying for them. Mostly spam is commercial advertising of questionable products, bogus schemes, or false and fraud services possibly may cost considerable time and huge money. Spam costs multifold to the receiver than sender. Vulnerability for targeted attacks to steal our passwords and data comes from the fact that we share and shop more online to let more selective opportunities to target us. Cybercriminals enhancing their game are perfecting their campaign abilities, is a rising trend. These kinds of attacks have grown significantly over the past several years.

Advanced Persistent Threats (APTs) with features selection of right target, silence and duration of attack i.e. stay unnoticed for longer periods of time, may also be called Sophisticated Spam, and are increasing quite rapidly by exploring social engineering techniques. The modality of this crime is to incite victims to reveal their confidential information or perform some undesirable actions. The victims of these attacks range from large firms to individuals. [6,7]

IV. STEALING DATA: HEALTHCARE COMPANIES

The growing no. of breaches to Health Information and other sensitive data via electronic medical records and the growing popularity technology holding the health information makes the healthcare industry a vulnerable and attractive target for cybercriminals. The healthcare industry is a prime target for cybercriminals.

Rampant attacks on financial institutions like banks are common but Cybercriminals are increasingly attacking healthcare companies. These attacks never comes to public knowledge due to confidentiality reasons is more alarming. Cybercriminals tend to go after bigger targets which can generate more gain for them. Healthcare data are valuable because medical records can be used to commit several types of fraudulent activities or identity theft. Since Patient records now in digital form, healthcare company’s biggest security challenge is keeping personally identifiable information from falling through security cracks and into the hands of hackers.

Healthcare industry is a potential target for data hungry hackers to steal Electronic Health Records of individual’s containing personal health information like address, private medical records to credit card information. These records are used for identity theft. The healthcare industry breaches are increasing because of numerous weak links in healthcare industry systems. Healthcare organizations do not perform encryption of records and encryption of data at rest and transit. Once the Cybercriminals get their hands on Health insurance information, it’s difficult for the victim to do anything to protect them. [8,9]

V. RANSOMWARE: HOLDING INFORMATION RANSOM AND DATA DESTRUCTION

Ransomware is a type of malware that prevents or limits legitimate users from accessing their computer system. The malware forces its victims to pay the ransom in order to get access to their computer systems, or to get their data back. No guarantee that even paying for the ransom users can surely be able to access the infected system. Ransomware stops you from using your own computer, holds your computer or files for ransom and they will all ask you to do something before you can use your computer.

Ransomware is the most common forms of malware. Victims remain with no option but to can do anything to free up their locked information systems or to prevent their sensitive information like personal photos, documents, and other material, from being leaked in the public. Cryptolocker is mechanism used by Cybercriminals accuse them to do various unpleasant crimes or extorts money from victims, in which they encrypts people's important files and then demands money in order to unencrypt them.[10,11]

VI. CONCLUSION

Cyberattacks-Espionage-Disrupting Critical Infrastructure, Smart Spam-Release of Confidential Information, Ransomware- Holding and Destruction of Data, Stealing Data of Healthcare Companies are only the most important emerging and big trend worldwide adopted by Cybercriminals. The increasing use of mobile, smartphone's, tablets for online transactions using malware has also increased the vulnerabilities to a great extent.

Personal data of individual is of high importance and high valued so that no one can afford these attack. There is a Firm and growing identification that Cybercrime is perfect professional and organized crime. In the wake of increased Cybercriminal activities, there is an urgent need of continued and increased Cyberdefence attention i.e. disruption of Cybercrime infrastructures by individuals, companies and organizations all over the globe to combat cyber crime.

REFERENCES

[1] Mc Quade, Samuel C., "Understanding and Managing Cybercrime", Pearson Education, Incorporation, (2010)

[2] "Organized Crime Situation Report: Focus on the Threat of Cybercrime." Council of Europe Octopus Program, (2014), http://www.coe.int

[3] R. Clarke, R. Knake, "Cyber War", New York, NY: Harper Collins, (2010)

[4] David Talbot, "Cyber-Espionage Nightmare", (2015), https://www.technologyreview.com/s/538201/cyber-espionage-nightmare/

[5] Elias Kyriakides, Marios Polycarpou "Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems", Springer,(2014)

[6] Feinstein K., "How to do everything to fight spam, viruses, pop-ups & Spyware", McGraw-Hill/Osborne, California, (2014)

[7] Rebecca Herold, Christine Hertzog, "Data Privacy for the Smart Grid", CRC Press, (2015)

[8] Thomson Reuters ,"Combating Cybercrime in the Healthcare Industry", (2015), www.cisco.com/c/dam/en/us/products/.../cybercrime-healthcare.pdf

[9] Susan W. Brenner, "Cybercrime: Criminal Threats from Cyberspace", ABC-CLIO, (2010)

[10] S. Schjolberg, S. Ghernaouti-Helie, "A Global Treaty on Cybersecurity and Cybercrime", 2nd ed. AiTOslo, (2011)

[11] "Ransomware: Malware that kidnaps your data to extort money from you", (2014), White Paper, www.invincea.com/wp.../Invincea_Ransomware_whitepaper_061614.pdf