International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET207443

Predicting and Analysis of Phishing Attacks and Breaches In E-Commerce Websites

N. Ram Mohan[1], N. Praveen Kumar[2]
[1]M. Tech Scholar Department of CSE, NRI Institute of Technology Visadala (V&M), Guntur(Dt), Andhra Pradesh, India
[2]Assistant Professor Department of CSE, NRI Institute of Technology Visadala (V&M), Guntur(Dt), Andhra Pradesh, India

Article Info
Volume 7 Issue 4
Page Number : 170-175
Publication Issue :
July-August-2020

Article History
Accepted : 01 Aug 2020
Published : 05 Aug 2020

ABSTRACT

Analyzing cyber incident data sets is an important method for deepening our understanding of the evolution of the threat situation. This is a relatively new research topic, and many studies remain to be done. In this paper, I reported a statistical analysis of a breach incident data set corresponding to 12 years (2005–2017) of cyber hacking activities that include malware attacks. I shown that, in contrast to the findings reported in the literature, both hacking breach incident inter-arrival times and breach sizes should be modeled by stochastic processes, rather than by distributions because they exhibit autocorrelations. Then, I proposed a particular stochastic process models to, respectively, fit the inter-arrival times and the breach sizes. I also shown that these models can predict the inter-arrival times and the breach sizes. In order to get deeper insights into the evolution of hacking breach incidents, we conduct both qualitative and quantitative trend analyses on the data set. I drew a set of cyber security insights, including that the threat of cyber hacks is indeed getting worse in terms of their frequency, but not in terms of the magnitude of their damage.

Keywords: Hacking, Cyber-Attacks, Cyber Threats, Breach Prediction, Times Series, Cybersecurity Data Analytics.

I. INTRODUCTION

Data breaching is an act of disseminating the highly sensitive data which are intended to be kept secret. Disclosing the data to the unsecured domain either with a motive or unintentionally. It occurs when the third-party or an unauthorized individual tries to steal or access the data which may comprises of top secrets, company shares, transaction details or legal information. There are different types of data breaching which includes phishing, denial of service attack, malware and exfiltration. From time to time we hear about several companies and industries announcing that their systems have been breached. This might happen by illegal action of the intruders.

Or also by an individual within the organization. They might even belong to an organized group of criminals whose main target is money. This is known as cyber attack and those who perform such illegitimate practices are known as cyber criminals. Overcoming this situation is not an easy task. But, several steps of prevention towards data security can be followed. Maintenance of data can be improved by adopting to new technologies. There are several threats and consequences in data breaching. Cyber Threat Management can be taken into consideration.

II. RELATED WORK

The nature of the system breaches and the attacks on the system affects the state of operation and working of the system. A system may incur active or passive attack which makes the whole system collapse. When a system is attacked, the data security is breached and all the information contained in the system are hacked or obtained by the hacker in the successful attack. When a system is under attack and if the access to the system is granted, all the potential information will be lost or damaged depending on the intention of the attacker

System States & Cyber-attacks:

In order to know the details of the current state of the system, the changes that are made by the cyber attacks must be analysed and the ways in which system has experienced the attack with respective to the changes to the operating system. The purpose and intention of the attacker is to intrude into the system and gain unauthorized access to the system or the information and the resources contained in the system under attack. A malicious code will be sent to the system without the knowledge of the system's owner which can be able to write or transmit the data from the system to the attacker's system through which he can exploit its resources.

Contemporary Attacks:

These types of attacks are carried out in order to gain elevated or higher access privileges. Through the cotemporary attacks, the attacker can gain administrative privileges of the system under attack. Any modification, changes that are intended by the attacker can be carried out at once he has access to the administrative privileges of the system. The third type of the cotemporary attack can make the system in operable and isolate the system by flooding the information and data contained in the system .This will make the system unresponsive the administrative privileges. The system will respond to the attacker rather than the owner of the system

Determining the breach probability:

By comparing the statistics of the attacks in the past on the system and similar type of attacks across the world and the respective models are taken into account for determining the probability of the attacks across the system .Analyzing the breach probability is an important objective for the system security and protection. It analyses the attacks that succeeded inspite of the different counter measures taken by the system administrator and it assess the risks and threats that are posed by the cyber attacks. If the counter measures are involved during the cyber attack then the overall breach probability will be able to compute the breach probability.

Determining the Access Matrix :

We can identify the nature of the access granted to the system to an attacker by listing the attack matrix and the access matrix is determined by coupling with the task of the attack matrix. The privileges that are granted to the attacker are enlisted in the form of matrix and the different types of attacks that are made to breach the security of the system and the combination of the modality is listed in the access matrix. Advanced Persistent Threat An attack in a

network in which a person extracts a network and access important and highly confidential information rather than doing any actual damage to the network or an organization.

III. SECURITY ISSUES

Due to these various breaches and cyber attacks that take place in various systems this has led to a significant financial loss as these hackers stole account information and breach security to relocate money to their account. These threats can range from small losses to an entire information loss. These threats can affect at various levels also like some affect confidentiality of data and others affect the entire system. There are various types of attackers that attack in different methods.
Some such attackers are briefed below.

Bot-network Operators:

Bot-network operators are hackers that penetrate into the networks. They do so to take over multiple systems. Like this the whole organisation can be brought down and malicious attacks can be executed. These network services are made available to shady markets and hence can be misused.

Criminal Groups

These group of people or hackers attack the systems for getting financial profits. Different groups use various ways tod a malicious attack and acquire all the confidential information to commit identity theft and online fraud.

Hackers:

These group of people breach into systems to challenge or for bragging rights. This requires a good skill or computer knowledge to breach into the systems or securities. They pose a high threat causing massive damage world-wide. Once they understand the algorithm to crack the security of any site then they can do anything they want to the system.

Insiders:

These are the people who are already working inside the organisation. They have all the liberty to access to the system, hence they can easily understand the system and can use it for their own use. They can steal crucial information. The insider threat also includes outsourcing of data and inception of malware into systems.

Phishers:

Phishers are groups that use the phishing scheme so that they can steal information for own financial profit. They may also introduce divers' ways as spam in pursuance of their objectives.

IV. GLOBAL MARKET ANALYSIS

Crime	Annual Revenues
Illegal online markets	$860 Billion
Trade secret, IP theft	$500 Billion
Data Trading	$160 Billion
Crime-ware	$1.6 Billion
Ransomware	$1 Billion
Total cybercrime Revenues	$1.5 Trillion

As shown in the above figure firstly an event (such as establishment of network connection occurs) then a set of these events are passed through the analyzer. The analyzer then uses the system information and the specified detection policy to analyze the event, on the basis of this analysis a response is generated via response module which uses response policy to generate the response. In case a potential threat is detected the system alerts the user by notifying them saying threats found.

V. CYBER SECURITY

Cyber security provides prevention of data spill. As we all know, it is always better to prevent than to cure. Since the number of data breach is rapidly increasing as the years pass by, preventing data breaches has become the need of the hour. To eliminate the threats of data breaching, we have many cyber security techniques. These Cyber security techniques play
a vital role in the prevention of data breaches.

Some of the most common ways of preventing data breaches are as follows:-

a) **Reduce transfer of data**: It would be better to ban the migration of data from one device to another in an organization since loss of removable media will put the data under risk.

b) **Shred files**: Shredding files, folders and disks involves deleting the selected data files permanently without leaving a copy of the file. Hence shredding of the confidential data prevents data breaches.

c) **Banning of unencrypted devices**: The unencrypted devices are more prone to data leakage. So, it is important to ensure that all the unencrypted portable devices used in an organization are banned.

d) **An erratic password**: It is vital to set a password that is hard to crack and unpredictable in order to prevent illegal access of data. Also, it is preferable to change the passwords at regular intervals.

e) **Automate security**: Automated systems may be employed for checking the password settings, server and firewall configuration which helps in reducing the risk of data breaching.

f) **Restrict download**: Imposing restrictions on downloading of the confidential data reduces the chances of transferring data to an external device.

g) **Protect information**: The sensitive information should be protected wherever it is used. The personal information should not be revealed unwittingly.

h) **Breach response**: Setting up a breach response plan will help in sending alerts to the management in case of data breaches by notifying them about the attacks and thereby reduce the risk of data breaches.

VI. CYBER THREAT MANAGEMENT

CYBER SECURITY TOOLS

Contrast Security:

It provides security for the applications. To prevent false forging, the agents of contrast security are embedded into the application program which becomes a part of the program. It has undergone over 2000 tests without generating any data breaching on OWASP security standards. All the normal apps are converted into an application which are destined on security.

Crossbow:

Crossbow security provides vulnerability testing and platform for assessment. It is the most defensive program against frangibility. Historical attacks can be deployed for any vulnerability by exposing it to a secured network.

Red Seal:

Red seal is used to manage the firewall complications. A firewall is a system which ceases the merge of assured network and unsecured network. All the network elements hand-over their statistics to the Red Seal. Mapping of all the possible incoming and outgoing trackway. It is an extension of normal mapping, made possible by Red Seal.

VII.CONCLUSION

We analyzed a hacking breach dataset from the points of view of the incidents inter-arrival time and the breach size, and showed that they both should be modeled by stochastic processes rather than distributions. The statistical models developed in this paper show satisfactory fitting and prediction accuracies. In particular, we propose using a copula-based approach to predict the joint probability that an incident with a certain magnitude of breach size will occur during a future period of time. Statistical tests show that the methodologies proposed in this paper are better than those which are presented in the literature, because the latter ignored both the temporal correlations and the dependence between the incidents inter-arrival times and the breach sizes. We conducted qualitative and quantitative analyses to draw further insights. We drew a set of cybersecurity insights, including that the threat of cyber hacking breach incidents is indeed getting worse in terms of their frequency, but not the magnitude of their damage.

VIII. FUTURE SCOPE

The internet is not safe without the proper knowledge of it's working. The study on cyber hacking breaches and various attacks helps the server to maintain the quality of the service provided to the customers. It will also make sure that the data on a server or on a PC is safe. The sooner the breach is detected; we can cease further damage to the data or we can avoid data compromising. The frequency of the attack can be derived from the inter arrival time and this allows us to find what the hacker wants to derive from the server. The future of internet is not safe at all, the amount of hackers everyday is rising. So the study and algorithms helps us to understand and avoid the misuse of data to the unknown.

IX. REFERENCES

[1]. P. R. Clearinghouse. Privacy Rights Clearinghouse's Chronology of Data Breaches. Accessed: Nov. 2017. Online]. Available: https://www.privacyrights.org/data-breaches.

[2]. ITR Center. Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout. Accessed: Nov. 2017. Online]. Available: http://www.idtheftcenter.org/ 2016databreaches.html

[3]. C. R. Center. Cybersecurity Incidents. Accessed: Nov. 2017. Online]. Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents.

[4]. IBM Security. Accessed: Nov. 2017. Online]. Available: https://www.ibm.com/security/data-breach/index.html.

[5]. NetDiligence. The 2016 Cyber Claims Study. Accessed: Nov. 2017. Online]. Available: https://netdiligence.com/wp-content/uploads/2016/ 10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf.

[6]. M. Eling and W. Schnell, "What do we know about cyber risk and cyber risk insurance?" J. Risk Finance, vol. 17, no. 5, pp. 474-491, 2016.

[7]. T. Maillart and D. Sornette, "Heavy-tailed distribution of cyber-risks," Eur. Phys. J. B, vol. 75, no. 3, pp. 357-364, 2010.

[8]. R. B. Security.Datalossdb. Accessed: Nov. 2017. Online]. Available: https://blog.datalossdb.org.

[9]. B. Edwards, S. Hofmeyr, and S. Forrest, "Hype and heavy tails: A closer look at data breaches," J. Cybersecur., vol. 2, no. 1, pp. 3-14, 2016.

[10]. S. Wheatley, T. Maillart, and D. Sornette, "The extreme risk of personal data breaches and the erosion of privacy," Eur. Phys. J. B, vol. 89, no. 1, p. 7, 2016.

[11]. P. Embrechts, C. Klüppelberg, and T. Mikosch, Modelling Extremal Events: For Insurance and Finance, vol. 33. Berlin, Germany: Springer-Verlag, 2013.

[12]. R. Böhme and G. Kataria, "Models and measures for correlation in cyber-insurance," in Proc.

Workshop Econ. Inf. Secur. (WEIS), 2006, pp. 1-26.

[13]. H. Herath and T. Herath, "Copula-based actuarial model for pricing cyber-insurance policies," Insurance Markets Companies: Anal. Actuarial Comput., vol. 2, no. 1, pp. 7-20, 2011.

[14]. A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan, "Cyber-risk decision models: To insure it or not?" Decision Support Syst., vol. 56, pp. 11-26, Dec. 2013.

[15]. M. Xu and L. Hua. (2017). Cybersecurity Insurance: Modeling and Pricing. Online]. Available: https://www.soa.org/research-reports/ 2017/cybersecurity-insurance.

[16]. M. Xu, L. Hua, and S. Xu, "A vine copula model for predicting the effectiveness of cyber defense early-warning," Technometrics, vol. 59, no. 4, pp. 508-520, 2017.

[17]. C. Peng, M. Xu, S. Xu, and T. Hu, "Modeling multivariate cybersecurity risks," J. Appl. Stat., pp. 1-23, 2018.

[18]. M. Eling and N. Loperfido, "Data breaches: Goodness of fit, pricing, and risk measurement," Insurance, Math. Econ., vol. 75, pp. 126-136, Jul. 2017.

[19]. K. K. Bagchi and G. Udo, "An analysis of the growth of computer and Internet security breaches," Commun. Assoc. Inf. Syst., vol. 12, no. 1, p. 46, 2003.

[20]. E. Condon, A. He, and M. Cukier, "Analysis of computer security incident data using time series models," in Proc. 19th Int. Symp. Softw. Rel. Eng. (ISSRE), Nov. 2008, pp. 77-86.

[21]. Z. Zhan, M. Xu, and S. Xu, "A characterization of cybersecurity posture from network telescope data," in Proc. 6th Int. Conf. Trusted Syst., 2014, pp. 105-126. Online]. Available: http://www.cs.utsa.edu/~shxu/socs/intrust14.pdf.

[22]. Z. Zhan, M. Xu, and S. Xu, "Characterizing honeypot-captured cyber attacks: Statistical framework and case study," IEEETrans. Inf. Forensics Security, vol. 8, no. 11, pp. 1775-1789, Nov. 2013.

[23]. Z. Zhan, M. Xu, and S. Xu, "Predicting cyber attack rates with extreme values," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1666-1677, Aug. 2015.

[24]. Y.-Z. Chen, Z.-G. Huang, S. Xu, and Y.-C. Lai, "Spatiotemporal patterns and predictability of cyberattacks," PLoS ONE, vol. 10, no. 5, p. e0124472, 2015.

[25]. C. Peng, M. Xu, S. Xu, and T. Hu, "Modeling and predicting extreme cyber attack rates via marked point processes," J. Appl. Stat., vol. 44, no. 14, pp. 2534-2563, 2017.

[26]. J. Z. Bakdash et al. (2017). "Malware in the future? forecasting analyst detection of cyber events." Online]. Available: https://arxiv.org/abs/1707.03243.

[27]. Y. Liu et al., "Cloudy with a chance of breach: Forecasting cyber security incidents," in Proc. 24th USENIX Secur. Symp., Washington, DC, USA, 2015, pp. 1009-1024.

[28]. R. Sen and S. Borle, "Estimating the contextual risk of data breach: An empirical approach," J. Manage. Inf. Syst., vol. 32, no. 2, pp. 314-341, 2015.

[29]. F. Bisogni, H. Asghari, and M. Eeten, "Estimating the size of the iceberg from its tip," in Proc. Workshop Econ. Inf. Secur. (WEIS), La Jolla, CA, USA, 2017.

[30]. R. F. Engle and J. R. Russell, "Autoregressive conditional duration: A new model for irregularly spaced transaction data," Econometrica, vol. 66, no. 5, pp. 1127-1162, 1998.

Cite this article as :

N. Ram Mohan, N. Praveen Kumar, "Predicting and Analysis of Phishing Attacks and Breaches In E-Commerce Websites", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 4, pp. 170-175, July-August 2020. Available at

doi : https://doi.org/10.32628/IJSRSET207443

Journal URL : http://ijsrset.com/IJSRSET207443