1ZA-05

Analysis of Cyber-Attack Trends in India Using OSINT

Gedamkar Apurva Akalp[†] **Naoya Torii**[†]

SOKA University[†]

1. Introduction

Cyberattacks are rapidly gaining attention because they are reducing corporate profits, disclosing confidential information, and even stopping critical infrastructure. India is the third country in the world targeted by cyberattacks, and the cybercrime [12].

This paper summarizes current situation and future malware attack trends based on public information such as public web pages, reports from research companies, and newspaper article, based on an integrative. We focus on the cyber-attacks by malware and investigated some big cyber incidents using OSINT tools and analyzed cyber-attacks trend's in India.

2. Survey method

In order to conduct surveys based on public information, we mainly collected information using Web Crawling and Scrapping tools. In addition, Google, SHODAN and CENSUS were used as search engines. Regarding the status of malware, we collected and analyzed information published by each security vendors. In addition, information was collected using security blogger information and Twitter information in India.

3. Cyber security situation in India

3.1 Malware types

There are many common types, such as worms, viruses, Trojans, backdoors, and ransomware, but this article draws on Kaspersky's taxonomy [6].

To prevent from detecting antivirus, the code script techniques are known as code obfuscation and modification or attachment of a new behavior in the malware to improve strength and capability. Code obfuscation makes malware code unintelligible by malware detectors, it lessens the size of codes and help to deploy in short time span. In addition to this, code complications are categorized into polymorphic or metamorphic.

3.2 Incidents in India

This section explains serious security incidents caused by malware:

The rapidly growing automation enterprises in India are facing their security challenges. In Recent Times, the Reserve Bank of India (RBI) identified that around 50,000 cyber frauds which included malware attacks in India's Scheduled Commercial Banks (SCB) in 2018-19 fiscal. The popular malwares are related to ATM, debit and credit cards, and internet banking, which loss 145.08 crore rupees (223 Billion Yen) fraud in last fiscal. RBI recorded the overall number of banking attacks, detected in all the SCBs are 59,826 and the loss suffered is around 67,432.26 crore rupees (103 Billion yen) [9].

(1) Attack on nuclear power plants

In September 2019, NPCIL India Nuclear Power Corporation (NPCIL) had a malware attack on a 1,000 MW nuclear power plant system. The attack is aimed to steal technical information by the North Korean hacker group "Lazarus. The malware used in the attack is called Dtrack, which is a type of RAT (Remote Administration Tool). According to NPCIL, infected PCs are connected to a network for management purposes that is connected to the Internet, are not severely damaged because they are separated from important internal networks [8].

(2) Attacks on banks

a) In August 2018, the Cosmos Cooperative Bank's Debit Card payment system and SWIFT network were abused, and about 944 million rupees (1.5 billion yen) were stolen. The attack is said to have intruded the banking system in some way and infected ATM-related systems with multiple malware. Replying the response enabled unauthorized withdrawal. The attacker group is unknown. According to Indian Police, the bank has all its systems compliant with PCI DSS and has its own data center and SOC to protect customer data [10].

3.3 Malware characteristics in India

According to Kaspersky's information [11], the most popular malwares currently in India are reported as

follows.

(1) trojan.WinLNK.Runner.jo

A Trojan, the LNK file launches a malicious executable. Spreads via USB drive. In India, it is one of the most frequently used malware attacks occurring from year 2016 till now.

(2) trojan.winlnk.starter.gen

A Trojan horse is a malicious program that prevents Internet surfing. If user click on the link his system gets infect and opens a new tab, that floods the entire search into some advertising websites, and significantly slows down your computer or web.

(3) Hoax.MSIL.Seguras.a

It is a type of script that shows false information, gives a sense of crisis, and makes a mistake in purchasing software and services. It can be considered that attacks that take advantage of carelessness and lack of knowledge via USB and Internet access are mainstream.

4. Discussion

(1) Zero Day Attack

India is the second largest internet users in the world and the machineries used are relatively old. The software used is not licensed because the distribution environment is not well established. In many cases, the updates are considered insufficient.

Indian users are making every effort to take precautionary measures despite low awareness of cyber security; however, users try to use free antivirus software's which has less detection capabilities. But the number of mobile devices is speedily increasing and broadband connection too, it is expected that zero-day malware is relatively damaging mobile and other devices. In fact, a survey conducted in 2010 by Symantec reports that 76% of online adults are victims of cybercrime and negative online situations [13].

(2) Comparison with Japanese malware

According to Kaspersky's report, most of the malware that is distributed in Japan is attached to emails and spreads rapidly even though the security measures has been implemented. Around 40% - 50% Japan's popular malware attacks are mostly email and phishing based. It is thought that these are quite different from malware distributed in India. The malware which was trending from last year November 18th to December 17th are various types. At present, India is starting to work on security measures nationwide, and it is expected that the security measures will be expanded to the same level as Japan.

5. Conclusion

This paper described the malware trend in India. We explained that advanced attacks by various malwares are taking place due to the developing facilities and network environment in India. We also described major security incidents caused by malwares and discussed about zero-day attacks comparing with Japan malware situation. This paper summarized the malware attacks analysis based on the current as well as future malware trends using OSINT tools. India's security measures are requiring a major security to its internet infrastructure.

References

1. R. Rehman, Dr. G. C. Hazarika and G.Chetia https://www.researchgate.net/publication/267300795 Malware_threats_and_mitigation_strategies (July 2011).
2. Rami Sihwil, K. Omar and K. Ariffin. "A survey on malware analysis techniques" https://www.researchgate.net/publication/328760930 A_Survey_on_Malware_Analysis_Techniques_Static Dynamic_Hybrid_and_Memory_Analysis. (2017).
3. Gounder, Muni & Farik, Mohammed. New Ways To Fight Malware. International Journal of Scientific & Technology Research. 6. 313-318. (2017).
4. N. Zalavadiya and Dr. Priyanka Sharma "A Methodology of Malware Analysis, Tools and Technique for windows platform" http://www.ijircce.com/upload/2017/march/253_A% 20Methodology.pdf (March-2017).
5. N. Solanki, Dr. N. Sharma. "Malware Analysis: Types & Tools" https://pdfs.semanticscholar.org/80ac/88a3f5024ed6d 7664ba3ec1f5a378623ab12.pdf (2019).
6. Kaspersky classifying rules https://encyclopedia.kaspersky.com/knowledge/rules-for-classifying/
7. DSCI https://www.dsci.in/sites/default/files/documents/resource_centre/Cyber%20Security%20India%20Market.pdf
8. Zdnet news article. https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/
9. Around 50,000 Cyber Frauds reported in India during 2018-19: RBI https://www.cisomag.com/around-50000-cyber-frauds-reported-in-india-during-2018-19-rbi/
10. India's Cosmos Bank loses $13.5 mln in cyber attack https://www.reuters.com/article/cyber-heist-india/indias-cosmos-bank-loses-135-mln-in-cyber-attack-idUSL4N1V551G
11. Kaspersky Cyberthreat Real-Time Map https://cybermap.kaspersky.com/
12. India rank third among nation facing most cyber threats: Symantec https://economictimes.indiatimes.com/tech/internet/india-ranks-3rd-among-nations-facing-most-cyber-threats-symantec/articleshow/63616106.cms
13. Net Crime Report: Impact on People-Symantec https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Japanese-Human%20Impact-A4_Aug23.pdf (2010).