# BUILDING A KEY LOGGER USING PYTHON

1. Prof.R.Yadagiri Rao,professor,Head,H&S,Sri Indu Institute of Engineering&TechnologySIIET, Sheriguda,Ibrahimpatnam,Hydarabad,
2. D. NagaRaju,Assistant Professor,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad
3.S.Anitha, Asso professor,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad,
4.Ch.Akhila,Student,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad
3. 5.G. Himadeep,Student,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad
4. 6.A. Sirisha,Student,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad
5.

## ABSTRACT

A cyber-attack is malicious attempt by a person or organization to gain unauthorized access, steal data or cause damage to computers and destroying sensitive information. So in this study we will quickly detect and effectively respond to mitigate sophisticated key-logger Trojan horse and minimize the impact on sensitive data theft. Similarly securing and stating prevention majors in RFID and bundle a proper security protocol package in order to protect Sim cards from Sim cloning cyberattacks. Key-logger is software which is installed on your system and will fetch everything you type and attacker will easily get your information. Radio-Frequency Identification Technology (RFID) in this technology RFID theft occurs when someone uses their own RFID reader to trigger the RFID based financial access cards. and Sim cloning is the attack in which a SIM card is duplicated and after cloning the cloned SIM card's information is transferred onto the another SIM card and attacker can extract the SIM card's Authentication key(ki) and IMSI(Information Mobile Subscriber Identifier). Because of this digital industry faces billions of dollars financial loss, data loss and system or server crashes. There are so many organizations had experienced a data breach caused by issues like devices or documents being lost or computers being left unattended. So our purpose of this survey based on cyberattacks is to develop an sustainable cyber security model in future as well as an proper system architecture to help prevent these types of cyber-attacks.

## INTRODUCTION

From the past few years, technology has grown immensely and due to its ease of understanding, it is being used by people of all age groups. As the use of technology is increasing vigorously, the severity of cyber-attacks has also increased tremendously. Due to poor knowledge of cyber-attacks and neglecting the importance of cyber security many organizations and individuals have witnessed financial loss as well as data loss. However, the year 2020 has shown a whole new level of cyber-attacks. As the covid-19 pandemic introduced a new way of work to the world, it has accelerated cyber-attacks as well as data breaches. Many renowned companies were targeted and were hacked for essential data worth billions of rupees. Recently, In 2021,700 million LinkedIn users' data were exposed including email addresses, phone numbers, workplace information, account ids, links to their social media accounts, and gender details. In 2020 over 600 million accounts data of Sina Weibo website were leaked. Similarly, a 17-yearold hacker and his group breached twitter's network and grabbed control of Twitter accounts of high-profile users, and stole over $118,000 worth of bitcoin. Laundry's 63 restaurants' payment card details were hacked by malware targeting the restaurant's order entry systems which have card readers attached. In this study, the Author has mainly researched three attacks that cause breaching of sensitive and valuable data. It includes key-logging malware, RFID theft in banking transactions, and Sim cloning attacks. Key logger or keystroke logger is a program that monitors and logs all the keystrokes entered by the user through the keyboard including passwords, user names, and banking details. It can be programmed to monitor any type of data such as keystrokes, screens, and retrieving files from the user's system. Key logger logs all keystrokes and stores this log file into the local device and then sends it to a server from where the hacker can access this sensitive data. Key logger Trojan can be installed to the


Copyright @ 2022 Authors

victim's system without any permission along with the regular files and commonly used applications; this can be achieved by practicing social engineering. As key logger Trojan can enter into the system in the form of regular executable files, it can simply pass through antivirus software without detecting them. The authors studied several research papers and this study has shown that key logger Trojans are advancing into new versions making it difficult to detect by standard antivirus scanners and windows defender. RFID or Radio-Frequency Identification Technology is a wireless technology which works on Radio Waves and it is used in many industries for access control, supply chain logistics.

**PROPOSED SYSTEM:**

In RFID there is one microchip and antenna. A microchip contains identifying information and an antenna that transmits the information or data to the reader. Reader can read the information which is stored in tags. Any organization or industry could be at risk of cyberattack and there are many organizations due to cyber-attack affected and duped in financial loss, data loss. In the year 2013, information of 70 million credit cards of an organization called "Target" was stolen by using Card Skimming Malware attack.

The subscriber identity module (SIM) card is the transmitter of the signal to the mobile and tower. Our SIM cards contain two secret codes or keys called IMSI (international mobile subscriber identity) and KI (Authentication Key). These codes are the identifier of the Sim card .when someone gets IMSI and KI codes of Sim card then the attacker programs it into programmable empty SIM card for hacking and this procedure is known as Sim cloning. In the SIM cloning attackers create duplicate copy of the real SIM card. Not every SIM card is clone able, only some SIM card are clone able .now currently COMP128v1 architecture based SIM cards are mostly cloned. COMP12v1 is a first version of COMP12v architecture SIM cards. Because of SIM cloning attack we lost our important data like details of account information, financial information or other important document .so we will ensure to state the process between the subscriber and network which inhibits attacker to decrypt the encrypted and the operator in Sim cloning cyber-attacks and prevention majors against it.

**CONCLUSION**

The survey conducted in this paper mainly focuses on three abstruse attacks that are key-logging Trojan horse, Sim cloning, and RFID theft in banking transactions. To prevent data breaches caused by such attacks, organizations and individuals must be aware of such types of attacks. One must use the anti-virus software to scan systems periodically for any foreign material. The live survey mentioned in this paper has shown the severity of cyber-attacks and it has also shown how these attacks impact globally. It also proves the seriousness of having cyber security in organizations. The author has found out the undiscovered areas in research by surveying numerous research papers. This literature survey has shown that the advanced version of key logger is not yet detectable by any standard anti-virus software and windows defender. The majority of Sim cards operate on the basic encryption algorithm which is comp128, this algorithm is vulnerable to physical Sim cloning. When the Sim card is in a roaming service network, the information that needs for authentication is exposed on the air through which hackers can manage to obtain encryption keys which leads to OTA Sim cloning. Credit cards containing RFID tags can be accessed through an RFID tag reader by an attacker. This study has revealed the research gaps and the flaws in the existing systems. In the future, research will be conducted to minimize the flaws mentioned above as well as to protect the digital systems from a data breach.

## REFERENCES

[1] Dr Akashdeep Bhardwaj, Dr Sam Goundar , ELSEVIER,Keyloggers:silent cybersecurity weapons,Volume 2020, Issue 2, February 2020, Pages 14-19,10.1016/S1353-4858(20)30021-0.


Copyright @ 2022 Authors

[2] Huseyn Huseynov,Kenichi Kourai,Tarek Saadawi,Obinna Igbe,Virtual Machine Introspection for Anomaly-BasedKeylogger Detection,2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR) ,2020,10.1109/HPSR48589.2020.9098980
[3] Jia Wang, Brent Lagesse,KeyGuard: Using Selective Encryption to Mitigate Keylogging in Third-Party IME ,2020,arXiv:2011.10012
[4] Ahsan Wajahat; Azhar Imran; Jahanzaib Latif; Ahsan Nazir; Anas Bilal,A Novel Approach of Unprivileged Keylogger Detection,2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),IEEE,25 March 2019,10.1109/ICOMET.2019.8673404
[5] Yazeed Albabtain; Baijian Yang,The Process of Reverse Engineering GPU Malware and Provide Protection to GPUS, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),IEEE,06 September 2018, 10.1109/TrustCom/BigDataSE.2018.00248
[6] Nikhil Tekawade; Shruti Kshirsagar; Shripad Sukate; Leena Raut; Shubhangi Vairagar,Social Engineering Solutions for Document Generation Using Key-Logger Security Mechanism and QR Code,2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA),IEEE, 25 April 2019,10.1109/ICCUBEA.2018.8697420
[7] Darshanie Sukhram; Thaier Hayajneh,KeyStroke logs: Are strong passwords enough?, 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON),IEEE,08 January 2018,10.1109/UEMCON.2017.8249051
[8] Adam Prayogo Kuncoro; Bagus Adhi Kusuma,Keylogger Is A Hacking Technique That Allows Threatening Information On Mobile Banking User, 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE),IEEE,2019,10.1109/ICITISEE.2018.8721028


Copyright @ 2022 Authors