



Comprehensive Study in Preventive Measures of Data Breach Using Thumb-Sucking

Keinaz Domingo^(✉), Bryan Cruz, Froilan De Guzman^(✉), Jhinia Cotiangco, and Chistopher Hilario

University of the East, Caloocan, Philippines
keinazd6@gmail.com, bryancruz014@gmail.com,
froilan.deguzman@ue.edu.ph, jhiniaaa04@yahoo.com,
chris.hilario0108@gmail.com

Abstract. This research presents a method of data breach that is known as thumb-sucking. Through the insertion of a flash drive into a computer's USB port, it allows for the extraction of the user's private information. In order to protect against the possibility of data breach in the form of thumb-sucking, the researchers have devised preventive measures in order to protect a user from malicious hackers. These measures include testing on various Windows operating systems that are in use, mainly Windows 7, Windows 8.1, Windows 10 and some Linux platform. The choice of conducting tests on Windows is due to the problem that not all users of Windows are tech savvy enough to avoid their data being accessed without permission.

Keywords: Data breach · Thumb-sucking · Preventive measures

1 Introduction

In an age of information where what one is searching for is just a click away, it's also no wonder that there are people that wish to gain access to an individual's private information through illegal means. The sharing of data has become an essential means of communication. Although data sharing has become a necessity, many are still not aware of the possible dangers that it poses, especially owners of small establishments that may fall prey to this danger. [12] Since innovations in technology are constantly progressing and more data is being displayed in public, this constitutes a new risk for IT departments. [1] Although it is not only data on the internet that needs to be protected, but as well as data that's saved on personal storage devices. Portable devices are convenient for the purpose of business; however, it is also because of their portable nature that they are more likely to be stolen or even misplaced [3].

This act of data being leaked and becoming privy to the eyes of others is known as a data breach. A data breach is said to occur when private data is exposed to outside parties, whether it be unintentional or not. [7] Data breaches and illegal access to private information happens very often, although what makes this alarming is not the amount of common people being affected, but rather how hackers are targeting corporations that

have a considerable amount of value, not to mention that their methods of attack are improving [4].

Numerous ideas have been formulated in order to deal with the problem of data breaches. These include methods such as imposing restrictions on companies that use wireless networks, contributing to government projects to improve security, and as well as making personal improvements in the security of one's network. [6] Various governments have also taken to devising countermeasures against data breach, and making them known to the public. One method is through the restriction. Creating separate networks that do not have access to each other can help by limiting access from the outside, and firewalls can be implemented in order to further improve security [8].

2 Literature Review

According to study, mobile devices have also become a viable source for hackers to commit their attacks. This is because a large portion of the world is now covered by mobile networks, which only continue to increase in coverage over the years. [5] This means that the amount of personal information that a hacker potentially has access to can only increase as well, putting even more data at risk.

Another study conducted a survey on data breaching. According to their finds, organizations whether large or small are more prone to being targeted by outside parties, the attacks of which were able to compromise a great portion of these organizations. [9] The idea that most organizations suffer from being targets of data breach is definitely food for thought.

A different source explains that the employees of a company could actually be seen as a threat to security, explaining that the mistakes that an employee makes accounts to up to 95% of incidents. [10] This means to say that most data breaches could possibly result from human error, which is not a far off explanation given the fact that not all employees are trained properly. Even a portable device such as a flash drive can be used to commit data theft. A study on data breach says that portable devices such as hard drives, laptops and flash drives being stolen or lost has also been a contributor to the leakage of data. [2] This is because a simple portable device could be used by a hacker to infiltrate and retrieve an organization or individual's information, and very easily at that if they can manage to retrieve its contents.

Data breaches aren't completely restricted to physical storage, because with the advent of cloud computing, it allows for the possibility of storing data within a cloud on the internet. Although the technology is not without any risks, as the cloud can be used as a medium for hackers to commit their crimes. In this way, hackers are able to retrieve personal data from websites that store their information on the cloud, such as common social media sites like Facebook, Youtube, Twitter, and many others. [15] Although there are ways to protect a cloud against data breach, which involves using technology such as a cloud antivirus that scans files such as documents whenever a network cloud receives it [17].

While on the discussion of the internet and the cloud, a paper discussed the benefits of using an ANS (anonymizing network system). The way that an ANS works is by

making the user anonymous on the internet, protecting any personal information that could be stolen and used against the user. [11] This could help against data breaches by giving a user the benefit of anonymity. Through this anonymity, a potential hacker will not be able to infer any information from the user.

Another study claims that the traditional methods of defense are no longer enough to protect against targeted attacks. [16] There is some truth to it, because a persistent hacker could gain access to an organization's information with enough time and resources.

Because the protection of data is an important matter, other researchers have devoted their time to making a model that presents an attacker's possible methods of attack. The model which has been named Cyber Kill Chain is described as a model with 7 layers or phases of a cyber-attack. With the information that was presented in the paper, it could be seen as a valuable resource for those who are aiming to create new methods of defense against cyber-attacks, as this lets them gain understanding as to how an attacker plans out their attack [13].

Another paper by other researchers used a system called TrustBox. The system functions by preventing data breaches when a user is connected to a network, but it also provides protection even if a user is not currently connected to any networks. [14] Through the use of that system, sensitive data could not be leaked accidentally, and access was only granted by an authentication scheme. The implementation of a similar system to various organizations could possibly lessen the amount of data breach that happens.

One paper discussed how anti-viruses are vulnerable during updates, because they are either partly or totally deactivated during this time. The reasoning behind this is because a malware installer is able to monitor or even trigger an antivirus into installing an update, which leaves the system open to attacks in this brief window. [18] Through this method, the malware would gain access to the computer. Another paper on anti-viruses discussed a way of using an anti-virus to assist an attack, which is called an anti-virus assisted attack. This method of attack works by utilizing byte patterns in order to slip through an anti-virus undetected. [19] In theory, the anti-virus itself would be a means for an attack to get through.

3 Thumb-Sucking

Thumb-sucking is a method to obtain information from a computer by inserting a thumb drive into a USB port. For the specificity of testing, the researchers used a password recovery tool named WebBrowserPassView that was installed on a flash drive. It retrieves passwords by revealing the cached contents of the user's web browsers. It is normally used for recovering lost passwords, but for the purpose of this study, the researchers have used it as a way to access passwords that have been stored in a web browser cache.

The thumb-sucking procedure is shown in Fig. 1, the process of which the software goes through. The process of the attack is as follows:

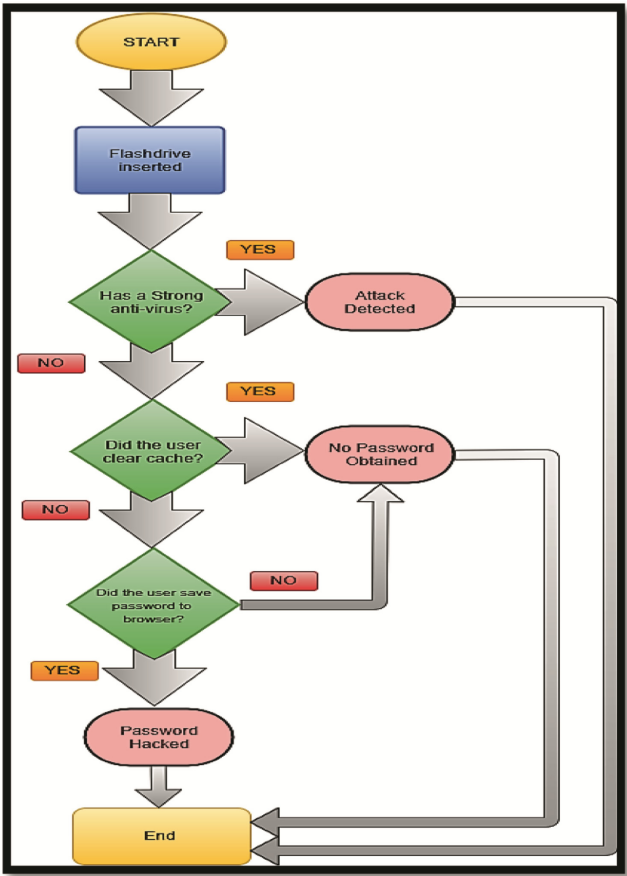


Fig. 1. Diagram of thumb-sucking process

1. Flash drive inserted – The beginning of the process starts with the insertion of the flash drive containing WebBrowserPassView into an open USB port on the target computer. Once it is finished, it moves onto the next step.
2. Has a strong anti-virus? – From here, the results can vary in two ways. If the computer has a strong anti-virus, it can detect the attack, rendering it useless and ending the process. If the anti-virus is weak, the diagram continues.
Attack detected – If detected by an anti-virus, the attack is halted.
3. Did the user clear cache? – If the software bypasses the anti-virus, it begins to scan the caches of the web browsers. If the cache has been cleared recently, or it contains no available information, then no password is obtained and the process ends. However, if it finds that there is content in the cache, it moves to the next step.

No password obtained – If the cache has been cleared recently, no passwords are obtained by the software.

- 4. Did the user save password to browser? – If the user did not save any passwords to the browser that was used, then no password is obtained and the process ends. In the event that the software detects any passwords in the browser cache, then the password is obtained and saved by the software.

No password obtained – If no passwords have been saved to the browser, then no information is obtained.

Password hacked – If passwords have been saved to the browser, then the software detects the passwords and retrieves them from the cache.

4 Testing and Discussion

In order to help protect against data breach, the researchers have conducted tests in order to observe the vulnerability of a user’s passwords being retrieved by an outside party through thumb-sucking. To begin with, the researchers first tested v1.85 of WebBrowserPassView on a laptop running the latest version of Windows 10. As shown in the figure that follows, the attack was detected by Windows 10 before it could retrieve any passwords from the caches of the browsers, and was subsequently prevented from doing so (Fig. 2).

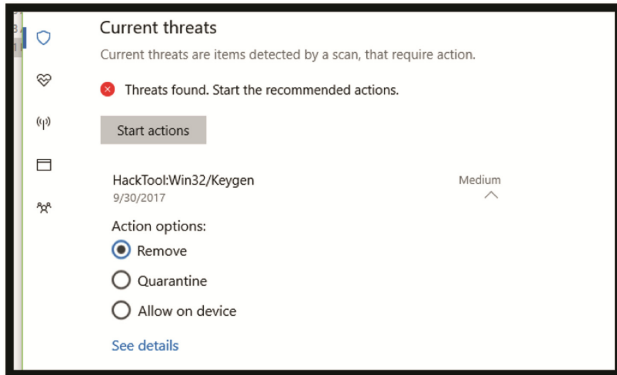
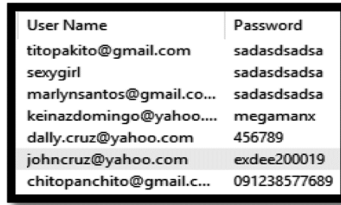


Fig. 2. The attack is detected by Windows

Next, we tried using v1.86 of WebBrowserPassView. Surprisingly enough, the software was not detected and it was able to obtain the passwords from various browsers, as shown in the figure below (Fig. 3).



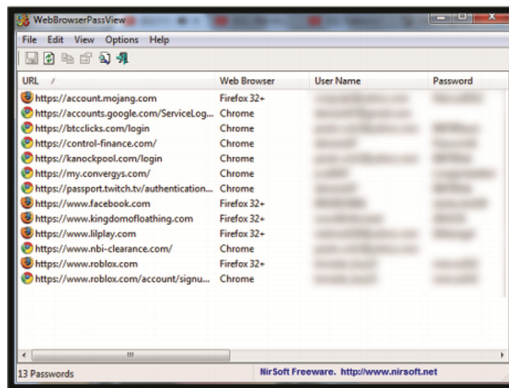
User Name	Password
titopakito@gmail.com	sadasdsadsa
sexygirl	sadasdsadsa
marlynsantos@gmail.co...	sadasdsadsa
keinazdomingo@yaho...	megamanx
dally.cruz@yahoo.com	456789
johncruz@yahoo.com	exdee200019
chitopanchito@gmail.c...	091238577689

Fig. 3. Password obtained

With this information, we can assume that having the latest version of your operating system installed, which in this case, was Windows 10, will decrease the risk of your passwords being hacked by password recovery tools. The reason why is because these updates might be able to fix potential vulnerabilities in earlier versions of the operating system, which hacking tools will be able to take advantage of in order to obtain your private information.

After testing on Windows 10, the researchers conducted another test on Windows 7 using the same tool. Upon opening the application, it was instantly detected by Microsoft Security Essentials. This test was done with the Windows Firewall turned off. After the attack was detected, it was quarantined and removed from the computer by Microsoft Security Essentials. Any subsequent attempts to download the application resulted in it being removed once it was extracted from its .zip file.

The researchers attempted another test with the anti-virus deactivated, and this time, the application opened and managed to obtain passwords from Firefox and Google Chrome’s browser caches. Passwords and usernames obtained were blurred in order to protect personal information (Fig. 4).



URL	Web Browser	User Name	Password
https://account.mojang.com	Firefox 32+		
https://accounts.google.com/ServiceLog...	Chrome		
https://btclicks.com/login	Chrome		
https://control-finance.com/	Chrome		
https://kanockipool.com/login	Chrome		
https://my.convergys.com/	Chrome		
https://passport.twitch.tv/authentication...	Chrome		
https://www.facebook.com	Firefox 32+		
https://www.kingdomofloathing.com	Firefox 32+		
https://www.klplay.com	Firefox 32+		
https://www.nbi-clearance.com/	Chrome		
https://www.roblox.com	Firefox 32+		
https://www.roblox.com/account/signu...	Chrome		

Fig. 4. Password obtained from Firefox and Google Chrome

Tests were conducted on Windows 8.1, and the application was able to access passwords that were stored on Firefox. WebBrowserPassView also allows for the viewing of detailed information of each individual instance that is retrieved from the browser

caches. It is able to show the type of username and password field used for that specific instance (Fig. 5).

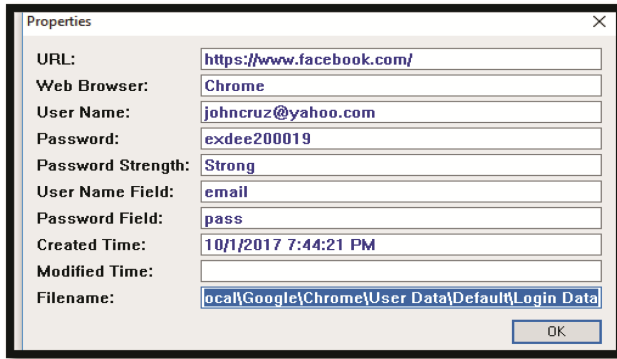


Fig. 5. Detailed account information

After testing, the researchers were able to compile the information obtained into a table. In some Linux environment such CentOs, Debian, Fedore and Ubuntu, and Kali Linux the thumb-sucking tool is tested (Table 1).

Table 1. Testing results

Operating system	Tool version	Penetrated	Secured
Windows 7	V1.85	No	Yes
Windows 7	V1.86	No	Yes
Windows 8.1	V1.85	No	Yes
Windows 8.1	V1.86	Yes	No
Windows 10	V1.85	No	Yes
Windows 10	V1.86	Yes	No
CentOs	V1.86	No	Yes
Debian	V1.86	No	Yes
Fedora	V1.86	No	Yes
Ubuntu	V1.86	No	Yes
Kali	V1.86	No	Yes

Although this kind of attack is easy to avoid for users who are aware of the possibility of being the target of such an attack, since the application needs to be inserted with a flash drive into a computer's USB port. But if a hacker were to modify the application to run automatically upon insertion of the flash drive, it could endanger a person's private information. To prevent that from happening, one can disable the autorun feature on removal devices on the Windows Registry. To do so, the following steps need to be followed on Windows 7:

1. Search for regedit and run it. Doing so opens the Registry Editor.
2. Go to the key that is shown as follows: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
3. Create a new Hex value with the name: NoDriveTypeAutoRun
4. Change the value of the newly created key to: 4 (HEX)
5. Restart Windows.

After completing the steps, it will disable the auto-run feature on all removable devices. By accomplishing this, it prevents devices that are inserted into the computer from automatically running any viruses or applications that could be used to tamper with your files. If instead, one's computer uses Windows 10, one can follow the steps below in order to protect their computer.

1. Search for regedit, run the application and browse the following path that is shown below: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
2. Create a new key named StorageDevicePolicies and press enter.
3. Select the newly created key, right-click on the right side and create a new DWORD (32-bit) value.
4. Name the new DWORD WriteProtect and change its value from 0 to 1

Upon completion of the steps, outsiders who connect a USB device to the user's computer or laptop will be denied copy privileges, which will protect the user's information since the outsider cannot obtain any of the user's information.

Ensuring that one constantly clears their cache from time-to-time can also prevent a person's information from being hacked. On Windows, CTRL + SHIFT + DELETE will open the Window. On the prompt that opens, you can select a time range of cached data to be cleared as well as specify what will be deleted. This will remove potential data that can be retrieved by a possible attacker.

If one uses Firefox, they can customize the configuration of the browser to never remember any browsing, download, search or form history, as well as clear history every time Firefox closes. By doing this, it ensures that no data enters the cache, and with the lack of data, it prevents a data breach from happening.

Although if the user instead makes use of Google Chrome, then one can click CTRL + H in order to open the cache. From there, various settings can be chosen in order to decide what data will be cleared or not.

5 Conclusion

The researchers believe that it is possible for a user to avoid a data breach simply through being aware. This awareness will make them more conscious of their actions, since human error is a common reason why information often gets leaked to outside entities. Knowing the proper steps of preventing a data breach can go a long way for a person without any professional training, as they are now aware of the possible consequences that can arise from being careless. Since the thumb-sucking flash drive only uses a simple method of attack, it is quite possible for a user who is aware of the risks to avoid the attack. The attack relies heavily on cached information not being cleared in order to

obtain any information. Therefore, if the user constantly clears their cache, then the risk of their information being sucked significantly decreases. The use of a strong anti-virus is also another layer of defense against such attacks, because it allows for the early detection of an attack. If a user wishes to further enhance the protection of their information, they can set their browser cache to not remember any information, thereby limiting the information that a hacker can potentially retrieve from their computer. Using the Registry tool can also aid in protecting one's information by modifying the registries.

Having access to tools that can aid a user in protecting against a data breach is also viable. Software such as anti-viruses can allow for the early detection of possible threats to a system.

References

1. Five Solutions for Improving Your Organization's Data Security. Kanguru, Secure. Anytime. Anywhere (2016)
2. Huq, N.: Follow the data: analyzing breaches by industry. TrendLabs Research Paper (2015)
3. Protecting the confidentiality of personal data, guidance note. Department of Finance (2008)
4. Data Protection and Breach. Online Trust Alliance (2015)
5. Internet Security Threat report. Symantec Corporation (2014)
6. Crews, C.W. Jr., Oberwetter, B.: Preventing identity theft and data security breaches: the problem with regulation. Competitive Enterprise Institute (2006)
7. Cheng, L., Liu, F., Yao, D.: Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Min. Knowl. Discov.* **7**, 1–14 (2017)
8. Basic Cybersecurity Measures. WaterISAC (2015)
9. Vaizey, E.: 2015 Information Security Breaches Survey. HM Government (2015)
10. Investing in Human Firewall. Lawroom (2014)
11. Clark, J, Stavrou, A.: Breaching & Protecting an Anonymizing Network System. In: Annual Symposium on Information Assurance (2011)
12. Frost, S.: Could a data breach cause your business to fail? Faronics
13. Yadav, T., Rao, A.M.: Technical aspects of cyber kill chain. In: Abawajy, J.H., Mukherjea, S., Thampi, S.M., Ruiz-Martínez, A. (eds.) SSCC 2015. CCIS, vol. 536, pp. 438–452. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22915-7_40
14. Schmidt, M., Fahl, S., Schwarzkopf, R., Freisleben, B.: TrustBox: a security architecture for preventing data breaches
15. Nandhakumar, C., Ranjithprabhu, K., Raja, M.: Counter measures for data breach in cloud computing. *Int. J. Res. Comput. Appl. Robot.* **2**, 124–129 (2014)
16. Balazs, Z., Effitas, M.: Breach detection system testing methodology
17. Chamorro, E., Han, J., Beheshti, M.: The design and implementation of an antivirus software advising system. In: Ninth International Conference on Information Technology (2012)
18. Min, B., Varadharajan, M., Tupakula, U., Hitchens, M.: Antivirus security: naked during updates. *Softw. – Pract. Exp.* Wiley Online Library (2013)
19. Wressnegger, C., Freeman, K., Yamaguchi, F., Rieck, K.: Automatically inferring malware signatures for anti-virus assisted attacks. In: Asia CCS (2017)