Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4697494, 11 pages
https://doi.org/10.1155/2022/4697494

Research Article

Air-Gapped Networks: Exfiltration without Privilege Escalation for Military and Police Units

Nachaat Mohamed,[1] **Saif Khameis Almazrouei**,[2] **Adel Oubelaid**,[3] **Mahmoud Elsisi**,[4,5] **Basem M. ElHalawany**,[5,6] **and Sherif S. M. Ghoneim**[7]

[1]*Rabdan Academy (Homeland Security Department), Abu Dhabi, UAE*
[2]*Ministry of Interior (Smart Security Systems Department), UAE*
[3]*Laboratoire de Technologie Industrielle et de l'Information, Faculté de Technologie, Université de Bejaia, Bejaia 06000, Algeria*
[4]*Department of Electrical Engineering, National Kaohsiung University of Science and Technology, Kaohsiung 807618, Taiwan*
[5]*Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo 11629, Egypt*
[6]*Electronics and Communication Engineering Department, Kuwait College of Science and Technology, Doha District 35004, Kuwait*
[7]*Electrical Engineering Department, College of Engineering, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*

Correspondence should be addressed to Mahmoud Elsisi; mahmoudelsisi@nkust.edu.tw
and Basem M. ElHalawany; basem.mamdoh@feng.bu.edu.eg

Received 7 October 2022; Revised 8 December 2022; Accepted 20 December 2022; Published 29 December 2022

Academic Editor: Pierre-Martin Tardif

Several security tools have been described in recent times to assist security teams; however, the effectiveness and success remain limited to specific devices. Phishing is a type of cyberattack that uses fraudulent emails and websites to obtain personal information from unsuspecting users, such as passwords and credit card numbers. Hackers can gain access to your information through a variety of methods, and the most common of which are king, phishing, spear phishing, social engineering, and dictionary attacks. Each of these techniques is unique, but they all have the same goal: to obtain your personal information. Nevertheless, there is the potential to exploit this problem in terms of security. In this paper, we used the Bash Bunny (BB), a new tool designed to assist military, law enforcement, and penetration tester teams with their work to conduct exfiltration without privilege escalation through T1200, T1052, and T1052.001 techniques in air-gapped networks with effectiveness/success 99.706%.

1. Introduction

The T1200 is a high-performance multirole aircraft that can carry out a variety of missions. It is the most recent addition to the US Air Force fleet and represents a significant upgrade over previous models [1]. The T1200 is intended to improve flexibility and capability in a variety of roles, including air-to-air combat, air-to-ground attack, intelligence, surveillance, reconnaissance (ISR), and search and rescue (SAR) [2]. The T1200 ATT&CK® model is based on the Cyber Kill Chain model and is tailored to enterprise networks. It includes a comprehensive set of attackers' tactics, techniques, and procedures (TTPs) for targeting and compromising an organization, as well as the mitigations and defenses that can be used to prevent or detect those attacks. The T1200 MITRE ATT&CK is a threat-based analytical framework for identifying, assessing, and forecasting cyber threats. This framework enables an organization's security posture and the effectiveness of its security controls to be evaluated and analyzed.

The T1200 MITRE ATT&CK can be used to: identify cyber threats and threat actors, understand an organization's security posture, predict cyberattacks, and assess the effectiveness of security controls. In recent years, there has been an increased focus on cybersecurity and the various threats that exist [3].

One of the techniques included in the MITRE ATT&CK for Windows suite is known as the T1052. This technique makes use of an executable file in order to carry out a script or command on a computer that is located elsewhere. The file can be sent to the remote system via a variety of different techniques, such as by attaching it to an email and downloading it from the web or by sharing it over a network. The code that is contained in the file will be run on the remote system when the file is executed [4].

Attackers have the capability of gaining access to distant systems and running arbitrary code through the use of the ATT&CK T1052 technique. Because of this, it is a potent weapon that can be utilized in a diverse array of different assaults. On order for businesses to protect themselves from this tactic, they should limit users' abilities to execute script files that are attached to emails, downloaded from websites, or stored in network shares [3, 5–11].

The MITRE ATT&CK T1052.001 covers techniques used by adversaries to gain remote access to systems. The techniques in this techniques group may be used in conjunction with other techniques groups to enable an adversary to fully compromise a system. Some of the techniques in this group may require compromised systems or user accounts to already be present within an environment to be successful [3, 5–11].

As such, various organizations have developed frameworks to help identify and mitigate these threats. One such framework is the MITRE ATT&CK framework [5]. The MITRE ATT&CK framework is a comprehensive list of common adversary tactics and techniques [12]. This framework is utilized by organizations in order to ascertain weak points in their security measures and gain a deeper comprehension of the dangers they confront. In this article, we are going to take a look at the MITRE ATT&CK framework and discuss the various ways in which it may be utilized to strengthen the security posture of your company [11]. The framework is broken up into fourteen different categories, and each of these categories corresponds to a different stage of an assault. The categories are as follows: reconnaissance, weaponization, delivery, exploitation, installation, command and control, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, and exfiltration [13].

Of course, Bash Bunny is a USB attack device made by the American company Hak5. If you look at this little USB, it looks like no different from any other USB. But when we examine its internal components, we will find that it contains many important components that work based on a quad-core ARM processor Cortex A7, 8 GB SLC NAND Disk, 512 MB DDR3 Memory, and 32 K L1/512 K L2 Cache. In addition to the USB port, the Bash Bunny has a small switch that can be changed to three different positions and is located on the side of the LED lamp (booting, update, and arming mode) as shown in the figure [14]. Figure 1 depicts the RGB and switch positions of the BB.

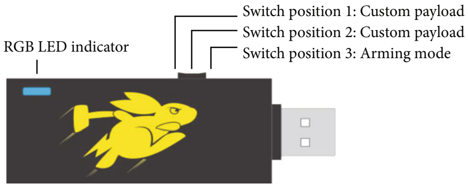

Switch position 1: Custom payload
Switch position 2: Custom payload
Switch position 3: Arming mode
RGB LED indicator

Figure 1: Bash Bunny using T1200, T1052, and T1052.001 techniques.

Air-gapped network is a network that has a physical separation from other networks that are not secure, such as the Internet. This allows the network to be more secure. Air-gapped networks are used to prevent attackers from compromising classified or sensitive information [15]. (Note: air-gapped networks are also known as sandboxes.) The military, the government, and the financial sector all frequently use networks that have air gaps between them. On the other hand, air-gapped networks can be found in any company that needs to prevent its data from being made available to the general public and uses those companies as their customers. There are a few different approaches one may take to physically divide a network. The use of firewalls and routers to physically isolate a network is the approach that is most frequently utilized. Another way is to use an air gap, which is a physical separation that is placed between the network and unprotected networks. It is possible to generate an air gap by physically isolating classified and unclassified networks on separate levels inside the same building [16].

2. Problem Statement

There are two parts to the problem. The first stage occurs when some criminals are apprehended by security personnel (army or police). These criminals have computers, and the security services must gain access to them as soon as possible in order to obtain evidence. If they use traditional methods to obtain passwords to unlock these devices, they will waste a lot of time and may not be successful. This tool can circumvent passwords and copy any data from those devices.

The second stage occurs when the penetration testing team requires strong and immediate proof of the attack scenarios that APT groups can use against the organization. In addition to demonstrating the disastrous extent of employees' and administrators' lack of security awareness, this tool is used to demonstrate it.

2.1. Related Work and Motivation. The use of ransomware as a method of attack has become increasingly common over the course of the previous few years. Ransomware is a type of malicious software that restricts access to a user's files or device until the attacker receives a payment known as a ransom. Attackers have begun to exfiltrate data from their targets before encrypting their devices or files in order to make ransomware attacks more effective [17]. This is done in order to enhance the amount of money that can be extracted from victims. The purpose of this paper is to provide a concise overview and describe how one may carry out exfiltration without elevating their privileges through BB (in order to carry out exfiltration, we first need to acquire initial access). Access To Start With When it comes to cyberattacks, the phase where the attacker first gains access to the system is likely the most crucial [5]. This is due to the fact that an attacker would be unable to get a foothold on a target system and carry out their payload if they were denied early access to the system. The strategies used for first access are perpetually undergoing change, and the creation of brand new procedures is ongoing at all times [18]. It is essential, in order to maintain a competitive advantage in this arena, to maintain awareness of the most recent tendencies and advancements in this field [18]. In this piece, we are going to take a look at some of the most common methods of initial access that are being utilized by cybercriminals in the modern era. In addition to this, we will offer some advice on how you can protect yourself from these assaults [3, 5–8, 13, 19, 20]. Phishing by email or physical access through USB is one of the most common ways used by attackers to get initial access [13]. Phishing is a form of social engineering assault that relies on fooling users into giving sensitive information such as passwords or credit card numbers. Phishing is also known as spear phishing and email phishing. Attackers will frequently send faked emails that appear to originate from a legitimate entity, such as a financial institution or an online retailer [18]. These emails will frequently contain links to malicious websites that are created with the express purpose of stealing the victim's personal information [20]. Phishing attacks are notoriously difficult to detect, yet they frequently succeed in subverting security measures and compromising systems. One more common method of first access is the employment of viruses and worms. These forms of malicious software are created with the purpose of propagating themselves throughout an entire network by copying themselves [3, 5–11, 13, 21–23]. After a computer has been infected by a virus or worm, the malware can then begin to carry out its intended function, known as its payload. This function could involve anything from the theft of sensitive data to the deletion of files or the formatting of disks. Attachments to malicious emails are a common vector for the propagation of viruses and worms, as is the practice of downloading malicious files from websites that cannot be trusted. The act of extracting information from a computer system is referred to as exfiltration. The information may come in the form of files, emails, or credentials for the user [3, 5–11, 13, 16, 21–25]. Exfiltration might be purposeful or inadvertent. Hackers that are aiming to steal confidential information will frequently perform intentional exfiltration as part of their attack. When an employee transfers company data to their personal email account or saves it to a USB device, this opens the door to the possibility of accidental data exfiltration [5]. Data can be extracted from a target system using a method known as exfiltration, which is a computer security approach. This can be accomplished either locally, by doing something like removing media from the location, or remotely, by making use of some kind of clandestine communication route [3, 5–11, 21, 22]. The latter has garnered a significant amount of interest in recent times due to the fact that it provides a number of benefits that are not offered by physical exfiltration. In this article, we will take a high-level look at the history and evolution of remote exfiltration techniques, with a special focus on recent improvements [16, 26].

Exfiltration has been around for as long as information has been passed from one location to another. With the advent of digital information, however, the method of exfiltration has taken on new forms [26]. In its most basic form, exfiltration is the unauthorized transfer of data out of a secure network or system. This can be done in several ways but is typically accomplished by taking advantage of security vulnerabilities to copy or extract data undetected. Exfiltration may use social engineering techniques to convince [27]. The Bash Bunny is a device that allows for data exfiltration from a target network. It operates as a keystroke injection USB device, and once inserted into a computer, it can be used to send keystrokes and commands at will. This makes it an ideal tool for gaining access to or extracting data from a target network [16]. In this poster, we will discuss how it can be used for data exfiltration [3, 6–11, 21–23]. Finally, regarding the motivations of using Bash Bunny, the Bash Bunny is a powerful USB device created for penetration testers and security professionals. It can be plugged into a computer's USB port, and once it is in, the user can remotely execute commands on the machine [26]. This makes it an excellent tool for stealing data, as it can be used to bypass security measures that would ordinarily prevent such activity. In addition to its data-stealing capabilities, the Bash Bunny can also be used to install malware on computers, making it a very powerful and dangerous tool [6–11, 16, 21–25].

2.2. Objectives. The main aim of this research is: to infect the target machine/network, to gain access to the target system, to produce evidence that demonstrates the capability of BB to aid law enforcement and military personnel in expeditiously removing evidence from devices used by criminals, to contribute to the penetration testing team's efforts to show how the importance of security awareness in companies may help protect against and uncover potential threats which is carried out by sophisticated attack groups (APT), and to transfer sensitive data from the target system without privilege escalation.

2.3. Methodology. There are a few ways that an attacker can get their initial access onto a company's network. The most effective way in our method will works through a social engineering attack. In this type of attack, the attacker tries to gain information about the company or its employees by pretending to be someone they are not [28]. Social engineering is the process of manipulating people into performing actions or divulging confidential information. One of the most common social engineering techniques is to use USB Bash Bunny to spread malware [29]. When someone inserts a USB Bash Bunny into their computer, they may be prompted to run a program or open a document. If the user does so, they may be unwittingly installing malware on their computer. Exfiltration over physical media (EoPM) is a

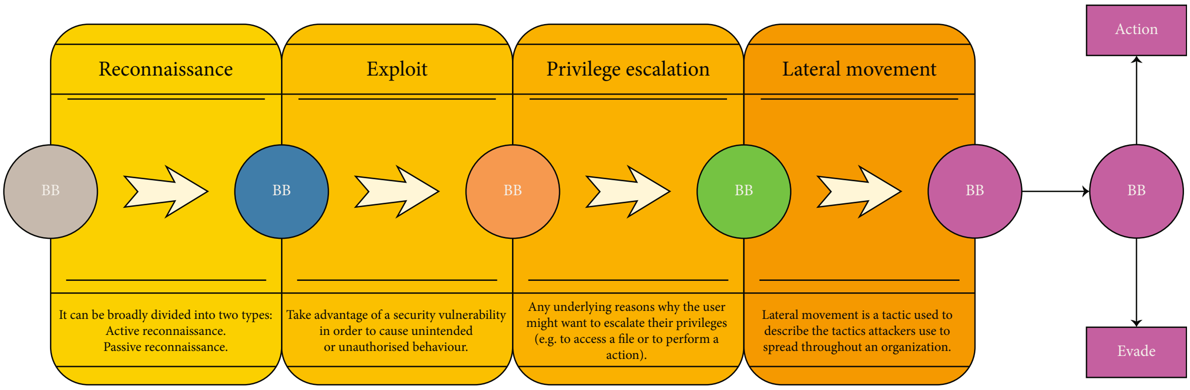

Reconnaissance
Exploit
Privilege escalation
Lateral movement
BB
BB
BB
BB
BB
BB
Action
Evade
It can be broadly divided into two types: Active reconnaissance. Passive reconnaissance.
Take advantage of a security vulnerability in order to cause unintended or unauthorised behaviour.
Any underlying reasons why the user might want to escalate their privileges (e.g. to access a file or to perform a action).
Lateral movement is a tactic used to describe the tactics attackers use to spread throughout an organization.

Figure 2: Kill Chain method.

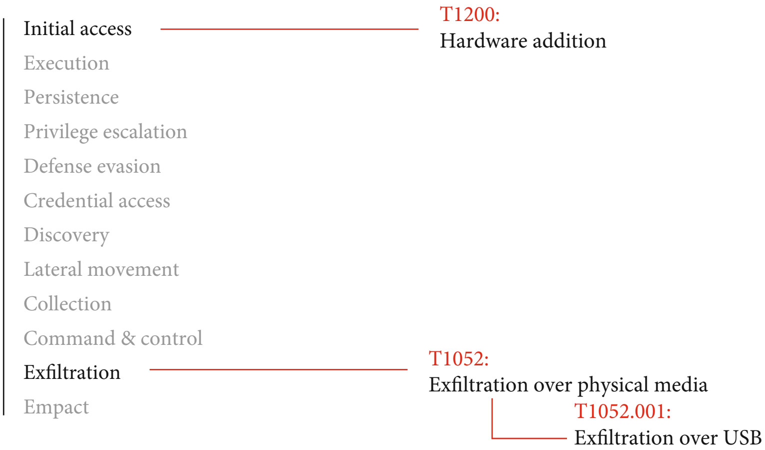


Figure 3: Employ T1200, T1052 and T1052.001 techniques to conduct exfiltration without privilege escalations.

technique that can be used to exfiltrate data from a secure network across an insecure medium [6–11, 21]. The term was coined in 2006 by security researcher Michael Ossmann and has been used primarily in the context of computer security [7]. EoPM can take many forms, but typically involves the installation of a covert communications channel between two systems. Data is transferred between the systems by physically transporting removable storage media through a USB Bash Bunny between them. Because the data is physically transported, it is not subject to the security measures [8].

Exfiltration is the process of extracting data from a system, and a Bash Bunny through applying T1200, T1052, and T1052.001 techniques can be an effective tool for this purpose [9–11, 16, 21–28]. The first step is to connect the Bash Bunny to the target system. Once the Bash Bunny is connected, we will use the BunnyHop payload to hop onto the target system. This payload will allow us to gain access to the target system and begin extracting the data we need. Now that we have access to the target system, we will use the exfiltrate payload to extract the data we need [8, 9]. This payload will allow us to save the data we need to a USB drive or other external storage device. We can then remove the Bash Bunny and take our data with us. The methodology steps are as follows:

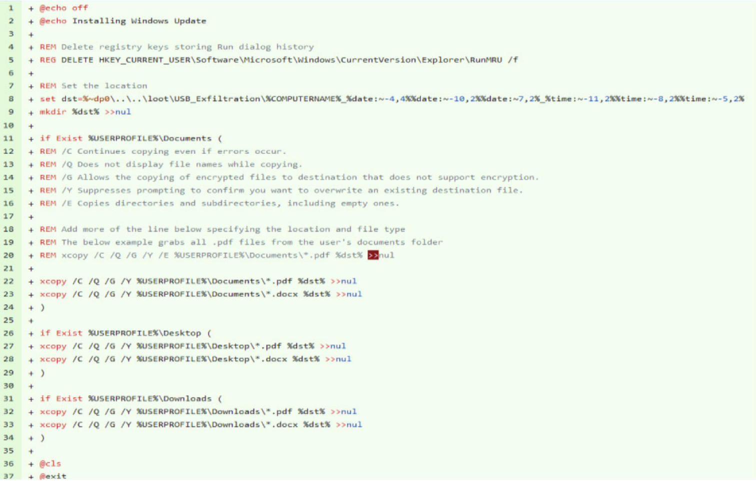
(1) Achieve initial access and bypass all windows defender through using T1200 technique over hardware addition

(2) Bypassed recon, exploit, privilege escalation, and lateral movement tactics through BunnyHop payload

(3) Use simple-USB-extractor payload to extract the files from the target system

(4) Conduct exfiltration through using T1052 technique, which is exfiltration over physical media, and T1052.001 technique which is exfiltration over USB

2.4. Kill Chain Method Used in Bash Bunny (BB). The standard procedure for achieving exfiltration consists of reconnaissance, exploit, privilege escalation, lateral movement, and then exfiltration. However, the BB method, which uses T1200, T1052, and T1052.001 techniques, will give us gain access and exfiltration without privilege escalation technique using MITRE ATT&CK framework. Additionally, all stages will be achieved automatically by BB through T1200, T1052, and T1052.001 techniques in the initial access and exfiltration stages. BB approach that utilizes the MITRE ATT&CK framework as its foundation. This framework is a knowledge base that contains adversary tactics and



```
+ @echo off
+ @echo Installing Windows Update
+
+ REM Delete registry keys storing Run dialog history
+ REG DELETE HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU /f
+
+ REM Set the location
+ set dst=%~dp0\..\..\loot\USB_Exfiltration\%COMPUTERNAME%_%date:~-4,4%%date:~-10,2%%date:~7,2%_%time:~-11,2%%time:~-8,2%%time:~-5,2%
+ mkdir %dst% >>nul
+
+ if Exist %USERPROFILE%\Documents (
+ REM /C Continues copying even if errors occur.
+ REM /Q Does not display file names while copying.
+ REM /G Allows the copying of encrypted files to destination that does not support encryption.
+ REM /Y Suppresses prompting to confirm you want to overwrite an existing destination file.
+ REM /E Copies directories and subdirectories, including empty ones.
+
+ REM Add more of the line below specifying the location and file type
+ REM The below example grabs all .pdf files from the user's documents folder
+ REM xcopy /C /Q /G /Y /E %USERPROFILE%\Documents\*.pdf %dst% >>nul
+
+ xcopy /C /Q /G /Y %USERPROFILE%\Documents\*.pdf %dst% >>nul
+ xcopy /C /Q /G /Y %USERPROFILE%\Documents\*.docx %dst% >>nul
+ )
+
+ if Exist %USERPROFILE%\Desktop (
+ xcopy /C /Q /G /Y %USERPROFILE%\Desktop\*.pdf %dst% >>nul
+ xcopy /C /Q /G /Y %USERPROFILE%\Desktop\*.docx %dst% >>nul
+ )
+
+ if Exist %USERPROFILE%\Downloads (
+ xcopy /C /Q /G /Y %USERPROFILE%\Downloads\*.pdf %dst% >>nul
+ xcopy /C /Q /G /Y %USERPROFILE%\Downloads\*.docx %dst% >>nul
+ )
+
+ @cls
+ @exit
```

Figure 4: Simple-USB-extractor payload (http://Github.com).

techniques that are employed in cyberattacks. It acts as a resource for understanding how adversaries work, thereby alerting cybersecurity defenders of the many hazards they are up against. Additionally, the framework serves as the foundation for a variety of security-related endeavors, including research, training, and product development. The MITRE ATT&CK matrix is a framework that may be used to describe cyberattacks as well as ways to protect against them [28]. The matrix provides a standard vocabulary for professionals in the field of cyber security to use when exchanging information regarding the strategies and procedures utilized by attackers. In addition to that, it is also utilized in the training and assessment processes. The MITRE ATT&CK matrix is founded on the experiences of cyber security professionals from both the private sector and the public sector that have worked in the real world. The Kill Chain outlined in the figure begins with reconnaissance, then moves on to exploitation, then privilege escalation, then lateral movement, then evidence, and finally, action or exfiltration [29]. BB's Kill Chain method is described in Figure 2.

2.5. Exfiltration without Privilege Method. One of the most important steps in adversary engagement is initial access. This is the process or technique that an adversary uses to gain the first foothold in a targeted environment [7–11]. There are many ways to gain initial access, and the method used will often depend on the adversary's objectives and capabilities.

The initial access phase of an engagement is often considered the most critical, as it sets the stage for everything that follows. This is why it's important to have a good understanding of the initial access techniques used by adversaries. In this paper, initial access used by BB before moving to achieve exfiltration to compromise the target machine then using T1200 technique over hardware addition, and finally exfiltration through T1052 technique, which is exfiltration over physical media, and T1052.001 technique which is exfiltration over USB to achieve the entire mission as shown below in exfiltration method. Figure 3 shows BB employ

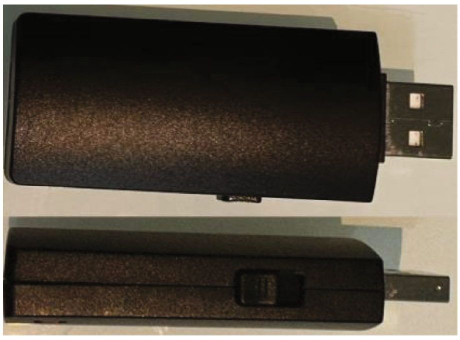


Figure 5: Our BB that was used in real scenario.

Table 1: Linear regression of each attempt.

$X - M_x$	$Y - M_y$	$(X - M_x)^2$	$(X - M_x)(Y - M_y)$
-0.0067	0.0133	0	-0.0001
-0.1067	0.1133	0.0114	-0.0121
0.0933	-0.0867	0.0087	-0.0081
-0.1067	0.1133	0.0114	-0.0121
-0.2067	0.1133	0.0427	-0.0234
0.1933	-0.1867	0.0374	-0.0361
0.0933	-0.0867	0.0087	-0.0081
0.1933	-0.1867	0.0374	-0.0361
-0.0067	0.0133	0	-0.0001
-0.1067	0.1133	0.0114	-0.0121
0.1933	-0.1867	0.0374	-0.0361
-0.0067	0.0133	0	-0.0001
-0.2067	0.2133	0.0427	-0.0441
-0.1067	0.1133	0.0114	-0.0121
0.0933	-0.0867	0.0087	-0.0081
		SS: 0.2693	SP: -0.2487

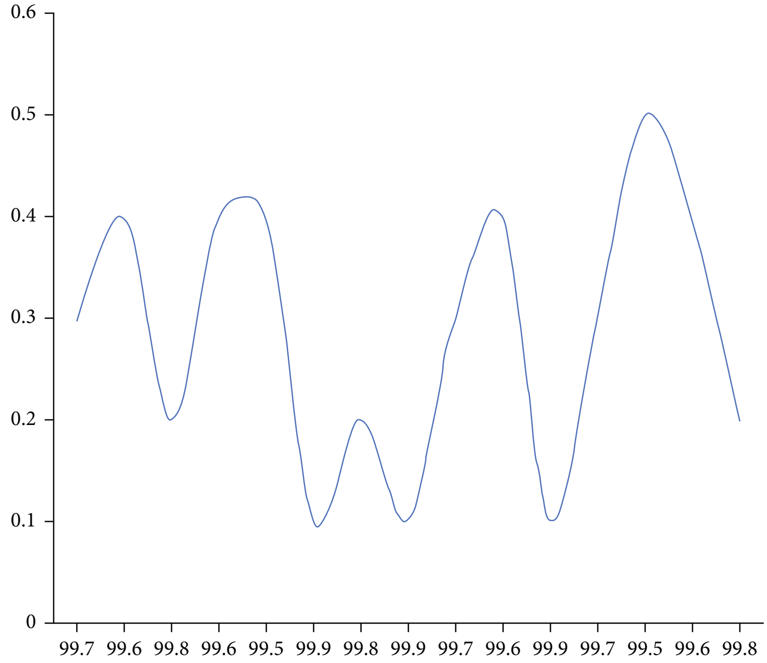


Figure 6: Plot of BB effectiveness, success, and regression.

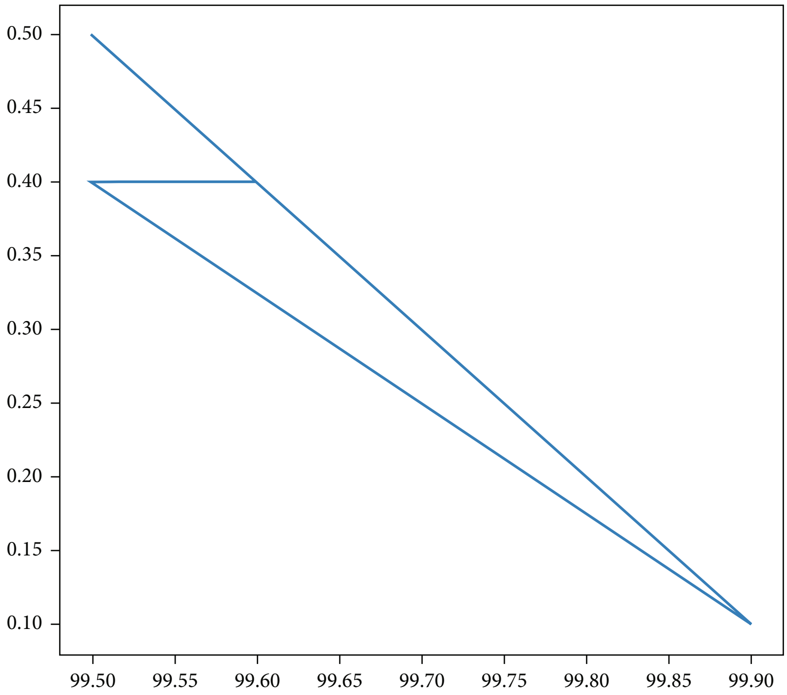


Figure 7: Plot of BB effectiveness, success, and regression.

T1200, T1052 and T1052.001 techniques to conduct exfiltration without privilege escalations.

2.6. Expected Results Based of Using Some Exfiltration Payloads. Exfiltration payloads are malicious files or codes that are used to secretly transfer data from one system to another without the knowledge of the system's owner. In order to provide attackers with a means to steal sensitive data, they are frequently utilized in conjunction with other types of malware, such as remote access tools (RATs). Exfiltration payloads come in a wide range of forms, and each of those forms has the potential to serve a distinct set of functions. The keylogger is by far the most prevalent kind, and its purpose is to record everything that the user types on their

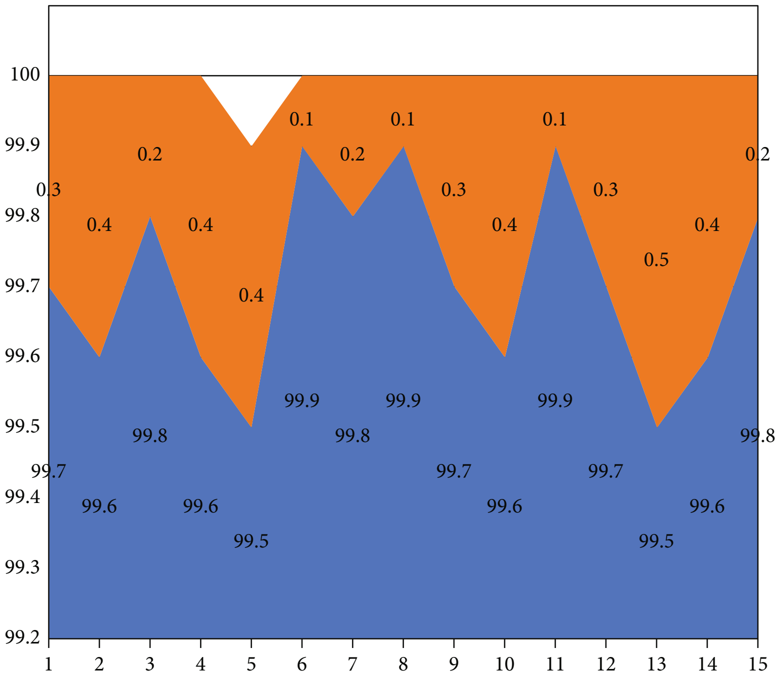


Figure 8: Plot of BB effectiveness, success, and regression.

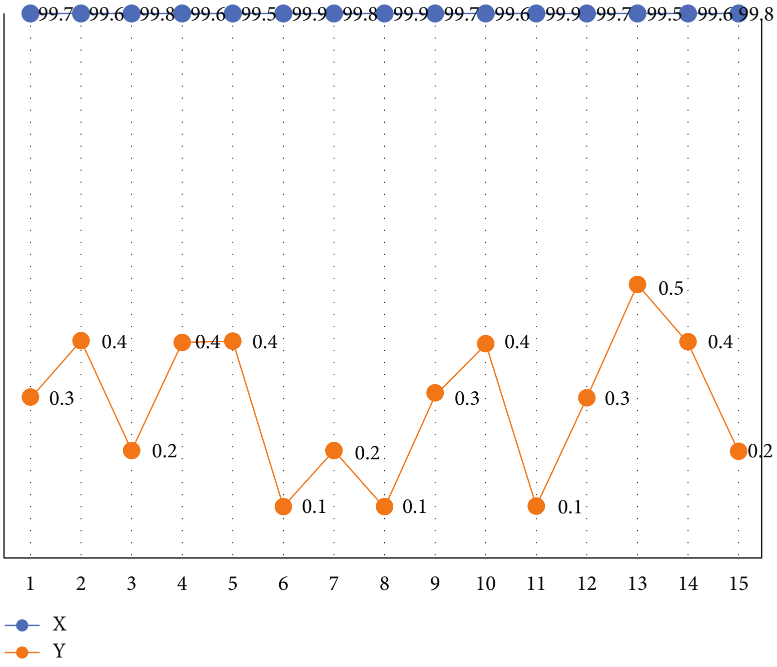


Figure 9: Plot of BB effectiveness, success, and regression.

keyboard. This can contain credit card numbers, passwords, and any other sensitive information. Other sorts of exfiltration payloads include programs that take screenshots of the user's activity and audio recorders that record the user's chats. These programs are known as screen capture programs and audio recorders, respectively. The fact that exfiltration payloads are so risky is due to the fact that they can be utilized to steal virtually any kind of information imaginable. It is imperative that you perform a security scan as soon as possible if you have any reason to believe that malware may have been installed on your system. Payloads such as SmartFileExtract Exfiltrator, browser data, dropbox-exfiltrator, FTP exfiltrator, optical-exfiltration, simple-USB-extractor, SMB exfiltrator, and USB exfiltrator are the ones that are utilized for exfiltration the most frequently. BlackBackup, FileInfoExfil, MacPDFExfil, Powershell TCP Extractor, and SmacAndGrab are the programs that are being discussed here [16, 26–31].

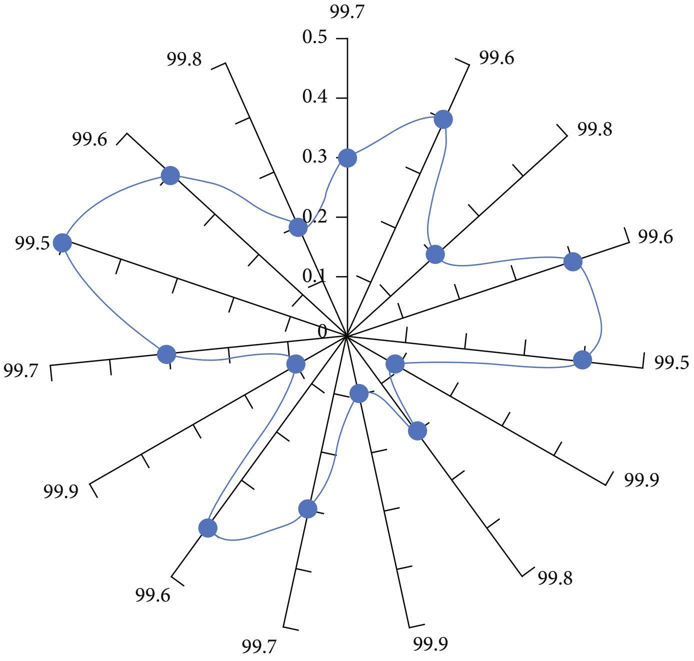


Figure 10: Plot of BB effectiveness, success, and regression.

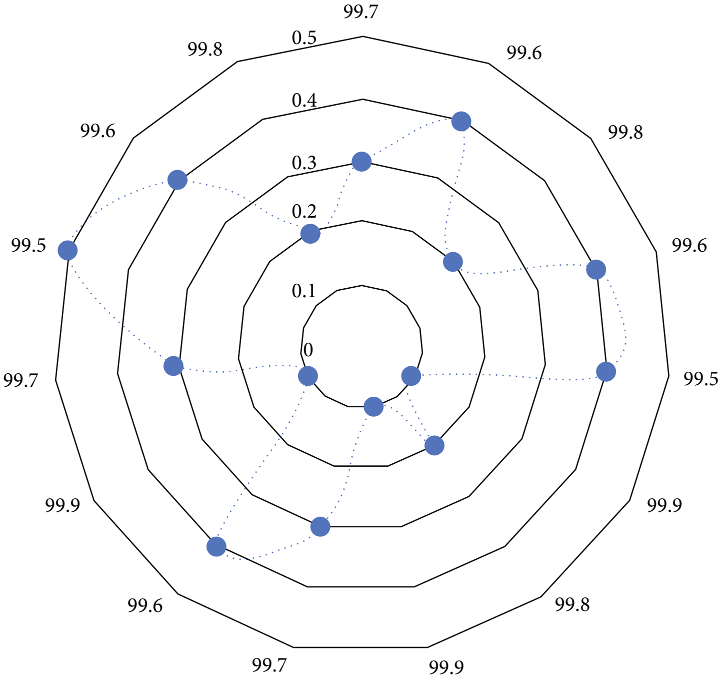


Figure 11: Plot of BB effectiveness, success, and regression.

One of the most popular payloads to conduct exfiltration is simple-USB-extractor payload which is written by author DanTheGoodman. As shown in the figure, simple-USB-extractor payload is a strong payload that allows you to easily extract files from target machine. This payload is designed for use to attack air gap network, protected systems, and collect evidence for by police and military units [31]. Figure 4 depicts the simple-USB-extractor payload.

In this paper, we have provided how to employ T1200, T1052, and T1052.001 techniques to conduct exfiltration without privilege escalations.

2.7. Real Scenario. We made a purchase of BB hardware from the company known as Hak5, which is the BB manufacturer. Then, we put it to use against three Windows computers; we gave each device five chances to circumvent

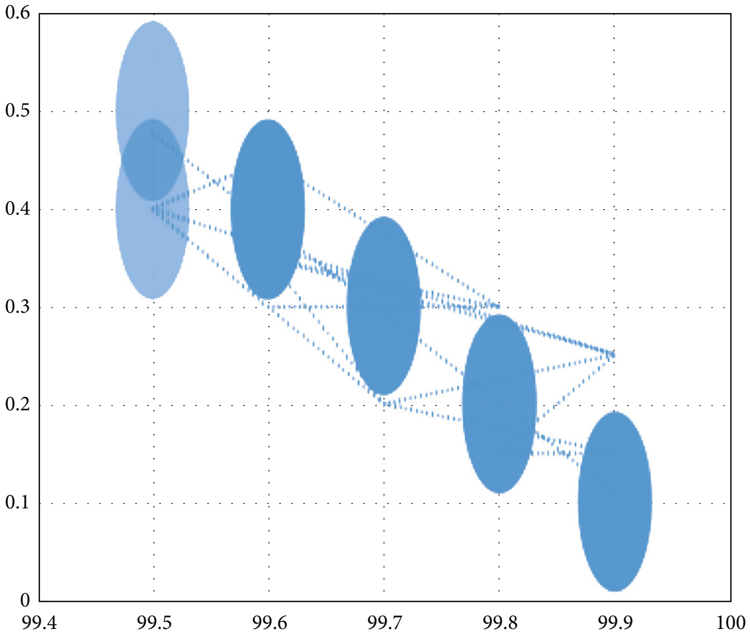


Figure 12: Plot of BB effectiveness, success, and regression.

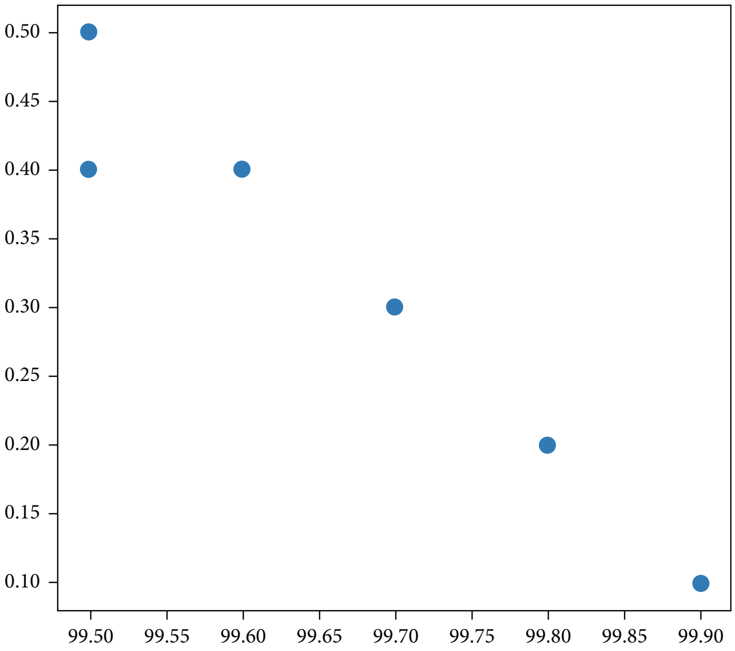


Figure 13: Plot of BB effectiveness, success, and regression.

passwords and copy data from the victim's device, and it was successful in all cases with an accuracy of 99.706%. Figure 5 shows our BB that was utilized all the way through this actual scenario.

We determined the effectiveness/success of each attempt, linear regression by utilizing Python libraries known as Matplotlib, SciPy, and NumPy, as indicated in Table 1, as well as analyzing what the graphs (Figures 6–13) depict in addition to the equations numbered 1 through 10.

$$\sum X = 1495.6, \tag{1}$$

$$\sum Y = 4.3, \tag{2}$$

$$X = 99.7067, \tag{3}$$

$$Y = 0.2867, \tag{4}$$

$$\sum(\mathrm{SSX}) = 0.2693, \tag{5}$$

$$\sum(\mathrm{SP}) = 0.2487, \tag{6}$$

$$\text{Regression} = \hat{y} = bX + a, \tag{7}$$

$$b = \mathrm{SP}/\mathrm{SSX} = -0.25/0.27 = -0.92327, \tag{8}$$

$$a = \mathrm{MY} - b\mathrm{MX} = 0.29 - (-0.92^{*}99.71) = 92.34257, \tag{9}$$

$$\hat{y} = -0.92327X + 92.34257. \tag{10}$$

3. Conclusions

We have described in this paper how to employ a Bash Bunny to conduct exfiltration using the T1200, T1052, and T1052.001 approaches that are based on MITRE ATT&CK. Exfiltration is the process of taking data from a system that is not intended to be accessible by a third party, as we have already stated. Exfiltration is frequently carried out with nefarious intentions, such as the theft of sensitive data or intellectual property, in the majority of cases. Exfiltration, on the other hand, can be put to lawful purposes, such as the retrieval of data from a system that is no longer accessible or the acquisition of specific evidence against criminals (used by police and military units). And as we have discussed previously, exfiltration can be carried out in a variety of different methods; however, one technique is to make use of a Bash Bunny. Bash Bunnies are little devices that may be programmed to carry out a variety of functions, one of which being the exfiltration of data with a success rate of 99.706%. In the beginning, you will have to set up it so that it can connect to the target system. After it has been connected, you will be able to use Bash Bunny to retrieve the information you require.

We strongly encourage researchers to focus their future efforts on MITRE ATT&CK and TTPs, and we encourage them to try to implement additional tactics on the victim's devices and machines. These tactics can easily be studied as the actual tactics that sophisticated attackers like advanced persistent threats (APT) use to infiltrate public and private institutions. This will have a big influence on both our ability to understand these tactics and design solutions that are strong against them.

Data Availability

The data supporting the conclusions of the study is available upon request via contacting the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors express their great gratitude and thanks to both the Rabdan Academy and the Ministry of Interior in the United Arab Emirates for supporting this work in terms of moral, material, and technical terms in this important field serving various institutions.

References

[1] R. Al-Shaer, J. M. Spring, and E. Christou, "Learning the associations of mitre att & ck adversarial techniques," in *2020 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, Avignon, France, 2020.

[2] O. Alexander, M. Belisle, and J. Steele, *MITRE ATT & CK® for Industrial Control Systems: Design and Philosophy*, The MITRE Corporation, Bedford, MA, USA, 2020.

[3] T. Thomas, M. Piscitelli, B. A. Nahar, and I. Baggili, "Duck hunt: memory forensics of USB attack platforms," *Forensic Science International: Digital Investigation*, vol. 37, article 301190, 2021.

[4] A. Niakanlahiji, J. Wei, and B. T. Chu, "A natural language processing based trend analysis of advanced persistent threat techniques," in *2018 IEEE International Conference on Big Data (Big Data)*, pp. 2995–3000, Seattle, WA, USA, 2018.

[5] A. Kuppa, L. Aouad, and N. A. Le-Khac, "Linking CVE's to MITRE ATT & CK techniques," in *The 16th international conference on availability, reliability and security*, pp. 1–12, Vienna, Austria, 2021.

[6] S. Zhao and X. A. Wang, "A survey of malicious HID devices," in *International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 777–786, Springer, Cham, 2019.

[7] N. Mohamed and B. Belaton, "SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique," *IEEE Access*, vol. 9, pp. 42919–42932, 2021.

[8] N. A. Mohamed, A. Jantan, and O. I. Abiodun, "An improved behaviour specification to stop advanced persistent threat on governments and organizations network," *Proceedings of the International Multi Conference of Engineers and Computer Scientists*, vol. 1, pp. 14–16, 2018.

[9] N. A. Mohamed, A. Jantan, and O. I. Abiodun, "Protect governments, and organizations infrastructure against cyber terrorism (mitigation and stop of server message block (SMB) remote code execution attack)," *International Journal of Engineering*, vol. 11, no. 2, pp. 261–272, 2018.

[10] O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. Mohamed, and H. Arshad, "State-of-the-art in artificial neural network applications: a survey," *Heliyon*, vol. 4, no. 11, article e00938, 2018.

[11] N. Mohamed, "Study of bypassing Microsoft Windows Security using the MITRE CALDERA framework," *F1000Research*, vol. 11, p. 422, 2022.

[12] W. Cai, Z. Hong, X. Wang, H. C. Chan, and V. C. Leung, "Quality-of-experience optimization for a cloud gaming system with *ad hoc* cloudlet assistance," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 12, pp. 2092–2104, 2015.

[13] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. G. Gourisetti, "Cyber threat dictionary using MITRE ATT& CK matrix and NIST cybersecurity framework mapping," in *2020 Resilience Week (RWS)*, pp. 106–112, Salt Lake City, UT, USA, 2020.

[14] Y. Shin, K. Kim, J. J. Lee, and K. Lee, "ART: automated reclassification for threat actors based on ATT & CK matrix similarity," in *2021 World Automation Congress (WAC)*, pp. 15–20, Taipei, Taiwan, 2021.

[15] N. Munaiah, A. Rahman, J. Pelletier, L. Williams, and A. Meneely, "Characterizing attacker behavior in a

cybersecurity penetration testing competition," in *2019 ACM/ IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, pp. 1–6, Porto de Galinhas, Brazil, 2019.

[16] M. Guri, B. Zadov, and Y. Elovici, "ODINI: escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1190–1203, 2019.

[17] K. Oosthoek and C. Doerr, "Inside the matrix: CTI frameworks as partial abstractions of complex threats," in *2021 IEEE International Conference on Big Data (Big Data)*, pp. 2136–2143, Orlando, FL, USA, 2021.

[18] F. S. Toker, K. O. Akpinar, and I. Özçelik, "MITRE ICS attack simulation and detection on ether CAT based drinking water system," in *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6, Elazig, Turkey, 2021.

[19] M. Kovtsur, A. Minyaev, D. Khramtsov, and G. Abramenko, "Investigation of attacks and methods of protection of wireless networks during authorization using the IEEE 802.1 x protocol," in *The 5th international conference on Future Networks & Distributed Systems*, pp. 555–561, Dubai, United Arab Emirates, 2021.

[20] P. Maynard and K. McLaughlin, "Big fish, little fish, critical infrastructure: an analysis of Phineas Fisher and the 'hacktivist'threat to critical infrastructure," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, pp. 1–7, Dublin, Ireland, 2020.

[21] A. E. Omolara, A. Jantan, O. I. Abiodun, H. Arshad, and N. A. Mohamed, "Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication," *International Journal of Electrical & Computer Engineering*, vol. 9, no. 3, p. 1879, 2019.

[22] N. A. E. Mohamed, A. Jantan, and A. E. Omolara, "Mitigation of cyber terrorism at ATMs, and using DNA, fingerprint, mobile banking app to withdraw cash (connected with IoT)," *International Journal of Engineering Research and Technology*, vol. 11, pp. 845–852, 2018.

[23] N. Mohamed, E. Alam, and G. L. Stubbs, "Multi-layer protection approach MLPA for the detection of advanced persistent threat," *Journal of Positive School Psychology*, vol. 6, no. 5, pp. 4496–4518, 2022.

[24] N. Mohamed, "State-of-the-art in Chinese APT attack and using threat intelligence for detection. A survey. Journal of positive school," *Journal of Positive School Psychology*, vol. 6, no. 5, pp. 4419–4443, 2022.

[25] N. A. Mohamed, A. Jantan, and A. E. Omolara, "Using fingerprint, pycrypto, and mobile banking app, to withdraw cash from ATMs in developing countries. (a confrontation to eavesdropping attack based on one-time password (OTP))," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 4, 2018.

[26] C. J. D'Orazio, K. K. R. Choo, and L. T. Yang, "Data exfiltration from internet of things devices: iOS devices as case studies," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 524–535, 2017.

[27] D. A. Haddon and H. Alkhateeb, "Investigating data exfiltration in dns over https queries," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, pp. 212–212, London, UK, 2019.

[28] Y. S. Takey, S. G. Tatikayala, S. S. Samavedam, P. L. Eswari, and M. U. Patil, "Real time early multi stage attack detection," *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, pp. 283–290, 2021.

[29] T. He and Z. Li, "A model and method of information system security risk assessment based on MITRE ATT & CK," in *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*, pp. 81–86, Sanya, China, 2021.

[30] I. Vaccari, S. Narteni, M. Aiello, M. Mongelli, and E. Cambiaso, "Exploiting Internet of Things protocols for malicious data exfiltration activities," *IEEE Access*, vol. 9, pp. 104261–104280, 2021.

[31] J. Fairbanks, A. Orbe, C. Patterson, E. Serra, and M. Scheepers, "ATT & CK tactics in android malware control flow graph through graph representation learning and interpretability," in *Proceedings of the 2021 IEEE international conference on big data (REU 2021 symposium)*, pp. 219–224, Hong Kong, 2021.