Forensic Implication of a Cyber-Enabled Fraud Taking Advantage of an Offline Adversary-in-the-Middle (AiTM) Attack

D.O. Lawal, D.W. Gresty, D.E. Gan, and T.C. Durojaiye
University of Greenwich/School of Computing and Mathematical Sciences, London, United Kingdom
D.O.Lawal@greenwich.ac.uk
D.W.Gresty@greenwich.ac.uk
D.Gan@greenwich.ac.uk
TD8962Q@greenwich.ac.uk

***Abstract* - Many computer users utilise the High-Definition Multimedia Interface (HDMI) for connecting external displays as this interface is common on modern computers. This work investigates the feasibility of performing an offline adversary-in-the-middle attack with a portable programmable device such as the Screen Crab which leverages the HDMI interface to covertly capture information being sent to the external display. This work also addresses the possibility of such attacks being carried out as the reconnaissance phase of a wider attack or being carried out as a standalone attack for data exfiltration, data theft, or espionage. Among the operational observations of the Screen Crab, while it was exfiltrating data, include its property of being storage and process efficient. In addition, there were no indicators on the external display (e.g., quality drop, lag/latency) to suggest to the target user that any form of tampering had been done to their machine. This paper also shows how it might be difficult for forensic analysts to detect the use of this device which poses a risk of the target user (victim) being falsely accused or wrongly prosecuted for divulging sensitive or classified information in this kind of situation.**

Keywords – Digital forensics, Adversary-in-the-middle, Cyber-enabled fraud, Screen Crab, Portable programmable devices, Miscariage of justice.

I. INTRODUCTION

Man-in-the-middle attacks (MiTM) or adversary-in-the-middle (AiTM) attacks are used to achieve a number of different attacks. A common use of an adversary-in-the-middle attack is to sniff or eavesdrop on communications that the attacker is not authorised to receive. There are a number of tools that help attackers achieve this, such as Wireshark, and Tshark, which could also be used by security administrators to monitor the flow of traffic for anomalies. ARP poisoning is a common technique applied by attackers to become the man-in-the-middle [1]. ARP poisoning tricks both ends of the communication into believing they are communicating with the intended recipient, when in fact they are communicating with an unauthorised third party (e.g., a client thinks it is communicating with the gateway router while communicating with the attacker machine, and the router also thinks it is receiving or forwarding packets to the intended client, also while talking to the man-in-the-middle). This is possible because the ARP protocol employs no form of authentication during communication which makes it easy for an attacker to send spoofed ARP responses and become the man or adversary-in-the-middle [1]. An AiTM attack through ARP poisoning can be detected while it is active using the 'arp -a' command to investigate the machine suspected of compromise. Investigation can also be done using other tools highlighted in [2].

An attacker could become the adversary-in-the-middle for the sole purpose of sniffing packets without modification or plans to use the captured information in a future attack. An attacker could also become the adversary-in-the-middle to capture information that would be useful to launch a larger attack where the information acquired is key to the success of the larger attack [1]. In this work, the information captured from the target is to be used to plan a larger attack of illegally modifying a record of accounts and whoever is considered responsible, could be charged with fraud if caught.

One common property of the highlighted AiTM methods is that they leave traces that can be detected during incident response or a criminal investigation [3]. This work investigates the effectiveness of the current digital forensic process in combatting the use of a portable programmable device like the Screen Crab when it has been used to commit or facilitate a crime; in this case, a crime of fraud by illegally modifying a record of accounts. The attacker would usually require adequate information about the target environment to successfully plan and execute a file tampering attack. Such information is acquired through reconnaissance which is usually the first phase of a cyber-attack [4]. The reconnaissance phase provides information about the target such as the operating system, applications, location of the system, location of the target file, and several other information that would be useful to the attacker.

This work focuses on the reconnaissance phase of a file tampering attack where the Screen Crab will be used for information gathering on the target. The experiment considered in this work is part of a larger file tampering

experiment involving the use of another portable programmable device (the O.MG Cable) for altering the file after the attacker has gathered information with the Screen Crab; however, this paper does not cover the file tampering aspect of the attack.

II. Related work

This section explores existing work and literature involving AiTM attacks and the use of portable programmable devices. There are many portable programmable devices that can be used to perform operations or automate tasks on a computer, and they include devices like the Bash Bunny [5], Rubber Ducky [6], LAN Turtle [7], and Shark Jack [8] to mention a few. Most of these devices are pocket-sized, thereby making them easily portable and not easily noticed or suspected. Some of these programmable devices like the Rubber Ducky and Bash Bunny have a USB interface. Some like the Shark Jack have LAN interfaces. The O.MG cable is able to operate both via USB and wirelessly [9]. The Screen Crab has HDMI (High-Definition Multimedia Interface) interfaces to capture screen data and store on the local storage or send it to a remote command and control server.

The harm caused by portable programmable devices does not end with disrupting system operations or stealing files. The implication of such devices includes a potential for miscarriages of justice where an employee is fired or an individual is punished for the actions of someone else (or in this case, actions of something else). Lawal, et al., [6] demonstrated how a portable programmable device could be used to plant false evidence like false web history and false file downloads on a target machine to implicate the user. This in turn could lead to innocent users being prosecuted for a crime they did not commit as the forensic analyst may mistake the actions of the programmable devices for the target user's. Many cyber-attacks can be achieved through plugin attacks (e.g., Stuxnet [4]), screen monitoring, malware installation, phishing, keystroke injection attack, etc. Many attacks like sniffing, data exfiltration, and data manipulation could be achieved or facilitated by becoming the adversary or man in the middle.

An AiTM attack or MiTM attack is a type of cyberattack where the attacker positions themselves between a communication source and its destination for ill intent [10]. In a network environment, this may be done with the intention of capturing packets to acquire sensitive information [1] from data in transit. It could also be done with the intention of modifying the packets in transit thereby compromising their integrity [11].

An attacker can also gather information about a target through the use of backdoors to create a reverse TCP connection [12] giving them unauthorised remote access to the target machine. The reverse TCP connection could be leveraged to take screenshots at specified intervals. Other types of information that can be stolen through a reverse TCP connection include web cookies and browser history. This approach often requires a clever delivery of the backdoor to lure the victim into clicking so the payload can be executed or installed on the target machine. The implication of this is that there is direct evidence that can be forensically examined or reverse-engineered to study its behaviour and gather other information. This would be to the advantage of forensic analysts; however, to the disadvantage of an attacker who would prefer to leave no trace.

Keystroke logging or monitoring is another means through which sensitive data can be exfiltrated [13]. Keystroke logging is the process of capturing keystrokes on a target computer and can be done using hardware or software [14]. Malicious software keyloggers could be planted on a target by attackers through phishing links, and trojans [15]. Programmable USBs could also be used to capture keystrokes or to install a software keylogger [16].

In the case of information theft or data exfiltration through a reverse shell connection, forensic analysts may still find tangible evidence such as an installed backdoor e.g., rootkits [17] which could be reverse-engineered to get further evidence as to the source and behaviour of the malware [18]. Tools like Wireshark could also be used for packet analysis to investigate a network MiTM attack [19]. Moreover, security solutions such as firewalls, antiviruses, and intrusion detection and prevention systems (IDPS) may be able to detect the presence of a trojan or network MiTM activity [20]. Security policies to prevent data exfiltration via USB may have also been put in place but the Screen Crab is not limited by these security solutions. It is still able to achieve data exfiltration and information gathering covertly without the interference or detection of security solutions or software security policies. The Screen Crab does not use the USB interface, nor does it need a network connection to capture information from the target machine. It acts as an adversary in the middle by abusing the HDMI connection between the target machine and the connected external display.

The Screen Crab does have some limitations, however, which will be discussed in detail in the results section of this paper.

In this work, the possibility of using the Screen Crab to facilitate a crime of fraud is considered, to determine the response of forensics to the use of such a device. Can a forensic analyst easily detect the presence or use of the Screen Crab during an investigation in situations where it might have been used to facilitate a crime or commit a crime?

III. Experimental setup

The experiment discussed in this work forms part of a larger file tampering experiment. The overall aim of this research is to determine the response of the current digital forensics process to the malicious use of portable programmable devices. However, this paper addresses the threats that devices like the Screen Crab pose; particularly their potential of causing a miscarriage of justice if they are not detected during a forensic investigation where they have been used to facilitate or commit a crime. There are three main phases of the attack simulated before the forensic investigation is carried out. The three phases are Reconnaissance, Arming, and Attack phases (see Figure

1). This work focuses on the reconnaissance phase of the wider file tampering attack. The attack phases for the experiment could also be viewed from the Cyber Kill Chain [21] perspective which breaks down the attack into seven steps including Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Action on objectives.

Figure 1 Attack Phases

The Reconnaissance Phase: this is where information is gathered about the target machine, and the environment. This includes information like the physical location of the machine, the operating system of the machine, the kind of physical and logical access needed (e.g., doors, passwords), the available ports on the machine (e.g., USB, HDMI), and the arrangement or format of the user interface. This phase also involves planting the recon device if a hardware device is used for reconnaissance. The tool used in this work as a recon device is the Screen Crab. The gathered information can then be used to more effectively plan and execute the attack. Figure 2 shows the experimental setup for the reconnaissance phase of the attack which is the focus of this paper. Figure 2 also shows the adversary planting the Screen Crab and using the information collected to write a targeted payload which would then be loaded onto the hacking device shown in the wider experiment setup.

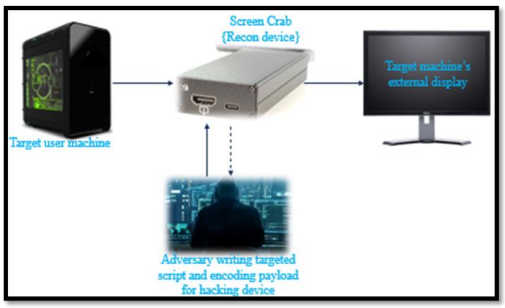

Figure 2 Setup of Reconnaissance Phase

The Reconnaissance phase is the focus of this work, to determine the response of forensics to the recon device used. The Screen Crab was set to video capture mode with a video interval of thirty seconds. The Screen Crab is then covertly positioned between the target system unit and its external display monitor and left to capture the target user's screen for three days simulating a near realistic amount of time needed to gather adequate information for the nature of the larger attack planned. The target system is connected to the Screen Crab's HDMI input interface while the external display is connected to the Screen Crab's HDMI output interface. Relating this experiment to the Cyber Kill Chain, this phase would also be considered as Reconnaissance. The Screen Crab is considered an offline AiTM tool in this work as it does not require network access to capture or exfiltrate data, unlike other methods of becoming the AiTM or MiTM discussed earlier in the literature review.

Arming/Exploit Development: this is the stage where the adversary or attacker uses the information gathered from the reconnaissance phase to develop and test a targeted payload. There is a need to test the payload on a clone of the target machine and environment to achieve a higher level of precision and accuracy when the payload is delivered. The payload needs to be tailored towards the Operating system, and user environment of the target machine as it might not operate as expected if programmed randomly or for a different machine. After the payload has been written and tested, there might be a need to encode the payload into a format the programmable device can process. The Rubber Ducky is an example of a programmable device that requires the payload to be encoded into binary before it can carry out the programmed instructions. In this phase, the attacker encodes the payload if necessary to do so and loads it onto the programmable device to carry out programmed instructions. Relating this to the Cyber Kill Chain, this phase would fall under Weaponization.

Exploit/Attack Phase: this is the final phase of the attack where the payload is delivered, and the target machine is exploited. The attacker plants the programmable device on the target machine when it is safe to do so, for the programmable device to execute the instructions programmed on it. The attacker could also utilise social engineering tactics to get the programmable device to the target machine. Relating this to the Cyber Kill Chain, this phase would cover Delivery, Installation, Command & Control, and Actions on Objectives.

IV. TOOLS AND TECHNOLOGIES

Screen Crab: this is the recon device used for information gathering on the target machine including its operating system, location of files, etc.

Target user machine: this is the target of the attack. The recon device is used to gather information about the user's activities and the location of the target file.

External Display with HDMI support: the external display needs to support HDMI as the Screen Crab has only HDMI interfaces for connection. The external display is connected to the output HDMI interface of the Screen Crab so it can receive data transmission from the target machine.

HDMI Cable: a minimum of two HDMI cables are needed for this kind of attack. One of the HDMI cables connects the target machine to the Screen Crab while the second connects the Screen Crab to the external display as seen in Figure 2.

Micro-SD Card: the Screen Crab requires a micro-SD card for local storage. A minimum micro-SD size of 16GB is recommended for the attack simulated in this work.

Micro-SD Card Reader: this is needed to view or modify the content of the micro-SD card on a computer. Among the content that can be viewed or modified include

the captured images, captured videos, and the Screen Crab's configuration file.

V. EXPERIMENT RESULTS

The results of the experiments are presented here. In this work, the Screen Crab was used for reconnaissance as part of a wider attack; however, it could also be used for standalone data exfiltration or espionage attacks. This raises the question of whether forensics can detect the use or presence of this device, especially when used as an offline AiTM.

A. *Result Overview*

The forensic investigation was conducted using industry-standard digital forensic tools Autopsy and FTK Imager and Registry Viewer. The results of the investigation were unable to detect any trace of the Screen Crab. This makes it near impossible for a forensics analyst to detect its presence.. Some risks associated with this include facilitating data exfiltration, or espionage which could lead to accusing an innocent person of divulging sensitive information, as the Screen Crab leaves very little to no forensics evidence. This may yield unreliable digital evidence leading to a miscarriage of justice (i.e. an innocent individual being punished or a guilty person walking free).

While the Screen Crab was operational, there were no signs such as lag or latency on the external display to raise suspicions to the target user that their computer connection had been tampered with. In addition, there was no drop in image quality on the external display which may have also been a cause for alarm.

Moreover, a stand-alone analysis was carried out on two different laptops including a Microsoft Surface Pro and a Toshiba laptop with Windows 10 installed. The computers detected only the monitor on the other end and not the Screen Crab in between. This suggests the Screen Crab works just like an HDMI splitter and requires no drivers to function. It relies solely on the signal going through the HDMI and so leave no trace on the registry.

In situations where the Screen Crab has been used against a target user who is the custodian of top-secret information related to national security, they may be falsely accused of disclosing classified information and charged with treason [22] [23].

The use of USB devices to extract data or steal files may still leave some traces like the product ID (PID) and Vendor ID (VID) [9]. However, the Screen Crab does not require any drivers and leaves no obvious Hardware ID that may have been an indicator of its use or presence to the forensic analyst during an investigation. The Screen Crab uses the HDMI interface and as mentioned, works like an HDMI splitter.

The Screen Crab can also use a Wi-Fi connection to gain access to the internet and communicate with a command and control (C2) server. However, it was used in an offline mode in this work. With Internet access, the Screen Crab can receive instructions from the remote C2 server, can store the captured files on the remote server, and can provide a live feed of the target screen to the adversary via the C2 server. If the wireless connection was used, it may be possible to use a tool like Wireshark to capture the traffic and see what kind of packets are being transmitted as seen in [19].

B. *Operational Observations of the Screen Crab*

The captured images are high resolution and are clear enough to pick out every detail on the screen (e.g., see figure 4). Picture quality is sharp and there is no evident effect of the screen crab on the functionality of the user's display. There was no drag, no delay, no break in transmission, and no cracks or shakes that would have led to the user attempting to check the connections.

The captured file sizes are not large which means the capture process for images is not storage intensive. The captured videos had varying file sizes with an average file size of 2MB. The Screen Crab can also detect when the computer screen is inactive (or off) and stops capturing. The Screen Crab resumes screen capture once it detects the computer screen being active again. This feature further increases the Screen Crab's storage efficiency as it prevents the capture of blank videos that would take up unnecessary space. There are two options for storage; either ROTATE or FILL. The FILL option continues the capture until the Screen Crab's storage is filled up whereas the ROTATE option continues the process while replacing the oldest files with the newest when the Screen Crab's local storage is full.

During the simulated attack, the Screen Crab was also not able to transmit audio despite its connection via HDMI which should be able to transmit audio. This may lead to the target user discovering the Screen Crab while attempting to troubleshoot.

C. *Using the Screen Crab Against Touchscreen Devices*

Figure 4 below is a screenshot from a video capture of the Screen Crab while the system user was entering their Windows logon password. The target machine used here was a Microsoft Surface Pro PC running Windows 10 operating system with its firewalls and the Microsoft

Figure 4 Screenshot from captured video during user logon

Windows Defender antivirus program active. Neither the firewall nor the MS Defender detected nor flagged up the Screen Crab while it was operational. As could be seen in figure 4, every keystroke or screen tap is picked including the user login password as the keys are pressed.

D. Limitations of the Screen Crab

The Screen Crab has only HDMI interfaces which means it might be useless against a computer and/or external display that has no HDMI ports. This would only be a limitation to the attackers who have no knowledge of alternative ways to use HDMI connections on devices that have no HDMI ports. This limitation could be overcome through the use of converters (e.g., VGA to HDMI converters or Display port to HDMI converters, etc.). It might be a slightly more complex improvisation, but it will get the job done on many systems.

The Screen Crab also requires physical access to be planted and to be removed which could be a setback for the attacker in certain situations. However, this limitation could be overcome through well-executed social engineering as seen in [24]. This would not be a limitation for personnel or individuals who would normally have access to the target machine's location e.g., office colleague, IT support, system administrator, janitors, security personnel or facility managers.

The Screen Crab requires a power supply through a USB Type C cable to function. No capturing can be done while it is turned off. Hence, proximity to a power source or a covert USB port for power is paramount for the successful operation of the Screen Crab.

Another limitation of the Screen Crab is that it does not transmit audio. HDMI is capable of transmitting both audio and video and in some situations where the target user expects audio to be transmitted, the absence of audio on the external display may raise concern e.g., if the target machine is connected to a TV that would normally play sound. This may prompt the user to troubleshoot the problem and may then lead to the discovery of the Screen Crab.

VI. Conclusion

This work demonstrates how a portable programmable device like the Screen Crab can be used to steal information anonymously from a target computer without much evidence left for investigators or forensic analysts to find. The investigation was conducted following an industry-standard forensic process and the use or presence of the Screen Crab on the victim's computer was not at any point flagged during the investigation. This increases the risk of a miscarriage of justice because an innocent person (the user of the target machine in this case), could be punished or prosecuted for an offence they did not commit. Possible repercussions for the victim include termination of employment, or in cases where non-disclosure agreements have been signed, they could be sued for a huge sum of money, or even worse, they could be prosecuted for divulging classified or top-secret information without authorisation. The user of the target computer could be charged with treason for such offences [22].

There are also security implications for individuals, organisations, or countries whose sensitive information might have been leaked through the use of devices like the Screen Crab. Such implications include a threat to national security, and facilitating espionage of organisations and countries. The possible applications of portable programmable devices are only limited by the creativity of the attacker.

In addition, there were no indicators on the external display (e.g., quality drop, lag/latency) to suggest to the target user that any form of tampering was taking place on their machine. This paper also shows how it might be difficult for forensic analysts to detect the use of this device which poses a risk of the target user (victim) being falsely accused or wrongly prosecuted for divulging sensitive or classified information in this kind of situation.

The experiment results indicate that the current digital forensics process may not be effective enough in combatting the use of portable programmable devices like the Screen Crab in situations where it has been used maliciously to commit a standalone crime or facilitate a larger attack. This means the evidence could be missed in the investigative stage by the forensic analyst and might also be missed in the expert presentation in court. This could potentially lead to a faulty conclusion in the court of law, as it looks like an open and shut case. Forensic investigators need to be aware of the potential of devices like the Screen Crab for spying or stealing confidential data and the subsequent potential for a miscarriage of justice.

In addition, this shows the need for a methodology for digital forensic investigations that could guide forensic analysts during an investigation to reduce the chances of missing evidence like this or at least consider its possibility in scenarios where its use is possible.

Investigations into this are still ongoing and future recommendations include investigating the Screen Crab's remote connection to the C2 server using Wireshark and other network investigation tools to determine the kind of information being transmitted. In addition, this may also provide information as regards the Screen Crab's indicators of compromise (IoCs).

References

[1] Nayak, G.N. and Samaddar, S.G., 2010, July. Different flavours of man-in-the-middle attack, consequences and feasible solutions. In 2010 3rd International Conference on Computer Science and Information Technology (Vol. 5, pp. 491-495). IEEE.

[2] Tuli, R., 2020. Packet Sniffing and Sniffing Detection. International Journal of Innovations in Engineering and Technology, 16(1).

[3] Saputra, D. and Riadi, I., 2019. Network forensics analysis of man in the middle attack using live forensics method. International Journal of Cyber-Security and Digital Forensics, 8(1), pp.66-73.

[4] Shaikh, R.A., Khan, M.S., Rashid, I., Abbas, H., Naeem, F. and Siddiqi, M.H., 2022, May. A Framework for Human Error, Weaknesses, Threats & Mitigation Measures in an Airgapped Network. In 2022 2nd International Conference on Digital Futures and Transformative Technologies (ICoDT2) (pp. 1-8). IEEE.

[5] Zhao, S. and Wang, X.A., 2020. A survey of malicious HID devices. In Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019) 14 (pp. 777-786). Springer International Publishing.

[6] Lawal, D., Gresty, D., Gan, D., and Hewitt, L., 2021. Have You Been Framed and Can You Prove it? In 2021 44th International Convention on Information and Communication Technology, Information System Security (MIPRO). IEEE.

[7] Slunjski, M., Sumina, D., Groš, S. and Erceg, I., 2022. Off-the-Shelf Solutions as Potential Cyber Threats to Industrial Environments and Simple-To-Implement Protection Methodology. IEEE Access, 10, pp.114735-114748.

[8] Hak5 (n.d) Shark Jack, Hak5. Available at: https://shop.hak5.org/products/shark-jack (Accessed: February 6, 2023).

[9] Lawal, D., Gresty, D., Gan, D., Hewitt, L. (2022), 'Facilitating a Cyber-Enabled Fraud Using the O.MG Cable to Incriminate the Victim', World Academy of Science, Engineering and Technology, Open Science Index 189, International Journal of Computer and Systems Engineering, 16(9), 367 - 372.

[10] Mallik, A., 2019. Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), pp.109-134.

[11] Bhushan, B., Sahoo, G. and Rai, A.K., 2017, September. Man-in-the-middle attack in wireless and computer networking—A review. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-6). IEEE.

[12] Tigner, M., Wimmer, H. and Rebman, C.M., 2021, October. Windows Reverse TCP Attack: The Threat of Out-of-Date Machinery. In 2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 555-560). IEEE.

[13] Akhtar, Z., 2021. Malware detection and analysis: Challenges and research opportunities. arXiv preprint arXiv:2101.08429.

[14] Singh, A. and Choudhary, P., 2021, August. Keylogger detection and prevention. In Journal of Physics: Conference Series (Vol. 2007, No. 1, p. 012005). IOP Publishing.

[15] Ayap, N.R.D., Dabu, A.C.Y., Reyes, A.M., Ventura, A.B.K., Trinidad, G.P. and Blancaflor, E.B., 2022, Beat the Bait: A Case Study on Phishing Attack.

[16] Charan, B.V., Kulkarni, L. and Karad, V., 2023. Survey On Micro-Controller Based Bad USB Attacks. Journal of Positive School Psychology, pp.965-974.

[17] Abuzaid, A.M., Saudi, M.M., Taib, B.M. and Abdullah, Z.H., 2013. An efficient trojan horse classification (ETC). International Journal of Computer Science Issues.

[18] Bao, C., Forte, D. and Srivastava, A., 2015. On reverse engineering-based hardware Trojan detection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 35(1), pp.49-57.

[19] Lan, H., Zhu, X., Sun, J. and Li, S., 2020, January. Traffic data classification to detect man-in-the-middle attacks in industrial control system. In 2019 6th International Conference on Dependable Systems and Their Applications (DSA) (pp. 430-434). IEEE.

[20] Aliyu, F., Sheltami, T. and Shakshuki, E.M., 2018. A detection and prevention technique for man in the middle attack in fog computing. Procedia computer science, 141, pp.24-31.

[21] Cyber kill chain® (2022) Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[22] Fabre, C., 2020. The Morality of Treason. Law and Philosophy, 39(4), pp.427-461.

[23] Dobrovidova, O., 2022. Russian scientist facing treason charges dies in custody. Science, 377(6604), pp.355-356.

[24] Bakhshi, T., 2017, December. Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors. In 2017 13th International Conference on Emerging Technologies (ICET) (pp. 1-6). IEEE.