Mobile Device Security

Scenario

In 2022, at the Royal Military Academy Sandhurst, where the officer in charge conducted a workshop for students to explain the college's goal, which is to be the center of national leadership excellence, and accordingly, there must be distinguished officers, educationally and militarily, to keep pace with external developments.

Where the workshop included an exchange of information, where the officer in charge presented his lecture and shared all the files presented through the Microsoft Team program and instructed all the students and guests to connect all their devices (phones, iPads, tablets, laptops) to the network provided by the academy, where he shared for the network name and password via the smart board.

He asked all the attendees to download the files that he had uploaded, and told them that in the event of a need for an inquiry or question, this could be done through the chat in the Team program by raising the hand and writing what was on their minds so that the questions and answers would remain archived for them to benefit from later, as he held a meeting on The team program and invited them to it through their e-mails, and after completing the lecture, everyone was asked to fill out the form in the files with the information learned from the lecture and to put suggestions and new ideas to develop the educational process and re-share it through the team . Where all questionnaires will be displayed via the smart board to be discussed.

Prepare a report
From above scenario Explain the ways used to connect malwares and sniffing devices to mobile devices and assess them.

Students Work

In the Above scenario described that during the workshop at Royal Military Academy Sandhurst. There are many security concerns about malware risks and monitoring devices via sniffing attack.

Following are the Risk Factors:

1- Email Invitations:
At workshop the officer invited audience to join meeting through link he shared through Email link. All attendees click that link without investigating the source of link as it is legit or not. As this link could potentially link to the malware website which could further exploit users. This can be a great Cyber Security attack surface so all attendees must double check

the source of the link origination before clicking as the links provided in the email invitations were compromised, it could lead to malicious actors gaining access to devices through phishing attacks or malicious attachments.

2- Network connectivity:
In above scenario the officer asked all the students and guests to connect their devices such as mobile phone and laptops to the Wi-Fi-network provided by the academy. This connection creates vulnerability that can possibly allow attacker to perform MITM (Man in the Middle) attack. Also There are different Wi-Fi attacks such as Wireless Packet Sniffing Brute Force Attacks Dictionary Attacks Evil Twin Attack Man-in-the-Middle (MitM) Attack Denial of Service (DoS) Attack De-Authentication Attack WPS (Wi-Fi Protected Setup) Attack that are possible by just connecting to Wi-Fi Network.

3- File Sharing via Microsoft Teams:
The File sharing feature in Microsoft Teams program that allow the sharing of files with different people in the meetings. Malicious Actors such as hackers can share the malicious files such as Virus and Malware files that could be named as legitimate ones, exploiting vulnerabilities in software or executing malicious code upon download or opening.

4- Interaction through Chat:
The audience were encouraged to interact through the chat feature that allows different people to talk with each other. But the problem here is that Malicious actors can exploit vulnerabilities in the chat system to inject malware or phishing links, potentially compromising devices that are communicating via chat system. Which can potentially cause damage to the people using that chat system.

5- Malware Infection: There is a risk of malware infection that attendees can be infected if they download, interaction in chat or compromise email Infection. Malware could include viruses, ransomware, spyware, or Trojans designed to steal sensitive information or disrupt operations.

6- Smart Board Connectivity:
In this scenario there is a possible chance of the disinfection of smart board connectivity. For example: the smart board has a computer inside that is using a kind of microprocessor and RAM and dedicated system. And it for sure contains Operating System. If the Smart board is not properly updated it could create a risk of Malicious actors could exploit vulnerabilities in the smart board's software or network protocols to gain access to connected devices or intercept data.

Conclusions:

To conclude the findings, the scenario at the Military Academy Sandhurst describes the different vulnerabilities and risks associated with malware infection and device monitoring. In the workshop we concluded there are many ways in which attendee's

devices can be exploited such as E-mail invitations, Network connectivity, File sharing and Chat system cause potential avenues for cyber-attacks. So Awareness is very important to protect our self from different attacks and we can safely use the Internet and Technology.

References:

1- Curran, K., Maynes, V., & Harkin, D. (2015). Mobile device security. International Journal of Information and Computer Security, 7(1), 1-13.
2- Halpert, B. (2004, October). Mobile device security. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 99-101).
3- Engel, M. M., Ramadhan, A., Abdurachman, E., & Trisetyarso, A. (2022). Mobile device security: a systematic literature review on research trends, methods and datasets. Journal of System and Management Sciences, 12(2), 66-78.