eForensics Magazine

MAGAZINE

MOBILE FORENSICS STARTER KIT

MOBILE FORENSICS 101

DIGITAL INVESTIGATION PROCESS IN MOBILE DEVICES

PAINTING THE BIG PICTURE:
STRATEGIC INSIGHTS ON MOBILE DEVICE SECURITY

CONDUCTING FORENSIC ANALYSIS IN MOBILE DEVICES

EMAIL FORENSICS

VOL.10 NO.06
ISSUE 06/2021 (122 JUNE
ISSN 2300 6986

TEAM

Publisher
Hakin9 Media Sp. z o.o.
02-511 Warszawa
ul. Bielawska 6/19
Phone: 1 917 338 3631

www.eforensicsmag.com

Word from the team

Dear Readers,

Mobile devices are nowadays an inseparable element of our reality. Probably none of us can imagine functioning without a smartphone, and tablets replace books, TV sets, or computers. These devices are also data carriers that can be a real treat for a forensic analysis specialist.

For this reason, this month we have prepared for you a magazine devoted to Mobile Forensics, dedicated to people who want to start their adventure in this field of forensics. Our wonderful authors have prepared texts that introduce this topic, describe the basic concepts, and show how to conduct specific investigations using various techniques step by step.

In the journal you will find, among other things:

- ***answer to the question about what Pegasus is,***
- ***a tutorial on how to extract and analyze data from iOS and Android devices,***
- ***tips on how to secure mobile devices to ensure the security of corporate data (VPN, NAC),***
- ***an explanation of the difference between mobile forensics and computer forensics,***
- ***a tutorial on how to use Oxygen Forensics Tool,***
- ***a guidebook, from which you will learn the forms of data extraction from mobile devices, what tools are most useful in specific data extraction cases (Cellebrite UFED Touch, MicroSystemation XRY), and how to prepare an analysis report!***

So if you want to learn mobile forensics, but expand your knowledge about securing mobile devices in your organization, be sure to reach out for this edition!

Check out our Table of Contents below for more information about each article (we included short leads for you).

We hope that you enjoy reading this issue! As always, huge thanks to all the authors, reviewers, to our amazing proofreaders, and of course you, our readers, for staying with us! :)

Have a nice read!
Regards,
Michalina Szpyrka
and the eForensics Magazine Editorial Team

Table of Contents

Effective Ways To Improve Business Firm Network Security

by Ahmed Adesanya

Dealing with security breaches is a real challenge for many organizations, and the threat of losing sensitive data is significant. It is critical to be ready for them because threats are unquestionably growing and changing. According to the recent Cybersecurity Ventures 2022 "Cybersecurity Almanac," organizations will spend approximately US$1.75 trillion on cybersecurity between 2021 and 2025 (https://cybersecurityventures.com/cybersecurity-almanac-2022/).

At the same time, by 2025, it is projected that cybercriminals and their activities will earn around $10.5 trillion. That means that cybercriminals will earn almost six times more in revenue than defenders will spend! It is a fair question to ask how these malicious cyber actors (MCA) can be so far ahead of their defender counterparts.

To begin with, all MCAs have negative intent. This negative intent could be as simple as defacing a website or as advanced as stealing intellectual property.

Recent research from IBM (https://www.ibm.com/security/data-breach) indicates that the average total cost of a data breach has grown to US$4.24 million, and a study from the Ponemon Institute (https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf) found that companies' stocks drop an average of 5% on the day that a data breach is announced. As you can see, the negative financial impact of a severe cyber incident is serious business.

The best organizations develop a culture of security (https://www.cpni.gov.uk/security-culture). This is especially important now, since most security firms agree that social networking sites will be a major channel for malware and other scams aimed at luring unsuspecting people to infected web sites. Also, threat actors may leave behind a digital footprint that must be closely examined in the aftermath of an attack. Proper logging (https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html) plays a big role here. If you aren't gathering logs, even the best cyber forensics team may not be able to accurately recount all the details of the incident, such as the timeline of events and insights into how the hackers were able to move laterally throughout different parts of the network.

Encryption is another area to focus on. Full device-level encryption can hamper performance and battery life, but it means all data are effectively unreadable, even if a device finds its way into the wrong hands. It's also less complex than file- or folder-level encryption with regard to data classifications and user interaction. In short, full encryption has become a must-have for any user with high-level access to ensure compliance with policies and regulations. Depending on your use case, you may need to consider third-party encryption products that can protect the phone as well as its removable SD cards or Internet of Thing (IoT) equipment—in fact, this may be necessary to meet certain data and regulatory requirements.

While security technologies like encryption can go a long way toward mitigating risk, good policy planning and enforcement can do even more. The following need to be considered:

- Smartphones should never be allowed to store personal information about customers or intellectual property.
- Access to the corporate network using a smartphone should be based not only on the user's role in the business, but also on his or her location and the connection used, such as from inside or outside the corporate network, or through a VPN. For example, a connection via an unsecured Wi-Fi network that is not going through the corporate VPN should be blocked.
- VPN access should also be restricted to specific business tasks, as an 'access all areas' approach is not necessary and is too risky.
- Accurate logging, on the other hand, enables your organization to develop strategies on how to catch suspicious activity as early as possible in order to prevent similar attacks in the future. Setting up automatic alerts in a tool, such as security information and event management (SIEM) software, will

let your security team know when something unusual is going on so it can be investigated as soon as possible.

- Extend network access control (NAC) technology to provide the necessary checks to establish a phone's access rights based on its patch and antivirus status and application configurations.
- Because security is a moving target, organizations must keep their ear to the ground to understand and combat emerging threats and methodologies on an ongoing basis. Usually, only larger organizations and enterprises can justify the cost of a dedicated threat intelligence team. Small to medium-size businesses should purchase tools to help fill these gaps and be sure they are correctly configured. Correctly configured technology, coupled with cybersecurity experts, will help your organization safeguard against the latest tactics hackers are using.
- People take all kinds of measures to protect their most valuable assets. Organizations should be doing the same thing to protect their data center systems, which are their most valuable assets. Their protection mechanisms can be categorized into five layers: physical, logical, network, application and information security.
- Use Mobile Device Management/ Device management (DM) to manage or deny access and remotely wipe data from lost or stolen devices.

Users need to appreciate that losing a smartphone is not just an inconvenience; it might also be the cause of a data breach, so there has to be a strong focus on avoiding loss or theft. To reduce theft or misuse, your enterprise should conduct risk training for end users that emphasizes information asset ownership and physical security awareness. It should also consider stronger disciplinary measures, including suspension or even termination in the event of a serious breach of policy, to focus employees' attention on safeguarding their phones and IoT equipment.

Effective risk management includes adapting quickly to new security threats and is crucial to getting the most benefit out of smartphones and other IoT equipment.

About the Authors

Ahmed Adesanya - MBA, CRISC, CGEIT, ACMA, ACPA. Patent on Enabling MDM on TV white space devices. IT Consultant, Petrovice Resources Int'l Ltd., Nigeria

Contact: luciano.quartarone@archivagroup.it