hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.16, NO. 04

ANDROID HACKING

Android for Pentesters and Networks

Mobile Threat Landscape

Kali NetHunter

Build your own Malware

AND MORE...

TEAM

Publisher
Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Bielawska 6/19
Phone: 1 917 338 3631

www.hakin9.org

Betatesters & Proofreaders

Lee McKenzie

Hammad Arshed

Bernhard Waldecker

Avi Benchimol

Amit Chugh

Kevin Goosie

Craig Thornton

Paul Mellen

Tom Updegrove

Christopher Pedersen

Bhuna Selvadurai

Girshel Chokhonelidze

Daniel W. Dieterle

Ricardo Puga

Ivan Gutierrez Agramont

Alex Giles

Dear Readers,

Smartphone and mobile are powerful industries these days - and each year they become larger and have a bigger impact on our lives. Almost everyone has their own mobile device and because this topic is so important and current, we decided to dedicate this month's issue to Android Hacking. Here's what we prepared:

We start off with Android for Pentesters and Networks, in which the author covers the best tools and techniques for mobile pentesting. Then we drift off to KaliNetHunter - For Those That Have Fear of Commitment - in this article you'll learn how to use rootless Kali NetHunter on your mobile phone.

In Mobile Threat Landscape the author discusses threats, mitigations and best practices in mobile security. Later on we have Introduction to Reverse Engineering of APKs - and the title speaks for itself.

If you're interested in mobile RATs, we also prepared a piece on Spynote - in this article the author covers the Spynote tool and presents examples of usage. You may also want to check out DIVA (Damn Insecure and Vulnerable Application) in which the authors present you the DIVA tool and cover all the techniques you can use it for.

If you're hungry for more offensive topics, we suggest you take a look at Build Your Own Malware, in which the author explains how to build a keylogger and a botnet, all in compliance with the principles of safety.

But there's more! We also prepared articles touching the topics of phishing, Dark Web, OSINT, vulnerability scanning - all the things that are becoming more and more important, especially during the pandemic.

We hope this issue will help you learn something new and prepare for whatever and whoever is waiting to hack your smartphone. We would also like to send gratitude to our contributors, reviewers and proofreaders, who helped us create this unique issue!

Stay safe and enjoy!

Hakin9 Editorial Team

Contents

MOBILE THREAT LANDSCAPE

SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering and Cyber Security teams.

"Oh, oh, telephone line, give me some time
I'm living in twilight
Oh, oh, telephone line, give me some time
I'm living in twilight"

— Electric Light Orchestra 1976

Introduction

The world as we know it today would have been a much different place had it not been for a revolutionary invention called the telephone. From its humble beginnings in 1876 (and often credited to Alexander Bell although there were others) as a means of delivering voice messages over the wire to the age of the smartphone delivering all manner of content wirelessly, this single device alone has had the power to transform the lives of billions of people around the world.

The modern era smartphone is so much more than a simple voice messenger to its billions of users. With the power of the internet in its sails, an ever-expanding apps ecosystem and the widespread adoption of generational high-speed broadband networks the smartphone of the 21st century delivers all manner of content besides audio, such as video, music, or financial information all seamlessly over the airways.

However, as in the inimitable words of Spiderman, "With great power comes great responsibility", as enterprise IT mobile devices now pose a new threat landscape and expose a surface footprint as diverse and unregulated as its user base. Mobile devices (smartphones and tablets) now represent the largest single computer device growth sector with established heavy-duty corporations vying for customer loyalty and attention. The pandemic has only accelerated their adoption for remote working, home schooling and binge-watching streaming services from Netflix and Amazon. At the height of the pandemic, as much as 68% of the American labor workforce was working from home full-time. The agility with which this paradigm shift in working modes was made possible was mostly based on the ability of enterprises availing their existing employees' mobile devices and the user's enthusiasm to utilize them for their regular work. Attempting to provision the number of required dedicated certifiable devices for the full workforce in such a short timeframe would have put a massive strain on the supply chain process and vendor delivery commitments.

Mobile devices present some unique challenges for enterprise IT shops that need to be addressed with a balanced strategy that allows users their freedom yet keeps private corporate data '*sandboxed*' and safe from prying eyes and enterprise applications secured to the finish line.

BYOD Conundrum

The usage of employee owned mobile devices (smartphones, tablets and personal laptops) in enterprise IT environments is called “BYOD”.

As defined by Wikipedia: *"Bring your own device BYOD — refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device ...in the workplace, where it refers to a policy of permitting employees to bring personally owned devices (laptops, tablets, smartphones, etc.) to work, and to use those devices to access privileged company information and applications. This phenomenon is commonly referred to as IT consumerization."*

With the majority of IT staffers being reluctant to go back to the old way of working, BYOD is here to stay for the foreseeable future and enterprises will need to address its important challenges, such as data leakage, unauthorized access and malware infection, in a deliberated and formally organized way.

Policies and Procedures & Mobile Device Management (MDM)

At the core of most corporate defensive strategies (and usually in line with the security framework they have adopted) are up-to-date policies and procedures that address the nascent threats posed by BYOD usage by their employees. Mobile Device Management (MDM) allows for the administration of user and application rights management on all manner of mobile devices such as mobile smartphones, tablets and laptops.

Besides regular review and due diligence, these steps are only meaningful when backed up by the installation of a third-party Mobile Device Management (MDM) solution that will help to enforce the best practices outlined within the policies and procedures. All the major players offer competing solutions that vie for your attention. Without an MDM solution in place, all paper policies will remain ineffective in securing the corporate network access via mobile devices.

Modern MDM solutions are based on a dual component strategy:

- A server component whereby the IT administrator can configure and send out policies via a management console interface to mobile devices.
- A client component that receives messages and implements commands from the server component on the end-user mobile device.

All available solutions typically center around perimeter/sandbox context with threat containerization as a principle. The MDM container is unique in that it typically uses cryptographic methods to secure corporate data on the mobile device and rigorously prevents attempts to move data across the data barrier from corporate into personal terrain on the device. The core objective remains to secure and process corporate data (such as emails, documents and applications) within the container itself. Both the level and manner of encryption will be a key factor depending on the solution adopted.

There are typically four major areas that are addressed by the MDM solution:

Email Security: This is a critical part of the MDM deliverable allowing enterprises to integrate their internal email product of choice (MS Exchange Server, Office 365, Lotus Notes, etc.) with the MDM solution. Ease of use in configuring and flexibility in options are key factors for consideration in selecting the right product fit for the enterprise.

Document Security: MDM solutions typically restrict all employee requests across the container barrier and attempts to download or copy corporate attachments to the personal device storage. The ability to restrict or disable clipboard movements across the container barrier is a huge advantage for device administrators. So too is the ability to prevent forwarding of attachments to insecure external or unknown domains as is saving to internal storage.

Browser Security: Typically, the MDM solution adopted will be supplied with its own custom-built internal secure browser thereby avoiding many further security risks. MDM provides flexibility to admins to disable standard personal browsers inside the container forcing users to use the secure browser in all instances. Administrators may need to address questions from users or provide some level of training as the custom-built browser supplied is rarely at par with their commercial counterparts. At worst, some of the latest CSS standards may not have been fully implemented yet but should be sufficient for general purpose usage.

App Catalog Security: The MDM solution also allows enterprises to distribute and manage applications within the container on the employee's mobile device. This allows flexibility in adding, upgrading and deleting applications at will. The App Catalog also provides a perfect venue to host enterprise specific, internally developed, private applications without having to publish them through the respective App Stores for iOS and Android.

Secure Remote Data Wipe: Allows admins to remotely (and securely) wipe clear all corporate data on the device. This may be one of the best features of the MDM solution in cases where the mobile device has been lost or fallen into the wrong hands.

Secure Remote Device Wipe: Allows admins to remotely execute a full device wipe if required. This is also a critical enterprise requirement at times when there may be no hope of recovery or retrieval of the mobile device.

Secure Remote Lockout: Allows admins to remotely secure the device by locking out all individuals. May be subsequently followed by a data and device wipe as well based on the circumstances.

In summary, all of these features make the MDM product an indispensable tool in the armory of the IT enterprise security team.

Am I hacked? What next?

Phone hacking has become a routine phenomenon these days and, although troubling, is not as surprising as before. If your mobile device is hacked, time is of the essence, as hackers will use every second to exfiltrate data out of your device and start a string of operations using the harnessed data.

If you suspect that your device may have been hacked, you should look for some unusual but telltale signs or behaviors on your device that can confirm your suspicions.

Unfamiliar Text messages or Calls: If you begin to notice a number of text messages or calls that were not made by you, then there is a high probability that your mobile device may have been hacked or is under the control of others.

Strange or inappropriate notifications: If you start receiving inappropriate rowdy or racy ads with X-rated content suddenly, it may indicate some type of malware or phishing attack upon your device. Assuming you're not burning the midnight oil on adult only porn sites, this should raise the alarm for you immediately.

Unexpectedly High Data Usage during normal operation: Although there may be several reasons for this, based upon the number and variety of apps on your device, if you begin to notice a sudden spike in data usage, there may be reason to investigate further and to be alerted to what is happening under the hood.

New or unknown Apps installed: If you begin to see completely new or unknown apps appearing on your device all of a sudden (that you are sure you never installed yourself), there may be malware to blame and your device may be under outside control.

Quick Battery Drain: If your device usage has consistently remained the same day-to-day or week-to-week but your battery seems to be draining too quickly recently, then hacking may be behind the rapid drainage behavior.

Best Practices and Mitigations

If you are certain that your mobile device has been hacked on account of your observations, there are a number of simple steps that you should take to reduce exposure and the ultimate damage that will take place thereafter.

Here are a few best practices and mitigation strategies to be considered:

Inform Contacts: Let your contacts know your current situation as the first order of the day for hackers will be to rifle through your contact list and approach them next for further malware expansion. Ask them to be suspicious of any strange text messages or requests from your mobile number or suspicious links that may lead to further malware infection.

Delete Suspicious Apps: The first step is always to identify the "critical" data that may be the target of the insider threat. This is no small endeavor and will possibly require the formation of a dedicated team with cooperation between IT, Human Resources, Finance and Audit to identify vulnerable data and how best to secure and limit its exposure on the mobile device to the applications installed.

Install and Run Anti-Malware Software: The next logical step after the Data Classification stage completes is the implementation of a best of breed DLP tool. This is an essential accessory in the struggle to prevent unlawful exfiltration of data from any organization.

Full Factory Reset: This may be the final option to bring your device back to its initial stage without the malware in order for you to set up from scratch again like new.

These are just some simple basic measures that can be taken to reduce your exposure surface and get you and your mobile device back on your feet.

Conclusion

With the advent of the COVID-19 pandemic there are few things to be cheerful about. If anything, the pandemic has exposed the fragility of our systems and made us fearful of the stress and mental health inducing fatigue of the perpetual "lockdown state". Thankfully being where we are on the technology curve (as opposed to the Spanish Flu era) organizations were able to scramble their teams and pull together required technologies to make remote working possible at scale. Maintaining a rigorous policy and implementing an appropriate MDM tool will shelter many from the dire risk factors that BYOD device users fall victim to.

References

Wikipedia Definition: https://en.wikipedia.org/wiki/Bring_your_own_device