

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.18, NO.04

SECURITY IN THE AGE OF AI

ZERO TRUST SECURITY COMPENDIUM

WHAT IS ZERO TRUST NETWORK ARCHITECTURE?

THE DEVELOPMENT OF ZERO TRUST SECURITY.

SECURITY OF ZERO TRUST

POST-AI MARKETING – MORE HUMAN THAN EVER

FROM SEH OVERWRITE WITH EGG HUNTER TO GET A SHELL

KEYS TO MITIGATING INSIDER THREATS

AND MORE...

proofreader Lee McKenzie

issue cover Hiep Nguyen Duc - Wiktoria Bukowska

reviewers Salman Aslam - Juanvb Petere - Frédéric Crequer - Paul Mellen
Craig - Gabriel Carvalhaes - Michal Jachim - Volker Skwarek
Alexandre D - Matthew Sabin - Zaher el-Siddik - Alex Lucas
Bev Robb - Jay Kay - Da Co

01	How the Human Factor Plays a Role in Android Security
05	Keys to Mitigating Insider Threats
10	Interview with D4RKR4BB1T
14	7 Essential Tips That Helped Me to Get into Offensive Security
24	Post-AI Marketing – More Human than Ever
30	Privacy: Protecting Your Personal Information Online
38	What is Zero Trust Network Architecture (ZTNA)?
51	Security of Zero Trust
69	The Development of Zero Trust Security
83	From SEH Overwrite with Egg Hunter to Get a Shell

INTRODUCTION

Wiktoria Bukowska

Dear Readers,

(honoring the theme of this issue we collaborated with ChatGPT on this first paragraph)

"In today's world, AI has become an omnipresent force. From virtual assistants to personalized healthcare solutions and autonomous vehicles, its integration is all-encompassing. In this issue, we explore the implications of Artificial Intelligence pervasiveness and the security challenges it brings. Join us as we navigate the ever-evolving landscape of 'Security in the Age of AI.' "

The future is truly bright and it's coming upon us faster than we could imagine. Protecting oneself is a human right, and we're very passionate about this and honored that we can collaborate with such informed experts.

In this issue, we're approaching security from different perspectives. You will find articles on insider threats as well as protecting your privacy online. D4RKR4BB1T, the author of our Hakin9 Crime Corner, agreed to give us an exclusive and uncensored (despite the risks!) interview about his work in the cyber investigation. We're also excited to publish a three-text compendium about zero trust security's history, architecture, and development. André Ricardo, a cybersecurity specialist from VIVO composed his list of essential tips on getting into the offensive security industry. After that, you can delve into the fascinating topic of how artificial intelligence tools affect modern marketing, by content marketing consultant Kuba Czubajewski.

We're very proud of this issue and hope it will be the start of important conversations and ideas. Delve in!

Wiktoria Bukowska and the Hakin9 Editorial Team

Mohammad Hossein Heydarchi

How the Human Factor Plays a Role in Android Security

When it comes to security, we should have a thorough understanding of how various components impact and interact with it. It is essential to consider security as an integrated system made up of various modules, activities, etc. Of course, we can say that some factors would have a greater impact if they were disregarded. We are going to take a look at the human role in Android security. A brief discussion of user data and privacy will be followed by a review of the most recent top malware and threats.

Each operating system has its own security features and privacy and data protection measures. This means that the threats act in different ways to get access to our private data. One thing they have in common, though, is how the user can be seduced and persuaded to take the first step (maybe we can say how the first mistake can take place) to open the gate for an attack. As long as the user is aware of what he/she is being asked, the most powerful system guard is up and will not be knocked down. By checking the sender's email addresses, links, etc., and alerting the user of any likelihood of fraud, the majority of Android vendors now offer some protection against phishing and other threats. However, it is clear that because the attackers have advanced in sophistication and the complexity of their scenarios, filtering spam emails and messages is no longer sufficient.

The most common ways to install malware are listed below:

- Being part of another app
- Install from 3rd party app stores
- Direct download & install via links

Despite advancements in Google Play malware detection over the past few years, we continue to hear reports of infected applications being

downloaded and installed on numerous mobile devices. The methods used today to conceal malicious code have evolved to steal user data while they are trying to be out of sight. We must realize that the challenges we face today and in the future are distinct from those of the past, and more challenging. Our policies and equipment need to be updated. Some traditional ideas, like user awareness and education, nevertheless, continue to be effective. Although we must admit that we can not just rely on that, the security system needs to be improved.

Some tips to minimize malware threats:

- Download from Google Play Store and official websites
- Pay attention to requested permissions
- Not following/clicking on untrusted and unknown links/URLs
- Update system and applications regularly
- Don't use mobile phones that are no longer receiving updates

To make it easier to follow, we intentionally ignore using specific malware types, such as adware, ransomware, keylogger, spyware, etc.

Let us look at some Android malware in 2023:

AhMyth

According to ESET reports, AhMyth infected more than 50,000 devices before it was discovered. The malicious codes were found in an application called iRecorder – Screen Recorder, which was published on the Play Store. As implied by the name, it requests a lot of permissions, including the ability to write to and read from external storage, and use the camera and microphone, among other things. At first glance, giving a screen recorder those permissions seems appropriate. It attempted to hide its activities by using the guise of a screen recorder, which many users installed on their phones. The Play Store analysis was unable to identify it as a rat. (Rat applications are those that behave in that way.) Google swiftly removed the application from the Play Store in response to the ESET warning. Malicious code was added to the most recent versions of the application after it was found to be absent from earlier

versions. It was possible to deceive the user because the application appeared legitimate.

FluHorse

This malware was spread through a phishing campaign employing deceptive tactics. The victim had to be an Android device to download this malware. The user was directed to a website that hosted the application. Once the application was installed, it asked for SMS permission, followed by asking for the user's credential information. This malware's interesting feature was the platform that was used to create it. It was challenging to evaluate its functionality using the Flutter framework.

SpinOk

In the following Doctor Web report, the security team at CloudSEK reported discovering more than 100 applications on the Play Store that were contaminated with malicious code. According to Doctor Web's analysis, this malware could take data from storage and the clipboard and upload it to a remote server. Additionally, the malicious code was able to access the sensor data and use it to avoid being discovered. The harmful code was a component of an SDK that was meant to offer an advertisement utility used in other programs and video games. To accomplish their objective, the attackers used the SDK to upload or inject malicious Javascript code.

These are just a few instances of how malware and malicious code have attempted to steal user data by abusing legitimate functionalities and SDKs, which may have an impact on many users and reliable applications. There was a chance for prevention through user awareness, at least in the first two instances.

Some tips if you get infected

- Restart to Safe Mode and uninstall the infected app
- Use Play Protect from Play Store to check the apps
- Use Antivirus
- Restart your phone
- The last option is to use the “Reset Factory” option. (You need to know if you use this option, you might lose all of your data, including, photos, videos, contacts, etc.)

Note: You need to search and find the best solution for yourself, especially if it's moderate malware. You also need to be aware of what you're doing since it might end up causing you to lose your data if you use the “Reset Factory” option.

Check out pentestmag.com new course!

Aerospace Cybersecurity: Satellite Hacking



Gain deep understanding of satellite communication systems,
space-based OSINT skills,
decoding satellite communication protocols and much more