ADMM Cybersecurity and Information Centre of Excellence

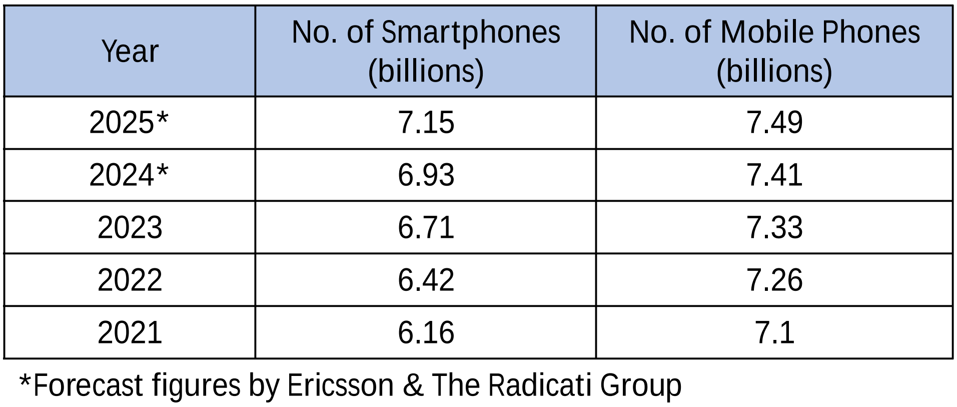
# UPDATE ON THE CYBER DOMAIN

Issue 2/24 (February)

## Rise of Mobile Malware: Risks and Best Practices

### INTRODUCTION

1. With mobile phones being integrated into our daily lives, it is no surprise that mobile malware has been increasingly used to facilitate cyber attacks against individuals and organisations. As the number of unique mobile users grow worldwide, mobile devices will remain highly attractive targets for threat actors. This has resulted in an exponential growth in the volume and level of sophistication of mobile malware developed by cyber attackers, exposing mobile users to heightened risks.



| Year | No. of Smartphones (billions) | No. of Mobile Phones (billions) |
|---|---|---|
| 2025* | 7.15 | 7.49 |
| 2024* | 6.93 | 7.41 |
| 2023 | 6.71 | 7.33 |
| 2022 | 6.42 | 7.26 |
| 2021 | 6.16 | 7.1 |

*Forecast figures by Ericsson & The Radicati Group

Growing Number of Mobile Device Users Worldwide (Source: bankmycell)

2. A 2022 study by Microsoft revealed that more than two-thirds (67%) of workers used their personal mobile phones for work-related matters. This represents a real vulnerability, not just for our personal data, but also for potentially sensitive work information. As our collective reliance on mobile devices continues to grow in tandem with the threat posed by mobile malware, individuals and organisations alike are exposed to heightened risks. It is therefore important to understand the threat that mobile malware poses, and to take proactive measures so as to continue to enjoy the benefits of mobile technology without compromising security.

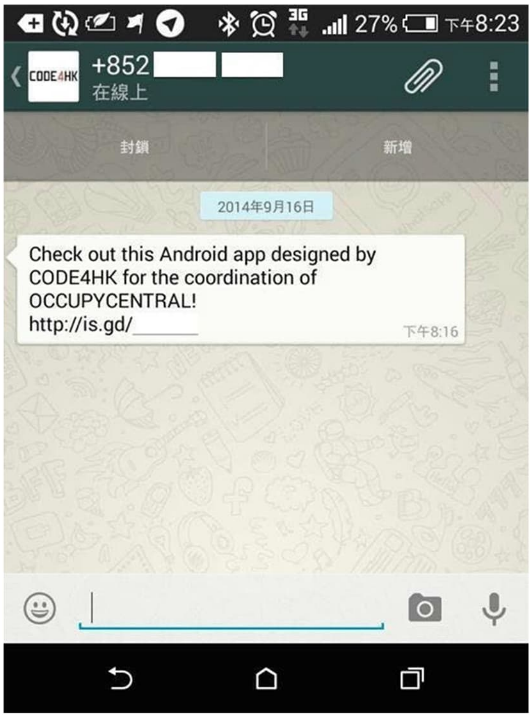
# TYPES OF MOBILE MALWARE

3. While mobile malware is often portrayed as a singular threat, it is crucial to recognise that it comprises various forms, each with distinct characteristics and methods to infect devices. Among the most prevalent types are trojans and ransomware.

## Trojans

4. In a manner reminiscent of the Trojan Horse strategy employed in ancient Troy, Trojan malware hides malicious code within legitimate software to gain system access. Trojans are particularly effective on mobile devices given the near-24/7 usage. Once installed, it performs unauthorised functions in the background, which can range from harvesting personal data to intercepting messages from the device. Moreover, Trojans often serve as a gateway for more sophisticated threats, such as Remote Access Trojans (RATs). RATs facilitate covert surveillance operations by granting attackers extensive control over compromised devices, enabling them to monitor activities, exfiltrate sensitive information, and execute malicious commands remotely.

5. An example of the malicious usage of a RAT was the spreading of a fraudulent smartphone application claiming to coordinate the Occupy Central pro-democracy movement in Hong Kong in 2014. Activists received links to download the application via WhatsApp messages from unknown phone numbers, with messages like “Check out this Android app designed by Code4HK, for the coordination of Occupy Central!” However, beneath the seemingly legitimate application lay an advanced RAT, which allowed threat actors to extract a wide range of data from the device – such as call logs, browser history, network data, and location – and carry out actions such as initiating audio recordings and executing commands.



27% 下午8:23

CODE4HK +852 [redacted]
在線上

封鎖 新增

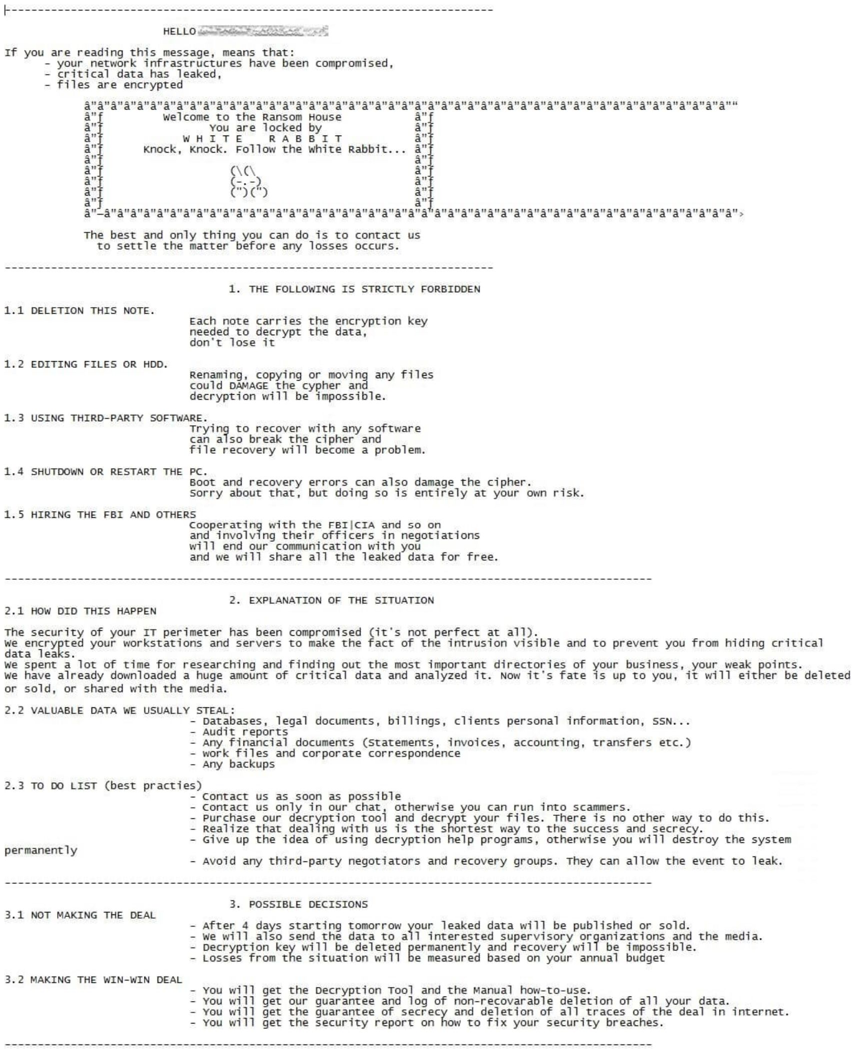
2014年9月16日

Check out this Android app designed by CODE4HK for the coordination of OCCUPYCENTRAL!
http://is.gd/______
下午8:16

An example of a phishing message delivered to Whatsapp users in Hong Kong.
(Source: New York Times)

## Ransomware

6. Ransomware is a type of malware crafted to lock and encrypt a victim's data, rendering them inaccessible and unusable by legitimate users. Attackers would then demand a ransom for the recovery of users' data and systems. Modern ransomware actors typically carry out 'double extortion' tactics, involving the traditional encryption of data (as in a traditional ransomware attack), as well as exfiltrating personal data stored on the mobile device for subsequent sale.



```
|-----------------------------------------------------------------------

                       HELLO [redacted]

If you are reading this message, means that:
      - your network infrastructures have been compromised,
      - critical data has leaked,
      - files are encrypted

            â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â""
            â"f          Welcome to the Ransom House             â"f
            â"f                You are locked by                 â"f
            â"f             W H I T E    R A B B I T             â"f
            â"f       Knock, Knock. Follow the White Rabbit...   â"f
            â"f                                                  â"f
            â"f                   (\(\                           â"f
            â"f                   (-.-)                          â"f
            â"f                   (")(")                         â"f
            â"f                                                  â"f
            â"–â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"›

            The best and only thing you can do is to contact us
              to settle the matter before any losses occurs.

-----------------------------------------------------------------------

                                1. THE FOLLOWING IS STRICTLY FORBIDDEN

1.1 DELETION THIS NOTE.
                           Each note carries the encryption key
                           needed to decrypt the data,
                           don't lose it

1.2 EDITING FILES OR HDD.
                           Renaming, copying or moving any files
                           could DAMAGE the cypher and
                           decryption will be impossible.

1.3 USING THIRD-PARTY SOFTWARE.
                           Trying to recover with any software
                           can also break the cipher and
                           file recovery will become a problem.

1.4 SHUTDOWN OR RESTART THE PC.
                           Boot and recovery errors can also damage the cipher.
                           Sorry about that, but doing so is entirely at your own risk.

1.5 HIRING THE FBI AND OTHERS
                           Cooperating with the FBI|CIA and so on
                           and involving their officers in negotiations
                           will end our communication with you
                           and we will share all the leaked data for free.

-----------------------------------------------------------------------------------------------

                                2. EXPLANATION OF THE SITUATION
2.1 HOW DID THIS HAPPEN

The security of your IT perimeter has been compromised (it's not perfect at all).
We encrypted your workstations and servers to make the fact of the intrusion visible and to prevent you from hiding critical
data leaks.
We spent a lot of time for researching and finding out the most important directories of your business, your weak points.
We have already downloaded a huge amount of critical data and analyzed it. Now it's fate is up to you, it will either be deleted
or sold, or shared with the media.

2.2 VALUABLE DATA WE USUALLY STEAL:
                           - Databases, legal documents, billings, clients personal information, SSN...
                           - Audit reports
                           - Any financial documents (Statements, invoices, accounting, transfers etc.)
                           - work files and corporate correspondence
                           - Any backups

2.3 TO DO LIST (best practies)
                           - Contact us as soon as possible
                           - Contact us only in our chat, otherwise you can run into scammers.
                           - Purchase our decryption tool and decrypt your files. There is no other way to do this.
                           - Realize that dealing with us is the shortest way to the success and secrecy.
                           - Give up the idea of using decryption help programs, otherwise you will destroy the system
permanently
                           - Avoid any third-party negotiators and recovery groups. They can allow the event to leak.

-----------------------------------------------------------------------------------------------

                                3. POSSIBLE DECISIONS
3.1 NOT MAKING THE DEAL
                           - After 4 days starting tomorrow your leaked data will be published or sold.
                           - We will also send the data to all interested supervisory organizations and the media.
                           - Decryption key will be deleted permanently and recovery will be impossible.
                           - Losses from the situation will be measured based on your annual budget

3.2 MAKING THE WIN-WIN DEAL
                           - You will get the Decryption Tool and the Manual how-to-use.
                           - You will get our guarantee and log of non-recovarable deletion of all your data.
                           - You will get the guarantee of secrecy and deletion of all traces of the deal in internet.
                           - You will get the security report on how to fix your security breaches.

-----------------------------------------------------------------------------------------------
```

An example of a 'ransom note' from the White Rabbit ransomware (Source: Trend Micro)

7. Ransomware has been traditionally associated with attacks on computers, with mobile devices being more protected due to in-built malware scans and the application sandboxing present on official app stores. However, ransomware attacks are growing in sophistication, and increasingly targeting mobile devices. A 2023 report from cybersecurity firm CloudSEK highlighted the threat posed by the 'Daam' ransomware to new Android devices. Beyond exfiltrating sensitive information, this ransomware has the capability to encrypt all files on an infected Android smartphone without user consent, and change a smartphone's device password to completely lock a user out of their phone. Moving forward, we can expect attackers to continue adapting their modus operandi to increase the effectiveness of ransomware attacks, such as through targeting backup data.

## PROACTIVE DEFENCE STRATEGIES

8. The personal mobile device has become an inseparable part of our lives in a world that is digitally connected. It is also common that the same mobile device is designated for personal and professional use. There is a need for individuals and militaries to be vigilant to mitigate malicious cyber activities and to focus on maintaining operational resilience. Below are some proactive defence strategies to protect both the individual and the organisation.

9. **Individual-level**. Today, many of us perform personal and work-related functions on our mobile device. Individuals must recognise that cyberattacks on their personal mobile devices have the potential to be extended to the organisational networks they are connected to, and can potentially lead to large-scale data loss. As such, it is crucial to adhere to a comprehensive set of best practices to mitigate the risks posed by malware, such as:

a. Equipping your device with reputable mobile security software capable of detecting and thwarting potential malware infections;

b. Practicing discernment in granting app permissions;

c. Keeping your operating system and security software updated; and

d. Implementing two-factor authentication (2FA) wherever feasible.

10. **Organisational-Level**. The risks to sensitive outfits like militaries are heightened if the personal mobile devices of employees are compromised. Militaries should consider extending their security measures by implementing robust Mobile Device Management (MDM) policies. These policies establish guidelines for the usage and security of all employee-owned mobile devices within the organisation, ensuring consistent protection across all devices accessing company data. For militaries, an MDM policy may include:

a. **Restricting device functionalities (i.e., GPS-enabled features) within sensitive operational areas**. Since 2018, US Department of Defence personnel are prohibited from using geolocation features on all mobile devices while in operational areas. This minimises the likelihood of exposing operational areas and compromising mission security.

b. **Mandating the use of secure communication channels and encrypted messaging platforms**. By leveraging military-grade encryption measures (e.g., end-to-end encryption, cryptographic protocols), militaries can ensure the confidentiality of sensitive information transmitted over mobile networks against interception attempts by hostile actors.

c. **Establishing clear protocols for reporting losses, data breaches, or stolen devices**. With every minute counting in the recovery of lost devices and keeping data secure, it is important that employees report the loss and/or breach of devices as soon as possible, with clear directions and systems for them to do so. For devices with extremely sensitive data, militaries can also consider installing location-tracking applications or having measures in place to wipe data remotely.

## CONCLUSION

11. As our reliance on mobile devices for personal and professional communication intensifies, militaries must invest more to protect the mobile devices of their service members from cyber-attacks. With mobile cyber-attacks being one of the most insidious modern-day threats, militaries must ensure that the risk of a breach through this less-protected access point is mitigated. As such, militaries must invest more in consistent education, enforcing best cyber-practices, and taking a proactive and informed approach to mitigating risks. When done collectively and consistently, militaries can ensure that the battlefront of mobile malware is something that they are well-prepared to defend against.

# Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
**ADMM Cybersecurity and Information Centre of Excellence**

••••

# References

1. Zimperium Report: Increase in Sophisticated Attacks Against Mobile Devices [https://www.zimperium.com/resources/press-releases/zimperium-research-reveals-significant-increase-in-sophisticated-attacks-against-mobile-devices/]

2. 200,000 New Mobile Banking Trojan Installers Discovered - Research [https://www.tahawultech.com/news/200000-new-mobile-banking-trojan-installers-discovered/amp/]

3. Beware of These Mobile Security Threats on Halloween [https://vmblog.com/archive/2023/10/25/beware-of-these-spine-chilling-mobile-security-threats-this-halloween.aspx]

4. Understanding the Rise of Mobile Ransomware [https://www.mimecast.com/content/mobile-ransomware/]

5. Mobile Security Index 2023 [https://www.verizon.com/business/resources/reports/mobile-security-index/?CMP=OLA_SMB_NA_11111_NA_20210406_NA_M20210052_00001]

6. Daam Android Malware can hold your phone hostage – what you need to know [https://www.tomsguide.com/news/daam-android-malware-can-hold-your-phone-hostage-what-you-need-to-know]

7. Mobile Malware and APT Espionage: Prolific, Pervasive, and Cross-Platform [https://blogs.blackberry.com/en/2019/10/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform]

8. New Ransomware Spotted: White Rabbit and Its Evasion Techniques [https://www.trendmicro.com/en_us/research/22/a/new-ransomware-spotted-white-rabbit-and-its-evasion-tactics.html]