Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies

Moses Ashawa*, and Sarah Morris

Centre for Electronic Warfare Information and Cyber, Cranfield University, Shrivenham, United Kingdom.

Received 17 Jul. 2021; Accepted 22 Nov. 2021; Available Online 30 Dec. 2021

Abstract

The open-source and popularity of Android attracts hackers and has multiplied security concerns targeting devices. As such, malware attacks on Android are one of the security challenges facing society. This paper presents an analysis of mobile malware evolution between 2000-2020. The paper presents mobile malware types and in-depth infection strategies malware deploys to infect mobile devices. Accordingly, factors that restricted the fast spread of early malware and those that enhance the fast propagation of recent malware are identified. Moreover, the paper discusses and classifies mobile malware based on privilege escalation and attack goals. Based on the reviewed survey papers, our research presents recommendations in the form of measures to cope with emerging security threats posed by malware and thus decrease threats and malware infection rates. Finally, we identify the need for a critical analysis of mobile malware frameworks to identify their weaknesses and strengths to develop a more robust, accurate, and scalable tool from an Android detection standpoint. The survey results facilitate the understanding of mobile malware evolution and the infection trend. They also help mobile malware analysts to understand the current evasion techniques mobile malware deploys.

I. Introduction

The world is undergoing a rapid information transformation piloted by redefining and restructuring technological processes. This fast technological growth has caused the evolution and advancement of major security issues worldwide, in addition to its many benefits (e.g. fast financial transactions, automation, short-time processing of data) [1], [2]. Information technology usage ushers in new security challenges (e.g. impersonations, sensitive data exposure, malware attacks, other cyber-threat issues) [3]. Malware has become a global issue and is now a sophisticated threat that information security is battling on a national and international scale. Cyber-threats have increased significantly during the COVID-19 pandemic as cybercriminals have taken advantage of the COVID outbreak, especially during the adaption of the work from home (WFH) approach to curbing the spread of the virus [4], [5].

While the pandemic claims human lives in the millions and creates anxiety and considerable uncertainty, cyber-attacks are also harming peoples'

Keywords: Infection Strategies, Malware Evolution, Mobile Malware, Information Security.

Production and hosting by NAUSS

* Corresponding Author: Moses Ashawa
Email: m.ashawa@cranfield.ac.uk

doi: 10.26735/KRVI8434

1658-7782© 2021. JISCR. This is an open access article, distributed under the terms of the Creative Commons, Attribution-NonCommercial License.

livelihoods. Government and non-governmental organizations have been compelled to adopt precautionary measures and adapt to remote working during the pandemic, with little or no adequate and necessary training of their employees to be cyber smart when working remotely. Even for those that have the training, working from home on a poorly secured network is a concern. As a result, cybercriminals are exploiting individuals and government vulnerabilities for financial gain through pandemic-related threats such as fraud, phishing, and malware. Among the cyber threats, the research of Cristea [6] reported that malware attacks on mobile devices are the most challenging current security threat in the national and international context. Malware has evolved and has become sophisticated, so detecting of some variants becomes very difficult. McLaren et al. [7] stated that bot writers deploy evasion techniques like code encryption to make detection by pattern recognition less effective.

The advancement in mobile technology has brought about corresponding effects on mobile malware, which attacks mobile devices. Among the mobile OS, Android is the fastest-growing OS used worldwide [8], [9], [10]. Research has shown that the Android operating system outran other mobile OS due to some factors such as ease of use, affordability, open-source code, and compatibility commitment [11], [12], [13]. The first malware, called Creeper [14], was created to target personal computers, but as technology advanced, malware evolved to attack mobile devices as well. The first mobile malware, known as Cabir [15], was designed to target Symbian-based mobile platforms. Since the advent of Cabir, mobile malware has evolved into different variants and with differing complexities. According to the cybersecurity report released by Check Point software technology [6], mobile malware is one of the current security threats at national and international levels. Unlike PC malware, mobile malware has become so pronounced due to the enormous amount of personal and financial information cybercriminals harvest from those devices. Consequently, data breaches and financial loss cases caused by mobile malware keep increasing.

The research published by the UK Department for Digital, Culture, Media & Sport in 2020 shows that malware caused 87% of the total cybersecurity attacks that caused financial loss [16]. In addition, the growth of malware attacks on mobile devices continues to increase despite the number of industrial solutions, scant systematic reviews, and meta-analyses focusing on identifying strategies mobile malware deploys as infection strategies or attack vectors to infect mobile devices. Also, while there are several mobile malware detections, classification, and analysis techniques, the systematic review and meta-analysis of the infection strategies are deficient. Our systematic meta-analysis aims to look at the mobile malware evolution and infection strategies. Manymobile malware attack goals can be fragmented into the motives and the behavior related to the motive. The World Economic Forum (WEF) threat risk report highlighted that every cyberattack caused by malware leaves indelible impacts, even after the malware has been detected and removed [17].

This paper has the following aims: (1) To advance understanding of the mobile malware history and its position in the cyber threat landscape, examining the major security threats to mobile devices; (2) To provide a discussion on the evolution of Android malware to identify security transformation and propagation modes adopted at each evolutionary stage; (3) To examine different evasion techniques adopted and their security implications; and (4) To critically examine android malware infection strategies and raise recommendations and awareness of malware impacts and how to curb the attacks and infection rates. Our research made the following contributions:

- Providing an up-to-date study of mobile malware evolution and infection strategies.
- Classifying mobile malware evolution trends into distinct categories based on their sophistication, characteristics, and the motivations behind attacks.
- Providing a general overview of the mobile malware infection model based on the meta-analysis of the infection strategies.
- Identifying factors that limited the fast spread of the early mobile malware. These include

(a) the lack of mobile OS standardization, (b) the lack of mobile OS cross-platform, and (c) the lack of Bluetooth technological advancements in data communication.

- Identifying factors that enhance the fast spread of recent mobile malware. These include (a) the advancement in threat dimensions, (b) improved security and business communication on Tor using a multi-signature transaction and encryption approach, (c) mobile platforms' integration with the IoT-based applications, and (d) the emergence of evasion techniques and the advancements in mobile malware Toolkits on the dark web.
- Providing recommendations as countermeasures to cope with emerging mobile malware and its increasing threats. These include (a) the deployment of software solutions from enterprise mobility management to enhance the security of enterprise devices, (b) observation of mobile application plugins and codecs during mobile application download and installation, (c) the adoption of risk mitigation strategies by organizations, and (d) development of a mobile malware infection model to understand the immunity state of a mobile device during and after recovery from malware infection.

The remainder of the paper is structured as follows: Section II provides the research methodology, section III provides the background of the study, Section IV presents the discussion, Section V presents the infection and attack vectors, and Section VI presents the conclusion.

II. Methodology

Scientometrics was used to assess and analyze the finite features of the selected papers used for this study [18]. The source of literature for this study came from the Web of Science collections. Field tags such as parenthesis, wildcards, Boolean OR operator, and quotation marks were used to create the query for exact words and phrases. Two datasets (core dataset (CD) and extended dataset (ED)) were ultimately used for our study. Web of Science retrieval was used to obtain the core dataset which contained many kinds of literature. For further filtering, the repeated literature was eliminated using CiteSpace, a function of the Web of Science as shown in Fig. 1. The final database was then generated, combining the core and expanded dataset containing the reviews and the articles. The topic search (TS) was used as the target to perform a holdout data search to pull out all the keywords essential for both the core and extended dataset. This was to determine the total increase in node purity of the most important variables (Keywords) in the TS Fig. 2. In summary, different articles were collected during the filtering process. However, only 243 papers met our selection criteria, including time span and language. For instance, some papers contained keywords, but the content was written in languages other than English. Many more were eliminated according to our selection criteria.

To discover the essential organization of the CD and ED, we conducted an exploratory factor analysis [66] using the applied rotation method, simplimax, to identify latent keywords that were not observed but share common variances. The aim of conducting the exploratory factor analysis on the combined dataset generated was to enhance the complexity reduction of the large data (articles and reviews). The exploratory factor analysis brought out the factor correlations and the uniqueness characterising the CD and ED articles with their influencing TS tag-keywords as shown in Fig. 3.

III. Background

A. History of Mobile Malware

General malware appeared in the 1970s when Bob Thomas wrote a self-replicating virus called Creeper Worm. Creeper worm was Adware that displayed popups on systems with the message "I'm the Creeper, catch me if you can!" [19], [20], [21],. After the emergence of Creeper, other significant PC malware such as Wabbit [22], Elk Cloner [23], Brain Boot Sector Virus [24], PC-Write Trojan [25], Morris Worm [26], Michelangelo Virus [27], and Melissa Virus [28] also emerged. The emerging technology in mobile devices has brought about a proportional malware threat to mobile devices. Smartphones are speedily substituting PCs both in the workplace and at home. Most activities such as web surfing and financial transactions rely

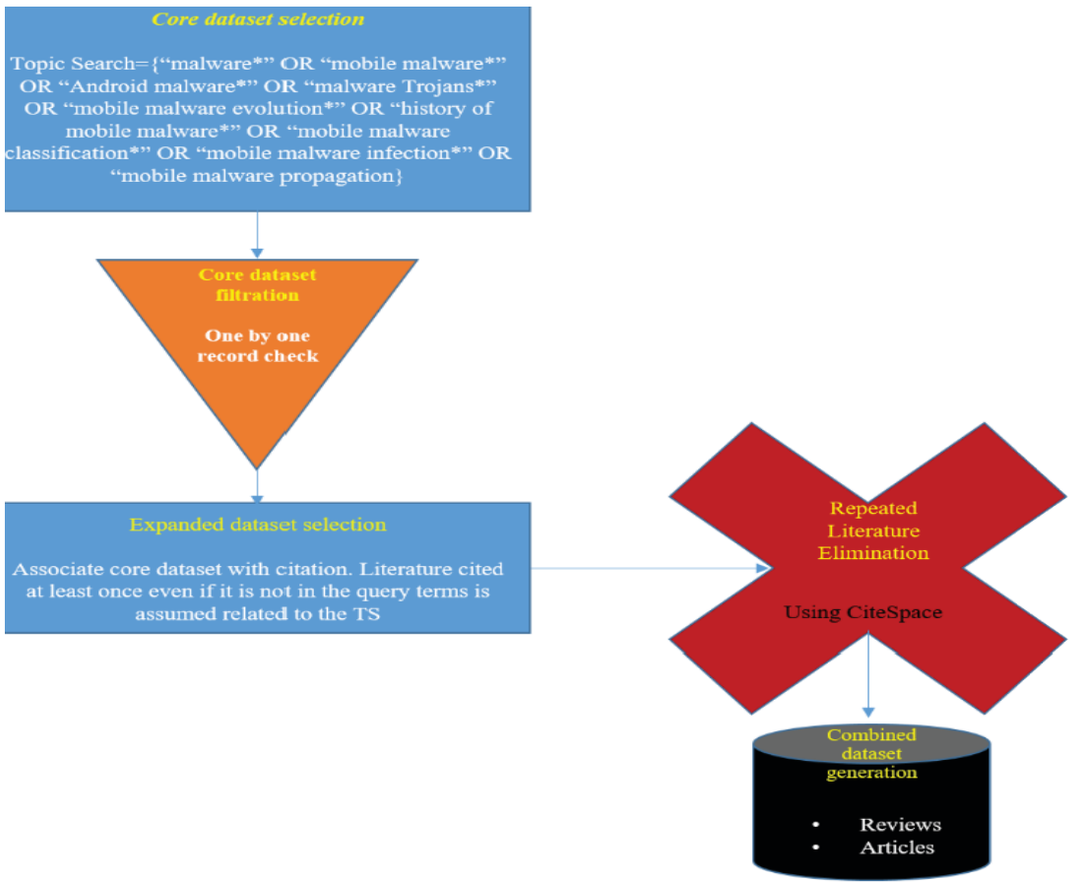

Fig. 1 Scientometrics dataset selection, filtration, and elimination process.

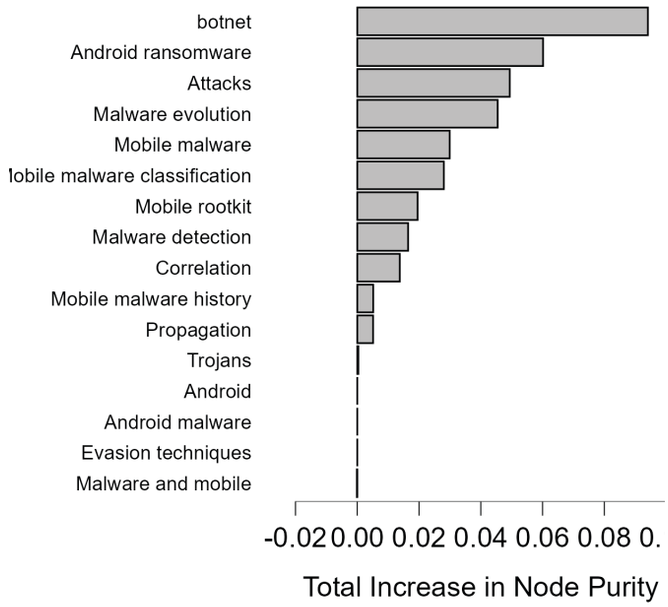

Fig. 2 Determining the total increase in node purity of the most important keywords in the Topic Search from the combined dataset.

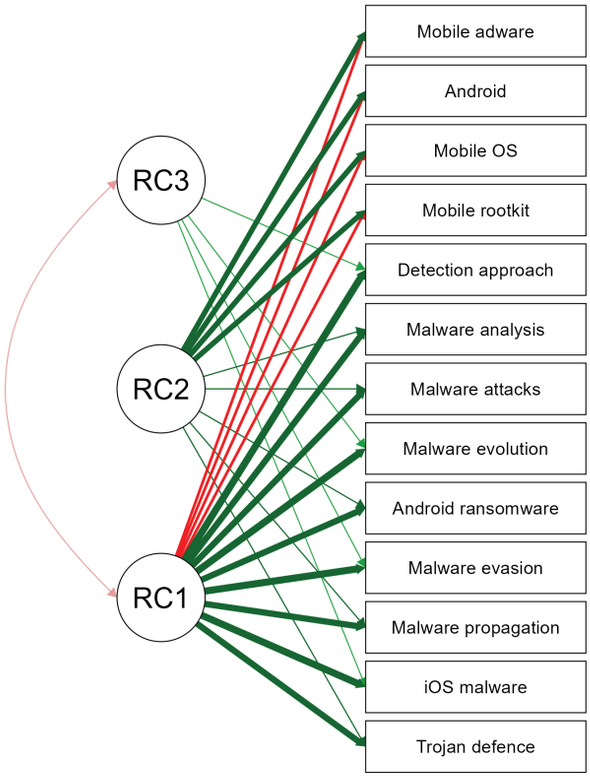

Fig. 3 Path diagram showing the keywords characterization and the number of factors using simplimax as the rotation method and minimum residual as the estimation method.

on mobile devices. Due to the increased dependence on smartphone devices and the financial information they store, malware writers' attention has significantly shifted from PC to mobile devices. s

According to Shah et al. [29], the history of malware attacks on mobile devices can be traced back to 2004 when the first mobile malware called Cabir was written by Vallez to target Symbian-based devices. Being a worm, Cabir injected its payload into the victim's devices via Bluetooth file-sharing as a spreading mechanism. The malware was not sophisticated in its operation. It displayed annoying popups that made the infected mobile device unpleasant to operate. Due to the limitations of Bluetooth technology in data communication, slow data speed, and short signals, the rapid spread of the malware was impeded. Another factor that impeded the rapid spread of Cabir was the fact that the devices had to be close to each other to establish a connection before the infection could occur. The lack of standardization in mobile OS was also another limiting factor that inhibited the rapid spread of Cabir.

Another mobile malware called Skulls [30] was developed in the same year with criminal motives and later formed the basis of PC malware. The later malware was found to overwrite mobile application files and substituted applications' icons with crossbones and skulls that stopped mobile device functionalities. In 2005, malware moved into the realm of information theft when more dangerous mobile malware called Commwarrior and Pbstealer [31] were discovered targeting the Nokia 7160. Both Commwarrior and Pbstealer targeted and harvested information-sensitive data such as passwords and usernames using nearby connected mobile devices. Looking at the malware pattern, the study by Mayrhofer et al [32] shows the paradigm shift in malware development from Symbian devices to Android, particularly the development of malware for Java 2 Micro Edition (J2ME).

The major trend followed by malware writers in this paradigm was developing malicious codes using J2ME to send premium rate texts or using SMS as a social engineering mechanism to trick victims into confirming non-existing financial operations.

The first android mobile malware was called "ANDROIDOS_DROIDSMS.A" [33]. It was detected as a Trojan in 2010 by Trend Micro, while the Ikee worm was also uncovered for iOS-based devices (Apple iPhones). The mobile infection trend in this era focused on phone jailbreaking, rooting, Rickrolling, and changing the phone background to display Rick Astley's image leaving the message on the screen "Ikee is never gonna give you up" [34]. Android malware was originally spread by using third-party application marketplaces, due to android openness in its App ecosystems circulation, which undoubtedly accelerated this misuse, unlike Apple.

From 2011 till date, there has been a progressive growth of malware threat complexity. For Android, the kill switch was used by Google, but the challenge remains that the kill switch will not be effective if an earlier download has an infection on the device. iPhone/FindAndCall [35] and Android/DroidKungFu [36] malware snip individual data and forward this personal information to remote network servers. Other malicious software such as FinSpy, Android/Nickispy, and Android/Spybubble have been developed to record mobile phone calls, send SMS, and monitor mobile location as spy instruments. The research of [37] observed that the number of malware attacks on android from 2013 grew to 98.05% compared to Symbian (0.27%), J2ME (1.55%), and others (0.13%), as shown in Fig. 4.

The study by Chen et al [38] asserted that malware infections and threats on mobile devices are increasingly spreading to affect other smart devices such as smart cities, smart TVs, smartwatches, cloud-based technology, and IoT device platforms. This shows the susceptibility of smart devices to attacks such as buffer overflow, which can be deployed by hackers to remotely control those devices. Apart from attacks on smart devices, the medical field has recently been severely affected by the number of malware attacks. Malware attacks cardiac devices and reconfigures them [39], resulting in failures during cardiovascular implantation and, thus, putting the lives of patients at risk. The attack of WannaCry Ransomware [40] on the UK NHS infrastructure in 2017 affected several NHS computers have a considerable effect on the system operation and patients records.

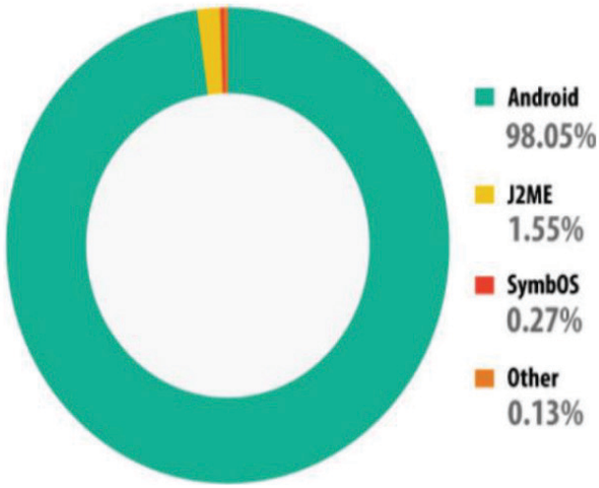

Fig. 4 Comparison of malware attack rates on mobile OS platforms in 2013 [38].

From the above history, we noted that many malware codes were written for fun and probably for behavioural testing of software from the beginning. However, evolution in writing malware has increased the complexity of its impacts on financial institutions, businesses, and information leakage. It has evolved to be used for financial gain, vengeance, system sabotage, cyberstalking, and political influence. Table I shows a detailed review of major mobile malware incidents and evolution and propagation strategies.

B. Evolution of Android malware

Android open model architecture is one of the potential factors that encouraged fast malware progression, where the Google bouncer uploads malware applications written by hackers on the play store without adequate security checks. The Android open framework model is one of the major factors that pose a security risk. The open-source nature of the Android platform enables OS modification by the manufacturers for feature enhancement and thus makes the source code susceptible to attackers. It also provides opportunities for tinkering the OS-based devices, thus, weakening the security of the device.

In 2010, AndroidOS.DroidSMS.A [41] emerged as the first Android mobile malware. AndroidOS.

TABLE I
MOBILE MALWARE INCIDENTS AND EVOLUTION

Year	Research	OS Targeted	Malware	Malware type	Malware functionality
2000	[92][91][90]	Symbian	Timofonica	Worm	Propagates through Bluetooth
2004	[95][94][93]	Symbian	Cabir	Worm	Propagates through Bluetooth
2004	[98][97][96]	Symbian	Skull	Trojan	Displays icons and replaces system applications and files
2004	[101][100][99]	Windows CE	Brador	Backdoor	Gains remote access to a network
2005	[104][103][102]	Symbian	Commwarrior	Worm	Infects files by propagating through MMS and Bluetooth
2005	[106][105]	Symbian	Locknut	Trojan	Enables installation of corrupted applications
2005	[107][106][97]	Symbian	Drever	Trojan	Swaps antivirus loaders
2005	[109][108]	Symbian	Skudoo	Trojan	Installs Skull and Cabir
2005	[110]	Symbian	Singlejump	Trojan	Disables system functions
2005	[111]	Symbian	Cardtrap	Trojan	Deletes antivirus files
2005	[122][62]	Symbian	Pbstealer	Trojan	Steals sensitive data
2006	[113]	J2ME	RedBrowser	Trojan	Sends premium SMS
2006	[114]	Symbian	Rommwar	Trojan	Replaces device applications
2007	[115]	Symbian	Flexispy	Trojan	Steals sensitive data
2009	[35]	iOS	Ikee	Worm	Jailbreaks Apple devices
2010	[35]	Android	DroidSMS.A	Trojan	Sends premium SMS
2010	[116]	Blackberry, Android, windows, and Symbian	Zitmo (Zeus-(in-the-mobile	Trojan	Online banking attacks
2010	[117]	Android	Tap Snake	Spyware	Location monitoring
2010	[118][45]	Android	FakePlayer	Trojan	Sends premium SMS
2011	[119]	Android	DroidDream	Trojan	Roots devices, installs other malicious apps at the backdoor
2012	[120]	Android	Boxer	Trojan	Sends premium SMS
2012	[122][121]	Android	Opfake	Trojan	Device rooting
2012	[122]	Android	Fakeinst	Trojan	Performs update attacks
2013	[124][123]	Android	fakeDefender	Ransomware	Prompts users to buy security app
2013	[125]	Android	Obad	Backdoor	Zero-day attack
2014	[126][68]	Android	NotCompatible.CA	Trojan	Side loading apps to hinder security .assurance
2015	[127]	Android	Acecard	Trojan	Banking Trojan
2015	[128]	iOS	XcodeGhost	Trojan	Overlays apps, Steals, and uploads user data to C2 servers

TABLE I
MOBILE MALWARE INCIDENTS AND EVOLUTION (*Continued*)

Year	Research	OS Targeted	Malware	Malware type	Malware functionality
2015	[98]	iOS	YiSpecter	Adware	Attacks both jailbroken and non-jailbroken iOS phones
2016	[92]	Android, iOS	HummingBad	Trojan	Rogue software app
2016	[129]	Android	Xbot	Ransomware	Sends premium SMS and steals banking details
2016	[130]	Android	AndroidOS. Fusob	Ransomware	Remotely access infected devices. demands ransom
2016	[131]	iOS	AceDeciever	Trojan	Exploits Apple DRM design flaws
2017	[132][6]	Android	Ztorg	Trojan	Roots devices
2017	[133]	Android	ToastAmigo	Backdoor	Deploys toast overlay attack to install more malicious apps
2018	[134][80]	Android	Chamois	Backdoor	steals OAuth tokens
2018	[135]	iOS	Pegasus	Spyware	Records calls, keylogging, zero-day exploit
2019	[137][136]	Android	TimpDoor	Spyware	Click fraud attack
2019	[138][11]	Android	Cerberus	Trojan	Intercepts calls
2019	[139][12]	Android	XHelper	Trojan	Displays popup adds, redirects users
2020	[140]	Android	Ghimob	Trojan	Demands ransom

DroidSMS.A is a fraudulent application for the SMS premium rate. Using SMS services, the Trojan subscribes to victims' Android devices. The affected devices received different text messages at a premium rate using automatic subscription premium SMS service. AndroidOS.DroidSMS.A installed itself on the phone once permission request attributes related to SMS features were granted. Another Trojan discovered in the same year was Tap Snake [42], which propagated via HTTP by acquiring the victim's device location via GPS or network services. Tap Snake masqueraded as a mobile game but was a spy tool, remotely monitoring mobile conversations and locations. The monitored data are then forwarded to malicious servers in the background for further attacks and vulnerability exploits. AndroidOS.DroidSMS.A and Tap Snake Trojans were wreaking havoc on Android in 2010. Their counterpart Ikee worm [43], [44] was jailbreaking iOS-based mobile devices to use an SSH password. Based on the meta-analysis of their operation mode, we can assert that it was very easy to avoid being infected by Tap Snake if users pay attention to the services the application requests to access. For instance, during the installation, it requests permission to access network communication, device location, and system tools. We can infer that this infection could have been avoided if users prioritise their security over the need to use the masquerading applications.

Three other Android malware that emerged in 2010 included SMSReplicator, Geinimi, and Fakeplayer [45]. Both AndroidOS.DroidSMS.A and the Tap Snake game did not infect many devices, because the attack vectors were limited due to a lack of cross-platform propagation ability. According to the research of [46], [47], another factor that limited the spread of those Trojans was that Android (4.45%) was still not as popular as Symbian OS (34.33%), iOS (32.92%), and BlackBerry OS (10.16%). Apart from cross-platform propagation limitation and lack of Android popularity, other fac-

tors such as low mobile features like weak internet connectivity and short Bluetooth range were also contributing factors that repressed rapid propagation of the first emergent malware. The common behavioral goal amongst the two malware applications is their monetization motive towards the mobile space.

While only a few Android malware families emerged in 2010, the number of Android malicious applications multiplied greatly in 2011 with over 44 different Android malware families discovered. Among the variants discovered, DroidDream [48] was one of the notable families that rooted the victims' devices to steal sensitive data. Thus, android malware evolved from SMS premium to modification of mobile functionalities. While the family of DroidDream focuses on stealing users' private information, the Genimi family [49] takes control from the attacker's remote server. DroidDream was an Android botnet type of malware which stole Unique Identification Information (UII) by gaining root access to the victim's Android device. Hackers were able to control the infected devices remotely by abetting automatic download of other malicious files without the victim's awareness or authorisation.

As noted in the study of Yan and Yan [50], the emergence of this malware family led to the mainstream Android malware Toolkits. This became the foundation of the mobile cybercrime market worldwide. As the attack success progressed, DroidDream and its likes were sold on the dark web illegally where virtual access can be deployed to harm. This evolution made Android-malware-spreading kits available and accessible worldwide. We can infer that this evolution made buying, ownership, and deployment of Android malware easy. Hackers pay for the toolkits in Bitcoin and are provided with the necessary tutorials needed for effective Android malware infection. This led to a rapid proliferation of malware samples and the corresponding attacks.

Opfake [51] and Fakeinst [52] were the most prominent Android Trojans discovered by Kaspersky in 2012, with over 1,083 Android malware samples discovered by different security companies such as Kaspersky and F-Secure. Most of the Android malware samples were the repackaged versions of legitimate applications, which lead to the policing requisite of developing techniques that could detect repackage applications. Our research observed that this malware family adopted drive-by downloads and updated attacks to infect victims' devices, which was more difficult to detect. According to Meng [53], samples of the families discovered in 2012 could influence root exploits to completely compromise the security of Android. Thus, this presented a high level of privacy threats to the Android community. Some of the Android malware families in 2012 had inherent attributes of the 2010 and 2011 samples. Similar attributes included sending premium text messages, turning compromised devices into botnet, harvesting users' account details and calling in the background without the awareness of the owner. Root-level exploitation by these Android malware families caused poor security stability of the Android OS, leading to other different consequences such as device bricking, loss of device warranty, financial loss, and more openings of attack surfaces to make the compromised devices more vulnerable to attacks. Other Android malware, Plankton [54], [55], [56] and Foncy IRC bot later emerged towards the end of 2012. Kaspersky reported that the latter was not as sophisticated and prevalent as Opfake and Fakeinst.

While mobile security was devising strategies to tackle the spread of emerged Android malware, new variants of Android malware emerged in 2013, namely Fave-Av-Reader, Plapka, Simplocker, Rough_Skype, Dendroid [57], among others. The most sophisticated among thousands of variants discovered in 2013 was Obad. Android malware Code obfuscation was the first experience with the emergence of Obad Trojan. Writers of Obad infused obfuscation techniques that enabled Obad to take the role of device administrator in the background. We can infer that Obad was a backdoor Trojan that used cracked sites and Playstore for pinging precise resources through pre-defined SMS strings. Financial platforms such as mobile banking apps, e-wallets, and credit card thefts were major attack goals for the Trojan, as highlighted by Austin [58]. The emergence of this malware trend leads to an increase in Android cybersecurity black markets where stolen data are sold. The obfuscation meth-

od adapted by 2013 Android malware developers to evade detection by anti-malware engines is a factor that advances the fast propagation of Obad Trojan.

Due to the obfuscation technique, the static analysis would be much harder to achieve by cybersecurity experts and anti-virus engineers than could be done on the previous trends. While root level exploit was common in the previous trend (2012), Obad exploits zero-day weaknesses to gain more and higher privileges on the infected devices.

The 4G-enabled Android devices involved a technological shift that motivated malware writers to exploit further vulnerabilities existing on Android phones via off-the-shelf creation of malware tools and deployment strategies. This led to many Android malware families being discovered in 2014; many samples displayed the same features seen in the previous variants. The notable Android malware family that exhibited unique characteristics from the already known samples between 2010 and 2013 is NotCompatible.CA as highlighted by Ariyapala et al. [59]. NotCompatible.C is self-protecting and persistent through encryption and redundant activities, thus making static analysis hard to achieve. Being a botnet kind of Android malware, over 8.5 million devices were infected via spam emails.

Notable impacts of NotCompatible.C included WordPress accounts cracking and the bulk purchase of event tickets from the infected devices. Unlike previous families, dynamic analysis became very difficult on NotCompatible.C due to its awareness of the emulated and virtual environments. Due to its obfuscated method, it can evade the vetting processes on play store and anti-virus products. Scalability, clustering, and memory analysis may be essential as the Android malware analysis approach with the annual increase in the sophistication and explosion of different Android families. The obfuscation of the botnet made the Android security threat more formidable. The mode of operation of NotCompatible.C malware as shown in Fig. 5, shows its propagation strategies.

C. Dark web advancement and new malware variant

In 2015, different Android malware emerged such as Spy, Simack, Jssmsers, Benews, Braintest,

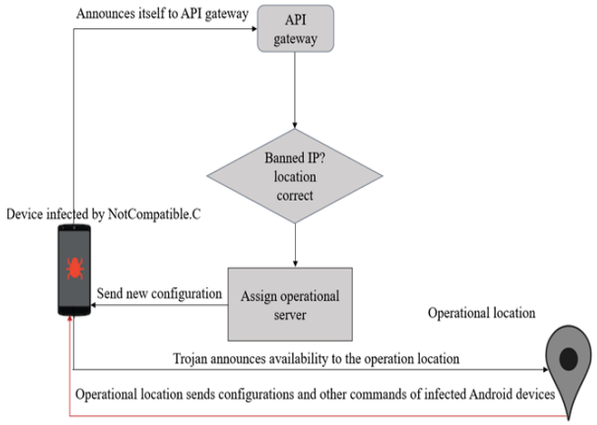

Fig. 5 Illustrating mode of operation of NOtCompatible.C Android malware.

Feabme, and Xbot [60]. However, an unknown Android Trojan is comparatively new and different from the former ones, which focuses on harvesting banking details via SMS interception. The Trojan specializes in sniffing banking-related SMS, emails, and forwarding the sniffed data to a hardcoded phone number and email service based in China. While analyzing the intercepted SMS, keywords such as balance, pay, bank, validation, and check are sniffed as part of the data collection and information gathering process. Several Android mobiles infected by the Trojan experienced brute-force which enabled the Trojan to take advantage of the infected devices to exploit the security vulnerabilities and collect sensitives information. Some researchers revealed that user privacy as mobile numbers stored in the database and address book faced security threats when stolen by hackers [61]. Cybercrimes such as identity camouflage become easy to perpetrate when the user's geographical location and phone number are is leaked. Also, many mobile banking apps require the owner's mobile number during registration associated with their location.

As the Dark web technologies advance, diverse means are provided where criminal actors (including malware attackers) engage in secure communications and transactions of malicious toolkits and other products and services. Android malware continued evolving with different attack strategies and evasion techniques. Android malicious Buyers and vendors began to exploit the security and business mechanisms on Tor using a multi-signature transaction and

encryption approach to spread malware. Secure communications and transactions on malicious applications as software packages became a business of interest on forums and vendor online shops [62], [63], [64]. Different Android malware families include Rumms, Krep, Triada, Descarga, Mazar_Bot, Rootnik, AndroidOS.Fusob, and DroidJack emerged in 2016 [65-67]. According to the mobile security report by Mead et al. [68], AndroidOS.Fusob Trojan ransomware was the most popular and persistent android malicious program in 2016 that infected users in different geographical locations including the UK, US, China, and Germany. Over 230 countries were attacked by Android malware with varying degrees of threat and impact. Some of the stolen information was sold in the dark web market.

One interesting observation is that Android malware began to evolve to infect wider geographical locations, unlike the previous variants and families. Hackers began to decompile legitimate applications and repackage them with embedded malicious code to sell to the marketplaces and increase financial gain. Android malware evolved to a more sophisticated level when AndroidOS.Fusob and DroidJack were used as RATs and can survive a factory reset. These variants were used for state-sponsored attacks and espionage according to Li et al. [69]. Due to their open-source nature, leaked sourced code, and special plugins, the Fully Undetected Remote Access Trojans (RATs) market began to mature with this evolvement of Android malware.

D. Smart malware evasion trends using technological techniques

Android malware took a new dimension when the repackaging of Android applications became very popular in official and third-party markets in 2017. Hackers began to repackage benign applications using reverse-engineering techniques. Consequently, trust in an application has diminished due to repackaging techniques by hackers. Trust in applications influences mobile users' decisions on which market store to download applications from. Mobile vendors must trust that mobile users get legitimate applications during purchases on the marketplace.

According to [70], the Dark Web became a web of cybercriminals where Android and other RATs are sold openly for high prices on Clearnet but with a lower price on Dark Web. Kaspersky reported that in China, AndroidOS.Fusob changes the PIN code and enables Android safety function by resetting the infected device PIN to their Passcode. Android malware continued to evolve through 2016. Different Android malware types significantly grew, especially with the growth in RiskTool. According to Kaspersky, RiskTool files increased from 29% to 43% in 2015 to 2016, respectively. According to the report, Trojan ransom experienced the most significant growth in 2016 with an increase of 4%, which was nearly 6.5 times higher than in 2015.

Trust must be a fundamental component of mobile applications. Mobile applications are being used daily for transactions and other inter-personal collaborations and interactions. However, the trustworthiness of these services and applications, especially in the market store, is still a concern that needs thorough security implementations and checks. The study by Khanmohammadi et al [71] highlighted that the percent of repackaging android applications grew to 54.38% in 2017 with permissions added in the repackaged applications. The number of malware attacks on Android mobile devices continued to rise from the beginning until the end of 2017.

According to Kaspersky Lab security bulleting [72], Android malware increased about 1.2 times more in 2017 than in the previous year. According to the report, rooting malware is the biggest security threat Android users experienced in 2017, and the percentage of its effects keeps increasing. Super-user rights were gained by the rooting malware (Ztorg) and system vulnerabilities were exploited. The rooting malware was distributed through the play store, which infected and modified over 100 Android applications. This malware family did not affect many devices due to the limited number of Android devices running older versions. While 230 countries were affected in 2016, the rooting Trojan infected only 161 countries in 2017, according to the Kaspersky report. To keep pace with the security threats presented by potential harmful applications (PHAs) [73], Google introduced multiple layer

security architecture during its review of Android security in 2017. The multiple layers of the security and protection architecture advanced to form Google play protection. Though Google play protection has been a fundamental security feature in Android, other features were added in 2017 for better identification of potentially harmful applications on Android devices. Features such as regular updates of Google play were introduced so that the update no longer depends on Over Air updates (OTAs) for security improvement. Our research, however, observed that Google play protect was not sufficient for the total protection of PHAs because its enablement was only on Android devices running 4.3+ versions.

Devices running lesser (older) versions were still subject to PHAs and application exploits. In summary, while the number of Trojan-SMS decreased significantly in 2017, Trojan-Ransomware increased by 5.22% in 2017 compared to 2016. In 2018, Android malware took a different dimension of attack, infection, and propagation strategies, though a built-in mechanism for defense against PHAs was enhanced in the previous year. Potential Harmful Applications infected mobile platforms that installed applications from outside the play store eight times more than those from Google play. While Google Play Protect played a significant role to reduce the rate of mobile infection in 2017, other protection mechanisms such as application sandbox [74], hardened APIs [75], discrete tamper-resistant [76], and BiometricPrompt [77] were developed in 2018 to bring about a reduction in Android malware attacks. The introduction of these security mechanisms in conjunction with platform improvements of Treble [78], [79], original equipment manufacturer (OEM) agreements and Android Enterprise Recommended has significantly advanced and improved the Android ecosystem security.

Despite all the security advancements, 0.11% of Android mobile devices were compromised by user-wanted (UW) PHAs called Chamois [80] in 2018. Other variants such as Snowfox, Cosiloon, BreadSMS, View SDK, Triada, CardinalFall EagerFonts, and Idle Coconut [81] later emerged with similar characteristics. Chamois was, however, judged to be more sophisticated and injected several sideloaded applications because it infected over 20 million android users. As demonstrated in Fig. 6, the backdoor generates invalid traffic, performs artificial application promotion, telephone fraud, and dynamic execution of additional plugins.

The User-wanted PHAs disabled SELinux and root Android devices by disabling the SELinux security feature. SELinux disablement led to increasing

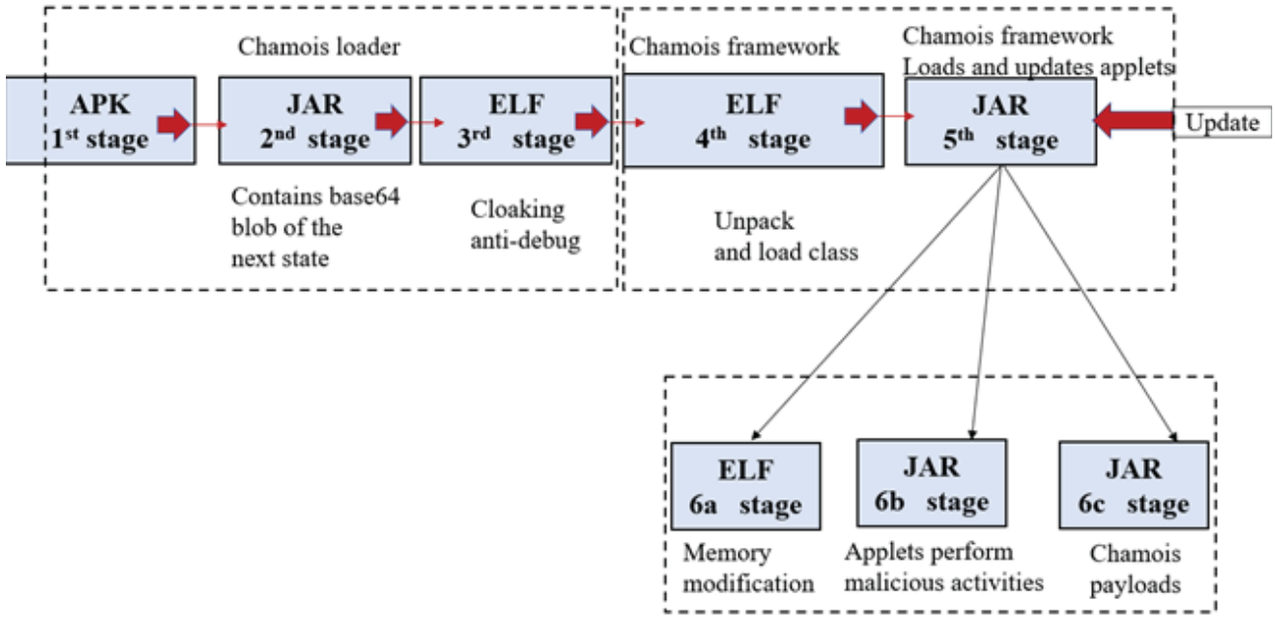

Fig. 6 Chamois backdoor operational propagation stages. Each stage is encrypted and obfuscated.

pre-installed PHAs and increased threats of backdoor SDKs. Also, the excessive privileges permit potential harmful applications to defend themselves against any attempt for removal by users. Backdoored SDKs code injected into genuine Android functionalities significantly enhanced the propagation of pre-installed PHAs that compromised Android device integrity, click fraud, and attribution fraud. Compared to applications downloaded outside of the play store, the rate of PHAs was high compared to those from Google play as shown in Fig. 7.

Android malware continues to increase in both scope and complexity, despite the security implantation in the Android operation system. The more the security experts deploy techniques to detect and prevent attacks, the more adversaries deploy alternative and innovative strategies to adapt to the current security situation. This was evident when a sophisticated Android malware family known as TimpDoor emerged in 2019 with unique attributes and rapid propagation and threats. TimpDoor malware bypasses the play store by infecting Android victims through SMS. According to the McAfee threat report [82], the TimpDoor malware family proves extremely effective by infecting more users than the older known Android malware families. The spyware exfiltrates victims' contact, photos, and SMS. The evolving functionality observed of TimpDoor is that the malware uses a SOCKS proxy that redirects traffic. The most probable attacks added by this evolution are click fraud and DoS attacks.

The most worrying characteristic of this threat is the use of filched data such as photos and phone contacts to create false accounts on social media and other online services to steal more identities of users and attack Android-based IoT devices. As shown by Kumar et al [83], the Android platform's integration with IoT-based applications facilitates malware propagation. IoT revolution has covered different spheres of life including remote monitoring, the healthcare sector, and there are many others that create attack platforms for extensive exploitation of Android-IoT devices. This is a result of the malicious data storage in the IoT blockchain which most of the time is undetected and hard to access for analysis. The study by Taylor et al [84] affirms that malware data deposited in blockchain history are easily transferred via the network and the propagation attack surface enlarges, thus infecting many devices. Though TimpDoor was more sophisticated, LeifAccess Android malware impacts were significantly felt in the USA more than in any other country.

2020 witnessed the tremendous effects of COVID-19 that resulted in lockdown worldwide. While the threat actor strategies and procedures are the same, organizations' exposure to risk levels has greatly increased due to slow response and recovery approaches during the pandemic. As employees continued working from home due to the COVID-19 pandemic, different variants of Android malware emerged. Most employees prefer to use their mobile devices for personal and busi-

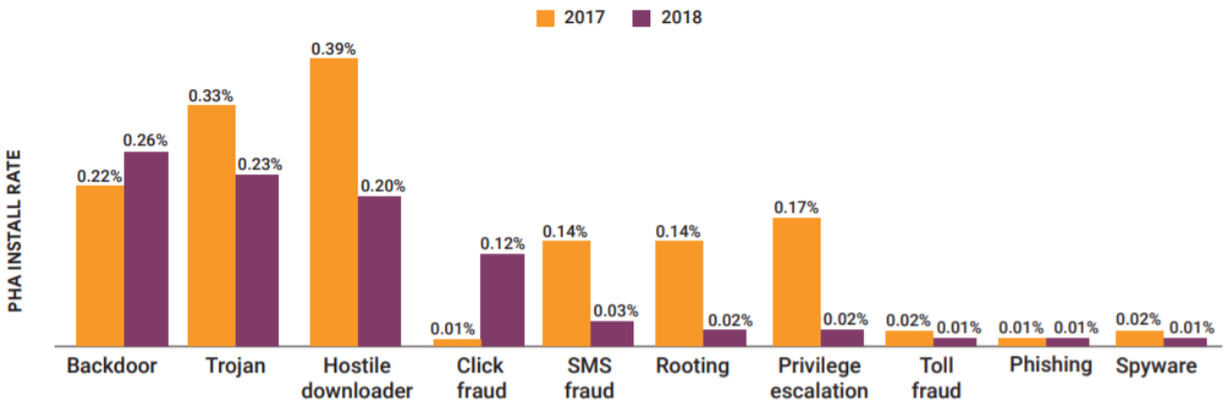

Fig. 7 Comparison of PHA categories distribution outside of Google Play in 2017 and 2018 [75].

ness transactions under a poorly protected home network. According to the Deloitte security report [85], the contact tracing application launched by the NHS has become a threat actor for social engineering leverage that tricks users into installing fake and malicious COVID-19 contact tracing apps. According to the report, the fake COVID-19 application is being used to deliver different threats.

A new Android mobile malware Unicorn emerged in Italy that targets doctors, pharmacies, businesses, and universities. The ransomware uses social engineering to encrypt users' devices and requests a ransom in euros. Other malicious threats such as email spam, fake landing pages, phishing, and so on emerged when four other variants of the same malware surfaced later. One of the major evasion strategies adopted by recent malware is the Trojan defense approach, as identified in the security report of ESET [86]. Table II summarises Android malware evolution from 2010 to 2020.

Based on the papers examined as part of this study, we classified mobile malware evolution into five (5) categories based on sophistication, characteristics, and intents:

Category 1: This group of mobile malware is characterized by annoying pop-ups and ads usually displayed on the mobile screen. The propagation mechanism is usually via SMS, MMS, and Bluetooth. The intent is for fun, behavioral software testing, knowledge testing, or both.

Category 2: This group of mobile malware is characterized by information theft and privacy violation. The propagation mechanism is usually via social engineering, drive-by download, and key-permutation. The intent is for knowledge testing and financial gain.

Category 3: This group of mobile malware is characterized by device rooting, jailbreaking, and rickrolling. The intent is for financial gain and physical damage to the mobile device. The propagation mechanism is usually via the third-party application and marketplace.

Category 4: This group of mobile malware is characterized by remotely accessing mobile devices. The intent is for financial gain, industrial espionage, vengeance, organization of state-sponsored attack, buffer overflow, remote monitoring, installation of other Trojans, spying, and stealing corporate secrets. The propagation mechanism is usually the internet.

Category 5: Our research referred to this group of mobile malware as modular malware. This group of mobile malware can gain administrative rights of a device and can perform a DDoS attack. The propagation mechanism is usually the internet.

E. Classification of Mobile Malware

Smartphone development and its popularity have brought about a surge in the number of mobile variants. Despite anti-malware advancement solutions, sophisticated malware variants use techniques such as code encryption, code obfuscation, among others to evade detection. The advent of COVID-19 has accelerated mobile and PC variants, because most workers work remotely using unsecured and weak security networks with no physical monitoring and the help of IT support teams. As businesses face economic insecurity due to the advent of the pandemic, the number of cyber threats such as mobile malware is also increasing correspondingly, as highlighted by Brown [87]. It will be unjust to expect employees who work at home using the home network with weak security to be able to protect themselves and their organizations from being attacked by malware without understanding malware variants. Our review examined some of the malware variants and their modus operandi.

1) Ransomware

Although ransomware is commonly experienced on computers, mobile devices are not immune from being infected with this type of malware. Ransomware attack locks the mobile screen and encrypts files with a displayed ransom message, usually demanding a Bitcoin payment. Android ransomware is currently increasing, and it is of paramount significance to have a defensive approach that will guarantee the data security of mobile users. Most of the defensive approaches are signature-based and, thus, ineffective for the current state-of-the-art malware variants. Mobile ransomware is a malicious variant whose design and operation block entrance

TABLE II
ANDROID MALWARE EVOLUTION

Year	Prominent malware	Malware type	Kind of havoc	mode of propagation	Description
2010	AndroidOS. DroidSMS.A	Trojan	Premium SMS	Botnet	A Trojan sends an SMS and charges the victim without his consent.
2010	Tap Snake	Spyware	Location monitoring	Native code execution	Sends the device location with the recorded phone conversation to a remote malicious server.
2011	DroidDream	Trojan	Device rooting	Code encryption	Roots devices and steals sensitive information from victims.
2012	Boxer	Trojan	Premium SMS	Via SMS	The Trojan automatically installs once the victim receives SMS
2012	Opfake	Trojan	Root-level exploit,	Drive-by-download	Performs update attacks.
2012	Fakeinst	Trojan	Update attack	Key permutation	Performs update attack. Compromises devices and makes them more vulnerable to more attacks.
2013	FakeDefender	Ransomware	Social engineering	Drive-by download	Prompts the user to buy a security app
2013	Obad	Backdoor	Zero-day attack	code obfuscation	Obad exploits zero-day weaknesses to gain more and high privileges on the infected devices.
2014	NotCompatible. CA	Trojan	Device side loading	Drive-by download	Self-protecting and persistence through encryption and redundant activities. Aware of the emulated and sandbox and evades detection. Sideloading apps to hinder security assurance.
2015	Acecard	Trojan	Apps Overlays	repackaging	Steals banking data of the victim.
2015	888.apk	Trojan	Brute force	Repackaging	The Trojan specializes in sniffing banking-related SMS, emails, and forwarding the sniffed data to a hardcoded phone number and email service based in China.
2016	HummingBad	Trojan	Rootkit	Drive-by download	Establishes persistent rootkit.
2016	Xbot	Ransomware	Locks screen and files	Code encryption	Steals banking credentials send premium SMS.
2016	AndroidOS. Fusob	Trojan-ransomware	RATs	Drive-by download	Remotely access infected devices. Demands ransom.
2017	ToastAmigo	Backdoor	Apps Overlays	repackaging	Deploys toast overlay attack to install more malicious apps
2017	Ztorg	Trojan	Device rooting	Play store	Super-user rights were gained by the rooting malware (Ztorg) and system vulnerabilities were exploited. The rooting malware was distributed through the play store.
2018	Chamois	Backdoor	RATs	Dynamic code loading	The backdoor steals OAuth tokens. Significantly enhances the propagation of pre-installed PHAs that compromised Android device integrity, click fraud, and attribution fraud.
2019	TimpDoor	Spyware	Click fraud	Java reflection	TimpDoor malware bypasses play store by infecting Android victims through SMS.
2019	Cerberus	Trojan	Apps Overlays	Drive-by download	Intercepts calls.
2019	XHelper	Trojan	Premium SMS	Drive-by download	Displays popup adds, redirects users, send premium SMS.
2020	Ghimob Unicorn	Ransomware	Encrypts files	Drive-by download	The ransomware malware adopts a Trojan defense approach to evade detection.

or access to a mobile device until the amount of money is paid. Recent research has shown that 74% of companies in the 21st century are under terrific ransomware siege, especially those whose operations are connected to mobile devices [88]. Mobile ransomware harvest data such as photos, videos, usernames, and passwords related to a financial transaction.

2) Adware

Initially, adware was known for the annoying and frustrating pop-up characteristics without any specific malicious intent. However, it has now moved from the realm of just pop-up displays to data collection. Some adware goes as far as rooting (for android) and jailbreaking (for Apple) mobile devices, while others have the capability of draining the device battery when not observed and prevented. Mobile adware such as Cydia [89] steals user data and modifiers mobile IMEI, IMSI, and steals android mobile Transaction numbers (mTAN). Mobile adware has evolved from creating banners and ads to easy and un-noticed mobile rooting and jailbreaking. Some create adverts as a link to lure victims into malicious sites for auto-download of malicious applications once visited. For instance, a banner or an ad may appear on your phone screen while online with the statement 'Amazon is giving out £350 worth of voucher cards, click the link below to claim yours. This trick harvests sensitive data used to carry out sophisticated attacks. These details are then used to launch an attack on the victim's mobile device. Some adware variants create backdoors on mobile devices when infected to facilitate further and future attacks. Some adware could deploy social engineering tactics to lure the victim into divulging sensitive information that is after that used for the attack.

3) Trojan

Android Trojans are camouflaged as legitimate Android applications. Trojans harvest sensitive information on a device, spy on the user's activities, delete the user's files, and can download other malicious activities. The study by Imtiaz et al [90] reports that some Android Trojans masquerade as legitimate mobile banking applications, mostly targeting android mobile phones. The research reported that an Android mobile unnamed Trojan "888.apk" intercepts and sniffs mobile banking transaction packets during SMS alerts and transaction commands such as Check, Validation, and pay as an attack banner grabbing process. Apart from the 888.apk mobile Trojan, Kaspersky reported the emergence of a new Android banking Trojan Svpeng known as Trojan-SMS.AndroidOS.Svpeng. Svpeng steals mobile banking credentials such as passwords and usernames upon launching a mobile banking application. The Trojan targeted only Russians using android phones and later people in other countries. Mobile Trojan horses are a dangerous set of mobile malware which on most occasions appear fictitious as beneficial applications but with hidden malicious content and action when executed. Some mobile Trojans can obliterate a whole mobile or computer drive when infected, while some serve as a backdoor for device remote control.

Malware writers apply the principle of social engineering as a means of gaining financial benefits from victims using SMS premium service. Through this strategy, victims subscribe to certain services or applications without their consent. Scammers usually use users' phone numbers or emails to execute this malicious scheme. Most malicious premium messages to victims seem very real and appealing such as: 'Know who blocks you on WhatsApp' 'Click here to see the message sent to you by a friend', 'Install battery speedometer to see how long your battery lasts', and 'Amazon is giving a free £25 to prime members'; click here to claim yours'. Hackers make these tricks look appealing and real to entice the victim. Once the phone number is supplied, an automatic subscription to your monthly mobile bill is activated for any SMS received or sent. For advanced SMS premium service attacks [91], the victim does not have to be tricked into giving his phone number. Hackers' banners grab the social networks account details of the victim, specifically his phone number. Therefore, it is advisable to critically look at the content of any email sent to you before opening it, especially if it looks suspicious. More importantly, it is worth not trusting easy financial claim links sent to

you if not from your financial institutions such as banks and cooperatives. It is pertinent to note that the SMS premium service charge attack cannot be achieved if the malware does not have permission to access the device service "send Text Message", which is the mobile privacy permission SMS service. Hence, understanding permission requests are very significant in fighting mobile SMS Trojans.

4) Rootkit

A rootkit is a mobile malware type that controls and exploits a mobile device through remote access. A rootkit comprises a loader, rootkit, and dropper. The rootkit gains administrative access and installs other applications at the backdoor that are malicious without the consent of the victim. Rootkit alters the configurations of a device once installed. Due to their silence and underground operations, it is very difficult to identify and remove the rootkit. Evasion techniques such as obfuscation are adopted by roots to make it stay undetected in a device for a long time. HummingBad [92] is an example of a rootkit that steals credentials by installing other malicious applications in the background to create fake ads.

5) Botnets and viruses

Botnets are compromised devices whereby an attacker remotely accesses and controls the infected devices. The botmaster controls the infected mobile phones without the knowledge of the victims. Botnets have become a serious threat to information and mobile security, as attacks such as DDoS are launched using mobile botnets. DoubleDoor [93] is an example of a popular mobile malware botnet. Mobile viruses are small computer codes built to attack devices operating in cellular environments, such as mobile phones and PDAs. They are computer programs whose designs are borne out of curiosity to gain general attention and target and exploit vulnerable mobile phones and other applications with a high degree of versatility. A mobile virus is propagated the moment an infected file or application is executed, causing a speedy escalation to connected devices and other application segments. The ruinous consequences of a virus on mobile devices and applications range from data loss, application loss, and device destruction on most occasions, if not discovered early. Some viruses invade detection and may be difficult to be identified by traditional detection mechanisms. When the running OS of memory in a device (mobile or computer) is infected with virus code, all the programs including the executable code running in the core memory of such a device can also be infected including its internal storage Fig. 8. The virus program first requests permission from the device OS to attach its code to the device object module, especially at the system start-up. After the septic virus code is invoked in the device memory, the virus then switches over and takes over the entire system. The infected code then spreads to the device operating system. In the case of a computer, a floppy disk serves as the object code, which helps in virus invocation and execution at system start-up.

6) Worms

Android worms are malicious codes that black hackers develop for malicious intents and operations for mobile devices. Worms have the capability to self-replicate from one susceptible mobile device to another with little or no external trigger such as human behavior. Mobile worms assume different file formats, such as pdf and file extensions, to invade a vulnerable device. The peculiar infection

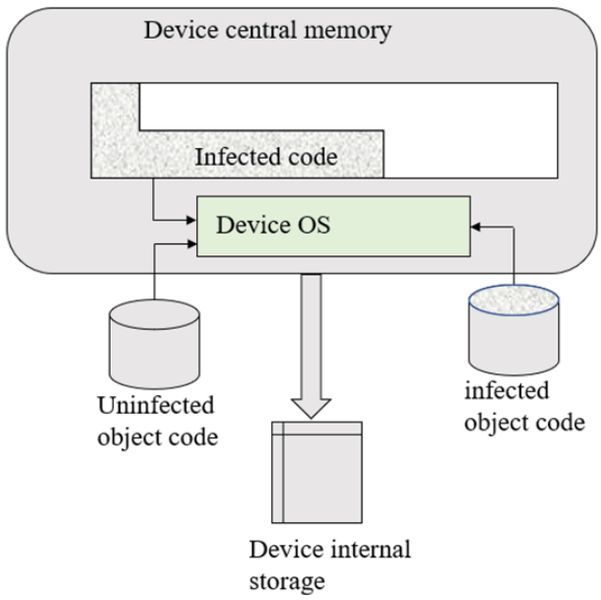

Fig. 8 Mobile virus infection strategy.

character of worms is that the payload executes once on the initial device and later escalates to other targeted devices via attack vectors such as TCP, email, IP, SMS, etc. Based on the papers examined as part of this study, we classified mobile worms into five (5) main categories with their major characteristics (see Table III) as follows:

Binary file worms: These are forms of worms that infect device executable files. They are usually programmed in machine language for easy payload distribution.

Multi-partite worms: These are worms with the capability of affecting mobile and computer boot sectors and executable files. This form of worm is rare.

Script file worms: These are worms technically written in human-readable form, which requires translation, by an interpreter to perform machine-executable.

Binary stream worms: The infection vector deployed by this form of worms is pure via a network connection. It relies on the device to be linked to the network before implementing its infection.

Macro worms: These are worms that infect applications and data files such as documents. Macro worms seem to be the most common. To reduce worm infections on Android devices and mobile platforms in general, it is pertinent to regularly upgrade the mobile OS to the latest versions to avoid mobile susceptibility to signature-based and zero-day attacks. A summary of the malware classes and their distinct but related behavior is presented in Table III.

The use of the latest antivirus engines is very significant, but it is recommendable to ensure that the latest mobile device patches are constantly installed and updated. By this, the worm infection rate and worm propagation can be considerably reduced. This strategy is essential, because our research believes that the worm's infection rate on mobile devices is directly proportional to the propagation speed. An increase in worm removal on affected devices can also subdue its propagation, thus reducing the number of mobile devices that can be contaminated. Other types of Android malware include Spyware and key loggers. Android OS fragmentation and open source have created security loopholes resulting in the great increase in attacks we are seeing now. Apart from the entire android platform, the majority of the android applications have untrusted digital signatures within their security parameters. While Apple has a proactive approach to malware and general threats, Google is more concerned about taking reactive defense approaches when a threat occurs. In addition, while iOS sticks to Xcode [94]

TABLE III
MOBILE MALWARE VARIANTS WITH THEIR DISTINCTIVE CHARACTERISTICS.

Mobile Malware variants	Characteristics
Mobile Ransomware	Locks out users' documents Encrypts files Request for ransoms usually in the form of bitcoin
Mobile adware	Creates annoying pop-ups Creates backdoors Auto-download Use social engineering tactics
Mobile SMS Trojans	Does not replicate itself Creates backdoors May engage in secondary infection Does not infect other files Utilizes social engineering principle for payload execution Uses SMS, Links, and MMS for distribution
Mobile worms	Self-replicating May have no payload Could be benign or malignant
Mobile virus	Written in small sizeable codes Highly versatile Exceedingly reoccurring during propagation to other devices Effective in data loss and device damage Wide variety of functions
Botnets	An attacker remotely accesses and controls the infected devices
Rootkit	Gains administrative access and at the backdoor and installs other applications

with default IDE choice with minimal platforms which are maximally managed and embedded with better security primitives, Android has several platforms with little security entrenchment. These factors made Android devices the devices most infected by malware. The report produced by Li et al [95] affirmed that two-thirds of mobile malware targeted Android platform devices. This shows the degree of android vulnerability to malware. It, therefore, calls for appropriate security strategies to address this problem timely.

IV. Mobile Malware Infection Vectors

Infection strategies are attack vectors through which designed mobile malware access the target device to execute their payload. Malware files remain non-executable and uninfected, until a path is created via which access to the device could be achieved. While malware was written earlier, its propagation rate was slow compared to recent malware. The speed of malware propagation is significantly enhanced by internet advancement. Internet connectivity is one of the major routes via which malware payloads are easily transmitted to other subsidiaries such as Bluetooth, SMS, cellular networks, Wi-Fi, physical access, and USB-PC connections.

A. Bluetooth/SMS distribution

Mobile malware such as Commonwarrior was discovered in 2005 and spread through Wi-Fi and SMS as an attack vector. As cited in Fig 9, mobile malware spreading through this medium has a large spectrum of infecting an entire continent, since there is nothing to restrict the spread except the exhausted balance of the user's device. Pebler mobile is known to infect mobile phones by exploiting vulnerabilities found in Wi-Fi and network connectivity to devices. The only limitation of this attack vector is that mobile devices with no internet features suffer little. As technology advances, mobile devices with embedded Bluetooth technology can communicate and share files with nearby devices, which are a few meters away. Some Trojans exploit Bluetooth to spread to other devices. The danger of this attack vector is that although it can only infect nearby devices, it can cause a devastating septicity where many Bluetooth devices are enabled [96].

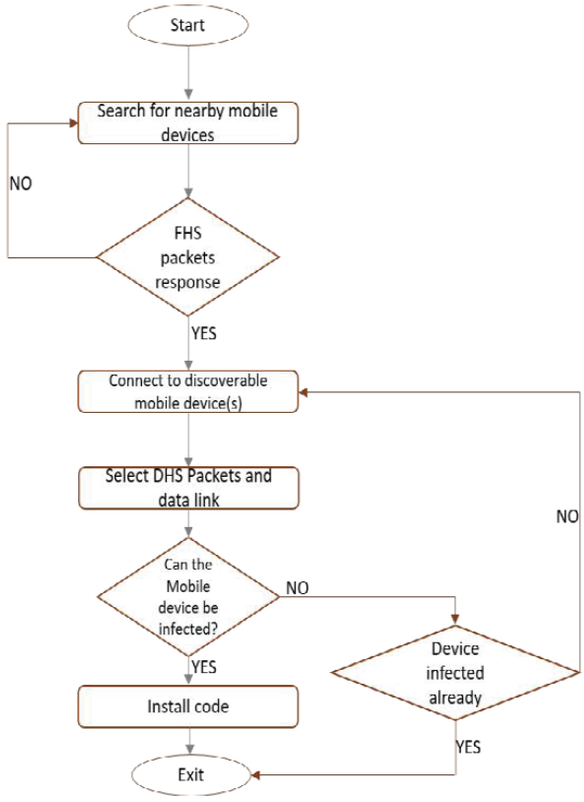

Fig. 9 Malware propagation using Bluetooth technique.

Bluetooth attack vector has a high threshold of spreading malware since the majority of mobile users share mobile files such as pictures, videos, and audio files without considering the consequences. Advancement in Bluetooth technology to enhance the location down to centimetre-level precision has created and expanded mobile malware propagation conduit. For instance, the inclusion of a point of interest application (POI) [97] for information solutions enhances the speedy replication of worms using Bluetooth. SMS is another mobile malware distribution strategy where malware payload is being disseminated to mobile or devices through SMS or MMS. The propagation could either be through sending SMS or MMS from one mobile device to another or from the cloud to the mobile device. Malware uses SMS as a distribution attack vector to mobile devices where the target device is infected to send illegal and unauthorised texts, and the victim is directly charged for the call or text message.

B. USB/network to device distribution

Apart from the Bluetooth infection strategy, USB is one of the distribution strategies. Different developers upload and update their malicious codes on the Apps store, camouflaging them as genuine software. When the user installs a malicious application, malware unknowingly infects the user's device. When mobile devices connect to PCs through USB, this offers the opportunity for a malware-infected PC to transmit to the victim's device. The attack vector serves as a thumb drive for PC-Mobile malware infection. This is where malware is distributed from Universal Serial Bus (USB) to any device, which could be PCs and mobile devices. As was announced by IBM, many USB sticks with the following product model "2071, 02A and 10A are infected with malware which has access to the device via USB cables or port when a connection is established between the USB and the device. When a mobile device is connected via a USB port to an infected computer, malware distribution to the phone becomes inevitable. This distribution technique is used by malware in the form of ads or applications connected to the internet and masquerading as real applications.

C. Market/application to device distribution

Application to Device known as A2D is a distribution mechanism where the mobile malware depends solely on the application vulnerability to distribute itself. An example of android malware, which exhibits spreading and infection vector via A2D approach, is Andr/Opfake [98]. In the Market to Device strategy in distributing malware, a malicious application is uploaded into the application store market. The infection by users is dependent on the application reception in the market and user's installation on their mobile phones. On a general note, some of these infections happen when users make conscious resolutions to carry out an act. Behavior like scanning barcodes, QR codes, or logging into an unsecured compromised Wi-Fi network is an example that led to users' mobile devices to be exploited by malware.

In summary, we assume a malware type could infect a susceptible mobile device after effective communication with a contagious device if an immunity to that same type of malware is not developed. Based on the meta-analysis of the infection strategies, we assume that when a mobile device becomes infected, it can develop immunity to that same type of malware and can recover if adequate security strategies are applied immediately. However, such a device will remain vulnerable to other variants of the same malware after recovery. Also, an infected device has the capacity to spread the malware if not kept under control.

V. Classification of Smart Malware Based on Behavioral

Different criteria are used in classifying mobile malware such as classification based on device-platform [99], [100], family [101], file system [102], resource consumption [103], and many other criteria. Our research uses behavioral attributes as a major classification criterion of mobile malware. Under behavioral attributes, our research focused mainly on privilege escalation and attack goals as discussed in the subsection.

Malware privilege escalation has attack goals. For instance, people downloading pornographic files do so to gratify their carnal urges, just like those who indulge in online provocation and harassment do so to have power over the other party. In addition, just like any other cybercrime, the goals behind every cybercrime are financial incentives, power greed, adventure, and vengeance. Some malicious activities on mobile devices are to steal sensitive personal credentials, while others are for SMS premium where charges are made without embarking on any service or SMS by the user unknowingly.

A. Classification based on privilege escalation

Privilege means what a device user is allowed or permitted to do on such a device. Examples of such include file editing or modifications. In the context of our research, it is viewed as the art of malware exploiting a vulnerability, bug, configuration, or design flaw of a mobile device or application to have enough unauthorized privileges to access mobile resources. When this occurs, malware reads and writes to files, may insert or attach a permanent backdoor see Fig. 10.

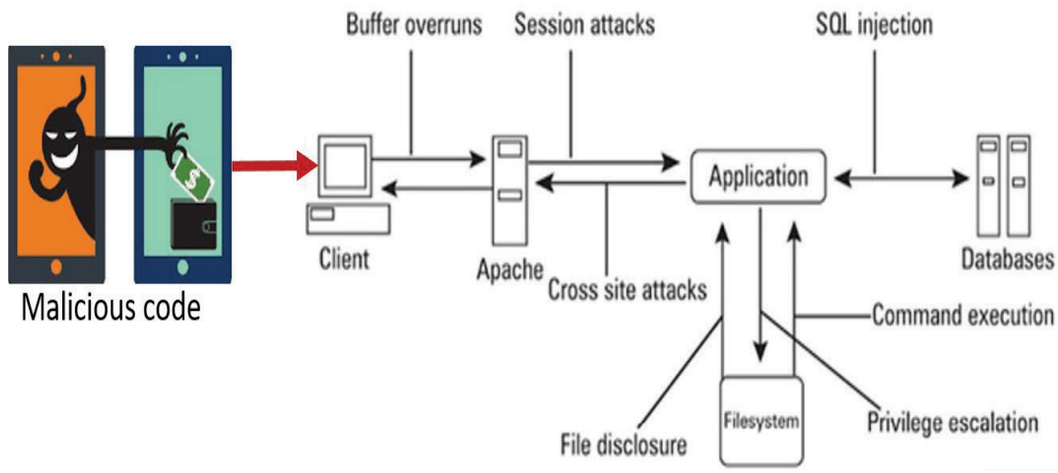

Fig. 10 Mobile malware Privilege escalation illustration.

Malware exploits some strategies to gain the required privilege. Some of these strategies could be user manipulation or technical exploitation. The technical exploitation path usually followed by malware to gain escalated privilege to mobile devices is through platform misconfiguration or technical susceptibility. Malware technical exploitations modify the security restrictions of a device. Once this is accomplished, exploiting other vulnerabilities on the affected system becomes very easy. This technical exploitation malware imbibes to achieve privilege escalation including buffer overruns, session attacks, SQL injection, cross-site attacks, file disclosure system vulnerability, and networking configuration flaws.

The attack behavior and goals include sabotage, spam, and service misuse. This analysis clearly shows that mobile malware displays different behavioral sets. It is worthy to note that the mobile malware attack goal has different categories of incentives, which are interwoven. It means that an attack goal can have more than one motivation. For instance, SPAM as an attack goal has both personal information theft and financial profit as motivation types.

B. Classification based on attack goals

Though malware keeps evolving to take different attack trajectories, their attack goals and motivations remain the same (see Fig. 11). While some malware writers could focus on stealing sensitive information as a primary step upon which subsequent attacks could be relied upon, others focus on the actual attack goal in their code implementation. Our research classified mobile malware attack goals based on their motivation type and behavior related to the motivations. Table IV shows the motivation types and major attack goals classified in our research. Cybercriminals perform attacks to achieve one form of intention or the other. This means that for every attack, there is an equal motivation behind it. Just as malware writers develop malicious applications for different motives such as financial profit, identity theft, industrial espionage, and a host of others, people that use these applications also have motives behind their usage. Based on their characteristics, mobile malware deploys different infection strategies based on the attack goals.

We observed that the motivations behind every mobile attack are different: financial, power, greed, adventure, and vengeance. While some malicious activities on mobile devices target sensitive personal credentials, others are for SMS premium where charges are made without embarking on any service or SMS by the user unknowingly. The attack behavior and goals include sabotage, spam, and service misuse. These are pure types of motivations for mobile malware attacks.

The attack schemes that formed the behavior related to those motivations could include eavesdropping, profiling, and loggers. Kocher et al [104] show how to pattern malicious behavior using security inspection

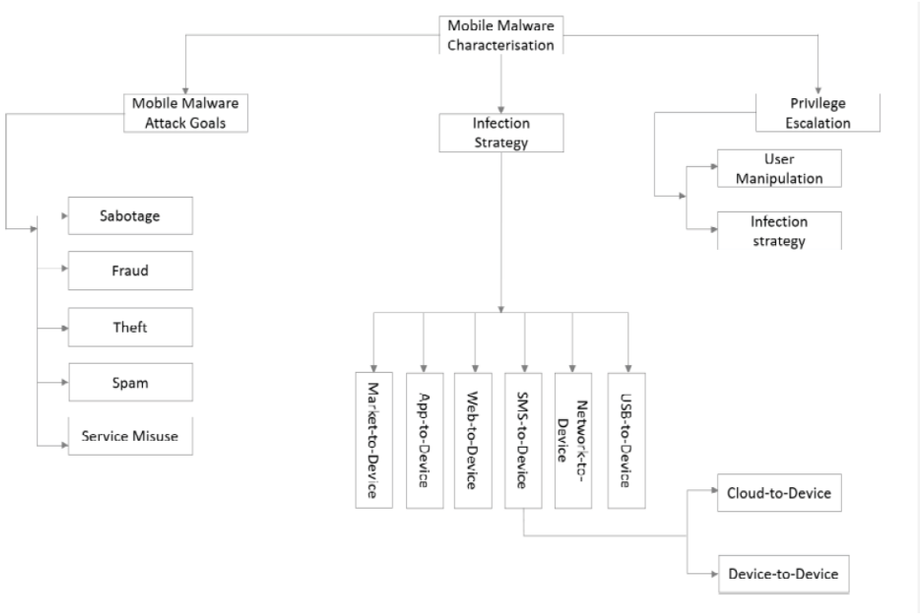

Fig. 11 Mobile malware characterization.

TABLE IV
MOBILE MALWARE ATTACK GOALS

Major Attack Goals					
Motivations	**Sabotage**	**Fraud**	**Data Theft**	**Spam**	**Misuse of Service**
Types of Motivations	Financial profit* Industrial Espi-* onage	Financial profit* ID theft* Personal Informa-* tion Theft Industrial Espio-* nage	Financial profit* ID theft* Personal Information* Theft Industrial Espionage*	Financial profit* Personal Infor-* mation Theft	Financial profit
Behaviour Related to the Motivations	Eavesdropping* SMS-Multimedia-Photo* Audio* Video*	Loggers* • Touch • Key	Loggers* • Touch • Key	Profiling * • Apps • Location	Combination of any of the previous

strategies. This confirms that mobile malware exhibits different attack goals during execution. It is worthy to note that mobile malware attack goals have different categories of motivations, which are interwoven. This means that an attack goal can have more than one motivation. For instance, SPAM as an attack goal has both information theft and financial profit as motivation types.

The unusual behavior of an application should be reported promptly. During application download and installations, mobile application plugins and codecs are pointers to be observed that the app is from a legitimate store. Mobile users could deploy software solutions from Enterprise Mobility Management to enhance the security on enterprise devices. These security strategies could help reduce the impact of the rising mobile malware threats.

VI. CONCLUSION

Malware attacks on mobile devices are increasing with the increase in the number of mobile applications published on the App and Play store daily.

Furthermore, mobile malware infection increases as mobile technology keep advancing. Most of the emerging mobile functionalities constitute the attack vectors malware deploys to infect mobile devices. For instance, the first-generation mobile malware could not spread quickly due to low knowledge of wireless hacking, short Bluetooth range coverage, a small Wi-Fi network population, and the lack of cross-platform propagation. Other factors that enhance the spread of mobile malware include advancement in threat dimensions, improved security, and business communication on Tor using multi-signature transaction and encryption approach, mobile platforms' integration with the IoT-based applications, the emergence of evasion techniques, and the advancements in mobile malware Toolkits on the dark web. To achieve the aim of the paper, we conducted an up-to-date study of mobile malware evolution and infection strategies. This enabled us to classify mobile malware evolution trends into distinct categories based on their sophistication, characteristics, and attack intents. We identified factors that limited the fast spread of the early mobile malware such as lack of mobile OS standardization, lack of mobile OS cross-platform, and lack of Bluetooth technological advancements in data communication. Finally, we identified factors that enhanced the fast spread of recent mobile malware. These included the advancement in threat dimensions, improved security and business communication on Tor using a multi-signature transaction and encryption approach, mobile platforms' integration with the IoT-based applications, the emergence of evasion techniques, and the advancements in mobile malware Toolkits on the dark web.

Furthermore, this paper has discussed research conducted from 2000-2020 on mobile malware evolution with their infection strategies. In the end, the paper identifies the need to analyse the existing detection techniques to identify their strengths and weaknesses to help develop more robust and accurate tools for an Android malware detection standpoint. We suggest the need for a malware infection model to prevent mobile malware spread among mobile platforms with random additive perturbations of infection rate. This strategy will help to understand the immunity state of a mobile device during and after recovery from malware infection. The effect of the random perturbation on malware stability behaviour might be essential in determining some transient characteristics of malware infection states.

Acknowledgment

This work is supported by the Petroleum Technology Development Fund (PTDF) under Grant PTDF/ED/PHD/AMA/1245/17-17.

References

[1] E. Goh and M. Sigala, "Integrating Information & Communication Technologies (ICT) into classroom instruction: teaching tips for hospitality educators from a diffusion of innovation approach," *J. Teach. Travel Tour.*, vol. 20, no. 2, pp. 156–165, 2020, doi: 10.1080/15313220.2020.1740636.

[2] Z. G. Shatri, "Advantages and disadvantages of using information technology in learning process of students," *J. Turkish Sci. Educ.*, vol. 17, no. 3, pp. 420–428, 2020, doi: 10.36681/tused.2020.36.

[3] L. Maglaras, G. Drivas, N. Chouliaras, E. Boiten, C. Lambrinoudakis, and S. Ioannidis, "Cybersecurity in the Era of Digital Transformation: The case of Greece," in *2020 Int. Conf. Internet Things Intell. Appl. ITIA 2020*, no. September 2017, pp. 0–4, 2020, doi: 10.1109/ITIA50152.2020.9312297.

[4] H. S. Lallie et al., "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the paandemic," *Comput. Secur.*, vol. 105, p. 102248, 2020, doi: 10.1016/j.cose.2021.102248.

[5] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic," *TechRxiv Powered by IEEE*, pp. 1–6, 2020, doi: 10.36227/techrxiv.12278792.v1.

[6] L. M. Cristea, "Current security threats in the national and international context," *J. Account. Manag. Inf. Syst.*, vol. 19, no. 2, pp. 351–378, 2020, doi: 10.24818/jamis.2020.02007.

[7] P. McLaren, G. Russell, and B. Buchanan, "Mining malware command and control traces," in *Proc. Comput. Conf. 2017*, vol. 2018-January, no. July, pp. 788–794, 2018, doi: 10.1109/SAI.2017.8252185.

[8] M. S. Saleem, J. Misic, and V. B. Misic, "Examining Permission Patterns in Android Apps using Kernel Density Estimation," in *2020 Int. Conf. Comput. Netw. Commun. ICNC 2020*, pp. 719–724, 2020, doi: 10.1109/ICNC47757.2020.9049820.

[9] J. Gamba, M. Rashed, A. Razaghpanah, J. Tapiador, and N. Vallina-Rodriguez, "An analysis of pre-installed android software," in *Proc. - IEEE Symp. Secur. Priv.*, vol. 2020-May, pp. 1039–1055, 2020, doi: 10.1109/SP40000.2020.00013.

[10] J. Mcgiff, W. G. Hatcher, J. Nguyen, W. Yu, E. Blasch, and C. Lu, "Towards Multimodal Learning for Android Malware Detection," in *2019 Int. Conf. Comput. Netw. Commun. ICNC 2019*, pp. 432–436, 2019, doi: 10.1109/ICCNC.2019.8685502.

[11] Oxera, "Android in Europe: Benefits to consumers and business," Oct. 2018. [Online].Available: https://www.oxera.com/wp-content/uploads/2018/10/Android-in-Europe-1.pdf

[12] A. Adekotujo, A. Odumabo, A. Adedokun, and O. Aiyeniko, "A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS," *Int. J. Comput. Appl.*, vol. 176, no. 39, pp. 16–23, 2020, doi: 10.5120/ijca2020920494.

[13] A. Gerber and C. Clifton, *Learn Android Studio. Build Android Apps Quickly and Effectively*, NY, USA: Apress, May 2015.

[14] S. Mierzwa, S. RamaRao, J. A. Yun, and B. G. Jeong, "Proposal for the Development and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health," *Int. J. Cybersecurity Intell. Cybercrime*, vol. 3, no. 2, pp. 48–61, 2020, [Online]. Available: https://vc.bridgew.edu/ijcic/vol3/iss2/4

[15] M. Adeel and L. N. Tokarchuk, "Analysis of mobile P2P malware detection framework through Cabir & Commwarrior families," in *Proc. - 2011 IEEE Int. Conf. Privacy, Secur. Risk Trust IEEE Int. Conf. Soc. Comput. PASSAT/SocialCom 2011*, pp. 1335–1343, 2011, doi: 10.1109/PASSAT/SocialCom.2011.243.

[16] E. Johns, "Cyber Security Breaches Survey 2020," *Comput. Fraud Secur.*, vol. 2020, no. 4, p. 4, 2020, doi: 10.1016/s1361-3723(20)30037-3.

[17] Marsh & McLennan and Zurich Insurance Group, "The Global Risks Report 2020," 2020. [Online].Available: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[18] S. Shi and J. Yin, "Global research on carbon footprint : A scientometric review," *Environ. Impact Assess. Rev.*, vol. 89, no. March, p. 106571, 2021, doi: 10.1016/j.eiar.2021.106571.

[19] A. P. Namanya, A. Cullen, I. U. Awan, J. P. Disso, and R. Kit, "The World of Malware : An Overview," in *2018 IEEE 6th Int. Conf. Future Internet Things Cloud (FiCloud)*, 2018, pp. 420-427, doi: 10.1109/FiCloud.2018.00067.

[20] L. J. García Villalba, A. L. Sandoval Orozco, A. López Vivar, E. A. Armas Vega and T. Kim, "Ransomware Automatic Data Acquisition Tool," *IEEE Access*, vol. 6, pp. 55043-55052, 2018, doi: 10.1109/ACCESS.2018.2868885.

[21] T. Szuba and D. Sztuba, "Can Adam Smith's Invisible Hand phenomenon be used for the analysis of Fourth Estate's impact and behavior?," in *2020 Int. Jt Conf. Neural Netw. (IJCNN),* 2020, pp. 1-8, doi: 10.1109/IJCNN48605.2020.9207576.

[22] W. Pranoto, "Malicious Software Analysis," (in Indonesian), *CyberSecurity dan Forensik Digital,* vol. 1, no. 2, pp. 62–66, 2018, doi: 10.14421/csecurity.2018.1.2.1374.

[23] S. Levy and J. R. Crandall, "The program with a personality: Analysis of Elk cloner, the first personal computer virus," *arXiv:2007.15759*, 2020. [Online]. Available: https://arxiv.org/abs/2007.15759

[24] H. J. Highland, "History of computer viruses - the famous `trio'," *Comput. Secur.*, vol. 16, no. 5, pp. 416–429, 1997, doi: 10.1016/S0167-4048(97)82246-8.

[25] L. Fu, "Design of hidden communication remote monitoring based on C / C MFC," *Proc. - 2019 4th Int. Conf. Mech. Control Comput. Eng. ICMCCE 2019*, pp. 589–591, 2019, doi: 10.1109/ICMCCE48743.2019.00135.

[26] CheckPoint Security, "5 TH GENERATION CYBER ATTACKS ARE HERE AND MOST BUSINESSES ARE BEHIND A New Model For Assessing and Planning Security," 2018, [Online]. Available: https://www.checkpoint.com/downloads/product-related/whitepapers/preventing-the-next-mega-cyber-attack.pdf

[27] M. Bartolo et al., "Urgent Measures for the Containment of the Coronavirus (Covid-19) Epidemic in the Neurorehabilitation/Rehabilitation Departments in the Phase of Maximum Expansion of the Epidemic," *Front. Neurol.*, vol. 11, no. April, pp. 1–6, 2020, doi: 10.3389/fneur.2020.00423.

[28] J. Kaur, "Taxonomy of Malware : Virus , Worms and Trojan," *Int. J. Res. Anal. Rev.*, vol. 6, no. 1, pp. 192–196, 2019.

[29] P. R. Shah, Y. Shah, and S. Madan, "Mobile Viruses," in *IJCA Proc. Int. Conf. Recent Trends Info. Technol. Comput. Sci.*, Mar. 2012, pp. 42–48.

[30] M. Chikapa and A. P. Namanya, "Towards a fast off-line static malware analysis framework," in *6th Int. Conf. Future Internet Things Cloud Workshops*, 2018, pp. 182–187, doi: 10.1109/W-FiCloud.2018.00035.

[31] S. Pillet et al., "Contamination of healthcare workers' mobile phones by epidemic viruses," *Clin. Microbiol. Infect.*, vol. 22, no. 5, pp. 456.e1-456.e6, 2016, doi: 10.1016/j.cmi.2015.12.008.

[32] R. Mayrhofer, J. Vander Stoep, C. Brubaker, and N.

Kralevich, "The android platform security model," *arXiv:1904.05572*, 2019. [Online]. Available: https://arxiv.org/abs/1904.05572

[33] M. R. Khan, R. C. Tripathi, and A. Kumar, "A malicious attacks and defense techniques on android-based smartphone platform," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8 Special Issue 3, pp. 361–369, 2019.

[34] N. R. Techniques, H. D. D. Expose, A. Target, and M. Lucrative, "McAfee Labs Threats Report: December 2018," *Comput. Fraud Secur.*, vol. 2019, no. 1, p. 4, 2019, doi: 10.1016/s1361-3723(19)30004-1.

[35] B. Runciman, "Cybersecurity Report 2020," *ITNOW*, vol. 62, no. 4, pp. 28–29, 2020, doi: 10.1093/itnow/bwaa103.

[36] F. Alswaina and K. Elleithy, "Android malware family classification and analysis: Current status and future directions," *Electron.*, vol. 9, no. 6, pp. 1–20, 2020, doi: 10.3390/electronics9060942.

[37] M. O. Topgul and E. I. Tatli, "The Past and Future of Mobile Malwares," in *7th Int. Conf. Inf. Secur. Cryptol.*, Turkey, 2014, pp. 123–129.

[38] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustain. Cities Soc.*, vol. 66, no. October 2020, 2021, doi: 10.1016/j.scs.2020.102655.

[39] A. Baranchuk et al., "Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?," *J. Am. Coll. Cardiol.*, vol. 71, no. 11, pp. 1284–1288, 2018, doi: 10.1016/j.jacc.2018.01.023.

[40] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *J. Telecommun. Inf. Technol.*, no. 1, pp. 113–124, 2019, doi: 10.26636/jtit.2019.130218.

[41] Z. Zhu and T. Dumitras, "FeatureSmith : Automatically Engineering Features for Malware Detection by Mining the Security Literature," in *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur.*, Vienna, Austria, pp. 767–778, 2016, doi: 10.1145/2976749.2978304.

[42] S. K. Sasidharan and C. Thomas, "ProDroid – An Android malware detection framework based on profile hidden Markov model," *Pervasive Mob. Comput.*, vol. 72, p. 101336, 2021, doi: 10.1016/j.pmcj.2021.101336.

[43] J. Spaulding, A. Krauss, and A. Srinivasan, "Exploring an Open WiFi Detection Vulnerability as a Malware Attack Vector on iOS Devices," in *7th Int. Conf. Malicious Unwanted Softw.*, 2012, pp. 87–93, doi: 10.1109/MALWARE.2012.6461013.

[44] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding Users' Requirements for Data Protection in Smartphones," in *IEEE 28th Int. Conf. Data Eng. Workshops*, 2012, pp. 228-235, doi: 10.1109/ICDEW.2012.83.

[45] A. Mathur, L. M. Podila, K. Kulkarni, Q. Niyaz, and A. Y. Javaid, "NATICUSdroid: A malware detection framework for Android using native and custom permissions," *J. Inf. Secur. Appl.*, vol. 58, no. 1, p. 102696, 2021, doi: 10.1016/j.jisa.2020.102696.

[46] P. Yan and Z. Yan, "A survey on dynamic mobile malware detection," *Softw. Qual. J.*, vol. 26, no. 3, pp. 891–919, 2018, doi: 10.1007/s11219-017-9368-4.

[47] T. H. Huang and H. Kao, "R2-D2: ColoR-inspired Convolutional NeuRal Network (CNN)-based AndroiD Malware Detections," in *2018 IEEE Int. Conf. Big Data (Big Data)*, 2018, pp. 2633-2642, doi: 10.1109/BigData.2018.8622324.

[48] V. Rastogi, Y. Chen, and X. Jiang, "DroidChameleon : Evaluating Android Anti-malware against Transformation Attacks," in *ASIA CCS '13: Proc. 8th ACM SIGSAC Symp. Inf. Comput. Commun. Secur.*, China, May 2013, pp. 329–334, doi: 10.1145/2484313.2484355.

[49] D. Wang, H. Shu, F. Kang, and W. Bu, "A Malware Similarity Analysis Method Based on Network Control Structure Graph." In *2020 IEEE 11th Int. Conf. Softw. Eng. Serv. Sci. (ICSESS)*, Beijing China, Oct. 2020, pp.16-18, doi: 10.1109/ICSESS49938.2020.9237633.

[50] P. Yan and Z. Yan, "A survey on dynamic mobile malware detection," *Softw. Qual. J.*, vol. 26, no. 3, pp. 891–919, 2018, doi: 10.1007/s11219-017-9368-4.

[51] M. Yousefi-azar, L. G. C. Hamey, V. Varadharajan, and S. Chen, "Malytics : A Malware Detection Scheme," *IEEE Access*, vol. 6, pp. 49418–49431, 2018, doi: 10.1109/ACCESS.2018.2864871.

[52] S. M. Gene and W. Hongyan, "Analyzing and Recognizing Android Malware via," in *2017 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, Changchun, China, Oct. 2017, pp. 17-20, doi: 10.1109/CyberC.2017.36.

[53] Meng, X., "An integrated networkbased mobile botnet detection system," Ph.D. dissertation, Dep. Comput. Sci., Univ. London, UK, 2018.

[54] M. Ashawa and S. Morris, "Analysis of Android Malware Detection Techniques: A Systematic Review," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 3, pp. 177–187, 2019, doi: 10.17781/p002605.

[55] S. Y. Yerima, S. Sezer, and G. Mcwilliams, "Analysis of Bayesian Classification based Approaches for Android Malware Detection Analysis of Bayesian Classification based Approaches for Android Malware Detection," *IET*

Inf. Secur., vol. 8, no. 1, pp. 25–36, 2014, doi: 10.1049/iet-ifs.2013.0095.

[56] M. Yusof, M. M. Saudi, and F. Ridzuan, "A new mobile botnet classification based on permission and API calls," in *Proc. - 2017 7th Int. Conf. Emerg. Secur. Technol. EST 2017*, pp. 122–127, 2017, doi: 10.1109/EST.2017.8090410.

[57] M. Ashawa and S. Morris, "Host-Based Detection and Analysis of Android Malware: Implication for Privilege Exploitation," *Int. J. Inf. Secur. Res.*, vol. 9, no. 2, pp. 871–880, 2019, doi: 10.20533/ijisr.2042.4639.2019.0100.

[58] M. Kazdagli, V. J. Reddi and M. Tiwari, "Quantifying and Improving the Efficiency of Hardware-based Mobile Malware Detectors," in *49th Annu. IEEE/ACM Int. Symp. Microarchitecture (MICRO),* Taipei, Taiwan, Oct. 2016, pp. 1–13, doi: 10.1109/MICRO.2016.7783740.

[59] K. Ariyapala, G. D. Hoang, H. A. Huynh, K. N. Wee, and M. Conti, "A Host and Network Based Intrusion Detection For Android Smartphones," in *2016 30th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Switzerland, Mar. 2016, pp. 849-854, doi: 10.1109/WAINA.2016.35.

[60] X. Zhong, Y. Fu, L. Yu, R. Brooks, and G. K. Venayagamoorthy, "Stealthy Malware Traffic – Not as Innocent as It Looks," in *2015 10th Int. Conf. Malicious Unwanted Softw. (MALWARE)*, Fajardo, PR, USA, Oct. 2015, pp. 110–116, doi: 10.1109/MALWARE.2015.7413691.

[61] R. Barona and E. A. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," in *2017 Int. Conf. Circuit Power Comput. Technol. (ICCPCT)*, 2017, pp. 1-8, doi: 10.1109/ICCPCT.2017.8074287.

[62] S. Hsiao and D. Kao, "The static analysis of WannaCry ransomware," in *2018 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2018, pp. 153-158, doi: 10.23919/ICACT.2018.8323680.

[63] E. B. Karbab and M. Debbabi, "ToGather : Automatic Investigation of Android Malware," in *Proc. 13th Int. Conf. Availab. Reliab. Secur.*, Aug. 2018, pp. 1-10, doi: 10.1145/3230833.3230870.

[64] K. S. Yim, I. Malchev, A. Hsieh, and D. Burke, "Treble : Fast Software Updates by Creating an Equilibrium in an Active Software Ecosystem of Globally Distributed Stakeholders," *ACM Trans. Embed. Comput. Syst.*, vol. 18, no. 5, pp. 1-23, 2019, doi: 10.1145/3358237.

[65] F. Alswaina and K. Elleithy, "Android malware family classification and analysis: Current status and future directions," *Electron.*, vol. 9, no. 6, pp. 1–20, 2020, doi: 10.3390/electronics9060942.

[66] C. Uppin and G. George, "Analysis of Android Malware Using Data Replication Features Extracted by Machine Learning Tools," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 5, no. 5, pp. 193–201, 2019, doi: 10.32628/CSEIT195532.

[67] A. Talha and I. Alper, "An in-depth analysis of Android malware using hybrid techniques," *Digit. Investig.*, vol. 24, pp. 25–33, 2018, doi: 10.1016/j.diin.2018.01.001.

[68] F. C. Mead, J. M. Zielinski, L. Watkins, and W. H. Robinson, "A Mobile Two-Way Wireless Covert Timing Channel Suitable for Peer-to-Peer Malware." in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC)*, 2017, pp. 1-6, doi: 10.1109/PIMRC.2017.8292638.

[69] F. Li, A. Lai and D. Ddl, "Evidence of Advanced Persistent Threat: A case study of malware for political espionage," in *2011 6th Int. Conf. Malicious Unwanted Softw.*, 2011, pp. 102-109, doi: 10.1109/MALWARE.2011.6112333.

[70] N. Tavabi, N. Bartley, A. Abeliuk, S. Soni, E. Ferrara, and K. Lerman, "Characterizing Activity on the Deep and Dark Web," in *Companion Proc. 2019 World Wide Web Conf.*, May 2019, pp. 206–213, doi: 10.1145/3308560.3316502.

[71] K. Khanmohammadi, N. Ebrahimi, A. Hamou-lhadj, and R. Khoury, "Empirical study of android repackaged applications," *Empir. Softw. Eng.*, vol. 24, pp. 3587-3629, 2019, doi: 10.1007/s10664-019-09760-3s.

[72] "Kaspersky Security Bulletin : OVERALL STATISTICS FOR 2017," 2017. [Online].Available: https://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2017_Statistics-PR-1045.pdf

[73] K. Liu, S. Xu, G. Xu, D. Sun, and H. Liu, "A Review of Android Malware Detection Approaches Based on Machine Learning," *IEEE Access*, vol. 8, pp. 124579–124607, 2020, doi: 10.1109/ACCESS.2020.3006143.

[74] S. Turker and A. B. Can, "AndMFC: Android malware family classification framework," in *2019 IEEE 30th Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC Workshops*, 2019, pp. 1-6, doi: 10.1109/PIMRCW.2019.8880840.

[75] Android, "Android Security & Privacy 2018 Year In Review," Mar. 2019. [Online].Available: https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf

[76] M. Stone. (2019). A Deep Dive into Reversing Android Pre-Installed Apps Securing the System. [Online].Available: https://i.blackhat.com/USA-19/Thursday/us-19-Stone-Securing-The-System-A-Deep-Dive-Into-Reversing-Android-Preinstalled-Apps.pdf

[77] R. Samani and G. Davis, "McAfee Mobile Threat Report: Mobile Malware Continues to Increase in Complexity and Scope," McAfee, Santia Clara, CA, USA, McAfee Mobile

Threat Report Q1, 2019. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf

[78] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features," *IEEE Access*, vol. 7, pp. 64411-64430, 2019, doi: 10.1109/ACCESS.2019.2916886.

[79] N. Tavabi, N. Bartley, A. Abeliuk, S. Soni, E. Ferrara, and K. Lerman, "Characterizing Activity on the Deep and Dark Web," in *Companion Proc. 2019 World Wide Web Conf.*, May 2019, pp. 206–213, doi: 10.1145/3308560.3316502.

[80] M. Al-Janabi and A. M. Altamimi, "A comparative analysis of machine learning techniques for classification and detection of malware," in *Proc. - 2020 21st Int. Arab Conf. Inf. Technol. ACIT 2020*, 2020, doi: 10.1109/ACIT50332.2020.9300081.

[81] H. Cai, N. Meng, B. Ryder and D. Yao, "DroidCat: Effective Android Malware Detection and Categorization via App-Level Profiling," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1455-1470, June 2019, doi: 10.1109/TIFS.2018.2879302.

[82] R. Samani and G. Davis, "McAfee Mobile Threat Report: Mobile Malware Continues to Increase in Complexity and Scope," McAfee, Santia Clara, CA, USA, McAfee Mobile Threat Report Q1, 2019. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf

[83] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features," *IEEE Access*, vol. 7, pp. 64411-64430, 2019, doi: 10.1109/ACCESS.2019.2916886.

[84] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Networks*, vol. 6, no. 2, pp. 147–156, 2020, doi: 10.1016/j.dcan.2019.01.005.

[85] Deloitte Cyber Threat Intelligence, "COVID-19 Global Cyber risks : Is a major cyberattack looming ?," June 3, 2020. [Online].Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/gx-cyber-covid-19-deloitte-global-cyber-covid-executive-briefing-issue-8release-date-6-3-2020-vf.pdf

[86] M. Faou, "TURLA LIGHTNEURON One email away from remote code execution," *Eset*, no. May, pp. 1–33, 2019, [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

[87] R. Brown and A. Rocha, "Entrepreneurial uncertainty during the Covid-19 crisis: Mapping the temporal dynamics of entrepreneurial finance," *J. Bus. Ventur. Insights*, vol. 14, no. April, p. e00174, 2020, doi: 10.1016/j.jbvi.2020.e00174.

[88] A. Balachandar, S. Abdul Alsowdh, and K. Arumugam, "Design and Development of Future Estimate in Confronting Ransomware," *J. Phys. Conf. Ser.*, vol. 1717, p. 012063, 2021, doi: 10.1088/1742-6596/1717/1/012063.

[89] L. García and R. J. Rodríguez, "A Peek under the Hood of iOS Malware," in *2016 11th Int. Conf. Availab. Reliab. Secur. (ARES)*, Salzburg, Austria, 2016, pp. 590-598, doi: 10.1109/ARES.2016.15.

[90] S. I. Imtiaz, S. ur Rehman, A. R. Javed, Z. Jalil, X. Liu, and W. S. Alnumay, "DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 844–856, 2021, doi: 10.1016/j.future.2020.10.008.

[91] L. Vokorokos, P. Drienik, O. Fortotira and J. Hurtuk, "Abusing mobile devices for Denial of Service attacks," *2015 IEEE 13th Int. Symp. Appl. Machine Intell. Inform. (SAMI)*, Slovakia, 2015, pp. 21-24, doi: 10.1109/SAMI.2015.7061886.

[92] F. Martinelli, F. Mercaldo, V. Nardone, A. Santone, and G. Vaglini, "Simulation Modelling Practice and Theory Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation," *Simul. Model. Pract. Theory*, vol. 105, p. 102169, 2020, doi: 10.1016/j.simpat.2020.102169.

[93] H. Wang, W. Zhang, S. Member, and H. He, "An Evolutionary Study of IoT Malware," *IEEE Internet Things J.*, vol. 8, no. 20, pp. 15422–15440, 2021, doi:10.1109/JIOT.2021.3063840

[94] D. Schultes, "SequalsK — A Bidirectional Swift-Kotlin-Transpiler," in *IEEE/ACM 8th Int. Conf. Mob. Softw. Eng. Syst. (MobileSoft)*, Madrid, Spain, May 2021, pp. 73–83, doi: 10.1109/MobileSoft52590.2021.00017.

[95] C. Li, D. He, S. Li, S. Zhu, S. Chan, and Y. Cheng, "Android-based Cryptocurrency Wallets: Attacks and Countermeasures," in *Proc. IEEE Int. Conf. Blockchain Blockchain*, pp. 9–16, 2020, doi: 10.1109/Blockchain50366.2020.00010.

[96] Y. Sun, Y. Chen, Y. Pan, and L. Wu, "Android Malware Family Classification Based on Deep Learning of Code Images," *Int. J. Comput. Sci.*, vol. 46, no. 4, 2019.

[97] K. K. Tam, "Analysis and Classification of Android Malware," Ph.D. dissertation, Inf. Secur. Dep., Univ. London, UK. 2016.

[98] A. Cimitile, F. Martinelli, and F. Mercaldo, "Machine Learning Meets iOS Malware : Identifying Malicious Ap-

plications on Apple Environment," in *Proc. 3rd Int. Conf. Inf. Syst. Secur. Priv. Volume 1: ICISSP*, 2017, pp. 487–492, doi: 10.5220/0006217304870492.

[99] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an and H. Ye, "Significant Permission Identification for Machine-Learning-Based Android Malware Detection," *IEEE Trans. Industr. Inform.*, vol. 14, no. 7, pp. 3216-3225, July 2018, doi: 10.1109/TII.2017.2789219.

[100] N. Xie, X. Wang, W. Wang, and J. Liu, "Fingerprinting Android malware families," *Fornt. Comput. Sci.*, vol. 13, pp. 637–646, 2019, doi: 10.1007/s11704-017-6493-y.

[101] S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun, and S. Ahmed, "Ransomware: A framework for security challenges in internet of things," in *2nd Int. Conf. Comput. Inf. Sci. ICCIS*, 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257660.

[102] P. Patidar, and D. Kaushal, "Review of Information Protection on Android Application Devices," *Int. J. Sci. Res. Eng. Trends*, vol. 6, no. 4, pp. 2751–2758, 2020.

[103] R. Samani, "McAfee Mobile Threat Report Mobile Malware Is Playing Hide and Steal," McAfee, Santia Clara, CA, USA, McAfee Mobile Threat Report Q1, 2020. [Online]. Available: https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf

[104] P. Kocher et al., "Spectre Attacks: Exploiting Speculative Execution," in *2019 IEEE Symp. Secur. Priv. (SP)*, 2019, pp. 1-19, doi: 10.1109/SP.2019.00002.

[105] F. Mercaldo and A. Santone, "Deep learning for image-based mobile malware detection," *J. Comput. Virol. Hacking Tech.*, vol. 16, no. 2, pp. 157–171, 2020, doi: 10.1007/s11416-019-00346-7.

[106] M. La Polla, F. Martinelli and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 1, pp. 446-471, First Quarter 2013, doi: 10.1109/SURV.2012.013012.00028 .

[107] S. Shahriar, S. Das, and S. Hossain, "Security threats in Bluetooth technology," *Comput. Secur.*, vol. 74, pp. 308–322, 2018, doi: 10.1016/j.cose.2017.03.008.

[108] H. Chiang and W. Tsaur, "Mobile Malware Behavioral Analysis and Preventive Strategy Using Ontology," in *IEEE Second Int. Conf. Soc. Comput.*, 2010, pp. 1080-1085, doi: 10.1109/SocialCom.2010.160.

[109] C. Martin, L. Juil Legand, I.Burge, I. Joseph, N. Gill, Alicia, A. Marcus "Modelling the spread of mobile malware," *Int. J. Comput. Aided Eng. Technology*, vol. 2, no.1, pp. 3-14, doi: 10.1504/IJCAET.2010.029592.

[110] S. Pirani, A. Johansen, and A. J. Mustill, "On the inclinations of the Jupiter Trojans," *Astronomy & Astrophysics*, vol. 631, no. 2019, pp. 1–10, Oct. 2019, doi: 10.1051/0004-6361/201936600.

[111] S. Kalpana and S. Karthikeyan, "A survey on rise of mobile malware and detection methods," in *2017 Int. Conf. Innovations Inf. Embed. Commun. Syst. (ICIIECS)*, 2017, pp. 1-5, doi: 10.1109/ICIIECS.2017.8276158.

[112] W.-S. Chun and D.-W. Park, "Malicious code hiding android APP's distribution and hacking attacks and incident analysis," in *8th Int. Conf. Inf. Sci. Digit. Content Technol. (ICIDT2012)*, 2012, pp. 686-689.

[113] S. Töyssy and M. Helenius, "About malicious software in smartphones," *J. Comput. Virol.*, vol. 3, no. 4, pp. 109–119, 2006, doi: 10.1007/s11416-006-0022-0.

[114] S. Peng, S. Yu and A. Yang, "Smartphone Malware and Its Propagation Modeling: A Survey," in *IEEE Commun. Surv. Tutor.*, vol. 16, no. 2, pp. 925-941, Second Quarter 2014, doi: 10.1109/SURV.2013.070813.00214.

[115] Y. L. Ho and S. H. Heng, "Mobile and Ubiquitous Malware," in *Proc. 7th Int. Conf. Adv. Mob. Comput. Multimed.*, Dec. 2009, pp. 559–563, doi: 10.1145/1821748.1821856.

[116] K. P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis and S. Shiaeles, "Understanding and Mitigating Banking Trojans: From Zeus to Emotet," in *IEEE Int. Conf. Cyber Secur. Resil. (CSR)*, 2021, pp. 121-128, doi: 10.1109/CSR51186.2021.9527960.

[117] H. Chi, "Integrate Mobile Devices into CS Security Education," in *Proc. 2015 Inf. Secur. Curric. Dev. Conf.*, Oct. 2015, pp. 1–4, https://doi.org/10.1145/2885990.2885991.

[118] J. Malik and R. Kaushal, "Credroid : Android Malware Detection By Network Traffic Analysis," in *Proc. 1st ACM Workshop Priv. Aware Mob. Comput.*, Germany, pp. 28–36, 2016, doi: 10.1145/2940343.2940348.

[119] Z. Chen et al., "Machine learning based mobile malware detection using highly imbalanced network traffic," *Inf. Sci. (Ny).*, vol. 433–434, pp. 346–364, 2018, doi: 10.1016/j.ins.2017.04.044.

[120] V. Svajcer, "When Malware Goes Mobile: Causes, Outcomes and Cures," 2012. [Online].Available: https://www.sophos.com/en-us/enus/medialibrary/Gated%20Assets/white%20papers/Sophos_Malware_Goes_Mobile.pdf

[121] Xie, X. Wang, W. Wang, and J. Liu, "Fingerprinting Android malware families," *Fornt. Comput. Sci.*, vol. 13, pp. 637–646, 2019, doi: 10.1007/s11704-017-6493-y.

[122] H. Cai, N. Meng, B. Ryder and D. Yao, "DroidCat: Effective Android Malware Detection and Categorization via App-Level Profiling," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1455-1470, June 2019, doi: 10.1109/TIFS.2018.2879302.

[123] J. Chen, C. Wang, Z. Zhao, K. Chen, R. Du and G. Ahn, "Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection," in *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 5, pp. 1286-1300, May 2018, doi: 10.1109/TIFS.2017.2787905.

[124] I. A. Chesti, M. Humayun, N. U. Sama and N. Jhanjhi, "Evolution, Mitigation, and Prevention of Ransomware," in *2020 2nd Int. Conf. Comput. Inf. Sci. (ICCIS)*, 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257708.

[125] T. M. Chen and Y. Rahulamathavan, "PIndroid : A novel Android malware detection," *Comput. Secur.*, vol. 68, pp. 36–46, 2017, doi: 10.1016/j.cose.2017.03.011.

[126] S. Hojjatinia, S. Hamzenejadi and H. Mohseni, "Android Botnet Detection using Convolutional Neural Networks," in *2020 28th Iranian Conf. Electr. Eng. (ICEE)*, 2020, pp. 1-6, doi: 10.1109/ICEE50131.2020.9260674.

[127] F. Pierazzi, G. Mezzour, Q. Han, M. Colajanni, and V. S. Subrahmanian, "A Data-driven Characterization of Modern Android Spyware," *ACM Trans. Manag. Inf. Syst.*, vol. 11, no. 1, pp. 1-38, 2020, doi: 10.1145/3382158.

[128] Z. Yixiang and Z. Kang, "Review of iOS Malware Analysis," in *2017 IEEE Second Int. Conf. Data Sci. Cyberspace (DSC)*, 2017, pp. 511-515, doi: 10.1109/DSC.2017.104.

[129] C-C. Hu, T-H. Jeng, and Y-M. Chen, "Dynamic Android Malware Analysis with De-Identification of Personal Identifiable Information," in *ICCBD '20: 2020 3rd Int. Conf. Comput. Big Data*, Aug. 2020, pp. 30–36, doi: 10.1145/3418688.3418694.

[130] D. Emm, R. Unuchek, M. Garnaeva, A. Ivanov, D. Makrushin, and F. Sinitsyn, "IT THREAT EVOLUTION IN Q2 2016," 2016. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07185743/Kaspersky_Q2_malware_report_ENG.pdf (Accessed 2nd July, 2021).

[131] F. Mercaldo and A. Santone, "Deep learning for image-based mobile malware detection," *J. Comput. Virol. Hacking Tech.*, vol. 16, no. 2, pp. 157–171, 2020, doi: 10.1007/s11416-019-00346-7.

[132] F. Wei, Y. Li, S. Roy, X. Ou, and W. Zhou, "Deep Ground Truth Analysis of Current Android Malware," in *Detetion of Intrusions and Malware, and Vulnerability Assessment*, M. Ploychronakis, and M. Meier, Eds., Cham: Springer, 2015, pp. 252-276.

[133] S. Garg and N. Baliyan, "Comparative analysis of Android and iOS from security viewpoint," *Comput. Sci. Rev.*, vol. 40, p. 100372, 2021, doi: 10.1016/j.cosrev.2021.100372.

[134] A. M. Alashjaee, S. Duraibi and J. Song, "IoT-Taint: IoT Malware Detection Framework Using Dynamic Taint Analysis," in *2019 Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, 2019, pp. 1220-1223, doi: 10.1109/CSCI49370.2019.00229.

[135] S. Garg and N. Baliyan, "Comparative analysis of Android and iOS from security viewpoint," *Comput. Sci. Rev.*, vol. 40, p. 100372, 2021, doi: 10.1016/j.cosrev.2021.100372.

[136] P. Wu, D. Liu, J. Wang, B. Yuan, and W. Kuang, "Detection of Fake IoT App Based on Multidimensional Similarity," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7021–7031, 2020, doi: 10.1109/JIOT.2020.2981693.

[137] H. Talal and R. Zagrouba, "A Robust Framework for MADS Based on DL Techniques on the IoT," *Electron.*, vol. 10, no. 21, p. 2723, Nov. 2021, doi: 10.3390/electronics10212723.

[138] A. H. Amarullah, A. J. S. Runturambi and B. Widiawan, "Analyzing Cyber Crimes during COVID-19 Time in Indonesia," in *3rd Int. Conf. Comput. Commun. Internet (ICCCI)*, 2021, pp. 78-83, doi: 10.1109/ICCCI51764.2021.9486775.

[139] K. Khariwal, J. Singh, and A. Arora, "IPDroid : Android Malware Detection using Intents and Permissions," in *2020 Fourth World Conf. Smart Trends Syst. Secur. Sustain. (WorldS4)*, 2020, pp. 197-202, doi: 10.1109/WorldS450073.2020.9210414.

[140] A. Talha and I. Alper, "An in-depth analysis of Android malware using hybrid techniques," *Digit. Investig.*, vol. 24, pp. 25–33, 2018, doi: 10.1016/j.diin.2018.01.001.

https://dspace.org/

Analysis of mobile malware, evolution and infection strategies: a systematic review

Ashawa, Moses; Morris, Sarah

2021-12-30
NAUSS
https://doi.org/10.26735/KRVI8434
Ashawa M, Morris S. (2021) Analysis of mobile malware, evolution and infection strategies: a systematic review, Journal of Information Security and Cybercrimes Research, Volume 4, issue 2, December 2021, pp. 01-29

Downloaded from a DSpace repository. https://dspace.org/