ingenieur
wissenschaften
htw saar

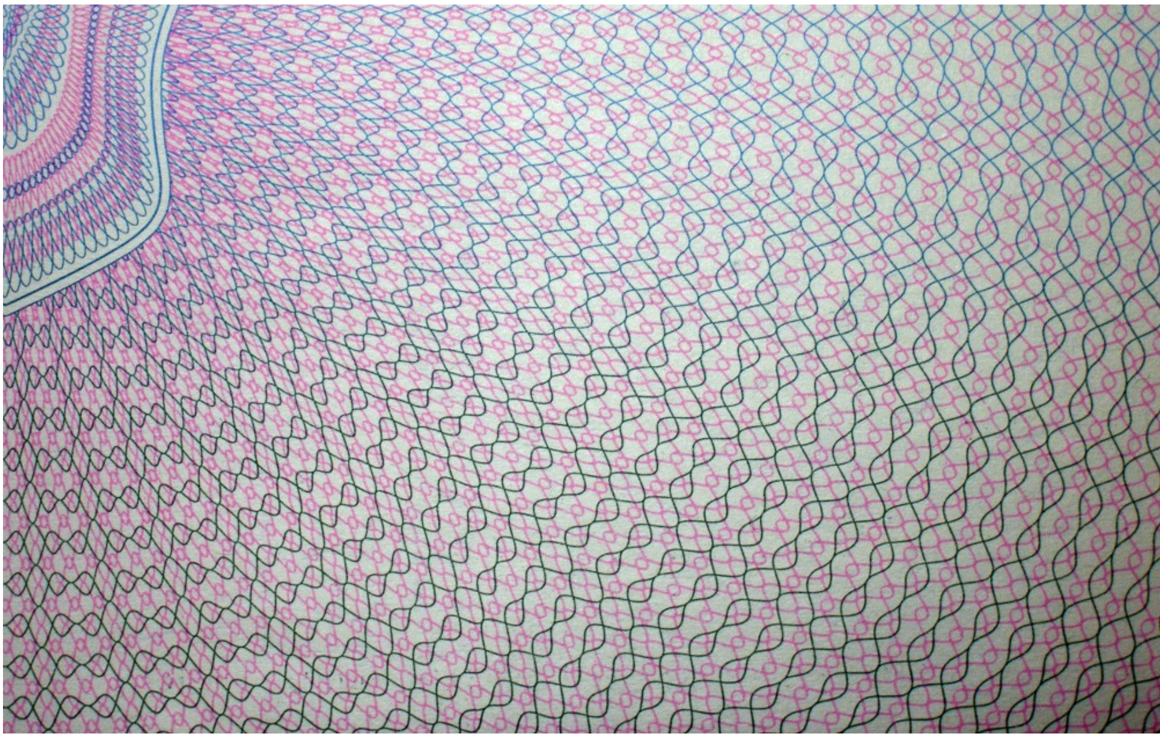
Hochschule für
Technik und Wirtschaft
des Saarlandes
University of
Applied Sciences

STL SYSTEMTECHNIKLABOR

The Evolution of Ransomware on Mobile Devices

Axel Czuck

Technical Report – STL-TR-2018-01 – ISSN 2364-7167



stl.htwsaar.de

Technische Berichte des Systemtechniklabors (STL) der htw saar
Technical Reports of the System Technology Lab (STL) at htw saar
ISSN 2364-7167

Axel Czuck: The Evolution of Ransomware on Mobile Devices
Technical report id: STL-TR-2018-01

First published: January 2018
Last revision: January 2018
Internal review: André Miede

For the most recent version of this report see: https://stl.htwsaar.de/

Title image source: Maira Kouvara (mai05), http://www.freeimages.com/photo/497641

htw saar – Hochschule für Technik und Wirtschaft des Saarlandes (University of Applied Sciences)
Fakultät für Ingenieurwissenschaften (School of Engineering)
STL – Systemtechniklabor (System Technology Lab)
Prof. Dr.-Ing. André Miede (andre.miede@htwsaar.de)
Goebenstraße 40
66117 Saarbrücken, Germany
https://stl.htwsaar.de

The Evolution of Ransomware on Mobile Devices

Axel Czuck
htw saar – Hochschule für Technik und Wirtschaft des Saarlandes
Seminar “Angewandte Informatik/Computer Science and Society”
Wintersemester 2017

Abstract—**Mobile devices have never formed such an attractive target group for hackers to profit from, resulting in an exponential growth of attacks. In contrast to the descending turnover of personal computers, the growth of popularity of mobile devices seems not to stagnate in the near future. Simulteanously the purpose of mobile devices is not limited to conventional phone calls or writing a SMS anymore. Nowadays they hold your personal data, help interacting with your social environment and faciliate daily routines. This chain-like dependency builds an easy target for criminals. A sensitization by outlining the question of ’why’ will harden our mobile devices not in a technical way, but in a psychological way, which results in the most complex obstacle to overcome by any attacker. This paper surveys mobile ransomware and why it is important to distinguish its usage in comparison to personal computers. It outlines its rising attractiveness for malicious hackers and gives a forecast, from which every user is able to draw a conclusion regarding to his/her personal behaviour with mobile devices.**

I. Introduction

≫MOBILE ransomware is an underestimated threat, which enjoys a great degree of popularity within the criminal milieu of hackers. The fact that the amount of mobile devices grows unstoppably enlarges the spectrum of possibilities to affect any mobile device user easily, anonymously and in a troublesome manner.

Mobile ransomware infects a device and spreads rapidly encrypting data or locking the machine. While having no access to any data anymore, the user is summoned to pay a certain amount of ransom to get his files unencrypted and accessible. Using Bitcoins or any other untraceable currency makes it unreasonable trying to take advantage of a police authority, because identifying the perpetrator is almost impossible.

Expecting the number of mobile device users passing the five billion mark in 2019 [1], targeting mobile devices, in contrast to personal computers, becomes more and more attractive to hackers. Ransomware is not merely an underdog within the entourage of malicious malware anymore [2], but rather one of the most popular mobile malware nowadays (cf. Figure 1). Nevertheless, I step in further detail in Section III regarding to this diagram, it can easily be seen, that Trojan-Ransomware went through a tremendous process and now is, despite the Risk Tool, the main threat, cybersecurity has to deal with. Not many years ago mobile ransomware was seen in an experimental stage of development [3] and, in comparison to ransomware affecting personal computers, of a small effect. This and the fact, that these devices are increasingly used to store sensitive personal information such as financial data used for mobile banking, photos and videos, chat-logs and many more, should exhort everyone, that the usage of mobile devices should be treated with caution.

In recent years, researchers have recognized the importance of mobile security and examined not only the possible threats, we have to deal with. Furthermore they stepped in-depth technically, examined malicious code and why it was possible for the ransomware taking place on the users device. But, what we can observe for years, is a neck-and-neck race between researchers, whitehats, governmental authorities and criminals. When the ’good ones’ find a way to plug a certain hole, criminals ’dig’ another one. So preventing intruders from your mobile device is not guaranteed by installing new updates/patches or antivirus-programs. The truth, I believe, lies in the sensitization of any user worldwide. By keeping in mind the seriousness of attackers’ intentions to affect a mobile phone with ransomware, the user benefits knowing about this risk and begins to use his mobile device more carefully. Therefore I place particular focus on the ’Why’ instead of the ’How’. Mobile device users without technical background, of which an tremendous percentage exists in the overall amount of mobile device users, are not capable of the technical know-how to understand the technical reasons and therefore must be reached by showing up, why an attacker is attracted by their mobile device. This paper is organized as follows. In Section II, I briefly describe ransomware in general and examine its functional behaviour on mobile devices and why it is difficult to harden them technically; in Section III, I focus on the temporal development of mobile ransomware and its rise within the past years; in Section IV, I examine the Use-Scenarios of mobile devices and the resulting attractiveness for ransomware and lastly try to give mature advices in Section V, which hopefully prevents everyone falling victim to mobile ransomware.

II. Key Information

Mobile ransomware can be categorized into two main sections. First: Locker-Ransomware and second: Crypto-Ransomware. Ransomware itself can be seen as the ultimate revenue-generating malware in comparison to other direct revenue-generating malware such as misleading apps and fake antivirus scams. Generating an average of US$300 [3] through payment vouchers and bitcoins, ransomware developes quickly and is being innovated constantly by cybercriminals. Although both aim to deny the access to the users’ mobile phone, Locker-Ransomware and Crypto-Ransomware are technically different. While Locker-Ransomware locks the device, Crypto-

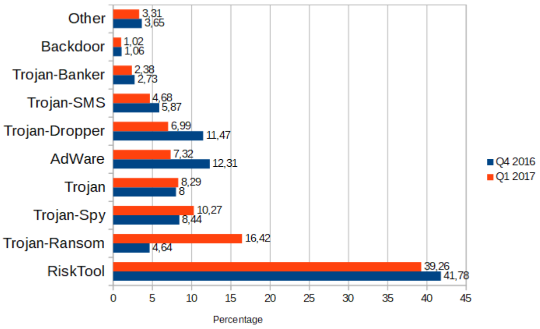


Figure 1. Distribution of new mobile malware by type (Q4 2016 and Q1 2017) [4]

Ransomware locks its data. Anyhow, the results for the mobile device user is the same; he can not use his device properly anymore. Contrary to the opinion ransomware only gets to the device by a chain of unforbearance while browsing dubious websites and installing malicious software with administrative rights, ransomware found their way into the generally trusted App-Stores. Just searching online for the term 'Malicious Apps in App-Store' reveals filled pages with different forms of apps in official App-Stores such as Google Play Store or Apple's App Store, which could be found almost daily. Hidden behind flashlight-apps, game-tutorials/games such as the well-known FIFA-Series malicious malware aims for a widespread target group.

A. Functional Behaviour

Locker-Ransomware mostly prevents access to the user interface largely leaving the underlying system untouched. So how is this locking done? Modern Locker-Ransomware creates an overlay above the user interface - inclusively system monitors - and makes it impossible to use the device properly. Another nasty method some Locker-Ransomware uses, is a change of the device-pin, which thankfully requires administrative rights set beforehand. Unlocking the device is only possible by contacting the blackmailer here. Nonetheless - if the user is lucky and there is 'just' an user interface overlay - Locker-Ransomware owns an Achilles' heel. The possibility to potentially remove the malware and restore the device to something close to its original state makes it more harmless. Especially if the user is tech-affine, the usage of various tools and techniques offered by security vendors lets him effectively restore his device. This does not apply to the Device-Pin-Changing ransomware, which causes a technical oneway making the usage of the device impossible. Despite the pin-changing method, Locker-Ransomware masquerades itself as law enforcement authorities on the UI-Overlay mostly.

On the other hand Crypto-Ransomware is much more aggressive. It is designed to find and encrypt valuable data, stored on the device, quietly while staying below the radar. This led to the fact, that the data is useless unless the user obtains the decryption key. Using asymmetric cryptography makes it mathematically impossible to decrypt the data without obtaining the key. Being affected by a poorly implementation of asymmetric cryptography in the Crypto-Ransomware is like winning the lottery. In most cases the user has no other chance to get his data back than by paying the fee. Cybercriminals target one main weakness of the user; not speaking about negligence or ingenuousness, but rather the fact, user do not realize the value of their data until its loss. Avoiding laborious backup processes is the main weakness, which a cybercriminal targets. Although backup processes became intuitive and can concurrently exist without main maintenance, users keep distance. Encrypting memories of loved ones, a college project due for submission or perhaps a financial report for work let the victims prefer paying the ransom to restore access than simply lose it forever and suffer the consequences. Being victimized by Crypto-Ransomware becomes present when the malware's message appears. At this point the damage is already done.

B. Security Challenges

Aside from the architectural differences, concretely speaking the hardware architecture, mobile devices suffer from two technical disadvantages. First: Hosting multiple techniques; and second: Resource constraints. Both are ironically the main reasons, which led mobile devices to its attractiveness in present. Hosting multiple techniques let the user access the Internet from any place at any time. Connecting to others via Phone calls, SMS and Internet by using *Long Term Evolution* (LTE), *Universal Mobile Telecommunications System*(UMTS) and *Enhanced Data rates for GSM Evolution* (EDGE); via Networking Technologies such as *Bluetooth* for connecting over a small area through short wavelength radio transmission or more widespread in medium term *Near Field Communication*(NFC) and lastly *Wireless LAN IEEE 802.11* gives a huge variety for connection canals compared to personal computer [5]. The possibility to not only rely on one wired internet connection to communicate with the world, makes the mobile device much more attractive and finally results in its rising omnipresence - five smartphones for each computer sold in 2013 [1] - in everyone's life.

Furthermore we have to face the resource constraints, which makes it difficult to harden a mobile device. Unlike desktop PCs, mobile devices have strict resource constraints in computational and power capabilities due to their mobility and small size. Fortunately security vendors have marketed mobile-specific versions of antivirus software to detect malware. But even the simplest signature-based algorithm e.g. initializing its signature database is quite exhaustive for a mobile device. For example, the ClamAV requires 57 seconds of processing and consumes 40 Megabyte only for initializing this particular database [6]. Additionally, more computationally expensive algorithms such as behavioral detection engines become more and more important for detecting sophisticated threats and requires heavyweight resources [7].

Concurrent to the ubiquitous usage of mobile devices today the number of threats targeting mobile devices grows signif-

Table I
DISTRIBUTION OF MOBILE TROJAN RANSOM Q4 2016 VS. Q1 2017 COMPARED TO THE TOTAL AMOUNT OF MOBILE MALWARE [4]

	Q4 2016	*Q1 2017*
Mobile Malware	1,333,509	1,333,605
Mobile Trojan Ransom	61,832	218,625
Percentage of total	4,26%	16,42%

icantly(cf. Figure 1). The deluge of mobile attacks depends inevitably from the mobile device sales and the attractiveness of this revenue-generating malware. Recapitulatory speaking this effect is hard to halt and therefore must be supressed urgently; not only technical, but rather by sensitizing the user.

III. TEMPORAL DEVELOPMENT AND RISE

Regarding to the facts described above, mobile ransomware enjoys increasing popularity. Specifically Crypto-Ransomware becomes more and more attractive, which led to a an evolution, making Crypto-Ransomware the headliner of ransomware by about 70% of the overall coverage(cf. Figure 2). Starting with around 2% in 2010 Crypto-Ransomware reached its leadership within the past years in the new malware-families.

Throughout the year 2016 Kaspersky detected 261,214 installation packages only of mobile ransomware in total, which is almost 8.5 times more than 2015. Mobile ransomware was a small player in the malware-game back in 2015 only covering approximately 0.66% of the overall number of detected installation packages [2]. The alarming number is 218,625. This is the number of installation packages in **Q1 2017 only**. It is 3.5 times more than in the previous quarter and 83% of the complete previous year. Mobile ransomware coverage jumped from 4.64% in Q4 2016 to 16.42% in Q1 2017. Table I summarizes these numbers briefly.

These numbers should be an alarming statement for all mobile device users worldwide. Despite the mere numbers and percentages, which show the rise and development of mobile ransomware in the past years, there is another fact, which users should be concerned of: Well-known for 'Techies' are catchwords like *Infrastructure-as-a-Service*(IaaS), *Platform-as-a-Service*(PaaS) and *Software-as-a-Service*(SaaS); ever heard of *Ransomware-as-a-Service*? It is quite common to rent out ransomware nowadays. Agreeing to a share from up to 85% of the weekly generated revenue, everyone can just rent a ransomware and keeps e.g. 106,25 Bitcoins from 125 Bitcoins in total. To be honest: This example-calculation was found on the 'Petya-Pricelist' in the Dark Web and is a bit outdated. Earning approximately 1.305.273,5000 Euro in one week is strictly dependant from the high-specutaled bitcoin. Nevertheless: The single fact, that the possibility renting ransomware exists and even getting some kind of a helpdesk and technical support, shows the professionalism of this business. To crown it all: One out of five victims will, although he had payed the fee, never receive any decryption-key.

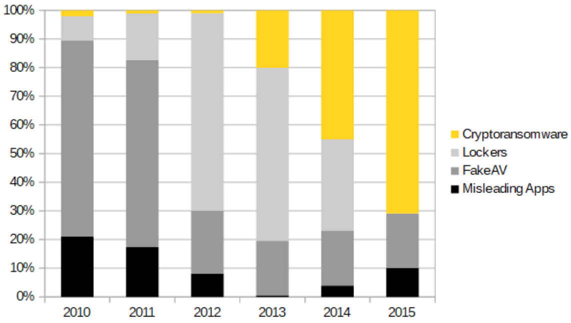


Figure 2. Percentage of new families of misleading apps, fake AV, Locker-Ransomware and Crypto-Ransomware [3]

Hoping that this rise in the past years is comparable to any other economic bubble, we could observe in the past years, borders is naive. It can not be expected, that it will implode in the near future. It is absolutely necessary to keep one point in mind: 'Normal' ecomonic bubbles suffer from the ingenuosness of their participants; they bet on a demand, which does not exist yet and hope to fill this gap, which lets this certain business grow unstoppably. Contrary to the 'normal' bubbles; the so called ransomware-business rely on a demand, which always exists and ever will. Every mobile device user is addicted to his device (and his data). This is not least attributed to the tech-companies, which led us slowly into this addiction over the past years. The following chapter will examine this dependency more precisely.

IV. USE-SCENARIOS AND RESULTING ATTRACTIVENESS

This section aims to outline the Use-Scenarios of mobile devices and the resulting attractiveness for attackers. It is inalienable to understand the ubiquity of mobile devices in our daily lifestyle to conclude the importance of building not only technical obstacles against attackers but also - from even higher priority - psychological obstacles by being sensitized using a mobile device. Four main key aspects let mobile devices become omnipresent in our daily life: *mobility*, *strong personalization*, *strong connectivity* and *technology convergence*. *Mobility* makes it possible, that each device can come with us anywhere we go; *strong personalization* means, that an owner of one device is its unique user; *strong connectivity* lets the user send emails, check the online banking account, send SMS, socialize via social media and many more; *technology convergence*, which bequeath *strong connectivity*, is the combination of different technologies [8]. These four key aspects are responsible for our daily intercourse with mobile devices. They became irreplaceable and make it harder to interact with the social environment from day to day without such a mobile device. The mobile device metamorphosed from a little helper reaching wide distances and crossing borders to a powerful swiss-knife, which is capable of doing almost everything.

Table II
% OF SMARTPHONE OWNERS WHO USED THEIR PHONE FROM THE FOLLOWING LOCATIONS AT LEAST ONCE OVER THE COURSE OF 14 SURVEYS SPANNING A ONE-WEEK PERIOD [10]

Location	*Percentage*
At home	99%
In a car or public transit	82%
At work	69%
Waiting in line	53%
At a community place	51%
Walking from a place to place	50%
Exercising	17%

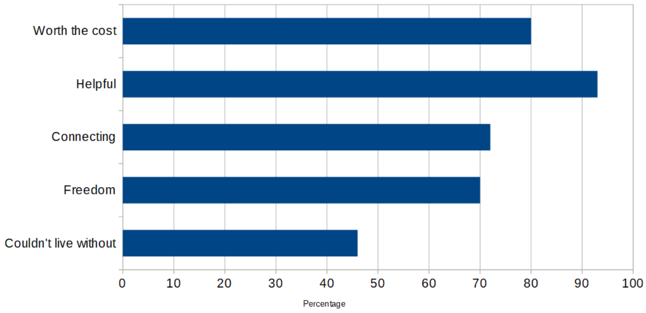


Figure 3. % of owners who say that the following items from each pair best describe how they feel about their phone [9]

Without stepping into depth, how the mobile-device-economy accomplished this dependency over the past years, I want to give a point of view of today's state of affairs. Despite the negative facts of the frequent usage of mobile devices, they let the user associate with an interesting variety of feelings (cf. Figure 3). These feeling are strongly connected to the possibilities a mobile device reveals, such as text messaging, voice/video calls, internet, Email, social networking, taking pictures/videos, news, watching videos, games, maps and music or podcast [9].

Apart from those many different Use-Scenarios, which led to our behaviour or even habits, the usage of a mobile device for some situation instead of doing it 'vintage-style' is oft preferred. Ordering a Pizza by phone? Why not using one of those plenty apps, which orders the pizza by one-click? Why using a US$700 camera shooting photos of a weeding, when my smartphone has around 23 megapixels? And: Instead of describing the address to a nearby visitor, taking advantage of the Maps-API in the messenger to send the location directly, so the receiver just has to click on the message, which opens his Routing-App, letting him know 'how long' he has to drive and where he has to expect traffic jams etc. Questions, which make a few of us head-shaking, but can everyone claim, that he has never benefit from one of the advantages mentioned above? It is not about creating a pessimistic point of view on mobile device usage, but realizing, that it is used at any time anywhere. As it is shown in Table II the 'anywhere' is spread over every location, we get in touch during the day.

These circumstances result in the ultimative attractivity for possible cybercriminals. Knowing about the fact, that this possible vulnerable device lays in the users' hands approximately around 4 hours a day, which means around 10 minutes per hour (Assumes no sleep), is like an unspoken invitation [11]. The probability, that the user falls victim to malicious apps, Web-Urls with a drive-by download is higher than it would be on any other device, such as personal computer. Society, influenced by the powerful tech-market, aims to operate connected at any time and anywhere. Society's tool is inter alia the mobile device. Agreements like *Bring You Own Device*(BYOD) strengthened this effect in an unpredictable manner and gives the user the possibility to be connected anywhere at any time. This results in the fact, that the user is also targetable anywhere at any time. This led to the inevitable fact, that the usage of mobile devices should not only be a gimmick, with which we all learn to interact autodidactically. I rather want to go over to the statement, that the usage of mobile devices should not be regulated, but well educated. Facing the fact, that a mobile device belongs to any of us, like owning a car, requires at least usage-lessons, like we know from the driving-license. Anyhow, this unregulated ethical responsibility, which we have towards others, but also towards ourselves is valid to rethink and intervene; not at least to harden ourselves against possible threats. I want to give step-by-step advices (technical and non-technical) in the next section, which every user should keep in mind, while using his device.

V. Step-by-Step Advices

A. *Technical - Thou should back thine files*

Any state of your data is just as actual as your backup is. Once the access to the device is blocked by a locked ransomware or a Crypto-Ransomware, restoring the latest version of the backup, gives the opportunity accessing your data as if you got never affected. Use services, which provide an automatic synchronization. Differentiate the discretion of the data. Photos of the loved ones should stay in the local backup such as an external hard-drive; while the college-project is allowed to stay in the cloud. Placing your external hard-drive in a complete different system, which is not connected to the internet, is highly advised.

B. *Technical - Thou should be suspicious*

Being suspicious of emails, websites and apps should enclose all the interaction with your device. Timeless classics like suspicious links and mails are still present. Unfortunately trusting apps from the official app stores is naive. Reading the valuation and comment-section of an app is absolutely needed. A so-called 'system-cleaner' with three ratings around five stars out of five should at least be concerning. Apart from that: Which device-services does an app really need? Does a star-wars-lightsaber app really need access to your contacts?

C. Technical - Thou should use an antivirus program

Although an antivirus program can not be as powerful as it is on a personal computer regarding to the device's technical constraints, an antivirus program can at least minimize the risk. Common security vendors, who knows about the development mobile malicious malware had in the past years, have been working to harden antivirus programs for the mobile usage ever since . It is all about building one obstacle after another to defeat an attacker's plan.

D. Technical - Thou should install updates

Admittedly updates can be bugging. Nevertheless they do not just exist to add new features to an app or system. In many cases they 'plug' holes in Zero-Day-Exploits and minimize other threat scenarios. Especially system updates have highest priority. Fixed vulnerabilities obstruct ways to intrude the users' device.

E. Non-Technical - Thou should never pay the ransom

Despite the fact, which was mentioned above, that one victim out of five never receives the decryption key, although he payed the ransom; you should never pay the ransom. Anyhow: Why should you not pay the ransom then? Easy to answer, because knowing about the fact, that your willingness to pay the fee makes you even more attractive for the cybercriminals. Every cybercrimal will try it at least once again, since he is certain of one thing: He will very likely be paid again. On the other hand, not paying the fee can be some kind of mass phenomenon. If nobody pays the fee anymore, generating revenue with ransomware will become less attractive.

F. Non-Technical - Thou should stay wise

Stay wise while online. Never enter personal information into a website if you are unsure or the website seems suspicious. The market with stolen online-identities is profitable.

G. Non-Technical - Thou should rethink routines

Which routines are meant here? I am talking about the usage of mobile devices, which is a daily routine nowadays. From waking up and checking the news and incoming messages overnight to the pizza-order in the early afternoon. It is not about stopping this routine, but rethink the word 'routine' here. As soon as something becomes a matter of habit, you might become negligent. Negligent in your interactions with your device. Today the device surrogates many things, such as photo-albums, credit-cards, your ID and many more. Envision the importance of this device should redefine the word 'routines'.

VI. Summary and Outlook

In this paper I examined the reasons of the rise of ransomware in the past years due to increasing mobile device sales and the inherent usage of mobile devices at any time. By summarizing its evolution, along with some notable examples; the ransomware's rise could be visualized and should be implanted in everyone's mind. I classified ransomware and took a look behind its face relating to its functionality; I have also outlined the security challenges a mobile device must face, because of its widespread canals, which makes it an allrounder in communication with the environment. Furthermore I threw an eye on the user's hands and analyzed his behaviour and habits interacting with mobile devices and lastly tried to give advices for a circumspect handling with mobile devices.
Regarding the fact, that mobile devices surround us in any manner, let them become an attractive target for cybercriminals. It can be expected, that mobile devices continue their rapid expansion in terms of sophistication and functionality. The effect will be a devil of a fellow, which participates in almost every interaction a human being can have with his environment. The temptation targeting a mobile device will increase, so that the device **and** the user will have to face a range of new security threats. While mobile ransomware experienced a metamorphosis from an experimental stage to a protagonist in the entourage of malicious malware, a further increase of incidents influenced by ransomware can be highly expected.

VII. Acknowledgement

The author wants like to thank the anonymous reviewer for their valuable comments and suggestions, which have greatly improved the quality of the paper. Furthermore the author's thanks goes to Mr. Donald E. Knuth and Mr. André Miede for the lessons learned in the course of this worthwhile lecture.

References

[1] M. Kitagawa, "Forecast analysis: Pcs, ultramobiles and mobile phones, wordwide, 4q17 update," Gartner, Tech. Rep., 2018.

[2] K. Lab, "Mobile malware evolution 2016," Kaspersky, Tech. Rep. 13, 2016.

[3] K. Savage, P. Coogan, and H. Lau, "The evolution of ransomware," Symantec, Tech. Rep. 16, Aug. 2015.

[4] R. Unuchek, F. Sinitsyn, D. Parinov, and V. Stolyarov, "It threat evolution q1 2017. statistics," Kaspersky Lab, Tech. Rep., 2017.

[5] M. L. Polla, F. Martinelli, and D. Sgandurra, Eds., *A Survey On Security For Mobile Devices*, vol. 15, no. 1, IEEEE Communications Surverys & Tutorials, 2013.

[6] J. Oberheide, K. Veeraraghavan, E.Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," *Workshop on Virtualization in Mobile Computing*, 2008.

[7] J. Oberheide and F. Jahanian, "Demystifiying security challenges in mobile environments," in *When Mobile is Harder Than Fixed (and Vice Versa)*, J. Oberhe, Ed., 2010.

[8] C. R. Mulliner, "Security of smart phones," Master's thesis, University of California, Santa Barbara, 2006.

[9] A. Smith, "A "week in the life" analysis of smartphone users," *Pew Research Center Internet & Technology*, 2015.

[10] ——, "Usage and attitudes toward smartphones," *Pew Research Center Internet & Technology*, 2015.

[11] "Mobile time is mostly 'app time'," Apr. 2016, average Time Spent per Day with Mobile Internet Among US Mobile Users, In-App vs. Mobile-Web 2012-2018. [Online]. Available: https://www.emarketer.com/corporate/coverage/be-prepared-mobile