 doi:10.20944/preprints201705.0123.v1

Article

Abuse of Mobile Devices by Making Reverse Proxy Server

Dogukan Aydinli [1], Emre Koroglu [1] and Volkan Erol [2,*]

[1] Okan University Insitute of Science, Tuzla Campus, Istanbul Turkey 34959; nbilisim@gmail.com, emkoroglu@gmail.com
[2] Okan University Computer Engineering Department; volkan.erol@okan.edu.tr
* Correspondence: volkan.erol@okan.edu.tr; Tel.: +90-533-362-19-47

Abstract: Mobile devices have become tools we spend our free time where we carry them with us every moment, they allow us to interact with the environment, we immortalize the moment when necessary. These devices which we spend most of our daily life become very common in recent years and even there are unique business areas emerged. It was announced that the number of people using smartphones is over than 2.5 billion in the first quarter of 2016. As people become more addicted to mobile technology, they become the target of malevolent people. A huge increase in the number of mobile malware is observed as the number of the users increase. Billions of users at risk day by day due to the development of the methods. We have addressed the recent methods used and the types of malware that target mobile devices in our study. We have mentioned the proxy server and reverse proxy server operation logic. We discuss the method of turning mobile devices into reverse proxy servers, risks involved and protection methods.

Keywords: Mobile device threats; mobile device malware; reverse proxy server; cyber security; android security; ios security; abuse of local area network; DNS spoofing; DNS hijacking

1. Introduction

In recent years, there is a significant increase in the rate of mobile application development and use together with the rise in the use of mobile devices. Applications that are indispensable for mobile devices provides great benefits. Applications which allow us to interact with our friends and other people, we immortalize the moment by taking photos or video, we can follow daily life may have undertaken the task of spying and attacking without our information.

According to figures shared as of March 2017; it is known that there are 2.800.000 applications on Google Play Store, 2.200.000 applications on Apple App Store and 1.503.500 applications on other application distributors[1]. Android devices have surpassed 1.4 billion [2] active users in September 2015 while Apple has surpassed 1 billion [3] active users in January 2016. When we consider that each user may be an active victim, this means that 2.5 billion users are at risk. Mobile devices and users are in great danger due to reasons such as applications that are not adequately audited, users do not sufficiently care the authorization parts and development of social engineering techniques.

In the statistics of the threat report targeting mobile devices and published by McAfee Labs, it is stated that attack on mobile devices has increased by 75% in the last quarter of 2015.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

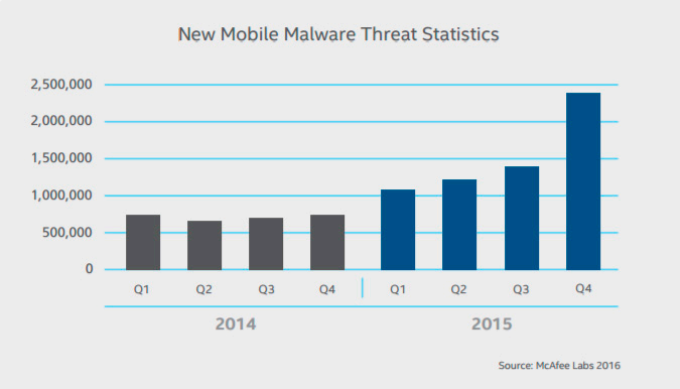

Figure 1. McAfee Labs. Mobile Threat Report, Mobile Malware Threat Statistics

2. Target: Mobile Devices

Today, computers left their popularity to mobile devices. When we consider the computers and mobile devices in the eye's of an attacker;

- While the daily time spent with the computer is decreasing day by day, the addiction on mobile devices is increasing. Access to the victim will be much easier due to mobile device usage is greater during the day.
- In general, the device is shut down after a person spends few hours on the computer and it is hard to have an access from a remote place. However, there is always the possibility of being attacked since the mobile devices operate every hour of the day.
- People are next to their computers when they have a work to do. Mobile devices are always with the people. In this way, access to confidential information such as the location of the victim can be achieved.
- While computers are often connected to a local network, mobile devices can ensure connection with wireless networks at anywhere due to they are always with us. In this way, many devices can be affected through the local network.
- The biggest drawback of mobile devices is their processing power. The personal computers have much more powerful system features than mobile devices. However, the gap is gradually closing as days pass.

Mobile devices appetize many attackers due to these features and it puts the users at great risk.

2.1. Mobile Malware

Malicious software targeting mobile devices may be programmed for many purposes.

2.1.1. Spyware and Adware

Spyware collects your personal and confidential information secretly without your information and they send these to 3rd party network. Depending on how they are programmed, they can have an access to your location information, messages, personal lists, photographs, browser history and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

the information of the accounts you use. This information can be sent to advertising agencies and you may be subjected to ad impressions without your consent.[4]

2.1.2. DDoS Malware

DDoS is a method of attack aimed at disabling the entire system or target service by invading the resources of the target system and/or bandwidth. The size of the attack depends on the bandwidth of the victims and the total processing power of the devices. The new target of DDoS malicious developers is mobile and IoT devices. When we consider these devices which are active and accessible during the most of the day are using a broadband connection, it will be sufficient to check the DDoS attacked performed by MIRAI malware in the last quarter of 2016 in order to understand the size of the attack to be performed.

MIRAI malware which turned the IoT devices into zombies on September 20, 2016, performed an attack between 620 Gbps and 1Tbps to famous DNS organization Dyn. As a result, many popular web services such as Github, Twitter, Reddit, Netflix were not accessible. [5]

2.1.3. Ransomware

It is the malware which encrypts the files on your device and asks you to make a payment in order to recover the files on your device as a general operating method. The ransomware has increased as Bitcoin usage and value increased which is especially hard to be tracked and refunded.[6]

It was noted that ransomware found on 261.214 mobile devices in 2016 Mobile Malware Evolution published by Kaspersky[7].

2.1.4. Trojan

They are the malware which seize the manage of the device and allow the attacker to manage the device remotely. The general features of trojan horses in mobile devices are; the attacker can perform the following by using the device whenever he wants; have an access to your files, read and send messages, take photos, make a call, open a web page on your device. Trojans can perform any task depending on the authorization.

Trojan developers used to code themselves as the client and code the victims as the server in the early days. In this case, the attacker had to connect to the device of the victim. However, due to the difficulties in running a port on the victim's device and connection problems with the device lead the next generation attackers to develop a server and connect the victim as a client.

2.1.5. Banking Malware

They target the bank accounts of the victims. They send the information to attacker once they capture the banking and personal information. It has been observed that these types of malware also tries to seize the OTP (one-time password) code which is sent via text message or call.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

The malware which appeared in 2014 and known as Android.Bankosy code name managed to get the OTP codes by directing the incoming calls to the device to the attackers' mobile phones [8].

2.1.6. DNS Spoofing and DNS Hijacking

DNS Hijacking means the DNS servers are changed without the permission of the user. The device which host malware that is coded for DNS spoofing performs its task by connecting to the network devices after they connect to any network. Any device user who is connected to the network will connect to the server of the attacker rather than connect to target server when he is going to connect by using the domain name of the website. The websites use the HTTPS protocol which HSTS activated in order to protect the users from attacks such as MiTM (Man-in-the-Middle) and DNS spoofing. The visit to the website by the user is prevented since the certification validation will not be valid.

A malware named Switcher identified in the last quarter of 2016. It is hosted on Android devices and performed DNS hijacking by having access to the interfaces of network devices where the user connected to the network. 1,300 network devices were affected by this malware in China. [9]

2.1.7. PowerOffHijack

This malware type which is firstly seen in February 2015 prevent the device from being switched off during the switch off of the devices that use the Android operating system and it used to mimic the animations of the device while switching off (screen fade-out, switch off sound). Thus, the victim would believe that he switched off the device however the malware used to continue to work at background and fulfill its task [10].

3. Discussion

3.1. Detection, Protection and Recommendations

3.1.1. Network Device Configuration

Changing the default login information of the used network devices and restricting access to administration interfaces will prevent the access of the devices which host malware to network devices. Regularly performing firmware updates of network devices will mean the prevention of possible security vulnerabilities. The servers used for the access to victim devices by the attacker may be blocked through the firewall and devices which host this malware can be determined.

3.1.2. Personal Devices Should Not Be Connected to Corporate Networks

Personal devices and corporate devices must be completely separate from each other. The connection of personal mobile devices to intercorporate networks will endanger will endanger the devices in the company. In addition to the possibility of harming intercorporate devices, a malware in the personal device can lead the corporate identity to be damaged as a result of the harm on 3rd party individuals and institutions through the corporate network.

 doi:10.20944/preprints201705.0123.v1

3.1.3. Checking the Application Authorizations

Applications in mobile devices request the required authorizations from the device user during the installation or use. Some applications may require several authorizations although they don't need them. You need to be careful in case there is no link between the purpose of the application and the requested authorizations. Innocent looking applications may host malware that operates in the background.

3.1.4. Downloading Applications from Official and Known Sources

Attention should be paid to download applications from known and official sources such as Google Play, Amazon Store for Android devices and iTunes Store for iOS devices. You need to be careful when you are going to install applications from 3rd party markets which are not unreliable.

3.1.5. Mobile Device Applications and Operating System Should Be Always Kept Up-to-Date

Many security vulnerabilities are coming to light in each passing day. Mobile device applications and operating system must be kept up-to-date all the time, critical patches must be downloaded and installed.

3.1.6. Excessive Data Transmission, System Source Usage and Dead Battery in a Short Time

If the device consumes excessive data transmission, system source and/or if the battery dies in a short time, it may host a malware. In this case, applications in the device must be reviewed.

3.1.7. Always Recording the Network Traffic

Recording and storing the used network traffic can be an evidence in terms of the relief. It will be useful to keep the entire network traffic under control including individual and enterprise encrypted traffic without neglecting the privacy rules.

4. Materials and Methods

As each technology can be used for useful purposes, they can be used for harmful purposes. In general, proxy servers used for privacy, security and network communication are divided into two.

4.1. Proxy Server

4.1.1. Forward Proxy Server

The proxy servers establish a connection between the user and the target server during the access to the internet. They are also named as "proxy servers" only.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

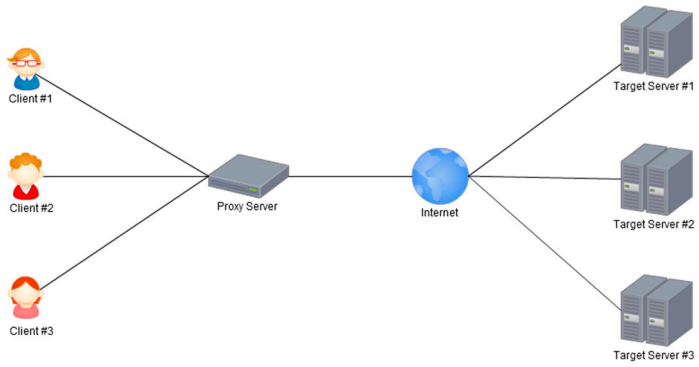

Figure 2. Forward Proxy Server – Client Communication

4.1.2. Reverse Proxy Server

They are usually used for load balancing, security, and confidentiality during the construction of web servers. They serve as a bridge between the user and the web server rather than the user will connect to web server directly which performs the operations [11].

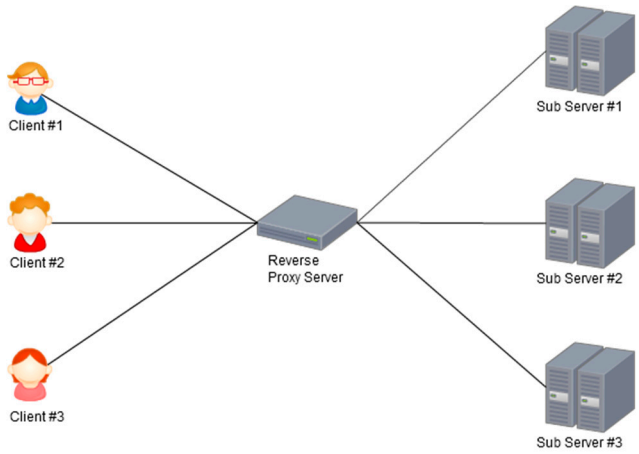

Figure 3. Reverse Proxy Server Communication

4.2. Turning Mobile Device Into Reverse Proxy Server

Two types of identity are used in order to identify the devices on the internet. IP and MAC addresses. These identities have a vital importance for the detection of people in illegal activities in the virtual environment and the relief of the victim. When the identity information and the time of the event took place are filtered, it is possible to have an access to many details such as the ISP company used by the attacker, his information on ISP, the city he connected. The attackers are using many methods to be anonymous. Some of these methods are using protocols such as TOR, proxy server, and VPN.

The term "reverse proxy server" mentioned in our method is also known as “web bot proxy” in some other sources. The method used as a tool in previously discovered and illegal R.A.T. (remote administration tool) software. [12] The attackers who preferred the method in the years when it was discovered were quite a few due to lack of legislation targeting cybercrime and not enough attention

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

were paid. However, the attackers began to use former methods which are hard to detect but have a high possibility of success with the creation of new laws and as a result of the importance paid to the cyber security.

4.2.1. Implementation of the Method

The difference of the method from forward proxy servers is the attacker is the server side and the victim devices act as a bridge between the target servers. The victim devices must be connected to the internet and the malware must be granted to full internet connection authority for the implementation of the method.

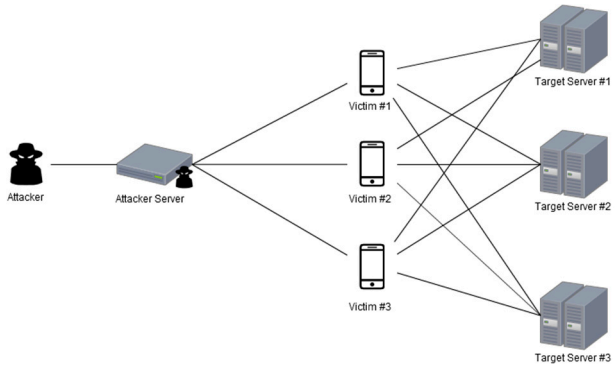

Figure 4. Attacker, Victim Devices, and Connection Flows Between the Target Servers

We can divide the method into three sections as the attacker, attacker server and malware uploaded to victim devices. We have created a packet structure in order to ensure the communication between attacker server and victim devices as indicated in Figure 5, 6, 7. This packet structure is created to ensure an understanding of the method.

Attacker Side

The attacker makes the forward proxy connection to the attacker server. In this way, the method can be easily integrated with 3rd party software (web browser, chat tool, so on).

Attacker Server Design

The intermediate server specified as the attacker server on Figure 4 designed for the synchronized communication between the attacker and victim devices. There are two different services on the attacker server. The communication between the attacker and attacker server is ensured with the standard forward proxy server while the communication between the attacker server and the victim devices is ensured with TCP protocol developed specifically. The attacker server converts the requests of the attacker to a format which can be delivered to victim devices. It also delivers the replies from the victim devices to the attacker through the forward proxy server.

1 BYTE	1 BYTE	2 BYTE	MAX: 65,536 BYTE
MAIN HEADER	SUB HEADER	DATA SIZE	DATA

Figure 5. Packet Parameter Structure

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

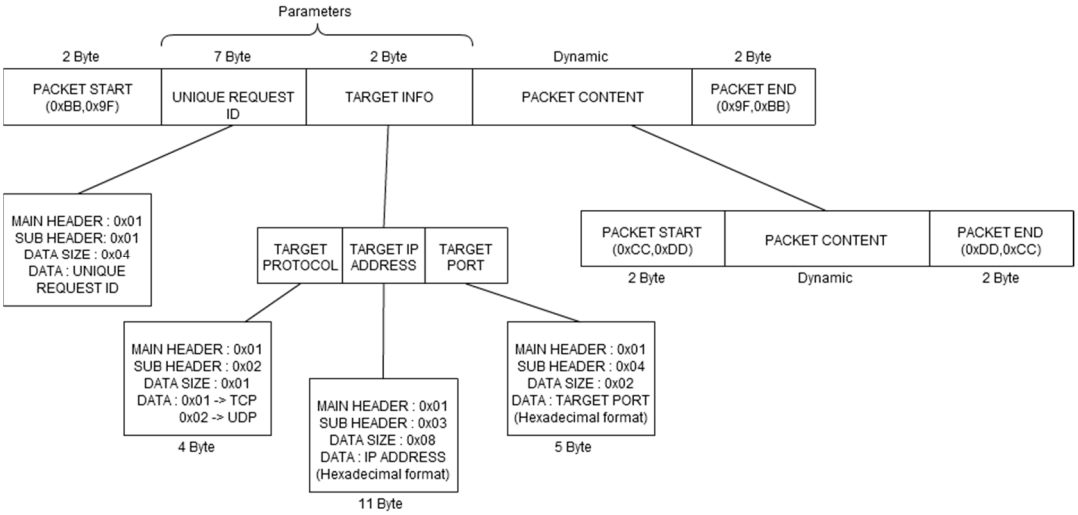

Figure 6. Packet Structure of the Attacker Server Requesting from Victim Device

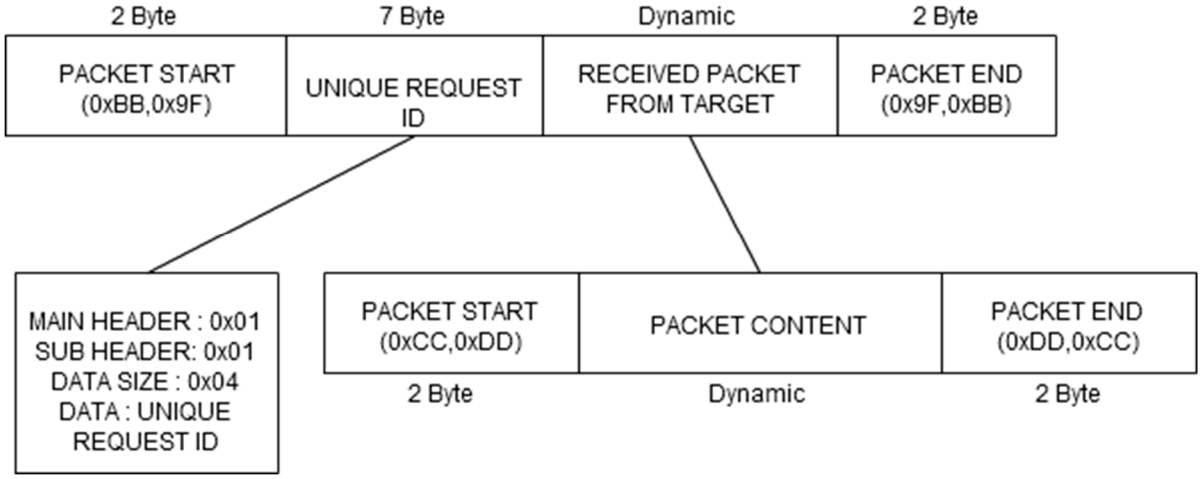

Figure 7. Packet Structure of Victim Device Sending Replies to Attacker Server

When one of the victim devices communicates with the attacker server, a unique identity is created for the victim device. In this way, it can identify and display victim devices in the system. The attacker must determine which victim device will be used via attacker server software before sending any request.

The attacker server converts the request of the attacker received via forward proxy protocol to package structure in Figure 6. The parameter structure of the packages is in line with the information indicated in Figure 5.

The package starts with 0xBB,0x9F value. 4 bytes identity is created specially for each request of the attacker. A total of 7 bytes data creates the first parameter.

20-byte target information creates the target protocol, target IP address and the target port. Firstly, which protocol will be used for the 4-byte request will be determined. Then the next 11-byte

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

indicate the target IP address and the last parameter of the target information will indicate the port number of the target by using 5-byte data.

For the last thing, the package content (HTTP, FTP, SSH, so on) which is delivered by the attacker via proxy server service is placed between 0xCC,0xDD and 0xDD,0xCC. And the request package structure ending will be 0x9F,0xBB value.

By checking the identity of the data received from the victim device, the reply will be delivered through the channel (thread) where the request sent to the proxy server by the attacker.

4.2.2. Malware in the Device of the Victim

When the internet connection is active on the device of the victim, it communicates with attacker server and notifies when the device is active. Then it will start to wait for the request to be received from attacker server. When request delivered from attacker server in the form of Figure 6, the client socket is created with the parameters specified via a new channel. The specified package content will be delivered to target server. The replies received from the target server will be delivered to attacker server by using the package format in Figure 7. In this way, it serves as a reverse proxy server.

An attacker who uses such a method can perform anything on the internet by using the victim devices synchronously through intermediate server created by himself. A malware using a similar method identified and analyzed in Malware Analysis Report - Android Web Proxy Bot notification published by Alcatel-Lucent in 2014. [13]

4.3. Possible Goals of the Attacker Using the Method

4.3.1. Anonymization and Privacy on the Web

The attacker can have the possibility to surf the internet anonymously. There can be major problems in legal sense since the illegal activities will be performed through the device. It can lead to serious legal problems when we consider the possibility of the attacker may perform the connection with the device through an SSL layer, the possibility of using deletion method such as Gutmann [14] after the illegal activity has taken place and the victim is not aware of the malware.

4.3.2. Capture of Personal Accounts and Unauthorized Transactions

Access to bank accounts through the victim's own device can be ensured when it is used with the malware developed for banking. In this case, it will be thought that the transaction carried out by the victim and unauthorized transactions will be difficult to detect.

4.3.3. Interference to Restricted Domains and Local Network

The attacker has an access to restricted areas where the victim has the right to access. He can have an access to critical information and perform an action on behalf of the user. Also as it can have access to the local network where the device is connected, he can have an access to devices connected to the local network and can copy more devices for himself by exploiting vulnerabilities in the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2017 doi:10.20944/preprints201705.0123.v1

devices. He can make the devices unusable or change the configuration without permission such as DNS hijacking with interference to network devices.

4.3.4. Fake Ad Clicks

The advertising companies consider factors such as IP address, the location of the user in order to determine the fake ad clicks. The attacker may mimic the action of clicking on the ads of the companies serving ads publishing in order to provide financial gain and get through the fake ad clicking filters. Therefore, he can damage financially..

4.3.5. Website Statistics / Membership Fraud

The attacker can provide hits for target websites. He may aim to manipulate search engines, increase the value of the website with fake visits. Also, he can get through the bot detection algorithms of services which pay attention to the reality of the users (Facebook, Gmail etc.). He can perform attacks to these services with fake accounts.

4.3.6. DDoS Attack

Firewall devices and software developed to provide protection against DDoS attacks has a critical importance in order to understand the connection is established by a real person. It ensures the access of the real users to the services while it repels the attacker devices. The detection algorithm can get through with the method, in this case, the attack can be successful since firewall devices and software may have difficulty in terms of identifying who performed the connection.

Another dimension of danger is, even 0.04% of mobile devices which host malware that uses this method will mean more than 1.000.000 victims. It was noted that the detected malware consumes 4 KB of traffic in a second in Alcatel-Lucent[14] report. When the consider that the malware will operate all day, this means that the data transfer will be in the size of 321.8 TB.

5. Conclusion

The attackers will continue to discover new methods in time. The damages that people may suffer become predictable and irreversible situations in case of uncontrolled use of mobile devices and not enough attention will be paid. The attacker may have been given full authority with the reverse proxy method. As relief will not be carried out in cases where carelessness of judicial institutions and lack of investigations takes place, it can also lead more damage on victim individuals and institutions. It needs to be investigated with a very hard work in the case of any victimization since the possibility of the mentioned operates in a highly subtle manner.

 doi:10.20944/preprints201705.0123.v1

References

1. Statista.com, "Number of apps available in leading app stores as of March 2017", https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/
2. Vincent, James, "Android is now used by 1.4 billion people", https://www.theverge.com/2015/9/29/9409071/google-android-stats-users-downloads-sales
3. Statt, Nick, "1 billion Apple devices are in active use around the world", https://www.theverge.com/2016/1/26/10835748/apple-devices-active-1-billion-iphone-ipad-ios
4. DuPaul, Neil, "Common Mobile Malware Types: Cybersecurity 101", https://www.veracode.com/blog/2013/10/common-mobile-malware-types-cybersecurity-101
5. Herzberg, Ben ve Bekerman, Dima ve Zeifman Igal, "Breaking Down Mirai: An IoT DDoS Botnet Analysis", https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
6. Pollack, Doug, "Bitcoin's strategic place in ransomware", https://iapp.org/news/a/bitcoins-strategic-place-in-ransomware/
7. Kaspersky Lab., "Mobile Malware Evolution 2016", https://securelist.com/files/2017/02/Mobile_report_2016.pdf
8. Verma, Adarsh, "Android.Bankosy Trojan Learns To Steal Your One-Time Passwords Sent Through Calls" https://fossbytes.com/android-bankosy-trojan-has-now-learnt-to-steal-one-time-passwords-sent-sent-through-voice-calls/
9. Kumar, Mohit, "New Android Malware Hijacks Router DNS from Smartphone", http://thehackernews.com/2016/12/android-dns-malware.html
10. AVG, "Malware Is Still Spying On You Even When Your Mobile Is Off", http://now.avg.com/malware-is-still-spying-on-you-after-your-mobile-is-off/
11. Nginx, "WHAT IS A REVERSE PROXY SERVER", https://www.nginx.com/resources/glossary/reverse-proxy-server/
12. @granner, "Advanced Proxying to use DarkComet Slaves to surf the web using PLINK and NCAT", https://hackforums.net/showthread.php?tid=2774692
13. Alcatel-Lucent, "Malware Analysis Report – Android Web Proxy Bot", http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9594-notcompatibleandroid-web-proxy-bot-malware-analysis-report.pdf
14. Wikipedia, "Gutmann Method", https://en.wikipedia.org/wiki/Gutmann_method