FOX IT
part of nccgroup

Expert Witness Report on ByLock Investigation

18 August 2017
Version: 0.1
Status: Draft
Pages: 28

Reference: PR-160860
Principal: Fatih Sahinler
Author: Ivo Pooters & Gina Doekhie
Classification: **COMMERCIAL.RESTRICTED**

COMMERCIAL.RESTRICTED

This document is classified as COMMERCIAL.RESTRICTED. Any information published in this document and its appendices is intended exclusively for the addressee(s) as listed on the document management distribution list. Only these addressee(s) and additional persons explicitly granted permissions by any of these originally authorized addressee(s) may read this document. Any use by a party other than the addressee(s) is prohibited. The information contained in this document may be COMMERCIAL.RESTRICTED in nature and fall under a pledge of secrecy.

If your name is not listed on the document management page or if you have not obtained the appropriate (written) authorization to read this document from an authorized addressee, you should close this document immediately and return it to its original owner.

Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox-IT cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by its contained information.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
Nederland

Telephone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: fox@fox-it.com
Internet: www.fox-it.com

Trademark

Fox-IT and the Fox-IT logo are trademarks of Fox-IT B.V.
All other trademarks mentioned in this document are owned by the mentioned legacy body or organization.

Document Management

Version Management

Project name : Breezewood**Error! Reference source not found.**
Reference : PR-160860
Principal : Fatih Sahinler **Error! Reference source not found.**
Subject : Expert witness report on Bylock investigation
Date : 18 August 2017
Version : 0.1
Status : **Error! Reference source not found.**
Author : Ivo Pooters & Gina Doekhie**Error! Reference source not found.**

This version replaces all previous versions of this document. Please destroy all previous copies!

Distribution List

Version	Date	Distribution method	Name/function/remarks
0.1	Aug 18, 2017	PDF via clientportal	Fatih Sahinler

Reviews

Version	Date	By	Remarks

Changes

Version	Date	By	Remarks

Related documents

Version	File name

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

Fox-IT was contacted with a request for an expert witness report in ongoing legal proceedings in Turkey by a representative (hereafter: Principal) for Fatih Sahinler who is requesting an expert opinion on the following matter.

The Turkish government is currently actively pursuing the prosecution of members of the alleged terrorist organization *fethullahçı terör örgütü/paralel devlet yapılanması (FTÖ/PDY)*. To this end, the Turkish Intelligence organization MIT (Millî İstihbarat Teşkilatı) has investigated the relation of the chat application *ByLock* to FTÖ/PDY. MIT has written a report on this investigation describing the ByLock application and MIT's findings regarding the relation of the ByLock users to the alleged FTÖ/PDY. This report (hereafter: the MIT report) was distributed to the main prosecutor's office in Ankara.

According to Principal, the report is used by Turkish prosecutors to identify a large number of people as members of the alleged FTÖ/PDY and to place people in preliminary imprisonment based merely on the fact that they have used ByLock. The findings and conclusions of the MIT report are, according to Principal, not sufficiently scrutinized and incorrect. Therefore, Principal requests Fox-IT to review the report and assess the soundness of the methodology, findings and conclusions.

Fox-IT has received two translated copies of MIT's report titled "ByLock Application Technical Report". The first translated report is a sworn translation from Turkish to Dutch by drs. E. Battaloglu. The second translated report is a sworn translation from Dutch to English by Jannie Johanna van Ravesteijn-Prins released on July 19th, 2017.

1.2 Biographical Statement

voorletters en naam	I Pooters
beroep	
correspondentieadres	
telefoonnummer	
faxnummer*	
e-mailadres*	

2 Brief Summary of Conclusions

Sort of management summary of the expert witness report

3 Issues Addressed

1. What is Fox-IT's opinion on the investigation methodology used by MIT in the ByLock investigation?

2. How sound is MIT's identification of persons that have used the ByLock application?
    a. How are ByLock accounts linked to persons and how reliable is this method?
    b. How are ByLock accounts created and is it possible to add accounts linked to another person?
    c. How is it determined that a ByLock user was actually active on ByLock and how reliable is this method?

3. How sound is MIT's conclusion on the relation between ByLock and the alleged FTÖ/PDY?
    a. How is it concluded that the ByLock application is used exclusively by the alleged FTÖ/PDY?
    b. What is Fox-IT's opinion on the stated findings and the resulting conclusion?
    c. How does the ByLock application relate to other similar chat applications available with respect to security?

4. Are there any other issues identified by Fox-IT which are relevant to the ByLock investigation?

4 METHODOLOGY

This research is performed by Fox-IT in July and August 2017. The investigation is executed from the office in Delft, the Netherlands.

4.1 Analysis of MIT investigation and reporting

During this research, Fox-IT analyzed the report on the soundness of the digital investigation process used by MIT in their investigation. In specific, the methodology, argumentation, findings and conclusions of MIT investigation. A digital forensic process is the need to ensure that the results do not lose evidentiary weight and therefore, its admissibility as evidence. So, what makes a process forensically sound? Generally, four criteria are used for ascertaining the forensic soundness of a digital process[1]:

1. Meaning
   When potential electronic evidence is acquired and analyzed, it is important that it be preserved in the state in which it was found and that it not be changed by a digital forensic process.
2. Errors
   Any possible error and its impact on the accuracy and reliability of the evidence, and any potential interference on the forensic process are all issues that must be discussed.
3. Transparency
   It is of importance that the forensic process be transparent and capable of being independently verified. A key element of verification is the ability to reproduce the forensic process under the same conditions with a consistent level of quality being observed each time the process is run. Sources for all hypotheses should be included.
4. Experience
   All possible hypotheses should be analyzed and evaluated in which the investigator had no tunnel vision and is unbiased to perform the investigation.

These criteria are used when performing the analysis of the report. Also the general soundness of the methodology, argumentation, findings and conclusions of the MIT report are evaluated on completeness.

4.2 Fact-checking

Fox-IT attempted to verify facts and observations relevant to the conclusions of the MIT report. To this end, open and closed sources were researched and data from ByLock was analyzed to the extent that this was available at the time of this research. Analysis was performed by decompilation of Java bytecode and static analysis of the decompiled code.

Fox-IT was able to acquire the following versions of the ByLock Android application:

- ByLock 1.1.6 with MD5 hash[2] `b43eeb3fed4c20061e0c87f4d371508d` available on:
  - http://downloadapk.net/down_ByLock-Secure-Chat-amp-Talk.601634.html
  - http://apkrestricted.com/down_Free-download_ByLock-Secure-Chat-amp-Talk.601634_APK-file.html
- ByLock 1.1.7 with MD5 hash `84fddf10a23f4f25b5212232b73cd557` available on:
  - https://m.downloadatoz.com/bylock-secure-chat-talk/net.client.by.lock/bylock-secure-chat-talk,v1.1.7-download.html

[1] McKemmish, Rodney. "When is digital evidence forensically sound?." *Advances in digital forensics IV* (2008): 3-15.

[2] A hash value is the result of a mathematical calculation, using an algorithm. The calculation only works in one direction, meaning that the hash value cannot be used to determine the original data. A hash value represents a digital fingerprint of the data and consists of a series of numbers (of a fixed length). Typically, a hash value is recorded during the creation of a forensically sound copy. The integrity of that copy can be checked (possibly by others) by calculating the hash value again, and checking it against the originally recorded hash value. Known and commonly used hash algorithms are MD5 and SHA1.

The following versions were mentioned in the MIT report, but were no longer available in online public sources for analysis:

- ByLock 1.1.3
- ByLock 2.0 (ByLock++)

Data from the ByLock servers was not available for analysis by Fox-IT. This data has not been made available by MIT.

Furthermore, online open sources were researched to verify observations described by MIT related to Google searches, Twitter and other online platforms.

5 Findings and Conclusions

5.1 What is Fox-IT's opinion on the investigation methodology used by MIT in the ByLock investigation?

An investigation is performed by MIT on a communication application for smartphones, ByLock. The ByLock application and the corresponding communicating servers have been subjected to technical examination by MIT. In the MIT report, the methodology is not described explicitly. Fox-IT has deduced from the described findings that the following investigation steps have been performed by MIT:

- Section 2 provides general information on the ByLock application.
- Section 3.1 describes the legal grounds for and methods used in obtaining data stored in the ByLock application servers.
- Section 3.2 describes an analysis of IP-addresses and domain names related to ByLock performed by MIT. Through analysis of the different versions of the application and a certificate which previously identified by MIT, nine different IP-addresses had been used for the ByLock application. MIT does not mention how this certificate was identified. The certificate was issued in the name of "David Keynes". MIT concludes that only IP-address 46.166.160.137 had been used for bylock.net from 1 September 2015 to 9 October 2016.
- Section 3.3 describes results from an open-source research on ByLock performed by MIT. MIT compared the searches made for the word ByLock in search engines from Turkey and Worldwide. MIT beliefs that all searches made have Turkey as source country, and searched from outside of Turkey were utilizing VPN. Next, MIT states that the Twitter users who posted content via "ByLock" before the coup, the vast majority appear to have been posting content in support of the alleged FETO/PDY.
- Section 3.4 describes results from analysis of cryptographic protocols used by ByLock and reverse engineering performed by MIT. During the examination of the source codes, MIT found that blurring (obfuscation) had been applied.
- Section 3.5 describes results from an analysis of a ByLock server performed by MIT. The supposed administrator of the ByLock server blocked the access of some Middle Eastern IP addresses to the application. MIT believes that because almost all of the blocked IP addresses are from Turkey, the users were required to use VPN which prevents the identifications of these users.
- Section 3.6 describes the results of the examination of database files derived from the server. MIT obtained a database file of 109GB where the ByLock application data was stored.
- Section 3.7 describes statistical data of the ByLock server analyzed by MIT.
- Section 4 holds the assessment and conclusion. MIT concludes that ByLock has been offered to the exclusive use of the member of the terrorist organization of FETO/PDY.

5.1.1 ByLock.net

The first finding that MIT presents in section 3.2 is that only IP-address 46.166.160.137 had been used for bylock.net from 1 September 2015 to 9 October 2016. MIT identified nine different IP addresses by work conducted in connection with a self-signed SSL certificate issued in the name of "David Keynes". Fox-IT did research on the IP-addresses and domain names used by ByLock in order to verify the findings.

ByLock is an Android Package Kit (APK). An APK must be digitally signed before it can be installed on a phone[3]. This digital signature is formed by a certificate in which the developer only has the private key. Android use this design to identify the developer and to create a trust relationship between published applications. A developer is allowed to use self-signed certificate. The certificate does not have to be signed by a Certificate Authority. In each APK, a certificate is present. In the ByLock application, the certificate is available in the location:

META-INF/BYLOCK.RSA

[3] https://developer.android.com/studio/publish/app-signing.html

In both version 1.1.6 and 1.1.7 of ByLock, the certificate owner is “David Keynes”

```
Owner: CN=David Keynes, OU=Application CA, O=by Lock,
L=Beaverton, ST=Oregon, C=US
```

See Appendix 7.1, for the full details of the certificate. Fox-IT resulted in a number of ten IP addresses when researching IP addresses with David Keynes in the SSL certificate:

- 46.166.160.137
- 46.166.164.176
- 46.166.164.177
- 46.166.164.178
- 46.166.164.179
- 46.166.164.180
- 46.166.164.181
- 46.166.164.182
- 46.166.164.183
- 69.64.56.133

The last IP address was not mentioned in the MIT report . Also, Fox-IT concludes that of the above IP addresses only 46.166.160.137 had been used for ByLock.net. MIT states that the ByLock application had been used during the coup attempt of 15 July 2016 in which ByLock.net used 46.166.160.137. Fox-IT performed an open-source investigation on the IP address 46.166.160.137 and its relation to ByLock.net in order to verify the MIT statement. In multiple sources, it is found that the IP address 46.166.160.137 resolved to ByLock.net from August 2014 to March 2016.Fox-IT also created a complete timeline of the domain name ByLock.net and to which IP address it resolved, see Table 1**Error! Reference source not found.**.

Based on this investigation, Fox-IT is of opinion that the results of MIT in which they state that IP address 46.166.160.137 had been used for ByLock.net from 1 September 2015 to 9 October 2016 is not founded and unlikely. The ByLock server and therefore also its application was not available from March 2016 on 46.166.160.137. For this reason, Fox-IT states that the ByLock application was not available during the coup on 15 July 2016.

5.1.2 Google Trends

The second finding MIT addresses in section 3.3 is the result of their open-source research on ByLock. MIT connects the number of searches made for the word ByLock in search engines to users gaining access to the ByLock application available on APK websites as a result of its removal from Google Play before 15 July 2016. MIT links the number of these search statistics to the number of users found on the application server, 215.092.

First, the source of the search statistics is not mentioned in the report. Derived from examining the figures included in the report, Fox-IT assumes this investigation was performed using Google Trends[4]. The numbers shown in Google Trends do not represent the actual number of searches, rather these numbers represent the popularity in search interest relative to highest peak popularity for a given search term. A value of 100 is the peak popularity for the term and a value of 50 means that the term is half as popular.

Fox-IT attempted to reproduce the research by use of the “bylock” search term on Google Trends. MIT studied the searches of the term ByLock between 17 December 2013 and 17 February 2016. Within this period, Fox-IT analyzed the worldwide search statistics. The regions with the most interest to the “bylock” search term are Turkey and Sweden. The popularity of the search term “bylock” is more popular in Sweden than Turkey, see Figure 1.

[4] Google Trend is a Google web service that provides free insight in Google search statistics.

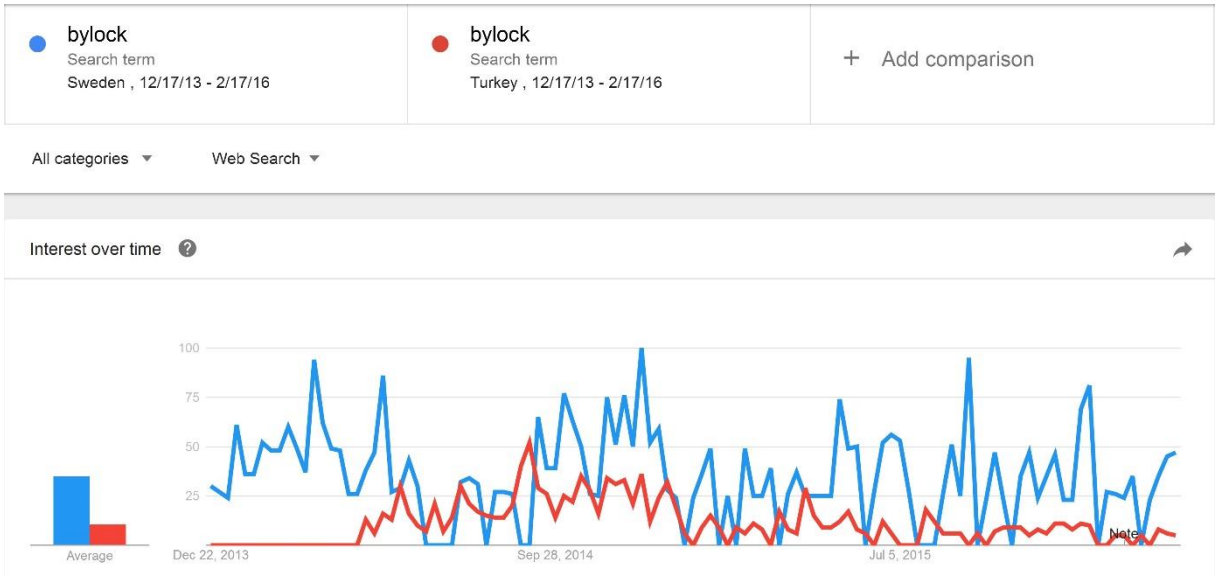


Figure 1: bylock Search term statistics on Google Trends in the period 17-12-2013 until 17-2-2016 Turkey and Sweden.

This can probably be attributed to a famous author in Sweden who goes by the name “Maj Bylock”. Other related topics in this period are:

- iPhone – Smartphone
- iOS – Operating system
- App Store – iOS

Next, the search interest for the term “bylock” in the overall period of 17 December 2013 until the time of this investigation, 14 August 2017, for only the region Turkey is analyzed. A clear difference can be observed between the amount of searches before the coup and after the coup on 15 July 2017, see Figure 2.

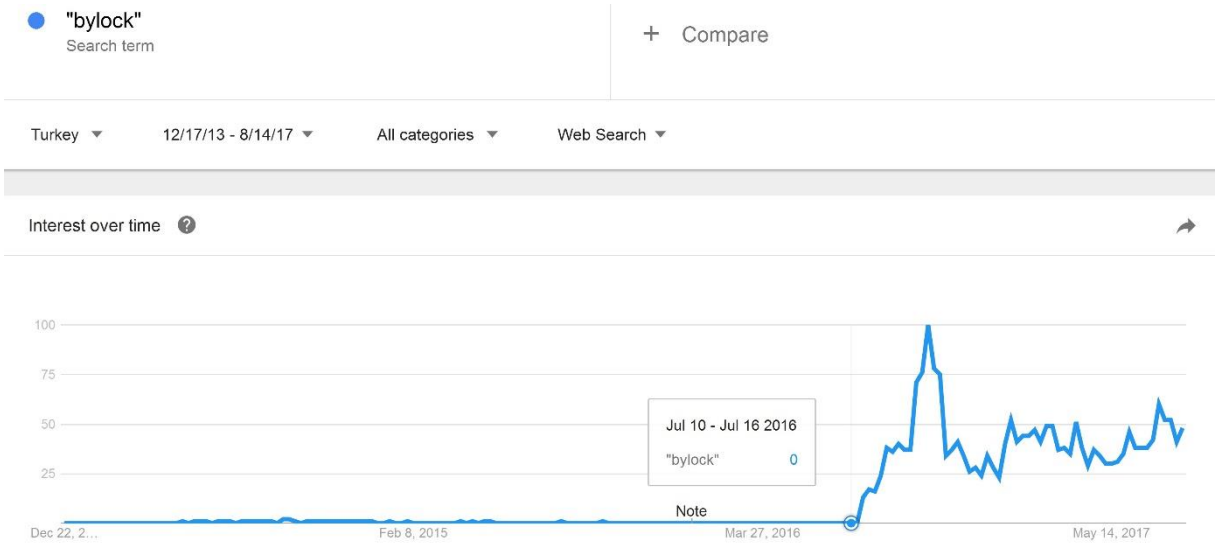


Figure 2: bylock Search term statistics on Google Trends in the period 17-12-2013 until 14 August 2017 in Turkey.

The search interest in the term “bylock” is significantly increased right after the coup of 15 July 2016. This increase is of such a high value that the search interest before the coup is negligible. The incline in searches on the term can be explained by the media interest in ByLock after the coup attempt on 15 July 2016. Also, the amount of search interest in the term “bylock” before the coup does not imply a similar amount of usage of the ByLock application. Fox-IT concludes that in the light of the statistics no link can be determined between the number of search interest and the actual number of users of the ByLock application. The numbers shown in Google Trends only represent how a search term becomes more or less used in the Google search engine, thereby visualizing a trend. It does this by giving the day in which the search term was searched most a score of 100 and 0 for the day it was least searched. Therefore it is very difficult, next to impossible, to compare a trend of popularity to actual numbers.

5.1.3 General

In general, Fox-IT is of opinion that the investigation methodology used by MIT is not forensically sound based on the following criteria and associated observations:

- Section 3.2: In the analysis of ByLock’s IP and domain name, MIT concludes that the IP address 46.166.160.137 had been used for bylock.net from 1 September 2015 to 9 October 2016. However, Fox-IT investigation shows that this IP address had been used from August 2014 to April 2016. The investigation performed by MIT based on this finding is not credible and therefore reliable.
- Section 4: In the conclusion, MIT address issues not discussed in the report. Scientifically, the conclusion cannot hold new findings.
- Section 2.4: A difference is made between ByLock and global and commercial instant messaging apps. MIT implies that ByLock is not ease of use and does not have a commercial interest by reaching the most possible users. This implication is not founded by research and therefore biased.
- Section 3.3: MIT is not able to verify if the searches made from France, UK and US are from users that were utilizing VPN. Next to that, MIT uses subjective terms in their statement that the vast majority of Twitter users who posted content via ByLock also have been posting content in support of the alleged FETO/PDY. Fox-IT is of opinion that MIT is biased and suggestive to a certain outcome in light of the statistics.
- Section 3.1: In this section, MIT create legal support for their method in obtaining data stored in the application server. Sensitive methods to collect intelligence have been excluded. This means that the digital process is not transparent and cannot be independently verified or reproduced.
- Same applies for the results presented in section 3.5 and 3.6. Screenshots have been depicted in the report of the logs/data available on the application server. This data is easily crafted and does not ensure its authenticity

5.1.4 Conclusions

5.2 How sound is MIT's identification of persons that have used the ByLock application?

5.2.1 How are ByLock accounts linked to persons and how reliable is this method?

Section 3.6 of the MIT report describes the results of the investigation into the ByLock database data. This is the only section containing a reference to identification of individuals as ByLock users.

The MIT report does not describe how ByLock accounts are linked to actual persons. The only reference found in the report to identification of the person is mentioned in section 3.6.2.11. There, MIT describes that entries in the *Log* table of the ByLock database have been used to identify individuals. These entries contain the IP-address of the ByLock user during login or registration.

The MIT report does not describe how this IP-address is linked to an individual. However, this attribution of IP-address to individual is not trivial and can be prone to mismatching since an IP-address is usually not strictly assigned to one individual. There are multiple challenges with attributing an IP-address to an individual:

Shared wifi access points. ADSL subscription number may lead to wrong individual.

VPN or other anonymizing technology.

In the MIT report, the possibility is mentioned that users use a Virtual Private Network (VPN). It is very common nowadays to use a VPN server, which keeps web browsing secure and private. When a VPN connection is used, the IP address available in the "log's" table on the application server belongs to the VPN server. See **Error! Reference source not found.**, for an example of a VPN connection to a webserver, in this case the ByLock application server. In this scenario, the VPN hosting party holds which IP address connects to which IP address at what time. This information should be first requested in legal proceedings and after that the information of the IP address at the ISP should be requested. However, most of the time this information is not available on the VPN server as it is a private service. It also possible to use multiple VPN connections, which means that at each point of the path the IP address should be traced and requested.

Figure 3:Example VPN connection

IMEI cloning. IMEI number may lead to wrong individual.

Telecom log retention.

An IP address is a unique identifier of a device in a computer network that uses the Internet Protocol for communication. A device can be a personal computer, laptop, tablet, phone, server, etc. An IP address is issued by a Regional Internet Registry (RIR). There exist five RIRs, each for a particular region of the world, and manage the allocation and registration of IP addresses. The customers of a RIR could be both an Internet Service Provider (ISP) or end-user organization. In order to link an IP address to a registrar, information from the RIR can be obtained. However, when the registrar is an ISP, the ISP holds the information about which IP address is assigned to which customer. This information can be requested in legal proceedings.

Any of the abovementioned issues may lead to incorrect attribution or impossible attribution of an IP-address to an individual. Since this is a crucial step in identifying the individuals, this method should be scrutinized. Currently, MIT does not provide any information that allows the scrutiny of their method.

5.2.2 How are ByLock accounts created and is it possible to add accounts linked to another person?

As mentioned, Fox-IT analyzed versions 1.1.6 and 1.1.7 of the ByLock application. In both versions, a user can register by creating a username and entering a password. Figure 4 depicts the registration screen of ByLock v1.1.7. No e-mail address, phone number or other personal identifying information is entered when creating an account. Fox-IT has confirmed, by reverse engineering of the ByLock application that no other information of the phone or user is sent to ByLock servers.

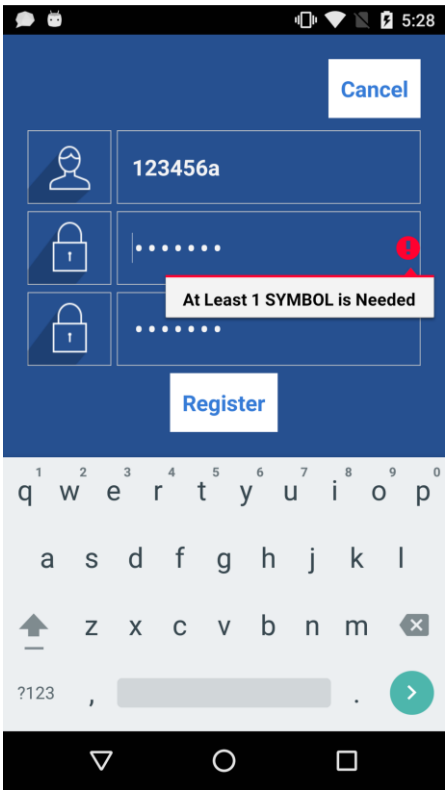


Figure 4: Register for ByLock account.

The loose registration scheme allows creation of arbitrary accounts, since:

- There are no restrictions found to a specific group membership as a condition of use.
- There is no verification of phone number or email address by the application.
- There are no restrictions in the username chosen during registration.

This allows creation of suggestive accounts by registering and using an account with a name or other identifier (e.g. email address or phone number) related to a real individual while that individual is unaware of the existence of the ByLock account.

5.2.3 How is it determined that a ByLock user was actually active on ByLock and how reliable is this method?

Section 5.2.2 of this report describes that arbitrary ByLock users may be registered by anyone having access to the ByLock application. This leads to the question how MIT has differentiated between users that have been registered and logged on to ByLock and users that have actually used ByLock to communicate.

In the report it is not explicitly described if and how MIT determined the actual activity of the ByLock users. It is therefore unclear whether the individuals identified by the ByLock investigations have actually been communicating using ByLock

5.2.4 Conclusions

Fox-IT has analyzed the MIT investigation as described in the MIT report. The sub-issues are addressed in section 5.2.1 to 5.2.3.

How are ByLock accounts linked to persons and how reliable is this method?

The MIT report states that the IP-address value from the ByLock database is used for identifying individuals using ByLock. However, the report omits the method used to attribute the IP-addresses to individuals. This is, however, not trivial and prone to incorrect attributions.

Fox-IT identified the issues that may lead to incorrect attribution or impossible attribution of an IP-address to an individual. Since this is a crucial step in identifying the individuals, the method should be scrutinized. Currently, MIT does not provide any information that allows the scrutiny of their method.

5.3 How sound is MIT's conclusion on the relation between ByLock and the alleged FTÖ/PDY?

5.3.1 How is it concluded that the ByLock application is used exclusively by the alleged FTÖ/PDY?

Below, Fox-IT has summarized the arguments and conclusions as described in the MIT report and as interpreted by Fox-IT.

MIT concludes that the ByLock application is used exclusively by the alleged FTÖ/PDY based on the following:

1. The ByLock application is designed to communicate with a strong cryptographic system over the internet, which allows sending each message with a crypto key. Fox-IT assumes MIT intends to describe that the messages can be encrypted using a crypto key instead of sending the crypto key.
2.
    a. MIT states multiple observations and findings about the developer of ByLock and concludes that the developer does not have any corporate or commercial nature.
    b. MIT states multiple observations with respect to ByLock and Turkyish language and users. Then MIT goes on to conclude that ByLock was meant to be used by the members of the alleged FTÖ/PDY under the disguise of a global application. Some of the arguments listed are:
        - The administrator blocked IP addresses with origin Turkey.
        - Users were forced to use VPN in order to hide their identities.
        - Almost all searches on Google for the search term "bylock" were made from Turkey and significantly increased as of the date access to the application from Turkish IP addresses were blocked.
        - Publications related to ByLock have mostly been posted through fake accounts and in which the content was in favour of the alleged FTÖ/PDY.
        - Before the coup attempt on 15 July 2017, the ByLock application was not known to Turkish public or known outside of Turkey.

3. Utmost security of user id and communication was an aim of the ByLock application. Also, the reason why the application does not require personal information during sign up and does not have a verification system is to ensure anonymity.
4. The application developer used personally “developed” SSL certificated instead of verified SSL certificates. Fox-IT assumes that with the term personally developed SSL certificate, MIT means to refer to a self-signed certificate. MIT goes on to conclude on that observation and on the intentions of the developer; MIT believes that a self-signed certificate was chosen to prevent the flow of information to servers other than his own.
5. In order to be able to communicate with another registered user, both parties need to mutually add each other’s username/code. The application is therefore considered to have been designed to allow communication suitable to “the cell structure”.
6. The application meets all organizational communication needs and are controlled and supervised by the application administrator.
7. The automatic deletion of messages from the device after a certain period without manual intervention indicates that the system is designed to prevent access to communication data and details in the event of a possible legal confiscation of the device.
8. MIT makes an inference of the users intention to hide their identity, based on the following observations:
    - Users create long passwords;
    - Users manually download the application on APK websites instead of Android Market or Apple Appstore;
    - Users did not use the real name as user ID during sign up;
    - Users used inter-organizational code names instead of real identities in their contact lists and communication.

    Further, MIT states that ‘almost all’ of the content of the decrypted messages are of communications and activities of alleged FTÖ/PDY and matched the organization’s jargon.
9. Members of the organization who were subjected to judicial control measures following the coup attempt of 15 July 2016 conducted by the alleged FTÖ/PDY have stated that ByLock had been used as an inter-organizational communication medium by the member of the alleged FTÖ/PDY.

Based on the above, the MIT concludes that ByLock has been offered to the exclusive use of the members of the alleged terrorist organization of FTÖ/PDY.

5.3.2 What is Fox-IT’s opinion on the stated findings and the resulting conclusion?

Fox-IT is of opinion that the resulting conclusion is not founded by the stated findings of MIT above. In this section each of the arguments is analyzed to determine the accuracy, correctness and soundness. Finally, Fox-IT will provide an opinion on the overall conclusion.

1. Strong crypto. MIT states that the ByLock application makes use of a strong cryptographic algorithm. Strong is a relative term and Fox-IT does not regard the ByLock crypto stronger than other known chat applications. The use of cryptography has become common practice in communications in recent years. Chat applications for the masses like Whatsapp and Facebook use the signal protocol which implements sophisticated crypto protocols for securing communications[5][6]. The encryption used in the ByLock application is readily available using the default Application Programming Interface (API). ByLock used standard, publicly available Java libraries to provide encrypted communication between users of the application. Those are included in java.security and javax.crypto[7] and are well-documented[8][9].

2a. Lack of commercial nature. Fox-IT follows this reasoning.

2b. Disguise of global application. MIT's finding that all Google searches for the "bylock" term originated from Turkey is invalid. Figure 5 shows that Sweden has the highest popularity rank for this term. There is also no significant increase observed in Google searches for the "bylock" term after the IP addresses from Turkey were blocked by the Administrator on 15 November 2014, see Figure 6 for only search interest in Turkey.

[5] https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper-1.pdf

[6] https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

[7] https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html

[8] https://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html

[9] http://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

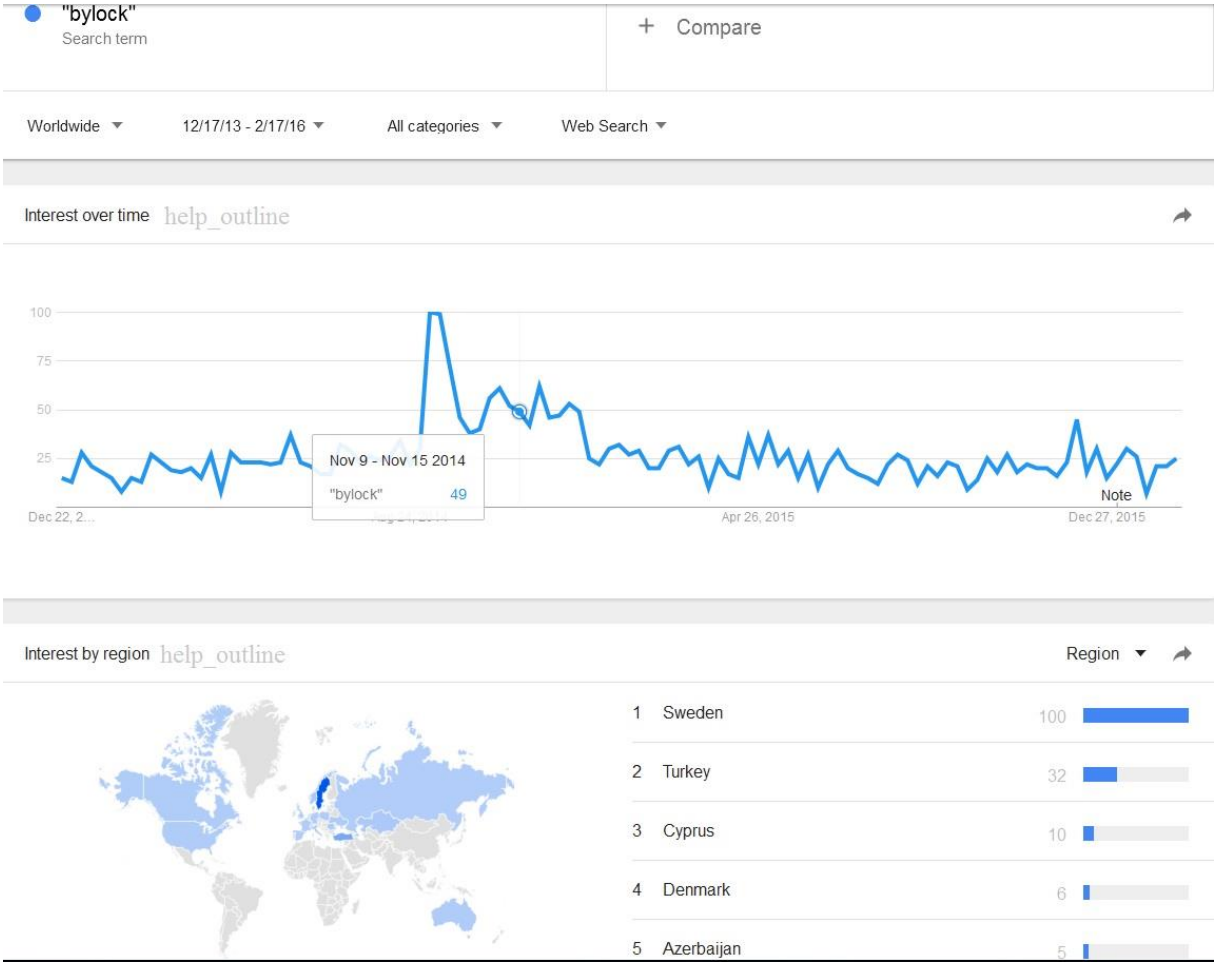


Figure 5: Google Trends search interest for the search term "bylock" worldwide in the period similar to the MIT research.

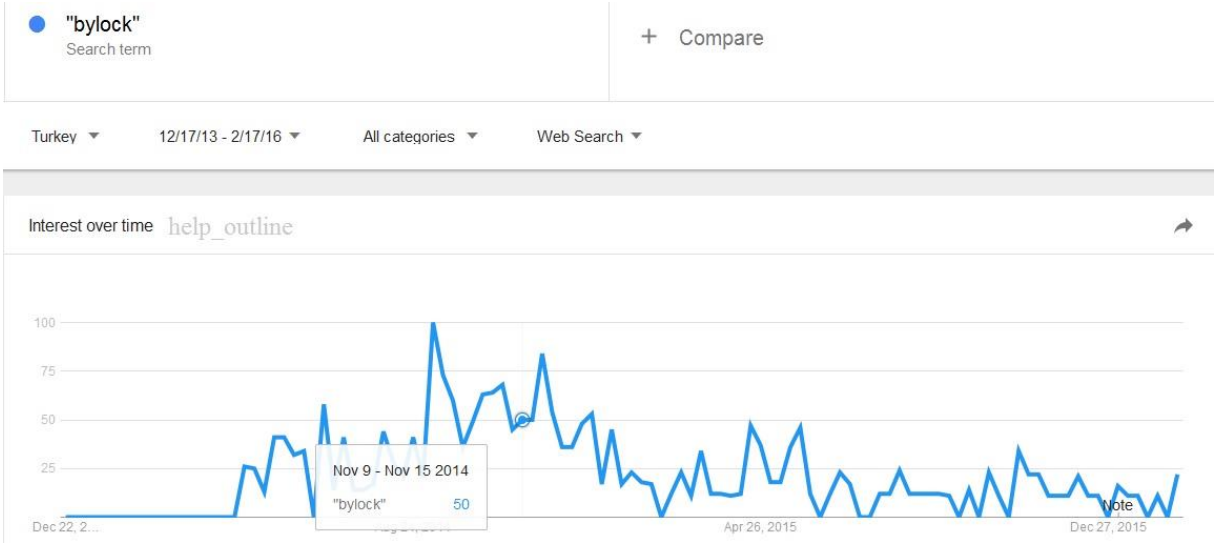
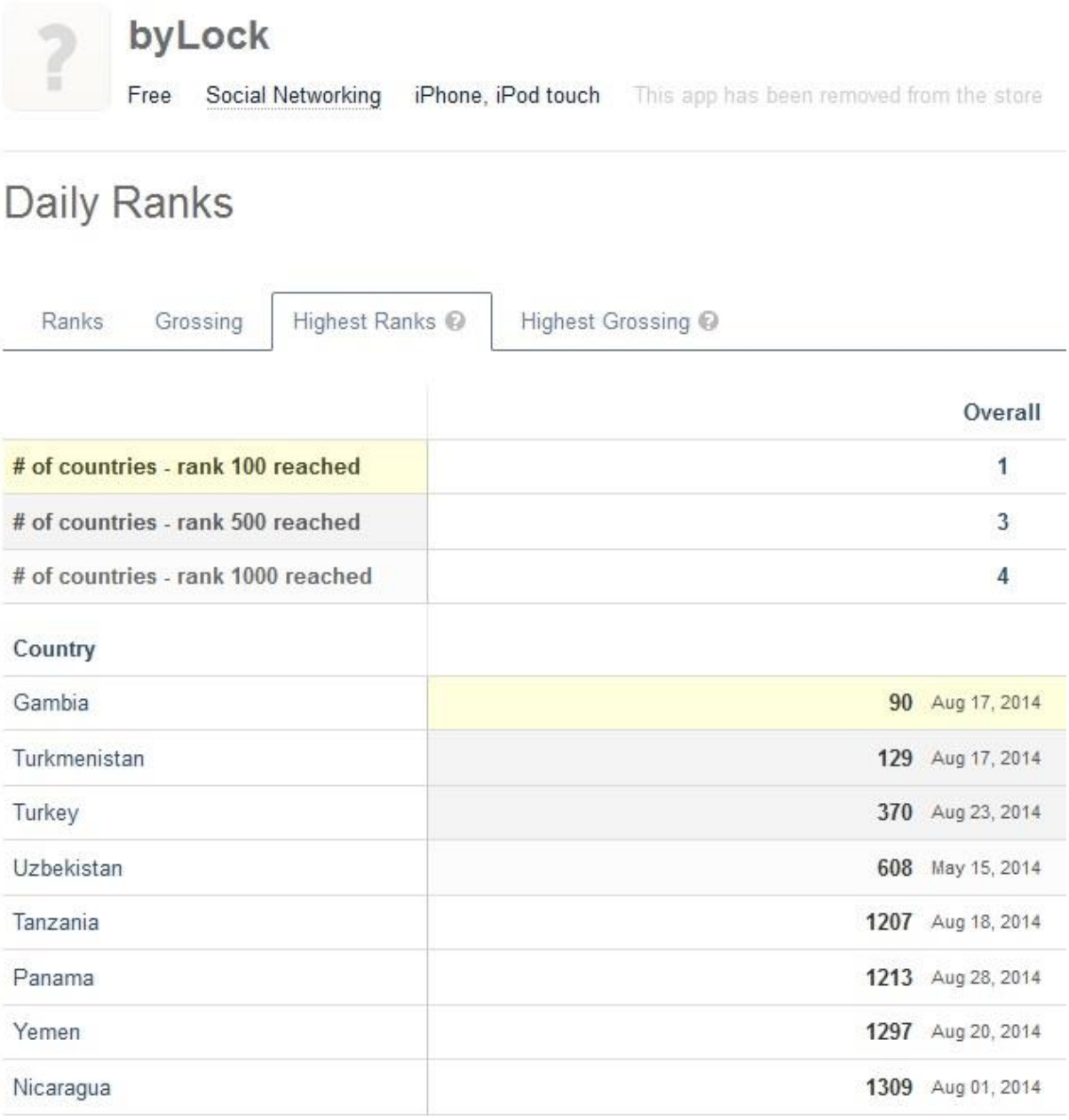


Figure 6: Google Trends search interest for the search term "bylock" in Turkey in the period similar to the MIT research.

The MIT also stated that the ByLock application was not known outside of Turkey before the coup attempt on 15 July 2016. However, according to the website AppAnnie[10], the ByLock application was on 17 August 2014 ranked in the top 100 in Gambia, ranked in the top 500 in August 2014 in Turkmenistan, Turkey and in May 2014 in Uzbekistan. In four other countries the ByLock application was ranked in the top 1000 in August 2014.



byLock

Free Social Networking iPhone, iPod touch This app has been removed from the store

Daily Ranks

Ranks | Grossing | Highest Ranks | Highest Grossing

	Overall
# of countries - rank 100 reached	1
# of countries - rank 500 reached	3
# of countries - rank 1000 reached	4
Country	
Gambia	90 Aug 17, 2014
Turkmenistan	129 Aug 17, 2014
Turkey	370 Aug 23, 2014
Uzbekistan	608 May 15, 2014
Tanzania	1207 Aug 18, 2014
Panama	1213 Aug 28, 2014
Yemen	1297 Aug 20, 2014
Nicaragua	1309 Aug 01, 2014

Figure 7: Rank statistics on AppAnnie for the ByLock application.

[10] https://www.appannie.com/apps/ios/app/bylock/app-ranking/?type=best-ranks&date=2014-09-07

3. Aim at security and anonymity. Fox-IT finds it likely that the developer had a focus on creating a secure communication application allowing anonymous use of the application. In a world where privacy is of high importance, Fox-IT is of the opinion that the ByLock application's anonymity is not with intended use for suspicious activities. For example, the Tor project[11] is a well-known anonymity browser that improve privacy and security on the internet. Journalists uses Tor and also the U.S. Navy for surveilling websites without leaving government IP addresses.

4. Self-signed certificate. It is unclear whether the MIT author is referring to SSL certificates on the ByLock servers (for HTTPS) or SSL certificates on the application. In both cases, the SSL signing party does not impact the 'flow of information' as the MIT author states it. In case of HTTPS certificates, having an authority sign the certificate does not give the authority access to the data, since the private key is not shared with the authority.

Fox-IT finds it unlikely that the self-signed certificate was implemented by the developer to prevent data flowing to servers other than its own. In general, self-signed certificates are easier to implement and are free of cost. It is possible that this was an incentive for the developer to use self-signed certificates.

5. Communication only in a way suitable to the cell structure. The term cell structure is undefined and ambiguous in this context. Fox-IT assumes here that it refers to the way the alleged FTÖ/PDY is organized. Organizational structures are outside the expertise of Fox-IT.

With respect to the registration procedure, it is relevant to nuance the requirement to meet face-to-face or by intermediary to exchange login details. The author fails to identify a third, more likely scenario to exchange ByLock details out of band: use of another communication application (e.g. WhatsApp, Facebook, Skype). Assuming 2 individuals are in contact by WhatsApp (the MIT author does not seem to scrutinize how two individuals meet on WhatsApp), they could exchange their ByLock details and then switch to communication by ByLock.

6. Organizational communication needs. This is outside the expertise of Fox-IT.

7. Prevent access in case of legal confiscation. Fox-IT is of the opinion that insufficient knowledge of the developers intention is available to agree or disagree with the MIT report on this argument. Following, Fox-IT is of the opinion that MIT is jumping to conclusions on the intent of the developer based on the observations stated in the report, unless more information is available to MIT corroborating their conclusion. Automatic deletion of message is also used in popular social media applications like SnapChat.

8. Identity hiding. Fox-IT is of opinion that users do not explicitly hide their identity by creating long passwords, manually download the application from APK websites, use another name as user ID during sign up. The application does not enforce the use of a real identity and therefore in light of privacy users doesn't want to reveal their real identity. This is not in relation to suspicious activity.

9. ByLock used during coup attempt. Fox-IT is unable to verify the statement that ByLock was used by the alleged FTÖ/PDY during the coup attempt in July 2016. However, in any case, this argument is invalid since it is victim to the base-rate fallacy in statistics[12]. This is best explained by example:

Based on this, Fox-IT is of opinion that no true findings are reported by the MIT that founds their allegation that ByLock had been used as an inter-organizational communication medium by the member of the alleged FTÖ/PDY.

5.3.3 How does the ByLock application relate to other similar chat applications available with respect to security?

In this paragraph, Fox-IT will elaborate on the difference between the ByLock application and other communication applications. The goal of this investigation is to question the purpose of ByLock as suggested by MIT, that it is used for communication between only members of the alleged FTO/PDY. These allegations are partly founded on the security features of the ByLock application.

[11] https://www.torproject.org/

[12] https://en.wikipedia.org/wiki/Base_rate_fallacy

Fox-IT will compare ByLock with:

- instant messaging apps with similar amount of users

- platform with similar purpose like the TOR network

- popular instant messaging apps like Whatsapp and Telegram

In this comparison, the typical users groups of these apps are described and its (security) features.

5.3.4 Conclusions

5.4 Are there any other issues identified by Fox-IT which are relevant to the ByLock investigation?

5.4.1 Notable Inconsistencies

Figure 5 in Section 3.6.2.4 (screenshot of SQL output) and Figure 15 in section 3.6.2.15 (another screenshot) are remarkable. The output of an SQL query is shown, showing the rows and a total number of rows returned. The total number of rows does not match the depicted rows. Also, there is a subtle spacing difference in the rows. This suggest manipulation of the screenshot.

Also in section 3.6.2.15 MIT describes

> Examples of decrypted data stored in the user table are shown below: ("Username" indicates the user name / code for the information, and "plain" indicates the user password decrypted on the basis of the work done.)

The above suggests that the column "plain" was added to the user table by MIT for analysis. It is no longer clear which of the information in the report is from the original data and which information is manipulated by MIT (and also to which end). When presenting information as evidence, transparency is crucial in differentiating between original data (the actual evidence) and data added or modified by the analyst.

5.4.2 Phone investigation

Fox-IT investigated the source codes of the ByLock application on what information is stored on the device. In this scenario, MIT should have confiscated the actual phone to perform investigation on the activity of the user. However, it has been found that the logging methods are empty and does not log identifiable information (like userid). On the Android OS events are logged of the starting and stopping of an application and also getting and losing focus of the application.

6 Documents Reviewed

Legal documents reviewed by the expert	FIXME: identificatie document?
Other documents	FIXME Translated by sworn translator for the English language, Jannie Johanna van Ravensteijn-Prins.
Document not reviewed by expert	None

7 APPENDIX

7.1 ByLock certificates

ByLock 1.1.7

```
santoku@santoku-virtual-machine:~/Desktop$ unzip -p
net.client.by.lock-1.1.7-17_APKdot.com.apk META-INF/BYLOCK.RSA
| keytool -printcert

Owner: CN=David Keynes, OU=Application CA, O=by Lock,
L=Beaverton, ST=Oregon, C=US

Issuer: CN=David Keynes, OU=Application CA, O=by Lock,
L=Beaverton, ST=Oregon, C=US

Serial number: 53329ac2

Valid from: Wed Mar 26 10:15:46 CET 2014 until: Sun Aug 11
11:15:46 CEST 2041

Certificate fingerprints:

   MD5:  97:6C:34:23:EB:05:53:1A:A4:90:FF:CD:22:4A:28:82

   SHA1:
C8:57:8B:48:2F:69:AA:0C:1F:17:09:FB:81:5B:64:66:EA:41:BC:96

   SHA256:
D7:35:64:9C:2E:87:90:01:FF:20:B5:84:63:9B:10:12:E7:2C:01:B0:7D
:C7:E1:E6:2A:0F:EE:6B:DA:31:82:B1

Signature algorithm name: SHA1withRSA

Version: 3
```

ByLock 1.1.6

```
santoku@santoku-virtual-machine:~/Desktop$ unzip -p ByLock-
Secure-Chat-amp-Talk.1.1.6.apk META-INF/CERT.RSA | keytool -
printcert

Owner: CN=David Keynes, OU=Application CA, O=by Lock,
L=Beaverton, ST=Oregon, C=US

Issuer: CN=David Keynes, OU=Application CA, O=by Lock,
L=Beaverton, ST=Oregon, C=US

Serial number: 53329ac2

Valid from: Wed Mar 26 10:15:46 CET 2014 until: Sun Aug 11
11:15:46 CEST 2041

Certificate fingerprints:

 MD5:  97:6C:34:23:EB:05:53:1A:A4:90:FF:CD:22:4A:28:82

 SHA1:
C8:57:8B:48:2F:69:AA:0C:1F:17:09:FB:81:5B:64:66:EA:41:BC:96
```

```
 SHA256:
D7:35:64:9C:2E:87:90:01:FF:20:B5:84:63:9B:10:12:E7:2C:01:B0:7D
:C7:E1:E6:2A:0F:EE:6B:DA:31:82:B1

 Signature algorithm name: SHA1withRSA

 Version: 3
```

7.2 ByLock.net timeline

Table 1: Bylock.net timeline.

Date	Event	Source
12-3-2014 21:10 – 14-3-2014 21:30	Between these dates, it was observed that ByLock.net resolved to IP address 184.168.221.39 hosted by godaddy.com	RiskIQ - PassiveTotal
18-3-2014	At this date, it was observed that ByLock.net resolved to IP address 184.168.221.39.	DomainTools
31-3-2014	At this date, it was observed that ByLock.net resolved to IP 184.168.221.39 was changed to IP 69.64.56.133	DomainTools
29-4-2014 19:39 – 10-8-2014 16:53	Between these dates, it was observed that IP 69.64.56.133 was hosted by server4you-inc.	RiskIQ – PassiveTotal
4-8-2014	At this date, it was observed that ByLock.net was last resolved to 69.64.56.133	ViewDNS
10-8-2014 17:01 – 12-3-2016 20:47	Between these dates, it was observed that IP 46.166.160.137 was hosted by uab-cherry-servers	RiskIQ – PassiveTotal
14-8-2014	At this date, it was observed that the ByLock.net hosted on IP 69.64.56.133 was changed to 46.166.160.137	DomainTools
19-2-2016	At this date, the last activity was observed for 46.166.160.137	VirusTotal
15-3-2016	On this date, IP 46.166.160.137 was last resolved on this date, located in Republic of Lithuania, owned by Dedicated servers	ViewDNS
30-3-2016 08:12 – 21-4-2016 09:32	Between these dates, it was observed that IP 184.168.221.72 was hosted by godaddy.com	RiskIQ – PassiveTotal
2-4-2016	At this date, it was observed that ByLock.net resolved to IP 46.166.160.137 was changed to IP 184.168.221.72	DomainTools
19-4-2016	ByLock.net hosted on IP 184.168.221.72 was last seen on this date, located in Scottsdale - United States, hosted by GoDaddy.com, LLC	ViewDNS
4-5-2016	At this date, it was observed that the IP address 184.168.221.72 was not resolvable	DomainTools

10-8-2016 07:56 – 10-8-2016 11:20	Between these dates, the IP 217.70.184.38 was hosted by gandi-sas	RiskIQ – PassiveTotal
11-8-2016	At this date, it was observed that ByLock.net is resolved to a new IP-address: 217.70.184.38	DomainTools
12-8-2016	At this date, it was observed that ByLock.net resolved to IP 217.70.184.38 was changed to IP 104.27.169.137	DomainTools
13-8-2016 21:30 – 2-8-2017 07:31	Between these dates, it was observed that IP 104.27.169.137 was hosted by cloudflare	RiskIQ – PassiveTotal
24-8-2016	At this date, it was observed that ByLock.net resolved to IP 104.27.169.137 was changed to IP 104.27.168.137	DomainTools
13-10-2016 20:58 – 2-8-2017 07:31	Between these dates, IP 104.27.168.137 was hosted by cloudflare	RiskIQ – PassiveTotal
1-8-2017	ByLock.net hosted on IP 104.27.168.137 was last seen on this date, located in San Francisco - United States, hosted by Cloudflare, Inc.	ViewDNS
1-8-2017	ByLock.net hosted on IP 104.27.169.137 was last seen on this date, located in San Francisco - United States, owned by Cloudflare, Inc.	ViewDNS