Summary-Report ECCHR Plausibility Check 03.2018

Cure53, Berlin

Index

Introduction

This report documents the findings of a security assignment centered on verifying the plausibility of a document provided to Cure53 by ECCHR. Carried out in late March of 2018 and enriched by additional revisions in late April of the same year, this plausibility check answers both general and specific questions on the technical feasibility and likelihood of certain claims made in the provided documents and the included commentary.

In terms of the resources and personnel, this ECCHR-commissioned project was executed by two members of the Cure53 team. A total of 1.5 days constituted a time budget invested by Cure53 and the work was divided into various project tasks, encompassing the analysis of both the original and the revised documents, as well as the write-up process for this report, which ultimately delivers the key plausibility check results.

The main objective of the assessment was to find out whether the information contained in the documents handed over to Cure53 by the ECCHR team should be seen as plausible and probable from a technical angle. The overarching and broader aim was to gauge the usability of the claims in a possible scenario of a court case. In other words, ECCHR sought to gather expert opinions about the claims holding up to scrutiny during potential legal proceedings.

The scope of the project consequently revolved around the document analyzing the results of specific malware, allegedly used by a government-level actor. The authors of the document aimed to prove that the investigated malware product was part of the FinFisher family and has been knowingly employed by a governmental entity against its citizens.

The project initially proceeded on schedule with Cure53 receiving access to the target-document in late March 2018. The file in question was shared with the testing team as an MS Word document. After reading the initial document and having found too many questions unanswered and several aspects covered in a rather vague fashion, Cure53 created a response that called for clarifications. The resulting information and a set of queries about the contents of the document were then relayed to the authors by the ECCHR contact person. Over few weeks the questions were processed and a revised version of the document was prepared. In late April 2018, Cure53 received the new version for further review.

In the following sections, this report elaborates on the scope and then zooms in on the results of the plausibility check performed by Cure53. The results are based primarily on the revised document and a set of eleven enumerated claims. These have been analyzed from a technical security standpoint with reference to plausibility, feasibility and likelihood. Foreshadowing the conclusions, it can be stated that nine out of eleven items were verified and flagged as plausible. The issue of plausibility could not be determined for the remaining two claims with sufficient strength of conviction. Therefore, two items were given an “unclear” status.

Scope of Investigation

- **ECCHR-Shared Malware Analysis Report**
    - Original document was analyzed by Cure53 in late March 2018
    - Revision document was analyzed by Cure53 in late April 2018

Verified Claims

The following section sheds light on the results obtained in regard to the claims made in the reviewed document. Each item was verified by Cure53 and hence used as the foundation for the final verdict on whether the overall information contained in the document is plausible. As a reminder, the benchmark was set high as it was assumed that evidence behind the verdict would need to hold up to an even more thorough investigation in a court of law. For reference, the claims are numbered and presented in an orderly fashion from C1 to C9.

C1: Several social media accounts promote *adaleticinyuru.com*

The analyzed document lists several Twitter and Facebook social media accounts that share and promote the URL of the *adaleticinyuru.com* website. These accounts include the link in Twitter messages or a direct link to a website in the profile data. They encourage targeted users to visit the site located at *adaleticinyuru.com*. It is therefore confirmed that the analyzed document claim about the promotion of the domain *adaleticinyuru.com* holds from a technical stance.

C2: Social media accounts target protesters

The Twitter messages that promote the *adaleticinyuru.com* website include prominent hashtags which are affiliated with the protest or respond to other tweets affiliated with the protest. It is therefore fair to assume that the malware indeed specifically targeted protesters. There is a high likelihood that this targeting process was intentional.

C3: Repurposing accounts from previous campaigns

Several social media accounts promoting *adaleticinyuru.com* and the protest have been engaged in different campaigns previously. It was shown that Twitter accounts created long before the protest march originally tweeted about starkly different topics. At some later points in time, these accounts suddenly started to promote the *adaleticinyuru.com* domain. It is therefore fair to assume that the accounts in question are generally being used in social media operations and were repurposed for the promotion of this particular campaign.

C4: Coordinated Use of Twitter Accounts

Several Twitter accounts tweeted the exact same messages, promoted the same tweets or used very similar text snippets. It is therefore fair to assume and claim that these accounts are being controlled by a central instance. In other words, they are not believed not to be used by real individuals.

C5: Domain *adaleticinyuru.com* hosts Android malware

The promoted *adaleticinyuru.com* website hosts an Android application file and encourages visitors to download and install the application. Notably, the application file is to be downloaded directly rather than being distributed through the official Google Play store. This is concerning as it otherwise uses the Google Play store's logo and it can be inferred that the probable goal here is to deceive visitors.

Upon installation and execution, the application exhibits odd behavior, for instance attempting to hide itself. Moreover, it does not offer any apparent functionality to a user. Upon further analysis, it is clear that the application shares many behavioral traits with a typical malware item. It is therefore accurate to assume that the website was intentionally set up to spread this Android malware.

C6: The *adaleticinyuru.com* domain reachable via an IP in the OVH Brand Network

While the website attempts to conceal its true origin by using CloudFlare services, it remains reachable via an IP that belongs to the OVH Brand Network, namely an address at *178.32.214.175*.

As described correctly in the analyzed document, this can be verified by a HTTP request with the use of the *Host* header set to *adaleticinyuru.com*. The IP in question is also shared by several other Turkish websites. As a result, an assumption that the website is hosted on the network of a shared hosting provider targeting the Turkish market can be verified.

C7: Existing similarities to FinFisher malware

The analyzed documents lists similarities that the malware item under investigation allegedly has to the previously identified FinFisher malware. When compared with the malware from *adaleticinyuru.com*, certain items are argued as similar. The following item demonstrated the verified similarity between the Android application shared on *adaleticinyuru.com* and the malware item identified as FinFisher in the past:

- *tmp460 .dat* used as filename pattern for the recorded phone calls.

There were also several decompiled excerpts from the malware, highlighting different malware functionalities.

- *GeofenceTransitionsIntentService*
- *buildWhatsAppFileMetaInfo*
- Accessing *data/data/com.facebook.orca/databases/threads_db2*
- Accessing */data/data/org.telegram.messenger/files/cache4.db*
- Accessing */sdcard/WhatsApp/Media/WhatsApp Audio/*
- Accessing */sdcard/WhatsApp/Media/WhatsApp Video/*
- Accessing */sdcard/WhatsApp/Media/WhatsApp Documents/*
- Observing intents about *com.viber.voip* and *com.whatsap*
- Handling *SmsMessage*

While not all claims could be verified due to the absence of technical documentation and lack of access to samples of the other malware samples within the comparative framework, the claim that the documented malware resembles the FinFisher software is reasonable.

C8: Utilized network communication protocol

The analyzed document shows code extracted from the Android malware and this code is said to be implementing network encryption features. It should be clarified that the variable names shown in the excerpt, such as "*TrojanID*", are interpretations made by an analyst and have not been included in the sample.

Example from the Report:

- `shaDigestInstance.update(TrojanUID);`

Original Values:

- `v0.update(arg7);`

Having acknowledged that, the interpretation of these names match the implemented functionality. Consequently, the description of the protocol can therefore be seen as accurate.

C9: Similarities with the FinFisher Malware Report by Sophos (Part 1)

The Adalat sample and previous FinFisher-related malware share similarities with reference to the command-and-control (C&C) network protocol. The Sophos report referenced in the analyzed document provides data on the FinFisher malware sample which shares many similarities with the analyzed sample. For example, the constants for *Master Command* and *Master Config* values used for the *"onReceive SMS"* functionality are exactly the same constants in both the Adalat sample and in the Sophos report. Furthermore, the general C&C message format using the known separator '/' is the same for both items. This is further evidence that the malware sample is in fact FinFisher or a very similar product.

Unverified Claims

Listed below are the two claims made in the document that Cure53 could not verify, As can be seen, the number of the claims with unclear status is significantly lower than the number of claims that were verifiable. The latter is believed to indicate the high quality of the analyzed document.

C10: Similarities with the FinFisher Malware Report by Sophos (Part 2)

The analyzed document shares the *SHA256* hash of the analyzed Android malware. This ensures that the verification by Cure53 can be done on the same sample.

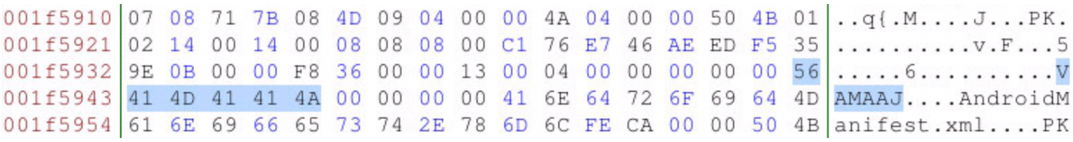
SHA256 hash of the malware sample:

```
c2ce202e6e08c41e8f7a0b15e7d0781704e17f8ed52d1b2ad7212ac29926436e
```

What follows after that is an overview of technical claims that could not be verified in reasonable time. Specifically, the analyzed document states:

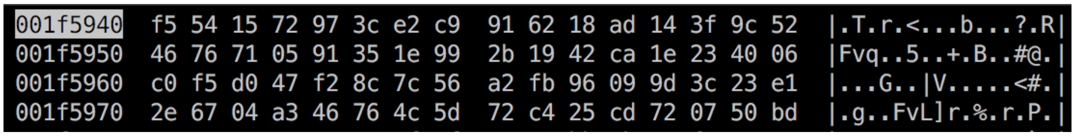
> *"For instance, the samples examined here contain the configuration attributes RemovalAtDate and RemovalIfNoProxy, and Geofencing, which were described as "non-traditional malware properties" by Sophos in the company's 2015 analysis of FinSpy. [...] The configuration of FinSpy is steganographically encoded in the APK using free fields in the ZIP file format"*

The document also shows a hexdump (Fig. 1) of the sample but it is not clear which file is exactly shown. The application file itself (Fig. 2) does not resemble the screenshot provided in the document.



```
001f5910 07 08 71 7B 08 4D 09 04 00 00 4A 04 00 00 50 4B 01 ..q{.M....J...PK.
001f5921 02 14 00 14 00 08 08 08 00 C1 76 E7 46 AE ED F5 35 ..........v.F...5
001f5932 9E 0B 00 00 F8 36 00 00 13 00 04 00 00 00 00 00 56 .....6..........V
001f5943 41 4D 41 41 4A 00 00 00 00 41 6E 64 72 6F 69 64 4D AMAAJ....AndroidM
001f5954 61 6E 69 66 65 73 74 2E 78 6D 6C FE CA 00 00 50 4B anifest.xml....PK
```

Fig. 1: Hexdump from Report



```
001f5940  f5 54 15 72 97 3c e2 c9  91 62 18 ad 14 3f 9c 52  |.T.r.<...b...?.R|
001f5950  46 76 71 05 91 35 1e 99  2b 19 42 ca 1e 23 40 06  |Fvq..5..+.B..#@.|
001f5960  c0 f5 d0 47 f2 8c 7c 56  a2 fb 96 09 9d 3c 23 e1  |...G..|V.....<#.|
001f5970  2e 67 04 a3 46 76 4c 5d  72 c4 25 cd 72 07 50 bd  |.g..FvL]r.%.r.P.|
```

Fig. 2: APK Hexdump from Malware Sample

There were also other items for which the claims made in the document could not be verified. These were the following:

- Several hundreds of zero-byte files are not included in the *.apk*
- Thus, no configuration attributes (such as *RemovalAtDate* and *RemovalIfNoProxy*) could be identified.
- *Fig. 1* shown in the report does not resemble the sample Cure53 had access to, with the latter displayed on *Fig. 2*.
- No reference to the assets */artdump*, *s1cr33nshot* or *chaud/** could be found.

The technical details of these claims were not sufficient from a technical perspective. Therefore, it was impossible to verify them in a given timeframe.

C11: satgas.net linked to SATGAS Task Force

The analyzed report takes a broader look at other, seemingly related malware samples and campaigns. A suggestion is made that the *satgas.net* domain is tied to the Indonesian Task Force on Counterterrorism and Transnational Crimes (SATGAS). Because anybody can register any domain name and no additional evidence to support this claim has been presented, this claimed connection could not be verified.

Review Verdict

As already noted in the *Introduction* section, Cure53 managed to positively verify nine out of eleven specific claims made by the investigated document. After examining the original and revised documents in spring of 2018, the Cure53 team believes the majority of the claims contained in the documents to be plausible.

To give some context, the key points presented in the documents provided to Cure53 for analysis by ECCHR revolved around the use of social media accounts as means to advertise a website to political activists. The analyzed document argued that the website enticed visitors to install an Android application which was, in turn, believed to be the FinFisher malware. The studied document takes a broader perspective when looking at related malware samples and how they were being used across different political situations.

Cure53 concludes that nearly all evidence presented in the document could be verified. However, some of the technical analyses of the malware could not be reproduced due to the missing detailed documentation and lack of access to samples. Nevertheless, the analyzed malware shares technical similarities with the previously reported and discussed FinFisher malware. Importantly, the malware spread among the Turkish protesters did not attempt to hide or obfuscate the malicious code. It is also very much unclear whether its aim was to gather incriminating evidence against the protesters, or if it was purposefully spread overtly to only threaten activists.

Some broader and crucial points related to the campaign in Turkey could be verified. In particular, the evidence shows that political activists have been targeted by a social media campaign which was evidently spreading malware. At the same time, the conclusion found in the examined document which stated that repressive regimes were actively engaged in crushing dissent and were behind the examined campaigns, could not be verified. From the collected factual evidence and the verifiable claims made in the examined document, the latter is still considered a plausible deduction. In conclusion, the document furnished to Cure53 by ECCHR passed the plausibility check.

Cure53 would like to thank ECCHR for their excellent project coordination, support and assistance, both before and during this assignment.