A brief note on "Exonerating Morocco disproving the spyware"

Technical Report · March 2023

CITATIONS
0

READS
4

1 author:

Łukasz Siewierski

2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

A brief note on *Exonerating Morocco disproving the spyware*

Łukasz Siewierski

Abstract
Jonathan Scott has published an opinion piece called ”Exonerating Morocco disproving the spyware” in which he is making three claims without giving any proper evidence. This note shows the logical problems with the arguments he is presenting and how they are used to create disinformation.

Introduction

While on vacation I have found myself in a situation in which the laundry was running (for details of the equipment used see figure 1) and I was making breakfast.

Figure 1. Equipment used in preparation for this note

These two tasks do not require significant cognitive abilities, therefore, out of a lack of mental stimulation I have decided to open the Twitter[1] website. As I have opened it I have noticed that there is a button made specifically for expressing my thoughts. As such I have decided to express my thoughts regarding Jonathan Scott’s (known on Twitter as `@jonathandata1`) opinion piece titled ”Exonerating Morocco disproving the spyware”[1] and debunk all the claims he makes there. Afterwards I have decided to publish the debunking tweets here in a form of a brief, but highly technical note.

[1]This website can be found at https://www.twitter.com

1. Arguments

Jonathan’s oped is making three somewhat technical arguments, which is quite unusual for an opinion piece [1]. These are:

1. IP address cannot be reliably mapped to a country.
2. There is a false positive IoC in the attack timeline.
3. Backup can be tampered with before it is run through MVT.

I will debunk each of these arguments in the next sections.

2. IP to country mapping

Jonathan’s oped cites court cases which say that an IP address cannot be mapped to a person (not a country) and concludes that an IP address cannot be mapped to a country (not a person). This of course is a severe logical error in his opinion piece. The claim actually made by Citizen Lab (see figure 2) is that the IP address belongs to a specific Autonomous System (AS). This is different than geographical IP designation Jonathan references. This is a mapping to a country, not a person.

The IP from which the targeting message was uploaded (41.137.57.198) is from a Moroccan range dedicated to mobile 3G Internet users in the capital Rabat and its surroundings:

```
inetnum: 41.137.56.0 – 41.137.57.255
netname: INWI-PDSN1-Rabat001
country: MA
admin-c: AN2-AFRINIC
tech-c: AN2-AFRINIC
```

Figure 2. Excerpt from Citizen Lab’s report

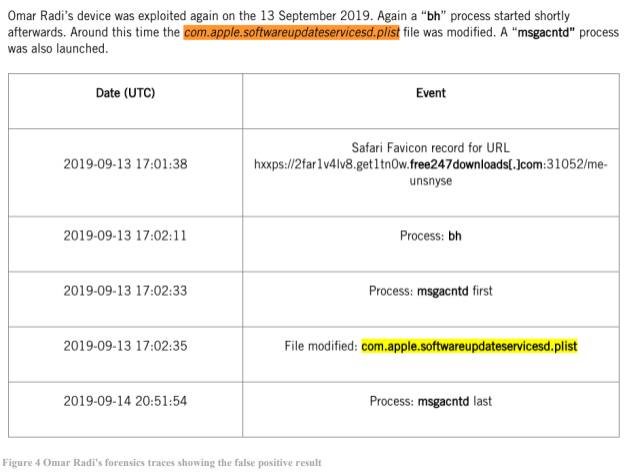
If Jonathan believes the AS referenced here is wrongly defined he should show a proof of that fact and notify IANA[2].

[2]IANA is the organisation responsible for the assignment of the IP address pools

However, since it is only an opinion and not a fact Jonathan did not show any proof.

3. False Positive IoC

Figure 3 is the timeline that Jonathan himself cites in the writeup. He says that the highlighted indicator of compromise (IoC) is a false positive. I am not sure it is true, but let me be generous and assume it is. Perform the following experiment: cover the highlighted indicator of compromise with a piece of paper and decide if this still looks like a Pegasus infection. To me it does[3] and I am speaking from years of professional experience.



Omar Radi's device was exploited again on the 13 September 2019. Again a "**bh**" process started shortly afterwards. Around this time the *com.apple.softwareupdateservicesd.plist* file was modified. A "**msgacntd**" process was also launched.

Date (UTC)	Event
2019-09-13 17:01:38	Safari Favicon record for URL hxxps://2far1v4lv8.get1tn0w.**free247downloads[.]com**:31052/me-unsnyse
2019-09-13 17:02:11	Process: **bh**
2019-09-13 17:02:33	Process: **msgacntd** first
2019-09-13 17:02:35	File modified: com.apple.softwareupdateservicesd.plist
2019-09-14 20:51:54	Process: **msgacntd** last

Figure 4 Omar Radi's forensics traces showing the false positive result

Figure 3. Timeline as presented in Jonathan's oped

4. MVT and evidence tampering

Final claim – that the backup can be tampered with – does not show any proof of the tampering, just the fact that it might be tampered with today (not even at the time of infection). Again, since this is an opinon piece, no actual evidence is being presented. In particular Jonathan fails to address the following questions:

- How did the person who tampered with backup know which IoCs to fake and how to fake them?
- Why did they fake it?
- Is there any proof that the evidence was tampered with?
- Why would an analyst doing manual analysis miss the obvious signs of tempering?

In my previous high quality technical report I have discussed these issues at length [2]. I would encourage reader to refer to that discussion.

[3] I have used an alternative version of this experiment in which I have painted over the claim with a pink glitter. I also did statistical analysis to make sure this variable did not influence the result of the experiment.

A brief note on the brief note

I would like to briefly mention that this PDF is published on ResearchGate. I would like to thank ResearchGate for providing a space for any kind of research, whether it is all the Jonathan opinion pieces used to spread disinformation or this brief note with a picture of a washing machine (see figure 1).

Acknowledgments

I would like to thank the manufactures of washing machines, pots, pans, knives, induction stoves, cutlery and plates, without whom I would not be able to perform activities mentioned in the first section of this brief note.

Peer review status

This highly technical brief note has been peer reviewed anonymously and accepted without corrections.

References

[1] Jonathan Scott. Exonerating morocco exonerating morocco disproving the spyware, 02 2023.

[2] Łukasz Siewierski. Misinformation in malware analysis, 07 2022.