Security

Microsoft can secretly update Raspberry OS

Microsoft repositories included in Raspberry OS update

Filip Pynckels

February 6, 2021

Table of contents

List of figures

Introduction

Raspberry Pi’s have proven to be one of the cheapest ways to create an isolated test network for looking into security issues. During the software update of a test configuration (*Figure 1*) the name Microsoft popped up in the list of the repository servers after doing an update followed immediately by a second update (*Figure 2*)

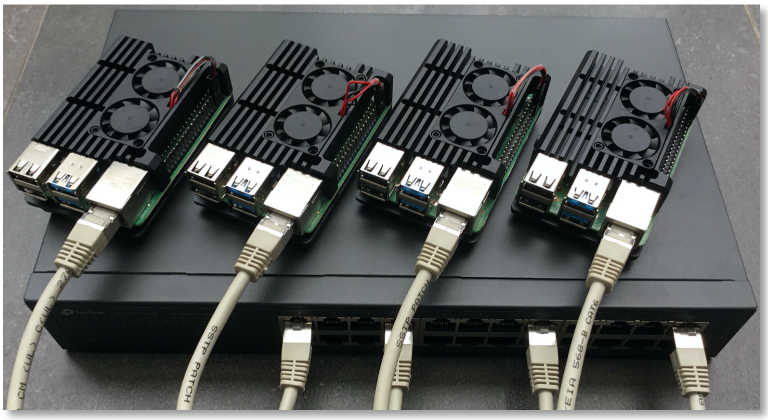
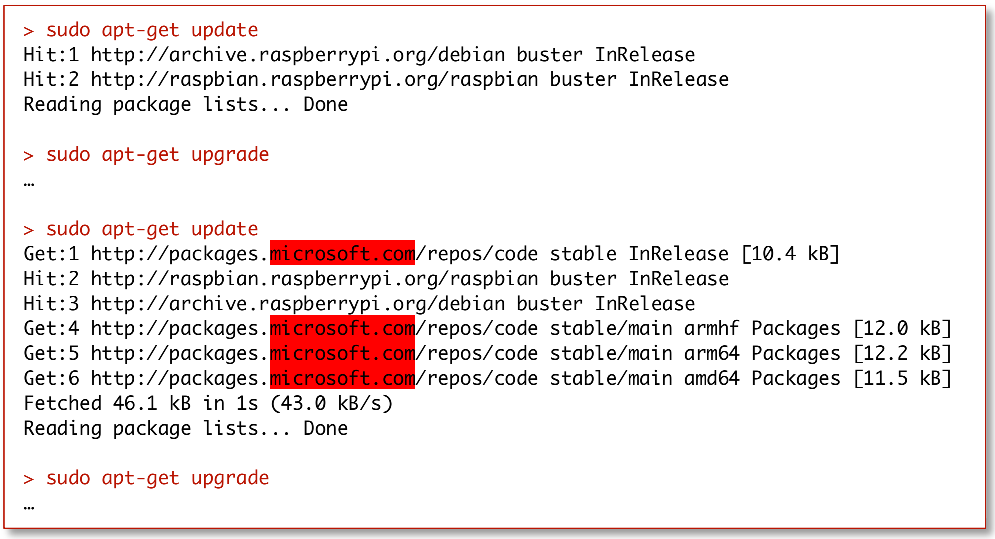


FIGURE 1 - TEST NETWORK

The test configuration is running Raspberry OS (a Debian spin-off). Raspberry OS is maintained by the Raspberry Pi Foundation.



```
> sudo apt-get update
Hit:1 http://archive.raspberrypi.org/debian buster InRelease
Hit:2 http://raspbian.raspberrypi.org/raspbian buster InRelease
Reading package lists... Done

> sudo apt-get upgrade
…

> sudo apt-get update
Get:1 http://packages.microsoft.com/repos/code stable InRelease [10.4 kB]
Hit:2 http://raspbian.raspberrypi.org/raspbian buster InRelease
Hit:3 http://archive.raspberrypi.org/debian buster InRelease
Get:4 http://packages.microsoft.com/repos/code stable/main armhf Packages [12.0 kB]
Get:5 http://packages.microsoft.com/repos/code stable/main arm64 Packages [12.2 kB]
Get:6 http://packages.microsoft.com/repos/code stable/main amd64 Packages [11.5 kB]
Fetched 46.1 kB in 1s (43.0 kB/s)
Reading package lists... Done

> sudo apt-get upgrade
…
```

FIGURE 2 - SURPRISE DURING THE SECOND UPDATE

To my surprise the Microsoft repository was added after the second update without even the slightest warning, question, … from the side of the Raspberry Pi Foundation. Even more to my surprise, the installed version of the OS was the Raspberry Pi OS LITE meaning that one can suppose that only the necessary software and updates are applied, and nothing else. But alas…

This document is the summary of the actions I took, and of my conclusions. All actions were taken on the command line of the machine in question, due to the fact that it is a LITE version without a graphical user interface, and because I’m an old fashioned command line user.

1 The extent of the problem

1.1 Perception

It’s not a secret that Linux users are not keen on surprises in the setup of their machines. Most of them also have a certain discomfort when hearing the name Microsoft. On the one side, Microsoft is known for its unbridled urge to gather all kinds of data, and even if this is not the case here, who can guarantee it?

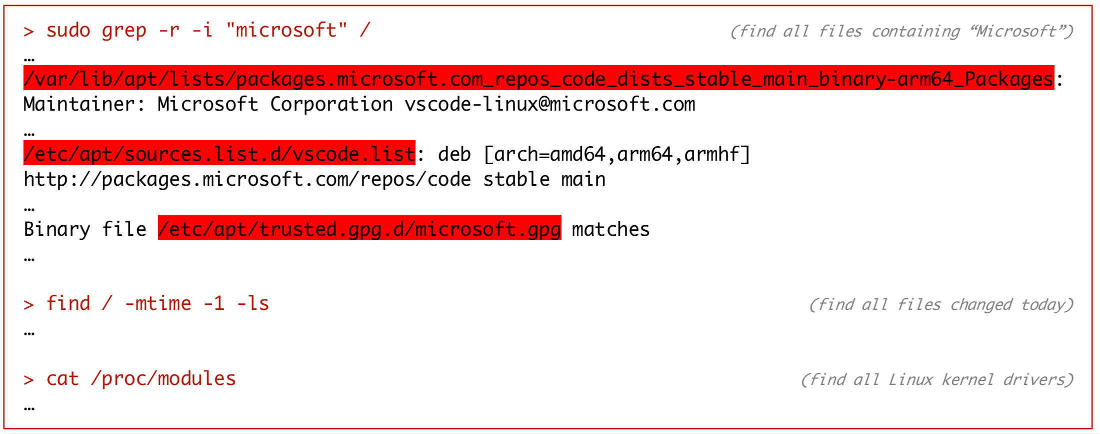
A second element that plays a role is the fact that there is such a thing as the Clarifying Lawful Overseas Use of Data Act. This CLOUD Act (H.R. 4943) asserts that U.S. data and communication companies must provide data stored for a customer or subscriber on any server they own and operate to the US government when requested. In theory there are a number of safeguards that allow the company in question to go to court to reject the question. But we all know the even more unbridled urge of the US government three letter agencies to collect data on everything and everyone.

Linking the attitude of Microsoft with regards to gathering metrics to that of the US government agencies leads to a general conclusion in the free software (read: Linux) community that seeing the name Microsoft during the update of a Linux system is a red flag. I’m not pretending that this specific case is a risk, but which guarantees do the users and administrators of RaspberryOS have with regards to the software surprises they will get during the next update?

To summarize: *even if there is no current danger of data-theft, the Raspberry Pi foundation has created a major perception problem by including unnecessary and even useless (in the case of Raspberry Pi LITE) Microsoft software into their update*.

1.2 Analysis of the “Microsoft” changes

Below, we show the first steps that we took to assess the impact of the “Microsoft” update (*Figure 3*). After each executed command, some of the returned lines are shown. Showing all output would be overkill. The grey text at the end of a command line is not part of the command, but some further information. When only three dots are shown after the command, we have seen nothing fishy.



```
> sudo grep -r -i "microsoft" /                              (find all files containing “Microsoft”)
…
/var/lib/apt/lists/packages.microsoft.com_repos_code_dists_stable_main_binary-arm64_Packages:
Maintainer: Microsoft Corporation vscode-linux@microsoft.com
…
/etc/apt/sources.list.d/vscode.list: deb [arch=amd64,arm64,armhf]
http://packages.microsoft.com/repos/code stable main
…
Binary file /etc/apt/trusted.gpg.d/microsoft.gpg matches
…

> find / -mtime -1 -ls                                               (find all files changed today)
…

> cat /proc/modules                                                 (find all Linux kernel drivers)
…
```

FIGURE 3 - IMPACT ASSESSMENT OF THE UPDATE

The results of *Figure 3* show us that there are four further things to investigate.

- `http://packages.microsoft.com/repos/code`
- `/var/lib/apt/lists/packages.microsoft.com_repos_code_dists_stable_main_binary-arm64_Packages`
- `/etc/apt/sources.list.d/vscode.list`
- `/etc/apt/trusted.gpg.d/microsoft.gpg`

1.2.1 Contents of the Microsoft repository

When digging deeper in the URL `http://packages.microsoft.com/repos/code` we find two interesting pages that lead to the same conclusion:

- `http://packages.microsoft.com/repos/code/dists/stable/main/binary-arm64/`
- `http://packages.microsoft.com/repos/code/pool/main/c/`

The first URL leads to 3 download repositories:

- `code`
- `code-exploration`
- `code-insiders`

The first URL leads to a file with a package list that we can filter:

```
> curl http://packages.microsoft.com/repos/code/dists/stable/main/binary-arm64/Packages |
  grep "Package: " |
  awk  '{print $2}' |
  uniq                                                      (find package names in packet list)

code
code-exploration
code-insiders
```

FIGURE 4 - MICROSOFT PACKAGE CONTENTS

A first conclusion is that *the "Microsoft" package contains Visual Studio Code, which is at least weird, since we are talking about a Raspberry Pi OS LITE that has no graphical user interface, and that is used in most cases as a server/firewall/bridge/router/…*

1.2.2 Contents of the /var/lib/apt/lists repository

```
> ls /var/lib/apt/lists                                            (show directory contents)

…
packages.microsoft.com_repos_code_dists_stable_InRelease
packages.microsoft.com_repos_code_dists_stable_main_binary-amd64_Packages
packages.microsoft.com_repos_code_dists_stable_main_binary-arm64_Packages
packages.microsoft.com_repos_code_dists_stable_main_binary-armhf_Packages
…
```

FIGURE 5 - /VAR/LIB/APT/LISTS DIRECTORY CONTENTS

Looking at the information in the /var directory (*Figure 5*) shows us that *the found files contain MD5SUM, SHA1, SHA256 and SHA512 hashes for several files, and a PGP signature at the bottom* (*Figure 6*)

```
> cat /var/lib/apt/lists/packages.microsoft.com_repos_code_dists_stable_InRelease

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Origin: code stable
Label: code stable
Suite: stable
Codename: stable
Date: Fri, 5 Feb 2021 06:48:53 UTC
Architectures: amd64 arm64 armhf
Components: main
Description: Generated by aptly
MD5Sum:
 0ddedf28ca32535dcf025515b98a8d76   563809 Contents-amd64
 d8dc12722d872c36de79b810b21ba0ee    34294 Contents-amd64.gz
 ee06fa6aa901e5428c11052275598dd3   564025 Contents-arm64
 bd9b6148644d715f74fb61cfd6edfeb5    34308 Contents-arm64.gz
 7f62c0017215f8302f4bfa3e11847604   564160 Contents-armhf
 ccc17f265eae9b39c71f54495fba8096    34317 Contents-armhf.gz
 0ddedf28ca32535dcf025515b98a8d76   563809 main/Contents-amd64
 d8dc12722d872c36de79b810b21ba0ee    34294 main/Contents-amd64.gz
 ee06fa6aa901e5428c11052275598dd3   564025 main/Contents-arm64
 bd9b6148644d715f74fb61cfd6edfeb5    34308 main/Contents-arm64.gz
 7f62c0017215f8302f4bfa3e11847604   564160 main/Contents-armhf
 ccc17f265eae9b39c71f54495fba8096    34317 main/Contents-armhf.gz
 8a172cbb8acbd65f915427bff1f20709    71172 main/binary-amd64/Packages
 f5a64b5b697e341e02dbdfc19f83d5b2    11465 main/binary-amd64/Packages.bz2
 8c78a85c449330d4c671728dc7937a4b    11724 main/binary-amd64/Packages.gz
…
```

FIGURE 6 - /VAR/LIB/APT/LISTS FILE CONTENTS

1.2.3 Contents of vscode.list

```
> cat /etc/apt/sources.list.d/vscode.list                     (show directory contents)

### THIS FILE IS AUTOMATICALLY CONFIGURED ###
# You may comment out this entry, but any other modifications may be lost.
deb [arch=amd64,arm64,armhf] http://packages.microsoft.com/repos/code stable main
```

FIGURE 7 - VSCODE.LIST CONTENTS

1.2.4 Contents of microsoft.gpg

```
> gpg --list-packets /etc/apt/trusted.gpg.d/microsoft.gpg     (show directory contents)

# off=0 ctb=99 tag=6 hlen=3 plen=269
:public key packet:
        version 4, algo 1, created 1446074508, expires 0
        pkey[0]: [2048 bits]
        pkey[1]: [17 bits]
        keyid: EB3E94ADBE1229CF
# off=272 ctb=b4 tag=13 hlen=2 plen=55
:user ID packet: "Microsoft (Release signing) <gpgsecurity@microsoft.com>"
# off=329 ctb=89 tag=2 hlen=3 plen=309
:signature packet: algo 1, keyid EB3E94ADBE1229CF
        version 4, created 1446074508, md5len 0, sigclass 0x13
        digest algo 2, begin of digest 1a 9b
        hashed subpkt 2 len 4 (sig created 2015-10-28)
…
```

FIGURE 8 - MICROSOFT.GPG CONTENTS

1.3 Conclusion

On the side of perception, the Raspberry Pi Foundation has made an error that Linux users will remember for a while. Since perception can even hurt more than facts, it is advisable for the Raspberry Pi Foundation to communicate about this unexpected surprise in their update routines. *Most people are not against Visual Studio Code and it can be used as a versatile development tool, but care should be taken that it doesn't surface in the LITE version anymore, and maybe that it can be installed as the thousands of other packages on all versions of Raspberry Pi OS*. It is far from clear why Microsoft's Visual Studio Code is getting a privileged treatment, even in OS distributions that are only used as servers. There is also the trust element. *Installing unwanted GPG or other software keys on a system is sloppy and undesirable*.

There seems to be no real impact on the system as it was before. For the moment, there are 6 files added to the OS within the context of the aptitude (installation) routines. But *nothing prevents the repositories added to aptitude to pull in other information as yet another surprise for the user or the administrator*. What has been done to the system is similar to the first step of what malware does, which is in fact unacceptable.

However, *there can be an impact in the future because the installed key(s) permit Microsoft to tune future updates of this Linux system to their wishes, including other software that does gather information on this Linux system.* On top of that, every update that is done on this Linux system gives a signal to the Microsoft server. Even this is undesirable. Linux users hate it when they are fooled this way, because contacting the Microsoft server can lead to geolocation, and even more if other people on your local network are logged into a Microsoft service like GitHub, LinkedIn, Office365, …

So, *it seems better to erase the changes made for the Microsoft software and to make sure that no new Microsoft information can be installed in the future*. The first is rather easy, the second is not 100% waterproof but sufficient for our goals.

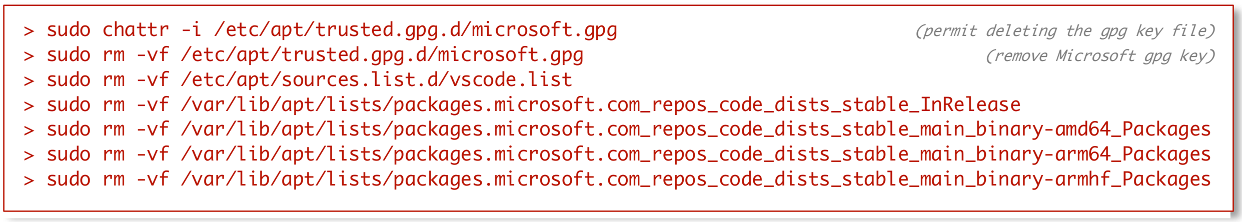
Finally, *it is advised that installation logs of RaspberryOS are investigated by the user or administrator each time an update is done*, to be sure that no further "surprises" emerge.

2 Removing and preventing the “Microsoft” changes

In order to prevent Microsoft tuning of future updates of the RaspberryOS, the actual files have to be removed and future creation of new keys must be made difficult.

Some would advise to stop using RaspberryOS or Raspberry Pi. Although the author is a major fan of Blackarch Linux, it is undeniable that the Raspberry biotope is a versatile and cheap learning and testing tool that even offers possibilities for certain production tasks.

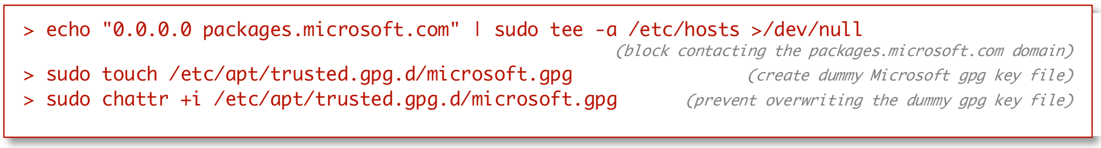
2.1 Removal of the added files



```
> sudo chattr -i /etc/apt/trusted.gpg.d/microsoft.gpg                                   (permit deleting the gpg key file)
> sudo rm -vf /etc/apt/trusted.gpg.d/microsoft.gpg                                           (remove Microsoft gpg key)
> sudo rm -vf /etc/apt/sources.list.d/vscode.list
> sudo rm -vf /var/lib/apt/lists/packages.microsoft.com_repos_code_dists_stable_InRelease
> sudo rm -vf /var/lib/apt/lists/packages.microsoft.com_repos_code_dists_stable_main_binary-amd64_Packages
> sudo rm -vf /var/lib/apt/lists/packages.microsoft.com_repos_code_dists_stable_main_binary-arm64_Packages
> sudo rm -vf /var/lib/apt/lists/packages.microsoft.com_repos_code_dists_stable_main_binary-armhf_Packages
```

FIGURE 9 - REMOVE THE “MICROSOFT” UPDATE

2.2 Prevention of future “Microsoft” updates



```
> echo "0.0.0.0 packages.microsoft.com" | sudo tee -a /etc/hosts >/dev/null
                                                   (block contacting the packages.microsoft.com domain)
> sudo touch /etc/apt/trusted.gpg.d/microsoft.gpg                      (create dummy Microsoft gpg key file)
> sudo chattr +i /etc/apt/trusted.gpg.d/microsoft.gpg       (prevent overwriting the dummy gpg key file)
```

FIGURE 10 - PREVENTING A FUTURE “MICROSOFT” UPDATE

3 General conclusion

From the trust and general perception point of view, the Raspberry Pi Foundation and/or Microsoft have made a big mistake. Creating an update that does about the same as a malware seems not advisable.

Especially on distros that are marked as LITE (no unnecessary software) it seems at least weird to push a software that needs a graphical shell through the troat of the users and/or administrators. This kind of actions make people hate a system that is otherwise not bad (Raspberry Pi), and a company that is already seen by many as the average between "The wolf of Wall Street" and the the lap dog of the US government.

For the moment, there is no real impact on the system (as far as the author could test it). However, to prevent future breaches of the system (RaspberryOS), removal of the "Microsoft" part of the update is advisable, and preventing Microsoft from penetrating the system again seems necessary. Both elements are shown in *Figure 9* and in *Figure 10*.

Looking into each update log will be necessary, since the Raspberry Pi Foundation and/or Microsoft (if they knew that their software would be included in the RPI platform) have shown to be unreliable regarding their commitments to the ideas of the free- and open software world.