Blue Merle: Reducing your cellular footprint

11-13 minutes

2/2/2023

Research by:

Nicholas Farnham, Matthias Marx, Linus Neumann, Dominik Oepen, Laura Pros Segura, Jannes Quer and Folkert Saathoff

Key takeaways

- 4G LTE routers offer users a reliable internet connection when other options are unavailable, but render associated activity and traffic vulnerable to tracking methods used by mobile network operators.
- Users interested in using mobile networks anonymously must change each identifying element associable with 4G LTE routers and linked devices, namely IMSI/IMEI numbers, router BSSIDs, and device MAC addresses.
- The SRLabs research team behind the open-source blue merle project have identified and mitigated remote and local data leakage risks for users of the GL.iNet Mudi 4G LTE router

Using cellular networks anonymously is hard

Mobile network operators use several identifiers to identify their users, making it hard to use cellular networks anonymously. Techniques typically used to avoid tracking, such as changing SIM cards, fail to account for other personal identifiers such as International Mobile Equipment Identity (IMEI) numbers. Device owners looking to use mobile networks anonymously must instead use techniques that change each identifying element of their mobile phones.

SRLabs researchers recently examined the **GL.iNet Mudi (GL-E750) 4G LTE router** as part of our company’s ongoing mobile network security research efforts. The travel router features native privacy-enhancing features such as Tor and user-defined VPN support shielding its user’s associated network traffic. Despite this, our examination of the Mudi 4G LTE router uncovered several unmitigated tracking risks at the Wi-Fi and cellular protocol levels. The Mudi also stores Media Access Control (MAC) addresses of connected devices, which can be used to identify user devices that have previously connected to the travel router.

SRLabs recently released the *blue merle* software package containing fixes our researchers developed to mitigate deanonymization risks uncovered during the investigation of the Mudi 4G LTE router. The *blue merle* project adds additional privacy protections to the Mudi device designed to reduce forensic traces that could be used by mobile network operators to identify its users. The project’s source code and detailed documentation has already been released on our **GitHub**.

This blog post details the most critical privacy risks posed by modern-day device tracking methods used by mobile network operators and the features included within the *blue merle* project designed to mitigate those impacting owners of the Mudi 4G LTE router.

Privacy risk assessment

1/ Tracking of the Mudi's activity, location, and, in some cases, the identification of the purchaser is possible through the IMEI. The simplest method of mobile-network tracking uses the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a subscriber by their SIM card. This tracking method can be mitigated by regularly changing SIM cards. However, the mobile device counterpart to the IMSI, namely its unique IMEI, remains the same across SIM changes. The common notion that changing the SIM card – ideally to an anonymous one – results in a completely new identity is wrong. If a user changes their SIM but continues to use the same device, a connection to their so-called new identity can be drawn through the unchanged IMEI. A device IMEI might even be traceable to a specific purchase, allowing for direct identification of the purchaser.

Figure 1 illustrates how IMSI and IMEI identifiers can be linked if not changed simultaneously**. Only by changing IMEI and IMSI at the same time can the user shake off all traces accumulated by their previous subscriber- and device-based identity.**

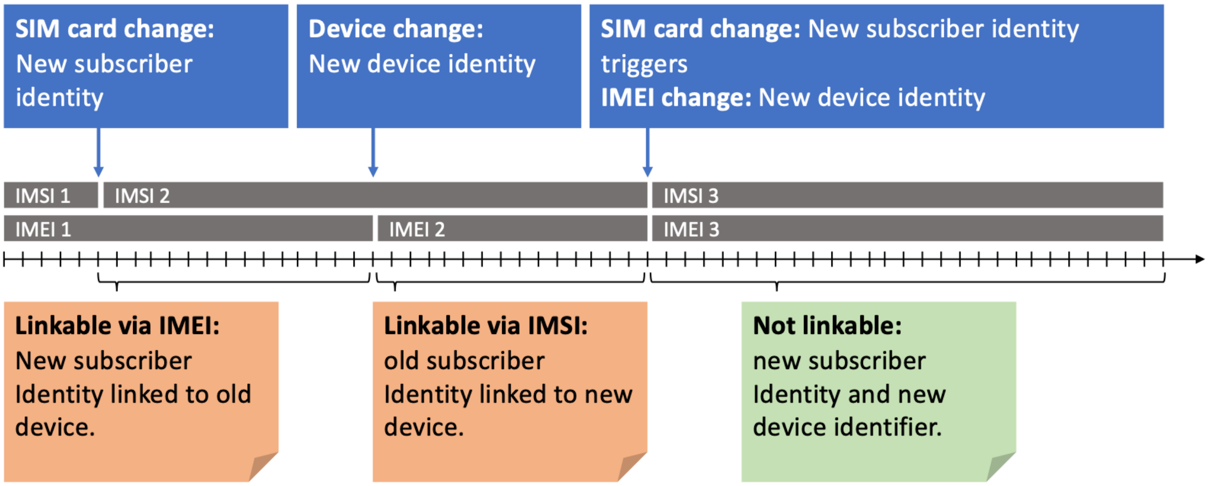

SIM card change: New subscriber identity
Device change: New device identity
SIM card change: New subscriber identity triggers IMEI change: New device identity
IMSI 1
IMSI 2
IMSI 3
IMEI 1
IMEI 2
IMEI 3
Linkable via IMEI: New subscriber Identity linked to old device.
Linkable via IMSI: old subscriber Identity linked to new device.
Not linkable: new subscriber Identity and new device identifier.

Figure 1: Identity linkability across different IMEI and IMSI change scenarios

2/ The BSSID and MAC address allow for activity and Wi-Fi-based location tracking. The Basic Service Set Identifier (BSSID) is associated with a specific WLAN access point and is referenced in all wireless packets associated between the access point and connected clients. By convention, an access point's MAC address is used as the ID of a BSS. BSSIDs are constantly transmitted by both the Mudi device and connected clients when the Mudi is offering a Wi-Fi network. By passively collecting Wifi network identifiers such as BSSIDs, device identifiers – including that of the Mudi router – can be mapped to fixed locations.

Like other mobile routers, the Mudi 4G LTE router records the MAC addresses of connected devices. MAC addresses uniquely identify a device's network adapter and are assigned during the manufacturing process. A connected device's stored MAC address serves as a uniquely identifying element that can be tied to the device user. In case of a device's loss, theft or confiscation, this data collection may prove detrimental to the users' privacy interests. Additionally, the MAC address can be collected by passive intercept as it is not encrypted. Therefore, the unique and static MAC address is in itself a risk for activity and location tracking.

Features of *blue merle* to mitigate tracking risks

SRLabs' open-source software package *blue merle* addresses the privacy limitations of the Mudi router by providing the following features:

1/ IMEI randomization. *Blue merle* enforces an IMEI randomization upon every SIM card change to break the linkage between the subscriber and device identities. The Mudi router's baseband unit is a **Quectel EP06-E/A Series LTE Cat 6 Mini PCIe module**. Its IMEI can be changed by issuing Quectel LTE series-standard AT commands. The AT command to write a new IMEI to a Quectel EP06-E/A-based device is *AT+EGMR*.

Blue merle's IMEI randomization functionality is built around this command and offers two distinct approaches to IMEI generation. The first deterministic method seeds the new value with the user's IMSI, while the second generates a fully random IMEI. To minimize risks associated with an IMEI change, we considered the following:

- Multiple IMEI changes increase the likelihood of alerting an ISP of suspicious behavior. Therefore, the blue merle project team recommends constraining usage of the IMEI randomization option to when the SIM card is changed
- Ideally IMEI randomization occurring when the SIM card is changed would associate a single, randomly generated IMEI to that SIM card. However, this would require the new IMEI to be stored within the device. The *blue merle* package ensures the IMEI is deleted from the router when the SIM card is removed
- To ensure that there is no leakage of the old IMEI after rebooting the device, the radio is turned off in advance. This disrupts the device's connection with the mobile network during the time the IMEI is changed, and the connection is only reestablished after rebooting the device

2/ BSSID and MAC randomization. Since BSSIDs are another case of personally identifiable data, randomizing it serves as a strong privacy measure. The *blue merle* package regularly randomizes the Mudi router's BSSID to eliminate another uniquely identifying artifact. Also, Wi-Fi clients such as mobile phones frequently leak SSIDs – and in some cases BSSIDs – of Wi-Fi connections they have previously connected to. Changing the Mudi router's BSSID eliminates the risk posed by this source of persistent data leakage and subsequent Wi-Fi-based location tracking attempts.

A *blue merle*-modified Mudi router removes links to past activities, whereabouts, and Wi-Fi connections by using a different MAC address on each boot. The Mudi router BSSID is set by the process *hostapd* using the function *mac80211_prepare_vif()* in */rom/lib/netifd/wireless/mac80211.sh*. The resulting BSSID is stored in */etc/config/wireless*. The *blue merle* BSSID randomization function generates a valid unicast address value and overrides the current MAC values set for the *wlan0* and *wlan1* interfaces. This is done by issuing the OpenWrt command *uci set* targeting the *macaddr* fields of *wireless.@wifi-iface[0]* and*wireless.@wifi-iface[1]*. The Mudi router's Wi-Fi is then reset to implement the changes.

The BSSID randomization feature is run on boot, ensuring that a new BSSID is generated each time the device is started.

3/ MAC address log wiper. By wiping the Mudi router's cache of stored MAC addresses at each boot, third parties with remote or physical access can no longer enumerate the devices that have connected to the Mudi router.

MAC addresses of devices that connected to the Mudi's Wi-Fi connection are stored in */tmp/tertf(_bak)*and */etc/tertf(_bak)*. The *blue merle* MAC address log wiper first symbolically links the *gl_tertf* file responsible for the *gltertf* process, which reads and logs MAC addresses. It then kills the *gltertf*process if active, checks if either file contains any data, and uses *shred* to delete any data if found. The MAC address log wiper is run on boot, ensuring that the Mudi device's initial MAC log read/write functionality is disrupted each time the device is started.

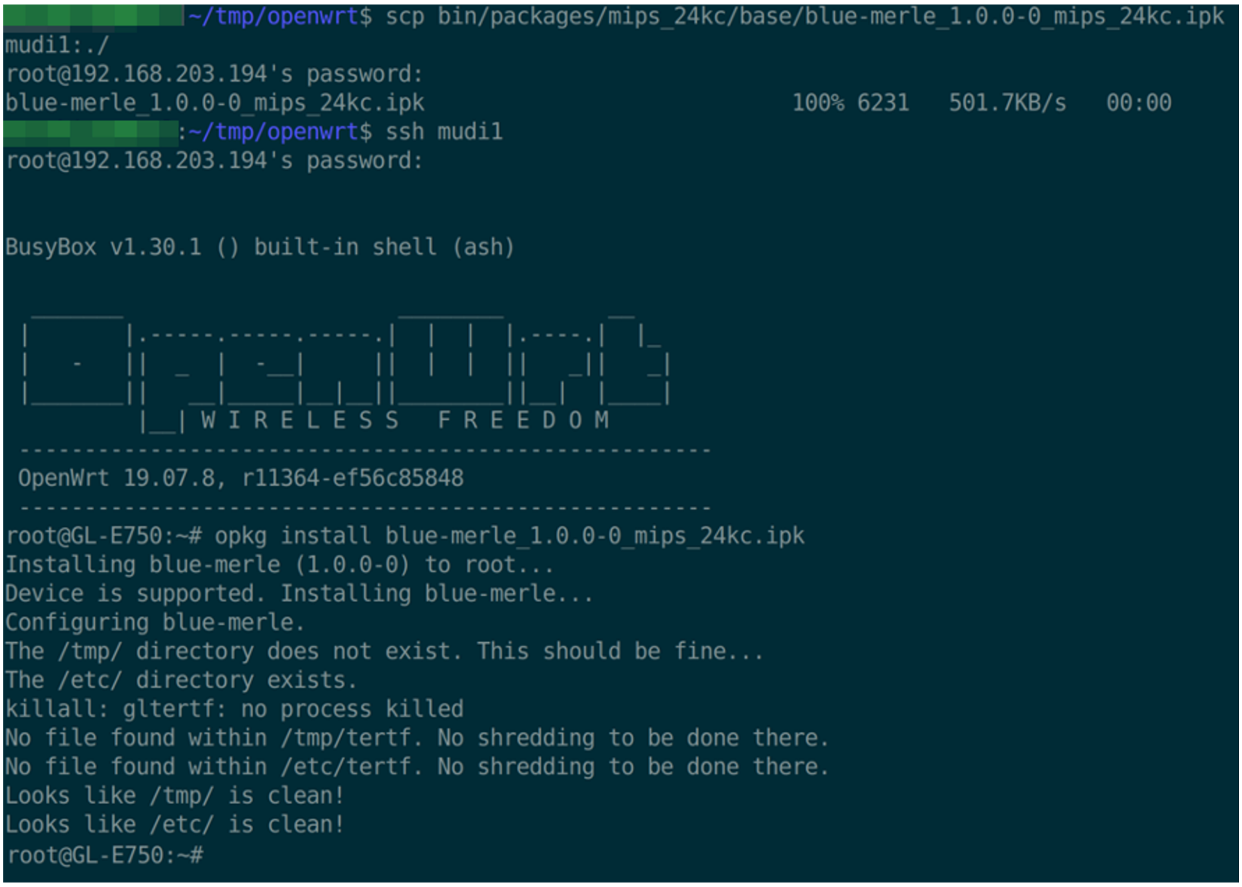
How to install *blue merle*

A few simple steps allow users to use the *blue merle* package on their Mudi router, as exemplified by Figure 2. Note: The *blue merle* project was developed and tested on firmware version 3.215 and might not be compatible with future firmware updates.

1. Update the Mudi router to firmware version 3.215

2. Copy the OPKG file to the Mudi router via scp

3. Install the package: opkg install blue-merle*.ipk



```
[redacted]~/tmp/openwrt$ scp bin/packages/mips_24kc/base/blue-merle_1.0.0-0_mips_24kc.ipk
mudi1:./
root@192.168.203.194's password:
blue-merle_1.0.0-0_mips_24kc.ipk                    100% 6231   501.7KB/s   00:00
[redacted]:~/tmp/openwrt$ ssh mudi1
root@192.168.203.194's password:


BusyBox v1.30.1 () built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 19.07.8, r11364-ef56c85848
 -----------------------------------------------------
root@GL-E750:~# opkg install blue-merle_1.0.0-0_mips_24kc.ipk
Installing blue-merle (1.0.0-0) to root...
Device is supported. Installing blue-merle...
Configuring blue-merle.
The /tmp/ directory does not exist. This should be fine...
The /etc/ directory exists.
killall: gltertf: no process killed
No file found within /tmp/tertf. No shredding to be done there.
No file found within /etc/tertf. No shredding to be done there.
Looks like /tmp/ is clean!
Looks like /etc/ is clean!
root@GL-E750:~#
```

Figure 2: Example installation of the *blue merle* package via ssh

Disclaimer and call for action

Users should use *blue merle* at their own risk and only if they understand what it does and does not do for them. While *blue merle* improves the anonymity and reduces traceability of a GL.iNet Mudi 4G LTE router, the actual level of anonymity it offers depends on other factors.

The *blue merle* project does not provide any protection against user error or improper implementation.

Firstly, *blue merle*permanently removes all traces of the router's old identity. However, any resulting privacy benefits depend on the degree of anonymity of the used SIM card and the used IP anonymization technology (VPN/Tor). In some countries, anonymous SIM cards may be difficult to acquire. Secondly, *blue merle* can lead to issues when changing the router's identifier to an IMEI that is also active within the same network or to the IMEI of a stolen device. Depending on your jurisdiction, changing your IMEI might violate local regulation or law. Finally, *blue merle* is a research project and further or unanticipated modifications to the Mudi router can significantly impact its effectiveness.

The *blue merle* project is hosted on the **SRLabs' GitHub** repository. We look forward to contributions from the community. In particular, we welcome pull requests to support other devices using the Quectel EP06-E/A baseband, or other basebands that allow changing the IMEI. The *blue merle* project was also recently featured in the **Q1 2023 edition of the *Unredacted* magazine**.

For more information on our research and consultancy work within the mobile network field, check out more of **our research blog posts** or consider **joining our team of technical experts.**