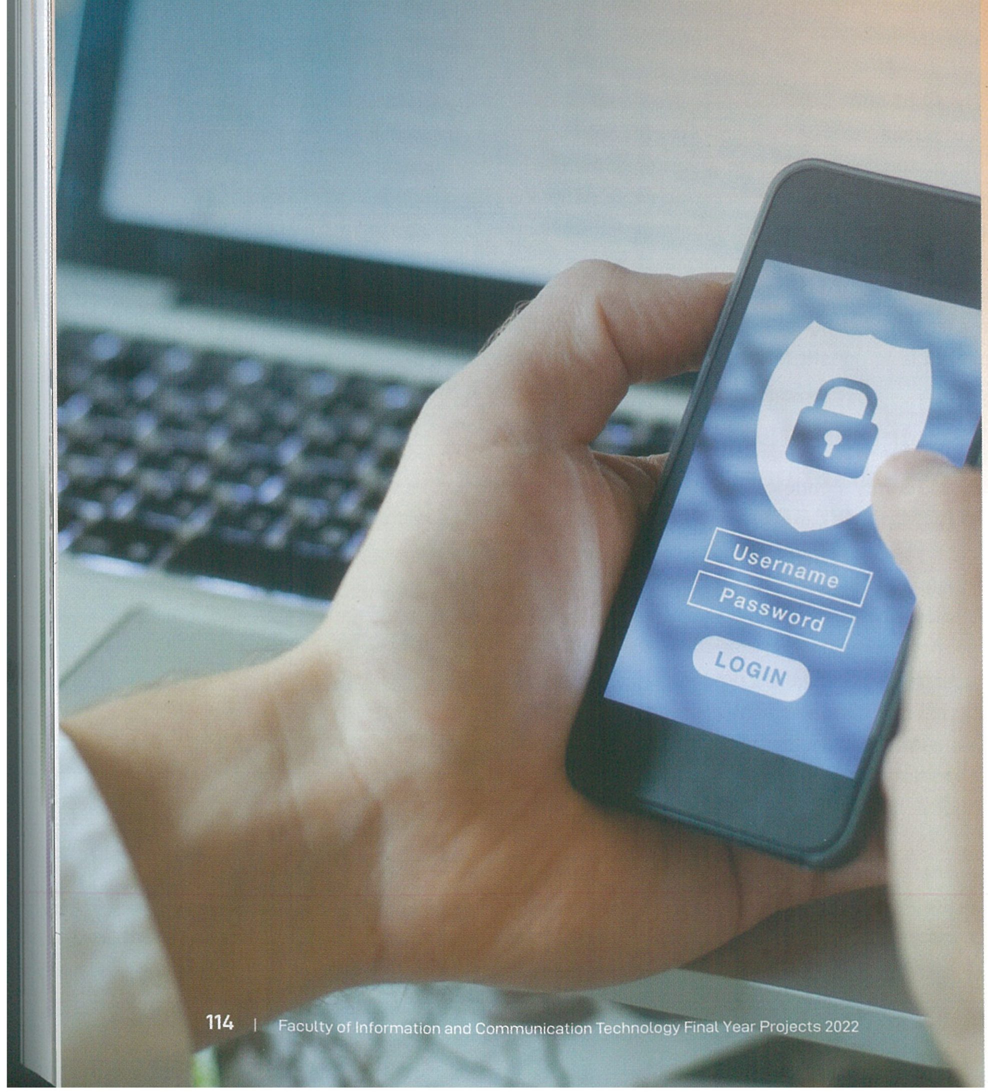
VIRTUAL CRIME SCENE: detecting malware attacks

High-profile people have high-profile information worth stealing – but with hackers now able to delete their tracks, pinning them down is getting harder. Could the answer lie in add-ons to certain Android apps? PhD student JENNIFER BELLIZZI believes so.



Our phones have become a lot more than just a tool for making calls. They're now our personal assistants with access to our bank accounts, photo albums, private conversations, and health records. Unfortunately, they are also susceptible to attacks by hackers, which is problematic for everyone, but it's doubly worrying when the phone belongs to high-profile individuals whose information could be used for malicious purposes. Now, Jennifer Bellizzi's PhD may offer some hope.

"Over the years, hackers have become more astute," says Jennifer, who is in the second year of her PhD in Android Digital Forensics. "We've reached a point where a hacker can bypass anti-virus software, install malware on your phone, and send messages to people in your phone book, load apps, or even see your screen."

What's worse is that some of these pieces of malware, often referred to as 'trojans' or 'worms', can sometimes delete any traces of their activities, making it almost impossible to find out whether your phone has been hacked. This, in turn, places the victims of such stealthy attacks at a disadvantage and leaves criminal investigators with a gap in their timeline of how and when the attack may have happened.

But there may be a way to counteract this. Jennifer's PhD focuses on a piece of software that can be added to apps on Android phones, which tend to be more prone to such attacks.

"It's called the Just In Time – Memory Forensics [JIT-MF] driver, and its job is a simple yet crucial one as it acts as a black box, meaning that it cannot be erased or manipulated. A mobile phone application can then 'dump' certain relevant information into it."

Ms Jennifer Bellizzi.

Basically, the JIT-MF driver records all the activities undertaken on a particular app. So, among other things, criminal investigators could have access to information on when and to whom messages were sent, when the app was opened, whether the user had been active right before or after such activities took place, and so on.

Nevertheless, for the JIT-MF driver to offer a complete log, the programmer needs to be specific about what the app is used for and what kind of attacks it could suffer.

"Let's take my first JIT-MF driver as an example," she continues. "This was created specifically for messaging apps like WhatsApp, Telegram, and Signal. It was given clear instructions on what such apps can be used for, such as loading the app, messaging, calling, or sending photos. These are, of course, all legitimate actions the phone's rightful owner may do multiple times a day, but they're also the actions a hacker might undertake through a messaging hijack attack.

"So the JIT-MF driver will start recording every time the app is used for whatever action we have asked it to. This, in turn, will allow criminal investigators to know whether the app was opened when the user was otherwise inactive, or when messages were sent and deleted in quick succession."

However, the idea behind this driver isn't for users to have their messages monitored by default. Instead, it is an add-on that high-profile users can choose to install on specific apps to safeguard their business and personal information. It can then be used to keep a record that could help criminal investigators in instances of such hijackings, which can lead to the theft of money, leaking of sensitive information, and even blackmail.

"As things stand, hackers have the upper hand in such situations, with even state-of-the-art forensic tools unable to find logs of certain activities. The JIT-MF driver will hopefully change that and become an integral tool for investigators to use when they're putting together their timelines of such crimes," Jennifer concludes.

> **"The JIT-MF driver will hopefully ... become an integral tool for investigators"**

The JIT-MF driver's role in mobile phone-related crime detection and prevention is promising, particularly as it is so versatile. This means that as hackers up their game, those fighting crime can also have updated tools that keep users safe – and that's undoubtedly one of the best uses of information and communication technology we can think of!

The next phase of JIT-MF driver research will be carried out as part of the Digital Evidence Targeting covErt Cyberattacks through the Timely Information Forensics (DETECTIF) project, launched in July 2022. Project DETECTIF is financed by the Malta Council for Science & Technology for and on behalf of the Foundation for Science and Technology through the FUSION: R&I Research Excellence Programme.