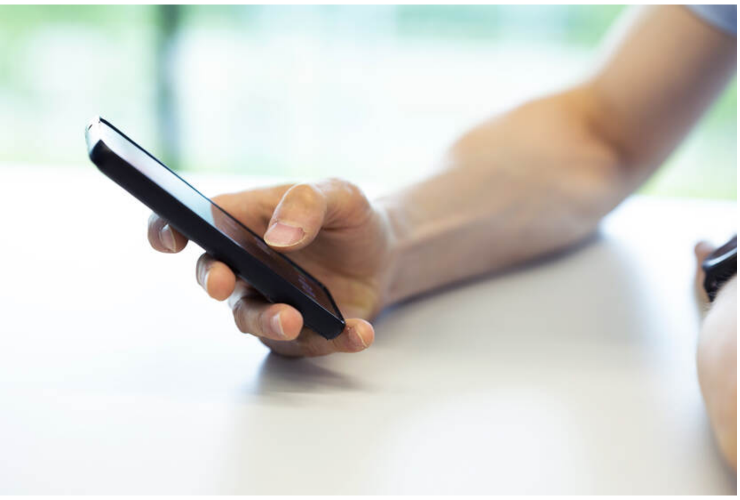
Netherlands Forensic Institute
Ministry of Justice and Security

NFI helps keep open-source software up to date in order to hack cryptophones

News item | 12-07-2023 | 09:37

Criminals frequently use cryptophones to communicate. In order to obtain access to confiscated cryptophones, one of the things the Netherlands Forensic Institute (NFI) is focusing on is cracking the users' passwords. The tools used for this purpose by forensic examiners include ones with names like 'John de Ripper', 'Hashcat', 'Brutus' and 'Aircrack'. In order to be able to manage these kinds of tools effectively, the open-source program Hashtopolis is used. The software was originally created by a student. The NFI's use of open-source software developed by a student is not so strange in itself, but for government authorities to subsequently decide to help improve an open-source program, is very rare indeed. And yet, NFI forensic examiners are now the ones who are helping keep Hashtopolis up-to-date.

With open-source programs such as Hashtopolis, the software's source code can be accessed by anybody wishing to inspect or modify it. The program was developed five years ago by a student, who after three years no longer had time to keep updating the program. "It was no longer being updated, bugs were no longer being repaired and no new functionality was being added," says an NFI crypto researcher. In the meantime, several international investigative agencies had started using the program to crack passwords. "We had to make a choice: we could either start from square one and rewrite and rebuild everything ourselves or we could build on the existing program and make improvements. Re-doing everything ourselves would have been very time-consuming. That's why we decided to use what was already there and continue with that."



Supervisor

Hashtopolis can be viewed as a kind of supervisor at a construction site, says the crypto researcher. “The foreman manages the workers who are doing the building; he distributes the work.” To crack a password, computers need to have a lot of processing power. Multiple passwords have to be tried in as short a time as possible and that can be done in numerous different ways. “If you try to crack a password using a regular computer, it can take months or even years. It's best to use multiple computers; those are your ‘workers’, so to speak. Hashtopolis can manage the different computers and distribute the work, as a result of which, instead of taking months, passwords can sometimes be cracked within just few hours.”

Several ways

There are countless different ways to crack a password. The easiest is simply try to guess the password, says the crypto researcher. “Some people have easy passwords, such as their child's name, plus a date of birth. Then you don't need a lot of processing power; you just need information about the specific suspect.” Other ways include using password dictionaries or ‘brute force’. That means you just keep trying new combinations of characters and words, until you find the right password. In order to be able to crack passwords, you need a small piece of the telephone. This piece, in which the password is stored, is referred to as the ‘hash’. The NFI Hardware team retrieves this from the telephone. “Then you make a copy, as it were, of the lock, after which you try using different keys. If you are able to figure out the key to the hash, you’ll also know the password and then you can open the real telephone lock.” Guessing the key in this way can be done using tools such as ‘John de Ripper’ and ‘Hashcat’. Hashtopolis manages the various methods.

Eight thousand lines

In the meantime, the NFI has made two hundred contributions and written eight thousand program lines. Partly thanks to the NFI's input, four updates have already been released. By incorporating the changes into the open-source Hashtopolis, they not only benefit the NFI, but also the community, including other international investigative agencies and security researchers. And in that way, thanks to a program once developed by a student, the passwords of criminals' cryptophones can keep being cracked in a smarter, more efficient and more effective manner.