AMNESTY INTERNATIONAL
QUESTIONS AND ANSWERS

Index: DOC 23/001/2014

EMBARGO: 20 November 2014 at 00:01Hs GMT.

Detekt: New tool against government surveillance – Questions and Answers

DETEKT

What is *Detekt* and how does it work?
Detekt is a free tool that scans your computer for traces of known surveillance spyware used by governments to target and monitor human rights defenders and journalists around the world. By alerting them to the fact that they are being spied on, they will have the opportunity to take precautions.

It was developed by security researchers and has been used to assist in Citizen Lab's investigations into government use of spyware against human rights defenders, journalists and activists as well as by security trainers to educate on the nature of targeted surveillance.

Amnesty International is partnering with Privacy International, Digitale Gesellschaft and the Electronic Frontier Foundation to release *Detekt* to the public for the first time.

Why are you launching *Detekt* now?
The increasing use of intrusive surveillance has had a dramatic impact on the right to privacy and other human rights like freedom of association and freedom of expression.

The latest technologies enable governments to track, monitor and spy on people's activities like never before. Through the use of these technologies, governments can read private correspondence and even turn on the camera and microphone of a computer without its owner knowing it.

By increasing people's awareness of these issues we hope they will be able to take practical steps to protect themselves.

We also hope that by knowing more about the dangers of these technologies more people will join Amnesty International in calling for stricter controls on their international trade to stop their use in violation of the right to privacy, freedom of expression and other human rights.

Our ultimate aim is for human rights defenders, journalists and civil society groups to be able to carry out their legitimate work without fear of surveillance, harassment, intimidation, arrest or torture.

Has anyone used *Detekt* successfully to know if they were being spied on?
Detekt was developed by researchers affiliated with the Citizen Lab, who used a preliminary version of the tool during the course of their investigations into the use of unlawful surveillance equipment against human rights defenders in various countries around the world.

For example, according to research carried out by Citizen Lab and information published by Wikileaks, FinSpy – a spyware developed by FinFisher, a German firm that used to be part of UK-based Gamma International-- was used to spy on prominent human rights lawyers and activists in Bahrain.

How effective is this tool against technologies developed by powerful companies?
Detekt is a very useful tool that can uncover the presence of some commonly used spyware on a computer, however it cannot detect all surveillance software. In addition, companies that develop the spyware will probably react fast to update their products to ensure they avoid detection.

This is why we are encouraging security researchers in the open-source community to help the organizations behind this project to identify additional spyware or new versions to help *Detekt* keep up to date. Contact information is available here.

It is important to underline that if *Detekt* does not find trace of spyware on a computer, it does not necessarily mean that none is present. Rather than provide a conclusive guarantee to activists that their computer is infected, our hope is that *Detekt* will help raise awareness of the use of such spyware by governments and will make activists more vigilant to this threat.

In addition, by raising awareness with governments and the public, we will be increasing pressure for more stringent export controls to ensure that such spyware is not sold to governments who are known to use these technologies to commit human rights violations.

SURVEILLANCE
How widely do governments use surveillance technology?
Governments are increasingly using surveillance technology, and targeted surveillance in particular, to monitor the legitimate activities of human rights activists and journalists.

Powerful software developed by companies allows governments and intelligence agencies to read personal emails, listen-in on Skype conversations or even remotely turn on a computers camera and microphone without its owner knowing about it.

In many cases, the information they gather through those means is used to detain, imprison and even torture activists into confessing to crimes.

It's impossible, however, to give an accurate estimate of how many people are affected by this surveillance spyware. This is because the companies that build and sell such software market themselves on their ability to hide it from users.

Recent research has shown that known spyware has been found present in dozens of countries, covering all regions of the world.

Detekt is the first public tool that will assist activists, journalists and civil society groups to scan their computers for spyware.

How big is the unregulated trade in surveillance equipment? What are the main companies and countries involved?
The global surveillance industry is estimated to be worth approximately US$5 billion a year – with profits growing 20 per cent every year.

European and American companies have been quietly selling surveillance equipment and software to countries across the world that persistently commit serious human rights violations.

Industry self-regulation has failed, and government oversight has now become an urgent necessity.

Privacy International has extensively documented the development, sale and export of surveillance technologies by private companies to regimes around the world. Recipient countries include: Bahrain, Bangladesh, Egypt, Ethiopia, Libya, Morocco, South Africa, Syria and Turkmenistan.

Isn't publicizing the existence of this tool giving governments a heads up about how they can avoid being caught (by adapting new equipment which avoids detection)?
The technologies that allow governments to efficiently and covertly monitor the digital communications of their citizens are continuously improving. This is happening across the world.

The growing trend in indiscriminate mass surveillance on a global scale was laid bare by the Edward Snowden disclosures. Following the lead of the USA and other industrialized countries, governments everywhere now justify the use of such surveillance. This has a chilling effect on the rights to freedom of expression and peaceful assembly in countries across the world.

In addition to mass surveillance technologies, many governments are using sophisticated tools to target specific human rights defenders and journalists who work to uncover abuses and injustice.

The new spyware being developed and used is powerful and dangerous and putting many human rights activists and journalists at risk of abuse.

As surveillance technologies develop in sophistication, it is vital that civil society groups learn how to protect their digital communications. No one tool or intervention will be enough to do this. We hope *Detekt* will become a new approach for investigating surveillance while sensitizing people to the threats.

However, long term we must also demand that governments live up to their existing commitments to human rights and that they and companies put in place stronger protections to ensure that new technologies are not used to violate human rights.

Surveillance is also used to carry out legitimate criminal investigations, why are you against it?
Targeted surveillance is only justifiable when it occurs based on reasonable suspicion, in accordance with the law, is strictly necessary to meet a legitimate aim (such as protecting national security or combatting serious crime and is conducted in a manner that is proportionate to that aim and non-discriminatory.

Indiscriminate mass surveillance – the widespread and bulk interception of communication data that is not targeted or based on reasonable suspicion – is never justifiable. It interferes with a range of human rights, particularly the rights to privacy and freedom of expression.