Decline of the Scientific Method: New (Austrian) “Trojan” Law without Technical Expertise

Posted on **August 03,2017** by **sanna**

The Crypto Wars are still raging despite everyone relying on secure communication. Everyone means everyone. The good thing is that mathematics still works, even though some people wouldn't want it to. The latest cryptographic review comes from Amber Rudd, the current UK Home Secretary. She said recently: "Real people often prefer ease of use and a multitude of features to perfect, unbreakable security." The corollary in turn states that DeepSec conferences aren't attended by real people. Since we are not yet a purely robot-based event, there is something wrong with this approach to secure communication. The common denominator is simply the lack of technical expertise. There is no surprise there. Ever since the Internet was discovered by the rest of the world (which was in the 1990s, don't get fooled by web sites who claim to have invented the Internet), politics, government, and society struggles to keep up. This is exactly why we constantly emphasise that DeepSec tries to bring together the world's most renowned security professionals from academics, government, industry, and the underground hacking community – things go horribly wrong without experts who use and understand what science means. Hence our motto for DeepSec 2017 - Science First!

In order to illustrate how thing can go wrong, we have translated an article by Erich Möchel, a journalist specialised in all things digital. The original text was published at the FM4 web site and is called *Neues „Trojaner“-Gesetz ohne technische Expertise*.

New (Austrian) "Trojan" Law without Technical Expertise

ByErich Möchel

As the explanatory notes on the draft show, the convened expert group served mainly to legally secure the access rights of the police. There were no technicians among them.

As part of the "security package" of the federal government, which has been in appraisal since Monday, the use of police Trojans takes a central position. Ten out of a total of 16 pages of the explanatory notes on the new Code of Criminal Procedure concern the use of malicious software by the police. In order to implement this new, technically complex measure correctly, a high-level expert committee, consisting exclusively of lawyers, was convened.As a matter of fact, the subject matter of the discussion was only the legal basis, primarily the legal delimitation of the monitoring of encrypted communications in an "online search". The legal hurdles for the search of a computer are significantly higher than for monitoring communications. The text not even mentions that both types of monitoring use the same type of Trojan malicious software.

"A kind of communications monitoring"

Apart from the lack of an assessment of its technological impact, the explanatory notes to the draft show that apparently no technicians were involved in this bill. In sum, the draft contains only one technically exactly formulated passage – which concerns a completely meaningless and therefore misleading fact – otherwise it’s just an abstract requirement catalogue of lawyers. And its foundation is based on basic assumptions, which are technically simply not tenable. One example of this is the juridical demarcation of an "online search" and "communications monitoring" which dominates the entire Trojan chapter.

Which Aspect was discussed

After a lengthy legal discussion, whether the "technical process of such an encryption can be considered as part of the transmission", the convened experts arrive at the conclusion that this is indeed the case. The use of such a "software" is therefore "to be regarded as a kind of communications monitoring", and could therefore be "delimited from online monitoring". Thus "only the requirements of the secrecy of telecommunications must be met, but not the (more qualified) requirements of the IT fundamental right", states the expert group.

This "IT fundamental right" is derived directly from Article 8 of the European Convention on Human Rights and demands a higher threshold for access of prosecutors. Thus, the fundamental rights of all Austrian citizens were discussed only in the light of the fact that state access should be facilitated as much as possible. Already the monitoring of traffic and conversations gets approved easily even in the case of minor offences. The conclusio of the experts on this point: It is therefore important "that a software is used, which [recognizes and] decodes only transport encryption".

What a Trojan does

This is exactly what a Trojan doesn't do, no matter, whether it is called "communications monitoring" or an "online search". To operate at all, the malicious software must first take over the operating system of the terminal device, because a Trojan has to have administrator rights. It already needs that in order to install various auxiliary programs from a hidden server of the police authority on the monitored PC or smartphone. This involves massive interventions in the operating system and the storage media of the device, which must also be searched in order to identify anti-virus programs. In addition to the search for "digital fingerprints" of already known malicious software ("virus signatures"), anti-virus softwares also analyze the behaviour of installed software through heuristic methods.

Trojan twins

This is why every professional malicious software downloads a so-called "rootkit", which deeply interferes with the operating system of the smartphone or PC in order to deceive anti-virus apps and conceal the technical processes on the device from the user. What the Trojan actually taps, depends solely on the features of one and the same software. In a whole series of completely identical functions, there is only one feature, and it's technically trivial, which distinguishes the "monitoring Trojan" from the "communications Trojan": The latter can not access files stored by the user himself.

However, on how private files could be identified as such without searching the storage medium the experts remain silent. The Ministry of Justice emphasizes that this is "technically possible," the experts say measures must also be "practicable" and "target-oriented" and include "preventive measures against dispersed / collateral damage and provide effective abuse control".

"Technically possible, practicable, precise"

Technically it is, of course, possible to program such a malware suite, and as the ongoing trojan attacks by criminals using blackmail software show, it is also "practicable" to contaminate a device over the Internet with a Trojan. How "target oriented" it is, however, to try to apply a Trojan to a certain terminal device via a mobile network, in which the IP addresses of tens of thousands of active terminals constantly change, is highly doubtful. In the only – at least to some extent – technically meaningful passage of the whole explanation, it is not entirely clear whether this is a matter of blank ignorance or deliberate deception.

Hardware keylogger forbidden, software keylogger allowed

Literally, it says: "Only the installation of a program in the computer system" is permissible. "Other technical possibilities such as, for example, the collection of electromagnetic radiation "is firmly prohibited.

This method from the nineties has become obsolete since the disappearance of tube screens. In addition, "the incorporation of hardware components into the computer system (eg a" keylogger ") is not permitted, in spite of the fact that hardware keyloggers are probably only still available in technical museums. However, the explanations are silent on the legality of software keyloggers, because without such a function, a Trojan could not make any recordings of WhatsApp chats, and then transfer them to a command-control server of the authorities.

Posted in:Discussion,High Entropy,Security |
Tagged:Cybercrime,Cyberwar,Infrastructure,Malware,Mindset,Politics,Risk | With 0 comments