Trojans And Rule of Law

The purpose of TrojansAndRuleOfLaw.org is to help fueling a debate to make Lawful Interceptions legal again. (i.e. adherent to the Rule of Law)

In the good old world of POTS (plain old telephone systems) lawful telephone interception was clearly defined and processes and safeguards have been rather easily defined and implemented adhering to the rule of law, finding a way to ensure respect of fundamental rights and law enforcement possibilities.

The digital age has blurred the boundaries between interception, search, tailing, etc.

It is a fact that investigations have moved to the edges, onto citiziens' devices and that the attack surface has broadened from telephones to videogame consoles, to cars, to IoT devices, etc.

Although activists cry foul and try to stop them, it is a fact that such investigations are being performed everywhere, often devoting limited attention to the rule of law.

When elected in the italian parliament, Hon. Stefano Quintarelli tried to put forward a proposal to ensure adherence to the rule of law in this area.

A former hacker, entrepreneur, computer security professor, he managed to form a board of advisors under the oversight of Pres. Luciano Violante, a former Speaker of the House (also former member of the legislative office of the Ministry of Justice, investigative magistrate, professor of legal institutions and penal procedure).

The board was composed by three outstanding lawyers with specific experience, agreed with Pres. Violante, and with a significant reputation with legal institutions, consumer advocacy groups and industry.

This board engaged in a number of iterations with relevant stakeholders representing all italian LEUs, major consumer and civil rights advocacy groups, authorities, former MPs and scholars (both from technical and legal academia).

The bill proposed amendments to the Italian Penal code and the Code of penal procedure as detailed in this repository.

Trojan Bill Regulation Proposal (Captatori Informatici)

The Bill Proposal project has been made by an interdisciplinary team with a high numbers of volounteers and reviewers over around 2 years time. It didn’t become a reality because the Italian Government collapsed before the Law was scheduled to be discussed by the Parliament.

The core team that worked on the the bill proposal was composed as follow: * Stefano Quintarelli, MP expert in IT and Cybersecurity * Stefano Aterno, Criminal Lawyers expert in Hacking Cases * Fabio Pietrosanti, Security and Digital Rights Expert * Andrea Ghirardini, Security and Computer Forensic Expert

This repository is made up for valuable juridical, human rights, forensics and technical interests on the topic internationally.

No, this bill proposal doesn’t have anything todo with export control or undisclosed vulnerabilities (0day).

The Bill Proposal and its artifacts

There are many artifacts around the trojan regulation bill proposal we’ve done in Italy in 2017, most in Italy, with some in English for a bigger audience.

ITA: * The Bill Proposal * The Technical Regulation of the Bill Proposal * Motivations on why a Technical Regulation is needed for the jurists

- Press Conference of the Civici and Innovatori parliamentary group preenting the Trojan Bill Proposal
- Talking notes for the Press conference

ENG:

- Italy unveil a legal proposal to regulate hacking article on boingboing summarizing for an international audience the principles of the proposal Here the Online Article
- Summary of the Bill Proposal

Third party opinions / review / interests

1. CCC issued an expert information on the political groups on risks when using malware in prosecution that explicitly mention and include references to the safety principles of the trojan bill regulation proposal. For non German speaker, here Google Translated edition. The CCC position paper inlcude the principles of Italian trojan proposal from Page 16, specifically in addressing the issue of “*Lack of technical verifiability and traceability*”:

- “1.” The source code must be stored and verifiable.
- “2.” Every action must be documented completely, tamper-proof and verifiable.
- “3.” The malware must not weaken the general security level of the device
- “4.” The development and use of malware must be carried out by means of a central recording be understandable.
- “5.” Independent certification of technical and data protection requirements be renewed regularly.
- “6.” Encryption and integrity protection of the data collected.
- “7.” Limitation of sovereign tasks to government agencies.

2. EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) published in 2017 Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices583137_EN.pdf#page86) that at Page 86 does a review of the bill proposal concluding that

    - *“The abovementioned conditions provide for many of the relevant and expected fundamental rights safeguards.“*

3. Access Now on 29 March 2017 publish a Policy Review of the Bill Proposal while condemning any government hacking, express a generally favourable opinion, with several improvements suggestions:

    - “While Access Now does not condone government hacking activity […] we believe it is of pivotal importance that if it is to be conducted, it is done within a robust legal framework.”
    - “We appreciate the provision within the proposal that seeks to establish strict use limitations for these authorities.”
    - “We strongly support the provisions in Civici e Innovatori’s proposal intended to ensure integrity, authenticity, and immutability of data and devices impacted by government hacking”
    - “There are several other provisions in the proposal that we believe will help protect human rights. First, we are in favor of the provision that prohibits the use of contractors to employ hacking tools”
    - “We are appreciative of Civici e Innovatori’s engagement on this important issue and incorporation of several human rights protections into the draft proposal.”

4. Privacy International has been interested in the review and consulting on the bill proposal, with talks with Asaf Lubin, with which we did also a set of written question and answers that has been used as informative contribution for their Submission to Human Rights Committee 119 at Office of the United Nations High Commissioner for Human Rights where it’s stated

    - *“The bill calls for amending Article 266 to reflect the Court’s judgment, as well as establish a more robust system for authorizing remote and covert hacking”*

5. Eva Gasperin, Cybersecurity Director at EFF expressed on Twitter that this bill proposal “doesn’t look bad”

6. Claudio Guarnieri made a poll on Twitter to his audience showing that 51% of respondant are against any kind of regulation

Conferences

- Round table Government hacking in different national contexts organized by EDRi (European Digital Rights) at Privacy Camp 2018
- Talk at SHA2017 Hacker Camp in the Netherland on Regulating Law Enforcement use of Trojans (SHA2017) by Fabio Pietrosanti and Andrea Ghirardini (Here the Slides)
- Journalism Festival 7/04/2017 Panel on Lawful state hacking: necessary investigative upgrade or privacy nightmare?

License