November 11, 2013

To Whom It May Concern:
(cc. Bits of Freedom)

Thank you for your letter posted here (https://www.bof.nl/live/wp-content/uploads/Letter-to-antivirus-companies-.pdf) and your interest in our detection policies.

Your questions are based on something of a logical fallacy, in that; there are too many Anti-Malware companies, too dispersed – geographically and politically – for a government (any government) agency to trust all of them. No doubt if agencies *were* able to insist on such cooperation, they would, but only the most draconian regimes can do that, and even then, only locally. ESET is a global company with research facilities in several parts of the world, and is therefore not subject to a single jurisdiction or government.

However, since you have addressed these questions to us publicly, here are our answers. Most are taken from previous answers to similar questions.

- *Have you ever detected the use of software by any government (or state actor) for the purpose of surveillance?*

  There are instances where we *know* we detect malware alleged to be used by government agencies, since after the fact it becomes known that this was the purpose, for example the Win32/R2D2.A Trojan mentioned in the links below.

  However, in many cases binary analysis doesn't tell us exactly why malware was planted or by whom. So we don't always know whether we detect a state-sponsored malware. Nevertheless, from our point of view, malware is malware, no matter who created it, and we will dedicate all of our efforts to detect as much as malicious software as possible.

- *Have you ever been approached with a request by a government, requesting that the presence of specific software is not detected, or if detected, not notified to the user of your software? And if so, could you provide information on the legal basis of this request, the specific kind of software you were supposed to allow and the period of time which you were supposed to allow this use?*

  No government agency has ever asked us not to detect any specific software, nor have we been asked not to notify such detection to the user.

- *Have you ever granted such a request? If so, could you provide the same information as in the point mentioned above and the considerations which led to the decision to comply with the request from the government?*

  Since we've never received such a request, the situation hasn't arisen.

- *Could you clarify how you would respond to such a request in the future?*

  We don't envisage any circumstances in which we would comply with such a request. Our mission is to allow everyone to enjoy a safer digital world. It's our job to detect malware, and our customers expect us to deal with it when we find it. There is no such thing as a good Trojan and any such code can turn malicious in the hands of crooks and terrorists.

There is nothing new about our stance, as you can see from the links below with ESET's writing on this topic:

http://www.welivesecurity.com/2012/08/31/finfisher-and-the-ethics-of-detection/
http://blog.eset.com/2011/10/10/german-policeware-use-the-farce-er-force-luke
http://www.welivesecurity.com/2011/10/11/government-public-interest-and-trojans/
http://go.eset.com/us/resources/white-papers/Please_Police_Me.pdf

And some other relevant links:

http://www.wilderssecurity.com/showthread.php?t=319731
http://www.wilderssecurity.com/showthread.php?t=5281
http://www.virusbtn.com/virusbulletin/archive/2007/04/vb200704-comment

Regards,

Richard Marko, CEO, ESET
Palo Luka, CTO, ESET
Juraj Malcho, Chief Research Officer, ESET
Ignacio Sbampato, Chief Sales & Marketing Officer, ESET
Andrew Lee, CEO, ESET North America