House of Representatives Standing Committee on Communications

Additional Question

Internet Industry Association

Inquiry into Cybercrime

Topic: **Botnet detection**

Hansard Page: **COMM 14**

Question:

- **Is software available to detect botnets?**
- **Is it possible to set up an online site that is capable of detecting botnets on computers?**

Software is able to check for infection on computers but not whether a computer is part of a botnet per se. This can only be done using network intelligence and even then is not a trivial exercise as the behaviour of individual computers needs to be assessed. There are of course millions of computers on Australian networks.

Online scanning websites offer some remote scanning possibilities for users, but scanning is limited to browser's security settings. The prior installation of a 'root kit' may render such scanning ineffective. Online scans are not to our knowledge able to detect if a computer is part of a botnot, only whether it may have software installed that could render it susceptible to such. And even then, this is not infallible. The increasing sophistication and funding of the zombie threat seems to be reducing the effectiveness of such approaches.

Topic: **Brochure for point of sale**

Hansard Page: **COMM 20**

Question 2:

- **Provide a copy of sample brochure being prepared for manufacturers to give to consumers at point of sale of routers and modems.**

This is provided as an attachment to this response. As this is a draft it is confidential and not authorised for publication.

House of Representatives Standing Committee on Communications

Additional Question

Internet Industry Association

Inquiry into Cybercrime

Q3

Topic: Statutory obligations to take action to prevent violations of Commonwealth, State or Territory laws.

Additional Question:

The *Telecommunications Act 1997* (Cth) sets out the obligations of carriers and carriage service providers to prevent telecommunications networks and facilities from being used in the commission of an offence against the laws of the Commonwealth or the States and Territories (s.313).

Subsection 313(5) provides immunity from liability for damages arising from acts done in good faith or in compliance with court order or an ACMA direction.

ISPs are regulated primarily by the *Telecommunications Act 1997.* However, evidence given by Telstra (Hansard 42 11/09) suggests s.313 does not apply to the online environment.

a) Can you clarify whether, in your view, s.313 does or does not apply ISPs, and, if not, should similar provisions apply to the online environment?

b) Has the IIA had any policy discussion on the issue of protection from liability with ACMA or the Department of Broadband, Communications and Digital Economy?
c) If so, what is the status of those discussions?

Answers:

a. No we have not considered this question to date.
b. Not, in this context, since 2001 when the Cybercrime legislation was amended specifically to deal with this matter.
c. Does not apply.

Topic: Consumer access to remedial software

Question 4:

Several witnesses have argued that Australia's response to malware and cyber crime generally is too fragmented, and, consumers lack incentives to deal with infected machines/websites because of lack of easy access to tools to remediate the problem. The Japanese Government has established the Clean Computer Centre and program, which brings together the government, the cert and Trend Micro, in a combined and

centralised effort to combat cyber crime (esp malware). Consumers are provided with free tools to disinfect their machine.

a. Does IIA see merit in developing a more integrated response to the problem of cyber crime with combined IT analytical skills, with IT vendor(s) developing anti virus software, the regulator and ISPs?

b. From an industry perspective, what strengths and weaknesses does IIA see in the Japanese approach?

Answers:

a. Does IIA see merit in developing a more integrated response to the problem of cyber crime with combined IT analytical skills, with IT vendor(s) developing anti virus software, the regulator and ISPs?

The IIA has often sought to bring together diverse stakeholders from Government, Community, Industry and Broader Telecommunication sectors where sharing intelligence alerts and strategies are appropriate.

We understand Japan's Cyber Clean Center work closely with ISPs and a number of security vendors https://www.ccc.go.jp/en_ccc/index.html; see also http://blog.cytrap.eu/?p=287

It uses an approach similar to that of the IIA's eSecurity code by alerting owners of compromised PCs by email and web site in combination. It sends a mail to an infected user together with a URL of the "BOT disinfestation website" that option on how to disinfect BOTs. It aims to give the infected users easy-to-understand explanations of how dangerous BOTs are and how to clean BOTs. https://www.ccc.go.jp/en_activity/index.html.

At the same time it has links to relevant software or services that may assist infected users.

b. From an industry perspective, what strengths and weaknesses does IIA see in the Japanese approach?

The Cyber Clean Center works provided there are adequate resources to fund its operations, research and promotion. Its most recent report suggests that the rate of bot infections declined by 2.5% over the most recent year. https://www.ccc.go.jp/en_report/h20ccc_en_report.pdf

House of Representatives Standing Committee on Communications

Additional Question

Internet Industry Association

Inquiry into Cybercrime

Particularly useful is the CCC's publication of rates of botnet infections and responses to inform policy and education campaigns.

It would appear to be much better resourced as a public body compared with Australia.

Significantly only 30% of users contacted by CCC seemed to download the free removal tool. See http://www.ipa.go.jp/security/english/economics/slide/SecurityEconomics.pdf

In short 7 out of 10 users thought to have compromised devices did not respond.

More incentives such as the option of quarantining users subject to an agree procedure may assist.

See also http://www.nca.gr.jp/jws2008/WS1-ccc.pdf

Topic: **E Security Code of Practice**

Question 5:

Cyber crime, especially malware, is predicted to increase and represents a significant public policy issue for consumers, business and government. Several witnesses have argued that underreporting means intelligence data is not aggregated and this, in turn, undermines efforts to combat the problem.

The draft Code of Practice appears to leave the reporting of network attacks entirely to the discretion of the ISP based on whether or not an attack is considered 'serious':

a. What constitutes a 'serious' attack?

b. What is the justification for allowing such a wide discretion to the industry?

c. Isn't there a danger that institutionalising this approach will perpetuate the problem of under reporting?

d. Spamming, DDOD and malware infections are all illegal activities – isn't the public entitled to expect that once detected these activities will be routinely reported to an organisation like AusCert?

House of Representatives Standing Committee on Communications

Additional Question

Internet Industry Association

Inquiry into Cybercrime

Answer:

a. What constitutes a 'serious' attack?

   This would be elaborated in future guidelines. Generally, the view the drafting committee is that where an attack is likely to be of such extent in its scope or apprehended harm as to threaten national security, it should be reported to the relevant authorities.

b. What is the justification for allowing such a wide discretion to the industry?

   The primary aim of the Code is to alert and educate users that their system may be compromised. The overwhelming evidence is that such alerts are received well by users and remedial action becomes the main focus. The reporting function is there for extreme attack situations. Were reporting of all incidents or incidents above a low threshold to be the test, then it is likely authorities would be overwhelmed by data and little intelligence gained. Hence the discretion to ISPs. The Code guidelines will make this clear.

c. Isn't there a danger that institutionalising this approach will perpetuate the problem of under reporting?

   There is no evidence to support this being a risk. In practice the IIA and ISPs would aim to promote improved understanding of the risks of having compromised PCs. Reporting is intended only for major attacks so that the authorities can build a picture of the national situation. Minor attacks are not likely even in aggregate to represent a threat to the entire network.

Topic: **Trust Logo**

Question 6:

The Draft Code of Practice provides that an ISP, which is Code compliant, will be entitled to display the trust logo:

a. How will the E Security Code of Practice be monitored to protect the integrity of the IIA trust logo?

Answer

House of Representatives Standing Committee on Communications

Additional Question

Internet Industry Association

Inquiry into Cybercrime

Regular reviews are envisaged based initially on feedback or complaints made directly to the IIA or indirectly through TIO or other means. A review of the program's effectiveness – eg trends in reducing bots, would also consider the issues of industry compliance is built into the draft Code.

Topic: **Civil Actions against Spammers by ISPs**

Question 7:

In Europe ISPs are being given the right to take legal action against spammers. This reform appears to recognise that ISPs are also victims of this illegal activity and creates an avenue to recover economic losses.

a. Would reform giving ISPs a right to take legal action against spammers be a useful addition to the telecoms/broadcasting legal framework in Australia?

Answer:
In our early consideration of the Spam legislation there was some support from within the membership for civil recovery, but in the end the Government opted for harsh penalties which it considered an adequate deterrent measure. A recent case saw penalties of about $15 million awarded against local spammers. Since the passage of the Spam Act we have not received any representations from ISPs seeking amendment of the Act to allow for recovery. We are therefore not in a position to say whether this would have industry support.