icode

Submission by the Australian Communications Consumer Action Network to the Internet Industry Association

20 June 2013

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation

Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will activate its broad and diverse membership base to campaign to get a better deal for all communications consumers.

Contact

Steven Robertson
Policy officer

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: steven.robertson@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

Contents

1. Executive Summary

ACCAN welcomes the opportunity to comment on the Internet Industry Association's draft icode version 2.0. The icode, while voluntary, provides useful guidance to ISPs in how to manage incidents of malicious or suspicious activity detected on their customers' services. Our recommendations are intended to help ensure that ISPs' responses to such activity are carried out in a manner that balances the need for a secure and functional network with the need for consumers to have functional communications services.

1.1. List of recommendations

Recommendation 1: The icode should include a principle to the effect that inconvenience to the consumer should be limited to what is necessary and proportionate in the context.

Recommendation 2: The icode should explicitly encourage ISPs, at or about clause 6.4, to limit their actions to what is proportionate and necessary in the circumstances.

Recommendation 3: The icode should encourage ISPs to limit their actions, where possible, to avoid restricting services that do not pose a threat to the network.

Recommendation 4: ISPs should be encouraged to provide information about suspicious or malicious activity to their customers when it is detected.

Recommendation 5: The icode should call on ISPs to maintain anonymised statistics on the number and type of suspicious and malicious activities detected and the actions taken in response. This information should be made publicly available.

Recommendation 6: The icode should discourage ISPs and their resellers from providing consumer hardware in an unsecured, easily exploitable state.

Recommendation 7: The language of schedule 1 should be revised for a non-technical audience.

2. Responses to the draft icode version 2.0

2.1. General support for principles

While the principles in section 5 of the draft icode are generally appropriate, we suggest that an additional principle is needed to ensure that the icode is not applied in a way that causes disproportionate inconvenience for consumers.

Recommendation 1: The icode should include a principle to the effect that inconvenience to the consumer should be limited to what is necessary and proportionate in the context.

2.2. Proportionality of ISPs' actions

Our primary concern is that any actions taken by ISPs are proportionate to the risk a compromised device poses to the network. The icode should encourage ISPs to take a measured approach to compromised devices, and not all of the actions listed in clause 6.4 of the draft icode will be appropriate in every instance. While individual ISPs are able to exercise their own judgment, it would be beneficial for the icode to reflect this need for proportionality.

Recommendation 2: The icode should explicitly encourage ISPs, at or about clause 6.4, to limit their actions to what is proportionate and necessary in the circumstances.

In order to determine the potential harm to the network presented by particular suspicious or malicious activity, ISPs should consider ratings schemes to categorise particular threats.

Some of the actions given under clause 6.4 are, we suggest, excessive in particular situations, and may cause unnecessary inconvenience to the customer. For example:

- A customer whose device is sending spam should not automatically be placed in a walled garden or have their password regenerated if an ISP can instead simply block that customer's outgoing email; and
- A customer whose device is using a particular TCP/IP port for problem traffic should not have their entire service restricted if that port can be restricted.

A particular concern is for customers who rely on a single ISP account for all their communication needs—for instance, where an ADSL connection is bundled with a VoIP service or where a mobile device uses voice, SMS and data services. In these cases, placing the customer in a 'walled garden' or regenerating the customer's password may result in the customer losing the ability to contact their ISP to find out what has happened or to seek advice on how to remedy the problem. We suggest that the icode encourage ISPs to be granular in their actions, for example by restricting only non-voice services provided to a customer, or by allowing a customer to specify services (such as webmail) that are of high importance to them should they be placed in a walled garden.

Recommendation 3: The icode should encourage ISPs to limit their actions, where possible, to avoid restricting services that do not pose a threat to the network.

Particular care is needed where the customer's voice telephony services or critical services (such as medical priority assists or home alarms) would be unnecessarily blocked by the ISP's actions.

2.3. Phone and SMS contact with customer

The icode should discourage ISPs who call customers about compromised devices from requesting credentials such as passwords, security questions, or personal information during an ISP-initiated call. Clearly establishing that no such information will be sought on ISP-initiated calls would be useful in helping consumers identify possible scam calls.

ISPs should also give consideration to any complex communication requirements of the particular customer. A Deaf customer, for instance, might require the use of their computer and the internet in order to contact the ISP's customer assistance service.

2.4. Reporting incidents

In addition to the recommendations in clause 6.5 that ISPs report suspicious or malicious activity to relevant government agencies, ISPs should provide information about such incidents to their customers. This could be presented, for instance, on an ISP's website along with the other information recommended in clause 6.1(b).

Recommendation 4: ISPs should be encouraged to provide information about suspicious or malicious activity to their customers when it is detected.

2.5. Monitoring and reporting

While the icode is voluntary, it would be useful to have some record of the frequency with which the actions listed in clause 6.4 are taken by ISPs. This would add transparency and increase consumer confidence that the actions being taken by ISPs are a necessary response to the threat of malicious and suspicious activities. Although the icode recommends reporting various kinds of suspicious or malicious activity to relevant authorities, ISPs could be called on to maintain, for example, anonymised statistics on the number of actions taken each month under the icode, including the type of action taken and the type of suspicious or malicious activity detected.

Recommendation 5: The icode should call on ISPs to maintain anonymised statistics on the number and type of suspicious and malicious activities detected and the actions taken in response. This information should be made publicly available.

Consideration should be given to having a centralised reporting system managed by, for example, the IIA or the ACMA.

2.6. Prevention

As incidents such as the 'Carna Botnet'[1] demonstrate, a significant point of weakness in networks lies in home gateways being shipped with poor default security settings. ISPs and their resellers who provide hardware are in a position to proactively reduce this element of risk by shipping hardware that has appropriate security settings by default.

Recommendation 6: The icode should discourage ISPs and their resellers from providing consumer hardware in an unsecured, easily exploitable state.

2.7. Consumer information

We are concerned that the information included in schedule 1 may not be at a level that will be useful for many consumers. For instance, the advice to '[i]nstall a firewall to prevent unauthorised access to your devices' will only be of use to consumers who understand, at least in general terms, what a firewall is and how to install and configure one. Similarly, the instructions on securing a wireless network may be overly technical for general consumers. While it may be difficult to set out advice of a technical nature in non-technical language, consideration should be given to revisiting the language of schedule 1 in order to make it more accessible to consumers with little or no technical background.

Recommendation 7: The language of schedule 1 should be revised for a non-technical audience.

[1] <http://internetcensus2012.bitbucket.org/paper.html>