Supplementary Submission No. 30.1

AusCERT

Australia's National Computer Emergency Response Team

House of Representatives Standing Committee on Communications – Inquiry into Cyber Crime

Supplementary submission from AusCERT

Background

AusCERT made a written submission to the House of Representatives cybercrime inquiry.

AusCERT has also provided oral evidence at the request of the Committee conducting the inquiry in Canberra on 11 September 2009.

Subsequent to this AusCERT referred to strategies being undertaken by the Japanese government and the Japanese CERT (JPCERT) to help detect and clean compromised computers within Japan.

The purpose of this supplementary submission is to explain how the Japanese Cyber-Clean program works, describe its benefits and advocate its adoption in Australia.

Terms of Reference

a) Future initiatives that will further mitigate the e-security risks to Australian internet users;

In AusCERT's previous submission, we identified steps that would more quickly enable compromised computers in the control of criminals (remotely) to be detected and cleaned, specifically:

> At the national level implement regulations which require ISPs to have counter-measures and processes in place, on notification, to help mitigate:
>
> - Distributed Denial of Service attacks
> - Restrict the activity of identified bot hosts used by their customers which are part of the ISP network address range (such as through walled gardens).

If adopted in Australia, the approach taken by the Japanese Cyber Clean program would provide a mechanism to improve the ability detect computers that are compromised with (bot[1]) malware and for the owners and users of these computers to receive professional, dedicated assistance to recover from these attacks with ease and minimal disruption.

By eradicating existing populations of compromised computers (bots) within Australia, it helps prevent further cyber attacks and crimes occurring through the use of these compromised computers.

[1] Bot is short for robot, which is a name given to a compromised computer that has 'bot' malware installed, and which is under the remote control of a cyber criminal.

What is the Japanese Cyber-Clean program and how does it work?

The key function of the Cyber-Clean program is to analyse, test and develop specific file signatures that will clean the computers known to be infected with malware in Japan by eradicating or removing the malware. It achieves this by working with all Japanese ISPs which in turn communicate with their known affected customers. The ISPs direct their customers to the Cyber-Clean Center which provides the solution for their particular type of malware.

Being a tailor-made solution to the specific malware on specific computers, it is far superior and more effective than relying on the user's own anti-virus software to achieve the same result.

Who operates the Cyber-Clean program?

The Cyber-Clean program is funded by the Japanese government and overall control is managed by the Cyber Clean Center (CCC) Steering Committee chaired by two government ministries – Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry (METI).

The Cyber Clean Center and program are operated by the Japanese CERT (JPCERT) in conjunction with an anti-virus (AV) vendor, Trend Micro, under contract.[2] JPCERT conducts the malware analysis and tests the signature developed by the AV vendor and the AV vendor develops specific file signatures for the malware referred to them that will clean the computers known to be infected with malware in by eradicating or removing the malware.

The program requires the cooperation of Japanese ISPs, which notify and communicate with customers whose computers are infected with bot malware and directing them to the Cyber Clean Center.

How it compares with the Stay Smart Online Alert Service

The Cyber Clean program is run by the Cyber-Clean Center (CCC). In addition to the bot eradication, the CCC has a number of other functions including security awareness raising to help owners and users prevent their computers from becoming infected with (bot) malware which cyber criminals use to harvest useful data from the computers and use them to facilitate other cybercrimes and attacks.

[2] Besides the work it does for the Cyber Clean Center, JPCERT operates as the national CERT for Japan and is fully funded by METI.

The awareness raising and prevention activities of the CCC is similar to the Australian government's Stay Smart Online Alert Service provided and operated by AusCERT which aims to keep users' aware of new threats and software bugs which criminals exploit to take control over their computers and information.

However, the Australian government's Stay Smart Online initiative is primarily about cyber security awareness raising to *prevent* cyber attacks. It provides limited **practical assistance** to recover from malware compromises; rather it provides generic advice only.

How it compares with the Australian Internet Security Initiative

The Japanese Cyber-Clean program is a far more complete and effective approach than the Australian ISI (AISI) approach because it directly targets the specific malware itself rather than simply advising the ISPs about compromised computers on their network and asking the ISPs to advise their customers without providing *a specific and reliable* means of helping the customer to recover from the malware compromise.

Other than advising their customers they are compromised with some type of bot malware, the ISPs have no ability to help the customer remove the malware. Being a tailor-made solution to the specific malware on specific computers, the Cyber Clean approach is far superior and more effective than relying on the user's own anti-virus software to achieve the same result.

The ISPs' customers still have the responsibility and cost to eradicate the malware from their computers. The reality is that once malware is on a computer, the ability to reliably detect and remove it through traditional anti-virus (AV) software is limited, due to the features of the malware which disable or bypass the AV software.

In most cases, once the malware is on the computer, it requires professional expertise to remove it and generally involves taking the computer off-line to a computer technician, which can be a costly and time consuming task and even then provides no assurance the malware will actually be removed, given the sophisticated nature of the malware, its ability to hide and subvert anti-virus scanning programs. It is unlikely these computer technicians will use commercial-off-the shelf anti-virus detection tools, which will provide little improvement in the ability to detect malware than users are able to do themselves.

In such cases, where the ability to detect and remove the malware is difficult, AusCERT advocates formatting the hard disk drive and reinstalling all software from trusted sources (after back-ups have been made of user files and settings). The process of formatting and reinstalling software and files tends to be an arduous and time-consuming task and one which most users are reluctant to do. On the positive side it does represent the most reliable means of eradicating serious forms of malware from the computer.

By contrast, the Cyber-Clean program provides a more reliable and option for removing serious forms of malware that is currently not available to Internet users in Australia and one that is far less painful and easier to manage than formatting the hard disk drive.

Goals and benefits of the cyber-clean program

The goal of Cyber-Clean Program is to help prevent direct harm to the owners and users of computers that are compromised, as bot malware often seeks to steal valuable information from the compromised computer to support identity theft and associated fraud.

Secondly, by removing the malware from compromised computers, the Cyber-Clean program prevents these computers being used to support further cyber crimes and attacks. Typically, compromised computers are dual use and most would be used by cybercriminals also to support any number of further cyber crimes and/or cyber attacks such as:

- Send out illegal spam (crime), including that which aims to compromise computers of recipients of that spam (attack)
- Participate in distributed denial of service attacks (attack)
- Host malware web sites (attack)
- Host phishing web sites (attack)
- Host copyright infringed material such as pirated music, movie, software (crime)
- Host child pornography images (crime)

The cyber attacks specifically aim to harm the computers and/or information of third parties. All cyber attacks are cyber crimes as well but not all cyber crimes involve an attack on a third party's computer or information. Most of these activities have a financial motive. Most involve the generation of large sums of illicit revenue.

The Cyber-Clean initiative is important because detecting and cleaning computers that are compromised, ie, infected with malware controlled by criminal elements remotely, is not an easy or straightforward exercise. It is known that most malware is being installed on computers despite the presence of up to date anti-virus programs. **Similarly, once malware is installed, the ability of up to date anti-virus programs to actually detect and effectively remove the malware is significantly undermined due to the ability of many types of malware to evade detection and subvert the anti-virus software.**

Establishing a program like the Japanese Cyber-Clean program, that automates this process, and which utilises the resources and skills of malware analysts on a nationwide scale is an appropriate level of response for the scale and seriousness of the problem that needs to be addressed and which is not able to be effectively addressed by individuals and organisations that have the malware installed on their computers.

The Cyber-Clean program minimises the harm arising from cybercrime and prevents further harm from occurring to the information on the compromised computers and to prevent these computers being used to facilitate further cyber attacks.

The UK House of Lords, Science and Technology Committee, Personal Internet Security, Volume I,[3] concluded that:

> The current emphasis of Government and policy-makers upon end user responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. It is time for Government to develop a more holistic understanding of the distributed responsibility for personal Internet security.

As recognised in the House of Lords report, end-users bear much of the burden and responsibility for their own cyber security but are least able to assess, prevent or mitigate the risks to which they are exposed online. As such many ordinary users' computers and organisational networks continue to be easy targets for cyber attack and as such indirectly contribute to the prevalence of cybercrime and cyber attack cycle.

The Cyber-Clean program is a program that helps address the limited ability of end-users to adequately protect and recover from cyber attacks directed at them.

How does it work?

A diagram and overview of how the CCC works is available online, which includes details of their metrics in terms of samples obtained and disinfection files distributed to the Japanese public.[4]

The numbers of the paragraphs below align with the numbers in the aforementioned diagram.

The Cyber Clean Center both collects and receives information about infected computers in Japan from external and internally derived sources.

[3] UK House of Lords, Science and Technology Committee, *Personal Internet Security*, Volume I, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (2007), page 26

[4] https://www.ccc.go.jp/en_report/200907/index.html

1. Internal sources involve the use of honeypots which are computers in control of the CCC which are used as decoys to get infected.

2. Once the decoy honeypots are infected, the CCC analysts are able to obtain a new malware sample.

3. Analysis involves identifying the attacking source as it is also likely to be a compromised and infected (bot) computer and any other relevant behaviour of the malware which involves connecting to other computers on the internet as part of the attack process.

4. Analysis also involves determining if the sample is already known or a new variant; if the latter then a new disinfection file needs to be developed.

5. Once the new disinfection file is developed, it is added to the suite of other disinfection tools available for download to the Japanese public as required.

6. Information about compromised hosts that are within Japan are passed to the relevant Japanese ISP to notify their customers who are directed to the CCC counter-measures site where they can obtain the appropriate disinfection file for their particular piece of malware.

7. Users (customers of the ISP) who have been notified that their computers have been compromised connect to the CCC counter-measures site and download the tailor made disinfection tool suitable for their particular infection and run it on their computer.

In addition, the disinfection files are also made available to other AV vendors for inclusion in their products.

How effective is it?

The CCC reports monthly metrics on its activities and usage. [5] The monthly reports show the size of the botnet problem in Japan is quite large, but equally, the Cyber Clean program is effective at obtaining new malware samples, developing disinfection files and getting affected members of the public to download them.

Implementation in Australia

If the Cyber Clean program was to be implemented in Australia, AusCERT is already ideally placed to undertake the work that JPCERT does for the Cyber Clean program in Japan,

[5] https://www.ccc.go.jp/en_index.html

given our role as the national CERT and expertise and experience of its staff. AusCERT already operates the government's Stay Smart Online Alert Service and the Stay Smart Online web site we host (www.ssoalertservice.net.au) could host the disinfection files for download by the Australian public.

About AusCERT

AusCERT[6] is Australia's national computer emergency response team (CERT). [7]

AusCERT, which was formally established in 1993, is an independent, self-funded, not-for-profit, non-government organisation, based at the University of Queensland. AusCERT employs around 20 information and IT security experts.

As the national CERT for Australia, AusCERT is the primary point of contact for the provision of advice about computer network threats and vulnerabilities in Australia and provides an incident response service for Australian networks for cyber attacks emanating from both overseas and from within Australia.

Based on its unique operational role, AusCERT helps improve Internet security for Australian Internet users by:

- Detecting, monitoring and stopping Internet based attacks in progress directed at Australian Internet users and networks; and where possible taking further action to mitigate the harm that has already occurred from such attacks;

- collecting, analysing and providing advice about computer network threats and vulnerabilities; and

- providing education and advice about issues affecting Internet security in Australia and globally.

In making this submission, it should be recognised that due to AusCERT's substantial experience monitoring, analysing and responding to cyber attacks in Australia and from abroad for over 15 years, AusCERT has a sound understanding of e-security risks more generally. This understanding extends to a strong technical understanding of :

[6] www.auscert.org.au

[7] In May 2009, the Attorney-General's Department advised AusCERT that the Australian government would take over the role of national CERT from AusCERT and that it would contract AusCERT to provide some services to the Department in support of this role. As the new national CERT is not yet established, AusCERT continues to perform the role of national CERT on a self-funded basis.

- how cyber criminals are able to defeat the security of computer systems, attack computer systems, take control of them and steal data from them;

- how the underlying infrastructure is open to attack and compromise and the limitations of various security related technologies and mechanisms which are put in place in an attempt to prevent or detect attacks.