Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

15-Jun-2007

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2007)15
Unclassified

Working Party on Information Security and Privacy

APEC-OECD WORKSHOP ON MALWARE

SUMMARY RECORD

Held on 22 and 23 April 2007, Manila, The Philippines

Anne Carblanc, tel: +33 1 45 24 93 34; Email: anne.carblanc@oecd.org
Audrey Plonk, tel: +33 1 45 24 15 08; Email: audrey.plonk@oecd.org

JT03229193

English - Or. English

Asia-Pacific
Economic Cooperation

APEC-OECD WORKSHOP ON MALWARE

SUMMARY RECORD

Held on 22 and 23 April 2007, Manila, The Philippines

APEC TEL and the OECD held a joint workshop on malware on 22-23 April 2007 in Manila, The Philippines, in conjunction with the 35th meeting of the APEC TEL. The objectives of the joint workshop were to develop a common understanding of:

- The malware landscape, how it has changed and the most important issues of concern.
- The roles and responsibilities of various communities from governments to vendors to civil society in combating malware.
- The challenges to addressing malware and available mechanisms for combating it.
- How co-operative mechanisms, both domestic and cross-border, can be improved to better combat malware.

The workshop drew over 80 participants from APEC economies and OECD countries, including policy makers, computer security incident response teams (CSIRTs), and representatives from business and civil society communities.

OPENING SESSION

Angelo Timoteo Diaz de Rivera, *Philippines Commissioner from the Commission on Information Communications and Technology (CICT)*, welcomed workshop attendees and noted the Philippines' interest in malware.

Inuk Chung, *Chair of the APEC TEL Working Group*, welcomed participants to the workshop and to the 35th APEC TEL. He reminded them that the first APEC-OECD joint workshop was held in Seoul, Korea at APEC TEL 32 and that ongoing joint work on malware was a result of the success of that first workshop. Dr. Chung noted that the APEC TEL changed its structure to give the important issues of security their own steering group, now the Security and Prosperity Steering Group (SPSG) and highlighted the important work of the APEC and OECD on malware.

Shamsul Jafni Shafie, *Convenor, SPSG-APEC TEL,* and **Keith Besgrove**, *Chair, WPISP-OECD,* discussed the objectives of the Joint APEC-OECD Work on Malware in two tiers: this workshop and the analytical report (currently under development). They highlighted that the workshop brought together

representatives from the various communities addressing malware in order to inform policy makers of the issues and gain a better collective understanding of how to improve prevention and detection of, and response to, this global phenomenon.

SESSION 1 - TRENDS & OVERVIEW: WHY IS MALWARE AN IMPORTANT ISSUE?

Issues and problems, rate of evolution

Yuejin Du, *National Computer Network Emergency Response Technical Team Co-ordination Center (CNCERT/CC) China,* focused on how malware can cause harm by stealing information, abusing computer and network resources, spying on private activities, and by secretly controlling an information system. He noted that "nobody" is behind malware because even the malware writer cannot control the propagation of malware. Types of malware discussed included viruses that destroy personal data and computer systems, trojans, and spyware with hidden and hostile capabilities. For example, new versions of worms can leave backdoors, build up a botnet (deloader to crack passwords), and be used to launch DDoS attacks.

In 2006, CNCERT/CC found 12 million IP addresses in China controlled by botnets. They also found more than 500 botnets and more than 16 000 botnet command and control servers outside China. In addition, CNCERT/CC received over 26 000 incident reports in 2006.

In closing, Dr Du noted that international co-operation should cover all aspects of malware including legal issues, technical issues, information sharing and incident response.

Impact on businesses

Colin Whittaker, *Association for Payment Clearing Services (APACS), United Kingdom)*, detailed the malware threat profile to UK financial institutions. The consequences of malware for financial institutions include direct financial loss, loss of business, impact on shareholder worth, collateral damage through information leakage, and erosion of effective controls. Mr. Whittaker noted that while phishing is not directly malware, phishing attacks are largely successful because malware is controlling infected computers. Mr. Whittaker described increased unique phishing, trojan malware, and money mule incidents from 2005 to 2006. For example, APACS found 18 000 accounts compromised at the end of 2006 with an average loss of GBP 2 000 – 3 000 per customer.

Malware writers are increasingly targeting tools deployed to protect clients from malware. The problem of malware persists because infected customers often stay infected because malware is exceedingly difficult to detect and remove. One recent and growing threat is that of "pump and dump" when malicious actors buy stock at a low price using compromised computers (bots) and subsequently "pump" up the value of the stock at which point the malicious actors sell the stock for a much higher price. Despite the increased occurrence of malware and the increasingly deceptive techniques of malicious actors, APACS reported a steady increase in online banking customers from June 2000 to December 2005.

Impact on government

Sabeena Oberoi, *Department of Communications Information Technology and the Arts (DCITA), Australia,* focused on malware as a public policy issue and highlighted to workshop participants that due to the interconnected nature of the online environment, a holistic approach to the problem needs to be taken. She outlined that the protection of home users and SMEs is a significant element in the protection of government networks and critical infrastructure. Home users and SMEs are the weakest link as their appreciation for the need for e-security is often low. A recent survey shows that only one in seven Australian online users have firewalls and about one in three use up-to-date virus protection software. This shows that a large number of online users may be exposed to e-security threats. For example, last year

over 170 Australian citizens' personal information was compromised by a Trojan known as Haxdoor. This compromise was not due to a flaw or attack on the Australian online tax system, rather the lack of appropriate security protection on these computers.

It was indicated that malware is an important issue for governments because it can seriously affect their ability to conduct business online and maintain the critical infrastructure.

Malware presents many policy challenges because it is a global problem that is evolving at rapid rates. Continued growth of online users will result in more targets for online crime.

Impact on government

Satoshi Murakami, *Ministry of Internal Affairs and Communications, Japan* and **Masayasu Murano**, *Ministry of the Economy Trade and Industry, Japan,* focused on anti-bot countermeasures in Japan. They reported that an average of 70 kinds of malware, including bots, are detected each day and 400 000 – 500 000 Internet users in Japan are affected. In 2006, Japan began a project to reduce the number of bot infected computers in Japan. The objectives of the project include preventing infections (in co-operation with anti-virus software vendors), and blocking spam e-mails and cyber attacks originating from bot infected computers in Japan (in co-operation with ISPs). To accomplish this, Japan created a bot removal tool known as "CCC cleaner" which can be downloaded free of charge at ccc.go.jp.

Current results from the project include 31 000 trapped bot programs (hash unique) and 1 300 bot programs reflected in the removal tool. To date, a total of 57 000 users in Japan have downloaded the removal tool. Next steps for enhancing the project could include changing the composition of honeypots and broadening the reach of ISPs.

Impact on consumers

Beau Brendler, *Consumer Reports WebWatch and StopBadware.org*, focused on the impact of malware on consumers. Consumer Reports WebWatch is US-based but has done Internet governance work with Malaysia, Thailand and Europe though Consumers International and the Trans Atlantic Consumer Dialogue (TACD).

StopBadware.org, a joint venture of WebWatch, Harvard Law School and Oxford University, reports 59 million Americans have spyware or other types of malware on their computers. Consumer Reports surveys in 2006 show US home PC users paid as much as USD 7.8 billion over two years to repair or replace computers infected with malware, while, in contrast, only 21% have enabled anti-virus protection software or installed firewalls on their machines. In the United Kingdom, more than 20 pieces of spyware exist for every PC. Consumer education on malware issues has been difficult. Consumers have trouble understanding the nomenclature and technical terms and issues, or are simply indifferent. In addition, in the United States there is little to no legal or legislative protection from spyware. Cybercrime laws across countries are not harmonised. And makers and purveyors of adware and badware often argue successfully in its favour from a marketing and free speech perspective.

SESSION 2 – MALWARE IN FOCUS

Malcode

Kevin Houle, *Computer Emergency Response Team / Co-ordination Center (CERT/CC),* focused on the exponential growth and trends in malicious code as well as challenges to addressing the problem. He noted that characterisations of malware are not as important as functional explanations. He also noted that

the information and statistics given were only one organisation's perspective and that no single organisation has a grasp of the complete malware picture.

In March 2007, CERT/CC reported 90 000 new malware artifacts; an unprecedented amount. Currently, the security community is reacting to problems of yesterday. Analysis of malware takes significant time and expertise and thus it is challenging to prioritise analysis. As a result, discussion of malware often addresses only surface level details rather than the much needed in-depth analysis.

It is important to recognise that not all computer security incident response teams (CSIRTs) are alike. While a global community of CSIRTs is being created, there is a need for this development to happen at a much faster rate. Furthermore, there has recently been a convergence between incident response and forensics as incident response is shifting toward law enforcement. Because forensics is always resource-starved, it might be useful to have national CSIRT teams' expertise co-located with law enforcement expertise.

Current information sharing is based on well-established, and often personal, bilateral relationships. Real-time sharing of statistics between CSIRTs is limited and CSIRT co-ordination with government varies according to that CSIRTs' scope of responsibilities.

Botnets

Douwe Leguit, *Computer Emergency Response Team for the Dutch Government (GovCERT.NL) – The Netherlands,* focused on botnets and how they are used to commit cybercrime. A bot is an autonomous program that performs actions without user intervention. Bots can be used for good things such as searching for information; however, malicious bots allow the complete compromise of information systems. A botnet is a large number of bots under the control of a one actor, often known as a "bot master". Botnets are controlled though command and control servers.

Botnets have been more successful and become more prevalent with the development and uptake of broadband because it allows more computers to be compromised at a faster rate. For example, in early October 2004, a botnet of only 4 000 computers – small by today's standards – launched denial of service (DoS) attacks that took down several government websites in The Netherlands. The Netherlands has recently reported botnets that average between 100 000 bots and up to 1.5 million bots.

Malware, and in particular botnets, is a profitable business and therefore bot masters are concerned about business continuity of the infrastructure. Botnets are the infrastructure for cybercrime and because they provide for successful cyber attacks, criminals are deploying techniques such as encryption and root kit technology to keep their botnets from being detected and "taken down". Malicious actors are also beginning to use smaller botnets to evade detection.

There are several challenges to combating botnets including privacy, consumer education, and co-operation across the responsible communities (*e.g.* CSIRTs, ISPs, AV vendors etc.). For example, IP addresses are sometimes considered private information and therefore cannot be shared with CERTs, ISPs or other organisations who may be responsible for taking a botnet "offline". It is important to note that there are differences among ISPs and their policies and procedures for intervening. Consumers often do not realise they have been compromised and when they do realise, they do not have a place to go for assistance. Finally, authorities are often forced to decide whether to "take down" the botnet and possibly destroy crucial evidence for identifying and prosecuting the perpetrators, or leave the botnet active to attempt an investigation while also risking the compromise of more users.

Who is behind malware, their capabilities and activities?

Sergio Staro, *Postal and Communications Police Service, Italy,* focused on capabilities and motivations of malicious actors. Malicious actors use malware for fun, to commit crime, or for ethical or political motivations. While statistics on the number of computer attacks exist, they are often not realistic because the actual numbers are higher than those reported, as many people and organisations who are victims do not report the incident to authorities.

One significant challenge to addressing malware is the lack of harmonisation of cybercrime laws across countries – some countries may not have any laws while others may have laws that are inadequate or not properly enforced. One simple solution could be the adoption of the Council of Europe Convention on Cybercrime because it allows for the harmonisation of legislation. There is also a need to prioritise crimes such as those against the critical infrastructure, organisations and civilians.

Collaboration with the private sector and international partners is critical for success in combating malware. The Botnet Task Force initiative (international collaboration with law enforcement and the private sector) is one example of such collaboration. There is also a need for effective points of contact between government and private sector to facilitate a timely exchange of information. The G8 24/7 points of contact network is an example of such co-operation and is open to non-G8 member countries.

What are the challenges (all types) to combating malware?

David Pollington, *Microsoft UK,* focused on the evolving threat landscape, prevalence, and impact of malware. It was noted that the use an actor makes of any software determines whether or not it becomes malware. The software itself is not malicious but rather the intent and motivation of the person using it.

The malware threat landscape has evolved to include social engineering, hyperjacking, application attacks, and targeted attacks. In 2006, Microsoft found that backdoor trojan malware accounted for 62% of malware cleaned from computers running the Microsoft Malicious Software Removal Tool (MSRT).

SESSION 3 – IDENTIFYING COUNTER MEASURES AND CAPABILITIES FOR RESPONSE TO CYBER ATTACKS

Current counter-measures and responses by CERTs

Jeong, Hyun-Cheol, *Korea Internet Security Center* KrCERT/CC, described the role of a CERT as the responsible body to receive and filter incident reports.

Malicious code injections are very serious in Korea and malicous code attacks are considered serious cybercrime. Attackers are making money from attacking banks and online games. An unprotected PC can be infected within 30 minuters of being connected to the Internet. Case studies show that rapid reaction to incidents is important and that international co-operation and information sharing could improve the response. One countermeasure used by KrCERT/CC is the implementation of MCFinder (Malicious Code Finder) which locates malware on compromised websites. MCFinder identifies an average of 500 exploited websites every month in Korea.

Current counter-measures and responses by product and anti-virus vendors

Patrik Runald, *F-Secure – Finland,* focused on malware counter-measures by anti-virus vendors and noted that the information provided by F-Secure is based on data gathered from customers running their products. F-Secure maintains a map of the world that tracks malware (http://www.f-

secure.com/security_center/virus_world_map.html). Using a honeynet on a dark space on the Internet, F-Secure catches automated traffic in order to understand the geographic origins of malware.

F-Secure receives an average of 15 000 files – and as may as 70 000 – per day from their product users as well as CSIRTs and others in the security community. Anti-virus vendors like F-Secure need these malware samples to detect malware through signatures and update the signatures on the anti virus software. Although signatures are very important, it was noted that signature-based detection alone is not sufficient for combating malware. When files are received, F-Secure undertakes a process to determine if the file is indeed malicious. This is done by confirming from other vendors, conducting automated analysis, or by conducting manual analysis (conducted only when other methods fail to determine the maliciousness of the code).

If a file is deemed malicious, F-Secure releases a detection and sends an update to their customers. It takes about 40 minutes to go through the cycle and they release an average of 10 updates per day. It would be impossible to report everything due to the overwhelming quantity of files they receive daily.

Current counter-measures and responses by regulators in partnership with Internet service providers (ISPs) and domain name registrars

Horacio Cadiz, *Philippine Internet Services Organisation (PISO),* focused on counter-measures by regulators in co-operation with ISPs. ISPs traditionally do not monitor the data passing through the pipes (Internet) for subscribers of their transit service due to privacy and other legal considerations. However, for hosted services (web, e-mail, and the like), ISPs do maintain certain levels of monitoring to implement their Acceptable Use Policy agreements. In the Philippines, ISPs have a "take-down" policy in case of a violation of an Acceptable Use Policy (AUP); however to date this take-down has not been invoked.

In The Philippines, if PISO receives a lawful order from a competent government authority to remove a computer from the Internet, they will comply; however, they do not generally respond to other non-binding requests from other parties.

The Philippine top level domain (TLD) is a united registry but without community oversight. The CICT Memorandum of 2004 has not been fully implemented and therefore nobody knows many domain names exist in The Philippines. Other efforts in The Philippines include: *i*) Anti cybercrime bill in the congress; *ii*) Establishing a national CERT; *iii*) Signed Seoul-Melbourne MOU.

Current counter-measures and responses by the domain name system community

Paul Twomey, *Internet Corporation for Assigned Names and Numbers (ICANN),* focused on threats to the Internet infrastructure and counter-measures by the domain names system community. ICANN's role is to co-ordinate the allocation and assignment of the three sets of unique identifiers for the Internet (domain names, Internet Protocol (IP) addresses, and protocol port and parameter numbers), operation and evolution of the DNS root name server system, and the development of policy related to these technical functions. One hundred and twenty governments sit on the advisory committee in ICANN.

The threats to the Internet infrastructure include: *i*) physical disruption of major lines and switching centers; *ii*) loss of routing infrastructure continuity and/or fidelity; *iii*) loss of DNS service continuity and/or fidelity; and, *iv*) flooding of network or specific site. It is important to note that not all Internet-based systems are Internet infrastructure. Routing information is maintained in routing registries where it is relatively secure from physical attack but inputs to the routing registries could be compromised and false routing information could be compromised.

Normal DNS traffic continues to increase at the rate of about 100% every month. The three levels of threat to the DNS infrastructure include: *i)* loss of service; *ii)* hijacking; and, *iii)* loss of coherence. While there is significant work underway to secure the infrastructure, it is going to take more time and money than people are willing to spend to fully address the problem.

System threats include distributed denial-of-service attacks (DDOS) against high-value targets such as DNS servers and domain and address theft. In some cases, domain name theft can be covered by ID theft laws; there is no legislation that specifically makes stealing address space illegal. Although motivations for attacks on the Internet infrastructure are unclear, they could be devastating. For example, the February 2007 attack on root servers affected 6 of the 13 servers; however, most users were not affected. By contrast, a series of amplified, distributed DDOS attacks in 2006 resulted in disruption of DNS services in a minority of cases. One of the victim DNS providers was sent the equivalent of 150 million queries per second. There is not a single country code operator in the world that could withstand this scale of attack.

One possible solution for securing the DNS infrastructure may include the implementation of DNS Security Protocol (DNSSEC). Sweden and Bulgaria have moved their country code TLD to DNSSEC; however, it is important to have government, business, banking, and registry co-operation to successfully implement DNSSEC.

Current counter-measures and responses by law enforcement bodies, including through public/private partnerships

Anthony Teelucksingh, *Department of Justice (DOJ) – United States,* focused on counter-measures by law enforcement. In his introduction, Mr. Teelucksingh noted that while law enforcement can have a deterrent effect on criminals, cybercrime is not only a law enforcement problem.

In the United States, writing malware is not criminal conduct, but releasing it is. An attack on a US infrastructure or a US computer connected to the Internet is a crime in the United States and can be indicted. Indicting and bringing a person for prosecution are two different and equally difficult matters. It is generally preferable that countries develop adequate legal frameworks for cybercrime so that perpetrators can be prosecuted domestically. In addition to developing legal frameworks, it is important for countries to commit adequate resources for training police, judges, and prosecutors.

Information sharing among law enforcement entities is challenging. Co-operation and prompt exchange of evidence are needed, as well as joint investigations where appropriate. One available mechanism is the Council of Europe Convention on Cybercrime that binds signatories of the convention, and ensures a level of information sharing and co-operation among designated parties.

One example of domestic co-operation is the US INFRAGARD program. The US established the INFRAGARD program to improve and extend information sharing between private industry and the government, including law enforcement, on threats to critical national infrastructures. Examples of international co-operation include the Botnet Task Force, the Forum for Incident Response Security Teams, the G8 24/7 Network, and the ASEAN Regional Forum.

Presentation of a case study on a cyber attack from beginning to end with international dimensions

Graham Ingram, *Australian Computer Emergency Response Team (AusCERT), Australia*, introduced a case study consisting of related cyber attacks using spam e-mail to infect computers around the world over a six month period [see Annex]. He then moderated the discussion among the above-mentioned speakers and an additional panellist (Douwe Leguit from Govcert.nl), based on the following set of questions:

Is there a need to respond?

All participants agreed that in the event of an attack such as the one presented in the case study, there would be a need to respond and co-ordinate across multiple communities.

What is the threshold to react?

The case study demonstrated that for law enforcement to take official action there must be a nexus with their domestic legal frameworks. In the United States, the crime must involve a US citizen or a computer in the United States.

Would a request to Domain name registrars to remove the DNS be reasonable?

The case study demonstrated that existing agreements prohibit registrars from damaging a third party; however, they can deregister a registry in some cases. While removing DNS information by registrars is possible, it is currently done informally. One problem is that if criminals are taken offline they probably will not complain, but if a legitimate company or user is taken offline it could result in a lawsuit. In the United States, there is a safe harbour provision for ISPs but not registrars, so it is more difficult for registrars to remove the DNS. Another challenge is the harmonisation of the country code domains; there are 143 country codes in the world that set their own policies which are not necessarily harmonised or co-ordinated.

Which organisation is best placed to lead/co-ordinate the response?

The case study demonstrated that there is no clear answer for who co-ordinates response to an attack, but rather it varies depending on the country. CSIRTs often conduct the technical analysis and then pass the information to anti-virus vendors so that signatures can be updated. If the attack is deemed a crime, law enforcement is competent and would be involved. However, it was generally agreed they would not be best placed to lead the response due to information sharing constraints.

What is the role of the user? Should users be informed of compromises and information breaches?

The case study evoked three priorities for end users: *i*) stopping the attack; *ii*) mitigating further damage; and *iii*) investigating the attack. It demonstrated that the most important issue for users is stopping the attack. It was noted that users themselves do not have the knowledge or ability to stop the attack and thus are reliant on security experts. The second most important issue for users is mitigating further impacts of the attack and distributing the necessary information to users. It was noted by anti-virus vendors that while they agree that informing users is important, there are so many issues that they could easily overwhelm the users with too much information. The final priority for users is that law enforcement investigates the attack and brings perpetrators to justice.

What role does public policy play?

The case study demonstrated that government response must occur at both the policy and operational levels. It also highlighted the importance of giving users helpful information they can understand and apply, versus scaring them with complex information about threats they may not understand.

Should compromised computers be taken off the Internet?

Some participants noted that the focus here should be on co-operation with industry, in particular ISPs. Arrangements must be agreed on and put in place before an incident for effective co-operation to be realised. For example, ISPs have case resolvers and can potentially give early warning of incidents.

Final comments

Participants noted that the security community should be more aware of CSIRT activity as there is a need to share information across communities about incidents.

Participants suggested that perhaps a notice to the ISPs would be sufficient to have them notify their customers to clean up their systems. ISPs do not want to act unilaterally, but rather in a co-ordinated manner, to ensure there is no abuse of the ability to take users offline. Vendors noted that ISPs should take more responsibility for taking machines "offline," and that effective automated tools already exist.

Case study participants agreed that the goal should be to develop a structured, organised approach that works.

SESSION 4 – PANEL DISCUSSION: GAPS AND CHALLENGES

Sabeena Oberoi, *DCITA, Australia*, **Pei-wen Liu,** *Information & Communication Security Technology Center, Chinese Taipei*, **Suresh Ramasubramaniam**, *Outblaze Limited, Hong-Kong, China*, **Dr. Yuejin Du**, *CNCERT, China*, **Rosemary Sinclair**, *International Telecommunications Users Group (INTUG)*, and **Ravi Sahita**, *Communications Technology Labs. INTEL,* discussed major themes highlighted during the workshop such as user awareness, government's role in combating malware, the evolving nature of malware, the speed at which attacks occur, and whether or not disconnecting infected users is a viable response. Highlights from the discussion include:

- There is a circular dependence of software on software platforms and legacy problems.
- Malware is difficult to control – spreads quickly and the end user is most vulnerable and with the least understanding.
- Users need a clear, simple message. People should know when they have been compromised and find a way to report. There should be mechanisms available to assist them. Awareness and education will not reduce the malware risk completely. Ensuring the privacy of the users is also very important.
- Governments should consider the security implications of broadband.
- Many regions of the world are not aware and not taking action – Africa, Nigeria, Brazil, and Eastern Europe.
- There is a need for more secure end points and an understanding that not all activities and resources should be connected to the Internet.
- It was noted that disconnecting users from the Internet would deprive them of access to ICTs, which is one of the primary goals of the APEC TEL's mandate. Perhaps something similar to the Internet Security Initative in Australia would be a useful alternative to disconnecting infected users from the Internet. The program sends IP addresses to ISPs so they can contact the customer. Most customers have no idea and are very eager to rectify the situation. In Australia, for example, there is a provision that allows ISPs to disconnect customers if they do not adequately respond to being notified of a compromise.
- In the near future there may be cases of malware that cannot be removed and thus this community should be thinking about the complex problems to come.

Day 2 –23 April

SUMMARY FROM DAY 1

Andy Purdy (moderator), *BigFix/DRA Enterprises,* highlighted the reoccurring themes of our dependency on the Internet and connected information systems, the serious threat environment, and the need for international collaboration. He challenged participants to further explore these dependencies and vulnerabilities and work toward enhanced collaboration in priority areas. He made a case for enhanced international collaboration in light of the dependency and the risk. Mr. Purdy suggested that some major areas for strategic and operational collaboration might be: *i*) Resiliency/risk; *ii*) response/preparedness; *iii*) Research and development.

SESSION 5 – BREAK OUT GROUP DISCUSSIONS

Participants split into three break out groups [see Session 6].

SESSION 6 – WRAP UP AND GENERAL DISCUSSION ON POLICY

Report by Breakout Group Moderators

Break Out Group 1 - Colin Whittaker: *How can vendor, CERT, ISPs, domain name registrars response be improved?* Break Out Group 1 recognised that there is no one silver bullet to solving the problem of malware. It is necessary to engage with key policy makers to develop coherent policies and ensure adequate resources to implement them. In addition, resources for research should be improved.

Efforts to establish CSIRTs around the world should continue, especially in areas where they do not exist at the government and national levels. Options for responding to incidents by mitigating their possible effects (*e.g.* quarantining users' PCs) should be considered. However, it is important to strike a balance between response that leads to prosecution and response that stops an attack.

Incentive structures need to be developed to encourage all stakeholders to apply good information security policies. Efforts to educate users should begin early on.

Break Out Group 1 noted the work by the OECD on spam and the development of the Spam Tool Kit and suggested developing a similar toolkit for Malware.

Break Out Group 2 - Anthony Teelucksingh*: How can government policy, law enforcement and regulatory response be improved?* Break Out Group 2 noted three models for domestic regulatory structure:

i) In some countries, a non-law enforcement government agency or agencies have plenary authority – complete power to investigate and prosecute criminals – and regulatory authority.

ii) In some countries, non-law enforcement government agencies do not have plenary authority and thus need law enforcement to participate in investigating and prosecuting cyber attacks. This often results in a slower response.

iii) In some countries, there is not existing or adequate cybercrime legislation and thus no organisation or agency has authority to investigate cybercrime.

Break Out Group 2 also noted the following as possible areas for improvement:

- Joining the Convention of Cybercrime provides substantive and procedural mechanisms for investigating cyber crime domestically, and can apply to both modes one and two mentioned above.
- Work to increase risk to criminals who conduct malicious activity online such as through stringent legal frameworks that increase the consequences for committing crime online, as well as other technical and policy countermeasures to decrease the success of attacks.
- Law enforcement could work as an active partner with all stakeholders.
- ISPs could develop voluntary codes of practice where regulation does not exist or is not feasible.

Break Out Group 3: *How can awareness, education, and training of individuals, business – in particular small and medium-sized enterprises (SMEs)* – and users be improved? **Ernie Newman**. Break Out Group 3 stressed that the problem of malware is getting worse, especially for end users and small and medium-sized enterprises (SMEs). The general public does understand the problems with computers (such as worms, viruses, etc.); however, they do not understand the affects that security compromises can have on other assets such as the critical infrastructure. Children represent the future generation of computer users and therefore should be educated about security from an early age. ISPs have a low margin business, but are probably in the best position to do something about botnets. ISPs should compete on safety and security practices rather than bandwidth and number of customers. Governments could consider establishing a trusted agency to audit public agencies – similar to airline safety.

Some possible actions to assist end users and SMEs to cope with malware:

- Compulsory PowerPoint for users when they renew their antivirus or firewall software.
- Establish an Internet Safety Week to raise awareness among all users.
- Work to drive people to trusted websites for customers.
- Include computer security in school curriculum.

General discussion on how government policy and international frameworks for cyber response/security can be improved, and final wrap-up

Andy Purdy, *BigFix/DRA Enterprises*, highlighted the need to work across our economies to address the issues of malware and focus on the areas of the greatest concern. He stressed that the necessary actions cut across issues tackled by all three breakout groups. He noted the importance of learning from past lessons and events to adequately prepare for future events.

To accomplish this, Mr. Purdy suggested that the APEC and OECD could continue to bring together stakeholders across a variety of communities to develop a framework – a collaboration model – for working together to assess and mitigate cyber risk of importance to the global information infrastructure. Such a collaboration framework could build on efforts in different economies, learn from them, and prioritise joint efforts for the future.

Conclusions and next steps by APEC and OECD

Based on the workshop discussion, **Shamsul Jafnie Shafie** and **Keith Besgrove** highlighted the three following conclusions:

- There are variations across countries.

- There is no clear organisation of roles. There is a need for structured co-ordination at national and international levels with involvement of all stakeholders.
- Response and mitigation are mainly reactive. There is a need for strategic and proactive collaboration of all stakeholders.

They also suggested that possible recommendations for APEC-OECD could include developing a collaboration model at both **operational and strategic levels**:

- **Operational** cross-border co-operation against malware / e-attacks. Policy framework for cross-border co-operation against malware / e-attacks (operational objectives - non binding) could work toward:
  - Establishing domestic frameworks.
  - Improving the ability to co-operate.
  - Improving procedures for co-operation.
  - Co-operating with relevant private sector entities.
- **Strategic** collaboration:
  - OECD and APEC could consider an annual conference of public and private stakeholders regarding the risk to, and efforts to promote resiliency of, the Internet and connected information systems.
  - In addition, such a group might consider convening virtual meetings/work streams of key stakeholders during the year between conferences to focus on co-ordinating mitigation of priority cyber risks.

ANNEX

APEC-OECD MALWARE WORKSHOP – SESSION 3 CASE STUDY

PRESENTATION OF A CASE STUDY ON A CYBER ATTACK FROM BEGINNING TO END WITH INTERNATIONAL DIMENSIONS

Presenter - Graham Ingram, General Manager, AusCERT

Summary and objectives of the attack

- Series of related cyber attacks that occur over approximately a six-month period.
- In the public domain.
- Uses spam e-mail as the initial propagation vector which leads to the infection (compromise) of the computers of many thousands of Internet users around the world.
- Country A is most affected although countries B, C, and D are also greatly affected.
- Principal attack tool is several variants of a multi-functional trojan and associated malware.
- The trojan enables the system compromise of vulnerable computers.
- Captures and transfers passwords, other online access credentials, and web form data.

Attack description

1. Spam e-mail is sent with the following content:

   Subject: National Bank goes bankrupt?!

   People starting panic withdrawals, some of the accounts were reported closed due to technical reasons, many ATMs are not operating. Does it seem that one of the Australia's greatest goes bankrupt?

   The full story could be found here: http://www.compromised-domainA.com/news.php[1]

   Well, hope that isn't true... Anyway You'd rather check your balance...

2. User clicks on the link http://www.compromised-domainA.com/news.php

3. When the user's machine connects to the URL a commercially available piece of malware profiles the operating system, service pack and web browser of the user to determine which exploit (malware) may be most effective at compromising the computer

4. If a vulnerable system is detected, the user's computer is immediately redirected to another web page within the same domain.

[1] As the attacker compromised a computer using a legitimately owned and registered domain, the domain name has been changed for the purposes of this case study.

5. When the user's machine connects to the new URL, an exploit suited to compromising that computer is downloaded, thus compromising the user's computer.

6. The browser of the compromised computer is then directed to another page within the same domain where a trojan dropper is automatically downloaded.

7. Once installed, the trojan dropper is programmed to connect to another URL in a different domain.

8. When this connection occurs, the primary trojan (a Haxdoor variant) is downloaded and installed on the user's computer.

9. The trojan disables various security counter-measures.

10. The trojan systematically extracts stored passwords from the computer and captures web data, including access credentials for web sites visited.

11. The captured data is sent to a domain controlled by the attacker and the attacker harvests the data on a regular basis.

Features of the attack include:

- Compromised hosts using legitimate domains involved in the attack are located in several countries.

- Registered fraudulent domains involved in the attack are registered in several countries.

- Around 6GB of text was captured over the 6 month period. A subset was distributed to over 100 organisations within country A which had customers/clients/users computers compromised and trusted third parties in several other countries for their constituents who have compromised (captured) data.

- 34 553 computers compromised (by unique IP address) around the world.

  - 149 countries with compromised computers.

  - 11 449 compromised computers within country A, with 33% of total infections.

  - Countries with the highest number of infections, in order:

Country	Number of compromised machines	Percent of total compromises
A	11 449	43%
B	4 889	25%
C	3 605	20%
D	2 459	12%

Possible goals for responding to a cyber attack of this nature:

- Stop an ongoing attack and prevent further compromises.
- Mitigate existing damage for those who have already been compromised.
- Investigate, identify and prosecute attackers involved in the attack.

Sample of possible actions:

- Issue a public security threat alert.
- Request to disconnect and/or clean computers hosting separate legitimately registered domain names.
- Request to deregister domains fraudulently registered to support the attack.
- Identify and request closure of open mail relays and/or compromised hosts being used to send the spam.
- Analysis of multiple malware samples acquired.
- Requests for analysis from other parties, including AV vendors, for malware samples acquired.
- Submission of malware samples to anti-virus vendors for updating signature patches.
- Request that antivirus vendors include the malware signature in their antivirus products.
- Request for log files from ISPs.
- Notification and distribution of compromised log files to appropriate trusted parties, such as national CSIRTs or appropriate contacts within organisations (such as banks or government agencies) whose customer data has been compromised.

Questions Round 1 – for all panelists

1. Is cyber attack response in cases like this desirable or necessary?

    a. If so, what does a response seek to achieve, *e.g.* stop ongoing attack and prevent further damage; mitigate existing damage, identify and prosecute perpetrators

    b. Are all goals possible or realistic?

    c. What are the criteria for responding? For example: type of vulnerability; number of compromised machines, type of data being captured, evidence of specific targeting vs. indiscriminate targets etc.

2. Who/what community would learn of this incident first (*i.e.* CSIRT, vendor, government etc)?

3. What communities would have a role in responding?

4. Could it have an impact on critical infrastructure or government services?

5. If you were country A, would you have a role? If B? If C? If D?

6. What is the threshold for engagement in cross-border co-operation?

7. Which organisation/s would be the best placed to lead or co-ordinate the response? Are there existing thresholds for engaging?

Questions Round 2 – specific questions for each community

Questions for Computer Security Incident Response Teams (CSIRTs)

1. How would your CSIRT learn of this incident?

2. To what extent would your CSIRT take action? What action would be taken? How quickly would you be able to respond?

3. What would your response entail?

4. What impediments (legal, resources, expertise or other) exist which may prevent a response?

5. What impediments (legal, resources, expertise or other) exist which may prevent your CSIRT from taking action against similar types of attacks directed at constituents in your jurisdiction?

6. What problems arise from attempting to redistribute compromised log data to organisations within your constituency?

7. Would you communicate and co-ordinate a response within your economy, the private sector or the international community?

Questions for ISPs

8. What policies and procedures exist to disconnect a host which a trusted third party (such as a CSIRT) alleges is compromised and/or serving trojan malware to visitors to a page, hosted by the computer?

9. Which organisations would you regard as 'trusted' for the purposes of accepting and responding to their request? (*e.g.* some will only respond to a local law enforcement request).

10. Are such policies and procedures common within the industry?

11. Do you notify the customer or consult with the customer prior to taking action or determining an appropriate course of action?

12. How quickly are you able to respond?

13. What does your response entail?

14. What impediments (legal, resources, expertise or other) exist which may prevent a response?

15. What policies and procedures exist to recover log files and malware artifacts and provide them to a trustworthy third party (such as a CSIRT) from such hosts to help mitigate the harm which may ensue from the captured data?

16. What impediments (legal, resources, expertise or other) exist which may prevent a response?

17. Do you believe the ISP has a role to help mitigate this type of attack and minimise further harm arising from the attack?

18. What other actions do you believe ISPs could effectively implement to help prevent and/or respond to such attacks in future?

Questions for anti-virus vendors

19. What is the process for finding new malware and deploying the new signatures to AV products?

20. What techniques do attackers use to create new, undetectable variants of malware?

21. What priority is given to updating signatures for propagating (virues and worms) versus non-propagating malware such as Trojans, backdoors, droppers etc.

22. A number of CSIRTs report that a majority of the Trojan malware being discovered that is designed to steal credentials and personal information (inter-alia) is not detectable by up-to-date AV products at the time they discover the malware in public circulation.

23. What can be done to improve the effectiveness of detection and signature release times?

Questions for the domain name system community

24. What policies and procedures exist to deregister a domain which a trustworthy third party (such as a CSIRT) alleges is being used for fraudulent or other criminal purposes, including hosting a phishing site or a trojan malware to visitors to a page, hosted by the computer?

25. Are such policies and procedures common within the industry?

26. What impediments (legal, resources, expertise or other) exist which may prevent a response?

27. If so, what is a reasonable response time?

28. Do you believe the domain name system community has a role to help mitigate this type of attack and minimise further harm arising from the attack?

29. What other actions do you the domain name system community effectively implement to help prevent and/or respond to such attacks in future?

Questions for law enforcement

30. What is an appropriate or inappropriate response from law enforcement?

31. If you consider these attacks to be illegal within your jurisdiction, do you believe law enforcement should routinely be involved in responding to all incidents?

32. What impediments (legal, resources, expertise or other) exist which may prevent a timely response?

Questions Round 3 – for the audience

Questions for software vendors

33. In addition to social engineering (deceiving humans to take an action that aids the compromise process), the attackers exploited software vulnerabilities in a web browser. What are software companies doing to help prevent such attacks in future?

Questions for end-users, civil society and SMEs – individuals and organisations with compromised data due to the trojan infections

34. In some cases, it is possible to provide organisations details of information about their customers or clients who have compromised data captured. Those institutions may or may not notify particular individuals of the compromised computer and their compromised data.

35. In some cases, it is clear that computers belonging to organisations are compromised. Is this something that individuals or organisations have a right to know in the event that CSIRTs or law enforcement agencies receive details of captured data?

36. If so, who should should take the lead in notifying all these organisations and/or individuals, assuming it is possible to find appropriate contact details for them and could pass the data securely (typically using encryption electronically) to them.

37. How would you "recover" from the incident if you were compromised?