Making the Internet Clean, Safe and Reliable

Asia Pacific Regional Collaboration Activities

Yurie Ito
Chair
Asia Pacific Computer Response Teams (APCERT)
Tokyo, Japan

Abstract— **This paper introduces Asia Pacific Regional Collaboration activities for making the Internet Clean, Safe and Reliable.**

Keywords-component; Asia and Pacific; Internet Clean up; Common good; Confidence Building Measures in Cyber Crisis, Incident Response

I. INTRODUCTION

APCERT is a coalition of the forum of CSIRTs in the Asia Pacific. The forum was established in 2003 to support the member CSIRT teams in achieving more effective incident response. There are 27 member teams from 18 economies working together within the APCERT forum. APCERT members are Incident Response Teams that serve the constituents located geographically within the region served by APNIC.

The members have built trust and operational collaboration across regions with significant cultural differences. Each economy has a different approach to governmental control of information and the related authority over ISPs to block traffic. For example, while action by ISPs can be directed by the National CSIRT in certain nations (which is part of the government), a National CSIRT in a different economy may only request action from the ISPs, but have no authority to compel action. Members have come to learn the variety of authorities and operational processes used by members, understand how this impacts the speed at which others can react when a request for Incident Response assistance and broader information sharing between members are received.

II. NEW VISION OF 2011

After 9 years of successful collaboration and activities, APCERT revised its vision at the last Annual General Meeting in March 2011. The new vision is; "APCERT will work to help create a Safe, Clean and Reliable Cyber Space in the Asia Pacific Region through global collaboration." While each member CSIRT serves its own constituency for security incident response and Information Infrastructure Protection, and APCERT members support each other to achieve that mission. APCERT also looks to serve as a regional collaboration forum for members to work together to act for improving a shared common good – the Internet.

A. A New Mindset – Treating the Internet and its health as a connected common shared infrastructure

The members have had the core realization that motivates effective responses to cyber-security threats. This is: "my security depends on your security." In addition, members understand just like air and water are shared resources, routing and addressing within cyber space are also common shared resources of the infrastructure. Ecosystems must react to disruptive forces. There are a number of global environmental regimes and norms that have been developed as transnational initiatives. Similarly the Internet ecosystem faces significant challenges and we need to begin to think of solving problems at a global level and using strategies and approaches that work to improve the ecosystem and its health in addition to protecting against and reacting to specific threats and incidents. The APCERT members realize the need to jointly work and that global efforts are required to solve common cyber security challenges. We plan to contribute to making the Internet ecosystem cleaner and healthier as a basis for improved cyber security in the Asia Pacific as a mutual gain for all in the long-term.

III. MAKING THE INTERNET CLEAN

National level initiatives already exist that support such a "Clean the Ecosystem" approach in the region.

Australia has the Australian Internet Security Initiative (AISI), operated by ACMA with 102 ISP members collaborating on the initiative. ACMA collects compromised IP addresses data from trusted sources, validates the information and passes that to member ISPs. The ISPs then identify the customer and notifies them. It is a voluntary program, but ISPs are expected to provide notification of infection and some guidance on how to fix the problem. The Australian Internet Industry has adopted a standardized, voluntary code for action on compromise through the "icode". "icode" is the Cyber Security Code of Practice in Australia, which came into operation 1 December 2010. It was developed jointly by the Internet Industry Association (IIA), Department of Broadband, Communication and the Digital

978-0-615-51608-0/11 ©2011 EWI

Economy and the Attorney-Generals Department. One of the recommended types of action given in the code is that ISPs participate in the AISI and act on the compromised report. The code also recommends working closely with the Australian national CERT for serious incidents. The "icode" website provides information to users with infected computers on how to fix the problem. More information is available at "icode" --- http://icode.net.au

Japan has operated its Cyber Clean Center (CCC) for 5 years, funded by Ministry of Internal Affairs and Communication and Ministry of Economy Trade and Industry. The CCC is operated by Telecom ISAC, JPCERT/CC and Information Technology Promotion Agency with cooperation from 76 ISPs and 7 Anti-Virus/Security Vendors. CCC captures, analyzes and develops disinfection tools for malware, identifies infected users, and the ISP involved sends an alert email to the infected user. The alert email contains a URL of a Bot disinfection website with a user-specific string that enables the ISP to monitor the customer's disinfection response. Notified customers access the CCC's Bot disinfection website, download the Bot disinfection tool and remove the Bot from their machine. The CCC site also provides awareness and education materials. More information is available at https://www.ccc.go.jp/

Korea initiated its cyber treatment project as a private and public partnership to combat malware infection during major incidents, funded by the Korea Communications Commission (KCC). Korea Internet & Security Agency (KISA) installed specialized notification devices in 3 major domestic ISPs and collaborate with 3 anti-virus vendors to develop the dedicated vaccine related to major incidents. KISA collects and provides the information on infected machines, such as the IP, timestamp and malware involved, to the relevant ISPs. When users turn on the computer, a pop-up window appears just after the computer is connected to the Internet. The pop-up notifies that the computer is infected with malware and asks users to run the dedicated vaccine or malware disinfection tool. During the DDoS attacks that targeted Korean governments and businesses in March 2011, more than 10 million Korean users downloaded the dedicated scan and clean-up tool.

China is running its 'Network Monitoring and Disposal Mechanism for Trojan Horse and Botnet' for nearly 4 years, which is under the regulation by the Ministry of Industry and Information Technology. CNCERT/CC, the national CERT of China is authorized to organize and coordinate all the Chinese ISPs and domain name registrars to detect, collect and stop Botnet and trojan horse control servers that located in Chinese networks. Meanwhile, from the industrial layer, the Internet Society of China (ISC) initiatives the Anti-Network-Virus Association (ANVA) to detect and handle threats from malware propagation sources to control servers, from phishing URLs to hackers underground economy forums. Besides CNCERT/CC, numbers of ISPs and new emerged online services such as online game, video & music, online banking joined the ANVA. The members are collaborating on a self-discipline principle. Those initiatives have mitigated large number of security threats, for example, in 2010, more than 5300 IP and domain names used by malware have been successfully disposed. Furthermore, as the mobile Internet growth, ANVA members have started to monitor and handle mobile malware. In 2010, more than 4 million mobile phone users have benefit from the jointly strike on mobile malware.

A. APCERT Project

To achieve the APCERT vision of making the Internet clean, we support good practice and sharing among members. Additionally, we seek to define what is meant by a "clean" Internet and how to measure whether the Internet is actually becoming "cleaner" due to the conduct of activities like those listed above.

IV. MAKING THE INTERNET SAFE AND RELIABLE

A. APCERT Point of Contact Arrangement

Each APCERT member economy assigns one CSIRT as a single point of contact for that economy for serious and time critical security issues information sharing and response.

B. Good Practice from members; Confidence Building Measures to Limit Cyber Conflict (China, Japan and Korea)

Hacking attacks are being used for a variety of political purposes between China, Japan and Korea. Activity appears to be ongoing and is increasingly causing confrontations between the parties. Fears regarding Internet attacks could lead to political crises or more broadly, simply conflict escalation between the countries. As a result, China, Japan, and Korea have identified a need to develop more effective conflict management approaches to cyber conflict. As part of a larger trilateral dialogue between the countries, in 2005 their information technology ministers signed a Memorandum of Understanding to build a framework of information sharing and cooperative incident-handling procedures to control cyber attacks and mitigate the consequences of these activities. The collaboration framework divides the response players into three layers by function, Computer Security Incident Response Teams (CSIRT), Internet Service Providers (ISP) and Governments. It also defines the process and policy of collaboration response along the incident timeline within and between each country.

Examples of cyber incidents handled under this agreement include the massive Distributed Denial of Service (DDOS) attacks between Korea and Japan over the Takeshima/Dokdo island territory dispute and the extensive DDOS attacks between China and Japan over Japan's handling of the

collisions between a Chinese fishing boat and Japan Coast Guard patrol boats near disputed East China Sea islands.

C. Strategic vision

Diplomatic relations between China, Japan, and Korea are plagued by politically sensitive issues, such as territorial disputes and historical animosity, and citizens of all three countries often hold negative emotions that could escalate a dispute during a cyber attack. In the cyber conflict management context, this alliance is the first of its kind in the world, and it provides a strategic showcase for how nations can work together to overcome political conflict and keep the Internet stable and connected.

More generally, internet operators need to maintain service whatever the motivation of the attack and governments need to make sure the attack is not politically motivated or state-sponsored. As demonstrated by the CJK approach, public-private partnerships on both sides addressing participant needs and incentives are key to the success of these conflict management arrangements. Having a global vision is also vital, given that the Internet is a common shared ecosystem.

D. Organizational Learning & Leveraging Partners Expertise

China, Japan, and Korea initiated an annual cyber exercise to assess these communications and joint response procedures in 2006. The activities have become more complex as they have progressed from simple communications checks to establishing procedures for quickly involving other domestic organizations responsible for critical infrastructure protection. This exercise now has been extended to 18 nations as part of an Asia-Pacific regional exercise program known as the APCERT exercise. The three CSIRTs signed a new MOU for next 5 years strategic collaboration in 2011. This agreement includes the establishment of an annual review process to identify lessons learned and set goals for the partners for the following year. This agreement also includes developing new cyber security norms.

E. Lessons Learned from the Alliance

Trust is key, especially given the current informal operational arrangements within the alliance. The key activities are governed by the economic incentives of quick recovery from disruptive activities and efficiency in response, as well as fear of the politically motivated actions of private citizens leading to a more significant crisis between governments. To reach a more effective, mature level of collaboration within the alliance, the implementation of an annual Activities Review mechanism is essential.

V. CONCLUSION

APCERT believes the vision of a clean, safe and reliable Internet is fundamental to improving cyber security globally. Programs within members economies are already making a difference. Establishing metrics and measurement systems will be crucial in progress towards this vision and APCERT will be focusing its efforts in this area. We also believe that improved communications to strengthen cyber crisis management within the APCERT framework is crucial. APCERT has evolved as an organization and its members are increasingly looking to make a major impact on the health of the Internet ecosystem building from our foundations of share trust in coordinating incident response.

REFERENCES

[1] APCERT, http://apcert.org/index.html

[2] The Australian Internet Security Initiative (AISI), http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317

[3] The Internet Industry Association's "icode", http://icode.net.au

[4] Cyber Clean Center, https://www.ccc.go.jp/en_index.html