The Importance of a Multistakeholder Approach to Cybersecurity Effectiveness

- Area: ROADMAP FOR THE FURTHER EVOLUTION OF THE INTERNET GOVERNANCE ECOSYSTEM
- Entitled by: Cristine Hoepers, Klaus Steding-Jessen, Henrique Faulhaber
- Region: Brazil
- Organization: Brazilian Internet Steering Committee - CGI.br
- Sector: Other
- Keywords: Multistakeholder, Internet Ecosystem, Cyber security, Internet Security, CERTs

Abstract

Most Internet security threats are increasingly complex, affecting multiple sectors at the same time, and requiring coordinated efforts to be detected and effectively mitigated. This is specially true to incidents involving botnets, spam, malware and DDoS.In the past 20 years several multistakeholder forums and initiatives that deal with Internet security threats were created - most of them have been very successful in bringing different sectors together to mitigate security incidents and counter cybercrime. All these efforts highlighted that the effectiveness depends on cooperation among different stakeholders, and that cybersecurity can't be achieved via a single organization or structure. Also, governments need to participate more in security forums and improve cooperation with other stakeholders.New forums and initiatives should not replace existing structures; they should aim at leveraging and improving the multistakeholder structures already in place today.

Document

The Importance of a Multistakeholder Approach to Cybersecurity Effectiveness

1. Introduction

Most Internet security threats are increasingly complex, affecting multiple stakeholders at the same time, and requiring coordinated efforts to be detected and mitigated. This is specially true to incidents involving botnets, spam, malware and DDoS (Distributed Denial of Service) attacks.

The scenario gets more complicated when critical national infrastructures are connected to the Internet, becoming exposed to the same vulnerabilities as other systems, and can be attacked by the same tools or techniques used for attacks in other contexts.

The protection of critical infrastructures and government networks connected to the Internet have both Internet security and defense aspects - the protection of these infrastructures is done most of the time by government organizations. What is worrisome is that we are increasingly seeing purely Internet security issues being perceived by governments as purely defense issues. This is leading to a scenario where, for example, the vital cooperation already existing among CERTs (Computer Emergency Response Teams) with National Responsibility being undermined by a tendency to move all existing Internet security capabilities into government or intelligence organizations.

The Internet ecosystem's security, stability and resilience should remain multistakeholder. The cooperation among different sectors and stakeholders, already existing today, is key to mitigate most of the current threats.

In the remainder of this proposal, we will briefly discuss several current multistakeholder forums and initiatives, pointing out their strengths, and bringing to attention issues that need to be considered when discussing a framework to improve the multistakeholder approach in order to achieve more effective cybersecurity.

2. Existing Multistakeholder Forums

There are some international forums that already exist today and that congregate different stakeholders, cooperating to handle security incidents and mitigate specific threats. Most of these forums were created to mitigate specific categories of attacks or threats. As nowadays the threat landscape changed and there is a prevalence of what is technically referred to as combined threats, most of these organizations are dealing with similar security issues. What follows is a description of each one of these organizations.

2.1. FIRST - Forum of Incident Response and Security Teams

FIRST is the Forum of Incident Response and Security Teams - http://first.org/. A Computer Security and Incident Response Team (CSIRT), sometimes also referred as CERT, is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client (Source: http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm).

The first CSIRT, the CERT Coordination Center, was created in November 1988, after the security incident known as "Internet worm" or "Morris worm" brought major portions of the Internet to its knees, and made clear the need to more coordinated efforts to respond to security incidents on the Internet. After this incident, several other teams were created. The FIRST was formed in 1990 in response to a second worm, the "Wank worm", and this incident highlighted the need for better communication and coordination among teams of different organizations.

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs. FIRST brings together a wide variety of CSIRTs from around the globe including educational, commercial, vendor, national, government and military. FIRST members develop and share technical information, tools, methodologies, processes and best practices, and use their combined knowledge, skills and experience to promote a safer and more secure Internet environment.

2.2. CSIRTs with National Responsibility and the NatCSIRT Annual Meeting

Since 2006, the CERT(R) Coordination Center (CERT/CC) has been hosting an annual technical meeting for CSIRTs with national responsibility. This meeting provides an opportunity for the organizations responsible for protecting the security of nations, economies, and critical infrastructures to discuss the unique challenges they face while fulfilling this role. As a result of these meetings, an online Forum is maintained throughout the year, as well as a list of CSIRTs with National Responsibility: http://www.cert.org/incident-management/national-csirts/national-csirts.cfm

It is noteworthy that there are very different models of National CSIRTs, ranging from not for profit, to academic, to government teams. Also, several countries have more than one team, demonstrating the complexity of increasing cybersecurity and performing incident handling at a national level.

2.3. APWG

APWG (http://apwg.org/) was founded in 2003 as the Anti-Phishing Working Group, at which time its mission was to counter phishing attacks. But, as the technology evolved, APWG is not focused only on phishing anymore, but on mitigating other attacks that are used to perpetrate cybercrime. APWG has more than 2000 members and research partners worldwide, from financial institutions, retailers, solutions providers, ISPs, telcos, CSIRTs, universities, defense contractors, law enforcement agencies, trade groups, treaty organizations and government agencies.

2.4. MAAWG - The Messaging, Malware and Mobile Anti-Abuse Working Group

MAAWG is The Messaging, Malware and Mobile Anti-Abuse Working Group (http://www.maawg.org/) and brings the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations. To accomplish this, MAAWG develops initiatives in the three areas necessary to resolve the messaging abuse problem: industry collaboration, technology, and public policy.

2.5. ISOC - The Internet Society

ISOC - The Internet Society (http://www.internetsociety.org/) - is an organization dedicated to ensuring that the Internet stays open and transparent. It has initiatives in Internet policy, technology standards, and future development. ISOC has a special project called "Combating Spam Project", in partnership with MAAWG, dedicated to demonstrating to policy makers, clearly and effectively, the tools and industry partnerships that are available to tackle spam.

3. Examples of Successful Multistakeholder International and National Initiatives

In the past few years, CSIRTs, Network Operators and members of the aforementioned forums became involved in some specific projects and working groups aimed at mitigating specific big threats, implementing best practices or better understanding the Internet threat environment. In this section we are going to describe some of these successful multistakeholder initiatives.

3.1. The Conficker Working Group

Starting in late 2008, and continuing through June of 2010, a coalition of security researchers worked to resist an Internet borne attack carried out by malicious software

known as Conficker. This coalition became known as "The Conficker Working Group", and seemed to be successful in a number of ways, not the least of which was unprecedented cooperation between organizations and individuals around the world, in both the public and private sectors (Source: http://www.confickerworkinggroup.org/).

The work of this group involved members of Internet Governance Bodies, Software and Hardware Vendors, Content providers, Universities and Research Centers, and was vital to mitigate the worm's malicious payloads and to help clean systems throughout the Internet. A Lessons Learned document can be find in the previously listed homepage.

3.2. DNS-changer Working Group

The DNS Changer Working Group (DCWG - http://www.dcwg.org/) was an ad hoc group of subject matter experts, and included members from organizations such as Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, and the University of Alabama at Birmingham. The work of the DCWG was coordinated with FBI investigations, and received help from several National CERTs and ISPs.

This working group was created to help remediate Rove Digital's malicious DNS servers. The botnet operated by Rove Digital altered user DNS settings, pointing victims to malicious DNS in data centers in Estonia, New York, and Chicago. The malicious DNS servers would give fake, malicious answers, altering user searches, and promoting fake and dangerous products. Because every web search starts with DNS, the malware showed users an altered version of the Internet.

The cooperation among all these stakeholders made it possible to gradually alert and help disinfect the end users' devices, without disrupting their access to the Internet.

3.3. Multistakeholder initiatives at a National level

There are several multistakeholder initiatives at a National level. In this section we will briefly describe some of these initiatives.

3.3.1. The Dutch Cyber Security Council

The Dutch Cyber Security Council has 15 members from government, industry, and the scientific community, for a total of three scientists, six public sector and six private sector representatives. The Council is supported by an independent secretariat. The Council oversees the Dutch National Cyber Security Strategy and offers both solicited and unsolicited advice to the Dutch government and society. The role that the Council played during the DigiNotar incident, for example, demonstrated the effectiveness of this kind of public-private partnership in the digital domain.

In July 2013, the Council issued an advice on the new National Cyber Security Strategy,

published in October 2013. The advice specifically focused on the need for close cooperation and coordination in the field of incident detection and response. Only through active information sharing, timely response and seamless collaboration can a secure digital environment be established.

Source:

https://www.ncsc.nl/english/current-topics/news/best-practices-in-computer-network-defense.html

3.3.2. The Japanese Cyber Clean Center

The Cyber Clean Center (CCC) is a core organization taking a role to promote bot cleaning and prevention of re-infection of users' computers, which were once infected by bots, based on cooperation among government, software vendors and ISPs. The Cyber Clean Center has a Steering Committee and three working groups in the layer below: the bot countermeasure system operation group; the bot program analysis group; and the bot infection prevention promotion group.

Source:

https://www.ccc.go.jp/en_ccc/

3.3.3. CGI.br Port 25 Management Initiative

For a long time, Brazil was present on most spam rankings as a top spam relaying country. Determined to reverse this situation, the Brazilian Internet Steering Committee (CGI.br) has conducted, since 2005, a number of activities, such as academic studies and technical analyses, which lead to the adoption of Port 25 management as the most effective measure to be taken to prevent spammers from abusing the Brazilian broadband infrastructure. This initiative was lead by CGI.br's Anti-Spam Working Group (CT-Spam), which provided a forum where different stakeholders were able to meet.

For almost 20 years, Brazil has developed a model of multistakeholder Internet governance. Therefore, a measure of such importance as the blocking of outgoing port 25 traffic in residential networks could not be adopted without all sectors affected being asked to contribute to this decision-making process.

Bringing together the experience of more than a dozen telecom companies, thousands of Internet service providers, representatives of civil society and the academic community, as well as the technical staff of CGI.br, the process of adopting Port 25 management was broadly discussed. This was specially important because the implementation required a concerted effort, with e-mail service providers making sure they offered Message Submission via a different port (587), and migrated at least 90% of their users' base

before broadboand providers could block outbound port 25 traffic.

It is also important to highlight that both the National Telecommunications Agency (Anatel) and the Ministry of Justice have played a key role in providing support for the telecom companies and the consumer protection entities respectively. Anatel signed a Cooperation Agreement with CGI.br, which gave the telecom companies legal grounds to proceed with the adoption. The Ministry of Justice, on the other hand, published a Technical Note explaining the benefits of such measures for consumers.

As a result of this initiative, Brazil is no longer listed as one of the top spam relaying countries in the world, according to several public rankings.

Source:

http://www.nic.br/imprensa/clipping/2013/midia182.htm

http://www.cert.br/docs/palestras/certbr-citel-itu-isoc2013.pdf

3.3.4. CERT.br - Computer Emergency Response Team Brazil

CERT.br is the Computer Emergency Response Team Brazil, maintained by NIC.br, a not for profit organization created to implement the decisions and projects designed by the Brazilian Internet Steering Committee - CGI.br. All CERT.br activities take into account the need to involve all stakeholders to successfully increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Besides doing Incident Handling activities, CERT.br also works to increase security awareness in the Brazilian community, maintaining an early warning project with the goal of identifying new trends and correlating security events, as well as alerting Brazilian networks involved in malicious activities. CERT.br also helps new Computer Security Incident Response Teams (CSIRTs) to establish their activities in the country.

A clear example of the success of this approach is the Brazilian Distributed Honeypots Project, which, through a network of distributed honeypots in the Brazilian Internet space, increases the capacity of incident detection, event correlation and trend analysis in the country. These honeypots are passive sensors that provide valuable situational awareness, without collecting production traffic neither performing any type of surveillance. This project has sensors in more than 40 Brazilian partner organizations, ranging from government and energy sectors, to academia, ISPs and Telecommunication Providers.

Source:

http://www.cgi.br/english/activities/

http://www.nic.br/english/about/

http://www.cert.br/about/

http://honeytarg.cert.br/honeypots/

4. The need for improvement of the multistakeholder collaboration in cybersecurity

Achieving a satisfactory level of Internet Security is not an easy task, but the experience accumulated by several successful initiatives demonstrates that, in order to be effective, any cybersecurity initiative needs to involve several stakeholders. More than that, the reality is that more often than not, the security measures need to be taken by systems administrators, network operators or security professionals in their own networks. However, cooperation with others is key to be able to understand the threats and better evaluate the effectiveness of their actions.

In the document "Conficker Working Group: Lessons Learned" (http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_ published in January 2011, although the word "multistakeholder" is not used, some of the success factors listed point to the importance of cooperation and the involvement of different stakeholders. Here are some examples:

- Utilize a trust model; the scope of the working group needs to be a manageable size to be effective and include those directly affected, and yet large enough to include a broader universe of those impacted.
- Incorporate a consensus model without hierarchy to allow the group to adapt and respond to fast changing conditions.
- Gain the participation and support of key governing and regulatory bodies.
- Formalize communications with stakeholder groups vs. relying on social networks.

These four points bring to light issues like the rapid change of the threat landscape, the need for rapid communication, the involvement and support of governments and the fact that several stakeholders need to cooperate.

Although the Conficker Working Group was very successful, as well as other initiatives listed in the previous section, there are still some stakeholders that could improve their cooperation. For example:

- Network Operator Groups (NOGs) and Regional Internet Registries (RIRs)

should be more involved with security issues. There are some areas like routing security (and newly proposed protocols like RPKI or SBGP) or DNSSEC that need worldwide adoption to be effective. RIRs could also work more closely with the CSIRT community to improve the WHOIS system to help the incident handling process.

- Software vendors need to become involved and be more pro-active; after all, most of the security problems we face today are software-related problems. The real challenge is to improve software security and get the software industry to a more mature level.
- The governments, including military and intelligence sectors, in addition to traditional security and defense strategies, need to improve their awareness of the multistakeholder nature of the Internet and the vital importance of the cooperation to address security threats. They need to participate more in the national and international security forums and improve cooperation with other stakeholders.

Considering government cyber security strategies, it is noteworthy that about 130 parties, including public and private parties, knowledge institutions and social organisations, were involved in the drafting of the Dutch "National Cyber Security Strategy 2 - From awareness to capability" (NCSS2) (https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html). The strategy starts with the following statement:

> "We are moving from structures to coalitions in which all parties -- national and international -- are represented in order to achieve supported standards."

And adds that

> "The correlation between security, freedom and social-economic benefits proposed in the NCSS2 is a dynamic balance that is intended to be realised in a constantly open and pragmatic dialogue between all stakeholders, both national and international. (...) In order to bring the dialogue about cyber security between the various stakeholders to a new level of maturity, the following three management areas are of the utmost importance: (self) regulation, transparency and knowledge development."

This is a good example of the recognition of the importance of a multistakeholder approach to the Internet ecosystem's security, stability and resilience.

5. Recommendations

As stated before, achieving a satisfactory level of Internet Security is not an easy task, and the multistakeholder initiatives previously discussed are good examples of frameworks that can effectively deal with cybersecurity current and emerging issues. Therefore, it is recommended that all national and international organizations involved with Internet Governance, for instance, Local Governments, RIRs, United Nations, European Union, ISOC Chapters, among others, should take the following into consideration:

1. The experience accumulated by the several successful initiatives described in this contribution demonstrates that, in order to be effective, any cybersecurity initiative depends on cooperation among different stakeholders, and it can't be achieved via a single organization or structure.
2. There are stakeholders that still need to become more involved, like network operators and software developers.
3. Governments, including military and intelligence sectors, in addition to traditional security and defense strategies, need to improve their awareness of the multistakeholder nature of the Internet and the vital importance of cooperation to address security threats. They need to participate more in the national and international security forums and improve cooperation with other stakeholders.
4. There is room and a need for new forums and initiatives, but they should not replace existing structures. Any new initiative should aim at leveraging and improving the multistakeholder structures already in place today.