Input to the Commission on Enhancing National Cybersecurity: Federal Governance

Executive Summary

While the US government has an extraordinary amount of resources and capabilities at its disposal, it cannot address the state of cybersecurity alone. Only with a strong partnership with industry, and the major economic influences that international corporations have at their disposal, will there be any chance to affect significant change in the current high profile malicious behavior on the internet. However, the government must first establish credibility and trust within industry. Only by combatting smaller targets, such as botnets and spammers, will the government be able to demonstrate its ability to lead a fight against malicious internet actors and establish the reputation for itself as a proactive governance organization. Once viewed in this manner, the government and industry will be able to consider cooperation and coordination in the use of international economic reprisals in response to large scale internet attacks.

Introduction

A strong security posture is not a state that can be exclusively implemented by government. The domain of cybersecurity is massive - much larger and more complex than the physical world - and, as a result, the policing of it must be undertaken by a combination of industry and government. Of course there are challenges to forming this partnership, with an already long and somewhat sordid history that has been well documented in other sources. However, we are seeing growing maturity in this field, with significant governmental strides coming from institutions like NIST and their standards around security controls, as well as from industry with the growth of the Information Sharing and Analysis Centers (ISACs). The long term future of incident response will likely need to come from a concerted, lock-step partnership between major corporate powers and the federal government, as economic penalties will need to be asserted by corporate entities instead of just government saber-rattling. However, this maturity is not yet in place and it will take time and increased trust between corporate entities and government before such partnerships can be effective. In the meantime, the government can take steps to curb some of the more basic internet-based criminal activities. In addition to increasing the safety of cyberspace, action on the part of the government would demonstrate its commitment to the effort, ability to build consensus and coordinate technical capabilities, and establish trust among the major corporations – all of which would serve as a foundation for tackling the more challenging cybercrimes.

Observations

While the growth of the internet has created a new lexicon and concepts that are intended to explain and portray the amazing capabilities of our interconnected world, it has also brought new negative concepts. This includes such words as “botnet”, “spam”, and “DDOS”. We often look at these notions through the lens of vandalism and petty theft and do not normally associate them with the more high profile cybercrimes. However, if the government wants to make an immediate impact on the security of the private sector, then successfully tackling these lower-visibility crimes will go a long way to establishing the government’s credibility (to both the general public and industry) in the area of information security.

One of the great advantages that the government has over industry is its ability to coordinate contractors. This has come from decades of contractor management, to the point that many government agencies have more contractors than they do actual employees. The result is often that many government agencies do not have the technical depth in some of the security specialties (such as the latest techniques used by botnets, which run some of the largest spam and DDOS capabilities in the world). However, the government does have the funding and organizational infrastructure to mobilize the right businesses to conduct the work that is needed. This is the strength that the government should emphasize. The government has had success in some botnet takedowns, but they have accomplished these achievements by providing support and coordination between the technical companies that have the rare skills to do so.   There have been some successes in botnet takedowns without government involvement (such as the Grum botnet), but with the government as a supporting, coordinating player, there could be many more.

Another advantage where the government acts as a critical supporting player is bringing legal oversight to a (potentially) international activity. A key aspect to botnet disruptions are the legal questions and considerations that go along with potentially affecting another entity's network. These are the kind of resources that most contractors cannot provide, and the potential risks for a takedown that goes bad can easily sink a small business. However, teamed with an entity such as the Department of Justice, which brings the 800 pound gorilla to the table in terms of legal power, the takedown of a major botnet may be reduced to pure technical know-how – something that America (and our technical industry in particular) prides itself in having in abundance.

Conclusion

There is no shortage of internet crime. From malware to phishing scams to theft of intellectual property, there is a dark side to the considerable capabilities that the internet brings to our daily lives. Building a strong, united defense will take time, and it is not something that either industry or government can do alone. Yet, the government needs to demonstrate that it can be a trustworthy partner in this fight, and that it brings skills and capabilities to the table that are critical for victory. The government should not strive to have the technical skills in-house to stop all cybercrimes, as those skills are orders of magnitude more valuable in industry. However, if a specialized government committee, dedicated to mitigating cybercrime, can coordinate the bringing of technical resources to bear against an adversary, it is unlikely that any target could resist. Taking these actions against the low-profile security problems of the internet will demonstrate the advantages of teaming with the government. This is the credibility that the government needs to demonstrate in order to eventually mobilize major corporations to its call in order to address the more complex security attacks with potentially economic responses, instead of just technical.