Meeting Minutes

Attendees

Commissioners: Tom Donilon, Steve Chabinsky, Keith Alexander, Annie Anton, Peter Lee, Pat Gallagher, Herb Lin, Joe Sullivan, Maggie Wilderotter, Ajay Banga

Others: Kiersten Todt, Karen Scarfone, Roger Cressey, Rob Knake, Matt Barrett, Jon Boyens, JP Chalpin, Robin Drake , Matt Scholl, Bruce Potter, Jeff Greene, Amy Mahn

Agenda:

I. Discussion on Recent DDOS Attack
II. Commissioner Comments
III. Discussion of the chart

Discussion:

I. Discussion on Recent DDOS Attack led by Jeff Greene, Matt Scholl, Bruce Potter

a. **Mr. Scholl:** There was a large scale distributed denial of service (DDOS) attack against an individual and a domain name server (DNS) provider that happened last week.
b. The volume of the DDOS attack was larger than has been seen, forcing adjustments.
c. Malware used was new or newly seen. Exploited cameras and DVRs. There was a scan on open default user names and passwords that had not been reset.
d. The authors made the malware open source. Variants and hybrids may be developed.
e. Forensics are still underway. Analysis is disparate. The use of internet of things devices, may have been ten percent besides other devices. This is the current state.
f. There may be 1.5 million affected devices. Many are in Asia-Pacific, and manufacturers are Chinese products.
g. Dyn is now back online following the attack.
h. **Mr. Greene:** Is there anything else we should think of in relation to this? Possible thoughts:
    i. It did not require a lot of work to get onto the devices, because of poor configuration.
    ii. Suggesting an aggressive user campaign to change user name and passwords.
    iii. An alternative is some sort of mandate, to force companies to use different usernames and passwords.
    iv. Consumer security cannot be considered in a vacuum.
    v. Manufacturers to push out patches to require changes to user name and passwords.
    vi. What obligation is there for an internet service provider (ISP) to look for malicious activity, and notify individuals they have infected devices.

i. **Mr. Scholl:** Senator Mark Warner has asked FTC, FCC and DHS for potential capabilities to respond. It may be that the Chinese company may do a recall.
j. **Mr. Potter:** Dyn – There has been a history of DDOS attacks against infrastructure. There has been a large increase in the volume and size of the attacks.

II. Commissioner Comments

a. **Mr. Donilon:** The National Security Telecommunications Advisory Committee (NSTAC) report and the weaponization of the internet of things (IoT) would call for direct action, but seeking opinion of others.
    i. **Mr. Alexander:** Do we know why the attack was conducted? We don't know that at this point. There are government tools that can track, does NIST have access? There is a small subset that is available, but can't say what to do or not do.
    ii. There is some recommendations that can be made. We need to be careful how it is framed, because most of the devices are outside the US. It must be considered as an international problem.
        1. **Mr. Donilon:** We can do something about devices sold in the US. Plays to the labeling and Underwriters Laboratories (UL) ideas that have been suggested.
        2. **Mr. Alexander:** Can we find a solution that doesn't stifle innovation? It may be good to have smaller companies discuss what they can do in this context.
        3. **Mr. Lee:** On innovation, it can be a bit murky. The technical knowledge and capabilities in smaller shops are pretty low. Manufacturer and vendor may have received components with no engineering knowledge. Establishing a baseline in this context may be beneficial for innovation. It may be pro-business to establish standards now.
        4. **Ms. Murren:** The more uncertainty there is on the part of consumers, the worse it may be for business. Making devices safer is better. Balancing innovation with safety is better over the longer term
        5. **Mr. Lin:** It still seems the way is some sort of liability regime. Also, most of the discussion does not address incentives. How to deal with misaligned incentives is something that must be addressed.
        6. **Mr. Lee:** Cheap connected devices were very directly involved.
        7. Almost all were located and manufactured outside the US. Regulation in the US would have not had effect.
        8. **Mr. Greene:** Once devices are sold in the US, it doesn't matter where the company is located. FTC can sanction companies because of the poor security, even if they are outside the US. Selling in US creates jurisdiction.
        9. US leverage for devices sold here, establishing set of standards, labeling UL, consumer education, content from Mr. Gallagher's email yesterday.
        10. **Mr. Donilon:** Authentication standards integrated in NIST framework. Also consider direct intervention. These events put the commission on notice to adopt some significant steps.

11. **Mr. Chabinsky:** Outline for botnet action. Mitigation, enhancing capabilities of government and private, and enhancing international, mitigating vulnerabilities, and others. Will send to Mr. Scholl for consideration and inclusion.
12. **Mr. Lee:** We must acknowledge that this has been a topic. It may be too early to jump to regulatory requirements, but it will need to be revisited over the next five or ten years as technologies evolve.
13. It may also put industry on notice that more action is in the future.
14. **Mr. Lee:** Question of DNS security in general. Many may argue it is one of soft underbellies of security. The attack Friday raised that issue, want to make sure we don't focus on that one thing.
    a. **Mr. Alexander:** We also need to address what the nation does in such an attack. We need to think in terms of securing the nation and getting device security correct. It is an issue we face in the next few months.
15. We are setting an important tone in this area. Push the line toward regulation.
16. **Mr. Gallagher:** The intent of the framework was to forgo regulation. Any voluntary framework must be very muscular to truly avoid regulation. Standards must be framed to create a high integrity system.
17. Matt will capture international, and topics captured here.

III. Discussion of the Chart

a. Next draft will be due on October 31st.
b. Presenting a notional listing of imperatives (buckets).
c. Implementation actions need to be built out. Focusing today on proposed recommendations.
d. Not all discussion has been represented in its entirety as yet, some representation.
e. Listing of the five:
    i. Commission consideration of the five
        1. The theme of protecting small and medium businesses seems lost – Mr. Banga's "weakest link".
        2. Staff will create a narrative for each imperative, then develop proposed recommendations.
        3. List a separate proposed recommendation under that imperative.
        4. There are a number of themes that need to be hit hard. Small entities or individual consumers being disadvantaged. Moving security away from end users, and other themes play into.
    ii. Protecting today's internet, shaping tomorrow, better equipping government, consumers and citizens, international functioning in a global economy
    iii. Most commissioners received the imperatives positively.
f. Presenting 11 proposed recommendations in support of the five imperatives
    i. Proposed Imperative 1 – Cleaning up the internet.
        1. General positive reception
            a. **Mr. Sullivan and Mr. Chabinsky:** The language seems unclear.

b. **Ms. Wilderotter:** Proposed sending around in email.
c. Reviewing the chart now with five proposed imperatives, eleven proposed recommendations, and possible implementations.
d. Will send the chart, commissioners should review and return by 10 a.m. Thursday.
e. Staff will continue working to build out the report.
f. We want to make sure we capture the major ideas, and top potential recommendations, and get perspective from the commission on implementations of those recommendations.

ii. We want to confirm we have the right potential recommendations and are they in the right categories. Email, or call Ms. Todt with responses.
iii. Staff will have a draft for the commission on October 31st.
iv. There needs to be awareness of "altitude control". Open with those that have the most impact. Lesser ones to provide balance and color. Input on level of proposed recommendations also welcome.