Scott Pinkerton

Coordinating Attack Response at Internet Scale

When events are occurring on the millisecond (or faster) scale,
and distribution has no real limits

Background and Assumptions

To put this challenge into an appropriate context, the community must first acknowledge a couple of truths:

- A very large number of latent software errors exist in the systems currently in use across the Internet today—no big surprise there.
- It is likely that there is going to be a steady increase in the number of devices (things connected to the Internet) that will be purchased "pre-infected," that is, with malware *of some sort* already built into the device before it's taken out of the box.

Looking to the future, we will need to provide clear and unambiguous definitions for what defines an attack. With the growth of the "Internet of Things", and problems caused by unintended consequences of software misbehaving, possibly unintentionally, establishment of a standard framework will be of great benefit.

Response vs. Recovery

Coordinating attack response implies events that are currently under way and implies, at some level, that there is still hope that the attack can be thwarted. However, adopting a more pragmatic view of the future also suggests that while we are evaluating our options for response, we should also begin a dialogue around the concept of recovery. The huge interdependence of things attached to the Internet leads me to worry about the hard failure scenario: where we have to figure out how to reboot everything — from a "failed shutdown state."

Getting a Grasp on the "Now"

On the basis of research on STUXnet (e.g., by Symantec, Kim Zetter's *Countdown to Zero Day*, the Kapersky reports, etc.), it is evident that most of the "attack" software will employ multiple layers of countermeasures in attempts to obscure the reality of what is happening at the moment of attack.

Further difficulties emerge when combining this challenge (i.e., understanding what is happening in real time) with the inherent lack of formal "chains of command" when viewed from a global perspective. Thus, formulating an option will be hard enough; formulating *optimal* options in real time is likely to be impossible given diverse points of view. One analogy with interesting parallels is to the problem domain of forest fires, where decision makers must decide where to draw the line for

the fire break: one side of the line is typically sacrificed, whereas the other side of the line is saved. How would similar choices be made in the cyber domain on a planetary scale?

Directing /Coordinating / Controlling the Execution of Options

One key area of significant challenge that will continue to emerge is the coordination phase. Responses in the cyber domain might likely require very fine-grained timing and sequencing of actions to be successful—efforts that might be significantly compromised if the Internet is operating in an unreliable state. Furthermore, if the Internet itself is being used to manage the coordination—that is, the same infrastructure you are being attacked on, to try and coordinate a defense on—poses significant risk, as well.

Acknowledgment of the People Who Are Likely to Be Involved

It is important to acknowledge the mix of private and public sector participants who will likely be active in this space. The actors/attackers could range from nation states and their sub-contractors to criminal or terrorist-based groups or even individuals operating alone The defender space is equally diverse, including a mix of both public and private sector individuals – with the added challenge of global legal systems and cultural norms. It should be assumed that there would be a wide range of capabilities/talents.

Specific Challenges

Some of the specific challenges that this workshop and the Internet Architecture Board can address are:

- (global ?) Chain of command—or the lack there of
- Measuring the current state of response and developing options
- Directing and coordinating response
- Evaluating and recommending the future tools that will be required to facilitate coordinated response efforts

Things We Need to Be Doing—or at Least Discussing—Now

We need to develop our frameworks and tools to support:

- Distributed collaboration
- Operation at, or near, machine speed (millisecond?)
- Coordination of appropriate taxonomies of information representation
- The start of testing notional/potential response methods so as to understand unintended consequences, that is, what things might exist in the toolkit?
    - Sequenced disruptions (changes) to global domain name system (DNS) infrastructure
    - Border Gateway protocol (BGP) infrastructure
    - Time infrastructure
- Efforts necessary to create appropriate trust communities