Collective Defense - Applying Public Health Models to the Internet

Scott Charney

The Internet – A Global Shared Domain

The Internet continues to grow at an almost unprecedented rate – connecting people, stimulating ideas, and enabling innovation for consumers, enterprises, and governments. The small number of users in the 1990's has grown to over 1.96 billion in 2009 and that number will continue to increase for years to come. This growth is enabled by increases in bandwidth and a proliferation of computing devices. For example, it is estimated that there will be 500 million broadband subscribers worldwide by the end of 2010 and the International Telecommunications Union has reported that mobile phone usage increased from 12 percent to 61 percent between 2000 and 2008, with a growing demand for smart phones. Along with this increased connectivity and a growing number and diversity of devices such as smart phones, netbooks, and e-readers, the computing model is shifting to one dependent on "anywhere access" and remote datacenters (that is, "the cloud"). For governments in particular, cloud computing offers potential productivity increases and cost reduction in a time of economic constraint. The growth in new users and devices, the richness of data being created or stored by users, and the volume of transactional data generated as a byproduct of computing activity produces valuable targets for attack.

The Threat to Internet Security

Cyber threats and attacks on users are difficult to characterize and respond to for seven reasons:

1. There are many different malicious actors.
2. These actors have many different motives.
3. The attacks look similar, so the nature of the attack does not always help to identify the actor and the motive.
4. The Internet is a shared and integrated domain. It is shared by individuals, organizations, and nation states and used by these groups for many different activities which cannot easily be distinguished from one another (for example, a packet may contain malware or political speech). In addition, it is hard to tease apart the different actors and activities. For instance, it is hard to monitor only the packets of individuals engaged in certain activities without in any way observing other actors and activities.
5. The speed of attack may overwhelm response methods that require human interaction.
6. The potential consequences of an attack can be hard to predict.
7. The worst-case scenarios are alarming.

It is also important to understand that most countries have already established organizations that deal with problematic conduct, including malicious Internet activity, and that these organizations often use different agencies with differing levels of authority and effectiveness, depending on who is attacking and the reasons for the attack. Yet, the "who" and "why" are often unknown when a system is under attack, which can make response challenging. Identifying cyber criminals will reduce, but not eliminate, some of the uncertainty regarding attack response. And while attribution will never be perfect, with improved attribution, cyber threats can be broken down into specific categories that will help determine what an appropriate response may be. Those categories include:

- Cybercrime.
- Economic espionage and other activities where actors may disagree on the appropriateness of particular conduct.
- Military espionage.
- Cyber warfare.

Responding to the Cyber Threat – New Collective Defense Efforts

A spectrum of actions can be taken to defend against cyber threats, even if the source of the threats cannot be specifically attributed. These activities can generally be categorized as 1) individual defense, 2) collective defense, 3) active defense, and 4) offense. This cyber defense spectrum ranges from the simplest and least controversial (individual defense) to increasingly challenging and complex responses (offense). For example, individual defense involves a single point of control (such as a person, company, or government organization) engaging in activities that affect its own assets (such as installing firewalls, running intrusion detection systems, and restricting access to information), so there is generally no objection to such activities – an entity can always raise its own defenses. By contrast, collective defense may require coordination across multiple points of control and the sharing of sensitive or even legally protected information.

Adopting a Public Health Model for Internet Security

To address cyber threats generally, and botnets in particular, governments, industry and consumers should support cyber security efforts modeled on efforts to address human illnesses. The public health model relies upon several core concepts that can be applied to Internet security. For a society to be healthy, its members must be aware of basic health risks and be educated on how to avoid them. Common practices to limit the propagation of disease range from the simple (washing hands) to the systematic (in schools, students may be required to be vaccinated before admission; warned if other students show symptoms; required to stay at home if infected; and notified and required to meet specified criteria for re-admission to school). In the physical world, there are also international, national and local health systems that identify, track, and control the spread of disease including, where necessary, quarantining people to avoid the infection of others. To improve the security of the Internet, governments and industry could similarly engage in more methodical and systematic activities to improve and maintain the health of the population of devices in the computing ecosystem by promoting preventative measures, detecting infected devices, notifying affected users, enabling those users to treat devices that are infected with malware, and taking additional action to ensure that infected computers do not put other systems at risk. Enterprise IT departments (including those in government organizations) have professional staff to help do this already. They often have Chief Information Officers, Chief Security Officers, professional IT staff, incident response teams, employee education and training, tools to inspect machines, and processes to ensure that devices that do not meet security health requirements are made compliant. By contrast, consumers have no such support. Moreover, many consumers have no desire to become IT professionals, let alone security experts, and information technology can be so complex that knowing how to protect oneself online is not intuitive. As a result, many consumers may be unwittingly running malware and their computers may be part of a botnet. Such botnets may be used to send spam and engage in illegal activities, including launching denial of service attacks against critical infrastructures.

Building a Sustainable Model that Balances Security and Privacy

As cyber security policy and corresponding legislation is being actively discussed in many nations around the world, there is a huge opportunity to promote this Internet health model. As part of this discussion, it is important to focus on building a socially acceptable and financially sustainable model. While the security benefits may be clear, it is important to achieve those benefits in a way that does not erode privacy or otherwise adversely impact freedom of expression and freedom of association. Ensuring users have control over health certificates and the way they can be used – and that users understand the implications of refusing to attest to good health – is an important first step in ensuring appropriate user engagement. It is important to decide, too, whether health certificates will reveal simply the state of the machine, or more about the identity of the device and, potentially, its user. Certainly, a machine could be denied unfettered access to the Internet based upon certain health attributes without determining more about the machine or its user.

Shared Principles for Progress

With security and privacy in mind, the following statements reflect the concepts outlined in this policy statement document and are intended to help guide stakeholders efforts, promote action, address challenges, and influence future initiatives.

- The risk that botnets present to Internet users and critical infrastructures must be addressed.
- Collective defense can and should be used to help improve the security of consumer devices and protect against such cyber threats.
- A public health model can empower consumers and improve Internet security.
- Voluntary behavior and market forces are the preferred means to drive action, but if these means fail, governments should ensure these concepts are advanced.
- Privacy concerns must be carefully considered in any effort to promote Internet security by focusing on device health. In that regard, examining health is not the same as examining content; communicating health is not the same as communicating identity; and consumers can be protected in privacy-centric ways that do not adversely impact freedom of expression and freedom of association.

SCOTT CHARNEY is a Corporate Vice President, Trustworthy Computing, Microsoft Corp.