This product is part of the RAND Corporation occasional paper series. RAND occasional papers may include an informed perspective on a timely policy issue, a discussion of new research methodologies, essays, a paper presented at a conference, a conference summary, or a summary of work in progress. All RAND occasional papers undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

OCCASIONAL
PAPER

A Cyberworm that Knows no Boundaries

Isaac R. Porche III, Jerry M. Sollinger,
Shawn McKay

Prepared for the Office of the Secretary of Defense

NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was prepared for the Office of the Secretary of Defense (OSD). The research was conducted within the RAND National Defense Research Institute, a federally funded research and development center sponsored by OSD, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002.

Published 2011 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Iran's announcement that a computer worm called Stuxnet had infected computers that controlled one of its nuclear processing facilities marked a signal event in cyber attacks. Although such attacks were known to be theoretically possible, the Stuxnet incident proved that a cyberworm could indeed be planted in a system and produce physical damage. Furthermore, the sophisticated nature of the worm and the resources that would have been required to design, produce, and implant it strongly suggest a state-sponsored attack.

Although the implications of the attack are still unfolding, three are immediately discernable. First, it ends the debate about whether such worms are feasible. Clearly, they are. Second, Stuxnet-like worms pose a serious threat. The creators were able to implant the worm on computers that were almost certainly not connected to the Internet, and they were apparently able to mask its presence even while it was modifying the signals that the industrial control systems were sending. Reportedly, the worm damaged hundreds of gas centrifuges. Industrial control systems are ubiquitous; they control electrical power, gas, refineries, and many other systems. The ability to tamper with them and cause physical damage is worrisome. Third, the fact that Stuxnet apparently required the resources of a nation (and perhaps more than one) suggests a new willingness on the part of governments to use cyber attacks to further national goals.

Purpose

This paper explores the implications of Stuxnet-like worms for the United States and specifically for the U.S. Department of Defense. It discusses what makes cyber defense difficult and outlines the bureaucratic and legal issues and boundaries in the United States that can compound the problem. It then offers some conclusions and recommendations for how the United States can confront the increasing risk posed by such threats.[1]

Why Cyber Defense Is Difficult

Stuxnet aside, fending off cyber attacks is difficult. The inherent characteristics of cyberspace favor the attacker, not the defender. Furthermore, unlike conventional or nuclear war, a cyber attack is not always obvious. Additionally, the responsibility for defending the nation against a cyber attack spreads across many federal agencies and the private sector, which complicates

[1] Stuxnet revealed vulnerabilities that could prove inviting to adversaries planning future attacks (see Harris, 2008, p. 62).

mustering a coherent response to an attack. Legal boundaries govern who can do what in response to such attacks, so it will be necessary to sort through these issues to ensure that when an attack comes—and we believe one surely will—government agencies can work in concert with private-sector organizations either to blunt the attack's effects or to minimize the damage afterward.

Cyberspace Favors the Attacker

Several characteristics of cyberspace tilt the playing field in favor of the attacker. First, cyberspace has no boundaries, which means that an attack can come from virtually anywhere. It takes only a computer and an Internet connection to obtain a passport to cyberspace. Individuals with sinister intentions can mask their electronic identity or steal one from an unsuspecting individual, either by collecting the information required to take on the purloined identity or by using a "bot" to take over a computer that can be used to enable or perpetrate the attack. Second, cyberspace changes constantly. Sites are added and dropped daily, which means that assuming a new identity is far easier in cyberspace than it is in the physical world.

What this means is that it is not possible to stop all attacks. Firewalls and intrusion prevention systems will thwart only so many attacks.[2] Defenders must be right all the time; the attacker, only once.[3] Careless use of a portable hard drive, the failure to update virus protection software, a compromised password, and dozens of other events can open the door to an attack.[4] Thus, a key policy focus must be how to respond once an attack has occurred.

Cyber Attacks Are Hard to Identify

Mounting a response to a cyber attack requires knowing that one has occurred, and in cyberspace that is not necessarily easy. Malicious activity is common in cyberspace, but not all such activity constitutes an attack. Some examples are phishing expeditions designed to steal personal or financial information, efforts to obtain proprietary information from private-sector firms, and or simple hacking attempts to penetrate computer systems for the purpose of espionage. These are not technically classified as attacks but, rather, as espionage attempts.[5] However, they could pave the way for more destructive activity, or they could be used to plant a worm that, at some later time, could launch its own attack. Presumably, this is the way Stuxnet was programmed to operate. Worms can lie dormant until the circumstances they have been

---

[2] In his guide to the Certified Information Systems Security Professional exam, Shon Harris states that an intrusion prevention system is intended "to detect [nefarious] activity and not allow the traffic to gain access to the target [e.g., the network or device] in the first place" (Harris, 2008, p. 260). An intrusion prevention system is supposed to be an advancement over intrusion detection systems, which are configured to "spot something suspicious happening on the network" (Harris, 2008, p. 250).

[3] This is, of course, also the case with terrorism.

[4] According to the U.S. Army Information Assurance Training Center (undated),

> Malware is an acronym that stands for MALicious software and it comes in many forms. Generally speaking, malware is software code or snippets of code that is designed with malice in mind and usually performs undesirable actions on a host system.

[5] Such collection activities or probes are known as computer network exploitation and are differentiated from computer network attacks, which seek to destroy, alter, or degrade capabilities.

built to exploit appear,[6] and only then do they become active. Thus, the actual "attack" can occur days, weeks, or even months after the initial exploit.

Bureaucratic and Legal Issues Can Hamper Defense

Defending against worms like Stuxnet requires excellent capabilities marshaled into a coherent and coordinated response. The United States has plenty of the former but, in our view, has difficulty with the latter. Responsibilities can overlap or conflict. For example, stealing financial information is a crime, and the Federal Bureau of Investigation is charged to deal with such criminal activity. But the U.S. Department of Homeland Security has a mandate to protect the civilian agencies of the federal executive branch and to lead the protection of critical cyberspace. The former would include the federal banking system, and the latter could include the nation's banking system. Good intelligence has always been a prerequisite to good defense, but many attacks come from overseas locations. Therefore, efforts to garner intelligence outside the United States would involve the agencies authorized to do so. Many regard the National Security Agency as the most capable government entity when it comes to analyzing and defending against cyber attacks (see Clarke and Knake, 2010, p. 37; Dilanian, 2011; Alexander, 2010a, 2010b; and Shanker and Sanger, 2009). But legal limits constrain what the U.S. Department of Defense can do. Much illicit activity masks itself in emails, but privacy laws preclude the extent to which the government can monitor such transmissions.

None of this is to say that these limitations cannot be overcome. Indeed, a number of proposed pieces of legislation attempt to deal with them. Furthermore, federal agencies have improved their ability to effect the kind of coordination needed to deal with these problems. However, the challenge is great and is compounded by the speed needed to respond to increasingly sophisticated threats. Worms can be scrubbed from systems if its administrators know the systems have been breached. But they need to act quickly, or the worm will have done its damage and then erased itself.

Conclusions and Recommendations

This examination of Stuxnet and similar threats and their implications resulted in the following observations and conclusions:

- The threat of and opportunity for real damage from cyberspace is increasing.
- It is not possible to prevent all attackers from intruding on all networks and devices.
- The best defense includes an offense.
- Current organizational boundaries hinder efforts to successfully identify and mitigate intrusions.

Accordingly, we recommend additional congressional action to grant new authorizations that accomplish at least the following two goals:

[6] There is also a school of thought that such exploits constitute cyber crime if they can be identified as misuse under the Council of Europe Budapest Convention on Cybercrime (Robinson, 2011). The tenets in the Budapest Convention are cited in the President's *International Strategy for Cyberspace* (2011).

- Enable substantially better collaboration among the various government organizations that have a role in cyberspace and between these organizations and the private sector.
- Grant *at least one capable organization* the authority to track cyber intruders and criminals with the same freedom of maneuver that these adversaries enjoy. New authorities must be established for this to occur and it will likely require substantial revisions to the U.S. Code—undoubtedly a daunting challenge—and significant public debate.

These recommendations will require additional analysis and further development. However, as goals, they are essential to informing that process.

There is no simple solution to the threat posed by adversaries in cyberspace. Clearly, one challenge is determining how best to navigate within the requirements and expectations of a democratic society that relies heavily on its computer systems and networks, against an enemy that has no boundaries and can act with impunity in the face of national or international norms and legal frameworks.