Securing America Against Cyber War

Jayson McCune, College of Information Science & Technology, University of Nebraska at Omaha, Omaha, NE, USA

Dwight A. Haworth, Department of Information Systems, University of Nebraska at Omaha, Omaha, NE, USA

ABSTRACT

This paper expands on one aspect of Clarke and Knake’s (2010) recommendation for defending the United States’ Internet infrastructure from external attack. First it summarizes the threat that has been demonstrated in the recent past. Included are a number of data compromises that have been traced to servers in China. Also identified are potential physical attacks against facilities that employ supervisory control networks, with the Stuxnet virus being a recent example. Lastly, the fact that malware has been planted on computers in the electric power grid for later use makes an ability to block the command messages or the remote login sequence an absolute necessity. The paper identifies the 12 entry points into the United States’ Internet and, following Clarke and Knake’s (2010, p. 196) suggestion, specifies a firewall platform for those entry points. The total one-time cost for this defensive effort is estimated and found to be feasible. Finally, limitations of this approach are considered.

Keywords: Cyberwarfare, Firewall Platform, Internet Protection, Malware, Packet Inspection

INTRODUCTION

There is a serious threat to America’s current and continued security. This threat comes from reliance on the Internet. With the openness of the Internet and the potential for anonymity, the Internet becomes an easy avenue for enemies to stage a covert attack. “Some governments, like China, have made cyber-warfare a critical part of their military doctrine, in part to help counter the advantage the U.S. has in conventional and nuclear warfighting capability” (Cordesman & Cordesman, 2002, p. 12). The United States is highly vulnerable to a timed, well-organized attack from another state or non-state organization that would wish the country harm.

The severity of the damage that could be done varies greatly. It could range from nothing more than an inconvenience all the way to the collapse of the power grid or economic structure. The potential for damage increases as the American public and government rely more and more on the Internet for daily activities. The backbone of the American economy has increasingly incorporated high technology, principally computers and communications networks. Dependence on this electronic backbone is at a state that this backbone is now part of the
critical infrastructure of the country. Moreover, it is a highly vulnerable infrastructure, having evolved from components that were developed with no thought of security. “The result is a new form of critical infrastructure, one that is vulnerable to a new family of threats, loosely grouped together as information warfare” (Cordesman & Cordesman, 2002, p. 2).

They’ve [U.S. Government officials] got to be concerned about the information on their networks and ingress into their networks,” he [Shawn Henry, of the FBI] said. “The threat actor shouldn’t be all that important to them because once the information is gone, it’s gone. (Gross, 2008, p. 1)

The purpose of this paper is to examine, using open sources, the threat to the American Internet infrastructure and to develop in some detail one component of the defense of the American Internet infrastructure that is outlined by Clarke and Knake in Cyber War. First, the nature of the threat over the past decade will be examined. Then the first step that can be taken to reduce the number, and the severity, of cyber attacks will be explored. The paper will lay out the physical needs of the plan for this first step, the cost of the plan, and finally the limitations involved with this plan.

THE THREAT

Krekel (2009) summarizes a number of reports of attacks on the United States from 2004 to 2009. In November 2004, U.S. media reported that China-based hackers were able to penetrate several unclassified government networks. These networks included the U.S. Army’s Information Systems Engineering Command, the Defense Information Systems Agency, the Naval Ocean Systems Center, and the U.S. Army Space and Strategic Defense installation. In July 2006, the U.S. media again reported that hackers had infiltrated the U.S. Department of State networks, stealing information, logon credentials, and leaving many backdoors in the system. In August 2006, the Pentagon stated that hostile agents, originating in China, launched attacks at the American Government’s Non-classified Internet Protocol Router Network (NIPRNET) and downloaded up to 20 terabytes of data. In June 2007, approximately 1,500 computers were taken offline after a penetration of the email system in the Office of the Secretary of Defense. In November 2008, a report was published, stating that NASA had a significant cyber breach in their systems, dating back several years. The NASA penetration resulted in performance and engine data about the Space Shuttle being stolen. These and the other breaches reported by Krekel (2009) are only a small part of the activity going on in that period.

Diebert and Rohozinski (2009) report on an extensive effort to identify and investigate a cyber-network of more than 1200 compromised computers, of which “… close to 30% can be considered as high-value diplomatic, political, economic, and military targets” (p. 6). Diebert and Rohozinski (2009) report that control of this network is exercised from commercial accounts on Hainan Island in the People’s Republic of China. Diebert and Rohozinski’s (2009) conclusion is that their investigation “reveals a covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems” (p. 6). This threat has not diminished. McCaney (2012) summarized information from a Symantec report and an NSA speaker as “underscoring the growth in international cyber activity” (p.1).

But the threat extends beyond the loss of data. The Department of Homeland Security (DHS) conducted a security test, codenamed “Aurora”, on the control systems for a turbine electric generator at the Idaho National Laboratory. This must not be confused with the “Aurora attacks” of 2010 mentioned above. In this experiment, the researchers were able to destroy the generator through an Internet connection. The researchers were able to gain access to the mechanism that controlled the turbine’s rate of rotation. Through this control mechanism, the researchers were able to make
Related Content

Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape
www.igi-global.com/chapter/emerging-threats-for-the-human-element-and-countermeasures-in-current-cyber-security-landscape/199894?camid=4v1a

Strategic Communication for Supporting Cyber-Security
www.igi-global.com/article стратегическое-связи-для-поддержки-цибер-безопасности/104524?camid=4v1a
The Comprehensive Approach as a Strategic Design to Run the Military-Industrial Complex in Operations
[www.igi-global.com/article/the-comprehensive-approach-as-a-strategic-design-to-run-the-military-industrial-complex-in-operations/81251?camid=4v1a](www.igi-global.com/article/the-comprehensive-approach-as-a-strategic-design-to-run-the-military-industrial-complex-in-operations/81251?camid=4v1a)

The Value of Interaction for Russia, the USA and China Facing the Information Warfare
[www.igi-global.com/article/the-value-of-interaction-for-russia-the-usa-and-china-facing-the-information-warfare/105187?camid=4v1a](www.igi-global.com/article/the-value-of-interaction-for-russia-the-usa-and-china-facing-the-information-warfare/105187?camid=4v1a)