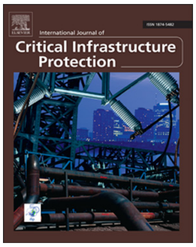
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



# Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices

Roland Bodenheim, Jonathan Butts*, Stephen Dunlap, Barry Mullins

Air Force Institute of Technology, Wright-Patterson Air Force Base, OH 45433, USA

ARTICLE INFO

Article history:
Received 15 January 2014
Accepted 27 March 2014
Available online 2 April 2014

Keywords:
Industrial control systems
Shodan
Security implications
Mitigation

ABSTRACT

The Shodan computer search engine has received significant attention due to its ability to identify and index Internet-facing industrial control system components. Industrial control systems are employed in numerous critical infrastructure assets, including oil and gas pipelines, water distribution systems, electrical power grids, nuclear plants and manufacturing facilities. The ability of malicious actors to identify industrial control devices that are accessible over the Internet is cause for alarm. Indeed, Shodan provides attackers with a powerful reconnaissance tool for targeting industrial control systems.

This paper investigates the functionality of the Shodan computer search engine. In the experiments, four Allen-Bradley ControlLogix programmable logic controllers were deployed in an Internet-facing configuration to evaluate the indexing and querying capabilities of Shodan: all four programmable logic controllers were indexed and identified by Shodan within 19 days. This paper also describes a potential mitigation strategy that employs service banner manipulation to limit the exposure to Shodan queries.

Published by Elsevier B.V.

## 1. Introduction

Industrial control systems are integral to the critical infrastructure, allowing the real-time remote management of large-scale industrial processes in oil and gas pipelines, water distribution systems, electrical power grids, nuclear plants and manufacturing facilities. In 2005, Hildick-Smith [4] estimated that more than three million industrial control systems were active; the expected annual growth of 8.9% means that there are more than six million industrial control systems in use today. This growth coupled with the market demand for sophisticated industrial control systems has contributed to increased network connectivity in order to reduce operational costs and increase efficiency. In many cases, industrial control systems are connected to corporate networks; in other circumstances, they are directly accessible over the Internet.

The Shodan computer search engine is designed to crawl the Internet and attempt to identify and index connected devices. Shodan has identified thousands of Internet-facing devices associated with industrial control systems [5]. The ability to identify devices that monitor and control critical infrastructure assets has raised major security concerns. The U.S. Department of Homeland Security recently published a report on Shodan that details the risk to exposed industrial control devices [7]. A CNN article [3] claims that Shodan is “the scariest search engine on the Internet.”

This paper examines the functionality of Shodan. Four programmable logic controllers (PLCs) were deployed to evaluate the indexing and querying capabilities of Shodan. The PLCs were configured to be Internet-facing and collocated with an industrial control system integrator. Experiments were conducted to demonstrate the ability of Shodan to identify and

*Corresponding author.
E-mail address: jonathan.butts@afit.edu (J. Butts).

http://dx.doi.org/10.1016/j.ijcip.2014.03.001
1874-5482/Published by Elsevier B.V.

index unadvertised PLCs. Additionally, the experiments evaluated the ability to limit the exposure of industrial control devices to Shodan queries by performing service banner manipulation.

## 2. Background

The U.S. Department of Homeland Security Industrial Control System Cyber Emergency Response Team (ICS-CERT) cited 171 unique vulnerabilities that affect industrial control system products as of December 2012 [11]. A recent NSS Labs report [2] notes a six-fold increase in industrial control system vulnerabilities from 2010 to 2012 [2]. The ability to compromise industrial control systems and the critical infrastructure assets they monitor and control presents real concerns and dangers.

In 2009, programmer John Matherly launched Shodan, a computer search engine with a graphical user interface that identifies Internet-facing devices [6]. In particular, Shodan can identify devices with routable IP addresses, including computers, printers, webcams and industrial control devices. Shodan crawls the Internet, indexing devices and interrogating available services along the way. It stores the collected device IP addresses along with ports and service banner data in a searchable database accessible via the Shodanhq.com web interface or via the Shodan API. Users may query the Shodan database using a series of filters that include country, hostname, net (i.e., specific IP address range), operating system and port.

Initially, Shodan interrogated basic ports such as port 21 (FTP), port 22 (SSH), port 23 (Telnet) and port 80 (HTTP), but its port interrogation has since been expanded to cover the 40 services listed in Table 1. In addition to device indexing, Shodan offers an exploit database, a raw nmap data output visualization tool and an enumeration module built into the Metasploit exploitation framework.

In October 2010, ICS-CERT published a Control Systems Analysis Report that details Shodan's ability to identify potentially vulnerable control system interfaces and discusses the importance of minimizing network exposure by ensuring that control system devices are not visible on the Internet [9]. Subsequently, ICS-CERT released five ICS alerts (ICS-ALERT-10-301-01, ICS-ALERT-10-301-01A, ICS-ALERT-11-343-01A, ICS-ALERT-12-046-01 and ICS-ALERT-12-046-01A) that highlight the concerns about Shodan's ability to identify Internet-facing industrial control devices [10].

In 2011, Leverett [5] used Shodan to counter claims of industrial control network segregation. Leverett presented 2 years of historical evidence, including timelines and geolocation data, for more than 7500 industrial control devices that were connected to the Internet – HVAC systems, building management systems, meters, human–machine interfaces and PLCs. A total of 29 Shodan search queries were used to identify industrial control devices. An evaluation 2 years later, in 2013, using the same queries revealed that the number of identified devices had increased dramatically from 7500 to 57,409. Leverett's research highlights Shodan's ability to serve as a reconnaissance tool for attackers interested in targeting industrial control systems.

**Table 1 – Shodan-documented service interrogation filters [6].**

| Port | Service |
|---|---|
| 21 | FTP |
| 22 | SSH |
| 23 | Telnet |
| 25 | SMTP |
| 53 | DNS |
| 80 | HTTP |
| 81 | HTTP |
| 110 | POP3 |
| 119 | NNTP |
| 137 | NetBIOS |
| 143 | IMAP |
| 161 | SNMP |
| 443 | HTTPS |
| 445 | SMB |
| 465 | SMTP |
| 623 | IPMI |
| 993 | IMAP+SSL |
| 995 | POP3+SSL |
| 1023 | Telnet |
| 1434 | MS-SQL |
| 1900 | UPnP |
| 2323 | Telnet |
| 3306 | MySQL |
| 3389 | RDP |
| 5000 | Synology |
| 5001 | Synology |
| 5432 | PostgreSQL |
| 5560 | Oracle |
| 5632 | PC Anywhere |
| 5900 | VNC |
| 6379 | Redis |
| 7777 | Oracle |
| 8000 | Qconn |
| 8080 | HTTP |
| 8129 | Snapstream |
| 8443 | HTTPS |
| 9200 | ElasticSearch |
| 11211 | MemCache |
| 27017 | MongoDB |
| 28017 | MongoDB Web |

In 2012, Radvanovsky and Brodsky [8] launched Project SHINE (Shodan Intelligence Extraction) in collaboration with the U.S. Department of Homeland Security. Project SHINE used the Shodan API and approximately 700 specially designed queries to identify more than 500,000 Internet-facing industrial control devices worldwide. Further research performed in coordination with industrial control system experts and ICS-CERT focused on 7200 devices, many of them lacking the most basic security controls (e.g., weak, default or no authentication mechanisms) [11].

## 3. Evaluation

This section evaluates Shodan's indexing functionality by examining its scanning routine, scanning frequency and web database identification timelines. Additionally, the use of service banner manipulation to limit the exposure of industrial control device to Shodan searches is discussed.