Emmeline Kuoch

21 April 2022

Shodan Analysis

Shodan was launched in 2009 by John Matherly and is ”the world's first search engine for Internet-connected devices” (Matherly, 2022). These “Internet of things”, or IoT devices, can be embedded in any system including “smart home, surveillance cameras, traffic lights, industrial control system, servers, routers, etc.” (TechTarget, 2016). Unlike search engines that are used for searching for websites like Google, which “crawls the World Wide Web”, “Shodan crawls the entire Internet every week” (Matherly, 2022). Shodan has been created with good intentions to find vulnerabilities and misconfigured gaps in IoT devices before hackers can exploit them (Gumaste, 2020). Cybersecurity professionals use Shodan to leverage their network security infrastructure through its data collection capabilities and to pinpoint which devices have little to or no security both at the professional and societal levels. This ensures that any loose backdoors are identified and secured. Several cybersecurity researchers make use of Shodan to “detect devices like routers, firewalls, that make use of default credentials or simple passwords” (Fernández-Caramés & Fraga-Lamas, 2020). Information from Shodan is essentially limitless. It includes where devices are geographically located through their IP address, country of origin, the name of the organization, server name, and who is using them. Shodan utilizes a banner grabbing technique in order to extract metadata from computer systems and services that are running on open ports. Surprisingly, roughly more than “3.7 billion public IPV4 Addresses and hundreds of millions of IPV6 Addresses are collected by Shodan” (Bada & Pete, 2021). Shodan is free to explore and comes with “hundreds of pre-made search queries that are designed for exploiting VOIP devices, webcams, and routers” (Rae et al., 2019). Shodan’s platform enables

policymakers and journalists to spread systemic security issues that the internet is facing on a daily basis (Porup, 2022). This illustrates the vast scale of authorized surveillance where critical information is constantly being utilized. Shodan is made publicly available and monitored by the cybersecurity community that serves as a backhand for external visibility for organizations throughout the world.

However, with Shodan being practically free to roam and explore, it can potentially be dangerous especially if it goes into the wrong hands. With Shodan's ability to find devices such as controls systems for nuclear power plants, gas stations, garage doors, printers, servers, cameras, etc., they can instantly become a prime target. These devices can easily lure in hackers at a global level, given very little security built into them such as "weak credential security and the lack of basic authentication measures which are common in IoT devices" (Fernández-Caramés & Fraga-Lamas, 2020). Cybersecurity measures often times are neglected until the "very final stages of product development in IoT products" (Fernández-Caramés & Fraga-Lamas, 2020). With very few safeguards, a malicious hacker can do a quick search for a "default password" in Shodan to obtain credentials for controls that lack security. As a matter of fact, "many more connected systems require no credentials at all -- all you need is a Web browser to connect to them" (Goldman, 2013). With that ability in hand, cybercriminals can comprise these vulnerable devices and interconnect them to make an army of Botnets. Botnets give hackers the upper hand to perform an overwhelming large-scale attack by sending spam, stealing data, and Distributed Denial-of-Service aimed at a target. In particular, Shodan's API is highly used to create botnets by "automating scanning for devices" (Bada & Pete, 2021). Through this, hackers can gain personally sensitive information by having control of these IoT devices remotely. Such sensitive information includes usernames, passwords, user identification,

health records, etc. Likewise, hackers can access cameras remotely for IP camera trolling to "collect images and videos and use them in for example extortion use cases" (Bada & Pete, 2021). This is a major concern as most users are not aware of the information that they are giving away when utilizing these solutions in their day today. Shodan proves to be a versatile attack resource for cybercriminals in the IoT hacking community, as it is actively used to gather information thus providing easier access to hackable devices (Bada & Pete, 2021).

All in all, Shodan has transformed the IoT landscape and its capabilities have proven to be used for both malicious purposes and for the better, to improve society's information security ecosystem. It "has brought face to how the human factor will continue to be a force for security professionals to contend with as more and more devices are brought into the internet world network. Shodan's capability has allowed for both sophisticated attacks to be executed as well as providing powerful ways to identify threats and harden managed networks" (Rae et al., 2019).

References

Bada, M., & Pete, I. (2021, February 2). *An exploration of the cybercrime ecosystem around shodan*. IEEE Xplore. Retrieved April 21, 2022, from https://ieeexplore.ieee.org/document/9340224

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020, May 27). *Teaching and learning IOT cybersecurity and vulnerability assessment with shodan through practical use cases*. MDPI. Retrieved April 21, 2022, from https://www.mdpi.com/1424-8220/20/11/3048/htm

Goldman, D. (2013, April 8). *SHODAN: The Scariest Search Engine On the internet*. CNNMoney. Retrieved April 21, 2022, from https://money.cnn.com/2013/04/08/technology/security/shodan/index.html

Gumaste, P. (2020, August 31). *What is Shodan?* Whizlabs. Retrieved April 21, 2022, from https://www.whizlabs.com/blog/what-is-shodan/

Matherly, J. (2022). Shodan. Retrieved April 21, 2022, from https://www.shodan.io/

Porup, J. M. (2022, March 29). *What is Shodan? the search engine for everything on the internet*. CSO Online. Retrieved April 21, 2022, from https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html

Rae, J. S., Chowdhury, M. M., & Jochen, M. (2019, May 20). *Internet of things device hardening using shodan.io and shovat: A survey*. IEEE Xplore. Retrieved April 21, 2022, from https://ieeexplore.ieee.org/document/8834072

TechTarget, C. (2016, August 10). *What is shodan? - definition from whatis.com*. WhatIs.com. Retrieved April 21, 2022, from https://www.techtarget.com/whatis/definition/Shodan