# An exploration of the cybercrime ecosystem around Shodan

Maria Bada* and Ildiko Pete*
Department of Computer Science and Technology, University of Cambridge
Cambridge, UK
firstname.lastname@cl.cam.ac.uk
*These authors contributed equally to this work

***Abstract*—Discussions on underground forums provide valuable insights to hackers' practices, interests and motivations. Although Internet of Things (IoT) vulnerabilities have been extensively explored, the question remains how members of hacker communities perceive the IoT landscape. In this work, we present an analysis of IoT related discussions that are potentially cybercriminal in nature. In particular, we analyse forum threads that discuss the search engine Shodan. The source of these posts is the CrimeBB dataset provided by the Cambridge Cybercrime Centre (CCC)[1]. We analyse 1051 thread discussions from 19 forums between 2009 and 2020. The overall aim of our work is to explore the main use cases of Shodan and highlight hackers' targets and motivations. We find that Shodan is versatile and is actively used by hackers as a tool for passive information gathering providing easier access to hackable targets. Our results suggest that Shodan plays a prominent role in various specific use cases including remote control of target devices, building botnets, Distributed Denial of Service attacks and identifying open databases.**

***Index Terms*—Shodan, Internet of Things (IoT), IoT Security, Underground Communities, Dark Web**

## I. Introduction

Internet of Things (IoT) solutions, which have permeated our every day life, present a wide attack surface. They are present in our homes in the form of smart home solutions, and in industrial use cases where they provide automation. Despite the obvious benefits they offer, vulnerabilities in IoT solutions are numerous and pose serious challenges ranging from security to privacy issues [1], such as leaking personally identifiable and sensitive information. 70% of IoT devices do not support granular access controls, strong encryption and secure programming principles [2]. An indicator of the potential harm neglecting the security of IoT devices can cause, is the Mirai botnet demonstrating the power of IoT botnets in carrying out DDoS attacks [3].

The potentially profound effects of IoT attacks have attracted much research attention with a focus on an in-depth understanding of IoT related security issues, for example through the identification and classification of vulnerabilities [4], or through observing attacks [5], to name a few. However, currently there is a lack of understanding of the IoT landscape from the perspective of the hacking community. Analysing interactions of members of underground forums provides a novel perspective of IoT security and reveals vulnerabilities that are actively discussed, the main targets, and hackers' motivations to exploit these vulnerabilities.

Specifically in this study, we analyse discussions around *Shodan*, one of the most popular search engines of Internet facing devices and services. *Shodan* is designed to crawl the Internet and to index discovered services [6], and it allows the discovery of vulnerable devices [7]. Thus, it is widely used by security professionals and have greatly contributed to raising awareness of the problems facing the IoT landscape. *Through analysing Shodan related discussions on underground forums we explore the role it plays in the cybercriminal ecosystem of IoT hacking and exploitation.* Relatedly, we are also interested in exploring the main motivations of using *Shodan*, and popular targets of exploits in scenarios where *Shodan* is used. Since it has been around for over a decade, naturally the question arises how its perception and popularity evolved over time and whether at present it is deemed a mature tool that is well-known by the community and used in multiple use cases. To answer these questions we performed a *qualitative analysis* of threads and posts extracted from multiple underground forums. We found themes related to the type of post, targets, motivations, tools and the human factor, which paint a general picture of these discussions including hackers' motivations and targets. Next, we identified the main use cases of Shodan to gain an understanding of the role it plays. The remainder of the paper is structured as follows. We provide background on Shodan and a summary of related work in underground forum analysis in Section II. We describe our methodology in Section III, and detail our findings in Section IV. We conclude with a discussion in Section V.

## II. Background

### A. Shodan

Launched in 2009 by John Matterly [6], *Shodan* is one of the most popular search engines used to discover Internet connected devices besides alternatives including Zoomeye[2],

[1]https://www.cambridgecybercrime.uk/

[2]https://www.zoomeye.org

Censys[3], PunkSpider[4] and Ichidan[5]. It aggregates information on more than 3.7 billion public IPv4 addresses and hundreds of millions of IPv6 addresses [8], and provides information for vulnerability assessments [6] as well as data on the magnitude of IoT [9]. A quick search on Shodan reveals different types of systems connected to the internet, such as SCADA systems, and associated information such as IP address, city, country of origin, open ports and services, name of the organisation and ISP. To filter for specific systems, search filters can be utilised. Basic functionality requires setting up an account, while advanced functionality requires paid credits [10].

With the growth of IoT, interest in malware attacks against IoT devices has been at the forefront of cybercrime. Malicious actors focus on attacking these devices to create Botnets to be used to further an illegal agenda. Shodan can be used to compromise and recruit vulnerable devices to create a large Botnet in a short amount of time [11].

**Shodan as a tool for vulnerability analysis of IoT devices.** In literature Shodan appears mostly with respect to vulnerability analysis of IoT devices and solutions [12] [8] [6]. Previous research has focused on the use of Shodan and other search engines from the perspective of the security expert or the researcher, revealing that their vulnerabilities expose them to attacks by malicious actors [12].

Findings from vulnerability assessments using the Shodan search engine and the Common Vulnerabilities and Exposures database indicate that a significant number of smart cameras are prone to diverse security and privacy vulnerabilities [13]. Another study on webcams discovered by Shodan found that most hosts have little to no firewall protection and, as such, are great attack facilitators in direct and reflective DDoS attacks [14]. In addition, IoT botnets have exposed two main issues: a) a large number of IoT devices are accessible over public Internet and b) security (if considered at all) is often an afterthought in the architecture of many wide spread IoT devices [15]. The ease by which attackers can locate IoT devices using online services, such as Shodan, provides an ever expanding pool of attack resources. By leveraging multitudes of these vulnerable IoT devices, attackers can perform large scale attacks such as spamming, phishing and Distributed Denial of Service (DDoS) [16]. Therefore, Shodan and other search engines allow malicious hackers to find and exploit vulnerable target devices. The popularity of Shodan amongst malicious actors, especially to exploit IoT devices, has led this study to focus on underground forum discussions centred around Shodan as a tool for IoT exploitation. In the following subsection, we provide a brief overview of underground forum literature, where this study is positioned.

[3]https://censys.io/

[4]https://www.darknet.org.uk/2016/09/punkspider-web-vulnerability-search-engine/

[5]https://threatvector.cylance.com/en$_us/home/ichidan-a-search-engine-for-the-dark-web.html$

### B. Underground Forum Analysis

IoT security enjoys active research attention. The reader may refer to the following surveys to explore the area [1] [4]. However, currently, there is little research examining underground forum discussions related to IoT. A recent report by Trend Micro [17] analyses conversations in underground communities. It shows that IoT is a popular subject on Russian, Portuguese, English, Arabic, and Spanish language underground forums. Additionally, the report highlights that these forums serve as thriving marketplaces for IoT-based attacks and services, and predicts a growing interest in the area by hacking communities.

Previous studies in underground forum analysis have focused on understanding criminal pathways, characterising key actors related to illegal activity in underground forums [18] or understanding the tools used [19]. Our work draws on insights from these studies on underground forum analysis.

## III. Methodology

### A. Qualitative Analysis

Our methodology is based on a *qualitative analysis approach*. Specifically, we performed thread-level *thematic analysis* of content to identify Shodan related topics discussed in the analysed forums [20]. We chose this approach due to its potential to provide a detailed understanding of the problem area this study aims to research. First, the two authors familiarised themselves with the data, followed by a coding step, in which the authors created labels and notes for each sample while reading posts to extract relevant themes from the data [21]. After initial candidate themes were generated based on the labels, the authors reviewed and refined the themes.

### B. Data - the CrimeBB dataset

We extract relevant underground forum posts from the *CrimeBB* dataset [22], collected and made available to researchers through a legal agreement by the *Cambridge Cybercrime Centre (CCC)*. Our selection of the dataset was motivated by the opportunity this data provides us with, to assess cybercrime correlates of engagement and macro-level trends [23]. CrimeBB contains a collection of dark and surface web forums to allow analyses of communities active in these forums. The forums, which provide a platform to exchange ideas and engage in activities, some of which are illegal, are typically structured in a similar manner. That is, they are usually divided into sub-forums containing discussions around specific topics ranging from hacking to marketplaces. Discussions in each sub-forum that revolve around a specific subject are organised into threads. Finally, threads contain individual posts written by members of the forums.

Our analysis spans multiple surface web and dark web forums available in CrimeBB presenting discussions from *2009* to *2020*. Each forum has a specific profile shown by the users it attracts and the topics its members discuss. Thus, we expect that they exhibit varying interests in IoT related subjects. Specifically, the majority of posts we analyse stem from Hackforums (HF), one of the largest general purpose

hacking forums covering a wide range of topics, including IoT. HF is notable for being the platform where the source code of the Mirai malware was released in 2016 [24]. Further forums providing posts for our analysis include lolzteam, Torum, RaidForums, PirateBay Forum, Nulled, GreySec Forums, Garage4hackers, Dread, KernelMode, FreeHacks, Offensive Community, V3rmillion, BlackHatWorld, Antichat, Cracked.to, MPGH, The Hub, and UnKnoWnCheaTs.

To extract the data required for our analysis we performed a database wide search in CrimeBB using the keyword 'Shodan'. This yielded a dataset of approx. 1,200 posts. Next, we reconstructed each individual thread that contained the 'Shodan' related posts, which provides a greater detail and context to each post, and makes the intent of the participants clearer. This step resulted in *1051* threads, which contained a total of *94293* posts. We performed thematic analysis on these posts, which resulted in the identification of themes that provide a deeper understanding of the cybercrime ecosystem around Shodan. It is not within the scope of this work to carry out a quantitative analysis of the data. However, as a future research avenue, the current analysis can be complemented by quantitative methods. Specifically, given the textual nature of the data, Natural Language Processing methods can be applied.

**Ethical Considerations.** We received approval for this work from the ethics committee of the Department of Computer Science and Technology. The ethics approval was granted based on the criteria of data handling, confidentiality and anonymity, risks to participants and to researchers. The data collected from underground forum posts are publicly available. We do not publish any user names or process personal information. In accordance with the British Society of Criminology's Statement on Ethics, this approach is justified as the dataset is collected from public forums. Therefore, no consent was obtained from users, as this would be infeasible and contradictory to the goals of our study.

**Limitations.** The main limitation of this study stems from the fact that the analysis focuses on specific underground forums. Thus, the generalisability of our results needs to be further studied using different data sets.

## IV. Findings

### A. Themes

The thematic analysis of posts resulted in the discovery of a number of themes. These themes, detailed in the remainder of this subsection, provide insights to the discussions and a framework to investigate the role of Shodan in the cybercrime ecosystem.

**1. Type of post.** The first theme that emerged from our analysis indicates whether the author of the post aims to share or request information on a subject related to *Shodan*. Members typically provide either guidance on a specific subject, such as exploiting a particular service, or general hacking advice. Some users ask for help with identifying vulnerable devices or specific targets using Shodan. On the other hand, some requests centre around getting started with Shodan, with members seeking advice which suggests that these members are new to Shodan and exploiting IoT devices. Users also request information on alternative tools, which suggests some experience with Shodan, and perhaps being aware of its limitations in specific usage scenarios. Others request advice about Shodan to understand whether it is a useful tool for their purposes or whether it is legal to use it. As shown by 'getting started with Shodan' posts from 2018, some members have discovered Shodan particularly late considering that it has existed since 2009. Finally, the discussions suggest that some users aim to monetise their knowledge, whereas others request to buy certain services or exploits. The majority of such posts concern Shodan accounts, however some serve as advertisements for selling hacking tools or web application attacks.

In tutorials members describe in detail the methodology of an IoT hacking activity. Examples include tutorials on passive reconnaissance techniques, intelligence gathering, identifying vulnerable webcams and routers, and exploiting targets. Tutorials also help identify the role Shodan plays in IoT attacks and provide a glimpse into hackers' IoT related practices. The methodology of IoT hacking is similar to that of hacking in general. They both start with information gathering on the target. Shodan and similar tools play a key role in passive information gathering. Whereas in case of general hacking attackers may use 'nmap' or 'zmap' to find their targets as part of active information gathering. In both cases the next phase of attacks is the exploitation of the target through some vulnerabilities. As expressed by the following post, Shodan simplifies IoT hacking:

> '... Shodan and other tools, such as exploit-db make hacking almost like a recipe that you can follow.' (Quote 1)

**2. Target.** The next theme provides insights to active areas of interest and the most popular IoT target devices. We found that members who post about Shodan aim to achieve one or more of the following:

1) Scan for specific targets or vulnerable devices in general
2) Gain access to vulnerable devices
3) Exploit specific targets or vulnerable devices in general
4) Buy or sell Shodan accounts, credits, results

| Type of Target | Specfic Instances |
|---|---|
| Cameras | IP, Web, CCTV |
| Systems, Devices & Servers | VPN & NFS servers, VNS & SCADA systems, NAS devices, Embedded serial device server: NE-4110S, Seagate external hard drive, Supermicro motherboard, Heating systems, Polycom video conferencing, PBX, Open databases |
| Miscellaneous | Series-to-Ethernet converters of type GC-NET2 32-DTE used by Spanish gas stations, Billboard systems, Power plants, Traffic light and traffic control systems, cPanel hosting platform |
| Smart Homes | TV boxes, Thermostats |
| Routers | - |

TABLE I: Targets discussed on underground forums

Findings from vulnerability assessments indicate that a significant number of smart cameras are prone to diverse security and privacy vulnerabilities [13]. In addition, most might have little to no firewall protection and, as such, are vulnerable to future direct and reflective DDoS attacks [14]. A single study alone highlights more than 120,000 exploited Internet-facing IoT devices in 2019, some of which operate in critical infrastructure sectors such as health and manufacturing [25]. In the light of this, identifying popular targets is useful in raising awareness of the vulnerabilities associated with these systems. Table I shows the main device categories that were discussed as potential targets.

**3. Motivation.** The third theme we explored relates to factors that motivate users of the analysed forums to target specific services. The true impact from unauthorized access to a system depends on both what the system is doing and on what the agenda of the person accessing the system is.

Through an analysis of a sample of posts in a more generic IoT related board 'IoT, Embedded Devices, Electronics and DIY' on Hackforums, a category of motivations emerged. These are not criminal in nature, and relate to learning about technologies out of curiosity primarily to conduct hobby projects, for example for home automation purposes. This stands in contrast with our findings based on the 'Shodan' related posts. Overall we found that some members request or provide advice on scanning for and exploiting their targets simply for fun, either as a project to get started in IoT hacking, or to test their knowledge and skills in the form of IP cam trolling.

> 'The only purpose to hacking cameras is for fun, it's pretty easy. Any skid like myself can do this.'
> (Quote 2)

**4. Tools.** Hackers utilise a variety of tools to carry out reconnaissance and perform attacks. General hacking tools mentioned alongside Shodan include *Hydra*, a password cracker, which was mentioned in the context of exploiting IP cameras discovered through Shodan. Hackers utilise Google searches to find default usernames and passwords of devices they plan to compromise. *'Google dorks'*, that is, advanced Google search operators, are considered an outdated yet still widely discussed approach to finding exploitable devices, which can also be identified using *exploit-db*. 'GitHub' provides valuable resources for security professionals, however hackers can also make use of code hosted there to find backdoored versions of legitimate apps and other malicious code. It can also be used to find alternatives to Shodan. Finally, the discussions revealed that users who mention Shodan, also discuss the following information gathering, scanning and pentesting tools: 'Maltego', 'Metasploit', 'Armitag', 'Recong-ng', 'The Harvester', 'nmap', and 'zmap'. These tools are summarised in Table II.

There exist multiple tools that improve on different aspects of Shodan and automate the processing of query results. These are: 1) 'Argo' automates host gathering from Shodan and Censys; 2)'Shogun' is a custom Shodan CLI that makes it easier to search using Shodan; 3) 'Leaklooker' is used specifically to reduce effort in finding open databases when using Shodan; 4) 'Shodanier' provides an extended version of Shodan; 5) 'Shodansploit' also extends Shodan by allowing users to perform more detailed searches using the Shodan API.

Members also discuss multiple alternatives to Shodan such as 'Zoomeye' - a search engine that provides data from publicly exposed devices and web services, the 'Cencys' search engine, 'PunkSpider' - a web vulnerability search engine, and custom code written by members. Another similar search engine, 'Ichidan', operates on the dark web and searches for Tor Onion sites, making it possible to find security holes in dark web services.

| | |
|---|---|
| **General Hacking Tools** | Hydra, Google dorks, exploit-db, GitHub, Maltego, Metasploit, Armitag, Recong-ng, The Harvester, nmap, zmap |
| **Tools used with Shodan** | Argo, Shogun, Leaklooker, Shodanier, Shodansploit |
| **Shodan alternatives** | Zoomeye, Cencys, PunkSpider, Ichidan |

TABLE II: Overview of hackers' toolkit used with Shodan

**5. The human factor.** The final theme highlights a prominent aspect of IoT security, the human factor, which naturally appears in discussions, as users' competences and practices also influence whether an IoT solution presents an attractive target. In particular, we found that discussions related to the human factor concern:

1) *Social engineering*, the manipulation of people to give out information
2) *Using default passwords*
3) *Users' skills or the lack thereof.* At the centre of these discussions is the concept of human weaknesses and their exploitation.

### *B. The role of Shodan*

We set out to explore the cybercrime ecosystem around Shodan and understand how the tool is used by hackers. Now that we highlighted the main topics that are discussed in Shodan related posts, we are in a better position to gain a deeper understanding of the role it plays. We discover this through the main use cases for Shodan that emerged based on the previously discussed themes.

**Use Case 1: Gain Personally Identifiable Information (PII).** IoT devices can expose personally identifiable information, sensor data, video surveillance footage, audio recordings, or activity data exposing how a user interacted with a device [26]. This is a serious concern, as average users are not aware that they share their information when using IoT solutions [27]. This is in line with our findings, which suggest that members of underground forums actively discuss using Shodan to gain personally identifiable information, which allows for the identification of an individual, and may include passwords, usernames, or health records.

Forums are ripe with discussions on identifying open databases using Shodan. In particular we found discussions of MongoDB database leaks. According to a 2018 article, as of 2018 there were around 54 000 unsecured MongoDB

databases accessible on the internet [28]. Members also discuss MongoDB related vulnerabilities:

> 'Mongo DB NoSQL, or rather NoAuthentication, has been a great gift for the hacker community. Just when I was worried that all authentication bypass errors in MySQL had finally been patched, new databases went into the style that lacked authentication by design.' (Quote 3)

Indeed, Shodan proves to be an immensely useful tool for such exploits, as open MongoDB databases can be easily searched via the following query: *"Set-Cookie: mongo-express=" "200 OK"*. The search process can be further simplified by using the tool *Leaklooker*, which reduces effort in finding open databases with Shodan (paid plan is required):

> '...takes the results and shows only instances bigger than 217 MBs and accelerates your hunt. In some cases it was hard to exclude hacked databases, because when hacker left ransom note, data are still present, it applies to Elasticsearch and MongoDB. Among found information by script, there were a lot of personal identification information (PII), medical data, casinos transactions, credit card owners data, GPS tracking information, archived data of accounts of specific groups in social media, API tokens...' (Quote 4)

**Use Case 2: Building botnets.** Botnets are created by hackers enslaving vulnerable devices into an 'army' of resources that can be used in subsequent attacks aimed at overwhelming a target. Due to their specific characteristics, IoT devices in particular represent a low hanging fruit for hackers who are thus encouraged to build botnets that comprise of IoT devices to launch DDoS attacks [29]. Building a botnet at the most basic level consists of multiple steps including scanning for vulnerable - in this case IoT - devices, accessing them, downloading malware to the device, executing the malware and communicating with the infected device [29]. We found that discussions were ripe with tutorials on how to perform these steps and there is a considerable interest in building botnets. The specific role Shodan, and in particular the Shodan API plays is that it automates scanning for devices which could be used to create a botnet. Shodan is discussed as a tool that lowers the barrier to enter IoT hacking and is particularly useful when users seek a simple way of getting started with building botnets:

> 'you don't need fancy exploits to get bots just look for bad configurations on shodan.' (Quote 5)

To effectively use Shodan for this purpose, Shodan credits are required. In Use case 5 we describe the trading activities of members with respect to Shodan credits and accounts in greater detail.

> 'This is a guide on how to make a clever bot using only web programming languages and Shodan ... First visit Shodan [LINK], create an account and buy some credits. This credits will be used by your bot to request new ip addresses to spread ... Now start by coding a GET request using your keys with the search term for the device you are targeting and manipulate the values into your programming environment. From this point, extract the ip addresses and create a authentication method (for example http-basic). Now with a help of jQuery and Ajax you can make POST requests to authenticate and change the information in the device. For example, if it's a router you can change the SSID to whatever you want. A good choice will be to advertise in the small SSID space a service or anything you have to offer including a number or email. That's it, happy hacking.' (Quote 6)

Finally, users build botnets for various purposes. In this example the member is interested in building a botnet to perform cryptocurrency mining:

> '... i've used autosploit & shodan to gather vulnerable devices and added several linux exploits but no luck...i have a linux miner ready to go, anyone able to assemble a net for mining monero?' (Quote 7)

**Use Case 3: Remote control of a target device.** The theme 'Target' highlighted that a major use case of Shodan is identifying devices and exploiting them to control them remotely. This can either take a more passive form, where the hacker gains access only, or an active form, where they can perform modifications, such as playing audio through the device. It is well documented that security camera systems are one of the least secure amongst IoT devices, and account for 47% of attacks. This is partly due to the fact that they are built on similar models, thus making it easier for hackers to access them [30]. It is therefore not surprising that cameras constitute one of the most popular targets. We found both general and specific information on how to scan for and exploit these. As noted by Vlajic and Zhou, the surge of interest in IP cameras besides their apparent security flaws might also be attributed to their weak anti-DDoS protection and reflective potential, which makes them ideal targets [14]. Despite efforts of security professionals to raise awareness of the issue, it remains true today, and members of underground forums show interest in targeting these devices, as shown by a post from 2019:

> 'I need help in cracking IP cameras.' (Quote 8)

**IP Camera Trolling.** The motivations to gain remote control of a camera are manifold: watching the video stream of and listening to audio through a compromised vulnerable camera; watching people; or exposing someone through their camera recording. Hackers frequently utilise Shodan to gain remote access to cameras for 'IP camera trolling'. This is also shown by the related Google search terms, and the number of search results for 'IP Camera Trolling' that appear on YouTube. Discussions also contain a significant number of posts sharing leaked video footage and websites that list hacked cameras. With regards to the motivating factors to carry out IP Camera Trolling, one of the reasons is to play pranks, while more maliciously inclined actors can use such exploits

to collect images and videos and use them in for example extortion use cases. We found evidence to support the former:

> 'We could do some serious trolling. Get the persons name and have a few people do a quick dox, lol. We could social engineer someone into doing something, and we would get to see it happen live on cam. Do it for the lulz anyone?' (Quote 9)

**Use Case 4: Distributed Reflection Denial of Service attacks.** It has been established that Shodan and similar search engines are a goldmine for distributed denial of service (DDoS) hackers as they facilitate effective searches and remove the first step of the traditional attack process [14].

As a specific type of distributed denial of service attacks, reflective attacks make use of reflectors, that is, a host that returns a packet when sent a packet. When an attacker has a sufficient number of reflectors, they send spoofed packets to them, with the source IP address set to that of the victim. Thus, traffic is generated and sent to the victim [31]. This kind of attack normally consists of two major parts. First, the malicious actor performs a scan to identify potential reflectors. Once a list of reflectors is in place, the attack phase can begin, which directs unsolicited traffic to the victim. Shodan comes into play in these attacks in the first step when a list of reflectors is gathered, e.g. NTP servers, which then can be used to carry out the actual attack.

> 'Shodan is currently detecting around 762,644 NTP servers in the DMZ. How do I do it? Manipulate the UDP header yourself or use the python script: [LINK] Requires root and scapy library (sudo apt-get install python-scapy)' (Quote 10)

In a similar vein, this post from 2019 describes the role Shodan can play in carrying out DDoS attacks.

> '....Just search shodan for some dns servers and do dns reflection attack spoofing target ip. Or you can use ntp servers, spoof victim ip and send the list of ntp servers the get monlist command and bam game over. Or if you really want to really fugg Clay Davis up and break the internet with terabit addos attacks find memcached servers.' (Quote 11)

Besides providing advice, members also share tools, which process data obtained from Shodan. For example a DDoS exploit tool, which utilises a list of memcached servers to be used in a reflection attack.

> '... a Python script called Memcacrashed.py which scans Shodan for vulnerable Memcached server IP addresses and allows a user to launch a DDoS attack against a desired target in a matter of seconds after executing the tool... (Quote 12)

**Use Case 5: Shodan account trading.** Although anyone can setup a Shodan account for free and each account comes with a free API plan, performing queries and processing query results are somewhat limited. For example, at the time of writing this paper the Freelancer plan caps queries at 1 million results per month, while the Corporate plan allows for unlimited results. Additionally, certain filters are available only in specific plans. Shodan operates a credit plan model both for the website and the API. There are three types of credits: *query credits* to allow searching on Shodan, *scan credits* used to scan IP addresses and *export credits* to download results. Out of the available packages only the Corporate plan provides unlimited *scan credits*, while the others set a limit. One *scan credit* allows the scanning of one IP address, and one *export credit* lets users download at most 10 000 results [7].

Based on the use cases introduced above it is apparent that to effectively utilise Shodan as a tool in hackers' repertoire used with automated scripts, hackers need to and strive to obtain premium plans to allow unlimited queries, scans and exports. For example, if a forum member would like to use the 'Memcrashed' DDoS exploit tool mentioned in the previous section, they require an upgraded Shodan API as stated on the tool's GitHub page. Thus, a system of trading with Shodan accounts has evolved on the forums where actors can buy and sell Shodan related assets. Subject to the hacking activities forum users intend to perform, we found that they were interested in buying Shodan API keys, premium Shodan accounts, and search results (exports). Sellers mostly offered Shodan (premium) accounts, Shodan credits, alternative scanners, and .edu email accounts, which provide a free upgrade.

> 'I have recently started using Shodan for ip pulling and haven't had much success, so i decided to look into upgrading. The prices i saw were outstanding for just pulling ips. I then found a thread on a website saying you can be freely upgraded if you have a .edu email. I thought how lucky am i? i sell them, so i have alot on hand.' (Quote 13)

Prices for export credits range from *0.50 USD* (when bulk buying) to *4 USD*, and payments were requested to be made in bitcoin. The following example shows the price of premium accounts:

> 'Sell Shodan.io Premium Membership Account. What you get: 1) All add-ons (HTTPS, Telnet, view up to 10,000 search results); 2) 100 Export credits; 3) Improved API plan (access up to 20 million results/ month); 1 Account = $10 / 0.0025 BTC, Stock = 100+ Account' (Quote 14)

Lastly, we found that besides premium accounts and API keys there is demand for Shodan XML files, which contain Shodan query results, ready-to-use. This suggests that a subset of Shodan users do not search for vulnerable targets themselves, instead they purchase the output of Shodan searches, that is, a list of vulnerable services/devices of interest.

### *C. Shodan as a hacking tool*

In the previous section we introduced five specific use cases of Shodan. In this section we highlight where it falls in a typical hacking workflow. In general, it is utilised in the first step as a reconnaissance and passive information gathering tool:

> 'Open reconnaissance tools like dnsdumpster.com and shodan.io make it easy to find hosts and open

ports/services associated with a given domain without ever having to scan the target.' (Quote 15)

The discussions highlight that Shodan is a versatile tool and can be used to explore easy-to-hack targets:

> 'for toying around with new exploits in the wild when you just can't seem to build it on a vm your self'. (Quote 16)

The following excerpt from a tutorial demonstrates the steps of using Shodan in the context of a specific exploit. This user also highlights a limitation of the search engine worth noting, that is, not all the results returned by Shodan are relevant.

> 'I will be explaining how to search Shodan.io for VNC (Virtual Network Computing) Devices With Authentication Disabled. (Remotely Controlling A Computer)
> Step 1: Get Shodan ... your first step of course is to sign up for a shodan.io free account
> Step Two: Get a VNC Client
> Step Three: Secure Yourself ... use a VPN ...
> Step Four: Searching For Connections. Shodan is only powerful if you know how to utilize its resources. Filters play a huge part in the ability to target and find your victims. If you know what is in the banner info that is displayed, or if you can find out how a specific device communicates with Shodan's crawler, you can find what you are looking for quite easy ... we are looking for non-password protected vnc connections. Searching ""Vnc"" yields excessive, worthless results, so we need to get more specific ... If you wanted to get more specific, and have sprung for a paid account (for 2+ Filters), you can get more specific with your searches ... we have narrowed our search down to US based IPs, and it is now time to find ourselves a victim.
> Step Five: Finding and Increasing Chances of Good Hosts. Not every result we get from Shodan is currently going to be live, and to save yourself some time, theres about an 85% chance that the results which appear as all black boxes are not going to be online, so we will skip around the search results until we find what looks like an eligible result...
> Step Six: Using VNC-Viewer and Connecting ...' (Quote 17)

**Specific exploits.** The following examples provide a glimpse into cases where hackers either have a specific target or a specific vulnerable service in mind to exploit.

- Scan for WiMAX routers: *'Most of these routers are running defualt usernames and password which I put in the thread. The username:password to these boxes are wimax:wimax820. You can write a simple checker in bash. You need a shodan API key.... Use them as SSH tunnels.' (Quote 18)*
- Find vulnerable SCADA systems: *'We will be using Shodan for finding vulnerable SCADA systems ... Here are some useful queries: [SHODAN QUERIES] ... After getting the SCADA, they can be brute forced or Bypassing Authentication can be used.' (Quote 19)*
- Hack Wordpress Websites

**Is IoT still of interest in hacking communities?** The latest discussions related to Shodan reveal whether it is mentioned in novel contexts and if its popularity has changed over time. Posts from 2020 show that there is continued interest in Shodan, demonstrated for example by discussions mentioning the 'Shodan-eye' script, which makes use of the Shodan API to collect information about Internet connected devices. Given Shodan's credit plan, Shodan API keys remain a key consideration when it comes to utilising the search engine for specific exploits, and Shodan is actively used: *'Just wrote up a quick little script that will rotate out a Shodan API object with a random key when given a keyfile!' (Quote 20)* Further, users show continued interest in utilising Shodan to identify leaked databases, exploiting cameras and other vulnerable services. Finally, let's take a look at a full thread titled 'Iot is dead', which highlights that although the IoT landscape is ever changing, it remains an invaluable asset for hackers.

> 'Went around and bought a couple servers. Setup a QBOT, and did some scanning. The results were very poor, just a couple bots from the classic SSH, a few more from telnet, and none from the usual exploits. So, is IOT fully dead now? ...'
> 'Do not forget QBOT is way old - sure, it's not working as good as in its glory days. Nevertheless, IOT is not dead. Always a question which botnet you use ;-)'
> 'Bruteforcing credentials isn't as good of a vector as it used to be; but, IoT definitely isn't dead because lots of new exploits come out daily for different types of devices.' (Quote 21)

## V. Discussion & Conclusions

In this study we presented an analysis of underground forum discussions related to Shodan and explored the cybercrime ecosystem around it. Shodan is actively used by hackers as a tool for passive information gathering providing easier access to hackable targets thus simplifying IoT hacking. Similar to previous findings [13] [14], our results also suggest that Shodan plays a prominent role in various specific use cases, such as scanning for and thus enabling remote control of target devices; building botnets; gaining personally identifiable information and launching DDoS attacks [3] [17]. However, our analysis revealed that Shodan is also often used for fun or trolling.

The majority of users agree that Shodan provides value and is a useful tool and do suggest its use. They mention Shodan both in the context of searching for targets and exploiting devices or services with known vulnerabilities, such as web cameras, smart home devices. In some cases Shodan is actually called 'The Search Engine for the IoTs'.

In all these use cases Shodan provides easier access to vulnerable targets. However, it is worth noting that from the perspective of hackers a significant factor determining the

utility of Shodan is if those targets can indeed be utilised. For example, if all scanned hosts in scan results are active and whether they can be used for exploitation. Thus the value of Shodan as a hacking tool is determined by its intended use cases.

Discussions around selling or buying Shodan accounts show that forum members trade these accounts and associated assets due to Shodan's credit model, which limits its use. To effectively utilise the output of Shodan queries, premium accounts are required.

Although Shodan and other search engines alike attract malicious actors, they are widely used by security professionals and for penetration testing [12] to unveil IoT security issues. Raising awareness of vulnerabilities provides invaluable help in alleviating these issues. Shodan provides a variety of services, including Malware Hunter, which is a specialised Shodan crawler aimed at discovering malware command-and-control (CC) servers [32]. The service is of great value to security professionals and in the fight against malware reducing its impact and ability to compromise targeted victims.

As described in this study, Shodan and similar engines can be used for both malicious and non-malicious purposes. This study stresses the risks emerging from IoT devices and highlights the need for actions towards securing the IoT ecosystem. The findings suggest that more focus needs to be placed upon the security considerations while developing IoT devices, as a measure to prevent their malicious use.

## REFERENCES


[1] J. S. Kumar and D. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, 02 2014.

[2] Hewlett-Packard, "Hp study reveals 70 percent of internet of things devices vulnerable to attack," 2014. [Online]. Available: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[4] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, pp. 180–187.

[5] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "Iotpot: A novel honeypot for revealing current iot threats," *Journal of Information Processing*, vol. 24, no. 3, pp. 522–533, 2016.

[6] B. Genge and C. Enăchescu, *ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services*. Security and Communication Networks, 2015.

[7] "Shodan," https://www.shodan.io/, accessed: 2020-03-13.

[8] M. Arnaert, Y. Bertrand, and K. Boudaoud, "Modeling vulnerable internet of things on shodan and censys : An ontology for cyber security," in *SECURWARE 2016*, 2016.

[9] B. Radvanovsky, "Project shine: 1,000,000 internet-connected scada and ics systems and counting," *Tofino Security*, vol. 19, 2013.

[10] M. Long, "I can show you the world: How shodan is used to exploit vulnerable scada systems."

[11] B. Herzberg, D. Bekerman, and I. Zeifman, "Breaking down mirai: An iot ddos botnet analysis," 2016. [Online]. Available: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html?utm_source=twitter&utm_medium=organic_emp&utm_campaign=2016_Q4_miraiddos

[12] E. Leverett, "Quantitatively assessing and visualising industrial system attack surfaces," *University of Cambridge Computer Laboratory, Darwin College, June 2011*, 2011. [Online]. Available: http://www.cl.cam.ac.uk/~fms27/papers/2011-Leverett-industrial.pdf

[13] J. Bugeja, D. Jönsson, and A. Jacobsson, "An investigation of vulnerabilities in smart connected cameras," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2018, pp. 537–542.

[14] N. Vlajic and D. Zhou, "Iot as a land of opportunity for ddos hackers," *Computer*, vol. 51, no. 7, pp. 26–34, 2018.

[15] K. Angrishi, "Turning internet of things(iot) into internet of vulnerabilities (iov) : Iot botnets," 2017.

[16] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the internet of things using deep learning approaches," in *2018 International Joint Conference on Neural Networks (IJCNN)*, 2018, pp. 1–8.

[17] T. Micro, "Uncovering iot threats in the cybercrime underground," 2019. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground

[18] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 2018, pp. 207–227.

[19] S. Samtani, R. Chinn, and H. Chen, "Exploring hacker assets in underground forums," in *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 2015, pp. 31–36.

[20] J. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative Sociology*.

[21] Y. Zhang and B. M. Wildemuth, "Qualitative analysis of content by," *Human Brain Mapping*, vol. 30, no. 7, pp. 2197–2206, 2005.

[22] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "Crimebb: Enabling cybercrime research on underground forums at scale," in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW '18. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2018, p. 1845–1854. [Online]. Available: https://doi.org/10.1145/3178876.3186178

[23] C. J. Howell and G. W. Burruss, *Datasets for Analysis of Cybercrime*. Cham: Springer International Publishing, 2020, pp. 207–219. [Online]. Available: https://doi.org/10.1007/978-3-319-78440-3_15

[24] F. Chen and Y. Luo, *Industrial IoT Technologies and Applications: Second EAI International Conference, Industrial IoT 2017, Wuhu, China, March 25–26, 2017, Proceedings*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer International Publishing, 2017. [Online]. Available: https://books.google.hu/books?id=tdIxDwAAQBAJ

[25] M. S. Pour, E. Bou-Harb, K. Varma, N. Neshenko, D. A. Pados, and K.-K. R. Choo, "Comprehending the iot cyber threat landscape: A data dimensionality reduction technique to infer and characterize internet-scale iot probing campaigns," *Digital Investigation*, vol. 28, pp. S40 – S49, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287619300246

[26] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 267–279.

[27] A. Subahi and G. Theodorakopoulos, "Detecting iot user behavior and sensitive information in encrypted iot-app traffic," *Sensors (Basel, Switzerland)*, vol. 19, 11 2019.

[28] J. Davis, "Telemedicine vendor breaches the data of 2.4 million patients in mexico," 2018. [Online]. Available: https://www.healthcareitnews.com/news/telemedicine-vendor-breaches-data-24-million-patients-mexico

[29] K. Angrishi, "Turning internet of things(iot) into internet of vulnerabilities (iov) : Iot botnets," 2017.

[30] S. S. Network, "New research exposes the vulnerabilities of smart home networks through security cameras and smart hubs," 2019. [Online]. Available: https://www.itsecuritynews.info/new-research-exposes-the-vulnerabilities-of-smart-home-networks-through-security-cameras-and-smart-hubs/

[31] V. Paxson, "An analysis of using reflectors for distributed denial-of-service attacks," *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 3, p. 38–47, Jul. 2001. [Online]. Available: https://doi.org/10.1145/505659.505664

[32] B. Computer, "New shodan tool can find malware command and control (cc) servers," 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-shodan-tool-can-find-malware-command-and-control-candc-servers/