Revealing Informed Scanners by Colocating Reactive and Passive Telescopes

Dario Ferrero
Delft University of Technology
Delft, The Netherlands
d.ferrero@tudelft.nl

Georgios Smaragdakis
Delft University of Technology
Delft, The Netherlands
g.smaragdakis@tudelft.nl

Harm Griffioen
Delft University of Technology
Delft, The Netherlands
h.j.griffioen@tudelft.nl

***Abstract*—Network telescopes have been utilized for decades to detect scanning activity on the Internet. Such telescopes are typically passive, i.e., they do not reply to TCP SYN packets. Recently, reactive network telescopes that respond to TCP SYN packets have been proposed to unveil a new wave of scanners, namely two-phase scanners, and collect malicious payloads from TCP ACK packets.**

In this paper, we propose a methodology that combines the modus operandi of passive and reactive telescopes to identify an additional wave of scanners – that we call "informed scanners"– that participate in attacks. Our main observation is that small reactive telescopes operating within larger passive telescopes are visited by "informed" clients that are aware of the liveness of hosts without performing scanning themselves; thus, are not visible in the passive telescope. We identify these informed clients as an additional class of highly targeted scanners and attackers. Indeed, by operating a /25 reactive telescope within a /16 passive telescope, we can filter out routine and two-phase scanning activity from informed one and identify clients that participate in service-targeted attacks. We discuss the scalability and sensitivity of our methodology and how it can be used to swiftly identify and profile malicious hosts on the Internet. We show that "mini-telescopes" of relatively smaller sizes, such as /20, can be comparably effective as larger sizes, such as a /16. Thus, our methodology can be useful to security operators that may only be able to allocate a relatively small address space to run a telescope.

***Index Terms*—Network Scanning, Network Scouting, Intrusion Detection, Network Telescope, Reactive Telescope**

I. Introduction

Scanning and scouting activity on the Internet is at an all-time high [1], [2], [3]. Commoditization of scanning tools such as ZMap [4] that are stateless has made it possible to scan the entire IPv4 address space and a large number of ports in minutes. Malware-based cyberattacks, e.g., Denial of Service (DoS) [5], [6], and ransomware [7], utilize scanning, i.e., checking for active ports, and scouting, i.e., try credentials for unauthorized access, to create harm and gain profit.

To derive threat intelligence about attackers' tactics, techniques, and procedures (TTPs), telescopes and honeypots have been used for decades monitoring this activity. Telescopes [8], [9], i.e., routed unused address space, have been used for decades to observe Internet scanning, e.g., botnet identification [10], DDoS campaigns [11], [5], [6], and exploitation of vulnerabilities [12]. However, passive telescopes may have a myopic view as they do not reply to requests by scanners and rarely collect payloads. Honeypots that mimic the behavior of real systems to capture scanning, scouting, and unauthorized activities [13], [14] can provide insights on the strategies deployed by attackers. Honeypots, especially the high interactive ones, can engage with the attackers and thus collect richer attack payloads. However, scaling honeypots to collect information on all ports is challenging as it requires implementing protocols of many services to cater to the requests of adversaries.

To collect data on all ports and identify the protocols requested by adversaries, we can use reactive telescopes, such as Spoki [15] and DScope [16], which have been recently proposed to respond in real-time to TCP SYN packets received by telescopes. Reactive telescopes provoke a follow-up from the adversaries by posing as an open port where a potentially interesting service is running. This is an advantage compared to passive telescopes that only capture the first TCP SYN packet and honeypots that do not collect data on all ports. Using this methodology, recent work has reported on "two-phase" scanning which is commonly performed by botnets such as Mirai [10], [15].

In this paper, we reveal a new class of scanners by combining a reactive telescope and passive telescope in the same network range. This class of scanners consists of separated infrastructures which (1) perform the initial scan and (2) connect to one of our measurement endpoints. This scanning methodology leads to part of the adversarial infrastructure going unnoticed by traditional methods such as a passive network telescope. Our measurement technique utilizes the passive telescope to monitor the routine scanning activity, whereas the reactive telescope, colocated with the passive one, identifies both scanners and follow-up connectors. By combining these two views, we can identify scanners that *only* visit the reactive telescope (i.e., are not visible in the colocated passive telescope) and thus have been informed about the liveness of address space that is utilized to operate the reactive telescope.

The contributions of this paper can be summarized as follows:

- We propose a novel methodology and use it to show that there is a set of devices which is "informed" about the liveness of a host. We validate our methodology through a 2.5-month longitudinal study by utilizing a *reactive* telescope consisting of a /25 network range deployed within a large *passive* telescope that utilizes a /16 address space. Additionally, we deploy the same network a year later to validate our findings.

- We provide insights on the sensitivity of our approach and the feasibility of deploying it across the Internet. We show that smaller telescopes can also be effectively used to identify the "informed" hosts.
- We analyze scanning patterns of a small set of campaigns that keep their reporting and infecting infrastructures strictly separated.
- We curate and share a dataset collected by our reactive measurement infrastructure.

The rest of this paper is structured as follows: First we place this work into the existing body of knowledge in Section II. Second, in Section III we discuss the datasets that made this work possible, the infrastructure used to collect the data, and the vantage point. In Section IV we propose and validate a new methodology to detect a class of Internet scanners which was not known to this day. We use this methodology in Section VI to identify what these scanners are used for and how they behave throughout our experiments. We discuss this work and future directions in Section X, and end with a conclusion in Section XI.

II. Related work

A. Internet Scanners

Network scanning has been for years the de-facto technique to discover active hosts and potentially uncover vulnerable services over an IPv4 address space [1], [2]. Several tools have been developed for the task [17], [18], but only in the last decade the focus has been shifted to scanning the entire internet, first with the introduction of MASSCAN [19], followed by the popularization of ZMap [4]. The efficient scanning routine introduced by the latter has had strong influence, leading to the appearance of Internet Scanning services and institutions [20], [21], as well as the adoption of its primitives into the host discovery routines of botnets [10], [22], [23]. More recent works have focused on extending its application from host discovery to service identification [24], [25]. Internet-wide scanning has become ubiquitous, both for legitimate measurements [26] and malicious objectives [27]. This increase in scan coverage and fingerprinting capabilities requires further advances in monitoring infrastructures, bringing efficient detection over both dimensions of address space size and depth of the monitored interactions.

B. Internet Telescopes

Monitoring large portions of the internet for unsolicited traffic has been a successful way to observe, measure and react to events originating from internet scanners. In the last two decades we've seen the instrumentation of unutilized IPv4 address blocks (*darknets*), for the collection and analysis of traffic via *network telescopes* [8], [9], the largest ones spanning over /8 IPv4 blocks. The applications of telescopes are not limited to security [11], [28], [29], [5], but a broader set of internet-wide measurements [30], [31]. As expected, their presence has been increasingly known over time by more sophisticated scanners. Recent work has therefore focused on exploring telescope deployments across less researched areas, such as residential networks [32] and cloud computing [33]. In terms of alternative implementations, Wagner et al. [34] proposed a methodology to infer darknet prefixes from unoperated ASes, while still being able to collect and analyze Internet Background Radiation (IBR).

C. Reactive Telescopes

Another known limitation of telescopes is their passive nature, preventing them from collecting connections that would occurr following a successful scan. Providing monitoring coverage of a large number of endpoints, and at the same time simulating more or less interactive services, is still an open problem in terms of efficiency and efficacy of deception techniques. On the other hand, honeypots [35], [36] have allowed to better profile the tactics, techniques and procedures (TTPs) of attackers, but while their depth of interaction is valuable, they require significant resources in order to fully cover the address scope of telescopes.

Recent works have been focusing on introducing interactiveness to Telescopes, without sacrificing the aspect of scalability. Hiesgen et al. [15] developed Spoki, a scalable component enabling efficient Layer 4 responsiveness to TCP SYN packets by multiple addresses of a Telescope. The measurements they conducted demonstrated how a significant number of hosts, labeled as *"Two-Phase Scanners"*, attempt to establish a stateful TCP connection as a follow-up to a first stateless probe. Their approach not only solicits scanners to "return" with a second-phase, but as well to deliver Application-Layer data for service scanning and exploitation, all which would not be visible by a traditional passive telescope. Similarly, Pauley et al. [16] proposed DScope, a reactive telescope fully deployed on the Cloud. By making use of a major provider's pool of randomly assigned IPv4 addresses, this work brought a first large measurement study regarding scanning activity targeting cloud computing resources. Among many findings, DScope showed how cloud IP ranges are subject to higher and more variable levels of scanning if compared to traditional Darknets. More recently, Soro et al. [37] performed a measurement combining several deployments with increasing levels of interaction, ranging from baseline Darknets to Layer-4 and 7 responders. Within one of these address spaces the authors introduced *DPIPot*, a Honeypot providing real-time Application-layer responses based on the services detected through Deep Packet Inspection of the requests.

Each of these studies has improved the efficiency and measured the effects of techniques aimed at finding a middle ground between internet telescopes and honeypots. The contributions of our work aim at adopting these insights in order to explore more in depth the nature of the additional scanners which are attracted by reactive telescopes. To this end, we deploy our own version of a reactive telescope, and take advantage of this novel monitoring infrastructure

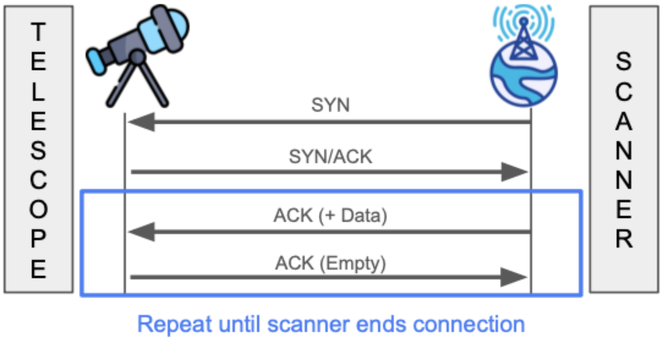


Fig. 1: Reactive telescope data collection. When a scanner sends a SYN packet (1), our system replies with a SYN/ACK (2). When the handshake is completed (3), we reply with an empty ACK (4) on every subsequent packet, allowing the scanners to send multiple payloads.

to analyze a previously unreported kind of internet scanners, while comparing their behavior to previously studied scanner categories.

III. Datasets

The analysis in this paper is made possible through the combination of two datasets, each capturing Internet background radiation (IBR). First, we use a large network telescope to identify all scanners that indiscriminately probe the Internet for TCP services. Second, we operate a *reactive telescope* similar to Spoki [15]. In this Section, we will describe both datasets in more detail.

A. Passive telescope

Table I shows a summary of the time ranges and overall counts for each deployed Telescope. The passive telescope address space used in this study consists of around 65 thousand IPv4 addresses spread over three Class B subnets located in an enterprise network. These addresses are unused and all traffic sent to them is stored. IBR sent to these IP addresses consists of Internet-wide scans, DDoS backscatter, and misconfigurations [8]. For this study we solely focus on TCP SYN scans [26] and filter the data collected by the telescope to only include these packets.

This dataset is mainly used to identify Internet-wide scanning behavior, which is a vital part of our methodology. While we have access to this data for the sake of this study, we show in this paper that such a large dataset of IP addresses is not strictly needed to perform this analysis.

B. Reactive telescope

At the core of this study is a reactive telescope that leverages similar techniques to Spoki [15] and DScope [16], in which we actively respond to scanning traffic sent by Internet-wide scanners and emulate a non-responsive layer 7 service. Figure 1 shows how our system responds to packets in a TCP session. When a session is established our system will keep sending empty ACK responses on client requests, indicating that the TCP session is still ongoing and allowing the client to attempt to elicit a response using different payloads. The system responds on all 65,536 ports.

We deploy this system on a /25 network consisting of 128 consecutive IP addresses located in the same network range as the *passive telescope*. We choose to colocate the telescopes to increase the likelihood that scanners targeting the reactive telescope will also hit the passive telescope, since scanners using a regional or block scan instead of an Internet-wide scan will be more likely to hit both ranges if they are in the same network block. The system was deployed on the 13th of March, 2024, and collected data until May 31st, 2024 for the first run. Over this time period, as shown in Table I, we collect ≈273 million connections, either only initiated or established, originating from ≈700 thousand source IPs. After stopping the active responses to TCP packets, we monitor the range for another month to identify transient effects on formerly active IP addresses.

We deploy the same setup a year later for the period of 1 month to validate our findings and to make sure that there are no temporary effects that would influence our results. Between the two runs of the experiment the reactive IP space was unused and the IP addresses did not respond to any traffic. The downtime of several months intends to reduce the likelihood that these IP addresses are still known to be "active".

The choice of running the measurement from a /25 network derives from our availability of IPv4 subnets allocated to our monitoring infrastructure. As we show in this paper, any size network could be used, as long as the passive counterpart is large enough. For the purposes of our methodology, this allows us to leverage even more the size difference between our passive and reactive infrastructure, as further described in Section IV-B.

IV. Methodology

Previous works [15], [37], [16] demonstrated how *reactive* telescopes can be used to extract information on "two-phase" scanners, identifying bot routines similar to Mirai [10], to a degree that was not possible with a *passive* telescope. In our methodology, we distinguish the sets of scanners that a *passive* telescope would not even see.

In the following, we describe how we define and separate regular Internet-wide scanning traffic and that originating from "informed" hosts, which as we show have prior knowledge of services running on a system.

A. Categories of Internet Scanners

Internet-wide scanning has been a popular method to enumerate hosts connected to the Internet for a long time. While in the past it took days to search through the entire Internet, stateless scanning tools such as ZMap [4] have made it possible within 5 minutes from a single host [38]. This speedup is achieved by scanning from a raw socket, instead of trying to open a TCP socket towards the target through the operating system, and sending as many crafted packets as fast as possible. The technique has been adopted by bots scanning

TABLE I: Summary of TCP Traffic collected from each deployed Network Telescope.

	Telescope Size	Start Time	End Time	Duration	# Sessions	# IPs
Passive Telescope	3x /16 (≈65,000 IPs)	Mar. '24	Apr. '25	13 months	181.82B	10.34M
Reactive Telescope	1x /25 (127 IPs)	Mar. '24	May '24	2.5 months	273.61M	706.77K
Reactive Telescope	1x /25 (127 IPs)	Mar. '25	Apr. '25	1 month	175.42M	254.42K

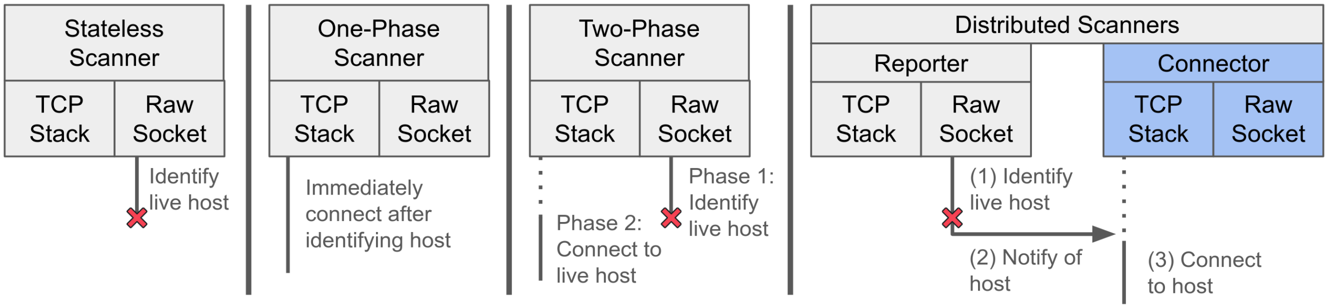


Fig. 2: Scanner categories based on recorded behavior. The first group consists of stateless scanners that identify a host but do not make an actual connection. The second group directly follows-up the initial SYN packet to establish a connection. The third group scans using a raw network socket and then connects through the operating system. Our contribution: The final group splits the scanning and connecting over two separate hosts.

the Internet to find vulnerable devices ever since its successful inclusion by the Mirai botnet [10]. Bots regularly scan the Internet using a raw socket and connect using an operating system socket when an open port has been identified. This behavior has been called "two-phase" scanning by Hiesgen et al. [15].

In this paper, we investigate another form of two-phase scanners, namely those that split their operation into two parts: first, a scanning host is used to identify a live system with an open port of interest, and second, a host receives information on open ports and connects to the target. The main motivation behind such a distributed infrastructure would be the reduced chances of detection and blocking; hosts responsible of scanning larger portions of the IPv4 space are more likely to be detected by organizations and having their IP addresses added to Threat Intelligence feeds. By separating their infrastructure, adversaries only show their second-stage hosts against potential targets, and not to the entire Internet. It is worth noting that the "second-phase" of these scanners would not be detected by passive monitoring ranges such as a network telescope.

Figure 2 shows a taxonomy of the four scanning methods that Internet-wide scanners can employ. ① is a fast, Internet-wide *Stateless Scanner* that runs on a tool such a ZMap. ② is a traditional scanner which relies on the operating system to open a port to a host on the Internet. When successful, this *One-Phase Scanner* immediately interacts with the system. ③ is a *Two-Phase Scanner* that combines the first two categories. It rapidly finds hosts by using a stateless scan, and when a host is found connects to it using a regular socket. ④ is a system that uses a scanner to detect hosts, and uses another host to actually perform a connection. This includes at least two hosts or endpoints: one for detection (a *"Reporter"*) and one for interaction (a *"Connector"*). In this paper, we aim to report on this last group of hosts that connect to a system without having scanned the Internet themselves.

When looking at the recorded interactions of individual hosts with our reactive telescope, we are able to assign behavioral labels indicating the above mentioned categories. Figure 3 shows a state diagram summarizing our process to apply labels on each session between a remote host and a (destination IP, destination port) target couple of our measurement infrastructure. We begin by considering only hosts directly initiating a TCP handshake by delivering a SYN-flagged packet, excluding other kinds of backscatter traffic [31]. A scanner that does not complete a handshake after our returned SYN-ACK is labeled as *Stateless*. On the contrary, hosts that directly send a valid TCP ACK are marked as *One-Phase*. This category does not yet give insight into the Distributed Scanners from Figure 2 since we are not attributing co-operation, but looking at the activity of individual sources. To label a scanner as *Two-Phase*, we follow the definition given in [15]: we label a session as such when a host contacts again the same target within an interval of ten minutes from a previous TCP SYN, this time following-up with an ACK. During this labeling process, we make sure to exclude re-transmissions, and to include sessions initiated with different TCP source ports. While we try to align our terminology with the previous work, our taxonomy and approach presents some differences. First, we decide not to adopt the proposed fingerprints for "Irregular SYNs" in the initial detection of Two-Phase Scanners, since we observed significantly lower shares of these in TCP SYNs, comprising less than 30% of all that are received by our reactive telescope. The volatility of these values can be explained by the fact that

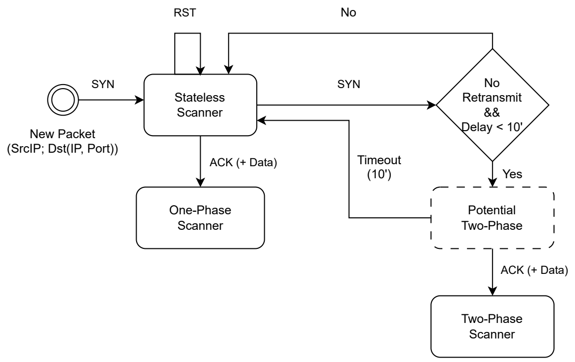


Fig. 3: State diagram of our labeling process. A source is flagged as a stateless scanner when a SYN is received. If the SYN is followed up by an ACK it transitions to a connector. If another SYN is received shortly after and the connection is set up, the source is labeled as a two-phase scanner.

they can easily change depending on custom configurations of or modifications to the scanning tools adopted. Second, while in [15] the term "One-Phase Scanners" is used in a broader sense, we separate them in our terminology from the hosts that do not complete handshakes, i.e. the "Stateless" ones.

B. Identifying Service-Aware IPs

To identify IPs that demonstrate awareness of specific services or infrastructure, we analyze the targeting behavior of hosts across our passive and reactive telescope datasets. In particular, we are interested in hosts that appear to deliberately restrict their probing activity to a narrow subset of the available address space—suggesting that they may be informed by prior reconnaissance or intelligence, rather than conducting blind or randomized scanning.

To isolate these IPs, we leverage the size difference between our passive and reactive telescope address spaces: for a duration of two and a half months, we observe that a subset of IPs consistently contacts only a contiguous /25 subnet within a broader /16 prefix. This means their activity is confined to just 0.2% of the available addresses in that range. Such behavior indicates a selective targeting pattern, which we interpret as a sign of service-aware scanning.

We identify *Connectors* through a straightforward set difference approach. Specifically, we begin with the full set of IPs observed by the reactive telescope throughout the experiment. From this set, we subtract any IP that, at any point, also made contact with the passive telescope segment. The remaining IPs are uniquely visible through the reactive telescope and have not engaged with the passive infrastructure.

We designate these as *"Informed Scanners"*, reflecting the assumption that their targeting behavior is guided by prior knowledge of host availability or service presence. Their absence from passive observations suggests they bypass indiscriminate scanning and instead operate with intent. This method effectively partitions the IPv4 addresses observed at the reactive telescope during the experiment into two distinct groups: *Informed* and *Non-Informed* scanners.

This methodology is restrictive, and its purpose is to detect a baseline of Informed Scanners. False Positives (FP) can occur when within the 2.5 months of measurements an IP only scans the reactive telescope without contacting the passive one, but has no prior knowledge of our endpoint's liveness. False Negatives (FN) on the other hand are cases in which a host is scanning the reactive telescope because informed, but is not labeled as such because the same IP also scans the passive range at least once, again over the entire experiment. These can happen for several reasons:

Measurement Gaps and Selective Scanning. While the size of our passive telescope is significant for an internet measurement study, it still only covers about 0.001% of the entire IPv4 address space. This can affect the count of FPs, since a host scanning only a random partition of the internet could potentially hit the reactive telescope without ever probing the passive address range. For example, ZMap allow this partitioning of the target list via "sharding" [38]. This type of FPs are not quantifiable since they are an inherent symptom of many internet measurement studies.

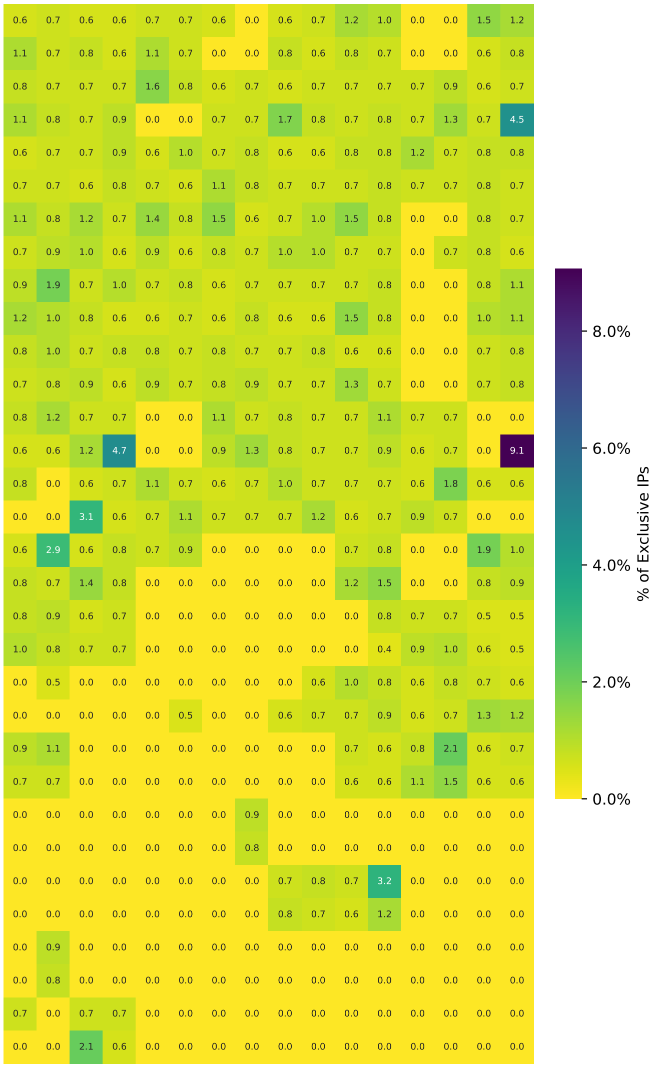
Address Space Churn. A more common error is due to the dynamic re-assignment of public IPv4 addresses to end hosts. It is likely that a host's public IP will change over time, either during a scan or in between different ones. FPs are affected in the scenario when a scanner hits the reactive telescope, is labeled as "Informed", and is assigned a new IP address before it continues its activity, potentially targeting the passive subnets. FNs on the other hand are caused by separate scans originating from the same IP but actually performed by different hosts. Similarly, this can happen because of re-infections by bots competing for the same vulnerable hosts [23]. Correlating scanner activity beyond IP addresses is a known open problem [39] and it requires some form of fingerprinting technique [40].

In a potential application scenario, classifying scanners as Informed would lead to them receiving further analysis, generating CTI, being blocked, etc. FPs will lead us to investigate more some Non-Informed scanners, which shouldn't lead to an excessive overhead. FNs are more critical, since we would not classify scanners that behave in a more sophisticated way and deserve more attention.

In the next Section, we show the results following the application of our methodology and introduce several validation steps to give an empirical baseline of False Positives in detecting Informed Scanners.

V. Methodology Validation

In order to assess the robustness and specificity of our identification methodology, we replicate the analysis across every other /25 subnet within our telescope infrastructure. These subnets, unlike the one linked to the reactive telescope, do not respond to incoming traffic. As such, they provide a useful control group: scanners that contact these silent ranges are presumed to behave like typical Internet-wide scanners,



0.6	0.7	0.6	0.6	0.7	0.7	0.6	0.0	0.6	0.7	1.2	1.0	0.0	0.0	1.5	1.2
1.1	0.7	0.8	0.6	1.1	0.7	0.0	0.0	0.8	0.6	0.8	0.7	0.0	0.0	0.6	0.8
0.8	0.7	0.7	0.7	1.6	0.8	0.6	0.7	0.6	0.7	0.7	0.7	0.7	0.9	0.6	0.7
1.1	0.8	0.7	0.9	0.0	0.0	0.7	0.7	1.7	0.8	0.7	0.8	0.7	1.3	0.7	4.5
0.6	0.7	0.7	0.9	0.6	1.0	0.7	0.8	0.6	0.6	0.8	0.8	1.2	0.7	0.8	0.8
0.7	0.7	0.6	0.8	0.7	0.6	1.1	0.8	0.7	0.7	0.7	0.8	0.7	0.7	0.8	0.7
1.1	0.8	1.2	0.7	1.4	0.8	1.5	0.6	0.7	1.0	1.5	0.8	0.0	0.0	0.8	0.7
0.7	0.9	1.0	0.6	0.9	0.6	0.8	0.7	1.0	1.0	0.7	0.7	0.0	0.7	0.8	0.6
0.9	1.9	0.7	1.0	0.7	0.8	0.6	0.7	0.7	0.7	0.7	0.8	0.0	0.0	0.8	1.1
1.2	1.0	0.8	0.6	0.6	0.7	0.6	0.8	0.6	0.6	1.5	0.8	0.0	0.0	1.0	1.1
0.8	1.0	0.7	0.8	0.8	0.7	0.8	0.7	0.7	0.8	0.6	0.6	0.0	0.0	0.7	0.8
0.7	0.8	0.9	0.6	0.9	0.7	0.8	0.9	0.7	0.7	1.3	0.7	0.0	0.0	0.7	0.8
0.8	1.2	0.7	0.7	0.0	0.0	1.1	0.7	0.8	0.7	0.7	1.1	0.7	0.7	0.0	0.0
0.6	0.6	1.2	4.7	0.0	0.0	0.9	1.3	0.8	0.7	0.7	0.9	0.6	0.7	0.0	9.1
0.8	0.0	0.6	0.7	1.1	0.7	0.6	0.7	1.0	0.7	0.7	0.7	0.6	1.8	0.6	0.6
0.0	0.0	3.1	0.6	0.7	1.1	0.7	0.7	0.7	1.2	0.6	0.7	0.9	0.7	0.0	0.0
0.6	2.9	0.6	0.8	0.7	0.9	0.0	0.0	0.0	0.0	0.7	0.8	0.0	0.0	1.9	1.0
0.8	0.7	1.4	0.8	0.0	0.0	0.0	0.0	0.0	0.0	1.2	1.5	0.0	0.0	0.8	0.9
0.8	0.9	0.6	0.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.8	0.7	0.7	0.5	0.5
1.0	0.8	0.7	0.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4	0.9	1.0	0.6	0.5
0.0	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.6	1.0	0.8	0.6	0.8	0.7	0.6
0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0	0.6	0.7	0.7	0.9	0.6	0.7	1.3	1.2
0.9	1.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.7	0.6	0.8	2.1	0.6	0.7
0.7	0.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.6	0.6	1.1	1.5	0.6	0.6
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.7	0.8	0.7	3.2	0.0	0.0	0.0	0.0
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.8	0.7	0.6	1.2	0.0	0.0	0.0	0.0
0.0	0.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.0	0.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.7	0.0	0.7	0.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.0	0.0	2.1	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Fig. 4: Hilbert diagram of the IPv4 /25 subnets (128 addresses each) in the main telescope /16, showing the percentage of Exclusive Scanners inferred for each of them. The reactive subnet (purple), is contacted by twice as many informed hosts than a regular "dark" netblock.

exhibiting broad and often randomized targeting behavior across multiple passive subnets without exclusive focus.

Under our classification scheme, such broadly scanning IPs should be excluded, as they are observed in multiple locations within the passive telescope space. Therefore, we expect our method to yield only a negligible number of *Informed Scanners* in these control subnets.

When applying our methodology to the reactive subnet, we initially record that almost *50%* of the IPs targeting it do not connect to the rest of the Telescope over the entire experiment. On inspection of this data we find that this significant share is due to unsolicited P2P scanning from a large number of clients. We filter this traffic out from our analysis while reporting on this event in Section V-A. We use the second experiment of the reactive telescope to validate our findings, and find that this does not contain this amount of P2P scanning traffic, and instead relates with the first experiment after filtering the P2P traffic. In the remainder of this validation and analyses we will therefore work without traffic belonging to these anomalies.

Figure 4 presents the proportion of IPs labeled as *Exclusive* across a subset of the /25 networks within the larger /16 subnet where the reactive telescope is deployed. We classify the scanners that exclusively hit the reactive telescope as *Informed*. This means that the higher the number in this heatmap, the more hosts we classify as *Informed*. As anticipated, the vast majority of these subnets exhibit minimal presence of *Exclusive* IPs. Two other subnets exhibit a larger share of *Exclusive* IPs, but these are still below the 5% noise floor we established in Section V-B. We discuss these further in the remainder of this section.

As detailed in Section III-A, our passive telescope spans three disjoint /16 address blocks. During the measurement period, many of the smaller subnets within these blocks were already in use by external services or had existing assignments. Consequently, we limit our validation to unassigned /25 segments that are known to be "dark" throughout the experiment, ensuring consistent conditions across the tested address space.

It stands out that the /25 containing the Reactive subnet is reached by an additional 4.4% more unique IPs than any other passive subnet (of which the largest receives 4.7% hosts exclusively targeting this subnet). Experimentally we verified that on average only a baseline of ≈1-2% sources targeting a netblock do not target any other subnet in the telescope, as shown in Figure 4. The share of unique hosts targeting the *reactive* netblock however is 9.1% of all sources, showing a large number of hosts that might not scan the Internet themselves, but do target a service once they know that a port is open. We use this validation as the foundation of our methodology.

The size of the resulting set can be seen in Table II. Out of the 706,765 unique IPs that contacted the /25 containing the Reactive Telescope, we remove approximately 46% that were associated with BitTorrent activity over few specific TCP ports in the "ephemeral" range: an expected source of noisy, peer-to-peer communication that can generate unsolicited traffic without clear scanning intent [31], [41]. After filtering, we are left with 380,410 IPs, from which 34,470 are labeled as *Informed Scanners* under our methodology.

Taken together, this supports the central assumption of our work: that the presence of hosts which exclusively interact with the reactive segment—despite the larger size and visibility of the passive ranges—is indicative of prior knowledge. In other words, these scanners likely received information about responsive systems from an external source, rather than discovering them independently through scanning.

A. BitTorrent Scans and Filtering

As mentioned in the validation step, the dataset obtained during the first run of our experiment contains a temporal stream of P2P messages.

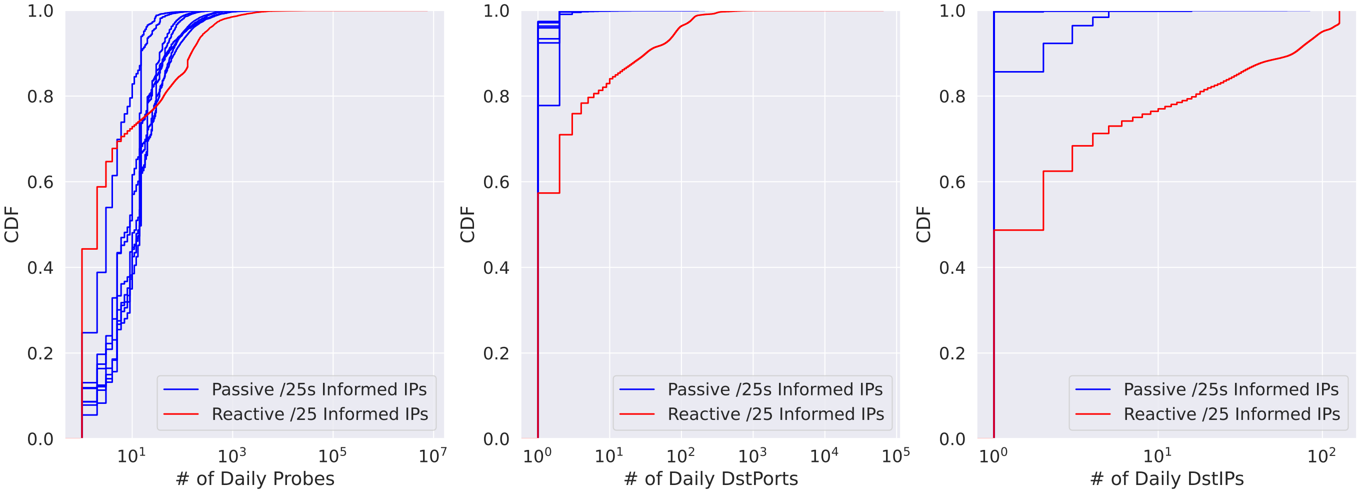


Fig. 5: CDFs of the daily activity per Informed Scanner IP, comparing those detected by the reactive /25 and the major passive /25 subnets

	IP Count
Passive Telescope (3x /16)	2,899,438
Passive Telescope (main /16)	2,533,697
Reactive Telescope (/25)	706,765
Excluding BitTorrent Targets	380,410
"Informed" Connector IPs	34,470

TABLE II: Filtered counts of observed IPs over the experiment's duration (March 13th - May 31st 2024)

When manually looking at the traffic trends we noticed that this behavior was influenced by a major surge of sources targeting a small set of ten ports over an even smaller number of five addresses of the reactive telescope. This anomalous event started on April 14th 2024 with ≈ 30,000 additional daily hosts contacting the reactive telescope, and continued with a slow decrease in daily total counts until the end of our measurement. Almost all traffic comprising this activity consisted of connections starting with a BitTorrent handshake and followed by keep-alive messages. Including traffic from this event would affect the results derived from our methodology, since IPs participating in these scans did not target the passive portion of our telescope during the experiment.

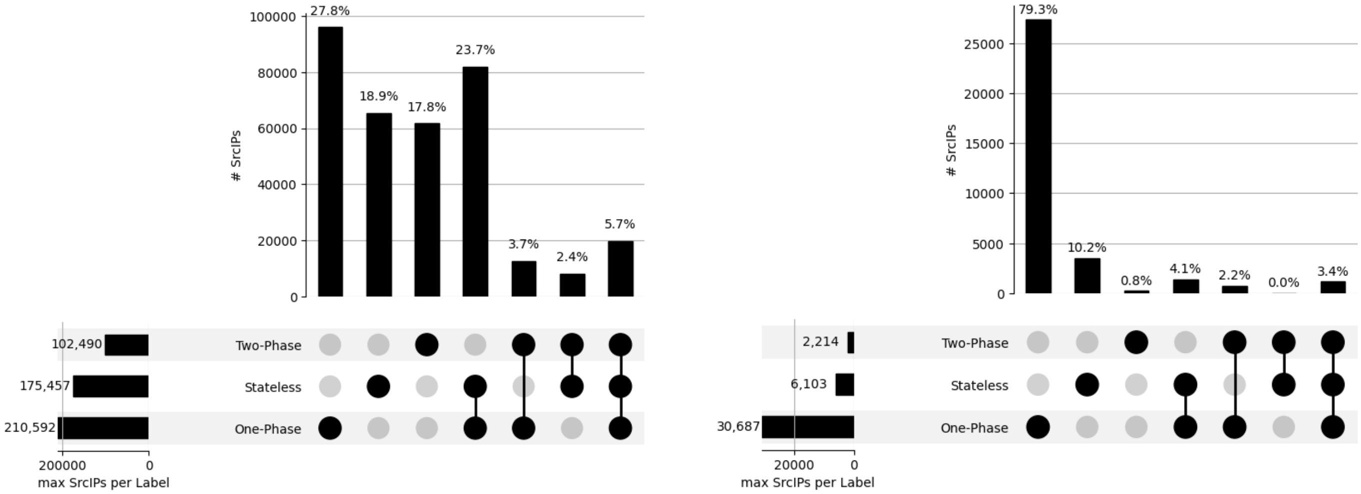
While we expected the counts of Sources to be influenced by P2P-based Internet Background Radiation [31], and these numbers to increase due to our reactiveness, we do not have a valid explanation to this amount of P2P clients contacting our telescope. One possible reason could be that turning this subnet responsive has lead some addresses being added to a list of BitTorrent peers maintained by a *tracker*. This however does not comply to the BitTorrent protocol [42], for which a properly configured peer would send a specific reply to a handshake message, while we simply acknowledge the incoming ACK packet.

Another option on this matter is that our address had been spoofed for a *Torrent Poisoning* attack [41]. In this case, adding to a peer list an IP which is not hosting any P2P-related service would allow the perpetuator to slow down communications for a given Torrent stream by having valid peers needing to search over a bigger list of non-existing peers before they can initiate transfers. This technique has been used in the past to combat P2P-based piracy. We manually grouped and searched the most popular *Info Hashes* fields from the BitTorrent handshake messages, seeing that most of them relate to (presumably) illegal transfer of recent movies, pirated versions of videogames, and other generic content, but we did not notice requests for Botnet or malicious material.

The number of Informed IPs we still have after filtering out BitTorrent peers is reported in Table II. While we cannot bring a sound explanation of this event, this case study is an illustrative example of how even the most simple and uninformative reply can elicit follow-ups from several different hosts, which might be of use for future studies involving the deployment of reactive telescopes. We determined that out of these hosts, almost all delivered exclusively BitTorrent messages and did so specifically towards those few affected TCP endpoints. On top of that, the amount of BitTorrent scans on known ports such as 6881 did not appear to be affected by this event, same as the overall scanning baseline collected by these addresses and ports. These outliers in our measurement can therefore be safely ignored when applying our set-difference methodology.

B. *Validating the Baseline of Exclusive Scanners*

In Section IV-B, we discussed how reactive telescopes attract a disproportionately high share of IPs that exclusively target the subnet, compared to regular passive segments. However, this observation is not without caveats: we also identify a non-negligible number of IPs that appear to *exclusively* contact other /25 networks in our measurement infrastructure, despite those networks being passive and non-responsive. This raises the question of whether such "exclusive" targeting might occur



(a) Non-Informed Scanners

(b) Informed Scanners

Fig. 6: UpSet plots comparing the overlaps in session labeling per each Informed partition

by chance, and whether some degree of exclusivity is simply inherent to background Internet scanning activity.

In this section, we investigate these high percentages observed in certain passive subnets to establish a baseline of expected "exclusive" activity. Understanding this noise floor is essential to differentiate between true service-aware behavior and statistical anomalies.

As shown in Figure 4, while the reactive subnet exhibits an exclusive source rate of approximately 9.1%, some passive subnets also exceed the baseline rate of ≈1%, reaching exclusivity levels in the range of 2–5%. Although highly-targeted and selective scanning has become more prevalent in recent years [16], [2], such behavior is not expected to significantly affect multiple passive subnets—especially those which do not respond to probes.

To further explore the nature of this activity, we compare the behavioral characteristics of IPs deemed exclusive to each subnet. Specifically, we analyze three dimensions: (1) the number of probes initiated daily, (2) the number of unique destination TCP ports contacted per day, and (3) the number of IP addresses in the subnet contacted per day.

Figure 5 displays cumulative distribution functions (CDFs) for these three metrics. The red line corresponds to hosts that exclusively contact the reactive subnet, while blue lines represent scanners observed in the most "exclusive" passive subnets.

In the left plot, we observe a small divergence in daily scanning activity. Hosts exclusive to the reactive telescope exhibit consistently higher probe rates, with roughly 20% of them initiating 100 or more sessions per day—10 percentage points above the most active passive subnet. The lower 80% of hosts exclusive to the reactive subnet are however not clearly distinguishable from the "noise" in the passive subnets.

The middle plot, which shows the number of unique destination ports contacted daily, shows a clearer behavioral distinction. Nearly 99% of scanners exclusive to passive subnets probe only three or fewer ports per day, aligning with common host-liveness scans focused on a minimal set of ports [26]. In contrast, exclusive scanners on the reactive subnet demonstrate a broader probing behavior, which is more consistent with targeted or service-aware interaction. When using a "noise-floor" of 5%, where we assume that 5% of the hosts in a given subnet can be "exclusive" by chance, roughly 45% of the exclusive hosts in the reactive subnet (in which we measure 9.1% of exclusive hosts) should be indeed *informed*. We do observe a measureable difference between this part of the exclusive hosts in the reactive subnet as opposed to the passive subnets.

We observe the same distribution in the daily IP addresses probed by hosts, where the majority of exclusive hosts in the reactive subnet is vastly different than the ones of the passive subnets. More than 50% of the exclusive hosts target more than one IP address per day, whereas in the passive subnets only a few exclusive hosts target more than one IP address. This could explain the level of "noise", as slow-scanning sources that only target few hosts will not show up in the rest of the passive telescope [43].

Taken together, these distributions support the hypothesis that the majority of "exclusive" IPs seen in passive subnets do not exhibit service-aware behavior, and are more likely the result of statistical noise or chance targeting. Their activity profiles remain consistent with typical Internet-wide scanners, who may simply miss the rest of our measurement space by coincidence.

C. Analyzing Label Overlaps

The final step in our validation is to validate our hypothesis that *informed* connectors behave like "one-phase" scanners, e.g. they will immediately connect to an IP address after sending an initial SYN packet. We classify all IP addresses

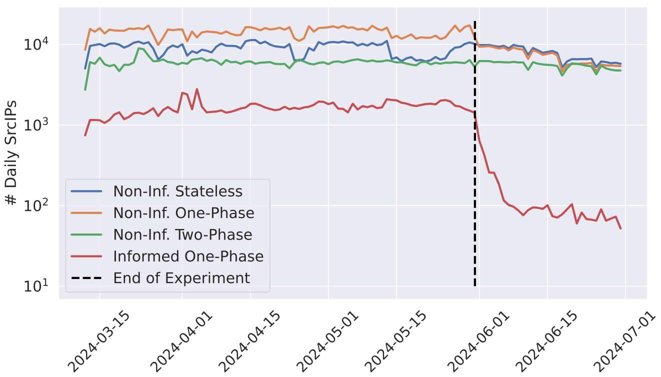


Fig. 7: Daily # of Source IPs per scanner label targeting the reactive /25 during the experiment and the following month

we observe during the exeriment into one of the categories listed in Figure 2 using the method shown in Figure 3. Our classification runs from the start of the experiment until the end. This means that in practice we observe hosts that change their behaviour throughout the experiment due to temporal effects such as IP churn or devices being infected by several different malwares during the 2.5 months [40]. We classify these hosts as belonging to a tuple of categories and report on them as such.

Figure 6 shows the result of classifying scanners into their respective categories using an UpSet plot. The set of scanners we classify as *informed*, as they are exclusively targeting the reactive telescope, indeed consists mainly of one-phase hosts connecting directly to an IP address. In the following section, we will focus on these informed hosts, as for the other classifications the results fall below a conservative noise floor of 5% and are therefore classified as false-positives.

VI. Results

Having defined and isolated the set of *Informed Scanners*, we now compare their behavior to that of broader Internet-wide scanners. This analysis provides insight into how awareness of an open service port influences probing strategies.

We focus on two key dimensions while analyzing the differences between informed scanners and the other scanner types:

1) **Informed scanner behavior:** The effect that reactive networks have on certain scanning types.
2) **Traffic Categorization:** Range of destination ports and protocols probed and interacted with.

A. Scanner Behavior

When activating a reactive telescope, it is well-documented that additional sources are drawn to the network [15], [37], and we are the first to go beyond showing the increase but instead identify and classify the additional sources in the network. Figure 7 presents the time series of unique IP addresses per scanner category throughout the duration of our experiment and into the month that followed.

Across all categories, we observe a relatively stable baseline of daily sources throughout the 2.5-month measurement period, suggesting that the total number of scanning IPs is not dramatically impacted by the introduction of a single reactive subnet. When looking at the mapping of hosts after the experiment concludes, we observe a large decrease in activity of the informed hosts immediately after the reactive responses cease. This persistence supports the hypothesis that these sources represent a dedicated secondary scanning infrastructure that reacts to live endpoints, rather than engaging in indiscriminate scanning.

Approximately six days after the end of the experiment, the daily number of informed connectors stabilizes at around 100 unique IPs, which is a tenfold decrease compared to their peak. This residual level is consistent with the false-positive rates inferred from our baseline analysis in Figure 4. This finding indicates that there is is a week-long “memory” of scanners that have identified a host similar as the “memory” of DDoS amplification servers [44].

The immediate decline of *informed* hosts indicates that there is a short feedback-loop between *reporters* and *connectors*, where after being informed, the connector shows up within hours. Using this insight, we are able to identify some tuples of reporters and connectors in Section VII.

B. Traffic Categorization

Figure 5 illustrates the divergence in daily activity between informed and non-informed sources. Informed scanners tend to establish more connections per day, suggesting a more deliberate and persistent engagement pattern. Moreover, informed sources probe a wider range of ports on average, although a significant portion still targets a relatively small set of service-specific ports—likely reflecting prior knowledge of a particular application or protocol running on the open host.

In this section, we analyze the application-layer traffic observed during our experiment, focusing on the most commonly requested protocols and services. Table III presents a comprehensive breakdown of payload types across three scanner categories: Informed One-Phase, Non-Informed One-Phase, and Non-Informed Two-Phase.

These payloads span a wide range of protocols—from generic handshake attempts to targeted probes aimed at specific services. For example, HTTP GET requests, while labeled under a single protocol, may target diverse services based on request paths. Similarly, HELP commands typically probe FTP, Telnet, or SMTP, with low diversity in payload content. In contrast, TLS Client Hello and Apache Cassandra CQL scans often contain randomized elements that result in a high count of unique payloads. We classify these payloads by applying pattern matching to the application-layer data. The full annotated dataset is available on request.

1) General scanning patterns: The results in Table III show that while some behaviors are vastly different between scanner types, in the broad lines the scanners target the same protocols. We identify the main differences in scanning exhibited by the different groups.

Payload Type	Informed One-Phase				Non-Inf. One-Phase				Non-Inf. Two-Phase			
	# Pays	# Uniq Pays	# Src IPs	# Ports	# Pays	# Uniq Pays	# Src IPs	# Ports	# Pays	# Uniq Pays	# Src IPs	# Ports
HTTP GET	**2.73M (7.8%)**	435K	9.1K	7.8K	**14.88M (20.4%)**	3.88M	92.1K	65.5K	**7.88M (41.3%)**	857K	48.6K	10.7K
TLS	**2.56M (7.3%)**	1.91M	16.2K	5.7K	**14.38M (19.8%)**	12.7M	102.8K	65.5K	**5.43M (28.5%)**	4.35M	10.5K	9.1K
RDP	**16.57M (47.3%)**	471	1.81K	46.7K	3.80M (5.2%)	9.34K	4.53K	9.0K	111K (0.6%)	95.6K	1.95K	1.0K
SSH	**3.86M (11.0%)**	22	1.12K	411	**8.43M (11.6%)**	41.6K	7.95K	1.17K	**857K (4.5%)**	8.15K	8.75K	440
Cassandra DB	**3.27M (9.3%)**	3.27M	28	1	**6.61M (9.1%)**	6.61M	12	1	36.2K (0.2%)	36.2K	12	1
TPKT Header	1.56M (4.4%)	51	1.94K	4.9K	2.89M (4.0%)	178	8.79K	8.7K	61.7K (0.3%)	48	2.73K	1.0K
MSSQL	733K (2.1%)	5.42K	1.69K	6.3K	620K (0.9%)	7.77K	3.96K	3.7K	23.7K (0.1%)	1.38K	419	866
SMB	538K (1.5%)	11	1.04K	5.1K	731K (1.0%)	22	2.41K	3.7K	21.5K (0.1%)	11	1.2K	948
X11	405K (1.2%)	1	1.17K	2.9K	744K (1.0%)	2	4.21K	2.8K	42.8K (0.2%)	2	1.19K	945
HELP	313K (0.9%)	2	1.00K	517	600K (0.8%)	5	2.64K	1.59K	1.90K (0.0%)	4	158	112
SOCKS	96.6K (0.3%)	482	1.51K	21.1K	2.32M (3.2%)	427	5.07K	3.9K	190K (1.0%)	402	1.78K	1.5K
HTTP CONNECT	38.2K (0.1%)	27	113	21.4K	**10.10M (13.9%)**	107	1.53K	65.5K	**1.42M (7.4%)**	55	302	4.3K
SOCKS5	27.9K (0.1%)	1	99	21.4K	1.72M (2.4%)	1	892	2.9K	159K (0.8%)	1	459	1.1K
CNXN	12.2K (0.0%)	4	234	12	216K (0.3%)	618	5.82K	379	215K (1.1%)	81	726	12
MicroTik	946 (0.0%)	2	722	2	9.15K (0.0%)	431	82	2	183K (1.0%)	26	52	1
OPENX	-	-	-	-	10.0K (0.0%)	193	133	5	211K (1.1%)	314	281	8
RIPE Atlas	-	-	-	-	898 (0.0%)	883	67	63	**1.85M (9.7%)**	33.0K	874	260

TABLE III: Summary of Application Layer Traffic by Payload Type across each Scanner Label.

The Informed One-Phase group is highly concentrated: nearly half of its payloads (47.3%) are RDP scans presenting a “mstshash” Cookie, spread across a large number of destination ports (46.7K). This is in stark contrast to the Non-Informed groups, where RDP probes are rare (5.2% and 0.6%), and suggests that Informed One-Phase scanners selectively target RDP services identified in earlier stages.

Conversely, HTTP CONNECT traffic is almost absent from Informed One-Phase (0.1%), yet constitutes a substantial share of Non-Informed One-Phase (13.9%) and Two-Phase (7.4%) traffic. This suggests that CONNECT scans are associated with broad reconnaissance rather than targeted follow-ups. For SOCKS and SOCKS5 however, which are also payloads to identify proxy servers, we find that the informed group spreads their scans over a much larger range of ports to identify whether this protocol is running on a device.

2) HTTP Requests: Table IV summarizes the most frequent HTTP GET request paths issued by each scanner group. While all groups perform HTTP-based reconnaissance, the specific paths they target reveal significant behavioral differences. The bulk of HTTP GET requests are aimed at the root of the webpage for all groups. However, the subsequent requests show a large difference in targeting between the different groups.

The *Informed One-Phase* scanners focus on infrastructure and management endpoints. Their top paths include `/config` and various Apache Solr admin panels, along with embedded system login pages like `/cgi-bin/authLogin.cgi`.

In contrast, *Non-Informed One-Phase* scanners exhibit broad reconnaissance behavior, frequently accessing generic paths such as `/login.cgi`, and various version and server information pages such as `/version` and `/server-info`. These scanners appear to sweep widely for exposed web interfaces, with no apparent targeting.

The *Non-Informed Two-Phase* group displays more aggressive probing toward known exploitation vectors, including request paths such as `/cgi-bin/luci/;stok=...`, `/shell?...` (both indicative of command injections, omitted for brevity), and various paths associated with Tomcat, Kubernetes, or misconfigured CI/CD environments. These patterns suggest a focus on identifying vulnerabilities or footholds for automated exploitation.

While non-informed scanners cast a wider net overall, informed scanners are more deliberate and aim to find specific protocols on many different ports.

VII. Linking Reporters and Connectors

To correlate the infrastructures used in scanning campaigns, we aim to identify links between scanners that initially probe the network (*reporters*) and those that subsequently establish full connections to our reactive telescope (*connectors*). This is complicated because of the noisy nature of Internet-wide scanning, where many unrelated sources operate simultaneously. As such, we use a method that prioritizes precision in identifying meaningful links, but is only able to find a very strict lower bound.

To this end, we analyze all occurrences of connector activity and examine the 1-hour window preceding each connection. Within this window, we collect for each connector activity the set of reporter IPs that scanned the same target (IP, port). By intersecting these reporter sets over time, we isolate IPs that consistently scan the same target endpoint before that connector. As mentioned above, this approach can be affected by other scanning noise towards the same endpoint, especially if the destination port is a popular one. In particular, we report that the top 1% TCP ports receive more than 50% of scanning traffic. To counter this, we focus on the 99% less popular ports.

The choice of the time window has been made empirically by comparing the effect of different window sizes on the resulting sets. Starting from the scans of connector IPs, we consider those that have at least one reporter scanning the same target within the previous time intervals, looking back at most up to 1 day. After intersecting the sets of reporter IPs across all scans from the same connector, we focus on non-empty sets, which are the reporters constantly preceding a connector. This set might still be biased by individual observations, so we filter those out by looking at cases where connectors target more than five TCP endpoints over the course of the experiment. From this analysis, we identify that when a connector shows up within a day after a reporter, it is likely within the first five minutes. We therefore only consider the first hour after a reporter has been seen to make computation tractable.

We consider links only when the intersection yields a single reporter IP *and* the connector has been seen at least

Informed One-Phase	Path	Non-Inf. One-Phase	Path	Non-Inf. Two-Phase	Path
1,604,892	/	12,612,788	/	6,886,373	/
116,445	/config	316,387	“Nmap scanner”	110,358	/v1.16/version
111,932	“Nmap scanner”	290,985	/login.cgi	98,419	/login.cgi
94,641	/wsman	97,218	/version	37,505	/cgi-bin/luci/;stok=...
40,932	/solr/admin/cores?action=STATUS&wt=json	57,776	/wsman	23,295	/aaa9
38,069	/v2/_catalog	47,049	SERVER	22,265	/version
37,059	/solr/admin/info/system	45,758	/hazelcast/rest/cluster	21,209	/.env
36,027	/query?q=SHOW+DIAGNOSTICS	45,728	/v1.16/version	11,433	/stacks
31,356	/cgi-bin/authLogin.cgi	44,495	/?CAVIT	10,638	/shell?...
9,642	/version	44,239	/api	9,883	/manager/html
7,467	/jmx?qry=Hadoop:service=NameNode,name=NameNodeInfo	43,930	/server-info	8,294	/manager/text/list

TABLE IV: Top request paths in HTTP GET requests.

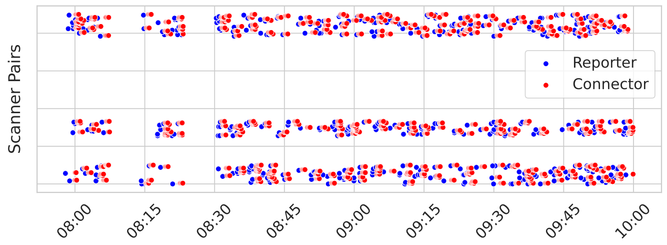


Fig. 8: Follow-ups between identified Distributed Scanners. Each row on the y-axis represents a different reporter-connector pair over time, and every dot refers to a connection.

five times, suggesting a persistent relationship between the reporter and connector. To further reduce the likelihood of coincidental co-occurrence, we validate these links by ensuring the reporter is never observed without a subsequent visit from its corresponding connector. This conservative approach helps eliminate spurious matches, but has some obvious limitations: (1) as we show before in this paper, connectors keep visiting our infrastructure way after shutting it down, indicating that the feedback loop between reporters and connectors is longer than the 1-hour window we use here. (2) The reporting infrastructure may be spread over multiple hosts, which this method does not account for.

Using this methodology, we identify 192 tuples of reporters and connectors where the reporter is exclusively active within an hour before the connector. For only 10% of tuples we identify, the reporter and connector are in the same /24 network range. When looking at the time between a reporter identifying an open port and a connector showing up we see that for most identified tuples this time is very short, with the bulk of the connectors contacting us within a minute after obtaining a report. We visualize these dynamics in Figure 8, which shows the behavior of reporters and their corresponding connectors for a sample observation window. The image shows that the top connectors immediately follow up with multiple probes after being informed of a live IP by a reporter.

In this paper, we show that these relations exist. To accurately map the reporting and connecting infrastructures together, future work could use a method such as used by [45] where IP addresses selectively respond to queries. This method will however also suffer from the limitation that it only considers pairs of reporter/connector, whereas in practice there may instead be a Many-to-Many mapping.

VIII. Operationalizing Colocated Telescopes

An important premise to our methodology is the difference in address space between the available Passive Telescope (≈65 thousand IPv4 addresses) and the amount of addresses we turn into Reactive (128). That is, ≈0.2% of our initial darknet becomes responsive during our experiment. While having such a wide IPv4 set available for passive monitoring is important for research purposes, purchasing and allocating such a wide address space might not always be feasible, both from an infrastructural as well as economic point of view. Because of this, we want to investigate how much the size of the surrounding Darknet (our *“Control Telescope”*), influences the resulting set of IPs we can classify as “Informed”.

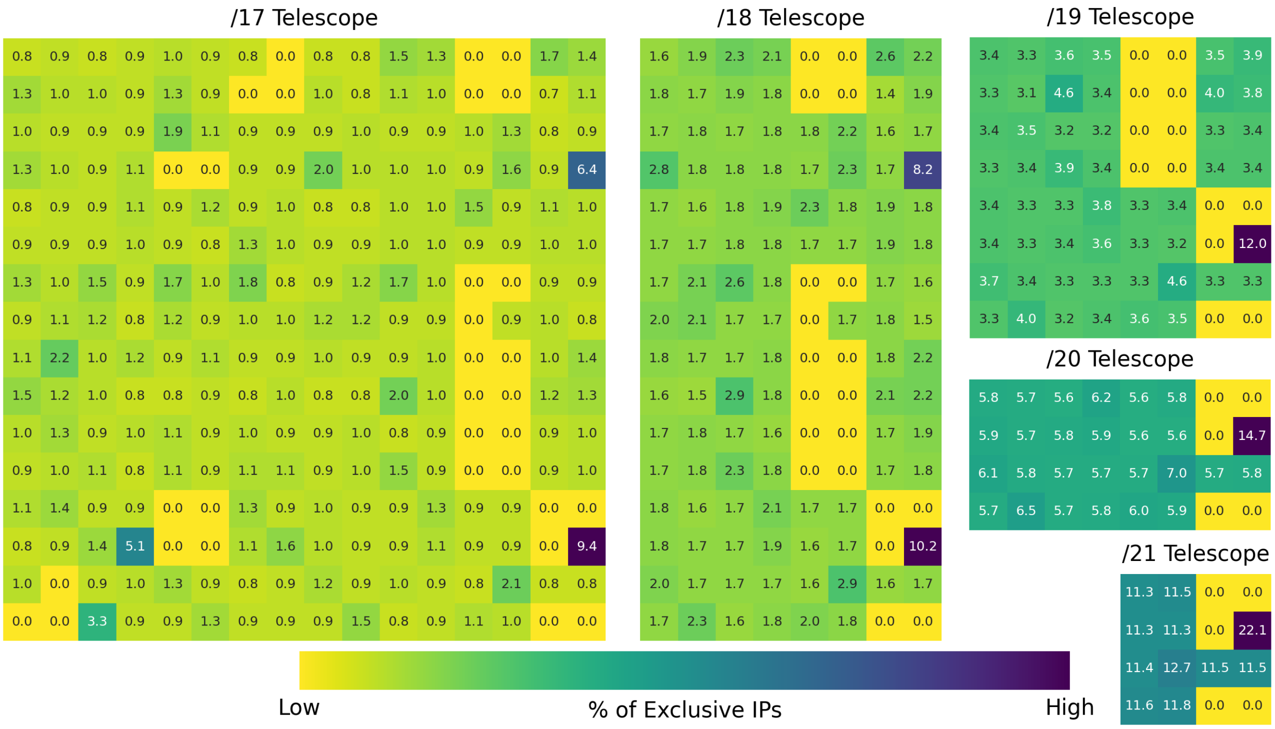
In this section we experimentally analyze how well this methodology will scale in settings where this infrastructure is not available, and instead smaller networks are used.

A. Sensitivity of the System

To understand how the size of the passive telescope impacts the visibility of informed scanners, we repeat our set-difference analysis while progressively reducing the subnet size of the telescope. As the telescope shrinks, the number of hosts observed exclusively in one subnet naturally increases, raising the noise floor and the likelihood of false positives.

Figure 9 presents the same set-difference view introduced in Section IV, now showing how the share of exclusive sources changes as we reduce the passive telescope from a /16 to a /17, and further down to a /21. In the reactive subnet, we observe that the proportion of exclusive sources nearly doubles when reducing to a /17. However, subsequent halving (to /18, /19, etc.) yields more modest growth, until a sharp increase at /21, suggesting that very small telescopes lead to a significant inflation of false-positive exclusive sources.

In contrast, the noise floor used for baseline comparisons exhibit a more consistent doubling of exclusivity at each halving step. This is expected: with smaller telescopes, we reduce the set of observable IPs contributing to the overlap, inflating the number of apparent exclusive sources. These results illustrate a trade-off between telescope size and the accuracy of the measurements: while smaller telescopes may still capture useful trends, their reduced visibility amplifies



/17 Telescope

0.8	0.9	0.8	0.9	1.0	0.9	0.8	0.0	0.8	0.8	1.5	1.3	0.0	0.0	1.7	1.4
1.3	1.0	1.0	0.9	1.3	0.9	0.0	0.0	1.0	0.8	1.1	1.0	0.0	0.0	0.7	1.1
1.0	0.9	0.9	0.9	1.9	1.1	0.9	0.9	0.9	1.0	0.9	0.9	1.0	1.3	0.8	0.9
1.3	1.0	0.9	1.1	0.0	0.0	0.9	0.9	2.0	1.0	1.0	1.0	0.9	1.6	0.9	6.4
0.8	0.9	0.9	1.1	0.9	1.2	0.9	1.0	0.8	0.8	1.0	1.0	1.5	0.9	1.1	1.0
0.9	0.9	0.9	1.0	0.9	0.8	1.3	1.0	0.9	0.9	1.0	1.0	0.9	0.9	1.0	1.0
1.3	1.0	1.5	0.9	1.7	1.0	1.8	0.8	0.9	1.2	1.7	1.0	0.0	0.0	0.9	0.9
0.9	1.1	1.2	0.8	1.2	0.9	1.0	1.0	1.2	1.2	0.9	0.9	0.0	0.9	1.0	0.8
1.1	2.2	1.0	1.2	0.9	1.1	0.9	0.9	1.0	0.9	0.9	1.0	0.0	0.0	1.0	1.4
1.5	1.2	1.0	0.8	0.8	0.9	0.8	1.0	0.8	0.8	2.0	1.0	0.0	0.0	1.2	1.3
1.0	1.3	0.9	1.0	1.1	0.9	1.0	0.9	0.9	1.0	0.8	0.9	0.0	0.0	0.9	1.0
0.9	1.0	1.1	0.8	1.1	0.9	1.1	1.1	0.9	1.0	1.5	0.9	0.0	0.0	0.9	1.0
1.1	1.4	0.9	0.9	0.0	0.0	1.3	0.9	1.0	0.9	0.9	1.3	0.9	0.9	0.0	0.0
0.8	0.9	1.4	5.1	0.0	0.0	1.1	1.6	1.0	0.9	0.9	1.1	0.9	0.9	0.0	9.4
1.0	0.0	0.9	1.0	1.3	0.9	0.8	0.9	1.2	0.9	1.0	0.9	0.8	2.1	0.8	0.8
0.0	0.0	3.3	0.9	0.9	1.3	0.9	0.9	0.9	1.5	0.8	0.9	1.1	1.0	0.0	0.0

/18 Telescope

1.6	1.9	2.3	2.1	0.0	0.0	2.6	2.2
1.8	1.7	1.9	1.8	0.0	0.0	1.4	1.9
1.7	1.8	1.7	1.8	1.8	2.2	1.6	1.7
2.8	1.8	1.8	1.8	1.7	2.3	1.7	8.2
1.7	1.6	1.8	1.9	2.3	1.8	1.9	1.8
1.7	1.7	1.8	1.8	1.7	1.7	1.9	1.8
1.7	2.1	2.6	1.8	0.0	0.0	1.7	1.6
2.0	2.1	1.7	1.7	0.0	1.7	1.8	1.5
1.8	1.7	1.7	1.8	0.0	0.0	1.8	2.2
1.6	1.5	2.9	1.8	0.0	0.0	2.1	2.2
1.7	1.8	1.7	1.6	0.0	0.0	1.7	1.9
1.7	1.8	2.3	1.8	0.0	0.0	1.7	1.8
1.8	1.6	1.7	2.1	1.7	1.7	0.0	0.0
1.8	1.7	1.7	1.9	1.6	1.7	0.0	10.2
2.0	1.7	1.7	1.7	1.6	2.9	1.6	1.7
1.7	2.3	1.6	1.8	2.0	1.8	0.0	0.0

/19 Telescope

3.4	3.3	3.6	3.5	0.0	0.0	3.5	3.9
3.3	3.1	4.6	3.4	0.0	0.0	4.0	3.8
3.4	3.5	3.2	3.2	0.0	0.0	3.3	3.4
3.3	3.4	3.9	3.4	0.0	0.0	3.4	3.4
3.4	3.3	3.3	3.8	3.3	3.4	0.0	0.0
3.4	3.3	3.4	3.6	3.3	3.2	0.0	12.0
3.7	3.4	3.3	3.3	3.3	4.6	3.3	3.3
3.3	4.0	3.2	3.4	3.6	3.5	0.0	0.0

/20 Telescope

5.8	5.7	5.6	6.2	5.6	5.8	0.0	0.0
5.9	5.7	5.8	5.9	5.6	5.6	0.0	14.7
6.1	5.8	5.7	5.7	5.7	7.0	5.7	5.8
5.7	6.5	5.7	5.8	6.0	5.9	0.0	0.0

/21 Telescope

11.3	11.5	0.0	0.0
11.3	11.3	0.0	22.1
11.4	12.7	11.5	11.5
11.6	11.8	0.0	0.0

Fig. 9: Percentages of Informed Scanners for progressively smaller Telescope sizes.

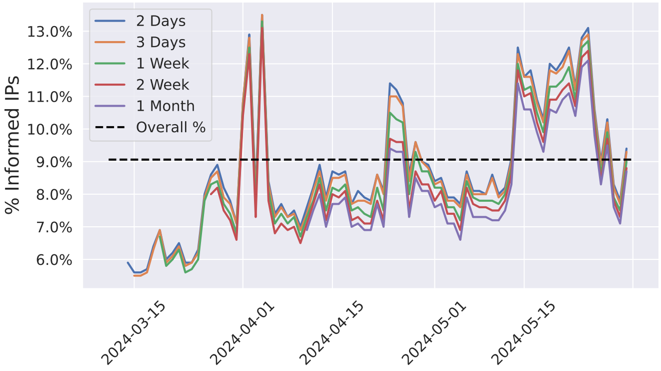


Fig. 10: Variation of Informed IP percentages when applying the set difference over rolling time windows of specified length

noise, and risks misclassifying scanner behavior. However, using even a relatively small passive network where only part is reactive would allow a network operator to isolate behavior that is strictly targeted. The insights gained in this system can aid in alert triage and in turn reduce alert fatigue for defenders.

B. Time Window

The previous section demonstrates that smaller networks can remain effective when combining passive and reactive telescopes. However, since the IP set differences were computed over a relatively long period of two and a half months, we also investigate how the choice of time window affects the identification of exclusive hosts.

While this study adopts a more conservative, long-term analysis, shorter time windows are essential in more realistic operational settings. Maintaining a global list of scanner IPs over months is not only inefficient but may also introduce false negatives due to the dynamic and often ephemeral nature of IPv4 address assignments [46]. In practice, telescope operators may benefit from dynamically isolating the set of Exclusive scanners within shorter windows—potentially linking them to earlier stateless probing activity.

Figure 10 presents the percentage of sources identified when applying the same methodology to rolling time windows with size of days, weeks, up until one month, while calculating the percentages over the last day in the window. Broadly, we observe that when using a shorter window to use for the set difference, this leads to more hosts being classified as "exclusive". This is expected as we are essentially limiting the dataset used to perform the set difference operation. However, the amount of variability between the different observation windows is small. This means that even with a short backlog, the error margin can be acceptable.

IX. Ethical Considerations

In this study, we deploy over a range of 128 IP addresses a service responding to incoming connections. Our infrastructure does not send any data without a request being made, but could be tricked into sending traffic to a secondary host when receiving a message with a spoofed source. In this case, our infrastructure would send a reply to the spoofed source instead, effectively reflecting (but not amplifying) a request. This is however no different from a regular service on the Internet, where an adversary can also send a spoofed connection packet for which the reply is sent to another host.

We intend to share the data collected in the reactive telescope during the experiments [1]. Because this contains exploit attempts, and to ensure the privacy of the networks and hosts that have interacted with our system, we will only share anonymized data publicly [47]. Our collected internet traffic, consisting of TCP SYN scans and elicited ACK packets along potential data payload, contains sensitive information mainly in two forms:

1) **IPv4 Addresses.** Disclosing source and destination IPs would affect the privacy respectively of potentially infected end-users and of our measurement infrastructure. To prevent this while guaranteeing the reproducibility of our study we plan on releasing only key-hashed values of the original addresses, so that the 1-to-1 mapping is preserved for further analysis based on Prefix-Preserving anonymization [48].
2) **Application-Layer Payloads.** Data carried by layer 7 probes might contain sensitive information from the end-users, especially in the case that these have been infected by malware that originates the scanning or exploitation. On the other hand, because both passive and reactive telescopes are part of a darknet, we have no visibility on legitimate end-user traffic from our vantage points. To reduce the risk of disclosure of personal information, we decide to release a sanitized version of the application-layer payloads collected, that is providing hash values of selected fields which might allow for fingerprinting, such as HTTP Host header, and references to loader IPv4 addresses contained within RCE attempts.

X. Discussion

Operational Reactive Telescopes. The efficient application of reactive telescopes has been investigated in previous works [15], [16], both in terms of allowing scalability and reducing costs. Our work focuses on exploring the monitoring capabilities introduced through the combination of traditional passive telescope deployments along the more recent reactive ones. We show how this allows for the categorization of new scanners, and we show the effects of reducing the surrounding darknet size on our result set. Limiting the address space of a passive internet telescope might reduce visibility into hosts scanning the whole Internet, but we argue that allocating a smaller part of it to be active can compensate by making the deployment more flexible by allowing distributed setups while significantly reducing costs linked to IPv4 address space.

Linking Distributed Scanners. Over this paper, we commonly refer to the set of IPs obtained through our methodology as "informed". As initially mentioned in Section IV-A, this is largely based on the assumption that if a host directly connects to a small, active address space within a larger, passive one, then it has likely been informed of its activeness by a previous, separate scan. We show for a small subset of these scanners how their interaction looks like, but state some limitations in what we are able to "link" together. An interesting future work on this point would be to make a telescope's responsiveness more selective using a methodology similar to the one introduced by [45] on linking DDoS attacks to scans. This could potentially allow linking initial scanning campaigns to follow-ups, shedding light on the open problem of linking distributed scanners' activity. As we saw from our collected data, informed hosts appear in short bursts, which would facilitate this linking process.

Limitations. We previously explained in Sections IV and VIII-A how our approach is sensitive to false positives or false negatives in detecting informed scanners. The total IPv4 address space available and the choice in the time window for detection can influence results, and exploring their combination can be an important addition to this work. Similarly, the current data collection methodology in reactive telescopes does not allow for the attribution of all reporters to the connectors they inform. There is room for future work to combine our methodology with other methods to allow for this attribution.

XI. Conclusion

In this paper, we reveal an additional class of scanners, the "informed" scanners that have been notified about the liveness of hosts and have not visited the address space before. This class can be identified when a reactive telescope is colocated with a passive telescopes. Informed scanners can not be identified as "two-phase" scanners as they do not have a second-phase scanning behavior. By leveraging the passive telescope, we monitor the routine scanning and scouting activity. By leveraging the colocated reactive telescope, we identify the two-phase scanners. Thus, by combining the two views, we can identify scanners that *only* visit the reactive telescope (i.e., are not visible in the colocated passive telescope) and are *not* two-phase scanners, therefore having been informed about the liveness of address space that is utilized to operate the reactive telescope. We investigate the tactics and objectives of informed clients by looking at the Layer 7 payloads they sent. Our results show that this set of informed clients differs from previously studied two-phase clients. We also show that "mini-telescopes" of relatively smaller sizes, such as /20, can be equally effective as larger sizes, such as a /16. This way, our methodology can be useful to security operators that may only be able to allocate a relatively small address space.

As part of our future research agenda, we plan to operate distributed mini-telescopes to better study the profile, techniques and tactics of informed scanners. We also plan to offer a real-time service to report informed scanners monitored at different locations on the Internet.

Acknowledgement

This work was supported by the European Commission under the Horizon Europe Programme as part of the project SafeHorizon (Grant Agreement #101168562).

[1] Dataset available at: https://delftintellab.com/projects/raid2025-informed-scanners

References

[1] Z. Durumeric, D. Adrian, P. Stephens, E. Wustrow, and J. A. Halderman, “Ten Years of ZMap,” in *Proceedings of the 2024 ACM on Internet Measurement Conference*, ser. IMC ’24. New York, NY, USA: Association for Computing Machinery, 2024, p. 139–148. [Online]. Available: https://doi.org/10.1145/3646547.3689012

[2] H. Griffioen, G. Koursiounis, G. Smaragdakis, and C. Doerr, “Have you SYN me? Characterizing Ten Years of Internet Scanning,” in *ACM Internet Measurement Conference (IMC) 2024*, Madrid, Spain, November 2024.

[3] A. Anand, M. Kallitsis, J. Sippe, and A. Dainotti, “Aggressive Internet-wide Scanners: Network Impact and Longitudinal characterization,” in *Companion of the 19th International Conference on emerging Networking EXperiments and Technologies*, 2023, pp. 1–8.

[4] Z. Durumeric, E. Wustrow, and J. A. Halderman, “ZMap: Fast internet-wide scanning and its security applications,” in *22nd USENIX Security Symposium*, 2013.

[5] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, “Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks,” in *Proceedings of the 2014 Conference on Internet Measurement Conference*, ser. IMC ’14. New York, NY, USA: Association for Computing Machinery, 2014, p. 435–448. [Online]. Available: https://doi.org/10.1145/2663716.2663717

[6] R. Hiesgen, M. Nawrocki, M. Barcellos, D. Kopp, O. Hohlfeld, E. Chan, R. Dobbins, C. Doerr, C. Rossow, D. R. Thomas, M. Jonker, R. Mok, X. Luo, J. Kristoff, T. C. Schmidt, M. Wählisch, and kc claffy, “The age of DDoScovery: an empirical comparison of industry and academic DDoS assessments,” in *Proceedings of the 2024 ACM on Internet Measurement Conference*, 2024, pp. 259–279.

[7] K. Oosthoek, J. Cable, and G. Smaragdakis, “A Tale of Two Markets: Investigating the Ransomware Payments Economy,” *Communications of the ACM*, vol. 66, no. 8, pp. 74–83, 2023.

[8] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, “Network Telescopes: Technical Report,” Cooperative Association for Internet Data Analysis (CAIDA), Tech. Rep., 2004.

[9] M. D. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, “The Internet Motion Sensor - A Distributed Blackhole Monitoring System,” in *NDSS*, 2005.

[10] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, “Understanding the Mirai Botnet,” in *26th USENIX security symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[11] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, “Inferring Internet Denial-of-Service Activity,” *ACM Trans. Comput. Syst.*, vol. 24, no. 2, p. 115–139, May 2006. [Online]. Available: https://doi.org/10.1145/1132026.1132027

[12] E. Pauley, P. Barford, and P. McDaniel, “The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits against Two Years of Zero-Days,” in *Proceedings of the 2023 ACM on Internet Measurement Conference*, ser. IMC ’23. New York, NY, USA: Association for Computing Machinery, 2023, p. 236–252. [Online]. Available: https://doi.org/10.1145/3618257.3624810

[13] T. Barron and N. Nikiforakis, “Picky Attackers: Quantifying the Role of System Properties on Intruder Behavior,” in *Proceedings of the 33rd Annual Computer Security Applications Conference*, ser. ACSAC ’17. New York, NY, USA: Association for Computing Machinery, 2017, p. 387–398. [Online]. Available: https://doi.org/10.1145/3134600.3134614

[14] Y. Wu, P. M. Cao, A. Withers, Z. T. Kalbarczyk, and R. K. Iyer, “Mining Threat Intelligence from Billion-scale SSH Brute-Force Attacks,” in *NDSS*, 2020.

[15] R. Hiesgen, M. Nawrocki, A. King, A. Dainotti, T. C. Schmidt, and M. Wählisch, “Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope,” in *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 431–448. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/hiesgen

[16] E. Pauley, P. Barford, and P. McDaniel, “DScope: A Cloud-Native Internet Telescope,” in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 5989–6006. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/pauley

[17] J. C. Louis. (2024, Oct) Unicornscan. [Online]. Available: https://sourceforge.net/projects/osace/files/unicornscan/

[18] G. F. Lyon. (2009) Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure, USA.

[19] R. Graham. (2013) MASSCAN. [Online]. Available: https://github.com/robertdavidgraham/masscan

[20] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, “A Search Engine backed by Internet-wide Scanning,” in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 2015, pp. 542–553.

[21] (2024) Shodan: Search Engine for the Internet of Everything. [Online]. Available: https://www.shodan.io/

[22] S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, “Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet,” in *NDSS*, 2019.

[23] H. Griffioen and C. Doerr, “Examining Mirai’s Battle over the Internet of Things,” in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 743–756.

[24] T. Z. Project. ZGrab 2.0: Fast Go Application Scanner. [Online]. Available: https://github.com/zmap/zgrab2

[25] L. Izhikevich, R. Teixeira, and Z. Durumeric, “LZR: Identifying Unexpected Internet Services,” in *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 3111–3128. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich

[26] Z. Durumeric, M. Bailey, and J. A. Halderman, “An Internet-Wide view of Internet-Wide scanning,” in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 65–78.

[27] A. Wang, W. Chang, S. Chen, and A. Mohaisen, “Delving Into Internet DDoS Attacks by Botnets: Characterization and Analysis,” *IEEE/ACM Trans. Netw.*, vol. 26, no. 6, p. 2843–2855, Dec. 2018. [Online]. Available: https://doi.org/10.1109/TNET.2018.2874896

[28] V. Yegneswaran, P. R. Barford, and D. Plonka, “On the Design and Use of Internet Sinks for Network Abuse Monitoring,” in *International Symposium on Recent Advances in Intrusion Detection*, 2004. [Online]. Available: https://api.semanticscholar.org/CorpusID:10721387

[29] A. Dainotti, A. King, k. Claffy, F. Papale, and A. Pescapè, “Analysis of a “/0” Stealth Scan from a Botnet,” in *Proceedings of the 2012 Internet Measurement Conference*, ser. IMC ’12. New York, NY, USA: Association for Computing Machinery, 2012, p. 1–14. [Online]. Available: https://doi.org/10.1145/2398776.2398778

[30] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, “Internet Background Radiation Revisited,” in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC ’10. New York, NY, USA: Association for Computing Machinery, 2010, p. 62–74. [Online]. Available: https://doi.org/10.1145/1879141.1879149

[31] K. Benson, A. Dainotti, k. claffy, A. C. Snoeren, and M. Kallitsis, “Leveraging Internet Background Radiation for Opportunistic Network Analysis,” in *Proceedings of the 2015 Internet Measurement Conference*, ser. IMC ’15. New York, NY, USA: Association for Computing Machinery, 2015, p. 423–436. [Online]. Available: https://doi.org/10.1145/2815675.2815702

[32] P. Richter and A. Berger, “Scanning the Scanners: Sensing the Internet from a Massively Distributed Network Telescope,” in *Proceedings of the Internet Measurement Conference*, ser. IMC ’19. New York, NY, USA: Association for Computing Machinery, 2019, p. 144–157. [Online]. Available: https://doi.org/10.1145/3355369.3355595

[33] L. Izhikevich, M. Tran, M. Kallitsis, A. Fass, and Z. Durumeric, “Cloud Watching: Understanding Attacks Against Cloud-Hosted Services,” in *Proceedings of the 2023 ACM on Internet Measurement Conference*, ser. IMC ’23. New York, NY, USA: Association for Computing Machinery, 2023, p. 313–327. [Online]. Available: https://doi.org/10.1145/3618257.3624818

[34] D. Wagner, S. A. Ranadive, H. Griffioen, M. Kallitsis, A. Dainotti, G. Smaragdakis, and A. Feldmann, “How to Operate a Meta-Telescope in your Spare Time,” in *Proceedings of the 2023 ACM on Internet Measurement Conference*, ser. IMC ’23. New York, NY, USA: Association for Computing Machinery, 2023, p. 328–343. [Online]. Available: https://doi.org/10.1145/3618257.3624831

[35] N. Provos *et al.*, “A Virtual Honeypot Framework,” in *USENIX Security Symposium*, vol. 173, no. 2004, 2004, pp. 1–14.

[36] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, “A Survey on Honeypot Software and Data Analysis,” *arXiv preprint arXiv:1608.06249*, 2016.

[37] F. Soro, T. Favale, D. Giordano, I. Drago, T. Rescio, M. Mellia, Z. B. Houidi, and D. Rossi, “Enlightening the Darknets: Augmenting Darknet Visibility with Active Probes,” *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 5012–5025, 2023.

[38] D. Adrian, Z. Durumeric, G. Singh, and J. A. Halderman, “Zippier ZMap: Internet-Wide Scanning at 10 Gbps,” in *8th USENIX Workshop on Offensive Technologies (WOOT 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/woot14/workshop-program/presentation/adrian

[39] L. Böck, D. Levin, R. Padmanabhan, C. Doerr, and M. Mühlhäuser, “How to Count Bots in Longitudinal Datasets of IP Addresses,” in *Network and Distributed System Security (NDSS) Symposium*, 2023.

[40] H. Griffioen and C. Doerr, “Quantifying Autonomous System IP Churn using Attack Traffic of Botnets,” in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES ’20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3407023.3407051

[41] R. Cuevas, M. Kryczka, A. Cuevas, S. Kaune, C. Guerrero, and R. Rejaie, “Is Content Publishing in BitTorrent Altruistic or Profit-driven?” in *Proceedings of the 6th International COnference*, ser. Co-NEXT ’10. New York, NY, USA: Association for Computing Machinery, 2010. [Online]. Available: https://doi.org/10.1145/1921168.1921183

[42] B. Cohen. The BitTorrent Protocol Specification. [Online]. Available: https://www.bittorrent.org/beps/bep_0003.html

[43] H. Griffioen and C. Doerr, “Discovering Collaboration: Unveiling Slow, Distributed Scanners based on Common Header Field Patterns,” in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020, pp. 1–9.

[44] H. Griffioen, K. Oosthoek, P. van der Knaap, and C. Doerr, “Scan, Test, Execute: Adversarial Tactics in Amplification DDoS Attacks,” in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’21. New York, NY, USA: Association for Computing Machinery, 2021, p. 940–954. [Online]. Available: https://doi.org/10.1145/3460120.3484747

[45] J. Krupp, M. Backes, and C. Rossow, “Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’16. New York, NY, USA: Association for Computing Machinery, 2016, p. 1426–1437. [Online]. Available: https://doi.org/10.1145/2976749.2978293

[46] H. Griffioen and C. Doerr, “Quantifying autonomous system ip churn using attack traffic of botnets,” in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–10.

[47] E. Pauley and P. McDaniel, “Understanding the Ethical Frameworks of Internet Measurement Studies,” in *The 2nd International Workshop on Ethics in Computer Security (EthiCS 2023)*, San Diego, CA, Feb. 2023.

[48] J. Xu, J. Fan, M. Ammar, and S. B. Moon, “On the Design and Performance of Prefix-Preserving IP Traffic Trace Anonymization,” in *Proceedings of the First ACM SIGCOMM Internet Measurement Workshop*, vol. 31. ACM Press, 2001, p. 263.