Overview of Network Telescopes

Niklas Feurstein, Tim Betzer*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: niklas.feurstein@tum.de, betzer@net.in.tum.de

***Abstract*—Network telescopes, also known as darknets, are tools that aid in identifying and characterizing events that happen on the Internet. Without a clear-cut classification of the different network telescopes, it is difficult to keep track of them. Therefore, we present an overview of the different telescopes. In this paper, we classify those tools into two main groups. In addition to highlighting the main differences between passive and reactive network telescopes, we list the largest active telescopes and describe their properties.**

***Index Terms*—Network telescopes, Darknets, UCSD, Orion, NICTER**

1. Introduction

Internet security is becoming more and more important. Every day, thousands of machines are infected with malware. Malicious actors continuously try to discover unpatched vulnerabilities in online hosts. This not only puts companies and governments at risk of cybersecurity incidents but also endangers ordinary citizens. One thing is certain: The damages victims of hacking attacks suffer are not to be underestimated.

1.1. Tools for Security

To achieve their goals, hackers rely on a variety of programs and strategies. One of the first steps for cyber criminals is identifying a suitable victim. Instead of doing this manually, many hackers make use of automated programs called scanners. After a potential victim has been found, its computer can be attacked. [1]

In order to adequately defend against cybercrime, attacks should be detected as early as possible. Therefore, it is crucial that security researchers stay on top of the latest developments in the cybersecurity sphere.

To identify ongoing attacks, researchers and analysts need lots of data. Network telescopes provide this data by monitoring a part of the unused IP address space [2]. Packages sent to those regions are frequently related to malicious activities [3].

By leveraging this data, the latest exploits can be discovered and mitigated. Depending on their goals and objectives, researchers and companies make use of network telescopes. To make better use of those tools, organizations like IBM developed their own darknet. This allows them to have a tailor-made network telescope for their use case. [4]

1.2. Telescope Categorization

A categorization scheme is required to keep track of the multitude of telescopes.

One main difference between telescopes is how they react to incoming packets. Based on this characteristic, they have been grouped into two categories.

Passive telescopes store the data of the incoming package, but they do not send a response. They simply ignore the sender. Reactive telescopes, on the other hand, actively respond to incoming packages in real-time. This allows them to gain insight into more types of attacks. [5]

Chapter 2 presents the background information needed to understand network telescopes and their benefits. Chapter 3 explains how the telescopes work in general. In Chapter 4 and 5, we showcase the two main types of telescopes and list what we think are the largest projects in this field.

2. Background

To fully understand how network telescopes work, we need to look at the basics of networking using IPv4 and IPv6. Recognizing the benefit of darknets also requires us to examine the different types of attacks that cybercriminals use.

2.1. IPv4 Networking

Devices require an Internet Protocol version 4 (IPv4) address to communicate over the Internet. An IPv4 address identifies computers. It is 32 bits long. Therefore, the address space is limited to $2^{32} = 4\,294\,967\,296$ addresses. The 32 bits of an IP address are made up of a network identifier and a host identifier. [6]

One popular way of writing IPv4 addresses is the CIDR notation. In CIDR notation, the "/" character indicates how many bits are used for the network identifier. /x indicates that x bits are used to encode the network part of the address. The remaining 32-x bits identify the host. Such a network contains 2^{32-x} hosts. Using the CIDR notation is especially useful when it comes to network telescopes.

Assume a host sends a packet to a random IP address. We want to calculate the probability that the randomly chosen IP address is within a specific targeted address range. This probability is described by the ratio of targeted IP addresses to all the available IP addresses [2]. Using the CIDR notation, we can quickly compute this with the

 doi: 10.2313/NET-2025-11-3_02

following formula: $p_x = \frac{1}{2^x}$ So for a /10 network the probability is $p_{10} = \frac{1}{2^{10}} = \frac{1}{1024}$.

As mentioned, the number of IPv4 addresses is limited. Yet more and more people own a digital device and use it to connect to the Internet. The growing demand for IPv4 addresses can only be met using workarounds like Network Address Translation and dynamic IPv4 address assignment. [6]

Besides the very limited number of available addresses, there are other problems with IPv4. One of those problems is that IPv4 packages are not authenticated when they are transmitted. [6]

2.2. IPv6 Networking

The Internet Protocol version 6 (IPv6) is the successor to IPv4. In contrast to the previous version, the address length in IPv6 is much larger and totals 128 bits. So the available address space of 2^{128} addresses is 2^{96} times larger than IPv4. This larger address space prevents IP address exhaustion and ensures that hosts benefit from better network performance. [6]

The shift from IPv4 to IPv6 has already begun [6]. According to Fachkha and Debbabi [4], this far-reaching change impacts the attack and defense capabilities of hackers and security analysts. The larger address space and sparse distribution of addresses make it infeasible to scan all possible addresses [7]. This makes it harder for attackers to find victims. This is due to the fact that the number of devices with IP addresses assigned is only a fraction of the total IPv6 addresses. Fachkha and Debbabi [4] conclude that hackers need to scan more addresses to find one that is currently in use. In this case, the attackers also need to expend more computational and financial resources.

On the flip side, network telescopes will have trouble monitoring huge segments of the unused IP address space, as this would require more computation power. They are only able to monitor a fraction of the available data because packets from denial-of-service attacks, worms, and network scans are distributed among the entire IP address range. The smaller share of packets they can inspect is due to the lower percentage of addresses that they can monitor. [4]

2.3. Scanners

Scanners serve a variety of purposes. Amongst other reasons, they can be used by researchers to check if an IP address is currently in use or which services are running on a device. Those scanners can also be utilized by network administrators or security analysts for network maintenance or to provide a security assessment. [8]

However, they can also be used by malicious actors. In this case, scanners are often used to check the ports of a system for vulnerable applications. They not only focus on specific operating system exploits but also scan for vulnerable services such as SSL, SMTPS, and so on. [5]

Bakar and Kijsirikul [9] state that traditional scanners establish TCP connections to various ports of an IP address. They describe that using a particular payload, traditional scanners can check for vulnerabilities. Yet according to Li et al. [8], this type of scanner does not scale well. He and his team found that lots of processing power needs to be used upfront, without the scanner knowing if there is a machine behind the targeted IP address.

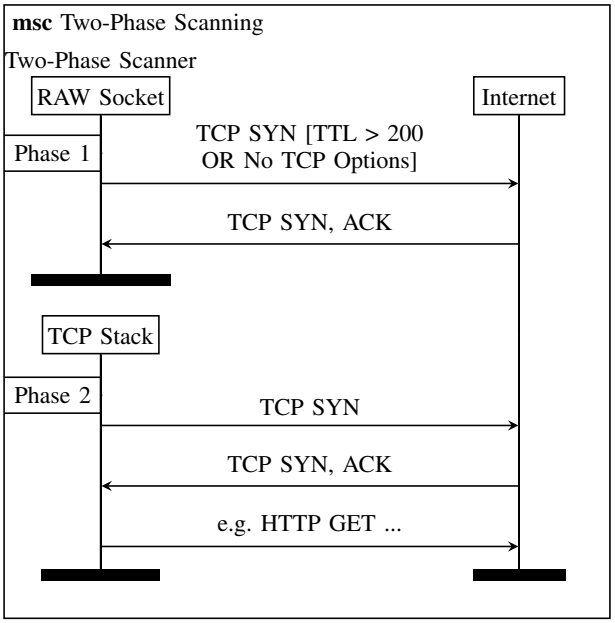

Figure 1: Two-phase scanning adapted from [5].

In order to prevent this waste of resources, the scanning process is split into two phases, as depicted in Figure 1. In the first phase, the scanner enumerates targets that need to be checked in more detail. This is achieved by sending an initial request to a host and waiting for a reply. If the host reacts to the original message, it is alive. [5]

In the second phase, the scanner will conduct a more in-depth scan of the targets that it has discovered. This approach reduces the scanning complexity and addresses the scalability issues. Two-phase scanners do not need to maintain a state, as they can make use of SYN cookies to encode information. [5]

Stateless scanners often use handcrafted packets to increase their scan speed. These irregular packages typically have larger TTL values, no TCP Options, or both. [5]

2.4. Malicious Activities

Hackers use a variety of strategies and actions to achieve their goals. They make use of network reconnaissance, spread malware, and try to disable computer systems. In this chapter, we only cover the activities that are related to network telescopes.

2.4.1. Denial-of-Service. A denial-of-service (DoS) attack describes an act by which an attacker sends a multitude of requests to a computer to make it unavailable to its normal users. One single device can hardly send enough requests to achieve this. Therefore, attackers rely on a large set of hosts to launch a coordinated attack on a victim. [4] [10]

In order to prevent the target from easily blocking such requests, the malicious actors spoof (forge) their IP

 doi: 10.2313/NET-2025-11-3_02

address. The spoofed IP address is typically chosen at random and included in the TCP package as the source address. When the victim receives a request, it sends a reply to the faked source address. As the attacker used a random IP address, the victim's response will be randomly distributed across the entire IP address space. Some of those packages will be directed to random addresses monitored by a network telescope. The addresses monitored by the telescope are globally routed but unutilized. This means that besides the telescope, no active hosts or services are assigned to them. For this reason, those unsolicited responses can indicate that the sender is a victim of a DoS attack. In order to classify such traffic as a denial-of-service attack, the number of packets, the attack duration, and the packets received per second need to be taken into account. [10]

2.4.2. Internet Worms. One more use case for network telescopes is detecting computer worms [4]. Viruses and trojans require human interaction to spread. According to Li et al. [11], worms can automatically infect other devices in a network. The researchers identified two classes of computer worms. Classical worms do not take measures to evade worm detectors. The more advanced evasive worms continuously evolve. Li et al. outline that this allows the evasive worms to bypass existing detectors.

Network telescopes make it possible to collect large amounts of data so that the characteristics and spread of computer worms can be better understood [12].

2.4.3. Network Scans. One of the most important steps in carrying out an attack on a network is reconnaissance [4]. Using network scans, malicious actors can identify vulnerable machines. If such attacks are detected early, security experts can effectively mitigate them. [3]

Network scanning accounts for most of the data received by the telescopes. TCP packets comprise most of the network telescope traffic. This is because the TCP protocol allows for a variety of scanning techniques. [4]

3. How do Network Telescopes work?

Network telescopes are one of the many tools in the arsenal of researchers and security analysts. In contrast to defending and protecting a particular company or set of devices, network telescopes are used to monitor large-scale events occurring across the Internet [3]. The intelligence gained from network telescopes can help protect all Internet users [4].

To accomplish their task, the darknets monitor globally routed and unutilized IP address space that has been assigned to them [2]. An address is *unutilized* if there are no devices assigned or services running on it besides the network telescope. As none of those IP addresses are allocated to a normal host, there is no legitimate traffic to those address ranges. The unrequested packages are typically referred to as Internet Background Radiation (IBR) [3].

This data can be analyzed to gain insight into various types of malicious events, which have been described in Section 2.4. Network telescopes have proven to be an invaluable tool for gaining information on the spread of malware, network reconnaissance, denial-of-service, misconfigured devices, and software bugs [2] [12] [13] [14] [15]. Security analysts and researchers can leverage this data to mitigate the damage of attacks currently in progress and to prevent similar future attacks [3].

Depending on the number of IP addresses a network telescope is monitoring, it can also detect rare network events and provide more context. Like astronomical telescopes that provide a better resolution, the larger its aperture, the resolution of a network telescope increases the more unutilized addresses it is monitoring. [2]

In practice, a network telescope is only useful if its resolution is large enough to witness the type of events we want to detect with high enough probability. Small telescopes with very few monitored addresses will only rarely detect important events. Therefore, analyzing them by classifying the events and counting them becomes unreliable. To get meaningful results, we require a lot of data. [2]

4. Types Of Telescopes

In order to better understand network telescopes, it is essential to classify them. Broadly speaking, there are two main categories of network telescopes.

4.1. Passive Telescopes

As the name indicates, passive telescopes simply capture the packages that have been directed to one of their monitored IP addresses. This rather simple approach allows them to surveil large blocks of the IP address space using minimal resources and processing power. They can be utilized to gain information on malware spread, DoS attacks, and misconfigured devices. Passive telescopes are also suited for detecting and identifying network reconnaissance. They can be used to monitor traditional scanners and also provide basic insight into the initial phase of stateless two-phase scanners. However, since passive telescopes do not respond to any of the received packages, they are not able to see the second phase of such a scanning effort. [5]

4.2. Reactive Telescopes

Most network telescopes are passive measurement instruments. Due to this, they can not fully detect all types of attacks. Reactive telescopes were invented to address the shortcomings of this approach. Reactive network telescopes respond to TCP SYN packages in real-time. By answering the original packages, a reactive network telescope continues the interaction and gains more insight as it receives more packages from the adversary. Therefore, this telescope category offers the additional benefit of fully detecting two-phase scanners. One example of a reactive network telescope is Spoki. [5]

5. Network Telescope Projects

Over the years, many network telescopes have been created. They were used for very specific purposes, and many of them have changed over the years. The aim of this section is to present a selection of large and influential network telescopes. The findings of this section are summarized in Table 1.

TABLE 1: Comparison of different telescopes

	Telescope			
Property	**Spoki**	**UCSD**	**Orion**	**NICTER**
Type	Reactive	Passive	Passive	Passive
Size	not actively deployed could handle /8 IPv4 prefixes	∼12,500,000	∼500,000	∼300,000
Use-Cases	Monitor two-phase scanners	Monitor DoS attacks, Internet worms and networks scans	Track botnets, monitor DoS attacks and network scans	Analyze network attacks

5.1. Spoki

Spoki is a reactive network telescope developed by the researchers Hiesgen et al. [5]. One of the aims of their newly developed telescope is to gain more insight into two-phase scanners. To achieve this, they deployed Spoki to four /24 IP prefixes. The research team demonstrated that their newly developed scanner can handle one million packages per second.

Spoki replies to the SYN packages that are sent to the unutilized IP space it monitors. If the original request is sent by a regular scanner, a host infected by a worm, or a misconfigured device, we do not gain any more information than from a passive telescope. In case the originator of the SYN package is a two-phase scanner, the scanner ignores the telescope's response at first. However, after a short delay, the scanner sends a regular SYN package, thereby starting phase two. Spoki also completes the second handshake, resulting in the stateless scanner sending its payload. The reactive telescope then stores the payload that the scanner sent and resets the connection. [5]

5.2. UCSD Telescope

This passive telescope is run and maintained by the University of California, San Diego (UCSD). Currently, the project makes use of a globally routed /9 and /10 network [15]. Those IP ranges have been allocated to "Amateur Radio Digital Communications" (ARDC) and are typically referred to as 44Net [16].

Before 2019, the network spanned more than 16 million routable IPs and made up $\frac{1}{256}$ of all IPv4 addresses. Nowadays, the network telescope contains approximately 12.5 million addresses and makes up roughly $\frac{1}{340}$ of all IPv4 addresses. [17]

A very small fraction of the IPs within this range are utilized by ARDC to educate their members on digital radio communication and to conduct experiments [15]. The UCSD telescope simply filters out legitimate traffic to the utilized addresses and focuses on those that are not assigned to an active host [15]. In 2018, the UCSD telescope received an average of 3.6 TB of network data per day [18].

The UCSD telescope has already been used in the past to detect events like DoS attacks, Internet worms, and network scans [15].

On July 19, 2001, a computer worm called Code-Red infected multiple hundred thousand machines. It caused economic damage exceeding $2.6 billion. Normally, analyzing the spread of such worms is very challenging. Using the UCSD network telescope, Moore et al. managed to detect more than 359,000 hosts infected with Code-RedI v2. To conclusively identify a machine as infected by the worm, it had to send two probes to IP addresses monitored by the network telescope. [12]

The UCSD telescope was also used by Dainotti et al. [19] to analyze the network scans conducted by the Sality botnet.

The researchers Gao et al. [14] developed the analytical framework DarkSim. DarkSim makes use of the UCSD telescope data to identify traffic patterns that need to be investigated further. The project was used to detect a change in scanning behavior after the disclosure of vulnerabilities related to Microsoft products. They also managed to gain insight into the systems conducting those scans.

5.3. Orion Network Telescope

The Orion Network Telescope is operated by the Merit Network, an independent nonprofit corporation run by universities in Michigan. The telescope is accessible to researchers. Like the UCSD telescope, it is entirely passive. One difference between those two darknets is that the Orion telescope makes use of /24 networks. By combining 1856 of those /24 networks, they created a network telescope that can monitor roughly 500,000 IP addresses. [20]

By aggregating all those networks, this telescope effectively tracks a /13 address block. On a typical day, the telescope run by Merit Network captures ∼100GB of compressed network data consisting of roughly 3 billion packages. [21]

All the traffic that reaches the Orion Network Telescope is saved in the PCAP file format [20]. The stored data includes the origin IP, targeted port, timestamp, and other information. In the past, the Orion Network telescope had coverage of roughly 75% of a /8 address block [22].

The Orion Network Telescope is used for tracking botnets, detecting scanners, and gaining insight into DoS attacks [20]. Near the end of 2016, the Mirai malware popped up. This malware infected IoT devices, which it then used to conduct DDoS attacks. Antonakakis et al. [23] made use of the Orion Network Telescope to retrospectively analyze how the botnet emerged. They also managed to provide a history of the botnet's DDoS victims. They found that during the 7-month timeframe starting from July 18, 2016, the Orion Network Telescope received roughly 1.6 billion packages per day.

5.4. NICTER

The Network Incident Analysis Center for Tactical Emergency Response (NICTER) project aims to analyze and understand ongoing network attacks [24]. This large-scale passive network telescope is run by the Japanese Research Institute NICT [24]. The project was launched in 2005 and monitored approximately 16,000 addresses. In the following years, the number of captured IP ranges constantly increased. Currently, the size of the network telescope hovers around 300,000 IP addresses. Using the captured data, NICTER publishes a detailed report every year. According to NICTER's yearly report, they observed roughly 1.9 billion packets per day in the year 2024. [25]

NICTER's darknet observations have been used to gain insight into botnets like Mirai and Hajime [26] [27].

6. Conclusion

In this paper, we examined multiple different network telescopes. All the telescopes were either classified as passive or as reactive. Chapter 4 also highlighted the key differences between those two categories. The main difference is how the telescope reacts to incoming packages. This behavior decides how well the network telescope can monitor tools used for network reconnaissance.

References

[1] W. Mazurczyk and L. Caviglione, "Cyber reconnaissance techniques," *Commun. ACM*, vol. 64, no. 3, pp. 86–95, Feb. 2021. [Online]. Available: https://doi.org/10.1145/3418293

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

[3] M. Kallitsis, R. Prajapati, V. Honavar, D. Wu, and J. Yen, "Detecting and interpreting changes in scanning behavior in large network telescopes," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3611–3625, 2022.

[4] C. Fachkha and M. Debbabi, "Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1197–1227, 2016.

[5] 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

[6] O. Babatunde and O. Al-Debagy, "A comparative review of internet protocol version 4 (ipv4) and internet protocol version 6 (ipv6)," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 13, no. 1, 2014.

[7] Y. Fang, L. Zhang, L. Li, C. Sun, Y. Guo, H. Zhang, B. Lin, J. Wang, and W. Xia, "An ipv6 address fast scanning method based on local domain name association," *Scientific Reports*, vol. 15, no. 11524, Apr 2025.

[8] G. Li, M. Zhang, C. Guo, H. Bao, M. Xu, H. Hu, and F. Li, "IMap: Fast and scalable In-Network scanning with programmable switches," in *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*. Renton, WA: USENIX Association, Apr. 2022, pp. 667–681. [Online]. Available: https://www.usenix.org/conference/nsdi22/presentation/li-guanyu

[9] R. Abu Bakar and B. Kijsirikul, "Enhancing network visibility and security with advanced port scanning techniques," *Sensors*, vol. 23, no. 17, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/17/7541

[10] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems*, vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: https://doi.org/10.1145/1132026.1132027

[11] J. Li, D. Sisodia, and S. Stafford, "On the detection of smart, self-propagating internet worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 3051–3063, 2023.

[12] D. Moore, C. Shannon, and J. Brown, "Code-Red: a case study on the spread and victims of an Internet worm," in *Internet Measurement Workshop (IMW)*, November 2002, pp. 273–284.

[13] K. Benson, A. Dainotti, k. claffy, A. Snoeren, and M. Kallitsis, "Leveraging Internet Background Radiation for Opportunistic Network Analysis," in *ACM Internet Measurement Conference (IMC)*, October 2015.

[14] M. Gao, R. Mok, E. Carisimo, k. claffy, E. Li, and S. Kulkarni, "DarkSim: A Similarity-Based Time Series Analytic Framework for Darknet Traffic," in *Proceedings of the 2024 ACM on Internet Measurement Conference*, November 2024.

[15] C. for Applied Internet Data Analysis, "The UCSD Network Telescope," https://www.caida.org/projects/network_telescope/, 2025, [Online; accessed 25-May-2025].

[16] A. R. D. Communications, "AMPRNet Wiki," https://wiki.ampr.org/wiki/Main_Page, 2024, [Online; accessed 25-May-2025].

[17] A. Camargo, L. Bertholdo, and L. Granville, "Less is more? exploring the impact of scaled-down network telescopes on security and research," in *Anais do XLII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Porto Alegre, RS, Brasil: SBC, 2024, pp. 1050–1063. [Online]. Available: https://sol.sbc.org.br/index.php/sbrc/article/view/29854

[18] A. Mangino, M. S. Pour, and E. Bou-Harb, "Internet-scale insecurity of consumer internet of things: An empirical measurements perspective," *ACM Trans. Manage. Inf. Syst.*, vol. 11, no. 4, Oct. 2020. [Online]. Available: https://doi.org/10.1145/3394504

[19] A. Dainotti, A. King, K. Claffy, F. Papale, and A. Pescapé, "Analysis of a "/0" Stealth Scan From a Botnet," *IEEE/ACM Transactions on Networking*, vol. 23, no. 2, pp. 341–354, 2015.

[20] M. Network, "Orion Network Telescope," https://www.merit.edu/research/projects/orion-network-telescope/, [Online; accessed 25-May-2025].

[21] R. Prajapati, V. Honavar, D. Wu, J. Yen, and M. Kallitsis, "Shedding light into the darknet: scanning characterization and detection of temporal changes," in *Proceedings of the 17th International Conference on Emerging Networking EXperiments and Technologies*, ser. CoNEXT '21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 469–470. [Online]. Available: https://doi.org/10.1145/3485983.3493347

[22] 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 Internet Measurement Conference*, ser. IMC '14, 2014, pp. 435–448. [Online]. Available: https://doi.org/10.1145/2663716.2663717

[23] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium*. Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[24] NICTERWEB, "What is the NICTER Project?" https://www.nicter.jp/en/project, [Online; accessed 25-May-2025].

[25] N. I. of Information and C. Technology, "NICTER Observation Report 2024," National Institute of Information and Communications Technology (NICT), Tech. Rep., February 2025.

[26] S. Pham Anh and Y. Nakamura, "A baseline investigation into the evolution and prevalence of mirai and hajime utilizing a network telescope," *IEEE Access*, vol. 12, pp. 103 789–103 809, 2024.

[27] T. Kasama, "Long-term darknet analysis in nicter," *Journal of the National Institute of Information and Communications Technology*, vol. 63, no. 2, pp. 25–31, 2016.