3 Cybersecurity Technologies : Darknet Monitoring and Analysis
3-1 Long-term Darknet Analysis in NICTER

Takahiro KASAMA

We have been developing the NICTER, which is the R&D project/system against cyber-attacks in NICT, and monitoring darknet traffic. In this report, we provide statistical analysis results based on a long-term darknet monitoring on NICTER. In addition, we show a characteristic changes in cyber-attacks observed in NICTER.

1 Introduction

The first step in cyberattack countermeasures is to quickly and correctly understand actual attack activities. We have been performing research and development at the Network Incident Analysis Center for Tactical Emergency Response (NICTER), to understand the overall attack trends of cyberattacks on the internet, and have observed and analyzed a darknet for approximately 11 years since 2005 [1]–[3]. "Darknet" means a set of routed but unused IP address spaces on the internet. Since there are no real hosts and servers, darknet traffic includes only abnormal traffic and reflects malicious activities such as scanning by malware-infected hosts, sending shellcode with UDP packets, and backscatters of distributed denial of service (DDoS) attacks. Therefore, monitoring darknet traffic is a very effective method of observing and understanding cyberattacks on the internet.

This paper statistically analyzes NICTER's darknet monitoring results, clarifies attack activities over time, and describes characteristic attack activities.

2 Number of darknet addresses

Generally, the more the number of observed darknet address increases, the more attack activities are observed. Also, in order to understand whether the observed attack activities are generated locally or broad based, it is desirable that the observed darknet be widely distributed on the internet, not only in a specific address range. This is why NICTER is building a darknet monitoring system that distributes installation of darknet sensors based on cooperation with various organizations in Japan and overseas, then collects and manages the darknet traffic observed by these sensors in real time. This darknet monitoring system started from approximately 16,000 addresses in 2005, and reached 300,000 addresses in April 2016. Now, NICTER has built the largest darknet monitoring system in Japan.

3 Statistics of long-term darknet observation

3.1 Number of observed packets and number of unique hosts over time

To clarify quantitative changes in darknet observation results, Fig. 1 shows the number of packets, and Figure 2 shows the number of unique source IP addresses (hereinafter, "Number of Unique Hosts") observed each day in our darknet from January 1, 2011, to December 31, 2015 (all packets, only TCP packets, only UDP packets). In time series line graphs below, the number of observed packets is strongly affected by changes in the number of observed darknet addresses, so we normalized the number of observed packets by using the number of darknet addresses. Also, to make it easier to see trends, we plotted a 2-week moving average in the figures.

As seen in Fig. 1, the number of packets observed in the darknet fluctuates to some extent, but it shows a long term trend to increase, and we can see the number of observed packets especially increased suddenly since 2014. This increase was mainly caused by more active DDoS attacks such as Distributed Reflection Denial of Service (DRDoS) attacks and attack activities related to embedded devices as described later. Corresponding to the increase in the number of observed packets, the Number of Unique Hosts in Fig. 2 is partly affected by an increase in the

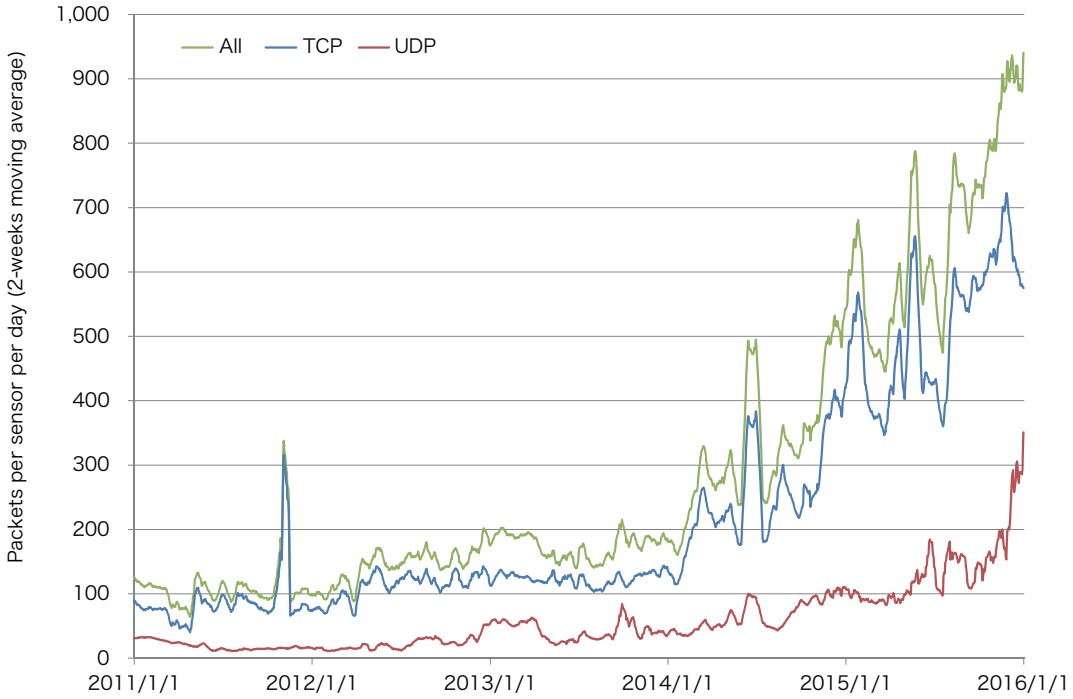

Fig. 1 Number of packets observed for five years

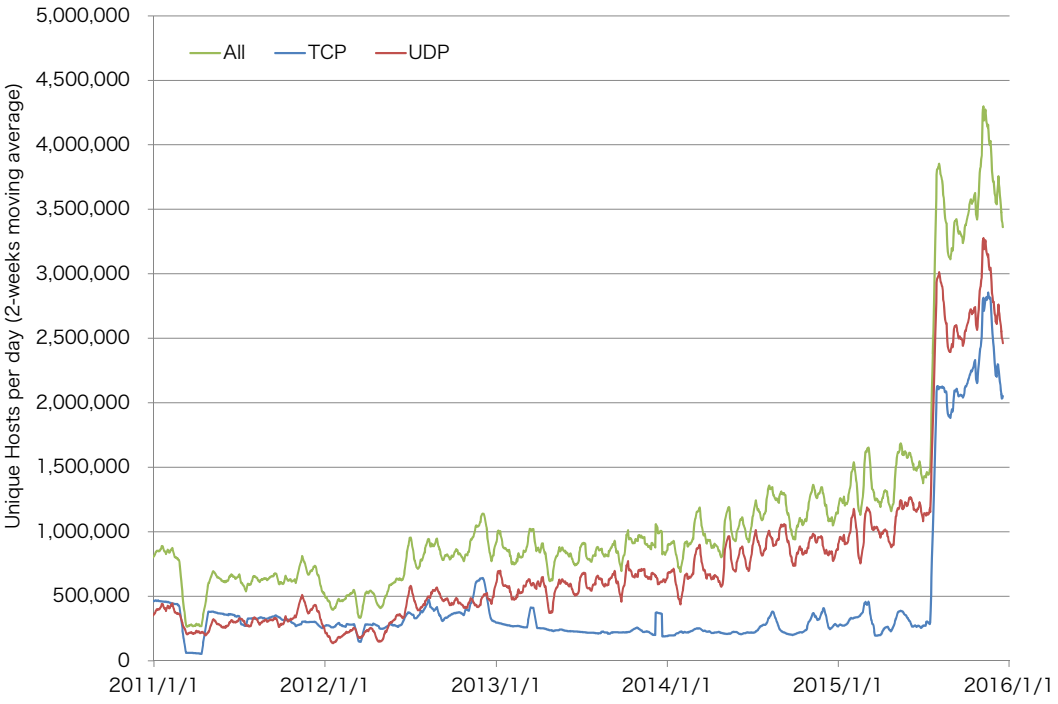

Fig. 2 Number of unique hosts for five years

number of sensors, but it shows an overall increasing trend. The sudden increase since mid-2015 was affected by the large number of hosts observed that send packets viewed as Peer-to-Peer (P2P) to the darknet, but details of the causes are unclear.

Previously, many packets observed in the darknet were scans by worm type malware (mainly aimed at Windows OS). However, with the decrease in the number of unique hosts observed in the darknet until the first half of 2008, many security researchers said that large-scale infections of worm type malware like Sasser, Blaster and SQL Slammer that appeared in the first half of the 2000s could not occur any more. However, many large-scale pandemics of worm type malware still occurred since then, such as the Conficker worm in the second half of 2008, Morto worm in 2011, and Carna botnet in 2012, and the number of observed

Table 1 Percentages of annual observed packets by destination port & protocol

2011		2012		2013		2014		2015	
Port	%	Port	%	Port	%	Port	%	Port	%
445/TCP	51.3	445/TCP	47.8	445/TCP	36.0	23/TCP	20.9	23/TCP	21.4
1433/TCP	6.4	3389/TCP	8.8	3389/TCP	5.7	445/TCP	15.1	445/TCP	7.0
53/UDP	5.1	1433/TCP	6.6	10320/UDP	5.5	22/TCP	6.2	22/TCP	4.7
22/TCP	2.6	23/TCP	6.6	53/UDP	4.3	80/TCP	4.5	80/TCP	3.1
3389/TCP	2.3	22/TCP	3.3	1433/TCP	3.8	3389/TCP	3.7	8888/TCP	2.2
80/TCP	2.2	10320/UDP	3.2	23/TCP	3.8	53/UDP	3.6	8080/TCP	2.2
135/TCP	1.6	80/TCP	3.1	80/TCP	3.1	8080/TCP	3.6	3389/TCP	2.0
3306/TCP	1.1	8080/TCP	2.0	22/TCP	2.7	5000/TCP	3.2	53413/UDP	1.9
5060/UDP	1.1	210/TCP	1.6	8080/TCP	1.5	1433/TCP	2.9	443/TCP	1.6
23/TCP	0.9	3306/TCP	1.4	18991/UDP	1.3	443/TCP	2.6	53/UDP	1.5

packets has kept increasing. Additionally, in recent years, many packets that differ from scans by previous worm type malware are also being observed, such as scans using open source high speed network scanners such as Zmap and masscan, periodic scans for surveys by security vendors and research organizations, and scans to search for reflectors for DRDoS attacks. Attack activities that can be seen in darknet observations are increasing not only quantitatively; they are also increasing in diversity from a qualitative viewpoint.

3.2 Changes in the trend of targeted services

Next, in order to understand changes in targeted services, Table 1 shows the top ten destination ports and protocols in terms of number of packets counted, for each year from 2011 to 2015.

Conficker, among the most infamous pandemic malware, appeared in 2008. It exploited a vulnerability in the Windows Server service on port 445/TCP to spread its infections. Attacks on port 445/TCP are still one of the top port/protocols observed by NICTER. The report by the Conficker Working Group also showed that there are approximately 600,000 hosts still infected with Conficker at the end of 2015, so Conficker's scans still have large impacts even though approximately seven years have now passed since it appeared. Similarly, the Morto worm appeared in 2011; it scans 3389/TCP (Windows Remote Desktop Protocol) and tries to login as admin to spread its infections. We have been observing scans on port 3389/TCP.

Scans by these kinds of worm type malware that were prevalent in the past are still being observed, and many new attack activities are also being observed. The most remarkable change in the past 5 years was the increase in scans of 23/TCP (Telnet). Telnet is a protocol to access and remotely operate another computer beyond the network. Telnet itself does not encrypt any data sent over the connection, so it is very risky to use on the internet. However, in the past few years, the growing trend of the Internet of Things (IoT) is connecting a wide variety of devices to the internet. We found that many of these devices use Linux OS, and can be accessed from the internet through Telnet service. Attacks on Telnet aimed at these embedded devices became more active since 2012, resulting in many scans of Telnet in our darknet monitoring. Besides Telnet, we also observed some attacks on port 5000/TCP, 53413/UDP, etc. targeted to vulnerabilities in specific embedded devices such as routers and Network Attached Storage (NAS). These attacks differ from conventional attacks on Windows OS, and are expected to continue to be very active in the future. Also, scans on port 53/UDP that search for open DNS resolvers increased remarkably since 2011, becoming one of the top of the list. In addition to DNS, searches for various reflectors that can be misused in DRDoS attacks, such as NTP and SNMP, are also increasing.

4 Case studies

This section describes characteristics of phenomena observed in the past five years.

4.1 Increase in attacks targeting embedded devices

As shown in Table 1, scans on port 23/TCP (Telnet) increased suddenly the past two years. Figure 3 shows changes in the number of packets and number of unique hosts on port 23/TCP. Looking at Figure 3, the number of unique hosts shows a sharp peak in the second half of 2012, at over 300,000 hosts observed per day. Our analysis shows that we observed large-scale scans by the Carna bot which was active in the same period [4]. The anonymous creator(s)

of the Carna bot reported that they were able to distribute Carna by using large-scale scans of Telnet and login attempts by dictionary attacks, and approximately 420,000 embedded devices such as routers and webcams were infected with Carna. Many of these embedded devices are operating without changes to their simple ID and password in default settings, such as "admin", "password" and "1234". Thus, it is easy to log in to them with admin rights via the internet. The Carna bot's creator(s) misused these devices to scan the entire IPv4 address space, and published its results. The Carna bot stopped its activities after a short period, so scans of Telnet on the darknet also subsided temporarily, but it became active again since early 2014, and many such scans continue to be observed since then.

In order to clarify what kind of devices are actually conducting these scans on Telnet, we used Telnet and HTTP to access approximately 200,000 addresses for which scans were observed during the week from August 25 to 31, 2015, in an attempt to identify devices from the responses. This resulted in us collecting responses from 40,000 addresses (approximately 20%), and confirmed that these devices are actually embedded devices including digital video recorders, webcams, and Wi-Fi routers[5]. These devices differ from the usual PCs and servers, in that they are often not managed appropriately with firmware updates, etc. after setup. This makes them good targets for attackers, and we found that many devices are already infected. We also observed and analyzed a honeypot system developed to capture and analyze malware that actually infects embedded devices. With the honeypot, we observed 43 types of malware running on 11 different CPU architectures, and saw that infected devices were used in various attacks such as DDoS attacks[6].

Our observations show that the most common attacks observed were against Telnet, but embedded device-related vulnerabilities other than Telnet were also reported several times, and attacks on those are also observed in the darknet. For example, the vulnerability in NAS made by Synology on port 5000/TCP was reported in January 2014, and 2 months after that, a sudden increase in scans on 5000/TCP was observed. This relationship is also true for backdoors (32764/TCP) found in routers made by Cisco and NetGear, etc., and a vulnerability (53413/TCP) in routers made by Netis. Therefore, it is important to quickly detect such changes.

4.2 Increase in DDoS attacks (DRDoS attacks)

The DRDoS attack is one type of DDoS attack. It is also called a reflection attack or an amplification attack. In the DRDoS attack, the attacker(s) sends a huge number of queries that spoof the sender's IP address as the victim's IP address, to reflectors that can be used on the internet (typically, open DNS resolvers, etc.). This results in responses that amplify the data size to be larger than the

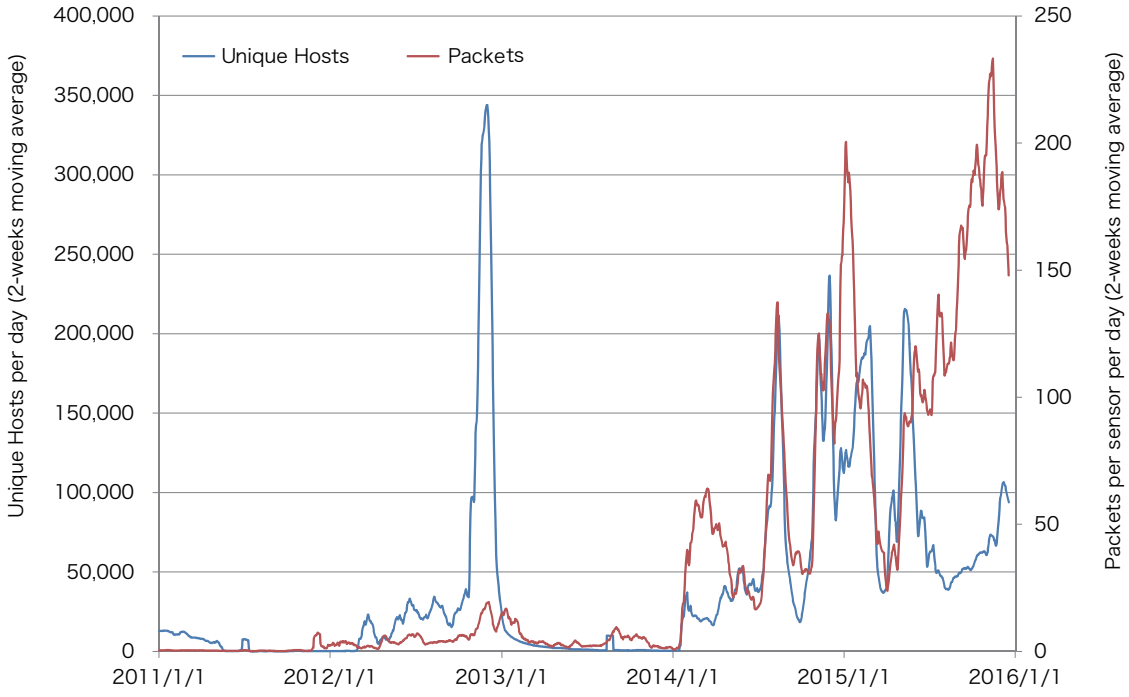

Fig. 3 Statistics of darknet traffic on Port 23/TCP (Telnet)

query size, sent from a huge number of reflectors to the victim, thus maxing out the bandwidth (Fig. 4). The existence of such reflection attacks have been known for a long time, but in 2013, a huge DRDoS attack was generated that reached up to a huge 300 Gbps against Spamhaus, which was widely discussed. In the background of this attack, there were a huge number of household routers behaving as open DNS resolvers[7]. In addition to DNS, it is known that many protocols such as NTP and SNMP can be misused in DRDoS attacks, and many cases of attacks are being reported. To efficiently make a DRDoS attack, an attacker must search for reflectors in advance, so corresponding to the activity of DRDoS attacks, various reflector search scans are also increasing. Figure 5 shows changes in numbers of observed darknet packets for DNS (53/UDP), NTP (123/UDP) and SNMP (1900/UDP), which are used in many DRDoS attacks. Looking at Fig. 5, we see that DNS scans were observed from around 2013, and NTP and SNMP from around 2014. DDoS attacks have various aims, for example the OpKillingBay DDOS attack by Anonymous to protest dolphin hunting, and DDoS attacks by the DDoS for BitCoin (DD4BC) criminal organization that demand bitcoin payments to stop a DDoS attack on a company website. It's becoming increasingly important to understand attack activities related to DDoS attacks.

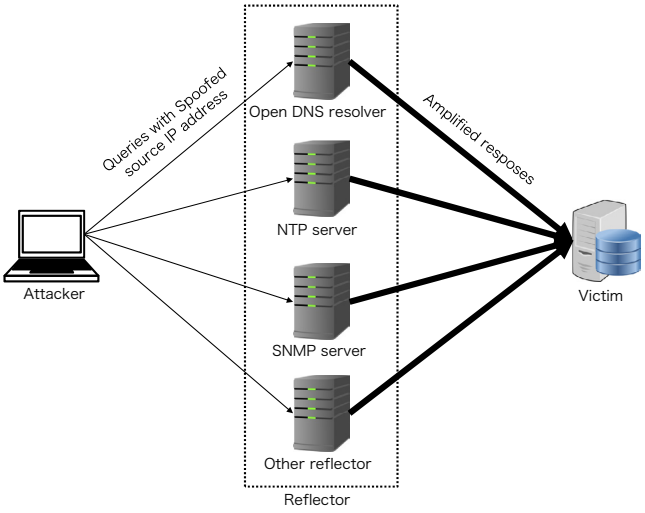

Fig. 4 Overview of DRDoS attack

4.3 Appearance of high speed network scanners and scans from security organizations

In recent years, open source network scanners have been developed that can perform high speed network scans, even on general spec machines. Among them, Zmap is an especially famous scanner developed at the University of Michigan in 2013. To achieve higher speeds, Zmap foregoes per-connection state and tracking. It is reported that if proper conditions are arranged, Zmap can scan the entire IPv4 address space in 45 minutes. The existence of such high speed network scanners is certainly useful for people who research the internet, including security research, but attackers can also benefit from this.

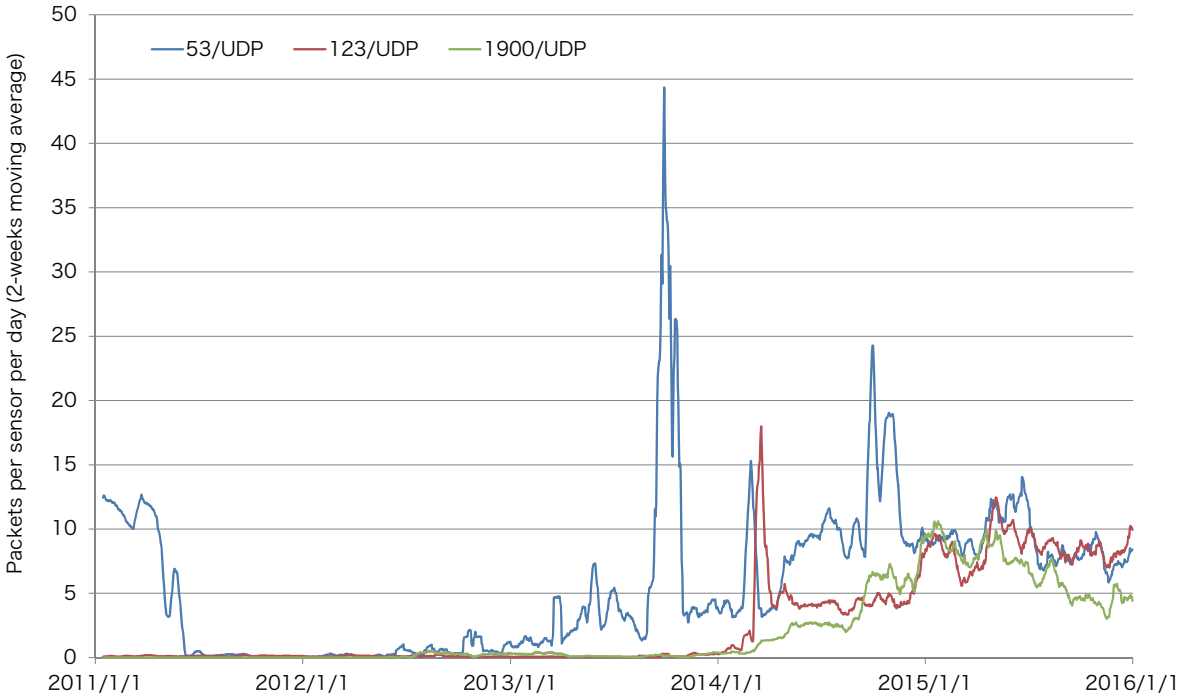

Fig. 5 Statistics on number of observed packets related to reflector searches

To understand the usage situation of Zmap in actual scans, Figure 6 shows scans that used Zmap among TCP SYN packets observed each month from June to December 2015 in the darknet. To judge whether packets were generated by Zmap, we used a system that judges characteristic packets based on header information[8]. This system judges by using characteristics such as that in Zmap's default settings, the IP header's ID value is always set to 54321. In Figure 6, we found that around 10% of all TCP SYN packets observed were sent using Zmap. Approximately 10 to 30 million packets were observed per day. This confirmed that many scans using Zmap were observed.

These senders include the University of Michigan which developed Zmap. They use Zmap to periodically scan the entire internet, for survey purposes. For example, to find servers affected by the Heartbleed vulnerability in OpenSSL, and find IoT devices connected to the internet, etc. In recent years, other than the University of Michigan, there are various security related organizations and research institutes that perform large-scale network scans for research purposes: Shodan, Shadowserver, Rapid7, etc. Much scan traffic from these organizations is also observed in the darknet, appearing as noise that affects analyses. Therefore, we have to exclude these scans when analyzing the darknet traffic.

5 Conclusion

This paper statistically analyzed darknet traffic observed at NICTER from 2011 to 2015, and showed changes in characteristic attack activities observed.

Recent years have brought more diverse attack techniques, such as the rise of using the web for drive-by download attacks, and targeted attacks against specific organizations. Those attacks cannot be observed by only using passive monitoring techniques like darknet monitoring. However, our long-term darknet monitoring results show that attack activities that can be seen in darknet monitoring are in an increasing trend. In addition to previous types of attack activities, we see that new attack activities are appearing. It is important to continue to observe and analyze darknet traffic, and use that knowledge to research and develop countermeasure techniques. On the other hand, it is difficult to observe all attack activities by only using darknet monitoring, so further study is required that analyzes by effectively combining a wide variety of cybersecurity information from honeypots, web crawlers, various vulnerabilities information, etc.

References

1 D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, "nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis," In WOMBAT Workshop on Information

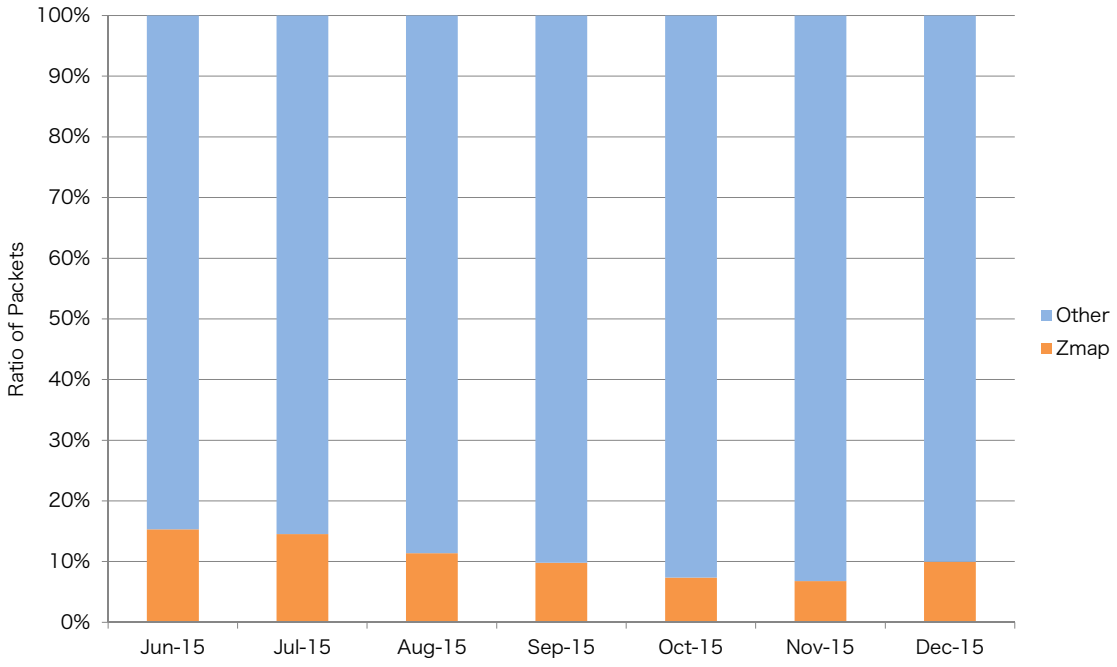

Fig. 6 Ratio of zmap packets to the total number of observed packets (TCP SYN packets)

Security Threats Data Collection and Sharing, pp.58-66, 2008.
2 K. Nakao, D. Inoue, M. Eto, and K. Yoshioka, "Practical Correlation Analysis between Scan and Malware Profiles against Zero-Day Attacks Based on Darknet Monitoring," IEICE TRANSACTIONS on Information and Systems, vol.E92-D, no.5, pp. 787-798, May 2009.
3 M. Eto, D. Inoue, J. Song, J. Nakazato, K. Ohtaka, and K. Nakao, "nicter: A Large-Scale Network Incident Analysis System," In Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2011), April 2011.
4 E. L. Malècot, and D. Inoue, "The Carna Botnet Through the Lens of a Network Telescope," In Proceedings of the 6th International Symposium on Foundations and Practice of Security (FPS 2003), October 2013.
5 T. Kasama, J. Shimamura, and D. Inoue, "Understanding Malicious Activities of Embedded Devices Based on Correlating Observation Results from Passive and Active Monitoring (in Japanese)," IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, vol.J99-A, no.2, pp. 94-105, February 2016.
6 Y. M. Pa Pa, S. Suzuki, K. Yoshioka, T. Tsutomu, T. Kasama, C. Rossow, "IoTPOT: Analysing the Rise of IoT Compromises,"In Proceedings of The 9th USENIX Workshop on Offensive Technologies (WOOT '15), August 2015.
7 https://www.nic.ad.jp/ja/copyright.html
8 T. Koide, D. Makita, T. Kasama, M. Suzuki, D. Inoue, K, Nakao, K. Yoshioka, T. Matsumoto, "tkiwa: A Detection Tool for Packets with Characteristic Network Protocol Header (in Japanese)," IEICE technical report, vol.115, no.334, ICSS2015-38, pp.19-24, November 2015.

Takahiro KASAMA, Ph.D.

Researcher, Cybersecurity Laboratory,
Cybersecurity Research Institute
Cybersecurity