NICTER Analysis report 2016

Cybersecurity Laboratory, Cybersecurity Research Institute
National Institute of Information and Communications Technology

1. Introduction

This report summarized the status of cyberattack-related communications detected in 2016 through darknet monitoring, a part of the NICTER (Network Incident Analysis Center for Tactical Emergency Response) projects. During this year, we observed outbreaks of malware (e.g., Mirai), infecting such IoT devices as home routers and web cameras, and record-scale DDoS (distributed denial of service) attacks, resulting in malicious exploitation of infected devices. Darknet monitoring is an effective technique to grasp the extent of attack activities by Mirai and other worm-type malware actively expanding their infection ranges. This report also presents the temporal change in the number of malware attacks detected over the year.

2. What is darknet monitoring?

First, we will explain “darknet monitoring,” a term generally unfamiliar to the public. A darknet refers to a set of accessible but unused IP addresses on the Internet. These IP addresses are “unused” as they are unconnected to any servers or computers. Accordingly, darknets are expected to be inaccessible by normal Internet users. To illustrate darknets, please consider the following metaphoric example. IP addresses are addresses of devices connected to the Internet, and a darknet represents addresses of “empty houses” on the Internet. Nobody visits empty houses under normal circumstances. However, darknet monitoring has revealed that such empty houses actually receive large amounts of communications daily. Most of these communications are conducted by malware searching for the next target to attack. Such malware usually is not capable of locating computers susceptible to attack over the Internet, and it therefore randomly or sequentially selects potential targets, transmits data to them, and scans them by means of waiting for their response. This type of transmission reaches not only existing servers and computers but also devices on darknets. As such, it is feasible for us to grasp the general trends of cyberattacks occurring on the Internet (particularly the status of worm-type malware infections) by monitoring data transmission (packets) reaching darknets.

We have been monitoring darknets for about 12 years since the NICTER projects launched in 2005. For your reference, we present yearly statistics from 2005 in Table 1, including the number of packets detected, the scale of darknet monitoring (i.e., the number of IP addresses monitored), and the number of packets detected, which was normalized by the number of IP addresses monitored. We expanded the scale of darknet monitoring from about 16,000 IP addresses in 2005 to about 300,000 in 2016 by collaborating with various organizations in Japan and overseas. This expansion enabled us to detect more scanning activities of worm-type malware. The total number of packets detected annually*[1] in Table 1 is greatly influenced by the number of ID addresses monitored. Therefore, the number of packets detected per IP address per year listed in the right-hand column is the appropriate measurement of malware scanning activities occurring on the Internet. This measurement doubled yearly from about 60,000 packets detected in 2013 to about 110,000 in 2014, and again to about 210,000 in 2015 and again to about 470,000 in 2016. As we will explain later in this report, this doubling trend was caused by the emergence of Mirai and other malware targeting IoT devices, and the attacks appear to be further intensifying. Our report will focus on the 2016 statistics and some notable events observed during that year.

*[1] These numbers only represent the range of darknets monitored by NICTER and do not properly indicate the number of cyberattacks that have occurred throughout Japan.

Table 1. Number of packets per 1 IP address per year

Year	Number of packets par year (in billion)	Number of IP addresses for darknet (in thousand)	Number of packets per 1 IP address per year
2005	0.31	16	19,066
2006	0.81	100	17,231
2007	1.99	100	19,118
2008	2.29	120	22,710
2009	3.57	120	36,190
2010	5.65	120	50,128
2011	4.54	120	40,654
2012	7.78	190	53,085
2013	12.88	210	63,655
2014	25.66	240	115,323
2015	54.51	280	213,523
2016	128.1	300	469,104

3. Statistics

3.1. Statistics obtained from different protocol data

We will discuss the 2016 monitoring results in more detail here. Figure 1 indicates the number of packets detected on a daily basis. Two graphs are shown: one resulting from the TCP (Transmission Control Protocol) data and the other resulting from the UDP (User Datagram Protocol) data. The number of UDP packets had a slightly decreasing trend over the course of the year, although a rapid increase was observed temporarily between July 23 and the first half of August. In contrast, TCP packets had a clear increasing trend over the course of the year. Accordingly, it is obvious that the number of packet detections increased from 2015 to 2016 (Fig. 1) due to increased TCP packets. We then counted daily the number of different IP addresses (hereinafter referred to as “attack source IP addresses”) from which TCP packets were transmitted (Fig. 2). The number of attack source IP addresses spiked at times as illustrated in the figure. There is a possibility that some devices might have been infected with malware due to the influence of switching DHCP (Dynamic Host Configuration Protocol) IP addresses and of the NAT (Network Address Transition) environment. Therefore, the number of attack source IP addresses cannot be simply interpreted as the number of infected devices. However, we are certain that not only the number of packets but also the number of devices scanned had an increasing trend.

3.2. Number of packets detected in relation to different destination port numbers

Next, we will compare the total number of packets detected during 2016 among different destination port numbers (Fig. 3). More than a half of the packets monitored were detected from the destination port 23/TCP. Port 23/TCP uses a protocol called Telnet by default. Hackers exploit Telnet to gain control of a remote host by logging in to it using an ID and password. As media has frequently pointed out these days, Telnet runs on many devices, such as home routers, web cameras and digital video recorders, and these devices are accessible via the Internet using a simple ID and password (e.g., both ID and password are frequently set to “admin” by default) set by the manufacturer. The Mirai malware, which attracted much attention in 2016, and other Telnet-targeting malware search for vulnerable devices by scanning devices that use port 23/TCP. When the malware finds vulnerable devices to attack, it attempts to log in to them by trying various combinations of commonly used IDs and passwords. Once malware successfully logs in to a target device, the hacker can easily gain control of it as the malware uploads and executes itself (For a detailed explanation about the Mirai malware’s behavior, see Reference [1]: the report by the Internet Initiative Japan Inc.). In most devices, port 23/TCP is assigned to Telnet by default, but in some devices, different ports are assigned to Telnet. Relatively small numbers of packet receptions have been detected from port 2323/TCP (Fig. 3) as well as other ports such as 5358/TCP and 6789/TCP (not shown in the figure). However, malware scanning activities have been detected many times from devices in which these types of ports are assigned to Telnet. Accordingly, assigning different port numbers to Telnet will not make the device safe from malware attacks.

Telnet is currently the simplest route for hackers to take control of various devices, and that is why we have detected intensive

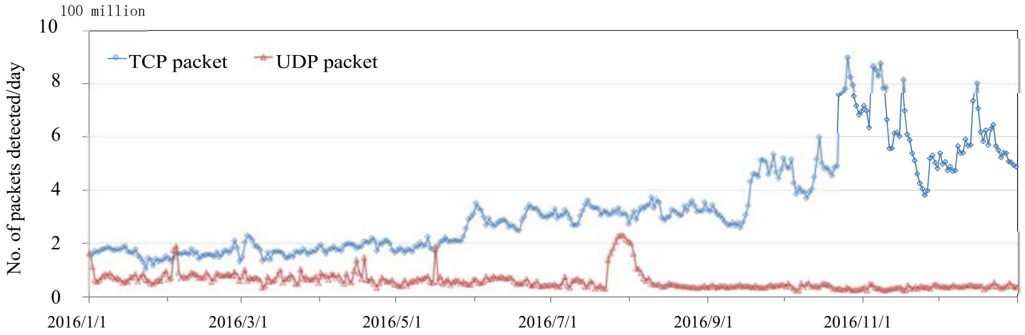

Figure 1. Change in the number of packets detected per day in 2016

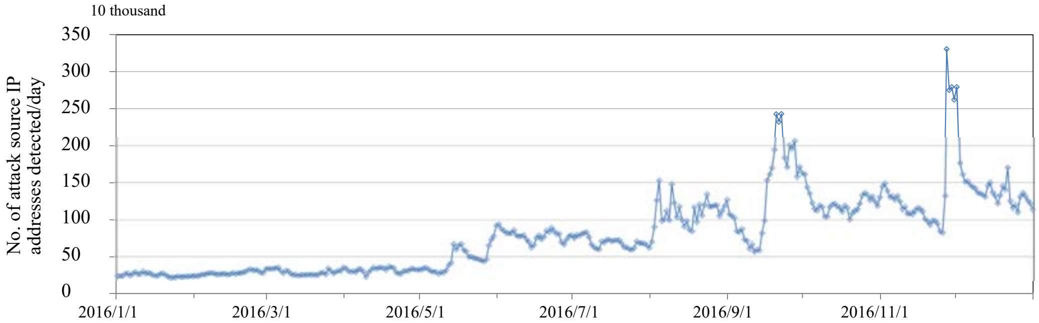

Figure 2. Change in the number of attack source IP addresses detected (TCP)

attacks through this route. However, attacks targeting IoT devices are not limited to the Telnet route. For example, the second largest numbers of packet receptions were detected on port 53413/UDP (Fig. 3). This vulnerability exists in Netis/Netcore-manufactured routers [8]. The number of UDP packet detections increased from mid-July to early August 2016 (Fig. 1) because the number of port 53413/UDP scans increased during that period. In addition, a new type of malware, which tries to log in to devices via SSH (Secure Shell) ports (22/TCP and 2222/TCP) by entering IDs and passwords [5], has been discovered recently. Therefore, merely addressing Telnet issues is insufficient to protect devices from malware attacks.

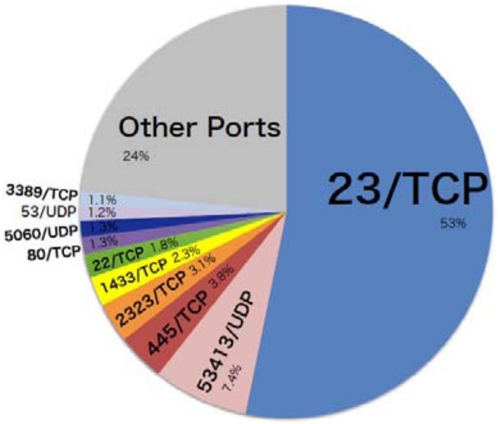

Figure 3. Proportion of packets detected in relation to different destination port numbers in 2016

3.3. Notable cyberattack events

We detected rapid increases in the number of attack source IP addresses in 2016 particularly at the four types of destination ports: 23/TCP, 323/TCP, 5555/TCP and 7547/TCP (Fig. 4). Mirai is known to scan port 2323/TCP, and such scanning activities were monitored from September 6. The number of scans increased rapidly until it peaked on September 20 when about 1.3 million attack source IP addresses were involved. This abrupt increase in attack source IP addresses have been commonly observed when pandemics of new malware break out. It was reported that a massive (620 Gbps) DDoS attack was conducted against the “Krebs on Security” blog site around September 20 using Mirai-infected equipment [2]. Our darknet monitoring also detected the spiked scanning activities on ports 23/TCP and 2323/TCP on the same date. The Mirai source code leaked to GitHub revealed that scanning conducted by the Mirai malware has several notable characteristics: it has a fixed source port number, the sequence

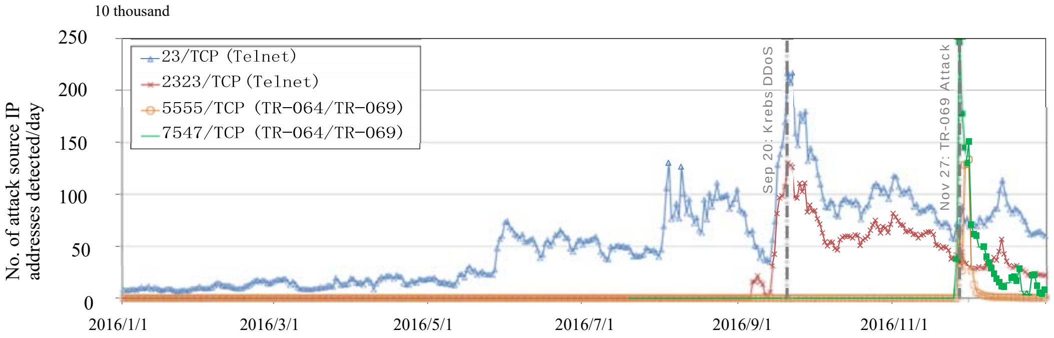

Figure 4. Change in the number of attack source IP addresses detected in 2016 in relation to different types of destination ports. Rapid detection increases are illustrated.

number in the TCP header is identical to the destination IP address, IP headers for different packets have different ID values, and it transmits only one packet to each destination IP address. Our darknet monitoring in fact began to detect scanning activities with these characteristics from September 14, approximately one week before the Mirai outbreak. Another interesting observation was that we began to detect scanning activities with almost the same characteristics (the only difference was that IP headers for different packets had the same ID value) from the beginning of August when the detection of attack source IP addresses rapidly increased. We speculate that Mirai probably first appeared in August and its updated version emerged in September.

On the other hand, attack source IP addresses targeting ports 5555/TCP and 7547/TCP rapidly increased in the second half of November. Port 7547/TCP is used by management protocols for controlling home gateways such as TR-069 and TR-064 as well as devices linked to them. It was reported that when the scanning of this port rapidly increased, a large number of Deutsche Telekom's customer routers in Germany were adversely affected by the spreading malware infection exploiting the vulnerability of TR-069 [6]. In some devices, port 5555/TCP is used in place of port 7547/TCP, which explains similar patterns of increasing and decreasing scanning activities observed between the two port types.

For your reference, we present distribution of attack source IP addresses by country when the number of accesses to port 23/TCP or port 2323/TCP peaked on September 20 and when the number of accesses to port 7547/TCP or 5555/TCP peaked on November 27 (Table 2). Brazil hosted the largest number of attack source IP addresses on both dates while the relative importance of other hosting countries varied greatly between the two dates. It is surprising for us to see Iran and the UK ranked second and third, respectively, on November 27, as it had been rare for them to be ranked high in darknet monitoring. Overall, it appears that attack source IP addresses were more strongly biased toward specific countries on November 27 (when TR-069/TR-064 attacks were most intensive) than September 20 (when Telnet attacks were most intensive). In relation to the massive malware infection which seriously affected Deutsche Telekom's customer routers, it was reported that the malware attack specifically targeted Zyxel’s DSL modems and routers [7, 3]. However, we believe that the difference in the international distribution of attack source IP addresses between the two dates is related to the distribution of vulnerable target devices. Incidentally, we detected only a few cases of IP addresses in Japan responsible for the scanning of ports 7547/TCP and 5555/TCP. Therefore, it is likely that relevant devices in Japan were virtually unaffected by this malware attack incident.

3.4. Status of cyberattacks originating from Japan

Next, we discuss the cases of devices infected with malware where both sources and targets are situated in Japan. Figure 5 shows the daily change in the number of attack source IP addresses in Japan involved in the scanning of port 23/TCP. We detected about 500 to 1,000 such IP addresses on a daily basis. The high peak observed in early December was caused by many scans originating from IP address bands for a Japanese ISP’s (internet service provider’s) mobile network. The peak lasted for about two weeks and no further peak of a similar magnitude was detected after that. People may have different opinions as to whether the detection of 500 to 1,000 attack source IP addresses per day is significant or not. However, considering the fact that several 10,000 to 100,000 such addresses

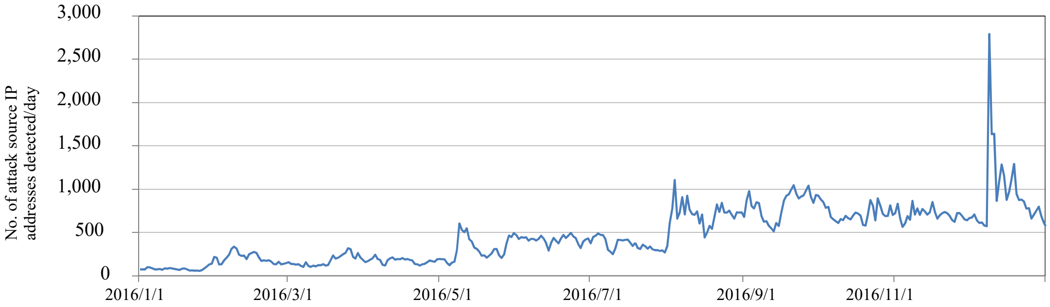

Figure 5. Number of attack source IP addresses in Japan responsible for the scanning of port 23/TCP

are detected daily in many other countries, we think that Japan has relatively low detection frequencies.

As we mentioned earlier, we cannot equate the number of attack source IP addresses detected with the number of devices infected, due to the effect of dynamic IP address assignment implemented by DHCP and because scanning to be conducted by certain malware is timed by C&C (command and control) servers. However, we believe that the number of detections shown in Fig. 5 approximately matches conservative estimates of infected devices. This is because the effect of dynamic IP addresses on the number of attack source IP addresses is eased to some degree by tallying IP addresses daily. Based on this assumption, we estimate that at least about 1,000 devices were infected with malware in 2016.

Table 2. Distribution of attack source IP addresses by country on September 20 and November 27 when the number of accesses to vulnerable devices by these IP addresses peaked

Sep. 20 (23/TCP or 2323/TCP)			Nov. 27 (7547/TCP or 5555/TCP)		
Country	#IPs	Proportion	Country	#IPs	Proportion
Brazil	456,778	21%	Brazil	1,206,589	49%
Vietnam	283,997	13%	Iran	334,510	14%
India	225,457	10%	UK	272,590	11%
China	190,843	9%	Turkey	187,296	8%
Russia	129,979	6%	Chile	84,755	3%
Indonesia	98,752	4%	Italy	83,816	3%
Colombia	82,806	4%	Ireland	53,869	2%
Mexico	49,605	2%	Thailand	40,418	2%
Turkey	44,161	2%	Argentina	34,861	1%
Argentina	43,779	2%	India	32,123	1%
Others	593,654	27%	Others	138,675	6%

4. Measures

In light of radically increased cyberattacks against IoT devices in 2016, it is critical to take security measures that will address two major points: securing the safety of new devices to be installed in the future, and dealing with existing devices that already have been infected with malware. Here, we discuss security-related issues from different perspectives.

4.1. Comprehension of malware infection status and information sharing

First, when many devices have been infected by malware, it is very important to accurately grasp the infection status. Darknet monitoring is an effective technique to grasp the extent of cyberattack activities, but it alone is insufficient. Accordingly, it is necessary to combine this with other monitoring methods. For example, actual malware specimens can be collected and analyzed using honeypot decoy systems, and the Internet should be actively scanned to identify the distribution of devices that are susceptible to malware attacks. Combined techniques will allow continuous and comprehensive information gathering. It is also vital for relevant organizations to share information they collect so proper measures, such as updating vulnerable devices, can be implemented.

4.2. Measures by manufacturers and installers

The key measure to protect new devices to be installed in the future is to set the devices inaccessible from the Internet during the manufacturing processes. We believe that users rarely need to access their web cameras or routers via the Internet. Given that most malware attacks detected recently began by malware trying to log in to Telnet, setting devices inaccessible from the Internet by default will greatly reduce the risk of attacks. If users need to remotely log in to their devices, it is desirable for them to use public key authentication with SSH, when possible, or at least make devices accessible only from appropriate IP addresses.

There had been cases where authorized installers set devices accessible via the Internet, against the intention of manufacturers. In principle, it is desirable for manufacturers to take proper protective measures, but in reality, many existing devices are not set to be properly secure, and manufacturers and installers often implement inconsistent device settings. Taking account of these issues, it is vital for authorized installers to recognize the risk of malware attacks and set devices appropriately with caution.

4.3. Confirmation and measures by users

It is also desirable for users of devices to grasp the environment in which their devices are installed, from the perspective that they need to protect their own devices. It would be good practice for users to confirm whether their devices are accessible via the Internet, whether the vulnerability of their devices is publicly known, whether patches are available to correct issues with their devices, and whether firmware is updated.

4.4. Operation and management of installed devices

Unlike operation and management practices established for personal computers and servers, those for IoT devices, after they are installed, have not yet been adequately established. While it is preferable for users to be able to manage their devices properly, many users do not have sufficient computer knowledge to do so. Therefore, it may be impractical for users to be fully responsible concerning all aspects of device management and operation such as device updates. Instead, it may be necessary to introduce automatic device updating mechanisms, just like PCs today are updated automatically, which do not require close attention by users. It is also important to address various device issues. For example, some very low-priced devices do not allow firmware updates after purchasing.

5. Conclusion

In this report, we presented the status of cyberattack activities monitored throughout 2016 under the framework of the darknet monitoring project being implemented by the Cybersecurity Laboratory at NICT. The outbreak of the Mirai malware and its intensive attacks against IoT devices were the highlight of our 2016 monitoring efforts. It has been reported that the Conficker worm was detected accessing more than 1 million IP addresses globally per day, even though six years have passed since its large-scale outbreak in 2008 [4]. We anticipate that infection and attacks of various IoT devices by malware will continue to be a major issue in 2017, and therefore, we plan to continue our effort in monitoring and analyzing malware activities.

References

[1] Internet Infrastructure Review (IIR) Vol.33. http://www.iij.ad.jp/company/development/report/iir/033/01_04.html, 2016.

[2] KrebsOnSecurity Hit With Record DDoS. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, 2016.

[3] New Mirai Worm Knocks 900K Germans Offline. https://krebsonsecurity.com/2016/11/ new-mirai-worm-knocks-900k-germans-offline/, 2016.

[4] M. Asghari, Hadi Ciere and M. van Eeten. Post-mortem of a zombie: Conficker cleanup after six years. 24th USENIX Security Symposium (USENIX Security 15), 2015.

[5] M. Malik and P. Kálnai. New Linux/Rakos threat: devices and servers under SSH scan (again). http://www.welivesecurity.com/2016/12/20/new-linuxrakos-threat-devices-servers-ssh-scan/l, 2016.

[6] P. Paganini. More than 900k routers of Deutsche Telekom German users went offline. http://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html, 2016.

[7] J. B. Ullrich. TR-069 NewNTPServer Exploits: What we know so far. https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/, 2016.

[8] T. Yeh. Netis routers leave wide open backdoor. http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/, 2014.