NSFOCUS

An Anatomy of WS-Discovery Reflection Attacks

NSFOCUS Security Labs

CONTENTS

Executive Summary

The Web Services Dynamic Discovery protocol (WS-Discovery or WSD) is becoming an eye catcher because of its potential of being exploited for distributed denial-of-service (DDoS) reflection attacks. This article starts with a brief introduction of WSD and then analyzes related reflection attacks from the aspects of WSD's exposure on the Internet and the related threats captured by our honeypots.

We have the following brief findings:

- Since being disclosed by Baidu security researchers in February 2019, WSD reflection attacks had steadily grown in numbers, especially in the second half of the year.
- Since mid-August, WSD reflection attacks captured by our honeypots have been on the rise. In September we saw a sharp increase in such attacks. All parties concerned, including security vendors, service providers, and telecom operators, should pay due attention to this type of threats.
- Around the world about 910,000 IP addresses (80% of which (730,000) were video surveillance devices) runs the WSD service and were thus at risk of being exploited to launch DDoS attacks.
- The top 5 countries with the most devices that had the WSD service enabled were China, Vietnam, Brazil, the USA, and South Korea. Among these five countries, Vietnam had the most video surveillance devices that have the WSD service publicly available.
- Close to 24% of the devices did not respond to WSD response packets with port 3702, which poses a new challenge to DDoS protection.
- When conducting a WSD reflection attack, the attacker does not ussually use legitimate service discovery packets as attack payloads, but attempts to craft a very short payloads to their target. Most attack payloads contain only three bytes, registered in two-thirds of attack log messages.
- During a network-wide probe of three-bytes attack payload, we found that not all WSD services responded to them and the number of IP addresses that did respond was approximately 30,000. The top 3 countries hosted with active responding devices were USA, South Korea, and China. A majority of such devices were video surveillance devices and printers. The average bandwidth amplification factor (BAF) achieved by such payloads was 443.
- 92% of attack incidents where threat actors attacked only one port of the target IP address. In average we saw 3% of incidents where attackers attacked over 1000 ports of the target IP address.

This would saturate the internet bandwidth of the target IP address, causing forwarding devices to randomly drop excess packets.

- When conducting a DDoS attack, the malicious actor may also attack the same network segment of the target IP address, which would also consume the internet bandwidth of the target IP address. In such cases, the victim does not know they were under attack.
- According to our honeypot data, China was the top target of the WSD reflection attacks, home to 33% of victim IP addresses, followed by the USA at 21%.

1 Introduction to WSD

WSD is a multicast discovery protocol to locate services on a local area network (LAN). However, due to device vendor's design flaw in the implementation, when a legitimate IP address sends a service discovery packet, devices would respond to the request. When exposed on the Internet, these devices could potentially be exploited for DDoS reflection attacks. In February 2019, security researchers from Baidu[1] published an article about WSD reflection attacks[1]. This was the first report we learned about such attacks. In a post[2], ZDNet mentioned that WSD reflection attacks were first reported in May, and in August, many organizations began to use this protocol to launch DDoS attacks. According to Akamai[3], one of their customers in the gaming industry suffered a WSD reflection attack with an incoming traffic peak at 35 Gbps.

The WSD protocol was approved as a standard by the Organization for the Advancement of Structured Information Standards (OASIS) with its latest version at V1.1 released in July 2009. It listens over port 3702 for device discovery and uses IPv4 multicast address 239.255.255.250 or IPv6 multicast address FF02::C. Messages were transferred using SOAP over UDP.

Currently, the ONVIF specification[4] for video surveillance devices specifies WSD as the service discovery protocol, and some printers[5] also have the WSD service publicly accessible.

The following is an example of responses returned by devices at the device discovery stage. Key fields in this response will be explained later.

```
<?xml version="1.0" encoding="UTF-8"?><root xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:wsa="http://
schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsd="http://schemas.xmlsoap.org/ws/2005/04/discovery"
xmlns:dn="http://www.onvif.org/ver10/network/wsdl" xmlns:tds="http://www.onvif.org/ver10/device/wsdl">
    <Header>
        <Action>http://schemas.xmlsoap.org/ws/2005/04/discovery/ProbeMatches</Action>
        <MessageID>uuid:00001111-0011-0011-0011-000000111111</MessageID>
        <RelatesTo>11110000-1100-1100-1100-111111000000</RelatesTo>
        <To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</To>
        <AppSequence InstanceId="1559751701" MessageNumber="87"></AppSequence>
    </Header>
```

1 The article revolves around ONVIF-based reflection attacks. Our analysis shows printers aside from ONVIF devices, were probably involved too. The Open Network Video Interface Forum (ONVIF) communicates based on WSD at the device discovery stage. In terms of reflection attacks, ONVIF devices are not the only targets. Although this article does not mention WSD reflection attacks, we do take it as the first report on these attacks.

```
<Body>
    <ProbeMatches>
        <ProbeMatch>
            <EndpointReference>
                <Address>urn:uuid:11111111-1111-1111-1111-111111111111</Address>
            </EndpointReference>
            <Types>dn:NetworkVideoTransmitter tds:Device</Types>
            <Scopes>onvif://www.onvif.org/type/video_encoder onvif://www.onvif.org/type/ptz onvif://www.onvif.org/type/audio_encoder onvif://www.onvif.org/hardware/HDS-7204TVI-BX%2FN onvif://www.onvif.org/Profile/Streaming onvif://www.onvif.org/Profile/G onvif://www.onvif.org/name/Embedded%20Net%20DVR onvif://www.onvif.org/type/Network%20Video%20Storage</Scopes>
            <XAddrs>http://192.168.1.254:89/onvif/device_service</XAddrs>
            <MetadataVersion>10</MetadataVersion>
        </ProbeMatch>
    </ProbeMatches>
</Body>
</root>
```

- **MessageID:** a randomly generated string of numbers to identify the message. In the process of communication, the message ID in the request packet appears in the RelatesTo field of the response packet.
- **Address:** unique ID of the device.
- **Types:** indicates the type of the target service. The value of this field must be the same as that of the Types field in the request packet; otherwise, the server would not return any information. This field can, to some extent, indicate the type of the device. For example, the value of NetworkVideoTransmitter indicates a video surveillance device, PrintDeviceType a printer, and Computer a computer (Windows system).
- **Scopes:** indicates characteristics of a device. For example, Profile indicates the profile supported by the device; Location indicates the location of the device vendor; Hardware indicates the hardware model of the device; Name indicates the retrievable name of the device.
- **XAddrs:** indicates the point of entry of the web service.
  For more information, refer to *Web Services Dynamic Discovery (WS-Discovery)*[6].

2 Exposure of the WSD Service

To accurately analyze WSD reflection attacks, we learned the WSD service exposed on the Internet, and at the same time created WSD honeypot and deployed them in our honeynet system. Data obtained using the two methods were analyzed respectively in chapters 2 and 3.

Unless otherwise indicated, all data provided in this chapter was obtained from a single-round global survey conducted in July 2019.

Around the world, about 910,000 IP addresses (80% of which (730,000) were video surveillance devices) runs the WSD service and were thus at risk of being exploited to launch DDoS attacks.

We analyzed the **Types** field in the banner of the WSD service and found that, aside from video surveillance devices (dn:NetworkVideoTransmitter), other devices such as network attached storages (NASs[2]) and printers (wprt:PrintDeviceType) uses WSD.

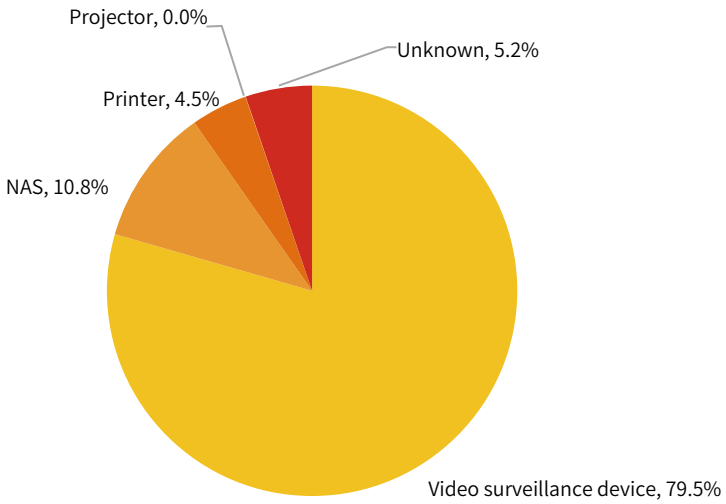

Figure 2.1 Distribution of device types with the WSD service enabled

The top 5 countries with the most devices that runs the WSD service enabled were China, Vietnam, Brazil, the USA, and South Korea. Among these five countries, Vietnam had the most video surveillance devices that had the WSD service publicly available.

2 The Types field in the banner does not expressly indicate the NAS device type, but through analysis, we believe that most banners sharing the same value of a certain type indicate the device type as NAS.

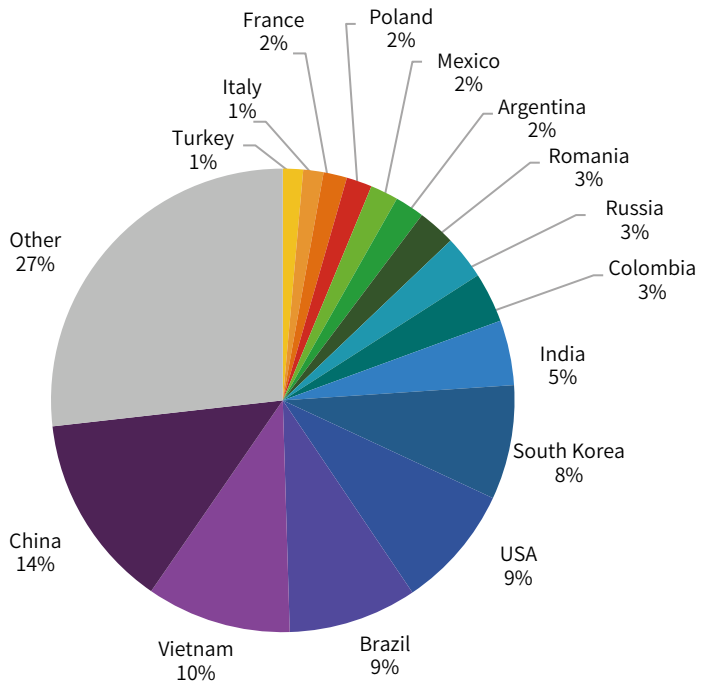

Figure 2.2 Global distribution of WSD devices

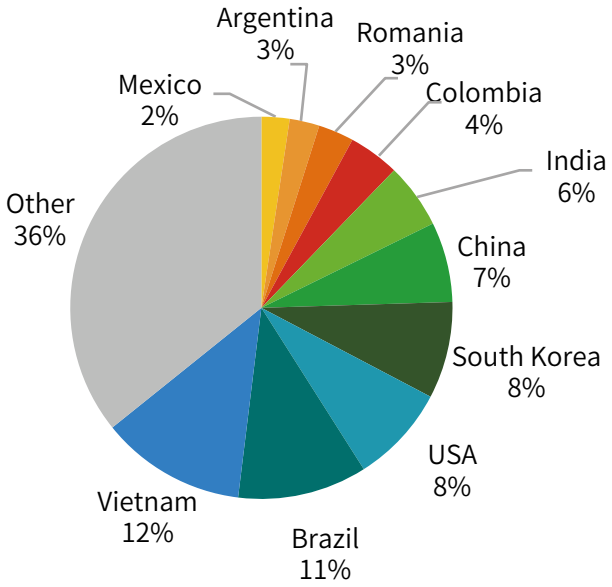

Figure 2.3 Global distribution of WSD devices (video surveillance devices)

Close to 24% of devices did not respond to WSD request packets with port 3702, which poses a new challenge to DDoS protection.

This data comes from A10 Networks's WSD security research report[7], which mentions that about 46% of devices responded with random ports. What we did was verifying such findings. According to our data, close to 24% of devices did not respond to WSD request packets with port 3702. We also found that not all of these ports were random (see Figure 2.4) and some of them, such as ports 2050 and 1024, were repeatedly used (see Figure 2.5). This can be found in video surveillance devices, NAS, and printers. Projectors has a rather small percentage and can be ignored. If a DDoS protection policy blocks only port 3702, it is impossible to completely block WSD reflection attacks.

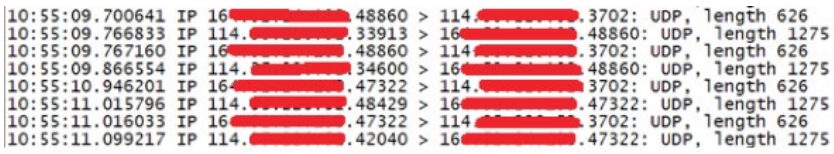

Figure 2.4 Example of random ports used as the source port of response packets

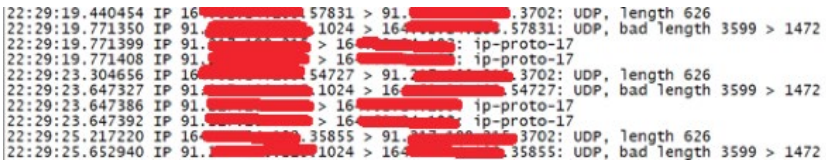

Figure 2.5 Example of other ports than port 3702 repeatedly used as the source port of response packets

Table 2.1 Source ports of response packets from WSD devices (incomplete, sorted by the number of occurrences)

Port Number	Number of Occurrences
2050	772
1024	298
1900	252
2051	123
1025	53
3703	34
32769	27
36870	22
57115	21
47302	21
…	…

Table 2.2 Proportions of devices of various types that did not respond with port 3702

Device Type	Proportion of Devices Not Responding with Port 3702
Video surveillance device	27.3%
NAS	13.7%
Printer	11.2%
Projector	1.0%

During the process of our investigation, we mined statistical data from different sources with the exposure of the WSD service, which may vary a bit from one another. zeroBS's[8] research report[2] published on ZDNet provides the number of 630,000 based on data collected from the cyberspace search engine BinaryEdge[9]. From the screenshots in our report, we find that such number covers only devices responding with port 3702. Our number were close, standing at 690,000. A10 Networks's[7] number is 850,000, not varying much from our number (total 910,000 devices using the WSD service).

We were puzzled with data from Shodan[10], which indicates that only 170,000 devices responded with port 3702. It turns out that Shodan probes only ONVIF devices, omitting devices such as printers and computers. Besides, it eliminated data of response packets with multiple source ports other than 3702 alone. With the same filtering condition, our number still stands at 530,000 which is much greater than the number provided by Shodan.

3 Analysis of WSD Reflection Attacks

From data captured by our WSD honeypots deployed worldwide, we were able to learn the current threat landscape of WSD reflection attacks. Our data are based on log messages generated over a 74-day period from July 10 to September 21, 2019. The following sections analyze these log messages from the aspects of the attack method, attack incidents, and victims.

3.1 Attack Method

The attack method is analyzed among the attack payload length, the number of source ports revealed in attack traffic, and the network segments where victim IP addresses belong.

When executing a WSD reflection attack, the attacker does not usually use legitimate service discovery packets as attack payloads but attempts to craft very short payloads to attack the target. Most attack payloads contain only three bytes, accounting for two-thirds of the total attack traffic.

We analyzed the payload revealed in WSD reflection attack log messages. In order to prevent such attacks, we do not provide specific contents of attack packets and name payloads with their respective lengths. According to our statistics, the top 5 payloads in total represented over 99% of all attack traffic. We also found that none of these five types of payloads were legitimate service discovery packets and the smallest contained only two bytes. Most attack payloads contained three bytes, accounting for two-thirds of the total attack packets. ZDNet mentioned payload3 in an article[2] and claimed that a proof-of-concept script for launching WSD-based attacks were published on GitHub[3] in late 2018. It is possible that attackers gained knowledge from the script on GitHub and executed such reflection attacks.

3 In order not to make the attack payload known to malicious actors, no link to the article on GitHub is provided here.

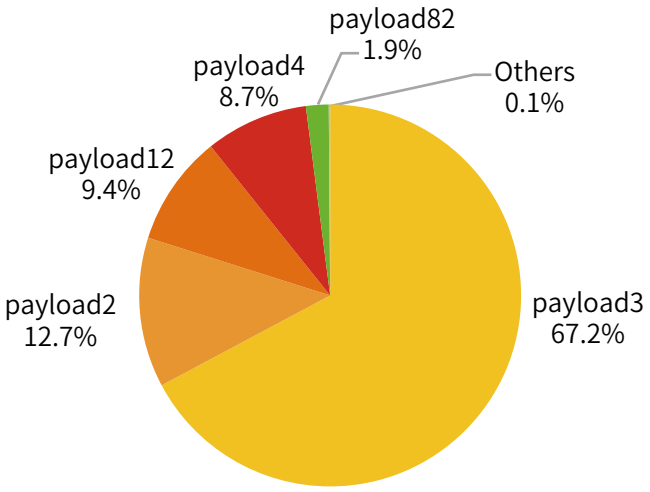

Figure 3.1 Proportions of WSD reflection attack payloads of various lengths captured by honeypots

A network-wide probe of payload3 packets revealed that not all WSD services responded to them. In total there were 28,918 IP addresses responding to these requests.

The top 3 countries with active devices responding to payload3 were the USA, South Korea, and China (see Figure 3.2). In terms of device types, video surveillance devices and printers dominated, with the former accounting for 75% of the total devices.

Response packets captured by honeypots varied from hundreds to thousands of bytes in length, averaging out at 1330 bytes. Thus, the average bandwidth amplification factor (BAF)[4][11] stood at 443. A single device with 10 Mbps bandwidth is possible to generate a reflection attack of up to 282 Gbps.

4 The amplification factor here follows the definition of BAF given in *Amplification Hell: Revisiting Network Protocols for DDoS Abuse* in NDSS 2014 and does not consider UDP packet headers.

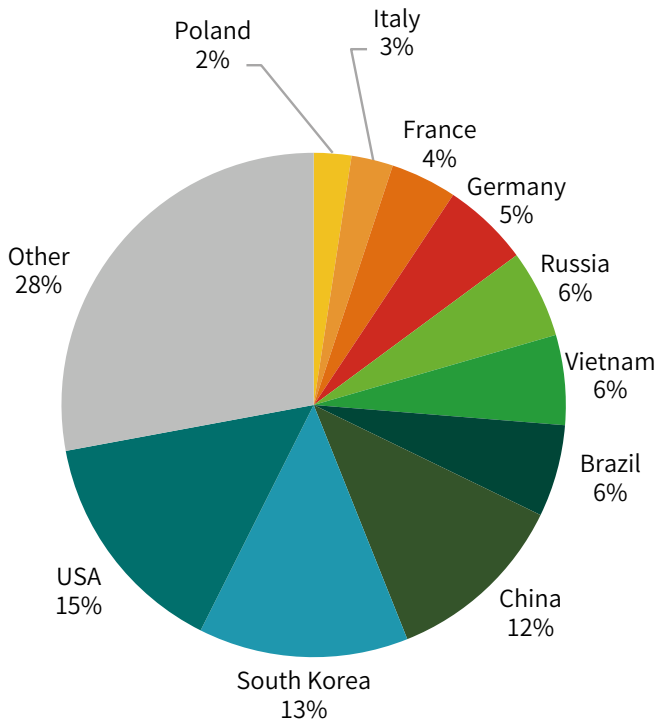

Figure 3.2 Global distribution of devices responding to payload3

92% of attack incidents where threat actors attacked only one port of the target IP address. In average we saw 3% of incidents where attackers attacked over 1000 ports of the target IP address. This would saturate the internet bandwidth of the target IP address, causing forwarding devices to randomly drop excess packets.

The number of ports attacked varied with specific attacks, as shown in Figure 3.3. In a reflection attack, malicious actors tend to attack only one port of the target IP address, such as port 53 (DNS) or port 80 (HTTP). Among 3% of attacks where over 1000 ports of the target IP address received reflection attack packets. Even if the target port were not publicly accessible, such attacks would consume the internet bandwidth of the victim IP address, causing forwarding devices to randomly drop excess packets. This would to some extent, affect the quality of service provided by the victim IP address.

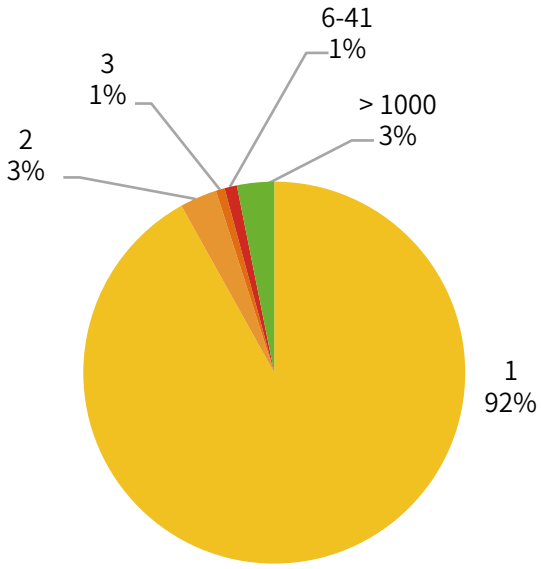

Figure 3.3 Distribution of reflection attacks by the number of attacked ports

When conducting a DDoS attack, the malicious actor may also attack the same network segment of the target IP address, which would also consume the internet bandwidth of the target IP address. In such cases, the victim does not know they were under attack.

When sorting out victim IP addresses, we found that some belongs to the same network segments. According to our data, only few IP addresses (about 2-6 of them) were in the same network segment over the same period. We randomly selected some IP addresses for analysis, in an attempt to check whether they belong to the same domain or were associated. Result shows that these IP addresses had no connection with one another, and we deem it necessary to mention this. Even if a customer has an active DDoS protection service, if any of their network segments come under such attack, their internet bandwidth will still be impacted. In such cases, they are likely to be unaware of the under attack, hence compromising service availability of their business.

3.2 Attack Incidents

We analyzed attack incidents recorded in WSD attack log data of our honeynet system. About one IP address in a day add up to an attack incident[5]. Figure 3.4 shows the daily number of attack incidents. At a glance, WSD reflection attack incidents fluctuated all the time, but have been on the rise generally

5 Our definition of attack incidents may not be very precise, however is sufficient to make our point.

since mid-August, especially in September. This indicates that WSD reflection attacks have been gradually adopted as a regular weapon of DDoS attacks, to which all parties concerned, including security vendors, service providers, and telecom operators, should pay due attention.

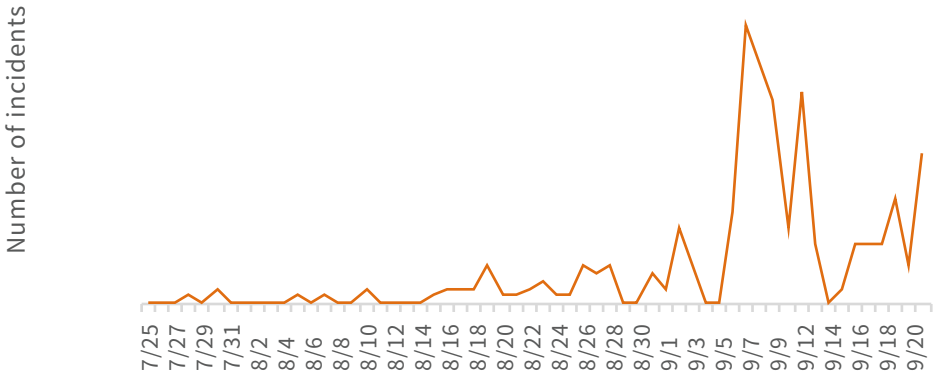

Figure 3.4 Daily number of WSD reflection attacks

In terms of the attack duration, most attack incidents lasted 5 minutes to half an hour. Specifically, 38.4% of attacks lasted 5 to 10 minutes, 33.6% lasted 10 to 30 minutes, and only 0.3% lasted over 12 hours, with the longest one standing at 50 hours. The maximum number of packets received by individual honeypots reached 24 million.

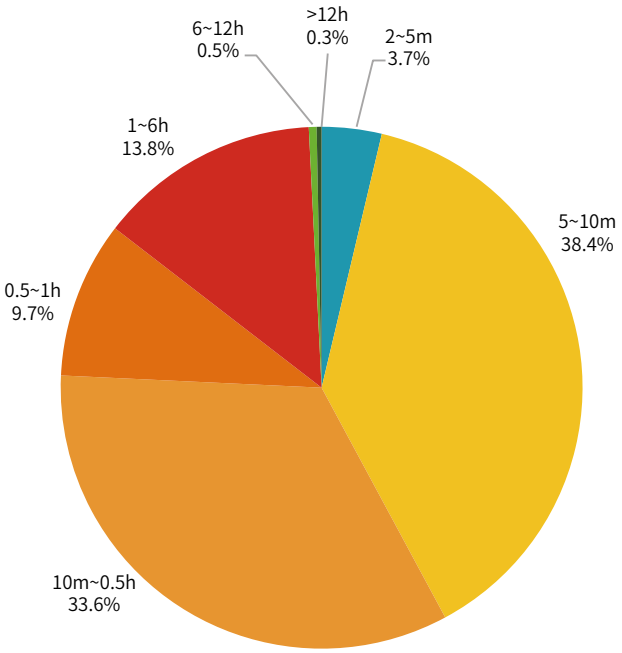

Figure 3.5 Distribution of WSD reflection attacks by duration

3.3 Victims

Figure 3.6 shows the global distribution of victim IP addresses of WSD reflection attacks. In total there were 24 countries and regions suffered such attacks. China was the top target of WSD reflection attacks, home to 33% of victim IP addresses, followed by the USA at 21%.

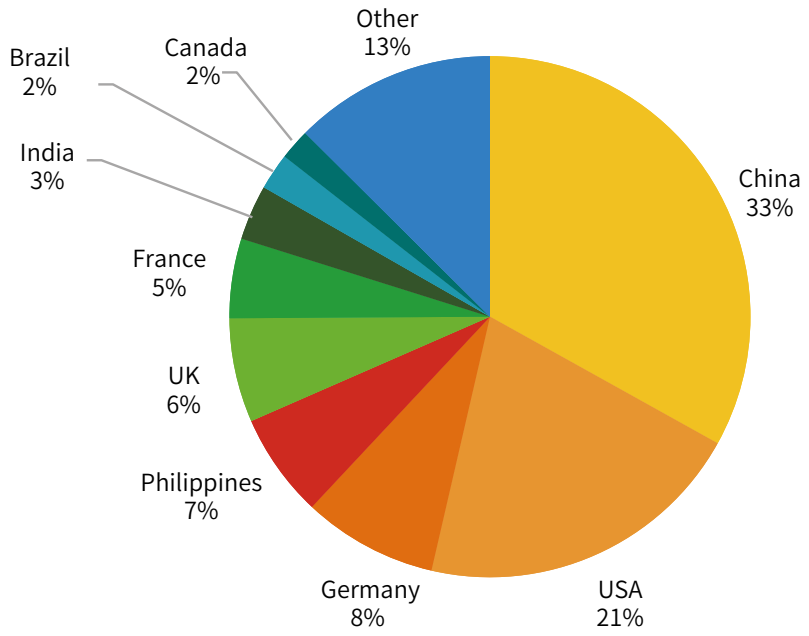

Figure 3.6 Global distribution of WSD reflection attack victims

4 Summary

This article began with a brief introduction of WSD and then analyzes related reflection attacks from the aspects of WSD's exposure on the Internet and the related threats captured by our honeypots. WSD as a new reflection vector, has great potentials for attackers. With the growth of more ONVIF devices, the exposure of the WSD service being publicly accessible will cause more threats to the internet. When the WSD reflection attacks becomes an imminent threat, all parties concerned should be actively involved. Only in doing so, can WSD security be improved.

Security vendors are advised to:

1. Add the WSD scanning capability in scanning products to promptly discover security risk in customers' networks.
2. Add the WSD traffic detection capability in protection products to promptly discover security threats in customers' networks. As devices may respond to WSD request packets with other ports than port 3702, to counter a WSD reflection attack, it is necessary to detect packet signatures[6] besides configuring a traffic control policy to block the source port. Associating with Threat Intelligence[7] for IP address that uses the WSD service is recommended. This way, packets with matching source IP addresses can be blocked effectively.

Device vendors should design their products in a way to **check whether WSD request packets are from multicast source IP addresses and, if not, ignore such packets.** This way, WSD reflection and SSDP reflection attacks can be prevented.

Telecom operators should address DDoS attacks in their own networks.

Watchdogs are advised to:

1. Monitor WSD-related threats in networks and make them known to the public once discovered.
2. Promote security assessment of the WSD functionality in devices and forbid devices not up to the standard to be sold in the market.

6 WSD reflection attack packets have identifiable signatures. Those interested can contact us for more information.

7 Currently, NSFOCUS Threat Intelligence center (NTI) is capable of providing such threat intelligence. Those interested in such intelligence can contact NTI at nti@nsfocus.com.

Device users are advised to:

1. Disable the WSD functionality when necessary.
2. Restrict WSD-enabled devices within internal networks to maximize the difficulty of exploiting these devices.
3. If WSD-enabled devices have to be deployed on the Internet, deploy routers (NAT functionality required) or security devices (such as firewalls) to limit external access to such devices.

Customers are advised to subscribe or purchase DDoS protection service from security vendors that are capable of defending against WSD reflection attacks. If existing products support customization of application-layer signatures, it is advisable to add signature-based rules.

References

[1] ONVIF-based IoT devices used to launch DDoS reflection attacks, https://www.freebuf.com/articles/system/196186.html, 2019/9/24

[2] Protocol used by 630,000 devices can be abused for devastating DDoS attacks, https://www.zdnet.com/article/protocol-used-by-630000-devices-can-be-abused-for-devastating-ddos-attacks/, 2019/9/24

[3] NEW DDOS VECTOR OBSERVED IN THE WILD: WSD ATTACKS HITTING 35/GBPS, https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html, 2019/9/24

[4] ONVIF Application Programmer’ s Guide, https://www.onvif.org/wp-content/uploads/2016/12/ONVIF_WG-APG-Application_Programmers_Guide-1.pdf, 2019/9/19

[5] HP Web Jetadmin – Ports, https://support.hp.com/lv-en/document/c05996543, 2019/9/19

[6] Web Services Dynamic Discovery (WSDiscovery), http://specs.xmlsoap.org/ws/2005/04/discovery/ws-discovery.pdf, 2019/9/19

[7] WS-DISCOVERY AMPLIFICATION ATTACK, https://downloads-a10networks.s3-us-west-2.amazonaws.com/collateral/A10-MS-23239-EN.pdf, 2019/9/19

[8] New DDoS Attack-Vector via WS-Discovery/SOAPoverUDP, Port 3702, https://zero.bs/new-ddos-attack-vector-via-ws-discoverysoapoverudp-port-3702.html, 2019/9/19

[9] BinaryEdge, https://www.binaryedge.io/, 2019/9/19

[10] Shodan, https://www.shodan.io/search?query=port%3A3702, 2019/9/19

[11] Amplification Hell: Revisiting Network Protocols for DDoS Abuse, https://www.ndss-symposium.org/ndss2014/programme/amplification-hell-revisiting-network-protocols-ddos-abuse/, 2019/9/19

NSFOCUS

An Anatomy of WS-Discovery Reflection Attacks

WWW.NSFOCUSGLOBAL.COM