WS-DISCOVERY AMPLIFICATION ATTACK

WS-Discovery amplification is one of an ever-growing-array of weapons that attackers use to create very large DDoS attacks. This paper talks about it from a DDoS defender’s perspective and provides some recommendations to mitigate the threat.

EXECUTIVE SUMMARY

The Web Services Discovery or WS-Discovery is a UDP-based protocol that allows an attacker to spoof request with the victims IP that causes a reflected and amplified response toward the victim’s infrastructure or service. In this advisory, we will provide a brief overview from the perspective of a DDoS defender and offer advice for protection.

Summary of WS-Discovery research findings:

- There are >800k potential WS-Discovery amplification sources
- Nearly 50 percent of the hosts respond with random high UDP ports
- Observed amplification factor of up to 95 times
- IoT devices account for a significant portion of the exploitable hosts
OVERVIEW

The WS-Discovery protocol uses TCP and UDP ports 3702 to respond to a multicast address that gives information on services provided in the local network. In some cases, the response provides the requester quite a bit of data about these services (see below).

```xml
<)?xml version="1.0" encoding="UTF-8">
<soap:Envelope
 xmlns:soap="http://schemas.xmlsoap.org/2003/05/soap-envelope"
 xmlns:ws="http://schemas.xmlsoap.org/2003/05/soap-encoding"
 xmlns:class="http://schemas.xmlsoap.org/wss/2005/04/discovery"
 xmlns:wsns="http://schemas.xmlsoap.org/ws/2005/04/addressing"
 xmlns:wsdl="http://www.onvif.org/ver10/network/wsdl"
 xmlns:soap:encoding="http://www.onvif.org/ver10/device/wsdl">
  <soap:Header>
    <wsns:MessageID uid="471110ba3-b778-4e31-9744-893e9f29be02"/>
    <wsns:To>/wsns:soap-encoding/</wsns:To>
    <wsns:RelatesTo>urn:uuid:ce494a9a-5d56-4236-9146-1a2b24e1115</wsns:RelatesTo>
  </soap:Header>
  <soap:Body>
    <wsns:ProbeMatches>
      <wsns:ProbeMatch>
        <wsns:EndpointReference>
          <wsns:Address>urn:uuid:08f3e118-3b86-4b64-aaca-886b335d8dd/</wsns:Address>
        </wsns:EndpointReference>
      </wsns:ProbeMatch>
    </wsns:ProbeMatches>
  </soap:Body>
</soap:Envelope>
```
If the number of services is large enough, the responses come in many full-sized packets with trailing UDP fragments.

To the left is a packet capture of a WS-Discovery amplification attack filtered to the output of one node.

Notice a one-packet request was replied to with nearly 40 full-sized and fragmented packets. Each blue line shows a complete UDP packet with each trailing fragment shown in white.

---

### Packet Lengths

<table>
<thead>
<tr>
<th>Topic/Item</th>
<th>Count</th>
<th>Average</th>
<th>Min val</th>
<th>Max val</th>
<th>Rate (ms)</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-19</td>
<td>0</td>
<td>979.333</td>
<td>60</td>
<td>1514</td>
<td>0.0007</td>
<td>100.00%</td>
</tr>
<tr>
<td>20-39</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0.0000</td>
<td>0.00%</td>
</tr>
<tr>
<td>40-79</td>
<td>1467</td>
<td>68.166</td>
<td>60</td>
<td>79</td>
<td>0.0045</td>
<td>7.33%</td>
</tr>
<tr>
<td>80-159</td>
<td>3891</td>
<td>94.10</td>
<td>80</td>
<td>159</td>
<td>0.0118</td>
<td>19.45%</td>
</tr>
<tr>
<td>160-319</td>
<td>869</td>
<td>204.654</td>
<td>160</td>
<td>317</td>
<td>0.0026</td>
<td>4.29%</td>
</tr>
<tr>
<td>320-639</td>
<td>274</td>
<td>467.30</td>
<td>322</td>
<td>621</td>
<td>0.0008</td>
<td>1.37%</td>
</tr>
<tr>
<td>640-1279</td>
<td>2707</td>
<td>1166.02</td>
<td>640</td>
<td>1279</td>
<td>0.0082</td>
<td>13.54%</td>
</tr>
</tbody>
</table>

| 1280-2559  | 10802 | 1449.75 | 1280    | 1514    | 0.0328    | 54.01%  |
| 2560-5119  | 0     | -       | -       | -       | 0.0000    | 0.00%   |
| 5120 and greater | 0 | - | - | - | 0.0000 | 0.00% |

Over half of all packets in this attack are between 1,280 and 1,514 bytes.

The rest of the attack is made up of various sizes of UDP fragments.
As with any protocol, not all implementations are alike. As such, there is a difference in behavior between the above node and the single node to the left.

Even though the scan packet was destined to UDP 3702, the node replies back from an ephemeral UDP port.

Recent scans performed by A10 Networks Research have yielded as many as 850k sources that respond to WS-Directory requests with a properly formatted Web Services response.

Some targets responded with UDP source port 3702 but slightly less than half of targets responded from the ephemeral range.

Since the source port is not deterministic, this makes blocking based on UDP port less effective.
OVERALL SCOPE

We decided to get a full understanding of the size and overall scope of this weapon by compiling its geo-location and the organization ID of the owner of the source IP as gleaned through BGP. Then, we dug a bit deeper to understand the stated equipment and location by the devices themselves through the WS-Discovery reply.

GEOGRAPHIC BREAKDOWN

The top-five locations are a bit too close to call as Vietnam, Brazil, U.S., Korea, and China all come within two percentage points of each other. Interestingly, the location string stated within the Web Services response itself is overwhelmingly China, which shows the location that the offending device was manufactured.

BREAKDOWN BY BGP ORGANIZATION ID

The top-five organizations, however, have a similar, but not the same, breakdown as their geographies. Here, Korea Telecom, Chinanet, VNPT Corp, Viettel, and Telefonica Brazil take the top honors, while U.S. carriers are diffused across many smaller ASNs.
**IMPORTANT FACTS ABOUT WSD**

1. WS-Discovery functions like SSDP are service discovery protocols. The WS-Discovery specification came much later in 2009 and the responses are in SOAP unlike the case of SSDP, which would give a HTTP like response.

2. 15 percent of the hosts that are potential WS-Discovery amplifiers respond to SSDP, as well. This means that the devices in the network use multiple service discovery protocols.

3. 160,000 devices, 60 percent of which are IP cameras and DVRs, are exposed to the internet because of the WS-Discovery protocol. This makes them susceptible to being hijacked to become botnets.

4. Here is a list of the top-three manufacturers of the IP cameras and DVRs along with their numbers:

<table>
<thead>
<tr>
<th>MANUFACTURER</th>
<th>NUMBER OF DEVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dahua</td>
<td>112K</td>
</tr>
<tr>
<td>IntelBras</td>
<td>42K</td>
</tr>
<tr>
<td>Hikvision</td>
<td>31K</td>
</tr>
</tbody>
</table>

5. The fact that Dahua and Hikvision are on top of the list is supported by the fact that 99 percent of these devices have a ONVIF geo-location of China.

6. The IP geo-location distribution graph shows that Brazil houses 15 percent of these WS-Discovery sources, which is backed by the fact that IntelBras is number-two on the list of top manufacturers of the hardware.

**PROTECTING YOURSELF FROM THE THREAT**

Here we will outline various ways that organizations can to protect themselves from these attacks, along their strengths and weaknesses.

**BLOCKING AT LAYER 4 ONLY (THE ACCESS LIST OR FLOWSPEC METHOD)**

Unlike many amplification protocols such as DNS and NTP, which send attack packets on deterministic source ports (UDP 53 and 123 respectively), WS-Discovery attack packets happen over a combination of UDP 3702 and the ephemeral range of UDP ports. Using the ephemeral range is non-deterministic in nature and blocking it will create too much collateral damage for any service that is being protected, those that are real UDP requests. As such, blocking this particular attack at Layer 4 only cannot be done.

**BLOCKING UDP FRAGMENTS AT ATTACK TIME**

Because UDP fragments (any packet with the MF bit set or a fragment offset not equal to 0) make up a large portion of this type of attack, one strategy that could be undertaken is blocking all UDP fragments at attack time. This would be an effective method to reduce the attack by a large amount but becomes problematic with all of the valid UDP fragmentation that occurs in the network or streaming in from the internet. Depending on the service being offered or the way the network uses DNS, this approach could be a problem and should be avoided due to unpredictable bad behavior. If low collateral damage is the goal, then this method should be avoided.
BLACKLISTING DURING THE ATTACK

Although the attack starts with spoofing the victim’s IP address, each of these amplification sources are real IP addresses and not spoofed. As such, there is a finite number of these systems that could be attacking the service at any point in time. As discussed above, A10 Networks Research maintains an up-to-date list of WS-Discovery-enabled systems (over 800k at this writing) and can provide this as a means to block these systems. As with any scan-based data set, however, the number received depends highly on external factors including the time of day, provider changes in DHCP leases and so on. To make up for this, we also recommend that the next method should be used in conjunction.

A10 NETWORKS ZERO-DAY AUTOMATED PATTERN RECOGNITION (ZAPR)

A10 Networks created this functionality for this exact problem. As attack patterns tend to be ephemeral, any amount of up-front preparation will still have cracks and some of the attack will leak through. To ensure that this is not the case, we created a machine-learning-based system to look at each packet in an attack, understand the important features of the packet and analyze and cluster it together to find the appropriate pattern to block. As this happens without the need for a peacetime data set, it is perfect for these sorts of situations.

CONCLUSION

It is our feeling that understanding the functionality, size, and overall scope of a DDoS weapon is important information to have before attempting mitigation. This advisory provides a good foundation of the steps to take to protect the network from the WS-Discovery threat, as well as the upsides and downsides of the various mitigation options.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™, with a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices in more than 80 countries worldwide. For more information, visit: a10networks.com and @A10Networks.