

باسمه تعالی

# حملات DDoS با سوءاستفاده از پیکربندی نامناسب پروتکل SSDP

SSDP<sup>1</sup> یک پروتکل شبکه برای تبلیغ و شناسایی سرویس‌ها و اطلاعات مرتبط با آن‌ها در شبکه است. این کار بدون کمک مکانیزم‌های مبتنی بر سرور مانند DHCP یا DNS انجام می‌شود.

پروتکل SSDP به عنوان اساس پروتکل شناسایی UPnP<sup>2</sup> می‌باشد و توانایی شناسایی تجهیزات Plug & Play را دارا می‌باشد. در اصل این پروتکل با همکاری شرکت‌های میکروسافت و HP در سال ۱۳۹۹ ابداع شده و هرچند که در استانداردهای UPnP به کرات استفاده شده ولی خود به صورت استاندارد مستقلی پذیرفته نشده است.

SSDP از پروتکل UDP و آدرس‌های تک‌پخشی<sup>3</sup> و چند پخشی<sup>4</sup> (239.255.255.250) استفاده می‌کند. همچنین SSDP همانند پروتکل HTTP از روش‌های NOTIFY و M-SEARCH برای شناسایی و تبلیغ سرویس‌ها استفاده می‌کند.

در اواسط سال ۲۰۱۴ میلادی محققان امنیتی PLXsert پی بردند که از این پروتکل نیز در حملات تقویت‌شده DDoS سوءاستفاده می‌گردد. موفقیت این روش مدیون وجود تعداد زیادی تجهیز UPnP آسیب‌پذیر (اغلب از نوع مودم‌ها و مسیریاب‌های خانگی، سرویس‌دهنده‌های مدیا، دوربین‌های دیجیتال مبتنی بر وب، تلویزیون‌های هوشمند، چاپگرها و ...) در سطح جهان است که به حمله‌کننده اجازه می‌دهند تا ترافیک ارسالی خود را تقویت نموده و برای فرد قربانی ارسال نماید.

در حقیقت پروتکل SOAP<sup>5</sup> برای ارسال پیام‌های کنترلی (M-SEARCH) به سوی تجهیزات UPnP و دریافت اطلاعات پاسخ به کار گرفته می‌شود. اما می‌توان با ارسال درخواست‌های خاص SOAP با تعداد بایت کم موجب تولید پاسخ‌هایی با تعداد بایت زیاد شد. فرمت درخواست ارسالی و پاسخ دریافتی به منظور شناسایی تجهیزات UPnP آسیب‌پذیر در دو شکل زیر به تصویر کشیده شده است.

1 Simple Service Discovery Protocol

2 Universal Plug and Play

3 unicast

4 multicast

5 Simple Object Access Protocol

```

User Datagram Protocol, Src Port: 60720 (60720), Dst Port: ssdp (1900)
  Source port: 60720 (60720)
  Destination port: ssdp (1900)
  Length: 105
  Checksum: 0x6439 [validation disabled]
Hypertext Transfer Protocol
  M-SEARCH * HTTP/1.1\r\n
  HOST:239.255.255.250:1900\r\n
  ST:upnp:rootdevice\r\n
  MX:5\r\n
  MAN:"ssdp:discover"\r\n
  \r\n
  [Full request URI: http://239.255.255.250:1900*]
  [HTTP request 1/1]
  [Response in frame: 3]

0000 00 00 0c 9f f0 04 f2 3c 91 50 99 05 08 00 45 00 .....< .P....E.
0010 00 7d 2e f6 40 00 40 11 a7 bb 48 0e bf 9a af 75 ..}.@.@. .H...u
0020 ac a0 ed 30 07 6c 00 69 64 39 4d 2d 53 45 41 52 ...0.L.i d9M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e OST:239. 255.255.
0050 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 75 70 6e 250:1900 ..ST:upn
0060 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d 58 p:rootde vice..MX
0070 3a 35 0d 0a 4d 41 4e 3a 22 73 73 64 70 3a 64 69 :5. .MAN: "ssdp:di
0080 73 63 6f 76 65 72 22 0d 0a 0d 0a scover". ...
  
```

فرمت درخواست M\_SEARCH ارسالی به منظور شناسایی تجهیزات UPnP آسیب پذیر

```

Frame 2: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits)
Ethernet II, Src: Cisco_5a:0b:41 (84:78:ac:5a:0b:41), Dst: f2:3c:91:50:99:05 (f2:3c:91:50:99:05)
Internet Protocol Version 4, Src: [REDACTED], Dst: [REDACTED]
User Datagram Protocol, Src Port: ssdp (1900), Dst Port: 42244 (42244)
  Source port: ssdp (1900)
  Destination port: 42244 (42244)
  Length: 240
  Checksum: 0x409e [validation disabled]
  [Good Checksum: False]
  [Bad Checksum: False]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  CACHE-CONTROL: max-age=1800\r\n
  EXT:\r\n
  LOCATION: http://192.168.0.1:1900/rootDesc.xml\r\n
  SERVER: Ubuntu/7.10 UPnP/1.0 miniuPnP/1.0\r\n
  ST: upnp:rootdevice\r\n
  USN: uuid:fc4ec57e-b051-11db-88f8-0060085db3f6::upnp:rootdevice\r\n
  \r\n
  [HTTP response 1/1]

0000 f2 3c 91 50 99 05 84 78 ac 5a 0b 41 08 00 45 00 <.P....x.Z.A..E.
0010 01 04 b5 44 00 00 2a 11 cb 0f b4 da 53 12 48 0e ..D. * . .S.H.
0020 bf 9a 07 6c a5 04 00 f0 40 8e 48 54 54 50 2f 31 ..l...@.HTTP/1
0030 2e 31 20 32 30 30 20 4f 4b 0d 0a 43 41 43 48 45 ..1 200 0 K..CACHE
0040 2d 43 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 -CONTROL : max-ag
0050 65 3d 31 38 30 30 0d 0a 45 58 54 3a 0d 0a 4c 4f e=1800.. EXT:..LO
0060 43 41 54 49 4f 4e 3a 20 68 74 74 70 3a 2f 2f 31 ATION: http://1
0070 39 32 2e 31 36 38 2e 30 2e 31 3a 31 39 30 30 2f 92.168.0 .1:1900/
0080 72 6f 6f 74 44 65 73 63 2e 78 6d 6c 0d 0a 53 45 rootDesc .xml..SE
0090 52 56 45 52 3a 20 55 62 75 6e 74 75 2f 37 2e 31 RVER: Ub untu/7.1
00a0 30 20 55 50 6e 50 2f 31 2e 30 20 6d 69 6e 69 75 0 UPnP/1. 0 miniu
00b0 70 6e 70 64 2f 31 2e 30 0d 0a 53 54 3a 20 75 70 npnP/1.0 ..ST: up
00c0 6e 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a 55 p:rootd evice..U
00d0 53 4e 3a 20 75 75 69 64 3a 66 63 34 65 63 35 37 e-b051-1 1db-88f8
00e0 65 2d 62 30 35 31 2d 31 31 64 62 2d 38 38 66 38 e-0060085 db3f6::u
00f0 2d 30 30 36 30 30 38 35 64 62 33 66 36 3a 3a 75 -0060085 db3f6::u
0100 70 6e 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a pnp:root device..
0110 0d 0a
  
```

فرمت پاسخ M\_SEARCH دریافتی به منظور شناسایی تجهیزات UPnP آسیب پذیر

پس از استخراج لیستی از تجهیزات آسیب‌پذیر، حمله‌کننده اقدام به ارسال درخواست‌های مجعولی جهت ایجاد پاسخ‌های تقویت شده می‌نماید. سائز پاسخ و در نتیجه ضریب تقویت حمله به عواملی همچون محتوای فایل توصیف تجهیز، سائز سرایند، بنر، نوع سیستم عامل و UUID بستگی دارد. در شکل‌های زیر یک حمله تقویت ترافیک SSDP نمایش داده شده است.

```

244 27.934045000 192.168.1.1 192.168.1.100 SSDP 374 HTTP/1.1 200 OK
.....
> Frame 244: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0
> Ethernet II, Src: Cisco-Li_73:67:b6 (00:13:10:73:67:b6), Dst: Apple_06:93:62 (40:6c:8f:06:93:62)
> Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.100 (192.168.1.100)
< User Datagram Protocol, Src Port: ssdp (1900), Dst Port: ssdp (1900)
  Source port: ssdp (1900)
  Destination port: ssdp (1900)
  Length: 340
  Checksum: 0x7c2e [validation disabled]
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  ST:urn:schemas-upnp-org:service:Layer3Forwarding:1\r\n
  USN:uuid:0013-1073-67b6000b2dc::urn:schemas-upnp-org:service:Layer3Forwarding:1\r\n
  Location: http://192.168.1.1:5431/dyndev/uuid:0013-1073-67b6000b2dc\r\n
  Server: Custom/1.0 UPnP/1.0 Proc/Ver\r\n
  EXT:\r\n
  Cache-Control:max-age=1800\r\n
  DATE: Thu, 01 Jan 1970 00:10:07 GMT\r\n
  \r\n
  [HTTP response 92/308]
  [Prev response in frame: 240]
  [Next response in frame: 246]
.....
0000 40 6c 8f 06 93 62 00 13 10 73 67 b6 08 00 45 00 @l...b...sg..E.
0010 01 68 00 00 40 00 40 11 b5 cf c0 a8 01 01 c0 a8 .h.@.@.....
0020 01 64 07 6c 07 6c 01 54 7c 2e 48 54 54 50 2f 31 .d.l.l.T|.HTTP/1
0030 2e 31 20 32 30 30 20 4f 4b 0d 0a 53 54 3a 75 72 .1 200 0 K..ST:ur
0040 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f n:schema s-upnp-o
0050 72 67 3a 73 65 72 76 69 63 65 3a 4c 61 79 65 72 rg:service:Layer
0060 33 46 6f 72 77 61 72 64 69 6e 67 3a 31 0d 0a 55 3Forwarding:1.U
0070 53 4e 3a 75 75 69 64 3a 30 30 31 33 2d 31 30 37 SN:uuid: 0013-107
0080 33 2d 36 37 62 36 30 30 30 30 62 32 64 63 3a 3a 3 67b600 00b2dc::
0090 75 72 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 urn:sche mas-upnp
00a0 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 4c 61 79 -org:ser vice:Lay
00b0 65 72 33 46 6f 72 77 61 72 64 69 6e 67 3a 31 0d er3Forwa rding:1.
00c0 0a 4c 6f 63 61 74 69 6f 6e 3a 20 68 74 74 70 3a .Locatio n: http:
00d0 2f 2f 31 39 32 2e 31 36 38 2e 31 2e 31 3a 35 34 //192.16 8.1.1:54
00e0 33 31 2f 64 79 6e 64 65 76 2f 75 75 69 64 3a 30 31/dynde v/uuid:0
00f0 30 31 33 2d 31 30 37 33 2d 36 37 62 36 30 30 30 013-1073 -67b6000
0100 30 62 32 64 63 0d 0a 53 65 72 76 65 72 3a 20 43 0b2dc..S erver: C
0110 75 73 74 6f 6d 2f 31 2e 30 20 55 50 6e 50 2f 31 ustom/1. 0 UPnP/1
0120 2e 30 20 50 72 6f 63 2f 56 65 72 0d 0a 45 58 54 .0 Proc/ Ver..EXT
0130 3a 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c ..Cache -Control
0140 3a 6d 61 78 2d 61 67 65 3d 31 38 30 30 0d 0a 44 :max-age =1800..D
0150 41 54 45 3a 20 54 68 75 2c 20 30 31 20 4a 61 6e ATE: Thu , 01 Jan
0160 20 31 39 37 30 20 30 30 3a 31 30 3a 30 37 20 47 1970 00 :10:07 G
0170 4d 54 0d 0a 0d 0a MT....
  
```

```

12:31:43.468520 IP 192.168.1.100 > 192.168.1.1: ICMP 192.168.1.100 udp port 1900
unreachable, length 36
E..8)k@.@.....d.....E..f..@.@.....d.l.l.R..
12:31:43.469991 IP 192.168.1.1.1900 > 192.168.1.100:1900: UDP, length 332
E..h..@.@.....d.l.l.T..HTTP/1.1 200 OK
ST:urn:schemas-upnp-org:service:WANPPPPConnection:1
USN:uuid:0013-1073-67b60200b2dc::urn:schemas-upnp-org:service:WANPPPPConnection:1
Location: http://192.168.1.1:5431/dyndev/uuid:0013-1073-67b60000b2dc
Server: Custom/1.0 UPnP/1.0 Proc/Ver
EXT:
Cache-Control:max-age=1800
DATE: Thu, 01 Jan 1970 00:10:35 GMT

12:31:47.474006 IP 192.168.1.1.1900 > 192.168.1.100:1900: UDP, length 268
--
--
ST:urn:schemas-upnp-org:service:WANPPPPConnection:1
USN:uuid:0013-1073-67b60200b2dc::urn:schemas-upnp-org:service:WANPPPPConnection:1
Location: http://192.168.1.1:5431/dyndev/uuid:0013-1073-67b60000b2dc
Server: Custom/1.0 UPnP/1.0 Proc/Ver
EXT:
Cache-Control:max-age=1800
DATE: Thu, 01 Jan 1970 00:10:37 GMT
  
```

تحقیقات نشان داده است که ضریب تقویت ترافیک در این حمله می‌تواند بیش از ۳۰ باشد.

### راه حل پیشگیری

پیشگیری از وقوع این حمله به دلیل وجود تعداد بسیار زیاد تجهیز آسیب‌پذیر در کل سطح جهان بسیار دشوار است. اما به عنوان یک راه حل کلی می‌توان ترافیک UDP که دارای پورت مبدا با شماره ۱۹۰۰ است را بلوک نمود. همچنین در صورت عدم نیاز به پروتکل SSDP و پذیرفتن عواقب آن (مانند صرفنظر کردن از قابلیت Home Group در سیستم عامل ویندوز) می‌توان آن را غیرفعال نمود. برای انجام این کار در سیستم عامل ویندوز می‌توان با اجرای services.msc و انتخاب و غیرفعال‌سازی SSDP Discovery service در local system این کار را انجام داد. در برخی از مودم‌های خانگی نیز گزینه disable UPnP بدین منظور وجود دارد.