باسمه تعالی

حملات DDoS با سوءاستفاده از پیکربندی نامناسب پروتکل SSDP

SSDP[1] 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.

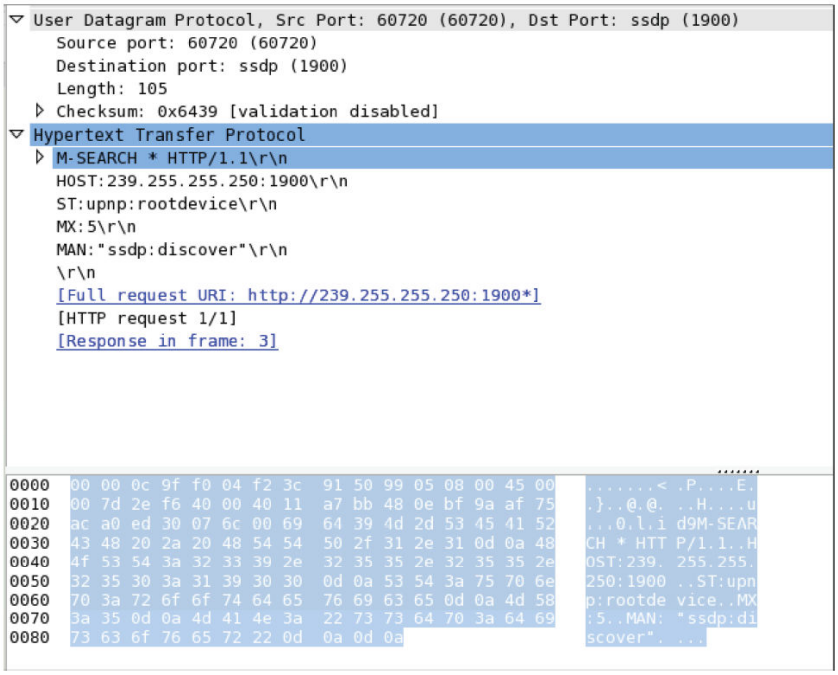
پروتکل SSDP به عنوان اساس پروتکل شناسایی UPnP[2] می‌باشد و توانایی شناسایی تجهیزات Plug & Play را دارا می‌باشد. در اصل این پروتکل با همکاری شرکت‌های مایکروسافت و HP در سال ۱۳۹۹ ابداع شده و هرچند که در استانداردهای UPnP به کرات استفاده شده ولی خود به‌صورت استاندارد مستقلی پذیرفته نشده است.

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

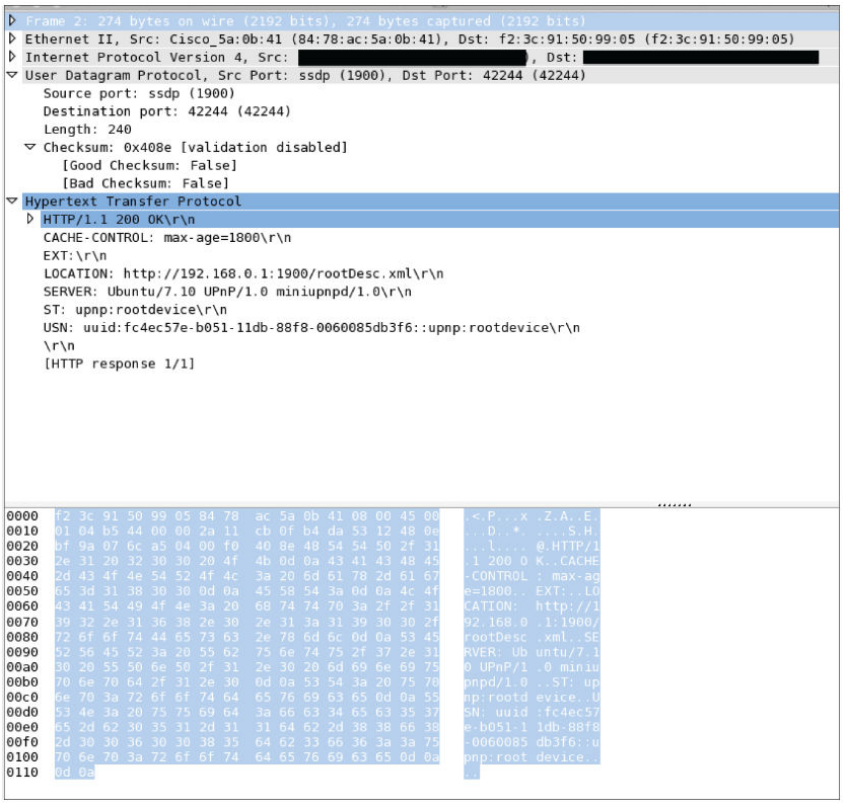
در اواسط سال ۲۰۱۴ میلادی محققان امنیتی PLXsert پی بردند که از این پروتکل نیز در حملات تقویت‌شده DDoS سوءاستفاده می‌گردد. موفقیت این روش مدیون وجود تعداد زیادی تجهیز UPnP آسیب‌پذیر (اغلب از نوع مودم‌ها و مسیریاب‌های خانگی، سرویس‌دهنده‌های مدیا، دوربین‌های دیجیتال مبتنی بر وب، تلویزیون‌های هوشمند، چاپگرها 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[5] برای ارسال پیام‌های کنترلی (M-SEARCH) به سوی تجهیزات UPnP و دریافت اطلاعات پاسخ به‌کار 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

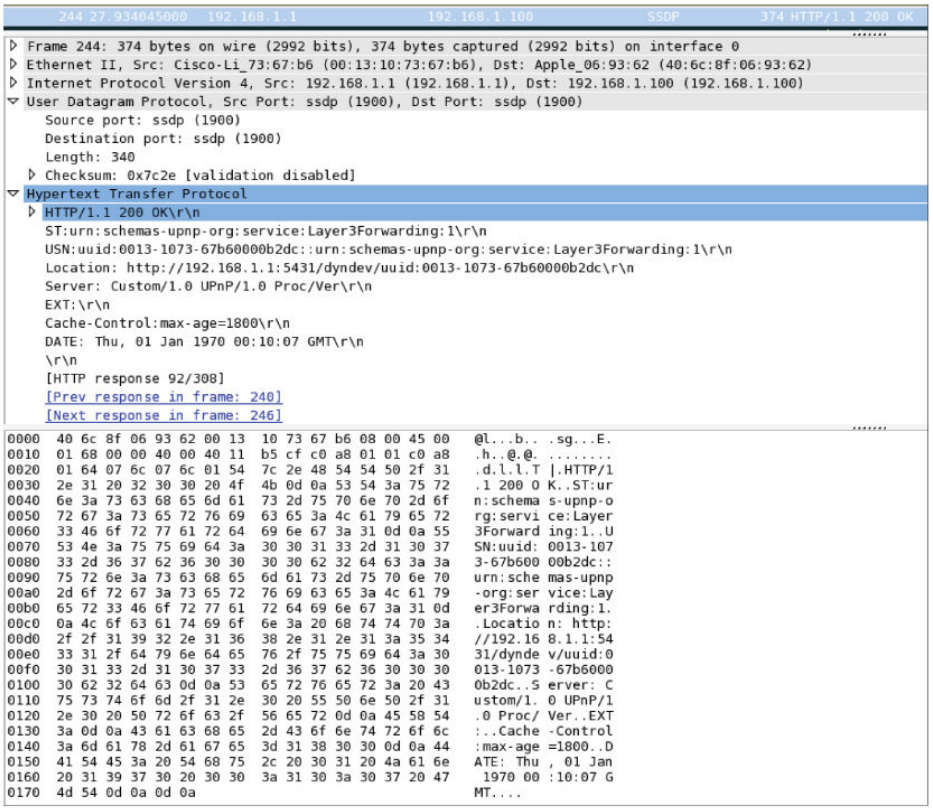


فرمت درخواست M_SEARCH ارسالی به منظور شناسایی تجهیزات UPnP آسیب‌پذیر



فرمت پاسخ M_SEARCH دریافتی به منظور شناسایی تجهیزات UPnP آسیب‌پذیر

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




```
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:WANPPPConnection:1
USN:uuid:0013-1073-67b60200b2dc::urn:schemas-upnp-org:service:WANPPPConnection: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:WANPPPConnection:1
USN:uuid:0013-1073-67b60200b2dc::urn:schemas-upnp-org:service:WANPPPConnection: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.

راه‌حل 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 مبداء 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.