تحلیل آسیب پذیری QOTD و شناسایی آدرس های IP دارای آسیب پذیری مذکور در ایران

حملات منع سرویس از جمله حملاتی می‌باشند که به طور چشم‌گیری در حال استفاده می‌باشند. این حملات که به دنبال منع دسترسی کاربران و از کار انداختن سرویس‌های خاصی از یک سرور ارائه‌دهنده سرویس می‌باشند، معمولاً باعث پایین آمدن سرعت و کیفیت سرویس‌دهی شبکه و در نهایت از دسترس خارج شدن شبکه مورد هدف می‌باشند.

پروتکل لایه انتقال UPD از جمله پروتکل‌هایی می‌باشد که امروزه بسیار مورد هدف این‌گونه حملات قرار گرفته است. پروتکل‌های زیر برخی از پروتکل‌های این لایه می‌باشند که از آنها برای اجرای این‌گونه حملات استفاده شده است:

- DNS
- NTP
- SNMPv2
- NetBIOS
- SSDP
- CharGEN
- QOTD
- BitTorrent
- Kad
- Quake Network Protocol
- Steam Protocol

پروتکل UDP یک پروتکل ذاتاً بدون اتصال است و به همین جهت آدرس IP مبدا را بررسی نمی‌کند. درنتیجه اگر پروتکل‌های لایه نرم‌افزار اقدامات جبران‌کننده‌ای مثل session initiation برای جلوگیری از جعل آدرس مبدا انجام ندهند، به راحتی می‌توان بسته‌های IP را به گونه‌ای تغییر داد تا در فیلد آدرس مبدا آنها، آدرس IPفرد قربانی قرار گیرد. هنگامی که مجموعه‌ای از این بسته‌ها که آدرس مبدا آن‌ها تغییر کرده است به سمت یک سیستم ارسال شود، سیستم/ سرور دریافت‌کننده جواب این بسته‌ها را به سمت کاربر قربانی ارسال می‌نماید و درنتیجه یک حمله reflected denial of service شکل می‌گیرد.

روش‌های کلاسیک برای اجرای حملات منع سرویس به این صورت بودند که فرد حمله‌گر برای اجرای حمله نیاز داشت تا تعداد زیادی بسته را به سمت مقصد مورد نظر ارسال نماید تا از این طریق بتواند پهنای باند کاربر هدف را اشغال نماید. ولی امروزه با استفاده از این نوع حملات به راحتی می‌توان با استفاده از یک درخواست ساده برای پروتکل‌های آسیب‌پذیر مثل qotd، در جواب ترافیکی ۱۰ها و یا ۱۰۰ها برابر ترافیک ارسالی ایجاد نمود و این ترافیک را به سمت کاربر قربانی هدایت کرد. به این دسته از حملات، amplification attack گفته می‌شود و هنگامی که با reflective dos Attack ها ترکیب شده و در یک گستره بزرگ اجرا شوند، به راحتی می‌توانند یک حمله DOS توزیع شده را شکل دهند.

برای شناسایی این حملات از ضریبی تحت عنوان Bandwidth Amplification Factor (BAF) استفاده می‌شود. BAF را می‌توان از طریق محاسبه تعداد UDP payload byte هایی که یک amplifier برای پاسخ به درخواست‌ها ارسال می‌نماید در مقایسه با تعداد UDP payload byte هایی که به‌عنوان درخواست ارسال شده‌اند، به‌دست آورد.

فرد حمله‌گر به راحتی می‌تواند از این پروتکل‌ها برای ایجاد یک حمله DOS توزیع‌شده استفاده نماید و از این طریق ترافیکی ناخواسته و عظیم را به سمت قربانی ارسال نماید.

سرویس QOTD

سرویس Qoute Of The Day (QOTD) عضوی از خانواده پروتکل‌های اینترنت است که در RFC 865 به طور کامل معرفی شده است. این سرویس درگذشته کاربرد داشته است به این صورت که کاربران از سیستم مدیریتی خود روزانه یک شعار برای همان روز را درخواست می‌نمودند. این پروتکل علاوه بر این هدف، برای عیب‌یابی و تست شبکه نیز مورد استفاده قرار می‌گیرد و هر کاربر می‌تواند به یک سرور که از پروتکلQOTD پشتیبانی می‌نماید، روی پورت ۱۷ پروتکل TCP و یا UDP متصل گردد. برای اینکه بتوانیم اندازه این quote را در یک اندازه قابل قبول نگه‌داری نماییم، حداکثر طول ۵۱۲ کاراکتر برای هر quote در نظر گرفته شده است.

امروزه سرویس QOTD به ندرت فعال است و اغلب توسط دیواره‌های آتش برای جلوگیری از حملات ping-pong فیلتر می‌گردد. در ضمن به دلیل اینکه امروز تست و ارزیابی شبکه‌های IP عموماً توسط دستوراتی مثل ping و یا

traceroute صورت می‌گیرد (زیرا خیلی مطمئن‌تر از پروتکل echo می‌باشند)، دیگر این پروتکل مورد استفاده قرار نمی‌گیرد و کاربردی ندارد.

برای تست سرورهای QOTD می توان با پورت مورد نظر در آن سرور یک ارتباط برقرار نمود و درصورت برقراری ارتباط، فعال بودن پورت نتیجه گرفته می‌شود. برای انجام این کار می‌توان از دستور telnet استفاده نمود:

telnetcyguns-net 17

URI	TCP Port	IPv4	IPv6	Change Rate
cygnus-x.net	17	Yes	No	Unknown (Not Each Request)
qotd.nngn.net	17	Yes	No	Daily
qotd.atheistwisdom.com	17	Yes	Yes	Daily
djxmmx.net	17	Yes	Yes	Each Request
alpha.mike-r.com	17	Yes	No	Each Request

حملات منع سرویس QOTD

در این نوع حملات، ابتدا سرور سرویس‌دهنده‌ی QOTD شناسایی می‌شود. سپس فرد حمله‌گر درخواست‌های QOTD خود را برای سرور مورد نظر ارسال می‌نماید. با این تفاوت که بسته‌های ارسالی خود را به گونه‌ای تغییر می‌دهد که در فیلد آدرس مبدا آنها، آدرس IP سیستم قربانی قرار گیرد. با استفاده از این روش، فرد حمله‌گر می‌تواند با استفاده از یک درخواست ساده، یک ترافیک قابل توجه را به سمت کاربر هدف ارسال نماید.

برای اینکه تاثیر حمله بیشتر شود، می‌توان از یک شبکه بات بهره گرفت. به این صورت که مجموعه‌ای از کاربران که با استفاده از یک بدافزار به نحوی تحت کنترل یک حمله‌گر قرار گرفته‌اند، در یک زمان مشخص همگی درخواست‌های خود با آدرس مبدا جعلی را به سمت سرور مورد نظر فرستاده و سپس سرور پاسخ خود را برای کاربر قربانی flood می‌نمایند. با استفاده از این روش، نه تنها سیل عظیمی از بسته‌ها به طرف کاربر هدف ارسال

می‌شوند، بلکه شناسایی مبدا حمله نیز سخت‌تر می‌گردد. میزان ریسک این حمله کم بوده و سیستم‌های مبتنی بر Unix را تحت تاثیر قرار می‌دهد.

برای مقابله با این حمله، مجموعه اقدام‌های زیر پیشنهاد می‌گردد:

- غیرفعال‌سازی پورت‌ها و سرویس‌های غیرضروری (خصوصاً QOTD)
- تنظیم دیواره آتش جهت مسدودسازی پورت UDP۱۷ و TCP۱۷ برای همه سیستم‌ها
- در یونیکس، غیرفعال سازی qotd وقتی از شاخه inetd شروع شده است:
  - ویرایش فایل /etc/inetd.conf
  - تعیین خط کنترلی qotd daemon
  - تایپ یک # هنگام شروع خط فرمان خارج از daemon
  - راه اندازی مجدد inetd