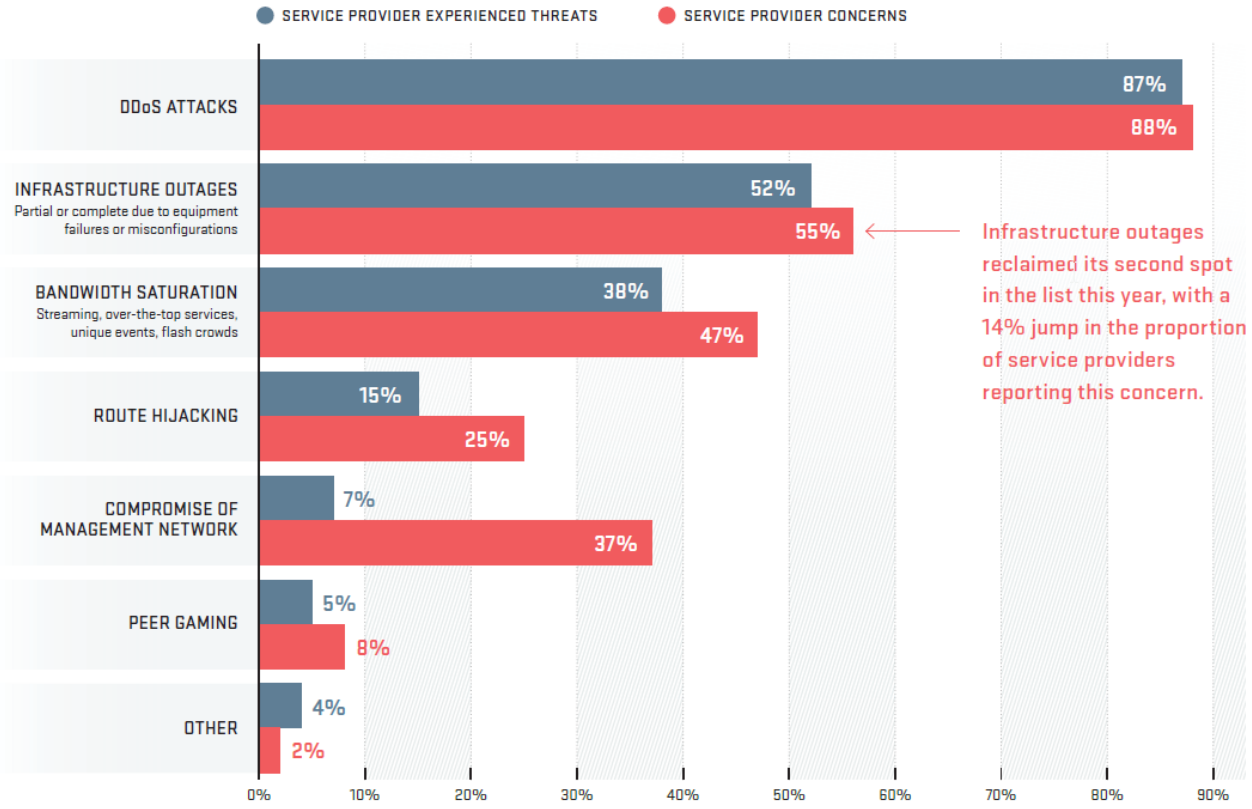
مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

بررسی و تحلیل تهدیدات DDOS برای فراهم‌کنندگان سرویس
در سال ۲۰۱۷

حمله DDoS مخفف (distributed denial of service) به معنی سرازیر کردن تقاضاهای زیاد به یک سرور و استفاده بیش از حد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) به طوری که سرویس‌دهی عادی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود. در این نوع حمله‌ها در یک زمان به صورت مداوم از طریق کامپیوترهای مختلف که ممکن است خواسته یا حتی ناخواسته مورد استفاده قرار گرفته باشند، به یک سرور (با آی پی مشخص) درخواست دریافت اطلاعات ارسال می‌شود و موجب از دسترس خارج شدن سرور می‌شود.

حملات DDoS در رأس تهدیدات فراهم‌کنندگان سرویس در سال ۲۰۱۷ با سهم ۸۷ درصد از کل تهدیدات قرار دارد(شکل ۱). خرابی‌های زیرساخت (Infrastructure outages) نیز به عنوان یک تهدید ۵۲ درصد عامل‌های تهدیدات فراهم‌کنندگان سرویس را شامل می‌شود که نسبت به سال ۲۰۱۶ شش درصد افزایش یافته است. درصد اشباع پهنای باند (bandwidth saturation) نیز نسبت به سال ۲۰۱۶ ثابت مانده است. به طور مکرر نگرانی اصلی ۸۸ درصد فراهم‌کنندگان سرویس در سال ۲۰۱۸ حملات DDoS است. با توجه به نگرانی‌های مربوط به باتنت‌های IOT و آسان‌تر شدن کار مهاجمان برای دستیابی به حملات پیشرفته این مسئله تعجب‌آور نخواهد بود.



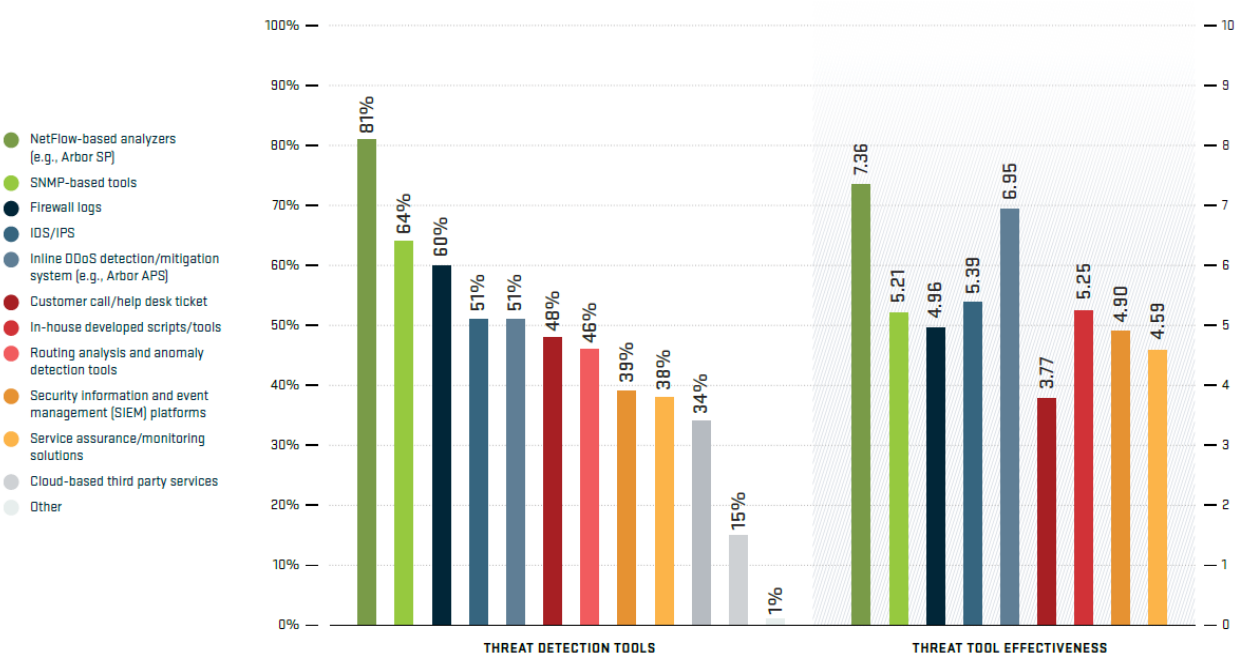
شکل ۱. تهدیدات و نگرانی‌های فراهم‌کنندگان سرویس

همانطور که در سال‌های گذشته ابزارهای مختلفی برای تشخیص تهدیدات علیه شبکه‌های کامپیوتری استفاده می‌شد، این بررسی نشان می‌دهد که ابزارهای تحلیلی NetFlow-base گزینه انتخابی فراهم‌کنندگان سرویس در این سال‌ها باقی مانده است و تنها در سال ۲۰۱۸ استفاده از آن از ۸۶ درصد به ۸۱ درصد کاهش یافته است (شکل ۲).

همچنین استفاده از ابزارهای SNMP-based به ۶۴ درصد افزایش یافته است که در سال ۲۰۱۶ این درصد ۵۳ بود. استفاده از لاگ‌های فایروال نیز همراه با IDS/IPS در رتبه چهارم قرار دارند.

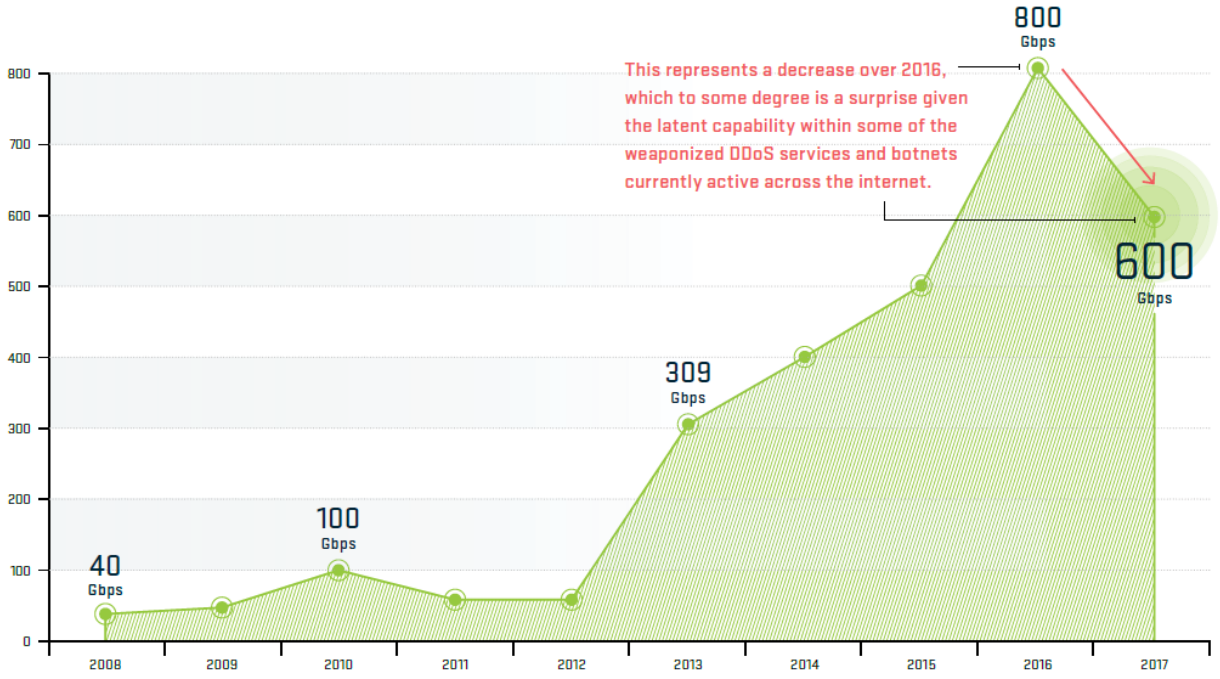
استفاده از سیستم تشخیص/کاهش DDoS درونی (Inline DDoS detection/mitigation system) از ۴۲ درصد به ۵۱ درصد افزایش داشته است. استفاده از راه‌حل‌های دفاع DDoS ترکیبی یک روند در حال پیشرفت است.

به طور کلی، نتایج اثربخشی ابزارهای تشخیص تهدید مشابه با سال ۲۰۱۶ بوده است. نتایج بررسی‌ها نشان می‌دهند که ابزارهای تحلیلی NetFlow-based و inline DDoS detection/mitigation بهترین و موثرترین راه‌حل‌های مقابله با تهدیدات DDoS بوده‌اند.



شکل ۲. اثربخشی و میزان استفاده ابزارهای تشخیص تهدید

در سال ۲۰۱۷، مهاجمان با استفاده از تکنیک‌های بازتاب/تقویت (reflection/amplification techniques) از آسیب‌پذیری‌های موجود در DNS، NTP، SSDP، CLDAP، Chargen و پروتکل‌های دیگر برای به حداکثر رساندن مقیاس حملات خود استفاده کردند. علاوه براین افزایش قابل ملاحظه‌ای در بهره‌برداری از دستگاه‌های IOT برای تولید سیلی از بسته‌های بزرگ و حملات لایه کاربردی به وجود آمده است. بزرگترین حمله گزارش شده توسط یک فراهم کننده سرویس ۶۰۰ گیگابایت در ثانیه بوده است و حملات دیگری نیز مانند ۵۸۸، ۳۳۸ و ۳۱۶ گیگابایت در ثانیه گزارش شده‌اند (شکل ۳).



شکل ۳. اندازه حملات

در شکل ۴ شایع‌ترین اهداف این حملات نشان داده شده است که از این بین کاربران نهایی با ۷۰ درصد در رأس اهداف حملات قرار دارند. خدمات مالی بالاتر از خدمات ابری و هاستیگ و حکومت جزو اهداف اصلی حملات هستند.

شکل ۴. اهداف حملات

رایج‌ترین نوع حملات DDoS

مهاجمان سایبری به صورت مداوم در حال توسعه روش‌های استفاده از بردارهای حمله متفاوت برای فرار از دفاع و تشخیص هستند. به طور کلی بردارهای حمله به سه گروه تقسیم می‌شوند.

۱- حملات حجمی (Volumetric Attacks)

این حملات تلاش می‌کنند تا پهنای باند را در داخل شبکه یا سرویس هدف، یا بین شبکه هدف یا سرویس و اینترنت مصرف کنند. این حملات به سادگی باعث ایجاد ازدحام می‌شوند.

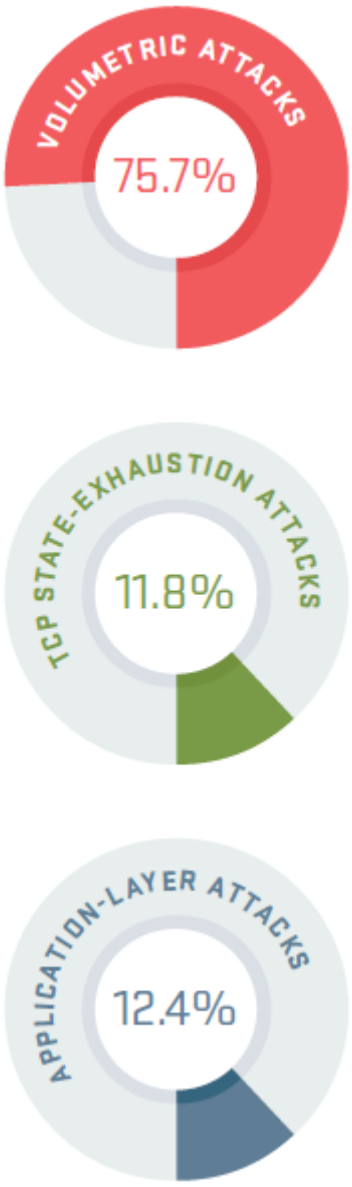
۲- حملات TCP State-Exhaustion

این حملات سعی در مصرف جداول حالت اتصال را دارند که در بسیاری از اجزای زیرساخت مانند load balancers، firewall، IPS و سرورهای اپلیکیشنی استفاده می‌شوند. آن‌ها همچنین می‌توانند دستگاه‌های با ظرفیت بالا را که قادر به نگهداری میلیون‌ها اتصال هستند از دسترس خارج کنند.

۳- حملات لایه کاربرد (Application-Layer Attacks)

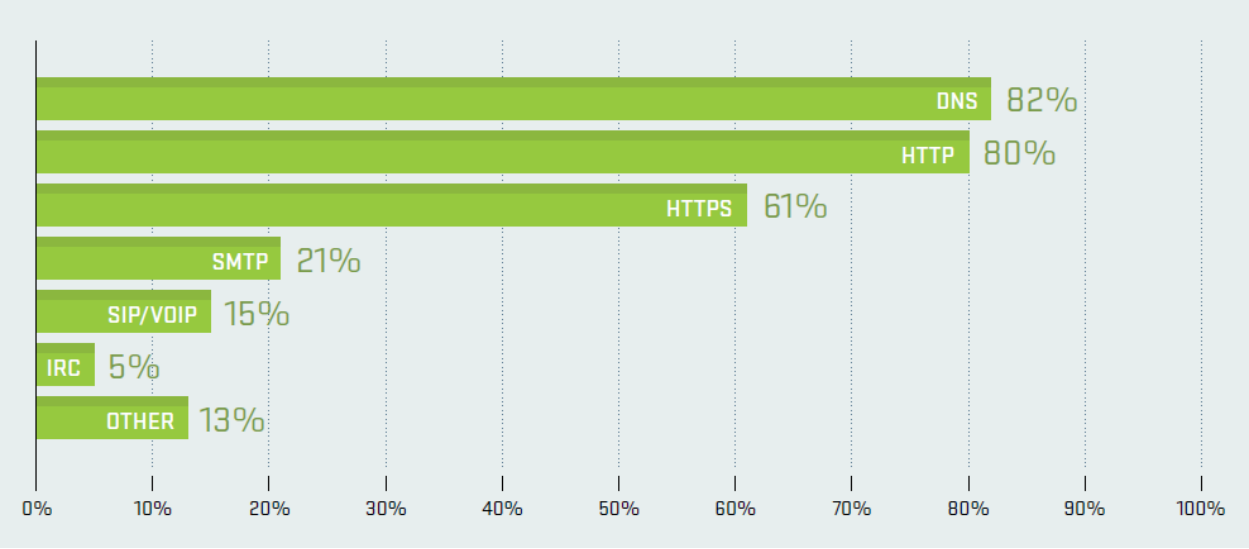
این حملات مربوط به سرویس‌ها و قابلیت‌های لایه ۷ شبکه هستند. این نوع حملات پیچیده‌تر بوده زیرا آن‌ها می‌توانند با تولید یک ترافیک با نرخ کم بسیار موثر باشند.

با نگاهی به ترکیب انواع حملات بر فراهم‌کنندگان سرویس، حملات حجمی رایج‌ترین نوع حمله گزارش شده است. همچنین این نوع حمله در سال ۲۰۱۷ افزایش قابل ملاحظه‌ای داشته است (شکل ۵).



شکل ۵. انواع حملات DDoS

نکته قابل توجه این است که حملات لایه شبکه همچنان به استفاده از سرویس‌های آسیب‌پذیر ادامه می‌دهند. سرویس DNS در سال گذشته بیشترین هدف حملات لایه شبکه بوده است. طبق گزارش‌های بدست آمده ۸۲ درصد فراهم‌کنندگان سرویس از این طریق آسیب‌پذیر بوده‌اند (شکل ۶). پروتکل HTTP با ۸۰ درصد در جایگاه بعدی قرار دارد. میزان سوءاستفاده از پروتکل HTTPS نسبت به سال گذشته از ۵۲ درصد به ۶۱ درصد افزایش داشته است که به این معنی است که همیشه رمزنگاری تنها راه‌حل موفقی برای مقابله با حملات DDoS نیست و راه‌حل های مقیاس پذیر موردنیاز است.



شکل ۶. سرویس‌های هدف حملات لایه کاربرد

منبع:

https://www.netscout.com/