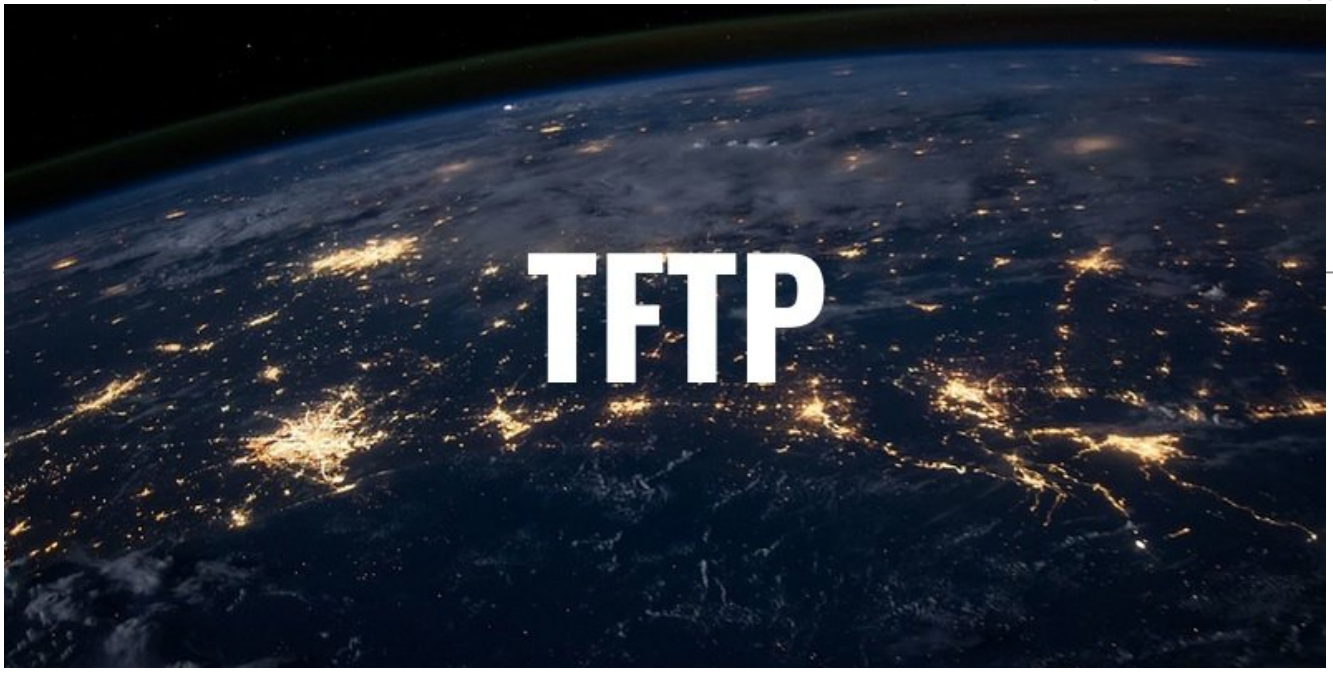
حملاتی سریع و موثر

پروتکلی که تقویت‌کننده حملات DDoS شد!



چند ماه قبل پژوهش‌گران امنیتی دانشگاه نایپر ادینبورگ مقاله‌ای در ارتباط با مدل خاصی از حمله منع سرویس توزیع شده (DDoS) و راه‌کار تقویت این مدل حمله با استفاده از پروتکل انتقال موقت فایل (TFTP) را منتشر کردند. اما به تازگی پژوهش‌گران شرکت آکامای هشدار داده‌اند که این چنین تکنیکی ممکن است در دنیای واقعی خطر بالقوه‌ای را به وجود آورد.

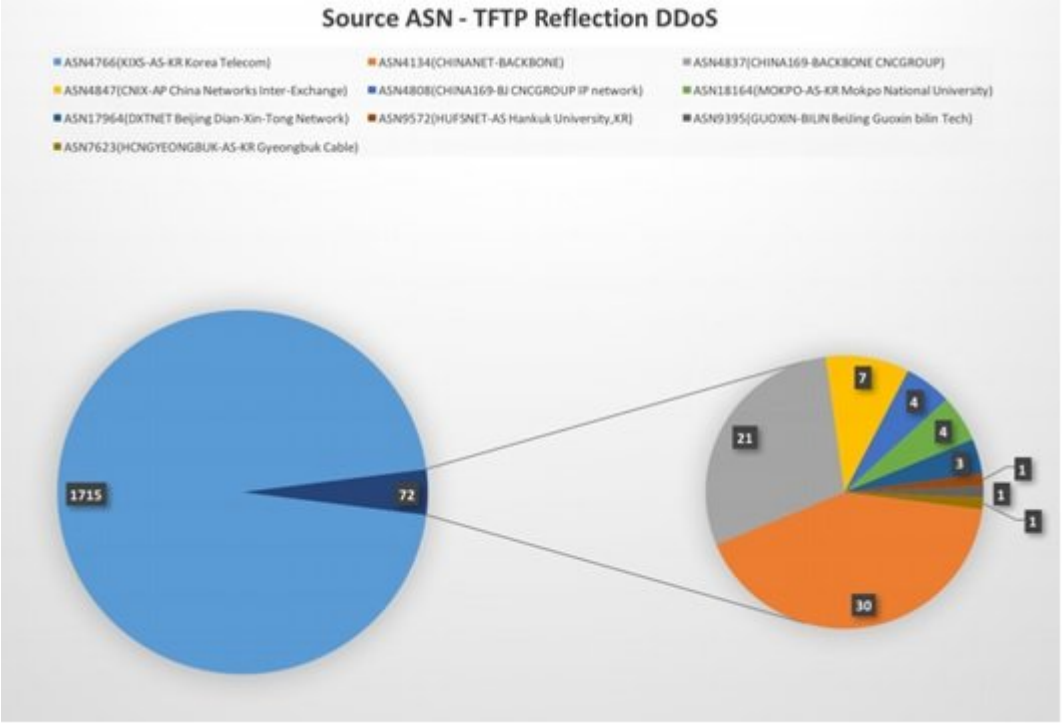
حملات DDoS به‌طور معمول بر پایه بات‌نت‌های فراوان و از طریق منابع متفاوتی به مرحله اجرا در می‌آیند. این مدل حملات باعث به وجود آمدن حجم گسترده‌ای از ترافیک می‌شوند. اما هکرها برای آن‌که بر شدت حملات خود بیفزایند از دستگاه‌های میانی تقویت کننده (amplifiers) برای تقویت ترافیک تخریبی استفاده می‌کنند. اما نکته مهمی که پژوهش‌گران دانشگاه ادینبورگ کشف کرده‌اند این است که TFTP این توانایی را دارد تا به عنوان یک عامل تقویت کننده تقریبا 60 برابری مورد استفاده قرار گیرد. به‌طوری که در مقایسه با روش‌های موجود از نرخ بالاتری بهره می‌برد.

مطلب پیشنهادی

راه‌کار جدید در دنیای محاسبات

تولید اعداد تصادفی که واقعا تصادفی هستند!

ریچارد مک فارلین، بوریس سیکلیک و ویلیام ج بوکانن، محققان این دانشگاه، در مقاله خود عنوان کرده‌اند که این روش تقویتی ممکن است تبدیل به یک مخاطره جهانی شود. به دلیل این‌که پروتکل TFTP تقریبا توسط 599600 سرور باز TFTP مورد استفاده قرار می‌گیرد. در حالی که این محققان از سال 2014 سرگرم تحقیق در خصوص این مشکل امنیتی بودند، اما مقاله آن‌ها ماه مارس در مجله computer & science به چاپ رسید و اکنون سرتیتر اخبار سایت‌های مختلف شده است. البته لازم به توضیح است که این سه پژوهش‌گر اولین کارشناسان امنیتی نیستند که نشان دادند سرورهای TFTP این پتانسیل را دارند تا به عنوان تقویت کننده حملات DDoS مورد استفاده قرار گیرند. در سال 2013 نیز جیسون شولتز، مهندس بخش تحقیقات و تهدیدات سیسکو، این چنین پیشامدی را پیش‌بینی کرده بود. او در آن زمان گفته بود: «تشدید قدرت حمله DDoS با استفاده از پروتکل TFTP روش بهینه‌سازی شده‌ای برای حمله نیست، اما اگر به تعداد کافی، سرورهای عمومی TFTP در دسترس باشند این حمله به شیوه موثرتری می‌تواند پیاده‌سازی شود.»



تیم واکنش هوش امنیتی شرکت آکامای (Security Intelligence Response Team) موفق به کشف ده حمله بر مبنای اهرم TFTP شد. حملاتی که از تاریخ 20 آوریل آغاز شده و مشتریان شرکت را تحت‌الشعاع خود قرار داده‌اند. جوز آرتیگا از کارمندان شرکت آکامای در این ارتباط اعلام کرده است: «اسکرپیت حمله کننده TFTP فعالیت خود را از ماه مارس آغاز کرده است. به نظر می‌رسد این حمله همزمان با انتشار تحقیقات در مورد این شیوه حمله در رسانه‌های جمعی صورت گرفته است. » آن‌گونه که آرتیگا گفته است، بیشتر این حملات چند برداری بوده و ردپایی از تکنیک انعکاسی TFTP در آن‌ها به چشم می‌خورد. تحلیل‌ها نشان می‌دهند که حداقل یک سایت حملات DDoS را در غالب یک سرویس یکپارچه انتقال داده است.

در شرایطی که این سبک از حمله، نرخ بسته آن‌چنان بالایی را تولید نمی‌کند، اما در مقابل حجم بسته‌های تولید شده به اندازه کافی زیاد هستند تا پهنای باند سایت‌ها را مورد هدف قرار دهند. گزارش این محققان نشان می‌دهد که این ابزار حمله از کد یکسانی همسو با دیگر ابزارهای انعکاسی پایه UDP استفاده کرده و خط فرمان مشابهی نیز دارد. تحلیل‌ها نشان می‌دهند که این چنین حمله‌ای پهنای باندی به میزان حداکثر 1.2 گیگابیت در ثانیه برابر با 176.4 هزار بسته در ثانیه تولید می‌کند.

```
▾ Trivial File Transfer Protocol
    Opcode: Read Request (1)
    Source File: /x
    Type: netascii

0000  1e 00 00 00 60 02 94 59  00 16 11 40 00 00 00 00   ....`..Y ...@....
0010  00 00 00 00 00 00 00 00  00 00 00 01 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 01 f1 3e 00 45   ........ .....>.E
0030  00 16 00 29 00 01 2f 78  00 6e 65 74 61 73 63 69   ...)../x .netasci
0040  69 00                                             i.
```

این بردار حمله انعکاس TFTP از پورت 69 به عنوان پورت منبع استفاده می‌کند. اما این احتمال وجود دارد که حملات پورت خاصی را هدف قرار نداده و پورت‌ها را به صورت تصادفی انتخاب کنند. با این وجود دامنه تاکتیکی این حمله محدود است، به دلیل این‌که TFTP به گونه‌ای طراحی شده است تا فایل‌ها و به ویژه فایل‌های پیکربندی شده را برای تعداد محدودی از میزبان‌ها آن هم در زمان مشخصی ارسال کند. در نتیجه این احتمال وجود دارد که سرورهای TFTP این توانایی را نداشته باشند تا حجم زیادی از درخواست‌هایی که توسط ابزارهای بردار حمله TFTP ارسال می‌شوند را انتقال دهند. در بخشی دیگری از مقاله منتشر شده توسط این پژوهش‌گران آمده است که TFTP تنها قادر به تولید نرخ 1.2 گیگابیت است، اما در حملات چند برداری که حمله TFTP یکی از بردارهای آن‌ها به شمار

می‌رود، این میزان به عدد 44 گیگابیت در ثانیه می‌رسد. منابع جمع‌آوری شده در ارتباط با حملات انعکاسی TFTP نشان از آن دارند که مراحل اولیه حمله توزیع شده ضعیف بوده است. منشا بخش عمده‌ای از این منابع آسیایی بوده است اما در ادامه این حملات از منابع اروپایی نیز استفاده کرده‌اند. کارشناسان امنیتی به مدیران سرورهایی که پروتکل TFTP را میزبان می‌کنند، توصیه کرده‌اند، پورت شماره 69 که برای اتصال به اینترنت مورد استفاده قرار می‌گیرد را مورد ارزیابی قرار دهند. این پورت باید به یک دیوار آتش تجهیز شده و تنها به منابع ورودی معتبر اجازه ورود دهند. ضروری است مدیران از ابزارهای شناسایی سوء استفاده از سرورهای TFTP در یک شبکه استفاده کنند.

تاریخ انتشار:

12 تیر 1395

نشانی منبع: https://www.shabakeh-mag.com/security/3495