بکارگیری تجهیزات اینترنت اشیا برای پیاده‌سازی حملات منع سرویس توزیع شده پیچیده

گزارشی از سوی شرکت امنیتی NETSCOUT Arbor منتشر شده است، نشان می‌دهد دستگاه‌های اینترنت اشیای آسیب‌پذیر نه‌تنها به هکرها اجازه می‌دهند تا حملات منع سرویس توزیع شده را پیاده‌سازی کنند، بلکه به آن‌ها اجازه می‌دهند این حملات را با پیچیدگی هرچه تمام‌تر به سرانجام برسانند. سیزدهمین گزارش سالانه منتشر شده از سوی این شرکت که در ارتباط با امنیت زیرساخت شبکه‌ها بوده نشان می‌دهد در سال گذشته میلادی هکرها به‌شکل هوشمندانه‌ای به‌دنبال پیچیده کردن حملات خود بوده و برای این منظور از تجهیزات اینترنت اشیا بهره برده‌اند.

این رویکرد که چند سالی است از سوی هکرها دنبال می‌شود، اکنون به مرحله دیگری وارد شده که افزایش حملات را به همراه داشته است. این گزارش با استناد به آمار و اطلاعاتی آماده شده که از شرکت‌های فعال در زمینه ارائه‌دهنده خدمات مختلف همچون میزبانی، ارائه سرویس‌های متنوع اینترنت و سرویس‌های مرتبط با گوشی‌های هوشمند به دست آمده است. در این گزارش آمده است که سال گذشته میلادی، منابع شبکه 57 درصد از سازمان‌ها، دولت‌ها، بخش‌های آموزشی و منابع شبکه 45 درصد از شرکت‌هایی که در زمینه سرویس‌های شبکه همچون مراکز داده به فعالیت اشتغال داشته‌اند، تحت تأثیر حملات منع سرویس توزیع شده قرار گرفته‌اند. این شرکت که در زمینه ایمن‌سازی شبکه‌ها به فعالیت اشتغال دارد در گزارش آورده است که سال گذشته میلادی چیزی حدود 7.5 میلیون حمله منع سرویس توزیع شده را شناسایی کرده است. در بخشی از این گزارش آمده است: «بزرگ‌ترین حمله به وقوع پیوسته در سال گذشته میلادی از سوی یک ارائه‌دهنده خدمات گزارش شده که اعلام داشته است قدرت این حمله به 600 گیگابیت بر ثانیه رسیده است. همچنین نزدیک به یک چهارم از پاسخ‌دهندگان اعلام داشته‌اند حمله‌ای با قدرت 100 گیگابیت بر ثانیه را تجربه کرده‌اند.»
همچنین، در سال گذشته میلادی نیز مدت زمان حملات منع سرویس توزیع شده افزایش قابل ملاحظه‌ای داشته است. 29 درصد ارائه‌دهندگان سرویس‌ها گزارش کرده‌اند حملاتی که زیرساخت‌های آن‌ها را تحت تأثیر خود قرار داده بود، نزدیک به 12 ساعت به طول انجامیده است. 45 درصد از این شرکت‌ها اعلام داشته‌اند که هر ماه بیش از 21 بار در معرض چنین حملاتی قرار گرفته‌اند. بدتر آنکه نزدیک به 17 درصد از این شرکت‌ها اعلام داشتند در هر ماه دست‌کم 500 مرتبه تجربه تلخ حمله منع سرویس انکار شده را چشیده‌اند! در حالی که اغلب ارائه‌دهندگان سرویس‌ها اعلام داشته‌اند که حملات حجمی (volumetric attacks) به کسب و کار آن‌ها آسیب جدی وارد کرده است، اما در مقابل دیگر شرکت‌ها اعلام داشته‌اند یک رشد 30 درصد حمله در لایه کاربردی را شاهد بوده‌اند. حملات چندبرداری (multi-vector) نیز به‌ترتیب
59 درصد ارائه‌دهندگان سرویس‌ها و 48 درصد شرکت‌ها را نشانه رفته است. حملات مستتر لایه کاربردی که زیاد مورد توجه هکرها قرار نداشت، در سال گذشته میلادی رشد 30 درصدی را تجربه کرده بود. 73 درصد از این حملات پروتکل انتقال ابرمتن، 69 درصد سامانه نام دامنه (DNS) و 68 درصد نیز پروتکل انتقال ابرمتن ایمن را نشانه رفته بودند. حملاتی که سرورهای رمزنگار را هدف قرار داده بودند افزایش رشد قابل ملاحظه داشتند، به طوری که 53

درصد از این مدل حملات لایه کاربردی و 43 درصد پروتکل SSL/TLS این سرورها را هدف قرار داده بودند. واقعیت این است که حملات DDoS نه‌تنها به‌نام یک برند آسیب جدی وارد می‌کند، بلکه اعتماد مشتریان آن برند را نیز تحت تأثیر قرار می‌دهد.
این گزارش نشان می‌دهد که نزدیک به 56 درصد شرکت‌ها اعلام داشته‌اند یک ضرر مالی 10 تا 100 هزار دلار را به‌واسطه این حملات تجربه کرده‌اند. جالب آنکه در این میان 88 درصد از ارائه‌دهندگان سرویس‌ها اعلام داشته‌اند برای مقابله با این گونه حملات به سراغ راه حل‌های مبتنی بر یادگیری ماشینی و الگوریتم‌های هوشمند رفته‌اند. در این میان 36 درصد از شرکت‌ها عنوان داشته‌اند الگوریتم‌های
یادگیری ماشینی باعث شده است تا کمتر زیرساخت‌های آن‌ها تحت تأثیر این حملات قرار گیرد. نکته قابل تأملی که در ارتباط با این گزارش وجود دارد این است که اکثر ارائه‌دهندگان سرویس‌ها و شرکت‌ها اعلام داشتند در زمینه جذب کارشناسان حرفه‌ای یا حفظ آن‌ها با مشکل روبه‌رو هستند. همین موضوع باعث شده است تا آن‌ها زمان کمی برای آموزش کارکنان در اختیار داشته باشند. در سال گذشته میلادی باج‌افزارها در رتبه اول تهدیدات و حملات منع سرویس توزیع شده در رتبه دوم قرار داشته‌اند. با وجود این، حملات DDoS تنها ارائه‌دهندگان سرویس‌ها را نشانه رفته بود. برای مشاهده کامل این گزارش به نشانی زیر مراجعه کنید:
http://www.securityweek.com/iot-devices-fuel-complex-ddos-attacks-report

منبع:

securityweek
تاریخ انتشار:
28 خرداد 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/12533/%D8%A8%DA%A9%D8%A7%D8%B1%DA%AF%DB%8C%D8%B1%DB%8C-%D8%AA%D8%AC%D9%87%DB%8C%D8%B2%D8%A7%D8%AA-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%A7%D8%B4%DB%8C%D8%A7-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D9%85%D9%86%D8%B9-%D8%B3%D8%B1%D9%88%DB%8C%D8%B3-%D8%AA%D9%88%D8%B2%DB%8C%D8%B9-%D8%B4%D8%AF%D9%87-%D9%BE%DB%8C%DA%86%DB%8C%D8%AF%D9%87