چرا حملات باج‌افزاری تا به این اندازه محبوب شده‌اند؟

2019 سال حملات انکار سرویس توزیع‌شده و باج‌افزارها

کارشناسان امنیتی معتقدند: شیوع باج‌افزارها به این دلیل جهان‌شمول شده که حتی کاربران غیرحرفه‌ای و فاقد تجربه فنی با اتکا بر ابزارهای آماده، بدون دردسر خاصی می‌توانند زیرساخت‌های یک شبکه عظیم سازمانی را قربانی کنند. شاید این پرسش برای شما به وجود آید که چرا حملات باج‌افزاری تا به این اندازه محبوب شده‌اند؟ پاسخ ساده است. پیاده‌سازی این مدل حملات ساده بوده، خطرهای جدی را به شکل مستقیم متوجه هکرها نکرده و هزینه پیاده‌سازی آن ناچیز بوده است. هکرها و مجرمان سایبری از باج‌افزارها برای هدف قرار دادن سامانه‌های حیاتی همچون فایل سرورها و بانک‌های اطلاعاتی استفاده می‌کنند. حمله به سامانه‌ها و زیرساخت‌های سازمان‌ها در مقایسه با حمله به کامپیوترهای شخصی سود کلانی عاید هکرها می‌کند، زیرا صدها دستگاه مسیریاب و سوییچ قربانی می‌شوند. عدم رعایت اصول اولیه امنیتی مانند تهیه نسخه پشتیبان از فایل‌ها، ضریب موفقیت این حملات را دوچندان کرده است. هر اندازه بر تعداد سامانه‌ها و تجهیزاتی که در اثر یک حمله آسیب می‌بینند، افزوده شود، هکرها می‌توانند به همان نسبت باج بیشتری طلب کنند. از سوی دیگر، حملات انکار سرویس توزیع‌شده قرار دارند که شبکه‌های توزیع محتوا بهترین دفاع در برابر آن‌ها به شمار می‌روند. حملات سیلابی بزرگ در کسری از ثانیه می‌توانند خسارت‌های مالی فراوانی به وجود آورند. حملاتی که هیچ سازمانی دوست ندارد حتی برای یک‌بار هم که شده ضعیف‌ترین مدل آن را تجربه کند.

حملات انکار سرویس توزیع‌شده قدرتمندتر شده‌اند

گزارش شرکت ترندمیکرو نشان می‌دهد، از تعداد **حملات منع سرویس توزیع‌شده** کاسته شده، اما در مقابل بر شدت این حملات افزوده‌شده است. این گزارش نشان می‌دهد، در سه‌ماهه نخست سال 2018 نزدیک به 23 درصد از حجم **حملات انکار سرویس توزیع‌شده** کاسته شده، اما در مقابل شدت و قدرت این مدل حملات 26 درصد بیشتر از قبل شده است. آمارها نشان می‌دهند، **حملات انکار سرویس توزیع‌شده** در سال جاری میلادی قدرتی به‌مراتب بیشتر از سال‌های قبل داشته‌اند. به‌گونه‌ای که در برخی از موارد شدت این حملات به 10 گیگابیت بر ثانیه هم رسیده است. پژوهشگران ترندمیکرو اعلام داشته‌اند: در سه‌ماهه نخست سال 2018 حمله‌ای با قدرت 120 گیگابیت بر ثانیه را شناسایی کرده‌اند. حمله‌ای که نزدیک به 90 میلیون بسته در هر ثانیه ارسال می‌کرد. در این حمله که نزدیک به 15 ساعت به طول انجامید، سیل عظیمی از بسته‌های اطلاعاتی، با شدت 60 گیگابیت بر ثانیه به سمت شبکه هدف ارسال‌شد. پژوهشگران ترندمیکرو گفته‌اند: در این حمله هکرها از رویکرد ماندگاری و از بدافزار معروف و قدرتمند اینترنت اشیا موسوم به Mirai استفاده کرده بودند. متیو بینگ، کارشناس امنیتی ترندمیکرو گفته است: «هکرها اکنون به دنبال آن هستند تا از Miria برای ساخت شبکه‌ای از بات‌نت‌های لینوکسی استفاده کنند و به این جمع‌بندی کلی رسیده‌اند که دوربین‌ها و روترها قدرت بالایی در اختیار آن‌ها قرار نمی‌دهند. در نتیجه به فکر افتاده‌اند که به سرورهای لینوکسی نفوذ کنند.» در بخشی از گزارش ترندمیکرو آمده است: «در 57 درصد از **حملات انکار سرویس توزیع‌شده** هکرها از انواع مختلفی از بردارهای حمله استفاده کرده‌اند، در 46 درصد از حملات هکرها از تکنیک ارسال حجیم بسته‌های اطلاعاتی مبتنی بر UDP و در 23 درصد از حملات مبتنی بر پروتکل TCP استفاده

کرده‌اند. در این میان زیرساخت‌های ابری بیش از سایر صنایع و سرویس‌ها در معرض **حملات انکار سرویس توزیع‌شده** قرار داشته‌اند.»

مطلب پیشنهادی

دفاع در برابر حمله منع سرویس انکار شده
راهکارهایی برای شناسایی و دفع حمله منع سرویس توزیع شده (DDoS)

حملات منع سرویس توزیع‌شده فقط سازمان‌ها را هدف قرار نمی‌دهند

رفتار هکرها کمی با گذشته تغییر پیداکرده است. در گذشته، هکرها الگوی مشخص و شناخته‌شده‌ای داشتند و فقط به سراغ زیرساخت‌های یک سازمان مشخص می‌رفتند. اما اکنون هکرها یک گام جلوتر رفته‌اند و نه‌تنها زیرساخت سازمان‌های بزرگی همچون داین را هدف قرار می‌دهند، بلکه به سراغ سایت‌های دولتی و حتی سایت‌های متعلق به افراد سرشناسی همچون رایان کربس (کارشناس مسائل امنیتی) نیز می‌روند. رشد روزافزون گجت‌های اینترنت اشیا، یکی از عوامل اصلی بزرگ‌تر و گسترده‌تر شدن این مدل حملات است. در نگاه اول بسیاری از کاربران می‌پندارند که سازوکار منسجمی برای مقابله با این مدل حملات وجود ندارد، اما با رعایت برخی اقدامات پیشگیرانه می‌توانیم مانع از آن شویم تا ناخواسته به یکی از بازیگران این گونه حملات تبدیل شده و روتر یا دستگاه هوشمند ما ناخواسته به زیرساخت شبکه‌ای حمله کند، بدون آن‌که خود از این موضوع مطلع باشیم. ترندمیکرو معتقد است: «در اغلب موارد **حملات منع سرویس انکار شده** پوششی برای سایر حملات بوده و پس از اجرای موفقیت‌آمیز این حمله، در مرحله بعد هکرها بدافزارهای خاص‌منظوره‌ای به شبکه یک سازمان تزریق می‌کنند.» در این گزارش آمده است، یک **حمله انکار سرویس توزیع‌شده** این پتانسیل را دارد تا میلیون‌ها دلار خسارت به ابر سازمان‌های بزرگ وارد کند. درحالی‌که شدت و قدرت این‌گونه حملات رشد دو برابری داشته و به 50 گیگابیت بر ثانیه رسیده است، اما متاسفانه سازمان‌ها و حتی کاربران حداقل تمهیدات امنیتی لازم را برای مقابله با این‌گونه حملات اتخاذ نکرده‌اند.

مطلب پیشنهادی

کاربرد دوگانه فناوری‌های رایج
۱۰ فناوری کاربردی که هکرها آن‌ها را به ابزارهای حمله تبدیل می‌کنند

گزارش موسسه BCI چه می‌گوید؟

موسسه تداوم تجارت (BCI) به‌تازگی پژوهشی انجام داده و نتایج آن را منتشر کرده است. این پژوهش نشان می‌دهد، سال گذشته میلادی حدود 64 درصد از شرکت‌های کوچک و بزرگ سراسر جهان حداقل یک اختلال سایبری در زیرساخت‌های خود تجربه کرده‌اند. در این پژوهش از 734 نفر از مدیران ارشد شرکت‌ها که در 69 کشور جهان به فعالیت اشتغال داشتند، درباره مشکلات و اختلالات سایبری سوال شد. این پژوهش نشان داد، تقریبا نیمی از این افراد در یک سال گذشته حداقل 10 مرتبه اختلالات و مشکلات سایبری را در زیرساخت‌های خود شناسایی کرده‌اند. در این گزارش واژه اختلال به هرگونه رخداد اینترنتی که به‌طور مستقیم بر کارکرد یک سازمان تاثیر منفی می‌گذارد، تعریف شده است. در این میان سهم حملات فیشینگ و مهندسی اجتماعی بیش از 57 درصد بوده است. موسسه فوق پیشنهاد داده، سازمان‌ها باید در سریع‌ترین زمان ممکن آموزش‌های لازم را برای مشتریان و کارمندان خود به مرحله اجرا درآورند. بر اساس این گزارش در سال 2015 میلادی حملات فیشینگ تنها 8 درصد عامل بروز مشکلات امنیتی بوده، اما در سال 2016 این رقم 21 درصد افزایش رشد داشته است. درحالی‌که 67 درصد از شرکت‌ها اعلام کرده‌اند، در بازه زمانی یک‌ساعته قادر به دفع این حملات هستند و در مقابل 16 درصد اعلام کرده‌اند، دفع حملات حداقل چهار ساعت به طول انجامیده است. درحالی‌که 33 درصد از شرکت‌ها گفته‌اند، یک اختلال امنیتی

نزدیک به 50 هزار یورو برای آن‌ها هزینه‌بر بوده(خسارت به بار آورده است)، در مقابل 13 درصد از شرکت‌ها اعلام داشته‌اند یک اختلال امنیتی بیش از 250 هزار دلار خسارت به بار آورده است. حملاتی که نزدیک به دو سال پیش از سوی باج‌افزارهای واناکرای و نات‌پتیا به وقوع پیوست، نشان داد حتی زیرساخت شرکت‌های بزرگ نیز در برابر اختلالات امنیتی آسیب‌پذیر هستند. موسسه تداوم تجارت معتقد است: «سازمان‌ها زمانی قادر هستند در برابر تهدیدات امنیتی از خود محافظت کنند که دپارتمان‌های فناوری اطلاعات با بخش امنیت اطلاعات در تعامل باشند و تیم پاسخگویی سریع به رخدادهای امنیتی کامپیوتری (CSIRT) در یک سازمان وجود داشته باشد.»

پژوهش ورایزن اطلاعات نگران‌کننده‌ای ارائه می‌دهد

براساس گزارش شرکت ورایزن، باج‌افزارها به یکی از شایع‌ترین گونه‌های بدافزاری تبدیل‌شده‌اند که به شکل مستقیم و روبه‌رشدی کسب‌وکارها را هدف قرار داده‌اند. گزارش بررسی افشای اطلاعات (Data Breach Investigations Report) شرکت ورایزن نشان می‌دهد، هکرها به دنبال آن هستند تا رخنه‌ای در زیرساخت‌های ارتباطی یک سازمان پیداکرده یا حساب‌های کاربری رده بالا (مدیریتی) را هک کرده و باج‌افزار خود را به درون شبکه‌های ارتباطی یک سازمان تزریق کرده و همه فایل‌ها و گزارش‌های مهم شرکت را رمزگذاری کنند. در تهیه این گزارش داده‌های 67 سازمان مختلف، بیش از 53 هزار حمله هکری و بیش از 2200 مورد افشای رکوردهای اطلاعاتی در 65 کشور جهان ملاک ارزیابی قرارگرفته است. در این گزارش آمده است، در 39 درصد از حملات هکری باج‌افزارها به شکل مستقیم استفاده‌شده‌اند. برایان سارتین، مدیر اجرایی بخش خدمات امنیتی شرکت ورایزن گفته است: «در ارتباط با پژوهش انجام‌شده نکته قابل تاملی وجود دارد. باوجود اخبار متعدد منتشرشده در ارتباط با باج‌افزارها و خسارت‌های سنگینی که تا به امروز به شرکت‌ها وارد کرده‌اند، هنوز هم بسیاری از شرکت‌ها و کسب‌وکارها هیچ‌گونه تمهیدات خاصی برای مقابله با حملات باج‌افزاری در دستور کار خود قرار نداده و مهم‌تر از آن بودجه قابل‌توجهی برای به‌کارگیری مکانیزم‌های امنیتی برای مقابله با باج‌افزارها تخصیص نداده‌اند. به عبارتی شرکت‌ها در زمان رویارویی با یک حمله باج‌افزاری تنها گزینه پرداخت باج را پیش روی خود دارند. پس نباید تعجب کنیم، در این میدان بازی، هکرها برنده همیشگی میدان باشند. پس وظیفه شرکت‌های امنیتی این است که با تمام وجود تلاش کنند تا به کسب‌وکارها نشان دهند با به‌کارگیری زیرساخت‌های امنیتی درست در برابر هکرها مصون بمانند. شما تنها زمانی می‌توانید از اصول مطمئنی برای محافظت از خود در برابر حملات استفاده کنید که در ابتدا درک درستی از تهدیدات به دست آورید.»

در یازدهمین گزارش منتشرشده این شرکت آمده است، انگیزه مالی دلیل اصلی اغلب حملات هکری بوده که باعث افشای نزدیک به 76 درصد رکوردهای اطلاعاتی شده؛ جاسوسی‌های سایبری (صنعتی) در مکان دوم قرار داشته که نزدیک به 13 درصد افشای اطلاعات را به همراه داشته‌اند. درحالی‌که نیمی از حملات رخ‌داده از طریق هکرهای سازمان‌یافته انجام‌شده، در مقابل 12 درصد حملات از سوی هکرهایی بوده که تحت حمایت نهادهای خاصی قرار داشته‌اند. همچنین سه چهارم حملات از جانب هکرهایی بوده که در ظاهر به هیچ ارگان یا نهادی وابسته نبوده‌اند. تقریبا نیمی از حملات هکری را که شرکت ورایزن تحلیل کرده، در ارتباط با نفوذهایی بوده که از طریق به‌کارگیری بدافزارها رخ داده است. از هر 5 مورد حمله موفقیت‌آمیز، یک مورد به دلیل سهل‌انگاری کارمندان با موفقیت به ثمر رسیده است. از جمله این اشتباهات می‌توان به پیکربندی اشتباه وب‌سرورها، ارسال ایمیل اشتباهی برای افراد و عدم امحاء اسناد محرمانه اشاره کرد. اطلاع‌رسانی دقیق در ارتباط با حملات فیشینگ، باعث شده 76 درصد کارکنانی که در شرکت‌های مختلف شاغل هستند، با مشاهده لینک‌های فیشینگ، این مسئله را تشخیص داده و روی لینک‌های

مشکوک کلیک نکنند که این اطلاع‌رسانی کاهش 4 درصدی را نشان می‌دهد. اما دقت کنید، اگر تنها یک حمله فیشینگ با موفقیت به سرانجام برسد، به هکرها اجازه می‌دهد به سامانه‌های درون‌سازمانی دسترسی پیدا کنند. در این گزارش ذکر شده کارمندانی که در بخش منابع انسانی کار می‌کنند، به‌شدت موردتوجه هکرها قرار دارند، زیرا هکرها درصدد هستند، به اطلاعات شخصی افراد دست پیداکرده و از این اطلاعات برای نشان دادن پرداخت‌های مالی جعلی استفاده کنند.

تاریخ انتشار:

09 بهمن 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/14509/2019-%D8%B3%D8%A7%D9%84-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D8%A7%D9%86%DA%A9%D8%A7%D8%B1-%D8%B3%D8%B1%D9%88%DB%8C%D8%B3-%D8%AA%D9%88%D8%B2%DB%8C%D8%B9%E2%80%8C%D8%B4%D8%AF%D9%87-%D9%88-%D8%A8%D8%A7%D8%AC%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%D9%87%D8%A7