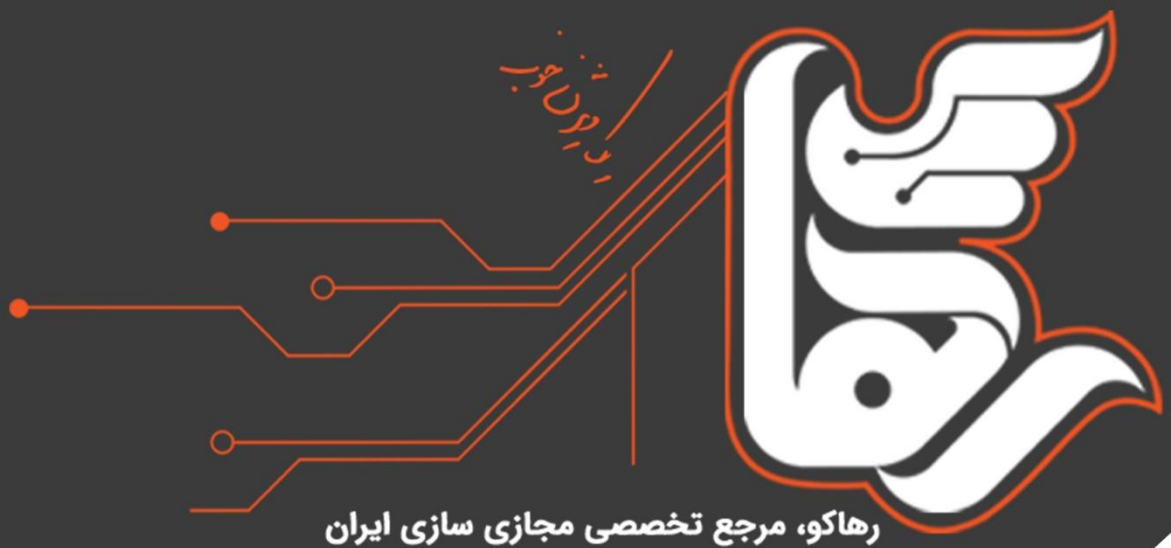
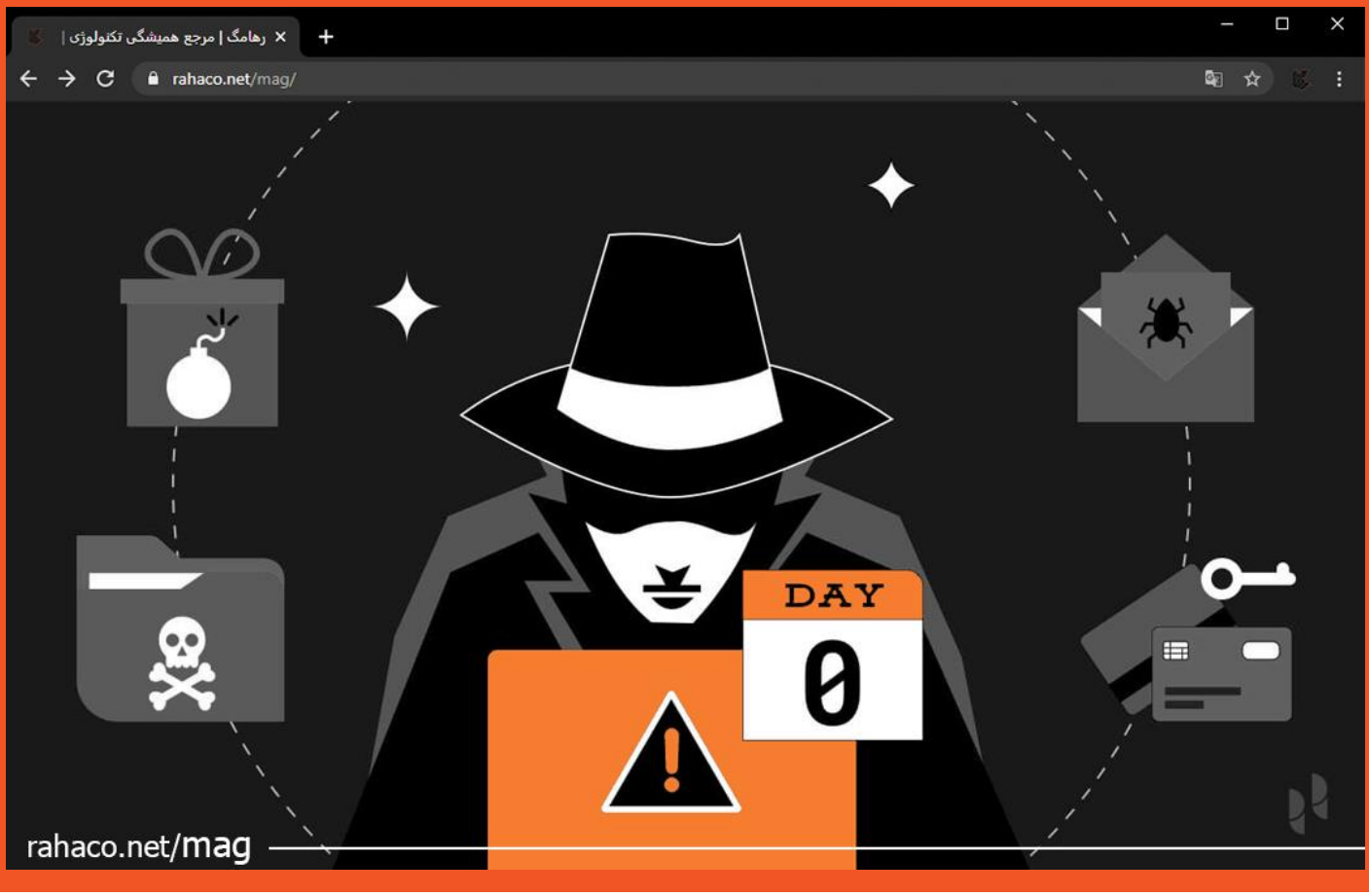


مجله رهاکو

RAHA MAG

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک 12
www.rahaco.net کدپستی1583616414 تلفن :02154521



فهرست

چرا به آن روز صفر می گویند؟ 3
حملات روز صفر چگونه کار می‌کند؟ 3
چگونه می‌توانید در برابر حملات روز صفر از خود محافظت کنید؟ 4
کشف حملات روز صفر 4
نمونه‌هایی از حملات روز صفر 4
چرا حملات روز صفر خطرناک اند؟ 4
نتیجه گیری 5

در برابر حمله روز صفر چه می‌توان کرد؟

اصطلاح "روز صفر" در دنیای امنیت سایبری نسبتا رایج است. در ماه‌های اخیر، شرکت‌های فناوری برتر از مایکروسافت و گوگل گرفته تا اپل مجبور بوده‌اند حمله روز صفر را اصلاح کنند، اما این به چه معناست؟ در ادامه نحوه عملکرد و نحوه محافظت در برابر آن‌ها را توضیح می‌دهیم.

چرا به آن روز صفر می گویند؟

اصطلاح «روز صفر» به آسیب پذیری اشاره دارد که بدون اطلاع سازنده نرم افزار آن‌ها را در معرض حمله قرار می‌دهد. یعنی هنگامی که با مشکل مواجه شدند، "صفر روز" برای رفع آن فرصت دارند و هیچ فرصتی برای جبران نخواهند داشت. آسیب پذیری روز صفر یک ضعف نرم افزاری است که قبل از اینکه سازنده نرم افزار از آن آگاه شود، مهاجم به آن حمله می‌کند. از طرفی دیگر، هکرها از این حمله جهت ورود به سیستم برای سرقت داده یا آسیب زدن استفاده می‌کنند. بنابراین این آسیب پذیری یک نقطه ضعف است. آسیب پذیری روشی است که هکرها به نرم افزار وارد می‌شوند و حمله زمانی است که هکر از این آسیب پذیری برای ایجاد آسیب استفاده می‌کنند.

حملات روز صفر چگونه کار می‌کند؟

حتی با وجود توسعه دهندگان و تولیدکنندگان نرم افزار که سخت‌کوشانه محصول خود را از نظر نقص بررسی می‌کنند، اشتباهاتی رخ می‌دهد و هکرها به دنبال نقاط ضعف یا منافذی هستند تا از آن‌ها سوء استفاده کنند. هنگامی که مهاجم سایبری نقاط ضعف و آسیب پذیری را پیدا کرد، می‌تواند با نوشتن کد از آن استفاده کند. اینکه آن کد چیست و چه کاری انجام می دهد به نوع آسیب پذیری‌هایی که کشف شده است بستگی دارد. گاهی اوقات مهاجمان فقط با استفاده از حمله روز صفر می‌توانند به سیستم دسترسی پیدا کنند. اگر نتوانند این کار را انجام دهند، سعی می‌کنند با فریب افراد به آن وارد شوند.

مهاجمان سایبری اغلب این کار را از طریق مهندسی اجتماعی انجام می‌دهند؛ تکنیکی که از لحاظ روانی انسان تاثیر می‌گذارد تا آن‌ها را فریب دهد. کلاهبرداری‌های فیشینگ که پیام‌های تهدید آمیزی برای ترساندن مردم جهت انجام اقدام مورد نظر خود ارسال می‌کند، نمونه‌ای از این مدل است. به عنوان مثال، کلاهبردار با ارسال یک ایمیل جعلی که به نظر می‌رسد از بانک ارسال شده می‌گوید که حساب شما هک شده است و «برای جزئیات بیشتر اینجا را کلیک کنید». مهندسی اجتماعی تقریبا در تمام جنبه‌های حملات سایبری استفاده می‌شود. حمله روز صفر تا ماه‌ها قبل از شناسایی وجود دارد و در طول این مدت، مهاجمان می‌توانند با سرقت داده‌ها و آسیب رساندن به سیستم‌های حساس منتظر شوند تا زمانی که نرم افزار دستکاری شده اجرا شود. هکرها اغلب اطلاعات مربوط به حملات روز صفر را در دارک وب با مبالغ هنگفتی به فروش می‌رسانند. حملات Zero-day بسیار بیشتر از رمز عبور ایمیل یا حتی داده‌های بانکی مشکل ایجاد می‌کنند. اهداف این حملات از گذرواژه‌ها و اطلاعات شخصی گرفته تا آسیب‌پذیری‌ها متغیر است.

چگونه می‌توانید در برابر حملات روز صفر از خود محافظت کنید؟

ماهیت حمله روز صفر محافظت از آن‌ها را سخت می‌کند، اما تا حدودی در برابر این نوع حملات می‌توان از خود دفاع کرد. برای شروع، تمام سیستم‌ها و نرم افزارهای خود را به روز نگه دارید. در سال 2017، حملات بدافزار WannaCry از آسیب پذیری‌های سیستم‌های مایکروسافت ایجاد شد که با به روز رسانی رایگان میشد در برابر آن از سیستم محافظت کرد. بنابراین هر چقدر هم که وسوسه انگیز به نظر برسد، به هیچ عنوان روی گزینه «Remind me later» کلیک نکنید. با دانلود برنامه‌هایی که می‌دانید ضروری هستند و واقعا از آن‌ها استفاده می‌کنید از سیستم خود محافظت نمایید. هرچه برنامه‌های بیشتری داشته باشید، راه‌های بیشتری برای ورود به سیستم شما در اختیار مهاجم قرار می‌گیرد.

نرم افزار آنتی ویروس و ضد بدافزار یک حرکت مثبت است. آن‌ها معمولا به اطلاعات تهدید آمیز گذشته متکی هستند و اغلب به روز می‌شوند. نرم افزارهای خود را طوری تنظیم کنید که به طور خودکار اسکن‌های منظم انجام دهند تا آن را فراموش نکنید. برای ایجاد لایه امنیتی، فایروال یک گزینه مناسب است. در مرحله آخر باید به اعضای سازمان خود آموزش‌های لازم را ارائه دهید.

کشف حملات روز صفر

خبر خوب این است که فقط هکرها به دنبال این نقاط ضعف نیستند. شرکت‌های نرم افزاری و فناوری اغلب با استفاده از هکرهای «کلاه سفید» یا «کلاه خاکستری» سیستم‌های خود را در برابر حمله آزمایش می‌کنند تا قبل از ورود محصولاتشان به بازار، آسیب‌پذیری‌ها را تشخیص دهند. برخی از فروشندگان این آسیب‌پذیری‌ها را جمع آوری کرده و به اشتراک می‌گذارند. بخش اطلاعات ابری سیسکو به نام Talos Intelligence، یکی از این شرکت‌هاست که آسیب‌پذیری‌های گزارش شده توسط کاربر از جمله حملات روز صفر را در وب‌سایت خود فهرست کرده است.

نمونه‌هایی از حملات روز صفر

در سال 2020، یک شرکت بزرگ فناوری اطلاعات در ایالات متحده هدف حمله روز صفر قرار گرفت. هکرها کدهای مخرب را به نرم افزار شرکت وارد کردند و آن شرکت به‌طور ناآگاهانه کدهای آلوده را بین مشتریانش توزیع کرد. نرم افزار در معرض خطر بود و این بد افزار یک «پنجره» برای دسترسی به اطلاعات مشتریان نصب کرد. براساس گزارش وال استریت ژورنال، این آسیب تا ماه‌ها ناشناخته باقی ماند و منجر به آسیب پذیری‌های روز صفر در 18000 سازمان از جمله صدها شرکت بزرگ و سازمان‌های دولتی شد. مورد دیگر در سال 2020 اتفاق افتاد. هکرها با یک حمله روز صفر به یک پلتفرم ویدئو کنفرانس محبوب به رایانه‌های قدیمی دسترسی پیدا کردند. هکرها کامپیوترهای کاربران را از راه دور کنترل کردند و حدود 500000 رمز عبور را به سرقت بردند و آن‌ها را در دارک وب به فروش گذاشتند.

چرا حملات روز صفر خطرناک اند؟

چیزی که حمله روز صفر را خطرناک می‌کند این است که برخی از مهاجمان سایبری حرفه‌ای از این حملات به صورت استراتژیک استفاده می‌کنند. این گروه‌ها حملات روز صفر را برای اهداف با ارزش مانند موسسات پزشکی یا مالی یا سازمان‌های دولتی

انجام می‌دهند. در این فرایند کشف آسیب پذیری توسط قربانی سخت می‌شود و طول عمر آسیب رسانی افزایش می‌یابد. کاربران همچنان باید سیستم‌های خود را به روز کنند. اگر این کار را انجام ندهند، مهاجمان می‌توانند تا مدت‌ها از اثرات این حمله سوء استفاده کنند.

نتیجه گیری

حملات روز صفر تقریبا 80 درصد از کل حملات بدافزار را تشکیل می‌دهند. در این حمله هکرها در کمین‌اند تا آسیب پذیری نرم افزاری را پیدا کنند بدون اینکه شما متوجه آن شوید. یکی از عناصر کلیدی در محافظت در برابر حملات روز صفر، داشتن یک برنامه مناسب و امن برای مقابله با آن‌هاست. یک واکنش سریع و کنترل شده به حمله روز صفر می‌تواند به کاهش تاثیر آن کمک کند.