حفره‌های Adobe در سالی که گذشت

محمد مهدی واعظی نژاد

شرکت Adobe در طول یک سال گذشته با حفره‌های متعددی در نرم‌افزارهای کاربردی و پرطرفدار خود مواجه بود که با وجود تمام تلاش‌های این شرکت برای انتشار سریع اصلاحیه‌های امنیتی، بازهم تا زمان انتشار این وصله‌ها، به طور گسترده‌ای مورد سوءاستفاده نفوذگران قرار گرفت.

با توجه به گستردگی جغرافیایی و دامنه کاربرد نرم‌افزارهای Adobe، حملات صورت گرفته توانست در گستره وسیعی از کشورهای جهان، کاربران بی‌شماری را تحت تأثیر خود قرار داده و فعالیت‌های مخرب را روی سیستم‌های رایانه‌ای آنها انجام دهند.

هکرها سال گذشته و بخصوص در آخرین ماه‌های پایانی آن، تمرکز بسیاری روی محصولات Adobe داشتند و با شناسایی نقاط ضعف متعدد در نرم‌افزارهای محبوب این شرکت و انتشار کدهای مخرب آنها یکی پس از دیگری توانستند حملات بزرگی را در سراسر جهان ترتیب دهند که این مسأله با واکنش‌های شدیدی در مجامع امنیتی مواجه شد.

یکی از عملیات‌های جاسوسی سایبری سال گذشته که اسفند توسط شرکت کسپرسکی با همکاری دانشگاه بوداپست مجارستان کشف شد، می‌توانست با سوءاستفاده از نقاط ضعف موجود در نرم‌افزار Adobe Reader که اگرچه قبلا توسط شرکت Adobe ترمیم شده بود، برای نفوذ و دسترسی غیرمجاز به رایانه قربانی از طریق نامه‌های الکترونیک حاوی یک فایل pdf مخرب بهره ببرد.

این حمله که از طریق نامه‌های الکترونیک هدفمند به قربانیانی خاص ـ که دریافت کننده این نامه‌ها نیز از قبل شناسایی و انتخاب شده و شامل ارگان‌های بین‌المللی و پیمان‌های همکاری جهانی بود ـ توانست در طول یک سال فعالیت مخفیانه خود، ۵۹ رایانه را در ۲۳ کشور مختلف جهان مورد هدف قرار دهد.

این حمله که با نام MiniDuke نامگذاری شد، شامل یک بدافزار ۲۰ کیلوبایتی و نوشته شده به زبان Assembler بود که شناسایی آن با توجه به قربانیان خاص خود، بازتاب بسیار وسیعی را در سطح جهان داشت.

دوم اسفند ۹۱ نیز شرکت Adobe در یک به‌روزرسانی اضطراری، نسخه‌های به‌روز شده‌ای از نرم‌افزارهای Adobe Reader و Acrobat را منتشر کرد که شامل نسخه‌های ۹، ۱۰ و ۱۱ این دو نرم‌افزار می‌شد. این به‌روزرسانی‌ها برای رفع دو حفره امنیتی با درجه حیاتی در این دو نرم‌افزار بود که پس از سوءاستفاده‌های متعدد، مدتی قبل (بیست و ششم بهمن ۹۱) توسط شرکت امنیتی FireEye همراه برنامه مخربی که از این نقاط ضعف سوءاستفاده می‌کند، کشف شده بودند.

هر یک از این حفره‌ها امکان دور زدن تدابیر امنیتی Sandbox در نرم‌افزارهای Adobe Reader و Acrobat را فراهم نموده و سوءاستفاده از آنها باعث از کار افتادن سیستم یا ایجاد دسترسی غیرمجاز به رایانه هدف، به منظور جمع‌آوری و ارسال اطلاعات و مشخصات شخصی کاربران می‌شود.

گفتنی است پس از شناسایی این دو حفره، شرکت Adobe که آنها را «مهم» به شمار می‌آورد، برای مقابله با آنها تنها به ارائه راه‌حل موقت که شامل فعال‌کردن گزینه Files from potentially unsafe locations در قسمت Protected view در این نرم‌افزارها بود، اقدام کرده و ده روز بعد به انتشار نسخه‌های جدید و اصلاح شده این نرم‌افزارهای خود پرداخت. فعال‌سازی این گزینه اجازه اجرای خودکار برنامه‌های اجرایی را در محیط Acrobat و Reader نداده و فقط با تائید کاربر، چنین برنامه‌هایی قابل اجرا خواهد بود. برای فعال‌سازی این گزینه، ابتدا نرم‌افزار Reader یا Acrobat را باز کرده، روی منوی Edit کلیک کرده، گزینه Preferences را انتخاب سپس روی گزینه Security (یا Security Enhanced) کلیک می‌کنیم.

نرم‌افزار Flash که از دیگر محصولات کاربردی شرکت Adobe محسوب می‌شود نیز سال گذشته دور از دید هکرها نماند و هکرها توانستند با سوءاستفاده از حفره‌های موجود در این نرم‌افزار، عملکرد رایانه‌های کاربران را مختل کرده و همچنین کنترل آنها را در دست گیرند.

یکی از آسیب‌پذیری‌های Flash که اوایل اسفندماه سال گذشته کشف شد، از طریق لینک‌های مخرب ارسالی به کاربران و سپس هدایت آنها به سمت سایت‌های حاوی محتوای فلش آلوده، مورد سوءاستفاده قرار گرفت که شرکت Adobe برای رفع این نقص، مجبور به انتشار اصلاحیه فوری شد و با انتشار سه وصله امنیتی سعی کرد تا از نفوذ بیشتر هکرها جلوگیری کند.

جدیدترین آسیب‌پذیری‌های Flash در سال گذشته، سعی داشت توسط پلاگین‌های نصب شده روی مرورگرها، مورد بهره‌برداری قرار گیرد که در این میان، مرورگر فایرفاکس به علت افزونه‌های زیاد آن، مورد توجه بیشتری قرار گرفت.

Flash Player، از دیگر محصولات بسیار محبوب شرکت Adobe هم در ماه پایانی سال گذشته با دو آسیب‌پذیری اصلاح نشده در نسخه ۱۱/۵ خود به طور گسترده توسط مهاجمان و نویسندگان بدافزار مورد سوءاستفاده قرار گرفت. با شناسایی این حفره‌ها، شرکت Adobe به انتشار یک اصلاحیه برای این نرم‌افزار اقدام و طی اطلاعیه‌ای از کاربران سیستم‌عامل‌های ویندوز، مکینتاش، لینوکس و اندروید درخواست کرد تا در اسرع وقت، فلش را روی رایانه‌های خود به‌روزرسانی کنند.

شرکت Adobe همچنین در روز سه‌شنبه هشتم اسفند ۱۳۹۱، به به‌روزرسانی نرم‌افزار Flash Player برای اصلاح سه نقطه ضعف موجود در این نرم‌افزار اقدام کرد که دو نقطه ضعف آن، به طور جدی مورد سوءاستفاده هکرها قرار گرفته و کاربران مرورگر فایرفاکس را با تهدید روبه‌رو کرد. توسط این آسیب‌پذیری‌ها، کاربران مرورگر فایرفاکس به روش‌های مختلفی فریب داده می‌شدند تا روی لینک‌هایی کلیک کنند که آنها را به سمت سایت‌های مخرب هدایت می‌کرد. در این سایت‌ها، برنامه‌های مخرب فلش در متن صفحات، پنهان گشته و تنها پس از به نمایش درآمدن صفحات، اجرا شده و امکان سوءاستفاده از نقاط ضعف شناسایی شده را فراهم می‌کردند.

انتشار این اصلاحیه که دومین به‌روزرسانی نرم‌افزار Flash Player در کمتر از یک ماه و سومین به‌روزرسانی فوق‌العاده شرکت Adobe برای محصولات خود بود، موج شدیدی از اعتراض‌های کارشناسان امنیتی را نسبت به اعمال نشدن کنترل‌های امنیتی در نرم‌افزارهای Adobe دربرداشت؛ زیرا شرکت Adobe روز سه‌شنبه بیست و چهارم بهمن، برای برطرف‌سازی ۱۷ حفره امنیتی موجود در نرم‌افزار Flash Player اقدام به انتشار نسخه‌های به‌روزشده جدیدی برای این نرم‌افزار را منتشر کرده بود و چند روز قبل از آن نیز با انتشار یک نسخه فوق‌العاده و فوری برای نرم‌افزار Flash Player تلاش کرد تا چند حفره امنیتی را که توسط هکرها مورد سوءاستفاده قرار گرفته بود، برطرف کند.

این شرکت همچنین علاوه بر ارائه نسخه‌های جدیدی از این نرم‌افزار، نسخه‌های فلش را که در مرورگرهای کروم و اینترنت اکسپلورر به کار رفته است هم به‌روز کرد.

بیست و سوم اسفند، شرکت Adobe برای پنجمین بار در سال ۲۰۱۳ اقدام به به‌روزرسانی Flash Player کرد تا چهار آسیب‌پذیری بحرانی آن را برطرف کند. این اصلاحیه که به صورت APSB13-09 مشخص شده است، توانست یک مشکل استفاده پس از آزادسازی، چند سرریز بافر و یک رخنه نامشخص تخریب حافظه را ترمیم کند. از این آسیب‌پذیری‌ها برای اجرای کدی مخرب، هک‌کردن فلش و ارتباط با یک رایانه شخصی ویندوز یا مکینتاش استفاده می‌شود.

تمام این اقدام‌ها در حالی است که شرکت Adobe هنوز نتوانسته است مشکلاتی را که در مسابقه pwn2own توسط یک محقق آسیب‌پذیری فرانسوی، کشف شده و به هک‌کردن فلش منجر شود اصلاح کند و برطرف سازی آن را در اصلاحیه بعدی فلش وعده داده است.

نرم‌افزار Shockwave که یکی دیگر از محصولات شرکت Adobe است نیز از این به‌روزرسانی‌ها دور نماند و در بیست و چهارم بهمن توسط شرکت Adobe به‌روزرسانی شد.

با این حال، توصیه همیشگی ما به کاربران این است که به محض انتشار یک اصلاحیه، هر چه سریع‌تر نسبت به دریافت و نصب وصله‌های امنیتی اقدام و همواره از نسخه‌های جدید و به‌روز شده نرم‌افزارها استفاده کنند.

منابع:

Blog.fireeye.com
Cnet.com
Adobe.com
ftp.adobe.com