سرقت گواهینامه‌های SSL برای سایت‌های مشهور

به دنبال سرقت تعدادی گواهینامه دیجیتال SSL (SSL Digital Certificate) برای برخی سایت‌های مشهور جهان، تمامی تولیدکنندگان مرورگر، مرورگرهای خود را بروز کردند.

روز سه شنبه ۲۴ اسفند سال گذشته (۱۳۸۹) افراد نفوذگر با استفاده از رمزهای عبور معتبر به شبکه یکی از موسسات صادرکننده گواهینامه SSL دسترسی پیدا کرده و اقدام به صدور ۹ گواهینامه غیر مجاز ولی معتبر برای سایت‌های مشهوری، نظیر Gmail، Yahoo، hotmail، Skype کردند.
موسسه صادرکننده گواهینامه‌ها (Comodo) در روز چهارشنبه سوم فروردین ماه سال جاری (۱۳۹۰) خبر سرقت گواهینامه‌ها را بطور عمومی اعلام کرد. در فاصله بین ۲۴ اسفند تا سوم فروردین ماه، گواهینامه‌های به سرقت رفته باطل شدند و موضوع به اطلاع شرکت‌های مایکرو سافت، Google و Mozilla رسید تا هرچه سریعتر مرورگرهای خود را بمنظورجلوگیری از سوءاستفاده از این گواهینامه‌ها بروز کنند.
شرکت Google روز پنجشنبه ۲۶ اسفند ۸۹ مرورگر Chrome خود را بروز کرد. شرکت مایکرو سافت و Mozilla نیز در روزهای دوم و سوم فروردین ماه ۹۰ مرورگرهای IE و Firefox را بروز کردند. در نسخه‌های بروز شده این مرورگرها، گواهینامه‌های به سرقت رفته شده در فرمت سیاه مرورگرها قرار گرفته تا در صورتیکه کاربر به سایت جعلی که توسط هریک از این گواهینامه‌ها به عنوان سایت واقعی معرفی می‌شوند، مراجعه کرد، هشدارهای لازم داده شود.

افرادی که این گواهینامه را در اختیار داشته باشند می‌توانند با ساختن سایت‌های جعلی مشابه سایت‌های واقعی (نظیر Gmail و Yahoo) و استفاده از گواهینامه، کاربران را فریب دهند و بدون هیچگونه هشدار و اعلام خطر از سوی مرورگر، کاربران به تصور اینکه در سایت‌های واقعی هستند، اقدام به وارد کردن رمز های عبور خود کنند. دراینصورت رمزهای کاربران در اختیار افراد خلافکار قرار خواهد گرفت. البته برای چنین عملیاتی، به تغییر آدرس اینترنتی (DNS) این سایت‌های مشهور نیاز است تا کاربران به سوی سایت‌های جعلی (به جای سایت‌های واقعی) هدایت شوند. انجام چنین تغییراتی معمولاً فقط در اختیار شرکت‌های مخابرات و گردانندگان اصلی اینترنت در هر منطقه و کشور است.

شرکت Google با انتشار نسخه Chrome10 و شرکت Mozilla با انتشار نسخه‌های جدیدی برای Firefox 3.5 و Firefox 3.6 اقدام به مقابله با سرقت گواهینامه‌ها کردند. نسخه جدید Firefox 4 قبل از انتشار عمومی اصلاح شده بود. شرکت مایکرو سافت نیز اقدام به ارائه اصلاحیه فوق‌العاده و خارج از برنامه ماهانه خود کرد. این اصلاحیه برای کاربرانی که از سرویس‌های بروزرسانی مایکروسافت استفاده می‌کنند، بطور خودکار نصب شده است.
اطلاعات بیشتر درباره این اصلاحیه در هشدار امنیتی شماره 2524375 ارائه شده است. دسترسی به این هشدار از طریق پیوند زیر امکان پذیر است.
www.microsoft.com/technet/security/advisory/2524375.mspx

لازم به توضیح است که در مرورگرهای IE7، Firefox3، Opera8، Chrome امکانی با عنوان Online Certificate Status Protocol(OCSP)وجود دارد که به صورت زنده در هنگام مراجعه به یک سایت، از معتبر بودن گواهینامه SSL آن سایت اطمینان حاصل می‌کند. اینکار با مراجعه به یک سرویس دهنده خاص (Certificate

Authority-CA) انجام می‌گیرد. پس به دلیل ابطال گواهینامه‌های به سرقت رفته، مرورگرها باید هشدارهای لازم را هنگام مواجهه با این گواهینامه‌ها نشان دهند. ولی در صورتیکه، به هر دلیلی مانند قطع ارتباط شبکه، امکان دسترسی مرورگر به سرویس دهنده CA فراهم نشوند، پیش فرض مرورگر، معتبر و اصل بودن گواهینامه است و مرورگر بدون نشان دادن هشداری، امکان دسترسی کاربر به سایت دارای گواهینامه جعلی را خواهد داد.

به دلیل اینکه موضوع همچنان در دست بررسی و تحقیق توسط مقامات امنیتی است، تا روز سوم فروردین ماه جزئیات و توضیحات بیشتر درباره دلایل این سرقت، محل نفوذ به شبکه موسسه صادر کننده گواهینامه، صاحب اصلی رمزهای عبور مورد استفاده توسط نفوذگران و ... منتشر نشده بود.

طی چند روز گذشته، یک شخص ناشناس ایرانی که خود را Ich Sun معرفی کرده است، با ارائه مدارک و اطلاعات دقیق، نشان داده که وی مسئول تمام این عملیات بوده است. در یک مصاحبه که از طریق نامه‌های الکترونیکی با وی صورت گرفت، این شخص مدعی شده است که به چند موسسه مشابه دیگر که گواهینامه‌های الکترونیکی صادر می‌کنند، نفوذ کرده است. این فرد اطلاعات بیشتری ارائه نکرده است.

رقابت تنگاتنگ مرورگرها

انتشار تقریباً همزمان نسخه‌های جدید دو مرورگر IE و Firefox، رقابت جدیدی بین این دو مرورگر بوجود آورد.

نسخه جدید IE9 روز دوشنبه ۲۳ اسفند ۸۹ از سوی شرکت مایکروسافت منتشر شد. در۲۴ ساعت اول پس از انتشار مرورگر IE9، نزدیک به ۲/۴ میلیون نسخه از این مرورگر توسط کاربران دریافت (download) شد. این رقم یعنی کاربر در هر ثانیه، اقدام به دریافت مرورگر IE9 کرده‌اند.

در مقابل، نسخه جدید **Firefox 4** که در روز سه شنبه دوم فروردین ۹۰ از سوی موسسه **Mozilla** منتشر شد، موفق شد رقم ۲/۴ میلیونی مایکروسافت را به سه برابر برساند. در ۲۴ ساعت اول از انتشار **Firefox 4** نزدیک به ۷ میلیون نسخه از این مرورگر توسط کاربران در اقصی نقاط جهان دریافت شد. البته این میزان در مقایسه با ۸ میلیون کاربر برای اولین روز انتشار نسخه فعلی **Firefox 3** کاهش اندکی را نشان می‌دهد.

یکی از دلایل برتری مرورگر جدید Firefox 4 به مرورگر IE9 که تا بحال اشاره زیادی به آن نشده است، سازگاری آن با سیستم عامل قدیمی Win XP است. مرورگر IE9 مایکروسافت در محیط های Win XP قابل استفاده نیست.

یکی از امکاناتی که در مرورگر IE9 به تقلید از مرورگر Firefox گنجانده شده، امکان "Do Not Track" است. این امکان به سایت‌هایی که رفتار کاربران را زیر نظر داشته و اطلاعاتی درباره سلایق و موارد مورد علاقه کاربر جمع‌آوری می‌کنند، هشدار می‌دهد.

به همراه هر درخواست ارسالی از طرف مرورگر، یک اطلاعات خاص نیز به سایت مورد درخواست ارسال می‌شود که مشخص می‌کند کاربرمایل نیست رفتارهایش زیر نظر گرفته شود و اطلاعاتی در این موارد توسط سایت جمع‌آوری شود. مرورگر IE9 امکان مشابهی با نام Tracking Protection از قبل دارد که فقط بر اساس فهرست‌های سیاه و سفید (مجاز و غیر مجاز) سایت‌ها عمل می‌کند. ولی امکان جدید Do Not Track توسط بسیاری از کارشناسان و صاحب‌نظران از مایکروسافت خواسته شده بود و امکان بسیار زنده و پویاتری نسبت به Tracking Protection است.

در کنار این رقابت تنگا تنگ بین دو سازنده بزرگ مرورگر در جهان، یک سنت قدیمی بین دو شرکت همچنان پایدار مانده است. گروه سازنده مرورگر IE همزمان با انتشار هر نسخه جدید از مرورگر Firefox یک کیک بزرگ برای گروه رقیب می‌فرستند. اولین بار در سال ۲۰۰۶ میلادی بود که گروه سازنده IE به مناسبت انتشار Firefox 2 کیک بزرگی فرستادند و اینکار را در سال ۲۰۰۸ برای Firefox 3 تکرار کردند. حالا هم گفته می‌شود که Firefox 4، یک Firefox نیست تا موقعی که کیک مایکروسافت برسد.

طبق آخرین آمار منتشر شده در ۱۲ فروردین ماه، مرورگر Firefox 4 با ۴۱ میلیون کاربر که در ده روز گذشته اقدام به دریافت این نسخه جدید کرده‌اند، اکنون نزدیک به ۴ درصد از بازار مرورگرها را در اختیار دارد. این میزان برای مرورگر جدیدIE9 فقط به ۱.۸درصد رسیده است.

نقاط ضعف جدید در Flash

روز دوشنبه ۲۳ اسفند ۸۹، شرکت Adobe از کشف یک نقطه ضعف امنیتی جدید در نرم‌افزار Flash Player خبر داد. طبق اطلاعیه این شرکت، مواردی از سوی استفاده از این نقطه ضعف نیز مشاهده و گزارش شده بود.

این نقطه ضعف جدید در نسخه Flash 10.2.152.33 و قدیمی‌تر از آن وجود دارد. همچنین این نقطه ضعف در دو نرم‌افزار Adobe Reader و Acrobat نیز قابل سوءاستفاده است. بخش authpaly.dll در این دو نرم‌افزار، وظیفه پردازش Flash را در درون فایل‌های PDF بر عهده دارد و لذا در صورت وجود فرامین Flash مخرب در داخل فایل PDF امکان سوءاستفاده از این نقطه ضعف از طریق دو نرم‌افزار Reader و Acrobat فراهم می‌شود.

شرکت Adobe همزمان با اعلام کشف نقطه ضعف، قول داده بود که در اسرع وقت اصلاحیه‌ای برای ترمیم آن تهیه و منتشر کند. روز دوشنبه اول فروردین ۹۰، Adobe به قول خود عمل کرده و نسخه‌های بروز شده Flash و Acrobat و Reader را عرضه کرد.

در طی این چند روز فاصله از زمان اعلام شناسایی نقطه ضعف و ارائه اصلاحیه آن، تنها یک مورد جدی از سوءاستفاده از این نقطه ضعف مشاهده شد. در این مورد خاص، فایل Flash مخرب که از این نقطه ضعف سوءاستفاده می‌کرد، در یک فایل Excel جاسازی شده بود و از طریق نامه‌های الکترونیکی منتشر می‌شد . به همین منظور نیز، شرکت مایکروسافت با انتشار اطلاعیه‌ای از کاربران خواسته بود تا با اجرای یک ابزار کمکی به نام EMET مانع از اجرای Flash در نرم‌افزار office شود.

و باز هم بروزرسانی

چهارم فروردین ماه ۹۰، شرکت Google با انتشار نسخه جدیدی از مرورگر Chrome اقدام به اصلاح شش نقطه ضعف امنیتی در این مرورگر کرد. از جمله نقاط ضعفی که ترمیم شده‌اند، اصلاح و تکمیل فهرست سیاه (Black List) مرورگر Chrome برای مقابله با گواهینامه‌های SSL به سرقت رفته شده، است. این گواهینامه‌ها برای فریب کاربران و هدایت آنها به سایت‌های جعلی، مشابه سایت مشهور واقعی مثل Gmail و Yahoo سرقت شده بودند که پس از اطلاع از سرقت آنها، گواهینامه‌ها فوراً باطل شدند. شماره نسخه جدید مرورگر Chrome 10.0.648.204 است.

همچنین روز اول فروردین ۹۰، شرکت Apple با انتشار نسخه بروز شده سیستم عامل Mac OSX 10.6.7 اقدام به اصلاح ۵۶ نقطه ضعف در این سیستم عامل کرد.
گرچه شرکت Apple بر خلاف شرکت مایکروسافت ، نقاط ضعف کشف شده را از لحاظ میزان خطر و آسیب‌پذیری، درجه‌بندی نمی‌کنند، اما براساس اطلاعات منتشر شده از طرف شرکت Apple درباره هریک از این نقاط ضعف، بیش از ۴۵ نقطه ضعف امکان سوءاستفاده و نفوذ به سیستم عامل OSX را بدون دخالت و اطلاع کاربر فراهم می‌کند.

نابودی شبکه مخرب Rustock

روز جمعه ۲۷ اسفند ۸۹، شرکت مایکروسافت از انهدام و نابودی شبکه مخرب **Rustock** خبر داد. در گذشته نه چندان دور، نیمی از نامه‌های الکترونیکی ناخواسته و تبلیغاتی (هرزنامه- **Spam**) توسط این شبکه مخرب تولید و ارسال می‌شد و طبق آخرین آمار شرکت **Symantec**، در ماه گذشته شبکه مخرب **Rustock** مسئول ارسال ۱۲ درصد از کل هرزنامه‌ها در جهان بوده است.

شبکه‌های مخرب که **Botnet** نامیده می‌شوند از هزاران (و در مورد شبکه **Rustock** از میلیون‌ها) کامپیوتر کاربران عادی بر روی اینترنت به نام **Bot**، تشکیل می‌شوند. گردانندگان این شبکه‌های مخرب با استفاده از ابزارهای مخرب و بدافزارها (**Malware**) کامپیوترهای آسیب‌پذیر برروی اینترنت را به تسخیر و کنترل خود در می‌آورند. در بیشتر موارد کاربران این کامپیوتر کاملاً بی‌اطلاع هستند. از طریق کامپیوترهای تسخیر شده گردانندگان شبکه‌های مخرب می‌توانند به اهداف سوء خود، نظیر ارسال انبوه هرزنامه، سرقت اطلاعات شخصی و یا حمله هماهنگ و یکپارچه به یک سایت خاص دست پیدا کنند.

شرکت مایکروسافت با جمع‌آوری و ارائه اسناد و مدارک بر علیه شبکه مخرب **Rustock** از دادگاه‌های آمریکا مجوز لازم برای ضبط سرورهای مرتبط با این شبکه و مسدودسازی نشانی‌های **IP** این شبکه را دریافت کرده و با کمک پلیس و دیگر مقامات امنیتی دست بکار شد.
این اولین بار نیست که مایکروسافت دست به چنین اقدامی می‌زند. سال گذشته، در یک عملیات مشابه، شرکت مایکروسافت توانست شبکه مخرب **Waledac** را متوقف کرده و از هم بپاشد.

البته اینگونه اقدامات نتیجه صد در صد ندارد و بسیاری از گردانندگان شبکه‌های مخرب قادر بوده‌اند تا از چنگ قانون گریخته و شبکه‌های مشابهی را مجدداً راه‌اندازی کنند. اینگونه اقدامات قانونی تا مدت زیادی از شدت این فعالیت‌های مخرب می‌کاهد و تا به حال موردی مشاهده نشده که نتوانسته باشد به اوج و قدرت سابق خود بازگردد.

خرید شرکت امنیتی Sentigo توسط McAfee

شرکت **McAfee** اعلام کرد که شرکت **Sentigo** را که در زمینه امنیت بانک‌های اطلاعاتی تخصص دارد، خریده است. مبلغ خرید اعلام نشده است.

شرکت **Sentigo** سالهاست با شرکت **McAfee** در ارائه فناوری اطلاعات امنیتی جدید برای محافظت از بانک‌های اطلاعاتی همکاری مشترک دارد. بسیاری از محصولات نرم‌افزاری **Sentigo** با ابزار امنیتی **McAfee e-Policy** سازگار بوده و تحت مدیریت یکپارچه این ابزار نرم‌افزاری عمل می‌کند.
همچنین محصولات امنیتی **McAfee** که اختصاصاً برای تأمین امنیت بانک‌های اطلاعاتی طراحی و تهیه شده‌اند، از فناوری‌های **Sentigo** استفاده می‌کنند. محصولاتی نظیر **McAfee Vulnerability Manager for Data bases** و **McAfee Integrity Monitoring for Data bases** .

همزمان، شرکت **Intel** که سال گذشته شرکت **McAfee** را به قیمت ۷/۷ میلیارد دلار خریداری کرد، اعلام کرده از فناوری امنیتی **McAfee** برای ارائه " خدمات امنیتی ابری" **(Cloud Security Services)** استفاده خواهد کرد. این خدمات برای سخت‌افزارها و دستگاه‌های قابل حمل **(Mobile Devices)** خواهد بود.
به اعتقاد مسئولان **Intel**، در آینده وجه تمایز دستگاه‌های قابل حمل، میزان و درجه امنیت آنها خواهد بود. ارائه خدمات امنیتی به اینگونه دستگاه‌ها نیز باید بصورت " سرویس‌های ابری " **(Cloud Services)** باشد و طراحی و ساخت این سرویس به این آسانی و سرعت قابل انجام نیست. ولی **Intel** با استفاده از فناوری‌های حاضر و آماده **McAfee** امیدوار است قدم‌های بزرگی را در زمان کوتاهی بردارد.
هدف **Intel** گنجاندن امکانات مدیریت امنیت در سخت‌افزار دستگاه‌های قابل حمل است. این امکانات مدیریتی می‌تواند قابلیت‌های امنیتی مختلفی را بر روی دستگاه فعال کرده و ارائه دهد. امکاناتی نظیر مقابله با بدافزارها، تشخیص اصالت کاربر **(User Autheutication)** و تأیید اعتبار نشانی‌های **IP (IP Verification)**.

حفره‌های امنیتی در سایت McAfee

روز دوشنبه ۸ فروردین ماه، یک گروه از کارشناسان امنیتی که هویت خود را فاش نکرده‌اند، خبر از کشف حفره‌های امنیتی بر روی سایت رسمی شرکت **McAfee** دادند. در این خبر به سه نوع حفره امنیتی اشاره شده بود: **Cross Site Scripting** که امکان سوءاستفاده از سایت جمعی مشابه سایت اصلی **McAfee** را می‌دهد، **Information Disclosure** که امکان دسترسی به اطلاعاتی را که نباید بر روی اینترنت قابل دسترس باشد را می‌دهد و **Source Code Disclosune** که امکان مشاهده برنامه (**Source**) صفحات سایت را می‌دهد.

روز سه شنبه ۹ فروردین ماه، شرکت **McAfee** وجود این حفره‌های امنیتی را تأیید و اعلام کرد که اقدامات لازم برای برطرف کردن این موارد آغاز شده است. در عین حال، این اطمینان خاطر را داد که هیچگونه اطلاعات شخصی شرکت و مشتریان تحت‌تأثیر این حفره‌های امنیتی قرار نگرفته و سوء استفاده از این حفره‌ها، امکان دسترسی به این اطلاعات را فراهم نکرده است.

روز پنج شنبه ۱۱ فروردین ماه، شرکت **McAfee** با انتشار اطلاعیه جدیدی، خبر از رفع و ترمیم حفره‌های امنیتی کشف شده اخیر داد. در این اطلاعیه مجدداً بر عدم افشای اطلاعات سازمانی **McAfee** و مشتریان این شرکت تأکید شده است. به گفته مسئولان این شرکت، دستورالعمل‌ها و راهکارهای موجود در حال بازنگری هستند تا دلایل این سهل‌انگاری‌ها و عدم رسیدگی به موقع به این حفره‌های امنیتی مشخص و بر طرف شوند تا بار دیگر شاهد اینگونه اتفاقات نباشیم.

تبرئه سامسونگ، شرمندگی GFI

شرکت سامسونگ از طرف شرکت امنیتی **GFI** متهم به استفاده از ابزارهای جاسوسی و مخرب بر روی کامپیوترهای قابل حمل خود شد. این اتهام بر اساس اطلاعاتی بود که مسئولان **GFI** از نرم‌افزار ضدویروس **Viper** خود به دست آورده بودند.

این خبر آنچنان بزرگ و تکان دهنده بود که برای مدتی مسئولان شرکت سامسونگ را گیج و مبهوت کرد و به مسئولان شرکت **GFI** فرصت داد نتایج خود را یکبار دیگر بررسی و مرور کنند. در این موقع بود که شرکت **GFI** مجبور شد بطور رسمی از بابت خبر منتشر شده و اتهام وارده به شرکت سامسونگ معذرت خواهی کرده و مطالب خود را تصحیح کند.

شرکت **GFI** مدعی شده بود که شرکت سامسونگ یک ابزار جاسوسی از نوع **Key logger** را که کلیدهای زده شده توسط کاربر بر روی صفحه کلید را کنترل و ضبط می‌کند، بر روی کامپیوترهای قابل حمل خود نصب کرده است. تحقیقات دقیق‌تر نشان داد که اصلاً چنین ابزار و فایلی بر روی کامپیوترهای سامسونگ وجود ندارد و نرم‌افزار ضدویروس **viper** که متعلق به شرکت **GFI** است، به اشتباه تنها با تشخیص شاخه **C:\windows\SL** که محل نصب یک ابزار جاسوسی به نام **Star Logger** است، کشف و شناسایی این برنامه مخرب را اعلام کرده است.
شاخه مورد نظر توسط سیستم عامل **windows** برای نرم‌افزار **Live Application** ایجاد می‌شود و محل نصب فایل‌های زبان‌های مخلف برای این نرم‌افزار است.

مسئولان **GFI** اقرار کردند که تنها تشخیص این شاخه برای اعلام آلودگی سیستم کافی نبوده و نرم‌افزار ضد ویروس **Viper** باید کنترل‌های بیشتری را قبل از اعلام و هشدار آلودگی انجام می‌داد.