دوشنبه 17 مرداد 1390 - 09:37

باز کردن قفل خودروها با پیامک

سرقت خودروهای جدید با کمک ارسال پیامک، از کار انداختن سیستم های امنیتی خانه ها و اعلام آسیب پذیری بالای سیستم عامل «کروم» از جمله رویدادهای مهم و هشدار دهنده در کنفرانس امنیتی کلاه سیاه در «لاس وگاس» بوده اند.

جام جم آنلاین: سرقت خودروهای جدید با کمک ارسال پیامک، از کار انداختن سیستم های امنیتی خانه ها و اعلام آسیب پذیری بالای سیستم عامل «کروم» از جمله رویدادهای مهم و هشدار دهنده در کنفرانس امنیتی کلاه سیاه در «لاس وگاس» بوده اند.
به گزارش مهر، هکرهای خوب و متخصصان امنیت شبکه از سرتاسر جهان با آغاز کنفرانس سالانه کلاه سیاه در «لاس وگاس» آمریکا، برای چهار روز گرد هم جمع می شوند تا به بررسی رویدادهای اخیر در زمینه حملات سایبری ، آسیب پذیری های نرم افزاری و اینترنتی و دیگر نقطه ضعف های امنیتی در انواع تجهیزات بپردازند.

در این دور از گرد همایی کلاه سیاه ها، متخصصان امنیت شبکه و شرکت های امنیتی و رایانه ای اطلاعات جدید و گاه باور نکردنی را ارائه کرده و برنامه های جدیدی را برای مقابله با پدیده جنایت های سایبری معرفی کردند. از جمله این برنامه ها طرح مسابقه 250 هزار دلاری مایکروسافت با نام جایزه کلاه آبی است.

جایزه کلاه آبی مایکروسافت

مایکروسافت برای دست پیدا کردن به ایده های جدید در زمینه رویکردهای دفاعی در مقابل تهدیدهای امنیتی رایانه ها به جامعه روی آورده است. این شرکت اعلام کرده در ازای بهترین راه حل به منظور مقابله با تهدیدهای رایانه ای، 250 هزار دلار جایزه نقدی اهدا خواهد کرد.

این رقابت در کنفرانس کلاه سیاه معرفی شد و «کتی موسوری» سیاستگذار ارشد امنیتی در مایکروسافت اعلام کرد این شرکت در جستجوی شیوه هایی جدید برای الهام بخشیدن به توسعه راه حل های امنیتی قابل اطمینان است.

مایکروسافت می خواهد متخصصان بیشتری را تشویق کند تا راه های متنوعی را برای کاهش دادن خطرهای رایانه ای ارائه کنند. این شرکت معتقد است جایزه کلاه آبی می تواند نابغه ترین متخصصان و دانشمندان را برای مهار این مشکل جهانی تشویق کند.

برنده اول در این رقابت 200 هزار دلار جایزه دریافت خواهد کرد در حالی که برنده رتبه دوم 50 هزار دلار و برنده رتبه سوم عضویت در سازمان جهانی برنامه نویسان مایکروسافت به ارزش 10 هزار دلار را دریافت خواهد کرد.

بازکردن در نیمی از خودروهای آمریکا با استفاده از چند پیامک

در این کنفرانس متخصصان حقایقی را درباره آسیب پذیری های موجود در سیستم های خودکار رایانه ای و الکتریکی معرفی کردند که می توانند با در نظر گرفتن رشد صعودی پیچیدگی های موجود در فناوری های مدرن، آینده وحشتناکی را برای انسان ها رقم بزنند.

برای مثال «دان بیلی» مشاور ارشد امنیت شبکه در کنفرانس امنیتی «کلاه سیاه» اعلام کرد می تواند قفل درهای هزاران خودرو در سرتاسر ایالات متحده را به سادگی و با ارسال چند پیامک از گوشی آندرویدی خود باز کند.

«بیلی» در این کنفرانس در گفتگو با سی ان ان اعلام کرد با استفاده از شیوه پیامکی باز کردن در خودروها و حتی روشن کردن آنها می توان در حمله به سیستم های رایانه ای صنعتی، شبکه برق و سیستم آب نیز استفاده کرد.

به گفته وی، شاید بازکردن در خودروها با کمک یک پیامک در ابتدا جالب توجه و سرگرم کننده به نظر بیاید، اما با همین شیوه ساده می توان کنترل تلفن های همراه، سیستم های ترافیکی و شبکه برق را نیز در دست گرفت.

وی از بیان جزئیات درباره نام خودروها یا سیستم های خودکاری که در برابر هک شدن با استفاده از پیامک آسیب پذیر هستند، خودداری کرد.

این شیوه از حمله هکری می تواند ابزارهای متعددی که به شبکه GSM موبایل اتصال دارند را تحت تاثیر قرار دهد و از آنجایی که امروزه تقریبا همه چیز در حال وصل شدن به شبکه سلولی و اینترنت هستند، آسیب پذیری کوچکترین و غیر ممکن ترین ابزارهای روزمره زندگی افزایش ترسناکی پیدا کرده است.

حمله به سیستم های خودکار سازی خانه های مسکونی

تعدادی دیگر از متخصصان حاضر در این کنفرانس نیز چگونگی ایجاد اختلال و جاسوسی در شبکه اتوماتیک خانه های مسکونی را با اتصال به شبکه های اترنت که از طریق خطوط برق عمومی به یکدیگر وصل می شوند را به نمایش گذاشتند.

«دیو کندی» و «راب سیمون» ابزاری را ابداع کرده اند که می توان آن را در خارج از خانه مورد نظر به خروجی برق وصل کرد و آن را به گونه ای برنامه ریزی کرد که با شبکه اترنت درونی خانه تداخل پیدا کند.

این ابزار می تواند سیگنال هایی که برای خاموش و روشن کردن چراغ ها به کار گرفته می شوند را مختل کرده، سیستم های امنیتی منزل را خاموش کرده و دوربین های امنیتی را نیز از کار بیاندازند.

این ابزار همچنین می تواند ابزارهای متصل به شبکه داخلی را مشاهده کرده و از باز و بسته بودن درها یا خاموش و روشن بودن چراغ ها مطلع شود.

می توان با کمک این ابزار و حسگرهای حرکتی حرکات انسانها را درون خانه ردیابی کرد و از منطقه ای که در آن حضور دارند اطلاع به دست آورد.

سیستم عامل گوگل هک شد

علاوه بر این نکات مهم امنیتی که در کنفرانس مطرح شد، سیستم عامل گوگل نیز در این کنفرانس زیر ذره بین متخصصان امنیت شبکه قرار گرفت و این متخصصان شیوه سرقت اطلاعات از سیستم عامل گوگل کروم که کاملا مبتنی بر شبکه است را معرفی کردند. با استفاده از وابستگی این مرورگر به اینترنت علیه خودش، متخصصان توانستند به نام کاربری و رمز عبور و اطلاعات ذخیره شده در این سیستم عامل دسترسی پیدا کنند.

با اینکه بسیاری از آسیب پذیری های این سیستم عامل قابل رفع هستند، اما برای رفع تعدادی از آنها هیچ راه حلی وجود ندارد.

گوگل سیستم عامل خود را رویکردی متحول کننده در جهان محاسبات رایانه ای معرفی کرده و بر قابلیت های امنیتی آن بسیار تاکید داشته است اما «مت جانسون» و «کیل آزبورن» از شرکت امنیتی کلاه سفید، نشان دادند که وابستگی به اینترنت خطرهای زیادی را برای این سیستم عامل در بر دارد.

این دو با استفاده از تکنیک های رایج هکرها توانستند به سرعت به این سیستم عامل نفوذ کنند. در این شیوه یک صفحه وب با کدی که در مرورگرهای کاربران فعال می شود به درون سیستم تزریق می شود. این کدها در نهایت در رایانه های هدف فعالیت های تخریبی انجام می دهند.

«کروم» به گونه ای طراحی شده تا با استفاده از تکنیکی به نام Sandboxing از آسیب های احتمالی این کدها جلوگیری کند.

این دو متخصص از برنامه نویسی متقاطع سایت برای حمله به پسوند مرورگر سیستم عامل گوگل کروم استفاده کردند. در گوگل کروم، پسوندهای مرورگرها بسیار قدرتمند تر از دیگر مرورگرها هستند و متخصصان نیز دریافتند این پسوندها می توانند به آنچه در مرورگر کاربران در حال وقوع است، دسترسی کامل داشته باشند.

به بیانی دیگر متخصصان دریافتند این پسوندها در برابر برنامه نویسی متقاطع سایت ها به شدت آسیب پذیر هستند.