خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج

اخبار فناوری اطلاعات و ارتباطات

۹۲

هفته نامه | سال دوم | شماره نود و دوم | ۱۶ بهمن ۱۳۹۵

جوایز ۳ میلیون دلاری گوگل برای نفوذگران کلاه‌سفید

در سال ۲۰۱۶ میلادی، گوگل مبلغی در حدود ۳ میلیون دلار را در قالب برنامه‌های کشف خطای خود به نفوذگران پرداخت کرده است، این رقم قابل ملاحظه نشان‌دهنده‌ی میزان اهمیت چنین برنامه‌هایی برای آن دست از افرادی است که در آن شرکت می‌کنند.

به این طریق، اشکالات گوگل برطرف می‌شوند و نفوذگران فرصت سوءاستفاده از آن‌ها به عنوان در پشتی برای ورود به سامانه‌ها را پیدا نمی‌کنند؛ همچنین نفوذگران تغییر رویه داده و راه درست را در پیش می‌گیرند و تمام تلاش خود را برای گزارش نواقص موجود به این غول فن‌آوری به خرج می‌دهند.

با نگاهی به گزارش عملکرد برنامه‌ی کشف خطای گوگل در سال ۲۰۱۶ متوجه می‌شویم که در این سال میلادی ۳۵۰ محقق در این برنامه شرکت کرده‌اند، این محققان از نقاط مختلف جهان، به ویژه ۵۹ کشور خاص خود را به این برنامه رسانده‌اند.

در مجموع بیش از ۱۰۰۰ خطا در برنامه‌ها و سرویس‌های گوگل کشف و به گزارش گزارش شده است. بد نیست بدانید که بیشترین مبلغ پرداختی برای این خطاها ۱۰۰هزار دلار بوده است. بله درست متوجه شدید! از آنجایی‌که می‌دانیم آسیب‌پذیری‌های متداول چنین جایزه‌ای را برای محققان به ارمغان نمی‌آورند، به این نتیجه می‌رسیم که پای یک آسیب‌پذیری بسیار مهم در میان بوده است.

پرداخت‌های هنگفت، اشکالات مهم

در مقایسه با سال ۲۰۱۵ که گوگل مبلغ ۲ میلیون دلار را بابت برنامه‌ی کشف خطای خود پراخت کرده بود، سال ۲۰۱۶ و پرداخت ۳ میلیون دلاری گوگل جهشی عظیم محسوب می‌شود. این موضوع این‌چنین توجیه می‌شود که گوگل مبلغ جوایز را در برخی از موارد تا ۵۰٪ افزایش داده است.

گوگل تنها شرکتی نیست که این قبیل رقابت‌ها را برگزار می‌کند. در حقیقت بیشتر شرکت‌های عرصه‌ی فن‌آوری چنین کاری را انجام می‌دهند و با بررسی موشکافانه مشخص می‌شود که برگزاری چنین رقابت‌هایی برای این شرکت‌ها سودآوری نیز به همراه دارد.

افشای ۴.۲ میلیارد رکورد در سال ۲۰۱۶ میلادی

سال گذشته، آمریکا هدف اصلی حملات سایبری بوده است و در پی این حملات رتبه‌ی نخست نقض اطلاعات به این کشور تعلق گرفته است.

به گزارش Risk Based Security، در طول سال ۲۰۱۶ میلادی حدود ۴۱۴۹ نقض اطلاعات رخ داده که به دنبال آن ۴,۲ میلیارد داده افشا شده است. حدود نیم یا به‌طور دقیق‌تر ۴۷,۵٪ از این نقض‌ها که منجر به افشای اطلاعات کاربران شده متعلق به ایالات متحده‌ی آمریکا بوده است.

بنابراین، ۶۸,۲٪ از این رکوردهای نقض‌شده به شهروندان آمریکایی تعلق داشته است.

با این وجود نمی‌توان گفت که چنین رخدادی خاص آمریکا است. بلکه بایست به این نکته توجه داشت که چنین آسیب‌پذیری‌هایی در بسیاری از نقاط جهان هرگز دیده نمی‌شوند و شاید نقض‌های داده گزارش داده نمی‌شوند چرا که اصلاً تشخیصی راجع به آن‌ها صورت نمی‌گیرد.

۳,۲ میلیارد گذرواژه در سال ۲۰۱۶ برملا شده است

نکته‌ی حائز اهمیت دیگری که در این گزارش وجود دارد این حقیقت است که شمار رخدادهایی که روی اطلاعات محرمانه‌ی مربوط به دسترسی تأثیر گذاشته‌اند در سال ۲۰۱۶ در مقایسه با سال ۲۰۱۵ رو به کاهش گذاشته است. به‌طور مثال در سال ۲۰۱۵ نزدیک به نیمی از نقض‌های داده باعث افشای گذرواژه‌ها شده است. در مقایسه تنها ۳۸,۱٪ از نقض‌های اطلاعاتی سال ۲۰۱۶ روی گذرواژه‌ها تأثیرگذار بوده‌اند.

هنگامی که نگاهی به این ارقام می‌اندازیم، متوجه تصویری متفاوت و متناقض می‌شویم. در سال ۲۰۱۵ تعداد گذرواژه‌های تحت تأثیر حملات حدود ۱۵۱ میلیون بوده است، اما در سال ۲۰۱۶ این رقم به ۳,۲ میلیارد رسیده و به عبارتی سر به فلک کشیده است. این بدان معناست که در حالی که درصد نقض‌های اطلاعاتی که روی گذرواژه‌ها اثرگذار بوده در سال ۲۰۱۶ به مراتب پایین‌تر بوده است،

آیا ترامپ تدابیر امنیت سایبری را نادیده می‌گیرد؟

تدابیر امنیتی که توسط دولت جدید مستقر در کاخ سفید اتخاذ شده همه‌ی کارشناسان حوزه‌ی فن‌آوری را متحیر کرده است، این کارشناسان نمی‌دانند که بایست به این اوضاع بخندند یا برای آن گریه کنند. نفوذگران با بررسی موشکافانه‌ی حساب توییتر چندین تن از اعضای دولت متوجه شد که دونالد ترامپ، ملانیا ترامپ، مایک پنس، و حتی سخن‌گوی جدید کاخ سفید یعنی شان اسپایسر از رایانامه‌های شخصی خود برای کارهای رسمی و اداری استفاده می‌کنند.

نفوذگری ملقب به WauchulaGhost، که به خاطر سرنگون کردن حدود ۵۰۰ حساب کاربری توییتر متعلق به گروهک داعش سرشناس شده است، گفت که هیچ نفوذ سایبری را در مورد رئیس‌جمهور تازه‌ی آمریکا و وابستگانش صورت نداده است، اما درصدد بوده تا این هشدار را به آن‌ها بدهد: «امنیت خود را ارتقاء دهید!»

جیمیل، امنیت ضعیف، و تلفن‌های شخصی

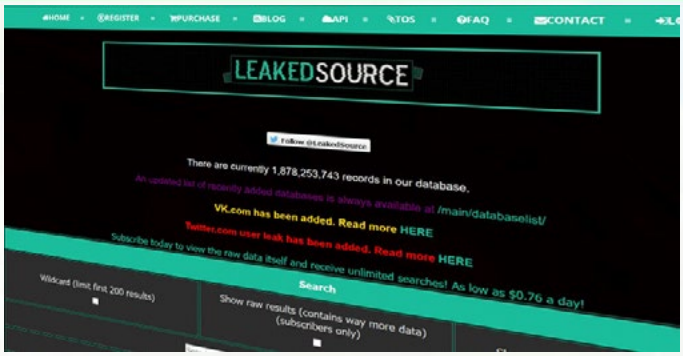
به نظر نمی‌رسد طی روزهای گذشته تغییر خاصی رخ داده باشد، اما این سؤال پیش می‌آید: آن‌ها چگونه می‌توانند نسبت به امنیت ملی بی‌اعتنا باشند؟

مطمئناً جیمیل بسیار امن است، اما قابل نفوذ می‌باشد. شیوه‌ی کار نفوذگران این نیست که از طریق گوگل اقدام کنند و خط به خط اقلام جست‌وجو شده را برای یافتن سر نخی برای ورود به کارگزارها و به دست آوردن اطلاعات لازم بگردند، بلکه آن‌ها تلاش می‌کنند تا به واسطه‌ی نفوذ به حساب‌های شخصی که از هویت مالکین آن‌ها اطلاع دارند به هر آنچه که می‌خواهند دست پیدا نمایند. این بدان معناست که به دست آوردن اطلاعات لازم در مورد ترامپ چندان زمان نمی‌برد زیرا وی و سایر همراهانش در کاخ سفید نسبت به تدابیر امنیتی لحاظ‌شده در توییتر بسیار سرخوشانه عمل کرده‌اند.

رایانامه‌های شخصی، رایانامه‌های بی‌دردسر

این موضوع دقیقاً همانند استفاده از کارگزارهای خصوصی رایانامه نیست، چیزی که ترامپ در کمپین انتخاباتی خود بسیار از آن یاد کرده بود، در حقیقت این موضوع نشان‌دهنده‌ی درک نادرست از امنیت برخط و قوانین امنیتی از سوی کسانی است که وارد کاخ سفید می‌شوند.

وب‌گاه اطلاع‌رسانی نقض داده‌ی LeakedSource از کار افتاد



وب‌گاه LeakedSource که به دلیل جمع‌آوری اطلاعات نقض‌شده معروف است، از حالت برخط خارج شد. هنوز هیچ اطلاعات رسمی درباره‌ی علت وقوع این حادثه در دست نیست ولی شایعات حکایت از این دارد که دخالت نیروهای پلیس در میان بوده است.

این وب‌گاه چند ساعتی است که از کار افتاده و کاربران قادر نیستند بر روی آن جزئیات حساب‌های لوررفته‌ی خود را مشاهده کنند. این وب‌گاه حاوی اطلاعات مربوط به نقض داده‌های متعددی بود و این اطلاعات برای بسیاری از کاربران مفید واقع می‌شد.

تنها وب‌گاه نیست که از حالت برخط خارج شده بلکه حساب‌های کاربری در شبکه‌های اجتماعی متعلق به این وب‌گاه نیز به حالت تعلیق درآمده و شرایط به وضعیت کاملاً نامعلومی تبدیل شده است. در حالی‌که هنوز اطلاعات رسمی در مورد علت وقوع این مشکل در دست نیست، بلافاصله بعد از خاموشی وب‌گاه، پستی در Pastebin منتشر شد که این وب‌گاه مورد یورش پلیس قرار گرفته است. در این پست آمده است، نهادهای قانونی تمامی داده‌های میزبانی شده بر روی این وب‌گاه را ضبط کرده‌اند و کارگزارهای آن نیز تحت بررسی قرار گرفته است.

در این پست می‌خوانیم: «وب‌گاه Leakedsource برای همیشه از کار افتاد و دیگر برنخواهد گشت. صاحب این وب‌گاه مورد یورش پلیس قرار گرفته و تمامی SSD ها از او گرفته شده است ولی دستگیر نیست.» ولی همان‌طور که گفتیم این ادعا ثابت نشده و هیچ مقام و منبع مطلعی این گفته‌ها را تأیید نکرده است.

سؤالات متعددی پیش می‌آید. یک اینکه چرا باید نهادهای قانونی این وب‌گاه را از کار بیندازند؟ وب‌گاه LeakedSource به هیچ وب‌گاهی نفوذ نمی‌کند و تنها با استفاده از وب تاریک، پایگاه داده‌ای از اطلاعات نقض‌شده را ایجاد می‌کند. این وب‌گاه به کاربران اجازه می‌دهد تا ببینند کدام حساب آن‌ها به‌طور برخط افشاء شده و از گستره‌ی نقض داده‌های اتفاق افتاده مطلع شوند.

هرچند انتقادات زیادی به LeakedSource وارد بود که اطلاعات و گواهی‌نامه‌های کاربرانی که مورد نفوذ قرار گرفته‌اند را از وب تاریک در معرض دید دیگران قرار می‌دهد ولی تاکنون صحبتی از تعطیل کردن این وب‌گاه بخاطر عملیات غیرقانونی به میان نیامده بود.