حمله‌ی بدافزار Adwind به ۱۵۰۰ سازمان متعلق به ۱۰۰ کشور مختلف جهان

بار دیگر از ابزار دسترسی از راه دور Adwind در حمله علیه بیش از ۱۵۰۰ سازمان مستقر در ۱۰۰ کشور جهان استفاده شده است.

به گفته‌ی کسپرسکی، این حملات روی بخش‌های مختلف صنعتی، خرده‌فروشان، و توزیع‌کنندگانی تأثیر گذاشته‌اند که ۲۰٪ سازمان‌های آسیب‌دیده را تشکیل می‌دهند. سازمان‌هایی که در بخش معماری و ساخت و ساز فعالیت می‌کنند در حدود ۹,۵٪ از حملات حضور داشته‌اند، همچنین شرکت‌های حمل و نقل و تدارکاتی در ۵,۵٪ و در نهایت شرکت‌های مشاور، بیمه و حقوقی ۵٪ از قربانی‌های این حملات را به خود اختصاص می‌دهند.

به نظر می‌رسد که قربانی‌های Adwind رایانامه‌های ساختگی را دریافت می‌کنند که در ظاهر از سوی سرویس مشاوره‌ای HSBC فرستاده شده‌اند، در این رایانامه‌ها از mail.hsbcnet.hsbc.com به عنوان دامنه استفاده شده است. این پیام‌ها شامل یک مشاوره در مورد پرداخت در ضمیمه‌ی خود هستند، ضمیمه‌ای که مشخصاً حاوی یک نمونه‌ی بدافزار است نه مشاوره.

در صورتی که پرونده‌های زیپ باز شوند، یک پرونده‌ی JAR به نمایش درمی‌آید. این بدافزار به سرعت به‌طور خودبه‌خود نصب می‌شود، سپس تلاش می‌کند تا با کارگزار فرمان‌دهی و کنترل ارتباط برقرار کند، این کار به نفوذگران اجازه می‌دهد تا کنترل کامل دستگاه مورد نفوذ قرار گرفته را در دست بگیرند. این نفوذگران اغلب از در پشتی برای سرقت اطلاعات محرمانه استفاده می‌نمایند.

این حمله جهانی می‌شود

داده‌های کسپرسکی نشان می‌دهد که حدود ۴۰٪ از کلیه‌ی حملات اهداف خود را از میان سازمان‌های موجود در کشورهای زیر انتخاب کرده‌اند:

مالزی، انگلستان، آلمان، لبنان، ترکیه، هنگ‌کنگ، قزاقستان، امارات متحده‌ی عربی، مکزیک و روسیه.

به گفته‌ی محققان آزمایشگاه کسپرسکی، از آن‌جایی‌که این قربانی‌ها شامل درصد بالایی از

بخش‌های تجاری هستند، مجرمان دست‌اندرکار می‌توانند از فهرست رایانامه‌ی ویژه‌ی صنایع برای حمله به اهداف خود استفاده کنند.

حمله‌ی کوکی‌های جعلی، ۳۲ میلیون حساب کاربری یاهو را تحت تأثیر قرار داد

یاهو اعلام کرد، مشکل امنیتی که اخیراً کشف شده بود و از کوکی‌های جعلی استفاده می‌کرد، 32 میلیون حساب کاربری یاهو را تحت تأثیر قرار داده است. شرکت یاهو در چند سال گذشته، چندین نقض داده‌ی عظیم را تجربه کرده و این موضوعات باعث شده معامله‌ی این شرکت با وریزون 350 میلیون دلار افت کند.

اولین نقض داده‌ی این شرکت در ماه سپتامبر سال 2016 میلادی اعلام شد. یاهو معتقد بود این نفوذ توسط عواملی که توسط دولت‌ها پشتیبانی می‌شوند صورت گرفته و در این نفوذ 500 میلیون حساب کاربری تحت تأثیر قرار گرفته است. آن زمان اعلام شد این نقض داده در اواخر سال 2014 اتفاق افتاده است.

در ماه دسامبر سال 2016، این شرکت نقض بزرگ‌تری را افشاء کرد که در سال 2013 اتفاق افتاده و 1 میلیارد حساب کاربری را تحت تأثیر قرار داده بود.

بررسی‌های بیشتر نشان داد، مهاجمان توانسته‌اند به نحوه‌ی تولید کوکی‌ها دست یافته و آن‌ها را جعل کنند.

با استفاده از کوکی‌های جعلی، نفوذگران می‌توانند بدون نیاز به گذرواژه، به حساب‌های کاربران دسترسی داشته باشند. بررسی‌ها نشان داد از این کوکی‌های جعلی برای دسترسی به حساب‌های یاهو در سال‌های 2015 و 2016 استفاده شده و تقریباً 32 میلیون حساب کاربری تحت تأثیر قرار گرفته است.

بررسی‌هایی که توسط محققان خارجی انجام شده نشان می‌دهد، شرکت یاهو نقض داده‌ی سال 2014 را به‌خوبی بررسی نکرده است. شرکت یاهو اواخر سال 2014 متوجه شد ابزارهای مدیریت حساب توسط نفوذگران مورد بهره‌برداری قرار گرفته و مهاجمان توانسته‌اند به 26 حساب کاربری دست یابند.

روز چهارشنبه، مدیرعامل یاهو، ماریسا مایر در پستی در تامبلر اعلام کرد، قصد دارد از پاداش سالیانه‌ی خود به مبلغ ۲ میلیون دلار چشم‌پوشی کند. او گفت تمایل دارد این مبلغ بین کارکنان سخت‌کوش یاهو که برای موفقیت این شرکت در سال ۲۰۱۶ بسیار تلاش کردند، توزیع شود.

نقض داده در شرکت بوئینگ: اطلاعات ۳۶ هزار کارمند افشاء شد

یکی از کارمندان شرکت بوئینگ، سهواً اطلاعات 36 هزار نفر از همکاران خود را افشاء کرد. او زمانی‌که می‌خواست رایانامه‌ای برای همسر خود ارسال کند، یک پرونده‌ی صفحه گسترده حاوی اطلاعات کارکنان را ارسال کرده بود. اخبار این نقض داده اوایل همین ماه، پس از اینکه معاون شرکت بوئینگ نامه‌ای را برای دادگستری ارسال کرده بود، منتشر شد.

چهل و هفت ایالت از جمله واشنگتن دارای قوانینی هستند که اگر نقض داده‌ای رخ داده باشد، باید زمان وقوع آن را مشخص کنند و اگر این نقض داده، بیش از 500 نفر را در یک ایالت تحت تأثیر قرار داده باشد، این موضوع باید به دادگستری ایالت گزارش شود. بوئینگ اعلام کرده در اثر این حادثه، اطلاعات 7288 نفر از ساکنان ایالت واشنگتن تحت تأثیر قرار گرفته است.

براساس نامه‌ای که معاون بوئینگ برای دادگستری ارسال کرده، این نقض داده در تاریخ 1 آذر ماه اتفاق افتاده است. یکی از کارمندان بوئینگ با یک مشکل قالب‌بندی مواجه شده و پرونده‌ی صفحه گسترده را برای همسر خود که در این شرکت کار نمی‌کند، ارسال کرده است. در این پرونده اطلاعات حساس و شخصی نزدیک به 36 هزار نفر از کارمندان شرکت بوئینگ وجود داشته است. پرونده حاوی اطلاعاتی از جمله نام، محل تولد، شماره شناسایی کارمندی و شماره امنیت اجتماعی کارکنان بوئینگ بوده است. برخی از این اطلاعات در ستون‌های مخفی قرار گرفته بودند.

برخی از پرونده‌های صفحه گسترده مانند اکسل، به کاربران این امکان را می‌دهد تا بتوانند برخی از ستون‌ها را مخفی کنند. این مخفی کردن از این بابت خوب است که کاربران دیگر نمی‌توانند اطلاعات این ستون‌ها را مشاهده، ویرایش یا حذف کنند. براساس نامه‌ی ارسالی به دادگستری، بوئینگ این نقض داده را اوایل سال 2017 میلادی کشف کرد ولی آن را یک ماه بعد به کارکنان خود اطلاع‌رسانی کرد.

معاون بوئینگ اظهار کرد، رونویسی از پرونده‌ی صفحه گسترده وجود داشت و برای بررسی‌های جرم‌شناسی از آن استفاده شد. این بررسی‌ها به این دلیل انجام شد تا اطمینان حاصل شود بر روی سامانه‌ی همسرِ کارمند خاطی، این پرونده به‌طور کامل حذف شده باشد.

ما در میانه‌ی راهِ رسیدن به رمزنگاریِ کل وب هستیم

جنبش حرکت به سمت رمزنگاری وب به نقطه‌ی عطف خود رسیده است. گزارش‌ها حاکی از آن است که از اوایل این ماه، تقریباً نیمی از ترافیک وب با استفاده از HTTPS رمزنگاری شده است. به‌عبارت دیگر، در نیمه‌ی راه رسیدن به وبی امن و عاری از استراق سمع، سرقت کوکی‌ها و سانسور هستیم. تمامی این حفاظت‌ها با استفاده از HTTPS بدست آمده است.

شرکت موزیلا اخیراً در گزارشی اعلام کرد در مرورگر فایرفاکس میزان ترافیک رمزنگاری‌شده از ترافیک رمزنگاری‌نشده پیشی گرفته است. نمودارهایی که گوگل کروم از استفاده‌ی HTTPS منتشر کرده، این موضوع را تأیید می‌کند. یافته‌های گوگل نیز نشان می‌دهد بیش از 50 درصد صفحات که بر روی سامانه‌های عامل مختلف در حال اجرا هستند، با استفاده از HTTPS محافظت می‌شوند.

این نقطه‌ی عطف در رمزنگاری وب، به‌دنبال پیروزی در پیاده‌سازی HTTPS حاصل شده است. از غول‌های فناوری، ارائه‌دهندگان محتوا تا وب‌گاه‌های کوچک و حتی خود کاربران، در حال حاضر از HTTPS استفاده می‌کنند.

از سال 2010، اعضای EFF شرکت‌های فناوری را تحت فشار قرار دادند تا از بهترین شیوه‌های رمزنگاری استفاده کنند. در ادامه کار فیس‌بوک و توییتر به‌خاطر پیاده‌سازی پیش‌فرض HTTPS مورد تحسین گرفتند و وب‌گاه‌های بزرگ دیگری مانند ویکی‌پدیا نیز از این پیاده‌سازی پیروی کردند. گوگل همچنین در الگوریتم‌های رتبه‌بندی و جستجوی خود نیز انجمن‌های مختلف را وادار به استفاده از HTTPS کرده است. از امسال نیز در صفحاتی که مربوط به پرداخت بانکی است و کاربران نیاز دارند اطلاعات کارت‌های اعتباری خود را وارد کنند، گوگل هشداری مبنی بر امن نبودن آن صفحه را نمایش می‌دهد. گزارش رمزنگاری وب که توسط EFF منتشر می‌شود نیز نقش بزرگی در تشویق و ترغیب سایر وب‌گاه‌ها در این جنبش داشته است.

پروژه‌های Let's Encrypt و Certbot بازی را تغییر دادند

امن کردن وب‌گاه‌های بزرگ تنها بخشی از این جنبش بوده است. به‌عبارت دیگر وب‌گاه‌های کوچک نیاز دارند تا به‌طور مستقل به پیاده‌سازی HTTPS دسترسی داشته باشند. پروژه‌های Let's Encrypt و Certbot بازی را تغییر دادند.