بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

حمله مهندسی اجتماعی روی نرم‌افزار Webex سیسکو

۱ چکیده

اخیرا یک کمپین فیشینگ یا مهندسی اجتماعی مشاهده شده است که قربانیان را با یک توصیه امنیتی سیسکو درباره یک آسیب‌پذیری بحرانی، فریب می‌دهد. این کمپین، قربانیان را ترغیب می‌کند تا اقدام به بروزرسانی نرم‌افزار نمایند تا از این طریق بتواند اعتبارات کاربران در بستر کنفرانس وب Webex سیسکو را برباید. محققان به کاربران هشدار داده اند، مراقب برنامه‌های جعلی کنفرانس آنلاین و همکاری مجازی باشند تا مورد سوءاستفاده مهاجمان قرار نگیرند. به طور کلی، مهاجمان با ایمیل‌های فریبنده مهندسی اجتماعی، با وعده‌های مربوط به اطلاعات درمانی و... به دنبال سودجویی از نگرانی‌های عمومی درباره ویروس کرونا هستند.

۲ محصولات تحت تاثیر

این کمپین به دنبال بهره‌برداری از موج کارکنانی است که برای جلوگیری از شیوع ویروس کرونا، از راه دور به فعالیت خود ادامه می‌دهند و از ابزارهای کنفرانس آنلاین مانند Webex یا دیگر نرم‌افزارها استفاده می-کنند. از این رو، با افزایش سریع جلسات آنلاین، ربودن اعتبارات نرم‌افزار Webex می‌تواند برای مهاجمان مانند یک بلیط طلایی برای شرکت در تماس‌های کنفرانس آنلاین باشد تا به داده‌ها و اطلاعات حساس در این جلسات، دسترسی یابند.

۳ تاثیر آسیب پذیری

با توجه به شیوع ویروس کرونا و دستورالعمل بسیاری از سازمان‌ها و شرکت‌ها مبنی بر در خانه ماندن کارمندان غیرضروری، استفاده از نرم‌افزارهای کنفرانس آنلاین مانند Webex نیز افزایش یافته است و از این رو، می‌توان پیش‌بینی کرد که در ماه‌های آینده شاهد حملات مهندسی اجتماعی بیشتری با هدف قرار دادن این نرم‌افزارها باشیم. حمله فیشینگ اخیر روی Webex، مهاجمان را قادر می‌سازد تا بتوانند اعتبارات کاربران را ربوده و امکان شرکت در جلسات آنلاین را با استفاده از این اعتبارات به دست آورند. در نتیجه این کار مهاجمان می‌توانند به فایل‌ها و اطلاعات حساس اشتراک گذاشته شده در جلسات، دسترسی پیدا کنند.

۴ بررسی حمله مهندسی اجتماعی

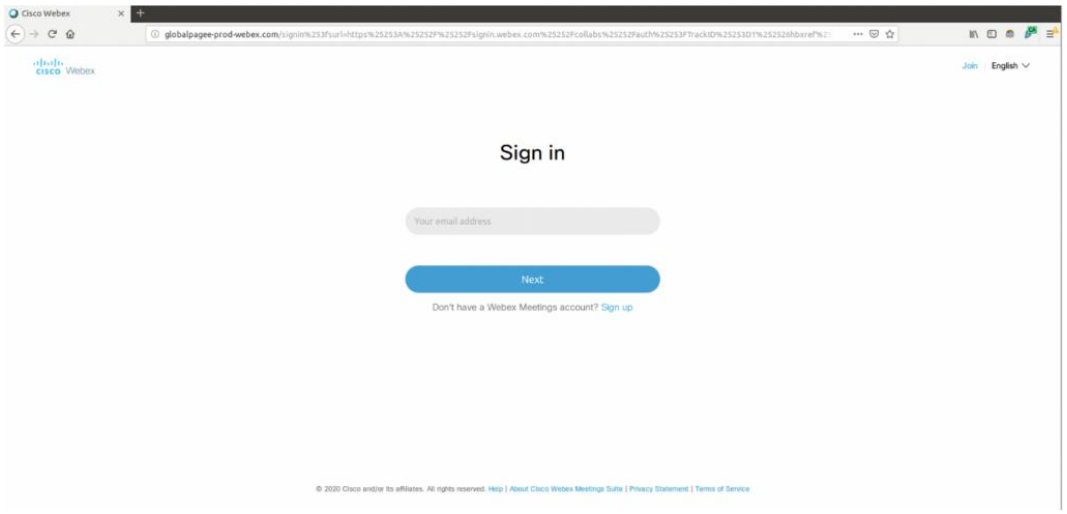
به گفته محققان، حملات مهندسی اجتماعی برای به سرقت بردن اعتبارات کاربران در نرم‌افزار Webex، از طریق ایمیل‌هایی با موضوعات مختلف از جمله "به‌روزرسانی بحرانی" یا "هشدار" و از آدرس ایمیل‌هایی مانند "meeting@webex.com" ارسال می‌شوند. ایمیل‌های این کمپین، تعداد زیادی توسط کاربران نهایی دریافت و گزارش شده است که از صنایع مختلف از جمله خدمات درمانی و مالی هستند.

ترکیب موضوع و محتوای ایمیل می‌تواند کنجکاوی کاربران را جلب کند تا به منظور انجام عمل درخواستی، روی آن‌ها کلیک کنند.

بدنه ایمیل مربوط به محتوای یک توصیه امنیتی واقعی سیسکو در دسامبر ۲۰۱۶ است که نشان تجاری Webex را نیز داراست. در این ایمیل، به قربانیان گفته می‌شود برای رفع آسیب‌پذیری در نرم‌افزار، توصیه می‌کنیم نسخه برنامه دسکتاپ جلسات سیسکو برای ویندوز[۱] را بروزرسانی کنید. همچنین به آنان گفته می‌شود برای اطلاعات بیشتر درباره بروزرسانی، روی دکمه "Join" کلیک کنند.

به نظر می‌رسد مهاجمین این کمپین، بسیار دقیق به جزئیات پرداخته‌اند، به طوری که اگر گیرنده‌های ایمیل محتاط‌تر باشند و بخواهند لینک موجود در دکمه "Join" را کنترل کنند، پیوند hxxps://globalpagee-prod-webex.com/signin را مشاهده خواهند کرد که بسیار شبیه پیوند اصلی سایت قانونی Webex سیسکو به آدرس hxxps://globalpage-prod.webex.com/signin می‌باشد.

قربانیانی که روی دکمه "Join" کلیک کنند، به یک صفحه فیشینگ هدایت می‌شوند که با صفحه ورود سایت مشروع Webex سیسکو یکسان است. به گفته محققان تفاوت کوچکی که وجود دارد این است که وقتی در صفحه ورود قانونی، آدرس ایمیل وارد می‌شود، این آدرس بررسی می‌شود تا مشخص شود که این آدرس ایمیل مربوط به حسابی است که وارد شده است یا نه. در حالی که در صفحه فیشینگ، هر آدرسی که قالب ایمیل درستی داشته باشد، کاربر را به صفحه بعدی هدایت می‌کند که در آن رمز عبور درخواست می‌شود.



تصویر ۱: صفحه ثبت‌نام دامنه جعلی

[۱] Cisco Meetings Desktop App for Windows

مهاجمان حتی تا آنجا پیش رفته‌اند که برای دامنه جعلی خود، گواهی SSL نیز گرفته‌اند تا از این طریق بیشتر اعتماد کاربران را جلب کنند. گواهی SSL رسمی سیسکو توسط HydrantID تایید شده است، در حالی که گواهی سایت جعلی مربوط به Sectigo Limited می‌باشد. اگرچه، نتیجه نهایی یکسان است و در کنار پیوند هر دو دامنه علامت قفل دیده می‌شود که می‌تواند برای جلب اعتماد بسیاری از کاربران کافی باشد.