به نام خداوند بخشنده مهربان

حملات Pharming

گردآوری : پیمان شاهکار
Peyman.shahkar@Gmail.com
Y Id : Peyman_shahkar
www.Desperado.coo.ir

آشنایی با حملات pharming

تهدیدهای جدیدی که هویت و اطلاعات کاربر را هدف قرار داده اند،رویکردهای جدید امنیتی را طلب می کند.

امروزه، حملات phishing ساده تر و کم خطرتر از تهدیدهای آنلاینی که در حال تجربه شدن هستند، به نظر می رسند. حملات phishing به آسانی شناخته می شوند و می توان به سرعت آنها را از کار انداخت. جرائم سازمان یافته از این حد گذشته و پیچیدگی آنها به طرز چشم گیری افزایش یافته است. امروزه، کاربران با اشکال موذیانه تری از حمله مواجه می شوند و کشف و مقابله علیه آنها بسیار مشکل تر است.

گونه ای جدید از حمله

این گونه جدید حمله بعنوان pharming شناخته می شود. pharming بجای اینکه کاربر را گول بزند تا به یک ایمیل تقلبی پاسخ دهد تا او را به یک وب سایت جعلی هدایت کند، برای فریب دادن کاربر برای تسلیم هویت و اطلاعات حساسش، از روش های زیرکانه تری استفاده می کند. این حملات از اسب های تروا (تروجان) برای نصب برنامه های کلیدخوان و برنامه های هدایت کننده استفاده می کنند تا به یک نفوذگر اجازه دهند کلمات عبور و شماره کارت های اعتباری را بدست آورد، بدون اینکه کاربر مجبور به انجام کاری غیرعادی باشد. در اینجا دو مثال از نحوه این حمله آورده شده است:

۱- کاربر یک ایمیل ظاهراً صحیح را باز می کند که او را تشویق می کند تا فایل الحاقی به ایمیل را باز کند. این فایل الحاقی بصورت مخفیانه یک «کلیدخوان» (برنامه ای است که کلیدهایی را که توسط کاربر زده می شود، ثبت می کند) نصب می کند. هنگامی که کاربر به بانک آنلاین خود سر می زند، کلیدخوان این را تشخیص می دهد و ورودی های صفحه کلید کاربر را هنگامی که وی اسم و کلمه عبور را تایپ می کند، ثبت می کند. سپس این اطلاعات برای نفوذگر ارسال می شود تا برای دسترسی به حساب کاربر استفاده شود.

۲- یک کاربر ممکن است با دانلود کردن یک فایل یا مشاهده یک وب سایت که حاوی ActiveX control است، سهواً یک «هدایت کننده» (redirector) را روی سیستم خود نصب کند. این کار باعث می شود که فایل های موجود در سیستم دچار تغییراتی شود و هنگامی که کاربر به بانک آنلاین خود سر می زند، به وب سایت نفوذگر هدایت شود. این عمل می تواند با مسموم کردن سرور DNS انجام گیرد که برای آدرس بانک آنلاین کاربر، IP وب سایت نفوذگر را می فرستد. حملات پیچیده تر می توانند ارتباط را با بانک کاربر برقرار کنند و هنگامی که پروسه در حال انجام است، ترافیک عبوری بین کاربر و بانک (شامل کلمات عبور و اطلاعات شخصی) را مشاهده کنند. در اصل نفوذگر خود را بین کاربران و بانک قرار می دهد.

چه می توان کرد؟

از نظر تاریخی، رویکرد امنیتی که برای این نوع از حملات بکار گرفته شده است، مشابه مفهوم گارد مرزی (Boarder Guard) بوده است. ورود موارد زیان رسان را به کامپیوتر متوقف کنید و جلوی کاربر را از رفتن به مکان های بد بگیرید. ابزارهایی مانند آنتی ویروس، ضدجاسوس، فایروال ها و تشخیص دهندگان نفوذ، همگی چنین رویکردی دارند. به هرحال، همچنانکه حملات به رشد خود ادامه می دهند و پیچیده تر می شوند، نمی توان از احتمال

نصب شدن موفقیت آمیز یک کلیدخوان یا هدایت کننده علیرغم این گاردهای مرزی، غافل ماند.

برای سروکار داشتن با این احتمال، رویکرد متفاوت دیگری مورد نیاز است. علاوه بر ابزارهایی که ذکر آنها رفت، نیاز است که هویت و اطلاعات کاربران توسط محافظ شخصی (body guard) مراقبت شود. یعنی، نیاز است که هویت و اطلاعات شخص بدون در نظر گرفتن نوع حمله و جایی که اطلاعات کاربر به آنجا می رود، همواره امن باقی بماند. این نوع امنیت قابلیت های محافظ شخصی را برای هویت کاربر ایجاد می کند و اهمیتی ندارد که اطلاعات کاربر به کجا فرستاده می شود و کلیدخوان نصب شده است و یا اینکه نفوذگر می تواند ترافیک اینترنت را نظارت کند.

دو قابلیت امنیتی وجود دارد که می تواند توانایی این محافظ شخصی را پیاده کند. اولی تصدیق هویت قوی (strong authentication) است. امروزه، کاربران عموماً برای محافظت از هویتشان به یک کلمه عبور اطمینان می کنند، اما احتمال زیادی وجود دارد که کلمه عبور توسط کسی که نظاره گر login است، دزدیده شود. داشتن یک عامل اضافی برای تصدیق هویت، یعنی چیزی که کاربر باید بصورت فیزیکی داشته باشد علاوه بر آنچه که می داند، می تواند یک هویت آنلاین را در برابر حمله محافظت کند. این کار قابل مقایسه با چگونگی تأیید هویت کاربران در ماشین های خودپرداز بانک است. کاربران هم کارت بانکی دارند و هم PIN را می دانند. با تصدیق هویت قوی، اگر کلیدخوان هم نصب شده باشد، می تواند تنها کلمه عبور را بگیرد و نه عامل فیزیکی استفاده شده در پروسه تصدیق هویت را. کلمه عبور به تنهایی و بدون فاکتور فیزیکی نمی تواند توسط نفوذگر برای دسترسی به حساب کاربر مورد استفاده قرار گیرد.

توانایی مهم دوم رمزنگاری مداوم است. امروزه، SSL (Secure Socket Layer) از اطلاعات ارسال شده توسط کاربران بگونه ای محافظت می کند که انگار تنها به سرور هدف ارسال می شوند. برای مثال، اگر یک کاربر کلمه عبور خود را وارد کند، به راحتی تا زمان رسیدن به و ب سرور در طرف دیگر، قابل مشاهده است. در مورد یک حمله هدایت کننده، ارتباط امن در سایت نفوذگر پایان می پذیرد و قبل از اینکه به سازمان آنلاین قانونی ارسال شود، دیتای کاربر در معرض افشاء قرار می گیرد. رمزنگاری مستمر می تواند از دیتا ،بدون در نظر گرفتن امنیت ارتباط، محافظت کند. ورودی های کاربر قبل از ترک کامپیوتر کاربر رمز می شوند و می توانند تنها توسط سازمان قانونی که به سرورهای طرف دیگر دسترسی دارد، رمزگشایی شوند. حتی اگر دیتا به این سرور نرسد، رمزشده باقی خواهد ماند و برای یک نفوذگر قابل استفاده نیست.

این دو قابلیت به همراه هم، می توانند نقش محافظ شخصی را برای محافظت از هویت و اطلاعات کاربر در دنیای خصمانه! اینترنت ایفاء کنند.

بررسی دنیای واقعی

چند انتخاب وجود دارند که می توانند امنیت محافظ شخصی را فراهم کنند اما باید با استفاده از نیازهای دنیای واقعی اینترنت ارزیابی شوند. چنانچه کاربر با یک تکنولوژی احساس راحتی نکند، آن را نخواهد پذیرفت. اگر تکنولوژی خیلی گران باشد، نه برای کاربر انتهایی قابل تهیه خواهد بود و نه برای سازمان مربوطه.

چندین عامل وجود دارد که باید به هنگام تشویق کاربران به پذیرش تکنولوژی مورد نظر مورد توجه قرار گیرند:

· نرم افزار کلاینت ـ هر نیازی به دانلود و نصب نرم افزار به عنوان یک مانع است...

· واسط نرم افزار ـ خطرات و پیچیدگی که کاربر برای پیاده سازی تجربه می کند...

· راحتی استفاده ـ مخصوصاً برای تصدیق هویت دو عامله! ، راحتی استفاده شامل قابلیت حمل، دوام است. سهولت کار با واسط کاربر نیز مورد توجه جدی است.

مشخصاً زمانی که از این نوع فناوری با مقیاس بالا بکارگرفته شود، هزینه این رویکرد می تواند در امکانپذیری آن موثر باشد. اگر هزینه کل سیستم خیلی بالا باشد، سازمان ها برای برقراری این امنیت اضافی برای یک مورد تجاری مورد قبول، نیاز به مطالبات مالی از کاربران دارند. در این موارد کاربران به راحتی راضی به پرداخت های اضافی برای برقراری این امنیت بیشتر نمی شوند.

به این منظور تکنولوژی های محافظ شخصی باید سطح بالایی از امنیت را در حالی که هزینه کمی در بردارند و برای استفاده آسان هستند، فراهم کنند.

از: ircert