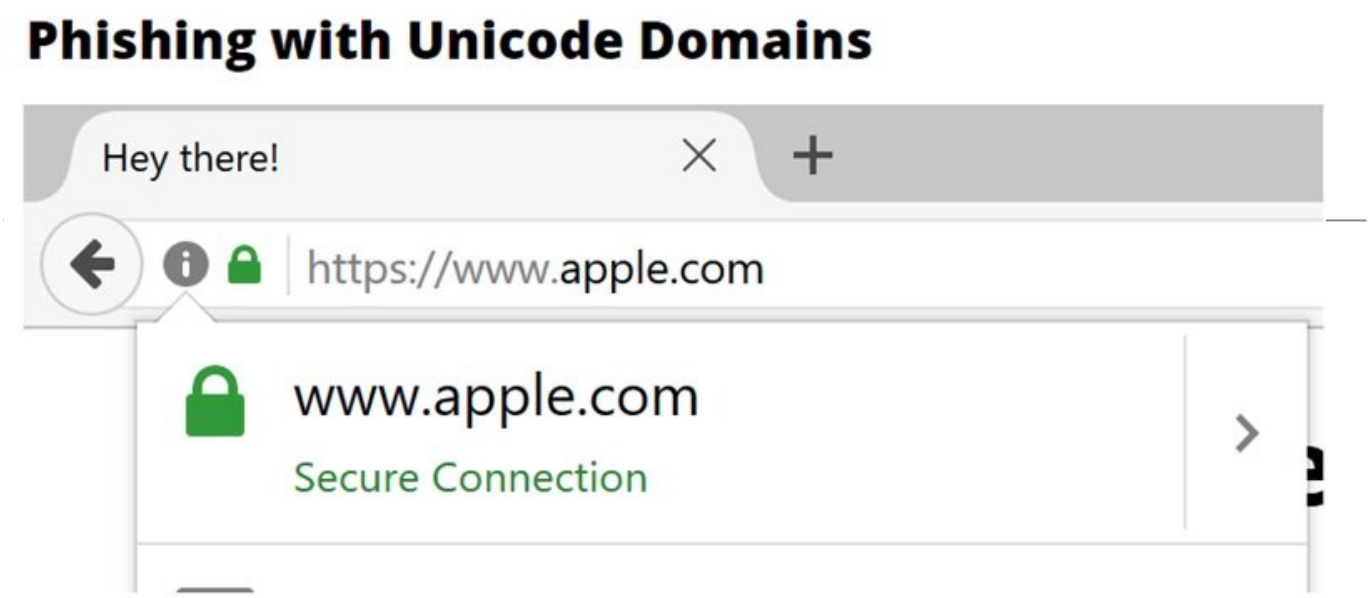
حمله هم‌نگاره در یک قدمی کاربران

شناسایی این حمله فیشینگ برای کروم، فایرفاکس و اپرا تقریبا غیرممکن است



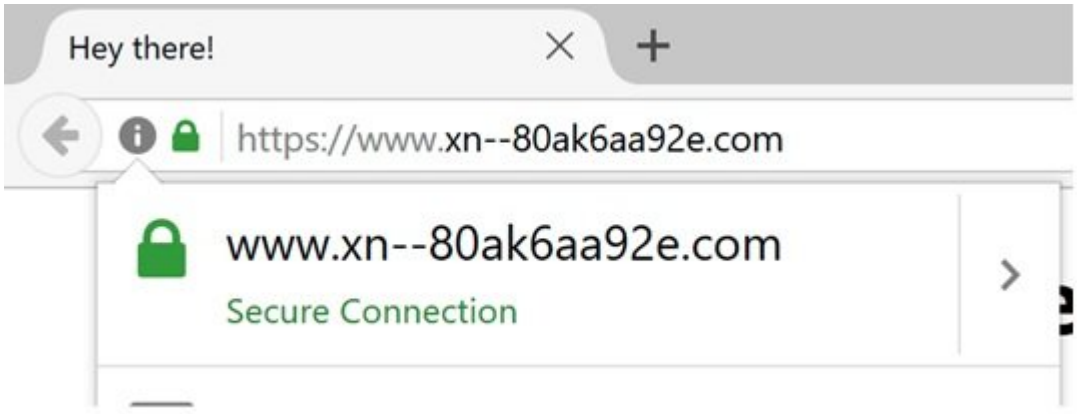
یک پژوهش‌گر چینی درباره یک حمله فیشینگ که شناسایی آن تقریبا غیرممکن است، گزارش داده است. حمله‌ای که می‌تواند محتاط‌ترین کاربران اینترنتی را نیز فریب دهد.

زدی‌دانگ ژنگ، پژوهش‌گر امنیتی گفته است: «هکرها می‌توانند از آسیب‌پذیری موجود در مرورگرهای کروم، فایرفاکس و اپرا سوءاستفاده کرده و صفحات غیرواقعی را در قالب سایت‌های معتبری همچون گوگل، اپل یا آمازون به کاربران نشان داده و در ادامه داده‌های حساس و اطلاعات مربوط به لاگین کاربران را به سرقت ببرند.»

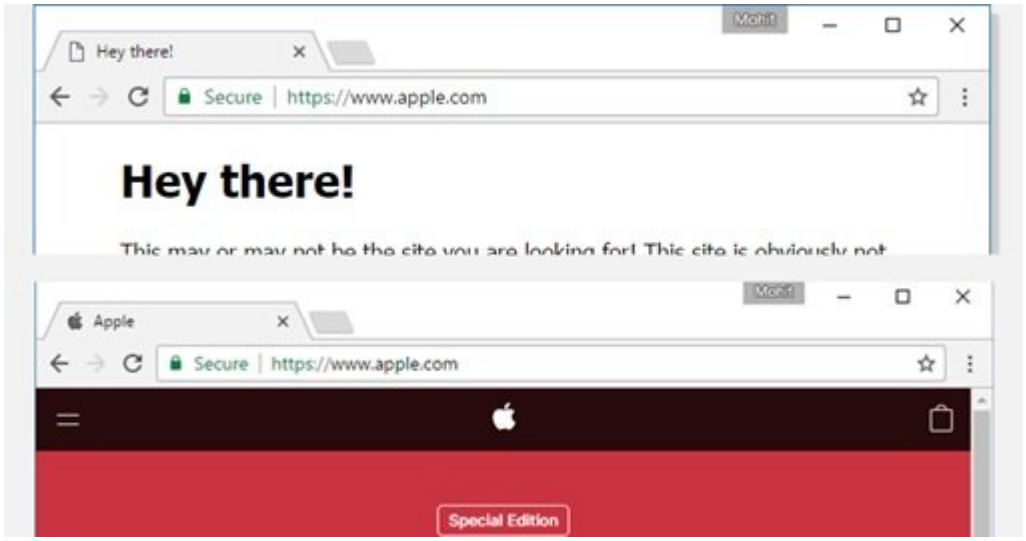
مطلب پیشنهادی

آسیب‌پذیری روز صفر دردسرساز
به‌روزرسانی حیاتی مایکروسافت ورد را دانلود کنید تا قربانی نشوید

کارشناسان امنیتی همواره به کاربران توصیه می‌کنند برای مقابله با حملات فیشینگ پس از بارگذاری کامل یک سایت، نوار آدرس را مشاهده کرده و از درست و دقیق بودن آدرس اطمینان حاصل کنند. در مورد سایت‌های حساس نیز توجه داشته باشند که واژه https در نوار آدرس درج شده باشد. اما به نظر می‌رسد این تکنیک در ارتباط با حمله فوق جواب‌گو نیست. این پژوهش‌گر چینی گفته است حتا اگر راهکاری که در بالا به آن اشاره شد را مورد توجه قرار دهید باز هم ممکن است آدرس apple.com را همراه با نوارآدرس نشان‌دهنده SSL مشاهده کنید اما محتوای صفحه از سرور دیگری برای شما ارسال شده باشد.



لازم به توضیح است که این تکنیک حمله فیشینگ جدید نبوده و قدمت آن به سال 2001 میلادی باز می‌گردد. حمله‌ای که به نام حمله هم‌نگاره (Homograph attack) از آن نام برده شده و متاسفانه تعدادی از سازندگان مرورگرهای اینترنتی راهکار مناسبی را برای مقابله با این حمله در نظر نگرفته‌اند. این حمله آدرس سایت‌ها را به شکل هوشمندانه‌ای مورد تهدید قرار داده و در حالی که در ظاهر همه چیز درست به نظر می‌رسد، اما کاراکترهای آدرس‌ها دستکاری شده و کاراکترهای یونیکد جایگزین آن‌ها می‌شوند.



در حالت پیش‌فرض بیشتر مرورگرها از سیستم کدگذاری punycode برای نمایش کاراکترهای یونیکد در آدرس‌های اینترنتی استفاده می‌کنند تا به این شکل از بروز حملات هم‌نگاری ممانعت به عمل آورند. Punucode یک سیستم رمزنگاری ویژه است که از سوی مرورگرها به منظور تبدیل کاراکترهای یونیکد به مجموعه کاراکترهای محدود اسکی از آن استفاده می‌شود. به طور مثال، دامین چینی .co در سیستم punycode معادل xn--s7y.co است. سیستم رمزنگاری punycode در ارتباط با تبدیل کاراکترهای زبان‌های مختلف به یکدیگر با محدودیت‌هایی روبرو است. همین موضوع باعث می‌شود تا اگر یک آدرس اینترنتی متشکل از زبان‌های مختلفی باشد، یک رخته به وجود آمده و از آن سوء استفاده کرد.

مطلب پیشنهادی

مشکلی دیگر در ارتباط با اثرانگشت
اثرانگشتی که قفل هر گوشی هوشمندی را باز کند

آسیب‌پذیری فوق به زدی‌دانگ ژنگ این توانایی را داد تا دامنه‌ای با آدرس xn--80ak6aa92e.com را ثبت کرده و مکانیزم‌های امنیتی را به راحتی دور بزند. در مرورگرهای کروم، فایرفاکس و اپرا آدرس فوق به آدرس apple.com تبدیل شده و به کاربر نشان داده می‌شود.

مرورگرهای اینترنت اکسپلورر، مایکروسافت اج، سافاری، براوو و ویوالدی در برابر این آسیب‌پذیری ایمن هستند. ژنگ آسیب‌پذیری فوق را در ماه ژانویه به موزیلا و گوگل گزارش کرده است. موزیلا گفته است وصله مربوطه را در اولین فرصت ارائه خواهد کرد. گوگل در نسخه آزمایشی Chrome Canary 59 وصله مربوطه را ارائه کرده و گفته است وصله کامل را همراه به به‌روزرسانی کروم 58 که قرار است این ماه منتشر شود ارائه خواهد کرد. به کاربران توصیه می‌شود تا عرضه به‌روزرسانی‌های فوق پشتیبانی از punycode را در مرورگرهای خود غیرفعال کنند تا از این حمله فیشینگ در امان باشند.

تاریخ انتشار:

02 اردیبهشت 1396

نشانی منبع: https://www.shabakeh-mag.com/security/7574