بولتن تحلیلی ■ آذر ماه ۱۳۹۸

امنیت اطلاعات

پادویش®
Padvish®

بولتن تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

درباره فیشینگ بیشتر بدانیم

فیشینگ راهی است که مجرمان اینترنتی، اطلاعاتی مانند کلمه کاربری، رمز عبور، شماره ۱۶ رقمی کارت بانکی، رمز دوم و CVV۲ را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می‌برند که امروزه به رایج ترین شیوه کلاهبرداری در فضای سایبری تبدیل شده است. البته این روش سرقت اینترنتی از راه‌های گوناگونی صورت می‌گیرد، از جمله فیشینگ جعل وب‌گاه، فیشینگ فریبنده، فیشینگ تلفنی، دوقلوهای شر(Evil twins) و غیره. ما در اینجا به طور مختصر تکنیک‌های کلی و شایع فیشینگ جعل وب‌گاه و فیشینگ فریبنده را توضیح می‌دهیم.

نحوه کار فیشینگ جعل وب‌گاه

مهاجمان در این تکنیک با طراحی یک سایت تقلبی که بسیار شبیه به سایت اصلی می‌باشد، تلاش می‌کنند به روش‌هاي مختلف قربانیان را به سمت سایت تقلبی مورد نظر خود هدایت کنند تا فرد قربانی اطلاعات محرمانه خود را در آن وارد کند.

در نگاه اول صفحه کاملاً شبیه صفحه مورد نظرمان می‌باشد، درحالی که در آدرس بار که آدرس سایت در آن نوشته شده عباراتی اضافه شده‌است و شما غافل از این تغییر، نام کاربری و رمز عبور خود را وارد می‌کنید و اطلاعات خود را در اختیار هکرها قرار می‌دهید.

به طور مثال : آدرس سایت بانک ملی www.bankmelli-iran.com است، در حالی که برای شما صفحه‌ای کاملا مشابه سایت بانک ملی با آدرس دامنه www.bankmelli-iran.asd.com باز شده‌است. این آدرس جعلی است.

گاهی بخش اضافه شده در آدرس تقلبی به قدری طولانی است که در نگاه اول آدرس اصلی سایت قابل دیدن نیست و این باعث گمراه شدن قربانی می‌شود. متاسفانه کاربران به اندازه کافی به آدرس سایت دقت نمی‌کنند و فقط با دیدن استایل صفحه، شروع به وارد کردن اطلاعات می‌کنند! حتی برخی از افراد به آدرس بار نگاه کرده و با دیدن عبارت bankmelli-iran به این صفحه اعتماد می‌کنند.

در مثالی دیگر آدرس معتبر درگاه‌های پرداخت اینترنتی امن باید shaparak.ir باشد و هرگونه ترکیب دیگری از کلمه shaparak و هر پسوند دیگری از شاپرک به جز ir. نامعتبر می‌باشد. به عنوان مثال ترکیب‌هایی نظیر shaaparak و یا shaparakk شما را وارد صفحه‌ی درگاه پرداخت اینترنتی تقلبی می‌کند.

کاربران باید به درگاه‌هایی با شکل آدرس https://xxx.shaparak.ir توجه کنند که به جای مقدار xxx حتما باید نام یکی از شرکت‌های پرداخت الکترونیک مطرح درج شده باشد. مانند به پرداخت ملت https://bpm.shaparak.ir یا پرداخت الکترونیک سامان https://sep.shaparak.ir که درگاه‌های بانکی معتبر می‌باشند.

نحوه کار فیشینگ فریبنده

در این فیشینگ مهاجم با ارسال یک ایمیل با محتوای تقلبی (مشابه یک ایمیل قانونی)، اقدام به فریب دادن کاربر کرده و از کاربر خواسته می‌شود که اطلاعات حساب خود را (نام کاربری و کلمه عبور) مجدد وارد کند. مهاجم امید دارد که کاربر با کلیک روی لینک جعلی فریب خورده و در صفحه مربوطه login کند. استفاده از ایمیل برای به دام انداختن کاربران بسیار رایج است.

تکنیک هایی که معمولاً در فیشینگ برای فریب کاربران استفاده می‌شوند

ه ارسال پیامک‌های جعلی ثبت‌نام کارت سوخت با آدرس جعلی شرکت پخش فرآورده‌های نفتی .

• ارسال ایمیل از طرف فردي که ادعا می‌کند دوست یا همکار شما است.

• ارسال ایمیل و درخواست اطلاعات از سوي بانکی قلابی

• آگهی‌هاي تبلیغاتی سایت‌هاي دیگر یا تبلیغ در شبکه‌هاي اجتماعی

• وب‌سایتی تقلبی که براي امور خیریه تقاضاي کمک می‌کند.

• وب‌سایتی با نامی مشابه وب‌سایت‌هایی که شما مدام به آنها سر می‌زنید.

• اعلام برنده‌شدن شما در قرعه‌کشی

و ....

راه‌هایی براي حفاظت در مقابل حملات فیشینگ

• هرگز اطلاعات کاربری (رمز عبور و نام کاربری) خود را از طریق فرم‌هایی که از طریق ایمیل دریافت می‌کنید، وارد نکنید.

• برای وارد کردن اطلاعات کاربری، یک صفحه جدید در مرورگر باز کنید و آدرس آن وب‌سایت را به صورت دستی وارد کنید.

• اگر روی لینکی کلیک کردید و صفحه جدیدی باز شد، حتما به آدرس آن دقت کنید. همچنین دقت کنید دامنه شامل بخش‌های اضافی نباشد.

• به هیچ وجه و به هیچ عنوان به آدرس ارسال کننده ایمیل اعتماد نکنید!

• اگر ایمیلی در پوشه هرزنامه، اسپم یا Spam شما بود، به احتمال زیاد محتوای آن یا تبلیغاتی و یا فیشینگ است!

• اطلاعات کارت اعتباري را روي حافظه سیستم خود نگهداري نکنید.

• براي اطمینان از واقعی بودن سایت و همچنین وارد کردن اطلاعات کاربری، یک صفحه جدید در مرورگر باز کنید و آدرس آن وب‌سایت را به صورت دستی وارد کنید.

• برای وارد کردن اطلاعات کاربری همیشه از وب سایت های ایمن که با https://: شروع می‌شوند استفاده کنید.

• به‌طور دوره‌اي و مرتب به حساب خود سر بزنید، یعنی آن را براي مدت طولانی بدون کنترل رها نکنید.

• مراقب دکمه‌های دانلود جعلی باشید.

• متن و فونت دکمه با بقیه قسمت‌های وب‌سایت همخوانی داشته باشد.

• مرورگر خود را بطور مرتب به روز کنید و همه وصله‌های امنیتی آن را نصب و فعال کنید.

• از افزونه ضدفیشینگ پادویش استفاده نمایید. این افزونه با هدف شناسایی و مقابله با انواع حملات فیشینگ فضای مجازی (صفحات جعلی درگاه‌های پرداخت الکترونیک) ساخته شده است.

ویندوز 10، قربانی کرم جدیدی به نام Boxter

بدافزار boxter با هدف سرقت و ذخیره اطلاعات کاربران ویندوز ۱۰، تلاش می‌کند تا کنترل از راه دور سیستم قربانی را در اختیار هکرها قرار دهد. به همین منظور، با انجام اقداماتی مانند ذخیره کلیدهای فشرده شده در صفحه کلید و همچنین اتصال به آدرس‌هایی مشخص برای دانلود، کنترل سیستم را در دست می‌گیرد.

بدافزار boxter در دسته کرم‌ها طبقه‌بندی می‌شود. کرم‌های کامپیوتری نوعی از بدافزار محسوب می‌شوند که توان تکثیر کردن خود را به‌صورت خودکار دارند. کرم‌ها برای بقا، روش‌هایی را تنظیم می‌کنند تا در هر بار راه‌اندازی سیستم، آلودگی تداوم داشته باشد. ویژگی بارز کرم‌ها در نحوه انتشار آن‌هاست که عموماً از طریق درایوهای قابل‌حمل (مثل فلش، هارد دیسک و..) صورت می‌گیرد.

علائم آلودگی به بدافزار boxter

• آشکارترین علامت آلودگی به بدافزار boxter در هنگام اتصال فلش به سیستم، پنهان شدن فایل های موجود بر روی آنهاست.

• نشانه بعدی وجود فایل‌هایی ناشناس با پسوند lnk بر روی درایو قابل حمل می‌باشد.

• پیامد دیگر آلودگی به این بدافزار، خاموش شدن یا ریستارت شدن های ناگهانی سیستم شماست.

بدافزار boxter به صورت یک فایل با پسوند lnk خود را منتشر می‌کند. با رسیدن این فایل به سیستم کاربر و اجرای آن، فایل دیگری که وظیفه انجام عملیات اصلی بدافزار را بر عهده دارد، به طور خودکار دانلود و اجرا می‌شود. پس از دانلود و اجرای فایل اصلی، بدافزار اقدام به کپی کردن خود در مسیرهای مشخصی از سیستم می‌نماید که شامل چندین مسیر اصلی ویندوز می‌باشد.

پس از کپی شدن بدافزار در مسیرهای حیاتی سیستم، برخی از قابلیت‌های محافظتی ویندوز که از تغییرات غیرمجاز در سیستم عامل جلوگیری می‌کنند، غیر فعال می‌شوند.

با غیرفعال شدن ویژگی های محافظتی ویندوز، عملیات مخرب بعدی بدافزار بدون نیاز به اعتبارسنجی توسط سیستم صورت می‌گیرند.

روش های انتشار بدافزار

۱. توسط درایوهای قابل حمل

۲. در پیوست ایمیل‌ها خود را کپی و ایمیل را ارسال می‌کند.

روش مقابله و پاک‌سازی سیستم

آنتی ویروس پادویش با دارا بودن قابلیت UMP که جزء محافظت رفتاری آن است، جلوی آلوده شدن سیستم از طریق درایو قابل‌حمل را می‌گیرد. ازاین‌رو جهت پیشگیری از آلودگی به انواع بدافزارهایی مانند این بدافزار که از طریق درایو قابل‌حمل انتقال می‌یابند، پیشنهاد می‌شود با نصب پادویش از ورود بدافزار به سیستم خود جلوگیری کنید.

چنانچه سیستم شما توسط بدافزار Boxter آلوده شده است، مراحل زیر را دنبال کنید:

۱. پادویش را بر روی سیستم خود نصب کنید.

۲. درایو قابل حمل آلوده را به سیستم وصل کنید.

۳. با استفاده از پادویش درایو قابل‌حمل خود را اسکن کنید تا درایو قابل‌حمل و سیستم آلوده شما پاکسازی شوند.

کشف آسیب پذیری مهم در افزونه محبوب وردپرس

وردپرس یک سیستم یکپارچه طراحی و سایت‌ساز رایگان است که امکان مدیریت هر وب‌سایتی بدون داشتن دانش برنامه‌نویسی را برای ما فراهم می‌کند. وردپرس به دلیل سادگی در مدیریت کارهای وب‌سایت، همزمان با رعایت استانداردهای کدنویسی جهانی توانسته به یک سیستم محبوب برای کاربران اینترنت در سراسر جهان و به‌خصوص ایران تبدیل شود. در سیستم مدیریت محتوای وردپرس برای ایجاد هر امکانی افزونه‌ای خاص وجود دارد و بسیاری از این افزونه‌ها رایگان هستند. تنها کافی است سری به مخزن وردپرس بزنید و برای فعالیت مورد نظرتان افزونه‌ای را جستجو و تنها با چند کلیک نصب و راه‌اندازی کنید. یکی از این افزونه‌های بسیار قدرتمند که امکانات متعددی را در اختیار شما قرار می‌دهد، افزونه محبوب jetpack است. به وسیله این افزونه به راحتی می‌توانید از ویژگی‌های امنیتی و مدیریت سایت رایگان برخوردار شوید که شامل پشتیبان‌گیری سایت، ورود ایمن به سیستم و اسکن نرم‌افزارهای مخرب است که توسط Automattic، شرکت پشتیبان وردپرس ارائه می‌شود.

این افزونه محبوب با چندین میلیون نصب فعال در سراسر دنیا، این روزها با آسیب‌پذیری جدیدی رو به رو شده است. از همین رو از ادمین‌های سایت‌های وردپرسی خواسته شده تا به سرعت آخرین به روزرسانی افزونه jetpack را نصب کنند تا از خطرات احتمالی پیش رو در امان بمانند.

البته از این آسیب‌پذیری تا به حال سوء استفاده‌ای صورت نگرفته و در عین حال جزئیاتی نیز از آن منتشر نشده است. با این حال توسعه دهندگان درباره تاثیرات گستره این آسیب‌پذیری هشدار داده‌اند که با توجه به اعلام عمومی شدن آن، بهتر است هر چه سریع‌تر با نصب به‌روزرسانی جدید از خطرات احتمالی مصون بمانید، چرا که تمامی نسخه های ۵٫۱ به قبل تا ژوئیه ۲۰۱۷ دارای آسیب‌پذیری مشابه می‌باشند. این آسیب‌پذیری در نسخه ۷٫۹٫۱ ترمیم و اصلاح شده است.

اخبار باج افزارها

• باج‌افزار Stop: فعال‌ترین باج افزار سال گذشته به نقل از منابع خبری، در نسخه های جدید خود به فایل‌های قربانیان پسوندهای hets. را اضافه می‌کند. آلودگی به این بدافزار در کشورمان نیز گزارش شده است.

• باج‌افزار Phobos: نسخه های جدید از باج افزار Phobos اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوندهای com. را اضافه می‌کند.

• باج‌افزار Dharma: این باج افزار که چندین سال از اولین مشاهده آن می‌گذرد در نسخه های جدید خود اقدام به رمزگذاری اطلاعات قربانی با پسوندهای .kharma ،VIRUS ،nvram ،.money ، xda ،.wiki ، .bot ، .ROGER می‌کند.

• باج‌افزار Zeppelin: باج افزار نو ظهور Zeppelin که در کشورمان نیز شیوع دارد، اقدام به رمزگذاری اطلاعات قربانی با پسوند Zeppelin. می‌کند.

• باج‌افزار MegaCortex: باج افزار نو ظهور MegaCortex اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوندهای megac0rtx. را اضافه می‌کند.

• باج‌افزار Clop: این باج‌افزار که اولین بار در اوایل سال ۲۰۱۹ مشاهده شد، در حملات اخیر خود اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند Clop. را اضافه می‌کند.

• باج‌افزارRyuk: نسخه های جدید از باج افزارRyuk اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوندهای Ryuk. را اضافه می‌کند. تا به حال گزارشی از آلودگی به این باج‌افزار در کشورمان منتشر نشده است.

WWW.PADVISH.COM