بخش هفتم

امنیت در مرورگرهای وب

ادامه از صفحه اول

دسک‌تاپ فیشینگ یکی از روش‌های کلاهبرداری به قصد سرقت هویت کاربران اینترنت با استفاده از دسترسی به اطلاعات محرمانه آنان است. با وجود اینکه استفاده از این شگرد مجرمانه رو به افزایش است، افراد اطلاعات کاملی از این نوع کلاهبرداری ندارند و در دام آن گرفتار می شوند. فیشینگ به تلاش برای به دست آوردن اطلاعات شخصی کاربر گفته می شود. به عبارت ساده تر، وقتی شخصی سعی می کند کاربر را فریب دهد تا اطلاعات شخصی او را در اختیارش بگذارد، یک حمله فیشینگ اتفاق می افتد.

«فیشینگ» (Phishing) روش متداولی برای دسترسی به اطلاعات شخصی کاربران اینترنت مانند نام کاربری، رمز عبور و اطلاعات کارت های بانکی و اعتباری است. نام این روش شبیه به نام «Fishing» به معنی ماهیگیری انتخاب شده است، چون روش کار افرادی که از این طریق به اطلاعات شخصی نفوذ می کنند شباهت به ماهیگیری و شکار طعمه دارد. اما «دسک تاپ فیشینگ» روش پیشرفته فیشینگ است که در آن، کاربران به راحتی نمی توانند صفحات اصلی را از جعلی تشخیص دهند، زیرا حتی آدرس سایت جعلی نیز کاملاً با سایت اصلی یکسان است و شخص رجوع کننده به چنین سایتی در ظاهر با موارد مشکوکی مواجه نمی شود.

روش فیشینگ کمی قدیمی شده ولی روش دسکتاپ فیشینگ شیوه ای جدیدتر در زمینه سرقت اطلاعات است. مجرم در این شیوه، ابتدا با ارسال یک بدافزار به سیستم قربانی، سعی بر دستکاری در فایل هاست رایانه قربانیان را دارد و«آی پی» سایت جعلی خود را اضافه می کند و به سبب آن با این که کاربر آدرس واقعی را در آدرس بار مرورگر خود وارد می کند، به جای صفحه اصلی، صفحه جعلی باز شده و در اختیار قربانی قرار می گیرد.

قربانی نیز بی اطلاع از اتفاقات پشت پرده ای که افتاده، اطلاعات محرمانه خود را وارد صفحه جعلی می کند و در نهایت اطلاعات وی برای مجرم ارسال می شود. به این ترتیب، اطلاعات حیاتی و مهم کاربر از طریق سایت جعلی به یک در پشتی (back door) به نفع هکر وارد می شود. این شیوه نیازمند آلودگی سیستم کاربر است و مجوز آلوده شدن سیستم را خود قربانی باید صادر کند. بدین معنی که فرد هکر با استفاده

– وقتی شخصی سعی می کند کاربر را فریب دهد تا اطلاعات شخصی او را در اختیارش بگذارد، یک حمله فیشینگ اتفاق می افتد

– برای مقابله با فیشینگ و دسک تاپ فیشینگ، کاربران باید آدرس درون نوار مرورگر خود را با آدرس واقعی سایت مورد نظر تطبیق دهند

از مهندسی اجتماعی قربانی را ترغیب به اجرای فایل آلوده (تروجان) می کند.

این روش که معمولاً برای وبگاه های پرداخت آنلاین استفاده می شود، تغییر جزیی در آدرس اینترنتی صفحه اصلی به وجود می آورد که با آدرس های اصلی یک یا دو حرف تفاوت دارد و در نگاه نخست کسی متوجه آن ها نمی شود. به این ترتیب کاربر با تصور این که وارد وبگاه اصلی مورد نظر شده است، شروع به وارد کردن اطلاعات و رمز می کند. معمولاً فیشرها از طریق لینک هایی که در ایمیل می فرستند، کاربر را دچار خطا می کنند.

شیوه دیگر استفاده از «جاوا اسکریپت» برای تغییر آدرس در نوار آدرس مرورگر است که قربانی بیشتری می گیرد. در این حالت هنگامی که کاربر از وبگاه دیگری وارد سامانه بانکی خودش می شود، همه چیز به ظاهر عادی است اما در واقع آدرس پیوند به آن سامانه دستکاری می شود و فیشر به اطلاعات وارد شده دسترسی پیدا می کند. دسترسی به اطلاعات بانکی به این روش از طریق تماس تلفنی نیز ممکن است.

برای مقابله با فیشینگ و دسک تاپ فیشینگ، کاربران باید آدرس درون نوار مرورگر خود را با آدرس واقعی سایت مورد نظر تطبیق دهند و از طریق لینک های مشکوک (لینک های موجود در صفحات اینترنتی، ایمیل ها، شبکه های اجتماعی و غیره) وارد درگاه های پرداخت بانک ها، صفحات لاگین و وب سایت های مهم نشوند.

بهترین راه مقابله با فیشینگ دقت در درست بودن آدرس وبگاه ها است. همچنین می توان پیش از آن که روی آدرس وبگاه مورد نظر کلیک کرد، نشانگر را روی لینک نگه داشت تا آدرس کامل را مشاهده کرد. در این حالت با اطمینان از دانستن آدرس صحیح وارد وبگاه مقصد شویم.

در ورود به وبگاه بانک ها و مؤسسات مالی معتبر باید دقت کرد که نشانی اینترنتی با https آغاز شود. نشانی http مخصوص وبگاه های معمولی است. ممکن است اقدام به فیشینگ در وبگاهی با ظاهر درگاه ورود به حساب بانکی انجام شود که با توجه به نوار ابزار بالای صفحه و مشاهده نکردن https می توان به تقلبی بودن آن مشکوک شد.

همچنین بهتر است آدرس وب سایت را مستقیماً برای مرورگر تایپ کنیم. قبل از کلیک روی لینک باید با موس آن را متوقف کرد تا ببینیم ما را به کجا هدایت می کند. املای URL نیز دو بار چک شود. با تایپ URL در مرورگر باید املای آن را به درستی چک و تأیید کرد.

املای غلط URL ممکن است باعث کلاهبرداری فیشینگ شود. لازم است مراقب غلط املایی بود؛ کلاهبرداری های فیشینگ معمولاً از طریق غلط املایی انجام می شوند. چنانچه یک ایمیل از یک شرکت معتبر دریافت شد، نباید در آدرس آن غلط املایی وجود داشته باشد و قبل از کلیک روی لینک باید املای آن را چک کرد.ایمن ترین راه، تایپ URL در مرورگر، با املای صحیح است. زمانی که حداقل دو نوع تأیید، از جمله رمز عبور و پرسش امنیتی را قبل از ثبت حساب های حساس در اختیار داریم باید از تأیید چند سطحی استفاده کنیم.

نباید از نسخه های قدیمی سیستم عامل ویندوز استفاده شود و همواره برای به روز کردن آن اقدام کرد. باید از یک آنتی ویروس مناسب و قوی استفاده شود و همواره آن را به روز رسانی کرد.

از مرورگرهای با قابلیت آنتی فیشینگ استفاده شود و مرورگرها را باید همواره به روز کرد. از دانلود و اجرای فایل های پیوست ایمیل های مشکوک و ناشناس باید جداً خودداری شود و نرم افزارهای مورد نیاز را از سایت های معتبر دارای اصالت، خریداری و دانلود کرد. به نرم افزارهای رایگان و کرک شده که در اینترنت قرار داده می شود نباید اعتماد کرد.

***گردآوری: فرهنگ البرزی**
***عکس از: itespresso.fr**

آشنایی با باج افزارها و بدافزارها

بدافزار Slingshot

مؤسسه امنیتی کاسپراسکای از شناسایی بدافزار پیچیده و خطرناکی خبر داده است که با حمایت یکی از دولت های جهان طراحی شده و برای نفوذ به رایانه ها از روترهای اینترنتی استفاده می کند.متخصصان امنیتی این مؤسسه گروهی از هکرها را شناسایی کرده اند که از سال ۲۰۱۲ مودم های اینترنت بی سیم وای فای کاربران را هک می کرده اند.

این هکرها از شش سال پیش تاکنون در تلاش بودند به مودم و روتر وای فای کاربران نفوذ یابند و اطلاعات شخصی و محرمانه آن ها را به سرقت ببرند. کارشناسان کاسپراسکای در بیانیه خود اعلام کرده اند هکرها با انتشار یک بدافزار خطرناک و مخرب، دستگاه های اینترنت بی‌سیم وای فای کاربران را هک کرده و با روش پیچیده و هوشمندانه ای به اطلاعات مورد نظر خود دسترسی پیدا کرده اند.

بدافزار یاد شده که Slingshot نام دارد، حملات خود را به صورت کاملاً مخفیانه و لایه لایه انجام می دهد و ابتدا روترهای MikroTik را هدف قرار می دهد. این بدافزار ابتدا یک فایل library را حذف و به جای آن کدهای مخربی را جاسازی می کند و بارگذاری بقیه کدهای آلوده نیز به همین شیوه انجام می شود. سپس حمله بدافزار Slingshot به رایانه شخصی در دو مرحله صورت می گیرد. در مرحله اول هسته سیستم عامل رایانه هدف قرار گرفته و آلوده می شود و بدافزار به حافظه و اطلاعات ذخیره شده دسترسی عمقی پیدا می کند. در مرحله دوم کدهای مخرب با هدف هماهنگ سازی فعالیت های خود،

مدیریت فایل های سیستمی و فعال و هشیار نگه داشتن بدافزار اقداماتی را انجام می دهند. این بدافزار در فایل های به دقت رمزگذاری شده مخفی می شود و لذا شناسایی و مقابله با آن بسیار دشوار است.

کدهای مورد استفاده برای نگارش این بدافزار از سال ۲۰۱۲ فعال بوده اند و البته هنوز مشخص نیست کدهای یادشده برای چه فعالیت های مخربی به کار گرفته شده اند. از آن سال تاکنون، این بدافزارهزاران کاربر قربانی در مناطق مختلف جهان به خصوص خاورمیانه و آفریقا بر جای گذاشته است.

کاسپرسکی در گزارش بلند بالا و ۲۵ صفحه ای خود خاطر نشان کرده است که هکرها و مجرمان سایبری با سوءاستفاده از آسیب پذیری و حفره های امنیتی موجود روی پروتکل های مودم های وای فای توانستند که به طور چراغ خاموش و کاملاً ناشناس به رایانه و اطلاعات ذخیره شده کاربران نفوذ و دسترسی پیدا کنند.

گمانه زنی های کاسپراسکای با توجه به انگلیسی بودن بخش عمده کدنویسی ها و روان بودن زبان به کار گرفته شده نشان می دهد که احتمالاً یک یا تعدادی از کشورهای عضو گروه پنج چشم (آمریکا، انگلیس، استرالیا، نیوزلند و کانادا) در نگارش این بدافزار مخرب دخالت داشته اند. البته تحقیقات در این زمینه هنوز در جریان است.

مدت‌هاست که پژوهشگران بسیاری از امنیت ضعیف پروتکل های مودم های اینترنت بی سیم وای فای می گویند و همواره به کاربران وای فای هشدار می دهند که به امنیت سایبری در مودم های خانه یا محل کارشان اطمینان نکنند.امنیت اینترنت بی سیم وای فای همچنان در هاله ای ابهام و شک و شبهه های متعددی به سر می برد.