شنبه 15 مرداد 1390 - 09:38

ایمیل شما چگونه هک می شود

در هفته های اخیر در داخل کشور کاربران بسیاری مورد هجوم حملات هکری به ID ایمیلهای شخصی قرار گرفته اند.

در هفته های اخیر در داخل کشور کاربران بسیاری مورد هجوم حملات هکری به ID ایمیلهای شخصی قرار گرفته اند. در این موارد، از سوی قربانی ایمیلهای بدون موضوع (No Subject) به آدرسهای ذخیره شده در لیست تماس کاربر ارسال می شود.
کاربران اینترنت به موازات توسعه فناوری اطلاعات در معرض معضلی به نام حملات سایبری هکرها قرار گرفته اند که در این حملات، اطلاعات شخصی و بانکی کاربران به روشهای مختلفی مانند ایمیل با خطر سرقت مواجهند.

به گزارش خبرنگار مهر، در هفته های اخیر در داخل کشور کاربران بسیاری مورد هجوم حملات هکری به ID ایمیلهای شخصی قرار گرفته اند. در این موارد، از سوی قربانی ایمیلهای بدون موضوع (No Subject) به آدرسهای ذخیره شده در لیست تماس کاربر ارسال می شود.

این ایمیلها می توانند به عنوان مثال محتوی لینکهای تبلیغات دارویی باشند که کاربران را تشویق به خرید محصولات خود می کنند.

این نوع سایتها اغلب جعلی هستند و به محض اینکه کاربر اطلاعات شخصی و بانکی خود را برای خرید کالا وارد کند هکرها به این اطلاعات دسترسی پیدا می کنند.

چگونه یک اکانت ایمیل هک می شود

کلید لاگینگ (Keylogging)

کلید لاگینگ، آسانترین راه برای هک کردن ایمیل است. در این فرایند، هر کلیکی که کاربران بر روی صفحه کلید یک رایانه خاص می کنند ثبت می شود. این ثبت اطلاعات با نرم افزار کوچکی به نام keylogger که همچنین با عنوان "نرم افزار جاسوسی" نیز شناخته می شود امکانپذیر است.

به محض اینکه شما این برنامه را بر روی رایانه هدف نصب کنید، این نرم افزار به طور خودکار فعال شده و هر نوع کلیک و یا ضربه ای که بر روی صفحه کلید انجام می شود را ثبت می کند. از آنجا که این ضربه ها شامل نوشتن رمزعبور و نام کاربری نیز می شود، بنابراین با این نرم افزار، هکر می تواند به راحتی این اطلاعات را سرقت کند.

برای استفاده از این نرم افزار به دانش هکری بالایی نیاز نیست. هر کسی با یک آگاهی نسبی از رایانه قادر خواهد بود این نرم افزار را نصب و از آن استفاده کند. بنابراین، احتمال اینکه با استفاده از این برنامه اطلاعات شما از سوی افراد آشنا سرقت شود بسیار بالا است.

"کمین گر جاسوسی" (SniperSpy)

این نرم افزار به استفاده کننده اجازه می دهد که از راه دور رایانه شخصی شما را تحت کنترل بگیرد و تمام کارهایی را که بر روی رایانه خود انجام می دهید به صورت زنده و همزمان بر روی نمایشگر رایانه خود مشاهده کند.

این نرم افزار کاملا با هر نوع دیوار آتش (firewall) ویندوز "ایکس پی"، ویستا، ویندوز 7، ویندوز 2000 و سیستم عاملهای مک سازگاری دارد. این برنامه فعالیتهای کاربر را ثبت می کند و اطلاعات جمع آوری شده را به اکانت آنلاین هکر ارسال می کند.

با این برنامه، کاربر می تواند به تمام رمزهای عبور شامل رمز عبور شبکه های اجتماعی و اکانتهای ایمیل دسترسی پیدا کند و بدون دسترسی فیزیکی، به صورت از راه دور و مجازی به رایانه هدف وارد شود و برای مثال از جریان مکالمات روی چت و یا اطلاعات شخصی کاربر مطلع شود و یا وارد پست الکترونیک کاربر شده و ایمیلهای جعلی ارسال کند.

فیشینگ (Phishing)

در مفهوم انفورماتیکی، این اصطلاح که هم تلفظ واژه fishing به معنی "ماهیگیری" است فعالیتی غیرقانونی است که با استفاده از یک تکنیک مهندسی اجتماعی می تواند به اطلاعات شخصی کاربر دسترسی پیدا کند و به خصوص هویت کاربران را در ارتباطات الکترونیکی به ویژه پیامهای پست الکترونیک، سرویسهای چت و حتی تماسهای تلفنی سرقت کند.

در حملات فیشینگ، هکر پیامهایی را از سوی سایتهای جعلی که از گرافیک و لوگوی سایتهای رسمی تقلید کرده است برای آدرس ایمیل کاربر ارسال می کند. به این ترتیب، کاربر فریب می خورد و اطلاعات شخصی به ویژه شماره حساب جاری، شماره کارت اعتباری، کدهای شناسایی و ... را وارد این سایتها می کند.

به این ترتیب، تمام این اطلاعات از طریق سایت جعلی به یک در پشتی (back door) وارد می شود و برای مصارف جنایتکاری انفورماتیکی به ویژه جعل هویت و دسترسی به موجودی حسابهای بانکی، در اختیار هکر قرار می گیرد.

فرایند استاندارد حملات فیشینگ در پنج مرحله

-1 فیشر (هکر فیشینگ) یک پیام ایمیل را برای کاربر قربانی ارسال می کند. گرافیک و محتوای این پیام شبیه به پیامهایی است که معمولاً از سوی بانک و یا سایت معتبر خریدهای آنلاینی که کاربر در آن ثبت نام کرده است برای قربانی ارسال می شود. به این ترتیب کاربر بدون آنکه متوجه جعلی بودن پیام شود آن را باز می کند.

-2 این ایمیل تقریباً همیشه مربوط به موقعیتهای ویژه و یا بررسی رفع مشکلات ساده بر روی حساب جاری/ اکانت کاربر (مثل تمدید تاریخ کارت اعتباری) است و یا به کاربر پیشنهاد وسوسه کننده عرضه پول (مثل برنده شدن حساب بانکی و یا یک جایزه) را می دهد.

-3 ایمیلی که به مقصد ارسال شده است محتوی یک لینک است. متن این ایمیل برای گیرنده توضیح می دهد که برای حل مشکل خود با سازمان و یا شرکتی که گرافیک و لوگوی سایت آن جعل شده است بر روی این لینک کلیک کند(Fake login).

-4 لینک ارائه شده کاربر را به سایت رسمی آن سازمان هدایت نمی کند، بلکه با یک پوشش ظاهری که از سایت اصلی کپی شده است کاربر را به سروری که توسط "فیشر" کنترل می شود می رساند و از قربانی می خواهد که برای "تائید" بار دیگر اطلاعات اولیه ای چون نام، نام کاربری، رمزعبور، آدرس، شماره حساب، شماره کارت اعتباری و ... را وارد کند. به این ترتیب تمام این اطلاعات در دستان فیشر قرار خواهد گرفت.

-5 "فیشر" از این اطلاعات برای خرید کالا، انتقال وجه و یا حتی به عنوان پلی برای انجام حملات بیشتر به افراد دیگر استفاده می کند.

دفاع در برابر این حملات

پیشگیری همیشه بهتر از علاج است. بنابراین بهترین توصیه این است که در بازدید سایتهای غیرمعتبر نهایت دقت را بکنید.

در مواردی که سایت از کاربر اطلاعات شخصی، شماره حساب، رمز عبور و یا شماره کارت اعتباری را خواست، پیش از وارد کردن این اطلاعات، یک کپی از آدرس سایت را برای مقامات ذی صلاح (بخش انفورماتیک بانک و یا سایت حراجهای آنلاینی که عضو هستید) ارسال کنید تا از صحت آنها مطمئن شوید.

کاربر می تواند گردش مالی حساب خود را از طریق عابربانک و یا بر روی پروفایل حساب آنلاین خود مشاهده کند.

بسیاری از بانکها یک سرویس "اس. ام. اس" نیز در اختیار مشتریان خود می گذارند. از طریق این سرویس که SMS alert نام دارد بانک تمام گردشهای مالی حساب مشتری را برای وی ارسال می کند. به این ترتیب، در صورتیکه سارقان انفورماتیکی اقدام به موجودی حساب کاربر دسترسی پیدا کرده باشند مشتری متوجه خواهد شد.

رمز عبور ساده استفاده نکنید

یکی دیگر از روشهای دسترسی هکرها به رمز عبور کاربران، استفاده از رمزهای عبور ساده است. انتخاب رمزهای نامناسب موجب می شود که هکرها با انجام گزینه های آزمون و خطا پس از چند بار امتحان کردن به رمزعبور کاربر دسترسی پیدا کنند.

در سال 2009 موسسه "ایمپروا" متخصص در بخش امنیت در شبکه در تحقیقات خود نشان داد که میلیونها کاربر اینترنت از یک رمز عبور استفاده می کنند.

نتایج این بررسیها حاکی از آن بود که کلمات کلیدی مثل 123456، 0، passwordو abc123رایج ترین کلماتی هستند که توسط تعداد بسیار زیادی کاربر به عنوان رمز عبور اطلاعات محرمانه استفاده می شوند.

به گفته این محققان، استفاده از کلمات و یا اعدادی که به آسانی قابل شناسایی هستند یک خطر جدی برای کاربران به شمار می روند و هکرها به راحتی می توانند آنها را شناسایی کرده، وارد اکانتهای کاربران شده و اطلاعات شخصی آنها را سرقت کنند و یا به نام آنها ایمیل ارسال کنند.

خطر بزرگتر زمانی رخ می دهد که این رمزهای عبور رایج برای حسابهای جاری و یا کارتهای اعتباری مورد استفاده قرار گرفته باشند.

برخی از سایتها برای حمایت از کاربران خود و جلوگیری از حمله هکرها بلافاصله پس از چند نوبت مشخص که رمز عبور اشتباه وارد شد اکانت را مسدود می کنند.

سایتهای دیگر نیز به کاربران خود توصیه می کنند که رمزعبور خود را ترکیبی از اعداد و حروف مختلف انتخاب کنند.

"جف ماس" هکر سابق که اکنون با این شرکت امنیت انفورماتیکی همکاری می کند توصیه کرده است که کاربران حداقل باید از 12 حرف به جای 6 حرفی که به طور نرمال به کار می رود استفاده کنند. به این ترتیب کشف این کلمات کلیدی برای هکرها دشوار می شود.

همچنین شرکت مایکروسافت نیز اعلام کرده است که قصد دارد استفاده از رمز عبور "123456" و "ilovecats" را که به راحتی قابل شناسایی و نفوذ هستند، ممنوع کرده و به این شکل امکان نفوذ هکرها و استفاده از تکنیک آزمون و خطا برای ورود به اکانت کاربران سرویس Hotmailرا کاهش دهد.

رمزهای عبور قوی رمزهای طولانی و ترکیبی از حروف بزرگ و کوچک، اعداد و دیگر نشانه ها هستند. این رمزها نباید بر اساس واژه های لغتنامه ای و یا اطلاعات شخصی از قبیل تاریخ تولد باشند.
در هر صورت بهترین کار بعد از هک شدن تغییر سیستم عامل و ساده ترین کار تغییر رمز عبور است.

بوت نت (Botnet)

"بوت نت"، شبکه ای از رایانه ها است که به اینترنت متصل هستند و همگی تحت کنترل یک رایانه واحد با عنوان "بوت مستر" قرار دارند.

این رایانه ها از طریق حفره های امنیتی و یا عدم توجه لازم از سوی کاربر و یا مدیریت سیستم می توانند توسط یک ویروس انفورماتیکی و یا اسبهای تراوا (تروجانها) آلوده شوند.

پس از آلوده شدن، هکری که این شبکه بوت نت را سازمان دهی کرده است کنترل رایانه ها را از راه دور در دست می گیرد.

کنترل کننده های بوت نتها می توانند از این سیستمها برای انجام حملات مختلف سایبری استفاده کنند. برای مثال، از این رایانه های برای ارسال ایمیلهای تبلیغاتی، ایمیلهای ویروسی و هرزنامه ها استفاده می شود. بنابراین، اگر با اکانت شما ایمیلهایی برای دوستانتان ارسال شد (علاوه بر مواردی که در مورد هک شدن و دسترسی به رمزعبور پست الکترونیک گفته شد) این احتمال نیز وجود دارد که رایانه شما در یک بوت نت گرفتار شده باشد.

کاربران این رایانه ها که با اصطلاح "رایانه زامبی" و یا "رایانه برده" شناخته می شوند اغلب متوجه نمی شوند که در این شبکه به دام افتاده اند.

رایانه زامبی

رایانه زامبی، رایانه و یا دستگاه موبایلی است که پس از اتصال به اینترنت بدون اطلاع کاربر توسط یک "کراکر" و یا "ویروس" آلوده می شود و تحت کنترل یک شخص ثالث قرار می گیرد.

برپایه تحقیقاتی که در سال 2009 انجام شد 18 درصد از آدرسهای IP در آمریکا، 13 درصد در چین و 6 درصد در استرالیا رایانه های زامبی هستند.