بررسی تشخیص و صحت بلادرنگ فیشینگ وب سایت درگاه های پرداخت های اینترنتی

علی رضایی تیلکی[1]، حمید رضا خدادادی[2]

چکیده

تشخیص و شناسایی فیشینگ وب سایت بصورت بلادرنگ مخصوصا برای پرداختهای الکترونیکی درگاههای بانک مشکلی پویا و پیچیده می باشد که به عوامل و شاخص های بسیاری مرتبط می شود، مجرمان سایبری از روشهایی مانند ارسال لینک های جعلی از طریق ایمیل و هدایت کاربران به صفحات فیشینگ ، راه اندازی یک وب سایت جعلی دارای نشان نماد اعتماد الکترونیکی با امکان پرداخت اینترنتی، سوء استفاده از پروتکل HTTPS یا دستکاری در URL و DNS سیستم کاربر و غیره، کاربران را به سمت درگاه بانک الکترونیکی جعلی سوق داده و مورد حملات فیشینگ قرار می دهند.

در این مقاله ابتدا به معرفی مهمترین روش های موجود جهت تشخیص صفحات فیشینگ پرداخت های الکترونیکی بانکی پرداخته و سپس با ارائه راهکاری ابتکاری مبتنی بر برنامه نویسی با نام RTP مشکل تشخیص و شناسایی صفحات فیشینگ درگاه های بانک ها را برای عموم کاربران برطرف ساخته است.

این طرح مراحل نهایی ثبت در سازمان اسناد و املاک (اداره کل مالکیت صنعتی) است و جزئیات اجرایی و الگوریتم آن به ثبت رسیده است.

واژگان کلیدی: فیشینگ ، پرداخت اینترنتی ،بانکداری اینترنتی ، تشخیص بلادرنگ فیشینگ وب سایت ، صحت سه مرحله ای

[1] دانشجوی دکتری it، آموزش و پرورش ناحیه، ساری، ایران

Ali rezaei tiltaki
Rezaei t.ali@gmail.com

[2] دکتری حسابداری دانشگاه آزاد اسلامی واحد ساری، ایران

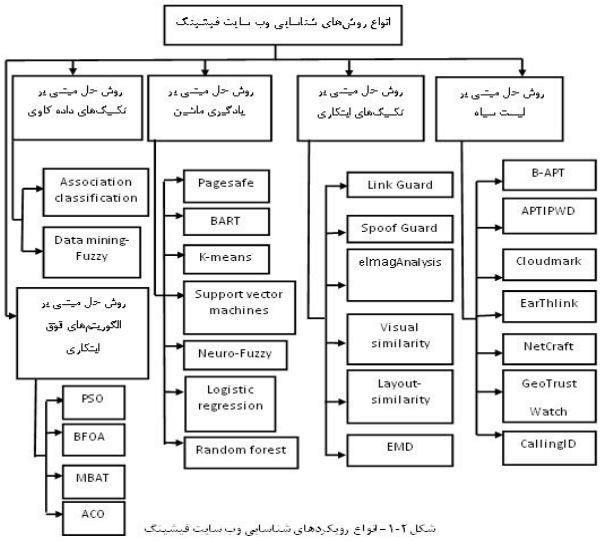
۱. مقدمه

متد فیشینگ [1] یک تکنیک قدیمی و تهدید اینترنتی است که حمله کنندگان با استفاده از روش‌هایی همچون مهندسی اجتماعی و ساختن صفحات جعلی مشابه درگاه بانک ها و هدایت کاربران به آن صفحات، در قالب خرید اینترنتی، اطلاعات کارت اعتباری و هویت فردی آنان را به دست آورده و در فرصتی مناسب اقدام به سوء استفاده از حساب آنها می کنند. . این دسته از مجرمان جهت گم کردن رد پای خود و عدم شک کاربران، گاهی بعد از ثبت مشخصات، فرد را وارد صفحه اصلی درگاه بانک می کنند و گاهی نیز با ارائه پیغامی مبتنی بر اینکه سیستم بانک در حال حاضر قادر به سرویس دهی نمی باشد اعتماد فرد را جلب می کنند.

فقدان دانش کافی کاربران در مورد انواع حملات فیشینگ زمینه ساز رخداد یک حمله موفق از سوی مجرمان سایبری خواهد شد. همچنین با بوجود آمدن شیوه های جدید فیشینگ و بروز شدن انواع بد افزارها، داشتن دانش کافی در زمینه رایانه ، اینترنت ، شبکه هم نمی تواند متضمن این امر باشد که کاربر در دام صفحات فیشینگ گرفتار نشود. در بخش بعدی مقاله ، به بازبینی کارهای انجام شده نگاهی انداخته و در بخش سوم به تشریح طرح پیشنهادی و سناریو آن می پردازیم و در بخش پایانی نیز نتیجه گیری آورده شده است .

با تمام تلاشها و اقداماتی که شرکت های بزرگ امنیتی دنیا در حوزه امنیت درگاههای بانکی انجام داده اند ، مهاجمان سایبری هم بیکار ننشسته و دانش خود را بصورت مدام بروز می نمایند و این امر موجب شده است که هر روز اخبار جدیدی پیرامون اینکه مهاجمان سایبری توانسته اند از سد نفوذ یک سیستم امنیتی عبور کنند و دست به سرقت اطلاعات بزنند به گوش برسد.

متناسب با افزایش سطح تهدیدات فیشینگ، تنوع راهکارهای شناسایی وبگاههای فیشینگ و تقابل با این تهدیدات نیز افزایش یافته است. لذا راهکارهای ارائه شده را میتوان در 5 گروه دسته بندی و تشریح نمودکه در شکل۲-۱ می توانید انواع رویکردهای این نوع تهدیدات را مشاهده کنید. [2]



شکل ۲-۱ – انواع رویکردهای شناسایی وب سایت فیشینگ

در راستای اقدامات و تدابیر امنیتی که کارشناسان بانک در این زمینه اندیشیده اند مهاجمان سایبری هم توانسته اند به روشهای نوینی اینگونه اقدامات را دور زده و مورد سوء استفاده قرار دهند. در جدول ۲-۱ می توانید برخی از موارد ذکر شده را مشاهده کنید.

هشدارها و راهکارهای امنیتی کارشناسان بانکی	راه ها و روشهای مهاجمان سایبری جهت نفوذ
اطمینان از صحت نماد اعتماد الکترونیک	ساخت وب سایت جعلی و جعل نماد اعتماد الکترونیک
وارد کردن مستقیم آدرس وب سایت در مرورگر	جعل و دستکاری پیوندها و آدرس‌ها
بررسی URL وب سایت و اطمینان از پروتکل امن https	ابداع انواع روشهای فیشینگ مانند فیشینگ کلاسیک یا دسکتاپ فیشینگ یا فیشینگ هدف دار و ....

جدول ۲-۱ اقدامات کارشناسان امنیت و روش مهاجمان سایبری

در ادامه یک مورد از نحوه چگونگی جعل و دستکاری URL وب سایت توسط مهاجمان را مورد بررسی قرار خواهیم داد.

۲-۱ فیشینگ کلاسیک و دسکتاپ فیشینگ [1]

از معروفترین مدلهای فیشینگ می توان به : فیشینگ کلاسیک و دسکتاپ فیشینگ اشاره کرد.

دسکتاپ فیشینگ [3] یک مدل جدید تر از فیشینگ کلاسیک است که مشکلاتی که فیشینگ قدیمی دارد را ندارد. مهم ترین تفاوت دسکتاپ فیشینگ با فیشینگ معمولی این است که در دسکتاپ فیشینگ آدرس لینک صفحه ای که حاوی کد مخرب است هیچ تفاوتی با لینک سایت اصلی نخواهد داشت!

یعنی نفوذ گر با آلوده کردن سیستم قربانی و تغییر در فایل مرتبط به DNS ، آدرس سایت را بصورت واقعی نمایش میدهد.

بعنوان مثال کاربر آدرس سایت را همان AOL.com می بیند و ابدآ شک نمی کند که این صفحه بتواند یک صفحه فیشینگ باشد. در حالی که در فیشینگ قدیمی، کاربر با کمی دقت و مشاهده URL صفحه وب سایت می تواند تشخیص دهد که وارد یک صفحه تقلبی شده است.

مزیت دیگر دسکتاپ فیشینگ این است میتوان با یک کد تمام سایتها را آلوده کرد و نیازی به طراحی یک صفحه تقلبی جداگانه برای هر وب سایت نیست .

درجدول۲-۲ تفاوت فیشینگ کلاسیک با دسکتاپ فیشینگ را مشاهده می کنید .

فیشینگ قدیمی	دسکتاپ فیشینگ
قابل شناسایی از طریق لینک	لینک واقعی و غیر قابل شناسایی
صفحه تقلبی جداگانه برای هر وب سایت	ایجاد اتوماتیک صفحه تقلبی برای تمام سایتها
بدون نیاز به تغییر فایل ها قربانی	نیاز به آلود کردن سیستم قربانی قبل از اجرا
بدون نیاز به IP اختصاصی	نیاز به هاست با IP اختصاصی
شناسایی توسط آنتی ویروس با احتمال کم	شناسایی توسط آنتی ویروس با احتمال بالا

جدول ۲-۲ تفاوت فیشینگ کلاسیک و دسکتاپ فیشینگ

۲. روش پژوهش

با گستردگی پرداختهای الکترونیکی میزان تهدیدهای امنیتی بخصوص برای درگاههای بانکی از قبیل فیشینگ و انواع بدافزار، افزایش چشمگیری داشته است . بهترین راهکار موجود در حال حاضر برای تشخصیص صفحات فیشینگ بررسی URL و اطمینـان از پروتکل HTTPS است به ایـن ترتیب که کاربـران می بایست ابتدا از تقبلی نبودن صفحه درگاه بانکی اطمینان حاصل کرده و سپس اقدام به درج مشخصات کارت و سایر اطلاعات لازم نمایند.

اما مشکل این روشها این است که عموم کاربران با واژه هایی همچون URL، پروتکل HTTPS، تروجان، بدافزار و انواع روشهای فیشینگ و بسیاری از واژه های دیگر رایانه آشنا نیستند و یا اکثر اوقات بی‌حوصلگی و یا عدم توجه کاربران به هشدارهای امنیتی باعث به دام افتادن کاربران در دام کلاهبرداران اینترنتی میشود. همچنین با بوجود آمدن انواع نرم افزارهای موبایل، کلاهبرداران اینترنتی با شیوه هایی جدید کاربران را در دام صفحات فیشینگ گرفتار می کنند. بدین گونه که کاربر هنگام خرید یک نرم افزار موبایل و پرداخت درون برنامه ای، اصلا قادر به دیدن URL درگاه نبوده و به راحتی در دام فیشر می افتد.

با توجه به اینکه بعضی ابزارها یا برنامه ها هستند که به کاربران در تشخیص قلابی بودن سایتهای اینترنتی کمک می کنند اما تا کنون هیچ راهکاری ساده برای مقابله با شناسایی صفحات فیشینگ درگاههای بانکی بصورت **بلادرنگ**

عنوان نشده و تمام راه‌ها کماکان دارای نقاط ضعف خاص خود هستند. اما در راه حل مبتنی بر برنامه نویسی که این مقاله به آن اشاره دارد، با نام RTP عموم کاربران قادر خواهند بود بصورت بلادرنگ و بدون نیاز به بررسی URL و یا موارد امنیتی ذکر شده صفحات فیشینگ را تشخیص دهند.

3-1 ارزیابی سناریو RTP

نحوه عملکرد RTP[1] به گونه ای است که کاربر از طریق بانک یا دستگاههای خودپرداز **رمز سومی** را بعنوان شناسایی صفحه فیشینگ ثبت و در مرحله بعدی اعدادی به دلخواه از همان رمز سوم را بعنوان کلید انتخاب و ثبت می نماید.

نحوه عملکرد رمز سوم و کلید انتخابی به گونه ای است که هنگامی که کاربر شماره کارت خود (PAN) و کد اعتبارسنجی دوم (CVV2) را وارد کرد روی دکمه نمایش کلید ، کلیک می کند و یک درخواست [2] برای سرور بانک ارسال میشود ، سرور بانک در صورت اطمینان از صحت اطلاعات وارد شده پاسخی[3] که همان رمز سوم بهمراه کلید انتخابی که بصورت رنگی متمایز شده می باشد را برای کاربر بصورت بلادرنگ نمایش میدهد

کاربر در صورت مشاهده بلادرنگ رمز سوم و کلیدی که از روی این رمز قبلا انتخاب کرده بود، اطمینان حاصل خواهد کرد که این پاسخ از طرف سرور بانک مورد نظر برایش ارسال شده و این صفحه نمی تواند تقلبی باشد در صورت هرگونه تاخیر در نمایش این اطلاعات کاربر پی خواهد برد که درگاه بانکی جعلی و از وارد کردن بقیه اطلاعات خودداری خواهد کرد .

از آنجایی که مجرمان سایبری با استفاده از روشهایی مانند ارسال لینک های جعلی از طریق ایمیل [4] و هدایت کاربران به صفحات فیشینگ، راه اندازی یک وب سایت جعلی دارای نشان نماد اعتماد الکترونیکی با امکان پرداخت اینترنتی ، سوء استفاده از پروتکل HTTPS یا دستکاری در URL و DNS [5]سیستم کاربر و غیره، کاربران را به سمت درگاه بانک الکترونیکی جعلی سوق داده و مورد حملات فیشینگ قرار می دهند این روش میتواند جلوی این نوع حملات را گرفته و آنها خنثی نماید.

در شکل ۳-۱ مراحل اجرای شناسایی صفحه فیشینگ بصورت بلادرنگ توسط کاربران نمایش داده شده است.

شکل ۳-۱ مراحل اجرای شناسایی صفحه فیشینگ بصورت بلادرنگ

حتی در صورتی که مهاجمان سایبری بتوانند کاربران را به صفحات درگاه جعلی سوق دهند و از طریق حمله مرد میانی [1] اقدام به حمله هدفمند کنند **بدلیل آنکه پروسه نمایش رمز سوم و کلید انتخابی با کلیک کردن روی دکمه بصورت بلادرنگ انجام و نمایش داده می شود می تواند این حمله فیشنگ هدفمند را خنثی خواهد شد.**

از مزیت های این روش می توان به موارد زیر اشاره کرد:

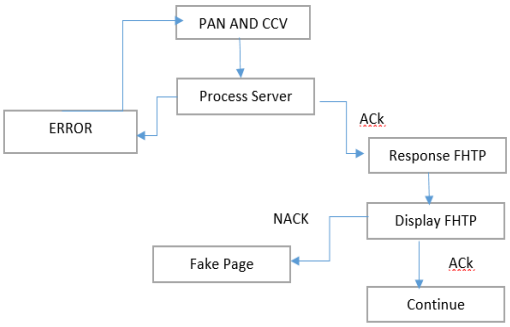
۱- چنین راهکارهایی سطح اعتماد به بانکداری اینترنتی را ارتقا می‌بخشد.

۲- بسیار ساده و کارآمد و بدون هیچ پیچیدگی خاصی میباشد.

۳- قابل شناسایی برای عموم کاربران حتی بدون داشتن دانشی خاص در زمینه کامپیوتر

۴- صرفه جویی در وقت و هزینه مشتریان و نیازی به استفاده از پیامک و هزینه های ناشی از آن نمی باشد کاهش جرائم سایبری و در نتیجه کم کردن هزینه‌های قضایی و پلیسی

در شکل ۳-۲ عملکرد شناسایی صفحات فیشینگ بصورت بلادرنگ درگاه پرداخت بانک توسط کاربران به روش
RTP نمایش داده شده است.



شکل ۳-۲ نمودار عملکرد شناسایی صفحات فیشینگ بصورت بلادرنگ درگاه پرداخت بانک به روش RTP

٤- نتیجه گیری

یکی از جدیدترین تهدیدات امنیتی در فضای مجازی، سرقت اطلاعات شخصی و مالی افراد توسط فیشر میباشد.

روشهای متنوعی در شناسایی وبگاه فیشینگ مورد بررسی و تحلیل قرار گرفته اند .در روشهای موجود، به طور همزمان به طول عمر کوتاه وبگاههای فیشینگ، کاهش حجم محاسبات و امکان تحلیل و کنترل حجم گسترده ای از وبگاهها توجه نشده است. در این مقاله به بررسی روشی مبتنی بر برنامه نویسی بصورت بهینه و بلادرنگ به نام RTP جهت تشخیص صفحات فیشینگ درگاههای بانکی برای عموم کاربران بدون داشتن دانش فنی خاص، پرداخته و مشاهده شبیه سازی در دفعات مختلف نشان می دهد که معیار استفاده از روش فوق به طور قابل ملاحظه ای درصد حملات مجرمانه به درگاه های فیشینگ را کاهش داده و شناسایی صفحات فیشنگ درگاه های بانک به صورت بلادرنگ را امکان پذیر کرده است. و نهایتا اینکه این رمز ارتباطی به امنیت ندارد و صرفا در جهت شناسایی صفحات درگاه جعلی می باشد و حتی اگر رمز سوم افشا شود کاربر می تواند به طرق مختلف آن را تغییر دهد

منابع و مآخذ

[1] Automatic Phishing Detection System Pinky M S, Neethu Tom
M.Tech Student, Dept. of CS., Mangalam College,M G university, Kottayam, Kerala, India
Assistant Professor, Dept. of CS., Mangalam College, M G university, Kottayam, Kerala, India ,august 2015

[2] لنگری نفیسه ، عبدالرزاق نژاد مجید "شناسایی وب گاه فیشینگ در بانکداری الکترونیکی با استفاده از الگوریتم بهینه سازی صفحات شیب دار". مجله علمی –پژوهشی پدافند الکترونیکی و سایبری سال سوم شماره ۱ . بهار ۱۳۹۴ .ص ۲۹-۴۰

Information Processing-2015 (IMCIP-2015) [3] Eleventh International Multi-Conference on PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach Routhu Srinivasa Rao∗ and Syed Taqi Ali

[4]A Bird's Eye view of Anti phishing Techniques for classification of phishing E-Mails NiharikaVaishnaw1, S R Tandan2
1,2Department of Computer Science and Engineering, Dr. C. V. Raman University, Bilaspur (C.G), India – June 2015

[5] Phishing webpage Detection for Secure Online Transactions Sathish.s,, Thirunavukarasu.A Department of computer science and engineer,Anna University ,March 2015