روش هاوتکنیک های فیشینگ و ضدفیشینگ

محمدعلی مسلمی[1]،mo.a.moslemi@gmail.com
جواد وحیدی[2]،دانشگاه علم و صنعت ، jvahidi@iust.ac.ir

چکیده

در دهه های گذشته ، با پیشرفت علم ، سارقان اینترنتی با تکیه بر دانش و روش های متفاوتی ،وب سایت های جعلی متعددی در شبکه جهانی وب منتشر کرده اند و با جذب اعتماد و قوه تحریک پذیری انسان و شکستن رمزهای دیجیتالی ،با هدف سرقت نام کاربری ، حساب ها ، اموال و غیره گامهای در این راه برداشتند.این نوع حملات که زیر مجموعه مهندسی اجتماعی می باشد؛ فیشینگ نام دارد.

در این مقاله در مورد فیشینگ ،ضد فیشینگ و روش ها، متدها و تکنیکهای آنها تحقیق شده است .

کلمات کلیدی

فیشینگ ، صفحات جعلی ، مهندسی اجتماعی ، فیشر، ضد فیشینگ

۱. مقدمه

فیشینگ ، سعی و تلاش برای بدست آوردن گذر واژه ، حساب کاربری ، ایمیل و غیره از طریق شبکه های اجتماعی و وب سایت های پرداخت انلاین و بانکداری الکترونیکی می باشد. نخستین هدف فیشینگ طراحی کدهای مخرب می باشد و هر فردی با دانش کم می تواند این کدها را طراحی و پیاده سازی نماید و به اهداف خود برسد.فیشینگ وابسته به نوع سیستم عامل یا سرور و غیره نمی باشد ؛ فقط به کاربر وابسته می باشد.

۲. فیشینگ چیست ؟

فیشینگ نوعی از مهندسی اجتماعی است که در آن حمله کننده با تقلید ارتباطات الکترونیکی برای جذب کاربران ، که اطلاعات محرمانه خود را ارائه دهند[1]. چنین ارتباطاتی اغلب از طریق وب سایت های جعلی ،پست الکترونیکی، تلفن برای جمع آوری اطلاعات افراد از قبیل حساب کاربری ،گذرواژه و غیره می باشد.

۳. طرح سوال

۱- آیا می توان صفحات جعلی (فیشینگ) را تشخیص داد؟
۲- فیشرها از چه روش و متدی برای بدست اوردن اطلاعات محرمانه استفاده می کنند
۳- راهکارهای مقابله با فیشینگ چه می باشد؟

۴. هدف از تحقیق

تشخیص متدها و ورش هایی که فیشرها از ان استفاده می کنند و راهکارهای مقابله با فیشینگ پرداخته شده است .

۵. انواع فیشینگ

۱- کاراکتر و واژگان
۲- بدافزارها (ویروس ، malware)
۳- شبکه های اجتماعی بر روی تلفن همراه
۴- فیشینگ مبتنی بر DNS
۵- بازی های آنلاین
۶- اتاق های گفتگو و چت
۷- ارسال پیام های لینک دار به ایمیل
۸- محتوای پنهان در تصاویر

۶. انواع حملات فیشینگ

۱- بر خط : از بستر اینترنت و با استفاده از کدهای مخرب در صفحات جعلی
۲- برون خط: از طریق وسائل فیزیکی و فریفتن افراد

۷. مهندسی اجتماعی

۷-۱. اعتماد

یکی از روشهای متداول در مهندسی اجتماعی می باشد.انسانها بطور معمول به یکدیگر اعتماد می کنند و به راحتی اطلاعات شخصی خود در زمینه های مختلف زندگی خود اعم از ایمیل ، حساب های کاربری ، آدرس و غیره در احتیار یکدیگر قرار می دهند . افراد سود جو طراحی سایت های جعلی و یا با استفاده از ابزارهاو برنامه کاربردی در این زمینه ،به شکستن رمزهای مختلف حساب کاربری افراد با توجه به آنچه از آنها داشتند می پردازند.

۸. مباحث فیشینگ

فیشینگ یک سرقت آنلاینی برای بدست آوردن اطلاعات کاربری ، رمز عبور ، اکانت های سایت ، دسترسی به حساب های بانکی و غیره می باشد. با این حال ، اموزش در این زمینه برای افراد بسیار مفید و سازنده می باشد. با توسعه فناوری و پیشرفت تکنولوژی می توان با طراحی اپلیکشن های موبایلی و یا سایت های آموزشی مرتبط با فیشینگ و ضد فیشینگ کاربران رسانه های دیجیتالی را برای محافظت از خود در برابر این نوع حملات پرداخت و سطح شناخت و دانش افراد را در صفحات جعلی و مهندسی اجتماعی بالا برد .

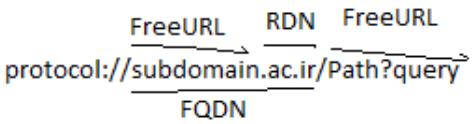
در این قسمت مباحث مهمی در زمینه، فیشینگ ، ساختار URL و منابع داده (ساموئل مارچال وهمکارانش،۲۰۱۶)[2] شرح داده شده است.

۸-۱. فیشینگ

فیشینگ اشاره به کلاس حملات دارد که قربانی را به یک صفحه وب جعلی که به عنوان یک وب سایت هدف مورد استفاده قرار می گیرد تحریک می کند. برای اینکه صفحات فیشینگ قابل اعتماد باشد ، فیشر ممکن است برخی از محتوا(HTMLکد،تصاویر و غیره)بطور مستقیم از وب سایت هدف می گیرند.[3]

۸-۲. URL

uniform resource locator (URL) نشانی عمومی تمامی منابع و صفحات برای آدرسهای وب سایت می باشدکه مطابق شکل ۱ می باشد



شکل ۱. ساختار URL

fully qualified domain name(FQDN)محل دقیق یک کامپیوتر در شبکه یا DNS می باشد

registered domain name (RDN) نام دامنه ثبت شده است

8-3. منابع اطلاعات

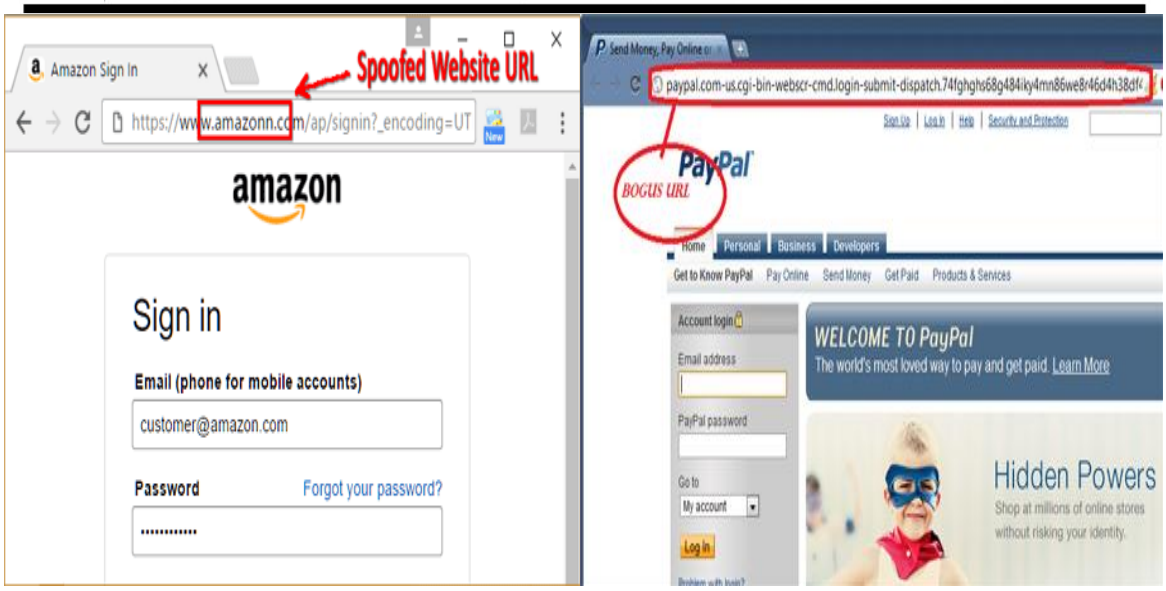
ازتجزیه وتحلیل صفحات وب فیشینگ ، شناسایی منابع داده زمانی که صفحه بارگذاری می شود در دسترس می باشد؛که می تواند در شناسایی صفحات فیشینگ مفید باشد. این موارد :

- شروع URL: نشانی اینترنتی داده شده به کاربر برای دسترسی به سایت
- آدرس فرود: آخرین URL نشان دهنده محتوای ارائه شده به کاربر می باشد
- زنجیره هدایت مجدد:مجموعه ای ازURL رفته شده ازشروع URL تا ادرس فرود
- HTML:کدهای HTML وIFRAMES موجود در صفحه

۹. تمرکز بر واژگان

الگوریتم وروش های متفاوتی درزمینه شناسایی صفحات جعلی پیشنهادشده است. الگوریتم هایی مانند الگوریتم چک کردن استاتیک HTML و یادگیری ماشین (هو وای تی و همکارانش ،۲۰۱۰)[4] اگرچه الگوریتم چک کردن صفحات استاتیک سریعتر است[5]؛و ویژگی های واژگان[6] ، ویژگی های WHOIS [7]و غیره پیشنهاد شده است .اکثر صفحات URL سایت های فیشینگ از موارد فوق تقلید می کنند[۸] وبه طراحی صفحات می پردازند.

صفحات فیشینگ با کم یا اضافه نمودن کلمات در URL سایت مطابق شکل ۲ طراحی می شوند.سارقان سایت هایی که دارای رنکینگ بالا در الکسا یا موتورهای جستجو از جمله گوگل می باشند برای انجام اعمال فریبانه استفاده می نمایند



شکل ۲. تمرکز بر واژگان

در این دو شکل مشاهده می کنید که در شکل اول مربوط به صفحه جعلی سایت https://www.paypal.com/ ،بدون داشتن https و استفاده از واژگان متعدد می باشد و در شکل دوم مربوط به صفحه جعلی سایت https://www.amazon.com می باشدکه در این صفحه با استفاده از تکرار کلمه(یااستفاده از عدد ۰ بجای حرف o) و تکنیک خطای دید سایت فیشینگ طراحی شده است.

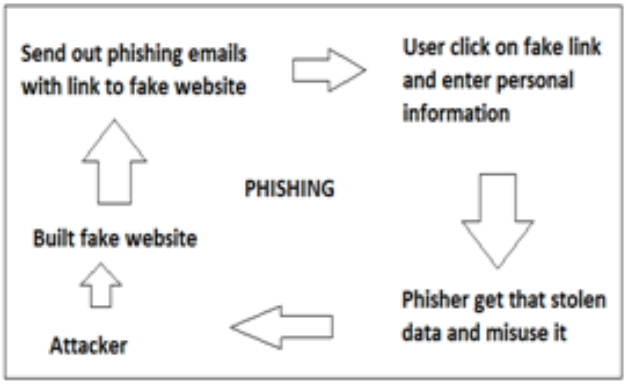
یکی دیگر از روشهایی که سارقان از آن استفاده می کنند و کارایی بیشتری دارد استفاده از کاراکترهایی که کلمات قبلی را منفی می کنند و تاثیری در URL صفحه ندارند.یکی از کارکترها @ می باشد. بهURL زیر توجه فرمائید:

Google.com@yahoo.com

با تایپ این کلمات در url سایت yahoo.com بالا می آید.این متد یکی از روش های مورد علاقه سارقان اینترنتی می باشدکه با قراردادن وبسایت جعلی بعد از کاراکتر @ می باشد .

۱۰. فیشینگ ایمیل

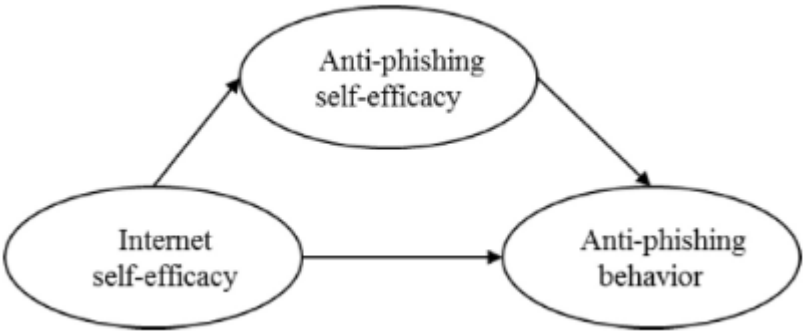
یکی از متداولترین روش دست یابی به حساب کاربری وگذر واژه مطابق شکل ۳[9] ،ارسال ایمیل به قربانیان می باشد. در این روش فیشر با ارسال ایمیل به افراد که وانمود می کند از طرف سازمان یا بانکی می باشد اقدام به سرقت می کند.در این روش فیشر برای جذف افراد با فرستادن پیامی مانند "گذر واژه کارت اعتباری شما مستهلک شده است گذر واژه خود را ازطریق لینک زیر وارد کنید " اقدام می کند.فیشر طوری سایت هدف را طراحی می کند که بسیار شبیه به سایت واقعی می باشد سپس با وارد کردن حساب کاربری و گذر واژه توسط کاربر پیغام خطایی برای کاربر نشان داده می شود حال حساب کاربری و گذرواژه در پایگاه داده سرور فیشر ذخیره می شود.



شکل ۳. فیشینگ ایمیل

۱۱. تاثیر فواید اینترنت بر فیشینگ

مطالعه و تحقیق (جری چین و همکارانش ،۲۰۱۶)[10] بر روی دانشجویان دانشگاه با مقیاس خودکارآمدی اینترنت و مقیاس رفتار ضد فیشینگ نشان داد که خود، فایده اینترنت یک پیش فرض مثبت برای رفتارهای ضدفیشینگ است و خود، فایده ضد فیشینگ به طور معنا داری ارتباط بین خودکارآمدی اینترنت و رفتارهای ضد فیشینگ را بر عهده داردمطابق شکل ۴و مربیان می توانند ازاستراتژی هایی برای بهبود خودکارآمدی اینترنت و ضد فیشینگ استفاده نمایند.



شکل ۴. مدل تحقیقی جری چین و همکارانش

با این موضوع ، مطالب بسیار زیادی در سطح اینترنت در مورد فیشینگ وضد فیشینگ قرار دارد . افراد با مطالعه این مطالب سطح آگاهی های خودرا بالابرده و با جمع آوری اطلاعات در زمینه فیشینگ وضد فیشینگ به دانش خود می افزایند . در مقابل نفوذگران فیشینگی نیز علاوه بر همین عمل ، شروع به روش های نوین در این زمینه می پردازند واین روند، با استفاده از اینترنت تاثیرگذار می باشد.

۱۲. راه پیشگیری از فیشینگ

۱- باز نکردن ایمیل در صورت مشکوک بودن
۲- استفاده از سیستم های اختصاصی برای پرداختی ها
۳- غیرفعال نمودن فلش مموری بر روی سیستم
۴- به روز بودن فایروال ها و نرم افزارها

۵- استفاده از سیستم مجزا در صورت مشاهده پیام های مشکوک
۶- گزارش به مراجع بالا در صورت مشاهده سایت های فیشینگی

۱۳. راهکارهای ضد فیشینگ

۱- استفاده از گذر واژه های یکبار مصرف
۲- استفاده از توکن سخت افزاری
۳- طراحی وب سایت های با پایگاه داده عظیمی از وبگاهای معتبر
۴- استفاده از وبگاههایی که با https شروع می شوند.(فیشرها به طراحی سایت های جعلی با استفاده از پروتکل https پرداخته اند)
۵- تمرکز بر روی واژگان URL

۱۴. پیشنهاد

استفاده از گذر واژه های یکبار مصرف برای ورود به حساب کاربری و بانکداری الکترونیکی می باشد. در این روش در صورت صحیح وارد کردن گذر واژه در سایت های جعلی ، امکان استفاده مجدد از گذر واژه برای فیشر نباشد.در صورت ورود مجدد شخص به سایت ، سازمانها و یا بانکها با ارسال گذر واژه جدید به تلفن همراه شخص ، امکان ورود به سایت برای فرد امکان پذیر شود.

۱۵. نتیجه

در دهه گذشته ، وبا پیشرفت علم سارقان اینترنتی با طراحی صفحات جعلی اقدام به جمع آوری اطلاعات از افراد نموده اند در این راستا با کسب دانش و آگاهی در سطح ملی واستفاده از راهکارهای مقابله با فیشینگ و بهره گیری از گذر واژه های یکبار مصرف بتوان در این زمینه ، فعالیت های فیشر به ثمر نرسد.

مراجع :

[1].JIAN MAO , WENQIAN TIAN , PEI LI , TAO WEI ,AND ZHENKAI LIANG.Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity.2017 IEEE

[2].Samuel Marchal , Kalle Saari , Nidhi Singh and N. Asokan.Know Your Phish: Novel Techniques for Detecting Phishing Sits and Their Targets.1063-6927/16 $31.00 . 2016 IEEE

[3]. Y. Pan and X. Ding, "Anomaly based web phishing page detection,in Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC), 2006, pp. 381–392.

[4].Hou Y T, Chang Y, Chen T,et al. Malicious web content detection by machine learning. Expert Systemswith Applications, 2010(01): 55-60.

[5].Wang Haifeng, Duan Youxiang. Virus detection based on behavior analysis engine improvement research.Computer applications. 2004(24):109-110.

[6].vJ. Ma, L.K. Saul, S. Savage, G.M. Voelker. Beyond Blacklists: Learning to detect malicious web sites frsuspicious URLs, In: Proc. 15th ACM SIGKDD Conf. Knowledge Discovery and Data Mining, PaFrance, 2009:1245-1254.

[7].Chen Zhuang, Liu Longfei. Malicious sites detectiobased on the information of registration authorComputer CD software and application. 2015

[8].Ying Xue,Yang Li,Yuangang Yao,Xianghui Zhao,Jianyi Liu,Ru Zhang.Phishing Sites Detection Based On URL correlation.978-1-5090-1256-5/16/$31.00. 2016 IEEE

[9].Monali Deshmukh , Shraddha K. Popat , D .Y. Patil.Different Techniques for Detection of Phishing Attack. International Journal of Engineering Science and Computing, April 2017

[10]. Jerry Chih,Yuan Sun, Katherine Pin-Chen Yeh.The effects of attention monitoring with EEG biofeedback on university students' attention and self-efficacy: The case of anti-phishing instructional materials.2016 ELSEVIER