



مرکز آموزش الکترونیکی دانشگاه علم و صنعت

روشهای تشخیص حملات فیشینگ و راههای مقابله با آنها

پایان نامه برای دریافت درجه کارشناسی ارشد در رشته مهندسی فناوری اطلاعات
گرایش مخابرات امن

شکرالله شکری

استاد راهنما:

دکتر رضا پرنگی

بهمن ماه ۱۳۹۰



اجرای این پایان نامه مورد حمایت مالی سازمان بنادر و دریانوردی قرار گرفته است و سازمان به عنوان تنها مرجع حاکمیتی کشور در امور بندری، دریایی و کشتیرانی بازرگانی به منظور ایفای نقش مرجعیت دانشی خود و در راستای تحقق راهبردهای کلان نقشه جامع علمی کشور مبنی بر "حمایت از توسعه شبکه‌های تحقیقاتی و تسهیل انتقال و انتشار دانش و سامان‌دهی علمی" از طریق "استانداردسازی و اصلاح فرایندهای تولید، ثبت، داوری و سنجش و ایجاد بانک‌های اطلاعاتی یکپارچه برای نشریات، اختراعات و اکتشافات پژوهشگران"، اقدام به ارایه این اثر در سایت SID می‌نماید.



سازمان بنادر و دریانوردی

چکیده

فیشینگ یک نوع حمله اینترنتی در سطح وب می باشد که هدف اساسی آن سرقت مشخصات فردی کاربران می باشد. در حمله فیشینگ مهاجم تلاش می کند اطلاعات حیاتی و محرمانه کاربران مانند نام کاربری، رمز عبور و شماره کارت اعتباری را با فریب دادن افراد از طریق تغییر قیافه دادن و ظاهر شدن به عنوان یک شخص یا شرکت معتبر در ارتباطات الکترونیکی بدست آورد. در حقیقت فیشینگ یک شکل از دزدی برخط می باشد که از طریق فریب دادن کاربران کامپیوترها و بدست آوردن اطلاعات شخصی آنها با استفاده از وبسایت جعلی اتفاق می افتد. فارمینگ یکی از گونه های پیشرفته حملات فیشینگ می باشد که از نقاط ضعف سرویس نام دامنه¹ برای تغییر جهت ترافیک یک سایت وب به سایتی دیگر سوء استفاده می کند. به عبارت دیگر فارمینگ یک حمله بر روی یک DNS سرور است که به فیشر امکان می دهد کاربران را از سایت واقعی به سایت جعلی هدایت نماید. تاکنون روشهای مختلفی برای مقابله با حملات فیشینگ ارائه شده اند اما هیچکدام از آنها نتوانسته اند این حمله را به صورت کامل متوقف سازند. در این پایان نامه ضمن مرور حملات فیشینگ و روشهای جلوگیری از آنها، راهکاری جهت مقابله با این حمله ارائه شده است که با ساز و کارهای کنونی دنیای وب همخوانی داشته و بکارگیری آن نیازی به اعمال تغییرات گسترده در ابزارهای کنونی وب ندارد. در روش ارائه شده سعی بر این است تا با پوشش آسیب پذیری سرویس های نام دامنه، از دسترسی کاربران به سایت جعلی جلوگیری بعمل آورده تا بدین ترتیب با نوع جدید حملات فیشینگ موسوم به فارمینگ مقابله گردد. نتایج آزمونهای آماری نشان داده که این روش از نرخ موفقیت بسیار بالائی برخوردار بوده و در جلوگیری از حملات فارمینگ کارائی مناسبی داشته و تقریباً صد درصد حملات فارمینگ را به خوبی تشخیص می دهد.

کلمات کلیدی: فیشینگ، فارمینگ، سرقت اطلاعات، حملات اینترنتی، امنیت اطلاعات

¹ Domain Name Service(DNS)

فهرست مطالب

فصل اول: مقدمه

- 1-1 حملات اینترنتی 2
- 2-1 موضوع و اهداف پایان نامه 3
- 3-1 مراحل اجرای پایان نامه 4
- 4-1 ساختار پایان نامه 5

فصل دوم: شناخت حملات فیشینگ

- 1-2 مقدمه 7
- 2-2 شناخت فیشینگ 7
- 3-2 بررسی آماری حملات فیشینگ 9
- 4-2 گام‌های اجرای حمله فیشینگ 11
- 5-2 گونه‌های مختلف حملات فیشینگ 13
- 1-5-2 حملات فیشینگ مبتنی بر فریبکاری 13
- 1-1-5-2 فیشینگ سنتی 13
- 2-1-5-2 فیشینگ سرنیزه یا فیشینگ هدفدار 14
- 2-5-2 حملات فیشینگ مبتنی بر بدافزار 16
- 1-2-5-2 استفاده از نصب بدافزارهای ثبت کلید 16
- 2-2-5-2 ربودن نشست 17
- 3-2-5-2 تروجان وب 17
- 4-2-5-2 آلوده کردن فایل میزبان 17

18تنظیم مجدد سیستم	5-2-5-2
18سرقت اطلاعات	6-2-5-2
18حملات فیشینگ مبتنی بر DNS	3-5-2
18حمله فیشینگ مرد میانی	4-5-2
19حمله فیشینگ تزریق محتوا	5-5-2
19حمله فیشینگ موتور جستجو	6-5-2
20بررسی ایمیل‌های فیشینگ	6-2
22ساختار وبسایت‌های فیشینگ	7-2
23ترفندهای مورد استفاده توسط فیشرها	8-2
24جعل شرکتهای مشهور	1-8-2
25تفاوت آدرس فرستنده و آدرس پاسخ ایمیل	2-8-2
25ایجاد یک فرضیه قابل باور	3-8-2
25نیاز به پاسخ فوری	4-8-2
25وعده امنیت	5-8-2
26مخفی کردن لینک	6-8-2
استفاده از آدرس IP26	7-8-2
26استفاده از لینک‌های مبهم	8-8-2
27استفاده از لینک‌های تصویری	9-8-2
27استفاده از آدرس‌های هوموگراف	10-8-2
27هدایت مجدد آدرس	11-8-2
28تغییر پورت پیش فرض	12-8-2

28 9-2 نتیجه‌گیری

فصل سوم: روشهای جلوگیری از حملات فیشینگ

30 1-3 مقدمه

31 2-3 روشهای مقابله با فیشینگ

31 1-2-3 مرحله اول: ایجاد و ارسال لینکهای بدکار

33 2-2-3 مرحله دوم: دریافت پیوند بدکار توسط کاربران

37 3-2-3 مرحله سوم: هدایت به سایت جعلی و نمایش سایت

37 4-2-3 مرحله چهارم: ورود اطلاعات محرمانه کاربر در سایت جعلی

39 1-4-2-3 نوار ابزار اسپوفاستیک

39 2-4-2-3 نوار ابزار اسپوف‌گارد

39 3-4-2-3 نوار ابزار eBay's Account Guard

39 4-4-2-3 نوار ابزار نت‌کرفت

40 5-4-2-3 نوار ابزار وب‌والت

41 6-4-2-3 نوار ابزار آنتی‌فیش

42 7-4-2-3 نوار ابزار مرور امن گوگل

42 8-4-2-3 نوار ابزار ارثلینک

43 9-4-2-3 نوار ابزار پوسته امنیتی پویا

43 10-4-2-3 فیلتر ضد فیشینگ اینترنت اکسپلورر

43 11-4-2-3 نوار ابزار سایبر دیفندر

44 12-4-2-3 نوار ابزار NC

44 13-4-2-3 نوار ابزار Prevx SafeOnline

45 14-4-2-3 نوار ابزار فیش لاک
47 5-2-3 مرحله پنجم: انتقال اطلاعات کاربر
48 6-2-3 مرحله ششم: جعل هویت کاربر
48 1-6-2-3 احراز هویت دوفاکتوری
49 2-6-2-3 درهم سازی اسم رمز
49 7-2-3 مرحله هفتم: دریافت وجه از حساب کاربر
50 3-3 نتیجه گیری

فصل چهارم: تشریح روش پیشنهادی جهت جلوگیری از حملات فیشینگ

52 1-4 مقدمه
52 2-4 حملات فارمینگ
54 3-4 تشریح روش پیشنهادی
57 4-4 تحلیل و ارزیابی روش پیشنهادی
62 1-4-4 آزمون مقایسه دو گروه از داده‌های مستقل
66 2-4-4 آزمون مقایسه دو گروه از داده‌های وابسته
71 3-4-4 تحلیل رگرسیون
76 5-4 نتیجه گیری

فصل پنجم: جمع‌بندی و نتیجه گیری

78 1-5 مرور
79 2-5 کارهای آتی
80 3-5 نتیجه گیری
81 منابع
86 فرهنگ لغات