مهمان سردبیر

مجرمان اینترنتی در تکاپوی جاسوسی از پژوهشگران

در حدود یک ماه پیش رایانامه ای از جانب سردبیر یکی از مجلات معتبر ISI دریافت کردم. در این رایانامه از من خواسته شده بود که با کلیک روی لینک موجود در رایانامه، فرم حق انتشار مقاله را فراخوانی کرده و پس از امضا برای آنها ارسال کنم. بنده قبلاً با سردبیر این مجله مکاتبات علمی داشتم، ولی مقاله ای برای این مجله ارسال نکرده بودم تا نیاز به فراخوانی و پر کردن چنین فرمی باشد. وقتی روی لینک جاسازی شده درون رایانامه کلیک کردم به صفحه وبی هدایت شدم که از من تقاضا میکرد با نام کاربری و رمز عبور رایانامهام وارد شوم. از آنجایی که من از سرویس رایانامه Gmail استفاده میکنم برای ورود گزینه‌ای با نام کاربری و رمز عبور این سرویس وجود داشت. همچنین امکان ورود با حساب‌های کاربری مختلف نیز فراهم بود. با توجه به اینکه زمینه علمی و پژوهشی سابق بنده، امنیت اطلاعات بود متوجه شدم که با حمله ای از نوع فیشینگ روبه رو هستم. در ادبیات امنیت اطلاعات، حمله فیشینگ به تلاش مجرمان اینترنتی برای سرقت نام کاربری و رمزهای عبور کاربران به وسیله سایتهای جعلی گفته میشود. در این حمله، مهاجمان اینترنتی با طراحی سایتهایی شبیه به سایتهای قانونی و معتبر اقدام به فریب کاربران و هدایت آنها به صفحات جعلی خود میکنند. وقتی کاربران فریبخورده اطلاعات خود را در وبسایتهای ساخته شده توسط مجرمان وارد میکنند اطلاعات آنها سرقت شده و مورد سوءاستفاده قرار می‌گیرد. به طور خلاصه یک حمله فیشینگ از چهار مرحله اصلی به شرح زیر تشکیل شده است: ابتدا مجرمان اینترنتی هدف خود را انتخاب میکنند؛ سایتی شبیه به سایتی که قصد سرقت اطلاعات کاربران آن را دارند، طراحی میکنند؛ مجرمان اینترنتی در تکاپوی جاسوسی از پژوهشگران رهیافت با ارسال رایانامه های متعدد و هرزنامه ها ، لینک سایت جعلی خود را بین کاربران مختلف توزیع میکنند. محتوای هرزنامه های فریبنده به گونهای نگارش میشود تا افراد را مجاب کند که با یک ایمیل مهم از طرف یک نهاد قانونی روبه رو هستند. هنگامی که افراد فریب‌خورده سایتهای فیشینگ را مشاهده کرده و اطلاعات خود را وارد میکنند، مجرمان اینترنتی اقدام به سرقت اطلاعات آنها می‌کنند.

در حمله فیشینگی که من با آن روبه رو شدم مجرمان اینترنتی توانستند با استفاده از نقص امنیتی موجود در سرور مجله مورد بحث، نام کاربری و رمز عبور وی را سرقت کنند. سپس با استفاده از رایانامه وی اقدام به ارسال رایانامه‌های متعدد با محتوای فریبنده بهمنظور سرقت رمز عبور و نام کاربری تمام پژوهشگرانی کنند که این سردبیر قبلاً با آنها مکاتباتی داشته است.

به طور کلی، هدف بیشتر حملات فیشینگ، منافع مالی است و مجرمان اینترنتی برای کسب درآمدهای مالی اقدام به حملاتی از این قبیل میکنند و اغلب به منظور سرقت اطلاعات کارت‌های اعتباری صورت می‌پذیرند. از آنجایی که با سرقت اطلاعات حساب‌های رایانامه‌ای پژوهشگران، اهداف مالی قابل توجهی به دست نمی‌آید. بنابراین می‌توان این چنین قلمداد کرد که مجرمان اینترنتی به جاسوسی از پژوهشگران و احتمالاً فروش اطلاعات آنها روی آورده‌اند. در برخی از حملات فیشینگ، مجرمان اقدام به ارسال رایانامه‌هایی با محتوای فریبنده به قربانیان خود می‌کنند که در آنها اطلاعات دقیقی ارائه شده است و کمتر کسی پی به جعلی بودن آنها میبرد؛ به طور مثال، از یافته‌های علمی پژوهشگری تمجید شده و وی را به عضویت در یک سامانه علمی دعوت میکنند، در حالی‌که سامانه علمی مطرح شده درچنین رایانامه‌هایی در واقع یک سایت فیشینگ است. چنین حملات فیشینگی «حملات فیشینگ هدفمند» نام گرفته اند.

در سالهای اخیر حملات فیشینگ هدفمند در حال گسترش و ورود به دنیای اکادمیک هستند. پژوهشگران همواره با دریافت رایانامه هایی از جانب افراد شناخته شده، مؤسسات، دانشگاه‌های معتبر و سازمان‌های بین-المللی روبه رو هستند که محتوای مشکوکی را به اشتراک می‌گذارند. در این رایانامه‌های مشکوک از پژوهشگران خواسته می‌شود تا اطلاعات شخصی خود را به رایانامه‌ای خاص ارسال کرده یا اطلاعات حساب کاربری خود را در وبسایتی وارد کنند. در بعضی موارد این رایانامه‌ها شامل فایل پیوست هستند. در صورتی که پژوهشگران دریافت کننده چنین رایانامه هایی، اطلاعات خود را در سایت های مشکوک وارد کنند مورد سوءاستفاده های بعدی توسط مجرمان اینترنتی قرار خواهند گرفت.

همچنین اغلب فایل‌های پیوست موجود در این رایانامه های مشکوک، آلوده به بدافزارهای پیچیده رایانه ای هستند که توسط بیشتر نرم افزارهای ضدویروس قابل شناسایی نیستند. ممکن است این پرسش مطرح شود که چگونه مجرمان اینترنتی می‌توانند با استفاده از رایانامه رسمی دانشگاه‌ها و مراکز شناخته شده و یا پژوهشگران، اقدام به ارسال رایانامه‌هایی با محتوای مخرب کنند؟

جواب این پرسش در نقص‌های امنیتی موجود در شبکه‌های اینترنتی فعلی نهفته است. در برخی موارد مجرمان اینترنتی با استفاده از آسیب‌پذیریهای موجود در سرور و وبسایت چنین نهادهایی اقدام به سرقت رمز عبور و حساب‌های کاربری رایانامه افراد شناخته‌شده میکنند. سپس با استفاده از حساب‌های کاربری ربوده شده اقدام به فریب سایر پژوهشگران میکنند. در موردی که در ابتدای این نوشته شرح آن داده شد مجرمان از چنین روشی استفاده کرده‌اند. راه دوم، تکنیک جعل آدرس رایانامه است. به دلیل وجود نقصهایی در پروتکل TCP/IP فعلی که ارتباطات شبکه‌ای دنیا برمبنای آن صورت میپذیرد، این امکان برای مهاجمان و مجرمان اینترنتی وجود دارد

تا به راحتی بتوانند از هر آدرس رایانامه‌ای اقدام به ارسال محتوا کنند. در این روش مجرمان اینترنتی تنها قادر به ارسال چنین رایانامه‌هایی هستند و قادر به دریافت پاسخ‌های ارسالی قربانیان نیستند. به همین دلیل در بیشتر این رایانامه‌های جعل شده به این روش، از قربانیان خواسته شده است تا روی لینکی کلیک کرده و یا پاسخهای ارسالی خود را به آدرس رایانامه دیگری به‌جای ارسال پاسخ به آدرس رایانامه فرستنده ارسال کنند. بهترین راه برای حفاظت پژوهشگران از چنین خطرهایی، استفاده از ابزارهای ضدویروس مطمئن و بهروز شده و رعایت اصول امنیتی در فضای مجازی است. همچنین پژوهشگران باید از پاسخ به رایانامههایی با محتوای مشکوک که تقاضای پاسخ سریع یا ارسال اطلاعات شخصی میکنند، خودداری کنند.

رفع مسئولیت: این نوشته علمی تنها با هدف آگاهسازی پژوهشگران و دانشمندان کشور عزیزمان به نگارش درآمده و دور از هرگونه سوءگرایی و غرضورزی است. طبیعی است که مسئولیت هرگونه سوءاستفاده از محتوای این نوشته بر عهده شخص خاطی خواهد بود.

مهدی دادخواه

منابع

[۱] Dadkhah M and Bianciardi G. (۲۰۱۶). Hackers Spy Scientists. Indian Pediatrics, ۵۳ (۱۱), pp. ۱۰۲۷.

[۲] San Martino A and Perramon X. (۲۰۱۰). Phishing Secrets: History, Effects, and Countermeasures. International Journal of Network Security, ۱۱(۳), pp. ۱۶۳-۱۷۱.

[۳] Parmar B. (۲۰۱۲). Protecting against spear-phishing. Computer Fraud & Security, ۲۰۱۲(۱), pp. ۸–۱۱. DOI: ۱۰,۱۰۱۶/S۱۳۶۱-۳۷۲۳(۱۲)۷۰۰۰۷-۶