Ouch! دسامبر 2024

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

SANS SECURITY AWARENESS

پرده برداری از سایه ها: چگونه مجرمان سایبری رمزهای عبور شما را می دزدند

یک کابوس دیجیتال: قرار گرفتن در معرض ناخواسته لیزا

لیزا، یک طراح گرافیک با استعداد خلاقیت، بیشتر زندگی خود را به صورت آنلاین گذراند. او تعاملات بانکی، خرید و اجتماعی خود را از طریق برنامه ها و وب سایت های مختلف مدیریت می کرد. یک روز، او متوجه برداشت‌های عجیب و غریب از حساب بانکی‌اش شد – اقلامی که هرگز از فروشگاه‌هایی که هرگز به آن سر نزده بود، نخریده بود. حساب‌های رسانه‌های اجتماعی او سپس شروع به ارسال پیام‌های اسپم برای تبلیغ محصولات و خدمات عجیب و غریب کردند و دوستان گزارش دادند که ایمیل‌های غیرعادی از او دریافت کرده‌اند.

وقتی لیزا متوجه شد که کنترل هویت دیجیتال خود را از دست داده است، وحشت زده شد. عکس های شخصی او فاش شد و مکالمات خصوصی او نیز در دسترس قرار گرفت. مشتریان شروع به زیر سوال بردن قابلیت اطمینان او کردند و شهرت او ضربه خورد. پس از مشورت با کارشناسان امنیت سایبری، لیزا متوجه شد که رمزهای عبور او به خطر افتاده است. مجرمان سایبری به حساس ترین حساب های او دسترسی پیدا کرده بودند و دنیای دیجیتال او را تکه تکه آشکار می کردند. این سوال مطرح شد: چگونه این اتفاق افتاد؟

تاکتیک های پنهان مجرمان سایبری: پنج روش رایج

عوامل تهدید سایبری از تکنیک های مختلفی برای جمع آوری رمز عبور استفاده می کنند. در اینجا پنج راه متداول وجود دارد که آنها می توانند مانند لیزا رمزهای شما را بدست آورند:

1. **حملات مهندسی اجتماعی**

مهندسی اجتماعی جایی است که مهاجمان خود را به عنوان کسی یا چیزی که می‌شناسید یا به آن اعتماد دارید، ظاهر می‌کنند و شما را فریب می‌دهند تا کاری را انجام دهید که نباید انجام دهید. آنها ایمیل‌ها یا پیام‌هایی می‌فرستند که مشروع به نظر می‌رسند، که اغلب باعث ایجاد حس شدید فوریت، ترس یا کنجکاوی می‌شوند.

چگونه اتفاق افتاد: لیزا ایمیلی دریافت کرد که به نظر می‌رسید از بانک او بود، همراه با آرم‌ها و برندهای رسمی. این ایمیل ادعا می‌کرد که فعالیت مشکوکی در حساب او وجود دارد و از او می‌خواست برای تأیید هویتش روی پیوندی کلیک کند. این پیوند به یک وب‌سایت جعلی منتهی شد که اعتبار ورود او را هنگام وارد کردن آنها ضبط کرد.

2. **بدافزار**

بدافزار نرم افزار مخربی است که برای آلوده کردن رایانه ها طراحی شده است. مجرمان سایبری پس از آلوده شدن می توانند هر کاری که می خواهند انجام دهند. کی لاگرها (گاهی اوقات به آنها سارقان اطلاعات نیز گفته می شود) نوعی بدافزار هستند که هر ضربه زدن روی یک دستگاه از جمله ورود به سیستم، گذرواژه ها و سایر داده های حساس را ضبط می کنند.

چگونه اتفاق افتاد: لیزا آنچه را که فکر می کرد یک بسته فونت قانونی برای کار طراحی خود دانلود کرد. داخل آن یک کی لاگر پنهان بود که خودش را روی کامپیوترش نصب می کرد. با گذشت زمان، جزئیات ورود او را برای حساب های مختلف ضبط کرد و آنها را برای مهاجم ارسال کرد.

3. حملات Brute Force

در حملات brute force، مجرمان سایبری از ابزارهای خودکار استفاده می کنند تا ترکیب های رمز عبور متعددی را امتحان کنند تا زمانی که درست را حدس بزنند. رمزهای عبور ضعیف به ویژه در برابر این روش آسیب پذیر هستند.

چگونه اتفاق افتاد: لیزا از رمزهای عبور ساده ای مانند "lisa2020" برای بسیاری از حساب های خود استفاده کرد. مهاجمان از نرم‌افزاری استفاده می‌کردند که به‌طور سیستماتیک رمزهای عبور رایج را امتحان می‌کرد و به راحتی حساب‌های او را شکست می‌داد.

4. نقض داده ها

هنگامی که یک وب سایت یا سرویس هک می شود، می تواند حساب های همه افراد را که ممکن است در سرور ذخیره شده است تحت تأثیر قرار دهد. اگر شخصی از رمز عبور یکسانی برای چندین حساب استفاده کند، زمانی که آن رمز عبور برای یک حساب در معرض خطر قرار می‌گیرد، می‌توان از آن رمز عبور برای دسترسی به سایر حساب‌های قربانی نیز استفاده کرد.

چگونه اتفاق افتاد: پلتفرم رسانه اجتماعی محبوبی که لیزا از آن استفاده می کرد، با نقض داده مواجه شد. از آنجایی که او از همان رمز عبور در جاهای دیگر استفاده می‌کرد، مهاجمان با استفاده از اطلاعات کاربری لو رفته به حساب‌های دیگر او دسترسی پیدا کردند.

5. اعتبار (رمزهای) خریداری شده

مجرمان سایبری به سادگی می توانند رمزهای عبور شما را در اینترنت، اغلب در دارک وب، خریداری کنند. برخی از مجرمان سایبری در سرقت رمز عبور قربانیان با استفاده از هر یک از روش‌هایی که تاکنون در مورد آنها صحبت کردیم، تخصص دارند. آنها سپس رمزهای عبور سرقت شده را ذخیره کرده و به مجرمان سایبری دیگر می فروشند.

چگونه اتفاق افتاد: یک مجرم سایبری تصمیم گرفت که می خواهد در آخر هفته تا حد امکان درآمد کسب کند، بنابراین به دارک وب رفتند و بیش از 100000 حساب کاربری در معرض خطر را با رمزهای عبور کامل خریداری کردند. یکی از حساب های لیزا در آن لیست بود.

سه گام کلیدی که می توانید بردارید

خوشبختانه، با انجام سه مرحله ساده، می توانید راه طولانی برای محافظت از حساب های کاربری خود و زندگی آنلاین و دیجیتالی خود داشته باشید.

1. برای هر یک از حساب های خود از یک رمز عبور طولانی و منحصر به فرد استفاده کنید. ما عبارات عبور را توصیه می کنیم که رمزهای عبور طولانی هستند که از چندین کلمه تشکیل شده اند.
2. از یک مدیر رمز عبور برای ذخیره و مدیریت ایمن همه آن رمزهای عبور برای خود استفاده کنید.
3. هر زمان که ممکن است برای مهم ترین حساب های آنلاین خود، احراز هویت چند عاملی (MFA) را فعال کنید.

ویرایشگر مهمان

Lekshmi Nair یک رهبر ارشد امنیت سایبری با 22 سال تجربه غنی در مشاوره امنیت اطلاعات و استراتژی امنیت سایبری است. او در حال حاضر مدیر ارشد مشاوره امنیت برنامه با نرم افزار BlackDuck است. او بنیانگذار و رئیس WiCyS هند است.

منابع

صداهای فانتوم: دفاع در برابر حملات شبیه سازی صوتی : https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
حملات پیام‌های متنی: حماسه‌ای عجیب: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/
سه راه اصلی که مهاجمان سایبری شما را هدف قرار می دهند: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
قدرت عبارات عبور: https://www.sans.org/newsletters/ouch/power-passphrase/
قدرت مدیران رمز عبور: https://www.sans.org/newsletters/ouch/power-password-managers/

ترجمه شده برای انجمن توسط: مجید هدایتی، هومن خجاو