سپهر مقیسه

مبانی امنیت اطلاعات

تکلیف خواندنی

پاییز ۱۴۰۱

در ظهر پنج‌شنبه در تاریخی نامعلوم شرکت اوبر مورد حمله یک هکر ۱۸ ساله قرار گرفت و تصاویر سیستم‌های داخلی شرکت، ایمیل‌ها و سرور اسلک که در آن گفت‌وگو انجام میشد به اشتراک گذاشته شد. با توجه به گزارش‌های بدست آمده مشخص شد که به بسیاری‌ها سیستم‌های IT شرکت مانند نرم‌افزارهای امنیتی و دامنه‌های ویندوز دسترسی پیدا کرده است. از سایر سیستم‌ها میتوان به سرویس تحت وب آمازون شرکت، ماشین‌های مجازی و محل‌کار مجازی گوگل اشاره کرد.

اوبر گزارشی مبنی بر آگاهی به این اتفاق تنظیم و اشاره کرد که با دستگاه‌های قضائی در ارتباط است. روزنامه NY TIMES با هکر موردنظر مصاحبه کرده و مشخص شد که یک حمله مهندسی اجتماعی[1] به یکی از کاربرها کرده و سپس اطلاعات شخصی مانند رمز عبور وی را دزدیده است.سپس از این اطلاعات برای ورود به دستگاه شرکت استفاده کرده است.

در ادامه شرکت اوبر یک گزارش تنظیم کرد با مفاد زیر:

- که این نفوذ به اطلاعات کاربران دسترسی پیدا نکرده است.
- تمامی خدمات شرکت به صورت عادی به کار خود ادامه می‌دهند.
- بعضی از نرم‌افزارهای مورد استفاده که قطع شده بودند،از امروز صبح به کار خود ادامه می‌دهند.

نفوذکننده اعلام کرده بود که به سرور اسلک دسترسی پیدا کرده تا از آن برای استفاده در برنامه hackerone bug bounty استفاده کند. وی افزود با یک حمله به یکی از کارمندان توانست به اطلاعات دسترسی پیدا کند اما این که چگونه رمز عبور را پیدا کرده است توضیح نداد.

در ادامه مشخص شد که به دلیل محافظت چند مرحله ای اکانت اوبر از حمله‌ی MFA Fatigue استفاده کرده و وانمود کرد که کارمند IT شرکت اوبر است. و درخواست MFA را چند بار فرستاد.

سپس افزود دستور PUSH Auth را برای بالغ بر یک ساعت برای کارمند فرستاد و در whatsapp به او پیام داد که باید آن را قبول کند تا درخواست از بین برود. بعد از قبولی او، اطلاعات را به دستگاه خود اضافه کرد. از این حملات در زمانی استفاده میشود که اطلاعات کاربر را دارد ولی به دلیل محافظت چند مرحله‌ای نمیتواند به آن دسترسی داشته باشد و در ادامه آن‌قدر این درخواست به قربانی داده می‌شود تا آن را قبول کند. بعد از ورود به آن به vpn شرکت وصل شده و شروع به استخراج اطلاعات محرمانه اوبر کرد. از نتایج هک میتوان به پیدا کردن اسکریپتی که اطلاعات مدیر pam را در بر داشت اشاره کرد که برای ورود به دیگر سرویس های اینترنتی شرکت استفاده می‌شد. همچنین به بانک داده و کد منبع اوبر دسترسی پیدا کرد.

[1] Social Engineering

با توجه به گفته های یک مهندس امنیت اطلاعات، هکر به برنامه hakcerone bb نیز دسترسی داشت که بر تمامی bug bounty ها کامنت گذاشته. این برنامه به این صورت است که متخصصان می‌توانند نقاط ضعف سیستم را در این برنامه در قبال جایزه به اشتراک بگذارند.

این هکر به تمامی گزارشات نقاط ضعف دسترسی داشت و تمامی آن هارا دانلود کرد که شامل بعضی از نقاط ضعف های اصلاح نشده نیز می‌شد. در پایان این برنامه به صورت کامل غیر فعال شد و دسترسی به نقاط ضعف به صورت کل قطع شد. اما ممکن است همچنان این حمله کننده، اطلاعات پیدا شده را برای پول به دیگر حمله‌کننده‌ها بفروشد.