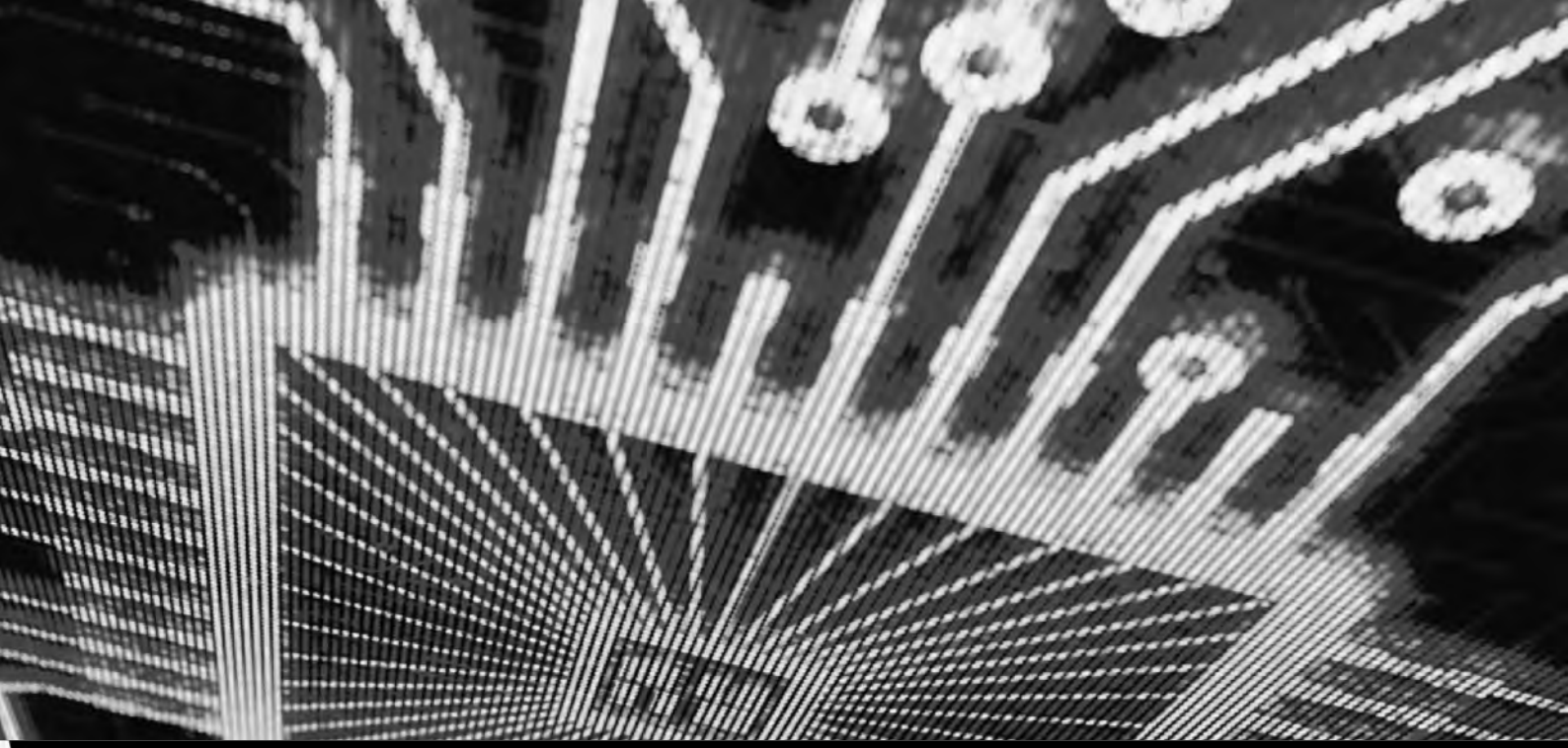
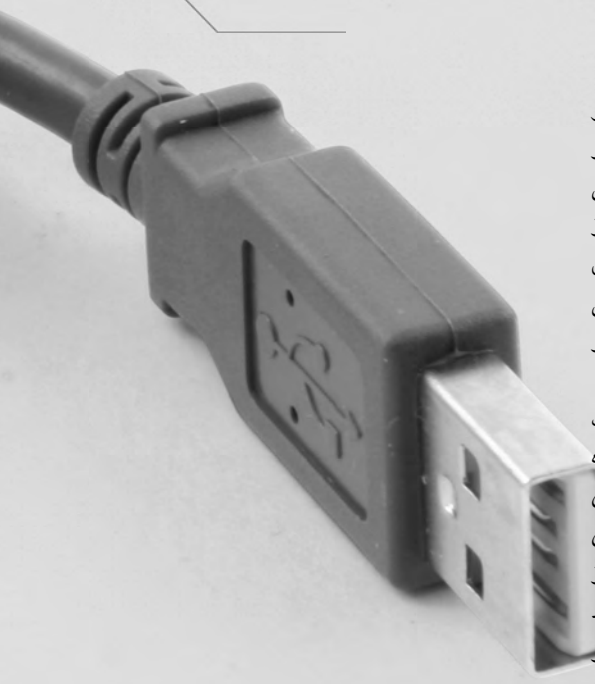


شش تهدید سایبری در حال رشد

» نویسنده: جان براندون » منبع: کامپیوتر ورلد » ترجمه: احمد شریف‌پور

به نظر می‌رسد که هکرهای بزهکار هرگز نمی‌خوابند. درست در همان زمانی که فکر می‌کنید تمام راه‌های نفوذ را بسته‌اید و تجارت‌تان را در برابر خطرهای امنیت الکترونیک به‌طور کامل محافظت کرده‌اید، دوباره حفره و راه نفوذ جدیدی پیدا می‌شود که باعث بی‌خوابی شما در نیمه شب خواهد شد. این عامل می‌تواند یک پیامک با محتوای آلوده باشد یا تعقیب‌کننده‌ای که تمام مراحل فعالیت‌های آنلاین شما را دنبال‌می‌کند یا حتی ممکن است فناوری جدیدی مانند ارتباطات وای‌فای داخل خودرو باشد که خط سیر دیگری برای حمله‌های دیجیتال به‌وجود می‌آورد.

مواظب این تهدیدها باشید، چون می‌توانند گوشی هوشمند شما را به یک بات‌نت ارسال پیامک تبدیل کنند، جریان الکتریسیته را قطع کرده یا در سیگنال‌های GPS تداخل ایجاد کنند.



اگر شما مدیر IT شرکتی باشید که از کارمندان و سیستم‌های شرکت محافظت می‌کنید یا فردی باشید که تلاش دارد امنیت داده‌های شخصی خود را تأمین کند، در هر صورت این تهدیدها (که برخی به سرعت در حال رشد هستند و برخی در حال ظهور) خطرهای بالقوه‌ای را برای شما در پی خواهد داشت. خوشبختانه چندین روال و ابزار امنیتی وجود دارد که به شما کمک می‌کند در این نبرد بر خلافکاران پیروز شوید.

۱- بدافزارهای پیامکی

رادنی جوف رئیس و متخصص فناوری ارشد شرکت پیامک‌های موبایلی Neustar و مدیر Conficker Work Group (ائتلافی از محققان امنیتی) است. او می‌گوید: «درحالی‌که ویروس‌های تلفن‌های هوشمند به نسبت نادر و کمیاب هستند، حمله‌های مبتنی بر پیامک بیشتر معمول شده‌اند. اکنون دیگر پی‌سی‌ها به خوبی محافظت می‌شوند، به همین دلیل، برخی از هکرهای کلاه‌سیاه به سراغ تجهیزات قابل حمل رفته‌اند. انگیزه اصلی آنان به طور معمول مالی است. پیامک راهی برای نفوذ و کسب درآمد در اختیار آن‌ها قرار می‌دهد.»

خویی نگوین، مدیر گروه محصولات امنیت موبایلی در سیمانتک تأیید می‌کند که با استفاده روزافزون مردم از تلفن‌های هوشمند، حمله‌های مبتنی بر پیامک‌های متنی که سیستم‌عامل‌های تلفن‌های هوشمند را هدف گرفته‌اند نیز معمول‌تر شده‌اند. او می‌افزاید: «به طور کلی فقط مصرف‌کننده‌های این دستگاه‌ها نیستند که در

معرض خطر قرار گرفته‌اند. بلکه هر کارمندی که با استفاده از یک تلفن هوشمند متعلق به شرکت، گرفتار یک آلودگی پیامکی شود، می‌تواند کل شبکه تجاری و داده‌های آن را به خطر بیاندازد و حتی ممکن است مرتکب تخلف از قوانین شرکتی شود.»

نگوین توضیح می‌دهد: «این دقیقاً شبیه حمله‌هایی است که به کامپیوترهای شخصی انجام می‌شود. یک SMS یا MMS به همراه ضمیمه‌ای که ادعا می‌شود تصویر جالبی است، به دست کاربر می‌رسد و از او می‌خواهد که این فایل را باز کند. زمانی که کاربر تصویر را دانلودمی‌کند، بدافزاری روی دستگاه نصب‌خواهد شد و هنگامی که این بدافزار اجرا شود، مجوزهای دسترسی را در اختیار گرفته و شروع به تکثیر خود از طریق فهرست مخاطبان تلفن می‌کند. مخاطبانی که به نوبه خود پیامکی از تلفن کاربر آلوده دریافت می‌کنند.» به گفته جوف به این ترتیب هکرها بات‌نتی برای ارسال اسپم از طریق پیامک‌های متنی به‌وجود می‌آورند که پیام‌هایش حاوی لینکی به محصولی است که هکر می‌فروشد و شما به ازای هر یک از این پیامک‌ها باید هزینه بپردازید. او می‌افزاید که در برخی موارد، بدافزار شروع به خرید آهنگ‌های تماسی (Ring tone) می‌کند که هزینه آن در صورت‌حساب دوره‌ای شما منظور خواهد شد و به این ترتیب جیب هکر فروشنده آهنگ، پر پول‌تر خواهد شد.

نگوین می‌گوید: «ترفند دیگر پیامکی حاوی لینکی برای دانلود یک App است که ادعا می‌شود دسترسی رایگان به اینترنت را فراهم می‌آورد، اما در واقع تروجانی است که چندین هزار پیامک (آن هم با نرخ ویژه ۲ دلار به ازای هر پیامک!) از طریق تلفن همراه کاربر ارسال خواهد کرد.»

کریرهای بی‌سیم می‌گویند، که برای مبارزه با این حمله‌ها تلاش می‌کنند. به عنوان نمونه برندا رانی (Brenda Raney) سخنگوی شرکت مخابراتی ورایزون می‌گوید شرکتش پیامک‌ها را برای یافتن حمله‌های بدافزاری اسکن کرده و پیامک‌های آلوده را در شبکه‌های سلولی بلوک می‌کند. این شرکت حتی با واحدهای جنایی فدرال برای خنثی کردن حمله‌ها همکاری دارد.

اما همان‌گونه که جوف به تمسخر می‌گوید: «هنوز هیچ راه‌حلی برای حماقت پیدا نشده است.» و حتی برای اشتباهات کارمندان نیز روش پیش‌گیری وجود ندارد. برای نمونه، او تعریف می‌کند که چگونه او و دیگر متخصصان امنیتی درباره کرم‌هایی که از طریق پیامک تلفن‌های هوشمند را تهدید می‌کنند، به تک‌تک کارمندان یک شرکت توضیح داده‌اند و درست پس از پایان آموزش بسیاری از آن‌ها بازهم روی لینک‌ها کلیک می‌کنند.

جوف پیشنهاد می‌کند که برای دور نگه داشتن این تهدیدها از تلفن‌های کاربران، نهادهای تجاری باید قوانین شرکتی را سخت‌گیرانه‌ترکنند و تعداد افرادی را که مجوز ارسال پیامک از طریق تلفن‌ها و شبکه سازمان دارند و همچنین نوع کارهایی را که از طریق پیامک می‌توان به انجام رساند، محدودتر کنند. راه‌حل دیگر غیرفعال‌کردن کامل پیامک‌ها است؛ دست‌کم تا زمانی که صنایع نحوه مبارزه با این تهدیدها را بیابند. برای کاربران، بهترین دفاع مراجعه به عقل سلیم است. از کلیک روی لینک‌ها یا ضمیمه‌های

پیامک‌هایی که از افراد ناشناس دریافت می‌کنید، پرهیز کنید. درباره کسانی هم که می‌شناسید، نهایت احتیاط را به کار ببرید، چون ممکن است ناخواسته جزئی از یک بات‌نت باشند.

۲- نفوذ به گریدهای هوشمند

یکی از اشتباه‌های رایج این است که تنها شبکه‌های باز (مثلاًشبکه بی‌سیمی که در شرکت شما برای دسترسی بازدیدکنندگان عام به اینترنت فراهم شده است) قابل هک‌کردن هستند. جاستین مورهاوس معتقد است، این تصور اصلاً درست نیست. او یکی از مشاوران ارشد Startum Security است که در کنفرانس امنیتی DefCon سال گذشته درباره امنیت شبکه سخنرانی کرده است. او می‌گوید: «یافتن یک نقطه دسترسی برای اتصال به شبکه‌ای که به اصطلاح "بسته" نامیده می‌شود، چندان هم دشوار نیست.» (شکل ۱)

به عنوان مثال، در سال گذشته کرم استاکس نت ده‌ها هزار کامپیوتر ویندوزی را که سیستم‌های SCADA زیمنس را اجرا می‌کردند، آلوده کرد و این آلودگی بیش از هر چیز از طریق فلش‌های یواس‌بی آلوده منتقل‌شده است.

جوف می‌گوید: «استاکس نت ثابت کرد که ایجاد خرابی‌های بالقوه فاجعه‌آفرین در شبکه‌های کنترل صنعتی، چندان هم دشوار نیست.» به گفته مورهاوس، گریدهای هوشمند یکی دیگر از نقاط حمله خواهند بود. گریدهایی که برای ساده‌ترکردن مدیریت نیرو، در قسمت‌های مختلف از اندازه‌گیری‌های الکترونیک استفاده می‌کنند. شرکت‌های فراهم‌کننده خدمات در سراسر دنیا، شروع به آزمایش و نصب تجهیزات اندازه‌گیری هوشمند در خانه‌ها و ساختمان‌های تجاری مشتریان کرده‌اند. این فناوری که قادراست داده‌ها را به یک سیستم مرکزی ارسال کرده یا از آن دریافت کند، می‌تواند برای کارکنان بخش IT نیز بسیار مفید باشد. به عنوان مثال، آن‌ها می‌توانند با باز کردن یک کنسول، میزان برق مصرفی یک قسمت از ساختمان را مشاهده کنند (شکل ۲).

اما گریدهای هوشمند ممکن است در برابر حمله‌هایی که به هکرهای بدذات اجازه می‌دهد برق خانه‌ها یا مراکز تجاری را قطع کرده و از این طریق خسارت‌های دیگری به بار بیاورند، نفوذپذیر باشد. مثلاً به گفته مورهاوس، یک شرکت خدمات‌رسانی آلمانی به نام Yello Strom از یک سیستم‌گرید استفاده می‌کند که همانند یک کیت اتوماسیون خانه عمل می‌کند. حسگرهای این سیستم با استفاده از شبکه وای‌فای صاحبخانه میزان مصرف انرژی را به سرور مرکزی گزارش می‌دهند.

به گفته مورهاوس، به همین دلیل کاربران نهایی می‌توانند به شبکه خانگی خود وارد شده و کنترل زیرسیستمی که وظیفه انتقال نیرو را برعهده دارد، به دست بگیرند. او می‌گوید: «مسئله این است که این نوع شبکه‌ها به درستی تقسیم‌بندی و محافظت نمی‌شوند. زمانی که یک هکر توانست وارد یک قسمت شود، ممکن است با او همانند یک کاربر مورد اطمینان رفتار شود و او به سایر قسمت‌ها نیز دسترسی پیدا کند. آیا این احتمال وجود دارد که آن‌ها بتوانند یک ایستگاه کوچک توزیع یا یک شهر را از کار بیاندازند؟ به یقین ممکن است. آن‌ها ممکن است یک "در پشتی" در سیستم تعبیه کنند که اجازه می‌دهد، در هر زمان دلخواه برق را قطع کنند.»

شرکت‌های فراهم کننده خدمات در امریکا، به طورمعمول از شبکه‌های اختصاصی کابلی یا بی‌سیم خود استفاده می‌کنند، اما مورهاوس نگران این موضوع است که برخی از آن‌ها ممکن است به استفاده از روش Yello Strom روی بیاورند و به جای شبکه‌های اختصاصی از شبکه‌های خانگی کاربران استفاده کنند.

یکی دیگر از نگرانی‌ها، نفوذپذیری خود تجهیزات اندازه‌گیری (نه شبکه آن‌ها) است که به نوبه خود باز هم بر گرید هوشمند شرکت تأثیر خواهد گذاشت. به عنوان مثال، محققان شرکت ارائه‌کننده خدمات امنیتی IOActive مستقر در سیاتل، چندین باگ در تجهیزات اندازه‌گیری گریدهای هوشمند یافته‌اند که هکرها می‌توانند با استفاده از آن‌ها به شبکه گرید دست یافته و برق برخی مشترکان را قطع کنند.

مورهاوس می‌گوید: «هکرها از اخبار رسانه‌ها برای آگاهی از فناوری به‌کار رفته در این گریدها استفاده کرده و بعد به سراغ زیرساخت‌ها رفته و راه‌های نفوذ را کشف می‌کنند. پس اگر به عنوان مثال وال- مارت گریدی را بر مبنای فناوری‌های زیمنس معرفی کند، یک هکر به سادگی پاسخ بسیاری از پرسش‌ها را درباره یافتن و نفوذ به آن کنترل کننده در اختیار خواهد داشت.»

مورهاوس معتقد است کاراترین اقدام بازدارنده در این مورد ایزولاسیون کامل است. یک گرید هوشمند نباید به هیچ‌وجه با

شـبکه دیگری تعامل داشته باشد. او می‌گوید: «بـه واسـطه وجـود خطـر احتمالـی نفوذ و در دسـت‌گرفتن کنتـرل سیسـتم‌های توزیع نیرو، لازم اسـت که تمام شـبکه‌های بسته نیز آزمون‌های نفوذپذیری را انجام دهند و مطمئن شـوند که فایروال شبکه به‌صورت کامل از آن محافظت می‌کند. او اسـتفاده از ابزارهایی نظیر Core Impact و Metasploit را پیشـنهاد می‌کند.»

قانـون «ایزولاسـون کامل» بایـد درباره کاربـران خانگـی نیز صدق کنـد. مورهاوس می‌گویـد: «کاربـران خانگی نیـز نباید به هیچ عنـوان داده‌های‌گریدهـای هوشـمند را روی شبکه‌هایشـان منتقل‌کنند.» همچنین او توصیه می‌کنـد کـه کاربران بـا تجهیزات هوشـمند اندازه‌گیری منازلشـان آشـنا باشند و بتوانند تشـخیص دهند که آیا این تجهیزات دستکاری شده است یا خیر و همین‌طور از تأمین‌کنندگان خدمات بپرسـند که چه تمهیـدات امنیتی برای محافظت از ابزار اندازه‌گیری و شبکه مرتبط با آن اندیشیده شده است.

۳- جعل حساب‌های شبکه‌های اجتماعی

بسـیاری از افراد از شـبکه‌های اجتماعی بـرای ارتبـاط با دوسـتان، افراد خانـواده یا همکاران اسـتفاده می‌کنند و ایـن امر آن‌ها را در برابـر تکنیک جدیدی که جعل حسـاب‌های شـبکه‌های اجتماعی نامیده می‌شود، نفوذپذیر می‌کنـد. روال کار بـه این ترتیب اسـت که یک شـیاد وانمود می‌کند، یکی از آشـنایان شما یا دوسـت یکی از دوسـتان شما اسـت و از این طریق به شـما نزدیک می‌شـود و شما را گول می‌زنـد تا اطلاعات شـخصی و محرمانه خود را فاش کنید. پس از آن او از این اطلاعات برای به دست گرفتن کنترل سایر حساب‌های شما یا حتی جعل هویت شما استفاده می‌کند.

بـه گفتـه جـوف، در یـک روش معمول، شـخصی روی یکی از این شبکه‌های اجتماعی، مثلاً LinkedIn، با شما تماس می‌گیرد و خود را دوست دوست شـما یا همکار یکی از آشنایان شما معرفی می‌کند. این «دوست جدید» از طریق ایمیل یا پیامک به‌صورت مسـتقیم با خود شما تماس می‌گیرد.

ممکن است تعجب کنید که این دوست جدید خارج از شـبکه اجتماعی و به طورمسـتقیم با شـما تماس گرفته اسـت، اما او کاملاً موجه به نظر می‌رسـد. زیرا شـما فکر می‌کنید او با یکی از افرادی که می‌شناسـید و بـه آن‌ها اطمینان داریـد، ارتباط دارد. در سـناریویی دیگر، فرد شـیاد خود را به جای شـخص دیگری که شما قبلاً می‌شـناخته‌اید، معرفی کـرده و مثلاً ادعا می‌کند که یکی از دوسـتان دوران دبیرسـتان شما است.

این افراد اطلاعات خود را از طریق بررسی ردپاهای عمومی شـما یا مراجعه به فهرسـت همکاران شما در شبکه‌ای مانند LinkedIn کسب می‌کنند. جایی که شما اطلاعات حرفه‌ای خود را در آن وارد کرده‌اید.

هنگامی که فرد شـیاد ارتباطی را با شـما برقرارکرد، از روش‌های مختلفی برای سـرقت اطلاعات شخصی شما استفاده می‌کند. مثلاً به کمک چت، از نام افراد خانواده شـما، گروه‌های موسـیقی مورد علاقه‌تان، سرگرمی‌ها و سایر اطلاعات به ظاهر کم اهمیت آگاه می‌شـود و در نهایـت از این اطلاعات به عنـوان رمز عبور یا پاسخ سـؤال‌های امنیتی سایت‌های بانکداری، ایمیل و دیگر سایت‌ها استفاده می‌کند.

همان‌طـور کـه جـوف اشـاره می‌کنـد، ایده موجود در پشـت کلاهبـرداری از طریق شـبکه‌های اجتماعـی، قدمتـی هزاران سـاله دارد. به‌دسـت‌آوردن اطلاعات شخصی افراد و سـوء اسـتفاده از آن ترفندی بسیار قدیمی است. شبکه‌های اجتماعی امروزی، راهی جدید برای کلاهبـرداران هنرمند و خلافکاران فراهم آورده‌اند تا به شـما نزدیک‌تر شوند. این ترفند در اغلب موارد کار می‌کند، زیرا به طور معمول هیچ روشـی وجود ندارد که شـما به کمک آن متوجه شـوید، شـخصی که می‌خواهید به او اعتمـاد کنید، دقیقاً همان کسـی اسـت که ادعا می‌کند.

جـوف می‌گوید: «مشـکل ارتباط از طریق شـبکه اجتماعی یا LinkedIn این است که شما به رابط‌های وبی محدود هسـتید. نمی‌توانید IP یا اطلاعـات Header پیام‌ها را بررسـی کنید. همه چیز در یک دنیای دوسـتانه و دل چسـب به شما عرضه می‌شود.» مورهاوس از شرکت Startum Security معتقد اسـت که خلافکاران به شکل فزآینده‌ای ماهرتر می‌شوند. آن‌ها ابتدا یک هدف را درنظرمی‌گیرند، سـپس شروع به تحقیق می‌کنند. این فرد چگونه آدمی است؟ چه کسانی را دنبال (Follow) می‌کند؟ دوست دارد چه کارهایی انجام دهد؟

مورهـاوس می‌گویـد، علاوه بـر این‌ها، حمله‌های مبتنی بر شـبکه‌های اجتماعی ممکن اسـت بـا کلاهبرداری‌های ایمیلی یـا وبی هم ترکیب شـوند. شـما ممکن اسـت با کسی در LinkedIn دوسـت شوید؛ سـپس ایمیلی از آن شـخص دریافت کنیـد که به نظر می‌رسـد از طریق LinkedIn ارسـال شده است، اما در واقع ایمیلی جعلی اسـت. زمانی که شـما روی لینک پاسـخ کلیک می‌کنید، به یک سـایت LinkedIn جعلی هدایت‌می‌شـوید. ورود به آن سایت، نام کاربری و رمز عبور شما را برای سارق آشکار خواهد کرد.

شکل۱ به عقیده جاستین مورهاوس از شرکت Startum Security نیـاز به آزمون‌های نفوذ در گریدهای هوشمند بسیار حیاتی است.

شکل۲ تجهیزات هوشمند اندازه‌گیری مانند این کنتور، به یک گرید هوشمند متصل می‌شوند تا عملیات مدیریت انرژی را ساده‌تر کنند. متخصصان می‌گویند، ممکن است بتوان به آن‌ها نفوذ کرد.

مورهاوس نوع دیگری از حمله‌ها را توضیح می‌دهـد که شـرکت‌ها را همانند افـراد هدف می‌گیرد. کلاهبردار یک صفحه شـبکه‌اجتماعی ایجـاد کـرده و وانمود می‌کند کـه این صفحه رسـمی یک شـرکت بزرگ؛ مثـلاً تولیدکننده کالاهای اداری Staples اسـت. کلاهبردار برای معتبر جلوه‌دادن این صفحه حتی ممکن اسـت ادعا کند که این صفحه روشـی رسـمی برای تماس با شرکت یا ثبت شکایات است.

این صفحه حتی ممکن اسـت برای ترغیب افراد به عضو شدن، کوپن‌های تخفیفی (مطمئناً جعلـی) نیز عرضه کنـد و هنگامی که افراد این صفحه را به شبکه دوستانشان‌معرفی کنند، این صفحه به شـکلی ویروسی‌گسترش می‌یابد. به


---------- Forwarded message ----------
From: Nathan Miller via LinkedIn <member@linkendin.com>
Date: Fri, Oct 15, 2010 at 2:37 PM
Subject: Hey
To: Justin Morehouse <justin@stratumsecurity.com>

LinkedIn

Nathan Miller has sent you a message.
Date: 10/15/2010
Subject: Hey
Hey buddy, Heard the good news. We should catch up!

View/reply to this message

Don't want to receive e-mail notifications? Adjust your message settings

© 2010, LinkedIn Corporation

شکل ۳ به نظر می‌رسد که این ایمیل از سوی یکی از دوستان شما در LinkedIn ارسال شده باشد، اما به دقت به نام دامنه آن نگاه کنید، با استفاده از این روش متوجه خواهید شد که این یک ایمیل جعلی است.

شکل ۴ اگر روی یک پیام جعلی LinkedIn کلیک کنید، به یک سایت جعلی هدایت می‌شوید. این روشی برای سرقت نام کاربری و رمز عبور شما است.

گفته مورهاوس، زمانی که این صفحه صدها یا هزاران عضو پیدا کرد، صاحب صفحه سعی می‌کند آن‌ها را فریب داده و اطلاعات شخصی‌شان را برباید. این کار ممکن است از طریق دعوت به ثبت‌نام برای دریافت کوپن‌های بیشتر یا شرایط ویژه فروش انجام شود.

این حمله‌ای دوگانه است. مشتریان ضرر می‌کنند، چون اطلاعات شخصی آن‌ها فاش شده است و شرکت هم آسیب می‌بیند، چون افراد این صفحه جعلی را با شرکت واقعی مرتبط فرض کرده و تصمیم می‌گیرند که دیگر از این شرکت خرید نکنند.

به عقیده جوف بهترین دفاع افراد در برابر این حمله‌ها درست همانند حمله‌های پیامکی، تکیه بر عقل سلیم است. خلافکاران معمولاً نمی‌توانند به خوبی نقش یک فرد یا شرکت خاص را بازی‌کنند و برای گول‌زدن شما لینک‌ها و ایمیل‌های فیشینگ را ارسال می‌کنند. آن‌ها ممکن است سعی کنند مانند یک دوست رفتار کنند، اما نمی‌توانند شخصیت آن دوست را به دقت بازسازی کنند.

در برخی موارد این حمله‌ها از طریق هدرهای ایمیل یا آدرس‌های IP قابل‌ردیابی است. همچنین بیشتر این حمله‌ها کلی و بدون هدف هستند، به گونه‌ای که هر کسی که اندکی محتاط باشد متوجه جعلی بودن آن‌ها خواهد شد (شکل ۳ و ۴).

دیگر احتیاط‌های پیشگیرانه هرچند ممکن است بدیهی به نظر برسند، اما اغلب مورد غفلت قرار می‌گیرند. اگر کسی ادعا می‌کند که دوست دوست شما یا آشنای همکار شما است، مطمئن شوید که همکار یا دوست شما هویت این فرد جدید را تأیید می‌کند. همچنین ایده خوبی است اگر دسترسی به اطلاعات شخصی خود را در تنظیمات امنیتی شبکه‌های اجتماعی مورد استفاده‌تان محدود کنید. به این ترتیب، اطلاعات تماس شما، پست‌ها، عکس‌ها و سایر موارد در معرض دید همگان نخواهد بود.

برای شرکت‌ها این کار کمی دشوارتر است. به گفته جوف، هیچ راهی وجود ندارد که مانع از ایجاد صفحه جعلی یک شرکت در شبکه‌های اجتماعی شود، اما شرکت‌ها می‌توانند از ابزارهای پایش نظیر Social Mention استفاده کرده و ببینند که نام شرکت در مجامع آنلاین چگونه مورد استفاده قرار می‌گیرد. در این صورت اگر یک صفحه بدون مجوز پیدا شود، می‌توان از صاحبان شبکه اجتماعی خواست که نسبت به حذف آن صفحه جعلی اقدام کنند.

۴- مزاحمت آنلاین

شبکه‌های اجتماعی روش تعامل افراد را در زندگی شخصی و کاری تغییر داده‌اند؛ در عین حال همین پورتال‌ها می‌توانند راه‌هایی را به‌وجود بیاورند که دیگران از طریق آن‌ها زندگی ما را به تباهی بکشانند.

ایده جدیدی که به دفعات «تعقیب سایبری» (Cyberstalking) آزار سایبری (Cyberharassment) یا باج‌گیری سایبری (Cyberbullying) نامیده شده است، در واقع عبارت است از حمله‌های آنلاینی که به صورت مکرر از سوی فرد یا گروهی علیه شما انجام شود. این حمله‌ها ممکن است، نوشتن نقدهای منفی در ادامه هر پست توییتر شما یا ارسال عکس‌های دستکاری شده و نامرتبط شما در شبکه‌های اجتماعی باشد. عاملان این کار می‌توانند هویت خود را در پس نام‌های مستعار آنلاین مخفی نگه دارند. باج‌گیری سایبری در صورتی‌که با تهدیدهای جانی همراه باشد، براساس قانون فدرال جرم محسوب می‌شود.

بیشتر ما داستان‌های متعددی را از موارد اخاذی سایبری از نوجوانان شنیده‌ایم، اما به عقیده کاتلین بتی این نوع اخاذی درباره بزرگسالانی که از محل کارشان به شبکه‌های اجتماعی متصل می‌شوند نیز در حال رشد است. کاتلین مشاور امنیت فردی و مدیرعامل شرکت SafetyChick Enterprises است. به گفته او این اخاذی‌ها ممکن است از سوی یکی دیگر از کارمندان یا از سوی کسی که می‌خواهد اطلاعاتی را از شرکت سرقت کند، انجام شود(شکل ۵).

کاتلین بتی می‌گوید: «اخاذی‌های سایبری مرتبط با محل کار بیش‌ازپیش معمول شده‌اند، اما تعریف دقیق آن‌ها به سادگی ممکن نیست.

زیـرا انواع زیـادی از آزار و تهدیـد در دنیای دیجیتال وجـود دارد که هریک انگیزه متفاوتی در پس خود پنهان کرده‌اند. این انگیزه می‌تواند با یک رابطه عاطفی یا شـخصی که با مشـکل روبه‌رو شده‌مرتبط‌باشد یا نتیجه درگیری‌های کاری وتجـاری بـا یکـی از رقبایی باشـد که می‌خواهد با این خرابکاری‌ها انتقام بگیرد.

به عقیده‌بتی،برای‌حذف‌این‌آزارهای‌آنلاین از شبکه‌های شرکت، تمام ابزارها و روش‌های معمول امنیت سـازمانی (ماننـد فایروال‌ها و رمزگذاری‌ها) باید توسـط شرکت پیاده‌سازی شود. علاوه بر این، شرکت‌ها باید یک شیوه‌نامه رسانه‌های اجتماعی (Social Media Policy) را تبیین کنند که در آن به‌وضوح مشـخص شـده باشد که انتشـار و صحبت درباره چه مطالبی در شبکه‌های اجتماعی برای کارمندان مجاز یا غیر مجاز است.

اگر شـما نیز قربانی آزار یا اخاذی آنلاین شـده‌اید، بتـی به شـما توصیه می‌کنـد که به سـرعت مراتـب را با مراجع قانونـی در میان بگذاریـد. اگر این اتفـاق در محیط کار رخ داده اسـت، حتماً آن را به بخش منابع انسـانی نیز گـزارش کنیـد. او می‌گوید که بـه هیچ‌عنوان پست‌ها یا سـایر مدارک مرتبط با این موضوع را پاک نکنید، بلکه آن‌ها را به عنوان شـواهد این مزاحمت نگه‌داری کنید. در برخی موارد علاوه بر اسـتفاده به عنوان مـدارک وقوع جرم، این پسـت‌ها و ایمیل‌ها حاوی هدرهایی هستند که ممکن اسـت برای ردیابی مزاحم مورد استفاده قرار بگیرند.

گفته می‌شـود که بهترین دفاع این است که از اطلاعات شـخصی‌تان با شدت هرچه تمام‌تر مراقبت کنید. به عنوان مثال هرگز مکان زندگی و نقل‌مکان‌های خود را به‌صورت آنلاین اعلام نکنیـد. هیچ‌گاه به‌صورت آنلاین اعلام نکنید که به تعطیلات رفته‌اید یا کامپیوتر شرکت خود را بـدون محافظ رهاکرده‌اید و مثلاً به همین دلیل استفاده از سرویس اجتماعی و عمومی «اعلام ورود» Foursquares را متوقف کنید.

۵- هکرها ماشین شما را کنترل می‌کنند

دوران «ماشین‌های متصل به هم» در حال فرا رسیدن است. اتومبیل‌هایی مانند فورد Edge اکنون امکان دسترسـی به شـبکه‌های 3G، یک روتر درون ماشـین و حتـی قابلیت اتصال به شبکه بی‌سـیم خانگی شـما را (فقط در حالت پارک شده) با خود به ارمغان آورده‌اند. در چند سال آینده دیگر سـازندگان خودرو نیز امکان اتصال بی‌سـیم را برای مـرور وب و دریافت فیلم‌های با کیفیت بالا به محصولاتشان خواهند افـزود. در سـال ۲۰۱۳، یکی از سـیگنال‌های بی‌سیم تأیید شده توسط FCC که DSRC (سرنام Dedicated Short Range Communications) نامیده می‌شـود روی فرکانـس ۵/۹ گیگاهرتز فعـال خواهد شـد و امکان ایجاد شـبکه‌های ارتباطی ماشین به ماشین را فراهم خواهد کرد.

افزوده شـدن این قابلیت‌ها به وسـیله‌ای کـه در حال حرکت اسـت؛ برای هر شـخصی که مطالب مرتبط با محاسـبات شبکه‌ای یا حتی به‌صورت عام کامپیوترهـا را دنبال‌می‌کند، به مثابـه یک زنگ‌خطر خواهدبود. چون روشـی دیگر را در اختیار هکرهای بزهکار قرارمی‌دهد که از طریق آن مشـکلات تازه‌ای ایجاد می‌کنند. به گفته استفان ترانوتزر (Stephan Tranutzer)؛ مدیر ارشد یکی از سازندگان کنسول‌های کنترل خودرو DGE، چون این سیستم‌ها به طور معمول به تجهیزات عیب‌یابی و ایمنی خودروها متصل هستند، یک هکر می‌تواند به این سیستم‌ها نفوذ کرده و از این طریق به عنوان مثال باعث شـود که موتور یک خودرو در زمان نامناسبی شتاب بگیرد (شکل۶).

در حالی‌کـه تاکنـون هیـچ حملـه‌ای در دنیای واقعی صورت نگرفتـه، محققان امنیتی دانشگاه‌های کالیفرنیا، سان‌دیه‌گو و واشینگتن توانسـته‌اند به کامپیوترهای تعدادی از آخرین مدل‌هـای اتومبیل‌ها نفوذ کـرده و از راه دور سیستم ترمز را از کار بیاندازند، سرعت‌نمایش داده‌شده را تغییر دهند، موتور را خاموش کرده و حتی مسـافران را در داخل خودرو محبوس کنند. نخستین آزمایش این محققان بر اتصال یک لپ‌تاپ به سیستم عیب‌یابی خودرو مبتنی بود، اما آزمایش‌های بعدی نشـان دادند که راه‌های دیگری مانند اتصال‌هـای بلوتوث یا اتصال از طریق شـبکه‌های سلولی نیز برای ورود به این سیستم وجود دارد. اتصال‌های بی‌سیم بیشتر در ماشـین‌های آینده، راه‌های نفوذ بیشتری را برای هکرها فراهم خواهد کرد.

به گفتـه ترانوتزر، نکته مثبـت ماجرا این اسـت که بیشـتر فناوری‌های بی‌سیم در حال ظهور بـرای خودروها از نوع مسـافت کوتاه (Short Range) هستند و مثلاً حداکثر می‌توانند در فاصله بین دو مسیر سواره‌رو یا در محدوده یـک چهارراه به برقراری ارتباط اقدام کنند. این موضوع کار را برای هکرها دشوار خواهد کرد، چون باید در فاصله‌ای نزدیک به خودرو باشند تا به سیستم دسترسی پیدا کنند.

در هر صـورت ارتباطات بی‌سـیم درون خودروهـا به یقیـن هدفی وسوسـه برانگیز

شکل۵ کاتلیـن بتی مشـاور امنیت فردی، معتقد اسـت که تحت‌نظر گرفتن‌هـای مرتبط با محل کار ممکن اسـت توسط یکی از همکاران یا کسی که می‌خواهد اطلاعاتی را از شرکت سرقت کند، انجام پذیرد.

بـرای هکرها خواهد بود. به گفته ترانوتزر، تنها راه‌حل این اسـت که صنایع خودروسـازی به رمزنگاری‌های پیشـرفته مبتنی بر سخت‌افزار روی بیاورند.

به عنوان مثال، سرویس امنیتی و ارتباطی OnStar قابلیتـی بـرای ردیابـی خودروهای مسـروقه عرضه‌می‌کنـد که از سـیگنال‌های بی‌سـیم اسـتفاده می‌کند. اگر خودروی شما دزدیده شـود، می‌توانید این سرقت را به پلیس گـزارش دهیـد تا با OnStar تمـاس بگیرد. در ایـن وضعیـت OnStar سـیگنالی را از طریق شبکه‌های 3G ارسال می‌کند که موتور خودرو مسـروقه را از کار می‌انـدازد. ارتباطـات و سیگنال‌های OnStar رمزگذاری شده‌اند تا مانع از تلاش برای نفوذ به سیسـتم و ایجاد اختلال در عملکرد خودروها شوند.

به یقین، شـرکت‌های خودروسـازی نیز از احتمـال ایجـاد اختـلال توسـط هکرها در

شکل۶ این ماجول و نمونه‌های شـبیه آن که به سیستم‌های عیب‌یابی خودروها متصل می‌شوند، توسط فناوری‌های قدرتمند رمزنگاری محافظت می‌شوند. در آینده سازندگان خودروها و وزارت حمل و نقل باید دستگاه‌هایی را که به شبکه‌های بی‌سـیم متصل می‌شوند، کنترل و تأیید کنند.

خدمات بی‌سیم خودروها آگاه هستند. به عنوان مثال، نمایندگانی از فورد و جنرال موتورز اعلام کرده‌اند که در حال توسعه استانداردهای قدرتمند رمزگذاری برای ارتباطات میان خودروها و همین‌طور اتصالات میان خودرو و زیرساخت‌های پشتیبانی کارخانه هستند.

به عقیده ترانوتزر، فناوری‌های مرتبط با «ماشین‌های متصل به هم» در بیشتر زمینه‌ها هنوز در مرحله آزمایش است. او می‌افزاید: «شبکه‌های DSRC به‌طور خاص توسط شرکت‌های خودروسازی و وزارت حمل‌ونقل ایالات متحده تحت آزمایش‌های دقیق و سخت‌گیرانه قرار خواهد گرفت تا اطمینان حاصل شود که از رمزگذاری قدرتمند استفاده می‌کند و می‌تواند در برابر تلاش‌های هکرها برای نفوذ مقاومت کند.»

او می‌گوید: «به همین دلیل است که در مقایسه با زمان شش ماهه مورد نیاز برای دریافت مجوز تولید یک تلفن هوشمند، ارزیابی کیفی یک خودرو به دو تا سه سال زمان نیاز دارد.»

۶- جعل و ایجاد اختلال در GPS: تهدید یا آزار

یکی دیگر از تاکتیک‌های مجرمانه در حال ظهور، ایجاد اختلال در سیگنال‌های GPS است که متخصصان تنها در میزان خطری که این اختلال می‌تواند در آینده ایجاد کند با هم اختلاف دارند.

به گفته فیل لیبرمن، بنیان‌گذار شرکت امنیت سازمانی Lieberman Software، ایجاد اختلال در سیگنال‌های GPS در مبدأ به طور عملی غیرممکن است. مسدودکردن سیگنال‌های ارسالی ماهواره‌های GPS به فرستنده‌ای با قدرت ارسال بسیار بالا نیاز دارد. ایجاد اختلال در گیرنده‌های GPS با مختل‌کننده‌های ارزان قیمتی نظیر آنچه توسط Brando عرضه می‌شود، بسیار ساده است.

این دستگاه با ارسال دائمی سیگنال‌های مشابه باعث اختلال در دریافت سیگنال‌های GPS واقعی می‌شود. در چنین حالتی گیرنده گیج می‌شود، چون نمی‌تواند یک ارتباط پایدار ماهواره‌ای را برقرار کند.

به عقیده لیبرمن، این نوع اختلال‌ها بیشتر نوعی مزاحمت محسوب می‌شوند تا یک تهدید امنیتی جدی. یک هکر خرابکار می‌تواند به عنوان مثال، یک مختل‌کننده در یک چهارراه نصب کند و دریافت GPS را در خودروهای در حال عبور مختل کند. لیبرمن معتقد است، چنین حمله‌هایی نادر هستند و می‌افزاید: «معمولاً فقط افراد ضداجتماع این کار را انجام می‌دهند.»

لیبرمن به ترس از اختلال در کار هواپیماها یا سیستم‌های کنترل ترافیک هوایی چندان اعتقاد ندارد، چون این شبکه‌ها از سیگنال‌های GPS کاملاً متفاوتی نسبت به خودروها و دستگاه‌های GPS قابل حمل استفاده می‌کنند. او می‌گوید: «این اختلال زمانی که به سوابق مالی مرتبط باشد می‌تواند به موضوعی خطرناک تبدیل شود، چون از دستگاه‌های GPS در صنعت بانکداری برای افزودن برچسب‌های زمانی به تراکنش‌های مالی استفاده می‌شود. هرچند مسدود کردن کامل سیگنال‌های GPS بسیار دشوار خواهد بود، اما به نظر لیبرمن یک هکر ماهر به‌صورت تئوری می‌تواند این ارتباطات را مختل کرده و برای بانک‌ها دردسر ایجاد کند.»

راجر جانستون که یک متخصص امنیت است و به عنوان مهندس سیستم در Argonne National Laboratory شیکاگو کار می‌کند، معتقد است، مختل‌کردن سیگنال‌های GPS خطری به مراتب بزرگ‌تر است. او توضیح می‌دهد که گیرنده‌های GPS ابزارهایی با مصرف پایین انرژی هستند که از قدرتمندترین سیگنال موجود استفاده می‌کنند. برای آزمایش، او سیگنال مختل‌کننده‌ای ایجاد کرد که از درون یک ماشین منتشر می‌شد و اطلاعات نادرست GPS را به گیرنده‌های مجاور ارسال می‌کرد. او می‌گوید: «لازم نیست چیزی درباره الکترونیک یا GPS بدانید تا بتوانید چنین چیزی را سرهم کنید. این ابزارها بسیار کاربرپسند هستند!» (شکل ۷).

جانستون معتقد است ایجاد اختلال در سیگنال‌های GPS می‌تواند برای جرائم واقعی مورد استفاده قرار بگیرد، برای مثال با ارسال سیگنال‌های اشتباه، کامیون‌های حاوی کالا به مناطق خلوتی کشیده‌شوند که خلافکاران در آنجا به انتظارشان نشسته‌اند یا تراکنش‌های مالی با برچسب‌های زمانی اشتباه به ثبت برسند یا حتی وسایل نقلیه امدادی از یافتن مسیرهای درست در زمان مناسب ناتوان شوند. تاکنون گزارشی از ایجاد تداخل در سیگنال‌های GPS با اهداف خرابکارانه دریافت نشده است، اما جانستون هشدار می‌دهد که دولت و صنایع باید برای کنترل این حمله‌ها دست به کار شوند.

او معتقد است، به صورت معمول صنایع امنیتی «واکنشی» هستند و می‌گوید: «ما آن‌قدر صبر می‌کنیم تا یک فاجعه رخ‌دهد و بعد کار درباره آن را آغاز می‌کنیم.» با قطعاتی که ارزش آن‌ها در نهایت به پانزده دلار می‌رسد، می‌توان دستگاه‌های GPS را قادر به تشخیص اختلال کرد و به کاربر هشدار داد که حمله‌ای در حال شکل‌گیری است. جانستون می‌گوید: «اما چون تقریباً هیچ کس به اختلال در GPS توجهی ندارد، این پروژه در دست اقدام قرار نخواهد گرفت.»

شکل ۷ آزمایشگاه ملی Argonne سیستم مختل‌کننده‌ای را برپا کرده است که می‌تواند اطلاعات نادرست را از صندوق عقب یک اتومبیل به خورد گیرنده‌های GPS بدهد. گیرنده‌هایی که در آمبولانس‌ها یا کامیون‌ها مورد استفاده قرار می‌گیرد.

در نهایت همان‌گونه که لیبرمن توضیح می‌دهد، افراد نمی‌توانند برای جلوگیری از حمله‌های GPS کاری انجام دهند. اگر هنگامی که شما در حال راندن یک خودرو یا استفاده از یک گیرنده دستی GPS هستید، شخصی سیگنال‌های GPS دروغین را ارسال کند، گیرنده شما یا از کار خواهد افتاد یا گول خواهد خورد. اما به خاطر داشته باشید که به مجرد بیرون آمدن از محدوده پوشش آن فرستنده، دستگاه شما دوباره به‌صورت عادی‌کار خواهدکرد. به هر حال، بهتر است بدانید که ایجاد اختلال در سیگنال‌های GPS در ایالات متحده غیرقانونی است و قوانین FCC را نقض می‌کند.

برای سایر تهدیدهایی که در این مقاله از آن‌ها نام بردیم، انجام چند اقدام ساده پیشگیرانه؛ نظیر استفاده از رمزگذاری‌های قدرتمند، محدودکردن ارتباطات در شبکه‌های اجتماعی تنها به دوستان مورد اطمینان و استفاده از سیستم‌های کنترل نفوذ در شبکه‌های سازمانی می‌توانند تا حدودی از نگرانی‌ها بکاهد، حتی اگر بزهکاران به روش‌های جدیدی درصدد برآشفتن زندگی ما باشند.

درباره نویسنده:

– جان براندون (John Brandon) یکی از مدیران سابق IT در شرکت Fortune 100 بوده که اکنون درباره فناوری مقاله می‌نویسد. او طی ده سال گذشته بیش از ۲۵۰۰ مقاله نوشته است.