احتمال هک اینترنت اشیا و خطرات در حال رشد آن

ما به سرعت در حال وارد شدن به مرحله ی جدیدی از تکامل تکنولوژیکی هستیم که در آن تقریبا هر چیز در اطراف ما به اینترنت متصل است. اصطلاح به کار گرفته شده برای شرح دادن این اکو سیستم متصل در حال رشد ، اینترنت اشیا (IoT) یا (Internet of Things) بوده و در حال جذب کردن بزرگ ترین نام ها در صنعت تکنولوژی به سوی خود است، از Apple و Samsung گرفته تا دیگر شرکت ها در کنار آن ها.

اگر کار شناسان تکنولوژی این بار هم درست باشند، به زودی هر چیزی از تستر ها گرفته تا لامپ های حبابی کارایی های اینترنتی خواهند داشت.

در حالی که تکنولوژی متصل شده به اینترنت حجم عظیمی از فرصت های جدید و هیجان انگیز ایجاد می کند، اما همچنین به همراه خود چالش های زیادی نیز می آورد که بزرگ ترین این چالش ها احتمالا بحث امنیت خواهد بود. هر دستگاه فعال با اینترنت به صورت بالقوه در برابر حمله از سوی هکر ها آسیب پذیر است، در نتیجه زمانی که تقریبا همه لوازم و چیز هایی که ما از آن ها استفاده می کنیم به اینترنت متصل است ، تنها ریسک ها و خطرات آن را تصور کنید که بطور مثال می توان به فیلمبرداری غیر محسوس تلویزیون های هوشمند از محل زندگی ما و ارسال آن، ارسال یک نسخه کپی از مطالب پرینت شده به شرکت سازنده ی آن،ردیابی تمامی اطلاعاتی که در طول روز رد و بدل می کنیم و...

اکثریت جامعه ی استفاده کننده از تکنولوژی ، با وجود هشدار های همیشگی از سوی دولت و سازندگان صنعت تکنولوژی، همچنان از این تهدید ها و خطرات نا آگاه باقی مانده اند. طبق گفته ی Canonical، کمپانی سازنده ی سیستم عامل Ubuntu ، چیزی حدود نیمی از جمعیت کشور انگلیس از امکان هک شدن دستگاه های متصل به اینترنت نا آگاه و بی خبر هستند!

اما با این وجود خطر های موجود احتمالی بسیار جدی و واقعی بوده. از در دست گرفتن کنترل ماشین های متصل به اینترنت گرفته تا استفاده از لوازم خانگی روزمره همچون یخچال فریزر و انجام حمله های سایبری فاجعه بار، هکر ها به شدت در حال سو استفاده از تکنولوژی اینترنت اشیا می باشند.

خودرو های در معرض خطر

یک صنعتی که در بهره گرفتن از پتانسیل بالای ارائه شده توسط اینترنت اشیا بسیار سریع بوده است صنعت ساخت وسایل موتوری یا همان صنعت خودرو می باشد. تولید کنندگان خودرو به سرعت و به صورت روز افزون در حال عرضه ی مدل هایی هستند که دارای سیستم های سرگرمی و اطلاع رسانی فعال با اینترنت می باشند و خودرو های خودران بدون راننده نیز دیگر چندان با ما فاصله ندارند. اما در حالی که صنعت خودرو های متصل به اینترنت در حال رشد و موفقیت است ، جاده ی پیش روی آن چندان هموار به نظر نمی رسد.

خودروی Jeep Cherokee با قابلیت های متصل به اینترنت

سال گذشته FBI شروع به همکاری با وزارت حمل و نقل ایالات متحده آمریکا، سازمان ملی ترافیک بزرگ راه و اداره ایمنی نمود تا به مردم در مورد تهدید های سایبری امنیتی وارد به خودرو ها هشدار دهد. این هشدار ها به همراه یک آزمایش کنترل شده توسط دو هکر بود که آن ها توانسته بودند یک دستگاه خودروی جیپ چروکی را در حال حرکت با سرعت ۷۰ مایل بر ساعت (۱۱۲ کیلو متر بر ساعت) هک کرده و در معرض خطر قرار دهند و کنترل فرمان و ترمز آن را از راه دور به دست گیرند.

اگر این اتفاق به صورت واقعی در زندگی واقعی بیافتد امکان دارد جان مردم را در معرض خطر قرار دهد Adam Boulton ، معاون ارشد بخش امنیت تکنولوژی در کمپانی Black Berry ، می گوید که هر دوی تولید کنندگان خودرو های خودران و متصل به اینترنت و هم خریداران و مصرف کنندگان آن ها ، نیاز دارند تا در مورد این پیامد های امنیتی آگاه باشند. آقای Boulton عصری را پیش بینی می کند که در آن خودرو ها برای باج گیری توسط هکر ها به گروگان نگه داشته می شوند ، یا دست کاری و خراب می شوند و یا در حمله های سایبری مورد استفاده قرار می گیرند. او همچنین در این رابطه می گوید:

ما در حال حاضر خودرو های خودران و متصل به اینترنتی را در بازار می بینیم که از قابلیت های خودکاری همچون کروز کنترل تطبیقی ، پارک اتوماتیک و کمک کننده ی ترافیکی بهره می برند. این باید به پیام رسان عصری از تصادفات کاهش یافته، آلودگی کم تر ، ترافیک روان تر و بهره وری بیش تر باشد.

اگر چه بدون وجود تکنولوژی امنیتی کامل در پایه و زیر بنای این خودرو ها، این می تواند پیام رسان عصری از خاموشی از راه دور موتور خودرو ها، گروگان نگه داشته شدن خودرو ها برای باج گیری توسط هکرها و حتی استفاده از آن ها برای پشتیبانی حمله های DDoS بر روی وب سایت های بزرگ باشد.

جلوگیری از به کنترل گرفته شدن خودرو ها توسط هکر های مخرب نیاز به تعادلی ظریف و حساس در مهندسی دارد تا مطمئن شوند که خودرو نه تنها امن است بلکه ایمن و بی خطر هم باقی می ماند. خودرو های متصل شده به تکنولوژی های پیشرفته همچون بوت امن نیاز دارند تا اطمینان حاصل کنند که تمامیت خودرو دست نخورده باقی مانده است.

هکر های دخالت کننده

علاوه بر هک کردن و نفوذ به سیستم های کامپیوتری برای به وجود آوردن هرج و مرج ، مجرمان سایبری به صورت روز افزون در حال تلاش و اقدام کردن برای نفوذ به گجت های متصل به اینترنت همچون روتر های وای فای، وب کم ها، ترموستات های هوشمند و پوشیدنی های هوشمند هستند تا حملات وسیع بر روی کمپانی ها و سازمان ها به انجام برسانند.

هکر ها و مجرمان سایبری پدیده ی جدید اینترنت اشیا را به عنوان فرصتی پرمنفعت می بینند.

Mirai نوعی محبوب از بد افزار ها در میان هکر ها است که به آن ها توانایی تبدیل سیستم ها به بات نت ها برای شروع در معرض خطر قرار دادن شبکه ها را ارائه می دهد. در ماه سپتامبر سال ۲۰۱۶ هکر ها از ۱۵۲ هزار دستگاه متصل به اینترنت اشیا مصرف کنندگان استفاده کردند تا یک حمله ی DDoS را بر روی ارائه دهنده خدمات میزبانی فرانسوی ،OVH، آغاز نمایند. آن ها توانستند این کمپانی را با

۱ ترا بایت بر ثانیه ترافیک اشباع کنند , مشکلات عظیمی برای مصرف کنندگان آن ها در سر تا سر دنیا ایجاد کنند.

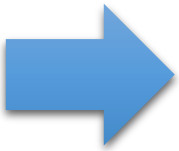
مصرف کنندگان و دستگاه های آن ها به صورت نا خواسته ای به هم دستان و کمک کننده در حمله های سایبری تبدیل شده اند و هیچ چیزی برای جلو گیری از دوباره اتفاق افتادن آن وجود ندارد . Paul McEvatt، مدیر ارشد اطلاعات تهدید سایبری برای بریتانیا و ایرلند در کمپانی Fujitsu ، پیش بینی می کند که در چند سال آینده شاهد اتفاق های بیش تر از این دست خواهیم بود. او همچنین در این باره اظهار داشته است:

با ادامه ی دیدن رشد و پیشرفت دستگاه های بهره گرفته از اینترنت اشیا ، ما همچنین به دیدن مشکلات امنیتی که پیش از این در نظر نگرفته ایم نیز ادامه خواهیم داد.

زمانی که یک معمار طراحی تابلو های هوشمند جاده ها را به انجام رساند ، آن ها هیچ وقت حتی به این موضوع فکر هم نمی کردند که یک هکر از آن ها برای نشان دادن پیام های سیاسی استفاده کند. همین داستان در مورد سازندگان اینترنت اشیا که صدها هزار دوربین امنیتی CCTV و DRV ها و روتر های SOHO که هم اکنون بات نت اینترنت اشیا Mirai را تشکیل می دهند، نیز صدق می کند.

هکر ها در حال حاضر هم از این آسیب پذیری ها به نفع خودشان سو استفاده کرده اند ، در نتیجه در حالی که بد افزار های باج گیری با داشتن توانایی از کار انداختن شهری از چراغ های هوشمند متصل تا ۱۲ ماه پیش بعید و نشدنی به نظر می رسید ، رویداد های اخیر این دیدگاه را تغییر داده اند.

McEvatt سازندگان را برای این مشکلات سرزنش می کند. او می گوید که :«مشکل این است که سازندگان از جاسازای کنترل امنیتی قدرتمند از همان ابتدا باز مانده اند ، چه برای روتر ها، دستگاه های هوشمند و یا حتی خودرو های متصل به اینترنت.



یادمان باشد هیچ دستگاهی امن نیست

صنعت اینترنت اشیا در حال گسترش می باشد و با مراجعه ی دسته جمعی مصرف کنندگان به فروشگاه ها برای دست یابی به جدید ترین تکنولوژی های متصل به اینترنت، مجرمان سایبری این را به چشم یک فرصت سود آور و پر منفعت می بینند از آن جایی که بیش تر سخت افزار های در دست مصرف کنندگان به راحتی قابل هک شدن می باشند.

طبق یک پژوهش صورت گرفته ی جدید ، صد ها میلیون از دستگاه های متصل به اینترنت در مقابل حمله های از سوی مجرمان سایبری آسیب پذیر بوده و در معرض خطر می باشند **Nick Shaw** ، معاون ارشد و مدیر عامل شرکت سازنده ی نرم افزار آنتی ویروس ، **Norton**، می گوید که دستگاه های عادی و معمول همچون تلویزیون های هوشمند، سیستم های امنیتی خانگی و دوربین های مراقبت از کوکان همگی قابل هک شدن می باشند و می توانند به عنوان بات نت ها مورد سو استفاده قرار گیرند یا برای باج گیری و تقلب. او همچنین در این زمینه می گوید:

با استفاده ی بیش تر ما از دستگاه های فعال شده با اینترنت در زندگی روزمره مان ، مجرمان اینترنتی در حال توجه بیش تری به این موضوع می باشند. ما در حال دیدن هک شدن و ربوده شدن دستگاه های هوشمند مصرف کنندگان می باشیم زیرا که به اینترنت متصل هستند و پسورد های پیش فرض آن ها نیز تغییر داده نشده است.

از لپ تاپ ها و گوشی های هوشمند گرفته تا دستگاه های اندازه گیری تناسب اندام و روتر ها ، سیستم های امنیتی خانه ها، دوربین های مراقبت از بچه و هر دستگاه دیگر متصل به اینترنت به صورت بالقوه یک هدف برای هکر ها بوده اما آن هایی با رمز های عبور پیش فرض، آپدیت های نامنظم و کم و پروتکل های امنیتی ضعیف، از همه آسیب پذیر تر هستند و بیش تر در معرض خطر قرار دارند.

در بیش تر مواقع مصرف کنندگان تصور نمی کنند که پوشیدنی های هوشمند متصل به اینترنت آن ها و یا دستگاه های خانه شان مورد همان تهدید ها و خطراتی قرار دارند که لپ تاپ ها و گوشی های

هوشمندشان در معرض آن ها می باشند، در نتیجه آن ها هیچ اقدامی برای امن تر کردنشان انجام نمی دهند.

Shaw همچنین اضافه می کند که مصرف کنندگان می توانند با تغییر دادن اختیارات و رمز های پیش فرض، غیر فعال کردن خدمات استفاده نشده ، تغییر دادن تنظیمات حریم خصوصی دستگاه و به روز نگه داشتن نرم افزار دستگاه ، از ریسک مورد هک قرار گرفتن دستگاه کم کنند.

با فراگیر تر شدن اینترنت اشیا در دستگاه های اطراف ما، تهدیدات امنیتی جدی تر شده و وظیفه ی مصرف کنندگان برای ایمن کردن دستگاه هایشان با اهمیت تر.

اینترنت اشیا هنوز در مراحل آغازین و کودکی خود قرار دارد و با گسترش و تکامل یافتنش ، این احتمال وجود دارد که تهدیدات امنیتی که به همراه خود می آورد نیز پیچیده تر و گسترده تر خواهند شد.

همچنین در آینده ای نزدیک باید منتظر هجوم هکرها به صورت ابر الکترونی در فضای مجازی باشیم، برای مثال آنها قادر خواهند بود با کنترل یک چیپ به ژن هر انسان دست یافته و با تزریق مواد نابود

کننده مثل سم و دستور حرکت به آن توسط امواج مغناطیسی و یا هوا، شخص را یافته و چیپ مربوطه را با توسط علم هوش مصنوعی و بدون اینکه شخص متوجه شود از طریق دم و بازدم وارد بدن او کند سپس سم را تزریق و او را نابود نماید.

در حال حاضر نیازی ضروری برای سازندگان و دیگر سازمان ها وجود دارد تا راه های حافظتی به وجود بیاورند تا هکر ها را در راهشان متوقف کنند. و همگی ما نیز با به انجام رساندن وظیفه ی خودمان باید مطمئن شویم نقش خود را در کاهش تهدیدات ایفا کرده ایم و از احتمال این که دستگاه های اینترنت اشیا ما قربانیان بعدی خواهند بود بکاهیم.