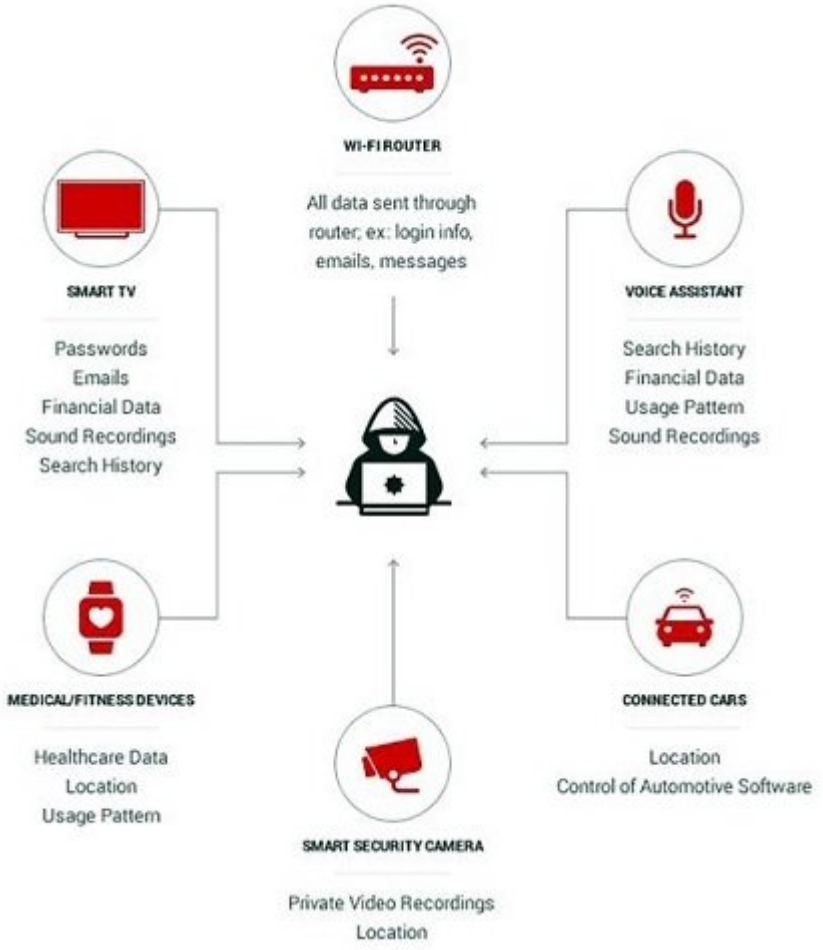
داستان هک شدن تجهیزات اینترنت اشیا

یک سناریو واقعی از روزی که هک شدید

هر زمان یک دستگاه الکترونیکی (محاسباتی یا هوشمند) را روشن می‌کنید، اتفاقات غیرمنتظره در انتظار شما هستند. خرابی ناگهانی دستگاه، باز نشدن یک برنامه کاربردی به دلیل انقضای اعتبارنامه، عدم ورود به سامانه به دلیل درج اشتباه گذرواژه، چند نمونه ساده از دردسرهای ناخواسته‌ای هستند که هر کاربری را تهدید می‌کنند. در این مقاله قصد داریم یک سناریو واقعی حمله هکری را بررسی کنیم که ممکن است در یک شبانه‌روز زندگی را به کام شما تلخ کنند. در این مقاله به محصولات هوشمندی اشاره شده که مشابه آن‌ها یا همان محصولات در بازار ایران وجود دارند. شاید در زمان خواندن این مقاله از تجهیزات هوشمندی مانند این‌ها استفاده نکنید، اما در چند سال آینده به سراغ آن‌ها خواهید رفت و تازه متوجه خطراتی خواهید شد که ممکن است با آن‌ها روبرو شوید!

آمارها نشان می‌دهند از هر سه کارمند یک اداره یا شرکت، تنها یک نفر درباره خطرات باج‌افزارها اطلاعات کافی دارد. آمارهایی از این دست به وضوح نشان می‌دهند که صنعت سایبری هنوز هم در تلاش است تا اصول اولیه امنیت و تهدیدات هکری را به افراد آموزش دهد. زمانی‌که هکرها بتوانند از طریق بدافزارها یا باج‌افزارها به سامانه‌های هوشمند و حتا سامانه‌های نظارتی که والدین برای کنترل فرزندان خود از آن‌ها استفاده می‌کنند، نفوذ کنند، بدون مشکل به اطلاعات شخصی و مالی آن‌ها دسترسی خواهند داشت اطلاعاتی که برای اخاذی یا جعل هویت از آن‌ها استفاده می‌شود. در یک شبانه‌روز شما ممکن است هر لحظه از سوی دوربین نظارتی هوشمند، دستگاه‌های تناسب‌اندام/مراقبت‌های پزشکی، دوربین‌های متصل به شبکه، تلویزیون هوشمند، روتر وای‌فای یا دستیار صوتی در معرض هک احتمالی قرار داشته باشید.



□□□□ *1* - □□ □□□□□□□ □□□□□□□□ □□ □□□□ □□ □□□□□□ □ □□ □□ □□ □□□□□□□□ □□□□□□□ □□ □□□□ □□ □□□ □□□□ □□□□□. □□□□□□ □□□ □□□ □□ □□□□□□□□ □□□□□□□ □□ □□ □□ □□□□□□ □□□□□□□□ □□□□□ □□ □□□□□□□ □□ □□□□ □□□□□ □□□□□ □□□□□□.

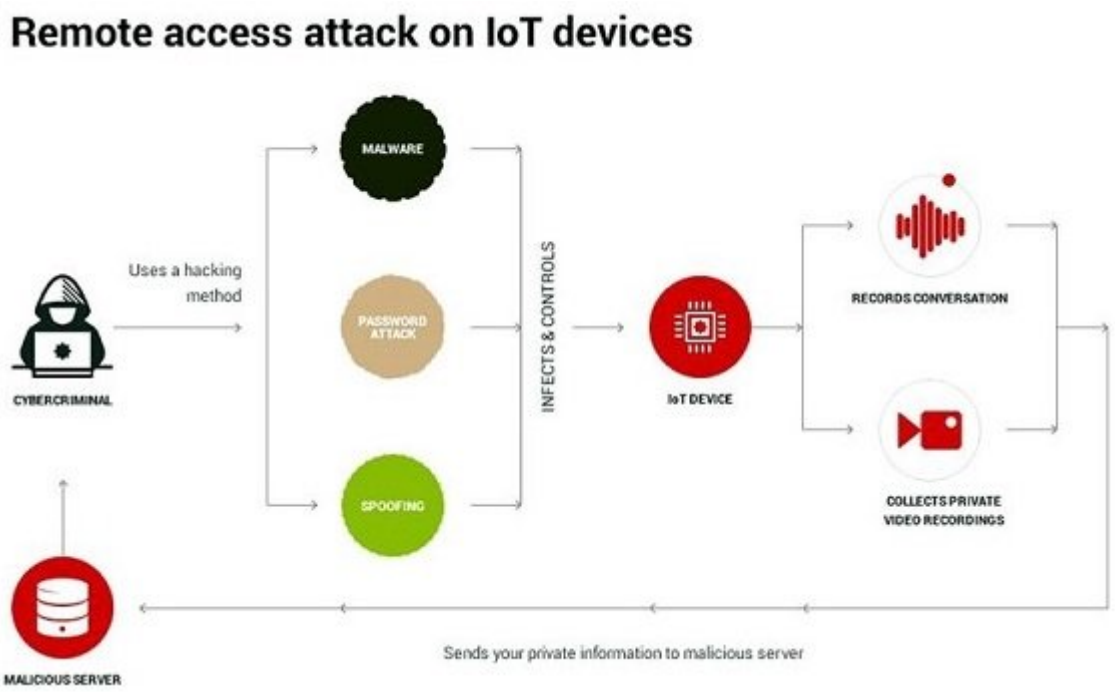
اینترنت در سال‌های پایانی دهه 60 میلادی اختراع شد، اما روند به‌کارگیری گسترده و تجاری آن با پایان یافتن دهه 80 میلادی و زمانی که ارائه‌دهندگان خدمات اینترنتی (ISP) به میدان وارد شدند آغاز شد و اینترنت را به شاهراه تبادل اطلاعات تبدیل کرد. اولین دستگاه متصل به اینترنت، یک دستگاه اینترنتی فروش نوشابه بود که توسط دانشجویان دانشگاه کارنگی ملون در دهه 80 میلادی اختراع شد. عملکرد دستگاه به این شکل بود که ریزسوییچ‌هایی درون آن قرار داشت تا تعداد بطری‌های نوشابه درون ستون‌های ششگانه دستگاه را محاسبه کند. سوییچ‌ها به کامپیوتر اصلی در دفتر مرکزی که CMUA نام داشت متصل بودند. اختراع چنین دستگاهی در زمان خود یک شاهکار بود، زیرا دستگاه می‌توانست مدت زمانی‌که بطری‌ها درون دستگاه قرار داشتند را نشان دهد. در عصر جدید، فناوری به اندازه‌ای پیشرفت کرده که تیترهایی همچون یخچال‌های هوشمند، اسپیکرهایی که با کاربر سخن می‌گویند یا حتا دستیاران صوتی روی گوشی‌های هوشمند خبری عادی تلقی می‌شوند. اکنون باید خود را برای شنیدن تیترهایی همچون "توستر خانگی درب خانه را به روی هکرها گشود"، آماده کنید. مهم نیست در تهران یا سایر کلان شهرها سکونت دارید. اگر به فروشگاه‌های لوازم الکترونیکی در شهر خود مراجعه کنید و به آن‌ها بگویید که قصد دارید خانه خود را به معنای واقعی کلمه هوشمند کنید، آن‌ها برآورد قیمتی انجام داده و به‌طور مثال می‌گویند با پرداخت 20 تا 35 میلیون تومان تجهیزات مهم خانه شما از چراغ‌های روشنایی و دوربین‌های نظارت تصویری گرفته تا کنترل وضعیت دمای خانه و حمام کاملا هوشمند خواهند شد. به عبارت دیگر، شما خواسته یا ناخواسته به دنیای اینترنت اشیا وارد می‌شوید. یک دنیای هوشمند که تمامی حس‌گرهای درون آن به‌طور مداوم در حال تبادل اطلاعات با یکدیگر هستند و در برخی موارد اطلاعات خود را روی بستر اینترنت قرار می‌دهند. با این حساب دوست دارید درباره نقش تاثیرگذار تجهیزات اینترنت اشیا روی زندگی شخصی خود اطلاعات جالبی به دست آورید و ببینید در یک شبانه‌روز ممکن است چه اتفاقاتی برای شما رخ دهد؟ اجازه دهید به زندگی شما زمانی‌که به‌طور کامل حول محور اینترنت اشیا در حرکت است نگاه کنیم تا ببینیم در 24 ساعت چه تهدیدات سایبری مستتری پیرامون شما قرار دارد.

مطلب پیشنهادی

درمان پس از آسیب‌دیدگی
پس از هک شدن حساب کاربری چه کارهایی باید انجام دهیم؟

ساعت 8 صبح است و شما به یک فنجان چای یا قهوه نیاز دارید؛ اما دستگاه هوشمند پیغام عجیبی نشان می‌دهد

قهوه‌سازی که با گوشی هوشمند یا سایر تجهیزات متصل به اینترنت همچون کتری‌های هوشمند کنترل می‌شود، رفتاری عجیب از خود نشان می‌دهد، زیرا سازنده تنها به دنبال آن بوده تا یک دستگاه قهوه‌ساز هوشمند تولید کند و هیچ‌گونه مکانیزم امنیتی برای مقابله با یک حمله هکری در نظر نگرفته است. کد دستگاه و قابلیت اتصال به اینترنت پس از تولید دستگاه به آن افزوده شده‌اند، در نتیجه یک مکانیزم امنیتی برای مقابله با نفوذ در نظر نگرفته شده است. هکر یا هکرهایی موفق شده‌اند با هک کردن قهوه‌ساز به دستیار شخصی درون خانه همچون الکسا نفوذ کنند.



- 2□□□
□□□□□
□□□□□□□
□□□□□
□□□□
□□□□□□
□□□□□

چگونه این اتفاق رخ داده است؟

زمانی‌که یک دستگاه متصل به اینترنت روشن می‌شود، در اغلب موارد یک هات‌اسپات فاقد رمزگذاری ایجاد می‌کند. کسپرسکی می‌گوید: «زمانی که این اتفاق رخ دهد، اطلاعات مهمی همچون SSID و گذرواژه شبکه بی‌سیم خانگی ممکن است فاش شوند. خانه مکانی است که وای‌فای شما به شکل خودکار به همه چیز متصل است.» در یک سناریو واقعی، یک حمله باج‌افزاری در مقیاس کلان یک شرکت پتروشیمی را قربانی خود کرد، در این حمله یک دستگاه قهوه‌ساز باعث شد تا هکرها کنترل اتاق فرمان کارخانه را به دست گیرند.

راه‌های مقابله با چنین حمله‌ای چیست؟

- هیچ‌گاه از تنظیمات پیش‌فرض کارخانه روی دستگاه‌های هوشمند خود استفاده نکنید و همواره گذرواژه‌ها را تغییر دهید.

- اگر از گوشی هوشمند، کامپیوتر شخصی یا لپ‌تاپ برای کنترل وسایل هوشمند استفاده می‌کنید، اصول امنیتی

را رعایت کنید.

- سعی کنید گذرواژه دستگاه در بازه‌های زمانی کوتاه مدت تغییر کند، هیچ‌گاه از گذرواژه پیش‌فرض دستگاه برای مدت زمان طولانی استفاده نکنید.

قهوه‌سازهای هوشمند به تدریج در حال ورود به بازار ایران هستند. قهوه‌ساز نسپرسو شیائومی SCISHARE نمونه‌ای از محصولات خانگی هوشمند این شرکت است. به تدریج نمونه‌ها و برندهای مختلفی نیز به بازار عرضه می‌شوند، تعجب نکنید چرا ما به سراغ محصولی رفته‌ایم که در آینده مهمان خانه شما خواهد بود! اگر تمایلی ندارید در هر بار استفاده قهوه‌ساز خود را به شکل دستی به اینترنت متصل کنید، بهتر است زمانی که به وای‌فای متصل شد، گذرواژه پیش‌فرض آن‌را تغییر دهید. روزانه صدها نفر در سراسر جهان به واسطه عدم رعایت همین نکته امنیتی ساده هک می‌شوند.

مطلب پیشنهادی

شناسایی نفوذهای غیرمجاز
چگونه می‌توانیم از هک شدن حساب‌های آنلاین خود مطلع شویم؟

ساعت 8:30 صبح شده، سامانه کنترل والدین را تنظیم می‌کنید تا فرزندان بیش از اندازه به فضای مجازی وارد نشوند و در همین حال با دستیار مجازی (الکسا) آهنگ گوش می‌کنید

هر دو دستگاه به دلیل عدم پیکربندی درست تنظیمات امنیتی از سوی کاربر، بستر مناسبی برای ورود هکرها به شبکه خانگی هستند. متاسفانه دستگاه‌های کنترل والدین به انواع مختلفی از آسیب‌پذیری‌ها آلوده هستند. کارشناسان امنیتی در جریان برگزاری جشن هالووین سال گذشته میلادی اعلام کردند 23 آسیب‌پذیری در محصول کنترل والدین شرکت والت دیزنی را وصله کردند. 23 آسیب‌پذیری روی دستگاهی شناسایی شد که چند ماه به شبکه وای‌فای خانگی کاربران متصل بود تا امکان مدیریت روی سایر دستگاه‌ها را فراهم کند. پژوهشگران امنیتی شرکت Cisco Talos در خصوص آسیب‌پذیری فوق گفته‌اند: «اگر سامانه کنترل والدین دیزنی هک می‌شد، هکرها می‌توانستند، ترافیک شبکه را تغییر داده، کدهای از راه دور را به دستگاه تزریق کرده، نرم‌افزارهای غیرمجاز را نصب کرده، فرآیندهای احراز هویت را دور زده، دستگاه را دومرتبه راه‌اندازی کرده، کدهای دسترسی پایدار را به میان‌افزار دستگاه وارد کرده، فایل‌ها را بازنویسی کرده یا حتا به‌طور کامل دستگاه را خراب کنند.» در اوت 2017 میلادی، پژوهشگران شرکت MWR InfoSecurity خبر از هک کردن دستیار صوتی الکسا دادند. در این حمله هکری، پژوهشگران موفق شدند به شنود مکالمات پرداخته و مکالمات را برای یک کامپیوتر راه دور ارسال کنند. این حمله فیزیکی به اکو آمازون نشان داد که هکرها می‌توانستند به سیستم‌عامل لینوکس دستگاه حمله کرده و کدهای مخرب را بدون هیچ‌گونه دستکاری فیزیکی درون دستگاه نصب کنند. در این حالت هکرها می‌توانستند هر لحظه به مکالمه‌های شما گوش دهند. در نمونه دیگری که به‌نام حمله دلفین‌ها معروف شد، کارشناسان امنیتی نشان دادند با ارسال فرمان‌های صوتی اولتراسونیک که گوش انسان قادر به شنیدن آن‌ها نیست، امکان هک دستیاران صوتی همچون سیری، الکسا و Ok Google وجود دارد. (در حال حاضر دستیار صوتی آمازون، Echo Show نسل دوم به قیمت 4 میلیون و نهصد هزار تومان در ایران به فروش می‌رسد.)

چه تمهیداتی باید در نظر گرفت؟

- گذرواژه پیش‌فرض روتر و دستگاه‌های متصل به اینترنت را تغییر دهید

- زمانی که دستگاه را خریداری کردید، گذرواژه آن‌را تغییر دهید.

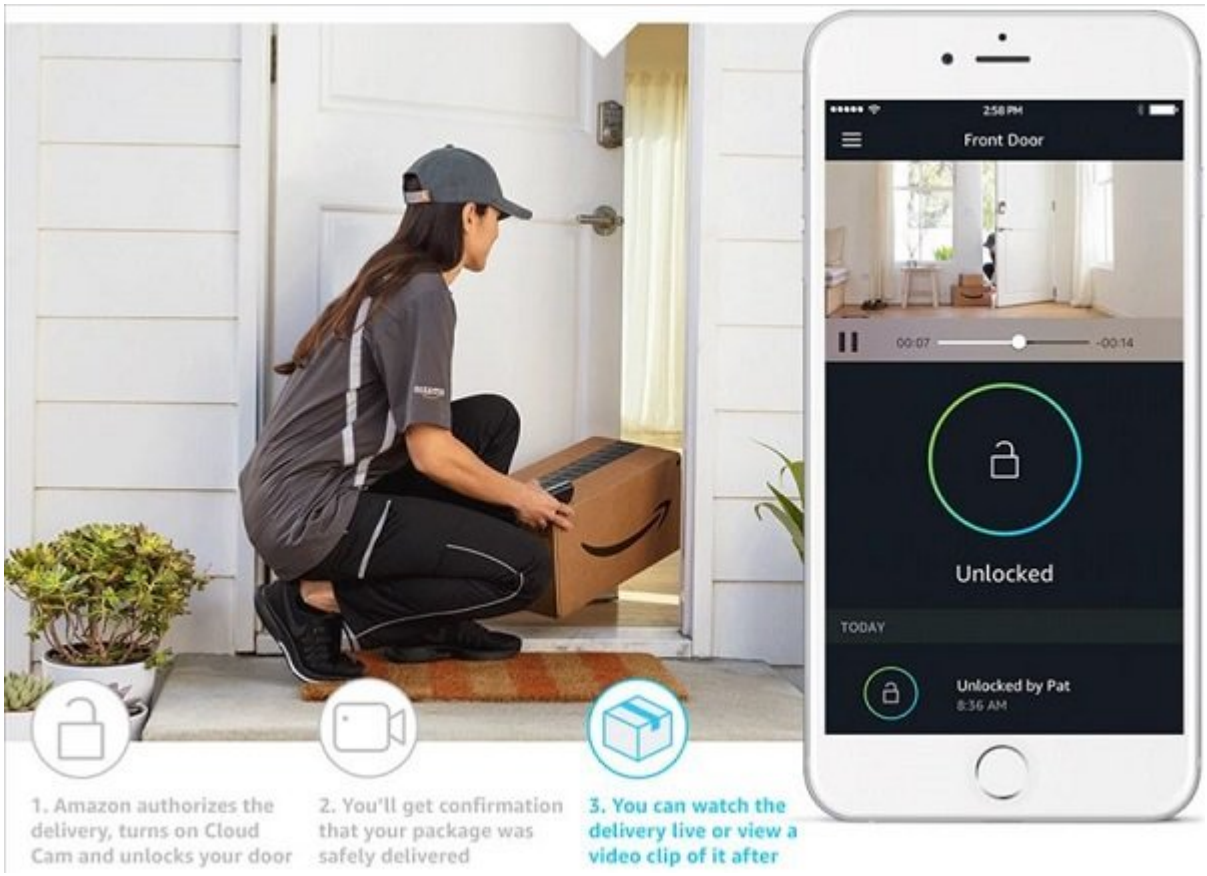
- از گذرواژه یکسان روی همه دستگاه‌ها استفاده نکنید.

مطلب پیشنهادی

اتخاذ رویکردی منطقی به منظور مقابله با هکرها
5 باور اشتباه پیرامون بهبود امنیت وای‌فای

ساعت 9 صبح شده و آماده ترک خانه هستید، اما پیک آمازون (یا فروشگاه‌های مشابه ایرانی) هنوز نرسیده‌اند، مجبور هستید کلید هوشمند درب خانه را برای او تنظیم کنید

آمازون جزء پیشگامان عرضه قفل‌های هوشمند درب منازل است. این شرکت قفل هوشمندی به‌نام Amazon Key دارد. یک سامانه قفل و دوربین که اجازه می‌دهد از راه دور در خانه را برای افراد (در این‌جا پیک) باز کرده و کنترل جامعی روی باز و بسته کردن درها داشته باشید. این سامانه می‌تواند در منزل را برای یک پیک باز کرده و زمانی که بسته درون خانه روی زمینه قرار گرفت فیلمی از آن تهیه کند. سامانه فوق قابلیت جالب دیگری نیز دارد. Amazon Key با تولید رمزهای موقت به دوستان یا آشنایان اجازه می‌دهد زمانی که قادر به کنترل در خانه نیستید از راه دور این‌کار را برای شما انجام دهند (شکل 3).



□□□3 - □□□ □□□□□□ □□□□□□ □□□□ □□□□ □ □□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □ □□□□ □□ □□□□ □□□□□ □□□□ □□□□□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□□.

آمازون می‌گوید: «این سامانه اجازه می‌دهد بدون نگرانی از بابت به سرقت رفتن بسته‌ها، آن‌ها را درون خانه دریافت کنید.» اما شرکت امنیتی MALWARBYTES موافق چنین راهکاری نیست و می‌گوید: «شما نباید قفل هوشمند آمازون را خریداری کنید، زیرا آمازون هیچ‌گونه اطلاعاتی درباره نرم‌افزار Amazon Key ارائه نکرده است. در نتیجه هیچ‌گونه مکانیزمی برای بررسی قابلیت‌های امنیتی آمازون کی در دسترس نیست. با توجه به این‌که مشخص نیست کاربر تا چه اندازه قادر به کنترل نرم‌افزار است، تضمینی وجود ندارد که مکانیزم‌های امنیتی ابزار فوق به درستی کار کنند. با این توصیف ممکن است هکری رخنه‌ای پیدا کند و به خانه وارد شود.»

مطلب پیشنهادی

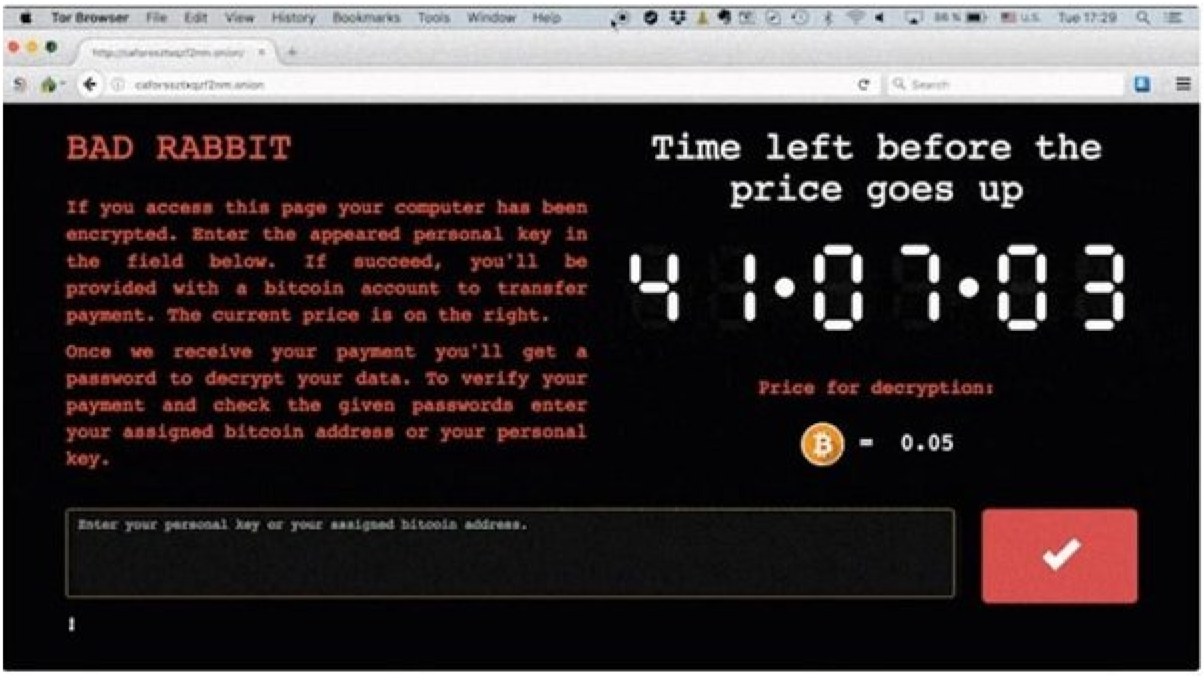
تنها نیم ساعت زمان برای شکستن قفل‌ها
قفل‌های الکترونیکی تا چه اندازه در برابر نفوذ ایمن هستند

ساعت 9:10 صبح است و از دستیار صوتی گوشی خود درخواست می‌کنید برنامه مسیریابی همچون گوگل مپ را باز کند

حمله دلفین نشان داد دستیارهای شخصی هوشمند هک‌پذیر هستند. اگر از ویژگی جامعیت یا یکپارچگی صوتی استفاده کنید، بدافزار EVIL-DOERS در کمین شما است. بدافزار فوق به یک دستیار صوتی شبیه به سیری اعلام می‌کند قفل هوشمند در خانه را باز کن و بدتر از آن موقعیت مکانی شما را در اختیار هکرها قرار می‌دهد. روزانه اطلاعات خود را ناخواسته در اختیار برنامه‌هایی قرار می‌دهیم که روی گوشی هوشمند خود نصب کرده‌ایم. شما در حال حرکت به سمت شرکت هستید، غافل از آن‌که قفل هوشمند در خانه باز شده و موقعیت مکانی شما نیز برای هکرها ارسال شده است. سال 2016 میلادی نزدیک به 1.3 میلیون حساب گوگلی از طریق برنامه‌های مخرب اندرویدی در معرض خطر قرار گرفتند. در شش ماهه نخست سال 2017 میلادی باج‌افزارهای اندرویدی رشد 137.8 درصدی داشتند، اما اکنون هکرها به سراغ سیستم‌عامل iOS رفته‌اند. با این توصیف و برای مقابله با این تهدیدات، باید نظارت دقیقی روی مجوزهایی داشته باشید که برنامه‌ها درخواست می‌کنند.

ساعت 10 صبح شده و در محل کار حاضر هستید، اما کامپیوتر قفل شده و مسئول فناوری‌اطلاعات سراسیمه است

بدون توجه به وضعیت مسئول نگون‌بخت، به سراغ کامپیوتر خود می‌روید که یکی از همکاران می‌گوید، همه سامانه‌ها تحت تاثیر حمله باج‌افزار خرگوش بد قفل شده‌اند. همه کامپیوترها پیام یکسانی نشان می‌دهند که حکایت از قفل شدن همه داده‌ها دارد. هکر بازه زمانی را برای دریافت باج سنگین که باید به شکل بیت‌کوین پرداخت شود، تعیین کرده است (شکل 4). این حمله باج‌افزاری در اکتبر سال 2017 میلادی و پس از به‌روزرسانی جعلی نرم‌افزار ادوبی فلش رخ داد و شرکت‌های بزرگی در روسیه، ترکیه، بلغارستان و اوکراین را قربانی کرد و بدتر از آن عملکرد چند شرکت ترانزیت را به‌طور کامل متوقف کرد.



- 4□□□ □□□□□□□ □□□□□ □□ □□□□□ □□□□ □□ □□ □□□ □ □□□□ □□□ □□ □□□□□□□ □□□□□□□ .□□□

چه تمهیداتی وجود دارد؟

از اطلاعات خود نسخه پشتیبان تهیه کرده و سعی کنید سامانه‌های حیاتی و اصلی شرکت را به شکل مستقیم به اینترنت متصل نکنید. ابزارها و سامانه‌های فرعی را برای به دام انداختن حملات هکری استفاده کنید و فهرستی از ابزارهای رمزگشایی باج‌افزار تهیه کنید. پرداخت باج در اغلب موارد مشکل شما را حل نمی‌کند.

ساعت 1 بعدازظهر است، از جلسه‌ای که پیرامون حمله هکری اتفاق افتاده خارج می‌شوید و سعی می‌کنید به تیتر اخبار نگاهی کنید، اما سایت موردنظر باز نمی‌شود

حمله بات‌نتی سایت شما را قربانی کرده است. بات‌نت شبکه‌ای بزرگ از دستگاه‌های متصل به اینترنت است که بدون اطلاع مالک قربانی تحت کنترل هکرها قرار گرفته‌اند. هکرها از بات‌نت‌ها برای پیاده‌سازی یک حمله DDoS استفاده می‌کنند. در یک روز آشفته، نزدیک به 300 هزار دوربین مداربسته و قهوه‌ساز هوشمند به یک‌باره به سایتی که شما قصد مراجعه به آن‌را دارید حمله کرده‌اند.
سرورهای سایت به دلیل حمله گسترده از دسترس خارج شده و قادر به سرویس‌دهی نیستند. مشابه چنین حمله‌ای در سال 2016 توسط بات‌نت میرای عملکرد شرکت داین را برای چند ساعت مختل کرد و دسترسی به سایت‌های مهمی همچون توییتر، نت‌فلیکس و.... را غیر ممکن کرد.

چه تمهیداتی باید در نظر گرفت؟

- گذرواژه پیش‌فرض تمام دستگاه‌ها را تغییر دهید تا هکرها به سادگی موفق نشوند به دستگاه‌ها نفوذ کنند.

- قبل از خرید هر دستگاهی تحقیقی انجام دهید تا مشکلات احتمالی را مشاهده کنید. همچنین، بررسی کنید که سازنده هر چند وقت یک‌بار برای دستگاه‌های خود به‌روزرسانی امنیتی ارائه می‌کند.

مطلب پیشنهادی

اضافه کردن یک لایه امنیتی مضاعف
چگونه می‌توانیم یک دیوارآتش به گوشی اندرویدی خود اضافه کنیم؟

ساعت 4 بعدازظهر است و در حال ترک شرکت هستید. با اوبر یا تاکسی‌های اینترنتی تماسی برقرار می‌کنید. تاکسی می‌آید و اطلاعات شما می‌رود!

در سال 2017 میلادی خبری منتشر شد که اپل به تاکسی‌های تلفنی اوبر اجازه داده به شکل کم سابقه‌ای صفحات گوشی آی‌فون را بخوانند، حتا زمانی که برنامه اوبر در پس‌زمینه قرار دارد و فعال نیست. مجوزی که اجازه می‌داد، اوبر در زمان بسته بودن برنامه، اطلاعات روی صفحه‌نمایش را به دست آورده و به اطلاعات حساس کاربران دسترسی داشته باشد.
حال تصور کنید، حمله هکری که سال 2014 میلادی برای رانندگان اوبر رخ داد یکبار دیگر در سال 2017 میلادی تکرار می‌شد و هکرها موفق می‌شدند به اطلاعات حساس کاربران دسترسی پیدا کنند. فاجعه‌ای بزرگ رقم می‌خورد و حساب‌های کاربری و هویت واقعی افراد به سرقت می‌رفت و در وب تاریک به فروش می‌رسید.

چه تمهیداتی باید در نظر گرفت؟

پس از به‌روزرسانی سیستم‌عامل گوشی، مجوزها و سطح دسترسی که برنامه‌ها درخواست کرده‌اند را بررسی کنید.

ساعت 6 عصر است، سعی می‌کنید به محل قرار ملاقاتی بروید که به شکل اینترنتی با شخصی هماهنگ کرده بودید، اما متوجه می‌شوید قربانی فیشینگ شده‌اید!

با شخصی در یک شبکه اجتماعی قرار ملاقاتی فیزیکی می‌گذارید. شخص مذکور لینک محل ملاقات را برای شما ارسال می‌کند، اما قربانی یک حمله فیشینگ شده‌اید که قصد داشته اطلاعات شخصی شما را به سرقت ببرد، زیرا شما در حال گفت‌وگو با یک ربات بودید. آمارها نشان می‌دهند جوانان 11 درصد بیشتر از افراد مسن قربانی حملات

فیشینگ می‌شوند (شکل 5). ساده‌ترین شکل یک حمله فیشینگ، حساب‌هایی است که درون لینکدین مشاهده می‌کنید که سعی می‌کنند از شما اطلاعاتی به دست آورند و پس از گذشت مدت زمانی از لینکدین پاک می‌شوند و تنها پیام‌های خود را مشاهده می‌کنید.

□□□5 - □□□□□ □□□□□□ □□□□□ □□□□□□□□ □□ □□□□□ □□ □□□ □□□□ □□□□□□.

ساعت 9 شب است، به خانه دوست‌تان می‌روید که علاقمند به فناوری‌های هوشمند است

در خانه نشسته‌اید که ناگهان چراغ‌ها خاموش می‌شوند، ترموستات از کار می‌افتد و صدای ضبط صوت بلند می‌شود. یک دستگاه متصل به اینترنت همواره در معرض هک قرار دارد، حال تصور کنید یک خانه هوشمند چه وضعیتی دارد. اگر هکرها به واسطه عدم وجود تنظیمات امنیتی صحیح به دستگاه‌های متصل به اینترنتی که درون خانه هوشمند قرار دارند متصل شوند، عکس‌های شخصی، اطلاعات کارت‌های اعتباری، شماره تامین اجتماعی و.... را به‌راحتی سرقت می‌کنند. بهترین راه مقابله با این تهدیدات عدم اتصال به وای‌فای عمومی و نصب یک دیوارآتش میان تجهیزات خانه و اینترنتی است که به خانه وارد می‌شود.

ساعت 22:30 دقیقه است و دوست شما قصد دارد با ماشین ساخت شرکت تسلا شما را برساند که متوجه می‌شوید ماشین هک شده است

هکرها توانسته‌اند به یکی از قفل‌های در ماشین نفوذ کرده و آن‌را قفل کنند. مجبور هستید از صندلی عقب پیاده شوید که ناگهان صدای رادیو ماشین بلند می‌شود. ماشین‌های الکتریکی به اینترنت متصل هستند و هر یک از مولفه‌های آن‌ها در معرض تهدید قرار دارند. سال 2016 میلادی بود که پژوهشگران چینی توانستند به شکل بی‌سیم و از طریق هات‌اسپات آلوده و از فاصله 12 مایلی کنترل ماشین برقی تسلا و ترمزها را به دست آوردند. تا زمانی که وضعیت ماشین‌های الکتریکی و نواقص امنیتی آن‌ها بهتر نشده به سراغ خرید این مدل ماشین‌ها نروید.

ساعت 11 شب است و تصمیم می‌گیرد از برنامه‌های آرامش اعصاب استفاده کنید، اما برنامه هک شده است!

ساعت 11 شب است و شما در طول روز دائما در معرض حملات هکری بودید. بیشتر مردم پیش از خواب تصمیم می‌گیرند از برنامه‌های آرام‌بخش استفاده کنند، اما برنامه‌های فوق ایمن نیستند. یک برنامه مدیتیشن را دانلود کرده و روی گوشی اجرا می‌کنید که ناگهان متوجه می‌شوید عملکرد گوشی اندرویدی کاهش پیدا کرده، زیرا هکرها توانسته‌اند از فیلترهای پلی‌استور عبور کرده و نسخه آلوده به معدن‌کاوی این برنامه را روی فروشگاه آپلود کنند. در سال

2016 میلادی، هر 4.6 ثانیه یک بدافزار جدید ساخته شد که این روند تصاعدی تا سال 2017 نیز ادامه پیدا کرد (شکل 6).

کلام آخر

در این مقاله سعی کردیم به شکل کوتاه یک روز پر خطر که پیش روی هر یک از ما قرار دارد را به تصویر بکشیم. در سناریوهای پیچیده هکرها می‌توانند حتا از طریق صدای فن پردازنده و امواج الکترومغناطیس که توسط پردازنده مرکزی منتشر می‌شوند، اطلاعات را سرقت کنند. پیشنهاد می‌کنیم پیش از خرید هر محصولی تحقیقی در مورد آن انجام دهید و تا حد امکان به سراغ خرید محصولاتی نروید که تازه روانه بازار شده‌اند. سعی کنید گذرواژه‌های پیش‌فرض دستگاه‌ها را تغییر داده و به وای‌فای عمومی متصل نشوید.

تاریخ انتشار:
21 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/16156/%DB%8C%DA%A9-%D8%B3%D9%86%D8%A7%D8%B1%DB%8C%D9%88-%D9%88%D8%A7%D9%82%D8%B9%DB%8C-%D8%A7%D8%B2-%D8%B1%D9%88%D8%B2%DB%8C-%DA%A9%D9%87-%D9%87%DA%A9-%D8%B4%D8%AF%DB%8C%D8%AF