تحلیلی پیرامون حمله اخیر اینترنتی

۱۰ نکته‌ای که باید درباره فروپاشی اخیر اینترنت امریکا بدانید!

اخبار مختلفی در ارتباط حمله‌ای که چند روز پیش به وقوع پیوست و باعث شد دسترسی کاربران سراسر جهان به تعدادی از سایت‌های بزرگ و معروف همچون وایرد، گیت‌هاب و... با قطعی چند ساعته همراه شود، منتشر شده است. کار به جایی رسید که حتا تعدادی از کاربران ساکن در بخش شرقی ایالات متحده دیگر قادر نبودند به سایت‌های مورد نیاز خود مراجعه کنند. اما این حمله سیگنال مهمی را برای ما مخابره کرد و نشان داد یک حمله DDoS در کمترین حالت قادر است بخش‌های بزرگی از اینترنت را از مدار خارج کند.

بدون شک مکانیزم‌ها و سرویس‌هایی که امروزه مردم از آن استفاده می‌کنند، در مقایسه با سال‌های گذشته تغییرات شگرفی پیدا کرده است. ورود نسل‌های مختلفی از شبکه‌های ارتباطی همچون 3G، 4G، تا چند وقت دیگر 5G و دستگاه‌های اینترنت اشیا دستاوردهای بزرگی به همراه آورده و خواهند آورد. در حالی که جنبه‌های مثبت این فناوری‌ها کاملا مشهود است، اما در مقابل تهدیداتی که به واسطه این فناوری‌ها ما را به چالش می‌کشند جدی بوده و شوخی‌بردار نیست. حمله‌ای که چند روز پیش باعث شد سرویس‌دهی به کاربران جهان با اختلال همراه شود از این جهت حائز اهمیت است که تا پیش از این بسیاری از کارشناسان بر این باور بودند که زیرساخت‌های ارتباطی در ابعاد و مقیاس بزرگ در تیررس هکرها قرار ندارند و ما سطح قابل قبولی از امنیت را برای زیرساخت‌های خود به وجود آورده‌ایم.

مطلب پیشنهادی

حملات DDoS قربانی تازه‌ای گرفت
چرا دیروز بخشی بزرگی از امریکا اینترنت نداشت؟

در شرایطی که در نگاه اول این‌گونه به نظر می‌رسد که سامانه نام دامنه DNS مقصر اصلی این جریان است، اما واقعیت این است که DNS خود قربانی حمله‌ای بوده که از سوی دستگاه‌های تسخیر شده به سمت آن روانه شده است. مارک گافان، مدیر کل شرکت Imperva Incapsula در توصیف این حمله گفته است: «تصور کنید، ناگهان همه علائم خیابان شما به یکباره از میان بروند. هیچ‌کس نمی‌داند باید به کجا برود. زمانی که هدف یک حمله DDoS سازمان‌های مالی یا سایت‌های مربوط به بازی‌های آنلاین باشد، قربانیان سعی می‌کنند به برنامه‌های کاربردی خود دست پیدا کنند. در این حالت اطلاعات دست نخورده باقی مانده و افشا نمی‌شوند. فقط دسترسی به طور موقت امکان‌پذیر نیست. اما در ارتباط با Dyn این حمله درست زیرساخت مرکزی اینترنت را نشانه رفته بود. به طوری که سازمان‌هایی که برای فعالیت‌های تجاری خود به Dyn متکی بودند عملا تحت تاثیر این حمله قرار گرفتند. اکنون ما با چند پرسش چالش‌برانگیز روبرو هستیم.»

مطلب پیشنهادی

جهشی بزرگ برای آزادی اینترنت
پایان سیطره آمریکا بر کنترل اینترنت

1.تعدد سرویس‌های آنلاین خوب است اما به چه قیمتی؟

تنها در سه ماهه نخست سال جاری میلادی، چیزی در حدود 19 حمله منع سرویس انکار شده سرورهای سرویس‌دهنده اینترنتی را تحت‌الشعاع خود قرار داد. گزارش شرکت‌های امنیتی نشان می‌دهد که ترافیک این حملات بالغ بر 100 گیگابیت بر ثانیه بوده است. واقعیت این است که تنها تعداد بسیار محدودی از شرکت‌ها قادر هستند از سرورهای خود در برابر این‌گونه حملات محافظت به عمل آورند. شرکت‌های امنیتی هشدار داده‌اند، امروزه مجرمان سایبری از سرویس‌های خودکار و البته ارزان‌قیمتی همچون بوستر یا استرسر برای سازمان‌دهی حملات خود استفاده می‌کنند. این دو سرویس به منظور بررسی و تحلیل سرورها در برابر تهدیدات امنیتی مورد استفاده قرار می‌گیرد. آمارها نشان می‌دهند در 60 درصد حملات منع سرویس انکار شده، پروتکل‌های SSDP به میزان هفت درصد، DNS به میزان 18 درصد، NTP به میزان 12 درصد و CHARGEN به میزان 11 درصد نقش داشته‌اند. همچنین از هر چهار حمله گزارش شده در سال جاری یکی از آن‌ها از پروتکل UDP استفاده کرده است. بدون شک سازوکارهای امنیتی این پروتکل‌ها باید مورد بازبینی قرار بگیرد.

2.ردپایی از دوربینهای تحت وب در حمله به Dyn کشف شد

Dyn در ارتباط با حمله هفته گذشته اعلام داشته است: «طیف بسیار گسترده‌ای از آدرس‌های IP به منظور از کار انداختن سرویس‌های DNS این شرکت حمله منع سرویس انکار شده را به مرحله اجرا در آوردند. حداقل برای تعدادی از این دستگاه‌ها از سوی شرکت الکترونیکی Hangzhou Xiongmai فراخوان صادر شده است. شرکت فوق در زمینه تولید مولفه‌ها و بردهای الکترونیکی فعالیت دارد. بردهایی که در دستگاه‌های مختلفی منجمله دوربین‌های تحت وب مورد استفاده قرار می‌گیرند. بررسی‌ها نشان می‌دهند در این حمله وب‌کم‌ها نقش کلیدی را بازی کرده‌اند. تجهیزاتی که به بدافزار Mirai آلوده شده بودند، شبکه‌ای از بات‌نت‌ها را به وجود آورده بودند. این دستگاه‌ها همگی از گذرواژه‌های پیش‌فرض استفاده می‌کردند. همین موضوع باعث شده بود تا هکرها به راحتی به این دستگاه‌ها نفوذ کرده و آن‌ها را به منظور ساخت شبکه‌ای از بات‌نت‌ها به یکدیگر متصل کنند.»

با این وجود شرکت Xiongmai این موضوع را رد کرده و گفته است: «به نظر می‌رسد این حمله از جانب تجهیزات سخت‌افزاری بوده که از سوی تولیدکنندگان دستگاه‌های اینترنت اشیا تولید شده‌اند.» با این وجود شرکت Xiongmai فراخوانی به منظور جمع‌آوری همه وب‌کم‌هایی که از بردها و مولفه‌های مختلف این شرکت استفاده کرده‌اند، صادر

کرده است. فراخوان حجم قابل توجهی از دستگاه‌ها را شامل می‌شود. به سبب آن‌که Xiongmai با بسیاری از شرکت‌ها به منظور تامین تجهیزات مورد نیاز آن‌ها در ارتباط است.

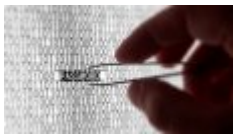
3. حمله به اصل دسترس‌پذیری داده‌ها

جاستین هاروی، مشاور امنیتی شرکت Gigamon که در زمینه نظارت بر ترافیک شبکه به فعالیت اشتغال دارد، گفته است: «در حالی که امروزه تمرکز اصلی دنیای امنیت تنها بر محرمانگی اطلاعات و پیشگیری از دسترسی افراد غیرمجاز به داده‌ها قرار دارد، حمله بزرگ نشان داد که دسترس‌پذیری به همان نسبت دو مولفه محرمانگی و یکپارچگی حائز اهمیت است و به نظر می‌رسد ما نسبت به این اصل کمی بی توجه بوده‌ایم.»

4. قربانی این حمله، سازمان‌هایی بودند که برای انجام یکسری از فعالیت‌های حیاتی تجاری خود به SaaS اعتماد کردند

حمله منع سرویس توزیع شده به Dyn باعث شد سرورهای DYN از مدار خارج شوند. اما این حمله فراتر از آن بود که تنها نام این شرکت را تحت الشعاع خود قرار دهد. این حمله باعث شد فعالیت‌های حیاتی و تجاری مهم سازمان‌های مربوطه مختل شود. سازمان‌هایی که به فناوری SaaS اعتماد می‌کنند هیچ گزینه دیگری در اختیار ندارند و در صورت بروز حمله فقط باید به انتظار بنشینند تا ارائه‌دهندگان سرویس در اولین فرصت سرویس را به وضعیت آنلاین خود باز گردانند. از دیدگاه ارائه‌دهندگان سرویس SaaS نه تنها گزینه‌های محدودی برای دفع این مدل حملات وجود دارد، بلکه احتمال بروز این مدل حملات در آینده نیز وجود دارد. اما این شرکت‌ها برای کاستن از شدت اثرگذاری این مدل حملات می‌توانند از ارائه‌دهندگان چندگانه DNS استفاده کنند.

مطلب پیشنهادی



در یکی از بزرگترین حراج اینترنتی صورت گرفت
فروش اطلاعات سرقتی 170 هزار سرور سایت در اینترنت

5. گذرواژه‌های پیش‌فرض دستگاه‌ها باید تعویض شوند

امروزه طیف بسیار گسترده‌ای از کاربران از گذرواژه‌ها و نام‌های کاربری پیش‌فرض دستگاه‌ها استفاده می‌کنند. به سبب آن‌که یادآوری آن‌ها ساده است. Xiongmai می‌گوید در این حمله دارندگان وب‌کم‌ها همگی از گذرواژه‌های پیش‌فرض استفاده کرده بودند. شرکت امنیتی ESET صبح امروز 25 اکتبر گزارش مطالعاتی خود را پیرامون وضعیت مصرف‌کنندگان ایالات متحده منتشر کرده که نشان می‌دهد، امروزه به کارگیری گذرواژه‌ها و مکانیزم‌های اعتبارسنجی پیش‌فرض برای بسیاری از مردم به یک امر عادی تبدیل شده و بسیاری از دارندگان این دستگاه‌ها سالیان سال است از گذرواژه‌های پیش‌فرض استفاده می‌کنند.

6. امنیت دستگاه‌های اینترنت اشیا به یک چالش جدی تبدیل شده است

امروزه دستگاه‌های اینترنت اشیا در هر مکان و خانه‌ای ممکن است حضور داشته باشند. این دستگاه‌ها که در اغلب موارد به ارتباطات اینترنتی مجهز هستند از سوی کاربرانی مورد استفاده قرار می‌گیرند که ممکن است به مسائل امنیتی توجه چندانی نداشته باشند. به طوری که تقریبا یک چهارم دستگاه‌هایی که امروزه در اختیار مصرف‌کنندگان قرار دارند، آماده بهره‌برداری و سوء استفاده هستند. با این وجود بیش از 40 درصد از دارندگان این دستگاه‌ها معتقد هستند که تجهیزات متصل به اینترنت همچون ترموستات‌ها و لوازم خانگی در ارتباط با حریم خصوصی و امنیت آن‌گونه که بایدوشاید ایمن نیستند.

مطلب پیشنهادی

کنترل اینترنت از دستان امریکا خارج و به دستان آیکان سپرده می‌شود
تغییر مدیریت اینترنت برای ما چه فایده‌ای دارد؟

7. مکانیزم‌های ارتباطی به بازنگری نیاز دارند

گزارش منتشر شده از سویESET نشان می‌دهد، 88 درصد دستگاه‌های اینترنت اشیا که داده‌هایی را تولید کرده و این داده‌ها را از طریق شبکه‌های بی‌سیم ارسال می‌کنند، به راحتی در تیرراس هکرها قرار دارند. آگاه و نگران بودن از بابت این دستگاه‌ها چاره کار نیست. این دستگاه‌ها باید به مکانیزم‌های پیشگیرانه یا واکنشی تجهیز شوند.

8. کم اطلاعی کاربران عامل اصلی بروز این چنین حملاتی است

در حالی که بیش از 50 درصد از شرکت‌کنندگان در نظرسنجی ESET اعلام کرده‌اند که از خرید دستگاه‌های اینترنت اشیا ناامید شده‌اند، با این وجود آمار خطرناک‌تری نیز وجود دارد. بیش از 14 درصد از شرکت‌کنندگان در این نظرسنجی هیچ‌گونه اطلاعی ندارند که چه دستگاه‌هایی به روترهای آن‌ها متصل شده‌اند و با آن‌ها در ارتباط هستند. بدتر آن‌که 30 درصد از این افراد حتا گذرواژه و مکانیزم‌های امنیتی روتر خود را از زمان خرید آن تا به امروز تغییر نداده‌اند و 20 درصد اصلا اطلاع ندارند چه زمانی اینکار را انجام داده‌اند.

مطلب پیشنهادی

پیوند اینترنت و لینوکس
آیا اینترنت بدون لینوکس زنده می‌ماند؟

9. فریم‌ورک‌های تاریخ گذشته

مکانیزم‌های اعتبارسنجی پیش‌فرض و میان‌افزارهای تاریخ گذشته دستگاه‌ها هر دو نقش مهمی در شکل‌گیری این حمله داشتند. این دو فاکتور تاثیرعمیقی بر قدرتمند شدن بات‌نت Mirai گذاشت. این حمله اکوسیستم اینترنت اشیا را به شکل معکوسی به شدت متحول کرد. به‌طوری که اکنون اعتماد بسیاری از مصرف‌کنندگان به این دستگاه‌ها متزلزل شده است.

10. سامانه نام دامنه مورد توجه هکرهای خاص

حقیقت مهم این است که DNS در اغلب موارد مورد توجه هکرهای عادی قرار ندارد. بسیاری از هکرهای عادی به دنبال آن هستند تا سرویس‌های رایج و عمدتا کاربران اینترنتی را مورد حمله قرار دهند. به دلیل این‌که حمله به سامانه نام دامنه به‌طور مستقیم سودی را عاید آن‌ها نمی‌سازد، فرآینده پیچیده‌ای بوده، زمان‌بر است، به طیف گسترده‌ای از تجهیزات هک شده نیاز دارد و در اغلب موارد به دانش فنی زیادی از هدف نیاز دارد. DNSها زمانی قربانی می‌شوند که هکرها تصمیم بگیرند دسترسی کاربران به سایت‌های خدمات گیرنده را غیر ممکن سازند. زمانی که حجم گسترده‌ای از درخواست‌ها به سمت سرورها ارسال شود، سرورها قادر به پاسخ‌گویی نخواهند بود و در نتیجه مرورگرها دیگر نمی‌دانند اطلاعات مربوطه به سایت‌ها را باید از چه منبعی دریافت کنند تا بتوانند به درخواست کاربر پاسخ دهند. بهترین راهکاری که برای مقابله با این حملات می‌توان از آن بهره برد، تکنیک اندازه‌گیری جریان داده‌ها است. در این تکنیک سامانه از بسته‌های داده‌ای نمونه‌برداری کرده و قادر به کشف الگوی ارسال درخواست‌ها خواهد بود. در نتیجه این توانایی را خواهد داشت تا درخواست‌های معتبر را از غیر معتبر تشخیص دهد. این همان تکنیکی است که DYN در ساعت‌های اولیه حمله از آن استفاده کرده بود.

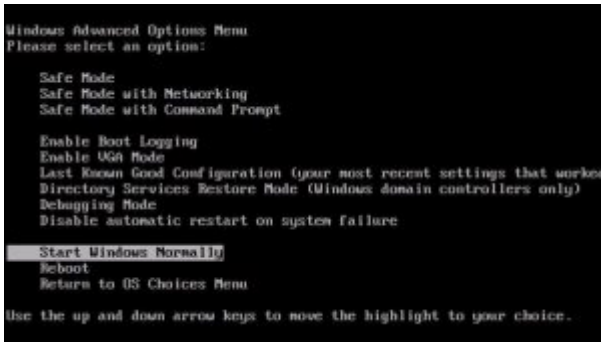
==========

شاید به این مقالات هم علاقمند باشید:

دانلود کنید: اپلیکیشن محاسبه و ارزیابی تعرفه اینترنت در ایران

ضدبدافزار بومی «پادویش» محافظت از کاربران ایرانی را آغاز کرد + لینک دانلود

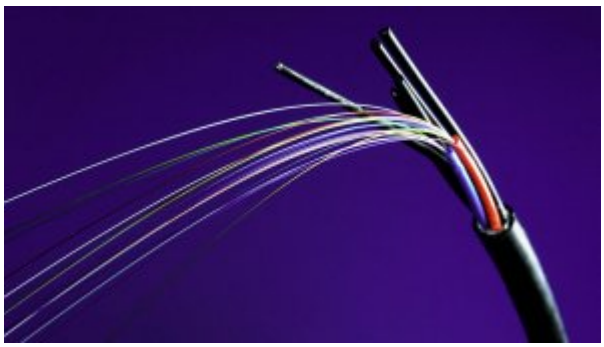
به اشتراک‌گذاری صندلی خودروها در ایران امکان‌پذیر شد



حالت امن ویندوز به هکرها اجازه نفوذ به ویندوز 10 را می‌دهد

گالری عکس: دوچرخه الکتریکی متصل به اینترنت با صفحه‌نمایش اندرویدی

5G در ایران مشکل کمبود فرکانس دارد



نوکیا رکورد اینترنت پر سرعت دنیا را شکست!

دسترسی ۹۸ درصدی انگلیسی‌ها به اینترنت ۲۴ مگابیت

تاریخ انتشار:

06 آبان 1395

نشانی منبع: https://www.shabakeh-mag.com/security/5216