اینترنت اشیاء

در حملات توزیع شده برای از کاراندازی سرویس

شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: اینترنت اشیاء، در حملات توزیع شده برای از کاراندازی سرویس

شناسه سند: SPT-A-0120-00

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

تاریخ تهیه: دی‌ماه ۱۳۹۵

در طی دهه گذشته، ضعف‌های امنیتی سیستم‌های عامل کامپیوتری به‌شدت مورد سوءاستفاده ویروس‌نویسان و نفوذگران قرار گرفتند و از جمله راه‌های انتشار بدافزار و اجرای حملات سایبری محسوب می شدند. اما با تلاش و هزینه فراوان سازندگان این سیستم‌های عامل و افزوده شدن برنامه‌ها و لایه‌های امنیتی، اکنون دیگر خبری از آن ضعف‌های فراوان و ناشیانه گذشته نیست. ناگفته پیداست نفوذگران به دنبال راه‌های ساده‌تر برای انجام کارهای خرابکارانه خود هستند.

چندین سال است که کارشناسان در خصوص امنیت ضعیف وسایل و تجهیزات متصل به اینترنت، موسوم به اینترنت اشیاء (IoT) هشدار داده‌اند.

امنیت ضعیف و پیکربندی آسیب‌پذیر این تجهیزات از یک سو و اتصال آنها به شبکه اینترنت از سویی دیگر، این تجهیزات را به هدفی بسیار مناسب و در عین حال آسان برای مهاجمان تبدیل کرده است.

یکی از اصلی‌ترین بهره‌جویی‌های تبهکاران سایبری از این وسایل و تجهیزات، تسخیر نمودن آنها برای اجرای حملات توزیع شده برای از کاراندازی سرویس (DDoS) است.

در جریان این حملات، لشکری از این تجهیزات هک شده با ارسال درخواست‌های همزمان به سرور قربانی آن را بمباران می‌کنند. دریافت همزمان درخواست، از هزاران و در برخی مواقع ده‌ها هزار دستگاه با نشانی‌های IP مختلف، در نهایت، منجر به کندی و یا حتی توقف خدمات‌دهی سرور به کاربران می‌شود.

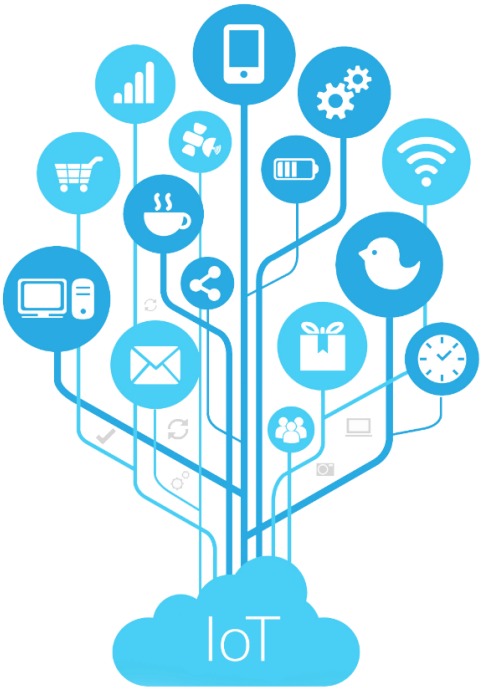
واقعیت آن است که دستگاه‌های متصل به اینترنت، صرفاً دستگاه هایی با منابع محدود نیستند. بلکه کامپیوترهایی هستند که اگر به طور صحیح پیکربندی و ایمن‌سازی نشوند، می‌توانند به ابزاری مخرب در دست نفوذگران تبدیل شوند.

در این مقاله، به روش‌های سوءاستفاده نفوذگران از اینترنت اشیاء به‌منظور اجرای حملات توزیع شده برای از کاراندازی سرویس و برخی بدافزارهای ویژه این بسترها پرداخته شده است.

تعاریف

اینترنت اشیاء[1]

اینترنت اشیاء به شبکه‌ای از دستگاه‌ها و تجهیزات گفته می‌شود که قادر به برقراری ارتباط و یا حتی تعامل با سایر دستگاه‌های موجود در شبکه داخلی و یا اینترنت هستند. اینترنت اشیاء طیف وسیعی از تجهیزات و وسایل پیشرفته امروزی را در بر می‌گیرد. برای مثال، دستگاهایی که از آنها با عنوان هوشمند یاد می‌شود – نظیر یخچال هوشمند – نمونه‌هایی از اینترنت اشیاء محسوب می‌شوند.



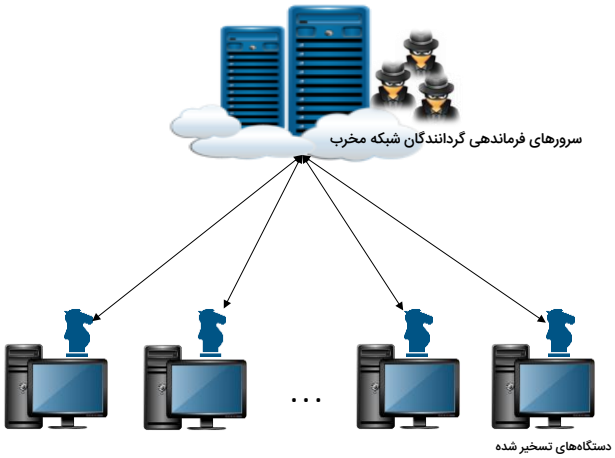
شکل ۱: نمونه‌ای از تجهیزات موسوم به اینترنت اشیاء

شبکه مخرب[2]

شبکه‌های مخرب که به Botnet مشهورند، از تعداد قابل توجهی از دستگاه کاربران عادی که به بدافزار خاصی آلوده شده‌اند و از طریق آن تحت کنترل گردانندگان شبکه مخرب قرار گرفته‌اند، تشکیل می‌شوند. به این دستگاه‌های تسخیر شده، Bot گفته می‌شود.

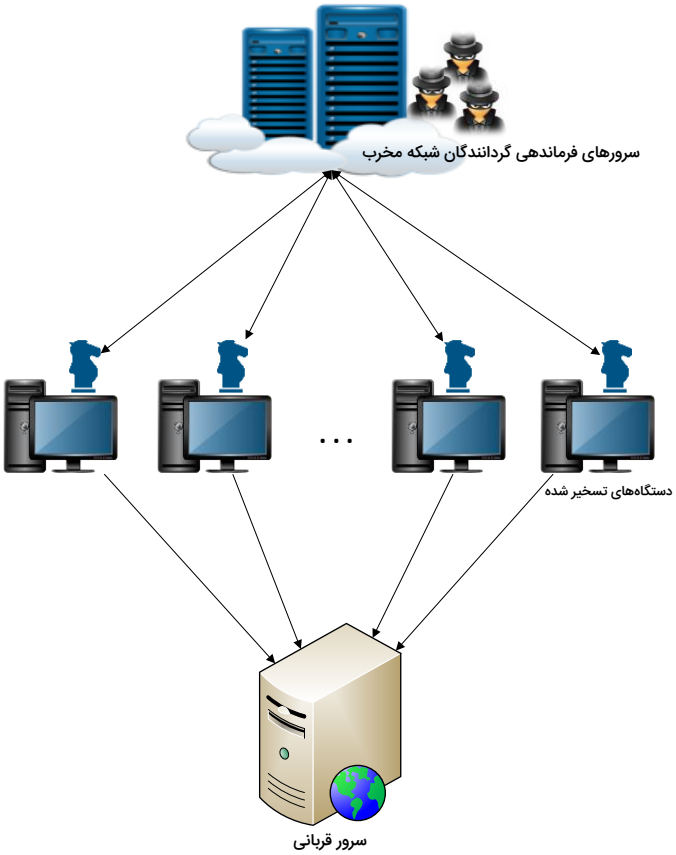
با افزایش تعداد دستگاه‌های تحت سیطره، گردانندگان شبکه مخرب قادر خواهند بود بدون شناسایی شدن و در حجم و وسعت زیاد، عملیات مخربی را به اجرا بگذارند.

میزان قدرت شبکه‌های مخرب به تعداد دستگاه‌های تسخیر شده بستگی دارد. تبهکاران سایبری، در بازارهای زیرزمینی خود، این شبکه‌ها را اجاره می‌دهند. متقاضی با پرداخت اجاره بها، تعدادی مشخص از دستگاه‌های تحت سیطره را برای مدتی معین به کنترل خود درآورده و از آنها برای اهداف مخرب خود سوءاستفاده می‌کند.



شکل ۲: ساختار شبکه مخرب

[1] Internet of Things (IoT)
[2] Botnet



شکل ۳: ساختار حمله توزیع شده برای از کاراندازی سرویس

حمله توزیع شده برای از کاراندازی سرویس[۳]

هدف از اجرای حمله توزیع شده برای از کاراندازی سرویس، همانطور که از نام آن پیداست، از کاراندازی سرویس‌دهنده هدف قرار گرفته شده است.

در این حملات، لشکری از دستگاه‌های تسخیرشده با ارسال درخواست‌های همزمان به سرور یا سایت قربانی آن را بمباران می‌کنند. دریافت همزمان درخواست، از هزاران و در برخی مواقع ده‌ها هزار دستگاه با نشانی‌های IP مختلف، در نهایت، منجر به کندی و یا حتی توقف خدمات‌دهی سرور یا سایت به کاربران می‌شود.

اجرای این حملات در مقایسه با سایر حملات سایبری بسیار آسان است. همچنین با توجه به اینکه اجرای حمله از نقاط مختلف جهان صورت می‌پذیرد مقابله با آنها کاری بسیار دشوار محسوب می‌شود. به‌نحوی که در برخی موارد، گردانندگان حمله از قربانی جهت متوقف نمودن حمله مبالغ بالایی را اخاذی می‌کنند.

اینترنت اشیاء و حملات توزیع شده برای از کاراندازی سرویس

تا چند سال پیش، شبکه‌های مخرب محدود به کامپیوترهای کاربران عادی بودند. گردانندگان این نوع شبکه‌های مخرب، معمولاً، از طریق هرزنامه‌ها[۴] و یا سایت‌های مخرب اقدام به آلوده نمودن کامپیوتر کاربران به بدافزار می‌کنند. این بدافزار معمولاً از نوع اسب تروا[۵] است.

اسب‌های تروا در ظاهر به‌عنوان یک برنامه سودمند بر روی کامپیوتر نصب شده و سپس اقدام به باز کردن یک درب مخفی[۶] و برقراری ارتباط با مرکز فرماندهی[۷] خود می‌کنند. به‌عبارتی دیگر باقی ماندن و حیات اسب تروا بر روی کامپیوتر قربانیان، رمز بقای این شبکه های مخرب است.

با افزایش تعداد کامپیوترهای تحت سیطره، گردانندگان شبکه مخرب قادر خواهند بود بدون شناسایی شدن و در حجم و وسعت زیاد، عملیات مخربی از جمله اجرای حملات توزیع شده برای از کاراندازی سرویس را به اجرا بگذارند.

اما در سال‌های اخیر، تبهکاران سایبری روش‌های جدیدی برای ایجاد شبکه‌های مخرب و اجرای حملات توزیع شده برای از کاراندازی سرویس ابداع کرده‌اند. یکی از این روش‌ها تسخیر دستگاه‌ها و تجهیزات موسوم به اینترنت اشیاء و تحت کنترل قرار دادن آنها برای اجرای چنین حملاتی است. بدیهی است لازمه این کار متصل بودن این دستگاه‌ها به شبکه اینترنت است.

---

[۳] Distributed Denial of Service (DDoS)
[۴] Spam
[۵] Trojan Horse
[۶] Backdoor
[۷] Command and Control (C&C)

در مهر ماه ۱۳۹۵ یکی از شرکت‌های امنیتی در گزارشی هشدار داد که روند هک شدن تجهیزات غیرامن در اینترنت اشیاء و سوءاستفاده از آنها برای اجرای حملات توزیع‌شده برای از کاراندازی سرویس در حال افزایش است. همچنین در این گزارش به استفاده مهاجمان سایبری از بدافزارهای چندبستری اشاره شده که قربانیان آنها دستگاه‌های با ثابت‌افزار[۸] مبتنی بر سیستم عامل Linux هستند.

بررسی‌های انجام شده نشان می‌دهد که اکثر این سیستم‌ها از طریق آسیب‌پذیری‌های مختص هر سخت‌افزار تسخیر نشده‌اند؛ بلکه اعمال نشدن حداقل تنظیمات امنیتی بر روی این دستگاه‌ها بوده که آنها را به یکی از اعضای شبکه مخرب تبدیل کرده است.

از جمله مواردی که به‌صورت بالقوه می‌توانند سبب تسخیر شدن این تجهیزات شوند عبارتند از:

- استفاده از نام کاربری و گذرواژه[۹] پیش‌فرض بر روی دستگاه که در نتیجه آن مهاجم با شناسایی دستگاه در شبکه اینترنت، از راه دور[۱۰] کنترل دستگاه را در دست می‌گیرد.
- بهره‌جویی[۱۱] از آن دسته از ضعف‌های امنیتی[۱۲] دستگاه که امکان اتصال یا اجرای کد را به‌صورت از راه دور فراهم می‌کند.
- پیکربندی نادرست دستگاه به‌نحوی که سوءاستفاده از دستگاه را ممکن کند.

متأسفانه سازندگان دستگاه‌ها و تجهیزات اینترنت اشیاء بندرت اقدام به عرضه اصلاحیه برای ترمیم ضعف‌های امنیتی دستگاه‌های ساخت خود بخصوص دستگاه‌های قدیمی‌تر می‌کنند. بسیاری از این دستگاه‌ها، هیچ مکانیزم امنیتی مناسبی در خود ندارند. کم نیستند سازندگانی که نه تنها استانداردهای امنیتی را طی مراحل برنامه‌نویسی در نظر نمی‌گیرند بلکه هیچ روالی نیز برای واکنش به رخدادها در زمان کشف ضعف‌های امنیتی در محصولاتشان ندارند. ضمن اینکه بخش قابل توجهی از این دستگاه‌ها فاقد قابلیت به روزرسانی خودکار[۱۳] هستند و این خود می‌تواند مشکل را دو چندان کند.

تمامی موارد مذکور در کنار این واقعیت که کاربران این نوع دستگاه‌ها معمولاً کاربران خانگی با دانش کم کامپیوتری هستند، سبب گسترش این شبکه‌های مخرب گردیده است.

SSDP، پودمان مورد علاقه گردانندگان شبکه‌های مخرب

در اواسط سال ۱۳۹۳، مشخص شد برخی گردانندگان شبکه مخرب از دستگاه‌هایی که پودمان SSDP[۱۴] بر روی آنها فعال است به‌منظور اجرای حملات توزیع شده برای از کاراندازی سرویس بهره‌جویی می‌کنند.

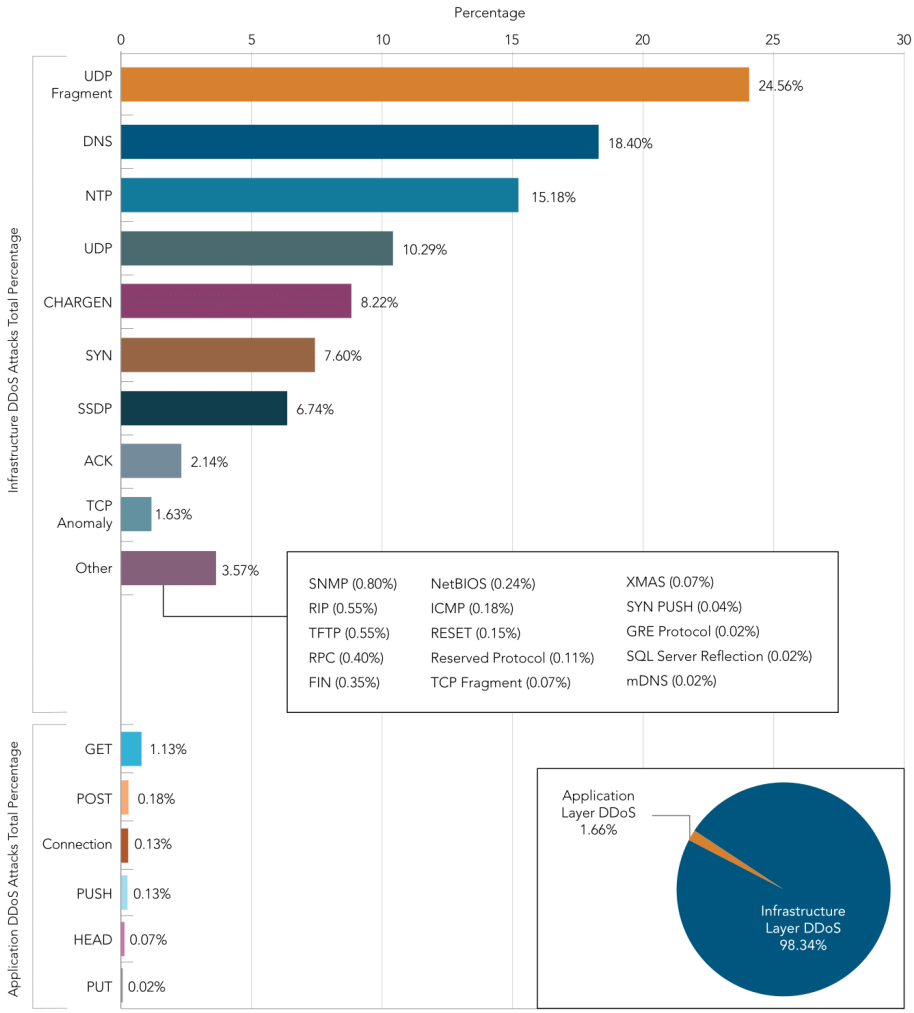
پودمان SSDP بخشی از UPnP[۱۵] است. UPnP مجموعه‌ای از پودمان‌های شبکه‌ای است که به دستگاه‌ها امکان می‌دهد یکدیگر را بدون نیاز به دخالت کاربر بیابند. اما مشکل اینجاست که تعداد زیادی از رهیاب‌ها[۱۶] و به‌طور کلی دستگاه‌های موسوم به اینترنت اشیاء به‌نحوی پیکربندی شده‌اند که به درخواست‌های SSDP پاسخ دهند. در صورت متصل بودن این تجهیزات به اینترنت، هر یک از آنها به‌صورت بالقوه می‌توانند به وسیله‌ای برای تقویت حملات توزیع شده برای از کاراندازی سرویس تبدیل شوند.

---

[8] Firmware
[9] Password
[10] Remote
[11] Exploit
[12] Vulnerability
[13] Automatic Update
[14] Simple Service Discovery Protocol
[15] Universal Plug and Play
[16] Router

با گذشت بیش از ۲ سال از زمان کشف این آسیب‌پذیری، سوءاستفاده از دستگاه‌های با پودمان SSDP همچنان یکی از روش‌های مورد استفاده برای اجرای حملات توزیع شده از کاراندازی سرویس است.

بر اساس آمار، در سه ماهه سوم سال ۲۰۱۶ میلادی، ۶/۷۴ درصد حملات توزیع شده برای کاراندازی سرویس با بهره‌جویی از این پودمان صورت گرفته است.



شکل ۴: سهم هر یک از روش‌های اجرای حمله توزیع شده برای از کاراندازی سرویس در سه ماهه سوم ۲۰۱۶ | منبع: Akamai Technologies

حملات توزیع شده برای از کاراندازی سرویس از طریق پودمان SSDP به SSDP Reflection Attack with Amplification معروف هستند که خود زیرمجموعه‌ای از حملات برگشت‌خورده[۱۷] محسوب می‌شوند.

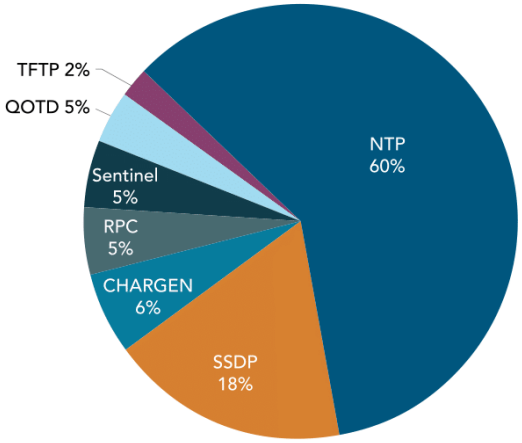
در حملات برگشت‌خورده، نفوذگر با ارسال بسته‌های درخواستی که در آنها نشانی IP فرستنده، یک نشانی جعلی است، سبب می‌شود که پاسخ دستگاه گیرنده به نشانی جعلی که در واقع نشانی دستگاه قربانی است ارسال شود. بسته‌های درخواست دارای حجم بسیار

[۱۷] Reflected

کمی هستند ولی بسته‌های پاسخ حجیم‌تر هستند. لذا نفوذگران به‌طور غیرمستقیم باعث شدت بخشیدن هجوم ترافیک به سوی دستگاه قربانی می‌شوند.

از سرورهای DNS و NTP آسیب‌پذیر در سال‌های اخیر به کرات برای حملات برگشت‌خورده استفاده شده است. با وجودی که ضریب تقویت حملات از طریق پودمان SSDP در مقایسه با پودمان‌های DNS و NTP کمتر است، اما امتیاز بزرگی برای نفوذگران دارد و آن هم وجود میلیون‌های دستگاه آسیب‌پذیر در سراسر دنیاست.

بر طبق آمار در سه ماهه سوم سال ۲۰۱۶، ۱۸ درصد حملات برگشت خورده از طریق سوءاستفاده از پودمان SSDP انجام شده‌اند.



شکل ۵: سهم SSDP در حملات برگشت‌خورده توزیع شده برای از کاراندازی سرویس در سه ماهه سوم ۲۰۱۶ | منبع: Akamai Technologies

همچنین بر اساس آمار، در حال حاضر حدود ۱۸ میلیون دستگاه متصل به اینترنت وجود دارد که درگاه SSDP آنها باز و فعال است. شکل ٦ گستره این دستگاه‌ها را در منطقه خاورمیانه نمایش می‌دهد.

شکل ۶: گستره دستگاه‌های متصل به اینترنت با SSDP باز و فعال در منطقه خاورمیانه | منبع: Shadowserver Foundation

دوربین‌های مداربسته نمونه‌ای از قربانیان

در آبان ۱۳۹۴، شرکت Incapsula اعلام کرد که بر اساس بررسی‌های انجام شده توسط این شرکت، نفوذگران از شبکه‌ای مخرب، متشکل از ۹۰۰ دوربین مدار بسته[۱۸] که در کشورهای مختلف پراکنده‌اند، به‌منظور اجرای حملات توزیع‌شده برای از کاراندازی سرویس بر ضد سایت های اینترنتی استفاده می‌کنند.

سامانه‌های مدیریتی این دوربین‌ها به سبب دارا بودن گذرواژه‌های پیش‌فرض یا ضعیف و پذیرفتن تمامی درخواست‌های اینترنتی آسیب‌پذیر اعلام شدند. همچنین تمامی این دستگاه‌ها از برنامه‌ای با نام BusyBox استفاده می‌کردند. BusyBox نرم‌افزاری است که مجموعه‌ای از ابزارهای Unix را در قالب یک فایل اجرایی ارائه می‌کند. این فایل ویژه دستگاه‌های با سیستم‌های عامل نهفته با منابع محدود طراحی شده است.

گردانندگان این شبکه مخرب از بدافزاری استفاده می‌کردند که با پویش شبکه، دستگاه‌های BusyBox که درگاه Telnet/SSH آنها باز بود را شناسایی کرده و به روش سعی‌وخطا[۱۹] می‌کوشید تا به آنها متصل شده و آنها را تحت سیطره شبکه مخرب در آورد.

این نفوذگران با فرستادن فرامینی به دستگاه‌های تسخیر شده سبب ارسال بسته‌های درخواست به سایت قربانی می‌شدند. بررسی‌های شرکت Incapsula نشان می‌داد در اوج حملات این شبکه مخرب، در هر ثانیه، ۲۰ هزار درخواست به سایت قربانی ارسال می‌شده است.

در تیر ماه ۱۳۹۵ نیز شرکت Sucuri از سوءاستفاده مهاجمان از بیش از ۲۵ هزار دوربین مدار بسته و دستگاه ضبط تصویر دیجیتال[۲۰] به‌منظور ایجاد شبکه‌ای مخرب از آنها و اجرای حمله توزیع شده برای از کاراندازی سرویس بر ضد سایت یکی از مشتریانش خبر داد.

در اوج این حمله، حدود ۵۰ هزار درخواست بر ثانیه به سایت ارسال می‌شد. چنین حملاتی می‌توانند براحتی یک سایت کوچک را که توان خدمات‌دهی به این تعداد درخواست را ندارد از کار بیندازند.

به گفته محققان Sucuri، ترافیک از سمت دستگاه‌های مدار بسته و به‌خصوص دستگاه‌های ضبط تصویر دیجیتال ارسال می شده است.

مشخص نسیت که دست درازی به این دوربین‌های مدار بسته چطور انجام شده بود.

پیش از آن یک محقق امنیتی وجود یک ضعف امنیتی اجرای از راه دور کد را در دستگاه‌های ضبط تصویر دیجیتال ساخت بیش از ۷۰ شرکت گزارش کرده بود. در اواخر سال ۱۳۹٤ نیز محققان Risk Based Security اعلام کردند که نزدیک به ٤٦٦ هزار دستگاه ضبط تصویر دیجیتال ساخت سازندگان مختلف از گذرواژه تزریق شده در کد یکسانی استفاده می‌کنند.

راهکار اصلی برای جلوگیری از سوءاستفاده مهاجمان از دوربین‌های مدار بسته برای اجرای حملات توزیع شده برای از کاراندازی سرویس عدم اتصال مستقیم آنها به اینترنت است. ضمن اینکه در صورتی که دسترسی به دستگاه‌ها بر روی بستر اینترنت ضروری باشد می‌توان از ارتباطات VPN برای این منظور بهره برد.

---

[۱۸] Closed Circuit Television Camera (CCTV Camera)

[۱۹] Brute Force

[۲۰] Digital Video Recorder

شبکه مخرب Mirai

Mirai بدافزاری است که با نفوذ به دستگاه با سیستم عامل Linux، آن را به عضوی از شبکه مخرب تبدیل می‌کند. دستگاه‌های قربانی این بدافزار عمدتاً رهیاب‌های خانگی و دوربین‌های اینترنتی[۳۱] با گذرواژه‌های ضعیف و تنظیمات آسیب‌پذیر هستند.

در مهر ماه، کد منبع[۳۲] این بدافزار به‌صورت کد باز[۳۳] توسط کاربری با نام مستعار Anni-senpai، بر روی سایت hackforums.com به اشتراک گذاشته شد. در زمان انتشار کد، این کاربر ادعا می‌کرد بدافزار Mirai موفق به آلوده کردن ۳۸۰ هزار دستگاه شده است. با در دسترس قرار گرفتن کد منبع این بدافزار انتظار می‌رود از روش‌های مورد استفاده این بدافزار در بدافزارهای دیگر نیز استفاده شود.

در ۲۳ مهر ماه ۱۳۹۵، وزارت امنیت داخلی آمریکا[۳۴]، با انتشار توصیه نامه‌ای در خصوص خطر اجرای حملات شبکه مخرب Miraii هشدار داد.

شبکه مخرب Mirai در برخی از بزرگترین و مخرب‌ترین حملات توزیع شده برای از کاراندازی سرویس نقش داشته است.

در یکی از جدیدترین نمونه‌ها، در مهر ۱۳۹۵، یک شرکت فرانسوی ارائه‌دهنده خدمات میزبانی سرور بر روی بستر ابری[۳۵] به نام OVH از اجرای دو حمله توزیع‌شده برای از کاراندازی سرویس که در مجموع ۱۱ ترابیت بر ثانیه توان داشتند بر ضد برخی سرورهایی که بر روی بستر این شرکت میزبانی می‌شدند خبر داد. منبع این حملات ۱۴۵،۶۰۷ دستگاه هک‌شده ضبط تصویر دیجیتال و دوربین تحت شبکه عضو شبکه Mirai اعلام شد. با در نظر گرفتن توان ایجاد ترافیک از ۱ تا ۳۰ مگابیت بر ثانیه توسط هر یک از این دستگاه‌های این شبکه مخرب، گردانندگان آن عملاً قادر بودند که حملات توزیع شده از کاراندازی سرویس با توان ۱/۵ ترابیت بر ثانیه اجرا کنند.

پیش از این حمله نیز krebsonsecurity.com که سایتی متعلق به یک روزنامه‌نگار امنیت سایبری با نام Brian Krebs است هدف حمله توزیع شده برای از کاراندازی سرویس شبکه مخرب Mirai با توان ۶۲۰ گیگابیت بر ثانیه قرار گرفته بود. شدت این حمله آنقدر زیاد بود که شرکت Akamai Technologies که خدمات حفاظت از این سایت را ارائه می‌کرد ناچار شد برای متوقف نشدن خدمات به سایر مشتریان، این سایت را در حالت محافظت نشده رها کند. توان این حمله نزدیک به دو برابر پر قدرت‌ترین حملاتی بوده که Akamai Technologies تا آن زمان ثبت کرده بود. Brian Krebs در نهایت سایت را با حفاظت Google Project Shield مجدداً برخط کرد.

در نمونه‌ای دیگر در جریان حمله‌ای مشابه، سرورهای DNS شرکت Dyn هدف قرار گرفتند که در نتیجه آن، سرویس‌دهی سایت شرکت‌های بزرگی نظیر Twitter، Pinterest و PayPal دچار اختلال شد. در اول آبان ۱۳۹۵، شرکت Dyn، در بیانیه‌ای اعلام کرد که هدف حمله‌ای پیچیده توسط میلیون‌ها دستگاه‌های اینترنت اشیاء تحت سیطره شبکه مخرب Mirai قرار گرفته بود.

در پی آن، شرکت چینی Hangzhou XiongMai که دستگاه‌های آن به‌صورت گسترده‌ای توسط مهاجمان این حملات مورد بهره‌جویی قرار گرفته بودند اعلام کرد که برخی از تجهیزاتش را که در آمریکا به فروش رسانده فراخوانی خواهد کرد. همچنین گفت که برای بعضی از محصولاتش نیز اصلاحیه‌های امنیتی عرضه خواهد کرد. اما مشکل اساسی اینجاست که از اجزای آسیب‌پذیر این شرکت در محصولات ساخت شرکت‌های ثالث نیز استفاده شده و در همه آنها از ترکیب نام کاربری و گذرواژه root : xc3511 استفاده شده است.

بر اساس بررسی‌های انجام شده توسط شرکت ESET، 15درصد رهیاب‌های خانگی با گذرواژه ضعیف حفاظت می‌شوند. ضمن اینکه پودمان Telnet بر روی ۲۰ درصد این دستگاه‌ها باز است.

---

[۳۱] IP Camera
[۳۲] Source Code
[۳۳] Open Source
[۳۴] United States Department of Homeland Security
[۳۵] Cloud

شبکه مخرب Hajime

در ۲۵ مهر ماه ۱۳۹۵، محققان شرکت Rapidity Networks گزارشی را منتشر کردند که در آن به بدافزار پیشرفته جدیدی پرداخته شده بود. انتشار این گزارش اندکی پس از به اشتراک گذاری کد منبع Mirai صورت گرفت. با توجه به اینکه Mirai کلمه‌ای ژاپنی به معنای "آینده" بود این محققان بدافزار جدید را Hajime – به زبان ژاپنی به معنای "آغاز" – نامگذاری کردند.

علیرغم وجود برخی شباهت‌ها، محققان کاشف Hajime بر این باورند که ساختار این دو بدافزار متفاوت و مجزا از یکدیگر است.

Hajime بر روی دستگاهی که خود به این بدافزار آلوده شده اقدام به پویش نشانی‌های تصادفی IP بر روی شبکه می‌کند. در صورت شناسایی دستگاهی با نشانی IP پویش شده بدافزار تلاش می‌کند که با اجرای حمله‌ای از نوع سعی‌وخطا و از طریق نام‌های کاربری و گذرواژه‌های تزریق شده در کد از طریق درگاه ۲۳ که مربوط به پودمان Telnet است به آن متصل شود.

در صورت موفقیت در برقراری ارتباط، بدافزار بررسی می‌کند که سیستم عامل دستگاه هدف قرار گرفته شده Linux باشد. Hajime قابلیت اجرا شدن بر روی بسترهای زیر را داراست:

- ARMv5
- ARMv7
- Intel x86-64
- MIPS, little-endian

در صورتی که سیستم عامل دستگاه قربانی Linux تشخیص داده شود فایلی که هدف آن ایجاد درگاه ارتباطی با سرور فرماندهی بدافزار است بر روی دستگاه اجرا می‌شود. در ادامه فایل مخرب اجرا شده بر روی دستگاه از سیستم DHT[۲۶] برای برقراری ارتباط نقطه‌به‌نقطه[۲۷] در شبکه مخرب استفاده کرده و فایل‌ها و قابلیت‌های جدید را از طریق پودمان µTP دانلود می‌کند. DHT و µTP[۲۸] هر دو از پودمان های اشتراک‌گذاری BitTorrent هستند.

بر اساس بانک اطلاعات اصالت‌سنجی موجود در کد Hajime مشخص است که دستگاه‌های رهیاب، دوربین‌های مداربسته و ضبط دیجیتال از اهداف اصلی آن هستند.

رعایت موارد زیر آسان‌ترین راه برای حفاظت از دستگاه‌های موسوم به اینترنت اشیاء است:

- گذرواژه‌های پیش‌فرض دستگاه به گذرواژه‌های پیچیده تغییر داده شده‌اند. نام‌های کاربری و گذرواژه‌های پیش‌فرض براحتی دستگاه را به تسخیر شبکه‌های مخرب در می‌آورند.
- دستگاه‌های اینترنت اشیاء به آخرین نسخه به‌روز شوند.
- پودمان‌های Telnet و SSH و همچنین پودمان‌های مرتبط با UPnP بر روی این دستگاه‌ها غیرفعال شود؛ مگر آنکه واقعاً به آن نیاز باشد.
- از دستگاه های مصتل به اینترنت توسط دیواره های آتش کارآمد حفاظت شود.
- دستگاه‌های متصل به اینترنت حتی الامکان از شرکت‌های خوشنام خریداری شود.

[۲۶] Distributed Hash Table
[۲۷] Peer-to-Peer (P2P)
[۲۸] Micro Transport Protocol

منابع

- http://newsroom.shabakeh.net
- http://www.shabakeh.net/tv/sgc/what-is-botnet
- http://businessinsights.bitdefender.com/iot-ddos-attacks-scada-incidents
- http://hub.dyn.com/static/hub.dyn.com/dyn-blog/dyn-statement-on-10-21-2016-ddos-attack.html
- http://www.csoonline.com/article/3034284/security/hard-coded-password-exposes-up-to-46000-video-surveillance-dvrs-to-hacking.html
- http://www.gartner.com/it-glossary/internet-of-things
- http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks
- https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective
- https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html
- https://content.akamai.com/PG7659-q3-2016-state-of-the-internet-connectivity-report.html
- https://krebsonsecurity.com/2016/10/iot-device-maker-vows-product-recall-legal-action-against-western-accusers
- https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/iot-devices-ddos-attack
- https://securingtomorrow.mcafee.com/mcafee-labs/top-5-things-know-recent-iot-attacks
- https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf
- https://ssdpscan.shadowserver.org
- https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html
- https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks
- https://www.us-cert.gov/ncas/alerts/TA16-288A

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولید کننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management – UTM) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه‌اندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

CSQ
ISO 9001:2008
Cert No 9150.C528

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار	۴۲۰۵۲-۰۲۱
تارنمای شرکت	www.shabakeh.net
سامانه پشتیبانی	help.shabakeh.net
خدمات پس از فروش	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net