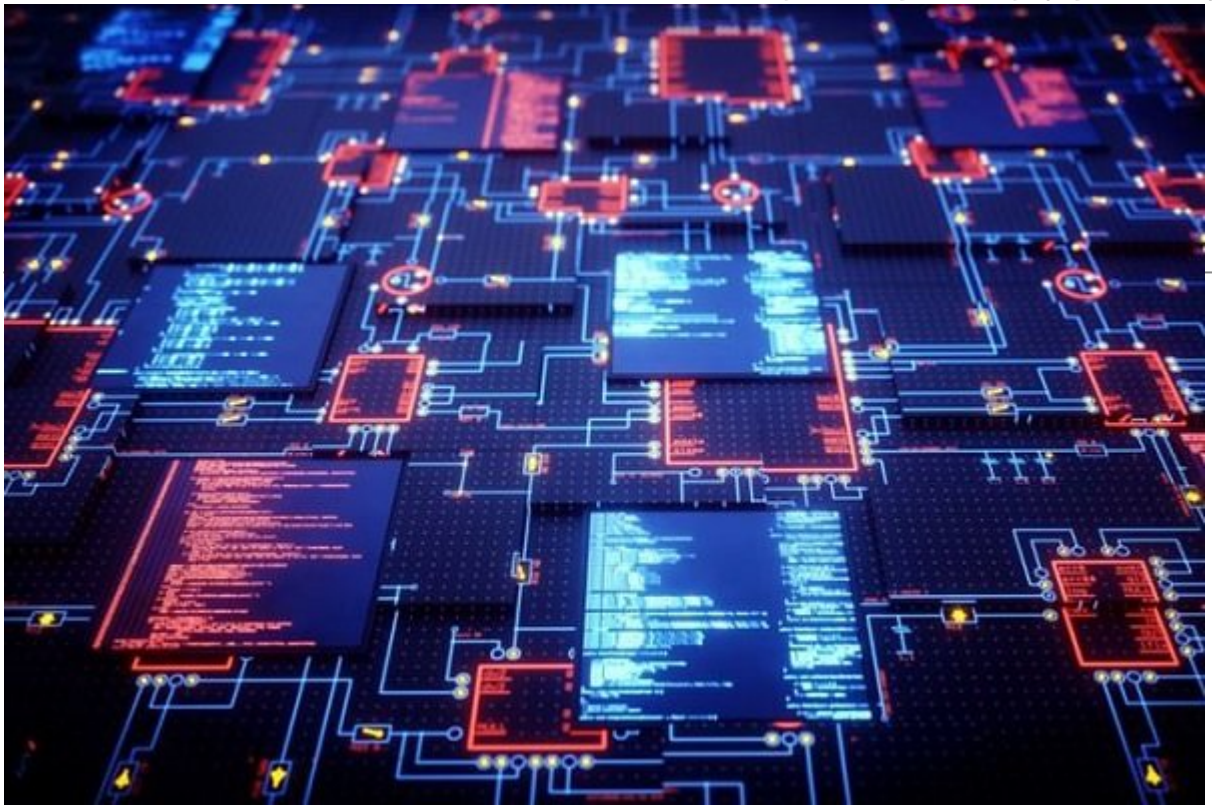
لشکری از دستگاه‌های زامبی

بات نت چیست و چرا بالقوه خطرناک است



در دنیای امنیت کامپیوتری دو واژه خطرناک وجود دارد که تعامل مستقیمی با یکدیگر دارند. حمله‌های منع سرویس توزیع‌شده و بات‌نت‌ها دو اصطلاحی هستند که در ترکیب با یکدیگر هر زیرساختی را با چالش جدی روبه‌رو می‌کنند. در این میان، بات‌نت‌ها عملکردی به‌مراتب فراتر از یک تخریب ساده دارند. بات‌نت‌ها می‌توانند زمینه‌ساز انتشار اخباری جعلی و غیرواقعی شوند. درحالی‌که یک حمله منع سرویس توزیع‌شده به‌خودی‌خود خطرناک بوده و ما در شماره‌های گذشته به‌تفصیل درباره آن سخن گفته‌ایم، اما واقعیت دیگری در بطن این حمله قرار دارد. یک حمله منع سرویس توزیع‌شده زمانی به شکل درست و دقیقی به مرحله اجرا درمی‌آید که طیف گسترده‌ای از کامپیوترهایی که در کنترل هکرها قرار دارند، در آن واحد به یک هدف حمله کنند. کامپیوترهایی که به‌واسطه رخنه‌های نرم‌افزاری یا باز بودن پورت‌ها به‌گونه‌ای هک شده‌اند که مالک دستگاه از این موضوع اطلاع نداشته است. در این حالت هکر می‌تواند شبکه‌ای از کامپیوترهای زامبی را تحت کنترل خود قرار داده و انواع مختلفی از عملیات مجرمانه را انجام دهد. شبکه‌ای که در اصطلاح رایج به آن بات‌نت گفته می‌شود.

بات‌نت چیست؟

بات‌نت (BotNet) مخفف دو واژه Robot و Net(work) است. در اصطلاح فوق واژه Robot به بدافزارهایی اشاره دارد که از سوی هکرها ایجادشده و هکرها با اتکا بر این بدافزارها می‌توانند دسترسی‌های سطح بالای مدیریتی را روی کامپیوتر قربانی یا حتی سرورها به دست آورند. بدافزارهایی که ممکن است همانند کرم‌ها قابلیت خودتکثیری داشته باشند. این قابلیت خودتکثیری که از طریق اسکریپت‌ها یا روبات‌ها انجام می‌شود، در عمل به هکر اجازه می‌دهد وقت خود را بیهوده صرف هک کردن طیف گسترده‌ای از تجهیزات الکترونیکی نکرده و در یک‌چشم برهم زدن ده‌ها هزار دستگاه را آلوده کند. اما هکرها برای آن‌که بتوانند دستگاه‌های آسیب‌پذیر درون شبکه‌ها را پیدا کنند، در بیشتر موارد از موتوری موسوم به Shodan استفاده می‌کنند. این موتور قادر است در تمام طول شبانه‌روز دستگاه‌های آسیب‌پذیر متصل به شبکه را که در کشورهای مختلف مورداستفاده قرار می‌گیرند، پیدا کند. در اغلب موارد هکرها به میان‌افزارهای نصب‌شده روی روترها، گجت‌های اینترنت اشیا یا حتی گوشی‌های هوشمند حمله می‌کنند. زمانی‌که این حمله با موفقیت انجام پذیرد، شبکه‌ای از کامپیوترهای آلوده به وجود می‌آید که به بدافزار نصب‌شده روی کامپیوترهای آلوده اجازه می‌دهد با سرور در ارتباط باشند. این سرور از راه دور نقش یک مرکز کنترل و فرمان‌دهی را بازی کرده و دستورهای لازم را برای حمله به یک هدف برای کامپیوترها ارسال می‌کند.

بات‌نت‌ها چطور کار کرده و به یک سامانه کامپیوتری حمله می‌کنند؟

پس از آن‌که طیف گسترده‌ای از سامانه‌های کامپیوتری و گجت‌های هوشمند هک شدند، بدافزارها به سرورها متصل می‌شوند. در این مرحله افرادی که به آن‌ها هکرهای فرمانده گفته‌شده و برخی منابع با اصطلاح BotManager از آن‌ها نام می‌برند، کنترل کار را به دست می‌گیرند. هکرهای فرمانده این قابلیت را در اختیار دارند تا دستورالعمل‌های صادرشده را برای کامپیوترهای آلوده به شیوه رمزگذاری شده ارسال کنند. این کار باعث می‌شود تا نرم‌افزارهای ضدویروس در عمل قادر نباشند کار چندان خاصی را انجام دهند. در این میان هکرهای فرمانده از ماهیتی به نام

BotMaster استفاده می‌کنند. **بات‌مسترها** اطلاعات مدنظر هکر را جمع‌آوری کرده و در ادامه نقشی که **بات‌نت‌ها** در حمله‌ها ایفا می‌کنند، در قالب فرمان‌ها و دستورهایی برای کامپیوترهای قربانی ارسال می‌کنند. با توجه به این‌که **بات‌نت‌ها** در بیشتر مواقع آنلاین هستند، در نتیجه در هر لحظه آماده دریافت دستورها و حمله به اهداف مشخص‌شده هستند. زمانی‌که فرمان حمله‌ای صادر می‌شود، کامپیوترهای آلوده شروع به ارسال حجم بسیار بالایی از درخواست‌ها به سمت آدرس‌هایی می‌کنند که از طریق سرور کنترل و فرمان‌دهی مشخص‌شده است. در چنین حالتی با توجه به تمهیدات امنیتی و زیرساخت‌های یک سازمان ممکن است فرایند سرویس‌دهی برای چند ساعت یا چند روز مختل شود.

مطلب پیشنهادی

محافظت از داده‌های مالی و نام تجاری
چگونه می‌توانیم از شبکه، سرورها و نقاط پایانی کسب‌وکارمان در برابر هکرها محافظت کنیم؟

بات‌نت‌ها انواع مختلفی دارند

در سری مقاله‌های حمله منع سرویس توزیع‌شده در شماره‌های گذشته به این موضوع اشاره کردیم که این حمله الگوها و روش‌های مختلفی دارد. این موضوع در ارتباط با **بات‌نت‌ها** نیز صدق می‌کند. درحالی‌که **بات‌نت‌ها** همه دستورهای خود را به شکل کدگذاری شده و پنهان از سوی سرور کنترل و فرمانی دریافت می‌کنند، اما بر مبنای پروتکلی که از آن استفاده می‌کنند، در حالت کلی به سه گروه متمرکز، غیرمتمرکز و ترکیبی تقسیم می‌شوند.

1.بات‌نت‌های متمرکز

در این مدل، **بات‌نت**‌های متمرکز مادامی‌که با **بات‌مستر** در ارتباط باشند، قادر به انجام عملیات مخرب هستند. در نتیجه، هر زمان اتصال میان **بات‌نت‌ها** و **بات‌مسترها** از کار بیفتد، شبکه به‌طورکلی غیرفعال خواهد شد. اما بات‌نت‌های متمرکز خود به مدل‌های مختلفی تقسیم می‌شوند که از آن جمله به موارد زیر می‌توان اشاره کرد.

بات‌های C&C

این مدل **بات‌نت‌ها** بر مبنای یک زیرساخت کنترل و فرمان‌دهی کار می‌کنند. در این مدل **بات‌مستر** وظیفه ارسال دستورها و کنترل **بات‌نت‌ها** را بر عهده می‌گیرد.

بات‌نت‌های IRC

این مدل از **بات‌نت‌ها** از پروتکل IRC (سرنام Internet Relay Chat) استفاده می‌کنند. در این روش **بات‌نت‌ها** به کانال‌های IRC متصل شده و در انتظار دریافت فرمان‌ها به شکل بلادرنگ هستند. این روش نسبت به مدل C&C مزایای مختلفی به همراه دارد که از آن جمله به موارد زیر می‌توان اشاره کرد:

• با توجه به این‌که کامپیوترهای آلوده از پروتکل IRC استفاده می‌کنند، در نتیجه این قابلیت را در اختیار هکر قرار می‌دهند تا کامپیوترهای آلوده را به چند کانال متصل کنند. اتصالی که به نام Multicasting از آن نام برده می‌شود. مزیت رویکرد فوق در مدیریت سریع بات‌نت‌ها از طریق بات‌مستر است.

• در این روش **بات‌مسترها** از طریق به‌کارگیری کانال‌های ارتباطی متفاوت می‌توانند **بات‌نت‌ها** را کنترل کنند. در نتیجه، در صورت بسته بودن یک کانال امکان سوییچ کردن به کانال‌های دیگر وجود دارد و هکرها بدون وجود هیچ‌گونه تاخیری به‌سرعت می‌توانند دستورها را برای کامپیوترهای زامبی ارسال کنند.

درحالی‌که این روش مزایایی برای هکرها به ارمغان می‌آورد، اما در مقابل با محدودیت‌هایی نیز روبه‌رو است. یکی از مهم‌ترین معایب این روش در شناسایی سریع بدافزارها است. به این نکته دقت کنید که پروتکل IRC در عمل استفاده چندانی برای همه سرورها ندارد، در نتیجه امکان شناسایی و همچنین قطع ارتباط بدون مشکل خاصی امکان‌پذیر است.

بات‌نت مبتنی بر پروتکل انتقال ابرمتن

این روش که به شکل گسترده‌ای از سوی هکرها مورد استفاده قرار می‌گیرد، به آن‌ها اجازه می‌دهد تا دستورهای مدنظر خود را از طریق پروتکل HTTP برای **بات‌نت‌ها** ارسال کنند. در این روش دستورهای مخرب و اهداف مشخص‌شده در قالب یک فایل متنی از طریق آدرس‌های http سرورها برای کامپیوترهای آلوده ارسال می‌شود. در ادامه بدافزارهای نصب‌شده روی کامپیوتر قربانی فایل متنی را خوانده و دستورهای آن را یک‌به‌یک اجرا می‌کنند.

2. بات‌نت‌های غیرمتمرکز

همان‌گونه که در چند پاراگراف بالاتر به آن اشاره کردیم، **بات‌نت**‌های متمرکز معایب مختلفی دارند. برای برطرف کردن این معایب بات‌نت‌های غیرمتمرکز به وجود آمدند. در این روش هکرها به‌جای آن‌که از یک بات‌مستر استفاده

کنند، در عمل از چند بات‌مستر و پروتکل‌های مختلف برای این منظور استفاده می‌کنند. همین موضوع باعث می‌شود تا کارشناسان امنیتی در زمینه شناسایی و قطع کامل ارتباط کامپیوترهای آلوده با **بات‌مستر**ها با مشکلاتی عدیده‌ای روبه‌رو شوند.

3. بات‌نت‌های ترکیبی

در این الگو، هم از مدل کنترل و فرمان‌دهی و هم از نوع غیرمتمرکز به‌منظور برقراری ارتباط با یک کامپیوتر آلوده استفاده می‌شود. البته توجه داشته باشید، **بات‌نت**‌های ترکیبی عملکردی پیچیده داشته و بر مبنای یک مدل ترکیبی و تصادفی کار می‌کنند. در نتیجه دستورالعمل‌ها و پارامترهایی که برای هر کامپیوتر آلوده در شبکه ارسال می‌شود، متفاوت از دیگری است. همچنین از یک الگوی تصادفی به‌منظور برقراری ارتباط با بات‌مستر استفاده می‌شود. در این مکانیزم تمامی بات‌نت‌ها در قالب شبکه‌ای مبتنی بر روبات‌های (P2P) به شکل ترکیبی حضور دارند. جالب آن‌که خود این روبات‌ها نیز به دو گروه سرویس‌دهنده و سرویس‌گیرنده تقسیم می‌شوند.

کارشناسان امنیتی در خصوص شیوع روزافزون بات‌نت‌ها ابراز نگرانی کرده‌اند

تقریبا یک سال پیش بود که حمله باج‌افزار واناکرای باعث مختل شدن فعالیت بسیاری از شرکت‌ها در سراسر جهان شد. اکنون پس از گذشت یک سال از آن حادثه و بررسی ابعاد دقیق‌تر آن حمله، کارشناسان امنیتی اعلام داشته‌اند: «این امکان وجود دارد تا شبکه‌ای از کامپیوترهای هک شده را که در قالب **بات‌نت**‌ها به زیرساخت‌های یک سازمان حمله می‌کنند، شناسایی کرده و حمله آن‌ها را دفع کنند. اما امکان بررسی این موضوع که آیا این کامپیوترها دو مرتبه به وضعیت قبلی خود باز می‌گردند یا خیر وجود ندارد. همچنین این امکان وجود ندارد تا متوجه شویم چه افرادی در پس‌زمینه ساخت شبکه‌ای از **بات‌نت**‌ها قرار داشته‌اند. این شبکه‌ها که از راه دور کنترل می‌شوند، در برخی مواقع از حمایت‌های دولتی نیز برخوردار هستند و به‌منظور سرقت داده‌ها، جاسوسی‌های صنعتی، اختلال در سرویس‌دهی ارتباطات و در کل از دسترس خارج کردن فناوری‌های روزمره زندگی مردم مورد استفاده قرار می‌گیرند. **بات‌نت**‌ها این پتانسیل را دارند تا شبکه‌هایی را که کامپیوترها به آن‌ها متصل هستند و از نرم‌افزارهای آسیب‌پذیر یا از گذرواژه‌های پیش‌فرض ساده استفاده می‌کنند، پویش کرده و در ادامه به شکل خودکار به بهره‌برداری از رخنه‌ها پرداخته یا با اتکا بر تکنیک‌های مهندسی ـ اجتماعی ایمیل‌هایی را به صندوق پستی کاربران ارسال کرده و مکانیزم‌های امنیتی سامانه‌ها را درهم‌شکسته و سامانه‌های بیشتری را قربانی کنند. پس از ساخت شبکه‌ای از بات‌نت‌ها، هکرها به‌طورمعمول یکی از سه استراتژی زیر را پیاده‌سازی می‌کنند: در اولین سناریو اطلاعات شخصی، مالی و حتی محرمانه را به سرقت می‌برند؛ در دومین سناریو اطلاعات اشتباه را به درون شبکه‌های اجتماعی تزریق می‌کنند. در سومین سناریو از طریق ساخت ترافیک مصنوعی مانع از آن می‌شوند تا مشتریان یک شرکت بتوانند از سرویس‌های آنلاین به شکل مطلوبی استفاده کنند.»

مطلب پیشنهادی

دفاع در برابر حمله منع سرویس انکار شده
راهکارهایی برای شناسایی و دفع حمله منع سرویس توزیع شده (DDoS)

چه عواملی باعث شده بات‌نت‌ها تا به این اندازه خطرناک شوند؟

در مقطع فعلی **بات‌نت**‌ها یکی از مؤثرترین ابزارهایی هستند که برای انتشار نرم‌افزارهای مخرب یا کرم‌های اینترنتی

در اختیار هکرها قرار دارند. حملات واناکرا و نات‌پتیا نشان دادند، **بات‌نت**‌ها می‌توانند تا چه اندازه قدرتمند ظاهر شوند. **بات‌نت**‌ها ضمن آن‌که با سرعت بالایی در شبکه‌ها کار می‌کنند، این توانایی را نیز دارند تا موقعیت مکانی هکرها و به‌ویژه سرورهای کنترل و فرماندهی را در میان هزاران کامپیوتر شخصی آنلاین پنهان کنند. در مقاله «کارشناسان امنیتی چگونه از وب تاریک برای شناسایی آسیب‌پذیری‌ها استفاده می‌کنند» اشاره شد که در دنیای زیرزمینی وب تاریک بازارچه‌های مختلفی برای انجام کارها وجود دارد. یکی از کارهای انجام‌شده در وب تاریک به فروش رساندن آسیب‌پذیری‌ها یا اجاره دادن بات‌نت‌های ساخته‌شده از سوی هکرها است. بات‌نت‌ها در اغلب موارد به قیمت‌های خوبی اجاره داده می‌شوند. نزدیک به 16 سال پیش **بات‌نتی** به نام Coreflood از سوی هکرها ساخته شد.

این **بات‌نت** در ابتدا، در قالب یک ابزار برای **حمله‌های منع سرویس توزیع‌شده** (a Tool For Distributed Denial of Service DDoS) اجاره داده شد، اما پس از مدت کوتاهی هکرها تغییرهایی در **بات‌نت** یاد شده به وجود آورند و تصمیم گرفتند از هزاران آدرس آی‌پی متعلق به سامانه‌های کامپیوتری در سراسر جهان به‌منظور انجام سایر فعالیت‌های غیرقانونی به شکل ناشناس استفاده کنند. شش سال بعد بات‌نت Coreflood دومرتبه مورد باز طراحی قرار گرفت تا این مرتبه به بانک‌ها و موسسات مالی حمله کرده و اطلاعات کارت‌های اعتباری و جزئیات مربوط به حساب‌های کاربران را به سرقت ببرد.

خرابکاری، ارسال اطلاعات اشتباه و نفوذ به زیرساخت‌های حساس و مالی

گسترش‌پذیری و سرعت بالای **بات‌نت**‌ها بر کسی پوشیده نیست. همین موضوع باعث شده تا **بات‌نت**‌ها به بهترین ابزار جاسوسی تبدیل شوند. در نتیجه، بسیاری از سازمان‌ها و حتی کشورها از بات‌نت‌ها به‌منظور به سرقت بردن اسرار محرمانه طرف مقابل و همچنین انجام یک حمله سایبری استفاده می‌کنند. بات‌نت GamerOver Zeus یکی از معروف‌ترین بات‌نت‌هایی است که در این زمینه ساخته شد و با هدف دسترسی به اطلاعات کاربران خاص به کار گرفته شد. این **بات‌نت** شبکه‌ای بسیار عظیم از سامانه‌های کامپیوتری (یک میلیون سامانه) آلوده را به وجود آورد. شبکه‌ای که با هدف حمله به حساب‌های بانکی و دسترسی به اطلاعات حساسی که روی سامانه‌های کامپیوتری ذخیره‌سازی شده بود، به کار گرفته می‌شد. در نهایت، بات‌نت یاد شده از طریق یک تلاش چندجانبه در سال 2014 شناسایی و نابود شد. **بات‌نت**‌ها با هدف دیگری نیز مورد استفاده قرار می‌گیرند. از کار انداختن سرویس‌های اینترنتی یکی از این اهداف است. در سال 2007 میلادی زیرساخت‌های دولتی کشور استونی، هدف یک حمله منع سرویس انکار شده قرار گرفت. **بات‌نت** میرایی نمونه خطرناک دیگری بود که در سال 2016 به سامانه نام دامنه (DNS) شرکت داین حمله کرد و باعث شد اینترنت بخش شرقی ایالات‌متحده برای چند ساعت قطع شود. اما همان‌گونه که پیش‌تر اشاره کردیم، بات‌نت‌ها به‌منظور انتشار اطلاعات اشتباه نیز مورد استفاده قرار می‌گیرند. نزدیک به دو سال پیش کارشناسان حوزه رسانه و کارشناسان امنیتی نسبت به انتشار اخبار کذب در شبکه‌های اجتماعی ابراز نگرانی کردند. در ابتدا مدیران ارشد شبکه‌های اجتماعی نسبت به این موضوع واکنش نشان دادند و اعلام کردند، انتشار اخبار جعلی در مقیاس بسیار جزئی بوده، اما گذشت زمان نشان داد تنها در شبکه اجتماعی توییتر بیش از 36 هزار بات به شکل خودکار چیزی حدود 288 میلیون توییت جعلی هدفمند را در سال 2016 منتشر کرده است. «تاد روزنبلوم»، یکی از کارشناسان امنیتی در این ارتباط گفته است: «**بات‌نت**‌ها تهدیدی جدی برای امنیت عمومی و دیجیتالی هر کشوری هستند. آن‌ها در نقش یک شتاب‌دهنده قادر هستند به انتشار اخبار جعلی سرعت بخشیده و اخباری را که مطابق با میل جریان‌های خاصی است، پخش کنند. فراموش نکنید، **بات‌نت**‌ها امروزه به یک تجارت بزرگ آن هم در مقیاس بین‌المللی تبدیل شده‌اند. بات‌ها با ضریب نفوذ بالا در فضای مجازی قادر هستند از هشتک‌های یکسان به‌منظور پنهان‌سازی منشأ شیوع خود استفاده کنند. زمانی که هکرها اطمینان حاصل کنند، موقعیت جغرافیایی آن‌ها قابل‌شناسایی نبوده و وضعیت بات‌ها به تثبیت رسیده، در ادامه به سراغ انتشار و تبلیغ اخبار جعلی می‌روند. در این میان کاربران به شکل ناخواسته با بازنشر مطلب آن را تقویت کرده و اخبار جعلی را گسترش می‌دهند. پیاده‌سازی شبکه‌ای از بات‌ها هزینه‌بر نیست، در نتیجه بهترین ابزاری است که برای انتشار اخبار جعلی هدفمند از سوی سازمان‌های خاص مورد استفاده قرار می‌گیرند. در اغلب موارد کاربران عادی تصور می‌کنند، بات یک شهروند عادی است، درحالی‌که بات ابزاری بدون هویت بوده که از سوی هکرها به کار گرفته‌شده است.»

مطلب پیشنهادی

آشنایی با مفاهیم امنیتی
۱۰ مفهوم امنیتی وب که بهتر است هر کاربری بداند

بات‌ها چگونه شناسایی و نابود می‌شوند؟

فرایند فنی شناسایی و از کار انداختن بات‌ها در اصطلاح رایج به نام Skinholing معروف است. در این فرایند کارشناسان امنیتی به ضعیف‌ترین نقطه از یک بات سنتی، یعنی ساختار کنترل متمرکز حمله می‌کنند. ساختار کنترل متمرکز، سرورهایی هستند که وظیفه ارسال دستورهای مخرب را برای کامپیوترهای آلوده برعهده دارند. در اولین گام کارشناسان امنیتی سعی می‌کنند کنترل یک یا چند نام دامنه را که از سوی سرور کنترل مورد استفاده قرار می‌گیرد، به دست گرفته و در ادامه بات‌ها را به سمت سروری که تحت نظارت کارشناسان امنیتی قرار دارد، هدایت کنند. این مرحله Skinhole نام دارد. در این مرحله حفره‌ای ایجاد می‌شود تا دستورها از سوی **بات‌مستر** به سمت کامپیوترهای آلوده ارسال نشود. در ادامه کارشناسان امنیتی به ردیابی کامپیوترهایی می‌پردازند که درون شبکه **بات‌نت** قرار داشته و با سرور مخرب در ارتباط بوده‌اند. در این مرحله آدرس‌های آی‌پی روبات‌هایی که در سراسر جهان به کار گرفته شده‌اند، ثبت و موقعیت جغرافیایی آن‌ها شناسایی می‌شود و به این شکل یک تخمین نسبتا دقیق از اندازه شبکه بات‌نت به دست می‌آید. در این مرحله کاربران به شکل مستقیم یا از طریق ارائه‌دهندگان سرویس‌های اینترنتی در جریان قرار می‌گیرند که جزئی از شبکه **بات‌نت** بوده‌اند تا در ادامه بتوانند تمهیدات لازم را اجرا کنند. درحالی‌که تکنیک Skinholing قادر است در کار **بات‌نت**‌ها اختلالی به وجود آورد، اما فراموش نکنید که بات‌مسترها به‌راحتی می‌توانند یک سرور کنترل و فرمان‌دهی دیگر را ایجاد کرده و همه تلاش‌های انجام شده در این زمینه را بی‌اثر کنند. مشکل موجود دیگر در این زمینه به هماهنگی‌ها در سطح بین‌المللی بازمی‌گردد که فرایند شناسایی به‌موقع را با دشواری روبه‌رو می‌کند. بر همین اساس، کارشناسان امنیتی پیشنهاد داده‌اند تا فرایند تشخیص بات‌ها به شکل آنلاین و خودکار انجام شود. به عبارت دقیق‌تر، ابزارهای امنیتی به مکانیزم‌های هوشمند تجهیز شوند تا در کنار عامل انسانی بتوانند به‌خوبی بات‌ها را شناسایی کنند.

منبع:

researchgate
botnerds
thecipherbrief
wired
getmoreabout

تاریخ انتشار:
01 دی 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/14244/%D8%A8%D8%A7%D8%AA-%D9%86%D8%AA-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D8%B1%D8%A7-%D8%A8%D8%A7%D9%84%D9%82%D9%88%D9%87-

%D8%AE%D8%B7%D8%B1%D9%86%D8%A7%DA%A9-%D8%A7%D8%B3%D8%AA