مروری بر بات‌نت‌ها روی تلفن‌های هوشمند همراه و راه‌کارهای مقابله

الهام عابد[1] و رضا ابراهیمی آتانی[2]

[1] دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه گیلان، گیلان، ایران
elham.abed@gmail.com

[2] استادیار گروه مهندسی کامپیوتر، دانشگاه گیلان، گیلان، ایران
rebrahimi@guilan.ac.ir

چکیده

مفهوم بسیاری از حملات و آسیب‌های امنیتی در حال تغییر از شبکه‌های رایانه‌ای به سمت گوشی‌های هوشمند است و ما روزانه شاهد ظهور گستره وسیعی از بدافزارها بر روی انواع پلتفرم‌های گوشی‌های هوشمند هستیم. پژوهش‌گران معتقد هستند یکی از این حملات بات‌نت‌هاست که به‌تازگی بر روی گوشی‌های هوشمند مشاهده می‌شود. واژه تلفن همراه بات‌نت اشاره به گروهی از گوشی‌های هوشمند تحت نفوذ دارد که از راه دور توسط مدیر بات از طریق کانال فرمان و کنترل برای انجام فعالیت مخربانه کنترل می‌شود. از مهم‌ترین اجزای یک بات‌نت، وجود زیرساختی به نام کانال فرمان و کنترل است که مدیر بات فرمان‌های خود را از طریق این کانال به بات‌ها ارسال کرده و آن‌ها پاسخ خواهند داد. در طراحی یک موبایل بات‌نت باید سه جنبه روش انتشار، توپولوژی و کانال فرمان و کنترل مورد بررسی قرار گیرد. در این مقاله به بررسی طرح‌های جدید ارائه‌شدهٔ بات‌نت‌های تلفن همراه از سه جنبهٔ بیان‌شده پرداخته و در انتها روش‌هایی برای پیش‌گیری، تشخیص و مقابله از تلفن همراه بات‌نت ارائه شده است.

واژگان کلیدی: تلفن همراه هوشمند، بات‌نت، بدافزار، کانال فرمان و کنترل.

۱- مقدّمه

با افزایش نرخ رشد گوشی‌های هوشمند و قرارگرفتن اطلاعات محرمانه مانند شماره کارت بانکی، نام کاربری و رمز عبور برای عملیات بانکی برخط و غیره در گوشی‌های هوشمند، این وسیله به‌عنوان هدف حملهٔ جدید مهاجمان تبدیل شده است. مهاجمان حملاتی مانند حملات منع سرویس، ارسال انبوه پیام کوتاه و رایانامه و دزدیدن اطلاعات شخصی را انجام می‌دهند. طبق آمار منتشرشده در لابراتوار کسپراسکای در سال ۲۰۱۵، ایران پنجمین کشور از نظر تعداد کاربران آلوده به بدافزارهای تلفن همراه در جهان است [۱] .طبق آمار منتشرشده در سال ۲۰۱۴ در سایت F-secure از هر پنج تهدید بدافزاری روی تلفن همراه یکی از آن‌ها مربوط به تهدید بات‌نت‌هاست[۲].

بات‌نت‌ها یکی از بزرگ‌ترین تهدیدات برای دنیای اینترنت و رایانه‌ها محسوب می‌شوند؛ ولی تلفن همراه بات‌نت‌ها هنوز به بزرگ‌ترین تهدید در دنیای تلفن همراه‌ها تبدیل نشده‌اند؛ ولی حملات بر روی شبکه‌های سلولی و تجهیزات موبایل از نظر تعداد و پیچیدگی رو به افزایش است و در مقایسه با بات‌نت‌های قدیمی ارتقای تلفن همراه بات‌نت در مراحل اولیه خود به سر می‌برد و پژوهش‌های محدودی بر روی آن صورت گرفته است. واژه تلفن همراه بات‌نت اشاره بر گروهی از گوشی‌های هوشمند تحت نفوذ دارد که از راه دور توسط مدیر بات از طریق کانال فرمان و کنترل برای انجام فعالیت مخربانه کنترل می‌شود. مدیر بات فرمان‌های خود را از طریق کانال فرمان و کنترل[1] به بات‌ها ارسال کرده و از طریق این کانال از آن‌ها پاسخ خواهد گرفت[۲].

تفاوت‌های زیادی بین گوشی‌های هوشمند و رایانه‌ها هست که این تفاوت‌ها منجر به چالش‌های زیادی در طراحی تلفن همراه بات‌نت شده است. ازجملهٔ این تفاوت‌ها به موارد زیر می‌توان اشاره کرد:

[1] Command & Control

- توان باتری گوشی‌های هوشمند بسیار کمتر از رایانه‌هاست.
- قبض گوشی‌های هوشمند یک موضوع مهم برای کاربران است.
- ترافیک بیش از اندازهٔ کانال فرمان و کنترل توجه کاربر را به خود جلب می‌کند.
- نبود یک نشانی IP عمومی و تغییرات محدود در اتصالات شبکه باعث می‌شود کانال مستحکم فرمان و کنترل نظیر به نظیر بر روی گوشی‌های هوشمند غیرکاربردی و عملی باشد.

هم‌چنین در کنار چالش‌های بیان‌شده، سیستم‌عامل‌های مختلفی برای تلفن همراه ازجمله سیمبیان، اندروید، آیفون، بلک‌بری و ویندوز وجود دارد که در میان آن‌ها اندروید محبوب‌ترین هدف حمله برای مهاجمان است؛ زیرا این سیستم‌عامل متن‌باز است. در سه ماهه نخست سال ۲۰۱۴ از ۲۷۷ نمونه جدید بدافزارهای کشف شده، ۲۷۵ مورد آن بر روی سیستم عامل اندروید بود [**Error! Bookmark not defined.**].

۲- مروری بر تاریخچهٔ بدافزارها

بعد از ظهور نخستین کرم تلفن همراه،Cabir، در سال ۲۰۰۴ شاهد یک انقلاب بزرگ در بدافزارهای تلفن همراه بودیم. این بدافزار فعالیت‌های اولیه ازجمله آلوده‌کردن فایل‌ها، جایگزین‌کردن فایل‌های مخرب به‌جای فایل و برنامه‌های سیستمی، ارسال پیام کوتاه و پیام چندرسانه‌ای اشاره کرد. این کرم بر روی سیستم‌عامل سیمبیان کار می‌کرد و از طریق بلوتوث می‌توانست به دیگر دستگاه‌ها منتقل و گسترش یابد [۳] هرچند که تعداد خانواده بدافزارهای موبایل و انواع آن‌ها به‌طور پیوسته رو به افزایش بود؛ ولی عملکرد آن‌ها یکسان بود؛ تا زمانی که نخستین تلفن همراه باتنت در سال ۲۰۰۹ ظهور کرد. تروجان SymbOS.Exy.A در فوریه ۲۰۰۹ کشف شد و نوع دیگر آن به نام SymbOS.Exy.C در جولای ۲۰۰۹ دوباره ظاهر شد. این تروجان با دیگر بدافزارهای موبایل تفاوت داشت و الگوی رفتاری شبیه به یک بات از خود نشان می‌داد؛ زیرا بعد از آلوده‌سازی دستگاه‌ها به سرورهای HTTP بدخواهانه متصل و اطلاعات دستگاه و کاربر را به آن سرورها گزارش می‌داد [۴].

در اواخر همان سال کرم IkeeB در نوامبر ظهور کرد که هدف آن گوشی‌های آیفون بود و شبیه به SymbOS.Exy رفتار می‌کرد. این کرم از طریق سرورهای HTTP کنترل و کامپوننت اضافی‌تری را دانلود و اطلاعات کاربر را به سرورها ارسال می‌کرد [۵]. در دسامبر ۲۰۰۸ نخستین موبایل باتنت اندروید به نام Geinimi در چین ظهور کرد و از کانال فرمان و کنترل HTTP استفاده می‌کرد. با این اتصال از راه دور مهاجمان قادر بودند تا به‌طور دوره‌ای دستورهای خود را منتشر و از دستگاه‌های آلوده‌شده برای شروع یک حمله در مقیاس بزرگ استفاده کنند [۶]. با درنظرگرفتن این پتانسیل، باتنت‌ها به‌زودی تبدیل به یک تهدید برای کاربران گوشی‌های هوشمند خواهند شد.

۳- اجزای یک باتنت

برای اطلاع از عملکرد بهتر باتنت به بررسی برخی از اجزای کلیدی می‌پردازیم [۲]:

بات: یک بات، برنامه نرم‌افزاری (بدافزاری) است که بر روی میزبان‌های آسیب‌پذیری که قادر به فعالیت‌های مخربانه است، نصب می‌شود.

باتنت: باتنت‌ها مجموعه‌ای از بات‌ها هستند که به کانال کنترل و فرمان متصل شده و منتظر دریافت دستورها برای اجرای فعالیت‌های مخربانه می‌باشند.

مدیربات: مدیر بات کاربر مخربی است که کنترل بات‌ها را با اعمال و انتقال دستورها به بات‌ها، برای انجام فعالیت‌های مخربانه به دست می‌گیرد.

کانال فرمان و کنترل: یکی از مهم‌ترین اجزای باتنت‌ها وجود زیرساخت فرمان و کنترل است که شامل بات‌ها و واحدهای کنترل‌کننده بات است. به‌طورمعمول زیرساخت فرمان و کنترل تنها راه ارتباط بین بات‌ها و مدیر بات است.

۴- حملات موبایل باتنت‌ها

حملات موبایل باتنت‌ها به‌طور کلی شامل موارد زیر می‌شود [۷]:

دستور کلی	جزئیات
انتقال فایل	رونوشت فایل از دستگاه به کامپیوتر، رونوشت فایل از رایانه به دستگاه، حذف یک فایل از دستگاه
انتقال پیامک	نمایش تمامی پیام‌های دستگاه، نمایش صندوق پیام به‌صورت انحصاری، نمایش صندوق ارسال به‌صورت مجزا،

انتقال پیامک	نمایش گفتگوهای متنی، ارسال پیامک از دستگاه، اضافه کردن یک پیام در دستگاه، جستجو در میان پیامک‌های دستگاه، حذف یک پیام مشخص از دستگاه، پشتیبان‌گیری از پیامک‌ها،
مدیریت تماس	شنود تماس‌های برقرارشده، بازیابی تماس‌های انجام‌گرفته، ایجاد تماس از دستگاه،
مدیریت فهرست مخاطبان	فهرست کردن مخاطبان دستگاه، اضافه‌کردن یک مخاطب، ارسال پیامک، برقراری تماس با مخاطب، جستجوی مخاطبان با استفاده از نام یا شماره تلفن، پشتیبان‌گیری از فهرست مخاطبان،
شنود پنهانی از راه دور	شنود زنده از میکروفن دستگاه، ضبط صدا از میکروفن دستگاه،
تاریخچه مرورگر	نمایش تاریخچه، نمایش صفحات موردعلاقه کاربر، جستجو در بین صفحات وب بازشده توسط کاربر
موقعیت‌یاب مکانی	دریافت آخرین موقعیت مکانی دستگاه و نمایش آن بر روی نقشه گوگل
مدیریت برنامه کاربردی	دریافت اطلاعات برنامه‌های کاربردی در حال اجرا در پس‌زمینه دستگاه، دریافت اطلاعات تمام برنامه‌های کاربردی نصب‌شده بر روی دستگاه، اجرای یک برنامه کاربردی بر روی دستگاه
جزئیات اطلاعات	دریافت شماره IMEI دستگاه، دریافتWiFi Mac Address، بررسی زمان root شدن دستگاه

۵- طراحی بات‌نت

جهت ارائه طرح برای بات‌نت‌های موبایلی باید سه جزء و قسمت اصلی بررسی شود [۸]:

۱) طریقه انتشار کد بات‌نت به گوشی‌های هوشمند

۲) کانال فرمان و کنترل برای انتشار دستورها

۳) توپولوژی برای سازمان‌دهی بات‌نت‌ها

انتشار کد: انتشار کدهای مخرب به گوشی‌های هوشمند به دو گروه انتشار از طریق درگیرکردن کاربر و استخراج آسیب‌پذیری‌ها تقسیم می‌شود. نخستین شیوه که معروف‌ترین راه آن مهندسی اجتماعی است، توسط بات‌نت‌ها بیشتر مورد استفاده قرار می‌گیرد. به‌عنوان مثال فرد مهاجم یک پیام کوتاه شامل پیوند بدخواهانه یا یک بات تغییر چهره یافته‌ای را به‌عنوان یک برنامه جذاب در فروشگاه‌های بارگیری نرم‌افزارهای تلفن همراه منتشر می‌کند و افراد با دریافت آن برنامه کدهای مخرب را بر روی دستگاه تلفن همراه خود قرار می‌دهند. در اندروید معمول‌ترین راه، بارگذاری بات در فروشگاه مربوط به برنامه‌ها یا تجمیع آن‌ها در بسته‌های سفارشی شدهٔ سیستم عامل است. درواقع بیشتر پژوهش‌گران بات‌نت تلفن همراه، بر روی شیوهٔ انتشار بات‌ها تمرکز نمی‌کنند؛ زیرا مهندسی اجتماعی هنوز به‌عنوان مشهورترین، معمول‌ترین و مؤثرترین راه برای انتشار بات‌ها از نظر هزینه و کارایی به‌حساب می‌آید [۹].

کانال فرمان و کنترل: برخلاف تروجان‌ها و ویروس‌ها، یک ویژگی خاص بات‌نت‌ها وجود کانال فرمان و کنترل است که مسئول انتقال دستورها و فرمان‌ها از مدیر بات به بات‌های تحت کنترل است و این دو را مانند یک پل به یکدیگر متصل می‌سازد. مدیر بات به‌طورمعمول از پروتکل‌ها برای برقراری ارتباط با بات‌ها استفاده می‌کند؛ به‌عنوان‌مثال پروتکل‌های معمول در بات‌نت‌های قدیمی IRC و HTTP بود. گوشی‌های هوشمند پروتکل‌های مخصوص به خود را دارند که پروتکل‌های رایانه‌ها بر روی آن‌ها قابل اجرا نیست. یکی از معمول‌ترین پروتکل‌ها، پیام کوتاه است؛ زیرا بر روی تمامی اپراتورها و کاربران قابل‌اجراست. یکی دیگر از پروتکل‌های مشهور که توسط مهاجمان استفاده می‌شود، HTTP است که کنترلی شبیه به بات‌نت‌های قدیمی را ارائه می‌دهد و می‌تواند از تمامی منابع موجود در اینترنت برای بات‌نت‌ها استفاده کند [۹].

توپولوژی: ساختار شبکه را که شامل مدیر بات، سرورهای فرمان و کنترل و بات‌هاست، را توپولوژی تعریف می‌کنند. توپولوژی به چهار دسته می‌توان تقسیم کرد. به‌طور کامل متمرکز، به‌طور کامل نامتمرکز، ساختار ترکیبی و ساختار تصادفی. معمول‌ترین نوع ساختار، ساختار متمرکز است که هر بات تنها با یک سرور فرمان و کنترل ارتباط برقرار می‌کند [۹]. در این مقاله مروری به بررسی سناریوهای طراحی موبایل بات‌نت‌ها، نوآوری‌ها و بیان نقاط ضعف هر یک می‌پردازیم.

۵-۱- موبایل بات‌نت بر پایه بلوتوث

در این مقاله [۱۰] Singh و گروهش در سال ۲۰۱۰ به بررسی چالش‌های ساخت و نگه‌داری موبایل بات‌نت براساس ارتباطات کوتاه‌برد مانند بلوتوث پرداختند. از طریق شبیه‌سازی

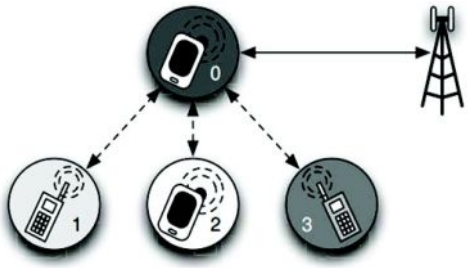
انجام‌شده در مقیاس گسترده و بررسی مقدار پوشش آلودگی بلوتوث، بیان‌شده که این زیرساخت مخربانه با توجه به ویژگی «تکرار عادت‌های روزانه افراد» در محیط‌های مختلف، قابل پیاده‌سازی بوده و به‌طور خاص نشان داده شد که با استفاده از این زیرساخت، پیام‌های فرمان و کنترل منتشرشده توسط مدیر بات طی ۲۴ ساعت، به دست ۲/۳ گره‌های آلوده‌شده خواهند رسید.

آلوده‌سازی: در این طرح در مورد نحوهٔ آلوده‌سازی حرفی به میان نیاورده است و فقط به بیان و معرفی روش‌های معمول آلوده‌سازی پرداخته است.

مدل حمله: ابتدا در این مدل فرض شده که بات‌ها بر روی دستگاه‌های موبایل از قبل نصب‌شده‌اند، ولی هنوز زیرساخت فرمان و کنترل آن برقرار نشده است. هم‌چنین مدافعان در زمینه کد بات و نحوه عملکرد آن اطلاع دارند؛ ولی با توجه به ویژگی کوتاه‌بردبودن ارتباطات بلوتوث، مدافعان برای تشخیص، باید در زمان برقراری ارتباط در بازه و محدودهٔ تجهیزات آلوده‌شده قرار داشته باشند که با توجه به ماهیت متحرک شبکه‌های ad-hoc این امر غیرعملی است.

البته تکیه بر این ارتباطات کوتاه‌برد چالش‌هایی را نیز به وجود خواهد آورد. به‌طور خاص مدیر بات برای انتشار موفق دستورها باید به این فرض تکیه کند که گره‌های آلوده‌شده طی یک اصول معینی در گروه رادیویی یکدیگر قرار خواهند گرفت. البته واقعیتی در این زمینه وجود دارد که تعداد بسیاری زیادی از افراد روزانه الگوی تکراری را دنبال می‌کنند. طبیعت این روال معمول، زیرساختی را در یک محیط غیرساختاریافته ایجاد خواهد کرد. هرچند ممکن است مدیر بات در هر لحظه از توپولوژی شبکه خود اطلاعی نداشته باشد؛ ولی اطمینان خواهد داشت که دستگاه‌های آلوده به‌طور روزانه در یک‌زمان و مکان خاص با یکدیگر برخورد خواهند داشت.

ساخت بات‌نت و انتشار دستورها: اکنون به بررسی نحوه ساخت و عملکرد موبایل بات‌نت ارائه‌شده در مدل حملهٔ بیان‌شده می‌پردازیم. نویسنده مقاله برای مقابله با تشخیص در روش‌های قدیم و برطرف‌ساختن برخی از چالش‌ها، سازوکار جدیدی را بهبود داده است. به‌عنوان‌مثال مدیر بات باید از هویت تمامی دستگاه‌های تحت نفوذ خود اطلاع داشته باشد؛ که این مستلزم ارتباط مستقیم بین مدیر بات و بات‌هاست. علاوه‌براین مدیر بات باید طی یک‌زمان کوتاه دستورها را به دست بات‌های زیادی برساند که متأسفانه راه‌حل استفاده از بلوتوث به‌تنهایی بر این عملکرد کافی نبوده و مهاجم باید به‌طور فیزیکی نزدیک به گره‌های آلوده باشد که این درعمل نشدنی است. درنتیجه یک راه‌حل ترکیبی برای به حداکثررساندن سرعت توزیع دستورها و مخفی‌ماندن هویت مدیر بات ارائه شده است. به‌طور خاص مدیر بات دستورها را به یک گروه کوچک از بات‌ها از طریق شبکه‌های سلولی و پیام کوتاه ارسال خواهد کرد. انتخاب این گره براساس میزان گره‌های آلوده در اطراف آن‌ها است. برای نائل‌شدن به این هدف، دستگاه‌های آلوده‌شده در هنگام عبور از محدوده یکدیگر، هویت دستگاه‌های اطراف خود را ذخیره کرده و بعد از رسیدن به یک حد آستانه‌ای که توسط مدیر بات تعریف‌شده، گزارشی از حساب‌های کاربری ذخیره‌شده را به مدیر بات ارسال خواهند کرد. با این کار مدیر بات هم از هویت گره‌های تحت کنترل خود اطلاع خواهد داشت و هم این‌که گره‌هایی را که به انتشار سریع دستورها کمک می‌کنند شناسایی خواهد کرد.



(شکل- ۱): نحوه ارتباط گره‌ها با یکدیگر [۱۰]

شکل (۱) نشان‌دهنده سناریوی معمولی از این طرح است، که رنگ سیاه دور هر دستگاه نشان‌دهندهٔ میزان گره‌های آلوده اطراف آن گره است. در شکل دیده می‌شود که دستگاه صفر مشهورترین گره است و به‌عنوان گره بذر[1] برای ارتباط با مدیر بات انتخاب می‌شود. درصورتی‌که گره صفر به هر دلیلی از بین برود دستگاه سه به‌عنوان گره بذر به مدیر بات معرفی خواهد شد.

مدیر بات نیز با استفاده از این ساختار سلسله‌مراتبی دستورها را منتشر خواهد کرد. درصورت وجود یک دستور جدید، مدیر بات با گرهٔ بذر ارتباط برقرار کرده و دستور را به آن ارسال خواهد کرد. گره بذر با توجه به میزان اتصال‌های اطراف خود، این دستور را به دست دیگر گره‌ها نیز خواهند رساند. درنتیجه دستورهای بدون ارتباط مستقیم با مدیر بات از طریق گره بذر به دست دیگر گره‌ها خواهد رسید.

[1] Seed node

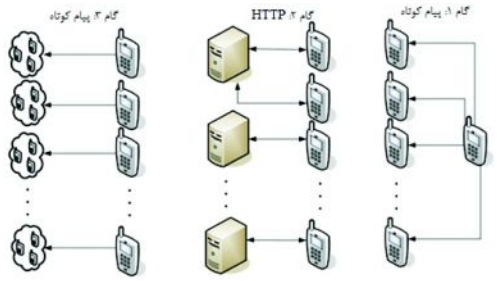
با توجه به ارتباط گره بذر با یک نقطهٔ مرکزی، تشخیص آن هدف جذابی برای مدافعان محسوب شده و مدافعان با کشف آن قادر به فلج‌کردن ارتباطات در این طرح خواهند بود. حتی کم‌کردن حجم ترافیکی این گره‌ها، برای اجتناب از تشخیص کافی نیست؛ درنتیجه گره‌های بات، فعالیت‌ها و هویت خود را از طریق استفاده از تکنیک‌های نام مستعار در شبکه‌های تر و استفاده از نشانی رایانامه‌های موقت، مخفی خواهند کرد. هم‌چنین این ارتباطات از طریق اتصالات Wi-Fi نیز قابل مخفی‌سازی هستند. هم‌چنین از طریق جعل نشانی مبدأ می‌توان ارتباطات را مخفی کرد.

۵-۲- موبایل بات‌نت بر پایه پیام کوتاه در آیفون

مولینر در سال ۲۰۱۰ به معرفی طرح [۱۱] و طراحی، پیاده‌سازی و ارزیابی بات‌نت موبایل بر روی گوشی‌های آیفون پرداخته است. در این طرح در ابتدا به طراحی یک موبایل بات‌نت نظیر به نظیر[1] پرداخته و با توجه به‌سادگی طراحی، از آن به‌عنوان بات‌نتی برای افراد غیرحرفه‌ای یادکرده، سپس به ایجاد موبایل بات‌نت براساس پیام کوتاه[2] پرداخته که کنترل بات‌ها از طریق پیام کوتاه صورت می‌پذیرد؛ سپس با بهبود طرح پیام کوتاه خود و ایجاد باتی ترکیبی از پیام کوتاه و HTTP، به کاهش تعداد پیام‌های کوتاهی ارسالی و افزایش کارایی بات خود پرداخته است.

در طراحی این بات‌نت از شبکه نظیر به نظیر نامتمرکز overnet و پروتکل مخصوص آن یعنی kademlia برای پیاده‌سازی طرح خود استفاده کرده است. ایده اصلی طراحی این کانال استفاده از شبکه نظیر به نظیر به‌عنوان یک نقطه ملاقات[3] است. مدیر بات یک دستور را در شبکه منتشر و بات‌ها برای بازیابی دستورها، یک کلید خاص را جستجو خواهند کرد و چون عملکرد انتشار و جستجو بر پایه جدول درهم‌سازی توزیع‌شده است، درنتیجه هیچ فایل واقعی نه در سمت مدیر بات و نه در سمت بات‌ها به اشتراک گذاشته نخواهد شد. در این طرح به چهار جنبه آلوده‌سازی[4]، ارتباطات[5]، ترمیم[6] و مدیریت[7] طراحی موبایل بات‌نت پرداخته است. در شکل ۲ کانال ترکیبی از این طرح مشاهده می‌شود.

1 P2P
2 SMS
3 Rendezvous point
4 Infection
5 Communication
6 Repair
7 Managment



(شکل ۲): کانال فرمان و کنترل بر پایه پیام کوتاه و HTTP [۱۱]

آلوده‌سازی: در ابتدا نرم‌افزار بات بر روی گوشی هدف از طریق تنظیمات آسیب‌پذیر سیستم‌عامل نصب شده، سپس بات آلوده‌شده یک پیام کوتاه به فرد مهاجم ارسال می‌کند و در انتها مهاجم شماره تلفن را در مکانی ذخیره خواهد کرد. فقط بعد از ارسال پیام کوتاه به فرد مهاجم شماره او از تلفن بات تازهٔ آلوده‌شده حذف و شماره تلفن بات تازه آلوده‌شده از فهرست مهاجم نیز حذف می‌شود.

ارتباطات: ارتباطات و نوعی توپولوژی بات‌نت به‌صورت درخت است. ایدهٔ اصلی این طرح، تقسیم ارتباطات به دو قسمت پیام کوتاه و HTTP است. پیام کوتاه شامل دستور که توسط مدیر بات دستکاری شده است به‌عنوان یک فایل رمزشده در برخی از سایت‌ها بارگزاری شده؛ سپس نشانی اینترنتی[8] این فایل به‌صورت تصادفی به برخی از بات‌ها از طریق پیام کوتاه ارسال خواهد شد. بات فایل موردنظر را دانلود و رمزگشایی کرده و دستورات را از آن استخراج خواهد کرد. کلید رمزگشایی قسمتی از پیام کوتاهی است که در آن آدرس اینترنتی فایل ارسال‌شده بود.

بخش ترمیم: مدیر بات به‌طور دوره‌ای به جستجوی بات‌ها برای تشخیص وضعیت آن‌ها می‌پردازد. مدیر بات با ارسال یک پیام ping به‌صورت همه‌پخشی از وضعیت بات‌های خود اطلاع می‌یابد درصورتی‌که باتی به این پیام پاسخ نداد، تنها از فهرست جهانی و کلی بات‌ها حذف خواهند شد و درنتیجه پیام‌ها دیگر به آن بات ارسال نخواهد شد.

مدیریت: مدیریت از آن‌جهت ضروری است که هر گره به‌تنهایی با تعداد زیادی گره به‌صورت مستقیم در ارتباط نباشد؛ زیرا در صورت خرابی آن گره باید تمامی آن زیرگره‌ها به گرهٔ دیگری انتقال یابند. مدیر با بررسی وضعیت پخشی گره‌ها توازن را در درخت ایجاد خواهد کرد.

استراتژی ارتباطات: با توجه به محدودیت‌های گوشی‌های همراه، ارتباطات اولیه و پس‌زمینه‌ای مثل ارتباطات نظیر به

8 URL

نظیر از طریق شبکه موبایل صورت می‌پذیرد؛ زیرا نظارت بر آن سخت‌تر است؛ ولی داده‌های حجیم و بزرگ در صورت امکان از طریق Wi-Fi انتقال یابند.

در این طرح هم‌چنین برای افزایش امنیت کانال هر دستور با یک کلید عمومی رمز می‌شود و برای جلوگیری از حمله پاسخ[1] تمامی پیام‌ها شماره ترتیبی[2] را دارند که تنها دستورها با شماره ترتیبی بالاتر به‌عنوان دستور قابل‌قبول پذیرفته خواهند شد.

۵-۳- موبایل بات بر پایهٔ ارسال سیل‌آسایی پیام کوتاه

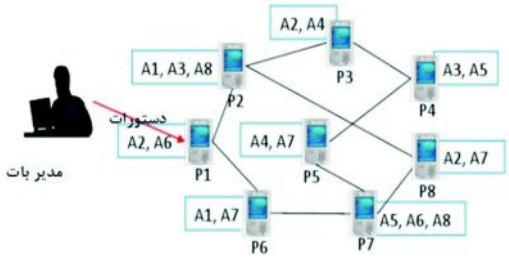
طرح [۱۲] توسط دو دانشجوی دکترای ژاپنی به نام‌های J.Hua و K.Sakurai در سال ۲۰۱۰ ارائه شد. در این طرح از پیام کوتاه به‌عنوان کانال و فرمان برای طراحی بات‌نت موبایل استفاده و طرح ارائه‌شده را از جنبه‌های مختلفی ازجمله نهان‌کاری[3]، انتخاب توپولوژی و حفظ و نگه‌داری بات‌نت[4] مورد بررسی قرار داده‌اند.

آلوده‌سازی: در این طرح در مورد نحوهٔ آلوده‌سازی گوشی‌های هوشمند و تبدیل آن‌ها به بات‌هایی فعال حرفی به میان نیاورده و فرض را بر این گذاشته است که دستگاه‌ها از قبل آلوده شده‌اند.

مروری بر طرح: در این طرح، هر گوشی هوشمند تحت نفوذ، فهرستی از نظیرها[5] را به‌عنوان همسایگان مجازی خود انتخاب کرده به‌گونه‌ای که قادر خواهد بود با آن‌ها به‌طور مستقیم از طریق پیام کوتاه در ارتباط باشد؛ سپس دستورها بر پایه این معماری با استفاده از الگوریتم سیل‌آسای اصلاح‌شده انتشار می‌یابند.

مدیر بات در ابتدا دستور را به گره‌هایی از شبکه ارسال کرده، به‌محض دریافت پیام و دستور جدید، گوشی‌های هوشمند به‌طور پیوسته و مداوم دستورها تا زمان رسیدن به یک حد آستانه، به گوشی‌های دیگر انتقال خواهند داد. شکل (۳) نمایشی از نحوه انتشار دستورها در این طرح است.

از ویژگی‌های این بات می‌توان به موارد زیر اشاره کرد: معماری آن نظیر به نظیر بوده، زیرا هر گره در این معماری یکسان و برابر بوده و هیچ زیرساخت مرکزی وجود ندارد. چون هر بات تنها تعداد محدودی از همسایگان خود را می‌شناسد، درصورت شناسایی و فاش‌شدن یک گره، تنها همسایگان محدودی از آن گره شناسایی و فاش خواهند شد؛ درنتیجه، مقاومت این طرح بالاست. برای جلوگیری از شناسایی از دید کاربران و اپراتورها، سازوکارهای نهان‌کاری در این طرح به کار گرفته‌شده است. برای نهان‌کاری از دید کاربر، امکان ارسال و دریافت پیام کوتاه بدون اطلاع کاربر و محدودساختن تعداد پیام‌های ارسالی توسط هر گوشی استفاده شده است. برای نهان‌بودن از دید اپراتور، از ارسال پیام‌های همه‌پخشی[6] در شبکه خودداری می‌شود. هم‌چنین تمامی پیام‌های دستوری، قبل از ارسال رمزگذاری‌شده و چون بین هر دو گره جفت، کلید خاصی به اشتراک گذاشته می‌شود، در نتیجه ظاهر این پیام‌های دستوری متفاوت از یکدیگر خواهد بود و با استفاده از الگوریتم پنهان‌نگاری[7]، آن‌ها را تبدیل به متن‌هایی نزدیک به زبان‌های طبیعی خواهد کرد.



(شکل ۳): مثالی از موبایل بات‌نت ارائه‌شده بر پایه پیام کوتاه [۱۲]

توپولوژی: در این طرح بعد از مقایسه سه توپولوژی از سه جنبه دسترس‌پذیری گره‌ها[8]، تأثیر انتقال محدود[9] و مقاومت در مقابل نقطهٔ شکست، مدل ER، برای ساختن بات‌نت بر پایهٔ پیام کوتاه مؤثرتر دیده شد. در این مدل دستوری که به‌تازگی منتشر شده در طی زمان بیست دقیقه با استفاده از الگوریتم سیل‌آسا، ۹۰٪ یک شبکه ۲۰۰۰۰ بات‌نتی را تحت پوشش خود قرار خواهد داد. هم‌چنین در این پروسه هر بات به ارسال حداکثر چهار پیام کوتاه نیاز داشته و بات‌نت ارائه‌شده در مقابل نقطهٔ شکست تصادفی[10] و انتخابی[11] مقاوم است.

یکی از چالش‌هایی که این طرح با آن روبه‌رو بود، چگونگی یافتن گوشی‌ها و درنهایت ساخت یک بات براساس توپولوژی گراف تصادفی است. برای این کار از یک سرور اینترنت کمک گرفته شده است. در این طرح ابتدا یک سرور

1 Reply attack
2 Sequence number
3 Stealthiness
4 Botnet Maintaing
5 Peer
6 Broadcast
7 Steganography
8 Reachabilities
9 Forwarding bound
10 Random node failure
11 Selective node failure

در اینترنت راه‌اندازی خواهد شد و بعد از آلوده‌سازی دستگاه‌های تلفن همراه، گوشی‌های هوشمند به این سرور متصل شده و اطلاعات خود را در آن سرور ثبت خواهد کرد و فهرستی از همسایگان تخصیص‌یافته را از این سرور دریافت خواهد کرد.

یکی دیگر از چالش‌های پیش‌روی بات‌نت‌ها که در این طرح به آن پاسخ داده شده نگه‌داری از این شبکه است؛ درنتیجه از کانالی که برای بات‌نت‌های قدیمی رایانه‌ای به‌وجود آمده برای نگه‌داری تلفن همراه بات‌نت استفاده می‌شود.

۵-۴- تلفن همراه بات‌نت برپایه پیام کوتاه و ساختار نظیر به نظیر

این مقاله [۸] در سال ۲۰۱۲ توسط Zeng و دوستان با رویکرد جدیدی برای استفاده از پیام‌های کوتاه به‌عنوان کانال فرمان و کنترل برای ساخت یک تلفن همراه بات‌نت پرداخته است و ساختارهای مختلف معماری نظیر به نظیر برای تلفن همراه بات‌نت‌ها را بررسی و ارزیابی کرده است. نتایج شبیه‌سازی نشان می‌دهد که پروتکل kademlia اصلاح‌شده گزینهٔ مناسب‌تری برای توپولوژی بات‌نت‌هاست.

انتشار: شیوه انتشار در این طرح، روش مهندسی اجتماعی بوده و از پیام کوتاه به‌عنوان کانال فرمان و کنترل استفاده شده است.

طراحی پروتکل: در این طراحی برای هر گوشی یک کد عبوری[1] هشت بیتی در نظر گرفته شده است. به‌محض دریافت یک پیام کوتاه، گوشی به جستجوی کد عبوری و دستورهای تعبیه‌شده در پیام کوتاه می‌پردازد. به‌محض پیداشدن، دستورها به‌سرعت اجرا خواهند شد. نحوهٔ تخصیص کدهای عبوری به هر بات به این صورت است که مدیر بات در ابتدا بات‌ها را به چند گروه تقسیم و هر گروه را مسئول عملکرد خاصی خواهد کرد. هر گروه توسط کد عبوری منحصربه‌فرد خود شناسایی خواهد شد که به‌صورت کد سخت[2] در کد دودویی بات قرار داده شده است. به‌عبارت‌دیگر تمامی بات‌ها در یک گروه، کد عبوری یکسانی را به اشتراک خواهند گذاشت درنتیجه قادر به برقراری ارتباط با یکدیگر و هم‌چنین ارتباط با مدیر بات خواهند بود. برای تغییر چهره پیام‌ها به شکل پیام‌های هرزنامه، هر دستور به یک الگوی هرزنامه نگاشت خواهد شد. برای دیکدکردن پیام‌ها، فهرستی از نگاشت دستور- الگو در هر بات وجود داشته و با توجه به کم‌بودن تعداد دستورها در هر بات، پس این فهرست طولانی نبوده و درنتیجه تشخیص را سخت‌تر خواهد کرد.

برای مخفی‌ماندن هویت مدیر بات این روش‌ها پیشنهاد شده است:۱- استفاده از سایت‌های تبلیغاتی برای ارسال رایگان پیام کوتاه در حجم کم ۲- ارسال و دریافت پیام‌های کوتاه از طریق رایانامه درصورت بزرگ‌بودن بات‌نت. ۳- استفاده از تکنیک جعل پیام کوتاه[3] برای دست‌کاری نشانی فرستنده ۴- به‌کارگرفتن چند شماره برای تغییر مبدأ فرستنده پیام‌ها به‌دفعات.

در این طرح دستورها در حالت pull دریافت خواهند شد. در این حالت، مدیر بات دستورها را منتشر و بات‌ها به‌صورت فعالانه به یافتن دستورها می‌پردازند. این حالت ظاهر توزیع‌شده‌تری نسبت به حالت push داشته و آشکارسازی فعالیت‌های مخربانه در آن سخت‌تر است.

توپولوژی: در این طرح بعد از مطرح‌کردن معماری‌های مختلف در بات‌نت‌ها و بررسی مزایا و معایب هر یک، دو معماری ساختاریافته و غیرساختاریافته را برای استفاده در تلفن همراه بات‌نت‌ها مناسب دید؛ زیرا طبیعت غیرمتمرکز این معماری‌ها هویت مدیر بات را مخفی نگه خواهد داشت. در این طرح پروتکل kademia را برای معماری ساختاریافته و پروتکل Gnu برای معماری غیر ساختاریافته در نظر گرفته و به ایجاد تغییراتی و اصلاحاتی در آن‌ها پرداخته است.

با توجه به تفاوت گوشی‌های هوشمند و رایانه‌های شخصی، نویسنده تغییرات زیر را در kademila معمول به وجود آورده تا برای استفاده در تلفن همراه مناسب باشد. نخست این‌که از پیام‌های ping برای بررسی وضعیت گره‌ها استفاده نمی‌شود؛ زیرا پیام کوتاه همیشه به دست گیرنده خواهد رسید. دوم این‌که به‌جای ایجاد یک شناسه تصادفی برای گره‌ها، شناسه گره‌ها از درهم‌سازی شماره موبایل‌ها ایجاد می‌شوند تا با این کار جلوی حمله سیبیل[4] تا حد زیادی گرفته خواهد شد و در انتها با استفاده از الگوریتم کلید متقارن AES به‌عنوان سازوکار احراز هویت این کانال امن شده است. هم‌چنین نویسنده با ایجاد تغییراتی در پروتکل Gia بهبودیافته، از آن برای طراحی تلفن همراه بات‌نت خود استفاده کرد. ۱- از پروتکل انطباق توپولوژی[5] برای قراردادن گره‌ها در نزدیکی و همسایگی گره‌ها با ظرفیت بالا استفاده شده است.۲- یک طرح کنترل جریان فعال[6] برای جلوگیری از

[1] Passcode
[2] Hard-code
[3] SMS spoofing
[4] Sybil
[5] Topology adaptation protocol
[6] Active flow control

سربار گره‌ها با توجه به ظرفیت آن‌ها در نظر گرفته شده است. ۳-تکرار یک گامی[1] برای اشاره به محتوای همسایگان نزدیک حذف شده است.۴- از الگوریتم قدم‌زدن[2] تصادفی برای یافتن گره‌هایی که تمایل به پاسخ‌گویی دارند، استفاده شده است؛ ولی در انتها نتایج شبیه‌سازی انجام‌شده، نشان می‌دهد که استفاده از حالت ساختاریافته ازنظر تعداد پیام ارسالی، تعداد گام‌ها، تأخیر در ارسال و تعادل بار، بهتر از حالت غیر ساختاریافته است.

۵-۵- موبایل بات‌نت Andbot

در این طرح [۱۳] که توسط Xinag و همکارانش با حمایت بنیاد علوم طبیعی ملی[3] چین و مؤسسه ملّی پژوهش‌های فناوری‌های سطح بالا و برنامه‌های توسعه[4] چین ارائه شد با عنوان‌کردن چالش‌هایی که یک مدیر بات با آن‌ها روبه‌روست و ارائه راه‌حل‌هایی برای آن‌ها به طراحی یک بات‌نت پیشرفته به نام Andbot بر روی گوشی‌های هوشمند با سیستم‌عامل اندروید پرداخته است. این موبایل بات‌نت که سال ۲۰۱۲ ارائه شد، استراتژی کانال فرمان و کنترل آن URL-Flux بود و توپولوژی آن ساختار متمرکزی داشت.

انتشار: در این طرح در مورد شیوه انتشار بات‌ها به گوشی‌های تلفن همراه صحبتی به میان نیاورده است.

توپولوژی: این بات‌نت توپولوژی متمرکزی دارد، به این صورت که به‌تعداد مشخصی سرور فرمان و کنترل متصل شده و از آن‌ها دستورها را دریافت خواهد کرد. برخلاف بات‌نت‌ها با ساختار متمرکز بر پایه IRC و HTTP، در کانال فرمان و کنترل این بات یک سازوکار نامحدودکننده، «استفاده از نام‌های کاربری مختلف و نامحدود در میکروبلاگ‌ها» در نظر گرفته شده است که به آن URL-Flux گفته می‌شود. این سازوکار به این صورت است که در ابتدا چند سرور میکروبلاگ در نظر گرفته می‌شود، درصورتی‌که یک نام کاربری در میکروبلاگ‌ها بلوکه و یا ازکارافتاده باشد، بات به نام کاربری دیگری متصل خواهد شد و درنتیجه کانال فرمان و کنترل آن حالت ارتجاعی خواهد داشت.

برای روشن‌شدن طرح کانال فرمان و کنترل به توضیح دنباله عملیات در این بات‌نت براساس شکل (۴) می‌پردازیم:

(شکل ۴): معماری کانال فرمان و کنترل Andbot [۱۳]

۱) مدیر بات دستورها را رمزگذاری و امضا می‌کند؛ سپس مدیر این متن رمزشده و طول آن را به انتهای یک فایل عکس اضافه می‌کند.

۲) مدیر بات عکس را در وب‌سایت‌های عمومی میزبان تصاویر آپلود می‌کند و نشانی اینترنتی فایل را با استفاده از سرویس‌های معروفی مثل bit.ly و Tinyurl.com فشرده می‌سازد.

۳) مدیر بات برای جلوگیری از حمله پاسخ «تاریخ شروع»، «تاریخ پایان» و نشانی کوتاه‌شده را با یکدیگر ترکیب کرده و سپس آن‌ها را رمزگذاری، امضا و کد می‌کند.

۴) مدیر بات متن رمزشده را در صفحه خانگی کاربران میکروبلاگ‌ها قرار می‌دهد. نام کاربری این کاربران به‌صورت پیشرفته در میکروبلاگ‌ها توسط مدیر بات، ثبت نام شده‌اند.

۵) اکنون بات به میکروبلاگ‌هایی که در کد بات تعبیه‌شده است؛ مراجعه کرده و صفحه خانگی کاربران مختلف را مشاهده خواهد کرد. این عمل تا پیداکردن کاربری که مدیر بات پیام خود در صفحه خانگی آن قرار داده است ادامه خواهد یافت.

۶) بعد از پیداشدن پیام رمزشده در صفحه خانگی کاربر، صحت پیام توسط کلید عمومی که در کد بات تعبیه شده، بررسی و درصورتی‌که از تاریخ انقضای پیام نگذشته باشد، نشانی اینترنتی مربوط به عکس رمزگشایی خواهد شد.

۷) اکنون می‌توان به عکس از طریق نشانی اینترنتی آن دسترسی داشت و عکس را از درون وب‌سایت‌های عمومی مثل بلاگ و سایت‌های میزبان تصاویر دانلود کرد.

۸) دستورها با استفاده از کلید متقارن RC4، که از عکس دانلودشده، رمزگشایی می‌شود.

۹) بات دستورها آشکارشده را اجرا خواهد کرد.

---

[1] One Hop replication
[2] Random walk
[3] National Natural Science Foundation
[4] National High Technology Research and Development Program

از ویژگی‌های این بات می‌توان به موارد زیر اشاره کرد:۱- سرور فرمان و کنترل بر پایه IP است که هر گام از کانال فرمان و کنترل وابسته به ارتباطات TCP/IP به‌جای پیام کوتاه و یا بلوتوث است. ۲- از خوراک[1] RSS و فشرده‌سازی Gzip برای کاهش ترافیک شبکه تلفن همراه بات‌نت‌ها استفاده شده است. ۳- نشانی اینترنتی طی مدت مجاز و معتبر خود ذخیره‌سازی خواهد شد. ۴- برای خودداری از انتشار پیام‌های جدید و افزایش زمان بین ارسال دستورها از دستور sleep استفاده کند تا منابع استفاده‌شده درگوشی کاهش یابد.

۵-۶- موبایل بات‌نت SoCellBot

با توجه به محبوبیت گوشی‌های هوشمند و شبکه‌های اجتماعی برخط حملات مشترکی بر روی این دو آغاز شده است. در این مقاله [۱۴]، یک بات‌نت سلولی به نام SoCellBot توسط محمدرضا فغانی در سال ۲۰۱۲ معرفی‌شده است. شبکه‌های اجتماعی برخط یا OSN[2] ها کانال مناسبی برای بات‌نت‌ها به‌حساب می‌آیند؛ زیرا بیش‌تر شبکه‌های سلولی امروزی دسترسی به شبکه‌های اجتماعی را به‌صورت مجازی برای کاربران خود فراهم می‌کنند؛ درنتیجه از این نظر سامانهٔ پیام‌رسانی شبکه اجتماعی برخط یک راه‌حل مناسب از نظر کارایی و هزینه برای ارسال و دریافت پیام‌های فرمان و کنترل در بات‌های سلولی هستند. هم‌چنین پیام‌های مبادله‌شده در شبکهٔ اجتماعی برخط به‌طورمعمول رمز شده و تشخیص و بلوکه‌سازی این پیام‌های مخربانه را برای اپراتورها سخت می‌کند. علاوه‌براین، توپولوژی بات‌نت‌های بر این اساس در مقابل شکست مقاوم‌تر و پنهان‌سازی آن در مقایسه با پیام کوتاه راحت‌تر است. این بات‌نت از پلتفرم شبکه‌های اجتماعی برخط برای کنترل بات‌های سلولی استفاده می‌کند. ساختار و ویژگی‌های شبکه‌های اجتماعی برخط، تشخیص بات را سخت‌تر، مقاومت آن را بیش‌تر و نگرانی از بابت هزینه قبض تلفن همراه را از بین خواهد برد. اکنون ما به بررسی سازوکار انتشار، کانال فرمان و کنترل و توپولوژی آن می‌پردازیم.

سازوکار انتشار: این بات‌نت از دو نوع سازوکار انتشار، مهندسی اجتماعی و استخراج آسیب‌پذیری‌ها استفاده می‌کند؛ به این صورت که یک کاربر ممکن است پیوند وب بدخواهانه را دنبال کرده و بدافزار درون آن را اجرا کند یا اینکه سیستم‌عامل گوشی هوشمند در مقابل یک حمله خاص آسیب‌پذیر بوده و با وقوع حمله، باعث اجرای کد بدافزار بر روی دستگاه بدون مداخله کاربر شود. برای شروع، مهاجم قسمتی از یک شبکه اجتماعی را به‌وسیله نفوذ[3] آلوده می‌کند. نفوذ می‌تواند با ایجاد تعدادی پروفایل جعلی که سعی در برقراری ارتباط با کاربران واقعی را دارد، شروع شود. بعد از برقراری نخستین اتصال، سعی در برقراری ارتباط با دوستان آن کاربران آلوده‌شده را خواهد داشت و این روال ادامه خواهد یافت. به‌عنوان مثال شبکه‌های اجتماعی برخطی مثل فیسبوک برای شروع یک بات بسیار مؤثر هستند.

کانال فرمان و کنترل: چون در بسیاری از کشورها ارسال و دریافت پیام کوتاه هزینه‌بر است. مدیر بات، دستورهای اولیه را به یک گروه کوچکی از بات‌ها از طریق پیام کوتاه ارسال می‌کند سپس هر بات دستورها خود را از طریق سامانه پیام‌رسانی شبکه‌های اجتماعی برخط انتقال می‌دهد. چون بیش‌تر اپراتورها اتصال به شبکه‌های اجتماعی برخط را به‌طور رایگان در اختیار کاربران قرار می‌دهند؛ درنتیجه نگرانی از جهت هزینه وجود نخواهد داشت. همچنین برای جلوگیری از شک کاربر دستورها به‌گونه‌ای تغییر شکل داده خواهند شد که شبیه پیام‌های نرمال به نظر برسند. هم‌چنین مدیر بات می‌تواند به ارسال پیامی به یک کاربر تصادفی در فیسبوک بپردازد؛ ولی چون برخی از کاربران ویژگی عدم دریافت پیام از افراد ناشناس را فعال کرده‌اند، این نوع کاربران در گام نخست آلوده‌سازی شرکت نخواهند داشت؛ ولی آن‌ها از طریق دریافت پیام‌های آلوده از دوستان خود نیز آلوده خواهند شد.

توپولوژی: با توجه به ویژگی کلاسترینگ و خوشه‌بندی بالای شبکه‌های اجتماعی برخط، بات‌ها همیشه متصل به یکدیگر هستند و توپولوژی آن براساس گراف اتصال شبکه‌های اجتماعی است. براساس شبیه‌سازی انجام‌شده نشان داده شد که استفاده از گراف تصادفی برای انتشار بات‌ها سریع‌تر از گراف اصلی خود شبکه‌های اجتماعی است؛ هر چند که حجم پیام‌های ارسالی در گراف اصلی خود شبکه‌های اجتماعی کمتر بوده و توجه مدیر شبکه را برای شروع یک حمله جلب نخواهد کرد.

۵-۷- موبایل بات‌نت ناهمگون برپایهٔ پیام کوتاه

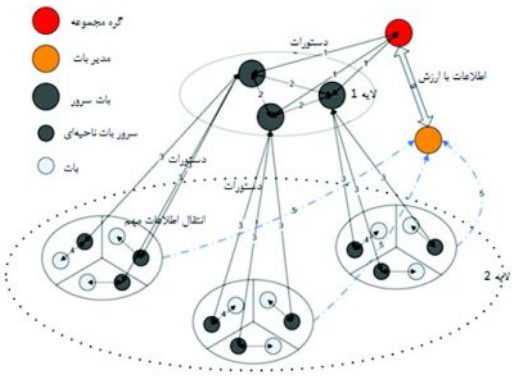
در طرح [۱۵] که با حمایت مؤسسهٔ علوم و فنّاوری بین‌المللی[4] چین توسط *Geng* و همکاران در سال ۲۰۱۲ انجام شد، یک بات‌نت ناهمگون بر پایه پیام کوتاه ارائه شده که

[1] feed
[2] Online social networking
[3] Infirtration
[4] National Science and Technology

ساختار شبکه‌ای آن، درخت چندگانهٔ ناهمگون ساختاریافته[1] بود. تمامی دستورها از طریق پیام کوتاه منتقل شده و با استفاده از درخت چندگانهٔ ناهمگون قابلیت مقیاس‌پذیری و مقاومت خوبی از خود نشان می‌دهد. همچنین فهرست تمامی بات‌ها و برخی دستورهای مهم نیز رمزگذاری خواهد شد.

در این طرح در ابتدا به توضیح انواع مختلفی از گره‌ها پرداخته و سپس بر روی انتشار، توپولوژی شبکه، سازوکار فرمان و کنترل و سازوکار جایگزینی[2] گره‌ها در بات‌نت موبایل تمرکز کرده است. شکل ۵ معماری این موبایل بات‌نت را نشان می‌دهد.

انواع گره‌ها: گره‌های آلوده‌شده با درنظرگرفتن تفاوت‌هایی مثل کارایی، منابع انرژی، اتصالات و شبکه‌های اطراف آن‌ها به انواع مختلفی از گره‌ها دسته‌بندی می‌شوند که شامل مدیر بات، گره مجموعه[3]، گره‌های سرور بات[4]، گره‌های سرور بات ناحیه‌ای[5] و تعداد مشخصی گره‌های بات است.



(شکل ۵): موبایل بات‌نت ناهمگون بر پایه پیام کوتاه [۱۵]

انتشار: مرحلهٔ انتشار به سه گام تقسیم شده است: در گام نخست، مدیر بات سیستم‌عامل و تنظیمات آسیب‌پذیر آن را پیدا و با استفاده از آن‌ها، نرم‌افزار بات را روی دستگاه تلفن همراه نصب خواهد کرد. بعد از نصب نرم‌افزار، فرض شده است که در گرهٔ بات، سازوکار نهان‌کاری به‌کارگرفته‌شده که جلوی مشاهدهٔ برنامهٔ نصب‌شده توسط کاربر را خواهد گرفت. در گام دوم مدیر بات از میان گره‌های تحت نفوذ قرارگرفته، گره‌ای را به‌عنوان گره سرور بات به‌عنوان گره‌های لایهٔ نخست انتخاب خواهد کرد. انتخاب این گره با توجه به شرایطی مثل منابع انرژی موجود در آن، ناحیه‌های اطراف آن و اتصالات آن است.

بقیهٔ گره‌هایی که به‌عنوان سرورهای بات انتخاب نشده‌اند هر یک با توجه به ناحیه خود به گره‌های سرورهای بات به‌عنوان گره‌های لایهٔ دو اختصاص داده خواهند شد. در گام سوم تمامی گره‌های موجود در این شبکه به آلوده‌سازی دستگاه‌های دیگر، تحت نظارت و کنترل مدیر بات ادامه خواهند داد. با توجه به توسعهٔ بات‌نت، تعداد سطوح نیز به‌مراتب افزایش خواهد یافت.

توپولوژی: توپولوژی این مدل درخت چندگانه ناهمگون ساختاریافته است. از بالا به پایین، مدل یک شبکهٔ ساختاریافته درخت چندگانه است؛ ولی توپولوژی هر لایه به‌عنوان مثال لایهٔ سرور بات و لایهٔ سرورهای بات ناحیه‌ای، ساختاریافته نظیر به نظیر است. درنتیجه ناهمگونی هم در ساختار و هم انواع مختلف گره‌ها دیده می‌شود.

کانال فرمان و کنترل: همان‌طور که در تصویر دیده شد، ایده نخستین طراحی برای این بات‌نت، استفاده از شبکهٔ درخت چندگانه ناهمگون به‌عنوان شبکهٔ کانال فرمان و کنترل است؛ شبکه شبیه یک کانال عمل کرده و تمامی گره‌های مشکی به‌عنوان سرور بات هستند. شبکهٔ کانال فرمان و کنترل شامل مدیر بات، بات سرور و سرور بات ناحیه‌ای است. برای جلوگیری از واردکردن مقادیر توسط مدافع و شروع حمله جعل شاخص[6]، قبل از برقراری ارتباط، هویت گره‌ها باید محرز و پیام مهم نیز رمزگذاری شود. برای افزایش کارایی، تنها دستورهای مهم مانند «انتقال مقادیر ارزشمند» رمز خواهند شد و دستورها برای برقراری ارتباطات نظیر به نظیر مثل «یافتن گره‌ها» تنها با تغییر چهره و بدون رمزگذاری ارسال خواهند شد. با توجه به وجود فهرست بات‌ها در گره‌های سرور بات، این گره‌ها تنها دو عملکرد اصلی جستجو و ارسال را اجرا خواهند کرد. دستورهای مهم رمز شده و دستورهای از گره‌های لایه‌های بالا به گره‌های لایه‌های پایین، از مدیر بات به گره سرور بات، از گره سرور بات ناحیه‌ای به گره‌های بات ارسال خواهند شد. هم‌چنین فهرست گره‌ها رمز خواهند شد تا درصورتی‌که یکی از کلیدها آشکار شد، مدافع قادر به بازیابی ارتباط بقیه گره‌ها از طریق آن و ردیابی مدیر بات نباشد.

سازوکار جایگزینی گره‌ها: در مواقعی که یک گره کلیدی مثل گره سرور بات و یا گره سرور بات ناحیه‌ای از فعالیت بازمی‌ایستد و از عملکرد نرمال خود خارج می‌شود و یا بنا با بر دلایلی نیاز به جایگزینی بات‌ها با یکدیگر احساس شود و به‌عبارت‌دیگر نیاز به تغییر نوع گره‌ها باشد، سازوکار جایگزینی به کار گرفته خواهد شد. برای این کار در ابتدا فرض شده

1 Heterogeneous multi-tree structure
2 Replacement
3 Collection node
4 Bot server
5 Region bot server
6 Index poisoning

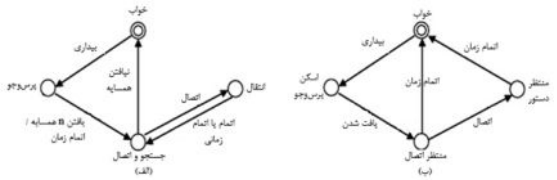
است که مدیر بات قادر به حذف گره شکست‌خورده[1] است و دوم این‌که تمامی بات‌ها یک سازوکار خود از بین برندگی[2] دارد و قادر به حذف فهرست بات‌های ذخیره‌شده در خود هستند. برای حالت نخست باید گره موردنظر از توپولوژی حذف گردد برای این کار در ابتدا مدیر بات بعد از تشخیص گرهٔ دچار مشکل، کلیدهای جدید را در نظر خواهد گرفت؛ سپس با ارسال پیامی به گره‌های سرور بات و سرور بات ناحیه‌ای، کلید جدید را به آن‌ها ارسال خواهد کرد؛ سپس شماره تلفن گره شکست‌خورده، از فهرست تمامی گره‌ها حذف خواهد شد.

درصورتی‌که مدیر بات بخواهد نوع گره‌ای را تغییر دهد، در ابتدا گره قدرتمندی را از میان بات‌ها و یا گره‌های سرورهای ناحیه به‌عنوان سرور بات جدید (بنا به استانداردهای گفته‌شده در بخش انتشار) انتخاب می‌کند؛ سپس کلیدهای جدید مرتبط به این گره را به او ارسال خواهد کرد. گره جدید کلیدهای خود را با گره‌های سرور بات و سرورهای بات ناحیه‌ای به اشتراک خواهد گذاشت.

۵-۸- موبایل بات‌نت مجاورتی

با توجه به متحرک‌بودن دستگاه‌های موبایل، دو گوشی هوشمند که از کنار یکدیگر عبور می‌کنند، می‌توانند داده‌های خود را از طریق پروتکل‌های بی‌سیم با برد کوتاه مانند بلوتوث تبادل کنند. درنتیجه Hua و Sakurai در تکمیل و بهبود کار قبلی خود [۱۲]، به ارائه طرح بات‌نت مجاورتی[3] در سال ۲۰۱۲ پرداختند که در این طرح [۱۶]، از بلوتوث به‌عنوان پروتکل نزدیکی برای انتشار مؤثر دستورها بین موبایل بات‌نت‌ها استفاده می‌شود.

انتشار دستورها: در طرح بات‌نت‌های مجاورتی، زمانی که مدیر بات یک دستور را منتشر می‌کند، ابتدا آن را به تعداد محدودی از گره‌های بات از طریق شبکه‌های سلولی ارسال می‌کند. برای حفظ انرژی در ابتدا همه گره‌ها در وضعیت خواب قرار می‌گیرند. پس از طی مدتی، آن‌ها همه با یکدیگر بیدار شده و یک دور ارسال جدید را آغاز می‌کنند. وقتی‌که یک گره قابل‌دست‌یابی فعال می‌شود در ابتدا چرخهٔ پرس‌وجو را برای یافتن همسایگان در نزدیکی خود آغاز می‌کنند. چرخه پس از پیداشدن N_{ixg} همسایه یا سپری‌شدن T_{ixg} ثانیه از شروع کار پایان خواهد یافت. اگر این گره با موفقیت فهرستی از همسایگان جمع‌آوری کند به‌دفعات به این همسایگان وصل شده و دستورها را به آن‌ها منتقل خواهد کرد و سپس این گره به حالت خواب خواهد رفت. متفاوت از چرخهٔ بالا وقتی یک گره غیرقابل دسترسی فعال می‌شود در ابتدا یک چرخهٔ پرس‌وجو برای یافتن اتصالات شروع می‌کند. درصورتی‌که بعد از سپری‌شدن یک زمان خاص، هیچ گره‌ای یافت نشد، گره به حالت خواب خواهد رفت. در حالت دیگر گره، عمل پرس‌وجو را متوقف کرده و منتظر برای پیداشدن توسط گره‌های دیگر را خواهد کرد. روال بالا به‌صورت گراف انتقال وضعیت در شکل (۶) مشاهده می‌شود.



(شکل ۶): گراف انتقال وضعیت در طرح بات‌نت نزدیکی: (الف (نشان‌دهنده گره‌هایی که دستورات در دریافت کرده‌اند.) ب)نشان‌دهنده گره‌هایی که دستورات را دریافت نکرده‌اند [۱۶]

از مزایای این بات‌نت، مجاورت این است که به‌طورکامل توزیع شده است و هیچ گره‌ای، اطلاعاتی در مورد دیگر گره‌ها نگه‌داری نمی‌کند؛ ولی از معایب آن این است که انتشار دستورها به میزان زیادی وابسته به حرکت انسان‌هاست که تا حد زیادی تصادفی و تضمین کارایی آن سخت است. به‌عنوان مثال اگر حامل گوشی هوشمند تحت نفوذ تمام روز در یک مکان ساکن باشد، قادر به ارسال و دریافت دستورها نخواهد بود. به‌طورکامل واضح است که انتشار دستورها به چگالی بات‌ها وابسته است. به‌عنوان مثال تعداد متفاوت گره‌ها در یک ناحیه خاص.

نویسنده با درنظرگرفتن سه سناریو «استاتیک»، «راه رفتن تصادفی» و «راه رفتن انسان‌ها» برای بررسی نحوهٔ انتشار دستورها، به این نتیجه رسید که کارایی بات‌نت مجاورتی ارائه‌شده در سناریوی آخر خیلی بهتر از سناریوی حرکت تصادفی است و با توجه به این‌که تحرک انسان‌ها در محیط‌های مختلف متفاوت است، این بات برای محیط‌های با تحرک بالاست. براساس نتایج شبیه‌سازی حتی اگر نرخ آلوده‌سازی خیلی بالا نباشد، در محیط‌های با تحرک زیاد، دستورها به‌سرعت از طریق این کانال منتشر خواهند شد.

[1] Failed node
[2] Self destory
[3] Proximity botnet

سازوکار کاوش‌گر تطبیق‌پذیر[1]: در طرح بات‌نت مجاورتی زمانی که یک گره دستوری را دریافت می‌کند، به‌دفعات پرس‌وجوهایی را با گره‌های دیگر برقرار خواهد کرد. اگر گرهٔ مورد پرس‌وجو به‌طور کل از محدوده خارج‌شده باشد، پس، انجام این عملیات به‌دفعات خیلی منطقی به نظر نمی‌رسد؛ درنتیجه یک سازوکار کاوش‌گرانه مؤثری ارائه تا یک گره خود را با وضعیت دیگر گره‌ها منطبق کرده و درصورت دردسترس‌بودن، با آن‌ها ارتباط برقرار خواهد کرد. برای طراحی این سازوکار دو مورد زیر بررسی شد. ۱- یافتن راهی برای پیش‌بینی صریح وضعیت گره‌ها در یک ساعت آینده ۲- یافتن ارتباط بین نسبت مفقودشده‌ها و تعداد کاوش‌گران.

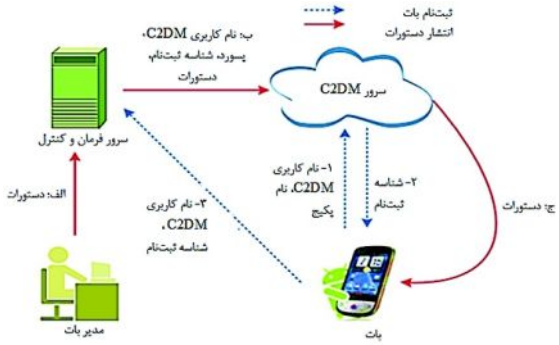
براساس نتایج مشاهده‌شده، استفاده از راه‌حل‌های انطباق‌پذیر تعداد کاوش‌گرانی را که به‌دنبال یک گرهٔ خاص می‌گردند به میزان قابل توجه‌ای کاهش می‌دهد. هم‌چنین، مصرف انرژی یک بات، متناسب است با تعداد جستجوها و کاهش تعداد جستجو، انرژی را ذخیره خواهد کرد درنتیجه راه‌حل انطباق پذیر کارا بوده و می‌توان با آن به پیش‌بینی وضعیت گره‌ها پرداخت. طبق پژوهش‌های صورت‌گرفته نشان داده شده که افراد بسیاری در روز از الگوی رفتار خاصی تبعیت می‌کنند و نویسنده بعد از بررسی‌های انجام‌شده به دو الگوی مهم برای پیش‌بینی وضعیت گره‌ها دست‌یافته است:۱- الگوی ساعتی: رفتار گره‌ها در ساعت‌های مجاور[2] و نزدیک به هم به‌طورکامل همبسته[3] و یکسان است و رفتار آن‌ها به‌کندی تغییر می‌کند. این نشان می‌دهد که یک دستگاه بات با استفاده از ثبت اطلاعات بات‌های همسایهٔ خود در چند ساعت گذشته، قادر به پیش‌بینی رفتار یک ساعت آیندهٔ آن‌ها خواهد بود. ۲- الگوی روزانه: بیشتر بات‌ها در ساعت‌های یکسان و مشابه در روزهای مجاور و پشت‌هم رفتار یکسانی را خواهد داشت و به‌طورکامل همبستگی دارند. این قضیه نشان می‌دهد که یک دستگاه می‌تواند به ثبت اطلاعات گره‌های بات همسایهٔ خود در ساعت‌های یکسان در چند روز اخیر به پیش‌بینی رفتار آن در ساعت بعدی بپردازند.

۵-۹- موبایل بات‌نت بر پایه C2DM

در این مقاله [۱۷]، با هدف ارائه آسیب‌پذیری سرور C2DM[4] گوگل در سیستم‌عامل اندروید، از این سرور به‌عنوان کانال فرمان و کنترل برای ایجاد یک بات جدید به نام C2DM پرداخته است. طرح بیان‌شده در سال ۲۰۱۲ با حمایت بنیاد علوم طبیعی ملی چین توسط Zhao و همکاران انجام شد. در این کانال، ارتباط مستقیمی بین مدیر بات و بات‌ها وجود ندارد. سرور C2DM به‌عنوان یک واسط و رله کاربرد دارد. مدیر بات می‌تواند دستورها را از طریق این سرویس به دست بات‌ها رسانده و ترافیک بات‌نت را در بین ترافیک قانونی برنامه‌های C2DM مخفی کند. هدف از ارائه این سرویس توسط گوگل کمک به برنامه‌نویسان برای انتقال اعلان‌ها و به‌روزرسانی‌های برنامه‌های خود بر روی دستگاه‌هایی است که این برنامه‌ها بر روی آن‌ها نصب شده است.

در این مقاله ابتدا یک طراحی اولیه برای بات‌نت C2DM را ارائه و سپس به بررسی یک معماری بهبودیافته پرداخته است.

معماری اولیه بات‌نت C2DM: مدیر بات مثل برنامه‌های معمول C2DM ابتدا در این سرویس ثبت‌نام کرده، سپس برای پیوستن یک بات جدید به این شبکه و انتشار پیام‌ها مراحل زیر را طبق شکل (۷) طی می‌کند.



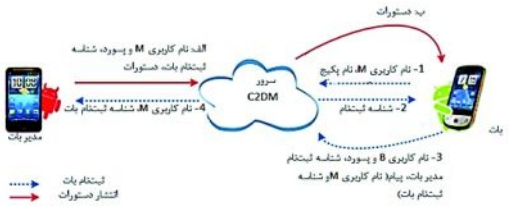
(شکل ۷): معماری اولیه بات‌نت C2DM [۱۷]

ثبت‌نام بات (گام ۱ تا ۳): وقتی‌که یک بات به شبکه بات‌نت می‌پیوندد، ابتدا خود را با اطلاعاتی نظیر نام پکیج، نام کاربری[5] C2DM (این دو از قبل در کد بات تعبیه شده‌اند) و شناسه حساب کاربری[6] گوگل در یکی از سرورهای C2DM ثبت نام می‌کند. سرور گوگل، درصورت موفقیت‌آمیزبودن این چرخه، یک شناسهٔ ثبت نام[7] را بازخواهد گرداند؛ سپس بات شناسه ثبت نام و نام کاربری C2DM را به سرور فرمان و کنترل مدیر بات ارسال می‌کند که این شناسهٔ ثبت نام در پایگاه داده مدیر بات ضبط می‌شود تا بعدها پیام‌ها از این طریق منتشر شوند.

[1] Adaptive probing mechanism
[2] Adjacent
[3] Correlation
[4] Cloud to Device Mannagment service
[5] Username
[6] Google's account ID
[7] Registration ID

انتشار پیام‌ها (گام الف تا ج): مدیر بات پیام‌ها را به‌تمامی موبایل‌بات‌های ثبت‌نام‌شده از طریق سرور فرمان و کنترل انتشار می‌دهد. این سرور فرمان و کنترل، ابتدا خودش را برای سرور C2DM از طریق شناسهٔ حساب کاربری گوگل و رمز عبور احراز هویت می‌کند. بعد از احراز هویت، سرور C2DM یک بسته احراز هویت به سرور فرمان و کنترل ارسال می‌کند و سپس به ساخت یک درخواست C2DM برای هر دستگاه موبایل می‌پردازد. این درخواست شامل دستورها مدیر بات، شناسهٔ ثبت نام بات و بستهٔ احراز هویت است. سرور فرمان و کنترل درخواست را به سرور C2DM ارسال و براساس شناسه ثبت نام، سرور C2DM پیام را به بات‌ها ارسال می‌کند. نکته قابل توجه این است که هر درخواست C2DM شامل یک شناسهٔ ثبت نام مجاز است که درنتیجه، برای ارسال دستورها به چندین بات، مجبور به ارسال چندین درخواست به سرور فرمان و کنترل خواهد بود.

بهبودیافتهٔ معماری بات C2DM: به این خاطر که در ارسال مستقیم شناسهٔ ثبت نام به سرور فرمان و کنترل، امکان آشکارسازی و تشخیص هویت سرور فرمان و کنترل وجود داشت، درنتیجه برای بهبود قابلیت نهان‌بودن این معماری، ارتباط مستقیم بین بات و مدیر بات در معماری بهبودیافته حذف‌شده است. در این معماری مدیر بات قبل از ساختن بات‌نت، ابتدا دو حساب کاربری C2DM ایجاد می‌کند.C2DM Username-M توسط مدیر بات برای ارسال دستورها از سرور فرمان و کنترل به بات‌ها استفاده می‌شود. C2DM Username-B توسط بات برای ارسال پیام به سرور فرمان و کنترل استفاده می‌شود. مدیر بات خودش را در سرور C2DM با استفاده از نام کاربری B برای دریافت شناسهٔ ثبت نام، ثبت نام می‌کند که بعدها توسط بات‌ها برای ارسال پیام C2DM به سرور فرمان و کنترل ارسال می‌شود. همچنین، فرض شده این دو نام کاربری و شناسهٔ ثبت نام مدیر بات در کد برنامه بات از قبل تعبیه شده است. شکل ۸ نشان‌دهندهٔ نحوهٔ ثبت‌نام بات و انتشار دستورها در معماری بهبود یافته است.



(شکل ۸): معماری بهبودیافتهٔ بات C2DM [۱۷]

ثبت نام بات (گام ۱ تا ۴): وقتی یک بات به شبکهٔ بات C2DM می‌پیوندد، خود را در یکی از سرورهای C2DM با استفاده از نام پکیج و نام کاربری M ثبت‌نام می‌کند. درصورت موفقیت‌آمیز بودن؛ سرور C2DM یک شناسه ثبت‌نام یکتا به بات ارسال می‌کند؛ سپس بات با استفاده از نام کاربری B و شناسهٔ ثبت نام مدیر بات (هر دو در پکیج بدافزار از قبل تعبیه شده‌اند) به ارسال شناسهٔ ثبت نام خود و نام کاربری M به مدیر بات می‌پردازد. از این اطلاعات بعدها برای پخش دستورها استفاده می‌شود.

انتشار دستورها (گام الف تا ب): برای انتشار پیام بین تمامی گوشی‌های موبایل ثبت‌نام‌شده، سرور فرمان و کنترل یک درخواست C2DM برای هر بات می‌سازد. برخلاف معماری اولیه، این درخواست شامل نام کاربری M، شناسه ثبت نام بات و دستورها است. سرور فرمان و کنترل این درخواست را به سرور C2DM ارسال می‌کند و سپس با توجه به شناسه ثبت نام، دستورها به بات مورد نظر ارسال خواهد شد.

۵-۱۰- تلفن همراه بات بر پایهٔ GCM

در این طرح [۱۸]، Wei و همکاران در سال ۲۰۱۳ از آسیب‌پذیری سرویس GCM[1] گوگل به‌عنوان کانال فرمان و کنترل برای موبایل بات‌نت‌ها استفاده کردند. این سرویس به برنامه‌نویسان اجازه می‌دهد پیام‌های خود را به برنامه‌های نصب‌شده بر روی سیستم‌عامل اندروید ارسال کنند. این سرویس جنبه‌هایی ازجمله صف‌بندی پیام‌ها و ارسال پیام‌ها به گوشی‌های اندروید را نیز ممکن می‌سازد. در این طرح از استراتژی اتصال شبکه انطباقی بهره برده است تا از مزیت شبکه‌های سلولی و Wi-Fi هم‌زمان استفاده شود. در مقایسه با شبکه‌های سلولی مانند 3G، Wi-Fi مزیت‌های بسیاری دارد ازجمله پهنای باند بیش‌تر، مصرف باتری کم‌تر، هزینه ارسال دادهٔ ارزان‌تر و غیره را دارد. با استفاده از این استراتژی انطباق‌پذیر، موبایل بات‌نت می‌تواند برای اجرای دستورهایی که ترافیک زیادی را مصرف می‌کند از Wi-Fi استفاده کند و از شبکهٔ 3G برای پوشش‌دادن سطح بیشتری نسبت به Wi-Fi و ارسال پیام‌های ضروری از مدیر بات‌نت به بات‌ها استفاده کند.

کانال فرمان و کنترل: سازوکار کانال فرمان و کنترل بر پایه GCM به چهار گام تقسیم می‌شود.۱- پنهان‌سازی دستورها توسط مدیر بات‌نت. ۲-ارسال‌کردن دستورها توسط GCM. ۳- ارتباط شبکهٔ انطباق‌پذیر. ۴- استخراج دستورها توسط بات.

[1] Google Cloud Messaging

ابتدا مدیر بات دستورها را در یک عکس از طریق فنّاوری پنهان‌سازی اطلاعات[1] مخفی می‌کند؛ سپس مدیر بات این عکس را در سایت‌های مثل میکروبلاگ‌ها و بلاگ‌ها بارگذاری کرده و نشانی اینترنتی[2] این عکس را ذخیره می‌کند. با توجه به اضطراری‌بودن و یا نبودن دستورها و هم‌چنین میزان مصرف ترافیک شبکه در صورت حمله، مدیر بات یک پرچم خاص در انتهای نشانی اینترنتی عکس اضافه و نشانی اینترنتی عکس را به موبایل مربوطه از طریق GCM، ارسال می‌کند؛ بات پیام ارسال‌شده توسط GCM را خوانده و چرخهٔ انطباق‌پذیر اجرا خواهد شد.

پنهان‌سازی دستورها: برای جلوگیری از آشکارسازی دستورها در حین انتقال در شبکه از فنّاوری پنهان‌سازی استفاده می‌شود. الگوریتم پنهان‌سازی دستورها به این صورت است که در ابتدا مدیر بات عکس حامل و دستورها را خوانده و بایت انتهایی عکس حامل و طول دستور را محاسبه می‌کند. با توجه به مقادیر مشخص‌شده، مدیر بات دستورها را در انتهای عکس حامل اضافه کرده و در انتها طول دستورها را در انتهای فایل عکس نیز می‌نویسد. بعدازاین پنهان‌سازی، عکس را در وب‌سرورهایی مثل بلاگ‌ها، میکروبلاگ‌ها و شبکه‌های اجتماعی و غیره بارگزاری و نشانی عکس را ذخیره می‌کند.

با توجه به اولویت دستورها، پرچمی[3] در انتهای نشانی اینترنتی اضافه می‌شود. پرچم یک، یعنی اینکه دستور بسیار ضروری است و حمله باید بی‌درنگ اجرا شود و پرچم صفر نشان‌دهندهٔ این است که این دستور خیلی ضروری نبوده و حملات می‌تواند با تأخیر اجرا شوند. بعد از اضافه‌کردن پرچم در انتهای نشانی اینترنتی، این نشانی به بات‌ها از طریق GCM، ارسال می‌شود.

استخراج دستورها: چون دستورها در یک عکس خاص توسط مدیر بات مخفی شده‌اند و طول دستورها به انتهای فایل عکس اضافه شده است، بات اطلاعات عکس را خوانده و طول دستور را محاسبه خواهد کرد؛ سپس بات دستورها را از عکس استخراج و دستورها را ذخیره و در انتها فایل حامل عکس را حذف خواهد کرد.

۵-۱۱- موبایل بات‌نت بر پایه پیام کوتاه و توئیتر

در این مقاله [۱۹]، که با حمایت بنیاد علوم طبیعی ملّی چین توسط Li و دوستان در سال ۲۰۱۳ معرفی شد، یک موبایل بات‌نت بر پایه پیام کوتاه و پیام‌های توئیتر به‌عنوان کانال فرمان و کنترل آن، معرفی شده است. بر این پایه نویسندهٔ مقاله دو الگوریتم معمول برای توپولوژی شبکه برای محیط‌های واقعی معرفی کرده و با توجه به شبیه‌سازی انجام‌شده، نشان داده شد که این بات مقاوم، انعطاف‌پذیر و نامرئی و غیرقابل مشاهده است.

بخش بات‌نت بر پایه توئیتر: در این بخش از طرح، موبایل بات‌نت، با توپولوژی نظیر به نظیر است که هیچ زیرساختی مرکزی وجود ندارد و هر بات در شبکه بات‌نت دستورها را از طریق پیام‌های توئیتر منتشر می‌کند. دستورهایی که با امضای مدیر هستند به بات‌ها اطلاع می‌دهند، به‌طور خودکار پیام‌های توئیتر را به بقیه بات‌ها منتشر کنند. این ساختار نظیر به نظیر در مقابل از بین رفتن مقاوم است؛ زیرا هیچ ساختار مرکزی وجود ندارد و راه‌های ارتباطی بسیاری بین بات‌ها وجود دارد.

درصورتی‌که مدیر بات برای راه‌اندازی شبکه برای هر بات یک حساب توئیتر ثبت کند، مدافع از طریق پی‌گیری حساب‌های کاربری ارتباط بات‌ها را کشف خواهد کرد، درنتیجه برای هر بات، یک جفت حساب کاربری مستقل از دیگری ثبت خواهد شد. یکی از حساب‌های کاربری، مسئول دریافت پیام‌ها و دیگری مسئول ارسال پیام‌های توئیتر است.

چرخهٔ ثبت نام: در ابتدا بات یک جفت حساب کاربری توئیتر را در وب‌سایت توئیتر ایجاد می‌کنند؛ سپس بات جدید این دو حساب کاربری را با کلید عمومی مدیر بات رمز کرده و آن را به مدیر بات ارسال می‌کند. مدیر بات فایل دریافت‌شده را با کلید خصوصی خود رمزگشایی می‌کند؛ سپس با توجه به فهرست حساب‌های کاربری و نوع الگوریتم تولید توپولوژی به راه‌اندازی شبکه می‌پردازد؛ سپس بات برای دریافت دستورها بات وارد حساب کاربری دریافت‌کنندهٔ دستورها شده و منتظر دریافت دستورها می‌شود، به‌محض دریافت دستورها، بات وارد حساب کاربری ارسال‌کننده شده و فعالیت مخربانه را اجرا خواهد کرد و برای دریافت دستور بعدی دوباره به وضعیت وارد حساب کاربری دریافت‌کننده خواهد شد.

بخش پیام کوتاه بات‌نت: چون شبکه 3G و GPRS برای دریافت پیام‌های توئیتر همیشه موجود نیستند و ممکن است حساب‌های کاربری توئیتر توسط مدافعان مسدود شوند درنتیجه راه‌حل پشتیبان استفاده از پیام کوتاه است. برای حالت نخست دستورها از طریق پیام کوتاه انتقال خواهند یافت؛ برای حالت دوم پیام کوتاهی حاوی یک جفت حساب کاربری توئیتر و دستور بازیابی‌شده به بات ارسال خواهد شد.

---

[1] Information hiding
[2] URL
[3] Flag

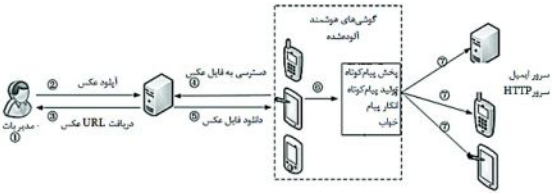
توپولوژی: انتخاب نوع توپولوژی در این طرح بر عهده مدیر بات با توجه به نیاز شبکه است. الگوریتم تولید توپولوژی که بر روی سرور مدیر بات است دو الگوریتم ساختاریافته نظیر به نظیر درخت تصادفی[1] و الگوریتم ساختاریافته نظیر به نظیر تصادفی[2] است. بعد از انجام‌شدن شبیه‌سازی‌ها مشخص شد که کارایی انتشار در درخت تصادفی، بالاتر از حالت تصادفی است؛ ولی ممکن است که تمامی بات‌ها به یکدیگر متصل نشوند؛ درنتیجه مدیر بات با توجه به وضعیت، توپولوژی بات را انتخاب می‌کند.

۵-۱۲- موبایل بات‌نت SUbot

در مقاله [۲۰] طرح بات‌نت موبایل به نام SUbot توسط Shaui و همکاران در سال ۲۰۱۳ ارائه شده است. این بات توسعه‌یافته و بهبودیافتهٔ Andbot است که از روش Shorten-URL Flux برای طراحی کانال فرمان و کنترل خود استفاده کرده است. با استفاده از این روش، می‌توان برای دریافت دستورها به‌جای اتصال به دو سرور موجود در طرح Andbot تنها به یک سرور شبکه مراجعه کرد.

انتشار: در این مقاله در مورد نحوه انتشار بات‌ها حرفی به میان نیامده و فقط گوشی‌های موبایل آلوده‌شده را SUbot نامیده است.

برای روشن‌شدن طرح کانال فرمان و کنترل به توضیح دنباله عملیات در این بات‌نت براساس شکل (۹) می‌پردازیم:



(شکل ۹): معماری کانال فرمان و کنترل موبایل بات‌نت SUbot [۲۰]

۱) ابتدا مدیر بات دستورها را با الگوریتم RC4 رمزگذاری کرده و آن را با کلید خصوصی خود امضا می‌کند. مدیر این متن رمزشده را در انتهای یک فایل عکس اضافه می‌کند.

۲) مدیر بات این عکس را در سایت‌های میزبان تصاویر، بارگزاری می‌کند.

۳) مدیر بات نشانی اینترنتی در گام دو را، با استفاده از سرویس‌های معروفی مثل bit.ly، TinyURL.com فشرده کرده و یک نشانی اینترنتی خاصی تولید می‌کند.

۴) اکنون با استفاده و ترکیب الگوریتم تولید دامنه و یک یا چند نشانی وب‌سایت کوتاه‌کننده که در کد دودویی بات قرار داده شده است، بات به تولید فهرستی از نام‌های دامنه پرداخته و با استفاده از Shorten-URL-Flux این نام‌های دامنه را با نشانی وب‌سایت‌های مختصرکننده، ترکیب خواهد کرد.

۵) بات سعی در اتصال به نشانی‌های تولیدشده توسط Shorten-URL-Flux می‌کند و درصورتی‌که نشانی مورد نظر وجود داشته باشد، فایل عکس را از آن نشانی بارگیری خواهد کرد.

۶) بات با استفاده از کلید عمومی که در کد بات وجود دارد، عکس را ارزیابی کرده و پیام با استفاده از کلید متقارن RC4 رمزگشایی می‌کند.

۷) بعد از رمزگشایی دستورها، بات به اجرای دستورها می‌پردازد.

ازجمله تفاوت Andbot و SUbot این است که Andbot ابتدا باید به سرور میکروبلاگ برای دریافت نشانی اینترنتی فایل عکس مراجعه کند؛ سپس با استفاده از این نشانی اینترنتی باید به‌عکس مورد نظر دسترسی داشت؛ درنتیجه هر دستور نیاز به دو مراجعه به سرور دارد که طی این مدت فایل‌های XML غیرضروری زیادی نیز بارگیری خواهند شد. همچنین تعداد میکروبلاگ‌ها که برای دسترسی کاربران نیاز به احراز هویت نداشته باشد، کم است. درنتیجه پیداکردن یک میکروبلاگ مناسب برای Andbot سخت است، بنابراین در این بات از میکروبلاگ‌ها استفاده نشده و قابلیت تطبیق‌پذیری بیشتری در این بات ارائه شده است.

۵-۱۳- موبایل بات‌نت هوشمند

در مقاله [۹] Wang و همکاران در سال ۲۰۱۴ به ارائه یک بات‌نت موبایل برای سیستم‌عامل اندروید پرداخته‌اند. مدل ارائه‌شده از دید یک مهاجم است. برای انتشار بات از مهندسی اجتماعی استفاده کرده و کانال فرمان و کنترل آن بر پایه پروتکل SMS-HTTP و توپولوژی آن متمرکز ساخت‌یافته است. در این مدل یک بات هوشمند برای افزایش مقاومت آن در نظر گرفته شده است. اکنون به‌طور خلاصه به بررسی این بات می‌پردازیم.

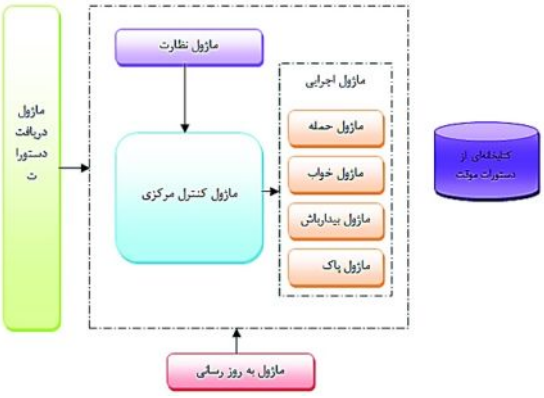
انتشار: روش انتشار در این طرح مهندسی اجتماعی در نظر گرفته شده است.

[1] Random tree P2P-structured algorithm
[2] Random P2P-structured algorithm

کانال فرمان و کنترل و توپولوژی: کانال فرمان و کنترل آن SMS-HTTP با توپولوژی متمرکز در نظر گرفته شده و در این مدل، فرمان‌ها از دو طریق منتشر می‌شوند. دستورها به بات‌ها از طریق پیام کوتاه و یا درصورت وجود اتصالات شبکه‌ای، دستورها از طریق سرورهای ابری عمومی ارسال خواهند شد.

بات هوشمند: بعد از دریافت پیام‌ها گام بعدی اجرای دستورهاست؛ چون اجرای دستورها منجر به تغییراتی در دستگاه می‌شود؛ درنتیجه بات هوشمند به‌محض دریافت دستورها آن‌ها را اجرا خواهد کرد. ابتدا نتیجهٔ اجرای دستورها بر پایه وضعیت فعلی گوشی هوشمند بررسی خواهد شد. درصورتی‌که اجرای دستور منجر به یک رفتار غیرمعمول در دستگاه شود، بات دستورها را به‌طور موقت ذخیره کرده و در یک زمان دیگر آن‌ها را اجرا خواهد کرد.

در شکل (۱۰) نمایی از بات مشاهده می‌شود. ماژول‌های این بات به شرح زیر هستند:



(شکل ۱۰): معماری ماژولار بات هوشمند[۹]

ماژول نظارت: مسئول بررسی وضعیت قسمت‌های مختلف است.

ماژول کنترل مرکزی: با توجه به وضعیت دستگاه موبایل و دستورهای دریافت‌شده بهترین تصمیم را اجرا خواهد کرد.

ماژول خواب: بعد از تصمیم‌گیری در مورد عدم اجرای دستورها، یک‌سری از عملکردها و ماژول خاموش خواهد شد.

ماژول بیدارشدن: ماژول‌های خاموش‌شده توسط ماژول خواب را روشن خواهد کرد.

ماژول به‌روزرسانی: شامل به‌روزرسانی ماژول‌ها، پایگاه داده و تنظیمات است.

ماژول پاک‌کردن: درصورتی‌که وضعیت گوشی هوشمند مناسب برای اجرا بات نبود، این ماژول بات را از روی گوشی هوشمند حذف خواهد کرد.

طراحی ماژولار دارای مزایای فراوانی است؛ از یک جهت جداسازی درستی از عملکردهای بات به‌صورت ماژول‌های جدا از یکدیگر صورت گرفته است. از جهت دیگر اندروید با نوع جدیدی از حملات که حملات هماهنگ شده است، روبه‌روست؛ به‌طوری‌که برنامه‌های مختلف در اندروید می‌توانند با یکدیگر همکاری و یک حمله را شروع کنند. در این معماری بات، هر ماژول به‌طور مجزا در برنامه‌های مختلف می‌تواند قرار بگیرد و درنتیجه بات پیچیده‌تری به وجود خواهد آمد.

۵-۱۴- موبایل بات‌نت بر پایه PNS

در این مقاله [۲۱] که با حمایت بنیاد ملی تحقیقات کره توسط Lee و همکاران در سال ۲۰۱۴ صورت گرفته، کانال فرمان و کنترل جدیدی برای موبایل بات‌نت‌ها براساس سرویس اعلان ارسال یا PNS[1] ارائه شده است. این سرویس در سیستم‌عامل اندروید GCM نامیده می‌شود. نویسندگان این مقاله دریافتند که در چرخهٔ ثبت نام GCM، تنها درستی نشانی رایانامه گوگل بررسی می‌شود. همچنین در برنامه‌ها امکان ارسال مخفی پیام‌ها از دید کاربران وجود دارند؛ که درنتیجه با استفاده از این دو آسیب‌پذیری تلفن همراه بات‌نتی به نام Punobot ارائه شد.

انتشار: روش انتشار این بات مهندسی اجتماعی است. مهاجم، برنامه‌های معروف را به‌همراه کدهای بدخواهانه بر پایه PNS دوباره بسته‌بندی کرده و در فروشگاه‌های فروش نرم‌افزار موبایل قرار می‌دهد.

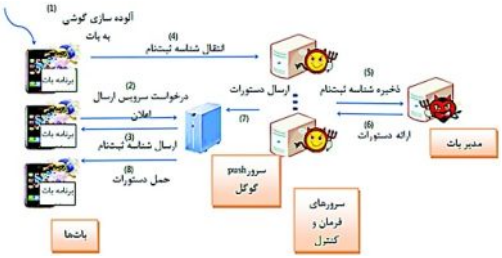
توپولوژی: در این بات سرورهای فرمان و کنترل از فنّاوری معرفی‌شده در بات Conficher به نام Domain Flux بهره می‌جویند؛ یعنی مدیر بات در یک سطح بالا از تمامی بات‌ها قرارگرفته است و سرورهای فرمان و کنترل به‌عنوان واسط و پروکسی بین مدیر بات و بات‌ها فعالیت می‌کنند. این توپولوژی تشخیص و یافتن مدیر بات را سخت‌تر می‌سازد.

پروتکل فرمان و کنترل: این بات برای برقراری ارتباط با اجزای خود از سه پروتکل زیر استفاده می‌کند.۱- پروتکل PNS: این پروتکل توسط تمامی اعضا استفاده می‌شود و نقش اصلی را در انتقال پیام‌ها از مدیر بات به بات‌ها را دارد.۲- پروتکل Domain Flux: این پروتکل، پروتکل اصلی بین سرور فرمان و کنترل و بات‌هاست. زیرا بعد از دریافت شناسهٔ ثبت نام از سرورهای push گوگل، بات باید با سرورهای فرمان و کنترل برای ارسال شناسهٔ ثبت نام با آن‌ها ارتباط برقرار کند. درنتیجه نشانی IP یا نام دامنه سرورهای فرمان و کنترل باید

[1] Push Notification Service

در کد دودویی بات تعریف‌شده باشد؛ درنتیجه برای جلوگیری از تحلیل ایستا در این بات از پروتکل Domain Flux استفاده‌شده است ۳- پروتکل Email-Flux: این پروتکل برای استفاده از آسیب‌پذیری در هنگام ثبت‌نام در PNS است. زمانی که یک برنامه‌نویس یک پروژه در سایت رسمی GCM ایجاد می‌کند سرویس GCM برای هر نشانی رایانامه گوگل یک شناسهٔ پروژه در نظر می‌گیرد. از طریق استفاده از این ویژگی یک مهاجم با استفاده از چند نشانی رایانامه گوگل می‌تواند به دفعات در این سرویس ثبت نام و درنتیجه یک دستگاه تلفن همراه قادر خواهد بود چند شناسهٔ پروژه دریافت کند و درصورتی‌که یکی از شناسه‌های ثبت نام تولیدشده، توسط گوگل بلوکه شوند، مهاجم از شناسهٔ پروژهٔ دیگری برای دریافت شناسهٔ ثبت نام کاربران استفاده می‌کند.

سناریوی حمله: بعد از توزیع و نصب برنامهٔ آلوده بر روی دستگاه‌ها، بات درخواست PNS خود را ارسال می‌کند و درصورت صحیح‌بودن، شناسهٔ ثبت نام برای دستگاه ارسال می‌شود؛ تا به اینجا هیچ تغییری در سناریوی اصلی سرویس دیده نمی‌شود. اکنون بات شناسهٔ ثبت نام را به سرور فرمان کنترل می‌کند؛ سرور اطلاعات را به مدیر بات ارسال خواهد کرد. اکنون مدیر بات دستورهای خود را از طریق سرور فرمان و کنترل و کانال GCM به بات ارسال خواهد کرد. در شکل (۱۱) تصویری از این سناریو مشاهده می‌شود.



(شکل ۱۱): سناریو حمله Punobot [۲۱]

۵-۱۵- موبایل بات‌نت بر پایه شبکهٔ گمنامی تُر

تولیدکنندگان بات به‌طورمعمول به دنبال تکنیک‌هایی برای مخفی‌سازی حضور خود، ترافیک و مکان سرورهای فرمان و کنترل هستند و به‌طورمعمول از تکنیک‌هایی مثل الگوریتم تولید دامنه برای ایجاد نشانی‌های پویای فرمان و کنترل استفاده می‌کنند تا از تشخیص و بلوکه‌نمودن این ترافیک جلوگیری به‌عمل آورند. یکی از این تکنیک‌ها استفاده از شبکه‌های گمنامی است [۲۲].

پژوهش‌گران امنیتی، بات‌نتی بر روی رایانه‌ها شناسایی کردند که بر روی شبکهٔ بی‌نام تر کنترل می‌شود. این بات‌نت اسکای‌نت نامیده می‌شود و می‌تواند برای راه‌اندازی حملات منع از خدمات توزیع‌شده، تولید Bitcoin ها، استفاده از قدرت پردازش کارت گرافیک نصب‌شده در رایانه‌های آلوده‌شده، بارگیری و اجرای فایل‌های دلخواه و یا سرقت اطلاعات مربوط به حساب‌های بانکداری برخط مورد استفاده قرار بگیرد. آنچه که این بات‌نت را فعال نگه‌داشته است، سرورهای فرمان و کنترلی است که از سرویس نهان‌تر استفاده می‌کند که تنها از داخل شبکهٔ تر قابل دسترسی است. سرویس نهان تر یکی از خدمات ارائه شده توسط شبکهٔ تر است و برای ارئه میزبانی از پروتکل‌هایی مانند IRC و SSH و غیره مورد استفاده قرار می‌گیرد؛ ولی رایج‌ترین آن‌ها میزبانی سرورهای وب است که از طریق ارائه دامنه‌هایی با پسوندonion. و تنها از طریق شبکهٔ تر قابل دسترسی هستند [۲۳]

بعد از کشف بات‌نت مربوط به تر بر روی رایانه‌ها، از این تکنیک نیز بر روی موبایل‌ها استفاده شده است. برای نخستین بار بات اندروید backdoor.AndroidOS.Torec.a بر روی شبکهٔ تر در مقاله [۲۴]توسط Unuckek در فوریه ۲۰۱۴ کشف شد که طبق گفتهٔ کسپراسکای نام رسمی آن slempo است و یک توزیع و یا تکمیل‌یافتهٔ بات‌نت stoned cat است[۲۲]. در اواسط ماه می سال ۲۰۱۵ نویسنده این بدافزار قیمت پنج‌هزار دلار برای فروش این بات‌نت اندرویدی با امکان سرقت اطلاعات مالی در نظر گرفت. با توجه به آمار منتشرشده، سه کشور اروپایی آلمان، ترکیه و لهستان هدف این بدافزار بوده است[۲۵].

هرچند در مورد جزئیات این بات از جمله روش انتشار، توپولوژی و کانال فرمان و کنترل آن اطلاعات دقیقی وجود ندارد، ولی در ادامه به ارائه اطلاعات موجود در مورد این بات‌نت اندرویدی می‌پردازیم.

تُر یک نرم‌افزار برای گمنامی کاربران در هنگام دسترسی به اینترنت است و نرم‌افزار مؤثر و مفید برای افرادی است که نگران نشت اطلاعات محرمانه خود هستند. این بات از شبکه گمنامی تُر به‌عنوان شبکه‌ای از سرورهای پروکسی، استفاده می‌کند و علاوه‌بر این‌که برای کاربران، گمنامی فراهم می‌کند، این قابلیت را نیز دارد که سایت‌های گمنام با دامنهٔ onion. تنها از طریق این شبکه قابل‌دسترس باشند. این بات از نرم‌افزار orbit که برای شبکهٔ تُر است، استفاده می‌کند، مجرمان کدهای خود را به این برنامه اضافه کرده‌اند و این بدافزار از طریق استفاده از قابلیت orbit به شبکه متصل و فعالیت‌های بدخواهانه انجام خواهد داد [۲۶]. در تصویر (۱۲)

نمونه‌ای از اطلاعات ارسالی به سرور وب تر با پسوندonion. مشاهده می‌شود.

```
localJSONobject.put("type", "device check");
localJSONobject.put("phone number", Utils.getPhoneNumbers(paramcontext));
localJSONobject.put("country", Utils.getCountry(paramoontext));
localJSONobject.put("irei", Utils.getcutIMEI(paramcontext));
localJSONobject.put("model", Utils.getModels());
localJSONobject.put("OS", Itlls-get S1);
localJSONobject.put("client number", "1");
String str = localJSONobject.toString();
 try {
        if (send(sparamcontext, "nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p",
str).getstatusLine().getStatuscodex() != 200)
                {
                        throw new Exceptions():
                }       }
```

(شکل ۱۲): اطلاعاتی ارسالی این بات به سرورها با پسوند onion [۲۴]

این بات دستورهای زیر را از سرورهای فرمان و کنترل بازیابی می‌کند:

- مداخله در پیام‌های کوتاه دریافتی
- سرقت پیام‌های کوتاه ارسالی
- اجرای درخواست USSD
- ارسال اطلاعات دستگاه ازجمله شمارهٔ تلفن، کشور، IMEI، مدل و نسخه سیستم‌عامل به سرورهای فرمان کنترل
- ارسال فهرستی از برنامه‌های کاربردی نصب‌شده بر روی دستگاه موبایل به سرور فرمان و کنترل
- ارسال پیام کوتاه به شماره خاص[۲۴]

در هنگام استفاده از تُر به‌عنوان بستر انتقال اطلاعات فرمان و کنترل، مزایا و معایبی وجود دارد؛ از جنبهٔ مثبت قضیه، توقف سرورهای فرمان و کنترل غیرممکن است؛ ولی از معایب اصلی آن افزودن کدهای مخربانه زیاد به برنامه اصلی است که درنتیجه کد بدافزار حجیم [۲۴] و از جهت دیگر تجمیع نرم‌افزار اولیه با بدافزار باعث سنگین‌شدن برنامه خواهد شد و درنتیجه بارگیری، انتقال و اجرای مخفیانه را سخت‌تر خواهند کرد. از جهت دیگر شبکهٔ تُر کارایی زیادی در ارسال و دریافت اطلاعات ندارد؛ هم‌چنین مصرف انرژی بیشتر شده و به‌طورکلی استفاده از منابع سیستم بیشتر می‌شود[۲۳].

۶- راه‌های پیش‌گیری

برای پیش‌گیری از این بدافزار، از ابزارهای داده‌محوری که مشخص می‌کنند برنامه‌های کاربردی به چه نوع داده‌هایی دسترسی دارند و چه نوع داده‌ای را به کجا و چگونه انتقال می‌دهند، استفاده کرد. این برنامه‌ها به بررسی، رفتارهای برنامهٔ کاربردی نصب‌شده بر روی دستگاه خود می‌پردازند. برای نمونه برنامه Xposed Framework را می‌توان نام برد که به‌راحتی بر روی گوشی‌های هوشمند اندرویدی قابل نصب است.

راه حل بعدی، انتخاب صحیح برنامه‌های کاربردی است. بهتر است قبل از نصب برنامه‌ها بررسی اندکی بر روی آن‌ها صورت گیرد و همچنین اجازه دسترسی‌های موردنیاز برنامه‌ها بررسی شود؛ که اگر فراتر از حد موردنیاز بود آن برنامه‌ها نصب نشود.

براساس ساختار سیستم‌عامل اندروید بدافزارها، بیش‌تر به‌صورت مستقل قابلیت نصب و گسترش نداشته و مجبور به اتصال به یک برنامه به‌ظاهر مفید است؛ درنتیجه تا حد امکان توصیه می‌شود برنامه‌های موردنیاز خود را از فروشگاه رسمی اندروید گوگل برای کاربران سیستم‌عامل اندروید و فروشگاه‌های رسمی کاربران سیستم‌عامل iOS، تهیه و نصب کنید. البته این امر یک راه‌حل قطعی نیست، زیرا در فروشگاه‌های معتبر نیز امکان وجود بدافزار به‌صورت آگاهانه و یا غیرآگاهانه (هک‌شدن اکانت کمپانی-کامپایلر آلوده) وجود دارد.

۷- راه‌های تشخیص وجود یک بدافزار

درصورتی‌که باتری گوشی به شکل غیرمعمولی به‌سرعت خالی می‌شود؛ این نقص می‌تواند نشانهٔ وجود یک بدافزار جاسوسی بر روی گوشی باشد. البته نمی‌توان به‌طور قطع عنوان کرد که کم‌شدن میزان انرژی باتری نشانهٔ وجود بدافزار بر روی آن است؛ زیرا باتری‌ها به‌مرور زمان فرسوده می‌شوند و کاهش عملکرد آن‌ها به‌مرور زمان امری طبیعی است و بدافزارهای جاسوسی پیشرفته کمترین تأثیر را در مصرف انرژی دارند. درصورت امکان می‌توان باتری این دستگاه را روی گوشی‌های دیگر نیز امتحان کرد.

بدافزارهای جاسوسی، معروف به مصرف پهنای باند هستند؛ به همین علت هزینه‌های اینترنت افزایش خواهد یافت که علت آن، انتقال اطلاعات به سرور مورد نظر بدافزار از طریق اینترنت است؛ که با نصب برنامه‌های کاربردی مدیریت اینترنت و پهنای باند درگوشی هوشمند می‌توانید رفتار گوشی هوشمند را بررسی کرد.

به‌طوراصولی تشخیص بات‌نت‌هایی که به‌آرامی و در پس‌زمینه اجرا می‌شوند، کار بسیار پیچیده‌ای است و شاید تنها با مشاهدهٔ فرایند ذخیره‌سازی اطلاعات مربوط به رویدادهای یک شبکهٔ همراه با ثبت جزئیات آن امکان ایجاد شک در کاربر را به‌وجود آورد. به‌طورمعمول در بات‌نت‌های گمنام از پروتکل‌هایی غیرمعمول استفاده می‌شود که همین می‌تواند نشانهٔ وجود یک بدافزار بر روی دستگاه باشد. بعد از این شک اولیه و برای اطمینان در تشخیص، نیازمند مهندسی معکوس برنامه به‌منظور تشخیص صحیح خواهیم بود. یکی دیگر از مباحث شک‌برانگیز، وجود سرویس و حالت همیشه‌فعال در برنامه‌هایی است که همواره نیاز به اجرا ندارند و درنتیجه با بررسی جزئی‌تر این برنامه‌ها از وجود و یا عدم وجود بدافزار بر روی آنها می‌توان اطمینان حاصل کرد.

۸- راه مقابله

راه مقابله برای ازبین‌بردن برنامهٔ کاربردی آلوده از گوشی کاربر این است که به قسمت تنظیمات گوشی وارد شده و از بخش مدیریت برنامه‌ها[1] اقدام به حذف این برنامه کنید. اگر تهدید بعد از آخرین پاک‌سازی برنامه از روی دستگاه دوباره ظاهر شد؛ بدان معنی است که بدافزار موفق به نصب ماژول تداوم در مسیر سیستم شده است؛ در این مورد دستگاه باید دوباره با یک سیستم‌عامل رسمی فلش شده و یا به تنظیمات اولیه کارخانه در صورت عدم تخریب آن توسط بدافزار، بازگردد.

[1] manage

به‌طورکلی سرورهای فرمان و کنترل در شبکه بات‌نت یا به‌صورت گمنام و یا به‌صورت غیرگمنام هستند. در حالت غیرگمنام، ارتباط با سرورهای فرمان و کنترل یا به‌صورت مستقیم و یا به‌صورت ارتباط با یک‌سری سایت‌هایی (رله) است که آن‌ها با تغییر مسیر به سرور اصلی، ارتباط را برقرار می‌کنند. در حالت نخست زمانی که ارتباط با سرورها به‌طور مستقیم است، بعد از کشف ارتباط با این سرورها، باید آن‌ها را از سرویس خارج کرد؛ در حالت استفاده از سایت‌های رله، باید صاحبان سرورهای آلوده‌شده را مطلع کرد، تا آن‌ها سرورهای خود را از آلودگی رفع کنند؛ سپس بعد از یافتن این سایت‌های رله، نشانی سرور اصلی را پیدا کرد. در مورد سرورهای فرمان و کنترل گمنام بحث بسیار پیچیده‌تر است. سرورهای اصلی در شبکه‌های قدرتمندی مانند تُر وجود دارند که به‌راحتی نمی‌توان نشانی این سرورها را پیدا کرد و یافتن این سرورها به معنای هک‌کردن شبکه‌تر و خروج این سرورها از گمنامی است. در این حالت برای مقابله، باید از طریق مهندسی معکوس و پیداکردن پروتکل‌های ارتباطی و بسته‌های تبادل شده، حملاتی را به این سرورها ایجاد کرد. به‌عنوان مثال با ارسال بسته‌های زیادی به این سرورها، پایگاه دادهٔ آن‌ها را پر کرد. به‌عبارت دیگر به‌گونه‌ای حملهٔ منع از خدمت را بر روی این سرورها ایجاد کرد که درنهایت منجر به غیرفعال ساختن سرور اصلی می‌شود. البته نحوهٔ طراحی حمله به سرورها بسیار پیچیده است. روش دیگر از طریق ایجاد امضا از بات است که می‌توان با استفاده از فایل‌ها، سرویس‌ها و رشته‌های درون طبقه‌های بات یک امضا ایجاد کرد و از طریق قراردادن این امضا در دیوار آتش، آنتی‌ویروس و یا برنامه‌های حذف‌کنندهٔ بدافزار، امضای ایجادشده را با برنامه‌های نصب‌شده بر روی دستگاه بررسی کرد و آن‌ها را از لحاظ صحت مورد بررسی قرار داد.

۹- کارهای آینده

بستر موبایل، تهدیدها و چالش‌های برای ایجادکنندگان بات‌نت‌های موبایل ایجاد کرده است که درنتیجه پژوهش‌گران باید در زمینهٔ تحلیل، پیش‌گویی و مهاجرت موبایل‌ها پژوهش کنند. حتی پژوهش‌گران باید به طراحی موبایل بات‌نت‌های جدید به‌عنوان یک اعلان و اثبات خطر بپردازند.

با توجه به پیچیدگی و ویژگی‌های خاص موبایل‌ها تشخیص موبایل بات‌نت امری چالش‌برانگیز است؛ هرچند تکنیک‌ها و روش‌هایی برای تشخیص فعالیت بات‌نت در شبکه‌های

رایانه‌ای مثل استفاده از کندوی عسل، تحلیل رفتار حمله، مشاهده و تحلیل سرویس نام دامنه، تشخیص بر پایهٔ امضا و تشخیص بر پایهٔ رفتار وجود دارد؛ ولی حتی با درنظرگرفتن کارایی و دقت این روش‌ها، بیشتر آن‌ها مناسب برای محیط‌های موبایلی نیستند؛ درنتیجه ارائهٔ راه‌حل برای تشخیص بات‌نت‌های موبایل ضروری به نظر می‌رسد.

با توجه به این‌که در برخی از طرح‌ها از آسیب‌پذیری موجود بر روی وب ۲ و میکروبلاگ‌ها استفاده شده، درنتیجهٔ پژوهش بر روی سرورهای عمومی و جلوگیری از سوءاستفاده از آن ضروری به نظر می‌رسد.

همان‌طور که بیان شد، معمول‌ترین شیوه برای انتشار بات‌ها و به‌طورکلی بدافزارها روش مهندسی اجتماعی است؛ زیرا مهاجم به‌راحتی با قراردادن کدهای مخرب در برنامه‌های نرمال و بسته‌بندی دوباره این برنامه‌ها، آن‌ها را در فروشگاه‌ها منتشر می‌کند؛ درنتیجه ارائه راه‌کارهایی برای نظارت بیشتر فروشگاه بر روی محتوای برنامه‌های خود و ارائهٔ سازوکارهای مطمئن و ایمن برای بسته‌بندی دوباره برنامه‌ها از کارهای پیش‌روی پژوهش‌گران است.

۱۰- نتیجه‌گیری

بعد از بررسی بات‌نت و آمارهای گزارش‌شده توسط منابع معتبر مبنی بر افزایش بدافزارها به‌خصوص بات‌نت‌ها بر روی سیستم‌عامل اندروید، مطالعه تکنولوژی‌های کلیدی برای ایجاد بات‌نت موبایل از دیدگاه مهاجم ضروری به نظر می‌رسد؛ و باید درصدد برطرف‌سازی آن‌ها برآمد. در این مقاله با مروری بر روی طرح‌های موبایل، بات‌نت‌ها از سه جنبهٔ انتشار، کانال فرمان و کنترل و توپولوژی به بررسی این تکنولوژی‌ها و آسیب‌پذیری‌ها پرداخته شد و ویژگی‌ها، مزایا و معایب هر یک مورد بررسی قرار گرفت. این مقاله قسمتی از یک پروژهٔ بزرگ‌تر برای طراحی یک بات‌نت موبایل بر روی سیستم‌عامل اندروید و ارائه راه‌حل‌های دفاعی برای آن به حساب می‌آید.

نام طرح	نوع بستر	کانال فرمان و کنترل	توپولوژی	ویژگی‌ها	معایب
۲۰۱۰[۱۰]	مستقل از بستر	بلوتوث	حرکت انسان‌ها	توسعه خصوصیات کانال فرمان و کنترل برپایه بلوتوث برای تجهیزات موبایل، ایجاد معماری جدید براساس شهرت گره‌ها، ارزیابی از طریق شبیه‌سازی، ارائه راهکارهای تدافعی	کوتاه برد بودن بلوتوث و عدم مقیاس پذیری آن، پوشش منطقه محدود
۲۰۱۰[۱۱]	بستر IOS	SMS-HTTP	نظیر به نظیر	معرفی سه کانال فرمان و کنترل، دارای فازترمیم و مدیریت گره‌ها، استفاده از استراتژی مبهم کاری، ارزیابی از طریق ساخت پروتوتایپ	وابستگی به یک بستر خاص، عدم پیاده‌سازی واقعی
۲۰۱۱[۱۲]	مستقل از بستر	پیام کوتاه	گراف تصادفی	نهان‌کاری از دید کاربر و اپراتور، تعریف یک حد آستانه‌ای برای کاهش تعداد پیام‌ها، پیاده‌سازی نحوه یافتن گره‌ها، توضیح نحوه نگه‌داری از بات، ارزیابی از طریق شبیه‌سازی، ارائه راه‌کارهای تدافعی	ارسال تعداد زیاد پیام کوتاه و ایجاد شک در کاربر
۲۰۱۲[۸]	مستقل از بستر	پیام کوتاه	نظیر به نظیر ساختاریافته	تغییر چهره پیام از طریق نگاشت دستورات به الگوی اسپم، مقایسه دو نوع ساختار برای موبایل بات‌نت‌ها، ارزیابی از طریق شبیه‌سازی، ارائه راه‌کارهای تدافعی	ارسال تعداد زیاد پیام کوتاه و ایجاد شک در کاربر، پیاده‌سازی مشکل ساختار عنوان شده
۲۰۱۲[۱۳]	بستر اندروید	URL-Flux	متمرکز	پنهان‌سازی دستورات در فایل عکس، استفاده از میکروبلاگ‌ها، نهان‌کاری، تعریف چندین نام کاربری، ارائه حملات ممکن، ساخت پروتوتایپ، ارائه راه‌کارهای تدافعی	وابستگی به یک بستر خاص، عدم پیاده‌سازی واقعی
۲۰۱۲[۱۴]	مستقل از بستر	شبکه‌های اجتماعی	گراف تصادفی	انتشار از طریق مهندسی اجتماعی و استخراج آسیب‌پذیری، استفاده از شبکه‌های اجتماعی، مقایسه دو گراف تصادفی و گراف اصلی برای توپولوژی، ارائه ارزیابی از طریق شبیه‌سازی	عدم پیاده‌سازی واقعی
۲۰۱۲[۱۵]	مستقل	پیام کوتاه	درخت چندگانه	انتشار از طریق استخراج آسیب‌پذیری، تعریف انواع	ارسال تعداد زیاد پیام کوتاه

	از بستر		ساختاریافته ناهمگون	گره‌های مختلف با توجه به منابع و سطح انرژی هریک، ارائه مکانیسمی برای جایگزینی گره‌ها، ارزیابی تحلیلی، رمز پیام‌های مهم و تغییر چهره پیام‌های با اهمیت کمتر،	و ایجاد شک در کاربر، پیاده سازی مشکل ساختار عنوان شده
۲۰۱۲[۱۶]	مستقل از بستر	بلوتوث	حرکت انسان‌ها	معرفی مکانیسم کاوشگر انطباق پذیر، پیش‌بینی وضعیت گره‌ها، بررسی سناریو حرکت انسان‌ها، ارزیابی از طریق شبیه‌سازی، ارائه راه‌کارهای تدافعی	پوشش منطقه محدود
۲۰۱۲[۱۷]	بستر اندروید	سرور C2DM	متمرکز	انتشار از طریق استخراج آسیب‌پذیری و مهندسی اجتماعی، طراحی و پیاده‌سازی بات‌نت براساس C2DM، بیان نحوه انتشار و حملات این بات، توسعه به پلتفرم‌های دیگر، ارزیابی عملکرد بات‌نت، ارائه راه‌کارهای تدافعی	وابستگی به اینترنت
۲۰۱۳[۱۸]	بستر اندروید	GCM	متمرکز	استفاده از عکس برای پنهان سازی اطلاعات، افزودن مکانیسم انطباق پذیر، افزودن نشانه برای رتبه‌بندی اهمیت و اولویت اجرای دستورات، ارزیابی از طریق شبیه‌سازی، ارائه راه‌کارهای تدافعی	وابستگی به اینترنت و وجود یک نقطه شکست مرکزی
۲۰۱۳[۱۹]	مستقل از بستر	توئیتر و پیام کوتاه	نظیر به نظیر	استفاده از پیام کوتاه به عنوان راه‌حل پشتیبانی، استفاده از دو حساب کاربری توئیتر برای جلوگیری از ردیابی، انتخاب نوع الگوریتم تولید توپولوژی باتوجه به نیازمندیهای مدیر بات	عدم پیاده‌سازی طرح
۲۰۱۳[۲۰]	بستر اندروید	S-URL-Flux	متمرکز	بهبودیافته طرح AndBot، استفاده در یک سرور برای دستیابی به دستورات به جای دو سرور	وابستگی به اینترنت و یک بستر خاص
۲۰۱۴[۹]	بستر اندروید	SMS-HTTP	متمرکز	طراحی ماژولار، تعریف بات هوشمند با تأخیر در اجرای دستورات با در نظر گرفتن شرایط دستگاه، تغییر چهره بات، استفاده قابلیت از خود نابودسازی، استفاده همزمان از مزایای SMS و HTTP، ارائه راه‌کارهای تدافعی	وابستگی به یک بستر خاص، عدم بیان شرایط لازم دستگاه برای اجرا و یا عدم اجرای دستورات
۲۰۱۴[۲۱]	بستر اندروید	GCM	پروتکل PNS، domain Flux و Email Flux	روش انتشار مهندسی اجتماعی، ارائه حملات ممکن، ارزیابی از طریق حلیل امنیتی، ارائه راه‌کارهای تدافعی	امکان شناخته شدن و تشخیص توسط مدافع
۲۰۱۴[۲۴]	بستر اندروید	شبکه‌تر	ساختار خود شبکه‌تر	افزودن کدهای مخرب به برنامه orbit برای انجام فعالیت‌های مخربانه، استفاده از سرویس مخفی درتر برای مخفی ماندن سرورها	شک کاربر در صورت تخلیه سریع باتری، سنگین بودن برنامه

۱۱-مراجع

[1] D. Emm, M. Garnaeva, R. Unuchek, D. Makrushin and A. Ivanov, (2015), "IT Threat evelutaion in Q3 2015".

[2] S. Sérgio S.C, S. Rodrigo M.P, P. Raquel C.G and S. Ronaldo M, (2013), "botnet: A survey", *Computer Networks,* vol. 57, no. 2,p.p 378–403.

[3] Symantec corporation, (2004), "SymbOS.Exy.A", [Online].Available:https://www.symantec.com/security_response/writeup.jsp?docid=2004-061419-4412-99. [Accessed 29 1 2016].

[4] Symantec corporation, (2009), "SymbOS.Exy.A", [Online].Available:https://www.symantec.com/security_response/writeup.jsp?docid=2009-022010-4100-99&tabid=2. [Accessed 29 1 2016].

[5] Symantec Corporation, (2009), "Ikee.B" [Online]. Available:https://www.symantec.com/security_response/writeup.jsp?docid=2009-112217-4458-99. [Accessed 29 1 2016]

[6] T. wyatt, (2010), "Geinimi, Sophisticated New Android Trojan Found in Wild", [Online]. Available: https://blog.lookout.com/blog/2010/12/29/geinimi_trojan/. [Accessed 29 1 2016].

[۷] مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه، (۱۳۹۴)، " بررسی محبوبیت جاسوس‌افزارها در بین

کـاربران ایرانـی و معرفـی جاسـوس افـزار DroidJack"، بازیابی شده از آدرس:
https://www.certcc.ir/index.php?module=cdk&func=loadmodule&system=cdk&sismodule=user/content_view.php&cnt_id=332929&ctp_id=104&id=7894&sisOp=view

[8] Y. Zeng, X. Hu and K. G. Shin, (2012), "Design of SMS commanded-and-controlled and P2P-structured mobile botnets," in *WISEC '12 Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*.

[9] P. Wang, C. Zhang, X. Li and C. Zhang, (2014), "A Mobile Botnet Model Based on Android System," in *Trustworthy Computing and Services*, Springer Berlin Heidelberg, pp. 54-61.

[10] K. Singh, S. Sangal, N. Jain, P. Traynor and W. Lee, (2010), "Evaluating Bluetooth as a medium for botnet command and control", in *DIMVA'10 Proceedings of the 7th international conference on Detection of intrusions and malware, and vulnerability assessment*, Heidelberg. Vol. 6201, pp. 61-80.

[11] C. Mulliner, J.P. Seifert. *Rise of the iBots: 0wning a telco network*. 5th International Conference on Malicious and Unwanted Software (MALWARE), pp 71-80, 2010.

[12] J. Hua and K. Sakurai, (2011), "A sms-based mobile botnet using flooding algorithm," in *Proceedings of the 5th IFIP WG 11.2 international conference on Information security theory and practice: security and privacy of mobile devices in wireless communication*, Heidelberg.Vol. 6633, pp. 264–279.

[13] C. Xiang, F. Binxing, Y. Lihua and L. Xiaoyi, (2011), "Andbot: towards advanced mobile botnets", in *LEET'11 Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats*, CA, USA.pp. 11.

[14] M. R. Faghani and U. Trang Nguyen, (2012), "Socellbot: A new botnet design to infect smartphones via online social networking", in *Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on*, Montreal, QC. pp. 1-5.

[15] G. Geng, G. Xu, M. Zhang and Y. Yang, (2011), "An improved SMS based heterogeneous mobile botnet model," in *Information and Automation (ICIA), 2011 IEEE International Conference on*, Shenzhen, pp. 198 – 202.

[16] J. Hua and K. Sakurai, (2013), "Botnet command and control based on Short Message Service and human mobility", *Computer Networks: The International Journal of Computer and Telecommunications Networking,* vol. 57, no. 2, pp. 579-597.

[17] S. Zhao, P. P. C. Lee, J. C. S. Lui, X. Guan, X. Ma and J. Tao, (2012), "Cloud-based push styled mobile botnets: A case study of exploiting the cloud to device messaging service", in *ACSAC '12 Proceedings of the 28th Annual Computer Security Applications Conference*.pp. 119-128.

[18] W. Chen, P. Gong, L. Yu and G. Yang, (2013), "An adaptive push-styled command and control mechanism in mobile botnets", *Wuhan University Journal of Natural Sciences,* vol. 18, no. 5, pp. 427-434.

[19] Y. Li, L. Zhai, Z. Wang and Y. Ren, (2013), "Control Method of Twitter- and SMS-Based Mobile Botnet," in *Trustworthy Computing and Services*, vol. 320, Springer-Verlag Berlin Heidelberg, Vol 320, pp.644-650.

[20] W. Shuai, C. Xiang, L. Peng and L. Dan, (2013), "S-URL Flux: A Novel C&C Protocol for Mobile Botnets," in *Trustworthy Computing and Services*, vol. 320, Springer Berlin Heidelberg, Vol. 320, pp. 412-419.

[21] H. Lee, T. Kang, S. Lee, J. Kim and Y. Kim, (2014), "Punobot: Mobile Botnet Using Push Notification Service in Android," in *Information Security Applications*, Switzerland, Springer International Publishing, pp 124-137.

[22] A. Kujawa, (2014), [Online]. Available: https://blog.malwarebytes.org/mobile-2/2014/02/android-botnets-hop-on-the-tor-train/. [Accessed 29 1 2016]

[۲۳] مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه، (۱۳۹۱)، "شناسـایی بـاتنـت skynet"، بازیـابی شـده از آدرس http://www.certcc.ir.

[24] R. Unuchek, (2014), [Online]. Available: https://securelist.com/blog/incidents/58528/the-first-tor-trojan-for-android/. [Accessed 29 1 2016]

[25] Eleven Paths, (2016), "Financial cyber threats Q4 2015".

[26] F.-s.Corporation, (2014), [Online].Available:https://www.f-secure.com/v-descs/trojan_android_torsm_a.shtml. [Accessed 29 1 2016]

الهام عابد در ۱۳۹۴ موفق به اخذ مدرک کارشناسی ارشد خود در رشته مهندسی فناوری اطلاعات – شبکه های کامپیوتری از پردیس دانشگاه گیلان شد. موضوع پژوهشی اصلی نامبرده روی امنیت در شبکه های موبایل و بانت های روی گوشی های هوشند بوده است.نامبرده عضو شاخه دانشجویی انجمن رمز ایران در دانشگاه گیلان بوده و زمینه های پژوهشی مورد علاقه ایشان می‌توان به محافظت از نرم‌افزار، امنیت در شبکه های تلفن همراه و امنیت سیستم عامل اندروید است.

رضا ابراهیمی آتانی استادیار گروه مهندسی رایانهٔ دانشکده فنی و مهندسی دانشگاه گیلان است. نامبرده دکترای خود را در سال ۱۳۸۹ در رشتهٔ مهندسی الکترونیک از دانشگاه علم و صنعت ایران دریافت کرد. ایشان عضو پیوستهٔ انجمن رمز ایران و انجمن‌های بین المللی IACR و IEEE هستند. از ایشان تاکنون دو عنوان کتاب و بیش از یکصد مقاله در مجلات و کنفرانس‌های ملی و بین‌المللی به چاپ رسیده است. زمینهٔ پژوهشی مورد علاقهٔ وی طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری، امنیت شبکه و امنیت نرم‌افزار است.