تشخیص بات‌نت‌های شبکه‌های اجتماعی

مهدی مودی[۱]، مهدیه قزوینی[۲و۳]، محمد علائی[۴]، حسین مودی[۵]

[۱] دانشجوی کارشناسی ارشد معماری کامپیوتر، دانشگاه شهید باهنر کرمان
mahdi.moodi.72@gmail.com
[۲] استادیار گروه مهندسی کامپیوتر، دانشگاه شهید باهنر کرمان
[۳] دانشگاه آزاد اسلامی، واحد بافت، باشگاه پژوهشگران جوان و نخبگان، بافت، ایران
mghazvini@uk.ac.ir
[۴] استادیار گروه مهندسی کامپیوتر، دانشگاه شهید باهنر کرمان
m_alaei@uk.ac.ir
[۵] مربی گروه مهندسی کامپیوتر، دانشگاه صنعتی بیرجند
hmoodi@birjandut.ac.ir

چکیده

با محبوبیت شبکه‌های آنلاین اجتماعی، زمینه سوء استفاده برای سود جویان اینترنتی دو چندان شده است، چرا که بستر شبکه-های اجتماعی زمینه مناسبی را برای پخش هرزنامه‌ها و بدافزارهای مختلف فراهم آورده است. یکی از این بدافزارها، بات‌های اجتماعی می باشدکه از شبکه‌های اجتماعی به عناوین مختلفی سوء استفاده می‌کند. از طرفی آسان بودن گسترش بات‌ها در این شبکه‌ها و استفاده از این بستر به عنوان کانال فرمان و کنترل، سبب شده که طراحان بات‌نت‌ها تمایل زیادی به استفاده از این شبکه-های اجتماعی پیدا کنند. در این مقاله به معرفی تعدادی از بات‌های اجتماعی شناخته شده، روش‌های انتشار، بررسی ویژگی‌ها و راه های شناسایی این نوع از بات‌های اجتماعی پرداخته می شود. هدف از این پژوهش، تجزیه و تحلیل و مقایسه رفتار این نوع از بات-نت‌ها با یکدیگرست.

کلمات کلیدی

بات‌های اجتماعی، مدیربات‌ها، کانال فرمان و کنترل(C&C)، سرور C&C، بات‌نت، شبکه‌های آنلاین اجتماعی.

۱- مقدمه

یکی از بزرگ‌ترین تهدیدات امنیتی بر بستر اینترنت بات‌نت‌ها هستند. بات‌نت‌ها از دو واژه ی کلیدی BOT که اشاره به ربات و NET که اشاره به NETWORK دارد، تشکیل شده است. یعنی رباتی که در شبکه اینترنت کار می‌کند. بات‌نت به تعداد زیادی از بات‌ها گفته می‌شود، که به سیستم کاربران عادی نفوذ کرده‌اند. براساس گزارش جهانی امنیت اینترنت[1]، تایپه به شهری با بالاترین تراکم بات‌نت‌ها تبدیل شده است، که بالای 80% کامپیوترها و گوشی‌های هوشمند آن ممکن است به بات آلوده باشند. بات‌نت‌ها از سه عنصر بات، سرور فرمان و کنترل و مدیربات تشکیل شده و تهدیدات آنها نیز توسط این عناصر سازماندهی می‌شود. عملکرد این عناصر به شرح زیر است[3,2]:

۱) بات، یک برنامه نرم‌افزاری است که بر روی میزبان‌های آسیب پذیر نصب شده و قادرست اقدامات مخربی را انجام دهد. پس از اینکه برنامه بات بر روی کامپیوتری نصب گردید آن کامپیوتر، به یک بات یا زامبی تبدیل می-شود.

۲) سرور فرمان و کنترل، دستورات را از مدیربات دریافت کرده و برای دیگر بات‌ها ارسال می‌کند.

۳) مدیربات یا هدایت کننده بات، شخص یا گروهی از اشخاص است که بات‌ها را با ارسال دستورات خود، از راه دور کنترل می‌کنند تا فعالیت‌های غیرقانونی یا مخرب را انجام دهند.

ویژگی منحصر به فردی که بات‌نت‌ها را از دیگر بدافزارها متمایز می‌سازد، زیر ساخت ارتباطی آن یعنی کانال فرمان و کنترل است، مدیربات از کانال فرمان و کنترل برای دستور دادن به بات‌ها به منظور انجام فعالیت‌های

مخرب(سرقت اطلاعات حساس، تخریب بخش هایی از سیستم قربانی و...) استفاده می‌کند[5,4]. از جمله می توان به STUXNET اشاره کرد، که خسارت زیادی را به سانترفیوژهای ایران وارد کرد.

شبکه‌های آنلاین اجتماعی، بستر مناسبی را برای مدیربات‌ها جهت کنترل و هدایت بات‌ها فراهم کرده است. بات‌نت‌های اجتماعی برای اولین بار در سال ۲۰۰۹ کشف شدند. که می توان به Koobface و Nazbot اشاره کرد، که Koobface در Facebook ، Twitterو Myspace؛ و Nazbot در Twitter فعالیت می‌کردند[6].

در این مقاله ابتدا با معرفی تعدادی از بات‌های اجتماعی ویژگی‌های هر یک را بیان شده، و راه های مقابله با آنها و ابزارهای شناسایی آنها معرفی می‌گردد.

سایر بخش‌های مقاله به شرح زیر سازماندهی شده است: بخش ۲ دلایل محبوبیت شبکه‌های اجتماعی برای بات‌نت‌ها، بخش ۳ انواع بات‌نت‌های شبکه‌های اجتماعی، بخش ۴ روش‌های انتشار، بخش ۵ روش کاری و ویژگی‌های بات‌نت‌های اجتماعی، بخش ۶ روش‌های مقابله بات‌نت‌ها در برابر شناسایی و ابزارهای شناسایی بات‌نت‌های شبکه‌های اجتماعی، بخش ۷ مقایسه بات‌نت‌های شبکه‌های اجتماعی مختلف را عنوان می‌کنند، و در نهایت نتیجه‌گیری و بررسی کارهای آتی می‌پردازد.

۲- دلایل محبوبیت شبکه‌های اجتماعی برای بات-نت‌ها

در ابتدا دلایل استفاده از شبکه‌های اجتماعی از دید مدیربات‌ها مورد بررسی قرار می‌گیرد سپس دلایل محبوبیت شبکه‌های اجتماعی از دیدگاه بات‌های اجتماعی بیان می‌گردد.

دلایل محبوبیت شبکه های اجتماعی برای مدیر بات‌ها و بات‌نت‌ها به شرح زیر می‌باشند:

۱- زیر ساخت ارتباطات شبکه‌های اجتماعی می‌تواند، به عنوان کانال C&C بات‌نت‌ها، مورد استفاده قرار گیرد [11].

۲- تعداد کاربرانی که از شبکه‌های اجتماعی استفاده می‌کنند بسیار زیاد است و همین مورد پتانسیل بالقوه ای را برای بات‌نت‌ها جهت پخش لینک‌های بدافزارها، فراهم می‌آورد [11]. به عنوان مثال: Koobface با ارسال URL های مخرب و مبهم برای قربانی هایش در Facebook و Twitter قصد گسترش خود را دارد [12,11].

۳- هزینه پایین ارسال پیام در شبکه‌های اجتماعی توجه بسیاری از بات‌نت‌ها را برای پخش انواع هرزنامه ها در شبکه‌های اجتماعی جلب کرده است، که این مورد سود قابل توجهی را برای مدیر بات‌ها به همراه داشته است[10] . به عنوان مثال: تحقیقات در سال ۲۰۱۲ نشان داده است که 40% از اکانت های Facebook و Twitter و دیگر شبکه های اجتماعی محبوب، یک اکانت پخش کننده هرزنامه(آلوده به بات) هستند و 8% از کل پیام‌هایی که در شبکه‌های اجتماعی ارسال می‌شوند، هرزنامه هستند[10].

۴- توانایی بالای مخفی‌سازی بات‌نت‌های شبکه‌های اجتماعی[7,8]. به عنوان مثال: StegoBot ها این قابلیت را دارند تا اطلاعات را درون عکس ها مخفی کنند، به گونه‌ای که در عکس هیچ گونه تغییری ایجاد نشود[7,8].

۵- توانایی رمزگذاری دستورات به کمک الگوریتم های RSA یا MD5[1] در شبکه های اجتماعی و سخت شدن شناسایی آنها توسط محققان امنیتی[9]. به عنوان مثال:ASP2P، یک نمونه از بات‌نت‌های شبکه‌های اجتماعی است که از این تکنیک استفاده می‌کند[9].

۶- بات‌نت‌های شبکه های اجتماعی با تقلید رفتار کاربران عادی و داشتن آدرس IP معتبر، راه شناسایی خود را برای محققان امنیتی سخت و دشوار کرده است[6].

۷- ایجاد/خرید اکانت برای بات‌نت‌ها، توسط مدیربات‌ها کار آسانی است[10]. به عنوان مثال: خرید هزار حساب کاربری Twitter برای مدیر بات هزینه‌ای معادل ۵۷ دلار را به همراه دارد[10] .

۳- انواع بات‌نت‌های شبکه های اجتماعی

پس از شناسایی اولین بات اجتماعی در سال ۲۰۰۹، تلاش‌های محققان امنیتی منجر به شناسایی تعدادی از بات‌های اجتماعی گردید، البته تعدادی از بات‌های اجتماعی توسط خود محققان امنیتی ساخته شده است، که بعضی ویژگی‌های بات‌های معمولی و بات‌های اجتماعی را به ارث می‌برد. و هدف محققان بررسی ویژگی‌های جدید بات‌های ترکیبی بوده است.

در زیر به معرفی تعدادی از بات‌نت‌های شبکه‌های اجتماعی که تا به امروز کشف شده‌اند پرداخته شده است:

۱- Koobface
۲- ASP2P
۳- DR-SNBOT[2]
۴- SoCellBot
۵- StegoBot
۶- Wbbot
۷- SocialNetworkingBot
۸- Facebot
۹- Nazbot
۱۰- FaceCat

در ادامه اطلاعات بیشتری درباره‌ی این بات‌نت‌ها آمده است.

٤- روش های انتشار

در این قسمت به معرفی انواع روش‌های انتشار تعدادی از بات‌نت‌های شبکه-های اجتماعی پرداخته شده، و نحوه ی نفوذ این بات‌ها، به سیستم‌های کاربران عادی برای سوء استفاده از سیستم‌های آنها، بیان می شود.

۱- Koobface: این نوع بات اجتماعی با ارسال URL های مخرب و مبهم به قربانی هایش در Facebook و Twitter که اکانت آنها به خطر افتاده است و با هدایت قربانی به یک

صفحه جعلی در Facebook یا Twitter بدافزار را روی آنها نصب می‌کند. همچنین این نوع از بات‌های اجتماعی با استفاده از هرزنامه ها خود را گسترش می‌دهند[12,11,6].

۲- ASP2P: این نوع بات اجتماعی با رمزنگاری دستورات و با کمک ساختار سلسله مراتبی P2P ترکیبی[3] می‌توانند به سرعت منتشر شوند[9]. همچنین ASP2P ها با استفاده از هرزنامه آگاه به متن[4] و استفاده از پروتکل HTTP راه را برای انتشار خود هموار می‌کنند[9].

۳- SoCellBot: این نوع بات اجتماعی به دو طریق خود را می‌تواند گسترش دهد[13, 12]:

۱) سوء استفاده از آسیب پذیری سیستم‌عامل‌های گوشی‌های هوشمند نظیر: IOS، Android، Symbian .

۲) با نفوذ به بخش‌های به خطر افتاده‌ی گراف شبکه‌های اجتماعی، تعدادی پروفایل جعلی ایجاد می‌کند تا از این طریق کاربران عادی را آلوده نماید.

۴- StegoBot: این نوع بات اجتماعی توانایی پنهان کردن اطلاعات مخرب را در درون عکس دارند. به طوری که هیچ گونه تغییری در عکس ایجاد نشود، سپس با دانلود شدن این عکس توسط کاربر عادی، سیستم کاربر قربانی، آلوده به این نوع بات می‌شود[8]. همچنین StegoBotها با پخش URLهای مخرب در بین ایمیل های عادی می‌توانند خود را گسترش دهند[6].

۵- FaceCat: این نوع از باتها با سرقت کوکی‌های Facebook کاربرانی که از مرورگر IE استفاده می‌کنند، راه را برای ورود غیر مجاز خود به حساب‌های کاربری کاربران قربانی فراهم می‌آورند [7].

۶- Torping Botnet: این نوع بات با استفاده از راه‌اندازی به وسیله دانلود[5]، کاربران عادی را آلوده می‌کند [12].

۵- روش کاری و ویژگی‌های بات‌نت‌های شبکه-های اجتماعی

در ابتدا ویژگی‌های هر یک از بات‌های معرفی شده در بخش ۳، مورد بررسی قرار می‌گیرد، سپس نحوه سوء استفاده آنها از شبکه‌های اجتماعی و کاربران قربانی تشریح می‌گردد:

۱- Koobface: از کاربران شبکه‌های اجتماعی برای ایجاد حساب کاربری در این شبکه‌ها استفاده نموده و با استفاده از مهندسی اجتماعی خود را با کاربران قربانی دوست می‌کند، تا بدافزارها را از طریق ارسال هرزنامه بر روی آنها اجرا نماید[12]. مدیر بات‌ها از طریق HTTP پیام‌های رمزنگاری شده را به بات ها ارسال می‌کند. سپس باتها با رمزگشایی این پیام‌ها، جهت اتصال به سرورهای C&C متفاوت می بایست یک سری اجزای متفاوت را دانلود و اجرا نمایند. در نتیجه به کمک این اجزای متفاوت به سرور های متفاوت C&C متصل می‌شوند، تا به اجرای دستورات متفاوتی که شامل پخش URLهای، Koobface است بپردازند[6]. همچنین حوزه‌ی کاری Koobface در Facebook و Twitter می‌باشد.

۲- ASP2P: این نوع از باتنت‌ها با ترکیب ویژگی‌های مثبت شبکه-های اجتماعی و ساختار P2P ترکیبی ایجاد شده‌اند. ASP2P باتنت‌ها توانایی بالقوه‌ای در مخفی‌سازی دستورات در پروتکل HTTP دارند، درنتیجه راه را برای شناسایی خود، به حداقل رسانده‌اند. ASP2Pها از شبکه‌های آنلاین اجتماعی که سیاست ناامنی دارند به عنوان سرور C&C برای منتشر کردن دستورات رمزنگاری شده ی خود استفاده می‌کنند [9]. این نوع از بات-نت‌ها را می‌توان به دو دسته تقسیم کرد[9]: ۱) Server Bots ۲)Client Bots.

۱) Server Bots : دستورات را از سرور اصلی گرفته و همچون سروری این دستورات را به بات‌های مشتری یا بات‌های سرور ارسال می کنند.

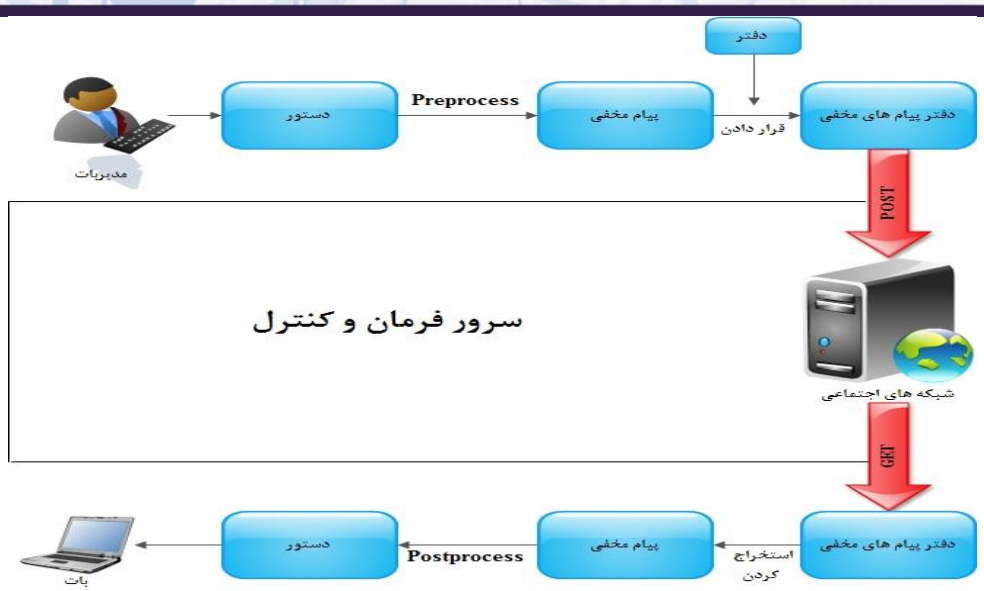
۲) Client Bots: دریافت دستورات از Server Botها و اجرای آنها. همچنین حوزه ی کاری ASP2Pها در Facebook و Twitter می-باشد.

۳- DR-SNBOT: در این نوع از باتنت‌ها، مدیر بات دستورات موجود در کانال C&C را برای اینکه مورد حمله پاسخ[6] و حمله‌ی مرد میانی[7] قرار نگیرد، با استفاده از الگوریتم RSA و AES رمزنگاری می‌کند. هنگامی که ترافیک شبکه های اجتماعی بالا می‌رود، مدیربات ها دستورات را داخل یک عکس یا فیلم مخفی می‌کند و به سرورهای C&C(که در داخل شبکه های اجتماعی قرار دارند) ارسال می‌کند[14]. درشکل۱ دو مرحله کلیدی آن را نشان می‌دهد[14]:

۱)پیش پردازش: در ابتدا مدیربات یک برچسب زمانی را به دستور می-چسباند، سپس دستور و برچسب زمانی را با استفاده از الگوریتم های AES و RSA، رمزنگاری کرده و امضاها را به متن رمزنگاری شده چسبانیده و پیام مخفی را تولید می‌کند.

۲) پس پردازش : بات پیام را دریافت کرده و با استفاده از کلید عمومی RSA، امضاهای متن رمزگذاری شده را تایید نموده و سپس با رمزگشایی آن، برچسب زمانی دستور مورد نظر را بررسی می‌کند و این برچسب زمانی، زمان حمله یا سرقت اطلاعات را برای بات مشخص نموده، و با توجه به این برچسب زمانی، بات دستور را اجرا می‌نماید.

۴- SoCellBot: یک نوع موبایل باتنت جدید است که برای ارتباطات C&C، از شبکه‌های اجتماعی استفاده می‌کند. همچنین این نوع از باتنت‌ها با رمزگذاری پیام‌های ارسالی جلوی شناسایی سریع خود را می‌گیرند. استفاده از شبکه‌های اجتماعی جهت ارسال پیام صرفه‌ی اقتصادی را برای این نوع از باتنت‌ها، در مقایسه با موبایل باتنت‌هایی که جهت ارسال پیام از SMS استفاده می‌کنند، به همراه داشته است[13,12]. از طرفی ساختار پرخوشه‌ی گراف شبکه‌های اجتماعی، سبب شده است تا توپولوژی این نوع از باتنت-های اجتماعی در برابر خرابی و از دسترس خارج شدن خیلی انعطاف پذیر و مقاوم شود[13]. حوزه‌ی کاری SoCellBotها، Facebook می‌باشد.



شکل(۱): مراحل مختلفی که پیام طی می کند تا به دست بات مورد نظر برسد[14].

۵- StegoBot: این نوع از باتنت‌ها، عکس‌های Facebook را سرقت، و اطلاعات مهم را در داخل این عکس‌ها مخفی می‌کنند، به گونه‌ای که عکس‌ها هیچ گونه تغییری نمی‌کنند[8,7] . علاوه بر مدیریت، باتنت‌ها هم این توانایی را دارند، تا با پنهان کردن اطلاعات در داخل عکس‌ها، آنها را ارسال نمایند. این نوع از باتنت‌ها توانایی انجام فعالیت‌های زیر را دارند[8]: ۱) سرقت آدرس‌های پست الکترونیک. ۲) سرقت رمزها و اطلاعات کارت‌های اعتباری. ۳) ضبط کلیدهای فشرده شده در صفحه کلید.

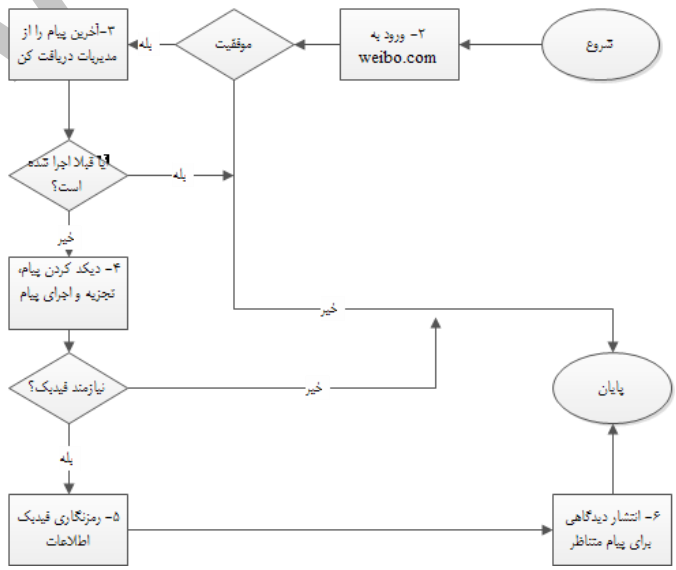
لازم به ذکرست که StegoBotها با ایجاد کانال‌های مخفی، و پنهان سازی اطلاعات در داخل عکس‌ها، شناسایی و ردیابی ارتباطات خود را برای محققان امنیتی به حداقل رسانده‌اند[7]. همچنین حوزه کاری StegoBotها، Facebook می‌باشد.

۶- Wbbot: این نوع از باتها بر پایه Sina Weibo طراحی و ساخته شده اند. با توجه به رفتار این گونه از باتها آنها را می توان به دو دسته تقسیم کرد[6]: ۱) مبتنی بر میزبان. ۲) مبتنی بر شبکه‌های اجتماعی.

در شکل ۲ جزئیات جریان کنترل Wbbotها بر روی میزبان نشان داده شده است.

7- SocialNetworkingBot: مدیریت توئیت‌هایی را به بات-هایش ارسال می‌کند، که این توئیت‌ها شامل دستورات مخربی هستند. سپس باتها با توجه به دستورات، حملات مخربی نظیر: مرور صفحات وب[8]، حملات DOS [9] را اجرا کرده، و فایل‌ها یا اطلاعات سیستم قربانی را، به مدیریت ارسال می‌کنند[12]. همچنین حوزه ی کاری این باتهای اجتماعی، Twitter می‌باشد

8- Facebot: این نوع بات اجتماعی با سوء استفاده از نرم افزارهای مشروع Facebook، حملات DDOS ای را بر روی میزبان قربانی تدارک می‌بینند[7]. این نوع از باتنت‌ها توانایی سرقت اطلاعات حساس کاربران، نظیر پسوردها را دارند. Facebotها با پنهان‌سازی اطلاعات مهم در داخل عکس های پروفایل کاربران، زمینه را برای ایجاد ارتباط C&C فراهم می-آورند. بعد از پروسه مخفی‌سازی، بات و مدیریت به یک گروه Facebook



شکل(۲): جزئیات جریان کنترل Wbbotها بر روی میزبان[6].

می‌پیوندند، سپس مدیربات عکس های پروفایل کاربران جدید این گروه را اسکن می‌کند، و با رمزگشایی این عکس ها به اطلاعات حساس موجود در آنها دست می‌یابد[6]. حوزه کاری Facebotها، Facebook می باشد.

9- Nazbot: مدیربات‌ها پیام ها را رمزگذاری(Base64-encoded) کرده، سپس آنها را به سمت بات‌نت‌ها ارسال می‌کند. بات‌ها ابتدا متن را رمزگشایی کرده، سپس با توجه به URLهای موجود در متن فایل های مخرب را دانلود و اجرا می‌کنند، در نهایت بات‌ها اطلاعات سرقت شده‌ی کاربران را از طریق HTTP به سرور کنترل شونده توسط مدیربات ارسال می‌کنند[6].

10- FaceCat: حوزه کاری این نوع بات Facebook می‌باشد و از آن به عنوان سرور C&C استفاده می‌کند[7].

٦- روش های مقابله باتنت‌ها در برابر شناسایی و ابزارهای شناسایی بات نت‌های شبکه‌های اجتماعی

در این قسمت ابتدا انواع روش‌هایی که باتهای اجتماعی و مدیربات‌ها برای مخفی ماندن خود انجام می‌دهند بیان می‌شود، سپس روش‌ها و ابزارهایی که می توان برای شناسایی این گونه از باتها مورد استفاده قرار داد، معرفی می-گردند.

۱- ASP2P: این نوع از باتنت‌ها برای جلوگیری از شناسایی خودشان، اقدامات زیر را انجام می دهند[9]:

۱) تعداد Server Botهایی که به عنوان سرور انتخاب می‌شوند بیشتر از یکی است.

۲) در اطراف هر بات یک مجموعه حسگرهایی وجود دارد، که این حسگرها وظیفه پاک سازی آثار به جامانده از باتنت‌ها را دارند. و معمولا با به پایان رسیدن ارتباطات باتنت‌ها با مدیربات، حسگرها شروع به پاک سازی آثار باتنت‌ها می کنند.

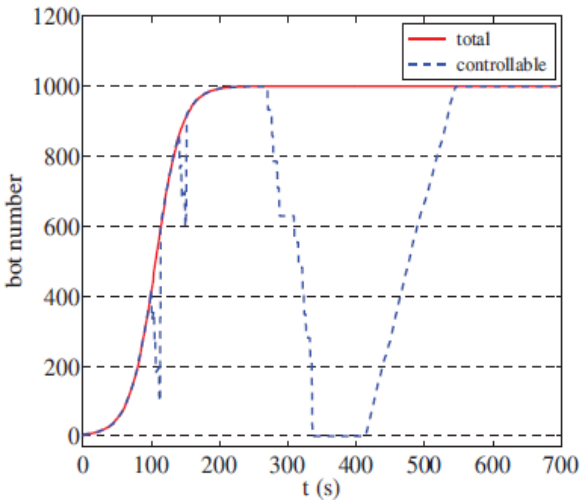
۳) وقتی که یک حسگر توسط محققان امنیتی یا مهاجمان شناسایی شد، مدیربات با ارسال دستور جدید به باتهایش، آنها را از قرارگیری در مکان حسگر مورد نظر یا پاسخ به این حسگر باز می‌دارد.

۴) باتها از ارسال اطلاعات به حسگر مورد نظر خودداری می کنند، حتی اگر دستوری از طرف این حسگر به باتها ارسال شده باشد.

Lei Cao و همکارش نشان دادند که بدلیل رفتار مخفیانه ASP2Pها میزان استفاده آنها از پردازنده کم، و مصرف حافظه و ترافیک تولید شده توسط این نوع باتنت‌ها پایین است[9]. به دلیل کارایی بالای این نوع باتها در برابر فروپاشی، باید از روش شناسایی مبتنی بر ناهنجاری استفاده کرد[9].

۲- DR-SNBOT: در این نوع از باتنت‌ها، مدیربات با تعریف یکسری حدهای آستانه در کنار باتها، سعی می‌کند تا باتهای خود را هر وقت که خواستند از این حدود تجاوز کنند، بالانس نماید، تا جلوی شناسایی آنها توسط محققان امنیتی گرفته شود. همچنین با کمک این حدهای آستانه یک بات می تواند متوجه شود که چه تعداد از باتهای همسایه‌اش از کار افتاده است و اگر تعداد باتهای از کار افتاده از یک حد آستانه عبور کند، بات مورد نظر خود را از کار می‌اندازد[14].

Tao Yin و همکارانش نشان دادند، که با از کار انداختن تمامی سرورهای C&C در یک زمان کوتاه توسط محققان امنیتی، باتها از کنترل خارج شده ولی بعد از مدت کوتاهی مجددا تمامی باتها به صورت تصادفی، به سرورهای C&C موجود متصل می‌شوند. سپس تمامی باتها تحت کنترل خواهند بود[14]. با توجه به شکل ۳ سوالی مطرح می شود، که چطور امکان دارد، باتها به سرورهای C&C موجود متصل شوند در حالی که تمامی سرورها از کار افتاده‌اند. محققان امنیتی برای شناسایی DR-SNBOTها از روش هانی‌پات[10] استفاده می‌کنند، هر چند که این روش برای شناسایی DR-SNBOTها با چالش هایی رو به رو می‌شود[14].



شکل(۳): رفتار بات ها را بعد از کار انداختن سرورهای C&C [14].

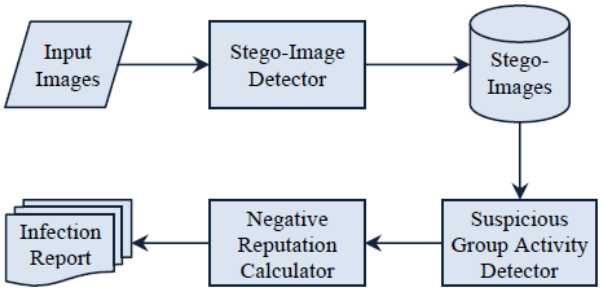
۴- SoCellBot: توپولوژی SoCellBot بدلیل تعداد خوشه های زیاد شبکه های اجتماعی، بات ها را در برابر خرابی و از دسترس خارج شدن مقاوم می‌کند[13]. با تجزیه و تحلیل و شبیه سازی رفتار این گونه از باتنت‌ها و اجرای گراف سنتز، که پردازش تمامی مشخصات یک شبکه‌ی اجتماعی را شامل می‌شود به شناسایی این گونه از باتهای اجتماعی می‌پردازد[13].

۵- StegoBot: قندی و همکارش نشان دادند که این نوع از باتنت‌ها با استفاده از کانال پنهان و پنهان سازی اطلاعات در داخل عکس و ویدئو زمینه کشف و شناسایی خود را به حداقل می‌رسانند[7].

این نوع از باتنت‌ها را با استفاده از SocialClymene می توان با نرخ بالا شناسایی کرد[7]. SocialClymene شامل سه جزء اصلی است[7]: ۱) کشف کننده Stego-image. ۲) کشف کننده فعالیت های گروه های مشکوک. ۳) محاسبه ی سوابق منفی کاربران. شکل ۴ معماری SocialClymene را نشان می دهد.

5- Wbbot :Yuede Ji و همکارانش با ایجاد Wbbot، سیستمی را برای شناسایی Wbbotها معرفی کردند که از سه جزء تشکیل شده است[6]: ۱) نظارت بر رفتار میزبان. ۲) تجزیه و تحلیل رفتار میزبان. ۳) روش شناسایی.

برای شناسایی Wbbotها، ابتدا درخت رفتارهای مشکوک ساخته می‌شود، سپس آن را با کتابخانه ای که ویژگی‌های Wbbot را دارد مقایسه کرده و



شکل(٤):معماری SocialClymene [7].

در صورت یافت شدن ویژگی‌های مشترک (بین درخت و کتابخانه) یک Wbbot کشف می‌شود. هر چند که نرخ False-Negative این روش خیلی زیاد است(31.8%).

۷- مقایسه بات‌های اجتماعی مختلف

در زیر به بررسی مزایا و معایب تعدادی از بات‌های اجتماعی بخش 3 پرداخته شده است.

۱- ASP2P: مزایا : ۱)استحکام زیاد در برابر حذف Server Botها (اگر 80% از Server Botها حذف شوند فروپاشی هنوز رخ نمی‌دهد.). ۲) میزان بهره‌وری ASP2P از پردازنده پایین است. ۳) میزان حافظه استفاده شده توسط ASP2Pها پایین است. ۴) ترافیک مصرفی توسط ASP2P در مقایسه با بات‌نت‌های همتا به همتا پایین است.

۲- DR-SNBOT: مزایا: ۱) رمزنگاری دستورات. ۲) مخفی سازی اطلاعات درون عکس یا فیلم. ۳) مکانیزم بازیابی خودکار DR-SNBOTها بعد از قطع ارتباط آنها با سرورهای C&C.

معایب: ۱) هر سرور C&C یک محدودیت بار دارد، که این محدودیت را یک حد آستانه مشخص می‌کند. ۲) از طریق مهندسی معکوس NGA[11] می‌توانیم به تمامی لقب‌ها و نام‌های مستعاری که DR-SNBOTها برای مخفی‌سازی خود تولید کرده اند، دست یابیم. ۳) با استفاده از روش هانی‌پات می‌توان سرور C&C، DR-SNBOTها را شناسایی کرد.

۳- SoCellBot: مزایا: ۱) توپولوژی قدرتمند SoCellBot. ۲) بار ترافیک پایین. ۳) سرعت انتشار بالا. ۴) قابلیت دسترسی زیاد. ۵) شناسایی سخت SoCellBotها. ۶) صرفه اقتصادی. که موارد ۶-۲ در مقایسه با موبایل بات‌نت‌هایی است، که از پیامک استفاده می‌کنند.

عیب: ارسال بیشتر پیام در ERG[12]، نسبت به شبکه های اجتماعی اصلی، که زمینه شناسایی SoCellBot را فراهم می‌آورد.

۴- Stego-Bot: مزایا: ۱) مخفی کردن اطلاعات حساس در عکس ها. ۲) الگوی ارتباطی متفاوت بدلیل طراحی و پیاده سازی متفاوت آنها. ۳) استفاده از کانال پنهان.

عیب: نرخ شناسایی بالا توسط Social Clymene.

جداول ۱ و ۲ مقایسه بات‌نت‌های شبکه‌های اجتماعی محبوب را نشان می‌دهند.

8- نتیجه گیری و کارهای آتی

در این مقاله ابتدا به معرفی تعدادی از بات‌نت‌های اجتماعی و نحوه‌ی نفوذ این نوع از بدافزارها به حساب کاربران عادی، پرداخته شد. و با آشنایی از سوء استفاده‌هایی که این نوع از بات‌نت‌ها، از شبکه‌های آنلاین اجتماعی می‌کنند، راهکارهایی جهت مقابله با این نوع از بدافزارها معرفی گردید. هر چند که بات‌نت‌های شبکه‌های اجتماعی همواره راه‌هایی را برای جلوگیری از شناسایی خود مورد استفاده قرار می‌دهند، با این وجود روش‌های معرفی شده با نرخ بالایی، توانایی شناسایی بات‌نت‌های شبکه‌های اجتماعی را دارند.

پیشنهاد می شود در کارهای آتی، نحوه ی ارتباط بات‌نت‌های شبکه‌های اجتماعی با موبایل بات‌نت‌ها مورد بررسی قرار گیرد.

مراجع

[۱] M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, S. Entwisle, B. Graveland, D. McKinney, J. Mulcahy, and C. Wueest, "Symantec Global Internet Security Threat Report: Trends for 2009", Technical Report, Symantec Corporation, 2010.

[2] B. AsSadhan, J. Moura, D. Lapsley, C. Jones, and W. Strayer, "Detecting botnets using command and control traffic", Eighth IEEE International Symposium on Network Computing and Applications, 2009. NCA, 2009, pp. 156–162.

جدول(۱): مقایسه بات‌نت‌های سایر شبکه های اجتماعی محبوب

بات‌نت	روش کاری و ویژگی‌ها	روش‌ها و ابزارهای شناسایی	راه‌های جلوگیری از شناسایی
DR-SNBOT	رمزنگاری دستورات و مخفی کردن آنها در داخل عکس یا فیلم	شناسایی بر اساس روش Honeypot	تعریف حدهای آستانه برای بات‌ها، اتصال بات‌ها به طور تصادفی به سرورهای C&C بعد از دسترس خارج شدن آنها
Wbbot	سرقت اطلاعات خصوصی کاربران	استفاده از روش Tree-based و ساخت درخت رفتارهای مشکوک	----------
Nazbot	رمزنگاری دستورات، دزدیدن اطلاعات حساس کاربران	----------	----------

جدول (۲): مقایسه بات‌نت‌های شبکه‌های اجتماعی Facebook و Twitter

حوزه کاری	راه‌های جلوگیری از شناسایی	روش‌ها و ابزارهای شناسایی	روش کاری و ویژگی ها	روش های انتشار	بات‌نت
Facebook و Twitter	----------	----------	ارسال Spamهایی که حاوی بدافزار است	ارسال URL مخرب و مبهم	Koobface
Facebook و Twitter	افزایش Servent botها، پاک سازی آثار بات‌ها جلوگیری از پاسخ و قرارگیری در محل، سنسور شناسایی شده	شناسایی مبتنی بر ناهنجاری	استفاده از OSNها به عنوان سرور C&C	رمزنگاری دستورات، ساختار Hybrid-P2P	ASP2P
Facebook	تعداد خوشه‌های زیاد OSN ها	با اجرای گراف سنتز	استفاده از OSNها به عنوان سرور C&C،رمزنگاری دستورات، مقاوم در برابر خرابی و از دسترس خارج شدن	سوء استفاده از باگ های سیستم عامل، ایجاد اکانت های جعلی	SoCellBot
Facebook	استفاده از Covert Channel و پنهان سازی اطلاعات در داخل عکس و ویدئو	با استفاده از روش SocialClymene	سرقت عکس و قرار دادن اطلاعات درون آن، سرقت ایمیل آدرس، پسوردها و...	پخش URLهای مخرب، پنهان سازی اطلاعات در عکس‌ها	StegoBot
Twitter	----------	----------	توییت هایی شامل دستورات مخرب برای انجام حملات مخرب	----------	SocialNetworkingBot
Facebook	----------	----------	سرقت اطلاعات حساس کاربران، پنهان سازی اطلاعات در عکس ها، سوء استفاده از نرم‌های Facebook	----------	Facebot
Facebook	----------	----------	استفاده از Facebook به عنوان سرور C&C	سرقت کوکی های Facebook و سوء استفاده از آنها	FaceCat

[۱۲] Sebastian, Silpa, Sonal Ayyappan, and P. Vinod. "Framework for design of Graybot in social network." *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014.
[۱۳] Faghani, Mohammad Reza, and Uyen Trang Nguyen. "Socellbot: A new botnet design to infect smartphones via online social networking." *Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on*. IEEE, 2012.
[۱۴] Yin, Tao, Yongzheng Zhang, and Shuhao Li. "DR-SNBot: A Social Network-Based Botnet with Strong Destroy-Resistance." *Networking, Architecture, and Storage (NAS), 2014 9th IEEE International Conference on*. IEEE, 2014.

زیر نویس‌ها

[1] Message-Digest
[2] Destroy-Resistance Social Network Bot
[3] Hybrid P2P
[4] Context-Aware Spam
[5] Drive-By-Download
[6] Replay Attack
[7] Man-In-The-Middle Attack
[۸] Browsing Webpage
[9] Dos Attack
[۱۰] Honeypot
[11] Nickname Generation Algorithm
[12] Equivalent Random Graph

[3] J. Govil and J. Govil, "Criminology of botnets and their detection and defense methods", International Conference on Electro/Information Technology, IEEE, 2007, pp. 215-220.
[4] Tyagi, Amit Kumar, and G. Aghila. "Detection of fast flux network based social bot using analysis based techniques." *Data Science & Engineering (ICDSE), 2012 International Conference on*. IEEE, 2012.
[5] G. Gu, V. Yegneswaran, P. Porras, J. Stoll, and W. Lee, "Active botnet probing to identify obscure command and control channels", Annual Computer Security Applications Conference, IEEE, 2009, pp. 241-253.
[۶] Ji, Yuede, et al. "Towards Social Botnet Behavior Detecting in the End Host."
[7] Ghanadi, Mansoureh, and Mahdi Abadi. "SocialClymene: A negative reputation system for covert botnet detection in social networks." *Telecommunications (IST), 2014 7th International Symposium on*. IEEE, 2014.
[۸] Natarajan, V., Shina Sheen, and R. Anitha. "Multilevel Analysis to Detect Covert Social Botnet in Multimedia Social Networks." *The Computer Journal*(2014): bxu063.
[۹] Cao, Lei, and Xiaofeng Qiu. "ASP2P: An advanced botnet based on social networks over hybrid P2P." *Wireless and Optical Communication Conference (WOCC), 2013 22nd*. IEEE, 2013.
[10] Zhang, Jinxue, et al. "On the impact of social botnets for spam distribution and digital-influence manipulation." *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 2013.
[۱۱] Yan, Guanhua. "Peri-Watchdog: Hunting for hidden botnets in the periphery of online social networks." *Computer Networks* 57.2 (2013): 540-555.