پنصلنامه علمی-ترویجی پدافند غیرعامل

سال سوم، شماره ۲، تابستان ۱۳۹۱، (پیاپی ۱۰): صص ۵۷-۶۵

بات‌نت و حملات آن

تیمور سلیمی [۱]، مهدی دهقانی [۲]

تاریخ دریافت: ۹۱/۰۳/۱۲
تاریخ پذیرش: ۹۱/۰۵/۰۸

چکیده

بات‌نت‌ها در میان انواع مختلف بدافزار، به‌عنوان تهدیدی بسیار جدی علیه امنیت سایبری مطرح شده‌اند و برای اهداف مخربی چون انتشار هرزنامه، حملات انکار سرویس توزیع شده، سرقت اطلاعات محرمانه و سرقت هویت به‌کار می‌روند. بات‌نت‌ها توسط مهاجمان و از راه دور هدایت می‌شوند و اعضای آن‌ها در منازل، مدارس، شرکت‌ها و سازمان‌های سراسر جهان وجود دارند. ویژگی برجسته بات‌نت‌ها استفاده از کانال‌های فرماندهی و کنترل است که از طریق آن‌ها به‌روز شده و هدایت می‌گردند. بررسی بات‌نت و حملات آن و نیز روش‌های مقابله و تشخیص آن‌ها، مربوط به پدافند غیرعامل در حوزه امنیت فناوری اطلاعات می‌باشد و یکی از جنبه‌های اهمیت آن، حملات اخیر سایبری علیه کشورمان است که عمدتاً دارای ویژگی شبکه‌های بات هستند. در این تحقیق، ابتدا بات‌نت و مفاهیم مرتبط با آن معرفی می‌شود، سپس روش‌های فرماندهی و کنترل بات‌نت مطرح شده و با هم مقایسه می‌گردند. در ادامه، مهم‌ترین حملات و عملیات مخرب بات‌نت‌ها مطرح گردیده و به جدیدترین اهداف آن‌ها اشاره شده است، سپس تعدادی از حملات سایبری خصوصاً علیه زیرساخت‌های کشورمان بررسی شده و با توجه به مطالب تحقیق، درباره شباهت آن‌ها به حملات بات‌نت، مباحثی ارائه شده است و در پایان، نتیجه‌گیری و پیشنهادها مطرح گردیده است.

کلیدواژه‌ها: بات‌نت، بات، سرور فرماندهی و کنترل، حمله انکار سرویس توزیع شده، حمله سایبری

۱- دانش‌آموخته کارشناسی ارشد مهندسی فناوری اطلاعات- گرایش امنیت- دانشگاه جامع امام حسین(ع) salami.84@gmail.com- نویسنده مسئول
۲- دانشجوی دکتری کامپیوتر- نرم افزار mdehghany@ihu.ac.ir

۱- مقدمه

«بات‌نت»[1] شبکه‌ای از رایانه‌های آلوده متصل به اینترنت است که تحت کنترل سرور فرماندهی و کنترل[2] قرار دارد و برای حملات انکار سرویس[3]، فرستادن هرزنامه و عملیات مخرب دیگر مورد استفاده قرار می‌گیرد. ممکن است بات‌نت‌ها دارای کارکردهای قانونی نیز باشند، ولی در اغلب موارد بافعالیت‌های مجرمانه برای انتشار هرزنامه، بدافزار یا حملات سرقت هویت در ارتباط‌اند[۱]. اندازه یکبات‌نت، به پیچیدگی و تعداد کامپیوترهای استخدام‌شده در آن بستگی دارد. معمولا کاربران کامپیوترها از این موضوع که سیستم‌هایشان از راه دورکنترل شده و مورد سوءاستفاده قرار می‌گیرند اطلاعی ندارند . بات‌نت‌ها برای مجرمان اینترنتی جذاب هستند، زیرا این قابلیت را دارند که برای جرائم مختلف مجددا تنظیم شوند، برای سرویس‌های میزبانی جدید تغییر مکان پیدا کنند، ودر پاسخ به پیشرفت‌های جدید امنیتی دوباره برنامه‌ریزی گردند.

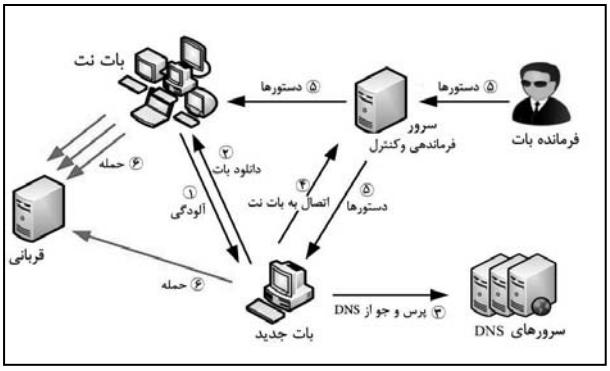
بات‌نت‌ها جهت جلوگیری از شناسایی شدن‌شان، سعی می‌کنند در مقیاس‌های بزرگی ایجاد شوند، یعنی تعداد کامپیوترهایی که به این گروه می‌پیوندند زیاد می‌باشد. همچنین اندازه باتنت یا تعداد میزبان‌هایی که مورد سوءاستفاده قرار گرفته‌اند، عامل بالقوه‌ای برای ارسال هرزنامه و حملات انکار سرویس توزیع شده[4] فراهم می‌کند[۳]. در قیاس باتنت با بدافزارهای موجود، مانند کرم و ویروس، وجود کانال‌های فرماندهی و کنترل، تفاوت کلیدی است؛ چون بات‌ها تحت کنترل مهاجم، دستور را دریافت و رفتارهای مخرب انجام می‌دهند[۶]. امروزه با به وجودآمدن امکاناتی که در فضای سایبر وجود دارد، تولید و به‌کارگیری بات‌نت‌ها آنقدر آسان شده است که هر فردی می‌تواند با استفاده از ابزارهای مخصوص، باتنت موردنظر خود را به نحو دلخواه طراحی کند و از آن استفاده نماید. ممکن است بات‌نت‌ها توسط دولت‌ها یا سازمان‌ها و شرکت‌های وابسته به آن‌ها، برای مقاصد سیاسی یا اقتصادی علیه کشورهای رقیب به‌کار روند. بات‌نت‌ها در کنار سایر بدافزارها، از ابزارهای نبرد اطلاعاتی هستند.

در ادامه این مقاله، مفاهیم مرتبط با باتنت معرفی می‌گردد و تاریخچه، سیر تکامل و چرخه زندگی باتنت بیان می‌شود. روش‌های فرماندهی و کنترل مطرح شده و باهم مقایسه می‌شوند، سپس به مهم‌ترین حملات و کارکردهای مخرب بات‌نت‌ها پرداخته می‌شود. نمونه‌هایی از بات‌نت‌های موجود نیز معرفی شده‌اند. در ادامه به روش‌های مقابله و تشخیص باتنت اشاره شده است و با استفاده از آمارهای اخیر[۸]، درباره وضعیت فعلی بات‌نت‌ها و اهداف جدید آن‌ها یک جمع‌بندی ارائه می‌شود. سپس تعدادی از حملات سایبری خصوصاً علیه زیرساخت‌های کشورمان بررسی شده و با توجه به مطالب تحقیق، درباره شباهت آن‌ها به حملات باتنت، مباحثی ارائه شده است. در نهایت، نتیجه‌گیری و پیشنهادها مطرح گردیده است.

۲- معرفی باتنت و مفاهیم مرتبط با آن

با توجه به شکل (۱) مفاهیم مرتبط به باتنت شرح داده می‌شوند:

بات[5]: کلمه بات از کلمه روبات[6]مشتق شده است. بات‌ها طراحی شده‌اند تا برخی از توابع از قبل تعریف شده را به‌صورت خودکار انجام دهند. به عبارت دیگر، بات‌های منفرد برنامه‌های نرم‌افزاری هستند که روی رایانه میزبان اجرا می‌شوند و موجب می‌گردند مهاجم فعالیت‌های میزبان را از راه دور کنترل کند[۲]. برخی اوقات به جای کلمه بات اصطلاح زامبی[7] به‌کار برده می‌شود.



شکل ۱- چرخه زندگی و ساختار یک باتنت برپایه IRC [۹]

بات دو مورد استفاده دارد:

- کارکرد خوب که به‌عنوان عامل‌های هوشمند در موتورهای جستجو و بازی‌های آنلاین مورد استفاده قرار می‌گیرد.
- کارکرد بد که در سرقت اطلاعات، حملات ممانعت از سرویس، ارسال هرزنامه و دیگر حملات کاربرد دارند و به مفهوم برنامه‌های نرم‌افزاری هستند بر روی رایانه قربانی اجرا می‌شوند و کنترل کامل فعالیت‌های میزبان را بدون اینکه میزبان از این موضوع اطلاعی داشته باشد به‌صورت از راه دور در اختیار مهاجم قرار می‌دهند[۳]. در این مقاله منظور از بات همان کارکرد بد آن است.

بات‌نت: بات‌نت شبکه‌ای از رایانه‌های آلوده به نام بات‌ها استکه تحت کنترل مهاجم قرار دارند و برای حملات انکار سرویس توزیع شده، کلاهبرداری، تقلب کلیک و انتشار بدافزارها، مورد استفاده قرار می‌گیرند. باتنت را ارتش زامبی‌ها نیز می‌گویند [۲و۱۱].

سرور فرماندهی و کنترل: بات دستورات خود را از سرور فرماندهی و کنترل که توسط مهاجم هدایت می‌شود، دریافت می‌نماید. استفاده

1- Botnet
2- Command and Control Server
3- Denial of Service
4- Distributed Denial of Service
5- Bot
6- Robot
7- Zombie

از این سرور موجب گمنامی مهاجم می‌شود تا به راحتی قابل ردیابی نباشد.

فرمانده بات یا مهاجم[1]: مهاجم به فردی گفته می‌شود که تمامی کارهای یک شبکه باتنت - از ایجاد تا کنترل - را به‌دست دارد؛ بدین ترتیب که بات را پیکربندی و پیاده‌سازی می‌نماید، سپس بات را بر روی سیستم قربانی نصب کرده و در نهایت، بات‌ها را از طریق کانال کنترلی هدایت و رهبری می‌کندو دستورهای حمله را صادر می‌نماید.

IRC[2]: یک سیستم گفتگو است که یک ارتباط یک به یک یا یک به چند را در اینترنت برای رد و بدل کردن پیامهای فوری ارائه می‌دهد[۳].

۲-۱- تاریخچه و سیر تکامل باتنت

از نظر تاریخی می‌توان ریشه‌های بات را از زمان بات اگدراپ[3] ردیابی نمود که توسط فیشر در سال ۱۹۹۳ به‌عنوان ابزاری جهت مدیریت کانال IRC ساخته شد و کار مانیتور کردن کانال را بر عهده داشت. این بات در آن زمان به‌عنوان یک بات غیر مخرب IRC به‌طور گسترده‌ای مورد استفاده قرار گرفت. اما پس از آن بات‌های IRC با اهداف بسیار مخرب به‌وجود آمدند. اولین بات مخرب، جی‌تی‌بات[4] بود که در سال ۱۹۹۸ شناسایی شد. امروزه حداقل یکصد نوع از این بات در اینترنت موجود می‌باشد.

پرتی‌پارک[5] اولین کرمی بود که در سال ۱۹۹۹توسعه پیدا کرد تا از IRC به‌عنوان وسیله‌ای جهت کنترل از راه دور استفاده کند. در سال ۲۰۰۲ منبع کد آگوبات[6] در بسیاری از وب‌سایت‌ها منتشر شد.

جدول ۱- سیر تاریخی تکامل باتنت ها [۴]

نام باتنت	اگدراپ	جی‌تی بات	پرتی پارک	آگوبات	اسلپر	اس‌دی بات
تاریخ شناسایی	۱۹۹۳	۱۹۹۸	۱۹۹۹	۲۰۰۲	۲۰۰۲	۲۰۰۲
نام باتنت	اسپای بات	ساینت	فتبات	جایوبات	نوگوچه	پیکام
تاریخ شناسایی	۲۰۰۳	۲۰۰۳	۲۰۰۴	۲۰۰۴	۲۰۰۶	۲۰۰۷

1- Botmaster
2- Internet Rellay Chat
3 -Eggdrop
4- GT-Bot(Global Threat Bot)
5- PrettyPark
6- AgoBot

اسلپر[7] اولین کرمی بود که از پروتکل ارتباطاتی نظیر به نظیر[8] استفاده کرد و در سال ۲۰۰۲ پدیدار گشت. اس‌دی بات[9] در سال ۲۰۰۲ ظاهر شد. انواع دیگر اس‌دی باتبرای کارایی بهتر از کلاینت IRC متعلق به خود استفاده می‌کردند. در قیاس با آگوبات، کد نوشته شده در اس‌دی باتکه به زبان C است ساده‌تر و کوتاه‌تر است. اسپای‌بات[10] در سال ۲۰۰۳ ظاهر شد. ساینت[11] قدیمی‌ترین بات نظیر به نظیر مخرب است که از پویش تصادفی برای یافتن اعضاء استفادهمی‌کند و در سال ۲۰۰۳ پدیدار شد. فتبات[12] یکی دیگر از بات‌های نظیر به نظیر است. در سال ۲۰۰۶ ظهور نوگوچه[13] به‌طور گسترده‌ای در ضد ویروس و بدافزار مستند شد. در سال ۲۰۰۷ بات پیکام[14] پدیدار شد که از نوع نظیر به نظیر است. جدول (۱) سیر تاریخی تکامل باتنت را نشان می‌دهد[۴].

باتنت‌های اولیه غالبا با زبان‌های C یا C++ و دلفی پیاده‌سازی شده‌اند و پروتکل مورد استفاده در آن‌ها بیشتر IRC و گاهی پروتکل نظیر به نظیر است. باتنت‌های اخیر با زبانهای VC++ و PHP پیاده‌سازی شده‌اند و پروتکل‌های مورد استفاده در آن‌ها HTTP و نظیر به نظیر است.

۲-۲- چرخه زندگی باتنت

فرایند ایجاد باتنت به حداقل مهارت‌های برنامه نویسی و تکنیکی نیازمند است. حتی تعدادی برنامه آموزشی برای ایجاد، انتشار و استفاده از باتنت ارائه می‌شود. کد بات دارای اجزایی است که قابلیت پیکربندی و اعمال تنظیمات دلخواه مهاجم را دارد. این اجزاء عبارت‌اند از: اطلاعات سرور فرماندهی و کنترل، اطلاعات کانال ارتباطی، پورت سرویس TCP از راه دور، مکان و نام فایل کد بات که بر روی ماشین آلوده قرار دارد و اجزایی که به مهاجم این امکان را می‌دهد تا به‌صورت پویا حمله را تغییر دهد و لیست حمله کنندگان و اطلاعات مربوط به آن‌ها را پنهان سازد.

مراحل مختلف چرخه زندگی یک باتنت معمولی به‌طور خلاصه در شکل (۱) نشان داده شده است. باتنت معمولاً قربانیان جدید را با بهره‌برداری از آسیب‌پذیری ماشین قربانی به‌دست می‌آورد و با استفاده از برنامه‌هایی همچون ویروس‌ها[15] و کرم‌ها[16] که با روش‌هایی مثل ارسال پست‌های الکترونیک بر روی اینترنت پخش می‌کند، رایانه‌های قربانیان را آلوده می‌نماید. هنگامی که آلودگی انجام

7- Slapper
8- Peer to Peer
9- SDbot
10- Spybot
11- Sinit
12- Phatbot
13- Nugache
14- Peacomm
15- Virus
16- Worm

می‌شود، قربانی یک اسکریپت مشخص را به‌عنوان شل‌کد[1] اجرا کرده و برنامه بات را دریافت می‌کند. برنامه بات خودش را روی قربانی نصب نموده و به‌طور خودکار اجرا می‌شود. بات جدید با سرور DNS تماس می‌گیرد تا آدرس IP سرور IRC را به‌دست آورد، سپس برنامه بات یک کانال فرماندهی و کنترل ایجاد کرده و بات را به کانال فرماندهی و کنترل متصل می‌کند. اکنون بات عضوی از بات‌نت است. سپس بات به‌طور خودکار می‌تواند محتوای کانال را تجزیه و اجرا کند که حاوی دستورات پیش فرض است. زمانیکه بات بر روی ماشین قربانی نصب می‌شود، با استفاده از کلمه کلیدی یکتای خود به‌عنوان بخشی از شبکه مهاجمبه کانال وصل می‌شود و منتظر رسیدن دستورات می‌ماند. کانال کنترلی که توسط فرمانده بات ایجاد می‌گردد، به‌عنوان نقطه وعده‌گاه و قرارگاه تمامی بات‌ها به شمار می‌آید، به‌طوری که هر بات بعد از نصب شدن خود بر روی سیستم قربانی به‌صورت خودکار سعی می‌کند تا به این کانال وصل شود. میزبان آلوده از طریق سرور IRC، دستورات مهاجمرا اجرا می‌کند؛ به‌عنوان مثال، دستورات راه‌اندازی حمله انکار سرویس توزیع شده یا ارسال انبوه هرزنامه‌ها. کانال فرماندهی و کنترل باعث می‌شود فرمانده بات تعداد زیادی از بات‌ها را از راه دور کنترل و فعالیت‌های غیرقانونی را هدایت کند[۲و۴].

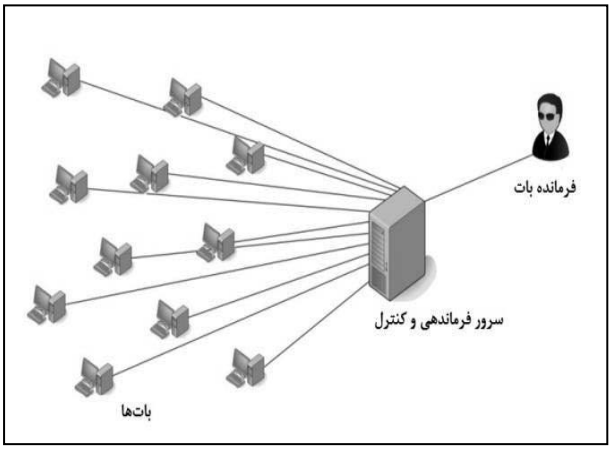
۲-۳- تکنیک‌های فرماندهی و کنترل بات‌نت

یکی از مسائل مهم برای فرمانده بات برقرای ارتباط با بات‌ها است. اکثر مهاجمین مایل‌اند دستورات خود را به سرعت به بات‌ها ارسال نمایند ولی در عین حال ارتباطشان کشف نشود و یا مبداء دستورات فاش نگردد [۱۱].

یکی از ساده‌ترین روش‌های ممکن، ارتباط مستقیم بین مهاجم و بات‌ها می‌باشد که در این صورت، می‌توان به آسانی مهاجمرا ردیابی نمود. مهاجم به‌دلیل امنیت پایین از این روش استفاده نمی‌کند و به جای آن تکنیک‌های فرماندهی و کنترل را به‌کار می‌برد. در اینجا به سه تکنیک اشاره می‌کنیم و مزایا و نقاط ضعف آن‌ها را در جدول (۲) نمایش می‌دهیم.

۲-۳-۱- تکنیک متمرکز[2]

این تکنیک از یک سرور مرکزی با پهنای باند زیاد برای میزبانی استفاده می‌نماید تا پیام‌ها را مابین بات‌های مختلف انتقال دهد. سرور فرماندهی و کنترل در بات‌نت یک ماشین آلوده است که از پروتکل‌هایی همچون IRCیا HTTP برای ارائه سرویس استفاده می‌نماید. نوع متمرکز سرور فرماندهی و کنترل از متداول‌ترین تکنیک‌ها می‌باشد که بسیاری از بات‌ها از آن بهره می‌گیرند. این روش، تأخیر انتشار پایینی دارد اما دو نقطه ضعف عمده دارد: ۱) به راحتی قابل کشف است چون کلاینت‌های زیادی به یک نقطه متصل هستند، و ۲) کشف سرور مرکزی تمام سیستم را به مخاطره می‌اندازد[۱۱]. در شکل (۲) بات‌نت متمرکز نمایش داده شده است.



شکل ۲- بات‌نت متمرکز[۵]

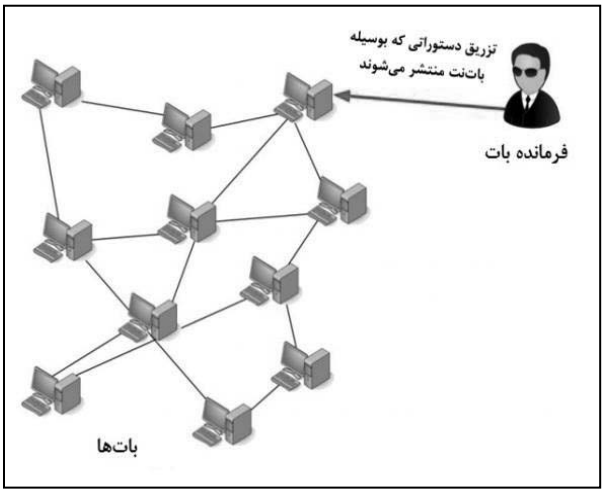
۲-۳-۲- تکنیک نظیر به نظیر

به‌دلیل مشکلاتی که تکنیک متمرکز دارد، مهاجمان به روش نظیر به نظیر روی آورده‌اند. برخلاف سیستم‌های متمرکز که یک سرور مرکزی به‌عنوان سرویس‌دهنده خدمات عمل می‌کند، در این معماری سرور مرکزی وجود ندارد.

همان‌طور که در شکل (۳) مشاهده می‌گردد تمامی رایانه‌های عضو چنین شبکه‌ای، هم به‌عنوان کلاینت عمل می‌کنند و هم به‌عنوان سرور. هر رایانه کلاینت می‌تواند به‌طور مستقیم با هرکدام از رایانه‌های کلاینت دیگر ارتباط برقرار کند. به این دلیل که در این مدل هیچ نیازی به وجود سرور مرکزی برای انتقال پیام‌ها نیست، کشف آن دشوار است. با استفاده از این تکنیک، پایداری شبکه نیز افزایش می‌یابد؛ زیرا با از کار افتادن یکی از رایانه‌ها، رایانه‌های دیگر کار آن را بر عهده می‌گیرند و شبکه قادر به ادامه ارائه سرویس خود خواهد بود. قابل ذکر است که اندازه بات‌نت‌هایی که با سیستم نظیر به نظیر پشتیبانی می‌شوند کوچک می‌باشند.

از ضعف‌های این روش می‌توان به تأخیر انتشار و نبود تضمین در رسیدن پیام اشاره کرد. طراحی چنین سیستمی هم بسیار پیچیده است[۱۱]. برخی بات‌ها مثل فت‌بات و پیکام از تکنیک نظیر به نظیر به‌عنوان وسیله کنترل بات‌نت استفاده می‌کنند.

1- Shell code
2- Centeralized



شکل۳- باتنت نظیر به نظیر [۵]

۲-۳-۳- تکنیک تصادفی[1] یا غیرساخت‌یافته[2]

در این روش، مهاجمبه یکی از باتها پیام رمز شده را به‌طور تصادفی می‌فرستد. هر بات تنها از وجود یک بات دیگر اطلاع دارد که این ارتباط می‌تواند توسط بات دیگری قطع شود و ارتباط دیگری شروع گردد. در این روش، تأخیر انتشار بسیار بالا می‌باشد و تضمینی برای رسیدن پیام نیست. طراحی چنین سیستمی نسبتاً ساده است و با کشف یک بات، کل باتنت به خطر نمی‌افتد، به‌علاوه رفتار جستجوی تصادفی قابل کشف است[۱۱و۱۳].

با توجه به جدول (۲) و مقایسه تکنیک‌های مختلف فرماندهی و کنترل با یکدیگر می‌توان نتیجه گرفت که در تکنیک متمرکز اگر سرور فرماندهی و کنترل از کار بیفتد، کل باتنت از کار خواهد افتاد، در حالی که تکنیک نظیر به نظیر به‌دلیل معماری غیرمتمرکز چنین نقطه ضعفی ندارد [۶]. مشکل تکنیک نظیر به نظیر، کندی سرعت رله پیام است؛ زیرا فاقد سرور فرماندهی و کنترل جهت انتشار دستورات است. اما اگر پروتکل مسیریابی خوب طراحی شود، آنگاه سرعت خیلی کند نمی‌شود. اخیرا باتنت‌های خیلی پیشرفته از پروتکلنظیر به نظیر استفاده می‌کنند، شناسایی و مانیتور کردن این نوع از پروتکل‌ها بسیار مشکل است.

۳- انواع حملات و عملیات مخرب باتنت‌ها

باتنت‌ها با توجه به حملات و عملیاتی که می‌توانند انجام دهند به‌عنوان ابزارهای هوشمند برای سودجویی‌های مالی، تبلیغات، سرقت اطلاعات حساس و حملات سایبری علیه اهداف استراتژیک به‌کار می‌روند. در ادامه به تعدادی از مهم‌ترین حملات و عملیات مخرب آن‌ها می‌پردازیم.

جدول ۲-مقایسه تکنیک‌های فرماندهی و کنترل [۱۱]

نام تکنیک	پیچیدگی طراحی	قابلیت آشکارسازی	تأخیر پیام	میزان مقاومت برای باقی ماندن
تکنیک متمرکز	پایین	متوسط	پایین	پایین
تکنیک نظیر به نظیر	متوسط	پایین	متوسط	متوسط
تکنیک تصادفی	پایین	بالا	بالا	بالا

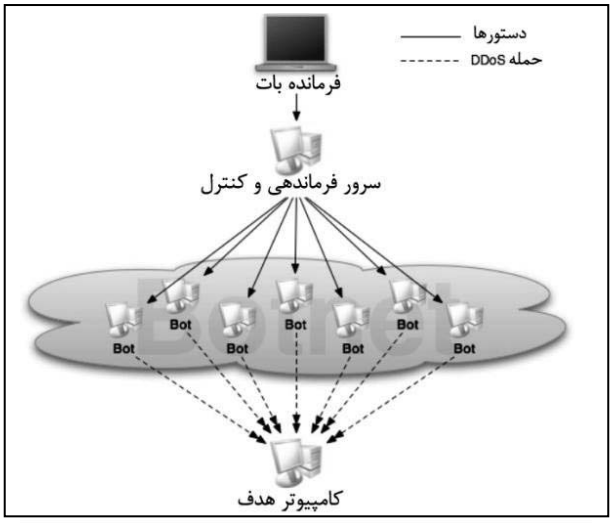
۳-۱- حملات انکار سرویس توزیع شده

این حمله از مهم‌ترین موارد کارکرد باتنت‌ها می‌باشد. یک باتنت با هزاران عضوی که در سراسر جهان دارد می‌تواند یک حمله گسترده و هماهنگ را برای خراب کردن یا از کار انداختن سایت‌ها و سرویس‌های مهم راه‌اندازی نماید و منابع و پهنای باند این سیستم‌ها را اشغال کند. برای مثال، مهاجم ممکن است در ابتدا باتنت را برای اتصال به کانال IRC قربانی تنظیم کند، سپس این هدف به‌وسیله هزاران درخواست سرویس توسط باتنت غرق می‌شود. در این نوع حمله DDoS، شبکه IRC قربانی از کار می‌افتد [۱]. در [۱۰] بات-هایی که در حملات DDoS کاربرد دارند بررسی و منبع کد باتهای مشهور حمله DDoS مثل آگوبات، اس‌دی بات، آربات[3] و اسپای‌بات به‌صورت جزیی تشریح شده‌اند. در شکل (۴) نمونه‌ای از این نوع حمله را مشاهده می‌نمایید.

	Botnet Operator Name	Victim Population	Popular Name
1	OneStreetTroop	9.3%	SpyEye Operator
2	RudeWarlockMob	9.0%	TDL/TDSS Gang
3	FreakySpiderCartel	7.0%	Rogue AV Operator
4	WhiteGloveGang	6.2%	Neosploit Operator
5	FiveLakeTrippers	4.5%	Rogue AV Operator
6	WildLightPosse	2.9%	Gbot Operator
7	SouthSideRiders	2.9%	Rogue AV Operator
8	TenPrisonMagicians	2.7%	Avalanche Syndicate
9	GreedySideBoys	2.6%	Virut Operator
10	SmallRockNerds	2.1%	Eleonore Downloader Gang

شکل ۵- رتبه بندی باتنت‌ها در نیمه اول سال ۲۰۱۱[۸]

1- Random
2- Unstructured
3- RBot



شکل۴- مثالی از حمله DDoS [۷]

۳-۲- سرقت اطلاعات حساس

فرمانده بات به‌راحتی می‌تواند کلمات عبور و اطلاعات کافی از قربانیان به‌دست آورد، این کار با تصویر گرفتن از صفحه نمایش، سرقت کلمه عبور، ارسال فایل و نرم‌افزار ثبت صفحه کلید انجام می‌شود. برای مثال اس‌دی‌بات از نرم‌افزار پیشرفته ثبت صفحه کلید برای جمع‌آوری اطلاعات شخصی استفاده می‌کند[۴]. در اغلب موارد، بات‌نت‌ها برای سرقت اطلاعات هویت شخصی افراد، داده‌های مالی و تجاری، یا کلمات عبور کاربران و سپس فروش یا استفاده مستقیماز آن‌ها به‌کار می‌روند[۱۲] .

۳-۳- ارسال هرزنامه[1]

امروزه بین ۷۰ تا ۹۰ درصد از هرزنامه‌های جهان از طریق بات‌نت‌ها منتشر می‌شوند[۱] . پس از اینکه یک رایانه مورد سوءاستفاده قرار گرفت، فرماندهبات می‌تواند از اینزامبی جدید به همراه سایرزامبی‌هایبات‌نتاستفاده کرده و باجمع‌آوری آدرس‌های ایمیل نسبت به ارسال گروهی هرزنامه و یا ایمیل‌های سرقت هویت اقدامنماید.

اگر هرزنامه‌ها از یک منبع متمرکز ارسال می‌شدند، پیگیری کردن آن و تقاضا از سرویس‌دهنده مربوطه برای لغو دسترسی رایانه ارسال‌کننده هرزنامه به اینترنت یا متهم کردن کاربر برای عمل غیرقانونی فرستادن هرزنامه می‌توانست نسبتاً آسان باشد. برای خلاصی از این مشکلات است که مهاجمین به رایانه‌های زامبی متکی هستند. رایانه آلوده نقش یک پروکسی را ایفا می‌کند، یعنی هکر یک قدمردپای خود را از منشاء ایمیل‌های هرزنامه زدوده است. برخی از بات‌نت‌هامانند آگوبات شامل دستوراتی جهت جمع‌آوری آدرس‌های ایمیل، برای استفاده هرزنامه‌نویسان جهت انتشار هرزنامه به آن‌ها هستند[۱۲].

1- Sending Spam

روستاک[2] نمونه‌ای از یک بات‌نت برای انتشار هرزنامه بود که از پروتکل HTTP استفاده می‌کرد و از سال ۲۰۰۶ تا سال ۲۰۱۱ فعالیت می نمود و در تاریخ ۱۶ مارس ۲۰۱۱ غیرفعالشد. روستاک از حدود یک میلیون رایانه که تحت کنترلش بودند تشکیل می‌شد و با استفاده از ترفندهایی، سال‌ها از شناسایی شدن خود جلوگیری می‌کرد. از زمانی که حملاتی به سخت‌افزارهای این شبکه انجام شد، میزان ارسال هرزنامه‌های جهان به شدت کاهش پیدا کرد و به سطح نسبتاً پایینی رسید. حدود نیمی از کل هرزنامه‌های ارسالی از بات‌نت‌ها از روستاک سرچشمه می‌گرفتند. روستاک روزانه بیش از ۳۰ میلیارد هرزنامه ارسال می‌کرد. روستاک در ارسال هرزنامه‌هایی که قرص‌های تقلبی تبلیغ می‌کردند تخصص داشت.

۳-۴- تقلب کلیک[3]

امروزه تعداد زیادی از مهاجمین به سود حاصل از انجام تبلیغات روی آورده‌اند و با ایجاد ترافیک جعلی شبکه، به منافع فراوانی دست می‌یابند. بدین ترتیب که مهاجمین یک سایت تبلیغی مجازی ایجاد می‌کنند و با مالکان آن به توافق می‌رسند که به ازای کلیک‌های تبلیغی، مبلغی دریافت کنند. با کمک بات‌نت، هزاران بات باید در زمان بسیار کوتاهی روی تبلیغات کلیک کنند. اعضای بات‌نت در هنگام آغاز به کار یک مرورگر به‌طور خودکار روی یک سایت کلیک می‌کنند. به‌عبارت دیگر، اینبات‌نت‌ها تعداد کلیک‌های یک آگهی تبلیغاتی را به شکل مصنوعی افزایش می‌دهند[۱۲]. ممکن است مهاجمین با وب‌سایت‌های قانونی توافق نمایند تا با استفاده از بات‌نت‌های بزرگ، موتورهای جستجو را فریب داده و رتبه آن سایت‌ها را بالا ببرند. عملکرد بات‌نت کلیک‌بات[4]برای تقلب در کلیک است.

۳-۵-صیادی[5] یا کلاهبرداری

در بسیاری از موارد، بات‌ها برای میزبانی سایت‌های کلاهبرداری به‌کار می‌روند. مهاجمان می‌توانند باتبدیل نمودنبات‌ها به وب سرورها یا سرورهای DNSاز طریقآنهااطلاعاترا استخراج نمودهو کلاهبرداری را اداره کنند[۱۴]. به عبارت دیگر، بات‌ها خود را به جای یک وب‌سایت معتبر جا می‌زنند و اطلاعات حساس کاربران را به‌دست می‌آورند.

۴- روش‌های مقابله و تشخیصبات‌نت

برای جلوگیری از آلودگی سیستم به بات، سیستم باید همیشه به‌روز باشد و تمامی به‌روز رسانی‌ها و فایل‌های وصله سیستم عامل نصب

2- Rustock
3- Click Fraud
4- Clickbot
5- Phishing

شده باشند. به‌کار بردن بازی‌ها و نرم‌افزارهای بدون کسب اجازه ناشر[1] و دیگر تجهیزات غیرقانونی آنلاین، همواره منبع کدهای مخرب هستند و تهدیدات امنیتی جدی به شمار می‌آیند. دیواره‌های آتش و برنامه‌های ضد ویروس باید بر روی سیستم‌ها نصب گردند و به صورت دوره‌ای به‌روز رسانی شوند تا از آلوده شدن سیستم جلوگیری شود. استفاده از تست‌های کپچا[2] بر روی وب‌سایت‌ها و دیگر سرویس‌ها، راه حل دیگری است تا بتوان با کمک آن‌ها در مقابل باتها و دیگر عامل‌های مخرب مقابله کرد [۱۱] . کپچا که سرنام برابر انگلیسی "آزمون همگانی کاملاً خودکار شده تورینگ برای مجزا کردن انسان و رایانه" می‌باشد، یک سامانه امنیتی و روند ارزیابی است که برای جلوگیری از برخی حمله‌های خرابه‌کارانه باتها به‌کار می‌رود. این روند می‌تواند مشخص کند که مراجعه‌کنندگان به یک وب‌سایت و یا سایر خدمات آنلاین انسان هستند یا رایانه. بدین منظور برنامه کپچا آزمون‌هایی را تولید می‌کند که تنها انسان‌ها قادر به پاسخ‌گویی به آن‌ها باشند. چون رایانه‌ها و نرم‌افزارهای فعلی احتمالا نمی‌توانند پاسخ درستی به این آزمون بدهند، هر کاربری که آن را درست حل کند، انسان فرض می‌شود. کپچا در وب‌سایت‌های مختلف، تصویری از حروف و اعداد است که عمدا کج و ناواضح رسم شده‌اند و از کاربر خواسته می‌شود تا آنرا به شکل صحیح خوانده و با دقت در جعبه متن وارد کند[۱۵].

روش‌های تشخیص یا کشف باتنت در منابع مختلف دارای دسته‌بندی‌های گوناگونی هستند. در [۲] این روش‌ها به‌صورت دقیق‌تری دسته‌بندی شده‌اند. روش‌های تشخیص باتنت بر اساس مشاهده ترافیک غیرفعال شبکه، چهار دسته‌اند که شامل روش مبتنی بر امضا، مبتنی بر رفتار غیرعادی، مبتنی بر DNS و مبتنی بر داده‌کاوی است. روش‌های مبتنی بر امضا فقط باتنت‌های شناخته شده را تشخیص می‌دهند، در حالی که سایر روش‌ها قادرند باتهای ناشناخته را نیز تشخیص دهند. نهایتاً براساس مقایسه این روش‌ها نتیجه‌گیری می‌شود که برخی از روش‌های مبتنی برDNS و مبتنی بر داده‌کاوی دارای خصوصیات مناسب‌تری برای تشخیص باتنت‌ها می‌باشند [۲].

۵- وضعیت فعلی و اهداف جدید باتنت‌ها

Dambalaیک شرکت امنیتی رایانه است که بر روی تهدیدات پیشرفته سایبری از جمله باتنت‌ها تمرکز دارد[۸]. این شرکت گزارش داده است که در نیمه اول سال ۲۰۱۱، باتهای جدیدی به وجود آمده‌اند. از ۱۰ باتنت بزرگ در این دوره، تنها سه‌تای آن‌ها در فهرست ۱۰ باتنت بزرگ سال ۲۰۱۰ بوده‌اند. "OneStreetTroop" یک گروه باتنت است که براساس خانواده SpyEye می‌باشد و از رتبه ۱۰ در سال ۲۰۱۰ به رتبه اول در نیمه اول سال ۲۰۱۱ صعود کرده است. آماری که در شکل (۵) مشاهده می‌گردد در قیاس با آمار سال ۲۰۱۰ نشان دهنده رشد و گسترش باتنت‌ها است. موضوع دیگر در مورد باتنت‌ها این است که نسبت به دوره قبل، تعداد قربانیانی که توسط بیش از یک باتنت آلوده شده‌اند، حدود ۱۸ درصد افزایش یافته و به بیش از ۴۱ درصد رسیده است. بنابراین آلودگی‌های متعددی روی هر قربانی وجود دارد به‌طوری که سیستم‌هایشان مکررا توسط مهاجمان مورد سوءاستفاده قرار می‌گیرد. مهاجمان برای کسب درآمد، دسترسی به ماشین قربانی را اجاره می‌دهند یا به دیگر مهاجمان می‌فروشند.

تا چندی پیش، عملیات مخرب بدافزارهای تلفن همراه، به دریافت پول به ازای تقلب سرویس پیام کوتاه و یا تاکتیک‌های دیگری که به معماری فرماندهی و کنترل نیاز نداردمحدود بوده است. اما اخیرا بدافزارهای تلفن همراه سعی به برقراری ارتباط با سرورهای فرماندهی و کنترل دارند. اهداف جدید و جذاب برای باتنت‌ها، تلفن‌های هوشمند و تجهیزات سیار هستند [۸]. باتنت‌های تلفن‌های همراه روی انواع دستگاه‌ها مثل سیمبین، اندروید و غیره نصب می‌شوند و پیام‌های کوتاه را شنود می‌کنند تا کلمات عبور ارسال شده توسط آن‌ها را سرقت نمایند.

۶- باتنت و حملات سایبری

باتنت‌ها ممکن است برای اهداف سیاسی یا نظامی به‌کار روند. یک نمونه مشهور از حملات DDoS در سال ۲۰۰۷ در کشور استونی اتفاق افتاد و کل زیرساخت‌های اینترنتی این کشور را تحت تاثیر خود قرار داد؛ البته هدف اصلی، وب‌سایت‌های دولتی و سازمانی، بانک‌ها و روزنامه‌ها بودند. این حملات DDoS توسط باتنت‌ها راه‌اندازی شدند. گمان بر این است که انگیزه این حمله بر سر برداشتن یادبود جنگ شوروی از پایتخت استونی بود. مقامات استونی روس‌ها را عامل اصلی این حملات می‌دانند. به نظر می‌آید این مورد اولین حمله سایبری با انگیزه سیاسی در این حد و اندازه باشد[۵].

نمونه دیگر، بدافزار استاکس‌نت[3] استکه بسیار شبیه باتنت عمل کرده و برای جاسوسی صنعتی به‌کار رفته است. استاکس‌نت، به‌عنوان یکی از پیچیده‌ترین انواع نرم‌افزارهای مخرب که تاکنون شناسایی شده است، مطرح است. استاکس‌نتپس از آلوده نمودن موفق میزبانی که به مخاطره افتاده است، اتصال به اینترنت را تأیید نموده و سپس تلاش می‌کند به دو سرور فرماندهی و کنترل متصل شود تا از طریق آن‌ها اطلاعات سیستم را ارسال کند و نیز از طریق آن‌ها به‌روز رسانی شود. استاکس‌نت فقط سیستم‌های صنعتی حاوی تنظیمات خاصی را مورد شناسایی و حمله قرار می‌دهد و از این رو اولین کرم برای هدف

1- Pirated
2- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
3- Stuxnet

قرار دادن زیرساخت‌ها است. علاوه بر این، چهار اکسپلویت[1] ناشناخته (روز صفر[2]) و دو گواهینامه دیجیتالی برای مکانیسم گسترش استاکس‌نت مورد استفاده قرار گرفت. با توجه به شناسایی و توسعه چنین اکسپلویت‌هایی، و همچنین استفاده از دانش دقیق سیستم‌های صنعتی، که برای ایجاد این کرم استفاده شد، احتمالاً توسط یک تیم متخصص و با برنامه‌ریزی دقیق طراحی شده است[۵]. براساس نظر کارشناسان شرکت سیمانتک، این بدافزار به دنبال خرابه‌کاری در تأسیسات غنی‌سازی اورانیوم‌نطنز بوده‌است. روزنامه نیویورک‌تایمز در تاریخ ۱۶ ژانویه.۲۰۱۱ میلادی، در مقاله‌ای مدعی شد که «اسرائیل استاکس‌نت را در مرکز اتمی دیمونا و بر روی سانتریفیوژهای مشابهی که ایران از آن‌ها در تأسیسات غنی‌سازی اورانیوم نطنز استفاده می‌کند، با موفقیت آزمایش کرده‌بود». این در حالی است که دولت اسرائیل یا دولت آمریکا هیچ‌گاه به‌طور رسمی دست‌داشتن در انتشار استاکس‌نت را تایید نکرده‌اند[۱۶].

اخیراً نیز در پی بررسی‌های تخصصی انجام شده توسط کارشناسان مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای یا مرکز ماهر و در ادامه تحقیقات صورت گرفته پیرامون حملات هدفمند استاکس‌نت و دیوکیو، این مرکز برای نخستین بار اقدام به انتشار اطلاعات آخرین نمونه از حملات این خانواده نمود. این حمله توسط بدافزاری با نام شعله آتش[3] صورت می‌گیرد. ابزار شناسایی و پاکسازی این بدافزار در مرکز ماهر تهیه شده و در اختیار متقاضیان قرار می‌گیرد[۱۴]. این بدافزار نیز ویژگی‌هایی شبیه باتنت دارد؛ مثلاً دارای سرورهای فرماندهی و کنترل است و قادر است اطلاعات حساس موجود در شبکه یا دیسک رایانه و حتی تصویر صفحه نمایش و یا صوت دریافتی از طریق میکروفن را ذخیره نموده و برای سرورهای خارج از کشور ارسال نماید. شناسایی و تهیه ابزار پاکسازی این بدافزار توسط کارشناسان مرکز ماهر، یک موفقیت قابل توجه در عرصه فضای سایبری برای کشورمان محسوب می‌شود.

۷- خلاصه و نتیجه‌گیری

در این تحقیق، مفاهیم مرتبط با شبکه‌های باتنت معرفی شد. ویژگی برجسته باتنت‌ها استفاده از کانال‌های فرماندهی و کنترل است که از طریق آن‌ها به‌روز شده و هدایت می‌گردند. بنابراین تکنیک‌های فرماندهی و کنترل مورد استفاده در باتنت‌ها شرح داده شد و بین آن‌ها مقایسه‌ای انجام گرفت. مهم‌ترین حملات و کارکردهای مخرب باتنت بررسی و به تعدادی از روش‌های مقابله و تشخیص آن‌ها اشاره گردید، سپس وضعیت موجود و اهداف جدید باتنت‌ها بررسی شد واین نتیجه به‌دست آمد که از زمان پیدایش باتنت‌ها تاکنون، دائماً بر مخاطرات و کارکرد آن‌ها افزوده شده است. اهداف جدید و جذاب برای باتنت‌ها تلفن‌های هوشمند و تجهیزات سیار هستند. در آینده شاهد افزایش مواردی چون استفاده از تلفن‌های همراه به‌عنوان باتنت برای ارسال هرزنامه و سرقت اطلاعات و سایر موارد مخرب خواهیم بود.

با وجود گسترش روزافزون باتنت‌ها هنوز تحقیقات درباره آن‌ها به تکامل نرسیده است و می‌توان به زمینه‌های تحقیقی دیگری مثل بررسی و مطالعه ساختار، مخاطرات و اهداف باتنت‌های جدید و مدرن پرداخت. مطالعه و طراحی روش‌های پیشگیری و تشخیص و مقابله در برابر باتنت‌ها زمینه پژوهشی دیگری است.

در چند سال اخیر، تهدیدات اینترنتی از انگیزه‌های فردی و سودجویی‌های مالی، به حملات سایبری سازمان‌یافته به دولت‌ها و سازمان‌های دولتی گسترش‌یافته است. در اغلب این حملات از باتنت یا شبه باتنت‌ها در کنار سایر بدافزارها استفاده می‌گردد. حملات اخیر سایبری به زیرساخت‌های کشورمان عمدتا با اهداف سیاسی و اقتصادی صورت می‌گیرد. بدافزارهای استاکس‌نت و شعله آتش و موارد مشابه، دارای خصوصیات باتنت‌های مدرن هستند. آن‌ها به‌عنوان بخشی از برنامه‌های گسترده قدرت‌های بزرگ و با پشتوانه مالی قابل توجه، برای حملات سایبری به ایران ایجاد شده‌اند. بنابراینمطالعه و پژوهش درباره آن‌ها بسیار ضروری استتا بتواناز این تسلیحات هوشمند سایبری برای دفاع و مقابله، در نبرد اطلاعاتی در برابر دشمنان استفاده نمود.

مراجع

1. Jing Liu, et al. , "Botnet: Classification, Attacks, Detection, Tracing,and Preventive Measures", (**2009**).
2. Maryam Feily, AlirezaShahrestani, SureswaranRamadass. ," A Survey of botnet and botnet Detection", (**2009**).
3. Jennifer A. chandler, "Liability for Botnet Attacks", (**2005**).
4. Chao Li, Wei Jiang, XinZou, " botnet: Survey and Case Study", (**2009**) Fourth International Conference on Innovative Computing, Information and Control
5. Botnets: Detection, Measurement, Disinfection &Defence-The European Network and Information Security Agency (ENISA), (**2011**) Available http://www. enisa. europa. eu
6. LI Heng-Feng, HOU Ru-Xin. "A Survey of botnet Detection", (**2010**).
7. Joseph Massi, Sudhir Panda, GirishaRajappa, SenthilSelvaraj, and SwapanaRevankar, "botnet Detection and Mitigation",Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 7th, (**2010**).
8. Available: http://www. damballa. com/downloads/ r_pubs/Damballa_Threat_Report-First_Half_2011. pdf

1- exploit
2- Zero day
3- Flame

9. JunewonPark," Acquiring Digital Evidence from Botnet Attacks: Procedures and Methods: M. Sc Thesis", (**2011**).
10. Vrizlynn L. L. Thing, Morris Sloman, and NarankerDulay, "A Survey of Bots Used for Distributed Denial of Service Attacks", (**2006**).
11. M. Bailey, et al. ,"A Survey of botnet Technology and Defenses", in Conference for Homeland Security, (**2009**). CATCH.
12. Available http://www. ircert. cc/fa/default
13. Evan Cooke, FarnamJahanian, Danny McPherson,"The Zombie Roundup:Understanding, Detecting, and Disrupting Botnets", (**2005**).
14. Available http://www. certcc. ir/index. php?name= news &file=article&sid=1892
15. Available http://en. wikipedia. org/wiki/CAPTCHA
16. Available http://en. wikipedia. org/wiki/Stuxnet

Botnet and Its Attacks

T. Salami[1]

M. Dehghani[2]

Abstract

Among the various forms of malware, botnets are emerging as the most serious threat against cyber security, they are used for malicious purposes such as sending spam, launching Distributed Denial of Service (DDoS) attacks, Spying and theft of confidential information, and identity theft. Botnets, are remotely controlled by the attackers, and whose members are located in homes, schools, businesses, and governments around the world. The defining characteristic of botnets is the use of command and control channels through which they can be updated and directed. Survey of botnet and its attacks and also botnet detection and defense are related to passive defense in the field of information technology and one of the important aspects of it, is cyber attacks against our country that mainly have properties of botnets. In this paper, We first discuss fundamental concepts of botnets, then command and control techniques are introduced and finally a brief comparison of these techniques is explained. Subsequently, we introduce several related attacks and malicious operation of botnets and then we point out theirr latest targets, and eventually, some cyber attacks, especially those that are against our country infrastructures have been discussed and according to this study, some discussions are also presented about their similarity to botnet attacks, and finally, conclusions are drawn and recommendations are made.

Keys Words: *Botnet, Bot, Command and Control Server, DDoS Attack, Cyber Attack*

1- MS in Information Technology Engineering, Security Major, Imam Hossein Comprehensive University (Pbh), Writer in Charge (Email: salami.84@gmail.com)
2- PhD Candidate of Computer Software (Email: mdehghany@ihu.ac.ir)