ITRC

مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

**مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها**

**cert@shirazu.ac.ir**

# ظهور باج افزارها


تنظیم کننده:

Babu Nath Giri

Nitin Jyoti

**مترجم:**

**مریم باصری**


**ویرایش: ۱**

**شماره سند: WP-89/6-2**

**چکیده :**

جرائم رایانه در راه های مختلفی برای انجام وظایف خود، خودشان را همانند موجودات زنده (مانند (اسب تروا) مدل می کنند (طراحی می ویروس ها و کرم ها) و یا در اقدامات زندگی واقعی یا حوادث کنند). ما باج افزار را به عنوان یک تروجان تعریف می کنیم که کدگذاری شده اند و یا منابع ، فایل ها ، داده ها و ... یک کامپیوتر و یا یک سیستم را در کنترل خود برای باج (منافع تجاری یا اطلاعات) در ازای آزاد کردن منابعی که به دست گرفته اند نگه داری می کند.

رفتار این خانواده از بدافزار شبیه به حوادث زندگی واقعی از موجودی تا دارایی های ارزشمند و خواستار پرداخت در قبال آزادی است.

این مقاله به ظهور باج افزار توسط توضیح مختصر حملات باج افزار های مختلف و پیچیدگی آنها نگاه کنند.

**واژه های کلیدی:**

باج افزار،ویروس،ضد ویروس،تروجان، بات نت

آپا ؟؟؟

**مقدمه**

جرائم رایانه در راه های مختلفی برای انجام وظایف خود، خودشان را همانند موجودات زنده (مانند ویروس ها و کرم ها) و یا در اقدامات زندگی واقعی یا حوادث (اسب تروا) مدل می کنند (طراحی می کنند).

بعضی از این روش ها همواره استفاده شده و در طول زمان بهبود یافته اند تنها برای بازگشت به زمانی که توانایی های بالقوه خود را دوباره کشف کنند.

ما باج افزار را به عنوان یک تروجان تعریف می کنیم که کدگذاری شده اند و یا منابع ، فایل ها ، داده ها و ... یک کامپیوتر و یا یک سیستم را در کنترل خود برای باج (منافع تجاری یا اطلاعات) در ازای آزاد کردن منابعی که به دست گرفته اند نگه داری می کند.

رفتار این خانواده از بدافزار شبیه به حوادث زندگی واقعی از موجودی تا دارایی های ارزشمند و خواستار پرداخت در قبال آزادی است.

بطور موثر برای اولین بار در اواخر سال ۱۹۸۹ با عنوان "PC CYBORG/AIDS information Trojan" استفاده شد، این تروجان و خطر ناشی از آن نشان داده شده است. اما اجرای باج افزار سودی نداشت و محبوبیت زیادی در میان افراد بد بدست آورد.

باج افزار ظاهرا به مدت ۱۵ سال رها شده بود و در سال ۲۰۰۵ دوباره متولد شد. به عنوان نویسنده بدافزار بالقوه، باج افزار در دوران استفاده گسترده از اینترنت و تجارت الکترونیک به رسمیت شناخته شد.

با نویسندگان بدافزار بهتر در مهندسی اجتماعی و روش های دیگر برای دریافت بدافزار برای کاربران ، هر کسی که دسترسی به اینترنت دارد قربانی بالقوه است.

باج افزار تهدیدی بزرگتر برای دنیای شرکت های بزرگ به شمار می آید زیرا داده به عنوان یک منبع ارزشمند محسوب می شود. کاربران خانگی ، در هر حال مصون از این حملات نیستند ، همانطور که حداقل

اقدامات امنیتی را اجرا می کنند.

این مقاله به ظهور باج افزار توسط توضیح مختصر حملات باج افزار های مختلف و پیچیدگی آنها نگاه کنند.

ما باید احتمال ترکیب بدافزار دیگر با باج افزار برای تبدیل شدن به یک تهدید موثر را کشف کنیم، این نسل جدید از بدافزارها اساسا توسط پیوستگی وجود دارند و در زمینه فعالیت های خود حتی پس از تشخیص حمل می شوند.

ما همچنین باید به راه های جدید خرید آنلاین اقتباس شده توسط یکی از انواع باج افزارها برای اخاذی کاربران نگاه کنیم.

روزهایی که بدافزار کامپیوتر برای شهرت نوشته شده بود طولانی شده است. نویسندگان ویروس و دشمنان خود در بازی موش و گربه درگیرهستند.هر روز نوآوری در هر دو طرف برای شکست دادن یکدیگرمی بینیم. با افزایش جمعیت کاربران اینترنت و تجارت الکترونیک، تعدادی از فرصت ها برای نویسندگان بدافزارها برای تسخیر وجود دارد. نویسندگان بدافزارها برای دریافت کردن این فرصت های موثر، نیاز به چند پیش نیاز مهم برای قانع شدن دارند. بقا یکی از عناصر کلیدی است. پنهان کاری از کاربران و یا داشتن رفتار پنهان یکی از مهم ترین خصوصیات از هر بدافزار برای زنده ماندن در میزبان است. با انجام این کار بدافزار از کاربران فرار می کند و مهمتر برنامه های ضد ویروس است. نویسنده بدافزار دائما سعی در تکمیل کردن هنر پنهان بودن دارد. باج افزار در سوی دیگر اعلام موجودیت خود را به کاربر می کند و سرنوشت برخی از منابع سیستم قربانی بستگی به بقای بدافزار دارد. پس از به دست آمدن این هدف ، باج افزار می تواند کاربر را به عمل بر اساس دستورالعمل نویسنده بدافزارفرمان دهد (با فرض اجرای کامل باج افزار).

باج افزار شبیه به انواع دیگر بدافزارها در انتقال است. این می تواند از تمام روش های موجود برای رسیدن به کاربران استفاده کند.

**The Abductors so Far**

در قسمت زیر برخی از محبوب ترین باج افزارهایی که ما در طول سال ها دیده ایم توضیح می دهیم.

**اولین باج افزار(PC CYBORG/AIDS Trojan - 1989):**

PC CYBORG/AIDS Information Trojan یکی از اولین در این راه جدید از بدافزار است. این باج افزار نه تنها مفهوم را نشان می داد ، بلکه این روزها با برخی از روش های شناخته شده استفاده شده توسط نویسندگان بدافزار یکپارچه شده است. این تروجان در بسته مهندسی اجتماعی شامل فلاپی دیسک برای فریب، گیرندگان فرستاده شده است. در زمانی که استفاده از اینترنت عمومی وجود نداشت ، نویسنده قسمت عمده از بسته را از طریق پست سطحی می فرستاد و آن را به لیست پستی که نویسنده عضو آن بود نشان دهی می کرد. توسعه دهنده این تروجان به اتهام اخاذی دستگیر شد.

**فعالیت ها**

هنگامی که بر روی سیستم از روی فلاپی دیسک نصب می شود ، این برنامه جایگزین با یک فایل autoexec.bat می شود که شمارش می کند چند بار سیستم ری بوت شده است. پس از اینکه شماره به ۹۰ می رسد ، تروجان پوشه ها را پنهان می کند و تمام نام فایل را در فهرست ریشه کدگذاری می کند. در این مرحله تروجان پیام درخواست از کاربر به پرداخت ۳۷۸ $ برای تجدید مجوز و بازیابی فایل ها و دایرکتوری های از دست رفته نمایش می دهد. پول به آدرس در پاناما فرستاده می شد. [۱ ، ۲]

**May 2005 –GPCoder**

پس از ۱۵ سال ساکت شدن باج افزار ، شکل جدید ، GP-Coder ، برای اخاذی از کاربران دوباره ظهور کرد. در زمانی که GP-Coder منتشر شد اینترنت در استفاده گسترده بود و این کمک کرد تا نویسنده، این

بدافزار را به سیستم های کامپیوتری ارائه کند. بسیاری از مدل های GPCoder وجود دارد ، تازه ترین آنها در ژوئن ۲۰۰۶ منتشر شد. انواع دیگری از GPCoder روش خود را از رمزگذاری بهبود دادند، از الگوریتم خود مؤلف در نسخه اول تا به رمزگذاری RSA بسیار پیچیده تر در آخرین نسخه.

**فعالیت ها**

ورود به سیستم از طریق هرزنامه ، این تروجان بسیاری از فایل ها الحاقی از پیش تعیین شده را جستجو و کدگذاری می کند. سپس یادداشت باج را در هر دایکتوری که آن را کدگذاری کرده است قرار

می دهد و از کاربران برای فرستادن پست الکترونیکی به آدرس خاص به منظور دریافت رمزگشای متناظر درخواست می کند. در نهایت،کاربران برای انتقال باج به حساب بانکی آنلاین آموزش داده می شدند. [۳]

**March 2006 – CryZip**

حدود یک سال پس از اینکه GPCoder ظاهر شد ، CryZip به نبرد پیوست. عمل کردن CryZip بسیار متفاوت از GPCoder نبود. اما بر خلافGPCoder ، CryZip از روش رمزگذاری استفاده نمی کرد. به جای آن از کتابخانه فایل های فشرده تجاری برای ذخیره فایل ها در فایل های فشرده که با کلمه عبور محافظت می شود استفاده می کرد.

**فعالیت ها**

بعد از نصب ، خود را به تمام فرایندهای در حال اجرا وصل می کند و آن را برای فایل ها و فروشگاه های آنها در یک فایل فشرده با کلمه عبور محافظت شده جستجو می کند در حالی که فایل اصلی حذف شده است، سپس یادداشت باج با دستورالعمل چگونه فایل را به عقب بر گردانیم را قرار می دهد. برای انتقال باج ، CryZip شماره حساب E-Gold را که به طور تصادفی از یک لیست انتخاب می کند اضافه می کند. [۴]

**May 2006–MayArchive**

در حال حاضر روند باج افزار در مسری شدن به نظر می رسد [5, 6]. تروجان قابل توجه بعدی MayArchive بود، که فایل ها را تصرف می کرد و یادداشت باج به دیگران را کاهش می داد. اما MayArchive خود را از دیگران در یادداشت باجی که قرار می داد متمایز کرده بود. یادداشت اظهار می کرد که " ما هیچ پولی ازشما درخواست نمی کنیم! ما فقط با شما می خواهیم تجارت کنیم. شما حتی می توانید با ما پول اضافی کسب درآمد کنید." این تغییر نمونه در نویسندگان بدافزار برای راه اخاذی برنامه ریزی شده بود. در این نوع از اخاذی به عنوان مثال MayArchive بعدا در این مقاله با جزئیات نگاه خواهیم کرد.

**فعالیت ها**

MayArchive سیستم را برای فایل های با پسوندهای مختلف جستجو می کند و سپس آنها را به آرشیو خود اضافه می کند و فایل اصلی را حذف می کند. این فایل آرشیو با رمز محافظت شده است ، اما فایل های در داخل آرشیو رمزگذاری نمی شوند. MayArchive یادداشت باج را در مورد چگونگی به دست آوردن رمز عبور به منظور استخراج فایل ها قرار می دهد. این یادداشت نسخه ی نمایشی از آرشیو است برای نشان دادن نحوه ای که آرشیو این نسخه ها کار می کند. [۷]

**عادت کردن به اخاذی**

باج افزار همانطور که از نام آن پیداست برای درخواست باج است. باج می تواند در هر شکل باشد : منابع سیستم ، اطلاعات شخصی ، و یا پول و از جمله امکانات دیگر.

در اغلب موارد گزارش شده باج به شکل پول است. در بسیاری از پیاده سازی ها، نویسندگان سریعتر از آنچه

که ممکن است پول را تقاضا می کنند قبل از آنکه کاربر بتواند سیستم یا منابع خود را اصلاح کند. روند گرفتن کاربر برای پرداخت پول باج به عوامل زیادی بستگی دارد.

در اینجا سه مورد آن بیان می شود :

- **آموزش کاربر**:

کاربران تحصیل کرده خوب هرگز تسلیم چنین تهدیدی نمی شوند. آنها می توانند به خوبی با داشتن سیاست نسخه پشتیبان خوب یا با استفاده از گزینه بازیابی سیستم برای چنین حملات مخربی خود را آماده کنند. در این موارد معامله هرگز اتفاق نمی افتد. این سناریو است که خارج از کنترل نویسنده است.

- **سطح پیچیدگی بدافزار :**

تعیین میزان خسارت بدافزار ممکن است علتی برای یک سیستم و شانس برای کاربر یا برای ابزار ترمیم برای بازیابی منابع خراب شده باشد. بسته به پیچیدگی ، یک کاربر ممکن است آنچه را که برای بهبود یافتن مصالحه منابع برایش غیر ممکن است را بدون تماس با نویسنده بدافزار پیدا کند. گاهی اوقات سیستم برای عملکرد خود وابسته به بدافزار می شود[۸].

- **ضرورت ها و الزامات دوباره بدست آوردن منابع تصرف شده :**

باج افزار ممکن نیست بسیار موفق گردد مگر اینکه منابعی که تصرف کرده است به اندازه کافی برای کاربر برای دوباره بدست آوردن آن مهم باشد. برای منابع ناچیز ، یک کاربر ممکن است به خوبی تصمیم به چشم پوشی از آن بگیرد.

اینها معیارهایی که ممکن است برخی از کاربران را به پرداخت باج القاء کند ، اما این ها تنها نیست. برای نویسنده باج افزار روند گرفتن کاربر به پرداخت باج فقط نیمی از کار است، نتیجه نهایی نیز وجود دارد.

معامله نا امن ممکن است هویت نویسنده را افشا کنند ، پس نویسندگان باج افزار باید معامله را در راهی که تنها به تعقیب غاز وحشی منجر شود ایجاد کنند.

در قسمت بعد ، در مورد برخی از راه هایی که می تواند مورد استفاده قرار گیرد برای پرداخت باج صحبت خواهیم کرد.

**Escaping the "Follow the money" Trail**

روش پرداخت کردن باج عنصر کلیدی در اجرای موفق باج افزار است. این ، بعد از همه ، یکی از مسیرهای احتمالی که می تواند منجر به ایجاد آن شود. در هر صورت از تروجان AIDS در سال ۱۹۸۹ ، اکثر حملات باج افزار خواستار پول هستند. با ظهور و استفاده گسترده از اینترنت ، راه های داد و ستد نیز بطور قابل توجهی تکامل یافت. روش ارجع از داد و ستد باج با روش پرداخت آنلاین مانند PayPal (تجارت الکترونیکی و کسب و کاری که به پرداخت و انتقال پول از طریق اینترنت اجازه می دهد) [۹] و یا E-Gold [۱۰] می باشد.

با این حال ، این روش ها کاملا هویت اخاذ را پنهان نمی کنند. در اینجا برخی از مشکلات این حالت برای نویسنده باج افزار بیان می شود:

- هنوز تمام کاربرانی که آلوده شده اند پی پال ، E-Gold و یا حساب مشابه دارند آنها نیاز به ساخت یکی از اینها را دارند.
- پس از حمله های تروریستی ۱۱ سپتامبر سال ۲۰۰۱ ، بیشتر جرم و جنایت سازمان یافته تحقق یافتند و جرایم اینترنتی شروع به همپوشانی کرده اند[۱۱]. تسهیل کننده حساب اقدامات احتیاطی زیادی برای بالا بردن امنیت این پرداخت حساب آنلاین گرفته اند به طوری که مجرمان نمی توانند از آنها برای اهداف غیر قانونی از قبیل پولشویی و تامین بودجه استفاده

کنند.

- این افزایش آگاهی امنیت منجر به تعدادی از اقدامات لازم برای پیگیری بودجه و هویت مربوط به این حساب می شود.

پرداخت آنلاین به دنبال امن تر شدن است و بیشتر کشورها در حال ورود به موافقتنامه های دو جانبه در مورد این مسائل و تلاش برای متوقف کردن این نوع از فعالیت های مجرمانه می باشند. بنابراین امیدواریم که حساب های دیجیتال، دیگر برای بهره برداری فعالیت های غیر قانونی استفاده نشود. اما مجرمان همیشه به دنبال راه هایی برای فرار از ردیابی توسط تلاش های متفاوت هستند.

**پولشویی**

پول شویی یکی از موثر ترین ترفندهای استفاده شده توسط مجرمان درگیر در فعالیت های غیر قانونی برای فرار از دنباله پول غیر قانونی می باشند. پولشویی منبع غیر قانونی پول و دریافت کننده نهایی از طریق زنجیره پیچیده ای از معاملات مالی را پوشش می دهد.

استفاده گسترده از اینترنت ، عدم وجود قوانین سختگیرانه اینترنتی جهانی ، و سهولت تجارت برخی از دلایلی است که باعث جذب نویسندگان باج افزار برای استفاده از پول شویی از طریق اینترنت شده است.

راههای زیادی برای معاملات وجود دارد ؛ بودجه نامنظم یکی از آنها است. بودجه نامنظم روشی از مسیر یابی غیر قانونی پول از طریق تجارت مشروع است و با داشتن مقدار باج سپرده در حساب جداگانه مقدار مشخصی برای این سرویس پرداخت می شود.متناسب با بودجه نامنظم کاملا در چارچوبی از خرید آنلاین ، می تواند از آن برای معامله کردن باج استفاده کند. خرید آنلان را در بخش بعدی توضیح خواهیم داد.

**خرید آنلاین**

MayArchive [7] نمونه انتقالی را ایجاد کرد که در این راه خواستار باج بود. خرید آنلاین به عنوان حالتی

از معامله باج استفاده می شود ، و به قربانیان، خرید کالا از وب سایت های خاص را پیشنهاد می دهد.

دلایل متعددی که چرا راه معامله باج می تواند ساده تر و کارآمد باشد وجود دارد :

- در اکثر سایت های خرید آنلاین اینترنتی کارت اعتباری قبول می کنند. خرید آنلاین نیز روشهای پرداخت ، از جمله کارت های اعتباری و حساب های آنلاین مانند پی پال و یا دیگرحساب ها را ارائه می دهد.
- از دیدگاه مهندسی اجتماعی ، این بهترین راه برای درخواست باج است. مانند رویکرد توسط MayArchive ، برنامه ایالت می خواهد تجارت انجام دهد و پولی نمی خواهد. این بنظر میرسد بهتر از این است که فقط خواستار پرداخت باشد. اما به هیچ وجه این راه قانونی نیست ؛ و هنوز به عنوان یک عمل مجرمانه واجد شرایط است.
- خرید آنلاین برای پرداخت باج هنوز هم از طریق تجارت قانونی می تواند کار کند. دریافت کننده این معامله یک شرکت قانونی خواهد بود. از سوی دیگر ، انتقال باج به حساب آنلاین شخصی متعلق به نویسنده بدافزار می تواند مشکوک بنظر رسد. ویژگی خرید به عنوان معامله باج می تواند آسان تر برای نویسنده باج افزار با استفاده از تکنیک ردیابی باشد. رایج ترین روش استفاده از پارامتر های رشته پرس و جو و کوکی ها می باشد [۱۲]. نویسنده باج افزار می تواند پولی را که از کمیسیون بدست آمده برای تسهیل در خرید آن به او پرداخت کند.

تا کنون با نگاه در باج افزار ، حملات مختلف ، و اینکه چگونه تکامل یافته اند و روش های مختلف اخاذی آنها مشخص می شود. حملاتی که ما تا کنون مشخص کردیم حملات مستقیم هستند ، یعنی یک تروجان در سیستم نصب شده و منابع را توقیف می کند و در نهایت خواستار نوعی باج می شود. اما باج افزار می توان به عنوان بخشی از بدافزار و یا در ارتباط با دیگر رده های بدافزاراستفاده شود.

در بخش بعدی باید بحث کنیم که چگونه برخی از پیاده سازی ها مـی تواننـد از خاصـیت ذاتـی بـاج افـزار خواستار چیزهای برای تکمیل وظایف خود یا برای زنده ماندن در دستگاه های میزبان خود استفاده کنند.

**نمایش باید ادامه پیدا کند**

دریافت بر روی سیستم کاربر روز به روز آسان تر می شود. بسته به نوع بـدافزار ، ناقـل آلـودگی مـی توانـد متفاوت باشد. بدافزار خود تکثیر می تواند از فایل آلوده یا توده های پستی برای گسترش استفاده کند. بـاج افزار در رده ای از تروجان ها که بدافزار خود تکثیر نیستند سقوط می کنـد و از روش هـای مختلـف بـرای انتقال خود استفاده می کند.

همکار ما Dmitry Gryaznov برخی از اینها را در انتشـار خـود *Malware in Popular Networks* شـرح داده است [13] .

اما وارد شدن به سیستم فقط نیمی از کار است. وظیفه مهم تر باقی ماندن و کارآمد بـودن در سیسـتم مـی باشد. هنگامی که یک بدافزار وارد سیستم می شود ، کاربران باید آلودگی را توسط خود یـا بـا اسـتفاده از اسکنر ضد ویروس شناسایی کنند ، انتخاب زنده ماندن بدافزار یا رهاشدن از بدافزار برعهده خود کـاربر مـی باشد. بقای بدافزار بستگی به انتخاب کاربران دارد. اثر بخشی برخی از بدافزارها نیـز بـه تعامـل انسـانی در برخی از سطح چرخه زندگی بستگی دارد . به طور خودکار این پیوند انسانی انجام وظیفه ای دشوار است.

در پاراگراف های زیر باید در مورد راه هایی که بعضی از کلاس های بدافزار با استفاده از تکنیک بـاج افـزار می تواند کاربر را بزور به انتخاب وادار کنند بحث کنیم.

**ابزارهای تبلیغاتی مزاحم و اعضای آن**

ابزارهای تبلیغاتی مزاحم ابعاد تازه ای است که به میدان بدافزار اضافه شده است. صنعت امنیت حتی نوع

جدیدی از طبقه بندی "برنامه بالقوه ناخواسته" [۱۴] برای شناسایی این تهدیدات که اغلب بیشتر از مزاحم های خطرناک برای کاربران هستند ایجاد کرده است. همانگونه که از نام آنها پیداست ، رفتار اصلی آنها برای نشان دادن تبلیغات به کاربران است ؛ تبلیغات گاهی اوقات بر اساس عادات گشت و گذار کاربر را مورد هدف قرار می دهند. کلیک روی این تبلیغات و یا آگهی ها معمولا کاربر را به سایت حامی می برد. با استفاده از نرم افزار های بات نت و هرزنامه های پستی ، شرکت های تبلیغاتی مزاحم در ارائه ابزارهای تبلیغاتی مزاحم برای کاربران بسیار موفق اند.

این پنجره و تبلیغات بنرها و هزنامه تنها در نمایش تبلیغاتی موفق هستند ، انتخاب با کلیک بر روی این تبلیغات و در نهایت بازدید از این سایت ها تنها به کاربر بستگی دارد. کاربر تحصیل کرده خوب و یا کاربر با تجربه های قبلی با ابزارهای تبلیغاتی مزاحم هرگز بر روی این تبلیغات کلیک نمی کند. کسب و کار ابزارهای تبلیغاتی مزاحم در شبکه های وابسته پیشرفت کرده است.

این کسب و کار و جنبه های مالی آن به خوبی در مقاله

"Adware and Spyware: Unraveling the Financial web" توضیح داده شده است [۱۲].

در این مقاله توضیح می دهد که چگونه وابسته به پرداخت پول توسط کاربر در بسیاری از انواع برنامه های مختلف می باشد.

یکی از انواع برنامه های وابسته"pay per profile" می باشد. در این برنامه ، هر یک از سهامداران مبالغ مختلف بسته به نوع عمل کاربر پرداخت می کنند که می توانند از ارسال نشانی های پست الکترونیک تا پر کردن فرم خالی متفاوت باشد.

انتخاب اقدامات با درخواست ابزارهای تبلیغاتی مزاحم با کاربر باقی مانده است. ممکن است این امکان برای ابزارهای تبلیغاتی مزاحم به استفاده از روشهای توسط باج افزار به کار رود که کاربر را بزور به این انتخاب

وادار کند. ما می توانیم تصور کنیم با ابزارهای تبلیغاتی مزاحم این اتفاق می افتد که یا کاربران را تهدید می کند که برای عملی اقدام نکنند و یا با پرسیدن از قربانیان اقداماتی به عنوان دستمزد برای امداد رسانی خود از بدافزار انجام می دهند.

**بات نت ها**

بات نت نرم افزار شبکه ربات است؛ بات نت ها مانند ارتش در اینترنت برای چندین سال اشغال کرده اند. معمولا هر بات نت هزاران نوع از رباتها را دارد. تعداد ربات ها در بات نت می تواند هر روز افزایش و کاهش یابد و تعدادی از آنها به طور عمده در بقای خود به ماشین های میزبان بستگی دارند.

هر بدافزاری در ماشین میزبان خودش تا زمانی که کاربر سیستم متوجه وجود و پاکسازی آن و یا تا زمانی که برنامه ضد ویروس آنرا تشخیص دهد و بدافزار را پاک کند زنده می ماند. برنامه های ضد ویروس شایع ترین دشمنانی هستند که بقا بدافزار را تهدید می کنند. سیستم هایی که توسط بات نت ها کنترل می شوند هیچ استثنائی ندارند.

با انواع دیگری از آلودگی ها، تحویل ربات ها به ماشین های آسیب پذیر در حال تبدیل شدن سریع تر در طول زمان می باشند.

SANS مرکز طوفان اینترنت گزارش داده است که زمان زنده ماندن کامپیوتر کاهش یافته است [۱۵]، مطالعه دیگری نشان می دهد که این زمان می تواند به میزان کم، ۲۰ دقیقه برسد [۱۶].

یکی از دلایل متعدد برای پنجره آسیب پذیری کوتاه تر این واقعیت است که بیشتر و بیشتر آسیب پذیری ها در حال حاضر به سوء استفاده zero-day تبدیل شده اند [۱۷].

بقا هنوز چالشی برای این رباتها است به دلیل اینکه فروشندگان نرم افزار ضد ویروس گاهی بروزرسانی

های ضد ویروس را غالبا هر ساعت منتشر می کنند.

ما می توانیم کنترل بات نت ها را با استفاده از برخی از تکنیک های به کار گرفته شده توسط باج افزار برای افزایش بقای برنامه ربات تصور کنیم.

در اینجا دو سناریو که ممکن است ما به آن مراجعه کنیم وجود دارد :

- توقیف کردن آنها در آغاز. تکنیک باج افزار می تواند از زمان متعلق به یک ربات کـه در دسـتگاه نصب شده است بهره برداری کند. این موضوع جمعیت ثابت برای ربات ها در هر زمان را تضمین می کند.
- توقیف کردن آنها به عنوان نیاز ناشی. مدیر ربات بعدا میتواند باج افـزار را از دسـتور بـات نـت و مرکز کنترل برای دستکاری نرخ انتشار بات نت ارسال کند.

Dagon و همکاران، در انتشار آنها شرح داده شده است [۱۶] که میزان انتشار برای بات نت متفاوت است به عنوان کاربرانی که سیستم های کامپیوتری خود را در طول شب خاموش می کنند. مدیر ربات به طور مـوثر می تواند از تکنیک های باج افزار برای اطمینان از اینکه هیچ تغییر قابل توجهی در جمعیت بات نت وجـود ندارد استفاده کند ، بنابراین نرخ انتشار مداوم را تضمین می کند. قربانیان می تواند با استفاده از این تکنیک که کامپیوترهای خودشان را در طول شب و یا برای دوره های دیگر روشن بگذارند آنها را تهدیـد کننـد. در سناریو اول در بالا ، با این حال ، برنامه های ربات بیشتر در معرض آسیب پذیری تشخیص و پـاک کـردن توسط نرم افزار ضد ویروس هستند اگر کاربران در ابتدا توسط یادداشت باج آگاه شوند.

**نتیجه**

ترکیبی از حالت های مختلف حمله، تکامل طبیعی برای هر دسته از بدافزارها برای تحویل انواع اجناس مقرون بصرفه برای حمل و نقل به ماشین کاربر داشته است. دیدن بدافزار با استفاده از بهره برداری zero-day برای رها کردن اجناس مقرون بصرفه برای حمل و نقل ابزارهای تبلیغاتی مزاحم برای توزیع بهتر و افزایش درآمد غیر معمول نیست. ما هنوز باج افزارهای که در ترکیب با تهدیدهای بدافزار دیگر برای افزایش کارایی و بقای یکدیگر استفاده می شوند مشاهده می کنیم، خطر باقی مانده است. بهترین راه برای بررسی حملات بدافزار از طریق شناسایی رفتاری آن می باشد ، و این چیزی است که فروشندگان امنیتی برجسته صنعت برای آن تلاش می کنند. ما کاربران را تشویق می کنیم که به خواسته های نویسندگان نرم افزارهای مخرب تسلیم نشوند. افزایش آگاهی و آموزش های بهتر کاربر راه درازی برای کمک به خنثی کردن این حملات خواهد بود.تحریک باج افزار ناشی از ظاهر محدود آن و اجرای مقهور تاکنون آن می باشد. ما افزایش روند باج افزار را در حالاتی که نویسندگان نرم افزارهای مخرب ممکن است در نهایت با استفاده از تکنیک های رایج توسط باج افزار استفاده کنند را پیش بینی می کنیم.

منابع:


1. Solomon, A., Nielson, B., and Meldrum, S., AIDS Technical Information, June 2000, The Center for Education and Research in Information Assurance and Security, September 2006, http://ftp.ce-rias.purdue.edu/pub/doc/general/aids.tech.info

2. Computer Incident Advisory Capability, *Information about the PC CYBORG (AIDS) Trojan horse,* December 1989, U.S. Dept. of Energy, September 2006, http://ciac.llnl.gov/ciac/bulletins/ a-10.shtml

3. McAfee Virus Information Library, *GPcoder,* June 2006, McAfee Inc., September 2006, http://vil. nai.com/vil/content/v_133901.htm

4. McAfee Virus Information Library, *CryZip,* March 2006, McAfee Inc., September 2006, http://vil.nai.com/vil/content/v_138886.htm

5. Krebs, B., *Ransomware Rising,* May 2006, The Washington Post, September 2006, http://blog. washingtonpost.com/securityfix/2006/05/ran-somware_rising_1.html

6. Espiner, T., *Beware of ransomware, firm warn*s, July 2006, CNET News.com, September 2006,http://news.com.com/Beware+of+ransomware,+firm+warns/2100-7349_3-6097741.html

7. McAfee Virus Information Library, *MayArchive,* May 2006, McAfee Inc., September 2006, http:// vil.nai.com/vil/content/v_139543.htm

8. Young, A, and Yung, M, "Crypto virology: Extortion Based Security Threats and Countermeasures," *Proceeding from the IEEE Symposium on Security and Privacy,* 1996

9. *About us,* PayPal, September 2006, http://www. paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside

10. *What is e-gold*, e-gold, September 2006,http:// www.e-gold.com/unsecure/qanda.html

11. Williams, P., "Organized Crime and Cyber-Crime: Implications for Business," *Global issues electronic journal of U.S. Dept. of State on Arrest-ing Transactional Crime* August 2001

12. McAfee Avert Labs Technical White Papers, *Ad-ware and Spyware: Unraveling the Financial Web,*
July 2006, McAfee Inc., September 2006,
http://www.mcafee.com/us/threat_center/white_pa-per.html

13. Gryaznov, D., "Malware in Popular Networks,"
*Proceedings of the 15th virus bulletin international conference,* 2005

14. *Anti-Spyware Coalition Definitions Document,* June 2006, Anti–Spyware Coalition, September 2006,
http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm

15. Internet Storm Center, Survival Time History, http://isc.sans.org/survivalhistory.php

16. Dagon, D., Zou, C., Lee, W., Modeling بات نت Propagation Using Time Zones,
*Proceedings of the 13th Annual Network and Distributed System Security Symposium,* 2006

Thomas, V., *Internet browsers and cyber-crime,* September 2006, McAfee Inc., September 2006, http://www.avertlabs.com/research/blog/?p=91