





دانشگاه پیام نور استان تهران مرکز

تهران شمال

پروژه کارشناسی

رشته مهندسی کامپیوتر

گرایش نرم افزار

عنوان پروژه :

عملکرد بدافزارها

استاد راهنما

جناب آقای دکتر سید علی ابراهیمی رضوی

تهیه کننده: زینب جلیوند (935121562)

تیر 1400

قدردانی و سپاس

پروردگار متعال را شاکر و سپاسگذاریم که توانستیم این مرحله از تحصیل را با راهنمایی های اساتید بزرگوارمان به پایان برسانیم.

بر خود لازم می دانیم که از استاد راهنمای ارجمندمان جناب آقای دکتر سید علی ابراهیمی رضوی که با راهنمایی های دقیق و ارزنده خویش در طول تحصیل و اجرای این پروژه همواره ما را یاری نموده و حق استادی را بر ما تمام کردند سپاسگذاری کنیم.

چکیده

یکی از مسائل مهم و حیاتی در امنیت سایبری امروز، ظهور حملات هدفمند با استفاده از ابزارهای پیشرفته توسط دشمنان می باشد. (اغلب تحت عنوان تهدیدهای پیشرفته مداوم¹ نامیده می شوند).

این حملات علیه سازمان ها و افراد شکل می گیرند و با یک حضور مستمر و ناشناخته و هدفمند در زیرساخت ها، اکثر موارد به دنبال جاسوسی و بدست آوردن اطلاعات هستند.

با توجه به گستردگی و تنوع و مخفیانه بودن این گونه حملات طبیعتاً مقابله با این تهدیدها و حفاظت از زیرساخت ها در برابر این گونه حملات کاری دشوار و چالش برانگیز است.

در این پژوهش سعی بر آن داریم تا به بررسی بخش فرماندهی و کنترل در این گونه حملات بپردازیم که نقشی اساسی در این حملات دارند. هدف درک روش های اسقرار فرماندهی و کنترل²، تشخیص و حذف کانال های ارتباطی آن ها می باشد.

در ادامه برای درک هرچه راحت تر روش های فرماندهی و کنترل این حملات ابتدا به طور خلاصه وضعیت فعلی حملات سایبری را بررسی می کنیم و با آخرین تغییرات در نحوه و چگونگی انجام چنین حملاتی آشنا خواهیم شد. سپس نحوه راه اندازی بخش فرماندهی و کنترل را بررسی خواهیم کرد، به این صورت که تکنیک هایی که مهاجمان برای راه اندازی کانال های ارتباطی و پنهان سازی آنها و ابزارهای امنیتی که در این راستا استفاده می شوند را ارائه خواهیم کرد.

ایجاد و استفاده از سیستم فرماندهی و کنترل بخش مهمی از حملات سایبری از راه دور است. فرماندهی و کنترل برای هدایت و کنترل سیستم آلوده شده به سمت انجام فعالیت های مورد نظر مهاجمان امری ضروری است. فرماندهی و کنترل همچنین در زمینه استخراج اطلاعات از سیستم آلوده نقش مهمی بر عهده دارد. آمار منتشر شده از حملات سایبری بیان گر آن است که این گونه حملات محدود به بخش یا سازمان یا فرد فعال در زمینه خاص نیست و در طیف وسیعی از فعالیت ها و سازمان ها و افراد حملاتی صورت گرفته که همین گستردگی تشخیص نفوذ و مقابله با آن را دشوار می کند.

یکی از روش های موثر برای مقابله با این حملات تشخیص و از بین بردن بخش فرماندهی و کنترل حملات می باشد. حداقل تاثیر این مقابله قطع ارتباط بین سیستم های آلوده با مهاجمین است که باعث ناقص ماندن حمله و در مواردی جلوگیری از نشت اطلاعات می شود.

فهرست مطالب

| | |
|----|---|
| 11 | 1- حملات هدفمند |
| 11 | 1-1- مخفی سازی حملات |
| 12 | 1-1-1- مبهم سازی الگوها |
| 12 | 1-1-2- مقابله با سیستم های تحلیل پویا |
| 13 | 1-1-3- منحرف کردن سیستم های اعتبار سنجی |
| 15 | 2- شناسایی |
| 15 | 3-1- نفوذ اولیه |
| 16 | 4-1- فرماندهی و کنترل |
| 17 | 1-4-1- ارتباطات و ترافیک فرماندهی و کنترل |
| 18 | 2-4-1- تشخیص و ایجاد اختلال در فرماندهی و کنترل |
| 22 | 3-4-1- جلوگیری از فعالیت فرماندهی و کنترل |
| 23 | 5-1- استخراج |
| 23 | ببرسی برخی نمونه های موجود |
| 23 | 1-6-1- جاسوسی سیاسی |
| 24 | 2-6-1- جاسوسی نظامی |
| 24 | 3-6-1- حملات زنجیره تامین |
| 25 | 4-6-1- جاسوسی صنعتی |
| 25 | 5-6-1- بدافزارهای مخرب منابع زیر ساختی |
| 25 | 6-6-1- بد افزار های پلی مورفیک |
| 26 | 2- شبکه های اجتماعی |
| 27 | 3- بدافزارهای مسری: ویروسه و کرم ها |

| | |
|----|--|
| 28 | 1-3- مخفی کارها: اسبهای تروا. روتکیتها و بکدورها |
| 29 | 2-3- ردگم کن (ROOTKITS) |
| 30 | 3-3- بکدورها |
| 30 | 3-4- ویروس |
| 30 | 5-3- کرم |
| 33 | 6-3- اسب تروا |
| 34 | 7-3- نرم افزار جاسوسی |
| 35 | 8-3- تبلیغات ناخواسته |
| 36 | 4- نحوه تکثیر به چه صورت است |
| 37 | 5- برنامه های ضد بدافزار |
| 38 | 6- آنالیز بدافزار |
| 47 | 7- نتیجه گیری |
| 48 | 8- مراجع |

مقدمه

Malware یا بدافزار از دو واژه تشکیل شده است ، Mal مخفف Malicious یا مخرب و Ware مخفف Software یا نرم افزار است. تمامی کدهای مخربی که نوشته می شود در رده Malware ها یا بدافزارها طبقه بندی می شوند ، این کدها می توانند شامل ویروس ها ، کرم ها ، اسب های تروجان ، adware ها ، Scare ware ها ، روتکیت ها و سایر نرم افزارهای ناخواسته باشند . البته این تعریف شخص من در خصوص بدافزارها است اما در یک وب سایت دیگر نیز در خصوص بدافزار ها چنین نوشته است : بدافزار- مخفف عبارت نرم افزار بدخواه (Malware) - یک اصطلاح فراگیر و جامع است که به هر برنامه نرم افزاری اطلاق می شود که عمدتاً برای انجام اعمال غیرمجاز و گاهیگاهاً مضر ایجاد شده است. ویروسها ، backdoor ها، کی لاگرها، برنامه های سارق کلمه عبور و سایر برنامه های تروجان، ویروسهای ماکرو در Word و Excel ، ویروس های بوت سکتور، ویروس های اسکریپت (java ، windows shell ، batch و غیره) و تروجانها، برنامه های تبهکارانه، بدافزار جاسوسی (spyware) و بدافزار تبلیغاتی (adware) تعدادی از نمونه های بدافزار هستند. زمانی، نامیدن چیزی با ویروس یا تروجان کافی بود، اما روشها و حاملهای آلودگی توسعه یافت و اصطلاح ویروس و تروجان دیگر تعریف رضایت بخشی برای همه انواع برنامه های مخرب موجود ارائه نمی کند. بصورت کلی هر نوع کد نرم افزاری که بر روی سیستم شما قرار بگیرد و عملیاتی ناخواسته را انجام دهد به عنوان بدافزار شناخته می شود ، برای مثال Spyware ها نرم افزارهای جاسوسی هستند که بدون اینکه کاربر متوجه شود کلیه اطلاعات شخصی وی را دریافت کرده برای شخص نویسنده بدافزار ارسال میکند ، worm ها یا کرم های اینترنتی بدافزارهایی هستند که خودشان را در شبکه تکثیر کرده و عملیات های مختلف تخریبی انجام میدهند، برای مثال فایل های شما را پاک میکنند، فایل های اضافی بر روی سیستم شما ایجاد می کنند و در نهایت فعالیت سیستم شما را دچار اختلال می کنند ، ویروس ها نیز جزو بدافزارهایی هستند که مشابه کرم ها عمل می کنند با این تفاوت که از طریق شبکه منتشر نمی شوند و اساس کار آنها تکثیر با استفاده از رسانه هایی مثل حافظه های فلش و سی دی ها است ، اسب های تروجان یا همان Trojan Horse ها در عین اینکه نرم افزار مفیدی به نظر می رسند خود را به یک نرم افزار مفید کاربردی متصل کرده و فعالیت های جاسوسی یا سرویس هایی که نویسنده بدافزار از آن انتظار دارند را ارائه میکند ، Adware ها را به احتمال زیاد احساس کرده اید ، اینگونه بدافزارها در هنگام استفاده از دستگاه کامپیوترتان باعث اجرا شدن صفحات تبلیغاتی مزاحم می شوند که واقعا کار کردن با سیستم را دچار مشکل کرده و

کاربر را آزار می دهند ، Scareware ها نیز همانطور که از نامشان پیداست باعث ترساندن کاربر می شوند، Root kit ها و Backdoor ها نیز جزو بدافزارهایی هستند که مهاجمین از آنها برای سوء استفاده و حمله به سیستم هدف استفاده می کنند و کاربرد تخریبی چندانی ندارند ، اما انواع بدافزارها به همین چند تا تقسیم نمی شود و بسیاری دیگر از این نوع کدهای مخرب وجود دارد.

حالا وقت آن رسیده که پاسخ این سوالات را پیدا کنیم و بدانیم که بدافزارها چگونه عمل میکنند، چرا کاربران به آنها آلوده میشوند و چگونه به گوشیهای هوشمند راه پیدا میکنند؟

رویکرد ما در مواجهه با این مساله بر مبنای یک بررسی جامع و سیستماتیک است. در حوزه کارهای آکادمیک به بررسی نشریات

ارائه شده در کنفرانس های برتر و مجلات مانند USENIX Security، ACM CCS، IEEE Security & Privacy و NDSS پرداخته ایم. در حوزه کارهای تجربی و فنی به بررسی ارائه های کنفرانس هایی مانند RSA و BlackHat ، همچنین گزارش های فنی ارائه شده توسط شرکت های امنیتی فعال در جهان پرداخته ایم.

بدافزارها توسط برنامه نویسان برای اهدافی نظیر خرابکاری و ایجاد خسارت به کار می رفتند، اما پس از گذشت چندین سال مجرمان از آن به عنوان یک منبع درآمد استفاده کردند. وقتی یک بدافزار روی رایانه شخصی شما نصب شود، آن را اصطلاحاً به یک کامپیوتر زامبی¹ تبدیل میکند که صدها هزار ایمیل اسپم² را از مردم سراسر دنیا برایتان میفرستد؛ بدون اینکه حتی بدانید یا ببینید که رایانه شما هم در توزیع حمله های این سرویسهای ناخواسته³ (DDoS) نقش کوچکی را بازی میکند. بنابراین، این طور که به نظر میرسد بدافزارها تنها میتوانند دسکتاپ ها و لپتاپ ها را هدف قرار دهند. اما متأسفانه این طور نیست!

اولین ویروس موبایل در سال 2004 توسط یک کمپانی به نام اُجام⁴ هنگام ساختن بازی موسکیتو⁴ پدیدار شد. این ویروس بدون اطلاع کاربر پیامهایی را ارسال میکرد و هزینههایی برای کاربر به وجود میآورد. چند هفته بعد، خورهایی کامپیوتر شکلی

¹ zombie computer

² distributed denial-of-service

Ojam

³ spam

⁴ Musquito

از یک ویروس مفهومی به نام کایبر¹ ایجاد کردند که میتواندست تا شعاع 10 متری خود را به هر تلفن همراهی که بلوتوث آن روشن است انتقال دهد.

اگرچه، تنها زمانی روی گوشی نصب میشد که کاربر نصب آن را بپذیرد. هرچند انتقال فایل از طریق بلوتوث کمی عذاب آور است و باتری زیادی مصرف میکند اما با ورود Commwarrior-A در سال 2005 موج جدیدی از حملات ایجاد شد که هزینه زیادی برای مردم در برداشت. این ویروس از طریق پیام چندرسانه ای انتقال پیدا میکرد و به همه دفترچه تلفن همراه (لیست مخاطبان) و سپس به تلفن دریافت کننده ها (گیرنده) راه پیدا میکرد.

تولیدکننده نرم افزار امنیتی سیمانتک² خاطر نشان کرد جذابیت تلفنهای همراه برای مجرمان سایبری افزایش پیدا خواهد کرد.

همچنین افزود احتمال اینکه کاربران اطلاعات کارت اعتباری یا کارت بانکی خود را برای خرید نرم افزار به صورت آنلاین و پرداخت به صورت بیسیم، روی تلفن همراهشان ذخیره کنند زیاد است. بنابراین سارقان علاقه زیادی دارند تا میزان آسیبپذیری این اطلاعات را امتحان کنند.

گوگل اخیراً برنامه هایی را در فروشگاه مجازی نرم افزارهایش پیدا کرده که بدافزار DroidDream در آنها پنهان بوده است البته به سرعت این برنامه ها را که بیش از 50 تا بودند از فروشگاه مجازی حذف کرد. چند بخش از این بدافزارها نیز در آیفونها یافت شدند. اما تنها در آیفونهای قفل شکسته یا اصطلاحاً جیل بَرک، زیرا خود کاربرها با این کار به نوعی امنیت دستگاههای تلفن همراهشان را تهدید میکنند. چند نوع از ویروس زئوس هم گوشیهای بلکبری را هدف قرار دادند. سیمین و ویندوزموبایل هم گاهی مورد تهدیدات امنیتی ویروسها بودهاند. به نظر میرسد که هیچ کس از دست آنها در امان نیست. پس آیا باید نگران باشید؟ سیکو بر این باور است که سالی که پیش رو داریم، سیستم عامل اندروید و iOS بزرگترین هدف تهدیدات امنیتی هستند.

¹ Cabir

² Symantec

مقاصد

انگیزه های حمله مهاجمین تغییرات اساسی کرده و از حملاتی که به خاطر کسب اعتبار و شهرت صورت می گرفت به سمت درآمد زایی و اهدافی نظری جاسوسی صنعتی یا اسناد محرمانه تغییر جهت داده {1}.

امروزه گروه های خلافکار کاملاً سازمان یافته عمل می کنند. برای هر بخش از حمله نیروهای متخصص در آن زمینه را استفاده می کنند. برای مثال نیروی متخصص برنامه نویسی بر روی کد بدافزار مخرب کار میکند، نیروی وظیفه تمرکز بر روش های درآمد زایی از اطلاعات بدست آمده را برعهده دارد و نیروی دیگر بررسی می کند که چه اطلاعاتی از سیستم های هدف می تواند درآمد زایی کافی را داشته باشد یا مورد نیاز گروه های سفارش دهنده حمله است.

گروه هایی که کمتر پیشرفته هستند بیشتر از اکسپلویت های آماده {2} یا ابزارهای فیشینگ {3} آماده استفاده می کنند البته این گروه ها همچنان به دنبال کسب شهرت از طریق انجام این حملات هستند.

فعالیت این گروه ها باعث رونق بازارهای زیر زمینی در زمینه فروش بدافزار ها، اطلاعات سرقت شده و یا هرچیزی که به این حوزه مربوط است شده است {4}{5}

گروههای سنتی فعال در این زمینه بیشتر بر روی بدست آوردن شماره و رمز حساب های بانکی تمرکز دارند که به سرعت امکان درآمد زایی فراهم شود. با این حال اخیراً آمار حملاتی که برای سرقت اطلاعاتی همچون قراردادها، طرح های تولیدی و... به طور فزاینده ای رشد پیدا کرده. جاسوسی های صنعتی و تجاری از اهداف اینگونه حملات هستند.

اخیراً برخی دولت ها برای دستیابی به اهداف خود حمایت های گسترده ای از مهاجمان می کنند تا حملاتی تا برای رسیدن به اهداف دولت برنامه ریزی و پیاده سازی کنند. حملات در سطح کشورها اغلب دارای دو هدف عمده است:

- جاسوسی سیستماتیک و جامع از کل بخش های اقتصادی و صنعتی کشورهای دیگر با هدف دستیابی به اهداف استراتژیک {6}

- خرابکاری زیرساخت های حیاتی ملی مانند نیروگاه ها و سیستم های کنترل حمل و نقل

پیامدهای این گونه حملات به اندازه ای است که برخی کارشناسان از آن ها به عنوان جنگ سایبری اشاره می کنند {7}.

شناخته شده ترین نمونه این حملات استاکس نت است که توسط ایالات متحده آمریکا و رژیم صهیونیستی برای خرابکاری در تأسیسات هسته ای جمهوری اسلامی ایران اتفاق افتاد {8و9}.

بسیاری از برنامه های آلوده کننده اولیه، از جمله اولین کرم اینترنتی و تعدادی از ویروس های سیستم عامل داس¹، به قصد آزمایش یا سرگرمی نوشته شدند. آن ها عموماً به مقاصد بی ضرر یا فقط به قصد آزار بودند، تا اینکه بخواهند خسارات جدی به سیستم های رایانه وارد کنند. در برخی موارد سازنده نمی توانست تشخیص دهد که چقدر کارش می تواند مضر باشد. برنامه نویسان جوان وقتی درباره ویروس ها و ترفندهایش می آموختند، تنها به منظور تمرین یا به این قصد که ببینند چقدر شیوع پیدا میکند، آنها را می نوشتند. در سال 1999 ویروسهای شایعی مانند ویروس ملیسا² و ویروس دیوید³ تنها به قصد سرگرمی نوشته شده بودند. اولین ویروس تلفن همراه در سال 2004 با نام ویروس کایبر بر روی تلفنهای همراه منتشر شد. با این حال مقاصد سوء به منظور خرابکاری را می توان در برنامههایی یافت که برای ایجاد آسیب به سیستم رایانه ای و یا از دست رفتن اطلاعات، طراحی شده اند. بسیاری از ویروس های سیستم عامل داس، با این هدف طراحی شدند تا فایل های موجود در یک دیسک سخت را نابود کنند یا فایل های سیستمی را با نوشتن اطلاعات نادرست بر روی آنها دچار اختلال کنند.

از زمان گسترش دسترسی به اینترنت پر سرعت، بدافزارهایی به منظور ایجاد سود طراحی شده اند. به عنوان مثال از سال 2003، اغلب ویروسها و کرم های رایانه ای، طراحی شدند تا کنترل رایانه های کاربران را به منظور بهره گیری در بازار سیاه به کار گیرند.

1 - حملات هدفمند⁴

حملات هدفمند با سناریو پیچیده و صرف هزینه های هنگفت تلاش برای دستیابی و نفوذ به اطلاعاتی از سازمان ها یا اشخاص از پیش تعیین دارند در صورتی که در گذشته حملات علیه اهداف متعددی انجام می شد و از بین افراد یا سازمان های بیشماری که آلوده شده بودند اطلاعات مورد نیاز در صورت وجود استخراج می شد.

در حملات هدفمند مهاجمین فقط بر روی یک هدف تمرکز می کنند و در صورت نفوذ به سیستم های دیگر یا افراد دیگر انتشار پیدا نمی کنند.

¹ DOS

² Melissa

³ David

⁴ APTs

چرخه عمر یک حمله به این صورت است که شامل یک مرحله شناسایی که در این مرحله ابزار دفاعی سیستم هدف مورد بررسی و تحلیل قرار می گیرند تا نقاط ضعف احتمالی شناسایی شود. {10}. سپس یک سناریو هدفمند نیاز است تا به سیستم های هدف به مدت هر چه بیشتر نفوذ شود و بدافزار در آن مستقر باشد.

1-1- مخفی سازی حملات

منظر دیگری که می خواهیم در این گزارش بررسی کنیم استفاده روز از افزون از تکنیک های مخفی سازی در این گونه حملات است که همواره در حال پیچیده تر شدن و آشکار سازی آنها سخت تر است. مهاجمان تلاش دارند تا جایی که ممکن است شناسایی نشوند و سیستم های امنیتی هدف را تحریک نکنند. برای این منظور روش هایی را استفاده می کنند که تاثیر قابل توجهی در پنهان سازی مخصوصا در سیستم های سنتی دارد.

1-1-1- مبهم سازی الگوها¹

مکانیسم های دفاعی قدیمی (مانند آنتی ویروس های قدیمی و سیستم های تشخیص نفوذ) اغلب به شناسایی الگو و ساختار برای شناسایی حملات یا کدهای مخرب تکیه می کنند. هر الگو به طور منحصر به فرد یک نوع حمله را مشخص می کند که با استفاده از مجموعه ای کاراکترها بیان می شود. این کاراکترها بر اساس نوع توابع و عبارات به کار رفته در کدهای مخرب ایجاد می شوند. مهاجمان برای اینکه در دام آنتی ویروس ها گرفتار نشوند از روش های مختلفی برای مبهم سازی کدها استفاده می کنند تا الگوی ایجاد شده توسط کدها متفاوت با نمونه های قبلی باشد و توسط آنتی ویروس ها شناسایی نشود. برای مثال پولی مورفیسم یک از روش های است که در آن کد مخرب بسته به شرایط محل اجرا رفتارهای متفاوتی از خود بروز می دهد و از شکلی به شکل دیگر تبدیل می شود و حتی یک نسخه کملا جدید از خود ایجاد می کند که همین امر باعث عدم شناسایی توسط آنتی ویروس ها می شود. {11}. اخیرا شرکت KasperSky اعلام کرده که در هر دو ثانیه بیش از دو بدافزار که از الگوها یکتا استفاده می کنند کشف می شود که به احتمال زیاد از تکنیک های چندریختی یا پولی مورفیسم² استفاده می کنند. {12}

1-1-2- مقابله با سیستم های تحلیل پویا

شرکت های امنیتی برای مقابله با روش های پولی مورفیسم که مهاجمین استفاده می کنند از ابزارهای تجزیه و تحلیل پویا سندباکس ها (جعبه شنی) استفاده می کنند. {13} این ابزار ها ابتدا کد یا برنامه ر در یک محیط ایزوله مخفی اجرا می کنند و پس از مشاهده رفتارهای کد یا ابزار نمونه، تشخیص می دهند که از نوع مخرب است یا نه. مهاجمین برای فرار از این دام نکاتی را بررسی می کنند که در اصطلاح قرص قرمز نامیده میشوند. عملکرد به این گونه است که هنگامی که بدافزار یا کدمخرب اجرا می شود در صورتی که هر نشانه ای مبنی بر این که در محیط سندباکس اجرا می شود مشاهده کند رفتارهای مخرب خود را متوقف می کند {14}

برخی از نکاتی که از آنها به عنوان قرصهای قرمز استفاده می شود بررسی فایل ها، کلیدهای رجیستری یا پروسه های در حال اجرا است تا از آنها بفهمند که آیا اثری از ابزارهای تجزیه و تحلیل بدافزار بر روی سیستم هدف است یا نه.

Signature

Polymorphism

از آنجایی که برخی از کدهای مخرب یا بدافزارهایی که توسط مهاجمین استفاده می شوند در محیط های واقعی و محیط های مجازی و شبیه سازی شده رفتار متفاوتی دارند {15،17،18،16} مهاجمین نکات دیگری را نیز بررسی می کنند تا از اجرای برنامه در محیط واقعی اطمینان حاصل کنند. برای مثال بررسی رفتارها و زمان بندی CPU که در محیط مجازی و واقعی متفاوت است.

از دیگر روش هایی که مهاجمین استفاده می کنند این است که اجرای کد مخرب یا بدافزار خود را وابسته به یک پیش شرطی می کنند تا اگر آن پیش شرط برقرار باشد برنامه اجرا شود. {19} برای مثال برنامه مخرب بررسی کند که یک فایل خاص یا یک مسیر خاص بر روی سیستم هدف وجود دارد یا نه و در صورت وجود بخشی از کد را اجرا کند و مرحله بعد را باز منوط به وجود پیش شرطی دیگر.

یا برخی وجود اتصال اینترنت را به عنوان پیش شرط قرار می دهند. برخی دیگر فقط در یک محدوده زمانی خاص فعال می شوند یا برخی منوط به وجود یک آی پی یا نام کاربری خاص هستند. یا برخی منتظر دریافت یک دستور از بخش فرماندهی و کنترل می مانند تا مراحل بعدی را اجرا کنند.

در گام بعدی جنگ بین مهاجمان با مکانیسم های دفاعی، بدافزارنویسان شروع به نوشتن کدهایی کردند تا انرژی مکانیسم های دفاعی را هدر دهند {20}. قبل از اجرای هرگونه فعالیت مخرب توسط بدافزار این کدها اجرا می شوند، هدف از این کدها ایجاد تاخیر در فعالیت سیستم های دفاعی تا با افزایش زمان فرصت بررسی کدهای اصلی بدافزار را به مکانیسم های دفاعی ندهند. در نتیجه مکانیسم های دفاعی کدها را مخرب تشخیص نداده و هیچ گونه فعالیت مشکوکی مشاهده نخواهند کرد.

از آنجایی که سند باکس ها و ابزارهای تجزیه و تحلیل پویا باید حجم زیادی از برنامه ها را بررسی کنند، برای اینکه منبع سیستم را بیش از حد اشغال نکنند زمان محدودی را به این امر اختصاص می دهند. بدافزارنویسان کدها و برنامه مخرب خود را طوری طراحی می کنند تا در این مدت زمان مشخص هیچ فعالیت مشکوکی از خود بروز ندهد و پس از آن فعالیت اصلی خود را انجام دهد. همین کار باعث فرار از شناسایی توسط سیستم های دفاعی می شود.

1-1-3 - منحرف کردن سیستمهای اعتبار سنجی

یک از مکانیسم های دفاعی که در سالهای اخیر کشف شده است استفاده از اطلاعات اعتبار سنجی شده (نام دامنه و سرورها) در شبکه است. این ایده به این صورت است در صورتی که اتصالات زیادی یا بلند مدتی به دامنه ها یا آی پی هایی که اعتبار سنجی نشده اند صورت بگیرد پس از مدتی این دامنه ها یا آی پی ها مسدود میشوند.

بدافزار نویسان برای مقابله با این سیستم دفاعی از یک روش سخت اما موثر استفاده می کنند. آنها از یک سرور یا دامنه خاص برای یک مدت زمان محدود استفاده می کنند، پس از آنکه آی پی و یا نام دامنه در لیست سیاه قرار گرفت دیگر از آن آی پی و دامنه استفاده نمی کنند و آی پی و نام دامنه دیگری جایگزین می کنند. این استراتژی هزینه و نیروی مضاعفی از مهاجمان در اختیار می گیرد اما موثر است.

نتایج منتشر شده از محققان گوگل نشان می دهد که این روش اکنون به خوبی در حال اجرا توسط مهاجمین است و متوسط مدتزمان طول عمر دامنه و سرورهای آنها 5.2 ساعت است. {2}

1-4-1 - استکانوگرافی¹

در حالی که سیستم هایی مانند Tor به منظور ناشناس بودن مبدا و مقصد ارتباط ایجاد شده اند، روش هایی نیز وجود دارند که داده مبادله شده را نیز غیر قابل رهگیری و شنود می کنند. رایج ترین روش برای ارتباط غیر قابل شنود استفاده از روش استکانوگرافی است.

استکانوگرافی کلمه است یونانی به معنی مخفیانه نوشتن و به روشی اتلاق می شود که در آن پیام ها طوری نوشته می شوند که فقط گیرنده و فرستنده قادر به خواندن پیام هستند. دو راه برای استفاده از استکانوگرافی توسط بدافزار برای ارتباطات فرماندهی و کنترل وجود دارد. اول اینکه بدافزار ها می توانند پروتکل ارتباطی خود را مانند دیگر پروتکل ها در نظر بگیرند. دوم می توانند داده های مبادله ای خود را در محتوای قانونی مانند تصاویر بگنجانند. امروزه اکثر انواع فایل مانند متنی، عکسی و ویدیو می توانند داده هایی را به روش های مختلف درون خود مخفیانه ذخیره کنند. در ساده ترین روش استفاده از اضافه کردن متادیتا² به فایل برای ذخیره سازی اطلاعات است البته این روش به راحتی قابل کشف شدن است. از روش های جایگزین نیز می توان استفاده کرد به عنوان نمونه استفاده از تغییر در محتوای خود فایل پیشرفته تر و بهتر است. برای مثال در یک فایل تصویر هر پیکسل می تواند مقداری اطلاعات ذخیره کند که بر حسب اندازه و کیفیت تصور این میزان میتواند مقدار قابل توجهی باشد. و تغییراتی که در عکس ایجاد می شود به راحتی با چشم تشخیص داده نمی شود.

در فایل صوتی با استفاده از ایجاد اکو و ایجاد تاخیر در حد میلی ثانیه که گوش معمولی متوجه آن نمی شود می توان اطلاعاتی را ذخیره کرد. روش های مختلفی برای استکانوگرافی وجود دارد اما در حال حاضر تعداد کمی از بدافزارها از استکانوگرافی استفاده می کنند. انتظار می رود با گذشت زمان و پیشرفت مکانیسم های دفاعی استفاده از روش های استکانوگرافی افزایش پیدا کند.

یکی از بدافزارهایی که از یک فرم از استکانوگرافی استفاده میکند تروجان trojan.downbot است {21}

این بات از طریق ایمیل گسترش پیدا کرد و اولین کاری که پس از اجرا انجام می دهد به وبسایتی تحت کنترل مهاجم که آدرس آن ها در کد بدافزار است متصل می شود. این وبسایت در ظاهر یک سایت آموزشی کدنویسی است که هر کسی به راحتی می تواند به آن دسترسی پیدا کند و بی ضرر است. اگر سورس صفحه تحلیل شود این کد شامل توضیحات رمز شده و کدهایی

است که در بایت های فایل تصاویر اضافه شده است. این توضیحات و تصاویر حاوی دستورات بخش فرماندهی و کنترل برای بدافزارها هستند، برای مثال آی پی و پورت هایی که برای آپلود اطلاعات توسط بدافزارها باید استفاده شود.

Steganography

MetaData

این روش یک تکنیک موثر برای ارتباط با بدافزارهاست زیرا که لاگ ذخیره شده کاملاً نرمال و قانونی است زیرا یک صفحه html عمومی بازدید شده است و همچنین امکان مسدود کردن آن وجود ندارد زیرا این ارتباط یک ارتباط http است و در صورت مسدود نمودن http کاربر برای مشاهده سایر صفحات نیز به مشکل بر می خورد.

بررسی نمونه stegobot

stegobot یک نمونه از بات نت غیرمتمرکز است که از پروتکل های بر پایه استکانوگرافی غیر قابل شنود استفاده می کند.

این بدافزار از آپلود تصاویر توسط کاربران در شبکه ای اجتماعی برای مبادله اطلاعات استفاده می کند. برای مثال استفاده از شبکه اجتماعی facebook را در دستور کار خود دارد. شبکه اجتماعی facebook به این صورت است که کاربر تصویری را از طریق وب بارگزاری میکند و هنگامی که به مرور دیگر فعالیت های کاربران دیگر می پردازد تصاویر تازه بارگزاری شده آنها به طور موقت در دستگاه لوکال کاربر ذخیره می شود. این بدافزار قبل از آپلود شدن تصاویر اطلاعات را درون آنها قرار می دهد. همچنین از تصویری که به طور موقت در سیستم لوکال کاربر ذخیره می شود اطلاعاتی را دریافت می کند. هدف اصلی این بدافزار جمع آوری اطلاعات بانکی و رمز های عبور است.

1-2- شناسایی

در این مرحله مهاجمان اطلاعاتی را درباره هدف بدست می آورند و نقاط ضعفی را که می توان از آنها برای نفوذ استفاده کرد را شناسایی می کنند. این شناسایی هم بر روی افراد و هم تجهیزات هدف صورت می گیرد. مهاجمین شبکه ها و سیستم های هدف خود را با استفاده از روش های معمول مانند پورت اسکن و ... شناسایی می کنند تا حفره های امنیتی را کشف کنند. مهاجمین همچنین اطلاعاتی را در مورد افراد کلیدی در سازمان هدف بدست می آورند تا از آنها برای رسیدن به هدف خود استفاده کنند برای مثال در این مرحله می توان از اطلاعاتی که افراد در صفحات اجتماعی خود قرار می دهند استفاده کرد.

1-3- نفوذ اولیه

در این مرحله مهاجمان می توانند به شبکه هدف نفوذ کنند. اغلب نفوذهای معمولاً از روزنه فیشینگ¹ انجام می شود. یک پیام فیشینگ ممکن است یک پیوست آلوده یا یک لینک وبسایت آلوده باشد {22}. معمولاً پیامی که برای پیام های فیشینگ طراحی می شود بر اساس اطلاعاتی است که در مرحله شناسایی بدست آمده و هدف نسبت به آن واکنش نشان می دهد و مورد توجه هدف است.

روش دومی که برای ایجاد روزنه نفوذ اولیه استفاده میشود استفاده از وب سایت هایی است که مورد علاقه اهداف می باشد (روش حفره آبی¹). در این روش مهاجمان کدهای مخرب خود را در وبسایت هایی قرار می دهند که احتمالاً توسط هدف مورد بازدید قرار می گیرند:

هنگامی که هدف از وبسایت بازدید می کند کدهای مخربی برای ایجاد ارتباط اولیه بر روی سیستم قربانی ایجاد خواهد شد. حملات حفره آبی نسخه پیشرفته ای از حملات مبتنی بر داندلود ناخواسته است {23،24}. قربانیان با توجه به علائق خود از وبسایت هایی بازدید می کنند که این وب سایت ها بدون کسب اجازه از قربانی کدهای مخربی را بر روی سیستم هدف بارگذاری می کنند که معمولاً به زبان جاوا اسکریپت نوشته می شوند. معمولاً آسیب پذیری هایی که مهاجمان از آنها استفاده می کنند در مرورگرها و یا پلاگن هایی که مرورگرها از آنها استفاده می کنند وجود دارد و باعث می شود کنترل سیستم هدف در اختیار مهاجمین قرار گیرد {25،26}

1-4- فرماندهی و کنترل

ما در حال حاضر در مرکز یک بحران در زمینه امنیت کامپیوترها هستیم:

تعداد حملات ، پیچیدگی و تاثیر بالقوه آنها در چند سال گذشته به طور قابل ملاحظه ای رشد داشته است. به طور خاص حملات هدفمند به چالش برانگیزترین تهدید امروز تبدیل شده است. حملات هدفمند افراد خاص یا سازمان هایی را هدف قرار می دهند که داده های محرمانه مانند قراردادهای، طرح های تجاری و تولیدی، اسناد نظامی و... در اختیار دارند. این حملات ابتدا شناساییهای گسترده و جمع آوری اطلاعات دقیقی برای بدست آوردن نقاط ضعف در مکانیسم دفاعی اهداف انجام می دهند سپس با استفاده از ابزارهای مخرب پیچیده اقدام به انجام حمله می کنند (به طور مثال مکان یابی و سرقت اسناد حساس از داخل شبکه هدف).

به علت ماهیت این گونه حملات مقابله با آنها بسیار دشوار است. مهاجمین در این حملات برای نفوذ کردن و کنترل کردن سیستمهای هدف گاهی اوقات از اکسپلویت های زیرو دی². {27} و هم چنین کدهای مخربی که برای مقابله با مکانیسم های دفاعی هدف طراحی شده اند استفاده می کنند.

¹ Phishing

آنها هم چنین ممکن است از تکنیک های مهندسی اجتماعی که برای سوء استفاده از انسان ها طراحی شده، استفاده کنند. به اینصورت که با متقاعد کردن افراد مشغول به کار در مجموعه هدف آنها را به سمت اجرای اهداف خود هدایت می کنند مانند نصب و راه اندازی نرم افزارهای مخرب. وجود یک فرد در سازمان که نکات امنیتی را رعایت نمی کند کافی است تا کل زنجیره دفاعی سازمان از هم متلاشی شود {28}. شناسایی روزنه اولیه که باعث ایجاد ارتباط بین فرماندهی و کنترل با سیستم هدف شده استدر مقابله با این حملات بسیار حائز اهمیت است.

watering hole

Zeroday

مسدود کردن کانال ارتباطی فرماندهی و کنترل چندین مزیت دارد. اگر اطلاعات حساس از بین نرفته باشند به سرعت از نشتبیشتر این اطلاعات جلوگیری می شود. در حالی که امنیت سازمان هدف به خطر افتاده است اما هنوز اسناد و اطلاعات با ارزش برای سازمان حفظ خواهد شد. حتی اگر اطلاعاتی نیز به سرقت رفته باشد درک ساختار فرماندهی و کنترل بدافزار می تواند برای یافتن سر منشا اصلی حمله مفید باشد تا برای طی مراحل قانونی اقدام شود.

مرحله فرماندهی و کنترل مرحله ای است که پس از نفوذ اولیه انجام می شود. به طور دقیق تر سیستم آلوده شده یک کانال ارتباطی با مهاجمین ایجاد می کند تا مهاجمین بتوانند سیستم را تحت کنترل خود قرار دهند. این کانال ارتباطی با فرماندهی و کنترل مهاجمین را قادر می سازند تا با استفاده از ابزارهای دسترسی از راه دور اقدام به نصب و اجرای ماژول های مخرب یا گسترش آلوده سازی به سایر قسمت های هدف و یا حملات DOS کنند. بخش فرماندهی و کنترل با توجه به اطلاعاتی که پس از اولین اتصال از سمت سیستم آلوده به سمت مهاجمان می آید مراحل بعدی حمله را مشخص می کند تا به نتیجه دلخواه از حمله برسند.

حوزه امنیت بسایر حوزه پیچیده و تغییر پذیری است به این معنی که بر اساس انواع حملاتی در حوزه سایبری اتفاق می افتد امنیت سایبری نیز متناسب با آنها تغییر می کند تا توانایی مقابله با حملات جدید را داشته باشد. در این پژوهش فرض را بر این قرار دادیم که این تغییرات در نوع حملات به کندی اتفاق می افتد و بیشتر به حملاتی که اکنون رایج هستند پرداخته ایم.

1-4-1 - ارتباطات و ترافیک فرماندهی و کنترل

مهاجمان روش ها و استراتژی های مختلفی را برای ایجاد یک ساختار فرماندهی و کنترل قوی و قابل اعتماد با کانال های ارتباطی مخفیانه پیاده سازی می کنند. که همین امر باعث به وجود آمدن طیف وسیعی از معماری ها و روش های مختلف و کارآمد در پیاده سازی بخش فرماندهی و کنترل گردیده است. به عنوان مثال برخی از مهاجمان معماری های خود را بر اساس

پروتکل های ارتباطی HTTP و IRC بنا می کنند. برخی دیگر از مهاجمان به تازگی به سمت استفاده از پروتکل های P2P برای ارتباط با بخش فرماندهی و کنترل گرایش پیدا کرده اند که از کار انداختن این گونه معماری دشوار تر از روش HTTP یا IRC است. همچنین استفاده از معماری هایی که بر پایه ارتباط مستقیم از طریق کانال هایی که اطلاعات به صورت رمز از آن ها عبور می کنند باعث می شود دسترسی دیگر افراد به اطلاعاتی که در حال مبادله است محدود و حتی غیر ممکن شود. برخی دیگر از مهاجمان از طریق صفحات و تصاویر در شبکه های اجتماعی و یا شبکه های ارتباطی ناشناس مانند Tor اقدام به مبادله داده بین بخش فرماندهی و کنترل با سیستم های آلوده می کنند.

سیستم فرماندهی و کنترل برای اکثر بدافزارهای مدرن دارای سه بخش است. کشف کننده کنترلر، پروتکل ارتباطی کنترل کننده بات و ساختار فرماندهی و کنترل.

در فاز کشف کنترل کننده بدافزار تلاش می کند تا موقعیت سیستم کنترل کننده را پیدا کند. توپولوژی سیستم ممکن است اشکال مختلفی داشته باشد و از انواع متمرکز یا غیر متمرکز باشند. در آخر نیز یک ارتباط از بدافزار به کنترل کننده ایجاد می شود. این سه فاز اغلب از هم جدا و به طور مستقل هستند به این معنی که می توان یک فاز را تغییر و به روز رسانی کرد در حالی که قسمت های دیگر ثابت هستند.

1-4-2 - تشخیص و ایجاد اختلال در فرماندهی و کنترل

معماری بخش فرماندهی و کنترل اوایل از نوع متمرکز بود مانند استفاده از کانال IRC در این نوع معماری اگر سیستم های دفاعی حمله و کانال ارتباطی را شناسایی می کردند و سرور را از کار می انداختند به طور موثری بخش فرماندهی و کنترل دیگر کارایی نداشت. چنین معماری هایی بسیار شکننده و با شیوهی مهندسی نرم افزاری ضعیفی همراه بود. به عنوان مثال معمولا آدرس سرورها داخل کد بدافزار به صورت استاتیک قرار میگرفت.

گسترش بات نت ها و به طبع آن مکانیسم های شناسایی سرورهای فرماندهی و کنترل متمرکز {37,63,53,43,3233,13,03,29} باعث شد تا طراحی غیر متمرکز یک به یک با بات نت ها شکل بگیرد.

بات نت هایی که در سال های اخیر کشف شده اند مانند storm،peacomm و conficker اغلب از ساختار شبکه های چندلایه استفاده می کنند. {38,93,40}

این شبکه ها حاصل تحقیق در ساختارهای ارتباطی کارآمد هستند و مزایایی هم دارند. غیر متمرکز بودن فرماندهی و کنترل کار را برای اتصال به این بخش توسط بات نت سخت تر می کند اما توانایی مخفی کاری بات نت را افزایش می دهد.

تکنیکها و روش های مختلفی برای شناسایی و از کار انداختن بخش فرماندهی و کنترل ارائه شده است. این روش ها معمولا بر پایه مانیتورینگ و تجزیه و تحلیل ترافیک شبکه برای شناسایی ترافیک های مخرب می باشند. مهاجمان برای کاهش ضریب شناسایی به طور مداوم در حال تغییر روش های ارتباط هستند به همین دلیل نظارت و آنالیز مداوم شبکه امری ضروری است. در ادامه لیستی از اقدامات برای شناسایی و از بین بردن بخش فرماندهی و کنترل در زمان وقوع این حملات ارائه شده است.

شناسایی ترافیک های مخرب در شبکه بر اساس الگوهای از پیش شناخته شده

جمع آوری و تجزیه و تحلیل ترافیک شبکه برای شناسایی فعالیت هایی که توسط کانال های ارتباطی فرماندهی و کنترل ایجاد می شوند.

* مانیتور ترافیک DNS برای شناسایی دستگاه های داخلی ای که تلاش می کنند با دامنه مخرب شناخته شده ارتباط بگیرند. برای این منظور باید همواره لیستی از دامنه های شناخته شده به عنوان فعال در زمینه فرماندهی و کنترل (این لیست باید حاوی نام دامنه های مخربی که به طور عمومی توسط شرکت های امنیتی منتشر شده و هم نام دامنه هایی که توسط تیم آنالیز داخلی سازمان کشف شده باشد) موجود باشد که در صورت مشاهده ارتباط گیری دستگاه ها با هریک از این دامنه ها اقدام متقابل صورت گیرد.

* مانیتور ترافیک IP برای شناسایی دستگاه های داخلی ای که تلاش می کنند با IP مخرب شناخته شده ارتباط بگیرند. برای این منظور می توان از اطلاعاتی که ابزارهایی مانند NetFlow و sFlow در اختیار قرار میدهند و همچنین لیست سیاهی که حاوی IP های شناخته شده مخرب است استفاده کرد.

* مانیتور محتوای ترافیک شبکه برای شناسایی محتواهایی که الگوی منطبق با الگوهای مخرب شناخته شده دارند. برای این منظور می توان یک Sniffer بر روی شبکه فعال کرد و اطلاعات بدست آمده را با الگوهای مخرب مقایسه کرد.

اقدامات فوق برای تشخیص کانال های ارتباطی با فرماندهی و کنترل هایی که توسط بدافزارهای شناخته شده ایجاد شده اند یا بدافزارهایی که از این کانال های از پیش شناخته شده استفاده می کنند به کار می روند.

با گسترش و تکامل بخش فرماندهی و کنترل سیستم های دفاعی رویکرد جدیدی اتخاذ کردند، آنها پورت ها و پروتکل هایی را که در شبکه بدون استفاده بودن را مسدود کردند و فقط پورت ها و پروتکل هایی که ابزارهای قانونی و مورد نیاز از آنها استفاده می کردند را قابل استفاده گذاشتند. همین امر مهاجمین را تشویق کرد تا سعی کنند تا از پورت ها و پروتکل های رایج و قانونی استفاده کنند. برای مثال از طریق درج نظر در صفحات وب یا درج پست در انجمن های عمومی برای تبادل داده استفاده می کنند.

همین کار باعث می شود امکان مسدود کردن یا غیر فعال کردن کانال ارتباطی به شدت کم شود.

پیشرفت جالب طراحان بخش فرماندهی و کنترل این است که سعی در ناشناس کردن مقصد ارتباطات خود کرده اند. به این معنی که با استفاده از پروکسی ها، نقاط انتهایی این ارتباطات را مخفی کنند.

اخیرا مهاجمان استفاده از سیستم هایی مانند JAP،Tor را آغاز کرده اند {41،42}. مخفی کردن نقاط مقصد ارتباطات مانع از شناسایی و فیلتر کردن بخش فرماندهی و کنترل توسط سیستم های دفاعی می شود حتی اگر الگوهای ترافیکی را هم شناسایی کنند.

تشخیص فعالیت های مخرب شبکه که مطابق با الگوی از پیش شناخته شده نیستند

جمع آوری و تجزیه و تحلیل ترافیک شبکه به منظور شناسایی فعالیت هایی غیر معمولی که در شبکه اتفاق می افتد.

* ایجاد یک پایگاه داده های ترافیکی عادی شبکه که حاوی الگوهای ارتباطی نرمال، حجم داده های مبادله شده و... می باشد که در ساعات و روزهای مختلف بررسی و جمع آوری شده است.

* مقایسه ترافیک فعلی شبکه با پایگاه از پیش ایجاد شده برای ترافیک های نرمال، در صورتی که ترافیک فعلی شبکه مطابق با الگوی نرمال از پیش تعیین شده نباشد احتمال وقوع حمله وجود دارد.

اقدامات فوق کمک به شناسایی کانال های ارتباطی بین بخش فرماندهی و کنترل با سیستم های آلوده می کند، کانال هایی که از قبل شناخته شده نیستند و توسط هیچ بدافزار شناخته شده ای قبلاً استفاده نشده اند.

- معماری متمرکز

طراحی های ابتدایی فرماندهی و کنترل بر پایه معماری متمرکز بودند به این صورت که یک یا چند سرور منحصراً برای ارتباطات استفاده می شدند.

طراحی دیگری که در این زمینه استفاده می شد استفاده از سرور های IRC بود. IRC در سال 1988 ایجاد شد و پروتکلی بود که برای مبادله متن بر بستر اینترنت استفاده می شد. به همین منظور کانال هایی ارائه داده بود که امکان چت های گروهی یا شخصی را فراهم می کرد. کانال ها بر روی سرورهایی قرار داشتند که بخشی از شبکه IRC را تشکیل می دادند. علاوه بر اینکه برخی کانال ها عمومی بودند این امکان نیز وجود داشت تا برای ورود به کانال اعتبار سنجی صورت بگیرد. همچنین اعضای کانال دارای سطح دسترسی های مختلفی بودند. چیزی مانند کانال های تلگرامی امروزه. این سیستم یک امکانی را برای ارتباطات بدافزارها فراهم کرد بود تا دستورات از فرماندهی و کنترل به بدافزارها برسد و بالعکس. معماری متمرکز ساده و مدیریت آن راحت بود البته امکان از دست رفتن ناگهانی شمار زیادی از سیستم های آلوده نیز در آن بسیار است. {43} - معماری غیر

متمرکز

برای مقابله با ضعف های ساختاری و محدودیت های معماری متمرکز بسیاری از طراحان C2 به سمت طراحی فرماندهی و کنترل غیر متمرکز یا p2p گرویدند. اهداف اصلی این معماری عبارت است از:

توسعه پذیر باشد به این معنی که با رشد تعداد بات ها با صرف هزینه اندک بتوان بخش فرماندهی و کنترل را متناسب با آن رشد داد. تحمل خطای بالا به این معنی که در صورتی که مشکلی در فرماندهی و کنترل پیش آمد امکان رفع سریع آن یا جایگزینی آن وجود داشته باشد. در یک شبکه p2p سرور کنترل مرکزی وجود ندارد بلکه هر عضو شبکه می تواند به عنوان یک سرور عمل کند.

علاوه بر نکات فوق معماری غیر متمرکز در برابر حملات سیستم های دفاعی مقاوم تر است زیرا برای از کار انداختن کل بخش فرماندهی و کنترل باید تمامی بخش های کوچکتر و جدا از هم از بین بروند.

استفاده از شبکه های غیرمتمرکز C2 برگرفته از شبکه های اشتراک گذاری فایل p2p است.. در شبکه p2p هر عضو شبکه می تواند با تعداد نامحدود از دیگر اعضای و مجاورانش در شبکه ارتباط برقرار کند.

اعضای شبکه فقط می توانند با مجاوران خود در شبکه ارتباط برقرار کنند با ترکیب انواع مختلفی از شبکه p2p می توان تبادل داده را در کل شبکه برقرار کرد. شبکه های p2p میتوانند از نوع چند لایه بدون ساختار باشند (Bittorrent, Gnutella, orKazaa) یا شبکه های چندلایه ساختار یافته مانند:

CAN, Chord, Pastry, deBruijnbased options (Koorde, ODRI, Broose ,D2B), Kautz, Accordion, Tapestry ,Bamboo, and Kademilia

اکنون به بررسی عملکرد شبکه بیت تورنت می پردازیم. برای دستیابی به یک فایل در شبکه، کاربر یک فایل ردیاب را دانلود میکند که شامل لیست اعضای از شبکه است که دارای قسمتی یا کل فایل هستند. سپس کاربر به طور مستقیم به آنها وصل می شود و قسمتی را که نیاز دارد دانلود میکند. در نهایت شما کل فایل را دانلود خواهید کرد. هرچه تعداد نیزبان ها بیشتر باشد سرعت دانلود فایل نیز سریع تر خواهد بود.

به این ترتیب شبکه می تواند یک روش آسان برای انتشار اطلاعات در میان تعداد زیادی از کاربران بدون استفاده از یک سرور مرکزی فراهم کند.

یک روش معمول برای بدافزارها این است که بدافزار لیستی از میزبان ها که می تواند به آن ها متصل شود را در اختیار دارد و به طور تکرارشونده بررسی می کند که از این طریق دستوری ارسال شده است یا نه. کنترل کننده بات دستوری را برای یک یا گروهی از گره ها که در هر جای شبکه ممکن است قرار داشته باشند ارسال می کند و از طریق الگوریتم سیل آسا دستور به تمام گره ها می رسد. مزیت این روش این است که نیازی به یک ارتباط مستقیم بین داده ها و ارسال کننده (مانند سیستم متمرکز) نیست.

Tor

سرویس است که امکان ناشناس بودن در محیط اینترنت را فراهم می کند. از این امکان هم اشخاص و هم دولت ها استفاده می کنند.

اصول کار این سرویس بر این اساس است ترافیک اینترنت را از تعداد زیادی گره عبور می دهد و در هر عبور رمزنگاری و رمزگشایی می شود. شناسایی فرستنده و گیرنده داده ها از این طریق بسیار دشوار است. همین امر سبب شده برخی از بدافزار نویسان از این سرویس برای تبادل داده بین قربانی ها و بخش فرماندهی و کنترل استفاده کنند. برای اینکه از این سرویس استفاده کنید ابتدا باید به سادگی نرم افزار این سرویس را نصب کنید پس از آن شما به عنوان بخشی از این شبکه خواهید بود. یکی از قابلیت های پیشرفته تر tor توانایی ایجاد سرویس های مخفی است. این امر به یک سرور اجازه می دهد تا پشت

پروکسی مخفی شود و هویت واقعی آن را از کسانی که به آن دسترسی دارند پنهان نگه دارد. در سال 2013 شبکه تور با افزایش ناگهان کاربران مواجه شد اما با بررسی گره های خروجی این شبکه مشخص شد که این ترافیک خیلی افزایش نداشته است. پس از بررسی های بیشتر مشخص شد که بات نت SDC مشغول به استفاده از شبکه تور است {44} بات نت SDC بخش فرماندهی و کنترل خود را در پشت تور مخفی کرده بود.

بررسی نمونه: اسکای نت

اسکای نت یک بات نت با اندازه متوسط 12000 دستگاه جزو بدافزارهای خانواده زئوس است. نکته جالب توجه درباره این بدافزار (به جز استفاده از تور) این است که کنترل کننده آن در بخش آی ام ¹ (پرسش و پاسخ) در ردیت ² است. زمانی که یک تیم از محققان {45} یک نمونه بدافزار را کشف کردند، با مطالعه اطلاعاتی که در پست ردیت قرار داشت و هم چنین استفاده از مهندسی معکوس به شناخت تقریباً کاملی از بات نت مورد نظر برسند. این بدافزار از طریف شبکه اشتراک گذاری فایل یوزنت ³ گسترش پیدا کرد و عمدتاً برای حملات ddos، سرقت اطلاعات و استخراج بیت کوین استفاده می شد. زمانی که بدافزار بر روی یک سیستم نصب می شد، نرم افزار Tor نیز نصب شده و یک سرویس مخفی تور بر روی دستگاه تنظیم میکرد. تمام ارتباطات با بخش فرماندهی و کنترل از طریق پروکسی های تور که بر روی سیستم تنظیم شده بودند انجام می شد. سرویس مخفی ایجاد شده بر روی پورت 55080 فعالیت میکرد. بخش فرماندهی و کنترل که یک سرور IRC بود پشت سرویس مخفی تور فعال بود.

سرور بر روی دامنه uy5t7cus7dptkchs.onion و پورت 16667 قرار داشت. کنترلر از طریق کانال IRC دستور را به بدافزار می فرستاد. این بدافزار همچنین شامل یک نسخه نرم افزار مخرب از خانواده زئوس نیز بود. زئوس یک تروجان بانکی رایج است که هدف اصلی آن سرقت اطلاعات شخصی مالی (مانند شماره کارت های اعتباری و رمز عبور آنها) است. زئوس یک سرور فرماندهی و کنترل دارد که کنترل کننده آن پشت سرویس مخفی تور قرار دارد. پس از دسترسی پیدا کردن به سرور کنترل کننده، محققان یک فایل xml حاوی اسامی وب سایت های هدف را پیدا کردند. قسمت نهایی بدافزار وظیفه استخراج بیت کوین را برعهده داشت. بدافزار با استفاده از برنامه GCMiner اقدام به استخراج بیت کوین میکرد. جالب توجه این بود که هفت آی پی متعلق به پروکسی سرورها یافت شد که دو تای از آنها فعال بودند و هیچ کدام توسط تور مخفی نشده بودند. با توجه به استفاده از تور تقریباً غیر ممکن بود که صاحب و مکان سرورهای فرماندهی و کنترل مشخص شود. از طریق پاسخ های در پست ردیت و همچنین تمرکز بات نت ها در مرکز اروپا (به ویژه هلند و آلمان) به احتمال زیاد اپراتور در آلمان مستقر بود.

1-4-3- جلوه‌گیری از فعالیت فرماندهی و کنترل

طراحی و پیاده سازی شبکه باید به گونه ای باشد که بخش فرماندهی و کنترل در حملات کارایی لازم را نداشته باشد و تا حد زیادی از فعالیت این بخش جلوه‌گیری شود.

* جداسازی شبکه به بخش های مختلف بر اساس میزان امن بودن، سطح طبقه بندی داده های موجود در شبکه و... (به عنوان مثال بخش سرورهای عمومی، سرورهای داخلی، ذخیره سازها و ...)

* قوانین و سیاست های را ایجاد کنید که سرعت ترافیک داده در نقاط ناامن شبکه کاهش پیدا کند.

* مسدود کردن ارتباطات ناخواسته یا بدون استفاده تا مورد سوء استفاده بخش فرماندهی و کنترل قرار نگیرند.

¹<https://www.reddit.com/r/IAMa/>

www.reddit.com

³ Usenet

بررسی نمونه: طوفان¹

یکی از بات نت های که به خوبی از شبکه p2p برای فرماندهی و کنترل خود استفاده می کند طوفان است. بات نت طوفان در بیشترین حالت خود در سال 2007، بین یک تا 50 میلیون سیستم را آلوده کرده بود. بدافزار طوفان تنها از طریق ایمیل های اسپم، که دارای محتوای لینک به وبسایت های مخرب یا لینک های تبلیغاتی که بدافزار را بر روی سیستم قربانی بارگیری می کرد توانست این حجم آلوده سازی را انجام دهد. اولین کاری که بدافزار بعد از اجرا بر روی سیستم قربانی انجام می داد این بود که بررسی کند که ساعت سیستم صحیح باشد. آن موضوع برای تبادلات حیاتی است. بدافزار طوفان از OVER-NET استفاده می کرد که یک شبکه P2P مبتنی بر kademia و دارای جدول درهم سازی توزیع شده است (DHT).

هر بات دارای یک شناسه 128 بیتی است که به صورت تصادفی ساخته می شود. گره ای حامل پیامی برای گره ای دیگری بود پیام را به سمت نزدیک ترین شناسه به گره مقصد هدایت می کرد. بدافزار طوفان مانند بسیاری از شبکه های P2P از ارتباطات publish/subscribe style استفاده می کرد.

یک گره اطلاعات را با استفاده از شناسه تولید شده منتشر می کند سپس گیرنده اطلاعات با استفاده از شناسه اقدام به دریافت اطلاعات می کنند.

¹ Storm

1-5- استخراج

در این مرحله مهاجمین اطلاعات را از سیستم قربانی استخراج، جمع آوری و رمز گذاری می کنند. سپس اطلاعات از همان کانال ارتباطی که ابتدا ایجاد شده به بخش فرماندهی و کنترل ارسال می گردد. برای مثال اطلاعاتی از قبیل شماره حساب بانکی رمز و دیگر مشخصات که توسط ثبت کننده کلید ها جمع آوری و رمز می گردد و سپس برای بخش فرماندهی و کنترل ارسال می گردد. {46}{47}

1-6- بررسی برخی نمونه های موجود

در این بخش به بررسی چند نمونه از حملات هدفمند می پردازیم.

1-6-1 - جاسوسی سیاسی

در ماه ژانویه 2013، نیویورک تایمز اعلام کرد که به مدت چهار ماه تحت حملات هدفمند قرار گرفته است. حملات توسط هکر های چینی صورت گرفته بود {48}. با تحقیقات بیشتر بر روی روش های انجام این حملات مشخص شد که این حملات در طرح گسترده کمپانی هایی را که در زمینه اخبار و تحلیل های سیاسی فعالیت می کردند را هدف گرفته و مشخص شد شرکت هایی نظیر بلومبرگ به مدت حدود یکسال در معرض این حملات بوده اند.

تحقیق درباره این حادثه نشان داد که هکرهاي چینی از طریق نفوذ به چندین حساب کاربری در دانشگاه های ایالات متحده آمریکا سعی در پنهان سازی هویت خود داشته اند سپس با استفاده از روش های فیشینگ به شبکه روزنامه تایمز نفوذ کرده اند.

در زیر به بررسی گام به گام وقوع این حمله می پردازیم:

مهاجمین پسورد تقریباً همه کارکنان کمپانی تایمز را بدست آورده و با استفاده از آنها توانستند از حدود 53 عدد از سیستم های رایانه ای شخصی آنها دسترسی حاصل کنند. سپس با استفاده از کدی که نوشته بودند به جستجو در اسناد و گزارشات خبرنگاران درباره سیاستمداران چینی پرداختند.

بیانیه ای که مجله تایمز درباره این حمله منتشر کرد حاوی دو نکته مهم بود:

اول اینکه حمله ای که توسط فیشینگ انجام شد به طور کامل توانست سیستم دفاعی را دور بزند:

" مهاجمین از فایروال ما عبور نکردند آنها از افراد ما عبور کردند "

دوم اینکه کمپانی تایمز گزارش داد از 45 بدافزاری که در این حمله استفاده شده بود فقط یکی از آنها توسط آنتی ویروس های کمپانی شناسایی شده بودند که در واکنش به این اتفاق فروشندگان این آنتی ویروس ها اعلام کردند که ما به مشتریان اعلام می کنیم که وجود یک آنتی ویروس به تنهایی کافی نیست و باید از مجموعه ای مکانیسم های دفاعی با هم استفاده کرد. {49}

1-6-2 - جاسوسی نظامی

در مه 2013، نسخه محرمانه گزارش نهیه شده از سوی هیئت علمی دفاع پنتاگون برای واشنگتن پست ارسال گردید {50}.

این گزارش ادعا کرد طرح های بسیاری از ساخت سلاح های پیشرفته ایالات متحده آمریکا توسط هکریهای چینی به سرقت رفته. در این گزارش آمده اسناد و مدارکی که به سرقت رفته مربوط به چندین سیستم موشکی، هواپیماهای جنگنده و کشتی ها بوده است. به نظر می رسد این حملات از طریق شرکت هایی بوده که در ساخت این تجهیزات دخالت داشته اند. این نمونه یکی از مواردی است که حملات با هدف طرح های صنعتی صورت می گیرند. اسناد به سرقت رفته حاصل 15 سال تحقیق و توسعه بودند.

1-6-3 - حملات زنجیره تامین

در ماه فوریه 2013 شرکت امنیتی Bit9 گزارشی از اینکه مورد حمله قرار گرفته است ارائه داد. {51} این شرکت لیستی از محصولات خود را منتشر کرد که استفاده از آنها مشکل امنیتی ندارد و اعلام کرد محصولاتی که در این لیست نیستند همگی خطرناک هستند. این شرکت اعلام کرد که مهاجمان امضاهای دیجیتالی را که از آن برای انتشار محصولات استفاده می کردند را به سرقت برده اند و در برخی موارد از آن برای انتشار بدافزار های خود استفاده کرده اند. بسیاری از مشتریان شرکت Bit9 با فرض اینکه نرم افزارهای با امضای دیجیتال این شرکت قابل اعتماد هستند اقدام به نصب نرم افزارهای آلوده با امضای سرقتی کرده اند.

1-6-4 - جاسوسی صنعتی

در اوایل سال 2013 شرکت lastline شروع به مانیتور و بررسی یکی از تولید کنندگان فعال در زمینه مد کرد. در طول این بررسی مشخص شد که یکی از سرورهای داخلی مورد حمله واقع شده است: تحقیقات بیشتر مشخص کرد که یک اتصال از راه دور از کشور چین به سیستم های آلوده برقرار شده است. اطلاعاتی که مورد حمله و سرقت واقع شده بودند حاوی طرح

ها و اسناد مجموعه جدید شرکت بودند که هنوز رسماً ارائه نشده بودند. جاسوسی صنعتی در مواردی که طیف وسیعی از بخش های اقتصادی یک کشور را هدف قرار می دهد با حمایت دولت از مهاجمین همراه است. {10}

1-6-5 - بدافزارهای مخرب منابع زیرساختی

در سال 2013، یکی از محصولات امنیتی شرکت Lastline که بر روی سیستم های یک شرکت خدماتی نصب شده بود حمله ای از نوع داندلود ناخواسته را شناسایی کرد. این حمله زمانی آغاز شد که یکی از کارمندان شرکت یک وبسایت کاملاً قانونی که توسط مهاجمین آلوده شده بود را مورد بازدید قرارداد. این وبسایت اطلاعاتی درباره حوزه فعالیت شرکت و کارمندان ارائه می کرد. پس از وقوع حمله سیستم های آلوده تلاش می کردند تا با یک دامنه خاص ارتباط برقرار کنند اما از طرف دامنه جوابی دریافت نمی کردند. روز بعد سیستم های آلوده موفق به برقراری اتصال با همان دامنه ها شدند و پس از برقراری اتصال بین بخش فرماندهی و کنترل و سیستم های آلوده یک فایل کانفیگ مربوط به بدافزار مالی فراگیر برای سیستم های آلوده ارسال شد. این حمله نشان داد که مهاجمین همواره در حال فعال نگه داشتن منابع خود هستند و در صورتی که یکی از منابع که در اینجا دامنه بود بدرستی کار نکند فوراً آن را ترمیم میکنند. پس باید همواره نظارت بر شبکه ها و سیستم های سازمان وجود داشته باشد زیرا ممکن است بدافزاری که تا دیروز ظاهراً فعالیتی نداشته و تحت کنترل بوده امروز فعال شده و به سیستم ها آسیب برساند.

1-6-6 - بدافزارهای پلی مورفیسم

پس از اینکه یکی از محصولات Lastline بر روی سیستم های یک دانشگاه نصب شد، فعالیت بدافزاری در محیط سیستم های دانشگاه مشاهده گردید. یکی از کاربران بخش اداری یک ایمیل حاوی لینک مخرب دریافت می کند و در مدت زمان کوتاهی دوبار بر روی آن کلیک می کند که همین کار باعث بارگذاری یک بدافزار بر روی سیستم او می شود. نکته جالب اینجا بود که فایل هایی که پس از هر بار کلیک کارمند بر روی لینک مخرب داندلود شده بود با هم متفاوت بودند. آنها نه تنها دارای هش های متفاوتی بودند بلکه در ویروس توتال دارای امتیازهای متفاوت بودند. این نمونه استفاده از پلی مورفیسم را به خوبی نشان می دهد که یکی از تکنیک های کارآمد در زمینه مخفی سازی است. دیگر نکته موجود در این حمله استفاده از انسان به عنوان روزه نفوذ که یکی از ضعیف ترین حلقه های زنجیر امنیت یک سازمان به شمار می آید.

از آماري که در بالا ارائه شد نکات زیادی مشخص می شود، یکی از نکاتی که مشخص شد این است که جلوگیری از نفوذ کار بسیار دشواری است و در سازمان های با ضریب امنیتی خیلی بالا هم ممکن است نفوذ رخ دهد. از دیگر نکاتی که مشخص

شد این است که این حملات محدود به بخش خاصی نیست و در هر زمینه ای ممکن است رخ دهد. در برخی موارد نیز ممکن است نفوذ از طریق خارج از سازمان یا محیط هدف شروع شود و سپس به داخل سازمان و محیط هدف گسترش پیدا کند. برای مثال در سازمان هایی که از سیاست BYOD¹ استفاده می کنند.

2 - شبکه های اجتماعی

امروزه شبکه های اجتماعی نقش مهمی در زندگی بسیاری از مردم ایفا می کند. مزایای این شبکه برای کسب و کارها و کاربران آن بر کسی پوشیده نیست. فیس بوک، بزرگترین شبکه اجتماعی، در حال حاضر بیش از 1.1 میلیارد کاربر دارد و رتبه سوم را در آمار سایت های پربازدید سایت alexa دارد.

امکان تبادل حجم زیادی از اطلاعات و هم چنین توانایی ذخیره اطلاعات با کمترین هزینه شبکه های اجتماعی را به بستری جذاب برای بدافزار نویسان تبدیل کرده است. کانال های ارتباطی فرماندهی و کنترل می توانند در بستر این شبکه های اجتماعی هم به صورت متمرکز و هم غیر متمرکز ایجاد شوند.

اگرچه معمولاً شبکه های اجتماعی تعداد کمی سرور مرکز متصل دارند اما با توجه به شمار زیاد استفاده کنندگان از این شبکه ها امکان مسدود کردن سرورهای آن ها نیست. از طرفی دیگر با توجه به سرمایه گذاری های عظیمی که ارائه دهندگان شبکه های اجتماعی کردند مسدود شدن آنها زیان های هنگفتی به این شرکت ها وارد می سازد. توانایی ذخیره سازی انواع مختلفی از اطلاعات توسط این شبکه ها این امکان را مهاجمین می دهد تا از روش های مختلفی همچون استکانوگرافی برای تبادل اطلاعات و مخفی سازی آن استفاده کنند. در حال حاضر نمونه های زیادی در زمینه نرم افزارهای مخرب وجود دارند که از شبکه های اجتماعی یا سایت های مشابه به عنوان بخشی یا تمام سیستم فرماندهی و کنترل استفاده می کنند. در بررسی ها، بات نت هایی مشاهده شده اند که برای ارسال و دریافت دستورات از پست های تویتر استفاده می کنند[52].

در نمونه ای که توسط شرکت آربور[53] کشف شد نیز استفاده از تویتر به عنوان بخشی از کانال های ارتباطی تویتر مشاهده شد. در این نمونه لینک های رمز شده بیس 64 که احتمالاً سرورهای ثانویه بخش فرماندهی و کنترل بودند از طریق تویتر مبادله می شد.

¹ Bring your own device

بدافزارهای دیگری نیز مشاهده شد که از شبکه های اجتماعی نظیر جایکو و تامبلر استفاده می کردند. هم چنین بات نت ي مشاهده شد که با استفاده از لینک هایی که یک برنامه کاربردی مخرب که بر روی گوگل اپ بارگذاری شده بود ایجاد می کرد اقدام به اتصال به بخش فرماندهی و کنترل می کرد. {54}

یکی دیگر از بدافزارهای هدفمند که از شبکه های اجتماعی به عنوان بخشی از فرماندهی و کنترل خود استفاده می کرد بدافزار تایدور است. تایدور به سازمان هایی که مربوط به کشور تایوان بود حمله می کرد. شرکت امنیتی فایرآی کشف کرد که بدافزار از پست های یاهو برای ارتباط استفاده می کرده است. {55} این بدافزار ابتدا از طریق ایمیل یک فایل ورد آلوده وارد سیستم قربانی میشده و سپس اقدام به دانلود فایل آلوده اصلی میکرده است. دانلود به این صورت بود که داندلور اولیه به یک پست وبلاگ یاهو که ظاهراً داده های تصادفی و ناخوانا دارد متصل می شده است. این داده های بی معنی رشته رمز شده باینری فایل آلوده اصلی بوده که پس از رمز گشایی و به فایل اصلی بدافزار تبدیل می شد. پس از استخراج فایل آلوده اصلی بدافزار به طور مستقیم به دو سرور فرماندهی و کنترل متصل می شد.

3- بدافزارهای مسری: ویروس ها و کرم ها

انواع بدافزارها، ویروس ها و کرم ها هستند که به خاطر نحوه شیوع شان شناخته می شوند. عبارت ویروس کامپیوتری به برنامه ایاطلاق می شود که نرم افزار قابل اجرایی را آلوده کرده باشد و هنگامی که اجرا می شود، سبب شود که ویروس به فایل های قابلاجرای دیگر نیز منتقل شود. ویروس ها ممکن است قابلیت حمل یک بار اضافی را نیز داشته باشند، که می تواند اعمال دیگر نیز انجام دهد. این اعمال اغلب خرابکارانه هستند. از سوي دیگر یک کرم برنامه ای است که به طور فعالانه خود را روی یک شبکه منتقل می کند تا رایانه های دیگر را نیز آلوده سازد. کرم ها نیز قابلیت حمل یک بار اضافی را دارند. تعریف های بالا نشان می دهد که تفاوت ویروس و کرم در این است که یک ویروس برای شیوع نیاز به دخالت کاربر دارد، در حالی که یک کرم خود را به طور خودکار و از طریق شبکه گسترش پیدا می کند. در نتیجه آلودگی هایی که از طریق ایمیل یا فایل های مایکروسافت ورد منتقل می شوند، ویروس شناخته می شوند، زیرا باید دریافت کننده فایل یا ایمیل آن را باز کند تا سیستم آلوده شود. برخی نویسندگان در رسانه های محبوب نیز متوجه این تمایز نیستند و از این عبارت ها به اشتباه در جای یکدیگر استفاده می کنند.

3-1 مخفی کارها: اسبهای تروآ، روتکیتها و بک دورها



یک برنامه خرابکار برای اینکه بتواند به اهدافش برسد باید قادر باشد که اجرا شود بدون آنکه توسط کاربر یا مدیر سیستم رایانه خاموش یا پاکسازی شود. مخفی کاری همچنین این امکان را می دهد که بدافزار در اولین مکان نصب شود. وقتی یک برنامه خرابکار خود را به شکل چیز بی ضرر یا مطلوب در می آورد، کاربران ممکن است تشویق شوند تا آن را بدون آنکه بدانند چه می کند، نصب کنند. این، ترفند اسب تروآ است.

به بیان دیگر، یک اسب تروآ برنامه ای است که کاربر را ترغیب می کند تا اجرایش کند در حالی که قابلیت خرابکاریش را مخفی می کند. آثار منفی ممکن است بلافاصله آغاز شوند و حتی می توانند منجر به آثار نامطلوب فراوانی گردند. از جمله حذف کردن فایل های کاربر یا نصب نرم افزارهای خرابکار یا نامطلوب بیشتر. اسب های تروآ برای آغازسازی شیوع یک کرم استفاده می شوند.

یکی از مرسوم ترین راه هایی که جاسوس افزارها توزیع می شوند، از طریق یک اسب تروآ که به عنوان یک قطعه از یک نرم افزار مطلوب که کاربر آن را از اینترنت دانلود می کند، است. وقتی که کاربر نرم افزار را نصب می کند جاسوس افزار نیز در کنارش نصب می شود. برای مثال اسب تراوا در غالب یک نرم افزار دانلودنصب می شود و به صورت مستقل از نرم افزار اصلی یا مرتبط با آن شروع به دانلود برنامه و مدیاها گاهی با مضامین مستهجن می کند. مثال اخیر تروجان فوق سری نرم افزارهایی با پسوند finder می باشد.

نویسندگان جاسوس افزار سعی می کنند به صورت قانونی عمل کنند، ممکن است رفتار جاسوس افزار را در عباراتی مبهم در توافق نامه با کاربر بیاورند و البته کاربران بعید است که این توافق نامه را بخوانند یا بفهمند. تروآها به صورت عمده به منظور کارهای تجاری استفاده می شوند.

2-3 - رد گم کن (Rootkits)

رد گم کن واژه مصوب فرهنگستان زبان و ادب فارسی برای (Rootkits) است. هنگامی که یک برنامه خرابکار روی یک سیستم نصب می شود بسیار مهم است که مخفی باقی بماند تا از تشخیص و نابودی در امان باشد. همین وضعیت درباره یک مهاجم انسانی که بطور مستقیم وارد یک رایانه می شود برقرار است. ترفندهایی که به عنوان روتکیتها شناخته می شوند اجازه این مخفی کاری را می دهند. آنها این کار را با اصلاح سیستم عامل میزبان انجام می دهند به نحوی که بدافزار از دید کاربر مخفی بماند. روتکیتها می توانند از این که یک پروسه خرابکارانه در لیست پروسه های سیستم دیده شود ممانعت کنند، یا مانع خوانده شدن فایل های آن شوند. در ابتدا یک روتکیت مجموعه ای از ابزارها بود که توسط یک مهاجم انسانی بر روی یک سیستم یونیکس نصب می شد که به مهاجم اجازه می داد تا دسترسی مدیریتی داشته باشد. امروزه این عبارت بطور عمومی تر برای فرایندهای مخفی سازی در یک برنامه خرابکار استفاده می شود.

3-3 - بکدورها

یک بک در روشی است برای خنثی سازی رویه های معمول تایید اعتبار. وقتی یک سیستم دارای چنین رویه هایی باشد یک یا چند بکدور ممکن است نصب شوند تا دسترسی های آتی را آسان تر سازد. بکدورها ممکن است حتی پیش از یک نرم افزار خرابکار نصب شوند تا به مهاجمان اجازه ورود دهند.

4-3 - ویروس

ویروس virus به برنامه هایی گفته می شود که خود را تکثیر (Replicate) می کنند؛ بدین صورت که خود را به دیگر فایلها و برنامه های اجرایی سرایت می دهند. ویروس ها عموماً در کنار تکثیر و تولید مثل، یک سری اعمال خرابکارانه دیگر نیز از خود نشان می دهند. ویروس ها برای آلوده کردن کامپیوترها، نیاز به اجرا شدن توسط کاربر یا یک برنامه را دارند.

5-3 - کرم

worm کرم ها برنامه هایی هستند که از طریق آسیب پذیری های شبکه ای کامپیوتر، به آن نفوذ می کنند. غالباً کرم ها پس از نفوذ از طریق شبکه، اعمال مخرب یا مضر یا سودجویانه ای را روی سیستم انجام می دهند؛ مثلاً سیستم را به ویروس آلوده میکنند. رفتار عمومی کرم ها به صورت زیر است:

در شبکه، کامپیوترها را جستجو می کنند و سیستم های آسیب پذیر را پیدا می کنند به کامپیوتر آسیب پذیر حمله و نفوذ کرده و برنامه ای روی آن به اجرا در می آورند از کامپیوتر جدید برای حمله به دیگر سیستم ها استفاده می کنند

معرفی بدافزار RDN/SPYBOT.BFR

بدافزاری با درجه خطر کم (Low) و از نوع “کرم” (Worm) که به طور خودکار خودش را منتشر می کند



نامگذاری ها این بدافزار با نام های زیر توسط ضدویروس های

مختلف شناسایی می شود:

McAfee: RDN/Spybot.bfr

.ArchSMS32Ahnlab: Trojan/Win

:Dropper-gen32Avast: Win .BGMS (Trojan

horse)35AVG (GriSoft): Generic 74510.2Avira:

TR/Zusy.

.Inject.hfmu32Kaspersky: Trojan.Win

74510BitDefender: Gen:Variant.Zusy.

.Packer.UpxProtector32Clamav: PUA.Win

47Dr.Web: Trojan.InstallMonster.

/Inject.BB!tr32FortiNet: W

/InstallMonstr.BB application32Eset: Win

/Inject.BJMY32:win32Norman: win

Panda: Trj/Genetic.gen

043Sophos: Mal/Behav-

نحوه انتشار این بدافزار، مانند سایر کرم ها از روشهای متعددی برای انتشار استفاده می کند. از جمله، از طریق دیسک

های USB قابل حمل ،

CD های قابل نوشتن (Writable) و همچنین در محیط شبکه های محلی (LAN) بر روی شاخه های اشتراکی کپی می شود

تا سایر کاربران را آلوده کند.

عملکرد

به محض آلوده شدن یک دستگاه به این بدافزار، دستورات زیر به Registry سیستم اضافه می شود.

-HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ESENT\PROCESS

\C67050FFE603F9688CD804306D9B5F616FED\4448

-HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ESENT\PROCESS

\C67050FFE603F9688CD804306D9B5F616FED4448\DEBUG\

بدافزار RDN/Spybot.bfr پس از مقیم شدن در حافظه تلاش می کند کد مخربی را در هر پروسه ای که پیش آن در حافظه بار گذاری شده است، تزریق نموده و از این طریق باعث اجرای کد مورد نظر می شود. به بیان دیگر، این بدافزار تلاش می کند خود را در بخشی از حافظه سیستم آلوده قرار دهد که مربوط به یکی از پروسه های سیستمی و یا پروسه محافظت شده دیگری مانند پروسه Winlogon و یا Explorer است. بدین ترتیب بدافزار می تواند خود را از چشم کاربر یا سایر نرم افزارهای دیگر پنهان کند.

در نسخه های قبلی این بدافزار، پسوند بعضی فایلها تغییر داده می شد و هنگامی که کاربر فایل را اجرا می نمود، تصویر زیر به نمایش در می آمد. این تصویر مانند پیغام هشدار به کاربر می گوید که فایل مورد نظر رمزنگاری شده است و برای رمزگشایی آن باید فایلی با نام DirtyDecrypt.exe اجرا شود و یا کلید های CTRL+ALT+D زده شود.



کلیدهای زیر در Registry سیستم آلوده توسط بدافزار تغییر کرده و دستکاری می شوند.

-HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ESENT\PROCESS

\C67050FFE603F9688CD804306D9B5F616FED4448\DEBUG\TRACE LEVEL

-HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\Eventlog

\APPLICATION\ESent\CategoryCount = 16

-HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\Eventlog

\APPLICATION\ESent\CategoryMessageFile =

% Windir%\System32\ESent.dll

-HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\Eventlog

\APPLICATION\ESent\EventMessageFile = % Windir%\System32\ESent.dll

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\Eventlog\APPLICATION\ESent\TypesSupported = 7

بدافزار RDN/Spybot.bfr می تواند با استفاده از پودمان HTTP اطلاعاتی را از سیستم کاربر ارسال و یا دستوراتی را از یک سرویس دهنده راه دور دریافت نماید.

همچنین بدافزار سعی می کند با نشانی های زیر ارتباط برقرار نماید.

80:*5,149,254,

پیشگیری <http://webllavepri.gurcanozturk.com/api>

به روز نگه داشتن ضدویروس، نصب آخرین اصلاحیه های سیستم عامل و مرورگر و همچنین استفاده از تنظیمات توصیه شده توسط کارشناسان شرکت مهندسی شبکه گستر، در کنار آگاه کردن کاربران شبکه از خطرات کلیک بر روی لینک های ناآشنا، همگی با هم می توانند خطر آلوده شدن به این بدافزار و یا گونه های مشابه را به حداقل برسانند.

6-3 - اسب تروا

Trojan اسب تروا به برنامه هایی گفته می شود که مفید به نظر رسیده و کاربر را برای اجرا اغفال می کنند، در حالی که علاوه بر عمل مورد انتظار کاربر، یک عمل بدخواهانه دیگری را نیز به صورت مخفی انجام می دهند. برای مثال، کاربر یک برنامه بازی مجانی را از اینترنت گرفته و نصب می کند و در کنار اجرای بازی، سیستمش آلوده به ویروس نیز می شود. سب های تروجان برنامه هایی اند که در ظاهر به نظر می رسد در حال انجام کار بی ضرری هستند. اما در خفا دارای کدهای مخربی هستند که کار دیگری انجام می دهند. در بسیاری از موارد، تروجان ها یک در پشتی روی رایانه طعمه قرار می دهند که اجازه کنترل از راه دور کامپیوتر آلوده را به سازنده شان می دهند. یک کامپیوتر آلوده معمولاً به صورت مستقیم یا به عنوان عضوی از شبکه رایانه های الوده به تروجان و یا دیگر برنامه های مخرب (botnet) مورد سوء استفاده قرار می گیرد. تفاوت عمده بین ویروس و تروجان این است که تروجان خود را تکثیر نمی کند. همچنین تروجان توسط کاربر به شکل ناآگاه نصب می شود.

هنگامی که کامپیوتر شما به تروجان آلوده شد، طراح تروجان می تواند از آن برای هر هدف بدی استفاده کند. مانند حملات Dos (denial of service) ، به یک وب سایت ، استفاده از پراکسی سرور برای مخفی کردن حملات، و یا حتی بدتر ، برای ارسال ده ها اسپم (هرزنامه). حفاظت در مقابل حملات تروجان ها، همانند روش حفاظت در مقابل ویروس هاست ، ابتدا مطمئن شوید که برنامه آنتی ویروس شما به روز شده است. هیچ گاه فایل ضمیمه مشکوک را باز نکنید ، و همیشه قبل از اینکه فایل کرک برای برنامه ای مثل فتوشاپ را دانلود و نصب کنید ، به عواقب احتمالی اش خوب فکر کنید. چون اصولاً فایل های کرک مکانی ایده آل و مکان مورد علاقه تروجان نویسان برای مخفی کردن تروجان است .

7-3- نرم افزار جاسوسی

جاسوس افزار (Spyware) در تعریف، عبارت است از هر نرم افزار نصب شده بر روی کامپیوتر، که اطلاعات را بدون اطلاع شما جمع آوری کرده، و آنها را به سازنده خود بفرستد. سازنده برنامه با استفاده از اطلاعات شخصی شما، برای مقاصد سوء خود استفاده می کند. ممکن است این جاسوسی به شکل keylogging (جاسوسی صفحه کلید) برای کشف و استفاده از رمز عبور، تماشای نتایج جستجو، تغییر صفحه خانگی و موتور جستجوی مرورگر شما، اضافه کردن نوار ابزار مضر یا ناخواسته به مرورگر ، یا فقط سرقت شماره کارت اعتباری شما باشد.

از آنجا که نرم افزارهاي جاسوسی عمدتاً به منظور کسب درآمد از جیب شما طراحی شده اند، معمولاً نیازی به خرابکاری در کامپیوتر شما ندارند. در حقیقت بسیاری از کاربران بدون اینکه حتی از وجود آن اطلاع داشته باشند، روی رایانه خود نرم افزارهاي جاسوسی در حال اجرا دارند. اما به طور کلی آنهایی که دارای یک جاسوس افزار نصب شده روی رایانه خود هستند، احتمالاً تعداد دیگری هم بدافزار دارند. هنگامی که روی رایانه شما تعداد زیادی نرم افزار جاسوسی در حال اجرا باشند، خواه ناخواه سرعت رایانه هم پایین می آید. چیزی که بسیاری از مردم در مورد نرم افزارهاي جاسوسی درک نمی کنند، این است که هر نرم افزار آنتی ویروسی قابلیت شناسایی نرم افزارهاي جاسوسی را ندارد. شما باید از فروشنده بپرسید تا مطمئن شوید نرم افزاری که شما برای حفاظت از خود در برابر بدافزارها استفاده می کنید، در واقع نرم افزارهاي جاسوسی را هم شناسایی می کند یا خیر. اگر شما به رایانه ای برخورد کردید که در حال حاضر به شدت آلوده شده ، ترکیبی از برنامه های MalwareBytes و SuperAntiSpyware می تواند آن را کاملاً تمیز کند.

این دسته از بدافزارها اقدام به دزدیدن اطلاعات از سیستم های کامپیوتری می کنند. نرم افزارهاي جاسوسی می توانند توسط دیگر بد افزارها مانند اسب های تروا یا کرم، نصب شوند و یا اینکه فرد سودجویی مستقیماً اقدام به نصب آن ها بکند. یکی دیگر از راه های انتشار نرم افزارهاي جاسوسی، روش های تحریکات جمعی یا همان مهندسی اجتماعی (Social Engineering) مانند استفاده از ایمیل، برای ترغیب کاربر به نصب یک برنامه مجانی و به ظاهر مفید است. دسته ای از نرم افزارهاي جاسوسی به نام Keyloggerها وجود دارند که پس از اجرا، هر چیزی را که کاربر کامپیوتر تایپ می کند، در جایی ذخیره کرده و حتی می توانند از کارهای وی فیلم تهیه کنند و سپس این اطلاعات را در شبکه یا اینترنت برای فرد دیگری ارسال نمایند.

3-8- تبلیغات ناخواسته

adware تبلیغات ناخواسته، برنامه هایی هستند که بدون خواست کاربر به آن نمایش داده می شوند. صفحات pop-up نمونه ای از این نوع بد افزار است. میزان مخرب یا خطرناک بودن این بدافزارها می تواند متغیر باشد. برای مثال اگر این برنامه بر روی سیستم عامل نصب باشد، به صورت بالقوه می تواند هر نوع جمع آوری اطلاعات کاربر یا دستکاری در دیگر نرم افزارها را انجام دهد. اما برنامه های تبلیغاتی که روی مرورگر ست میشوند، سطح آسیب کمتری خواهند داشت. البته عموماً اطلاعاتی که توسط این نوع از بدافزارها جمع آوری می شود، اطلاعات کم حساس، مانند علاقه مندی های فرد به سایت های فروش کالا و . . . است.

4- نحوه تکثیر به چه صورت است ؟

ویروس های اولیه، کدهائی محدود بوده که به یک برنامه متداول نظیر یک بازی کامپیوتری و یا یک واژه پرداز ، الحاق می گردیدند. کاربری، یک بازی کامپیوتری آلوده را از یک BBS اخذ و آن را اجراء می نماید. ویروس، بخش کوچکی از نرم افزار بوده که به یک برنامه بزرگ متصل می گردد. ویروس های فوق بگونه ای طراحی شده بودند که در زمان اجرای برنامه اصلی، بعلت فراهم شدن شرایط مساعد، اجرا می گردیدند. ویروس خود را بدرون حافظه منتقل و در ادامه بدنبال یافتن سایر برنامه های اجرائی موجود بر روی دیسک، بود. در صورتیکه این نوع برنامه ها، پیدا می گردیدند ، کدهای مربوط به ویروس به برنامه اضافه می شدند. در ادامه ویروس، برنامه واقعی را فعال می کرد. کاربران از فعال شدن و اجرای ویروس آگاه نشده و در این راستا روش های خاصی نیز وجود نداشت. متاسفانه ویروس، نسخه ای از خود را تکثیر و بدین ترتیب دو برنامه آلوده می گردیدند. در آینده با توجه به فراهم شدن شرایط لازم ، هر یک از برنامه های فوق سایر برنامه ها را آلوده کرده و این روند تکراری ادامه می یابد.

در صورتیکه یکی از برنامه های آلوده از طریق دیسکت به شخص دیگری داده شود و یا فایل آلوده برای یک BBS ارسال تا بر روی سرویس دهنده قرار گیرد، امکان آلوده شدن سایر برنامه ها نیز فراهم خواهد شد. فرآیند فوق نحوه تکثیر یک ویروس کامپیوتری را نشان می دهد.

تکثیر و گسترش از مهمترین ویژگی های یک ویروس کامپیوتری بوده و در صورت عدم امکان فوق ، عملاً "موانع جدی در تکثیر ویروس های کامپیوتری بوجود آمده و برخورد با این نوع برنامه با توجه به ماهیت محدود میدان عملیاتی ، کار پیچیده ای نخواهد بود. یکی دیگر از ویژگی های مهم ویروس های کامپیوتری، قابلیت حملات مخرب آنان بمنظور آسیب رساندن به اطلاعات است . مرحله انجام حملات مخرب عموماً" توسط نوع خاصی چاشنی (نظیر ماشه اسلحه) صورت می پذیرد. نوع حملات متنوع بوده و از نمایش یک پیام ساده تا پاک نمودن تمام اطلاعات موجود را می تواند شامل گردد. ماشه فعال شدن ویروس می تواند بر اساس یک تاریخ خاص و یا تعداد نسخه های تکثیر شده از یک ویروس باشد . مثلاً" یک ویروس می تواند در تاریخ خاصی فعال و یا پس از ایجاد یکصد نسخه از خود ، فعال و حملات مخرب را آغاز نماید.

ایجاد کنندگان ویروس های کامپیوتری افرادی آگاه و با تجربه بوده و همواره از آخرین حقه های موجود استفاده می نمایند. یکی از حقه های مهم در این خصوص ، قابلیت استقرار در حافظه و استمرار وضعیت اجرای خود در حاشیه می باشد (مادامیکه سیستم روشن است). بدین ترتیب امکان تکثیر این نوع ویروس ها با شرایط مطلوبتری فراهم می گردد. یکی دیگر از حقه های موجود ، قابلیت آلوده کردن "بوت سکتور" فلش دیسک های هارد دیسک ها، می باشد. بوت سکتور شامل یک

برنامه کوچک بمنظور استقرار بخش اولیه یک سیستم عامل در حافظه است. با استقرار ویروس های کامپیوتری در بوت سکتور، اجراء شدن آنها تضمینخواهد شد. (شرایط مناسب برای اجرای آنها بوجود می آید). بدین ترتیب یک ویروس بلافاصله در حافظه مستقر و تا زمانی که سیستم روشن باشد به حضور مخرب خود در حافظه ادامه خواهند داد. ویروس های بوت سکتور قادر به آلوده نمودن سایر بوت سکتورهای فلاپی دیسک های سالمی که در درایو ماشین قرار خواهند گرفت ، نیز می باشد. در مکان هایی که کامپیوتر بصورت مشترك بین افراد استفاده می گردد(نظیر دانشگاه ها) ، بهترین شرایط برای تکثیر ویروس های کامپیوتری بوجود خواهد آمد (نظیر یک آتش سوزی بزرگ بوده که سرعت همه چیز را نابود خواهد کرد).

5 - برنامه های ضد بدافزار

با افزایش حملات بدافزارها توجه ها از محافظت در برابر ویروس ها و جاسوس افزارها به سمت محافظت از بدافزارها جلب شده است.

در نتیجه برنامه های مخصوصی برای مبارزه با آن ها توسعه یافته است. برنامه های ضد بدافزار از دو طریق با بدافزار نبرد می کند:

1 - آن ها محافظت بی درنگ را در برابر نصب بدافزار روی یک رایانه می توانند تامین کنند، در این نوع از محافظت نرم افزار ضد بدافزار تمام اطلاعات ورودی از شبکه را اسکن می کند تا از ورود بدافزارها و تهدیدهایی که با آنها می آیند جلوگیری به عمل آورد.

محافظت بی درنگ از بدافزار مشابه محافظت بی درنگ از ویروس عمل می کند. یعنی نرم افزار فایل ها را در زمان داندلود آن اسکن نموده و از فعالیت هر چیزی که بد افزار شناخته شود ممانعت به عمل می آورد.

2- برنامه های ضد بدافزار می توانند تنها به منظور تشخیص و پاکسازی بدافزارهایی که قبلاً روی یک رایانه نصب شده اند، مورد استفاده قرار گیرند. این نوع از محافظت در برابر بدافزار عمدتاً ساده تر و محبوب تر است. این نوع از ضد بدافزارها محتوای رجیستری ویندوز، فایل های اجرایی سیستم و برنامه های نصب شده روی یک رایانه را اسکن می کنند و لیستی از تهدیدهای پیدا شده را تهیه می کنند، که به کاربر اجازه می دهد که چه فایل هایی را حذف یا نگاه دارد.

6- آنالیز بدافزار

آنالیز بدافزار یکی از جذابترین مباحث دنیا امنیت است که امروزه در میان متخصصین ایرانی نیز محبوب گشته. اما شاید فکر کنید که آنالیز یک بدافزار کاری بسیار سخت و نیاز به دانش بسیار بالا دارد به خصوص در برنامه نویسی و مهندسی معکوس! به صورت کلی آنالیز بدافزار به دو بخش اصلی آنالیز ایستا (Static) و آنالیز پویا (Dynamic) تقسیم می شود. در بخش آنالیز ایستا شما نیاز به دانش زیادی در برنامه نویسی و مهندسی معکوس دارید و همچنین آشنایی کامل با ابزارهایی مانند IDA pro و یا OllyDbg نیز یک اصل اساسی است.

اما برای رفتارشناسی یک فایل مشکوک می توانید از آنالیز پویا که نیاز به دانش خیلی زیادی در برنامه نویسی ندارد استفاده کنید.

در آنالیز پویا ما به از یک سری ابزارها برای ردگیری رفتارهای یک مورد مشکوک استفاده می کنیم.

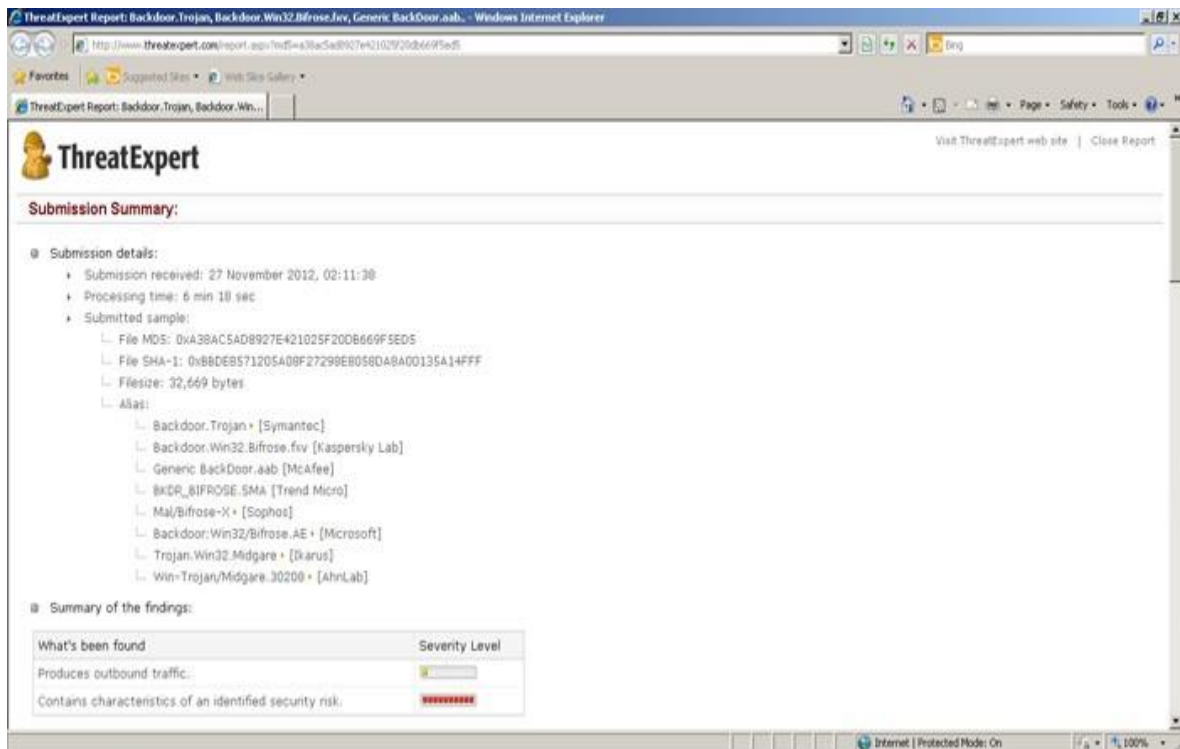
یکی از این ابزارها SandBox است. اما SandBox چیست؟ SandBox یک فناوری و ابزار است که هم توسط متخصصین آنالیز بدافزار و هم توسط آنتی ویروس ها مورد استفاده می گیرد. به طور کلی SandBox یک محیط مجازی و امن است که می توان مورد مشکوک را در آن اجرا و رفتار برنامه را مورد بررسی قرار داد بدون آنکه به سیستم اصلی آسیبی برسد. شما نیز می توانید یک SandBox برای تحقیق خود بر روی سیستم خود فراهم کنید. ابزارهای SandBox آماده رایگان بسیاری بر روی اینترنت هست که می توانید بهره ببرید

مثال از سندباکس www.threatexpert.com/submit استفاده می کنم.

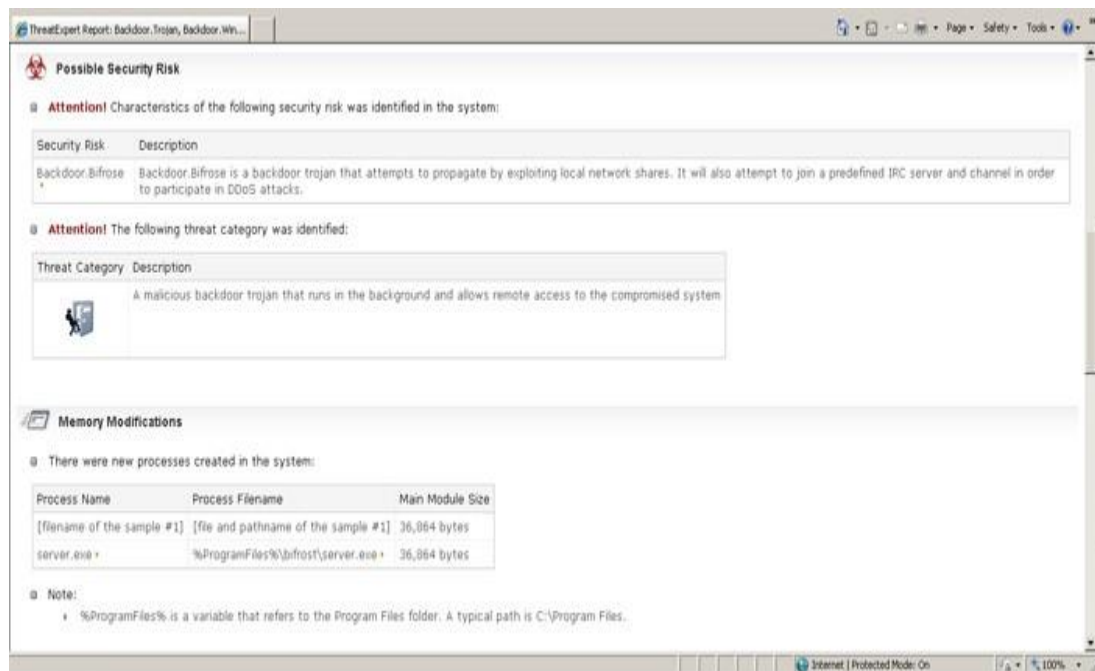
وقتی که یک فایل مشکوک را وارد می کنید پایگاه داده threatexpert بررسی می کند که آیا مورد مشکوک قبلاً بررسی شده است یا خیر، اگر جواب مثبت باشد شما می توانید گزارش کامل آن را مطالعه کنید.

در غیر این صورت برنامه مشکوک بر محیط مجازی بررسی می شود و مواردی مانند پروسه های ایجاد شده، تغییرات حافظه، تغییرات کلید های رجیستری، محلهایی که برنامه خود را کپی کرده است و کلی از موارد دیگر بررسی گشته و گزارش کاملی را برای شما نمایش می دهد.

حال یک مورد را به صورت کلی بررسی می کنیم.



در اینجا یک گزارش مختصر در مورد نمونه مورد بررسی ارائه می شود.



می

توانید تغییرات حافظه و تغییرات رجیستری را مشاهده کنید

شناسایی بدافزار ایرانی با نام "مارمولک"

این بدافزار در هنگام اجرا یک کپی از خود با نام Mcsng.sys در فولدر Sysytem32 ایجاد می کند. این بدافزار همچنین پروسه ای را اجرا می کند که فایل stmp.sys را در فولدر system32\config جایگذاری کرده و می نویسد.

این بدافزار از طریق ثبت ضربات صفحه کلید، رمز کردن آنها و ارسال آن برای نویسنده، اطلاعات را جمع آوری و سرقت می کند.

حملات هدفمند از چندین مرحله تشکیل می شوند که به زنجیره قتل APT شناخته می شوند. مهاجمان به عنوان بخشی از فاز مسلح کردن خود، اغلب Payload ی را در یک فایل قرار می دهند که زمانی که نصب می شود در فاز دستور و کنترل (C2) به مهاجم متصل می شود.

یک payload بسیار معمولی مورد استفاده بسیاری از بدافزارهای سرقت کلمه عبور، نرم افزار ثبت ضربات صفحه کلید (keylogger) است و هدف از ثبت ضربات صفحه کلید این است که ضربات صفحه کلید کاربر ضبط شود و اطلاعات اعتباری وی و لینک ها به منابع داخلی و خارجی جمع آوری شود.

از این رو مرکز ماهر ایران اعلام کرد: اخیرا بدافزار موسوم به مارمولک که یک نرم افزار ایرانی ثبت ضربات صفحه کلید است با

MD5 برابر با F09D2C65F0B6AD55593405A5FD3A7D91 شناسایی شده است.

نخستین ظهور این keylogger به یک فروم در خاورمیانه باز می گردد. اگرچه ممکن است برخی keylogger ها ضربات صفحه کلید را برای مقاصد قانونی ثبت کنند اما این نرم افزار قربانیان خود را با یک payload پنهان همراه می سازد. به نظر می رسد که تولید کننده این بدافزار با قرار دادن آن در فروم مذکور، قصد حمله به سایر اعضای این فروم را داشته که این کار تکنیکی مرسوم است.

نویسندگان بدافزارها اغلب برای جلوگیری از شناسایی شدن، از ابزارهای ارزان و ساده ای استفاده می کنند که بدافزار را با یک برنامه runtime فشرده سازی یا رمزگذاری، تغییر می دهد؛ البته در این مورد خاص، فایل های مرتبط توسط یک نسخه تغییر یافته از ابزار مشهور UPX پنهان شده اند.

این فایل در هنگام اجرا یک کپی از خود با نام Mcsng.sys در فولدر Sysytem32 ایجاد می کند. این بدافزار همچنین پروسه ای را اجرا می کند که فایل stmp.sys را در فولدر system32\config جایگذاری کرده و می نویسد.

اگرچه پسوند این فایل sys. (فایل سیستمی) است، اما در حقیقت این فایل سیستمی نیست. هدف این فایل این است که به عنوان یک فایل لاگ عمل کند که محتوی ضربات صفحه کلید کاربر است که به صورت رمز شده ذخیره شده اند. هر بار که یک کلید فشرده می شود، این پروسه ضربات صفحه کلید را ثبت میکند، آن را رمز کرده و به stmp.sys اضافه می کند. اگرچه الگوریتم رمزگذاری مورد استفاده برای این کار ساده است، ولی از رمزگذاری انتخابی با دو تکنیک استفاده می کند: هر بایت در صورتی که فرد باشد با استفاده از تکنیک 1 رمز می شود و در صورتی که زوج باشد، با استفاده از تکنیک 2 رمزگذاری خواهد شد؛ براین اساس پس از رمزگشایی نه تنها ضربات صفحه کلید قابل مشاهده هستند، بلکه اطلاعات زمانی ثبت این اطلاعات نیز قابل مشاهده است.

پس از ثبت و رمز گذاری ضربات صفحه کلید، این بدافزار این اطلاعات را برای نویسنده خود ایمیل می کند.

این بدافزار همچنین نام کامپیوتر و نام کاربر را نیز برای سازنده خود می فرستد.

لاگ رمز شده به آدرس marmoolak@red-move.tk ارسال می شود که بر روی دامنه ای میزبانی می شود که به میزبانی بدافزارها مشهور است.

مک آفی این تروجان keylogger و نسخه های مختلف آن را با عنوان Keylog-FAG می شناسد.

بد افزار Mahdi

این بدافزار هدفمند تعدادی از کشورهای خاورمیانه نظیر ایران، اسرائیل و افغانستان را مورد تهدید جدی قرار داده است. بر طبق این گزارش ها، این بدافزار به صورت یک سند ساختگی نرم افزار Word و یا اسلایدهای نرم افزار Power Point می باشد که به محض باز شدن، انتقال دهنده بدافزار را فعال می نماید.

بدافزار پس از فعال شدن، تصویری را در رابطه با نقشه کشور اسرائیل بر علیه برنامه هسته ای ایران با طراحی نقشه جنگ الکترونیکی که از طریق یکی از سایتهای خبری منتشر شده است نمایش می دهد.

آن طور که از نقطه نظر تحلیلگران آمده است، بدافزار فوق با استفاده از تکنیکی موسوم به مهندسی اجتماعی کاربر / قربانی را ملزم به اجرای سند آلوده می نماید. این در حالی است که سند آلوده با نمایش تعدادی عکس و بازی های ریاضی گونه ذهن کاربر را به دستورالعمل های ذکر شده در روی تصاویر معطوف و منحرف می نماید.

همچنین نکته قابل توجه در مورد برخی از نمونههای تحلیل شده حاکی از وجود سندهایی در خصوص نمایش عکسی معماگونه از حضرت علی (ع) بوده که بارها در سایت های پارسی زبان نمایش داده شده اند.

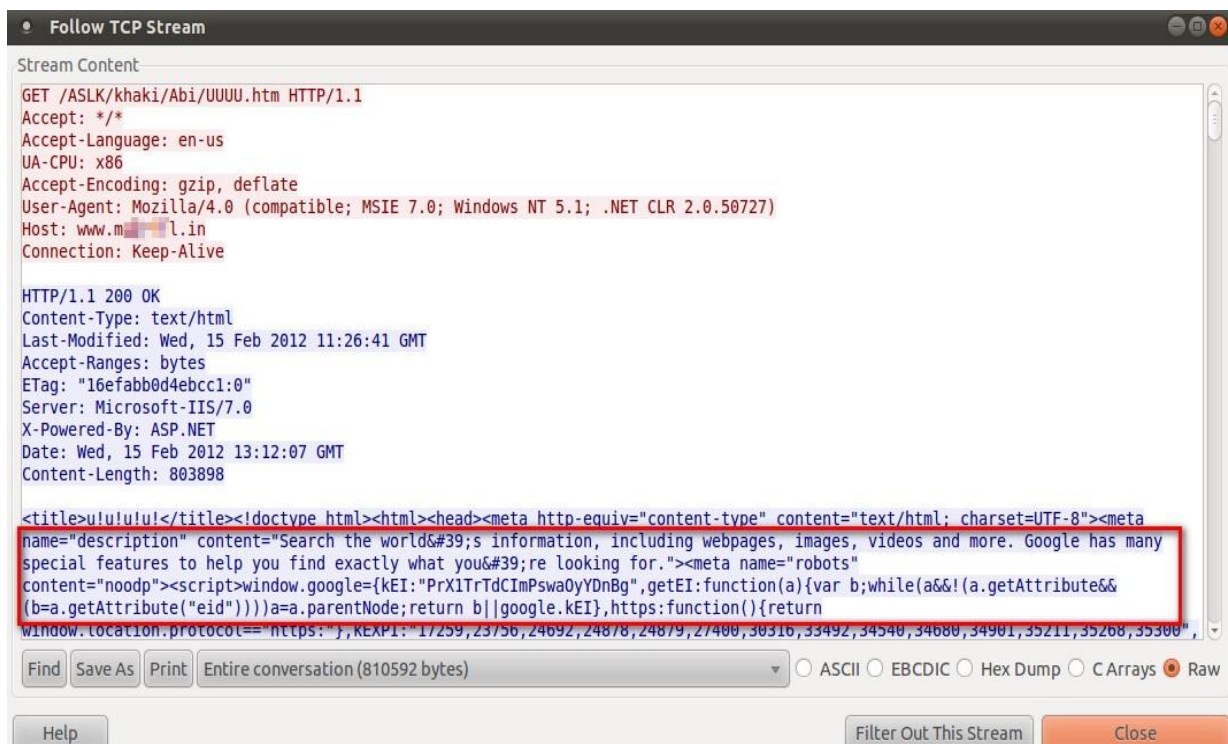


این بدافزار در جهت فریفتن کاربر از تکنیکی موسوم به RTLO به منظور تغییر نام هوشمندانه فایل های اجرایی به فایل های بایسوند pdf، jpg و یا scr و ppt استفاده مینماید. پس از اجرا نمودن این فایل، تعدادی ویدئو و عکس در جهت فریفتن و پنهان نمودن فعالیت اصلی بدافزار اجرا می شود.

بررسی های صورت گرفته از سرورهای C&C بیانگر شواهدی در خصوص منشاء حمله از کشور ایران می باشد.

```
IP and Time information:IPsik: 11.53 Timesik: 02/15/2012 - 8:09:09 PM TH: 90-11-26 چهارشنبه  
Coputername:N.M  
Username:h
```

همچنین این بدافزار در جهت مخفی نمودن ارتباطات و بروزرسانی ماژول های خود از یک صفحه غیرساختگی گوگل استفاده می نماید که به مخفی نمودن ارتباط کمک شایانی می نماید.



شواهد حاکی از وجود نمونه های قبلی این بدافزار از ماه دسامبر سال 2011 می باشد.

مشخصات فنی بدافزار

یکی از مهمترین مشخصه های بدافزار فوق این است که برای جلوگیری از کشف توسط سیستم های آنتی ویروس، با استفاده از نسخه ای جدید و یا تغییر یافته از پکر معروف UPX رمز شده است.

همچنین شواهد حاکی از آن است که بدافزار پس از فعال شدن و توسط قسمت Dropper خود، تعداد زیادی از فایل ها را در مسیر زیر قرار می دهد.

c:\documents and

settings\\Printhood فایل های نظیر UpdateOffice.exe و OfficeDesktop.exe نیز جز فایل های آلوده می باشند.

همچنین فایل با نام iexplorer.exe نیز به عنوان به سرقت برنده اطلاعات عمل می نماید.

مجموعه عملیاتی که این تروجان به منظور سرقت اطلاعات انجام می دهد به شرح زیر است:

- کیلاگ نمودن، به معنای به سرقت بردن کلیه کلمات تایپ شده بر روی کیبورد
- تهیه تصویر از صفحه کاربر قربانی
- بروزرسانی بکدور مربوط به تروجان

- ضبط نمودن صدا با پسوند wav. همراه با عملیات ذخیره سازی و آپلود
- نقشه برداری از ساختار پارتیشن و دیسک سخت کلیه ماشین های آلوده از طریق پروتکل http و با وب سرورهای با شماره آی پی نظیر 57.142.174 * (سه سرور) و 106.205.67 * (یک سرور) ارتباط برقرار می نمایند. همچنین پکتهای از نوع ICMP به سمت سرورهای فوق الذکر برای چک کردن وضعیت ارسال می شوند. همچنین بیش از 300 فایل با پسوندهای PRI، dll و TMP در مسیر زیر ایجاد می شوند:

C:\documents and settings\%USER%\Printhood
 MD5 از نمونه های مرتبط با این بدافزار شامل لیست زیر می باشد:

7b7abab9bc4c49743d001cf99737e383
 a9774d6496e1b09ccb1aeaba3353db7b
 885fceb0549bf0c59a697a7cfff39ad
 4be969b977f9793b040c57276a618322
 ea90ed663c402d34962e7e455b57443d
 aa6f0456a4c2303f15484bff1f1109a0
 caf851d9f56e5ee7105350c96fcc04b5
 1fe27986d9d06c10e96cee1effc54c68
 07740e170fc9cac3dcd692cc9f713dc2
 755f19aa99a0ccba7d210e7f79182b09
 35b2dfd71f565cfc1b67983439c09f72
 d9a425eac54d6ca4a46b6a34650d3bf1
 67c6fabbb0534090a079ddd487d2ab4b
 e4eca131cde3fc18ee05c64bcdd90299
 c71121c007a65fac1c8157e5930d656c
 a86ce04694a53a30544ca7bb7c3b86cd
 7b22fa2f81e9cd14f1912589e0a8d309
 061c8eeb7d0d6c3ee751b05484f830b1
 3ab9c5962ab673f62823d8b5670f0c07
 1c968a80fa2616a4a2822d7589d9a5b4
 1593fbb5e69bb516ae32bec6994f1e5d
 133f2735e5123d848830423bf77e8c20

01dc62abf112f53a97234f6a1d54bc6f
18002ca6b19c3c841597e611cc9c02d9
046bcf4ea8297cdf8007824a6e061b63
89057fc8fedc7da1f300dd7b2cf53583
461ba43daa62b96b313ff897aa983454
d0dd88d60329c1b2d88555113e1ed66d
9c072edfb9afa88aa7a379d73b65f82d
b86409e2933cade5bb1d21e4e784a633
3fc8788fd0652e4f930d530262c3d3f3
15416f0033042c7e349246c01d6a43a3
f782d10eab3a7ca3c4a73a2f86128aad
cfd85a908554e0921b670ac9e3088631
abb49a9d81ec2cf8a1fb4d82fb7f1915
b2b4d7b5ce7c134df5cb40f4c4d5aa6a
8b01fc1e64316717a6ac94b272a798d4
81b2889bab87ab25a1e1663f10cf7e9e
3702360d1192736020b2a38c5e69263a
8139be1a7c6c643ae64dfe08fa8769ee

331f75a64b80173dc1d4abf0d15458cc 398168f0381ab36791f41fa1444633cc
d6f343e2bd295b69c2ce31f6fe369af9 f45963376918ed7dc2b96b16af976966
حمله نموده و
آخرین خبرها حاکی از آن است که این بدافزار به بزرگترین بانک اسرائیل با نام Hapoalim خساراتی را به شبکه
این بانک وارد نموده است.

سرور دریافت کننده اطلاعات

بدافزار به منظور ارسال اطلاعات، با سروری به شماره آی پی 29.57.142.174 ارتباط برقرار می نماید. مشخصات فنی
سرور فوق به قرار زیر می باشد:

- سیستم عامل ویندوز سرور 2008
- پورت فعال سرویس FTP با شماره 21
- پورت فعال 139

- پورت فعال سرویس ایمیل Pop3 با شماره 110
- پورت فعال سرویس msrpc با شماره 135
- پورت فعال سرویس اشتراك گذاري فايل ها با شماره 445
- پورت فعال با شماره 44442
- پورت فعال با شماره 49154
- مقابلۀ با

Mahdi بدافزار

از آنجائی که به دلایل نامشخص، این بدافزار یک بدافزار با قابلیت های فنی پائین تر (به نسبت دیگر بدافزارهای استفاده شده در حوزه جنگ های سایبری نظیر استاکس نت، دیوکیو و فلیم) می باشد، لذا استفاده از روش های ساده تر به منظور مقابله و پاک سازی ماشین های آلوده به این بدافزار کاربردی تر می باشد.

ماشین های آلوده میتوانند با خاتمه دادن به پروسه UpdateOffice.exe بدافزار را غیر فعال نمایند. همچنین مسیر زیر، مسیری است که بدافزار یک نمونه از خود را به آن جا منتقل می نماید:

C:\Users\%USERPROFILE%\Windows

به منظور پاک سازی لازم است محتویات این پوشه حذف شود.

همچنین، جهت پاک سازی کامل نیز توصیه می شود محتویات پوشه در مسیر زیر نیز به طور کامل حذف شوند:

C:\Users\%USERPROFILE%\PrintHood

لازم به ذکر است که بدافزار جهت مخفی نمودن فعالیت ها، این پوشه را مخفی می نماید.

7 - نتیجه گیری

نخستین قدم لازم در مبارزه با تهدیدات سایبری توسعه روش های تشخیص موثر است. پس از تشخیص، قدم مهم بعدی به دست آوردن راه هایی برای از کار انداختن زیر ساخت های بخش فرماندهی و کنترل بدافزارها و مختل کردن آن ها است. رایج ترین روش های به کار گرفته شده برای تحقق این کار شامل قطع کانال فرمان و کنترل و جلوگیری از ارسال دستورات از سوی مدیر بات به بات ها هستند که در این پژوهش پیشنهاد های مختلف ارائه گردید. روش های مختلفی برای تشخیص بدافزارها وجود دارد

که بررسی و بحث شد آنچه از منظر نویسندگان و عاملین این بدافزارها طرح است این است که روش های فرار نیز در حال توسعه هستند که بدافزارهای موجود را مخفی کرده و با افزایش سرعت تغییر و از روش های مختلف ردیابی آن ها را دشوار می سازند. امروزه بدافزارها برای عملیاتی شدن روی پایگاه های جدید شامل گوشی های هوشمند، تبلت ها و دیگر وسایل همراه فعال تر شده اند. در این حیطه چالش های فراوانی باقی مانده است. در این پژوهش روش های تحقیقی جدیدی که قابل توسعه هستند بررسی و ارائه شد اما موضوع مهمی که محققان با آن مواجه هستند دشواری آزمون و ارزیابی روش های تشخیص در سناریوهای واقعی یا در استفاده از داده های واقعی است. برخی ابتکار عمل ها مانند ایجاد انبارهای ردپا، با درصدی موفقیت نسبی اجرایی شده اند، اما دسترسی به داده ها گاهی کنترل می شود یا محدود به برخی موارد خاص می شود.

8- مراجع

- [1] J. Franklin, V. Paxson, A. Perrig, and S. Savage. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. In Proc. of the ACM Conference on Computer and Communications Security(CCS), 2007
- [2] C. Grier, L. Ballard, J. Caballero, N. Chachra, C. J. Dietrich, K. Levchenko, P. Mavrommatis, D. McCoy, A. Nappa, A. Pitsillidis, N. Provos, M. Z. Raque, M. A. Rajab, C. Rossow, K. Thomas, V. Paxson, S. Savage, and G. M. Voelker. Manufacturing Cpromise: The Emergence of Exploit-as-a-Service . In Proc. of the ACM Conference on Computer and Communications Security(CCS), 2012.
- [3] M. Cova, C. Kruegel, and G. Vigna. There Is No Free Phish: An Analysis of “Free” and

Live Phishing Kits. In Proc. of the USENIX Workshop on Offensive Technologies (WOOT), 2008.

[4] M. Fossi, E. Johnson, D. Turner, T. Mack, J. Blackbird, D. McKinney, M. K. Low, T. Adams, M. P. Laucht, and J. Gough. Symantec Report on the Underground Economy. Technical report, Symantec, Inc., 2008.

[5] M. McGuire and S. Dowling. Cyber crime: A review of the evidence. Research Report 75, Home Office, 2013.

[6] J. Brenner. America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. The Penguin Press HC, 2011.

[7] R. Clarke. Cyber War: The Next Threat to National Security and What to Do About It. Ecco, 2010.

[8] R. Langner. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Technical report, Langner Group, Nov. 2013.

[9] D. Sanger. Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times, 1 June 2012.

[10] Mandiant. APT1: Exposing One of China's Cyber Espionage Units. Technical report, 2013.

[11] C. Hosmer. Polymorphic & Metamorphic Malware. In Proceedings of the Black Hat Conference, 2008.

[12] Kaspersky. Ask An Expert: The Brainstorming. <http://blog.kaspersky.com/askanexpertthe-brainstorming/>, 2013.

- [13] M.Egele,T.Scholte,E.Kirda,andC.Kruegel.ASurveyon Automated Dynamic Malware Analysis Techniques and Tools. ACM Computing Surveys, 44(2), 2012.
- [14] D. Balzarotti, M. Cova, C. Karlberger, C. Kruegel, E. Kirda, and G. Vigna. Efficient Detection of Split Personalities in Malware. In Proc. of the Symposium on Network and Distributed System Security (NDSS), 2010.
- [15] K.Adams,T.Garfinkel,A.Warfield,andJ.Franklin.
CompatibilityisNotTrans- parency: VMM Detection Myths and Realities. In Proc. of the USENIX Work- shop on Hot Topics in Operating Systems (HotOS), .7002
- [16] C. Rossow and C. J. Dietrich. ProVex: Detecting Botnets with Encrypted Com- mand and Control Channels. In Proc. of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2013.
- [17] P. Ferrie. Attacks on More Virtual Machine Emulators. Technical report, Syman- tec, 2007.
- [18] P. Ferrie. Attacks on Virtual Machines. In Proceedings of the Association of Anti-Virus Asia Researchers Conference, 2007.
- [19] A. Moser, C. Kruegel, and E. Kirda. Exploring Multiple Execution Paths for Malware Analysis. In Proc. of the IEEE Symposium on Security and Privacy, 2007.
- [20] C. Kolbitsch, E. Kirda, and C. Kruegel. The Power of Procrastination: Detec- tion and Mitigation of Execution-Stalling Malicious Code. In Proc. of the ACM Conference on Computer and Communications Security(CCS), 2011.

- [21] E.Young and E.Ward.Trojan.Downbot.
http://www.symantec.com/security_response/writeup.jsp?docid=2011-052413-1248-99,
2011.
- [22] TrendLabs APT Research Team. Spear-Phishing Email: Most Favored APT Attack Bait.
Technical report, Trend Micro Incorporated,2012.
- [23] N. Provos, P. Mavrommatis, M. A. Rajab, and F. Monroe. All Your iFrames Point to
Us. In Proc.of the USENIX Security Symposium, 2008.
- [24] N. Provos, M. A. Rajab, and P. Mavrommatis. Cybercrime 2.0:When the Cloud Turns
Dark. Communications of the ACM, 52(4), 2009.
- [25] M. Polychronakis, P. Mavrommatis, and N. Provos. Ghost Turns Zombie: Ex- ploring
the Life Cycle of Web-Based Malware. In Proc. of the USENIX Workshop on LargeScale
Exploits and Emergent Threats (LEET), 2008.
- [26] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N.Modadugu. The Ghost in the
Browser: Analysis of Web-based Malware. In Proc. of the USENIX Workshop on Hot
Topics in Understanding Botnet, 2007.
- [27] L. Bilge and T. Dumitras. Before We Knew It: An Empirical Study of Zero-Day Attacks
in the Real World. In Proc.of theACM Conference on Computer and Communication
Security (CCS), 2012.
- [28] M. Cloppert. Security Intelligence: Attacking the Cyber Kill Chain.
<http://computer-forensics.sans.org/blog/2009/10/14/securityintelligence-attacking-the-killchain>, 2009.
- [29] G. Gu, R. Perdisci, J. Zhang, and W. Lee. BotMiner: Clustering Analysis of Network

Traffic for Protocol- and Structure-Independent Botnet Detection. In Proc. of the USENIX Security Symposium, 2008.

[30] J. Goebel and T. Holz. Rishi: Identify bot contaminated hosts by IRC nickname evaluation. In Hot Topics in Understanding Botnets, Apr.2007.

[31] J. R. Binkley and S. Singh. An algorithm for anomaly-based botnet detection. In SRUTI'06: Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet, pages 7–7, Berkeley, CA, USA, 2006. USENIX Association.

[32] A. Barsamian. Network characterization for botnet detection using statisticalbehavioral methods. Masters thesis, Thayer School of Engineering, Dartmouth College, USA, June 2009.

[33] T.-F. Yen and M. K. Reiter. Traffic aggregation for malware detection. In DIMVA '08: Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pages 207–227, Berlin, Heidelberg, 2008. SpringerVerlag.

[34] W. T. Strayer, D. E. Lapsley, R. Walsh, and C. Livadas. Botnet detection based on network behavior. In Advances in Information Security. 2008.

[35] W. Lu, M. Tavallaee, and A. A. Ghorbani. Automatic discovery of botnet communities on large-scale communication networks. In ASIACCS, pages 1–10, New York, NY, USA, 2009. ACM.

[36] A. Karasaridis, B. Rexroad, and D. Hoeflin. Wide-scale botnet detection and characterization. In Hot Topics in Understanding Botnets, Apr. 2007.

- [37] G. Gu, J. Zhang, and W. Lee. BotSniffer: Detecting botnet command and control channels in network traffic. In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), February 2008.
- [38] P. Porras, H. Saidi, and V. Yegneswaran. A multi-perspective analysis of the Storm (Peacomm) worm. In SRI Technical Report 10-01, 2007.
- [39] P. Porras, H. Saidi, and V. Yegneswaran. A Foray into Conficker's Logic and Rendezvous Points. In Proc. of the USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2009.
- [40] S. Stover, D. Dittrich, J. Hernandez, and S. Dietrich. Analysis of the Storm and Nugache trojans: P2P is here. ;login, 32(6), Dec. 2007.
- [41] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second generation onion router. In Proceedings of the 13th USENIX Security Symposium, Aug. 2002.
- [42] JAP. Jap anon proxy. http://anon.inf.tu-dresden.de/publications/index_en.html.
- [43] R. Albert and A. Barabási. Statistical mechanics of complex networks. Reviews of Modern Physics, 74(1):47–97, 2002.
- [44] ydklijnsma. Large botnet cause of recent Tor network overload. <http://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/>, 2013.
- [45] C. Guarnieri. Skynet, a Tor-powered Botnet Straight from Reddit. <https://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit>, 2012.

- [46] T. Holz, C. Gorecki, K. Rieck, and F. Freiling. Measuring and Detecting FastFlux Service Networks. In Proc.of the Symposium on Network and Distributed System Security (NDSS), 2008.
- [47] B.Stone-Gross,M.Cova,L.Cavallaro,B.Gilbert,M.Szydlowski,R.Kemmerer, C. Kruegel, and G. Vigna. Your Botnet is my Botnet: Analysis of a Botnet Takeover. In Proc. of theACM Conference on Computer and Communications Security (CCS), 2009.
- [48] N. Perlroth. Hackers in China Attacked The Times for Last 4 Months. The NewYork Times, January 30 2013.
- [49] Symantec Corp. Symantec Statement Regarding New York Times Cyber Attack. <http://www.symantec.com/connect/blogs/symantec-statement-regarding-new-york-timescyber-attack,2013>.
- [50] E. Nakashima. Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. The Washington Post, May 27 2013.
- [51] B. Krebs. Security Firm Bit9 Hacked, Used to Spread Malware. Krebs on Secuity, February 13 2013.
- [52] C. Wisniewski. Twitter botnet command and control captured.<http://nakedsecurity.sophos.com/2010/05/18/twitter-botnetcommand-control-captured/>, 2010. [53] J. Nazario. Twitter-based Botnet Command Channel. <http://www.arbornetworks.com/asert/2009/08/twitter-based-botnetcommand-channel/>, 2009.
- [54] J. Nazario. Malicious Google AppEngine Used as a CnC. <http://www.arbornetworks.com/asert/2009/11/malicious-googleappengine-used-as-a-cnc/>, 2009.

[55] N. Villeneuve, N. Moran, and T. Haq. Evasive Tactics: Taidoor. <http://www.fireeye.com/blog/technical/2013/09/evasive-tacticstaidoor-3.html>, 2013.