دانشگاه پیام نور استان تهران مرکز

تهران شمال

پروژه کارشناسی

رشته مهندسی کامپیوتر

گرایش نرم افزار

عنوان پروژه :

عملکرد بدافزارها

استاد راهنما

جناب آقاي دکتر سید علی ابراهیمی رضوي

تهیه کننده:

مژده سریاری خان

خرداد1400

قدردانی و سپاس

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

بر خود لازم می دانیم که از استاد راهنماي ارجمندمان جناب آقاي دکتر سید علی ابراهیمی رضوي که با راهنمایی هاي دقیق و ارزنده خویش در طول تحصیل و اجراي این پروژه همواره مارا یاري نموده و حق استادي را بر ما تمام کردند سپاسگذاري کنیم.

چکیده

یکی از مسائل مهم و حیاتی در امنیت سایبري امروز، ظهور حملات هدفمند با استفاده از ابزارهاي پیشرفته توسط دشمنان می باشد.(اغلب تحت عنوان تهدیدهاي پیشرفته مداوم[1] 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 طبیعتا مقابله با این تهدیدها و حفاظت از زیرساخت ها در برابر این گونه حملات کاري 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 درك روش هاي اسقرار فرماندهی و کنترل[2] ، تشخیص و حذف کانال هاي ارتباطی آن ها می باشد.

در ادامه براي درك هرچه راحت تر روش هاي فرماندهی و کنترل این حملات ابتدا به طور خلاصه وضعیت فعلی حملات سایبري را بررسی می کنیم و با آخرین تغییرات در نحوه و چگونگی انجام چنین حملاتی آشنا خواهیم شد. سپس نحوه راه اندازي بخش فرماندهی و کنترل را بررسی خواهیم کرد، به این صورت که تکنیک هایی که مهاجمان براي راه اندازي کانال هاي ارتباطی و پنهان سازي آنها و ابزراهاي امنیتی که در این راستا استفاده می شوند را ارائه خواهیم کرد.

ایجاد و استفاده از سیستم فرماندهی و کنترل بخش مهمی از حملات سایبري از راه دور است. فرماندهی و کنترل براي هدایت و کنترل سیستم آلوده شده به سمت انجام فعالیت هاي مورد نظر مهاجمان امري ضروري است.فرماندهی و کنترل همچنین در زمینه استخراج اطلاعات از سیستم آلوده نقش مهمی بر عهده دارد. آمار منتشر شده از حملات سایبري 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 هاي موثر براي مقابله با این حملات تشخیص و از بین بردن بخش فرماندهی و کنترل حملات می باشد. حداقل تاثیر این مقابله قطع ارتباط بین سیستم هاي آلوده با مهاجمین است که باعث ناقص ماندن حمله و در مواردي جلوگیري از نشت اطلاعات می شود.

فهرست مطالب

مقدمه

MALWAREیا بدافزار از دو واژه تشکیل شده است ، Mal مخفف Malicious یا مخرب و Ware مخفف Software یا نرم افزار است. تمامی کدهاي مخربی که نوشته می شود در رده Malware ها یا بدافزارها طبقه بندي می شوند ، این کد ها می توانند شامل ویروس ها ، کرم ها ، اسب هاي تروجان ، adware ها ، Scare ware ها ، روتکیت ها و سایر نرم افزارهاي 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 افزاري اطلاق می شود که عمداعمداً براي انجام اعمال غیرمجاز و گاهاگاهاً مضر ایجاد شده است. ویروسها ،backdoor ها، کی لاگرها، برنامه هاي سارق کلمه عبور و سایر برنامه هاي تروجان، ویروسهاي ماکرو در Word و Excel ،ویروس هاي بوت سکتور، ویروس هاي اسکریپت (java، windows shell، batch و غیره) و تروجانها، برنامه هاي تبهکارانه، بدافزار جاسوسی (spyware) و بدافزار تبلیغاتی(adware) تعدادي از نمونه هاي بدافزار هستند. زمانی، نامیدن چیزي با ویروس یا تروجان کافی بود، اما روشها و حاملهاي آلودگی توسعه یافت و اصطلاح ویروس و تروجان دیگر تعریف رضایت بخشی براي همه انواع برنامه هاي مخرب موجود ارائه نمی کند. بصورت کلی هر نوع کد نرم افزاري که بر روي سیستم شما قرار بگیرد و عملیاتی ناخواسته را انجام دهد به عنوان بدافزار شناخته می شود ، براي مثال Spyware ها نرم افزارهاي جاسوسی هستند که بدون اینکه کاربر متوجه شود کلیه اطلاعات شخصی وي را دریافت کرده براي شخص نویسنده بدافزار ارسال میکند ، worm ها یا کرم هاي اینترنتی بدافزارهایی هستند که خودشان را در شبکه تکثیر کرده و عملیات هاي مختلف تخریبی انجام میدهند، براي مثال فایل هاي شما را پاك میکنند، فایل هاي اضافی بر روي سیستم شما ایجاد می کنند و در نهاید 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 هاي فلش و سی دي ها است ، اسب هاي تروجان یا همان Trojan Horse ها در عین اینکه نرم افزار مفیدي به نظر می رسند خود را به یک نرم افزار مفید کاربردي متصل کرده و فعالیت هاي 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 براي 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 بسیاري دیگر از این نوع کد هاي 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 گوشیهاي هوشمند راه پیدا میکنند؟

رویکرد ما در مواجه با این مساله بر مبناي یک بررسی جامع و سیستماتیک است. در حوزه کارهاي آکادمیک به بررسی نشریات

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

بدافزارها توسط برنامه نویسان براي اهدافی نظیر خرابکاري و ایجاد خسارت به کار میرفتند، اما پس از گذشت چندین سال مجرمان از آن به عنوان یک منبع درآمد استفاده کردند. وقتی یک بدافزار روي رایانه شخصی شما نصب شود، آن را اصطلاحا به یک کامپیوتر زامبی[1] تبدیل میکند که صدها هزار ایمیل اسپم[32] را از مردم سراسر دنیا برایتان میفرستد؛ بدون اینکه حتی بدانید یا ببینید که رایانه شما هم در توزیع حمله هاي این سرویسهاي ناخواسته[3] (DDoS) نقش کوچکی را بازي میکند. بنابراین، این طور که به نظر میرسد بدافزارها تنها میتوانند دسکتاپ ها و لپتاپ ها را هدف قرار دهند. اما متاسفانه این طور نیست!

اولین ویروس موبایل در سال 2004 توسط یک کمپانی به نام اُجام[4] هنگام ساختن بازي موسکیتو[4] پدیدار شد. این ویروس بدون اطلاع کاربر پیامهایی را ارسال میکرد و هزینههایی براي کاربر به وجود میآورد. چند هفته بعد، خورههاي کامپیوتر شکلی

[1] zombie computer
[2] distributed denial-of-service
Ojam
[3] spam
[4] Musqito

از یک ویروس مفهومی به نام کابیر[1] ایجاد کردند که میتوانست تا شعاع 10 متري خود را به هر تلفن همراهی که بلوتوث آن روشن است انتقال دهد.

اگرچه، تنها زمانی روي گوشی نصب میشد که کاربر نصب آن را بپذیرد. هرچند انتقال فایل از طریق بلوتوث کمی عذاب آور است و باتري زیادي مصرف میکند اما با ورود Commwarrior-A در سال 2005 موج جدیدي از حملات ایجاد شد که هزینه زیادي براي مردم در برداشت. این ویروس از طریق پیام چندرسانه اي 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 سیمانتک[2] خاطر نشان کرد جذابیت تلفنهاي همراه براي مجرمان سایبري افزایش پیدا خواهد کرد.

همچنین افزود احتمال اینکه کاربران اطلاعات کارت اعتباري یا کارت بانکی خود را براي خرید نرم افزار به صورت آنلاین و پرداخت به صورت بیسیم، روي تلفن همراهشان ذخیره کنند زیاد است. بنابراین سارقان علاقه زیادي دارند تا میزان آسیبپذیري این اطلاعات را امتحان کنند.

گوگل اخیرا برنامه هایی را در فروشگاه مجازي 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 مجازي حذف کرد. چند بخش از این بدافزارها نیز در آیفونها یافت شدند. اما تنها در آیفونهاي قفل شکسته یا اصطلاحا جِیل بِرِكِ، زیرا خود کاربرها با این کار به نوعی امنیت دستگاههاي تلفن همراهشان را تهدید میکنند. چند نوع از ویروس زئوس هم گوشیهاي بلکبري را هدف قرار دادند. سیمبین و ویندوزموبایل هم گاها مورد تهدیدات امنیتی ویروسها بودهاند. به نظر میرسد که هیچ کس از دست آنها در امان نیست. پس آیا باید نگران باشید؟ سیسکو 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 هاي حمله مهاجمین تغییرات اساسی کرده و از حملاتی که به خاطر کسب اعتبار و شهرت صورت می گرفت به سمتدرآمد زایی و اهدافی نظري جاسوسی صنعتی یا اسناد محرمانه تغییر جهت داده{1}. امروزه گروه هاي خلافکار کاملا سازمان یافته عمل می کنند. براي هر بخش از حمله نیروهاي متخصص در آن زمینه را استفاده می کنند. براي مثال نیروي متخصص برنامه نویس بر روي کد بدافزار مخرب کار میکند، نیروي وظیفه تمرکز بر روش هاي درآمد زایی از اطلاعات بدست آمده را برعهده دارد و نیروي دیگر بررسی می کند که چه اطلاعاتی از سیستم هاي هدف می تواند درآمد زایی کافی را گروه هایی که کمتر پیشرفته هستند بیشتر از اکسپلویت هاي آماده{2} یا ابزارهاي 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 بازارهاي زیر زمینی در زمینه فروش بدافزار ها، اطلاعات سرقت شده و یا هرچیزي که به این حوزه مربوط است شده است{4}{5}

گروههاي سنتی فعال در این زمینه بیشتر بر روي بدست آوردن شماره و رمز حساب هاي بانکی تمرکز دارند که به سرعت امکان درآمد زایی فراهم شود. با این حال اخیرا آمار حملاتی که براي سرقت اطلاعاتی همچون قراردادها، طرح هاي تولیدي و ...به طور فزاینده اي رشد پیدا کرده. جاسوسی هاي صنعتی و تجاري از اهداف اینگونه حملات هستند.

اخیرا برخی دولت ها براي دستیابی به اهداف خود حمایت هاي گسترده اي از مهاجمان می کنند تا حملاتی تا براي رسیدن به اهداف دولت برنامه ریزي و پیاده سازي کنند. حملات در سطح کشورها اغلب داراي دو هدف عمده است:

- جاسوسی سیستماتیک و جامع از کل بخش هاي اقتصادي و صنعتی کشورهاي دیگر با هدف دستیابی به اهداف استراتژیک{6}

- خرابکاري زیرساخت هاي حیاتی ملی مانند نیروگاه ها و سیستم هاي کنترل حمل و نقل

پیامدهاي این گونه حملات به اندازه اي است که برخی کارشناسان از آن ها به عنوان جنگ سایبري اشاره می کنند {7}.

شناخته شده ترین نمونه این حملات استاکس نت است که توسط ایالات متحده آمریکا و رژیم صهیونیستی براي خرابکاري در تاسیسات هسته اي جمهوري اسلامی ایران اتفاق افتاد {8و9}.

بسياري از برنامه هاي آلوده كننده اوليه، از جمله اولين كرم اينترنتی و تعدادي از ويروس هاي سيستم عامل داس[1]، به قصدآزمايش يا سرگرمی نوشته شدند. آن ها عموماً به مقاصد بی ضرر يا فقط به قصد آزار بودند، تا اينكه بخواهند خسارات جدي بهسيستم هاي رايانه وارد كنند. در برخی موارد سازنده نمی توانست تشخيص دهد كه چقدر كارش می تواند مضر باشد. برنامه نويسان جوان وقتی درباره ويروس ها و ترفندهايش می آموختند، تنها به منظور تمرين يا به اين قصد كه ببينند چقدر شيوع پيدا ميكند، آنها را می نوشتند. در سال 1999 ويروسهاي شايعی مانند ويروس مليسا[2] و ويروس ديويد[3] تنها به قصد سرگرمی نوشته شده بودند. اولين ويروس تلفن همراه در سال 2004 با نام ويروس كابير بر روي تلفنهاي همراه منتشر شد. با اين حال مقاصد سوء به منظور خرابكاري را می توان در برنامههايی يافت كه براي ايجاد آسيب به سيستم رايانهاي و يا از دست رفتن اطلاعات، طراحی شده اند. بسياري از ويروس هاي سيستم عامل داس، با اين هدف طراحی شدند تا فايل هاي موجود در يک ديسک سخت را نابود كنند يا فايلهاي سيستمی را با نوشتن اطلاعات نادرست بر روي آنها دچار اختلال كنند.

از زمان گسترش دسترسی به اينترنت پر سرعت، بدافزارهايی به منظور ايجاد سود طراحی شده اند. به عنوان مثال از سال 2003، اغلب ويروسها وكرم هاي رايانهاي، طراحی شدند تا كنترل رايانههاي كاربران را به منظور بهرهگيري در بازار سياه به كار گيرند.

1 - حملات هدفمند[4]

حملات هدفمند با سناريو پيچيده و صرف هزينه هاي هنگفت تلاش براي دستيابی و نفوذ به اطلاعاتی از سازمان ها يا اشخاص ازپيش تععين دارند در صورتی كه در گذشته حملات عليه اهداف متعددي انجام می شد و از بين افراد يا سازمان هاي بيشماري كهآلوده شده بودند اطلاعات مورد نياز در صورت وجود استخراج می شد.

در حملات هدفمند مهاجمين فقط بر روي يک هدف تمركز می كنند و در صورت نفوذ به سيستم هاي ديگر يا افراد ديگر انتشارپيدا نمی كنند. چرخه عمر يک حمله به اين صورت است كه شامل يک مرحله شناسايی كه در اين مرحله ابزار دفاعی

[1] DOS
[2] Melissa
[3] David
[4] APTs

سیستم هدف مورد بررسی وتحلیل قرار می گیرند تا نقاط ضعف احتمالی شناسایی شود. {10}. سپس یک سناریو هدفمند نیاز است تا به سیستم هاي هدفبه مدت هر چه بیشتر نفوذ شود و بدافزار در آن مستقر باشد.

1 -1- مخفی سازي حملات

منظر ديگري كه می خواهيم در اين گزارش بررسی كنيم استفاده روز از افزون از تكنيک هاي مخفی سازي در اين گونه حملاتاست كه همواره در حال پيچيده تر شدن و آشكار سازي آنها سخت تر است. مهاجمان تلاش دارند تا جايی كه ممكن است شناسايی نشوند و سيستم هاي امنيتی هدف را تحريک نكنند. براي اين منظور روش هايی را استفاده می كنند كه تاثير قابل توجهی در پنهان سازي مخصوصا در سيستمهاي سنتی دارد.

1 -1-1- مبهم سازي الگوها[1]

مكانيسم هاي دفاعی قديمی (مانند آنتی ويروس هاي قديمی و سيستم هاي تشخيص نفوذ) اغلب به شناسايی الگو و ساختار براي شناسايی حملات يا كدهاي مخرب تكيه می كنند. هر الگو به طور منحصر به فرد يک نوع حمله را مشخص می كند كه با استفاده از مجموعه اي كاراكترها بيان می شود. اين كاراكترها بر اساس نوع توابع و عبارات به كار رفته در كدهاي مخرب ايجاد می شوند. مهجمان براي اينكه در دام آنتی ويروس ها گرفتار نشوند از روش هاي مختلفی براي مبهم سازي كد ها استفاده می كنند تا الگوي ايجاد شده توسط كدها متفاوت با نمونه هاي قبلی باشد و توسط آنتی ويروس ها شناسايی نشود.

براي مثال پولی مورفيسم يک از روش هايی است كه در آن كد مخرب بسته به شرايط محل اجرا رفتارهاي متفاوتی از خود بروز می دهد و از شكلی به شكل ديگر تبديل می شود و حتی يک نسخه كملا جديد از خود ايجاد می كند كه همين امر باعث عدم شناسايی توسط آنتی ويروس ها می شود.{11}. اخيرا شركت KasperSky اعلام كرده كه در هر دوثانيه بيش از دو بدافزار كه از الگوها يكتا استفاده می كنند كشف می شود كه به احتمال زياد از تكنيک هاي چندريختی يا پولی مورفيسم[2] استفاده می كنند.{12}

1 -1-2- مقابله با سيتم هاي تحليل پويا

شركت هاي امنيت براي مقابله با روش هاي پولی مورفيسم كه مهاجمين استفاده می كنند از ابزارهاي تجزيه و تحليل پويا سندباكس ها (جعبه شنی) استفاده می كنند.{13} اين ابزار ها ابتدا كد يا برنامه ر در يک محيط ايزوله مخفی اجرا می كنند و پس از مشاهده رفتارهاي كد يا ابزار نمونه، تشخيص می دهند كه از نوع مخر است يا نه. مهاجمين براي فرار از اين دام نكاتی را بررسی می كنند كه در اصطلاه قرص قرمز ناميده ميشوند. عملكرد به اين گونه است كه هنگامی كه بدافزار يا كدمخرب اجرا می شود در صورتی كه هر نشانه اي مبنی بر اين كه در محيط سندباكس اجرا می شود مشاهده كند رفتارهاي مخرب خود را متوقف می كند{14}

برخی از نكاتی كه از آنها به عنوان قرصهاي قرمز استفاده می شود بررسی فايل ها ، كليدهاي رجيستري يا پروسه هاي در احال اجرا است تا از آنها بفهمند كه آيا اثري از ابزارهاي تجزيه و تحليل بدافزار بر روي سيستم هدف است يا نه.

Signature

Polymorphism

از آنجايي كه برخي از كدهاي مخرب يا بدافزارهايي كه توسط مهاجمين استفاده مي شوند در محيط هاي واقعي و محيط هايمجازي و شبيه سازي شده رفتار متفاوتي دارند{15،17،18،16} مهاجمين نكات ديگري را نيز بررسي مي كنند تا از اجراي برنامه در محيط واقعي اطمينان حاصل كنند. براي مثال بررسي رفتارها و زمان بندي CPU كه در محيط مجازي و واقعي متفاوت است.

از ديگر روش هايي كه مهاجمين استفاده مي كنند اين است كه اجراي كد مخرب يا بدافزار خود را وابسته به يک پيش شرطي مي كنند تا اگر آن پيش شرط برقرار باشد برنامه اجرا شود.{19} براي مثال برنامه مخرب بررسي كند كه يک فايل خاص يا يک مسير خاص بر روي سيستم هدف وجود دارد يا نه و در صورت وجود بخشي از كد را اجرا كند و مرحله بعد را باز منوط به وجود پيش شرطي ديگر.

يا برخي وجود اتصال اينترنت را به عنوان پيش شرط قرار مي دهند. برخي ديگر فقط در يک محدوده زماني خاص فعال مي شوند يا برخي منوط به وجود يک آي پي يا نام كاربري خاص هستند. يا برخي منتظر دريافت يک دستور از بخش فرماندهي و كنترل مي مانند تا مراحل بعدي را اجرا كنند.

در گام بعدي جنگ بين مهاجمان با مكانيسم هاي دفاعي، بدافزارنويسان شروع به نوشتن كدهايي كردند تا انرژي مكانيسم هاي دفاعي را هدر دهند {20}. قبل از اجراي هر گونه فعاليت مخرب توسط بدافزار اين كدها اجرا مي شوند، هدف از اين كدها ايجاد تاخير در فعاليت سيستم هاي دفاعي تا با افزايش زمان فرصت بررسي كدهاي اصلي بدافزار را به مكانيسم هاي دفاعي ندهند. در نتيجه مكانيسم هاي دفاعي كدها را مخرب تشخيص نداده و هيچ گونه فعاليت مشكوكي مشاهده نخواهند كرد.

از آنجاييكه سند باكس ها و ابزارهاي تجزيه و تحليل پويا بايد حجم زيادي از برنامه ها را بررسي كنند، براي اينكه منبع سيستم را بيش از حد اشغال نكنند زمان محدودي را به اين امر اختصاص مي دهند. بدافزارنويسان كدها و برنامه مخرب خود را طوري طراحي مي كنند تا در اين مدت زمان مشخص هيچ فعاليت مشكوكي از خود بروز ندهد و پس از آن فعاليت اصلي خود را انجام دهد. همين كار باعث فرار از شناسايي توسط سيستم هاي دفاعي مي شود.

1 -1-3 - منحرف كردن سيستمهاي اعتبار سنجي

يک از مكانيسم هاي دفاعي كه در سالهاي اخير كشف شده است استفاده از اطلاعات اعتبار سنجي شده (نام دامنه و سرورها) در شبكه است . اين ايده به اين صورت است در صورتي كه اتصالات زيادي يا بلند مدتي به دامنه ها يا آي پي هايي كه اعتبار سنجي نشده اند صورت بگيرد پس از مدتي اين دامنه ها يا آي پي ها مسدود ميشوند.

1
2

بدافزار نويسان براي مقابه با اين سيستم دفاعی از يک روش سخت اما موثر استفاده می کنند. آنها از يک سرور يا دامنه خاص براي يک مدت زمان محدود استفاده می کنند، پس از آنکه آي پی و يا نام دامنه در ليست سياه قرار گرفت ديگر از آن آي پی و دامنه استفاده نمی کنند و آي پی و نام دامنه ديگري جايگزين می کنند. اين استراتژي هزينه و نيروي مضاعفی از مهاجمان در اختيار می گيرد اما موثر است.

نتايج منتشر شده از محققان گوگل نشان می دهد که اين روش اکنون به خوبی در حال اجرا توسط مهاجمين است و متوسط مدتزمان طول عمر دامنه و سرورهاي آنها 5.2 ساعت است.{2}

1 -1-4 - استکانوگرافی[1]

در حالی که سيستم هايی مانند Tor به منظور ناشناس بودن مبدا و مقصد ارتباط ايجاد شده اند، روش هايی نيز وجود دارند که داده مبادله شده را نيز غير قابل رهگيري و شنود می کنند. رايج ترين روش براي ارتباط غير قابل شنود استفاده از روش استکانوگرافی است.

استکانوگرافی کلمه است يونانی به معنی مخفيانه نوشتن و به روشی اتلاق می شود که در آن پيام ها طوري نوشته می شوند که فقط گيرنده و فرستنده قادر به خواندن پيام هستند. دو راه براي استفاده از استکانوگرافی توسط بدافزار براي ارتباطات فرماندهی و کنترل وجود دارد. اول اينکه بدافزار ها می توانند پروتکل ارتباطی خود را مانند ديگر پروتکل ها در نظر بگيرند. دوم می توانند داده هاي مبادله اي خود را در محتواهاي قانونی مانند تصاوير بگنجانند. امروزه اکثر انواع فايل مانند متنی، عکسی و ويديو می توانند داده هايی را به روش هاي مختلف درون خود مخفيانه ذخيره کنند. در ساده ترين روش استفاده از اضافه کردن متاديتا[2] به فايل براي ذخيره سازي اطلاعات است البته اين روش به راحتی قابل کشف شدن است. از روش هاي جايگزين نيز می توان استفاده کرد به عنوان نمونه استفاده از تغيير در محتواي خود فايل پيشرفته تر و بهتر است. براي مثال در يک فايل تصوير هر پيکسل می تواند مقداري اطلاعات ذخيره کند که بر حسب اندازه و کيفيت تصور اين ميزان ميتواند مقدار قابل توجهی باشد. و تغييراتی که در عکس ايجاد می شود به راحتی با چشم تشخيص داده نمی شود.

در فايل صوتی با استفاده از ايجاد اکو و ايجاد تاخير در حد ميلی ثانيه که گوش معمولی متوجه آن نمی شود می توان اطلاعاتی را ذخيره کرد. روش هاي مختلفی براي استکانوگرافی وجود دارد اما در حال حاضر تعداد کمی از بدافزارها از استکانوگرافی استفاده می کنند. انتظار می رود با گذشت زمان و پيشرفت مکانيسم هاي دفاعی استفاده از روش هاي استکانوگرافی افزايش پيدا کند.

يکی از بدافزارهايی که از يک فرم از استکانوگرافی استفاده ميکند تروجان trojan.downbot است {21}

اين بات از طريق ايميل گسترش پيدا کرد و اولين کاري که پس از اجرا انجام می دهد به وبسايتی تحت کنترل مهاجم که آدرس آن ها در کد بدافزار است متصل می شود. اين وبسايت در ظاهر يک سايت آموزشی کدنويسی است که هر کسی به راحتی می تواند به آن دسترسی پيدا کند و بی ضرر است. اگر سورس صفحه تحليل شود اين کد شامل توضيحات رمز شده و کدهايی

است که در بایت هاي فایل تصاویر اضافه شده است. این توضیحات و تصاویر حاوي دستورات بخش فرماندهی و کنترل براي بدافزارها هستند، براي مثال آي پي و پورت هایی که براي آپلود اطلاعات توسط بدافزارها باید استفاده شود.

Steganography
MetaData

این روش یک تکنیک موثر براي ارتباط با بدافزارهاست زیرا که لاگ ذخیره شده کاملا نرمال و قانونی است زیرا یک صفحه htmlعمومی 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 براي مشاهده سایر صفحات نیز به مشکل بر می خورد.

بررسی نمونه stegobot

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

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

1 -2- شناسایی

در این مرحله مهاجمان اطلاعاتی را درباره هدف بدست می آورند ونقاط ضعفی را که می توان از آنها براي نفوذ استفاده کرد را شناسایی می کنند. این شناسایی هم بر روي افراد و هم تجهیزات هدف صورت می گیرد. مهاجمین شبکه ها وسیستم هاي هدف خود را با استفاده از روش هاي معمول مانند پورت اسکن و ... شناسایی می کنند تا حفره هاي امنیتی را کشف کنند. مهاجمین همچنین اطلاعاتی را در مورد افراد کلیدي در سازمان هدف بدست می آورند تا از آنها براي رسیدن به هدف خود استفاده کنند براي مثال در این مرحله می توان از اطلاعاتی که افراد درصفحات اجتماعی خود قرار می دهند استفاده کرد.

1
2

1 -3- نفوذ اولیه

در این مرحله مهاجمان می توانند به شبکه هدف نفوذ کنند. اغلب نفوذها معمولا از روزنه فیشینگ[1] انجام می شود. یک پیام فیشینگ ممکن است یک پیوست آلوده یا یک لینک وبسایت آلوده باشد{22}. معمولا پیامی که براي پیام هاي 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 براي ایجاد روزنه نفوذ اولیه استفاده میشود استفاده از وب سایت هایی است که مورد علاقه اهداف می باشد (روشحفره آبی[1]). در این روش مهاجمان کدهاي مخرب خود را در وبسایت هایی قرار می دهند که احتمالا توسط هدف مورد بازدید قرار می گیرند:

هنگامی که هدف از وبسایت بازدید می کند کدهاي مخربی براي ایجاد ارتباط اولیه بر روي سیستم قربانی ایجاد خواهد شد. حملات حفره آبی نسخه پیشرفته اي از حملات مبتنی بر دانلود ناخواسته است {24،23}. قربانیان با توجه به علائق خود از وبسایت هایی بازدید می کنند که این وب سایت ها بدون کسب اجازه از قربانی کدهاي مخربی را بر روي سیستم هدف بارگذاري می کنند که معمولا به زبان جاوااسکریپت نوشته می شوند. معمولا آسیب پذیري 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 اي رشد داشته است. به طور خاص حملاتهدفمند به چالش برانگیزترین تهدید امروز تبدیل شده است. حملات هدفمند افراد خاص یا سازمان هایی را هدف قرار می دهندکه داده هاي محرمانه مانند قراردادها، طرح هاي تجاري و تولیدي، اسناد نظامی و... در اختیار دارند. این حملات ابتدا شناساییهاي گسترده و جمع آوري اطلاعات دقیقی براي بدست آوردن نقاط ضعف در مکانیسم دفاعی اهداف انجام می دهند سپس بااستفاده از ابزارهاي مخرب پیچیده اقدام به انجام حمله می کنند(به طور مثال مکان یابی و سرقت اسناد حساس از داخل شبکههدف).

به علت ماهیت این گونه حملات مقابله با آنها بسیار دشوار است. مهاجمین در این حملات براي نفوذ کردن و کنترل کردن سیستمهاي هدف گاهی اوقات از اکسپلویت هاي زیرو دي[2].{27} و هم چنین کدهاي مخربی که براي مقابله با مکانیسم هاي دفاعیهدف طراحی شده اند استفاده می کنند.

[1] Phishing

آنها هم چنين ممكن است از تكنيک هاي مهندسی اجتماعی كه براي سوء استفاده از انسان ها طراحی شده، استفاده كنند. به اينصورت كه با متقاعد كردن افراد مشغول به كار در مجموعه هدف آنها را به سمت اجراي اهداف خود هدايت می كنند مانند نصب وراه اندازي نرم افزارهاي مخرب. وجود يک فرد در سازمان كه نكات امنيتی را رعايت نمی كند كافی است تا كل زنجيره دفاعيسازمان از هم متلاشی شود{28}. شناسايی روزنه اوليه كه باعث ايجاد ارتباط بين فرماندهی وكنترل با سيستم هدف شده استدر مقابله با اين حملات بسيار حائز اهميت است.

watering hole
Zeroday

مسدود كردن كانال ارتباطی فرماندهی وكنترل چندين مزيت دارد. اگر اطلاعت حساس از بين نرفته باشند به سرعت از نشتبيشتر اين اطلاعات جلوگيري می شود. در حالی كه امنيت سازمان هدف به خطر افتاده است اما هنوز اسناد و اطلاعات با ارزشبراي سازمان حفظ خواهد شد. حتی اگر اطلاعاتی نيز به سرقت رفته باشد درك ساختار فرماندهی وكنترل بدافزار می تواند برايیافتن سر منشا اصلی حمله مفيد باشد تا براي طی مراحل قانونی اقدام شود.

مرحله فرماندهی وكنترل مرحله اي است كه پس از نفوذ اوليه انجام می شود. به طور دقيق تر سيستم آلوده شده يک كانال ارتباطی با مهاجمين ايجاد می كند تا مهاجمين بتوانند سيستم را تحت كنترل خود قرار دهند. اين كانال ارتباطی با فرماندهی و كنترل مهاجمين را قادر می سازند تا با استفاده از ابزارهاي دسترسی از راه دور اقدام به نصب و اجراي ماژول هاي مخرب يا گسترش آلوده سازي به ساير قسمت هاي هدف و يا حملات DOS كنند. بخش فرماندهی وكنترل با توجه به اطلاعاتی كه پس از اولين اتصال از سمت سيستم آلوده به سمت مهاجمان می آيد مراحل بعدي حمله را مشخص می كند تا به نتيج دلخواه از حمله برسند.

حوزه امنيت بساير حوزه پيچيده و تغيير پذيري است به اين معنی كه بر اساس انواع حملاتی در حوزه سايبري اتفاق می افتد امنيت سايبري نيز متناسب با آنها تغيير می كند تا توانايی مقابله با حملات جديد را داشته باشد. در اين پژوهش فرض را بر اين قرار داديم كه اين تغييرات در نوع حملات به كندي اتفاق می افتد و بيشتر به حملاتی كه اكنون رايج هستند پرداخته ايم.

1 -4- 1 - ارتباطات و ترافيک فرماندهی و كنترل

مهاجمان روش ها و استراتژي هاي مختلفی را براي ايجاد يک ساختار فرماندهی وكنترل قوي و قابل اعتماد با كانال هاي ارتباطيمخفيانه پياده سازي می كنند. كه همين امر باعث به وجود آمدن طيف وسيعی از معماري ها و روش هاي مختلف و كارآمد درپياده سازي بخش فرماندهی وكنترل گرديده است. به عنوان مثال برخی از مهاجمان معماري هاي خود را بر اساس

1
2

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

سیستم فرماندهی و کنترل براي اکثر بدافزارهاي مدرن داراي 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. توپولوژي سیستم ممکن استاشکال 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 هاي دیگر ثابت هستند.

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

معماري بخش فرماندهی و کنترل اوایل از نوع متمرکز بود مانند استفاده از کانال IRC در این نوع معماري اگر سیستم هاي دفاعیحمله و کانال ارتباطی را شناسایی می کردند و سرور را از کار می انداختند به طور موثري بخش فرماندهی و کنترل دیگر کارایینداشت. چنین معماري هایی بسیار شکننده و با شیوهي مهندسی نرم افزاري ضعیفی همراه بود. به عنوان مثال معمولا آدرسسرورها داخل کد بدافزار به صورت استاتیک قرار میگرفت.

گسترش بات نت ها و به طبع آن مکانیسم هاي شناسایی سرورهاي 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 هاي اخیر کشف شده اند مانند peacomm،storm و conficker اغلب از ساختار شبکه هاي چندلایه استفاده می کنند. {38,93,40}

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

تکنیکها و روش هاي مختلفی براي 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 براي شناسایی ترافیک هاي مخرب می باشند. مهاجمان براي کاهش ضریب شناسایی به طور مداوم در حال تغییر روش هاي ارتباط هستند به همین دلیل نظارت و آنالیز مداوم شبکه امري ضروري است. در ادامه لیستی از اقدامات براي شناسایی و از بین بردن بخش فرماندهی و کنترل در زمان وقوع این حملات ارائه شده است.

شناسایی ترافیک هاي مخرب در شبکه بر اساس الگوهاي از پیش شناخته شده

جمع آوري و تجزیه و تحلیل ترافیک شبکه براي شناسایی فعالیت هایی که توسط کانال هاي ارتباطی فرماندهی و کنترل ایجاد می شوند.

* مانيتور ترافيک DNS براي شناسايي دستگاه هاي داخلي اي که تلاش می کنند با دامنه مخرب شناخته شده ارتباط بگيرند. براي اين منظور بايد همواره ليستی از دامنه هاي شناخته شده به عنوان فعال در زمينه فرماندهی و کنترل (اين ليست بايد حاوي نام دامنه هاي مخربی که به طور عمومی توسط شرکت هاي امنيتی منتشر شده و هم نام دامنه هايی که توسط تيم آنالیز داخلسازمان کشف شده باشد) موجود باشد که در صورت مشاهده ارتباط گيري دستگاه ها با هريک از اين دامنه ها اقدام متقابل صورت گيرد.

* مانيتور ترافيک IP براي شناسايي دستگاه هاي داخلي اي که تلاش می کنند با IP مخرب شناخته شده ارتباط بگيرند. براي اين منظور می توان از اطلاعاتی که ابزارهايی مانند NetFlow و sFlow در اختيار قرار ميدهند و همچنين ليست سياهی که حاوي IP هاي شناخته شده مخرب است استفاده کرد.

* مانيتور محتواي ترافيک شبکه براي شناسايي محتواهايی که الگوي منطبق با الگوهاي مخرب شناخته شده دارند. براي اين منظور می توان يک Sniffer بر روي شبکه فعال کرد و اطلاعات بدست آمده را با الگوهاي مخرب مقايسه کرد.

اقدامات فوق براي تشخيص کانال هاي ارتباطی با فرماندهی و کنترل هايی که توسط بدافزارهاي شناخته شده ايجاد شده اند يا بدافزارهايی که از اين کانال هاي از پيش شناخته شده استفاده می کنند به کار می روند.

با گسترش و تکامل بخش فرماندهی و کنترل سيستم هاي دفاعی رويکرد جديدي اتخاذ کردند، آنها پورت ها و پروتکل هايی را که در شبکه بدون استفاده بودن را مسدود کردند و فقط پورت ها و پروتکل هايی که ابزارهاي قانونی و مورد نياز از آنها استفاده می کردند را قابل استفاده گذاشتند. همين امر مهاجمين را تشويق کرد تا سعی کنند تا از پورت ها و پروتکل هاي رايج و قانونی استفاده کنند. براي مثال از طريق درج نظر در صفحات وب يا درج پست در انجمن هاي عمومی براي تبادل داده استفاده می کنند.
همين کار باعث می شود امکان مسدود کردن يا غير فعال کردن کانال ارتباطی به شدت کم شود.

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

اخيرا مهاجمان استفاده از سيستم هايی مانند JAP،Tor را آغاز کرده اند {41،42}. مخفی کردن نقاط مقصد ارتباطات مانع از شناسايی و فيلتر کردن بخش فرماندهی و کنترل توسط سيستم هاي دفاعی می شود حتی اگر الگوهاي ترافيکی را هم شناسايی کنند.

تشخيص فعاليت هاي مخرب شبکه که مطابق با الگوي از پيش شناخته شده نيستند

جمع آوري و تجزيه و تحليل ترافيک شبکه به منظور شناسايی فعاليت هايی غير معمولی که در شبکه اتفاق می افتد.

* ایجاد یک پایگاه داده هاي ترافیکی عادي شبکه که حاوي الگوهاي ارتباطی نرمال، حجم داده هاي مبادله شده و... می باشد که در ساعات و روزهاي مختلف بررسی و جمع آوري شده است.

* مقایسه ترافیک فعلی شبکه با پایگاه از پیش ایجاد شده براي ترافیک هاي نرمال، در صورتی که ترافیک فعلی شبکه مطابق با الگوي نرمال از پیش تعیین شده نباشد احتمال وقع حمله وجود دارد.

اقدامات فوق کمک به شناسایی کانال هاي ارتباطی بین بخش فرماندهی و کنترل با سیستم هاي آلوده می کند، کانال هایی که ازقبل شناخته شده نیستند و توسط هیچ بدافزار شناخته شده اي قبلا استفاده نشده اند.

- معماري متمرکز

طراحی هاي ابتدایی فرماندهی و کنرل بر پایه معماري متمرکز بودند به این صورت که یک یا چند سرور منحصرا براي ارتباطات استفاده می شدند.

طراحی دیگري که در این زمینه استفاده می شد استفاده ار سرور هاي IRC بود. IRC در سال 1988 ایجاد شد و پروتکلی بود که براي مبادله متن بر بستر اینترنت استفاده می شد. به همین منظور کانال هایی ارائه داده بود که امکان چت هاي گروهیی یا شخصی را فراهم می کرد. کانال ها بر روي سرورهایی قرار داشتند که خشی از شبکه IRC را تشکیل می دادند. علاوه بر اینکه برخی کانال ها عمومی بودند این امکان نیز وجود داشت تا براي ورود به کانال اعتبار سنجی صورت بگیرد. همچنین اعضاي کانال داراي سطح دسترسی هاي مختلفی بودند. چیزي مانند کانال هاي تلگرامی امروزه. این سیستم یک امکانی را براي ارتباطات بدافزارها فراهم کره بود تا دستورات از فرماندهی و کنترل به بدافزارها برسد و بالعکس. معماري متمرکز ساده و مدیریت آن راحت بود البته امکان از دست رفتن ناگهانی شمار زیادي از سیستم هاي آلوده نیز در آن بسیار است. {43}

- معماري غیر متمرکز

براي مقابله با ضعف هاي ساختاري و محدودیت هاي معماري متمرکز بسیاري از طراحان C2 به سمت طراحی فرماندهی و کنترل غیر متمرکز یا p2p گرویدند.اهداف اصلی این معماري عبارت است از:

توسعه پذیر باشد به این معنی که با رشد تعداد بات ها با صرف هزینه اندك بتوان بخش فرماندهی و کنترل را متناسب با آن رشد داد. تحمل خطاي 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 مرکزي وجود ندارد بلکه هر عضو شبکه می تواند به عنوان یک سرور عمل کند.

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

استفاده از شبکه هاي غيرمتمرکز C2 برگرفته از شبکه هاي اشتراك گذاري فايل p2p است.. در شبکه p2p هر عضو شبکه می تواند با تعداد نامحدود از ديگر اعضاي و مجاورانش در شبکه ارتباط برقرار کند.

اعضاي شبکه فقط می توانند با مجاوران خود در شبکه ارتباط برقرار کنند با ترکيب انواع مختلفی از شبکه p2p می توان تبادل داده را در کل شبکه برقرار کرد. شبکه هاي p2p ميتوانند از نوع چند لايه بدون ساختار باشند (Bittorrent, Gnutella, orKazaa) يا شبکه هاي چندلايه ساختار يافته مانند:

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

اکنون به بررسی عملکرد شبکه بيت تورنت می پردازيم. براي دستيابی به يک فايل در شبکه، کاربر يک فايل ردياب را دانلود ميکند که شامل ليست اعضايی از شبکه است که داراي قسمتی يا کل فايل هستند. سپس کاربر به طور مستقيم به آنها وصل می شود و قسمتی را که نياز دارد دانلود ميک ند. در نهايت شما کل فايل را دانلود خواهيد کرد. هرچه تعداد نيزبان ها بيشتر باشد سرعت دانلود فايل نيز سريع تر خواهد بود.

به اين ترتيب شبکه می تواند يک روش آسان براي انتشار اطلاعات در ميان تعداد زيادي از کاربران بدون استفاده از يک سرور مرکزي فراهم کند.

يک روش معمول براي بدافزارها اين است که بدافزار ليستی از ميزبان ها که می تواند به آن ها متصل شود را در اختيار دارد و به طور تکرارشونده بررسی می کند که از اين طريق دستوري ارسال شده است يا نه. کنترل کننده بات دستوري را براي يک يا گروهی از گره ها که در هر جاي شبکه ممکن است قرار داشته باشند ارسال می کند و از طريق الگورينم سيل آسا دستور به تمام گره ها می رسد. مزيت اين روش اين است که نيازي به يک ارتباط مستقيم بين داده ها و ارسال کننده (مانند سيستم متمرکز) نيست.

Tor

سرويسی است که امکان ناشناس بودن در محيط اينترنت را فراهم می کند. از اين امکان هم اشخاص و هم دولت ها استفاده می کنند.

اصول کار اين سرويس بر اين اساس است ترافيک اينترنت را از تعداد زيادي گره عبور می دهد و در هر عبور رمزنگاري و رمزکشايی می شود. شناسايی فرستنده و گيرنده داده ها از اين طريق بسيار دشوار است. همين امر سبب شده برخی از بدافزار نويسان از اين سرويس براي تبادل داده بين قربانی ها و بخش فرماندهی و کنترل استفاده کنند. براي اينکه از اين سرويس استفاده کنيد ابتدا بايد به سادگی نرم افزار اين سرويس را نصب کنيد پس از آن شما به عنوان بخشی از اين شبکه خواهيد بود. يکی از قابليت هاي پيشرفته تر tor توانايی ايجاد سرويس هاي مخفی است. اين امر به يک 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 هاي خروجی این شبکه مشخص شد که این ترافیک خیلی افزایش نداشته است. پس از بررسی هاي 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: اسکاي نت

اسکاي نت یک بات نت با اندازه متوسط 12000 دستگاه جزو بدافزارهاي خانواده زئوس است. نکته جالب توجه درباره این بدافزار (به جز استفاده از تور) این است که کنترل کننده آن در بخش آي ام ا[1] (پرسش و پاسخ) در ردیت[2] 1 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 تقریبا کاملی از بات نت مورد نظر برسند. این بدافزار از طریف شبکه اشتراك گذاري فایل یوزنت[3] گسترش پیدا کرد و عمدتا براي حملات ddos، سرقت اطلاعات و استخراج بیت کوین استفاده می شد. زمانی که بدافزار بر روي یک سیستم نصب می شد، نرم افزار Tor نیز نصب شده و یک سرویس مخفی تور بر روي دستگاه تنظیم میکرد. تمام ارتباطات با بخش فرماندهی و کنترل از طریق پروکسی هاي تور که بر روي سیستم تنظیم شده بودند انجام می شد. سرویس مخفی ایجاد شده بر روي پورت 55080 فعالیت میکرد. بخش فرماندهی و کنترل که یک سرور IRC بود پشت سرویس مخفی تور فعال بود.

سرور بر روي 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 هاي اعتباري 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 پیداکردن به سرور کنترل کننده ،محققان یک فایل xml حاوي اسامی وب سایت هاي 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 آي پی متعلق به پروکسی سرورها یافت شد که دو تاي از آنها فعال بودند و هیچ کدام توسط تور مخفی نشده بودند. با توجه به استفاده از تور تقریبا غیر ممکن بود که صاحب و مکان سرورهاي فرماندهی و کنترل مشخص شود. از طریق پاسخ هاي 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- جلوگيري از فعاليت فرماندهی و کنترل

طراحی و پياده سازي شبکه بايد به گونه اي باشد که بخش فرماندهی و کنترل در حملات کارايی لازم را نداشته باشد و تا حدزيادي از فعاليت اين بخش جلوگيري شود.

*جداسازي شبکه به بخش هاي مختلف بر اساس ميزان امن بودن، سطح طبقه بندي داده هاي موجود در شبکه و... (به عنوانمثال بخش سرورهاي عمومی، سرورهاي داخلی، ذخيره سازها و ...)

*قوانين و سياست هايی را ايجاد کنيد که سرعت ترافيک داده در نقاط ناامن شبکه کاهش پيدا کند.

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

[2][1] https://www.reddit.com/r/IAmA/

www.reddit.com

[3] Usenet

بررسی نمونه: طوفان[1]

يکی از بات نت هايی که به خوبی از شبکه p2p براي فرماندهی و کنترل خود استفاده می کند طوفان است. بات نت طوفان در بيشترين حالت خود در سال 2007، بين يک تا 50 ميليون سيستم را آلوده کرده بود. بدافزار طوفان تنها از طريق ايميل هاي اسپم، که داراي محتواي لينک به وبسايت هاي مخرب يا لينک هاي تبليغاتی که بدافزار را بر روي سيستم قربانی بارگيري می کرد توانست اين حجم آلوده سازي را انجام دهد. اولين کاري که بدافزار بعد از اجرا بر روي سيستم قربانی انجام می داد اين بود که بررسی کند که ساعت سيستم صحيح باشد. آن موضوع براي تبادلات حياتی است. بدافزار طوفان از OVER-NET استفاده می کرد که يک شبکه P2P مبتنی بر kademlia و داراي جدول درهم سازي توزيع شده است(DHT).

هر بات داراي يک شناسه 128 بيتی است که به صورت تصادفی ساخته می شود. گره اي حامل پيامی براي گره اي ديگري بود پيام را به سمت نزديک ترين شناسه به گره مقصد هدايت می کرد. بدافزار طوفان مانند بسياري از شبکه هاي P2P از ارتباطات publish/subscribe style استفاده می کرد.

يک گره اطلاعات را با استفاده از شناسه توليد شده متنشر می کند سپس گيرنده اطلاعات با استفاده از شناسه اقدام به دريافت اطلاعات می کنند.

[1] Storm

1 -5- استخراج

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

1 -6- بررسی برخی نمونه هاي موجود

در این بخش به بررسی چندنمونه از حملات هدفمند می پردازیم.

1 -6-1 - جاسوسی سیاسی

در ماه ژانویه 2013، نیویورك تایمز اعلام کرد که به مدت چهار ماه تحت حملات هدفمند قرار گرفته است. حملات توسط هکر هاي چینی صورت گرفته بود{48}. با تحقیقات بیشتر بر روي روش هاي انجام این حملات مشخص شد که این حملات در طرح گسترده کمپانی هایی را که در زمینه اخبار و تحلیل هاي 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 کاربري در دانشگاه هاي ایالات متحده آمریکا سعی در پنهان سازي هویت خود داشته اند سپس با استفاده از روش هاي فیشینگ به شبکه روزنامه تایمز نفوذ کرده اند.

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

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

بیانیه اي که مجله تایمز درباره این حمله منتشر کرد حاوي دو نکته مهم بود:

اول اینکه حمله اي 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 بدافزاري که در این حمله استفاده شده بود فقط یکی از آنها توسط آنتی ویروس هاي 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 اي مکانیسم هاي دفاعی با هم استفاده کرد.{49}

1 -2-6 - جاسوسی نظامی

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

این گزارش ادعا کرد طرح هاي بسیاري از ساخت سلاح هاي پیشرفته ایالات متحده آمریکا توسط هکرهاي چینی به سرقت رفته. در این گزارش آمده اسناد و مدارکی که به سرقت رفته مربوط به چندین سیستم موشکی، هواپیماهاي 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 مواردي است که حملات با هدف طرح هاي صنعتی صورت می گیرند. اسناد به سرقت رفته حاصل 15 سال تحقیق و توسعه بودند.

1 -3-6- 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 خطرناك هستند. این شرکت اعلام کرد که مهاجمان امضاهاي دیجیتالی را که از آن براي انتشار محصولات استفاده می کردند را به سرقت برده اند و در برخی موارد از آن براي انتشار بدافزار هاي خود استفاده کرده اند. بسیاري از مشتریان شرکت Bit9 با فرض اینکه نرم افزارهاي با امضاي دیجیتال این شرکت قابل اعتماد هستند اقدام به نصب نرم افزارهاي آلوده با امضاي سرقتی کرده اند.

1 -4-6- 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 سرورهاي داخلی مورد حمله واقع شده است: تحقیقات بیشتر مشخص کرد که یک اتصال از راه دور از کشور چین به سیستم هاي آلوده برقرار شده است. اطلاعاتی که مورد حمله و سرقت واقع شده بودند حاوي طرح

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

1 -5-6 - بدافزارهاي مخرب منابع زیرساختی

در سال 2013، یکی از محصولات امنیتی شرکت Lastline که بر روي سیستم هاي یک شرکت خدماتی نصب شده بود حمله اي از نوع دانلود ناخواسته را شناسایی کرد. این حمله زمانی آغاز شد که یکی از کارمندان شرکت یک وبسایت کاملا 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 هاي آلوده تلاش می کردند تا با یک دامنه خاص ارتباط برقرا کنند اما از طرف دامنه جوابی دریافت نمی کردند. روز بعد سیستم هاي آلوده موفق به برقراري اتصال با همان دامنه ها شدند و پس از برقراري اتصال بین بخش فرماندهی و کنترل و سیستم هاي آلوده یک فایل کانفیگ مربوط به بدافزار مالی فراگیر براي سیستم هاي 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 فورا آن را ترمیم میکنند. پس باید همواره نظارت بر شبکه ها و سیستم هاي سازمان وجود داشته باشد زیرا ممکن است بدافزاري که تا دیروز ظاهرا فعالیتی نداشته و تحت کنترل بوده امروز فعال شده و به سیستم ها آسیب برساند.

1 -6-6 - بدافزارهاي پلی مورفیسم

پس از اینکه یکی از محصولات Lastline بر روي سیستم هاي یک دانشگاه نصب شد،فعالیت بدافزاري در محیط سیستم هایدانشگاه مشاهده گردید. یکی از کاربران بخش اداري یک ایمیل حاوي لینک مخرب دریافت می کند و در مدت زمان کوتاهی دوباربر روي آن کلیک می کند که همین کار باعث بارگذاري یک بدافزار بر روي سیستم او می شود. نکته جالب اینجا بود که فایل هایی که پس از هربار کلیک کارمند بر روي لینک مخرب دانلود شده بود با هم متفاوت بودند. آنها نه تنها داراي هش هاي متفاوتی بودند بلکه در ویروس توتال داراي امتیازهاي متفاوت بودند. این نمونه استفاده از پولی مورفیسم را به خوبی نشان می دهد که یکی از تکنیک هاي کارآمد در زمینه مخفی سازي است. دیگر نکته موجود در این حمله استفاده از انسان به عنوان روزنه نفوذ که یکی از ضعیف ترین حلقه هاي زنجیر امنیت یک سازمان به شمار می آید.

از آماري که در بالا ارائه شد نکات زیادي مشخص می شود، یکی از نکاتی که مشخص شد این است که جلوگیري از نفوذ کار بسیار دشواري است و در سازمان هاي 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 اي ممکن است رخ دهد. در برخی موارد نیز ممکن است نفوذ از طریقی خارج از سازمان یا محیط هدف شروع شود و سپس به داخل سازمان و محیط هدف گسترش پیدا کند. براي مثال در سازمان هایی که از سیاست BYOD[1] استفاده می کنند.

2 - شبکه هاي اجتماعی

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

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

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

در نمونه اي که توسط شرکت آربور {53} کشف شد نیز استفاده از توییتر به عنوان بخشی از کانال هاي ارتباطی توییتر مشاهده شد. در این نمونه لینک هاي رمز شده بیس 64 که احتمالا سرورهاي ثانویه بخش فرماندهی و کنترل بودند از طریق توییتر مبادله می شد.

[1] *Bring your own device*

بدافزارهاي ديگري نيز مشاهده شد كه از شبكه هاي اجتماعی نظير جايكو و تامبلر استفاده می كردند. هم چنين بات نت ي مشاهده شد كه با استفاده از لينک هايی كه يک برنامه كاربردي مخرب كه بر روي گوگل اپ بارگذاري شده بود ايجاد می كرد اقدام به اتصال به بخش فرماندهی و كنترل می كرد.{54}

يکی ديگر از بدافزارهاي هدفمند كه از شبكه هاي اجتماعی به عنوان بخشی از فرماندهی و كنترل خود استفاده می كرد بدافزار تايدور است. تايدور به سازمان هايی كه مربوط به كشور تايوان بود حمله می كرد. شركت امنيتی فايرآي كشف كرد كه بدافزار از پست هاي ياهو براي ارتباط استفاده می كرده است.{55} اين بدافزار ابتدا از طريق ايميل يک فايل ورد آلوده وارد سيستم قربانی ميشده و سپس اقدام به دانلود فايل آلوده اصلی ميكرده است. دانلود به اين صورت بود كه دانلودر اوليه به يک پست وبلاگ ياهو كه ظاهرا داده هاي تصادفی و ناخوانا دارد متصل می شده است. اين داده هاي بی معنی رشته رمز شده بايني فايل آلوده اصلی بوده كه پس از رمزگشايی و به فايل اصلی بدافزار تبديل می شد. پس از استخراج فايل آلوده اصلی بدافزار به طور مستقيم به دو سرور فرماندهی و كنترل متصل می شد.

3- بدافزارهاي مسري: ويروس ها و كرم ها

انواع بدافزارها، ويروس ها و كرم ها هستند كه به خاطر نحوه شيوع شان شناخته می شوند. عبارت ويروس كامپيوتري به برنامه اياطلاق می شود كه نرم افزار قابل اجرايی را آلوده كرده باشد و هنگامی كه اجرا می شود، سبب شود كه ويروس به فايل هاي قابلاجراي ديگر نيز منتقل شود. ويروس ها ممكن است قابليت حمل يک بار اضافی را نيز داشته باشند، كه می تواند اعمال ديگر نيز انجام دهد. اين اعمال اغلب خرابكارانه هستند. از سوي ديگر يک كرم برنامه اي است كه به طور فعالانه خود را روي يک شبكه منتقل می كند تا رايانه هاي ديگر را نيز آلوده سازد. كرم ها نيز قابليت حمل يک بار اضافی را دارند.
تعريف هاي بالا نشان می دهد كه تفاوت ويروس و كرم در اين است كه يک ويروس براي شيوع نياز به دخالت كاربر دارد، در حالی كه يک كرم خود را به طور خودكار و از طريق شبكه گسترش پيدا می كند. در نتيجه آلودگی هايی كه از طريق ايميل يا فايل هاي مايكروسافت ورد منتقل می شوند، ويروس شناخته می شوند، زيرا بايد دريافت كننده فايل يا ايميل آن را باز كند تا سيستمآلوده شود. برخی نويسندگان در رسانه هاي محبوب نيز متوجه اين تمايز نيستند و از اين عبارت ها به اشتباه در جاي يكديگر استفاده می كنند.

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

یک برنامه خرابکار براي اینکه بتواند به اهدافش برسد باید قادر باشد که اجرا شود بدون آنکه توسط کاربر یا مدیر سیستم رایانه خاموش یا پاکسازي شود. مخفی کاري 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 تروآاست.

به بیان دیگر، یک اسب تروآ برنامه اي 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 هاي کاربر یا نصب نرم افزارهاي خرابکار یا نا مطلوب بیشتر. اسب هاي تروآ براي آغازسازي شیوع یک کرم استفاده می شوند.

یکی از مرسوم ترین راه هایی که جاسوس افزارها توزیع می شوند، از طریق یک اسب تروآکه 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. براي 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 سري 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 کارهاي تجاري استفاده می شوند.

2-3 - رد گم کن (Rootkits)

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

3-3 - بکدرها

یک بکدر روشی است براي خنثی سازي رویه هاي معمول تایید اعتبار. وقتی یک سیستم داراي چنین رویه هایی باشد یک یا چندبکدر ممکن است نصب شوند تا دسترسی هاي آتی را آسان تر سازد. بکدرها ممکن است حتی پیش از یک نرم افزار خرابکار نصبشوند تا به مهاجمان اجازه ورود دهند.

4-3 - ویروس

virusویروس به برنامه هایی گفته می شود که خود را تکثیر (Replicate) می کنند؛ بدین صورت که خود را به دیگر فایلها وبرنامه هاي اجرایی سرایت می-دهند. ویروس ها عموما در کنار تکثیر و تولید مثل، یک سري اعمال خرابکارانه دیگر نیز از خودنشان می دهند. ویروس ها براي آلوده کردن کامپیوترها، نیاز به اجرا شدن توسط کاربر یا یک برنامه را دارند.

5-3 - کرم

wormکرم ها برنامه هایی هستند که از طریق آسیب پذیري هاي شبکه اي کامپیوتر، به آن نفوذ می کنند. غالبا کرم ها پس ازنفوذ از طریق شبکه، اعمال مخرب یا مضر یا سودجویانه اي را روي سیستم انجام می دهند؛ مثلاسیستم را به ویروس آلوده میکنند. رفتار عمومی کرم ها به صورت زیر است:

در شبکه، کامپیوترها را جستجو می کنند و سیستم هاي آسیب پذیر را پیدا می کنند به کامپیوتر آسیب پذیر حمله و نفوذ کرده و برنامه اي روي آن به اجرا در می آورند از کامپیوتر جدید براي حمله به دیگر سیستم ها استفاده می کنند

معرفی بدافزار RDN/SPYBOT.BFR

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

نامگذاري ها این بدافزار با نام هاي زیر توسط ضدویروس هاي 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 روشهاي متعددي براي انتشار استفاده می کند. از جمله، از طریق دیسک هاي USB قابل حمل ،

CD هاي قابل نوشتن (Writable) و همچنین در محیط شبکه هاي محلی (LAN) بر روي شاخه هاي 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 اي که پیش آن در حافظه بار گذاري شده است، تزریق نموده و از این طریق باعث اجراي کد مورد نظر می شود. به بیان دیگر، این بدافزار تلاش می کند خودرا در بخشی از حافظه سیستم آلوده قراردهد که مربوط به یکی از پروسه هاي سیستمی و یا پروسه محافظت شده دیگري مانندپروسه Winlogon و یا Explorer است. بدین ترتیب بدافزار می تواند خود را از چشم کاربر یا سایر نرم افزارهاي دیگر پنهانکند.

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

کلیدهاي زیر در Registry سیستم آلوده توسط بدافزار تغییر کرده و دستکاري 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 هاي زیر ارتباط برقرار نماید.

80:**5،149،254،

پیشگیري hxxp://webllavepri.gurcanozturk.com/api

به روز نگه داشتن ضدویروس، نصب آخرین اصلاحیه هاي 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 روي لینک هاي ناآشنا ،همگی با هم می توانند خطر آلوده شدن به این بدافزار و یا گونه هاي مشابه را به حداقل برساند.

6-3 - اسب تروا

Trojanاسب تروا به برنامه هايی گفته می شود که مفيد به نظر رسيده و کاربر را براي اجرا اغفال می کنند، در حالی که علاوه برعمل مورد انتظار کاربر، يک عمل بدخواهانه ديگري را نيز به صورت مخفی انجام می دهند.براي مثال، کاربر يک برنامه بازي مجانيرا از اينترنت گرفته و نصب می کند و در کنار اجراي بازي، سيستمش آلوده به ويروس نيز می شود.

سب هاي تروجان برنامه هايی اند که در ظاهر به نظر می رسد در حال انجام کار بی ضرري هستند. اما در خفا داراي کدهاي مخربی هستند که کار ديگري انجام می دهند. در بسياري از موارد، تروجان ها يک در پشتی روي رايانه طعمه قرار می دهند که اجازه کنترل از راه دور کامپيوتر آلوده را به سازنده شان می دهند. يک کامپيوتر آلوده معمولا به صورت مستقيم يا به عنوان عضوي از شبکه رايانه هاي الوده به تروجان و يا ديگر برنامه هاي مخرب (botnet) مورد سوء استفاده قرار می گيرد. تفاوت عمده بين ويروس و تروجان اين است که تروجان خود را تکثير نمی کند. همچنين تروجان توسط کاربر به شکل ناآگاه نصب می شود.

هنگامی که کامپيوتر شما به تروجان آلوده شد، طراح تروجان می تواند از آن براي هر هدف بدي استفاده کند. مانند حملاتDos (denial of service) ، به يک وب سايت ، استفاده از پراکسی سرور براي مخفی کردن حملات، و يا حتی بدتر ، براي ارسال ده ها اسپم(هرزنامه). حفاظت در مقابل حملات تروجان ها، همانند روش حفاظت در مقابل ويروس هاست، ابتدا مطمئن شويد که برنامه آنتی ويروس شما به روز شده است. هيچ گاه فايل ضميمه مشکوك را باز نکنيد ، .و هميشه قبل از اينکه فايل کرك براي برنامه اي مثل فتوشاپ را دانلود و نصب کنيد ، به عواقب احتمالی اش خوب فکر کنيد. چون اصولا فايل هاي کرك مکانی ايده آل و مکان مورد علاقه تروجان نويسان براي مخفی کردن تروجان است .

7-3- نرم افزار جاسوسی

جاسوس افزار(Spyware) در تعريف، عبارت است از هر نرم افزار نصب شده بر روي کامپيوتر، که اطلاعات را بدون اطلاع شما جمع آوري کرده، و آنها را به سازنده خود بفرستد. سازنده برنامه با استفاده از اطلاعات شخصی شما، براي مقاصد سوء خود استفاده می کند. ممکن است اين جاسوسی به شکل keylogging (جاسوسی صفحه کليد) براي کشف و استفاده از رمزعبور، تماشاي نتايج جستجو، تغيير صفحه خانگی و موتور جستجوي مرورگر شما، اضافه کردن نوار ابزار مضر يا ناخواسته به مرورگر ، يا فقط سرقت شماره کارت اعتباري شما باشد.

از آنجا که نرم افزارهاي جاسوسی عمدتا به منظور کسب درآمد از جیب شما طراحی شده اند، معمولا نیازي به خرابکاري در کامپیوتر شما ندارند. در حقیقت بسیاري از کاربران بدون اینکه حتی از وجود آن اطلاع داشته باشند، روي رایانه خود نرم افزارهاي جاسوسی در حال اجرا دارند. اما به طور کلی آنهایی که داراي یک جاسوس افزار نصب شده روي رایانه خود هستند، احتمالا تعداد دیگري هم بدافزار دارند. هنگامی که روي رایانه شما تعدا زیادي نرم افزار جاسوسی در حل اجرا باشند، خواه ناخواه سرعت رایانه هم پایین می آید. چیزي که بسیاري از مردم در مورد نرم افزارهاي جاسوسی درك 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 افزاري که شما براي 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 اي برخورد کردید که در حال حاضر به شدت آلوده شده ، ترکیبی از برنامه هاي MalwareBytes و SuperAntiSpyware می تواند آن را کاملا تمیز کند.

این دسته از بدافزارها اقدام به دزدیدن اطلاعات از سیستم هاي کامپیوتري می کنند. نرم افزارهاي جاسوسی می توانند توسط دیگر بد افزارها مانند اسب هاي تروا یا کرم، نصب شوند و یا اینکه فرد سودجویی مستقیما اقدام به نصب آن ها بکند. یکی دیگر از راه هاي انتشار نرم افزارهاي جاسوسی، روش هاي تحریکات جمعی یا همان مهندسی اجتماعی (Social Engineering) مانند استفاده از ایمیل، براي ترغیب کاربر به نصب یک برنامه مجانی و به ظاهر مفید است. دسته اي از نرم افزارهاي جاسوسی به نام Keyloggerها وجود دارند که پس از اجرا، هر چیزي را که کاربر کامپیوتر تایپ می کند، در جایی ذخیره کرده و حتی می توانند از کارهاي وي فیلم تهیه کنند و سپس این اطلاعات را در شبکه یا اینترنت براي فرد دیگري 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 اي از این نوع بد افزار است. میزان مخرب یا خطرناك بودن این بدافزارها می تواند متغیر باشد. براي مثال اگر این برنامه بر روي سیستم عامل نصب باشد، به صورت بالقوه می تواند هر نوع جمع آوري اطلاعات کاربر یا دستکاري در دیگر نرم افزارها را انجام دهد. اما برنامه هاي تبلیغاتی که روي مرورگر ست میشوند، سطح آسیب کمتري خواهند داشت. البته عموما اطلاعاتی که توسط این نوع از بدافزارها جمع آوري می شود، اطلاعات کم حساس، مانند علاقه مندي هاي فرد به سایت هاي فروش کالا و . . . است.

4- نحوه تکثیر به چه صورت است ؟

ویروس هاي اولیه، کدهائی محدود بوده که به یک برنامه متداول نظیر یک بازي کامپیوتري و یا یک واژه پرداز ، الحاق می گردیدند. کاربري، یک بازي کامپیوتري 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 هاي فوق بگونه اي طراحی شده بودند که در زمان اجراي برنامه اصلی، بعلت فراهم شدن شرایط مساعد، اجرا می گردیدند. ویروس خود را بدرون حافظه منتقل و در ادامه بدنبال یافتن سایر برنامه هاي اجرائی موجود بر روي دیسک، بود. در صورتیکه این نوع برنامه ها، پیدا می گردیدند ، کدهاي مربوط به ویروس به برنامه اضافه می شدند. در ادامه ویروس، برنامه واقعی را فعال می کرد. کاربران از فعال شدن و اجراي ویروس آگاه نشده و در این راستا روش هاي خاصی نیز وجود نداشت. متاسفانه ویروس، نسخه اي 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 هاي فوق سایر برنامه ها را آلوده کرده و این روند تکراري ادامه می یابد.

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

تکثیر و گسترش از مهمترین ویژگی هاي یک ویروس کامپیوتري بوده و در صورت عدم امکان فوق ، عملا" موانع جدي در تکثیر ویروس هاي کامپیوتري بوجود آمده و برخورد با این نوع برنامه با توجه به ماهیت محدود میدان عملیاتی ، کار پیچیده اي نخواهد بود. یکی دیگر از ویژگی هاي مهم ویروس هاي کامپیوتري، قابلیت حملات مخرب آنان بمنظور آسیب رساندن به اطلاعات است . مرحله انجام حملات مخرب عموما" توسط نوع خاصی چاشنی (نظیر ماشه اسلحه) صورت می پذیرد. نوع حملات متنوع بوده و از نمایش یک پیام ساده تا پاك نمودن تمام اطلاعات موجود را می تواند شامل گردد. ماشه فعال شدن ویروس می تواند بر اساس یک تاریخ خاص و یا تعداد نسخه هاي تکثیر شده از یک ویروس باشد . مثلا" 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 هاي کامپیوتري افرادي آگاه و با تجربه بوده و همواره از آخرین حقه هاي موجود استفاده می نمایند. یکی از حقه هاي مهم در این خصوص ، قابلیت استقرار در حافظه و استمرار وضعیت اجراي خود در حاشیه می باشد (مادامیکه سیستم روشن است). بدین ترتیب امکان تکثیر این نوع ویروس ها با شرایط مطلوبتري فراهم می گردد. یکی دیگر از حقه هاي موجود ، قابلیت آلوده کردن "بوت سکتور" فلش دیسک هاي هارد دیسک ها، می باشد. بوت سکتور شامل یک

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

5 - برنامه هاي 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 هاي مخصوصی براي مبارزه با آن ها توسعه یافته است. برنامه هاي ضد بدافزار از دو طریق با بدافزار نبرد می کند:

1 - آن ها محافظت بی درنگ را در برابر نصب بدافزار روي یک رایانه می توانند تامین کنند، در این نوع از محافظت نرم افزار ضد بدافزارتمام اطلاعات ورودي از شبکه را اسکن می کند تا ازورود بدافزارها و تهدیدهایی که با آنها می آیند جلوگیري 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 دانلود آن اسکن نموده و از فعالیت هر چیزي که بد افزار شناخته شود ممانعت به عمل می آورد.

2-برنامه هاي ضد بدافزار می توانند تنها به منظور تشخیص و پاکسازي بدافزارهایی که قبلاً روي 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 محتواي رجیستري ویندوز، فایل هاي اجرایی سیستم و برنامه هاي نصب شده روي یک رایانه را اسکن می کنند و لیستی از تهدیدهاي 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 کاري 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 زیادي 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 براي رفتارشناسی یک فایل مشکوك می توانید از آنالیز پویا که نیاز به دانش خیلی زیادي در برنامه نویسی ندارد استفاده کنید.

در آنالیز پویا ما به از یک سري ابزارها براي ردگیري رفتارهاي یک مورد مشکوك استفاده می کنیم.

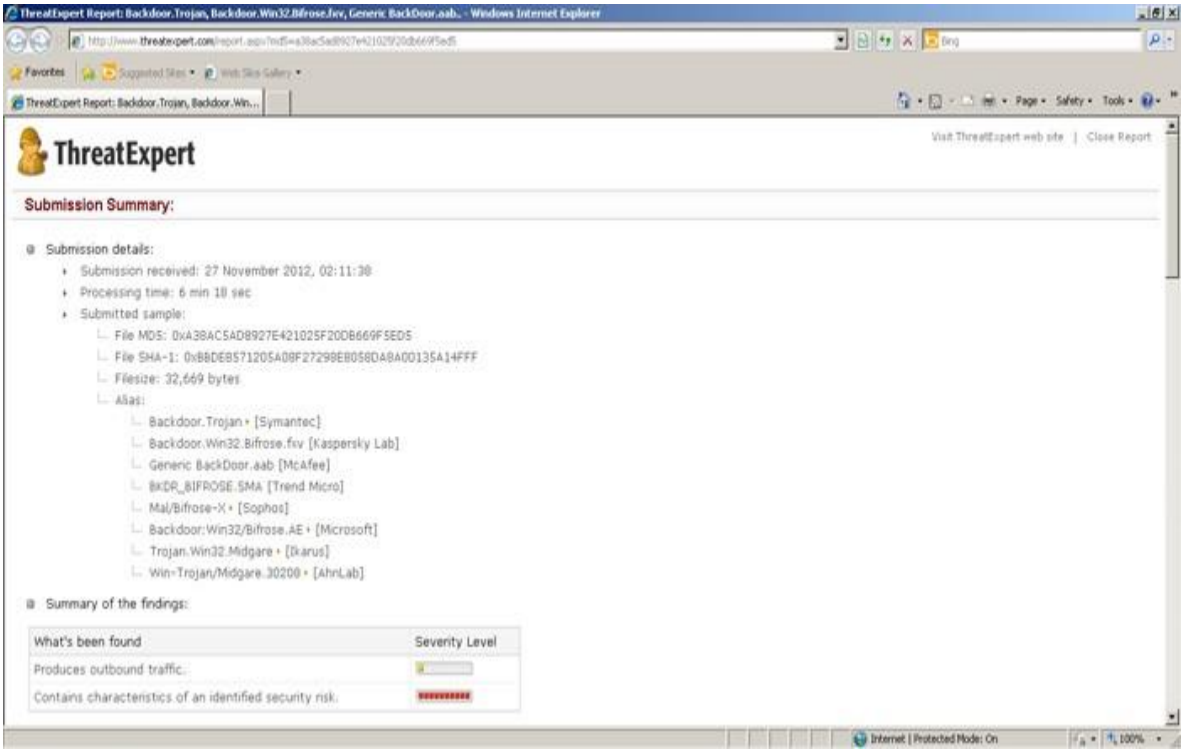
یکی از این ابزارها SandBox است. اما SandBox چیست؟ SandBox یک فناوري و ابزار است که هم توسط متخصصین آنالیز بدافزار و هم توسط آنتی ویروس ها مورد استفاده می گیرد. به طور کلی SandBox یک محیط مجازي و امن است که می توان مورد مشکوك را در آن اجرا و رفتار برنامه را مورد بررسی قرار داد بدون آنکه به سیستم اصلی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

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

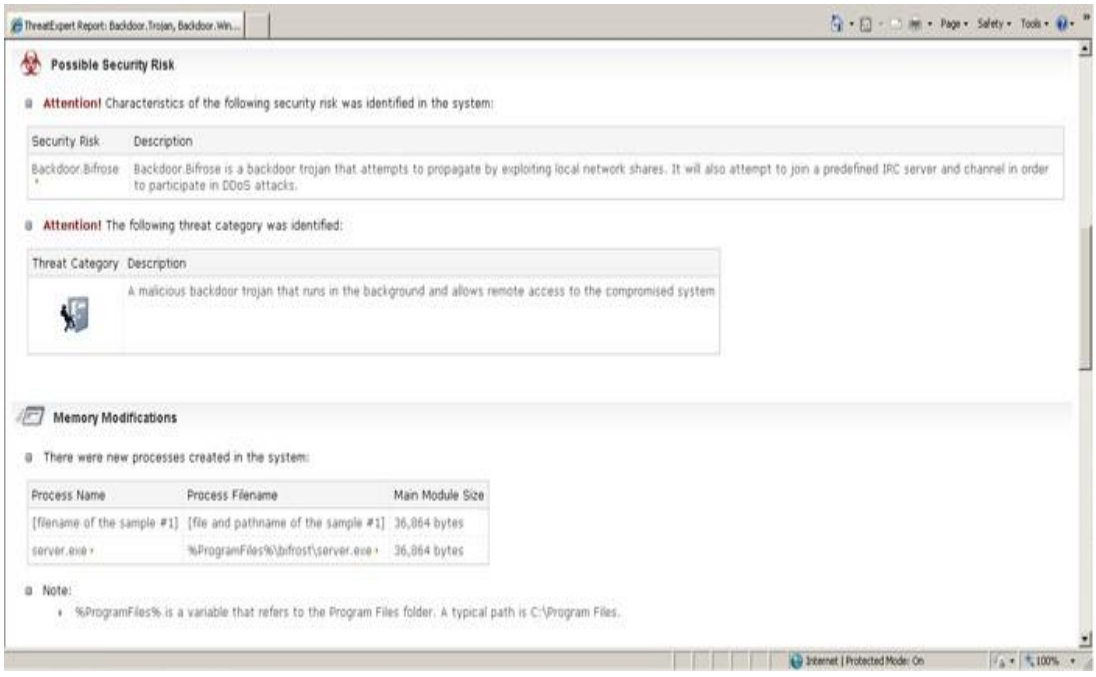
وقتی که یک فایل مشکوك را وارد می کنید پایگاه داده threatexpert بررسی می کند که آیا مورد مشکوك قبلا بررسی شده است یا خیر، اگر جواب مثبت باشد شما می توانید گزارش کامل آن را مطالعه کنید.

در غیر این صورت برنامه مشکوك بر محیط مجازي بررسی می شود و مواردي مانند پروسه هاي ایجاد شده، تغییرات حافظه ،تغییرات کلید هاي رجیستري، محلهایی که برنامه خود را کپی کرده است و کلی از موارد دیگر بررسی گشته و گزارش کاملی را براي 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 رجیستري 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 اي را اجرا می کند که فایل stmp.sys را در فولدر system32\config جایگذاري کرده و می نویسد.

این بدافزار از طریق ثبت ضربات صفحه کلید، رمز کردن آنها و ارسال آن براي نویسنده، اطلاعات را جمع آوري 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 ي 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 بسیاري از بدافزارهاي 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 اعتباري وي و لینک ها به منابع داخلی و خارجی جمع آوري 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

MD5برابر 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 براي مقاصد قانونی ثبت کنند اما این نرم افزار قربانیان خود را با یک payload پنهان گمراه می سازد. به نظر می رسد که تولید کننده این بدافزار با قرار دادن آن در فروم مذکور، قصد حمله به سایر اعضاي این فروم را داشته که این کار تکنیکی مرسوم است.

نویسندگان بدافزارها اغلب براي جلوگیري از شناسایی شدن، از ابزارهاي ارزان و ساده اي استفاده می کنند که بدافزار را با یک برنامه runtime فشرده سازي یا رمزگذاري، تغییر می دهد؛ البته در این مورد خاص، فایل هاي 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 اي را اجرا می کند که فایل stmp.sys را در فولدر system32\config جایگذاري 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 محتوي ضربات صفحه کلید کاربر است که به صورت رمز شده ذخیره شده اند. هربار 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 رمزگذاري مورد استفاده براي این کار ساده است، ولی از رمزگذاري انتخابی با دو تکنیک استفاده می کند: هر بایت درصورتی که فرد باشد با استفاده از تکنیک 1 رمز می شود و درصورتی که زوج باشد، با استفاده از تکنیک 2 رمزگذاري 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 گذاري ضربات صفحه کلید، این بدافزار این اطلاعات را براي نویسنده خود ایمیل می کند.

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

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

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

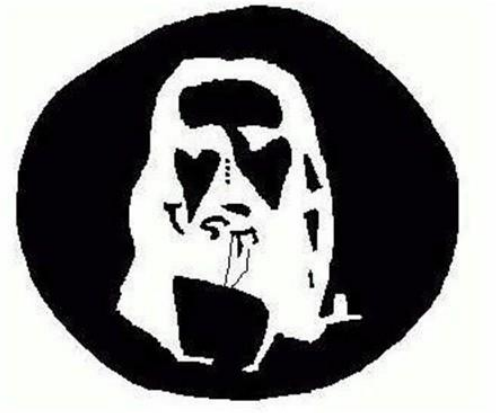
بد افزار Mahdi

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

بدافزار پس از فعال شدن، تصویري را در رابطه با نقشه کشور اسرائیل بر علیه برنامه هسته اي ایران با طراحی نقشه جنگ الکترونیکی که از طریق یکی از سایتهاي خبري منتشر شده است نمایش می دهد.

آن طور که از نقطه نظر تحلیلگران آمده است، بدافزار فوق با استفاده از تکنیکی موسوم بهمهندسی اجتماعیکاربر / قربانی را ملزم به اجراي سند آلوده می نماید. این در حالی است که سند آلوده با نمایش تعدادي عکس و بازي هاي ریاضی گونه ذهن کاربر را بهدستورالعمل هاي ذکر شده در روي تصاویر معطوف و منحرف می نماید.

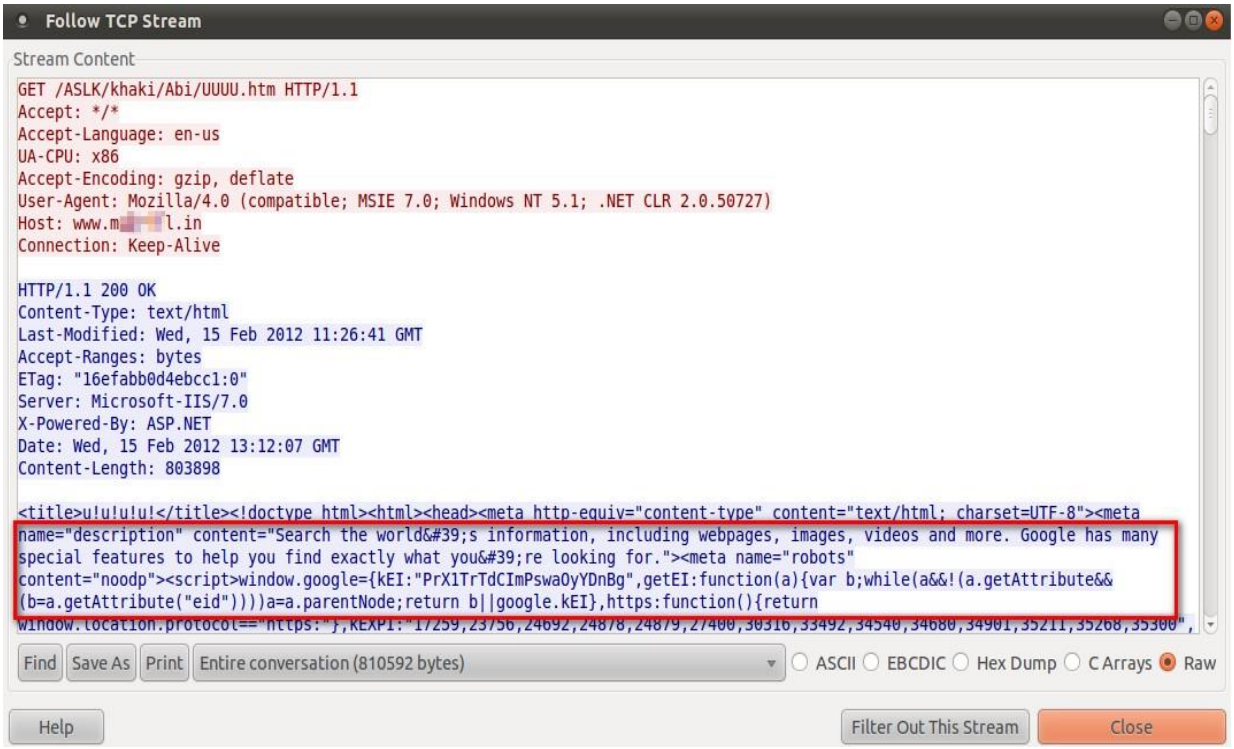
همچنین نکته قابل توجه در مورد برخی از نمونههاي تحلیل شده حاکی از وجود سندهائی در خصوص نمایش عکسی معماگونه ازحضرت علی (ع) بوده که بارها در سایت هاي پارسی زبان نمایش داده شده اند.



این بدافزار در جهت فریفتن کاربر از تکنیکی موسوم به RTLO به منظور تغییر نام هوشمندانه فایل هاي اجرائی به فایل هائی باپسوندpdf، jpg و یا scr و ppt استفاده مینماید. پس از اجرا نمودن این فایل، تعدادي ویدئو و عکس در جهت فریفتن و پنهاننمودن فعالیت اصلی بدافزار اجرا می شود.

بررسی هاي صورت گرفته از سرورهاي C&C بیانگر شواهدي در خصوص منشاء حمله از کشور ایران می باشد.

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



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

مشخصات فنی بدافزار

یکی از مهمترین مشخصه هاي بدافزار فوق این است که براي جلوگيري از کشف توسط سیستم هاي آنتی ویروس، با استفاده از نسخه اي 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 زیادي از فایل ها را در مسیر زیر قرار می دهد.

c:\documents and

settings\\Printhoodفایل هایی نظیر UpdateOffice.exe و OfficeDesktop.exe نیز جز فایلهاي 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 معناي به سرقت بردن کلیه کلمات تایپ شده بر روي کیبورد
- تهیه تصویر از صفحه کاربر قربانی
- بروزرسانی بکدور مربوط به تروجان

- ضبط نمودن صدا با پسوند*wav*.همراه با عمليات ذخيره سازي و آپلود
- نقشه برداري از ساختار پارتيشن و ديسک سخت کليه ماشين هاي آلوده از طريق پروتکل http و با وب سرورهائی با شماره آي پي نظير 57.142.174.* (سه سرور) و 106.205.67.* (يک سرور) ارتباط برقرار می نمايند. همچنين پکتهاي از نوع ICMP به سمت سرورهاي فوق الذکر براي چک کردن وضعيت ارسال می شوند. همچنين بيش از 300 فايل با پسوندهاي PRI، dll و TMP در مسير زير ايجاد می شوند:

C:\documents and settings\%USER%\Printhood

تعدادي مشخصه MD5 از نمونه هاي مرتبط با اين بدافزار شامل ليست زير می باشد:

7b7abab9bc4c49743d001cf99737e383
a9774d6496e1b09ccb1aeaba3353db7b
885fcebf0549bf0c59a697a7cfff39ad
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

حمله نموده و f45963376918ed7dc2b96b16af976966 d6f343e2bd295b69c2ce31f6fe369af9

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 سروري به شماره آي پي 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 فایل ها با شماره 445
- پورت فعال با شماره 44442
- پورت فعال با شماره

49154 **مقابله با**

بدافزار Mahdi

از آنجائی که به دلایل نامشخص، این بدافزار یک بدافزار با قابلیت هاي فنی پائین تر (به نسبت دیگر بدافزارهاي استفاده شده در حوزه جنگ هاي سایبري نظیر استاکس نت، دیوکیو و فلیم) می باشد، لذا استفاده از روش هاي ساده تر به منظور مقابله و پاك سازي ماشین هاي آلوده به این بدافزار کاربردي تر می باشد.

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

C:\Users\%USERPROFILE%\Windows

به منظور پاك سازي لازم است محتویات این پوشه حذف شود.

همچنین، جهت پاك سازي 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 گیري

نخستین قدم لازم در مبارزه با تهدیدات سایبري توسعه روش هاي تشخیص موثر است. پس از تشخیص، قدم مهم بعدي به دست آوردن راه هایی براي از کار انداختن زیر ساخت هاي بخش فرماندهی و کنترل بدافزارهه و مختل کردن آن ها است. رایج ترین روش هاي به کار گرفته شده براي تحقق این کار شامل قطع کانال فرمان و کنترل و جلوگیري از ارسال دستورات از سوي مدیر بات به بات ها هستند که در این پژوهش پیشنهادهاي مختلف ارائه گردید. روش هاي مختلفی براي تشخیص بدافزارها وجود دارد

که بررسی و بحث شد آنچه از منظر نویسندگان و عاملین این بدافزارها طرح است این است که روش هاي فرار نیز در حال توسعه هستند که بدافزارهاي موجود را مخفی کرده و با افزایش سرعت تغییر و از روش هاي مختلف ردیابی آن ها را دشوار می سازند. امروزه بدافزارها براي عملیاتی شدن روي پایگاه هاي جدید شامل گوشی هاي هوشمند، تبلت ها و دیگر وسایل همراه فعال تر شده اند. در این حیطه چالش هاي فراوانی باقی مانده است. در این پژوهش روش هاي تحقیقی جدیدي که قابل توسعه هستند بررسی و ارائه شد اما موضوع مهمی که محققان با آن مواجه هستند دشواري آزمون و ارزیابی روش هاي تشخیص در سناریوهاي واقعی یا در استفاده از داده هاي واقعی است. برخی ابتکار عمل ها مانند ایجاد انبارهاي ردپا، با درصدي 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: Insidethe New Threat Matrix of Digital Espionage, Crime, andWarfare. 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 Cre- ators Tried to Achieve. Technical report, Langner Group, Nov. 2013.

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

[10] Mandiant. APT1: Exposing One of Chinas 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. Effi- cient Detection of Split Personalities in Malware. In Proc. of the Symposium on Network and Distributed SystemSecurity (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. Monrose. 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 Associa- tion.

[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 AnnualNetwork 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 SRITechnical 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 secondgeneration onion router. In Proceedings of the 13th USENIX Security Symposium, Aug. .4002

[42] JAP. Jap anon proxy. http://anon.inf.tu-dresden.de/publications/index_en.html.

[43] R. Albert and A. Baraba ś i. 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-recenttor-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-poweredbotnet-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.