پرونده ویژه

بررسی فنی بدافزار شعله

بدافزارهای رایانه‌ای، یک به یک از راه می‌رسند؛ سیستم‌ها، شبکه‌ها و مجموعه‌های بزرگ، دستخوش اختلال می‌گردند. این اختلالات، در درجات ساده و خوشبینانه، شامل قطع سرویس و ایجاد وقفه در خدمات‌دهی است، و اما در لایه‌های عمیق‌تر و خطرناک‌تر، حاوی تهدیدات امنیتی سنگین و مهلک که گاه قادر است منافع ملی یک کشور را هدف گیرد. پیدایش و جولان پیاپی چند ویروس کامپیوتری در ایران، این زنگ خطر را به صدا درآورد که بدلایل زیرساختی و عدم آمادگی مناسب، چه میزان آسیب‌پذیری در این عرصه در کشورمان دیده می‌شود.

«فلیم» آخرین نوع از این رده بدافزارها بود که با فاصله کمی از اسلاف خود، بروز کرد و موجب جنجال رسانه‌ای فراوانی هم شد. اینگونه که به نظر می‌رسد، تجارب گذشته در این مورد کمی کارساز شد، و به ویژه تلاش مرکز ماهر در این زمینه توانست در جهت مهار موضوع مثمر باشد. سایت «ایتنا» به واسطه دغدغه همیشگی در زمینه امنیت، همواره توجه به این مقوله و اطلاع‌رسانی در این جهت را وجهه همت خود ساخته است. در این مقطع نیز ایتنا توانست پیش و بیش از دیگر رسانه‌ها، نقش یک رسانه تخصصی قابل اعتنا و مستند و در عین حال سریع و آنلاین را ایفا نماید و با انتشار اخبار و ارائه تحلیل‌های به مو.قع صاحبنظران و شرکت‌های فعال این عرصه، تاثیری مثبت در گسترش آگاهی و زمینه‌سازی رفع مشکل داشته باشد.

آنچه در پیش رو دارید، پرونده‌ای است که با توجه به اهمیت موضوع بدافزار فلیم تهیه شده و در آن از مطالب منتشره ایتنا، به همراه یادداشت‌ها و دیگر تحلیل‌های صاحبنظران استفاده شده است.

لابراتوار کسپرسکی و موسسه تحقیقات ITU سلاح های جدید سایبری پیشرفته را معرفی کردند

امیرمحسن عابدینی فر*
amir.abedinifar
@tejarateamn.com

لابراتوار کسپرسکی اخیرا خبر از کشف برنامه‌های مخرب بسیار پیچیده که به طور فعال به عنوان یک سلاح اینترنتی استفاده می شوند داده است و در حال حاضر هدف آنها حمله به موسسات و نهادهای مختلف در چندین کشور است. پیچیدگی و قابلیت‌های این برنامه‌های مخرب که به تازگی کشف شده، بیش از همه تهدیدات سایبری شناخته شده تا به امروز است.

این بدافزارهای مخرب توسط کارشناسان لابراتوار کسپرسکی و در بررسی‌های انجام شده توسط اتحادیه بین‌المللی مخابرات (ITU) کشف شده است. این برنامه‌های مخرب که به عنوان Flame.Worm.Win۳۲ توسط محصولات امنیتی کسپرسکی شناسایی شده، صرفا برای انجام فعالیت های جاسوسی سایبری طراحی شده است. از این جمله می توان سرقت اطلاعات ارزشمند، محتویات صفحه نمایش کامپیوتر، اطلاعات در مورد سیستم هدف قرار گرفته، فایل های ذخیره شده، اطلاعات تماس و حتی مکالمات صوتی اشاره کرد که فقط به اینها محدود نمی‌شود.

این تحقیقات مستقل توسط ITU و لابراتوار کسپرسکی بعد از وقوع یک سری حوادث پی در پی و ناشناخته صورت گرفت که بواسطه برخی بدافزارهای مخرب موسوم به WIPER، اطلاعات بر روی تعدادی از رایانه‌ها در منطقه غرب آسیا حذف شده است. این بدافزارهای مخرب به طور خاص هنوز کشف نشده اند، اما در تجزیه و تحلیل از این حوادث، کارشناسان لابراتوار کسپرسکی در یک اقدام هماهنگ و همکاری فشرده با ITU در این فرآیند، به نوع جدیدی از بدافزارهای مخرب که در حال حاضر به عنوان Flame شناخته شده است دست یافتند. یافته‌های اولیه نشان می‌دهد که این بدافزارهای مخرب "بصورت وحشی" به مدت بیش از دو سال - از ماه مارس ۲۰۱۰ مشغول به فعالیت بوده است. با توجه به پیچیدگی بسیار زیاد آن و به علاوه طبیعت هدف اینگونه حملات، هیچ نرم افزار امنیتی آن را شناسایی نکرده است.

اگر چه ویژگی‌های Flame یا (شعله) در مقایسه با سایر بد افزارهای شناخته شده از گذشته مانند Duqu و Stuxnet متفاوت است، اما جغرافیای حملات اینگونه سلاح‌های سایبری قابل توجه، و استفاده از آسیب پذیری‌های خاص نرم‌افزار، و این واقعیت که کامپیوترهای انتخاب شده بعنوان هدف نشان می دهد که Flame (شعله) متعلق به همان شاخه سلاح‌های فوق العاده سایبری قرار دارد.

در اظهارنظر در مورد کشف شعله (Flame)، یوجین کسپرسکی، مدیر عامل شرکت و از بنیانگذاران لابراتوار کسپرسکی گفت: "خطر

جنگ سایبری در حال حاضر یکی از جدی ترین مباحث در زمینه امنیت اطلاعات برای چندین سال بوده است. Stuxnet و Duqu متعلق به زنجیره ای از حملات هستند، که بعنوان دغدغه‌های مربوط به جنگ سایبر، در سراسر جهان مطرح است. بد افزارهای مخرب Flame به نظر می رسد مرحله دیگری در این جنگ، و برای درک این مهم است که چنین سلاح های سایبری به راحتی می تواند در مقابل هر کشور استفاده شود. بر خلاف متعارف با جنگ، در واقع کشورهای بیشتر توسعه یافته در این موارد آسیب پذیر هستند."

به نظر می رسد هدف اولیه Flame، اقدام به جاسوسی اینترنتی و سرقت اطلاعات از دستگاه‌های آلوده است. چنین اطلاعاتی سپس به شبکه ای از سرورهای "فرمان و کنترل از راه دور" واقع در بسیاری از نقاط مختلف جهان فرستاده شده است. ماهیت متنوع از اطلاعات به سرقت رفته، که می تواند شامل اسناد، تصاویر، ضبط صوتی و رهگیری از ترافیک شبکه باشد، آن را تبدیل به یکی از پیشرفته ترین و کامل ترین ابزار حمله کشف شده تا کنون کرده است. هنوز هم نمیتوان بردار دقیق عفونت و آلودگی را نشان داد، اما در حال حاضر روشن است که شعله توانایی سرایت و تکثیر در بیش از یک شبکه محلی با استفاده از روش‌های مختلف، از جمله همان آسیب پذیری Printer و روش تکثیر آلودگی از طریق USB که توسط Stuxnet مورد سوء استفاده قرار گرفت را دارد.

الکساندر Gostev، کارشناس امنیتی ارشد در لابراتوار کسپرسکی، اظهار داشت: "یافته‌های اولیه از این تحقیق که پس از یک درخواست فوری از ITU انجام شد، تایید ماهیت بسیار هدفمند از این برنامه های مخرب است. یکی از نگران کننده ترین حقایق این است که مبارزات و حملات سایبری Flame در حال حاضر در فاز فعال آن است، و اپراتور آن به طور مداوم اقدام به بررسی سیستم های آلوده، جمع آوری اطلاعات و هدف قرار دادن سیستم های جدید برای به انجام رساندن اهداف ناشناخته آن است."

کارشناسان آزمایشگاه کسپرسکی در حال حاضر مشغول به انجام تجزیه و تحلیل عمیق تر از Flame هستند تا در آینده نزدیک یک سری از اطلاعات تکمیلی با جزئیات بیشتری از تهدیدات جدید شناخته شده را فاش کنند. در حال حاضر آنچه از Flame شناخته شده این است که از ماژول های مختلف تشکیل شده و در کل از چندین مگابایت کد اجرایی ساخته شده است - و آن را حدود ۲۰ برابر بزرگتر از Stuxnet قرار داده است. این به این معنی است که تجزیه و تحلیل این سلاح سایبری نیاز به یک تیم بزرگ از کارشناسان امنیتی در ردیف بالا و مهندسین معکوس با تجربه گسترده در زمینه دفاع سایبری است.

* مدیرمحصول کسپرسکی در شرکت تجارت امن

متن کامل تحلیل فنی سیمانتک از بدافزار flame

شناسایی حمله سایبری هدفمند بدافزار Flamer

پس از انتشار خبرهای حمله سایبری در اوایل اردیبهشت ۹۱ به شبکه وزارت نفت و از بین رفتن اطلاعات هارد دیسک‌های برخی از Serverها و در پی آن قطع شبکه اینترنت شبکه وزارت نفت و برخی شرکت‌های تابعه، گمانه‌زنی‌های مختلفی در خصوص این حمله سایبری میان کارشناسان امنیتی رواج یافت. عدم انتشار هرگونه اطلاعات فنی در خصوص این حمله سایبری و از سوی دیگر عدم مشاهده حمله مشابه در کشورهای دیگر باعث شد که دسترسی به منابع معتبر درجهت شناسایی و تحلیل این حمله برای شرکت‌های امنیتی بسیار سخت باشد.

پس از انتشار اطلاعیه مرکز ماهر در تاریخ ۹۱/۰۳/۰۷ مبنی بر شناسایی عامل حمله سایبری با استفاده از بدافزاری موسوم به Flame ، شرکت‌های امنیتی مختلف نتایج تحلیل‌های اولیه خود را درخصوص این حمله منتشر کردند.

شماری از قابلیت‌های مهم این بدافزار عبارتند از:

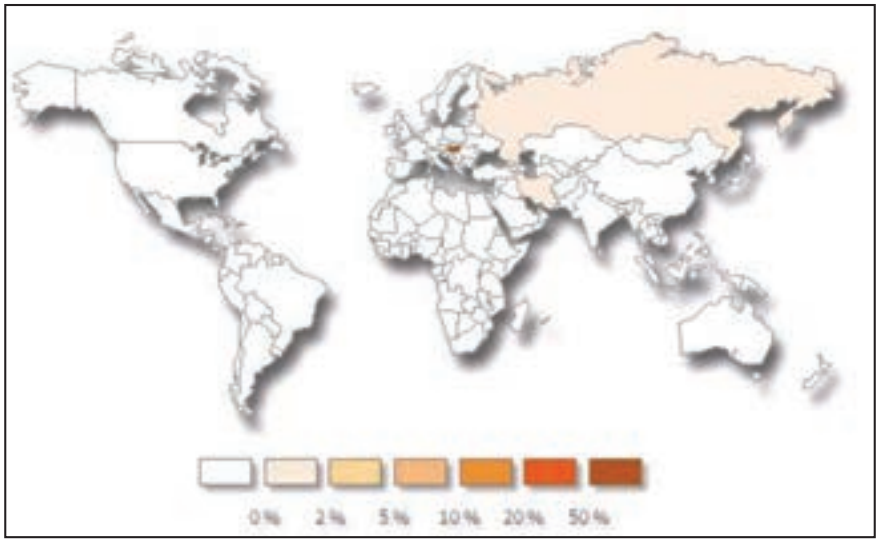
- انتشار از طریق حافظه‌های فلش
- انتشار در سطح شبکه
- پویش شبکه و جمع‌آوری و ثبت اطلاعات منابع شبکه و رمز عبور سیستم‌های مختلف
- پویش دیسک کامپیوتر آلوده و جست‌وجو برای فایل‌هایی با پسوندها و محتوای مشخص
- تهیه تصویر از فعالیت‌های خاص کاربر سیستم آلوده با ذخیره سازی تصاویر نمایش داده شده بر روی مانیتور کاربر
- ذخیره‌سازی صوت دریافتی از طریق میکروفن سیستم در صورت وجود
- ارسال اطلاعات ذخیره شده به سرورهای کنترل خارج از کشور
- دارا بودن بیش از ۱۰ دامنه مورد استفاده به عنوان سرور C&C
- برقراری ارتباط امن با سرورهای C&C از طریق پروتکل‌های SSH و HTTPS
- شناسایی و از کار انداختن بیش از ۱۰۰ نرم‌افزار آنتی‌ویروس، ضد بدافزار، فایروال و...
- قابلیت آلوده‌سازی سیستم‌های ویندوز XP، ویستا و ویندوز ۷
- قابلیت آلوده‌سازی سیستم‌های یک شبکه در مقیاس بالا

مرکز ماهر اعلام کرده که "این احتمال وجود دارد که حمله سایبری اوایل اردیبهشت ماه به شبکه وزارت نفت و تخریب اطلاعات سیستم‌ها توسط یکی از اجزای این بدافزار صورت گرفته باشد." تحلیل شرکت سیمانتک که در ادامه خواهد آمد این احتمال را تایید می‌کند. و با توجه به ماهیت عملکرد این بدافزار، می‌توان آن را محصولی از خانواده استاکس نت و دیوکیو دانست.

شرکت سیمانتک در خصوص این بدافزار اطلاعاتی را به این شرح منتشر کرده است:

این بدافزار که با نام‌های W32.Flamer

دامنه انتشار ویروس Flamer بر اساس ردیابی‌های فعلی در شکل زیر آمده است:



در شکل زیر اجزای شناخته شده این ویروس آمده است. توجه داشته باشید در برخی حملات این ویروس ممکن است نام فایل‌ها تغییر کند:

ویا Skywiper شناخته می شود ۲۰ برابر ویروس Stuxnet حجم دارد و مطالعات نشان می‌دهد که احتمالا در سال ۲۰۱۰ تولید شده است. تحلیل کدهای Flamer نشان می‌دهد که این بدافزار به طرز بسیار ماهرانه‌ای تولید شده و کدهای به کار رفته در آن درظاهر شبیه کدهای معمولی نرم‌افزارهای دیگر است اما درحقیقت قابلیت‌های هوشمندانه و مخرب و پنهانی در آن کدها قرار داده شده است. پیچیدگی به کار رفته در کدهای مخرب این بدافزار باعث شده که به همراه ویروس‌های Stuxnet و Duqu به عنوان پیچیده‌ترین ویروس‌های شناخته شده تاکنون به شمار برود. این بدافزار نیز همانند دو نمونه قبلی احتمالا نه توسط یک فرد بلکه توسط یک گروه با حمایت مالی قوی و برای اهداف خاصی ساخته شده است. فایل‌هایی که توسط این ویروس برای حمله به کار گرفته می‌شوند مشابه فایل‌هایی است که در حملات سایبری اخیر به وزارت نفت ایران نقش داشته‌اند.

تحلیل سیمانتک بر روی این بدافزار ادامه دارد اما نتایج بدست آمده نشان می‌دهد که هدف این ویروس جمع‌آوری اطلاعات و داده‌هاست. ردیابی‌های اولیه نشان می‌دهد که انتشار این ویروس در شرق اروپا و خاورمیانه بوده است.

بر اساس بررسی‌های سیمانتک ، اجزای بکار رفته در این ویروس که از این پس سیماتک آن را با نام W32.Flamer می‌شناسد حکایت از این دارد که اولین بار ویروس W32.Flamer در سال ۲۰۱۰ بوجود آمده است. اجزای شناخته شده این ویروس عبارتند از:

- advnetcfg.ocx
- ccalc32.sys
- mssecmgr.sys
- msglu32.ocx
- boot32drv.sys
- nteps32.ocx

دو نسخه مختلف از فایل advnetcfg.ocx کشف شده است. نوع اول برمی گردد به سپتامبر ۲۰۱۰ و نوع دوم در فوریه ۲۰۱۱. فایل پیکربندی ccalc32.sys نیز دارای دو نوع است که هر دو تقریبا در همان حاشیه زمانی فایل advnetcfg.ocx کشف شده است.

بر اساس آمار تعداد کامپیوترهایی که مورد حمله ویروس Flamer قرار گرفته‌اند هدف اصلی این تهدید کشورهای فلسطین، مجارستان، ایران، و لبنان بوده است. با این حال، سیمانتک گزارش‌هایی از این حمله در کشورهای اتریش، روسیه، هنگ کنگ و امارات متحده عربی نیز دریافت کرده است که احتمال می رود موارد گزارش شده شامل Laptopهایی باشند که از کشورهای آلوده شده اصلی به این کشورها آورده شده‌اند. نکته قابل توجه این است که علاوه بر شبکه‌های سازمان‌ها و ارگان‌های دولتی و صنعتی، سیستم‌های کاربران خانگی نیز به ویروس Flamer آلوده شده است.

تحلیل فنی ویروس Flamer:

تعدادی از اجزای این تهدید کشف شده است و در حال حاضر در حال تجزیه و تحلیل بر روی آنها ادامه دارد. اجزای کشف شده این ویروس بگونه ای نوشته شده اند که در نگاه اول به نظر نمی‌رسد حاوی کدهای مخرب باشند. اما تحلیل‌های دقیق‌تر نشان از مخرب بودن آنها دارد. کدهای این ویروس بسیار پیچیده است و همین امر مانع تجزیه و تحلیل آن می‌شود. از جمله قابلیت‌های کلی شناخته شده این ویروس می‌توان به توانایی سرقت اسناد، گرفتن تصاویری از دسکتاپ کاربران و انتشار از طریق Cooldisk اشاره کرد. این بدافزار همچنین قادر است برخی از نرم‌افزارهای امنیتی نصب شده روی سیستم کاربر را غیرفعال کند. همچنین این ویروس تحت شرایط خاصی می‌تواند از نقاط آسیب‌پذیری Windows استفاده کرده و خود را در سطح شبکه منتشر کند.

نحوه عملیات به این صورت است که ابتدا فایل advnetcfg.ocx در حافظه Load می شود. سپس به کمک آن یک فایل رمز شده با نام ccalc32.sys رمزگشایی می شود. فایل ccalc32.sys یک فایل رمزشده با روش RC4-encrypted و با یک کلید ۱۲۸ بیتی است. بدافزار بعد از ایجاد فایل ccalc32.sys به سراغ فایل kernel32.dll می رود و آنرا آلوده می سازد. فایل Kernel32.dll از جمله فایل‌های سیستمی Windows است. Windows تلاش می‌کند ایجاد تغییر در این فایل سیستمی را به User اعلام کند. فایل advenetcfg.ocx فرمان‌های صادر شده از یک جزء دیگر بدافزار را که هنوز تحلیل روی آن ادامه دارد و ناشناخته است به اجرا درمی‌آورد.

فایل advnetcfg.ocx با استفاده از روش‌های پیچیده خود را به winlogon.exe ، پروسس‌های نرم‌افزارهای امنیتی و یا پروسس‌های دیگر تزریق می‌کند، علاوه بر این، ممکن است فایل shell32.dll که از فایل‌های سیستمی ویندوز است نیز با نسخه آلوده شده ای جایگزین گردد. فایل advnetcfg.ocx قابلیت ضبط تصاویر نیز را نیز داراست.

این فایل همزمان دارای یک مترجم (LUA Interpreter)، کد SSH و قابلیت‌های SQL است. پیاده‌سازی و

mssecmgr.ocx . فایلی بزرگ و با قابلیت‌های پیچیده زیادی است که در شکل زیر آمده است:

نکته قابل توجه دیگر این است که درون کدهای این بدافزار بطور متعدد از واژه ‹FLAME› استفاده شده است که می‌تواند معنی خاصی داشته باشد.

استفاده از یک مترجم LUA باعث شده این ویروس بسیار قابل انعطاف و قابل تنظیم باشد. این به مهاجمان اجازه می‌دهد از راه دور بتوانند فرمان‌های متنوع خود را خیلی سریع و راحت به اجرا درآورند و حتی ماهیت عملکرد ویروس را تغییر دهند. اثر این فایل ممکن است در رجیستری ویندوز در آدرس زیر دیده شود:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\»Authentication Packages«= »mssecmgr.ocx«

چندین ماژول اضافی دیگر نیز در .mssecmgr ocx وجود دارد که در شکل آمده است. یکی از اجزایی که توسط فایل .mssecmgr ocx میتواند مورد فراخوانی قرارگیرد فایلی است بنام ~DEB93D.tmp. این فایل منشأ ویروس Wiper است که در اوایل اردیبهشت ماه به شبکه وزارت نفت ایران آسیب وارد کرد و باعث قطع چند روزه شبکه پایانه‌های نفتی ایران از اینترنت گردید.

بدلیل عملکرد این ویروس و حذف اطلاعات هارد دیسک سیستم‌ها، این ویروس بنام Wiper نامگذاری گردید. فایل nteps32.ocx مسئول ضبط تصاویر در این بدافزار است. این فایل به منظور ضبط تصاویر، اطلاعات تنظیمات خود را از فایلی بنام boot32drv.sys دریافت می‌کند.

در این فایل تعیین می‌شود که چه تصاویری و با چه تنظیماتی ضبط شود و چگونه ارسال گردد. این فایل نیز با کدینگ ۰xFF کد شده است.

فایل msglu32.sys حاوی کد است که سرقت اطلاعات را انجام می‌دهد. این فایل، وظیفه شناسایی و سرقت انواع فایل‌ها نظیر انواع اسناد، تصاویر، داده‌های GPS، فایل‌های پروژه و نقشه‌های فنی را بر عهده دارد.

این فایل همچنین دارای قابلیت‌های SQL است. جالب توجه است، این ماژول شامل عبارت‌های متعددی از واژه ‘JIMMY’ است. (مانند: ‘Jimmy Notice: failed to convert error string to unicode’)

طبیعت ماژولار این تروجان نشان می‌دهد که یکی از اهداف گروه طراحان آن، استفاده بلندمدت از این بدافزار برای طراحی حملات خود بوده است.

معماری بکار رفته در W32.Flamer اجازه می‌دهد تا طراحان بدون نیاز به دوباره کاری بتوانند عملکرد و رفتار ویروس را به دلخواه خود تغییر دهند و یا ماژول‌های جدیدی به آن اضافه کنند.

می‌توانند آن را ارتقا دهند و یا به منظور فرار از نرم‌افزارهای امنیتی تغییر شکل دهند.

سیمانتک درحال بررسی و تحلیل لایه‌های عمیق بکار رفته در این ویروس بوده و به زودی نتایج بررسی‌های خود را منتشر خواهد کرد.

تهیه شده در شرکت آینده‌نگاران (آیکو)

گزارش ویژه:

متن کامل گزارش مکافی از بدافزار flame

بر اساس گزارش مرکز تحقیقات McAfee Labs، عملیات متنوع و پیچیده این بدافزار - که شرکت McAfee آن را SkyWiper می‌نامد - از طریق چندین مرکز کنترل و فرماندهی (Command and Control – C&C) مدیریت و هدایت می‌شود. احتمال داده می‌شود که تعداد این مراکز فرماندهی بیش از ۱۰ مرکز باشد.

برای بررسی دقیق عملکرد ویروس‌های Stuxnet و Duqu ماه‌ها وقت صرف شد ولی در نگاه اول، پیش‌بینی می‌شود که بررسی و کسب اطلاعات دقیق درباره ویروس SkyWiper بسیار دشوارتر بوده و زمان بیشتری نیاز داشته باشد.

برای نمونه، یکی از بخش‌های کوچک و رمزگذاری شده بدافزار SkyWiper حاوی بیش از ۷۰ هزار سطر برنامه‌نویسی به زبان C است که شامل بیش از ۱۷۰ عبارت(string) رمزگذاری شده می‌باشد. به نظر می‌رسد که این بدافزار طی چندین سال توسط یک گروه برنامه‌نویسی حرفه‌ای طراحی و تهیه شده است.

اکنون با بررسی گزارش‌های برخی شرکت‌های امنیتی و فایل‌های Log منتشر شده در تالارهای گفت‌وگو (Forums)، علائمی از فعالیت این بدافزار در سال‌های گذشته(حدود سال ۲۰۱۰ میلادی) در ایران و چند کشور اروپایی مشاهده شده است.

بر خلاف ویروس‌های رایج امروزی، این بدافزار به کندی از طریق حافظه‌های USB Flash انتشار می‌یابد تا جلب توجه نکرده و به عنوان یک رفتار مخرب توسط ابزارهای امنیتی شناسایی نشود.

برخی از فایل‌های مرتبط با ویروس SkyWiper در ظاهر متعلق به شرکت مایکروسافت می‌باشد. بعنوان مثال، یک فایل در ظاهر Windows Authentication Client نسخه ۵.۱ و شماره ساخت (Build) ۲۶۰۰ و متعلق به Microsoft Corporation است. ولی بررسی دقیق‌تر نشان می‌دهد که مانند ویروس‌های Stuxnet و Duqu هیچیک از فایل‌های بدافزار SkyWiper دارای Authentication Key معتبر نیستند.

مرکز کنترل و فرماندهی SkyWiper قادر است، نام و پسوند فایل‌های مخرب و مرتبط با این بدافزار را تغییر دهد. حتی تنظیمات مورد استفاده این فایل ها هم قابل تغییر هستند. بدین نحو، بدافزار SkyWiper می‌تواند خود را از دید ابزارهای امنیتی و از جمله ضدویروس‌ها مخفی نگهدارد.

بر اساس اطلاعات جمع‌آوری شده توسط McAfee Labs که در نقشه زیر نمایش داده شده است، بخش عمده آلودگی به بدافزار SkyWiper مربوط به ایران بوده و چند مورد پراکنده نیز در آمریکا مشاهده شده است.

در حال حاضر به غیر از برخی شباهت‌ها در نحوه رمزگذاری فایل‌ها، نقطه مشترکی بین SkyWiper و ویروس‌های Stuxnet و Duqu مشاهده نشده است. تنها پیچیدگی این بدافزارها و محل فعالیت عمده آنها که کشور ایران است، باعث به وجود آمدن این فرضیه و احتمال شده که حداقل این سه ویروس، پروژه‌های مشابهی بوده‌اند که در سال‌های گذشته به طور موازی اجرا شده‌اند.

اندازه برنامه اصلی SkyWiper بیش از ۶ مگابایت است و مجموعه کامل برنامه‌های این بدافزار حدود ۲۰ مگابایت فضا اشغال می‌کنند. این حجم زیاد برای این بدافزار کمی تعجب‌آور است.

کاربران با تجربه می‌دانند که ویروس‌نویسان برای انتشار راحت‌تر فایل‌های مخرب، اندازه فایل‌ها را کم نگه می‌دارند. اما ساختار پیچیده این بدافزار نیاز به کتابخانه‌های پیچیده‌ای همچون Zlib، مفسر LUA و ... دارد که باعث ایجاد این حجم زیاد می‌شود.

آخرین تغییرات در فایل‌های بدافزار SkyWiper مربوط به بیش از یکسال گذشته (حدود زمستان ۸۹ و تابستان ۹۰) می‌شود. گر چه در برخی فایل‌ها به طور دستی، تاریخ ها از ۲۰۱۱ به ۱۹۹۴ تغییر داده شده‌اند.

بر اساس اطلاعات جمع‌آوری شده توسط McAfee Labs که در نقشه زیر نمایش داده شده است، بخش عمده آلودگی به بدافزار SkyWiper مربوط به ایران بوده و چند مورد پراکنده نیز در آمریکا مشاهده شده است.

در حملات SkyWiper مشاهده شده که برای مخفی ساختن حملات اصلی و جلوگیری از جلب توجه، در ابتدا برخی آلودگی‌ها در نقاط دیگر به غیر از اهداف اصلی ایجاد می‌گردد. در مراحل بعدی، SkyWiper از این نقاط آلوده به عنوان مرکز کنترل و فرماندهی استفاده می‌کنند.

یقیناً در بررسی و تحقیقات بعدی، توجه به این نکته بسیار ضروری است.

ضدویروس McAfee با آخرین فایل‌های به‌روزرسانی DAT، قادر به شناسایی بدافزار SkyWiper می‌باشد. اطلاعات و مشاهدات فعلی نشان می‌دهد که چندین گونه مختلف در این بدافزار وجود دارد.

اطلاعات فنی

این بدافزار که توسط ضدویروس McAfee با نام SkyWiper شناسایی می‌شود، قادر به انجام عملیات مخرب زیر می باشد:

- بررسی منابع شبکه
- سرقت اطلاعات
- تماس با مراکز فرماندهی خود از طریق پودمانهای SSH و HTTPS
- قابلیت تشخیص بیش از ۱۰۰ محصول امنیتی (ضدویروس، برنامه‌های ضدجاسوسی، دیواره آتش و غیره)
- اجرا شدن در سطح هسته و در سطح برنامه
- اجرا به همراه پروسه Winlogon.exe و تزریق خود به پروسه explorer.exe و ثبت خود بعنوان یک سرویس
- اضافه کردن علامت ~ در ابتدای نام فایل‌های خود برای مخفی ساختن حضور خود
- توانایی حمله به سیستم‌ها از طریق حافظه‌های USB و شبکه‌های محلی
- تصویربرداری از فعالیت‌های کاربر
- شنود و ضبط تماس‌های صوتی برقرار شده از طریق سیستم آلوده
- قابلیت‌های اجرا بر روی سیستم‌های عامل Win ۷و XP، Vista
- سوءاستفاده از ضعف‌های امنیتی سیستم عامل همچون Print Spooler و فایل‌های lnk
- استفاده از بانک داده SQLite برای ذخیره اطلاعات جمع‌آوری شده
- قابلیت توسعه و به روز شدن امکانات جدید
- استفاده از منابع PE رمز شده

فایل‌های اصلی بدافزار SkyWiper عبارتند از:

Windows\System32\mssecmgr.ocx
Windows\System32\msglu32.ocx
Windows\System32\nteps32.ocx
Windows\System32\advnetcfg.ocx
Windows\System32\soapr32.ocx

این بدافزار فایل‌های زیر را نیز ایجاد می‌کند:

~dra52.tmp
target.lnk
zff042
urpd.ocx
ccalc32.sys
boot32drv.sys
Pcldrvx.ocx
~KWI
guninst32
~HLV
~DEB93D.tmp
~DEB83C.tmp
~dra53.tmp
cmutlcfg.ocx
~DFL983.tmp
~DF05AC8.tmp
~DFD85D3.tmp
~a29.tmp
dsmgr.ocx
~f28.tmp
~dra51k.tmp
~d43a37b.tmp
~dfc855.tmp
Ef_trace.log
contents.btr
wrm3f0
scrcons.exe
wmiprvse.exe
wlndh32
mprhlp
kbdinai
~ZLM0D1.ocx
~ZLM0D2.ocx
sstab
~rcf0
~rcj0

با توجه به اینکه احتمالاً این بدافزار دارای گونه‌های متعددی می‌باشد، توصیه می‌شود که Access فایل‌های ذکر شده فوق، در بخش McAfee ضدویروس Protection مسدود شوند VirusScan.

همچنین با توجه به اهمیت موضوع ممکن است نیاز به استفاده از فایل‌های موقت شناسایی باشد که در این صورت (Extra DAT) هشدارهای لازم به مشترکین ارسال خواهد گردید.

توصیه می‌شود مدیران شبکه، موارد پیشگیری کننده، نظیر نصب آخرین اصلاحیه‌های سیستم عامل و مسدود ساختن حافظه USB از طریق ابزارهایی همچون McAfee Device Control را نیز در نظر داشته باشند.

چیزهایی که درباره «فلیم» نمی‌دانیم!

و اینکه چرا این ویروس رایانه‌ای نمی‌تواند تا این حد بزرگ و ترسناک باشد ...

درست مانند استاکس نت، حالا ویروس «فلیم» هم رنگ و بوی تند سیاسی به خود گرفته و تا حد غیرقابل باوری بزرگ و ترسناک شده است. چرا؟ آیا به‌راستی «فلیم» خطرناک‌ترین و ترس‌آورترین سلاح سایبری کشف شده در سرتاسر تاریخ امنیت فناوری اطلاعات است؟ پاسخ ما مطلقاً منفی‌ست ...

دلیل ما البته وجود هزاران و یا صدها هزار رایانه‌ای‌ست که در سطح کشور با وجود نفوذ و انتشار این کرم رایانه‌ای آلوده نشده‌اند و با اختلالات شدید دست و پنجه نرم نکرده‌اند.

حتی اگر حملات «فلیم» را هدف‌دار بدانیم، باز هم فقط شبکه‌هایی خاص دارای یک یا چند نوع مشخص از نرم‌افزارهای ضدویروس، با آلودگی و اختلال مواجه شده‌اند و بسیاری از مراکز سازمانی کشور (متصل به شبکه دولت و یا شبکه اصلی وزارت نفت) که ازانواع دیگری از برنامه‌های ضدویروس استفاده می‌کرده‌اند، دچار مشکلات امنیتی و اختلال عملیاتی نشده‌اند.

بدون شک «فلیم»یک بدافزار خطرناک و پیچیده است که ویژگی‌های منحصر به‌فردی دارد، اما هیچ دلیل فنی و تخصصی وجود ندارد که آن را بزرگ‌ترین و پیچیده‌ترین سلاح سایبری تاریخ بخوانیم. فلیم تنها یک کیت سرهم‌بندی شده و یا یک مجموعه ابزار تخریبی‌ست که می‌تواند به بهترین وجه، بستر مناسب را برای هر نوع فعالیت جاسوسی، سرقت اطلاعات و یا تخریب داده‌ها فراهم کند. روی این بستر مناسب می‌توان هر نوع بدافزار دلخواه را قرار داد و آن را از دوردست کنترل کرد.

اما با این حال، «فلیم» یک بدافزار اینترنتی مانند بسیاری دیگر از انواع بدافزارهای هدف‌دار است...یعنی برای ورود و انجام تخریب به یک راه نفوذ، سیستم عامل مناسب، سطح دسترسی بالا برای انتشار، دسترسی به اینترنت یا شبکه، دسترسی به اطلاعات ارزشمند و حساس، دسترسی به رایانه‌های هدف و ... نیاز دارد. انسداد، اختلال و یا عدم دسترس‌پذیری هر

فرمان خودکشی بدافزار فلیم صادر شد

مطابق گزارش شرکت امنیتی سیمانتک، طراحان بدافزار Flamer در روزهای اخیر از طریق تعدادی از Serverهای کنترل کننده این ویروس (C&C Servers) فرمان‌های جدیدی را برای سیستم‌های آلوده شده ارسال کرده‌اند. این فرمان‌ها در واقع دستور خودکشی به بدافزار Flamer است و باعث می‌شود که این بدافزار خودش را از روی سیستم‌های آلوده Uninstall کند! ویروس Flamer قابلیت ارتباط با تعداد زیادی Server کنترل کننده را دارا بوده است. پس از شناسایی ویروس، طراحان آن بسیاری از این Domainها و Serverها را غیرفعال کرده‌اند. اما تعداد اندکی از C&C Serverها همچنان برای برقراری ارتباط با بخش خاصی از سیستم‌های آلوده فعال هستند تا مهاجمان اجازه داشته باشند C&C Serverهای جدید و ناشناخته‌ای را برای پروژه خود تعریف کنند و به عملیات سایبری خود به روش‌های دیگری ادامه دهند. سیستم‌های آلوده شده طبق تنظیمات از قبل تعریف شده‌ای با C&C Serverها ارتباط برقرار می‌کنند تا فرمان‌های جدید مهاجمان را دریافت کنند. پس از برقراری ارتباط، C&C Server یک فایل بانام browse۳۲.ocx برای کامپیوتر قربانی ارسال می‌کند. این فایل شامل فرمان‌های جدیدی است

کدام از موارد فوق می‌تواند این ویروس به ظاهر پیچیده را زمین‌گیر کند.

شاید تا به حال این سئوال را از خود نکرده باشیم که ویروس «فلیم»، چه نوع اطلاعاتی را می‌تواند سرقت کند که بقیه ویروس‌های سارق اطلاعات نمی‌توانند. آیا این بدافزار می‌تواند برعکس ویروس‌های دیگر بی‌نیاز از یک راه نفوذ به درون شبکه‌های رایانه‌ای باشد و به اطلاعاتی دست پیدا کند که به طور کامل غیرقابل دسترس هستند؟

واقعیت این است که "فلیم" در نهایت می‌تواند به اطلاعاتی دست پیدا کند که در رایانه‌های متصل به اینترنت یا شبکه‌های محلی موجود و قابل دسترس باشند؛ یعنی اطلاعات نه چندان حساس و نه چندان محرمانه.

جالب اینکه تمام فعالیت‌های تخریبی "فلیم" توسط سایر بدافزارهای رایانه‌ای نیز قابل اجراست، با این تفاوت که "فلیم" یک بدافزار ترکیبی و هدف‌دار است که تعداد بی‌شمار قابلیت مخرب را در خود جای داده و می تواند به دقت از دوردست کنترل و مدیریت شود که همین قابلیت اخیر نیز در بسیاری از انواع دیگر کدهای مخرب وجود داشته و در دنیای امنیت اطلاعات تازگی چندانی ندارد.

از این نگاه، هیاهوی رسانه‌ای و جنجال آفرینی سیاسی توسط برخی از شرکت‌های ضدویروس که ادعا می‌کنند برای نخستین بار ویروس فلیم را کشف کرده‌اند، بی‌مورد، بی‌اساس و تنها در حد یک حربه تبلیغاتی و تجاری محسوب می‌شود.

فراموش نکنیم، هر کدام از شرکت‌های تولید کننده ضدویروس، تنها می‌تواند رایانه‌های موجود در قلمرو حفاظتی و عملیاتی خودش را از لحاظ امنیتی بررسی کند و نمی تواند نظرات و تحلیل‌های فنی خود را به تمام رایانه‌ها و شبکه‌های موجود در جهان و یا حتی یک کشور خاص تعمیم دهد.

برای مثال اگر شرکت کسپرسکی از آلودگی ۶۰۰ هدف مختلف خاورمیانه به ویروس "فلیم" خبر می‌دهد، بدان معناست که نزدیک به ۶۰۰ سازمان مجهز به ضدویروس کسپرسکی، با حملات موفق این بدافزار مواجه شده‌اند و "فلیم" توانسته از سد امنیتی ضدویروس و لایه‌های حفاظتی این مراکز عبور کند.

اتفاقاً کشف ویروس "فلیم" پس از حملات پی در پی و موفقیت‌آمیز آن و گذشت بیش از یک ماه از ایجاد اختلال‌های شدید، نشان می‌دهد که در ابتدا یک ضعف و آسیب‌پذیری طولانی مدت در نرم‌افزار ضدویروس وجود داشته که پس از بروز مشکلات امنیتی و خسارت‌های هنگفت مورد توجه واقع شده و نسبت به رفع آن اقدام شده‌است.

از طرف دیگر جست‌وجوی نمونه ویروس در رایانه‌های آلوده مدت‌ها طول کشیده و تحلیل آن آگاهی دیرهنگامی را از فعالیت‌های این ویروس بدست داده است.

این در حالیست که بسیاری از ضدویروس‌ها، به سادگی و با استفاده از سیستم‌های بازدارنده و فناوری‌های پیشرفته خود، حتی با وجود ناشناس بودن ویروس فلیم، موفق شده‌اند تا از حملات آن پیشگیری کنند و گزارش خاصی نیز از آلودگی به این بدافزار منتشر نکرده‌اند. زیرا در این صورت، کار اصلی انجام شده ... حمله رایانه‌ای خطرناک به صورت خودکار خنثی شده؛ سازمان یا رایانه هدف امن مانده و بنابراین حساسیت خاصی هم برانگیخته نشده تا احساس ضرورت به واشکافی و یا تحلیل بدافزار مهاجم انجام شود.

بر اساس اعلام شرکت امنیتی پاندا ویروس "فلیم" به‌راحتی و به سادگی قابل شناسایی، کشف و یا دست کم پیش شناسایی بوده است. حجم عظیم بیست مگابایتی این ویروس و قابلیت‌های خطرناک تخریبی آن می‌تواند مؤید این مسئله باشد.

به هر حال اکنون که ویروس "فلیم" به اذعان برخی شرکت‌های امنیتی از دو سال پیش تاکنون فعال بوده، پاسخ به این سئوالات ضرورت پیدا می‌کند: اول اینکه چه نوع اطلاعاتی از سیستم‌های مجهز به ضدویروس های آسیب پذیر از کشور خارج شده است؟

آیا تمام مکاتبات، اطلاعات و داده‌های حساس سازمانی در این دو سال، براحتی در اختیار منتشر کنندگان ویروس "فلیم" قرار می‌گرفته است؟ چرا ناگهان و در یک روز خاص دست‌کم سه شرکت امنیتی از شرق و غرب جهان با ترتیب دادن کنفرانس‌های خبری (البته با حضور رسانه‌های بزرگ "سیاسی")، ویروس فلیم را در سطح جهان مطرح می‌کنند و برای آن قابلیت‌های استراتژیک ضدامنیتی علیه کشوری خاص فرض می کنند؟

چرا ویروسی که "به سادگی و راحتی" می‌توانسته تحت کنترل و مدیریت باشد، روزها و ماه‌ها به فعالیت آزادانه مشغول بوده است؟

آیا درست به فاصله چند ساعت پس از کشف این ویروس توسط یک مرکز امنیت سایبر در کشور (ماهر)، شرکت‌هایی از روسیه و امریکا تصمیم گرفته‌اند تا مسئله انتشار این ویروس را رسانه‌ای و جهانی کنند؟ چرا در مدت زمانی که سازمان‌های آلوده به فلیم یا وایپر با اختلال شدید عملیاتی مواجه بوده‌اند، این شرکت‌ها هیچ واکنشی نداشته‌اند؟

البته امیدواریم شرکت‌های امنیتی خارجی که ادعای کشف اولیه "فلیم" را داشته‌اند بتوانند پاسخ‌گوی این سئوالات مهم باشند. بله ... زحمات بسیاری از شرکت‌های امنیتی که به بررسی، تحلیل و اطلاع‌رسانی درباره تهدیدهای امنیتی می‌پردازند، ستودنی و قابل تقدیر است، اما به این شرط که با بزرگ‌نمایی بیش از حد تهدیدها و کشاندن موضوع به رسانه‌های "سیاسی" جهان و جنجال آفرینی امنیتی در جست‌وجوی نام و افزایش سهم تجاری خود نباشند.

تهیه شده در شرکت پاندا

که ویروس باید آن را به اجرا درآورد. یکی از فرمان‌هایی که اخیرا ارسال شده است فرمان خودکشی ویروس(Uninstaller Command) است. ویروس برای خودکشی خود لیستی طولانی از فایل‌ها و Folderهای مختلف را حذف می‌کند و سپس با استفاده از کاراکترهای تصادفی آنها را(OverWrite) رونویسی می‌کند تا فایل‌های متعلق به ویروس به هیچ وجه و با هیچ ابزاری قابل بازیابی نباشند. لیست فایل‌ها و Folderهایی که توسط ماژول خودکشی ویروس Flamer حذف می‌شوند به این شرح است:

تمام سیستم‌های آلوده‌ای که فرمان خودکشی را دریافت کرده‌اند ویروس Flamer از روی آنها بطور کامل حذف شده است و دیگر هیچ اثری از آن دیده نمی‌شود.

همانگونه که پیش‌تر گفته شد ویروس Flamer

دارای ساختاری ماژولار است. در تحلیل‌های گذشته مشخص شده بود که یک ماژول بنام SUICIDE (که بسیار شبیه ocx.Browse۳۲ است) در بدافزار استفاده شده است که کار آن خودکشی ویروس بوده است. اما در ارسال فرمان خودکشی اخیر مهاجمان از آن استفاده نکرده‌اند. هنوز انگیزه مهاجمان از عدم استفاده از این ماژول آماده، مشخص نیست.

به نظر می‌رسد انگیزه اصلی مهاجمان از حذف ویروس از سیستم‌های آلوده، سعی در پنهان نگه داشتن زوایای ناشناخته عملکرد این ویروس بوده است و دور از ذهن نیست که مهاجمان پس از این عقب‌نشینی، درصدد حمله مجددی باشند.

نتایج کامل بررسی کارشناسان کسپرسکی درباره بدافزار Flame

رد پای استاکس‌نت در بدافزار شعله

محققان با بررسی کد کرم Flame دریافتند که این ابزار خرابکارانه با کرم استاکس‌نت بی‌ارتباط نبوده و هر دو از یک ریشه برخاسته‌اند.

به گفته متخصصان Kaspersky Lab، ماژول مهمی که Flame برای تکثیر خود به کار برده، مشابه همان ماژولی است که استاکس‌نت از آن استفاده کرده است. این ماژول در واقع یک نسخه ابتدایی از کرم استاکس‌نت است که در سال ۲۰۰۹، یعنی بیش از یک سال زودتر از شناسایی نسخه اصلی این کرم به وسیله شرکت ضد ویروس بلاروسی VirusBlokAda، در اینترنت فعال بود.

عده‌ای از کارشناسان کرم بدافزار Flame را مستقیما به استاکس‌نت مربوط می‌دانند؛ ویروسی که به گفته بسیاری از کارشناسان سایت غنی‌سازی هسته‌ای نطنز را هدف حملات خود قرار داده بود. ظهور استاکس‌نت و کمی بعد از آن بدافزار Flame از وقوع یک دوره جنگ سایبری و حملات شدید به اهداف گوناگونی در ایران دارد که سال‌ها به طول خواهد انجامید.

محققان کسپرسکی بر این باورند که نسخه‌های ابتدایی استاکس‌نت در واقع از دل چیزی برخاسته است که به آن «پلت‌فورم شعله» می‌گویند. بر اساس مطلبی که در وبلاگ Securelist شرکت کسپرسکی منتشر شده است، احتمال می‌رود که توسعه استاکس‌نت و Flame از سال ۲۰۰۹ مسیر تازه‌ای به خود گرفته بود، زیرا دو تیم برنامه‌نویسی مختلف با اهدافی متفاوت به صورت مستقل روی یک پلات‌فورم واحد مشغول به کار شدند.

متخصصان Kaspersky Lab و شرکت‌های دیگر ابتدا بر این باور بودند که استاکس‌نت و بر پایه دو ساختار نرم‌افزاری کاملا متفاوت بنا شده و شواهد زیادی برای ارتباط دادن این بدافزارها به یکدیگر وجود نداشت.

با وجود این رفته رفته دلایل و شواهد فراوانی کارشناسان را به ارتباط این بدافزارها به دیگری واداشت. از یک سو استاکس‌نت و Flame هر دو ایران و کشورهای همسایه این کشور را هدف قرار داده‌اند که پیش از این چنین الگوی رفتاری در هیچ بدافزاری دیده نشده است.

از سوی دیگر Flame به منظور تکثیر از یک کامپیوتر به کامپیوتر دیگر عمدتا از همان شیوه‌هایی استفاده می‌کند که استاکس‌نت هم برپایه آنها تکثیر و گسترش می یابد، مثل آلودگی از طریق USB و بهره‌گیری از آسیب‌پذیری Autorun ویندوز و یک آسیب‌پذیری دیگر دربخش پرینت.

اینگونه بود که محققان دریافتند گمان ابتدایی آنها در مورد Flame اشتباه بوده است. متخصصان کسپرسکی در تحقیقات خود به سرنخ‌هایی رسیدند که از طریق فناوری تحلیل خودکار ویروس کسپرسکی موفق به کشف و شناسایی آن شدند. این در حالی است که محققان از طریق همین فناوری در اکتبر سال ۲۰۱۰ فایل خرابکارانه‌ای را شناسایی کردند که شکل تغییریافته استاکس‌نت بود.

کارشناسان کسپرسکی در آن زمان با بررسی این نسخه تغییریافته، شباهت چندانی بین آن و استاکس‌نت پیدا نکردند و از این رو آن را Tocy.a نامیدند. بیش از دو سال پیش همان گروه محققان هنگام جست‌وجو برای یافتن نمونه‌های قدیمی تر بدافزارهایی شبیه به شعله به کرم Tocy.a برخوردند.

محققان با درنظر گرفتن تاریخچه Tocy.a و ریشه گرفتن به عنوان یکی از نسخه‌های

اولیه استاکس‌نت، تحقیقات خود را گسترش دادند تا دریابند که چرا هوش مصنوعی شرکت‌های امنیتی دو کد خرابکارانه را این چنین شبیه به هم در نظر می‌گیرد، ولی با سایر بدافزارهای شناسایی شده در پایگاه داده جامعه کسپرسکی شباهتی پیدا نمی‌کند. نتایج محققان از این قرار بود: ماژولی که در یک نمونه اولیه از استاکس‌نت پیدا شده بود، ۲۰۰۷ Resource نام گرفت.

این ماژول که کمی بیش از ۳۵۰ هزار بایت حجم دارد، در Stuxnet.a به کار رفته بود تا دسترسی کامل به سیستم‌های کامپیوتری را در مهاجمان قرار دهد.

پس از روی کار آمدن نسخه های بعدی استاکس‌نت اثری از ۲۰۷ Resource دیده نشد، از این رو کارشناسان توجه بیشتری به این نسخه از استاکس‌نت نشان دادند و رد پای این نمونه اولیه را در نسخه‌های پیشرفته تر بدافزار استاکس‌نت شناسایی کردند.

محققان با تحقیق بیشتر دریافتند که ۲۰۷ Resource تقریبا با ماژول بدافزار Flame تفاوتی ندارد. کسپرسکی هم اکنون ۲۰۷ Resource را یک پلاگین Flame یا به بیان دقیق‌تر «نمونه اولیه Flame» می‌نامد. در واقع ۲۰۷ Resource تقریبا از هر نظر با یکی از فایل های Comntemporary شعله به نام mssecmgr.ocx برابری می‌کند.

هر دوی این عناصر از ساختار مشابهی برخوردار است؛ فایل‌های زیرمجموعه هم نام، الگوریتم و رشته رمزگشایی مشابه و شیوه‌های کم و بیش یکسان نوشتن کد پایه. محققان کسپرسکی همچون کارشناسان شناسایی و تطابق دست خط به این نتیجه رسیدند که بی شک بخشی از عناصر استاکس‌نت و Flame به دست یک نفر یا یک گروه خلق شده است.

به اعتقاد محققان، ۲۰۷ Resource پایه پلت‌فرم شعله بوده است. کارشناسان کسپرسکی در وبلاگ Securelist نوشته‌اند: در بازه زمانی ماه ژانویه تا ژوئن ۲۰۰۹ که استاکس‌نت فعال شده بود، پلات‌فورم شعله هم خلق شده بود.

بر اساس محاسبات ما، تاریخ ساخت بدافزار شعله به تابستان ۲۰۰۸ بر می‌شود، یعنی زمانی که این کرم از ساختاری ماژولی برخوردار شده بود.

این کارشناسان معتقدند که استاکس‌نت از ماژول پایه پلت‌فرم Flame استفاده کرده است. به احتمال فراوان آن ماژول به طور خاص برای کارکرد در ساختار استاکس‌نت طراحی شده بود. به گفته محققان، این ماژول ابتدا از یک آسیب‌پذیری شناخته نشده موفق به نفوذ به یک سیستم کامپیوتری و کنترل کامل آن شد که مایکروسافت بعدا با انتشار وصله امنیتی MS 09-025 این آسیب پذیری را پوشش داد.

این ماژول سپس در سال ۲۰۱۰ از چرخه فعالیت خارج شد، زیرا هدایت‌کنندگان استاکس‌نت به دنبال شیوه‌های جدیدی برای نفوذ به سیستم از طریق آسیب‌پذیری بودند که مایکروسافت با عرضه وصله امنیتی MS 10-046 آن را مسدود کرد.

در سال ۲۰۰۹ تحول پلت‌فورم Flame از طریق تیمی که به طور مستقل روی استاکس‌نت کار می‌کردند، ادامه یافت.

در این حال محققان کسپرسکی احتمال دادند که کار روی برنامه‌های خرابکارانه به دو گروه برنامه‌نویس مستقل سپرده شده است؛ تیم F (Flame) و تیم D (Tilded) یا همان برنامه Flame) محققان کسپرسکی در این باره می‌گویند: هر یک از این دو گروه از سال ۲۰۰۷ به این سو مشغول توسعه پلت‌فرم خاص خود بوده‌اند، اما پایه و شواهد مشترکی در ساختار هر دو بدافزار به چشم می‌خورد.

علاوه بر ارتباط مستقیم بین Flame و استاکس‌نت، محققان پنج آسیب پذیری ناشناخته‌ای را کشف کردند که نسخه‌ای از استاکس‌نت در سال ۲۰۰۹ از طریق آن به سیستم‌های کامپیوتری نفوذ می‌کرد.

این نسخه از استاکس‌نت در ماژول استاکس‌نت و Flame هم به کار رفته بود. کد نفوذ از طریق آن آسیب‌پذیری همچنین در نمونه دیگری از استاکس‌نت که اوایل سال ۲۰۰۹ فعال بود، گنجانده شده بود. کد آن نسخه استاکس‌نت در فوریه ۲۰۰۹ نوشته شده بود و نفوذپذیری مربوط به آن هنوز کشف نشده بود. مایکروسافت این آسیب پذیری را چهار ماه بعد با انتشار به‌روزرسانی امنیتی MS ۰۲۵-۰۹ وصله کرد.

رول شوونبرگ، یکی از محققان ارشد بدافزار در کسپرسکی می‌گوید: برنامه‌نویسی که پشت حملات این حفره و حفره MS 10-073 بوده، در توسعه کرم Stuxnet.b هم نقش داشته است. محققان دقیقا نمی‌دانند که چرا ۲۰۷ Resource از کد استاکس‌نت حذف شد، هرچند می‌توان این اقدام را راهی برای مجزا کردن ساختار استاکس‌نت و شعله دانست. یک فرضیه می‌گوید که Flame یک ابزار جاسوسی سایبری برای مقاصد کلی است و برنامه نویسان نمی‌خواستند دو پلات‌فورم را بیش از حد لازم با هم درآمیزند.

تحقیقات متخصصان نتایج بسیار جالبی را به دنبال داشته است. دانستن این نکته که دو کد خرابکارانه با اهداف و مقاصد یکسان از یک منبع سرچشمه گرفته است، برای بسیاری از کارشناسان امنیتی تعجب‌آور نیست.

بسیاری تصور می‌کردند که اصل و اساس بدافزار Flame به یک دولت ناشناس بر می‌گردد و نه گروه‌های هکری و مجرمان سایبری. با این حال انتشار خبر حمله Collision بی‌سابقه Flame به منظور شبیه‌سازی یک به‌روزرسانی نرم‌افزاری مایکروسافت، شک کارشناسان را به یقین تبدیل کرد.

این در حالی است که گزارش‌های خبری اخیر به نقل از منابع دولتی ناشناس، ایالات متحده را عامل اصلی توسعه استاکس‌نت می‌داند. بر اساس این گزارش‌ها ممکن است آمریکا و متحدانش پس پرده بدافزار Flame هم نقش داشته باشند.

تهیه شده در شرکت پارس آتنا دژ

مرکز ماهر ابزار پاک‌سازی ضدبدافزار flame را منتشر کرد

به گزارش ایتنا مرکز ماهر وابسته به سازمان فناوری اطلاعات ایران ابزار پاکسازی مربوط به بدافزار flame را عرضه کرد. این نخستین باری است که راه حل یک بدافزار از سوی این مرکز و باسرعت قابل توجهی ارائه می‌شود. گفتنی ا ست که وجود بدافزار خطرناکی به نام tlame نیز چند روز پیش و توسط همین مرکز اعلام شده بود.

۵ درس بزرگ از ویروس Flame برای موسسات کوچک و متوسط

مشهور Flame با هدف حمله به موسسات کوچک و متوسط طراحی و تهیه نشده بود ولی با این حال می‌تواند چند درس بزرگ به این موسسات بیاموزد. در اینگونه اتفاقات بزرگ که خبرساز می‌شوند و توجه بسیاری را به خود جلب می‌کنند، حداقل برای مدت کوتاهی شاید بتوان توصیه ها و تذکراتی را به گوش کاربران عادی رساند.

ویروس Flame یک بدافزار جاسوسی بود که بر علیه برخی دولت‌ها از جمله ایران بکار گرفته شد. ولی در ماهیت، ویروس Flame هم بدافزاری است با اهدافی نه چندان متفاوت با دیگر تهدیداتی که موسسات کوچک و متوسط را بطور روزانه، هدف قرار می‌دهند. سرقت اطلاعات، شنود و جاسوسی از کارهای اصلی این بدافزار بوده است. هم اکنون هزاران بدافزار مختلف وجود دارند که همین کارها را انجام می‌دهند و تنها یک کشور و یا دولت را هدف نگرفته‌اند. همه ما می‌توانیم قربانیان این بدافزارها باشیم.

۱- هیچ طرح امنیتی صد در صد نیست. چیزی به معنی امنیت ۱۰۰٪ وجود ندارد. هیچ کارشناس و صاحبنظر امنیتی هم تا به امروز نبوده است که باوری به غیر از این داشته باشد. البته این نباید دلیلی باشد تا بنشینم و دست روی دست بگذاریم.

افراد خلافکار و مجرم به دو دلیل موسسات کوچک و متوسط را هدف قرار می‌دهند. اول اینکه می‌دانند، این موسسات سرمایه‌های با ارزشی دارند. این سرمایه‌ها می‌تواند مالی، نیروی انسانی، دانش فنی، اطلاعات بازار و مشتریان باشد. دوم اینکه، این افراد خلافکار می دانند موسسات کوچک و متوسط کمتر به مقوله امنیت توجه داشته و نفوذ به آنها ساده تر از موسسات بزرگ است که بر روی امنیت سازمان خود سرمایه گذاری خوبی می کنند.

پس موسسات کوچک و متوسط نیز باید سعی کنند تا هدف و قربانی سهل‌الوصولی نباشند. در حد امکانات و سرمایه خود، حداقل مراقبت‌های امنیتی را بعمل آورند و با مدیریت خطر و تهدیدات موجود و واقعی، ابتدا به آسیب‌پذیرترین نقاط و باارزش‌ترین سرمایه‌های خود توجه داشته باشند.

۲- شاید اصلاً ندانید که آلوده شده‌اید. ویروس Flame طی چند هفته گذشته کشف و شناسایی شد ولی بررسی‌ها نشان می‌دهد که این ویروس از چندین سال قبل وجود داشته و فعالیت می‌کرده است. حتی اگر کنترل و نظارت امنیتی مناسب و قوی در موسسه خود داشته باشید، لزوماً شاید متوجه وجود بدافزارهای فعال در شبکه خود نشوید. بدافزارهای امروزی تمام سعی و تلاش خود را می‌کنند تا مدت زمان طولانی‌تری مخفی مانده و بدون شناسایی شدن توسط ابزارهای امنیتی، به فعالیت های مخرب خود ادامه دهند. ویروس Flame هم از این قاعده مستثنی نبوده است. استفاده از فناوری‌ها و ابزارهای امنیتی نوین می‌تواند کمک بزرگی در کشف به موقع بدافزارها در شبکه سازمانی باشند. امروزه تنها یک ضدویروس نمی‌تواند جوابگوی نیازهای امنیتی باشد. شاید بهترین توصیه به موسسات کوچک و متوسط که از لحاظ سرمایه‌گذاری در زمینه امنیت IT محدودیت‌هایی داشته باشند، این است که منابع و منشاءهای اصلی تهدیدات را برای موسسه خود شناسایی و مشخص کنید و برای مقابله با این منابع خاص خطر و تهدید، به فکر بکارگیری از ابزارهای امنیتی مناسب باشید.

امروزه استفاده از ایمیل در موسسات به یک امر عادی و حتی ضروری تبدیل شده است. یکی از اصلی‌ترین منابع تهدید و انتشار بدافزار، ایمیل‌های ناخواسته، جعلی و تبلیغاتی هستند. پس از استفاده از یک ابزار ضدهرزنامه(Anti-Spam) می تواند یک تصمیم و اقدام امنیتی مناسب باشد. یا اگر در موسسه شما، استفاده از کامپیوترهای قابل حمل (Laptop) رایج است و این دستگاه‌ها بطور مستمر توسط پرسنل به بیرون از موسسه برده می‌شوند، شاید استفاده از ابزارهای امنیتی جهت مقابله با سرقت اطلاعات و یا حتی سرقت خود دستگاه، یک اقدام امنیتی مناسب باشد.

۳- حملات و تهدیدات امروزی بسیار پیچیده‌تر شده‌اند. این روزها با ظهور ویروس‌هایی مانند Flame، بسیاری از کارشناسان حسرت روزهای گذشته را دارند که با ویروس‌های ساده‌ای مانند "مجید" و "عباس کوهکن" روبرو بودند. اعتقاد قدیمی "تنظیم بکن و فراموش بکن" امروز به غیر از پشیمانی، حاصلی نخواهد داشت.

اقداماتی که سال قبل برای تامین امنیت شبکه سازمان خود انجام می‌دادید، احتمالاً امروز کارایی و ضریب اطمینان چندانی ندارد. حتماً باید سیاست‌ها و راهکارهای امنیتی موسسه خود را بطور مستمر مرور و بازنگری کنید. حتی اگر این کارها را به پیمانکاران حرفه‌ای خارج از سازمان، واگذار کرده باشید.

۴- صدمه به آبرو و سابقه موسسه می‌تواند برایتان گران تمام شود. شناسایی و انتشار اطلاعات ویروس Flame، پس از دو ویروس مشابه قبلی Stuxnet و Duqu، اکنون باید باعث خجالت و شرمندگی برخی مسئولان شود که چرا برای سومین بار غافلگیر و قربانی حوادث مشابه شده‌ایم.

فروپاشی سیاست‌ها و اقدامات امنیتی در یک موسسه کوچک و متوسط هم می‌تواند به نوبه خود، باعث خسارات مالی و از آن مهم‌تر، باعث صدمه و خدشه به آبرو و سابقه چندین ساله موسسه، شود. یقیناً موسسه‌ای که نتواند اطلاعات و سوابق مشتریان خود را محافظت کند، نباید انتظار داشته باشد که مشتریان به آسانی آن موسسه را از بین هزاران موسسه مشابه دیگر در بازار، برای همکاری انتخاب کنند.

۵- سرمایه و دارایی‌های خود را اولویت‌بندی کنید. شاید امکانات یک موسسه کوچک و یا متوسط اجازه ندهد که از تمام دارایی‌های موسسه محافظت کرد. در یک سیاستگذاری صحیح، سرمایه و دارایی‌های با ارزش موسسه باید شناسایی شده و امکانات موجود، صرف محافظت و نگهداری امن از این دارایی ها گردد. سرمایه می‌تواند حساب‌های بانکی، اطلاعات مشتریان، دانش فنی، فرمول ساخت و یا... باشد.

موسسات کوچک و متوسط نباید خود را فریب داده و بگویند: "ما که چیزی برای سرقت و دزدیده شدن نداریم". برای این موسسات ارزش دارد که بنشینند و با صرف وقت، بررسی کنند که در معرض چه تهدیداتی هستند، کدام سرمایه آنها بیشتر در خطر است و چه اقداماتی می توانند برای محافظت از آن، انجام دهند.

تهیه شده توسط شرکت مهندسی شبکه گستر

امنیت و مدیریت منابع دیجیتال سازمانی

- حفاظت جامع شبکه در برابر تهدیدات توسط UTM
- ارائه راهکارهای جلوگیری از نشت اطلاعات (DLP) و حفاظت از اسناد سازمانی
- محصولات و راهکارهای نظارت بر شبکه و اجزاء آن (Network Monitoring)
- راهکارهای نرم افزاری و سخت افزاری مدیریت پهنای باند و مصرف اینترنت (Accounting and Shaping)
- حفاظت جامع در برابر بدافزارها توسط نرم افزارهای Antivirus

ارائه خدمات با یک لبخند

خیابان ولیعصر، بلوار میرداماد غربی، مابین بلوار آفریقا و کوچه نور، پلاک ۳۱۵، واحد ۸

تلفن : (۱۰خط) ۹۲ ۳۶ ۶۴ ۸۸ نمابر : ۹۵ ۳۲ ۶۷ ۸۸

www.PersiaSysCo.com Info@PersiaSysCo.com

تحلیل آزمایشگاه ایمن از فلیم

بعد از حمله سایبری به شرکت نفت آزمایشگاه ضدبدافزار ایمن که نخستین آزمایشگاه ضد بدافزار ایرانی می‌باشد خود را موظف دانست تا همانند حملاتی همچون استاکس نت باز به دنبال راههای شناخت و مقابله با این بدافزار باشد. می‌توان ویروس شعله را در میان بدافزارها و جاسوس‌افزارها یکی از خطرناک‌ترین ومخرب‌ترین نوع بدافزار دانست، در یک نگاه می‌توان مدعی بود که این ویروس بسیار پیشرفته‌تر از Stuxnet و DuQu است، ساختار ماژولار و انعطاف پذیر و بسیار پیچیده و رمزگذاری شده به گونه‌ایست که امکان دیباگ و مهندسی معکوس کردن را بسیار دشوار و یا حتی غیرممکن می‌سازد، این ویروس ظاهرا هر اقدامی را برای مهاجمان فراهم می‌سازد. جمع آوری اطلاعات و فرستادن آنها ، نفوذ در شبکه‌های بزرگ(گاها صنعتی و مهم)، از بین بردن اطلاعات سیستم آلوده، قدرت جست‌وجو، تحلیل و پردازش گونه‌ای خاص از فایل‌ها، از کار انداختن آنتی‌ویروس‌ها، امکان ارتباط و ارسال گزارش با مرکز فرماندهی خود و ... اینها تنها بخشی از قابلیت‌های ویروس شعله است. در این گزارش بیشتر مواردی را مورد بررسی قرار میدهیم که از دید کثیری از تحلیلگران پنهان مانده است.

با بررسی ویروس شعله می‌توان بیان کرد که این ویروس از طریق فلش دیسک انتشار پیدا می‌کند و همچنین قابلیت منتشر شدن در سطح شبکه را نیز داراست، ویروس شعله برای آلوده ساختن از قابلیت Autorun ویندوز بهره می‌برد.

نکته جالب توجه در بررسی ویروس شعله این بود که این بدافزار برای بدست آوردن اطلاعات در مورد قابلیت‌های پهنای باند در فهرست وب سایت‌های خود از سه وب سایت ایرانی استفاده کرده است، که تاکید بر آن دارد،

ایران یکی از اهداف اصلی ویروس شعله بوده است.

برخی از اطلاعات ثبت شده توسط ویروس شعله عبارت است:

ثبت داده‌های برنامه‌های مختلف در رجیستری

Inno Setup
VNC
PenguiNet
RageWork File Manager
NetServe FTP Client
Jildi FTP Client
Cyd FTP Client
AceFTP 3 FreeWare
Intersoft Secure Key Agent
DameWare Nt Utilities
Bitkinex 2.7
SmartFTP
VanDyke SecureCrt
Ipswitch WS_FTP
BulletProof Ftp Client
CuteFTP
FTP Explorer
Robo Ftp
SoftX.org FTP Client
Mssh
Emurasoft EmFTP
Netx NetserverFtpClient
Web Drive From South River Technologies
(WinScp۲ (Martin Prikryl
TeamViewer
RADMin

از سایر ویژگی‌های ویروس شعله می‌توان به سوءاستفاده از حفره‌های امنیتی، سرقت کلمات رمز و عبور، متوقف کردن پروسه‌های امنیتی، شناسایی و از کار انداختن بیش از ۱۰۰ نرم‌افزار آنتی‌ویروس، ضد بدافزار، فایروال و ... ، قابلیت اجرا در Windows XP , Vista , ۷ ، پردازش و تحلیل فایل‌هایی با پسوندهای doc, *.docx, *.xls, *.dwg, *.kml.* *.ppt,*.csv,*.txt,*.url,*.pub,*.rdp, vsd, *.ora, *.eml.* ,*.ssh, *.ssh۲ تصویربرداری از صفحه نمایشگر ، ضبط صدا و استفاده از آنها برای مقاصد جاسوسی اشاره کرد. این ویروس توانایی از بین بردن خود را نیز دارد. لازم به ذکر است که قریب به ۹۰٪ اطلاعاتی که در محافل خبری معتبر و رسمی در مورد ویروس شعله ارائه شده درست بوده و مورد تائید آزمایشگاه ضد بدافزار ایمن می‌باشد.

گرچه برای پی بردن به تمامی اسرار نهفته در این بدافزار نیاز به زمانی به مراتب بیشتر از اینهاست. آزمایشگاه ضد بدافزار ایمن این افتخار را دارد که تا کنون دو گونه متفاوت از ویروس شعله را شناسایی و ضد بدافزار خود را بروز نموده است.

در پایان لازم است به این نکته اشاره شود که استاکس نت ، شعله و ... آخرین تهدیدات و حملات سایبری دشمنان این خاک نخواهند بود. به امید مقابله با چنین تهدیداتی قبل از وقوع اتفاق.

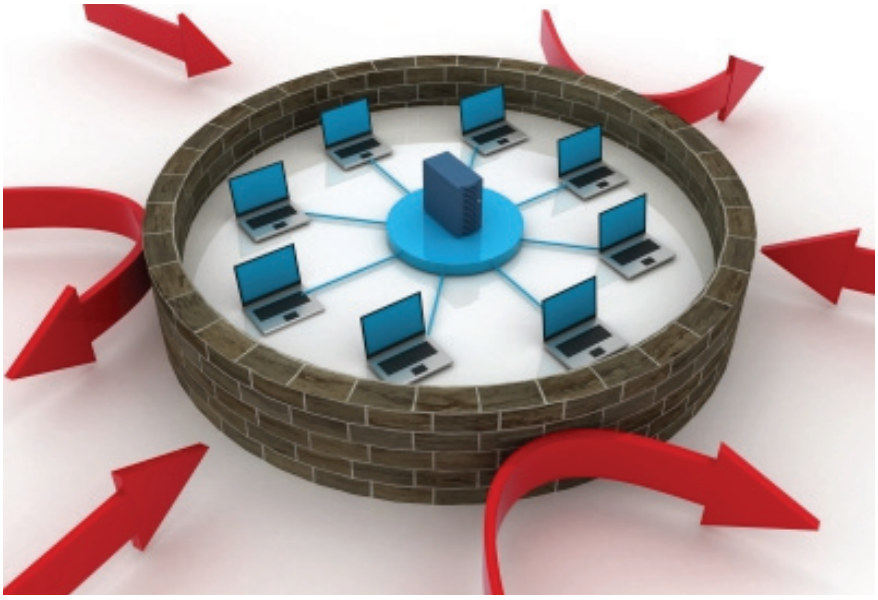
هشدار سازمان ملل درباره ویروس فلیم

سازمان ملل متحد قصد دارد تا هشدار جدی درباره ویروس فلیم صادر کند.

به گزارش ایتنا مارکو اوبیسو ـ مسئول بخش امنیت سایبری اتحادیه ارتباطات بین‌المللی سازمان ملل متحد مستقر در ژنو ـ گفت: این نهاد قصد دارد تا به زودی هشدار جدی درباره ویروس فلیم که به تازگی در ایران و دیگر کشورهای خاورمیانه کشف شده است، صادر کند.

وی تصریح کرد: این جدی‌ترین هشداری خواهد بود که تاکنون صادر شده است و به اعضای سازمان ملل خواهد گفت که ویروس کامپیوتری فلیم یک ابزار خطرناک است که می‌تواند به طور بالقوه برای حمله به تاسیسات زیربنایی مورد استفاده قرار بگیرد.

این مقام سازمان ملل با اعلام اینکه این ویروس توسط و یا از طرف یک کشور ساخته شده است، اظهار کرد: آنها (کشورها) باید هوشیار باشند.



حلقه‌های گم شده زنجیر امنیت اطلاعات

هومن پیرامون*
h.p@persiasysco.com

نقل قول مشهوری از یکی از نویسندگان وجود دارد که می‌گوید " تاریخ فی‌نفسه تکرار شدنی نیست اما موقعیت‌های تاریخی تکرار شدنی هستند " . شناسایی بد افزار بسیار پیچیده Flame که از دو سال پیش فعالیت خود را آغاز نموده در کنار حمله قبلی Stuxnet، ضمن زدن مهر تایید بر این نقل قول و گشایش فصلی جدید در مبحث امنیت شبکه‌های رایانه‌ای ، بار دیگر این واقعیت را به ما گوشزد نموده که فعالیت در این حوزه بسیار فراتر از یک تجارت عادی در زمینه فن آوری های پیشرفته می‌باشد.

در نگاهی نزدیک‌تر ، گذشته از نکات فنی و پیچیدگی‌های Flame ، نکته بسیار مهمی که در جریان آشکارسازی این بدافزار به چشم می‌خورد این است که بر خلاف موارد مشابه قبلی هیچ یک از تولید کنندگان محصولات ضد ویروس نتوانستند مدعی تشخیص و حتی کمک به تشخیص این بد افزار گردند که این امر پیام بسیار روشنی را با خود به همراه دارد: تشخیص و مقابله با گونه‌های جدید تهدیدات از عهده نرم افزارهای ضد ویروس رایج کاملاً خارج بوده و محصولی وجود ندارد که بتواند به تنهایی بار برقراری امنیت شبکه‌های رایانه‌ای را بر دوش کشد.

حال آیا این واقعیت بدان معنی است که دیگر دوران ضد ویروس‌ها به پایان رسیده ؟ قطعاً خیر اما این حقیقت را نیز باید پذیرفت که در سازمان‌های امروزی، نصب و استفاده از نرم افزار ضد ویروس دیگر معادل با برقراری امنیت ولو در سطح بسیار معمولی نیز نخواهد بود. به بیان دیگر، ضد ویروس‌ها جزو شروط لازم امنیت بوده اما دیگر کافی نیستند. پس چه عواملی باعث می‌شوند تا میزان آسیب پذیری سازمان‌ها افزایش یابد ؟ طبعاً" پاسخ به این سوال نیازمند کارشناسی مجدد فرآیندهای امنیتی در سطوح مختلف بوده و فراتر از چنین نوشته‌ای می‌باشد اما می‌تواند بهانه‌ای برای بررسی حلقه‌های ضعیف زنجیره امنیت شبکه باشد که می‌توان به برخی از آنها اشاره‌ای کوتاه داشت :

- عدم توجه به معماری لایه‌ای امنیت و استحکام زیر ساخت ها : مکانیسم انتقال ، انتشار و آسیب رسانی تهدیدات اخیر از جنس Stuxnet و Flame به خوبی این حقیقت را نشان داده‌اند که مباحث مستقلی همچون موارد زیر اهمیت بسیار زیادی در جلوگیری از نفوذ به سیستم‌ها و وارد آوردن آسیب و صدمات به شبکه داده‌ها داشته و غفلت از آنها به احتمال قریب به یقین آلودگی را به همراه خواهد داشت :
- نظارت و تجزیه تحلیل ترافیک شبکه سازمان (Network Monitoring)
- حفاظت از اسناد دیجیتال و جلوگیری از نشت اطلاعات در نقاط پایانی شبکه (DLP)
- معماری ساخت یافته و تجهیز مراکز داده
- پیاده سازی طرح‌های پیشگیرانه نظیر مقابله با بحران (Disaster Recovery Plan) و تداوم سرویس دهی (Business continuity plan)
- مدیریت جامع دسترسی به اینترنت در سازمان‌ها

نگاهی گذرا به آمار تقریبی ارائه دهندگان و خریداران خدمات و محصولات فوق نتایج دلگرم کننده‌ای را نشان نداده و نشان از طرز تلقی تجملی از آنها نزد مدیران دارد.

عدم توجه مدیریت کلان شرکت‌ها و سازمان‌های دولتی و خصوصی به ایجاد بستر مناسب برای مقابله با تهدیدات امنیتی:

تقریباً" اغلب شرکت‌های فعال در زمینه امنیت تجربه تلخ تلاش بی سرانجام برای متقاعد کردن مدیران و صاحبان صنایع به افزایش سطح امنیت شبکه خود را داشته‌اند. دیدگاه بسیار بدبینانه نسبت به تأمین کنندگان این محصولات و خدمات، عدم تخصیص بودجه مستقل به خرید خدمات و محصولات امنیتی حتی در سطح وزارتخانه ها ، استفاده از محصولات غیر اصلی و قفل شکسته و اعلام آن به عنوان یک موفقیت بزرگ در کاهش هزینه‌ها هر یک به تنهایی برای به صدا درآوردن زنگ خطر کفایت خواهند نمود. وجود این جو عدم اعتماد به سرعت مصرف کننده خدمات امنیتی را از جایگاه کارفرما و ناظر به پیمانکار تغییر داده و بی شک وسعت ، کیفیت و به روز بودن سیستم دفاعی سازمان را به نحو چشمگیری کاهش خواهد داد.

ضعف ساختاری بخش خصوصی به موازات مشکلات موجود در سمت خریداران محصولات امنیتی:

وجود برخی نقاط ضعف بنیادین در شرکت‌های تأمین کننده این محصولات و خدمات مزید بر علت گردیده تا تعداد حلقه‌های ضعیف زنجیره امنیت به نحو نگران کننده‌ای فزونی یابد. تمرکز اغلب شرکت‌ها بر محصولات رایج نظیر نرم افزارهای ضد ویروس و UTM ها و صرف منابع مالی و انسانی در این زمینه ، سنگینی کفه منافع تجاری نسبت به برتری‌های فنی را در سبد کالاهای ارائه شده در بازار موجب خواهد گردید. در میان مدت ، این امر سبب ایجاد جریانی غیر متخصص و صرفاً فروشنده در بازار امنیت گردیده که از یک سو قادر به پوشش نیازهای امنیتی مشتریان خود نبوده و از سوی دیگر موجب بدنامی سایر شرکت‌های امنیتی و بروز جو عدم اعتماد نزد مشتریان می‌گردد.

عدم سرمایه گذاری مدبرانه و در پیش گرفتن سیاست‌های اشتباه در حفظ و مدیریت نیروی انسانی متخصص ، رواج روزافزون عمل نکردن مدیران به تعهدات مالی نسبت به پرسنل و سرخوردگی کارشناسان و نخبگان این حوزه از این امر ، تخریب رقبا به جای رقابت با آنها و سوء استفاده برخی توزیع کنندگان منطقه‌ای این امر از جمله عواملی هستند که در سال‌های گذشته موجب افزایش تعداد شرکت‌های جدید التاسیس و تضعیف و حتی تعطیلی شرکت‌های قدیمی و با سابقه شده‌اند که برآیند این امر قطعاً" بی ثباتی و نزول فاحش سطح کیفی خدمات ارائه شده در بازار و آسیب پذیری در برابر تهدیدات جدید خواهد بود.

* مدیر بخش راهکارهای امنیتی پرشیاسیس خاورمیانه

تهدیدی به نام Flame

امروزه دنیای آی تی بخش عظیمی از زندگی روزمره ما انسان‌ها را به خود اختصاص داده و متاسفانه گاه اختلافات سیاسی به صورت جنگی تمام‌عیار در این حیطه نمایان می‌گردد. امروزه جنگ سایبری واژه‌ای است که همواره آن را می‌شنویم و در این گیرودار تنها برخورداری از ابزارهای امنیتی به‌روز و قدرتمند است که می‌تواند بقای فعالیت دیجیتال ما را رقم زند. فعالیتی مخاطره‌آمیز که در کنار هزاران تهدید و تهاجم صورت می‌پذیرد. سفارش همیشگی مدیران امنیت شبکه، بهره‌گیری از امکانات ضدویروس برای سیستم‌ها بوده و هست.

نمونه بارز تهاجم‌های سایبری، همین تهدید امنیتی اخیر انتشار ویروس فلیم است. البته به لطف ابزارهای ضدویروس قدرتمند، این ویروس در همان بدو ورود شناسایی شده و تمهیدات لازم نسبت به مسدودسازی مسیرهای نفوذ آن اندیشیده شده است. ویروس فلیم، اواخر ماه می پس از آن که صنعت نفت ایران را مورد حمله قرار داد، کشف گردید. پیش‌تر نیز اقدامات سایبری دیگری در خصوص صنایع زیرساخت ایران صورت گرفته بود که در ادامه به آن اشاره خواهد شد.

طراحی بسیار پیچیده و خطرناک این ویروس، حاکی از سازماندهی بزرگ و هزینه بالای تولید آن دارد، بنابراین می‌توان نتیجه گرفت این ویروس به سفارش دولتمردان متخاصم غربی جهت اختلال و جاسوسی در صنایع زیرساخت ایران طراحی شده باشد. اما نکته بسیار تامل‌برانگیز آنکه گفته می‌شود عاملین ساخت این ویروس، شرکت‌های امنیتی آی‌تی را نیز با خود همراه ساخته تا آن را شناسایی نکنند و از این طریق بر شدت میزان صدمات آن بر شبکه‌های کامپیوتری ایران افزوده شود.

هرچند کشف این ویروس موفقیتی بزرگ است، اما نباید برای بزرگ‌نمایی این موفقیت، مسایلی بسیار بدیهی نیز وارونه جلوه داده شود. ماهیت اصلی وجود شرکت‌های امنیت آی‌تی در تشخیص و مسدودسازی تهدیدهای کامپیوتری و اینترنتی است، پس چگونه می‌توانند این شرکت‌ها در برابر این نفوذ سایبری سکوت کرده باشند؟

برای روشن ساختن موضوع می‌توان به گزارش مفصل شرکت امنیتی Avira در این خصوص اشاره کرد که در وب‌سایت رسمی آن شرکت آمده است.

بدافزار فلیم

به گزارش اویرا، این ویروس که نام کامل آن TR/Flamer.A است، نوعی تروجان است که حدود یک ماه پیش، در تاریخ ۲۹ می ۲۰۱۲ (یعنی همان ایام حمله سایبری به صنعت نفت)، توسط ابزارهای امنیتی و ضدویروس اویرا کشف و اطلاع‌رسانی شده است. در همان زمان نیز تمهیداتی در خصوص مقابله با آن به کار گرفته شده است. حجم فایل این ویروس حدود ۶ مگابایت بوده و پلتفرم‌های هدف آن تمامی

نسخه‌های فعلی ویندوز (اعم از ملینیوم، ۲۰۰۰، ایکس‌پی، ویستا، ویندوز۷ و حتی ویندوز سرور ۲۰۰۳ و ۲۰۰۸) است.

در خصوص دامنه فعالیت این ویروس می‌توان به اجرای کدهای مخرب روی سیستم‌های آلوده، آلوده‌سازی فایل‌ها، ثبت فعالیت کیبورد، تغییر در رجیستری سیستم و در نهایت به سرقت اطلاعات و جاسوسی اشاره کرد. تغییرات رجیستری بدان منظور است که با هر بار اجرای ویندوز، این ویروس نیز فعال گردد. این ویروس پس از آنکه خود را در مسیر

%Program Files\Common Files\ Microsoft Shared\ MSAudio\Wavesup3.drv

کپی کرد، فایل‌های دیگری را ایجاد کرده و بدین ترتیب فعالیت مخرب خود را آغاز می‌کند.

تهاجم به همین جا ختم نمی‌شود؛ فلیم قادر است فایل‌های متنی ورد و پی‌دی‌اف را نیز بررسی کرده و خلاصه آنها را برای سرور خود ارسال نماید. بدتر آنکه گفته می‌شود ویروس فلیم حتی می‌تواند میکروفن و دوربین سیستم آلوده را فعال ساخته تا صحبت‌ها را شنود نماید و حتی عکس و فیلم تهیه کند.

این ویروس به گونه‌ای طراحی شده که می‌تواند در صورت خطر، دست به انهدام خود زده و آثارش را پاکسازی نماید. بدین ترتیب احتمال کشف آن به صفر می‌رسید. برای اطلاع کامل‌تر از نحوه عملکرد ویروس فلیم می‌توانید به این آدرس اینترنتی مراجعه نمایید:

http://www.avira.com/en/support-threats-description/tid/۷۴۸۶/tlang/en

تاریخچه نبرد سایبری علیه ایران

اولین تهدید جدی و شناخته شده در جنگ سایبری با ایران، بدافزار استاکسنت بوده، این بدافزار که ساختار بسیار پیچیده دارد نمی‌تواند توسط عده‌ای ویروس‌نویس معمولی تولید شده باشد، به گواه اغلب کارشناسان امنیتی پشت این بدافزار به احتمال بسیار دولت‌ها و سرمایه‌داران بزرگی قرار گرفته باشند. هدف اصلی این بدافزار تاسیسات هسته‌ای ایران بوده که خوشبختانه ناکام نیز ماند. اما بدافزار دیگری نیز با همین هدف طراحی شده بود که نام آن Doco است.

اما برگ جدید بازی بدافزار فلیم بوده است که جالب آن است که کشف آن تقریباً اتفاقی بوده و هنگامی کشف گردید که ویروس Viper سیستم کامپیوتری صنعت نفت ایران را آلوده کرده بود و اطلاعات زیادی را از بین برده بود. شرکت‌های ویروس‌یاب کامپیوتری که مستقل از یکدیگر به دنبال کشف و انهدام این ویروس بودند، به طور اتفاقی ویروس فلیم را کشف کردند.

آینده چگونه خواهد بود

شاید این پایان کار نباشد و بدافزار متعدد دیگری به ساختار امنیتی سازمان‌های ما یورش آورند، اما باید دانست که شک داشتن به سلاح‌های امنیتی خود بزرگ‌ترین تهدید در سیستم دفاعی به حساب می‌آید. این تفکر که شرکت‌های امنیتی خود ممکن است دستی در ماجرا داشته باشند ممکن است شبکه‌های ما را از دفاع مناسب دور کرده و مشکلات بیشتری برایمان بیافرینند.

شاید بهترین روش برای مقابله با تهدیدات، آموزش هرچه بیشتر مدیران شبکه‌ای و استفاده صحیح از ساختارهای دفاعی چندلایه مبتنی بر تکنولوژی روز دنیا خواهد بود.

تهیه شده توسط شرکت رایان سامانه آرکا

AVIRA

Avira Endpoint & Email Security

امنیت جامع شبکه

Avira Endpoint & Email Security includes:

Avira Professional Security (Windows, Unix)
the best possible protection for your desktop PCs.

Avira Server Security (Windows, Unix)
maximum security for your file servers.

Avira Management Console time saving, network-wide security management. **Incl. Avira Update Manager** automatically download the updates of a large number of your Avira products from the Internet.

NEW: Email Protection with Avira Managed Email Security (AMES)
Email traffic will be filtered in Aviras' data centers so nothing but clean mail enters your network.
Take back your bandwidth. Say goodbye to antispam software that slows your mail server to a crawl.

نگاهی به
حمله‌های APT

ایمان منصوری*
i.mansouri@pouyesh.net

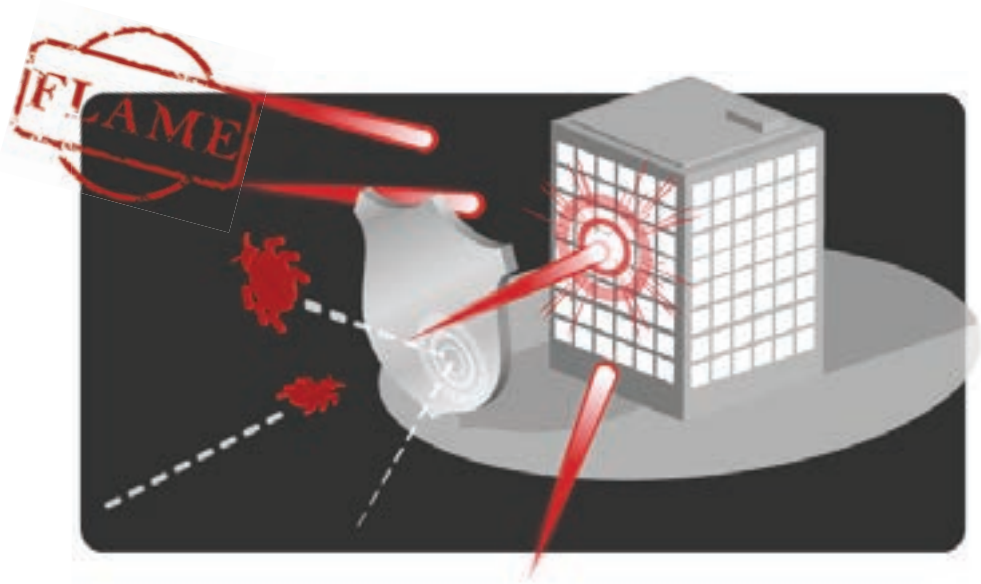
اصطلاح APT (Advanced Persistent Threat) در سال ۲۰۰۶ و توسط نیروی هوایی ایالات متحد آمریکا ابداع شد و حملاتی را شرح می‌دهد که سه خصلت بسیار مهم دارند. ابتدا اینکه Advanced هستند، این بدان معناست که نفوذگرها افراد متخصص با توامندی فنی بالا و بودجه‌های تحقیقاتی قابل توجه می‌باشند. هدف این تحقیقات ایجاد ابزارها و روش‌های کاملاً اختصاصی است که صرفاً برای نفوذ به قربانی‌های آنها طراحی شده است. نکته دوم در مورد این حملات Persistent بودن آنها است. قالباً مقاصد این حملات از قبل مشخص و انتخاب شده هستند، عملیاتی است که شاید ماه‌ها به طول انجامد و فعالیت‌های بسیار آرام و مخفیانه دارد. ویژگی سوم نیز Threat است. حملات APT کاملاً مدیریت شده می‌باشند و اهداف سیاسی، نظامی و یا تجاری را دنبال می‌کنند. هدف اصلی این حملات غالباً ارگان‌ها و تسهیلات دولتی، تولیدکنندگان تجهیزات دفاعی و نظامی و سازندگان بسیار مطرح در بازارها جهانی هستند. اگرچه این حملات می‌توانند سازندگان و همکاران مهم قربانیان اصلی را نیز شامل شود. گاهی نیز دیده می‌شود که شرکت‌های معمولی دارای اطلاعاتی در مورد یک تکنولوژی مهم و یا شرکت‌های مرتبط با سازمان‌ها و ارگان‌های مهم زیرساختی نیز هدف این حملات قرار می‌گیرد. این حملات کاملاً استراتژیک و دقیق طراحی می‌شوند به همین دلیل از لحظه نفوذ زمان نسبتاً طولانی در ساختار باقی می‌مانند تا ماموریت اصلی خود که در اکثریت موارد سرقت اطلاعات است را به پایان رسانند.

چون اکثر پروژهای APT نیازمند منابع انسانی، مالی و نفوذی زیادی هستند، اکثراً تحت نظارت مراجع اطلاعاتی و امنیتی فعالیت می‌کنند. البته در زمانی که پای مراجع دولتی و با اهداف ملی در میان است، این موضوع به جنگ یا Warfare تبدیل می‌شود که جنگ سایبری یا Cyberwar خوانده می‌شود. به همین دلیل بدافزارهایی نظیر Stuxnet ، Duqu و Flame همگی در دسته‌بندی این حملات قرار می‌گیرند.

یک حمله APT چرخه‌ای را طی می‌کند که «زنجیر مرگ» یا Kill-chain نامید می‌شود. زنجیر مرگ یک پروسه کاملاً سیستماتیک و مشخص است که منجر به یک نفوذ موفق می‌شود. در ادامه این چرخه شرح داده شده است: اولین مرحله از حملات APTها، Reconnaissance نامیده می‌شود. در این مرحله تیم نفوذگر سعی در شناسایی افراد، سیستم‌ها و ساختار داخلی هدف خود نموده و اقدام به پیدا کردن تمامی راهکارهای ممکن جهت ارسال کدهای مخرب می‌کند. این مرحله گاهاً مطالعات و تحقیقات وسیعی را طلب می‌کند تا آنها را با قربانی خود آشنا کند. تجهیزات نرم‌افزاری و سخت‌افزاری، سرویس‌های شبکه و غیرشبکه‌ای، روال‌ها، کارشناسان و کارمندان

و خصلت‌های رفتاری و فکری آنها، همکاران و پیمانکاران همگی مورد شناسایی قرار می‌گیرند. قسمتی از اطلاعات از طریق دسترسی‌های آنلاین و بخشی نیز از طریق تحقیقات حضوری انجام می‌شوند.

همانطور که اشاره شد، از موارد بررسی در این مرحله کسب اطلاعات در مورد راهکارهای ارسال فایل‌های مخرب می باشد تا با استفاده از آن نفوذگرها بتوانند مرحله بعدی یا همان infection یا آلوده‌سازی را پایه‌گذاری کنند. در مرحله infection یا آلوده‌سازی، نفوذگرها سعی در پیدا کردن راهکارهایی جهت اجرا شدن فایل مخرب خود می‌کنند. البته اصولاً آنها چندین راهکار را به صورت همزمان مورد استفاده قرار می‌دهند. مهم‌ترین و موثرترین راهکار در این مرحله، استفاده از تکنیک‌های Social Engineering است و به همین دلیل طیف وسیعی از راهکارهای عملی را شامل می‌شود. در ساده‌ترین راهکار ممکن است که فایل مخرب بر روی یک حافظه فلش یا CD-ROM کپی شوند و به نحوی آن را به دست یکی از کاربران شبکه برسانند تا آن را به رایانه خود متصل کند. با قرار دادن یک فایل Auto-RUN در آنها می‌توان به گونه‌ای عمل کرد که بلافاصله پس از اتصال، فایل مورد نظر اجرا شود. یکی دیگر از روش‌ها این است که یک فایل EXE درون یک فایل دیگر پنهان‌سازی شود تا پس از اجرای فایل اصلی، فایل دومی نیز اجرا شود. یکی از بهترین روش‌هایی که تمامی شبکه‌ها را بدین طریق مورد حمله خود قرار می‌دهند، فایل‌های Crack هستند. بارها دیده شده است که نرم‌افزارهای بسیار کاربردی و عمومی از قبیل Microsoft Office از کرک استفاده می‌کنند. لذا تنها لازم است نفوذگرها منابع مورد استفاده را شناسایی کرده و از طریق حملات Man-in-the-middle یا هک سایت مربوطه و جایگزینی فایل‌های اصلی با فایل‌های معیوب، فایل‌های مخرب جایگزین شوند. راهکار بسیار مرسوم و سهل‌تر دیگر، استفاده از پست الکترونیک است. در این روش ها نفوذگرها، Emailهایی را حاوی فایل‌های مخرب برای چندین کاربر انتخابی ارسال می‌کنند که شامل فایل‌های ضمیمه با پسوندهای PDF، فایل‌های Microsoft Office، Flash، java،multimedia و غیره می‌باشند و با باز کردن آنها بدافزار اجرا می‌شود. البته گاهی نیز لینکی به یک وب سایت ارسال می‌شود که با بازدید از آن یک عملیات مخرب اجرا می‌گردد. این نامه‌های الکترونیکی قالباً به نحوی طراحی می‌شوند که ظاهراً از سمت افراد trusted و مورد اطمینان ارسال شده‌اند. هرچند همانطور که گفته شده ظاهر این نامه‌ها بگونه‌ای طراحی شده‌اند که تشخیص مخرب



بودن آنها بسیار سخت و شاید غیرممکن است. آنچه پس از اجرای فایل‌های مخرب روی می‌دهد، اجرای مرحله Exploitation است. فایل‌های مخرب از طریق سوءاستفاده از ضعف‌های امنیتی و Bugهای نرم‌افزاری کدهای مخرب خود یا همان exploitها را اجرا می‌کنند. این کدهای مخرب غالباً به نحوی اجرا می‌شوند که Privilege Escalation انجام می‌دهند تا بتوانند تحت یک پروسس یا account با دسترسی بیشتر فعالیت کنند. در حملات APT، اصولاً چندین Exploit به صورت همزمان اجرا می‌شوند تا حتماً از موفقیت حمله اطمینان حاصل شود. نکته مهم دیگر در مورد این Exploitها، خاصیت day-۰ بودن آنها است. با توجه به اینکه تمامی حملات targeted هستند، از vulnerabilityهایی در این Exploitها استفاده می‌شود که عمومی نیستند و صرفاً برای حمله مورد نظر کشف شده‌اند. در راستای مقابله با این حملات که به client-side exploitation معروفند، می‌بایستی از راهکارهای HIDS و یا NIDS استفاده کرد تا مانع نفوذ کدهای مخرب در سطح شبکه شده و یا از فعالیت‌های مخرب در سطح سیستم جلوگیری شود. متاسفانه دیده شده که به دلیل مشکلاتی که HIDS/HIPS پس از نصب ایجاد می‌کنند و عمل tuning آن کاملاً زمانبر است. بسیاری از Adminها این نرم‌افزار را غیرفعال می‌کنند و مدتی پس از نصب آن را حذف می‌نمایند و در نتیجه درصد موفقیت این کدهای مخرب افزایش می‌یابد.

در مرحله بعدی که Installation نام دارد، فایل‌های اصلی بدافزار بر روی سیستم کپی می‌شوند. در برخی موارد فایل‌های اصلی همراه فایل مخرب اولیه قرار دارند. برخی malware نیز پس از طریق اتصال به اینترنت این فایل‌ها را از C&C خود دریافت می‌کنند. البته در برخی موارد نیز تنها یک backdoor ساده نصب می‌شود تا دسترسی‌های آتی فراهم گردد. در این مرحله، فایل جدیدی در بخش‌های محافظت شده سیستم عامل کپی می‌شوند، تغییرات جدیدی در برخی فایل‌ها سیستمی نظیر DDLها و حتی غیرسیستمی اعمال شده و یا کلیدهای رجیستری جدید ایجاد می‌گردد. متاسفانه مقابله با این مرحله از چرخه مرگ Malwareها به دلیل پیچیدگی آن، عمل سخت و دشواری است. لذا قطعاً نیاز است تا از نرم‌افزارهای integrity Monitoring استفاده شود تا هرگونه تغییرات در فایل‌ها و حتی برخی پروسس‌ها مانیتور شوند که برای این امر، اختصاص زمان و نیروی انسانی لازم است. البته در برخی موارد نیز با مانیتور کردن فعالیت‌های اینترنتی نیز می‌توان بارگذاری فایل‌های مخرب را شناسایی کرد.

تمامی Malwareها پس از عمل Exploitation از طریق اینترنت به C&C یا command and control serverهای خود متصل می‌شوند. هدف از این اتصال غالباً ثبت اطلاعات مربوط به قربانی، دریافت فرمان‌های بعدی، به روزرسانی فایل‌های ویروس و ارسال اطلاعات کسب شده است. نکته مهم در این است که این ارتباط در بیشتر ویروس‌ها از طریق ارتباطات covert channel بوده و غیرقابل شناسایی می‌باشند. در گذشته، بیشتر malwareها از پورت‌های مخصوص به خود استفاده می‌کردند و به همین دلیل به راحتی امکان شناسایی آنها وجود داشت که لیست نسبتاً کامل و دقیقی از این پورت‌ها در آدرس http://www.emsisoft.com/en/kb/portlist وجود دارد.

اما امروزه اکثر ارتباطات از طریق پروتکل‌های HTTP، SSL و SSH است. آمار بازدید سایت‌های متعدد در سازمان و ارگان‌های با تعداد کاربران زیاد آن قدر بالا است که امکان trace این ارتباطات برای مدیران امنیت شبکه عملاً غیرممکن است. متاسفانه ارتباطات با C&C از ساختارهای یکسان پیروی نمی‌کنند، لذا امکان استفاده از script ها و نرم‌افزارها جهت آنالیز آنها نیز وجود ندارد. البته در مورد ویروس‌های که شناسایی می‌شوند و یا با مهارت لازم نوشته نشده‌اند، امکان شناسایی و قطع این ارتباطات به نحوی امکان‌پذیر است، اما در حملات APT که به صورت مخفیانه و تنها برای گروه‌های خاصی فعالیت می‌کنند باز هم این امر به غیرممکن نزدیک است.

گام بعدی در حملات APT، عملیات Data Capture نام دارد. همانطور که اشاره شد حملات APT اهدافی خاصی را دنبال می‌کنند، لذا موفقیت آن وابسته به شناسایی کامل ساختار شبکه، راهکارهای دفاعی و mapping کامل شبکه قربانی آنها است. اطلاعات کسب شده نظیر توپولوژی شبکه، نام‌های کاربری، رمز عبور، انجام Inventory در شناسایی تجهیزات سخت‌افزاری و نرم‌افزاری و غیره همگی نفوذگرها را به سمت هدف اصلی حمله خود هدایت می‌کند. قسمت دوم اطلاعات پس از شناسایی و تسخیر منابع اصلی کسب می‌شوند که جمع‌آوری اطلاعات و harvesting دیتا موردنظر نفوذگرها است. البته با توجه به اینکه تهدیدات APT به صورت مخفیانه فعالیت می‌کنند، لذا این مرحله به گونه‌ای طراحی می‌شود که کاملاً ایمن و بدون هر گونه نویز انجام شود تا شناسایی آن امکان‌پذیر نباشد. البته تمامی در حملات APT هدف سرقت اطلاعات نمی باشد و در برخی موارد تنها معیوب‌سازی هدف آن می باشد و لذا این مرحله مشاهده نمی‌شود.

بعد از اینکه نفوذگرها کنترل سیستم را در اختیار گرفتند و اطلاعات کافی جمع‌آوری شد، گام بعدی Data Exfiltration است. در این مرحله، تمام اطلاعات جمع‌آوری شده به C&C های موجود ارسال می‌شوند تا توسط نفوذگرها بررسی شوند. این اطلاعات در بسته‌های رمزنگاری شده و یا password-protected ارسال می‌شوند تا قابل خواندن نباشند. برخی نیز از فایل‌هایی با فرمت‌های اختصاصی استفاده می‌کنند که کاملاً ناشناخته‌اند.

مرحله نهایی حملات APT، مرحله‌ای تحت نام Destruction است. این مرحله دو هدف را دنبال می‌کند. در برخی موارد هدف حملات APT ایجاد اختلال می‌شود، لذا پس از عمل Exploitation عملیات تخریب‌سازی نرم‌افزارها و سخت‌افزار مورد نظر و توقف عملیات‌های اجرایی صورت می‌پذیرد. در برخی موارد نیز پس از کسب اطلاعات لازم، عملیات Seize انجام می‌شود. در این عملیات نفوذگرها عملیات خودکشی و یا پاک‌سازی را اجرا می‌کنند و بدون اینکه هیچ گونه اتفاقی رخ دهد، کلیه اجزای مرتبط به بدافزار از بین می‌روند.

* مدیر دپارتمان ICT شرکت مهندسی پویش افزار هوشمند

بررسی ۱۰ ساله تکامل نرم‌افزارهای مخرب و دورنمایی از تهدیدات امنیتی

مینا سلطان محمدی
حمید خان زاده

توجه: مایکروسافت این اطلاعات آماری را صرفا جهت مقاصد اطلاع‌رسان منتشر کرده و استفاده از آن برای مقاصد تجاری را ممنوع اعلام نموده و حق انتشار آن را با ذکر منبع آن بلامانع دانسته است. با توجه به این موضوع و برای پایمال نشدن حقوق مایکروسافت و همچنین مترجمین آن از زبان انگلیسی به زبان فارسی، ذکر نام مترجمین آن لازم است. این گزارش اطلاعات موجود و دیدگاه‌های تصریح شده‌ای را فراهم می‌کند که ممکن است بدون اطلاع قبلی تغییر کند، از جمله URL و دیگر مراجع وب سایت‌های اینترنتی. لذا پیامدهای استفاده از آن برعهده استفاده کننده است.

آسیب‌پذیری

تعریف ساده‌ای از آسیب‌پذیری یعنی ضعف‌های نرم‌افزارها که یک هکر را قادر می‌سازد تا توسط آن نقاط ضعف، دسترسی یا اعتبار برنامه یا داده‌ای که آن برنامه پردازش می‌کند را در خطر قرار دهد.

برخی از بدترین آسیب‌پذیری‌ها به هکرها اجازه می‌دهد تا از یک کامپیوتر در معرض خطر بهره‌برداری کنند و باعث شوند تا کدهای دلخواه بدون اطلاع کاربر اجرا شوند.

گزارش ۱۰ سال گذشته نشان‌دهنده یک بازده زمانی بسیار جالب است در بررسی افشای آسیب‌پذیری و متعاقب آن تغییراتی که بر مدیریت ریسک در سازمان های IT

شکل ۱. صنعت گسترده افشای آسیب‌پذیری از سال ۲۰۰۲ از جمله سخت‌افزار، نرم‌افزار، و روند رشد آن

در سراسر جهان تاثیر گذاشته است.

روند افشای آسیب‌پذیری:

افشای آسیب‌پذیری در کل این صنعت در سال ۲۰۱۱ تقریبا ۱۱,۸ درصد از سال ۲۰۱۰ کاهش یافته است.

در حالی که شدت آسیب‌پذیری روندی مثبت داشته است اما بطور متوسط آسیب‌پذیری از نقاط اوج خود در سال‌های ۲۰۰۶ و ۲۰۰۷ به طور پیوسته کاهش یافته است. که نشان‌دهنده رشد امنیت می‌باشد.

روند بهره‌برداری از بولتن‌های امنیتی

مرکز پاسخگویی امنیت مایکروسافت(Microsoft Security Response Center (MSRC آسیب‌پذیری‌های امنیتی نرم‌افزارهای مایکروسافت را مشاهده می‌کند و آنها را شناسایی و سپس مشکل آنها را برطرف می‌کند. مرکز MSRCهر ماه برای رسیدگی به آسیب‌پذیری در نرم‌افزارهای مایکروسافت اعلامیه‌های امنیتی منتشر می‌کند. اعلامیه‌های امنیتی در هر سال به طور سریالی شماره‌گذاری می‌شوند. به عنوان مثال، "MS11-057" به اعلامیه امنیتی شماره ۵۷ اشاره دارد که در سال ۲۰۱۱ منتشر شده است.

• در سال ۲۰۱۱ مرکز MSRC۱۰۰ اعلامیه امنیتی منتشر کرده است که ۲۳۶ نوع از آسیب‌پذیری‌های شناسایی شده CVE را به طور جداگانه بررسی می‌کند، که به ترتیب، از سال ۲۰۱۰، ۷٪ و ۶٪ کاهش می‌یابد. همانطور که نمودار نشان می‌دهد، میانگین تعداد CVE های بررسی شده توسط هر یک از اعلامیه‌های امنیتی در طول زمان، از ۱,۵ در H۱۰۵تا ۲ در 2H11 افزایش یافته است.

نرم‌افزار مخرب و روند ناخواسته و بالقوه آن

ساختار تروجان به این شکل است که پس از ورود به سیستم عامل به تکامل خود نیز ادامه می‌دهد، نوسانات در شناسایی اشکالات مختلف در نرم‌افزارهای مخرب گاهی اوقات نشان‌دهنده موفقیت مداوم صنعت نرم‌افزار ضدمخرب است، نرم‌افزارهای ضدمخرب در برابر توسعه‌دهندگان نرم‌افزارهای مخرب ایستادگی می‌کنند تا آنها را از پای در بیاورند.

چگونه تهدیدها در طول زمان تکامل یافته‌اند

با مشاهده آمارها و چشم‌انداز چند ساله به این نتیجه خواهید رسید که، برخی از نرم‌افزارهای مخرب بالقوه اوج گرفته‌اند و بسیاری دیگر از این قبیل ابزارها شایع شده‌اند، تا مدت کوتاهی که فروشندگان برنامه‌های ضد مخرب تلاش خود را در شناسایی و از بین بردن این تهدید به کار گرفتند.

دوره اوج نرم‌افزارهای مخرب تا زمانی است که ضدویروس‌ها و ضدتروجان‌ها توانایی تشخیص یک ابزار مخرب را نداشته باشند و یا توان از بین بردن آن را نداشته باشند. تا آن زمان ابزارهای مخرب می‌توانند اوج بگیرند، اما به محض اینکه راه مقابله با آنها آشکار گردد نتیجه معکوس خواهد شد و روند رشد رو به کاهش خواهد گذاشت، این زمانیست که هکرها باید تاکتیک خود را تغییر دهند و در پی راه نفوذ و پیشروی دیگری باشند.

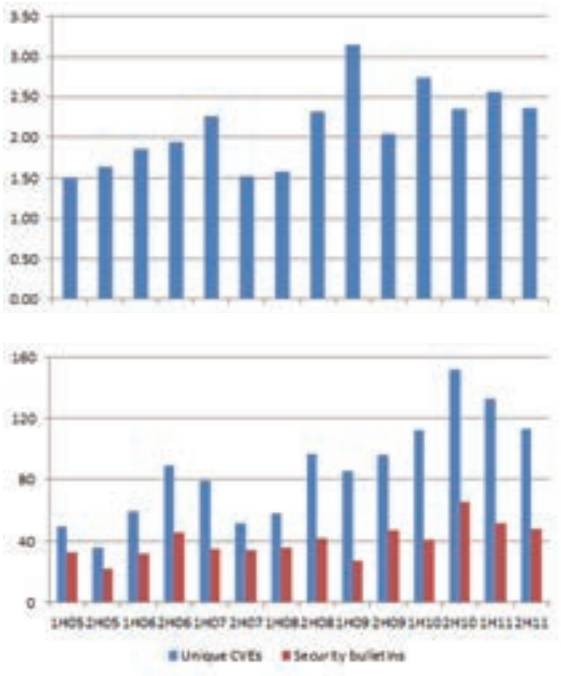
شکل شماره سه این پدیده را نشان میدهد. (محور عمودی درصد کامپیوترهایی را نشان می‌دهد که با نرم‌افزار مخرب آلوده شده‌اند.)

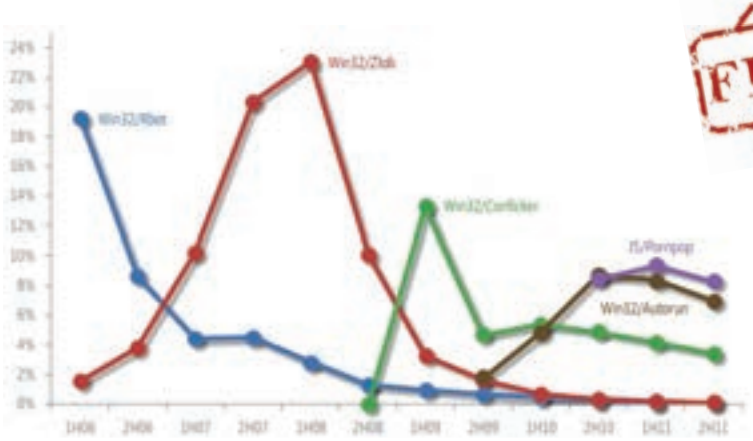
شیوع Win32/Rbot که از خانواده botnetبود از سال ۲۰۰۴ شروع و تا سال ۲۰۰۵ ادامه داشت و جزو یکی از بدنام‌ترین آلودگی‌ها بود که توانست رسانه‌ها و شبکه‌های دولتی را آلوده کند، "Rbot" از خانواده kit ها محسوب می‌شود.

Win32/Conficker از خانواده کرم‌هاست که در نوامبر ۲۰۰۸ کشف شد که در ابتدا توانست با بهره‌برداری از آسیب‌پذیری امنیتی MS۰۸-۰۶۷ ویندوز شروع کارش را آغاز کند.

JS / Pornpop نرم‌افزاری تبلیغاتی است که شامل ابزارهای دستکاری شده با قابلیت جاوا اسکریپت است که تلاش در نمایش تبلیغات پنهان شده دارند. دومین و شایع‌ترین خانواده کشف شده در 2H10 و 1H11 است که اولین بار در آگوست

شکل ۲. تعداد اعلامیه‌های امنیتی MSRC و آسیب‌پذیری‌های شناسایی شده CVE–بررسی شده، و میانگین تعداد CVE بررسی شده در هر اعلامیه امنیتی را نشان می‌دهد.





شکل ۳.نرم‌افزارهای مخرب و خانواده نرم‌افزارهای ناخواسته که از سال ۲۰۰۶ اوج و کاهش یافته‌اند

۲۰۱۰ کشف شد، و احتمالا شایع‌ترین خانواده کشف شده در 2H11 است.

Win32/Autorun کشف عمومی برای کرم‌هاست که تلاش می‌کند بین فضای برنامه‌های نصب شده کامپیوتر، با سوءاستفاده از قابلیت Autorun در ویندوز پخش شود. کشف Win32/ Autorun به تدریج برای چند دوره قبل از اوج گرفتن در 2H10 به عنوان شایع‌ترین ابزار مخرب توسعه یافت و سرعت انتشار آن افزایش یافت.

تهدیدات مختلف در زمان‌های مختلف

تصویر شماره چهار شیوع مربوط به شش طبقه‌بندی مختلف از نرم‌افزارهای مخرب کشف شده در کامپیوترها را از سال ۲۰۰۶ نشان می‌دهد.

تصویر شماره ۴. (تصویر بالایی)طبقه بندی کرم‌ها، backdoor ها، و نرم‌افزارهای متفرقه ناخواسته از سال ۲۰۰۶ را نمایش می‌دهد. همچنین (تصویر پایینی) طبقه‌بندی نرم‌افزارهای تبلیغاتی نرم‌افزار متفرقه ناخواسته و تروجان‌های متفرقه از سال ۲۰۰۶ را به تصویر کشیده است.

بسیاری از کرم‌های شایع در سال ۲۰۰۶ ایمیل‌های گروهی بودند، از قبیل Win32/ Wukill و Win32/Bagle، که با فرستادن ایمیل‌هایی از کپی خود بر کامپیوترهای آلوده پخش می‌شدند.

یک جفت از backdoor های شایع از خانواده botnet بودند که شامل Win32/Rbot و Win32/Sdbot می‌شدند. انواع دیگر این خانواده‌ها از ساختار کیت batnet ساخته شده‌اند که در بازار زیرزمینی نرم‌افزارهای مخرب معامله می‌شوند و در کنترل کامپیوترهای آلوده در Internet Relay Chat یا همان (IRC) استفاده می‌شود.

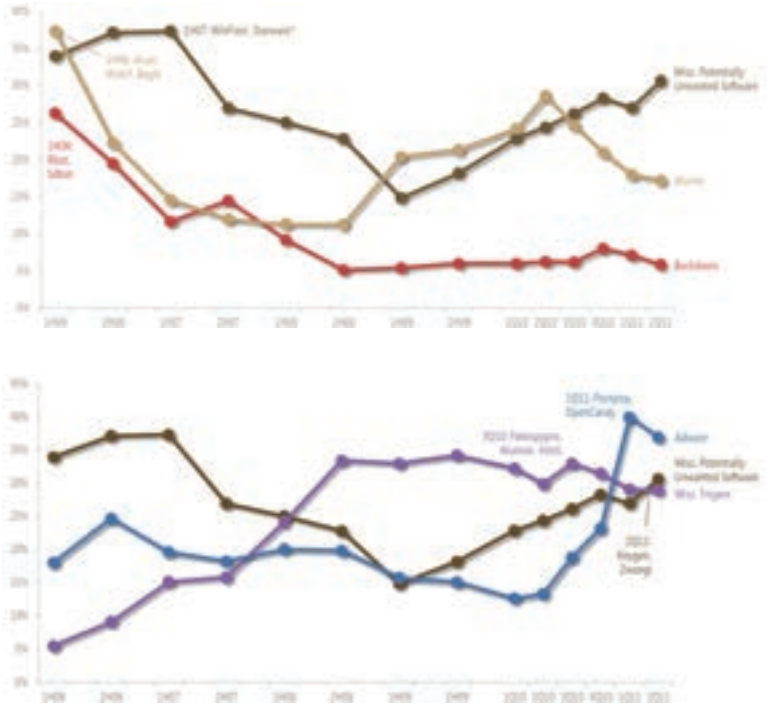
از تروجاه‌های شایع در سال‌های ۲۰۰۶ و ۲۰۰۷ Win32/WinFixer بود، و دیگری از همین خانواده Win32/Starware نام داشت که از نرم‌افزار سرگردان بود که به هر سوراخی وارد می‌شد، راه ورود اصلی آن به سیستم قربانی نیز از طریق نوار ابزار مرورگر اینترنت بود.

نرم‌افزارهای تبلیغاتی مزاحم، نرم‌افزار متفرقه ناخواسته و دسته‌ای از تروجان‌های متفرقه، معمول‌ترین طبقه‌بندی کشف شده در سال ۲۰۱۰ و ۲۰۱۱ بودند. کشف نرم‌افزارهای تبلیغاتی مزاحم به طور قابل توجهی در 1H11 افزایش یافت، از جمله خانواده‌های نرم‌افزارهای تبلیغاتی می‌توان از Win32/OpenCandy و JS / Pornpop نام برد که بیشترین شیوع را در بین این دسته داشتند.

خانواده‌های قابل توجه در این رده در 2Q11 نیز Win32/Keygen بودند، کشفی عمومی برای ابزارهایی که رمز عبور محصولات نرم‌افزاری را برای نسخه‌های غیرقانونی ایجاد می‌کردند و Win32/ Zwangi برنامه‌ای است که به عنوان یک سرویس در پس زمینه سیستم عامل اجرا می‌شود و به گونه‌ای ماهرانه تنظیمات مرورگر وب را برای بازدید از یک وب سایت خاص تغییر می‌دهد.

شماری از نرم‌افزارهای مخرب امنیتی که به آنها مخرب سرگردان نیز گفته می‌شود در دسته پایانی قرار می‌گیرند مانند Win32/ FakeSpyPro، که جزو شایع‌ترین خانواده نرم‌افزار امنیتی در سال ۲۰۱۰ بودند.

دیگر خانواده‌های شایع در این دسته عبارتند از Win32/Alureon، تروجان دزد داده‌ها، و Win32/Hiloti، که هر دو آنها از طریق مرورگر به سیستم کاربر وارد می‌شدند و فایل‌های دلخواه را دانلود و یا اجرا می‌کردند.



نسل جدید
راهکارهای امنیتی

KASPERSKY

راهکارهای امنیتی هوشمندانه برای مقابله
با جدیدترین تهدیدات امنیتی را با محصولات
تخصصی کسپرسکی تجربه کنید

- فناوری حفاظت چند لایه
- ابزارهای قدرتمند کنترل نقاط پایانی
- مدیریت تعاملی و دوطرفه
- پشتیبانی از سکوهای کاری چند گانه
- پشتیبانی از فناوری ابری

KASPERSKY
DISTRIBUTOR

تجارت امن
IT SECURITY SOLUTIONS

تهران، خیابان ولیعصر، نرسیده به میدان ونک، کوچه سیدالشهدا، پلاک ۳، طبقه ۴
تلفن: ۲۹-۸۸۲۰۱۴۲۸ فکس: ۸۸۶۴۲۸۸۷ / www.tejarateamn.com

تجارت امن، اولین توزیع کننده ایرانی و (کامگارد) تنها مرکز مجاز آموزش لابراتوار کسپرسکی در آسیای غربی ✣ جهت اخذ نمایندگی با ما تماس بگیرید