ویرایش اول: ۹ خرداد ۱۳۹۱

گزارش فنی

ویروس Wiper

شرکت McAfee با انتشار گزارش اولیه ای درباره ویروس Wiper یا Flame جزئیات کامل و دقیقی را از این ویروس مخرب ارائه کرد.

سوم اردیبهشت ماه سالجاری شاهد حمله سایبری به شبکه اینترنت و مخابرات وزارت نفت بودیم که خیلی زود، مشابهت این حملات جدید با حملات Stuxnet و Duqu مطرح گردید.

هفتم اردیبهشت نیز مرکز ماهر اطلاعات بیشتری درباره این حملات سایبری و بدافزاری که Flame نامیده شد، منتشر کرد.

در مشاهدات و گزارشات اولیه درباره این بدافزار از نام Viper یا Wiper استفاده شده است.

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

برای بررسی دقیق عملکرد ویروس های Stuxnet و Duqu ماه ها وقت صرف شد ولی در نگاه اول، پیش بینی می شود که بررسی و کسب اطلاعات دقیق درباره ویروس SkyWiper بسیار دشوارتر بوده و زمان بیشتری نیاز داشته باشد. برای نمونه، یکی از بخش های کوچک و رمزگذاری شده بدافزار SkyWiper حاوی بیش از ۷۰ هزار سطر برنامه نویسی به زبان C است که شامل بیش از ۱۷۰ عبارت (string) رمزگذاری شده، می باشد.

به نظر می رسد که این بدافزار طی چندین سال توسط یک گروه برنامه نویسی حرفه ای طراحی و تهیه شده است. اکنون با بررسی گزارش های برخی شرکت های امنیتی و فایل های Log منتشر شده در تالارهای گفتگو (Forums)، علائمی از فعالیت این بدافزار در سال های گذشته (حدود سال ۲۰۱۰ میلادی) در ایران و چند کشور اروپایی مشاهده شده است.

بر خلاف ویروس های رایج امروزی، این بدافزار به کندی از طریق حافظه های USB Flash انتشار می یابد تا جلب توجه نکرده و به عنوان یک رفتار مخرب توسط ابزارهای امنیتی شناسایی نشود.

برخی از فایل های مرتبط با ویروس SkyWiper در ظاهر متعلق به شرکت مایکروسافت می باشد. بعنوان مثال، یک فایل در ظاهر Windows Authentication Client نسخه 5.1 و شماره ساخت (Build) ۲۶۰۰ و متعلق به Microsoft Corporation است. ولی بررسی دقیق تر نشان می دهد که مانند ویروس های Stuxnet و Duqu هیچیک از فایل های بدافزار SkyWiper دارای Authentication Key معتبر نیستند.

مرکز کنترل و فرماندهی SkyWiper قادر است، نام و پسوند فایل های مخرب و مرتبط با این بدافزار را تغییر دهد. حتی تنظیمات مورد استفاده این فایل ها هم قابل تغییر هستند. بدین نحو، بدافزار SkyWiper می تواند خود را از دید ابزارهای امنیتی و از جمله ضد ویروس ها مخفی نگه دارد.

در حال حاضر به غیر از برخی شباهت ها در نحوه رمزگذاری فایل ها، نقطه مشترکی بین SkyWiper و ویروس های 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، پروژه های مشابهی بوده اند که در سال های گذشته به طور موازی اجرا شده اند.

اندازه برنامه اصلی SkyWiper بیش از ۶ مگابایت است و مجموعه کامل برنامه های این بدافزار حدود ۲۰ مگابایت فضا اشغال می کنند. این حجم زیاد برای این بدافزار کمی تعجب آور است. کاربران با تجربه می دانند که ویروس نویسان برای انتشار راحت تر فایلهای مخرب، اندازه فایلها را کم نگه می دارند. اما ساختار پیچیده این بدافزار نیاز به کتابخانه های پیچیده ای همچون Zlib، مفسر LUA و ... دارد که باعث ایجاد این حجم زیاد می شود.

آخرین تغییرات در فایل های بدافزار SkyWiper مربوط به بیش از یکسال گذشته (حدود زمستان ۸۹ و تابستان ۹۰) می شود. گر چه در برخی فایلها به طور دستی، تاریخ ها از ۲۰۱۱ به ۱۹۹۴ تغییر داده شده اند.

بر اساس اطلاعات جمع آوری 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 آلودگی ها در نقاط دیگر به غیر از اهداف اصلی ایجاد می گردد. در مراحل بعدی، SkyWiper از این نقاط آلوده به عنوان مرکز کنترل و فرماندهی استفاده می کنند. یقیناً در بررسی و تحقیقات بعدی، توجه به این نکته بسیار ضروری است.

ضد ویروس McAfee با آخرین فایل های به روز رسانی DAT، قادر به شناسایی بدافزار SkyWiper می باشد. اطلاعات و مشاهدات فعلی نشان می دهد که چندین گونه مختلف در این بدافزار وجود دارد.

اطلاعات فنی

این بدافزار که توسط ضدویروس McAfee با نام SkyWiper شناسایی می شود، 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، برنامه های 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 سیستم ها از طریق حافظه های USB و شبکه های محلی**
- **تصویر برداری از فعالیت های کاربر**
- **شنود و ضبط تماسهای صوتی برقرار شده از طریق سیستم آلوده**
- **قابلیتهای اجرا بر روی سیستم های عامل XP، Vista و Win 7**
- **سوء استفاده از ضعف های امنیتی سیستم عامل همچون Print Spooler و فایلهای lnk**
- **استفاده از بانک داده SQLite برای ذخیره اطلاعات جمع آوری 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

برنامه اصلی بدافزار از طریق مسیر زیر در محضرخانه (Registry) اجرا می گردد.

HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Authentication Packages

این بدافزار فایلهای زیر را نیز ایجاد می کند.

~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 گونه های متعددی می باشد، توصیه می شود که فایلهای ذکر شده فوق، در بخش Access Protection ضدویروس McAfee VirusScan مسدود شوند.
در صورت مشاهده نمونه ای ناشناس، لطفا آنرا در اسرع وقت از طریق http://help.shabakeh.net به شبکه گستر ارسال نمایید. همچنین با توجه به اهمیت موضوع ممکن است نیاز به استفاده از فایل های موقت شناسایی (Extra DAT) باشد که در اینصورت هشدارهای لازم به مشترکین ارسال خواهد گردید.

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

در صورت نیاز به اطلاعات بیشتر می توانید با گروه پشتیبانی شبکه گستر تماس حاصل نمایید.