به نام خدا

عنوان مقاله:

Stuxnet : look what we can do !

نویسنده: محمد مهدی واعظی نژاد
متخصص امنیت شبکه (مورد تأیید FBI)

استفاده از مطالب این مقاله به هر نحو ممکن ، بدون ذکر نام نویسنده شرعاً حرام است.

مقدمه

" Stuxnet " کرم اینترنتی که آرام و بی صدا در دل صنعت ایران می خزید و قلب تپنده صنایع تولیدی کشورمان را نشانه رفته بود، یکدفعه با کشف ناگهانی اش آنچنان هیاهویی برپا کرد که در کمتر از چند دقیقه به عنوان اول اغلب خبرگزاری های مهم بین المللی همچون CNN[1] ، Reuters[2] و Washington Post[3] تبدیل گردید.

محققان مراکز امنیتی هم با اظهار نظرهایی سریع، سعی در تشریح این کرم داشته و شرکت امنیتی Symantec اعلام می کند که رایانه های ایران مورد هجوم شدید کرم خطرناکی به نام Stuxnet قرار گرفته اند که اطلاعات سیستم های کنترل صنعتی[4] را سرقت کرده و بر روی اینترنت قرار می دهد.

محمود لیالی رئیس شورای فناوری اطلاعات وزارت صنایع و معادن کشورمان نیز علاوه بر اینکه هدف گیری این کرم را در راستای جنگ الکترونیکی علیه ایران می داند، از شناسایی شدن ۳۰ هزار IP صنعتی آلوده به این کرم در ایران خبر داده است.

Stuxnet، نخستین کرم صنعتی جهان است که با هدف حمله سایبری به زیرساخت های حیاتی صنعت ایران، آسیب به تأسیسات هسته ای نطنز و در نهایت، تأخیر در راه اندازی نیروگاه اتمی بوشهر طراحی و منتشر شده است.

این کرم قادر به ایجاد اخلال در تجهیزات حساس مانند تخریب سرعت چرخش روند بالا از آرایه های سانتریفیوژ و کاهش تعداد سانتریفیوژهای غنی عملیاتی، کنترل فعالیت های صنعتی، محدودیت دور توربین، روغن کاری و یا بستن سیستم های خنک کننده، تخریب لوله های گاز و حتی انفجار دیگ های بخار کارخانجات مختلف است.

سایر نام ها

این کرم در شرکت های امنیتی، به نام های زیر شناخته می شود:

Troj/Stuxnet-A [Sophos], W32/Stuxnet-B [Sophos], W32.Temphid [Symantec], WORM_STUXNET.A [Trend], Win32/Stuxnet.B [Computer Associates], Trojan-Dropper:W32/Stuxnet [F-Secure], Stuxnet [McAfee], W32/Stuxnet.A [Norman], Rootkit.Win32.Stuxnet.b [Kaspersky], Rootkit.Win32.Stuxnet.a [Kaspersky]

سیستم های آسیب پذیر

Microsoft Windows 2000 , Windows 95 , Windows 98 , Windows Me , Windows NT , Windows Server 2003 , Windows Vista , Windows XP on 32-bit Platforms

پراکنش جغرافیایی

Stuxnet برای حمله به نقاط جغرافیایی خاص، طراحی و منتشر شده است. علاوه بر ایران، کشورهای اندونزی و هند نیز مورد هجوم این نرم افزار مخرب قرار گرفته اند.

خبرگزاری چین هم در خبری اعلام کرده است که: " Stuxnet در بیش از شش میلیون رایانه چینی نفوذ کرده و مقامات پکن نگران هستند این کرم رایانه های بیشتری را در چین مورد حمله قرار دهد ".

تاریخچه کشف

بیست و دوم تیرماه سال جاری[5]، شرکت امنیتی VirusBlockAda بلاروس، نخستین بار Stuxnet را در رایانه یکی از مشتریان ایرانی خود مشاهده و کشف نمود.

این موضوع، در تاریخ بیست و چهارم تیرماه هم توسط شرکت زیمنس[6] آلمان گزارش گردید و یک ماه بعد، هنگامی که شرکت مایکروسافت[7] تأیید کرد که این کرم در حال هدف قرار دادن سیستم های ویندوز در مدیریت سیستم های کنترل صنعتی بزرگ موسوم به SCADA[8] است، به شهرت رسید.

اگرچه متخصصان امنیت هنوز در مورد زمان آغاز به کار Stuxnet اتفاق نظر ندارند ولی به گفته " الیاس لووی " مدیر ارشد فنی بخش " پاسخگویی ایمنی سایمنتک " با توجه به تاریخ نشانه های دیجیتالی که از این کرم رایانه ای به جا مانده، می توان گفت که از دی ماه ۱۳۸۸ این کرم میان رایانه ها در گردش بوده و ماه ها بدون شناسایی شدن به کار خود ادامه داده است.

نامگذاری

فایل ایجاد شده توسط Stuxnet از نام MYRTUS برای نفوذ در رایانه ها استفاده می کند. میرتاس کلمه ای با ریشه عبری است که اشاره به داستان " استر " دارد. استر، زن دوم خشایار شاه در ایران باستان است که زنی یهودی بوده و با وساطت عموی خود مردخاوی که از مشاوران پادشاه ایران بود، خشایار راضی به ازدواج با او می شود. بر این اساس، استر ملکه یهودیان شناخته می شود.

علاوه بر این، MYRTUS ممکن است به قطعات معروف به RTU[9] که یکی از ویژگی های مدیریت سیستم های SCADA است اشاره داشته باشد. همچنین عدد ۱۹۷۹۰۵۰۹ در درون کد این کرم، شاید بیانگر تاریخ ۹ مه ۱۹۷۹ یعنی روز "Habib Elghanian"، یک یهودی فارسی که در تهران اعدام شد نیز باشد.

طراحی و سازماندهی

Stuxnet که تقریباً نیم مگابایت حجم دارد به چندین زبان مختلف از جمله C، C++ و سایر زبان های شیء گرا نوشته شده است. این کرم، چنان در استفاده از آسیب پذیری های اصلاح نشده ویندوز ماهر است که کارشناسان امنیت معتقدند تیمی متشکل از متخصصانی با پشتوانه قوی و دارای انواع تخصص ها از Rootkit گرفته تا Database، آن را ایجاد کرده و هدایت می کنند. Symantec هم تخمین می زند که پنج تا ده نفر، شش ماه روی این پروژه کار کرده اند.

محققان Symantec و Kaspersky اعتقاد دارند با توجه به شناسایی کاملی که این کرم انجام می دهد، پیچیدگی کد و خطرناک بودن حمله آن، صرفاً نمی تواند کار یک گروه حرفه ای هک خصوصی باشد.

به نظر آن ها، منابع و هزینه های مورد نیاز برای انجام این حمله به همراه ریسک بالایی که پروژه در پی داشته است، آن را خارج از قلمرو یک گروه هک خصوصی قرار داده و تنها دولت ملی می تواند توانایی های آن را داشته باشد. همچنین، تیم ایجادکننده کرم به سخت افزار فیزیکی واقعی نیز برای تست نیاز داشته اند.

متخصصان با در نظر گرفتن تمامی شرایط، محتمل ترین سناریو در مورد این کرم را یک گروه هک وابسته به سرویس جاسوسی یک کشور می دانند. گمانه های موثق نیز حاکی از آن است که Stuxnet برای مقابله با برنامه های هسته ای نیروگاه بوشهر، توسط اسرائیل طراحی و به وسیله لپ تاپ پیمانکاران روسی در بوشهر، به تأسیسات هسته ای ایران منتقل شده است.

اگرچه این موضوع هنوز توسط دولت اسرائیل تأیید و اثبات نشده است اما اطلاع از آن می تواند اقدامات پیشگیرانه ایران برای مقابله با سایر روش های جاسوسی را با آگاهی بیشتری همراه کند.

عملکرد

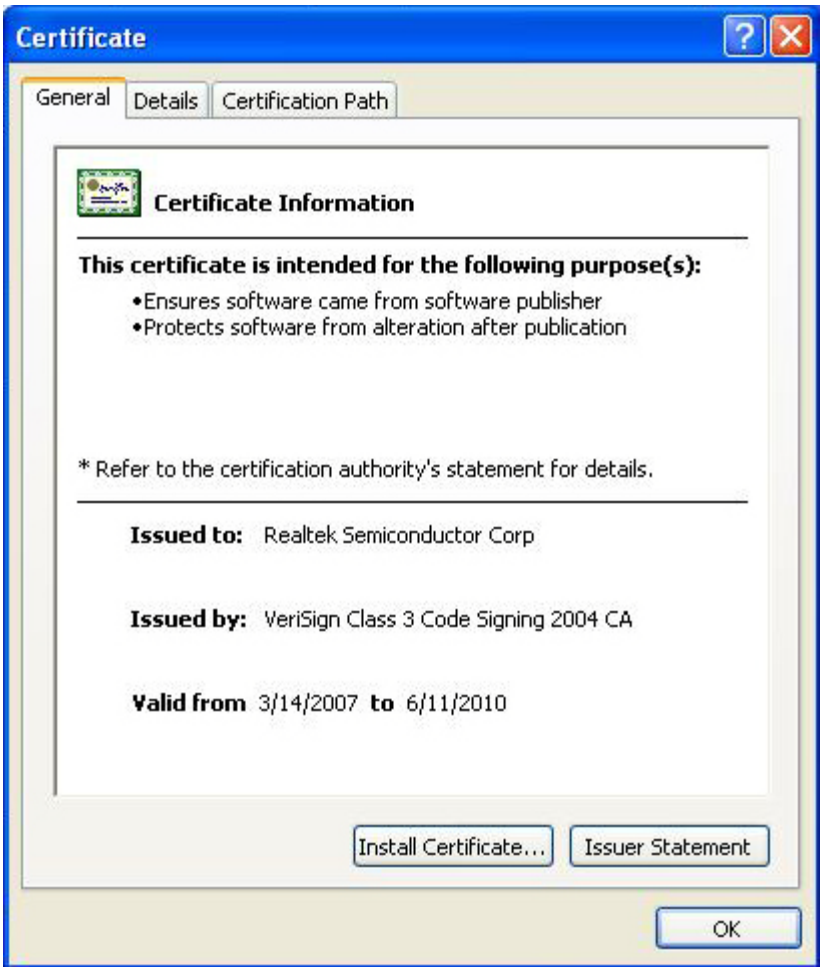
محققان ابتدا فکر می کردند که Stuxnet فقط از یک آسیب پذیری اصلاح نشده ویندوز سوء استفاده می کند[۱۰] و از آن به عنوان کرم نفوذ کننده از میان برهای ویندوز نام می بردند.

متخصصان Symantec و Kaspersky برای به دست آوردن اطلاعات بیشتر، کد این کرم را مورد بررسی و تحلیل عمیق تر قرار دادند. نخست در مدت یک هفته تا یک هفته و نیم، حفره Print spooler[۱۱] توسط محققان Kaspersky پیدا شده، سپس حفره EoP[۱۲] (تغییر حق دسترسی) ویندوز هم توسط این شرکت امنیتی کشف و حفره دوم EoP نیز توسط کارشناسان مایکروسافت شناسایی گردید. محققان Symantec هم به طور جداگانه آسیب پذیری Print spooler و دو آسیب پذیری EoP را در مرداد ماه پیدا کرده و کدهای مخربی که این سه آسیب پذیری اصلاح نشده ویندوز را هدف قرار می دهد، شناسایی نمودند.

اما عجایب Stuxnet که همزمان می تواند از چهار نقص امنیتی اصلاح نشده ویندوز، برای دسترسی به شبکه ها سوء استفاده کند به اینجا ختم نمی شود. این کرم همچنین از یک حفره ویندوز[۱۳] که در سال ۲۰۰۸ توسط به روز رسانی MS08-067 اصلاح شده بود نیز استفاده می کند. این نقص امنیتی همان آسیب پذیری مورد استفاده کرم Conficker در اواخر سال ۲۰۰۸ و اوائل سال ۲۰۰۹ بود که به میلیون ها سیستم در سراسر جهان آسیب وارد کرد.

هنگامی که Stuxnet از طریق درایو USB آلوده وارد یک شبکه می شود، با سوء استفاده از آسیب پذیری های EoP حق دسترسی Admin به سایر pcها را برای خود ایجاد کرده و سیستم هایی که برنامه های مدیریت Siemens SIMATIC WinCC و pcs 7 scada را اجرا می کنند پیدا می کند. سپس کنترل آن ها را با سوء استفاده از یکی از آسیب پذیری های Print spooler یا MS08-067 در دست گرفته و رمز عبور پیش فرض زیمنس را برای در اختیار گرفتن نرم افزار SCADA آزمایش می کند[۱۴]. بعد، کد خودش را همچون یک Rootkit درون PLC[۱۵] بارگزاری و پنهان می کند تا قابل مشاهده نباشد. آنگاه نرم افزار PLC را دوباره برنامه ریزی کرده و دستورات جدید را طبق اهداف خود صادر می نماید.

نکته قابل توجه این است که Stuxnet برای قانونی نشان دادن کدهای حمله خود و اعتباردهی به درایوهایش، دو گواهی معتبر دیجیتالی امضاء شده Realtek و JMicron را سرقت می کند:



نصب

هنگامی که یک درایو USB آلوده به کامپیوتر وصل می شود، Stuxnet خودش را به عنوان فایل های زیر به کامپیوتر غیرآلوده کپی می کند:

%System%\drivers\mrxcls.sys
%System%\drivers\mrxnet.sys

سپس فایل mrxcls.sys را به عنوان یک سرویس با مشخصات زیر ثبت می کند:

Display Name: MRXCLS
Startup Type: Automatic
Image Path: %System%\drivers\mrxcls.sys

آنگاه برای این سرویس، مسیر زیر را در registry ایجاد می کند:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\"ImagePath" = "%System%\drivers\mrxcls.sys"

این کرم، همچنین فایل mrxnet.sys را به عنوان یک سرویس با مشخصات زیر ثبت می کند:

Display Name: MRXNET
Startup Type: Automatic
Image Path: %System%\drivers\mrxnet.sys

برای سرویس بالا نیز، مسیر زیر را در registry ایجاد می کند:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\"ImagePath" = "%System%\drivers\mrxnet.sys"

این کرم، همچنین فایل های زیر را که هر کدام نسخه های رمز شده Stuxnet هستند، ایجاد می کند:

- %Windir%\inf\oem6C.PNF
- %Windir%\inf\oem7A.PNF
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\mdmeric3.PNF

در ضمن، اگر کرم از روی سیستم آلوده پاک شود، فایل %System%\drivers\mrxcls.sys فایل های بالا را برای تأثیرگذاری مجدد در کامپیوتر رمزگشایی می کند.

تغییرات در سیستم

فایل(های) زیر ممکن است در کامپیوتر آلوده دیده شود:

- %System%\drivers\mrxcls.sys
- %System%\drivers\mrxnet.sys
- %DriveLetter%\~WTR4132.tmp
- %DriveLetter%\~WTR4141.tmp
- %DriveLetter%\Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Copy of Shortcut to.lnk
- %Windir%\inf\oem6C.PNF
- %Windir%\inf\oem7A.PNF
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\mdmeric3.PNF

این کرم فایلی را از سیستم، پاک و یا اصلاح نکرده و در Registry سیستم آلوده نیز به جز ایجاد دو مسیر زیر، هیچ کدام از Subkeyها حذف یا تغییر دیگری صورت نمی گیرد:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\"ImagePath" = "%System%\drivers\mrxcls.sys"

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\"ImagePath" = "%System%\drivers\mrxnet.sys"

دو پردازش زیر در سیستم ایجاد می شود:

- iexplorer.exe
- lsass.exe

Stuxnet یک بسته قابل اجرا در کامپیوتر را از سرور C&C خود دانلود و اجرا نموده و همچنین اطلاعاتی را از طریق HTTP به آدرس زیر ارسال می کند:

http://[C&C SERVER ADDRESS]/index.php?data=[DATA]

DATA شامل اطلاعات زیر است:

- نسخه سیستم عامل ویندوز
- نام کامپیوتر
- نام گروه شبکه
- نشانه برای آگاهی از نصب بودن نرم افزار SCADA
- آدرس IP همه کارت های شبکه موجود

این اطلاعات با استفاده از یک کلید ۳۱ بایتی XOR رمزگذاری و ارسال می شود. پاسخ دریافت شده از سرور C&C هم با XOR اما توسط یک کلید ۳۱ بایتی متفاوت رمزنگاری شده که هر دو این کلیدها در فایل های dll. قرار داده شده در سیستم آلوده موجود است.

با اتصال کامپیوتر به اینترنت، کرم از طریق پورت ۸۰ با سایت های زیر که سرورهای C&C آن هستند، ارتباط برقرار می کند:

- www.mypremierfutbol.com
- www.todaysfutbol.com

سرور C&C پس از دریافت این اطلاعات، به دو روش می تواند پاسخ دهد: نوع نخست پاسخ، دستورالعمل کرم برای اجرای یکی از شیوه های موجود در کد تهدیدات آن است و نوع دوم پاسخ، یک فایل dll. به سیستم آلوده ارائه و به بارگزاری آن دستور می دهد.

از پاسخ نوع اول به عنوان پوششی برای RPC[۱۶] ها که می خواهد به سیستم فرستاده شود، استفاده می شود. RPC پس از فراخوانی شدن در کامپیوتر می تواند اقدامات زیر را انجام دهد:

- خواندن فایل
- نوشتن در فایل

- حذف فایل
- ایجاد پردازش
- تزریق یک فایل dll. به lsass.exe
- بارگزاری و اجرای یک فایل dll. اضافه
- استخراج منبع ۲۱۰ از فایل dll. اصلی (از این منبع برای تزریق به پردازش های دیگر استفاده می شود.)
- به روز رسانی پیکربندی اطلاعات کرم

این کرم پس از نفوذ به شبکه، فقط کامپیوترهایی که نرم افزار SCADA شرکت زیمنس برای کنترل و مدیریت فعالیت ها در آن ها نصب شده است را هدف قرار می دهد. سپس برای به دست آوردن اطلاعات مشخصی، تعداد زیادی querie در پایگاه داده نرم افزار Siemens Step 7 انجام داده و با فایل های dll. نرم افزار تعامل برقرار می کند. آنگاه تلاش می کند به فایل های زیر که توسط نرم افزار Step 7 ایجاد شده اند دسترسی یافته تا کد آن ها را برای طراحی پروژه ها سرقت کند:

- GracS\cc_tag.sav
- GracS\cc_alg.sav
- GracS\db_log.sav
- GracS\cc_tlg7.sav
- *.S7P
- *.MCP
- *.LDF

Stuxnrt همانند یک Rootkit کد خودش را به PLC در یک سیستم کنترل صنعتی که توسط سیستم های SCADA نظارت می شود، تزریق و پنهان می کند. PLC کامپیوتری است که از ویندوز برنامه ریزی شده تشکیل شده و حاوی کد ویژه ای می باشد که اتوماسیون فرآیندهای صنعتی را کنترل می کند.

این کرم که با نوشتن کد در PLC ، سیستم را کنترل کرده و یا فعالیت های آن را به تعویق می اندازد، برای جلوگیری از تشخیص فایل %DriveLetter%\~WTR4132.tmp آن را با رابط های برنامه های کاربردی (API) زیر از kernel32.dll و Ntdll.dll مرتبط می کند:

از Kernel32.dll :

- FindFirstFileW
- FindNextFileW
- FindFirstFileExW

از Ntdll.dll :

- NtQueryDirectoryFile
- ZwQueryDirectoryFile

کرم کد اصلی این توابع را هم با کدی که برای چک کردن فایل ها با مشخصات زیر است، جایگزین می کند:

- نام فایل با پسوند ".lnk"
- آغاز نام فایل با "~WTR" و با پسوند ".tmp"

آنگاه فایل %DriveLetter%\~WTR4132.tmp به فایل dll. دیگری به نام %DriveLetter%\~WTR4141.tmp بارگزاری می شود. Stuxnet برای انجام این کار، از رویکردی متفاوت استفاده کرده و به جای اینکه "LoadLibrary" رابط های برنامه های کاربردی را برای بارگزاری فایل dll. در حافظه اصلی فراخوانی کند، توابعی را به Ntdll.dll مرتبط کرده و سپس "LoadLibrary" را با نام فایل خاصی که ایجاد شده است، فراخوانی می کند. این فایل درخواست شده برای بارگزاری، در disk وجود ندارد اما توابع مرتبط شده به Ntdll.dll که به بارگزاری نام خاص فایل برای درخواست ها نظارت دارد، فایل dll. را از یک ناحیه در حافظه اصلی که قبلاً در آن رمزگشایی و ذخیره شده است، بارگزاری می کند. توابع مرتبط شده در Ntdll.dll برای این منظور عبارتند از:

- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwCloseFile
- ZwQueryAttributesFile
- ZwQuerySection

سپس فایل dll. فراخوانی شده و کنترل سیستم را در دست می گیرد. این کرم کد خود را نیز به iexplorer.exe به منظور دور زدن[۱۷] فایروال ها تزریق کرده و فرآیندهای امنیتی زیر را به پایان می رساند:

- vp.exe
- Mcshield.exe
- avguard.exe
- bdagent.exe
- UmxCfg.exe
- fsdfwd.exe
- rtvscan.exe
- ccSvcHst.exe
- ekrn.exe
- tmpproxy.exe

انتشار

Stuxnet با کپی کردن خودش در درایوهای USB، Emailهای آلوده و یا فایل های به اشتراک گذاشته شده در شبکه های رایانه ای که دارای نقاط آسیب هستند، منتشر می شود.

این کرم خودش را به عنوان فایل های زیر در درایوهای قابل جابجایی کپی می کند که هر دو نام فایل، hardcoded و در واقع فایل های dll. هستند:

- %DriveLetter%\~WTR4132.tmp
- %DriveLetter%\~WTR4141.tmp

همچنین فایل های زیر را به درایوهای بالا کپی می کند:

- %DriveLetter%\Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Copy of Shortcut to.lnk

هنگامی که این درایوها با برنامه ای که توانایی نمایش آیکون ها را دارد (مانند Windows Explorer) مورد دسترسی قرار می گیرد، به جای نمایش آیکون برای فایل های lnk. کدی را که قابلیت اجرای فایل %DriveLetter%\~WTR4132.tmp را دارد، اجرا می کند. هدف اصلی این فایل، اجرای فایل DriveLetter%\~WTR4141.tmp است که در درایوهای قابل جابجایی کپی شده و سپس در حافظه اصلی سیستم بارگزاری می شود. این فایل است که دو گواهی معتبر امضاء شده Realtek و JMicron را جعل می کند.

این کرم همچنین از یک کد مخرب RPC هم برای منتشر شدن استفاده می کند[۱۲]. علاوه بر این، از کد مخرب دیگری [۱۱] نیز که اجازه می دهد یک فایل به شاخه %System% کامپیوتر آسیب پذیر نوشته شود، برای کپی نمودن خودش از کامپیوتر آلوده به سایر کامپیوترها استفاده کرده و برای اجرای آن فایل از راه دور هم از یک ویژگی WBEM بهره می برد.

Stuxnet همچنین با کپی نمودن خودش به منابع اشتراک گذاشته شده در شبکه به عنوان فایل زیرکه در حقیقت یک فایل dll. است، منتشر می شود:

%DriveLetter%\ “DEFRAG[RANDOM NUMBER].tmp

البته یک راه که مهاجمان با استفاده از آن ریسک شناسایی شدن و جلوگیری از گسترش بیش از اندازه این کرم را کم کرده اند، قرار دادن یک شمارنده در درایو USB آلوده است که اجازه انتشار کرم از طریق یک داریو USB خاص به بیش از سه کامپیوتر را نداده و بعد از ۲۱ روز نیز خودش را پاک می کند.

نکته قابل توجه در خصوص Stuxnet آن است که درون کد پیچیده آن مشخص شده که این کرم در تاریخ ۲۴ ژوئن ۲۰۱۲ انتشار خود را متوقف کرده و خودش را نیز از سیستم آلوده پاک خواهد نمود.

جلوگیری

شرکت مایکروسافت در روز یازدهم مرداد ماه سال جاری، یک به روز رسانی مهم و فوری برای اصلاح نقص ابتدایی Stuxnet عرضه کرد[۱۸]. سپس شرکت های Symantec و Kaspersky نتایج تحقیقات خود را به شرکت مایکروسافت گزارش کردند که

باعث شد آسیب پذیری Print spooler به سرعت اصلاح شده[۱۹] و وعده اصلاح دو آسیب پذیری کم خطرتر EoP هم در به روز رسانی امنیتی بعدی داده شود.

اگر چه هم اکنون تمامی آنتی ویروس ها قادر به شناسایی و پاک کردن این کرم هستند اما انجام فعالیت های زیر توسط همه مدیران و کاربران سیستم می تواند باعث جلوگیری و یا کاهش خطر این کرم شود:

- غیر فعال کردن ویژگی AutoRun یا AutoPlay سیستم برای جلوگیری از اجرای خودکار فایل های قابل اجرا در درایوهای قابل جابجایی.
- غیر فعال کردن درایوهای قابل جابجایی از طریق Setup سیستم. در صورت نیاز، فقط حالت read-only را فعال کرده و حتماً یک رمز عبور هم برای setup در نظر گرفت.
- اصلاح نقاط آسیب پذیر سیستم عامل و نرم افزارهای نصب شده.
- به روز رسانی نرم افزار آنتی ویروس در فاصله های زمانی کوتاه مدت و فعال کردن گزینه automatic updates برای دریافت خودکار آخرین updateها.
- Stuxnet با سوء استفاده از نقاط آسیب پذیر مشخصی انتشار پیدا می کند. نصب patcheهای زیر می تواند باعث کاهش خطر این کرم شود:

  - Microsoft Security Bulletin MS10-046
  - Microsoft Security Bulletin MS08-067
  - Microsoft Security Bulletin MS10-061

- دسترسی به آدرس های زیر که سرورهای C&C کرم هستند با استفاده از فایروال و Router باید مسدود شده و با اضافه کردن به فایل local hosts به آدرس 127.0.0.1 تغییر مسیر داده شود:

  - www.mypremierfutbol.com
  - www.todaysfutbol.com

- استفاده از رمز عبور پیچیده که ترکیبی از عدد، حروف بزرگ و کوچک و نمادها[۲۰] می باشد برای کلمه عبور کاربران، به نحوی که این رمزها توسط dictionary attackها به راحتی قابل شناسایی و کشف نبوده و در عین حال، برای کاربران هم به یاد ماندنی باشد.
- همه ارتباطات ورودی از اینترنت به سرویس های سازمان که نباید در دسترس عموم باشد را با استفاده از فایروال deny کرده و تنها به سرویس هایی اجازه دهید که به مردم خدمات ارائه می دهند.
- هرگز نباید با یوزر administrator یا root به سیستم login کرد. کاربران و برنامه ها هم باید پایین ترین سطح دسترسی لازم را داشته باشند.
- غیرفعال کردن اشتراک گذاری منابع و فایل ها در شبکه اگر به اشتراک گذاری آن ها نیازی نیست. در صورت نیاز، از ACL ها استفاده کرده و مشخص نمایید که چه افراد یا کامپیوترهایی اجازه دسترسی به آن ها را دارند.

- غیرفعال کردن و حذف سرویس های غیرضروری فعال در سیستم. اگر هم کد مخربی علیه یکی از سرویس ها پیدا شد، تا زمانیکه patch آن سرویس در سیستم نصب نشده است، آن سرویس را غیر فعال کرده و یا دسترسی به آن را محدود نمایید.
- سرویس هایی همچون HTTP، FTP، Mail و DNS مهمترین سرویس های یک شبکه متصل به اینترنت هستند. بنابراین، همیشه patchهای این سرویس ها را مهم درنظر گرفته و به روز نگهدارید. همچنین توسط فایروال، دسترسی به آن ها را کنترل نمایید.
- پیکربندی email سرور در جهت حذف نامه های الکترونیکی که حاوی فایل ضمیمه است. از این فایل ها برای گسترش تهدیداتی همچون vbs. ، bat. ، exe. ، pif. و scr. استفاده می شود.
- کامپیوترهای آلوده را به سرعت برای جلوگیری از گسترش بیشتر آلودگی در شبکه ایزوله کنید و تا زمانیکه از برطرف شدن آلودگی مطمئن نشده اید، آن ها را وارد شبکه نکنید.
- استفاده نکردن از Bluetooth در شبکه. در صورت نیاز، دید دستگاه را در حالت Hidden تنظیم کنید تا توسط دستگاه های دیگر پیدا نشده و حتماً از رمز عبور نیز برای برقراری ارتباط بین دستگاه ها استفاده کنید.

پیشگیری

پیشگیری از حوادث و کنترل امنیت سیستم نیاز به یک رویکرد چند لایه دارد که از آن با عنوان " دفاع در عمق " یاد می شود. این لایه، شامل سیاست ها و رویه ها، آگاهی و آموزش، تقسیم بندی شبکه، کنترل دسترسی ها، اقدامات امنیتی فیزیکی، سیستم های نظارتی همچون فایروال و آنتی ویروس، سیستم های تشخیص نفوذ (IDS)، رمز کاربری و ... است.

بهترین روش برای پیشگیری هم معمولاً تجزیه و تحلیل خطر، شناسایی نقاط آسیب پذیر سیستم ها و شبکه، کنترل سیستم ارزیابی امنیتی و همچنین توسعه برنامه های اولویت بندی برای از بین بردن یا به حداقل رساندن ریسک خطر است.

پانوشت ها:

1- September 24,2010 title: Cyberworm “targets Iran”
-October 5,2010 title: Stuxnet : Fact vs.Theory
2- September 24,2010 title: Cyber attack appears to target Iran-US tech firm
3- October 1,2010 title: U.S. power plants at risk of attack by computer worm like Stuxnet
4- Industrial Control Systems
5- July 13,2010
6- Siemens
7- Microsoft
8- Supervisory Control And Data Acquisition
9- Remote Terminal Units
10- Microsoft Windows Shortcut ‘LNK/PIF’ Files Automatic File Execution Vulnerability (BID 41732)
11- Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073)

12- Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874)
13- W32.Downadup (a.k.a Confiker)
14- Server = .\wincc -- vid = winccconect -- pwd = 2wsxcder
15- Programmable Logic Control
16- Remote Procedure Call
17- Bypass
18- Microsoft Security Bulletin MS10-046
19- Microsoft Security Bulletin MS10-061 (September 14,2010)
20- symbols

ارتباط با نویسنده:

همراه: **۰۹۱۲۳۹۶۳۱۲۷**

Mahdivaezi61@yahoo.com