آنچه که باید در مورد استاکس‌نت بدانید

محمد مهدی واعظی نژاد
Mahdivaezi61@yahoo.com

مقدمه

(استاکس‌نت)، کرم اینترنتی که آرام و بی‌صدا در دل صنعت ایران می‌خزید و قلب تپنده صنایع تولیدی کشورمان را نشانه گرفته بود، با کشف ناگهانی خود آن‌چنان هیاهویی برپا کرد که در کمتر از چند دقیقه به‌عنوان اولین خبر اغلب خبرگزاری‌های مهم بین‌المللی مانند CNN،Reuters و Washington Post تبدیل شد.

محققان مراکز امنیتی نیز با اظهارنظرهایی سریع، سعی در تشریح این کرم داشتند و شرکت امنیتی Symantec اعلام کرد که رایانه‌های ایران مورد هجوم شدید کرم خطرناکی به نام استاکس‌نت قرار گرفته‌اند و اطلاعات سیستم‌های کنترل صنعتی (Industrial Control Systems) توسط آن به سرقت می‌رود و روی اینترنت قرار می‌گیرد.

رئیس شورای فناوری اطلاعات وزارت صنایع و معادن کشورمان نیز علاوه‌بر این‌که هدف‌گیری کرم استاکس‌نت را در راستای جنگ الکترونیکی علیه ایران می‌داند، از شناسایی شدن ۳۰ هزار IP صنعتی آلوده به این کرم در کشور خبر داده است.

نام‌های دیگری برای Stuxnet

استاکس‌نت، نخستین کرم صنعتی جهان به‌شمار می‌آید که با هدف حمله سایبری به زیرساخت‌های حیاتی صنعت ایران، آسیب به تأسیسات هسته‌ای و در نهایت تأخیر در راه اندازی نیروگاه اتمی بوشهر طراحی و منتشر شده است.

این کرم قادر به ایجاد اخلال در تجهیزات حساس است که از آن نمونه می‌توان به تخریب در سرعت چرخش روند بالا از آرایه‌های سانتریفیوژ و کاهش تعداد سانتریفیوژهای غنی عملیاتی، کنترل فعالیت‌های صنعتی، محدودیت دور توربین، روغن‌کاری یا بستن سیستم‌های خنک‌کننده، تخریب لوله‌های گاز و حتی انفجار دیگ‌های بخار کارخانجات مختلف اشاره کرد.

این کرم در شرکت‌های امنیتی، به نام‌های زیر شناخته می‌شود:

- 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]

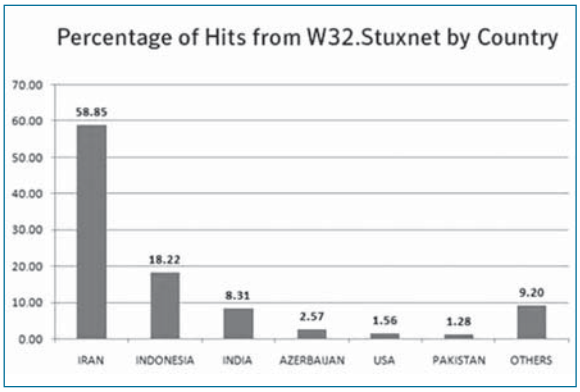
سیستم‌های آسیب‌پذیر

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

پراکنش جغرافیایی

استاکس‌نت 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 گرفته‌اند.

خبرگزاری چین نیز در خبری اعلام نمود: «استاکس‌نت در بیش



از شش میلیون رایانه چینی نفوذ کرده است و مقامات پکن نگران هستند که این کرم رایانه‌های بیشتری را در چین مورد حمله قرار دهد.»

تاریخچه کشف

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

این موضوع در تاریخ بیست و چهارم تیرماه نیز توسط شرکت زیمنس (Siemens) آلمان گزارش گردید و یک ماه بعد، هنگامی‌که شرکت مایکروسافت تأیید کرد که این کرم در حال هدف قراردادن سیستم‌های ویندوز در مدیریت سیستم‌های کنترل صنعتی بزرگی موسوم به SCADA (Supervisory Control And Data Acquisition) است، به شهرت رسید.

اگرچه متخصصان امنیت هنوز در مورد زمان آغاز به‌کار استاکس‌نت اتفاق‌نظر ندارند ولی به گفته مدیر ارشد فنی بخش پاسخگویی ایمنی Symantec با توجه به تاریخ نشانه‌های دیجیتالی که از این کرم رایانه‌ای مشاهده می‌شود، می‌توان گفت که از دی‌ماه ۱۳۸۸ میان رایانه‌ها در گردش بوده و ماه‌ها بدون شناسایی‌شدن به‌کار خود ادامه داده است.

نام‌گذاری

فایل ایجادشده توسط استاکس‌نت از نام Myrtus برای نفوذ در رایانه‌ها استفاده می‌کند. Myrtus، کلمه‌ای 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 به‌نام مردخای که از مشاوران پادشاه ایران بود، خشایار راضی به ازدواج با او می‌شود.

بر این اساس، استر ملکه یهودیان شناخته می‌شود. Myrtus ممکن است که به قطعات معروف (Remote Terminal Units) RTU که یکی از ویژگی‌های مدیریت سیستم‌های SCADA به‌شمار می‌رود، اشاره داشته باشد.

به‌علاوه عدد ۱۹۷۹۰۵۰۹ در درون کد این کرم، ممکن است تا بیانگر تاریخ ۹ می ۱۹۷۹ یعنی روز «Habib Elghanian» که یک یهودی فارسی که در تهران اعدام شد، باشد.

طراحی و سازماندهی

استاکس‌نت که تقریباً نیم مگابایت حجم دارد، به چندین زبان مختلف از جمله C، C++ و سایر زبان‌های شئ‌گرا نوشته شده است. این کرم چنان در استفاده از آسیب‌پذیری‌های اصلاح‌نشده ویندوز ماهر است که کارشناسان امنیت معتقدند تیمی متشکل از متخصصانی با پشتوانه قوی و دارای انواع تخصص‌ها از Rootkit گرفته تا Database، آن را ایجاد کرده و هدایت می‌کنند. Symantec نیز تخمین می‌زند که پنج تا ده نفر، شش ماه روی این پروژه کار کرده‌اند.

محققان Symantec و Kaspersky اعتقاد دارند تا با توجه به شناسایی کاملی که این کرم انجام می‌دهد، پیچیدگی کد و خطرناک‌بودن حمله آن صرفاً نمی‌تواند کار یک گروه حرفه‌ای نفوذگر خصوصی باشد.

به‌نظر آنها، منابع و هزینه‌های موردنیاز به همراه ریسک بالایی که پروژه در پی داشته است، آن را خارج از قلمرو یک گروه نفوذگرخصوصی قرار می‌دهد و تنها دولت ملی می‌تواند این توانایی‌ها را داشته باشد. به‌علاوه تیم ایجادکننده این کرم به سخت‌افزار فیزیکی واقعی برای تست نیز نیاز داشته‌اند.

متخصصان با در نظرگرفتن تمامی شرایط محتمل‌ترین سناریو در مورد این کرم را یک گروه نفوذگر وابسته به سرویس جاسوسی آن کشور می‌دانند. اخبار موثق نیز حاکی از آن هستند که استاکس‌نت برای مقابله با برنامه‌های هسته‌ای نیروگاه بوشهر طراحی و به وسیله لپ‌تاپ به تأسیسات هسته‌ای ایران منتقل شده است.

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

عملکرد

محققان ابتدا فکر می‌کردند که استاکس‌نت فقط از یک آسیب‌پذیری

اصلاح نشده ویندوز سوءاستفاده می‌کند و آن را کرم نفوذکننده از میانبرهای ویندوز نام می‌نامیدند. متخصصان Symantec و Kaspersky برای به‌دست‌آوردن اطلاعات بیشتر، کد این کرم را مورد بررسی و تحلیل عمیق‌تر قرار دادند. نخست در مدت یک هفته تا یک هفته و نیم، حفره Print Spooler توسط محققان Kaspersky پیدا شد و سپس حفره اول EOP (تغییر حق دسترسی) ویندوز به‌وسیله این شرکت امنیتی و حفره دوم EOP نیز توسط کارشناسان مایکروسافت شناسایی گردید. محققان Symantec نیز به‌طور جداگانه آسیب‌پذیری Print Spooler و دو آسیب‌پذیری EOP را در مرداد ماه پیدا نموده و کدهای مخربی که این سه آسیب پذیری اصلاح نشده ویندوز را هدف قرار می‌دهند، شناسایی نمودند.

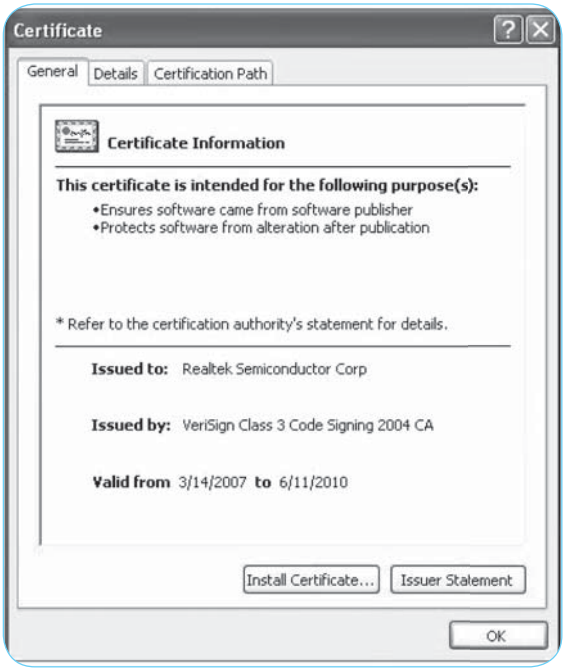
عجایب استاکس‌نت که همزمان می‌تواند از چهار نقص امنیتی اصلاح نشده ویندوز، برای دسترسی به شبکه‌ها سوءاستفاده کند، به اینجا ختم نمی‌شود.

این کرم همچنین از یک حفره ویندوز (w32.Downadup) که در سال ۲۰۰۸ توسط به‌روزرسانی MS08-067 اصلاح‌شده بود، نیز استفاده می‌کند. این نقص امنیتی همان آسیب‌پذیری مورداستفاده کرم Conficker در اواخر سال ۲۰۰۸ و اوایل سال ۲۰۰۹ بود که به میلیون‌ها سیستم در سراسر جهان آسیب وارد کرد.

هنگامی‌که استاکس‌نت از طریق درایو USB آلوده وارد یک شبکه می‌شود، با سوءاستفاده از آسیب‌پذیری‌های EOP حق دسترسی Admin به سایر PCها را برای خود ایجاد نموده و سیستم‌هایی که برنامه‌های مدیریت Siemens SIMATIC WinCC و PCS 7 SCADA را اجرا می‌کنند، پیدا می‌نماید.

حال کنترل آنها را با سوءاستفاده از یکی از آسیب‌پذیری‌های Print spooler یا MS08-067 در دست می‌گیرد و رمز عبور پیش‌فرض زیمنس را برای دراختیارگرفتن نرم‌افزار SCADA آزمایش می‌کند. سپس، کد خود را مانند یک Rootkit درون PLC (Programmable Logic Control) بارگذاری و پنهان می‌نماید تا قابل مشاهده نباشد. آنگاه نرم‌افزار PLC را دوباره برنامه‌ریزی نموده و دستورات جدید را طبق اهداف خود صادر می‌نماید.

نکته قابل توجه این است که استاکس‌نت برای قانونی نشان‌دادن کدهای حمله و اعتباردهی به درایوهای خود، دو گواهی معتبر دیجیتالی امضاشده Realtek و JMicron را سرقت می‌کند.



نصب

هنگامی‌که یک درایو USB آلوده به کامپیوتر وصل می‌شود، استاکس‌نت خود را به‌عنوان فایل‌های زیر به کامپیوتر غیرآلوده کپی می‌کند.

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

حال فایل mrxcls.sys را به‌عنوان یک سرویس با مشخصات زیر ثبت می‌کند.

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

آنگاه برای این سرویس، مسیر زیر را در Registry ایجاد می‌کند.

```
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 می‌کند.

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

برای سرویس بالا نیز مسیر زیر را در Registry ایجاد می‌کند.

```
HKEY_LOCAL_MACHINE\SYSTEM\
```

CurrentControlSet\Services\
MRxNet\»ImagePath» = «%System%\
drivers\mrxnet.sys"

این کرم همچنین فایل‌های زیر را که هر کدام نسخه‌های رمزشده استاکس‌نت هستند، ایجاد می‌کند.

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

درضمن، اگر کرم از روی سیستم آلوده پاک شود، فایل %System%\drivers\mrxcls.sys فایل‌های بالا را برای تأثیرگذاری مجدد در کامپیوتر رمزگشایی می‌کند.

تغییرات در سیستم

فایل‌های زیر ممکن است که در کامپیوتر آلوده دیده شوند.

- %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 یا اصلاح نکرده و در Registry سیستم آلوده نیز بجز ایجاد دو مسیر زیر، هیچ‌کدام از Subkeyها را حذف می‌کند یا تغییر دیگری صورت نمی‌دهد.

- 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 می‌شود.

- iexplorer.exe
- lsass.exe

استاکس‌نت یک بسته قابل اجرا در کامپیوتر را از سرور C&C خود بارگیری و اجرا نموده و اطلاعاتی را از طریق HTTP به آدرس زیر ارسال می‌نماید.

[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 نصب‌بودن نرم‌افزار SCADA
- آدرس IP همه کارت‌های شبکه موجود

این اطلاعات با استفاده از یک کلید ۳۱ بایتی XOR رمزگذاری و ارسال می‌شوند. پاسخ دریافت‌شده از سرور C&C نیز با XOR اما توسط یک کلید ۳۱ بایتی متفاوت رمزنگاری می‌گردد که هر دو این کلیدها در فایل‌های dll. قرارداده شده در سیستم آلوده موجود است.

با اتصال کامپیوتر به اینترنت، کرم از طریق پورت ۸۰ با سایت‌های زیر که سرورهای C&C آن هستند، ارتباط برقرار می‌کند.

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

سرور C&C پس از دریافت این اطلاعات، به دو روش می‌تواند پاسخ دهد. نوع نخست پاسخ، دستورالعمل کرم برای اجرای یکی از شیوه‌های موجود در کد تهدیدات آن است و نوع دوم پاسخ، یک فایل dll. به سیستم آلوده ارائه می‌گردد و به بارگذاری آن دستور می‌دهد.

از پاسخ نوع اول به‌عنوان پوششی برای RPCهایی (Remote Procedure Call) که می‌خواهند به سیستم فرستاده شوند، استفاده می‌گردد. RPC پس از فراخوانی‌شدن در کامپیوتر می‌تواند اقدامات زیر را انجام دهد:

- خواندن فایل
- نوشتن در فایل
- حذف فایل
- ایجاد پردازش
- تزریق یک فایل dll. به lsass.exe
- بارگذاری و اجرای یک فایل dll. اضافه

• استخراج منبع ۲۱۰ از فایل dll. اصلی که از این منبع برای تزریق به پردازش‌های دیگر استفاده می‌شود.

• به‌روزرسانی پیکربندی اطلاعات کرم

این کرم پس از نفوذ به شبکه، فقط کامپیوترهایی را که نرم‌افزار SCADA شرکت زیمنس برای کنترل و مدیریت فعالیت‌ها در آنها نصب شده است، هدف می‌گیرد؛ سپس برای به‌دست‌آوردن اطلاعات مشخصی، تعداد زیادی Query در پایگاه‌داده نرم‌افزار Siemens Step 7 انجام می‌دهد و با فایل‌های dll. نرم‌افزار تعامل برقرار می‌کند. آنگاه تلاش می‌کند تا به فایل‌های زیر که توسط نرم‌افزار Step 7 ایجاد شده‌اند، دسترسی بیابد تا کد آنها را برای طراحی پروژه‌ها سرقت نماید.

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

استاکس‌نت مانند یک Rootkit کد خود را به PLC در یک سیستم کنترل صنعتی که توسط سیستم‌های SCADA نظارت می‌شود، تزریق و پنهان می‌کند. PLC کامپیوتری است که از ویندوز برنامه‌ریزی گردیده تشکیل شده و حاوی کد ویژه‌ای می‌شود که اتوماسیون فرایندهای صنعتی را کنترل می‌کند.

این کرم که با نوشتن کد در PLC، سیستم را کنترل می‌کند و فعالیت‌های آن را به‌تعویق می‌اندازد، برای جلوگیری از تشخیص فایل `%DriveLetter%\~WTR4132.tmp` آن را با رابط‌های برنامه‌های کاربردی API زیر از kernel32.dll و Ntdll.dll مرتبط می‌نماید.

از Kernel32.dll:

- FindFirstFileW
- FindNextFileW
- FindFirstFileExW

از Ntdll.dll :

- NtQueryDirectoryFile
- ZwQueryDirectoryFile

کرم، کد اصلی این توابع را نیز با کدی که برای چک‌کردن فایل‌هایی با مشخصات زیر است، جایگزین می‌کند.

• 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` بارگذاری می‌شود. استاکس‌نت برای انجام این کار، رویکرد متفاوتی را به کار می‌برد و به‌جای این‌که «`LoadLibrary`» رابط‌های برنامه‌های کاربردی را برای بارگذاری فایل dll. در حافظه اصلی فراخوانی نماید، توابعی را به Ntdll.dll ارتباط می‌دهد و سپس "`LoadLibrary`" را با نام فایل خاصی که ایجاد شده است، فراخوانی می‌کند. این فایل درخواست‌شده برای بارگذاری، در Disk نیست اما توابع مرتبط شده به Ntdll.dll که به بارگذاری نام خاص فایل برای درخواست‌ها نظارت دارند، فایل dll. را از یک ناحیه در حافظه اصلی که قبلاً در آن رمزگشایی و ذخیره شده است، بارگذاری می‌کنند. توابع مرتبط‌شده در Ntdll.dll برای این منظور عبارتند از:

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

حال فایل dll. فراخوانی می‌شود و کنترل سیستم را در دست می‌گیرد. این کرم کد خود را نیز به iexplorer.exe به‌منظور دور زدن Firewallها تزریق می‌کند و فرایندهای امنیتی زیر را به پایان می‌رساند.

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

انتشار

استاکس‌نت با کپی‌کردن خود در درایوهای USB، پست‌های الکترونیکی آلوده یا فایل‌های به اشتراک گذاشته شده را در شبکه‌های رایانه‌ای که دارای نقاط آسیب هستند، منتشر می‌کند.

این کرم خود را به‌عنوان فایل‌های زیر در درایوهای قابل جابه‌جایی کپی می‌کند که هر دو نام فایل، hardcoded است و در واقع فایل‌های dll. هستند.

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

به‌علاوه فایل‌های زیر را به درایوهای بالا کپی می‌کند.

- `%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`

هنگامی‌که این درایوها با برنامه‌ای مانند Windows Explorer که توانایی نمایش آیکن‌ها را دارد، مورد دسترسی قرار می‌گیرند، به‌جای نمایش آیکن برای فایل‌های lnk. کدی را که قابلیت اجرای فایل `%DriveLetter %\~WTR4132.tmp` را دارد، اجرا می‌کنند. هدف اصلی این فایل، اجرای فایل `DriveLetter%\~WTR4141.tmp%` است که در درایوهای قابل جابه‌جایی کپی شده و در حافظه اصلی سیستم بارگذاری می‌شود. این فایل است که دو گواهی معتبر امضا شده Realtek و

JMicron را جعل می‌کند.

این کرم همچنین از یک کد مخرب RPC برای منتشرشدن استفاده می‌کند. علاوه‌براین، از کد مخرب دیگری نیز که اجازه می‌دهد تایک فایل به شاخه `%System%` کامپیوتر آسیب‌پذیر نوشته شود، برای کپی‌نمودن خود از کامپیوتر آلوده به سایر کامپیوترها استفاده می‌کند و برای اجرای آن فایل از راه دور نیز از یک ویژگی WBEM بهره می‌برد.

استاکس‌نت همچنین با کپی‌نمودن خود به منابع اشتراک گذاشته شده در شبکه به عنوان فایل زیرکه در حقیقت یک فایل dll. است، منتشرمی‌شود.

`%DriveLetter%\ "DEFRAG[RANDOM NUMBER].tmp`

یک راه که نفوذگران با استفاده از آن، ریسک شناسایی‌شدن و جلوگیری از گسترش بیش از اندازه این کرم را کم کرده‌اند، قراردادن یک شمارنده در درایو USB آلوده است که اجازه انتشار کرم از طریق یک داریو USB خاص به بیش از سه کامپیوتر را نمی‌دهد و بعد از ۲۱ روز نیز خود را پاک می‌کند.

نکته قابل توجه در خصوص استاکس‌نت آن است که درون کد پیچیده‌اش، مشخص شده است که این کرم در تاریخ ۲۴ ژوئن ۲۰۱۲ انتشارش را متوقف و خود را از سیستم آلوده پاک خواهد نمود.

جلوگیری

شرکت مایکروسافت در روز یازدهم مردادماه سال جاری، به‌روزرسانی مهم و فوری را برای اصلاح نقص ابتدایی استاکس‌نت

عرضه کرد؛ سپس شرکت‌های Symantec و Kaspersky نتایج تحقیقات خود را به شرکت مایکروسافت گزارش دادند که باعث گردید تا آسیب‌پذیری Print Spooler به سرعت اصلاح شده و وعده اصلاح دو آسیب‌پذیری کم خطرتر EOP نیز در به‌روزرسانی امنیتی بعدی داده شود.

اگرچه هم‌اکنون تمامی آنتی‌ویروس‌ها قادر به شناسایی و پاک‌کردن کرم استاکنت هستند اما انجام فعالیت‌های زیر توسط همه مدیران و کاربران سیستم می‌تواند باعث جلوگیری یا کاهش خطر آن شود.

• غیرفعال‌کردن ویژگی AutoRun یا AutoPlay سیستم برای جلوگیری از اجرای خودکار فایل‌های قابل اجرا در درایوهای قابل جابه‌جایی

• غیر فعال‌کردن درایوهای قابل جابه‌جایی از طریق Setup سیستم در صورت نیاز، فقط حالت Read-Only را فعال کنید و حتماً یک رمز عبور نیز برای Setup در نظر بگیرید.

• اصلاح نقاط آسیب‌پذیر سیستم‌عامل و نرم‌افزارهای نصب شده

• به‌روزرسانی نرم‌افزار آنتی‌ویروس در فاصله‌های زمانی کوتاه مدت و فعال‌کردن گزینه Automatic Updates برای دریافت خودکار آخرین Updateها

• استاکس‌نت با سوءاستفاده از نقاط آسیب‌پذیر مشخصی انتشار پیدا می‌کند. نصب Patcheهای زیر می‌تواند باعث کاهش خطر این کرم شود.

• Microsoft Security Bulletin MS 10-046
• Microsoft Security Bulletin MS 08-067
• Microsoft Security Bulletin MS 10-061

• دسترسی به آدرس‌های زیر که سرورهای C&C کرم هستند، با استفاده از Firewall و Router باید مسدود شده و با اضافه‌کردن به فایل Local Hosts به آدرس ۱۲۷.۰.۰.۱ تغییر مسیر داده شوند:

•www.mypremierfutbol.com
• www.todaysfutbol.com

• رمز عبور پیچیده که ترکیبی از اعداد، حروف بزرگ و کوچک و نمادها(Symbols) است، برای کلمه عبور کاربران استفاده می‌شود، زیرا این رمزها توسط Dictionary Attackها به‌راحتی قابل شناسایی و کشف نبوده و در عین حال، برای کاربران نیز به یادماندنی هستند.

• همه ارتباطات ورودی از اینترنت به سرویس‌های سازمان را که نباید در دسترس عموم باشند، با استفاده از Firewall Deny انجام داده و تنها به سرویس‌هایی اجازه دهید که به مردم خدمات ارائه می‌دهند.

• هرگز نباید با نام کاربری Administrator یا Root به سیستم Login کرد. کاربران و برنامه‌ها هم باید پایین‌ترین سطح دسترسی لازم را داشته باشند.

• اشتراک‌گذاری منابع و فایل‌ها در شبکه را اگر به اشتراک‌گذاری آنها نیازی نیست، غیرفعال کنید. در صورت نیاز، از ACLها استفاده کرده و مشخص کنید که چه افراد یا کامپیوترهایی اجازه دسترسی به آنها را دارند.

• سرویس‌های غیرضروری فعال در سیستمرا غیرفعال و حذف کنید. اگر کد مخربی علیه یکی از سرویس‌ها پیدا شد، تا زمانی‌که Patch آن سرویس در سیستم نصب نشده است، آن سرویس را غیرفعال کرده یا دسترسی به آن را محدود کنید.

• سرویس‌هایی مانند HTTP،FTP،Mail و DNS مهم‌ترین سرویس های یک شبکه متصل به اینترنت هستند، بنابراین همیشه patchهای این سرویس‌ها را مهم درنظر بگیرید و به روز نگه‌دارید؛ همچنین توسط Firewall، دسترسی به آنها را کنترل نمایید.

• Email سرور را در جهت حذف نامه‌های الکترونیکی که حاوی فایل ضمیمه هستند، پیکربندی کنید. از این فایل‌ها برای گسترش تهدیداتی مانند pif، exe، bat، vbs. و scr. استفاده می‌شود.

• کامپیوترهای آلوده را برای جلوگیری از گسترش بیشتر آلودگی در شبکه به‌سرعت ایزوله نمایید و تا زمانی‌که از برطرف‌شدن آلودگی مطمئن نشده‌اید، آنها را وارد شبکه نکنید.

• از Bluetooth در شبکه استفاده نکرده و دید دستگاه را در حالت Hidden تنظیم کنید تا توسط دستگاه‌های دیگر پیدا نشوید؛ همچنین حتماً از رمز عبور برای برقراری ارتباط بین دستگاه‌ها استفاده نمایید

پیشگیری

پیشگیری از حوادث و کنترل امنیت سیستم، نیاز به یک رویکرد چند لایه دارد که از آن با عنوان «دفاع در عمق» یاد می‌شود. این لایه، شامل سیاست‌ها و رویه‌ها، آگاهی و آموزش، تقسیم‌بندی شبکه، کنترل دسترسی‌ها، اقدامات امنیتی فیزیکی، سیستم‌های نظارتی مانند Firewall و آنتی‌ویروس، سیستم‌های تشخیص نفوذ (IDS)، رمز کاربری و غیره است.

بهترین روش درجهت پیشگیری نیز معمولاً تجزیه و تحلیل خطر، شناسایی نقاط آسیب‌پذیر سیستم‌ها و شبکه‌ها، کنترل سیستم ارزیابی امنیتی و توسعه برنامه‌های اولویت‌بندی برای از بین‌بردن یا به حداقل‌رساندن ریسک خطر است.