استاکس نت

فهرست

استاکس نت(STUXNET)بدافزار بسیار پیچیده ای است که با استفاده از پنجره های پنهان سیستم عامل ویندوز و سامانه مدیریت فرایند صنعتی(SCADA) بویژه از نوع زیمنس، مراکز صنعتی را مورد هدف و تهاجم قرار می دهد.

فصل ۱

تعاریفو مفاهیم

در این فصل به شرح تعاریف و مفاهیم در حوزه این کتابچه می پردازیم.

بدافزار

بدافزارها که با عناوینی چون ویروس، کرم، تروجان و ... شناخته و دسته بندی می شوند یکی از ابزارهای کارآمد در حملات الکترونیکی و حوادث امنیتی هستند که در شبکه های اطلاعاتی و ارتباطی الکترونیکی بکار گرفته می‌شوند.حملات الکترونیکی یا حوادث امنیتی در شبکه‌های ارتباطی و اطلاعاتی اصولاً در دو سطح دسته بندی و اجرا می‌شوند:

- حملات یا حوادثی که توسط نفوذگرها یا هکرهائی شامل افراد کنجکاو، ناراضی، ناراحت، سارقین اطلاعات یا سارقین حساب‌های

بانکی و... صورت می‌گیرند.که در گروه جرائم سایبری یا جرائم رایانه‌ای جای می‌گیرند.

که با این گروه از عاملان حوادث امنیتی می توان با اتکاء به قوانین حقوقی و جزائی، دستگاه قضائی و پلیس برخورد کرد و در سطح بین المللینیز از حمایت قانونی و قضائی و همکاری سایر کشورهابرخوردار بود.

- حملات یا حوادثی که توسط واحدهای سازماندهی شده غیر علنی دولت‌ها برنامه‌ریزی و اجرا می‌شوند و یا توسط گروه‌های سازمان‌یافته‌ای که از حمایت دولت‌های متخاصم با کشور هدف برخوردار هستند صورت می‌گیرد در این سطح از وقایع که با سوءاستفاده از قابلیت‌های پنهان موجود در فناوری‌های هوشمند خارجی و عموماً توسط کشورهای صاحب فناوری‌های پیشرفته صورت می‌گیرد. متأسفانه هیچگونه پوشش و حمایت حقوقی (حقوق بین‌الملل و ...) از کشور قربانی و هدف وجود ندارد.

این سطح از تهدیدات و حملات در گروه جنگ سایبری دسته بندی می شوند که در طی سال‌های اخیر شاهد هستیم بسیاری از دولت‌ها، سازمان‌ها و واحدهای تخصصی، جنگ سایبری و دفاع سایبری را ساماندهی و راه‌اندازی کرده‌اند و هرساله بر تعداد این گروه کشورها افزوده می‌شود.

اسکادا[1]

سامانه‌ای است که مدیریت و کنترل واحدها و مجتمع‌های بزرگ صنعتی و خدماتی را بعهده دارد و در سه لایه سازماندهی می‌شود:

۱. شبکه اتاق فرمان شامل کارگزارها و سوئیچ‌های مرکزی
۲. شبکه ارتباط میدانی شامل PLCها و ابزار دقیق
۳. شبکه مدیریت بالادستی -که در خارج از کشور مستقر بوده و در داخل کشور وجود ندارد.-

PLC

یک رایانه صنعتی است که در ابعاد مختلف متناسب با محیط صنعتی، ساخته و برنامه‌ریزی می‌شود و در کنار ابزارهای دقیق مثل شیرهای برقی، پمپ‌ها،جک‌های هیدرولیک، کلیدها و... امکان اجرای وظایف اسکادا را فراهم می‌کند.

جاسوس افزار

بدافزاری است که بدون اجازه کاربر بصورت پنهان بر روی سامانه‌های رایانه ای نصب شده و ضمن اینکه ممکن است کنترل سامانه را بدست بگیرد، مأموریت سرقت اطلاعات و در بسیاری از موارد تخریب، فریب و... را بعهده دارد.

مراکز آپا

مراکز دانشگاهی هستند که آگاهی‌رسانی، پشتیبانی و امداد رایانه‌ای را در مواقع رویدادهای امنیتی و اختلال در شبکه‌های رایانه‌ای بعهده می‌گیرند.

---

[1] SCADA- Supervisory Control and Data Acquisition

مرکز CERT[1] ملی یا ماهر[2]

کانونی است برای مدیریت و هماهنگی رخدادها و کاهش تهدیدات رایانه ای با مأموریت افزایش سطح امنیت فضای تولید و تبادل اطلاعات و کاهش تأثیرات مخرب رخدادها در سطح ملی.

مرکزCERTدستگاهی یا گوهر[3]

مرکزی است که مسئول دریافت، بررسی و پاسخگویی به گزارشات ارسالی مربوط به مشکلات و رویدادهای امنیتی رایانه‌ای در محدوده سازمان، وزارتخانه یا منطقه تحت پوشش است.

[1] Computer Emergency Response Team

[2] مدیریت امداد و هماهنگی رخدادهای رایانه ای

[3] گروه واکنش و هماهنگی رخدادهای رایانه ای

فصل ۲

آشنایی با بدافزار Stuxnet

Stuxnet اسم بدافزار جدیدی است که بسیاری از سامانه‌های منطقه را آلوده کرده است. این بدافزار اولین بار در تیرماه سال ۱۳۸۹کشف شد. اما طبق آخرین اطلاعات، بیش از یکسال پیش از این تاریخ در شبکه کشور فعال و با کارگزار خود در ارتباط بوده است.هنگامیکه یکی از رایانه‌هایمورد استفاده در کشور برای انجام کاری به بلاروس منتقل می‌شود و در یک شرکت ضدبدافزار بلاروسی مورد بررسی قرار می‌گیرد، آلودگی به یک ویروس ناشناس در آن تشخیص دادهمی‌شود.بر همین اساس شرکت بلاروسی با تشخیص این کرم جاسوس،اطلاعاتی را درباره آن منتشر کرد که متعاقب آن شرکت سیمانتک اطلاعاتی را ارائه کرد و پس از آن موضوع رسانه‌ای شد.

این بدافزار از طریق حافظه‌های جانبی و یا ایمیل های آلوده به صورت مخفیانه وارد سامانه قربانی شده واز طریق حافظه‌های جانبی شروع به انتشار خود می‌کند. هدف استاکس‌نت ایجاد اختلال در مراکز صنعتیو خدماتی است. بدافزار مذکور از طریق یک حفره امنیتی، در ویندوز و سامانه اسکادا نفوذ و گسترش پیدا می‌کند و به دنبال سامانه‌هایی است که از نرم‌افزار WinCCSCADA(متعلق به زیمنس)، استفاده می کنند.

توانمندی‌های ارائه شده برای این بدافزار عبارتنداز:

۱. اهداف تعریف شده را شناسایی می‌کند.
۲. به‌محض ورود،شروع به جمع‌آوری اطلاعات مربوط به کارگزارهای موجود در شبکه و نحوه پیکربندی آن‌ها کرده و در نهایت تلاش می‌کند از طریق ارتباط راه‌دور به کارگزار خود متصل شود.
۳. یک درپشتی را روی سامانه قربانی قرار می‌دهد تا بتواند از راه‌دور و به طور مخفیانه کنترل عملیات زیرساخت‌های مذکور را در اختیار گیرد.
۴. کد خود را در سامانه‌های صنعتی مخفی کرده و بدون اینکه کسی متوجه شود، در فعالیت‌های تأسیسات مورد هدف مداخله و همچنین فعالیت های جدیدی را برای تأسیسات تعریف می‌کند که ممکن است مسئولین متوجه آن نشوند. بعبارتی از طریق سامانه کنترل صنعتی(PLC) نصب‌شده که قابلیت برنامه‌ریزی و کنترل از راه دور را دارد، می‌تواند حوادث بزرگ و مخرب را در تأسیسات ایجاد نماید.
۵. بعد از مدتی نسخه‌های قدیمی خود را حذف و از طریق شبکه، نسخه‌های جدید را جایگزین می‌کند.

با توجه به توانمندی های فوق،سامانه‌هایی که آلوده شده‌اند باید کاملاً مورد بازرسی قرار گیرند تا اطمینان حاصل شود که پاکسازی به طور کامل انجام شده و تأسیسات به همان شیوه‌ای که مورد انتظار است، کار می‌کنند. واضح است که انجام

بازرسی مذکور زمان‌بر و در عین حال ضروری است و در واقع لازم است پاکسازی کامل در مورد رایانه‌های آلوده انجام شود.

در حال حاضر از روش‌هایی همچون مهندسی معکوس و تحلیل کد این بدافزار تقریباً روش کاری آن مشخص شده است اما اینکه دقیقاً هدف این بدافزار چه بوده و یا ممکن است در آینده چه تبعاتی برای سامانه‌های قربانی داشته باشد، مشخص نیست. با توجه به ساختار پیچیده، نحوه عملکرد و تغییرات مداوم کارگزارهای فرماندهی و کنترل این بدافزار، نحوه انتشار و مخفی ماندن وجود آن به مدت چندین ماه از سوی شرکت‌های بزرگ ضدبدافزار، نویسنده و پخش‌کننده این جاسوس‌افزار صنعتی که اولین نمونه در نوع خود محسوب می‌شود، نمی‌تواند یک گروه هکری باشد و به احتمال بسیار زیاد یک دولت در پس این موضوع قرار دارد.

برابر مطالعات و بررسی مراکز آپای کشور(دانشگاه‌های صنعتی شریف، امیرکبیر، صنعتی اصفهان و فردوسی مشهد) در تولید بدافزار استاکس‌نت از سطح دانش و فناوری بسیار پیچیده و پیشرفته استفاده‌شده‌است و این بدان معناست که در پشت صحنه استاکس‌نت نمی‌توانند بدافزارنویس‌ها و شرکت‌های کوچک قرار داشته باشند بلکه ضرورتاً تهیه‌کنندگان از حمایت و هدایت قدرت‌های صاحب دانش و فناوری برخوردار هستند.چند خصوصیت منحصر بفرد که این بدافزار را از بقیه بدافزارهای متداول مجزا می‌سازد عبارتند از:

۱. بهره‌گیری از یک آسیب‌پذیری جدید و ناشناخته (zeroday) ویندوز
۲. انتشار در برخی از کشورهای خاص مانند: ایران، هند، اندونزی و کشورهای حاشیه خلیج فارس
۳. تلفیقی از چند روش برای به خطر انداختن سامانه؛ حفظ دسترسی
۴. سرقت اطلاعاتی هدفمند

شرح عملکرد

استاکس‌نت که بستر اجرایی آن سیستم عامل خانواده ویندوز است، از طریق حافظه‌های جانبی و یا ایمیل های آلوده از طریق تکنیک های روتکیت خاص و به صورت مخفیانه وارد سامانه قربانی شده و پس از ایجاد فایلی تقلبی با پسوند 'LNK/PIF' شروع به انتشار خود می کند. با این روش وارد تمامی حافظه‌های جانبی شده و با تزریق خود به InternetExplorer از فایروال سامانه عبورمی کند.

این بدافزار به محض ورود به سامانه قربانی شروع به جمع‌آوری اطلاعات مربوط به کارگزارهای موجود در شبکه و نحوه پیکربندی آن‌ها کرده و در نهایت تلاش می‌کند از طریق ارتباط راه‌دور به سایت‌هایی متصل شودکه آدرس‌های IP آن‌ها مکرراً در حال تغییر هستند. در نهایت، این تروجان با استفاده از آسیب‌پذیری ویندوز، یک در پشتی در سامانه ایجاد کرده و بدین طریق به مهاجم اجازه می‌دهد به صورت راه دور، کنترل سامانه را به دست گیرد.

علائم آالودگی به این بدافزار

چنانچه فایل های زیر در سامانه وجود داشته باشد،

%System%\drivers\mrxcls.sys
%System%\drivers\mrxnet.sys[1]

و همچنین در صورت وجود کلید های رجیستری زیر:

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

---

[1] فایل های ایجادشده ممکن است با پسوند Tmp. در مسیر %DriveLetter%\~WTR[FOUR NUMBERS].tmp مخفی شده باشند.

سامانه آلوده به این بدافزاراست.

طریقه پاکسازی سیستم

با استفاده از ضدبدافزارهای معتبر سامانه را Scan کنید. ممکن است که تمامیفایل‌ها به صورت کامل پاک نشوند. در این صورتسامانه را درحالت Safe Mode مجدداً راه‌اندازی و Scan نمائید. سپس به مسیرهای زیر رفته وسرویس‌های فعال و مورد استفاده توسط این تروجان را که عناوین آن ها در ادامه ذکر شده استمتوقف نمائید.

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

روش متوقف نمودن سرویس‌های فوق به صورت ذیل است.

۱. Click Start > Run.
۲. Type services.msc, and then click OK.
۳. Select the service that was detected. (mrxnet.sys , mrxcls.sys)
۴. Click Action > Properties.
۵. Click Stop.
۶. Change Startup Type to Manual.
۷. Click OK and close the Services window.
۸. Restart the computer.

سپس:

۱. Start > Run.
۲. Type regedit
۳. Click OK

کلیدهای رجیستری زیررا پاک کنید.

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

و در نهایت Registry Editor را بسته و سامانه را مجدداً راه اندازی کنید.

فصل ۳

اهداف و سناریوهای احتمالی دشمن و راهکارهای ممکن

در این فصل با بررسی موضوع حمله از طریق استاکس‌نت، تلاش خواهد شد تا با شناخت اعماق موضوع، راهکارهای ضروری جهت مواجهه با حملات سایبری دشمن در فضای جنگ سایبری ارائه داده شود.

اهداف شناخته‌شده استاکس‌نت

۱. سرقت اطلاعات محرمانه صنعتی
۲. کنترل از راه‌دور نرم‌افزار مدیریت سامانه زیمنس (SCADA)،قابل استفاده در انتقال و توزیع نیروی برق،لوله‌های گاز و نفت، و بسیاری فرایندهای توزیع شده دیگر
۳. جاسوسی صنعتی، تروریسم صنعتی
۴. رفتاری همچون Worm، Agent و Rootkit را داراست که برای ادارات، وزارتخانه‌ها و کارخانجات صنعتی خطرناک است.

سناریوهای احتمالی

- اختلال در ارائه خدمات توسط صنایع و مراکز حیاتی و ایجاد بحران
- جمع آوری اطلاعات جهت اقدامات خرابکارانه بعدی
- دسترسی به کنترل صنایع و مراکز حیاتی جهت فراهم آوردن زمینه جنگ سایبری
- ضربه زدن به تولید و اقتصاد کشور
- در حال حاضر هدف آلوده سازی سامانه ها است که در زمان لازم فعال می شود.
- ارزیابی توان دفاعی کشور در حوزه سایبری

ارزیابی کلان موضوع

با بررسی ابعاد موضوع، نکات ذیل از اهمیت خاصی برخوردار است:

- استاکس‌نت از حفره‌های امنیتی سامانه‌های بزرگی مثل ویندوز و اسکادای زیمنس جهت نفوذ، انتشار، جستجوی اهداف و برقراری ارتباط با کارگزارهای فرمانده خود استفاده می‌کند و این بدان معناست که تولیدکنندگان آن به منابع کد(Source) ویندوز و اسکادای زیمنس دسترسی داشته اند.
- برابر گزارش‌های منتشرشده، شرکت‌های بزرگ ضدبدافزار و همچنین مایکروسافت و زیمنس حداقل یکسال قبل از کشف و افشای وجود استاکس‌نت، از وجود و فعال بودن آن مطلع بودند و لیکن علیرغم

تعهدات حقوقی خود به مشتریان، هیچ اقدامی جهت اطلاع‌رسانی و مقابله با آن نکردند.

لذا توضیحات مذکور تأکیدی است بر این حقیقت که جنگ سایبری واقعیتی است در سطح مخاصمات بین‌المللی که با عاملیت مستقیم دولت‌ها و یا مزدوران اجیر شده، در حال توسعه و تکامل است و همانطور که در موضوع استاکس‌نت ثابت شد تولیدکنندگان محصولات صنعتی و فناوری‌ها با قدرت‌های مهاجم همکاری کرده و به هیچ تعهد حقوقی و مقررات بین‌المللی پایبند نیستند.

راه حل اساسی برای مقابله با این مسئله

- ایجاد و توسعه ساختار مدیریت امنیت (پست‌های مدیریتی و مراکز CERT دستگاهی، ملی و منطقه‌ای) و اجرای هماهنگ در مقابل عملیات سایبری
- بومی‌سازی و تولید داخلی تجهیزات و فناوری‌های کلیدی و پایه‌ای مربوط به این حوزه با استفاده از تمامی ظرفیت ملی
- سرمایه‌گذاری جهت تولید و توسعه هرچه سریع‌تر تجهیزات بومی امنیتی سایبری(سخت‌افزاری و نرم‌افزاری)
- رعایت اصول دفاع سایبری(امنیت اطلاعات، ایمنی سرمایه‌ها و دارائی‌ها و پایداری شبکه)

فصل ۴

چند نمونه واقعی از حمله به سامانه های اسکادا

حملات به سامانه‌های اسکادا که به صورت مستقیم با زندگی و رفاه عمومی ارتباط دارند، سوابق بسیاری در دهه اخیر داشته‌است. این در شرایطی است که در بسیاری از این نوع حملات ممکن است هرگز مشخص نشود که تهاجم خارجی صورت گرفته و خرابی‌ها ناشی از یک اشتباه فنی یا فردی نبوده‌است، در این فصل جهت آشنایی با آثار ناشی از این دسته از حملات سایبری به ارائه برخی نمونه‌های این حملات و تحلیل اجمالی آن‌ها پرداخته‌شده‌است.

- در اوایل سال ۲۰۰۰ یکی از مشاوران یک شهرداری در منطقه کوئینزلند استرالیا به دلیل نارضایتی شغلی با استفاده از یک دستگاه رادیویی و یک نرم افزار کنترلی و از راه دور، بیش از یک میلیون لیتر فاضلاب را به رودخانه ها و آب های ساحلی و در نهایت به مناطق مسکونی سرازیر و بیش از یک میلیون دلار خسارت مالی به دولت وارد کرد .

لذا در یک شبکه امن اسکادا بخش بیسیم باید توسط سامانه های حفاظتی از سایر بخش های شبکه مجزا و تنها اجازه عبور ترافیک مجاز بین دو بخش صادر شود، ضمناً باید گزارش به هنگام تلاش برای دسترسی خارجی، تهیه و به مسئولین ارسال شود.

- در آگوست ۲۰۰۵، فردی از طریق یک لپ تاپ به درون شبکه رایانه ای ۱۳ کارخانه اتومبیل سازی در آمریکا نفوذ کرده و به رغم استفاده از تجهیزات فایروال حرفه ای در مرزهای شبکه، پس از ورود به شبکه با یک کرم اینترنتی ساده و طی چند ثانیه کل کارخانه ها را آلوده و حدود ۱۴ میلیون دلار خسارت به بار آورد.

لذا اگر راهبرد دفاع در عمق، مد نظر قرار گیرد و تجهیزات حفاظت صنعتی در لایه های مختلف نصب شود، عامل تهدید حتی در صورت ورود به شبکه در ناحیه محدودی باقی مانده و گسترش نخواهد یافت.

- در تاریخ ۱۹ آگوست ۲۰۰۶، سامانه های کنترل کننده گردش آب در یک نیروگاه هسته ای دربراونزفری در یک مورد اورژانسی عمل نکردند. بررسی ها علت مشکل را حجم بالای ترافیک در شبکه کنترل و به دلیل تبادل ناخواسته اطلاعات بین دو سامانه از دو تأمین کننده مختلف نشان داد و به همین دلیل رأکتور نیروگاه به مدت دو روز خاموش ماند و زیانی برابر ششصد هزار دلار وارد آمد.

لذا علت اینگونه مشکلات عدم جداسازی کارایی شبکه های کنترلی در تأسیسات صنعتی است و تجهیزات تخصصی ایمنی اسکادا با کارایی فایروال باید در مزر هر شبکه و در نواحی (Zone ها) نصب شود تا تنها ترافیک مورد تأیید، اجازه انتقال بین مرزها را داشته باشد.

- برخی دیگر از حوادث سال های اخیر مثل تهاجم سایبری مؤثر به شبکه توزیع برق شمال شرق امریکا و کانادا که منجر به قطع بیش از یک هفته ای برق و خسارات عظیم شد، تهاجم سایبری به مرکز مدیریت و کنترل (دیسپاچینگ) شبکه انتقال گاز روسیه در سیبری که منجر به وقوع بزرگ ترین انفجار غیرهسته ای تاریخ بشر شد، حملات سایبری مؤثر به کشورهای استونی و گرجستان که منجر به فلج شدن شبکه فرماندهی و کنترل بخش های دفاعی و مدیریت بخش های عمومی گردید و آخرین آن ها حمله استاکس نت به شبکه های مدیریت و کنترل صنعتی در جمهوری اسلامی ایران و بعضی کشورهای دیگر.

پس به روشنی مشخص می‌شود که فضای فناوری‌های هوشمند و فرمان‌پذیر اطلاعات و ارتباطات، آلوده به تهدیدات نوین، بسیار خطرناک و مؤثر بوده و عرصه این فناوری‌ها و شبکه‌های آن در حال تبدیل شدن به عرصه جدید جنگ یعنی جنگ سایبری است.

با نقض امنیت فناوری اطلاعات، ایمنی عمومی دنیای واقعی مردم دچار مخاطره می شود نه دنیای مجازی آنها