دفاع در برابر ابزار پنهان جنگ سایبری

ذبیح اله جیستان

Zj.jistan@gmail.com

چکیده

امنیت و آسایش، همواره از بزرگترین دغدغه‌های حکومت‌ها می‌باشد؛ ضرورت پرداخت به این موضوع در هزاره‌ای که دشمن با استفاده از تمام امکانات ممکن، مستعد تجاوز و رخنه به منظور پیشبرد اهداف سوء خود می‌باشد، امری کاملا محسوس و ملزوم است. بدون شک، دشمن از هر راه ممکن برای نفوذ و نیل به نیات خود استفاده خواهد نمود. امروز و با توجه به گسترش فناوری‌های نوین، تهدیدات، مخاطرات و نقاط رخنه‌پذیر متعددی به وجود آمده است که اغلب، مورد غفلت قرار می‌گیرند.

حافظه‌های جانبی بخصوص فلش مموری از طریق پورت USB به سیستم‌ها متصل می‌شوند. یکی از بزرگترین مشکلاتی که کاربران در هنگام استفاده از این نوع حافظه‌های جانبی به آن برخورد می‌کنند آلوده شدن این نوع حافظه‌ها می‌باشد. از آن جایی که این نوع حافظه‌ها بر روی چندین کامپیوتر مورد استفاده قرار می‌گیرد و بیشترین انگیزه کاربران برای استفاده از این نوع فایل‌ها در واقع انتقال فایل به سیستم‌های مختلف می‌باشد، بنابراین امکان آلودگی این حافظه‌ها بسیار بالا می‌باشد.

موفقیت نظام اسلامی در برابر هجمه‌های سایبری و نرم‌افزاری دشمنان انقلاب اسلامی از دیگر جنبه‌های دفاع خاموش در برابر حجم فزاینده تهدیدات نظام سرمایه‌داری غرب در قبال ملت ایران قابل ارزیابی است. از همین رو از جمله حوزه‌های قابل تحسین در پدافند غیرعامل کشور به رویارویی و شکست سیاست‌های ایران‌ستیزانه غرب در سناریو و توطئه ویروس استاکس‌نت می‌توان اشاره کرد.در این خصوص با عنوان نمودن چند طرح، دفاع در برابر ابزار پنهان جنگ سایبری را شروع نموده‌ایم. همچنین این حقیقت را تاکید می‌کنیم که با بومی سازی نرم افزارهای دفاعی مطرح شده در هر طرح، می‌توانیم از ورود ابزار پنهان جنگ سایبری از جمله ویروس‌ها که مورد توجه دشمنان ما می‌باشد به سیستم‌های رایانه‌ای سازمان‌های نظامی، دولتی و غیر دولتی جلوگیری نمود.

کلمات کلیدی:

جنگ سایبری، جنگ اطلاعات، سلاح سایبری، ویروس، ابزار پنهان، امنیت داده، کد گذاری، استاکس نت، سیستم فایل، فلش مموری

۱- مقدمه

قرن بیست و یکم، قرن نیروی کار آموزش دیده و با مهارت است. از عصر حاضر با عناوینی چون عصر دیجیتالی، عصر ارتباطات، عصر اینترنت، عصر شبکه‌ها و بزرگراه‌های اطلاعاتی و جامعه اطلاعاتی نام برده می‌شود که در این گستره عظیم، سربازان اینترنتی در دانشکده‌های اینترنتی واقع در شهرهای اینترنتی با کسب آموزش‌های اینترنتی، جنگ‌های اینترنتی را از طریق ارتباطات شبکه‌ای و با موشواره‌ها و سلاح‌ها و بمب‌های الکترونیکی برعلیه دولت‌های دیجیتالی و اهداف و ارتباطات شبکه‌ای و زیرساخت‌های حیاتی کشورها اجرا می‌نمایند.

بنابراین اینترنت و شبکه‌های متعدد و متنوع اطلاعاتی و ارتباطی، گرچه از یک منظر، «فرصت» تلقی می‌شود ولی از آنجا که اینترنت، شهری است «بی‌پلیس» لذا برای ورود به این شهر و دادوستد با عوامل و عناصر موجود در این «شهر شبکه‌ای» باید تدابیر لازم اندیشیده شود در غیر این صورت همین «فرصت» می‌تواند تبدیل به «تهدید» شود[۱] [۲].

۱-۱- جنگ اطلاعاتی

جنگ اطلاعاتی یعنی کاربرد اطلاعات و سیستم‌های اطلاعاتی به عنوان یک سلاح در درگیری هائی که اطلاعات و سیستم‌های اطلاعاتی یک هدف نظامی مهم به شمار می‌روند.

مارتین لیبیکی ضمن وفادار ماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل مختلف جنگ اطلاعاتی را به شرح زیر نام می‌برد:

۱. جنگ فرماندهی و کنترل: که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن،است.
۲. جنگ برپایه اطلاعات: که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم هائی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.
۳. جنگ الکترونیک: تکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری.
۴. جنگ روانی: که در آن از اطلاعات برای تغییر ذهنیت و طرزفکر دوستان، بی طرف ها، و دشمنان استفاده می‌شود.
۵. جنگ هکرها: که در آن به سیستم‌های رایانه‌ای حمله می‌شود.
۶. جنگ اطلاعاتی اقتصادی: ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.
۷. جنگ سایبر: ترکیبی از همه موارد شش گانه بالا[۳].

۱-۲- ویروس در جنگ شبکه‌ای

تولید، تکثیر و توزیع ویروس‌ها یکی از سلاح‌های موثر و مخرب در جنگ‌های شبکه‌ای می‌باشد. طبق بررسی «انجمن ایمنی کامپیوتر» حدود ۱۰ سال گذشته از هر ۳۰ استفاده‌کننده کامپیوتر،حداقل یک نفر مورد تهاجم یک ویروس کامپیوتری قرار می‌گرفت ولی با افزایش کاربرد رایانه در تمامی حوزه‌ها و گسترش شبکه‌ها این آمار چندین برابر، حتی با سرعت رو به گسترش است[۴].

کارشناسان در چند سال قبل ویروس‌های شناخته شده را از ۲۰/۰۰۰ تا ۴۰/۰۰۰ ویروس ذکر نموده‌اند که روزانه چندین ویروس (رایانه‌ای) جدید ساخته می‌شود. برخی نیز ویروس‌های رایانه‌ای شناخته شده را تا ۱۰ سال گذشته بالغ بر ۴۰۰/۰۰۰ ویروس ذکر نموده‌اند و پیش‌بینی شده بود که هر سال حدود ۱۰/۰۰۰ ویروس به این تعداد افزوده می‌شود. حدود ۸۰٪ ویروس‌ها به وسیله نرم‌افزارها منتقل می‌شوند.

۲- فضای سایبر

برای اولین بار توسط داستان نویسی به نام ویلیام گیبسون (1984) در یک داستان علمی-تخیلی و با عنوان بکار گرفته شد. در واقع به هر آنچه که مرتبط با شبکه‌های کامپیوتری و (Cyber Space) فضای سایبر اینترنت و فعالیت‌های کامپیوتری و مجازی باشد سایبر اطلاق می‌شود. بعلاوه برای معرفی گونه برخط، مجازی یا کامپیوتری هر چیزی نیز می‌تواند بکار رود. به دنیای کامپیوترها و جامعه‌ای که از آنها استفاده می‌نماید کلیه منابع اطلاعاتی موجود در شبکه‌های کامپیوتری و دارای فرهنگ خاصی مبتنی بر شبکه‌های ارتباطی الکترونیکی هستند، فضای سایبر یا دنیای مجازی گفته می‌شود[۵].

فضای سایبر مجموعه‌ای از شبکه‌های ارتباطی کامپیوتری شامل وسایل ارتباطی، انتقالی، کنترلی و سیستم‌های مدیریتی با یک‌سری اهداف ارزشمند برای پردازش‌ها و زیرساخت‌ها می‌باشد. اینترنت بزرگ‌ترین مؤلفه از فضای سایبر می‌باشد. بیشتر سامانه‌هایی که به فضای سایبر وابسته‌اند و از آن استفاده می‌کنند، از این فضا به عنوان یک ضعف امنیتی یاد می‌کنند که می‌توان از آن در جهت انجام

حملات استفاده نمود. بیشتر این سامانه‌ها به گونه‌ای طراحی شده‌اند که بتوانند استفاده ارزان و وسیعی از دسترسی به شبکه داشته باشند و این موضوع، توانایی سوءاستفاده مهاجمین به منظور استثمار و آسیب‌پذیر نمودن شبکه‌ها و سرویس‌های هدف را افزایش داده است.

۲-۱- ویژگی‌های فضای سایبر

از جمله ویژگی‌های اساسی فضای سایبر که باعث ایجاد محیطی مناسب برای سربازان جنگ‌های سایبر می‌شود، می‌توان به موارد ذیل اشاره نمود:

- **گمنامی**

شناسایی و ردیابی یک سرباز جنگ سایبر در فضای سایبر و پیدا کردن مکان فیزیکی وی با توجه به تکنیک‌های خاص پنهان‌سازی در این فضا، بسیار مشکل است.

- **تجهیزات ارزان و دردسترس**

سهولت دسترسی به ابزارهای حمله و جاسوسی و هزینه آنها نسبت به جنگ‌افزارهای حملات دیگر، سازمان‌های تروریستی را قادر ساخته تا با استفاده از تجهیزات پیچیده، پیشرفته، بروز سایبری و از طریق ارتباطات پنهان به زیرساخت‌های هدف، حمله و به اهداف خود دست یابند.

- **در دسترس بودن**

هدف اینترنت و ارتباطات به طور روزافزون در حال گسترش می‌باشد، و یک سرباز سایبری قادر است ۲۴ ساعته در حال ارتباط با هدف باشد. از دیگر مؤلفه‌های این فضا می‌توان از توجه رسانه‌ای، تأثیرگذاری بر میزان نیرو، تأثیرات فیزیکی، هوشمندی و سادگی استفاده نام برد.

۲-۲- اهداف جنگ‌های سایبر

اهداف نظامی، خدمات اجتماعی، سامانه‌های نقل‌وانتقال، مخابرات، نیرو، انرژی و هر زیرساخت حیاتی می‌تواند قربانی این جنگ‌ها بوده و امنیت، ایمنی و پایداری آن به خطر افتد. ویژگی‌های جنگ سایبر نسبت به سایر انواع جنگ‌ها جنگ فیزیکی و سایبر از برخی جهات کاملا شبیه به هم هستند؛ به عنوان مثال هدف اصلی در جنگ (از هر نوع) وارد آوردن ضرر و زیان به دشمن است و روش اصلی در جنگ قاعدتاً تصاحب منابع دشمن خواهد بود.

۲-۳- سلاح‌های سایبری

دسته‌بندی سلاح‌های سایبری به شرح ذیل می‌باشد:

۲-۳-۱- ابزارهای شناسایی عموم سلاح‌های شناسایی در خود فضای سایبر یا اینترنت وجود دارند. نمونه‌های کلی این ابزارها در ادامه آورده شده است:

- موتورهای جست‌وجوی دامنه‌ها
- ثبات دامنه اینترنتی
- ثبات آدرس اینترنتی
- تکنیک‌های ردیابی
- ابزارهای شناسایی DNS
- ابزارهای شناسایی شبکه و هم‌بندی آن
- ابزارهای متفرقه

۲-۳-۲- ابزارهای وارسی:

با سلاح‌های وارسی می‌توان سامانه‌های زنده و فعال قابل دسترسی از طریق اینترنت را مشخص نمود. نمونه‌های کلی این ابزارها شامل موارد زیر می‌باشد:

انواع جاروب کننده‌ها، انواع وارسی کننده‌های پورت‌های TCP و UDP، ابزارهای کنکاش سلاح‌های کنکاشگر عموماً درون سیستم‌های عامل حضور دارند. این ابزارها مبادرت به بیرون کشیدن اطلاعات خاص سیستم‌عامل‌ها و شبکه‌ها، نظیر عناصر کاربری و تولیدات نرم‌افزاری می‌نمایند.

۲-۳-۳- ابزارهای نفوذ:

این ابزارها شامل ابزارهای صرفاً سایبری، سلاح‌های فیزیکی-سایبری می‌باشد. مانند امواج کوتاه و بلند دستکاری شده، موسوم به بمب الکترونیکی

۲-۳-۴- ابزارهای ارتقاء مزایا این ابزارها شامل موارد ذیل می‌گردد:

- روش‌ها و ابزارهای تزریق

- متدهای فریبکارانه
- استراق سمع

۲-۳-۵- سلاح‌های پنهان این ابزارها شامل موارد ذیل می‌گردد:

- انواع اسب‌های تروآ
- انواع ویروس‌ها و کرم‌ها
- نقاط پنهان در سیستم‌های عامل

۲-۳-۶- جنگ افزارهای حملات DOS:

در استفاده از این نوع روش‌ها جنبه در دسترس بودن هدف مورد تهدید قرار می‌گیرد. این حملات به عنوان ابزار برای دیگر سناریوهای جنگی نیز مورد استفاده قرار می‌گیرند[۶] [۷] [۸].

۳- بررسی ویروس استاکس نت به عنوان ابزار پنهان در جنگ سایبری

استاکس‌نت یک بدافزار رایانه‌ای (طبق نظر شرکت‌های نرم‌افزار امنیت رایانه‌ای: کرم رایانه‌ای یا تروجان) است که اولین‌بار در تاریخ ۱۳ جولای ۲۰۱۰ توسط ضدویروس وی‌بی‌ای۳۲ شناسایی شد. این بدافزار با استفاده از نقص امنیتی موجود در میانبرهای ویندوز، با آلوده کردن رایانه‌های کاربران صنعتی، فایل‌های با قالب اسکادا که مربوط به نرم‌افزارهای WinCC و PCS7 شرکت زیمنس می‌باشد را جمع‌آوری کرده و به یک سرور خاص ارسال می‌کند[۹] [۱۰] [۱۱]. براساس نظر کارشناسان شرکت سیمانتک، این بدافزار به دنبال خرابکاری در تأسیسات غنی‌سازی اورانیوم نطنز بوده‌است.

۳-۱- روش انتشار استاکس نت

این بدافزار در اواسط تیرماه ۱۳۸۹ در سراسر جهان انتشار یافت. نخستین بار کارشناسان کامپیوتری بلاروس متوجه وجود ویروسی شدند که هدف آن سامانه‌های هدایتگر تأسیسات صنعتی با سیستم عامل ویندوز است. کارشناسان معتقدند طراحان این بدافزار یک منطقه جغرافیایی خاص را مدنظر داشته‌اند و طبق گزارش مجله Business week هدف از طراحی این بدافزار دستیابی به اطلاعات صنعتی ایران است[۱۲]. این بدافزار برای جلوگیری از شناسایی شدن خود از امضای دیجیتال شرکت Realtek استفاده می‌کند. روزنامه نیویورک تایمز در تاریخ ۱۶ ژانویه ۲۰۱۱ میلادی، در مقاله‌ای مدعی شد که «اسرائیل استاکس‌نت را در مرکز اتمی دیمونا و بر روی سانتریفیوژهای مشابه‌ای که ایران از آن‌ها در تاسیسات غنی‌سازی اورانیوم نطنز استفاده می‌کند، با موفقیت آزمایش کرده‌بود»[۱۳]. این در حالی است که دولت اسرائیل یا دولت آمریکا هیچ‌گاه به طور رسمی دست‌داشتن در انتشار استاکس‌نت را تایید نکرده‌اند.

وزیر ارتباطات ایران در آبان ۱۳۸۹ اعلام کرد که رایانه‌های آلوده شده به این ویروس شناسایی و در مرحله پاکسازی قرار دارند. وی همچنین اظهار کرد که منشاء ورود این ویروس به ایران نه از طریق شبکه اینترنت بلکه از طریق حافظه‌های جانبی بوده که افرادی از خارج از کشور به ایران آورده و بدون بررسی لازم به کامپیوترهای در داخل ایران متصل کرده‌اند[۱۴]. هفته‌نامه اشپیگل در مقاله‌ای این احتمال را مطرح کرده است که این ویروس ناخواسته توسط کارشناسان شرکت اتم استروی اکسپورت روسیه و به وسیله یک حافظه جانبی فلش به رایانه‌های نیروگاه اتمی بوشهر منتقل شده است.

۳-۲- عملکرد استاکس نت

استاکس‌نت از طریق رایانامه و حافظه‌های جانبی منتشر می‌شود.این بدافزار پس از آلوده ساختن سیستم، فایل‌های زیر را در سیستم کپی می‌نماید:

1. %Windir%\inf\mdmcpq3.PNF
2. %Windir%\inf\mdmeric3.PNF
3. %Windir%\inf\oem6C.PNF323
4. %Windir%\inf\oem7A.PNF
5. %windir%\system32\drivers\mrxcls.sys
6. %windir%\system32\drivers\mrxnet.sys

و برای راه‌اندازی سرویس‌های خود پس از بالا آمدن ویندوز کلیدهای زیر را در رجیستری ویندوز نصب می‌کند:

1. HKLM\System\CurrentControlSet\Services\Services\MRxNet
2. HKLM\System\CurrentControlSet\Services\Services\MRxCls

سپس این بدافزار در حافظه سیستم مقیم شده و برای عبور از دیوار آتش سیستم، کدهای خود را به اینترنت اکسپلورر تزریق می‌کند و پس از جمع آوری اطلاعات مربوط به شبکه‌ها و پیکربندی آنها در رایانه قربانی سعی به ارتباط با وب‌گاه‌های زیر از طریق راه دور می‌کند:

- www.windowsupdate.com
- www.msn.com
- www.mypremierfutbol.com
- www.todaysfutbol.com

استاکس نت همچنین برای گسترش و انتشار خود در سیستم‌های دیگر، فایل‌های زیر را در حافظه‌های جانبی که به رایانه‌های آلوده شده متصل شوند، کپی می‌کند:

1. %DriveLetter%\~WTR4132.tmp
2. %DriveLetter%\~WTR4141.tmp
3. %DriveLetter%\Copy of Shortcut to.lnk
4. %DriveLetter%\Copy of Copy of Shortcut to.lnk
5. %DriveLetter%\Copy of Copy of Copy of Shortcut to.lnk
6. %DriveLetter%\Copy of Copy of Copy of Copy of Shortcut to.lnk

۳-۳- هدف استاکس نت

بنابر اظهارنظر کارشناسان سیمانتک، این بدافزار سیستم‌هایی را هدف قرار داده است که دارای یک مبدل فرکانس هستند که نوعی دستگاه برای کنترل سرعت موتور است. بدافزار استاکس نت به دنبال مبدل‌هایی از یک شرکت در فنلاند و یا تهران بوده است. استاکس نت به دنبال این دستگاه‌ها بر روی سیستم قربانی می‌گردد و فرکانسی را که دستگاه‌های مذکور با آن کار می‌کنند، شناسایی کرده و به دنبال بازه‌ای از ۸۰۰ تا ۱۲۰۰ هرتز می‌گردد. دستگاه‌های صنعتی که از این مبدل استفاده کنند بسیار محدود هستند و غالباً در تاسیسات غنی‌سازی اورانیوم استفاده می‌شوند. هدف استاکس نت را نمی‌توان نیروگاه‌های هسته‌ای ایران دانست؛ به این دلیل که در این مراکز از این مبدل‌ها استفاده نمی‌شود. بنابراین مرکز غنی‌سازی نطنز تنها مرکز است که می‌تواند هدف احتمالی آن قرار گیرد.

این بدافزار فرکانس‌های مبدل را ابتدا تا بالاتر از ۱۴۰۰ هرتز بالا می‌برد و سپس آن را تا کمتر از ۲ هرتز پایین می‌آورد و سپس آن را فقط برای بالاتر از ۱۰۰۰ هرتز تنظیم می‌کند. در اصل، این بدافزار سرعتی را که موتور با آن کار می‌کند، به هم می‌ریزد که می‌تواند منجر شود هر اتفاقی بیفتد. برای مثال کیفیت محصول پایین آید و یا اینکه اصلاً تولید نشود، مثلاً تأسیسات غنی سازی نمی‌توانند به درستی اورانیوم را غنی سازی کند. این کار همچنین می‌تواند منجر به خرابی موتور به صورت فیزیکی نیز بشود[۱۵] [۱۶] [۱۷].

۴-۳- پیشگیری و پاکسازی استاکس نت

برای پاکسازی سیستم بصورت دستی ابتدا باید System Restore را غیر فعال نمود سپس در حالت Safe Mode تمام فایل‌ها و کلیدهای کپی شده توسط بدافزار در سیستم را پاک کرد. همچنین برای پیشگیری از آلوده شدن به استاکس‌نت لازم است نقص امنیتی موجود در ویندوز را با استفاده از اصلاحیه منتشر شده توسط مایکروسافت برطرف کرد.

۴- روش‌های دفاع در برابر ابزار پنهان جنگ سایبری

همیشه ویروس‌ها باعث ایجاد مزاحمت، تخریب و یا از دست رفتن اطلاعات می‌شود. حال از طرق مختلف منتقل می‌شوند؛ که با بررسی ویروس‌ها می‌تواند به این نتیجه رسید که بر روی پورت USB سرمایه‌گذاری ویژه‌ای شده است. این بدین دلیل است که چون حجم فلش مموری و دیگر حافظه‌های پورتابل رو به افزایش است و کاربرد آن در بین عموم مردم نیز به یک امر ضروری تبدیل گردیده است؛ در سازمان‌ها و ارگان‌های دولتی نیز با توجه به کاربردهای مختلف رایانه، استفاده از این نوع حافظه‌ها زیاد دیده می‌شود و باعث انتقال ویروس از این طریق می‌شود.

گاهی اوقات ویروس بر روی فلش مموری انتقال یافته و از بین بردن آن بسیار دشوار است. برخی از ویروس‌ها پس از این که بر روی فلش مموری انتقال یافتند و به محض وصل شدن به یک رایانه داده‌های تعریف شده برای آن ویروس بر روی فلش مموری انتقال داده می‌شود. پس از این که به رایانه‌ای وصل شود که ارتباط به اینترنت دارد؛ آن داده‌ها به سایت مشخص تعریف شده خود می‌فرستد بدون این که ما متوجه شویم.

حتی یک شخص جاسوس می‌تواند با استفاده از فلش مموری فایل هایی که خودش تعریف کرده را به محض وصل کردن فلش مموری به هر رایانه ای، فایل‌های تعریف شده از روی آن رایانه بر روی فایل مخفی داخل فلش انتقال داده می‌شود. و یا این که بر روی رایانه خود فایلی تعریف می‌کند که فایل‌های با پسوندهای تعریف شده توسط او با وصل شدن هر فلش مموری به رایانه وی از داخل آن فلش مموری، بر روی رایانه انتقال داده شود.

در برخی از سازمان‌ها و نهادهای دولتی و غیردولتی، کاربران رایانه مجاز به استفاده از فلش مموری نیستند. ولی آیا می‌توان از ورود این وسیله کم حجم به سازمان که در غالب یک جاسوئیچی کوچک نیز به بازار عرضه شده است، جلوگیری نمود؟

در برخی از رایانه‌ها می‌توان با نصب نرم افزار "قفل پورت" آن‌ها را بست. ولی کسانی که مجاز به استفاده از فلش مموری هستند و پسورد نرم افزار "قفل پورت" را دارند یا این که اصلا بر روی سیستم آن‌ها نصب نیست؛ می‌توان گفت که ویروس از این طریق منتقل نمی‌شود و با انتقال ویروس خارج از یک سازمان به داخل حتی روی یک سیستم می‌تواند در کل شبکه پخش شود.

با توجه به سرمایه گذاری‌های کلان در بخش آسیب رسانی از طریق ابزارهای پنهان جنگ سایبری از جمله ویروس‌ها می‌توان گفت همچنان بایستی منتظر ویروس‌های جدیدتر جاسوسی و خرابکاری باشیم. ما اگر بخواهیم ویروس استاکس نت را مورد بررسی قرار دهیم به این نتیجه می‌رسیم که یک طرح اساسی در رابطه با پورت USB از جمله فلش مموری باید داشته باشیم.

می خواهیم با مطرح کردن این موضوع که اگر فلش مموری در یک سازمان آزاد باشد، ولی نتوان غیر از مصارف سازمان از آن استفاده‌ای غیرمجاز نمود. مشکل را با ارائه چند طرح (قبل و بعد از نفوذ ویروس) رفع کنیم.

۴-۱- طرح اول(فرمت NIR با ساختار فایل جدید)

در طرح اول توسط یک تیم برنامه نویسی، نرم افزاری بومی جهت نصب بر روی سیستم عامل‌ها تهیه می‌شود. با نصب این نرم افزار بر روی رایانه، به محض این که فلش مموری را وصل می‌کنیم از ما می‌خواهد آن را فرمت کنیم، ولی این یک فرمت معمولی نیست. فرمت هایی مثل FAT32، NTFS داریم ولی ما فرمتی با ساختار فایل متفاوت که در نرم افزار نصب شده تعریف کرده ایم فرمت می‌کنیم.

اگر ما این فرمت را NIR بنامیم و آن فلش مموری فرمت شود، رایانه از این پس آن فلش مموری را می‌شناسد و می‌توان بر روی آن داده‌هایی کپی کرد ولی این فلش مموری فقط بر روی رایانه‌هایی که نرم افزار نوشته شده برای این منظور، بر روی آن نصب باشد؛ شناخته شده است. و اگر بر روی رایانه‌ای خارج از سازمان استفاده نماید نیاز به فرمت مجدد FAT32 و یا NTFS می‌باشد. در نتیجه اگر فردی فلش مموری خود را در سازمان توسط رایانه‌ای فرمت کند و داده‌هایی بر روی آن کپی کند پس از وصل کردن به رایانه شخصی در منزل نیاز به فرمت دارد و نمی‌تواند از آن داده‌ها استفاده کند. حتی ما می‌توانیم پا را فراتر گذاشته و بحث ساختار فایل جدید را به سیستم عامل جدید بکشانیم. سیستم عامل‌ها از ساختار فایل هم پشتیبانی نمی‌کنند پس اگر ما سیستم عاملی با ساختار فایل جدید داشته باشیم ایمنی داده‌ها را از این طریق حفظ می‌کنیم.

نمونه هایی مرتبط با طرح اول ما، که می‌توان از آنها ایده گرفت:

- **سیستم فایل**

NTFS که با ویندوز NT معرفی شد با این چیزی که در ویستا می‌بینید تفاوتهایی دارد و همین طور NTFS ویستا هم با XP یک تفاوت هایی دارد. برای اطمینان کافیست که یک درایور هارد را با xp فرمت کنید به NTFS و بعد ویستا را روی آن درایو نصب کنید حالا ببینید قبل از اینکه ویستا بخواهد نصب شود مجددا دستور فرمت NTFS را روی آن پارتیشن اجرا میکند و اگر نگذارید ویستا فرمت کند اصلا setup کنسل می‌شود یعنی این فرمت اجباری می‌باشد.

- **سیستم فایل جدید winfs**

در فاصله بین عرضه xp و ویستا قرار بود مایکروسافت سیستم فایل جدید به نام winfs را با ویندوز ویستا منتشر کند ولی بعد به نزدیکی عرضه ویستا که منتشر شد اعلام کرد که این سیستم از ویستا حذف شده است.

۴-۲- طرح دوم(ایجاد فضای امن برای داده‌ها و کنترل، مدیریت فضای فلش مموری)

در طرح دوم با کد کردن داده‌هایی که می‌خواهیم بر روی فلش مموری انتقال دهیم و همچنین مدیریت فضای فلش مموری از انتقال غیر مجاز داده بر روی آن، از ورود ویروس به فلش مموری جلوگیری کنیم. در این طرح دو نرم افزار وابسته به هم یکی در فلش مموری و دیگری بر روی رایانه نصب می‌شود. نرم افزار نصب شده بر روی رایانه در صورتی که فلش مموری به آن رایانه وصل شود چک می‌کند که بر روی آن فلش مموری نرم افزار فرزندش نصب است یا نه، در صورتی که وجود نداشته باشد آن فلش مموری توسط سیستم شناسایی نمی‌شود و نمی‌توان از آن فلش مموری استفاده کرد. همچنین نرم افزار داخل فلش مموری پس از اتصال فلش مموری به رایانه چک می‌کند که نرم افزار والدش بر روی رایانه نصب باشد؛ در صورتی که نصب نباشد آن فلش مموری خود را غیر قابل شناسایی برای رایانه نشان می‌دهد. کار این دو نرم افزار در انتقال داده‌ها به فلش مموری و بالعکس این است که وقتی فایلی را می‌خواهیم به فلش مموری انتقال دهیم بایستی توسط نرم افزار نصب شده بر روی رایانه انتقال یابد تا داده‌ها کد گذاری شوند. پس از کد کردن داده‌ها نرم افزار یک تأییدیه برای انتقال داده به فلش مموری از نرم افزار داخل فلش مموری می‌گیرد و پس از تأیید داده‌های کد شده بر روی فلش مموری انتقال می‌یابد. در این حین نرم افزار داخل فلش مموری داده‌ها را چک می‌کند که کد شده باشد. حال فقط داده‌های کد شده انتقال می‌یابد و اگر ویروس بخواهد خارج از دید ما داخل فلش مموری انتقال یابد، نرم افزار داخل فلش مموری با در دست گرفتن فضای فلش مموری و مدیریت آن، طوری نشان می‌دهد که بر روی فلش مموری فضای خالی وجود ندارد و از انتقال آن ویروس و یا هر فایل مخرب دیگر جلوگیری می‌کند. برای انتقال داده‌ها از فلش مموری به رایانه نیز به این صورت عمل می‌کند که با وصل کردن فلش مموری به رایانه هر دو نرم افزار، یعنی نرم افزار داخل فلش مموری و نرم افزار نصب بر روی رایانه یکدیگر را چک می‌کنند که وجود داشته باشند. در صورتی که مشکلی نباشد و هر دو نرم افزار وجود داشته باشد ما می‌توانیم فلش مموری را باز کنیم. در غیر این صورت فلش مموری را نمی‌توانیم باز کنیم. اگر نرم افزارها وجود داشته باشند،و بخواهیم از داخل فلش مموری فایلی را بر روی رایانه انتقال دهیم در ابتدا نرم افزار فلش مموری یک تأییدیه از نرم افزار نصب شده بر روی رایانه می‌گیرد، سپس انتقال صورت می‌گیرد. نرم افزار نصب شده بر روی رایانه داده‌ها را چک می‌کند که کد شده باشد، سپس دی کد می‌کند و به محل آدرس مورد نظر انتقال می‌دهد. در این طرح ما به دنبال جلوگیری از انتقال غیر مجاز ویروس و فایل‌های مخرب دیگر خارج از دید کاربر بر روی فلش مموری هستیم و تا حد زیادی این کار را می‌توانیم تضمین کنیم. این طرح در دست انجام است و در حال تجزیه و تحقیق‌های اولیه می‌باشد.

نمونه هایی از نرم افزارها یا روش‌های بکار گرفته شده مشابه که دارای برخی از امکانات روش ارائه شده در بالا بوده و می‌توان از آنها ایده گرفت:

- سرورهای امن

  تعداد رایانه‌های خدمات دهنده سرورهای ایمن؛ یعنی سرورهائی که فایلهای خود را رمزنگاری کرده و توسط دیواره‌های آتش، سیستمهای آشکارساز نفوذ آی دی اس، و دیگر روش‌های فنی از آنها حفاظت می‌کنند. وجود سرورهای دارای چنین مشخصاتی برای تجارت الکترونیک، بانکداری الکترونیک و به طور کلی همه فعالیت‌های حاوی ارتباطات امن ضروری است[۱۸].

- نرم افزار wipe جهت پاک کردن کامل هر نوع اطلاعاتی از هارد، فلش دیسک، مموری موبایل، درایوهای کامپیوتر

  مزایای این برنامه:

  - ✓ بازنویسی روی فایلها و فولدرها و درایوها و انواع مموری تحت ویندوز xp
  - ✓ نابودی فضاهای خالی روی درایوهای کامپیوتر
  - ✓ نابودی کل فضای خالی یک درایو از جمله بعد از فرمت کردن درایو (البته فضا باز هم بهتر قابل استفاده است)
  - ✓ عدم Recovery اطلاعات و یا Recovery بسیار سخت و تخصصی فایلهای خراب
  - ✓ مدیریت سیستم و بازنویسی فایل‌هایی که نمی‌خواهید آنها را داشته باشید
  - ✓ عدم نیاز به نصب و کرک

- نرم افزار USB Autorun Virus Removal به شما این امکان را می‌دهد که به راحتی autorunهای موجود در

حافظه‌های فلش را نابود سازید و سپس فایل‌های سالم موجود در آن را در کامپیوتر خود کپی کند.

برخی از ویژگی‌ها و امکانات این نرم افزار:

- قابلیت نابود سازی کامل ویروس autorun از فلش مموری.
- جلوگیری کامل از ورود ویروس‌های فلش مموری به داخل سیستم.
- یافتن تمامی عوامل مخرب موجود در حافظه خارجی نظیر ویروس، تروجان و...
- زیر نظر گرفتن و تحت اختیار گرفتن تمامی پورتهای USB سیستم.
- امکان حذف عوامل مخرب موجود در حافظه گوشی‌های موبایل.
- برسی پروسه‌های درحال اجرا جهت جلوگیری از آلوده شدن آنها.
- امکان حذف و پاکسازی فلش مموری از بدافزارهای یافته شده در آن.
- تعمیر برخی از فایل‌ها و برنامه‌های سیستم.
- امکان اسکن کامل درایوهای کامپیوتر.
- محافظت کامل از سیستم در کنار آنتی ویروس به روز.
- تشخیص و پاکسازی تنها با یک کلیک.
- محافظت کامل از سیستم در مقابل آلودگی‌ها.
- سازگار با آنتی ویروس‌های مختلف.
- سازگار با ویندوزهای مختلف.
- داشتن حجم کم.

- نرم افزار USB Disk Security

USB Disk Security نام نرم افزاری برای حفاظت از حافظه‌های جانبی مختلف و کوچک نظیر USB Storage Device, Flash Drive, USB Mass Disk, flash Memory Card, Ipod, Removable Storage Media و ... می‌باشد. این نرم افزار با استفاده از تکنیک‌های قرار داده شده در آن و با چک کردن حافظه جانبی و انجام مقایسه ها، در صورت وجود ویروس و برنامه مخرب بر روی حافظه مورد نظر کاربران را مطلع و اقدام به نابودی فایل مورد نظر می‌کند. این نابود سازی بسیار سریع و بدون آسیب رسیدن به حافظه شما می‌باشد و هیچ مشکلی جانبی دیگری ندارد. از ویژگی‌های این نرم افزار بی نیازی به انجام عملیات بروز رسانی می‌باشد که بر خلاف دیگر برنامه‌های ضد ویروس می‌باشد. این نرم افزار محصولی از International zbshareware می‌باشد.

قابلیت‌های کلیدی نرم افزار USB Disk Security:

- مقابله با ویروس‌های موجود در فلش دیسک‌ها و مموری‌های قابل حمل
- از بین بردن ویروس‌ها و جلوگیری از ورود آنها با سیستم
- پاکسازی فلش دیسک‌ها و مموری‌ها بدون آسیب رساندن به آنها
- حجم بسیار پایین و کند نشدن سیستم در هنگام استفاده از نرم افزار
- راحتی در کاربرد بدون نیاز به هیچ دانش فنی
- فعال بودن نرم افزار و چک کردن USBها در هنگام اتصال یک دستگاه به سیستم
- سازگاری با همه ویندوزهای ساخت مایکروسافت

- با نرم افزارsdformater شما می‌توانید حجم فلش مموری‌های خود را تغییر دهید یا فلش مموری را که حجمش کم شده است درست کنید.
- قفل کردن اطلاعات فلش مموری

نرم افزار USB Secure محصول شرکت NewSoftwares.net است که برای رمز گذاری روی تمام حافظه‌های قابل حمل تولید شده است. شما با این نرم افزار می‌توانید برای USB drives, Thumb drives, Memory cards, External drives and Flash drivesخود رمز بگذارید تا کسی به غیر شما نتواند اطلاعات آن را بازگشایی کند و اطلاعات را به سرقت ببرد. این نرم افزار با تنظیمات خود طوری عمل می‌کند که وقتی شما آن را به USB متصل می‌کنید، از شما پسورد می‌خواهد.

این نرم افزار نیاز به دانش فنی زیادی ندارد و بسیار آسان می‌باشد ومی تواند اطلاعات موجود در «فلش ممـوری» شما که شاید بسیار شخصی و یا بسیار ارزشـمند باشـد را محافظت کند تا از گزند سرقت در امان باشد.

- نـرم افـزار رمزگـذاری بـر روی فایـل‌هـا بـا Lark File Encryption 1.2.6

Lark File Encryption نـرم افـزاری کـم حجـم و قدرتمند در ضمینه رمز نگاری و قفل گذاری روی فایل‌هـا می‌باشد. توسط این نرم افزار به سادگی و به صورت کـاملا امن می‌توانید فایل‌های خود را محافظت نمایید.

- نرم افزار قطع ارتباط ایمن فلش ممـوری‌هـا USB Disk Ejector

USB Disk Ejector نـرم افـزاری کـم حجـم و سـریع می‌باشد که به وسیله آن می‌توانید ارتباط فلش ممـوری و سایر دستگاه‌هـای جـانبی کـه از طریـق USB بـه رایانـه متصل شده اند را به صورت امن قطع نمایید.

- قفل کردن پورتهای USB با USB lock AP2.5

قابلیت کلیدی نرم افزار USB lock AP۲.۵:

- غیر فعال کردن پورت‌های USB
- محافظـت از فولـدرهـای شخصـی بـا Drag و Drop کردن
- غیر فعال کردن درایوهای نوری و فلاپی درایـو "Floppy , CD-ROMs/RWs"
- قفل کردن کامپیوتر برای جلـوگیری از کـار بـا کامپیوتر
- خاموش کردن خودکار کامپیوتر در برابر اتصال حافظه به پورت USB بعد از ۱۵ ثانیه
- اننتخاب رمز عبور برای وارد شدن به برنامه
- نیاز به حجم بسیار کم برای نصب

۴-۳- طرح سوم (ترکیب دو طرح، ایمن سازی بیشتر)

این طرح ترکیبی از دو طرح قبل اسـت، یعنـی مرحلـه چـک کـردن فلش ممـوری دو بار انجام می‌گیرد یکـی زمـانی کـه بـرای شناسـایی فرمت چک می‌شود و اگر فرمت آن با فرمت تعریف شده در نرم افزار نصب شده بر روی رایانه یعنـی فرمـت NIR یکـی نباشـد، آن فلـش مموری باید فرمت شود. حال اگر فرمت NIR باشـد طبـق طـح دوم نرم افزار نصب شده بر روی رایانه و فلـش ممـوری همـدیگر را چـک می‌کنند تا نرم افزار فرزند و والد وجود داشته باشند. پـس از ایـن در ادامه طرح دوم داده‌ها برای انتقال باید کد شوند. مزیت ترکیـب ایـن دو طرح این است که در طرح اول داده‌ها کد نمی‌شوند ولی در طـرح دوم داده‌ها کد می‌شوند و همچنین در این طرح دو بار فلش ممـوری چک می‌شود که این امنیت را بالا می‌بـرد. در ایـن طـرح اولویـت بـا طرح اول یعنی فرمت NIR می‌باشد. پس هـم فرمـت NIR بـر روی فلش ممـوری اعمال می‌شود و هم کد کردن، کنترل و مدیریت فضای فلش ممـوری و داده‌های آن اعمال می‌شود.

۴-۴- طرح چهارم (طرح واکنش سریع)

در طرح دیگر به نام طرح واکنش سریع می‌خواهیم یک حرکت بـرق آسا در برابر ابزار پنهان جنگ سایبری یعنی ویروس‌ها انجـام دهـیم. بدین صورت که اگر ویروسی نفوذ کنـد مـدت زمـانی طـول خواهـد کشید تا ضد بدافزارها بتوانند آن را شناسـایی کننـد. ولـی در طـرح واکنش سریع ما از همان روشی که ویـروس‌هـا بـرای انجـام اهـداف تعریف شده خود به کار می‌برند استفاده مـی‌کنـیم و از همـان روش برای متوقف کردن ویروس‌ها استفاده مـی‌کنـیم. یعنـی ویـروس بـه محض شناسایی قبل یا بعد از نفوذ، با بررسی عکس العمـل ویـروس شناسایی شده، ویروسی را جهت از کارانداختن ویروس اصلی تهیـه و به سیستم تزریق می‌کنیم. با اجرای این طرح قبل از نفوذ و رسـیدن به اهداف ویروس می‌توانیم در برابر اینچنین حملات سـایبری دفـاع نموده و از هرگونه آسیب و یـا از دسـت رفـتن اطلاعـات جلـوگیری کنیم. هم اکنون روی این روش در حال کار شدن است.

نمونه ایی از یک کار مشابه برای طرح فوق که می‌توان از آن ایده گرفت:

۴-۴-۱- تعداد تیم‌های واکنش سریع CERT Team (Computer Emergency Reaction Team)

تیم هائی متشکل از خبرگان امنیت رایانه اسـت کـه بـه تهدیـدهائی مانند ویرو سها و نفوذها واکنش نشان می‌دهند .این تـیم‌هـا توسـط فعالان بخش خصوصی مانند بانک‌ها یا شرکت‌های تلفن (یا عمـومی) مانند FIRST دولت‌ها یا دانشگاه‌ها ایجـاد مـی‌شـوند. اکثـر چنـین تیم‌هایی عضو انجمن‌های بین المللی هستند [۱۹].

۵- نتیجه

مراحلی را مطرح نمودیم که به جلوگیری از نفوذ ابزار پنهان جنگ سایبری و حفظ داده و اطلاعات در برابر آنها می‌پرداخت. و روشی را ارائه نمودیم که در صورت نفوذ ویروس بتوان در کمترین زمان ویروس را مهار نماییم. همچنین در سطحی بالاتر به این موضوع اشاره نمودیم که اگر قرار است سیستم عاملی تهیه شود بایستی بر پایه ساختار سیستم فایل جدید باشد. قفل ورودی، خروجی‌های رایانه را تهیه نموده‌ایم و در حال کار بر روی روش دوم یعنی روشی که منجر به آزاد بودن فلش مموری در سطح سازمان‌های مختلف می‌شود، هستیم. روش واکنش سریع تا کنون چند با تست شده و در حال انجام شدن است. در روشهای بالا نرم افزارهای مشابه ارائه شد. که برخی از امکاناتش مشابه روشهای ما بود ولی باید توجه داشت که ما می‌خواهیم با بومی سازی روش‌های ارائه شده، امنیت را در کشور به دست بگیریم.

مراجع

[۱] نگاهی به نخستین جنگ عصر اطلاعات- استراتژی نظامی و وضعیت نیرویی آمریکا در قرن ۲۱، ترجمه احمدرضا تقاء و داوود علمایی، دافوس سپاه، ۱۳۸۰.

[۲] جنگ اطلاعات و امنیت- نشریه علمی ـ خبری انجمن، رمز ایران، شماره ۵، آذر ۱۳۸۰.

[۳] نشریه «ریزپردازنده»، سال ششم، شماره ۶۱، ص ۲۹.

[۴] جنگ و دفاع سایبری- اندیشگاه شریف و اندیشکده کاوشگران آینده- دی ماه ۱۳۸۴.

[۵] مقاله حملات سایبری شرکت ایزایران- مرکز پدافند غیرعامل- شماره ۸۲ / شبکه و امنیت / مهر ۱۳۸۸.

[۶] شناسایی منشاء ویروس رایانه‌ای استاکس نت/ وضعیت کنترل ویروس در کشور خبرگزاری مهر http://www.winbeta.net

[7] Roger C. Molander, Peter W. Wilson, David A. Mussington, Richard F. Mesic, Strategic Information Warfare Rising,RAND,۱۱۱۲۳۱۱۱۹۹۸۱۹۹۸, http://www.rand.org/publications/MR/MR964/MR964.pdf

[8] CYBERWAR,http://www.iu.hio.no/mark/xmas/14.html

[9] http://fa.wikipedia.org/wiki

[10] W32.Stuxnet,1389, http://www.securelist.com

[11] http://www.securelist.com/en/descriptions/15077693/Worm.Win32.Stuxnet.f

[12] http://www.f-secure.com/v-descs/trojan-dropper

[13] Iran was prime target of SCADA worm, http://fa.wikipedia.org/wiki

[14] Israel tests on worm called crucial in Iran nuclear delay". msnbc.com.http://www.msnbc.msn.com/id/41097319/ns/us_news-the_new_york_times

[15] Chien,Stuxnet: A Breakthrough, http://www.symantec.com/connect/blogs/stuxnet-breakthrough

[16] Symantec: Stuxnet clues point to uranium enrichment target, http://news.cnet.com/8301-27080_3-20022845-245.html

[17] stuxnet: targeting the iranian enrichment centrifuges in Natanz? , http://frank.geekheim.de/?p=1189

[18] World Bank Indicators Database

[19] http://www. first.org/team-info