طراحی ابزاری بومی جهت مقابله با تهدیدات بدافزارهای مبتنی بر USB

علی خاقانی اصل[۱]، سعید پارسا[۲]

[۱] دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی واحد شبستر

khaghani.a@gmail.com

[۲] دانشیار، گروه مهندسی کامپیوتر، دانشگاه علم و صنعت ایران

parsa@iust.ac.ir

چکیده

رشد بی‌سابقه بدافزارها در چند سال اخیر و محبوبیت روزافزون استفاده از وسایل ذخیره‌سازی اطلاعات با درگاه ارتباطی USB باعث شده که امروزه تهدیدات بدافزارهای مبتنی بر USB به مشکلی جدی تبدیل شود. از طرف دیگر فقدان ابزاری بومی جهت شناسایی و مقابله با این تهدیدات، و نیز وقوع حملات هدفمند بدافزارهایی همچون استاکس‌نت، استارس و اخیراً بدافزار دوکیو به کشور عزیزمان، ما را بر آن داشت تا در این راستا ابزاری طراحی و پیاده‌سازی نمائیم که با داشتن امکانات و ویژگی‌های بارز نسبت به ابزارهای مشابه خارجی در این حوزه، بتواند با دقت و درصد بالایی این گونه تهدیدات را شناسایی و با آنها مقابله نماید.

کلمات کلیدی:

بدافزار، USB، حمله، تشخیص نفوذ، مقابله، Auto run

۱- مقدمه

توسعه و تنوع وسایل ذخیره‌سازی اطلاعات با درگاه ارتباطی USB از یک طرف و مزایایی همچون قابلیت حمل و سهولت استفاده از آنها نسبت به دیگر وسایل ذخیره‌سازی اطلاعات و به تبع آن تبدیل شدن به محبوب‌ترین رسانه ذخیره‌سازی اطلاعات از طرف دیگر، توجه بسیاری از نفوذگران را به خود جلب کرده است تا آنجایی که این ابزارها به بهترین و سریعترین راه انتقال بدافزارها در بین سیستم‌های کامپیوتری بدل شده‌اند. از این رو در دنیای مجازی، حملات مبتنی بر USB از جمله مهمترین حملات طراحی شده توسط نفوذگران به شمار می‌رود.

بطور کلی مهمترین حملات مبتنی بر USB را می‌توان در پنج رده زیر دسته‌بندی نمود [۲و۱]:

۱. کپی‌برداری
۲. Hacksaw
۳. Switchblade
۴. سرریز بافر
۵. بدافزارها و کدهای مخرب

هر چند که هر یک از این حملات می‌تواند به تنهایی یا توأمان رخ دهد ولیکن در این بین حملات بدافزارها رشد فزاینده‌ای به خود گرفته است.

رشد بی‌سابقه بدافزارها در چند سال اخیر و محبوبیت روز افزون استفاده از وسایل ذخیره‌سازی اطلاعات با درگاه ارتباطی USB باعث شده که امروزه تهدیدات ناشی از بدافزارهای مبتنی بر USB به مشکلی جدلی بدل شود؛ به گونه‌ای که از هر چهار بدافزار منتشر شده در جهان، یک بدافزار مختص وسایل ذخیره‌سازی اطلاعات با درگاه ارتباطی USB است.

تنوع روز افزون حملات بدافزارهای مبتنی بر USB که از ضعف‌های ابزارهای محافظتی همچون ویروس‌کش‌ها و دیواره‌های آتش، سیستم عامل و دیگر نرم‌افزارهای کاربردی بهره می‌برند و به سرعت در سیستم‌های کامپیوتری نفوذ و تکثیر می‌یابند، شاهد و گواه این مطلب است. از این رو مسئله تشخیص و مقابله با چنین تهدیداتی امری ضروری و اجتناب‌ناپذیر به نظر می‌رسد.

۲- اهمیت موضوع

با توجه به گسترش روزافزون و بی‌سابقه بدافزارها که طبق بررسی‌های انجام شده توسط موسسه امنیتی پاندا [۳]، پنج میلیون بدافزار جدید در سه ماهه سوم سال ۲۰۱۱ میلادی در دنیای مجازی منتشر شده است و نظر به اینکه از هر چهار بدافزار فضای مجازی، یک بدافزار مربوط به ابزارهای USB می‌باشد، تشخیص و مقابله با حملات بدافزارهای مبتنی بر USB اولویت نخست را به خود اختصاص داده است.

از طرف دیگر وقوع حملات هدفمند بدافزارهایی همچون استاکس‌نت (stuxnet) در تیرماه ۱۳۸۹، استارس (stars) در اردیبهشت ماه امسال و اخیراً بدافزار دوکیو (duqu) در آبان ماه که عمده‌ترین روش انتشارشان در کشور از طریق ابزارهای USB بوده است [۴]، فقدان ابزاری بومی جهت تشخیص و مقابله با این تهدیدات بیش از پیش احساس می‌شد. از این رو در راستای تحقق چنین هدفی، ابزاری طراحی و پیاده‌سازی شد که با داشتن امکانات منحصربفرد می‌تواند با دقت و درصد بالایی حملات بدافزارهای مبتنی بر USB را شناسایی و با آنها مقابله نماید.

۳- معرفی ابزار

با مطالعات و بررسی‌های صورت گرفته موفق به طراحی ابزاری سازگار با سیستم عامل ویندوز ایکس پی و نسخه‌های بالاتر شدیم که ضمن پوشش عملکرد ابزارهای مشابه خارجی در این حوزه، نواقص و مشکلات مربوط به آنها نیز مرتفع و بهبود چشمگیری در عملکرد این ابزار نسبت به موارد مشابه خارجی رخ داده است تا آنجایی که در طراحی این ابزار، رفتارهای متداول بدافزارهای امروزی [۶و۵] نیز لحاظ شده است. در ادامه به بررسی امکانات و ویژگی‌های این ابزار و شرح بخش‌های مختلف آن خواهیم پرداخت.

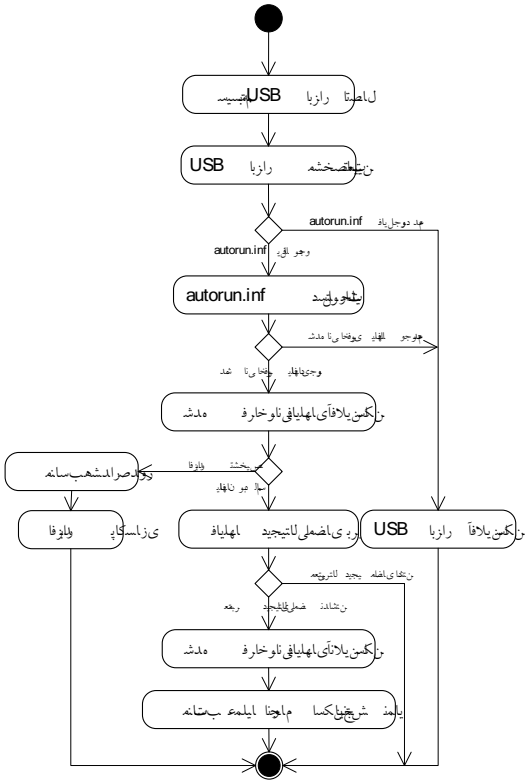
۳-۱- محیط اصلی برنامه

پس از نصب و اجرای ابزار طراحی شده در سیستم میزبان، به محض اتصال ابزارهای ذخیره‌سازی اطلاعات به درگاه ارتباطی USB سیستم میزبان، ابزار فعال شده و قادر به شناسایی آنی و ارائه اطلاعات سخت‌افزاری مربوط به آنها است و در صورت یافتن فایل autorun.inf در ریشه آن ابزارها راهکارهای متفاوتی نسبت به ابزارهای مشابه خارجی در این حوزه اتخاذ می‌نماید.

ابزار طراحی شده بجای حذف فایل autorun.inf، ابتدا با تحلیل دستورات موجود در آن، نسبت به شناسایی و بررسی فایل‌های فراخوانی شده توسط آن بصورت آفلاین و آنلاین اقدام می‌نماید و در این بین چنانچه با دستورات مخربی همچون دستورات تزریق مواجه گردد سریعا نسبت به خنثی‌سازی آنها نیز اقدام می‌نماید. فایل‌های فراخوانی شده از طریق autorun.inf ابتدا توسط پایگاه داده محلی شامل امضاء بدافزارهای مختلف بررسی شده و چنانچه به عنوان بدافزار تشخیص داده نشوند در صورت تمایل کاربر، از بررسی آنلاین استفاده خواهد شد. در شکل ۱، عملکرد کلی ابزار طراحی شده در مقابل بدافزارهای مبتنی بر USB که از فایل autorun.inf بهره می‌برند، نمایش داده شده است.

ابزار طراحی شده قادر به تعیین اعتبار امضای دیجیتالی فایل‌ها و شناسایی الگوی رفتاری بدافزارهای جدید همانند استاکس‌نت (stuxnet) بوده و بصورت لحظه‌ای هشدارهای مناسبی به کاربر اعلام می‌دارد.

در شکل ۲ نمایی از محیط اصلی برنامه ارائه شده است. از طریق همین محیط می‌توان به سایر بخش‌های ابزار دسترسی پیدا کرد.



شکل ۱: عملکرد ابزار در مقابل بدافزارهای مبتنی بر USB که از فایل autorun.inf بهره می‌برند

شکل ۲: نمایی از محیط اصلی برنامه

۳-۲- تنظیمات ویژه در سیستم میزبان

از طریق این بخش می‌توان در سیستم میزبان تنظیماتی جهت پیشگیری و مقابله با تغییرات متداول ناشی از حملات بدافزارهای مبتنی بر USB اعمال کرد. در شکل ۳ نمایی از بخش تنظیمات ویژه برنامه ارائه شده است.

شکل ۳: نمایی از بخش تنظیمات ویژه

مهمترین عملیاتی که می‌توان از طریق این بخش انجام داد عبارتند از:

- غیرفعال کردن تشخیص اتصال فلش دیسک [۱]
- جلوگیری از نوشتن داده روی فلش دیسک
- غیرفعال کردن ویژگی اتوران در سیستم میزبان [۸و۷و۱]
- جلوگیری از ورود برنامه‌ها به startup
- ساخت autorun.inf غیرقابل حذف و ویرایش در سیستم میزبان و فلش دیسک‌ها
- حذف autorun.inf موجود در سیستم میزبان و فلش دیسک‌ها
- غیرفعال کردن ویرایشگر رجیستری
- تعمیر مشکلات رجیستری ناشی از حملات بدافزارها
- تعمیر مشکلات ورود به حالت safe mode

- پشتیبان‌گیری از کلیدهای رجیستری
- بازگرداندنی فایل پشتیبان موجود از کلیدهای رجیستری

بـه عنـوان مثـال بـرای جلـوگیری از ورود برنامـه‌هـا بـه startup از الگوریتم زیر استفاده شده است:

۱. شروع

۲. به مسیرهای زیر در رجیستری برو

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

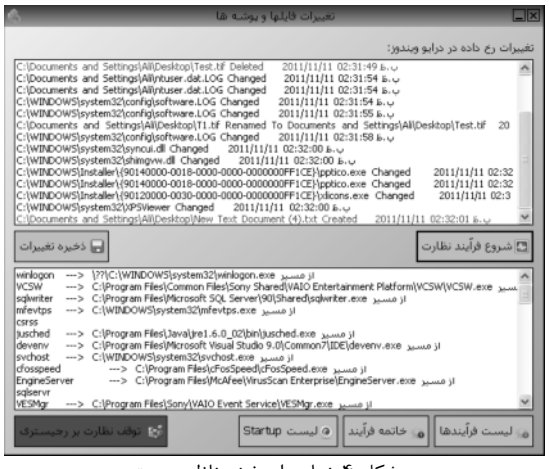
۳. Permission این مسیرها را فقط خواندنی قرار بده

۴. پایان

۳-۳- ناظر سیستم میزبان

از طریق این بخش می‌توان در سیستم میزبان بر فرآیندهای در حال اجرا، برنامه‌های موجود در startup، رجیستری و درایوی که سیستم عامل در آن نصب شده است، نظارت نمود.

با آگاهی از تغییرات رخ داده شده در هر قسمت مـی‌تـوان اطلاعـات مفیدی جهت مقابله با حملات بـدافزارهای مبتنـی بـر USB جمـع آوری نمود. به عنوان مثال می‌توان از تمامی تغییـرات رخ داده شـده اعم از ایجاد؛ حذف و تغییر نام فایل‌ها در درایوی که سیسـتم عامـل در آن نصب شده است، مطلع و بصـورت گزارشـی ذخیـره نمـود. در شکل ۴ نمایی از بخش ناظر سیستم ارائه شده است.



شکل ۴: نمایی از بخش ناظر سیستم

۳-۴- آنتی ویروس ابزار

ابزار طراحی شده از یـک پایگـاه داده امضـاءهای بـدافزارها بصـورت محلی و از پایگاه داده ۴۳ آنتی ویروس بصورت آنلاین بهره می‌بـرد و قادر به اسکن کل سیستم میزبـان، اسـکن درایـو یـا پوشـه انتخـابی توسط کاربر، اسکن اتوماتیک فایل‌های اتوران روی فلش دیسک‌هـا و اسکن آنلاین فایل‌های انتخابی توسط کاربر می‌باشد.

همچنین قادر است با شناسایی فایل‌های مشکوک موجود در سیستم میزبان یا فلش دیسک‌ها هشدارهای مناسبی را به کاربر صادر نمایـد. در شکل ۵ نمایی از بخش آنتی ویروس ارائه شده است.

شکل ۵: نمایی از بخش آنتی ویروس ابزار

در قسمت اسکن آنلاین فایل، ابزار طراحی شده قـادر اسـت گـزارش کاملی از نتایج اسکن آنتی ویروس‌های مختلف بروزرسانی شـده روی فایل انتخابی را به کاربر نمـایش داده و بـا توجـه بـه نتـایج حاصـله هشدارهای مناسبی را صادر نماید.

پس از انتخاب فایل موردنظر توسـط کـاربر، فایـل مـذکور از طریـق اینترنت به سرور مربوطه ارسال می‌گردد و همزمـان عملیـات اسـکن ۴۳ آنتی ویروس که تا تاریخ جـاری کـاملاً بـروز مـی‌باشـند روی آن انجام گرفته و کمتر از چند ثانیه نتایج بررسی‌ها بصورت گزارشی بـه کاربر اعلام می‌گردد و در این حین ابزار با تحلیـل نتـایج بررسـی‌هـا، پیغام‌های مناسبی نیز صادر می‌نماید. نمونه‌ای از گزارش ارائـه شـده توسط ابزار در قبال اسکن آنلاین فایلی در شکل ۶ ارائه شده است.

شکل ۶: نمایش نتایج اسکن آنلاین یک فایل مشکوک

الگوریتم استفاده شده در این مرحله به شرح ذیل می‌باشد.

۱. شروع
۲. اگر سیستم میزبان به اینترنت متصل نیست برو به مرحله ۱۳
۳. فایل مورد نظر را انتخاب کن
۴. فایل انتخابی را روی سرور هدف آپلود کن
۵. اگر ارسال فایل انتخابی به سرور هدف موفقیت‌آمیز نبود برو به مرحله ۱۳
۶. فایل آپلود شده را توسط آنتی ویروس‌های موجود در سرور اسکن کن
۷. اگر عملیات اسکن پایان پذیرفته برو به مرحله ۹
۸. برو به مرحله ۷
۹. نتایج عملیات اسکن را به سیستم ارسال کن
۱۰. اگر نتایج عملیات اسکن دریافت نشد برو به مرحله ۱۳
۱۱. نتایج عملیات اسکن را تجزیه و تحلیل کن
۱۲. نتایج عملیات اسکن را نمایش بده
۱۳. هشدارهای مناسب را صادر کن
۱۴. پایان

علاوه بر این سیستم قابلیت بروزرسانی اتوماتیک پایگاه داده محلی حاوی امضاءهای بدافزارها از طریق اینترنت را با امکان ازسرگیری مجدد عملیات بروزرسانی نیز دارا می‌باشد.

۳-۵- تست سیستم میزبان

در این بخش، سیستم میزبان مورد ارزیابی قرار گرفته و راه‌های نفوذ متداول بدافزارها بررسی شده و به کاربر هشدارهای لازم در جهت رفع آنها اعلام می‌گردد. بعنوان مثال فعال بودن ویژگی اتوران مورد سوء استفاده بیشتر بدافزارهای مبتنی بر USB است. [۸و۷]
ابزار طراحی شده در صورت مواجهه با راه‌های قابل نفوذ، سریعاً هشدار داده و نسبت به مسدودسازی آنها اقدام می‌نماید.

۴- ارزیابی ابزار طراحی شده

ابزار طراحی شده با بهره‌گیری از تحلیل ایستا و پویا نسبت به شناسایی حملات بدافزارهای مبتنی بر USB اقدام می‌نماید و راهکارهای مقابله و پیشگیرانه‌ای نیز در این راستا ارائه می‌نماید.
از آنجایی که ابزار طراحی شده مشابه داخلی ندارد؛ برای ارزیابی آن، قابلیت‌های کلیدی این ابزار با امکانات ۲۱ ابزار نسبتاً مشابه خارجی در این حوزه مقایسه گردید که نشان از جامع و کامل بودن قابلیت‌های این ابزار دارد.
بصورت اجمالی می‌توان قابلیت‌های کلیدی ابزار طراحی شده را چنین بیان کرد:

۱. شناسایی آنی اتصال فلش دیسک‌ها به سیستم میزبان
۲. ارائه اطلاعات سخت‌افزاری از فلش دیسک‌های اتصالی
۳. شناسایی بدافزارهای جدید مانند stuxnet از طریق الگوی رفتاری آنها
۴. تحلیل دستورات موجود در فایل autorun.inf فلش دیسک آلوده
۵. بررسی فایل‌های فراخوانی شده توسط autorun.inf موجود در فلش دیسک آلوده بصورت آفلاین و آنلاین
۶. استفاده از پایگاه داده ۴۳ ضدویروس و ضدبدافزار بصورت آنلاین
۷. بکارگیری پایگاه داده‌ای محلی شامل امضاءهای بدافزارهای مختلف با قابلیت بروزرسانی آن
۸. اسکن سیستم میزبان و فلش دیسک‌ها با استفاده از پایگاه داده محلی و پاکسازی بدافزارهای شناسایی شده
۹. ارائه هشدارهای مناسب فارسی بصورت لحظه‌ای
۱۰. امکان ذخیره گزارش‌های ارائه شده توسط ابزار
۱۱. امکان مشاهده فرآیندهای در حال اجرا در سیستم میزبان با ذکر جزئیات مربوط به آنها
۱۲. امکان مشاهده اطلاعات برنامه‌های موجود در startup
۱۳. نظارت لحظه‌ای بر تغییرات رخ داده در درایو سیستم عامل میزبان
۱۴. نظارت بر رجیستری سیستم میزبان
۱۵. تعمیر مشکلات رجیستری ناشی از اجرای بدافزارها
۱۶. غیرفعال کردن تشخیص اتصال فلش دیسک‌ها
۱۷. جلوگیری از نوشتن داده روی فلش دیسک‌ها
۱۸. غیرفعال کردن ویژگی اتوران در سیستم عامل
۱۹. غیرفعال کردن ویرایشگر رجیستری
۲۰. جلوگیری از ورود برنامه‌ها به startup
۲۱. ساخت autorun.inf غیرقابل حذف و ویرایش در سیستم میزبان و فلش دیسک‌ها
۲۲. حذف autorun.inf موجود در سیستم میزبان و فلش دیسک‌ها
۲۳. محیط کاربر پسند و تماماً فارسی

در جدول ۱ نتایج حاصل از مقایسه امکانات کلیدی ابزار طراحی شده با قابلیت‌های تحت پوشش ۲۱ ابـزار نسـبتاً مشـابه خـارجی در ایـن حوزه ارائه شده است.

جدول ۱: مقایسه امکانات ابزارهای خارجی مشابه با ابزار ارائه شده

نام ابزار	قابلیت‌های تحت پوشش
USB Disk Security	۱-۴-۸-۹-۱۱-۱۲-۱۵-۲۱-۲۲
USB Drive Antivirus	۱-۷-۸-۹-۱۱-۱۵-۱۶-۱۷-۱۸
USB Threat Defender	۱-۳-۴-۷-۸-۹-۱۵
Autorun Virus Remover	۱-۴-۷-۸-۱۱-۱۵-۱۶-۱۷-۱۸-۲۲
McAfee VirusScan USB	۱-۳-۷-۸-۹-۲۲
TrustPort USB Antivirus	۷-۸-۹-۱۰
BitDefender USB Immunizer	۱-۲-۱۸-۲۱-۲۳
Panda USB Vaccine	۱-۱۸-۲۱
Naevius USB Antivirus	۱-۲-۹-۲۱-۲۲
No Autorun	۱-۴-۱۷-۱۸-۲۲
USB Flash Drive Autorun Antivirus	۱-۱۱-۱۵-۲۱-۲۲
USB Guardian	۱-۴-۱۸-۲۲
Wenovo USB Disks Access Manager	۱-۱۶-۱۷
Autorun Protector	۱۸-۲۱-۲۲
USB FireWall	۱-۴-۲۲
Flash Disinfector	۱۸-۲۱
USB Lock AutoProtect	۱۶-۱۷
SuperAutorun	۲۱-۲۲
Ninja Pendisk	۲۱-۲۲
Analyze Lite	۲۱-۲۲
USB WriteProtector	۱۷

۵- نتیجه‌گیری

با توجه به رشد روز افزون تهدیـدات امنیتـی و اهمیتـی کـه امـروزه حملات بدافزارهای مبتنی بر USB پیدا کرده‌اند، در ایـن مقالـه بـه معرفی و شرح مختصر قسمت‌های مختلف ابزار بـومی طراحـی شـده جهت تشخیص و مقابله با این تهدیدات پرداخته شد.

هر چند که نمی‌توان انتظار داشت که به امنیتی تمام و کمال دسـت یافت و همیشه این نفوذگران بودند که یک گـام جلـوتر از روش‌هـا و ابزارهای امنیتی حرکت کردنـد و حمـلات جدیـدتری را پایـه‌ریـزی نمودند ولیکن می‌توان به کمـک ایـن ابـزار درصـد قابـل تـوجهی از حملات بدافزارهای مبتنی بر USB را کشف و خنثی نمود.

ابزار طراحی شده با بهره‌گیری از تحلیل ایسـتا و پویـا و نیـز داشـتن امکانات و ویژگی‌های بارز، می‌تواند با دقت و درصد بالایی ایـن گونـه حملات را در سیستم میزبان شناسایی و با آنها مقابله نماید.

امید است با حمایت مسـئولان ذیـربط و تکمیـل و توسـعه هـر چـه بیشتر این ابزار بتوان گـام مـؤثرتری در جهـت مقابلـه بـا تهدیـدات روزافزون بدافزارهای مبتنی بر USB بخصوص برای کشور عزیزمـان برداشت.

سپاسگزاری

از راهنمائی‌های مهندس ستار هاشمی، هادی خلیل پـور، سـیدجواد سیدحمزه و داود احدپور که ما را در تهیه این مقاله یاری نمـوده‌انـد؛ کمال امتنان و سپاس را داریم.

مراجع

[1] Anderson, Brian, Anderson, Barbara, "Seven Deadliest USB Attacks", Syngress Press, Elsevier Inc, 2010

[2] Pham D., Syed A., Halgamuge M. N., "Universal serial bus based software attacks and protection solutions", Elsevier Ltd, 2011

[3] ITProPortal 24/7 Tech Commentary & Analysis, November 2011, http://www.itproportal.com/2011/11/03/pandalabs-finds-pieces-malware-found-trojans/

[4] Orrey K., "A Survey of USB Exploit Mechanisms, profiling Stuxnet and the possible adaptive measures that could have made it more effective", March 2011, http://www.vulnerabilityassessment.co.uk/education/whitepaper.pdf

[5] Bayer U. , Habibi I. , Balzarotti D., Kirda E., Kruegel C., "A View on Current Malware Behaviors", 2009

[6] Carvey H., Altheide C., "Tracking USB storage: Analysis of windows artifacts generated by USB storage devices", Elsevier Ltd, 2005

[7] Pham D., Mohammad A., Syed A., Halgamuge M. N., "Threat Analysis of Portable Hack Tools from USB Storage Devices and Protection Solutions", 978-1-4244-8003-6/10 IEEE, 2010

[8] Pham D., Halgamuge M. N., Syed A., Mendis P., "Optimizing Windows Security Features to Block Malware and Hack Tools on USB Storage Devices", PIERS Proceedings, Cambridge, USA, July 2010