2nd Conference on Computer, IT, Electrical and Electronic Engineering 2012
دومین همایش ملی مهندسی کامپیوتر، برق و فناوری اطلاعات

ارائه روشی با ایجاد سیستم پویا و توزیع‌شده برای کشف بدافزارها

محمدرستمی [۱]، لادن مال عزیزی [۲]
[۱] دانشجوی کارشناسی ارشد نرم افزار کامپیوتر موسسه آموزش عالی جهاد دانشگاهی خوزستان ،
Mohamad.rostami10@yahoo.com
[۲] دکترای کامپیوتر، عضو هیئت علمی دانشگاه آزاد اسلامی واحد نجف آباد
Ladan_malazizi@yahoo.co.uk

چکیده-بدافزار به یک قطعه کد یا یک برنامه گفته می‌شود که به منظور نفوذ در سیستم هدف و جمع‌آوری اطلاعات شخصی یا سازمانی،خراب‌کاری یا کلاهبرداری و... نوشته شده است. به طور کلی وب سایت‌هایی که شامل بدافزار هستند به دو دسته‌ی زیر تقسیم می‌شود:

-وب‌سایت‌هایی که توسط نفوذگر یا نفوذگران مدیریت می‌گردند و بدافزارها در آنجا مقیم هستند و از آنجا پخش می‌شوند.

-وب‌سایت‌هایی که به وب‌سایت‌هایی که بدافزارها در آنجا مقیم هستند، ارجاع می‌کنند.

روش‌هایی جهت کشف بدافزار از جمله شرکت Google و روش قدیمی Signature Based ارائه شده است که در این مقاله یک سیستم جدید برای کشف صفحه‌های آلوده‌ایی ارائه می‌شود که به صفحات شامل بدافزار،ارجاع می‌کنند و به روش پویا و توزیع‌شده کار می‌کند. این سیستم از بخش‌های سرور،پایگاه داده و کلاینت‌ها تشکیل شده است که در سمت کلاینت‌ها یک نرم افزار کوچک بر روی مرورگر کاربر نصب می‌گردد. وظیفه‌ی سرور کنترل و به روز رسانی محتوای پایگاه داده و ارسال محتوای این مخزن به شکل لیست برای کلاینت‌هاست.کلاینت‌ها نیز بر اساس لیست ارسالی از سوی سرور اقدام به کشف وب‌سایت‌های Pass-Through جدید کرده و هر کدام از آن‌ها لیست‌های خود را در بازه‌های زمانی مشخص برای سرور ارسال می‌کنند تا سرور همواره محتوای پایگاه داده را به روز نگاه دارد. پایگاه داده شامل دو نوع لیست است، یک لیست که حاوی آدرس‌های URL وب‌سایت‌های Source و دیگری که شامل آدرس‌های URL وب‌سایت‌های Pass-Through است. سرور برای عملیات کشف توسط کلاینت‌ها هر دو نوع لیست را برای آنها ارسال می‌کند. سرور برای کاهش تأخیر از یک کش استفاده می‌کند (برای تسریع ارسال و دریافت لیست‌ها) و در زمانی که مرورگر کلاینت‌ها کمتر در حال خزیدن در بین صفحات هستند، محتوای پایگاه‌داده روی کش و دیسک را مطابقت می‌دهد.

کلمات کلیدی-بدافزار، پویا، توزیع شده.

۱- مقدمه

امروزه بدافزارها به دلیل این که فراهم‌کنندگان سرویس‌های اینترنتی و مدیران شبکه‌ها پورت‌هایی که بدافزارها از طریق آن‌ها خود را درمحیط اینترنت پخش می‌کنند را مسدود کرده‌اند، خود را از طریق وب‌سایت‌های مشهور در محیط اینترنت گسترش می‌دهند[2].

بدافزار یا Malware به یک قطعه کد یا یک برنامه گفته می‌شود که به منظور نفوذ در سیستم هدف و جمع‌آوری اطلاعات شخصی یا سازمانی،خراب‌کاری یا کلاهبرداری و... نوشته شده است[1]. به طور کلی وب سایت‌هایی که شامل بدافزار هستند به دو دسته زیر تقسیم می‌شود[3]:

Source Website: وب‌سایت‌هایی که توسط نفوذگر یا نفوذگران مدیریت می‌گردند و بدافزارها در آنجا مقیم هستند و از آنجا پخش می شوند.

Pass-Through Website: وب‌سایت‌هایی که به وب‌سایت‌هایی که بدافزارها در آنجا مقیم هستند، ارجاع می‌کنند.

آژانس اینترنت و امنیت کره (Korea Internet & Security Agency) یا به اختصارKISA ، یک سیستم برای کشف وب‌سایت‌هایی که بدافزارها را درون اینترنت پخش می‌کنند، طراحی و تولید کرده است. این آژانس با استفاده از این سیستم توانسته بین سال‌های ۲۰۰۵ تا ۲۰۰۹ ،تعدای زیادی وب‌سایت را از هر دو نوع کشف کند. این آژانس در ابتدای سال ۲۰۱۰ گزارشی آماری را بر اساس کشفیات این سیستم ارائه کرد. در این گزارش تعداد وب‌سایت‌های Pass-Through سه برابر وب‌سایت‌های Source بود.بنابراین این نکته اهمیت کشف وب‌سایت‌های Pass-Through در فرآیند مبارزه با بدافزارها را به وضوح نشان می دهد[8].

۲- مفهوم آلودگی

یک نفوذگر یا Attacker بدافزارها را در یک وب سایت قرار می‌دهد، سپس لینک‌هایی به این وب سایت آلوده در وب سایت‌های معروف و پرمراجعه می‌گذارد، هنگامی که کاربر به یکی از وب سایت‌هایی که به این وب سایت آلوده ارجاع می‌کند، مراجعه می‌کند به وب سایت آلوده متصل شده و بدافزار روی سیستم کاربر نصب می‌شود[2,10].

بدافزارها به روش Drive-by Download روی سیستم کاربر نصب می‌شوند، یعنی این که کاربر از نصب برنامه بر روی سیستم خود مطلع نیست یا این که اجازه نصب برنامه بر روی سیستم را می‌دهد ولی از تبعات انجام این کار و هدف برنامه آگاه نیست[4].

۳- مشکلات و موانع به کارگیری روش‌های کشف بدافزار

یکی از مشکلات در بررسی محتوای یک صفحه وب این است که ممکن است همه یا بخشی از کد منبع(Source Code) آن صفحه به کد مبهم تبدیل شده باشد.کد مبهم ، یک کد منبع است که خواندن و درک عملکرد کد توسط انسان دشوار است ولی از نظر اجرایی دقیقا همان عملکرد کد منبع را دارد. برنامه‌نویسان عمدا به دلایل متعدد از جمله پنهان کردن هدف کد، جلوگیری از تغییر کد منبع یا جلوگیری از مهندسی معکوس و...کد منبع نوشته خود را به کد مبهم تبدیل می‌کنند. در این صورت دو نسخه از کد نوشته شده وجود دارد، یکی کد منبع که در اختیار برنامه‌نویس قرار دارد و دیگری کد مبهم شده که در اختیار همگان قرار می‌گیرد. یکی از ویژگی‌های کد مبهم شده کاهش اندازه کد است به این دلیل که بسیاری از مواردی که در عملکرد کد هیچ تأثیری ندارند از آن حذف شده‌اند.کد مبهم بسیار وابسته به زبان و کامپایلری است که کد منبع به آن زبان نوشته و ترجمه شده است. امروزه نرم‌افزارهای بسیاری متناسب با زبان‌های برنامه‌نویسی وجود دارندکه کد منبع را به کد مبهم تبدیل می‌کنند[11]. این نرم‌افزارها از روش‌های گوناگونی استفاده می‌کنند ولی عملیات‌هایی که همه آن‌ها انجام می‌دهند به شرح زیر است[19] :

تبدیلات لغوی: توضیحات و فضاهای خالی از کد منبع حذف می‌گردند.

تبدیلات کنترلی: ساختار برنامه بدون این که عملکرد برنامه تغییر کند، دگرگون می‌شود، به عنوان مثال با استفاده از دستور Jump.

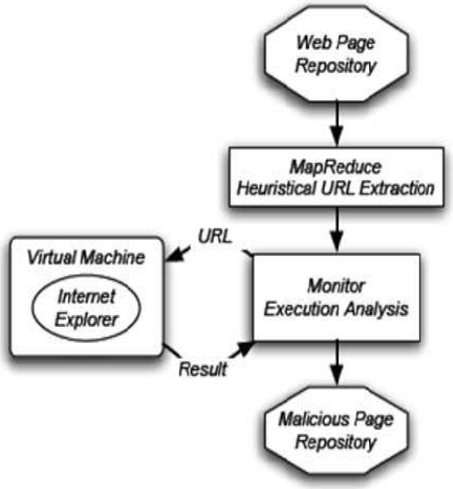
تبدیلات داده: ساختمان داده‌های کد منبع با ساختمان داده‌های مشابه جایگزین می‌گردد.

۴- روش مورد استفاده شرکت Google جهت کشف بدافزار

شرکت گوگل برای موتور جستجوی مشهور خود عملیات شاخص‌گذاری صفحات وب برای انجام سریع‌تر عمل جستجو توسط کاربران را انجام می‌دهد، بنابراین به محتوای صفحات وب نیز دسترسی دارد.این شرکت یک مدل برنامه‌نویسی به نام MapReduce را برای خوشه‌بندی(Clustering) داده‌ها در مجموعه‌های مشخص و سپس انجام عملیات پردازشی در این مجموعه‌ها ارائه کرد.آن‌ها با استفاده از این مدل برنامه‌نویسی، برنامه‌ای را به همین نام برای کشف وب‌سایت‌های شامل بدافزار از هر دو نوع تولید کردند.این برنامه در دو فاز Map و Reduce اجرا می‌شود و تا زمانی فاز Map به طور کامل انجام نشود، برنامه وارد فاز Reduce نمی‌گردد. ابتدا صفحات وب را با استفاده از پارسر پارس کردند و تمامی URL های موجود در صفحات را درون فایل‌هایی (سیستم فایل توزیع شده) ذخیره کردند، سپس در فاز Map یک سری زوج توالی‌هایی < key,value> ایجاد کردند که مقدار Key ،URLصفحه مورد نظر و Value ،URL صفحه‌ای است که به صفحه مورد نظر ما ارجاع می کنند. سپس در فاز Reduce کلیه URL هایی که به صفحه مورد نظر ارجاع می‌کنند در یک دسته مرتب می‌شود <key,list(value)>.در پایان فاز Reduce نتایج در فایل‌هایی (سیستم فایل توزیع شده) ذخیره می‌شود. در ادامه، مرورگر Internet Explorer را در ماشین‌های مجازی اجرا کردند و به URL های کلید یا هدف مراجعه کردند و تغییراتی که در محیط ماشین مجازی پس از رجوع به صفحه مورد نظر رخ می‌دهد را تحت بررسی قرار دادند.در پایان صفحات آلوده را شناسایی و در

موتور جستجوی برای کاربرانی که قصد بازدید از این صفحات را دارند، پیام هشدار قرار دادند[4,5].

معایب روش گوگل این است که این روش نمی‌تواند صفحاتی که دسترسی به محتوای آن‌ها نیازمند مجوز دسترسی است و همچنین صفحات پویا (Dynamic) را مورد بررسی قرار دهد و همچنین فقط زمانی که کاربر از طریق موتور جستجو قصد مراجعه به صفحه آلوده را داشته باشد، امکان نمایش پیام هشدار برای کابر وجود دارد[14].



شکل(۱).نمای کلی معماری کشف بدافزار توسط شرکت Google

۵- روش قدیمی Signature Based جهت کشف بدافزار

روش دیگرSigature Based یا مبتنی بر امضا نام دارد که یک روش قدیمی است.در این روش اگر بخشی از محتوای کد منبع(Source Code) یک صفحه با یک امضا در پایگاه‌داده مطابقت داشت، آن صفحه به عنوان یک صفحه آلوده در نظر گرفته می‌شود.Signature یا امضا می‌تواند URL یک صفحه وب یا یک دستور مانندIframe URL باشد[4].این روش به سبب استفاده آسان و کم بودن خطاهایی از نوع False Positive مورد استفاده قرار می‌گیرد. از آنجایی که این روش از تطبیق رشته استفاده می‌کند،کارایی پائینی دارد و صفحاتی که همه یا بخشی از کد آن‌ها مبهم شده باشد، نمی توان با استفاده از این روش کد منبع این صفحات را Scan و بررسی کرد(False Negative Error). به دلیل زمان‌گیر بودن این روش فقط صفحه اول یا اصطلاحا Main Page از یک وب سایت با این روش بررسی می‌گردد[20].

False Positive: این خطا هنگامی روی می‌دهد که در یک صفحه، کد یا کدهای آلوده وجود ندارد ولی سیستم صفحه را به عنوان یک صفحه آلوده اعلام می‌کند[6].

False Negative: این خطا هنگامی روی می‌دهد که در یک صفحه، کد یا کدهای آلوده وجود دارد ولی سیستم صفحه را به عنوان یک صفحه تمیز اعلام می‌کند. همان طور که در بالا ذکر شد این نوع خطا به دلیل مبهم و غیر قابل خواندنی شدن کد منبع روی می‌دهد، چرا که سیستم از تطبیق رشته‌ها استفاده می‌کند[6,12].

۶- روش پیشنهادی جهت کشف بدافزار

سیستم از بخش‌های سرور،پایگاه داده و کلاینت‌ها تشکیل شده است که در سمت کلاینت‌ها یک نرم افزار کوچک بر روی مرورگر کاربر نصب می‌گردد. وظیفه سرور کنترل و به روز رسانی محتوای پایگاه داده و ارسال محتوای این مخزن به شکل لیست برای کلاینت‌هاست.کلاینت‌ها نیز بر اساس لیست ارسالی از سوی سرور اقدام به کشف وب‌سایت‌های Pass-Through جدید کرده و هر کدام از آن‌ها لیست‌های خود را در بازه‌های زمانی مشخص برای سرور ارسال می‌کنند تا سرور همواره محتوای پایگاه‌داده را به روز نگاه دارد. پایگاه داده شامل دو نوع لیست است، یک لیست که حاوی آدرس‌های URL وب‌سایت‌های Source و دیگری که شامل آدرس‌های URL وب‌سایت‌های Pass-Through است. سرور برای عملیات کشف توسط کلاینت‌ها هر دو نوع لیست را برای آن‌ها ارسال می‌کند. سرور برای کاهش تأخیر از یک کش استفاده می‌کند (برای تسریع ارسال و دریافت لیست‌ها) و در زمانی که مرورگر کلاینت‌ها کمتر در حال خزیدن در بین صفحات هستند، محتوای پایگاه داده روی کش و دیسک را مطابقت می‌دهد[1,16].

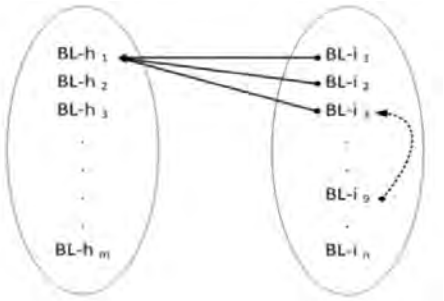
این روش می‌تواند محتوای کد منبع همه صفحات را که همه یا بخشی از آن مبهم شده باشد را بررسی نماید، به این دلیل که مفسر جاوا اسکریپت مرورگر قبل از اجرای صفحات آن‌ها را به طور کامل از حالت مبهم بودن خارج می‌کند. بنابراین مطمئن هستیم که به محتوای کد منبع همه صفحات دسترسی داریم. هنگامی که کاربر قصد مراجعه به یک صفحه وب را داشته باشد، قبل از این که مرورگر به سرور مربوطه متصل شده و صفحه را برای کاربر نمایش دهد، این روش آدرس URL صفحه را با آدرس‌های URL درون لیستی که سرور در اختیار کلاینت‌ها قرار می‌دهد، مقایسه می‌کند و در صورتی که URL صفحه مورد نظر درون لیست باشد از وصل شدن به سرور و نمایش صفحه خودداری می‌کند و در غیر این صورت به طور عادی صفحه درخواستی را برای کاربر نمایش می‌دهد[17].

۷- اجزای سیستم پیشنهادی

Tool with Client: یک نرم‌افزار کوچک که به شکل افزونه بر روی مرورگر Internet Explorer کلاینت قرار می‌گیرد.این ابزار آدرس URL صفحه‌ای که کاربر قصد مراجعه به آن را دارد با لیستی از آدرس‌های URL که از سرور دریافت کرده است، مقایسه می‌کند و اگر آدرس یا آدس‌های URL جدید یافت شد،آن‌ها را در یک لیست برای سرور ارسال می‌کند[2].

Blacklist Database: دو نوع لیست سیاه یا Balcklist وجود دارد،یک لیست که حاوی آدرس‌های URL، Source Website هاست که به نام BL-H شناخته می‌شود و دیگری لیستی حاوی آدرس‌های URL،Pass-Through Website که BL-I نام دارد[18].

هر BL-H می‌تواندتوسط چندین BL-I مورد ارجاع قرار گیرد و همچنین هر BL-I نیز می‌تواند توسطBL-Iهای دیگر مورد دسترسی قرار گیرد یعنی این که ممکن است برای متصل شدن به یک وب سایت Source چندین مرحله اتصال به وب سایت‌های Pass-Through را داشته باشیم[13].



شکل(۲). رابطه‌ی بین BL-H وBL-I

Server: سرور لیست‌های سیاه را برای کلاینت‌ها فراهم می‌کند و کلاینت‌ها نیز لیست‌های جدید خود را برای سرور ارسال می‌کنند تا سرور محتوای پایگاه داده را به روز نگاه دارد[7,2].

Response Authority: به یک یا چند سرور برای مدیریت همه سیستم نیاز داریم. این Response Authority همه لیست‌ها، ابزارها و پیام‌ها را مدیریت می‌کند. به عنوان مثال تعدادکل کلاینت‌ها و تعداد کلاینت‌های فعال در هر لحظه را مشخص می‌کند و نرم‌افزار را برای متقاضیان جدید فراهم کرده وکلاینت‌های جدید را فعال می‌کند[4,7].

۸- ویژگی‌های سیستم پیشنهادی

Distributed Computing: در این روش به جای این که یک یا چند سیستم به طور ایستا در فرایند کشف بدافزارها شرکت داشته باشند،کاربران با نصب نرم افزاری کوچک،که جزیی از سیستم است و با فعال‌سازی آن،به طور پویا در فرایند کشف شرکت می‌کنند[9].

Effective Inclusion and Exclusion: یک وب سایت از یک صفحه اصلی و یک مجموعه صفحه گرداگرد این صفحه تشکیل شده است که از طریق صفحه اصلی قابل دسترسی هستند.اگر قطعه کدی آلوده در یکی از صفحات وب سایت که لینک‌هایی به صفحات شامل بدافزار دارد، وجود داشته باشد ولی به دلایلی کاربران کمتر یا اصلا به این صفحه مراجعه نکنند، پس نیازی به بررسی این لینک‌ها نیست اما اگر صفحه‌ای از یک وب سایت وجود داشته باشد که پس از چندین مرحله خزیدن یا Crawling به آن صفحه برسیم و در آن صفحه قطعه کدی آلوده وجود داشته باشد و کاربران به طور مکرر به این صفحه مراجعه کنند،لازم است که لینک‌های درون صفحه مورد بررسی قرار گیرد[15].

Inevitable End-Point Deobfuscation: از آن جایی که سیستم پس از این که مفسر به طور کامل محتوای صفحات را از حالت مبهم خارج کرد و درست قبل از این که صفحه توسط مرورگر Browse شود، کار کند، به همه آدرس‌های URL درون صفحه دسترسی دارد[15].

Feedback System: سرور لیست بدافزارها را نگهداری و این لیست را برای کلاینت‌ها ارسال می‌کند،کلاینت‌ها نیز لیستی از URL های جدید که درون لیست ارسالی از سوی سرور وجود نداشت را برای سرور ارسال می‌کنند[21].

۹- مقایسه عملکرد سه روش بیان شده برای کشف بدافزار

ویژگی	Google	MC-Finder	WebCheckSystem
محدوده	صفحات اصلی(Main Page) و 🗝	صفحات اصلی(Main Page)	همه صفحات وب
کشف‌برای صفحاتی که نیازبه-مجوزدسترسی دارند	×	×	✓
سربار	آری	آری	خیر
سرور مرکزی برای کشف	نیاز دارد	نیاز دارد	نیاز ندارد
امکان بررسی صفحات مبهم	✓	×	✓
متد کشف	ایستا و پویا	ایستا	پویا
مکان ابزار	مرکزی	مرکزی	توزیع‌شده

امکان کشف برای Source Website	✓	×	×
امکان کشف برای Pass-Through Website	✓	✓	✓

۱۰- نتیجه گیری

این سیستم جدید برای کشف صفحه‌های آلوده‌ایی است که به صفحات شامل بدافزار،ارجاع می‌کنند و به روش پویا و توزیع‌شده کار می‌کند.این سیستم از چهار بخش تشکیل شده است :

- یک سیستم کاربر که ابزار روی مرورگر Internet Explorer آن نصب می‌گردد و با فعال‌سازی ابزار، سیستم کاربر به عنوان یک کلاینت جدید به حساب می‌آید.
- یک سرور که Blacklist ها را برای کلاینت‌ها فراهم می‌کند.
- یک پایگاه‌داده که Blacklist ها را نگهداری می‌کند.
- Response Authority که کل سیستم را برای ما مدیریت می‌کند.

یکی از مشکلات این سیستم این است که ما موتوری برای کشف وب‌سایت‌های Source نداریم و این سیستم با استفاده از آدرس‌های URL درون پایگاه داده اقدام به شناسایی وب سایت‌های Pass-Through می‌کند. امروزه مؤسسات بسیاری اقدام به کشف وب‌سایت‌هایی که شامل بدافزارها هستند(Source Website)،کرده و لیست این وب‌سایت‌ها را در اختیار سازمان‌ها و افراد قرار می‌دهند. بنابراین ما نیز از این لیست‌ها استفاده کرده و مخزن داده را در بخش BL-H ، در ابتدا شروع به کارسیستم و همچنین در ادامه کار سیستم با این آدرس‌ها پر می‌کنیم.

مشکل دیگر ممکن است این باشد که موتور کشف بر روی سیستم قرار نداشته باشد ولی این موضوع یک مشکل محسوب نمی‌گردد، زیرا که ابزار روی هر کلاینت توسط سرور پشتیبانی می‌شود و به جای این که حجم کل پایگاه داده روی یک سیستم قرار گیرد و حافظه زیادی مصرف کند، پایگاه‌داده به طور مستقل توسط یک سرور کنترل می‌شود، در نتیجه کاهش سربار سیستم را به همراه دارد.

مراجع

[1] Hwasu Shin, Manhyun Chung, Jong-sub Moon, "A distributed and dynamic system for detecting malware", Workshops of International Conference on Advanced Information Networking and Applications, Waina,People Republic of China, pp.738-788, 2011.

[2] Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, Nagendra Modadugu, “The ghost in the browser analysis of webbased malware", Proc. the first conference on First Workshop on Hot, Topics in Understanding Botnets (HotBots'07), USENIX Association Press, pp.4-4, 2007.

[3] Sung Hoon Kim, Eung-yong Lee, Hwa-su Shin, Jae-il Lee, "Study for development of Web Check System", World Academy of Science, Engineering and Technology,Kuala Lumpur, Malaysia, pp.669-672, 2009.

[4] Vinod P., V.Laxmi, M.S.Gaur, "Survey on malware detection methods", 10th International Conference on Internet Security, Malaviya National Institute of Technology, pp.760-765, 2007.

[5] Krishnaveni Raju, C.Chellappan, "Integrated approach of malicious website detection", International Journal Communication & Network Security(IJCNS), Volume-I, Issue-II, pp.64-67, 2011.

[6] Brendler, Beau; “Spyware/Malware Impact on Consumers”; APEC-OECD Malware Workshop; April 2007 (Source: StopBadware Project); available online at: http://www.oecd.org/dataoecd/33/55/38652920.pdf (last accessed 13 December 2007).

[7] CERT Coordination Center (2007), *The Use of Malware Analysis in Support of Law Enforcement*, available online at:http://www.securitynewsportal.com/securitynews/article.php?title=The_Use_of_Malware_Analysis_in_Support_of_Law_Enforcement (last accessed 11 December 2007).

[8] Computer Economics (2007), *2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other malicious code*, reference available at:http://www.computereconomics.com/page.cfm?name=Malware%20Report.

[9] Dancho Danchev (2006), *Malware – future trends*, available online at:www.linuxsecurity.com/docs/malware-trends.pdf (last accessed 7 December, 2007)

[10] Du, Yuejun Dr. (2007); APEC-OECD Malware Workshop; Presentation by CNCERT; available online at: http://www.oecd.org/dataoecd/33/59/38653107.pdf (last accessed 10 December, 2007)

[11] F-Secure (2007a), *APEC-OECD Joint Malware Workshop Summary Record*, available online at:www.oecd.org/sti/security-privacy.

[12] Govcert.nl (2007), APEC-OECD Malware Workshop, [presentation available at: http://www.oecd.org/dataoecd/34/36/38653287.pdf (last accessed 10 December 2007).

[13] Kaspersky Labs (2006), *Malware Evolution 2006: Executive Summary*, available online at: http://www.kaspersky.com/malware_evolution_2006_summary.

[14] Liu, Pei-Wen (2007), Information and Communication Security Technology Center, Chinese Taipei, OECD-APEC Tel Malware Workshop, available online at:http://www.oecd.org/dataoecd/34/19/38653499.pdf (last accessed 10 December 2007).

[15] NIST Special Publication 800-83, *Guide to Malware and Incident Handling*; page 2-10; available online at: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

[16] Oberoi, Sabeena (2007); *Addressing the malware Problem*, APEC-OECD Malware Workshop, available online at: www.oecd.org/sti/security-privacy.

[17] OECD (2007b), Bauer Johannes M., de Bruijne Mark, Groenewegen John P., Lemstra Wolter, and Van Eeten Michel, Delft University of Technology and Michigan State University, consultants to the OECD, *Economics of Malware: Security Decisions, Incentives and Externalities* (forthcoming).

[18] OECD (2007c); *Summary Record of the APEC-OECD Malware Workshop;* available online at http://www.oecd.org/dataoecd/37/60/38738890.pdf.

[19] Tippett, Peter (2006), *The Fourth Generation of Malware*, CIO Update, http://www.cioupdate.com/article.php/3598621 (last accessed December 7, 2007)

[20] Twomey, Paul, *Current Countermeasures and Responses by the Domain Name System Community*, APEC-OECD Malware workshop; available online at: http://www.oecd.org/dataoecd/34/40/38653402.pdf

[21] Whittaker, Colin, APACS, APEC-OECD Malware Workshop presentation; available at:http://www.oecd.org/dataoecd/33/53/38652807.pdf (last accessed 10 December, 2007).