



# ویروس‌های کامپیوتری مسئله جدیدی برای حساب‌برسان

● گردآوری : دکتر محسن شریفی

استاد و رئیس بخش حسابداری

دانشگاه میشیگان شرقی

● اهمیت کامپیوتر برای رشته حسابداری و نقش حسابداران و حساب‌برسان در کاربرد این وسیله محاسبه به میزان کافی مورد بحث و مذاقه قرار گرفته است. حسابداران از ابتدای کامپیوتریزه شدن سیستم‌ها نقش عمده‌ای را در تجزیه و تحلیل و طراحی این سیستم‌ها ایفا کرده‌اند. معذالك نوع این دخالت‌ها متناوب با تغییراتی که در تکنولوژی صورت گرفته در حال تغییر بوده است. در این زمینه پیشرفت‌های تکنولوژیک دهه اخیر به‌ترتیبی بوده که نیاز به تخصصی شدن وظایفی که توسط حسابداران و حساب‌برسان انجام می‌شود را به میزان بیش از پیش ضروری ساخته است.

این تخصصی شدن در حد خود مسائلی را پیش کشیده که قبلاً مطرح نبوده است. یکی از این مسائل در حال حاضر "ویروس‌های کامپیوتری" است که به‌صورت کابوس وحشتناکی برای مسئولان سیستم‌های کامپیوتری سازمان‌های مختلف اعم از دولتی و خصوصی درآمده است. حسابداران و حساب‌برسان افرادی هستند که در رابطه با مسائل کنترلهای داخلی در صف اول با این ویروس‌ها در مبارزه هستند.

اگرچه ویروس ها پدیده جدیدی برای میکرو کامپیوترها بحساب آمده و اخیراً "در زیر ذره بین قرار گرفته اند ، مفهوم آن اردمه ۱۹۵۰ در سیستم های بزرگ کامپیوتری مورد استفاده بوده است . این ویروس ها در ابتدا بمنظور آزمایش عکس العمل و اطمینان از امنیت سیستم های کامپیوتری بوجود آمده اند ، برنامه نویس های کامپیوتر نیز از آن بعنوان وسیله ای برای به رخ کشیدن قدرت خلاقه خود به سایر همکاران استفاده میکنند . در ابتدا این ویروس ها بطور کنترل شده و محدود در یک ناحیه خاصی از کامپیوتر توسط برنامه ریزهای بسیار مبرز بکار میرفتند . ولی متأسفانه در حال حاضر شماره افرادی که قادر به ایجاد این ویروس ها هستند روبه ازدیاد است . چیزی که این مسئله را بطور خطرناکتری مطرح میسازد نمونه کاربرد این ویروس ها بصورت آسیب زا و اشتیاق افراد به تسری این نوع ویروس ها به سایر سیستم های کامپیوتری میباشد .

دلیل دیگر برتسرز ارتسری ویروس های کامپیوتری شبکه ارتباطی مدرن امروزه است که موجبات انتقال داده های کامپیوتری را وسیله خطوط تلفن و ارتباط از طریق ماهواره فراهم ساخته است . این خطوط ارتباطی قادر هستند که در هر ثانیه میزان بسیار زیادی اطلاعات را بین سازمان های مختلف نقل و انتقال دهند . این نقل و انتقال ها و مشارکت اطلاعات بین دستگاهها خطر تسری ویروس های آسیب زا را بیش از پیش ساخته است .

نگرانی دیگری که این ویروس ها برای مسئولان سازمان ها بوجود آورده افزایش بیش از حد میکرو کامپیوترها و افرادی که از آنها استفاده میکنند میباشد . در حال حاضر میلیون ها نفر از این میکرو کامپیوترها در محل کار خود استفاده میکنند . این افراد قادر هستند که در محل کار خود از سیستمی که بطور اختصاصی برای آنها طراحی شده استفاده کرده و از اطلاعات موجود در سازمان بطور اشتراکی استفاده نمایند . در عین حال این افراد قادر هستند که با

کامپیوتر اصلی سازمان ( Main Frame ) تماس برقرار کرده و به داده پردازی مشغول شوند. گستردگی نقاط ورودی به کامپیوتر اصلی که نتیجه پراکندگی استفاده کنندگان آن میباشد خطر بالقوه ای برای گسترش این ویروس هابداخل سازمان هستند. استفاده کننده های این سیستم ها ممکن است که بدون اطلاع خود به این ویروس ها آلوده شوند. این آلودگی ممکن است از طریق ارتباط با شبکه محلی Local Area Network (LAN) یک دستگاه، برنامه کامپیوتری که از " تابلوی اعلانات " \* یک کامپیوتر اصلی پیاده شده است و یا از اشتراک یک دیسکت هایک دوست یا همکار اداری ایجاد شود.

باتوجه به اینکه تعداد واقعی حمله این ویروس ها که تاکنون گزارش شده بامقایسه باکل عملیات کامپیوتری که در هر لحظه انجام میشود ناچیز میباشد، تعداد وقایع تأیید شده ظرف چند سال اخیر بطرز سرسام آوری روبه افزایش است. این گسترش بیش از حد و افزایش در رشد این ویروس هاست که اکثر متخصصین این رشته را نگران میکند. پاره ای از این متخصصین معتقد هستند که دفعات واقعی حمله ویروس هابمراتب بیش از میزان گزارش شده آن میباشد. اردلائلی که برای آن ذکر شده بی میلی سازمانها از ایجاد تبلیغات وجو منفی است که در اثر حمله این ویروس ها برای یک دستگاه ایجاد خواهد شد. برای مثال اگر ویروس بدستگاهی که شمار آن کار میکنید حمله کند باعث رانده شدن مشتریان و بارآمدن زیانهای مالی

---

\* تابلوی اعلانات Bulletin Board به گروهی از برنامه ها و یا اطلاعات کامپیوتری اطلاق میشود که بصورت رایگان در اختیار عموم قرار داشته و پیاده کردن و یا کپی کردن از آنها مستلزم تخطی از قانون حفظ حقوق افرادی که آن برنامه ها و اطلاعات را بوجود آورده اند نمیشود.

فراوان خواهد شد. در این موارد اطمینان افرادی که با آن سازمان در سروکار هستند سلب شده و سعی میکنند که داد و ستد های خود را با سازمانهای دیگر انجام دهند. از طرف دیگر چون اکثر این ویروس ها بطور اختصاصی برای يك دستگاه طرح میشوند ممکن است باعث شوند که این نوع خاص ویروس به نام سازمان شما معروف شود. (مثلاً "ویروس بانک صنعت") صرفنظر از کلیه موارد فوق الذکر، بسیاری از سازمانها بی میل هستند که اقدامات حفاظتی موجود در سازمان خود را افشا سازند. علت آن واضح است. افشا این نوع اقدامات حفاظتی باعث کمک بیشتر به افراد خرابکار می باشد. این به نوبه خود سبب بارداری سازمانهای مختلف از اشتراك اقدامات احتیاطی بین خود خواهد بود.

#### ● انواع ویروس ها

قبل از ذکر انواع ویروس ها لازم به توضیح است که ویروس ها دارای مشخصات زیر هستند:

- ۱- مجموعه ای هستند از دستورالعمل های کامپیوتری
- ۲- قابلیت انتشار دارند
- ۳- قابلیت انجام کارهای غیرمجاز دارند
- ۴- بوجود آمدن آن بصورت عمدی است

ویروس ها معمولاً "برمبنای ویژه گیهای آنها نام گذاری میشوند". ویروس ها برنامه های (دستورالعمل) کامپیوتری هستند که موجبات آلودگی برنامه های عادی کامپیوتری را با کپی کردن خود بر روی آنها فراهم میسازند. این عمل کپی کردن و "حمله بخود" بطور مداوم ادامه پیدا کرده و از يك برنامه قابل اجرای ساده به دستورالعمل های سیستم عملیاتی (Operating System)، از يك سیستم کامپیوتری به يك سیستم دیگر از يك شبکه کامپیوتری به يك شبکه دیگر سرایت کرده و در پایان باعث نابودی کلیه این سیستم ها میشود. در نهایت این ویروس ها منظور اصلی خود را به

صورت محو کردن کلیه اطلاعات از روی دیسک ثابت ( Hard Disk ) ، قفل کردن کلیدهای کامپیوتر و ارسال پیام های ناخوشایند برآورده میکنند . خطرناک ترین نقطه مشخصه این ویروس ها کپی کردن از روی خودشان است که معمولا " هنگامی شروع میشود که ویروس مطمئن شود وارد سیستم شده و قابلیت زیستن در سیستم را خواهد داشت . ویروس ها معمولا " وجود خود را با ارسال پیامی به اطلاع افرادی که با سیستم سروکار دارند میرساند . نکته قابل تذکر اینست که کلیه ویروس ها جنبه تخریبی نداشته و پاره ای از آنها جهت محافظت سیستم کامپیوتری ( بصورت واکسن ) طراحی شده است . برای مثال ممکن است که شما برای صرفه جویی در کار برد میزان حافظه موجود در کامپیوتر و ویروسی را طرح نمایید که باعث شناسائی و نابود کردن ویروس های مضر بشود . پاره ای از ویروس های شناسائی شده عبارتند از :

" کرم " - کد ( Code ) هائی است که به جستجوی ناحیه های خالی ( استفاده نشده ) حافظه پرداخته و با کپی کردن خود آن ناحیه را پر میکند . هدف اصلی این کرم ها پر کردن کلیه ناحیه های استفاده نشده حافظه کامپیوتری به ترتیبی است که ادامه فعالیت های کامپیوتری را کلا " قطع کرده و در نهایت باعث نابودی سیستم بشود . وظیفه اصلی کرم فقط کپی کردن مداوم خود میباشد که تفاوت اصلی کرم با سایر ویروس ها است . فرق دیگر کرم با سایر ویروس ها اینست که کرم خط ارتباطی خود را با برنامه اصلی که در حافظه کامپیوتر قرار گرفته حفظ مینماید .

\* " اسب ترویا " - برنامه هائی هستند که ظاهرا " عملیات مجاز را انجام میدهند در حالیکه کد غیر مجاری را در داخل خود مخفی کرده

---

\* این اسم از داستان قدیمی غربی گرفته شده که سربازان خود را در داخل شکم اسبی بزرگ مخفی کرده و پس از اینکه اسب بدخل شهر ترویا انتقال پیدا کرد از تاریکی شب استفاده کرده و شهر را تسخیر کردند .

و در موقع مناسب بطور غیرمنتظره ضربه کاری خود را وارد میکنند .  
این ضربه بصورت پاك کردن يك پرونده كلي ( مانند پرونده لیست حقوق ) میباشد . این برنامه ها معمولاً " بطرزی نوشته شده اند که تامت مدیدی بصورت طبیعی دستورالعمل های مورد نظر را اجرا کرده و سپس بحض یافتن فرصت سیستم تخریبی خود را به کار می اندازند . از مشخصات اصلی این نوع ویس ————— روس اینست که هیچگاه کپی خود را ایجاد نمیکند .

" بمب منطقی " - قسمتی از کد تخریبی کامپیوتر است که منطبق بر يك واقعه از قبل پیش بینی شده ( مثلاً " شب یلدا و یا چهارشنبه سوری ) منفجر میشود . پاره ای از این نوع برنامه ها بترتیبی نوشته شده اند که انفجار آنها مبتنی بر وقوع شرایط غیرمعقول ( مثلاً " ماه ۲۲ روزه ) اتفاق خواهد افتاد .

" دریچه " - دریچه ها کد کامپیوتری نبوده و جز گروه ویروسهای اصلی طبقه بندی نمیشوند . در واقعیت " دریچه " ورود غیرمترقبه به داخل سیستم ویرش از روی اقدامات امنیتی عادی میباشد . این نوع برنامه ها باعث میشود افراد خاطی در شرایطی قرار گیرند که بتوانند بطور نامحدودی از برنامه ها و پرونده های موجود در سیستم استفاده نمایند در حقیقت این روشی است که توسط آن اشخاص مغرض وارد سیستم شده و پس از داخل کردن ویروس کلیه سیستمها را آلوده مینمایند .

ترکیب کردن روشهای فوق بصورت ایجاد ویروسی واحد باعث میشود که ضربه وارد کردن به سیستم کامپیوتری بطرز موثرتری انجام پذیرد . برای مثال ویروس معمولاً " در داخل برنامه ای مخفی شده و بصورت " اسب ترویا " به داخل سیستم راه داده میشود . در غیر اینصورت امکان نشر این آلودگیها از يك استفاده کننده به استفاده کننده دیگر و یا از يك تابلو اعلانات به سایر استفاده کنندگان امکان پذیر نخواهد بود .

ویروس ها اغلب دارای " چاشنی " ای هستند که معمولاً " جلب نظر

نکرده و قادر هستند مدت زیادی در سیستم کامپیوتری باقی بمانند .  
 این چاشنی ها دقیقاً همان بمب های منطقی هستند که منتظرند در  
 صورت یافتن فرصت مناسب کشیده شده و سبب انفجار سیستم را  
 فراهم نمایند . طبقه بندی فوق مانع الجمع نیست و ممکن است که  
 يك ويروس اريك يا چند خاصیت فوق برخوردار باشد . معذالك  
 شناخت آنها بر مبنای خاصیت غالبی است که در آن نوع ويروس به  
 خصوص مشاهده شده است .

### چگونگی همه گیر شدن ويروس ها

يكی از منابع بروز ويروس ها در دستگاه های دولتی و یا خصوصى  
 کارمندان ناراضی هستند . این قبیل کارمندان معمولاً چند روز  
 یا چند ساعت پس از دریافت اختاریه حاکی از اخراجشان و یا تذکر  
 برای کارهائی که انجام داده اند شروع به عملیات تخریبی مینمایند  
 در پاره ای از موارد مشاهده شده که این قبیل کارمندان با قرارداد  
 يك " بمب منطقی " باعث از بین بردن هزاران پرونده اطلاعاتی  
 مربوط به فروش و یا لیست حقوق شده اند .

سازمانها باید بمنظور جلوگیری از عواقب ناشی از اخراج این قبیل  
 کارمندان چند قاعده کلی را مراعات کنند . برای مثال هرگز  
 نباید به کارمندانی که اخراج شده اند امکان دسترسی به مدارك  
 و اسناد سازمان داده شود . عملی کردن این سیاست بصورت باطل  
 کردن " اسم رمزى \* " این نوع کارمندان و مطلع نمودن مسئولین  
 از اینکه این کارمندان حق استفاده از سیستم کامپیوتری را ندارند  
 امکان پذیر خواهد بود . مرتب گوش بزنگ باشید که آیا این کارمندان  
 از اسم رمز کارمندان دیگر استفاده میکنند یا خیر ؟ در صورت یافتن

---

\* اسم رمز معمولاً کلمه و یا شماره هائی است که بطور اختصاصی به  
 افراد واگذار شده و آنها را قادر میسازد که بتوانند به آزادی وارد سیستم  
 کامپیوتری شوند . در عمل معادل داشتن کلید برای وارد شدن به محل  
 کار یا منزل میباشد .

پاسخ مثبت به این سؤال فوراً" اسم رمز این نوع کارمندان را عوض کرده و به آنها گوشزد نمائید که از اسم رمز خود مراقبت کافی بعمل آورند.

کارمندان صادق خطرناک ترین نوع تهدید برای يك سازمان هستند ! این خطر معمولاً بصورت آوردن يك برنامه کامپیوتری شخصی به محل کار بروز میکند. این نوع برنامه ها معمولاً "از نوع پیچیده و تخصصی نبوده و در نتیجه اگر ویروسی در آنها وجود داشته باشد بمجرد تماس با کامپیوترها و یا ترمینال های سازمان منجر به سرایت به سایر کامپیوترها میشود. واضح است که این نوع کارمندان بیگانه از این خطر اطلاع نداشته و بدون توجه بانسخه گرفتن يك برنامه از روی يك تابلوی اعلانات سبب تسری ویروس بداخل سازمان میشوند. در بسیاری از موارد ممکن است که این همکاری مدیدی از این برنامه استفاده نمیکرده و تصادفاً نسخه جدیدی از این برنامه را (که تصادفاً آلوده نیز میباشد) در يك تابلوی اعلانات پیدا کرده که بمجرد نسخه گرفتن باعث پاك شدن نسخه قبلی خود شده و پس از این عمل باعث عفونت زدگی برنامه خود میشود.

مسئله مهم اینست که آیا کارکنان میتوانند نرم افزارهای خود را به محل کار بیاورند و یا باید طبق دستورالعملی از ورود آنها به محل کار جلوگیری بعمل آید. دلیل بروز وقوع این امر اینست که بسیاری از کارکنان کارائی به مراتب بیشتری از خود نشان میدهند در صورتیکه قادر باشند در محیط قابل انعطافی فعالیت نمایند. در اینجا مشکل مدیریت اینست که باید بین دو عامل مختلف یعنی کارائی کارکنان و خطر آلودگی سیستم های کامپیوتری یکی را انتخاب نماید. بسیاری از سازمان ها به پیچوجه به کارمندان خود اجازه نمیدهند که نرم افزارهای کامپیوتری خود را به محل کار بیاورند. در حالیکه پاره از شرکتها راه عملی تر را برگزیده و از کارکنان خود میخواهند که اولاً نرم افزارهای خود را قبل از استفاده حتماً از قرنطینه ای که به این منظور ایجاد شده بگذرانند ثانیاً فقط از نرم افزارهای به ثبت رسیده استفاده کرده و ثالثاً از آوردن نرم افزارهاییکه از روی تابلو

اعلانات کپی شده به محل کار خودداری نمایند. در بسیاری از موارد مشاهده شده که کارکنان مجاز هستند که فقط اطلاعات (داده های) کامپیوتری خود را به محل کار آورده و مجاز نیستند که برنامه های کامپیوتری به محل کار بیاورند. درپاره ای از سازمانها مشاهده میشود که پرونده های مربوط به "داده ها" و برنامه های کامپیوتری بصورت مجزا از یکدیگر نگهداری میشود. در حالت های دیگر مشاهده شده که ویروس ها بطور تصادفی وارد برنامه هایی شده اند که بصورت مجاز در بازار بفروش میرسند. برای جلوگیری از این خطرات لازم است که نرم افزارهای خود را از فروشندگان معتبر خریداری کرده و پس از اکتیاع مطمئن شوید که لاک و مهر بسته آن قبلاً "دست نخورده باشد".

چگونه سلامت سیستم کامپیوتری خود را تأمین کنید ؟

جهت جلوگیری از بروز وقایع ناگوار ناشی از ویروس ها راه های مختلفی وجود دارد ولی متأسفانه هیچکدام محفوظ از خطا نمیباشد. اگر چه امکان دفع کامل حمله ویروس ها وجود ندارد معذالك اقدامات احتیاطی که توسط يك سازمان میشود سبب کاهش بروز این حمله ها میگردد.

یکی از مهمترین اقداماتی که باید انجام گیرد ایجاد سیاستی واحد برای يك دستگاه و یا گروه صنعتی و اشاعه این سیاست بین کارکنان میباشد. این اقدامات باید از حمایت کامل مدیریت برخوردار بوده و عواقب تخلف از آن تعیین و به اطلاع کارمندان برسد. موارد زیر بصورت پیشنهادی ارائه شده است :

۱- مجاز نبودن از تهیه نسخه از برنامه هایی که در روی تابلوی اعلانات قرار دارد. اگر برنامه مفیدی در روی این تابلوی اعلانات پیدا شد باید مطمئن شد که از قرنطینه گذشته و بدون ویروس وارد سازمان بشود. قسمت قرنطینه باید مطمئن شود که این برنامه بطور دقیق مورد آزمایش قرار گرفته و از کپی کردن آن بروی دیسک های ثابت خودداری شود. ضمناً قرارداد دادن این نوع برنامه ها بر روی شبکه

محلی غیرمجاز اعلان شود.

۳ ایجاد سیاست روشن در رابطه با همراه آوردن نرم افزارها و پرونده اطلاعات ("داده ها) به محل کار. همانطور که قبلاً ذکر شد تدوین این سیاست باید با توجه به کارآئی کارکنان و اثر منفی آن بر روی روحیه کارمندان انجام پذیرد.

۴ ایجاد رویه خاص جهت جلوگیری از نوشتن بر روی برنامه های اجرایی موجود. در این حالت کلیه برنامه ها در پرونده هائی ضبط میشود که فقط "قابل خواندن" \* هستند و امکان نوشتن روی آن پرونده ها وجود ندارد.

۵ در هنگامی که از منابع کامپیوتری دیگران استفاده میشود کارمندان باید مطمئن شوند که از برنامه های "اجرایی" استفاده نکرده و فقط مجاز به استفاده از پرونده های اطلاعاتی (داده ها) باشند. تجربیات گذشته نشان داده که امکان فساد داده ها بمراتب کمتر از فساد برنامه های قابل اجرا میباشد.

۶ در هنگام استفاده از یک میکرو کامپیوتر حتماً قبل از استفاده آن را خاموش نمایند. عمل خاموش کردن باعث تمیز شدن حافظه میشود که در نتیجه ویروس هائی که بطور احتمالی در سیستم حافظه مرکزی کامپیوتر از برنامه های قبلی باقیمانده باشند از بین خواهند رفت.

۷ میکرو کامپیوترها فقط با دیسکت هائی روشن شوند که بطور اختصاصی برای کارمندان تهیه شده است. این رویه باعث خواهد شد که فقط سیستم عملیاتی (Operating System) مجاز وارد کامپیوتر شود.

---

\* نرم افزارها را اثر خواندن از بین نرفته و آلوده نمیشوند. عمل نوشتن بر روی این برنامه ها و یا نرم افزارهاست که سبب تخریب و آلودگی و یا از بین بردن کلی آنها میشود.

۷- سیستم های کامپیوتری چه بصورت " فیزیکی " و چه بصورت " منطقی " مورد محافظت قرار گیرند . قفل کردن میکرو کامپیوترها استفاده غیر مجاز آنها جلوگیری خواهد نمود . همچنین ایجاد اسم رمز برای بکاربردن برنامه های موجود باعث خواهد شد که افراد غیر مجاز قادر به دسترسی به آنها نباشند .

۸- نصب برنامه های ضد ویروس بر روی کامپیوترها . این نوع برنامه ها معمولاً " قادر هستند وقایع ناگوار را ( مثلاً " پاک کردن کامل دیسک ثابت ) اعلان نمایند .

۹- تهیه نسخ متعدد از پرونده های اطلاعاتی و برنامه های موجود در یک سازمان . این نسخه ها معمولاً " در مکان امن مثل گاوصندوق نگهداری میشوند . این رویه سبب بازسازی کلیه پرونده های از بین رفته میشود .

#### خلاصه

ویروس های کامپیوتری مجموعه دستورالعمل های کامپیوتری هستند که بسادگی از یک کامپیوتر یا دیسک به یک کامپیوتر یا دیسک دیگر انتقال پیدا کرده و با انجام کارهای غیر مجاز باعث تخریب و آلودگی سیستم میگردند . حسابداران و حسابرسان بخصوص آندسته از حسابرسان که با کامپیوتر سروکار دارند باید با این نوع ویروس ها آشنائی کامل داشته باشند . فقط در این صورت حسابرسان قادر خواهند بود توصیه های خود را در خصوص سیستم کنترلهای داخلی و حفظ تمامیت این نوع سیستم ها به مشتریان خود بنمایند . البته با کامپیوتری شدن کلیه سیستم های مالی و اطلاعاتی کلیه حسابداران ناگزیر خواهند بود که خود را با این بلای تکنولوژی آشنا ساخته و در صورت لزوم با آن مبارزه نمایند ●