همه چیز درباره ویروس‌ها، کرم‌ها، اسب‌های تروا و فراتر از آن

« بخش اول »

کلیه حقوق این مقاله متعلق به سایت امنیت وب و مترجم آن می باشد و هر گونه برداشت از آن فقط با ذکر نام سایت و نام نویسنده مجاز می باشد.

مترجم : رضا مددی / rzmadadi@yahoo.com

منبع : www.Sophos.com

تاریخ : ۱۴ اردیبهشت ۱۳۸۳

در صورتی که شما :

- یک مدیر شبکه هستید،
- فردی هستید که با دوستان خود دیسک مبادله می‌کند،
- از شبکه‌های محل کار خود استفاده می‌کنید،
- و یا فقط خواننده نامه‌های الکترونیکی هستید،

بدانید که این مطلب برای شماست!

ما حقایق را در باره ویروس‌های کامپیوتری بطور ساده و با زبانی قابل فهم برای شما بیان می‌کنیم.

فهرست مطالب

بخش اول

- چرا ویروس‌ها مهم هستند؟
- ویروس ها، اسب‌های تروا و کرم‌ها
- تعریفی ساده از ویروس، اسب تروا، کرم
- ویروس چیست؟
- ویروس چگونه بر روی کامپیوتر تاثیر می‌گذارد؟
- اسب‌های تروا
- کرم‌ها
- ویروس‌ها چه کارهایی می‌توانند انجام دهند؟
- خطر مربوط به ویروس‌ها در چه جاهایی وجود دارد؟
- جلوگیری کردن از ویروس‌ها
- ویروس‌های سکتور بوت
- ویروس‌های انگلی
- ویروس‌های ماکرو (کلان دستور)

بخش دوم

- نرم‌افزار ضد ویروس
- پویشگرها
- Checksummer ها
- نرم‌افزارهای کاشف (Heuristic)
- هزینه‌های پنهانی ویروس‌ها
- ویروس‌نویسان چه کسانی هستند؟
- آیا نوشتن ویروس همیشه نادرست است؟
- ویروس‌های گولزن (Hoax ها)
- Hoax ها چیستند؟
- چرا Hoax ها یک معضل هستند؟
- چه کارهایی را در مورد Hoax ها می‌توان انجام داد؟
- تاریخچه مختصری از ویروس‌ها
- ۱۰ ویروس برتر

بخش سوم

- پست الکترونیک
- آیا به صرف خواندن نامه، ویروسی می‌شویم؟
- ویروس‌هایی که بطور خودکار از طریق نامه‌ها گسترش می‌یابند
- خطرات فایل‌های پیوندی
- چگونه ویروس‌های پستی را متوقف کنیم؟
- اینترنت
- کلیک کردن و آلوده شدن؟
- آیا به صرف دیدن وب‌سایت‌ها، ویروسی می‌شویم؟
- دستورات برنامه‌نویسی وب‌سایت‌ها
- اسب‌های تروای «در پشتی» و اینترنت
- آیا کوکی‌ها خطرناک هستند؟
- حمله‌ها به سوی وب‌سرورها
- امنیت در شبکه

بخش چهارم

- تلفن‌های موبایل و کامپیوترهای کف‌دستی
- آیا ویروس‌های موبایل هم وجود دارند؟
- تلفن‌های WAP و ویروس‌ها
- خطرات آتی برای WAP
- سیستم‌عامل‌های کامپیوترهای کف‌دستی
- ویروس‌ها برای یخچال‌ها؟
- چگونگی محافظت از ابزارهای متحرک (Mobile)
- ده مرحله برای ایجاد امنیت در کار با کامپیوتر
- لینک‌های مفید

بخش اول

چرا ویروس‌ها مهم هستند؟

ویروس‌های کامپیوتری، هکرها، کراکرها و جرم‌های اطلاعاتی.

اینها تیترهای مهم خبری اخبارها شده‌اند - همان چیزی که رسانه‌ها خواستار آن هستند - و میلیونها هزینه برای ما دارند. اما آیا ویروس‌ها و بقیه موارد ناخوشایند واقعا مهم هستند؟ آیا آنها واقعا مضر می‌باشند؟

اگر شما ذره‌ای در این مورد شک دارید، فقط سعی کنید که تصور کنید چه اتفاقاتی میتواند در خانه یا محیط کار شما رخ دهد.

فرض کنید ماهها نرم‌افزار ضد ویروس خود را ارتقاء نداده‌اید و زمانی که این کار را انجام می‌دهید، متوجه می‌شوید که برنامه‌های صفحه گسترده شما با ویروس جدیدی که تصاویر را بطور تصادفی تغییر می‌دهد، آلوده شده‌اند. شما طبیعتا قبلا از آنها پشتیبان تهیه کرده‌اید، اما بدون اینکه بدانید ماهها این کار را بر روی فایلهای آلوده انجام داده‌اید. حالا شما از کجا می‌توانید بفهمید که کدام تصویر واقعا درست و کدام تصویر نادرست است؟

حالا تصور کنید که یک ویروس پستی جدید منتشر شده و بواسطه آن شرکت شما نامه‌های بسیار زیادی را دریافت می‌کند. بنابراین شما تصمیم می‌گیرید صندوق خود را ببندید و به همین سادگی سفارشی مهم که خریداری بزرگ آن را برای شما فرستاده بود را از دست می‌دهید.

فرض کنید که در حال آماده سازی پایان نامه برای تحویل به استاد دانشگاه می‌باشید. برادرتان یک سی‌دی بازی جدید را در کامپیوتر شما قرار داده و دستگاهتان را به ویروس آلوده می‌کند. ویروس همه چیز بر روی دیسک سخت دستگاه شما را پاک کرده و تمام زحماتتان را به باد می‌دهد.

فرض کنید دوستی فایل‌هایی را که از اینترنت گرفته، با پست الکترونیک برای شما ارسال می‌کند. شما فایل‌ها را باز کرده و باعث به جریان افتادن ویروسی می‌شوید که تمام اسناد و بخصوص اسناد محرمانه شما را برای تمام افرادی که آدرس آنها در دفترچه آدرس سرویس پست الکترونیکی شما قرار دارد، ارسال می‌کند (شاید بعضی از این افراد از رقبای شما باشند).

و در نهایت تصور کنید که بطور تصادفی سندی که شامل ویروسی بوده را برای شرکتی دیگر فرستاده‌اید آیا به نظر شما آنها دوباره برای انجام امور بازرگانی با شما، احساس امنیت از جانب شما خواهند داشت؟

چنین اتفاقاتی همیشه در حال وقوع هستند. اما در همه موارد با اقدامات احتیاط آمیز بسیار ساده‌ای که بعضی از آنها هیچ هزینه‌ای هم ندارند، می‌توان از رخداد اینگونه مسائل جلوگیری کرد.

در ادامه خواهیم گفت که چه خطراتی وجود دارند و شما چگونه می‌توانید مانع آنها شوید.

ویروس ها، اسب‌های تروا و کرم‌ها

در اواسط دهه ۸۰ میلادی،« امجد» و «بسیط» در لاهور پاکستان، به این مطلب پی بردند که بعضی افراد نرم‌افزارهای آنها را بدون اجازه منتشر می‌کنند. آنها این کار را با نوشتن اولین ویروس کامپیوتری پاسخ دادند. این ویروس برنامه‌ای بود که به هنگام کپی هر دیسکتی توسط استفاده کنندگان، یک نسخه از خود و یک پیغام کپی‌رایت را بر روی دیسکت کپی می‌کرد.

با این شروع ساده بود که فرهنگ همه‌گیر ویروس‌نویسی پدیدار شد. امروزه ویروس‌های جدید تمام سیاره خاکی را در عرض چندین ساعت پیموده و ترس‌های ویروسی به اخباری مهم تبدیل شده‌اند. مردم مات و مبهوت شده‌اند، اما هیچگاه به خوبی در پی آگاه شدن نرفته‌اند.

ادامه مطالب را بخوانید تا ببینید ویروس‌ها چگونه منتشر می‌شوند و شما چگونه می‌توانید از خود محافظت کنید.

تعریفی ساده از ویروس، اسب تروا، کرم

ویروس چیست؟

یک ویروس کامپیوتری برنامه‌ای کامپیوتری است که می‌تواند با ایجاد کپی از خود، در کامپیوترها و شبکه‌ها گسترش پیدا کند و این کار معمولا بدون آگاهی کاربر صورت می‌گیرد.

ویروس‌ها می‌توانند تاثیرات زیان‌بار گوناگونی از نمایش پیغام‌های تحریک‌کننده گرفته تا پاک کردن تمام فایل‌ها بر روی کامپیوترها داشته باشند.

ویروس چگونه بر روی کامپیوتر تاثیر می‌گذارد؟

یک برنامه ویروس باید اجرا شود تا بتواند بر روی کامپیوتر شما تاثیری بگذارد.

ویروس‌ها راههای گوناگونی برای اطمینان از رخ دادن این اتفاق دارند. آنها می‌توانند خود را به برنامه‌های دیگر بچسبانند و یا اینکه خود را در دستوراتی که به هنگام باز شدن انواعی از فایل‌ها بطور خودکار اجرا می‌شوند، مخفی کنند.

ممکن است شما فایل آلوده را بر روی یک دیسکت، در یک فایل پیوندی نامه الکترونیکی و یا به هنگام بارگذاری فایلی از اینترنت، دریافت کنید. به محض اینکه شما فایل را اجرا کنید، دستورات ویروسی اجرا خواهند شد. سپس ویروس می‌تواند خود را در فایل‌ها یا دیسک‌های دیگر کپی کرده و تغییراتی در دستگاه شما بوجود آورد.

برای جزییات بیشتر بخش‌های مربوط به ویروس‌های سکتور بوت (Boot Sector Virus)، ویروس‌های انگلی (Parasitic Viruses) و ویروس‌های تشکیل شده از کلان دستورها (Macro Virus) را در بخش‌های بعدی این فصل مطالعه کنید.

اسب‌های تروا

اسب‌های تروا برنامه‌هایی هستند که کارهایی را انجام می‌دهند که در مشخصه‌هایشان به آن کارها اشاره‌ای نشده است.

کاربران با اجرای برنامه‌ای که به تصورشان قانونی، مجاز و معقول است، اجازه می‌دهند تا آن برنامه کارهایی مخفی و اغلب مضر را انجام دهد.

بـرای مثال برنامه (اسب تروای) Zulu ادعا کرده بود که برنامه‌ای است برای درست کـردن مشـکل هـزاره (Millennium bug) ، اما در واقع برنامه‌ای بود که اطلاعات روی دیسک سخت را بازنویسی کرده و از بین می‌برد.

در اغلـب اوقـات اسـب‌هـای تـروا بـه عـنوان راهی برای آلوده کردن کاربر توسط ویروس‌های کامپیوتری مورد استفاده قرار می‌گیرند.

اسـب‌هـای تـروای با عنوان «در پشتی» یا «رخنه پشتی» برنامه‌هایی هستند که به کاربـران کامپـیوترهای دیگـر اجازه می‌دهند تا از طریق اینترنت کنترل کامپیوتر شما را در اختیار بگیرند.

کرم‌ها

کـرم‌هـا شـبیه بـه ویـروس‌هـا هسـتند با این تفاوت که نیازی به حامل‌هایی مانند ماکروها (کلان‌دستور) یا سکتور بوت ندارند.

کـرم‌هـا به سادگی کپی‌های دقیقی از خود ایجاد کرده و از ارتباطات بین کامپیوترها برای گسترش خود استفاده می‌کنند.

بسـیاری از ویـروس‌هـا مانـند (VBS/Kakworm) Kakworm یـا Love Bug (VBS/LoveLet-A) رفتاری مانند کرم‌ها داشته و از نامه‌های الکترونیکی برای فرستادن خود به کاربران دیگر استفاده می‌کنند.

ویروس‌ها چه کارهایی می‌توانند انجام دهند؟

ویـروس‌هـا علاوه بر کار اصلی خود، کارهای فرعی دیگری که در اکثر اوقات از آنها بـرای جلـب توجـه کاربر استفاده می‌شود (و به این قسمت از برنامه ویروس اکثرا Payload گفته می‌شود)، انجام می‌دهند. در قسمت زیر بعضی از اینگونه فعالیت‌ها آورده می‌شود.

پیغام‌ها : ویروس WM98/Jerk پیغام «من فکر می‌کنم ... – در اینجا اسم کاربر را ذکر می‌کند– یک احمق بزرگ است» را نمایش می‌دهد.

شـوخی‌هـا : ویـروس Yankee بـرنامه طـنز Yankee Doodle Dandy را در ساعت ۵ بعدازظهر اجرا می‌کند.

غـیر فعال کردن دسترسی‌ها : ویروس WM97/NightShade در جمعه‌های با تارخ ۱۳ هر ماه، متن‌های باز شده در دستگاه را توسط کلمه رمزی غیر قابل دسترسی می‌کند.

سـرقت اطلاعات : اسب تروای LoveLet-A اطلاعات مربوط به کاربر و دستگاه او را به آدرسی در فیلیپین ارسال می‌کند.

خـراب کـردن اطلاعات : ویروس XM/Compatable تغییراتی در اطلاعات صفحه‌های طراحی شده توسط برنامه Excel بوجود می‌آورد.

پـاک کردن اطلاعات : ویروس Michelangelo در روز ۶ ماه مارس قسمتی از اطلاعات بر روی دیسک سخت را بازنویسی کرده و از بین می‌برد.

غـیرقابل دسترسی کردن سخت‌افزار: ویروس CIH یا Chernobyl (W95/CIH-10xx) در روز ۲۶ مـاه آوریل اطلاعات بر روی بایوس را بازنویسی کرده و آنها را ازبین می‌برد. با این کار دستگاه غیر قابل استفاده خواهد شد.

خطر مربوط به ویروس‌ها در چه جاهایی وجود دارد؟

در این بخش مواردی که کامپیوتر شما در آنها آسیب‌پذیر خواهد بود، معرفی خواهد شد:

اینترنت:

با Download کردن برنامه‌ها یا فایل‌هایی که می‌توانند آلوده باشند.

نامه الکترونیکی:

نامـه‌هـا ممکـن است شامل فایل‌های پیوندی آلوده باشند. اگر شما بر روی یک فایل پـیوندی آلـوده دوبـار متوالـی کلـیک کنـید (آن را بـاز کنـید)، بـا این کار خطر آلوده شدن دسـتگاهتان را پذیرفته‌اید. بعضی نامه‌ها حتی شامل دستورات اسکریپتی مخربی هستند که هـر وقـت شـما بـه سـراغ پسـت الکترونیکـی خود می‌روید و یا محتوای نامه‌ای را مطالعه می‌کنید، اجرا می‌شوند.

برنامه‌ها:

بـرنامه می‌توانند حامل ویروسی باشند که به محض اجرا شدن برنامه دستگاه شما را ویروسی کنند.

اسناد (متون) و فایل‌های صفحه گسترده (فایل‌های طراحی شده توسط برنامه Excel و ...):

ایـن فـایل‌هـا ممکن است شامل ویروس‌هایی از نوع ماکرو (کلان دستور) باشند که می‌توانند اسناد و فایل‌های صفحه‌گسترده دیگر را آلوده کرده و یا تغییراتی در آنها بوجود آورند.

دیسک‌های نرم و سی‌دی‌ها:

دیسـک‌های نرم می‌توانند ویروسی در سکتور بوت خود داشته باشند. آنها همچنین ممکـن اسـت شـامل بـرنامه‌هـا یـا اسناد آلوده‌ای باشند. CD ها نیز موارد آلوده را در خود نگاه‌داری می‌کنند.

جلوگیری کردن از ویروس‌ها:

در اینجا اقدامات ساده‌ای برای انجام به هنگام آلوده شدن و یا جلوگیری از آلوده شدن بیان شده است.

آگاه کردن کاربران از خطرات:

به همه افراد سازمان خود بگویید که معاوضه کردن دیسکت با افراد دیگر، Download کردن فایل از وب‌سایت‌ها و یا باز کردن فایل‌های پیوندی نامه‌های الکترونیکی خطرناک می‌باشد.

نرم‌افزار ضد ویروس نصب کرده و مرتبا آن را Update کنید:

برنامه‌های ضد ویروس می‌توانند ویروس‌ها را شناسایی کرده و در اغلب اوقات آنها را از بین ببرند.

در صورتیکه برنامه ضد ویروس پیشنهاد می‌کند تا به هنگام اجرای نرم‌افزارهای گوناگون وجود ویروس را بررسی کند، اینکار را انجام دهید.

بررسی‌های به هنگام اجرای برنامه‌ها مانع از دسترسی کاربران به فایل‌های آلوده می‌شود.

بخش مربوط به نرم‌افزارهای ضد ویروس را در قسمت‌های بعدی همین فصل مطالعه بفرمایید.

از تمام اطلاعات خود پشتیبان تهیه کنید:

اطمینان پیدا کنید که از تمام اطلاعات، نرم‌افزارها و سیستم‌عامل‌های خود پشتیبان تهیه کرده‌اید. در صورتیکه شما توسط ویروسی آلوده شوید، می‌توانید فایل‌ها و برنامه‌هایتان را با کپی‌های تمیز آنها جایگزین کنید.

برای جزییات بیشتر، بخش « ده مرحله برای ایجاد امنیت در کار با کامپیوتر» را مطالعه کنید.

انواع ویروسها

ویروس‌های سکتور بوت (سکتور از بخش‌بندی‌های فضای بر روی دیسک‌ها می‌باشد).

ویـروس‌های سکتور بوت، اولین نوع ویروس‌هایی بودند که مشاهده شدند. آنها از طـریق تغیـیر دادن سـکتور بـوت - قسـمتی سخت‌افزاری از دیسک که در آن برنامه‌ای قرار می‌گیرد که باعث شروع به کار کامپیوتر شما می‌شود- گسترش می‌یابند.

هنگامی که شما کامپیوتر را روشن می‌کنید، سخت‌افزار به دنبال برنامه سکتور بوت - کـه معمـولا بر روی دیسک سخت است، ولی می‌تواند بر روی فلاپی یا سی‌دی هم باشد - می‌گردد تا آن را اجرا کند. این برنامه با اجرا شدن، وقفه سیستم‌عامل را در حافظه بارگذاری (Load) می‌کند.

یـک ویـروس سـکتور بـوت، نسخه اصلی برنامه سکتور بوت را با نسخه‌ای تغییر یافـته و مـربوط به خود جایگزین کرده و نسخه اصلی را معمولا در جایی دیگر روی دیسک سـخت پنهان می‌کند. هنگامی که شما در مرتبه بعدی دستگاه را روشن می‌کنید، سکتور بوت آلوده شده، مورد استفاده سخت‌افزار قرار خواهد گرفت و بنابراین ویروس فعال خواهد شد.

پـس در صـورتیکه شما دستگاه را به وسیله یک دیسکت آلوده - معمولا دیسک‌های نرمی که سکتور بوت آلوده دارند - راه‌اندازی کنید، در نهایت آلوده به ویروس خواهید شد.

بسـیاری از ویـروس‌های سکتور بوت در حال حاضر دیگر جزء ویروس‌های کهنه و قدیمـی محسوب می‌شوند. آنهایی که برای دستگاه‌های تحت سیستم‌عامل DOS نوشته شده بودنـد، معمولا نمی‌توانند از طریق سیستم‌عامل‌های ویندوز 95 ، 98 ، ME ، NT ، 2000 و XP گسـترش یابـند، گـرچه ممکـن است گاهی اوقات این سیستم‌عامل‌ها را از راه‌اندازی صحیح متوقف کنند.

معرفی ویروس‌هایی از این نوع:

ویـــروس Form : ویروســی است که پس از ۱۰ سال بعد از اولین مشاهده، هنوز هم رایـج اسـت. نسخه اصلی آن در روز ۱۸ هر ماه، فعال شده و هنگامی که هر دکمه‌ای بر روی صفحه کلید فشرده شود، باعث ایجاد یک کلیک می‌شود.

ویروس Parity Boot : ویروسی است که بطور تصادفی پیغام PARITY CHECK را نمـایش داده و سیستم عامل را قفل می‌کند. این پیغام مانند پیغامی واقعی است که به هنگام ایجاد خطا در حافظه کامپیوتر نمایش داده می‌شود.

ویروس‌های انگلی:

ویـروس‌هـای انگلـی کـه بـا نـام ویروس‌های فایل هم شناخته می‌شوند، خود را به برنامه‌ها یا همان فایل‌های قابل اجرا پیوند می‌زنند.

هنگامـی که شما اجرای برنامه آلوده شده توسط ویروسی را آغاز می‌کنید، در ابتدا ویـروس اجـرا خواهد شد. سپس ویروس برای مخفی نگاه‌داشتن حضور خود، برنامه اصلی را اجـرا مـی‌کند. سیستم عامل دستگاه که ویروس را بخشی از برنامه اجرا شده توسط شما مـی‌دانـد، بـه آن مجوزهای اجرا را می‌دهد. این مجوزها به ویروس اجازه می‌دهند تا از خود کپی بسازد، خود را در حافظه کامپیوتر قرار داده و بدنه خود را آزاد کند.

ویـروس‌هـای انگلـی در تاریخچه ویروس‌ها از نخستین انواع آنها می‌باشند، اما در حـال حاضر نیز از تهدیدات واقعی به شمار می‌روند. شبکه اینترنت که گسترش برنامه‌ها را ساده‌تر کرده، به ویروس‌ها نیز فرصتی جدید برای گسترش داده است.

معرفی ویروس‌هایی از این نوع:

ویـــروس Jerusalem : در جمعه‌های با تارخ ۱۳ هر ماه، تمام برنامه‌های اجرا شده در کامپیوتر را پاک می‌کند.

ویروس CIH یا همان Chernobyl : در روز ۲۶ از ماههای مشخصی، اطلاعات چیپ بـایوس را بازنویسـی کرده و از بین می‌برد. با این کار کامپیوتر غیرقابل استفاده می‌شود. این ویروس همچنین اطلاعات دیسک سخت را نیز بازنویسی می‌کنند.

ویـــروس Remote Explorer : ویـــروس WNT/RemExp(Remote Explorer) فـایل‌هـای اجرایی ویندوز NT را آلوده می‌کند. این ویروس اولین ویروسی بود که توانست خـود را به عنوان یک سرویس – برنامه‌هایی که در ویندوز NT حتی در زمان‌هایی که کسی Log in نکرده، اجرا می‌شوند – در ویندوز NT اجرا کند.

ویروس‌های ماکرو (کلان دستور)

ویـروس‌هـای ماکـرو کـه از مـزایای برنامه‌نویسی ماکرو سود می‌برند، دستوراتی هستند که در دستورات داخل فایل‌ها ادغام شده و به صورت خودکار اجرا می‌شوند.

بسـیاری از بـرنامه‌هـا مانـند برنامه‌های واژه‌پرداز یا تهیه‌کننده صفحه‌گسترده از خاصیت برنامه‌نویسی ماکرو استفاده می‌کنند.

ویروس ماکرو، یک برنامه ماکرو است که می‌تواند از خود کپی ساخته و از فایلی به فـایل دیگـر گسترش پیدا کند. در صورتیکه شما فایلی را باز کنید که حامل ویروسی از نوع

ماکـرو است، در اینصورت ویروس خود را در فایل‌های آغازین اجرای آن برنامه کپی می‌کند و این زمان زمانی است که کامپیوتر آلوده شده است.

زمانی که شما در مرحله بعد فایلی را باز می‌کنید که از همان برنامه استفاده می‌کند، ویروس، آن فایل را هم آلوده خواهد کرد. در صورتیکه کامپیوتر شما در یک شبکه باشد، این آلودگـی بـه سـرعت گسـترش پـیدا می‌کند و دلیل آن هم این است که هنگامی که شما فایلی آلوده را برای فرد دیگری می‌فرستید، او هم با باز کردن فایل آلوده خواهد شد.

یـک ماکـروی مخـرب همچنیـن مـی‌توانـد باعـث بوجود آمدن تغییرات در اسناد یا نتظیمات شما شود.

ویـروس‌هـای ماکـرو مـی‌توانـند فایل‌هایی که در بیشتر ادارات مورد استفاده قرار مـی‌گـیرند را آلـوده کنـند و همچنین بعضی از آنها می‌توانند چندین نوع متفاوت از فایل‌ها مانند فایل‌های برنامه‌های Word یا Excel را تحت تاثیر قرار دهند. همچنین آنها می‌توانند به تمـام فـایل‌هایـی کـه توسـط برنامه میزبان آنها مورد اجرا قرار می‌گیرد،گسترش پیدا کنند. بالاتـر از همـه اینکه آنها می‌توانند براحتی گسترش پیدا کنند، چرا که اسناد بطور مداوم در نامه‌های الکترونیک و وب‌سایت‌ها در حال تبادل هستند.

معرفی ویروس‌هایی از این نوع:

ویروس WM/Wazzu : فایل‌های تهیه شده توسط برنامه Word را آلوده می‌سازد. این ویروس بطور تصادفی در بین هر یک تا سه کلمه، عبارت wazzu را قرار می‌دهد.

ویـروس OF97/Crown-B : فـایل‌هـای بـرنامه‌های Word ، Excel و PowerPoint را آلـوده مـی‌کـند. هنگامـی کـه ایـن ویـروس، فایلی از برنامه Word را آلوده می‌سازد، بخش محافظتی ماکرو در سایر برنامه‌های نرم‌افزار Office را از کار انداخته و از این طریق آنها را تحت تاثیر قرار می‌دهد.