**ويروسها ، كرمها و تروجانها چه هستند؟**

**پروژه دات کام**

**www.Prozhe.com**

ويروسها ، كرمها وتروجانها برنامه هاي بدي هستند كه مي توانند باعث خطر براي كامپيوتر شما واطلاعات آن شوند. آنها مي توانند سرعت اينترنت را پايين بياورند وآنها حتي ممكن است از كامپيوترشما براي بخش كردن خودشان براي دوستانتان، آشنايان، شركت محل كار استفاده كنند ودرآدرس مجازي باقي بمانند. خبرهاي خوب آن است كه با يك جلوگيري اندك وتعدادي مفهوم رايج خوب شما احتمالا كمترقرباني اينها هستيد . به نظر مي رسد اين پيش قدم شدن شما براي جلوگيري تمام فاميل شما را محافظت مي كند. بخوانيد براي يادگرفتن درباره مشخصه ها وتفاوتهاي ويروسها ، كرمها وتروجانها .

* ويروس چيست؟
* كرم چيست؟
* تروجان چيست؟
* چطوركرمها وويروسهاي ديگر پخش مي شوند؟
* چطورمي توان اثركرم يا ويروس داشت؟

مرحله بعدي : كاهش خطر ويروس

ويروس چيست؟

ويروس يك تكه كد كامپيوتراست كه خودش وابسته به يك برنامه يا فايل است بنابراين آن مي تواند ازكامپيوتر به كامپيوتر پخش شود.ويروسها مي توانند موجب خطر نرم افزار، سخت افزار وفايلهاي شما باشند.

ويروس : كد نوشته شده با مفهوم روشن : تكرار خودش . يك ويروس براي پخش از كامپيوتربه كامپيوترتوسط وابستگي خودش به يك دسته برنامه تلاش مي كند. آن ممكن است براي سخت افزار، نرم افزاريا اطلاعات خطرناك باشد. فقط دامنه ويروسهاي انساني درشدت از1 بولا به 24 ساعت فلو، دامنه ويروسهاي كامپيوتر ازرنج آوري مختصر تا مخرب محض. اخبار جديد آن هست كه يك ويروس واقعي بدون اقدام انسان براي حركت آن پخش نمي شود، مثل اشتراك فايل يا فرستادن اي ميل.

 كرم چيست؟

يك كرم، مثل يك ويروس براي كپي خودش از يك كامپيوتر روي ديگري طراحي شده است، اما آن بطور اتوماتيك خصيصه كنترل روي كامپيوتر را مي گيرد كه مي تواند فايلها واطلاعات را ببرد. وقتي شما يك كرم درسيستمتان داريد آن ميتواند به تنهايي حركت كند.

يك خطر بزرگ كرمها تواناييشان براي بازگرداندن درصداي بلند است.براي مثال، يك كرم مي تواند كپي خودش رابراي هركسي كه درآدرس اي ميل شما ثبت شده بفرستد وسپس كامپيوترهايشان همان عمل را انجام خواهند داد ، باعث يك ترافيك شبكه سنگين مي شود كه سرعت شبكه ها پايين خواهد آمد واينترنت هم. موقعيكه، كرمهاي جديد آزاد هستند، آنها خيلي سريع پخش مي شوند، شبكه ها را كند مي كند وممكن است باعث شوند كه تومدت طولاني منتظرباشي براي ديدن هرصفحه سايت اينترنت.

كرم بخش اوليه ويروس . يك كرم بطوركلي بدون اقدام كاربر پخش مي شود وكپي

 هاي خودش را درسرتاسرشبكه ها به طور كامل توزيع مي كند يك كرم مي تواند

حافظه يا پهناي باند شبكه را مصرف كند، سپس باعث توقف پاسخ دهي كامپيوترشود. چون كرمها براي حركت نياز به يك دسته برنامه يا فايل ندارند، آنها همچنين مي توانند در داخل سيستم شما تونل بزنند واجازه دهند هركس ديگري كنترل سيستم شما رابگيرد اخيرا نمونه هاي كرمها شامل سايسر وبلاستراست.

تروجان چيست؟

اندكي پيش ازاين اسب تروجان اساطيري يك هديه بود، اما با دربرداشتن سربازان وخارج شدن آنها هنگام رسيدن به شهر تروي . امروزه ، تروجان ها برنامه هاي كامپيوتري هستند كه ظاهرا براي نرم افزارمفيد مي باشند، اما درعوض آنها امنيت تورا مصالحه مي كنند . باعث خطر زيادي مي شوند. اخيرا تروجان ازپيغام اي ميل مي آيد كه مدعي است جزء متعلقات امنيت برزو مايكروسافت است، اما سرانجام يك ويروس مي شود كه براي ازكار انداختن آنتي ويروس ونرم افزار ديوار آتش (نرم افزار حفاظتي) تلاش مي كند.

تروجان برنامه كامپيوتر كه ظاهرا مفيد مي باشد اما واقعا خطرناك است. تروجان مردم را درهنگام باز كردن برنامه گول مي زند وپخش مي شود، چون آنها فكر مي كنند كه آن از يك منبع قانوني آمده است. براي محافظت بهتر كاربر، مايكروسافت اغلب بيانيه هاي امنيتي توسط ميل مي فرستد، اما اين بيانيه ها هرگز شامل وابستگي نيستند. ما همچنين همه مشدار دهنده هاي امنيتي مان را روي وب سايت امنيتي منتشرمي كنيم قبل ازاينكه ما آگهي آنها را براي مشتريانمان بفرستيم. تروجان مي تواند همچنين جزئي درنرم افزاري باشد كه شما به طوررايگان دانلود مي كنيد. هرگز نرم افزاري راكه از يك منبع درست نيستند دانلود نكنيد. هميشه برنامه ها به روزهاي مايكروسافت را از ويندوز به روز يا شركتهاي به روز مايكروسافت دانلود كنيد.

**كرمها وويروسهاي ديگر چگونه منتشر مي شوند؟**

واقعا همه ويروسها وتعداد زيادي ازكرمها نمي توانند منتشر شوند مگراينكه شما باز كنيد يا اجرا كنيد يك برنامه آلوده را .

تعداد زيادي ازاين ويروسهاي خطرناك اصولا ازطريق متعلقات اي ميل فايلها كه همراه با پيغام اي ميل فرستاده شده ، منتشر مي شوند. شما مي توانيد معمولا اگر اي ميل شما ، شامل پيوستگي اي هست بگوييد . چون شما آيكن كليپي مي بينيد كه متعلقات ونامهاي آن را نشان مي دهد. عكسها ، نامه هاي نوشته شده در word مايكروسافت وحتي صفحه هاي گستردهexcel فقط تعدادي ازانواع فايلهاي شما هستند كه ممكن است هر روز ازطريق اي ميل برسد . ويروسها موقعيكه شما متعلقات فايل را باز مي كنيد شروع مي شوند . اگربه شما پيغام اي ميلي برسد با متعلقاتش از كسي كه شما نمي شناسيد، شما بايد فورا آن را پاك كنيد. متاسفانه ، شما ازمتعلقات اي ميل كسي را هم كه مي شناسيد ايمني نداريد. ويروسها وكرمها توانايي دزديدن اطلاعات خارج برنامه هاي اي ميل را دارند وخودشان را براي همه ليست آدرس هاي ثبت شده مي فرستند . بنابراين اگربه شما اي ميلي ازكسي با يك پيغامي كه نمي فهميد يا فايلي كه شما منتظرآن نبوديد رسيد، هميشه با شخصي تماس بگيريد ومحتويات متعلقات را قبل ازاينكه آن را باز كنيد بپذيريد . ويروسهاي ديگر مي توانند پخش شوند از طريق برنامه دانلود شده ازاينترنت يا ديسكتهاي پاك كننده ويروس كامپيوتر كه شما از دوستان قرض مي گيريد يا از فروشگاه خريداري مي كنيد . اينها هستند كمترين راه رايج براي منقبض كردن ويروس كامپيوتر . اكثرمردم از طريق باز كردن واجراي متعلقات اي ميل ناشناخته ويروسي مي شوند .

چطور مي توان گفت اگر كرم يا ويروسهاي ديگر داشت؟

موقعي كه شما باز مي كنيد يا اجرا مي كنيد يك برنامه آلوده را، شما ممكن است ندانيد منقبض كردن ويروس را . كامپيوتر شما ممكن است سرعتش پايين بيايد، پاسخ دهي اش متوقف شود يا از كار بيفتد و ري استارت شود . گاهي اوقات يك ويروس به فايلي كه شما براي بالا آمدن كامپيوترنياز داريد حمله خواهد كرد. در اين حالت، شما ممكن است دكمه power را فشار دهيد ودرصفحه خالي آيكن start را جستجو كنيد .

- همه اين علامتها هستند علامت رايج كه كامپيوترشما ويروس دارد، اگرچه كه آنها مي توانند معلول برنامه هاي نرم افزاري وسخت افزاري باشند كه هيچ عملي با دارنده ويروس ندارند. جدي بگيريد پيغامي را كه كامپيوتر مبني بر وجود ويروس مي دهد. اين ممكن است به معني آن باشد كه ويروس به عنوان فرستنده آلوده به آدرس اي ميل هاي ليست شده فرستاده مي شود. اين لزوما به معني داشتن ويروس نيست. بعضي از ويروسها توانايي تغييرآدرس اي ميل را دارند. مگر اينكه شما نرم افزارآنتي ويروس جديد را نصب كرده باشيد، وجود ندارد راه مطمئني براي اينكه شما بدانيد كه آيا ويروس دارد يا نه. اگر شما نداريد نرم افزارآنتي ويروس رايج را يا اگر شما علاقه اي به نصب انواع مارك نرم افزار آنتي ويروس نداريد، از صفحه نرم افزارامنيتي ما ديدن كنيد.

مرحله هاي بعدي : كاهش خطر ويروس شما

هيچ ضمانتي، كامپيوترشما را صد درصد ايمن نمي كند. با وجود اين شما ميتوانيد

بهبود دهيد امنيت كامپيوترتان توسط نرم افزارهاي نگه دارنده جديد ونگه داشتن آبونمان نرم افزارآنتي ويروس رايج .

براي ياد گرفتن چيزهاي بيشتردرباره آنچه كه مي توانيد انجام دهيد، اين صفحات راببينيد.

\* يادگرفتن درباره رويدادهاي امنيتي اخيروخطرات ويروس

\* جستجوبراي اينكه چرا شما نيازبه ديوارآتش (نرم افزار محافظتي) كامپيوتر داريد.

\* ديدن آنچه از ويندوز كه مي تواند به شما كمك كند.

\* 3 مرحله محافظت pc شما.

آنچه كه شما بايد درباره بلاستربدانيد.

كرم بلاستر هدف گيري مي كند با يك انتشار امنيتي مربوط به كارپردازنده كه مايكروسافت با آزاد كردن امنيت به روز متوجه ي شود.

بلاستر كامپيوترهايي با نرم افزارمنسوخ راهدف گيري مي كند وآن كامپيوترها

 درخطرآلودگي تا نصب به روزباقي مي مانند.

ما پيشنهاد مي كنيم كه مصرف كننده ها نصب كنند به روز را از بولتن امنيتي

MS03 – 039 براي كمك به حفاظت در برابراين نرم افزار بد. اگر كامپيوتر شما آلوده شده است، كامپيوترشما ممكن است نرمال عمل كند، ممكن است كه ظاهر شود يا ممكن است ري استارت شود بدون دادن ورودي. اگر كامپيوتر شما آلوده شده است ، شما ممكن است اين پيغام خطا را ببينيد.

- اگر سيستم شما shutt down است، مطابق اين مراحل براي توقف دوره، سپس به مرحله 2 براي توقف گرم پيش رويد.

10 فشار دهيد : CTRL+ ALT+Delete

20 كليك كن روي Task Manoger

30 كليك كن روي processes

40 كليك كن روي Image Name مرتب كردن به ترتيب حروف الفبا

50 جستجوي فرآيند ناميده مي شودMsblast .exe اگر شما پيدا كنيد آن را، كليك نام براي انتخاب فرآيند وسپس كليك رويd process

60 ببنديد Task Manager

2 0 چك كردن وبرطرف كردن بلاستر : استفاده ابزار متوقف نرم افزاربد ويندوزمايكروسافت براي جستجوي هاردتان وتوقف بلاسترمختلف.

3 0 حفاظت pc شما : كمك به امن بودن كامپيوترتان دربرابر بلاستر و خطرهاي ديگر در اينترنت، برطبق دستورالعمل محافظ pc براي برقرار كردن ديوارآتش ورسيدن به نرم افزار به روز واستفاده ازنرم افزارآنتي ويروس بروز.

كرم ساسر هدف گيري مي كند با يك انتشارامنيتي با سرويس زير سيستم نفوذ امنيتي كه مايكروسافت با آزاد كردن امنيت بروز متوجه مي شود. هدف ساسر كامپيوترهايي با نرم افزار منسوخ است وآن كامپيوترها با خطر آلودگي تانصب شدن به روز باقي ميمانند .

ما پيشنهاد مي كنيم كه مصرف كننده ها نصب كنند به روز را از بولتن امنيتي مايكروسافت 011 – MS04 براي كمك به حفظ دربرابر اين نرم افزارهاي بد.

قبل از اينكه شما مراحل ديگر را طي كنيد، مطمئن باشيد ازفعاليت ديوارآتش براي كمك به حفاظت كامپيوترتان در برابرآلودگي. اگر شما يك سخت افزار ديوارآتش داريد درخانه يا محل كار يا اگرشما استفاده مي كتيد ازديوارآتش با ويندوزXP ، كرم ساسر احتمالا مسدود شده است. اگر كامپيوترشما آلوده شده، يك ديوار آتش به محدود كردن اثرات كرم كامپيوتر شما كمك خواهد كرد. براي دستور العمل جامع نصب وفعال ساختن ديوارآتش از دستور العمل محافظ PC ديدن كنيد.

كمك براي حفاظت كامپيوترتان دربرابر ساسر، شما بايد ابتدا دانلود كنيد و نصب

 كنيد835732 به روز امنيتي را كه آزاد شده بود با بولتن امنيتي مايكروسافت011 - MS04 . شما مي توانيد پيدا كنيد 835732 به روز را روي وب سايت به روز ويندوز كه ليست شده دربه روز مهم وسرويس بخش فشرده . شما مي توانيد همچنين دانلود كنيد ونصب كنيد اين مقررات بروز را از Microsoft . com براي پيدا كردن دانلود براي سيستم عمليات شما، مراجعه كنيد به بولتن امنيتي Technical 011 – MS04

يادداشت : اگر شما نصب كنيد به روز را براي مقررات011 - MS04 يا از طريق به روز كردن اتوماتيك قبل از 30 بهار 2004 ، سپس شما آماده هستيد براي محافظت دربرابر اين انتشار.

استفاده از ويندوز مايكروسافت، ابزار توقف نرم افزار براي جستجو هارد شما وتوقف ساسر گوناگون .

**What are viruses, worms, and Trojans?**

Viruses, worms, and Trojans are malicious programs that can cause damage to your computer and information on your computer. They can also slow down the Internet, and they might even use your computer to spread themselves to your friends, family, co-workers, and the rest of the Web. The good news is that with an ounce of prevention and some good common sense, you are less likely to fall victim to these threats. Think of it as locking your front door to protect your entire family.

Read on to learn about the characteristics and differences of viruses, worms, and Trojans.

 [What is a virus?](http://www.microsoft.com/athome/security/viruses/virus101.mspx#EFAA)

 [What is a worm?](http://www.microsoft.com/athome/security/viruses/virus101.mspx#EEAA)

 [What is a Trojan?](http://www.microsoft.com/athome/security/viruses/virus101.mspx#EDAA)

 [How do worms and other viruses spread?](http://www.microsoft.com/athome/security/viruses/virus101.mspx#ECAA)

 [How can I tell if I have a worm or other virus?](http://www.microsoft.com/athome/security/viruses/virus101.mspx#EBAA)

 [Next steps: Reducing your virus risk](http://www.microsoft.com/athome/security/viruses/virus101.mspx#EAAA)

**What is a virus?**

****A virus is a piece of computer code that attaches itself to a program or file so it can spread from computer to computer, infecting as it travels. Viruses can damage your software, your hardware, and your files.

**Virus (n.)** Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or information.

Just as human viruses range in severity from Ebola to the 24-hour flu, computer viruses range from the mildly annoying to the downright destructive. The good news is that a true virus does not spread without human action to move it along, such as sharing a file or sending an e-mail.

**What is a worm?**

A worm, like a virus, is designed to copy itself from one computer to another, but it does so automatically by taking control of features on the computer that can transport files or information. Once you have a worm in your system it can travel alone. A great danger of worms is their ability to replicate in great volume. For example, a worm could send out copies of itself to everyone listed in your e-mail address book, and their computers would then do the same, causing a domino effect of heavy network traffic that would slow down business networks and the Internet as a whole. When new worms are unleashed, they spread very quickly, clogging networks and possibly making you wait twice as long for you (and everyone else) to view Web pages on the Internet.

**Worm (n.)** A subclass of virus. A worm generally spreads without user action and distributes complete copies (possibly modified) of itself across networks. A worm can consume memory or network bandwidth, thus causing a computer to stop responding.

Because worms don't need to travel via a "host" program or file, they can also tunnel into your system and allow somebody else to take control of your computer remotely. Recent examples of worms included the [Sasser](http://www.microsoft.com/security/incident/sasser.mspx) worm and the [Blaster](http://www.microsoft.com/security/incident/blast.mspx) worm.

**What is a Trojan?**

Just as the mythological Trojan horse appeared to be a gift, but turned out to contain Greek soldiers who overtook the city of Troy, today's Trojans are computer programs that appear to be useful software, but instead they compromise your security and cause a lot of damage. A recent Trojan came in the form of an e-mail message that included attachments claiming to be Microsoft security updates, but turned out to be viruses that attempted to disable antivirus and firewall software.

**Trojan (n.)** A computer program that appears to be useful but that actually does damage.

Trojans spread when people are lured into opening a program because they think it comes from a legitimate source. To better protect users, Microsoft often sends out security bulletins by e-mail, but these bulletins will never contain attachments. We also publish all our security alerts on our [Security Web site](http://www.microsoft.com/security/default.mspx) before we send notice of them to our customers.

Trojans can also be included in software that you download for free. Never download software from a source that you don't trust. Always download Microsoft updates and patches from [Microsoft Windows Update](http://windowsupdate.microsoft.com/) or [Microsoft Office Update](http://office.microsoft.com/officeupdate/default.aspx).

**How do worms and other viruses spread?**

Virtually all viruses and many worms cannot spread unless you open or run an infected program.

Many of the most dangerous viruses were primarily spread through e-mail attachments—the files that are sent along with an e-mail message. You can usually tell if your e-mail includes an attachment because you'll see a paperclip icon that represents the attachment and includes its name. Photos, letters written in Microsoft Word, and even Excel spreadsheets are just some of the file types you might receive through e-mail each day. The virus is launched when you open the file attachment (usually by double-clicking the attachment icon).

**Tip:**  Never open anything that is attached to an e-mail message unless you were expecting the attachment **and** you know the exact contents of that file.

If you receive an e-mail message with an attachment from someone you don't know, you should delete it immediately. Unfortunately, you're no longer safe opening attachments from people you do know. Viruses and worms have the ability to steal the information out of e-mail programs and send themselves to everyone listed in your address book. So, if you get e-mail from someone with a message you don't understand or a file you weren't expecting, always contact the person and confirm the contents of the attachment before you open it.

Other viruses can spread through programs you download from the Internet or from virus-ridden computer disks that you borrow from friends or even buy in a store. These are less common ways to contract a computer virus. Most people get viruses from opening and running unknown e-mail attachments.

**How can I tell if I have a worm or other virus?**

When you open and run an infected program, you might not know you've contracted a virus. Your computer may slow down, stop responding, or crash and restart every few minutes. Sometimes a virus will attack the files you need to start up a computer. In this case, you might press the power button and find yourself staring at a blank screen.

All of these symptoms are common signs that your computer has a virus—although they could also be caused by hardware or software problems that have nothing to do with having a virus.

Beware of messages warning you that you sent e-mail that contained a virus. This may mean that the virus has listed your e-mail address as the sender of tainted e-mail. This does not necessarily mean you have a virus. Some viruses have the ability to forge e-mail addresses.

Unless you have up-to-date antivirus software installed on your computer, there is no sure way to know if you have a virus or not. If you don't have current antivirus software or if you're interested in installing a different brand of antivirus software, visit our [Security software downloads](http://www.microsoft.com/athome/security/downloads/default.mspx) page.

**Next steps: Reducing your virus risk**

Nothing will guarantee the security of your computer 100 percent. However, you can continue to improve your computer's security by keeping your software up to date and maintaining a current antivirus software subscription.

# What You Should Know About Blaster

The Blaster worm (W32.Blaster.A and its variants) targets a security issue related to the Remote Procedure Call (RPC) function that Microsoft addressed with a released security update. Blaster targets computers with out-of-date software, and those computers remain at risk of infection until the update is installed. We recommend that customers install the update from [Security Bulletin MS03-039](http://www.microsoft.com/security/bulletins/200309_windows.mspx) to help protect against this malicious software.



 **Actions to Take Now**

**1.** **Symptoms of Infection**

  If your computer is infected, your computer may operate normally, may appear sluggish, or may restart every few minutes without your input.



**Shutdown error**. If your computer is infected, you may see this error message.

If your system is shutting down, follow these steps to stop the cycle. Then proceed to Step 2 to remove the worm.

**To end the Blaster worm process**

1. Press **CTRL+ALT+DELETE**.

2. Click the **Task Manager** button.

3. Click the **Processes** tab.

4. Click the **Image Name** column heading to sort the processes alphabetically by name.

5. Look for a process named **Msblast.exe**. If you find it, click the name to select the process, and then click the **End Process** button.

6. Close the **Task Manager**.

**2.** **Check For and Remove Blaster**

  Use the [Microsoft Windows Malicious Software Removal Tool](http://www.microsoft.com/security/malwareremove/default.mspx) to search your hard disk for and remove Blaster variants.

**3.** **Protect Your PC**

  To help secure your computer against Blaster and other threats on the Internet, follow our [Protect Your PC guidance](http://www.microsoft.com/protect/) to set up a firewall, get software updates, and use up-to-date antivirus software.

What You Should Know About Sasser

The Sasser worm (W32.Sasser.A and its variants) targets a security issue with the Local Security Authority Subsystem Service (LSASS) that Microsoft addressed with a released security update. Sasser targets computers with out-of-date software, and those computers remain at risk of infection until the update is installed. We recommend that customers install the update from [Microsoft Security Bulletin MS04-011](http://www.microsoft.com/security/bulletins/200404_windows.mspx) to help protect against this malicious software.



 **Actions to Take Now**



**1.** **Enable a Firewall**

  Before you take other steps, make sure you have a firewall activated to help protect your computer against infection. If you have a hardware firewall in place for your home or workplace connection, or if you use the firewall included with Windows XP, the Sasser worm is most likely blocked. If your computer has been infected, a firewall will help limit the effects of the worm on your computer. For comprehensive guidance to installing and enabling a firewall, see [our Protect Your PC guidance](http://www.microsoft.com/protect/).

**2.** **Install the Required Update**

  To help protect your computer against Sasser, you must first download and install security update 835732, which was released with Microsoft Security Bulletin MS04-011. You can find update 835732 on the [Windows Update Web site](http://windowsupdate.microsoft.com/) listed in the Critical Updates and Service Packs section. You can also download and install this update manually from the Microsoft.com Download Center. To find the download for your operating system, refer to [Technical Security Bulletin MS04-011](http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx).
**Note**  If you installed the updates for MS04-011 manually or through Automatic Updates before April 30, 2004, then you are already protected against this issue.

**3.** **Check For and Remove Sasser**

  Use the Microsoft Windows [Malicious Software Removal Tool](http://www.microsoft.com/security/malwareremove/default.mspx) to search your hard disk for and remove Sasser variants.