

The **lizamoon scareware** attack got a lot of attention because it supposedly infected 1.5 million web pages, but some experts are now saying the effect was likely orders of magnitude smaller.

Lizamoon was an attempt to get users to provide credit card information. It did so by inserting a piece of code into a web site that causes a browser to a site that simulates a virus scan and then prompts a user to download antivirus software, giving up their credit card information in the process.

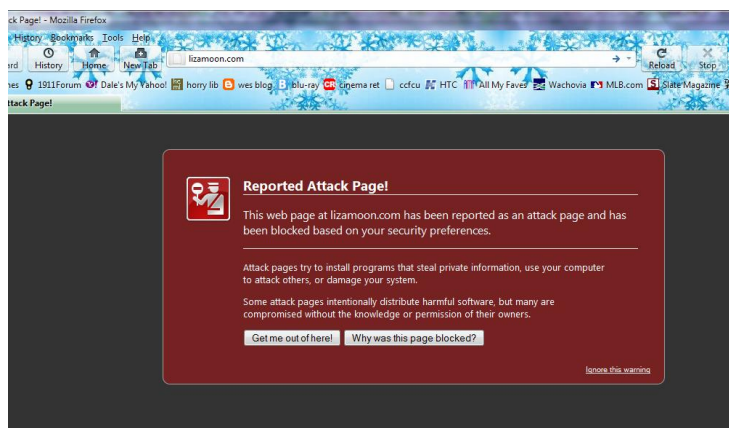


A screengrab provided by Websense shows a security console screen which appears as part of the LizaMoon web attack, which poses as a real security program.

Websense initially reported lizamoon's existence March 29. that it found 1.5 million sites infected. That finding was the result of a Google search, which showed the URLs with

the same address - lizamoon.com - from which the fake antivirus programs originated.

The news spread quickly and the 1.5 million web sites infected was widely cited. But a security expert at Cisco says that the number of sites infected was actually much smaller. Mary Landesman, a senior security researcher at Cisco, wrote in the company's [security blog](#) that this particular attack has been around for the last several months. She wrote that Cisco only found about 1,154 unique compromised web sites.



Here is a screen grab I got from Firefox. When I typed the address into IE9 it would not open the page, but displayed search results about the scareware.



This is NOT AdAware, which IS a legitimate program

THESE ARE EXAMPLES OF SCAREWARE- SCARY AREN'T THEY?



This report is not possible within a browser popup

The rule I use is that any browser window warning, or pop up window is always a fake. I have found nothing to disprove this

statement.

If you see pop up windows, ask yourself: Are they from the antivirus program you use already?



Here are some ways to protect yourself:

- Never ever click on a popup, banner, or any other kind of ad that claims your system is infected, your anti-virus software needs to be updated, or your registry is corrupted.
- If you find yourself redirected to a scareware site, don't click anything. Hit Ctrl-Alt-Del, go to Task Manager, and use End Task to shut down your browser. It's much safer that way. Once you've been redirected to a malicious site, clicking on anything, even the X in the corner, could trigger a download.
- Legit anti-virus programs are updated via the software's control panel, not popups.
- If you find yourself infected, Microsoft's Malicious Software Removal Tool can clean things up. Most of the major anti-virus sites also offer removal tools as well. Although if you have a legit and up to date anti-virus program installed it will probably detect and block the scareware from being installed in the first place, and you do have a legit and update anti-virus installed, right?

The thing that causes most instances of having a virus or malware program on your computer is this-- **the user causes it**, by taking a risky action.

Don't react to popup windows, except to close them. Right click the task bar to close them. If they are not on the task bar right click the window itself.

If you get large amounts of email from persons who always forward things they receive, stop opening them. The person sending them won't know!

Never be guilty of forwarding email with previous header information.

- ❖ Remove it by copying and pasting just the text of the email into a NEW email,
- ❖ or deleting the information while composing a forward.

If you see an attachment from someone you don't trust (or know) don't open it. Curiosity causes problems.

Don't believe most emails that warn you about things such as cell phones blowing up gas stations, or saving someone's life by sending them a card or email. Either delete them or research them yourself. For Heaven's Sake, don't forward them.

From Microsoft:

Q: How is Microsoft Security Essentials different from Windows Defender?

A: Windows Defender detects and removes known spyware only. It is not designed to protect against the full breadth of malicious software, and specifically does not prevent viruses, worms, Trojans, and other malicious software from infecting your machine. The best no-cost solution will be a comprehensive anti-malware solution. *Security Essentials DOES do protect from all of the above.*

Q: Is Microsoft Security Essentials designed to replace Windows Defender?

A: No but if you are running Microsoft Security Essentials, you do not need to run Windows Defender. Microsoft Security Essentials is designed to disable Windows Defender in order to manage the PC's real-time protection, including anti-virus, rootkits, Trojans and spyware. *This is confusing, since it is contradictory.*

Q: Does installing Microsoft Security Essentials disable Windows Defender

A: Microsoft Security Essentials should disable Windows Defender on Vista and Windows 7 and uninstall it from XP. In some cases, this does not happen automatically.

Q: Do I need to manually disable or uninstall Windows Defender if I am using Microsoft Security Essentials?

A: If Microsoft Security Essentials did not automatically disable Windows Defender on Vista or Windows 7, you should disable it to prevent conflicts. Windows Defender cannot be uninstalled from Vista or Windows 7.

If Microsoft Security Essentials did not automatically uninstall Windows Defender on XP, you should manually uninstall Windows Defender via Control Panel/Add or Remove Programs.

Q: What happens if I do not disable or uninstall Windows Defender if I am using Microsoft Security Essentials?

A: If Microsoft Security Essentials and Windows Defender are both running, your system may experience performance degradation and other problems caused by the conflict of two services providing real time protection simultaneously.

I found this information on a Microsoft website, and it is a bit confusing. Bottom line- If you have Security Essentials you have everything you need to be safe.