



Hey Folks,

We here at Malwarebytes take pride in our ability to find the latest threats that users face on daily basis and do our best to not only block and remove them with our products but also inform the general public about their danger through our blog.

In a very few cases, we jump the gun in our efforts to explain a threat and end up posting information that hasn't been thoroughly analyzed.

This is one of those cases.

We want to offer our most sincere apologies to WinRAR for any harm done by our reporting on a post first seen through the [Full-Disclosure](#) mailing list, we simply echoed the original reporting.

We have been in communication with WinRAR and performing our own in-depth analysis of the threat to identify that what we described in our post was simply a new attack vector that could mask itself as any executable.

Users of WinRAR have nothing to worry about as they are not being targeted nor is the WinRAR product itself malicious or allowing malicious files to be run on the system. We have since removed our post on the subject.

The malware itself would need to be double-clicked by a user (who has not patched their operating system since mid 2014) to be activated.

The best way to protect against this particular threat is to right click on any archive you might come across and open it using its associated tool (i.e. WinRAR) to extract it, as opposed to double clicking the archive.

In addition, make sure you install the latest Windows updates as a previously patched vulnerability in Internet Explorer makes this attack possible.

Thank you for your time and understanding

Safe Surfing!

**Adam Kujawa**  
*Head of Malware Intelligence, Malwarebytes*

0 Comments **Malwarebytes Unpacked**

Login ▾

Recommend Share

Sort by Best ▾

Be the first to comment.

Subscribe Add Disqus to your site Privacy

DISQUS

Related Posts

Beware of Tech Support Impersonators

Imgur Abused in DDoS Attack Against 4Chan!

Two Nominations for Malwarebytes in Annual Technology Awards

Browsefox variant High Stairs

My Conversations with Cybersecurity Influencers

Tweets

KEEP UP WITH THE LATEST NEWS AND OFFERS