Beware: Fake IRS tax email delivers Emotet malware

By Christopher Boyd

Published: 2023-03-22 · Archived: 2026-04-05 14:23:41 UTC

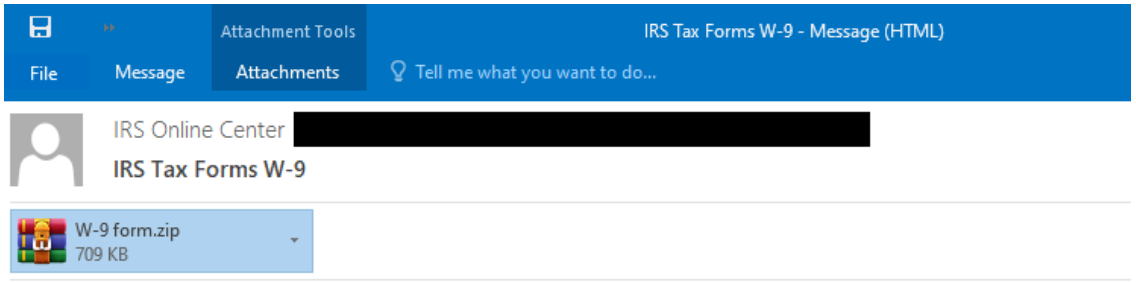
Tax season is upon us and, as with every year, we're seeing tax scammers rearing their heads.

Below, we have an example of a tax scam currently in circulation along with some suggestions for avoiding these kinds of attacks.

An IRS W-9 tax form scam

A Form W-9 is a form you fill in to confirm certain personal details with the IRS. Name, address, and Tax Identification Number are all things you can expect to fill in on one of these forms.

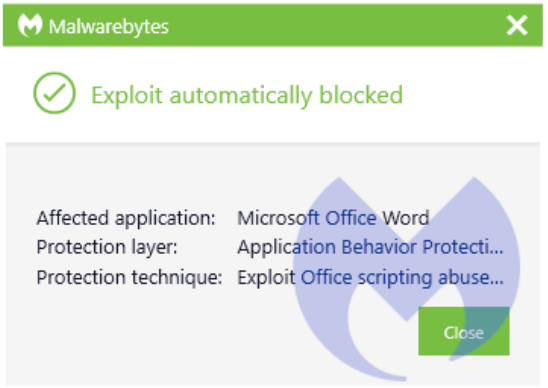
In this case, the Form W-9 is being used as a lure for people to download something sinister. Our Senior Director of Threat Intelligence, Jerome Segura, found an email being sent out with the title of "IRS Tax Forms W-9" which appears to have been sent from "IRS Online Center". The email, which contains an attachment and very little text, looks like this:



Let me know if you would like a hard copy mailed as well.

Respectifully,

Barbara LaCosta
Inspector
Department of Treasure
Email: info@irs.gov
https://www.irs.gov

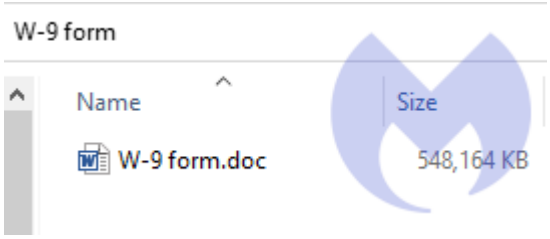


The rather short message reads as follows:

> Let me know if you would like a hard copy mailed as well.
>
> Respectifully [SIC]
>
> Barbara LaCosta
>
> Inspector
>
> Department of Treasure

The attachment, W-9 form.zip, is 709 KB in size.

Opening the attachment up reveals a Word document called W-9 form.doc

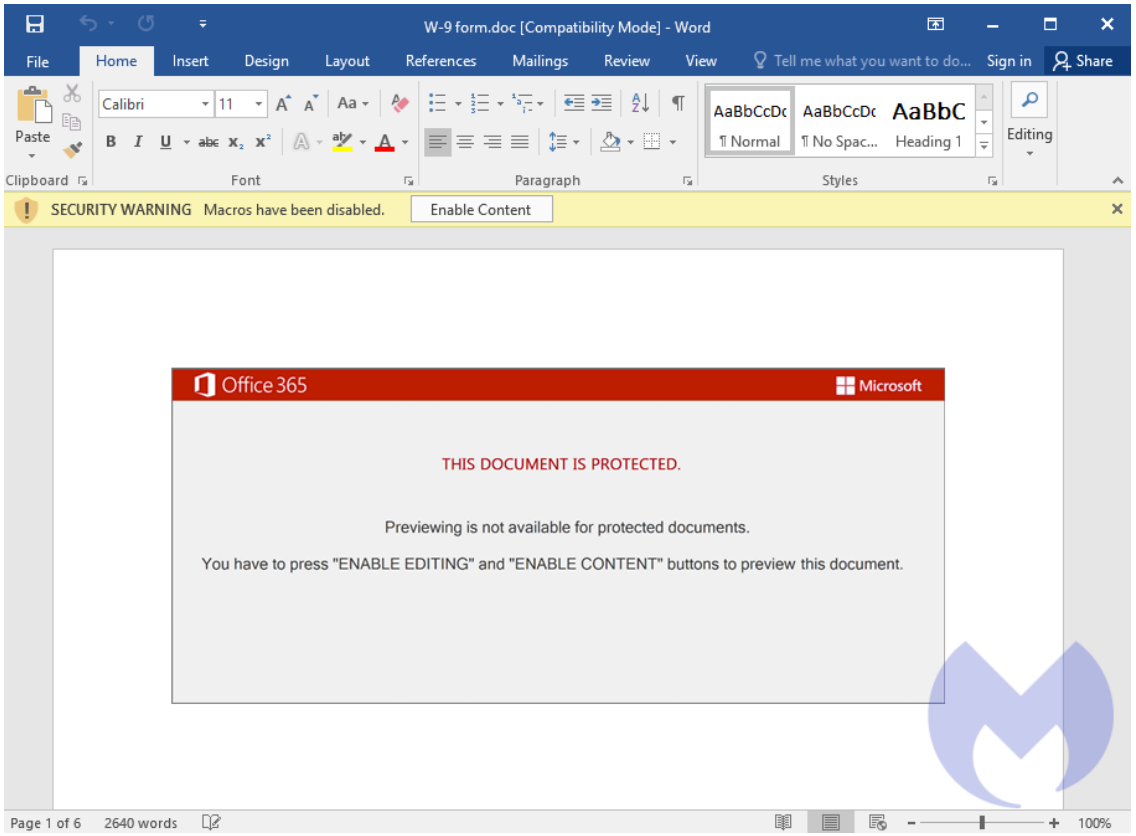


This file's size is 548,164 KB (548 MB), which is very suspicious. You won't find many genuine Word documents weighing in at 500MB or more. In fact, a file size of 500MB is a potential indicator that Emotet is lurking in the background. Malware authors are artificially pumping up the size of the document in order to try and fool or break security tools. This is because the large file size may prove too difficult for the tools to get a handle on and properly analyse.

Opening the document quickly becomes a game of Macro-related risk. Macros, used to automate aspects of your documents, are a tried and tested way of infecting a PC with malware. This is why you'll almost always see a message saying that Macros are disabled when opening a downloaded document.

Malware authors know this, and will do everything in their power to make you enable them. This is no exception. When opening W-9 form.doc, you'll see the following message:

> This document is protected
> Previewing is not available for protected documents. You have to press "enable editing" and "enable content" buttons to preview this document.



Enabling this will result in Emotet being downloaded onto the system.

Emotet has been around since 2014. Originally created as a banking trojan, later versions added malware delivery and spam services. Mostly featuring in email spam campaigns, a big focus of fake mails helping to deliver the infection include subjects like parcel shipping, invoices, and other forms of payment.

In fact, Emotet features as one of the top five cyberthreats businesses face in our 2023 State of Malware report. Flagged by Europol as “The world’s most dangerous malware”, law enforcement has never quite been able to shut it down permanently despite its entire global infrastructure being taken offline in 2021. Emotet’s ability to push additional forms of malware onto target systems including threats like TrickBot, IcedID, and Conti ransomware make it a formidable proposition for any security team to handle.

Avoiding tax scams

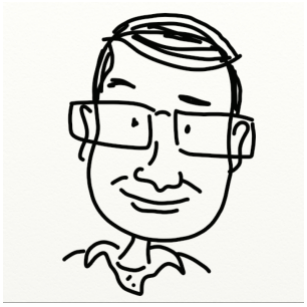
Here are some of the ways you can outsmart tax fraudsters and keep one step ahead of the phishing, malware, and social engineering attacks which come around every year during tax season.

- **File early**. One of the quickest ways to stumble into a trap is to leave filing your tax return until the last minute. That added pressure can mean responding to fake mails you otherwise would have ignored.
- **Be careful around suspicious refunds**. Tax agencies have a proper process for issuing refunds, found on their websites. Some, like HMRC, are very clear that refunds are never issued by email. If in doubt, phone the tax office directly and ask if what you have is the real deal or a fake.
- **Beware of fake bank portals**. Some tax scams will ask you who you bank with, and then open up a phishing page for that bank. Always navigate directly to your banking website, click throughs and redirects

typically spell danger.

- **Avoid the pressure pitch**. Tax scammers like to hurry you along to data theft and malware installs. Claims of only having 24 or 48 hours to file for a refund should be treated with skepticism. As with most solutions for these forms of social engineering, contact the tax entity directly.

About the author



Former Director of Research at FaceTime Security Labs. He has a very particular set of skills. Skills that make him a nightmare for threats like you.

Source: https://www.malwarebytes.com/blog/news/2023/03/beware-fake-irs-tax-email-delivers-emotet-malware