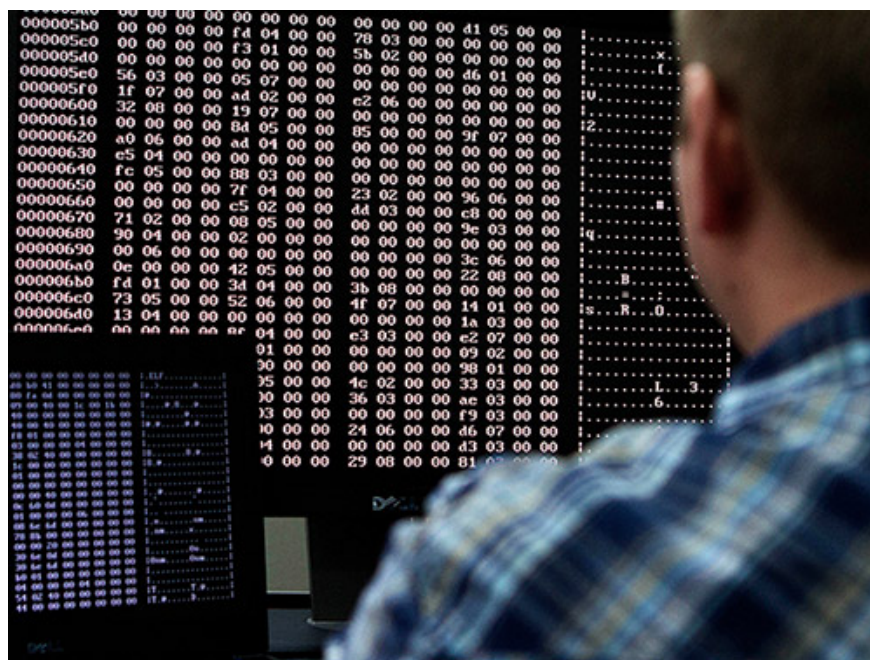


Microsoft has just 'lowered' the way hackers use to control computers

Updating in the Office 2016 Suite gives enterprise administrators the right to block the process of running macros in files.

Recently, Microsoft has successfully "eradicated" the popular way that computer criminals prefer to use it for years to take control of users' computers. Updating in the Office 2016 Suite gives **enterprise administrators the right to block the process of running macros in files** - macros can allow running authorized tasks but often lead to Internet connection and downloading software poisoning (malware).

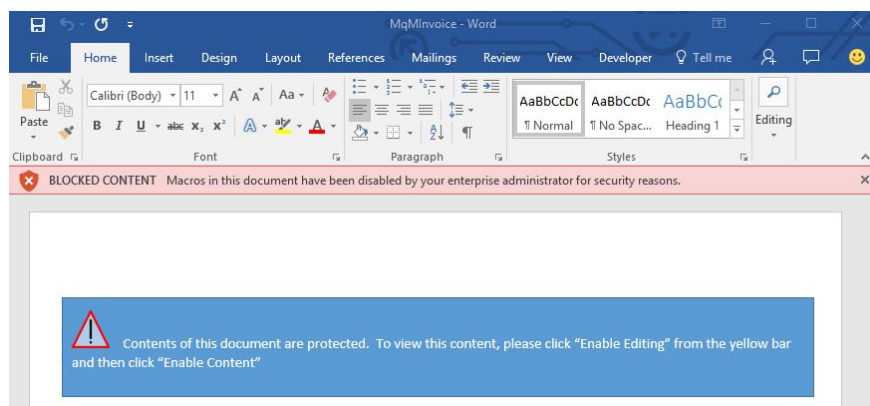
Usually, hackers send a phishing email with an Office file attached and claim to be someone in the company to get the recipient to open the file. This file will cause the user to activate the macro and thereby cause their computer to become infected despite repeated warnings.



An analyst is looking at code at a malware lab at Idaho National Laboratory's cybersecurity center in Idaho Falls, Idaho

Microsoft wrote on its blog, " *The appeal of using macro-based malware is because of very easy to activate macros. Previous versions of Office include warnings when opening macro files but The authors of these malware seem to have adapted quite quickly when using social engineer techniques - a non-technical method to*

break into a system or corporate network, attracting users, making them activate macros and news. that there will be no problem but still poisoned ".



Macros are blocked when users intentionally open files

Now the user no longer has the right to decide. If the administrator decides to block macros, the user will receive a message warning that the macro has been disabled for security reasons. Undoubtedly, this will undoubtedly be a change adopted by many businesses, especially businesses that are often the target of this type of attack. About **91% of attacks are targeted to use spear email - phishing** (a **phishing** form like phishing but designed to a specific goal) and Microsoft statistics show that **98% of the threats are related to Office software using macros** .

Although attack by macros is easy to remove, the consequences they bring can be surprising, for example, hackers who hold company data that can be used to extort money, or hacked machines can be Used to cut electricity of thousands of houses.

Author: Paul Szoldra

You finished reading the article "**Microsoft has just 'lowered' the way hackers use to control computers**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.