Keystone
TECHNOLOGY CONSULTANTS

Cybersecurity Tips and Reminders

This Month's Focus- Do Not "Enable Content"

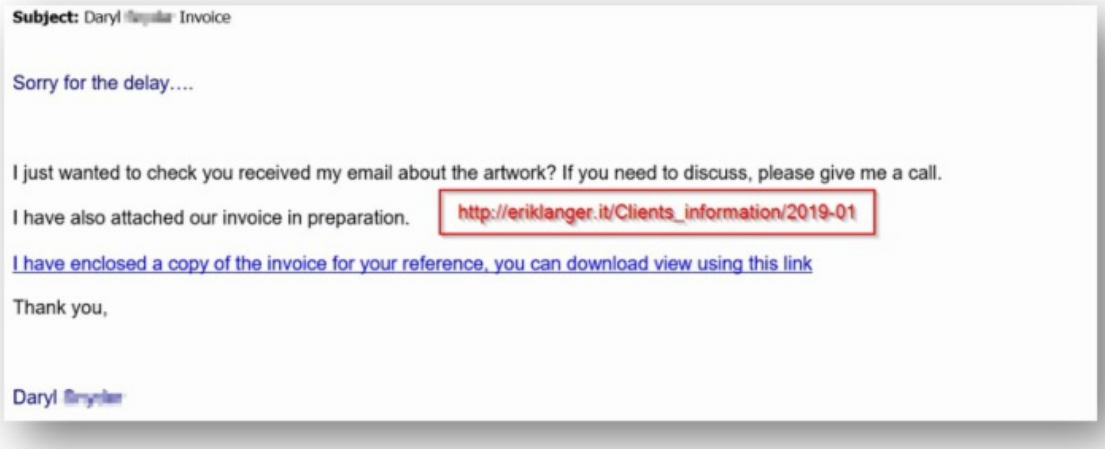
This article will discuss a tactic that has been utilized in different ways by hackers for over 10 years. Microsoft Office products have functionality built in to run programs called macros, which are programs that can be embedded in Word, Excel, and PowerPoint. Let's say you want Excel to carry out some background calculations to modify specific cells based on the data set specified, a macro could be created and clicked upon to allow this to occur in a split second. This is a legitimate use of macro code.

Hackers have taken advantage of this macro functionality by creating malicious software (malware) and embedding them in Office documents. They then find ways to trick recipients to "Enable Content" in these documents.

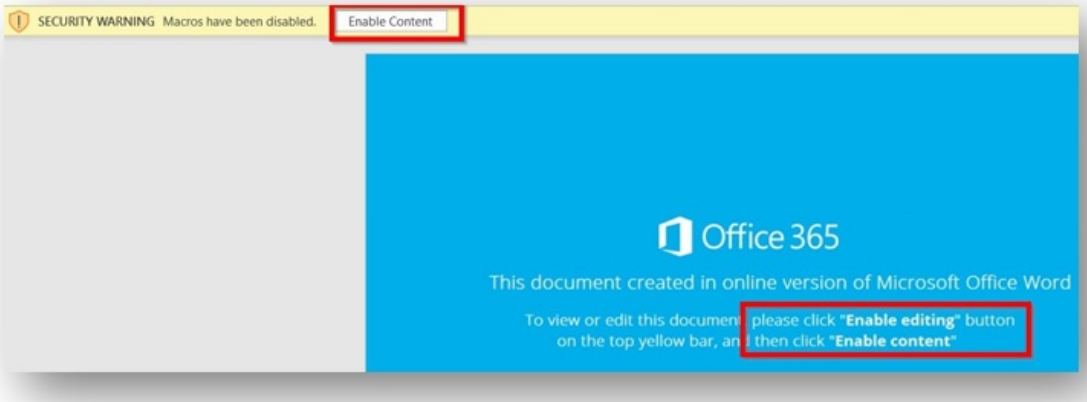
Send me more info

Be Suspicious. Something is not Right.

By clicking "Enable Content" the victim has unknowingly launched the malware. These documents often come from spam email messages. The recent sample I examined, came in an email urging a recipient to open and review an invoice as soon as possible. The hope by the hacker is to create a sense of urgency by the recipient thus causing them to rush and not be as careful. The message had a web link that supposedly would give them access to the invoice. This link directs the user to a website hosted in Italy. This website does nothing but immediately download a Microsoft Word document.



In the body of the document there are instructions to “Enable Editing” then click “Enable Content”.



When I did this on our crash test dummy PC, a Windows background process silently opened making connections to a server in Malaysia. Soon after that, a new process I did not recognize started making a connection to a server in the Netherlands. These hidden behaviors would be unnoticed for the average user. Then 10 minutes later, all the files in my documents were encrypted. They could be recovered if I paid the Bitcoin ransom for the decryption key. This is a classic example of ransomware.
The reason malicious Macros have been problematic for so long, is that Macros*CAN* be used for legitimate purposes. This makes them difficult for security vendors to just block outright. My experience has been that *MOST* people do not use these Macros and do not have the need to “Enable Content”. I strongly suggest no user clicks “Enable Content” for any file they receive in an email or downloaded from the internet. Delete it right away OR end it to us and we will evaluate whether it is legitimate or not.

Any Questions?
Please respond to this email if you have questions, comments, or desire more information.