Malicious Files

Along with credential harvesters, emails that convince targets to open malicious files are the most common phishing email classifications. This lesson will cover how malicious actors can get recipients to open malicious files, and what these can include. There are two main methods of delivering malware via phishing, as an attachment, or as a hyperlink taking the target to a web server that is hosting malware available for download.

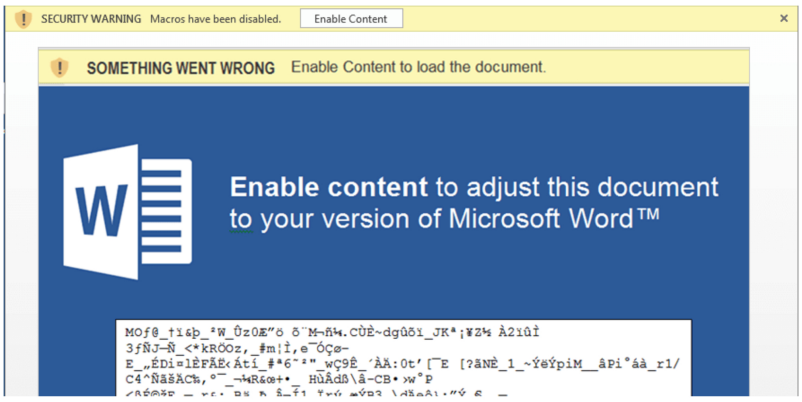
MALICIOUS ATTACHMENTS

It's not as easy as spamming random email addresses with your latest malware .exe file. Not only will most email providers prohibit sending attachments with certain file types, they can also perform basic attachment scans that can identify malware, and prevent you from sending it. If you received an email from a random address with a .vbs file, would you open it? The chances are that you don't deal with .vbs files, and because it's unexpected you'd immediately be cautious.

But what if someone sent you a Microsoft Office document, such as a Word or Excel document – these files are used daily within organisations, and receiving these would be less immediately suspicious. These files can't be malware right? They can – kinda.

Microsoft Office Macros

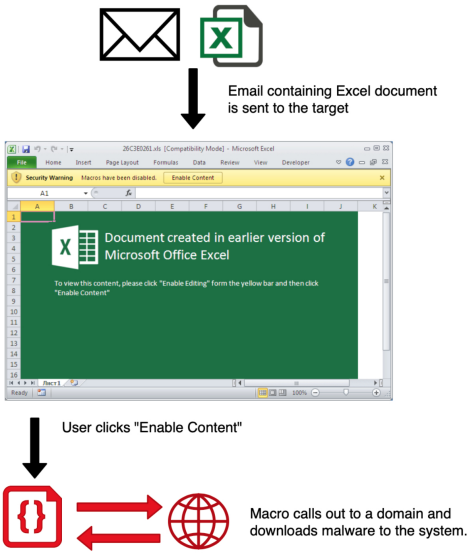
MS Office documents such as Word and Excel offer the ability to include macros. These are a series of commands and instructions that can be run automatically once enabled. Macro malware was fairly common several years ago because macros ran automatically when a document was opened. However, in recent versions of Microsoft Office, macros are disabled by default. This means malware authors need to convince users to enabled macros so their malware can execute. They do this by showing fake warnings when a malicious document is opened.



The above screenshot shows an example of a malicious Microsoft Word document. At the top we have the legitimate ribbon, where users can click "Enable Content" to unlock the document, allowing macros to run automatically. Everything below this ribbon is fake, and has been crafted by the malicious actor, including the second ribbon titled "SOMETHING WENT WRONG". The attack is trying to convince the recipient that this

document is an older version, and that they need to convert it to the latest version to run properly.

Once run, these macros can connect to domains on the internet and download malware directly to the system. This can range from viruses to trojans, ransomware to rootkits.



It is crucial that appropriate defensive measures are taken and users are trained to spot and respond to suspicious emails. Microsoft have published some good suggestions for defending against macro malware:

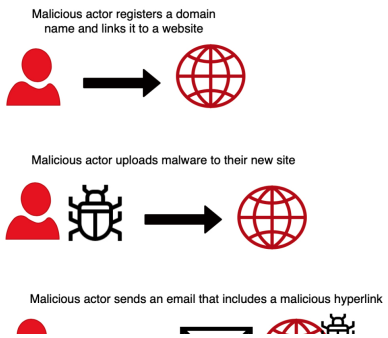
- Make sure macros are disabled in your Microsoft Office applications. In enterprises, IT admins set the default setting for macros: Enable or disable macros in Office documents
- Don't open suspicious emails or suspicious attachments.
- Delete any emails from unknown people or with suspicious content. Spam emails are the main way macro malware spreads.
- Enterprises can prevent macro malware from running executable content using ASR rules.

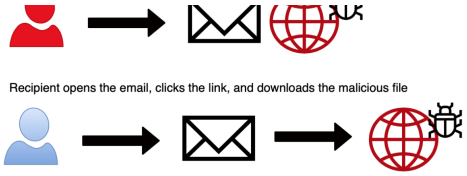
HOSTED MALWARE

The other primarily delivery method of malware is by hosting it on websites, and convincing users to click on a hyperlink, download a file, and then run it. It's very similar to macro malware, but users need to manually visit and download the malware themselves.

Malicious Domains

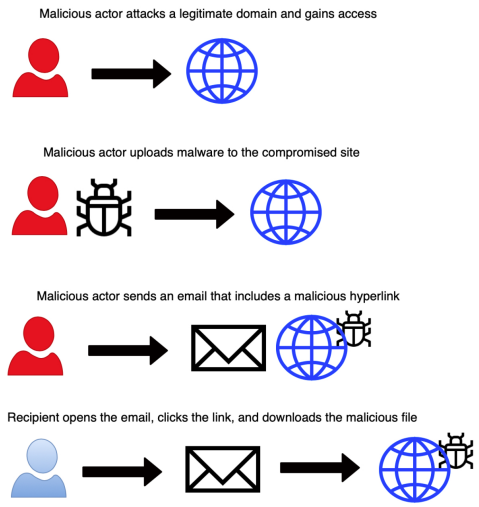
Domains can be created by anyone in a matter of minutes, and for as cheap as the price of a coffee. It's no surprise that SC Magazine reported in August 2019 that 200,000 new domains are registered a day, and "70 percent of these are malicious or suspicious and used for a wide range of nefarious activities". That's 140,000 malicious domains a day. Then all the attacker needs to do is host a malicious file on a URL, and include it in phishing emails.





Compromised Domains

Legitimate sites can be compromised by attackers, and then used to host malware. Often the legitimate site is left completely intact so that the site owner and visitors don't realise their site has been hacked and is being utilised for malicious purposes. A hyperlink to the malicious URL hosting the malware is then distributed in phishing emails.



Previous Topic
Back to Lesson
Next Topic