National Cyber Security Centre

2206221703-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Changing Criminal Tactics in Response to Microsoft's Blocking of Internet Macros
2022-06-22

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Summary

Recently, Microsoft has made changes in order to make it more difficult to enable macros in files obtained from the internet[1] meaning VBA macros obtained from the internet are now blocked by default. Once a user opens an attachment or downloads from the internet an untrusted Office file containing macros, a message bar displays a Security Risk that the file contains Visual Basic for Applications (VBA) macros obtained from the internet and a *Learn More* button. The *Learn More* button contains information about the security risk of bad actors using macros, safe practices to prevent phishing & malware, and instructions on how to enable these macros by saving the file and removing the Mark of the Web (MOTW)[2].

These changes have meant that some threat actors have also amended the way in which they are attempting to deliver malware to potential victims.

Criminal actors have been observed making further use of Email Thread Hijacking, HTML attachments using HTML smuggling techniques, malicious IMG files which will mount malware and LNK files which launch malicious DLL files.

These incidents illustrate a significant evolution in tactics, forced by changes in how Microsoft Office documents handle macros and Security administrators should be aware of the potential for these altered tactics to evade current security measures in place.

Organisations that use Macros may need to adjust the policies for how Microsoft Office handles macros and should ensure that users are aware of these changing tactics that are being used by threat actors.

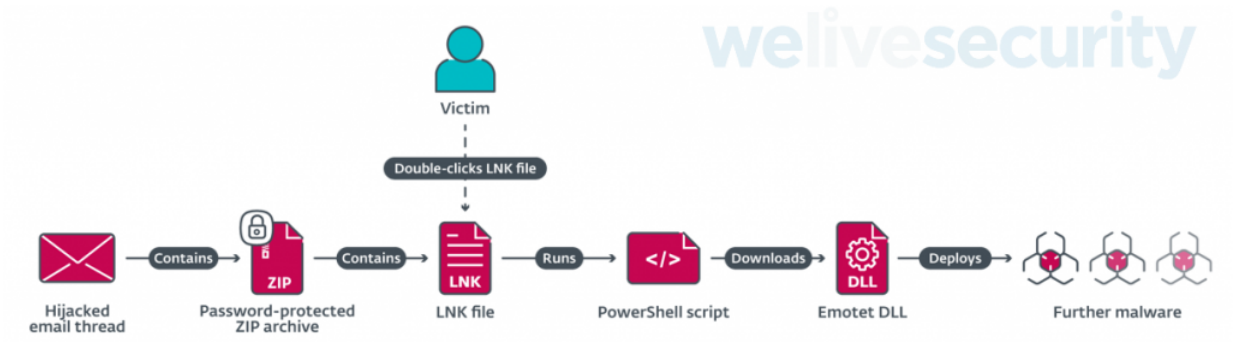

Figure1: Example Emotet Using new Tactics[3]

[1] https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

[2] The MOTW is an attribute added to files by Windows when it is sourced from an untrusted location (Internet or Restricted Zone). The files must be saved to a NTFS file system, the MOTW is not added to files on FAT32 formatted devices

[3] https://www.welivesecurity.com/2022/06/16/how-emotet-is-changing-tactics-microsoft-tightening-office-macro-security

Analysis

The NCSC has observed a number of recent incidents where threat actors have used changing tactics in order to deliver malspam. These new tactics include:

- **Email Thread Hijacking** - Threat actors are using previously compromised email systems to steal conversations and inserting this text into their malspam emails in order to add legitimacy to a malicious email. Users should be made aware of this technique and should ensure that the email sender is correct for the conversation contained therein.
- **HTML File** - The adversary makes use of an evasive technique called HTML smuggling in which the threat actor "smuggles" an encoded malicious script within a specially crafted HTML attachment or web page.
- **ZIP File** - HTML-smuggling technique is used to write a ZIP file with the same filename as the HTML attachment to the host. The ZIP file contains an IMG file that is then mounted.
- **IMG/ISO File** - contains .docx file, a malicious DLL and a LNK file that launches the DLL. In some instances, the *.docx* file is opened and a **ms-msdt/Follina exploit** is attempted.
- **LNK file** - launches the malicious DLL using the following command which executes the malware delivery chain (Qakbot in this instance):

  `C:\Windows\System32\rundll32.exe 019338921.dll, DllInstall`
- **PowerShell (PS) script** - An obfuscated Powershell script is used that likely contained a Cobalt Strike loader.

The campaigns observed by the NCSC have often used Email Thread Hijacking with phishing lures that downloaded a series of files and ultimately led to an attempt to execute Qakbot or Emotet on the victims device.

Recommendations

The Tactics, Techniques, and Procedures (TTPs) observed in these attacks are not novel or unusual, but were for a long time less common as the use of Microsoft Office files containing macro's was a more common attack vector in recent years.

These variations in TTPs are almost certainly in response to Microsoft's recent disablement of Excel 4.0 macros as default, which has encouraged several eCrime adversaries to adapt their TTPs in recent times.

Email thread hijacking is an effective vector for phishing attacks. Attackers increase their success by using the trusted email accounts involved in the thread to introduce malicious payloads. Any successfully compromised accounts are used to start a fresh wave of spam mails replying to email threads, in addition to conducting malicious operations on the computer. It is recommended that organisations ensure that users are aware of this attack vector and the associated risks.

The change of tactic should mean that organisations should review their current email security processes such as:

- Increase user awareness to ensure that these new types of attacks are known to users i.e. Email Thread Hijacking, unusual .html attachments.
- Some archiver software does not propogate Mark Of The Web, which can circumvent blocking. A useful github page has been set up to track which archiver software can propagate MOTW to extracted files: Github - Archiver-MOTW-support-comparison.
- Run phishing simulation exercises to test and renew employees' security awareness.
- Use an email security solution that can block phishing, spam, and other malicious emails from reaching inboxes.
- Implement DMARC for your domains in order to prevent email spoofing of your domain name.
- Ensure that systems are fully patched in order to prevent exploitation of the ms-msdt/Follina vulnerability.

Mitre Att&ck

Malicious Software Observed
https://attack.mitre.org/software/S0650/ - QBot
https://attack.mitre.org/software/S0367/ - Emotet

Malicious Techniques Observed
https://attack.mitre.org/techniques/T1566/001/ - SpearPhishing Attachment
https://attack.mitre.org/techniques/T1053/ - Scheduled Task Creation
https://attack.mitre.org/techniques/T1199/ - Trusted Relationship
https://attack.mitre.org/techniques/T1553/005/ - Subvert Trust Controls: Mark-of-the-Web Bypass
https://attack.mitre.org/techniques/T0863/ - User Execution
https://attack.mitre.org/techniques/T1105/ - Ingress Tool Transfer
https://attack.mitre.org/techniques/T1071/001/ - Application Layer Protocol: Web Protocols
https://attack.mitre.org/techniques/T1114/001/ - Email Collection: Local Email Collection

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie