MS Word Forensic Locations

Md. Abdullah Al Mamun

linkedin.com/in/mamun-infosec

Find Recent Macro Enabled Files

HKCU\SOFTWARE\Microsoft\Office\<version>\Word\Security\TrustedDocuments\TrustRecords

This registry key contains a list of file names. Here, look for the file names with value ‘FF FF FF 7F’ at the end. These files had macro enabled.

Find Recent Word Files

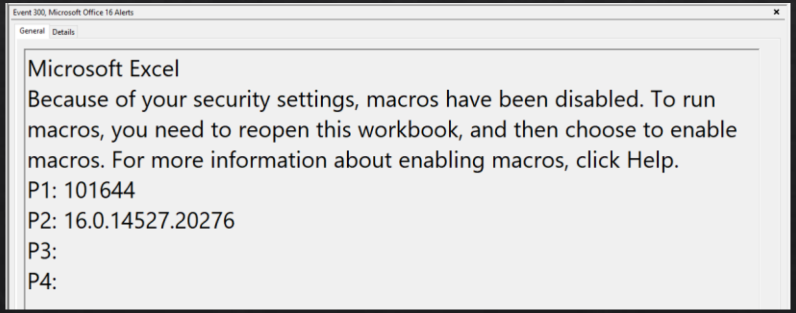
%appdata%\Microsoft\office\Recent

LNK files of recent MS Word files are stored in this location. Even, image files such as JPG that were used in Word documents are stored here.

Find Recent Alerts

Event Viewer > Applications and Services Logs > Microsoft Office Alerts

Open the Event Viewer and go to this location. You will get alerts, which were recently shown to the user such as below-



Microsoft Excel
Because of your security settings, macros have been disabled. To run macros, you need to reopen this workbook, and then choose to enable macros. For more information about enabling macros, click Help.
P1: 101644
P2: 16.0.14527.20276
P3:
P4:

Find Startup Files for Word

C:\Users\<user>\AppData\Roaming\Microsoft\Word\STARTUP

When a user starts MS Word, files in this location are automatically loaded.

These files will be in .dot, .dotx or .dotm format.

Find Macro Security

HKCU\Software\Policies\Microsoft\Office\<version>\Word\Security\VBAWarnings

Value of ‘VBAWarnings’ 1 means all macros are enabled, 2 means all macros are disabled with notification, 3 means all macros are disabled except those digitally signed, 4 means all macros are disabled without notification.

Find MS Word Cache

%LocalAppdata%\Microsoft\Windows\INetCache\Content.Word

This location is used to store MS Word scratch files in this location. So, if a user opens a .docx file with macro, Word may create ‘WRCxxxx.tmp’ file in this location. This file may contain various artifacts. Another location can be- ‘INetCacheContent.Word’.

Find Word Files Opened in Outlook

%LocalAppdata%\Microsoft\Windows\INetCache\Content.Outlook\<Folder>

Attachments opened in outlook are stored in this location. As malicious MS Word attachments with macro can be opened from email so, this location should be checked.