Microsoft Word and Sandboxes

bartblaze.blogspot.com/2024/08/microsoft-word-and-sandboxes.html

Today's post is a brief one on some Microsoft Word and sandbox detection / discovery / fun.

Collect user name from Microsoft Office

Most sandboxes will trigger *somehow* or *something* if a tool or malware tries to collect system information or user information. But what if we collect the user name via the registry and more specifically, what user info Microsoft Office sees?

This information is stored in the Current User hive, Software\Microsoft\Office\Common\UserInfo.

10-second code and we can whip up:

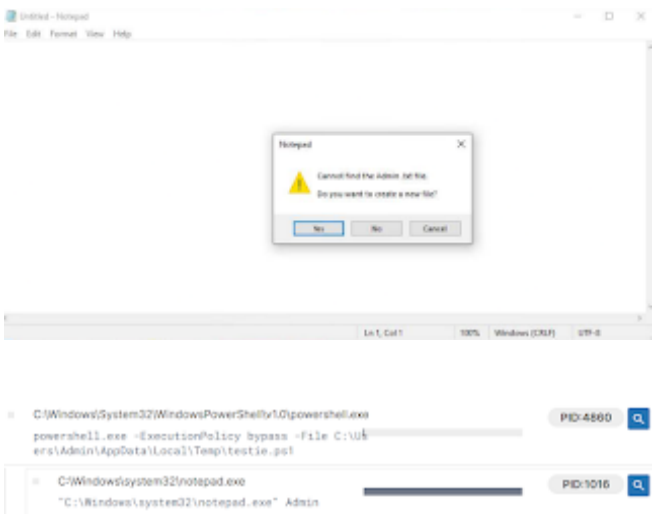
```
$userName = (Get-ItemProperty -Path "HKCU:\Software\Microsoft\Office\Common\UserInfo").UserName
Start-Process -FilePath "notepad.exe" -ArgumentList $userName
```

Text form:

> *$userName = (Get-ItemProperty -Path "HKCU:\Software\Microsoft\Office\Common\UserInfo").UserName*
>
> *Start-Process -FilePath "notepad.exe" -ArgumentList $userName*

And we get something like:

and the process tree:
Some sandboxes had a username of "Admin", "admin" or a completely random name.
In short, it's a potential technique for more stealth reconaissance that may not trigger a sandbox or detection mechanism.



Run a Microsoft Word doc with.. .asd extension

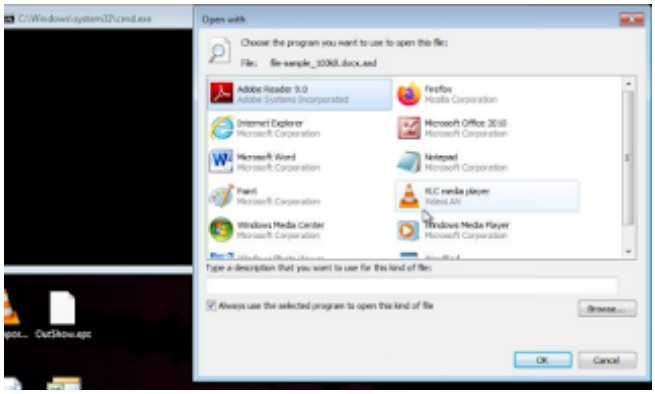
When Microsoft Word crashes, it will (usually) attempt to create a backup copy of all your opened documents. It typically saves these backups as .wbk (Word Backup) or .asd (Autosave or Autorecover) files.

These will be saved in one of these directories in normal circumstances:

- C:\Users\USERNAME\AppData\Local\Microsoft\Word
- C:\Users\USERNAME\AppData\Roaming\Microsoft\Word
- C:\Users\USERNAME\AppData\Local\Temp
- C:\Users\USERNAME\\AppData\Local\Microsoft\Office\UnsavedFiles

Most sandboxes however will be able to open the file just fine, but not all...:

I haven't seen much use of actual .asd files, likely as the documents will need to be loaded from one of the above directories, however... after crafting your malicious document, you can simply rename it from *badfile.docx* to *badfile.asd*, and it will run fine.



It seems at least 1 actor has used an .asd extension before, as reported on by Didier Stevens:

https://isc.sans.edu/diary/CrowdStrike+Outage+Themed+Maldoc/31116

In short, it's another way of evading sandboxes or other potential detection mechanisms thay may not support these .asd or .wbk extensions or even consider them harmless.