

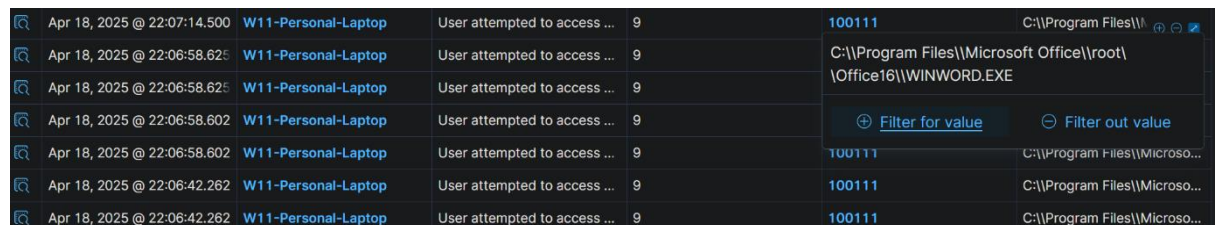
Event Analysis: Honeytoken Access

I started off by analysing events generated when accessing the monitored file "Passwords.docx". I did this by opening the file for approximately 20 seconds, which would very consistently generate 17-18 events. The events were heavily concentrated within the first 1-3 seconds, with a trailing event at the end of the duration (15-20 seconds after). The most interesting field of these events was access request information, which includes a field on Accesses (the action being carried out) and Access Mask (hexadecimal code for the access).

There were 3 different Access Masks which mapped to different Accesses:

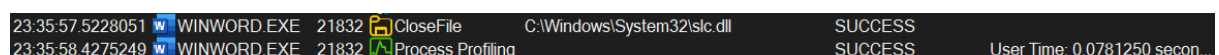
- READ_CONTROL (0x2000) - "The right to read the information in the object's security descriptor, not including the information in the system access control list (SACL)." (Microsoft)
- ReadData (0x1) - "For a file object, the right to read the corresponding file data." (Microsoft)
- ReadAttributes (0x80) - "The right to read file attributes." (Microsoft)

I then created a timeline of these events. Observing the time stamps, I noticed that a lot of the events were grouped into tight bursts and that some of the sequences of the Accesses repeated exactly. This made me think that there was a possibility that each pattern corresponded to a specific file process. To investigate this, I used Windows Process Monitor which can be used to observe real-time file system, registry and process/thread activity. This was ultimately unsuccessful as the timestamps did not match up. The two closest timestamp matches for the start of the run time were close file and a profiling activity, neither of which match the activity that was done at the time. This was something unexpected, as the ProcessName field in the event matched up with the source of the process that I was filtering with in Process Monitor (WINWORD.EXE).



Apr 18, 2025 @ 22:07:14.500	W11-Personal-Laptop	User attempted to access ...	9	100111	C:\\Program Files\\Microsoft Office\\root\\Office16\\WINWORD.EXE
Apr 18, 2025 @ 22:06:58.625	W11-Personal-Laptop	User attempted to access ...	9		
Apr 18, 2025 @ 22:06:58.625	W11-Personal-Laptop	User attempted to access ...	9		
Apr 18, 2025 @ 22:06:58.602	W11-Personal-Laptop	User attempted to access ...	9		
Apr 18, 2025 @ 22:06:58.602	W11-Personal-Laptop	User attempted to access ...	9	100111	C:\\Program Files\\Microsoft Office\\root\\Office16\\WINWORD.EXE
Apr 18, 2025 @ 22:06:42.262	W11-Personal-Laptop	User attempted to access ...	9	100111	C:\\Program Files\\Microsoft Office\\root\\Office16\\WINWORD.EXE
Apr 18, 2025 @ 22:06:42.262	W11-Personal-Laptop	User attempted to access ...	9	100111	C:\\Program Files\\Microsoft Office\\root\\Office16\\WINWORD.EXE

Figure 27: ProcessName of HoneyToken Events for Passwords.docx



23:35:57.5228051	WINWORD.EXE	21832	CloseFile	C:\\Windows\\System32\\slc.dll	SUCCESS	
23:35:58.4275249	WINWORD.EXE	21832	Process Profiling		SUCCESS	User Time: 0.0781250 secon...

Figure 28: CloseFile and Process Profiling Closest to the Correct Time Stamp (Target Timestamp was 23:35:57.926, Difference of Approximately +/- 0.4 Seconds)

Ultimately, I decided to repeat opening the file and recording the events to see what patterns I could uncover over eight data samples. The strongest pattern I found was “read_control, read_control, read_data, read_data, read_attributes, read_data, read_data, read_attributes, read_control, read_attributes”. This appeared as an exact match in isolated time bursts for the first, second and third samples as well as in the fourth and eighth with the caveat that the fourth and eighth did not have clean burst timings. The length, specificity and frequency of this sequence makes me inclined to think that this is a very specific action being performed as well as the fact it always occurred in the middle of the sequence.

The next pattern I observed was the samples ending with an isolated “read_attributes”. While all other events were grouped very tightly, 16-17 events within one to three seconds, this would often appear 10-20 seconds later. The first sample (albeit with an isolated double read_attributes instead of a single), third, fourth, fifth and eighth all had this appear. What makes this pattern strong is just how isolated it is from the rest of the events; it likely has something to do with the file being closed.

The final pattern I observed was a lot weaker than the other two in its specificity. It was very common to have each data sample open with read_control followed by a variable sequence of read_attributes and read_data, but it was difficult to ascertain a single recurring one. The closest was “read_control, read_data, read_attributes, read_data, read_attributes, read_attributes, read_attributes”. The first sample had an exact match to this and the second was missing the first read_control, but it was also one of only two samples that did not open with read_control. It is possible the read_control was missed out for some reason or another.

Though the matching of specific processes to Access Mask patterns was unsuccessful, it provides an avenue of exploration for comparing normal Access Mask patterns in important files against anomalous Access Mask patterns, which may signal malicious activity within a personal device.

Other key information includes the SubjectLogonID, which is a unique identifier for the session. This can be used to correlate activities performed within the session to create a timeline and understand both the actions performed within the session as well as the timescale it was performed within, creating a greater understanding of the breach if the Honeypot was accessed maliciously.

21:40:56.010	W11-Personal-Laptop	User attempted to access ...	9	100111	0x80
21:40:46.595	W11-Personal-Laptop	User attempted to access ...	9	100111	0x80
21:40:46.593	W11-Personal-Laptop	User attempted to access ...	9	100111	0x20000
21:40:46.585	W11-Personal-Laptop	User attempted to access ...	9	100111	0x80
21:40:46.230	W11-Personal-Laptop	User attempted to access ...	9	100111	0x1
21:40:46.227	W11-Personal-Laptop	User attempted to access ...	9	100111	0x1
21:40:46.226	W11-Personal-Laptop	User attempted to access ...	9	100111	0x80
21:40:46.219	W11-Personal-Laptop	User attempted to access ...	9	100111	0x1
21:40:46.219	W11-Personal-Laptop	User attempted to access ...	9	100111	0x1
21:40:46.216	W11-Personal-Laptop	User attempted to access ...	9	100111	0x20000
21:40:46.213	W11-Personal-Laptop	User attempted to access ...	9	100111	0x20000
21:40:45.350	W11-Personal-Laptop	User attempted to access ...	9	100111	0x80
21:40:45.344	W11-Personal-Laptop	User attempted to access ...	9	100111	0x80
21:40:44.418	W11-Personal-Laptop	User attempted to access ...	9	100111	0x1
21:40:44.418	W11-Personal-Laptop	User attempted to access ...	9	100111	0x80

Figure 1: Example Data Sample for HoneyToken Use Case, Access Masks are the Rightmost Column

read_attributes 21:40:44.418, read_data 21:40:44.418, read_attributes 21:40:45.344, read_attributes 21:40:45.350, read_control 21:40:46.213, read_control 21:40:46.216, read_data 21:40:46.219, read_data 21:40:46.219, read_attributes 21:40:46.226, read_data 21:40:46.227, read_data 21:40:46.230, read_attributes 21:40:46.585, read_control 21:40:46.593, read_attributes 21:40:46.595, read_attributes 21:40:56.010

Figure 2: Example Data Sample with Access Masks Converted to Accesses and Grouped Based on Timing

timestamp	agent.name	rule.description	rule.level	rule.id	data.win.eventdata.sub...
Feb 20, 2025 @ 16:50:46.1...	W11-Personal-Laptop	User attempted to access ...	9	100111	0xd6277e3
Feb 20, 2025 @ 16:50:46.1...	W11-Personal-Laptop	User attempted to access ...	9	100111	0xd6277e3
Feb 20, 2025 @ 16:50:46.1...	W11-Personal-Laptop	User attempted to access ...	9	100111	0xd6277e3
Feb 20, 2025 @ 16:50:46.1...	W11-Personal-Laptop	User attempted to access ...	9	100111	0xd6277e3

Figure 3: Set of Honeytoken Events with a Unique SubjectLogonID

timestamp	agent.name	rule.description	rule.level	rule.id	data.win.eventdata.sub...
Apr 12, 2025 @ 22:23:06.993	W11-Personal-Laptop	User attempted to access ...	9	100111	0x679108
Apr 12, 2025 @ 21:43:54.654	W11-Personal-Laptop	User attempted to access ...	9	100111	0x679108
Apr 12, 2025 @ 21:43:54.616	W11-Personal-Laptop	User attempted to access ...	9	100111	0x679108
Apr 12, 2025 @ 21:42:27.648	W11-Personal-Laptop	User attempted to access ...	9	100111	0x679108

Figure 4: Another Set of Honeytoken Events with a Different Unique SubjectLogonID