Analysis of Windows' Registry Key Value to Look for Malware Using AI Generated Code

Peter Bentley, School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham, UK

***Abstract* –** Advanced Persistent Threats are known to place some of their malware in the Windows registry. This is known as Fileless malware. Long Registry key values could indicate the existence of such malware, as could differences in Registry keys from a Reference set of Registry keys. This paper reviews the length of Registry Key values and well as looking for new Registry keys and uses the results to highlight possible malware. This analysis is supported by a bespoke program of AI generated C code. Although no malware was found it is believed that the technique is inexpensive and robust enough for purpose.

Keywords –Microsoft Windows; Encrypt; Decrypt; Encode; Decode; Compression, Advanced Persistent Threat (APT); Windows; Registry Key; Malware; Fileless malware; Indicator of Compromise; Artificial Intelligence; AI.

1. Introduction

This paper is the fifth in an occasionally issued series of post-doctoral Monographs. It is produced to demonstrate a cost-effective way to potentially identify the existence in Registry keys of items associated with malware.

One C program was generated by AI in support of this paper. Although the thrust of the paper is analysis of the Registry, part of it turned into an exercise to evaluate C code generated by Artificial Intelligence (AI) (Microsoft Perplexity, 2025). Work surrounding this code is discussed later in the Monograph. All other software is taken from Microsoft available software i.e. Living Off the Land. The data under analysis is taken from the HKEY_CURRENT_USER\Software\Microsoft portion of Registry of Windows 10 Enterprise machines.

This paper is agnostic towards the origin and intent of APTs.

2. Literature Review

It is known that some APTs store parts of the attack chain malware in the Windows Registry (Wüest and Anand, 2017). This is known as Fileless malware. Symantec define fileless malware as:

- "**Memory only threats**, such as SQL Slammer
- **Fileless persistence**, such as VBS in the registry
- **Dual-use tools**, such as psExec.exe, which are used by the attacker
- **Non-PE file attacks**, such as Office documents with macros or scripts"

(Wüest and Anand, 2017, p. 10)

APTs are known to add new Registry keys (Mitre ATT&CK, 2025). However, there is little evidence that APTs place Portable Executables (PEs) directly in the registry "(e.g., placing an executable in the Registry run key)" (Qi Liu et al, 2024).

Two desktop computers were used for this paper: one that had not been rebooted since 18th June 2025 (the Analysed computer) and one that was rebooted on 13th August 2025 (the Reference computer). Both computers were running Windows 10 Enterprise and were booted from the same Deep Freeze version (Faronics, 2025).

3. The AI Generated Program

It was decided that this analysis might be a good test bed of AI generated C code. Four programs were produced:

- Program One compiled with no structural/logical modifications but did not thoroughly search all subkeys;
- Program Two compiled with no structural/logical modifications and performed as required. Slight changes to the output format were needed to import the data into a Microsoft Excel spreadsheet;
- Programs Three and Four did not compile without structural modifications.

Programs One and Two were tested: The edge cases of start and end Registry keys were viewed to check that they had been correctly processed as well as random keys within the sub-tree under analysis (HKEY_CURRENT_USER\Software\Microsoft). As stated, Program One was not fit for purpose but Program Two was.

4. Analysis

Windows Registry Key types are well-documented (Microsoft (2024). Program Two was run against the Analysed computer. The Registry key value name, value type and value length were extracted, semi-colon separated. This was then imported into an Excel spreadsheet and the value length were analysed (Appendix A). Not all registry value types were seen (Microsoft, 2024) in the data. There are some long registry key lengths:

- The REG_SZ subkey with length 7730 is HKEY_CURRENT_USER\Software\Microsoft\Speech_OneCore\Isolated<redacted>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Speech_OneCore\PhoneConverters\Tokens\Chinese;
- The REG_BINARY sunkey with length 7168 is HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\officeclicktorun\ConfigContextData.

These keys were viewed to see if they might be associated with malware e.g Portable Executables (PEs), batch files, PowerShell files etc. They were not of types thought to be associated with malware.

APTs create registry keys as part of their attack chain. Program Two was run against the Reference computer. Again, the Registry key value name, value type and value length were extracted, semi-colon separated. This data was combined with the data from the Analysed computer and put into a Pivot Table. Any Registry Key with a frequency of one would be a candidate for creation by a process or program after reboot. All Registry keys with an odd frequency count may also be such a candidate. No such keys were found. This method of analysis is similar to that for file analysis in previous research (Bentley, 2025).

5. A Critique of this Work

The data for this paper was taken from a subset of the Registry, HKEY_CURRENT_USER\Software\Microsoft. Malware may not be restricted to this set of subkeys and the range could be extended.

Program Two did not extract the full Registry key name. Registry key modifications leaving (for example) the key length the same would not be highlighted.

6. Comments on Using AI Generated C Code

This was the first time that this author had used AI to generate code. The main lesson is that simple code can be generated but the question asked of AI should be precise. As usual with code through testing should be performed: just because the first program appeared to be correct and compiled at the first attempt it does not mean that the code is logically correct. The Software Devlopment Life-Cycle should not be ignored or stages omitted.

7. Suggested Lines of Further Work

A full analysis of a Reference and Analysed computer Registries could be performed. Full Registry key name could be used.

8. Concluding Remarks

This paper has demonstrated a cost-effective method of highlighting possible malware stored in changes to the Microsoft Windows Registry.

REFERENCES

Bentley, P. (2025) A Review of Some Windows’ File Metadata Which Could Highlight Indicators of Compromise. Accessed September 2025)

Faronics (2025) *Deep Freeze* Available at: https://www.faronics.com/en-uk/products/deep-freeze (Accessed 13th August 2025)

Microsoft Perplexity (2025) "c code to walk windows registry, output sub-key name, type, value and length". Available at Author’s Repository (Accessed August 2025)

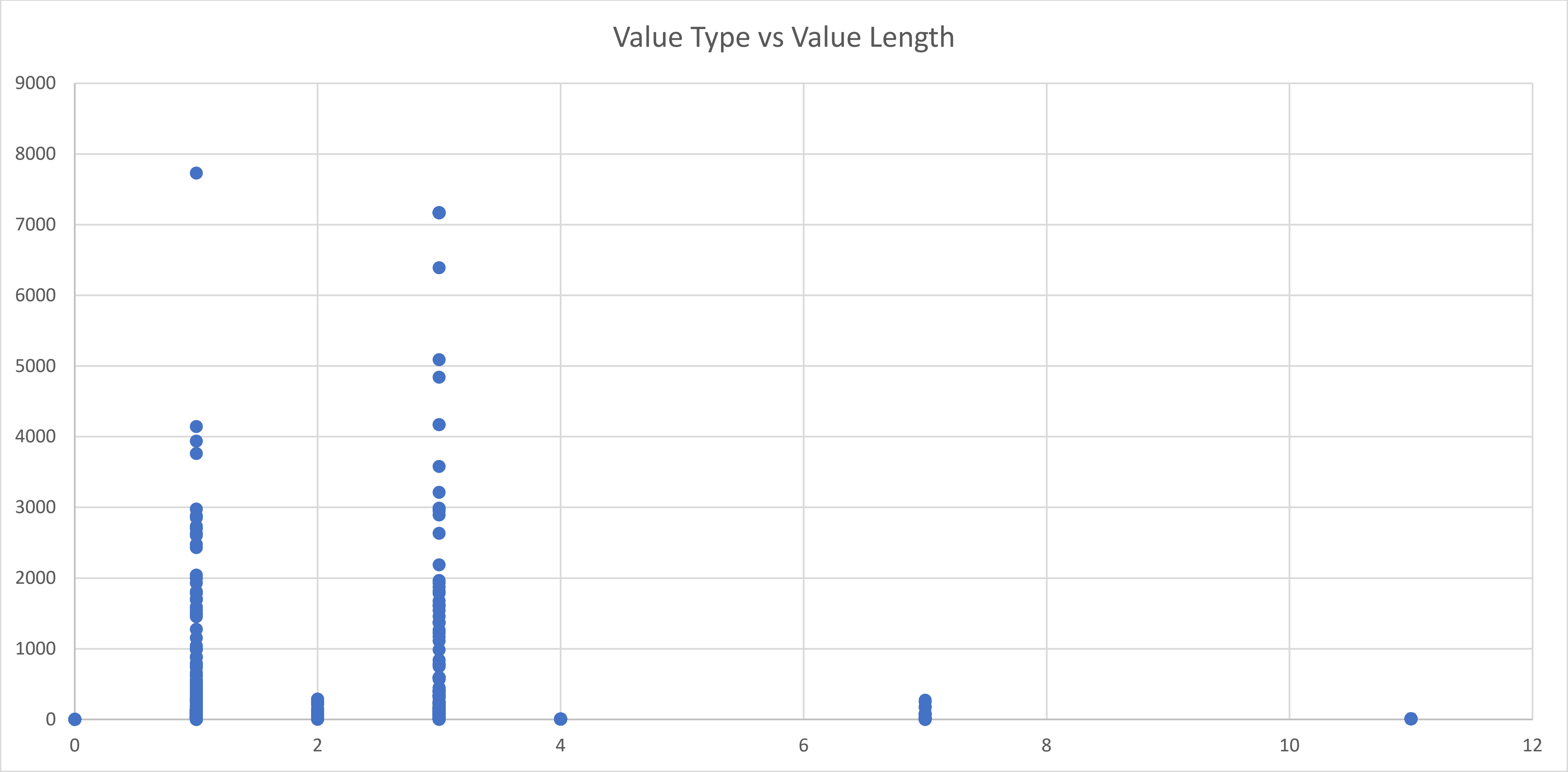
Qi Liu, Muhammad Shoaib, Mati Ur Rehman, Kaibin Bao, Veit Hagenmeyer, Wajih Ul Hassan (2024) Accurate and Scalable Detection and Investigation of Cyber Persistence Threats Available at: https://arxiv.org/abs/2407.18832 (Accessed 12th August 2025)

Microsoft (2024) *2.2.3.9 Registry Type Values.* Available at: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/25cce700-7fcf-4bb6-a2f3-0f6d08430a55 (Accessed 8th August 2025)

Mitre ATT&CK (2025) *Windows Registry: Windows Registry Key* Available at: https://attack.mitre.org/datasources/DS0024/#Windows%20Registry%20Key%20Creation (Accessed 13th August 2025)

Wüest, C. and Anand, H. (2017) Living Off the Land and Fileless Attack Techniques. Symantec Available at: https://www.symantec.com/content/dam/symantec/docs/securitycenter/white-papers/istr-living-off-the-land-and-fileless-attack-techniquesen.pdf (Accessed: 7th August 2025).

Appendix A: Registry Key Type vs Registry Value Length


Value Type vs Value Length