reg-entropy-scanner

TLDR

Scans through registry hives outputting entropy values for key/values, dumps binary contents to files…we are looking for those "fileless" malwarez!

Background

Console application that enumerates every value in the supplied registry hives outputing the string values into a TSV file for checking. For each value it calculates a **shannon entropy** (normalised specific) value for the data, and dumps any binary content to individual files for further analysis. The **dump** file (.bin) is uniquely named (GUID) since the key/value will generally create a file name greater than the maximum permitted by Windows. The .bin file name is stored in the TSV file for correlation back to the key/value

A number of entropy values are calculated:

- Base: calculated using all data
- 8 byte TLV (Type, Length, Value): calculated by skipping the first 8 bytes
- 16 byte TLV (Type, Length, Value): calculated by skipping the first 16 bytes
- 32 byte TLV (Type, Length, Value): calculated by skipping the first 32 bytes

TSV File Format

File	Key	ValueName	ValueType	Entropy	Entropy (8 byte TLV)	Entropy (16 byte TLV)	Entropy (32 byte TLV)	Bin File	Data	Data (ASCII)
SOFTWARE	Classes.air	Content Type	RegSz	0.3724863		application/vnd.adobe.air-application-installer-package+zip				
SOFTWARE	Classes\AppID{3F4D7BB8-4F38-4526-8CD3-C44D68689C5F}	AccessPermission	RegBinary	0.2773132	SOFTWARE53e50dc0-744b-434e-abdf-49d1274d8251.bin	01-00-04-80-60-	"? `pL???????? "			

Third Party

Uses Eric Zimmermans excellent Registry library: https://github.com/EricZimmerman/Registry