reg-entropy-scanner

TLDR

Scans through registry hives outputting entropy values for key/values, dumps binary contents to files…w e are looking for those "fileless" malw arez!

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** value for the data, and dumps any binary content to a file that is unique for that value.

TSV File Format

File	Key	ValueName	ValueType	Entropy	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???????"