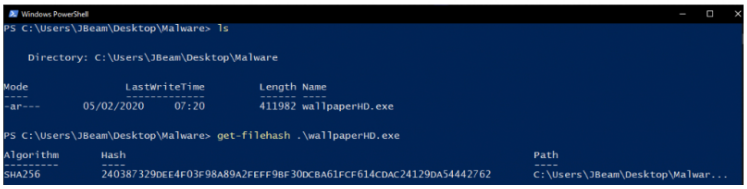
Manual Collection Techniques – File Artifacts

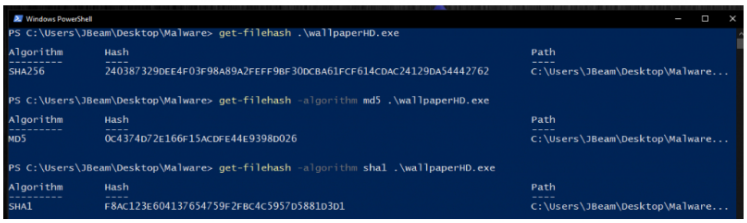
We need to collect file hashes of malicious attachments to perform reputation checks and implement defensive measures. Hashes are the output of a hashing algorithm, such as MD5 (Message Digest 5) or SHA (Secure Hash Algorithm). These algorithms will produce a unique string that is used to represent the file. If there is a single change to the file, such as editing a text file and changing one character, the hash will be completely different. You can read more about hashes here.

HASHES VIA POWERSHELL

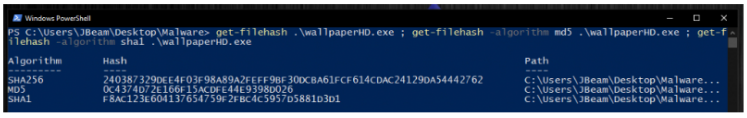
It's most likely that security analysts will be using the Windows OS for day-to-day work. File hashes can be retrieved using PowerShell with the `get-filehash` command. By default, this will generate a SHA256 hash.



We can also retrieve MD5 and SHA1 hashes using the `get-filehash` command with the `-Algorithm` switch.



To make it easier, we can chain PowerShell commands using the ; character and retrieve all three hash values at once.



HASHES VIA LINUX CLI

File hashes can be easily retrieved using the Linux command-line. The three commands we would use are;

- **sha256sum <file>**
- **sha1sum <file>**
- **md5sum <file>**

CONCLUSION

Whilst typically generating MD5 and SHA1 hashes are enough to perform reputation searches online and taking defensive measures within endpoint detection and response (EDR) platforms, some services such as Talos File Reputation require SHA256 hashes to perform checks against their databases. It's useful to know how to generate all three both in Windows and Linux.

Previous Topic
Back to Lesson
Next Topic