Article

Aug 2021

All is fair in Love, War and Anti-Virus Evasion

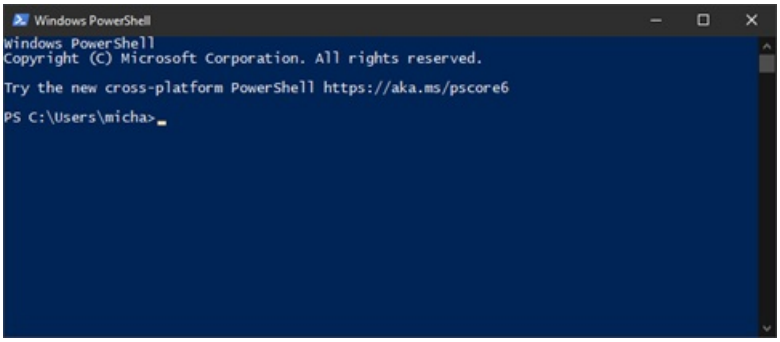
Are Anti-Virus Solutions all you need to secure your business from threats?

In nature, evolution exists as a mechanism of improvement, often helping species adapt to an ever-changing environment. Be it slight advantageous changes to help them attack or in many cases, defend, the ultimate goal is survival. One of the most intuitive and remarkable of these evolutionary traits belongs to the humble Chameleon. These little critters can alter their appearance at will, often in life threatening situations to avoid being spotted by looming predators. This disguise doesn't always work against the smartest of predators, however it is often good enough to fool most of them.

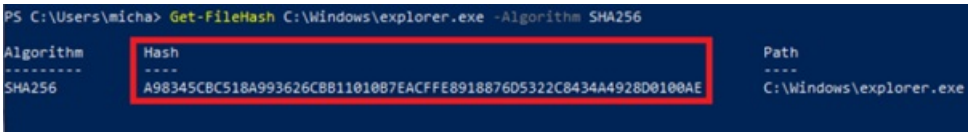
Ok, Technically speaking, within your computer's environment, an Anti-Virus can be considered a predator, with a constantly updating diet. I'm sure you have run into it before. A Basic Anti-virus software updates will often include a message that reads like the following: "Release 00066A44: Update virus definitions (August 2021)", but what does this diet update contain?

Simply put, most definitions are simply a list of hashes belonging to the latest newly discovered viruses and malicious files. So, what is a hash and how do we get one? These hashes are a big string of letters and numbers that is unique to every file. Essentially you can generate them by running them through an algorithm. The beauty of using a hash is that if you change a file just slightly and run it through the algorithm again, it will give you a different hash. Still a bit confusing? Let me demonstrate!

If you press the Windows key + R and run dialogue will pop up. Type in "powershell" without the quotes and hit enter. You should get a blue command prompt like window pop up:



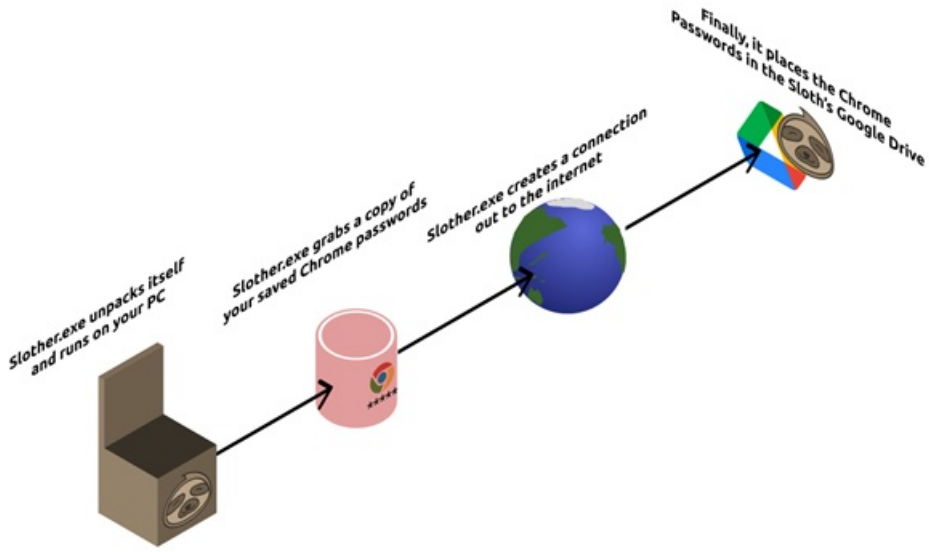
From here, if you type in "Get-Filehash C:\Windows\Explorer.exe -Algorithm SHA256" (again without the quotes) and then hit enter, it should give you the file hash for the Windows file explorer program:



If you're on the exact same version of Windows as me, your hash will likely be the same as mine above. If not, you may have a different version of explorer.exe, indicated by the different file hash. The advantage here is, regardless of the name of the file or where it is, if the contents are exactly the same, the hash will be too.

This is one of many techniques Anti-virus solutions use to detect and remove malicious software, knowing this, we can get into the fun part. To show you an example of why advanced logging and usage of tools such as Sysmon can greatly enhance your businesses cyber resilience, I wrote some basic Malware!

I decided to write a simple piece of malware (I called it Slother.exe) that would extract the target devices Google Chrome passwords from the locally stored SQlite database. It then made a copy of the URL, Username and Password for every saved credential in the database and exported them into an easy to read CSV file. This file would then be uploaded to my Google Drive. Once the file is uploaded the malware would then remove all the files it created and delete itself to hide its tracks.



I know what you are thinking and... No, I will not be providing you with my malware that you could use to steal passwords. I will however be using the malware I wrote in as an example as to why Anti-Virus solutions are not enough to mitigate potential cyber-attacks on your business' infrastructure.

I will be using https://www.virustotal.com/ to check my software against some of the more common antivirus solutions. By submitting a file on Virus Total, the hash is then distributed to vendors to add to their virus definitions (So my Slother.exe malwares hash is now known and being added to many Anti-Virus definitions right now!)

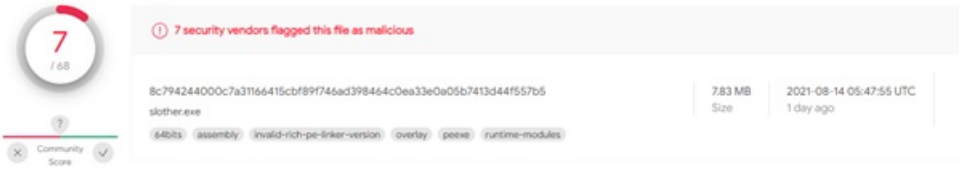
The first time I passed my python code that had been compiled using a free open-source compiler netted the result below.

Not bad 26 Anti-Virus solutions caught my software red-handed!

My Next step was to try a different open-source compiler to see if the number of detections changed. This netted the results below.

Ok, a little better but it's still being detected by a lot of Anti-Virus solutions. Third times the charm?

This time instead of just running a piece of pre-compiled software to package my malware. I downloaded the source code of the second packaging software used above and compiled it myself. By compiling the packaging software myself, my malware was much like the humble Chameleon. Able to change the hash (colour of the Chameleon) to sneak its way past the hungry predators (Anti-Virus).



Presto!

Just like that my malware is being detected by 70% fewer Anti-Virus solutions. Most of which are commonly used in many businesses today. If you would like to look at the results of the scans, there will be links at the bottom of the article.

How can we protect against these types of Anti-Virus mitigation techniques? Well, there are a few options available to help mitigate and respond to these threats quickly. One such technique is using Import Hashing. Import Hashing is the process of monitoring a piece of malware during execution in a controlled environment (Such as a Virtual Machine or Docker Container).

Once the malware has finished running, the data collected from monitoring the malware is the collated. The order and names of the files the malware accessed are then put together and first pass of "slother" at the time "v1" though Virus Total Second pass of "slother" though Virus Total cryptographically hashed. This hash is often referred to as an "IMPHASH". This allows Anti-Virus software to monitor potential malware by monitoring which files the malware accesses, creating an IMPHASH of this data and then comparing it to known IMPHASH data.

Using IMPHASH data we can detect families of malware that access similar files. This means that if the cryptographic hash of the file is different and not in Anti-Virus databases, we are still able to detect malware by monitoring the files it interacts with and the order. For example: If I was to release my Slother.exe malware source code and you were to use the techniques described within this article to re-compile it locally, it would no longer work on most systems. Once a file is uploaded to Virus Total, it creates an IMPHASH of the malware that is send to Anti-Virus vendors.

Unfortunately, the humble Chameleons little trick wont easily get past IMPHASH. Now this isn't a perfect solution, but it is another tool that can assist in detection of simple Anti-Virus mitigation techniques.

Another amazing tool for monitoring and detecting malicious activity is Sysmon. Sysmon is a scalable monitoring solution developed and maintained by Microsoft that provides additional advanced logging and information. Using Sysmon in conjunction with monitoring event ID 4688 provides SOC Engineers a lot more useful information in the battle against bad actors and malware. This additional information is key in early detection and remediation if the malicious little Chameleon manages to get past your Anti-Virus solution.

For information on services that we provide please feel free to get in contact with Andrey, our APAC Head of Customer Success who is always willing to understand your business requirements and needs!

If you want to take a look at the Virus Total scans, please click the links below:

first pass

second pass

third pass