Blue Team Lab

# Indicators

*A suspicious file was found on one of our servers. Use your technical analysis skills to retrieve various indicators that can be used for hunting.*

*Digital Forensics*

*Easy*

**Fairly straightforward in the beginning but I had a bit of trouble with this in the end due to lack of knowledge in wget request.**

File name and “syze” were easy to figure out by just opening the properties on the sample. Aside from some trouble with Exif tool crashing explorer it wasn’t too hard to figure out as well. Opening the help section by opening the application through PowerShell without any arguments told me how to use the tool. I moved the sample into that folder and ran Exif tool on that sample to figure out the typing and come CPU details on the sample. Next came getting the source URL that the sample was downloaded from. The challenge urged me to learn about **zone identifie**r and PowerShell’s “**Get-Content**” cmdlet. Zone identifiers are extra metadata files that browsers will attach upon downloading a file. Zone is there to remind us that it will also say what zone the file came from as well (internet or intranet, etc.).

As many times as it needs to be repeated: **Get-FileHash. Get-FileHash.**

We push the sha through to virus total and malware bazaar and would you look at that. It seems like it’s the famous botnet “**Mirai**”. I didn’t know **malware bazaar** existed until now and it’s an insanely useful resource so into the resource folder it goes. **URLhaus** as well.

These last sections gave me a lot of grief. After opening the sh4 file in notepad, I struggled to effectively navigate the HTTP request like I expected I would be able to do. I couldn’t get that there were 7 unique user-agents (No matter how I looked at it I got 8) and had trouble finding the correct domain referenced by the GET domain. The command was obvious, since it appeared almost every request and I do know Linux.

The download storage one took me a while. I knew that for data exfiltration you could use HTTP request, but I had no idea how to figure out what the destination folder would be for downloads…*which isn’t what the question was*. I had to simply see that all the tools were being fetched out of the same folder but instead I learned quite a bit more about wget that I expected to.

Time to move to the next one. After a good night's sleep.