Xin Yang

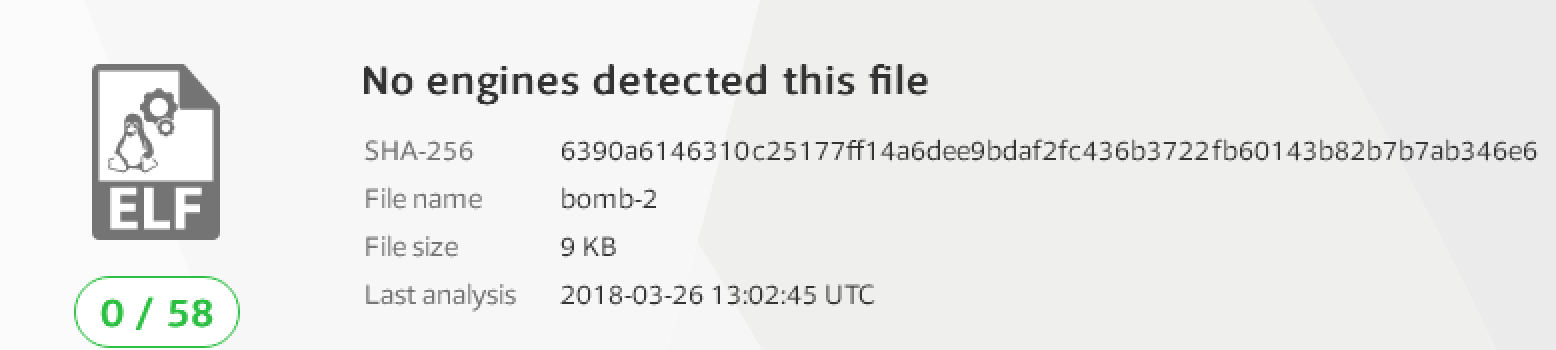
xy213

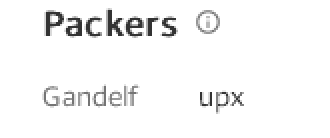
Midterm Malware Report

Static Analysis:

VirusTotal:

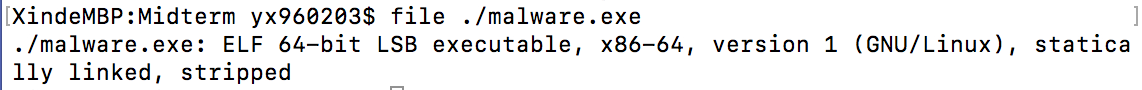
By uploading this malware.exe to VirusTotal, all engines report it as safe, and it’s a 64-bit ELF executable file rather than the MS Windows executable as the extension shows. Also VirusTotal shows it’s packed by UPX.





File:

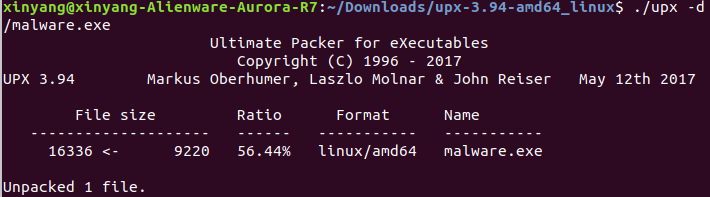
The file command shows this malware is a 64-bit ELF executable, same as VirusTotal.

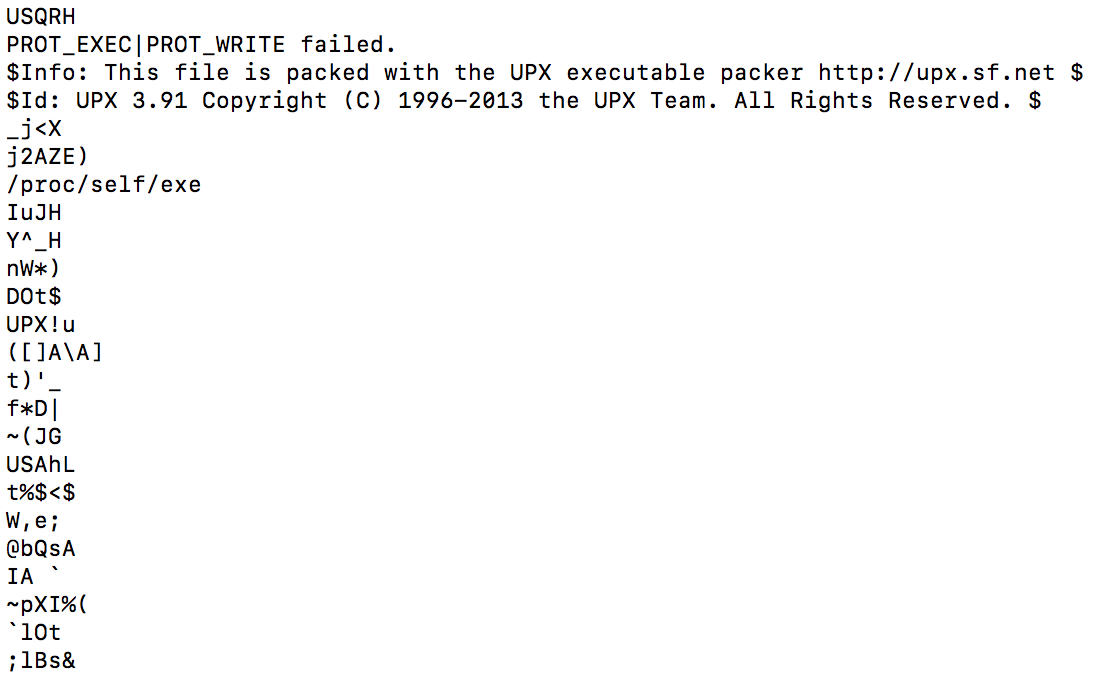


Strings:

The strings command shows some UPX packed information and gibberish as well as some path like “/proc/self/exe” and scattered words like “SUBMITD”, “DNS”.

In this case, I decided to unpack this malware first. Since it’s packed by UPX, I visited the official website and download the latest UPX release. To unpack, I used the command “upx -d malware.exe”, and it successfully unpacked this malware.





Dynamic Analysis: