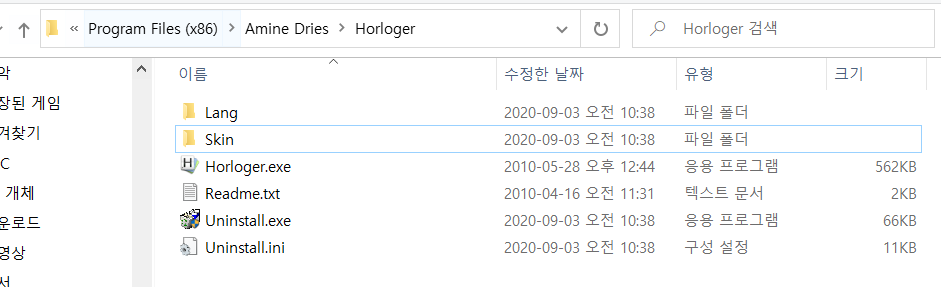
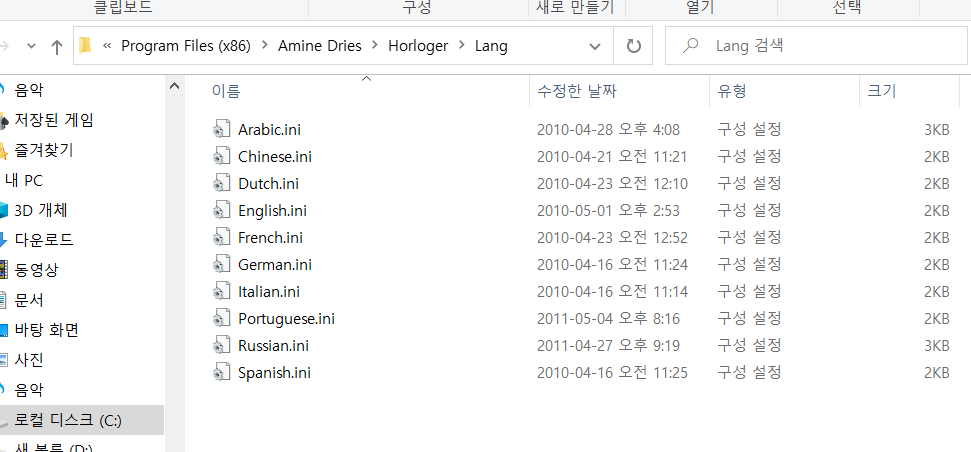


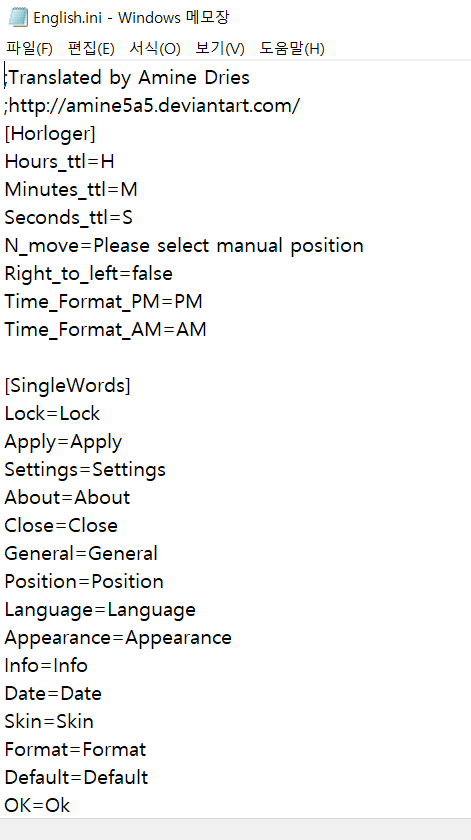
* CreateFile API 로 C:\Program Files (x86)\Amine Dries\Horloger\Lang\English.ini 파일의 핸들을 Desired Access: Generic Read 로 얻음



* C:\Program Files (x86)\Amine Dries\Horloger 내부 모습



* C:\Program Files (x86)\Amine Dries\Horloger\Lang 내부 모습



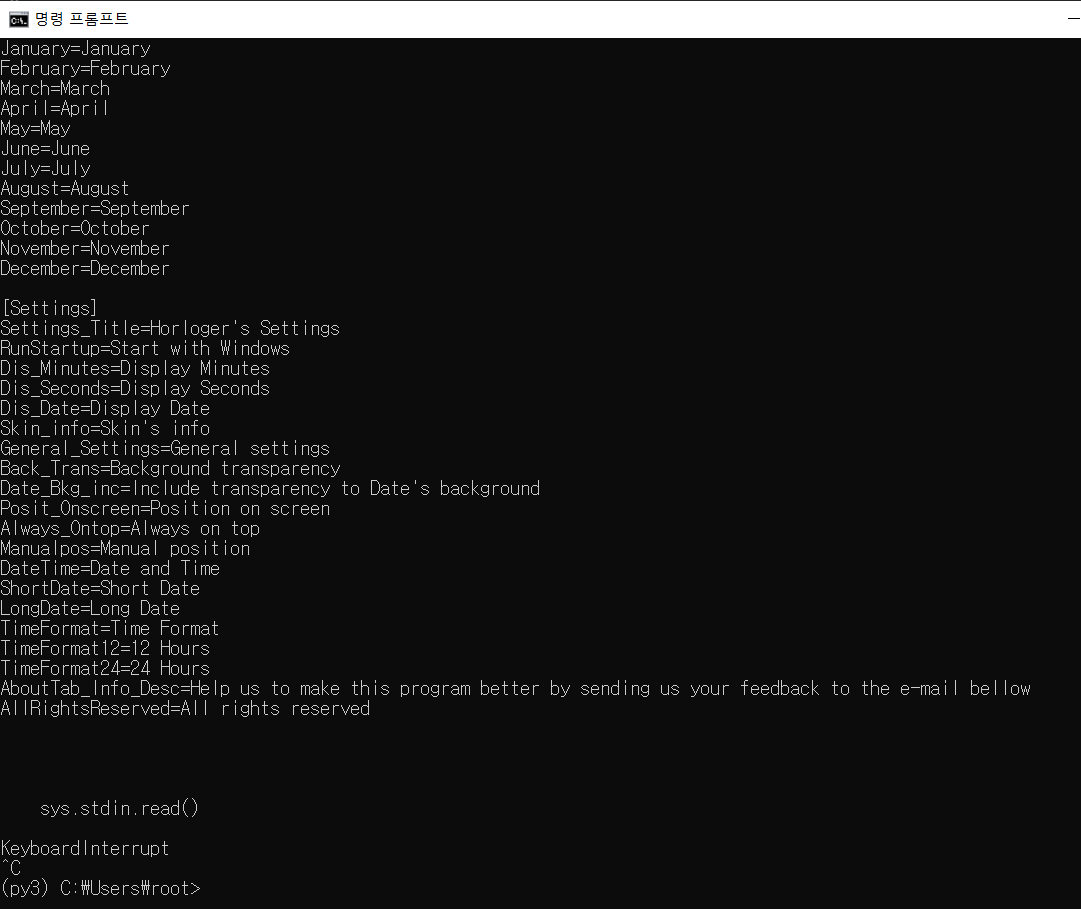
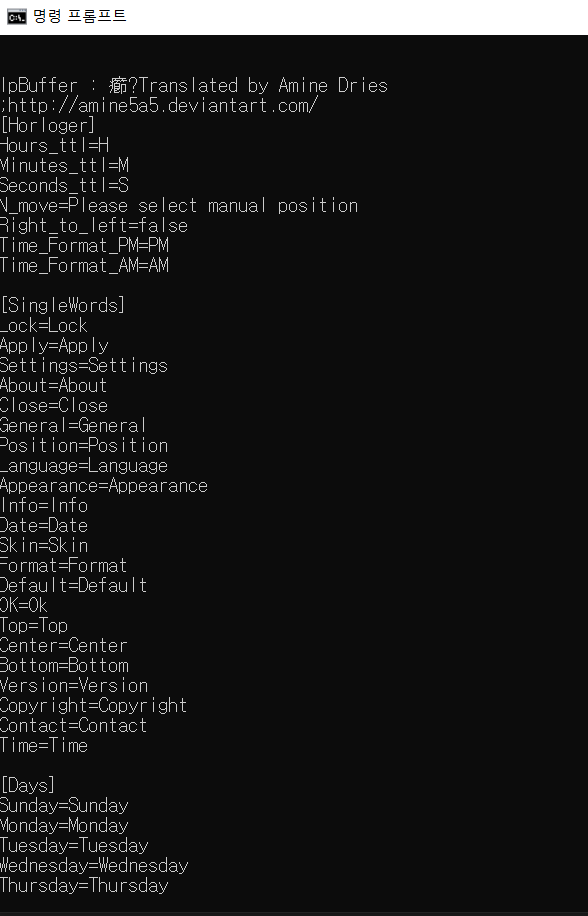
* C:\Program Files (x86)\Amine Dries\Horloger\Lang\English.ini 파일 내부

문득 든 생각:

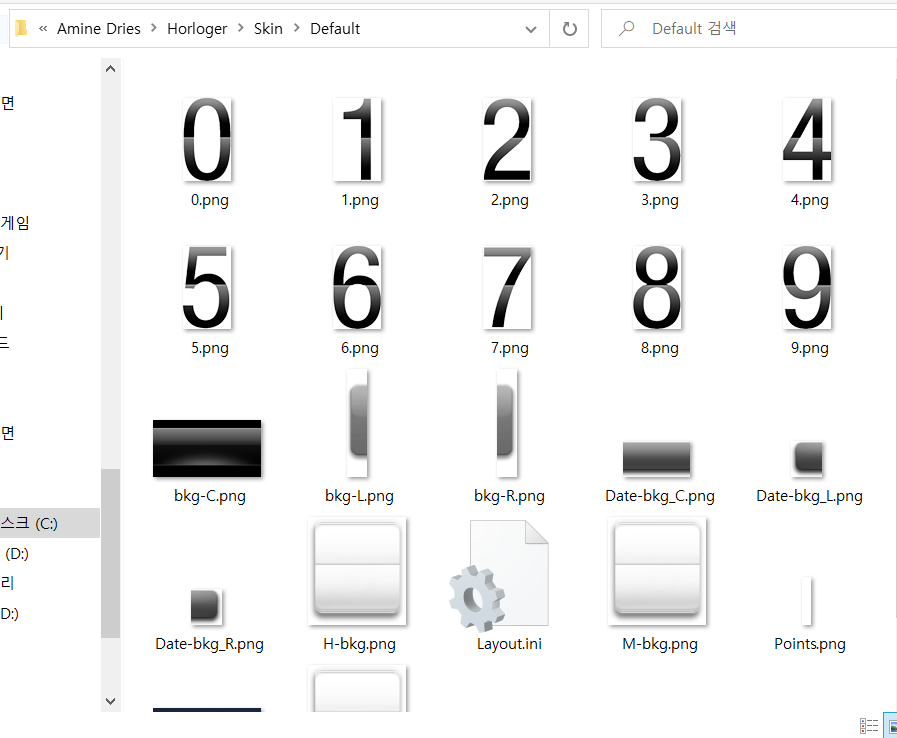
- English.ini 파일에서 뭔가를 계속 ReadFile API로 읽어오는데 저 파일에서 버퍼오버플로우 일어날 수 있지 않을까?

그 전에

ReadFile 후킹해서 뭘 읽어오는지 확인해보자



* C:\Program Files (x86)\Amine Dries\Horloger\Lang\English.ini 이 파일 내용을 계속해서 ReadFile API로 읽음
* **Buffer Overflow 취약점 있을 거 같음**

****

* C:\Program Files (x86)\Amine Dries\Horloger\Skin\Default 내부
* 여기서 이미지 파일 바꾸는 식으로 커스터마이징 가능