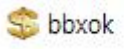
국내 개인정보DB 조회
불법 프로그램 분석 보고서

2023. 10. 23.

목 차

프로그램 정보

프로그램 아이콘 및 이름



(구 버전) bbxok.exe 기준

MD5	9fa041907c4a041d1dc2fe271105ed19
SHA-256	a0116fd6abd5bdff152b3188f88210ff467d42292a7abb128216f86330a9cd8b
File Size	2,592,768 Bytes
File Version	4.0.2020.7
Modified Time	2023-05-15 오전 2:54:14
Created Time	2023-05-31 오후 10:31:49
Extension	exe

Development Language	C/C++
Import	WINMM.dll WS2_32.dll RASAPI32.dll KERNEL32.dll USER32.dll GDI32.dll WINSPOOL.DRV ADVAPI32.dll SHELL32.dll ole32.dll OLEAUT32.dll COMCTL32.dll IMM32.dll WININET.dll comdlg32.dll
Packing/Protector	None
Operation system	Windows
Architecture	i386 , 32bit

동적 분석 (구 버전)

[사진1 - 프로그램 실행 시 화면]

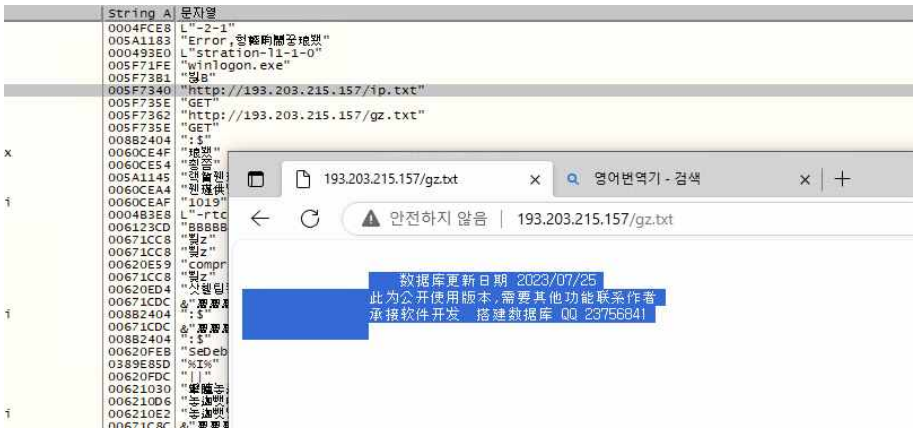
불법 프로그램 내 글자 깨짐 현상(인코딩 문제)을 복구하니 모든 문자는 중국어를 사용하고 있었고, 해당 중국어는 구글 번역기를 이용하여 번역하였고 아래 표를 참고하시면 됩니다.

[탭 메뉴]
1번째 탭 (로그인)
2번째 탭 (등록) : 회원가입으로 추정
3번째 탭 (충전) : 라이선스 등록 추정

구버전으로 로그인 시 최신파일을 다운로드 받으라고 안내하고 정상적으로 동작하지 않습니다.

번역 전	번역 후
点击下载最新版	클릭시 최신버전 다운로드
保存配置	ID , PW 저장
信息	소식 (공지사항)
初始化成功,当前版本不是最新版，不可以登陆!	초기화에 성공했습니다, 현재 버전은 최신판이 아니어서 로그인이 안됩니다!

로그인 및 초기화 수립 과정



[사진2 - Host 주소 및 텍스트 추출]

동적 분석용 디버그 도구인 x96dbg(x32dbg) 프로그램을 이용하여, Host 주소 및 텍스트를 추출한 결과 아래와 같은 텍스트를 추출하였습니다.

■ 추출된 Host 주소 및 텍스트

추출된 Host 주소 및 텍스트	http://193.203.215.157/gz.txt http://193.203.215.157/2.txt http://193.203.215.157/ip.txt http://193.203.215.157/ipok.txt
Request URL	https://api.freeyun.net/gateway.html
IP Address	43.248.190.215:443
Request Line	POST /gateway.html HTTP/1.1
Server	openresty
Host	api.freeyun.net

■ TCP/IP 송수신 수행

로그인 요청	193.203.215.157:9002
Established	122.136.174.68:2008
초기화 (api.freeyun.net)	43.248.190.215:443

■ 주요 함수 주소

버튼 이벤트 함수 프롤로그	bbxok.exe+1495B
로그인 Send 호출	bbxok.exe+14CE2
Recv 받고 분기	bbxok.exe+14CE7
Recv 호출	bbxok.exe+BB820

동적 분석 (신 버전)

[사진3 - 프로그램 실행 시 화면 (신 버전)]

[탭 메뉴]
1번째 탭 (로그인)
2번째 탭 (등록) : 회원가입으로 추정
3번째 탭 (충전) : 라이선스 등록 추정

기존(구 버전)과 동작 방식이 동일하나 로그인 시 정상적으로 이용 가능합니다.

번역 전	번역 후
软件版本	소프트웨어 버전

■ 주요 함수 주소

동적 안티디버깅	bbxok.vmp.exe+FDC5
Error1 - 일치하지 않는 계정	bbxok.vmp.exe+22274
1번째 탭 버튼 이벤트	bbxok.vmp.exe+ECE5
2번째 탭 버튼 이벤트	bbxok.vmp.exe+43DD5
3번째 탭 버튼 이벤트	bbxok.vmp.exe+32F1D
길이 오류 (Length Error)	bbxok.vmp.exe+F564B
로그인 성공 정적 문자열	bbxok.vmp.exe+20066E
성공 문자열 함수	bbxok.vmp.exe+32F1D

결론

로그인 관련 주요 함수와 초기화 과정 TCP/IP 연결 및 송수신 동작을 할 시 전송되는 Data, Host, 관련된 문자열은 추출하였으나 분석이 힘들도록 방해하는 안티 디버깅 기법 등이 적용되어 있어서, 실제 사용이 가능한 라이선스 코드 없이는 메인 파일에 접근이 되지 않아 실질적인 주요 동작(해킹 등의 경로로 유출된 대한민국 국민의 개인정보가 담겨있는 DB로 조회하는 기능 등)은 확인이 불가능 하였습니다.

■ 추출된 프로그램 개발자 연락처

QQ	23756841
Telegram	@areyouok119

끝.