JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 10: 1369~1374, Oct. 2021

중국 안티바이러스 제품 분석을 통한 정보유출 가능성 연구

박원형*

Possibility of Information Leakage through Analysis of Chinese Antivirus Software

Wonhyung Park*

*Associate Professor, Department of Information Security Protection, Sangmyung University, 31066 South Korea

요 약

최근, 중국산 네트워크 장비(화웨이 5G), 앱(틱톡 등) 및 각종 중국산 제품들에 대한 보안 안전성에 대한 논란이 제기되고 있으며, 중국 제품이나 소프트웨어를 사용하는 사람들의 정보를 수집하여 불법적인 사건들이 발생하고 있다. 특히, 2020년 국방부 조사결과에 따르면 해안 경계시스템으로 사용하는 군 감시 장비로 납품 받은 중국산 CCTV에서 악성코드가 발견되어 원격으로 중국 서버로 특정 정보가 전송되는 사고가 발생 하였다. 이러한 중국 보안 제품들의 안전성 문제는 기업이나 개인의 문제보다는 조직적으로 국가에서 주도하는 것을 의심해 볼 수 있다. 본 논문에서는 중국산 안티바이러스 소프트웨어인 360 Total Security(이하 360 TS)에 대한 네트워크 및 프로세스 수준의 분석을 수행한다. 또한, 국산 클라우드 기반 백신 V3 Lite제품과 비교 분석 한다. 이를 통해 중국 보안솔루션의 안전성을 점검하여 정보유출 및 위험성을 제시 한다.

ABSTRACT

Recently, controversy has been raised over the security and safety of Chinese-made network equipment (Huawei 5G), apps (TikTok, etc.). In particular, according to the results of the Ministry of Defense investigation in 2020, malicious codes were found in CCTVs made in China that were delivered as military surveillance equipment used as a coast guard system, and specific information was remotely transmitted to a Chinese server. The safety issues of these Chinese security products can be questioned as being systematically led by the state rather than by companies or individuals. In this paper, we perform network and process level analysis of 360 Total Security(360 TS), a Chinese antivirus software. In addition, it compares and analyzes the domestic cloud-based vaccine V3 Lite product. Through this, the safety of Chinese security solutions is checked and information leakage and risks are suggested.

키워드 : 중국 소프트웨어, 네트워크 분석, 정보유출, 취약점, 360 Total Security

Keywords : Chinese software, Network analysis, Information leakage, Vulnerability, 360 total security

Received 17 August 2021, **Revised** 15 September 2021, **Accepted** 23 September 2021

*** Corresponding Author** Wonhyung Park(E-mail:whpark@smu.ac.kr, Tel:+82-41-550-5301)
Associate Professor, Department of Information Security Protection, Sangmyung University, 31066 South Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.10.1369 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

사용자의 정보를 수집하여 일어나는 불법적인 사건에는 다양한 사례가 있다. 영국의 광고 디지털 기술 회사인 Phorm社는 스파이웨어로 분류되는 프로그램을 배포하고 사용자의 정보 검색 데이터를 광고회사에 판매하여 부당한 이득을 얻었다. 중국의 애플리케이션인 "TicTok"의 중국 버전인 더우인(抖音)은 사용자의 허락 없이 이름, 전화번호, 위치정보 등 개인정보와 같은 데이터를 저장하여 활용한다고 중국 법원에서 판결된 바 있다. 서비스 제공자의 무차별적인 정보 사용 권한을 이용한 악의적인 행동은 사용자는 알아채기 어려우며, 특히 중국에 파견된 사업가, 외교관 등 개인정보 수집으로 인한 치명적인 위험을 유발할 수 있다. 본 논문에서는 위와 같은 사례가 있는지 판단하기 위해 2021년 기준 5억여만 명의 사용자를 보유한 중국의 Qihoo사 백신 360 Total Security(이후 360 TS)를 조사하기로 하였다. 알려진 이슈로 360 TS는 AV Test(바이러스 백신 평가 웹사이트)에서 평가 조작혐의로 퇴출 되었고 수집된 데이터는 불법 악성 마케팅 전략으로 사용되기도 했다. 그리고 360 TS 개인정보 수집 정책은 기존의 타 사의 백신 프로그램 중 가장 많은 45개의 접근 권한을 요구하고 있고 실제 동작과는 전혀 무관한 권한까지 요구한다. 이처럼 360 TS가 어떠한 통신을 하며, 시스템에 어떠한 동작을 하는지 분석하고 의심스러운 기능과 노출된 취약점의 위험성 판단하여 연구를 통해 제시한다[1][2][3].

Ⅱ. 관련 연구

2.1. 360 안티바이러스 S/W (360 TS)

안티바이러스 소프트웨어(antivirus software)란 컴퓨터 바이러스 등 악성코드를 찾아내어 치료 또는 방어를 위한 소프트웨어를 의미한다. '360 TS'는 2014년 중국에 기반을 둔 인터넷 보안 업체 Qihoo사에 의해 개발되어 현재 중국에서 널리 사용되고 있다. 이후 여러 차례 업데이트를 거쳐 다양한 백신, 악성S/W, 맬웨어 방지 보호 기능이 포함된 메인으로 해외 엔진 + 자국산 엔진을 조합한 백신을 사용 한다[4]. 이러한 악성코드를 탐지하고 바이러스를 잡는데 이에 대한 증명으로 AV-TEST 테스트에서 최상위권에 있으며 검사 속도도 비교적 빠른 편으로 속하였다. 하지만 중국 Qihoo사에서 테스트 조작혐의 이후 2017년 10월 AV-TEST 결과에서는 윈도우 기본 안티바이러스 제품인 windows defender보다 못한 결과를 보여 주기도 했다. 그러나 중국 내에서는 2개의 바이러스백신 엔진이 있고 Cloud 기반이라 경량화 제품이기에 인기 있는 보안 솔루션으로 아래 그림 1과 같이 중국의 PC에 일반적으로 무료로 설치하고 널리 사용하고 있다[5][6].

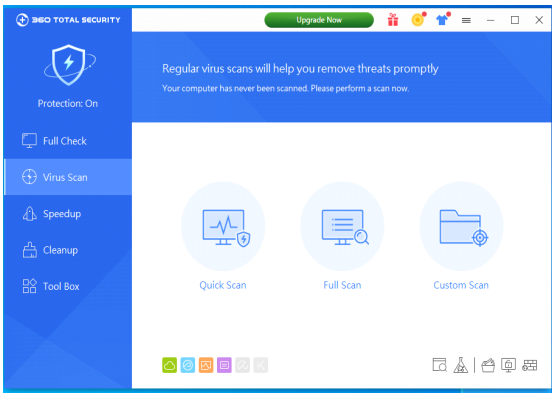

Fig. 1 Run screen of Chinese 360 TS

2.2. 클라우드 기반 탐지

클라우드는 웹에서 다양한 프로그램과 서비스를 사용자가 사용할 수 있도록 구성된 시스템으로 클라우드를 활용하면 네트워크를 통해 대외 서비스를 로컬에서 사용하는 것 처럼 이용 할 수 있다[7][8]. 보안 업체들이 사용하는 클라우드 기술은 보안 업체의 연구, 분석 서버와 다수의 사용자 시스템을 네트워크를 통하여 연결하여 정보를 실시간으로 주고받게 하는 것이다. 일반적인 클라우드 컴퓨팅과의 차이점은 클라우드 컴퓨팅[9]에서는 외부 서비스가 특정 어플리케이션이나 저장 공간을 의미한다. 그러나 클라우드 진단 외부 서비스는 악성코드 진단을 위한 엔진과 DB를 의미한다는 점이다. 여기서 'DB'는 악성코드 정보가 담겨 있는 패턴 정보를 의미하고, '엔진'은 이 DB와 실제 파일 또는 파일 정보를 비교하는 모듈을 의미한다. 쉽게 말해 진단에 필요한 대부분의 기능이 네트워크상에 위치해 있는 것이다. 즉 진단 DB와 진단 모듈이 로컬이 아닌 외부에 있다는 점이 클라우드 진단의 가장 큰 특징이다[10].

Ⅲ. 중국 360 TS 분석 기법

3.1. 분석 환경 및 도구

중국의 360 Total Security 안티바이러스 소프트웨어를 분석하기 위해서 아래 표 1과 같이 기본적으로 분석환경은 윈도우 10에서 가장 최신 버전으로 분석환경을 마련 하였다.

Table. 1 Analysis Environment

Division	Version
OS	Windows 10 pro
360 Total Security	10.8.0.1132
VMware	15.5
Wireshark	3.2.7

또한, 아래 5가지 동적 및 정적 분석 도구를 활용하여 중국 360 제품을 분석 한다.

(1) Wireshark : Network Protocol Analyzer. 네트워크에서 송수신 패킷들을 캡처하여 저장 및 분석을 할 수 있는 도구
(2) Autoruns : 설치한 프로그램 외의 프로그램 탐지하기 위한 도구
(3) Process Monitor : 프로세스 모니터링을 위한 도구
(4) Process Explorer : 특정 프로세스를 직접 찾기 위한 도구
(5) Ghidra : NSA에서 배포한 Decompile 및 DLL 네트워크 연결 확인 도구

3.2. 분석 방법

중국의 360 TS 안티바이러스 소프트웨어제품의 설치 과정부터 업데이트, 자동 스캔, 수동 스캔 등 각 단계에서 동적 분석을 실시하고, 패킷과 파일 등을 동적 분석한다. 또한, 제품 설치 단계에서 사용자가 원하지 않는 프로그램 혹은 기능이 설치되었는지를 파악하고 제품 제거 단계에서 불완전하게 삭제되는 파일이나 이미 삭제하였음에도 남아있는 파일들이 있는지 확인한다. 또한 Decompile을 하여 DLL의 기능을 분석한다.

Ⅳ. 중국 360 TS 분석 및 평가

4.1. 중국 360 TS 엔진 파일 및 주요 기능 분석

중국 360 TS 의 모든 파일을 분석할 수 없으므로 엔진 및 주요 기능과 관련된 파일을 대상으로 아래 표 2와 같이 분석하였다. 해당 파일들은 360 TS 설치 경로의 하위 'deepscan' 폴더 내에 존재하며 엔진 및 검사 관련 실행 파일 및 라이브러리 파일(dll)들 중에 중요 파일을 아래와 같이 선별하였다. 대상 파일들은 크게 QVM 관련, 클라우드 관련, AVIRA 엔진관련, 기본엔진 관련, 검사 및 부가기능 관련으로 분류 하였다.

Table. 2 Engine and Main Function Related Files (Update 30.09.2020, Version 10.8.0.1132)

Division	Filename	Function	Version
QVM	360QVM.dll	QVM Environment	4.0.0.1002
Cloud	cloudcom2.dll	Cloud Engine	3.3.9.3077
	CloudEngine.dll	Cloud Engine	8.0.0.1015
	cloudsec2.dll	Cloud Engine	3.2.8.2151
	Cloudsec3.dll	Cloud Engine	3.3.0.1016
AVIRA Engine	AVEngine.dll	AVIRA Engine	1.0.0.1013
	AVEI.dll	AVIRA Engine	1.0.0.1014
	ImAVEng.dll	AVIRA Engine import	1.0.0.1003
Basic Engine	PopSoftEng.dll	Basic Engine	1.0.0.1003
	pttlnkgkillers.dll	MBR	1.0.0.1021
	qutmload.dll	Quantum DeepScanner	7.2.1.1029
	360Quarant.dll	Quarnt	1.0.0.1002
	360QuarantPlugin.dll	Quarnt Plugin	1.0.0.1001
Inspections and add-ons	DsArk.dll	Full Inspection	1.0.0.1004
	DsExtend.dll	Full Inspection	1.0.0.2002
	DSFScan.dll	Full Inspection	1.0.0.3062
	DSMainUI.dll	Full Inspection UI	8.0.0.1015
	DsSysRepair.dll	Full Inspection	1.0.0.1051
	deepscan.dll	Full Inspection	3.3.0.1030
	BAPI.dll	File, Registry, Basic System Approach	2.0.0.1047
	APKCheck.dll	APK Inspection	1.0.0.1008
	WiFiSafe.dll	WiFi Security	1.0.0.1012
	CheckSM.dll	Integrity Verification	1.0.0.1006
	sysfilerepS.dll	System Filter	7.2.2.2002
	CQhCltHttpW.dll	HTTP	1.0.6.1003

Division	Filename	Function	Version
	softcheck.dll	Installation Verification	5.7.2.2001
	heavygate.dll	DB(sqlite3)	3.7.9.5

주요 기능들이 상호간에 어떠한 식으로 연계되어 있는지 확인하기 위해 주요 파일들의 상호 호출 관계를 정리하였다. 일반적인 정적분석에서 파일간의 상호 호출 관계를 통해 특정 기능을 분석하기 위한 파일들을 분류할 수 있다. 일반적인 S/W의 경우 파일별로 혹은 그룹별도 호출관계가 구분되는 경우가 많으나 360 안티 바이러스의 주요 파일들을 도식화 한 결과는 매우 복잡한 형태로 구성되어 있다. 이렇게 파일간의 상관관계가 복잡한 이유는 (1)안티 바이러스의 경우 모든 기능들이 엔진 및 검사 기능과 연관되어 있는 경우가 많으며, (2) 특히, 360 안티 바이러스의 경우 다수 엔진(기본엔진, QVM 엔진, 클라우드 엔진, AVIRA엔진, BitDefender엔진)으로 구성되어 엔진 및 검사 기능 상호간에 연동되어 구현된 부분이 많기 때문으로 판단된다. 아래 그림 2와 같이 분류된 연관분석 결과, 검사 기능(deepscan.dll) 외 클라우드 엔진 관련 파일(CloudEngine.dll, cloudsec2.dll)들에 호출이 집중되어 있는 것을 확인할 수 있다. 또한 직접적인 'WiFisafe.dll', 'APKCheck.dll', '360Verify.dll' 등 설정 확인 및 기타 기능과 관련된 파일들이 클라우드 엔진을 호출하는 것이 확인되었다. 이는 클라이언트와 서버간의 통신이 클라우드 기능을 통해 이루어지기 때문으로 각각 처리한 데이터를 서버로 전송하기 위해 클라우드 파일을 호출하는 것으로 판단된다.

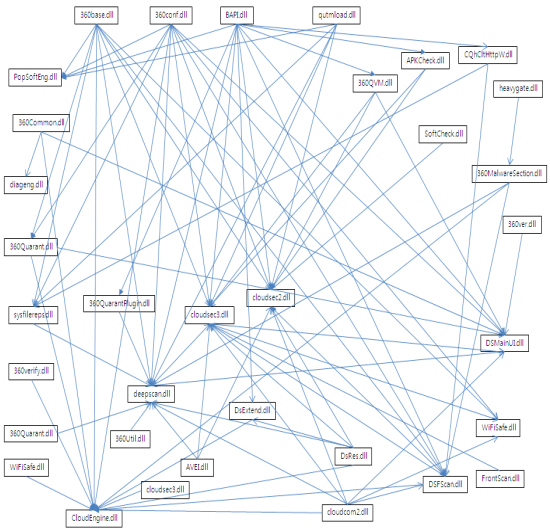

Fig. 2 Correlation Analysis between Key Files

4.2. 동작방식

클라이언트와 서버간에 전송되는 패킷들이 암호화되어 있어 확인이 불가능한 부분이 존재하였기에 실제로 확인되는 패킷 또는 추측 가능한 내용으로 분석 하였다. 클라이언트와 서버 간의 통신은 (1)검사 사전 단계, (2)검사 단계, (3)검사 완료 단계의 3가지 과정으로 분류한다.

(1) 검사 사전 단계 : 클라우드 서버에 접속 가능 여부를 확인하고 추가로 필요한 파일 다운로드, 검사 설정 정보 전송

(2) 검사 단계 : 검사를 진행하는 과정에서 로컬에서 탐지되지 않으나 탐지될 경우 서버로 전송하고 바이러스 여부를 수신

(3) 검사 완료 단계 : 서버에 검사 완료 및 바이러스 탐지 여부 통보

다음 그림 3은 검사 대상 파일 중 추가적인 정보가 필요하거나 로컬 엔진에 정보가 없는 경우 클라우드 서버에 파일정보를 전송하여 서버 DB의 정보 조회하여 다수파일의 정보를 한꺼번에 전송하는 형태로 서버로 전송하여 각 파일의 정보를 클라이언트로 전송하게 된다.

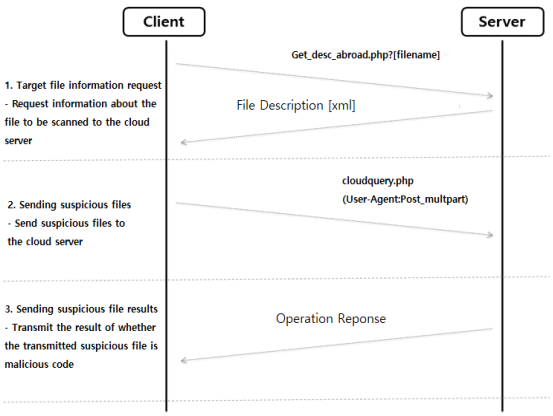

Fig. 3 360 TS Antivirus Scan Steps

아래 그림 4는 클라이언트 PC정보가 클라우드 서버로 허가없이 평문으로 시스템 정보가 유출 되는 것을 확인 할 수 있다.

Fig. 4 Target File Information Request

네트워크에 연결된 상태에서 악성코드 스캔을 하였을 경우 아래 그림 5와 같이 클라우드 서버에 해당 악성코드 가 업로드 되는 것을 알 수 있다. 결국 해당 패킷을 확인해 보면 암호화가 되어 있긴 하지만, 클라우드 서버로 악성코드 로 의심되는 파일이 클라우드 서버로 전송되고 있다.

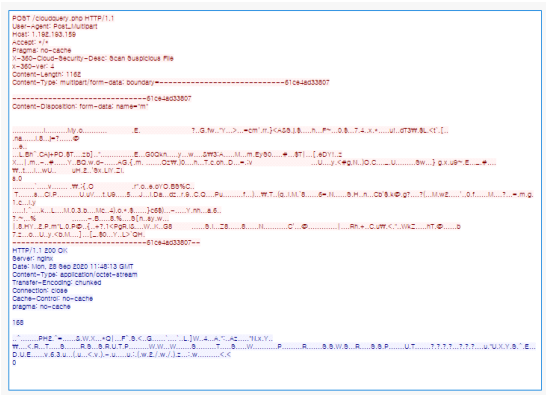

Fig. 5 Suspicious File Transfer

또한, 아래 그림 6은 의심 파일을 전송하는 프로세스로 의심되는 파일이 유출되는 상황이다.

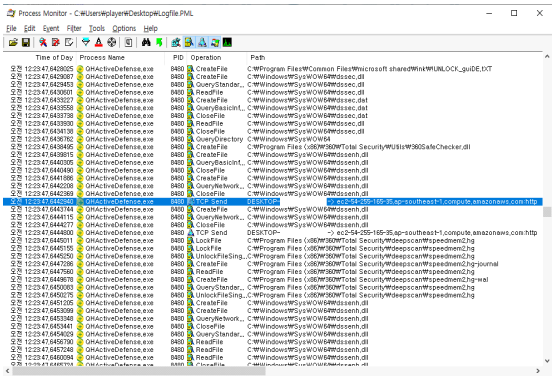

Fig. 6 Suspicious File Transfer Process

4.3. 클라우드 기반 중국 360 TS와 국내 V3 비교 분석

360TS AV와 같은 클라우드 기반 백신 서비스를 제공하는 V3 Lite와 패킷을 비교하여 아래 표 3으로 정리하였다. 360TS AV의 경우, WoTrus라는 기업의 SSL을 적용하여 Data 송수신을 보호한다. 그러나 그림 4를 확인해 보면 수집한 개인정보가 전혀 암호화되지 않은 상태로 노출된다. 하지만 V3 Lite의 경우 네트워크 보안을 위해 헤더에 여러 보안 옵션을 적용하여 안전한 것으로 분석하였다.

Table. 3 Comparison with cloud-based Antivirus Service

Division	360 TS	V3 Lite
Did you apply SSL?	O	O
XSS attack protection possible?	X	O
Data Injection Attack Defence?	X	O
Click jacking attack defense?	X	O
Sniffing attack defense?	X	O

또한, 추가적인 분석 내용으로 헤더 정보에는 CSP (Contents-Security-Policy)와 X-Frame-Options, X-XSS-production, X-Content-Type-Options을 사용하며, CSP는 사용자가 이용하는 웹 페이지의 context에서 악의적인 contents를 실행하게 하는 site 간 scripting (XSS, cross site scripting), code injection 공격을 방어하기 위해 사용되는 것으로 보인다. X-Frame의 경우 iframe 요소와 CSS를 활용하여 공격 대상 사이트를 해킹시도하여 사용자가 모르는 사이에 대상 사이트에 공격을 유도하는 Click jacking 공격을 방어 할 수 있다.

Ⅴ. 결 론

본 논문에서는 중국산 프로그램의 안정성 위험에 있어 백신 프로그램인 360 TS의 분석을 진행하였다. 시스템에서 백신 동작 과정을 확인하기 위해 Ghidra로 정적 분석을 진행하였다. 클라우드 동작 부분과 기본 엔진, AVIRA엔진 부분을 중점적으로 확인을 하였으나, 파일 상관관계가 복잡하여 정확한 과정을 분석하는 데 어려움이 있었다. 국내 클라우드 기반 백신인 V3 Lite와 네트워크 패킷 보안 기능 비교 분석을 하였다. V3 Lite의 경우 보안 관련 헤더와 SSL 적용되어 보안 수준이 높았으나, 360 TS는 신뢰성을 잃은 인증서만 적용되어 보안 수준이 매우 낮았으며, 사용자 정보를 수집하는 부분에서 개인정보 일부가 노출된 상태로 네트워크로 전송되는 과정이 확인 되었다. 본 연구를 통해 360 TS 제품에 여러 의심스러운 동작 및 프로세스가 확인되었으며, 매우 낮은 수준의 네트워크 패킷 보안 체계로 설계되어 있어 정보 노출에 위험이 있다. 특히, 사용자가 중국 360 TS를 설치하고 활용할 때 개인정보 및 보안취약점이 발생할 수 있어 사용자의 주의가 필요하다.

REFERENCES

[1] Do you agree to access location information for banking?. Economy NEWS [Internet]. Available: http://www.m-economynews.com/news/article.html?no=18909.

[2] Malicious Phishing Message Alert. Digital Times [Internet]. Available:.http://www.dt.co.kr/contents.html?article_no=2017032902101560041001.

[3] Chinese Certificate Authority to Ban Google Chrome, Chinese SSL Certificate Authorities, East Security [Internet]. Available: https://blog.alyac.co.kr/782.

[4] J. H. Kim, “A Study on Comparative and Analysis of Malicious Code Detection in Anti-virus Software based on Cloud Computing,” Konkuk University, MS, 2014.

[5] S. H. Kim and J. Yoo, “A Study on Prediction of Malicious Code Infectionin Websites Using Markov Chain,” *Journal of Security Engineering*, vol. 14, no. 1, 2017.

[6] Qihoo 360. namuwiki [Internet]. Available: https://namu.wiki/w/%EC%B9%98%ED%9B%84360.

[7] What is Cloud Diagnostics?. Blog [Internet]. Available: https://arrestlove.tistory.com/351.

[8] J. C. Na and G. P. Kumar, “Quality of Service in Meta Cloud,” *Asia-pacific Journal of Convergent Research Interchange*, vol. 1, no. 3, pp. 53-57, Sep. 2015.

[9] Cloud Computing [Internet]. Available: http://en.wikipedia.org/wiki/Cloud_computing.

[10] V. Sujatha, “Auditing of Storage Security on Encryption TORAGE SECURITY ON ENCRYPTION,” *Asia-pacific Journal of Convergent Research Interchange*, vol. 3, no. 2, Jun, 2017.

박원형(Wonhyung Park)

서울과학기술대학교 공학사, 공학석사 졸업
경기대학교 정보보호학과 이학박사 졸업
성균관대학교 사범대학 교육학박사 수료
호주 타즈매니아대학교 컴퓨터사이언스전공 수료
상명대학교 정보보안공학과 부교수
※관심분야 : 산업보안, 보안관제, 디지털 포렌식