오픈소스기반 악성코드 솔루션 분석

한동진[O], 정소정[*], 김동건[*], 최일영[**], 최상용[*], 이종락[*]
[O]영남이공대학교 사이버보안학과,
[*]영남이공대학교 사이버보안학과,
[**]주식회사 씨에이에스
e-mail: dwdwfe@naver.com[O], sj.jeong323@gmail.com[*], gch02603@gmail.com[*], casciy@casit.co.kr[**],
csyong95@gmail.com[*], jllee@ync.ac.kr[*]

The Analysis for Malicious Code Solution Based on an Open Source

Dong-Jin Han[O], So-Jeong Jeong[*], Dong-Gun Kim[*], Il-Young Choi[**], Sang-Yong Choi[*], Jong-Rak Lee[*]
[O]Dept. of Cyber Security, Yeungnam University College,
[*]Dept. of Cyber Security, Yeungnam University College,
[**]CAS

● 요 약 ●

최근 악성코드의 발전은 사이버 위협의 전방면에 걸쳐 영향을 주고 있다. DDoS, APT를 포함한 스팸 발송 등과 같은 사이버 공격은 악성코드를 기반으로 한다. 또한 이에 대응하기 위해 다양한 형태의 악성코드 솔루션이 존재하고 있다. 악성코드 솔루션은 오픈소스와 상업용 프로그램으로 나눌 수 있는데 상업용 프로그램은 악성코드뿐만 아니라 PC관리의 전반적인 부분을 담당하고 있다. 악성코드를 탐지하는 방법은 시그니처 방식과 해시DB를 이용한 방식 등 다양한 방식이 있다. 본 논문에서는 오픈소스기반 악성코드 솔루션을 비교하여 어떠한 방식이 더 효과적인가를 분석하였다. 이를 통해 악성코드 방지 프로그램을 개발하려는 개발자가 비용효과적인 악성코드 탐지 방법을 잘 선택할 수 있는 가이드라인을 제공한다.

키워드: 악성코드(malicious code), 오픈소스(Open Source), 안티바이러스(Antivirus)

I. Introduction

현대사회는 급속한 정보통신기술의 발전으로 컴퓨터와 인터넷의 보급이 크게 확산됨에 따라 인류가 많은 유익을 얻었지만 이에 따른 사이버공격 역시 급증하고 있다. DDoS공격, 대규모 스팸 발송 등 대부분의 사이버 공격은 악성코드를 통해 발생하고 있다. 최근 인터넷을 통해 악성코드 전문 제작 툴(Malware Construction Kit)이 보급됨에 따라 누구나 자능화된 탐지 회피 기술이 적용된 악성코드를 제작할 수 있게 되었고 그로 인해 신종 악성코드의 수가 급격히 증가하고 있다[1]. 자동화 도구로 제작된 악성코드는 EPO(Entry Point Obscuring)나 암호화 코드 부분만 변경하여 악성 행위는 같으나 겉모습만 바꾸어 백신의 탐지를 피하고 있다. 이러한 다형성 기법의 보편화로 인하여 유사·변종 악성코드가 급증하고 있으며 분석 방해 기법도 진화하는 추세이다[2]. 이렇게 급증하고 있는 대량의 악성코드에 대응하기 위해서는 악성코드 탐지 솔루션이 매우 중요한 의미를 가지고 있다. 악성코드 탐지 솔루션은 진화하는 악성코드에 맞춰 지속적으로 갱신하고, 이를 통해 사전에 대응할 수 있어야 한다.

본 논문에서는 악성코드 확산에 대응하기 위한 오픈소스기반 악성코드 탐지 솔루션의 특성을 조사하고 악성코드 탐지 동작을 비교 분석한다.

II. Preliminaries

1. Related works

1.1 악성코드

악성코드(Malware)란 악의적인 목적을 가지고 제작되어 컴퓨터에 악의적인 영향을 끼치는 모든 소프트웨어의 총칭으로, 이러한 소프트웨어는 사용자의 명령이나 승인 없이 설치되거나 실행되며 시스템의 성능 저하 또는 개인 정보 유출 등의 악의적인 행위를 수행한다. 통신 인프라의 발전에 따라 개인용 컴퓨터의 사용이 증가하면서 악성코드의 감염 방법과 증상들이 다양해지며 전자우편, 메신저,

취약한 사이트 접속 등을 통한 네트워크를 통한 전파가 급격히 증가하였다. 악성코드를 분류하는 기준은 소프트웨어제조사마다 다르다[3],[4]. 하지만 공통적으로 Table.1.과 같이 광고출력, 파일암호화, 정보유출, 좀비, 원격제어 등으로 분류 한다.

Table 1. Malicious Code Classification According To Behavioral Feature

Classification	Explanation
광고출력	사용자가 원하지 않는 광고를 보여주거나 강제로 특정 웹 사이트에 연결한다.
파일 암호화	감염된 PC의 데이터에 접근할 수 없도록 암호화하고, 복호화 비용을 요구한다.
정보유출	사용자나 시스템의 정보를 수집하여 공격자에게 전송한다.
좀비	C&C 서버로부터 명령을 받아 악의적인 기능을 수행한다.
원격제어	특정 포트를 열고 공격자의 명령을 기다린다. 열린 포트를 통해 공격자가 접근하여 시스템을 조종할 수 있다.
가상화폐채굴	사용자 PC의 자원을 이용하여 가상화폐를 채굴하여 공격자에게 가상화폐를 전송한다.

1.2 악성코드 탐지 방법

일반적으로 백신 제품들이 악성코드를 진단하기 위해 사용하는 탐지 기법에는 Hash 기반 탐지 방법, Signature 기반 탐지 방법과 Heuristic 기반 탐지 방법이 있다.

Hash 기반 탐지 방법은 각 파일이 생성됐을때 가지고 있는 고유의 값인 Hash를 이용하여 악성코드에 해시 값을 할당해 해시 값이 변조될 때마다 경고 메시지가 뜨는 형태로 악성코드를 탐지해 사용자에게 경고 메시지를 띄우는 기법이다.

Signature 기반 탐지 방법은 대부분의 백신 제품에 활용되는 기술로 악성코드 분석을 통하여 악성코드의 특징을 추출하고 특정 Signature (≒Pattern)를 데이터베이스로 만든다. 새로운 Signature는 정기적으로 업데이트되며 파일을 스캔할 때, 데이터베이스로부터 Signature와 파일과의 일치 여부를 확인한다. 일반적으로 Signature 기반 탐지 방법은 정확성이 높고 탐지 속도가 빠르나 악성코드 변종에 대한 탐지는 쉽지 않다.

Heuristic 기반 탐지 방법은 시스템의 룰과 패턴을 사용하여 알려지지 않은 악성코드를 탐지하기 위해 사용하는 기법이다. 대부분 백신 제품은 Signature 기반 탐지의 단점을 보조하기 위해 같이 사용한다. Heuristic 기반 탐지 방법은 향상된 탐지 능력과 효율성을 갖게 되지만 탐지속도가 느려지고 오탐률이 커진다[5].

1.3 악성코드 오픈소스 솔루션

오픈소스 기반 악성코드 솔루션을 조사한 바에 따르면 ClamAV, CyberGod, KicomAV, Moon Secure AV등이 있다. 이에 대한 주요특징 및 설명은 다음과 같다.

ClamAV(Clam AntiVirus)는 네트워크 장비로 유명한 시스코 시스템즈에서 지원하는 오픈소스 소프트웨어로 자유 크로스플랫폼 형식의 바이러스 검사 소프트웨어 툴킷이다. 주된 목적 가운데 하나는 서버 측면의 전자 메일 바이러스 검사기의 역할을 하면서 메일 서버에 이용하는 것이다[6].

Fig. 1. ClameAV

CyberGod KSGMPRH은 성능저하없이 주요 안티바이러스를 우선 순위 예약을 기반으로 탐지하는 오픈소스로 중복파일제거, 손실된 파일 복구기능을 제공한다[7].

Fig. 2. CyberGod AV

KicomAV는 악성코드를 검출하고 제거할 수 있도록 설계된 오픈소스(GPL v2) 안티바이러스 엔진이다. 실제로 1995년부터 C/C++로 작성되어 1998년 HAURI의 ViRobot 엔진에 통합되었다[8].

Fig. 3. Kicom AV

Moon Secure AV는 현재 ClamAV 엔진을 사용 하는 오픈 소스 소프트웨어로 Net Shield, 방화벽, On access, Exec 스캐너 및 루트킷 방지 기능을 제공한다[9].

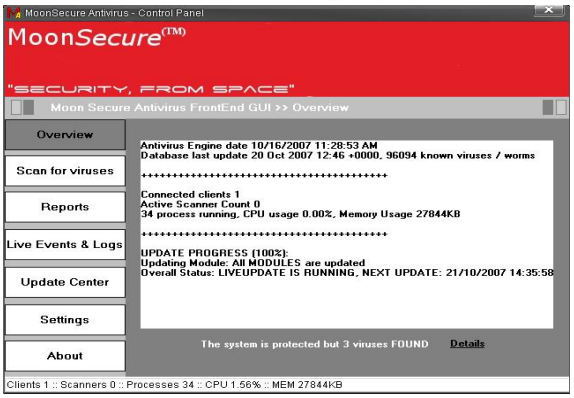

Fig. 4. Moon Secure AV

III. The Analysis of Malicious Code Solution Based on an Open Source

이번 장에서는 앞서 언급한 4개의 오픈소스 기반 악성코드 탐지 솔루션의 성능을 비교하였다. 비교를 위해 인터넷에서 수집한 100개의 악성코드를 이용하여 5회 이상의 동일한 실험을 통해 평균 값을 구하는 방식으로 진행하였다. 성능비교의 내용은 탐지속도와 탐지개수이다.

Table 2. Malicious code detection method

종류	Signature 기반	Pattern 개수	Database 기반	Hash 개수
Clam AV	O	-	O	1,300,000
Cyber God			O	420,000
Kicom AV	O	50		
Moon secure			O	370,000

먼저, 4개의 악성코드 탐지 솔루션의 탐지기능을 분석하였다. 오픈소스기반 악성코드 탐지솔루션의 탐지 기능은 크게 2가지로 나누어진다. Signature기반은 악성코드의 파일에 포함된 특징을 기반으로 탐지하는 방법이며 Database 기반 탐지방법은 알려진 악성코드의 해시값을 보유하고 있으며, 이를 기반으로 탐지하는 방법이다. 분석결과 Table 2. 와 같이 각각의 솔루션들이 Signature기반 탐지와 Database기반 탐지 방법으로 사용하고 있으며 각각의 패턴과 Database안 Hash값의 개수를 확인할 수 있다.

검증을 위해 동일한 컴퓨터 환경에서 가상머신을 활용하여 악성코드 솔루션이 실행되는 환경을 구축하였으며, 탐지속도와 탐지개수를 기준으로 실험하였다. 이는 악성코드 탐지 솔루션은 빠른 탐지가 우선되어야 하며, 이와 함께 정확한 탐지, 많은 악성코드 탐지가 병행되어야 하며, 이 두 가지 측면이 반비례의 관계에 있으므로 실험기준으로 적절하다.

실험 결과 Signature 패턴과 Database Hash값 개수에 따라 악성코드 탐지속도와 탐지개수의 차이를 확인할 수 있다. 먼저 탐지속도 측면에서는 KicomAV가 평균 3초로 가장 빠른 탐지속도를 보이고 있으며, 탐지개수 측면에서는 ClamAV가 가장 많은 탐지수를 보이고 있다. KicomAV가 가장 바른 이유는 한가지 방식(시그니처 방식)을 사용하고 있으며, 가장 최근까지 업데이트가 되고 있는 잘 관리되는 엔진이기 때문으로 분석된다. ClamAV는 100개의 악성코드 중 64개의 악성코드를 탐지하였으며, 이는 ClamAV의 경우 두 가지 방식 모드를 사용하고 업데이트 또한 최근까지 잘 이루어지고 있기 때문인 것으로 분석된다. 하지만 ClamAV는 속도 측면에서 가장 느린 속도를 보이고 있다. 특이한 점은 CyberGod AV가 Moon Secure AV대비 해시DB가 많지만 탐지개수에서는 Moon Secure가 앞서고 있다. 이는 단지 해시의 수 뿐만 아니라 가장 유행하는 악성코드의 해시를 얼마나 많이 보유하고 있는가가 중요한 요소로 작용하고 있다는 것을 보여준다.

실험결과를 종합하여 보면, 다양한 탐지방법을 활용하고 많은 DB를 보유하고 있으면, 탐지 수가 상대적으로 높게 나타나지만 속도 측면에서는 반대의 경향이 나타나고 있다. 따라서 백신 소프트웨어를 개발할 때에는 탐지 수와 속도 측면에서 적절한 조절이 필요할 것으로 판단된다.

IV. Conclusions

신종 악성코드와 변종 악성코드의 증가에 따라 기존의 악성코드 탐지 솔루션이 탐지 못 하는 영역이 늘어나고 이에 대한 보완이 요구되고 있다.

Table 3. Malicious code Detection test

종류	속도 (s)					탐지개수					평균	
	1	2	3	4	5	1	2	3	4	5	속도	개수
ClamAV	90	150	346	114	175	64	64	64	64	64	175	64
CyberGod AV	30	5	5	5	5	1	1	1	1	1	10	1
KicomAV	5	2	2	2	2	0	0	0	0	0	3	0
Moon secure AV	12	9	8	8	8	31	31	31	31	31	9	31

본 연구는 급증하고 있는 다양한 악성코드를 탐지하는 오픈소스 솔루션을 비교분석하기 위해 100여개의 파일을 바이러스토탈을 통해 악성코드임을 확인하고 종류별로 분류하였다. 이 악성코드를 기반으로 각각의 탐지 솔루션들의 기능과 구성을 분석 결과 하나의 탐지 방법을 구성하고 있는 솔루션보다 Database 기반 탐지 방법과 Signature 기반 탐지 방법이 함께 적용된 솔루션이 탐지율이 높은 결과를 얻을 수 있었다.

REFERENCES

[1] Boannews. “Malicious code development”, *https://www.boannews.com/media/view.asp?idx=18406,* (2020.06.03)

[2] ITFIND. “Malicious code analysis”, *https://www.itfind.or.kr/m/local/main/themeView.htm;jsessionid=593473D09156861AC0B04723D108696D.tomcat_itfind2?identifier=02-006-150121-000004&page=553&pageSize=10* (2020.06.03)

[3] Ahnlab, *https://www.ahnlab.com/*

[4] Estsoft, *https://www.estsoft.co.kr/*

[5] HAURI, "Malicious code detector method“, *https://hauri.co.kr/security/issue_view.html?intSeq=93&page=21&article_num=92* (2020.06.08)

[6] WikipediA, "Clam AntiVirus", *https://en.wikipedia.org/wiki/Clam_AntiVirus* (2020.06.08)

[7] GitHub, "CyberGod-KSGMPRH", *https://github.com/VISWESWARAN1998/CyberGod-KSGMPRH* (2020.06.08)

[8] KICOM Anti-Virus, *http://www.kicomav.com/*

[9] MoonSecureAntivirus, *http://moonsecure.net/df/*