행위기반 악성코드 프로파일링 시스템 프로토타입

강홍구*, 유대훈*, 최보민*
*한국인터넷진흥원
e-mail:redball@kisa.or.kr

Behavior based Malware Profiling System Prototype

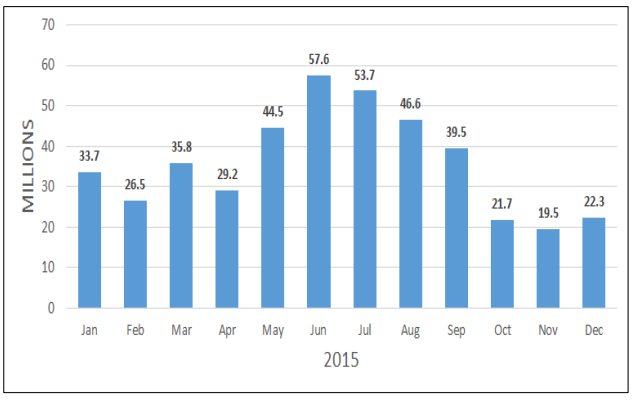
Hong-Koo Kang*, Bo-Min Choi*, Dae-Hoon Yoo*
*Korea Internet & Security Agency

요 약

전 세계적으로 악성코드는 하루 100만개 이상이 새롭게 발견되고 있으며, 악성코드 발생량은 해마다 증가하고 있는 추세이다. 공격자는 보안장비에서 악성코드가 탐지되는 것을 우회하기 위해 기존 악성코드를 변형한 변종 악성코드를 주로 이용한다. 변종 악성코드는 자동화된 제작도구나 기존 악성코드의 코드를 재사용하므로 비교적 손쉽게 생성될 수 있어 최근 악성코드 급증의 주요 원인으로 지목되고 있다. 본 논문에서는 대량으로 발생하는 악성코드의 효과적인 대응을 위한 행위기반 악성코드 프로파일링 시스템 프로토타입을 제안한다. 동일한 변종 악성코드들은 실제 행위가 유사한 특징을 고려하여 악성코드가 실행되는 과정에서 호출되는 API 시퀀스 정보를 이용하여 악성코드 간 유사도 분석을 수행하였다. 유사도 결과를 기반으로 대량의 악성코드를 자동으로 그룹분류 해주는 시스템 프로토타입을 구현하였다. 악성코드 그룹별로 멤버들 간의 유사도를 전수 비교하므로 그룹의 분류 정확도를 객관적으로 제시할 수 있다. 실제 유포된 악성코드를 대상으로 악성코드 그룹분류 기능과 정확도를 측정한 실험에서는 평균 92.76%의 분류 성능을 보였으며, 외부 전문가 의뢰에서도 84.13%로 비교적 높은 분류 정확도를 보였다.

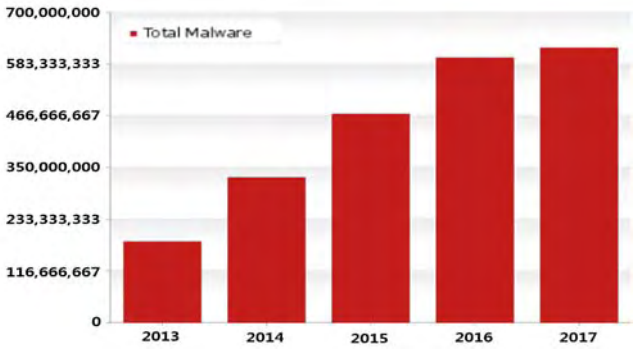
1. 서론

글로벌 보안업체인 시만텍에 따르면, 2015년에 약 4.3억 개의 새로운 악성코드가 발생한 것으로 나타났다. 이는 2014년도 대비 35% 이상 증가한 것으로 일평균 약 118만 개의 새로운 악성코드가 발생되고 있음을 의미한다.[1].



(그림 1) 신규 악성코드 증가 추이(시만텍, 2016)

이러한 악성코드 발생량은 매년 급증하고 있는 추세이다. 대표적인 보안제품 테스트 기관인 AV-TEST에 따르면, 2016년에 약 6억 개의 악성코드가 발생되었는데, 2017년 1분기에만 이미 6억 개를 넘어선 것으로 보고되고 있다[2]. 이러한 악성코드 급증의 원인 중 하나로 전문가들은 변종의 급증에 주목하고 있다. 공격자는 보안장비에서 악성코드 탐지를 우회하기 위해 기존 악성코드를 변형한 변종 악성코드를 주로 이용한다. 이는 새로운 악성코드를 개발하는 것의 비용이 상대적으로 높고, 매번 새로운 악성코드를 만들기 쉽지 않기 때문에 비용대비 공격 성공율이 높은 변종을 선택할 가능성이 높기 때문이다. 최근에는 악성코드를 자동으로 제작하는 도구가 등장하면서 전문적인 해커가 아니더라도 손쉽게 다양한 기능을 갖춘 악성코드를 대량으로 생성, 유포할 수 있는 환경이 되고 있다[3].



(그림 2) 악성코드 증가 추이(AV-TEST, 2017.3월)

현재 악성코드를 탐지하고 분류하기 위한 여러 연구가 진행되고 있다. Xin Hu는 악성코드의 Call flow Graph 간

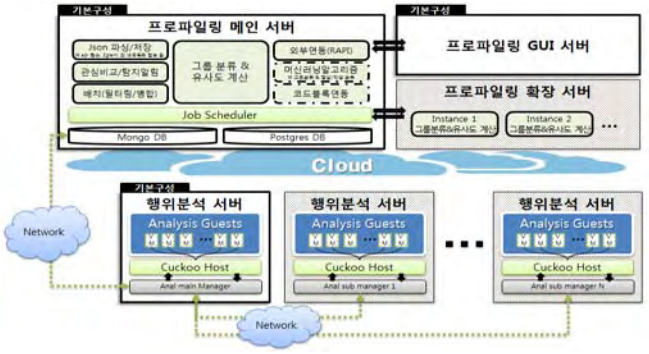
의 유사도 분석을 통해 분류하였고[4], M. Alazab은 API 호출에 대한 통계정보로 유사도를 측정하였다[5]. 이들 연구는 정적 분석을 기반으로 하고 있어 비교적 빠른 악성코드 분류가 가능하나 패킹이나 난독화된 악성코드 분석에는 한계를 보였다. L. Wu는 악성코드가 호출하는 API 시퀀스를 정규표현식으로 변환하여 유사도를 분석하였고[6], Natani와 Pratiksha는 악성코드의 API 호출빈도를 분석하였다[7]. 이들 연구는 동적 분석을 기반으로 하고 있어 패킹이나 난독화된 악성코드 분석이 가능하나, 일부 행위 특징만을 분석대상으로 하고 있고, 악성코드의 API 호출빈도 차이가 클수록 정확도가 떨어지는 한계가 있다.

본 논문에서는 대량으로 발생하는 악성코드의 효과적인 대응을 위한 행위기반 악성코드 프로파일링 시스템 프로토타입을 제안한다. 악성코드를 자동으로 제작하는 도구나 기존 악성코드의 코드를 재사용하는 동일한 변종 악성코드들은 실제 행위가 유사한 특징을 가지고 있다. 이러한 변종의 특징을 고려하여 악성코드가 실행되는 과정에서 호출되는 API 시퀀스 정보를 이용하여 악성코드 간의 유사도를 분석하고, 이러한 유사도를 기반으로 악성코드 그룹을 자동으로 분류하는 시스템 프로토타입을 구현하였다.

악성코드 그룹별로 멤버들 간의 유사도를 전수 비교하므로 그룹의 분류 정확도를 객관적으로 제시할 수 있는 장점이 있다. 실제 유포된 악성코드를 대상으로 악성코드 그룹분류 기능과 정확도 측정 실험에서는 평균 92.76%의 분류 성능을 보였으며, 외부 전문가 의뢰에서도 84.13%로 비교적 높은 분류 정확도를 보였다. 제안하는 시스템 프로토타입은 3.20, 6.25 등 북한발 사이버 테러와 같이 주요 사이버 공격에 사용된 악성코드와의 변종을 빠르게 식별, 제시할 수 있어 신속한 침해사고 대응에 활용될 수 있을 것으로 기대된다.

2. 행위기반 악성코드 프로파일링 시스템 프로토타입

본 논문에서 제안하는 행위기반 악성코드 프로파일링 시스템 프로토타입은 (그림 3)과 같다.



(그림 3) 행위기반 악성코드 프로파일링 시스템 프로토타입 구조

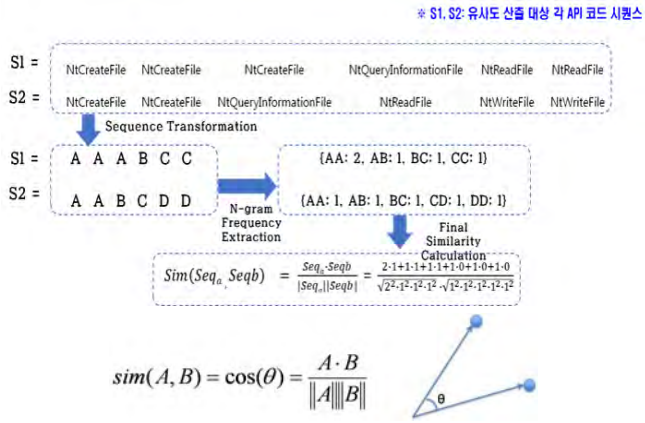
(그림 3)에서 보는 것과 같이 제안하는 시스템 프로토타입은 악성코드가 실행되는 과정에서 호출하는 API 시퀀스 정보를 추출하는 행위분석 서버, API 시퀀스 정보를 정규화하여 악성코드 간 유사도를 측정하고, 유사도를 기반으로 악성코드 그룹을 분류하는 프로파일링 서버, 악성코드 그룹분류 결과를 관리하고 시각화하는 프로파일링 GUI 서버로 구성된다.

행위분석 서버는 비교적 안정성이 높은 것으로 알려진 Cuckoo Sandbox[8]를 이용하여 악성코드를 자동 실행하고 실행과정에서 호출되는 API 시퀀스 정보를 추출한다. Cuckoo Sandbox에서 추출하는 API 종류는 169개이며 유형별로 호출빈도를 측정한 결과는 <표 1>과 같다. 또한, 대량의 악성코드 처리를 위해 서버당 10개의 GuestOS를 설치하고 여러개의 서버로 확장이 가능하도록 설계되었다.

<표 1> API유형별 호출빈도

API유형	호출빈도	비율
registry	37,973,055	52.820%
system	13,753,337	19.131%
filesystem	11,786,560	16.395%
process	5,947,942	8.273%
misc	810,270	1.127%
synch	414,308	0.576%
socket	393,847	0.548%
threading	315,836	0.439%
windows	207,982	0.289%
device	151,620	0.211%
services	69,806	0.097%
network	58,870	0.082%
anomaly	6,100	0.008%
hooking	1,984	0.003%

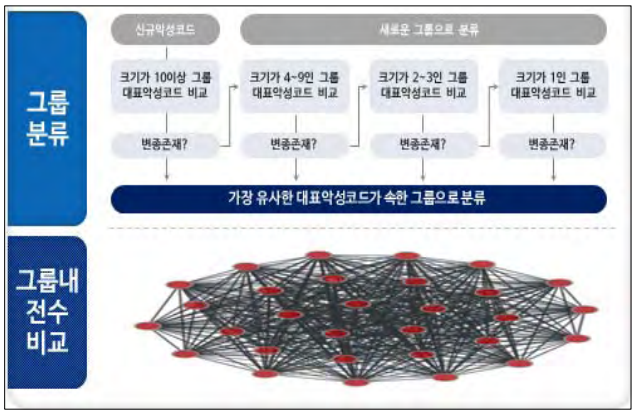
프로파일링 메인 서버는 동종 변종들의 실제 행위가 유사한 특징을 고려하여, 행위분석 서버에서 추출한 API 시퀀스로부터 주요 행위정보인 호출순서와 빈도를 동시에 분석이 가능한 N-gram 기반 유사도 측정 알고리즘을 이용하여 악성코드 분류를 수행한다.



(그림 4) N-gram 기반 유사도 측정

우선 악성코드가 실행되는 과정에서 추출된 API 시퀀스를 정규화하고, N을 선별하는 실험을 거쳐 2-gram으로 행위정보를 생성한다. 다음으로 Cosine Similarity 알고리즘을 이용하여 악성코드 간 유사도를 산출하였다. (그림 4)는 API 시퀀스 정보를 정규화하고 호출순서와 빈도를 2-gram 기반으로 생성하여 Cosine Similarity 알고리즘을 적용한 과정을 보여준다.

프로파일링 메인 서버는 악성코드 유입시, 축적된 악성코드와 전수비교가 아닌 그룹별 대표 악성코드와 비교를 수행한다. 왜냐하면 대규모 악성코드 축적환경에서 모든 악성코드와 전수 비교는 시간비용상 매우 비효율적이며 대상이 계속 증가할 수록 거의 불가능해지기 때문이다. 그룹별 대표 악성코드는 해당 그룹내 전체 멤버들과 가장 높은 평균 유사도를 갖는 멤버로 선택된다. 그룹분류의 속도와 정확도를 높이기 위해 멤버수가 많은 그룹부터 비교하여 소속될 그룹을 찾고, 해당 그룹내 멤버와 전수비교를 수행한다. 또한, 주기적으로 그룹내 연관도가 낮은 멤버를 필터링하는 과정을 수행한다. 그리고, 프로파일링 서버는 행위분석 서버와 마찬가지로 대량의 악성코드 처리를 위해 여러개의 서버로 확장이 가능하도록 설계되었다.



(그림 5) 그룹분류 처리과정

마지막으로 프로파일링 GUI 서버는 악성코드 그룹분류 현황과 그룹내 세부정보를 관리하고 시각화하는 기능을 제공한다.

(그림 6) 악성코드 그룹 전체 현황

(그림 6)은 시스템에서 분류된 악성코드 그룹의 전체 현황을 보여준다. 특정 기간에 생성되거나 업데이트된 악성코드 그룹 현황과 그룹별 정확도, 그룹의 멤버 개수가 높은 Top 5 정보를 확인할 수 있다. (그림 7), (그림 8)은 각각 선택된 악성코드, 악성코드 그룹의 세부정보를 보여준다. 악성코드 세부정보로 SHA -256, 수집일, 백신 진단명, 동일 그룹내 멤버간 유사도 정보를 보여준다. 그룹내 멤버간 유사도는 직관적인 시각화를 제공하고 있으며, 중앙에 선택된 악성코드를 중심으로 유사도가 높을수록 진한 색상과 짧은 거리차를 갖도록 되어 있다. 멤버 개수가 많아져도 크기가 자동적으로 조절되도록 구현하였다. 악성코드 그룹은 그룹생성일, 멤버 개수, 대표 악성코드, 그룹내 멤버간 평균 유사도 등을 보여준다. 대표 악성코드는 개수를 관리자가 조정할 수 있으며, 그룹내 멤버간 평균 유사도는 그룹분류 신뢰도를 나타낸다.

(그림 7) 선택 악성코드 대상 타 멤버와의 연관성 시각화

(그림 8) 특정 그룹에 대한 세부정보

3. 성능 실험결과

행위기반 악성코드 프로파일링 시스템 프로토타입의 성능 측정은 그룹분류 기능과 정확도에 대해서 수행하였다. 악성코드 그룹분류 기능 실험에 사용된 악성코드는 10,699개로 malwares.com[9]에서 실제 유포에 사용된 샘플을 제공받았다. 그룹내 변종관계 측정의 산출식은 다음과 같다.

$$\text{전체 변종관계 멤버수} = \sum_{\text{생성그룹}1}^{\text{생성그룹}N} \frac{\text{그룹내 변종관계 멤버수}}{\text{그룹내 멤버수}}$$

그룹내 변종관계 멤버평균 =

$$\left(\left(\sum_{\text{생성그룹1}}^{\text{생성그룹}N} \frac{\text{그룹내 변종관계 멤버 수}}{\text{그룹내 멤버 수}}\right)/N\right)\times 100$$

실험결과, 총 10,699개 악성코드 중 8,978개(83.9%)에서 변종관계를 식별(유사도 임계치 : 98% 기준)하였다. 나머지 1,721개(16.1%)에서는 변종관계 악성코드가 발견되지 않았으나, 실험상 설정된 임계치가 다소 높은 수준이므로 유사도 임계치를 조정함에 따라 변종관계 악성코드 비율을 다소 변동될 수 있다. 특히, 멤버수 10개 이상인 그룹은 변종관계인 멤버가 평균 92.8%로 높게 나타났다.

멤버개수 10개 이상인 그룹 대상 멤버개수 및 변종비율

그룹구분(멤버수 기준)	그룹개수	총 멤버개수	평균변종비율
1,000개이상	1	1,085	99.61%
500개이상	2	1,682	96.05%
100개이상	10	2,131	94.24%
50개이상	12	862	95.26%
10개이상	87	1,650	92.10%
합계	112	7,410	92.76%

(그림 9) 그룹분류 기능 검증

그룹분류 정확도에 대한 실험은 주요 침해사건과 관련된 악성코드와 랜덤한 악성코드를 모두 대상으로 시스템에서 분류하는 방식으로 진행하였고, 분류 결과를 외부 분석 전문가에 의뢰하여 성능을 검증하였다. 3.20, 금융탈취형, 랜덤선별 등 6개 유형의 악성코드 샘플을 대상으로 시스템에서 그룹분류를 수행하였다. 시스템에는 이미 6개 유형의 악성코드 샘플을 포함하여 랜덤한 악성코드 2.639개가 저장되어 있는 환경이다. 악성코드 그룹분류 정확도 산출식은 다음과 같다.

악성코드 그룹분류 정확도 =

$$\left(\left(\sum_{\text{검증대상1}}^{\text{검증대상}N} \frac{\text{전문가가 변종으로 탐지한 개수}}{\text{시스템에서 변종으로 탐지한 개수}}\right)/N\right)\times 100$$

검증대상			시스템 탐지변종	전문가 판정	
구분(SET)	MD5	출처(KISC)	탐지 변종수	변종판정 개수	변종탐지율
1	77eb…	3.20악성코드	4	4	100.00%
2	76a7…	3.20악성코드	3	3	100.00%
3	F235…	금융탈취형	5	5	100.00%
4	0fda…	랜덤선별	7	5	71.43%
5	426d…	랜덤선별	3	1	33.33%
6	5447…	랜덤선별	14	14	100.00%
평균 탐지율					84.13%

(그림 9) 그룹분류 정확도 검증

실험결과 시스템에서 6개 유형의 악성코드 샘플에 대해 2,636개 중에서 변종관계로 36개를 식별하고 그룹으로 분류하였다. 시스템에서 분류한 결과에 대해서 외부 전문가에 분석을 의뢰하였고, 36개 악성코드 중 32개(84.13%)가 변종으로 판별된 것으로 나타났다.

4. 결론 및 향후연구

사이버 침해사고의 주요 원인인 악성코드가 지속적으로 급증하고 있어 경제적, 사회적인 측면에서 막대한 피해가 발생하고 있다. 사이버 침해사고를 신속하고 효과적으로 대응하기 위해서는 대량의 악성코드 중에서 우선분석 대상을 선별하여 조치하는 것이 필요하다. 본 논문에서는 주요 침해공격에 사용되는 악성코드의 변종공격을 자동으로 탐지하고 분류할 수 있는 행위기반 악성코드 프로파일링 시스템 프로토타입을 제안하였다.

동일한 변종은 실제 행위가 유사한 특징을 가지므로, API 시퀀스 정보를 추출하여 악성코드 간 유사도 분석을 통해 자동으로 그룹분류를 수행하였다. 실험을 통해, 제안하는 시스템의 기능과 정확도가 우수함을 보였다. 향후에는 수만~수십만 이상의 악성코드를 대상으로 처리 성능을 검증하고 안정성을 보완하여 상용수준의 시스템화를 진행하고, 기존 악성코드 그룹분류 기술들과의 성능비교를 수행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (2016-0-00081, 악성코드 전 생명주기 통합 프로파일링 및 공격그룹 식별 기술 개발)

참고문헌

[1] Symantec, 인터넷 위협 동향 보고서(ISTR), 2016
[2] AV-TEST, https://www.av-test.org/en/statistics/malware/
[3] 강홍구, 최보민, 유대훈, 이태진, 행위기반 악성코드 분류 시스템 성능분석 연구, 정보보호학회 동계학술대회, 2016
[4] Xin H, Tzi-cker C, Shin Kang G, Large-scale Malware Indexing using Function-call Graphs, CCS 2009
[5] Alazab M et al, Towards Understanding Malware Behaviour by the Extraction of API Calls, CTC 2010
[6] Wu L et al, Behavior-based Malware Analysis and Detection, IWCDM 2011
[7] Pratiksha N, Deepti V, Malware Detection using API Function Frequency with Ensemble Based classifier, Security in computing and communications, 2013
[8] Cuckoo Sandbox, https://www.cuckoosandbox.org/
[9] Malwares.com, https://www.malwares.com/