제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

악성 코드 정의를 위한 속성 연구

박민우*, 서상욱**, 정태명*
*성균관대학교 전자전기컴퓨터공학과
**한국인터넷진흥원
e-mail:mwpark@imtl.skku.ac.kr, swseo@kisa.or.kr,
tmchung@ece.skku.ac.kr

A Study on Attributes to Define Malware

Min-Woo Park*, Sangwook Seo**, Tai-Myoung Chung*
*Dept of Electrical and Computer Engineering, Sungkyunkwan Univ.
**Korea Internet & Security Agency

요 약

악성코드의 수가 급격히 늘어나면서, 최근에는 하루에도 수 만개의 신·변종 악성코드가 쏟아져 나온다. 악성코드로 인한 국내 피해를 줄이기 위해 한국인터넷진흥원에서는 신·변종 악성코드를 즉각적으로 분석하고 분석 결과를 공유하기 위해 노력하고 있다. 하지만 악성코드를 정의하고 분류하는 방침에 있어서 표준화된 규칙이 없어 악성 코드 분석 결과를 공유하는 대에 어려움이 따른다. 본 논문에서는 현재의 악성코드 정의 및 분류 방안에 대한 한계점을 개선하기 위해 악성-속성을 규정하고 이를 이용한 악성 코드 정의 및 분류 방안에 대해 제시한다.

1. 서론

인터넷 경제 규모가 증가하고, 관공서나 기업 등에서 대량의 고객 정보들을 전산화 하여 취급하게 되면서 이를 노린 각종 범죄가 성행하게 되었다. 특히 악성코드를 이용한 사이버 범죄의 수와 규모가 크게 증가했다. 과거의 악성코드는 주로 자신의 우월함을 다른 사람에게 알리기 위해서나 장난스런 목적으로 만들어졌다. 하지만 최근에는 특정 정보 탈취를 목적으로 제작되거나 타인의 서비스를 방해하기 위한 뚜렷한 목적을 가지고 만들어지고 있다. 이에 따라 악성코드의 행동은 목표를 달성하기 위해 점차 복잡해지고 공격 방법은 더욱더 치밀해지고 있다.

독일에 AV-test의 보고에 따르면 신·변종 악성코드의 출현하는 숫자는 해마다 늘어나고 있으며, 특히 2010년에는 평균적으로 하루에 4만개가 넘는 신·변종 악성코드가 발생하였다[1]. 이러한 악성코드들로부터 국내 인터넷 환경을 보호하기 위해 민간 기업과 정부 기관에서 악성코드 분석 및 정보 공유를 위해 많은 노력을 쏟고 있다. 특히 한국인터넷진흥원은 신·변종 악성코드에 대해 분석하고 그 분석 결과를 다른 민간 안티바이러스 관련 기관에 공유하는 등 악성코드의 탐지 및 피해 최소화를 위해 앞장서고 있다. 하지만 각 기관별로 악성코드 자체에 대한 명기 방법이 서로 상이하며, 악성코드를 분류하는 기준이 일정하지 않다. 그 결과 각 기관별 정보를 공유하는 대에 어려움이 따른다.

본 논문에서는 악성코드를 구분하기 위한 악성-속성(Mal-Attribute)을 제안한다.

본 논문의 구성은 2장에서 기관별 악성코드 분류 기분에 대해 기술하고 3장에서 제안하는 악성-속성을 정의하며, 4장에서 연구 결과 및 향후 연구 제시한다.

2. 기관별 악성코드 분류 기준

악성코드는 기관별로 그룹을 나누는 기준이 상이하다. 아래 <표 1>에서는 시만텍, 안철수 연구소, 카스퍼스키랩의 분류 기준을 서술하였다[2, 3].

<표 1> 안티바이러스 업체별 악성코드 분류 기준

기준	시만텍	카스퍼스키랩	안철수연구소
대분류	위협(threat), 위험(risk)	네트워크 웜, 클래식 바이러스, 트로이목마, 기타 악성코드	
소분류	위험: 스파이웨어, 애드웨어, 다이얼러, 해킹 도구, 조크, 원격 접속, 혹스, 트랙웨어, 허위 안티바이러스, 컨텐츠 감시 등 위험: 트로이목마, 바이러스, 웜	네트워크 웜: 이메일, 메신저, 인터넷, P2P 바이러스: 파일, 부트섹터, 스크립트, 매크로 트로이목마: Backdoor 등	Adware Appcare Clicker Downloader Dropper Script Spyware Trojan virus Worm

3. 악성-속성(Mal-Attributes)

알려진 악성코드들로부터 악성코드를 정의할 수 있는 속성(attributes)를 추출할 수 있으며, 이를 악성-속성이라고 정의한다. 악성-속성은 특정 악성코드를 실행시키는 주체, 실행된 악성코드의 행위에 의해 규정되는 기본 속성과 전파 방법 및 악성코드에 내포된 우회 기술 등과 같은 추가 속성으로 구분된다. 기본 속성의 변화는 신·변종 악성코드로 구분할 수 있으며, 추가 속성의 변화는 신·변종 악성코드로 구분하지 않는다.

3.1 기본 속성

악성코드의 두 기본 속성은 악성코드 실행 속성과 악성코드 수행 속성이다. 악성코드 실행 속성은 해당 악성코드를 실행시키는 주체가 되는 대상에 따라, OS에 의한 실행, 사용자에 의한 실행, 웹브라우저에 의한 실행, 다른 응용프로그램에 의한 실행으로 구분된다. 이는 <표 2>에서 정리한다. 악성코드 수행 속성은 악성코드의 소단위 동작에 의해 구분된다. 서버 접속 시도, 정보 전송, 시스템 설정 변경, 파일 변경, 다른 응용 프로그램 설정 변경, 정보 수신, 정보 탈취, 광고 행위, 브라우저 관련 행위 등이 악성코드 수행 속성에 해당한다. 이는 <표 3>에서 정리한다.

3.2 추가 속성

악성코드의 두 추가 속성은 악성코드 전파 속성과 악성코드 우회 속성이다. 악성코드 전파 속성은 악성코드의 전파 경로를 나타내는 속성 값으로 다른 속성들과 배타적인 성격을 갖지 않으며, 악성코드 자체를 규정하기에는 적합하지 않다. 악성코드 전파경로로는 악의적인 사용자에 의한 직접 삽입, 저장 매체를 통한 유입, 웹사이트를 통한 자·수동 다운로드, 다운로드 사이트를 통한 다운로드, 인스턴트 메시징 프로그램을 통해 다운로드, 이메일을 통한 전파 등이 있다. 악성코드 우회 속성은 악성코드 탐지를 어렵게 하기위해 갖는 악성코드의 속성으로 난독화, 치료 방해 등이 이에 속한다. 이러한 기술 또한 악성코드 자체를 규정하기에는 적합하지 않다.

<표 2> 악성코드 실행 속성

실행 주체	실행 과정
OS	서비스 등록으로 인한 부팅 시 자동실행
	레지스트리 등록으로 인한 자동실행
	시작 프로그램 등록을 통한 부팅 시 실행
	Autorun.ini를 통한 장치 연결시 실행
사용자	사용자의 입력에 의한 실행
브라우저	BHO(Browser Helper Object) 의해 실행
	ActiveX에 의해 실행
다른 응용프로그램	매크로 등 다른 응용프로그램에 의해 사용자 의사에 무관하게 실행

<표 3> 악성코드 수행 속성

수행 종류	수행 원인
서버 접속 시도	HTML을 이용한 접속
	User Level Protocol을 이용한 접속
	기타 다른 프로토콜
정보 전송	주소록 전송
	PC정보 전송(포트, OS, 백신, 가상화)
	특정 계정 정보 전송
시스템 설정 변경	보안정책(방화벽, OS update, Host파일)
	포트
	서비스
	레지스트리
	시스템 파일
파일 변경	새로운 파일 다운로드 (악성코드)
	Log 파일
다른 응용프로그램 설정 변경	안티 바이러스의 보안 수준
	매크로 코드 변경
정보 수신	공격지 정보
	스케줄
	명령
	악성코드 유포지
정보 탈취	키 로깅
광고 행위	메인 프로그램의 광고 란
	팝업 형 광고
브라우저 관련 행위	Active X 등록, 변조
	BHO 등록, 변조

4. 결론

본 논문에서는 악성코드를 규정지을 수 있는 악성-속성을 추출하여 이에 대해 정리하였다. 악성-속성을 이용하면 동일한 악성코드에 대해 분류가 용이하며, 각 속성별 위험도를 지정하여 유사 신·변종 악성코드 유입 시 위험 정도를 빠르게 파악하고 대응할 수 있다.

향후 연구 부분으로는 신·변종 악성코드 예측 및 이에 대한 대응 방안을 수립하기 위한 악성-속성 구체적인 활용방안에 대해 연구할 계획이다.

Acknowledgements

본 연구는 2011년 한국인터넷진흥원의 “악성코드 유사 및 변종 유형 예측방법 연구” 위탁과제의 지원을 받아 수행된 연구임

참고문헌

[1] AVtest, http://www.av-test.org, 2011.

[2] Kaspersky Lab, http://www.kaspersky.com, 2011.

[3] Symantec, http://www.symantec.com/index.jsp, 2011.