트위터에서의 악성코드 유포 실태조사

강정인, 도희성, 이희조
고려대학교 컴퓨터 · 통신공학부
e-mail : {keijin, bestylish, heejo}@korea.ac.kr

A Survey on Twitter Malware Distribution

Jung-in Kang, Heesung Do, Heejo Lee
Division of Computer and Communication Engineering, Korea University

요 약

최근 전세계적으로 마이크로-블로그 형태의 소셜네트워크 서비스가 확산되어가고 있으며, 트위터(Twitter)란 이러한 가장 대표적인 소셜네트워크 서비스이다. 본 논문에서는 트위터를 매개로써 이루어지는 악성코드 유포 행위를 조사하기 위해 트위터에 올라오는 게시물(Tweet)들에서 약 93 만개의 링크를 임의 추출하여 다운받았고, 이중 7 개의 악성코드 배포 계정을 검출하여 해당 게시물과 계정의 특징을 조사하였다.

1. 서론

트위터는 트윗이라고 불리는 최대 140 글자의 게시물을 통해 이용자들 사이에서 정보를 공유하고 소통할 수 있는 마이크로블로그 형태의 소셜 네트워크 서비스이다. 빠른 확산속도를 보이고 있는 이 서비스는 2010 년 9 월기준으로 전세계 1 억 4500 만명의 가입자를 보유하고 있으며, 국내의 경우 역시 스마트폰 보급과 함께 그 이용률이 급속도로 증가하고 있다.

트위터에 대한 폭발적인 관심은 일반 사용자들뿐만 아니라 상업적 이용을 노리는 기업체, 스패머, 혹은 피싱을 시도하거나 악성코드를 배포하는 공격자들의 접근 또한 유도하였다. 특히 트위터의 글자수 제한이라는 특징은 이용자들이 URL 줄임서비스(URL-shortening)를 통하여 원본 링크를 감출 수 있게 허용하기 때문에 공격자들로 하여금 악성코드가 숨겨진 주소를 쉽게 숨길 수 있게 하였다. 또한 공격자가 @ 기호와 다른 이용자의 아이디를 붙여서 트윗에 삽입하는 경우(Mention-spam) 대상 이용자는 필터링 없이 해당 트윗을 보아야 하는 등 공격자에게 있어 여러 유리한 환경이 트위터를 통해 조성되었다.

실제로 지난 2009 년 4 월에 발생한 'StalkDaily' 웜[4]이나, 2010 년 9 월에 발생한 'Mouseover' 웜[5]의 경우 트위터가 충분히 악성코드 배포의 매개체가 될 수 있음을 입증하고 있다.

이에 본 논문에서는 트위터에서 발생하는 악성코드 배포행위들에 대한 실태를 조사하기 위해 이용자들의 트윗에서 링크들을 추출하여 다운받고, 안티바이러스 엔진을 통해 악성코드를 검출한다. 그리고 이와 동시에 해당 유포 계정에 대한 분석을 진행하여 발생하는 악성코드 위협들에 대응하기 위한 실태조사 자료를 제공한다.

이후 논문의 구성은 다음과 같다. 먼저 2 장에서는 기존의 관련 연구에 대해 소개하고, 3 장에서는 악성코드 수집을 위해 사용한 방법에 대해 대해 다루도록 한다. 4 장에서는 수집한 결과에 대해 설명하고, 5 장에서는 악성코드에 대한 분석을, 6 장에서는 악성코드를 배포하는 계정들에 대한 분석을 진행한다. 마지막으로 7 장에서는 논문의 요약과 결론, 향후 과제를 제시하며 마무리한다.

2. 관련 연구

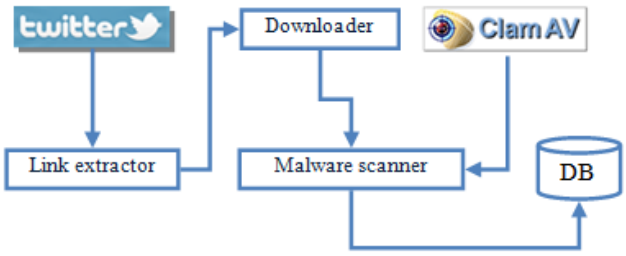
트위터에서의 악성행위에 대한 연구는 주로 스팸 계정 혹은 스팸 트윗을 대상으로 하고 있는데, Miranda Mowbray 는 트위터에서 발생하는 스팸 기법들에 대해 분류를 하였다. 이는 트위터에서 제공하는 스팸필터기인 @spam 에 레포팅된 스팸들을 분류한 것으로써, Mention-spam, Follow-spam, Trend Abuse, Fake Retweets 의 트위터에서의 여러 서비스들에 기반한 스팸 기법에 대해 구분을 하였다[1].

Kyumin Lee 등이 발표한 연구는 Honeypot 개념을 도입하여 트위터를 비롯한 여러 소셜 네트워크 서비스에서의 스패머 검출 시스템을 제시하였다. 또한 기계학습을 통한 분류기 제작을 위해 트위터 계정의 User profile, Tweets, Following, Follower 정보들에 대해 수치화하는 방법들에 대해 제안하였다[2].

하지만 상대적으로 활발한 스팸 연구에 비하여 악성코드 배포행위를 대상으로 한 통계/연구는 많지 않다. 따라서 본 논문에서는 악성코드 배포행위의 연구에 초점을 맞추고 기존 연구들이 제시한 스팸 분류기준을 변형, 이용하여 악성행위를 분석하였다.

3. 악성코드 수집 방법

이용자의 트윗에서 파생되는 주소로부터 악성코드를 수집하기 위해 Link extractor, Downloader, Malware scanner 세 모듈로 구성된 크롤러(Crawler) 시스템을 구현하였다. 각 모듈에 대한 설명은 다음과 같다.



(그림 1) 시스템 구성도

Link Extractor

트위터의 Search API 는 검색어를 통해 해당 단어를 포함한 트윗을 가장 최근의 순서부터 정렬해 보여주는 기능을 한다. 본 모듈에서는 이 기능을 이용하여 검색된 트윗들에서 링크를 추출한 뒤 Downloader 에 넘긴다. 검색어는 'http'로 하여 링크를 포함한 트윗들이 검색되도록 하였고, 추가로 'exe', 'pdf', 'download', 'get'과 같이 악성행위에 이용될 수 있는 파일의 확장자명과 특정 단어들을 OR 연산자를 이용하여 검색하도록 하였다.

Downloader

해당 링크가 연결한 페이지나 파일을 다운로드 하여 저장하는 역할을 한다. URL shortening 서비스를 이용한 경우에만 원본 링크를 따라가서 다운받는다. 트윗을 통하여 시도된 직접적인 악성행위만을 통계하기 위해 크롤러의 depth 옵션을 1 로 주어 direct 링크만을 다운로드 하였다.

Malware Scanner

다운받은 파일에 대한 악성코드 여부를 판단하는 역할을 한다. 본 논문에서는 시그니쳐 기반 오픈소스 안티바이러스 엔진인 ClamAV 를 이용하여 악성코드 여부를 검사하였다.

4. 수집결과

위와 같은 시스템을 이용하여, 2010 년 08 월~09 월 사이 약 93 만개의 링크 주소가 포함된 트윗을 수집하였다. 이중 서로 다른 유저 계정의 수는 약 22 만개, 서로 다른 트윗의 수는 35 만개였다. 수집된 자료에 대해 수작업으로 검토를 한 결과 여러 계정에서 동일한 스팸트윗을 발송하는 경우, 일반 트윗에 대해 다른 사용자들이 리트윗(Retweet, 답장)을 하는 경우와 같은 여러 행위들 때문에 이러한 중복되는 경우가 생긴 것으로 파악하였다. 이중 서로 다른 7 개의, 상호 별개의 계정에서 생성된 트윗에서 악성코드가 발견되었다. 즉 트위터에서 링크를 포함한 트윗 중 0.002%는 악성코드 배포 행위를 한 것이라고 추정된다.

Symantec 의 2010 년 6 월 State of Spam Report & Phishing Report 에 의하면, 전체 스팸 메일중 5%의 메일이 악성코드를 포함하고 있다고 한다. 2010 년 3 월에 트위터는 스팸 트윗 비율이 약 1%라고 발표하였다. 즉 트위터에서의 스팸 행위와 메일을 이용한 스팸 행위에서의 악성코드 배포 비율이 같다고 가정하였을 때, 이론적인 악성코드 배포 트윗의 비율은 0.05%라는 결론을 얻을 수 있다. 트위터에서 발표한 다른 통계에 의하면 약 25%의 트윗이 링크를 포함하고 있다고 하였기 때문에, 링크를 포함한 트윗만 수집한 본 논문에서의 실험 결과로는 0.0125%정도의 이론적인 결과가 나와야 한다. 즉 본 논문에서의 결과와는 어느 정도 차이가 있는 수치이다. 다만 트위터의 특성 상 링크를 포함한 트윗에서의 스팸 비율이 그렇지 않은 경우보다 더 높을 것이라는 점과, 전체 트윗중 스팸의 비율이 낮아지고 있다고 발표한 점을 감안하면 어느 정도 타당한 수집결과라고 할 수 있을 것이다.

5. 악성코드 분석

다음은 검출된 악성코드를 종류별로 나열한 표이다.

<표 1> 검출된 악성코드 목록

번호	진단명	검출수
1	Trojan.JS-34	2
2	JS.Agent-48	1
3	Exploit.JS.CVE-2006-1359	2
4	Trojan.Refroso-2601	1
5	Trojan.Inject-3597	1

이중 1~3 번의 경우 검출된 파일은 웹 페이지 데이터였으며, 4,5 번의 경우 Win32 바이너리 실행파일이었다. 특이점은 1~3 번의 경우 모두 URL 줄임서비스를 이용하여 배포된 반면 4,5 번은 바이너리 파일의 전체 링크를 직접 트윗에 포함하는 방식으로 배포되었다.

6. 악성코드 배포계정 분석

다음은 각 악성코드를 배포하고 있는 트위터 계정의 following, followers, listed, 트윗 수와 Bio, Web 정보를 가지고 있는지 여부를 표시한 것이다.

<표 2> 악성코드에 따른 배포계정의 속성

#	Mal#	#Following	#Followers	#Listed	#Tweet	Bio	Web
1	1	115	269	3	1072	N	Y
2	2	640	288	1	3728	Y	Y
3	3	1920	1202	19	25129	Y	Y
4	3	7	3030	463	5120	Y	Y
5	1	256	336	10	6055	N	Y
6	4	0	1	0	15	N	N
7	5	42	12	0	5	N	Y

각 계정의 성격을 분석한 결과, 1,2,4 번의 경우 각각 동일 도메인 웹사이트의 새로운 글로 연결된 링크를 트윗에 포함시켜 지속적으로 올리고 있었다. 해당 계정들이 기존에 작성한 트윗의 링크들을 검사한 결과, 링크된 사이트의 서로 다른 페이지들에서 모두 같은 악성코드가 검출되었다. 4 번의 경우 특정 언론사에서 운영하는 트위터 계정이었고 1,2 번 역시 상당한 수의 Followers 를 가지고 있는 정상적인 계정으로 보였다. 이와 같이 유효한 정보를 전달하며 다수의 Follower 를 통해 인지도를 확보한 계정에서 악성코드가 배포된다면, 이에 대해 일반 사용자가 악성 판단 여부를 판단하는 것이 매우 힘들기 때문에 큰 피해를 양산할 수 있는 위험을 지닌다.

3 번의 경우 지속적으로 링크를 포함한 트윗을 올리고 있었으나, 링크된 페이지의 웹사이트가 서로 다른 도메인이었고 기존의 다른 트윗에서 추가적인 악성코드는 검출되지 않았다. 즉 단순히 특정 주제에 대한 정보들을 수집하여 제공하는 일반 사용자 계정으로 판단된다. 5 번의 경우 특이사항이 없는 일반 사용자 계정이었다. 즉 3, 5 번의 경우 일반 사용자가 악성코드를 포함하는 웹 페이지를 우연히 배포하게 된 것으로 추정할 수 있다.

6, 7 번의 경우 1~5 번과 달리 무의미한 문자열을 계정 명으로 하고 있다. 이들은 파일공유사이트에서 제공하는 서비스를 이용하여 '. exe' 확장자의 바이너리파일 링크를 포함한 트윗을 URL 줄임서비스를 사용하지 않은 상태로 연속적으로 올려놓았다. 또한 링크와는 상관없는 피싱메시지를 트윗에 포함하여 클릭을 유도하였다. 6 번의 경우 하나뿐인 Follower 는 또 다른 스팸 계정이었다. 7 번의 경우 Friend Infiltrators [1] 특성을 보여주었는데, 특정 단어('israel' 혹은 'sex')가 들어간 임의 사용자들을 Following 하고 있었다. 특이점은 Follower 과 Following 이 일치되는 계정(즉 상호 Following 을 한 경우)이 발견되지 않았다는 점이다. 7 번의 Follower 는 대부분 선정적인 프로필사진/계정명을 가지고 있었으며, 매우 큰 Following / Follower 비율을 보여주는 스팸 계정들 이었다.

7. 결론 및 향후 과제

본 논문에서는 트위터에서의 악성코드 배포현황에 대한 조사를 통해, 실제 트위터에서 악성코드 배포 행위들이 발생하고 있음을 확인하였고 이에 대해 분석을 진행하였다.

특히 논문에서 다루고 있는 특정 계정들은 지속적으로 악성코드를 배포하고 있음에도 불구하고, 시간이 지나도 별다른 조치가 이루어지지 않은 채 조회가 가능하였기 때문에, 이에 대한 대처방안이 조속히 마련되어야 할 것이다.

트위터의 사용자는 지속적으로 증가 추세에 있으므로 이를 매개로 한 악성코드 배포 또한 증가할 것으로 예상된다. 본 연구의 수집결과들을 바탕으로 더 많은 양, 그리고 더 높은 검출 비율을 가진 악성코드 수집 시스템을 구현한다면 이러한 악성코드 배포 행위를 검출하는 데 큰 도움이 되리라 생각한다. 검출 비율의 향상에 대해서는, [6]에서 소개하는 것 과 같은 전통적인 기존 웹 페이지에서의 악성코드 유포사이트 탐지 기법이 응용될 수 있을 것이다. 또한 트위터의 @spam 과 같은 Mention-spam 행위를 근절하기 위해서는 지속적인 모니터링/경보를 수행함과 동시에, 트위터에서 발견된 샘플들을 수집/분석하여 특성 연구를 진행하는 것이 필요하리라 본다.

8. 사사

This study was funded by the R&BD Support Center of Seoul Development Institute and the South Korean government (Project title: WR080951, Establishment of Bell Labs in Seoul / Research of Broadband Convergent Networks and their Enabling Technologies).

본 연구는 지식경제부 및 한국산업기술평가관리원의 IT 산업원천기술개발사업 [KI001863, 신종 봇넷 능동형 탐지 및 대응 기술], 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업(NIPA-2010-C1090-1031-0005)의 연구결과로 수행되었음.

참고문헌

[1] M Mowbray, "The twittering machine", Journal of Applied Statistics, 17(2):211–217, 2010

[2] K Lee, J Caverlee, S Webb, "Uncovering Social Spammers: Social Honeypots+ Machine Learning", the 33rd international ACM SIGIR, 2010

[3] zeljka zorz, "Twitter malware campaign with a banking Trojan and keylogger combo", http://www.net-security.org/malware_news.php?id=1349, 2010

[4] Mikko, "Twitter Worm Outbreak Over Easter", http://www.f-secure.com/weblog/archives/00001653.html, 2009

[5] NIALL FIRTH, "Twitter 'mouseover' worm redirects hundreds of thousands of users to porn sites", http://www.dailymail.co.uk/sciencetech/article-1313981/Twitter-mouseover-worm-redirects-hundreds-thousands-users-porn-sites.html, 2010

[6] 서동원, Arindam Khan, 이희조, "악성 코드 유포 사이트 탐지에 관한 연구", 제 30 회 한국정보처리학회 추계학술발표대회 논문집 제 15 권 제 2 호, 2008

[7] Symantec, State of Spam & Phishing Report - June 2010, 2010
[8] Twitter, “State of Twitter Spam”, http://blog.twitter.com/2010/03/state-of-twitter-spam.html, 2010
[9] MG Siegler, “Twitter Hatches The New Twitter.com — A New Two-Pane Experience”, http://techcrunch.com/2010/09/14/twitter-event/, 2010