정 보 보 호 학 회 지
제24권 제2호, 2014. 4

APT 현황과 신종 악성코드 대응방안

임 설 화*, 김 종 수, 양 준 근, 임 채 호**

요 약

APT란 백신에서 탐지를 못하는 신종 악성코드로서 1 비트만 바뀌어도 탐지를 할 수 없는 안티 바이러스 제품의 오용탐지 기반, 즉 알려진 위협의 증거값(Signature)이 있어야만 탐지하는 구조에 기인한다. 일부에서 APT를 이메일에 첨부된 신종 악성코드라고 이야기하고 있으나 이는 APT의 전파 방법 중 하나일 뿐이고 올해 발생한 3.20 사이버 테러에서 알 수 있듯이 웹을 통한 불특정 다수를 목표로 한 신종 악성코드의 무차별 감염이 심각한 상태이다. 따라서 본 논문에서는 그동안의 사례를 분석하고 APT에 대응하기 위한 방안에 대해 살펴보고자 한다.

Ⅰ. 서 론

최근 발생한 6.25 사이버 공격과 3.20 사이버 테러, 그리고 2011년 11월 넥슨의 1,322만명과 7월 SK컴즈의 3,500만명의 개인정보가 유출되었고 같은 해 4월에는 APT공격으로 농협의 전산망이 마비되었다. 2월에는 현대 캐피탈 해킹으로 175만명의 개인정보가 유출되는 사건이 있었다. 또 2008년 1월에는 옥션이 해킹당해 1,080만명의 개인정보가 유출되었다.

2013년 6월 25일에 발생했던 6.25 사이버 공격으로 청와대와 정부기관 홈페이지가 변조되었고 이를 통해 개인정보가 유출되었다. 그리고 대전 정부통합전산센터에는 DNS쿼리를 이용한 분산서비스거부공격(DDoS)이 있었다. 이 공격은 공격 6개월 전부터 준비되었던 것으로 추정되고 있다.

또 같은해 3월 20일에 발생했던 3.20 사이버 테러는 MBC, KBS, YTN, 신한은행, 농협 등 주요 방송사와 금융권이 공격당하여 하드디스크가 파괴되는 등 전산이 마비되었다. 이 전산망 마비로 금융 거래 등이 중단되었다.

최근 몇 년간 이러한 APT 공격으로 인한 피해가 지속되고 있으며, KAIST에 따르면 3.20 사이버 테러의 경우 피해액이 8,823억 원에 달한다고 한다.

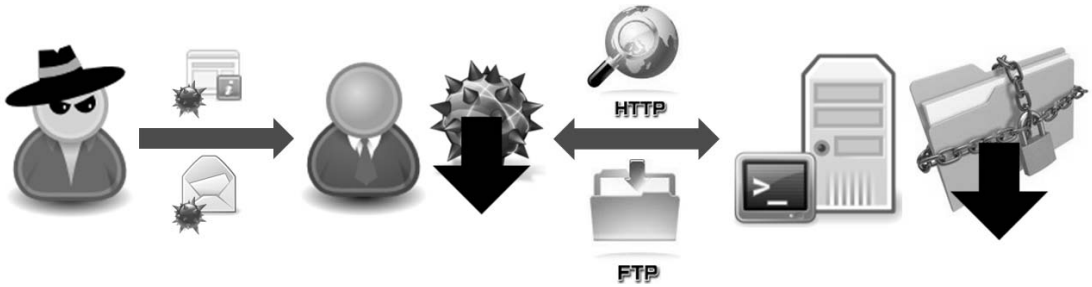
이처럼 최근 사이버 공격의 양상은 점점 지능화되어 사고가 발생하기 몇 년 전부터 타겟 네트워크 망에 침투해 모니터링을 하다가 적절한 타이밍에 공격을 가한다. 혹은 불특정 다수를 감염시킨 후에 이들을 모니터링하여 타겟을 정하고 공격을 행하기도 한다.

APT는 다단계의 공격 프로세스를 거쳐서 이루어진다. 먼저 공격자가 악성코드를 포함한 메일을 타겟이 된 기업, 기관 등의 사용자에게 보낸다. 또는 취약점이 존재하는 웹 서버를 감염시켜 방문자들을 감염시키고, 이들의 모니터링을 통해 공격자가 원하는 공격 대상을 선별한다.

〔표 1〕 최근 우리나라에서 발생한 사이버 공격

구분	피해 내용	감염 경로
2013.6.25 사이버 공격	정부기관 홈페이지 변조, 대전 정부통합 전산센터 DDoS 공격	웹
2013.3.25 사이버 테러	주요 방송사 및 금융권 마비로 약 8,800억원 손해	웹
2011.11 넥슨	1,322만명 개인정보 유출	웹
2011.7 SK 컴즈	3,500만명 개인정보 유출	·
2011.4 농협	농협 전상망 마비	웹
2011.2 현대캐피탈 해킹	175만명 개인정보 유출	·

* 동국대학교 국제정보대학원 (sulhwa.im@gmail.com)
동국대학교 국제정보대학원 (tndud4ah@gmail.com)
동국대학교 국제정보대학원 (junkune@gmail.com)
** 카이스트 정보보호대학원 (chlim@kaist.ac.kr)



〔그림 1〕 APT의 다단계 공격 프로세스

보통 사용자는 drive-by-download에 의해 악성코드가 다운로드 되고, 실행되면서 감염된다. 사용자가 감염이 된 후에는 보안 솔루션을 우회하기 위해 몇 주간을 휴면 상태로 지내기도 하고, 백신의 프로세스를 정지시키거나, 삭제가 되도 재설치하게 하는 등의 방법을 통해 장기적으로 공격을 할 수 있는 기반을 마련한다.

이렇게 공격 기점을 마련하면 공격자는 C&C 서버를 이용해 감염 대상을 제어하고, 네트워크 공유 파일 등을 통해 감염 대상을 확대시킨다. 이렇게 확보된 감염 대상에게서 중요 정보가 담긴 데이터들을 FTP, HTTP 등의 신뢰할 수 있는 서비스를 이용해 C&C 서버에 다운로드 받을 수 있다.

이처럼 사용자들은 점점 지능화되고 지속적인 위협에 노출되어 있지만, 공격자들의 치밀하고 다양한 침투 방법, 보안 솔루션을 우회하는 공격 등을 가하고 있어 보안 담당자들이 사전에 위협을 파악하고 대처하기가 어려운 실정이다.

APT(Advance Persistent Threat)란 1비트만 바뀌어도 백신에서 탐지를 못하는 신종 악성코드와도 같다. 이는 안티 바이러스 제품의 시그니처 탐지 기반 구조가 가지는 취약점을 이용한다. 따라서 기존에 백신이 탐지한 악성코드이더라도 1비트만 바꾸면 새로운 신종 악성코드가 된다.

이처럼 백신에서 탐지가 되지 않고, 정상적인 프로그램처럼 동작하면서 공격에 필요한 정보들을 수집하기 때문에 보안 담당자가 사전에 이를 파악하는 것은 무척이나 어렵게 된다.

또한 이런 APT 공격은 주로 금융, 매체, 사회기반시설 등 중요한 기관에 접근하여 시설을 파괴하거나 중요 정보를 유출하는 등의 형태로 일어나고 있다. 소규모가 아닌 대규모 공격으로 일어나고 있기 때문에 피해액수의 규모도 상당하다.

그래서 본 논문에서는 APT 공격 사례들의 공격 분석을 하고, APT 대응 방안에 대해 살펴보고자 한다. 특히 웹을 통해 감염된 APT의 공격에 대해서 더 상세히 살펴보고자 한다.

Ⅱ. 관련연구

2.2 Web을 이용한 APT 공격 사례 및 분석

2.2.1 Web을 이용한 APT 공격 사례

2.2.1.1 Facebook[1]

2013년 1월 Facebook社의 소수 직원이 손상된 모바일 개발자 웹 사이트에 방문하는 과정에서 악성코드에 감염되어 공격을 당했다. facebook측은 악성코드를 발견하자마자 OS, 백신 등의 패치를 수행했다.

이 후 지속적인 조사가 진행되었고, Facebook 사용자의 데이터 유출은 없는 것으로 확인되었다.

공격자가 이용한 취약점은 Java Sandbox를 우회하는 Zero-day 공격인 것으로 밝혀졌다. 이 제로데이 취약점의 패치는 2013년 2월 1일에 제공되었다.

2.2.1.2 미국 노동부

2013년 4월 말 미국 노동부 웹 사이트에서 핵과 관련된 컨텐츠에 접근하는 방문자들에게 악성코드가 전파되는 사고가 발생했다[2].

공격자는 Microsoft社의 웹브라우저인 Internet Explorer가 삭제된 객체나 제대로 할당되지 않은 메모리에 있는 객체에 접근할 때 발생하는 Zero-day 취약점을 이용했다[3].

2.2.1.3 미국 외교 협회[4]

2012년 12월 미국의 외교 협회 웹 사이트에서 발생한 사건으로 방문자들의 윈도우 시스템을 해킹하기 위해 Internet Explorer 8의 Zero-day 취약점을 이용했다. 공격은 중국 해커의 소행으로 의심되며, 공격이 발생한 웹 사이트에는 임원, 기자 등 주요인사 4,700여 명이 가입되어 있었다.

공격당한 기구가 미국의 정예 외교 정책 기구 중 하나이기 때문에 FBI에서 조사를 진행했지만, 공격자들이 보안 전문가들의 분석을 피하기 위해 악성 코드를 삭제해 더 자세한 조사는 진행되지 못했다.

2.2.1.4 국내 안보 관련 주요 연구소[5]

2013년 5월 16일 발생한 사고로 공격자는 JAVA Zero-day 취약점 중 2D 구성 요소의 색상 관리 기능에서 발생하는 취약점을 이용해 공격했다. 발견된 공격대상은 한국국사문제연구원, 한국안보문제연구소, 한국전략문제연구소, 한국해양전략연구소 총 4곳으로 조사되었다.

이 연구소들은 일반인들이 평상시에 거의 접근하지 않고, 연관된 사람들이 방문하는 특화된 연구소들이다. 따라서 이번 공격은 감염 대상을 한정한 워터링 홀 공격으로 볼 수도 있다.

2.2.2 Web을 이용한 APT 공격 분석

웹의 근본적인 문제점은 클라이언트 프로그램인 웹 브라우저가 웹 서버 애플리케이션의 통제 범위에 포함되지 않는 것이다. 따라서 웹 브라우저는 해당 웹서버의 통제 범위 밖에 존재하기 때문에 공격자가 임의로 조작된 입력 값을 통해 애플리케이션의 로직이나 기능을 훼손할 수 있고, 또한 애플리케이션 데이터에 접근할 수 있다[6].

OWASP TOP10에 나온 A1부터 A10의 취약점들을 보면 웹의 근본적인 문제를 이용한 취약점 공격이 대다수이고, 이런 취약점은 점차 형식을 교묘히 바꾸면서 다양하게 나타나고 있다. 다음 [표 2]는 이러한 웹 취약점을 이용한 공격 유형과 공격 방식에 대한 설명이다.

2.2.2.1 Watering hole attack[7]

Watering hole attack이란 타겟이 된 대상의 방문가능성이 높은 합법적인 웹 사이트를 손상시켜 공격하는 방법이다.

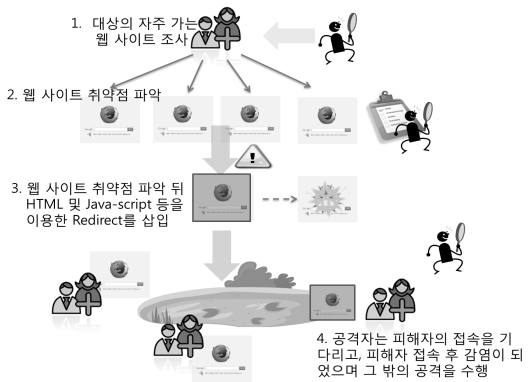
즉, 일반인들이 상시적으로 방문하는 사이트가 아니라 특정 계층이나 관련된 인사들만이 접근하는 사이트들을 대상으로 악성코드 감염을 유도하도록 하는 공격을 말한다[5].

이 공격은 대상 웹 사이트에 악성 스크립트를 미리 삽입한 후에 타겟이 웹 사이트에 방문했을 때, 타겟의 취약점 여부를 파악한다. 이렇게 취약점이 파악되면 악성 스크립트를 통해 그 취약점을 악용하는 악성코드로 리디렉션한다. 따라서 감염된 웹 사이트는 Drive by Download 방식을 이용하여 사용자를 감염시킨다.

워터링 홀 공격 절차를 살펴보면 공격자는 정해진 타겟의 특성과 형태에 따라 자주 찾는 웹 사이트 정보를 프로파일링 한다. 그 다음에는 자주 찾는 웹 사이트의 종류에 대한 분석을 실시한다. 이렇게 분석을 통해 특정

〔표 2〕 web 취약점을 이용한 공격 유형과 공격 방식〔6〕〔8〕

취약점	설명	방식
SQL-injection	SQL의 입력 값의 검증 절차 없을 시 발생 또는 우회하는 기법으로 발생하는 것	① 논리적 에러방식 ② Union Based SQL injection ③ Stroed Procedure SQL njection ④ Mass SQL injection
XSS (Cross Site cript)	사용자 입력 데이터를 검증하지 않고 동적 페이지에 악성 스크립트 코드가 포함되고 실행이 되는 것	① Reflected Cross Site Scripting ② DOM Cross Site Scripting ③ Stored Cross Site Scripting
Active-X	인터넷 익스플로러의 기능을 확장하기 위해 마이크로소프트(Microsoft)가 제공하는 기능으로서 PC 자원에 쉽게 접근이 가능	① Update URL 조작 ② File read/write method 조작



〔그림 2〕 Watering Hole Attack 개략도

웹 사이트를 정한 뒤, 웹 사이트 페이지 정보 및 각종 정보들을 통해 웹 사이트가 가지고 있는 취약점들을 찾아낸다.

공격자들은 특정 웹 사이트가 가지고 있는 이런 취약점들을 이용하여 웹 사이트를 공격하고, 웹 사이트에 악성코드를 삽입한다. 이렇게 공격 준비를 끝낸 공격자들은 타겟이 이 웹 사이트에 방문하기를 기다린다.

타겟이 감염된 웹 사이트에 접속을 하면, 접속과 동시에 Drive by Download 방식으로 타겟에게 악성코드 파일을 내려보낸다.

이러한 워터링 홀 공격은 SQL injection, XSS (Cross-Site-Script), File Upload, URL/Parameter 변조 등 다양한 웹 취약점을 이용해서 이뤄진다.

III. 웹을 통한 불특정 다수를 목표로 한 악성코드 분석

3.20 사이버 테러의 경우 웹 서버의 취약점을 이용해 웹 서버를 해킹한 후, 해당 웹 서버로 접속하는 사용자들에게 악성코드를 감염시켰다.

3.1 3.20 사이버 테러

2013년 3월 20일 오후2시경 MBC, YTN, KBS 방송 3사와 농협, 신한은행, 제주은행 금융 3사의 전산망이 일제히 마비를 일으켰다. 이로 인해 약 3만 2천대의 PC가 피해를 입었고, 약 8,800억 원의 피해를 입었다. 이 공격으로 마비되었던 전산망이 복구되기까지는 10일의 시간이 소요되었다. 이런 피해를 낳은 3.20 사이버 테러는 Web을 이용한 대표적인 APT공격이다.

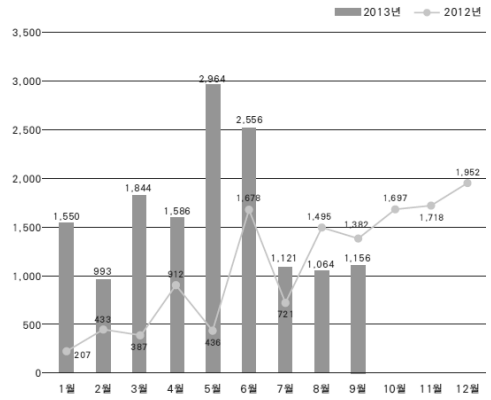
공격자는 APT 공격을 위해서 장기간 동안 다수의 시스템을 확보했다. 공격자는 취약점을 통해 웹 서버를 해킹하고 악성코드를 심어 놨고, 웹 Active-X 모듈의 업데이트 기능을 활용하여 파일경로를 변조하였다. 이 변조된 파일은 방문자가 감염된 사이트에 접속해 업데이트가 실행될 때 악성코드에 감염되도록 했다[9].

Active-X는 인터넷익스플로러의 기능을 확장하기 위해 제공된 웹 애플리케이션으로 언제 어디서든지 웹 인터페이스를 통해 PC의 레지스트리, 파일 등에 쉽게 접근을 할 수 있다. 그러나 이런 편리함이 있음에도 Active-X는 보안성 검증절차가 없는 취약점이 있다. 이 취약점은 공격자들의 주요 공격 수단이 된다[8].

이렇듯 공격자는 3.20 사이버 테러를 위해 Watering hole attack과 사회 공학적 기법, 취약점을 이용한 악성코드를 이용해 중장기적으로 공격을 준비했다.

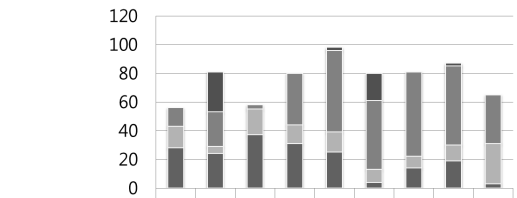
Ⅳ. 웹을 통해 유포되는 악성코드 대응 방안

APT 공격의 정확한 프로세스와 명확한 공격에 대한 흔적을 찾기는 어렵다. 하지만 웹에서 떠돌고 있는 악성코드들은 모두 APT 공격의 시발점이 될 수 있다.



〔그림 3〕 악성코드 은닉사이트 탐지조치 건수 추이('13년 10월)〔10〕

[그림 3]에서 보여 지는 것과 같이 악성코드가 은닉되어 있는 웹 사이트의 수는 작년보다 점점 더 많아지고 있는 추세이다. 따라서 3.20 사이버 테러와 같은 웹 취약점을 이용한 공격은 앞으로도 점점 증가할 것이고, 이로 인한 피해는 날이 갈수록 커질 것이다.



	1월	2월	3월	4월	5월	6월	7월	8월	9월
■키로깅,정보수집		28			2	19		2	
■원격제어	13	24	3	36	57	48	59	55	34
■드롭퍼	15	5	18	13	14	9	8	11	28
■다운로더	28	24	37	31	25	4	14	19	3

〔그림 4〕 웹 사이트로 유포된 악성코드 유형〔11〕

또한 [그림 4]을 살펴보면 웹 사이트를 통해 유포된 악성코드의 유형은 키로깅, 원격제어, 드롭퍼(Dropper), 다운로더(Downloader) 등이 있다. 이 중 드롭퍼, 원격제어, 다운로더는 APT 공격의 시발점이 될 가능성이 매우 크다.

이처럼 국내 주요 사이트는 실제 악성코드를 직접 유포하는 유포지로 사용되기도 하며, 악성코드 유포지 링크를 웹 페이지 내에 가지고 있는 경유지로도 이용되고 있다. 특히 공격자들은 목표 PC를 감염시키기 위해 목표 대상이 자주 접속하는 정상적인 웹 사이트를 경유지로 이용한다.

그리고 공격자들은 탐지를 회피하고 악성코드의 생존율을 높이기 위해 다단계로 경유지와 유포지를 구성하기도 한다. 또 지속적으로 경유지와 유포지를 변경하여 노출을 최소화해 악성코드 대응활동을 우회하고 있다.

웹 사이트에 악성코드를 은닉하는 방법은 다음 [표 3]과 같다. 악성코드 255개의 도메인에 대해 539개의 악성 URL 및 악성 웹 사이트를 분석한 것이다. 이 내용에 따르면 스크립트와 익스플로잇, 태그의 사용이 가장 많았다. 기존에는 이와 같은 은닉 기술들이 많이 사용되었지만, 향후에는 document.write와 같은 잘 알려진 메서드의 사용이 줄어 들 것으로 보여지며, 잘 알려지지 않은 스크립트 구동 메서드들이나 잘 알려진 메서드들을 대체할 수 있는 메서드들이 사용되어 질 것으로 보인다[12].

따라서 다음에서는 이렇게 웹 사이트로 유포되는 악성코드에 대응하기 위한 방안들에 대해 살펴보고자 한다.

4.1 악성 웹사이트 탐지 및 대응

웹사이트에 은닉된 악성코드를 탐지하는 기술은 BlackList 기반의 패턴매칭 방식이 많았다. 하지만 이 방식은 악성코드가 변경될 경우 탐지가 불가능 하고 이로 인해, 웹 사이트에 접속하는 많은 접속자들은 악성코드에 노출될 수 있다.

이처럼 BlackList 기반 방식은 공격 형태의 변화에 영향을 받아 신규 은닉 기법이나 패턴화 되어 있지 않은 신종 악성코드가 탐지 불가능하다. 이런 BlackList 기반의 한계점을 극복하기 위해 악성코드의 프로세스 행위를 분석하여 탐지하는 WhiteList 기반의 방식이 생겨났다. WhiteList 기반 방식은 웹 사이트 접속 시 다운로드된 실행 파일의 프로세스에 대한 행위 분석을 실시하여 패턴화 되어 있지 않은 악성코드 탐지, 플래시 파

[표 3] 웹 사이트 악성코드 은닉 기술[12]

은닉 기술	내용
document.write 사용	웹 페이지에 악성 행위에 대한 스크립트 내용을 직접 기록하지 않고, 악성코드 유포지나 경유지 정보를 삽입
외부링크 사용	외부 도메인을 통한 데이터 접근
URL 인코딩	알려진 악성 URL을 웹 페이지 소스 상에서 알아보기 힘든 형태로 인코딩
난독화 코드	키워드를 통한 정보 획득 회피를 위해 난독화된 소스코드나 인코딩된 문자열 형태의 스크립트 소스코드 사용
스크립트 사용	웹 페이지의 다양한 페이지 표현을 가능하도록 하는 스크립트를 이용하여 악성코드를 은닉
인코딩 사용	악성코드 유포 패턴 페이지 은닉을 위해 스크립트 코드를 알아보기 힘든 코드로 변경
태그 사용	웹 페이지 구성에 사용되는 javascript, script, vbscript, iframe 등의 태그를 이용하여 악성코드 유포
태그 size 사용	iframe과 같이 웹 페이지에서 대상 태그의 사이즈를 지정해야 하는 경우 악성코드 은닉 후 탐지를 우회하기 위해 사이즈 크기를 0,0이나 100,0과 같이 알아보기 어렵도록 작성
exploit 형식	악성 코드를 실행 파일 및 쉘 코드로 수행하거나 htm, js, php 등과 같은 웹 페이지 구성 파일을 중계

일 내 스크립트, 난독화, 유포지·경유지 변경과 같은 공격 형태의 변화에 영향을 받지 않는 방식이다[13].

이렇게 악성코드 은닉 사이트를 탐지하기 위해선 다음과 같은 기능들이 요구된다[14].

첫째, 공격 형태의 변화에 무관한 탐지 기능이 필요하다. 최근에 공격들은 악성코드 대응 활동에 대비해 유포지·경유지를 자주 변경하거나 난독화 등을 통해 우회하고, 바이너리 파일 내에 스크립트 등을 이용하여 공격 형태를 변화하고 있다.

둘째, 활성화된 공격에 적시에 대응하기 위해 신속한 악성코드 탐지가 이루어져야 한다.

셋째, 웹 사이트 접속 시 실행되는 프로세스 정보로 악성코드 여부를 분석하기 위해 가상화 환경을 구축하고, 악성코드가 실행되는 시점에 DLL Injection을 통해 프로세스 실행과 관련된 함수를 후킹하여 정보를 수집한다.

넷째, BlackList 기반의 패턴이 존재하는 악성코드 탐지 뿐만 아니라, 백신 패턴에 등록되어 있지 않은 신종 악성코드도 탐지해야 한다. 이는 WhiteList 방식을 적용하여 탐지가 가능하다. 정상적으로 설치되는 프로그램들을 분석하여 목록화해 악성코드 점검 결과를 WhiteList와 비교하여 BlackList에서 탐지할 수 없었던 악성코드를 탐지해 낼 수 있다.

마지막으로 중앙 집중적 탐지 및 대응 체계를 수립하여 주기적인 대단위 웹 사이트 점검이 가능해야 한다.

4.2 가상화를 통한 신종 악성코드 simulation 예측

보통의 APT 공격은 웹, 메일 등의 다양한 공격 경로를 통해 공격이 진행되고, 공격자들은 성공적으로 공격을 수행하기 위해 단계를 밟아가며 공격을 한다. 이처럼 다단계로 공격을 수행하게 되면, 시그니처 기반과 블랙리스트 기반을 사용하는 기존의 보안 솔루션의 방어를 무력화하기 때문에 공격을 탐지하기가 어렵다.

왜냐하면 공격자들은 실시간으로 공격의 형태를 바꾸기도 하고, 알려지지 않은 취약점을 이용하는 등의 동적인 공격을 감행하고, HTTP나 FTP같은 자주 사용하고, 잘 알려져 있는 서비스를 이용하기 때문이다.

따라서 기존의 패턴 매칭, 시그니처 기반의 정적인 탐지 모델은 동적이면서 실시간으로 알려지지 않은 위협을 탐지할 수 있는 가상화를 이용한 탐지 모델로 발전이 필요하게 되었다.

이러한 신종 악성코드를 예측하고 대응하기 위해서는 가상화를 이용한 시뮬레이션 예측이 필요하다. 가상화를 통한 시뮬레이션 예측을 통해 공격자의 의도와 공격 방법을 파악하고, 이에 대한 위협을 실시간으로 제거할 수 있다[15].

또한 동일한 환경을 가상 머신에 올려 시뮬레이션하기 때문에 오탐이 거의 없고, 실제 시스템에 영향을 미치지 않아 위험성이 적어 유용하게 사용이 가능하다.

4.3 실시간 웹 악성코드 탐지 방안

기존의 솔루션들은 앞서 말했듯이 증거값(Signature)을 이용한 분석이 대다수이다. 하지만 이 시그니처 기반은 코드의 변경 및 유포지·경유지의 변경만으로도 쉽게 탐지를 회피할 수 있다. 따라서 시그니처에 근거하여 탐지를 하기에는 한계점이 존재한다. 이러한 한계점을 극복하기 위해 기존의 웹 크롤링(Web-Crawling)을 이용한 동적 분석방식을 이용한다.

웹 크롤링은 여러 웹 사이트 데이터의 최신 상태 유지를 위해 웹을 구성하고 있는 Node와 Edge로 이루어진 정적HTML 페이지와 하이퍼링크(HyperLink)를 탐색하여 URL List에 추가한다. 이렇게 수집한 크롤링 정보를 다시 필터링을 통해 악성코드가 포함된 URL을 구분한다. 그리고 가상 PC를 이용해 클라이언트 허니팟을 만들어 수집된 URL을 직접 방문한다. 방문 후에 생성되는 파일의 행위를 모니터링하고 메모리, 프로세스, 레지스트리의 상태변화를 확인해 악성코드의 감염여부를 판별할 수 있다[16].

위에서 사용된 클라이언트 허니팟은 저 상호작용 클라이언트 허니팟과 고 상호작용 클라이언트 허니팟으로 나뉘게 된다. 저 상호작용 클라이언트 허니팟은 OS나 애플리케이션의 핵심 기능만 구현해 비교적 가볍고 빠른 처리가 가능하지만, 핵심 기능만 구현되어 있기 때문에 모든 공격에 대한 탐지가 불가능하다. 고 상호작용 클라이언트는 OS와 애플리케이션의 모든 기능을 사용해서 제약사항은 없지만 비교적 속도가 느리다[17].

고 상호작용 클라이언트 허니팟처럼 전체 기능을 포함하여 구현하면 모든 기능을 사용할 수 있지만, 속도가 느리다는 단점이 있다. 그래서 이를 해결하기 위한 측면으로 취약점에 노출되어 파생되는 프로세스 및 쓰레드의 이벤트를 비교 탐지하는 모듈이 개발되었다. 이 모듈은 웹 애플리케이션 취약점을 공격하는 3단계의 프로세

스를 기반으로 한다[18].

① 악성 URL에 최초 방문 시 방문자의 웹 브라우저 및 웹 애플리케이션들의 버전을 확인하고 가장 취약한 웹 애플리케이션을 공격하기 위한 링크로 이동

② 가장 취약한 웹 애플리케이션의 취약점을 공격해 쉘 코드를 실행시켜 악성코드를 drive-by-download

③ 2번째에서 다운로드 및 설치된 악성코드를 실행

따라서 위의 프로세스를 토대로 최초 링크에서부터 쉘 코드가 실행될 때까지의 방문 링크들을 참조하면 어떤 애플리케이션의 취약점을 이용하는지 알 수 있다. 또 웹 브라우저의 다운로드 이벤트 그리고 프로세스 및 쓰레드 생성 이벤트를 탐지하고, 웹 브라우저에서 파생되는 모든 프로세스와 쓰레드의 행동을 추적한다. 이렇게 하면 최초 악성링크 방문부터 쉘 코드의 실행 그리고 최종 악성 코드의 행위까지 전체적인 악성 행위를 탐지할 수 있다[18].

〔그림 5〕 웹 애플리케이션 취약점 공격 프로세스

4.4 정상 모델링 기법

악성행위를 탐지하는 기법 중 정상행위를 미리 모델링해서 만들어진 값을 벗어나는 비정상행위를 탐지하는 비정상행위 기반의 탐지기법이 있다.

정상행위를 모델링하는 기법에는 통계적(Statistical) 방법, 전문가 시스템(Expert System), 신경망(Neural Networks), 컴퓨터 면역 시스템(Computer Immune System), HMM(Hidden Markov Models), 데이터 마이닝(Data Mining) 등의 방식이 이용된다.

4.4.1 통계적 기법

통계적 기법의 대표적인 시스템으로는 SRI(Stanford Research Institute) International에서 개발한 NIDES가 있다. NIDES는 정해준 규칙에 따라 분석을 하여 악의적인 행위를 탐지하는 기법과 통계적인 분석을 통해 비정상적인 행위를 탐지하는 기법을 함께 사용한다.

통계적인 분석에 사용되는 값으로는 CPU 사용 시간, I/O 활동, 메모리 사용 등 사용자가 컴퓨터에서 행할 수 있는 다양한 행위를 장기간에 걸친 프로파일링과 단기간 프로파일링을 비교하는 방식으로 비정상행위를 탐지한다[19][20].

4.4.2 전문가 시스템 기법

전문가 시스템 기법은 비정상 행위를 탐지하기 위해 특정 기간 동안 사용자 행위를 기록하고, 그 기록을 이용하여 행위를 정의하는 규칙의 집합을 만든다. 이렇게 만들어진 규칙의 집합과 현재 행위를 비교하여 비정상 행위를 탐지한다. 이 기법은 정책 기반을 사용하는 프로파일에는 효과적이지만 대량의 정보를 처리하는데 비효율적이다〔21〕.

4.4.3 신경망 기법

신경망 기법은 통계적 기법과 유사한 부분이 존재하나 이에 비해 값들 간의 비선형적 관계를 나타내기가 유용하며 자동적인 학습이 가능하다. 대표적인 시스템에는 Hyperview가 있다〔21〕.

4.4.4 컴퓨터 면역 시스템 기법

컴퓨터 면역 시스템 기법은 사람의 몸이 상처나 감염에 대응하는 면역 체계에서 고안되었다[22]. 컴퓨터 면역 시스템에 대한 연구는 University of New Mexico에서 활발히 진행되고 있다[21]. 컴퓨터 면역 시스템이 갖춰야하는 규칙에는 여러가지가 있지만 그 중 몇 가지를 살펴보면 먼저 보안을 중앙 제어가 아닌 해당 지역 내에서 분산 처리할 수 있어야 한다. 또한 앞으로 증가할 네트워크나 CPU속도, 모바일 코드 사용 확산으로 인한 대부분의 보안 문제에 대해서 관리나 유지 보수 없이 시스템이 동작할 수 있어야 한다. 이러한 규칙 외에도

불완전한 탐지를 해야 하고, 방어할 수 있는 범위가 동적이어야 하는 등의 여러 가지 규칙이 있다[23].

이러한 면역 시스템은 사용자 기반이 아닌 서비스의 정상행위를 모델링 한다. 서비스의 정상적인 행위를 모델링 한 후 알려진 모든 system call의 정상 시퀀스를 포함한 참조 테이블을 추출하고 해당 시퀀스가 테이블에 있는지 비교한다[21].

4.4.5 HMM

HMM은 모델을 구성하는 상태들간의 전이가 어떠한 확률 값을 통해 이루어진다. 이 모델은 순차적 데이터 인식을 위해 다양하게 사용된 모델이다[24]. HMM이 처음 활용된 분야는 음성인식 분야였으나 이후 정보추출, 정보검색, 사용자의 프로파일링 등 다양한 분야에 사용되었다[25].

Ⅴ. 결 론

지금 까지 살펴본 바와 같이 APT는 악성코드의 생존율을 높이기 위해 다단계의 공격을 거쳐 공격 거점을 마련하고, 장기적으로 원하는 목적이 달성될 때까지 공격한다. 특히 이런 APT에 이용될 수 있는 악성코드의 대량 배포는 웹 사이트를 통해 더욱 활발히 일어나고 있다. 이처럼 우리를 위협하는 공격은 점점 더 지능화되고 있기 때문에 시그니처를 기반으로 하는 기존의 솔루션으로 탐지하고 방어하기에는 많은 한계점들이 존재한다.

따라서 이러한 한계점을 극복하기 위해서 첫째로는 악성 웹사이트를 탐지하고 대응하기 위한 WhiteList 기반의 악성코드 탐지 기술을 사용해야 한다. 둘째, 가상환경에서 신종 악성코드의 시뮬레이션 예측을 통해 공격자의 의도와 공격 방법을 파악하고 이에 대한 대응을 해야 한다. 셋째, 실시간으로 웹 악성코드를 탐지하기 위해 동적인 분석 방식을 이용해야 한다. 마지막으로 정상 행위를 모델링 해 정상값을 만들어 놓은 후 이에 벗어나는 행위를 탐지하는 비정상행위 기반의 탐지기법을 이용해야한다.

APT는 보안 솔루션을 도입한다고 해서 그 근본적인 문제 해결은 불가능하다. 지금까지 소개 했던 대응 방안들을 토대로 일회적인 대응이 아닌 지속적으로 APT를 방어할 수 있는 체계적인 대응 방안을 구축해야 할 것이다.

약 어 정 리

API	Application Programming Interface
APT	Advance Persistent Threat
DDoS	Distributed Denial of Service
DNS	Domain Name Service
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
URL	Uniform Resource Locator
XSS	Cross Site Script

참 고 문 헌

[1] Facebook 홈페이지 공지사항, https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766, Oct. 2013.

[2] “Department of Labor Watering Hole Attack Confirmed to be 0-Day with Possible Advanced Reconnaissance Capabilities”, Cisco blog, 2013.

[3] “Microsoft Internet Explorer CDwnBindInfo Object Processing Use-After-Free Vulnerability”, Cisco vulnerability alert, 2013.

[4] 길민권, “中 해커, IE 제로데이 취약점 이용 美 외교협회 공격!”, 데일리시큐, 2013.

[5] 김태형, “안보관련 연구소 대상 ‘워터링 홀’ 공격 발생!”, 보안뉴스, 2013.

[6] 데피드 스터타드, 마커스 핀토, “웹 해킹&보안 완벽 가이드”, 조도근, 김경곤, 장은경, 이현정(역), 에이콘, pp.50, 2008.

[7] “Internet Security Threat Report 2013”, Symantec, pp.21, 2013.

[8] “사례위주로 살펴본 ActiveX 취약점 공격 및 방어기법“, VMCraft

[9] 신영웅, 전상훈, 임채호, 김명철, “국가 사이버보안 피해금액 분석과 대안-3.20 사이버 침해사건을 중심으로-”, 국가정보연구, 제 6권, 제 1호, pp.134-135, 2013.

[10] “인터넷 침해사고 대응통계”, KISA, Oct. 2013.

[11] “월간 악성코드 은닉사이트 탐지 동향 보고서”, KISA, 2013.
[12] “홈페이지 은닉형 악성코드 유포 패턴 분석방법 연구”, 한국인터넷진흥원, pp.46-56, Oct.2010.
[13] 하정우, 김휘강, 임종인, “WhiteList 기반의 악성코드 행위분석을 통한 악성코드 은닉 웹사이트 탐지 방안 연구“, 한국정보보호학회 제 21권 제 4호, pp.62, Aug.2011.
[14] 하정우, 김휘강, 임종인, “WhiteList 기반의 악성코드 행위분석을 통한 악성코드 은닉 웹사이트 탐지 방안 연구“, 한국정보보호학회 제 21권 제 4호, pp.66-67, Aug. 2011.
[15] “지능형 표적 공격 차세대 사이버 공격을 방어하는 방법”, FireEye, 2013.
[16] 김탁호, “해시 값을 이용한 악성코드 탐지 효율성 향상 방법 연구”, 건국대학교 정보통신대학원 정보통신학과, pp. 5-7, Aug. 2012
[17] 이영욱, 정동재, 전상훈, 임채호, “웹 브라우저 기반 악성행위 탐지 시스템(WMDS)설계 및 구현”, 한국정보보호학회 제 22권 제3호, pp.668, June. 2012.
[18] 이영욱, 정동재, 전상훈, 임채호, “웹 브라우저 기반 악성행위 탐지 시스템(WMDS)설계 및 구현”, 한국정보보호학회 제 22권 제3호, pp.672-673, June. 2012.
[19] Debra Anderson, Thane Frivold, Ann Tamaru, Alfonso Valdes, “Next generation intrusion detection expert system (NIDES)”, SRI International, pp38, Dec, 1994.
[20] Debra Anderson, Thane Frivold, Ann Tamaru, Alfonso Valdes, “Next generation intrusion detection expert system (NIDES)”, SRI International, pp50 Dec, 1994.
[21] 박혁장, “침입탐지시스템의 성능향상을 위한 다중 척도 모델링기법 연구”, 연세대학교 대학원 컴퓨터과학과, pp.14-15, June. 2002.
[22] Anil Somayaji, Steven Hofmeyr, Stephanie Forres, “Principle of a Computer Immune System”, Department of Computer Science University of New Mexico Albuquerque, pp.3, 1998.
[23] Anil Somayaji, Steven Hofmeyr, Stephanie Forres, “Principle of a Computer Immune System”, Department of Computer Science University of New Mexico Albuquerque, pp.4, 1998.
[24] 엄재홍, “은닉마르코프모델을 이용한 정보추출”, 서울대학교 대학원 컴퓨터공학과, pp.3, Feb. 2001.
[25] 엄재홍, “은닉마르코프모델을 이용한 정보추출”, 서울대학교 대학원 컴퓨터공학과, pp.9-11, Feb. 2001.

〈저 자 소 개〉

임 설 화 (Sul-Hwa Im)
학생회원

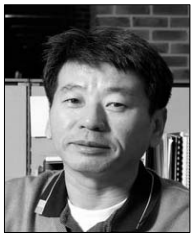
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 모바일 보안, 보안 컨설팅, 클라우드 컴퓨팅 보안, 네트워크 보안

김 종 수 (Jong-Soo Kim)
학생회원

2011년 2월 : 대구대학교 전산학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 네트워크 프로그래밍, 침투테스트, 네트워크보안

양 준 근 (Jun-Keun Yang)
학생회원

2013년 2월 : 한림대학교 전자물리학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 디지털포렌식, 암호



임 채 호 (Chae-ho Lim)
종신회원

1986년 : 홍익대학교 전산학과 학사
2001년 : 홍익대학교 전자계산학과 박사
2006년~2009년 : NHN(주) 보안실 실장, 연구센터 수석
2009년 : 한국정보보호학회 부회장
2010년 8월~현재 : KAIST 사이버보안연구센터 연구부소장
2011년 2월~현재 : KAIST 정보보호대학원 연구교수
관심분야 : 인터넷 보안, 정보보호 위험 관리, 정보보호 관리 및 정책