情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

사이버 환경에서의 보안위협

김 지 훈*, 조 시 행**

요 약

정보시스템과 인터넷의 발전은 모든 정보 자산의 네트워킹이 가능해짐에 따라, IT 인프라를 중심축으로 한 정보사회 발전의 견인차 역할을 하였다. 최근에는 참여·공유·개방으로 대변되는 웹 2.0 기술과 함께 가히 폭발적인 스마트폰 시장 환경이 맞물리면서 "모바일 웹 2.0"시대로의 빠른 진화를 거듭하고 있다. 하지만 그에 따른 정보사회의 역기능도 만만치 않게 나타나고 있다. 우리는 이미 해킹 및 악성코드로 인한 정보 유출 피해를 비롯하여 서비스 거부 공격으로 인한 비즈니스 연속성 침해에 이르기까지 끊이지 않는 사이버 침해사고를 겪고 있다.

본 논문에서는 진화하고 있는 악성코드에 대한 최근 동향 분석을 통해 미래 정보 사회를 주도할 소셜 네트워킹 환경에서의 보안위협이 어떻게 진화해 나가고 있는지 살펴보고자 한다. 또한 사이버범죄 및 사이버전쟁의 사례 분석을 통해 사이버 보안 문제에 대한 보다 적극적인 대응책 마련이 필요하다는 사회적 인지와 인식이 확립되고 보다 강력하고 안전한 대응 체계를 위한 우리의 노력이 끊임없이 연구되길 기대해 본다.

Ⅰ. 서 론

인터넷의 개방성 및 표준화, 인터넷 시스템의 복잡도(Complexity) 증가, 새로운 서비스 및 컨텐츠 시장 형성, IT 시스템에 대한 의존도 심화, 악성코드와 해킹 기술이 고도로 발달, 인터넷을 통해 악의적인 컨텐츠가 손쉽게 유통될 수 있는 구조가 되면서, IT 자산에 대한 보호가 점차 어려워지게 되었다.

또한, 웹 2.0과 모바일 환경이 결합된 모바일 웹 2.0 환경에서의 소셜 네트워크 서비스의 급속한 확산, 가상화 기술, 클라우드 컴퓨팅 등 새로운 미래 IT 패러다임의 변화속에서 새로운 형태의 보안위협에 대한 우려도 점차 증가하고 있다.

따라서 본 논문에서는 최근 악성코드 동향을 분석하고 악성코드와 결합된 다양한 보안위협의 사례 분석을 통해 효율적인 악성코드 대응 방안을 모색해보기로 한다. 본 논문의 2장에서는 2010년 상반기 주요 악성코드 동향 분석을 통해 최신의 보안위협 트렌드에 대해 살펴보고자 한다. 3장에서는 소셜 네트워킹 환경에서의 보안위협 사례 분석을, 4장에서는 사이버범죄 및 사이버전쟁의 사례 분석을 통해 미래 사회에서 나타날 수 있는 사이버 보안위협의 형태에 대해 예견해보고 이에 대한 효율적인 대응방안을 모색하고자 한다. 마지막으로 5장에서는 결론 및 향후 연구방향을 제시한다.

Ⅱ. 2010년 상반기 악성코드 동향

악성코드를 이용한 공격은 금전적인 목적으로 조직적인 형태로 진화하고 있고, 특정 공격 대상을 위한 타게팅 공격 (Targeted attack) 형태를 띄고 있으며, 국지

〔표 1〕 악성코드 제작 동기의 변화

과거	현재
개인	조직적인(coordinated) 범죄
아마추어	프로페셔널(sophisticated)
불특정다수	특정 목표 (targeted) 공격
글로벌	국지적 양상 (Local)
소란 일으키기	잠복형태
자료파괴/변조	정보유출
바이러스	바이러스+웜+트로이목마+스파이웨어+...

* 안철수연구소 ASEC(AhnLab Security E-response Center) 분석2팀장 (smallj@ahnlab.com)
** 안철수연구소 연구소장 (shcho@ahnlab.com)

〔그림 1〕 악성코드 전개 양상

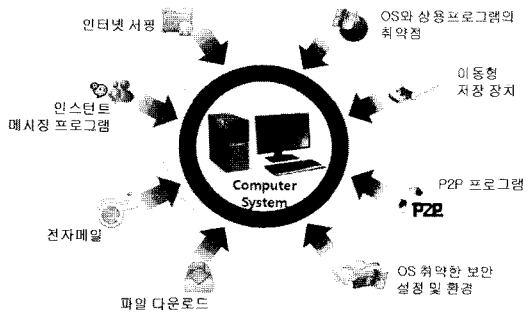
적인 양상을 보이기도 한다.

또한, 클라우드 컴퓨팅 (Cloud Computing), 스마트폰 (Smart Phone), 소셜 네트워킹 (Social Networking), 윈도우 7 (Windows 7) 등 새로운 IT 패러다임의 변화에 맞게 보안위협도 복잡하고 복합적인 양상을 보이게 된다.

공격자는 정보 유출, 분산 서비스 거부 공격 등의 목적 달성을 위해 악의적인 컨텐츠 유통을 활발하게 전개하고 있다. 운영체제 취약점, 웹, 이메일, 메신저 등의 전통적인 감염 경로 외에도 응용 프로그램의 취약점, P2P 프로그램, USB 이동형 저장 장치 등의 다양한 감염 경로를 통해 지속적인 피해를 유발하고 있다.

2010년 주요 상반기 악성코드 동향은 다음과 같다.

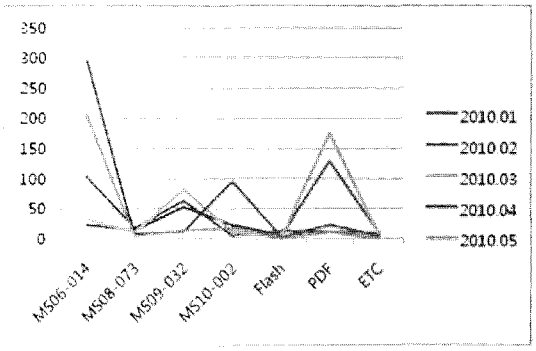
- 웹 플랫폼을 이용한 악성코드 유포
- 사회공학적 기법을 활용한 악성코드 유포
- 소셜 네트워킹 환경과 결합된 보안위협 증가
- 제로 데이 취약점을 악용하는 타게팅 공격
- 가짜 백신으로 인한 피해 증가
- 진단, 치료가 어렵도록 발전하는 악성코드
- 스마트폰 보안위협에 대한 관심 증가



〔그림 2〕 다양한 악성코드의 주요 감염 경로

〔표 2〕 웹 사이트 보안 요약

구분	4월	5월
악성코드 발견 건수	111,045	142,613
악성코드 유형	926	930
악성코드가 발견된 도메인	1,028	1,084
악성코드가 발견된 URL	3,898	4,950



〔그림 3〕 주요 취약점 통계

2.1. 웹 플랫폼을 이용한 악성코드 유포

안철수연구소의 ASEC Report Vol.5 의 웹 보안 동향에 따르면, 2010년 5월의 악성코드 발견 건수는 142,613 건이고, 악성코드 유형은 930건이며, 악성코드가 발견된 도메인은 1,084 건이며, 악성코드가 발견된 URL은 4,950 건이다. 2010년 4월보다는 다소 감소하였으나, 악성코드 발견 건수, 악성코드 유형, 악성코드가 발견된 도메인, 악성코드가 발견된 URL은 증가하였다.

월별 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 주요 취약점들에 대한 통계이다. 마이크로소프트 인터넷 익스플로러, 어도비 PDF 리더, 플래쉬 플레이어 등의 웹 브라우저, 문서 취급 프로그램의 취약점을 이용한 공격이 활발하게 진행되고 있음을 확인할 수 있다.

2.2. 사회공학적 기법을 활용한 악성코드 유포

최근 악성코드 유포를 위한 공격 기법은 사회공학적 기법을 수반하는 경우가 많다. 사회공학적 기법은 사회의 소통 문화의 흐름과 밀접한 연관성을 갖고 있다. 사람은 가장 취약한 정보 개체로 일컬어지고 있다. 눈에 보이는 욕심에 마음이 동요되기도 하고, 권력에 의한 명

령·지시에 여과없이 따르기도 하며, 세상의 관심사에 쉽게 노출될 수 있는 약한 존재이다. 이렇듯 외부의 다양한 환경에 의해 동일한 사람임에도 매번 다른 행동(결과)을 수반하게 된다. 공격자는 이러한 사람의 취약성을 공격하여, 자신이 원하는 의도에 맞게 행동할 수 있도록 유도하는 사회공학적 기법을 즐겨 사용하게 된다.

사회공학적 기법을 가장 활발하게 이용하는 통신 수단으로는 '이메일'을 꼽을 수 있다. 다음은 2010년 ASEC Threat Research 블로그를 통해 소개된 대표적인 사회공학적 기법의 '이메일' 사례들이다.

- "BC카드 이용대금 명세서" 통지 메일 위장
- "남아공 월드컵" 관련 메일 위장
- "AOL 메신저" 관련 메일 위장
- "UPS·DHL" 운송장 관련 메일 위장
- "입사 이력서" 메일 위장

공격자는 이메일 수신자를 현혹시킬 수 있는 본문 내용과 함께 악성코드 유포를 위한 악의적인 URL, 혹은 첨부파일을 함께 전달한다. 이메일 수신자가 별다른 의구심 없이 이메일의 첨부파일이나 URL 링크를 클릭하게 되면 연결된 악성코드가 PC를 감염시킴으로써 공격자가 내부 네트워크에 손쉽게 침투할 수 있는 활로를 열어주는 계기가 된다. 이렇듯 사회공학적 기법에서 사람을 현혹시키고 행동하게 만드는 주요 요소는 다음과 같다.

- 신분위장 (Impersonation)
- 신뢰관계형성 (Trust)
- 강한 영향 (Overloading/Strong Affect)
- 긴급성 (Urgency)
- 도덕적 책무 (Moral Duty)

2.3. 소셜 네트워크 서비스와 결합된 보안위협 증가

■ 트위터 봇넷 악성코드

2010년 5월에는 트위터 채널을 통해 봇넷C&C 서버를 구성하는 악성코드가 발견되었다. 지금까지 소셜 네트워크 서비스 관련 악성코드는 사용자 계정이나 버디 계정에 스팸성 메시지를 달거나 악성코드가 업로드된 사이트로 유도하는 게 일반적인 악용 방법이었다.

그러나 최근 발견된 악성코드는 먼저 악의적으로 생성한 사용자 계정이나 이미 훔쳐낸 계정을 통해 악성코드를 제어하는 C&C명령을 트윗한 후 악성코드가 이를 읽어 들인 후 악의적인 행동을 취하게 된다.

- 악의적인 트위터 계정을 생성하거나 다른 사람의 계정을 도용하여 공격 준비
- 트위터 봇 자체를 전송하거나 트위터 봇이 위치한 URL 주소를 클릭하도록 사회공학적 기법을 이용하여 유도함
- 트위터 봇에 감염되면, 사전 정의된 트위터 계정에 접속하여 미리 게시된 트윗 형태의 공격자의 지령을 받아 공격 명령을 수행하게 됨.

트윗 형태의 공격자 지령은 다음과 같다.

```
>
.DOWNLOAD*link.com/direct.exe*cutomnamefor.exe*0 [ 0 = Download, 1 = >  Download & Exec ]
> .DDOS*IP*PORT [ UDP  Attack ]
> .VISIT*link.com/video*0 [ 0 = Invisible, 1 = Visible ]
> .SAY*Hello my  infectants! [ Fun, useless command, Text To Speech ]
> .STOP [ Stops all  current processes. DDOS, Visiting.]
> .REMOVEALL [ Removes  all bots connected. ]
```

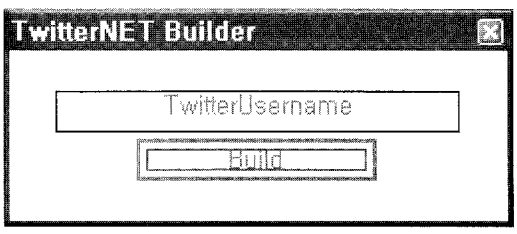
이미 트위터를 생성하는 도구도 나와 있어, 트위터 봇 프로그램을 쉽게 생성할 수 있다.

트위터가 대중적으로 이용되고 있는 만큼 공격자들은 트위터와 같은 SNS 환경을 공격을 위한 도구로 활용하는 사례가 늘어나고 있다. 이번 트위터 봇넷은 앞으로 발생할 수 있는 SNS를 이용한 공격의 시작일지도 모른다.

2.4. 제로데이 취약점을 이용하는 타게팅 공격

악성코드 유포 및 내부 PC 감염을 위해서는, 제로데이(0-day) 취약점이 주로 이용된다. 이 제로데이 공격은 해당 벤더사에서 보안패치를 내놓지 않은 상태의 제로데이 취약점을 공격하는 것을 말한다. 2010년 상반기 대표적인 제로데이 취약점은 다음과 같다.

- 인터넷 익스플로러 (CVE-2010-0249, MS10-002)



〔그림 4〕 트위터 봇을 생성하는 도구 화면 예제

- 인터넷 익스플로러 (CVE-2010-0806, MS10-018)
- 어도비 플레쉬 플레이어 (CVE-2010-1297, APSB10-14)
- 윈도우 도움말 및 지원센터 (CVE-2010-1885)

악성코드 유포의 성공률을 높이기 위해 하나 이상의 공격코드를 사용하게 되는데, 이러한 제로데이 취약점 공격코드가 많이 이용되는 경우 보호되지 않는 사각지대를 공격하게 되면, 보안패치가 제공되기 이전의 운영체제 및 응용 프로그램 취약점을 통해 내부 PC 감염을 손쉽게 달성할 수 있다.

제로데이 취약점을 이용하는 공격 방법은 크게 다음과 같이 분류할 수 있다.

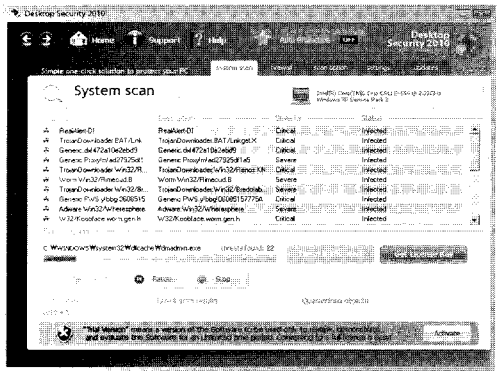
- 직접 근접/원격 시스템의 취약점을 검색하여 전파하는 방법 (ex. 컨피커 웜, MS08-067)
- 사회적 이슈와 결합된 사회공학적 기법을 통해 전파하는 방법 (주로 이메일의 첨부파일 형태, 문서 프로그램의 취약점)
- 웹 공격 툴킷 (Web Exploit Toolkit)을 이용한 웹 공격 (ex. IE 취약점, ActiveX 취약점)

2.5. 가짜 백신으로 인한 피해 증가

가짜 백신으로 인한 사용자 피해가 끊이질 않고 있다. 과거 가짜 백신은 ActiveX 컨트롤을 통해 불특정 다수의 사이트에서 배포되었는데, 여러 보안 업체 및 관련 기관의 노력으로 인해 그 수가 많이 줄어 들었다. 하지만 최근 가짜 백신은 보안취약점, 다른 애드웨어의 번들 또는 업데이트 프로그램을 사용, 웹 하드와 같은 인터넷 서비스의 제휴 프로그램으로 설치하는 사례가 부쩍 늘어나고 있다.

이렇게 설치된 가짜 백신의 경우 사용자 컴퓨터를 정상적으로 사용할 수 없도록 파일의 실행을 차단하거나, 바탕화면을 변경시켜 사용자의 불안감을 조성하고 허위 또는 과장된 진단 결과를 지속적으로 노출시켜 사용자의 유료 결제를 유도한다.

이러한 가짜 백신은 사용자 몰래, 또는 의도하지 않은 상태에서 설치된다. 가짜 백신으로 인한 피해를 막기 위해서는 새로운 프로그램을 설치하거나 서비스를 사용하게 될 경우, 무조건 "예"를 눌러 진행하지 말고 추가로 설치되는 프로그램이 있는지 잘 살펴보아야 하며 해당 프로그램이나 서비스가 나에게 정말 필요한 것인가를 다시 한번 살펴보고 진행하는 것이 중요하다.



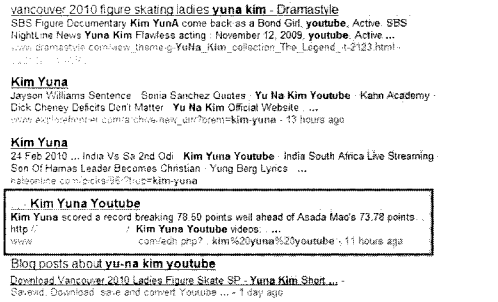
〔그림 5〕 사용자 동의 없이 설치된 가짜 백신

2010년 2월 24일 캐나다 밴쿠버 동계 올림픽에서 김연아 선수가 멋진 연기로 금메달을 획득하였다. 김연아 선수의 피겨 스케이팅 경기가 전세계로 중계된 이후 구글(Google) 검색 웹 사이트에서 김연아 선수의 동영상을 위장한 악성코드가 유포되었다.

이번 구글 검색 웹 사이트를 통해 유포된 허위백신은 2009년 이전부터 해외에서 악성코드 유포에 많이 악용되었던 BlackHat SEO (Search Engine Optimization) 이라는 기법이 사용되었다. 구글 검색 웹사이트에서 특정 단어를 입력하여 검색을 할 때 구글 검색 엔진의 랭킹(Ranking) 순위가 특정 알고리즘에 의해 가장 유사도가 높은 웹사이트가 첫 번째 페이지에 제공된다. 이러한 사항을 악용하여 BlackHat SEO 기법은 악성코드를 유포하기 위한 웹 사이트를 검색 결과 페이지의 상위권에 나타나도록 조작하는 기법이다.

2.6. 진단, 치료가 어렵도록 발전하는 악성코드

최초의 악성코드가 발견된 시점부터 지금까지 악성



〔그림 6〕 BlackHat SEO 기법을 이용한 가짜백신 유포

코드 제작자와 보안 전문가들의 쫓고 쫓기는 싸움은 계속되어 왔다. 매체가 다양해지면서 악성코드가 활용할 수 있는 전파경로도 확장되었고, 보안기술과 소프트웨어, 보안장비 등의 진보로 이를 우회하기 위한 악성코드 제작자들의 노력도 발전되어 오고 있다. 최근 악성코드에서는 기본적으로 탑재되는 다음과 같은 특징을 발견할 수 있다.

- 가상화(Vmware, VirtualBox)와 디버그(Ollydbg, Windbg) 환경 탐지
- 각종 분석툴, 보안프로그램에 대한 무력화 기능
- 자기 은폐 및 정보 수집을 위한 Hooking 기능
- C&C(Command and Control) 서버와의 통신 및 자체 업데이트를 위한 기능
- 탐지와 분석을 방해하는 암호화 기능

또한, 악성코드 제작자들도 제작된 악성코드가 백신 프로그램에서 기진단이 되는지 여부를 미리 체크할 수 있는 QA(Quality Assurance) 과정, 하나 이상의 악성코드를 배포하여 서로의 상태 정보를 크로스체킹하도록 하고, 악성코드가 보안 프로그램에 의해 무력화되는 경우 새로운 버전으로 신속하게 업데이트될 수 있도록 해주는 DR(Disaster Recovery) 기능을 제공하는 사례가 점점 많아지고 있다.

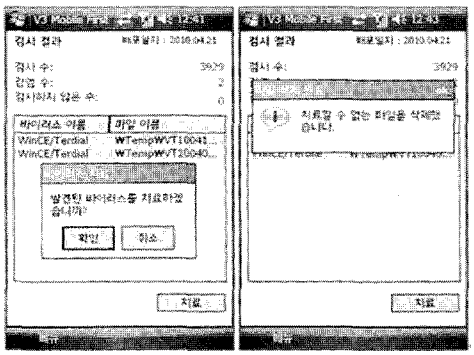
2.7. 스마트폰 보안위협에 대한 관심 증가

최근 들어 스마트폰 사용자가 많아지고 다양한 스마트폰 OS가 선보이고 있다. 국내에도 본격적인 스마트폰 시대의 장이 열려 PC에서 하던 일을 "내 손안의 PC"를 통해 언제 어디서든 할 수 있게 되었다.

스마트폰은 휴대용 단말기로, PC 환경에서 일어나고 있는 많은 보안위협들이 그대로 적용될 수 있다. 현재까지 알려진 모바일 악성코드의 주요 특징은 통화 기록이나 전화번호, 사진 등의 개인정보 탈취, 비정상 트래픽을 유발하여 과금을 유도하거나 배터리 소진시키는 것이 일반적이다.

모바일 악성코드의 대표적인 특징은 다음과 같다.

- 파일 실행 차단
- 파일 감염 및 덮어 쓰기
- 휴대폰의 원격 제어
- 응용 프로그램 혹은 아이콘의 변경
- Bluetooth 혹은 MMS를 통한 확산
- SMS 메시지 전송을 통한 부당 요금 발생



〔그림 7〕 V3 Mobile을 이용한 WinCE/TredDial.a (국제전화 무단발신 기능을 갖는 악성코드) 진단/치료 화면

- 메모리 카드 차단
- 사용자 데이터 은닉 및 도난
- 프리미엄 서비스 무단 접속 및 국제전화무단 발신으로 부당 요금 발생
- 사용자의 SMS 훔쳐보기
- 휴대폰의 정보 유출
- 다른 악성코드의 설치
- 휴대폰을 이용해 PC에 악성코드 설치

스마트폰 보안은 단지 몇가지 보안 기능을 제공하는 것보다 생태계(Eco-system) 전반의 보안 수준을 높이는 것이 중요하다. 악성코드뿐 아니라 피싱, 스파이웨어, DDoS (분산서비스거부공격) 등은 물론 도난 방지, 인터넷 뱅킹 보안 등 각종 보안 위협이 있을 수 있다. 따라서, 다양한 보안 솔루션 및 생태계 보안까지 다각도의 보안위협 대응 연구가 절실히 필요하다.

보안을 위한 보안이 아니라, 보안이 담보된 편리한 사용 환경을 뒷받침 하는 '스마트한' 보안이 중요하고, 폭넓은 관점에서의 접근이 필요한 이유이다.

Ⅲ. 소셜 네트워킹 환경에서의 보안위협

참여 · 공유 · 개방의 정신을 담은 웹 2.0 기술은 스마트폰 기반의 모바일 환경과 접목되면서 "모바일 웹 2.0 시대"로 강력한 진화를 진행해가고 있다. 이러한 엄청난 폭발력과 확장세의 중심에는 단연코 소셜 네트워크 서비스 (Social Network Service, 이하 SNS)가 우뚝 서 있다. SNS는 참여하는 구성원 개개인의 다양성을 존중하며 개인 · 기업의 새로운 소통의 도구로 자리매김하고 있다. SNS의 대표적인 서비스에는 '마이스페이스',

'LinkedIn', '페이스북'과 '트위터' 등을 들 수 있다. 이러한 SNS 서비스가 전세계의 소통의 플랫폼으로 발전해 나가고 있다.

하지만 SNS의 인기가 높아지면서 그에 대한 보안위협도 증가하고 있다. SNS의 활용과 그 중요성이 점차 증가함에 따라 발생할 수 있는 SNS 환경에서의 역기능은 어떤 것이 있는지 살펴보도록 하자.

3.1. SNS를 주제로 한 사회공학적 공격 기법

SNS와 연관된 주요 보안위협 사례는 다음과 같다.

악의적인 컨텐츠 유통에는 전통적인 방식의 이메일, 메신저 등의 커뮤니케이션 채널이 활용되지만 SNS와 연관된 내용을 주제로 다루게 되어, 보다 강력한 사회공학적 기법을 통해 사용자를 현혹시킴으로써 성인물, 성인약품 광고를 위한 스팸봇, 정보유출용 트로이목마와 같은 악성코드 유포, 허위백신 유포, 계정정보 및 신용카드 정보 탈취를 위한 피싱 웹사이트로의 링크 전송 등의 피해를 유발하고 있다.

〔표 3〕 SNS를 주제로 한 보안위협 사례들

목적	수단 (내용)	년/월
악성코드유포	트위터 초대메일 위장	09/06
서비스거부	트위터 서비스 공격	09/08
봇넷C&C	트위터 계정 활용	09/08
봇넷C&C	구글 뉴스그룹 활용	09/09
악성코드유포	페이스북 암호변경 요청	09/09
악성코드유포	트위터 초대메일 위장	09/09
악성코드유포	페이스북 암호변경 요청	09/10
악성코드유포	페이스북 피싱 웹페이지	10/02
악성코드유포	트위터 다이렉트 메시지로 피싱 링크 전송	10/02
스팸메일	트위터 다이렉트 메시지	10/02
신용카드정보	트위터 메시지를 이용한 메신저 추가 요청	10/03
악성코드유포	페이스북 관리자로 위장	10/04
스팸메일	트위터 메일로 위장한 성인약품 광고	10/05
허위백신유포	구글 그룹스 활용	10/05
봇넷C&C	트위터 계정 활용	10/05
악성코드유포	단축URL 활용	10/05
허위백신유포	트위터 암호변경 요청	10/06
악성코드유포	페이스북 위장	10/06

또, 작년부터 지속적으로 악의적인 봇넷의 명령·제어 서버(C&C)로 활용됨에 따라, SNS 환경에서의 새로운 보안위협에 대한 시도가 꾸준히 이어지고 있음을 확인하게 된다.

3.2. SNS를 통한 과도한 개인 정보 노출

SNS는 특정 공격 대상으로의 타게팅 공격(Targeted Attack)에 앞서, 공격 대상(Target)에 대한 풍부한 정보 제공처 역할을 할 수도 있다.

인터넷을 사용하는 사람이면 누구나 개인 블로그, 개인 트윗들, 본인이 속한 집단의 웹사이트, 카페 커뮤니티 등의 다양한 소셜 네트워크 서비스를 통해 자기 PR이나 소속된 집단과의 소통을 향유하게 된다. SNS의 속성상 자신의 소속, 연락처, 취미, 활동내역, 개인사진 등의 대부분의 정보를 오픈한 상태에서 상호 신뢰성을 바탕으로 소통하기 때문에 이러한 과정에서 의도하지 않게 많은 개인 정보들이 노출될 수 있다.

공격자는 SNS 채널을 통해 공격 대상에 대한 수많은 정보를 획득할 수 있고, 이러한 정보를 통해 친밀감과 신뢰감을 형성할 수 있는 계기를 마련할 수도 있다. 무심코 게시한 일련의 정보를 통해 공격자가 나의 일거수일투족에 대한 모니터링이 가능해지며, 오랜 기간 동안 쌓아온 공격자와의 유대 관계를 통해 점차 보안 경계심이 사라져가는 순간, 공격자의 좋은 먹잇감이 될 수도 있다.

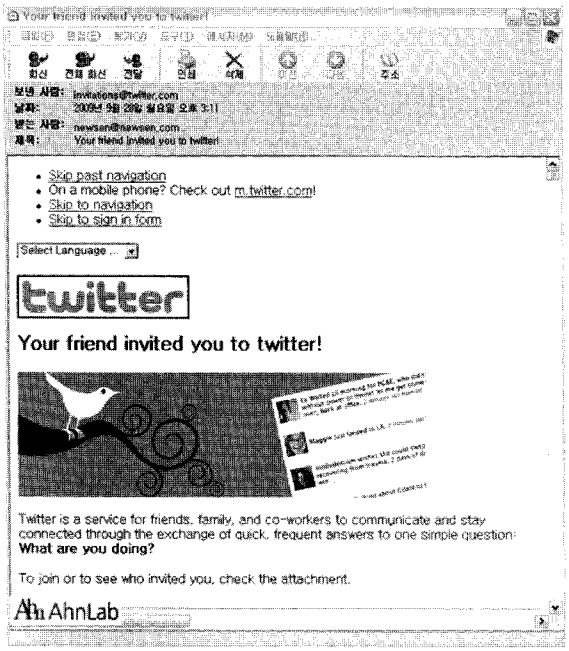
SNS 자체 검색 엔진 외에도 구글, 빙 등의 기존 검색 엔진이 SNS 검색에 대한 지원을 아끼지 않고 있어 개인 프로파일에 정보 수집이 한층 더 수월해질 것으로 보인다.

3.3. SNS을 통한 유해 컨텐츠 유통

우리는 이미 본 논문의 2장에서 소셜 네트워크 서비스와 결합된 보안위협을 통해 SNS 플랫폼을 악용한 보안위협이 꾸준히 증가할 것으로 예측하였다. 이외에도 SNS 플랫폼을 이용한 유해 컨텐츠 유통이 활발하게 전개될 것으로 예상된다.

국내에서도 많은 사용자 층을 확보하고 있는 '트위터' 서비스에서는 다음과 같은 보안위협이 존재한다.

- @(reply) 스팸

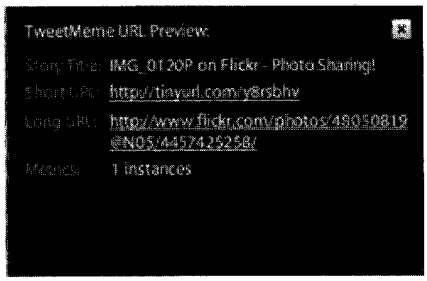


〔그림 8〕 트위터 초대장 메일 위장 악성코드 유포

- #(hash) 태그 스팸
- DM(Direct Message) 스팸
- 안전하지 않은 서드파티(3rd party) 서비스 연동 요청으로 인한 개인정보 유출 가능성
- 트위터 위장 피싱 웹사이트
- 트위터 메일 위장 악성코드 유포
- 신분위장, 허위정보 유포로 사회 혼란 야기
- 단문 URL 서비스를 통한 피싱, 악성코드 유포

140자라는 '트위터' 단문 서비스의 특성이 있어, 웹 컨텐츠의 위치 정보 공유시, 단문 URL 서비스가 많이 활용되고 있다. 그러나 악의적인 단문 URL이 유포될 경우 실제 연결되는 URL 주소를 쉽게 파악하기 어려워, 사용자 스스로 URL의 안정성에 대한 검증 과정을 거치기 어렵다는 우려하는 목소리가 제기되기도 한다. 다행히 단문 URL에 대한 안정성 검증을 지원하는 미리보기 기능 등의 다양한 서비스가 도입되고 있어 다소 위안이 되고 있다. 따라서, 사용자 스스로도 단문 URL에 대한 사전검증 절차를 거쳐 유해한 컨텐츠에 의한 피해를 입지 않도록 조심해야 할 것이다.

신분 위장 및 계정 도용도 중요한 보안위협 중 하나이다. 유명인을 사칭하거나 계정 도용을 통해 지인의 행사가 가능할 수 있으므로 그들과 인맥 네트워크를 형성하고 있는 많은 선의의 피해자를 유발시킬 수 있다.



〔그림 9〕 단축URL 미리보기 (출처: TweetDeck)

SNS 상에서의 허위 정보 유포는 사회 혼란이 야기될 수도 있다. SNS의 자정 능력에도 불구하고 SNS의 실시간성, 빠른 확산력으로 인해 잘못된 정보가 올바르게 전달될 시간적 여유가 충분치 않을 수 있다. 이러한 정보의 신뢰성 손상 행위는 정보와 연관된 개인 및 기업에 대한 이미지 추락 등으로 이어질 수도 있다.

또한, SNS는 특정 계층의 집단화를 부추길 가능성도 있다. SNS의 주 이용자는 주로 20대, 30대, 40대 등 젊은 세대에 포진되어 있다. 따라서, 일부 계층의 전유물로 각인되어 그 외의 계층에게 소외감을 느끼게 할 수 있다.

3.4. 안전한 SNS 서비스 이용 방법

우리는 본 장에서의 보안위협을 살펴보았다. 그리고 다음과 같은 안전한 SNS 서비스 이용 방법을 권고한다.

- 메시지에 포함된 URL 접근시 주의할 것
- 검증되지 않은 서드파티(3rd party) 서비스 이용을 자제할 것
- 지인의 메시지라도 다시 한번 확인할 것.
- 컴퓨터, 모바일 단말과 SNS 프로그램의 보안상태를 항상 안전하게 유지할 것
- 기업 SNS 운영 가이드라인을 준수할 것

Ⅳ. 사이버범죄, 사이버전쟁, 그리고 악성코드

4.1. 사이버 범죄 (CyberCrime as a Service)

우리는 이미 온라인 상에서 행해지는 불건전한 사이버 거래에 대한 수많은 정보를 접하고 있다. 이러한 블랙 마켓에서는 이메일 주소, 주민번호 등의 개인 정보 거래, 온라인 게임 아이템 거래, 스팸 메일 발송 혹은

분산 서비스 거부 공격 감행을 위한 봇넷 임대, 악성코드 유포를 위한 제로데이 취약점 거래 등을 통해 금전적인 이득을 추구하는 사이버범죄 집단의 행위에서도 주의깊게 모니터링을 하고 있다. 본 장에서는 인터넷 공간의 어둠의 영역에서 일어나고 있는 사이버범죄, 사이버전쟁에 대해 되짚어보고 지하 경제를 이해하는 시간을 갖도록 한다.

■ Russian Business Network[1]

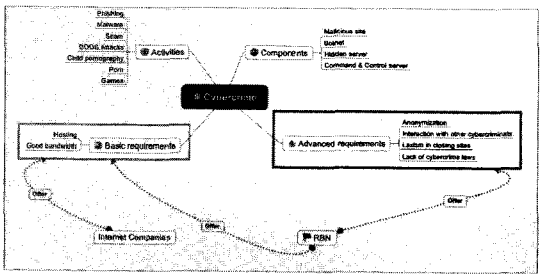
거대한 사이버범죄 (CyberCrime)의 대명사로는 러시아 해킹범죄 네트워크 (Russia Business Network)를 들 수 있다.

이 단체는 대규모 Cybercrime Service Provider 로서, 독자적인 인터넷망을 구축·운영하면서 악의적인 범죄 플랫폼 인프라를 제공함과 동시에 최신의 루트킷을 포함한 다양한 악성코드 제작 및 유포를 위한 웹사이트 운영, 도박 및 음란물 사이트 운영, 자동화된 익스플로잇 툴킷 제작 등을 지원하며 범죄의 시너지를 극대화하기로 악명이 높았다

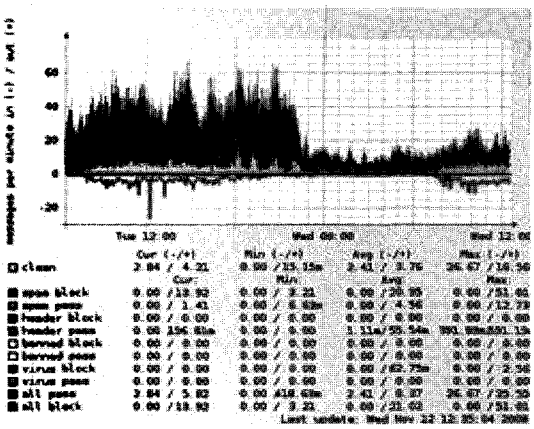
■ 아트리보[2], 맥콜로[3] ISP

아트리보(Atrivo), 맥콜로(McColo)는 대규모 스팸 발송을 위한 스팸 봇넷을 호스팅하던 악명높은 ISP로 알려졌다.

HostExploit 업체의 노력에 힘입어 아트리보는 2008년에, 맥콜로는 2009년에 서비스 단절이 되었고, 이로 인해 잠시나마 전세계의 스팸양이 줄어드는 효과를 거두기도 하였다. 그러나, 그것도 잠시 대부분의 봇넷 운영자들은 다른 악의적인 ISP 로 근거지를 이전함으로써, 서비스 단절 수개월 후의 스팸량이 예전의 수치가 회복되기도 하였다.



〔그림 10〕 Russian Business Network의 역할



〔그림 12〕 McColo 서비스단절 후 줄어든 스팸량
(출처: washingtonpost)

■ Golden Cash Network[4]

골든 캐쉬 네트워크 (Golden Cash Network)는 온라인에서 물건을 판매 및 구매할 수 있는 사용자간의 직거래 장터 형태의 웹사이트에서 발생하는 악성 봇 거래를 지칭하는 말이다.

골든 캐쉬 네트워크에서는 악성코드, 시스템을 공격할 수 있는 공격코드와 악성 봇에 감염된 좀비 시스템 등이 거래되고 있다고 한다.

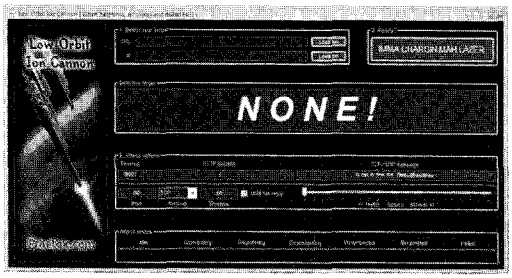
- 오스트리아 지역 - 악성 봇에 감염된 좀비 시스템 1000대당 100달러
- 한국, 중국, 일본 및 대만 지역 - 악성 봇에 감염된 좀비 시스템 1000대당 5달러

이렇게 판매되는 악성 봇에 감염되는 좀비 시스템들은 봇넷이라는 거대 네트워크를 형성하여 웹 사이트에 대한 분산 서비스 거부 공격(DDoS) 등의 사이버범죄에 악용될 소지가 높다.

4.2. 사이버전쟁 (CyberWar)

전 세계적으로 사이버전쟁에 대비해 사이버 전력을 증강하는 경쟁이 더욱 불붙고 있다. 총성없는 전쟁이지만, 적성국의 전산망을 마비시킬 수 있는 점 때문에 사이버 전력 육성은 군사력 못지 않은 위력을 지니고 있기 때문이다. 해킹 등을 통해 상대국의 군사 및 기업정보를 빼내거나 유사시 악성코드를 유포하는 데 이용이 가능하다.

- 미 국방부, 사이버사령부 창설 (2009)
- 영국, 사이버보안작전센터 신설 (2009)



〔그림 13〕 서비스 거부 공격 도구 (출처: SANS)

- 국방부, 사이버사령부 창설 (2010)
- 북한, '기술정찰조' 확대 운용
- 중국, 사이버 공격부대 대규모 육성

각국은 사이버 보안을 강화하고 새로운 세대의 온라인 무기를 개발하기 위해 노력중이다.

최근 지능형 지속 위협(Advanced Persistent Threat, 이하 APT)에 대한 관심과 주의가 요구되고 있다. APT는 과거 군, 정부 기관을 대상으로 활동하는 고도로 조직화되고 기술력이 뛰어난 사이버범죄집단의 타게팅 공격을 의미한다. 최근에는 금융, 상업 등의 기업을 대상으로 한 피해가 늘고 있는 것으로 보고된다. 공격 대상에 대한 집중 감시 및 진보된 사회공학적 기법의 활용을 통해 내부 네트워크에 대한 침투 능력이 뛰어나고, 악성코드 등의 다양한 공격도구 개발 및 활용 능력이 뛰어나 정보 수집 및 원격 접속·제어의 목적을 달성하는 것으로 파악되고 있다.

APT의 타게팅 공격 (Targeted Attack)을 위해서는 다음과 같은 절차를 거치게 된다.

- 타겟 공격을 위한 대상 선정
- 공격 대상에 대한 정보 수집 및 유대 관계 형성
- 사회공학적 기법을 이용한 악성코드 전파
- 제로데이 공격을 통해 악성코드 내부 감염
- 정보 수집 및 원격 접속·제어 권한 획득
- 목적 달성 후 침투 흔적 제거

■ 타겟 공격을 위한 대상 선정

주로 고급 정보를 획득할 목적으로 특정 공격 대상이 선정되며, 과거에는 정부나 군을 대상으로 한 공격이 주를 이루었으나, 최근에는 금융, 상업적인 기업 대상으로 한 피해가 늘고 있다.

■ 공격 대상에 대한 정보 수집 및 유대관계 형성

공격 대상(이하 타겟)이 선정되면, 그 타겟을 공략하기 위한 정보 수집 절차에 들어간다. 정보 수집 방법은 타겟과 관련된 웹사이트, 언론보도, 세미나 등의 공개된 정보 출처를 통해 내부 임직원에 대한 추가 선별작업이 진행되며, 블로그, 트위터, 페이스북 등의 소셜 네트워킹 서비스 (SNS, Social Network Service) 등의 다양한 인터넷 공간에서 해당 임직원과 연관된 세부 정보를 수집함과 동시에 유대 관계를 형성하는 것이 가장 중요하다.

■ 사회공학적 기법+제로데이 공격으로 내부 침투

내부 네트워크에 침투하기 위한 방법으로, 임직원에 대한 타게팅 공격을 감행한다. 그동안 형성한 유대 관계를 통해 신뢰 관계를 기반으로 한 공격이므로, 해당 임직원이 공격자에 대한 경계심이 낮아져 보안성이 결여된 상태이다. 주로 이메일, 메신저 등의 사회공학적 공격 기법을 이용하여 해당 임직원의 PC를 감염시키기 위한 악성코드, 또는 악성코드가 위치한 URL을 전송하여 클릭하도록 유도한다.

■ 정보 유출 및 원격 접속·제어 권한 획득

내부 PC감염에 성공한 이후, 감염 PC를 통해 충분한 내부 정보를 수집하게 되고, 원격 접속·제어 도구의 추가 설치를 통해 원하는 일이 가능하도록 할 수 있다. 수집할 수 있는 정보로는 군·정부 기관의 고급 문서, 기업의 지적재산권, 고객DB로의 접근 권한 등이 될 수 있다.

■ 목적 달성 후 침투 흔적 제거

지난 7·7 DDoS 공격 때도 경험해 보았듯이 공격 대상에 대한 고급 정보 수집 및 유출 행위 등의 목적 달성 이후에는 내부 네트워크 및 시스템 감염에 동원했던 악성코드 및 침해 흔적을 제거하기 위한 방법이 동원되고 있다.

V. 결 론

우리는 본 논문을 통해 급변하는 IT 패러다임 속에서 고도로 훈련된 공격자의 악성코드 제작 및 해킹 기술의 발전이 얼마나 우리에게 큰 위협이 되고 있는지 확인할 수 있었다.

미래 사회의 정보 시스템은 점점 더 복잡도가 증가하고 네트워크 결합도는 높아져가며 휴대용 단말을 통해

모바일 인터넷 환경의 저변 확대로 실로 유비쿼터스 사회로의 진입이 가시화 될 것이다. 이는 언제 어디서나 보안위협이 우리를 위험에 처하게 할 수 있음을 짐작케 한다.

우리도 이제는 '스마트한' 사이버 보안 대응 조직이 필요하다는 사실의 인식만으로는 공격자와의 사이버 상의 전쟁에서 필승할 수 없다. 공격자 보다 더 우월한 대응 기술과 조직력을 기반으로 수많은 침해사고 대응 경험을 통해 우리가 보유하고 있는 사이버 무기 체계를 지속적으로 발전시켜 나가야 한다.

지금 이 순간에도 우리의 정보 자산을 노리는 "총성 없는 전쟁"의 최전방에서 보안위협과의 사투를 벌이고 있다. 멀지 않은 미래에는 영화 "마이너리티 리포트"에서와 같이 언제나 공격자보다 한발 앞선 완전무결한 사전 방역 시스템이 구축되기를 간절히 희망해본다.

참 고 문 헌

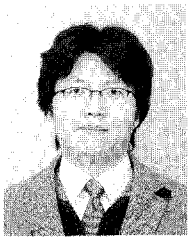
[1] David Bizeul, "Russian Business Network Study," Nov 2007.

[2] Jart Armin, HostExploit, "Atrivo, Cyber Crime USA," Sep 2008.

[3] Jart Armin, HostExploit, "McColo, Cyber Crime USA," 2008.

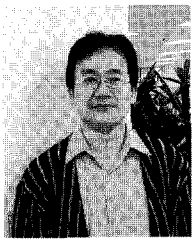
[4] FinJan, "Cybercrime Intelligence Report," Issue no.2, 2009

〈著者紹介〉



김 지 훈 (JiHoon Kim)

2000년 2월 : 충남대학교 졸업
2009년 2월 : 고려대학교 정보경영공학전문대학원 석사 수료
2004년 10월~현재 : 안철수연구소 ASEC(시큐리티대응센터) 분석2팀장
<관심분야> Information Security, Incident Response & Forensics, Early Warning System



조 시 행 (SiHaeng Cho)

1984년 2월: 한양대학교 건축공학과 졸업
1984년~1986년: 동아건설 전산실 근무
1986년~1991년: 쌍용정보통신 연구소 근무
1992년~1995년: 한컴퓨터주식회사 &한글과컴퓨터 근무
1996년~현재: 안철수연구소 연구소장
AVAR(Association of anti Virus Asia Researchers) Director Wild-List Reporter
<관심분야> Information Security, Anti-Virus Tech