ASEC Report 11월

® ASEC Report

2008. 12.

안철수연구소의 시큐리티대응센터(AhnLab Security Emergency response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스 분석 및 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 관련하여 보다 다양한 정보를 고객에게 제공하기 위하여 악성코드와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

I. ASEC Monthly Trend & Issue

(1) 악성코드 – 윈도우 시스템 파일을 바꿔치기 하는 악성코드

ASEC report 10월호에서 언급된 바와 같이 10월 말에 MS08-067 취약점이 보고되었고, zero-day attack 수준으로 이를 악용한 악성코드가 바로 발견/보고되어 이슈가 되었다. 11월 중에도 해당 취약점을 이용한 악성코드가 다시 발견되어 이슈가 되었고, 해당 취약점을 이용하는 악성코드가 지속적으로 발견될 것으로 예상된다. 그리고, 미국의 새 대통령이 당선이 되면서 해당 뉴스거리를 이용한 악성코드도 여러 변형이 보고가 되었고, 국내에서는 윈도우 시스템 파일을 악성코드로 바꿔치기 하여 정상적인 윈도우 기능을 사용하지 못하도록 불편을 초래하는 악성코드의 피해도 신고 되었다.

미국 최초의 흑인 대통령 관련 악성코드

미국 최초의 흑인 대통령이 당선되면서 이와 관련된 뉴스를 이용하는 악성코드가 반짝 강세를 보였다. 메일로 주로 전파된 악성코드는 주로 다음과 같은 메일 제목 또는 메일 본문을 가지고 있다.

> 2008 USA Government Official Web Site.
> Barack Obama can lost President's Chair.
> McCain has reached an agreement with the Obama lawyers that makes Obama resignation effective November 11.
> McCain Lawmakers Impeach Obama
> McCain Lawyer Impeach Obama!
> McCain video report 10 November

해당 악성코드는 이메일 웜이 아니므로 자체 전파력은 가지고 있지 않았지만, 메일 내에 특정 호스트로 유도하는 링크가 삽입이 되어 있었고, 해당 링크에서는 플래시 플레이어 새로운 버전을 가장한 파일을 다운로드하도록 유도하였는데, 해당 파일이 악성코드였다. 해당 파일의 대표적인 악성코드 진단명은 다음과 같다.

- Win-Trojan/Papras.31232.B
- Win-Trojan/Raitex.60928
- Win-Trojan/Agent.8192.BP

해당 악성코드들은 자신의 파일과 프로세스를 숨기면서 은밀하게 작동하면서 특정 응용 프로그램들의 사용자 정보를 가로채서 외부의 특정 호스트로 전송한다.

국제적인 뉴스나 문제들을 가지고 악성코드 전파에 이용되도록 하는 방법은 매우 고전적이다. 그러나 대부분의 사용자들의 호기심을 자극하는 이런 내용을 클릭하는 순간 악성코드로부터 자유롭지 못하게 된다.

시스템 파일을 바꿔치기 하는 악성코드

정상적인 윈도우 시스템 파일을 악성코드 자신으로 바꿔치기 하는 형태의 악성코드의 피해 문의가 증가하고 있는 추세이다. 특히 이번 달에는 윈도우 정상 시스템 파일인 rpcss.dll 파일을 악성코드 자신으로 바꿔치기 하는 형태가 자주 보고되었다. V3에서는 해당 악성코드를 Win-Trojan/RpcssPatch.Gen으로 Generic하게 진단하고 있어 변형에 대한 대응력을 강화하였다.

해당 악성코드에 감염되면, 해당 악성코드는 윈도우 파일 보호 기능을 잠시 무력화시키고 윈도우 시스템 폴더와 dllcache 폴더에 존재하는 rpcss.dll 파일을 삭제하고 원본은 spcss.dll 또는 srpcss.dll로 변경한다. 해당 RPC 관련 파일이 악성코드로 변경되면 일반적으로 파일 복사, 이동 및 클립보드 내 데이터 붙여넣기와 같은 작업을 수행하지 못하게 되므로 컴퓨터 사용에 불편이 초래 된다.

이러한 악성코드들이 사용하는 방법을 살펴보면 크게 다음과 같다.

- 파일의 일부 또는 전부를 수정 또는 바꿔치기 하는 경우
- 파일은 변조하지 않고 메모리에 로드된 모듈을 악성코드로 바꿔 치기 하는 경우

파일을 변경하는 경우 쉽게 진단이 가능하지만 메모리에 로드된 모듈을 바꿔치기 하는 경우에는 일반 사용자들은 물론 파워유저라도 감염 여부를 쉽게 확인하기 어렵다. 따라서 이와 같이 시스템 파일을 변경하는 증상을 갖는 악성코드에 대한 주의가 필요하다.

(2) 스파이웨어 – 3929.cn으로 홈페이지를 고정하는 스파이웨어

Adobe Flash Player의 SWF 취약점을 이용하여 설치되는 애드웨어 기승

11월 중순, 웹브라우저의 시작페이지가 “www.3929.cn”으로 고정된다는 신고가 다수의 고객으로부터 다량 접수되었다. 시작페이지 고정의 원인은 BHO(Browser Helper Object)로 설치된 중국산 애드웨어로 인한 것이었다.

[그림 1-1] 3929.cn으로 고정된 시작페이지

이 애드웨어는 해킹된 웹사이트에 삽입되어 있는 Adobe Flash Player의 SWF 취약점을 이용하는 악성 스크립트에 의해 사용자의 PC에 설치되는데, 국내 유명 웹사이트를 포함한 다수의 웹사이트가 해킹되어 애드웨어의 악성코드 유포 경로로 이용되어 국내 고객의 피해 수준은 심각하였으며, ㈜안철수연구소에서는 보안 위협등급을 3단계로 상향 조정하여 대응하였다.

그런데 이번 사건의 SWF 취약점은 사고 발생 이전에 이미 패치가 존재하였으며, 사용자가 미리 Adobe Flash Player의 업데이트만 실시하였다면 충분히 예방할 수 있는 사고였다.

국산 보안 제품을 제거하는 국산 애드웨어 - Win-Adware/NeSearch

바이러스나 웜, 트로이목마 등의 악성코드가 보안제품의 실행을 중지시키거나 삭제하는 경우는 많이 발견되고 있다. 이러한 악성코드의 대부분은 외국에서 제작된 것들이고, 보안제품의 실행을 중지시킨 뒤 시스템에 큰 문제를 일으키거나 게임의 계정정보를 탈취한다. 그런데 최근 국내에서 제작된 리워드 프로그램이 이와 같이 동작하는 것이 발견되었다. 진단명이 Win-Adware/NeSearch인 애드웨어는 다른 애드웨어의 번들 형태로 사용자의 적절한 동의 절차 없이 설치되어, Internet Explorer의 주소표시줄에 입력되는 키워드를 감시하고, 키워드와 관련한 광고를 노출하며, 쇼핑몰 등에 접속시 제휴마케팅 코드를 삽입하여 구매 수익의 일부를 얻는 리워드 프로그램이다.

Win-Adware/NeSearch는 국내 보안제품이 자신을 사용자의 시스템에서 제거하는 것을 막기 위하여 사용자 동의 없이 ㈜안철수연구소의 V3를 비롯한 국내 주요 백신들의 프로세스를 중지시키고 제거하려는 시도를 한다. 물론 V3의 경우 자체 보호 기능이 탑재되어 있기 때문에 해당 애드웨어의 의도와는 달리 중지되거나 제거되지 않는다. 그러나 일부 자체 보호 기능이 미비한 보안 제품의 경우, 이 애드웨어의 의도대로 사용자의 PC에서 보안제품이 중지 혹은 제거되며, 이렇게 될 경우 사용자의 PC가 악성코드로부터의 보안위협에 그대로 노출되기 때문에 매우 심각한 문제를 야기할 수 있다.

지속적으로 Win-Adware/NeSearch에 대하여 모니터링한 결과, 더 이상 배포되지 않고 있는 것으로 추정되며 V3나 스파이제로를 통해 전부 진단 치료가 가능하다. 그러나 앞으로 이와 같은 악성 프로그램이 계속해서 나올 것으로 예상되며 보안업체뿐만 아니라 사용자의 각별한 주의가 요구된다.

적절하지 못한 사용자 동의로 설치된 프로그램으로 인한 피해 증가

PC에 특정 프로그램이 설치되어 불편을 야기하게 될 경우, 해결법을 찾기 위해 인터넷 검색을 해보면 동일한 피해로 인한 사용자의 불만 글을 쉽게 찾아볼 수 있다. 최근에는 리워드 프로그램의 설치로 인한 피해와 이에 대한 해결 방안들이 많이 보고된다.

리워드 프로그램은 사용자가 제휴 쇼핑몰에서 물건을 구매하는 경우 추가 적립금을 지급해주는 하나의 비즈니스 모델로서 사용자에게 많은 이득을 줄 것 같지만, 엄밀하게 따져보면 사용자에게 주는 혜택은 전혀 없이 해당 프로그램 배포자만이 이득을 보는 경우가 대부분이다.

대부분의 리워드 프로그램이 설치되어 불편을 겪고 있는 PC 사용자들이 자신이 모르는 사이 프로그램이 설치되었다고 주장한다. 반면 리워드 프로그램 제작사는 합법적으로 자신의 프로

그램을 배포한다고 말하고 있다. 이 이유는 리워드 프로그램이 불법이라고 단정할 수 없는 방법으로 사용자가 쉽게 인지하지 못하는 방법으로 배포되고 있기 때문이다. 리워드 프로그램과 문제점이 발생하는 원인에 대해서는 'ASEC Report 11월 첫번째 컬럼'에서 자세히 소개한다.

(3) 시큐리티 – PDF 취약점

지난 10월 MS08-067 서버 서비스 취약점이 공개된 후, 이를 악용한 사례가 지속적으로 보고되고 있다. 원격에서 공격이 가능한 유형의 취약점은 악성코드에서 취약한 시스템을 찾는데 애용되고 있으며, 이러한 유형에는 대표적으로 DCOM, LSASS 취약점 등이 있다. 이에 대한 근본적인 대응책은 사용자들이 자신의 윈도우 시스템에 보안업데이트를 철저하게 하는 것이다.

방화벽, 안티바이러스 제품과 같은 보안제품에만 의존할 것이 아니라 주기적인 보안 업데이트, 강력한 패스워드 사용, 공유폴더 사용하지 않기 등의 기본적인 수칙만 지켜준다면 보다 안전한 인터넷 사용이 가능할 것이다. 더불어, MS 관련 취약점뿐만 아니라 시스템에 설치된 다른 소프트웨어의 취약점은 없는지도 살펴보아야 한다. 이번에 알려진 어도비(Adobe)사의 PDF Reader 프로그램의 취약점을 이용한 공격이 써드 파티 소프트웨어 위협의 좋은 예라고 할 수 있을 것이다. '보안'이라는 것은 언뜻 보면 해야 할 것도 많아 귀찮은 일이 될 수도 있겠지만 이 작은 노력이 컴퓨터를 안전하게 지킬 수 있는 최선의 길이다.

PDF 취약점을 이용한 문서 자주 발견

전자문서로 유명한 어도비사의 PDF Reader에서 또 다른 취약점이 공개되어 사용자들의 주의가 요구된다. 이번 취약점뿐만 아니라 이전에도 몇 차례 관련 취약점들이 공개되어 악의적으로 이용되었는데, 이렇게 어도비사의 취약점이 주목받는 이유는 전세계적으로 PDF (Portable Document Format)라는 포맷이 공용화 되었고 사용자층이 매우 두텁기 때문이다.

최근에 공개된 취약점은 PDF 파일에 삽입되어 실행되는 자바 스크립트 코드 중 "util.printf()" 처리 과정에서 입력 값이 제대로 검증되지 않아 발생하는 스택 오버플로우 (Stack Overflow) 취약점이다. 조작된 PDF 파일을 사용자가 열어보는 순간, 해당 취약점을 이용하여 악의적인 코드가 실행될 수 있으며 사용자 권한을 획득할 수도 있다. 해당 취약점에 영향을 받는 소프트웨어는 8.1.2 버전이며, 8.1.3 과 9 버전은 영향을 받지 않는다.

해당 취약점을 좀더 자세히 살펴보면, 숫자나 날짜를 포맷 형태로 출력하고 파싱하는 기능에서 발생한 것으로 다음과 같이 Utils 오브젝트에서 지원하는 printf 메소드에 넘겨지는 인자 값이 체크되지 않아 발생하는 것이다.

```
Util.printf("%.2f", value)
```

공격자가 PDF 문서에 취약점을 발생시킬 수 있는 Util.printf를 내포한 JavaScript 코드를 삽입함으로써 악용할 수 있게 된다. 취약점은 EScript.api 에서 발생되는 것으로 실제 코드

를 보면 아래와 같다.

```
238A3A37 |. 57 PUSH EDI     ; 전달될 바이트
238A3A38 |. 6A 20 PUSH 20
238A3A3A |. 56 PUSH ESI     ; 스택 오버플로우의 발생지
238A3A3B |. E8 4634F6FF CALL <JMP.&MSVCR80.memset> ; 버퍼 오버플로우 발생
```

취약점 공개와 함께 이를 이용할 수 있는 공격코드(PoC)가 이미 공개되어 있으므로, 이를 악용할 가능성은 더욱 높아진 상태이다. 따라서, PDF 문서 사용자는 해당 취약점에 해당하는 업데이트를 반드시 확인하고 출처를 알 수 없는 PDF 파일을 열어보지 않아야 한다. 만약, 업데이트가 힘든 사용자라면 PDF Reader 옵션 중 자바스크립트 기능을 해제하는 설정을 Enable 하여 스크립트 코드의 실행을 막는 것도 하나의 방법이 될 수 있다.

윈도우 비스타 TCP/IP 스택 취약점 존재

최근 윈도우 비스타에서 임의의 코드를 실행할 수 있는 취약점이 오스트리아의 한 연구자에 의해 발견되었다. 이번 취약점은 비스타의 네트워크 입/출력 서브시스템에서 발견된 것이며 특정 요청이 iphlpapi.dll에 전달되면 버퍼 오버플로우가 발생되어 커널 메모리를 망가뜨리고 이로 인해 블루스크린이 나타날 수 있다고 보고하였다. 해당 취약점은 현재 주로 사용되고 있는 Windows XP 시스템에는 영향이 없는 것으로 알려져 있다 현재 마이크로소프트사와 이번 문제를 해결하기 위한 작업을 진행하고 있으며 다음 번 윈도우 비스타 서비스팩에 포함될 것이라고 한다. 이 글을 쓰는 시점에서 비스타 서비스팩 2 번째 베타 버전이 공개되었다.

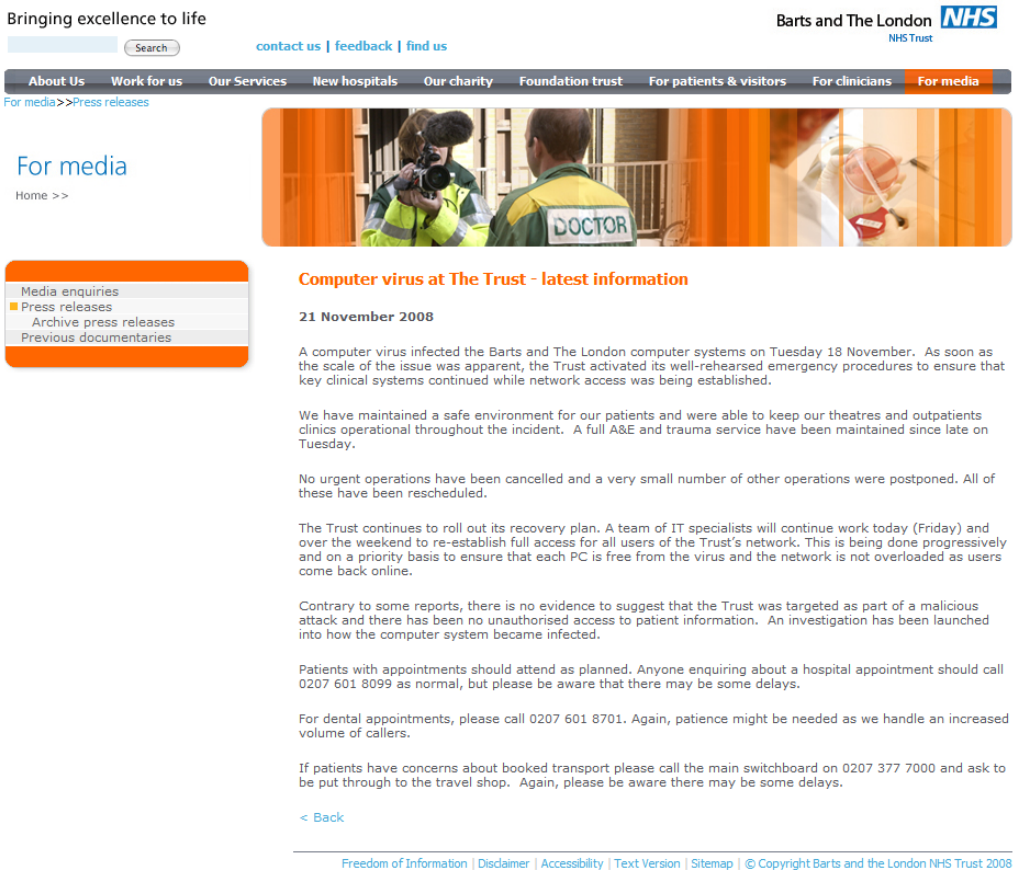
비즈니스를 위협하는 보안 문제

비즈니스와 IT 인프라의 의존성이 높아지면서 보안에 대한 관심 또한 나날이 높아지고 있다. 이것은 우리가 즐겨 이용하고 있는 대중교통만 보아도 알 수 있다. 버스와 지하철의 요금 처리, 티켓 구매, 버스 도착안내 이 모든 것이 IT 인프라에 의존하여 운영되고 있다. 어느 날 이런 시스템이 단지 몇 킬로바이트의 악성코드에 의해 감염되어 혼란을 줄 수 있다는 우려가 현실로 나타나고 있다. 이런 일이 일어나서도 안 되겠고, 일어나지 않도록 철저한 준비를 하고 있겠지만, 복잡한 IT 환경에서 이런 가능성은 언제나 존재한다.

최근 11월 18일(화)에 런던의 몇 개의 병원에서 악성코드가 감염되어 몇일 동안 시스템이 다운되는 사태가 실제로 발생했다. St Bartholomew's(Barts), Whitechapel의 로얄 런던 병원 그리고 Bethnal Green의 London Chest 병원에서 마이톱(Mytob) 웜에 감염되었다. 감염으로 인하여 병원의 시스템에 장애가 발생하여, 최첨단 IT 기술을 활용할 수 없게 되어 의사들

은 손으로 기록을 하였고, 앰블런스는 임시적으로 근처 병원으로 이동하여야만 했다. 병원 운영상 긴급한 수술의 취소 등과 같은 큰 문제점은 야기시키지 않았으나 일부 작업은 연기되거나 스케쥴이 재조정된 것으로 알려져 있다.

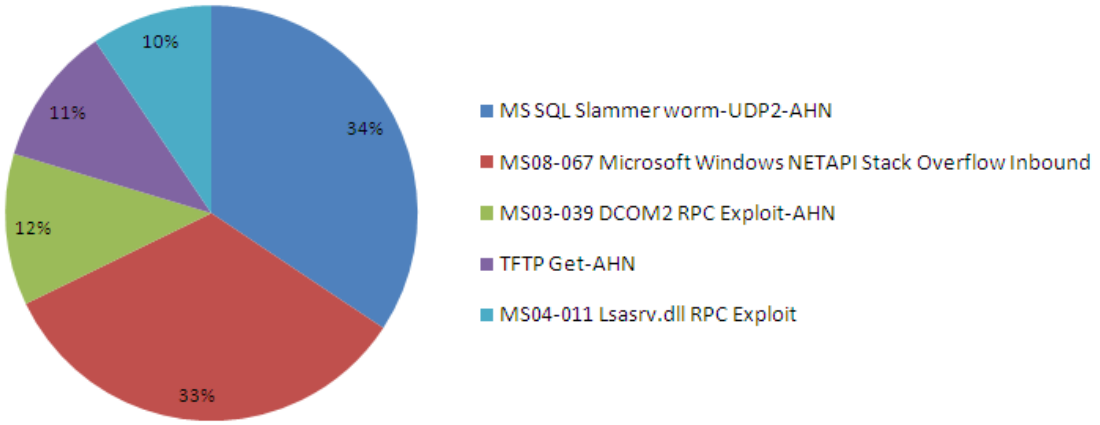
이번 사건은 고의적으로 병원을 대상으로 공격이 이뤄진 것이 아닌 것으로 알려져 있으며, 악성코드로 인해 환자의 개인 정보 유출 등은 없었고 단순한 감염사고로 추정된다. 하지만, 며칠 동안 병원은 과거로의 회귀를 경험하였고 업무 전반에 불편함을 끼쳤을 것이다. 만약 더욱 악의적인 악성코드였다면 보다 큰 피해를 입혔을 수도 있고, 더 나아가 환자의 생명과 직결되는 기계에도 영향을 줄 수 있었을지도 모른다. 이번 병원의 사례와 같이 이것이 여러 분들의 비즈니스에도 영향을 줄 수 있다고 생각되거나 IT 인프라에 의존적이라면 단순히 하나의 이야기 거리로 넘겨서는 안될 것이다. 지금 당신의 사업에 이런 일이 발생할 수 있다는 가정하에 "차선의 선택(Plan B)"를 준비해 놓아야 할 것이다.



[그림 1-2] 문제가 발생한 병원의 공지사항

(4) 네트워크 모니터링 현황 – MS08-067 공격 트래픽

최근 11월 한달 동안 네트워크 모니터링 시스템으로부터 탐지된 상위 Top 5 보안위협들은 다음과 같다.

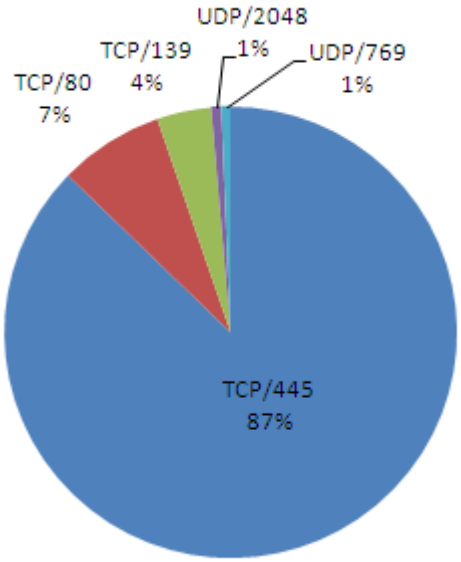


[그림 1-3] 상위 TOP 5 위협 탐지 이벤트

10월 말 MS08-067 서버 서비스 취약점이 발표된 이후 네트워크를 통해 해당 취약점을 이용하는 악의적인 트래픽이 급격히 증가되는 것이 관찰되기 시작하였다. 최근 새로운 취약점이 발표되고 이를 공격에 이용하는 악성코드가 제작되는 시간이 점점 짧아지고 있어 어느 때보다도 사용자들의 신속한 최신 업데이트 설치가 필요할 때이다.

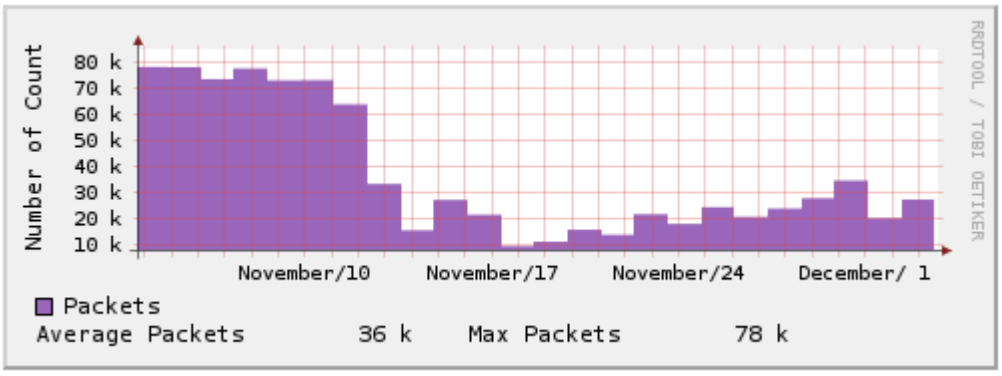
지금까지 상위를 차지하던 과거의 취약점들을 제치고 최근 발표된 MS08-067 서버 서비스 취약점이 상위에 올라왔으며, 이를 통하여 해당 취약점이 얼마나 빠른 속도로 확산되고 있는지를 추정해 볼 수 있게 한다.

특히, [그림 1-4]에서 보이는 바와 같이, 이번 달에는 TCP/445 포트가 전체 트래픽의 87%를 차지하였으며, 이 수치는 네트워크 모니터링을 시작한 이후 가장 큰 수치이다. 최근 발표된 MS08-067 서버 서비스 취약점이 TCP/139, TCP/445 포트를 사용하고 있으며 허니팟 내에 감염된 트래픽이 전파를 목적으로 또 다른 시스템을 스캐닝하는 과정에서 발생되기도 하였다. 네트워크 관리자들은 TCP/139, TCP/445 포트가 반드시 필요한지 여부를 확인하고, 불필요경우 방화벽과 같은 보안제품을 통해 차단할 필요가 있다.



[그림 1-4] 상위 TOP 5 포트

MS08-067 서버 서비스 취약점의 추이를 모니터링하기 위해 TCP/445포트 상의 트래픽을 집중적으로 살펴본 결과, 10월 27일부터 TCP/445 포트 상의 트래픽이 급격히 증가하였고 11월 13일 이후로 트래픽이 감소하는 모습을 아래 [그림 1-5]에서 확인할 수 있다. 최신 보안업데이트와 보안제품들의 탐지기능 추가로 인하여 MS08-067 서버 서비스 취약점을 이용하는 악성코드가 점차 감소하고 있는 것으로 추정해 볼 수 있다.



[그림 1-5] TCP/445 포트 상의 트래픽 추이

공격 발생지별로 살펴본 한달 간의 국가별 현황을 살펴보면, 기존 달과 마찬가지로 한국(KR)을 비롯하여 미국(US), 일본(JP), 중국(CN), 홍콩(HK) 등의 국가들이 차례로 높은 비중을 차지 하였다.

상위 10개 국가	백분율(%)	상위 10개 국가	백분율(%)
KR	43	MY	3
US	14	AU	3
JP	13	IN	2
CN	12	TW	2
HK	6	ZA	2

[표 1-1] 국가별 공격 발생지 분포[1]

[1] 이 표는 ㈜안철수연구소에서 운영 중인 허니넷으로 유입된 트래픽을 기준으로 한 것으로 전체적인 국가별 순위를 의미하는 것은 아니다.

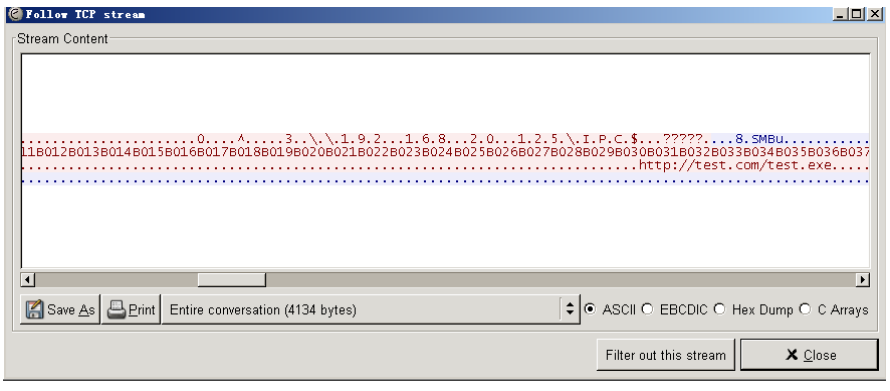
(5) 중국 보안 이슈 – 11월 중국 보안 이슈

MS08-067 취약점을 이용하는 공격 툴의 활성화

MS08-067 취약점이 중국 언더그라운드에 알려지면서 지난 11월 한 달 사이 ASEC으로 5종이 넘는 서로 다른 형태로 해당 취약점을 악용하는 툴들이 확보되었다. 이번에 확보된 툴들은 모두 스캐너 형태의 공격 툴로서 공격을 진행하는 GUI 파일과 MS08-067 취약점을 공격하는 파일 그리고 네트워크 대역을 스캐닝하는 파일 1개 이렇게 총 3개로 구성되어 있는 것이 일반적인 형태였다.

[그림 1-6] MS08-067 취약점 공격 툴

해당 스캐너 형태의 공격 툴들은 특정 IP 대역을 지정한 후에 다른 악성코드를 다운로드 할 수 있는 주소를 지정한 후 실행하도록 되어 있었다. 그리고 기존에 알려진 MS08-067 익스플로잇(Exploit)의 PoC 파일을 실행 압축하거나 암호화하여 재활용하고 있는 형태일 뿐 새로운 익스플로잇 코드는 발견되지는 않았다.

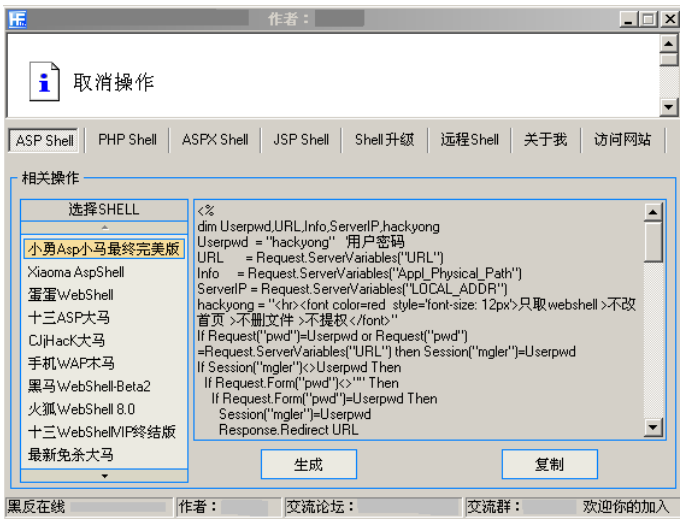


[그림 1-7] MS08-067 취약점을 공격하는 익스플로잇 전송

해당 공격 툴들을 실행하게 되면 [그림 1-7]과 같은 MS08-067 취약점을 공격하는 쉘코드와 함께 다른 악성코드를 다운로드 할 수 있는 주소를 동반한 4134 바이트 크기의 패킷을 설정한 네트워크 대역으로 전송하게 되어 있다. 해당 익스플로잇 패킷을 통해서 보안 패치가 적용되지 않은 시스템은 공격 패킷 내부의 공격자가 설정한 주소의 다른 악성코드를 다운로드 한 후 실행하게 된다. 현재까지 MS08-067 취약점을 공격하는 악성코드는 10월 말에 발견된 Win-Trojan/Gimmiv와 11월 말에 발견된 Win32/Conficker.worm이 있다. 그러나 더욱 우려스러운 점은 최근에 발견된 일부 악성 IRCBot에서 해당 취약점을 이용하여 시스템을 공격하고 있는 것으로 알려져 있다. 이러한 윈도우 시스템의 취약점을 공격하는 악성코드에 대응하기 위해서는 사용하는 운영체제의 최신 보안 패치를 적용하고 공격 익스플로잇 패킷을 방어 할 수 있는 방화벽 기능이 포함된 통합 보안 제품을 사용하여야 한다.

통합화된 다양한 기능의 웹쉘(WebShell) 생성기

최근 들어 다시 asp 또는 php 형태의 다양한 웹쉘들이 ASEC으로 접수되기 시작하여 중국 언더그라운드 웹 사이트를 조사한 결과 [그림 1-8]과 같은 다양한 기능을 수행 할 수 있는 웹쉘(WebShell) 생성기가 발견되었다.



[그림 1-8] 중국 언더그라운드에서 제작된 웹쉘(WebShell) 생성기

웹쉘은 일반적으로 asp와 php 그리고 jsp와 같이 다양한 형태의 스크립트 파일들로서 웹 서버에서 관리자 권한을 획득 한 후 다양한 쉘 명령(Shell Command)을 통하여 파일 업로드와 내부 자료 유출 등의 기능을 수행하도록 제작된 악의적인 스크립트 파일들을 이야기 한다. 이번에 발견된 웹쉘 생성기는 비교적 널리 알려진 ASP shell의 경우 총 11개의 다른 형태의 변형들을 제작할 수 있으며, PHP Shell의 경우 10개의 다른 형태의 변형들을 제작할 수 있도록 되어있다. 그리고 기본적으로 제공되는 창에서 해당 스크립트들을 편집할 수 있도록 구

성되어 있으며, 보안 제품의 탐지를 우회할 수 있도록 스크립트 난독화 기능 등이 제공되어 웹쉘과 스크립트 파일 제작에 대한 지식이 없더라도 다양한 형태의 웹쉘을 제작할 수 있도록 되어 있다.

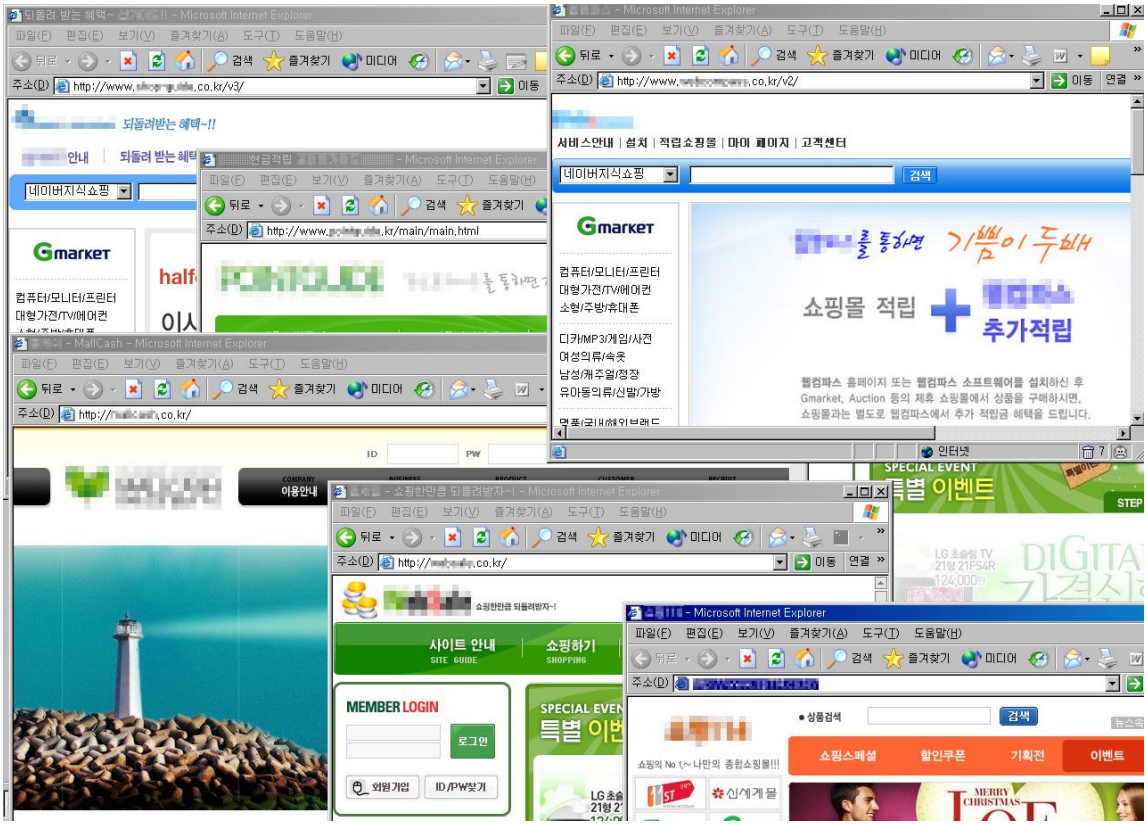
이러한 다양한 악의적인 기능을 수행하는 웹쉘의 공격으로부터 피해를 예방하기 위해서는 웹 서버에 존재하는 보안 취약점들을 제거하고 웹에 제공되는 게시판에는 불필요한 파일 업로드 및 쓰기 권한을 제거 하도록 한다.

II. ASEC 컬럼

(1) 리워드 프로그램은 과연 사용자를 위한 프로그램인가?

리워드(Reward)는 고객이 물건을 구매하거나 서비스를 이용할 때 다양한 보상을 통해 고객의 충성도를 높이는 마케팅 전략이다. 일반적으로 '캐시백', '포인트' 등의 이름으로 실생활에서 자주 접할 수 있다. 최근 인터넷상에서도 '리워드', '적립', '캐시백' 등의 단어를 포함하고, 다양한 제휴 쇼핑몰을 이용할 경우 추가 현금 적립을 해 준다는 리워드 프로그램의 수가 급격히 증가하고 있다. 리워드 프로그램은 클라이언트에 설치되는 소프트웨어로 인터넷 쇼핑몰과 제휴를 맺고 리워드 프로그램을 사용하는 고객이 제휴 쇼핑몰에서 상품을 구입할 경우에 발생하는 수수료를 수익 모델로 하고 있다.

리워드 프로그램은 수수료 수익 중 일부를 전자포인트 형태로 자신의 서버에 적립해 주며 여러 제휴사에서 각자 제공하는 포인트와는 별도의 포인트를 관리할 수 있게 해 준다. 또한 적립된 포인트가 약관에서 명시한 금액이 넘는 경우 현금으로 사용자에게 환원하는 서비스를 제공한다.



[그림 2-1] 수많은 리워드프로그램 제작사 홈페이지

인터넷 리워드 비즈니스 모델

인터넷 쇼핑 소비자의 입장에서 볼 때, 많은 소비자들이 인터넷 쇼핑몰을 이용해 상품을 구입하고 있으며, 좀더 유리한 조건에서 구매하기 위해 가격비교 사이트에서 제품을 검색하는 수고도 마다하지 않는다. 여러 사이트 중 가장 저렴한 제품을 찾고자 하는 알뜰한 구매자에게 추가 적립금을 제공하고, 많은 사이트의 적립금을 한번에 관리할 수 있는 기능을 제공하는 리워드 프로그램은 구매자에게 진정 유용한 프로그램일 것이다.

인터넷 쇼핑 사업자의 경우 보다 많은 매출을 달성하기 위해서는 더 많은 고객의 방문을 유도해야만 한다. 쇼핑몰의 주소를 인터넷 주소창에 직접 입력하고 필요한 물건을 구매하는 소비자도 있지만 가격비교나 인터넷 검색 등 다른 방법을 활용하는 경우도 많다. 가격비교 사이트나, 인터넷 포털 사이트에서 제품에 대한 정보를 검색하는 것은 잠재적인 고객일 확률이 높아지기 때문에 인터넷 쇼핑업체에게 검색 고객의 확보는 필수적이라 할 수 있다. 더 많은 고객 확보를 위해서 많은 인터넷 쇼핑몰들은 인터넷 포털 사이트나 가격비교 사이트와 제휴를 맺고 자사의 제품정보와 가격정보를 보다 많이 노출함으로써 고객의 방문을 유도하고 있다. 더 많은 고객을 확보해야 하는 인터넷 쇼핑몰에게 리워드 프로그램은 인터넷 포털 사이트나 가격비교 사이트와 동일한 고객 확보 경로라 할 수 있다.

이렇듯 리워드 프로그램은 많은 고객을 확보해야만 하는 인터넷 쇼핑몰과 알뜰한 쇼핑을 하려는 구매자 간의 필요성이 상호 충족하기에 발생한 훌륭한 인터넷 비즈니스 모델이라 할 수 있다.

리워드 프로그램의 문제점

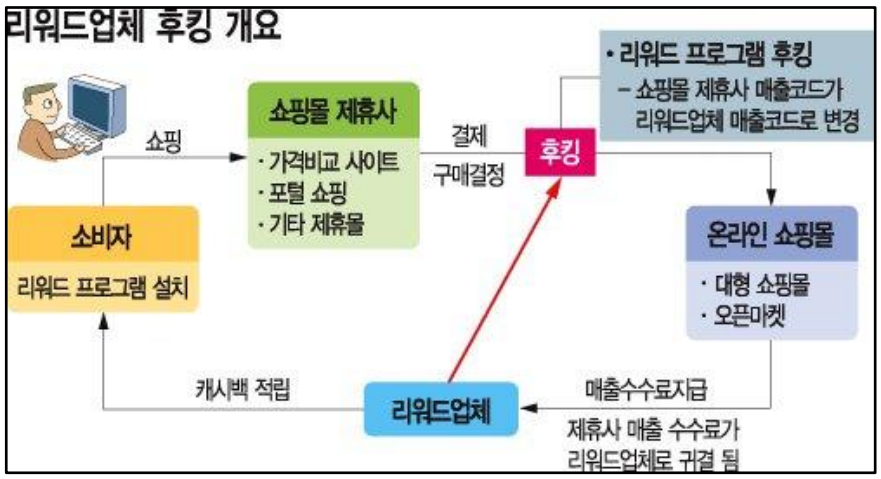
구매자와 판매자 모두에게 좋은 비즈니스 모델로 자리잡아야 할 리워드 프로그램은 현재 인터넷을 통한 프로그램 배포와 관련된 규정의 부재로 인해 서비스 사업자의 불법은 아니지만 잘못된 수익창출 형태와 우후죽순 생겨나는 여러 업체간의 부정 경쟁을 통해 많은 문제를 양산하고 있다.

1. 부정수익 창출

리워드 프로그램은 고객의 동의[1]를 받고 시스템에 설치되어 동작하는 클라이언트 프로그램이다. 클라이언트 프로그램은 PC에 설치되어 동작하는 프로그램을 의미하며 설치된 PC에서 발생하는 이벤트를 통제할 수 있다. 일부 리워드 프로그램의 경우 PC에서 제휴 쇼핑몰을 거쳐 온라인 쇼핑몰로 전해지는 트래픽을 조작하여 제휴마케

[1] 여기서 언급하는 '동의'는 정상적인 프로그램 설치 과정에서 발생하는 일반적으로 알려있는 동의 형태가 아닐 수도 있다.

팅 윤리에 혼란을 초래하고 있다.(디지털타임즈 2008.11.16: '리워드사이트' 유통질서 흐린다[1])



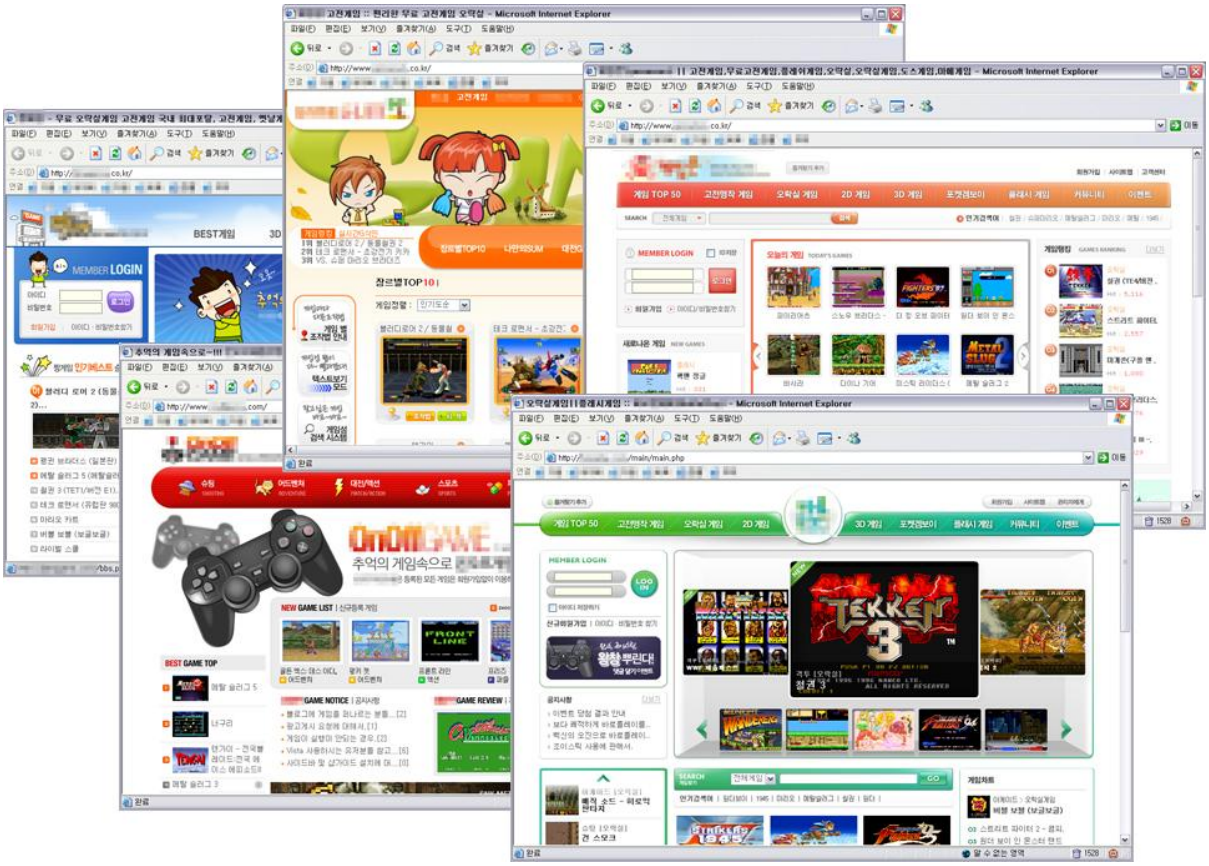
[그림 2-2] 쇼핑몰-제휴사간 수익흐름 (출처: 디지털타임즈 2008.11.16)

2. 부적절한 프로그램 배포방식과 부적절한 동의

제작사에서 리워드 프로그램을 제작하는 목적은 수익의 창출이다. 리워드 프로그램을 통해 수익을 창출하기 위해서는 보다 많은 PC에 자신이 제작한 프로그램을 설치해야 한다. 잘 알려지지 않은 홈페이지를 통해서 프로그램을 배포하는 것은 한계가 있기 때문에 리워드 프로그램은 유명 사이트의 툴바나 P2P프로그램, 고전게임[2] 등 사용자가 많이 찾는 프로그램의 번들(끼워넣기) 형식으로 설치가 되고 있다.

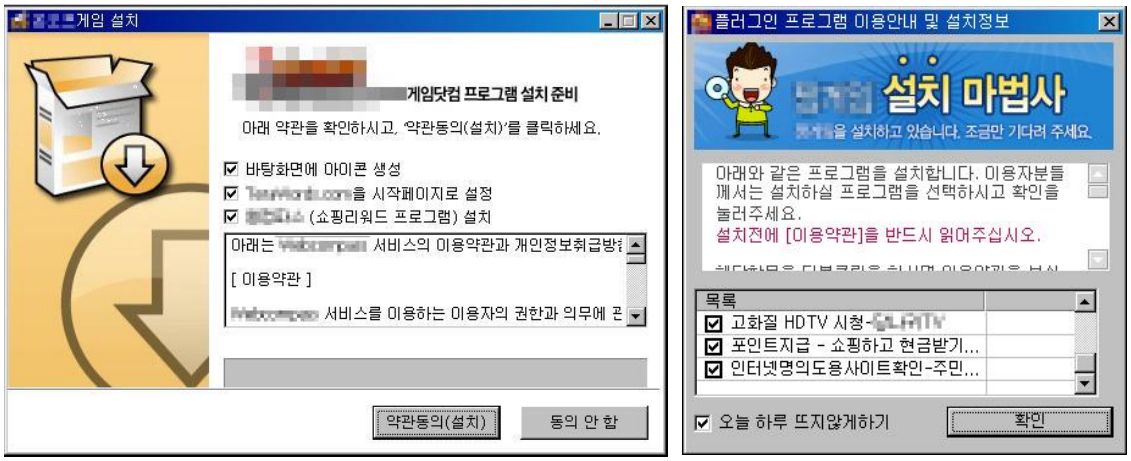
최근 무료로 서비스하는 고전 게임 프로그램들의 경우 서비스를 이용하기 위해 설치해야 하는 프로그램과는 전혀 무관한 프로그램을 번들 형식으로 설치하는 경우가 많이 늘고 있다. 이러한 방식으로 프로그램이 설치되는 경우 함께 프로그램의 목적을 사용자가 잘 인지할 수 없으며, 설치되는 프로그램의 경우 모든 프로그램은 각각에 대하여 동의를 구해야만 한다.[3] 그러나 이렇게 설치되는 프로그램은 일반적으로 정상적인 패키지 프로그램을 설치할 때와는 다른 방법으로 동의를 얻고 있다.

[1] 기사원문 http://www.dt.co.kr/contents.html?article_no=2008111702010151727002
[2] 고전게임은, 개인에 따라 기준은 다르지만, 주로 짧게는 5년~ 길게는 20여년 전의 어렸을 때 자신 혹은 많은 사람들이 즐겨 했던 게임을 일컫는다.
[3] 스파이웨어 사례집 http://www.boho.or.kr/infor_data/Spyware2007.pdf



[그림 2-3] 다수의 번들을 설치하는 고전게임 홈페이지

아래는 최근 리워드 프로그램 설치를 위해 가장 많이 이용되는 오락실게임 사이트를 통한 번들 프로그램 설치에 대해서 확인해 보았다.



[그림 2-4] 고전게임 사용자동의 형식

[그림 2-4]는 인터넷을 통해 손쉽게 구할 수 있는 고전게임 설치프로그램을 실행했

을 때 사용자의 동의를 구하기 위해 화면에 보여지는 동의창이다.

[그림 2-4] 왼쪽의 경우 특정 웹사이트를 시작페이지로 설정하고 리워드 프로그램을 설치하는 기능에 대한 동의를 구한다. 시작페이지는 고전게임 홈페이지를 예상할 수 있으나, 실제는 키워드 검색사이트로 시작 페이지를 고정하는 것이다. 리워드 프로그램 설치의 경우 오락 프로그램과 전혀 무관한 다른 프로그램이며, 다른 프로그램을 설치하기 위해서 리워드 프로그램에 대한 약관을 출력하고 동의를 구해야 한다. 그러나, 해당 동의창의 경우 하나의 텍스트박스에서 마우스 포인터를 '쇼핑리워드' 프로그램 설치'에 올리면 약관이 변환되어 마치 쇼핑 리워드 프로그램의 정상적인 동의까지 받는 것으로 속인다.

[그림 2-4] 오른쪽의 경우 또 다른 동의 방식을 사용한다. 고전게임을 설치하기 위해 프로그램을 실행하면, 인터넷주소변환프로그램, 즐겨찾기 등록, 인터넷 검색 도우미, 리워드 프로그램, 명의도용 차단 프로그램 등 7개의 프로그램이 번들(끼워넣기) 형식으로 설치된다. 다수의 번들 프로그램을 포함하는 동의창의 목록 아래에 표시된 각 프로그램 목록을 더블클릭하는 경우 약관이 표시된 웹사이트를 표시해 동의창을 확인할 수 있게 하였다.

추억에 잠겨 고전게임을 즐기기 위해 프로그램을 설치하는 사이 전혀 무관한 리워드 프로그램이 설치되었다. 이 경우 고전게임을 설치한 사용자는 리워드 프로그램의 설치에 대해 동의를 했으나 리워드 프로그램의 활용에 필요한 최소한의 정보인 포인트적립이 가능한 제휴사와 각 제휴사에 대한 적립 비율 등을 잘 이해하고 설치를 했다고 할 수 없다. 또한 리워드 프로그램 설치의 원천적인 기능인 보상의 관점에서 리워드 프로그램 제작사에는 제품을 설치한 사용자에 대한 최소한의 신상정보가 없기 때문에 설치된 PC에서 제휴 쇼핑몰로 구매가 발생하더라도 적립금을 저장할 계정정보를 가지지 않는다. 이 것은 고객에게 보상을 하겠다는 리워드 프로그램의 존재 이유에 의문을 가지게 하는 동시에 구매를 통해 발생한 수수료 수익이 정당하다고 볼 수 없다.

3. 비윤리적인 경쟁을 통한 사용자 피해

많은 업체에서 리워드 프로그램을 제작에 참여하고 있으며, 하나의 업체에서 두 개 이상의 제품을 배포하는 등 그 수적 증가가 아주 빠르다. 이렇듯 많은 프로그램이 존재하고, 번들 등 다양한 방법으로 배포하는 특성상 하나의 PC에 여러 개의 리워드 프로그램이 설치되어 있을 수 있다. 이 경우 쇼핑몰에 제휴사 정보를 전달하는 과정에서 문제가 발생할 수 있으며, 다수의 리워드 프로그램이 서로 충돌을 일으켜 시스템에 문제를 일으킬 수 도 있다. 이러한 문제점을 해결하기 위해 리워드 프로

그램들은 여러가지 자기방어 체계를 가지고 있다.

Process	Request	Path	Result	Other
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion	SUCC...	Access: 0x
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext	SUCC...	Access: 0x
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings	SUCC...	Access: 0x
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{A13E6D04-17B3-40FC-B69A-C47914BA377E}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{A13E6D04-17B3-40FC-B69A-C47914BA377E}\Flags	SUCC...	0x1
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{A13E6D04-17B3-40FC-B69A-C47914BA377E}\Ver...	SUCC...	"*"
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{2731C3A4-DF93-4AF1-98A6-88A8937057E7}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{2731C3A4-DF93-4AF1-98A6-88A8937057E7}\Flags	SUCC...	0x1
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{2731C3A4-DF93-4AF1-98A6-88A8937057E7}\Versi...	SUCC...	"*"
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{8DE24E17-88FF-4716-ACA0-C19396647974}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{8DE24E17-88FF-4716-ACA0-C19396647974}\Flags	SUCC...	0x1
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{8DE24E17-88FF-4716-ACA0-C19396647974}\Versi...	SUCC...	"*"
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{676F7A16-2D27-4E22-87F1-9D6E5BC49C57}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{676F7A16-2D27-4E22-87F1-9D6E5BC49C57}\Flags	SUCC...	0x1
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{676F7A16-2D27-4E22-87F1-9D6E5BC49C57}\Vers...	SUCC...	"*"
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{3CB0CF42-DA54-47d2-8999-23928A2DEA42}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{3CB0CF42-DA54-47d2-8999-23928A2DEA42}\Flags	SUCC...	0x1
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{3CB0CF42-DA54-47d2-8999-23928A2DEA42}\Vers...	SUCC...	"*"
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{54DC32B3-359C-4248-B0E7-B93610B8ADDD}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{54DC32B3-359C-4248-B0E7-B93610B8ADDD}\Fla...	SUCC...	0x1
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{54DC32B3-359C-4248-B0E7-B93610B8ADDD}\Ver...	SUCC...	"*"
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{6425C3F6-6BB2-45BB-BCFD-F76D011D7D92}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{6425C3F6-6BB2-45BB-BCFD-F76D011D7D92}\Fla...	SUCC...	0x1
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{6425C3F6-6BB2-45BB-BCFD-F76D011D7D92}\Ver...	SUCC...	"*"
pointg...	CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{472ABF56-AD5D-41C3-9139-675EE23A945A}	SUCC...	Access: 0x
pointg...	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{472ABF56-AD5D-41C3-9139-675EE23A945A}\Flags	SUCC...	0x1

[그림 2-5] 레지스트리 설정을 변경해 다른 프로그램의 ActiveX 설치를 방해

일부 리워드 프로그램은 자신의 정상동작을 위하여 다른 리워드 프로그램의 실행을 종료하고 프로그램의 일부를 삭제하거나, 경쟁 프로그램의 설치를 방해하는 기능을 포함하기도 한다. [그림 2-5]는 Win-Downloader/PointGuide.205312가 설치되면서 윈도우 레지스트리에 CLSID를 등록해 PC에 다른 리워드 프로그램이 설치되는 것을 방해하는 것이다. 이 경우 CLSID목록은 웹사이트에 저장되어 있으며, 프로그램 업데이트를 통해 변경이 가능한 것을 확인할 수 있었다.

시스템에 설치되어 실행중인 프로그램이 정상적으로 삭제되지 않고 일부 프로그램만 삭제된다면 시스템의 운영에도 문제가 발생할 수 있으며, 삭제된 프로그램이 사용자가 사용하는 프로그램인 경우 사용자는 영문도 모르고 시스템 가용성에 손상을 받는다. 또한 일부만 삭제된 프로그램은 쓰레기파일로 전락해 디스크의 공간만 차지할 수 도 있다.

4. 리워드 프로그램은 스파이웨어가 아니다?

2007년 (구)정보통신부에서는 스파이웨어 기준안과, 각 기준에 대한 사례[1]를 [표 2-1]과 같이 정의하였다. 이 기준에 따르면 적절한 사용자의 동의 없이 다른 프로그램이 다른 프로그램의 실행을 방해하거나 삭제하는 등의 행위를 하는 프로그램을 스파이웨어로 규정하고 있다. 이 기준안에서는 사용자 동의에 큰 비중을 두고 정상프로그램과 스파이웨어를 구분하고 있다. 따라서 리워드 프로그램의 경우 적절한 사용자의 동의를 받지 않았을 때만 스파이웨어로 분류할 수 있는 것이다.

[1] http://www.boho.or.kr/infor_data/Spyware2007.pdf

	ActiveX 보안 경고 창만을 이용한 설치는 동의로 간주하지 않으나, 해당 웹사이트의 서비스를 이용하기 위해 그 사이트를 방문 때만 실행되는 프로그램은 예외로 합니다.
1	ActiveX 보안 경고 창만을 이용한 설치는 동의로 간주하지 않으나, 해당 웹사이트의 서비스를 이용하기 위해 그 사이트를 방문 때만 실행되는 프로그램은 예외로 함
2	이용자의 동의 없이 또는 이용자를 속여 설치되어(설치되는 과정 포함) 정상 프로그램 또는 시스템의 운영을 방해, 중지 또는 삭제하는 행위
3	이용자의 동의 없이 또는 이용자를 속여 설치되어(설치되는 과정 포함) 정상 프로그램 또는 시스템의 설치를 방해하는 행위
4	이용자의 동의 없이 또는 이용자를 속여 설치되어(설치되는 과정 포함) 정상 프로그램 외의 프로그램을 추가적으로 설치하게 하는 행위
5	이용자의 동의 없이 또는 이용자를 속여 설치되어(설치되는 과정 포함) 이용자가 프로그램을 제거하거나 종료시켜도 당해 프로그램(당해 프로그램의 변종도 포함)이 제거되거나 종료 되지 않는 행위
6	이용자의 동의 없이 또는 이용자를 속여 설치되어(설치되는 과정 포함) 키보드 입력 내용, 화면 표시 내용 또는 시 스템 정보를 수집, 전송하는 행위 (다만, 정보통신서비스제공자가 이용자의 개인정보를 수집하는 경우는 정보통신망 이용촉진 및 정보보호 등 에 관한 법률 제50조의5의 규정을 적용한다)

[표 2-1] 스파이웨어 기준안

사용자 동의에 따라 정상 프로그램과 스파이웨어가 구분되는 현재 기준에 따라서 비록 사용자가 자신의 PC에 설치되는 프로그램의 기능과 성격을 정확하게 인지하지 못하더라도 형식적인 동의 과정만 갖춘다면 문제가 없는 상황으로 리워드 프로그램은 사용자에게 거부감 없이 동의를 구하기 위해 계속해서 진화하고 있다.

소프트웨어 이용 약관 모두 읽어야 한다!

'약관[1]'이란 계약의 당사자가 다수의 상대편과 계약을 체결하기 위하여 일정한 형식에 의하여 미리 마련한 계약의 내용을 의미한다. 일반적으로 현재 유통되는 소프트웨어 프로그램 설치 시에도 소프트웨어 이용 약관을 접할 수 있다. 그러나, 인터넷을 통해 프로그램을 설치할 경우 복잡한 약관을 주의 깊게 읽는 사람은 많지 않다.

사용자가 불편을 느껴 프로그램을 ASEC으로 접수하더라도 그 프로그램의 설치 시점에서 사용자 동의 과정이 존재한다면, 특별한 추가 사유가 없는 이상 스파이웨어로 분류하기 어렵다. 비록 약관의 내용과 동의 과정이 납득하기 어렵지만 동의 여부를 중요하게 여기는 스파이웨어 분류 기준으로는 사용자가 조심할 수 밖에 없다. 스파이웨어의 동작을 수행하는 프로그램도 약관에 행위를 기술한다면 그 방법과는 관계없이 동의과정을 거친 프로그램은 스파이웨

[1] http://terms.naver.com/item.nhn?dirId=108&docId=7750

어 분류를 할 수 없다는 약점이 있기 때문이다. 이 것이 각 개별 사용자 스스로가 소프트웨어 이용약관을 자세히 읽어야 하는 까닭이다.

약관내용	스파이웨어 특징
사용자의 시스템에 임의의 프로그램을 설치할 수 있으며 설치 전 동의를 추가로 구하지 않고, 이 약관에 동의를 함으로써 갈음함	사용자 동의 없이 다른 스파이웨어를 설치하며 사용자는 설치된 스파이웨어의 수량 종류를 알수 없다.
사용자의 인터넷 사용기록과 같은 개인 정보를 제3자에게 제공함	키워드 검색 시 선호도 조사 및 활용 접속 페이지 리다이렉트
사용자의 시스템 보안 설정을 변경함	웹 브라우저의 설정 변경 신뢰할 수 있는 사이트로 등록
인터넷 사용시 보여지는 내용을 조작함	검색결과 조작 광고 삽입 타사 광고 제거/교체
프로그램 설치로 인해 발생할 수 있는 어떠한 문제에 대해서도 책임지지 않음	시스템의 오동작에 의한 손상이 발생한 경우 책임회피
자동업데이트 기능, 자동 복구 기능 제공	프로그램의 임의제거가 어려울 수 있다. (프로그램 제거 시 재설치 문제발생)

[표 2-2] 문제가 될 수 있는 소프트웨어 이용약관 유형

문제가 될 수 있는 소프트웨어 이용약관 사례

리워드 프로그램의 약관중 사용자에게 불편을 끼칠 가능성이 있는 사례는 아래와 같다.

*** (리워드프로그램)

제 ?? 조. 손해배상 및 책임

1. ***는 무상 배포되는 *** 프로그램의 사용과 관련하여 사용자 또는 제 3자에게 발생하는 어떠한 형태의 손해에 대하여도 배상을 하지 않습니다.

→ 시스템이나 사용자 개인 정보 유출 등과 관련하여 발생 가능한 어떤 문제도 책임지지 않겠다는 의미로 해석 가능하다.

제 ?? 조. 개인정보 및 인터넷 사용정보 수집과 그 활용

5. 자동업데이트에서는 사용자의 컴퓨터에 피해를 끼치는 컴퓨터 바이러스 등의 악성 프로그램이 아닌, 상업적 용도의 프로그램이나 기타 ***가 서비스 향상을 위해 필요하다고 판단되는 프로그램들을 필요에 따라 임의의 파일이 사용자의 컴퓨터에 설치될 수 있으며, 설치 전 사용자의 동의를 추가로 구하지 않고 이 내용은 사용자가 약관동의를 함으로써 갈음합니다.

→ 사용자는 자신의 PC에 어떤 프로그램이 설치되어 동작하는지 알 수 없다.

6. 사용자는 ***를 이용해서 인터넷 이용 중 타사의 상업적 내용들을 제거할 수 있습니다. , 이 경우 해당 인터넷 서비스업체와의 모든 문제는 사용자의 권리와 책임으로 하며, ***의 상업적 내용은 제거되지 않을 수 있습니다.
→ 시스템에 설치된 다른 애드웨어의 동작을 방해하거나, 웹 페이지에 표시되는 광고 내용을 조작할 수 있으며, 이로 인해 발생하는 모든 책임은 사용자에게 있다.

9. *** 설치 시 자동으로 사용자의 인터넷 브라우저의 설정 중 *** 서비스 관련 URL을 신뢰할 수 있는 사이트로 추가하며, 변경된 설정은 사용자가 인터넷 옵션에서 다시 변경할 수 있습니다. 이 경우 *** 서비스가 정상적으로 동작하지 않을 수 있습니다.
→ 사용자 시스템의 보안 설정을 변경하는 행위로 약관에 포함되지 않았다면 스파이웨어의 행위에 해당. 해당 사이트가 신뢰할 수 있는 사이트로 추가될 경우 해당 사이트에서 배포되는 모든 ActiveX 컨트롤이 경고 없이 실행될 수 있다.

10. ***는 사용자가 컴퓨터에서 입력한 키워드를 검색 및 결과표시를 위해서 사용자의 컴퓨터이외로 전송할 수 있으며, ***는 이 키워드를 상업적 목적으로 사용하거나 제3자에게 익명으로 제공할 수 있습니다.
→ 사용자의 인터넷 사용기록을 외부로 전송하는 행위로 스파이웨어 행위로 의심할 수 있다.

툴바 (리워드프로그램)

5. 자동업데이트에서는 사용자의 PC에 피해를 끼치는 컴퓨터 바이러스 등의 악성 프로그램이 아닌, 상업적 용도의 프로그램이나 기타 ###와 회사가 서비스 향상을 위해 필요하다고 판단되는 프로그램들을 필요에 따라 임의의 파일이 사용자의 컴퓨터에 설치될 수 있으며, 설치 전 사용자의 동의를 추가로 구하지 않고 이내용은 사용자가 약관동의를 함으로써 갈음합니다.
6. 사용자는 ### 툴바를 이용해서 인터넷 이용 중 타사의 상업적 내용들을 제거할 수 있습니다.
단, 이 경우 해당 인터넷 서비스업체와의 모든 문제는 사용자의 권리와 책임으로 하며, 대출 ###와 회사의 상업적 내용은 제거되지 않을 수 있습니다.
8. ### 툴바는 사용자가 검색엔진이나 주소창 등에서 검색어를 입력하여 나타나는 결과와 연관되는 제3자의 상업적 내용을 사용자의 PC에 전송할 수 있습니다.
9. 회사는 사용자의 PC를 다른 사용자들의 사용편의를 위해서 P2P서비스의 중간 매개로서 사용할 수 있습니다.
10. ### 툴바 설치 시 자동으로 사용자 브라우저의 스크립트 오류메시지를 보지 않음으로 변경하며, 변경된 설정은 사용자가 인터넷 옵션에서 다시 변경할 수 있습니다.

이 경우 사용자가 변경한 설정에 의해서 스크립트 오류 메세지가 나타날 수 있습니다.
11. ### 툴바는 사용자가 PC에서 입력한 키워드를 검색 및 결과표시를 위해서 사용자의 PC 이외로 전송할 수 있으며, ### 와 회사는 이 키워드를 상업적 목적으로 사용하거나 제3자에게 익명으로 제공할 수 있습니다.

위와 같이 사용자에게 불리한 약관이 있는 줄 모르고 프로그램을 설치하게 되면 예기치 못한 불편에 직면할 수 있다.

약관의 경우 일방 당사자의 의견이 강하게 반영되기 때문에, 상대방 다수에게 불이익을 줄 우려가 있는 '불공정약관[1]'은 규제대상이 되어야 한다. 약관의 불공정 여부는 공정거래위원회에서 '약관의 규제에 관한 법률'에 의거해 심사하며, 고객에 대하여 부당하게 불리한 조항 등 불공정약관은 무효로 할 수 있으나 이 것은 계약 당사자가 스스로 부당함을 인지하고 조정을 요청해야 하는 문제를 가지고 있다. 수많은 소프트웨어 제품이 홍수처럼 쏟아져 나오고 있는 지금 사용자가 스스로 사용하는 모든 프로그램의 약관을 읽고 공정성여부를 판별해 대응한다는 것은 현실적으로 어렵다. 관련 기관 및 백신소프트웨어 제작 업체에서는 이러한 문제를 인식하고, 사용자에게 피해를 주는 행위를 정당화하는 소프트웨어 이용약관이 개선될 수 있도록 노력을 해야 한다. 더불어 법적 재제장치가 마련될 때까지 피해자로 방치될 가능성이 큰 PC 사용자들은 프로그램을 내려 받을 때 약관을 살피는 주의를 기울여야 한다.

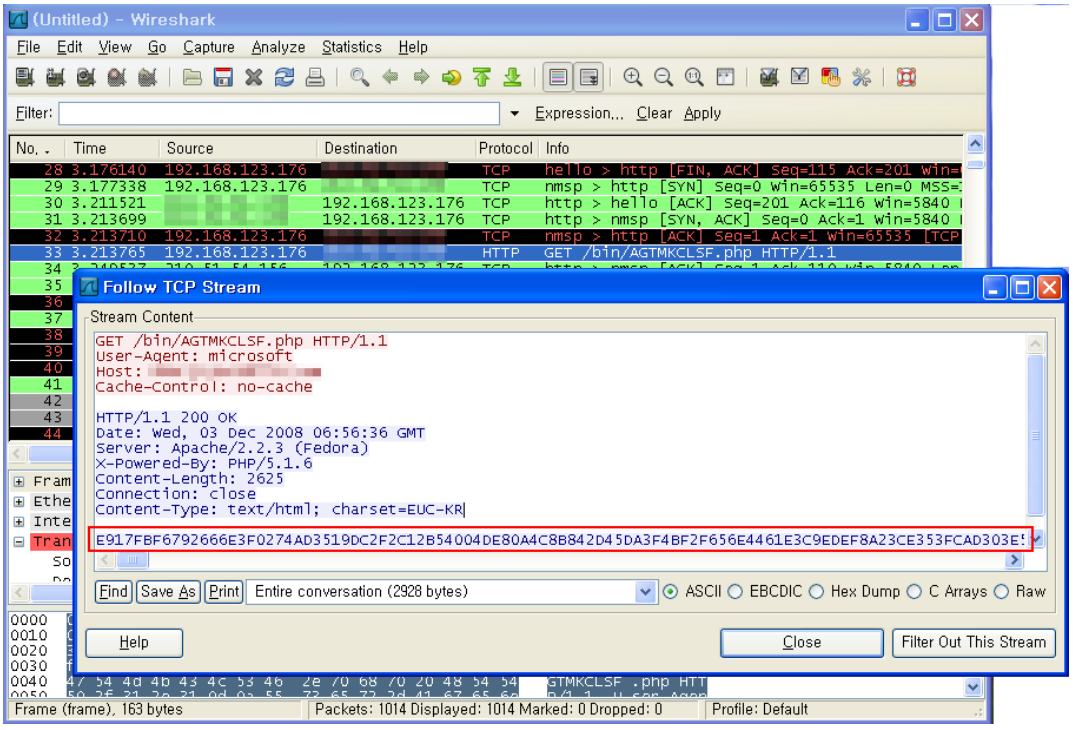
[1] http://terms.naver.com/item.nhn?dirId=701&docId=3317

(2) 인터넷 도박이 일반인을 유혹하는 방법

최근 유명 연예인이 인터넷 도박을 통해 거액을 잃고 공무원이 인터넷 도박으로 생긴 빚 때문에 몇십억에 달하는 공금을 횡령하는 등 인터넷 도박에 관련된 언론 보도가 계속 되고 있다. 이들 인터넷 도박이 어떠한 경로를 통해 사람들을 유혹하고 피해자로 만드는지 보다 자세히 살펴보고 그 문제점을 알아보자.

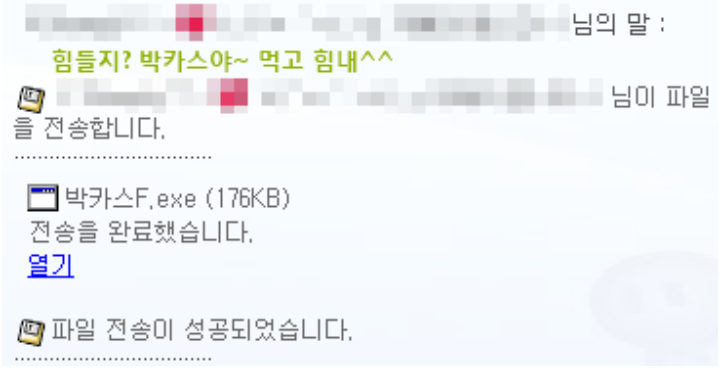
스파이웨어(spyware)를 통한 설치

인터넷 도박 사이트로 유도하기 위한 스파이웨어들은 자체 업데이트 기능을 가지고 있으며 생성하는 인터넷 바로 가기에 대해 암호화된 정보를 특정 서버로부터 받아와 다양한 사행성 사이트에 대한 인터넷 바로 가기를 생성해 일반적인 보안 제품에 의한 사전 예방을 어렵게 한다. 또한 임의의 이름으로 자동 시작 프로그램으로 등록되어 생성된 인터넷 바로 가기 아이콘을 삭제하더라도 언제든지 다시 생성될 수 있으며 그 내용 또한 매번 달라진다.



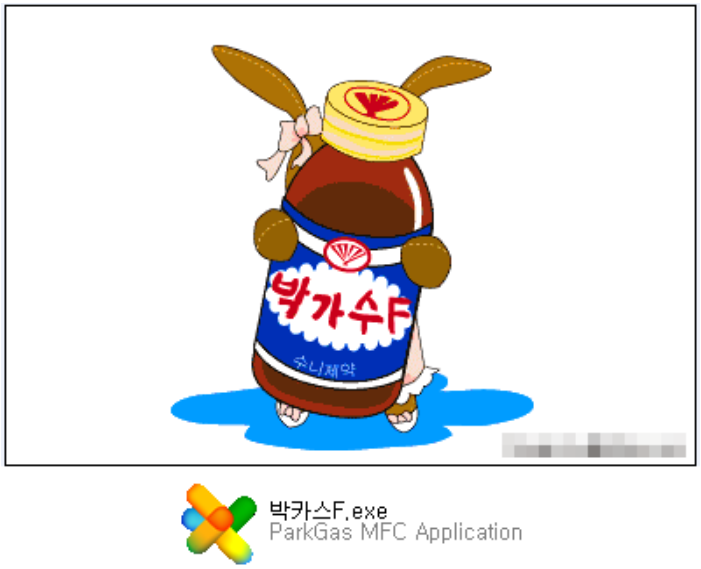
[그림 2-6] 암호화된 내역을 송수신하는 스파이웨어

실제 최근에 이슈가 되었던 스파이웨어 중에는 자양강장제로 위장해 메신저를 통해 지인에게 전파되는 형식으로 감염되었다.



[그림 2-7] 메신저를 통해 지인에게 전송받은 프로그램

지인에게 전송 받은 프로그램을 실행하면 아래 [그림 2-8]과 같은 그림이 나온다. 하지만 실제로는 스파이웨어를 설치하고 바탕화면에 인터넷 도박 사이트 바로가기 아이콘과 원격 제어 프로그램을 설치한다.



[그림 2-8] 메신저로 전송된 스파이웨어를 실행 했을 때 화면

이와 같이 사용자 동의 없이 사용자 동의 없이 설치되는 스파이웨어는 인터넷 바로 가기(Shortcut)를 생성해 사행성 게임 사이트로 접속을 유도한다.

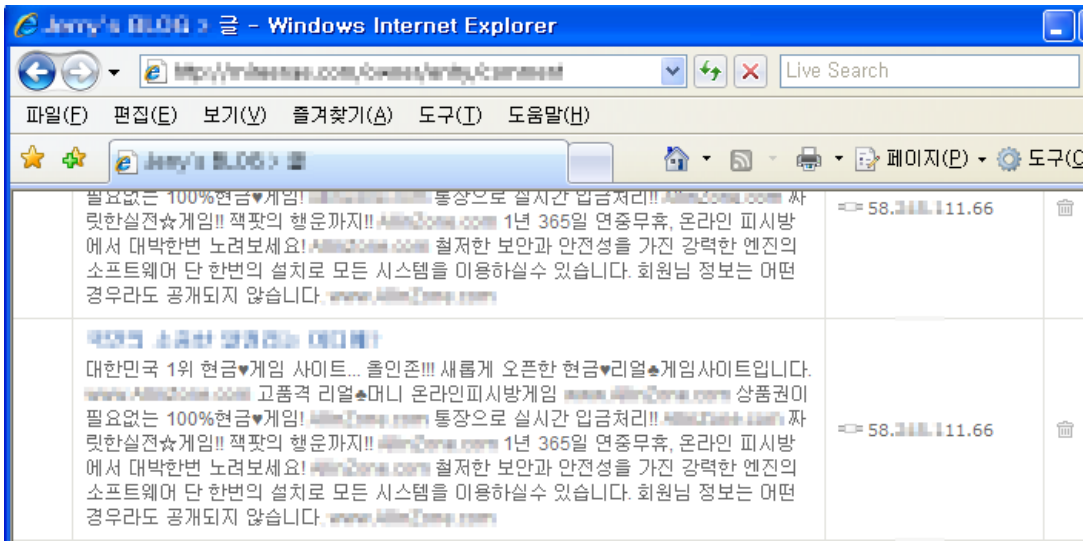
[그림 2-9] 스파이웨어에 의해 생성된 사행성 게임 인터넷 바로 가기 아이콘들

블로그(Blog)를 이용한 도박 사이트 홍보

인터넷의 정보 공유 기능을 악용한 사례로 인터넷 도박 사이트를 홍보하기 위해 블로그를 개설하고 특정 시간을 단위로 홍보 글을 예약 작성해 지속적으로 등록하는 방법을 사용한다. 또한 검색 엔진을 통해 검색을 용이하게 하기 위해 인터넷 도박과 관련된 단어 수 백개를 본문에 포함시켜 해당 단어를 통해 검색 시 해당 홍보글이 검색되어 노출될 수 있게 작성한다.

[그림 2-10] 30분 단위로 예약 작성되어 자동으로 등록된 인터넷 도박 사이트 홍보글 들

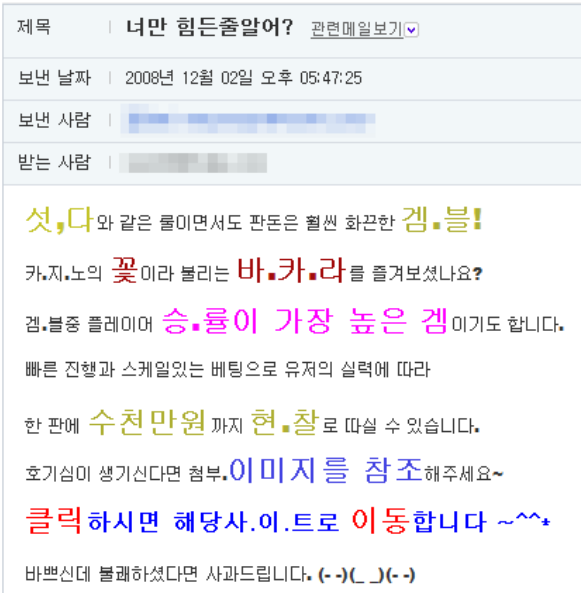
또한 [그림 2-11]과 같이 블로그의 댓글과 트랙백 기능을 악용하여 인터넷 도박 사이트 홍보글을 작성하는 경우도 지속적으로 발견되고 있다. 블로그 운영자가 일일이 확인하고 삭제하지 않으면 계속 방치되어 지속적인 피해를 가져올 수 있다는 문제점이 있다. 또한 해당 블로그 운영자는 본의 아니게 자신의 블로그에서 인터넷 도박 사이트를 홍보하는 피해자인 동시에 가해자가 될 수 있다.



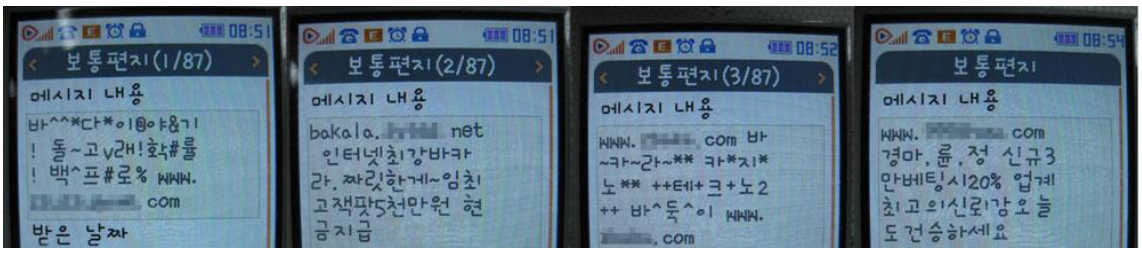
[그림 2-11] 블로그 댓글과 트랙백 기능을 악용한 인터넷 도박 홍보 글

스팸 메일, 휴대폰 SMS 서비스를 이용한 도박 사이트 홍보

휴대폰 단문자 서비스(SMS) 또는 스팸 메일(Spam mail)을 사용해 불특정 다수에게 인터넷 도박 사이트 광고를 전송한다. 스팸으로 필터링 대상이 될 수 있는 단어들 사이에 임의의 특수 문자를 추가하는 등의 방식으로 스팸으로 분류되지 않도록 다양한 회피 방법을 사용한다. 따라서 효과적인 차단이 어렵고 불특정 다수를 대상으로 하므로 누구나 피해자가 될 수 있다.



[그림 2-12] 스팸 메일을 이용한 인터넷 도박 사이트 홍보



[그림 2-13] 인터넷 도박 사이트를 광고하는 SMS

최근 인터넷 도박과 관련해 크게 이슈화 된 뉴스를 나열하면 다음과 같다.

- 야구 선수 '억대 도박' 정확 포착 : 프로야구 선수들 약 10여명이 인터넷 도박 사이트에서 약 10억원의 판돈으로 '바카라'게임을 한 것으로 알려졌음
- 인터넷도박 개발자 "이용자들은 냄비 속에 던져진 개구리" : 개인들은 게임을 하면 '따는 것'과 '잃는 것' 두가지만 생각하지만 수고비 명목으로 사업자에게 수수료를 뜯기고 있으며 매장 당 수익이 하루 평균 2000만~3000만원 정도 되며 이들 사업자들이 조직폭력배와 연관된 것으로 보임
- '인터넷 도박에 빠져' 26억원 횡령 공무원 붙잡혀 : 모 공무원이 인터넷 도박에 빠져 약 26억원을 횡령하고 해외로 도피했다 자진 입국함
- 인터넷도박 130명 수사...XXX씨 도박판돈 16억 : 1억원 이상의 판돈으로 인터넷 도박을 한 130명에 대해 수사를 진행한다는 내용이며, 유명 연예인의 경우 약 16억원의 판돈으로 인터넷 도박을 했음

인터넷 도박은 이렇게 다양한 경로로 사용자를 유혹하고 있어 그 피해자가 될 가능성이 더욱더 높아 지고 있다. 또한 인터넷이 되는 컴퓨터만 있으면 쉽게 접근할 수 있어 집에서도 간단하게 도박을 할 수 있다. 호기심에서 한번이라도 인터넷 도박 사이트에 접근하게 되면 누구나 피해자가 될 수 있다.

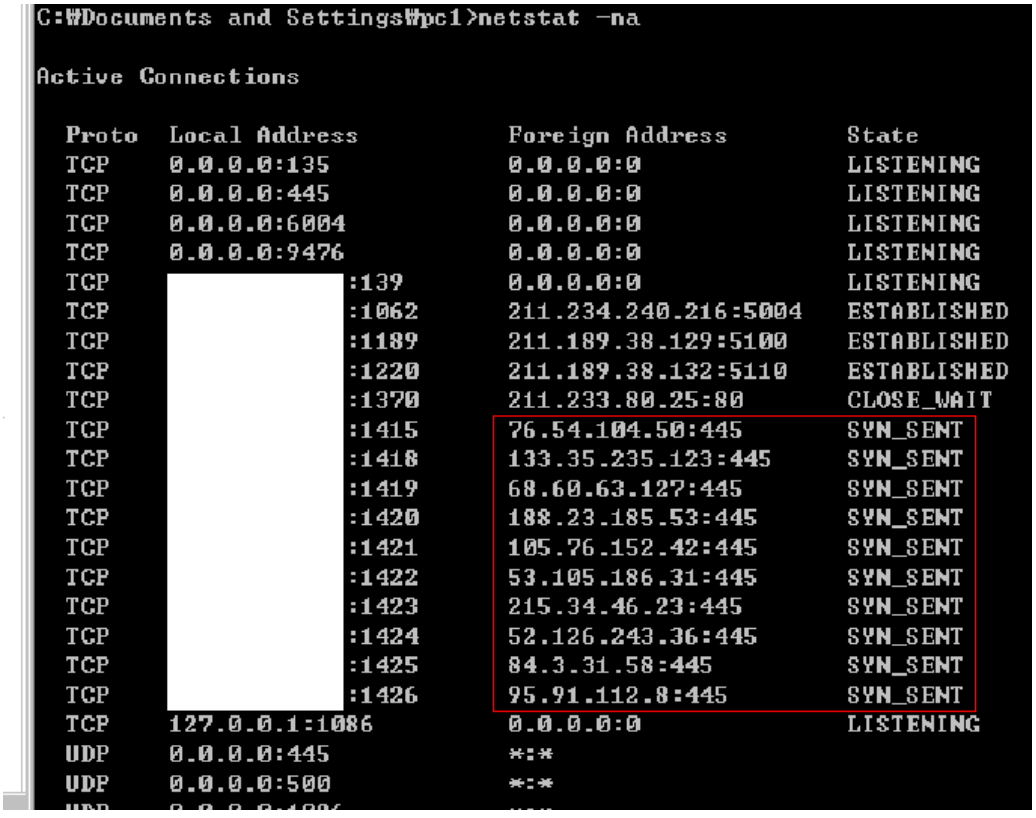
도박은 확률상 일반인이 게임에서 이길 확률이 매우 적다. 또한 인터넷 도박의 경우 게임을 할 때마다 일정 비율의 수수료를 받기 때문에 게임을 하면 할수록 돈을 잃을 수 밖에 없는 구조를 가지고 있다. 무엇보다 이런 인터넷 도박 사이트는 국내에선 불법이며 인터넷 도박의 특성상 게임과 관련된 자료가 모두 전산상 기록으로 남는다. 따라서 한 순간 호기심으로 즐긴 인터넷 도박으로 인해 본의 아니게 범법자로 남을 수 있다.

(3) 다시 강조해야하는 MS08-067 취약점 패치

11월 22일, ASEC팀으로 A라는 고객의 신고가 접수되었다.

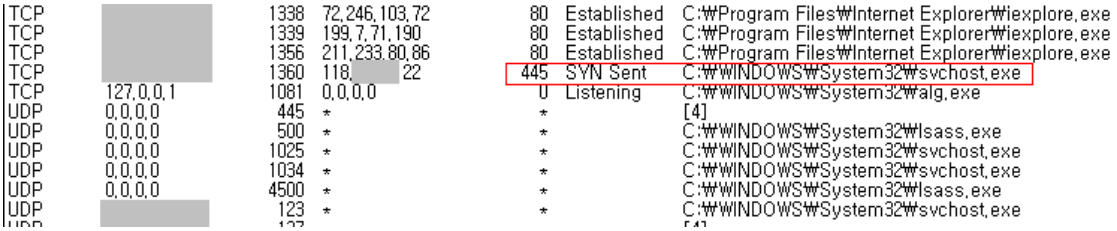
"웹브라우저 속도가 느려졌고, 사이트 접속이 안됩니다!"

당시 이슈가 되고 있었던 웹브라우저 시작페이지의 중국사이트 고정문제와는 전혀 다른 신고가 접수된 것이다. 우리는 재빨리 고객의 PC에서 접수된 AhnReport의 실행중인 프로세스와 로드된 모듈정보를 확인하였으나 어느 하나도 의심스런 파일은 찾을 수가 없었다. 하지만 고객PC의 네트워크 연결상태를 확인해보니 아래와 같이 TCP 445포트를 스캔하고 있는 것을 볼 수 있었다.



[그림 2-14] 해당 시스템의 netstat 실행결과

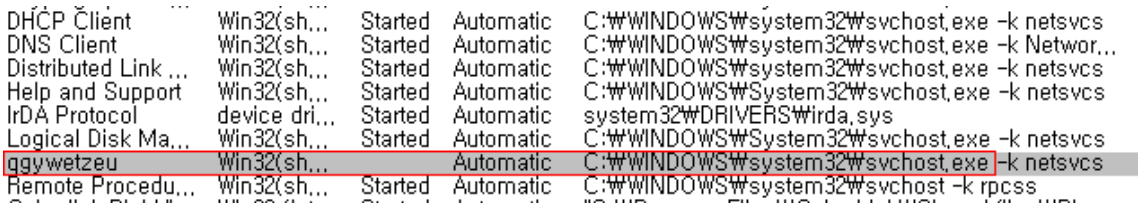
의심스런 패킷을 어떤 프로세스가 생성하고 있는지 확인하기 위해서 고객이 보내온 AhnReport의 네트워크 연결정보를 살펴보았다.



TCP	[redacted]	1338	72.246.103.72	80	Established	C:₩Program Files₩Internet Explorer₩iexplore.exe
TCP		1339	199.7.71.190	80	Established	C:₩Program Files₩Internet Explorer₩iexplore.exe
TCP		1356	211.233.80.86	80	Established	C:₩Program Files₩Internet Explorer₩iexplore.exe
TCP		1360	118.[redacted]22	445	SYN Sent	C:₩WINDOWS₩System32₩svchost.exe
TCP	127.0.0.1	1081	0.0.0.0	0	Listening	C:₩WINDOWS₩System32₩alg.exe
UDP	0.0.0.0	445	*	*		[4]
UDP	0.0.0.0	500	*	*		C:₩WINDOWS₩System32₩lsass.exe
UDP	0.0.0.0	1025	*	*		C:₩WINDOWS₩System32₩svchost.exe
UDP	0.0.0.0	1034	*	*		C:₩WINDOWS₩System32₩svchost.exe
UDP	0.0.0.0	4500	*	*		C:₩WINDOWS₩System32₩lsass.exe
UDP	[redacted]	123	*	*		C:₩WINDOWS₩System32₩svchost.exe

[그림 2-15] A고객 PC의 AhnReport 네트워크 연결정보

[그림 2-15]와 같이 AhnReport에 저장된 고객의 네트워크 연결정보를 확인하면 그 내용이 [그림 2-14]와 다른 이유는 netstat로 캡쳐한 시점과 AhnReport가 생성된 시점이 다른 것으로 판단되었다. 하지만 다행스럽게도 TCP 445포트를 스캔하고 있는 svchost.exe 프로세스를 찾을 수 있었고, svchost.exe 프로세스를 사용하여 패킷을 뿌리고 있는 서비스를 찾아보니 [그림 2-16]과 같이 랜덤한 서비스명으로 등록된 항목을 발견했다.



DHCP Client	Win32(sh...	Started	Automatic	C:₩WINDOWS₩system32₩svchost.exe -k netsvcs
DNS Client	Win32(sh...	Started	Automatic	C:₩WINDOWS₩system32₩svchost.exe -k Networ...
Distributed Link ...	Win32(sh...	Started	Automatic	C:₩WINDOWS₩system32₩svchost.exe -k netsvcs
Help and Support	Win32(sh...	Started	Automatic	C:₩WINDOWS₩System32₩svchost.exe -k netsvcs
IrDA Protocol	device dri...	Started	Automatic	system32₩DRIVERS₩irda.sys
Logical Disk Ma...	Win32(sh...	Started	Automatic	C:₩WINDOWS₩System32₩svchost.exe -k netsvcs
qgywetzeu	Win32(sh...		Automatic	C:₩WINDOWS₩system32₩svchost.exe -k netsvcs
Remote Procedu...	Win32(sh...	Started	Automatic	C:₩WINDOWS₩system32₩svchost -k rpcss

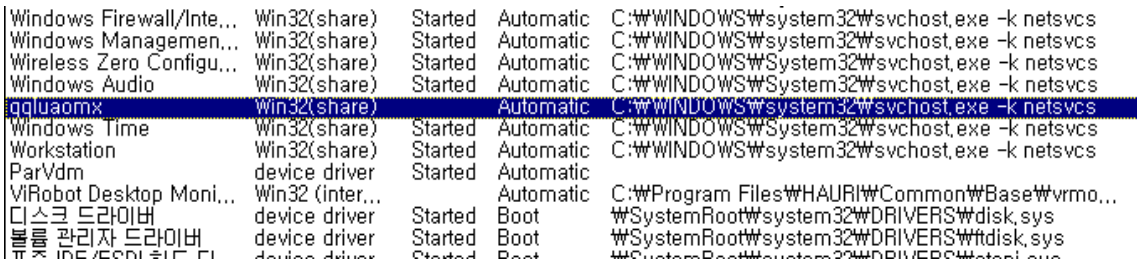
[그림 2-16] A고객 PC의 AhnReport 서비스 정보

마지막으로 서비스 항목에 등록된 qgywetzeu 라는 키값으로 레지스트리에 등록된 파일을 수집하여 긴급 엔진을 내보낼 수 있었다. 하지만 긴급엔진이 제작되는 동안에 또 다른 B고객으로부터

"윈도우 로그인후 5분 안에 컴퓨터가 다운됩니다!"

라는 신고가 접수되었다. B 고객께서 보내주신 AhnReport에서도 네트워크 연결상태가 A 고객과 유사하여 아래 [그림 2-17]과 같이 서비스명으로 등록된 파일을 수집하였으며, 수집된 파일은 분석결과 MS08-067 취약점을 이용하여 제작된 웜으로 네트워크를 통해 자체 전파가 가능하며, 이로 인해 네트워크 트래픽이 증가할 수 있으며, 인터넷 사용속도가 현저히 느려질 수 있다.

위에서 수집한 두 파일은 모두 동일한 악성코드로 V3엔진에 Win32/Conficker.worm.62976으로 진단값이 반영 되었다.



Windows Firewall/Inte...	Win32(share)	Started	Automatic	C:₩WINDOWS₩system32₩svchost.exe -k netsvcs
Windows Managemen...	Win32(share)	Started	Automatic	C:₩WINDOWS₩system32₩svchost.exe -k netsvcs
Wireless Zero Configu...	Win32(share)	Started	Automatic	C:₩WINDOWS₩System32₩svchost.exe -k netsvcs
Windows Audio	Win32(share)	Started	Automatic	C:₩WINDOWS₩System32₩svchost.exe -k netsvcs
qqluaomx	Win32(share)		Automatic	C:₩WINDOWS₩system32₩svchost.exe -k netsvcs
Windows Time	Win32(share)	Started	Automatic	C:₩WINDOWS₩System32₩svchost.exe -k netsvcs
Workstation	Win32(share)	Started	Automatic	C:₩WINDOWS₩system32₩svchost.exe -k netsvcs
ParVdm	device driver	Started	Automatic	
ViRobot Desktop Moni...	Win32 (inter...		Automatic	C:₩Program Files₩HAURI₩Common₩Base₩vrmo...
디스크 드라이버	device driver	Started	Boot	₩SystemRoot₩system32₩DRIVERS₩disk.sys
볼륨 관리자 드라이버	device driver	Started	Boot	₩SystemRoot₩system32₩DRIVERS₩dmboot.sys

[그림 2-17] 또 다른 고객 PC의 안리포트 서비스 정보

MS08-067취약점은 2년전에 발표된 서버서비스 취약점 MS06-040을 비롯하여 악성코드에서 지속적으로 사용하고 있는 LSASS 취약점(MS04-011), DCOM 취약점(MS03-026, MS03-029)과 같은 범주에 포함될 정도로 악성코드에서 활용도가 매우 높다.

이러한 취약점 정보는 해외 보안사이트 등에서 공개된 POC를 기반으로 악성코드 제작에 활용되면서 더욱 더 쉽게 악성코드를 제작할 수 있는 환경이 마련되고 있다. 또한 MS08-067 취약점을 이용한 웜과 같이 네트워크를 통한 직접적인 감염방법이 아니더라도 최근 중국에서 제작된 MS08-067취약점을 이용한 악성코드 자동 제작 툴의 유포로 급속도로 확산될 수 있으며, 스팸 메일이나 다운로더 등과 같이 다양한 방법으로 전파되어 감염될 수 있음으로 사용자는 마이크로소프트의 최신 보안패치를 반드시 설치하여 사고를 미연에 방지하도록 하여야 한다.

III. ASEC 월간 통계

(1) 악성코드 통계 – 트로이목마류 증가세

Top 10 피해 통계

11 월순위		악성코드명	건수	%
1	new	Win-Trojan/OnlineGameHack.863748	50	18.5%
2	new	Win-Trojan/Agent.76800.BP	46	17.0%
2	new	Win32/Mydoom.worm.371712	25	9.3%
4	new	Win-Trojan/Agent.61440.ML	23	8.5%
5	new	Win-Trojan/Agent.75264.BA	22	8.1%
6	new	Win-Trojan/OnlineGameHack.27136.BT	22	8.1%
7	new	Win-Trojan/DlLooee.61440	21	7.8%
7	new	Dropper/OnlineGameHack.20992	21	7.8%
9	new	Win-Trojan/Downloader.98304.AR	21	7.8%
10	new	Win-Trojan/Fakealert.21504.E	19	7.0%
합계			270	100.0%

[표 3-1] 2008년 11월 악성코드 피해 Top 10

[표 3-1]은 2008년 11월 악성코드로 인한 피해 Top 10에 랭크 된 악성코드들로 이들 악성코드들로 인한 총 피해건수는 270건으로 한 달 접수된 총 피해건 수(3,658건)의 7.4%에 해당하며, 지난 10월 227건(7.6%)보다 줄어든 것으로 나타났다.

10월의 Top 10은 모두 트로이목마류였으나, 11월에는 Win32/Mydoom.worm.371712와 Dropper/OnlineGameHack.20992이 순위권에 들었다, 게임핵류의 악성코드 3개가 Top 10에 포함되었으며, 일반적으로 게임핵류의 악성코드는 대부분 변조된 웹사이트를 통해 유포되고 있다는 것을 감안하면, 많은 사이트가 변조되었거나 방문자수가 많은 사이트가 변조되었다고 볼 수 있다.

또한, 3위를 차지한 Win32/Mydoom.worm.371712는 11월 10일경에 고객으로부터 이메일로 확산되고 있다는 신고로 접수된 악성코드로 메일의 주소와 제목은 아래와 같다.

메일 주소: postcards@hallmark.com

메일 제목: You've received A Hallmark E-Card!

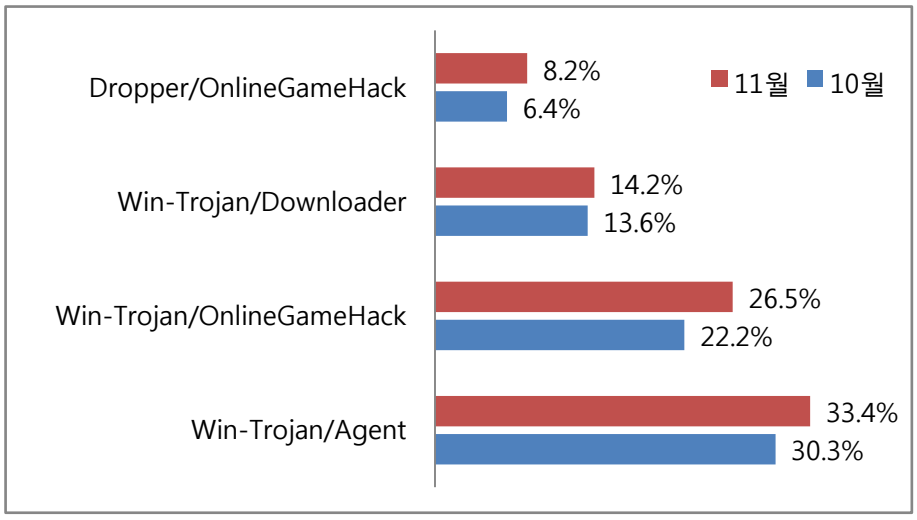
해당 메일에 첨부된 PDF파일로 가장한 실행파일(EXE)인 POSTCARD.PDF를 클릭하게 되면 악성코드 자체에 내장된 SMTP엔진을 이용하여 스팸메일을 발송하는 악성코드이다.

11 월순위	대표 진단명	건수	%
1	Win-Trojan/Agent	768	33.4%
2	Win-Trojan/OnlineGameHack	610	26.5%
2	Win-Trojan/Downloader	327	14.2%
4	Dropper/OnlineGameHack	189	8.2%
5	Dropper/Agent	106	4.6%
6	Win32/Autorun.worm	81	3.5%
7	Win-Trojan/Zlob	64	2.8%
7	Win-Trojan/Krap	57	2.5%
9	Win-Trojan/Autorun	50	2.2%
10	Win-Trojan/Bagle	47	2.0%
합계		2,299	100.0%

[표 3-2] 대표 진단명 기준 Top 10

[표 3-2]는 2008년 11월 악성코드의 대표진단명을 기준으로 대표진단명 Top 10 유형별 피해 순위를 나타내고 있다. 유형별 Top 10에 포함된 악성코드 총 피해건수는 2,299건으로 11월 한 달 접수된 총 피해건수(3,658)의 62.8%를 차지하고 있다.

11월 대표진단명의 건수는 10월 1,265건에 비해 181.7%가 증가하였으나 1, 2, 3, 4위에 랭크된 대표진단명의 비율이 지난 10월과 비교하여 아래 [그림 3-1]과 같이 아주 흡사하다.

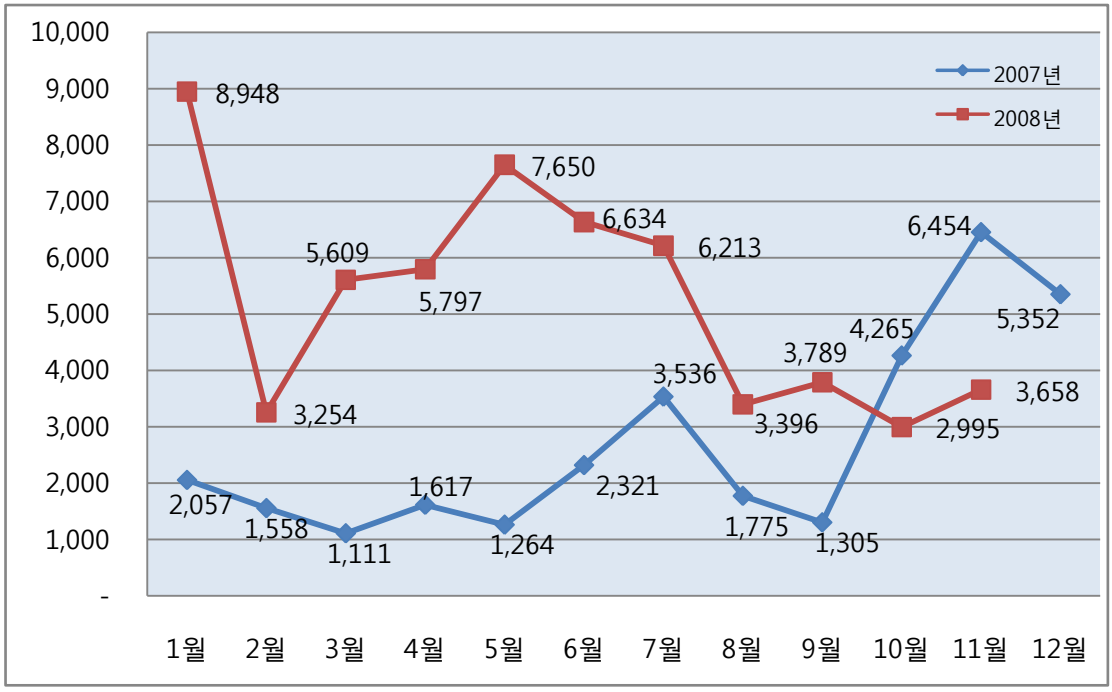


[그림 3-1] 2008년 10월, 11월 주요 대표진단명 비율

국내에서 발견되는 대부분의 악성코드들은 온라인게임핵과 관련된 드롭퍼와 다운로더이며, 이러한 악성코드들은 국내에서 개발된 온라인게임의 계정 및 패스워드를 탈취하기 위한 기능을 가지고 있다. 이러한 추세는 국내 온라인게임산업이 발전할수록 지속적으로 증가할 것으로 예상된다.

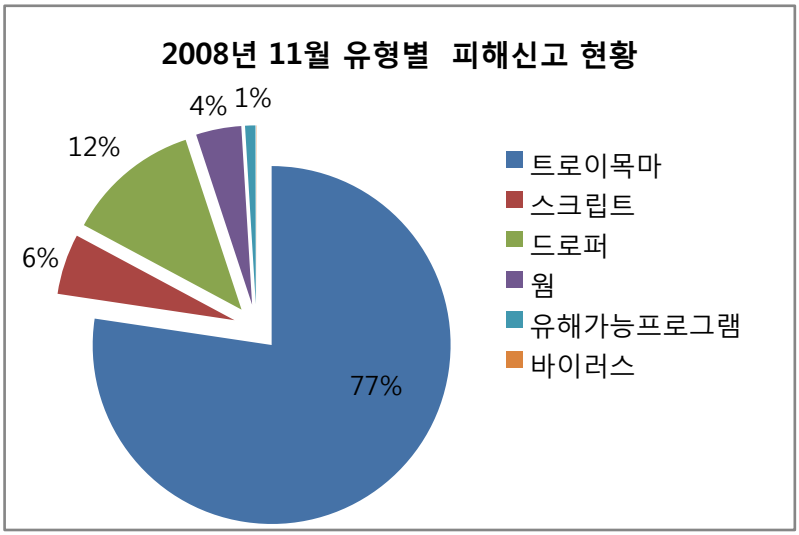
1위와 2위에 랭크된 Win-Trojan/OnlineGameHack.863748과 Win-Trojan/Agent.76800.BP를 제외한 대부분의 악성코드들이 9%, 8%, 7%로 비슷한 분포를 보여주고 있다. 11월은 특정 악성코드에 집중적인 피해는 발생하지 않고 있으나, 오래간 만에 메일로 유포되는 매스메일러인 Win32/Mydoom.worm.371712과 같은 악성코드에 의한 피해신고가 많이 접수되었다.

월별 피해신고 건수



[그림 3-2] 2007, 2008년 월별 피해신고 건수

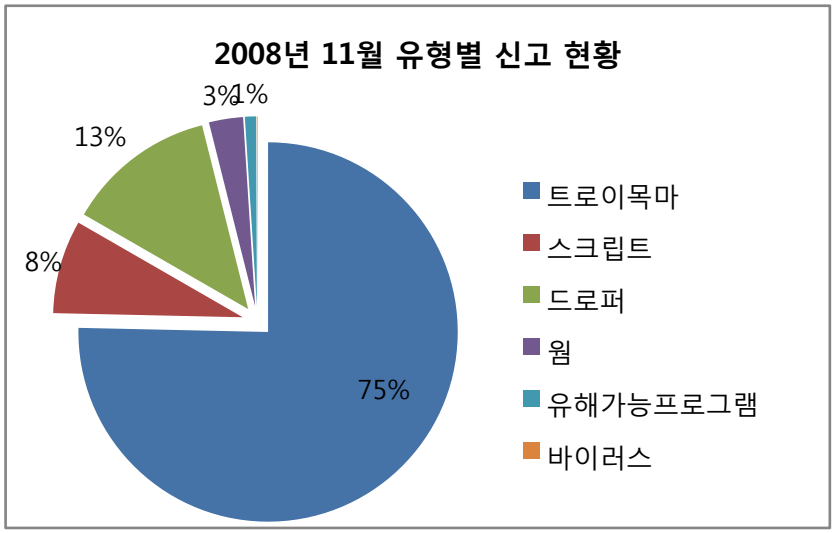
[그림 3-2]는 월별 피해신고 건수를 나타내는 그래프로 11월은 전체 3,658건의 피해신고가 접수되었다. 크리스마스 및 2009년 새해가 다가오면서 “Marry X-mas!”, “Happy new year!”과 같은 스팸 메일이 계속 증가하게 될 것으로 예상되며, 이와 함께 첨부되는 악성코드에 의한 감염으로 피해신고가 증가할 것으로 보인다. 따라서 12월은 발신자가 불분명한 사람으로부터 수신된 메일은 단호히 삭제하여 피해를 미연에 방지해야 할 것이다.



[그림 3-3] 악성코드 유형별 피해신고 건 수

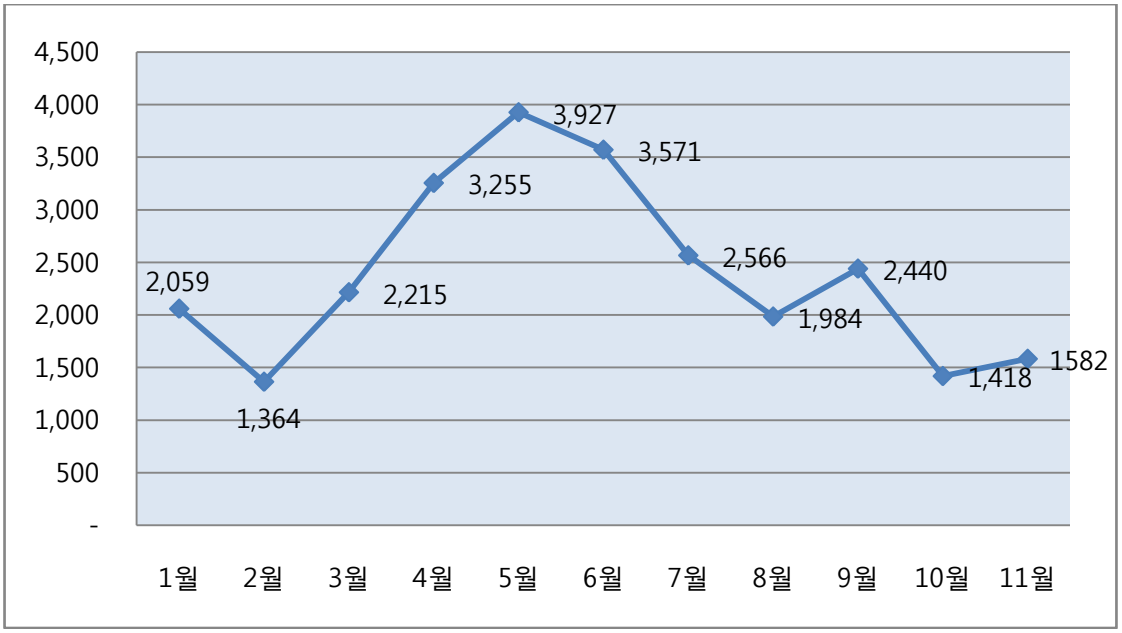
[그림 3-3]은 2008년 11월 전체 악성코드 유형별 피해신고 비율을 나타내고 있는 그래프로서, 여전히 트로이목마가 차지하는 비율은 77%로 높은 비중을 차지하고 있으며, 올해 상반기에 걸쳐 꾸준히 증가하고 있는 드로퍼가 지난달보다 1%증가하였다.

그리고 2008년 상반기부터 트로이목마중 대부분의 다운로더들은 실행될 경우 생성되는 악성코드가 수십개의 또 다른 악성코드를 다운로드하고 있는데, 이러한 다운로더가 다운받는 악성코드가 게임핵과 같은 트로이목마류에 그치지 않고 점차 그 종류가 다양해지고 있다. 그중에서 11월을 떠들석하게 만든 인터넷 시작페이지를 중국사이트(3929.cn)로 고정시키는 악성코드가 대표적이라고 할 수 있는데, 이 악성코드는 다운로더에 의해 다운되는 루트킷류의 악성코드와 함께 동작하였으며 윈도우 정상파일을 변경하고, 악성코드 그 자신이 정상파일인 것처럼 실행되었다. 또한, 11월은 이러한 복합적인 기능을 가진 악성코드가 실행되면서 발생시키는 트래픽으로 인하여 많은 피해신고가 접수되기도 하였다. 이러한 다운로더들은 다운받을 악성코드 URL정보를 빠르게 변경하여 네트워크 장비의 탐지를 우회하는 방법을 사용하며 점차 지능화되고 있다. 따라서 이러한 다운로더를 사전에 차단하기 위한 좀 더 많은 노력이 필요한 시점이다.



[그림 3-4] 피해 신고된 악성코드의 유형별 현황

[그림 3-4]는 11월 한달 간 접수된 유형별 신고건수로 [그림 3-3]의 유형별 피해신고 건수와 마찬가지로 트로이목마가 75%로 여전히 높은 비율을 차지하고 있다. 나머지 스크립트 8%, 드로퍼 13%, 웜 3%, 유해가능프로그램이 1%를 차지하고 있으며 여전히 바이러스는 전체 비율에서 1%도 안 되는 비율을 차지하고 있다.



[그림 3-5] 2008년 월별 피해신고 악성코드 종류

[그림 3-5]는 2008년 월별로 피해신고가 되는 악성코드의 종류를 나타낸 그래프이다. 월별로 신고되는 [그림 3-2]의 월별 피해신고 건수와 마찬가지로 10월에 비해 악성코드 종류도 10% 가량 증가한 것으로 나타났다.

국내 신종(변형) 악성코드 발견 피해 통계

11월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 3-3]과 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
09 월	64	867	97	91	2	0	0	0	13	0	1134
10 월	58	899	130	145	3	0	0	0	16	0	1251
11 월	57	1162	197	151	19	0	0	0	6	0	1592

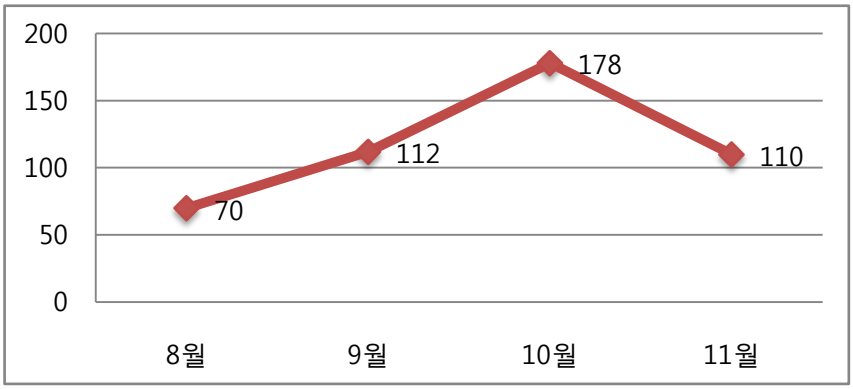
[표 3-3] 2008년 최근 3개월 간 유형별 신종 (변형) 악성코드 발견 현황

지난 달에 이어서 신종 및 변형 악성코드 수가 다시 증가하고 있는 추세이다. 이 번 달은 전월 대비 27% 정도 증가하였다. 특히 트로이목마와 드롭퍼류가 크게 상승하였다. 또한 실행 파일을 감염시키는 바이러스들도 증가 하였다.

트로이목마 유형은 전월 대비 29% 가량 증가하였고, 드롭퍼 유형은 52% 증가하였다. 특히 온라인 게임의 사용자 계정을 탈취하는 형태의 악성코드가 다시 증가를 하기 시작하여, 해당 유형의 악성코드의 트로이목마와 드롭퍼 유형이 전월대비 증가하여 전체적으로 악성코드 증가에 영향을 주었다.

웜 유형중에서는 AutoRun 웜이 가장 많은 비중을 차지하고 있으며, 외산 안티바이러스 업체의 블로그에서도 해당 유형의 악성코드가 증가하고 있다는 글이 포스팅되었는데 이는 어제 오늘의 일이 아니다.

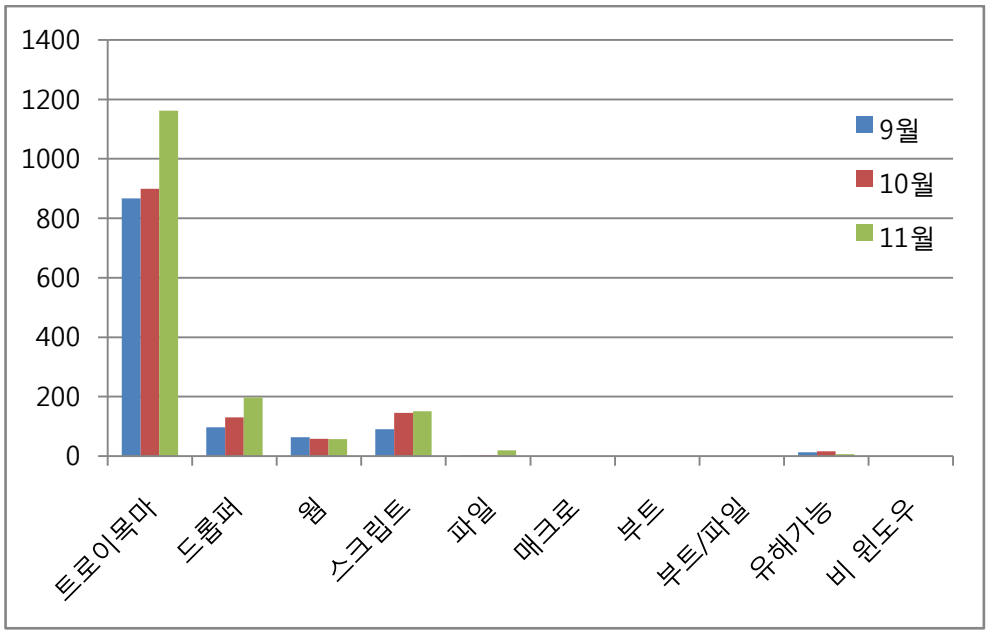
[그림 3-6]에서 지난 4개월간의 해당 유형의 악성코드의 추세를 보면 11월에 감소한 것으로 나오지만, 이는 해당 진단명으로 분류된 것으로 기준으로 했기 때문이고, 일반적인 트로이목마에서도 같은 기법으로 자신을 실행 하도록 하는 형태나 autorun 관련 진단 함수에서 사전에 진단되어 접수되지 않은 관련 유형의 악성코드를 감안하면 이보다 훨씬 많은 관련 유형의 악성코드가 제작되고 있다..



[그림 3-6] AutoRun 관련 악성코드 추세

파일 바이러스중에서는 Win32/Dzan.E, Win32/Golem, Win32/Vimes.B 가 주로 사용자들로부터 보고가 되었다. 이외의 바이러스는 주로 국외의 사용자로부터 감염 신고가 접수되어 엔진에 반영 되었다.

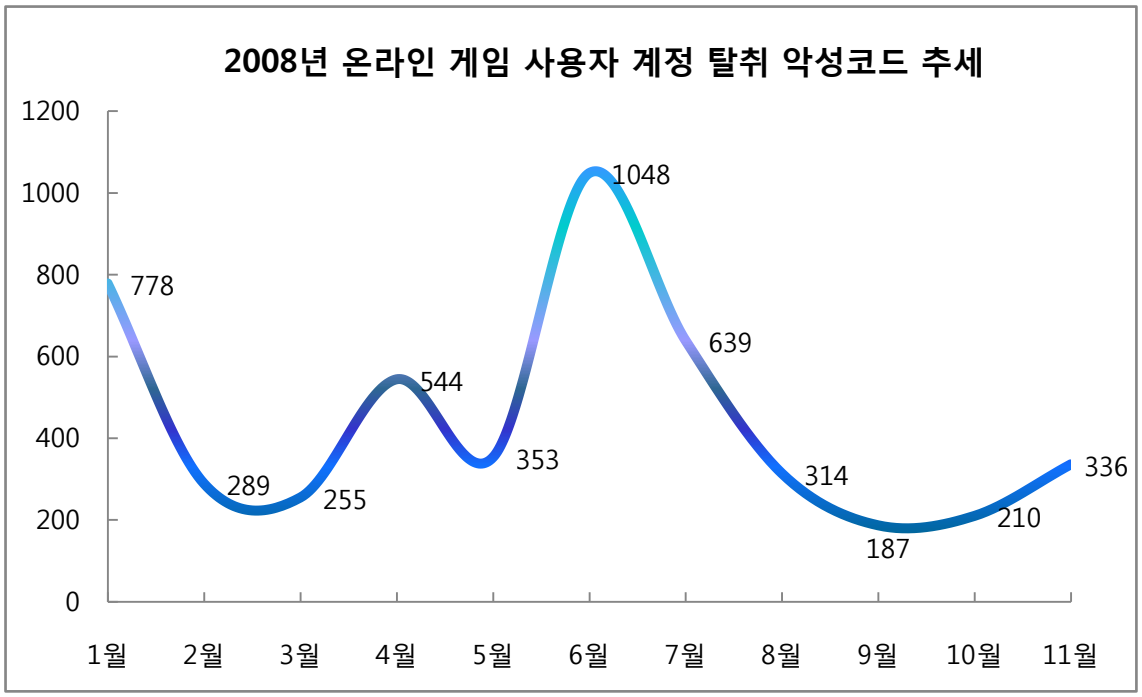
다음 [그림 3-7]은 최근 3개월간 악성코드 분포이다.



[그림 3-7] 최근 3개월간 악성코드 분포

트로이목마와 드롭퍼 유형은 전월 대비 큰 폭으로 상승하였으나, 올 여름 맹위를 떨쳤던 가짜백신 또는 그와 관련된 악성코드는 35건으로 전월과 큰 차이를 보이지는 않았다. 그러나 Win-Trojan/Zlob 이라고 알려진 악성코드는 46건이 발견 되어 전월 대비 30% 증가를 하였으며, 애드웨어 또는 스파이웨어 그리고 가짜백신 등을 다운로드 하여 설치하는 등 다양한 악성코드 또는 스파이웨어를 시스템에 설치하는 역할을 한다.

다음은 트로이목마 및 드롭퍼의 전체 비중에서 상당한 비율을 차지 하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 추세를 살펴보았다.



[그림 3-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

해당 트로이목마는 전월 대비 60% 가량 증가하면서 전월에 이어서 상승세를 유지하고 있다. 특히 한동한 잠잠 했던 특정 실행압축 형태의 변형이 또 다시 발생하면서부터 변형의 수가 증가하고 있다. 대부분 이 트로이목마의 유형이 대량 다운로드 형태가 많기 때문에 변형의 수는 한 동안 증가할 것으로 추정된다.

(2) 스파이웨어 통계 – 루트킷 스파이웨어

순위		스파이웨어 명	건수	비율
1	↑ 1	Win-Spyware/Agent.6144.O	32	22%
2	New	Win-Spyware/PWS.Matory.27136	19	13%
3	New	Win-Spyware/PWS.OnlineGame.14848	16	11%
4	New	Win-Spyware/PWS.WOW.16896.K	15	10%
5	New	Win-Downloader/RogueAnti.5120.B	12	8%
6	New	Win-Spyware/Agent.12800.K	12	8%
7	New	Win-Spyware/Agent.16384.P	11	7%
8	New	Win-Adware/PointGuide.207872	11	7%
9	New	Win-Adware/BHO.PointGuide.323072	10	7%
10	New	Win-Adware/Casino.98304	10	7%
합계			148	100%

[표 3-4] 2008년 11월 스파이웨어 피해 Top 10

스파이웨어 에이전트(Win-Spyware/Agent.6144.O)는 허위 안티-스파이웨어 설치를 목적으로 만들어진 루트킷이 사용하는 모듈로 11월 가장 많은 피해를 입힌 스파이웨어이다. 허위 안티-스파이웨어 프로그램에 대한 모니터링 및 진단 강화로 피해가 10월 이후 감소하긴 했지만 이와 관련된 루트킷 등은 현재도 많은 피해를 입히고 있는 것으로 생각된다. 스파이웨어 피해 Top10의 2위 ~ 4위에는 중국에서 제작된 온라인게임 계정 유출 목적의 스파이웨어가 랭크되어 있다. 이들 온라인게임 계정유출 스파이웨어는 IE취약점을 공격하는 형태로 현재도 널리 전파되고 있다.

스파이웨어 피해 7위와 8위에 올라있는 애드웨어 포인트가이드(Win-Adware/PointGuide)는 무료 자료실, 게임 사이트에서 사용자 동의 없이 ActiveX로 설치된다. 포인트가이드와 같은 적립금 제공 애드웨어는 감염된 사용자가 미리 지정된 쇼핑몰 웹사이트를 이용하는 경우 사용자의 의도와 관계 없이 적립금 서비스를 제공하며, 찾아가지 않는 적립금을 주 수익원으로 한다. 사생활 침해뿐만 아니라 검증되지 않은 프로그램에 의한 시스템 오류, 악성코드 감염의 원인이 될 수 있으므로 인터넷에서 제공되는 무료 서비스, 무료 게임, 무료 자료실 등을 이용할 때는 부가적으로 설치되는 프로그램이 없는지 꼼꼼히 확인하는 것이 필요하다.

순위	대표진단명	건수	비율
1	Win-Downloader/Zlob	226	34%
2	Win-Spyware/Agent	78	12%
3	Win-Spyware/Crypter	64	10%
4	Win-Spyware/Zlob	59	9%
5	Win-Dropper/Zlob	53	8%
6	Win-Adware/Kwsearch	45	7%
7	Win-Adware/CashBack	42	6%
8	Win-Spyware/PWS.OnLineGame	36	5%
9	Win-Downloader/Kwsearch	35	5%
10	Win-Clicker/FakeAlert	29	4%
		597	100%

[표 3-5] 11월 대표진단명에 의한 스파이웨어 피해 Top10

[표 3-5]는 변형을 고려하지 않은 대표진단명에 의한 피해 자료이다. 11월에도 여전히 스파이웨어 즐롭(Zlob)계열의 피해가 많았다. 10월과 비교하여 약간의 순위변화는 있으나 피해 양상은 유사하다.

2008년 11월 유형별 스파이웨어 피해 현황은 [표 3-6]과 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
9월	418	170	179	275	0	77	0	2	5	**1126**
10월	274	235	139	452	0	40	0	2	0	**1142**
11월	417	342	191	492	0	39	0	5	0	**1486**

[표 3-6] 2008년 11월 유형별 스파이웨어 피해 건수

10월에 감소하였던 스파이웨어류의 피해가 증가하였는데, 중국에서 제작된 온라인게임 계정 유출 스파이웨어에 의한 것으로 풀이된다. 캐쉬백(Win-Adware/CashBack), 포인트가이드(Win-Adware/PointGuide) 등의 적립금제공 애드웨어의 영향으로 애드웨어의 피해 신고도 100건 가량 증가하였다.

11월 스파이웨어 발견 현황

11월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표3-7]과 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
9월	244	108	112	188	0	30	0	1	1	**684**
10월	180	138	90	345	0	29	0	2	0	**784**
11월	194	165	120	314	0	26	0	2	0	**821**

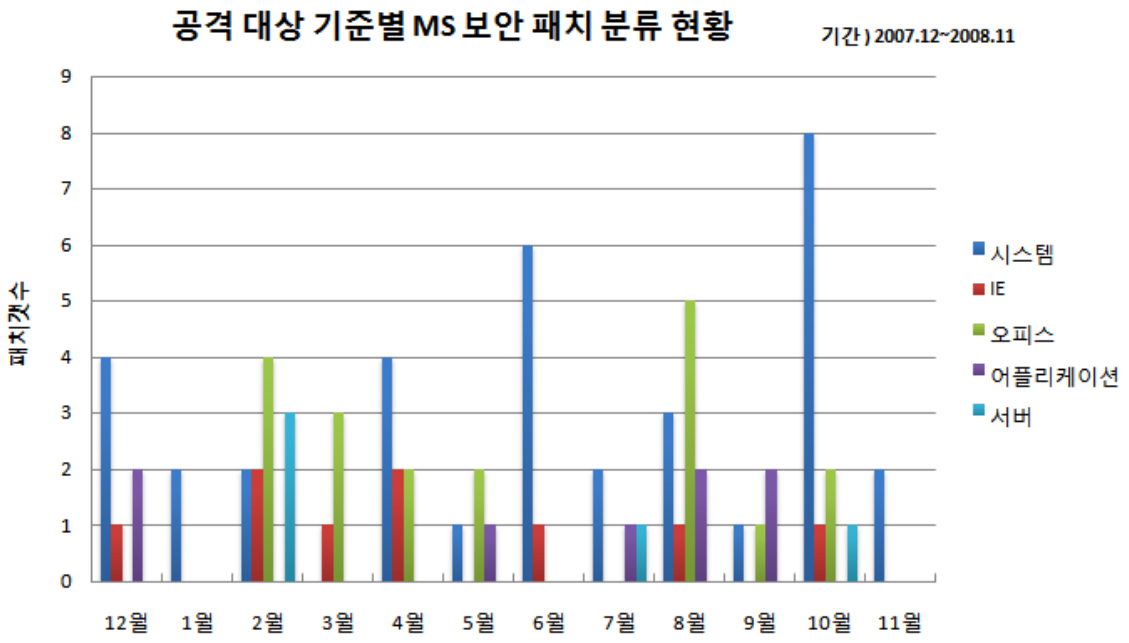
[표 3-7] 2008년 11월 유형별 신종(변형) 스파이웨어 발견 현황

전체적으로 10월과 비슷한 양상을 보이고 있으며 전체 발견 건수는 소폭 증가하였다. 2008년 하반기에 접어들면서 신종 및 변형 스파이웨어 발견 건수가 계속 증가하고 있고 당분간 증가세는 계속 유지될 것으로 예상된다.

(3) 시큐리티 통계 – 11월 시큐리티 통계

2008년 12월에 마이크로소프트사로부터 발표된 보안 업데이트는 총 2건으로 긴급(Critical) 1건, 중요(Important) 1건이다. 우연의 일치인지 모르지만 마이크로그소프트사의 보안 업데이트에서는 재미있는 나름의 비공식적인 법칙을 찾아볼 수 있다. 아래 그래프에서 보듯이 2달을 주기로 그 숫자의 변화가 일정하여 지난 달 업데이트 수가 많았다면 이 달에는 그 수가 매우 감소하는 규칙을 갖는다.

이 달에 발표된 MS08-069 MS XML Core 취약점[1]은 ActiveX 취약점을 이용하여 악의적인 스크립트를 로딩할 수 있는 취약점으로서 웹 공격에 또 다시 이용될 수 있는 충분한 가능성을 갖고 있다. 이미 공격코드가 공개되었으므로 웹 공격으로부터 안전성 확보를 위해 해당 패치에 대한 빠른 적용이 필요할 것이다.



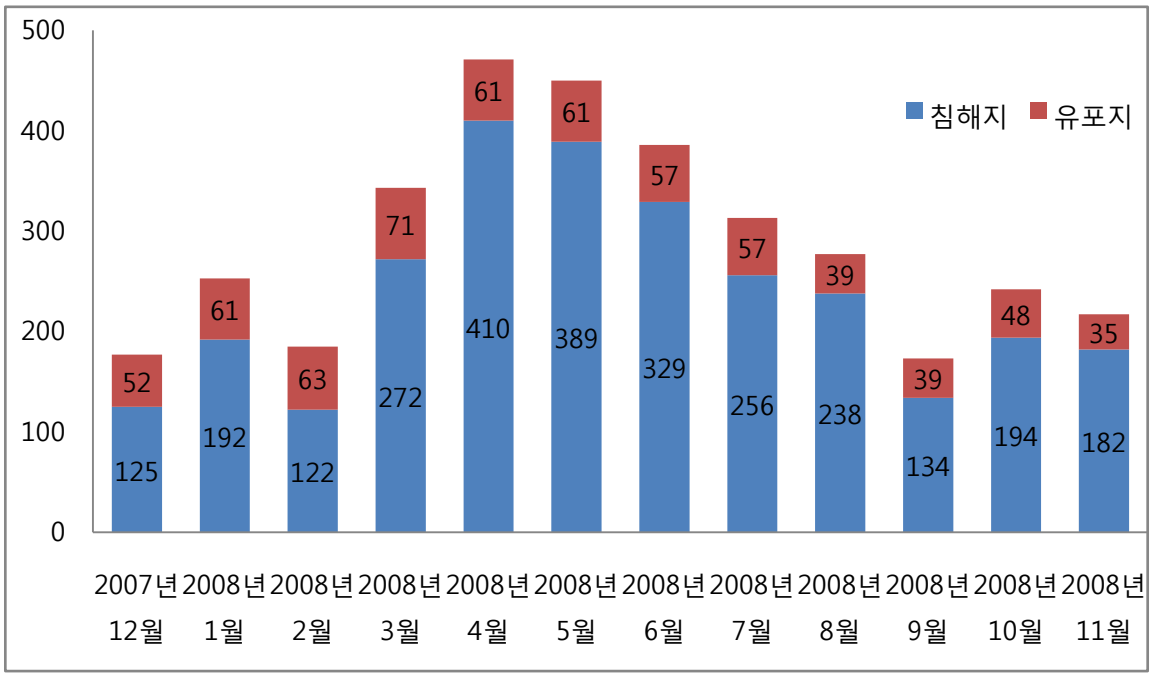
[그림 3-9] 최근 1년간 MS 취약점 건수

위험도	취약점	PoC
긴급	(MS08-069) Microsoft XML Core Services 의 취약점으로 인한 원격 코드 실행 문제점	유
중요	(MS08-068) SMB 의 취약점으로 인한 원격 코드 실행 문제점	무

[표 3-8] 2008년 11월 발표된 주요 MS 보안 패치

[1] http://www.microsoft.com/technet/security/bulletin/ms08-069.mspx

2008년 11월 웹 침해사고 현황



[그림 3-10] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2008년 11월의 웹 사이트 경유지/유포지 수는 182/35로 지난 달의 194/48과 비교하여 큰 차이가 없다. 또한, 11월의 발견 취약점 관련 동향에도 지난달과 큰 차이가 없다. MS07-017 취약점을 이용한 배포가 현저하게 줄었으며, MS08-041 Microsoft Access Snapshot Viewer 취약점을 이용해 악성코드 배포를 시도한 사례가 종종 발견되고 있다.