특집 08

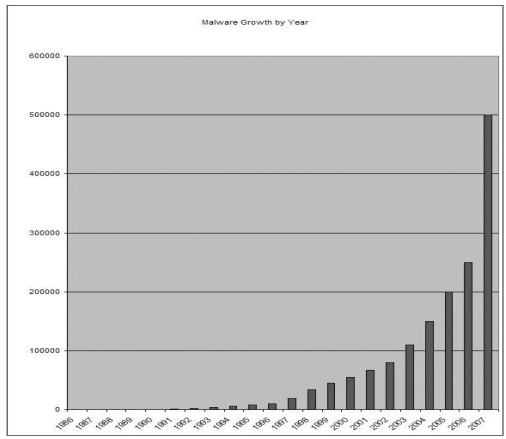
정보유출 방지를 위한 보안 업그레이드 대응방안

목 차

김 윤 근
(이스트소프트)

1. 서 론

1986년 파키스탄에서 세계 최초의 악성코드가 탄생한 이후, 수많은 악성코드들이 등장했다. 초기 악성코드들은 다른 사람을 골탕먹이거나 제작자의 실력을 과시할 목적으로 주로 탄생되었고 대부분 플로피디스크를 통해 다른 시스템으로 전파되었기 때문에 확산이 되는데 많은 시간이 필요했고 따라서 피해 규모가 아주 크진 않았다. 그러나, 2000년대에 들어오면서 악성코드는 인터넷/네트워크의 발전에 따라 (그림 1)과 같이 그 확산속도가 기하급수적으로 빨라졌으며 그에 따라 피해규모도 계속적으로 늘어나고 있다.



(그림 1) 1986~2007년까지의 연간 악성코드 증가율
〈출처: f-secure.com〉

게다가 쇼핑이나 금융거래, 영화감상 등 예전에는 실생활(오프라인)에서만 가능했던 일상의 많은 것들이 네트워크의 발달로 인해 온라인에서 가능하게 되면서 사용자들에게 많은 편의를 제공하게 되었고, 이에 따라 온라인에서 '나'라는 Identity를 구별할 수 있는 정보의 중요도와 가치가 재조명 되었다. 이러한 정보를 악용하여 손쉽게 돈을 벌 수 있다는 것을 깨닫게 된 악성코드 제작자들은 악성코드를 시스템에 침투시키고 다양한 방식을 이용해 시스템 사용자의 '가치'있는 정보를 남몰래 빼내기 시작한 것이다.

2. 정보유출형 악성코드 '트로이목마'

서론에서 언급했듯이, 네트워크 인프라와 정보기술의 급속한 발전으로 인해 일상의 많은 것들이 온라인에서도 가능해졌다. 온라인에서 쇼

핑몰 사이트 혹은 영화 관련 사이트에 접속하여 자신의 계좌번호 및 신용카드번호 그리고 비밀번호를 입력하여 결제를 진행하고, 온라인게임을 즐기기 위해 게임 클라이언트 로그인창에 자신의 아이디와 비밀번호를 입력하여 서비스에 접속하는 일은 몇 년 전부터 주변에서 아주 흔하게 볼 수 있는 부분이다.

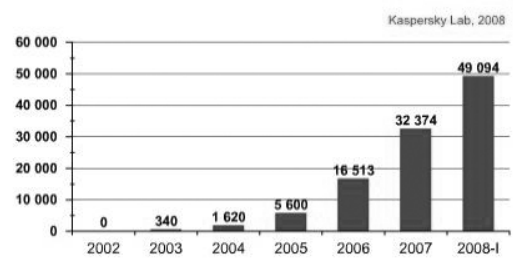
사용자의 정보를 유출시키는 악성코드는 이렇듯 사용자들이 일상 속에서 익숙하게 접하는 부분에서의 틈을 파고든다. 최근 가장 활발하게 유포되고 있는 '트로이목마'도 시스템에 침투하여 사용자 모르게 시스템에 저장되어 있는 데이터를 악성코드 유포자에게 전송하는 대표적인 정보유출형 악성코드이다.

트로이목마 악성코드는 겉에서 보기엔 전혀 문제가 없을 듯한 프로그램으로 가장하여 사용자에게 의심없이 프로그램을 설치하게 한 후 일단 시스템에 설치가 되면 고대 그리스 신화에서 목마에 숨어있던 그리스병사들이 뛰쳐나와서 난공불락이었던 트로이성을 점령하듯이 여러 가지 다른 악성코드들을 불러와서 시스템에 설치시키고 동작시켜 해커가 감염된 시스템을 컨트롤할 수 있게 만드는 것이 주목적이다. '백오리피스(Back Orifice)'와 '넷버스(Netbus)'가 가장 대표적인 트로이목마 악성코드이다.

물론 정보유출형 악성코드에는 트로이목마 외에도 키보드 입력값을 탈취하는 키로거, 해커가 시스템에 마음대로 접근할 수 있도록 시스템의 '뒷문'을 열어주는 역할을 수행하는 백도어 등 여러가지 형태가 존재한다. 하지만 보통 이러한 악성코드들은 따로따로 독립적으로 동작하기 보다는 위에서 언급했던 것처럼 트로이목마와 묶여서 함께 배포되고 동작하거나, 혹은 트로이목마 악성코드 자체에 이러한 기능들이 모두 포함된 경우가 종종 발견되고 있으므로 여기서는 정보를 유출시키는 악성코드들을 통칭하여 '트로이목마'로만 언급하도록 한다.

우리 주변에서 가장 쉽게 트로이목마 악성코드에 유출되기 쉬운 곳은 바로 공공장소에서 많은 사람들이 함께 사용하는 공용PC이다. 공용PC가 주로 많은 곳의 대표적인 예가 들면, 바로 PC방이다. 사람들은 PC방에 가서 별 거부감 없이 자신의 아이디와 비밀번호를 입력하여 온라인 게임에 접속한다. 또한 포털사이트에 로그인하여 이메일을 읽거나 쓰고, 자신의 미니홈피나 블로그에 접속하기도 한다. 그런데 만약 내가 사용하는 PC가 트로이목마 악성코드에 감염이 되어 있는 상태라면? 내가 입력한 정보들이나 PC에 저장된 index.dat같은 데이터파일들이 고스란히 해커의 손에 넘어갈 수 있는 것이다. 이러한 상황은 고등학교나 대학교 PC실습실, 학원 같은 곳에서도 마찬가지이다.

3. '트로이목마' 악성코드 관련 최근 동향



(그림 2) 2002~2008년 상반기까지의 온라인게임 계정 탈취하는 트로이목마 악성코드수 〈출처 : viruslist.com〉

(그림 2)를 보면 우리가 얼마나 많은 정보유출 관련 악성코드의 위협에 노출되어 있는지 알 수 있다. 러시아의 유명 보안업체 Kaspersky Lab에서 2003년부터 2008년 상반기까지 확인한 트로이목마 관련 통계자료만 봐도 온라인게임 계정을 탈취하는 트로이목마 악성코드의 개수가 기하급수적으로 증가했다는 것을 알 수 있다.

온라인게임 계정을 탈취하는 악성코드의 목적은 거의 대부분 금전적인 목적이 크다. 유명게임에서 획득이 어려운 아이템의 경우 아이템 거래

사이트 같은 곳에서 실제 현금 혹은 다른 아이템 등으로 거래가 이뤄지기 때문에 해커들은 온라인게임 계정을 탈취하여 게임에 접속, 해당 아이템을 빼내어 금전적인 이득을 취할 수 있기 때문이다.

예를 들어, 중국의 해커가 한국의 온라인게임 해킹 및 아이템 거래를 통해 2008년 기준 건당 아이템 평균 거래가격인 65,000원을 번다고 가정했을 때, 1주일에 한번만 거래한다고 잡아도 한달이면 26만원이 되며 이는 중국의 2008년 기준 1인당 실질국민소득(GNI) 2,770$을 월간소득으로 나눈 금액 230$과 거의 동일한 수준이 된다.

최근에는 악성코드 제작툴을 손쉽게 구매할 수 있게 되면서 기술적인 지식이 높지 않더라도 악성코드 제작이 간편해짐에 따라 악성코드를 유포하고 손쉽게 금전적인 이득을 취하려는 해커들의 시도가 점점 많아지고 있다.

얼마 전 이슈가 되었던 증권 관련 메신저 악성코드를 봐도, (그림 3)에서와 같이 감염된 시스템의 키보드 타이핑을 가로채고 이 가로챈 정보를 원격서버에 접속하여 전송하는 트로이 목마의 성격이 발견되었다.

```
00403BBA loc_403BBA:                            ; CODE XREF: sub_403B2F+DE
00403BBA                push    0               ; ThreadId
00403BBC                push    [ebp+ImageBase] ; hMod
00403BBF                push    403c19          ; Hook Procedure
00403BC5                push    0               ; WH_JOURNALRECORD (Macro)
00403BC7                call    SetWindowsHookExA
00403BCA                mov     [ebp+var_10], eax
00403BCD
00403BCD loc_403BCD:                            ; CODE XREF: sub_403B2F+E0
00403BCD                push    0
00403BCF                push    0
00403BD1                push    0
00403BD3                lea     eax, [ebp-2Ch]
00403BD6                push    eax
00403BD7                call    GetMessageA
00403BDA                cmp     [ebp+var_28], 12h
00403BDE                jnz     short loc_403C09
00403BE0                push    0F487E123h      ; UnhookWindowsHookEx
00403BE5                push    dword ptr [esi+0ABFh]
00403BEB                push    dword ptr [esi+0E1h]
00403BF1                call    402670          ; Get APIname from hash
00403BF7                push    [ebp+var_10]
00403BFA                call    UnhookWindowsHookEx
00403BFC                push    [ebp+var_30]
00403BFF                call    CloseHandle
```

(그림 3) 감염된 시스템의 키보드 타이핑을 가로채는 증권 관련 메신저 악성코드. SetWindowsHookExA의 후킹타입을 WH_JOURNALRECORD의 사용으로 사용자의 키 입력을 시스템 메시지 큐에서 가로채어 저장한다.

인터넷뱅킹의 경우 정상적인 거래를 위해서는 공인인증서와 보안카드등 여러 가지 인증을 거쳐야 하기 때문에 해킹이 온라인게임에 비해 상대적으로 쉽지 않다고 인식되어 왔으나 인터넷 소액 결제 시스템인 '안심클릭' 같은 경우는 공인인증서가 필요없기 때문에 해킹의 위협에 노출이 되어 있으며 실제로 지난 1월에는 유출된 고객의 카드번호와 안심클릭 비밀번호, 카드인증번호 등을 통해 해커들이 실제로 불법결제를 진행한 것으로 밝혀져서 충격을 주고 있는 상황이다.

4. 정보유출 방지를 위한 대응방안

그렇다면 정보유출을 노리는 악성코드로부터 피해를 예방하기 위해서는 어떻게 대응해야 할까?

4.1 OS 및 프로그램 보안패치 최신버전 유지

Microsoft의 OS인 Windows와 Adobe의 Flash Player등은 대부분의 시스템에 설치되어 있다. 이들에게는 보안취약점이 존재하여, 해커들은 그러한 보안취약점을 이용하여 시스템에 침투하려고 한다. 이를 방지하기 위해서는 제작사에서 발표하는 최신버전의 보안패치를 항상 업데이트하는 것이 좋다. OS와 자주 사용하는 프로그램의 보안패치만 최신으로 유지해도 많은 악성코드로부터의 피해를 예방하는 것이 가능하다.

4.2 백신 설치 및 실시간 감시 기능 활성화

백신 프로그램을 반드시 설치하여 정기적인 점검을 통해 악성코드 존재여부를 체크하고, 실시간 감시 기능을 활성화하여 시스템으로 침투하는 악성코드를 사전에 예방해야 한다. 악성코드는 시시각각 새로운 것들이 쏟아져 나오고 있으므로 악성코드 DB를 항상 최신버전으로 유지해야 함은 물론이다. 요즘 시중에서 쉽게 구할 수 있는 양질의 무료백신들의 경우 대부분 실시

간 감시 기능과 자동 업데이트 기능을 지원한다.

4.3 아이디와 비밀번호의 주기적인 변경

아이디와 비밀번호를 일정기간이 지나면 변경한다. 이때 가입된 모든 사이트의 아이디와 비밀번호를 동일하게 설정해두지 않는 것이 중요하다. 최근 대부분의 포털사이트에서는 일정주기가 지나면 비밀번호를 변경하라는 알림을 띄워주곤 하는데, 귀찮아하지 말고 내 소중한 정보를 지킬 수 있다는 생각으로 조금만 시간을 내서 로그인 정보를 변경하는 것이 좋다.

4.4 공용PC에서의 로그인 지양

많은 사람들이 함께 사용하는 PC에서는 되도록 로그인을 지양하는 것이 좋다. 여러 사람들이 함께 쓰는 PC이기 때문에 주기적인 관리가 쉽지 않기 때문이다. 어쩔 수 없는 상황이라면 반드시 PC가 악성코드에 감염되었는지 여부를 백신을 통해 점검하고, 무료로 제공되는 보안키보드 프로그램을 통해 로그인을 하는 것이 좋다.

4.5 출처가 불분명한 이메일 및 파일 열람 금지

모르는 사람에게서 온 출처가 불분명한 이메일과 첨부파일은 열람하지 말고 바로 삭제하고 P2P나 공유사이트 등에서 불법 파일을 다운로드하지 않는 것이 좋다. 불법으로 공유되는 파일 중 일부는 해커가 악성코드의 확산을 노리고 유포하는 것이 종종 있기 때문이다.

5. 결 론

정보유출 문제는 특히 한국과 같이 인터넷 인프라가 잘 갖춰진 나라에서는 더더욱 문제가 클 수 있다. 네트워크/시스템 인프라가 잘 갖춰져 있어서 악성코드를 유포하는 해커 입장에서는 조금이라도 더 많은 정보를 빠르게 전달받을 수 있고 더 많은 시스템에 악성코드를 확산시킬 수 있기 때문이다.

이러한 문제 때문에 국내의 경우 게임업체들이나 금융업체들의 경우 대부분 게임이나 인터넷뱅킹을 안전하게 할 수 있도록 보안키보드 혹은 온라인 백신 등의 보안모듈을 강제로 설치하게 하여 보안성을 높이고 있다. 또한 게임업계에서는 로그인할때마다 새로운 패스워드를 생성하는 보안시스템인 One Time Password(OTP)를 도입하여 안전한 게임 로그인이 가능하도록 하여 보안을 강화하고 있다.

하지만 이러한 수동적인 보안에는 어느정도 한계가 있기 때문에 정보유출을 방지하기 위해서는 개개인의 정보보호 의식 고취와 보안패치 업데이트, 무료백신 사용 등의 적극적인 실천이 가장 중요하다.

무엇보다도 가장 중요한 것은 개인의 보안의식인데 사실 '정보보호'에 대해 개개인의 의식을 강화시키기는 쉽지 않다. 대부분의 사람들에게는 보안이란 별로 흥미롭지 않고 어렵게 느껴지며, 실제로 실천해보면 번거로운 부분이 존재하기 때문이다. 따라서 국가적으로 보안의 중요성을 좀 더 깨닫고, 개개인의 보안의식 강화를 위해서 일정 비용을 들여서 정기적으로 보안 캠페인을 진행할 필요가 있으며, 초등학교때부터 이러한 부분의 교육이 별도로 이뤄져야 한다. 진정한 보안 업그레이드는 개인사용자로부터 시작되기 때문이다.

참고문헌 및 URL

[1] 악성 모바일 코드 / 한빛미디어, 2001년 12월

[2] 2008년 중국 1인당 GNI / 세계은행, http://www.worldbank.org

[3] 온라인게임 아이템 거래의 명암 / 중앙선데이, http://sunday.joins.com

저자약력

김 윤 근

2006년 연세대학교 경영정보학과 (학사)
2006년 이스트소프트 사업기획팀 입사
2007년 이스트소프트 알툴즈사업본부 알약기획팀
2009년~현재 이스트소프트 알툴즈사업본부 보안대응팀
관심분야 : 보안, UX, OS, 범용 어플리케이션
이 메 일 : deptkim79@estsoft.com