

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 3 월의 악성코드 통계 3

1. 악성코드 통계 3

 (1) 감염 악성코드 Top 15 3

 (2) 카테고리별 악성코드 유형 4

 (3) 카테고리별 악성코드 비율 전월 비교 4

 (4) 월별 피해 신고 추이 5

 (5) 월별 악성코드 DB 등록 추이 5

2. 악성코드 이슈 분석 - "Trojan.Rootkit.LoaderA" 6

 (1) 개요 6

 (2) 악성코드 분석 6

3. 허니팟/트래픽 분석 9

 (1) 상위 Top 10 포트 9

 (2) 상위 Top 5 포트 월별 추이 9

 (3) 악성 트래픽 유입 추이 10

4. 스팸 메일 분석 11

 (1) 일별 스팸 및 바이러스 통계 현황 11

 (2) 월별 통계 현황 11

 (3) 스팸 메일 내의 악성코드 현황 12

Part II 보안 이슈 돋보기 13

1. 3 월의 보안 이슈 13

2. 4 월의 취약점 이슈 14



Part I 3월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2012년 3월 1일 ~ 2012년 3월 31일]

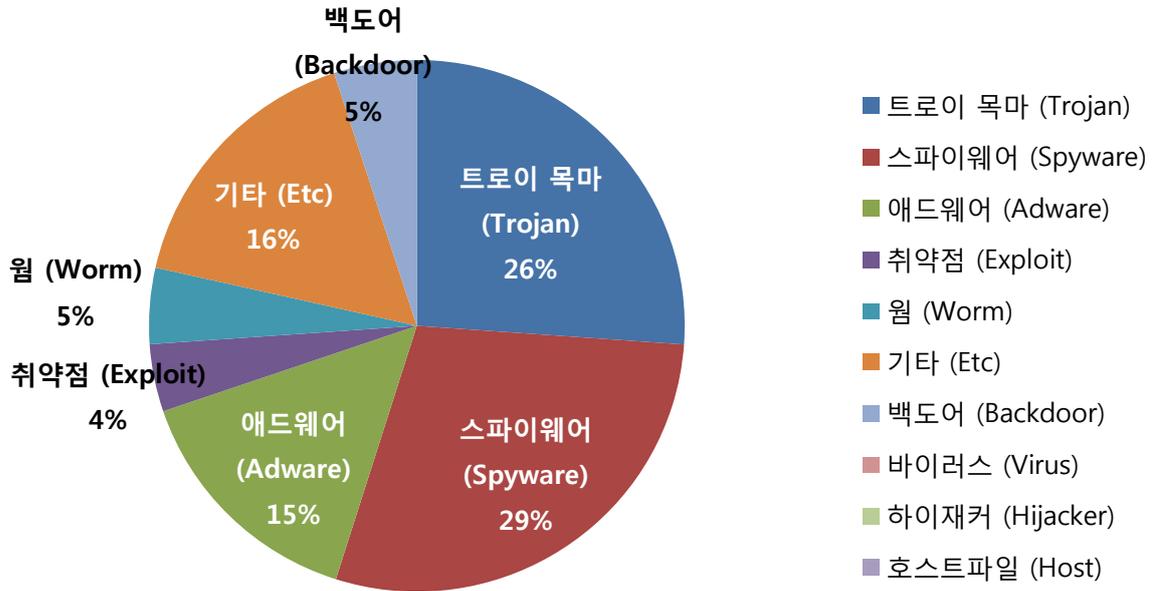
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	Spyware.OnlineGames.wsxp	Spyware	8,685
2	New	Adware.KorAdware.Symax	Adware	3,874
3	New	Variant.Graftor.17181	Etc	2,486
4	New	Trojan.Generic.KDV.569556	Trojan	2,171
5	New	Trojan.Generic.7283501	Trojan	2,156
6	New	Trojan.Generic.7254154	Trojan	1,930
7	New	Script.SWF.Cxx	Etc	1,852
8	New	Backdoor.Agent.RDS	Backdoor	1,822
9	New	Spyware.Lineag-GLG	Spyware	1,795
10	New	Trojan.JS.Agent.FFG	Trojan	1,787
11	New	Worm.Conficker	Worm	1,684
12	New	Gen:Variant.Graftor.Elzob.882	Etc	1,666
13	↓ 2	Adware.Kraddare.CA	Adware	1,555
14	New	Exploit.CVE-2012-0754.Gen	Exploit	1,495
15	New	Trojan.Generic.5663343	Trojan	1,471

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다. 3월의 감염 악성코드 TOP 15는 Spyware.OnlineGames.wsxp가 8,685건으로 TOP 15 중 지난 2월에 이어 압도적인 1위를 차지했으며, 감염자수는 소폭 증가했습니다. 2위는 3월에 새롭게 Top 15에 진입한 Adware.Kor.Adware.Symax가 차지했습니다. Adware.Kor.Adware.Symax는 사용자 모르게 Run 레지스트리에 등록되어 부팅시 자동실행이 되며, 실행이 된 이후에는 사용자가 검색창에 입력하는 검색어에 따라 추가적인 광고창을 팝업시키는 악성 애드웨어입니다. 3월에도 2월과 마찬가지로 주말(대부분 금요일 오후 ~ 월요일 오전 사이)를 이용한 온라인 게임 계정 유출 악성코드인 Spyware.OnlineGames.wsxp가 가장 많이 탐지되었습니다. 그 외 3월에는 Top15에 새로 진입한 악성코드가 총 13개나 된다는 부분이 이색적입니다.

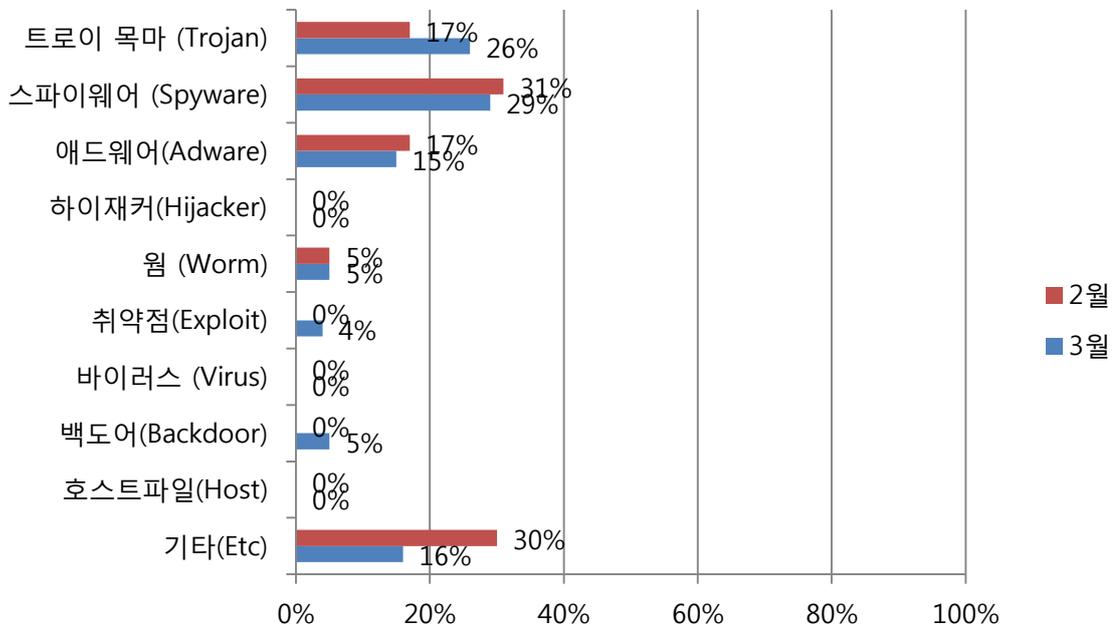


(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 스파이웨어(Spyware)와 트로이목마(Trojan)유형이 각각 29%와 26%로 가장 많은 비율을 차지하였고, 기타(Etc)와 애드웨어(Adware)도 각각 16%, 15%의 비율로 뒤를 이었습니다.

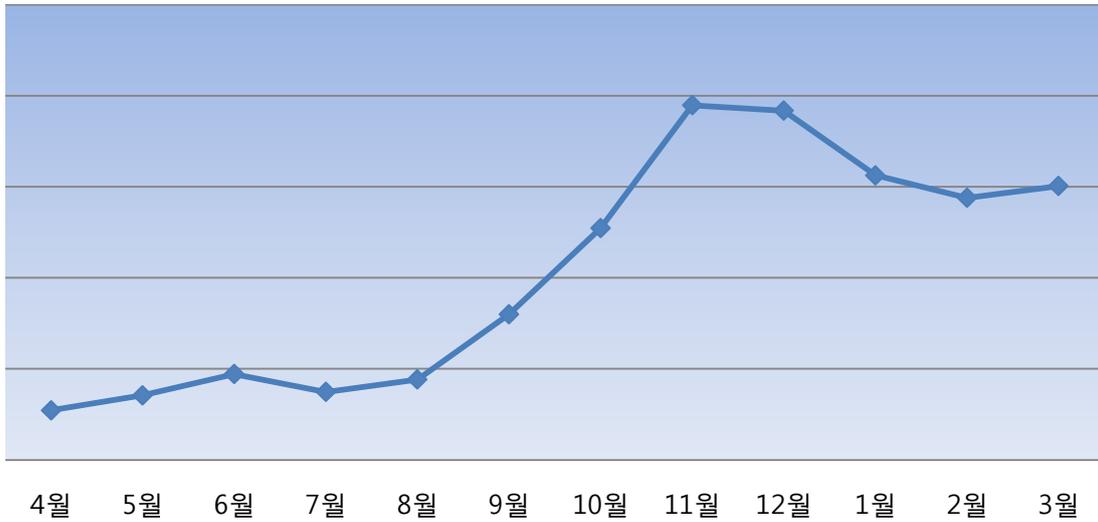
(3) 카테고리별 악성코드 비율 전월 비교



3월의 특이사항은 2월에 비해 트로이목마(Trojan) 유형의 악성코드가 전월에 비해 크게 증가했습니다. 사용자의 로그인 정보등을 유출시키는 스파이웨어(Spyware)의 경우, 2월에 비해 3월에 감염자수는 늘었으나 트로이목마가 급증한 관계로 카테고리별 악성코드 비율이 소폭 감소되었습니다.

(4) 월별 피해 신고 추이

[2011년 4월 ~ 2012년 3월]

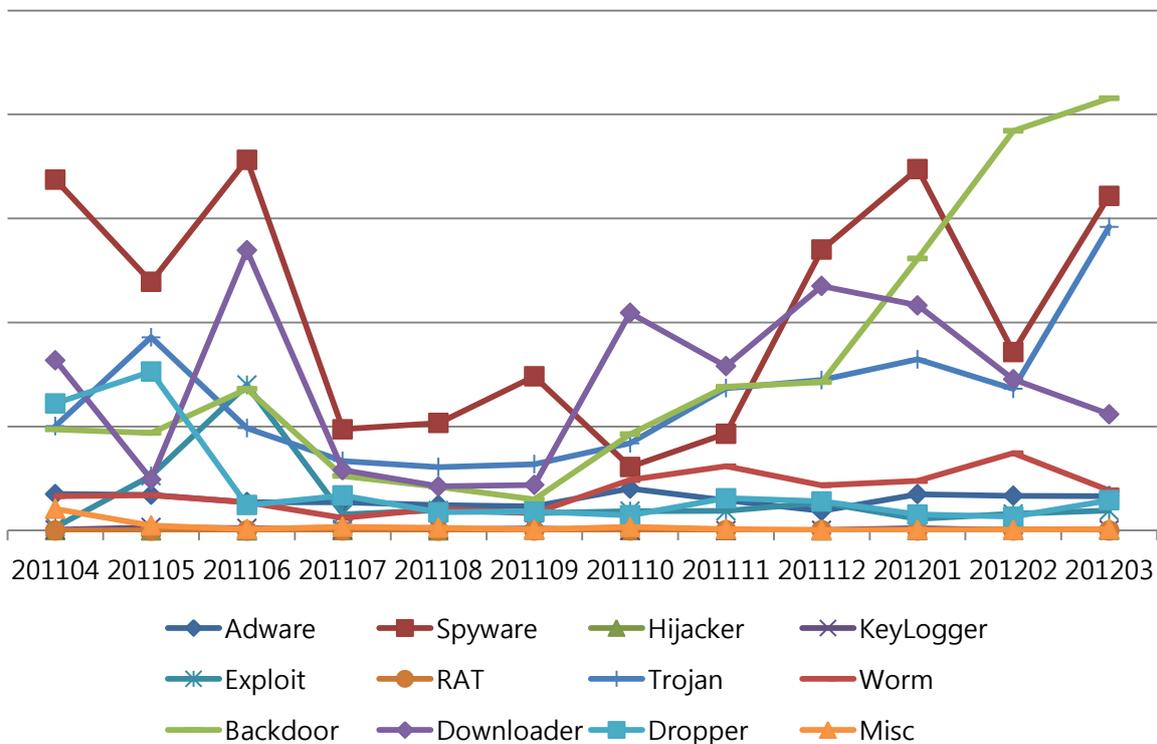


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 자동신고기능에 의해 접수된 데이터가 지난 11월 이후 올해 2월까지는 꾸준히 감소추세를 보이다가 이번 3월부터 신고건수가 소폭 증가하였습니다.

(5) 월별 악성코드 DB 등록 추이

[2011년 4월 ~ 2012년 3월]



Part I 3월의 악성코드 통계

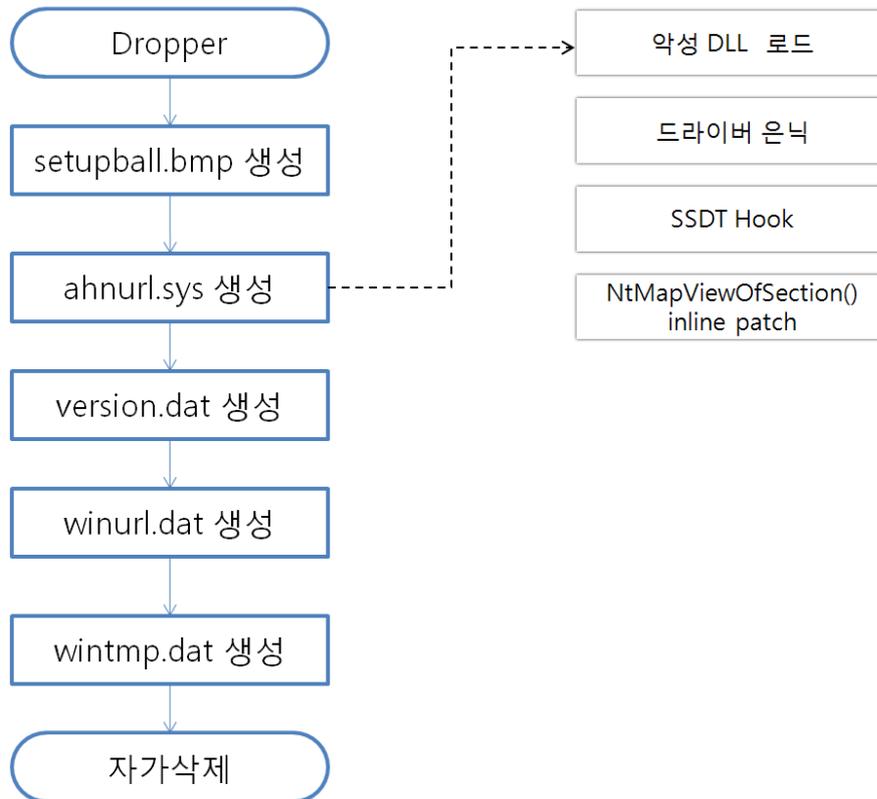
2. 악성코드 이슈 분석 - "Trojan.Rootkit.LoaderA"

(1) 개요

① 대상 파일

파일명	Hash	Size
ahnurl.sys	F386663EB8A0BF17AD4BB89D7FF4992C	28,928

② 프로그램 흐름도



최초 실행되는 Dropper의 경우 악성 DLL(setupball.bmp)과 드라이버 파일을 Drop 및 설치하는 행동을 한다. dat파일의 경우 Flag를 위한 정보를 담은 data파일로 정확한 용도는 확인할 수 없었다. 이 문서에서는 ahnurl.sys 파일에 대한 상세분석을 기술하였다.

(2) 악성코드 분석

① DKOM을 이용한 드라이버 은닉

다음은 설치된 ahnurl 드라이버에 대한 오브젝트 일부이다. 드라이버는 스스로를 은닉하기 위해 오브젝트 오프셋 +14h 위치의 (DriverSection) 메모리를 접근한다. DriverSection은 이중 링크드 리스트로 이루어진 드라이버 리스트에 대한 정보를 제공하기 때문에 여기에 접근하여 링크된 리스트 항목의 앞 뒤 드라이버를 자신을 뺀 채 연결하고 자신을 리스트에서 조회되지 않도록 수정한다.

```

WINDBG>dt _driver_object 80d75db0
ntdll!_DRIVER_OBJECT
+0x000 Type           : 4
+0x002 Size           : 168
+0x004 DeviceObject   : (null)
+0x008 Flags          : 2
+0x00c DriverStart    : 0xfaf24000
+0x010 DriverSize     : 0x7100
+0x014 DriverSection  : 0xffb736c0
+0x018 DriverExtension : 0x80d75e58 _DRIVER_EXTENSION
+0x01c DriverName     : _UNICODE_STRING "\Driver\ahnurl"
    
```

그림1. DriverObject의 DriverSection

```

[ 0x8055d1c0 - 0x80d9a428 ]
+0x000 Flink         : 0x8055d1c0 _LIST_ENTRY [ 0x80f1db20 - 0xffb736c0 ]
+0x004 Blink         : 0x80d9a428 _LIST_ENTRY [ 0xffb736c0 - 0x80da3c88 ]
[ 0x8055d1c0 - 0x80d9a428 ]
+0x000 Flink         : 0x8055d1c0 _LIST_ENTRY [ 0x80f1db20 - 0x80d9a428 ]
+0x004 Blink         : 0x80d9a428 _LIST_ENTRY [ 0x8055d1c0 - 0x80da3c88 ]
    
```

그림2. DriverSection을 통한 Driver Linked List 수정 (전/후)

② SSDT Hook

악성코드는 자신을 보호하기 위해 다음의 Native API대해 Hook을 한다.

NtQueryDirectoryFile(+244), NtEnumerateKey(+11c), ZwEnumerateValueKey(+124)

```

WINDBG>dds KiServiceTable +244 L2
804e48ec faf24dc4 ahnurl+0xdc4
804e48f0 805863a1 nt!NtQueryDirectoryObject
WINDBG>dds KiServiceTable +11c L2
804e47c4 faf24fd2 ahnurl+0xfd2
804e47c8 8064aad3 nt!NtEnumerateSystemEnvironmentValuesEx
WINDBG>dds KiServiceTable +124 L2
804e47cc faf250ce ahnurl+0x10ce
804e47d0 80627720 nt!NtExtendSection
    
```

그림 3. SSDT Hook

위의 함수들은 레지스트리 및 파일을 조회할 때 호출되는데, 이는 인자값을 감시하여 자신이 원하는 레지스트리나 파일을 삭제하지 못 하도록 보호하기 위함이다. *Hook으로 인해 실행되는 함수는 별도로 분석하지 않았다.

③ NtMapViewOfSection API Inline Code Patch

우선 NtMapViewOfSection함수를 패치하는 목적은 다음과 같다.

프로세스는 새롭게 생성될 때 OS에 의해 독립적인 유저 메모리를 공간을 할당받고 이 공간을 통해서 코드를 실행한다. 특히 DLL은 효율적인 메모리 활용을 위해 Mapping된 파일을 불러오게 되어 있는데 해당 정보를 조회할 때 NtMapViewOfsection이 호출되게 된다. 따라서 이 함수를 수정하면 DLL이 로드됨과 동시에 자신이 원하는 행동도 임의 실행할 수 있게 되는 것이다.

```

WINDBG>u nt!ntmapviewofsection
nt!NtMapViewOfSection:
80575b61 6a44          push    44h
80575b63 68e8404f80    push   offset nt!MMDB+0x50 (804f40e8)
80575b68 e8cee8f6ff    call   nt!_SEH_prolog (804e443b)
80575b6d 837d1415      cmp    dword ptr [ebp+14h],15h
80575b71 0f8752e50700 ja     nt!NtMapViewOfSection+0x141 (805f40c9)
80575b77 837d2402      cmp    dword ptr [ebp+24h],2
80575b7b 0f8fa7bf0600 jg     nt!NtMapViewOfSection+0x389 (805e1b28)
80575b81 33c0          xor    eax,eax

WINDBG>u nt!ntmapviewofsection
nt!NtMapViewOfSection:
80575b61 e970839e7a    jmp    ahnurl+0x1ed6 (faf5ded6)
80575b66 4f            dec    edi
80575b67 80e8ce        sub    al,0CEh
80575b6a e8f6fff837d   call   fddb5b65
80575b6f 1415          adc    al,15h
80575b71 0f8752e50700 ja     nt!NtMapViewOfSection+0x141 (805f40c9)
80575b77 837d2402      cmp    dword ptr [ebp+24h],2
80575b7b 0f8fa7bf0600 jg     nt!NtMapViewOfSection+0x389 (805e1b28)
    
```

그림 4. NtMapViewOfSection API 수정 (전/후)

Patch가 된 NtMapViewOfSection API는 사전에 buffer에 저장한 주소로 점프하게 되는데 해당 주소코드의 역할은 주요 온라인게임 계정을 해킹하는 악성코드 DLL파일을 로드하게 된다.

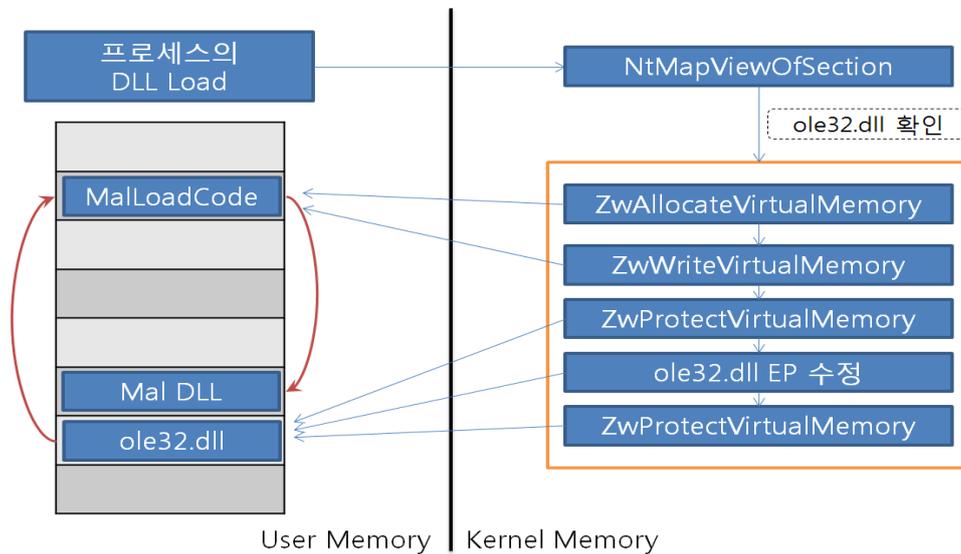
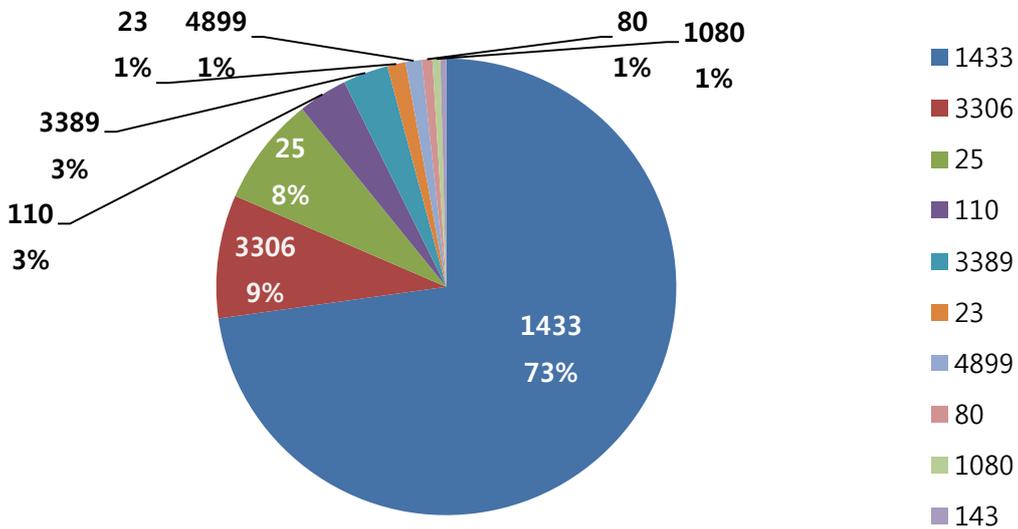


그림 5. NtMapViewOfSection Patch를 통한 악성 DLL 로드

Part I 3월의 악성코드 통계

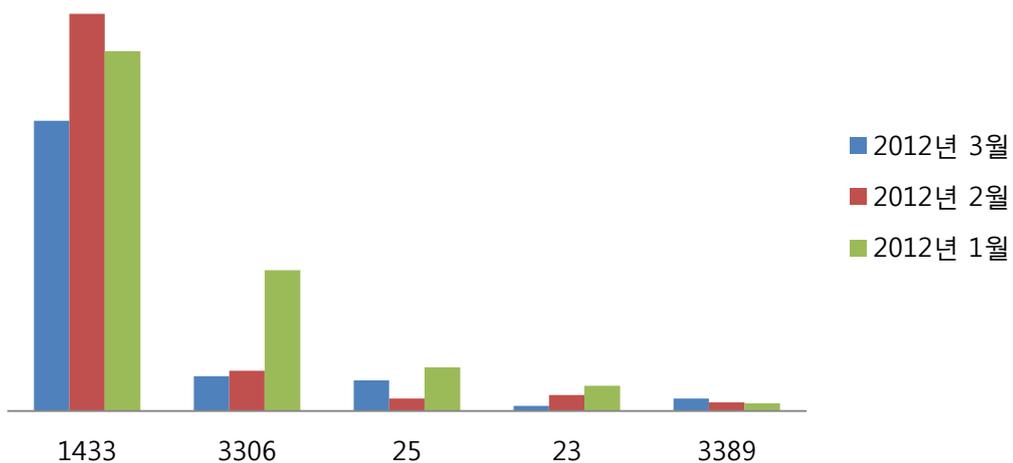
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



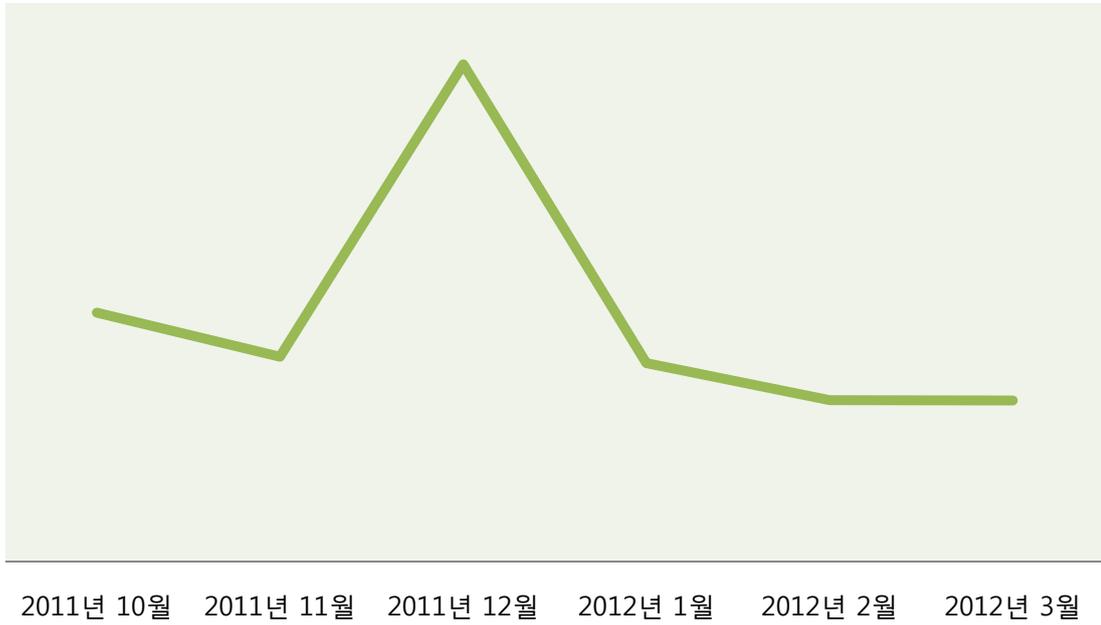
(2) 상위 Top 5 포트 월별 추이

[2012년 01월 ~ 2012년 03월]



(3) 악성 트래픽 유입 추이

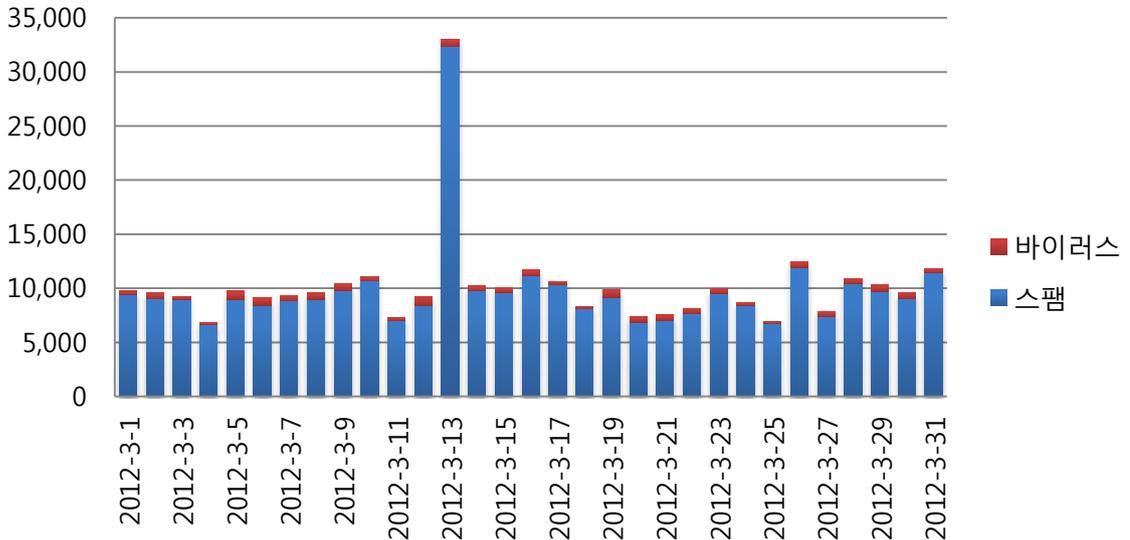
[2011년 10월 ~ 2012년 03월]



Part I 3월의 악성코드 통계

4. 스팸 메일 분석

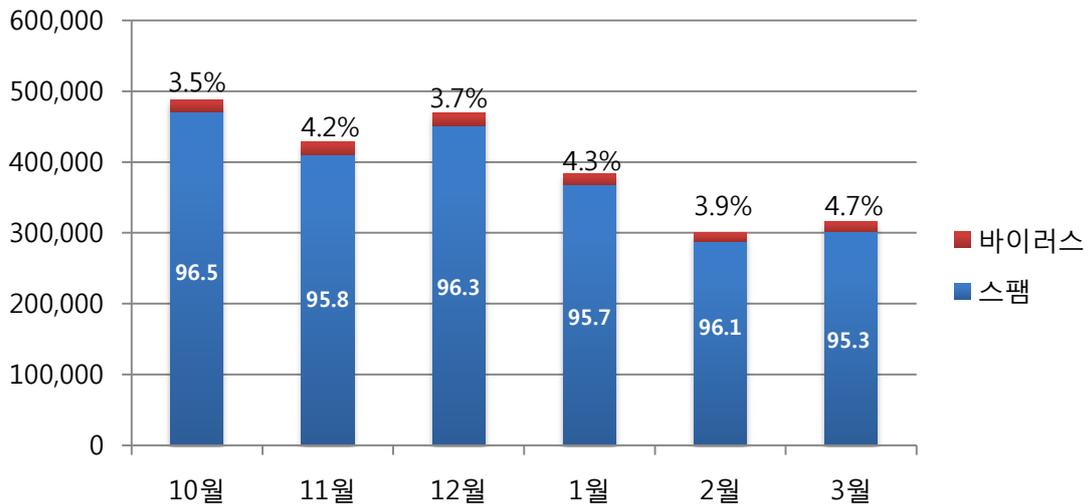
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 3월의 경우 2월에 비해 스팸메일 통계수치 및 바이러스 통계수치가 소폭 상승하였습니다.

(2) 월별 통계 현황

[2011년 10월 ~ 2012년 3월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 3월에는 스팸 메일이 95.3%, 바이러스첨부 메일이 4.7%의 비율로 수신된 것으로 나타났습니다.

(3) 스팸 메일 내의 악성코드 현황

[2012년 3월 1일 ~ 2012년 3월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	6,710	44.76%
2	W32/MyDoom-H	3,364	22.44%
3	Mal/ZipMal-B	2,312	15.42%
4	W32/Virut-T	471	3.14%
5	W32/Lovgate-V	421	2.81%
6	W32/Mytob-G	316	2.11%
7	Troj/Invo-Zip	134	0.89%
8	Mal/BredoZp-D	120	0.80%
9	W32/Bagz-D	91	0.61%
10	Mal/BredoZp-B	87	0.58%

스팸 메일 내의 악성코드 현황은 3월 한달동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 44.76%로 1,2월에 이어 3달 연속으로 1위를 차지하였으며, 2위는 22.44%를 차지한 W32/MyDoom-H, 3위는 15.42%를 차지한 Mal/ZipMal-B입니다. 2위와 3위 역시 비율의 변화는 있었으나 지난달과 동일한 순위를 보이고 있습니다.



Part II 보안 이슈 돋보기

1. 3월의 보안 이슈

국내 최대 포털사이트가 자사의 뉴스캐스트에서 악성코드가 포함된 인터넷 기사를 차단해 이슈가 되었습니다. 그밖에 구글 서비스 개인정보 통합, 개인병원 홈페이지 비밀상담 글 노출 문제, 카카오톡을 이용한 피싱 사기 등이 3월의 이슈가 되었습니다.

• 구글 논란 속 개인정보 통합

구글이 운영하는 60개 서비스의 사용자 정보를 통합하는 구글의 새 개인정보 취급정책이 많은 논란 중에 3월부터 시행되었습니다. 방송통신위원회는 개인정보의 활용 목적을 이용자에게 충분히 알리고 각각 동의를 받으라는 권고를 하였습니다.

• 악성코드 유포 언론사, 기사 차단

국내 최대 포털사이트는 인터넷 뉴스기사 내 악성코드가 포함되었다는 것을 이유로 뉴스캐스트 서비스에서 8개 언론사의 기사를 차단했습니다. 포털측은 이용자를 악성코드로부터 보호하기 위한 조치라고 했지만, 파급력있는 포털사이트가 특정 언론의 기사를 차단했다는 점에서 언론계는 반발하며 우려를 나타냈으며, 포털측도 기사차단 정책을 일단 보류하고 신중히 검토한다는 입장입니다.

• 특정 언론사에 직접적인 해킹공격 발생

일부 언론사가 자사의 서버에 직접 해킹공격을 받아 악성코드를 배포했습니다. 인터넷신문 기사를 통해 악성코드가 유포되는 경우, 주로 광고대행사의 서버가 공격을 당하게 되는데 이번 공격은 언론사 서버가 직접 해킹되어 이례적입니다. 뉴스캐스트 차단 등의 목적을 지닌 해킹이라는 주장도 있었지만 확인되지는 않았습니다.

• 모바일뱅킹 해킹앱 기승

변조된 스마트폰 응용프로그램을 통해 모바일뱅킹에 접속하는 사례가 수년 동안 확산되고 있으며 금융기관들이 이에 대해 거의 무방비 상태라는 지적이 나왔습니다. 검증되지 않은 해킹앱을 사용해 은행에 접속하거나, 접속 중에 개인 बैं킹정보를 입력하면 정보가 유출될 수 있으므로 위험합니다. 지난해 10월 개정 고시된 전자금융감독규정에 '전자금융거래프로그램의 위·변조 여부 등 무결성을 검증할 수 있는 방법 제공'에 관한 의무 규정이 신설됨에 따라 시중 은행들은 4월 10일까지 이에 대해 대비를 해야 합니다. 일부 은행들은 변조된 해킹앱을 통해서도 뱅킹에 접속할 수 없도록 보안조치를 완료했다고 밝혔습니다.

• 카카오톡 이용한 피싱사기 사례 발생

서울 동작경찰서는 카카오톡 이용자가 메신저피싱을 당했다고 신고해옴에 따라 수사에 착수했습니다. 피해자는 평소 카카오톡으로 대화를 하던 친구로부터 급하게 돈을 빌려달라는 부탁을 받았으며 평소처럼 대화명과 사진이 같아 의심 없이 송금했지만 10분후에 사

기피해임을 알았다고 합니다. SNS피싱의 사기수법이 끊임없이 발전하고 있어 온라인 송금 시에는 항상 상대방이 맞는지, 가짜 기관은 아닌지를 확인하는 습관이 필요합니다.

• 개인병원 홈페이지 상담 글 보안 허술

개인병원들이 의료시술 상담을 위해 운영하고 있는 게시판의 비밀 상담글이 손쉽게 노출될 수 있는 문제가 드러났습니다. 특히, 별다른 해킹기술 없이도 주소창의 숫자를 변경하는 것만으로 비밀 상담 글을 열람할 수 있어 개인병원 홈페이지의 보안 강화가 시급하다는 지적입니다.

2. 4월의 취약점 이슈

• Microsoft 4월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Windows의 취약점으로 인한 원격 코드 실행 문제, .NET Framework의 취약점으로 인한 원격 코드 실행 문제, Windows 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제해결 등을 포함한 Microsoft 4월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

<취약점 목록>

Internet Explorer 누적 보안 업데이트(2675157)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 5건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Windows의 취약점으로 인한 원격 코드 실행 문제점(2653956)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자나 응용 프로그램이 영향을 받는 시스템에서 특수하게 조작되고

서명된 이식 가능한 실행(PE) 파일을 실행 또는 설치할 경우 원격 코드 실행이 허용될 수 있습니다.

.NET Framework의 취약점으로 인한 원격 코드 실행 문제점(2671605)

이 보안 업데이트는 비공개적으로 보고된 Microsoft .NET Framework의 취약점 한 가지를 해결합니다. 사용자가 XBAP(XAML 브라우저 응용 프로그램)을 실행할 수 있는 웹 브라우저를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 이 취약점으로 인해 클라이언트 시스템에서 원격 코드가 실행될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다. 서버에서 ASP.NET 페이지 처리를 허용하고 공격자가 해당 서버에 특수하게 조작한 ASP.NET 페이지를 성공적으로 업로드하여 실행할 경우 이 취약점으로 인해 IIS를 실행하는 서버 시스템에서 원격 코드 실행이 허용될 수 있습니다. 이러한 경우는 웹 호스팅 시나리오에서 발생할 수 있습니다. 이 취약점은 CAS(코드 액세스 보안) 제한을 우회하기 위해 Windows .NET 응용 프로그램에서 사용될 수도 있습니다. 웹 탐색을 통한 공격의 경우 공격자는 호스팅하는 웹 사이트에 이 취약점을 악용하는 웹 페이지를 포함할 수 있습니다. 또한 사용자가 제공한 콘텐츠나 광고를 허용하거나 호스팅하는 공격 당한 웹 사이트에는 이 취약점을 악용할 수 있는 특수하게 조작된 콘텐츠가 포함되어 있을 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

Windows 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점(2664258)

이 보안 업데이트는 Windows 공용 컨트롤의 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 취약점을 악용하도록 설계된 특수하게 조작된 콘텐츠가 포함된 웹 사이트를 방문할 경우 원격 코드 실행이 허용될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다. 악성 파일은 전자 메일 첨부 파일로도 전송될 수 있지만 공격자가 이 취약점을 악용하려면 사용자가 첨부 파일을 열도록 유도해야 합니다.

Forefront UAG(Unified Access Gateway)의 취약점으로 인한 정보 유출 문제점(2663860)

이 보안 업데이트는 Microsoft Forefront UAG(Unified Access Gateway)에서 비공개적으로 보고된 취약점 2건을 해결합니다. 가장 심각한 취약점으로 인해 공격자가 UAG 서버에 특수하게 조작된 쿼리를 보내면 정보 유출이 발생할 수 있습니다.

Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2639185)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office 및 Microsoft Works의 취약점

을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 Works 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : <http://technet.microsoft.com/ko-kr/security/bulletin/ms12-apr>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/ms12-apr>

• **Adobe Reader/Acrobat 신규 취약점 주의 권고**

CVE Number : CVE-2012-0777 외

Adobe Reader 및 Acrobat에 영향을 주는 다중의 취약점을 해결한 보안 업데이트가 발표되었습니다. 낮은 버전의 Adobe Reader/Acrobat 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

- 윈도우, 매킨토시 환경에서 동작하는 Adobe Reader X (10.1.2) 및 10.x 이전 버전
- 윈도우, 매킨토시 환경에서 동작하는 Adobe Reader 9.5 및 9.x 이전 버전
- 리눅스 환경에서 동작하는 Adobe Reader 9.4.6 및 9.x 이전 버전
- 윈도우, 매킨토시 환경에서 동작하는 Adobe Acrobat X (10.1.2) 및 10.x 이전 버전
- 윈도우, 매킨토시 환경에서 동작하는 Adobe Acrobat 9.5 및 9.x 이전 버전

<해결 방법>

• **Adobe Reader 사용자**

아래의 Adobe Download Center를 방문하여 업데이트 버전을 설치하거나 [메뉴]→[도움말]→[업데이트확인]을 이용하여 업그레이드

- 윈도우 환경에서 동작하는 Adobe Reader 9.x 사용자

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows>

• **Adobe Acrobat 사용자**

아래의 Adobe Download Center를 방문하여 업데이트 버전을 설치하거나 [메뉴]→[도움말]→[업데이트확인]을 이용하여 업그레이드

- 윈도우 환경에서 동작하는 Adobe Acrobat Standard/Pro 사용자
<http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows>
- 윈도우 환경에서 동작하는 Adobe Acrobat Pro Extended 사용자
<http://www.adobe.com/support/downloads/product.jsp?product=158&platform=Windows>

<참고 사이트>

<http://www.adobe.com/support/security/bulletins/apsb12-08.html>

Contact us...

(주)이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

알약 Korea Master Brand Awards 2012
대한민국 대표브랜드 대상 수상기념
궁디팡팡 이벤트

보안솔루션 부문 1등
2012 MASTER BRAND

여러분의 성원에 힘입어 알약이 2012 대한민국 대표브랜드 대상을 수상하였습니다. 앞으로도 최선을 다하여 여러분의 사랑에 더 큰 감동으로 보답하겠습니다.

SNS를 통해서 알약 대표브랜드 대상 수상을 축하해주세요! 추첨을 통해 총 100분에게 다양한 경품을 드립니다.

- 참여기간**
2012년 4월 19일(목요일)부터 5월 3일(목요일) 까지
- 당첨발표**
2012년 5월 7일(월요일) 알뜰즈 블로그에 공지합니다.
- 당첨인원**
총 100명 (각 경품당 20명)
- 경품**
온라인문화상품권 버거세트 교환권 커피교환권 도넛&커피 교환권 아이스크림 교환권

참여방법

STEP 1
오른쪽 자신이 사용중인 SNS 버튼을 클릭하여 알약 수상을 축하해주세요!

STEP 2
SNS 작성후 하단의 응모란에, 경품 받을 연락처를 남기면 이벤트 응모 완료!

SNS로 궁디팡팡!

- 트위터로 궁디팡팡 >
- 페이스북으로 궁디팡팡 >
- 미투데이로 궁디팡팡 >
- 요즘으로 궁디팡팡 >

<http://expose.estsoft.com/?event=201111181660299>