www.alyac.co.kr

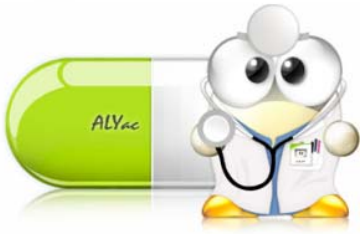
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part I 6월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

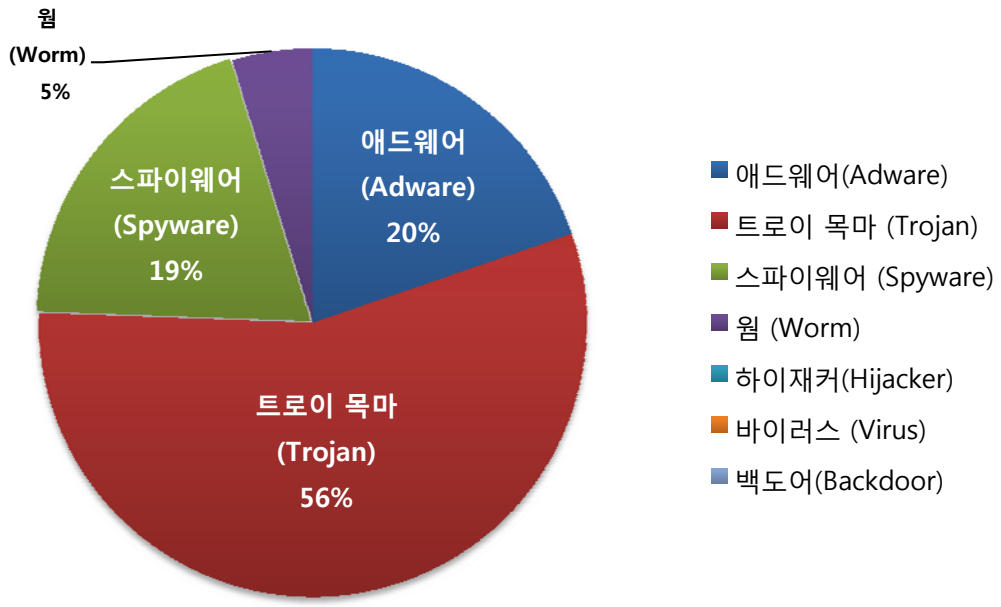
[2010년 6월 1일 ~ 2010년 6월 30일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	V.DWN.Agent.Pinsearch	Trojan	65,249
2	↓1	A.ADV.Admoke	Adware	56,579
3	↓1	S.SPY.Lineag-GLG	Spyware	44,852
4	New	Adware.Generic.133922	Adware	34,096
5	↓20	V.DWN.Agent.2456	Trojan	31,683
6	New	V.DWN.VB.paran	Trojan	29,160
7	New	Trojan.Generic.4079324	Trojan	25,989
8	New	Trojan.Generic.4119434	Trojan	25,657
9	↑1	S.SPY.OnlineGames.kb	Spyware	24,337
10	↓4	V.WOM.Conficker	Worm	21,771
11	↓5	S.SPY.OnlineGames-H	Spyware	21,266
12	New	Trojan.Generic.4303990	Trojan	21,104
13	New	V.DWN.el.39xxxx	Trojan	20,510
14	New	Trojan.Generic.4153251	Trojan	19,492
15	New	Trojan.Generic.4338298	Trojan	17,572

※ 자체수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

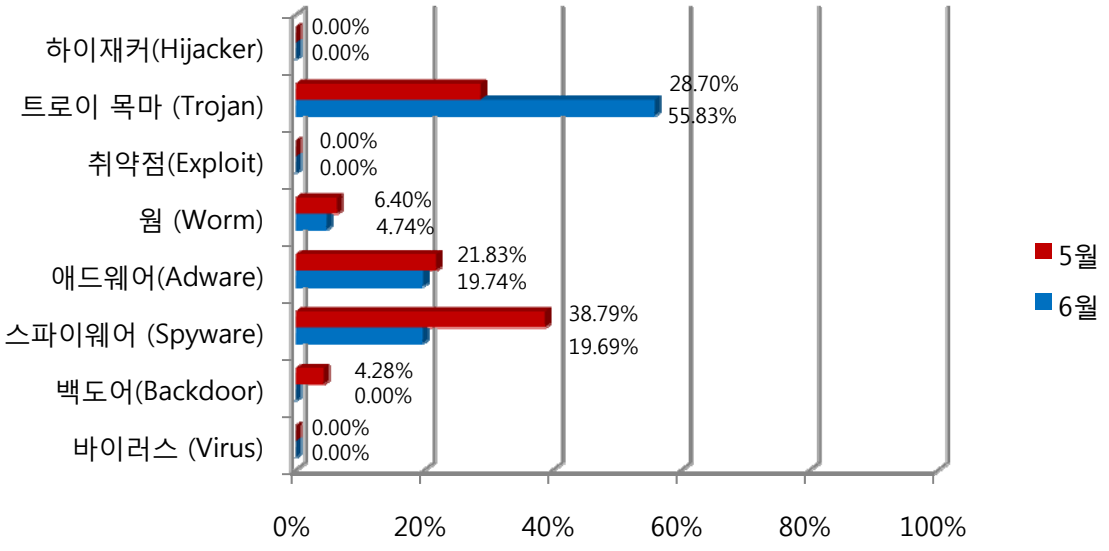
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
6월의 감염 악성코드 TOP 15는 V.DWN.Agent.Pinsearch이 65,249건으로 TOP 15 중 1위를 차지하였으며, A.ADV.Admoke가 56,579건으로 2위, S.SPY.Lineag-GLG가 44,852건으로 3위를 차지하였다. 이외에도 6월에 새로 Top 15에 진입한 악성코드는 9종이다.
이번 달의 특이사항은 전달에 비해 개별 악성코드의 감염자수가 전체적으로 증가하였고 특히 애드웨어(Adware)와 관련된 악성코드의 감염 비율이 매우 높았다.
1위를 차지한 V.DWN.Agent.Pinsearch은 국내 애드웨어(Adware) 프로그램를 사용자 동의 없이 PC에 다운로드하고 설치하는 악성코드이다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 59%로 가장 많은 비율을 차지하고, 애드웨어(Adware)가 20%, 스파이웨어(Spyware)가 19%의 비율을 각각 차지하고 있다. 이번에 56%의 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹 사이트에서 유포된 경우가 많이 발견되었다.

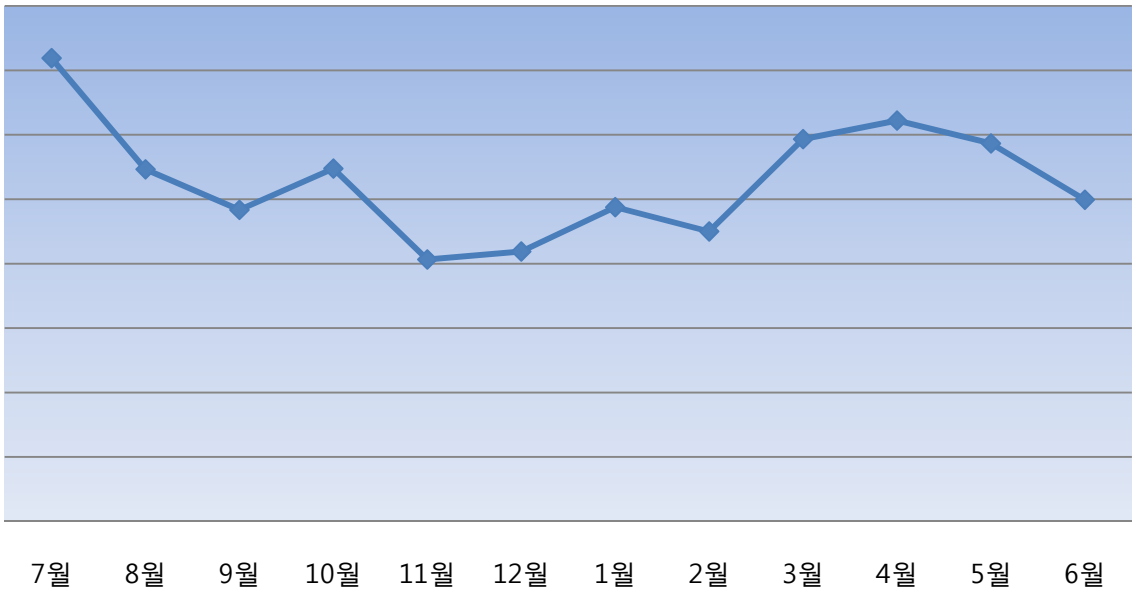
(3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 트로이목마(Trojan)의 경우 전달에 비해 27% 정도 비율로 증가하였고, 스파이웨어의 경우(Spyware) 19% 정도 감소하였다.
(바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

(4) 월별 피해 신고 추이

[2009년 7월 ~ 2010년 6월]

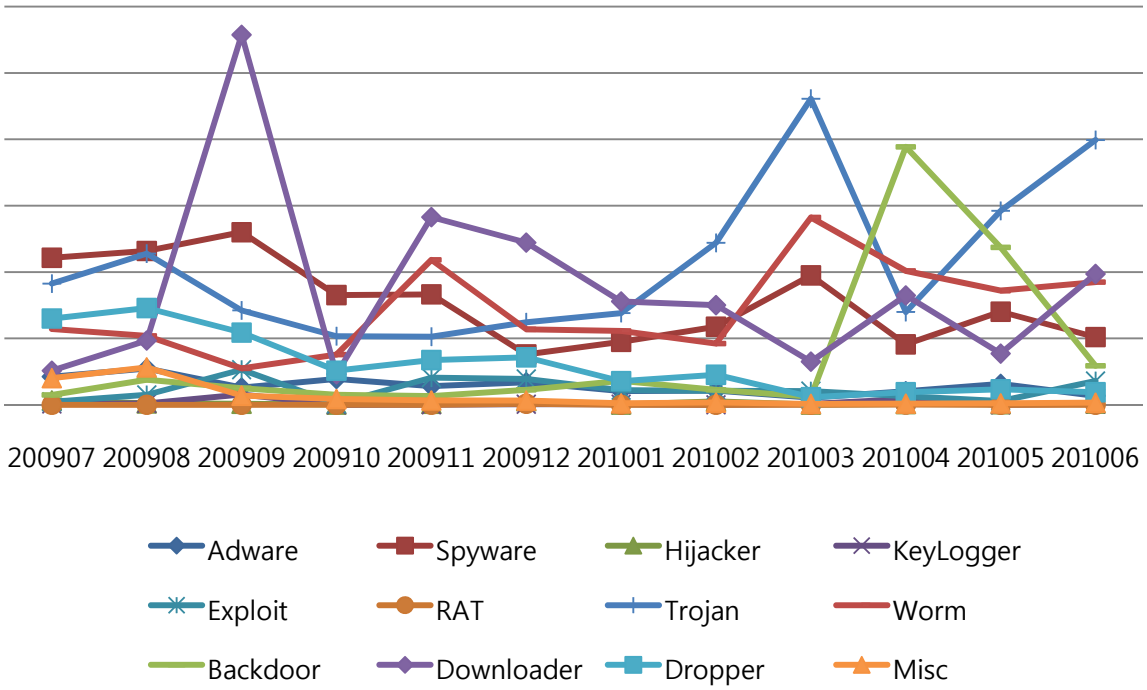


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 6월의 경우 전달(5월)보다 신고 건수가 감소했다.

(5) 월별 악성코드 DB 등록 추이

[2009년 07월 ~ 2010년 6월]

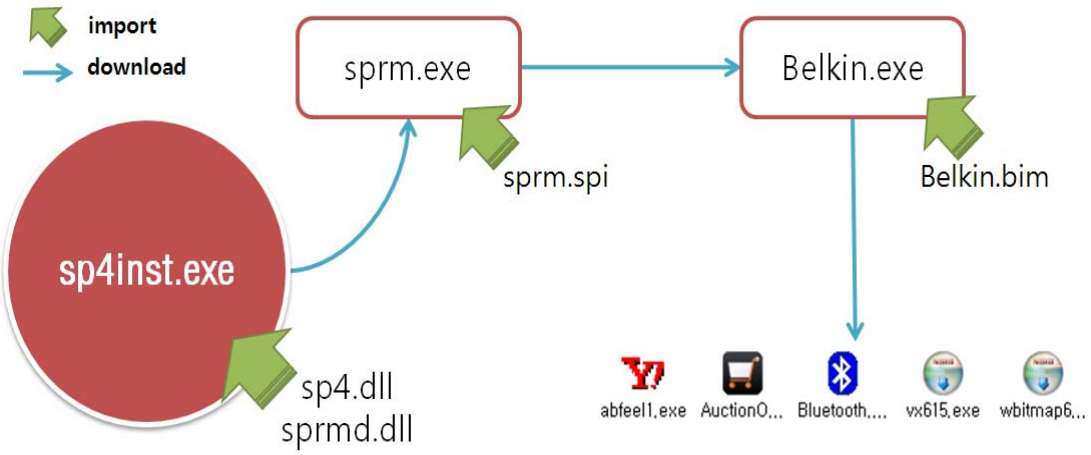


Part I 6월의 악성코드 통계

2. 악성코드 이슈 분석 – "국내산 애드웨어 다운로더 V.DWN.Agent.189440"

이번달에 살펴볼 악성코드는 5~6 월 사이에 유포된 것으로 추정되며, 일부 Drop 파일들의 신고가 급증한 V.DWN.Agent.189440 (Bitdefender 진단명 : Backdoor.Generic.36728)이다.

<6월 V.DWN.Agent.189440과 관련된 신고 내용>



< V.DWN.Agent.189440 악성코드 설치 방법>

V.DWN.Agent.189440 악성코드는 국내산 애드웨어를 다운로드하며, 이스트소프트로 악성ㅋ드 감염신고 건수가 크게 증가하였다.

1) sp4inst.exe (V.DWN.Agent.189440) 파일 분석

이 파일의 주요 기능은 다른 다운로더를 설치하는 것이다.
이를 위해 두 개의 DLL을 import하는데 sp4.dll을 통하여 레지스트리 등록을 하는 것이고, sprmd.dll을 통하여 다운로드한 파일을 실행한다.

다운로드 파일	hxxp://220.90.xxx.xxx/spxx2/sp4.dll hxxp://220.90xxx.xxx/spxx2/sprm.exe hxxp://220.90.xxx.xxx/spxx2/sprmd.dll
경로/속성	C:₩systen32₩sp4.dll (숨김) C:₩program files₩common files₩sprm.exe (숨김) C:₩Program Files₩Internet Explorer₩MUI₩sprmd.dll (파일이름 랜덤 변경, EX: POfISgWqa.dll)
레지스트리 생성	HCU₩SOFTWARE₩sprm

[sprm.exe 파일의 실행 흐름]
sp4.dll 다운로드 → sp4.dll의 DllRegisterServer 함수 Import
→ sprm.exe 다운로드 → sprmd.dll 다운로드 → sprmd.dll 파일명 변경
→ sprmd.dll의 ExecuteFile 함수 Import → sprmd.dll은 sprm.exe 실행

2) sp4.dll (Trojan.Generic.4131223) 파일 분석

해당 파일은 BHO로 실행되며 sp4inst.exe 파일을 다운로드해 실행시킨다. (CLSID→BHO생성)

Export 함수	Sp4.DllRegisterServer(), Sp4.UnregisterServer()
레지스트리 BHO	HLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Browser Helper Objects₩{40FD877F-B0AB-4753-AA69-016C1717D78A})
레지스트리 CLSID	HCR₩CLSID₩{40FD877F-B0AB-4753-AA69-016C1717D78A} HCR₩CLSID₩{40FD877F-B0AB-4753-AA69-016C1717D78A}₩InprocServer32

3) sprm.exe (V.DWN.Adware.Kor) 파일 분석

sprm.exe 파일은 밑에 설명할 Belkin.exe 파일과 구조가 같아 중복이 되기 때문에 간략하게 흐름을 파악하는 정도에서 작성해 보았다.

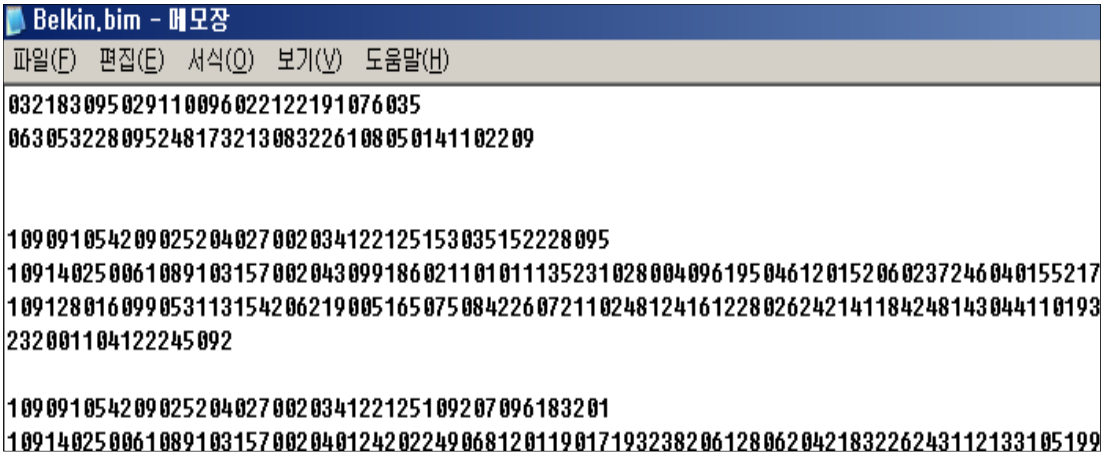
다운로드 파일	hxxp://114.207.xxx.xxx/Belkin.exe hxxp://220.90.xxx.xxx/spxx2/sprm.spi
경로/속성	C:₩Belkin.exe C:₩program files₩common files₩sprm.spi
레지스트리 생성	HCU₩SOFTWARE₩Belkin

[sprm.exe 파일의 실행 흐름]
sprm value를 확인하여 삭제
→ sprm.spi 다운, XOR, 버전 체크
→ c:₩Belki.exe 파일 다운로드(여러 명령 수행가능) → 종료

4) Belkin.exe (V.DWN.Adware.Kor) 파일 분석

sprm.exe 파일과 매우 흡사한 구조이다.
Belkin.bim이란 파일을 먼저 다운 받아 명령을 해석하고 실행시킨다.
Belkin.bim은 버전 별로 명령 처리를 위해 특별히 제작된 파일이며 대부분 다른 파일을 다운받기 위해 주소 값이 인코딩되어 있다.

bim 파일은 숫자로 인코딩 되어있고 이것을 해석하면 일정한 형식의 text가 나타난다.



다운로드 파일	hxxp://221.143.xxx.xxx/baxxx/Belxxx/Belkin.bim hxxp://114.207.xxx.xxx/Bluetooth.exe
경로/속성	C:₩Belkin.bim C:₩Blutetooth.exe C:₩Windows₩System32₩drivers₩Belkin
레지스트리 생성	HCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩Belkin c:₩Belkin HCU₩Software₩Bluetooth

다음은 XOR 하여 명령을 수행하는 부분이다.

```
mov eax, [ebp+var_10]           ; eax에 한줄씩 bim 파일의 TEXT 복사
call _xor_                      ; xor 한 값을 [edx]에 저장
mov edx, [ebp+var_38]           ; ebx를 카운트하여 명령을 수행
lea eax, [ebp+var_10]
call @System@@LStrLAsg$qqrpvpxv ; System::__linkproc__ LStrLAsg(void *,void *)
```

위의 숫자를 XOR후 메모리에 저장한 것을 정리해 보았다.

```
ver=1,0,0,0
idx=Belkin.bim
;옥X필맨1+3히플
;hxxp://220.90.xxx.xxx/vx615.exe
;dnexe=vx615.exe|c:₩₩windows₩₩temp₩₩|http://220.90.xxx.xxx/|0
;옥X필맨1+필맨3
;hxxp://114.207.xxx.xxx/AucxxxxOSG13.exe
;opexe=AucxxxxOSG13.exe|/S|c:₩windows₩temp₩|http://114.207.xxx.xxx/|
;hxxp://220.90.xxx.xxx/Yaxxx/abfeel1.exe.....0ÿX75
;opexe=abfeel1.exe|/S|c:₩₩temp₩₩|http://220.90.xxx.xxx/Yaxxx/|1
;hxxp://220.90.xxx.xxx/Yaxxx/wbitmap616.exe
;dnexe=wbitmap616.exe|c:₩₩windows₩₩system32₩₩drivers₩₩|http://220.90.xxx.xxx/Ya
hoo/|0
run=Axxxxx Vxxxx Tray Process
run=NxxxxPCxxxxx
run=ALxxx
run=NxxxxVxxxxxx
run=TrueXXXX
run=TrueXXXX
run=TCodXXXXX
run=certification
run=AceXXXX
run=best21_XXX
run=ctXXXX
run=HPMXXXX
run= NxxxxVxxxxxx
run=psngr_XXX
run=RealVXXXXXX
run=whoXXX
run=windstXXXX
run=wscnes
;hxxp://114.207.xxx.xxx/Bluetooth.exe
dnexe=Bluetooth.exe|c:₩₩|http://114.207.xxx.xxx/|0
```

메모리에 저장된 값을 (%d번째 || Key: %s || Value: %s) 구조로 해석하여 명령을 처리한다.

```
mov eax, offset _str__d________Key_.Text
call unknown_libname_141          ; _
mov eax, [ebp+var_40]
xor edx, edx
call _Copy_String_                ; %d 번째 || Key: %s || Value: %s
                                  ; 위와 같이 메모리에 값을 저장하여 실행
mov eax, [ebp+var_14]
call sub_45A53C                   ; 값을 체크하여 case별로 다른 명령 수행
and eax, 7Fh
cmp eax, 0Eh                      ; switch 15 cases
ja loc_47BBA4                     ; default
                                  ; jumptable 0047B8E5 case 0
jmp ds:off_47B8EC[eax*4]          ; switch jump
```

키가 run일 때 실행되는 루틴은 다음과 같다.

```
loc_47BB3F:                       ; CODE XREF: _module_main_+1B9↑j
                                  ; DATA XREF: _module_main_:off_47B8EC↑o
    mov eax, [ebp+var_18]         ; jumptable 0047B8E5 case 7
    call _cmd_run_key_            ; 키가 run일때 처리루틴
    jmp short loc_47BBA4          ; default
                                  ; jumptable 0047B8E5 case 0
```

앞에 XOR하여 메모리에 저장된 주소들은 모두 다운 가능하였으며 버전을 바꿔가며 계속 임의의 파일을 다운로드 할 것으로 추정된다.

5) 결론

이번 악성코드 파일은 정확하게 다운로더 형식이다.

중요한 것은 이번에 일시적으로 많은 신고가 들어왔으며 그만큼 유포가 상당수 진행되었다는 것을 알 수 있다.

또한 국내에서 광고 프로그램의 유포가 나름의 방식대로 진화되고 있지 않나 생각해본다.

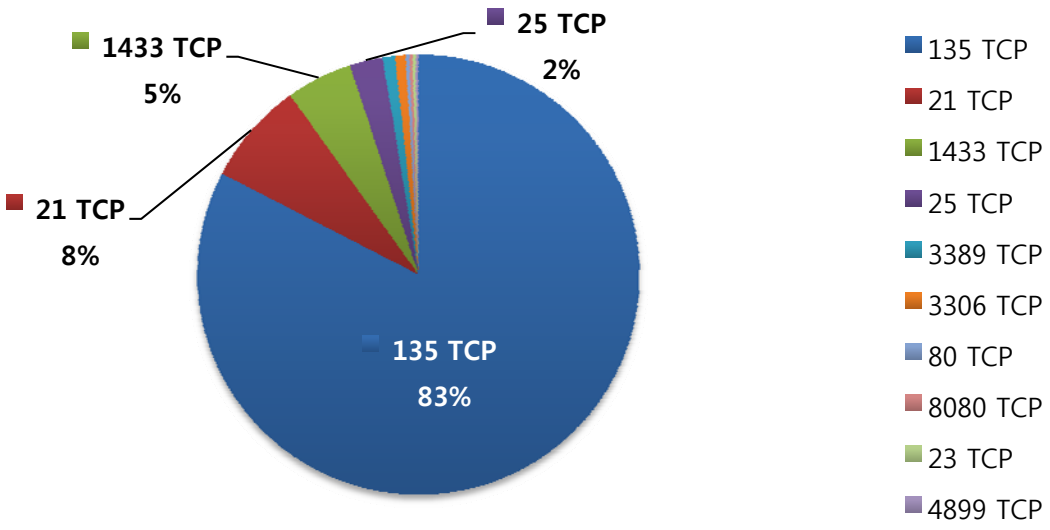
개인 사용자는 원하지 않는 프로그램 설치에 대해 관심을 기울이고 더 이상의 유포가 되지 않도록 적극적으로 신고가 되어야 한다.

국내에서 제작되는 만큼 법적인 제재가 면밀하게 이루어져 근본적인 대안이 되도록 해야 할 것이다.

Part I 6월의 악성코드 통계

3. 허니팟/트래픽 분석

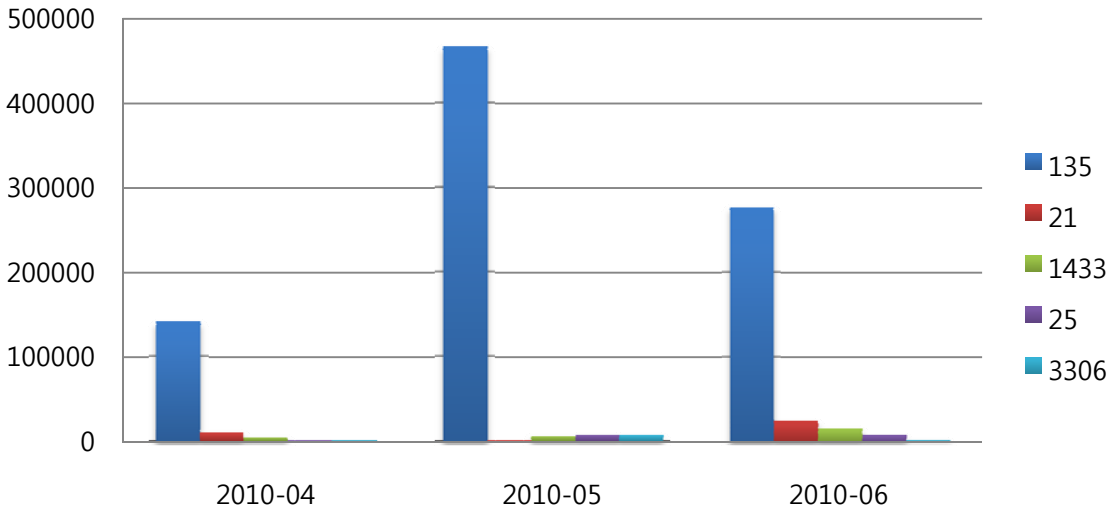
(1) 상위 Top 10 포트



6월에는 지속적으로 윈도우 자체의 취약점을 대상으로 한 135포트 침입 시도가 가장 많았다. 이는 백신으로 제거되지 않은 악성코드에 감염된 PC가 그만큼 많다는 뜻이기도 하다.
특이점은 FTP가 사용하는 21 TCP포트에 대한 침입시도이며, 주로 아이디와 비밀번호를 무작위로 대입하는 방법으로 침입시도를 한다. 지난달에 매우 높은 비율로 다시 증가했다.

(2) 상위 Top 5 포트 월별 추이

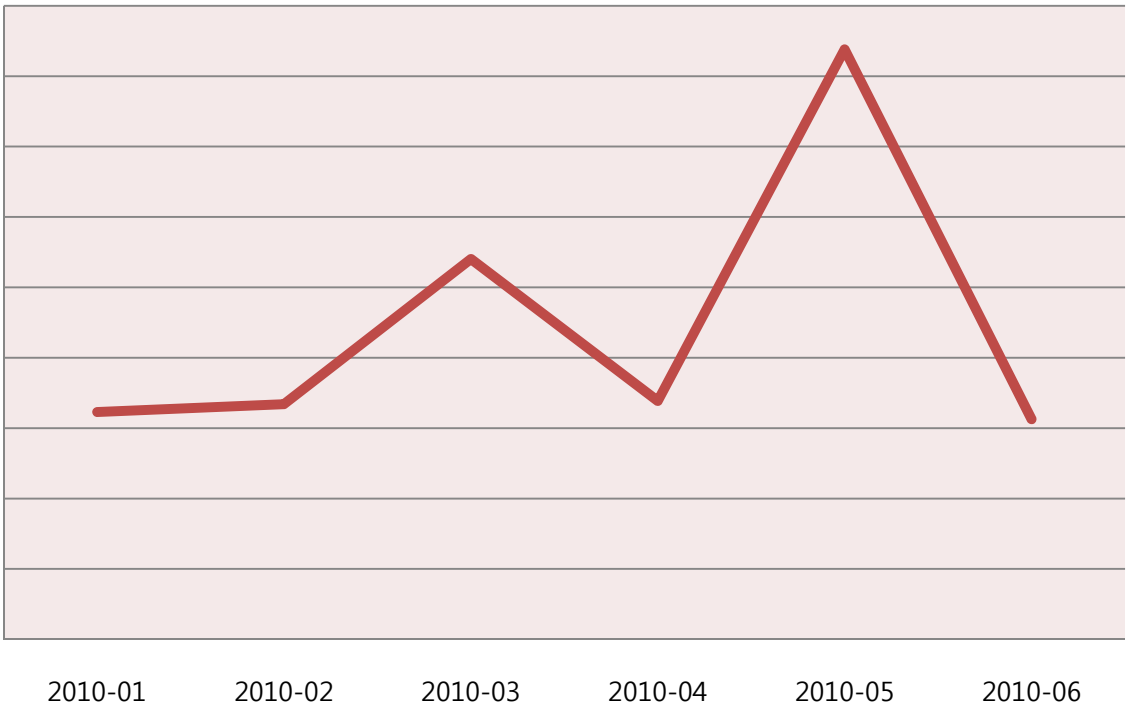
[2010년 4월 ~ 2010년 6월]



전체적으로 악성 트래픽 유입도 감소하였으나 135번 이외의 포트들이 전달에 비해 악성 트래픽 유입이 증가한 상태이다. 외부에서 135번 포트로 접근이 불필요한 경우 방화벽이나 IPS에서 차단하는 것이 보안 예방 효과에 좋다.

(3) 악성 트래픽 유입 추이

[2009년 1월 ~ 2010년 6월]

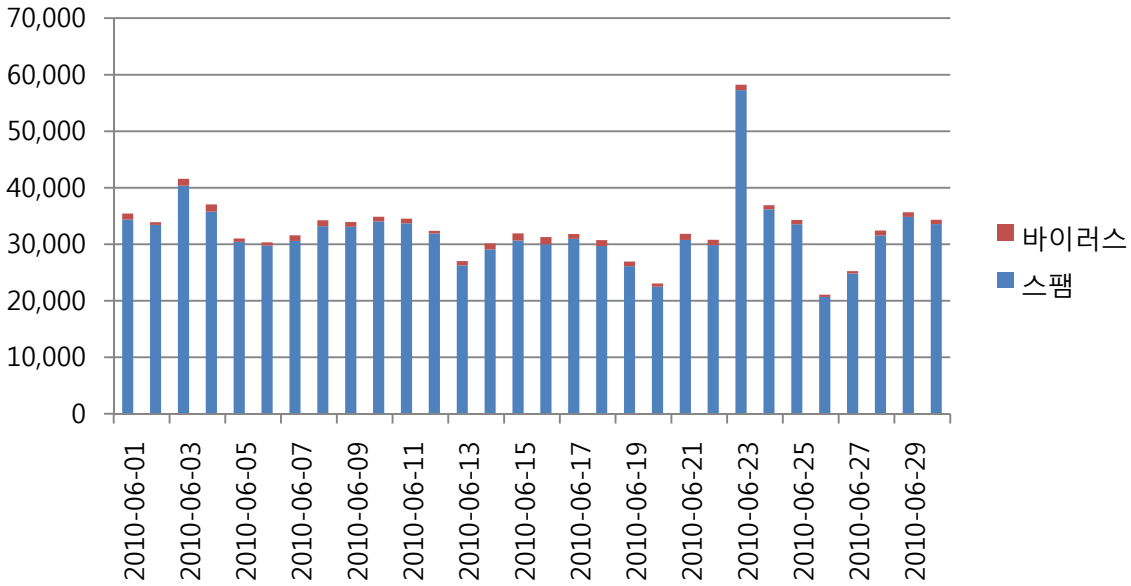


지난 달에 비해 악성 트래픽 유입이 4월 수준으로 크게 감소하였다.
인터넷 뱅킹, 쇼핑, 메신저나 트위터를 통한 사회활동 등 생각해보면 일상생활 거의 모든 분야에서 컴퓨터와 인터넷을 사용한다.
특히 자신이 사용하는 PC와 여러 단말기에는 자신이 인지하지 못하는 이상의 개인정보가 저장되게 된다.
해커들은 이러한 PC나 단말기에 저장된 개인정보를 훔치기 위해 항상 새로운 공격 방법을 개발하고 실행하고 있다. 사용자의 보안의식 또한 그와 비례해 높일 수 있도록 해야 한다.

Part I 6월의 악성코드 통계

3. 스팸 메일 분석

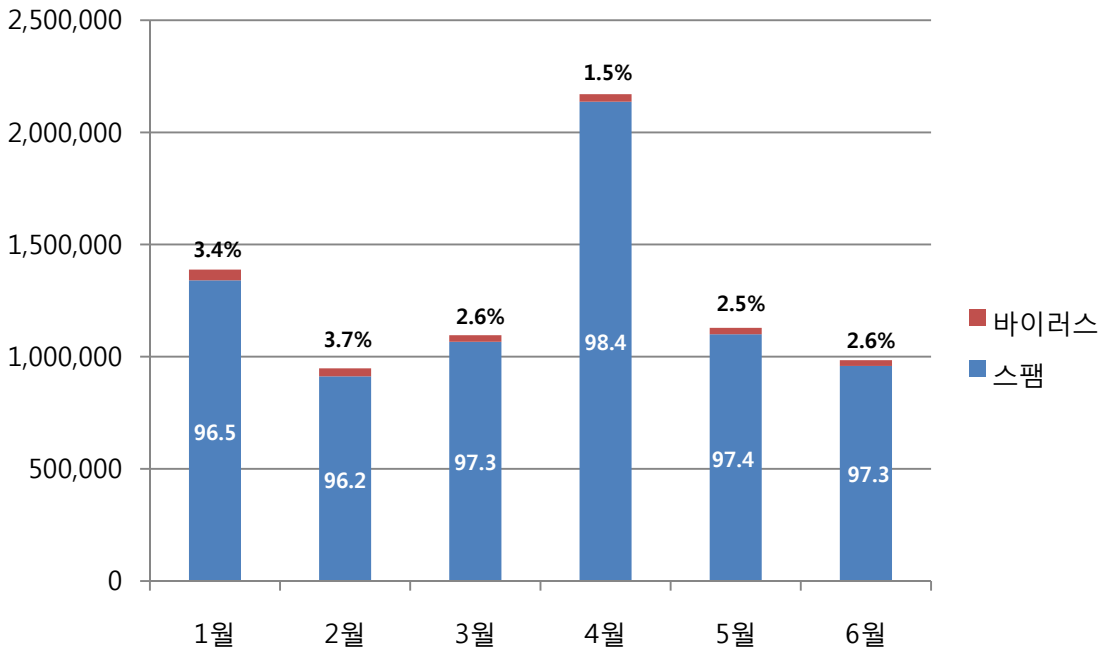
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 6월의 경우 국내에서 BC카드 이메일 명세서를 위장한 악성코드 메일 유포 사례가 보고되었다.

(2) 월별 통계 현황

[2010년 1월 ~ 2010년 5월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다.

6월달 스팸 메일은 97.3%, 바이러스 메일은 2.6%를 차지하였다. 5월에 비해 스팸메일과 바이러스 메일이 0.1% 비율로 감소·증가해 사실상의 큰 변동은 없었다.

(3) 스팸 메일 내의 악성코드 현황

[2010년 6월 1일 ~ 2010년 6월 30일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Virut-T	11,848	46.20%
2	W32/MyDoom-H	3,856	15.04%
3	Mal/ZipMal-B	3,642	14.20%
4	W32/Mytob-C	1,594	6.22%
5	Troj/JSRedir-BO	754	2.94%
6	Troj/CryptBx-ZP	748	2.92%
7	Troj/Invo-Zip	341	1.3%
8	W32/Sality-I	335	1.31%
9	W32/MyDoom-Gen	300	1.17%
10	W32/MyDoom-BZ	285	1.11%

스팸 메일 내의 악성코드 현황은 6월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Virut-T이 46.20%로 계속 1위를 차지하고 있다.

2위는 15.04%를 차지한 W32/MyDoom-H, 3위는 14.20%를 차지한 Mal/ZipMal-B이다.

특히, 6월달에는 이메일에 담겨진 악성 스크립트(Malicious Script)를 통해 감염을 시도하는 Troj/JSRedir-BO 악성코드 스팸 메일들이 새롭게 순위에 등장했다.

Part Ⅱ 6월의 이슈 돋보기

1. 6월의 보안 이슈

6월에는 MS 윈도우 XP 서비스팩 2 및 윈도우 2000의 보안 업데이트 종료와 이스트소프트 2010년 상반기 5대 보안 이슈 발표에 관한 보안 이슈들이 있었습니다.

• Windows XP Service Pack 2 및 Windows 2000 보안 업데이트 7월 종료

7월 13일에 Windows XP Service Pack 2 및 Windows 2000, Windows Vista RTM 버전의 연장기술지원(Extended Support Phase)이 종료됩니다. 기술지원이 종료되면서 패치 또한 함께 제공되지 않으므로 상위 버전의 윈도우로 반드시 업그레이드해야 합니다.
단, Windows XP의 경우 서비스팩 3로 업그레이드 한다면 2014년까지 연장 기술지원을 받으실 수 있고 무료로 설치 파일이 제공되기 때문에 반드시 설치하시기 바랍니다.

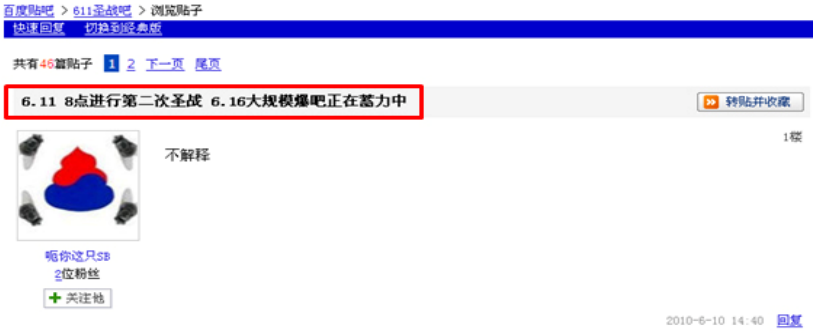
<관련 사이트>

http://alyac.altools.co.kr/SecurityCenter/Analysis/NoticeView.aspx?id=24

• 이스트소프트 2010년 상반기 5대 보안 이슈 발표

1) 새로운 형식의 DDoS 공격형태 발생

2009년의 7.7 DDoS 공격과 같은 기존 DDoS공격방식의 경우 악성코드에 감염된 좀비 PC그룹을 활용하여 목표를 공격하는 형태였으나, 2010년 6.16 성전이라고 불렸던 중국발 DDoS 공격의 경우 공격자들 스스로 온라인커뮤니티나 메신저 채팅 서비스등을 통해 공격인원을 모으고 DDoS 공격툴을 배포하여 카운트다운 방식을 통해 동시에 특정 목표를 공격하는 새로운 형태였다. 이러한 방식은 좀비PC그룹을 이용한 기존 DDoS 공격방식과 달리 아직까지 많은 트래픽을 발생시키지 못하고 있기 때문에 현재는 주로 규모가 작은 사이트를 타켓으로 공격하고 있지만, 향후 더 많은 인원을 규합하게 되거나 좀비PC를 보유한 해킹그룹의 지원을 받는다면 피해규모가 커질 우려가 있으므로 주의를 기울여야 한다.



2) 스마트폰 사용자를 위협하는 보안위협요소 등장

기존에 한국에 보급되던 휴대폰(피쳐폰)들에는 WIPI탑재가 법적 의무였기 때문에 이로 인해 사용자들은 모바일 악성코드의 위협으로부터 상대적으로 자유로웠으나, 아이폰의 국내 출시 이후 안드로이드폰등 스마트폰의 빠른 보급으로 모바일 악성코드의 위협이 증가하고 있다.

한국전자통신연구원(ETRI)가 구분한 모바일 악성코드의 주요형태로는 단말기에 저장된 사용자의 정보를 외부로 유출시키는 '정보유출형', 스마트폰등의 단말기를 통해 PC를 감염시키는 '크로스 플랫폼형', 기기사용을 불가능하게 만들거나 장애를 일으키게 하는 '단말기 장애 유발형', 단말기의 메시징 서비스나 전화통화를 시도하여 과금을 발생시키는 '통신요금 발생형'등이 있다.

안전한 스마트폰 이용을 위해서는 항상 검증된 어플리케이션 및 컨텐츠를 사용하고, 신뢰할 수 없는 사이트 혹은 메시지/메일등을 열어보지 않아야 한다.

3) 사회적 이슈를 활용한 가짜백신 유포

2010년 벤쿠버 올림픽때 김연아 선수 트위터를 사칭하거나 2010 남아공 월드컵 티켓 할인/무료제공등을 사칭하는 등 사용자들이 관심을 가질만한 이슈를 활용한 사회공학적 기법으로 가짜백신을 유포하고 유료결제를 유도하는 행태가 계속되고 있다.

이러한 가짜백신은 사용자들이 특정 웹사이트 방문시 사용자PC가 바이러스에 감염되었다라는 알림창을 띄우고 자동으로 PC를 검사해주는 듯한 애니메이션을 보여주어 설치를 유도하는 자연스러운 방식으로 사용자에게 접근하고 있는 것이 특징이며, 한번 설치된 가짜백신은 사용자가 수동으로 삭제하기가 쉽지 않으므로 주의해야 한다.

4) 많이 사용되는 SW의 보안취약점을 노리는 해커들

기존에 해커들은 주로 PC운영체제(OS)의 보안취약점을 노리고 공격을 시도해왔으나, 최근에는 많은 사용자들이 설치하고 사용하고 있는 SW제품의 보안취약점을 통해 악성코드를 유포하고 시도가 급증하고 있다.

지난 6월초에도 Adobe Flash Player/Adobe Reader와 같이 많은 사람들이 사용하는 SW가 원격코드 실행이 가능한 취약점이 발견되어 제작사측에서 긴급패치를 배포한 적이 있었다. 이제는 OS 보안패치만 최신버전으로 유지하는 것뿐만 아니라, 자주 사용하는 SW에 대한 보안패치도 항상 최신버전으로 업데이트하는 것이 필요하다.

5) 계속되는 개인정보 유출 사고

지난 3월 역대 최대규모인 2000만명의 개인정보 유출사고가 발생해 사용자들에게 충격을 안겨준 가운데, 최근 개인정보보호를 위한 '주민등록번호의 대안'이라고 알려졌던 아이핀(i-PIN)이 대량으로 부정 발급되어 타인에게 판매되는 사건이 발생하여 아직 보완해야 할 부분이 있는 것으로 여겨진다.

개인정보 유출을 방지하기 위해서는 개개인의 정보보호 노력이 가장 중요하지만, 개인의 정보를 보관하고 있는 기업에서도 관리에 각별한 노력을 기울이는 것이 필요하다.

Part Ⅱ 6월의 이슈 돋보기

2. 6월의 취약점 이슈

• Adobe Flash Player, Acrobat authplay.dll 취약점

취약점 : CVE-2010-1297

Adobe Flash/Acrobat 제품에서 원격 코드 실행이 가능한 보안 취약점이 발견되었습니다. 현재 Adobe 사에서 6월 30일자로 CVE-2010-1297 취약점을 해결하는 보안 패치를 발표하였으므로 반드시 설치하시기 바랍니다.

Adobe 제품의 authplay.dll 파일이 악의적으로 작성된 Flash 파일(SWF)을 처리하는 과정에서 원격코드 실행이 가능한 취약점을 가지고 있습니다.
또한, 이번 취약점이 윈도우 뿐만 아니라 Mac, UNIX 환경에서도 적용되 취약점에 따른 공격 위협이 매우 높습니다.

<해당 제품>

- Adobe Flash Player 10.0.45.2, 9.0.262, 10.0.x and 9.0.x 버전
  (Windows, Macintosh, Linux and Solaris 환경 포함)
- Adobe Reader and Acrobat 9.3.2, 9.x 이전 버전
  (Windows, Macintosh and UNIX 환경 포함)

※ Adobe Acrobat 8.x대 버전은 취약하지 않음.

<해결책>

Adobe Flash Player와 Acrobat를 최신버전으로 업그레이드 합니다.
Flash : http://get.adobe.com/kr/flashplayer/
Air : http://get.adobe.com/kr/air/
Acrobat : http://get.adobe.com/kr/reader/

<관련 홈페이지>

http://www.adobe.com/support/security/advisories/apsa10-01.html

• Microsoft 6월 정기 보안 업데이트

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제, IIS 취약점으로 인한 원격 코드 실행 문제, Internet Explorer 누적 보안 업데이트 등을 포함한 6월 Microsoft 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- Windows 2000 Service Pack 4/XP/2003/Vista/2008/7
  (MS10-032, MS10-033, MS10-034, MS10-037)
- Internet Explorer 5.01~8 (MS10-035)
- Microsoft Office XP SP3/Office 2003 SP3 (MS10-036)

- Microsoft Office XP/2003/2007/Excel Viewer (MS10-038)
- Microsoft Office InfoPath 2003/2007/SharePoint Server 2007
  Windows SharePoint Services 3.0 (MS10-039)
- Windows 2003/Vista/2008/7 (MS10-040)
- Microsoft .NET Framework 1.0~ 3.5.1 (MS10-041)
  (4.0 버전과 비스타, 윈도우 2008에서 실행중인 3.5 버전, 3.0 SP1~2는 해당되지 않음)

<취약점 목록>

미디어 압축 해제의 취약점으로 인한 원격 코드 실행 문제점 (979902)
ActiveX 킬(Kill) 비트 누적 보안 업데이트 (980195)
Internet Explorer 누적 보안 업데이트(982381)
Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점 (979559)
Microsoft Office의 COM 유효성 검사 취약점으로 인한 원격 코드 실행 문제점 (983235)
OpenType CFF 드라이버의 취약점으로 인한 권한 상승 문제점 (980218)
Microsoft Office Excel의 취약점으로 인한 원격 코드 실행 문제점 (2027452)
Microsoft SharePoint의 취약점으로 인한 권한 상승 문제점 (2028554)
IIS(인터넷 정보 서비스)의 취약점으로 인한 원격 코드 실행 문제점 (982666)
Microsoft .NET Framework의 취약점으로 인한 변조 문제점(981343)

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.
한글 : http://www.microsoft.com/korea/technet/security/Bulletin/ms10-jun.mspx
영문 : http://www.microsoft.com/technet/security/Bulletin/ms10-jun.mspx

• 윈도우의 도움말 및 지원센터 제로데이 보안 취약점

윈도우의 도움말 및 지원센터(Help and Support Center)에서 원격코드 실행이 가능한 보안 취약점이 발견되었습니다.
도움말 및 지원센터(Help and Support Center) helpctr.exe에서 UrlUnescape 함수는 -FromHCP 옵션을 사용한 화이트리스트 제한을 건너 뛸 수 있는(bypass) 취약점이 존재합니다.
이외에도 sysinfo/sysinfomain.htm에서 XSS(Cross Site Scriprting) 취약점도 존재하여 privileged zone에서 악성 스크립트 코드를 실행할 수 있습니다.

<임시 조치법>

HCP Protocol 레지스트리 등록을 해제하는 작업을 수행해야합니다.

<참고 사이트>

http://www.microsoft.com/technet/security/advisory/2219475.mspx

Contact us…

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약사이트 : www.alyac.co.kr

| 이벤트 안내 |

- 기 간 : 7월 12일 ~ 8월 31일
- 대 상 : 기업용 알툴즈통합팩 / 알집 / 알씨 / 알FTP 구 버전 보유고객
- 내 용 : 기존 버전 업그레이드 구매 시 60% 할인

업그레이드하기