www.alyac.co.kr

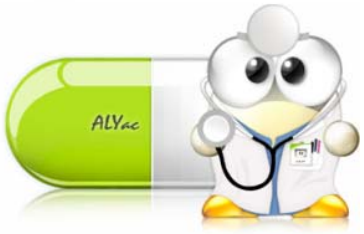
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part Ⅰ 5월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

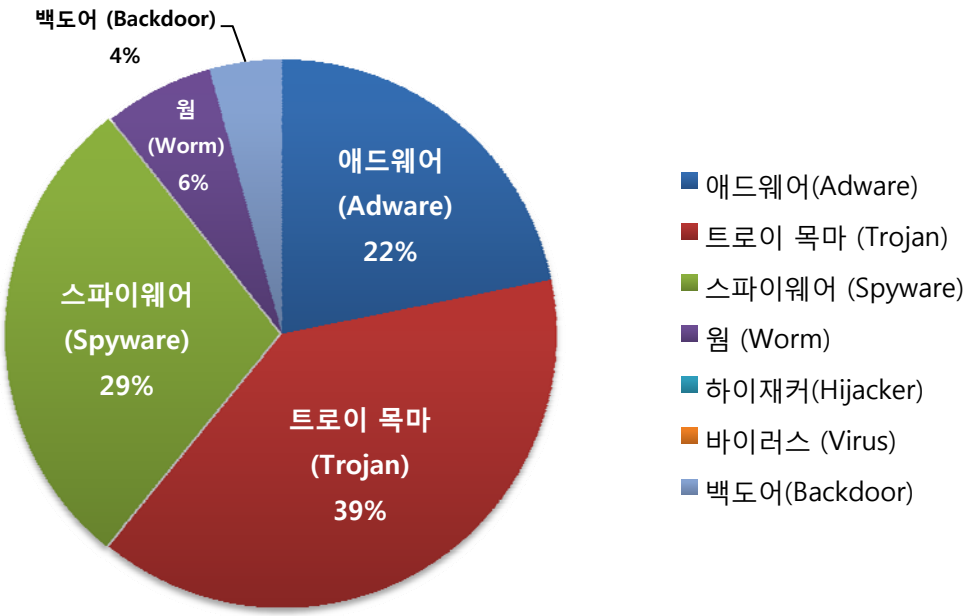
[2010년 5월 1일 ~ 2010년 5월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑1	A.ADV.Admoke	Adware	36,251
2	↓1	S.SPY.Lineag-GLG	Spyware	31,400
3	New	V.DWN.Agent.2456	Trojan	22,907
4	↑4	Trojan.Peed.Gen	Trojan	15,543
5	↑10	V.DWN.Agent.262144	Trojan	15,180
6	↓2	V.WOM.Conficker	Worm	14,169
7	↓4	S.SPY.OnlineGames-H	Spyware	12,602
8	↓3	A.ADV.BHO.IESearch	Adware	11,815
9	New	V.DWN.Agent.259072	Trojan	9,994
10	New	S.SPY.OnlineGames.kb	Spyware	9,723
11	New	V.BKD.Hupigon.aas	Backdoor	9,475
12	↓6	S.SPY.WoWar	Spyware	9,237
13	New	Trojan.Generic.3865549	Trojan	8,564
14	New	Trojan.Generic.3833102	Trojan	7,845
15	New	Trojan.Generic.3924384	Trojan	6,405

※ 자체수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

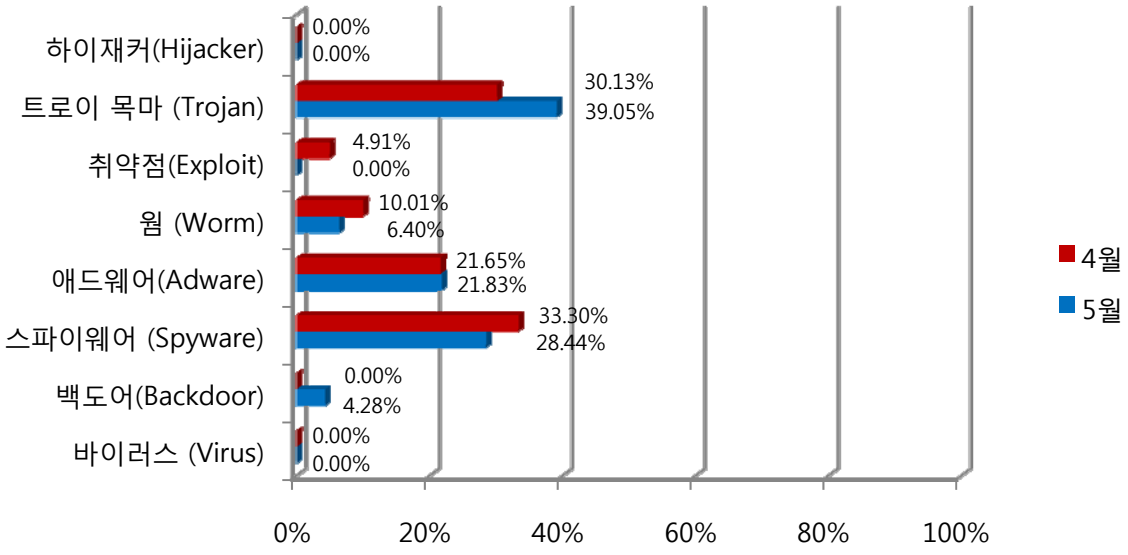
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
4월의 감염 악성코드 TOP 15는 A.ADV.Admoke이 36,251건으로 TOP 15 중 1위를 차지하였으며, S.SPY.Lineag-GLG이 31,400건으로 2위, V.DWN.Agent.2456이 22,907건으로 3위를 차지하였다. 이외에도 4월에 새로 Top 15에 진입한 악성코드는 7종이다.
이번 달의 특이사항은 전달에 비해 개별 악성코드의 감염자수가 전체적으로 감소하였다.
이는 악성코드 유포, 경유사이트가 5월에 들어 크게 줄어들었으며, 홈페이지 변조 사고도 줄어든 것으로 보여진다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 39%로 가장 많은 비율을 차지하고, 애드웨어(Adware)가 22%, 스파이웨어(Spyware)가 29%의 비율을 각각 차지하고 있다. 이번에 39%의 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹 사이트에서 유포된 경우가 많이 발견되었다.

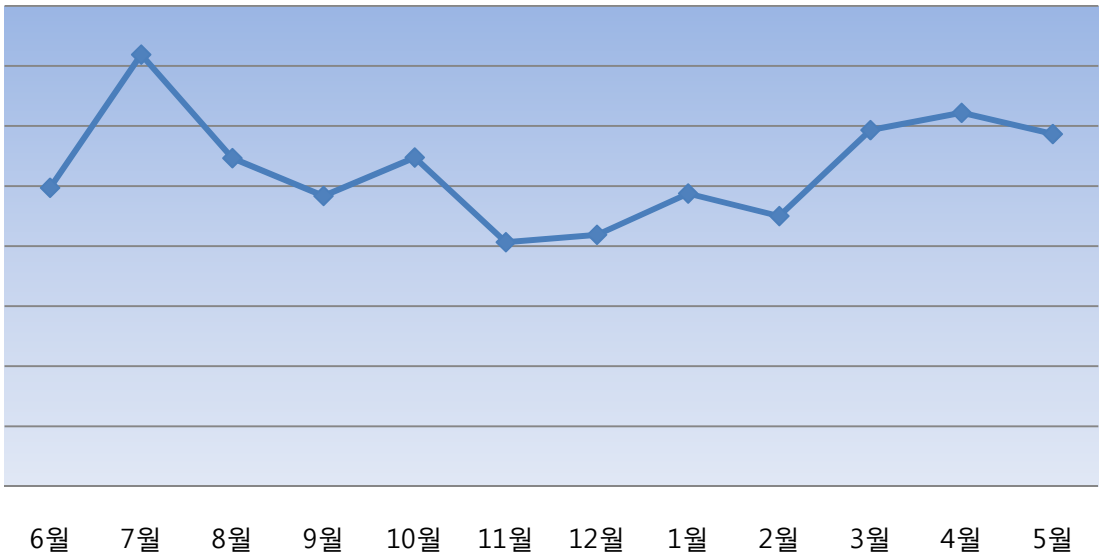
(3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 백도어(Backdoor)의 경우 전달에 비해 4.28% 정도 비율이 증가하였고 트로이 목마(Trojan) 또한 9% 정도 증가하였다.
(바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

(4) 월별 피해 신고 추이

[2009년 4월 ~ 2010년 5월]

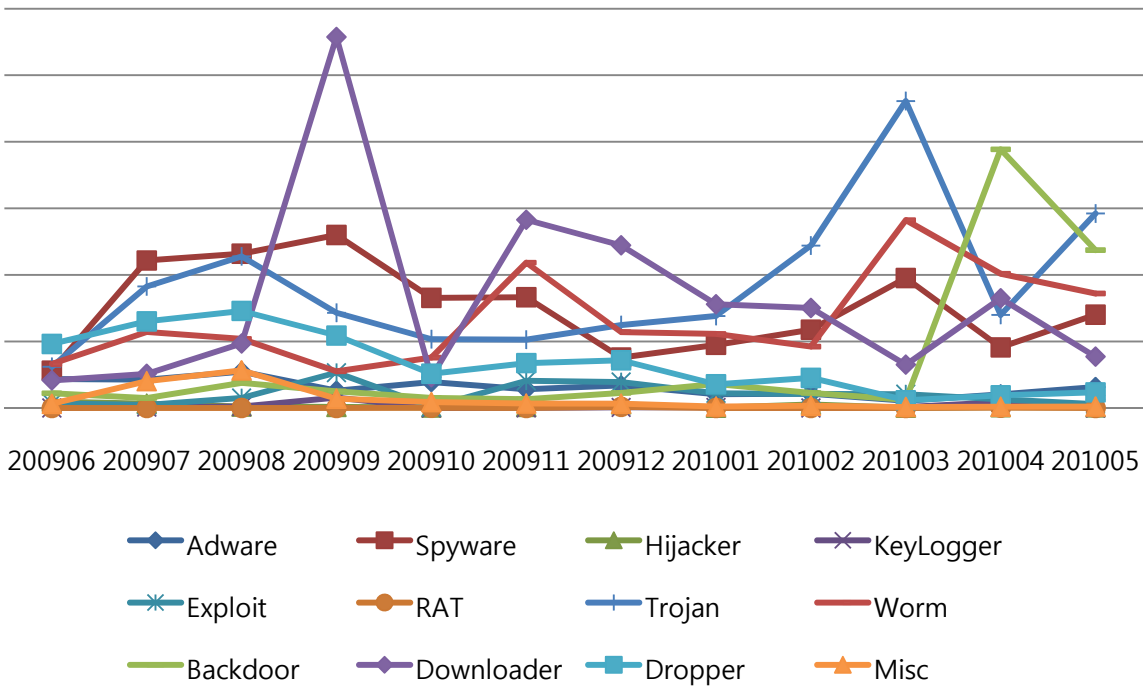


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 5월의 경우 전달보다 신고 건수가 감소했으며 개별 악성코드의 감염자수가 전체적으로 감소와 맞물려 나타난 것으로 보여진다.

(5) 월별 악성코드 DB 등록 추이

[2009년 06월 ~ 2010년 5월]

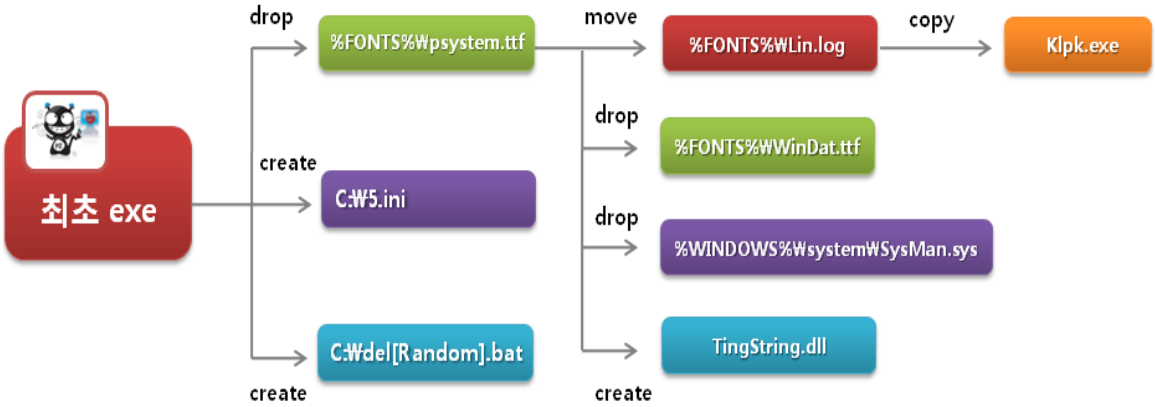


Part I 5월의 악성코드 통계

2. 악성코드 이슈 분석 – "네이트온으로 전파되는 V.WOM.Nateon.Baidog"

네이트온 메신저를 이용해 전파되는 V.WOM.Nateon.Baidog 악성코드는 기존에 네이트온 로그인 계정을 탈취하여 특정 사이트에 보내는 것이 대부분이었지만 최근에는 네이트온 계정 뿐만 아니라 던전앤파이터와 넥슨 홈페이지 계정도 탈취하는 기능도 추가되었다. 게다가 백신의 보안 메커니즘을 우회하는 코드도 포함되어 더욱 막강해진 위력(?)을 자랑한다.

<V.WOM.Nateon.Baidog 악성코드의 흐름>



최초 실행파일(exe)를 실행하면 PC에 여러 파일이 추가로 생성되며, 여기서 가장 중요한 파일은 두 개의 DLL 파일(Psystem.ttf, WinDat.ttf; 내부는 DLL 형태)과 한 개의 .sys 파일이다. 여기서 DLL 파일들은 계정을 탈취하는 기능을 가지고 있으며, .sys 파일(SysMan.sys)는 PC에 설치된 백신 제품을 무력화시키는 기능을 수행한다.

1) 최초 exe 파일 분석

최초 exe 파일은 주로 추가적인 파일을 생성하고 실행하는 역할을 담당한다.

① 다음 파일이 존재하는지 확인하고, 존재한다면 삭제한다.

```
%FONTS%₩psystem.ttf
%FONTS%₩Lin.log
%WINDOWS%₩system₩Klpk.exe
C:₩5.ini
```

② 리소스부터 psystem.ttf 파일을 Drop한다.
③ 5.ini 파일을 생성하여 exe 파일의 경로를 저장한다.
④ psystem.ttf을 실행시킨다.
⑤ Psystem.ttf의 export 함수인 KaiShi의 주소를 구해서 호출한다.
⑥ 자기 자신을 삭제하기 위해 del[Random].bat를 생성하여 실행한다.

2) psystem.ttf 파일 분석

psystem.ttf은 모든 프로세스에 삽입(injection)되어 계정을 탈취하는 역할을 한다.
최초 실행파일(exe)은 psystem.ttf를 로드하고 KaiShi 함수를 호출한다.
KaiShi는 중국어로 '시작하다'라는 뜻을 가지고 있다.

```
HHOOK __cdecl KaiShi()
{
  HHOOK result; // eax@1

  result = SetWindowsHookExA(3, (HOOKPROC)fn, hModule, 0);// 3 : WH_GETMESSAGE
  hhk = result;
  return result;
}
```

<그림 : Hex-rays로 본 KaiShi 함수>

KaiShi는 SetWindowsHookExA 함수를 사용해 WH_GETMESSAGE 메시지에 대한 hook을 걸어둔다. 다른 프로세스에서 해당 메시지가 발생하면 HOOKPROC인 fn함수를 호출하기 위해 fn 함수가 있는 dll 파일을 로드하게 된다.
즉, 프로세스에 dll 파일이 삽입 되고 dll 파일이 로드되는 과정에서 DllEntryPoint함수가 실행된다. 이 함수에는 계정을 탈취하는 악성 코드가 존재한다.

```
BOOL __stdcall DllEntryPoint(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpReserved)
{
  if ( fdwReason == 1 )
  {
    hModule = hinstDLL;
    GetModuleFileNameA(0, ModuleFilename, 0x104u);
    GetFileTitleA(ModuleFilename, FileTitle, 0x64u);
    strlwr(FileTitle);
    if ( StrStrA(FileTitle, "explorer") )
      CreateThread(0, 0, Thread_explorer, 0, 0, 0);
    if ( StrStrA(FileTitle, "dnf") )
      CreateThread(0, 0, Thread_dnf, 0, 0, 0);
    if ( StrStrA(FileTitle, "iexplore") )
      CreateThread(0, 0, Thread_iexplorer, 0, 0, 0);
    if ( StrStrA(FileTitle, "nateonmain") )
      CreateThread(0, 0, Thread_nateonmain, 0, 0, 0);
  }
  return 1;
}
```

<그림 : DllEntryPoint 함수>

Dll이 삽입된 프로세스가 탐색기(explorer), 던전앤파이터(dnf), 인터넷 익스플로러(iexplore) 네이트온(nateonmain)일 경우 쓰레드를 생성하여 해당 루틴을 실행한다.

- **Explorer Thread**

① KaiShi 함수를 호출해 Hook을 걸어둔다.
② 5.ini 파일에 저장되어 있는 파일 경로(최초 EXE를) %FONTS%₩Lin.Log로 복사하고, 백신의 탐지를 피하기 위해 "MZ" 파일 헤더를 "ML"로 바꾼다.
③ 5.ini 파일을 삭제하고 쓰레드를 하나 더 생성 한다.

④ 새로 생성된 스레드는 파일의 리소스 영역에서 두 개의 파일을 Drop하고 실행하는 일을 한다. 리소스 영역에서 WinDat.ttf와 SysMan.Sys 파일을 Drop한다.

⑤ 두 파일의 헤더를 "MZ"로 변경하고, SysMan.sys를 SystemFilse라는 서비스로 등록하여 실행한다. 그 후 SysMan.sys 파일을 삭제한다.
만약 백신로 의심되는 프로세스가 존재할 경우 HLM의Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Notify에서 systment 키를 삭제한다.
백신 제품이 PC에 없다고 판단될 경우 위의 키에 아래의 값을 생성한다.

```
StartShell;QiDongHan
DLLName;WinDat.ttf
Asynchronous;1
Impersonate;0
```

⑥ 프로세스 목록을 검사하여 dnf.exe, iexplore.exe, nateonmain.exe 프로세스가 존재하면 레지스트리 HLM의 SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run에서 모 백신 제품의 Tray Process 키를 삭제한다.
마지막으로 Lin.log파일의 헤더를 "ML"로 바꾸고 Klpk.exe라는 이름으로 복사한다.

• **dnf Thread**

① 던전앤파이터 프로세스에서 다음의 코드를 찾는다.

```
코드 1>
8D 8E 95 00 00 00                       lea     ecx, [esi+95h]
51                                      push    ecx
53                                      push    ebx
52                                      push    edx
FF 50 58                                call    dword ptr [eax+58h]

코드 2>
89 75 F0                                mov     [ebp-10h], esi
C7 45 E8 04 00 00 00                    mov     dword ptr [ebp-18h], 4
C7 45 EC 00 00 00 00                    mov     dword ptr [ebp-14h], 0
C7 45 E4 FF FF FF FF                            mov     dword ptr [ebp-1Ch],
0FFFFFFFFh
8D BE C8 01 00 00                       lea     edi, [esi+1C8h]
78 31                                   js      short near ptr unk_1000506D
```

② RtlLeaveCriticalSection 함수를 inline patch(후킹)하여 사용자 계정을 탈취한다.
탈취한 정보를 아래의 양식으로 TingSting.dll에 저장한다.

```
[MIZI]
ZHao -> 사용자 계정
MmA -> 패스워드
QuBie -> ZuoBian | YouBian
```

그 후 http://www.axxxxxxx.com/dxxxxx/sxx.asp 로 계정과 패스워드를 전송한다. (모자이크)

• **iexplore Thread**

HttpSendRequestA과 HttpSendRequestW 함수를 후킹하여 로그인시 전송되는 URL을 가로채 아이디와 패스워드를 추출한다. HttpSendRequest 함수의 네 번째 파라미터인 lpOptional 값을 감시한다. 이 파라미터는 POST와 PUT 오퍼레이션에 사용된다.

lpOptional 값이 다음의 형태이면 아이디와 패스워드 부분을 추출하여 악성 웹 사이트로 전송한다.

```
strNexonID=<아이디>strPassword=<패스워드>
login_mode_login&??&id=<아이디>&pw=<패스워드>
```

• **nateonmain Thread**

네이트온에서 사용되는 CKAppEx.dll을 Hooking하여 아이디와 패스워드를 탈취한다.

CKAppEx.dll 파일의 베이스 주소를 구하고, 베이스 주소+0x5035에 있는 명령어가 다음과 같다면 그곳을 inline patch 한다.

```
50              PUSH EAX
83C4 C4         ADD ESP,-3C
```

이 부분이 실행될 때 esi와 edi에 사용자 아이디와 패스워드 정보가 담긴 메모리 주소를 가지고 있기 때문에 이 레지스터 값을 추출하여 계정 정보를 얻을 수 있다.

이렇게 얻은 계정 정보는 악성 사이트로 전송시킨다.

3) SysMan.sys 파일 분석

SysMan.sys는 서비스로 실행되는 드라이버로 백신의 보호모드를 우회하기 위해 커널 메모리를 변조하여 훅을 설치한다.

위의 경우는 계정을 탈취하기 위한 것이었으나 이번 경우는 모 백신의 SSDT inline hooking을 회피 하기 위해 훅을 설치하였다. 그 후 프로세스 목록을 구해 그 중 V백신 제품 관련 프로세스가 있으면 해당 프로세스를 강제로 종료시킨다.

마지막으로 PsSetCreateProcessNotifyRoutine 함수를 사용하여 V백신 관련 프로세스를 감시한다. 이 함수는 프로세스가 생성되거나 삭제 되었을 때 호출되는 콜백 함수를 설치한다. 콜백 함수는 생성된 프로세스가 관련된 프로세스라면 해당 프로세스를 종료시키는 일을 한다.

4) 결론

계정 탈취는 아이디와 패스워드가 넘어가는 루틴을 찾아서 그곳을 inline patch 해 정보를 획득하는 방식이었다. 그리고 백신의 보호 모드를 회피하기 위해 보호 루틴이 시작되기 직전에 다른 곳으로 뛰어서 보호 루틴을 우회하기도 하였다.

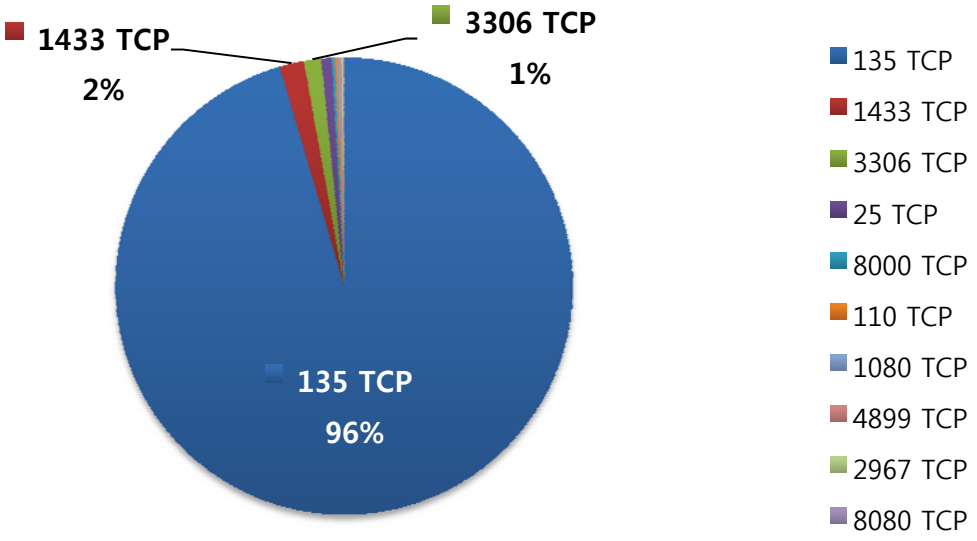
악성코드 제작자는 악성코드의 목적을 완수하기 위해 타겟을 정밀하게 분석하였다는 것을 알 수 있다.

이처럼 악성코드는 특정 타겟을 대상으로 정밀하게 분석 후 핵심을 공격하기 때문에 백신 제품에서도 그에 대응하기 위한 많은 노력이 필요하다.

Part I 5월의 악성코드 통계

3. 허니팟/트래픽 분석

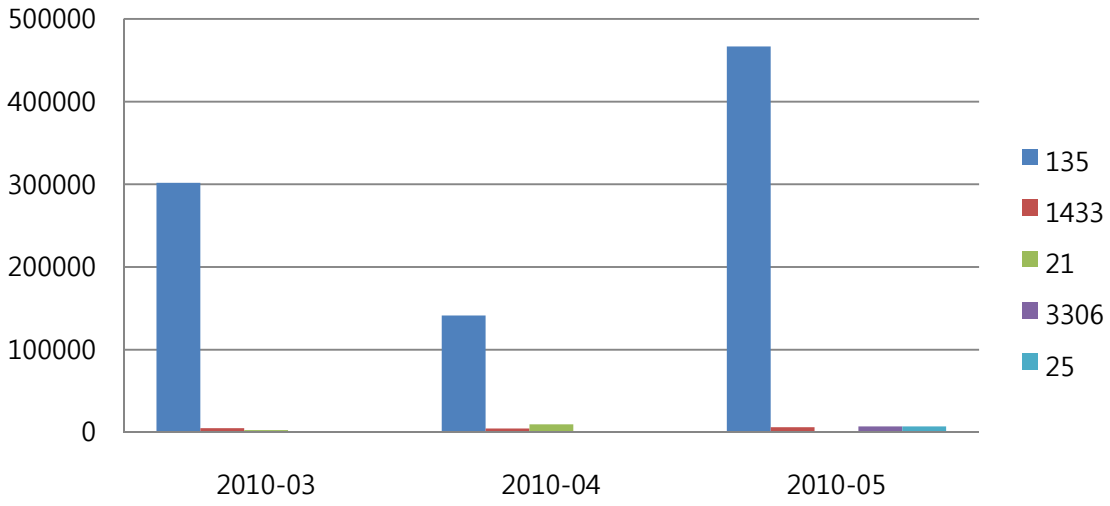
(1) 상위 Top 10 포트



5월에도 TCP 135번을 통한 악성 트래픽 유입이 많았으며, 취약점을 통해 악성코드가 침투한 후 같은 네트워트 대역단에서 추가 감염 PC를 만들기 위해 Brute-force 공격(아이디와 패스워드의 리스트를 사전(Dictionary) 형식으로 가지고 있다가 대입)을 수행하는 경우가 가장 많이 이용되고 있다.

(2) 상위 Top 5 포트 월별 추이

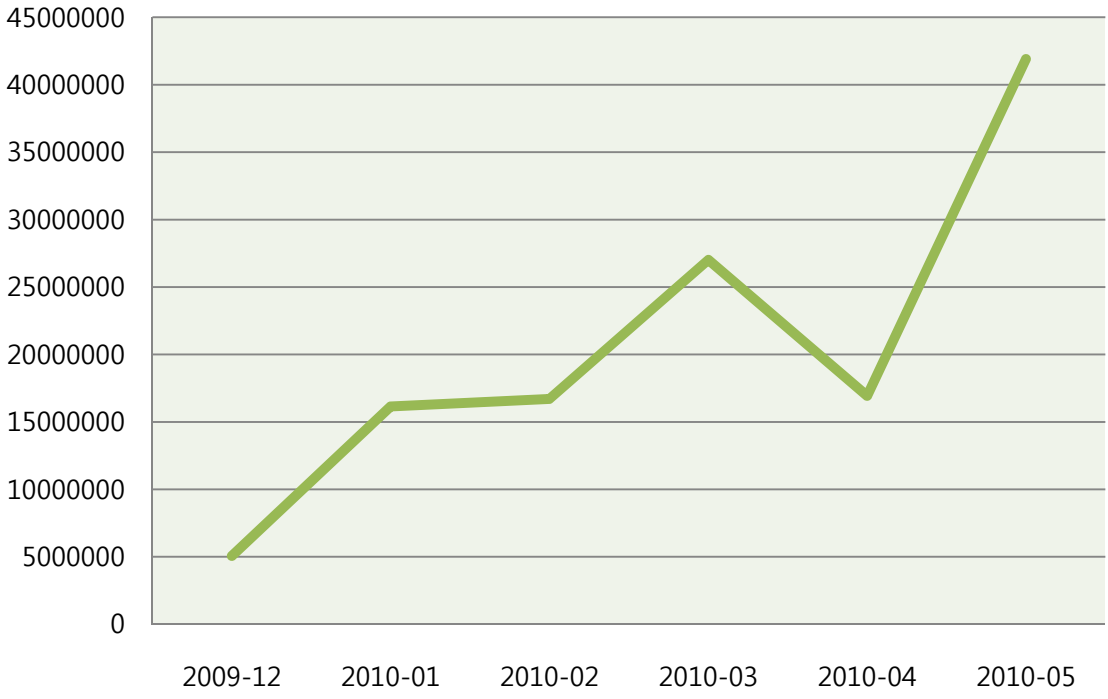
[2010년 3월 ~ 2010년 5월]



전체적으로 악성 트래픽 유입이 증가했으나 135번 이외의 포트들의 악성 트래픽 유입은 계속적으로 미미한 상태이다. 외부에서 135번 포트로 접근이 불필요한 경우 방화벽이나 IPS에서 차단하는 것이 보안 예방 효과에 좋다.

(3) 악성 트래픽 유입 추이

[2009년 12월 ~ 2010년 5월]

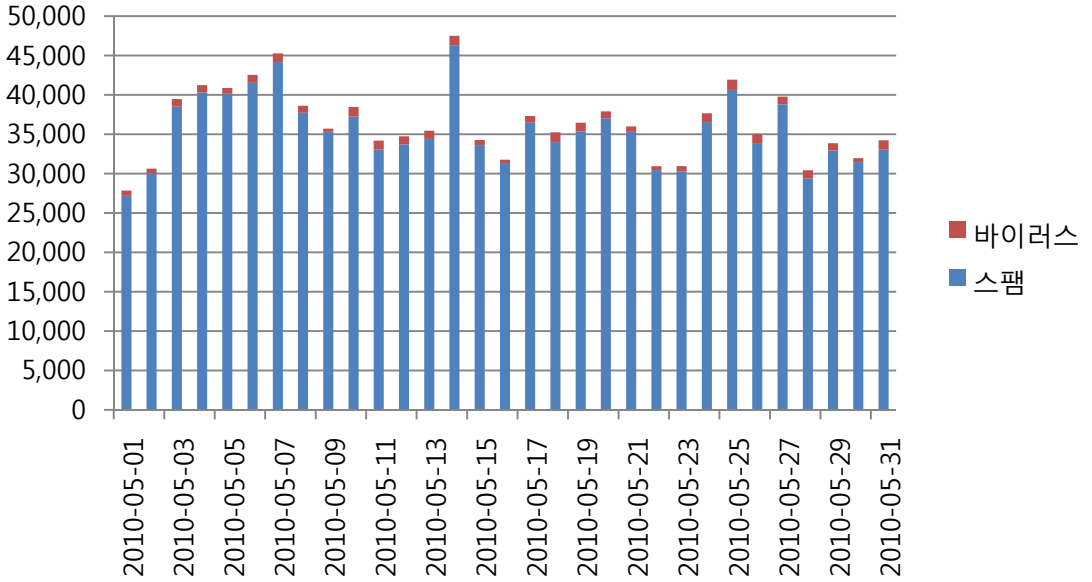


지난 달에 비해 악성 트래픽 유입이 크게 증가하였다.
자신이 즐기는 게임과 관련된 맵핵, 오토, 프리서버나 유료프로그램을 공짜로 사용하게 하는 크랙, 등록번호 생성기 등 남을 속이는 행위에 쓰이는 자료일수록 악성코드를 숨겨놓을 가능성이 높으므로 사용을 자제 해야 한다.
웹 서핑 중 사회적 이슈가 되는 검색 결과에 대한 자료는 항상 주의해야 하며, PC사용 중 가장 많이 쓰이는 프로그램을 사용자 스스로가 업데이트를 체크하는 습관이 필요하다.

Part I 5월의 악성코드 통계

3. 스팸 메일 분석

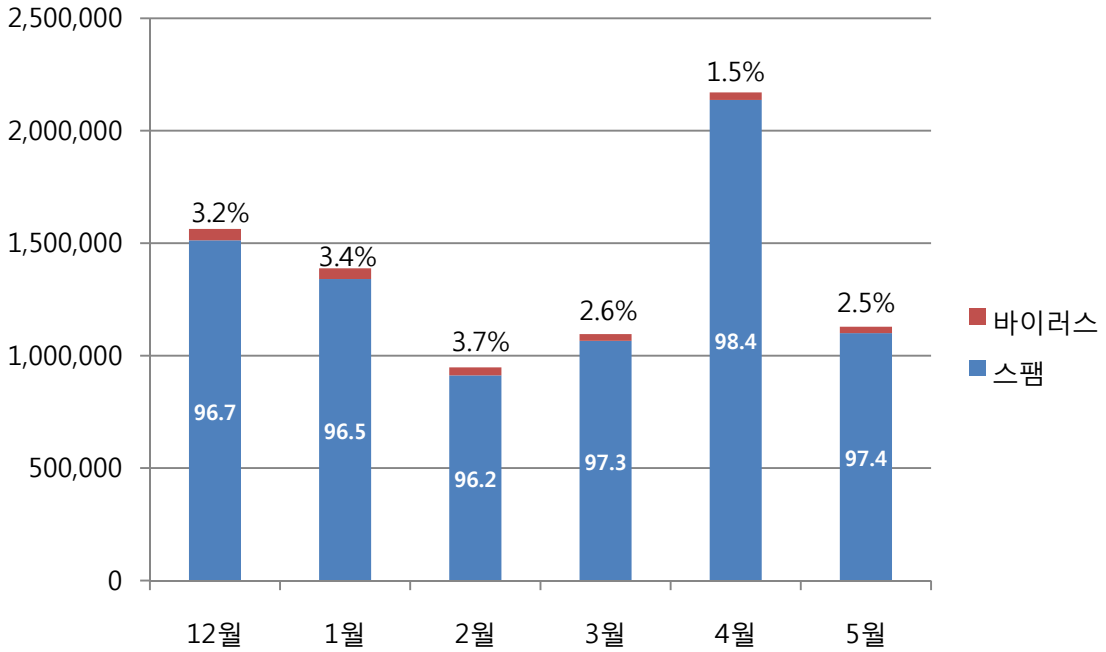
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 5월의 경우 남아공 월드컵과 관련된 내용의 악성코드 메일 유포 사례가 보고되었다.

(2) 월별 통계 현황

[2009년 12월 ~ 2010년 5월]



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

5월달 스팸 메일은 97.4%, 바이러스 메일은 2.5%를 차지하였다. 4월에 비해 스팸메일이 약 1% 감소하였으며, 바이러스 메일은 약 1.0% 증가하였다.

(3) 스팸 메일 내의 악성코드 현황

[2010년 5월 1일 ~ 2010년 5월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Virut-T	11,811	41.74%
2	Mal/ZipMal-B	4,201	14.85%
3	W32/MyDoom-H	4,053	14.32%
4	W32/Mytob-C	2,470	8.73%
5	W32/MyDoom-BZ	1,077	3.81%
6	Troj/CryptBx-ZP	830	2.93%
7	VPS-090709-DDoS-2	684	2.42%
8	Troj/Invo-Zip	382	1.35%
9	W32/Sality-I	371	1.31%
10	Mal/BredoZp-B	335	1.18%

스팸 메일 내의 악성코드 현황은 3월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Virut-T이 41.74%로 계속 1위를 차지하고 있다.

2위는 14.85%를 차지한 Mal/ZipMal-B, 3위는 14.32%를 차지한 W32/MyDoom-H이다.

특히, 5월달에는 Bredolab과 관련된 악성코드 스팸 메일들이 새롭게 등장했으며, Bredolab 악성코드 확산이 활발함을 알 수 있다.

Part Ⅱ 5월의 이슈 돋보기

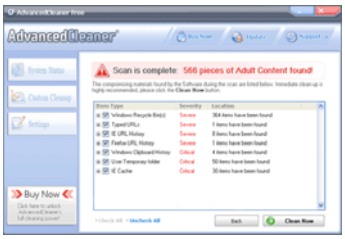
1. 5월의 보안 이슈

5월에는 가짜 백신으로 1억 달러 수익을 챙긴 일당 적발, 사이버 위협 경보 "관심"으로 상향 조정, 좀비 PC 방지법 소식 등 다양한 보안 이슈들이 많았습니다.

• 해외 가짜 백신으로 1억 달러 수익을 챙긴 일당 적발

컴퓨터가 허위로 악성코드에 감염되었다고 알려 결제를 유도하는 가짜 백신을 제작한 일당이 미국 당국에 적발되었습니다.

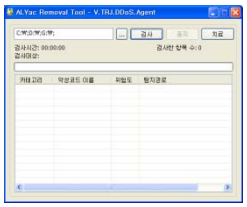
이들은 가짜 백신을 통해 전 세계적으로 1억 달러에 달하는 어마어마한 금액을 벌어들였다고 하며, 유령 광고 회사들을 차려 가짜 광고를 올리는 사업 또한 벌였다고 합니다.



• 방송통신위원회 좀비 PC 방지법 제정 초읽기

방송통신위원회에서는 2/4분기(6월까지) 악성 프로그램 확신 방지 등에 관한 법률(이하 좀비PC 방지법)을 추진할 계획을 밝혔습니다.

이번에 추진될 좀비 PC 방지법에서는 좀비 PC의 사이버 치료 체계를 구축하는 것을 목적으로 7.7 DDoS 같은 국가적인 사이버 위기 상황에서 긴급 대응이 가능한 전용 백신을 배포하며, 백신 회사 홈페이지 이외에도 포털 및 주요 사이트에서도 함께 다운로드 받을 수 있게 합니다.

• 방송통신위원회 사이버 위협 '관심' 경보 발령

국가정보원과 방송통신위원회, 행정안전부에서는 천안함 조사 결과 발표와 6.2 지방선거 등 국가적 이슈 상황을 틈타 사이버 공격 시도를 사전에 차단하기 위해 "관심" 단계로 사이버 위협 경보를 한 단계 상향 조정하였습니다.

현재까지 큰 국가적 사이버 공격 사례가 발견되지는 않았지만 7.7 DDoS 공격 1주년을 기념해 추가적인 공격이 재발할 수 있으므로 보안 업체와 정부기관에서는 긴장의 끈을 놓지 않고 있습니다.

Part Ⅱ 5월의 이슈 돋보기

2. 5월의 취약점 이슈

• Microsoft 5월 정기 보안 업데이트

Outlook Express, Windows Mail, Visual Basic for Applications(VBA)의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 5월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

Microsoft Outlook Express (MS10-030)
Microsoft Windows Mail (MS10-030)
Microsoft Windows Live Mail (MS10-030)
Microsoft Office XP/2003/2007 (MS10-031)
Microsoft Visual Basic for Applications, SDK (MS10-031)

<취약점 목록>

MS10-030 (978542) : Outlook Express 및 Windows Mail의 원격 코드 실행 문제점
MS10-031 (978213) : Microsoft Visual Basic for Applications의 원격 코드 실행 문제점

<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-may.mspx
영문 : http://www.microsoft.com/technet/security/Bulletin/ms10-may.mspx

• Microsoft Windows Canonical Display Driver (cdd.dll) 취약점

Canonical Display Driver (cdd.dll)에서 원격코드 실행이 가능한 취약점이 발견되었습니다.
이 취약점을 통해 원격코드 실행 가능성은 메모리 랜덤화(memory randomization) 기술로 인해 낮을 수 있으나 시스템 정지 혹은 재시작(reboot) 될 수 있습니다.
이 취약점은 윈도우 Aero 테마가 적용된 경우에만 영향을 받습니다.

<해당 제품>

Microsoft Windows 7 x64 CPU 환경
Microsoft Server 2008 R2 (x86, Itanium CPU 환경)
(Windows 2000/XP/2003/Vista/2008/7 32bit CPU 환경은 해당되지 않습니다.)

<임시 해결책>

현재 공식적인 보안 패치가 제공되지 않는 제로데이(Zeroday) 상태이므로 윈도우의 Aero 테마를 비활성화(disable) 시켜둡니다.
홈페이지 : http://www.microsoft.com/technet/security/advisory/2028859.mspx

Contact us…

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약사이트 : www.alyac.co.kr