
알약 월간 보안동향 보고서.

2014년 3월



알약 3월 보안동향보고서

CONTENTS

Part1 2월의 악성코드 통계

- 악성코드 통계
- 허니팟/트래픽 분석
- 스팸메일/악성코드가 포함된 메일 분석
- 스미싱 분석

Part2 2월의 악성코드 이슈

- 악성코드 개요
- 악성코드 흐름도
- 악성코드 상세분석
- 악성파일 분석
- 결론
- 치료방안

Part3 보안 이슈돌보기

- 2월의 보안 이슈
- 2월의 취약점

Part4 해외 보안동향

- 영미권
- 중국
- 일본

2월의 총평

2월은 소치 동계올림픽이 있었던 달이다. 이 때문에 사람들의 관심이 집중된 ‘소치올림픽’을 키워드로 악용한 스미싱 공격이 수 차례 발생했다. 이를 통해 사용자들의 스마트폰으로부터 다양한 개인정보 및 금융정보를 탈취하는 시도가 계속되었다.

그 외에는 중국의 춘절연휴가 끝난 2월 초부터 변조된 웹을 통해 악성코드를 유포하는 드라이브 바이 다운로드(Drive by Download) 공격이 1월에 비해 약 30% 이상 크게 증가한 점이 주목할 만하다. 이렇게 유포되는 악성코드는 주로 사용자들의 금융정보(계정, 공인인증서)를 노리는 형태이거나, 사용자PC를 좀비PC로 만드는 봇 형태인 경우가 대다수였다. 그 외에도, 애드웨어의 업데이트 서버를 해킹 후 설치된 PC에 직접 악성코드를 유포하는 경우가 종종 발견되었다.

Part1. 2월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸메일 및 악성코드가 포함된 메일 분석

스미싱 분석

1. 악성코드 통계

감염 악성코드 TOP15

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

2014년 2월의 감염 악성코드 TOP 15에서는 지난달 1위를 차지했던 Variant.Graftor.8654 악성코드는 2013년 11월 이후 4달 연속으로 1위를 차지했으며, 지난달 3위를 차지했던 TrojanDownloader.KorAdware.Gen가 한단계 상승하여 2위를 기록했다.

TrojanDownloader.KorAdware.Gen은 애드웨어 혹은 스폰서 프로그램들을 사용자 동의 없이 유포하는 악성코드를 말한다.

3위는 새롭게 등장한 Gen:Variant.Adware.Graftor.129002가 차지했다. 이는 정상적인 소프트웨어로 가장한 애드웨어의 변종이다.

전반적으로 2월은 1월에 비해 사흘이나 짧기 때문인지 악성코드 감염자수가 전반적으로 감소했다. 그러나 트로이목마의 초강세와 애드웨어들의 건재함이라는 큰 기조는 변함 없이 꾸준한 형태를 보여주고 있다.

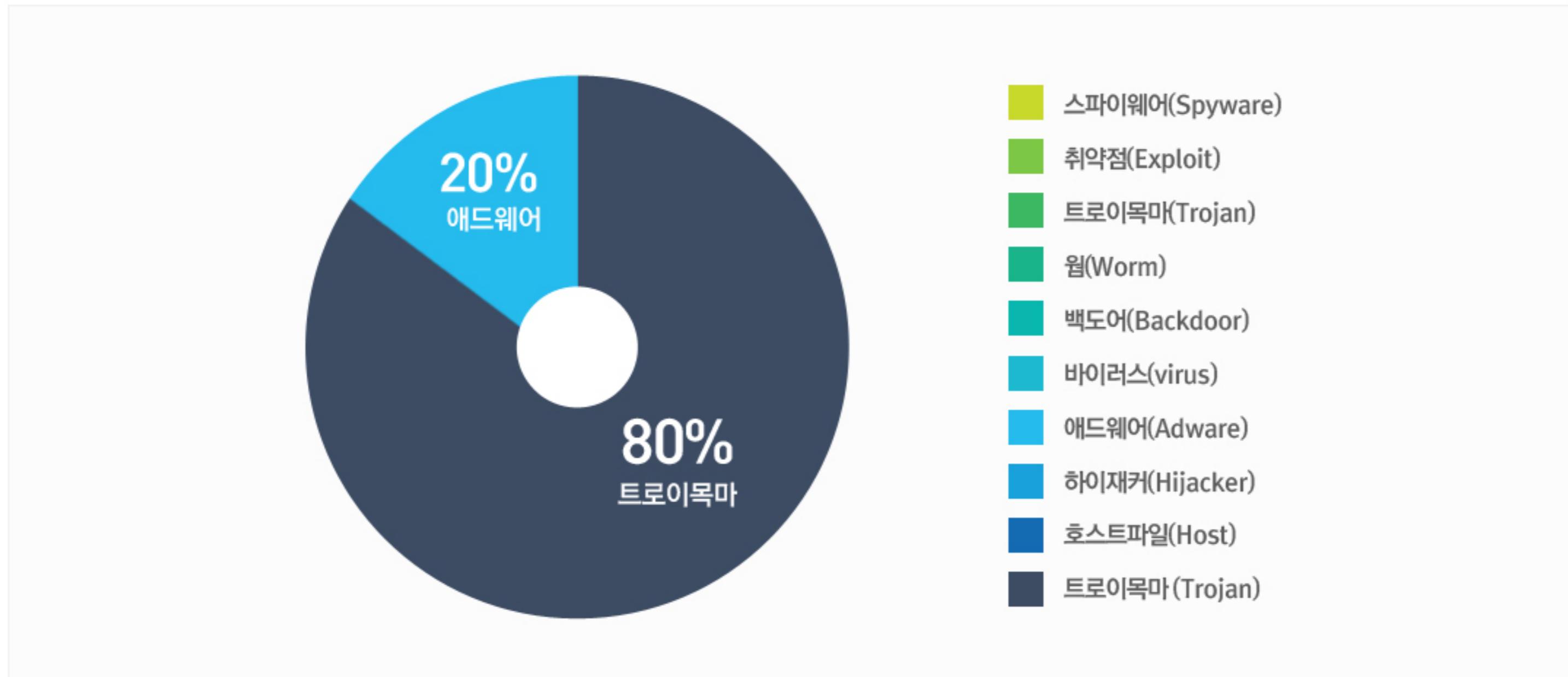
순위	동락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Variant.Graftor.8654	Trojan	3,595
2	▲ 1	TrojanDownloader.KorAdware.Gen	Trojan	2,368
3	NEW	Gen:Variant.Adware.Graftor.129002	Adware	1,813
4	NEW	Gen:Variant.Graftor.128868	Trojan	1,801
5	NEW	Gen:Variant.Adware.Graftor.125598	Adware	1,610
6	NEW	Gen:Variant.Graftor.128793	Trojan	1,371
7	NEW	Gen:Variant.Graftor.129002	Trojan	1,278
8	NEW	Gen:Trojan.Heur.JPuuW@a4mPwmhO	Trojan	1,139
9	NEW	Trojan.GenericKD.1470680	Trojan	1,116
10	NEW	Trojan.GenericKD.1472625	Trojan	1,114
11	NEW	Trojan.GenericKD.1470681	Trojan	1,025
12	NEW	Trojan.GenericKD.1470677	Trojan	1,019
13	NEW	Gen:Variant.Adware.Graftor.124966	Adware	1,009
14	NEW	Trojan.GenericKD.1470679	Trojan	956
15	NEW	Trojan.GenericKD.1470671	Trojan	946

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2014년 02월 01일 ~ 2014년 02월 28일

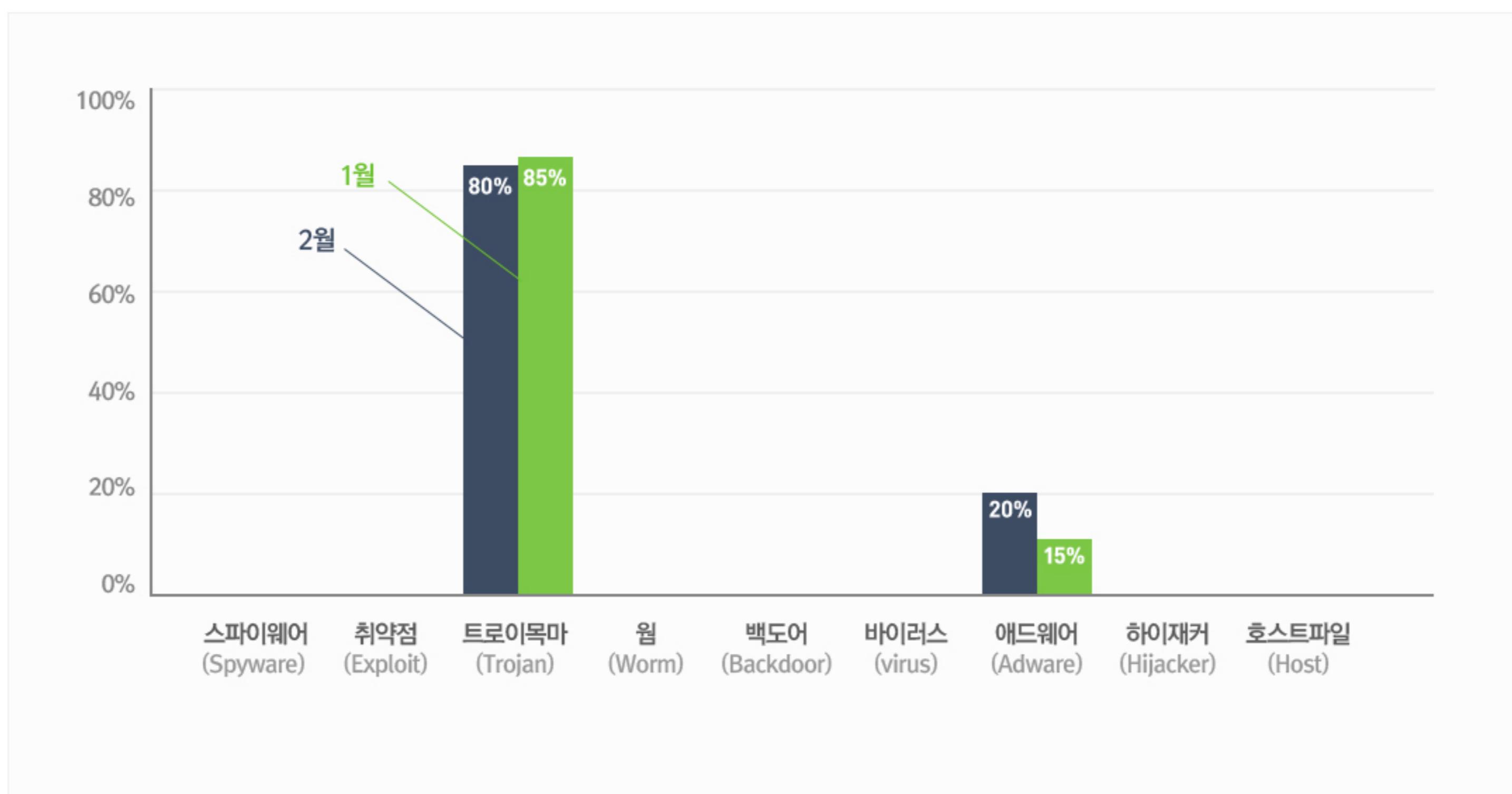
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 80%를 차지했으며, 이어 애드웨어(Adware) 유형이 20%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

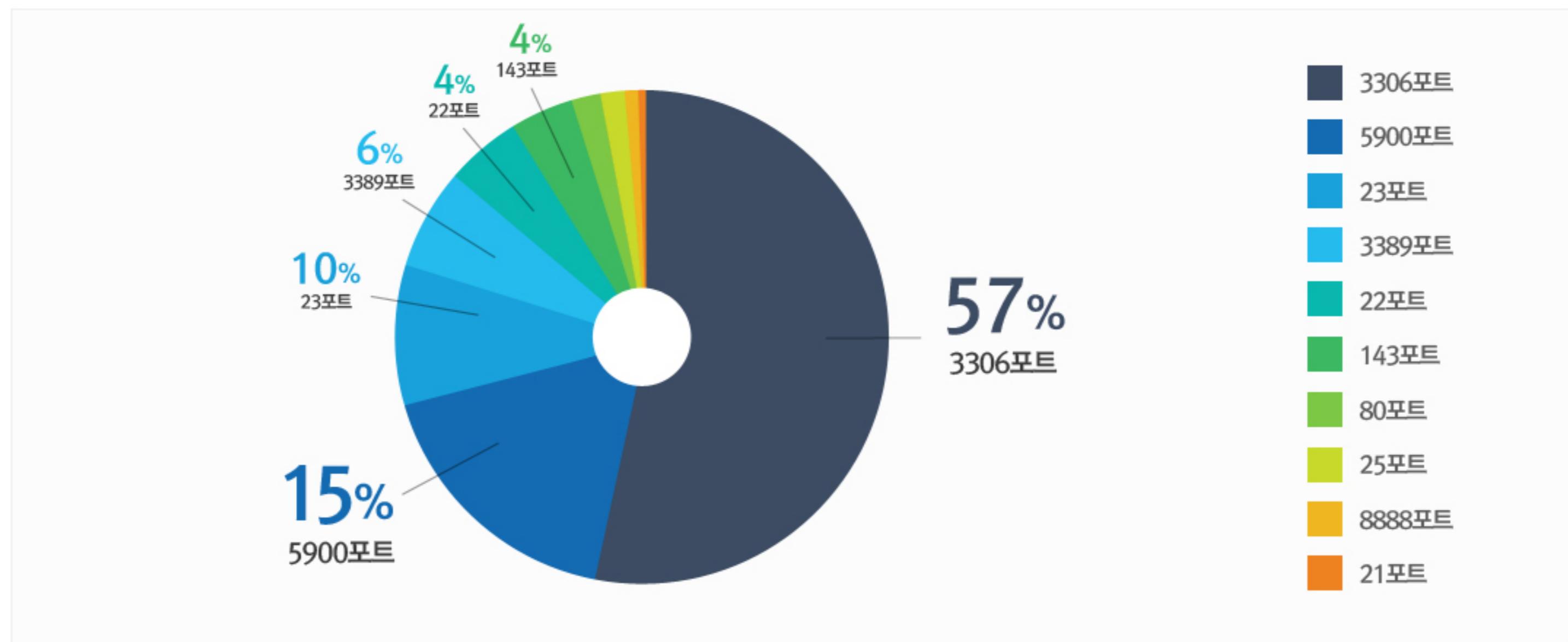
2월에는 지난 1월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 약간 감소하고, 애드웨어(Adware) 유형 악성코드가 소폭 증가했다.



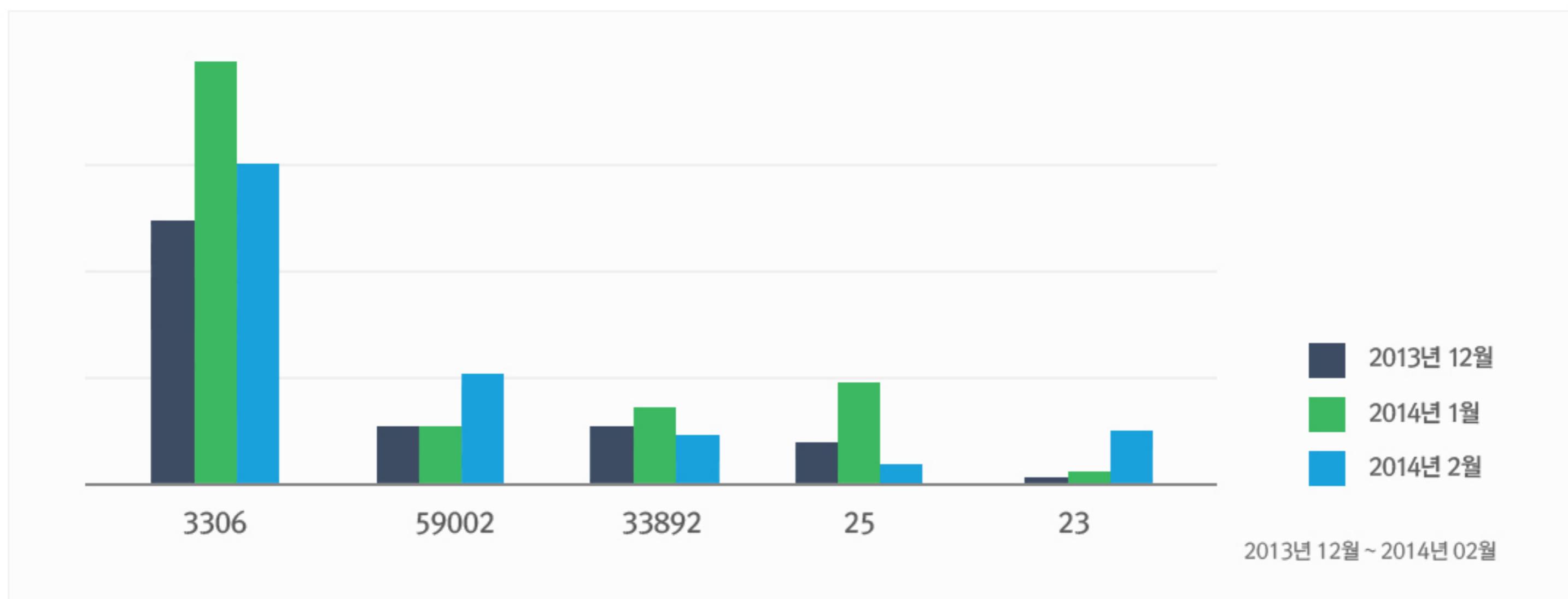
2.허니팟/트래픽 분석

2월의 상위 Top 10 포트

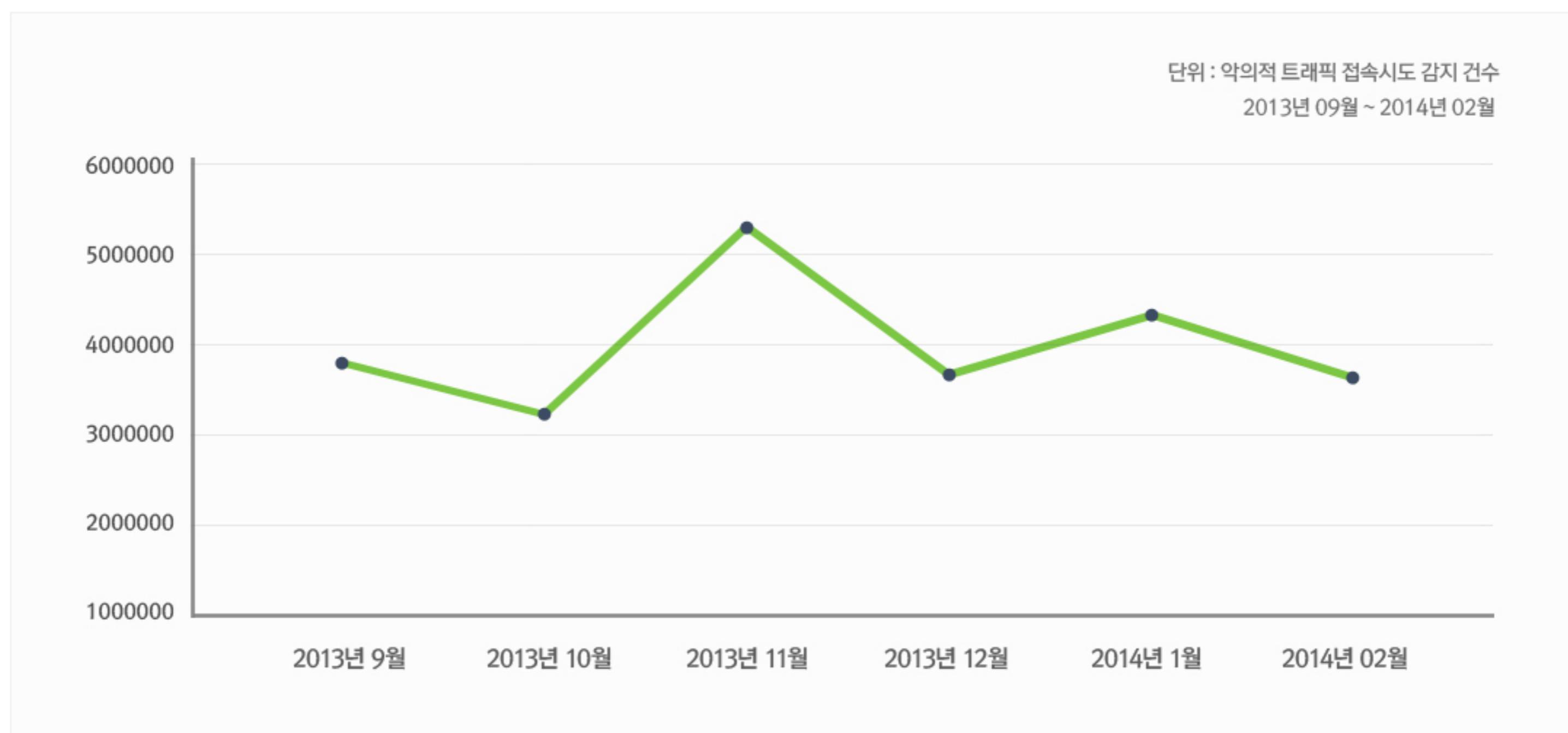
허니팟/정보수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트정보 및 악성트래픽을 집계한 수치



최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

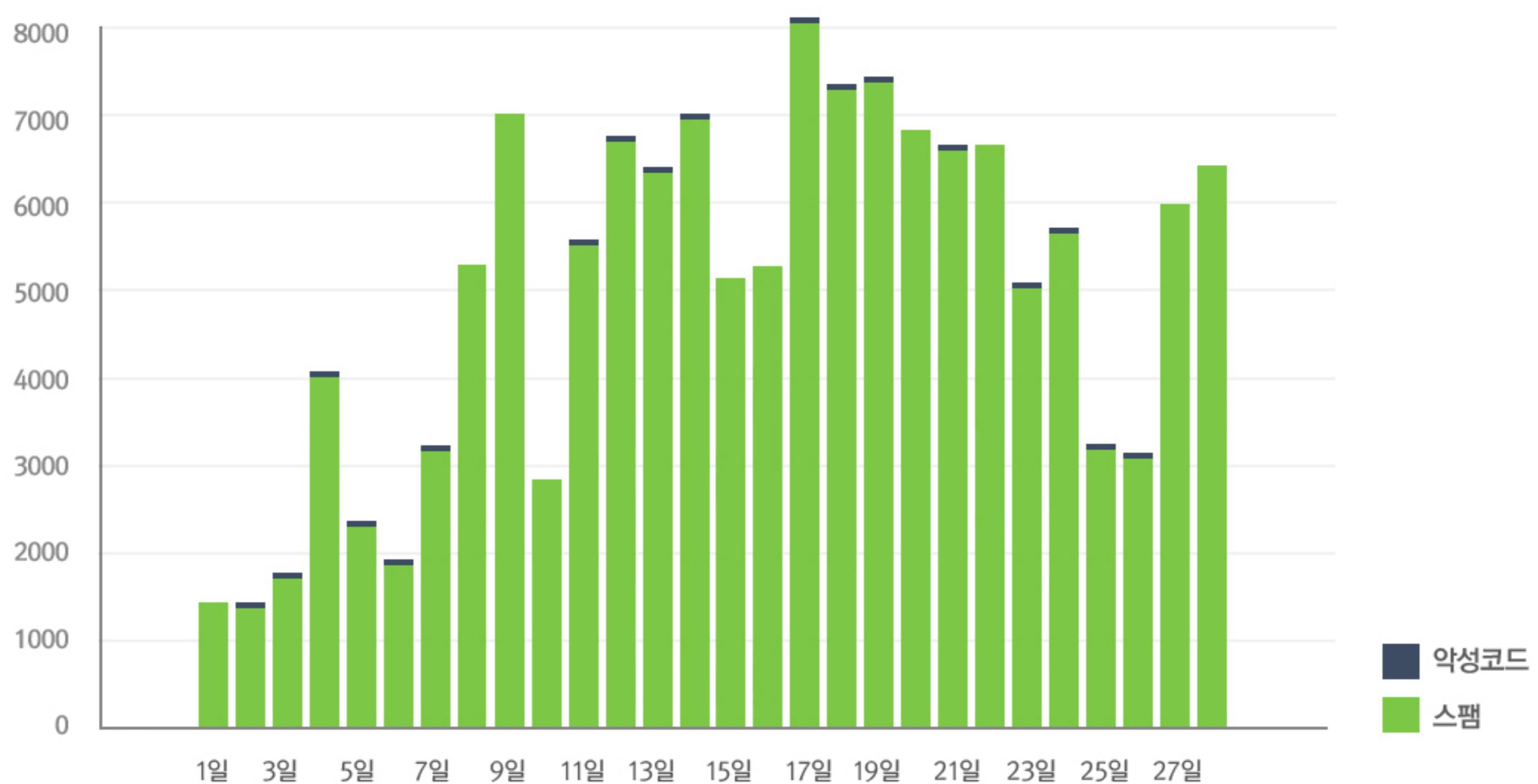


3. 스팸메일 및 악성코드가 포함된 메일 분석

일별 스팸 메일 및 악성코드 포함 메일 통계 현황

일별 스팸 및 악성코드 통계 현황 그래프는 하루에 허니팟 및 정보수집용 메일서버를 통해 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프이다. 2월의 경우 1월에 비해 사흘이나 기간이 짧았음에도 불구하고, 유입되는 스팸 메일수가 무려 54%나 증가했다. 이는 소치 올림픽 이슈와 함께 입학 및 졸업 시즌을 맞이하여 다양한 형태의 스팸 메일이 발생했기 때문인 것으로 보인다.

악성코드가 포함된 메일수치는 1월에 이어 2월에도 감소추세를 보였다. 2월에 가장 많이 발견된 메일에 포함된 악성코드는 Mydoom 악성코드이다. Mydoom은 주로 이메일을 통해 유포되는 트로이목마 악성코드이며, 일단 감염되면 백도어를 생성하는 것은 기본이고 정보 탈취와 같은 다양한 추가적인 악성행위를 한다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2014년 02월 01일 ~ 2014년 02월 28일
총 신고 건수	24,806건

키워드별 신고 내역

키워드	신고 건수	신고 건수
등기	7,160	28.86%
법원	4,851	19.56%
결혼	3,056	12.32%
훈련	2,736	11.03%
출석	1,977	7.97%
택배	1,153	4.65%
정보	744	3.00%
우편	678	2.73%
카드	449	1.81%
웃김	426	1.72%

스미싱 신고 추이

지난달 스미싱 신고 건수 41,510건 대비 이번 달 24,806건으로 알약 안드로이드 스미싱 신고 건수가 약 40% 감소했다.

2월의 스미싱 현황은 전달 대비 신고 건수가 크게 감소한 것으로 보인다. 각 주요 키워드의 신고 건수가 대폭 줄어들었고, 새로운 키워드의 신고가 증가했다. 1월에 모임, 카드, 새해 키워드가 높은 신고 건수를 기록했다. 반면, 2월에는 훈련, 정보, 출석, 결혼 키워드가 새롭게 상위 키워드로 떠올랐다.

훈련 키워드는 예비군, 민방위 훈련으로 인한 것으로 보이며, 정보 키워드의 경우 카드사 정보유출 문구에서 비롯된 것으로 분석된다. 특히, 이슈가 되고 있는 '스미싱' 자체를 사칭한 스미싱이 증가하고 있어 사용자들의 각별한 주의가 요구된다.

알약이 뽑은 2월 주의해야 할 스미싱

특이문자

순위	문자내용
1	소치 화제의 영상 재미있네요 ㅎㅎ
2	[민방위교육] 5년차이상 사이버교육으로 대체가능합니다
3	일요일결혼식잊지말고축복하러와주세요웨딩사진첩^o^

다수문자

순위	문자내용
1	[등기 발송하였으나[전달 불가]부재 중 하였습니다(내용확인).~
2	법원면책통지서상세내용
3	민방위 훈련 통지드립니다 2014 교육,훈련일정 확인요망
4	두근 두근 기다리는 내 택배.스마트택배가 어디쯤 오고 있는지 자동으로 알려드림
5	대박웃김 ㅎㅎ 꼭! 보세요

Part2. 2월의 악성코드 이슈 분석

악성코드 개요

악성코드 흐름도

악성코드 상세 분석

악성파일 분석

결론

치료방안

1. 악성코드 분석(Trojan.SnakeS)

개요

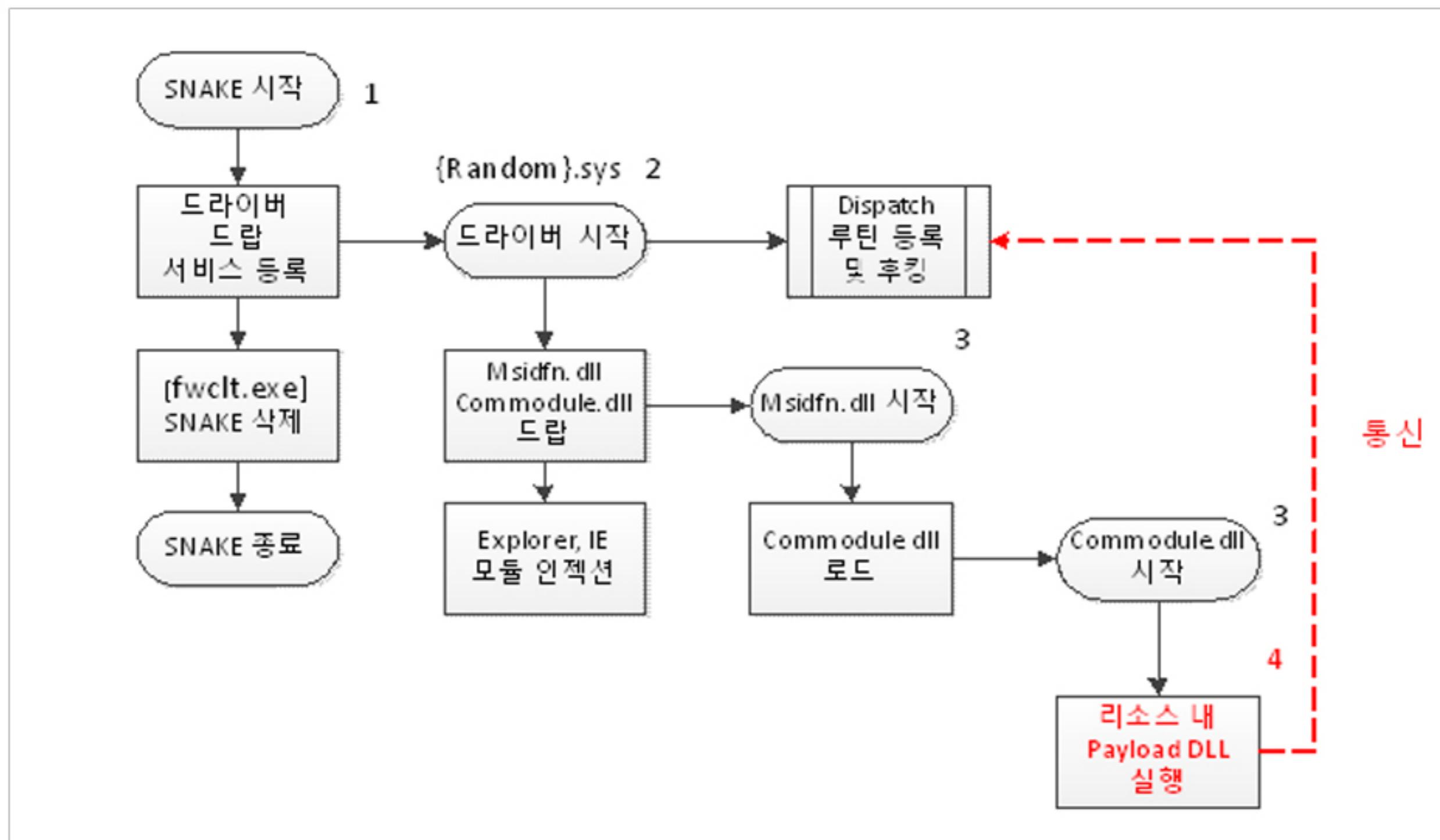
이 악성코드는 최근 외신에서 우크라이나 분쟁과 관련하여 보도한 것이다. 러시아가 제작하여 우크라이나를 대상으로 사이버 공격에 사용됐다고 추정하는 악성코드이다.

알약이 자체 분석한 결과, 해당 악성코드의 최초 시작은 2007년 그 이전으로 파악하고 있다. (이전 탐지명: Worm.Autorun.j)

봇(BOT) 악성코드는 오래 전부터 여러 유포 방식으로 다양하게 악용하고 있지만 목적에 따라 사이버 무기로도 사용될 수 있다. 주요 유포 경로는 정확히 알려지지 않았으나, 악성코드에 포함된 기능상 usb 자동실행과 이메일로 유포할 것으로 추정하고 있다. 버전에 따라 64비트 윈도우 전용 악성 파일도 포함하고 있으나 기능은 32비트 전용과 같다.

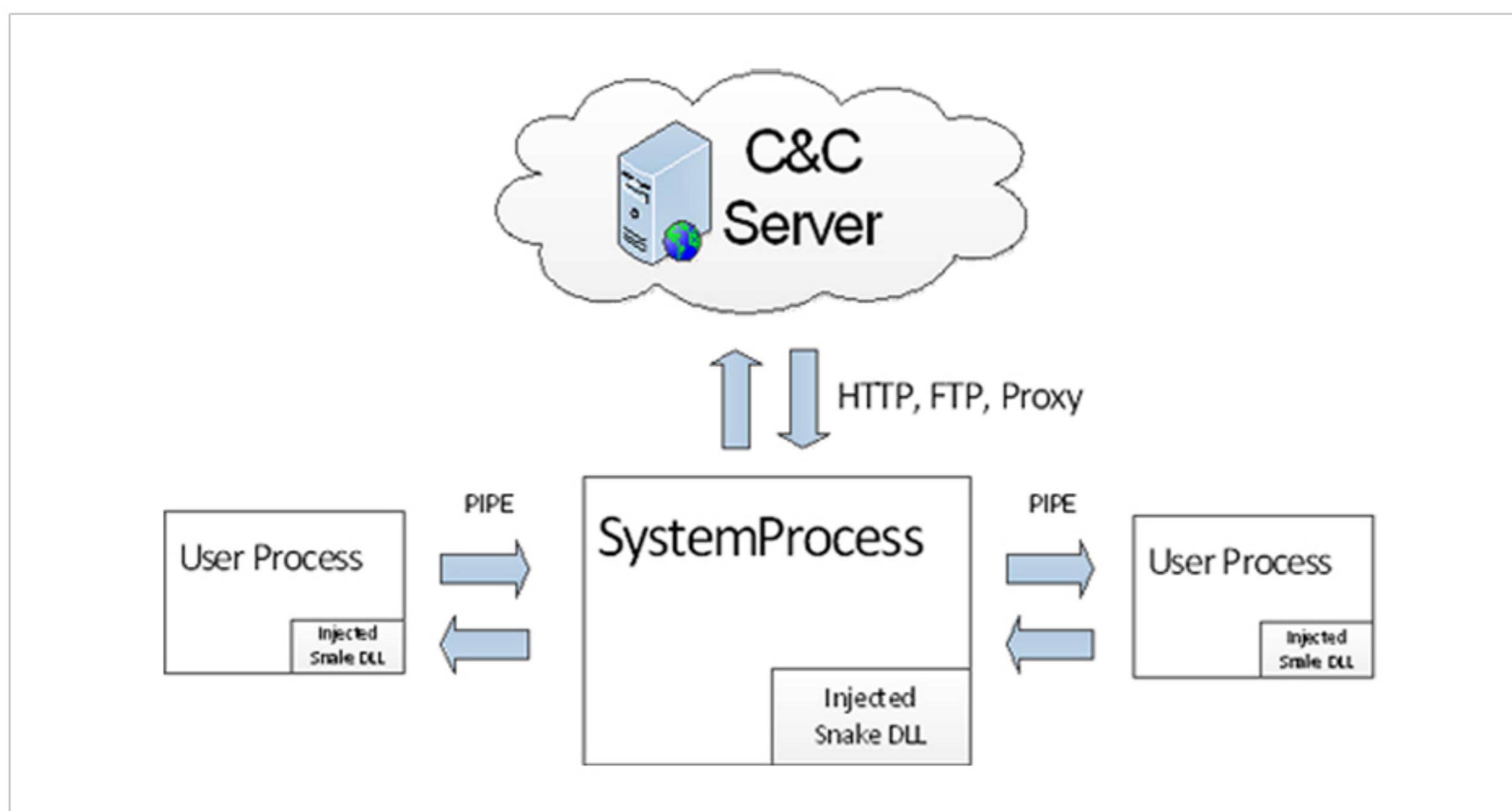
2. 악성코드 흐름도

악성코드 흐름도



악성코드 파일 실행 순서도

2007년 제작되어 알약에서 기탐지 중인 샘플과 복호화 코드 및 사용하는 파일명, 서버 도메인이 유사하다



Part2.2월의 악성코드 이슈 분석

File identification	
MD5	b41fbdd02e4d54b4bc28eda99a8c1502
SHA1	4b47c438a5fc320297eb57ae00756271a2920176
SHA256	05dc66031e4276bc20010743d8cd0ee36e4064cf087b6b4617febf86a4702873
ssdeep	1536.niKJHl1llkOw1gK78z1Ye9GkTHT/UoR4GigXq/uovA.9l1/Oo2BFITMaVdq/uot
imphash	80f26738f0789833e61779982b1c9d91
File size	96.0 KB (98304 bytes)
File type	Win32 DLL
Magic literal	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (67.3%) Win32 Dynamic Link Library (generic) (14.2%) Win32 Executable (generic) (9.7%) Generic Win/DOS Executable (4.3%) DOS Executable Generic (4.3%)
Tags	armadillo peddl
VirusTotal metadata	
First submission	2007-08-14 11:04:04 UTC (6년, 7개월 전)
Last submission	2014-02-25 17:43:08 UTC (2주, 1일 전)
파일 이름	Trojan.Win32.Agent.bve b41fbdd02e4d54b4bc28eda99a8c1502.dll

[그림 1] 기 탐지중인 2007년 샘플 정보

File identification	
MD5	440802107441b03f09921138303ca9e9
SHA1	819e4105028084c77f2df73863400f9539f76aee
SHA256	5d21324eddb511fd4630a46d78673d73777383d62fc3ac2c966fd922f7f21256
ssdeep	6144.zCsUQFxOqzKbDkdn9TziwsnjFmDjoe1Htcihk8hofptlQA2Ug zCsUQFxOq+3lowf
imphash	de83b03271429a0d0ae7c1f598d9412d
File size	428.0 KB (438272 bytes)
File type	Win32 DLL
Magic literal	PE32 executable for MS Windows (DLL) (console) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (67.3%) Win32 Dynamic Link Library (generic) (14.2%) Win32 Executable (generic) (9.7%) Generic Win/DOS Executable (4.3%) DOS Executable Generic (4.3%)
Tags	peddl
VirusTotal metadata	
First submission	2014-01-31 15:20:39 UTC (1개월, 1주 전)
Last submission	2014-03-12 08:40:02 UTC (16시간, 59분 전)
파일 이름	224735096_5d21324eddb511fd4630a46d78673d73777383d62fc3ac2c966fd922f7f21256 viruscan

[그림 2] 신규로 추가된 2014년 샘플 정보

그림 3과 그림 4를 보면, 난독화 알고리즘에서 사용되는 키의 정보를 볼 수 있다. 이는 2007년에 최초 발견된 샘플과 매우 유사하다.

```

if ( a2 && a3 )
{
    if ( a4 )
        v4 = *(_DWORD *) (this + 0xC);
    else
        v4 = 0;
    v5 = 0;
    if ( a3 )
    {
        do
        {
            *_BYTE *(v5 + a2) ^= a1dm3uu4j7fw4sjnbc[v4++];
            if ( v4 >= *(_DWORD *) "b" )
                v4 = 0;
            ++v5;
        }
        while ( v5 < a3 );
    }
    if ( a4 )
        *(_DWORD *) (this + 0xC) = v4;
}
    
```

[그림 3] 2007년도 샘플의 난독화 코드

```

if ( Src )
{
    v5 = a3;
    if ( a3 )
    {
        if ( a4 )
            v6 = *(_DWORD *) (this + 4);
        else
            v6 = 0;
        if ( a3 )
        {
            do
            {
                BYTE3(Src) = *(_BYTE *) v4 ^ a1dm3uu4j7fw4_0[v6];
                result = memcpy(v4, (char *)&Src + 3, 1u);
                ++v6;
                if ( v6 >= "b" )
                    v6 = 0;
                v4 = (char *) v4 + 1;
                --v5;
            }
            while ( v5 );
            this = v8;
        }
        if ( a4 )
            *(_DWORD *) (this + 4) = v6;
    }
}
    
```

[그림 4] 최근 발견된 샘플의 난독화 코드

```

if ( byte_10045066 == v9 )
    sub_1000F35F(v11);                                // Query Software\Microsoft\Internet Account Manager\Accounts\
else
    sub_1000F4F6(v11);                                // find file %LocalAppData%\Microsoft\Windows Mail\Local Folders\ oeaccount
    dword_10043BE0 = v11;
    sub_1000288A(v11);
return v11;
    
```

[그림 5] 안티 스팸 필터 솔루션 무력화

플러그인으로 제공하는 모듈 중 아웃룩 관련 악성코드가 있다. 주요 행위는 감염자 시스템에 저장된 이메일 계정을 수집하고, 특정 안티스팸 필터 솔루션을 무력화하는 것이다.

3.악성코드 상세분석

악성파일 분석(zxcvb.exe)

메인 EXE의 역할은 악성 드라이버 파일 드랍 및 서비스 등록이다. 동시에, 추후 핵심 악성코드에서 쓰일 환경 정보를 레지스트리에 기록한다. 즉, 악성코드 동작 구성을 설정하는 인터페이스로 볼 수 있다.

```
Reg Key Added HKLM\SYSTEM\CurrentControlSet\Services\map
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\DisplayName map
Reg Key Added HKLM\SYSTEM\CurrentControlSet\Services\map\Enum
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\Enum\0      Root\LEGACY_MAP\0000
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\Enum\1
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\Enum\NextInstance 1
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\ErrorControl 0
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\ImagePath  ??WC:\WINDOWS\system32\DRIVERS\map.sys
Reg Key Added HKLM\SYSTEM\CurrentControlSet\Services\map\Parameters
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\Parameters\dParam BINARY SIZE=9 MD5=36963E37ECC1AD30F81F0990E938BC1B
Reg Key Added HKLM\SYSTEM\CurrentControlSet\Services\map\Security
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\Security\Security BINARY SIZE=168 MD5=6F319799C67F03A2F4F875408BCC7D52
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\Start 1
Reg Val Added HKLM\SYSTEM\CurrentControlSet\Services\map\Type 1
```

[그림 1] 악성 드라이버 서비스 실행

위 행위는 악성코드의 드랍퍼에서 악성 드라이버를 드랍하고 레지스트리를 등록한 정보이다. 드랍퍼는 악성코드 동작에 시작이 되는 역할로, 드랍 및 레지스트리 설정등 수행이 종료될 경우 Fwclt.exe 샘플을 드랍한 뒤 실행한다. 해당 샘플은 입력된 경로의 파일을 삭제하는 것으로 마무리된다. 따라서 본 악성코드는 한 번 실행된 이후에는 최초 유포 악성코드를 습득할 수 없다.

언급한 드라이버는 초기 로드 시 유저모드에서 동작하는 핵심 악성코드를 드랍하며, [explorer.exe], [services.exe], 및 기타 브라우저에 인젝션을 수행하여 악성 행위를 시작하게 된다.

악성파일 분석(zxcvb.sys)

```
0: kd> !devobj 864fb2b8
Device object (864fb2b8) is for:
FaDevice0 \Driver\sdbas DriverObject 86359508
Current Irp 00000000 RefCount 0 Type 00000022 Flags 00000850
Dacl e148e48c DevExt 864fb370 DevObjExt 864fb3d8
ExtensionFlags (0000000000)
Device queue is not busy.
```

[그림 2] 악성코드에서 설치된 디바이스 정보

현재 설치된 디바이스 명은 \Driver\sdbas지만 sdbas라는 이름은 최초 드랍퍼에서 드랍하여 악성코드에 대한 설치 때 마다 바뀐다.

Part2.2월의 악성코드 이슈 분석

```
int __cdecl DropFiles()
{
    int v0; // eax@2
    int v1; // eax@2
    char filePathName[2]; // [sp+8h] [bp-100h]@3
    char v4; // [sp+Ah] [bp-FEh]@3
    _int16 v5; // [sp+106h] [bp-2h]@3

    if ( !dword_6D544 )
    {
        dword_6D544 = 1;
        v0 = sub_1D660(&Encoded_Path_comodule, 60);
        byte_6CA3C = 0;
        Decode_(v0, (int)&Encoded_PE_comodule, (int)&unk_37063);
        v1 = sub_1D660(&Encoded_Path_msidfn, 60);
        byte_6C9BC = 0;
        Decode_(v1, (int)&Encoded_PE_msidfn32, 3584);
    }
    *_WORD *filePathName = 0;
    memset(&v4, 0, 0xFCu);
    v5 = 0;
    // #SystemRoot#\system32\msidfn32.dll
    Decode(filePathName, &Encoded_Path_msidfn, strlen((const char *)&Encoded_Path_msidfn));
    if ( DropFile((const uchar_t *)filePathName, &Encoded_PE_msidfn32, 0xE00u) )
    {
        sub_1DB42((const WCHAR *)filePathName);
        dword_6E884 = 1;
    }
    else
    {
        LOG_(word_15262, filePathName);
    }
    Decode(filePathName, &Encoded_Path_comodule, strlen((const char *)&Encoded_Path_comodule));
    // #SystemRoot#\system32\comodule.dll
    if ( DropFile((const uchar_t *)filePathName, &Encoded_PE_comodule, (ULONG)&unk_37063) )
        sub_1DB42((const WCHAR *)filePathName);
    else
        LOG_(word_1526E, filePathName);
    dword_6E884 = 1;
    return 0;
}
```

[그림 3] 악성코드 드라이버 내의 PE 드랍 코드

현재 설치된 디바이스 명은 \Driver\sdbas지만 sdbas라는 이름은 최초 드랍퍼에서 드랍하여 악성코드에 대한 설치 때마다 바뀐다.

25	NtClose	0x8058E4EC	inline hook	0x8058E4EC	C:\WINDOWS\system32\ntkrnlpa.exe
53	NtCreateThread	0x805D2FD4	inline hook	0x805D2FD4	C:\WINDOWS\system32\ntkrnlpa.exe
173	NtQuerySystemInformation	0x8061308C	inline hook	0x8061308C	C:\WINDOWS\system32\ntkrnlpa.exe
249	NtShutdownSystem	0x80614644	inline hook	0x80614644	C:\WINDOWS\system32\ntkrnlpa.exe
257	NtTerminateProcess	0x805D499E	inline hook	0x805D499E	C:\WINDOWS\system32\ntkrnlpa.exe

[그림 4] 루트킷

악성코드는 시스템 내에서 완벽한 스텔스 기능 동작을 구현하기 위해 Ring0(kernel Level)에서 Hook을 이용하여 자신의 행위를 숨긴다.

Service System Descript Table(SSDT)에 Hook을 설치하는 방식이 아닌, Ring0에서 Nt 계열 함수의 코드를 수정하는 방식으로 동작하고 있고, 총 5개의 함수에 투이 설치되어 있다.

```
nt!NtClose:
805be4ec b001          mov     al,1
805be4ee cd55          int     55h
805be4f0 c3             ret
805be4f1 64a124010000  mov     eax,dword ptr fs:[00000124h]
805be4f7 0fbe8040010000 movsx   eax,byte ptr [eax+140h]
805be4fe 6a00          push    0
805be500 50             push    eax
805be501 ff7508          push   dword ptr [ebp+8]
```

[그림 5] 변조된 인라인 후킹

Part2. 2월의 악성코드 이슈 분석

예제로 사용된 코드는 NtClose 함수 1개 이지만, 다른 함수 모두 동일한 방식으로 Interrupt 코드를 설치하는 방식으로 동작한다. 모두 Interrupt 55번을 이용하여 설치된 루트 킷을 동작하고 있다.

```
4e: 80542c3c nt!KiUnexpectedInterrupt30
4f: 80542c46 nt!KiUnexpectedInterrupt31
50: 806e793c hal!HalpApicRebootService
51: 80542c5a nt!KiUnexpectedInterrupt33
52: 80542c64 nt!KiUnexpectedInterrupt34
53: 80542c6e nt!KiUnexpectedInterrupt35
54: 80542c78 nt!KiUnexpectedInterrupt36
55: ed803eaf sdbas+0x11EAF
56: 80542c8c nt!KiUnexpectedInterrupt38
57: 80542c96 nt!KiUnexpectedInterrupt39
58: 80542ca0 nt!KiUnexpectedInterrupt40
59: 80542caa nt!KiUnexpectedInterrupt41
5a: 80542cb4 nt!KiUnexpectedInterrupt42
```

[그림 6] 유저 Interrupt 설치 확인

0x55(10진수 85) 위치에 Interrupt 를 설치하여 혹이 설치된 Nt 계열 함수 호출 시 악성코드의 루트킷 드라이버가 호출되면 스텔스 기능이 동작된다. 악성코드 자체의 설치를 숨기기 위하여 위와 같은 동작을 한다. Ring0 모드 단에서의 후킹 및 Interrupt를 이용하여 악성코드 동작하는 과정에서 행위를 숨기고 있다.

각 후킹 된 NT 계열 함수

- NtClose
- NtCreateThread
- NtQuerySystemInformation
- NtShutDownSystem
- NtTerminateProcess

후킹된 5개의 함수는 모두 동일한 함수 코드를 호출하게 된다. 호출된 이후에는 현재 DeviceIoControl 을 이용하여 통신중인 모듈에서 생성된 EXE 의 PID 등 여러 가지 정보를 받게 되고 현재 동작중인 프로세스를 숨긴다.

```
int InBuffer; // [sp+4h] [bp-8h]@1
int v4; // [sp+8h] [bp-4h]@1

InBuffer = hProcess;
v4 = PID;
return DeviceIoControl_Logic(0x222048u, &InBuffer, 8u, 0, 0);
```

[그림 7] 생성된 PID 및 HANDLE 정보 전송

생성된 프로세스의 PID 및 HANDLE 드라이버로 전송한다.

```
hLibModule = atoi(&String2[v168]);
time(&Time);
RegSetValueExA(hKey, "B_STM", 0, 4u, &Time, 4u);
v128 = 86400 * hLibModule;
v137 = Time + 86400 * hLibModule;
RegSetValueExA(hKey, "E_STM", 0, 4u, &v137, 4u);
RegSetValueExA(hKey, "D_STM", 0, 4u, &v128, 4u);
RegCloseKey(hKey);
StealthMode(hLibModule);
Log_process(&unk_10073920, 1, "Go to stealth mode for %d days.", hLibModule);
```

[그림 8] 통신하는 DLL 의 코드

Part2.2월의 악성코드 이슈 분석

스텔스 모드 라는 기능이 동작할 경우 악성 코드는 아무런 연결을 하지 않으며, 동작이 되지 않고 지속적으로 PC에 잠복한다. 해당 기능이 동작 중에도 몇 일간 동작 하였는지에 대한 로그는 지속적으로 기록된다.

```
if ( dword_6CC38
    && (RtlInitUnicodeString(&DestinationString, L"\SystemRoot\SYSTEM32\winstat0.pdr"),
        ObjectAttributes.ObjectName = &DestinationString,
        ObjectAttributes.Length = 24,
        ObjectAttributes.RootDirectory = 0,
        ObjectAttributes.Attributes = 64,
        ObjectAttributes.SecurityDescriptor = 0,
        ObjectAttributes.SecurityQualityOfService = 0,
        ZwCreateFile(&FileHandle, 0x40100000u, &ObjectAttributes, &IoStatusBlock, 0, 0x80u, 0, 3u, 0x20u, 0, 0) >= 0 )
{
    ByteOffset.HighPart = sub_1E012(FileHandle);
    if ( ByteOffset.HighPart > dword_6CC38 )
    {
        sub_1E03C(FileHandle, 0i64);
        ByteOffset.HighPart = 0;
    }
}
```

[그림 9] 파일 열기

스텔스 기능 이외에도 유저모드에서 특정 IOCTL 코드를 이용하여 통신할 경우, winstat0.pdr라는 파일을 생성 혹은 오픈하여 로그를 남기고 있는 것을 확인할 수 있다.

```
while ( v4 );
v5 = v3 - (&Buffer + 1);
EncoderLogic(ByteOffset.HighPart, &Buffer, v3 - (&Buffer + 1));
ByteOffset = -1i64;
ZwWriteFile(FileHandle, 0, 0, 0, &LocalTime, &Buffer, v5, &ByteOffset, 0);
ZwClose(FileHandle);
result = 1;
```

[그림 10] 파일 쓰기

파일 오픈 이후에는 유저모드에서 받은 데이터에 날짜를 더하여, 해당 문자열에 대한 암호화를 수행한 암호화된 문자열을 파일에 쓴다. 또한, 파일을 닫는 역할을 하며 정보를 수집하는 것을 확인할 수 있다.

위 파일 열기 닫기 코드의 경우에는 DLL의 여러 곳에서 사용되고 있으며, 각종 문자열을 인자로 하여 드라이버로 전송하는 것을 확인할 수 있다. 여러 가지 문자열 및 수집된 데이터를 기반으로 드라이버에 전송하게 되면, 드라이버에서 자체적으로 암호화를 수행한 이후 파일에 저장한다. 또한 전송된 데이터와 드라이버 자체적으로 동작과정에서 생긴 정보를 저장한다.

악성파일 분석(common.dll)

본 악성파일은 services.exe 그리고 explorer.exe와 각종 웹 브라우저에 인젝션되어 각기 다른 역할을 수행한다. 그리고 각 프로세스간에는 통신을 위해 NamedPipe를 사용하는데, 다음과 같이 명명된다.

- User Process – UCM{ComputerName}
- System Process – SCM{ComputerName}

```
push    eax      ; nSize
lea     eax, [ebp+ComputerName]
push    eax      ; lpBuffer
call   ds:GetComputerNameA
lea     eax, [ebp+pcbBuffer]
push    eax      ; pcbBuffer
lea     eax, [ebp+UserName]
push    eax      ; lpBuffer
call   ds:GetUserNameA
```

[그림 11] 실행된 PC의 이름, 윈도우 계정 이름 습득 코드

```
if ( !lstrlenA(lpString) )
{
    OutLog(*((DWORD *)v4 + 1), 1, "%s: Error start server, because it pipe has no name.", v5);
    return 0;
}
if ( *((DWORD *)v4 + 136) )
{
    OutLog(*((DWORD *)v4 + 1), 1, "%s: already started.", v5);
}
else
{
    ResetEvent(*((HANDLE *)v4 + 2));
    if ( *((DWORD *)v4 + 135) )
        v6 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)ServerPipe, v4, 0, &ThreadId);
    else
        v6 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)ClientPipe, v4, 0, &ThreadId);
    *((DWORD *)v4 + 136) = v6;
    if ( !v6 )
    {
        v7 = GetLastError();
        OutLog(*((DWORD *)v4 + 1), 1, "%s: Error(%d) Start pipe server thread", v5, v7);
        return 0;
    }
    OutLog(*((DWORD *)v4 + 1), 1, "%s: Pipe server thread start, ", v5);
}
```

[그림 12] 통신용 NamedPipe 생성

```
19:20:42 !!!! DLL Type: Manager, User:system, service:0, BrowserStarter:0
SCMVM-28D4D51701F1: Pipe server thread start,
19:21:00 !!!! DLL Type: Manager, User:administrator, service:0, BrowserStarter:0
UCMVM-28D4D51701F1: Pipe server thread start,
```

[그림 13] 통신용 Pipe 생성 로그

유저 프로세스에서 본 악성코드는 추가적인 정보 등을 습득하여 로그 파일을 생성한다. 이를 서버 역할의 프로세스에서 C&C 서버의 명령을 받아 다운로드, 업로드, 등 봇넷의 역할을 수행함으로써 감염PC의 정보를 수집한다.

C&C 서버 주소

1. http://pressbrig.***.com
2. http://www.sc***pages.at
3. http://su***.5u.com
4. http://Wea***ine.hopto.org

C&C서버와의 통신에서는 HTTP, FTP 등 여러 프로토콜을 이용할 수 있도록 구성되어 있음을 확인했다. 더불어 서버 IP 차단 등을 우회하기 위한 것으로 보이는 프록시 모드가 존재한다.

C&C 서버에서 하달하는 명령은 다음과 같다.

1. 파일 다운로드
2. 파일 업로드
3. 파일 실행
4. 파일 삭제
5. 파일 검색
6. 스텔스 모드(지정된 기간동안 어떠한 인터넷 연결도 수행하지 않음)
7. 드라이버 업데이트

Part2.2월의 악성코드 이슈 분석

```
    if ( *(_DWORD *)dword_10073470 )
        OutLog(v6, 1, "UpLoad: Ftp upload %d file(s)", *(_DWORD *)dword_10073470);
    else
        OutLog(v6, 1, "UpLoad: no files to ftp upload");
    if ( !RegCreateKeyA(::hKey, (LPCSTR)&byte_10074E0C, &hKey) )
    {
        cbData = 1;
        RegQueryValueExA(hKey, "prot_test", 0, 0, &byte_10073918, &cbData);
        RegCloseKey(hKey);
    }
    sub_10018ECE((int)"&,&!08FgWt8&<;0!fg-{:6-;", 0, 1);
    v52 = *(_DWORD *)dword_10073470;
    for ( j = 0; j < dword_10068B60 && *(_DWORD *)dword_10073470; ++j )
    {
        if ( v7(*(LPCSTR *)&lpString[4 * j]) && *(_DWORD *)dword_10073470 )
            FTP_Upload(j);
    }
}
```

[그림 14] C&C 명령에 의해 FTP 프로토콜을 이용한 업로드 코드

```
MakeFile Error(%d) copy %s to %s
Module:0x%08X,Res:%d
Pgp Encrypt: error(%d) buffer size %d/%d
Pgp Encrypt: error(%d) get encrypt buffer size %d/%d
Pipe request exception
Run instruction: %d ID:%u%010u(%02d:%02d:%02d %02d/%02d/%04d)
Run cmd: %s
Run at start %s.
Run at start %s ... %d, error(%d).
Run [PID:%d]%s ... OK
Request completed OK
CommandsOnly Mode: %d
Days before goto PM %d
Enable proxy mode:%d, port:%d
Set Http Mode: %d
Set Max Upload File Size: %d(B)
Set PM MinDataSize: %d(B)
Set RegValue %sWW%d(%s) ... OK
Set Search custom proxy %d
Set Service Mode: %d, result %d
Set Smtip Address:%d
Set Use custom proxy:%d
Set browser owner:%d
```

[그림 15] 실행 과정 중 디버그 메시지

[그림 13]을 참고 하면 악성코드가 특정 행위 이후에 디버그 메시지를 출력하는 것을 쉽게 확인할 수 있다. [그림 15]은 이를 기반으로 문자열 기반으로 검색되어 디버그 메시지를 출력 하는 부분을 확인한 것이다. 해당 메시지와 메시지 출력 이전의 함수들을 확인하면 특정 기능을 동작 이후에 출력하고, 추가적으로 메시지를 수집하는 것을 확인할 수 있었다. (표에 남겨진 정보 이외에도 다수가 존재한다.)

.text:10001AB4 68 71 78 0D 0A+ db 'mMPG', 9, 'MPEG', 9, 'mpg', 0Dh, 0Ah
.text:10001AB4 4A 56 57 52 09+ db 'MSWD', 9, 'W8BN', 9, 'doc', 0Dh, 0Ah
.text:10001AB4 4A 50 45 47 09+ db 'MSWD', 9, 'W6BN', 9, 'doc', 0Dh, 0Ah
.text:10001AB4 6A 70 67 0D 0A+ db 'MSWD', 9, 'WDBN', 9, 'doc', 0Dh, 0Ah
.text:10001AB4 4A 56 57 52 09+ db 'MSWD', 9, 'WTBN', 9, 'dot', 0Dh, 0Ah
.text:10001AB4 47 49 46 66 09+ db 'MSWD', 9, 'TEXT', 9, 'txt', 0Dh, 0Ah
.text:10001AB4 67 69 66 0D 0A+ db 'MSWD', 9, 'RTF', 9, 'rtf', 0Dh, 0Ah
.text:10001AB4 53 49 54 21 09+ db 'MSWD', 9, '****', 9, 'doc', 0Dh, 0Ah
.text:10001AB4 42 49 4E 41 09+ db 'OTEX', 9, 'ODVI', 9, 'dvi', 0Dh, 0Ah
.text:10001AB4 7A 69 70 0D 0A+ db 'OTEX', 9, 'TEXT', 9, 'tex', 0Dh, 0Ah
.text:10001AB4 53 49 54 21 09+ db 'pgpM', 9, 'pgDS', 9, 'sig', 0Dh, 0Ah
.text:10001AB4 42 49 4E 41 09+ db 'pgpM', 9, 'pgEF', 9, 'pgp', 0Dh, 0Ah
.text:10001AB4 67 7A 0D 0A 53+ db 'pgpM', 9, 'pgSF', 9, 'pgp', 0Dh, 0Ah

[그림 16] 수집 되는 파일 확장자

[그림 16]은 수집되는 파일 확장자가 파일에 저장된 것을 확인한 내용이다. 확인된 파일 확장자의 개수는 대략 140개 정도이며, 해당 봇의 다운로드 및 업로드 기능 하위에서 해당 문자 셋을 참조하여 수집 명령이 C&C 서버에서 하달될 경우 파일을 수집하는 기능을 수행한다.

4. 결론

이번에 분석한 악성코드는 최소 7년전부터 제작되어 유포된 악성코드로 확인되었다. 주요 감염 원인은 악성코드에 포함된 기능인 ‘이동식 디스크 자동실행’과 ‘이메일’인 것으로 추정된다. 이는 기본적인 봇넷 역할을 수행함과 더불어 확장자 파일 검색(PDF, DOC, …)을 통해 군사 기밀 등 주요 정보를 습득하기 위한 것으로 보이는 ‘수집 기능’과 지정된 기간 동안 아무런 통신을 수행하지 않는 ‘잠복기능’을 포함한다. 따라서 치밀한 정보 탈취를 목적으로 하는 악성코드라고 할 수 있다.

5. 치료방안

기본적으로 해당 악성코드는 Interrupt Descriptor Table(이하 IDT) 의 Unexpected Interrupt 인 0x55(On85) 번에 인터럽트를 등록하고, NT 계열의 시스템 함수를 변조하여 등록된 인터럽트를 통하여 자신의 코드가 호출되는 기능을 가지고 있다. 따라서 악성코드 감지 자체가 어렵게 동작한다. 이는 널리 알려진 서드파티 AV 제품 등 기타 각종 보안 모듈 이외에는 실제 설치되는 경우가 드문 사례이다.

일반적으로 알려진 상용 AV 제품 이외에 위와 같은 행위를 할 경우에는 시스템상에 변조되어있는 메모리 영역을 복구하고, IDT에서 해당 번호를 삭제한 이후, 인터럽트가 발생할 경우 호출되는 IDT에 등록된 주소를 추적하여 해당 드라이버 제거 및 서비스를 종료한다.

Part3. 보안 이슈 돋보기

2월의 보안이슈

2월의 취약점

2월의 보안 이슈

알약이 뽑은 TOP 이슈

- 2016년부터 네트워크 장비도 보안인증

정부가 네트워크 장비에 대해서도 국제공통평가기준(CC)에 따른 보안인증을 적용할 예정이다. 지금까지 CC인증은 국가정보원 IT보안인증사무국에서 웹방화벽이나 침입방지시스템 같은 보안 제품을 대상으로만 제한적으로 해왔지만, 2016년 1월부터는 기지국 장비 등 네트워크 제품도 CC인증 대상이 된다.

- 31개국 주요 기관 노린 대형 악성코드 '마스크' 발견

미국, 영국, 독일, 프랑스, 중국, 중동 등 31개국 정부기관, 대사관, 에너지 회사 등을 노린 초대형 악성코드 '마스크'가 발견됐다. 이 악성코드는 과거에 발견된 스택스넷, 프레임 등과 마찬가지로 공격 규모나 수법 면에서 국가 차원에서 제작된 것으로 추정된다. 카스퍼스키랩 보고서에 따르면 이 악성코드는 지난 2007년부터 등장하기 시작하여, 올해 2월까지 31개국에서 사용하는 1천개 IP주소 중 380명을 공격한 것으로 조사됐다. 공격대상은 정부기관, 재외공관, 대사관, 에너지/석유/가스회사, 연구소, 사모펀드, 저명한 활동가 등이다. 특이한 점은 방문하면 바로 악성코드 감염이 이루어지도록 구성하는 대신 해당 웹사이트 내 특정 폴더를 통해 익스플로잇을 감염된 PC에 호스팅 하는데, 이런 방식은 전에 등장하지 않은 수법이다.

- ATM, POS용 임베디드 윈도XP, 보안 최대 5년 지원

오는 4월 8일 지원이 종료되는 윈도와 별개로 POS 단말기, ATM등에 특화된 윈도XP 임베디드 OS에 대한 핵심 보안 업데이트는 최대 5년까지 지원한다. PC용으로 쓰이는 윈도XP와 달리 윈도 XP 임베디드 OS의 경우, 출시 시기가 윈도 XP보다 늦은 만큼, 업데이트 지원종료 시점도 기존 윈도XP보다 늦다. 현재 윈도 XP 임베디드 제품은 총 5 종류이며, 각 제품마다 업데이트 지원 시점이 다르기 때문에, 지원종료시점은 각각 확인해야 한다. 이 기간 동안 오류 등을 수정한 핫픽스를 지원받기 위해서는 별도로 계약을 맺어야 한다.

- '미래부, SW업데이트 체계 보안 가이드라인 배포'

2월 19일, 미래창조과학부는 SW업데이트 취약점을 악용하여 악성코드가 확산되는 것을 예방하기 위해 SW업데이트 체계 보안 가이드라인 배포를 시작했다. SW업데이트 체계 보안 가이드라인은 SW개발 기업에서 자동 업데이트 기능 개발 시 준수해야 할 보안항목 및 주의사항을 따르지 않을 경우 발생할 수 있는 위험성, 해킹에 악용된 사례 및 문제 해결 방안을 제시한다.

- 인터넷뱅킹 사기 차단 위한 추가인증 도입

금융권이 오는 4월부터 메모리해킹 예방을 위하여 추가 인증을 도입하기로 했다. 이번에 구축되는 추가 인증 시스템은 은행이 메모리 해킹 시 이상 징후를 감지하면 곧바로 SMS나 ARS로 본인인지 여부를 추가로 확인하는 시스템이다. 한편, 지난해 연말에는 키보드 보안프로그램의 미비사항을 보완한 '확장E2E' 기능을 추가했다.

- 정부, 민간 사이버 전문가 300명 육성

정부가 잇따른 대형 보안사고를 방지하기 위해 사이버보안 전문가 300명으로 구성된 '사이버보안전문단'을 발족할 예정이다. 사이버보안전문단원은 평시에는 분과별로 분과장의 지시에 따라 정보보호 관련 기술세미나, 워크숍, 사이버 침해 위협 동향과 신규 위협 연구 등 관련 필요한 활동에 참여해야 한다. 침해사고 시, 민간인 이지만 침해사고 관계인의 사업장에 출입하는 권한을 부여 받아 사고 원인을 조사할 수도 있다.

2월의 취약점

Microsoft 2월 정기 보안 업데이트

- Internet Explorer 누적 보안 업데이트(2909921)

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건과 비공개로 보고된 취약점 23건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

- VBScript 스크립팅 엔진의 취약점으로 인한 원격 코드 실행 문제점(2928390)

이 보안 업데이트는 Microsoft Windows의 VBScript 스크립팅 엔진에서 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 사이트를 방문할 경우 원격 코드 실행이 허용될 수 있습니다. 공격자는 강제로 사용자가 웹 사이트를 방문하도록 할 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

- Direct2D의 취약점으로 인한 원격 코드 실행 문제점(2912390)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점은 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 공격자는 강제로 사용자가 특수하게 조작된 콘텐츠를 보도록 만들 수는 없습니다. 대신 공격자는 사용자가 공격자의 웹 사이트에 연결되는 전자 메일 메시지나 메신저 메시지에서 링크를 클릭하게 하거나 전자 메일을 통해 보낸 첨부 파일을 열도록 하는 등의 조치를 취하도록 유도해야 합니다.

- Exchange용 Microsoft Forefront Protection의 취약점으로 인한 원격 코드 실행 문제점(2927022)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Forefront의 취약점을 해결합니다. 특수하게 조작된 전자 메일 메시지가 스캔된 경우, 원격 코드 실행이 발생할 수 있습니다.

- Microsoft .NET Framework의 취약점으로 인한 권한 상승 문제점(2916607)

이 보안 업데이트는 Microsoft .NET Framework의 공개된 취약점 2건과 비공개적으로 보고된 취약점 1건을 해결합니다. 사용자가 특수하게 조작된 웹 사이트 또는 특수하게 조작된 웹 콘텐츠를 포함한 웹 사이트를 방문하는 경우 가장 위험한 취약점으로 인해 권한 상승이 발생할 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 공격에 노출된 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

- Microsoft XML Core Services의 취약점으로 인한 정보 유출 문제점(2916036)

이 보안 업데이트는 Microsoft Windows에 포함된 Microsoft XML Core Services의 공개된 취약점을 해결합니다. 이 취약점은 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 정보 유출을 허용할 수 있습니다. 공격자는 강제로 사용자가 특수하게 조작된 콘텐츠를 보도록 만들 수는 없습니다. 대신 공격자는 사용자가 공격자의 웹 사이트에 연결되는 전자 메일 메시지나 메신저 메시지에서 링크를 클릭하게 하거나 전자 메일을 통해 보낸 첨부 파일을 열도록 하는 등의 조치를 취하도록 유도해야 합니다.

- IPv6의 취약점으로 인한 서비스 거부 문제점(2904659)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 대량의 특수하게 조작된 IPv6 패킷을 영향을 받는 시스템으로 보낼 경우 서비스 거부가 발생할 수 있습니다. 이 취약점을 악용하려면 공격자의 시스템이 대상 시스템과 동일한 서브넷에 속해야 합니다.

Microsoft 보안 업데이트 해결법

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/ms14-feb>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/ms14-feb>

아래한글 임의코드 실행 취약점 보안 업데이트 권고

제품 : 한/글 2014, 한/셀 2014, 한/쇼 2014, 한/글 2010, 한/글 2007, 넥셀 2007, 슬라이드 2007, 한/글 2005, 한/글 2004, 한/글 2002, 한/셀 2010, 한/쇼 2010

- 상세정보

한글과컴퓨터社의 아래한글 등 오피스 프로그램에서 임의 코드실행이 가능한 취약점이 발견됨

공격자는 특수하게 조작한 웹페이지 방문 유도 또는 웹 게시물, 메일, 메신저의 링크 등을 통해 특수하게 조작된 문서를 열어보도록 유도하여 임의코드를 실행시킬 수 있음. 영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안 업데이트를 권고함

- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#16, 보안#17)으로 업데이트

다운로드 경로 : <http://www.hancom.co.kr/downLoad.downPU.do?mcd=001>

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

[참고사이트] <http://www.hancom.co.kr/downLoad.downPU.do?mcd=001>

Adobe Flash Player 신규 취약점 보안 업데이트 권고

제품 : Adobe Flash Player(윈도우즈 및 맥) 12.0.0.43 및 이전 버전

Adobe Flash Player(리눅스) 11.2.202.335 및 이전 버전

Adobe Flash Player(크롬) 12.0.0.41 및 이전 버전

Adobe Flash Player(윈도우즈8.0 버전의 인터넷 익스플로러10) 12.0.0.38 및 이전 버전

Adobe Flash Player(윈도우즈8.1 버전의 인터넷 익스플로러11) 12.0.0.38 및 이전 버전

- 상세정보

Adobe社는 Adobe Flash Player의 취약점 1개에 대한 보안 업데이트를 발표

임의코드 실행으로 이어질 수 있는 정수형 언더플로우 취약점 (CVE-2014-0497)

- 해결법

윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자

Adobe Flash Player Download Center(<http://get.adobe.com/flashplayer/>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

구글 크롬 브라우저 사용자

크롬 브라우저 자동 업데이트 적용

윈도우8.0 버전에서 동작하는 인터넷 익스플로러10 버전 사용자

윈도우8.1 버전에서 동작하는 인터넷 익스플로러11 버전 사용자

윈도우 자동 업데이트 적용

- 참고사이트

<http://helpx.adobe.com/security/products/flash-player/apsb14-04.html>

Adobe Flash Player 신규 취약점 보안 업데이트 권고 (2)

- 제품

Adobe Flash Player(윈도우즈 및 맥) 12.0.0.44 및 이전 버전

Adobe Flash Player(리눅스) 11.2.202.336 및 이전 버전

Adobe AIR(안드로이드) 4.0.0.1390 및 이전 버전

Adobe AIR SDK 3.9.0.1390 및 이전 버전

Adobe AIR SDK&Compiler 3.9.0.1390 및 이전 버전

Adobe社는 Adobe Flash Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표

공격자는 취약점을 이용하여 잠재적으로 시스템의 제어권한을 획득할 수 있음

- 상세정보

Adobe社는 Adobe Flash Player의 취약점 3개에 대한 보안 업데이트를 발표

임의코드 실행으로 이어질 수 있는 스택 오버플로우 취약점 (CVE-2014-0498)

ASLR을 우회할 수 있는 메모리 누출 취약점 (CVE-2014-0499)

임의코드 실행으로 이어질 수 있는 이중 해제 취약점 (CVE-2014-0502)

- 해결법

원도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자

Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

구글 크롬 브라우저 사용자

크롬 브라우저 자동 업데이트 적용

윈도우8.0 버전에서 동작하는 인터넷 익스플로러10 버전 사용자

윈도우8.1 버전에서 동작하는 인터넷 익스플로러11 버전 사용자

윈도우 자동 업데이트 적용

Adobe AIR SDK 사용자

<http://www.adobe.com/devnet/air/air-sdk-download.html>에 방문하여 Adobe AIR SDK 최신 버전을 설치

Adobe AIR SDK&Compiler 사용자

<http://www.adobe.com/devnet/air/air-sdk-download.html>에 방문하여 Adobe AIR SDK&Compiler 최신 버전을 설치

안드로이드 환경의 Adobe AIR 사용자

Adobe AIR가 설치된 안드로이드 폰에서 ‘구글 플레이 스토어’ 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트하거나 자동업데이트를 허용하여 업그레이드

- 참고사이트

<http://helpx.adobe.com/security/products/flash-player/apsb14-07.html>

Apache Tomcat 서비스 거부 취약점 보안 업데이트 권고

- 제품

Apache Tomcat 7.0.0 – 7.0.50 버전

Apache Tomcat 8.0.0-RC1 – 8.0.1 버전

- 상세정보

아파치 소프트웨어 재단은 Apache Tomcat에 영향을 주는 서비스 거부 취약점을 해결한 보안 업데이트를 발표

공격자는 HTTP 헤더를 특수하게 조작해 취약한 시스템에 요청할 경우, 서비스 거부를 유발시킬 수 있음. HTTP 헤더의 ‘Content-Type’ 항목 값을 변조해 서비스 거부를 일으킬 수 있는 취약점(CVE-2014-0050)

- 해결법

Apache Tomcat 7.x 버전 사용자

Apache Tomcat 버전을 7.0.51 버전으로 업그레이드

Apache Tomcat 7.x 버전 사용자

Apache Tomcat 버전을 8.0.2 버전으로 업그레이드

- 참고사이트

<http://tomcat.apache.org/security-7.html>

<http://tomcat.apache.org/security-8.html>

Adobe Shockwave Player 신규 취약점 보안 업데이트 권고

- 제품

Adobe Shockwave Player(윈도우즈 및 맥) 12.0.7.148 및 이전 버전

- 상세정보

Adobe社는 Adobe Shockwave Player의 취약점 2개에 대한 보안 업데이트를 발표

코드실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2014-0500, CVE-2014-0501)

- 해결법

원도우, 맥 환경의 Adobe Shockwave Player 사용자

Adobe Download Center(<http://get.adobe.com/shockwave/>)에 방문하여 최신 버전(12.0.9.149)을 설치하거나 자동 업데이트를 이용하여 업그레이드

- 참고사이트

<http://helpx.adobe.com/security/products/shockwave/apsb14-06.html>

MS Internet Explorer 원격코드 실행 신규 취약점 주의 권고

마이크로소프트(이하 MS)의 Internet Explorer에서 원격코드 실행이 가능한 신규 취약점이 발견됨

해당 취약점에 대한 보안 업데이트는 아직 발표되지 않았으나, 취약점을 악용한 공격 시도가 해외에서 확인되어 사용자의 주의가 특히 요구됨

- 상세정보

use-after-free 취약점을 이용한 원격코드 실행 취약점(CVE-2014-0322)

- 해결법

현재 해당 취약점에 대한 보안업데이트는 발표되지 않았음

MS의 보안 업데이트 발표 전까지 다른 인터넷 브라우저 사용을 권고 (취약점에 영향받지 않는 IE버전, Mozilla Firefox, Safari, Google Chrome, Opera 등)

Part3.보안 이슈 돋보기

MS의 보안 업데이트 발표 전까지 영향을 받는 Internet Explorer 버전을 사용할 경우 취약점에 의한 피해를 줄이기 위하여 다음과 같은 조치를 권장

- MS 홈페이지 “Fix it for me”섹션의 “Microsoft Fix it 51007”를 다운로드 후 설치
- 원상태로 복구하기 위해서는 “Microsoft Fix it 51008”을 적용
- 해당 Fix it은 보안 업데이트를 대체할 수는 없으며, 보안 업데이트 발표 시 반드시 보안 업데이트를 적용해야 함

취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수해야 함

- 신뢰되지 않는 웹 사이트의 방문 자제
- 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화
- 출처가 불분명한 이메일의 링크 클릭하거나 첨부파일 열어보기 자제

- 참고사이트

<http://technet.microsoft.com/en-us/security/advisory/2934088>

<http://support.microsoft.com/kb/2934088>

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

세계 최대 비트코인 거래소 Mt.Gox, “트랜잭션의 가변성” 문제로 비트코인 도난 당해

Alleged Bitcoin Theft on Mt.Gox; US Attorney, FBI Investigate Outage

비트코인 거래소인 마운트고스가 지난 7일 DDoS 공격으로 출금서비스를 중지한 이후 운영을 중지했다. 마운트고스는 수년간 이어진 트랜잭션 가변성 관련 절도로 744,408 비트코인을 도난 당했으며, 이로 인한 피해 금액은 약 5억 달러에 달한다. 트랜잭션의 가변성은 사용자가 디지털 서명을 이용하여 거래 시 사용하는 ID를 비트코인 네트워크가 확인하기 전에 변경할 수 있는 것으로, 서명을 경함으로써 같은 거래에서 두 개의 트랜잭션 ID를 생성할 수 있게 한다. 트랜잭션의 가변성 문제는 지난 2011년 한 차례 공개되었던 것으로, 마운트고스는 이에 따른 조치를 제대로 취하지 않았다는 비난을 피할 수 없을 것으로 보인다.

출처 : Hot for Security(<http://www.hotforsecurity.com/blog/alleged-bitcoin-theft-on-mt-gox-us-attorney-fbi-investigate-outage-8060.html>)

애플, iOS와 OS X에서 SSL/TLS 버그 발견

Apple and the SSL/TLS bug: Open questions

애플의 iOS와 OS X에서 SSL 버그가 발견되었다. 해당 버그는 iOS가 보안 접속 시 인증서 검증 절차에서 나타난 오류에 관한 것이다. 이는 iOS의 어느 부분에 위치한 인증서 검증 확인 절차가 일정 시간이 흐른 뒤에 알 수 없는 이유로 제거되는 것으로, 네트워크 권한을 획득한 공격자가 SSL/TLS로 보호된 세션의 데이터를 수집 및 수정할 수 있게 한다. SSL/TLS는 현재 가장 중요한 보안 프로토콜이기 때문에 애플의 이번 버그는 우선순위가 매우 높다고 할 수 있다. 이 인증서 검증 취약점은 OS X 10.9.1 버전에서도 발견되었지만, 이는 iOS와 동시에 업데이트 되지는 않았다.

출처 : ZDNet(<http://www.zdnet.com/apple-and-the-ssltls-bug-open-questions-7000026628>)

2. 중국

DEDECMS 보안 취약점 발견

2월 29일, 홈페이지 오픈소스 플랫폼인 DEDECMS에서 취약점이 발견됐다. 공격자들은 이 취약점을 이용하여 루트 권한을 획득할 수 있고, 사용자들의 각종 정보들을 탈취하거나 악성코드를 퍼트릴 수 있다. DEDECMS 툴은 중국 내에서 사용률이 매우 높다. 이번 취약점으로 인해 백만개가 넘는 홈페이지가 영향을 받을 것으로 예상된다.

DedeCMS는 PHP+MySQL기술을 결합하여 만든 플랫폼으로, 여러 환경의 서버를 지원한다. 2004년에 오픈된 이후 편리하고, 오픈소스 와의 뛰어난 호환성으로 CMS의 대부분의 시장을 점유했다. 현재 35만개가 넘는 홈페이지가 DedeCMS 또는 DedeCMS 핵심 기술로 제작되었으며, 설치율은 95만 번에 달한다. 현재 중국 내에서 가장 상용화 된 홈페이지 구축 프로그램일 뿐만 아니라, 해커들이 가장 관심을 갖는 대상이기도 하다.



이번에 발견된 취약점은 루트권한을 얻을 수 있다는 점 때문에 각종 악의적인 행위가 가능하여 2차 범죄가 일어날 수 있다.

출처 : <http://www.techweb.com.cn/news/2014-02-20/2009282.shtml>

중국 최대 SNS 메신저인 Wechat에서 취약점 발견

중국의 카카오톡인 Wechat에 취약점이 발견됐다. 이 취약점은 사용자들이 Wechat에서 공유한 동영상 URL이 노출되는 것으로, 다른 사용자들도 이 주소를 이용하여 영상을 볼 수 있다. 구글에서 site:wx.qq.com.video 검색 후 페이지에서 “생략된 결과 다시 표시”를 클릭하면 대량의 동영상이 나온다. 사용자는 이를 중에서 weixin.qq.com URL주소를 가진 동영상들을 쉽게 찾아볼 수 있다. 이러한 동영상들은 모두 사용자들이 Wechat에서 녹화한 것으로, 이것들이 검색결과에 잡히는 것이다. 사용자에게 이러한 취약점이 더욱 공포스럽게 다가오는 이유는 해당 동영상들이 사용자들의 일상생활을 촬영한 것들로, 민감한 동영상들도 매우 많기 때문이다.

Part4. 해외 보안 동향

이렇게 유출된 동영상들은 성인 사이트에 재 유포될 가능성이 매우 크다. Wechat은 6억 명이 이용하고 있으며, 최근 지불 기능이 포함되어, 각종 은행카드들과 연동이 되어 있다. 이렇게 풍부해지는 기능들은 보안사고가 자주 발생하는 이유가 되고 있다. 또한 트로이 목마, QR코드 악성코드 등이 Wechat 사용자들 사이에서 공공연하게 퍼지고 있다. 이번에 발견된 Wechat의 동영상 취약점은 해당 메신저의 보안이 얼마나 취약한지를 보여주고 있다.

출처 : <http://news.hsw.cn/system/2014/02/27/051867691.shtml>

3. 일본

※ 일본 보안 이슈는 내부 사정으로 인하여, 3월 한 달 간 쉽니다.
독자 여러분의 너른 양해 부탁 드립니다.

알약 3월 보안동향보고서

Contact us

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr