www.alyac.co.kr

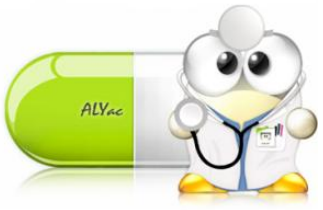
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part I 3월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2011년 3월 1일 ~ 2011년 3월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑2	S.SPY.Lineag-GLG	Spyware	59,577
2	New	Variant.Fosniw.6	Trojan	44,738
3	New	V.TRJ.Clicker.Winsoft	Trojan	40,295
4	↓2	V.DWN.86016	Trojan	39,236
5	↑8	V.DWN.Onlinegame.PA.Gen	Trojan	36,894
6	↑1	S.SPY.OnlineGames-H	Spyware	36,537
7	New	V.DWN.Enlog.417280	Trojan	34,868
8	↓4	Variant.FakeAlert.11	Trojan	30,730
9	↓1	Variant.Adware.Oso.1	Adware	27,363
10	New	Variant.Downloader.104	Trojan	23,087
11	New	A.ADV.BHO.IESearch	Adware	21,937
12	-	A.ADV.Clicki	Adware	21,377
13	New	Variant.Buzy.1797	Trojan	18,502
14	New	T.RHT.Hosts	Host	17,635
15	New	Trojan.Generic.5481775	Trojan	12,517

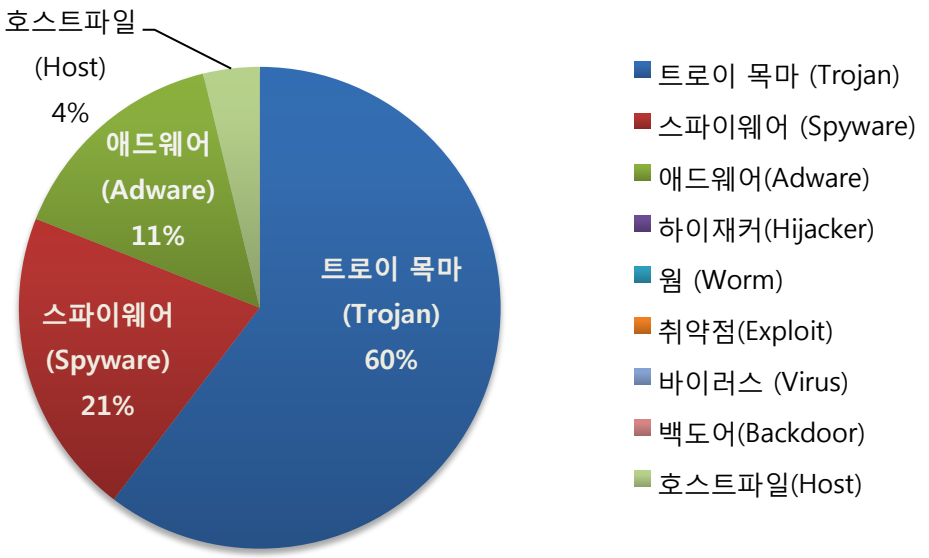
※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
3월의 감염 악성코드 TOP 15는 S.SPY.Lineag-GLG가 59,577건으로 TOP 15 중 1위를 차지하였으며, Variant.Fosniw.6이 44,738건으로 2위, V.TRJ.Clicker.Winsoft가 40,295건으로 3위를 차지하였다.
이 외에도 3월에 새로 Top 15에 진입한 악성코드는 총 8종이다.

3월의 최대 이슈는 3.4 디도스 공격이었다. 이번 공격은 지난 7.7 디도스 대란과 비교해 기술적으로 더욱 업그레이드된 공격이었다. 일부에서는 미미한 사건이었다고 평가하기도 하지만 이는 사실과 다르다.
보안업계에서 사전에 악성코드 배포처를 추적해 신속히 차단했고, 상황변화에 적절히 대응하였기 때문에 피해가 적었을 뿐이며, 3.4 DDos Agent가 TOP15에 오르지 않았던 이유도 이 때문인 것으로 판단된다. 현재 높은 순위를 차지한 게임 계정탈취 악성코드(S.SPY.Lineag-GLG, V.DWN.Onlinegame.PA.Gen, S.SPY.OnlineGames-H)는 3.4 디도스 공격 때문에 분주했던 보안업계의 상황을 악용해 이 기간 동안 다량 유포되었다.

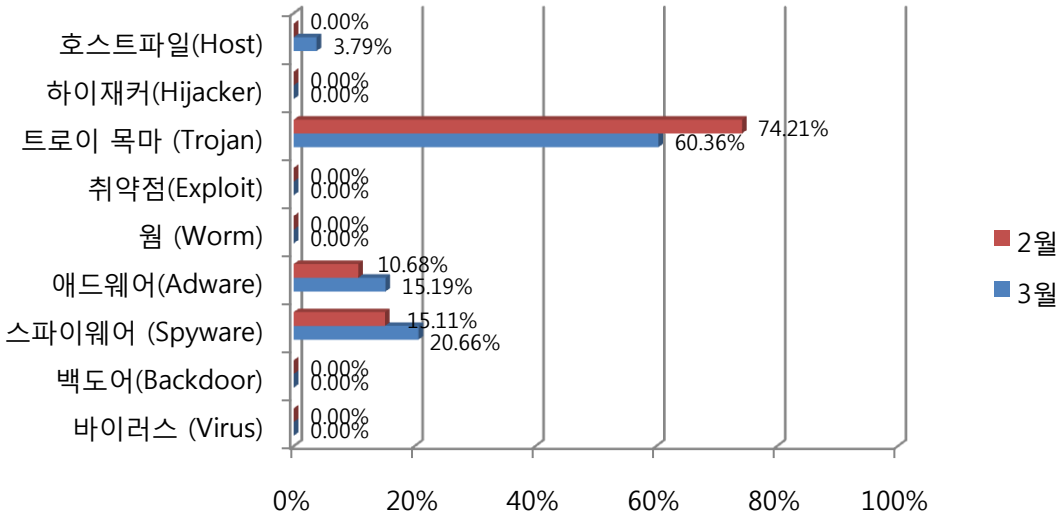
이처럼 3월에 큰 이슈가 되었던 두 악성코드의 주요 배포 경로가 파일공유 사이트로 드러나며, 파일공유 사이트의 보안관리 문제가 대두되고 있다.
하지만 대부분의 파일공유 사이트를 운영하는 업체들은 규모가 작기 때문에 보안투자에 신경을 못쓰고 있는 실정이며, 모니터링 등 적극적인 대응이 부족해 반복되는 해킹피해를 입으며 악성코드의 유포에 이용되고 있다.
이 같은 피해를 막기 위해서는 인터넷 이용 시 각종 서비스 사업자가 신뢰할 만한 업체인지 이용자 스스로 체크하는 노력이 필요하며, 웹 사이트 상단에 표시되는 `Active X'도 무조건 설치하지 말고 표시되는 정보를 꼼꼼히 읽어본 후 사용자 스스로의 필요에 의해 설치해야 한다.
확인할 수 없는 각종 보안 위협에 대한 최후의 방어선으로서 언제나 백신을 설치해 두어야 하며 낯선 인터넷 컨텐츠에 대해서는 혹시 악성 컨텐츠가 아닌지 이용 전에 먼저 의심해보는 습관도 매우 중요하다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 60%로 가장 많은 비율을 차지하고, 스파이웨어(Spyware)가 21%, 애드웨어(Adware)가 11%의 비율을 각각 차지하고 있다.

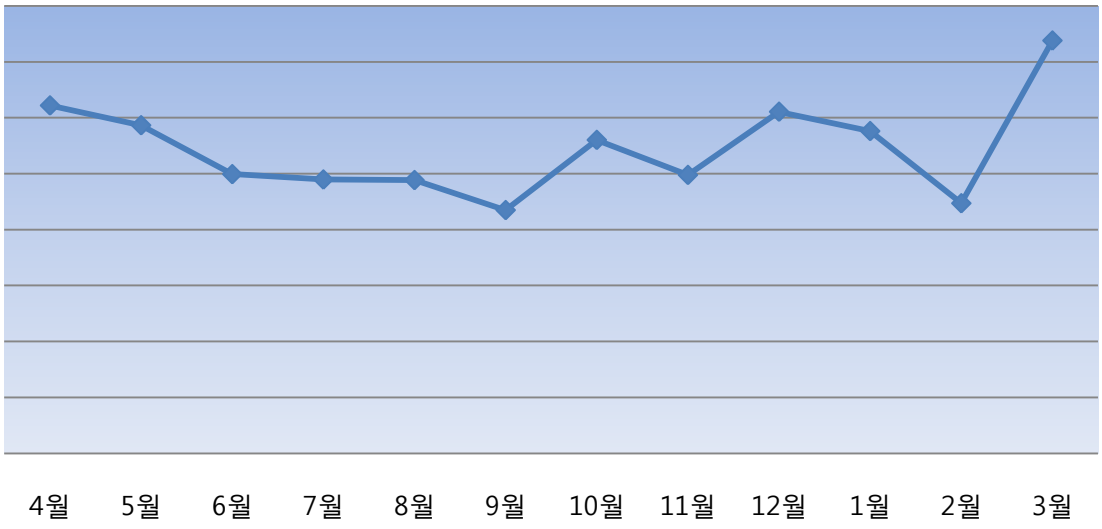
(3) 카테고리별 악성코드 비율 전월 비교



악성코드 유형별 비율을 전월과 비교한 그래프이다. 3월의 특이사항은 항상 강세였던 트로이목마(Trojan)가 전달에 비해 약 14% 감소하였다. 반면 애드웨어(Adware), 스파이웨어(Spyware)가 약 5%씩 증가하였으며, 호스트파일이 3.79% 차지하여 악성코드 Top 15가 다양한 카테고리에 분포되었다.

(4) 월별 피해 신고 추이

[2010년 04월 ~ 2011년 03월]

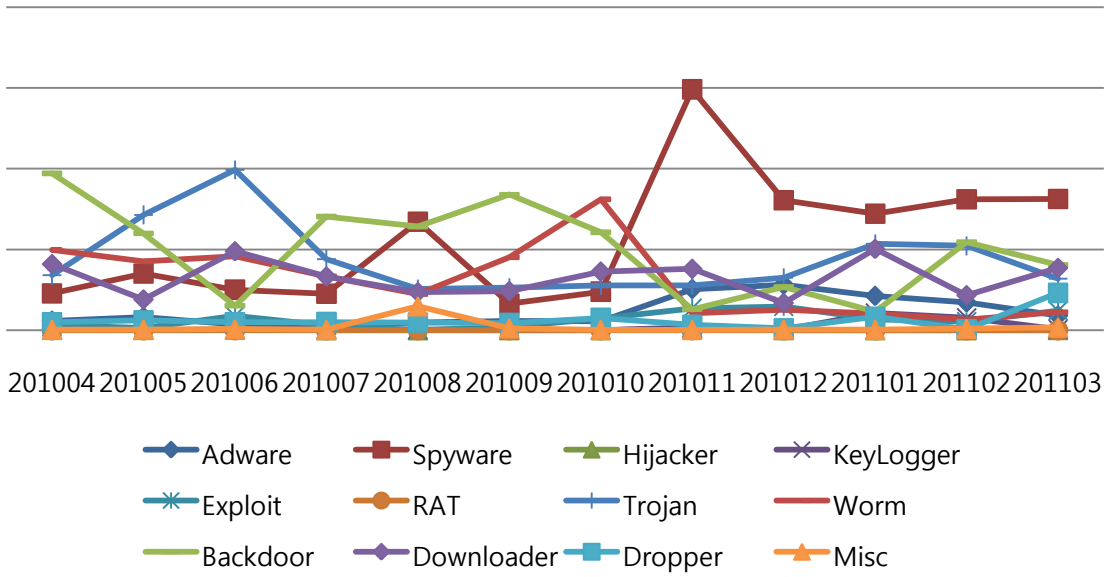


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 월의 피해 신고추이는 전월에 비해 대폭 증가하였다. 3.4 디도스 대란으로 사용자의 문의 및 피해 신고가 급증했기 때문이다.

(5) 월별 악성코드 DB 등록 추이

[2010년 04월 ~ 2011년 03월]



DB 등록추이는 변종이 많이 발생되는 순위라고도 할 수 있다. 3월은 3.4 디도스 사건으로 보안업계가 분주했던 틈을 타 활개를 친 '게임계정 해킹 악성코드'의 변종이 증가, 해당 카테고리가 전월보다 소폭 상승한 것을 확인할 수 있었다.

Part I 3월의 악성코드 통계

2. 악성코드 이슈 분석 – "설치된 프로그램에 따라 생성파일이 변경되는 악성코드"

(1) 개요

지금까지 발견된 악성파일들은 제작자에 의해 생성되는 파일명이 대부분 고정되어 있었다. 파일명을 난수로 표기하는 경우는 많이 있었지만, 사용자PC 환경에 따라 생성파일을 다르게 만드는 악성파일은 이번이 처음이라 어떤 비교를 통해 다른 파일을 생성하는지 살펴본다.

(2) 악성코드 분석

① 조건에 따른 파일생성

여러 파일을 분석 한 결과 현재까지 총 3개의 패턴을 가지고 있는 것으로 확인되었다.

첫번째, 섹션을 추가하여 정상파일 패치
두번째, 익스포트 포워딩을 이용하는 정상파일 로드
세번째, 특정 프로그램의 실행여부에 따른 파일 생성

위의 3개의 패턴은 모두 윈도우 정상파일인 imm32.dll을 대상으로 이루어지며, imm32.dll은 윈도우 보호파일 중 하나이기 때문에 공통적으로 WFP 해제가 이루어진다. 이전 방법과 마찬가지로 Sfc_os.dll의 Ordinal 5에 존재하는 unnamed API(SfcFileException)를 이용하여 보호모드를 해제시킨다.

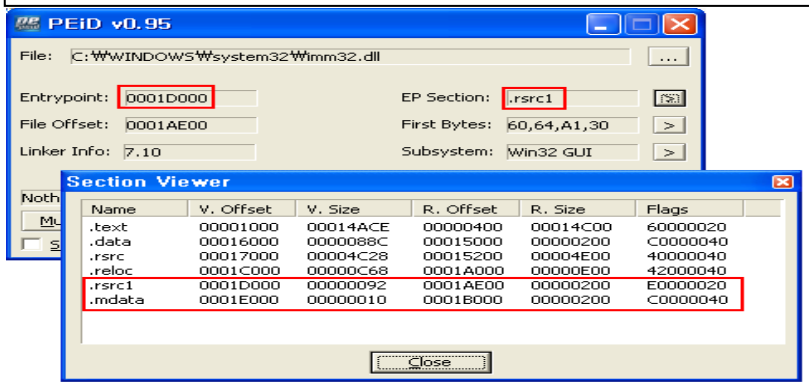
Ordinal 5:
DWORD WINAPI **SfcFileException**(DWORD **dwUnknown0**, PWCHAR **pwszFile**, DWORD **dwUnknown1**);

dwUnknown0	Unknown. Set to 0
pwszFile	Filename

② 섹션을 추가하여 정상파일 패치

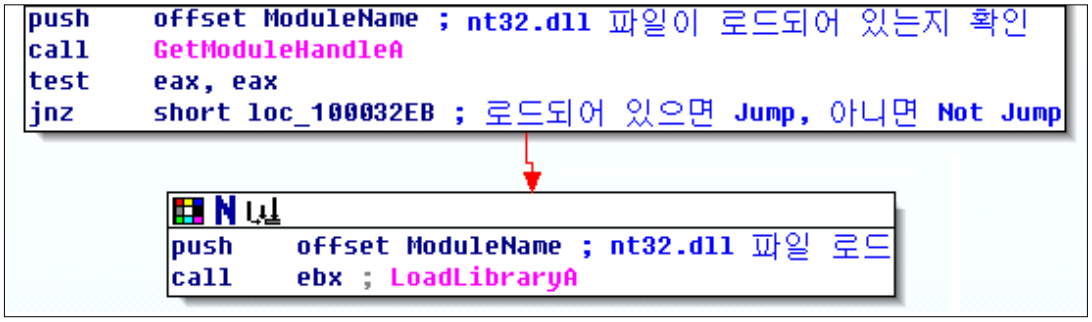
가장 초반에 나왔던 방법으로 WFP해제 이후에 정상파일에 섹션명을 추가하는 방식이다.

".ss32", ".s32", ".sy32", ".rs64", ".rscpm", ".vmpzmp", ".vsprt", ".cartp", ".rsrc1", ".mdata"



(그림. 정상 Imm32.dll 파일에 섹션이 추가 된 화면)

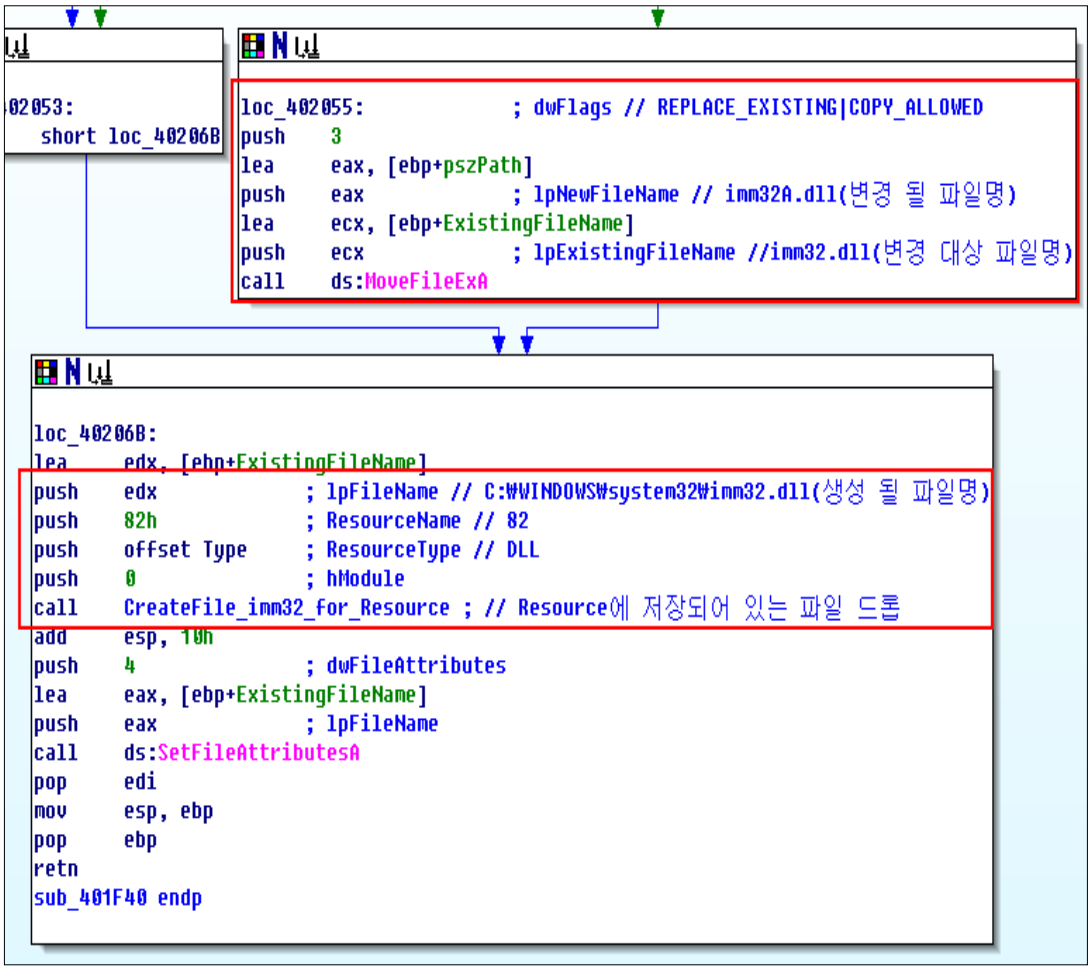
패치 된 정상파일에 추가 된 섹션들은 EP(Entrypoint)를 수정하여 악성파일인 "ole.dll", "kb.dll", "nt32.dll" 파일 등의 스파이웨어 악성파일을 로드하는 역할을 한다.



(그림. 섹션에 추가 된 코드가 악성파일을 로드시키는 코드화면)

③ 익스포트 포워딩을 이용하여 정상파일 로드

이 방법은 WFP해제 이후 정상파일을 다른 이름으로 변경하고, 드롭파일이 가지고 있는 DLL형식의 파일을 imm32.dll 파일로 생성하여 다른 이름으로 변경 된 정상파일의 익스포트 함수를 포워딩하여 사용하는 방법이다.



(그림. 정상파일 imm32.dll을 imm32A.dll로 수정하고 리소스에서 imm32.dll 파일을 만드는 코드화면)

이렇게 드롭된 imm32.dll은 자체가 악성파일로 생성된다. 그럼 일반 프로그램이 정상적인 imm32.dll 파일을 로드 시 문제가 되지 않는가? 라는 의문이 들게 된다.
악성파일 제작자는 이 문제를 Export Forwarding 방법으로 해결하였다.

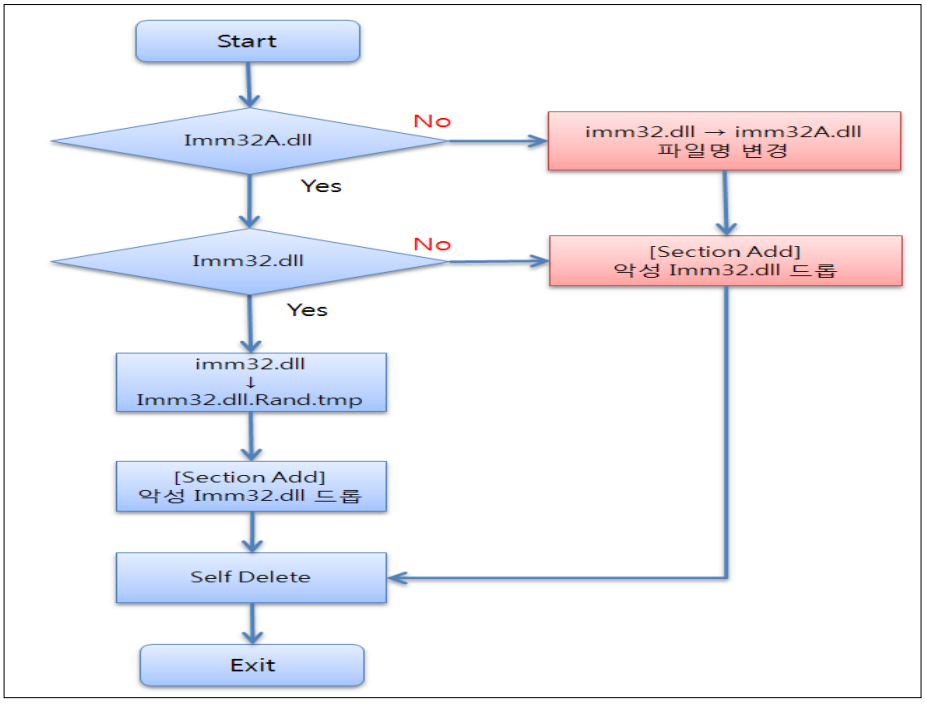
00009B48	0000A094	Forwarded Name RVA	0001	CtfAImmActivate -> imm32A.CtfAImmActivate
00009B4C	0000A0BD	Forwarded Name RVA	0002	CtfAImmDeactivate -> imm32A.CtfAImmDeactivate
00009B50	0000A0E3	Forwarded Name RVA	0003	CtfAImmIsIME -> imm32A.CtfAImmIsIME
00009B54	0000A10C	Forwarded Name RVA	0004	CtfImmCoUninitialize -> imm32A.CtfImmCoUninitialize
00009B58	0000A144	Forwarded Name RVA	0005	CtfImmDispatchDefImeMessage -> imm32A.CtfImmDispatchDefImeMessage
00009B5C	0000A186	Forwarded Name RVA	0006	CtfImmEnterCoInitCountSkipMode -> imm32A.CtfImmEnterCoInitCountSkipMode
00009B60	0000A1C2	Forwarded Name RVA	0007	CtfImmGenerateMessage -> imm32A.CtfImmGenerateMessage
00009B64	0000A1F1	Forwarded Name RVA	0008	CtfImmGetGuidAtom -> imm32A.CtfImmGetGuidAtom
00009B68	0000A21F	Forwarded Name RVA	0009	CtfImmHideToolbarWnd -> imm32A.CtfImmHideToolbarWnd
00009B6C	0000A251	Forwarded Name RVA	000A	CtfImmIsCiceroEnabled -> imm32A.CtfImmIsCiceroEnabled
00009B70	0000A28C	Forwarded Name RVA	000B	CtfImmIsCiceroStartedInThread -> imm32A.CtfImmIsCiceroStartedInThread
00009B74	0000A2C7	Forwarded Name RVA	000C	CtfImmIsGuidMapEnable -> imm32A.CtfImmIsGuidMapEnable
00009B78	0000A305	Forwarded Name RVA	000D	CtfImmIsTextFrameServiceDisabled -> imm32A.CtfImmIsTextFrameServiceDisable
00009B7C	0000A349	Forwarded Name RVA	000E	CtfImmLastEnabledWndDestroy -> imm32A.CtfImmLastEnabledWndDestroy
00009B80	0000A38B	Forwarded Name RVA	000F	CtfImmLeaveCoInitCountSkipMode -> imm32A.CtfImmLeaveCoInitCountSkipMode
00009B84	0000A3C9	Forwarded Name RVA	0010	CtfImmRestoreToolbarWnd -> imm32A.CtfImmRestoreToolbarWnd
00009B88	0000A400	Forwarded Name RVA	0011	CtfImmSetAppCompatFlags -> imm32A.CtfImmSetAppCompatFlags
00009B8C	0000A43C	Forwarded Name RVA	0012	CtfImmSetCiceroStartInThread -> imm32A.CtfImmSetCiceroStartInThread
00009B90	0000A472	Forwarded Name RVA	0013	CtfImmTIMActivate -> imm32A.CtfImmTIMActivate
00009B94	0000A49F	Forwarded Name RVA	0014	GetKeyboardLayoutCP -> imm32A.GetKeyboardLayoutCP
00009B98	0000A4CC	Forwarded Name RVA	0015	ImmActivateLayout -> imm32A.ImmActivateLayout
00009B9C	0000A4F9	Forwarded Name RVA	0016	ImmAssociateContext -> imm32A.ImmAssociateContext
00009BA0	0000A52A	Forwarded Name RVA	0017	ImmAssociateContextEx -> imm32A.ImmAssociateContextEx
00009BA4	0000A55C	Forwarded Name RVA	0018	ImmCallImeConsoleIME -> imm32A.ImmCallImeConsoleIME
00009BA8	0000A589	Forwarded Name RVA	0019	ImmConfigureIMEA -> imm32A.ImmConfigureIMEA
00009BAC	0000A5B2	Forwarded Name RVA	001A	ImmConfigureIMEW -> imm32A.ImmConfigureIMEW
00009BB0	0000A5DB	Forwarded Name RVA	001B	ImmCreateContext -> imm32A.ImmCreateContext

(그림. 악성 imm32.dll이 함수를 호출하기 위해 imm32A.dll을 포워딩 시키는 화면)

위의 사진은 악성파일에서 드롭된 imm32.dll 파일의 EAT(Export Address Table)의 구조이다.
화면에서 보이듯이 "CtfAImmActivate -> imm32A.CtfAImmActivate"를 imm32A.dll 파일의 함수를 사용하도록 설계되어 있다.
따라서 imm32A.dll이 존재하는 일반 프로그램 동작과는 전혀 문제가 되지 않는다.
**EAT: 라이브러리 파일에서 제공하는 함수를 다른 프로그램에서 가져다 사용할 수 있도록 해주는 매커니즘*

④ 특정 프로그램의 실행여부에 따른 파일 생성
이번 방법은 특정 프로그램(V3제품)의 프로세스 실행 여부에 따른 파일생성이 변경되는 방식으로 가장 최근에 발견되었다.
이 방법에서는 ②, ③에 사용 되었던 방법이 모두 활용된다.

1) V3 프로그램이 실행되지 않았을 경우
V3ClnSrv.exe, V3Svc.exe, V3LSvc.exe, V3LTray.exe 의 프로세스가 있는지 확인 후 프로세스가 없으면, 다음과 같은 순서로 악성파일이 동작한다.



(그림. 섹션이 추가되는 imm32.dll 생성 순서도 화면)

2) V3 프로그램이 실행되었을 경우

V3ClnSrv.exe, V3Svc.exe, V3LSvc.exe, V3LTray.exe 의 프로세스가 있는 지 확인 후 프로세스가 확인되면, 스레드를 생성하여 V3LSvc.exe 프로세스에서 ntdll.dll을 Unload 시킨다. (ntdll.dll을 Unload 시키면 V3LSvc.exe 프로세스가 종료된다. 현재는 V3제품에서 업데이트를 한 것으로 보여짐. V3LSvc.exe 파일은 V3 Lite Service 서비스 항목으로 등록된 V3 365 Clinic Service Application 파일로 실시간 검사, 업데이트 등의 기능을 담당한다.) 악성파일이 ntdll.dll을 Unload 시킨 방법은 다음과 같다.

LoadLibraryA(Ntdll.dll)
↓
OpenProcessToken(SeDebugPrivilege)
↓
memset & Mescat
↓
OpenProcess
↓
CreateToolhelp32Snapshot(TH32CS_SNAPMODULE)
↓
Module32First & Module32Next
↓
ntdll_ZwUnmapViewOfSection
↓
CloseHandle

Ntdll.dll을 Unload 시킨 후 위와 같은 순서로 악성파일이 동작한다.

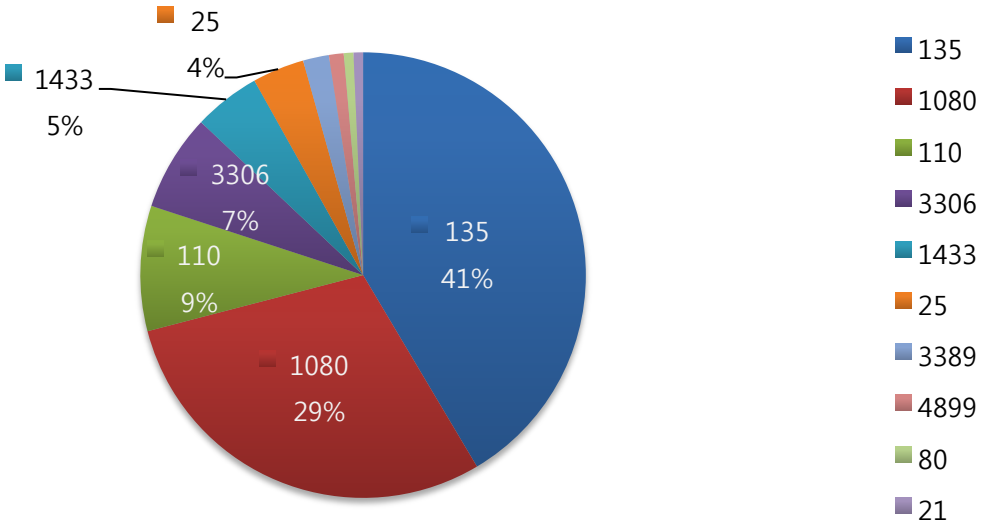
(3) 결론

윈도우 시스템 파일을 패치하는 악성파일들은 현재도 많이 존재하고 있지만, 보안제품의 실행 여부에 따라 설치되는 파일이 다른 경우에는 간단한 동적 분석만으로 정확한 파일을 확인하기 어렵다. 앞으로 분석 시에 시스템파일을 패치시키는 경우나, 보안제품의 KillAV기능이 있는 경우에는 정적으로 살펴 볼 필요성이 있다.

Part I 3월의 악성코드 통계

3. 허니팟/트래픽 분석

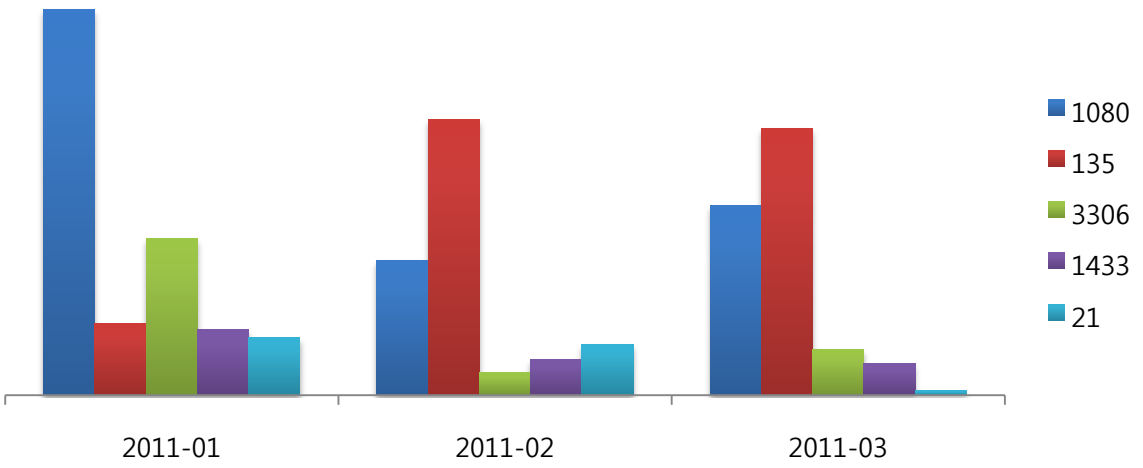
(1) 상위 Top 10 포트



자동화된 공격 툴이나 악성코드에서는 아직 특별한 포트를 악용하는 악성코드가 발견되지 않았다. 하지만 매번 타겟이 되는 포트는 보안 패치를 하지 않으면 항시 위협이 존재하므로 자신의 PC에 설치된 OS부터 일반 프로그램까지 보안패치가 배포되면 즉시 설치하는 것이 좋다.

(2) 상위 Top 5 포트 월별 추이

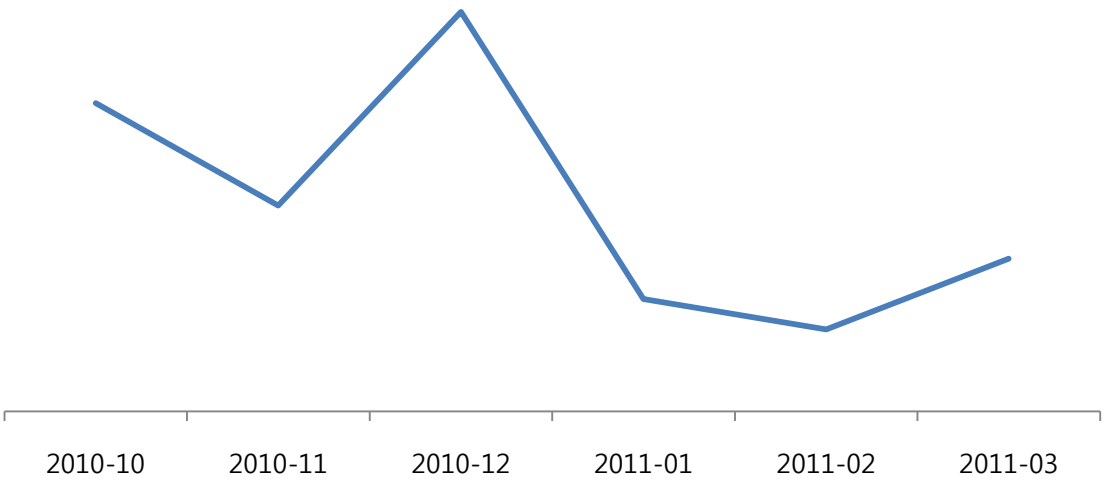
[2010년 01월 ~ 2011년 03월]



지난달에 비해 1080포트에 대한 연결시도가 증가하고 SQL서버의 권한 탈취를 위해 사전 대입 방법을 사용하는 공격 트래픽이 증가 했다. 일반 사용자는 반드시 백신을 설치하여 실시간 감시를 켜고, 되도록 방화벽을 사용해야 한다. 네트워크 관리자는 사용하는 서버의 비밀번호를 강력하게 관리하고 불필요하게 오픈된 포트는 없는지에 대해 항상 관심을 가져야 한다.

(3) 악성 트래픽 유입 추이

[2010년 10월 ~ 2011년 03월]

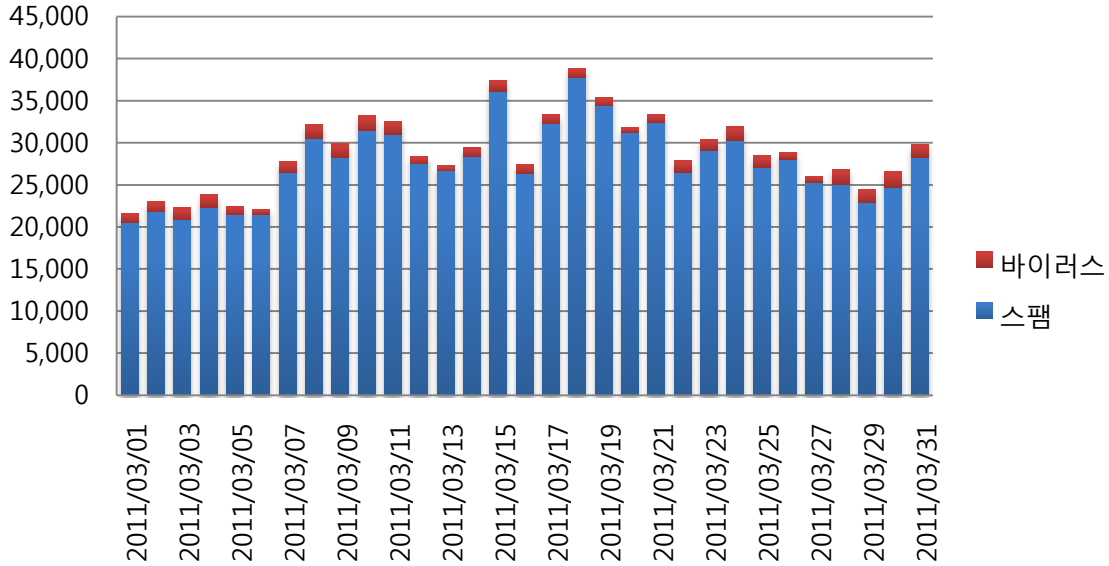


우려했던 만우절은 다행이 특별한 악성코드의 이슈가 없이 지나갔지만 최근 우리 삶에 이슈가 되는 사건, 사고를 주제로 하거나 택배 안내로 위장한 악성코드를 이메일의 첨부파일로 보내는 등, 사회공학적인 방법을 이용해 확산되는 악성코드가 계속 늘고 있다. 이런 경우 자신도 모르게 악성코드에 감염되는 사례가 많으며 악성코드 제작자도 이런 방법을 더 많이 사용할 것으로 예상되니 사용자 스스로가 PC보안에 관심을 가지고 주의를 기울여야 한다.

Part I 3월의 악성코드 통계

4. 스팸 메일 분석

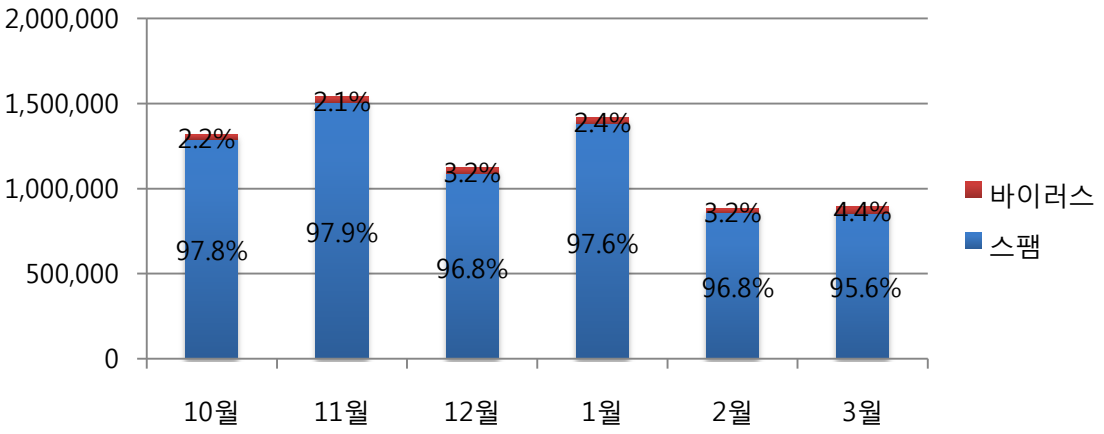
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 허니넷을 통해 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프이다. 3월에는 온라인 사기꾼 '스캐머'들이 일본 대지진을 이용해 신용사기 범죄를 저질렀다. 온라인 스캐머들은 사용자들에게 직접 영향을 미치는 이메일 형식과 피싱 그리고 악성코드가 포함된 웹사이트를 첨부 링크하는 형태를 이용하여 사용자 신용카드 정보를 요청하도록 하였다. 이메일, 피싱 등은 대부분 가짜 자선단체 형태로 위장해 전달되고 있으며, PC 사용자들의 감성을 자극해 가짜 기부웹사이트 등으로 이동하도록 유도하고 있다. 이처럼 PC 사용자들은 일본 대지진과 쓰나미에 대한 내용의 이메일을 더욱 주의 해야 한다. 피해를 막기 위해선 의심되는 이메일을 절대 열어보지 말고 의심되는 이메일 안에 포함된 URL링크 또한 클릭하지 말아야 한다.

(2) 월별 통계 현황

[2010년 10월 ~ 2011년 03월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다. 1월의 스팸 메일은 95.6%, 바이러스 메일은 4.4%를 차지하였다. 2월에 비해 서는 바이러스 메일 비율이 약 1% 증가 하였으며, 전체적인 메일 수신량은 전 월과 비슷하였다.

(3) 스팸 메일 내의 악성코드 현황

[2011년 3월 1일 ~ 2011년 3월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	13,590	34.91 %
2	W32/MyDoom-H	4,803	12.34 %
3	Mal/ZipMal-B	4,559	11.71 %
4	Mal/BredoZp-B	3,009	7.73 %
5	W32/Virut-T	2,498	6.42 %
6	W32/Bagz-D	1,671	4.29 %
7	W32/Lovgate-V	1,391	3.57 %
8	W32/MyDoom-Gen	1,096	2.82 %
9	Mal/EncPk-F	452	1.16 %
10	W32/Bagle-CF	422	1.08 %

스팸 메일 내의 악성코드 현황은 1월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Mytob-C 이 34.91 %로 1위를 차지하였다. 2위는 12.34 %를 차지한 32/MyDoom-H, 3위는 11.71 %를 차지한 Mal/ZipMal-B이다.

Part II 보안 이슈 돋보기

1. 3월의 보안 이슈

3월에는 지난 2009년 발생했던 7.7 DDOS 사건과 유사하게 전개된 대규모 DDOS 공격이 발생하여 전국을 또 한번 깜짝 놀라게 하였지만 규모에 비해 큰 피해 없이 마무리 되었습니다.

또 안드로이드 운영체제에서 동작하는 새로운 악성코드가 발견되었다는 소식이 많이 발표되었습니다. 한편, KISA는 안드로이드 마켓에서 앱들을 자동으로 다운로드 해 분석, 탐지, 경고를 실행하는 시스템을 개발키로 했다고 발표했으며 이로 인해, 모바일 보안에 대한 정부의 관심도 높아지고 있음을 알 수 있었습니다.

• 3월 4일 대규모 DDOS 공격 발생

이번 3.4 DDOS 공격은 국내 주요 웹사이트 및 정부기관을 표적으로 하며, 악성코드에 내장된 스케줄에 의해 공격이 진행되었다는 점 등이 지난 7.7 DDOS 사건과 비슷하였지만 공격자가 하드디스크를 파괴하는 명령을 원격에서 전송하며 자신의 흔적을 감추는 등 한층 향상된 공격기법들이 동원되었습니다.

다행히 정부 및 보안업체들의 공조가 잘 이루어져 공격규모에 비해 피해가 극히 적었으며, 지난 2009년과 비교해 안정된 대응이 이루어졌다는 평가들이 많았습니다.

• 구글 안드로이드마켓, 해적판 악성어플리케이션 삭제

안드로이드 마켓에서 21개의 악성어플리케이션이 발견되어 구글이 이들 명단을 공개하고 마켓에서 삭제조치 하였습니다. 이 앱들은 시스템의 루트 권한을 획득하거나 개인정보를 수집하는 것으로 알려졌으며 유명 게임과 유틸리티들의 해적판이어서 5만명이 넘는 사용자들이 별다른 의심 없이 다운로드 했다고 합니다.

• 개인정보보호법

3월 11일 개인정보보호법안이 국회 본회의를 최종 통과했습니다.

그 동안 여러 대체법이 있음에도 불구하고 개인정보보호법의 필요성이 끊임없이 제기되어왔으며 발의된지 3년만에 결국 본회의를 통과, 오는 9월 30일 부터 시행이 됩니다.

개인정보의 수집, 이용, 제공, 파기등 개인정보 관리의 전반에 걸쳐 구체적인 보호기준을 규정함으로서 개인정보보호법이 그 동안 다른 개별법이 보호하지 못했던 개인정보 보호의 사각지대를 크게 해소해줄 것으로 기대됩니다.

• 스팸메일 발송하는 러스톡 봇넷의 컨트롤 서버 차단

3월 16일, 마이크로소프트의 디지털 범죄 단속팀과 미국연방보안관은 법원의 영장을 받아 스팸메일 발송을 컨트롤하는 러스톡 봇넷서버들이 있는 IDC들을 급습하여 디스크를 압수하고 스팸발송을 차단시켰습니다.

스팸은 가장 확실한 범죄수익모델 중 하나이기 때문에로 앞으로 또 다른 스팸봇들이 활동할 것으로 예상되지만, 이번 단속을 통해 당분간은 전세계적으로 스팸메일 발송이 주춤할 것으로 보입니다.

그러나 이스트소프트 허니넷을 통해 감지된 국내 스팸메일의 양은 단속 전 보다 오히려 소폭 상승했습니다. 이번 러스톡 스팸봇 단속이 한국에는 별다른 영향을 미치지 못한 것으로 보입니다.

<출처: 마이크로소프트 / 압수된 스팸봇 서버의 하드디스크>

• EBS 디도스 공격 혐의자는 고3 수험생

EBS 수능강의 사이트 EBSi가 20일부터 21일까지 수 차례 디도스공격을 받아 서비스 장애를 일으켰습니다. 혐의를 받고 입건 된 범인은 고3 수험생인 김 모 군으로 밝혀졌으며 인터넷 카페를 통해 DDOS Agent, 일명 '좀비프로그램'을 유포해 PC 1,400대를 감염시켜 공격에 이용했습니다. 김군은 선생님께 꾸중을 듣고 학교 홈페이지를 해킹했다가 성공하자 호기심에 EBS 사이트의 공격을 시도했다고 합니다. 고3 학생이 큰 노력도 없이 호기심에 시도한 공격으로 인해 EBS 사이트가 다운되자 이번 사건을 계기로 느슨한 보안의식을 뒤돌아보아야 한다는 목소리가 높았습니다.

• 가짜 SSL 인증서 발급

SSL 인증서를 발급하는 인증기관인 코모도는 23일 성명서를 통해 자사의 인증으로 G-Mail, 스카이프 등 6개 도메인의 가짜 SSL인증서가 발급된 사실을 인정했습니다.

안전한 인증수단으로 인식되어왔던 SSL 인증서도 해킹에 의해 가짜로 발급될 수 있다는 것을 일깨워주는 사건이었습니다. 피해 웹도메인들은 발급된 허위 SSL 인증서를 차단하기 위해 긴급패치에 들어간 것으로 알려졌습니다.

Part Ⅱ 3 월의 이슈 돋보기

2. 3월의 취약점 이슈

• Microsoft 3월 정기 보안 업데이트

Windows Media의 취약점으로 인한 원격 코드 실행 문제, 원격 데스크톱 클라이언트의 취약점으로 인한 원격 코드 실행 문제, Microsoft Groove의 취약점으로 인한 원격 코드 실행 문제를 해결한 Microsoft 3월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows Server 2003**
- **Windows Server 2008**
- **Microsoft Groove 2007 (MS11-016)**

<취약점 목록>

Windows Media의 취약점으로 인한 원격 코드 실행 문제점(2510030)

이 보안 업데이트는 DirectShow의 공개된 취약점 1건과 Windows Media Player 및 Windows Media Center의 비공개적으로 보고된 취약점 1건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 특수하게 조작된 Microsoft Digital Video Recording(.dvr-ms) 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 공격에 성공하려면 사용자가 파일을 열도록 유도해야 하는데 이 보안 업데이트를 설치하면 모든 경우에 사용자가 파일을 열 수 없게 됩니다.

원격 데스크톱 클라이언트의 취약점으로 인한 원격 코드 실행 문제점(2508062)

이 보안 업데이트는 Windows 원격 데스크톱 클라이언트의 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 폴더에 있는 합법적인 원격 데스크톱 구성(.rdp) 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문하거나 이러한 위치에서 취약한 응용 프로그램이 로드되는 문서를 열어야 합니다.

Microsoft Groove의 취약점으로 인한 원격 코드 실행 문제점(2494047)

이 보안 업데이트는 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 디렉터리에 있는 합법적인 Groove 관련 파일을 열 경우 원격 코드 실행이 허용될 수 있는 Microsoft Groove의 공개된 취약점 1건을 해결합니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : http://www.microsoft.com/korea/technet/security/Bulletin/ms11-mar.mspx

영문 : http://www.microsoft.com/technet/security/Bulletin/ms11-mar.mspx

• Adobe Flash Player/Reader/Acrobat 신규 취약점 보안 업데이트 권고

CVE Number : CVE-2011-0609

Adobe Flash Player 및 Adobe Acrobat/Reader 프로그램에서 악성코드 감염 등에 악용될 수 있는 원격코드를 실행하는 신규 취약점을 해결한 보안 업데이트가 발표되었습니다. 공격자는 웹 페이지 은닉, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 Flash파일이 삽입된 엑셀 파일을 사용자가 열어보도록 유도하여 악성코드를 유포할 수 있으므로 주의가 필요하며 낮은 버전의 Flash Player 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

<해당 제품>

- Adobe Flash Player 10.2.152.33 및 이전 버전
- 크롬 웹브라우저에서 사용하는 Adobe Flash Player 10.2.154.18 및 이전 버전
- 안드로이드 환경에서 동작하는 Adobe Flash Player 10.1.106.16 및 이전 버전
- Adobe AIR 2.5.1 및 이전 버전
- Adobe Reader/AcrobatX (10.0.1), 10.x, 9.x 및 이전 버전

<임시 해결책>

Adobe Flash Player Download Center에서 Adobe Flash Player 최신 버전을 설치하거나 자동 업데이트를 이용하여 최신버전으로 업그레이드 하시기 바랍니다.

http://get.adobe.com/kr/flashplayer

http://get.adobe.com/kr/air/

http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-05.html

http://www.adobe.com/support/security/bulletins/apsb11-06.html

Contact us…

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

http://www.altools.co.kr/Event/nowornever_event/event.htm