www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 2월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

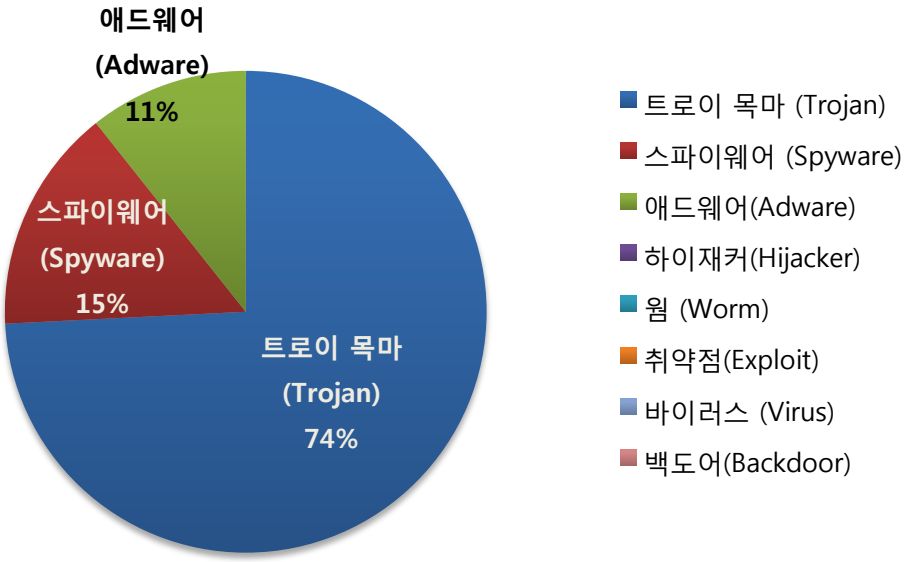
[2011년 2월 1일 ~ 2011년 2월 28일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	V.DWN.86016	Trojan	63,059
2	New	Trojan.Generic.KD.125022	Trojan	37,352
3	↓1	S.SPY.Lineag-GLG	Spyware	37,034
4	New	Variant.FakeAlert.11	Trojan	35,284
5	↓2	Trojan.Downloader.JNSD	Trojan	34,020
6	New	Trojan.Generic.KD.135083	Trojan	28,529
7	↑1	S.SPY.OnlineGames-H	Spyware	26,523
8	New	Variant.Adware.Oso.1	Adware	25,800
9	New	V.DWN.Agent.Pinsearch	Trojan	24,172
10	New	Trojan.Generic.KD.129794	Trojan	21,414
11	New	Trojan.Generic.KDV.128012	Trojan	20,018
12	New	A.ADV.Clicki	Adware	19,131
13	↓3	V.DWN.Onlinegame.PA.Gen	Trojan	18,742
14	New	Trojan.Generic.KDV.134704	Trojan	14,843
15	New	V.DWN.el.39xxxx	Trojan	14,733

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

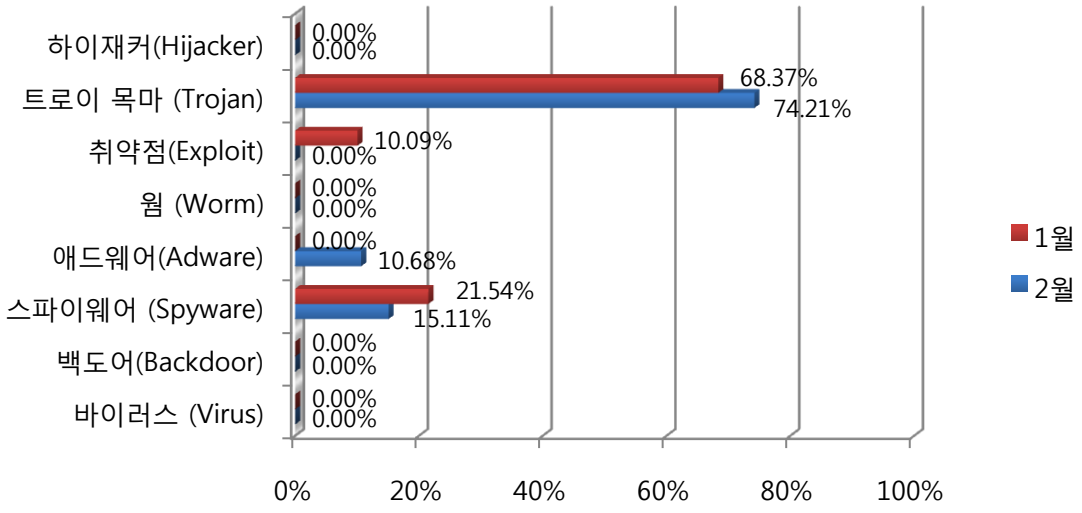
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2월의 감염 악성코드 TOP 15는 V.DWN.86016가 63,059건으로 TOP 15 중 1위를 차지하였으며, Trojan.Generic.KD.125022이 37,352건으로 2위, S.SPY.Lineag-GLG 가 37,034건으로 3위를 차지하였다. 이외에도 2월에 새로 Top 15에 진입한 악성코드는 총 11종이다. 2월에는 웹브라우저에서 특정 키워드를 입력하면 쇼핑몰이나 특정 사이트로 연결하는 악성코드가 극성을 부렸다. 아직까지 특정사이트로 연결되는 것 외에 별 다른 악성기능은 없는 것으로 파악되고 있지만 악성코드가 스스로 업데이트하는 기능을 가지고 있어 추 후 다른 악성기능이 추가될 가능성이 있다.
새로 랭킹된 악성코드들은 대부분 위와 같은 동작을 수행하는 악성코드이며, 급속도로 확산되고 있으니 주의가 필요하다. 다른 악성코드에 비해 용량이 큰 편인 점을 미루어 취약점에 의해 설치되었다기 보다는 웹하드 등의 프로그램과 함께 번들로 설치되었을 가능성이 높아 보이며, 이 같은 배포방식은 확산력이 높고 더 악의적인 의도를 가진 다른 추가프로그램을 얼마든지 다운로드할 수 있어 PC 사용자들이 알약을 최신 상태로 업데이트 하고 주기적으로 검사와 치료를 실행 해야 한다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 74%로 가장 많은 비율을 차지하고, 스파이웨어(Spyware)가 15%, 애드웨어(Adware)가 11%의 비율을 각각 차지하고 있다.

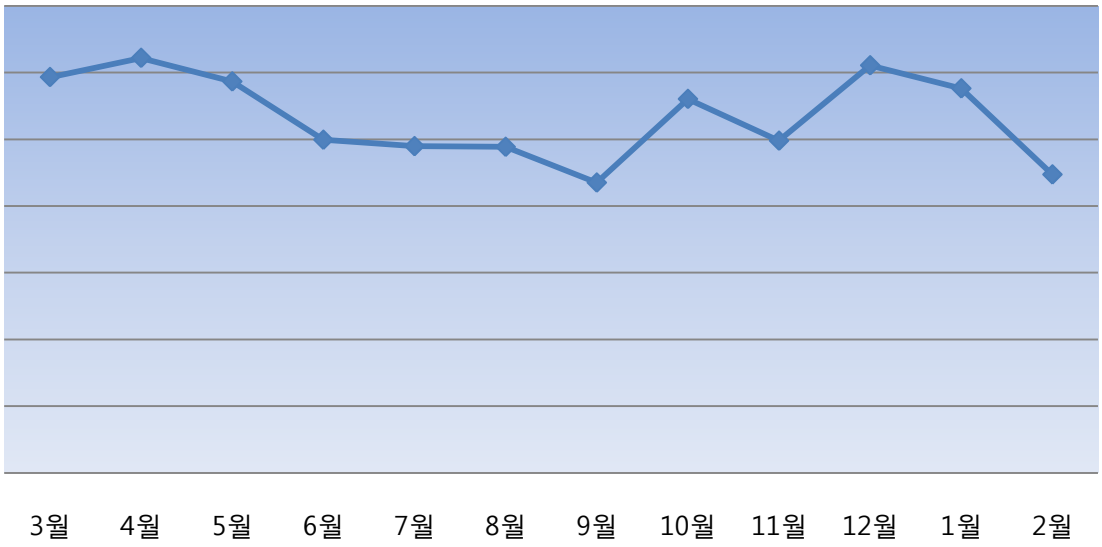
(3) 카테고리별 악성코드 비율 전월 비교



악성코드 유형별 비율을 전월과 비교한 그래프이다. 특이사항은 트로이목마(Trojan)가 약 6%, 애드웨어(Adware)가 약 10% 증가하였으며, 반면 스파이웨어(Spyware)가 약 6% 감소하였다. 위처럼 사이버 범죄자들은 자동 실행되는 애드웨어(Adware), 트로이목마(Trojan), 웹 기반 공격 등을 선호하고 있으며 트로이목마(Trojan)의 비중이 계속 커지고 있어 더욱 트로이목마(Trojan)에 주의가 필요하다.

(4) 월별 피해 신고 추이

[2010년 03월 ~ 2011년 02월]

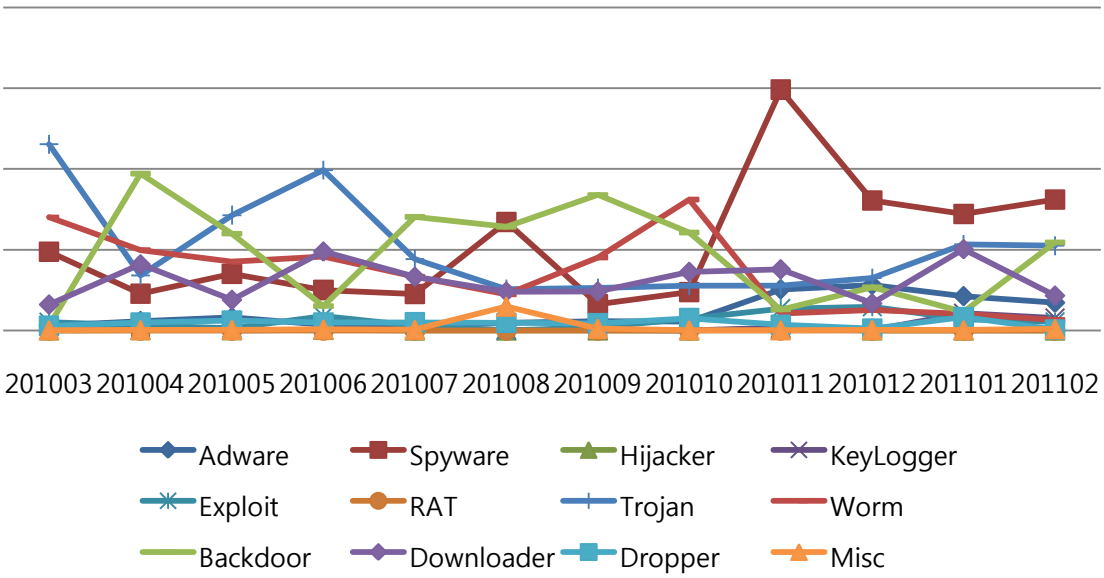


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 2월의 피해 신고추이는 전월에 비해 대폭 감소하였다.

(5) 월별 악성코드 DB 등록 추이

[2010년 03월 ~ 2011년 02월]



DB 등록추이는 변종이 많이 발생되는 순위라고 말해도 과언이 아니다. 2월은 전월에 비해 스파이웨어(Spyware)가 소폭 증가하며 가장 많은 양이 등록되고 있다., 이 밖에 백도어(Backdoor)도 전월에 비해 대폭 증가하였다.

Part I 2월의 악성코드 통계

2. 악성코드 이슈 분석 – "V.TRJ.DDoS.Nationddd"

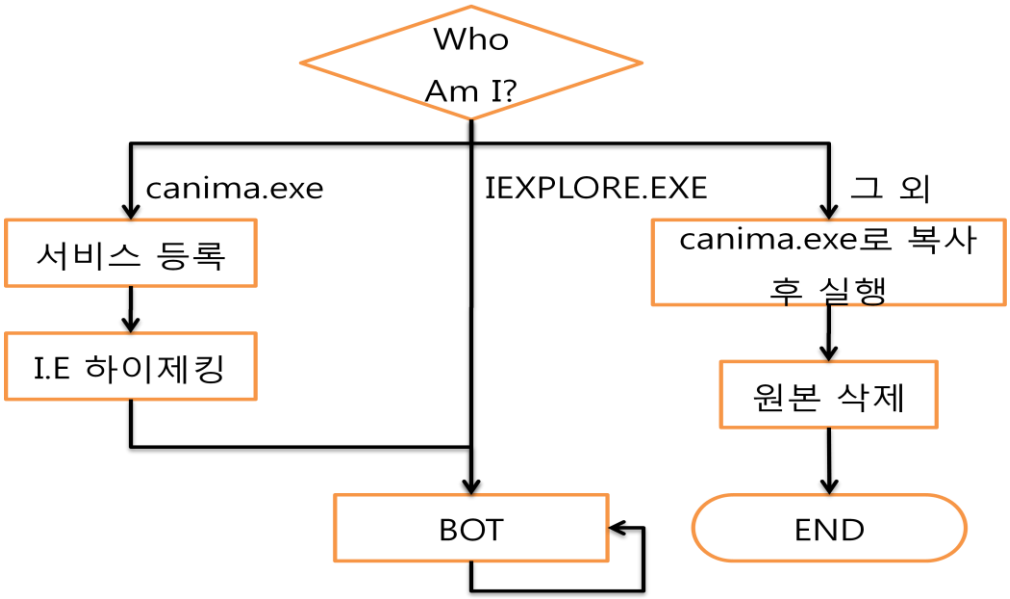
(1) 개요

지난 1월에 Nationddd 라는 레지스트리 키를 사용하는 악성코드가 여러 개 발견되었다. 이 악성코드는 Internet Explorer를 실행하고 서버의 명령을 받아 실행하는 BOT이다. BOT 기능 중에는 특성 사이트를 공격하는 DDOS도 있다. DDOS가 시작되면 과도한 트래픽 때문에 내부 네트워크가 마비되기도 한다.

악성코드의 전체적인 실행 흐름과 서버로부터 어떤 명령을 받아서 처리하는지 알아본다.

(2) 악성코드 분석

이 악성코드는 서버로부터 명령을 받아서 실행하는 BOT 기능을 주로 한다. BOT 기능을 실행하기 위해서 특정 폴더에 특정 이름으로 파일이 존재해야 하고, 프로세스가 쉽게 탐지되는 것을 막기 위해 Internet Explorer 프로세스인 것처럼 속이고 실행된다.



[그림] 전체 흐름도

처음 실행하면 실행된 경로를 구해서 canima.exe인지, IEXPLORE.EXE인지, 둘 다 아닌지 검사하고 각자의 루틴을 실행한다. 설명 편의상 둘 다 아닌 경우를 먼저 분석할 것이다.

A. 그 외

Canima.exe도 아니고 IEXPLORE.EXE도 아닐 경우 실행 파일을 %WINDOWS%₩canima.exe로 복사하고 복사된 파일을 실행한다. 그 후 원본 파일을 삭제하고 프로세스를 종료한다.

B. IEXPLORE.EXE

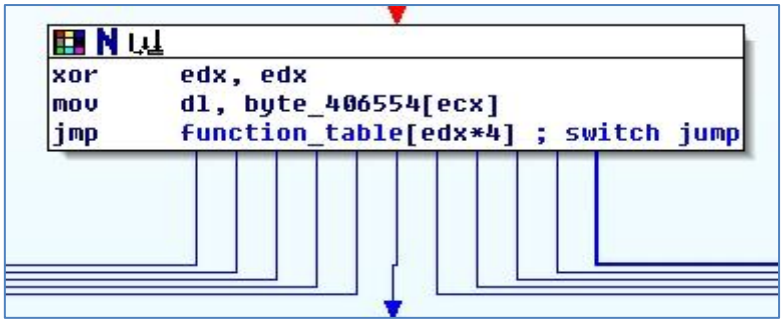
실행된 파일의 경로가 %PROGRAM_FILES%₩Internet Explorer₩₩IEXPLORE.EXE 라면 바로 BOT 동작을 실행한다. BOT의 자세한 동작은 아래에서 분석한다.

C. canima.exe

레지스트리에 등록된 서비스에서 "Nationadddljid" 값이 있는지 확인한다. 만약 없으면 canima.exe를 자동으로 실행하는 서비스를 추가한다. 그리고 suspended 상태로 Internet Explorer(이하 IE) 프로세스를 생성한다. 생성된 프로세스 내부에는 IE 실행코드가 있는데 이것을 모두 제거한다. 그리고 canima.exe 프로세스의 실행코드를 모두 IE 프로세스로 복사하여 entry-point부터 프로세스를 다시 실행시킨다. 겉으로 볼 때는 IE지만 내부적으로는 canima.exe 코드가 실행된다. 이것은 AV의 탐지를 피해서 좀 더 오래 살아남기 위함이다. 그리고 마지막으로 BOT 동작을 실행한다.

D. BOT

sunkind.vicp.net:5888에 접속하여 호스트 컴퓨터의 CPU와 메모리 정보 등을 전송한다. 그 후 서버로부터 여러 가지 명령을 받을 수 있다. DDOS 공격, 파일 다운로드, 파일 실행, 사이트 접속, 셧다운, 프로그램 종료의 명령이 가능하다.




```
  v10 = CreateThread(0, 0, (DWORD (__stdcall *)(LPVOID))DownloadAndExec,
  if ( Parameter == 18 )
    WaitForSingleObject(v10, 0xFFFFFFFFu);
  break;
case 22:
  WinExec((const CHAR *)&CmdLine, 0);
  break;
case 19:
case 20:
  ShellExecuteA(0, "open", "iexplore.exe", &CmdLine, 0, -(recv_data != 19
  break;
case 7:
case 8:
  _ShutDown(((recv_data == 8) + 1) | 4);
  break;
case 6:
  _Deinitialize();
  ExitProcess(0);
  return sd;
```

[그림] 받은 명령에 따라 해당 함수 실행

• **DDOS 공격**

서버로부터 공격할 IP와 공격 횟수를 받아서 해당 IP를 공격한다. 쓰레기 값을 보내기도 하고 http request를 보내기도 한다.

• **파일 다운로드**

다운로드 할 URL 주소를 서버에서 받는다. 해당 URL의 파일을 다운로드 받고 실행한다.

• **파일 실행**

서버에서 받은 명령어를 실행한다.

• **사이트 접속**

iexplore.exe를 실행하여 서버에서 받은 사이트(URL)에 접속한다.

• **셧다운**

컴퓨터를 종료시킨다.

• **프로그램 종료**

모든 작업을 마무리하고 프로그램을 종료한다.

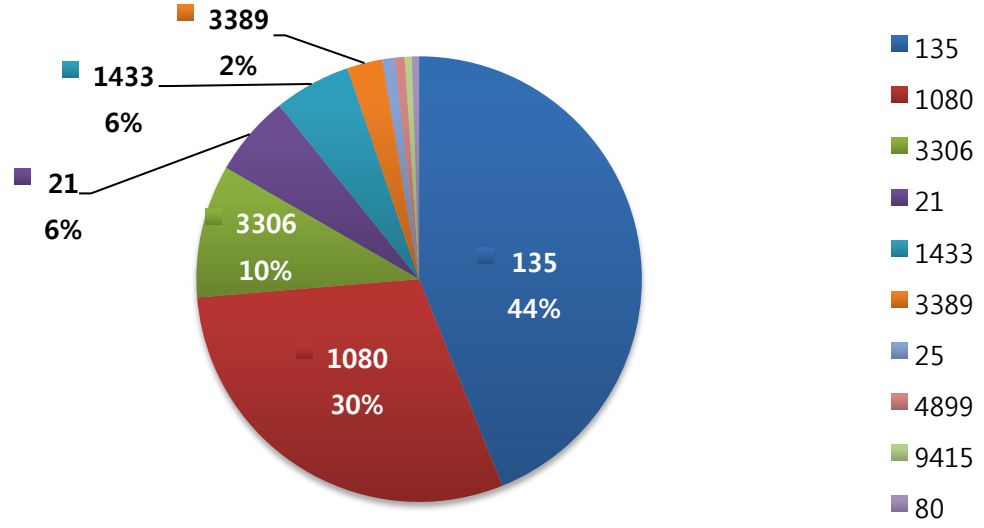
(3) 결론

보통의 DDOS 악성코드는 공격 리스트를 파일내부에 가지고 있는 경우가 많은데 이 악성코드는 실시간으로 서버에서 명령을 받아서 특정 사이트를 공격한다. 그리고 탐지를 피하기 위해 정상 프로그램을 가장하여 실행된다. 이 악성코드에 감염되면 본인도 모르게 공격자가 되기 때문에 백신을 최신으로 유지하며 이러한 일을 막는 것이 중요하다.

Part I 2월의 악성코드 통계

3. 허니팟/트래픽 분석

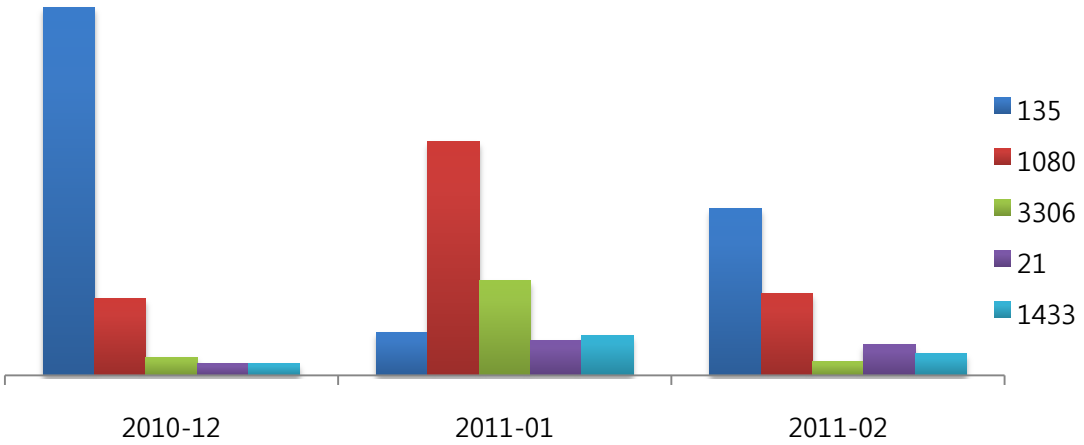
(1) 상위 Top 10 포트



135 TCP를 노리는 트래픽이 가장 많이 발생했으며, 주로 유입된 트래픽은 수 년 전부터 존재한 윈도우의 취약점을 노리는 악성 코드이다. 지금은 많은 사용자들이 윈도우에 보안 패치를 하고 있기 때문에 이런 트래픽의 영향을 받는 PC는 별로 없을 것이다. 그 외에 자동화된 툴을 이용하여 SQL서버나 SMTP서버 등 잘 알려진 서버들의 권한을 노리거나 스팸메일의 릴레이를 위한 악성 트래픽들이 발생하였다.

(2) 상위 Top 5 포트 월별 추이

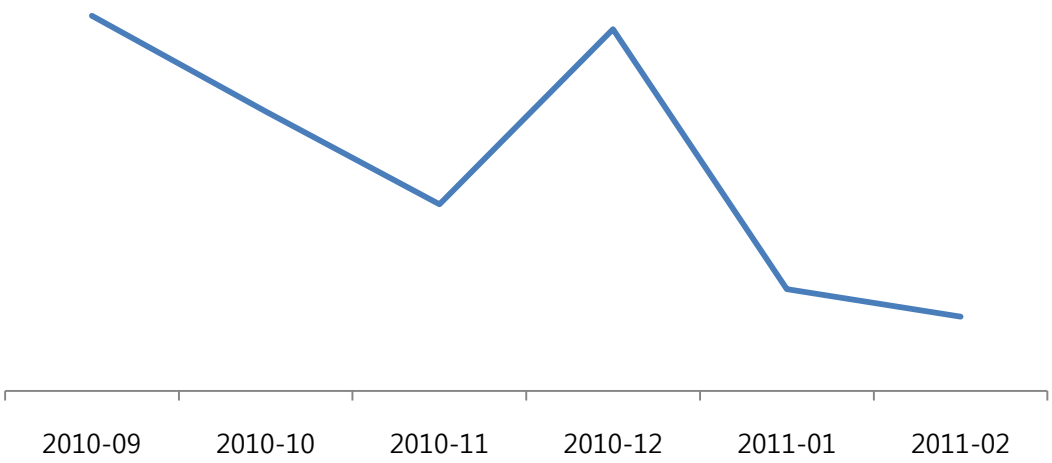
[2010년 12월 ~ 2011년 02월]



공격자는 자동화된 공격 툴을 사용하기 때문에 일반 사용자 및 서버 관리자는 매달 정기적으로 제공되는 마이크로소프트의 보안 업데이트를 반드시 설치해야 하며 사용중인 계정들 주기적으로 점검하고 비밀번호도 바꾸어야 한다.

(3) 악성 트래픽 유입 추이

[2010년 9월 ~ 2011년 2월]

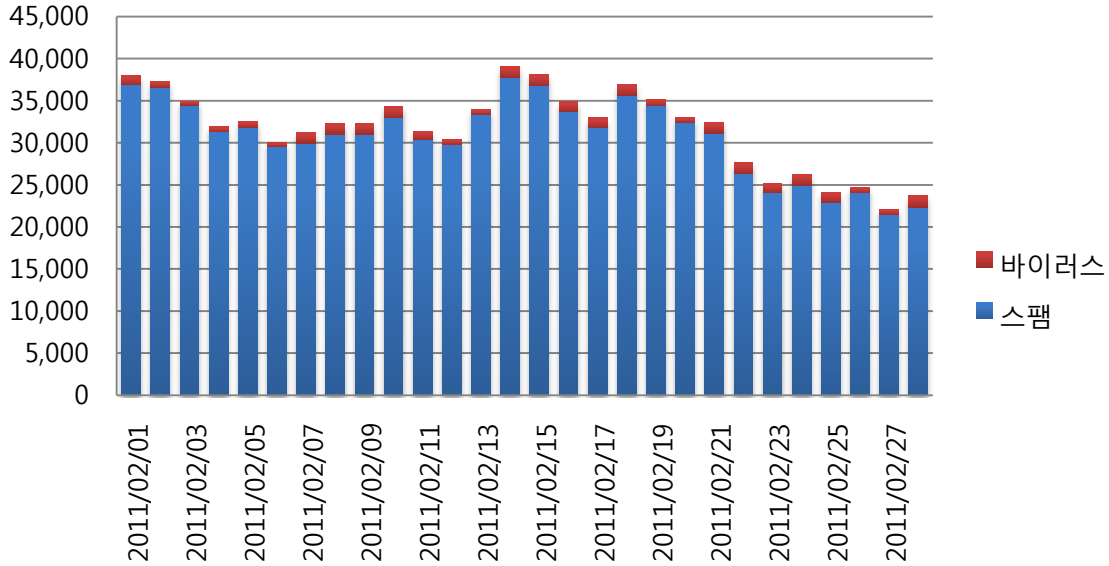


전체적인 악성코드 트래픽은 감소 했으나 2월 이므로, 날 수가 적은 요인이 있다. PC에서 문서를 읽을 때 자주 사용되는 PDF Reader (Acrobat Reader)는 주기적으로 보안 패치를 제공하는데 악성코드 유포 수단으로 Acrobat Reader의 취약점을 악용하는 사례가 있기 때문에 이 보안패치를 확인하고 설치해야 한다. 사용자는 PDF Reader 뿐 아니라 PC에 설치된 다른 프로그램들에서 제공하는 보안패치들도 주기적으로 확인할 필요가 있다. 중요한 개인 정보를 당연하게 PC에 저장하는 시대인 만큼 그런 정보를 노리는 악의적 행위에 대응하는 사용자 스스로의 노력도 중요하다.

Part I 2월의 악성코드 통계

4. 스팸 메일 분석

(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프이다. 2월은 발렌타인데이를 앞두고 선물소개와 기프트 카드, 개인 맞춤 카드 등 광고성 스팸이 증가하였다. 스팸메일은 발렌타인데이 전 후로 소비자들의 관심을 유발시킬만한 문구들을 포함하고 있으며, 이 메일들이 단순 제품광고를 넘어 피싱, 악성코드 유포 등의 다양한 공격 수단으로 악용되어 개인정보 유출이나 금융피해를 입힐 수 있으므로 주의하여야 한다. 스팸메일 피해를 막기 위해서는 의심되는 이메일을 절대 열어보지 말고 의심되는 이메일 안에 포함된 URL링크 또한 클릭하지 말아야 한다.

Part Ⅱ 보안 이슈 돋보기

1. 2월의 보안 이슈

2월에는 최근 발견되는 악성코드의 수량이 급격히 늘고 있다는 통계들이 많이 발표되었습니다. 최근 악성코드들은 보안프로그램에 의한 차단을 회피하기 위해 많은 양의 변종을 생산해 내고 있으며 신종 악성코드의 종류 또한 지속적으로 늘고 있는 추세입니다.
현재 모바일 보안에 관해 스마트폰 보안위협이 실제보다 다소 과장되어 있다는 의견과 그렇지 않다는 전문가들의 상반된 견해들이 보고되고 있는 가운데, '알약안드로이드'가 다운로드 수 100만 건을 돌파하여 스마트폰 사용자들의 보안의식이 높아지고 있음을 나타냈습니다.

• 트위터를 C&C 서버로 이용하는 좀비 프로그램 발견

특정 트위터 계정을 좀비PC의 C&C 서버로 이용하는 악성코드가 발견되었습니다.
지금까지의 좀비PC는 네트워크 관리자가 봇넷에 명령을 내리는 C&C서버의 인터넷 주소를 차단하면 더 이상 봇넷이 제 기능을 하지 못하도록 조치할 수 있었으나, 이번 트위터를 이용한 좀비 PC의 경우 C&C서버로 사용되는 트위터의 인터넷주소를 차단하는 것이 쉽지 않은 문제이며 공격자를 추적하기도 어려워지기 때문에 트위터의 특정 계정에서 트윗한 문자열을 봇넷의 제어명령으로 사용한 것이 특징입니다.

<SNS Twitter>

• '알약 안드로이드' 100만 다운로드 돌파

2010년 12월에 출시한 안드로이드폰 전용 백신 '알약 안드로이드'가 2월 21일 기준 다운로드 횟수 100만건을 돌파했습니다. 누구나 무료로 설치할 수 있는 알약안드로이드는 하루 평균 1만명 이상의 사용자가 다운로드하고 있으며, 안드로이드 마켓에서 4.6의 높은 별점을 획득하고 있습니다. 알약 안드로이드는 백신으로서의 기본적인 실시간 감시 및 악성코드 치료 기능 외에도, 애플리케이션과 스팸 관리 등 스마트폰에 최적화된 보안 기능을 함께 제공하여 사용자가 꾸준히 늘어나고 있습니다.

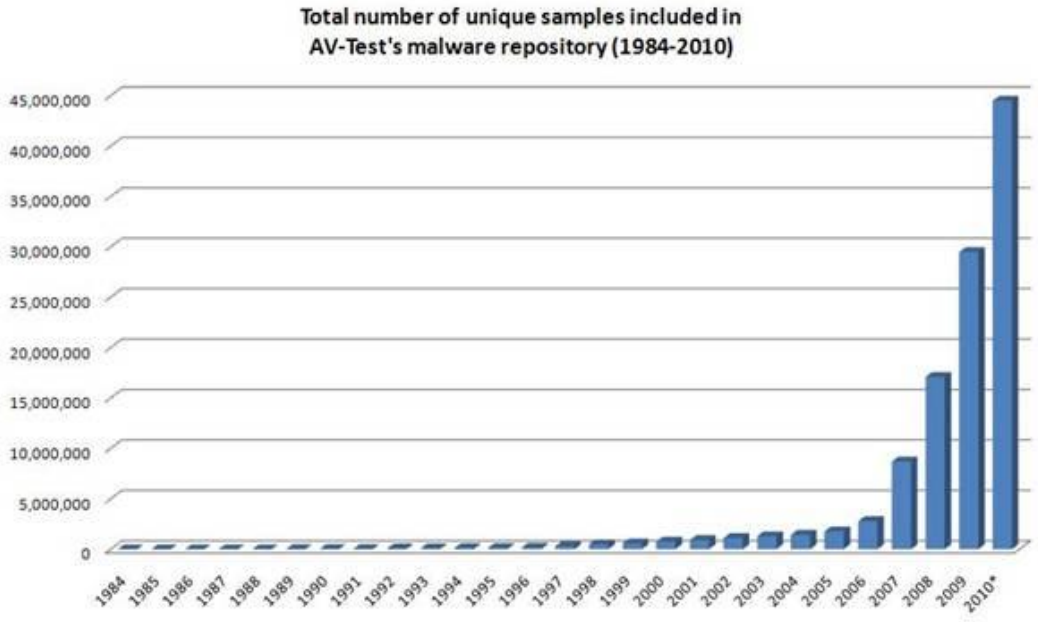
• 고교생 해커에 의해 정부기관등 100여개 서버 해킹

4억 명품녀로 알려진 여성의 개인 신상정보를 인터넷에 게시, 일명 '신상털이'를 저지른 해커가 2명의 고교생인 것으로 밝혀져 논란이 되었습니다.
이들은 특정인의 신상털이 뿐 아니라 관 공서, 방송국, 외국 정부기관 홈페이지 등 100여

개의 홈페이지를 닥치는대로 해킹했습니다. 이들은 특별히 금전적 이익을 노려 해킹을 한 것은 아니며 단지 자신들의 실력을 과시하고 싶었다고 합니다.
국내 많은 웹사이트가 중급 정도의 실력을 가진 이들에게 손쉽게 해킹당했다는 것은 많은 국내 홈페이지들의 보안이 매우 취약함을 나타내며, 해킹 피해를 입은 사이트들은 모두 동일한 보안취약점을 가지고 있었던 것으로 알려졌습니다.

• 악성코드 현재까지 약 4천 4백만개 발견

독일의 악성코드 연구기관인 AV-Test는 2010년 12월 31일을 기준으로 현재까지 발견된 악성코드가 약 4천 4백만개에 이른다고 밝혔다. 악성코드는 2007년도부터 수가 급격하게 증가했으며 2010년 한 해 동안 새롭게 발견된 악성코드가 약 1천 4백만개로 일 평균 약 4만 1 천개 악성코드가 발견되었다고 한다.



<출처: AV-Test>

• KISA 발표 국내 악성코드 신고건 수 급격히 증가

한국인터넷진흥원은 1월 국내 악성코드 전체 신고가 최근 5년 사이 최고치를 기록했다고 발표했습니다. 1월 국내 악성코드 신고는 2004년 9월 통계 이후 가장 많은 2920건이 접수되어, 최근 들어 악성코드가 급격히 늘어나고 있음을 나타냈습니다.

Part Ⅱ 1 월의 이슈 돋보기

2. 2월의 취약점 이슈

• Microsoft 2월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Windows 셸 그래픽 처리의 취약점으로 인한 원격 코드 실행 문제, 취약점으로 인한 원격코드실행 문제, OpenType CFF드라이버의 취약점으로 인한 원격 코드 실행 문제 등을 해결한 Microsoft 2월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**

<취약점 목록>

Internet Explorer 누적 보안 업데이트(2482017)

이 보안 업데이트는 Internet Explorer의 비공개적으로 보고된 취약점 2건과 일반에 공개된 취약점 2건을 해결합니다. 이 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 보거나 특수하게 조작된 라이브러리 파일을 로드하는 합법적인 HTML 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 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 셸 그래픽 처리의 취약점으로 인한 원격 코드 실행 문제점(2483185)

이 보안 업데이트는 Windows 셸 그래픽 프로세서의 공개된 취약점을 해결합니다. 이 취약점은 사용자가 특수하게 조작된 축소판 그림을 볼 경우 원격 코드 실행을 허용할 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.

OpenType CFF(Compact Font Format) 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2485376)

이 보안 업데이트는 비공개적으로 보고된 Windows OpenType CFF(Compact Font Format) 드라이버의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 CFF 글꼴로 렌더링된 콘텐츠를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 특수하게 조작된 콘텐츠를 보도록 만들 수는 없습니

다. 대신 공격자는 사용자가 전자 메일 메시지 또는 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

IIS(인터넷 정보 서비스) FTP 서비스의 취약점으로 인한 원격 코드 실행 문제점(2489256)
이 보안 업데이트는 Microsoft IIS(인터넷 정보 서비스) FTP 서비스의 공개된 취약점을 해결합니다. 이 취약점으로 인해 FTP 서버가 특수하게 조작된 FTP 명령을 받을 경우 원격 코드 실행이 허용될 수 있습니다. FTP 서비스는 IIS에 기본적으로 설치되지 않습니다.

Active Directory의 취약점으로 인한 서비스 거부 문제점(2478953)
이 보안 업데이트는 Active Directory의 공개된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 Active Directory 서버에 특수하게 조작된 패킷을 보낼 경우 서비스 거부가 발생할 수 있습니다. 공격자는 이 취약점을 악용하기 위해 도메인에 가입된 컴퓨터의 유효한 로컬 관리자 권한이 있어야 합니다.

Microsoft Visio의 취약점으로 인한 원격 코드 실행 문제점(2451879)
이 보안 업데이트는 Microsoft Visio에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 Visio 파일을 열 경우 원격 코드 실행이 발생할 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

JScript 및 VBScript 스크립팅 엔진의 취약점으로 인한 정보 유출 문제점(2475792)
이 보안 업데이트는 비공개적으로 보고된 JScript 및 VBScript 스크립팅 엔진의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 사이트를 방문할 경우 정보 유출이 발생할 수 있습니다. 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

Windows CSRSS(Client/Server Runtime Subsystem)의 취약점으로 인한 권한 상승 문제점(2476687)
이 보안 업데이트는 Windows XP 및 Windows Server 2003의 CSRSS(Microsoft Windows Client/Server Run-time Subsystem)에서 발견되어 비공개적으로 보고된 취약점 1건을 해결합니다.
이 취약점으로 인해 공격자가 이후 사용자의 로그온 자격 증명을 얻기 위해 시스템에 로그온하여 공격자가 로그오프한 후에도 계속 실행되도록 특수하게 조작된 응용 프로그램을 시작할 경우 권한 상승이 발생할 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 커널의 취약점으로 인한 권한 상승 문제점(2393802)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건과 비공개적으로 보고된 취약점 1건을 해결합니다. 이 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 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2479628)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 5건을 해결합니다. 이 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.

Kerberos의 취약점으로 인한 권한 상승 문제점(2496930)

이 보안 업데이트는 Microsoft Windows의 비공개적으로 보고된 취약점 1건과 공개적으로 보고된 취약점 1건을 해결합니다. 인증된 로컬 공격자가 도메인에 가입된 컴퓨터에 악성 서비스를 설치하면 가장 위험한 취약점으로 인해 권한 상승이 허용될 수 있습니다.

로컬 보안 기관 하위 시스템 서비스의 취약점으로 인한 로컬 권한 상승 문제점(2478960)

이 보안 업데이트는 Windows XP 및 Windows Server 2003의 LSASS(로컬 보안 기관 하위 시스템 서비스)에서 발견되어 비공개적으로 보고된 취약점 1건을 해결합니다.
공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 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.

<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-feb.mspx

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

• Adobe Flash Player 다중 취약점 보안 업데이트 권고

CVE Number : CVE-2011-0558 외.

Adobe Flash Player에 영향을 주는 다중의 취약점을 해결한 보안 업데이트가 발표되었습니다. 특수하게 조작된 Flash파일이 포함된 웹페이지를 열어보도록 유도해 악성코드를 유포 할 수 있으므로 주의가 필요하며 낮은 버전의 Flash Player 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

<해당 제품>

• Adobe Flash Player 10.1.102.64 및 이전 버전

<임시 해결책>

Adobe Flash Player Download Center에서 Adobe Flash Player 10.2.152.26 버전을 설치하거나 자동 업데이트를 이용하여 최신버전으로 업그레이드 하시기 바랍니다.

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

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-02.html

• Adobe Reader/Acrobat 다중 취약점 보안업데이트 권고

CVE Number : CVE-2010-4091 외

Adobe Reader/Acrobat의 다중 취약점을 해결한 보안 업데이트가 발표되었습니다.

낮은 버전의 Adobe Reader/Acrobat사용자는 서비스 거부 공격 및 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

• Adobe Reader X(10.0) 버전

• Adobe Reader 9.4.1 이하 버전

• Adobe Acrobat 9.4.1/X(10.0) 이하 버전

<임시 해결책>

Adobe Download Center에 방문하여 Adobe 제품의 최신버전을 설치하거나 [메뉴]→[도움말]→[업데이트확인]을 이용하여 업그레이드

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-03.html

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

http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows

http://www.adobe.com/support/downloads/product.jsp?product=158&platform=Windows

http://www.adobe.com/support/downloads/product.jsp?product=112&platform=Windows

• Adobe Shockwave Player 다중 취약점 보안업데이트 권고

CVE Number : CVE-2010-2587 외

Shockwave Player의 다수 취약점을 해결한 보안 업데이트가 발표되었습니다.

낮은 버전의 Adobe Shockwave Player를 사용할 경우 악성코드 감염에 취약할 수 있으므로 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

• Adobe Shockwave Player 11.5.9.615 이하 버전

<임시 해결책>

Adobe Download Center에 방문하여 11.5.9.620 버전을 설치

http://get.adobe.com/shockwave

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-01.html

• Oracle Java 다중 취약점 보안 업데이트 권고

2011년 2월 16일, Oracle Critical Patch Update를 통해 Java 제품에 대한 보안업데이트가 발표되었습니다. 관련 공격코드의 출현으로 인한 피해가 발생할 수 있으므로 Oracle Java 제품의 보안 업데이트를 실행하시기 바랍니다.

<해당 제품>

• Java SE:

- JDK, JRE 6 Update 23 및 이전 버전

• Java for Business :

- JDK, JRE 6 Update 23 및 이전 버전
- JDK, JRE 5.0 Update 27 및 이전 버전
- SDK, JRE 1.4.2_29 및 이전 버전

<임시 해결책>

개인사용자 경우, 설치된 제품의 최신 업데이트(Java SE 6 Update 24)를 다운로드 받아 설치하거나 Java 자동업데이트 설정에 의해 업데이트 합니다.

http://www.oracle.com/technetwork/java/javase/downloads/index.html

기업사용자 경우, 해결방안으로서 "Oracle Java SE and Java for Business Critical Patch Update Advisory - February 2011" 문서를 검토하고 유지보수업체와의 협의/검토 후 보안 업데이트 적용합니다.

각 기업 사정으로 보안업데이트 적용이 지연될 경우,

- 백신 등 보안솔루션 최신업데이트 적용
- 불필요한 계정을 삭제하고 디폴트 패스워드 변경
- 방화벽을 이용한 접근 통제를 구현하여 사용자에게 허가되는 권한을 최소화함으로써, 공격으로 인해 발생될 영향을 제한
- 영향을 받는 서비스에 대해서는 신뢰된 호스트 및 네트워크들만 액세스할 수 있도록 제한

<참고 사이트>

http://www.oracle.com/technetwork/topics/security/javacpufeb2011-304611.html

Contact us...

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 사이트 : www.alyac.co.kr