www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 12월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2011년 12월 1일 ~ 2012년 12월 31일]

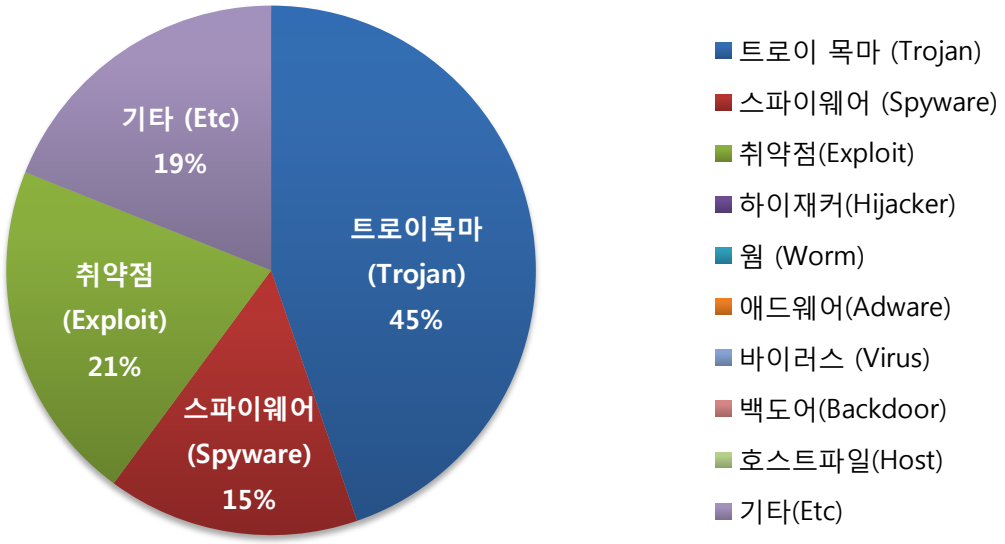
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑1	K.EXP.SWF.ShellCode.Gen	Exploit	17,130
2	↑3	S.SPY.OnlineGames.wsxp	Spyware	12,614
3	New	Trojan.PWS.YTO	Trojan	5,140
4	New	Variant.Graftor.11053	Etc	4,932
5	New	Trojan.Generic.KDV.484908	Trojan	4,766
6	New	Trojan.Generic.KDV.487267	Trojan	4,484
7	New	Trojan.Generic.KDV.495759	Trojan	4,482
8	New	Trojan.Script.6192	Trojan	3,998
9	↑5	V.DWN.86016	Trojan	3,897
10	New	Variant.Graftor.6348	Etc	3,780
11	New	Variant.Graftor.6394	Etc	3,703
12	New	Trojan.Heur.GZ.zKX@bzRCJSpG	Trojan	3,570
13	New	V.DWN.OnlineGame.svo	Trojan	3,183
14	New	Trojan.Generic.KDV.487061	Trojan	3,130
15	New	Variant.Graftor.7761	Etc	3,111

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
12월의 감염 악성코드 TOP 15는 K.EXP.SWF.ShellCode.Gen이 17,130건으로 TOP 15 중 1위를 차지했으며, S.SPY.OnlineGames.wsxp가 12,614건으로 2위, Trojan.PWS.YTO가 5,140건으로 3위를 차지했습니다. 이 외에도 12월에 새로 Top 15에 진입한 악성코드는 총 12종입니다.

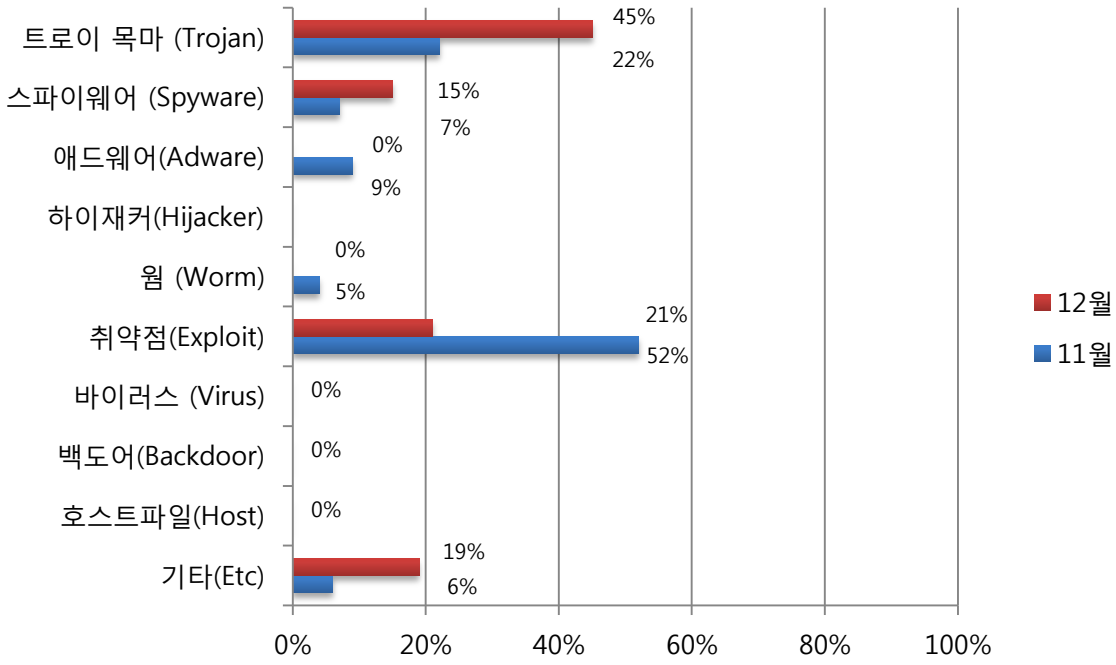
12월에도 주말(대부분 금요일~월요일 사이)을 이용한 온라인 게임 계정 유출 악성코드가 가장 많이 탐지되었습니다. 이와 관련된 대표적인 탐지명으로는 플래쉬 취약점을 이용해 악성코드를 설치시키는 K.EXP.SWF.ShellCode.Gen, 추가 다운로더(V.DWN.OnlineGames.svo), Windows₩system32 폴더의 정상 윈도우 파일(ws2help.dll)을 악성코드로 변조시키는 S.SPY.OnlineGames.wsxp 등이 있습니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이 목마(Exploit)은 45%로 가장 많은 부분을 차지하였고, 취약점(Exploit) 21%, 스파이웨어(Spyware)가 15%, 기타(Etc) 19%의 비율을 나타냈습니다.

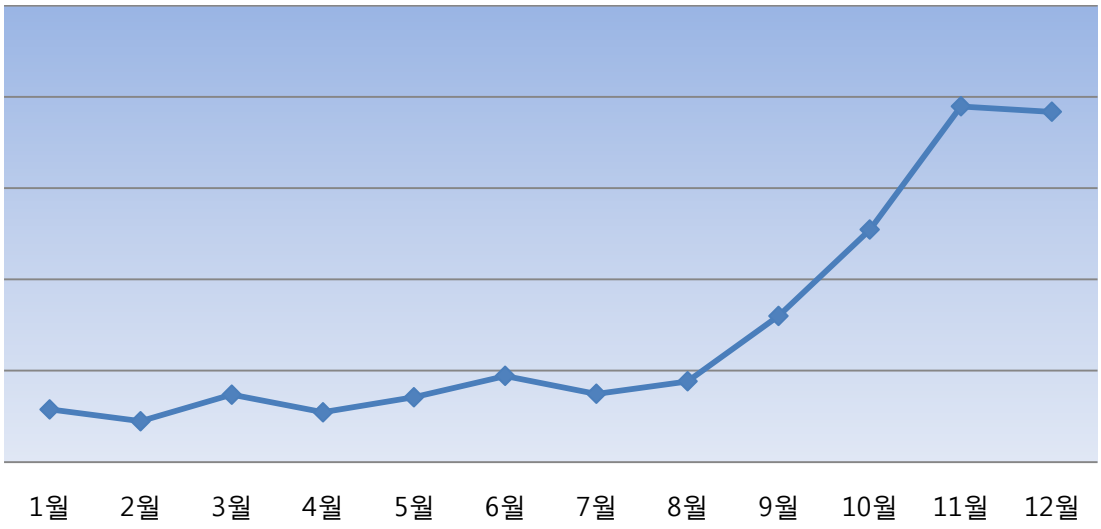
(3) 카테고리별 악성코드 비율 전월 비교



12월의 특이사항은 트로이 목마(Trojan)와 스파이웨어(Spyware)가 전달에 비해 2배 이상 크게 증가했고, 취약점(Exploit)의 경우 전달에 비해서는 수치가 감소하였으나 꾸준히 탐지되고 있습니다.

(4) 월별 피해 신고 추이

[2011년 1월 ~ 2011년 12월]

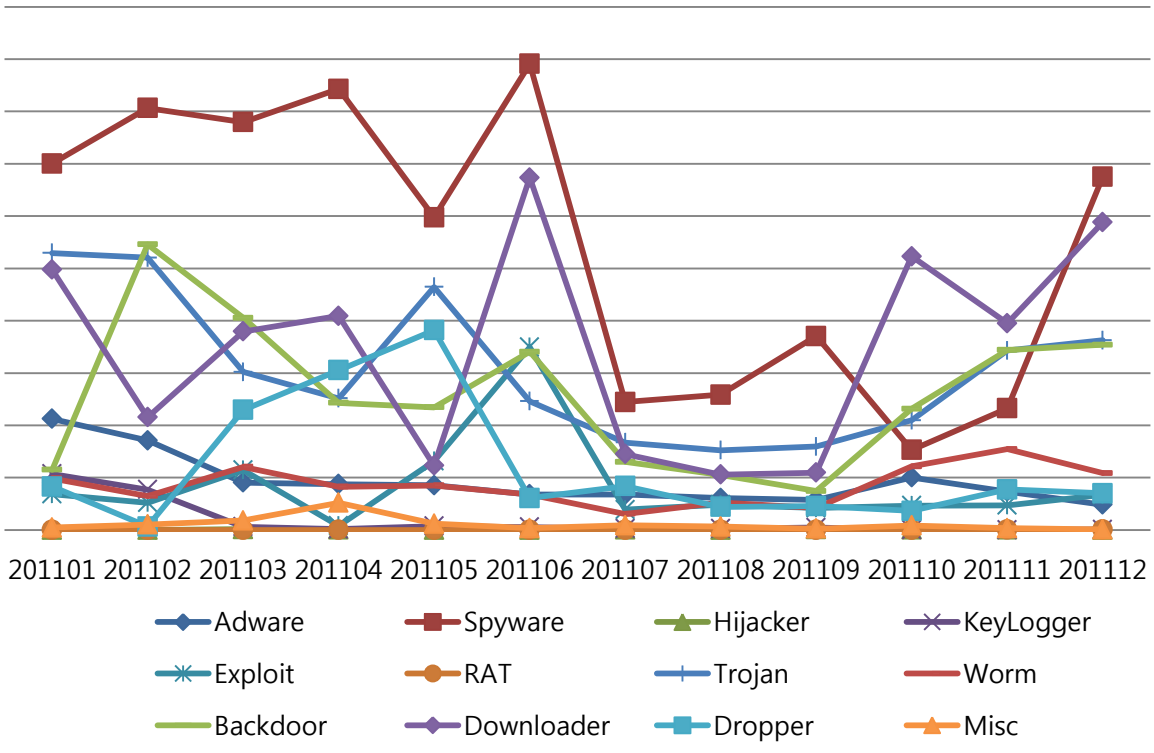


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0 신고 내용이 추가된 8월 이후 전달(11월)까지 신고 건수가 가파르게 증가하다가 12월에 들어 약간 수치가 감소하였습니다.

(5) 월별 악성코드 DB 등록 추이

[2011년 1월 ~ 2011년 12월]



Part I 12월의 악성코드 통계

2. 악성코드 이슈 분석 – "Trojan.Keylogger.Various.46472"

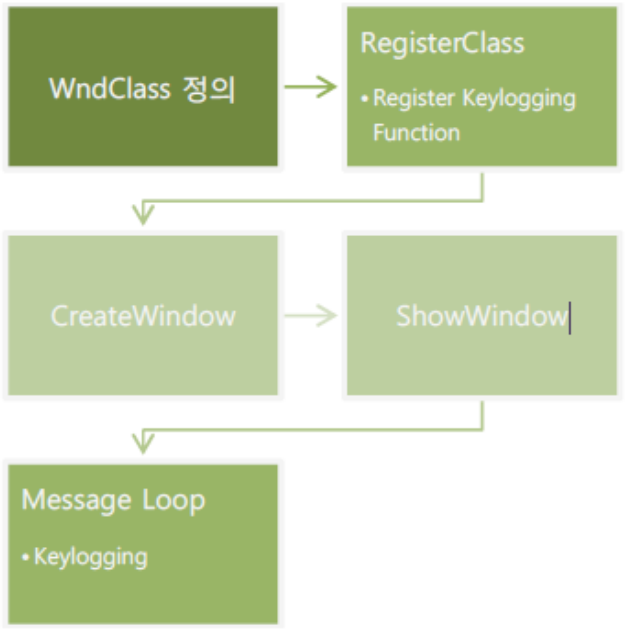
(1) 개요

이번 악성코드는 사용자의 키보드 입력을 로깅하는 전형적인 키로거입니다.
악성코드 제작자는 어려운 후킹 방식을 사용하지 않고도 단순하고 쉽게 키로깅을 할 수 있습니다. 본 문서에서는 악성코드가 어떻게 Raw input Model 을 이용하여 윈도우 클래스를 등록 시 윈도우 클래스의 메시지 처리 함수에서 키로깅 하는지 알아보겠습니다.

(2) 악성코드 분석

```
sub     esp, 60h
mov     dword_4097E8, 0
push    offset Name     ; "My159865478_Client"
push    0               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
```

먼저 악성 코드는 중복 실행 방지를 위해 위와 같은 "My159865478_Client"라는 이름으로 뮤텍스를 생성합니다.



위 그림은 키로거의 동작 과정입니다. 본 악성코드는 Raw input Model 을 이용하여 윈도우 클래스를 등록 시 윈도우 클래스의 메시지 처리 함수에서 키로깅합니다.

키보드 RAWINPUTDEVICE 구조체 설정	

rawInputDev[0].usUsagePage = 0x01;
rawInputDev[0].usUsage = 0x06;
rawInputDev[0].dwFlags = RIDEV_INPUTSINK;
rawInputDev[0].hwndTarget = GetSafeHwnd();
	v15 = 1;
	v16[0] = 6;
	*(_DWORD *)&v16[1] = RIDEV_INPUTSINK;
	v17 = v5;

먼저 악성코드는 위와 같이 RAWINPUTDEVICE 구조체를 설정하여 RegisterRawInput Devices 함수를 이용해 시스템에서 키보드 이벤트를 입력 받을 수 있도록 등록합니다. 이렇게 함으로써 멀티태스킹 환경에서도 전역적인 키보드 입력에 대한 포커싱이 가능해집니다.

따라서 윈도우가 활성화되지 않아도 시스템의 모든 키보드 이벤트를 입력 받을 수 있습니다. (이와 같은 방식은 Windows XP 이상에서만 지원한다.) 따라서 시스템은 해당 윈도우에 WM_INPUT 메시지를 보내 사용자로부터 Input 이벤트가 들어왔는지를 알 수 있습니다.

```
push    0                   ; lpParam
push    esi                 ; hInstance
push    0                   ; hMenu
push    0                   ; hWndParent
push    CW_USEDEFAULT       ; nHeight
push    CW_USEDEFAULT       ; nWidth
push    CW_USEDEFAULT       ; Y
push    CW_USEDEFAULT       ; X
push    0CF0000h            ; dwStyle
push    offset WindowName ; "tolog"
push    offset ClassName ; "log"
push    0                   ; dwExStyle
call    ds:CreateWindowExA
```

위와 같이 키보드 입력을 받기 위한 Message-Only 윈도우를 생성합니다.
Message-Only 윈도우이기 때문에 윈도우가 생성되지는 않고 GetSystemTime 함수를 이용해서 시스템의 시간 정보를 얻어옵니다.
그리고 그 값을 이용해서 C:₩Program Files₩Common Files₩Microsoft Shared₩drivers 위치에 k10 월일.sys 형태로 악성 드라이버 파일을 생성하지만 실제로는 키 입력에 대한 내용을 저장하는 파일입니다.

암호화 방식 예시
[F8] -> dyb

GetRawInputData() API 를 이용하여 WM_INPUT 메시지를 입력 받으며 윈도우의 이름, 입력된 키 값 등의 정보가 k10 월일.sys 파일에 저장되며 이때 암호화하여 저장합니다.

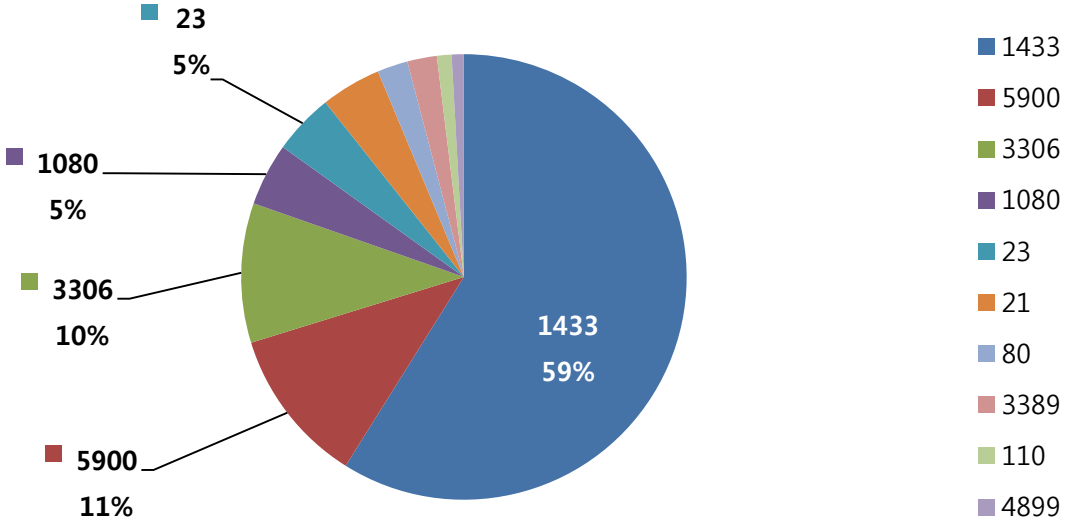
(3) 결론

이번 악성코드의 특이 점은 별다른 후킹 등의 행위를 하지 않고도 악성코드 제작자는 윈도우에서 지원하는 기능을 이용하여 쉽게 키로거를 제작할 수 있습니다.

Part I 12월의 악성코드 통계

3. 허니팟/트래픽 분석

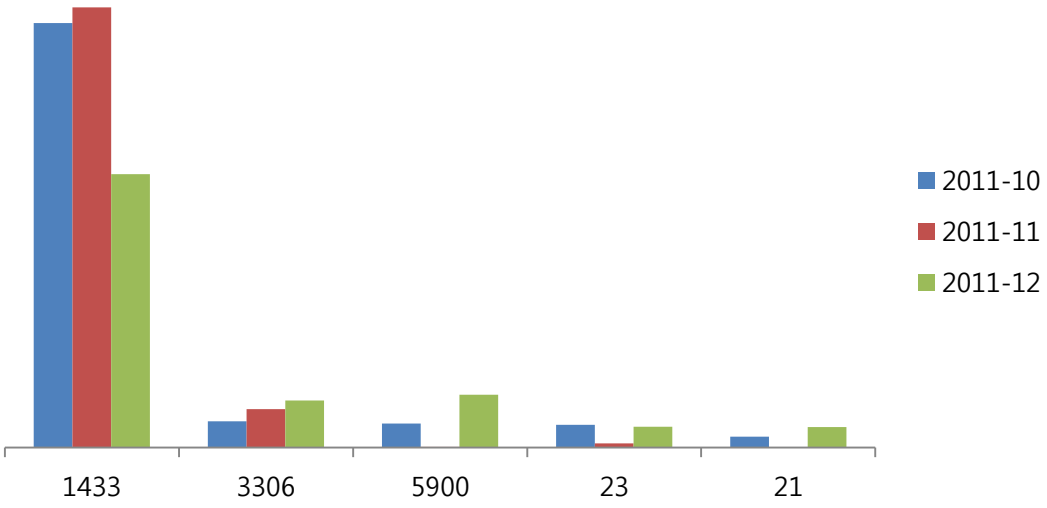
(1) 상위 Top 10 포트



12월에도 Microsoft SQL Server에서 사용하는 1433 포트에 대한 트래픽 유입이 가장 많았습니다. 이외에도 VNC 원격제어 포트인 5900을 통한 트래픽 유입이 두 번째로 높게 나타났습니다. 최근 악성코드들이 새로운 서버나 PC를 감염시키기 위해 취약한 패스워드를 설정한 터미널서비스, DBMS를 공격하고 있으므로 반드시 강력한 패스워드를 사용해야 합니다.

(2) 상위 Top 5 포트 월별 추이

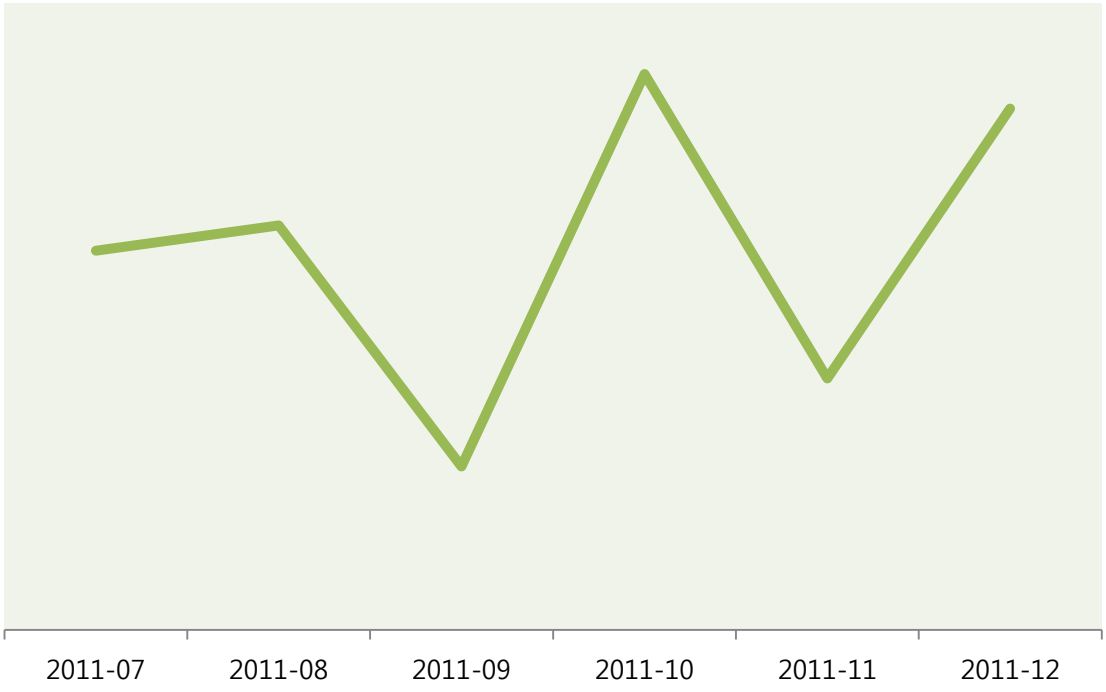
[2011년 10월 ~ 2011년 12월]



3개월 추이에서는 전체적으로 1433 포트의 트래픽이 감소했으며, MySQL DBMS가 주로 사용하는 3306 포트의 유입이 꾸준히 증가하고 있습니다.

(3) 악성 트래픽 유입 추이

[2011년 07월 ~ 2011년 12월]

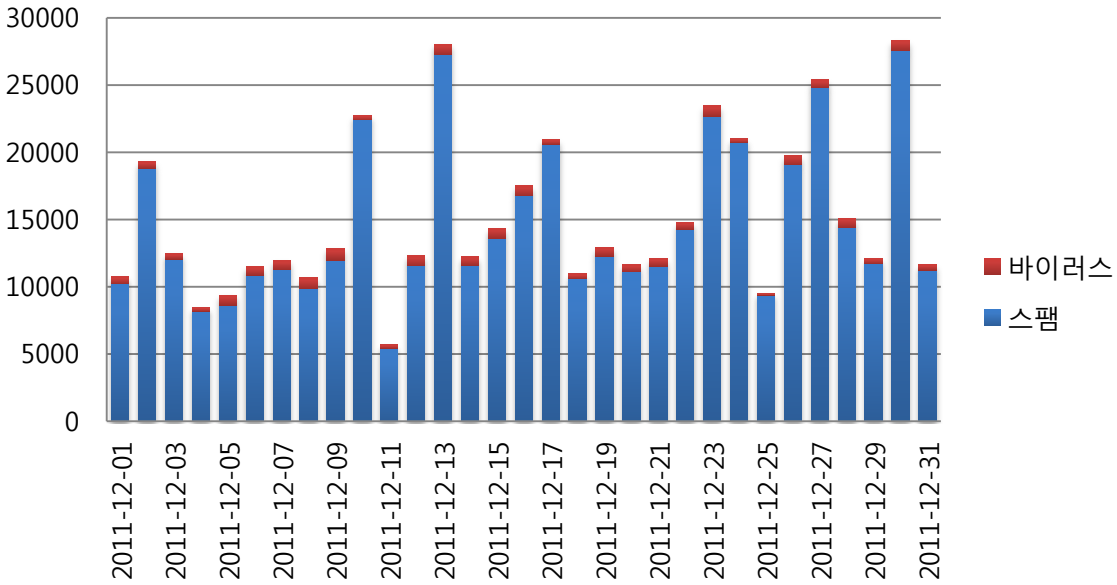


전체적인 악성 트래픽 유입이 증가하였습니다.
12월에도 주로 단순한 패스워드를 사용하는 Microsoft SQL Server와 MySQL DBMS를 노린 유해 트래픽이 많았습니다.
현재 악성코드에 의해 자동적으로 DB 서버로 패스워드 대입 공격(Brute force attack)을 시도하는 경우가 많이 발견되고 있으므로 DB Server에 대해 주기적으로 패스워드로 변경해야 하며, 단순한 패스워드 사용을 피해야 합니다.

Part I 12월의 악성코드 통계

4. 스팸 메일 분석

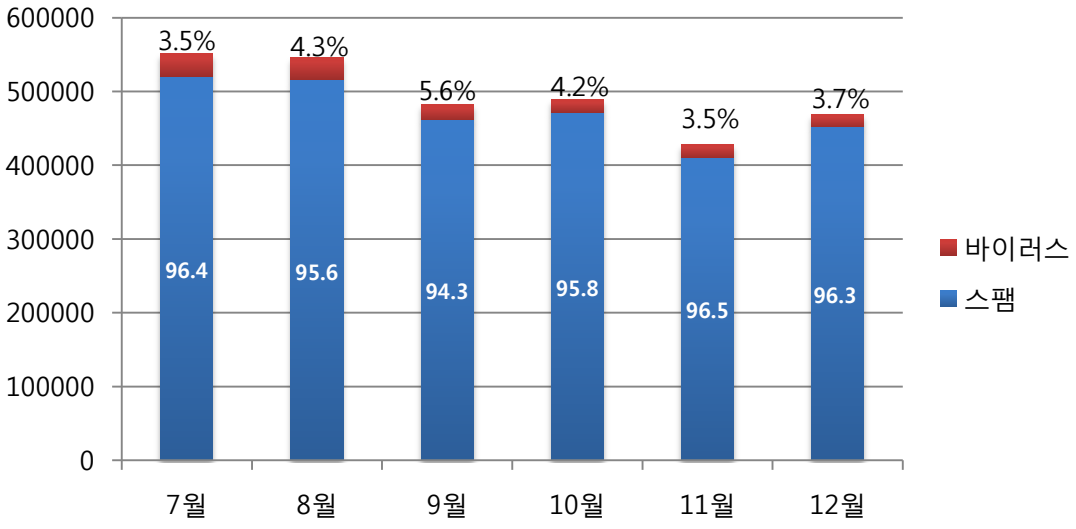
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 12월에는 크리스마스 선물이나 연하장으로 위장한 악성코드 메일이 발견되었으며, 스팸메일 발송은 월말에 크게 늘어난 경향을 보이고 있습니다.

(2) 월별 통계 현황

[2011년 7월 ~ 2011년 12월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프입니다. 12월의 스팸 메일은 96.3%, 바이러스 메일은 3.7%를 차지하였으며, 크리스마스와 신년 선물 혹은 연하장으로 위장한 악성 메일이 나타났습니다.

(3) 스팸 메일 내의 악성코드 현황

[2011년 12월 1일 ~ 2011년 12월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	7,305	41.97 %
2	W32/MyDoom-H	3,378	19.41 %
3	Mal/ZipMal-B	2,561	14.72 %
4	W32/Virut-T	1,308	7.52 %
5	W32/Bagz-D	715	4.11 %
6	Mal/BredoZp-B	339	1.95 %
7	Mal/BredoZp-D	262	1.51 %
8	W32/MyDoom-N	246	1.41 %
9	W32/Bagle-CF	205	1.18 %
10	Troj/ZipMal-AW	156	0.90 %

스팸 메일 내의 악성코드 현황은 12월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 41.97%로 1위를 차지하였으며, 2위는 19.41%를 차지한 W32/MyDoom-H, 3위는 14.72%를 차지한 Mal/ZipMal-B입니다.

Part Ⅱ 보안 이슈 돋보기

1. 12월의 보안 이슈

앞으로 웹상에서 주민등록번호 수집을 금지하는 정책이 시행되어 인터넷실명제가 단계적으로 폐지됩니다. 게임, 포털 업체들도 개인정보 수집을 최소화하는 정책을 발표하고 있습니다. 그 밖에 김정일 사망 악성코드, 미국 대형 체인마켓의 카드리더 해킹 등이 12월의 이슈가 되었습니다.

• 2012년부터 주민등록번호 수집 제한

인터넷실명제가 2012년부터 2014년까지 단계적으로 폐지됩니다. 방통위가 2014년까지 인터넷 상 영리목적의 주민등록번호 사용금지를 목표로, 금년 내 주민번호 사용제한을 위한 시행령·고시 등 하위법령 개정을 추진할 계획이라고 밝혔습니다. 이에 따라 앞으로는 인터넷 사업자들이 관행적으로 수집하던 이용자의 주민등록번호를 더 이상 수집할 수 없게 되었습니다.

• 김정일 사망 악성코드

김정일 북한 국방위원장이 사망하자 이 소식을 담은 동영상과 함께, 악성코드가 나돌았습니다. 사용자가 해당 동영상 소개에 적힌 링크를 클릭하면 광고성 악성프로그램이 설치되며 김정일 사망과 관련된 또 다른 악성 이메일들도 발견이 되었습니다. 사회적으로 큰 이슈가 있을 때마다 이슈를 이용한 악성코드 유포가 이루어지고 있어 주의가 요망됩니다.

• 게임, 포털 업체들이 주민등록번호 수집 제한 정책 발표

연말 잇따른 보안사고로 인해 인터넷 컨텐츠 사업자들의 정보보호 노력이 늘고 있습니다. SK커뮤니케이션즈, 넥슨, 엔씨소프트 등 대형 포털, 게임 업체들이 고객 개인정보보호를 위해 주민등록번호를 하지 않거나 보존기간을 대폭 축소하겠다고 발표했으며, 주민등록번호 수집정책개선 외에 개인정보 암호화, 사내 보안을 강화 등을 통해 개인정보유출에 대비한다는 계획들이 많이 발표되었습니다.

• 구글, 안드로이드 마켓 대청소

구글이 안드로이드 마켓에서 SMS과금 발생형 악성앱 등 27개의 악성 앱을 삭제하고 이 리스트를 공개했습니다. 구글 안드로이드 마켓의 악성앱 대량 퇴출이 이번이 처음은 아니며, 구글은 비 정기적으로 악성앱을 삭제해 자체적인 마켓 정화를 시도하고 있습니다.

• 해킹으로 페이스북 보안 취약점 찾다 체포

영국의 한 대학생이 페이스북의 보안취약점을 찾으려 해킹을 시도했다가 경찰에 체포되었습니다. 이 남성은 과거에 야후의 보안취약점을 발견해 야후로부터 보상을 받은 적이 있으며 페이스북 역시 취약점을 조사해 수정하게 하려는 의도였다고 주장했습니다.

• 신용카드 리더기 해킹

미국 슈퍼마켓체인과 레스토랑의 신용카드 처리시스템이 해킹을 당해 고객정보가 탈취되고 신용카드가 부정 사용되었습니다. 최근 국내에서도 신용카드 계산을 처리하는 POS단말기가 해킹되어 고객의 신용카드가 중국에서 부정 사용되는 사례가 있었습니다. 신용카드 리더기는 PC나 POS 컴퓨터에 연결되어 있기 때문에 악성코드 등에 쉽게 해킹될 수 있다는 점이 계속해서 지적되고 있습니다.

2. 1월의 취약점 이슈

• Microsoft 1월 정기 보안 업데이트

Windows Media의 취약점으로 인한 원격 코드 실행 문제, Windows 커널 취약점으로 인한 Kernel 보안 기능 우회 문제, Windows 개체 포장기의 취약점으로 인한 원격 코드 실행 문제 등을 해결한 Microsoft 1월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

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

<취약점 목록>

Windows Media의 취약점으로 인한 원격 코드 실행 문제점(2636391)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 사용자가 특수하게 조작된 미디어 파일을 열면 이러한 취약점으로 인해 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 커널 취약점으로 인한 Kernel 보안 기능 우회(2644615)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점은 공격자가 소프트웨어 응용 프로그램에서 SafeSEH 보안 기능을 우회할 수 있도록 합니다. 그런 후 공격자는 다른 취약점을 이용하여 구조적 예외 처리기가 임의 코드를 실행하도록 할 수 있습니다. Microsoft Visual C++ .NET 2003을 사용하여 컴파일한 소프트웨어 응용 프로그램만 이 취약점을 악용하는 데 이용될 수 있습니다.

Windows 개체 포장기의 취약점으로 인한 원격 코드 실행 문제점(2603381)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 실행 파일과 동일한 네트워크 디렉터리에 있는 포함된 패키지 개체를 포함하는 합법적인 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Windows CSRSS(Client/Server Runtime Subsystem)의 취약점으로 인한 권한 상승 문제점(2646524)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점 1건을 해결합니다. 이 보안 업데이트의 심각도는 지원 대상인 모든 Windows XP, Windows Server 2003, Windows Vista 및 Windows Server 2008 에디션에 대해 중요입니다. 지원 대상인 Windows 7 및 Windows Server 2008 R2 에디션은 이 취약점의 영향을 받지 않습니다.
이 취약점으로 인해 공격자가 영향을 받는 시스템에 로그온한 후 특수하게 조작한 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 그런 후 공격자는 영향을 받는 시스템을 완전히 제어하고 프로그램을 설치할 수 있으며, 데이터를 보거나 변경하거나 삭제할 수 있고, 모든 사용자 권한을 갖는 새 계정을 만들 수 있습니다. 이 취약점은 중국어, 일본어 또는 한국어 시스템 로캘로 구성된 시스템에서만 악용될 수 있습니다.

Microsoft Windows의 취약점으로 인한 원격 코드 실행 문제점(2584146)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점은 사용자가 악성의 내장형 ClickOnce 응용 프로그램이 들어 있는 특수하게 조작된 Microsoft Office 파일을 열 경우 원격 코드가 실행되도록 할 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.

SSL/TLS의 취약점으로 인한 정보 유출 문제점(2643584)

이 보안 취약점은 SSL 3.0 및 TLS 1.0의 공개된 취약점을 해결합니다. 이 취약점은 프로토콜 자체에 영향을 미치며 Windows 운영 체제와는 관련이 없습니다. 이 취약점은 공격자가 영향 받은 시스템에서 제공된 암호화된 웹 트래픽을 가로챌 경우 정보가 노출되도록 할 수 있습니다. TLS 1.1, TLS 1.2, 그리고 CBC 모드를 사용하는 모든 암호 그룹은 영향을 받지 않습니다.

AntiXSS 라이브러리의 취약점으로 인한 정보 유출 문제점(2607664)

이 보안 업데이트는 비공개적으로 보고된 Microsoft AntiXSS(사이트 간 스크립팅 방지) 라이브러리의 취약점 1건을 해결합니다. 이 취약점은 공격자가 AntiXSS 라이브러리의 삭제 기능을 사용하여 웹 사이트에 악성 스크립트를 제공할 경우 정보가 유출되도록 할 수 있습니다. 이러한 정보 노출의 결과는 정보 자체의 특성에 따라 좌우됩니다. 이 취약점으로 인해 공격자가 직접 코드를 실행하거나 해당 사용자 권한을 상승시킬 수는 없지만 영향을 받는 시스템의 손상을 악화시키는 데 사용할 수 있는 정보를 생성할 수 있습니다. AntiXSS 라이브러리의 삭제 모듈을 사용하는 사이트만 이 취약점의 영향을 받습니다.

<해결책>

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/MS12-jan
영문 : http://technet.microsoft.com/en-us/security/bulletin/MS12-jan

• Adobe Reader/Acrobat 다중 취약점 보안업데이트 권고

CVE Number : CVE-2011-2462 외

Adobe Flash Player 및 Acrobat에 영향을 주는 다중의 취약점을 해결한 보안 업데이트가 발표 되었습니다. 낮은 버전의 Adobe Reader/Acrobat 사용자는 시스템의 권한을 탈취 당하거나 응용 프로그램 충돌이 일어날 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

- 윈도우, 매킨토시 환경에서 동작하는 Adobe Reader X(10.1.1) 및 하위 10.x 버전
- 윈도우 환경에서 동작하는 Adobe Reader 9.4.7 및 하위 9.x 버전
- 매킨토시 환경에서 동작하는 Adobe Reader 9.4.6 및 하위 9.x 버전
- 윈도우, 매킨토시 환경에서 동작하는 Adobe Acrobat X(10.1.1) 및 하위 10.x 버전
- 윈도우 환경에서 동작하는 Adobe Acrobat 9.4.7 및 하위 9.x 버전
- 매킨토시 환경에서 동작하는 Adobe Acrobat 9.4.6 및 하위 9.x 버전

<해결 방법>

아래의 Adobe Download Center를 방문하여 업데이트 버전을 설치하거나 [메뉴]→[도움말]→[업데이트확인]을 이용하여 업그레이드

- 윈도우 환경에서 동작하는 Adobe Reader 사용자
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows

- 윈도우 환경에서 동작하는 Adobe Acrobat Standard/Pro 사용자
http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows

- 윈도우 환경에서 동작하는 Adobe Acrobat Pro Extended 사용자
http://www.adobe.com/support/downloads/product.jsp?product=158&platform=Windows

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb12-01.html

• 국내 인터넷 자료실 유포 안드로이드 악성코드 주의

안드로이드폰을 대상으로 동작하는 악성코드가 안드로이드 정식 마켓 및 국내 인터넷 자료실을 통해 유포되었습니다. 해당 악성코드에 감염된 경우, 이메일 주소 등의 개인정보가 유출될 수 있으므로 감염된 경우 아래 조치방법을 통해 치료하시기 바랍니다.

<해당 제품>

- 앱 이름: 'New Year 2012 Live Wallpaper'
- 패키지명: com.inoxapps.newyearlwp

<해결 방법>

'New Year 2012 Live Wallpaper' 앱을 설치한 안드로이드폰 이용자는 구글 안드로이드 마켓을 통해 '알약 안드로이드'를 다운로드 하여 검사 및 치료

*2012년 1월부터 알약보안동향보고서의 취약점 정보가 보안동향보고서 발행 전월 내역에서 당월 내역으로 변경되었습니다.

Contact us...

㈜이스트소프트 알약대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

http://advert.estsoft.com/?event=201111181660299