안철수연구소에서 발행하는 월간 보안 보고서

ASEC 리포트

2009년 1월호

이달의 보안 이슈

ASEC 칼럼

이달의 통계

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 – 콘피커 웜 변형 출현으로 인한 피해 증가

MS08-067 취약점을 이용하여 자신을 전파 하였던 콘피커 웜[1](Win32/Conficker.wom: 이하 콘피커 웜이라고 표기)의 새로운 변형이 발견되었다. 이번 변형은 자신을 전파하는 방법을 다양하게 가지고 있는 것이 특징이며, 국내에 많은 시스템을 감염시켰다. 또한 이스라엘의 가자 지구 침공과 관련한 이슈를 포함한 메일을 전송하여 사용자들로 하여금 감염을 유도하는 형태의 악성코드가 발견되었다. 그리고 기존의 Win32/Zhelatin.worm처럼 국제적인 정치, 사회적인 이슈를 이용하여 자신을 유포 중인 Win32/Waledac.worm 변형도 증가하였다.

(1) 콘피커 웜 변형 출현

이슈가 종료된 것으로 판단되었던 MS08-067 취약점을 이용한 콘피커 웜 변형이 새롭게 발견되었다. 특히 이 변형은 자신을 전파하기 위해 다음과 같은 다양한 방법을 사용하고 있다.

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

또한 악성코드에 대한 진단과 치료를 어렵게 하기 위해서 자신을 원격 파일 핸들로 특정 프로세스에 오픈하며, 특히, NTFS 파일 시스템인 경우 파일의 보안속성을 변경하여 사용자의 읽기, 쓰기 권한을 뺏는 방법을 사용한다.

다른 특징으로 DNS 쿼리 관련 함수를 조작하여 백신[2](Anti-virus, Anti-spyware : 이하 백신으로 표기) 업체와 같은 특정 도메인에 대한 접근을 차단하기도 하였다. 이런 경우 엔진 업데이트 그리고 해당 홈페이지 등에 접속할 수 없게 되어, 사용자들이 콘피커 웜을 진단하는 엔진을 다운받거나 정보를 확인하기는 것을 방해한다. 콘피커 웜 관련 자세한 내용은 이번 호 칼럼에서 소개되니 해당 부분을 참고 바란다.

[1] Win32/conficker.worm에 대한 다양한 표기법을 콘피커 웜으로 통일함.
[2] Anti-virus, Anti-spyware에 대한 다양한 표기법을 백신으로 통일함.

(2) 이스라엘 가자 지구 침공 관련 악성코드

이스라엘의 가자지구 침공과 관련하여 이와 비슷한 유형의 악성코드가 증가 하였다. 이처럼 국제적인 이슈를 이용하여 메일로 유포하는 사회공학적 기법이 오래 전부터 악성코드 배포 방법으로 사용되어 왔다. 이번에 메일로 유포되었던 Win-Trojan/Downloader.9790 악성코드의 유포 메일 중 하나는 다음과 같다.

> Subject: Israel War on Hamas: A Dozen Thoughts
>
> Israel offers short respite from strikes.
> Israel will halt its bombardment of Gaza for three hours every day to allow residents of the Hamas-ruled Palestinian territory to obtain much-needed supplies, a military spokesman says.
> The images broadcast here were graphic and striking.
> The Al Jazeera English report below captures the extent of the devastation caused by the initial strikes.
>
> Proceed to view details: (악성코드 다운로드 링크)

악성코드 다운로드 링크를 클릭하면 보통 다음과 같은 웹 페이지로 안내되고 파일을 다운로드 하도록 유도한다.

[그림 1-1] 이스라엘의 가지지구 침공 관련 악성코드

다운로드 되는 파일명은 'Adobe_Player10.exe'이며, 실행하면 특정 호스트로부터 백도어 증상을 가지고 있는 Dropper/Agent.36352.BR을 다운로드 받는다. 본 글을 작성하는 현재 해당 URL의 파일은 현재 다운로드 되지 않지만, 변형이 많기 때문에 유사한 메일을 받는다면 주의가 요구 된다.

해당 파일을 실행하면 'servicepack1.exe'라는 파일명을 가진 악성코드를 다운로드 받는다. 해당 파일을 실행하면 자신을 은폐시키고 인터넷 익스플로러, FTP, POP3 에 대한 사용자 계정과 비밀번호를 획득하려고 한다.

(3) Win32/Waledac.worm과 사회적인 이슈들

Win32/Waledac.worm은 위에 언급한 이스라엘의 가자지구 침공과 관련한 악성코드처럼 잘 알려진 사회적 이슈를 이용하여 메일로 유포 되었다. 이번 달의 경우 미국의 오바마 대통령 취임식과 발렌타인데이 내용을 담은 메일이 국외에서 대량 유포되었다. 악성코드를 다운로드 받도록 유도하는 웹 페이지 모습은 다음과 같다.

[그림 1-2] Waledac.worm 관련 가짜 웹 페이지

해당 웹 페이지에 접속을 하면 페이지의 내용에 맞는 특정 실행파일의 다운로드 창이 나타난다.

파일을 실행한 경우 특이하게 로컬 드라이브에는 자신의 복사본을 생성하지 않는다. 바이너리 내부를 보면 특정 웹 서버로 접속을 시도하는 내용과, RSA 인증 관련 내용이 존재한다. 이러한 내용들은 P2P 웜처럼 감염된 다른 시스템과 통신을 위해서 사용되는 것으로 보인다. 이 웜 역시 다른 이메일 웜처럼 내부에는 특정 파일 확장자로부터 메일주소를 수집하는 기능이 있다. 이는 자신이 업로드 되어 있는 URL을 전송하기 위한 수신자 메일주소를 수집하기 위한 목적이다.

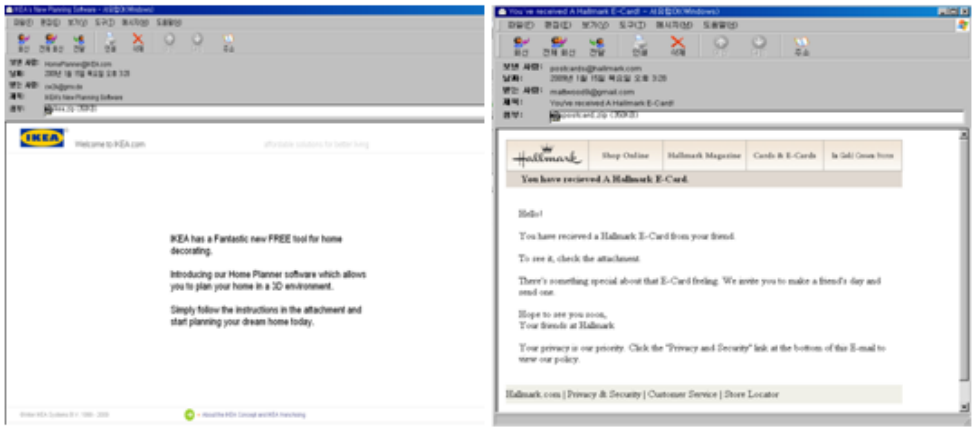
Win32/Waledac.worm은 Win32/Zhelatin.worm처럼 사회적인 이슈를 가지고 자신을 전파

하지만 실행 후 증상이나 자신의 암호화된 코드를 풀어내는 방법은 Win32/Zhelatin.worm과 비교하면 다른 형태를 가지고 있다. 그러나 이 악성코드 역시 조직적으로 만들어지고 유포되는 것으로 보여 Win32/Zhelatin.worm처럼 올 한 해 많은 변형으로 큰 피해를 줄 가능성이 높다.

2. 스파이웨어 - 스파이웨어 크립터와 가짜백신

(1) 매스메일러에 의해 전파되는 스파이웨어 크립터(Win-Spyware/Crypter)

분도(Vundo), 버츄몬드(Virtumonde) 등으로도 불리는 스파이웨어 크립터는 브라우저 도우미 객체(Brower Helper Objects)로 등록되어 인터넷 익스플로러(Internet explorer)가 실행될 때 함께 실행되어 인터넷 사용 도중 팝업 광고를 화면에 출력하거나, 우측 하단 트레이에 거짓 감염 메시지를 노출해 가짜백신(Rogue AntiVirus/AntiSpyware)의 설치를 유도하는 악성 코드이다. 지속적인 광고 노출과 감염 메시지 출력은 사용자에게 불편을 유발하고, 시스템의 성능을 저하시킨다. 스파이웨어 크립터는 일반적으로 OS의 취약점을 통해 주로 전파가 되었으나, 최근 E-mail의 첨부파일을 통해 전파되는 E-card 웜을 통해서도 감염되는 것이 확인되었다.



[그림 1-3] 악성코드가 첨부된 메일

[그림 1-4] 첨부파일

메일에 포함된 첨부파일을 다운로드 받아 압축을 풀면 [그림 1-4]와 같이 문서(.doc)파일을 가장한 스크린세이버(.scr)파일이 나타나게 된다. 윈도우 OS(Windows OS)의 기본 설정은 "알려진 파일형식의 파일 확장명 숨기기"가 되어 있기 때문에 이중 확장자는 일반적으로 문서파일로 인식될 수 있다.

[그림 1-4]와 같이 메일로부터 다운로드 받은 'postcard.doc .scr'파일은 악성코드가 포함된 메일을 발송하는 매스메일러의 기능을 수행하면서 외부 서버로부터 스파이웨어 크립터

를 다운로드 받아 사용자의 시스템에 설치한다.

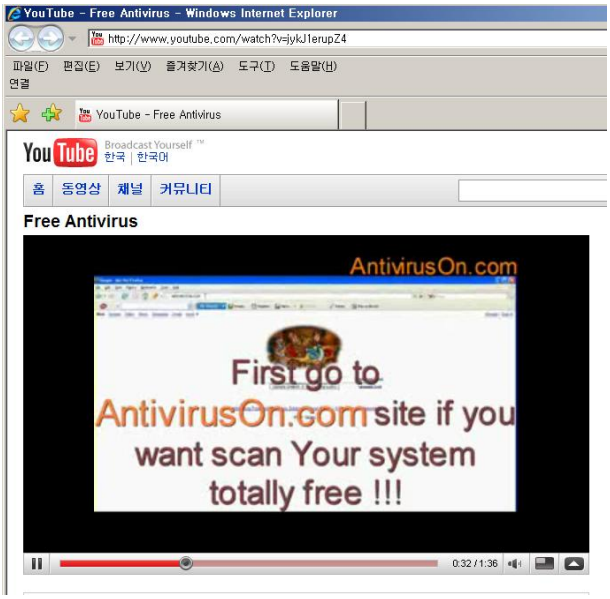
(2) 다양한 가짜백신의 배포방법

최근 안티스파이 2009(Antispy 2009)와 같은 외산 가짜백신(Rogue)이 지속적으로 증가하고 있다. 가짜백신(Rogue)은 더 많은 수익을 올리기 위해 다양한 배포방법을 이용하고 있다. 가짜백신은 스파이웨어 크립터(Win-Spyware/Crypter) 스파이웨어 즐롭(Win-Spyware/Zlob)등의 악성코드를 통해서도 배포되지만 사용자의 흥미를 유발하는 다양한 방법을 통해 설치를 유도하고 있다.

1) YouTube를 통한 튜토리얼 제공

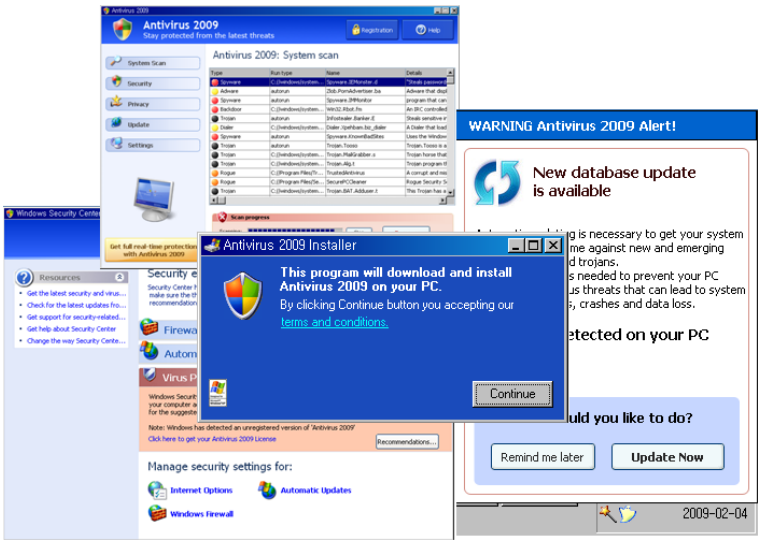
세계적으로 유명한 동영상 공유 사이트인 YouTube에는 개인의 흥미나 기업의 홍보를 위해 제작한 동영상부터 이라크전에 참전한 미군이 제작한 동영상까지 다양한 내용의 동영상이 등록되어 있다. 이 곳에서도 가짜백신을 배포하기 위한 의도가 확인되고 있다.

YouTube에서 FreeAntivirus라는 키워드를 이용해 동영상을 검색해 보면 [그림1-5]과 같은 백신 설치 튜토리얼을 쉽게 찾을 수 있다. 이 것은 특정 사이트에서 백신을 다운로드하여 설치하는 내용이다.



[그림 1-5] YouTube에 등록된 가짜백신 설치 동영상

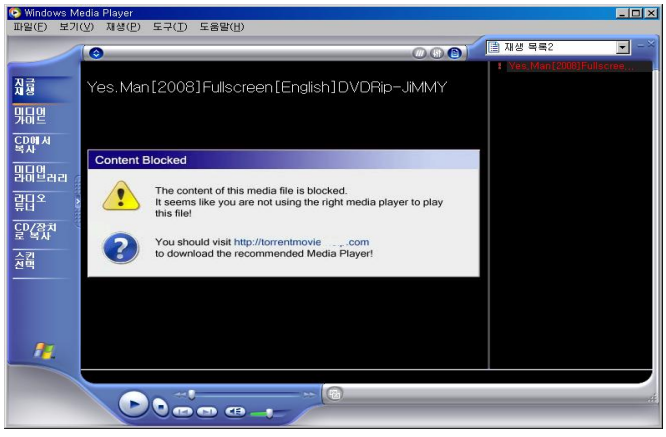
[그림 1-5]의 동영상이 가리키는 사이트에서 다운로드 받아 설치할 수 있는 프로그램은 [그림 1-6]의 안티바이러스 2009(Antivirus 2009)라는 가짜백신으로 무료백신과는 거리가 멀다.



[그림 1-6] 안티바이러스 2009(Antivirus2009)

2) 토렌트(Torrent) 공유파일을 통한 가짜백신 설치 유도

토렌트(Torrent)를 통해 배포되는 가짜 동영상을 통해서도 가짜백신의 설치를 유도하고 있다. 국내외의 많은 사람들이 Torrent라는 P2P 공유방식을 이용해 파일을 다운로드 받고 있다. 이렇게 공유된 파일은 어떠한 검증 절차가 없기 때문에 파일의 무결성을 보장하기 어렵다. [그림 1-7]은 공유사이트에서 다운로드 받은 700M의 동영상 파일을 실행한 것이다. 파일의 크기로 미루어 정상적인 동영상 파일로 보이지만 이 파일을 3분 20초간 오류화면만을 출력한다. 오류창에 표시되는 사이트에서는 동영상 플레이어를 가장한 가짜백신 설치와 결재를 유도한다.



[그림 1-7] 토렌트(Torrent)를 이용해 공유된 동영상 파일 실행 결과

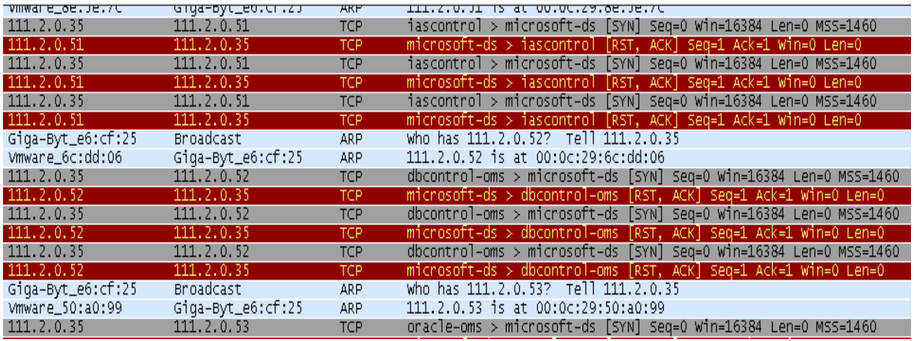
3. 시큐리티 - 콘피커 웜의 전파방법과 대처법

콘피커 웜은 2008년 10월 말 보고된 이후 현재까지도 극성을 부리고 있는 것으로 파악된다. ARBOR(http://asert.arbornetworks.com)에 따르면 1월 30일 기준으로 1200만개의 호스트가 콘피커 웜에 감염된 상태라고 한다. 따라서, 아직까지 확산이 되고 있는 콘피커 웜의 전파방법과 대처법을 알아보자.

(1) 콘피커 웜의 전파방법

해당 웜은 MS08-067 취약점을 이용하여 전파되기 때문에 해당 취약점에 대한 보안 업데이트가 적용되지 않은 시스템은 공격을 통해 감염될 수 있으며, 해당 취약점에 대한 보안 업데이트가 적용되어 있다 할지라도 단순한 패스워드로 설정된 네트워크 공유와 이동형 저장장치인 USB의 자동실행(Autorun)을 통해 감염될 수 있다.

아래 [그림 1-8]은 콘피커 웜이 전파를 위해 네트워크를 스캐닝하는 화면이다.

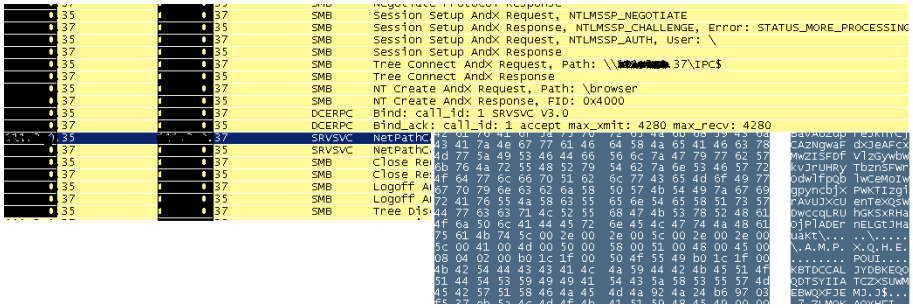


111.2.0.35	111.2.0.51	TCP	iascontrol > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
111.2.0.51	111.2.0.35	TCP	microsoft-ds > iascontrol [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111.2.0.35	111.2.0.51	TCP	iascontrol > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
111.2.0.51	111.2.0.35	TCP	microsoft-ds > iascontrol [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111.2.0.35	111.2.0.51	TCP	iascontrol > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
111.2.0.51	111.2.0.35	TCP	microsoft-ds > iascontrol [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Giga-Byt_e6:cf:25	Broadcast	ARP	Who has 111.2.0.52? Tell 111.2.0.35
Vmware_6c:dd:06	Giga-Byt_e6:cf:25	ARP	111.2.0.52 is at 00:0c:29:6c:dd:06
111.2.0.35	111.2.0.52	TCP	dbcontrol-oms > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
111.2.0.52	111.2.0.35	TCP	microsoft-ds > dbcontrol-oms [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111.2.0.35	111.2.0.52	TCP	dbcontrol-oms > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
111.2.0.52	111.2.0.35	TCP	microsoft-ds > dbcontrol-oms [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111.2.0.35	111.2.0.52	TCP	dbcontrol-oms > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
111.2.0.52	111.2.0.35	TCP	microsoft-ds > dbcontrol-oms [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Giga-Byt_e6:cf:25	Broadcast	ARP	Who has 111.2.0.53? Tell 111.2.0.35
Vmware_50:a0:99	Giga-Byt_e6:cf:25	ARP	111.2.0.53 is at 00:0c:29:50:a0:99
111.2.0.35	111.2.0.53	TCP	oracle-oms > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460

[그림1-8] 전파를 위한 취약한 시스템 스캐닝

[그림 1-8]에서 보는 바와 같이 SMB(서버 메시지 블록) 서비스가 사용하는 445/TCP, 139/TCP 포트를 이용하여 네트워크 상에 존재하는 공격 대상 시스템을 스캐닝한다. 이때 SMB를 사용하고 있는 공격 대상을 발견한다면 MS08-067 취약점 또는 취약한 공유 폴더를 이용하여 공격을 시작하게 된다.

아래 [그림 1-9]는 콘피커 웜이 실제로 MS08-067 취약점을 이용하기 위한 공격 패킷을 전송하는 화면이다.



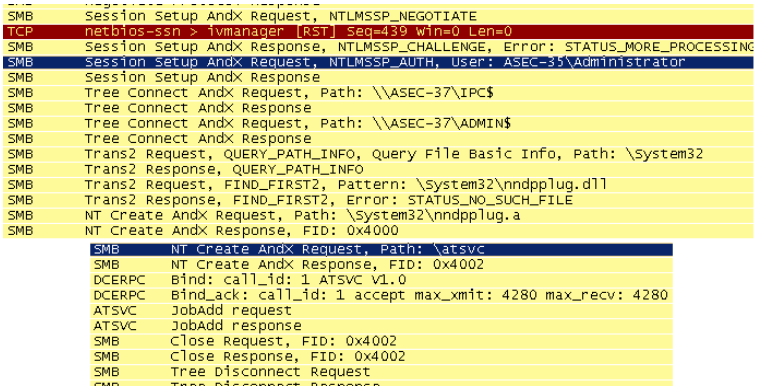
[그림 1-9] MS08-067 취약점을 이용한 공격패킷

해당 취약점 공격 패킷 속에 내포된 쉘코드(ShellCode)는 기본적으로 XOR 인코딩 되어 있고 외부의 다른 감염된 컴퓨터로부터 악성프로그램을 다운로드 할 수 있는 기능을 갖는다.

이렇듯 콘피커 웜에 의해 감염이 되면, 전파를 위해 랜덤으로 생성된 포트 주소로 웹 서버를 생성하게 된다.(추후 감염된 시스템이 이 웹 서버를 통해 자신을 다운로드 한다.)

http://xxx.xxx.xxx.xxx:3193/zbrlw

또 다른 전파 형태로 [그림 1-10]과 같은 공유 폴더를 이용한 전파 방법이 있다.



[그림 1-10] 공유 폴더를 이용한 전파

일단 콘피커 웜은 단순한 패스워드인 “0000”,”1111”,”admin” 등 225개 정도의 패스워드를 사용한다. 만약, 웜이 사용하는 취약한 패스워드를 사용하고 있는 시스템이 발견되면 관리자 권한의 숨은 공유인 “ADMIN$” 폴더로 접근하여 다음과 같은 형태로 자기 자신을 복사하게 된다.

[Share Machine Name]₩ADMIN$₩System32₩[Random File Name]

그 후 복사한 악성코드 파일을 실행시키기 위해 “예약 작업(ATSVC)”을 통해 특정 시간에 동작하도록 스케쥴에 등록한다. 또한, 콘피커 웜은 DNS 관련 함수를 메모리 상에서 패치하여, 백신, 보안 프로그램을 비롯하여 윈도우 업데이트를 방해하는 방법으로 자기 자신을 보호하기도 한다.

(2) 콘피커 웜 대처법

이처럼 콘피커 웜은 다양한 전파 방법과 자기 보호 방법을 갖고 있어 대처가 매우 까다롭다. 해당 콘피커 웜에 대한 대처방안으로 다음과 같은 방법을 참고할 수 있다.

첫 번째, 가장 근본적으로 웜이 사용하는 MS08-067 취약점에 대한 패치를 업데이트한다.

(1) MS08-067 취약점 패치 업데이트(아래 사이트 참조).
(영문) http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
(한글) http://www.microsoft.com/korea/technet/security/Bulletin/MS08-067.mspx

두 번째, 강력한 패스워드를 설정하고 불필요하다면 아래 방법을 통해 공유 폴더를 통한 확산을 방지하기 위해 공유를 제거한다.

(1) V3 제품에서 제공하는 방화벽 기능을 이용한 정책 설정 :
해킹차단 - 개인방화벽- 공유 규칙 - 직접접속 정책 사용(V3IS2007 기준)

(2) 수동으로 공유 폴더 제거하는 방법 :
설정 - 제어판 - 관리도구 - 컴퓨터 관리 - 공유폴더 클릭 후 나열된 숨김 공유 중 선택 후 우측 클릭하여 공유해제 적용. 재 부팅 시에는 숨김 공유가 재 활성화될 수 있기 때문에 아래와 같이 직접적인 레지스트리를 수정하여 재활성화를 방지할 수 있다. (* Windows 2000 시스템 기준)

① 레지스트리 편집기 실행 ([시작] →[실행]→regedit32 입력 후 Enter)
② 폴더 선택(KEY_LOCAL_MACHINE을 선택하여 “₩” 내부에 있는 항목 순으로 확장)
③ 키 수정 또는 생성하기
위치: KEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services ₩lanmanserver₩parameters
Value Name: **AutoShareWks** (Windows 2000 pro일 경우)
Value Name: **AutoShareServer** (Windows 2000 Server일 경우)
Type: **REG_DWORD**

Value: 0

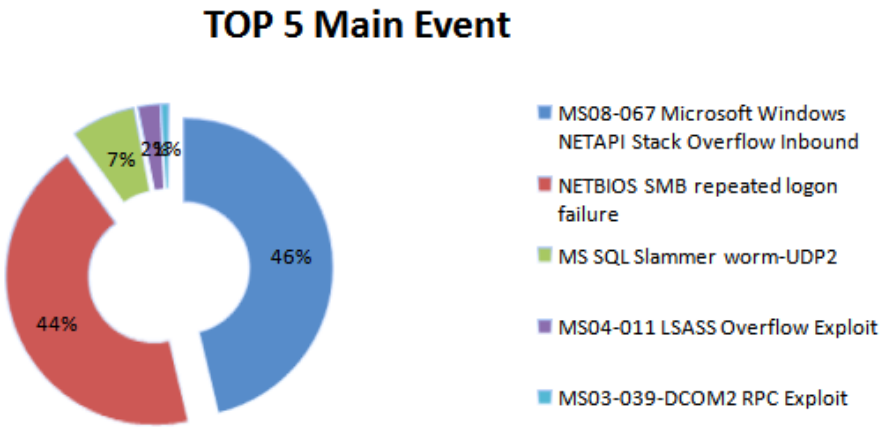
④ KEY_LOCAL_MACHINE을 선택하여 "₩" 내부에 있는 항목 순으로 확장하여 위의 값을 생성.

⑤ 레지스트리 편집기를 종료하고 재부팅하여 확인.

이 외에도 조직의 정책에 따라 다양한 보안 프로그램을 통해 해당 139/TCP, 445/TCP 포트 차단 정책을 적용하거나 원격 파일 복사 및 원격 스케쥴링 작업 등을 차단하는 방법도 고려할 수 있다.

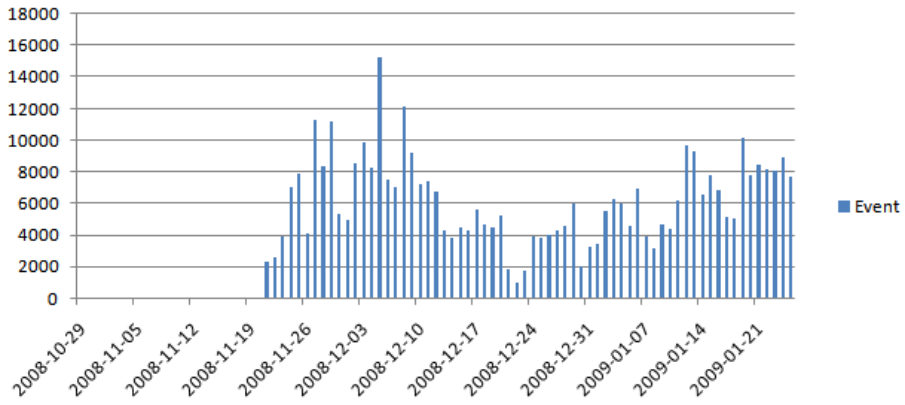
4. 네트워크 모니터링 현황 – 콘피커 웜의 확산

1월 한 달간 자사의 네트워크 모니터링 시스템으로부터 상위 TOP5 주요 이벤트들이 [그림 1-11]과 같이 탐지되었다. 지난 10월 말 MS08-067 서버 서비스 취약점에 발표된 이후, 다음과 같이 최상위 탐지 이벤트는 항상 해당 취약점을 이용하는 탐지 이벤트(MS08-067 MS Windows NETAPI Stack Overflow Inbound)가 차지하고 있다.



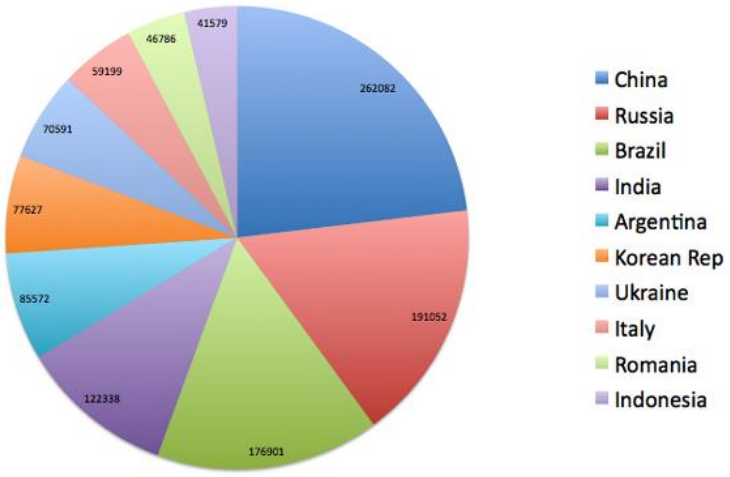
[그림 1-11] 주요 탐지 이벤트 현황 TOP 5

MS08-067 취약점이 본격적으로 콘피커 웜으로 발전하고 확산되면서 모니터링 시작 이후 평균 5600건 이상의 탐지 트래픽이 몇 개월 동안 꾸준히 탐지되고 있다. 이미 해당 취약점에 대한 MS 보안 패치가 배포되었음에도 불구하고, 콘피커 웜이 이용하는 방식(공유 취약점, USB를 통한 확산)의 높은 효과성으로 인하여 그 피해가 감소되지 않고 있다. 당분간 활용될 새로운 취약점이 발표되기 전까지 해당 콘피커 웜의 트래픽 발생은 지금 상태를 꾸준히 유지할 것으로 예상된다.



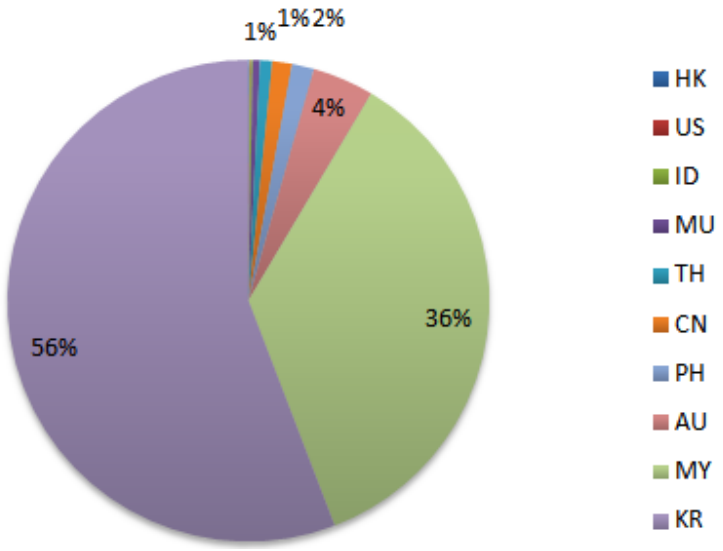
[그림 1-12] 콘피커 웜 트래픽

현재 자사를 비롯하여 많은 보안업체들이 콘피커 웜이 사용하는 다운로드 도메인이나 트래픽을 꾸준히 모니터링하고 있다. [그림 1-13]은 전세계를 대상으로 국가별 콘피커 웜의 피해현황을 나타낸 그래프이다. 모니터링 환경에 따라 다소 차이는 있을 수 있으나 중국과 러시아가 가장 큰 피해를 보이고 있으며, 국내 피해 또한 TOP 6에 올라있다.



[그림 1-13] 콘피커 웜 국가별 피해 현황 TOP 10 (출처: cymru.com)

[그림 1-14]는 자사의 네트워크 모니터링 시스템을 통해 탐지된 콘피커 웜 공격 트래픽을 국가별로 확인한 결과이다. 탐지 시스템의 지역적 특성을 감안하고, 탐지 트래픽의 소스 IP 주소만을 기준으로 하면 국내에서 발생되는 웜 트래픽이 50% 이상을 차지하고 있다. 해당 발생지는 기업체가 아닌 대부분 ISP 업체가 제공하는 동적 할당 IP들로 보안이 허술한 다수의 일반 사용자 PC를 통해 웜이 확산되고 있는 것으로 추정된다.



[그림 1-14] 콘피커 웜 국가별 공격 트래픽

탐지되는 콘피커 웜(Conficker) 웜 트래픽은 큰 형태적인 변화 없이 내부의 다운로드 URL을 XOR 쉘코드(Shellcode)형태로 가지고 있다. 당분간은 새로운 변형보다는 기존에 배포된 웜이 자가 확산을 하는 형태가 될 것으로 예상된다.

5. 중국 보안 이슈 – 2008년 악성코드 동향

(1) 지앙민 (JiangMin, 江民)의 2008년 악성코드 동향

중국 로컬 보안 업체 중 하나인 지앙민(JiangMin, 江民)에서 2008년 1년 동안 많은 피해를 입혔거나 새로 많이 발견된 악성코드에 대한 통계 데이터를 제공하였다. 이 통계 데이터는 2008년 한 해 동안 지앙민에서 집계한 악성코드 데이터에 기반하며 본 글을 쓰는 현재까지는 지앙민의 공식적인 2008년 동향 분석 리포트가 발표되지 않았음을 참고하기 바란다.

악성코드 명	감염 대수	V3 진단명
Checker/Autorun	903700	TextImage/Autorun
Trojan/PSW.OnlineGames.gen	338933	Win-Trojan/OnlineGameHack
Trojan/PSW.GamePass.Gen	236275	Win-Trojan/OnlineGameHack
Adware/Cinmus.Gen	196540	Win-Dropper/Cinmus
Trojan/PSW.GameDLL.Gen	174340	Win-Trojan/OnlineGameHack
Trojan/PSW.OnLineGames.sss	158563	Win-Trojan/OnlineGameHack
Adware/Yokbar.f	136541	-
Trojan/Ck88866.Gen	130795	-
Exploit.CVE-2007-0071	129330	Win-Trojan/SWF-Exploit.Gen
Trojan/Agent.bwp	92366	Win-Trojan/Agent

[표 1-1] 지앙민(JiangMin, 江民) 2008년 악성코드 TOP 10

[표 1-1]의 지앙민에서 집계한 2008년 악성코드 TOP 10을 살펴보면 2008년 3가지 키워드를 생각 해 볼 수 있다. 첫 번째가 USB 등의 이동형 저장 장치를 통한 악성코드 전파방식의 일반화, 두번째로 온라인 게임의 사용자 정보를 유출하는 악성코드의 대량 감염, 마지막으로 상업적인 애드웨어의 확산으로 들 수 있다.

1위를 차지한 Checker/Autorun은 Autorun 류의 악성코드가 자신을 실행시키기 위해서 생성하는 autorun.inf를 진단한 경우이다. 이러한 텍스트 파일이 1위를 차지하고 있다는 것은 중국 내에서 익히 알려진 바와 같이 autorun.inf를 통해 이동형 저장 장치로 전파되는 감염 기법이 이미 일반화 되었다고 볼 수 있다. 그리고 악성코드 TOP 10에 4 종이 등장 할 정도로 극심한 감염이 이루어지고 있는 온라인 게임 관련 트로이목마는 2007년에 이어서 2008년에도 유사한 양상을 보였다.

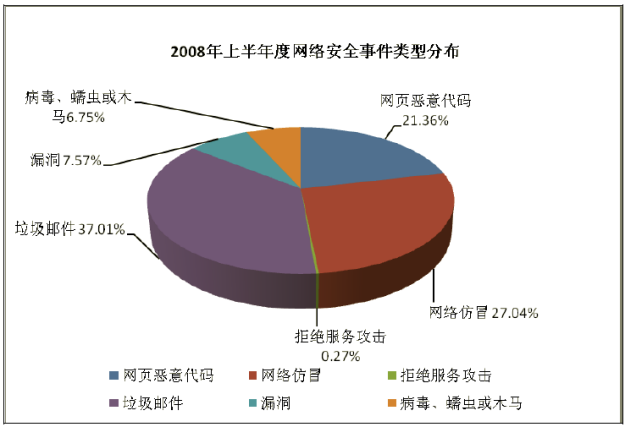
악성코드 명	감염 대수	V3 진단명
Adware/Cinmus.Gen	196556	Win-Dropper/Cinmus
Adware/Yokbar.f	136545	-
Exploit.CVE-2007-0071	129350	Win-Trojan/SWF-Exploit.Gen
TrojanSpy.OnLineGames.fbd	39856	Win-Trojan/OnlineGameHack
Trojan/Agent.aixq	34896	Win-Trojan/Agent
TrojanSpy.OnLineGames.euu	32627	Win-Trojan/OnlineGameHack
TrojanDownloader.JS.Agent.iz	30647	Win-Trojan/Downloader
Rootkit.Vanti.dmc	24617	Win-Trojan/Rootkit
Rootkit.Agent.da	23530	Win-Trojan/Rootkit
Backdoor/Popwin.ch	18339	Win-Trojan/Popwin

[표 1-2] 지앙민(JiangMin, 江民) 2008년 신종 악성코드 TOP 10

지앙민에서 집계한 [표 1-2]의 신종 악성코드 TOP 10을 살펴보면 애드웨어와 Adobe 취약점을 이용한 악성코드로 요약할 수 있다. 먼저 1위와 2위를 살펴보면 모두 상업적인 목적으로 배포되는 애드웨어들이 차지하고 있으며 그 뒤를 이어서 Adobe Flash의 취약점을 악용하는 SWF인 Exploit.CVE-2007-0071이 3위를 차지하고 있다는 것은 중국 내에서도 역시 Adobe Flash의 취약점이 악성코드 유포에 많이 악용되었다는 것을 보여주고 있는 사례라고 할 수 있다.

(2) CNCERT/CC의 2008년 상반기 보안 위협 동향 발표

중국의 대륙내의 보안 사고들을 총괄하는 CNCERT/CC에서 2008년 상반기 보안 위협 동향 보고서를 2008년 11월에 발간하였다. 시기적인 면에서 본다면 그리 적절하지 않으나 2008년 상반기 중국 대륙 내에서 발생한 보안 위협들에 대한 참고 자료로 삼을 수 있다.



[그림 1-15] CNCERT/CC의 2008년 상반기 인터넷 보안 위협 형태

먼저 [그림 1-15]과 같이 CNCERT/CC에서 집계한 2008년 중국 대륙 내에서 발생한 보안 위협 형태를 본다면 스팸메일이 37.01%로 가장 많이 집계 되었으며 그 뒤로 웹 사이트 변조가 27.04% 를 차지하고 있다. 2007년 자료와 비교해본다면 스팸메일은 27%에서 10% 가량 증가한 반면 웹 사이트 변조는 30%에서 3% 가량 감소한 추세를 보였다. 그 외 웹 사이트를 통한 악성코드 유포가 21.36%를 차지하여 2007년보다 5% 가량 감소한 것으로 집계되었다. 그 외 취약점은 7.57%, 악성코드는 6.75% 그리고 서비스 거부 공격은 0.27%로 2007년 전체 집계와 비교하여 큰 변화가 없었던 것으로 분석하였다.

排名	恶意代码名称	总捕获次数
1	Virus.Win32.Virut.n	42873
2	Net-Worm.Win32.Allaple.b	30215
3	Porn-Dialer.Win32.InstantAccess.dan	24435
4	Trojan.Win32.Qhost.aei	20349
5	Backdoor.Win32.VanBot.ax	18793
6	Trojan-Downloader.VBS.Small.gg	18224
7	Backdoor.Win32.SdBot.cpl	16280
8	Net-Worm.Win32.Allaple.e	42873
9	Virus.Win32.Sality.z	30215
10	Backdoor.Win32.EggDrop.au	24435

[표 1-3] CNCERT/CC의 2008년 상반기 악성코드 TOP 10

[표 1-3]은 CNCERT/CC에서 집계한 2008년 상반기 악성코드 TOP 10이다. 중국의 로컬 보안 업체인 라이징(Rising, 瑞星)과 지앙민(JiangMin, 江民)에서 집계한 것과는 많은 차이를 나타내고 있다. 우선 특이한 점은 1위와 9위에는 Virut 바이러스와 Sality 바이러스가 차지하고 있으며 그 외에도 VanBot과 SdBot 류의 악성 IRCBot 류가 2 종류나 순위를 차지하고 있다는 점이다. 그러나 2007년 악성코드 TOP 10에는 6 종이나 포함되어 있던 것과 비교한다면 악성 IRCBot 류의 활동이 많이 감소 한 것으로도 해석 할 수가 있다.

(3) 증가하는 중국 내 악성코드 유포 웹 사이트

2007년부터 웹페이지를 통해 취약한 인터넷 익스플로러를 악성코드 감염 경로로 이용하는 방식이 국내에는 이미 잘 알려져 있는데, 중국 역시 예외가 아니라는 점을 중국 로컬 보안 업체인 라이징(Rising, 瑞星)의 통계를 통해 확인 할 수 있다.

[그림 1-16] 라이징(Rising, 瑞星)이 집계한 웹 사이트를 통한 악성코드 감염 수치

특히 1월 9일 라이징의 홈페이지를 통해 발표한 [그림 1-16]의 통계에 따르면 1월 5일을 기준으로 하여 5,012,052회나 취약한 인터넷 익스플로러를 통한 악성코드 감염 시도가 발생한 것으로 알려져 중국 내에서 웹 사이트를 통한 악성코드의 감염 시도가 심각한 수준임을 알 수 있다. 이러한 라이징의 집계 외에도 중국의 비영리 보안 단체인 Knowledge of Security(知道安全)의 보고에 따르면 1월 한 달 동안 알려진 웹 사이트로만 "흑룡강위생감사국", "북경고시서점"과 "중국은행웹사이트연맹" 등의 총 19 개 웹 사이트가 악성코드 유포지로 밝혀져, 인터넷 익스플로러 취약점을 이용한 악성코드 감염이 전 세계적인 트렌드임을 알 수 있다.

II. ASEC 칼럼

■ 콘피커 웜 Technical Report

2009년 1월에 많은 피해가 발생한 콘피커 웜 중 특히 많은 피해를 일으킨 “Win32/Conficker.wom.173318”를 상세 분석을 통해 전파방법과 기능에 대해 알아보자.

(1) 기능 분석 요약

먼저 기능 분석으로 코드의 난독화와 전파방법, 레지스트리 등록 등에 대해 알아보자.

1) 코드의 난독화

- UPX 실행압축으로 되어져 있으며 압축을 풀고 나면 쓰레기 코드로 쌓여 있음
- 쓰레기 코드 루프를 돌면서 힙할당, 암호화된 코드를 디코딩한 후 메모리에 적재
- CALL [reg]코드를 통해 메모리에 적재한 실행코드로 이동
- 이동한 실행코드 역시 UPX로 압축되어 있음
- UPX를 풀고 나면 정상적인 실행코드로 이동

2) 전파

① MS08-067 취약점을 이용한 원격코드 실행

관련정보 : http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

② 네트워크 공유폴더를 통한 전파

- 취약한 암호의 네트워크 공유폴더(ADMIN$)를 스캔하여 접근시도

* 취약한 암호(일부)

000 11111 1234 2222 aaaaa abc123 academia admin codeword coffee forever freedom lotus nopassword password qqqq shadow share unknown web zzz .....

- 성공 시에 %System% 폴더아래 랜덤 파일명으로 복사본 생성
- 윈도우 시스템 스케쥴러 등록

(rundll32.exe를 이용하여 로딩하도록 AT*.job 파일생성)

- 네트워크 동시접속 제한을 높이기 위해 아래의 기능을 수행

* win2k이하

: 레지스트리값을 최대값으로 설정

HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩Tcpip ₩Parameters₩"TcpNumConnections" = "00FFFFFE"

* XP이상

: TCP/IP 프로토콜의 half-open connections 기능 무력화
tcpip.sys 파일정보와 드라이버 파일을 생성(01.tmp) 및 로딩하여 메모리 패치
(half-open connections 숫자를 0x10000000으로 변경)
생성한 드라이버 파일은 로딩 후 파일 & 레지스트리 삭제

* Vista
: Disable Auto tuning
Command 실행 - "netsh interface tcp set global autotuning=disabled"
관련정보 - http://www.vistax64.com/tutorials/72308-auto-tuning-tcp-ip-receive-level.html)

③ 이동디스크를 통한 전파
- RECYCLER₩S-x-x-x-xxx-xxx-xxx-x₩[Random file name] 파일 생성
(x는 랜덤한 번호)
- 루트 폴더에 Autorun.inf 파일 생성
- 생성된 파일과 폴더는 숨김속성

3) 레지스트리 생성
① 서비스 등록
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩hukic(랜덤명)
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩hukic₩
"DisplayName"=[%DisplayName%]
"Description"=[%Description%]
"ImagePath"="%SystemRoot%₩system32₩svchost.exe -k netsvcs"

HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩hukic
₩Parameters₩"ServiceDll"=[Path to worm]

* %DisplayName%은 아래문자열 중 2개를 임의로 선택하여 등록
Boot Center Config Driver Helper Image Installer Manager Microsoft Monitor Network Security Server Shell Support System Task Time Universal Update Windows

* %Description%은 서비스로 등록 되어진 Description 문자열 중 랜덤하게 하나를 가져와서 등록

② 자동실행 등록

HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion
₩Run₩
"[Random Name]" = "rundll32.exe" "[Random File Name].dll", [Random Value]"

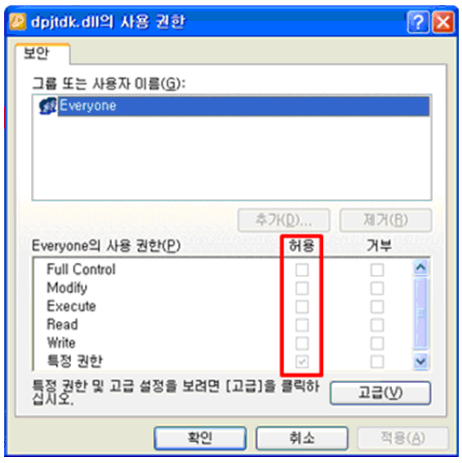
③ 탐색기 -> 폴더옵션 -> 숨김파일 및 폴도 옵션 변경 무력화
SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩explorer₩Advanced
₩Folder₩Hidden₩SHOWALL₩
"CheckedValue"=[DWORD]0

④ Applets 키값을 체크하여 생성
HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion
₩Applets₩"dl" = [REG_BINARY]0
HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion
₩Applets₩"ds" = [REG_BINARY]0
HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion
₩Applets₩"dl" = [REG_BINARY]0
HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion
₩Applets₩"ds" = [REG_BINARY]0

4) 파일 생성(윈도우 버전에 따라 다르게 생성)
- %Program Files%₩Internet Explorer₩[RANDOM FILE NAME].dll
- %Program Files%₩Movie Maker₩[RANDOM FILE NAME].dll
- %System%₩[RANDOM FILE NAME].dll
- %Temp%₩[RANDOM FILE NAME].dll
- C:₩Documents and Settings₩All Users₩Application Data ₩
[RANDOM FILE NAME].dll

* 생성되는 파일은 kernel32.dll 시간과 동일하게 변경됨

5) 생성한 파일 및 레지스트리 보안 속성 변경(NTFS)
- InitializeAcl, AddAccessAllowedAce, SetSecurityDescriptorDacl, SetFileSecurityA 등의 API 사용
- Read 권한을 삭제하여 파일/레지스트리 읽기 불가(진단 무력화)



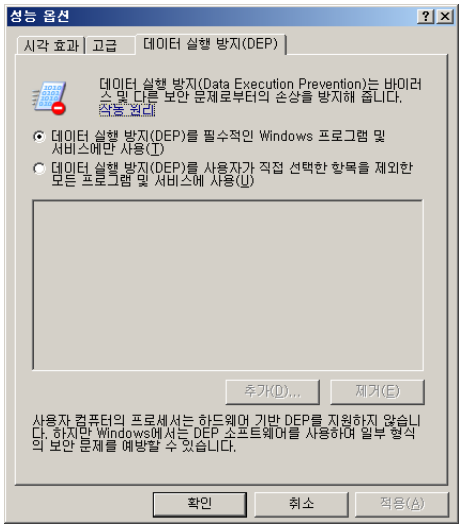
[그림 2-1] 생성된 복사본의 파일 보안 속성

6) 시스템 복원으로부터 복원지점 모두 삭제
- SrClient.ResetSR API 사용

7) 시스템 서비스 종료 및 설정 변경 (StartType = SERVICE_DISABLED)
- wuauserv : Windows Automatic Update Service
- BITS : Background Intelligent Transfer Service

8) Dll 인젝션(윈도우 버전에 따라 다름)
- svchost.exe -k NetworkService
  : ZwQueryInformationProcess API와 PEB 정보를 사용하여 프로세스 파라메타 구함
- explorer.exe
- services.exe

9) DEP(Data Execution Prevention) Mode off로 설정
- 관련 정보 : http://support.microsoft.com/kb/875352
- ZwSetInformationProcess(with flag 0x22) API 사용



[그림 2-2] DEP 속성보기

10) API Hooking

- ntdll.ZwQueryInformationProcess
  : DEP Query 정보 변경
- netapi32.NetpwPathCanonicalize
  : MS08-067 취약점에서 Exploit Code가 실행 안되게 Name Length를 체크하는 코드로 변경되어 실행됨
  : Exploit Code에서 복사본을 다운로드하기 때문에 중복 감염 방지
- dnsapi.DnsQuery_A, DnsQuery_UTF8, DnsQuery_W, Query_Main
  : 특정 URL 접속 불가

* 접속 불가 판별 문자열(일부분)

virus rootkit defender microsoft symantec norton mcafee trendmicro sophos panda etrust f-secure kaspersky f-prot nod32 eset drweb ahnlab esafe avast avira hauri ikarus k7computing avp avg ...

11) HTTP 서버 구축 (Port : Random)

- MS08-067 취약점 공격이 성공한 다른 컴퓨터에서 Exploit Shell Code가 실행되면 여기서 구축된 HTTP 서버로 접속하여 복사본을 다운받아 실행됨
- External IP 주소를 얻기 위해 아래의 사이트에 접속
  http://checkip.dyndns.org
  http://getmyip.co.uk
  http://www.getmyip.org
  http://www.whatsmyipaddress.com
- 취약점 공격이 성공한 다른 컴퓨터에서 다운받는 확장자는 다음과 같음

.bmp .gif .jpeg .png

12) 특정 URL에서 다른 악성코드를 다운로드

- 아래의 사이트 중 하나에 접속한 후 시스템 날짜를 Query하여 년/월/일/요일 숫자를 이용해 Domain Name 생성(같은 날짜에는 같은 domain이 만들어짐)
  (myspace.com, msn.com, ebay.com, cnn.com, aol.com, ask.com, yahoo.com, google.com, baidu.com)
- 생성되는 Domain Name의 예
  "vhqlkddd.org"
  "nxipfrpw.net"
  "pzaumio.cc"
  "vvnjxapnfz.org"
  "fhdduq.info"
  "liiekfx.biz"
  "shujuaji.com"
  "qfjvcoz.org"
  ...
- 10개의 스레드를 반복적으로 만들어 다운로드 시도
  (http://DomainName(Gernerated)/search?q=%d)
- 다운받아지는 파일형태는 [Random File Name].tmp

(2) 상세 코드 분석

상세 코드 분석을 통해 세부 기능을 어떻게 구현하는지 알아보자.(지면 한계로 인해 주요 기능 코드만 언급한다.)

1) DEP(Data Execution Prevention) Mode off 설정

```
0087D036  PUSH    4
0087D038  MOV     DWORD PTR SS:[EBP-4], EAX
0087D03B  LEA     EAX, DWORD PTR SS:[EBP-4]
0087D03E  PUSH    EAX
0087D03F  PUSH    22
0087D041  PUSH    -1
0087D043  CALL    DWORD PTR SS:[EBP-8]      ntdll.ZwQueryInformationProcess
```

[그림 2-3] ZwSetInformationProcess(with flag 0x22) 호출

2) API Hooking(ntdll.ZwQueryInformationProcess)

- ZwQueryInformationProcess 주소에 JMP Code 5바이트를 패치하여 자신의 코드로 점프

```
0087B3B8  PUSH    5
0087B3BA  LEA     EAX, DWORD PTR SS:[EBP-40]
0087B3BD  PUSH    EAX
0087B3BE  PUSH    DWORD PTR SS:[EBP+8]
0087B3C1  CALL    0088822C                    JMP to msvcrt.memcpy

0006F3D4  7C93E01B  dest = ntdll.ZwQueryInformationProcess
0006F3D8  0006F3EC  src = 0006F3EC
0006F3DC  00000005  n = 5
```

[그림 2-4] ZwQueryInformationProcess 주소 5바이트 패치

```
7C93E01B ZwQueryInformationProcess  JMP     0087ADCD
7C93E020                            MOV     EDX, 7FFE0300
7C93E025                            CALL    DWORD PTR DS:[EDX]
7C93E027                            RETN    14
```

[그림 2-5] 5바이트가 패치된 ZwQueryInformationProcess 주소

3) Dll 인젝션

- svchost.exe -k netsvcs 프로세스를 찾아서 LoadLibray, WriteProcessMemory API 사용으로 강제 dll 인젝션

```
0087CCF4  PUSH    874424                    ASCII "LoadLibraryA"
0087CCF9  PUSH    8743D4                    ASCII "kernel32.dll"
0087CCFE  CALL    EDI
0087CD00  MOV     EBX, DWORD PTR DS:[871130]  kernel32.GetProcAddress
0087CD06  PUSH    EAX
0087CD07  CALL    EBX                       kernel32.GetProcAddress
0087CD09  MOV     DWORD PTR SS:[EBP-C], EAX
0087CD0C  LEA     EAX, DWORD PTR SS:[EBP-1C]
0087CD0F  PUSH    EAX
0087CD10  INC     ESI
0087CD11  PUSH    ESI
0087CD12  PUSH    DWORD PTR SS:[EBP+C]
0087CD15  PUSH    DWORD PTR SS:[EBP-8]
0087CD18  PUSH    DWORD PTR SS:[EBP-14]
0087CD1B  CALL    DWORD PTR DS:[8711F0]     kernel32.WriteProcessMemory
0087CD21  TEST    EAX, EAX
0087CD23  JE      0087CE19
0087CD29  LEA     EAX, DWORD PTR SS:[EBP-20]
0087CD2C  PUSH    EAX
0087CD2D  XOR     ESI, ESI
0087CD2F  PUSH    ESI
0087CD30  PUSH    DWORD PTR SS:[EBP-8]
0087CD33  PUSH    DWORD PTR SS:[EBP-C]
0087CD36  PUSH    ESI
0087CD37  PUSH    ESI
0087CD38  PUSH    DWORD PTR SS:[EBP-14]
0087CD3B  CALL    DWORD PTR DS:[8711EC]     kernel32.CreateRemoteThread
0087CD41  CMP     EAX, ESI

Address   Hex dump                          ASCII
0088AE68  45 3A 5C 56 33 57 6F 72 6B 5  E:¥V3Work¥Cor
0088AE78  65 72 5F 77 6F 72 6D 5C 63 6  er_worm¥conf
0088AE88  00 00 00 00 00 00 00 00 00 0  ..........
0088AE98  00 00 00 00 00 00 00 00 00 0  ..........

0006F3E4  hProcess = 00000078
0006F3E8  Address = 920000
0006F3EC  Buffer = 0088AE68
0006F3F0  BytesToWrite = 22 (34.)
0006F3F4  pBytesWritten = 0006F424
```

[그림 2-6] Dll 강제 인젝션

4) TCP/IP 프로토콜의 half-open connections 기능 무력화

```
00877E69 CALL    DWORD PTR DS:[8710B8]          kernel32.GetSystemDirectoryA
00877E6F PUSH    ESI
00877E70 PUSH    8725E4                         ASCII "\drivers\tcpip.sys"
00877E75 LEA     EAX, DWORD PTR SS:[EBP-128]
00877E7B PUSH    EAX
00877E7C CALL    DWORD PTR DS:[8712C4]          msvcrt.strncat
00877E82 MOV     BYTE PTR SS:[EBP-25], 0
00877E86 LEA     EAX, DWORD PTR SS:[EBP-128]
00877E8C PUSH    EAX
00877E8D LEA     EAX, DWORD PTR SS:[EBP-20]
00877E90 PUSH    EAX
00877E91 CALL    0087C769                       Find data in tcpip.sys

0087807B CALL    DWORD PTR DS:[871124]          kernel32.WriteFile
00878081 TEST    EAX, EAX
008780CC PUSH    872608                         ASCII "\\.\TcpIp_Perf"
008780D1 CALL    ESI

008780EB PUSH    ESI
008780EC CALL    DWORD PTR DS:[871120]          kernel32.DeviceIoControl
008780F2 TEST    EAX, EAX
```

[그림 2-7] tcpip.sys 정보를 이용하여 드라이버 파일 생성 및 로딩

5) 특정 사이트에 시간을 Query하여 숫자를 기반으로 다운로드 받을 Domain Name 생성

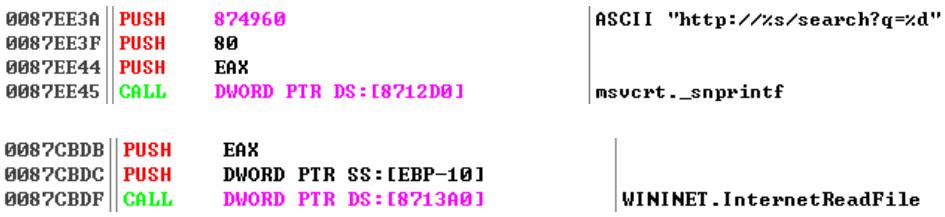
```
0087EB25 PUSH    EBX
0087EB26 PUSH    DWORD PTR SS:[EBP+8]
0087EB29 PUSH    EAX
0087EB2A CALL    DWORD PTR DS:[8713A4]          WININET.InternetOpenUrlA
0087EB30 MOV     EDI, EAX
0087EB32 CMP     EDI, EBX
0087EB34 JE      SHORT 0087EB91
0087EB36 PUSH    ESI
0087EB37 MOV     ESI, DWORD PTR DS:[8713A8]     WININET.HttpQueryInfoA

0006E558  0006EDDC ASCII "http://www.baidu.com"
0006E9A8 54 68 75 2C 20 30 35 20 46 65 62 20 32 30 30 39 Thu, 05 Feb 2009
0006E9B8 20 30 30 3A 34 38 3A 34 39 20 47 4D 54 00 06 00  00:48:49 GMT_-.
```

[그림 2-8] 특정 사이트에서 시스템 날짜 Query

```
0087EF7A MOV     EAX, DWORD PTR SS:[EBP-28]
0087EF7D MOV     BYTE PTR DS:[EAX+EBX], DL      Save string
0087EF80 INC     DWORD PTR SS:[EBP-28]
0087EF83 JMP     SHORT 0087EF60
0087EF85 MOV     BYTE PTR DS:[EBX+ESI], 0
0087EF89 CALL    0087ED54
0087EF8E AND     EAX, 7
0087EF91 PUSH    DWORD PTR DS:[EAX*4+88AD70]
0087EF98 PUSH    DWORD PTR SS:[EBP+EDI*4-488]
0087EF9F CALL    00888238                       JMP to msvcrt.strcat

0006EE28  000C50F0 ASCII "idgfmfssgab.com"
0006EE2C  000CA348 ASCII "cerwsrh.biz"
0006EE30  000C4D40 ASCII "ibzoerucq.cn"
0006EE34  000C8F88 ASCII "iiipoqk.cc"
0006EE38  000C8FC0 ASCII "xlkuacxbcvv.ws"
0006EE3C  000C8FF8 ASCII "eibzfk.org"
0006EE40  000C4ED8 ASCII "mqeqdad.org"
0006EE44  000C4F10 ASCII "dheyrizjy.cc"
0006EE48  000C4F48 ASCII "zlgawvn.ws"
0006EE4C  000C4F80 ASCII "hqmig.ws"
0006EE50  000C4FB8 ASCII "zjchlyi.org"
0006EE54  000C4FF0 ASCII "qautntgf.cn"
0006EE58  000C9D28 ASCII "hnmqwui.cc"
0006EE5C  000C9D60 ASCII "ctpakvlnsm.com"
0006EE60  000C9D98 ASCII "hisyrxosw.net"
0006EE64  000C9DD0 ASCII "tlwosy.info"
```



[그림 2-9] 생성한 Domain Name 생성 및 Domain Name에 접속하여 파일 다운로드 시도

III. 이달의 통계

1. 악성코드 – OnlineGameHack의 활동 뚜렷

(1) 1월 악성코드 통계

순위		악성코드명	건수	비율
1	-	Win-Trojan/Agent.67678	13	16.5%
2	new	Win-Trojan/Xema.variant	11	13.9%
3	new	Win-Trojan/SpamMailer.349696	10	12.7%
4	new	Win-Trojan/Buzus.224256	8	10.1%
4	new	Win-Trojan/Fakealert.85504.B	8	10.1%
5	new	Dropper/Autorun.171298	6	7.6%
5	new	Dropper/OnlineGameHack.171283	6	7.6%
5	new	Win-Trojan/Agent.175644	6	7.6%
5	new	Win-Trojan/Downloader.10240.LD	6	7.6%
10	new	Dropper/OnlineGameHack.33280.D	5	6.3%
합계			**79**	**100%**

[표 3-1] 2009년 1월 악성코드 피해 Top 10

[표 3-1]은 2009년 1월 악성코드로 인한 피해 신고 Top 10이다. 10위까지의 악성코드 종류를 살펴보면 모두 Trojan류이며, Win-Trojan/Agent.67678는 지난달과 마찬가지로 1위를 유지하고 있다. 이 악성코드는 Bagle 악성코드로 인해 생성되며 악성 Rootkit 드라이버를 설치하여 해당 Win-Trojan/Agent.67678를 보호하여 치료를 방해하는 특징을 가지고 있어, 완전한 치료를 위해서는 다음과 같이 치료하여야 한다

① Bagle 전용백신으로 해당 Win-Trojan/Agent.67678를 보호하는 악성 Rootkit 드라이버(파일명: srosa.sys)를 진단 삭제 후 시스템을 재 부팅한다.
② 시스템 재 부팅 후 V3 제품으로 치료해야 해당 악성코드에 관련된 파일이 모두 치료 가능하다.

온라인게임 관련 악성코드가 여전히 기승을 부리는 것에 대해서 이전 ASEC 리포트를 통해 여러 번 강조한 바 있다. 마찬가지로 1월에도 OnlineGameHack이 Top 10에서 두 자리나 차지하고 있다. 이는 한국 온라인 게임 뿐만 아니라 온라인 게임관련 악성코드의 제작지로 잘 알려져 있는 중국 내에서도 자국의 온라인게임 관련 사용자 정보를 취득하기 위한 악

성코드 등장이 수그러들지 않고 있는 것이 가장 큰 이유로 판단된다.

순위		악성코드명	건수	비율
1	↑2	Win-Trojan/OnlineGameHack	577	30.6%
2	↓1	Win-Trojan/Agent	417	22.1%
3	↑4	Win-Trojan/Downloader	179	9.5%
4	↓2	Dropper/OnlineGameHack	141	7.5%
5	new	Win32/Kido.worm	125	6.6%
5	↑7	Win-Trojan/Xema.variant	125	6.6%
7	↑9	Win-Trojan/Zlob	107	5.7%
8	new	Win32/Conficker.worm	77	4.1%
9	↓6	Win32/Autorun.worm	71	3.8%
10	↓5	Dropper/Agent	64	3.4%
합계			**1,883**	**100.0%**

[표 3-2] 2009 1월 악성코드 대표진단명 Top 10

[표 3-2]는 악성코드 동일한 대표진단명을 가진 변종 악성코드를 하나로 묶어서 대표진단명 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 작성된 것이다. 대표진단명 Top 10에 포함된 악성코드 총 피해건수는 1,883건으로 12월의 2,667건에 비해 소폭 감소하였다.

1월 악성코드 대표진단명 Top 10을 살펴 보면 OnlineGameHack이 1위와 4위를 차지하고 있으며, 그 비율을 합치면 38.1%로 전체 Top 10 피해건수의 1/3이상이다

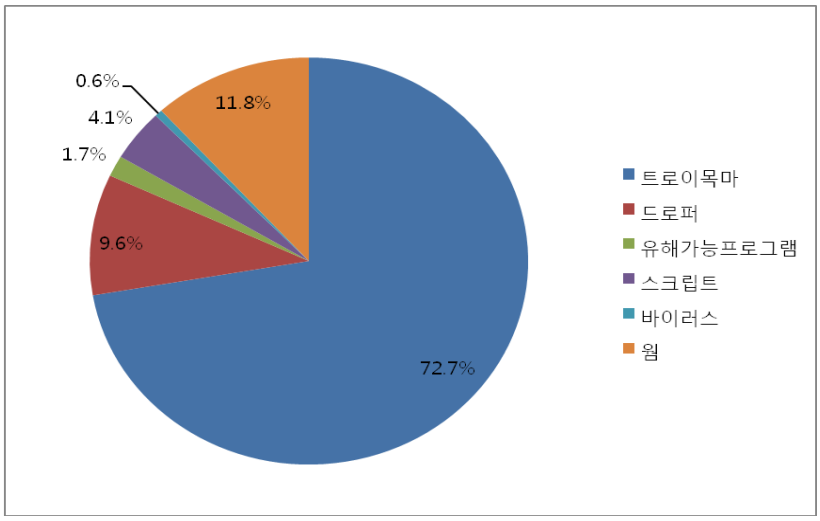
이에 OnlineGameHack의 유포되는 방법에 주목할 필요가 있다. OnlineGameHack은 `크로스 사이트 스크립트(Cross site script)' 공격으로 해킹된 웹사이트를 통해 주로 유포된다. 해킹된 웹사이트는 해당 악성코드를 유포하는 숙주 역할을 하며, 해킹 당한 웹사이트에 접속한 시스템은 인터넷 익스플로러의 취약점을 통하여 악성코드가 설치된다. 만약 해킹 당한 사이트가 인지도 높은 사이트일 경우 확산력도 함께 높아지는 특징을 갖는다. 보안패치를 설치하지 않은 사용자들은 자기도 모르는 사이 감염되며, 이런 종류의 피해를 막기 위해서 최신 보안패치와 함께 최신 버전의 백신프로그램으로 실시간 감시 기능을 사용하는 습관이 필요하다.

또한 TOP10에 2 종의 웜(Win32/Kido.worm, Win32/Conficker.worm)이 신규 진입하였다.

Win32/Kido.worm, Win32/Conficker.worm는 Server Service의 원격코드 실행 취약점(MS08-067)이 공개됨에 따라 해당 취약점을 이용한 악성코드이다.

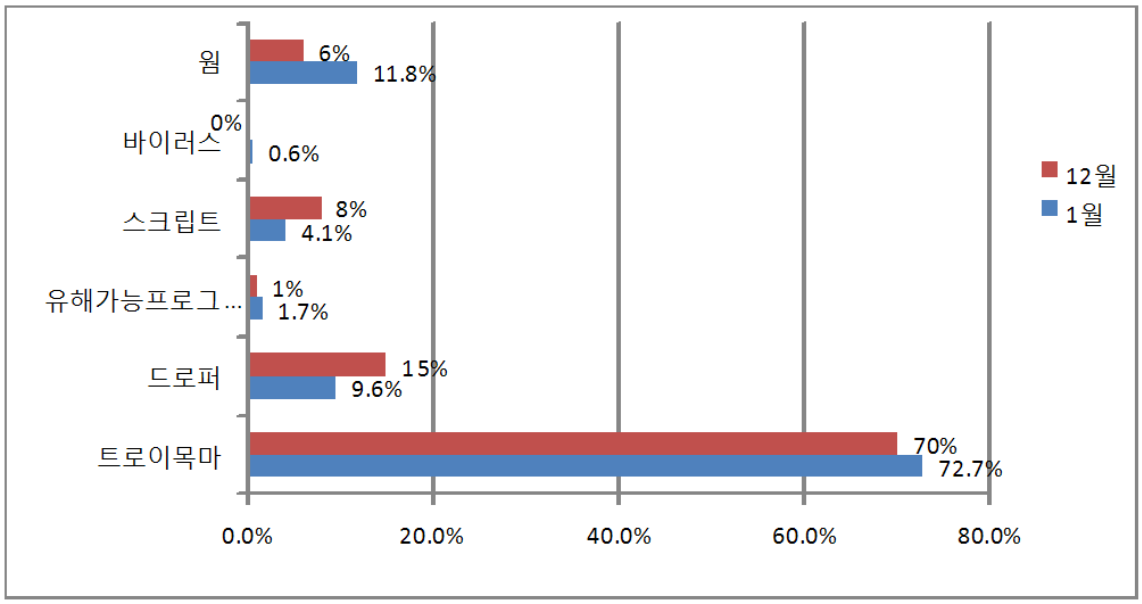
Win32/Conficker.worm은 작년 10월부터 꾸준히 늘어나고 있었으나 1월에 발견된 변형은 백신 프로그램의 진단을 방해하는 기능(파일의 속성과 권한 변경)이 추가되어 악성코드 대응 시 많은 어려움을 겪었다. 이러한 악성코드 치료를 위해 Win32/Conficker.wom 전용백신을 별도 제작 하였으며 해당 전용 백신은 안랩닷컴 전용백신 페이지[1]에서 다운받아 사용할 수 있다.

아래의 [그림 3-1]는 2009년 1월 전체 악성코드 유형별 피해신고 건 수를 나타내고 있는 그래프이다. 트로이 목마 프로그램이 72.7%의 점유율을 보이고 있는 악성코드 유형별 피해신고 부문에서는 드롭퍼와 웜이 각각 9.6%와 9.1%를 차지하고 있으며, 그 뒤를 스크립트 4.1%, 유해가능 프로그램이 1.7%를 차지하고 있다.



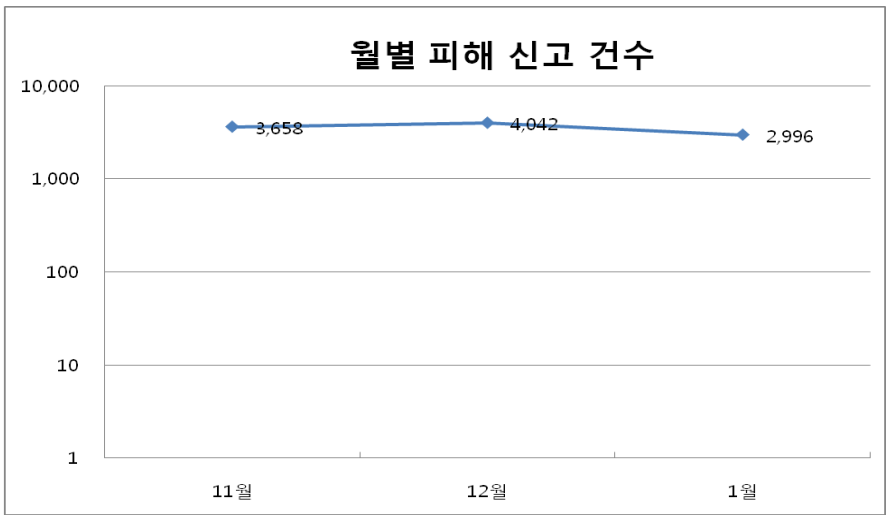
[그림 3-1] 2009년 1월 악성코드 유형별 피해신고 비율

[1] 전용백신 제공 URL : http://kr.ahnlab.com/dwVaccineView.ahn?num=80&cPage=1



[그림 3-2] 2009년 1월 악성코드 유형별 피해신고 비율 전월 비교

[그림 3-2]는 전월과 비교한 악성코드 유형별 피해신고를 나타낸 것이다. 증가한 것은 트로이목마의 경우 전월에 비해 2.7%가 늘어난 72.7%이며, 웜은 전월에 비해 5.2%가 늘어난 11.8%이다. 웜이 늘어난 것은 앞에서 언급된 MS08-067을 이용한 콘피커 웜의 증가와 연관된 것으로 보인다. 드로퍼와 스크립트는 전월에 비해 각각 소폭으로 줄어 들었으며, 유해가능 프로그램과 바이러스는 약간의 수치 차이는 있으나 전월과 많은 차이가 없다.



[그림 3-3] 월별 피해신고 건수

[그림 3-3]은 월별 피해신고 건수를 나타내는 그래프로 작년 11월에서 12월까지 소폭 증가하다가 올해 1월에는 다소 감소하였다. 온라인게임핵, 콘피커 등 악성코드의 상당수가 중

국발인 것을 감안하면, 춘절 연휴의 영향도 반영된 것으로 보인다.

악성코드의 유형이 점차 은폐형 악성코드 및 최신 취약점을 이용하는 악성코드가 늘어남에 따라 피해를 막기 위해서 최신 보안패치와 함께 최신 버전의 백신프로그램으로 주기적으로 검사하는 습관이 필요하다.

(2) 국내 신종(변형) 악성코드 발견 피해 통계

1월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 3-3] 과 같다.

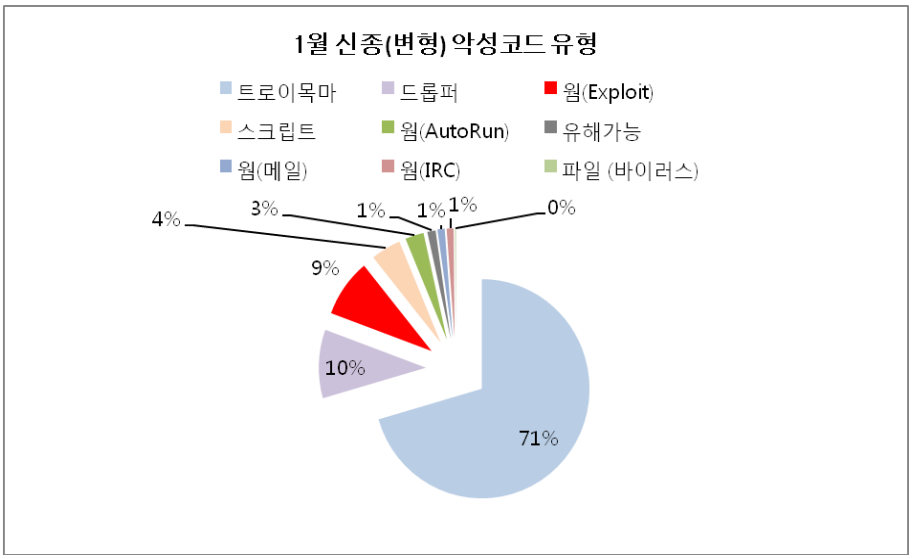
월	트로이목마	드롭퍼	스크립트	웜	파일	유해가능	합계
11 월	1162	197	151	57	19	6	1592
12 월	1431	370	263	85	3	23	2175
01 월	1361	195	87	260	3	24	1930

[표 3-3] 2008 ~ 2009년 최근 3개월 간 유형별 신종 (변형) 악성코드 발견 현황

이번 달 신종 및 변형 악성코드는 전월에 대비하여 11% 감소를 하였다. 위 [표 3-3]에서 알 수 있듯이 트로이목마, 드롭퍼, 스크립트 유형에서 소폭 감소를 하였다. 그러나 그 동안 1월 에 발견된 신종 및 변형 악성코드의 수치로서는 최고치이다. 작년 동월대비 해서는 14% 정도 상승한 수치이다. 전통적으로 방학이 있는 여름과 겨울에는 악성코드의 발견율이 증가하는 편이다. 이것은 이 시기 동안 컴퓨터(인터넷 접속, 온라인 게임 등) 사용자들이 많아지기 때문에 신고 및 수집율이 높은 편이라 할 수 있다.

이번 달 신종 및 변형 악성코드 발견율에서는 근래 들어서 볼 수 없었던 웜 유형의 급격한 증가율을 확인을 할 수가 있다. 이는 모두 한 가지 악성코드의 폭발적인 변형에 의한 수치인데 바로 작년 10월 알려진 윈도우 서버 서비스 취약점 (MS08-067)을 이용한 콘피커 웜이라고 명명된 악성코드가 그 원인이다. 웜 유형의 58%를 이 웜이 차지 하고 있다. 콘피커 웜은 이미 취약점이 알려진 후 얼 마 되지 않아서 이를 이용한 악성코드가 나왔으나 당시의 악성코드는 이번 변형처럼 큰 피해를 입히지 못하였다. 특히 이 웜은 자신을 전파시키는 방법이 다양하고 정확하게 발전됨에 따라 많은 감염 피해가 발생한 것으로 보인다. 또한 서버 측면의 다형성 방법[1] (Server Side polymorphism)을 사용하여 매번 코드를 변형하여 백신에 의한 탐지를 회피하려고 한다.
다음은 이번 달 악성코드 유형을 상세히 분류 하였다.

[1] Server Side polymorphism, 악성코드 제작자들은 안티 바이러스 탐지를 회피하기 위하여 악성코드를 손쉽게 수정하는데, 일반적으로 웹을 이용하여 다운로드 요청이 있을 때 웹 서버에서는 악성코드를 수정하는 프로그램을 이용하여 악성코드를 수정 한 뒤 다운로드 하도록 하는 기법.



[그림 3-4] 2009년 01월 신종 및 변형 악성코드 유형

트로이목마 유형은 전월 대비 5% 소폭 감소하였다. 감소의 원인은 온라인 사용자 계정을 탈취하는 유형에서 감소가 있었다. 그리고 일부 온라인 게임 악성코드는 안티 바이러스의 진단을 회피하기 위하여 실행압축 한 변형된 NsAnti (Anti007) 가 서서히 증가하는 추세에 있다. 특히 해당 실행압축을 사용하는 트로이목마 유형은 국내에 잘 알려진 백신 파일들을 삭제하여 정상적으로 동작하지 못하도록 하므로 주의가 요구 된다.

지난 12월 국내에 급격히 증가한 Win-Trojan/DNSChanger 역시 이번 달에도 변형이 꾸준히 발견되었다. 또한 가짜 백신이 다시 꿈틀거리면서 Win-Trojan/FakeAlert, Win-Trojan/Fraudload, Win-Trojan/FraudPack 류의 증가도 눈에 띄게 증가 하였다. 더블어 Win-Trojan/Vundo, Win-Trojan/Zlob도 변형이 꾸준히 발견되었는데 특히 Win-Trojan/Vundo는 전월 대비 65% 상승하였는데, 이는 모두 앞서 언급한 가짜 백신의 증가와 관련이 있다. 이외에도 은폐형 스팸 메일러류와 은폐에 이용된 루트킷 형태의 증가도 우리를 바짝 긴장시키고 있다.

드롭퍼 유형은 늘 그렇듯이 대부분 온라인 게임의 사용자 계정을 탈취하는 형태가 가장 많은 군집을 이루고 있다. 특이한 점은 위에서 설명한 변형 된 NsAnti가 사용된 드롭퍼 유형들이 이번 달 가장 많이 발견, 보고된 Top 10에 2종이 포함 되어 있다는 것이다. 따라서 한동안 해당 유형의 악성코드는 당분간 증가할 것으로 보인다.

앞서 언급 했듯이 웜 유형중 Exploit를 이용하여 자신을 전파하는 형태로 분류 하였을 때 전체 악성코드 비율중 콘피커 웜은 무려 9%를 차지할 만큼 이번 달 폭발적인 변형이 발

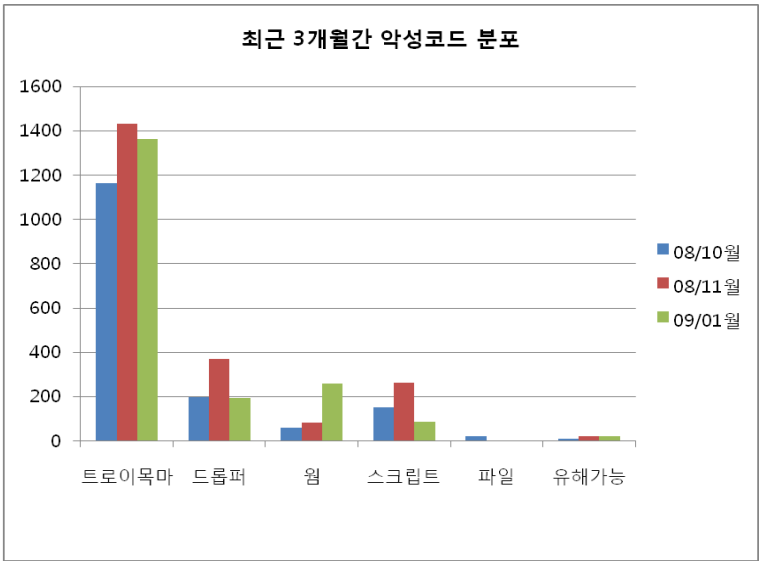
견 되었다. Autorun 웜 유형은 지난 달과 큰 차이는 없으며 IRCBot 웜 유형이 전월 대비 소폭 상승하였고 이를 두고 MS08-067 취약점과 관련을 유추할 수도 있지만 아직까지는 해당 취약점을 이용하는 형태는 발견, 보고 되지 않았다. 다만 일부 안티 바이러스 업체가 기존 취약점 (135/TCP. 445/TCP)을 제대로 인지하지 못하고 콘피커 웜으로 명명한 악성코드가 일부 존재함을 확인 되기도 하였다.

이메일 웜 유형에서는 일반적으로 형태가 주류를 이루었다. 특히 미국의 새 대통령 취임과 발렌타인 데이와 관련하여 사기성 스팸메일 형태로 확산 되는 'Win-Trojan/Waledac' 변형이 다수 발견, 보고 되었다. 이 악성코드는 트로이목마로 분류 되지만 대량의 사기성 스팸메일을 통해 사람들의 호기심을 자극하여 메일내 링크를 클릭하게 하는 등 기존에 알려진 Win32/Zhelatin.worm과 유사한 형태를 가지고 있다.

스크립트 유형은 지난 12월에 알려진 인터넷 익스플로러 제로데이(Zero-day) 취약점을 갖는 JS/Mult 변형이 큰폭으로 증가하였으나, 이번 달의 경우 급격히 하락하여 67% 감소 하였다. 이는 해당 취약점의 긴급패치가 주요원인으로 판단된다.

유해가능 프로그램 유형에서는 지난달과 비슷하게 취약점 점검 도구와 패킷 스니핑 프로그램이 대부분 추가되었다. 이번 달 안철수연구소에 보고된 바이러스는 3가지 형태이다. 이중 Win32/Gattman.16384는 기존에 알려진 변형 중 하나로 바이너리 파일 분석에 사용되는 IDA 도구의 IDC 파일을 감염시키는 증상이 있는 것으로 알려져 있다.

다음은 최근 3개월간 신종 및 변형 악성코드 분포이다.



[그림 3-5] 2009년 최근 3개월간 악성코드 분포

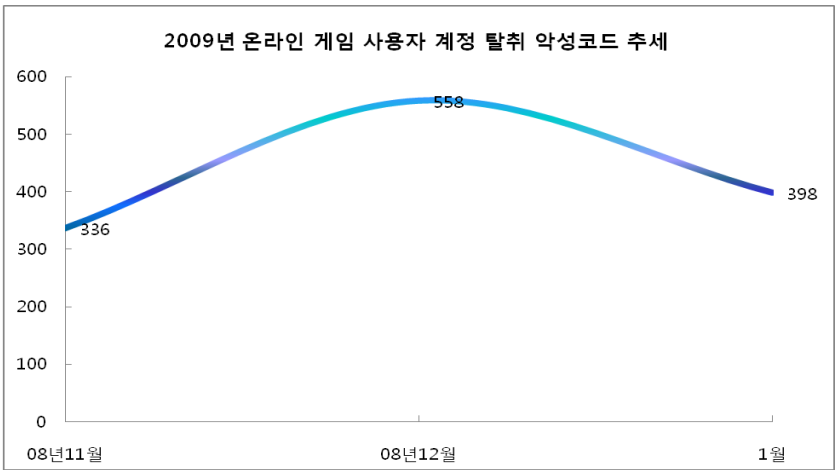
지난 달 큰 폭으로 상승한 신종 및 변형 악성코드 유형은 이번 달 들어서 소폭 감소를 하였

다. [그림 3-5]에서도 알 수 있듯이 웜 유형을 제외하고 감소한 수치이다.

전월 경우 인터넷 익스플로러 제로데이(zero-day) 취약점으로 인하여 스크립트 유형이 폭발적으로 증가하였다. 이외에도 트로이목마와 드롭퍼의 상승이 눈에 띄는데 역시 해당 취약점을 이용하여 drive by downloads 형 악성코드가 많았음을 짐작 할 수가 있다.

웜 유형의 상승은 콘피커 웜에 기인하는데 해당 변형의 추세가 다음달 까지는 이어지지 않을 것으로 보인다. 해당 웜의 경우 대부분의 안티 바이러스에서 Generic 한 진단을 하고 있기 때문에 기존 코드를 수정하지 않는 한 진단을 회피하는 형태의 변형이 당분간 나오기 어렵다고 생각된다. 또한 보안 연구가들이 해당 웜이 랜덤하게 생성하여 자신의 변형을 다운로드 가능하게 해주는 도메인 네임을 계속적으로 추적, 모니터링하고 있다. 또한 보안 관리자들은 이러한 내용을 네트워크 보안 장비에 직접 적용하거나 적용된 룰셋을 업데이트 하는게 바람직하다.

다음은 온라인 게임의 사용자 계정을 탈취하는 악성코드의 추세를 살펴보았다.



[그림 3-6] 온라인 게임 사용자 계정 탈취 트로이목마 현황

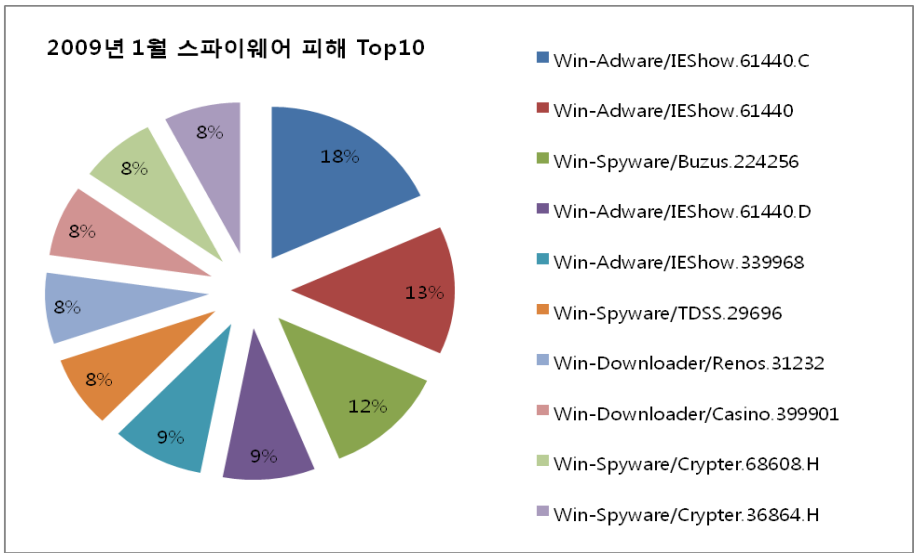
해당 악성코드의 유형은 11월에 비하여 11% 상승 하였으나 12월과 비교하여 29% 감소를 하였다. 12월에 감소 원인중 하나로는 온라인 게임핵 악성코드들이 안티 바이러스 진단을 회피 하거나 또는 분석지연 및 자신의 크기를 줄이는 목적으로 실행압축된 경우가 많았는데 이에 대한 generic한 진단이 추가된 것이 요인으로 보인다. 또한 전월의 경우 인터넷 익스플로러 제로데이(zero-day) 취약점으로 인하여 drive by downloads 형 악성코드가 많았다. 해당 취약점에 대한 보안패치가 나오고 취약점이 포함된 스크립트 파일을 백신 업체가 진단을 하면서 자연스럽게 관련 악성코드가 이번 달에 감소한 것으로 추정된다.

2. 스파이웨어 – 애드웨어 IEShow 피해 확산

(1) 1월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	New	Win-Adware/IEShow.61440.C	12	18%
2	New	Win-Adware/IEShow.61440	9	13%
3	New	Win-Spyware/Buzus.224256	8	12%
4	New	Win-Adware/IEShow.61440.D	6	9%
5	New	Win-Adware/IEShow.339968	6	9%
6	New	Win-Spyware/TDSS.29696	5	8%
7	New	Win-Downloader/Renos.31232	5	8%
8	New	Win-Downloader/Casino.399901	5	8%
9	New	Win-Spyware/Crypter.68608.H	5	8%
10	New	Win-Spyware/Crypter.36864.H	5	8%
합계			66	100%

[표 3-4] 2009년 1월 스파이웨어 피해 Top 10



[그림 3-7] 2009년 1월 스파이웨어 피해 Top 10

2009년 1월 스파이웨어 피해 Top10에서 가장 많은 피해를 입힌 스파이웨어는 애드웨어 IEShow(Win-Adware/IEShow)로 4개의 변형이 스파이웨어 피해 Top10의 상위 순위를 차지하고 있다. 애드웨어 IEShow는 사용자 동의 없이 IE에 광고를 포함하는 탐색 창과 사이드

바를 추가하는 애드웨어이다. 애드웨어 IEShow는 2008년 최초 발견되었으며, 광고 이외의 악의적인 기능은 없었으나 2009년 1월 발견된 변형은 유저모드 루트킷(User-mode Rootkit)과 함께 배포되어 IEShow 구성 요소의 삭제를 방해하는 기능이 포함되어 있다.

순위	대표진단명	건수	비율
1	Win-Downloader/Zlob	238	35%
2	Win-Spyware/Crypter	178	26%
3	Win-Spyware/Zlob	47	7%
4	Win-Adware/IEShow	44	6%
5	Win-Adware/Kwsearch	44	6%
6	Win-Dropper/AdRotator	39	6%
7	Win-Downloader/Kwsearch	24	4%
8	Win-Spyware/PWS.OnlineGame	24	4%
9	Win-Adware/CashBack	21	3%
10	Win-Dropper/Zlob	20	3%
합계		**679**	**100%**

[표 3-5] 1월 대표진단명에 의한 스파이웨어 피해 Top10

[표 3-5]는 변형을 고려하지 않은 대표진단명에 의한 피해 자료이다. 2008년에 이어 2009년에도 여전히 스파이웨어 즐롭(Win-Spyware/Zlob)과 스파이웨어 크립터(Win-Spyware/Crypter)가 전체 피해 신고의 절반 이상을 차지하고 있는 것을 확인할 수 있다. 단일 스파이웨어 피해 Top10에서 가장 많은 피해를 입힌 애드웨어 IEShow(Win-Adware/IEShow)는 4위에 올라 있다.

2009년 1월 유형별 스파이웨어 피해 현황은 [표 3-6]와 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
08'11월	417	342	191	492	0	39	0	5	0	1486
08'12월	291	437	193	419	3	22	3	4	0	1372
1월	370	286	162	384	1	29	0	1	0	1233

[표 3-6] 2009년 1월 유형별 스파이웨어 피해 건수

[표 3-6]은 2009년 1월 유형별 스파이웨어 피해 현황이다. 2008년 12월에 주춤했던 스파이웨어류의 피해가 다시 증가하였으며, 애드웨어에 의한 피해는 크게 감소하였다. 전체 피해

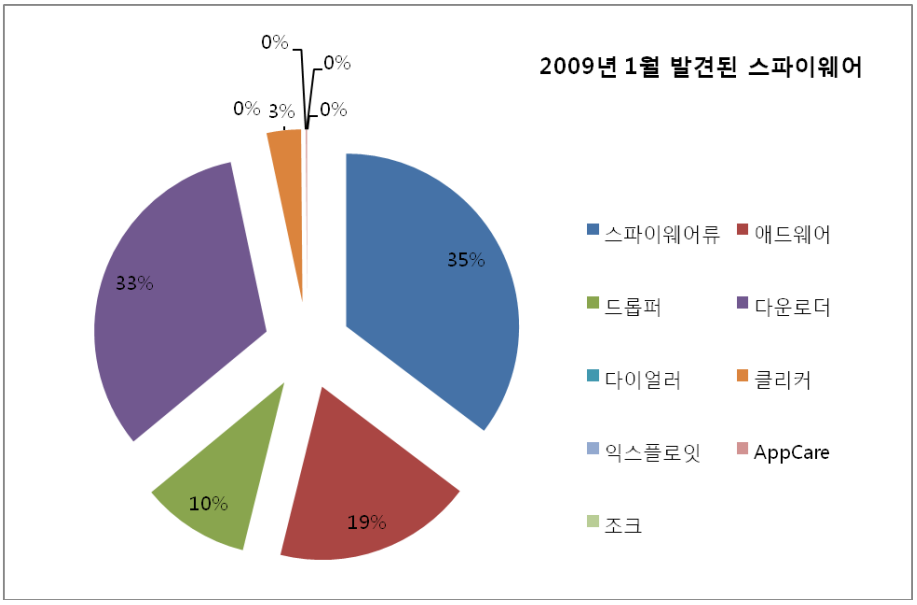
신고 건수는 2008년 12월에 이어 다소 감소세를 보이고 있다.

(2) 1월 스파이웨어 발견 현황

1월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-7], [그림 3-8]와 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
08'11월	194	165	120	314	0	26	0	2	0	821
08'12월	202	269	132	235	2	19	2	3	0	882
1월	264	139	76	244	0	24	0	1	0	748

[표 3-7] 2009년 1월 유형별 신종(변형) 스파이웨어 발견 현황



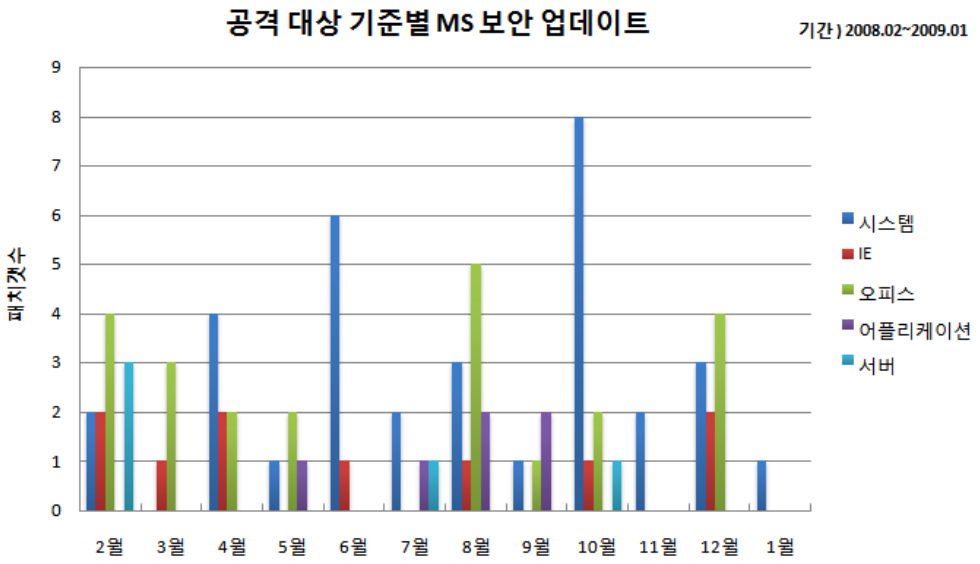
[그림 3-8] 2009년 1월 발견된 스파이웨어 프로그램 비율

[표 3-7]와 [그림 3-8]는 2009년 1월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 스파이웨어 피해 신고와 마찬가지로 스파이웨어류는 증가하고 애드웨어는 감소하였으며 신종 및 변형 발견 건수 또한 2008년 12월에 비하여 감소하였다.

3. 시큐리티 – MS09-001 SMB 취약점

(1) 1월 마이크로소프트 보안 업데이트 현황

2009년 1월에는 마이크로소프트사로부터 단 1건의 보안 업데이트가 긴급(Critical) 위험도로 발표되었다.



[그림 3-9] 2009년 01월 주요 MS 보안 업데이트

위험도	취약점	PoC
긴급	(MS09-001) SMB의 취약점으로 인한 원격 코드 실행 문제점	유

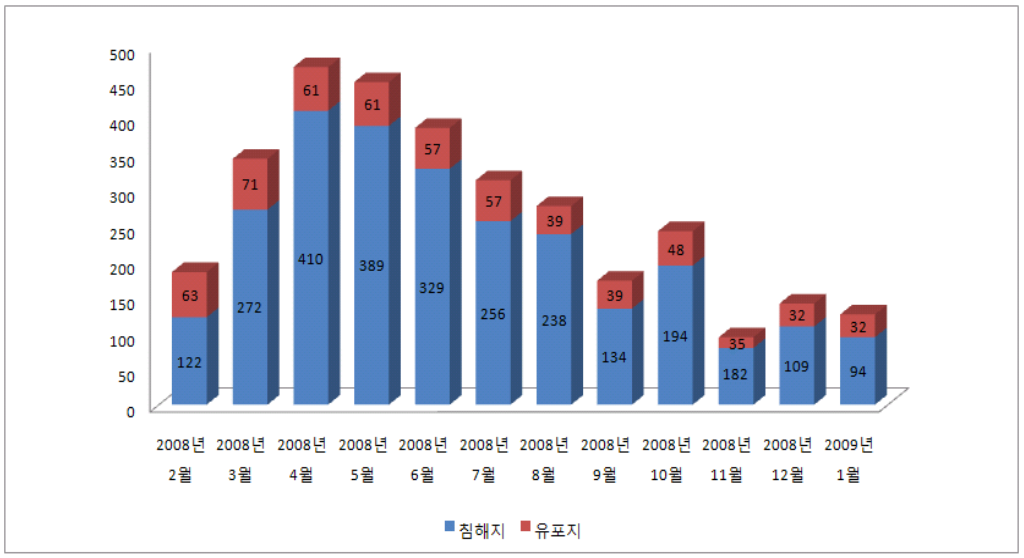
[표 3-8] 2009년 01월 주요 MS 보안 업데이트

이 달에 발표된 MS09-001 SMB 취약점은 특정 SMB 패킷을 처리하는 과정에서 발생하는 메모리 손상 취약점들로서 시스템 크래쉬 현상을 야기하며, 상황에 따라, 블루 스크린과 함께 시스템이 재 부팅되는 현상이 나타나기도 한다.

작년에 발표된 MS08-067 취약점 또한 SMB 서비스 상에서 발생하는 대표적인 취약점으로 현재까지 콘피커 웜을 통해 피해를 야기하는 대표적인 취약점이 되고 있다. 처음 MS09-001 취약점이 발표되었을 때, 제 2의 콘피커 웜으로 발전하지 않을까 하는 우려와 함께 많은 관심이 집중되기도 하였다. 그러나, 해당 취약점은 낮은 코드 실행 가능성과 SMB 세션 연결을 위한 사용자 정보 요구 등의 제약으로 인하여 현재까지는 웜으로 확산 가능성은 매우 낮을 것으로 추정하고 있다.

한동안 애플리케이션 쪽에 집중되어 있던 공격들이 최근 연이어 발표되는 SMB 취약점들로 집중되고 있어, 어느 때보다도 사용자 시스템의 보안 업데이트 적용을 통한 근본적인 문제 해결이 중요한 때이다.

(2) 2009년 1월 웹 침해사고 및 악성코드 배포 현황

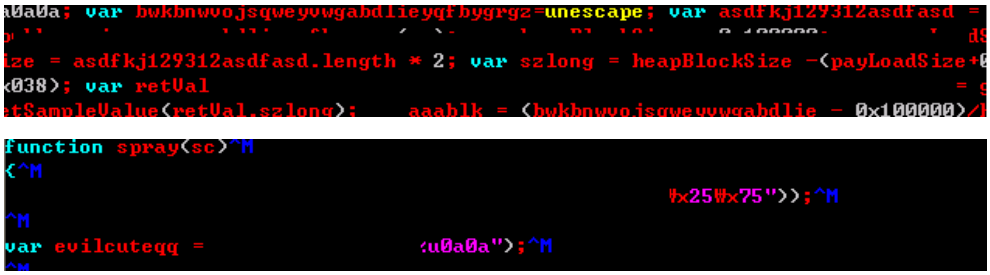


[그림 3-10] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

1월 한 달간 악성코드 유포를 목적으로 침해된 웹사이트의 수와 악성코드 유포 사이트의 수는 94/18로 지난 2008년 12월 109/32 에 비해 소폭 감소했다. 특별히 1월에 웹과 관련된 어플리케이션의 취약점 발표가 없었던 것을 감안하더라도 이와 같은 감소는 주목할 점이다. 하지만, 과거에도 이러한 감소 현상이 종종 있었다는 점을 보면 해당 추세가 단지 일시적 현상으로 그칠지에 대한 판단은 2월 이후의 결과를 종합적으로 분석해야 할 것으로 예상한다.

지난 2008년 12월 제로데이(zero-day) 공격이 발생하여 사회적 관심을 일으킨 MS08-078 (Microsoft Internet Pointer Reference Memory Corruption Vulnerability) 취약점은 제 12월 4건, 1월 3건으로 다른 취약점에 비해 그 빈도가 매우 적어 실제 사용자 피해는 크지 않은 것으로 추정된다. 해당 취약점이 영향을 주지 못한 이유로는 공격에 이용되는 힙스프레이(Heap-Spray) 기법이 다른 코드에 비해 상대적으로 길고, 공격의 성공여부 또한 메모리 환경에 따라 100% 확신할 수 없기 때문이다.

아래는 현재까지 배포된 MS08-078 공격코드의 유형이다. [그림 3-11]을 통해 2008년 1월에 발견된 MS08-078 공격코드의 변형된 유형을 확인할 수 있다.



[그림 3-11] 공격 코드 유형

해당 취약점은 전체적으로 이 달에 탐지된 수는 적지만 기존의 다른 웹 공격코드와 마찬가지로 탐지 우회를 위해 코드를 변형하고 있다. 따라서, 보안 관리자 역시 이러한 점에 대비하여 꾸준한 모니터링과 공격코드 변형에 따른 대응책을 모색하여 할 것이다.

4. 사이트가드 – 악성코드 급격한 증가 추세

(1) 2009년 1월 웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	138,505
악성코드 종류	731
악성코드가 발견된 도메인	790
악성코드가 발견된 URL	6,494

[표 3-9] 1월 웹 사이트 보안 요약

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

[표 3-9]는 2009년 1월 한달 동안 웹 사이트를 통해 발견된 악성코드 동향을 요약해서 보여주고 있다.

사이트가드의 집계에 따르면 1월 한달 동안 악성코드는 731종 138,505건 발견되어 지난 2008년 12월에 비해 급격한 증가세를 보였으며, 이런 악성코드를 포함하고 있는 웹 사이트도 지난 12월에 비해 증가한 도메인 790개, 배포 URL 6,494개로 확인되었다.

전체적으로 1월 한달 동안 악성코드 종류와 발견 건수, 도메인 그리고 URL 모두 지난 달에 비해 급격한 증가세를 보였다.

이에 대한 원인은 다음과 같이 요약된다.

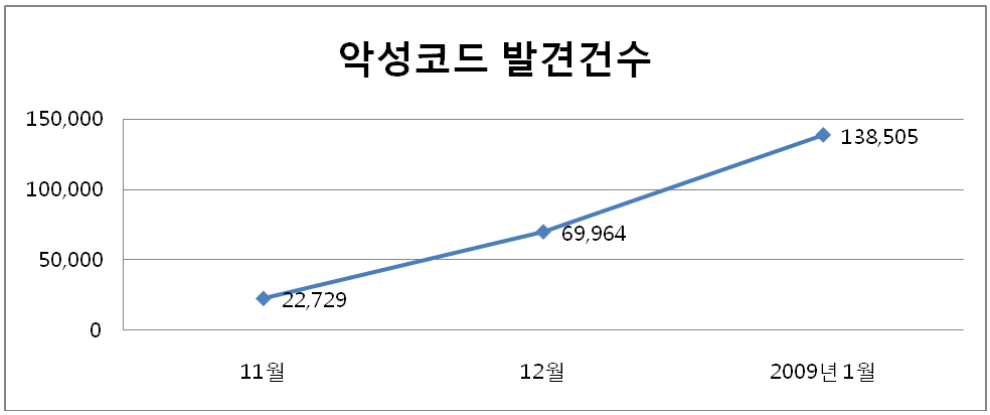
① 웹을 통한 악성코드의 배포 방식이 주요 배포방식으로 자리 잡음
② 사이트가드의 사용자 수 증가로 통계 추출 모집단 증가.

세부내용은 각 통계별로 확인해 보자.

[1] www.siteguard.co.kr

(3) 악성코드 월간 통계

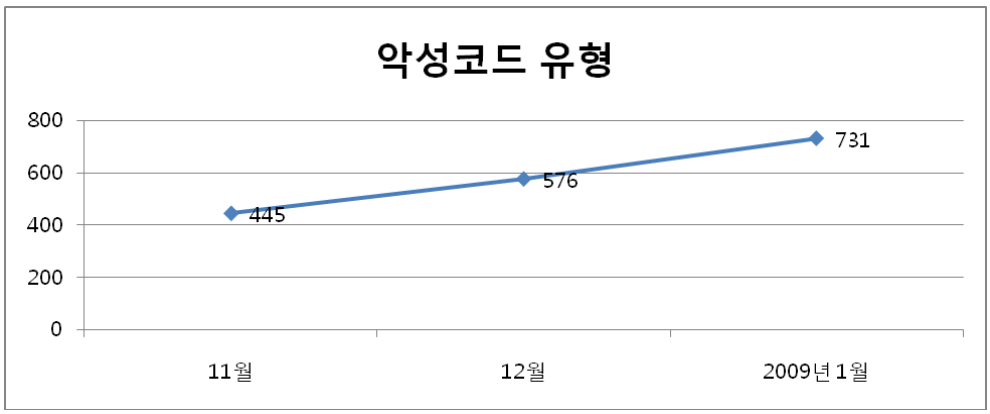
1) 악성코드 발견건수



[그림 3-12] 월별 악성코드 발견건수

[그림 3-12]는 최근 3개월인, 2008년 11월부터 2009년 1월까지의 악성코드 발견 건수의 추이를 나타내는 그래프로 1월 악성코드 발견 건수는 138,505건으로 지난달에 비해 2배정도의 급격한 증가세를 보였다.

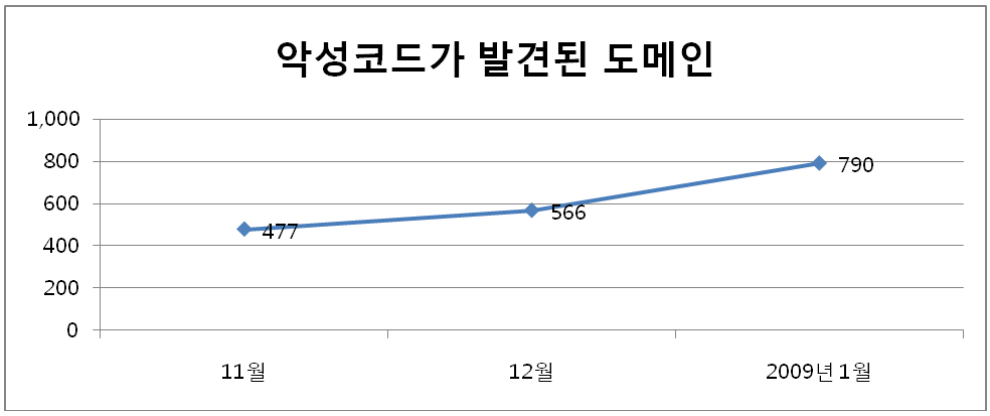
2) 악성코드 유형



[그림 3-13] 월별 악성코드 유형

[그림 3-13]는 최근 3개월간 발견된 악성코드의 유형을 나타내는 그래프로 역시 지난 12월의 576종에 이어 1월에 731종이 발견되어 지속적인 증가세를 보이고 있다.

3) 악성코드가 발견된 도메인

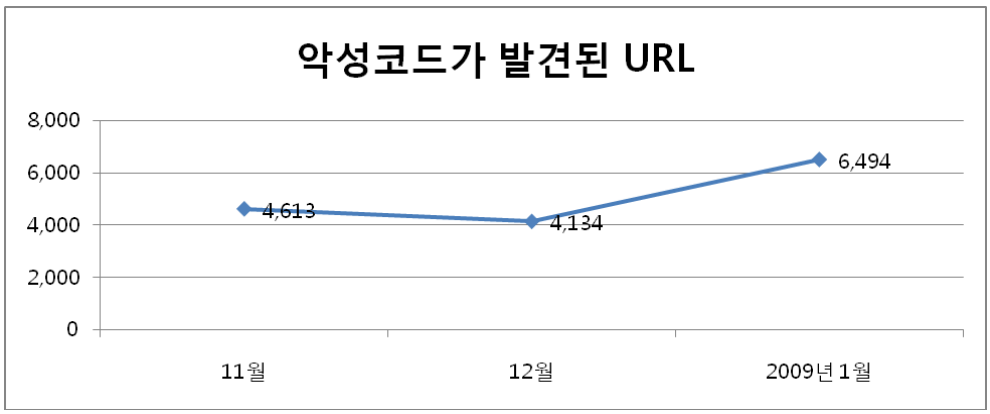


[그림 3-14] 월별 악성코드가 발견된 도메인

[그림 3-14]는 최근 3개월간 악성코드가 발견된 도메인 수의 변화 추이를 나타내는 그래프로 1월 악성코드가 발견된 도메인은 790개로 전월에 비해 40%나 증가하는 높은 증가세를 보이고 있다.

악성코드가 발견되는 도메인수가 급격히 증가한다는 것은 실제 악의적인 유포를 위해 해커들의 적극적인 도메인 공략이 증가하고 있다는 것이다. 이는 앞에 설명한 [그림 3-12]의 악성코드 발견 건수 증가와 맥을 같이 하고 있다고 볼 수 있다.

4) 악성코드가 발견된 URL



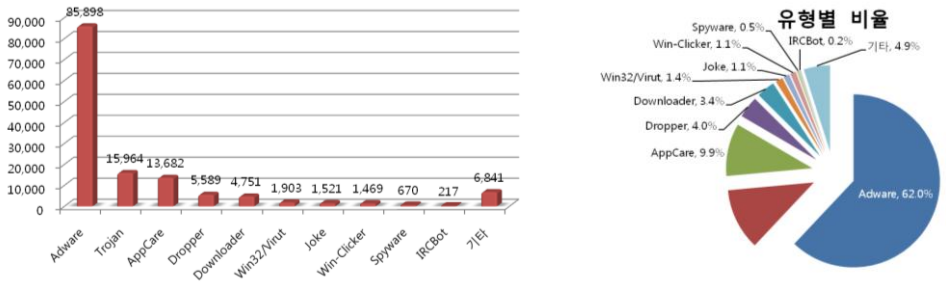
[그림 3-15] 월별 악성코드가 발견된 URL

[그림 3-15]는 최근 3개월간 악성코드가 발견된 URL 수의 변화 추이를 나타내는 그래프로 1월 악성코드가 발견된 URL은 6,494개로 전월에 비해 36%의 증가세를 보였다.

(2) 악성코드 유형별 악성코드 배포 수

유형	건수	비율
Adware	85,898	62.0%
Trojan	15,964	11.5%
AppCare	13,682	9.9%
Dropper	5,589	4.0%
Downloader	4,751	3.4%
Win32/Virut	1,903	1.4%
Joke	1,521	1.1%
Win-Clicker	1,469	1.1%
Spyware	670	0.5%
IRCBot	217	0.2%
기타	6,841	4.9%
합계	138,505	100.0%

[표 3-10] 악성코드 유형별 악성코드 배포 수



[그림 3-16] 악성코드 유형별 분포

[표 3-10]와 [그림 3-16]는 1월 한달 동안 발견된 악성코드를 유형별로 구분하여 발견 건수와 해당 비율(%)를 보여주고 있다.

1월 한달 동안 총 138,505개의 악성코드가 발견되었으며 이중 Adware류가 85,898개로 15,964개로 2위를 차지한 Trojan에 비해 5배 이상의 높은 비율을 차지하고 있다.

(3) 악성코드 배포 순위

순위		악성코드명	건수	비율
1	-	Win-Adware/PointGuard.633344	37,957	38%
2	↑6	Win-Adware/SaveUcc.253952	19,039	19%
3	-	Win-Adware/Onclub.446464	16,575	17%
4	↑5	Win-Trojan/Xema.variant	5,295	5%
5	↑1	Win-AppCare/WinKeyfinder.542720	4,405	4%
6	↑1	Win-AppCare/WinKeygen.94208	4,310	4%
7	↓2	Win-Downloader/PointGuide.644608	3,491	3%
8	new	Packed/Upack	3,236	3%
9	new	Win-Trojan/Shutdowner.241664	2,994	3%
10	↓6	Win-Appcare/RemoveWGA.49664	2,893	3%
합계			100,195	100%

[표 3-11] 악성코드 유형별 악성코드 배포 Top 10

[표 3-11]는 1월 한달 동안 웹 사이트에서 사이트가드를 통해 확인된 악성코드 배포 Top 10을 보여주고 있다. Top 10에 포함된 악성코드들의 총 배포건수는 100,195건으로 1월 한 달 총 배포건수 138,505건의 72%에 해당된다. 또한, 전월과 동일하게 Win-Adware/PointGuard.633344가 1월에도 1위를 차지고 하고 있으며, 1월에 새롭게 진입한 악성코드는 Packed/Upack, Win-Trojan/Shutdowner.241664가 있다.

요컨대, 전반적으로 drive by downloads 형태가 증가하고 있으며, 지속적으로 웹 사이트 취약점을 이용한 악성코드 배포가 급격히 증가하고 있다. 따라서, 웹 사이트 관리자는 자신이 관리하는 웹사이트에 대한 철저한 보안패치와 사이트 점검이 필요하며, 사용자는 사이트가드와 같은 웹 보안 프로그램을 설치하여 웹에서 배포되는 악성코드에 대한 사전 차단이 필요하다.