최근의 보안 패러다임 변화와 2004년 악성코드 동향

안철수연구소 정진성

1. 해킹과 악성코드의 차이

컴퓨터를 공격하는 것에는 두 가지 종류가 있다. 해킹과 바이러스, 더 정확하게 이야기하면 해킹과 악성코드이다.

해킹(hacking)은 알기 쉽게 설명하자면 해커가 인터넷을 통해서 특정 컴퓨터에 침입하여 자료를 훔쳐보거나 변형, 파괴를 일삼는 행위를 말한다. 이 과정에서 들키지 않기 위하여 여러 다른 컴퓨터를 경유지로 거친 다음에 최종 공격 목표에 침입하는 경우가 많다.

악성코드(malicious code)란 컴퓨터에서 사용자가 원하지 않는 일을 사용자 몰래 하는 소프트웨어를 총체적으로 일컫는 것으로, 컴퓨터 바이러스 뿐만 아니라 최근 언론에서 많이 보도가 되고 있는 웜, 트로이목마 프로그램 등이 모두 여기에 속한다.

컴퓨터 바이러스는 단순하게 설명하면 일종의 복사(copy) 프로그램이라고 할 수 있다. 단 한가지의 차이점은 컴퓨터의 복사 프로그램은 사용자가 원할 때, 명령을 내릴 때만 실행되는데 비해서, 컴퓨터 바이러스는 사용자가 원하지도 않고 명령을 내리지도 않았는데도 저절로 실행된다는 것이다. 즉, 컴퓨터 바이러스는 '사용자 몰래 실행되는 복사 프로그램'이라고 설명할 수 있다.

웜(worm)도 컴퓨터 바이러스와 마찬가지로 사용자 몰래 실행되는 복사 프로그램이지만, 공격목표가 다르다. 컴퓨터 바이러스는 다른 파일을 공격해서 거기에 붙어 다니는데 비하여, 웜은 다른 컴퓨터가 공격 목표가 된다. 따라서 컴퓨터 바이러스는 한 컴퓨터 내에서 가능한 많은 파일들을 감염시킨 다음에 다른 컴퓨터로 옮겨가지만, 웜은 바로 다른 컴퓨터로 옮겨갈 수 있다. 컴퓨터 바이러스가 전 세계를 감염시키는 데는 어느 정도 시간이 필요한데 비해서, 웜은 거의 30분 내로 전 세계의 컴퓨터를 감염시킬 수 있는 것도 이러한 특성에서 기인하는 것이다.

트로이목마(Trojan horse) 프로그램은 '트로이목마'라는 이름이 뜻하는 바대로, 정상적인 프로그램처럼 보이지만 사실은 프로그램 내부에 사용자 몰래 자료를 빼내가는 등의 기능이 숨겨져 있는 프로그램을 말한다. 그러나 컴퓨터 바이러스나 웜처럼 복사 기능은 없기 때문에, 스스로 다른 파일이나 컴퓨터를 감염시키지는 않는다.

이러한 악성코드들은 소프트웨어 불법 복사, 의심스러운 웹 사이트, 그리고 이메일을 통해서 퍼져나가는 경우가 많다. 그런데 해킹과 이러한 악성코드들은 세 가지 점에서 큰 차이가 있다.

첫째, 해킹은 1:1의 특성이 있다. 한 명의 해커가 한 번에 한 대의 컴퓨터를 공격하는 것이 기본적이다. 반면에 악성코드는 1:다수의 특성이 있다. 하나의 컴퓨터 바이러스나 웜이 스스로 증식하여 여러 대의 파일이나 컴퓨터를 동시에 공격하기 때문이다.

둘째, 해킹은 해커가 어떤 의도를 가지고 특정한 컴퓨터에 침입하는 법이기 때문에, 일반적으로 구체적인 공격 목표를 가진다. 반면에 악성코드는 자기 스스로 감염 또는 침입할 수 있는 곳을 찾아서 퍼져나가기 때문에 특정한 공격 목표를 가지기 보다는 불특정 다수를 공격하게 된다.

셋째, 해킹은 해커가 직접 컴퓨터에서 컴퓨터로 공격을 하기 때문에 흔적이 남을 수 있고 그에 따라 추적이 가능할 수 있다. 반면에 악성코드는 일단 한 컴퓨터에 침입한 다음에는 스스로 증식하고 퍼져나가기 때문에 추적이 불가능하며 어디를 통해서 왔는지 경로조차 파악하기가 힘들다.

2. 보안의 패러다임 변화 두 가지

그런데, 최근 들어서 전 세계적으로 1.25. 인터넷 대란 등 많은 사고가 발생하고 있는 것은 정보보호 분야에서 두 가지 커다란 패러다임(paradigm)의 변화가 진행되고 있기 때문이다. 컴퓨터 바이러스 기술과 해킹 기술의 결합, 그리고 개인용 컴퓨터 해킹이 그것이다.

가장 큰 패러다임의 변화는 컴퓨터 바이러스 기술과

해킹 기술의 결합이라고 할 수 있다. 예전에는 컴퓨터 바이러스와 해킹은 서로 전혀 다른 영역이었다. 컴퓨터 바이러스는 스스로 증식하는 프로그램으로 개인용 컴퓨터가 주 공격 대상이었고, 해킹은 해커가 여러 가지 기법을 사용하여 취약점이 있는 서버나 대형 컴퓨터에 침투하는 것이다. 또한 컴퓨터 바이러스는 백신 프로그램으로 막을 수 있었고, 해킹은 네트워크 보안 솔루션으로 막을 수 있었다.

그러나 컴퓨터 바이러스 기술과 해킹 기술이 합쳐지면서 커다란 패러다임의 변화가 생기게 되었다. 예전의 컴퓨터 바이러스는 한 컴퓨터 내에서는 무서운 속도로 증식하지만, 스스로 다른 컴퓨터를 감염시키지는 못했다. 사용자들이 감염된 디스크를 다른 컴퓨터에서 실행시키거나, 감염된 이메일을 열어보고 첨부파일을 실행시키는 실수를 통해서만이 수동적으로 다른 컴퓨터를 감염시킬 수 있었던 것이다.

그러나 이제는 컴퓨터 바이러스의 복제 기술과 해킹의 침입 기술이 결합하면서, 해킹 기술을 사용하여 네트워크에 연결된 컴퓨터들에게 스스로 능동적으로 침입하고 증식할 수 있게 되었다. 또한 한 걸음 더 나아가서, 공격당한 컴퓨터를 근거지로 이용하여 다시 다른 컴퓨터들을 공격하게 되면서, 전 세계로 급속하게 퍼져나갈 수 있는 엄청난 파괴력을 가지게 된 것이다.

또한 인터넷상에서 피해자와 가해자의 구별이 없어진 것도 이러한 패러다임의 변화에 기인한다. 과거에는 컴퓨터 바이러스나 해킹에 침입을 당한 사람만이 피해를 보았다. 따라서 컴퓨터 보안 사고는 당사자만의 문제로 생각되었고, 주위 사람들에게는 남의 일, 재수 없어 당한 일로 치부될 수밖에 없었다.

그러나 최근에는 컴퓨터 바이러스 기술과 해킹 기술이 합쳐지면서, 한 컴퓨터가 감염이 되면 이 컴퓨터가 다시 다른 컴퓨터들을 공격하는 전진기지가 되어버리고 말게 된다. 따라서 이제는 피해자와 가해자가 따로 있는 것이 아니라 피해자가 동시에 가해자가 되어버리는, '피해자 = 가해자'의 등식이 성립되는 세상이 되었다.

인터넷을 도로로 비유하자면, 예전에는 교통량이 적어서 자동차 사고가 나더라도 그 차만이 문제가 되었지만, 지금처럼 교통량이 많아진 상황에서 자동차 사고가 나면 뒤따라오는 차들도 연쇄 충돌이 일어나면서 도로가 전부 막혀 버리는 상황과 유사하다고 할 수 있다.

이제는 모두가 잘 방어를 하더라도 한 사람만 제대로 하지 않으면 거기를 통해서 모두가 피해를 입게 되며, 반대로 방어를 잘 하지 않은 사람은 자신만 피해를 입고 마는 것이 아니라 주위의 다른 사람들까지 피해를 입히게 된 것이다.

이것을 다른 표현으로 정보보호의 '하향 평준화' 현상이라고 부를 수 있다. 즉, 전체 중에서 가장 취약한 부분 또는 사람이 그 조직 전체의 정보보호 수준을 결정하는 상황이 된 것이다.

패러다임의 또 다른 변화는 개인용 컴퓨터에 대한 해킹이다. 예전에는 해킹의 목표가 중대형 컴퓨터였다. 그 당시의 컴퓨터 사용 환경은 중대형 컴퓨터에 단말기들을 붙여서 사용하는 형태였기 때문에 중요한 자료들은 모두 중대형 컴퓨터에 저장할 수밖에 없었다. 해커들의 관심은 중요한 자료들에 있기 때문에, 공격 목표는 중요한 자료들이 저장되어 있는 중대형 컴퓨터가 될 수밖에 없었다. 따라서 이를 막으려는 시스템 관리자와 해커 사이에 치열한 싸움이 전개되게 되었다. 프로와 프로간의 대결이었으며, 일반 사용자는 해킹에 대해서 신경 쓸 필요가 없었다.

개인용 컴퓨터가 등장하면서 해커에게 새로운 공격 목표가 나타났다. 그러나 초창기의 개인용 컴퓨터는 성능도 강력하지 못했고, 네트워크에 연결되지 않은 경우가 대부분이었다. 따라서 해커들이 직접 개인용 컴퓨터를 공격할 수 있는 수단이 없었다. 컴퓨터 바이러스는 이러한 상황 하에서 해커들의 욕구(?)를 충족시켜줄 수 있는 훌륭한 수단으로 등장했다. 80년대 중반에 나타난 컴퓨터 바이러스는 그 이후 놀랄 만한 전염력과 파괴력으로 전 세계를 휩쓸었다. 이리하여 중대형 컴퓨터에 대한 해킹과 개인용 컴퓨터에 대한 컴퓨터 바이러스의 공격이 공존하는 시대가 오랫동안 지속되었다.

그러나 90년대 중반부터 개인용 컴퓨터의 성능이 강력해져서 중대형 컴퓨터의 수준에 필적하게 되고, 많은 개인용 컴퓨터들이 인터넷에 직접 연결되게 되면서 이러한 상황이 서서히 바뀌고 있다.

중요한 자료들이 중대형 컴퓨터가 아닌 개인용 컴퓨터에 저장되게 되고, 전자상거래, 온라인 뱅킹, 사이버 주식 거래 등 중요한 경제 활동이 인터넷에 연결된 개인용 컴퓨터에서 이루어짐에 따라 해커들의 관심이 자연스럽게 개인용 컴퓨터로 옮겨가게 된 되었다. 해커들의 입장에서는 인터넷에 연결된 개인용 컴퓨터는 접근하기가 용이할 뿐만 아니라, 일반 사용자들은 정보보호에 대한 개념이나 지식이 부족하기 때문에 아주 손쉽게 값진 정보들을 많이 얻어낼 수 있기 때문이다.

인터넷 시대에 개인용 컴퓨터가 얼마나 큰 위험에 노출되어 있는지는 인터넷에서 널리 퍼져있는 자료 공유 프로그램을 보면 쉽게 알 수 있다. 이러한 프로그램들은 가입자들의 개인용 컴퓨터에 저장되어 있는 파일들을 전 세계에 흩어져 있는 다른 가입자들이 직접 보고 가져갈 수 있도록 해준다. 개인용 컴퓨터가 인터넷에 연결되어

있는 상황 하에서는 전 세계의 누구라도 내 컴퓨터로 쉽게 들어올 수 있다는 사실을 증명해 주는 셈이다.

개인용 컴퓨터 해킹은 이미 다양한 형태로 나타나고 있으며, 해커들이 사용하는 도구들도 다양해지고 있다. 가장 잘 알려져 있는 형태는 원격제어 프로그램이다. 사용자가 알지 못하는 사이에 설치되며, 컴퓨터에 이런 프로그램이 설치되어 있으면 사내의 동료나 심지어는 미국에 있는 해커도 자신의 컴퓨터처럼 자유롭게 자료들을 보고 변형하고 삭제하고 망가뜨릴 수 있다.

키보드 입력 정보를 빼내가는 프로그램도 있다. 이런 프로그램은 컴퓨터에 잠복해 있다가 사용자의 키보드 입력 내용을 파일로 남긴 다음에 특정한 이메일 주소로 그 내용을 전송한다. 실제로 국내에서 이를 이용하여 다른 사람의 은행 계좌번호와 비밀번호를 알아낸 다음에 자신의 계좌로 송금한 금융 사고가 발생한 적도 있다.

이러한 두 가지 패러다임의 변화에 가장 크게 타격을 입는 것은 일반 사용자들이다. 대부분의 개인용 컴퓨터가 윈도우라는 표준화된 운영체제를 사용하고 있고, 인터넷을 통해서 표준화된 형태로 연결되어 있으며, 일반 사용자들은 관리 지식이 부족하다 보니 공격이 진행되면 급속하고 광범위하게 피해가 확산될 수밖에 없는 것이다.

3. 2004년의 악성코드 동향

2004년 10월까지 국내 발견된 (변형 포함) 신종 악성코드는 모두 3,999종으로, 지난해 동기 961종에 비하여 거의 4배가 넘게 증가하였다(표 1, 표 2).

작년 동기에 비해 4배 가까이 증가한 주된 이유는 악성 IRCBot 웜류의 증가 때문이다. 악성 IRCBot 웜류에는 아고봇(AgoBot), 알봇(Rbot), 에스디봇(SdBot), 스파이 봇(SpyBot), 우트봇(WootBot), 포봇 ForBot) 등의 종류가 있다.

한편 올해 신종 악성코드의 동향은 ▸운영체계 및 응용 프로그램의 취약점을 이용한 악성코드 급증 ▸악성 IRCBot 웜 변형의 폭발적인 증가 ▸이메일로 무작위 발송하는 악성코드(Mass Mailer)의 급격한 증가 ▸모바일 및 64Bit 악성코드의 등장 ▸스팸(SPAM) 증가와 피싱(Phishing) 등장 ▸애드웨어의 심각성 증가 등으로 정리할 수 있다.

3.1 취약점을 이용한 악성코드 급증

지난해만 해도 해킹과 악성코드의 접목이라는 말로 표현되었던 악성코드의 동향은 도입기를 넘어서 활용기에 이르고 있다고 해도 과언이 아니다. 지난해 Win32/

표 1 2003년 상반기 신종 악성코드 유형별 집계표

월	리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	합계
1월	0	7	50	18	3	7	0	0	0	85
2월	0	2	78	15	3	13	1	1	0	113
3월	2	3	76	24	1	12	0	0	0	118
4월	0	1	46	11	3	11	0	0	0	72
5월	0	4	39	14	2	13	0	0	0	72
6월	0	2	52	6	4	21	0	0	0	85
7월	0	3	59	4	1	10	0	0	0	77
8월	0	2	92	13	3	20	0	0	0	130
9월	0	1	78	7	2	28	0	0	0	116
10월	0	0	60	3	0	30	0	0	0	93
합계	2	25	630	115	22	165	1	1	0	961

표 2 2004년 상반기 신종 악성코드 유형별 집계표

월	리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
1월	0	0	50	7	6	58	0	0	0	4	125
2월	0	1	130	8	1	146	0	0	0	0	286
3월	0	1	75	5	3	196	0	0	0	25	305
4월	0	1	111	0	7	403	0	0	0	4	526
5월	0	1	32	3	2	322	0	0	0	5	365
6월	0	0	59	2	1	402	0	0	0	0	464
7월	0	2	80	10	4	379	0	0	0	1	476
8월	0	0	87	9	8	358	0	0	0	0	462
9월	0	0	93	16	6	512	0	2	0	0	629
10월	2	0	77	11	0	271	0	0	0	0	361
합계	2	6	794	71	38	3047	0	2	0	39	3999

Blaster.worm(이하 블래스터 웜)이 이용하였던 취약점은 약 보름 정도가 걸려서 악성코드에 이용되었던 반면 최근에는 취약점이 발표된 후 얼마 지나지 않아 Exploit이 공개되는 소위 말하는 Zero-Day Exploit가 현실화 되고 있다는 것이다. 많은 사용자들이 사용하는 윈도우 운영체계는 물론 이에 포함된 인터넷 익스플로러까지 그리고 인터넷 기반의 FTP 및 WWW 서버까지 취약점이 있다면 악성코드 제작자들은 이를 이용한 악성코드 제작에 열을 올리고 있다. 일례로 아고봇 웜에서는 무려 10가지가 넘을 정도의 다양한 윈도우 및 응용 프로그램의 취약점 공격코드가 발견되었다. 아고봇 웜의 전파에 이용되는 취약점은 일반적으로 다음과 같다.

- RPC DCOM2 vulnerability (MS03-039)
- RPC DCOM vulnerability (MS03-026)
- RPC Locator vulnerability (MS03-001)
- WebDav vulnerability (MS03-007)
- UPnP vulnerability (MS01-059)
- Messenger Service Buffer Overrun Vulnerability (MS03-043)
- LSASS BufferOver flow Exploit (MS04-011)
- Workstation service buffer overrun vulnerability (MS03-049)
- NetBios (관리목적공유폴더 대상)
- DameWare의 Mini Remote Control Server Overflow vulnerability

이러한 취약점은 또한 네트워크 트래픽의 폭증이라는 결과를 가져오기도 한다. 악성 IRCBot 웜들의 소스코드는 모듈화 되어 있어 다른 누군가 새로운 취약점에 대한 Exploit 소스를 제공하면 이를 추가하여 새로운 변형 제작이 가능하도록 설계되었다.

또 하나의 변화는 이러한 취약점을 악성코드 제작자만 이용하는 것이 아니라 소위 애드웨어 제작자 또는 SPAM 메일을 보내는 스팸머들도 OS나 응용 프로그램의 취약점을 이용한다. 보통 다음과 같이 스팸메일을 받는 사람이 메일 확인시 스크립트가 실행되거나 ActiveX를 사용하여 사용자 시스템에 애드웨어를 설치하고 불필요한 광고를 지속적으로 내보내게 하기도 한다.

3.2 악성 IRCBot 기반의 웜 폭발적 증가

악성 IRCBot 웜의 폭발적인 증가의 원인은 다음과 같이 정리된다.

- 제작자간의 커뮤니티를 이용한 조직적인 활동 (스크립트 키디가 많음)
- 커뮤니티를 이용한 소스 공유
- 실행압축 프로그램류로 인한 변형의 제작

주로 실력이 뛰어난 제작자가 커뮤니티에 소스를 공개하면 다른 제작자들이 이를 다운로드하여 자신만의 변형을 만들거나 개량하여 다시 커뮤니티 내에 공유하는 방식으로 여러 가지 변형이 제작, 유포되었다.

이러한 웜이 확산된 큰 이유 중 하나는 시스템에 대한 사용자들의 관리지식이 부족해서 오는 경우가 대부분이었다. 즉, 보안패치 파일에 무관심하거나 윈도우 NT 기반의 시스템에서 로그인 암호가 없거나 누구나 유추하기 쉬운 암호인 경우 이러한 악성 IRCBot 웜에 쉽게 감염된다 하겠다. 또한 변형의 제작이 많았던 이유는 확산에 실패하거나 제작자가 개설한 채널(IRC 상에서 대화방을 뜻함)의 유지가 보통 1~2일을 넘지 않기 때문으로 추정되고 있다.

3.3 다양한 Mass Mailer의 등장

올 상반기에 두드러지는 또 하나의 특징은 바로 다양한 Mass Mailer들이 발견, 보고 되었다는 것이다. 주목할 것은 이러한 Mass Mailer들이 약 3달이라는 짧은 기간에 무려 각각 30가지가 넘는 변형이 나왔다는 것이고, 변형이 나올 때마다 기술적으로 발전하여 안티바이러스 업체로서는 골치 아픈 존재였다. 주로 다음과 같은 것들이 있었다.

- Win32/Bagle.worm (이하 베이글 웜)
- Win32/Netsky.worm (이하 넷스카이 웜)
- Win32/Mydoom.worm (이하 마이둠 웜)
- Win32/Dumaru.worm (이하 두마루 웜)

특히 베이글 웜과 마이둠 웜은 소스를 공개하였는데 마이둠 웜의 경우 변형이 제작되어졌으며, 다른 악성코드가 마이둠 웜이 감염된 시스템에 자신을 감염시키는 유형도 발견되었다. 베이글 웜은 상반기가 끝난 7월초 자신의 소스를 웜 내부에 하드코딩 하여 메일로 전파되도록 제작된 변형이 발견되기도 하였다. 또한 이러한 웜들은 지난해 다른 Mass Mailer와 달리 감염된 시스템에서 대량의 메일을 지속적으로 보내어 피해문의 건수가 대폭 증가하기도 하였다.

3.4 모바일 기기 관련 악성코드 등장

모바일 기기에 대한 보안위협은 계속적으로 문제시되어왔다. 이러던 가운데 올해 6월경 심비안 OS를 탑재한 특정 시리즈의 노키아 휴대폰에서 동작하는 세계최초의 휴대폰 악성코드가 발견 되었다. Caribe (이하 카비르)라고 알려진 이 웜은 또한 블루투스(BlueTooth)를 이용하여 전파된다. 즉, 감염된 휴대폰 반경으로 일정거

리에 위치한 휴대폰이 있다면 연결요청을 보내고 사용자가 이를 응답하면 해당 휴대폰도 감염되는 방식으로 전파된다.

카비르는 유럽지역의 GSM 단말기에서만 동작하므로 국내의 CDMA 환경에서는 동작하지 않지만 국내도 WIPI(위피) 플랫폼이 대중화되면 위피 역시 보안위협으로부터 안전하지 못할 것으로 보인다. 또한 모바일 기기의 플랫폼으로 이용되는 윈도우 CE에서도 악성코드가 제작되어 보고 되고 있다. 이렇듯 올해들어 모바일 기기에 대한 보안 위협은 급격히 증가했고 악성코드 또한 출현한 상태로 내년에는 모바일 기기 보안에 대한 새로운 안티 바이러스 제품의 출시등이 기대된다 하겠다.

3.5 64Bit 악성코드의 등장

현재 64Bit 시장은 프로세사 제조사에 의해서 양분되고 있다. 바로 AMD64와 IA64이다. 인텔은 64Bit 시장을 서버시장을 타겟으로 했지만 데스크탑용 64bit 프로세서(EMT64)도 최근 선보이고 있다. 이에 반해 AMD는 인텔보다 먼저 64Bit 프로세서를 개발, 생산하여 국내에도 제법 시장이 갖춰져 있다.

이러한 가운데 국외에서는 IA64, AMD64 환경에서 동작하는 악성코드가 5월과 8월에 각각 발견, 보고되었다. 물론 일반 사용자에게서 보고된 것은 아니며 악성코드 제작자가 제작 후 이를 안티 바이러스 업체에 보낸 것으로 추정된다. 이 두 악성코드는 모두 윈도우 파일 바이러스로 각 프로세서에 설치된 64Bit 윈도우 XP에서 완벽히 동작하여 다른 파일을 감염시킨다.

64Bit 시장은 아직 운영체제 및 관련 응용 프로그램 지원의 미약으로 많은 사용자가 사용중이지는 않다. 이로 인하여 아직은 64Bit 악성코드로부터는 안전하다고도 생각되지만 방심할 수는 없다. 운영체제 제작사가 관련 윈도우를 정식으로 출시하면 덩달아 악성코드의 피해도 예상되기 때문이다.

3.6 SPAM 및 Phishing의 증가와 Black Money

SPAM은 지난해에 이어서 아주 골치 아픈 존재이다. 매년마다 SPAM은 증가하고 있다. SPAM을 보내는 SPAMMER들은 지능적으로 발전했다. 이들은 더 이상 자신이 메일서버를 운영하지 않는다. 이들은 과거에 SPAM Mailer를 가지고 있었다. 확인되지 않은 정보에 의하며 최근 피해를 많이 입혔던 특정 E-Mail 웜이 Proxy 기능을 지원하는 SMTP 서버의 역할을 한다는 것이다. 즉, SPAMMER이 SPAM을 발송하기 위해서 그리고 추적을 피하기 위해서 E-Mail 웜에 감염된 불특정 다수의 PC를 이용한다는 것이다. 이는 매우 설득력 있는 정보이다. 또한 최근 문제가 되는 Phishing 역시 '사기'라는 전통적인 범죄수법이지만 이를 온라인 상에서 이용하여 '디지털 사기'라 불리고 있다.

최근 들어 악성코드 제작자의 제작 동기가 변화하였다. 과거 악성코드 제작자들은 호기심과 자신의 능력을 과시하기 위해서 악성코드를 제작했다. 하지만 최근 들어 이들은 자신의 경제적인 이익추구를 목적으로 SPAMMER들에게 감염된 시스템의 정보를 알려주거나 위장된 은행계정 입력을 요구하는 메일을 작성하여 유포하고 있다. 따라서 앞으로도 자신의 이익을 추구하기 위한 악성코드 및 애드웨어의 제작동기가 많아질 것이고 이는 곧 더 대량의 악성코드 및 복잡한 악성코드의 출현을 예고하고 있다.

3.7 애드웨어의 심각성 증가

애드웨어는 원래 광고목적으로 만들어진 프로그램들을 말한다. 그러나 간혹 프로그램의 버그로 인하여 웹 브라우저를 사용하지 못하게 하거나 시스템의 중요한 파일을 삭제하는 등 시스템 운영에 중대한 손실을 가져와 원래 목적과는 다르게 보여지는 경우가 있다.

실제로 사용자들은 불쑥불쑥 튀어 나오는 팝업창이나 웹 브라우저의 홈페이지 고정 등의 문제가 악성코드의 피해보다 더 현실감 있게 다가올 것이다. 이러한 증상은 대부분 눈에 보이므로 악성코드와 사뭇 구분이 되기 때문이다. 현재 안철수연구소 뿐만 아니라 다른 타사들도 애드웨어 중 그 성질이 유해하다고 판단되는 것은 유해가능 프로그램으로 별도로 분류해 두고 있으며 애드웨어 뿐만 아니라 원격의 파일을 실행시키거나 시스템에서 쓸모없는 리소스를 자치하는 정크 프로그램들도 모두 유해가능한 프로그램으로 보는 경향이 매우 강하다.

4. 2003, 2004년 신종 악성코드의 유형별 현황

표 1, 표 2의 악성코드 유형별 현황은 아래와 같다.

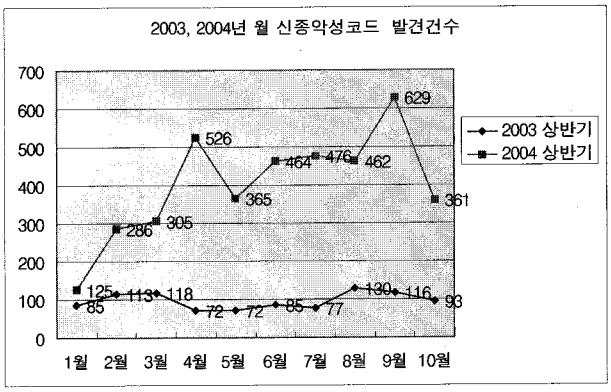


그림 1 2003, 2004년 월 신종 악성코드 발견 건수

2004년 경우 4월과 9월에 비약적으로 증가한 신종(변형포함) 악성코드의 수치를 볼 수 있는데 이는 모두 악성 IRCBot 웜 변형에 의한 것이다. 이는 2003년 수치와 비교했을 때 폭발적으로 증가한 수치이다. 그림 1에서 2004년 10월에는 갑자기 건수가 떨어진 것을 볼 수 있는데 이것은 V3의 엔진의 악성 IRCBot 진단기능을 향상한 결과이다.

다음은 2003년, 2004년 10월까지 신종(변형포함) 악성코드들은 어떠한 유형들이 있었는지 그림 2, 그림 3의 내용을 확인해보자.

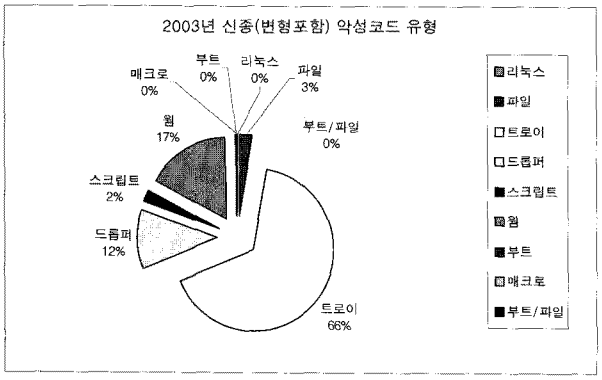


그림 2 2003년 신종(변형포함) 악성코드 유형

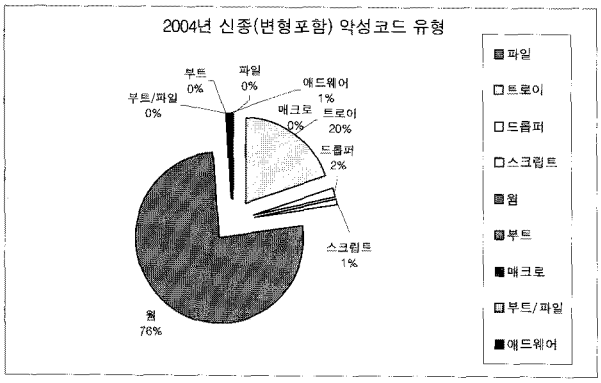


그림 3 2004년 상반기 신종 악성코드 유형

2003년 상반기는 웜보다는 트로이목마류-대부분이 악성 IRCBot 트로이목마-비중이 높았던 반면, 2004년은 트로이목마보다는 웜-대부분 악성 IRCBot 웜-이 증가하였다. 또한 시스템에 오류를 줄 수 있어 유해 가능한 프로그램으로 분류된 애드웨어들도 악성코드 유형에 자리를 잡았다.

올 상반기 발견된 국산/외산 제작 악성코드의 비율은 역시 외산 제작 악성코드가 월등히 많다. 국산 제작 악성코드 경우 전년 동기간 대비 5배 정도가 증가하였다.

대부분 발견되고 있는 악성코드의 유형이 외산인 것을 감안한다면 5배 증가한 국산 악성코드들의 발견건수는 매우 적다고 하겠다. 증가된 국산 악성코드는 대부분 애드웨어류이며 악성코드와는 다르다.

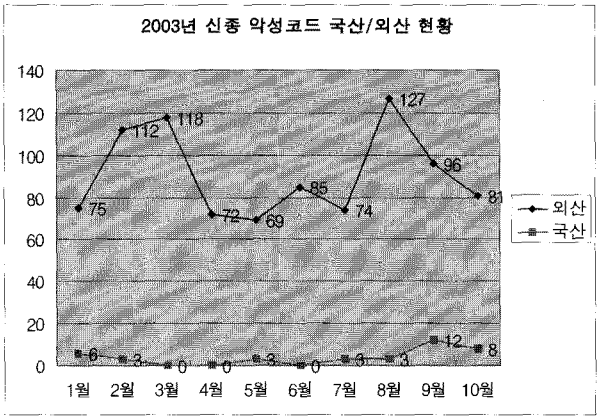


그림 4 2003년 상반기 신종 악성코드 국산/외산 현황

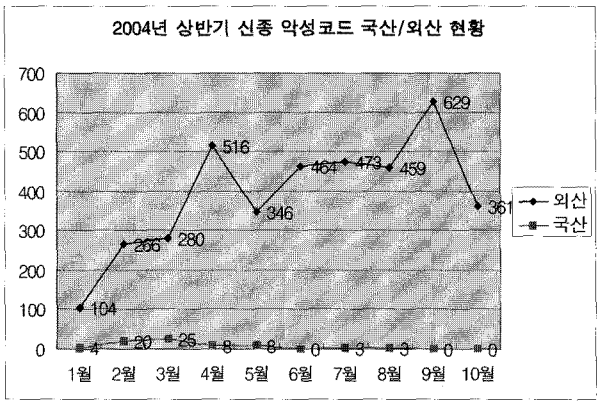


그림 5 2004년 상반기 신종 악성코드 국산/외산 현황

2004년 상반기 국산 악성코드는 지난해 동 기간보다 상승했지만 대부분이 유해 가능한 애드웨어들이었다. 또한 SPAM Mailer류는 현저히 줄었으며 대신 Active X와 BHO(Browser Helper Object)를 사용하여 시스템에 설치되고 동작하는 유해 가능한 프로그램들 때문에 사용자들은 더욱 피해를 입었다.

5. 악성코드의 미래

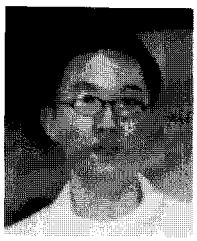
미래를 예측하기는 어렵지만 최근 악성코드 동향을 살펴보면 어느 정도 가늠할 수 있다. 앞서 소개된 유해 가능한 프로그램이 마치 악성코드처럼 자신을 실행하고 숨기는 현상도 보이고 있어 앞으로 이러한 유해 가능한 프로그램에 대한 심각성은 내년에도 크게 대두될 것으로 보여진다. 이러한 유해 가능 프로그램에 대한 대책으로 윈도우 XP SP2에서는 웹 브라우저에서 Active X를 제어하는 등 신뢰할 수 있는 브라우징 기술 등이 선보였다. Gateway에서 악성코드와 유해 트래픽을 차단하는 IPS/IDS 의 하드웨어 보안장비도 대거 선보였다.

이러한 장비들의 등장한 급격한 확산속도와 Zero-Day Exploit를 예방하기 위해서이다. 올해 첫 등장한 모바일 악성코드와 64Bit 악성코드의 등장도 새로운 보

안위협으로 다가왔으며 내년에 이와 관련 보안 연구와 관련 제품이 출시될 예정이다.

전산자원에 대한 인프라가 발전하고 증가함에 따라서 새로운 보안위협이 발생되고 이를 예방 및 대응하는 연구와 개발은 끊임없이 이루어졌다. 변화가 너무도 빠른 현시대에 앞으로 어떤 새로운 보안위협이 우리를 위협할지 예측하기 어렵다. 하지만 우리는 어떤 보안위협들이 발생할 수 있는지 정도는 예측할 수 있고 가장 위협적인 것들에 대한 예방 및 대응 연구를 통해서 좀더 안전한 유비쿼터스 시대를 맞이할 수 있을 것이다.

정 진 성



1996. 2 혜전전문대졸
1999. 5 안철수연구소 입사
1999. 7 안철수연구소 바이러스 신고센터 담당
2001. 10~현재 안철수연구소 시큐리티 대응센터 분석업무 담당
2004. 10 KISA 주관, 민관합동조사단 전문가 임명 (분석전문)
관심분야 : 악성코드 분석 및 연구, 안티 바이러스 기법 연구 (실행압축해제, 매모리 검사, metamorphism, polymorphic 등..)
E-mail : jsjung@ahnlab.com