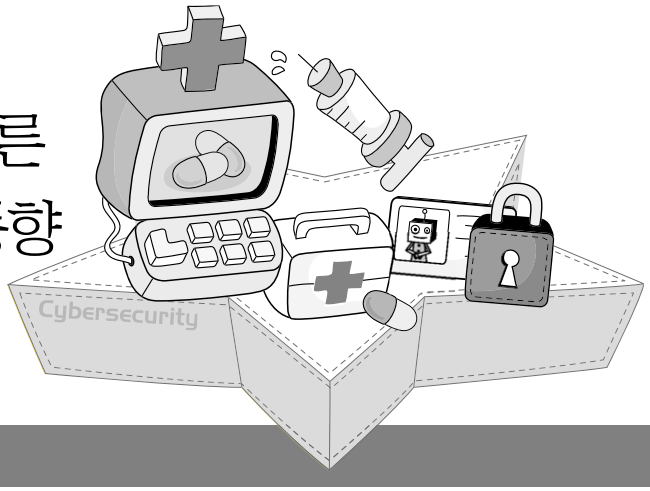
악성코드의 진화에 따른 대응기술 및 표준화 동향



조 시 행 • ASEC/ 안철수연구소

악성코드는 크게 기술적 흐름 및 변화와 함께 진화해 왔다고 할 수 있다. 악성코드는 바이러스가 출현한 20여 년 전부터 지금까지 기술적 발전을 거듭하면서 진화해 왔고, 대응 기술 또한 그에 맞추어 발전해 왔다. 하지만 창과 방패의 싸움이 아직까지도 끝이 나지 않는 이유는 무엇일까? 악성 코드 제작자들은 계속 백신이라는 방패를 뚫기 위해 노력하고 있고 백신 업계는 더 좋은 방패를 만들기 위해 노력하고 있으며 기존 파일 기반의 제품을 탈피하고 다양한 형태의 접근을 시도하고 있다.
본 글에서는 현재 주요 기술적 흐름의 변화를 살펴보고 그에 따른 대응 방법을 살펴보고 관련된 표준화 진행 사항에 대해서도 간단히 정리하고자 한다.

1. 주요 동향

최근의 동향은 확산 방법의 변화, 악성 코드 변형 형태의 변화, 보안 위협 기술의 산업화 그리고 해킹 목적의 변화 등을 꼽을 수 있을 것이다.

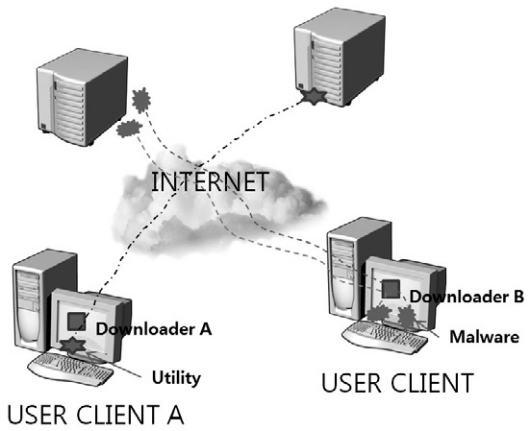
1.1 악성 코드의 확산 방법의 변화

90년대 초와 2000년대 초 그리고 현재의 악성코드 확산 방법은 큰 차이가 있다. 90년대 초 악성코드는 대부분 바이러스를 의미했다. 주로 소프트웨어 불법 복제 및 복제된 소프트웨어의 다운로드로부터 확산이

이루어졌다. 그러다 보니 사실상 광범위한 확산보다는 지역적 확산이 주를 이루었다.

그 뒤에는 인터넷의 사용이 대중화되면서 메일로 확산되는 유형이 일반화되었고 이제는 그 방법도 버퍼 오버런과 같은 방법에서 과거보다는 더 적극적으로 심리적 접근을 하는 피싱 방법으로 발전해 왔다. 아울러 기존에는 OS나 중요 서비스의 취약점을 이용했다면 많은 사용자가 이용하는 애플리케이션 취약점을 이용하는 방법 등으로 공격 방법도 다변화되고 있다.

최근의 악성코드의 확산 방법 중 주의 깊게 살펴볼 부분은 다운로더라는 툴을 이용한 확산이다. 다운로더라는 것은 이름에서도 알 수 있듯이 단순히 파일을 내려 받는 기능을 하는 프로그램을 말한다. 이러한 다운로더 프로그램이 [그림 1]에서의 Downloader A가 유용한 유틸리티 프로그램을 다운로드 하면 이 프로그램은 정상 프로그램이 되는 것이고 Downloader B와 같이 악성 코드를 다운로드 할 경우 악성코드로 정의하게 된다.



[그림 1] 다운로더의 역할

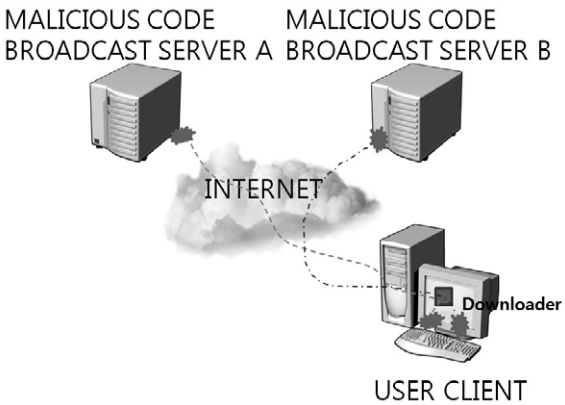
그러나 다운로더 코드는 매우 단순하여 몇 개의 API 함수만으로 구현이 가능해 다운로더만 놓고 악성코드를 규명하는 것은 참 어려운 문제라고 할 수 있다.

이러한 다운로더를 통한 악성 코드 확산은 매우 광범위하다. 특히 중국 사이트를 방문해서 프로그램 복제나 불법 이용자를 위한 코드 패치 프로그램이나 크랙 사이트 등을 방문한 경우 시스템 내 취약점으로 인해 ActiveX가 자동 설치될 수 있으며 이용자에 의해 수동처리 되는 경우도 많다. 이들 사이트 내의 콘텐츠들에는 다운로더가 다수 포함되어 있어 스파이웨어나 악성코드를 지속적으로 설치되는 피해를 가져올 수 있다.

이들 다운로더가 실행된 이후에는 어떤 악성코드든 내려 받아져 실행할 수 있는 상태가 되어 사실상 공격자에게 컴퓨터의 모든 자료가 노출되었다고 볼 수 있게 된다.

이러한 다운로더의 경우 기업 내부망에 파이어월이 설치되어 있더라도 내부자의 실수에 의해 다운로더가 설치된다면 파이어월도 우회하는 상황이 발생할 수 있게 되어 큰 피해가 발생할 수 있고 네트워크 공격 코드가 침투할 경우 내부망의 장애가 발생할 수 있다.

다운로더는 다음 [그림 2]와 같이 악성코드를 제공하는 서버를 두고 악성코드를 지속적으로 내려 받게 되며 악성 코드 서버는 새롭게 설치되는 다운로더에 의해 변경될 수 있게 되어 서버 경로가 폐쇄 되더라도 계속 동작하게 된다.



[그림 2] 배포 서버의 자동 변경

다운로더에 대한 대응 방법은 대체적으로 악의적으로 이용되는 다운로더 프로그램들을 찾아서 진단하는 방법이 주를 이루고 있으며 VIRUSTOTAL(http://www.virustotal.com)과 같은 샘플 진단 서비스를 통해서 의심 샘플로 많이 접수가 되고 있지만, 제작자 또한 백신을 이용해 진단을 해보고 출시할 수 있는 상황으로 완전하게 방어하기는 어려움이 존재한다.

다운로더의 경우 기존 정상 소프트웨어의 자동 업데이트를 실시하는 것과 메커니즘상에서는 별반 차이가 없어 사용자의 주의가 필요한 상황이며, 백신 업계에서도 효율적으로 새로운 다운로더를 검출하기 위한 기술을 연구하여 제품화라는 노력을 진행하고 있어 근시일 내에 좋은 결과를 얻을 수 있을 것으로 바라보고 있다.

1.2 외출복을 자주 갈아입는 악성 코드

코드 변형의 시작은 바이러스가 자신을 직접 변형시키는 형태의 다형성 기법으로부터라고 볼 수 있다. 당시 바이러스 제작자들은 MtE(Mutation Engine)라는 것을 채용하여 바이러스가 감염될 때마다 새로운 형태의

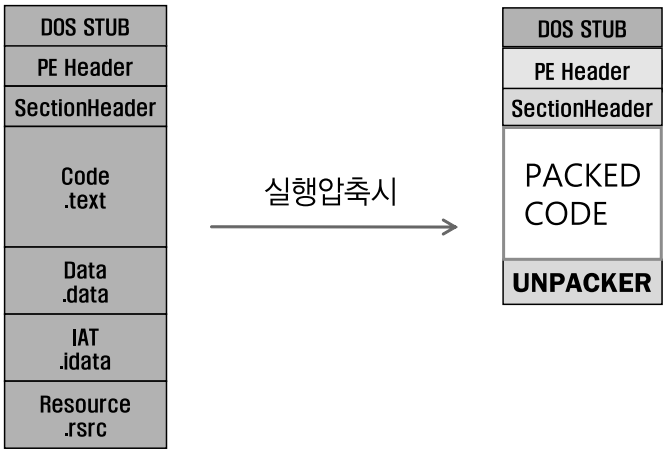
코드로 구성되도록 하였다. 당시만 해도 다형성 바이러스는 진단/치료가 매우 어려운 바이러스라고 해서 대응 시간도 일반 바이러스의 10배 가까이 소요되었었다. 이러한 다형성 바이러스의 일반적인 형태는 디코더는 감염할 때마다 변경되어 다른 코드로 보이게 되고 바이러스 바디는 키가 바뀌어 암호화되는 정도로 사실상 원본은 보존 상태가 되었다.

2000년대에 들어와 바이러스의 출현이 현저히 줄고 주로 웜이나 트로이목마의 출현율이 높아졌다. 웜의 확산은 바이러스와 달리 이메일이나 네트워크 공유 등의 방법으로 이루어졌으며 메일을 다수에게 보내는 방법으로 불특정 다수에게 광범위하게 확산되기도 하였다.

이 시기의 코드 변형 도구로 널리 사용한 방법은 실행 파일 압축(암호화 포함, Runtime Packer/Cryptor)이라는 방법이다. 과거에는 바이러스는 작은 크기의 코드로만 구성되어 파일 전체의 압축 방식으로는 접근할 수 없는 형태였지만 웜이나 트로이목마는 그 자체가 하나 이상의 파일로 존재하고 있고 크기도 바이러스의 수십 배 내지 수백 배에 이르러 압축을 통해 크기를 줄일 수 있게 된다.

실행 파일 압축은 실행이 가능한 프로그램 파일을 압축 기법을 이용하여 더 작은 파일로 만들고 프로그램이 메모리에서 실행될 때 압축을 풀어 원본 코드로 복원하는 기술로 원본의 데이터가 보존되는LZW, HUFFMAN과 같은 무손실(lossless)방식의 압축이 사용되게 된다.

실행압축을 하게 되면 [그림 3]과 같이 원본 파일의 코드와 데이터 부분이 모두 압축되어 외형상으로는 원본의 내용과 전혀 다른 코드를 가지는 프로그램으로 보여지게 된다. 하지만 원본과 기능은 동일하여 실행하는데 문제는 없다. 이러한 특성을 악성코드에 적용하면 실행 압축 방법만 바꾼다면 원본과 기능은 같지만 전혀 다른 악성코드가 된다.



[그림 3] 실행압축 후 파일의 변화

하나의 악성코드를 10개의 실행 압축 도구를 이용해 변형하면 10개의 악성코드가 되는 것으로 실제로는 수백가지의 도구가 존재하고 이들 도구를 조합할 수 있다는 측면에서 보면 그 변형 가지수는 수천 가지 이상이 될 수도 있다.

이러한 특성을 대응하는 입장에서 볼 때 압축 알고리즘을 파악하여 압축을 해제할 수 있어야 정확히 악성코드인지 정상 파일인지를 구분할 수 있고 또 정확한 진단을 위해서는 압축 해제 알고리즘을 구현해야 하는 등 분석과 대응에 시간이 많이 소요되는 문제점을 가져 결과적으로 대응을 어렵게 만드는 요인이기도 하다.

2000년대 초에는 실행 압축된 샘플의 수가 한 달에 30여 개 이하에서 발견되는 수준이었지만 지금은 한 달에 수 만가지 이상의 실행 압축된 악성코드가 새롭게 발견되는 상황이다.

지난 3년 간의 실행압축(암호화)도구들의 비중을 보면 2005년도의 경우 UPX의 비중이 컸지만 해마다 줄어들어 2008년 들어 10%미만으로 떨어져 있고 반대로 맞춤형 실행 압축의 비중은 과거 7.87%였지만 현재는 24%를 차지할 만큼 그 비중이 커지고 있다.

맞춤형 실행압축(Custom Runtime Packer)의 비중이 커지면서 압축을 풀어서 진단한다는 개념의 적용이 어려운 상황이 되었다. 이유는 1개의 악성코드에서 1번만 사용되는 경우도 많아 제작자는 한번에 수백 개의 변형을 만들어 낼 수 있지만 이를 대응하는 입장에서는 일일이 압축을 풀어내기도 쉽지 않고 그렇다고 변형 샘플 모두를 입수한다는 것도 어려운 상황이다.

AV업계에서는 지난 몇 년 전부터 이러한 압축을 풀기 위해 Generic Unpacking 기술을 연구하고 개발하고 있다. Generic Unpacking은 실행압축 되었다고 판단하는 파일을 알고리즘의 구현없이 원본을 풀어내는 기술로서, 크게 압축 여부의 판단, 그리고 가상 실행을 통한 원본 추출, 진단으로 이뤄지는 부분으로써 지금까지 매우 성공적으로 평가되는 방법은 나타나지 않고 있으나 가까운 시일내에 좋은 결과들이 도출될 것으로 예상하고 있다.

1.3 보안 위협 기술의 산업화

보안 위협 기술의 산업화는 이미 오래 전부터 서서히 진행되어 왔지만 음성적인 시장 내에서 이뤄지는 부분으로 크게 부각되지 못했다. 하지만 수년 전부터 국내에서 게임과 관련된 부분에서 크게 부각되어 나타나고 있다.

외국의 경우에는 보안 위협 기술의 산업화의 대표적인 사례로 스파이웨어나 애드웨어를 전문적으로 제작해 주는 다수의 업체가 합법적으로 영업을 한 경우를 들 수 있는데 그 규모가 얼마나 되는지는 알 수 없

다. 과거에는 광고를 보는 대가로 소프트웨어를 무료로 사용하게 해주는 좋은 목적의 의미로 애드웨어를 정의했지만 지금은 사용자가 원하지 않는 광고를 한다는 이유로 악성코드의 일부로 분류될 만큼 분류 기준과 사용자들의 시각이 변화되고 있어 앞으로는 이와 관련된 사업은 확장이 어려울 것으로 보고 있다.

보안 위협 기술의 산업 측면에서 살펴볼 수 있는 것 중 하나가 게임 보안 관련 부분이다. 더 구체적으로는 불공정한 게임 진행과 관련한 부분일 것이다.

게임 아이템 시장은 2005년에 1조에 가까울 것으로 예상된다는 기사가 소개된 적이 있다. 대부분 현금으로 거래되고 있어 그 규모를 정확히 파악할 수 없지만 여러 기사와 관련 기관의 조사를 통해 추정한 수치이다[DA0509].

이들 아이템과 관련하여, 2005년 경 아이템 공장이라는 말이 있었다. 이것은 게임에 능통한 여러 명을 고용하여 한 방에 모여 아이템 획득을 위한 게임을 24시간 진행하여 아이템을 획득하거나 게임 캐릭터의 레벨을 높이는 작업을 전문적으로 수행하는 곳을 의미하는 것으로 소수의 인력으로 다수의 컴퓨터를 놓고 오토마우스 및 아이디 도용과 같은 불법적인 방법을 통해 아이템 획득 및 캐릭터 레벨업을 진행한 것으로 알려져 있다.

또한 이런 음성적 산업이 발전했던 이유는 아이템의 경우 아이템 거래소를 통해 현금화 될 수 있었고 레벨업을 원하는 게임 이용자들이 현금을 주고 의뢰하는 중계 사이트들이 존재했기 때문으로 파악된다.

얼마 전에는 이러한 곳을 통해 주민등록번호 수집 및 다양한 방법의 해킹이 이루어지고 있다는 기사도 보게 된다.

최근에는 게임 아이템과 관련하여 해킹의 목적으로 게임 아이템을 갈취하고자 하는 목적의 악성 코드도 다수 등장하고 있어 2007년 한 해 동안 약 2000여 건이 발견된 반면 2008년 상반기에는 3300여 개가 등장하여 그 위험성은 점점 높아지고 있으며 과거에는 게임 보안 솔루션으로만 진단한 것들이 이제는 다수의 백신에서 게임 해킹 툴을 진단할 만큼 그 비중이 커지고 있다고 볼 수 있다.

게임 아이템과 관련한 보안 위협 기술의 산업은 ID도용이나 주민등록번호의 부정 이용으로 출발하였고 그 시장의 규모를 파악할 수 없을 만큼 발전해 있지만 쉽게 드러나지 않고 있다. 이에 대응하여 게임 업체나 게임 보안 업체는 불공정한 방법에 의한 게임을 진행할 수 없도록 다양한 대응 방법을 구현하여 적용하고 있지만 보안 위협 기술의 지속적인 공격을 받고 있다.

1.4 해킹의 목적의 변화

과거에 해킹은 취약점이 있는 목표를 찾아 공격하는 다소 불특정 목표를 선정하고 있는 것이 일반적인 모습이고 취약점이 있는 곳을 찾고 해킹을 하는 것이 보통이었다.

근래의 해킹 방법은 취약점을 발견한 사이트를 협박하여 돈을 요구하고 그에 불응할 경우 보복성 해킹을 하고 있으며 실제로 그러한 협박에 응하는 업체 또한 발생하게 된다[PC0805].

요즘의 가장 큰 이슈는 해당 사이트를 이용하고 있는 고객 정보이다. 고객 정보는 암암리에 돈을 주고 서로 사고 판다는 것은 뉴스나 신문 기사를 통해 잘 알려져 있다.

최근 1천만 건에 달하는 고객 정보가 유출된 사례와 수백만 명의 고객 정보를 팔아 넘긴 사례 등을 보면 고객 한 사람만 놓고 보면 몇 줄의 정보이지만 해커 입장에서는 큰 돈이 되는 정보일 것이다.

또한 서비스 거부 공격에 대한 협박의 경우 은행이나 증권사의 경우 실제로 서비스 중단으로 이어진다면 어마어마한 피해를 입을 수 있어 단순 협박이라고 보기에는 어려움이 있다[CB0807].

지난 5월경 미국인 해커를 고용한 은행 서버의 해킹으로 대규모 고객 정보 유출 가능성을 지적한 사건이 있었다. 이러한 공격에 있어서 망 내부에 있는 내부자에 의한 공격은 무방비라는 것이 확인된 사건이었다[DA0805].

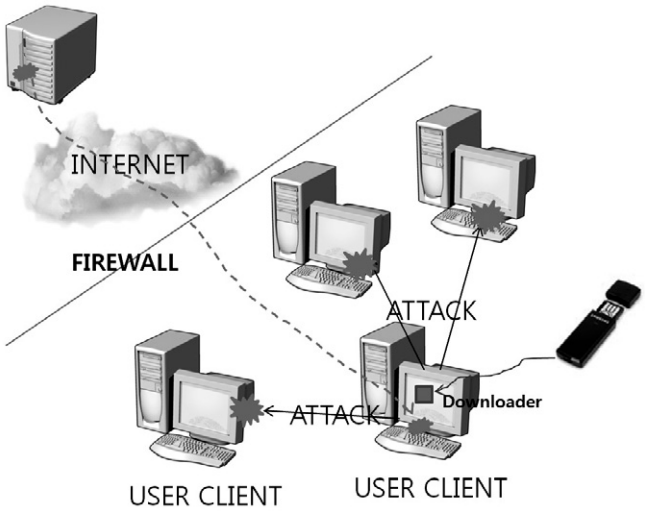
아울러 해당 공격은 은행 내부가 무선 네트워크를 통해 정보가 공유되고 있다는 점을 이용한 해킹 방법으로 고객 계좌번호와 비밀번호 등 암호화된 정보를 해독하기 위한 암호 해독 프로그램까지 동원한 점등은 우려할 만 하다.

비록 지금은 중요 정보가 노출되지 않았지만 언제든 이러한 공격은 발생할 수 있으며, 네트워크로 연결되어 있는 상황에서 내부자 및 외부로 연결되는 사소한 헛점만으로도 큰 피해가 발생할 수 있다는 점을 확인해 준 만큼 내부자에 대한 통제와 내부망에 대한 보안 정책이 무엇보다 중요한 시기라고 할 수 있다.

최근의 해킹 목적의 변화는 해킹 도구의 입수가 용이하여 과거와 같이 해킹과 관련한 기반 지식이 풍부하지 않더라도 도구의 이용만으로도 가능해진 점과 무관하지 않을 것이다.

악성코드의 양상이 기존에는 주로 감염 및 확산을 목적으로 했다면 지금은 내부 네트워크 마비와 같은 업무 방해 측면도 부각되고 있다.

[그림 4]에서와 같이 내부자의 외부 유입 노트북이나 USB를 통해 내부망에 존재하는 컴퓨터에 악성 코드나 다운로더가 설치되는 방법이나, 내부망 이용자들에게 피싱 메일을 발송하여 다운로더를 설치하게끔 유도한 다음에 악성 코드를 다운로드하도록 한 뒤 내부 망에 있는 다수의 PC를 공격하는 방법이 현실에서



[그림 4] 내부망 공격 유형

피해를 주고 있어 네트워크 보안 장비들의 설명과 내부 보안 정책에도 신경을 써야 한다.

이러한 상황은 ARP Spoofing을 유발하는 악성코드인 Win-Trojan/ARPSpoofer와 과거 Win-Trojan/IRCBot에 의한 내부망 네트워크 마비 등의 피해가 실제로 발생했다.

따라서 이러한 부분에 있어서 보안 솔루션 도입도 중요하지만 이용자의 보안 의식의 변화도 필요한 부분이며 무선 랜과 같은 도구를 사용할 경우 인증 기능을 이용하여 보다 높은 외부 공격자에 보안 헛점을 노출하지 않도록 해야 한다.

2. 표준화 동향

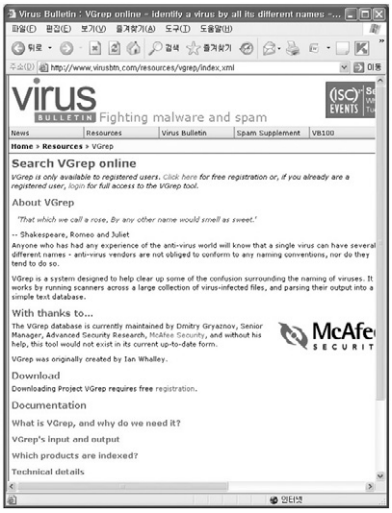
악성코드에 있어서 표준화라는 것은 사실상 없다. 가장 표준화가 필요하다고 요구된 것들은 악성코드명과 진단 능력을 어떻게 평가할 것인가에 대한 부분이지만 그간 십수년간 진행 과정을 볼 때 앞으로도 표준화 성공 가능성은 크지 않다고 보여진다.

2.1 악성코드명

악성코드명에 대한 표준화의 필요성은 동일한 악성코드에 대해 백신마다 서로 다른 이름을 부여함으로써 컴퓨터 이용자들에게 서로 다른 악성 코드가 발견된 것으로 오인하게 하는 문제가 있을 수 있다는 점과 악성 코드 확산을 막아야 하는 입장에서 정보의 전달이 어렵다는 측면 등이 부각되었다.

하지만 이 부분은 모든 백신 업체가 샘플을 동시에 받아서 처리하는 것이 아니고 백신 회사마다 샘플의 유입 시간이나 처리 절차 등이 서로 상이하고 각 회사별 Naming Rule이 존재하는 입장에서 다 바꾼다는 것은 현실적으로 매우 어려운 문제라고 할 수 있다.

다만 이름의 혼동을 줄이기 위한 노력으로 Virus Bulletin이라는 안티 바이러스 최대 학회를 운영하고 있는 기관에서 [그림 5]과 같이 VGrep이라는 도구를 제작하여 이름 비교 서비스를 시작한 것을 들 수 있는데, 기존의 방법들과 달리 악성 코드 샘플에 대한 각 백신별 진단명을 데이터베이스화한 것으로 이름 비교에 정확성을 높였다. 다만 이름의 추가가 실시간이 아니라 주기적으로 이루어지는 때문에 정보로서 이용하기는 어려움이 있고, 지금과 같이 한달에 수십만 개의 악성코드가 발견되는 상황에서 추가적으로 운영하기는 어렵다고 할 수 있다.



[그림 5] Virus Bulletin의 VGrep사이트

2.2 진단 능력에 대한 평가

백신의 주요 기능은 악성 코드 진단 및 치료에 있다. 따라서 백신의 진단 능력 평가가 중요한 요소 중에 하나이고 백신을 이용하는 이용자 입장에서도 매우 중요한 부분일 수 있다.

아직까지 진단 능력에 대한 평가의 객관적 지표나 절차는 마련되지 않고 있다. 이것은 백신이라는 제품의 특성과 각 나라의 문화적 상황, 컴퓨팅 환경 등도 한 원인이다. 가령 A라는 국가에서는 중요한 방어 대상이지만 B라는 국가에서는 확산조차 되지 않는 등의 지역적 성향이 달라 마땅히 좋은 지표를 만들기에 어려움이 있다.

AV업계에서는 나름대로의 기준을 적용해서 진단력을 검증받는 인증이라는 제도에 동참하고 있다. 인증에는 대표적인 인증으로 VB100 인증이 있고 나머지 CheckMark, ICSA, 중국 공안부 인증 등이 존재하며 제품으로는 CC인증도 포함되고 있다.

사실 인증에 대해서도 신뢰성을 논하기는 매우 어렵지만 VB100인증을 가장 기본으로 하고 있다고 봐도 될 것으로 본다. VB100인증은 WildList라는 백신업체 및 참여자의 보고 샘플에 대한 진단 여부를 평가하는 것으로 오진없이 100% 진단한다라는 증명이다.

VB인증에서는 악성 코드 진단 및 정상 파일 오진 여부가 파악되고 있으며 백신의 성능에 대해서도 평가를 진행한다. 이들 인증 각 국가별로 적용이 상이한 측면이 있다.

특별한 경우가 중국 공안부 인증으로 중국내 사업을 진행하기 위해서는 공안부 인증을 받아야 한다. 인증 방법은 샘플에 대한 진단 및 오진 테스트 항목을 포함하는 것으로 국가가 최소한의 신뢰성을 보장하겠다는 취지로 이해할 수 있을 것이다.

이러한 인증이나 비공식 테스트 모두 백신의 객관적 성능을 파악하기 힘들고 백신 업체의 가장 큰 역량은 대응 역량으로 악성 코드 발견 및 사고 대응에 관한 부분으로 그에 대한 평가 지표에 대한 논의가 업계 내에서도 수년째 활발이 이뤄지고 있지만 협의에 이르기는 어려움이 있어 보인다.

3. 결론

악성 코드의 발전은 눈에 보이는 발전이라기보다는 컴퓨팅 환경에 따른 변화가 원인이 된 것으로 본다. 어떻게 하면 원하는 목적을 달성하기 위해 사용자 모르게 시스템을 감염시킬 수 있는지 컴퓨팅 환경에 따라 진화해 온 것이다. 네트워크가 덜 발달된 2000년 이전엔 컴퓨터 바이러스가, 그 후엔 웜이 대세였고, 웹과 인터넷이 발전하면서 트로이목마가 피해를 입히는 주범이 되고 있다. 나름대로 변화되는 환경에 적응해 가면서 악의적인 기술의 발전 및 피해 규모의 확산이라는 문제를 사용자에게 남겨준 것이다.

예전에는 1년 또는 몇 년에 걸쳐 신고되는 악성코드의 양이 이제는 한달만에 신고될 정도로 60만~70만

개의 악성코드가 신고되고 있다. 과거와 달리 어느 하나의 방어 기술로만 악성코드나 해킹을 막기는 어려운 상황이고 다시 국지적인 특징을 보이기 때문에 보안 전문 업체의 역할이 더욱 중요해졌고 보안 관련 솔루션과 보안 서비스의 빈 틈을 사용자의 보안의식 제고와 함께 컴퓨팅 환경에 따라서 적절히 변화해야만 피해를 줄일 수 있을 것으로 본다.

물론 그에 발 맞춰 보안 업계의 노력도 더욱 더 필요하다고 할 수 있겠다.

참고 문헌

[HJ0710] Kyu-Beom Hwang and Deok-young Jung, "ANTI-MALWARE EXPERT SYSTEM", VB2007.

[GL0710] Guilaume Lovet, "MENACE 2 THE WIRES: ADVANCED IN THE BUSINESS MODELS OF CYBER CRIMINALS", VB2007

[DA0509] "재주는 한국이 부리고 돈은 중국이 갖는다?" http://gamedonga.co.kr/gamenews/ gamenewsview.asp?sendgamenews=14183

[PC0805] 믿지 못할 IT 코리아, http://www.ebuzz.co.kr/content/buzz_view.html?ps_ccid=51455

[CB0807] "미래에셋 해킹 뒤 금품 요구한 일당 검거", http://www.cbs.co.kr/Nocut/Show.asp?IDX=889360

[DA0805] "대부업자가 미국인 해커 고용…저축銀 7곳서 고객정보 빼내", http://www.donga.com/fbin/output?n=200805280128