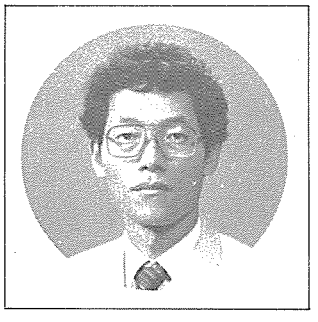
컴퓨터바이러스의 정의, 종류 및 작동원리

요사이 컴퓨터 관련 잡지 뿐만 아니라 일간 신문이나 잡지에서도 컴퓨터 바이러스에 관한 기사를 찾아보는 것은 어렵지 않다. 바로 며칠 전 우리나라에서는 매우 큰 연구소에 속하는 한국표준연구소의 전산실이 컴퓨터 바이러스의 침입을 당했다는 보도가 있었다.

여기서 우리가 알 수 있는 것은 컴퓨터 바이러스에 대한 것이 자주 지면을 장식하고 있으나 아직도 일반인들의 인식이 매우 낮은 편이며 피해 대상자인 컴퓨터 분야 종사자들도 이에 대한 대비가 안되어 있다는 것이다. 피해가 엄청난 컴퓨터 바이러스에 대한 이해를 높이기 위해 그 종류 및 특징들에 대하여 알아보고자 한다.

"다양한 技能과 種類로 被害커"



박 명 순
〈高麗大工大電算學科교수〉

바이러스 하면 우리는 쉽게 생물학적 바이러스를 떠오릴 수 있다. 이러한 바이러스는 대상물(예를 들어 우리 인간)에 침입하여 병을 일으키게 하며 또 다른 사람한테 전염을 시키기도 한다. 그러나 이러한 바이러스가 모든 사람한테 침투하는 것은 아니며 우리가 평상시 몸을 깨끗이 한다든가 혹은 예방 주사를 맞음으로써 이에 대비가 가능하다.

명칭에 '바이러스'라는 말이 붙어 있는 점에서 유추할 수 있듯이 컴퓨터 바이러스도 이와 비슷한 일을 한다. 다만 생물학적 바이러스와는 달리 컴퓨터 바이러스의 경우 대상물이 컴푸터라는 것과 바이러스균이라고 볼 수 있는 것이 생물학적 바이러스에서 처럼 어떤 생명력을 가지고 있는 것이 아니라 단지 컴퓨터 내부에서 돌아가는 프로그램에 지나지 않는다는 것이다.

이러한 생명력이 없는 프로그램에 지나지 않는 것이 어떻게 다른 대상물(컴퓨터)에 침투하며 또

어떤 병을 일으키며, 이것을 예방하려면 어떻게 해야 되고 또 병에 걸렸을 경우에는 어떻게 대처해야 하는가?

우리가 컴퓨터에서 어떤 일을 하기 위해서는 그 일을 위한 프로그램을 실행시키면서 적절한 데이타를 제공해야만 한다. 이렇게 함으로써 자신이 원하는 바를 달성할 수 있게 된다. 그러면 컴퓨터가 병이 난다는 것은 무슨 뜻인가? 사람이 어느 곳이 아프면 경우에 따라서 몸의 일부분을 전혀 쓸 수가 없게 되든지 쓸 수가 있더라도 힘이 약해지고 정신이 희미해져 원하는 바를 제대로 할 수가 없게 된다.

컴퓨터가 병이 난다고 하는 것도 이와 같다. 컴퓨터를 구성하고 있는 하드웨어의 어느 부분을 망가뜨린다든지 혹은 프로그램이 제대로 시행되도록 도와주고 있는 부분이나 데이타를 교묘히 바꿔 놓아서 어떤 프로그램을 실행시켜도 다른 일을 하거나 결과가 나오더라도 원래 나와야 하는 것과는 틀린 결과가 나오도록 만든다. 병균이 그러하듯이 컴퓨터 바이러스도 나쁜 일 만을 골라하기 때문에 더욱 문제가 된다.

어떤 일을 하기 위해 프로그램을 만들 경우에 이 같은 바이러스 프로그램을 일부러 만들어 넣을 사람은 없을 테니까 바이러스는 이같은 프로그램들이 실행될 때 끼어들어 자기가 원하는 바를 해야 한다. 그런데 이같은 감염대상프로그램들은 제각기 하는 일에 따라 프로그램 길이뿐만 아니라 구성이 매우 다르다.

이런 전염대상프로그램에 끼어들어 원하는 바를 하려면 그 프로그램을 살펴보고 자기가 끼어드는 위치를 잡아야 한다. 심부름꾼이 심부름할 때 주인이 시킨 일 이외에 다른 일을 하도록 만들려면 주인이 심부름꾼한테 준 일을 처리하도록 한 명령들이 써 있는 종이에 자기가 원하는 바를 끼어 넣어야 하는 것과 같다.

즉, 바이러스에 걸린 프로그램이 실행 중 자기 자신을 수정할 수 있는 능력이 있어야 한다. 이것을 '자기수정 능력'이라고 한다. 또한 다른 프로그램에 전염시켜야 하기 때문에, 즉 균(즉, 바이러스 프로그램)을 퍼뜨리기 위해서는 자신을 다른 프로그램에 복제할 수 있는 능력이 있어야 한다. 이것을 '자기복제능력'이라고 한다.

이렇게 하여 다른 프로그램도 자기와 같은 즉 바이러스 프로그램을 가지고 있게 만듬으로써 전염이 되는 것이다. 컴퓨터 바이러스의 또 다른 특징중의 하나는 면역성을 가질 수 있다는 점이다. 가령 감기는 평생에 걸쳐 여러번 걸리지만 홍역 같은 것은 한번 밖에 걸리지 않기 때문에 우리는 예방주사를 맞음으로써 면역성을 가질 수 있다. 컴퓨터 바이러스도 마찬가지이다.

어떤 바이러스는 한번 걸리면(즉, 바이러스 프로그램이 복제, 삽입되어 있으면) 다시는 또 한번 삽입(감염)되지 않는 반면에 어떤 바이러스는 몇번이고 같은 프로그램을 감염시킬 수 있다.

이상에서 살펴본 바를 정리하면 컴퓨터 바이러스는 다음과 같이 정의될 수 있다.

① 컴퓨터 바이러스는 전염대상 프로그램의 구조를 바꾸어 놓는다.

② 컴퓨터 바이러스는 어느 특정 프로그램 하나만을 전염시키는 것이 아니라 많은 프로그램에 대해 전염시킬 수 있다.

③ 컴퓨터 바이러스는 대상프로그램이 자기 바이러스에 전염되었는지 판단할 능력을 가지고 있다.

④ 감염인식후 같은 프로그램을 또다시 감염시키지 않는다.

⑤ 바이러스 프로그램에 의해 감염된 프로그램은 위의 ①에서 ④까지의 모든 특징을 가진다.

컴퓨터 바이러스의 위험성

위에서 이야기한 바와 같이 컴퓨터 바이러스에 전염된 프로그램은 중요한 자료를 없앤다든지 함으로써 피해를 입힌다는 것을 알았다. 이에 대하여는 자세히 알려진 것이 없고 단편적인 이야기들만 떠도는 실정이다.

그 이유는 개인적인 자료인 경우에는 본인 자신만 피해를 당하는 것이므로 다른 사람에게 알릴 필요가 없기 때문이고 또 공공기관에서 쓰는 자료인 경우에는 알려지면 공신력 문제가 제기되

어 그냥 쉬쉬하면서 넘어간다고 추측되어진다. 단지 며칠 전 신문에 보도된 사실들로부터 플로피 디스크인 경우 약 70%정도 감염된 경험이 있어 피해가 어떠했으리라는 것을 상상하게 만들 뿐이다.

그러면 왜 이와 같이 엄청난 피해가 생기는 것일까? 가장 큰 이유는 컴퓨터 바이러스의 전파 속도에 있다고 하겠다. 예를 들면, 바이러스 프로그램이 한번 수행되면 바이러스에 감염된 프로그램이 둘로 늘어가고 다음에는 4개, 그 다음엔 8개 등으로 불어난다.

이것은 한번 수행시 하나를 복제하는 경우이고 여러번 복제하도록 되어 있다면 이의 전파 속도는 2배 형태가 아닌 N배씩 불어나게 되어 엄청나게 빨라질 것이다. 이를 더욱 빨리 퍼뜨리기 위해 아예 RAM(대표적인 주기적 장치임)에 상주하여 대상 프로그램만 실행되면 무조건 전염시키도록 만든 것이 요사이의 바이러스 프로그램들이고 보면 그 전파 속도는 짐작하고도 남음이 있다.

이러한 전파 속도를 가진 바이러스 프로그램이 여러 사람이 공유하는 자료를 대상으로 파괴하였을 경우에는 참으로 커다란 문제가 야기된다. 왜냐하면 요사이 공공기관과 기업의 많은 업무가 컴퓨터에 의해 처리되고 있고 또 파괴되어 버린 자료를 복원시키는 것은 엄청난 작업을 필요로 하기 때문이다. 더욱 문제가 되는 것은 이러한 일을 자주 겪게 됨으로써 갖게 되는 심리적 불안감이다.

우리가 기계에 일을 시키는 가장 큰 이유 중 하나는 기계는 시킨대로 정직하게 반응하기 때문에 그 결과를 믿을 수 있다고 생각하기 때문인데 예측할 수 없는 일이 빈번하게 일어날 경우에는 제대로 나온 결과조차도 반신 반의하게 되어 이러한 믿음이 쉽사리 깨어지기 때문이다. 실제로 바이러스에 걸려 손실을 당한 경험이 있는 사람들은 상당한 기간 컴퓨터 쓰기가 겁이 났던 경험들을 많이 가지고 있을 것이다.

지금까지 알려진 바로는 컴퓨터 바이러스가 IBM-PC 계열의 컴퓨터에서 제일 많이 나타난다고 한다. 이것은 물론 개인용 컴퓨터가 제일 많이 보급되어 있어서 이기도 하지만 그 보다는 개인용 컴퓨터에서 쓰고 있는 운영 체제인 DOS가 컴퓨터바이러스에 대해 무방비 상태에 있기 때문이다. 개인용 컴퓨터가 만들어질 때에는 개인이 혼자 쓴다고 생각하고 설계했으므로 필요 자원들을 어떠한 제한없이 쓰도록 했고 시스템 기능을 사용자들한테 전부 공개하여 사용자들이 이것들을 마음대로 활용할 수 있도록 했기 때문이다.

종류 및 작동원리

그러면 이러한 컴퓨터 바이러스의 동작 원리와 특성을 종류별로 나누어 생각해 보자. 일반적으로 바이러스 프로그램을 나누는 방법에는 두가지가 있는데 하나는 Ross Greenberg의 분류 방법이고 다른 하나는 Ralf Burger의 분류방법이다.

Ross Greenberg는 바이러스의 기능을 기준으로 벌레 프로그램, 트로이 목마 프로그램, 컴퓨터 바이러스 프로그램등 3가지로 분류하였는데, 우리가 일반적으로 말하는 컴퓨터 바이러스는 세번째인 컴퓨터 바이러스 프로그램을 의미한다. 벌레 프로그램은 초창기 형태의 것으로 비교적 악영향을 미치지 않는다. 이 프로그램은 컴퓨터내의 다른 시스템에는 영향을 미치지 않고 단순히 자신이 허용가능한 권한내에서 자기 자신을 계속 복제하는 프로그램이다.

따라서 다른 곳에 대한 직접적인 영향은 없고 자신의 크기가 점점 커진다는 점이 특징이다. 트로이 목마 프로그램은 사용자가 모르는 다른 기능을 프로그램에 포함시켜 시스템을 파괴한다는 점에서 상당히 위험하다. 그러나 이 트로이 목마 프로그램은 스스로 증식을 하지 않기 때문에 감염된 프로그램을 실행시키지 않는 한 영향을 미치지 않는다는 점이 특징이다. 트로이 목마 프로그램의 변형인 컴퓨터 바이러스는 여기에 스스로 증식할 수 있는 기능을 포함시킨 프로그램이므로 다른 프로그램들에 대한 전염이 심각한 문제가 된다.

왜냐하면 감염된 프로그램 수가 늘어남에 따라 이들이 실행될 확률이 높아지기 때문이다. 우리

가 관심을 가지고 있는 종류가 바로 이것이며 여기에는 잘 알려진 (C) Brain, LBC 그리고 예루살렘 바이러스 등이 있다.

Ralf Burger는 세번째 종류인 컴퓨터 바이러스를 바이러스가 기생하는 장소에 따라 분류하였다. 보통은 감염된 프로그램의 맨 앞이나 맨 뒤 또는 RAM에 상주하든가 아니면 자신이 몰래 숨어있는 곳을 따로 만들어 놓고 그곳에 기거하든가 하게 되는데 이에 따라 다음의 4가지 종류로 분류된다.

겹쳐쓰기(Overwriting) 바이러스

이것은 감염대상 프로그램의 맨 앞부분에 바이러스 프로그램 자신을 복사하는 바이러스 프로그램이다. 그런데 대개의 상업용 프로그램들은 프로그램 화일의 앞 부분을 회사 이름 등, 그 프로그램에 대한 정보 또는 프로그램의 데이타를 저장하는 영역으로 쓰고 있다. 이 중요한 부분에다 바이러스 프로그램을 겹쳐 쓴 것이 되어 실제로 실행시켜 보면 대부분이 제대로 실행되지 않는다.

즉, 감염된 직후 증상이 나타나 별로 문제가 되지 않는다. 그러나 만일 제대로 실행된다면 이 형태의 바이러스는 찾아내기가 아주 힘들게 된다. 감염 대상 프로그램의 감염 전 크기와 감염 후 크기가 같기 때문이다.

덧붙이기(Non-overwriting) 바이러스

앞에 설명한 겹쳐쓰기 바이러스가 증상을 금방 드러내어 소기의 목적을 달성하지 못하자 나타난 것이 덧붙이기 바이러스 프로그램이다. 이는 바이러스 프로그램이 원하는 일(즉, 파괴활동 및 전염)을 할 뿐만아니라 원래 프로그램에 원했던 일을 하도록 해 줌으로써 주의 깊게 살피지 않는 한 눈치채지 못하도록 하기 위해서이다. 원래의 프로그램이 일을 제대로 하도록 하려면 원 프로그램을 파괴하지 않아야 하며, 바이러스 프로그램을 원 프로그램의 맨 뒤에다 그냥 덧붙이기만 하면 원 프로그램만 실행하고 끝내고 말테니까 소기의 목적을 달성할 수 없다.

그래서 바이러스 프로그램은 대상 프로그램을 전염시킬 때 다음과 같이 한다. 비유를 들어 설명하면 바이러스 프로그램이 대상 건물을 만나면 대상 건물안에 사람들이 차지하고 있는 사무실들의 맨 끝에 자기 사무실을 만들고 거기에 자기 자신을 복제한다(즉 똑같이 생긴 사람을 집어 넣는다).

그 다음에는 건물 입구에다(즉 전체 프로그램의 맨 앞) '이 건물을 들어오는 사람은 사무실 ××××(즉 바이러스 프로그램이 있는 곳)으로 오시오'라는 팻말을 써 놓아 사람들이 자신의 방으로 찾아오게 만들어 바이러스 자신의 일 즉, 그 손님을 감염시키고 또 원하는 파괴 행위를 하도록 한다. 그 다음에 그 팻말자리에 원래 있던 것을 복구 시킨 후 자신을 찾아 왔던 사람을 입구로 데리고 가서 그 손님이 원하는 일을 하도록 한다. 이렇게 함으로써 바이러스 자신의 일을 먼저 처리한 후 그 손님의 일도 제대로 처리하게 만들어 외부에서 보기에 의심을 사지 않도록 한다.

그러나 이 경우도 자세히 살피면 그 손님이 건물에 들어가서 일을 마치고 나오는 시간이 평상시보다 오래 걸리며 또한 사무실의 갯수도 옛날보다 많아졌다는 것을 알 수 있으므로 감염 여부를 알아낼 수 있다.

메모리 상주 바이러스

위 덧붙이기 바이러스의 경우에는 문제가 되는 것은 '건물 입구에 팻말을 갖다 놓고 사무실을 차려주고'하는 사람이 바이러스에 감염된 사람이라는 것이다. 다시 말하면 이 일을 하기 위한 연장 등이 들어있는 창고 열쇠가 바이러스에 걸린 직원한테 주어지지 않는 한(즉 바이러스에 걸린 프로그램이 CPU가 할당되어 실행되지 않는 한) 아무일도 안 일어난다는 것이다.

그래서 생겨난 것이 메모리 상주 바이러스인데 이것은 바이러스 프로그램이 한번 실행될 때(즉 처음 직원으로 채용될 때) 사무실을 만들어 놓고 빌딩 안내판의 일부를 바꾸어 다른 일(가령 A라는 일)로 찾아 온 손님을 바이러스 자신의 방으로 오도록 만들어 찾아올 때마다 전염시키며 이 전염된 사람이 다른 빌딩의 직원으로 채용되면 똑 같은 일을 하게 되어 전파 속도가 엄청나게

빠르다는 것이다.

즉, A라는 일을 하기를 원했던 손님은 모두 감염되고 이 사람들이 또 다시 A라는 일을 원하는 다른 사람들을 감염시키는 것이다. 이 경우에도 감염을 시킨 후에는 A라는 일을 하도록 해 줌으로써 쉽게 눈에 띄지 않도록 한다.

호출 바이러스

위와 같은 바이러스들은 하는 일이 다를 뿐 화일의 뒷 부분에 기생하는 점이 공통된 특징이다. 따라서 자세히 살펴보면 화일의 크기(즉, 프로그램 크기)가 늘어난 것을 금방 알 수 있어 찾아내기는 어렵지 않다. 그런데 이 호출 바이러스는 다른 바이러스와는 달리 눈에 잘 띄지 않도록 만들어진 바이러스 프로그램이다.

이 바이러스는 자기자신은 숨을 곳을 마련해 놓고(즉, 새로운 화일을 만듬) 화일 속성을 변환시켜 사용자의 눈에 띄지 않게 한다(즉, 미등록과 비슷). 그런 후에는 감염시킬 때는 감염대상 프로그램에는 자신을 호출하도록 호출 명령어 하나만 써 넣는다. 일단 호출되면 자신이 달려와 자신의 일을 처리한다. 이렇게 하면 감염된 프로그램 화일의 크기가 감염되기 전과 거의 같아 눈에 잘 띄지 않는다.

이상에서 우리는 컴퓨터 바이러스가 가하는 피해는 어떠한가, 이를 하기 위해 가져야 되는 특성은 무엇인가, 또 그들의 종류에는 어떠한 것들이 있는가, 그리고 그들은 어떻게 동작하는가에 대하여 알아보았다. 다른 사용자의 자료를 파괴하기 위해서 또는 경쟁상대 회사의 제품이나 신뢰도를 파괴하기 위해서 컴퓨터 바이러스를 만드는 일은 명백한 범죄행위이다.

해외화제

약을 微小 캡슐에 담아 癌細胞에 전달한다

환부에 약을 전달하는 새로운 방법을 영국에서 실시하는 초기시험으로, 암환자의 생존기간이 4배로 불어나고 있다.

스코틀랜드에 있는 스트래스클라이드 대학교 약학과의 토니 웨이틀리 박사는 지방병원의 두 연구원과 함께 암환자의 종양부위에 효과적이기는 하나 매우 독성이 강한 약을 정확히 전달하는 새로운 접근방법을 개발하고 있다. 웨이틀리 박사는 초기시험의 결과 이 새로운 약품 전달방법은 간암환자에게 수명을 새로 연장시켜 줄 수 있다는 낙관을 하게 해 주었다고 말하고 있다.

그것은 암세포뿐 아니라 다른 건강한 세포에도 치명적인 영향을 주는 제암계 「마이토마이신C」를 미소한 마이크로캡슐에 담고 이 캡슐을 약의 방출을 지연시켜 주는 물질로 코팅하는 방법이다. 이 캡슐을 간동맥과 간의 순환기계통에 주사하여 종양부위에 들여보내는 것이다.

이 기법을 이용하여 의사들은 약을 정상투여량의 3, 4배나 더 투여할 수 있고, 따라서 큰 암을 다스리는 기회는 더 커지는 것이다.

웨이틀리 박사와 그의 두 동료인 외과의사 콜린 맥아들씨와 종양학자 데이비드 커 박사는 지금 이 약품 전달방법을 임상시험에 붙일 계획을 세우고 있으며, 그 개발의 경과와 초기시험의 결과를 지난 4월 초에 개최된 마이크로캡슐 기술에 관한 제7회 국제심포지움에서 상세히 보고했다. 이 심포지움은 스트래스클라이드 대학교 약학과에서 주최했다.