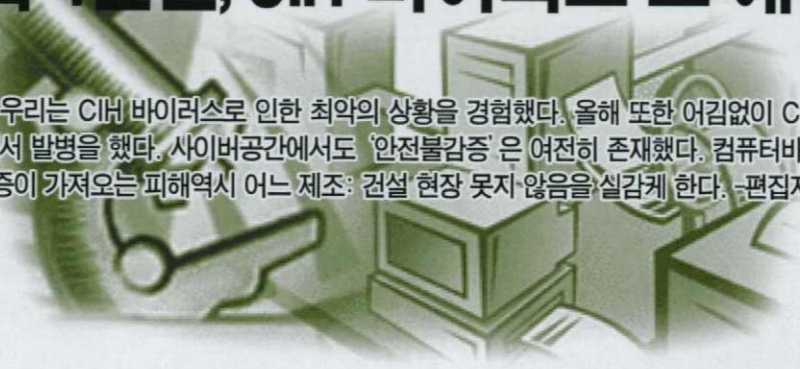
공포의 4월말, CIH 바이러스 그 예방과 치료



지난해 우리는 CIH 바이러스로 인한 최악의 상황을 경험했다. 올해 또한 어김없이 CIH 바이러스는 여러 곳에서 발병을 했다. 사이버공간에서도 '안전불감증'은 여전히 존재했다. 컴퓨터바이러스에 대한 안전불감증이 가져오는 피해역시 어느 제조 건설 현장 못지 않음을 실감케 한다. -편집자-

제작 시점, 유포 경로

지난해 우리는 CIH 바이러스로 인해 엄청난 피해를 경험했음에도 불구하고 바이러스 점검을 소홀히 한 결과 올해도 그 피해를 감수해야만 했다.

CIH 바이러스는 98년 4월 대만에서 제작되어 대만 지역 인터넷 뉴스 그룹에 올려진 후 일부 셰어웨어 프로그램에 감염된 채 전 세계로 확산되었다.

우리 나라에는 98년 6월 동영상으로 볼 수 있게 하는 셰어웨어 프로그램 MoviePlay 1.46버전에 감염된 채 통신망을 통해 유포되기 시작했고 일부 해적판 소프트웨어에 감염된 채 FTP 등을 통해 널리 퍼져 많은 피해가 발생했다. 윈도우 95/98용 실행 파일을 감염시키는 바이러스로, 윈도우 NT에서는 감염은 되지만 작동은 하지 않는다. 감염 파일 내부에는 "CIH v1.2 TTIT"라는 문자열이 존재한다.

특징 및 증상

CIH 바이러스는 그 파괴력이 과히 원자폭탄의 위력에 맞먹는다고 해도 큰 과장은 아니다. 하드 디스크를 데이터를 완전히 삭제(포맷)하고 BIOS 내용을 파괴해 '뇌사 상태'로 만드는 악성 바이러스에 속한다.

BIOS의 파괴 여부는 메인보드의 세팅 상태에 따라 달라진다. 최근의 BIOS들은 소프트웨어적으로 업그레이드할 수 있어서 쓰기가 가능한데, CIH는 이 점을 악용해서 엉뚱한 값을 BIOS에 써버려 CIH가 본격적인 활동을 개시하는 26일에는 시스템이 먹통 상태가 되어 부팅조차 안되는 현상이 발생한다.

BIOS(Basic Input Output System. 기본입출력장치)란 컴퓨터를 작동하게 하는 모든 제어 장치에 대한 정보를 담고 있는 칩으로, 이것이 손상되었을 때 컴퓨터는 고철 덩어리에 불과하다. 이 바이러스가 WinZip Self Extracter 파일에 감염되면 자동풀림 실행 압축파일에 에러가 있는 것으로 판단해 아래와 같은 메시지를 출력한 후 압축이 풀리지 않는 문제가 발생한다. 이는 날짜에 관계없이 나타나는 증상이다.

"Winzip Self-Extractor header corrupt.
Possible cause: bad disk or file transfer error"

CIH는 바이러스 제작자 이름 첸잉하오(Chen Ing Hou)의 이니셜이다. '체르노빌'이란 별명은 바이러스 활동일인 매년 4월 26일이 구 소련의 체르노빌 원전사고일과 같아서 붙여진 이름이다.

감염 방법

바이러스에 감염된 파일이 실행되면 기억장소에 상주한 후 오픈되는 PE(Portable Executable) 파일을 감염시킨다. 당시 기존의 윈도우 기반 바이러스들은 주로 VxD를 사용해서 재부팅한 후 바이러스가 상주하지만, 이 바이러스는 비공개 기법을 사용했다. 또한 파일 감염 방법 역시 기존 방법과 달리 파일에서 빈 영역을 찾아 겹쳐 쓰는 방법을 사용해 감염된 파일 크기에 변화가 없는 것도 특징이다.

감염 경로

국내에 처음 유포된 것은 지난해 6월 동영상을 볼 수 있는 셰어웨어 프로그램 무비플레이 1.46버전을 통해서다. 그 이후의 감염 경로는 대략 3가지 정도로 추정된다.

첫째, 컴퓨터 잡지 부록 CD와 통신 프로그램 CD, 아동 학습지 CD, 국산 워드프로세서 정품 CD 등 알려진 경우만 6건에 이를 만큼 공식 통로를 통한 유포가 심각한 수준이다.

둘째, 스타크래프트 게임 CD 등 불법복제한 프로그램을 통해 대거 유포되었다.

셋째, PC 통신이나 인터넷에 올려지는 실행 파일 대해 운영자가 관리를 소홀히 할 경우 감염된 파일이 게시되어 불특정 다수가 이를 내려받아 감염되는 경우도 많았다.

CIH 바이러스의 각 버전별 특징

CIH 바이러스는 소스가 공개되어 있기 때문에 많은 변종이 만들어질 가능성이 매우 높다. 공식적으로 CIH 1.2 1.3 1.4 1.5까지 있으며 매년 4월 26일에만 활동하는 원형과 매월 26일 활동하는 변형이 있고 아무런 파괴증상을 하지 않고 단순히 감염 증상만 나타내는 것도 있다.

이를 치료하는 백신은 이미 배포되고 있으므로 최신 엔진으로 업데이트한 후 바이러스를 검사해 아무 이상이 없다면 4월 26일에도 컴퓨터를 사용할 수 있다.

비코딘(멜리사 바이러스 제작자)이 만든 바이러스를 TNT 또는 remix CIH 바이러스라고 부르며 다음과 같은 내부 문자열이 있다.

	버전	활동일	감염크기	내부문자열
원형	V1.2	4/26	1003	CIH v1.2 TTIT
	V1.3	4/26	1010	CIH v1.3 TTIT
	V1.4	매월 26일	1019	CIH v1.4 TATUNG
	V1.5	매월 26일	모름	WinCIH ver 1.5 by TATUNG, Thailand
변형	V1.2	4/26	1019	CIH v1.2 TTIT
	V1.4	매월 26일	1035	CIH v1.4 TATUNG
	VicodinES	파괴증상없음	1024	하단 참조

CIH 〈TNN Remix〉 writen by TTIT of TATUNG —{.}—
remixed by VicodinES —{.}—
The Narkotic Network Virus Warehouse
http://users.skynet.be/somnus/virnvw.html —{.}—
.Vic.s Not Workin. With A Full Deck!

참고 사례

CIH 바이러스는 윈도우 NT에서 감염 활동은 하지 못해도 윈도우 NT 파일을 감염시킬 수는 있다. 모 회사의 경우 CIH 바이러스가 회사 서버에서 발견되어 확인한 결과 이 회사는 사원 로그온 기록을 NT 서버에서 특정 폴더를 읽기/쓰기 권한을 부여해 관련 파일이 감염되었다.

또한 해당 파일은 로그온 프로그램으로 전사원이 동시에 사용하므로 CIH 바이러스가 전체 회사 컴퓨터에 감염되어 회사 업무가 한동안 마비된 경우도 있었다.

따라서 전사원이 공유하는 폴더는 서버용 백신 프로그램으로 관리하고 가급적 전사원이 함께 공유하는 읽기/쓰기 폴더는 없애고 파일 교환시 임시 폴더를 사용하도록 해야 한다. 중요한 자료는 PC 내의 하드 디스크 이외에 별도의 저장 매체에 담아 두는 지혜도 필요하다.

대비책

현 시점에서 대처할 수 있는 방법은 V3Pro 2000 Deluxe나 V3+ Neo 최신 버전으로 진단해 치료하는 것이다. V3는 안철수연구소 홈페이지(www.ahnlab.com)와 PC 통신망(천리안, 하이텔, 나우누리, 유니텔 GO AHN)에서 내려받을 수 있다. 이외에 PC사용자가 알아야할 사항을 요약하면 다음과 같다.

●개인 사용자 지침

1. *비상시 데이터 손실을 최소화하기 위해 데이터는 사전에 정기적인 백업을 해놓는다.*
2. *백신 소프트웨어의 시스템 및 인터넷 감시 기능을 이용해 바이러스를 사전 검색한다.*
3. *출처가 불분명한 Email 첨부 파일의 경우 실행 전에 백신으로 검사하거나, 삭제한다.*
4. *불법복제된 제품의 경우 바이러스 감염 우려가 높으므로 정품 소프트웨어만을 사용한다.*
5. *비상시 대비 복구 디스켓을 준비해 놓는다.*
6. *안철수연구소 웹사이트(www.ahnlab.com)에 접속하여 관련 정보를 미리 숙지한다.*

● 기업 사용자 지침

1. 중요한 데이터를 수시로 백업하는 등 전사적인 백업 체계와 솔루션을 준비한다.
2. 최신 버전의 백신을 사용한다.
3. 백신 사용법, 바이러스 관련 정보 및 주의사항 등을 전사적으로 공지한다.
4. 파일 서버용과 이메일 서버용, 그룹웨어용 백신을 설치해 바이러스의 확산을 막는다.
5. 서버의 비인가된 부당 변경 작업 등을 확인하기 위해 체크리스트와 보안 관리 정책에 관한 지침을 마련한다.
6. 바이러스가 네트워크로 퍼질 가능성에 대비해 공유 폴더 이용에 유의한다.
7. 비상시 연락 가능한 백신 업체와 복구 업체 연락처를 알아둔다.

피해가 났을 경우 대처법

하드 디스크의 데이터가 삭제된 경우에는 복구 전문 업체에 의뢰해 복구 서비스를 받아야 한다. BIOS가 손상되어 부팅도 되지 않는 경우에는 복구가 불가능하므로 BIOS 칩을 새것으로 교체해야 한다. 이때 본인이 사용하고 있던 것과 같은 것을 구입해야 한다. 컴퓨터 생산 업체의 AS센터나 컴퓨터 전문수리 업체 등에 문의해 전문가의 도움을 받는 것이 좋다.

99년 피해 규모

99년 4월 26일에 안철수연구소로 접수된 피해 사례는 모두 3,000여 건이며, 정확히 집계하기는 어렵지만 국내 보급 PC 중 30만 대 이상이 피해를 당했을 것으로 추정한다. BIOS 교체 비용이 7~20만원, 하드 디스크 데이터 복구 비용이 25~50만원인 것을 감안하면 피해 금액은 실비만 최소 210억~2100억원의 재산 피해가 난 것으로 추산된다.

특히 우리나라와 중국, 터키, 방글라데시, 홍콩 등 아시아 지역은 피해가 상당했다. 외신에 따르면 우리나라 피해 규모가 상위 5위 안에 든다는 것이다. 상대적으로 미국과 유럽의 피해는 적었는데, 그 이유는 안티바이러스 솔루션으로 조직적인 대응을 했기 때문이다.

대표적인 사례로는 S전자, H통신, K동사무소, W출판사, S병원, H건설, H대학교 등 100여 곳의 기업 사이트에서 피해를 호소했으며, 한 회사에서 많게는 300여 대까지 피해를 당한 것으로 집계되었다.

한편 안철수컴퓨터바이러스연구소에는 전화 문의가 폭주해 전화 시스템이 마비될 정도였으며, 통화 시도 대비 실제 통화 건수가 10%에 불과해 많은 고객들이 불편을 호소하기도 했다.

CIH바이러스 관련 FAQ

Q CIH 바이러스에 감염되어 모두 치료하였으나 이후부터 스타크래프트의 배틀넷 접속 및 메뉴 선택시 속도가 매우 느립니다.

A CIH 바이러스는 파일의 빈 영역을 찾아 이 곳에 바이러스가 겹쳐 쓰는 기법을 사용이다. 그래서 일부 파일의 경우 이 영역이 부족하여 감염되면서 파일이 손상되는 경우가 있다. 치료 후 프로그램이 정상적으로 실행되지 않으면 다시 설치해야 한다.

따라서 치료 후 스타크래프트의 배틀넷 접속 속도가 저하하는 것은 Windows \system 폴더의 Pstores.exe 파일이 손상되었기 때문이다. 정상적인 속도가 나는 같은 버전의 윈도우 시스템에서 해당 파일을 복사하여 덮어 쓰면 문제가 해결된다.

Q CIH 바이러스의 활동일은 매년 4월 26일이라고 알고 있다. 당일만 컴퓨터를 사용하지 않으면 바이러스에 감염되지 않는 것인가?

A 말 그대로 '활동일'이지 '감염일'이 아니다. CIH 바이러스에 이미 감염되어 있는 상태에서 특정 파괴 증상이 4월 26일에 나타나는 것이다.

Q CIH 바이러스는 하드웨어를 고장낸다고 하는데 어떤 방법을 사용하는가

A CIH 바이러스는 다른 상주형 바이러스와 동일하게 메모리에 상주하고 있다가 사용자가 실행하는 PE 형태의 파일을 감염시킨다. 이 바이러스가 활동하는 날은 매년 4월 26일이며 이날 감염된 시스템을 부팅시키면 우선 플래시 메모리 영역의 삭제(혹은 쓰레기값을 입력)를 시도한 후, 하드 디스크 맨 앞의 특정 섹터를 포맷한다. 이렇게 되면 메인보드의 롬 바이오스가 파괴되며, 하드디스크를 부팅할 수 없게 된다. 단, 일부 롬 바이오스만 파괴된다.

Q 4월 26일 부팅하지 않고 감염된 PC를 4월 25일부터 밤새도록 사용하고 있다가 컴퓨터 시계가 4월 26일로 넘어가면 어떻게 되나. 부팅은 4월 25일에 했으므로 괜찮지 않나

A 그렇지 않다. 갑자기 컴퓨터가 다운되거나, 화면에 아무런 것도 보이지 않을 것이다. 이때 사용자는 시스템을 재부팅하려고 할 것이다. 그러나 전혀 부팅이 되지 않을 것이다.

Q CIH 바이러스는 윈도우 9x에만 활동하는 것으로 알고 있는데 윈도우 NT 시스템에서도 발견됐다

A Win9x 바이러스들은 윈도우 NT에서 정상적으로 메모리에 상주하지 못하며 다른 파일도 감염시킬 수 없다. 오히려 감염된 파일을 실행하면 시스템이 다운되는 증상이 있다. 윈도우 NT에서 Win 9x 바이러스들이 발견되는 것은 윈도우 NT를 사용하는 네트워 드라이브에 감염된 파일이 있는 경우이다. 즉 사용자가 감염된 파일을 네트워 드라이브에 복사해 놓았을 경우 V3Net for Windows Server로 검사할 때 발견된다.