악성코드 분석, 암호화 및 패키징 프로젝트

컴퓨터 바이러스에 대한 보고서

문서 번호 : SRP-004

목 차

Ⅰ. 바이러스의 정의

컴퓨터 바이러스는 정상 프로그램 코드 안에 숨어 있다가 해당 프로그램이 실행될 때 함께 작동하면서 스스로를 복제하고 퍼뜨리는 악성 프로그램입니다. 웜과 달리, 바이러스는 스스로 실행되지 않고 반드시 숙주프로그램에 의존해야 합니다. 트로이 목마도 바이러스처럼 독립적인 프로그램이지만, 자기 복제 능력이 없고 사용자가 직접 실행해야만 작동한다는 점에서 바이러스와 차이가 있습니다.

컴퓨터 바이러스의 역사는 1971 년에 개발된 크리퍼 바이러스로부터 시작됩니다. 크리퍼는 실험적으로 만들어진 자기 복제 프로그램으로, 당시 인터넷의 초기 형태인 아파넷을 통해 퍼졌고 메시지를 표시하는 기능이 있었습니다. 이후, 1986 년 브레인 바이러스가 본격적인 최초의 컴퓨터 바이러스로 인식되었습니다. 초기 바이러스들은 주로 시스템을 파괴하는 목적이었지만, 시간이 지나면서 랜섬웨어처럼 금전적 이익을 목적으로 한 교묘한 형태로 발전해왔습니다. 이후, 1986 년 브레인 바이러스가 본격적인 최초의 컴퓨터 바이러스로 인식되었습니다. 초기 바이러스들은 주로 시스템을 파괴하는 목적이었지만, 시간이 지나면서 랜섬웨어처럼 금전적 이익을 목적으로 한 교묘한 형태로 발전해왔습니다.

1980 년대 이후에는 파일 바이러스, 부트 바이러스, 매크로 바이러스, 스크립트 바이러스, 암호화 바이러스 등 다양한 형태의 바이러스들이 등장했으며, 이들은 점점 더 정교한 기술을 사용하여 자신을 숨기고 복제하는 방식으로 발전했습니다. 2000 년에는 러브레터 바이러스가 전 세계적으로 수십억 달러의 피해를 일으켰고, 컴퓨터와 네트워크의 확산으로 바이러스는 개인과 기업뿐만 아니라 국가 기반 시설에까지 심각한 위협을 가하는 중용한 문제로 자리잡게 되었습니다.

Ⅱ. 바이러스의 유형

2.1 파일 바이러스

파일 바이러스는 실행 파일이나 문서 파일에 자신의 코드를 삽입하여 감염시키는 바이러스입니다. 주로 .exe 나 .com 같은 실행 파일에 감염되지만, 문서 파일(.doc, .xls 등)에도 침투할 수 있습니다. 감염된 파일이 실행되면 바이러스가 복제되어 다른 파일로 퍼지게 됩니다.

파일 바이러스는 주로 이동식 저장 매체(USB, 외장 하드디스크 등), 네트워크 공유 폴더, 이메일 등을 통해 확산됩니다. 예를 들어, 2008 년 제나 바이러스는 USB 를 통해 전 세계 수십만 대의 컴퓨터를 감염시켰습니다.

파일 바이러스를 예방하려면 백신 프로그램을 정기적으로 업데이트하고, 출처가 불분명한 파일은 실행하지 않는 것이 중요합니다. 또한 중요한 데이터는 주기적으로 백업해야 하며, 이동식 저장 매체를 사용할 때도 반드시 바이러스 검사를 실행하는 것이 좋습니다.

2.2 부트 바이러스

부트 바이러스는 컴퓨터가 부팅될 때 시스템을 감염시키는 바이러스입니다. 이 바이러스는 부트 섹터나 **마스터 부트 레코드(MBR)**에 자신을 숨겨, 컴퓨터가 켜질 때마다 바이러스가 메모리에 로드되어 실행됩니다.

부트 바이러스는 주로 USB 드라이브, 외장 하드디스크, CD/DVD 와 같은 이동식 저장 매체를 통해 전파됩니다. 초기의 대표적인 예로는 1986 년에 등장한 브레인 바이러스가 있습니다. 이 바이러스는 플로피 디스크를 통해 감염되었으며, 당시 전 세계로 확산되었습니다.

부트 바이러스를 예방하려면 출처가 불분명한 저장 매체를 사용하지 않고, 정기적인 백신 업데이트를 통해 시스템을 보호하는 것이 중요합니다.

2.3 매크로 바이러스

매크로 바이러스는 문서 작성 프로그램이나 스프레드시트 프로그램에 내장된 매크로 기능을 악용하는 바이러스입니다. 매크로는 반복 작업을 자동화하는 기능인데, 바이러스가 이 코드를 삽입하여 문서 파일이 열릴 때 실행됩니다.

이러한 바이러스는 주로 이메일 첨부 파일이나 공유 폴더를 통해 전파됩니다. 1999 년에 발견된 멜리사 바이러스는 워드 문서를 통해 확산되었고, 이메일 주소록을 사용해 바이러스를 퍼뜨렸습니다.

매크로 바이러스에 대비하려면 신뢰할 수 없는 문서를 열지 말고, 매크로 기능을 차단하거나 필요한 경우에만 신중하게 활성화해야 합니다.

2.4 스크립트 바이러스

스크립트 바이러스는 웹 페이지나 프로그램에서 사용되는 스크립트 언어를 악용하는 바이러스입니다. 자바스크립트나 VBScript 와 같은 언어에 바이러스 코드를 심어, 사용자가 해당 스크립트가 포함된 웹 페이지를 열 때 바이러스가 실행됩니다.

2000 년의 루팅 바이러스는 VBScript 를 이용해 윈도우 시스템을 공격한 예로, 이메일과 네트워크 공유 폴더를 통해 빠르게 확산되었습니다.

스크립트 바이러스를 예방하려면 보안 업데이트를 유지하고, 신뢰할 수 없는 웹 페이지나 프로그램을 실행하지 않는 것이 중요합니다.

2.5 암호화 바이러스

암호화 바이러스는 자신의 코드를 암호화하여 탐지를 피하는 바이러스입니다. 이 바이러스는 폴리모픽(Polymorphic) 또는 메타모픽(Metamorphic) 기술을 사용해 계속 변형되기 때문에 탐지와 제거가 어렵습니다.

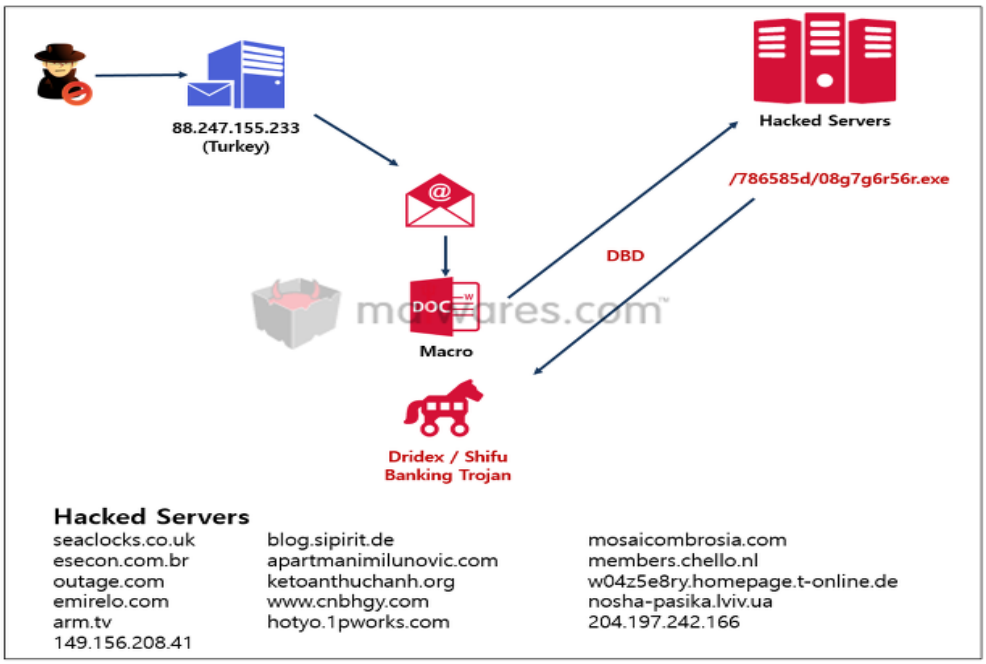
암호화 바이러스는 코드가 암호화된 상태로 파일에 포함되며, 실행될 때 복호화되어 메모리에서 동작합니다. 이러한 바이러스를 탐지하려면 고도의 분석 기술과 최신 백신 정보가 필요하며, 정기적인 백신 업데이트가 필수입니다.

Ⅲ. 바이러스 전파 방식

3.1 이메일 및 메신저 전파

바이러스는 이메일과 메신저 플랫폼을 통해 쉽게 퍼질 수 있습니다. 이메일이나 메신저는 파일 첨부와 링크 공유가 가능하기 때문에, 악성 파일이나 링크가 첨부된 메시지를 통해 바이러스가 쉽게 침투할 수 있습니다.

보통 바이러스는 실행 파일이나 문서 파일 형태로 첨부되어 전송되며, 악성 링크를 메시지에 포함시켜 사용자를 가짜 웹사이트로 유도해 감염시키기도 합니다. 특히 바이러스가 포함된 이메일은 의심스러운 제목이나 발신자가 불분명한 경우가 많으며, 피싱 이메일처럼 긴급하거나 당황스러운 내용으로 사용자를 속이는 경우도 있습니다.



3.2 이동식 저장 매체를 통한 전파

USB 드라이브, 외장 하드디스크, CD/DVD 와 같은 이동식 저장 매체는 바이러스 전파에 매우 취약한 경로입니다. 감염된 저장 매체가 다른 컴퓨터에 연결되면, 바이러스가 그 시스템으로 옮겨갈 수 있습니다.

이동식 저장 매체는 주로 세 가지 방식으로 감염됩니다. 첫째, 바이러스에 감염된 컴퓨터에 연결되면 매체 자체가 감염될 수 있습니다. 둘째, 바이러스가 포함된 파일을 이동식 매체에 복사하면 매체가 감염됩니다. 셋째, 저장 매체 자체의 보안 취약점을 악용하여 바이러스가 직접 매체에 침투할 수 있습니다.

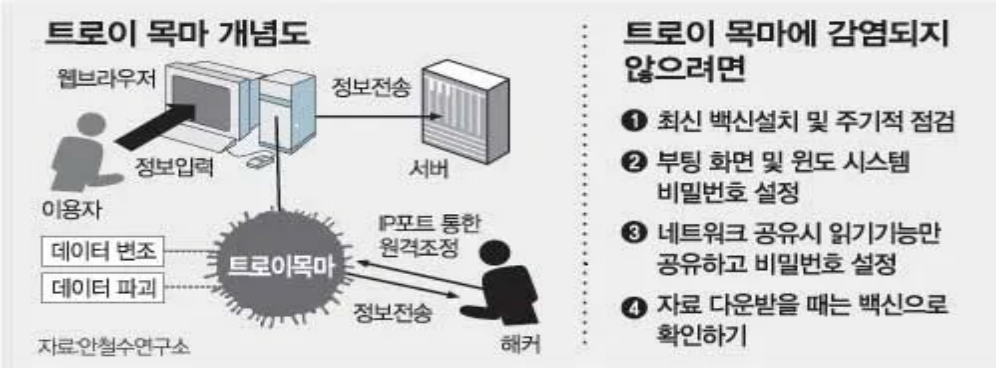
이렇게 감염된 저장 매체가 다른 컴퓨터에 연결되면 바이러스가 확산됩니다. 사용자가 매체의 파일을 열거나 복사할 때 바이러스가 실행되어 시스템을 감염시킬 수 있으며, 자동 실행 기능을 악용해 매체가 연결되자마자 바이러스가 작동하는 경우도 있습니다. 2008 년에 발견된 제나 바이러스는 USB 를 통해 전파되어 전 세계적으로 많은 컴퓨터를 감염시킨 예입니다.

< USB 웜 바이러스 전파기법 >

3.3 웹사이트 방문으로 인한 감염

웹사이트 방문도 바이러스 감염의 주요 경로 중 하나입니다. 악성 코드가 숨겨진 웹 페이지를 방문하면, 해당 웹 페이지가 로드될 때 바이러스가 자동으로 실행되어 시스템을 감염시킬 수 있습니다. 이 과정에서 자주 사용되는 공격 방법 중 하나가 **크로스 사이트 스크립팅(XSS)**인데, 공격자가 웹 페이지의 스크립트에 악성 코드를 심어 사용자가 접속할 때마다 바이러스가 실행되는 방식입니다.

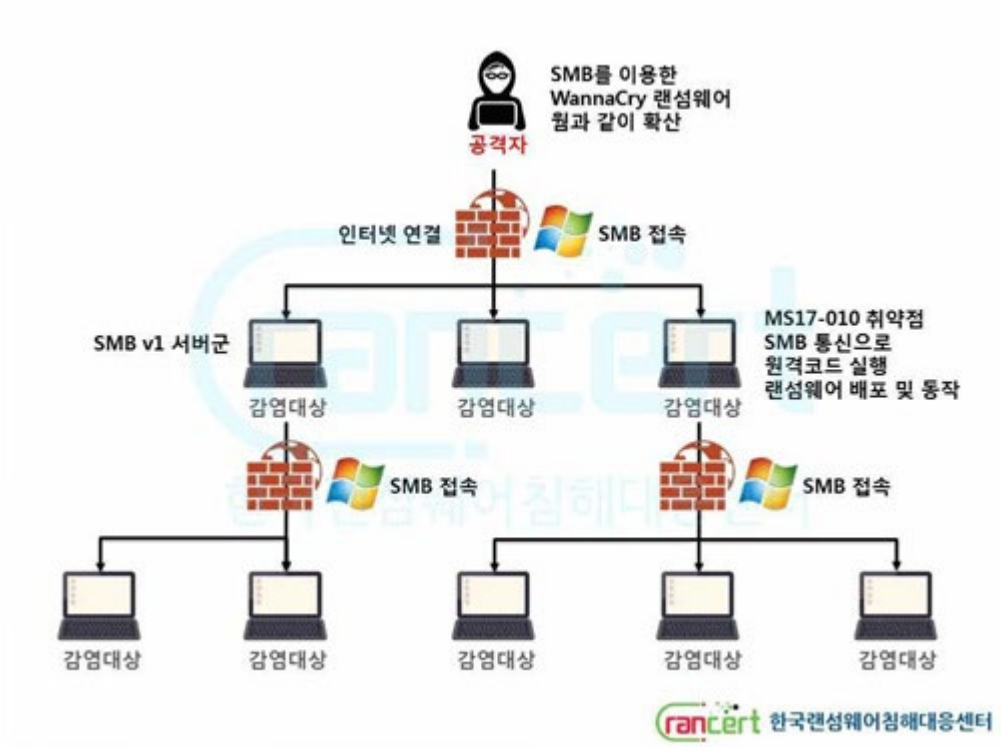
또한 웹 브라우저나 플러그인의 취약점을 이용한 공격도 흔합니다. 이런 공격은 드라이브-바이 다운로드라고 불리며, 사용자가 알지 못하는 사이에 바이러스가 다운로드되어 감염됩니다. 최근에는 익스플로잇 킷 같은 공격 도구를 웹사이트에 삽입하는 사례도 증가하고 있습니다. 예를 들어, 2016 년에는 구글 광고 네트워크를 통해 악성 광고인 말버타이징이 유포되어 많은 웹사이트 방문자가 감염된 사례가 있습니다.



3.4 네트워크 취약점 이용

바이러스는 네트워크 상의 취약점을 악용해 전파될 수 있습니다. 특히 네트워크에서 사용하는 프로토콜이나 프로그램의 보안 허점이 있다면, 바이러스는 이를 공격 경로로 삼아 빠르게 확산됩니다.

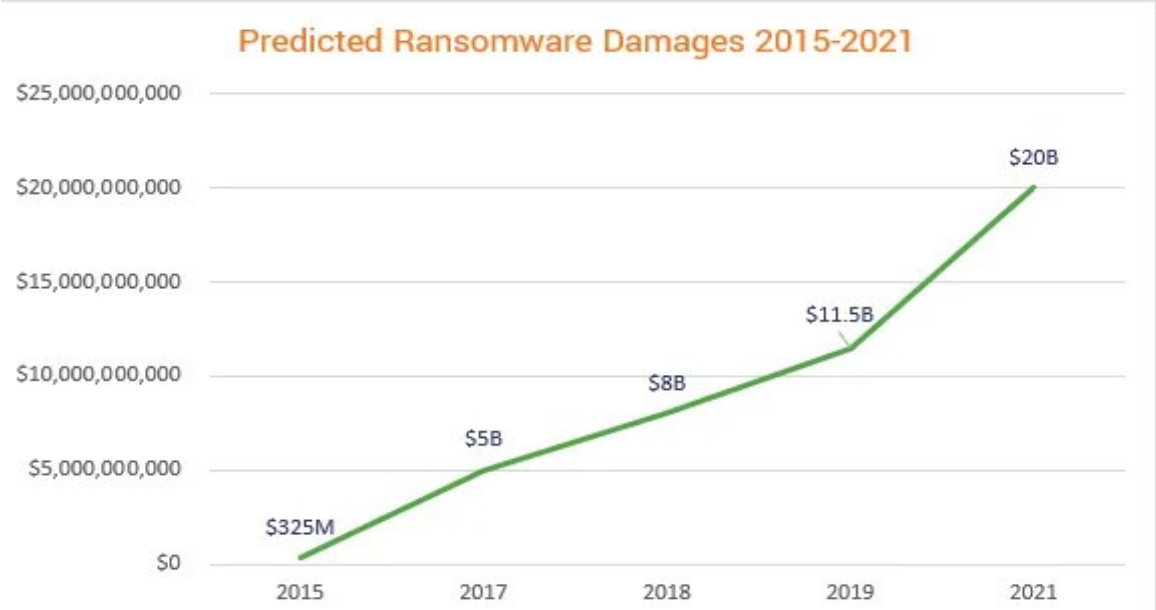
대표적인 사례로는 2017 년 전 세계에 큰 피해를 준 워너크라이(WannaCry) 랜섬웨어가 있습니다. 이 랜섬웨어는 윈도우 운영체제의 SMB(Server Message Block) 프로토콜의 취약점을 이용해 확산되었습니다. 워너크라이는 감염된 시스템에서 내부 네트워크를 따라 자동으로 확산되어 다른 컴퓨터들까지 연쇄적으로 감염시켰습니다. 이로 인해 러시아, 우크라이나, 인도, 대만 등 150 여 개국에서 큰 피해를 입었고, 특히 영국 NHS 병원 네트워크가 마비되는 등 심각한 결과를 초래했습니다.



Ⅳ. 바이러스 피해사례

과거 주요 바이러스 사건 중 2000 년 ILOVEYOU 바이러스는 이메일 첨부 파일의 형태로 전 세계로 급속히 확산되었습니다. 이 바이러스는 메일 주소록을 탈취하여 자신을 재전송함으로써 수억 달러의 경제적 손실을 입혔습니다. 2004 년 마이둠 웜 역시 이메일과 네트워크 공유 폴더를 통해 전파되어 당시 최악의 사건으로 기록되며 수백만 대 이상의 시스템을 감염시켰습니다. 2017 년 워너크라이 랜섬웨어는 운영체제 취약점을 노려 150 개국 이상에서 피해를 입혔고, 영국 NHS 병원망 마비 등 주요 인프라에 심각한 타격을 주었습니다.

개인 차원에서는 바이러스 감염으로 인한 데이터 손실과 시스템 복구 비용 발생, 개인정보 유출과 이로 인한 신원 도용 위험, 정신적 스트레스 등의 피해가 있습니다. 기업은 시스템 다운타임으로 인한 업무 마비와 생산성 저하, 데이터 유출에 따른 법적 분쟁 비용, 고객 이탈과 브랜드 이미지 실추, 바이러스 제거와 예방을 위한 보안 투자 비용 증가 등의 타격을 받습니다.



사회적으로는 주요 기반시설과 공공 서비스 마비로 인한 혼란과 경제적 손실, 국가 안보 위협 증가, 디지털 시스템에 대한 대중의 불신 확산 등의 문제가 발생할 수 있습니다. 2017 년 워너크라이 사태에서 볼 수 있듯이 병원 의료 서비스 지연으로 인한 생명 위험도 발생할 수 있습니다. 이처럼 대규모 바이러스 확산은 개인과 기업, 나아가 국가 전반에 심각한 피해를 줄 수 있는 주요 위험 요인입니다.

Ⅳ. 바이러스 예방 및 대응

컴퓨터 바이러스 위협에 효과적으로 대응하기 위해서는 예방, 탐지, 대응의 체계적인 접근이 필요합니다. 우선 예방 차원에서 바이러스 백신 프로그램을 최신 버전으로 유지하고 정기적인 업데이트를 수행해야 합니다. 새로운 바이러스 유형과 변종이 지속적으로 등장하므로 바이러스 정의 파일을 주기적으로 갱신하는 것이 중요합니다. 또한 운영체제와 애플리케이션의 보안 취약점을 해결하기 위해 공식 패치를 적시에 설치해야 합니다. 이와 함께 출처가 불분명한 파일, 웹사이트, 링크 등에 대한 실행과 방문을 자제하는 주의가 필요합니다. 개인과 기업 차원에서 바이러스 예방 교육을 통해 보안 인식을 높이는 것도 중요한 예방책입니다.

바이러스 탐지 측면에서는 실시간 검사 기능을 활성화하여 이메일, 메신저, 웹 브라우징 등에서 바이러스를 실시간으로 모니터링해야 합니다. 또한 행위 기반 탐지와 휴리스틱 분석을 통해 새로운 유형의 바이러스도 탐지할 수 있어야 합니다. 네트워크 트래픽과 시스템 로그를 모니터링하여 이상 징후를 포착하는 보안 관제도 중요한 역할을 합니다. 기업에서는 전문 보안 관제 센터를 운영하거나 외부 서비스를 활용하는 방안을 고려해볼 수 있습니다.

바이러스에 감염되었을 경우에는 신속한 대응이 필수적입니다. 먼저 정기 백업을 통해 깨끗한 상태로 시스템을 복원할 수 있어야 합니다. 감염된 파일과 프로세스는 격리 및 치료를 수행해야 하며, 상황에 따라 운영체제 전체를 재설치하는 것도 고려해볼 수 있습니다. 바이러스 확산 경로를 분석하고 취약점을 점검하여 재발 방지 대책을 마련하는 것 또한 중요합니다. 기업에서는 바이러스 대응 매뉴얼을 수립하고 전담 보안 조직을 운영하며, 직원 대상 정기 교육을 실시하는 등 체계적인 관리 체계를 갖추는 것이 바람직합니다.

바이러스 위협은 지속적으로 진화하고 있으므로 예방, 탐지, 대응의 다각적인 노력이 필수적입니다. 정기적인 보안 업데이트와 예방 조치, 다중 계층의 모니터링, 신속하고 체계적인 대응을 통해 개인과 기업은 안전한 디지털 환경을 구축할 수 있습니다.

VI. 참고 문헌

1. **“컴퓨터 바이러스 정의”,**

   https://www.fortinet.com/kr/resources/cyberglossary/computer-virus

2. **“멀웨어(Malware)란 무엇인가요?**

   https://www.ibm.com/kr-ko/topics/malware

3. **“컴퓨터 바이러스란 무엇인가?”, (2012.04.20) from**

   https://blog.naver.com/hdj20/40157301683

4. **“컴퓨터 바이러스”**

   https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0_%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4

5. **“악성코드란 무엇인가, 바이러스, 웜, 트로이목마, 그 이상의 것 이해하기”, (2018.08.14) from**

   https://www.itworld.co.kr/news/110408

6. **“컴퓨터 바이러스 유형에 따른 백신 프로그램의 성능분석 = The Performance Analysis of Vaccine Programs According to Computer Virus Classes”, (2011.02)**

   https://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=8c96bb342aac3677ffe0bdc3ef48d419&outLink=K

7. **“컴퓨터 바이러스와 소프트웨어 에러의 비교연구”, (1990.4)**

   https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE00620426