情報保護學會論文誌
第19卷 第1號, 2009. 2

전자우편을 이용한 악성코드 유포방법 분석 및 탐지에 관한 연구

양 경 철,[1†] 이 수 연,[1] 박 원 형,[2] 박 광 철,[1] 임 종 인[1‡]

[1]고려대학교 정보경영공학전문대학원, [2]경기대학교 정보보호학과

A Study on the Analysis and Detection Method for Protecting Malware Spreading via E-mail

Kyeong Cheol Yang,[1†] Su yeon Lee,[1] Won Hyung Park,[2] Kwang Cheol Park,[1] Jong in Lim[1‡]

[1]Information Management and Security CIST, Korea University, [2]Information Security, Kyonggi University

요 약

본 논문은 해커가 정보절취 등을 목적으로 전자우편에 악성코드를 삽입·유포하는 공격 대응방안에 관한 연구로, 악성코드가 삽입된 전자우편은 정보유출 時 트래픽을 암호화(Encoding)하는데 이를 복호화(Decoding) 하는 '분석모델'을 구현 및 제안한다. 또한 보안관제측면(네트워크)에서 해킹메일 감염時 감염PC를 신속하게 탐지할 수 있는 '탐지기술 제작 방법론'을 연구하여 탐지규칙을 제작, 시뮬레이션 한 결과 효율적인 탐지성과를 보였다. 악성코드 첨부형 전자우편에 대한 대응책으로 공공기관이나 기업의 정보보안 담당자·PC사용자가 각자의 전산망 환경에 맞게 적용 가능한 보안정책을 제안함으로써 해킹메일 피해를 최소화하는데 도움이 되고자 한다.

ABSTRACT

This paper proposes the detection method of spreading mails which hacker injects malicious codes to steal the information. And I developed the 'Analysis model' which is decoding traffics when hacker's encoding them to steal the information. I researched 'Methodology of intrusion detection techniques' in the computer network monitoring. As a result of this simulation, I developed more efficient rules to detect the PCs which are infected malicious codes in the hacking mail. By proposing this security policy which can be applicable in the computer network environment including every government or company, I want to be helpful to minimize the damage by hacking mail with malicious codes.

Keywords : Malicious Code, Detection Method, IDS, SNORT, Security Policy, Encrypted traffic

Ⅰ. 서 론

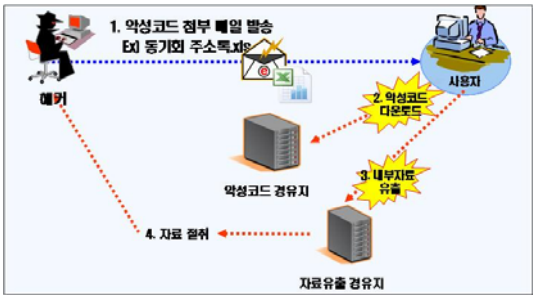
인터넷이 급속하게 보급되면서 과학기술 뿐 아니라 경제, 문화 등 사회 전반에 걸쳐 인터넷 의존도가 높아지고 있는 가운데 최근에는 해킹 기법들이 기존보다 정교한 기술력을 바탕으로 더욱 악성화가 되어가고 있다. 특히, 전자우편을 이용한 악성코드 유포 공격은 그 피해

접수일(2008년 11월 5일), 수정일(2008년 12월 23일),
게재확정일(2009년 1월 8일)
† 주저자, yes0590@gmail.com
‡ 교신저자, jilim@korea.ac.kr

가 날이 갈수록 급증하고 있으며 정보유출, 해킹 등 응용범죄의 수단이 되어가고 있다. 2008년에는 오피스 프로그램의 취약점이 발견되면서, 정상적인 문서(DOC, XLS, PDF, HWP 등)에 악성코드를 은닉시킨 후 지인으로 가장하여 국가기관의 공직자 등 특정인들에게 유포시켜 PC에 저장된 중요 자료들을 빼내가는 해킹수법이 지속적으로 발생하고 있다. 국내에서 컴퓨터 바이러스에 대한 연구는 활발히 이루어지고 있지만 해킹메일의 전파 특징과 자료절취 방법 그리고 이를 탐지, 예방하는 정책에 대한 연구는 소홀히 진행되어 왔다. 또한 전자우편을 이용한 악성코드 유포 공격은 시스템에 대한 직접적인 공격보다 훨씬 성공률이 높고 해킹한 PC를 경유하여 내부망으로의 추가적인 해킹까지 가능한 실정이다. 이에 본 논문은 악성코드가 첨부된 전자우편의 대응방안을 제안하여 정보유출을 조기에 차단하는 등 피해를 최소화하여 사고를 예방하고자 한다.

Ⅱ. 전자우편을 이용한 악성코드 유포방법 분석

정보절취를 목적으로 한 해킹메일은 공격대상자(Victim)가 해킹메일의 첨부파일 열람 時, 해킹프로그램이 은밀하게 설치되고 PC 중요자료가 공격자(Attack)에게 유출되는 특징을 가지고 있다. 특히, 해킹메일은 사회공학적 기법을 이용하고 있어 공격대상 PC는 쉽게 감염될 수 있다. 본 장에서는 정보절취형 해킹메일 분석을 통해 정보유출 과정을 설명하고자 한다.



[그림 1] 전자우편을 이용한 악성코드 유표 개요

전자우편을 이용한 악성코드 감염공격은 [그림 1]과 같은 전형적인 특징을 가지고 있고 공격유형을 자세히 분석해 보면 다음과 같다.

① 정보수집: 해커(전자우편 발신자)는 공격 대상자를 선정하기 위해 각 기관의 중요업무 담당자정보를 기관 홈페이지와 검색엔진 등을 통해 입수한다.

② 메일 발송 및 정보유출을 위한 중간 경유지 확보: 해커는 추적을 피하기 위해 해외 중간 경유지를 악용하거나 자신들의 컴퓨터주소를 세탁한 후 악성코드 은닉 및 정보유출 경유지로 활용한다.

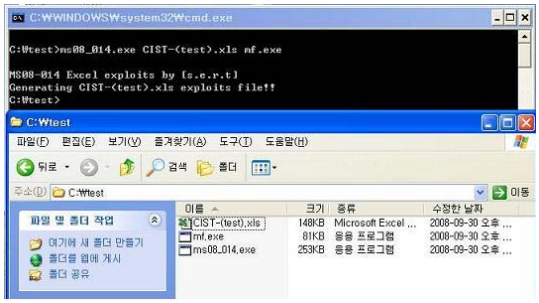
③ 악성코드를 포함한 전자우편 작성 및 발송: 해커는 전자우편 발송용 주소를 확보하기 위해서 무료메일에 타인의 명의를 도용하여 가입하거나 휴면계정을 입수한 후, 공격대상자가 의심없이 첨부파일을 열람토록 제목·본문을 작성하고 경우에 따라 발신자 명의를 공격대상자의 지인으로 위장하여 메일을 작성한다.

④ 해킹프로그램 감염 및 정보유출: 공격 대상자가 전자우편을 수신한 후 첨부파일을 열람하면 은닉된 해킹프로그램이 대상자 PC에 자동으로 설치, 해커가 사전에 확보해 놓은 중간경유지로 PC의 저장자료와 키보드 입력내용 등이 유출되고 해커의 역접속을 허용하는 백도어가 동작하게 된다[1].

이러한 첨부파일형 악성 전자우편의 경우 한글·MS 오피스문서(취약점 이용)로 작성되어 있고 실행하면 실제 문서 내용이 존재하므로 해킹프로그램의 포함여부를 판단하기 어렵기 때문에 자신이 감염된 사실조차 인지하기 어렵다.

2.1 해킹메일에 첨부되는 악성코드 제작방법

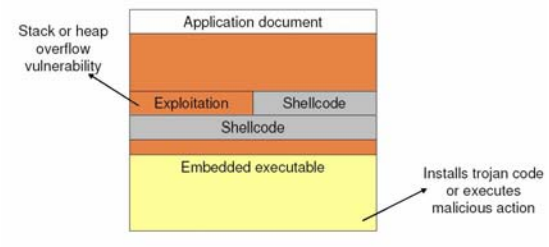
정상적인 문서에 악성코드를 삽입하는 방법(공격코드)은 인터넷상에서 쉽게 구할 수 있다. 중국에서는 이를 도구(Tool)로 만들어 배포하고 있는데, 이를 악용 時 정상적인 엑셀문서에 악성코드를 쉽게 포함시킬 수 있다. [그림 2]는 중국에서 만든 악성코드 인젝터 도구



[그림 2] 실제 악성코드를 삽입

(ms08_014.exe)를 활용하여 정상적인 엑셀문서(CIST-(test).xls)에 악성프로그램(mf.exe)을 삽입한 경우이다. [엑셀 취약점(MS08-014)을 이용]

위와 같이 공격도구(ms08-014.exe)를 이용하여 정상적인 문서에 악성코드를 삽입할 경우 다음과 같은 파일 구조를 갖는다.

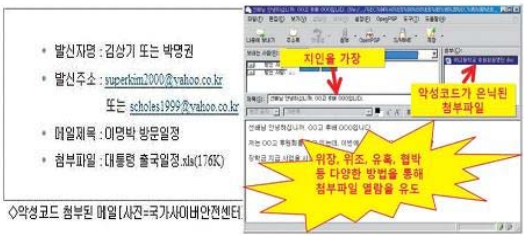


[그림 3] 악성코드가 삽입(Injection)된 파일 구조

2.2 피해사례 및 탐지기술 관련 연구

2.2.1 전자우편을 이용한 악성코드 피해사례

2008년 3월 일부 국가 및 공공기관에서 대통령 순방일정을 소개한다는 내용으로 위장된 해킹메일을 수신한 사례가 다수 발견 되었다.



[그림 4] 국가사이버안전센터 해킹메일 내용

[그림 4]와 같이 해킹메일은 수신자의 관심을 끌만한 사항을 메일제목으로 사용하였으며, 첨부파일도 MS Office(Word, Excel 등) 또는 HWP, PDF 등과 같이 다양한 포맷의 문서파일을 사용하였다. 첨부문서를 열람하는 순간 악성코드에 감염되어 PC 내부 자료를 xxx.3322.org, xxx.youngkoala.com, xxx.ods.org 등의 중간경유지로 전송함으로써 내부자료를 절취하였다[1].

2.2.2 기존 탐지기술 한계성

현재까지 침입탐지시스템에서 해킹메일을 탐지하기 위해 가장 많이 사용하는 방식은 콘텐츠 필터링(Contents Filtering)이다. 이 방식은 2006년 급속하게 확산되는 매스 메일러 웜(Mass Mailer Worm)이 발견되었을 때, 매스 메일러 웜(Mass Mailer Worm)이 전송하는 전자메일 형태, 즉 메일 제목(Subject), 본문(Body) 그리고 첨부파일(Attachment File) 명칭과 같이 특징적인 문구로 탐지하는 것이다[2]. 이 방식은 시그니처 기반(Signature Base)의 진단법과 유사한 개념으로 악성코드가 자신의 복사본을 전송할 때 고정된 형태의 전자메일 형태로 전송하기 때문에 탐지가 가능하다. 그러나 이 방식으로 최근 발생하고 있는 해킹메일을 탐지하기에는 역부족이다. 최근의 해킹메일은 자료절취를 목적으로 사회공학적 기법을 이용하기 때문에 메일 제목(Subject), 본문(Body) 그리고 첨부파일(Attachment File) 명칭이 매번 변경되기 때문이다. 아래 표는 2008년 상반기 유포된 해킹메일이다.

[표 1] E-메일 해킹관련 조치사항, 서해지방경찰청[3]

구분	특징	최근사례
발신자	- 출처 불분명 (간혹 지인으로 가장)	- 박명권, 김상기, 오용석, 김미희
발송ID	- 주로 상용메일 ID 사용 - 타인 ID 도용	~@yahoo.co.kr ~@hanmail.net
제목 내용	- 최근 이슈 및 현안관련 내용 - 공직자 대상 관심유발 내용 - 국내에서 사용치 않는 용어 - 핵포발, 스키즐, 즐그운 등 오탈자가 많이 포함된 내용 (외국인 작성원인)	- 이명박 대통령 순방일정 - 대통령 비서실입니다 - 인민군 무력현황 - 공직자 비리현황 - BBK 의혹, 삼성특검 - 키즈졸브 연습일정
해킹 첨부 파일	- ppt, xls, hwp 첨부파일 - 이력서사진 등 이미지 파일 - 제목과 내용이 상이한 파일	- ppt, xls, doc, jpg 등

최근 이슈화되고 있는 해킹메일은 2008년 3월에 발표된 취약점을 악용한 사례로 기존 탐지 기술로는 탐지가 불가능하고 관련연구는 현재까지 미흡한 실정이다.

Ⅲ. 정보유출時 트래픽 암호화기법 및 복호화 모델

3.1 정보유출時 트래픽 암호화기법

해커는 감염PC에서 내부자료를 절취하여 중간경유지로 전송할 때 보안시스템의 탐지를 우회(False Negative)하기 위해 트래픽을 암호화(XOR, base64 등)한다.

감염PC에서 해킹 중간경유지로 유출되는 트래픽은 암호화 되어있어 이를 탐지하기는 매우 어려운 일이다. 따라서, 정보보안 담당자는 다음과 같은 트래픽에 대해서는 주의 깊게 모니터링을 수행해야 된다.

기관內 정보유출이 의심되거나 점검이 필요할 경우 아래와 같이 집중적으로 트래픽을 분석해야 한다.

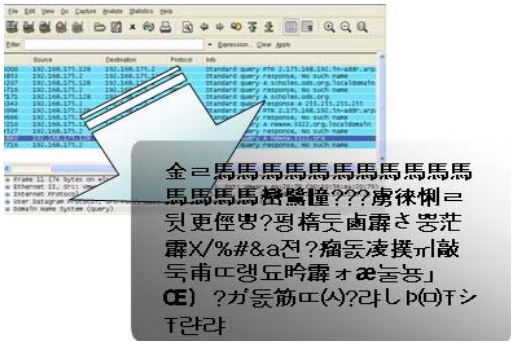
① 감염PC에서 해킹경유지 등으로 특정 포트(tcp 53, 80, 8080 등)를 이용하여 비정상적인 트래픽이 전송되는 경우 -> (감염신호 및 정보유출)

② 감염PC에서 국내·외 특정 시스템으로 일정한 시간을 가지고 주기적으로 지속 비정상적인 트래픽이 전송되는 경우 -> (감염신호)

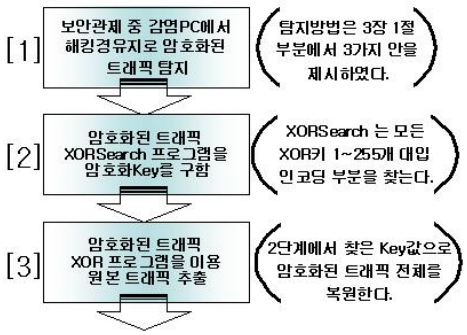
③ 감염PC에서 국내·외 특정 시스템으로 대용량의 트래픽이 전송되는 경우 -> (정보유출)

3.2 복호화 모델

본 장에서는 가장 대표적인 트래픽 암호화 방법인 XOR기법을 이용한 사례를 분석하고 이를 다시 복호화(Decoding)하는 방안을 모색하여 누구나 쉽게 복호화할 수 있는 도구를 개발하였다. 아래 [그림 5]은 실제 해커가 특정 Key값으로 트래픽을 암호화(Encoding)하여 해킹 중간경유지로 전송하는 과정을 보여 주고 있다.



[그림 5] 실제 특정Key값으로 Encoding된 트래픽

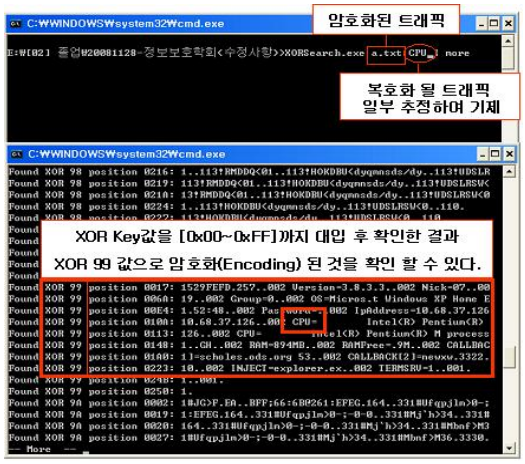


[그림 6] XOR기법 복호화 프로그램 구성

본 장에서는 암호화되어 전송된 트래픽을 분석하기 위해 [그림 9]와 같이 XOR기법으로 복호화하는 프로그램을 개발하였다. 개발환경으로는 MS社 Visual Studio 6.0, MFC프로그램을 사용하였으며 Windows 2000이상 버전의 모든 PC에서 사용가능하다. 同 프로그램은 간단한 입력값(암호화된 트래픽)에 대해서 특정 Key값으로 XOR하여 출력값(복호화된 트래픽)을 나타내 준다.

XOR 기법을 이용하여 암호화(Encoding)하는 방법은 해킹메일에 감염된 후 정보절취時 침입탐지시스템의 탐지를 우회하기 위해 사용되고 있다. 암호화된 트래픽을 어떻게 복원하는지 간략하게 요약하면 [그림 6]과 같다.

1단계 보안관제 활동 중 암호화된 트래픽[3장1절 3가지안 참고]을 탐지한다.



[그림 7] XORSearch 프로그램을 이용 Key검출

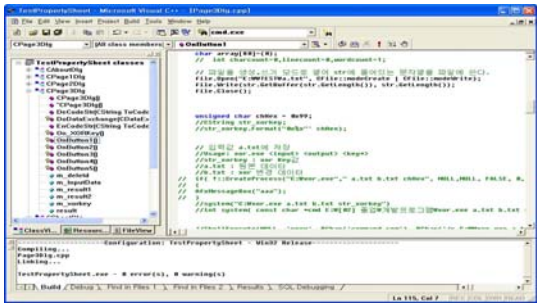
2단계 암호화된 트래픽에서 암호화Key값을 찾기 위해 1~255(0x00~0xFF)를 대입하여 Key 값을 찾는다[5]. [그림 7] 참고

3단계 2단계에서 XORSearch 프로그램을 이용하여 XOR Key값이 0x99인 것을 확인하였다. 아래 소스코스를 이용하여 암호화된 트래픽을 복호화 할 수 있다.

```
// expre_Bitwise_Exclusive_OR_Operator.cpp
// compile with: /EHsc
// Demonstrate bitwise exclusive OR
#include <iostream>
using namespace std;
int main() {
    unsigned short a = 0x5555;      // pattern 0101 ... (암호화된 트래픽)
    unsigned short b = 0xFFFF;      // pattern 1111 ...(Key 값)

    cout  << hex << ( a ^ b ) << endl;    // prints "aaaa" pattern 1010
}
```

위 소스(C++)는 MS사 MSDN XOR 코딩의 일부분이다. [그림 8]은 위 소스를 VC++ 코드로 이용하여 개발한 화면이다[Bitwise Exclusive OR Operator: ^][4].



[그림 8] XOR기법 복호화 프로그램 소스(MFC)

실제 보안관제(네트워크 단) 중 암호화(Encoding)된 트래픽을 대상으로 본 연구과정에서 개발한 프로그램을 이용하여 분석한 결과 [그림 9]과 같은 내용으로 복호화됨을 알 수 있다. 좌측이 실제 암호화된 트래픽으로 [그림 7]과정을 통해 특정 XOR Key 값을 찾은 후 복호화 할 경우 원본 트래픽이 우측이 출력 값으로 나오는 것을 볼 수 있다.

3.3 분석모델의 평가 및 분석

최근 해킹공격은 점차 고도화, 지능화되어 가고 있어

[그림 9] 실제 특정Key값으로 Decoding된 트래픽

이를 탐지하기가 점차 어려워지고 있는 실정이다.

악의적인 사용자 입장에서 보면 해킹을 위한 공격도구는 다양하다. 예를 들면, SQL-인젝션 공격도구 및 취약점 점검도구 등 다양한 종류의 자동화 도구가 존재하여 누구나 쉽게 사이버공격을 시도하고 있다. 그러나 이러한 사이버침해를 탐지하기 위한 보안관제와 관련된 도구는 쉽게 찾아 볼 수 없다.

최근 해킹기법인 이명박 제하 해킹메일은 정상적인 파일로 위장하여 메일에 첨부된 악성코드를 실행할 경우, 내부 전산망에 있는 자료가 암호화(Encoding)되어 유출되는 패턴을 보이고 있어 정상적인 트래픽인지 비정상적인 트래픽인지 구분하기 어렵다.

트래픽을 암호화하는 해킹수법은 최근에 발생한 기법으로 암호화된 트래픽을 분석하는 도구가 마련되지 않아 필요성이 요구되고 있었다. 보안관제 활동 중 암호화된 트래픽으로 추정될 경우, 제안한 분석도구를 이용 복호화를 하면 암호화여부를 확인 할 수 있고 복호화를 통해 암호화된 트래픽 전체를 복원 해커의 공격명령 및 자료유출 등을 분석할 수 있다. 즉 보안관제 업무 수행과정에서 악성코드에 의해 비정상적으로 조작된 트래픽을 효율적으로 분석할 수 있다. 분석도구는 모든 트래픽에 대해 복호화가 가능한 것이 아니고 다음과 같은 경우 트래픽 복호화가 가능하다.

[표 2] 트래픽 복호화 결과

구 분		복호화 여부
XOR 방식으로 암호화 된 경우	XOR 암호화 Key를 찾은 경우	복호가능
	XOR 암호화 Key를 찾지 못한 경우	복호불가
Base64 등 다른 방식으로 인코딩 된 경우		복호불가

Ⅳ. 악성코드가 삽입된 전자우편 대응정책

4.1 해킹메일 대응 보안정책 (악성코드에 감염 전)

현재까지 전자우편에 악성코드를 삽입하여 사회공학적 기법을 이용한 해킹 공격에 대해서는 뚜렷한 대응방법을 찾기가 어렵다. 일반적인 해결책으로는 상용백신(Anti Virus)제품을 주기적으로 갱신하거나, 바이러스월(Virus Wall)과 같은 보안장비의 전자우편 필터링 기술을 이용하여 내부 망으로 유입되는 악성코드가 삽입된 전자우편을 1차적으로 차단하는 것이 필요하다. 이러한 1차적인 방법은 일반적으로 인터넷상에서 잘 알려진 악성코드에 대해서만 탐지 및 차단이 가능하고 패턴이 알려지지 않은 새로운 바이러스에 대해서는 대처할 수 없는 단점을 가지고 있어 대응기술 및 정책이 절실한 실정이다.

해당 기관의 정보보안 담당자는 모든 직원들에게 해킹메일의 위험성을 전파하고 직원들로 하여금 의심가는 메일 수신시 정보보안 담당자에게 신고하도록 교육해야 한다. 이는 대부분의 해킹메일이 백신에서 탐지되지 않는 최신의 해킹기법으로 작성되었기 때문에 신속한 분석 및 정보공유를 통해 다른 기관의 추가적인 피해를 예방할 수 있기 때문이다. 이때 해킹메일은 실제 첨부파일과 메일헤더 분석이 추가적인 해킹 피해를 방지하기 위해 필수적이므로 전달기능이 아닌 원문저장 기능을 활용하여 전자우편 내용을 채증한 후 분석해야 한다. 정보보안 담당자가 수행해야 할 점검사항은 다음과 같다.

① 한글·MS오피스를 포함하여 최신 윈도우 보안패치를 주기적으로 적용하고
② 스팸메일 차단시스템 등을 활용, 해킹메일우편을 차단한다.
③ 침입차단시스템이나 스팸메일 차단시스템에서 발송자를 도용한 전자우편에 대해 차단기능을 적용
④ 업무망과 인터넷망을 분리하거나 문서파일이 유출되어도 열람이 불가능하도록 암호화하는 등 보안조치를 강구함과 동시에
⑤ 국가 중요업무 담당직원의 전자우편 주소는 홈페이지에 공개하는 것을 금지하고
⑥ 사고발생시 발신자 추적 등 조사가 용이하도록 침입차단시스템·전자우편서버 등의 각종 로그는 최소 3개월 이상 보존해야 한다.

정보절취형 해킹메일인 경우 일반 PC 사용자들은 정상메일과 구분하기 어려운 특징을 가지고 있다. 그러나 일반 사용자들이 몇 가지 주의사항을 지킨다면 전자우편 사고를 조기에 인지하고 피해 확산을 방지할 수 있다.

① 해킹목적의 전자우편 특징을 참조하여 의심스러운 전자우편을 수신한 경우에는 첨부파일을 열람하지 말고 발송자에게 발송여부 확인 및 정보보안담당자에게 신고한다.
② PC의 윈도우 보안패치(한글·오피스포함) 및 백신 업데이트를 항상 최신으로 유지하고
③ 상용 전자우편을 통한 업무자료 소통을 금지하는 등 업무용과 개인메일을 구분하여 사용한다.
④ 악성코드 유포에 악용되지 않도록 전자우편 주소를 인터넷에 공개하거나 대외적으로 배포하는 것을 제한하고 패스워드를 주기적으로 변경한다.
⑤ 또한 인터넷과 연결된 업무용PC에 업무상 중요비밀 및 문서 보관을 금지한다.

4.2 탐지기술 제작 방법론 (악성코드에 감염 후)

해킹메일에 첨부된 악성코드에 감염된 후 대응정책으로 가장 중요한 것은 해커의 중간경유지(악성도메인)를 확보하는 것이다 이는 감염PC를 찾기 위해 탐지규칙을 제작하는데 꼭 필요하기 때문이다.

4.2.1 중간경유지(악성도메인) 확보방법

해킹메일에 감염된 PC를 탐지하기 위한 효과적인 방법으로 감염신호 수신, 자료절취, 악성코드 은닉 등의 중간경유지를 찾아 모니터링하는 방법이다. 악성코드의 중간경유지를 확보하는 방법은 악성코드의 네트워크 접속 점검 부분을 통해 얻을 수 있다. 즉 중간경유지를 확보방법은 다음과 같다.

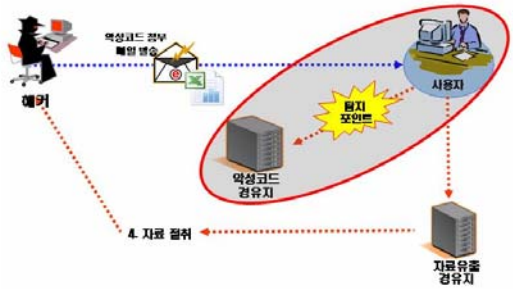
① 적절한 악성코드 테스트 환경을 구성
② 테스트PC에 악성코드를 감염시킨 후 네트워크 단에서 접속 트래픽을 모니터링한다.
③ ②과정에서 탐지된 트래픽이 중간경유지가 맞는지를 확인한다.

확보된 중간경유지(악성도메인)은 IP와 같이 지속 변경유무 등의 관리가 필요하다.

4.2.2 탐지기술 제작 방법론

감염된 PC를 탐지하기 위해서는 사이버공격 패킷 내용을 이해하고 이를 전산망 환경에 맞는 최적의 규칙을 생성하는 것이 무엇보다 중요하다. 인터넷에 알려진 악성코드는 백신(Anti Virus)과 바이러스 월(Virus Wall)과 같은 보안장비를 사용하여 1차적으로 차단하고, 알려지지 않은 해킹메일에 감염된 경우 네트워크 단에서 두 가지 중간경유지를 모니터링하는 방법론을 제안한다.

첫째, 감염된 PC는 해킹프로그램 원본 또는 추가 공격용 악성코드를 다운로드하기 위해 악성코드가 저장된 경유지에 접속하는데 [그림 10]와 같이 악성코드 다운로드 과정을 집중적으로 모니터링 한다.



[그림 10] 악성코드 다운로드 時 탐지

스노트(Snort) 탐지시스템을 이용하여 탐지규칙을 제작할 경우 content, pcre 옵션 등을 이용하면 정확도를 높일 수 있다[6].

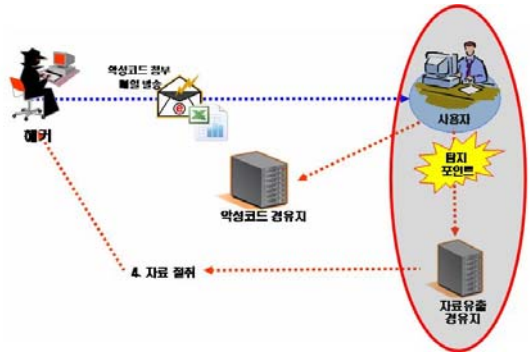
> 패턴기반 : alert tcp any any -> any 80 (content:"GET /"; depth:5; content:"HTTP/1.0|0d 0a|"; depth500; content:"악성코드 경유지 주소 도메인";)

위와 같이 제작하고 실제 테스트 한 결과 감염PC IP에 DNS서버 IP가 탐지되어 정확한 감염PC를 찾기 어렵다. 이를 보완하기 위해서는 반드시 IP기반의 탐지규칙을 동반하여야 정확한 감염PC를 찾을 수 있다.

> IP기반: alert tcp any any -> 악성코드 경유지IP any

실제 탐지규칙을 테스트한 결과, 위와 같이 악성코드 경유지 도메인과 경유지IP를 동시에 모니터링을 해야 정확한 감염자 PC를 찾을 수 있다는 결론이 도출되었다.

둘째, 감염PC 내에서 내부자료가 절취될 때 중간경유지를 사용하는데 아래 [그림 11]은 이를 모니터링 하는 방법이다.



[그림 11] PC내 내부자료 유출時 탐지

감염PC에서 정보유출 경유지로 자료가 유출될 때 앞에서 수행했던 방식과 동일하게 패턴기반 탐지규칙과 IP기반 탐지규칙을 적용하면 감염PC에서 정보유출 경유지로 접속하는 트래픽을 찾을 수 있다.

[표 3]과 같이 실제 패턴기반 탐지규칙과 IP기반 탐지규칙을 적용하여 실제 탐지 여부를 점검한 결과, [해킹메일 내 악성코드의 탐지률을 점검]

① 기존 악성코드(변종이 아닌 악성코드)는 패턴기반, IP기반 탐치규칙에서 100% 탐지가 가능하였고

② 변종 악성코드의 경우 패턴기반에서는 탐지를 못하고 IP기반 탐지규칙에서는 해킹경유지가 같을 경우 탐지가 가능하였다.

중간경유지를 찾은 후 전 세계적으로 가장 폭넓게 쓰이고 있는 침입탐지시스템 Snort를 기반으로 탐지규칙을 제작, 시뮬레이션 한 결과이다.

결론적으로, 2008년 상반기 발생한 이명박 방문일정

[표 3] 실제 Snort 탐지규칙을 제작하여 테스트한 결과

구분		기존악성코드	변종악성코드
악성 경유지 패턴	패턴기반	탐지가능	탐지못함
	IP기반	탐지가능	탐지가능 or 탐지못함 (패턴기반 탐지규칙 개발가능)
특정패턴		탐지가능	탐지가능 or 탐지못함

해킹 메일 관련 해킹 경유지(xxx.3322.org, xxx.youngkoala.com, xxx.ods.org)를 IP기반으로 관제할 경우 해커의 공격패턴 등 많은 정보를 모니터링 할 수 있다. 또한 경유지 변경시 IP기반 탐지룰을 같이 변경하여 관제를 해야함은 물론 해커가 사용하고 있는 중간경유지 관리가 필요하다.

악성코드 감염 후 대응정책을 간략히 요약하면 해킹메일에 대해 바이러스 월(Virus Wall) 등 보안장비에서 차단되지 못하고 악성코드에 감염되었을 경우, 감염PC를 찾아 다음과 같은 작업을 수행한다.

① 전자우편에 포함된 악성코드를 채증한다.
② 同 악성코드 감염 시 감염증상을 모니터링 한다.
③ 중간경유지를 추출하여 목록화 한다.
④ 탐지기술을 적용, 네트워크 단에서 모니터링 한다.

기존까지 사용된 중간경유지로 사용되는 악성도메인을 목록화(DB화)하고 채증하여 분석된 경유지에 접속하는 PC를 모니터링하면 감염PC를 쉽게 찾아낼 수 있다.

Ⅴ. 결 론

해킹메일을 이용한 공격은 빠른 속도로 지능화되어 발전하고 있으며 그 탐지에 있어서도 보안관리자의 탐지를 우회하고 있어 부지불식간에 확산되고 있는 실정이다. 탐지방안으로 우선, 알려진 해킹메일에 대해서는 바이러스 월 등과 같은 보안장비에서 차단하는 등 악성코드 감염에 대해 1차적인 대응과정(차단 또는 필터링 등)이 필요하고 이어서 알려지지 않은 악성코드의 탐지방안에 대해서는 현재까지 뚜렷한 대응방안이 없기 때문에 해킹메일을 조기에 채증하여 감염 후 발생하는 패킷의 특징을 분석, 보안관제에 적용하여 정보유출과 같은 피해를 최소화 할 수 있다. 본 논문에서는 알려지지 않은 악성코드 탐지방안으로 감염 후 특징을 모니터링 할 수 있는 방법론을 제안하였고, 해커가 탐지를 회피하기 위해 사용한 암호화한 트래픽을 복호화(Decoding) 할 수 있는 도구를 제안하였다. 신종 해킹메일은 탐지하기가 매우 어렵고 갈수록 지능적인 사회공학적 기법을 이용하고 있어 악성코드에 감염되는 수가 지속적으로 증가하고 있다. 또한 대부분의 피해자는 악성코드 감염 사실조차 모르고 있어 다량의 중요자료가 유출이 심각하게 우려되는 상황이다. 그러므로 정보보안 담당자와 PC사용자의 대응정책을 시행함으로써 전자우편에 의한 악성코드 감염을 사전에 예방하고 피해를 최소화해야 한다.

향후 개발된 프로그램을 지속적으로 업그레이드하여 Base64, URL Encoding 등 다양한 트래픽에 대한 복호화 기능을 추가할 예정이며 지능화・고도화・자동화되어가고 있는 공격도구에 대한 탐지분석도구가 지속적으로 연구되어야 할 것이다.

참고문헌

[1] 국가사이버안전센터, “Monthly Cyber Security,” pp. 28-38. 2008년 4월.
[2] Ahnlab, “알려지지 않은 악성코드 탐지 기법,” http://kr.ahnlab.com/securityinfo/infoView.ahn?seq=9532&category=01.
[3] 서해지방경찰청, “E-메일 해킹관련 조치사항,” http://wh.kcg.go.kr.
[4] Microsoft Corporation, “Bitwise Exclusive OR Operator,” http://msdn. microsoft.com/fr-fr/library/3akey979.aspx.
[5] Didier Stevens, XORSearch Tool, http://blog.didierstevens.com/programs/xorsearch/.
[6] J. Beale, Snort 2.0 Intrusion Detection, 2th Ed., Syngress Media Inc., May 2004.

<著 者 紹 介>

양 경 철 (Kyeong Cheol Yang) 학생회원
2002년 2월: 가톨릭대학교 컴퓨터 전자공학부 학사
2009년 2월: 고려대학교 정보경영공학전문대학원 석사
<관심분야> 보안관제, 사이버위협 침입탐지, 정보유출

이 수 연 (Su yeon Lee) 학생회원
2001년 2월: 동덕여자대학교 문헌정보학과 석사
2009년 2월: 고려대학교 정보경영공학전문대학원 박사 수료
<관심분야> 정보보호정책, 네트워크 포렌식

박 원 형 (Won Hyung Park) 종신회원
2002년 2월: 서울산업대학교 산업정보시스템공학과 학사
2005년 2월: 서울산업대학교 정보산업공학과 석사
2009년 2월: 경기대학교 정보보호학과 박사
경기산업보안기술특화센터 연구원
한국사이버테러정보전학회 논문 편집위원
<관심분야> 정보유출, 악성코드, 네트워크 포렌식

박 광 철 (Kwang Cheol Park) 학생회원
2003년 2월: 고려대학교 정보경영공학전문대학원 석사
2009년 2월: 고려대학교 정보경영공학전문대학원 박사 수료
<관심분야> 정보보호정책, 네트워크 포렌식, 보안관제

임 종 인 (Jongin Lim) 종신회원
1986년 2월: 고려대학교 대학원 수학과 박사(암호학)
2000년 8월: 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월: 국가정보원 정보보호정책 자문위원
2005년 7월: 대통령 자문 전자정부 특별위원
2005년 12월: 국회 과기정위원회 정보통신 정책 자문위원
<관심분야> 정보보호기술, 정보보호정책, PET, 컴퓨터 포렌식