2017년 4분기 정보보안 소식

2018.04.29

차민석 (車珉錫, CHA Minseok, Jacky Cha, mstoned7)

알림

- 본 발표 자료는 개인 의견으로
소속 회사의 공식 입장과 다를 수 있습니다.

- 덕질 자료가 포함되어 있을 수 있습니다.

시작하기 전에

- 보안이 완벽한 시스템은 이 세상에 없어
  - Matthew Broderick 주연 위험한 게임 (War Games)

* Source : War Games (1983)

Contents

01 2017년 동향

02 2017년 국내 보안 소식

03 2017년 4 분기 국내 사건 사고

04 2017년 국외 보안 소식

05 2017년 4 분기 국외 사건 사고

06 2017년 4 분기 취약점과 악성코드

07 Case Study : 여행사 해킹

01
2017년 동향

TheShadowBrokers 해킹 자료 공개

- TheShadowBrokers, NSA 해킹 자료 공개 주장
  - 2017년 4월 7일 공개

Lost in Translation

theshadowbrokers ▾ 56 in shadowbrokers 9 days ago

KEK...last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking fuck peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadowbrokers wanting you to be seeing. Sometime peoples not being target audience. Follow the links for new dumps. Windows. Swift. Oddjob. Oh you thought that was it? Some of you peoples is needing reading comprehension.

https://yadi.sk/d/NJqzpqo_3GxZA4
Password = Reeeeeeeeeeeeee

theshadowbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away. TheShadowBrokers rather being getting drunk with McAfee on desert island with hot babes. Maybe if all suviving WWIII theshadowbrokers be seeing you next week. Who knows what we having next time?

* Source : https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation

Wannacryptor & Petya

- Wannacryptor (Wannacry) & Petya 공격
  - 2017년 4월 TheShadowBrokers 가 공개한 취약점으로 제작
  - 2017년 5월 12일 & 6월 27일 확산

Anti-Malware , Cybersecurity , Risk Management

sponsored by SKYBOX SECURITY

WannaCry Ransomware Outbreak Spreads Worldwide

Spain's Telefonica, England's NHS Are Among the Victims

Mathew J. Schwartz (@euroinfosec) • May 12, 2017 • 1 Comment

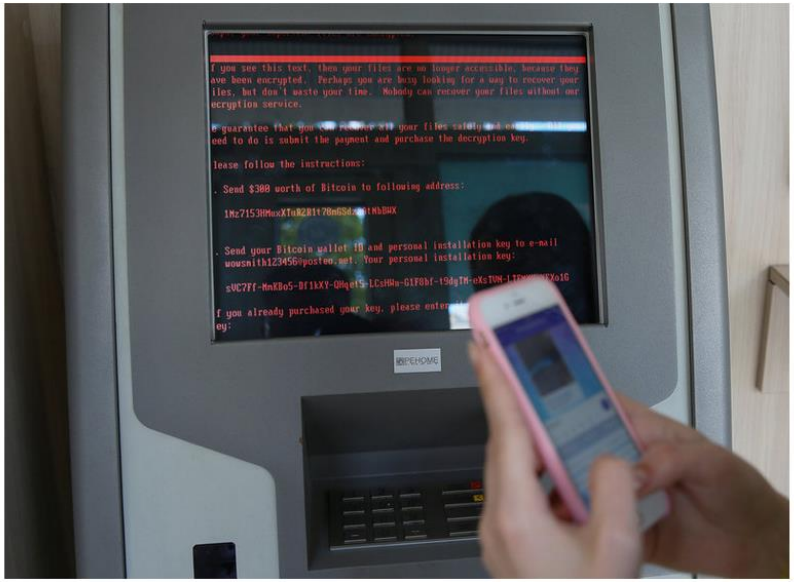
Twitter Facebook LinkedIn Credit Eligible Get Permission

The lockscreen displayed by the WannaCry crypto-locking ransomware used in the attacks. (Source: Lawrence Dunhill)

Massive Ransomware Attack Hits Ukraine; Experts Say It's Spreading Globally

June 27, 2017 · 11:59 AM ET

BILL CHAPPELL COLIN DWYER



A message demanding money is seen on a terminal monitor at a branch of Ukraine's state-owned Oschadbank after Ukrainian institutions were hit by a wave of cyberattacks earlier Tuesday in Kiev, Ukraine.

Valentyn Ogirenko/Reuters

* Source : http://www.govinfosecurity.com/wannacry-ransomware-outbreak-spreads-worldwide-a-9912

웹호스팅 업체 Ransomware 공격

- 웹호스팅 업체 Ransomware 공격
  - 2017년 6월 10일 새벽 웹호스팅 업체 내 파일 Ransomware 로 암호화 됨

* Source : http://www.nayana.com/

02
2017 년 국내 보안 소식

2017 년 국내 정보보안 소식

- 1월 2일 : 이스트시큐리티 설립

http://www.estsecurity.com/

- 1월 2일 : 한글 메일로 작성된 VenusLocker Ransomware 배포

http://www.etnews.com/20170102000507

- 1월 2일 : 북한 신년사 가장한 악성코드 확인

https://www.dailynk.com/korean/read.php?num=110033&cataId=nk00100

- 1월 3일 : 한글 메시지 포함한 매크로 Downloader 발견

http://blog.alyac.co.kr/917

- 1월 5일 : 원격조종 프로그램을 통해 빼낸 신용카드 정보로 2년 만에 12억 원을 챙긴 일당 검거

http://news.donga.com/3/all/20170105/82186046/1

- 1월 16일 : 특검에 대한 공격 포착

https://www.hankookilbo.com/v/b6b123f7d9014321821cc3f06119fa06

- 1월 19일 : 핸디소프트 인증서 도용 악성코드 발견

http://www.etnews.com/20170119000346

2017 년 국내 정보보안 소식

- 1월 23일 : 한국항공우주학회 홈페이지를 통한 워터링홀 공격 조사 중

http://news.jtbc.joins.com/article/article.aspx?news_id=NB11407111

- 1월 25일 : 경찰, 학술연구단체 사칭한 사이버공격은 북한 소행 발표

http://www.hani.co.kr/arti/society/society_general/780166.html

- 1월 26일 : 북한 해커 탈북 시도했으나 실패 보도

http://www.mediatoday.co.kr/?mod=news&act=articleView&idxno=134791

- 1월 26일 : Saint Security, MAX 베타 테스트 시작
- 2월 1일 : USB킬러 이용해 경쟁PC방 컴퓨터 고장 일으킨 30대 검거

http://news1.kr/articles/?2899904

- 2월 20일 : 아시아나항공 홈페이지 해킹

http://www.hani.co.kr/arti/economy/economy_general/783307.html

- 2월 23일 : KT, 사이버보안센터 개관

http://news.inews24.com/php/news_view.php?g_serial=1008138&g_menu=020300

-

2017 년 국내 정보보안 소식

- 3월 1일 : 롯데 중국 사이트 공격으로 다운

http://www.yonhapnews.co.kr/bulletin/2017/03/01/0200000000AKR20170301073000030.HTML?input=1195m

- 3월 8일 : 금융사 망분리 취약점 이용한 악성코드 발견

http://www.etnews.com/20170308000292

- 3월 14일 : Sophos 국내 진출

http://byline.network/2017/03/1-626/

- 3월 19일 : 국내 ATM 제조 회사에 대한 표적 공격 발생

http://www.etnews.com/20170317000244

- 3월 24일 : 여기어때 해킹으로 고객 정보 유출

http://byline.network/2017/03/1-652

- 4월 4일 : 국방부 작계 5027 해킹으로 유출 보도

http://www.edaily.co.kr/news/NewsRead.edy?newsid=02122166615892840&SCD=JF31&DCD=A00603

2017 년 국내 정보보안 소식

- 4월 5일 : No more Ransom 한국어 지원

https://www.nomoreransom.org/co/index.html

- 4월 13일 : 인터파크 개인정보 유출관련 사과공지 메일' 위장한 랜섬웨어 등장

http://www.boannews.com/media/view.asp?idx=54248

- 4월 20일 : 맥아피, 삼성 스마트TV에 백신 탑재

https://byline.network/2017/04/1-684/

- 4월 26일 : 여기어때 해킹 결과 발표

http://www.boannews.com/media/view.asp?idx=54489

- 4월 27일 : 동료 경찰에 악성코드 심은 경찰 영장

http://www.hani.co.kr/arti/society/area/792589.html

- 4월 28일 : 가상환경 일 때 하드디스크 내용 파괴 후 "Are you Happy?" 출력 악성코드 발견

http://www.boannews.com/media/view.asp?idx=54544&kind=0

- 5월 2일 : 국방망 해킹 수사 결과 발표

http://news.jtbc.joins.com/article/article.aspx?news_id=NB11462936

2017 년 국내 정보보안 소식

- 5월 11일 : 타백신 AhnLab V3 Mobile Plus 2.0 오진

http://www.zdnet.co.kr/news/news_view.asp?artice_id=20170512173003

- 5월 18일 : Cylance 국내 진출

https://byline.network/2017/05/1-725/

- 5월 18일 : 한글 사용 할 때만 동작하는 악성코드 발견

http://www.boannews.com/media/view.asp?idx=54815

- 5월 19일 : 네이버 밴드 도용 발생

http://www.hankookilbo.com/v/7df4a18d74d64156949ca64b1d6a3718

- 5월 29일 : 수원남부경찰서 사칭 VenusLocker 배포

http://www.boannews.com/media/view.asp?idx=54986

- 5월 30일 : CWIC사이버전연구센터, Active-X 취약점으로 감염되는 Operation GoldenAxe 공개

http://www.boannews.com/media/view.asp?idx=55023

http://www.etnews.com/20170530000352?mc=ev_001_00004

2017 년 국내 정보보안 소식

- 6월 1일 : 여기어때 해킹 용의자 검거

http://www.boannews.com/media/view.asp?idx=55057&kind=0

- 6월 10일 : 컴퓨터 수리 업체 Ransomware 배포

http://www.segye.com/newsView/20170609000492

- 6월 10일 : 나야나 Erebus Ransomware 감염으로 서비스 웹사이트 장애 발생

http://www.boannews.com/media/view.asp?idx=55215

- 6월 21일 : Armada Collective, 국내 은행 7곳에 DDoS 공격 협박해 비트코인 요구

http://www.etnews.com/20170621000224

- 6월 28일 : 케이사인, 62억 투자로 세인트시큐리티 최대주주 됨

https://byline.network/2017/06/1-794/

- 6월 28일 : 나야나 사고 조사 결과 발표

http://www.ddaily.co.kr/news/article.html?no=157523

- 6월 30일 : 빗썸 해킹

http://bithumb.cafe/archives/7329

2017 년 국내 정보보안 소식

- 7월 2일 : 빗썸 해킹 보도

http://www.hani.co.kr/arti/economy/it/801322.html

- 7월 4일 : AhnLab, 국내 방위산업체 공격 동향 보고서 발표

http://asec.ahnlab.com/1070

- 7월 7일 : 세인트시큐리티, Virustotal 에 MAX 등록 발표

http://www.ddaily.co.kr/news/article.html?no=157908

- 7월 10일 : Kaspersky, 국방부와 ATM 해킹 동일 조직 가능성 발표

http://news.inews24.com/php/news_view.php?g_menu=020200&g_serial=1034488

- 7월 13일 : 북 '우리민족끼리' 해킹으로 가입 확인 된 13명 검찰 송치

http://news.chosun.com/site/data/html_dir/2017/07/14/2017071400305.html

- 7월 14일 : 북 인권단체 겨냥 악성코드 담긴 이메일 유포

https://www.dailynk.com/korean/read.php?num=111049&cataId=nk00400

- 7월 27일 : 금융보안원, 사이버 인텔리전스 리포트 공개

http://www.fsec.or.kr/user/bbs/fsec/21/13/bbsDataView/910.do

2017 년 국내 정보보안 소식

- 8월 7일 : 넷사랑 설치 파일 악성코드 포함

http://www.netsarang.co.kr/news/security_exploit_in_july_18_2017_build.html

- 8월 14일 : LG 전자 서비스센터 Ransomware 감염

http://www.hani.co.kr/arti/economy/it/806979.html

- 8월 22일 : US 정부, KasperskyLab 제품 사용 금지 추진

https://www.grahamcluley.com/fbi-briefing-us-companies-using-kaspersky-products-claims-report/

- 8월 23일 : 가상화폐 거래소 피싱 공격

http://www.boannews.com/media/view.asp?idx=56539

- 8월 31일 : 정치학 교수에서 문재인 정부의 탈핵선언을 비판한다.hwp 메일로 공격

http://www.boannews.com/media/view.asp?idx=56738

- 9월 6일 : 경찰, ATM 해킹 수사결과 발표

http://www.itworld.co.kr/news/106281

- 9월 6일 : ESTsoft 개인정보 유출(도용) 정황 발표

http://cdn.estsoft.com/estsoft/notice/1

2017 년 국내 정보보안 소식

- 9월 19일 : 경찰, 보안 취약한 1402 대 IP 카메라 영상 유포한 11명 검거 발표

http://www.hani.co.kr/arti/society/area/811590.html

- 9월 26일 : 해군 잠수함 미사일 콜드런치 해킹 당함

http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201709260600045&code=910303

- 9월 27일 : 경찰 비트코인 거래소 해킹 수사 결과 발표

http://cyberbureau.police.go.kr/board/boardView.do?board_id=ect&id=6012&page=1&mid=040503

- 10월 7일 : 코인이즈 해킹으로 21억 손실

http://www.boannews.com/media/view.asp?idx=57354

- 10월 16일 : 검찰 빗썸 정보 유출 수사

http://news.donga.com/Main/3/all/20171016/86762345/1

- 10월 17일 : 공항 출입국 시스템 관리 업체 해킹

http://news.sbs.co.kr/news/endPage.do?news_id=N1004438303

- 10월 17일 : 하나투어 해킹

http://www.yonhapnews.co.kr/bulletin/2017/10/17/0200000000AKR20171017170300030.HTML

2017 년 국내 정보보안 소식

- 10월 17일 : AhnLab, Operation Bitter Biscuit 공개

http://image.ahnlab.com/file_upload/asecissue_files/ASEC_REPORT_vol.88.pdf

- 10월 19일 :

https://www.fireeye.com/blog/threat-research/2017/10/magniber-ransomware-infects-only-the-right-people.html

- 11월 1일 : DDE를 이용한 공격

http://www.boannews.com/media/view.asp?idx=57805

http://www.boannews.com/media/view.asp?idx=57828

- 11월 6일 : KoreaIDC 일부 호스팅서버 Ransomware 피해 발생

http://www.etnews.com/20171106000435

- 11월 14일 : Ransomware 제작 고등학생 사죄글 게시

http://www.dailysecu.com/?mod=news&act=articleView&idxno=25910

- 11월 15일 : 국방부 보안 회사에 50억 소송

http://news.joins.com/article/22123446

2017 년 국내 정보보안 소식

- 11월 20일 : Mobile 용 Lazarus 관련 악성코드 발견

https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-cybercrime-group-moves-to-mobile/

https://researchcenter.paloaltonetworks.com/2017/11/unit42-operation-blockbuster-goes-mobile

- 11월 28일 : 북한 관련 단체에 공격 중인 악성코드

http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html

- 11월 29일 : 교차로 홈페이지 Ransomware 감염

http://www.etnews.com/20171129000409

- 11월 30일 : Ursnif (Gozi)를 포함한 HWP 파일 발견

http://www.boannews.com/media/view.asp?idx=58310&kind=0

- 12월 5일 : VenusLocker 제작자 가상화폐로 채굴로 변경

http://www.dailysecu.com/?mod=news&act=articleView&idxno=26576

- 12월 6일 : 북한에서 제작한 온라인게임 해킹 핵 판매자 실형 선고

http://news.chosun.com/site/data/html_dir/2017/12/06/2017120601915.html

2017 년 국내 정보보안 소식

- 12월 14일 : KRCert 가장한 Cryptocurrency Exchange 공격 발생

https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=26888

- 12월 15일 : 자유 투어 해킹

http://www.jautour.com/customer/notice/view.asp?b_idx=56109&col=&search=&bow=&gotoPage=1

- 12월 16일 : NIS, 북한 Cryptocurrency Exchange 공격 했다고 밝힘

http://news.chosun.com/site/data/html_dir/2017/12/16/2017121600209.html

http://news.chosun.com/site/data/html_dir/2017/12/16/2017121600211.html

- 12월 18일 : 가상화폐 지갑 훔쳐가는 악성코드

https://byline.network/2017/12/1-970/

- 12월 18일 : 채굴기 추가 설치하는 프로그램 발견

http://www.boannews.com/media/view.asp?idx=58674&kind=0

- 12월 19일 : 유빗 파산 선언

http://news.mt.co.kr/mtview.php?no=2017121915562242232

https://byline.network/2017/12/1-972/

2017 년 국내 정보보안 소식

- 12월 25일 : Ransomware 감염 시킨 컴퓨터 수리 업체 적발

http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201712251434001&code=940100

- 12월 29일 : EPR 솔루션을 통해 악성코드 배포

http://www.boannews.com/media/view.asp?idx=65804&kind=0

http://www.ddaily.co.kr/news/article.html?no=164197

03
2017년 3 분기 국내 사건 사고

국방부 해킹

- 2016년 해킹
  -

North Korea hacked South's secret joint US war plans – reports

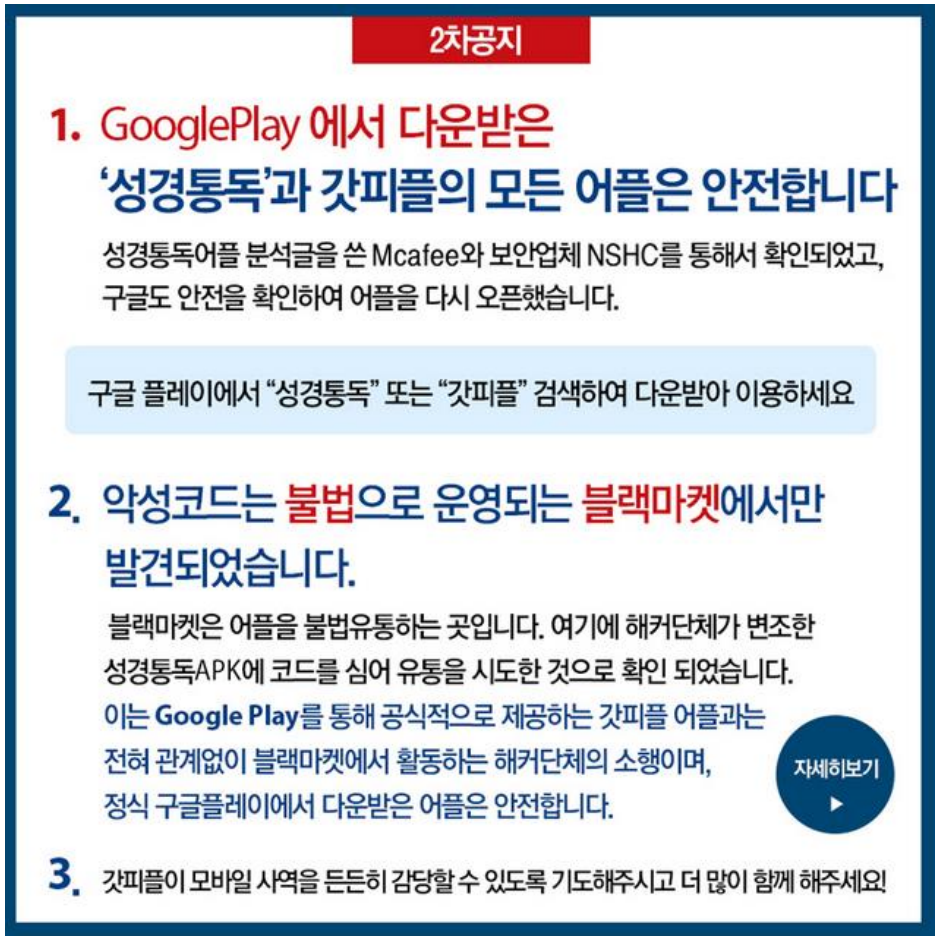
- Ruling party politician says data breach occurred in September 2016
- Leaked documents said to include plans for 'decapitation' attacks on Kim

South Korean marines take part in a US-South Korea joint landing operation drill. Details of joint military drills were believed to be among documents hacked by North Korea. Photograph: Kim Hong-Ji/Reuters

* Source : https://www.theguardian.com/world/2017/oct/10/north-korea-hacked-us-war-plans-south-korea-reports

Lazarus Mobile 악성코드

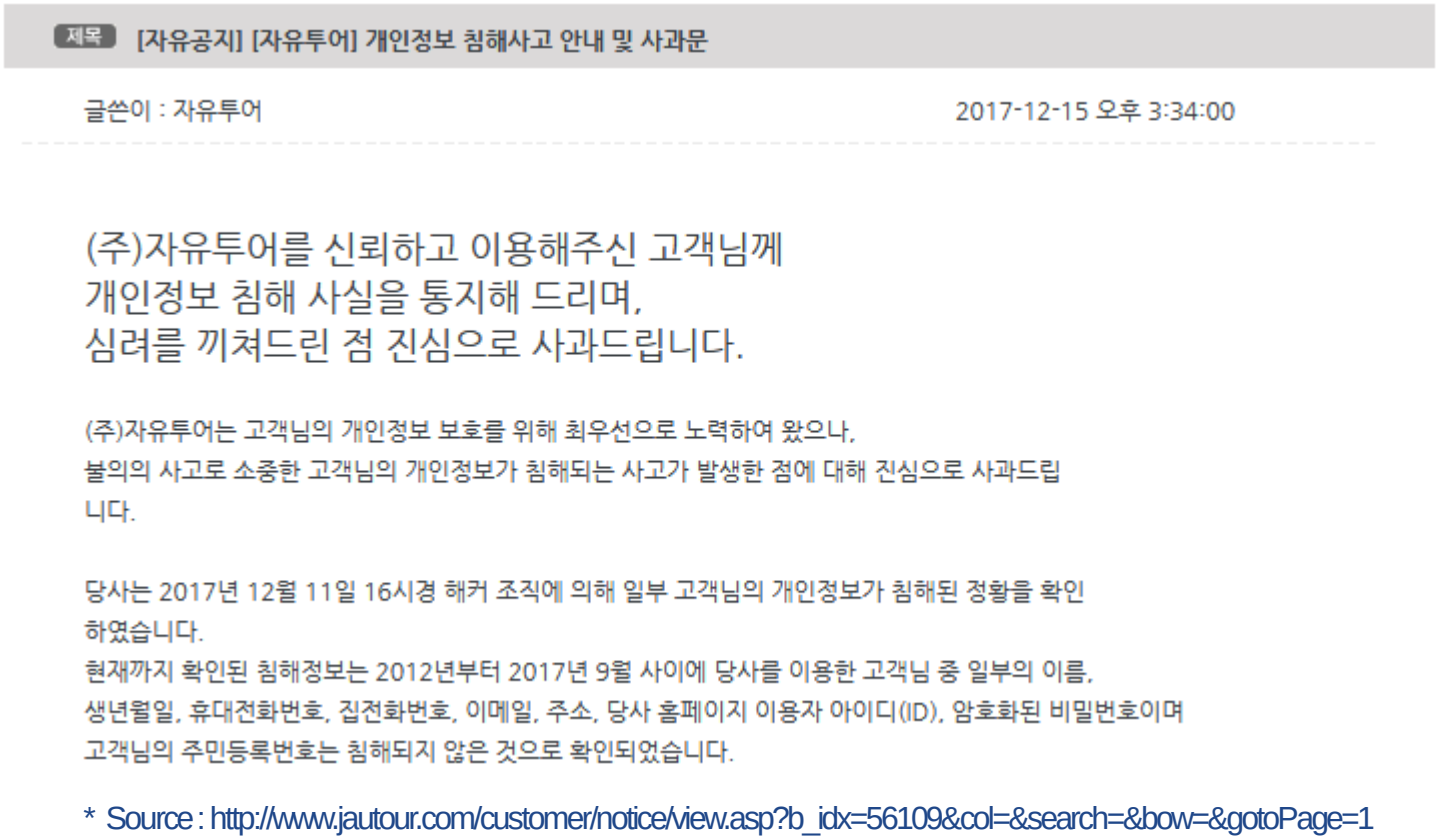
- 성경 관련 앱에서 악성코드 발견
  -



* Source : http://www.godpeople.com/?GO=mobile_detail&appid=93

자유투어 해킹

- 자유투어 해킹
  - 2017년 12월 11일 침해 정확 확인
  - Andariel Group 소행 추정



제목 [자유공지] [자유투어] 개인정보 침해사고 안내 및 사과문

글쓴이 : 자유투어 2017-12-15 오후 3:34:00

(주)자유투어를 신뢰하고 이용해주신 고객님께
개인정보 침해 사실을 통지해 드리며,
심려를 끼쳐드린 점 진심으로 사과드립니다.

(주)자유투어는 고객님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나,
불의의 사고로 소중한 고객님의 개인정보가 침해되는 사고가 발생한 점에 대해 진심으로 사과드립
니다.

당사는 2017년 12월 11일 16시경 해커 조직에 의해 일부 고객님의 개인정보가 침해된 정황을 확인
하였습니다.
현재까지 확인된 침해정보는 2012년부터 2017년 9월 사이에 당사를 이용한 고객님 중 일부의 이름,
생년월일, 휴대전화번호, 집전화번호, 이메일, 주소, 당사 홈페이지 이용자 아이디(ID), 암호화된 비밀번호이며
고객님의 주민등록번호는 침해되지 않은 것으로 확인되었습니다.

* Source : http://www.jautour.com/customer/notice/view.asp?b_idx=56109&col=&search=&bow=&gotoPage=1

유빗 해킹으로 파산 선언

- 유빗 (구 야피존) 해킹으로 파산 절차
  - 12월 19일 코인 출금지갑에서 손실 발생

가상화폐 거래소 '유빗', 해킹으로 파산 절차…국내 첫 사례

BY 이유지 *on* 2017년 12월 19일 · 💬(0)

가상화폐 거래소 '유빗(옛 야피존)'이 해킹으로 파산 절차를 진행한다고 19일 밝혔다. 해킹으로 국내 가상화폐 거래소가 파산하게 된 것은 이번이 처음이다.

유빗은 이날 홈페이지에 올린 긴급 공지에서 "금일 새벽 4시35분경 해킹으로 인해 코인 출금지갑에 손실이 발생했다"라면서 "코인손실액은 전체 자산의 약 17%"라고 밝혔다.

이 공지에서 유빗은 "㈜야피안의 경영진은 당사가 운영하던 코인거래소 유빗을 2017.12.19일 부로 거래 중단, 입출금 정지 조치 및 파산 절차를 진행하고자 한다"라며 "그에 따라 2017.12.19 오후 2시를 기준으로 모든 코인과 현금의 입출금은 정지된다. 파산으로 인해 현금과 코인의 정산은 모든 파산 절차에 준해 진행된다"고 알렸다.

* Source : https://byline.network/2017/12/1-972/

04
2017 년 국외 보안 소식

2017 년 국외 정보보안 소식

- 1월 1일 : Anonymous, FBI 해킹 주장

http://pastebin.com/5vwz6Wj4

- 1월 1일 : 미국 전력망 악성코드 감염 과장 보도로 확인

http://nypost.com/2017/01/01/washington-post-retracts-story-about-russian-hack-at-vermont-utility/

- 1월 3일 : Symantec, secure router Norton Core 발표

https://us.norton.com/core

- 1월 5일 : Mongodb 해킹 후 금품요구 발생

http://thehackernews.com/2017/01/mongodb-database-security.html

- 1월 5일 : Linux Killdisk Ransomware

http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/

- 1월 9일 : Shamoon 2 변형 등장

http://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/

2017 년 국외 정보보안 소식

- 1월 10일 : ShadowBrokers, NSA 해킹 툴 공개

https://onlyzero.net/theshadowbrokers.bit/post/messagefinale/

- 1월 12일 : Ukraine 정전 사이버공격으로 결론

http://www.bbc.com/news/technology-38573074

- 1월 18일 : 오래된 코드를 사용한 Mac 악성코드 발견

https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/

- 1월 17일 : Spain에서 NeverQuest 악성코드 관계자 검거

http://www.guardiacivil.es/en/prensa/noticias/6075.html

- 1월 19일 : St. Louis 도서관 Ransomware 감염으로 피해

http://money.cnn.com/2017/01/19/technology/st-louis-public-library-hack/index.html

- 1월 21일 : BBC, Nyt twitter 계정 해킹

https://www.hackread.com/bbc-nyt-twitter-accounts-hacked/

2017 년 국외 정보보안 소식

- 1월 23일 : 중국 정부 vpn 불법화

http://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall

- 1월 24일 : Checkpoint, Google Play에서 악성앱 Charger 발견

http://blog.checkpoint.com/2017/01/24/charger-malware/

- 1월 25일 : Russia 정부, Ruslan Stoyano 반역죄로 검거

http://www.kommersant.ru/doc/3200840

- 1월 28일 : Hotel 에서 Ransomware 감염으로 키시스템에 장애 발생

http://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms

- 1월 30일 : NetGear Routers 취약점

https://www.trustwave.com/Resources/SpiderLabs-Blog/CVE-2017-5521--Bypassing-Authentication-on-NETGEAR-Routers/

- 1월 31일 : Czech, 외무장관 메일 해킹

http://abcnews.go.com/Technology/wireStory/czech-foreign-minister-emails-hacked-foreign-state-45163676

2017 년 국외 정보보안 소식

- 2월 1일 : Licking County, Ransomware 감염으로 장애 발표

http://www.10tv.com/article/officials-ransom-demanded-licking-county-technology-hack

- 2월 3일 : InterContinental Hotels Group, 12개 호텔에서 Card 정보 유출 발표

http://www.prnewswire.com/news-releases/ihg-notifies-guests-of-payment-card-incident-at-12-properties-in-the-americas-300401996.html

- 2월 3일 : Several Polish banks hacked

https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/

- 2월 4일 : Washington DC CCTV 해킹 용의자 검거

http://www.dailymail.co.uk/news/article-4191080/British-man-woman-arrested-CCTV-Washington-DC-hacked.html

- 2월 6일 : MacOS Macro 악성코드 발견

https://objective-see.com/blog/blog_0x17.html

- 2월 6일 : iKittens: Iranian Actor Resurfaces with Malware for Mac

https://iranthreats.github.io/resources/macdownloader-macos-malware/

2017 년 국외 정보보안 소식

- 2월 6일 : Mirai 전파 시키는 Windows 악성코드 발견

https://news.drweb.com/show/?i=11140&c=5&lng=en&p=0

- 2월 8일 : Fileless attacks against enterprise networks

https://securelist.com/blog/research/77403/fileless-attacks-against-enterprise-networks/

- 2월 8 일 : Boeing 직원 개인정보 유출

https://agportal-s3bucket.s3.amazonaws.com/Breach%20The%20Boeing%20Company%202017-02-08.pdf

- 2월 14일 : Xagent Mac Malware Linked with the APT28

https://labs.bitdefender.com/2017/02/new-xagent-mac-malware-linked-with-the-apt28/

- 2월 22일 : macOS, Ransomware 발견

http://www.welivesecurity.com/2017/02/22/new-crypto-ransomware-hits-macos/

- 2월 28일 : AtomicBombing 기법이 적용된 Dridex 변형 발견

https://securityintelligence.com/dridexs-cold-war-enter-atombombing

2017 년 국외 정보보안 소식

- 3월 4일 : 미국, 북한에 대한 'Left of Launch' 작전 수행 ?

https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html

- 3월 6일 : Kaspersky, Diskwiper 악성코드 정보 공개

https://securelist.com/blog/research/77725/from-shamoon-to-stonedrill/

- 3월 7일 : WikiLeaks, CIA 기밀자료 공개

https://wikileaks.org/ciav7p1/

- 3월 8일 : New Apache Struts2 0 day 공격 발생

http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html

- 3월 10일 : CGI Vulnerability으로 감염되는 Linux 악성코드

http://blog.trendmicro.com/trendlabs-security-intelligence/new-linux-malware-exploits-cgi-vulnerability/

- 3월 14일 : Citadel 제작자 러시아인 Mark Vartanyan(Kolypto) 유죄 선고

https://www.justice.gov/usao-ndga/pr/russian-hacker-kolypto-extradited-norway

- 3월 10일 : Mobile 제품에 preinstalled malware 발견

http://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

2017 년 국외 정보보안 소식

- 3월 16일 : 미국, Yahoo 해킹에 러시아 관련 발표

https://www.welivesecurity.com/2017/03/16/us-charges-russian-fsb-officials-connection-massive-yahoo-security-breach

- 3월 21일 : Avtech devices multiple vulnerabilities

https://www.search-lab.hu/advisories/126-avtech-devices-multiple-vulnerabilities

- 3월 22일 : Antivirus 제품 권한을 가져오는 DoubleAgent

https://cybellum.com/doubleagent-taking-full-control-antivirus/

- 3월 27일 : Apple iOS Script 취약점 해결

https://blog.lookout.com/blog/2017/03/27/mobile-safari-scareware/

- 4월 3일 : Kaspersky, Lazarus 그룹 북한 연계 의혹 발표

https://securelist.com/blog/sas/77908/lazarus-under-the-hood/

- 4월 4일 : 독립 McAfee 출범

http://www.bloter.net/archives/276305

2017 년 국외 정보보안 소식

- 4월 5일 : Brickerbot

https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

- 4월 7일 : Office 취약점 CVE-2017-0199 이용한 공격 발생

https://securingtomorrow.mcafee.com/mcafee-labs/critical-office-zero-day-attacks-detected-wild/

- 4월 8일 : Shadow Brokers, NSA 해킹 자료 추가 공개

https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1

- 4월 8일 : 해킹으로 Dallas 지역 응급 사이렌 울림

https://www.dallasnews.com/news/dallas/2017/04/08/emergency-sirens-blare-across-dallas-county-despite-clear-weather

- 4월 10일 : India 유니언은행 2016년 7월 1천 950 억원 해킹 시도 보도

https://www.wsj.com/articles/cybertheft-attempt-on-indian-bank-resembles-bangladesh-heist-1491816614

- 4월 15일 : NSA, 세계 각국 은행 해킹 보도

http://www.bbc.com/news/technology-39606575

2017 년 국외 정보보안 소식

- 4월 19일 : InterContinental Hotels Group (IHG) 1150개 호텔 해킹

https://www.ihg.com/content/us/en/customer-care/protecting-our-guests/california-residents

- 4월 19일 : RawPOS

http://blog.trendmicro.com/trendlabs-security-intelligence/rawpos-new-behavior-risks-identity-theft/

- 4월 19일 : 사드 보복 비판 한국 인사 메일 해킹 보도

http://news.tvchosun.com/site/data/html_dir/2017/04/19/2017041990176.html

- 4월 24일 : Webroot Windows 파일 오진

https://community.webroot.com/t5/Announcements/W32-Trojan-Gen-False-Positive-Fix-April-24/td-p/290198

- 4월 27일 : macOS Dok 발견

http://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/

- 5월 1일 : Intel, Chip 취약점 패치 발표

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr

-

2017 년 국외 정보보안 소식

- 5월 3일 : Adobe Flash Installer 가장한 macOS Turla 발견

https://blog.fox-it.com/2017/05/03/snake-coming-soon-in-mac-os-x-flavour

- 5월 6일 : Malware Protection service 원격 실행 취약점

https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5

https://technet.microsoft.com/en-us/library/security/4022344.aspx

- 5월 6일 : Handbrake 홈페이지 해킹 후 악성코드 포함 된 설치판 배포

https://forum.handbrake.fr/viewtopic.php?f=33&t=36364

- 5월 9일 : KasperskyLab 러시아 정부와 연루설 부인

https://usa.kaspersky.com/about/press-releases/2017_May-9-2017-Statement-Regarding-Recent-False-Allegations-about-Kaspersky-Lab

- 5월 11일 : HP 오디오 드라이버에서 Keylogger 발견

https://www.modzero.ch/modlog/archives/2017/05/11/en_keylogger_in_Hewlett-Packard_audio_driver/index.html

2017 년 국외 정보보안 소식

- 5월 12일 : SMB로 전파되는 WannaCry 전세계 강타

https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/

- 5월 17일 : 해킹그룹 APT3, 중국 국가안전부 하청업체

https://www.recordedfuture.com/chinese-mss-behind-apt3/

- 5월 17일 : Raspberry Pi 목표로 한 악성코드 발견

https://vms.drweb.com/virus/?_is=1&i=15389228

- 5월 22일 : Russian Interior Ministry, Cron 그룹 용의자 20 명 검거

https://www.tripwire.com/state-of-security/latest-security-news/russia-announces-arrest-20-cron-malware-group-members/

- 5월 23일 : 대북제재 담당 유엔 전문가패널에 지속적 해킹

http://www.yonhapnews.co.kr/bulletin/2017/05/23/0200000000AKR20170523081200009.HTML

- 5월 23일 : 자막 파일 이용한 동영상 플레이어 공격 발견

http://blog.checkpoint.com/2017/05/23/hacked-in-translation/

2017 년 국외 정보보안 소식

- 5월 25일 : 국내 게임 업체에서 Judy 애드웨어 포함해 게임 출시
http://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/
- 5월 31일 : 성형외과 해킹 후 수술 사진 공개
http://www.bbc.com/news/technology-40106823
- 6월 1일 : FIREBALL – The Chinese Malware of 250 Million Computers Infected
http://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/
- 6월 2일 : EternalBlue exploit (MS017-010) 포함한 Nitol 변형 발견
https://www.fireeye.com/blog/threat-research/2017/05/threat-actors-leverage-eternalblue-exploit-to-deliver-non-wannacry-payloads.html
- 6월 5일 : Russia, US 투표 시스템 해킹 시도
https://www.theguardian.com/technology/2017/jun/05/russia-us-election-hack-voting-system-nsa-report

2017 년 국외 정보보안 소식

- 6월 6일 : Kaspersky, Microsoft 에 소송

https://blog.kaspersky.com/microsoft-european-trial/16976/

- 6월 7일 : Qatar investigation finds state news agency hacked: foreign ministry

http://www.reuters.com/article/us-gulf-qatar-cybercrime-idUSKBN18Y2X4

- 6월 8일 : Al-Jazeera 공격 받음

http://www.cbsnews.com/news/al-jazeera-cyberattack-hacking/

- 6월 12일 : Industroyer: Biggest threat to industrial control systems since Stuxnet

https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

- 6월 13일 : US Cert, Hidden Cobra

https://www.us-cert.gov/ncas/alerts/TA17-164A

- 6월 15일 : Cherry Blossom

https://wikileaks.org/vault7/#Cherry%20Blossom

-

2017 년 국외 정보보안 소식

- 6월 17일 : 미국 투표기 해킹 알려진 것 보다 광범위 해킹 보도

https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

- 6월 19일 : Eset, Industroyer

https://www.welivesecurity.com/2017/06/19/industroyer-interview-ics-developed-decades-ago-no-security-mind/

- 6월 21일 : Honda 일본 공장 Ransomware 감염으로 공장 중단

https://www.nytimes.com/reuters/2017/06/21/business/21reuters-honda-cyberattack.html?_r=0

- 6월 27일 : Ukraine를 시작으로 Petya 확산

https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

- 7월 2일 : Kaspersky, 미국 정부내 Kaspersky 사용 제한 하려하자 source code 도 공개 가능하다고 밝혀

https://apnews.com/37f7f26c48ec4c31bd01ed24704aaba6

2017 년 국외 정보보안 소식

- 6월 17일 : 미국 투표기 해킹 알려진 것 보다 광범위 해킹 보도

https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

- 6월 19일 : Eset, Industroyer

https://www.welivesecurity.com/2017/06/19/industroyer-interview-ics-developed-decades-ago-no-security-mind/

- 6월 21일 : Honda 일본 공장 Ransomware 감염으로 공장 중단

https://www.nytimes.com/reuters/2017/06/21/business/21reuters-honda-cyberattack.html?_r=0

- 6월 27일 : Ukraine를 시작으로 Petya 확산

https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

- 6월 30일 : WikiLeaks, OutlasCountry 공개

https://wikileaks.org/vault7/#OutlawCountry

- 7월 2일 : Kaspersky, 미국 정부내 자사 제품 사용 제한 시도에 source code 도 공개 가능하다고 밝혀

https://apnews.com/37f7f26c48ec4c31bd01ed24704aaba6

2017 년 국외 정보보안 소식

- 7월 4일 : Avanti Markets Data Incident

http://www.avantimarkets.com/notice-of-data-breach/

- 7월 6일 : New KONNI Campaign References North Korean Missile Capabilities

http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html

- 7월 13일 : 은행 정보 노리는 macOS Dok 변형

https://blog.checkpoint.com/2017/07/13/osxdok-refuses-go-away-money/

- 7월 17일 : Sweden, 개인정보 유출

https://www.thelocal.se/20170717/swedish-authority-handed-over-keys-to-the-kingdom-in-it-security-slip-up

- 7월 18일 : Linux Users Urged to Update as a New Threat Exploits SambaCry

http://blog.trendmicro.com/trendlabs-security-intelligence/linux-users-urged-update-new-threat-exploits-sambacry/

- 7

2017 년 국외 정보보안 소식

- 7월 21일 : Qatar says cyberattack ' originated from the UAE '

http://www.Aljazeera.com/news/2017/07/Qatar-sheds-light-cyberattack-official-media-170720151344996.html

- 7월 24일 : 스웨덴 개인정보 유출

http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=6743664

- 7월 25일 : 중국 경찰 Fireball 제작자 검거

http://finance.jrj.com.cn/tech/2017/07/25163122795031.shtml

- 7월 25일 : KasperskyLab, 무료 백신 출시 발표

https://eugene.kaspersky.com/2017/07/25/kl-av-for-free-secure-the-whole-world-will-be/

- 7월 26일 : Italy UniCredit 은행 해킹으로 400,000 계정 유출

http://www.express.co.uk/finance/city/833440/italy-unicredit-bank-hacked-cyberattack-italian-banking-major-security-breach

https://www.unicreditgroup.eu/en/press-media/press-releases-price-sensitive/2017/comunicato-stampa7.html

2017 년 국외 정보보안 소식

- 7월 28일 : Wikileaks, CIA Tools 공개

https://wikileaks.org/vault7/#Imperial

- 7월 30일 : Mandiant Leak

https://pastebin.com/6HugrWH4

- 7월 31일 : HBO 해킹

http://ew.com/tv/2017/07/31/hbo-hacked-game-of-thrones/

- 8월 3일 : Marcus Hutchins Kronos 제작 혐의로 검거

https://www.grahamcluley.com/fbi-arrests-wannacrys-accidental-hero-connection-kronos-banking-trojan,

https://www.theguardian.com/technology/2017/aug/04/wannacry-marcus-hutchins-kronos-malware-arrest

- 8월 14일 : CVE-2017-0199를 이용한 공격 증가

http://blog.talosintelligence.com/2017/08/when-combining-exploits-for-added.html

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

2017 년 국외 정보보안 소식

- 8월 21일 : Wikileaks, Angelfire 공개

https://wikileaks.org/vault7/#Angelfire

- 9월 6일 : 일본 13세 소년 악성코드 판매

http://the-japan-news.com/news/article/0003922876

- 9월 6일 : Lenovo, Adware 설치 관련 벌금

https://www.hackread.com/lenovo-to-pay-millions-for-secretly-installing-adware-in-750000-laptops/

- 9월 6일 : 에너지기업 노린 Dragonfly 2.0

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

- 9월 7일 : Equifax 1억 4300 만명 개인 정보 유출

https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

- 9월 7일 : Shadowbrokers Unitedrake 공개

http://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html

2017 년 국외 정보보안 소식

- 9월 12일 : CVE-2017-8759 를 이용한 공격

https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html

- 9월 12일 : Armis, BlueBorne 취약점

https://www.armis.com/blueborne

- 9월 18일 : CCleaner 설치 파일 변조되어 악성코드 포함해 배포

http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

http://www.piriform.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users

https://blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident

- 9월 21일 : TV 방송 중 메시지 출력

http://www.ocregister.com/2017/09/21/end-of-world-prediction-interrupts-tv-broadcasts-in-orange-county/

- 9월 25일 : Deloitte 해킹

http://www.bbc.com/news/technology-41385951

-

2017 년 국외 정보보안 소식

- 9월 29일 : Mac firmware 취약점

https://duo.com/blog/the-apple-of-your-efi-mac-firmware-security-research

- 10월 3일 : Yahoo 과거 해킹 당시 추가 정보 유출 확인

https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

- 10월 5일 : Kaspersky 제품 이용해 정보 수집 주장

https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108

- 10월 11일 : Israel 해커 Kaspersky Lab 해킹 해 Russia 해커 활동 파악 주장

https://www.theregister.co.uk/2017/10/11/israel_russia_kaspersky/

- 10월 13일 : Hyatt credit card breach again

https://threatpost.com/hyatt-hit-by-credit-card-breach-again/128440/

- 10월 16일 : KRACK attacks

https://www.krackattacks.com/

- 10월 16일 : Taiwan Heist: Lazarus Tools and Ransomware

https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html

2017 년 국외 정보보안 소식

- 10월 17일 : ATM 악성코드 판매

https://securelist.com/atm-malware-is-being-sold-on-darknet-market/81871/

- 10월 19일 : Bad Rabbit Europe 확산

https://www.hackread.com/bad-rabbit-ransomware-spreading-like-wildfire/

- 10월 20일 : Elmedia Player 를 통해 macOS 악성코드 배포

https://www.eltima.com/blog/2017/10/elmedia-player-and-folx-malware-threat-neutralized.html

- 10월 26일 : 일본 겨냥한 Ursnif

https://securityintelligence.com/ursnif-campaign-waves-breaking-on-japanese-shores/

- 10월 27일 : UK 정부 Wannacry 배후에 북한있다고 밝힘

https://www.cnbc.com/2017/10/27/uk-north-korea-behind-wannacry-cyber-attack-that-crippled-nhs.html

- 10월 28일 : 거리에서 주운 USB 메모리에서 Heathrow 정보 저장

http://www.mirror.co.uk/news/uk-news/terror-threat-heathrow-airport-security-11428132

2017 년 국외 정보보안 소식

- 10월 30일 : Mobile Coinminer

http://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play

- 10월 31일 : 말레이시아 전 인구 정보 유출

https://www.lowyat.net/2017/146339/46-2-million-mobile-phone-numbers-leaked-from-2014-data-breach/

- 11월 7일 : Sowbug: Cyber espionage group targets South American and Southeast Asian governments

https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

- 11월 7일 : HP 시스템에서 Keylogging 으로 악용 가능한 기능 발견

https://support.hp.com/us-en/document/c05827409

- 11월 10일 : Antivirus 격리소 취약점을 이용한 공격

https://bogner.sh/2017/11/avgater-getting-local-admin-by-abusing-the-anti-virus-quarantine/

2017 년 국외 정보보안 소식

- 11월 14일 : US Cert, Hidden Cobra

https://www.us-cert.gov/ncas/alerts/TA17-318A

- 11월 14일 : Forever21 해킹

https://www.forever21.com/protecting_our_customers/default.aspx

- 11월 21일 : Uber 개인 정보 유출

https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

- 11월 24일 : Mirai 변형 발견

http://blog.netlab.360.com/early-warning-a-new-mirai-variant-is-spreading-quickly-on-port-23-and-2323-en/

http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/

- 12월 11일 : Nissan Finance Canada 해킹으로 정보 유출

https://www.nissancanadafinance.ca/securitynotice

2017 년 국외 정보보안 소식

- 12월 12일 : Bitfinex에 대한 DDoS Attack

https://www.hackread.com/bitfinex-cryptocurrency-exchange-hit-by-ddos-attacks/

- 12월 13일 : Mirai 배포자 징역형

https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving

- 12월 14일 : Triton Critical Infrastructure 공격

https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

- 12월 15일 : Secureworks, Lazarus Group 공격 발표

https://www.secureworks.com/about/press/media-alert-secureworks-discovers-north-korean-cyber-threat-group-lazarus-spearphishing

- 12월 15일 : Eternalblue 이용한 Miner 배포

https://f5.com/labs/articles/threat-intelligence/cyber-security/zealot-new-apache-struts-campaign-uses-eternalblue-and-eternalsynergy-to-mine-monero-on-internal-networks

2017 년 국외 정보보안 소식

- 12월 17일 : Lazarus group 가상화폐 거래소 공격

https://www.hackread.com/lazarus-group-malware-attack-to-steal-bitcoins/

https://www.bankinfosecurity.com/lazarus-hackers-phish-for-bitcoins-researchers-warn-a-10535

- 12월 19일 : 미정부 Wannacryptor (Wannacry) 공격 배후로 북한 지목

https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html

- 12월 19일 : Proofpoint, Lazarus 가상화폐 관련 업체 공격

https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new

- 12월 27일 : 가상화폐 거래소 CEO 우크라이나에서 납치

https://strana.ua/news/114106-v-kieve-pokhitili-rossijskoho-ajtishnika.html

-

05
2017년 4 분기 국외 사건 사고

AV 제품 이용한 NSA 기밀자료 유출

- NSA 자료 유출
  -

Security

'Israel hacked Kaspersky and caught Russian spies using AV tool to harvest NSA exploits'

Explosive new claims also put a bomb under US-Israeli cooperation

By Richard Chirgwin 11 Oct 2017 at 01:19 143 SHARE ▼

Updated The brouhaha over Russian spies using Kaspersky antivirus to steal NSA exploits from a staffer's home PC took an explosive turn on Tuesday.

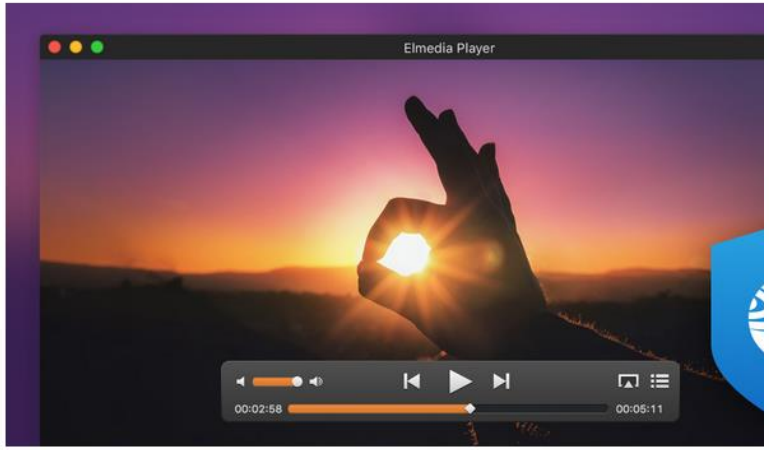
* Source : https://www.theregister.co.uk/2017/10/11/israel_russia_kaspersky/

Elemedia Player and Folx 에서 Proton 발견

- Elemedia Player and Folx 에서 Proton 발견
  - Eset 에서 발견발견

Elmedia Player and Folx malware threat Neutralized!

Alex Taylor in Free Software,Help/Support,Mac Software,System Utilities,The Company/Releases
20 Oct 2017, 14:12



On the 19th of October 2017 we were informed by a malware research company ES servers have been hacked and our apps namely Folx and Elmedia Player DMG files distributed with a malware.

OSX/Proton spreading again through supply-chain attack

BY ESET RESEARCH POSTED 20 OCT 2017 - 01:56AM

MALWARE

* Source : https://www.eltima.com/blog/2017/10/elmedia-player-and-folx-malware-threat-neutralized.html &

https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia

Darknet market에서 ATM malware 판매

- ATM 악성코드 판매
  -

ATM malware is being sold on Darknet market

By Konstantin Zykov on October 17, 2017. 9:00 am

Disclaimer and warning

ATM systems appear to be very secure, but the money can be accessed fairly easily if you know what you are doing. Criminals are exploiting hardware and software vulnerabilities to interact with ATMs, meaning they need to be made more secure. This can be achieved with the help of additional security software, properly configured to stop the execution of non-whitelisted programs on ATMs.

Worryingly, it is very easy to find detailed manuals of ATM malware. Anybody can simply buy them for around 5000 USD on darknet markets.

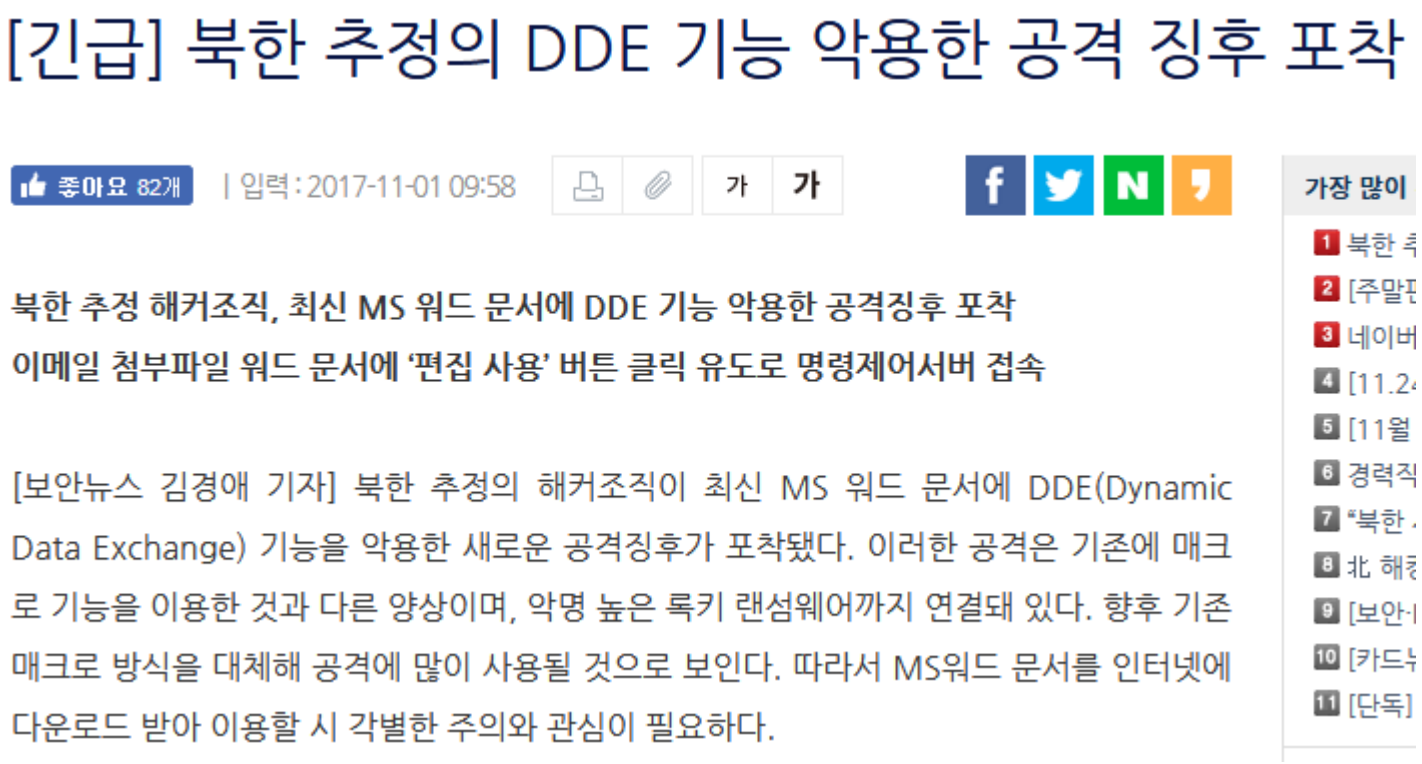
More information about CutletMaker ATM malware is available to customers of Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

* Source : https://securelist.com/atm-malware-is-being-sold-on-darknet-market/81871/

06
2017년 4 분기 취약점과 악성코드

DDE 를 이용한 공격

- Red Eyes Group에서 사용
  -



[긴급] 북한 추정의 DDE 기능 악용한 공격 징후 포착

좋아요 82개 | 입력 : 2017-11-01 09:58 가 가

가장 많이

1 북한 추
2 [주말판
3 네이버
4 [11.24
5 [11월
6 경력직
7 "북한
8 北 해킹
9 [보안
10 [카드뉴
11 [단독]

북한 추정 해커조직, 최신 MS 워드 문서에 DDE 기능 악용한 공격징후 포착

이메일 첨부파일 워드 문서에 '편집 사용' 버튼 클릭 유도로 명령제어서버 접속

[보안뉴스 김경애 기자] 북한 추정의 해커조직이 최신 MS 워드 문서에 DDE(Dynamic Data Exchange) 기능을 악용한 새로운 공격징후가 포착됐다. 이러한 공격은 기존에 매크로 기능을 이용한 것과 다른 양상이며, 악명 높은 록키 랜섬웨어까지 연결돼 있다. 향후 기존 매크로 방식을 대체해 공격에 많이 사용될 것으로 보인다. 따라서 MS워드 문서를 인터넷에 다운로드 받아 이용할 시 각별한 주의와 관심이 필요하다.

* Source : http://www.boannews.com/media/view.asp?idx=57805

DDE 를 이용한 공격

- DDE
  -

PowerShell, C-Sharp and DDE The Power Within

Reading time ~6 min

Posted by saif on 20 May 2016

Categories: Fun, Howto, Research

MS Excel Dynamic Data Exchange (DDE):

aka Exploiting MS1

A while ago this co
secondary login fu
about the vulnerab
you read James Fo

Around the same time another article came out to remind us that DDE can be used to perform command execution through Excel sheets formulas, the only down side is that the user gets two prompts instead on one, one to enable links and one to execute our payload, however this didn't stop unaware users from clicking OK to both. DDE is used by Excel workbooks for dynamic live data update as a sort of inter process communication, it allows applications to be called from within Excel formulas and even web requests to return live data to the WorkBook, more information about DDE commands can be found here. Actually, the first prompt the user has to accept is to allow the DDE links to update live data, the formula to execute CMD in Excel is very simple, just paste the following into any cell and click enter.

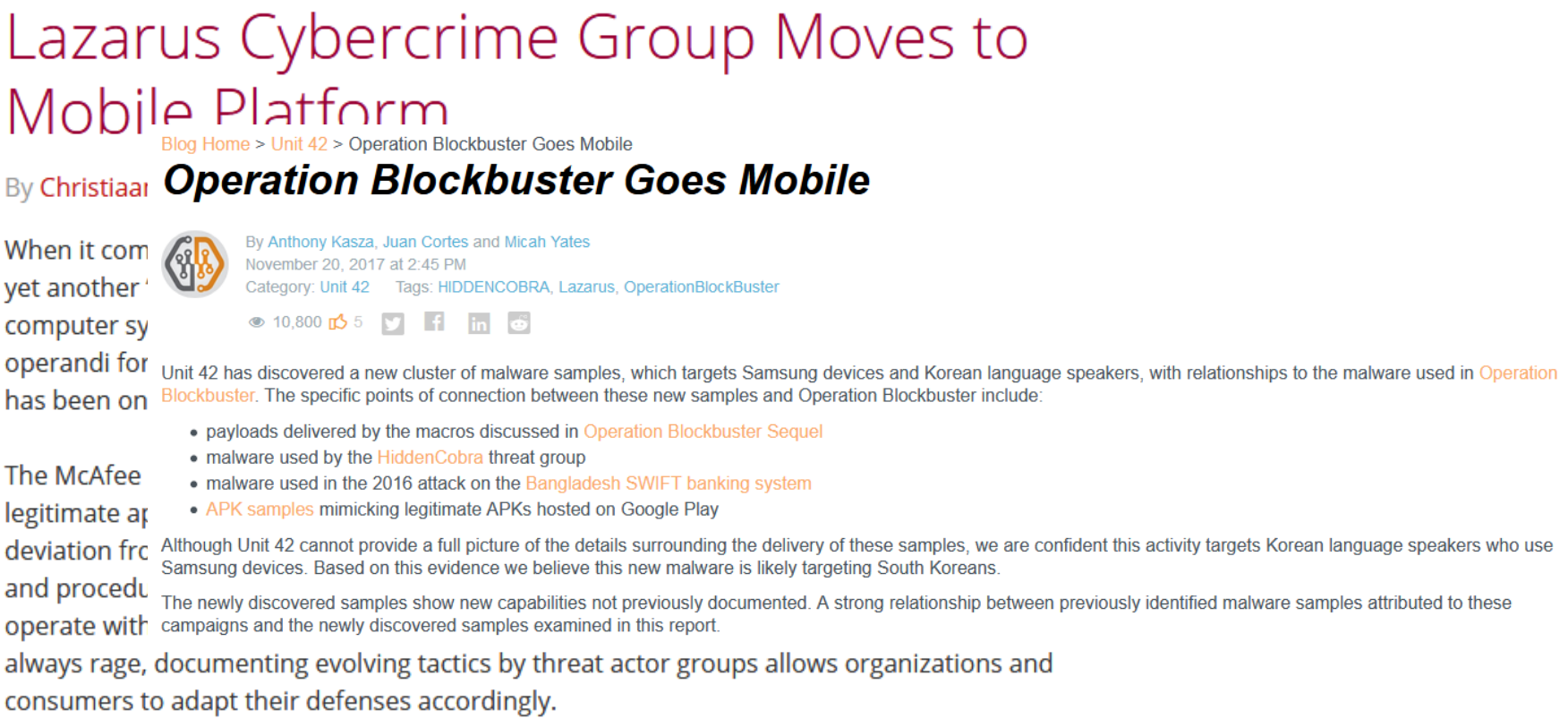
```
=cmd|'/c calc.exe'!A1
```

* Source : https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/

Lazarus Group Mobile 악성코드 발견

- Lazarus Group Mobile 악성코드

-



Lazarus Cybercrime Group Moves to Mobile Platform

By Christiaa

When it com
yet another
computer sy
operandi for
has been on

The McAfee
legitimate ap
deviation fro
and procedu
operate with

always rage, documenting evolving tactics by threat actor groups allows organizations and consumers to adapt their defenses accordingly.

Blog Home > Unit 42 > Operation Blockbuster Goes Mobile

Operation Blockbuster Goes Mobile

By Anthony Kasza, Juan Cortes and Micah Yates
November 20, 2017 at 2:45 PM
Category: Unit 42 Tags: HIDDENCOBRA, Lazarus, OperationBlockBuster

10,800 5

Unit 42 has discovered a new cluster of malware samples, which targets Samsung devices and Korean language speakers, with relationships to the malware used in Operation Blockbuster. The specific points of connection between these new samples and Operation Blockbuster include:

- payloads delivered by the macros discussed in Operation Blockbuster Sequel
- malware used by the HiddenCobra threat group
- malware used in the 2016 attack on the Bangladesh SWIFT banking system
- APK samples mimicking legitimate APKs hosted on Google Play

Although Unit 42 cannot provide a full picture of the details surrounding the delivery of these samples, we are confident this activity targets Korean language speakers who use Samsung devices. Based on this evidence we believe this new malware is likely targeting South Koreans.

The newly discovered samples show new capabilities not previously documented. A strong relationship between previously identified malware samples attributed to these campaigns and the newly discovered samples examined in this report.

* Source : https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-cybercrime-group-moves-to-mobile &

https://researchcenter.paloaltonetworks.com/2017/11/unit42-operation-blockbuster-goes-mobile/

07
Case Study : 여행사 해킹

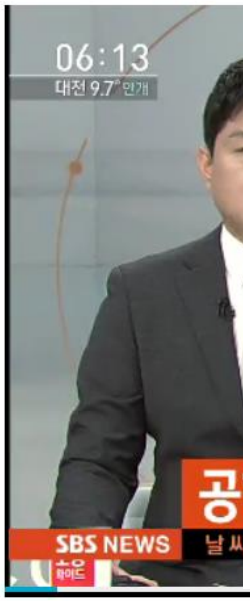
공항 자동출입국 시스템 관리 업체 해킹

• 공항 자동출입국 시스템 관리 업체 해킹

- 홈페이지 통해 악성코드 유포

공항 출입국 시스템 관리 업체 해킹...북한 소행 가능성

김수형 기자 sean@sbs.co.kr 작성 2017.10.17 06:21 수정 2017.10.17 08:51 조회 1,543 프린트 글자 크기



공항 자동출입국 시스템 제공업체 해킹 논란 짚어보니

좋아요 32개 | 입력 : 2017-10-18 15:45 가 가

해당 SI업체 "공항 자동출입국 시스템 유지보수는 지난해 종료, 관리주체 우리 아냐"

악성코드는 올해 5월부터 유포...5개월간 방치된 웹사이트 관리 부실 '도마 위'

[보안뉴스 김경애 기자] 국내 공항의 자동 출입국 시스템을 담당했던 SI 업체의 웹사이트가 해킹돼 방문자를 대상으로 악성코드를 유포한 것으로 드러나 논란이 커지고 있다.

가장 많이 본

1 자율주행
2 유명 웹하
3 보안 전문
4 정부 수사
5 포커·맞고
6 비트코인
7 가상화폐
8 리눅스 노

* Source : http://news.sbs.co.kr/news/endPage.do?news_id=N1004438303 & http://www.boannews.com/media/view.asp?idx=57543

H여행사 해킹

- 하나투어 해킹
  - 유지보수 업체 직원의 컴퓨터에 악성코드 감염

최신기사

하나투어 해킹, 회원정보 유출…"관계기관 수사중"

송고시간 | 2017/10/17 17:52

(서울=연합뉴스) 이도연 기자 =

유출된 것으로 알려졌다.

17일 하나투어는 홈페이지에 시

감염됐음을 인지하고 조사하던

확인했다"고 밝혔다.

유출된 개인정보 하나투어 이용

민등록번호·집전화번호·집주소·(

제목	개인정보 유출사고 안내 및 사과의 말씀		
글쓴이	하나투어	작성일	2017/10/18 10:23

하나투어를 신뢰하고 사랑해주신 고객님께
개인정보 유출 사실을 통지해 드리며,
심려를 끼쳐드린 점 머리 숙여 사과 드립니다.

하나투어는 고객님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나,
소중한 고객님의 개인 정보가 침해되는 사고가 발생한 점에 대해 진심으로 사과드립니다.

당사는 당사 유지 보수 업체 직원의 PC가 악성코드에 감염되었음을 인지하고 조사하던 중,
2017년 9월 28일 PC를 통해 개인정보 파일의 일부가 유출된 정황을 확인하였습니다.

* Source : http://www.yonhapnews.co.kr/bulletin/2017/10/17/0200000000AKR20171017170300030.HTML &

http://www.hanatour.com/asp/custcenter/bb-20000.asp

H여행사 해킹

• 하나투어와 SI 업체 해킹 연관성 존재

-

하나투어와 SI업체 해킹, 연관성 드러나...동일범 소행인가

좋아요 53개 | 입력 : 2017-10-20 10:40 가 가

하나투어 해킹에 악용됐던 악성코드가 통신하는 C&C서버 IP와 SI업체 IP 대역 유사

북한 추정 사이버공격의 공격방식과 악성 프로그램도 유사하다는 분석 제기

[보안뉴스 김경애 기자] 하나투어의 고객정보 유출에 악용됐던 악성코드와 통신하는 C&C 서버(명령제어 서버)의 IP 대역이 이보다 앞서 해킹된 SI업체 홈페이지의 IP 대역과 유사한 것으로 조사됐다. 더군다나 기존 북한 추정 사이버공격의 공격방식과 동원된 악성 프로그램도 거의 동일하다는 의견이 제기되면서 연쇄적인 사이버공격의 일부가 수면 위로 드러나기 시작한 것 아닌지 관심이 모아지고 있다.

가장 많이 본 기사

1 자율주행차 시험장
2 유명 웹하드 사이트
3 정부 수사 중인 인터
4 가상화폐 거래소 '코
5 리눅스 노린 MOTD
6 망분리 된 PLC 시스
7 北 사이버공격과 비
8 끊이지 않는 가상화
9 국내 IP 카메라 해킹
10 인터넷나야나 IDC
11 디지털 포렌식으로

* Source : http://www.boannews.com/media/view.asp?idx=57572

H여행사 해킹

- 유지보수 업체를 통한 침해 가능성
  -

하나투어의 유지보수 업체 둘러싼 의문점…고개 드는 고객사 해킹 의혹

좋아요 47개 | 입력 : 2017-10-20 18:25 가 가

하나투어 유지보수 업체 홈피, 개인정보 유출 시점 이후 변경돼 해킹 의혹 증폭

[보안뉴스 김경애 기자] 하나투어는 지난 18일 '개인정보 유출사고 안내 및 사과의 말씀'이란 제목의 공지사항으로 하나투어의 유지보수 업체 직원 PC가 악성코드에 감염돼 조사하던 중 개인정보가 유출됐다고 밝힌 바 있다. 이로 인해 하나투어 뿐만 아니라 유지보수 업체와 해당 업체의 다른 고객사들도 악성코드 감염과 해킹 사고가 발생했을 가능성이 커지고 있다.

가장 많이 본 기사 »

1 자율주행차 시험장 '케이-시티', 고속도로 구…
2 유명 웹하드 사이트, 무려 1년간 파밍 악성코…
3 정부 수사 중인 인터넷나야나에서 추가 랜섬웨어…
4 가상화폐 거래소 '코빗' 사칭 악성메일 주의보…
5 리눅스 노린 MOTD 랜섬웨어 등장! 리눅스 …
6 망분리 된 PLC 시스템 공격하는 방법, 또 …
7 北 사이버공격과 비트코인 그리고 랜섬웨어간 상…
8 끊이지 않는 가상화폐 거래소 해킹 피해…뫼…
9 국내 IP 카메라 해킹한 해커, 페이스북에 해…
10 인터넷나야나 IDC 사업부, 코리아IDC도 랜…
11 디지털 포렌식으로 풀어본 최순실 '태블릿 PC…

* Source : http://www.boannews.com/media/view.asp?idx=57594&page=2

자유투어 해킹

- 자유투어 해킹
  - 2017년 12월 11일 침해 정확 확인
  - Andariel Group 소행 추정

제목 [자유공지] [자유투어] 개인정보 침해사고 안내 및 사과문

글쓴이 : 자유투어 2017-12-15 오후 3:34:00

(주)자유투어를 신뢰하고 이용해주신 고객님께
개인정보 침해 사실을 통지해 드리며,
심려를 끼쳐드린 점 진심으로 사과드립니다.

(주)자유투어는 고객님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나,
불의의 사고로 소중한 고객님의 개인정보가 침해되는 사고가 발생한 점에 대해 진심으로 사과드립
니다.

당사는 2017년 12월 11일 16시경 해커 조직에 의해 일부 고객님의 개인정보가 침해된 정황을 확인
하였습니다.
현재까지 확인된 침해정보는 2012년부터 2017년 9월 사이에 당사를 이용한 고객님 중 일부의 이름,
생년월일, 휴대전화번호, 집전화번호, 이메일, 주소, 당사 홈페이지 이용자 아이디(ID), 암호화된 비밀번호이며
고객님의 주민등록번호는 침해되지 않은 것으로 확인되었습니다.

* Source : http://www.jautour.com/customer/notice/view.asp?b_idx=56109&col=&search=&bow=&gotoPage=1

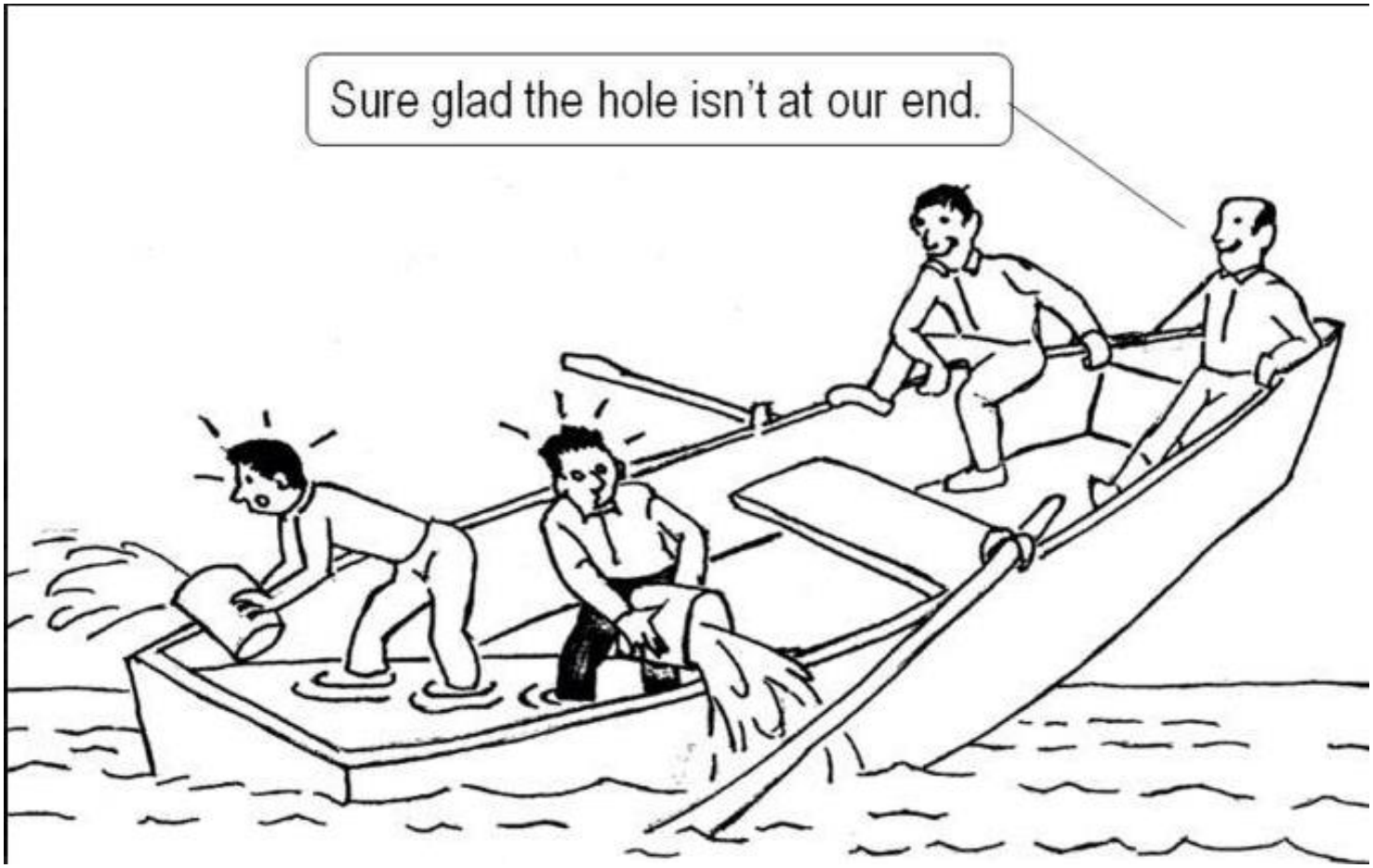
현재의 보안 문제

- Not really a fair fight

* source : http://image-store.slidesharecdn.com/81268b95-5c3b-4604-9129-d83ab3dc4600-large.png

현재의 보안 문제

- 모두가 함께 해야 하는 보안



* source : http://www.security-marathon.be/?p=1786

Q&A

email : minseok.cha@ahnlab.com / mstoned7@gmail.com
http://xcoolcat7.tistory.com, https://www.facebook.com/xcoolcat7
https://twitter.com/xcoolcat7, https://twitter.com/mstoned7