어떻게 조사할 것인가?

Byungkil Lee

nullhat@gmail.com

발표순서

1. 주요 사건 사례
2. 사건사고의 인지경위
3. 인지경위별 초동조치
4. 시나리오 적용
5. Q & A

사건 사례

분류	시스템 장애 및 파괴 (가용성)		악성코드 (무결성)	내부정보 유출 (기밀성)	
구분	서비스 장애	시스템 파괴	악성코드 유포, 웹쉘발견 이메일등을 통한 유포	개인정보 유출	기밀문서 유출
유형	DDoS	악성코드	홈페이지 등을 통한 악성코드 유포	네트워크 및 시스템 침입	
수법	Zombie C&C	시스템 주요 파일 삭제 HDD파괴	Drive by download OS, IE, APP등 취약점이용	사이트 취약점 이용 Spear Phishing App 업데이트등을 이용한 APT 악성코드 무작위 유포	
사례	7.7('09) 3.4('11)	농협('11) 320('13) 625('13)	중앙일보('12) 스미싱 & 파밍 IE 및 캐쉬서버 취약점('14)	옥션('08) SK컴즈('11) 넥슨('11) KT('11) EBS('12)	한수원('14)

사건사고 인지경위

1. DDoS에 의한 사건인지

2. 컴퓨터시스템의 논리적 파괴에 의한 사건인지

3. 내부자료 유출에 의한 사건인지

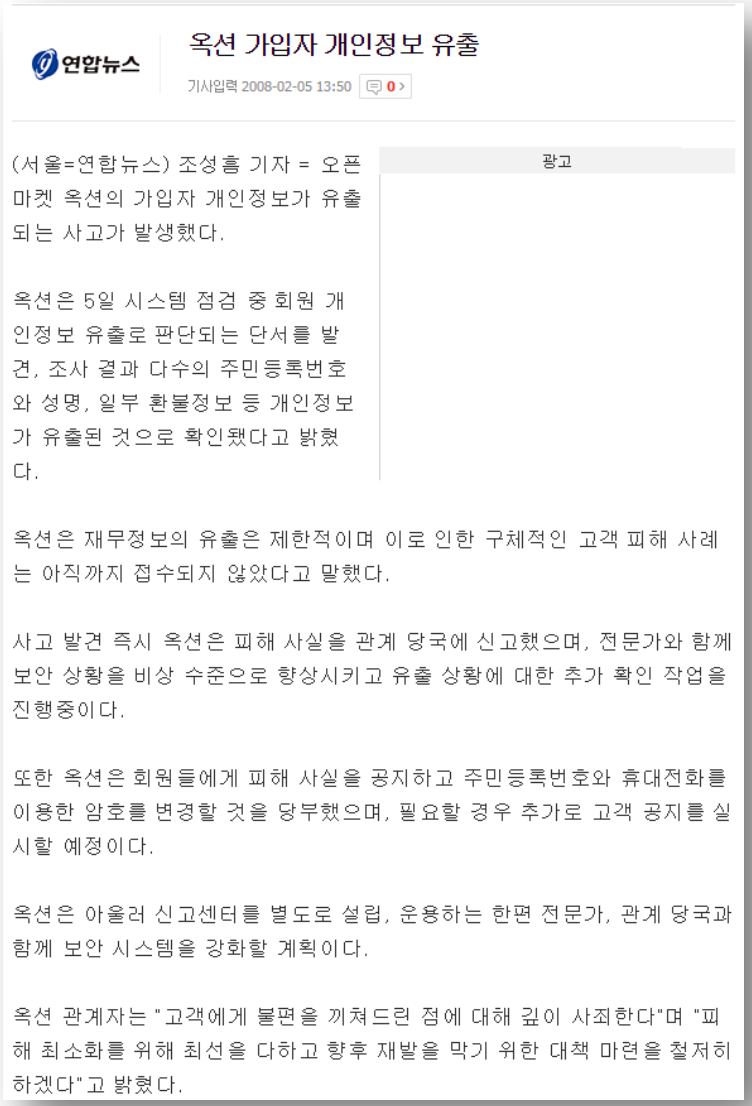
4. 설치된 악성프로그램의 발견에 의한 사건인지

5. 악성프로그램이 첨부된 이메일등 수신에 의한 사건인지

6. 페이지변조, 웹쉘 발견등 서버침입 사실인지

사건사고 인지경위

2008. 02. 05 – 옥션



연합뉴스

옥션 가입자 개인정보 유출

기사입력 2008-02-05 13:50 0

광고

(서울=연합뉴스) 조성흠 기자 = 오픈마켓 옥션의 가입자 개인정보가 유출되는 사고가 발생했다.

옥션은 5일 시스템 점검 중 회원 개인정보 유출로 판단되는 단서를 발견, 조사 결과 다수의 주민등록번호와 성명, 일부 환불정보 등 개인정보가 유출된 것으로 확인됐다고 밝혔다.

옥션은 재무정보의 유출은 제한적이며 이로 인한 구체적인 고객 피해 사례는 아직까지 접수되지 않았다고 말했다.

사고 발견 즉시 옥션은 피해 사실을 관계 당국에 신고했으며, 전문가와 함께 보안 상황을 비상 수준으로 향상시키고 유출 상황에 대한 추가 확인 작업을 진행중이다.

또한 옥션은 회원들에게 피해 사실을 공지하고 주민등록번호와 휴대전화를 이용한 암호를 변경할 것을 당부했으며, 필요할 경우 추가로 고객 공지를 실시할 예정이다.

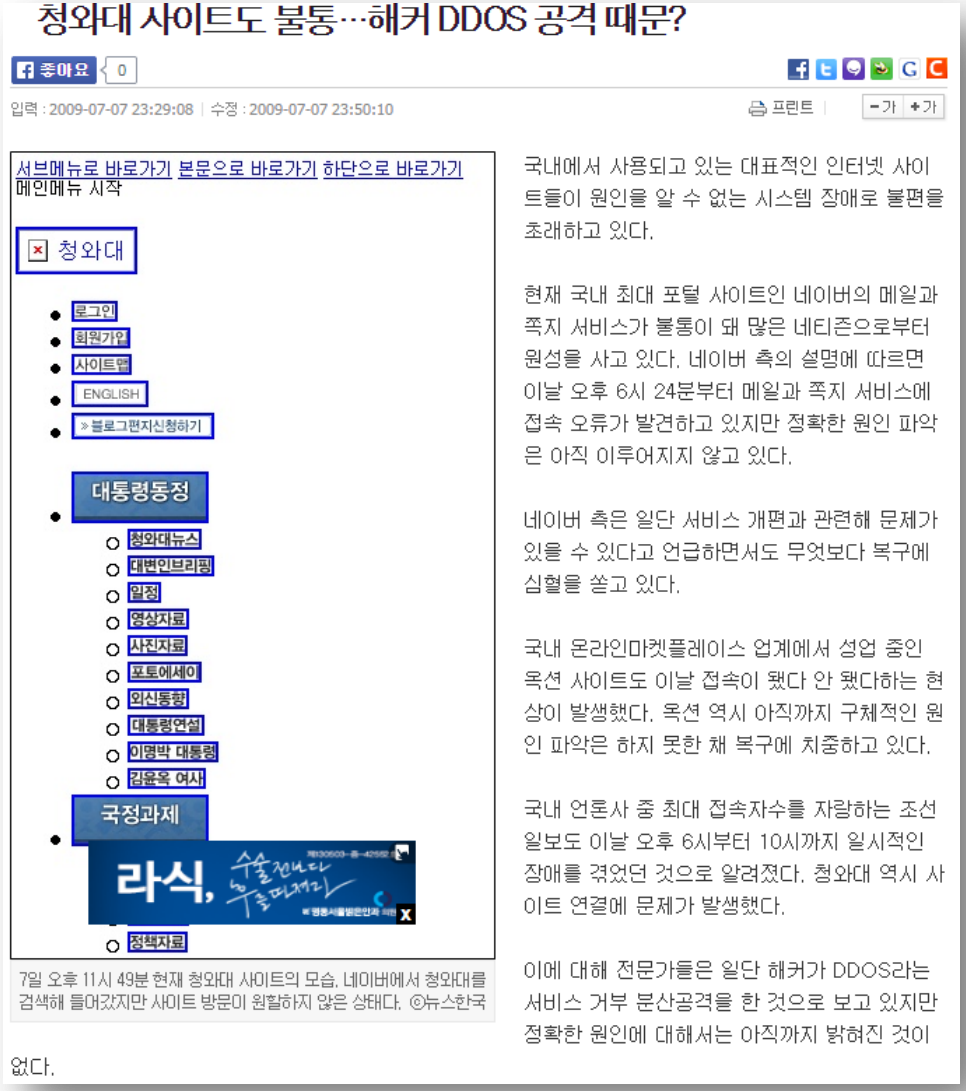
옥션은 아울러 신고센터를 별도로 설립, 운용하는 한편 전문가, 관계 당국과 함께 보안 시스템을 강화할 계획이다.

옥션 관계자는 "고객에게 불편을 끼쳐드린 점에 대해 깊이 사죄한다"며 "피해 최소화를 위해 최선을 다하고 향후 재발을 막기 위한 대책 마련을 철저히 하겠다"고 밝혔다.

- 보도일자 : 2008. 02. 05.
- 발생일자 : 2008. 01. 04.
- 인지경위
  - 외부자의 제보 및 공갈
- 보도경위
  - 피해업체의 피해사실 공개
- 수사착수 경위
  - 피해업체의 신고

사건사고 인지경위

2009. 07. 07 – 77 DDoS



청와대 사이트도 불통…해커 DDOS 공격 때문?

좋아요 0

입력 : 2009-07-07 23:29:08 | 수정 : 2009-07-07 23:50:10

프린트 | -가 +가

서브메뉴로 바로가기 본문으로 바로가기 하단으로 바로가기
메인메뉴 시작

청와대

- 로그인
- 회원가입
- 사이트맵
- ENGLISH
- »블로그편지신청하기
- 대통령동정
  - 청와대뉴스
  - 대변인브리핑
  - 일정
  - 영상자료
  - 사진자료
  - 포토에세이
  - 외신동향
  - 대통령연설
  - 이명박 대통령
  - 김윤옥 여사
- 국정과제
- 정책자료

7일 오후 11시 49분 현재 청와대 사이트의 모습. 네이버에서 청와대를 검색해 들어갔지만 사이트 방문이 원활하지 않은 상태다. ⓒ뉴스한국

국내에서 사용되고 있는 대표적인 인터넷 사이트들이 원인을 알 수 없는 시스템 장애로 불편을 초래하고 있다.

현재 국내 최대 포털 사이트인 네이버의 메일과 쪽지 서비스가 불통이 돼 많은 네티즌으로부터 원성을 사고 있다. 네이버 측의 설명에 따르면 이날 오후 6시 24분부터 메일과 쪽지 서비스에 접속 오류가 발견하고 있지만 정확한 원인 파악은 아직 이루어지지 않고 있다.

네이버 측은 일단 서비스 개편과 관련해 문제가 있을 수 있다고 언급하면서도 무엇보다 복구에 심혈을 쏟고 있다.

국내 온라인마켓플레이스 업계에서 성업 중인 옥션 사이트도 이날 접속이 됐다 안 됐다하는 현상이 발생했다. 옥션 역시 아직까지 구체적인 원인 파악은 하지 못한 채 복구에 치중하고 있다.

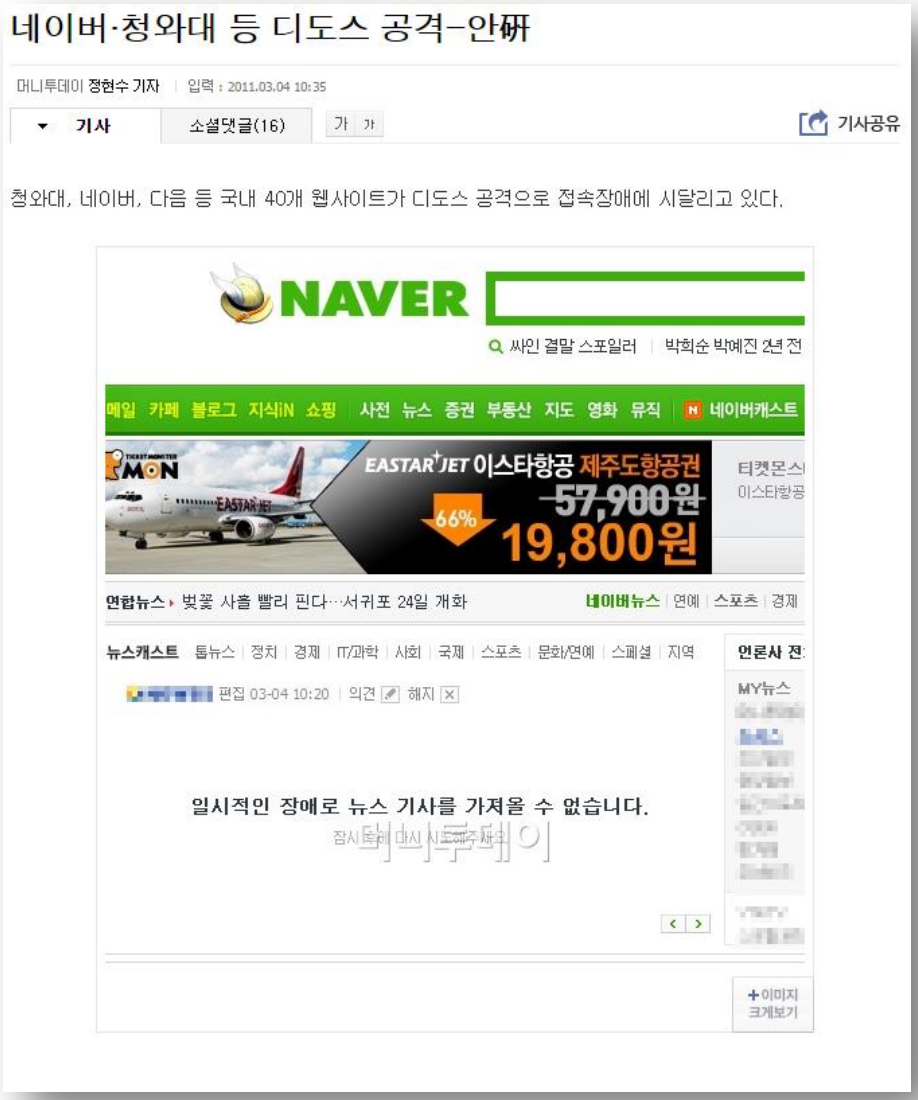
국내 언론사 중 최대 접속자수를 자랑하는 조선일보도 이날 오후 6시부터 10시까지 일시적인 장애를 겪었던 것으로 알려졌다. 청와대 역시 사이트 연결에 문제가 발생했다.

이에 대해 전문가들은 일단 해커가 DDOS라는 서비스 거부 분산공격을 한 것으로 보고 있지만 정확한 원인에 대해서는 아직까지 밝혀진 것이 없다.

- 보도일자 : 2009. 07. 07.
- 발생일자 : 2009. 07. 07.
- 인지경위
  - 트래픽의 폭주와 서비스 장애
- 보도경위
  - 트래픽의 폭주와 서비스 장애
- 수사착수 경위
  - 트래픽의 폭주와 서비스 장애

사건사고 인지경위

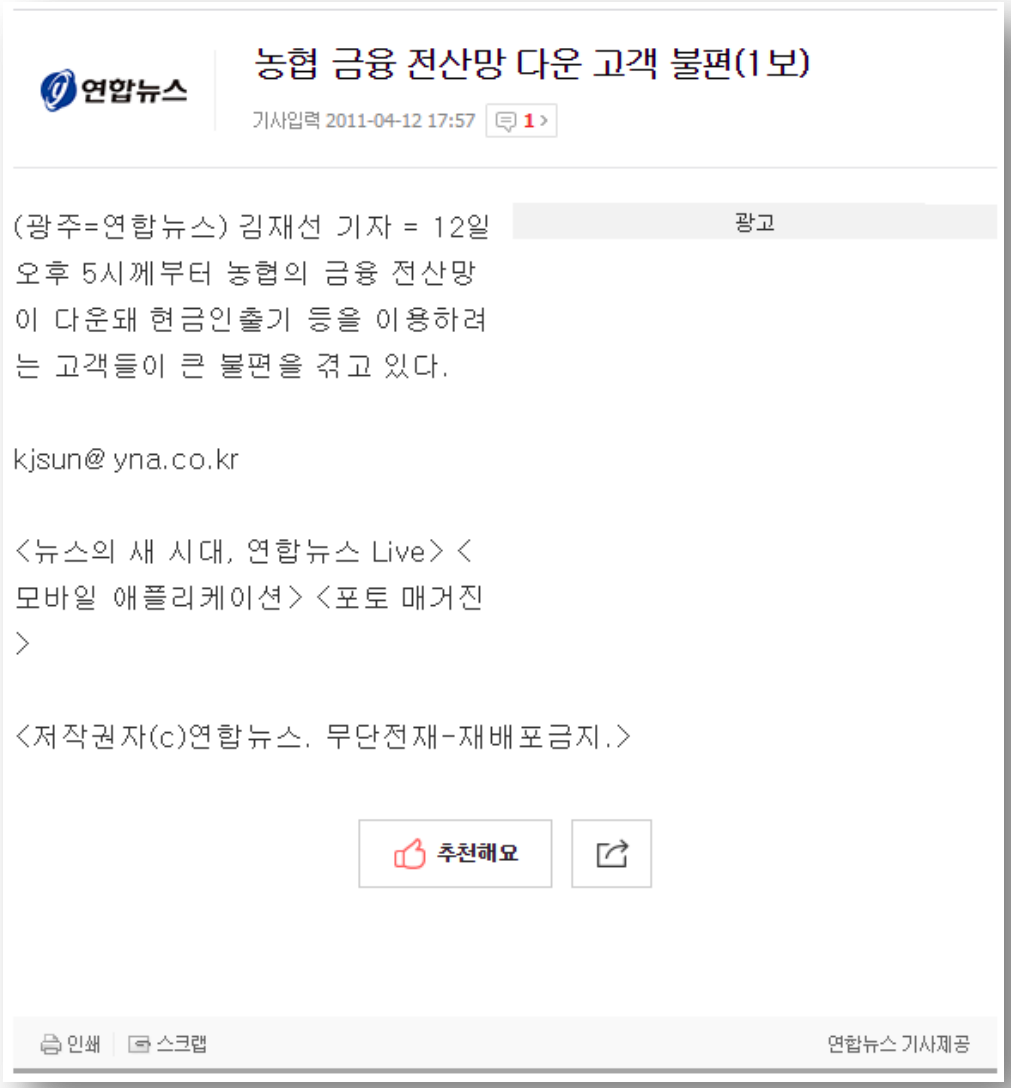
2011. 03. 04 – 34 DDoS



- 보도일자 : 2011. 03. 04.
- 발생일자 : 2011. 03. 04.
- 인지경위
  - 트래픽의 폭주와 서비스 장애
- 보도경위
  - 트래픽의 폭주와 서비스 장애
- 수사착수 경위
  - 트래픽의 폭주와 서비스 장애

사건사고 인지경위

2011. 04. 12 – 농협



연합뉴스

농협 금융 전산망 다운 고객 불편(1보)

기사입력 2011-04-12 17:57 1

(광주=연합뉴스) 김재선 기자 = 12일 오후 5시께부터 농협의 금융 전산망이 다운돼 현금인출기 등을 이용하려는 고객들이 큰 불편을 겪고 있다.

광고

kjsun@yna.co.kr

<뉴스의 새 시대, 연합뉴스 Live> <모바일 애플리케이션> <포토 매거진>

<저작권자(c)연합뉴스. 무단전재-재배포금지.>

추천해요

인쇄 스크랩 연합뉴스 기사제공

- 보도일자 : 2011. 04. 12.
- 발생일자 : 2011. 04. 12.
- 인지경위
  - ATM등 시스템 운영 장애
- 보도경위
  - ATM등 시스템 운영 장애
- 수사착수 경위
  - ATM등 시스템 운영 장애

사건사고 인지경위

2011. 07. 26 – SK커뮤니케이션

싸이월드·네이트, 중국발 해킹으로 고객정보 유출

2011.07.28 13:53:40 / 이민형 기자 kiku@ddaily.co.kr

[디지털데일리 이민형기자] SK커뮤니케이션(corp.nate.com 대표 주형철, 이하 SK컴즈)는 중국발 해커에 의해 고객 정보가 일부 유출됐다고 28일 밝혔다.

SK컴즈 관계자는 "지난 26일, 해킹으로 인해 고객 정보의 일부 유출이 있었음을 확인했다"며 "이에 고객 피해를 예방하고 범인을 조속히 검거하기 위해 신속하게 수사기관 및 관계기관에 즉시 조사를 의뢰한 상태"라고 말했다.

아직까지 정확한 유출 규모는 파악되고 있지 않으나 네이트, 싸이월드 가입자의 3500만 명의 가입정보 중 일부만 유출됐을 것으로 회사측은 유추하고 있다.

이번 고객정보 유출은 중국발 IP의 악성코드에 의한 것으로, 현재까지 확인한 유출된 개인 정보에는 ID와 이름, 핸드폰번호, 이메일주소, 암호화된 비밀번호, 암호화된 주민번호 등이다.

SK컴즈는 이번 개인정보 유출로 인해 보이스피싱이나 스팸메일 등 고객들의 2차 피해 방지 차원에서 핫라인 콜센터를 확대 운영할 예정이다.

또한 업계전문가 등 관련기관과의 연계 및 당사 기술 인프라를 적극 활용해, 보이스피싱 및 스팸메일 차단 프로그램을 신속히 운영할 계획이다.

이 회사 주형철 대표는 "이번 일과 관련해 고객들께 다시 한번 고개 숙여 사과드린다"며 "재발방지와 고객피해 최소화를 위해 회사의 모든 역량을 기울일 것과 조속한 원인파악 및 고객정보 회수를 위해 수사기관과의 적극적인 협조를 약속으며, 추후 수사기관 및 관계기관의 사실 확인을 바탕으로 자세한 내용을 고객들께 설명할 것"이라고 말했다.

- 보도일자 : 2011. 07. 28.
- 발생일자 : 2011. 07. 26.
- 인지경위
  - 데이터유출 탐지
- 보도경위
  - 피해업체의 피해사실 공개
- 수사착수 경위
  - 피해업체의 신고

사건사고 인지경위

2012. 05. 17 – EBS

EBS 뚫렸다… 400만명 개인정보 유출

수능사이트는 해킹 안돼

머니투데이 성연광 기자 | 입력 : 2012.05.17 13:53

기사 | 소셜댓글(0) | 가 가 | 기사공유

한국교육방송공사(EBS)이 해킹돼 400만명 규모의 개인정보가 유출되는 사고가 발생했다.

18일 EBS에 따르면, EBS 메인사이트(www.ebs.co.kr)가 지난 15일 중국발 IP로부터 해킹돼 일부 회원들의 개인정보가 유출된 것으로 확인됐다.

현재 유출된 개인정보는 2009년 12월 이전에 가입된 일부 회원의 이름, 아이디, 비밀번호, 전화번호, 이메일, 주소 등으로 추정된다. 그러나 주민등록번호와 계좌번호 등 정보는 보관하지 않고 있어 이번 사고와는 관련이 없다고 EBS측은 밝혔다.

EBS측은 수험생이 많이 이용하고 있는 EBS 수능사이트(www.ebsi.co.kr)는 별도로 강화된 보안 시스템으로 운영돼 이번 사고와는 무관하다고 덧붙였다.

EBS 메인사이트는 EBS TV와 라디오 방송 프로그램 관련 서비스를 제공하고 있으며, 2008년부터 KT에서 운영하고 있다.

현재 메인사이트 회원수는 총 2000만명으로, 이 가운데 약 400만명 가량의 회원정보가 빠져나간 것으로 EBS측은 보고 있다.

이번 사고와 관련, EBS는 만약의 피해에 대비해 동일 아이디와 비밀번호를 이용하는 타 사이트의 모든 비밀번호를 꼭 변경하고, 보이스피싱, 스팸 메일 등에 주의를 당부했다.

EBS 관계자는 "이번 침해 사고에도 불과하고 현재 EBS 전 사이트는 즉각적인 조치를 통해 아무런 이상 없이 운영되고 있으며, 유출가능성이 있는 회원들에게 바로 안내 메일을 발송했다"고 설명했다.

한편, 정확한 피해규모는 유관기관과 협조해 분석 중인 것으로 알려졌다. 회사측은 자세한 경위파악과 범인 검거를 위해 관계기관에 수사를 의뢰했다고 밝혔다.

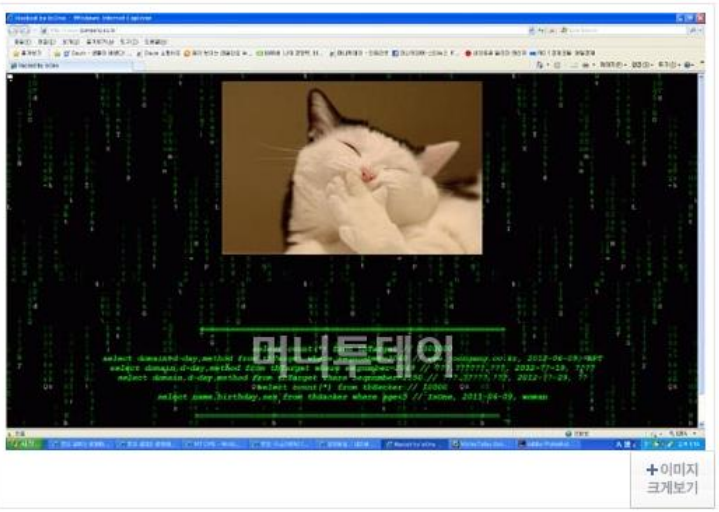
- 보도일자 : 2012. 05. 17.
- 발생일자 : 2012. 05. 13.
- 인지경위
  - 웹쉘 발견
- 보도경위
  - 피해업체의 피해사실 공개
- 수사착수 경위
  - 피해업체의 신고

2012. 06. 09 – 중앙일보

중앙일보 홈페이지 해킹당해

머니투데이 구경민 기자 | 입력 : 2012.06.09 19:05 | 조회 : 17209

기사 | 소셜댓글(4) | 가 가 | 기사공유



중앙일보 홈페이지가 해킹을 당했다. 지난달 EBS 교육방송이 해킹사고를 당한지 불과 한달도 채 안되서 일어난 일로 개인정보 유출에 대한 우려감이 높아지고 있다.

9일 현재 중앙일보 홈페이지는 정상적인 운영이 이뤄지지 않는 것으로 확인됐다. 접속할 경우 'Hacked by IsOne'라는 표시와 함께 고양이 사진이 게재돼 있다.

이번 해킹사고와 관련해 경찰청 사이버테러대응센터가 중앙일보 측의 수사 의뢰를 해 수사에 착수할지 여부가 주목된다.

한편, EBS 교육방송은 지난달 15일 해킹을 당해 약 400만명의 개인정보가 유출된 바 있다.

- 보도일자 : 2012. 06. 09.
- 발생일자 : 2012. 06. 09.
- 인지경위
  - 웹사이트 변조와 서버 정지
- 보도경위
  - 웹사이트 변조
- 수사착수 경위
  - 웹사이트 변조

사건사고 인지경위

2013. 03. 20 – 320

[속보] KBS·MBC·YTN, 정보전산망 완전 마비

오후 2시부터 추정…공영방송사 동시 전산망 마비는 사상 초유의 일

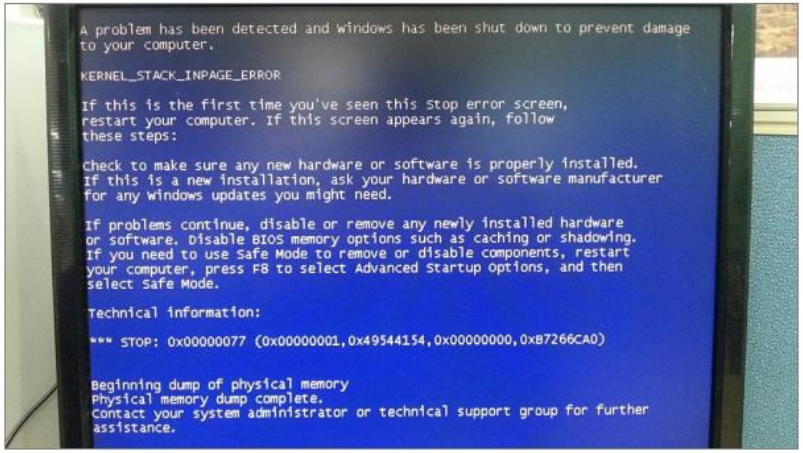
입력 : 2013-03-20 14:00:35 노출 : 2013.03.20 16:00:24 정철운 기자 | pierce@mediatoday.co.kr

AD) 누구나 마지막으로 선택하는 베개-배니굿 아치 필로우

KBS와 MBC, YTN이 오후 2시 이후 원인을 알 수 없는 해킹 공격을 당했다.

현재 KBS에선 데스크탑과 노트북을 사용할 수 없다. 인터넷도 안 되고 부팅도 안 되는 상황이다. MBC는 여의도 사옥과 일산 드림센터 모두 인터넷 사용을 할 수 없는 상황이다.

KBS는 현재 사내 안내방송을 통해 컴퓨터를 끄고 랜선을 뽑으라고 지시하고 있다. KBS 관계자는 "해킹당한 것처럼 도스 창이 몇초간 뜨다가 나가버린다"고 밝혔다. KBS와 MBC는 정확한 사고 원인을 조사중이다. YTN 또한 2시 30분 경 속보를 통해 전산망이 마비되었다고 밝힌 상황이다.



MBC 한 사무실의 컴퓨터가 작동되지 않고 있다.

- 보도일자 : 2013. 03. 20.
- 발생일자 : 2013. 03. 20.
- 인지경위
  - PC의 운영불가
- 보도경위
  - PC의 운영불가
- 수사착수 경위
  - PC의 운영불가

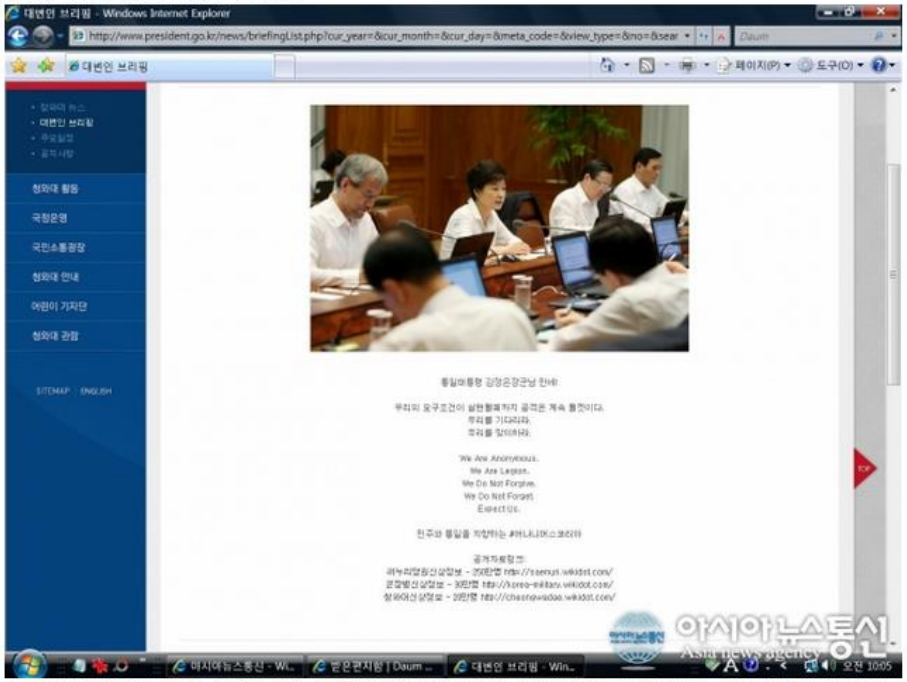
사건사고 인지경위

2013. 06. 25 – 625

청와대 홈피 해킹당해

기사입력 : 2013년06월25일 10시12분

(아시아뉴스통신=김종식 기자)



25일 오전 10시 청와대 홈페이지가 해킹을 당해 통일대통령 김정은장군님 만세!라는 문구가 떠있다.(사진캡처=청와대 홈페이지)

25일 오전 10시 현재 청와대 홈페이지가 해킹을 당했다.

청와대 홈페이지를 클릭하는 순간 '통일대통령 김정은장군님 만세! 우리의 요구조건이 실현될 때까지 공격은 계속 될것이다. 우리를 기다리라. 우리를 맞이하라. We AreAnonymous. We Are Legion. We Do Not Forgive. We Do Not Forget. Expect Us. 민주와 통일을 지향하는 #어나니머스코리아'라는 문구가 떠있다.

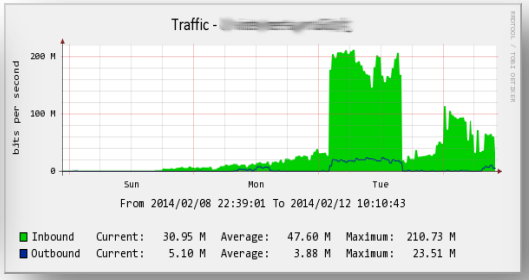
- 보도일자 : 2013. 06. 25.
- 발생일자 : 2013. 06. 25.
- 인지경위
  - 웹사이트 변조
- 보도경위
  - 웹사이트 변조
- 수사착수 경위
  - 웹사이트변조

1. DDoS 및 시스템파괴 적용법조

- 제48조(정보통신망 침해행위 등의 금지)
- ③ 누구든지 정보통신망의 **안정적 운영을 방해할 목적**으로 **대량의 신호 또는 데이터**를 보내거나 **부정한 명령을 처리**하도록 하는 등의 방법으로 정보통신망에 **장애가 발생**하게 하여서는 아니 된다.
- 5년 이하의 징역 또는 5천만원 이하의 벌금

분류	법률	내용	채증대상
누가	누구든지	직접적 인적사항 또는 추적 가능한 정보	공갈 협박 전화 또는 메일등
언제	제개정법률시행이후	공격이 시작된 일시와 종료된 일시	NMS, MRTG, DDoS방어장비등 기록, 방화벽, 전화, 메일
어디서	어디든지	공격 장소 또는 추적 가능한 정보	패킷, DDoS방어장비등 기록
무엇을	정보통신망	공격대상 컴퓨터와 네트워크	패킷, DDoS방어장비등 기록, 피해컴퓨터 HDD
어떻게	보내거나, 명령처리	대량의 데이터 전송, 시스템 중지 및 방해	패킷, DDoS방어장비등 기록, S/W c.m.d. History, 악성프로그램
왜	운영방해	공격의 이유	

인지경위별 초동조치



용의자는 2014. 03. 06. 12:10부터 같은날 12:30까지 IP주소 123.123.123.123등

35,000여대의 컴퓨터로 하여금 웹페이지 http://blahblah.com/에 대량의 데이

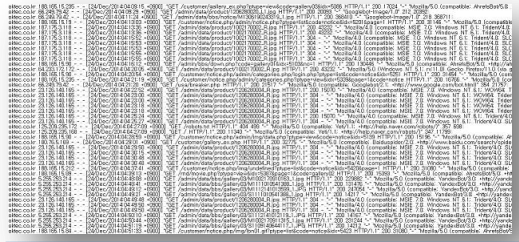
터를 전송케하는 방법으로 동 서버의 운영을 방해한 것이다.

1. 침입 및 악성프로그램 관련 적용법조

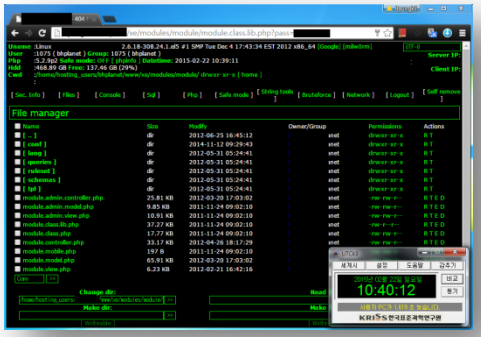
- 제48조(정보통신망 침해행위 등의 금지)
- ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.
  - ✓ 3년 이하의 징역 또는 3천만원 이하의 벌금

분류	법률	내용	채증대상
누가	누구든지	직접적 인적사항 또는 추적 가능한 정보	Wtmp, event로그등 접속기록
언제	제개정법률시행이후	접속한 일시와 종료된 일시	침입한 일시가 기재된 기록
어디서	어디든지	공격 장소 또는 추적 가능한 정보	IP주소가 기재된 로그 접속기록, 방화벽기록등
무엇을	정보통신망	공격대상 컴퓨터와 네트워크	피해컴퓨터 HDD
어떻게	접근권한이 없거나 넘어 침입	권한을 획득한 방법	웹로그, 백도어, 웹쉘등
왜	이유불문 (정당방위등 위법성조 각사유는 논외)	개인정보, 기술정보 유출등 공격의 이유는 추정만 가능	

인지경위별 초동조치



Blahblah.com 123.123.123.123 - - [06/Mar/2015:12:10:15 +0900] "GET /webshell.php "-"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET CLR 1[illegible]2; MSOffice 12)"



용의자는 **2014. 03. 06. 12:10부터 12:30까지** IP주소 123.123.123.123의 컴퓨터로 웹서버 http://blahblah.com/에 불상의 방법으로 저장된 웹쉘 webshell.php에 접속하여 권한없이 침입한 것이다.

용의자는 **2014. 03. 06. 12:00경** IP주소 123.123.123.123의 컴퓨터로 웹게시판 파일 업로드 취약점을 이용하여 webshell.php를 업로드하여 침입한 것이다.

1. 침입 및 악성프로그램 관련 적용법조

- 제48조(정보통신망 침해행위 등의 금지)
- ② 누구든지 **정당한 사유 없이** 정보통신시스템, 데이터 또는 프로그램 등을 **훼손·멸실·변경·위조**하거나 그 **운용을 방해**할 수 있는 프로그램(이하 "**악성프로그램**"이라 한다)을 전달 또는 **유포**하여서는 아니 된다.
  - ✓ 5년 이하의 징역 또는 5천만원 이하의 벌금

분류	법률	내용	채증대상
누가	누구든지	직접적 인적사항 또는 추적 가능한 정보	악성프로그램 제작 및 발송자 정보
언제	제개정법률시행이후	게시, 전달한 일시	웹로그, 메일송수신 기록 등
어디서	어디든지	유포 장소 또는 추적 가능한 정보	유포자 IP주소가 기재된 로그 접속기록, 방화벽기록등
무엇을	악성프로그램 (훼손,멸실,변경,위조, 운용방해)	악성 기능이 구현된 소프트웨어 파일	악성프로그램이 설치된 피해컴퓨터 HDD
어떻게	유포	0day 취약점, Spearphinshing	HTML소스, email원문등
왜	정당한 사유없이	내부침입, 개인정보 및 기술정보 유출등 유포의 이유는 추정만 가능	

인지경위별 초동조치

용의자는 C&C서버 234.234.234.234로 명령을 받아 하드디스크의 모든 정보를 삭제하는 기능의 악성프로그램 malware.exe를 제작한 뒤, 동 프로그램을 자동설치토록 조작된 파일 '기념행사.zip'을 제작하였다,

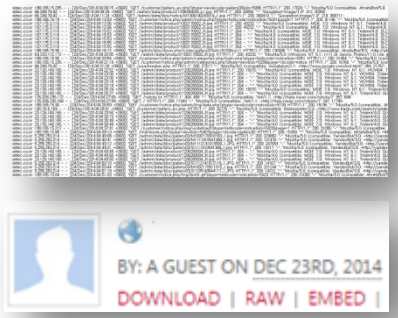
그리고 용의자는 2014. 03. 06. 12:10경 IP주소 123.123.123.123의 컴퓨터로 OOO@OOO.com계정을 통해 OOO@XXX.com등 12명에게 기념행사.zip을 첨부해 발송하는 방법으로 악성프로그램 malware.exe를 유포한 것이다

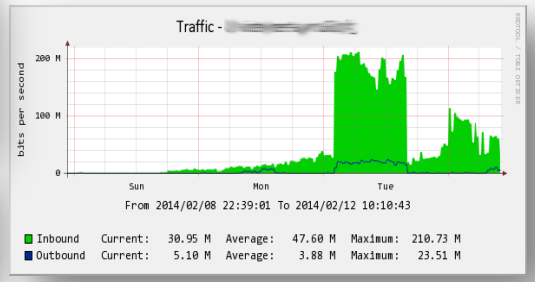
1. 내부정보유출 관련 적용법조

- 제49조(비밀 등의 보호)
- 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 **타인의 정보**를 훼손하거나 타인의 **비밀**을 **침해·도용 또는 누설**하여서는 아니 된다.
- 5년 이하의 징역 또는 5천만원 이하의 벌금

분류	법률	내용	채증대상
누가	누구든지	직접적 인적사항 또는 추적 가능한 정보	접속기록, 방화벽기록
언제	제개정법률시행이후	훼손, 침해, 도용, 누설한 일시	악성프로그램 작동일시, 유출트래픽
어디서	어디든지	유포 장소 또는 추적 가능한 정보	접속기록, C&C서버
무엇을	타인의 정보 (정보통신망에서 처리 보관전송되는)	유출된 정보 또는 삭제된 정보	피해 HDD, 유출정보 관리자 PC, 접근제한기록, DRM기록등
어떻게	정보훼손, 비밀 침해, 도용,누설	시스템의 파괴, 정보의 유출 또는 공개등	악성프로그램, DB쿼리, 웹로그등
왜	이유불문 (정당방위등 위법성조각사유는 논외)	정보의 판매, 혼란야기	

인지경위별 초동조치





용의자는 2015. 03. 06. 12:10경 ㈜OOO의 DB서버에 저장된 가입자 정보를 불상의 방법으로 지득한 아이디 sa와 암호 OOO를 이용하여 'select * from member' 명령어를 수행해 회원정보를 열람하는 방법으로 비밀을 침해하고, 같은날 12:30경 ㈜OOO의 회원정보를 인터넷 웹사이트 http://pastebin.com에 게시하는 방법으로 ㈜OOO의 비밀을 누설한 것이다.

분류	확인가능한 정보
누가	IP주소, 전화번호, 메일주소, 컴퓨터이름등
언제	모든 기록의 일시
어디서	IP주소
무엇을	악성프로그램, 침입등 피해입은 컴퓨터
어떻게	대량의 데이터 전송, 웹쉘의 업로드, 이메일의 발송, DB에 Query
왜	운영을 방해할 목적, 데이터의 유출, 악성프로그램의 유포

피의자는 신원 일체 불상의 자이다.

가. 정보통신망이용촉진및정보보호등에관한법률위반(정보통신망침해등)

피의자는 2015. 03. 06. 12:10경 불상의 장소에서 IP주소 123.123.123.123이 할당된 컴퓨터를 이용해 OOO 메인사이트의 접속권한 인증 웹페이지(URL: "http://www.OOO.co.kr/portal/Login.jsp"에 접속한 뒤, 피의자가 사전에 불상의 방법으로 지득하고 있던 관리자 아이디 'padmin'과 비밀번호 'rhksflwk 123'를 전송하여 위 아이디의 정당한 사용자인 것처럼 접속권한을 인증받는 방법으로 피해자 OOO에서 운영하는 정보통신망인 OOO 메인사이트에 정당한 권한없이 침입하였다.

피의자는 이상과 같은 방법으로 2015. 03. 06. 12:10경부터 같은날 13:40경까지 별지 **'범죄일람표1'** 기재 각 일시에, 각 기재된 IP를 할당받은 컴퓨터를 이용해 위 사이트의 접속권한 인증 웹페이지에 접속한 뒤, 각 아이디와 비밀번호를 입력하고 접속권한을 인정받아, 타인이 운영하는 정보통신망인 위 웹사이트에 모두 12회에 걸쳐 정당한 권한없이 침입하였다.

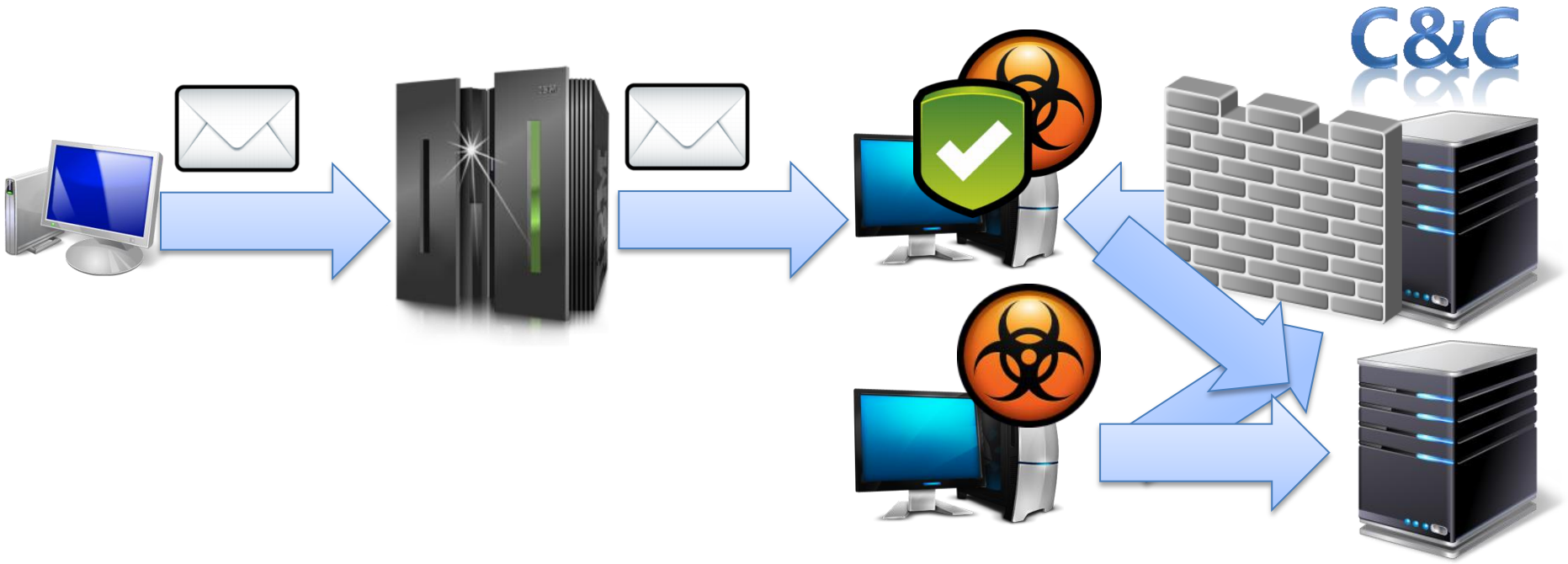
나. 정보통신망이용촉진및정보보호등에관한법률위반

피의자는 전 가항과 같은 일시 장소에서, 전 가항과 같은 방법으로 위 웹사이트에 침입한 뒤, 동 웹사이트 회원정보가 저장된 데이터베이스의 내용을 열람하거나 내려받는 기능을 가진 웹쉘 ccc.jsp등 57개를 동 웹사이트의 서버에 설치하고, 이를 이용하여 피해자 ㈜OOO의 비밀인 위 웹사이트 회원 홍길동의 성명, 아이디 'myid019', 주소 '서울 양천구 신창동 우리별아파트 102동 501호', 연락처 '010-5555-1234'등 정보를 열람하였다.

피의자는 이상과 같은 방법으로 **범죄일람표2**와 같이 2015. 03. 06. 13:02경부터 2015. 03. 06. 14:10경까지 모두 304회에 걸쳐 위 웹사이트 회원 도합 5,117,123명의 성명, 아이디, 비밀번호, 주소, 연락처등 정보를 열람하고, 이를 파일로 저장해 내려받는 방법으로 취득하여 피해자 ㈜OOO의 비밀을 침해하였다.

조사의 확대

조사의 확대

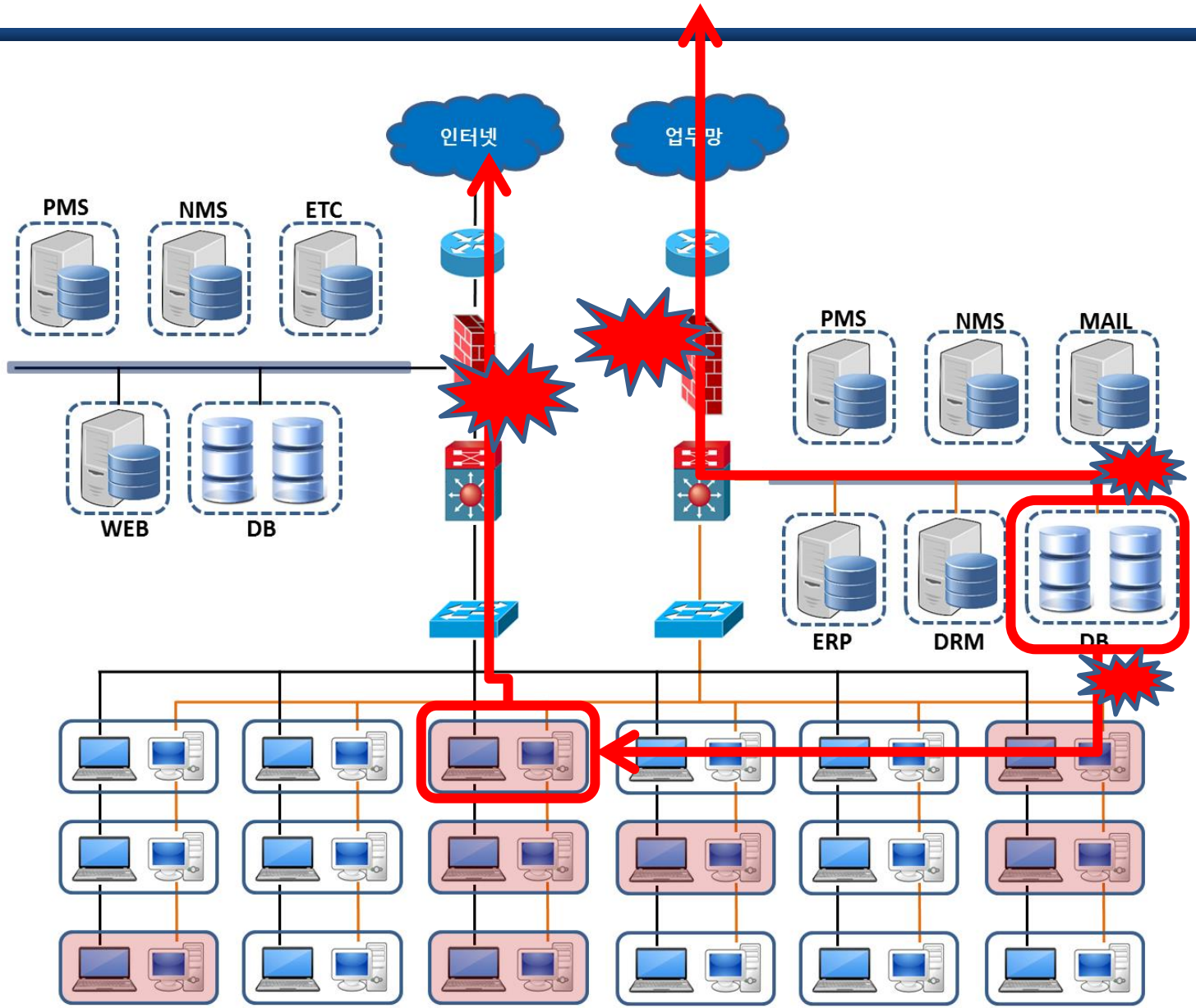


시나리오 적용

국내 언론사를 통해 회사에서 관리하는 고객정보가 중국에서 거래되고 있다는 사실을 확인하였습니다. 거래되고 있는 **고객정보를 취득**하여 확인한 결과, 인터넷망에서 관리되는 가공된 정보가 아닌 내부망에 저장된 전체 고객 정보였습니다.
급하게 내부감사를 진행한 결과, 다음과 같은 사실을 발견하였습니다.

1. 3개월 전부터 AV에 진단되는 **악성코드**가 급격하게 증가하였습니다.
2. 진단된 **PC는 모두 포맷**하여 위협을 제거해왔습니다.
3. 악성 링크가 포함된 **스피어 피싱 메일**이 5개월 전 45명의 직원에게 전달되었습니다.
4. 악성 링크의 클릭 여부를 조사해 보았으나 대부분의 직원이 오래전 일이라 기억하지 못하였습니다.
5. 평소 AV 실시간 감시만 수행하여 이번을 계기로 정밀 검사를 수행한 결과, 인터넷망(애드웨어 66건, 트로이목마 5건, 봇 12건)과 내부망(애드웨어 10건, 트로이목마 5건)에서 다수의 **악성코드가 발견**되었습니다.

시나리오 적용



시나리오 적용

1. 취득 가능한 전자적 정보 선별

- 피해 사실과 기 조사된 내용 청취
- 초동조치의 시작은 전산망 구조 파악에서 부터..
- 유효한 정보를 보관하고 있는 보안장비를 특정

2. 채증

- 악성프로그램 (애드웨어, 트로이목마, 봇등)
- Spearphishing mail 원문 (수신자 45명에 대한...)
- 악성프로그램이 진단된 기록과 피해PC의 하드디스크 이미지 (수신자 45명 포함)
- 방화벽로그, 접근제한장비 로그, DB쿼리기록, MRTG등 트래픽정보

3. 1차 분석과 확정 검색

- 회원정보가 유출되었을 기준시간 특정
- 악성프로그램이 통신하는 C&C IP주소를 파악

4. 2차 채증 및 채증자료의 분석

1. 메일서버와 피해자PC 이미지로 보아, 용의자는 2014. 10. 21. 10:45경 suspect@gmail.com으로 읽어봐.hwp를 첨부하여 직원 45명에게 발송하였다.

2. 악성프로그램을 분석한 결과, 읽어봐.hwp를 열람하면 1차 C&C 123.123.123.123으로 접속하여 추가 악성프로그램을 내려받아 설치하는 기능의 악성프로그램 taskmgr.exe가 설치된다.

3. 방화벽 기록으로 보아, 내부망 업무용 컴퓨터 중 120대가 123.123.123.123에 접속한 사실이 확인되었다.

4. 추가로 확인된 PC를 분석한 결과, 용의자가 발송한 전자우편을 추가로 3종 확인하였다. 이로서 4종의 이메일로 지원 200명이 수신한 사실이 확인되었다.

5. 좀비PC 120대를 분석한 결과, 2차 C&C 234.234.234.234로 접속하는 Gh0st RAT을 1차 C&C에서 내려받아 설치된 사실을 확인하였다.

6. DB 접근제한 기록으로 보아, 좀비PC 120대 중 1대인 DB admin의 PC에서 점심 시간 동안 DB를 덤프받은 사실이 확인되었다.

7. 방화벽기록으로 보아, 2014. 11. 01. 12:15경 DB admin의 PC에서 IP주소 111.111.111.111로 접속해 4Gbyte의 내용이 전송된 사실이 확인되었다.

8. DB admin의 PC 이미지에서 회원정보가 압축되어 삭제된 내역과 htran, arpstorm등이 확인되었다.

용의자는 성명불상으로 인적사항이 특정되지 않은 자이다.

용의자는 OO기관에 침입하고 회원정보등을 유출할 목적으로 악성프로그램 유포를 마음먹었다. 이를 위해 IP주소 234.234.234.234에 접속하여 원격제어를 받도록 Gh0stRAT 설치파일 svchost.exe(MD5해쉬값 BA4EE95E17750D9ACE306A134A5FF6AB)을 제작하였다.

그리고, 디지털포렌식커뮤니티 웹페이지 “http://forensicinsight.com/login.php”에 접속하여 Gh0stRAT 악성프로그램을 추가로 내려 받는 기능을 가진 악성프로그램 taskmgr.exe(MD5해쉬값 6E76CDEBB442FF816A09ADFB6F5F1AC8)을 제작하였다. 이후, 악성프로그램 taskmgr.exe가 자동설치되도록 조작된 ‘읽어봐.hwp’등 파일을 제작하여 범행할 준비를 마친 뒤,

가) 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보

통신망에 침입하여서는 아니 됨에도 불구하고

용의자는 일시불상경 장소불상지에서 악성프로그램 taskmgr.exe가 설치된 좀비 PC를 제

어하는 1차 C&C기능의 웹페이지 “http://forensicinsight.com/login.php”를 설치하기 위

하여 불상의 방법으로 디지털포렌식커뮤니티 포렌식인사이트 서버에 침입하였다.

나) 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 “악성프로그램”이라한다)을 전달 또는 유포하여서는 아니 됨에도 불구하고

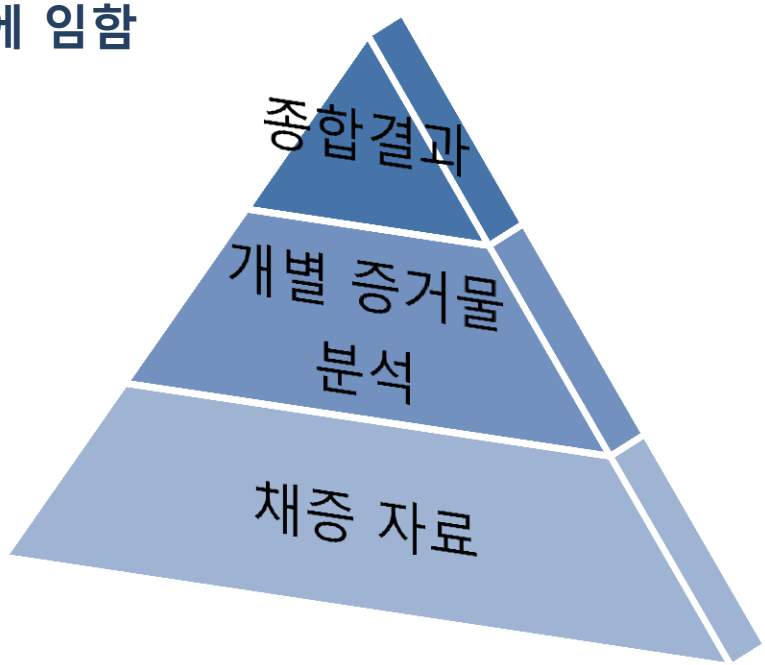
용의자는 2014. 10. 21. 10:45경 불상지에서 이메일 아이디 suspect@gmail.com으로 제목을 “병길아 신입포함 동문명단이다.”로 작성하고, 내용을 “다음주 토요일에 신입 환영회 계획이야 읽어보고 알려줘..”로 작성하고, 악성프로그램 '읽어봐.hwp'를 첨부하여 완성된 전자우편을 casestudy@OOO.com에게 발송하여 악성프로그램을 유포하는 등, 별첨 범죄일람표와 같이 2014. 10. 21. 124차례에 걸쳐 200명에게 악성프로그램 악성프로그램을 유포한 것이다.

다) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 됨에도 불구하고,

용의자는 2014. 11. 01. 12:15경 불상지에서 IP주소 234.234.234.234가 할당된 컴퓨터를 이용하여 ㈜OOO의 데이터베이스 관리자 홍길동의 PC를 원격제어하며 데이터베이스서버 OOOO에 접속해 동 회사의 회원정보인 이름, 아이디, 주소, 전화번호등이 저장된 user데이터베이스의 member 테이블의 홍길동등 2,000만명의 개인정보를 동 컴퓨터로 내려받은 뒤, IP주소 111.111.111.111로 전송하는 방법으로 동 회사의 비밀을 침해한 것이다.

Executive Summary

1. 신속한 의사결정을 위한 정확한 조사
2. 범죄이므로 기소(수사)를 염두하고 조사에 임함
3. 증거능력이 확실한 자료를 풍부히 확보
4. 빠짐없는 조사
5. 탄탄한 논리의 결과보고



Question and Answer