온라인 상거래 이상징후 대응 방안

2014.04.24

장현국

솔루션본부 솔루션사업팀 SI파트장

Infosec | SK C&C

인터넷 뱅킹 서비스 해킹

은행 인터넷뱅킹 시스템이 해킹당해 거액의 예금이 고객 몰래 인출되는 사건이 발생했다.

비밀번호 단순도용 사건이 존재했으나 인터넷뱅킹 시스템 자체를 해킹해 돈을 빼돌린 것은 이번이 첫 사례다.
특히 안전의 보루처럼 여겨졌던 보안카드도 '안전지대' 가 아닌 것으로 드러나 대비책 마련이 필요하다는 지적이다.
또한 범죄에 사용된 해킹프로그램은 인터넷 파일공유 사이트에서 쉽게 다운받을 수 있는 것이어서 유사범죄 발생도 우려되고 있다.

서울경찰청 사이버범죄수사대는 3일 해킹프로그램을 통해 인터넷뱅킹 비밀번호 등을 알아낸뒤 은행 계좌에서 거액을 인출한 이모씨(20) 등 2명에 대해 컴퓨터 등 사용사기 혐의로 구속영장을 신청했다.

경찰은 또 이들이 불법으로 빼낸 돈을 이체할 통장을 만들어준 후배 김모군(17) 등 2명을 불구속 입건했다.
경찰에 따르면 이씨 등은 인터넷 재테크 게시판에 글을 올린뒤 상대방이 이를 접속하면 상대방 컴퓨터에 해킹프로그램이 자동적으로 설치되도록 하는 '넷 XX(Net XXXXX)' 이란 프로그램을 이용했다.
있다"고 말했다.

- 경제신문 : 2005/06/03

해커가 온라인 은행계좌 제어

북경뉴스, 국가 컴퓨터바이러스 응급처리센터 알림 :

새로운 악성목마 프로그램이 개인 인터넷은행의 계좌번호와 패스워드를 도둑질 하고 있다. 일전에 공상은행 IT부 전문 담당자는 잠시 공상전자은행 "고객증서U" 를 신청하지 말고 사용자들은 자신의 인터넷은행 패스워드를 새로 설정하는 것이 좋을 것이라고 건의하였다.

2006년에 접어들면서, 홈페이지 바이러스와 트로이목마 바이러스를 이용해 계좌번호와 패스워드를 도둑질 하는 인터넷 은행 관련 해킹 사건들이 많이 일어나고 있다. 이들은 인터넷 은행에 접근한 다음 네트워크를 통해 인터넷 상에서 계좌이체를 하는 등의 방법으로 현금을 도둑질 하고 있는데, 이는 해커들이 돈을 획득하는 새로운 경로가 되고 있다.

요즘, 모 은행의 인터넷 은행 사용자들이 연속으로 거금을 도난 당하는 사건이 발생하였다. 현재까지 북경, 남경, 항주, 합비 등 10여개 도시 70여명의 사용자들이 피해를 당하였고 그 금액은 30만원(한화 약 3900만원)에 달한다. 그전에 이미 호남성 경찰은 인터넷 은행 전문강도집단을 체포한적이 있었다. 이 집단은 1000개가 넘는 은행계좌번호를 제어하고 있었으며, 그 금액은 40여 만원(한화 약 5200만원)에 달하였다.

- 중국 하남성 상업신문 : 06-07-07

악성코드 활용 해킹

온라인뱅킹 역사상 최대로 보이는 약 580,000 파운드(한화로약 10억원)의 보안사고가 스웨덴의 Nordea은행에서 발생

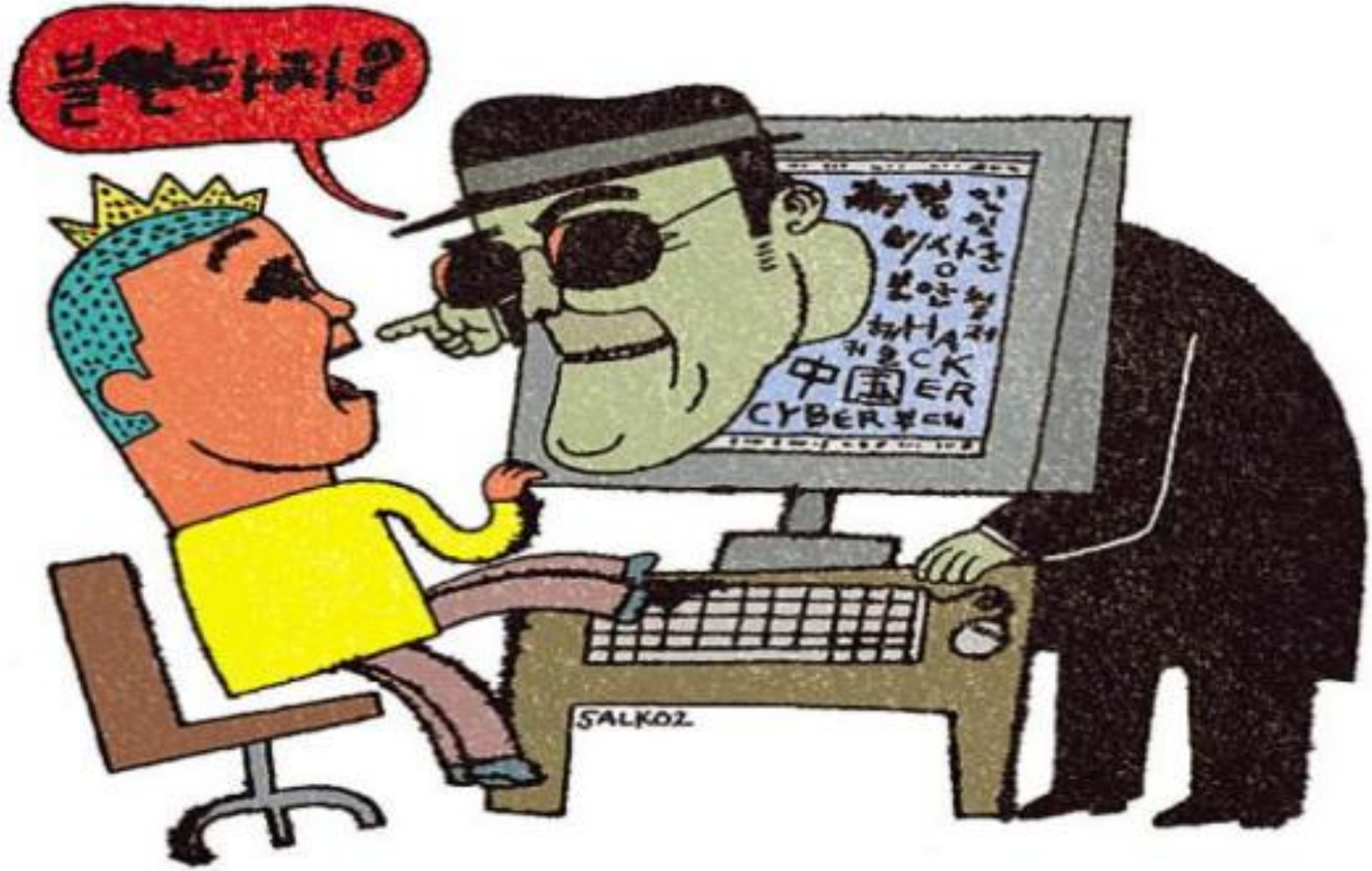
□공격자가 약 15개월 전부터 고객들을 대상으로 악성 코드(Trojan)가 첨부된 이메일이 발송되었으며,약 250명의 고객이 감염이 된 것으로 Nordea은행은 판단하고 있음
※Nordea은행은 약 200만명의 인터넷뱅킹 고객을 보유하고 있음

□악성코드가 첨부된 메일은 은행에서 보낸 것처럼 위장되어 고객들에게 보내어졌고 메일의 내용에는 고객들이 메일에 첨부된 "스팸차단 프로그램 "을 설치하라는 내용으로 되어 있었음

□raking.zip(또는 raking.exe)라는 첨부파일을 실행한 사용자들은 haxdoor.ki라는 악성코드에 감염이 되어 컴퓨터에서 키보드 입력 값들을 가로챘으며 위조된 Nordea 온라인 뱅킹사이트로 접속하도록 하여 중요한 로긴정보 등을 입력하도록 했음

□한편 은행은 이 사고로 인해 피해를 입은 고객들에게 모두 보상해주었음

- 금융보안 주간동향(금융보안연구원) : 07-01-29


HACK
中国
CYBER
SALKOZ

온라인 상거래 보안 적용 기능

온라인상거래
서비스 이용자

키보드 해킹 방지 프로그램
(계좌/공인인증서 비밀번호 입력 보호)

공인인증서
(본인부인방지 등 이용자 본인 증명)

암/복호화 프로그램
(전자금융거래 데이터 암호화)

백신 프로그램
(바이러스/웜/악성코드 차단)

목차

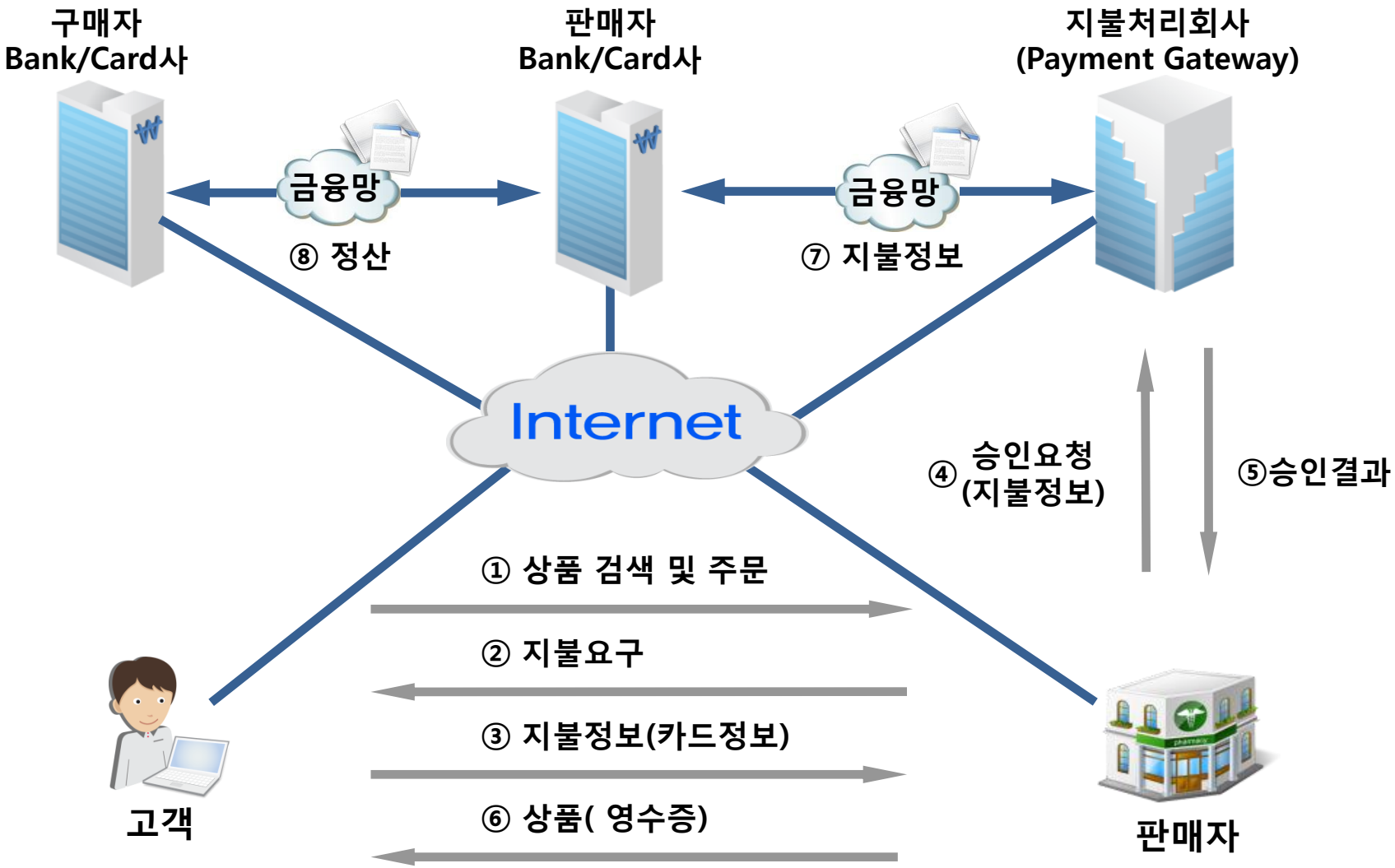
Contents

온라인상거래 이상징후 대응 방향

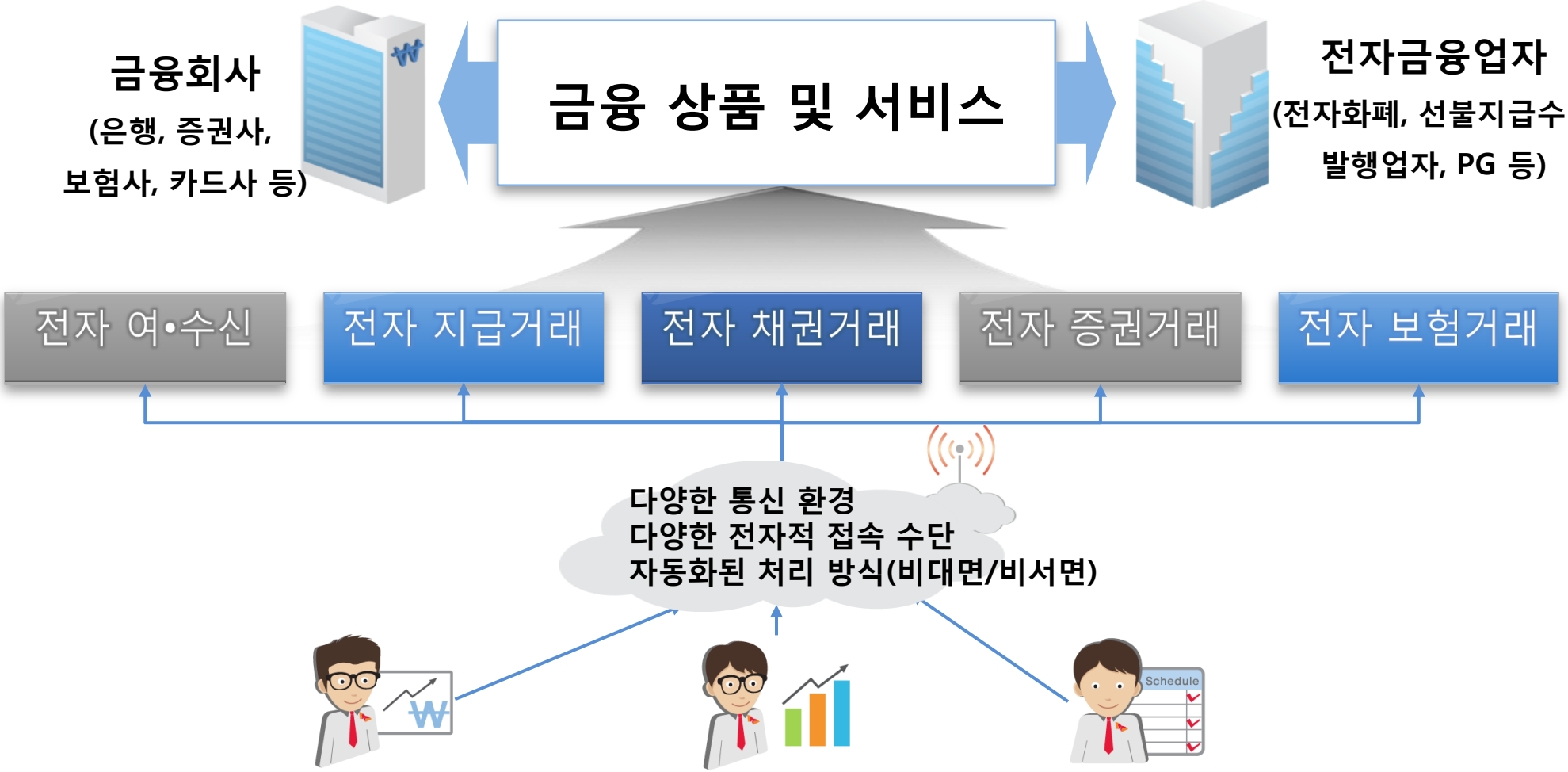
1. 온라인 거래란?

구 분	정 의	대상 서비스
전자상거래	공급자와 구매자간의 상호 전자적 수단을 통해 거래하는 행위	온라인 쇼핑몰, 월과금/내부구매 가능 게임서비스 등
전자금융서비스	전자적인 수단으로 화폐의 이동이 이루어지도록 지원하는 서비스	온라인 뱅킹, 온라인 주식 거래, 대금 납부 진행하는 지로서비스 등

1. 온라인 거래란?


구매자
Bank/Card사
판매자
Bank/Card사
지불처리회사
(Payment Gateway)
금융망
⑧ 정산
금융망
⑦ 지불정보
Internet
④ 승인요청
(지불정보)
⑤승인결과
① 상품 검색 및 주문
② 지불요구
③ 지불정보(카드정보)
⑥ 상품(영수증)
고객
판매자

1. 온라인 거래란?


금융회사
(은행, 증권사,
보험사, 카드사 등)
금융 상품 및 서비스
전자금융업자
(전자화폐, 선불지급수단
발행업자, PG 등)
전자 여•수신
전자 지급거래
전자 채권거래
전자 증권거래
전자 보험거래
다양한 통신 환경
다양한 전자적 접속 수단
자동화된 처리 방식(비대면/비서면)
₩
Schedule

1. 온라인 거래란?

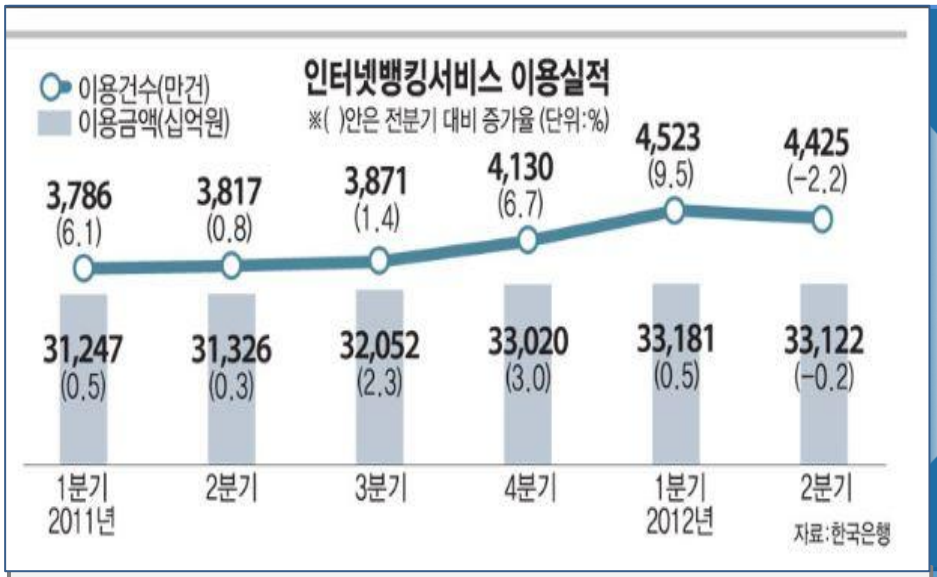
전자 상거래 규모

- ㅇ 규모: 년간 1144조7000억원
- ㅇ 증감내용: 2011년대비 14.5%증가
- ㅇ 주요 거래내용
  - B2B: 91.8%(1050조9850억원)
  - B2G: 5.4%
  - B2C+C2C: 2.7%

- ㅇ 규모: 년간 32조3470억원
- ㅇ 증감내용: 2011년대비 11.3%증가
- ㅇ 주요 거래내용
  - 여행 및 예약 서비스: 32.3%
  - 생활/자동차 용품: 17.1%
  - 가전/전자/통신기기: 10.0%

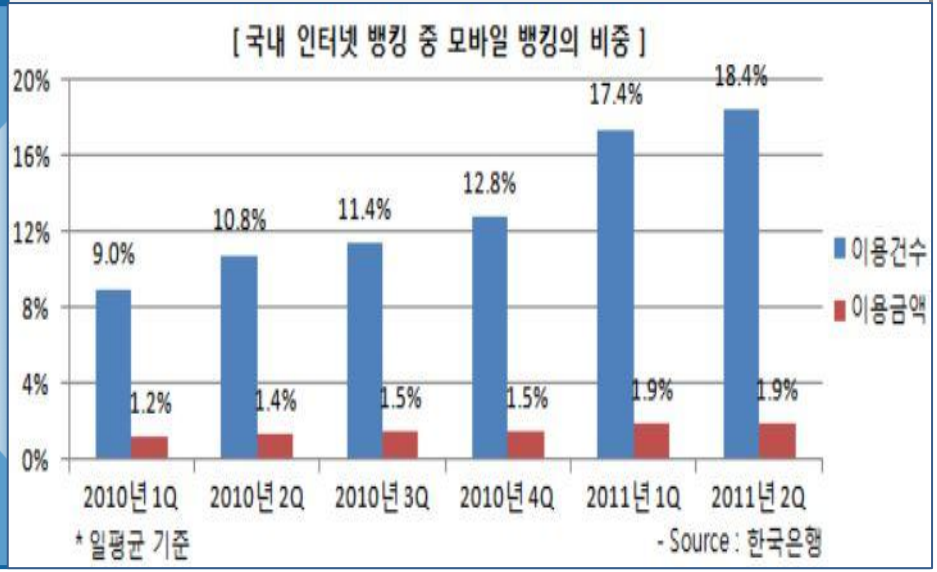
1. 온라인 거래란?

전자금융 서비스 규모



ㅇ 규모: 일평균 1조4192억원(2230만건)
ㅇ 증감내용: 2011년대비 8.5%증가

ㅇ 규모: 일평균 1조3723억원(2224만건)
ㅇ 99.7%이용자가 모바일뱅킹



진화되는 악성코드 침해

최근 금융당국은 전자금융사기 피해를 줄이기 위해 100만 원 이상 이체 시 추가 인증(2채널 인증) 절차를 거치도록 보안을 강화했다. 하지만 이를 우회하는 악성코드가 발견되어 마냥 안심할 수 없는 상황이 됐다.
한국인터넷진흥원(KISA)가 지난 2013년 9월부터 7개월간 악성코드 은닉사이트 탐지 시스템을 통해 탐지된 악성코드를 분석한 결과, 최근 악성코드가 기존 PC 인터넷 뱅킹을 노리는 파밍(Pharming)에 스마트폰의 금융정보를 노리는 큐싱(Qshing)을 결합한 형태로 진화하고 있는 것으로 확인되었다.

▲ 이미지 출처 : SKB 공식 블로그

파밍은 악성코드에 감염된 PC를 조작해 이용자가 금융회사 등의 정상적인 홈페이지 주소로 접속했음에도 가짜 사이트로 유도해 개인 금융 정보 등을 몰래 빼가는 수법을 말하며, 큐싱은 QR코드와 개인정보, 금융정보를 낚는다((Fishing)는 의미의 합성어로, QR코드를 통해 악성 링크 접속을 유도하거나 직접 악성코드를 심는 방법이다.
악성코드에 감염된 PC에서 사용자가 정상 금융 사이트에 접속하면, 가짜 금융 사이트로 연결된다. 여기에 해커는 사용자 스마트폰까지 악성코드에 감염시키기 위해 QR코드로 추가 인증을 유도한 후, QR코드에 저장된 인터넷 주소를 사용해 악성 앱 설치를 하게끔 한다.
설치된 악성 앱은 전화번호, 문자메시지 등 정보를 탈취하고, 문자 수신 방해, 착신 전환 서비스 설정 등을 시도할 수 있는 것으로 분석되었다. 현재는 착신 전환 설정이 홈페이지나 매장 방문을 통해서만 신청할 수 있지만, 이러한 방식을 악용한다면 전자금융거래 자금 이체 시 SMS, ARS 등 추가 인증을 우회하여 금융사기에 악용될 수 있을 것으로 보인다.

진화되는 온라인 거래 침해

中, 공용 와이파이 보안위협 현실화...69번 인터넷뱅킹 도용 사고 발생

"안녕하세요. 여기WiFi비밀번호가 어떻게 되죠?" 많은 이들은 공공장소에서 스마트폰, 노트북들을 이용해 인터넷에 접속하게 된다. 보안전문가의 조사에 따르면 대다수 공공장소의 무료 와이파이는 보안방어 조치가 부족하며, 또한 해커가 자체적으로 구성한 "가짜 와이파이"일 경우가 많은 것으로 밝혀졌다.

이는 계정, 패스워드 절취, 개인정보 유출, 인터넷 뱅킹 도용 등 심각한 결과를 초래한다.

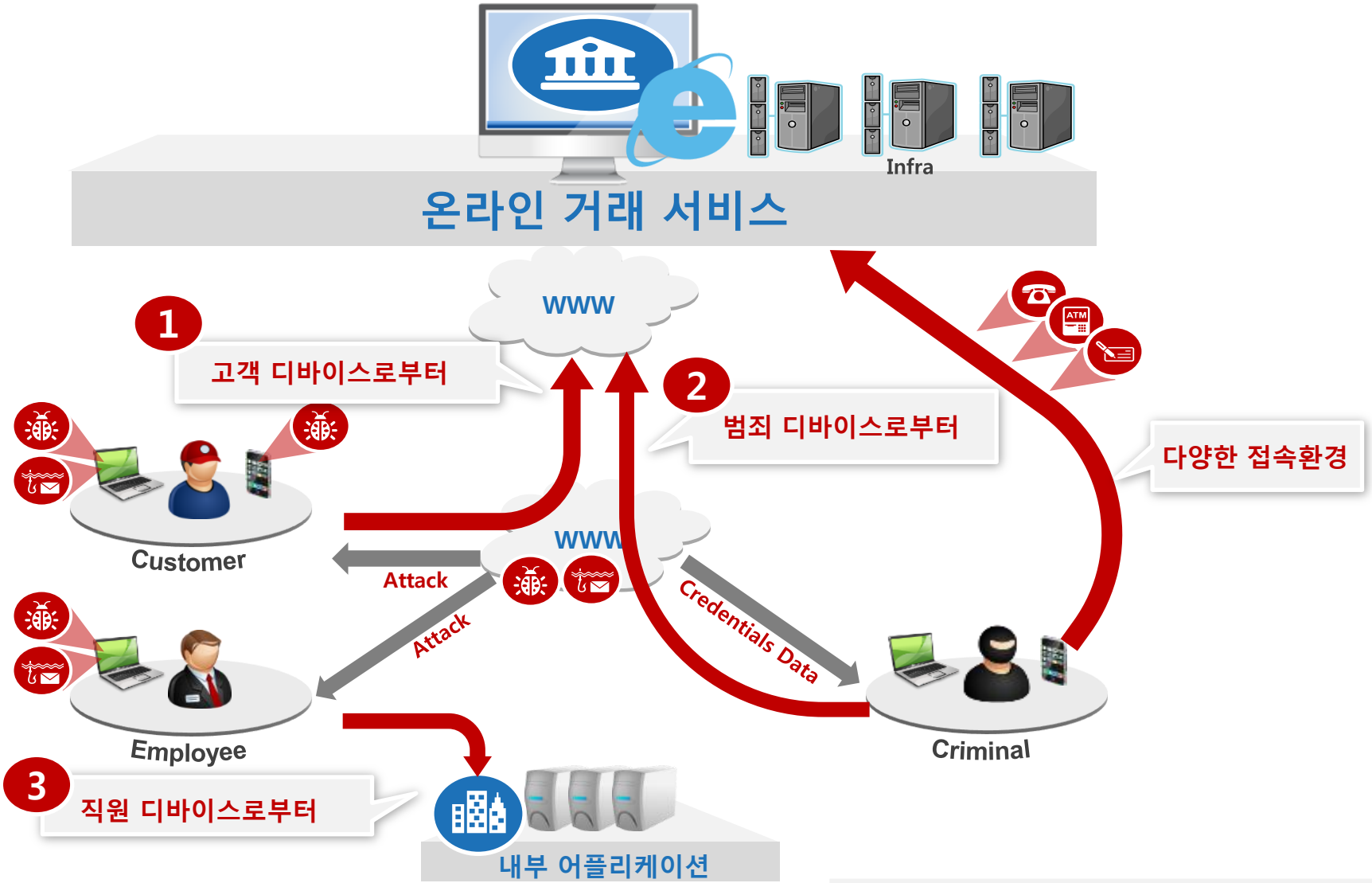
최근 중국 난징에 거주하는 장씨는 공공장소 와이파이를 사용한 후 노트북이 해커에게 침입당해 인터넷뱅킹 상의 잔고 6만 위안이 2일 사이에 500위안만 남게 된 것을 발견했다. 그의 보안USB, 은행 카드가 모두 본인한테 있었으며, 계정도 휴대폰 메시지와 연동했고, 패스워드도 절취 되지 않았지만 카드는 69번이나 도용된 것으로 조사됐다. 이 사건 조사에 따르면, 장씨의 돈은 서드파티 지불 플랫폼에 의해 인출 된 것으로 나타났다. 그의 휴대폰도 해커에게 제어당해 메시지 수신 기능이 차단되었기에 69번의 거래를 확인 할 수 없었던 것이다.

대부분 사용자는 무료 와이파이의 보안 위협에 대해 인식하지 못하고 있다. 많은 사용자들은 무료 와이파이가 안전하지 못하다는 것을 알지 못한다. 와이파이에 접속 할 때에는 일반적으로 보안을 고려하지 않으며, 대부분 스마트폰에는 자동접속 기능이 존재해 자동적으로 무료 와이파이에 접속하게 된다.

2. 온라인 거래의 위험

서비스 위협 요소와 요구되는 대응 기술

2. 온라인 거래의 위험

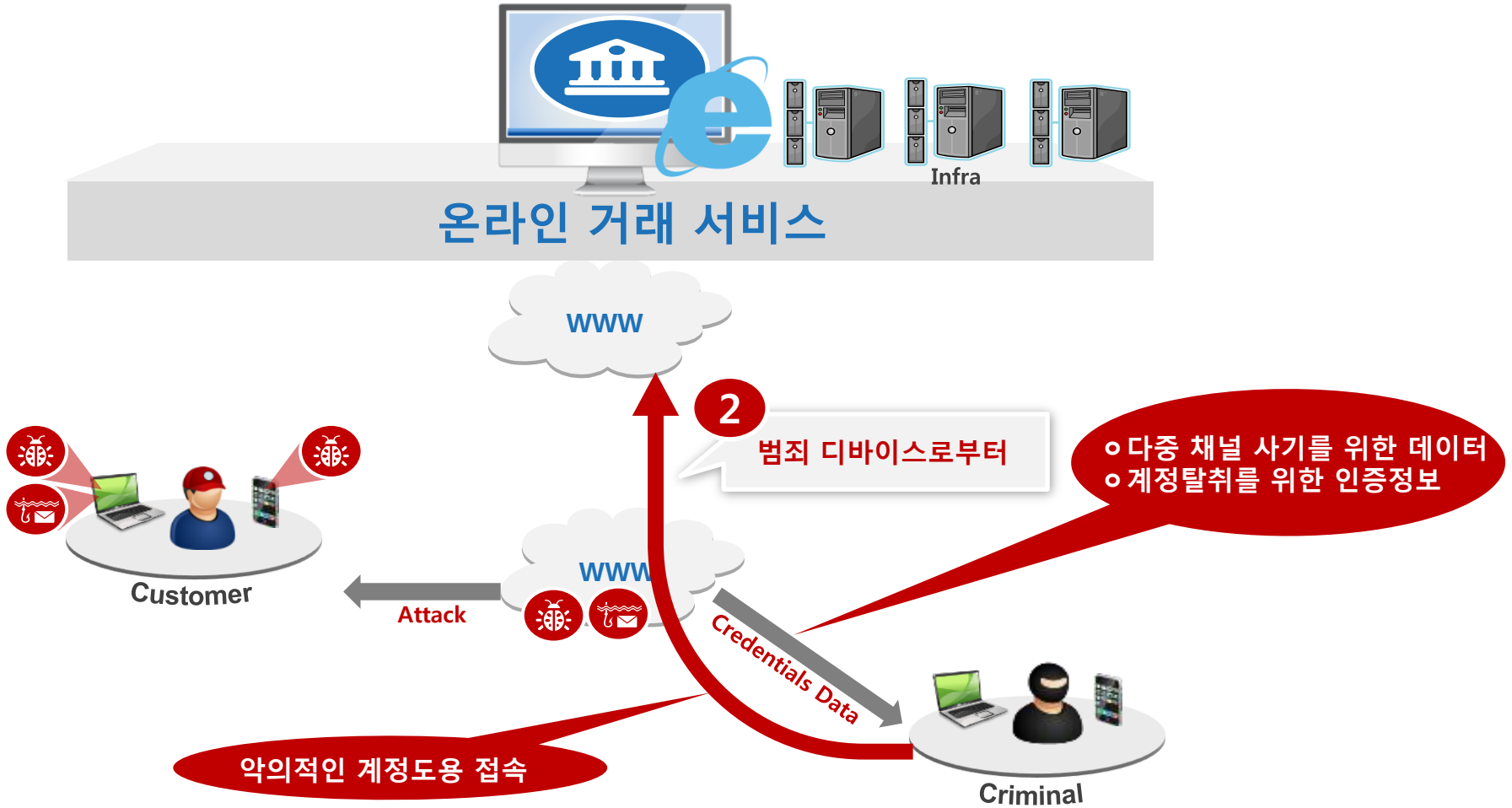

Infra
온라인 거래 서비스
www
1
고객 디바이스로부터
2
범죄 디바이스로부터
다양한 접속환경
Customer
Attack
www
Attack
Credentials Data
Employee
Criminal
3
직원 디바이스로부터
내부 어플리케이션
악성코드 설치
인증정보 피싱

2. 온라인 거래의 위험

침해된 고객 디바이스에 의한 위협

2. 온라인 거래의 위험

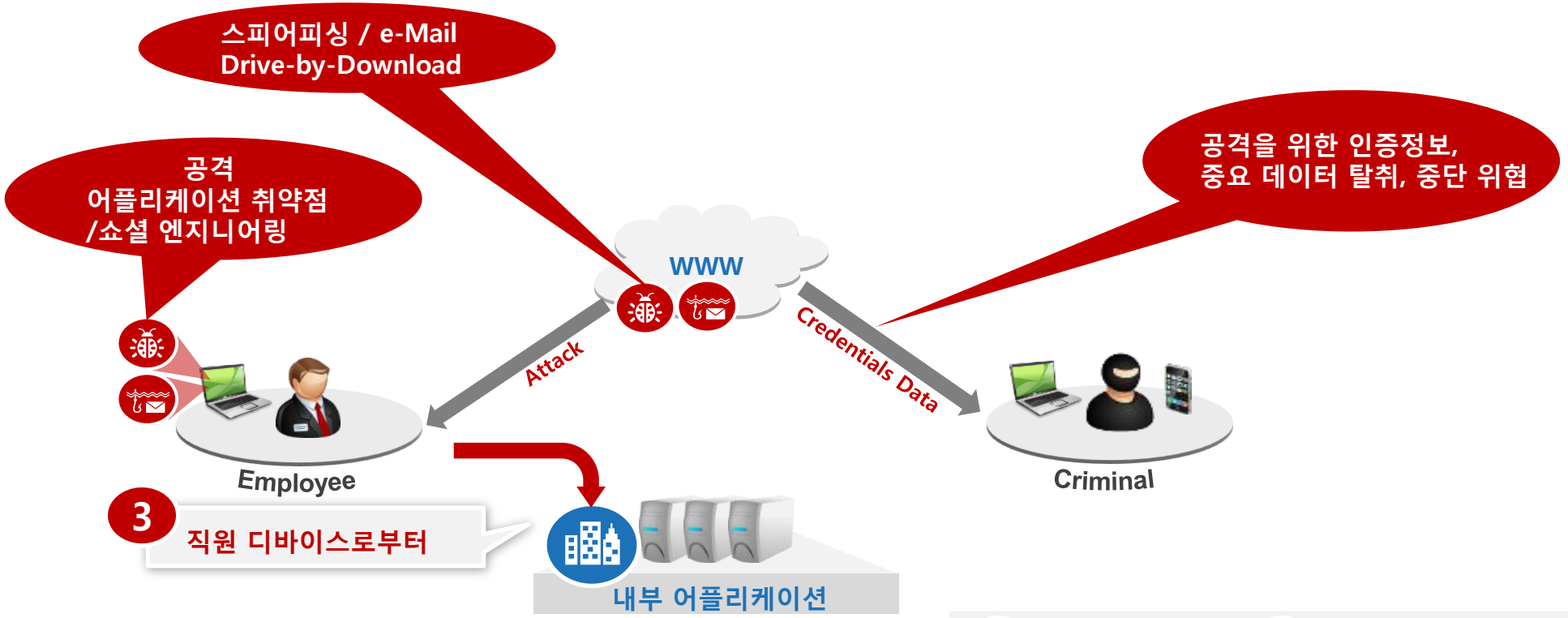
범죄 디바이스에 의한 위협



악성코드 설치 | 인증정보 피싱

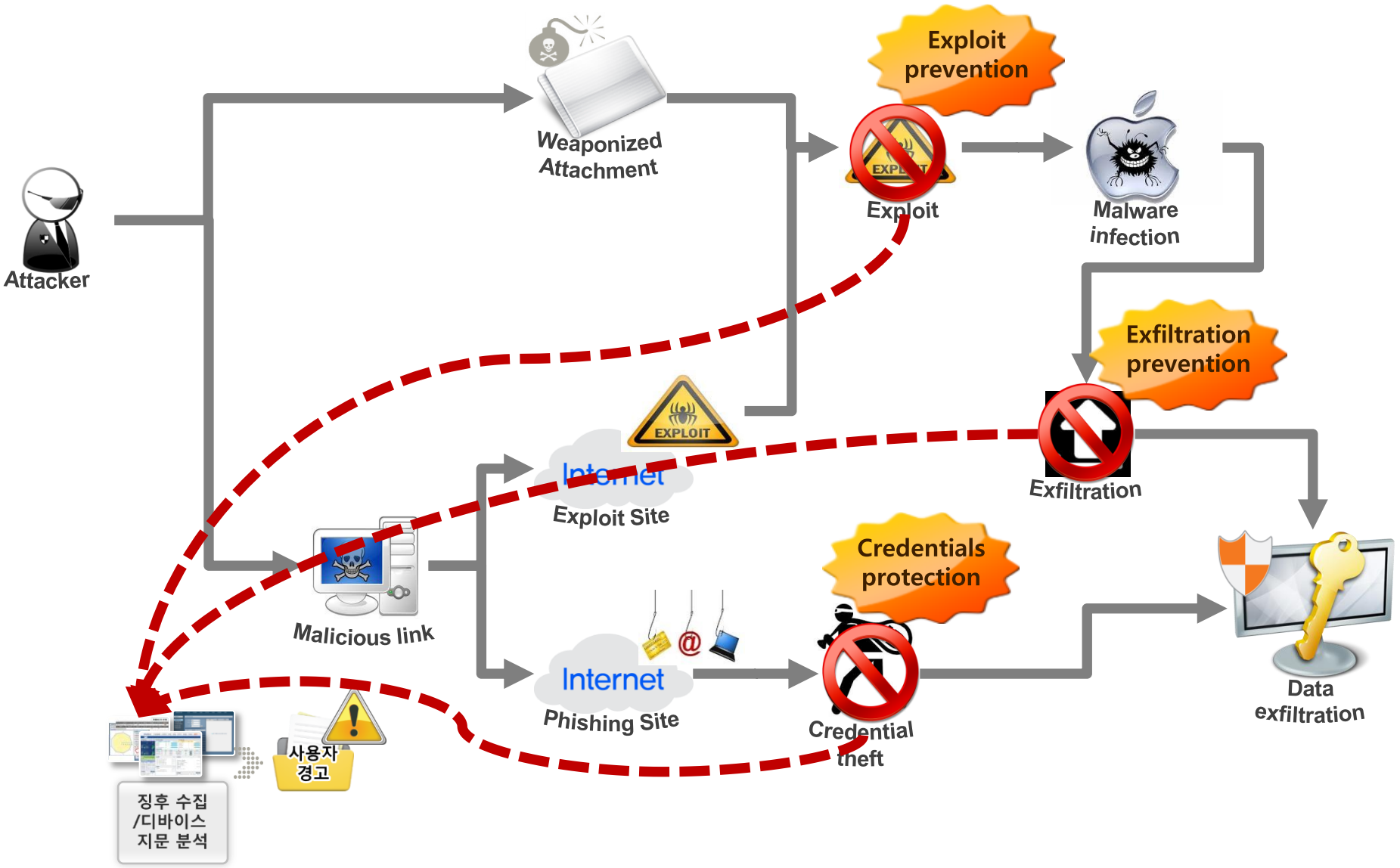
2. 온라인 거래의 위험

침해된 내부자 디바이스에 의한 위협



3. 온라인 거래 이상징후 개선 방안

Protection Point



3. 온라인 거래 이상징후 개선 방안

무엇에 대응해야 하는가?

- 알려지지 않은 공격, 악성코드 탐지 및 제거
- 피싱, 파밍, 메모리 해킹 및 브라우저 기반 공격 탐지 및 방어
- 디바이스 지문 및 위협 점수 기반 계정 탈취 여부 식별
- 악성코드 탐지와 위험분석/대응
- 사용자 PC 및 모바일 디바이스 보호: 제로데이/알려지지 않은 공격 방어
- 전자 금융 보안 : 전자 금융 관련 웹 브라우저 기반 공격 탐지 및 방어
- 모바일 보안 : 모바일 상의 위협(파밍, 악성코드, 안전하지 않은 WI-FI통신 등) 방어

어디에 적용해야 하는가?

- 엔드포인트 보안 분야 : APT 대응
- 인터넷금융 보안 분야 : 웹 브라우저 기반 트랜잭션 보호
- 모바일 보안 분야 : 모바일 위협 대응

End of Document