안드로이드 악성 앱 기반 보이스피싱

금융보안원 침해위협분석팀 장민창 과장
null@fsec.or.kr
CEAT of Financial Security Institute

About me

- 장민창 (Jang Min Chang)
  - 금융결제원 금융ISAC, 2012 ~ 2015
  - 금융보안원 침해대응부 침해위협분석팀 과장, 2015 ~ 현재
    - 보이스피싱 악성 앱 프로파일링 (Shadow Voice)
  - 고려대학교 정보보호대학원
    - 사이버전 전공 (M.S degree)
  - 다수의 국제컨퍼런스 발표
    - CODE BLUE, black hat ASIA, black hat EU

black hat EUROPE 2017 DECEMBER 4-7, 2017 EXCEL / LONDON, UK

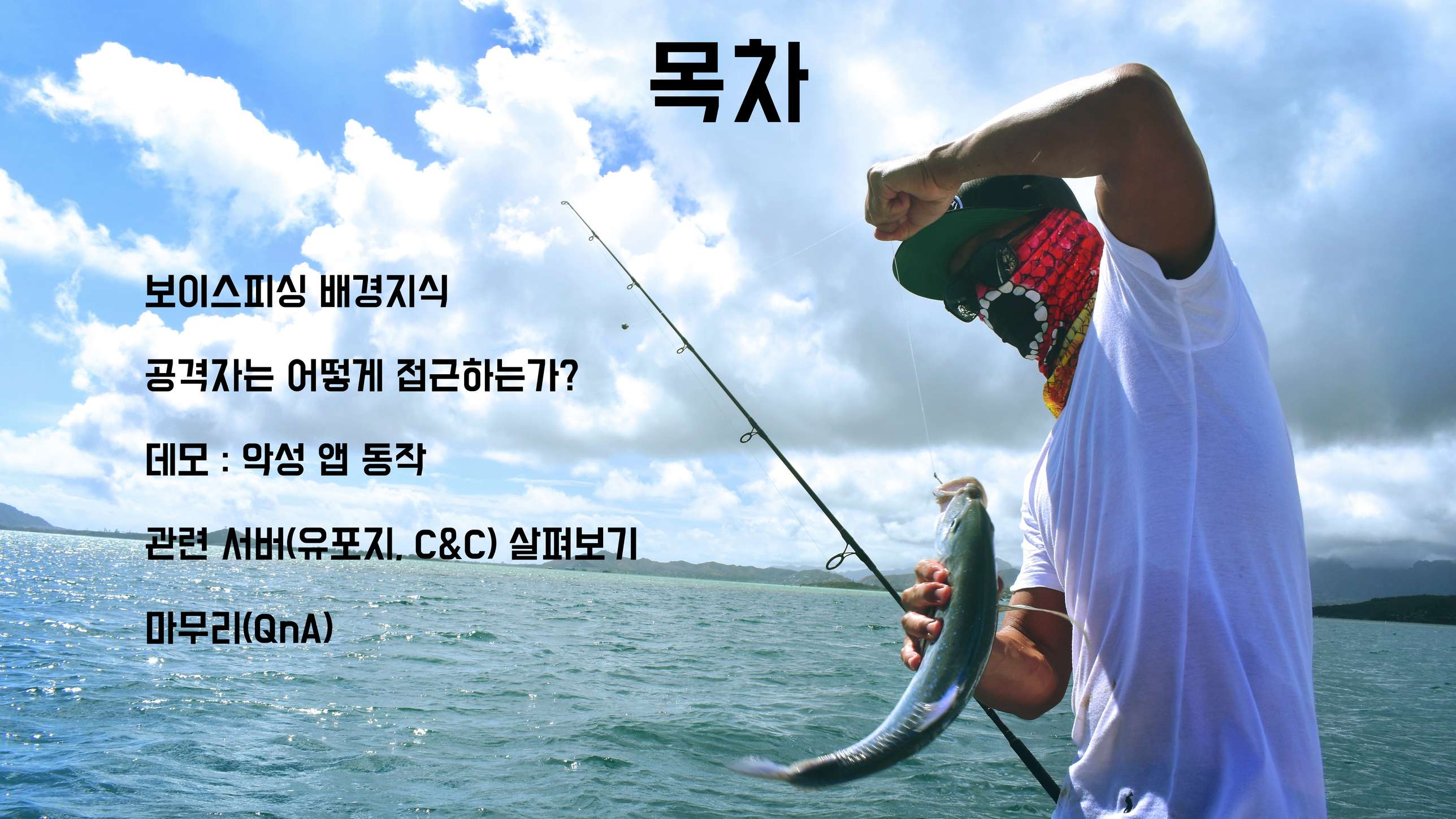
black hat ASIA 2018

CODE BLUE 2018 @TOKYO

black hat ASIA 2019

금융보안원 FINANCIAL SECURITY INSTITUTE

목차



보이스피싱 배경지식

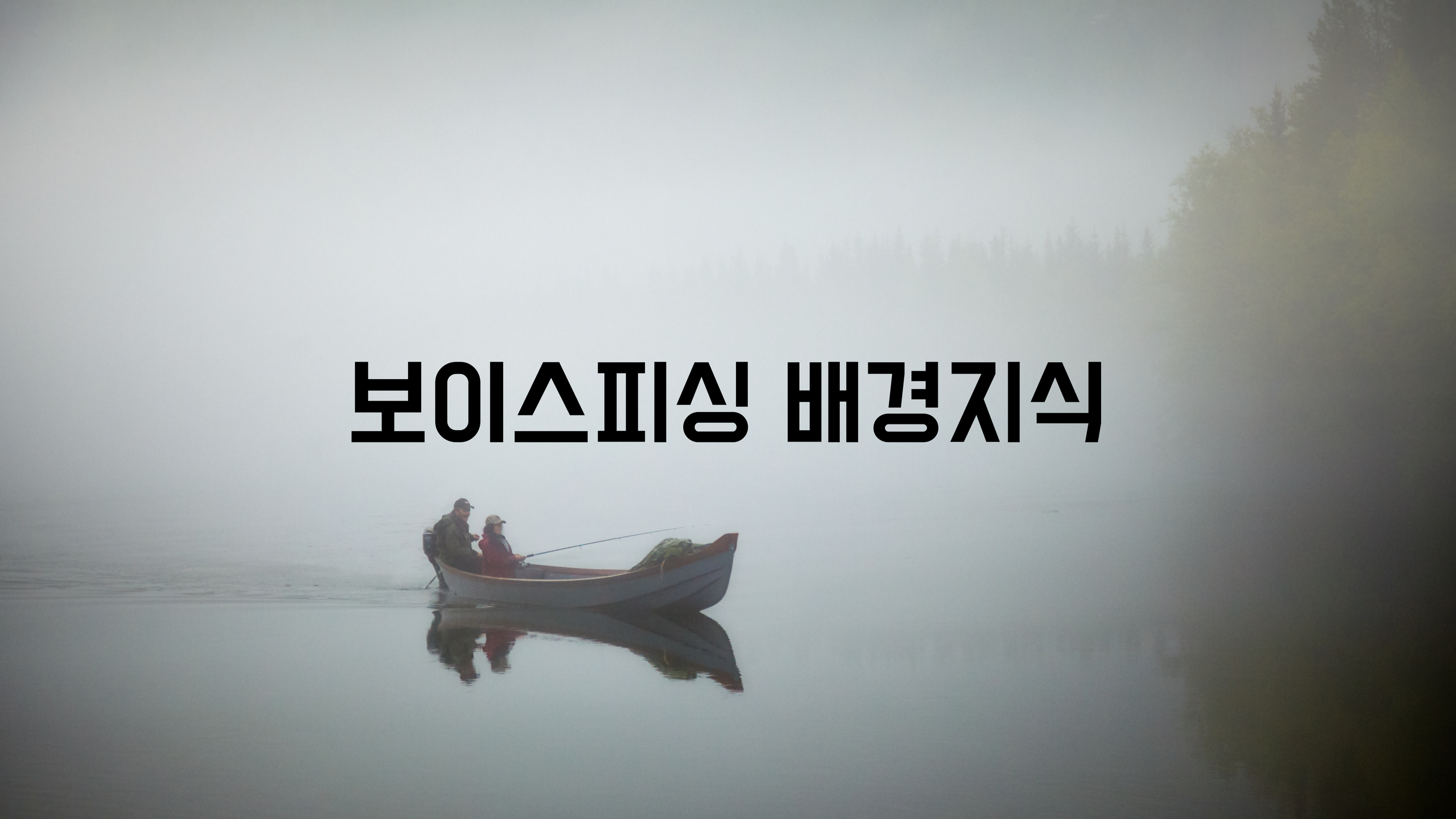
공격자는 어떻게 접근하는가?

데모 : 악성 앱 동작

관련 서버(유포지, C&C) 살펴보기

마무리(QnA)

보이스피싱 배경지식



"보이스 피싱" 이라고 하면 무엇이 가장 먼저 떠오르시나요?

보이스피싱(Voice Phishing) 오픈사전 ?

T

이 단어는 이용자들이 직접 참여하여 작성하였습니다.

흔히 전화금융사기단 으로 일컬어지는 보이스피싱은
음성(voice)과 개인정보(private data),낚시(fishing)를 합성한
신조어로 전화를통해 불법적으로 개인정보를 빼내서 사용되는 신종범죄이다.

- 잇단 '보이스 피싱'…개인정보 유출 주의

전기통신금융사기

위키백과, 우리 모두의 백과사전.

전기통신금융사기(電氣通信金融詐欺) 또는 **보이스 피싱**(voice phishing)은 범행 대상자에게 전화를 걸어 허위 사실을 이야기하고, 송금을 요구하거나 특정 개인정보를 수집하는 사기 수법을 말한다.


연예 수첩
"성대모사는 이렇게!"
아... 당황은 안 하셨구나

"김미영 팀장"


오후 6:00
39%
메시지
010-7217
편집
2010. 8. 26. 오전 9:41
김미영팀장입니다고객님께서는최저이율로최고3000만원까지30분이내통장입금가능합니다
2010. 8. 27. 오후 5:57
미영이 누나 사랑해요 사겨요 ლ(╹ ◡ ╹ ლ) 뿌잉 뿌잉
사귀자며 전화받어
누나 나중에 대출 필요하면 전화할께요 ლ(╹ ◡ ╹ ლ) 뿌잉 뿌잉
지금안내만 받어
누나나중에..
전송


주요 피의자 프로필
김 O O (37세, 여)
- 김팀 윤OO이네 팀장
- 대출사기로 대변대는 김미영 팀장의 실존 인물
- 현재 중국에서 도피 중 (체포영장)
천안동남경찰서

전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법(약칭: 통신사기피해환급법)

“전기통신금융사기” 전기통신기본법 제2조제1호에 따른 전기통신을 이용하여 타인을 기망·공갈 함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 다음 각 목의 행위를 말한다. 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공, 알선, 중개를 가장한 행위는 포함한다.

가. 자금을 송금, 이체하도록 하는 행위
나. 개인정보를 알아내어 자금을 송금, 이체하는 행위

*** 전기통신기본법 제2조제1호 : “전기통신”이라 함은 유선,무선,광선 및 기타의 전자적 방식에 의하여 부호,문헌,음향 또는 영상을 송신하거나 수신하는 것을 말한다.**

보이스피싱 역사

2000년대 초반 대만에서 시작

이후 중국, 한국, 일본, 싱가포르 등 아시아 지역으로 확산

출처 : 금융위원회 보도자료

보이스피싱 피해규모

보 도 자 료			
보도	2019. 2. 28.(목) 석간	배포	2019. 2. 27.(수)

담당부서	불법금융대응단	이성호 팀장(3145-8521), 장종현 선임조사역(3145-8534)

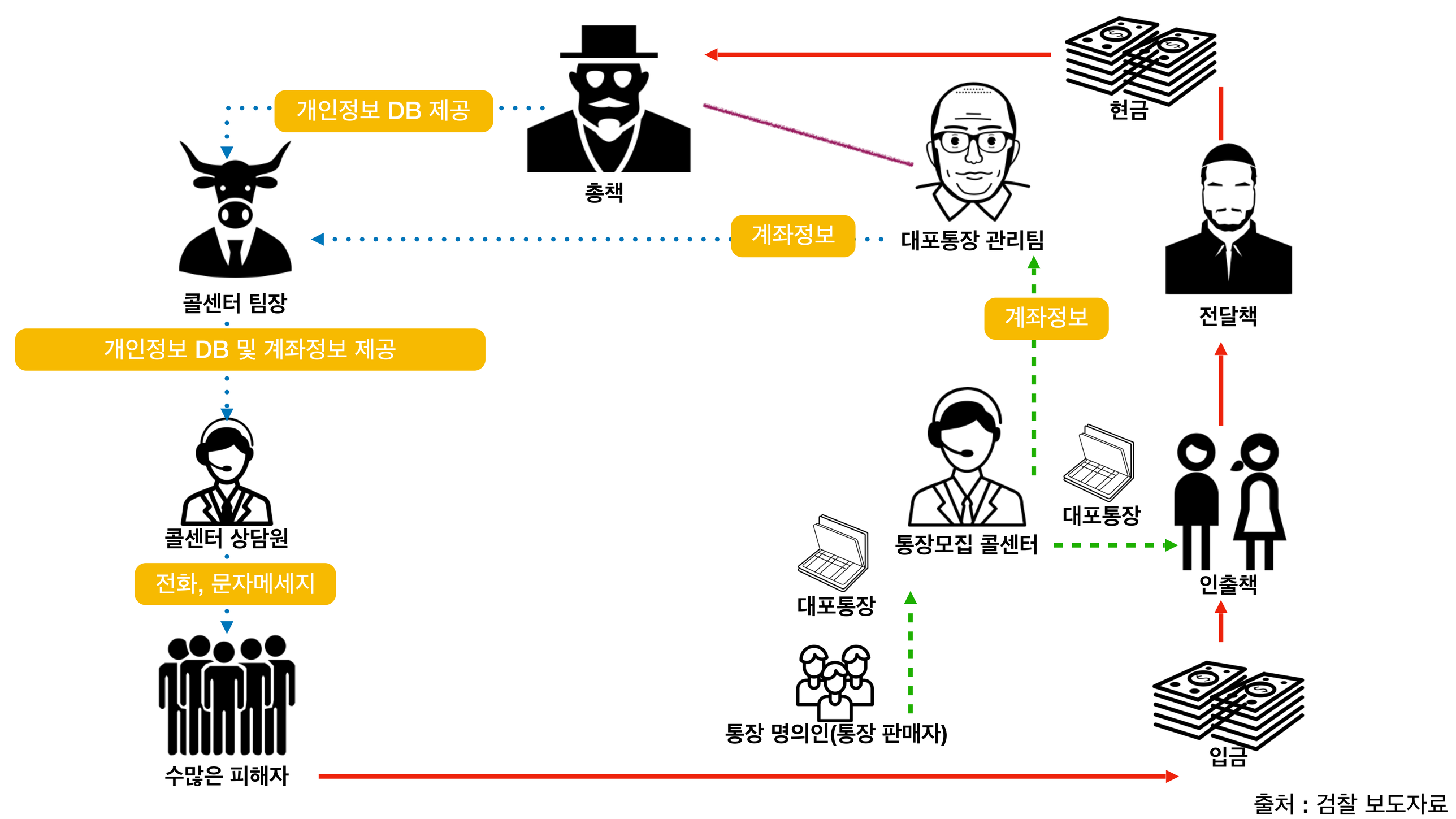
제 목 : 2018년 보이스피싱 피해액, 역대 최고수준!

1 보이스피싱 피해 현황

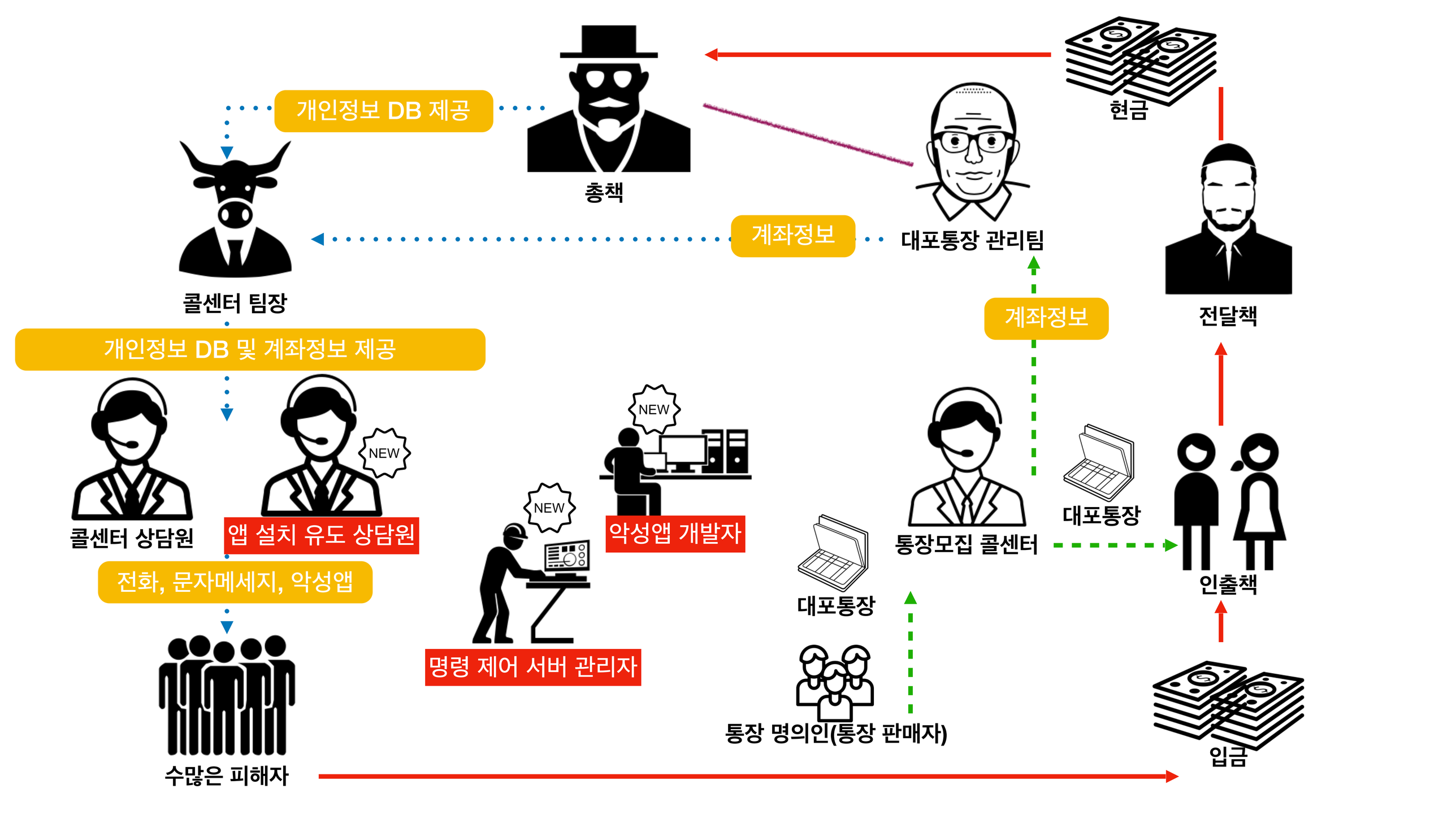
□ **(피해액)** '18년중 **4,440억원**으로 지난해(2,431억원) 보다 **82.7%(2,009억원↑)** **증가**하여 **역대 최고** 수준임

○ 보이스피싱 **피해자**는 **48,743명**으로 **매일 평균 134명**이 발생하였으며, 피해액은 **매일 평균 12.2억원**(1인당 평균 9.1백만원)이 발생하였음

일반적인 보이스피싱 과정

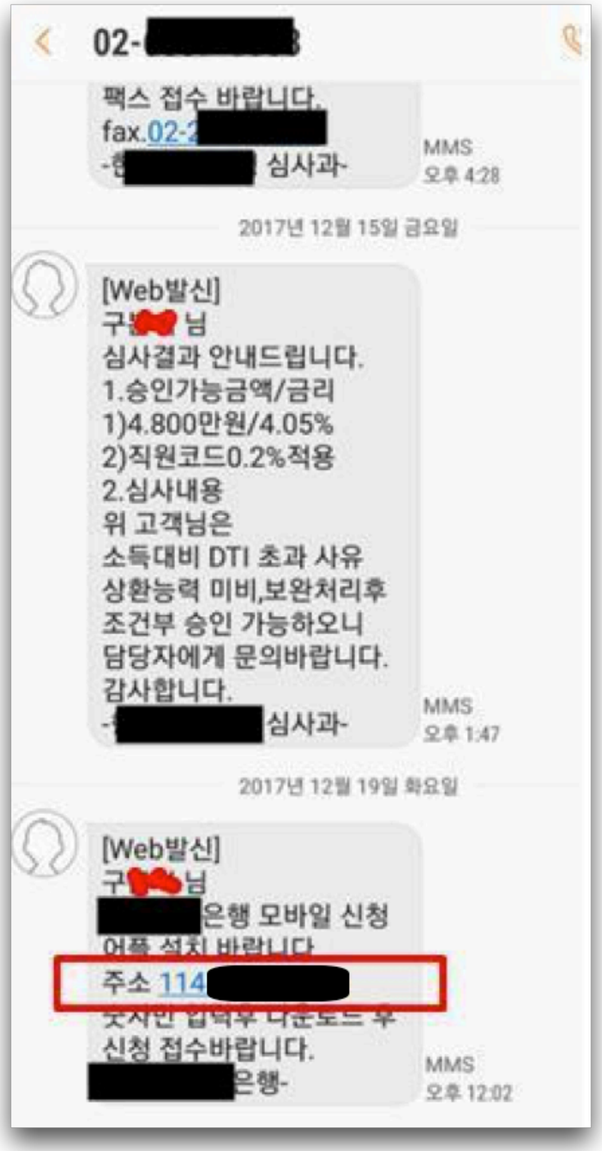

현금
총책
개인정보 DB 제공
대포통장 관리팀
계좌정보
콜센터 팀장
전달책
계좌정보
개인정보 DB 및 계좌정보 제공
콜센터 상담원
대포통장
통장모집 콜센터
인출책
대포통장
전화, 문자메세지
통장 명의인(통장 판매자)
입금
수많은 피해자

출처 : 검찰 보도자료


현금
총책
개인정보 DB 제공
대포통장 관리팀
계좌정보
콜센터 팀장
전달책
계좌정보
개인정보 DB 및 계좌정보 제공
NEW
NEW
NEW
콜센터 상담원
앱 설치 유도 상담원
악성앱 개발자
통장모집 콜센터
대포통장
인출책
전화, 문자메세지, 악성앱
대포통장
명령 제어 서버 관리자
통장 명의인(통장 판매자)
수많은 피해자
입금

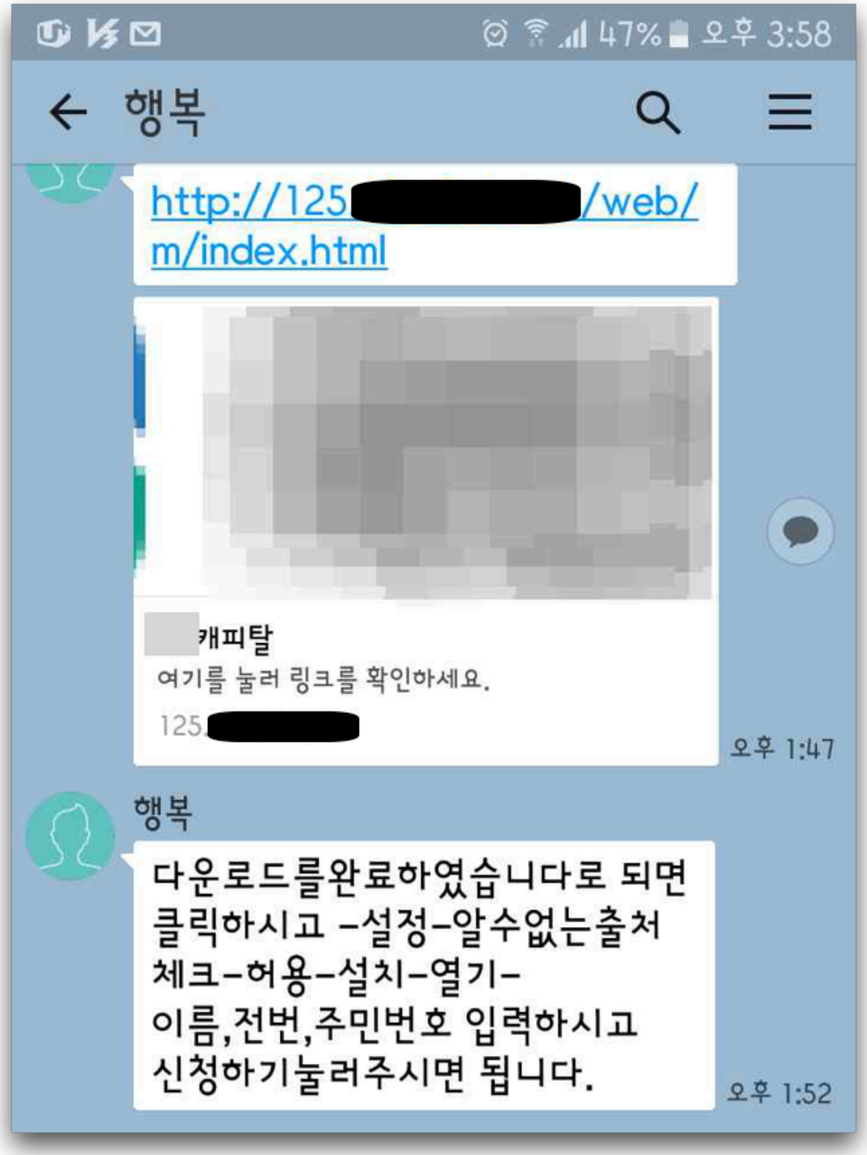
공격자는 어떻게 접근하는가?

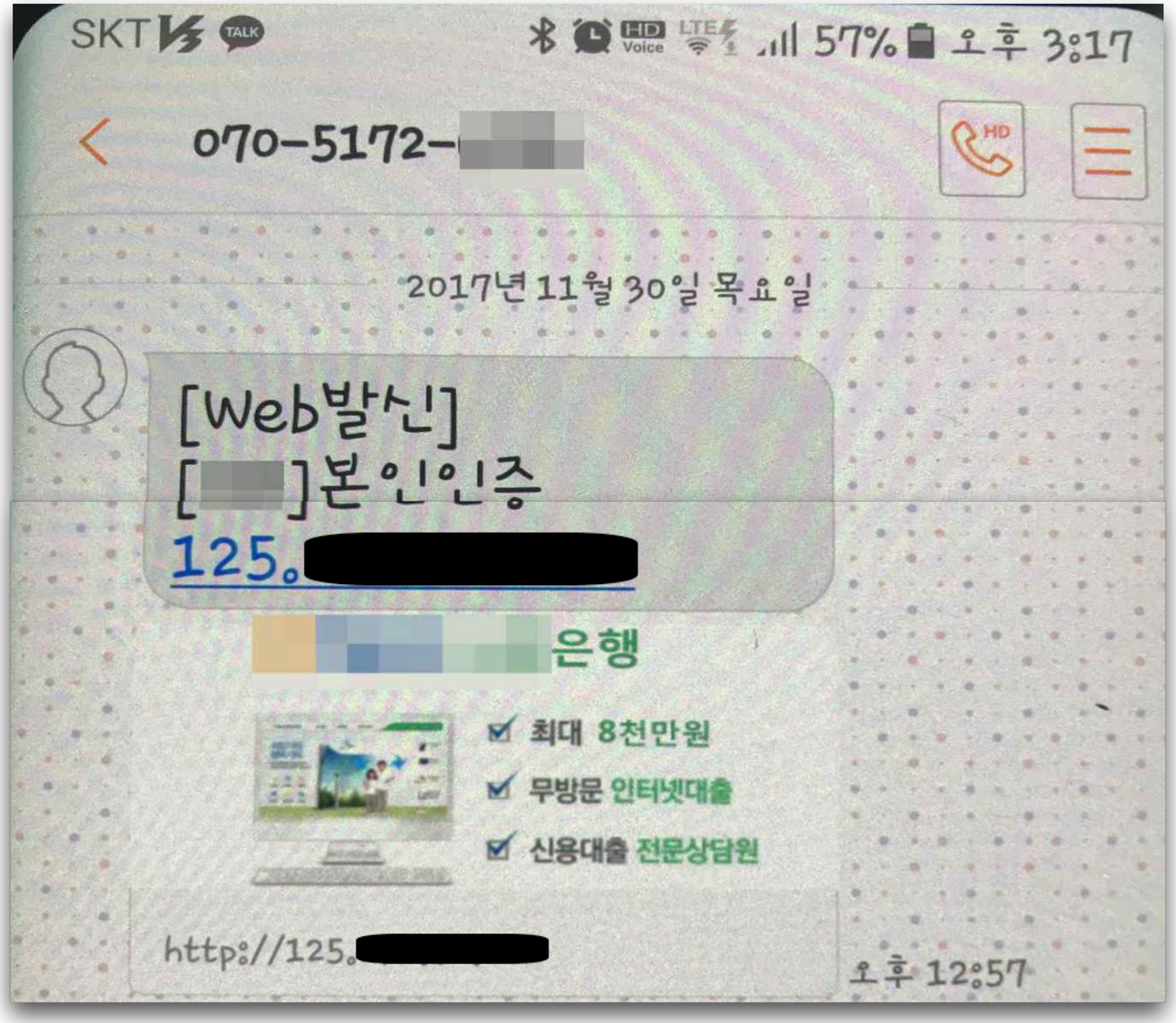
공격자는 어떻게 접근하는가?



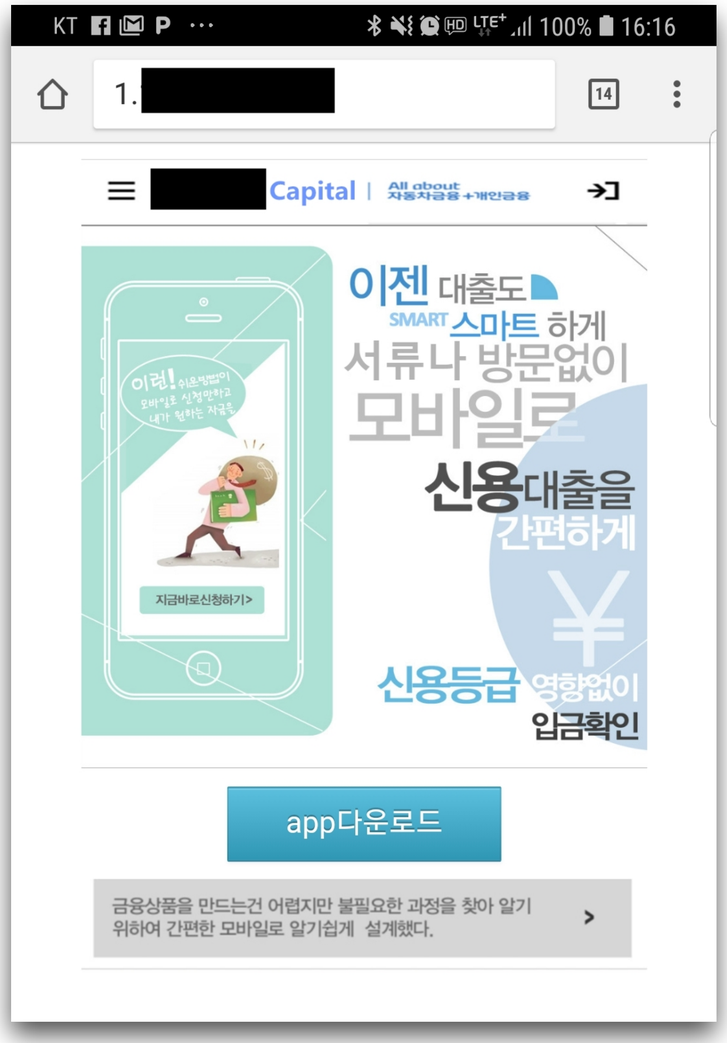
- **17.12.11. 피해자는 저금리 전환대출을 여기저기 알아봄**
- **17.12.14. xxxx-xxxx 번호에서 OO은행**
  김OO 대리라며 대출안내 전화가 옴
  대출심사 관련 필요 서류 FAX 요청
- **17.12.15. 심사결과 소득대비 DTI 초과 사유로 상환능력이**
  미비하니 보완 후 조건부 승인이 가능하다는
  SMS 안내를 받음
- **17.12.19. IP주소가 포함된 모바일 신청어플 설치**
  안내 문자를 받음
- **이후 인지대, 보증료 명목으로 선입금 요구**

공격자는 어떻게 접근하는가?

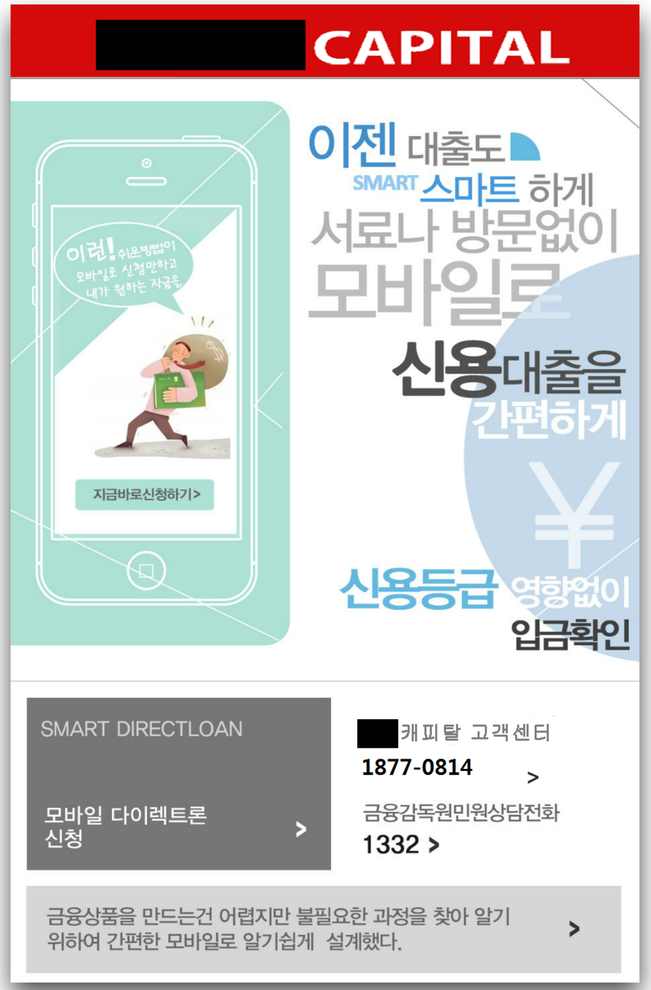




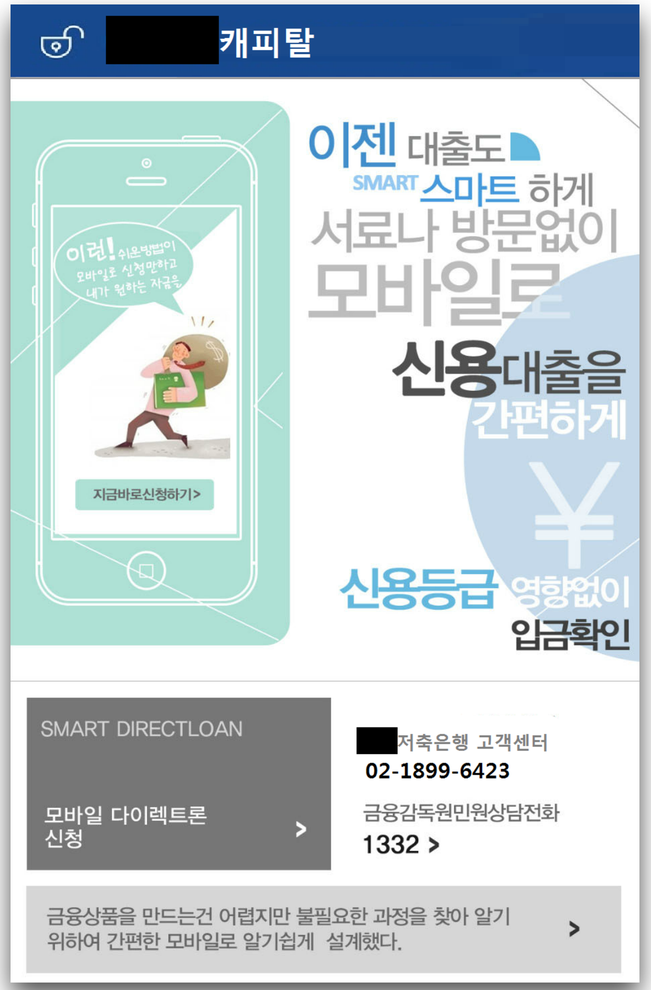
모바일기기에서 실제 접속한 화면



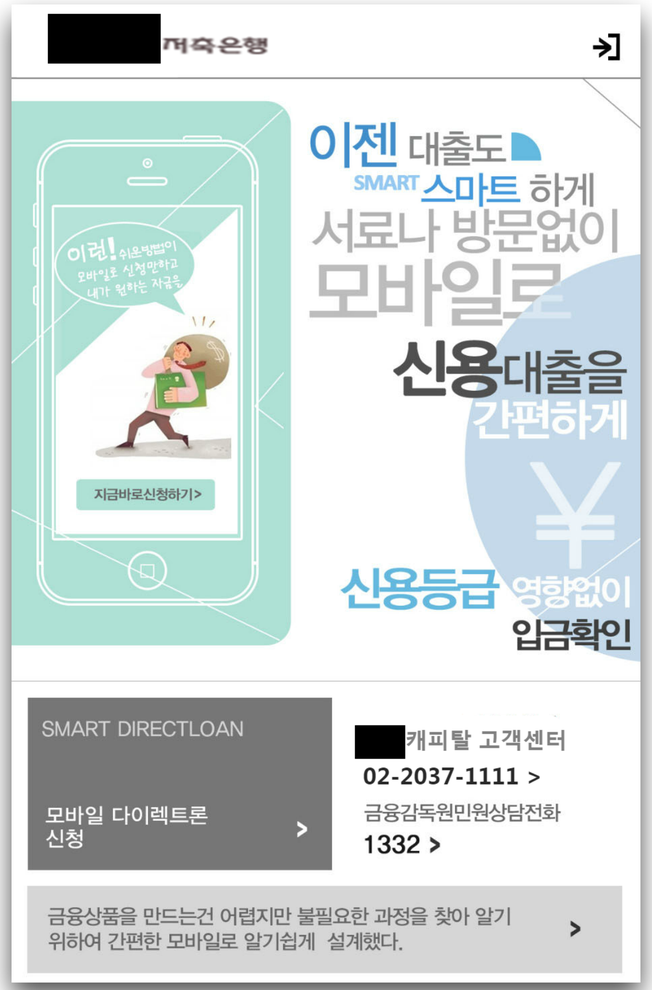
악성 앱 설치 후 실행 화면



L 캐피탈 사칭

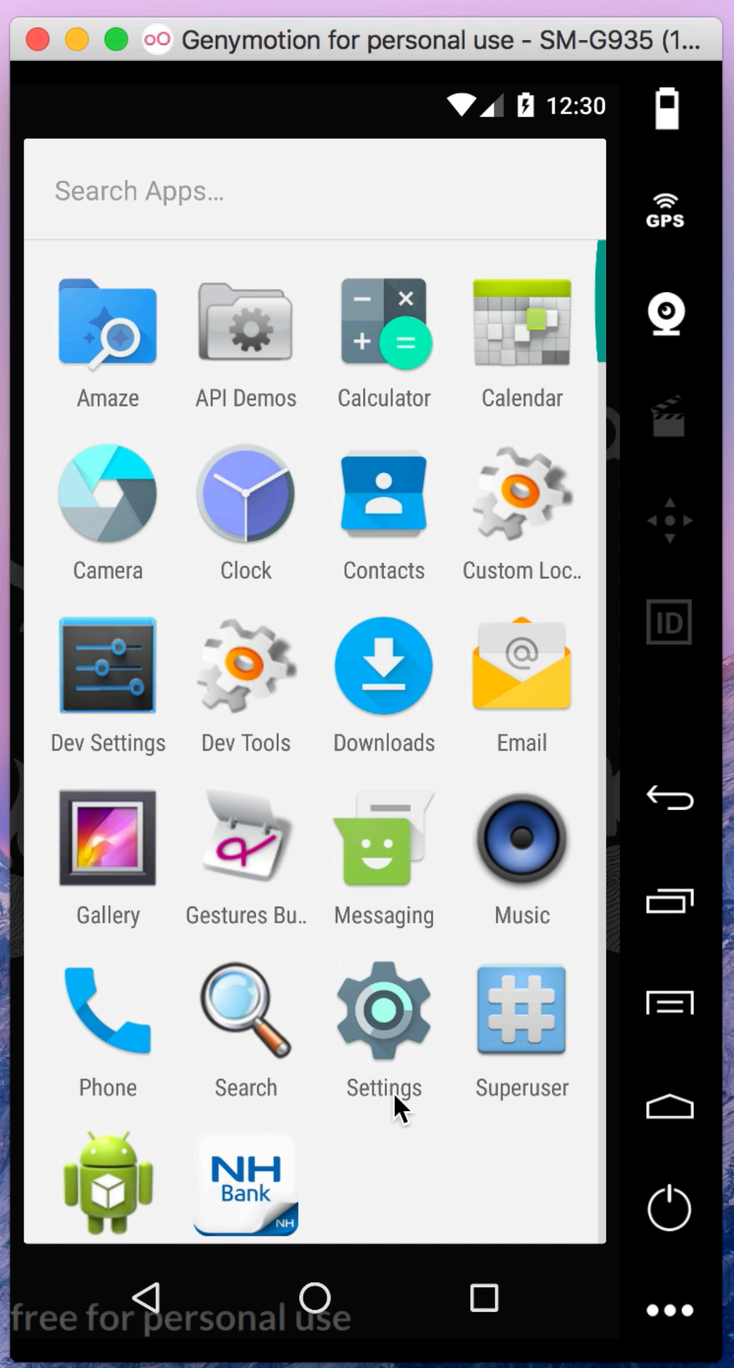


S 캐피탈 사칭

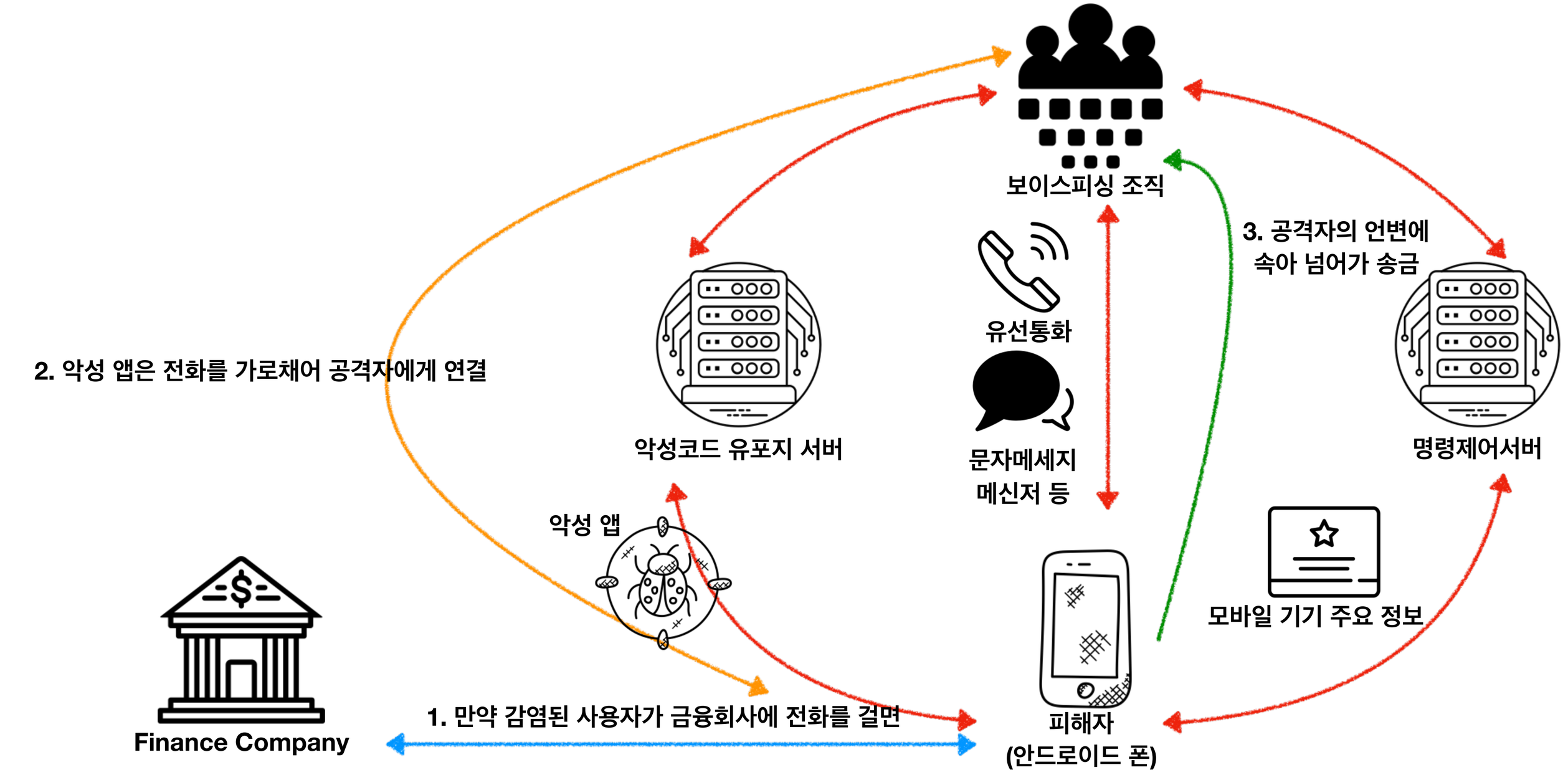


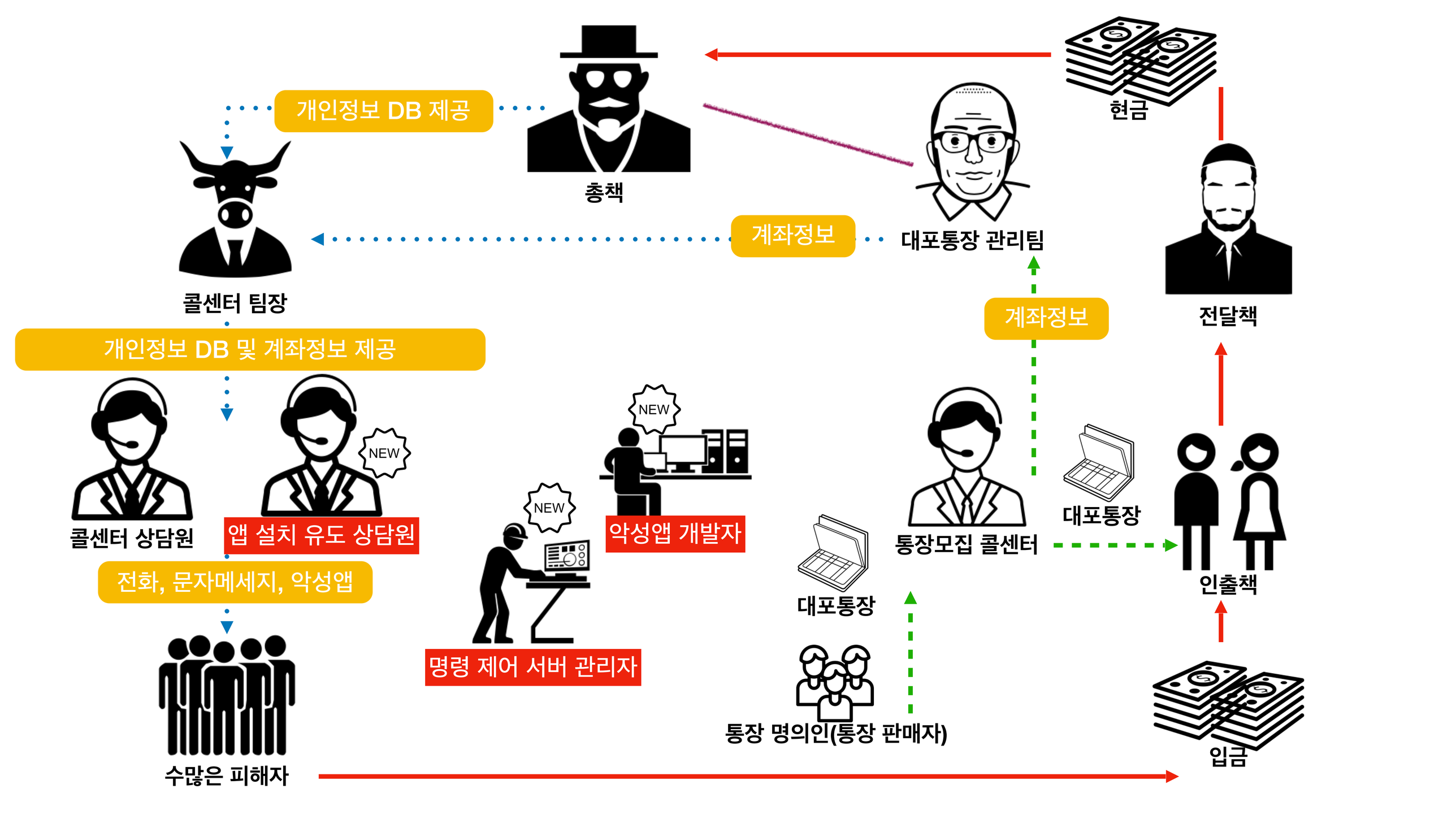
O 저축은행 사칭

데모 : 악성앱 동작

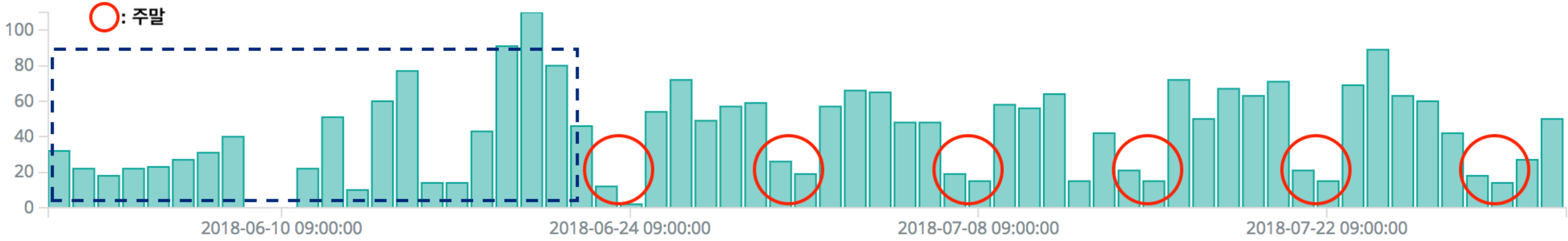

Genymotion for personal use - SM-G935 (1...
12:30
Search Apps...
Amaze
API Demos
Calculator
Calendar
Camera
Clock
Contacts
Custom Loc..
Dev Settings
Dev Tools
Downloads
Email
Gallery
Gestures Bu..
Messaging
Music
Phone
Search
Settings
Superuser
NH Bank
GPS
ID
free for personal use

새로운 유형의 보이스피싱



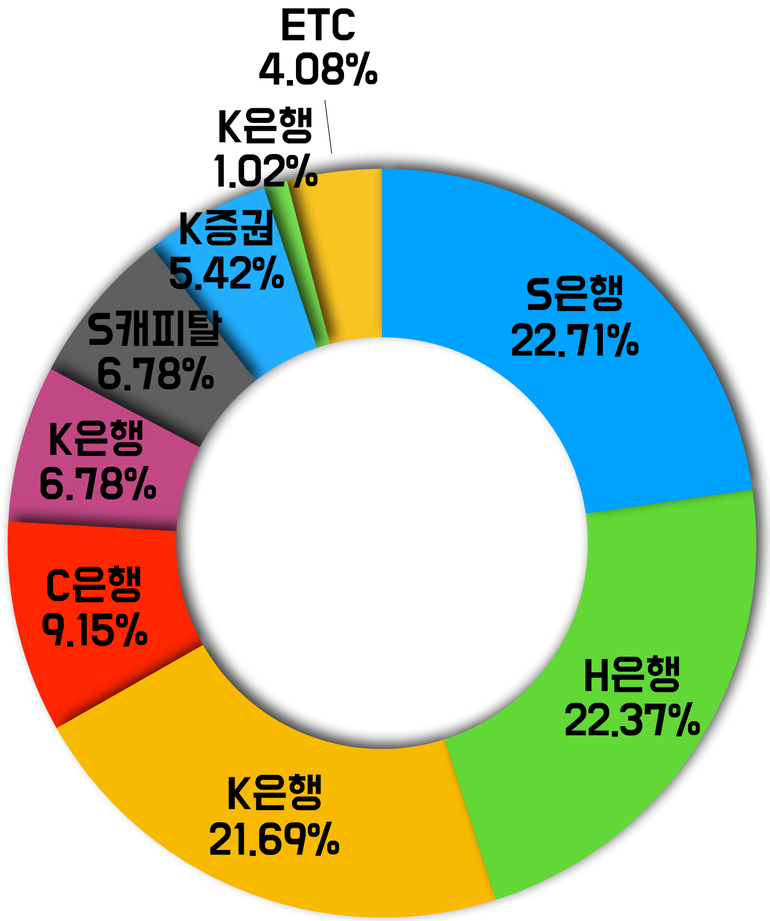

현금
총책
개인정보 DB 제공
대포통장 관리팀
계좌정보
콜센터 팀장
전달책
계좌정보
개인정보 DB 및 계좌정보 제공
NEW
NEW
NEW
콜센터 상담원
앱 설치 유도 상담원
악성앱 개발자
통장모집 콜센터
대포통장
인출책
전화, 문자메세지, 악성앱
대포통장
명령 제어 서버 관리자
통장 명의인(통장 판매자)
수많은 피해자
입금

악성앱 수집 건수


: 주말
100
80
60
40
20
0
2018-06-10 09:00:00
2018-06-24 09:00:00
2018-07-08 09:00:00
2018-07-22 09:00:00

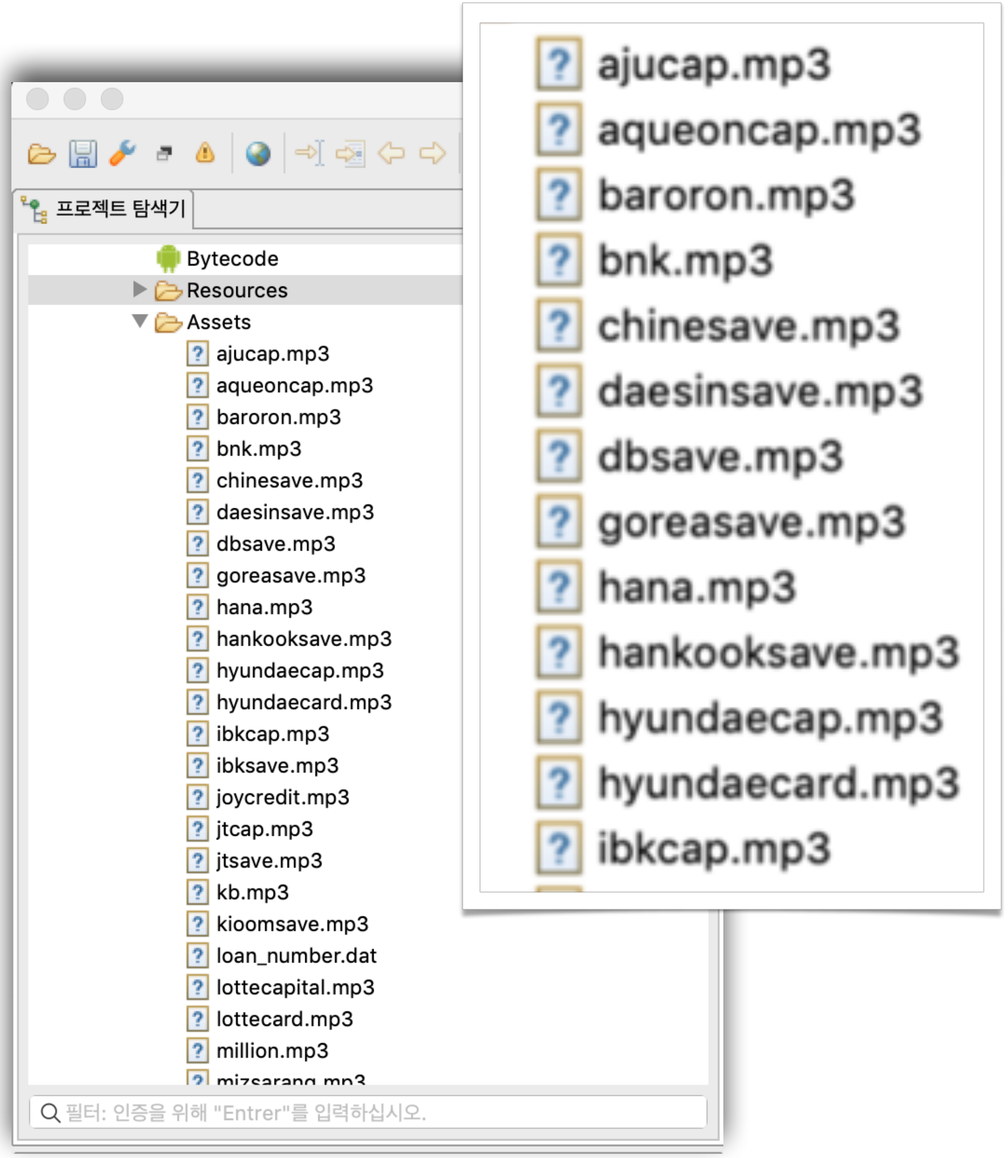
유포일	유포IP	유포도메인	유포국가	유포파일명	유포파일시간	sha256해시	패키지명	C2
2018-05-29	118.	http://118	TW	H k	2018-05-27 22:36:30	828d7b5abf17314f	com.samsung.appstore3	http://h
2018-05-29	1.16	http://1.16	TW	H .apk	2018-05-28 09:54:16	71222f25941110e6	com.samsung.appstore3	http://h
2018-05-29	36.2	http://36.2	TW	k apk	2018-05-23 10:31:25	e53f01dab2fbcfb9	com.android.willin	http://h
2018-05-29	118.	http://118	TW	a tal.apk	2018-05-27 21:27:30	5536596f45765015	com.samsung.appstore3	http://n
2018-05-29	111.	http://111	TW	N apk	2018-05-27 22:40:51	68c2919006a5a182	com.samsung.appstore3	http://n
2018-05-29	36.2	http://36.2	TW	w e.apk	2018-05-27 22:43:08	0c61236b1a04a9cc	com.samsung.appstore3	http://w
2018-05-29	220.	http://220	TW	H .apk	2018-05-20 21:54:32	89e385d49469074e	com.app.sm.dev	http://1
2018-05-29	125.	http://125	TW	s .apk	2018-05-27 22:42:37	90afc2df9c5edeb8	com.samsung.appstore3	http://1
2018-05-29	1.16	http://1.16	TW	N al.apk	2018-05-27 22:39:13	ae43c20cb604e317	com.samsung.appstore3	http://1
2018-05-29	1.16	http://1.16	TW	S ank.apk	2018-05-27 22:42:07	80760d79266a5551	com.samsung.appstore3	http://1
2018-05-29	1.16	http://1.16	TW	s .apk	2018-05-28 09:44:51	9edbb805cf458cba	com.samsung.appstore3	http://1
2018-05-29	36.2	http://36.2	TW	w e.apk	2018-05-27 22:42:47	b2dda2a9acf804c1	com.samsung.appstore3	http://w
2018-05-29	1.16	http://1.16	TW	N apk	2018-05-28 09:27:39	29c30aa50ff4c25e	com.samsung.appstore3	http://n
2018-05-29	61.2	http://61.2	TW	a tal.apk	2018-05-27 22:31:26	bc0215040de704ae	com.samsung.appstore3	http://1
2018-05-29	111.	http://111	TW	K	2018-05-20 21:55:01	47bfa3fc43d6e2b9	com.app.sm.dev	http://1
2018-05-30	111.	http://111	TW	I .apk	2018-05-27 22:37:10	5fb596b12e1afc69	com.samsung.appstore3	http://i
2018-05-30	61.2	http://61.2	TW	n .apk	2018-05-27 22:39:47	ce1e150aaae50d49	com.samsung.appstore3	http://n
2018-05-30	1.16	http://1.16	TW	n .apk	2018-05-29 17:06:22	95f7b61b3b776f87	com.android.willin	http://h
2018-05-30	36.2	http://36.2	TW	l ok	2018-05-27 22:38:36	81b2369021e18770	com.samsung.appstore3	http://1
2018-05-30	118.	http://118	TW	w .apk	2018-05-27 22:42:57	09daa06ba3ec7153	com.samsung.appstore3	http://w
2018-05-30	61.2	http://61.2	TW	H k	2018-05-27 22:35:48	8e8407da634f15b1	com.samsung.appstore3	http://1
2018-05-30	111.	http://111	TW	l ok	2018-05-27 22:38:18	e8e796e23cb58081	com.samsung.appstore3	http://1
2018-05-30	111.	http://111	TW	n .apk	2018-05-27 22:39:03	4ae89f46fc2d81fc	com.samsung.appstore3	http://n
2018-05-30	1.16	http://1.16	TW	C apk	2018-05-27 22:41:17	8d4f8445d4d4c861	com.samsung.appstore3	http://1
2018-05-30	61.2	http://61.2	TW	H .apk	2018-05-29 13:57:17	5c37b0e327a0ced1	com.samsung.appstore3	http://h
2018-05-30	114.	http://114	TW	K	2018-05-29 09:46:09	90836e641a7a5aac	com.samsung.appstore3	http://k
2018-05-30	125.	http://125	TW	s .apk	2018-05-29 13:51:02	6d6ee25a4a73954c	com.samsung.appstore3	http://1

악성 앱 파일명으로 분류한 사칭된 금융회사



계속 발전하고 있는 악성 앱

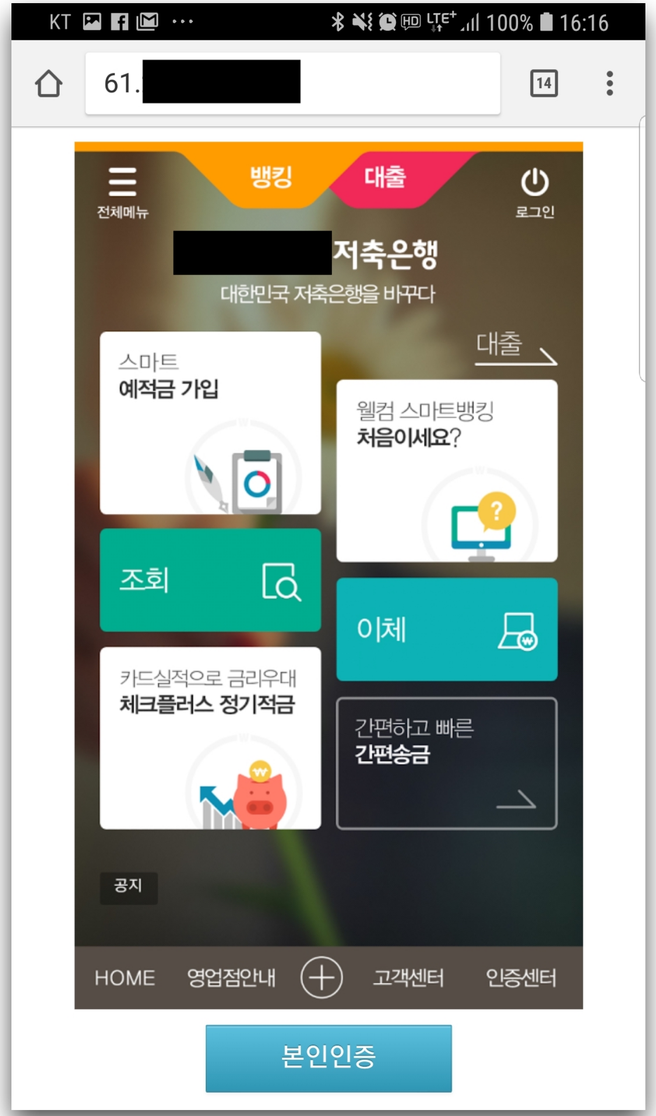
- 최근 수집되는 악성 앱의 경우 금융회사별 전화연결음을 들려주는 기능이 추가됨



관련 서버(유포지) 살펴보기

유포지 서버 접속(80)

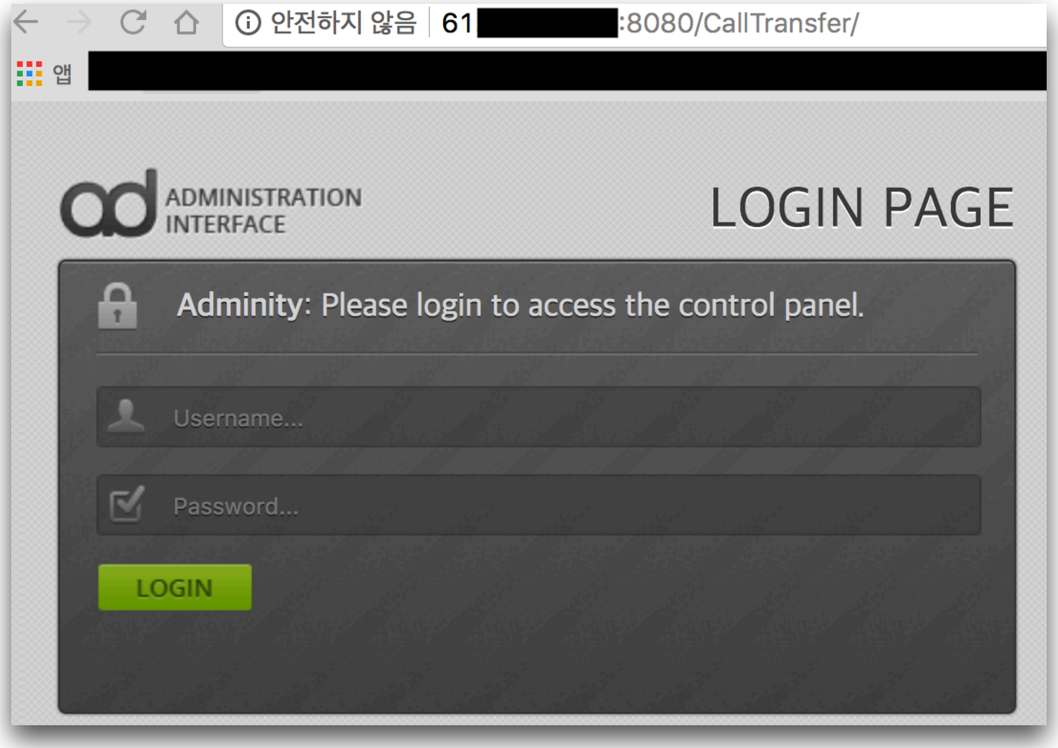

KT 100% 16:18
125.[redacted]
14
[redacted]저축은행
금리안내
OK e-안심정기예금
2.4%
정기적금
2.2%
OK e-대박통장
1.8%
예금상품
대출상품
카드/보험
간편대출신청
한번에 OK! 한도조회
비대면 계좌개설
가능상품 조회 OK
본인인증
OK저축은행
1899-7979
365일 09:00~18:00
신용대출
1800-8282
대출가능시간 : 평일 09:00~22:00
상담신청가능시간 : 365일 24시간
[redacted]저축은행
[redacted]저축은행
대표이사 : 정길호 / 사업자번호 : 211-88-90264
서울특별시 중구 세종대로 39 10층 (남대문로4가 대한상공회의소 10층)
Copyright © 2015 OK SAVINGS BANK. All Rights Reserved.

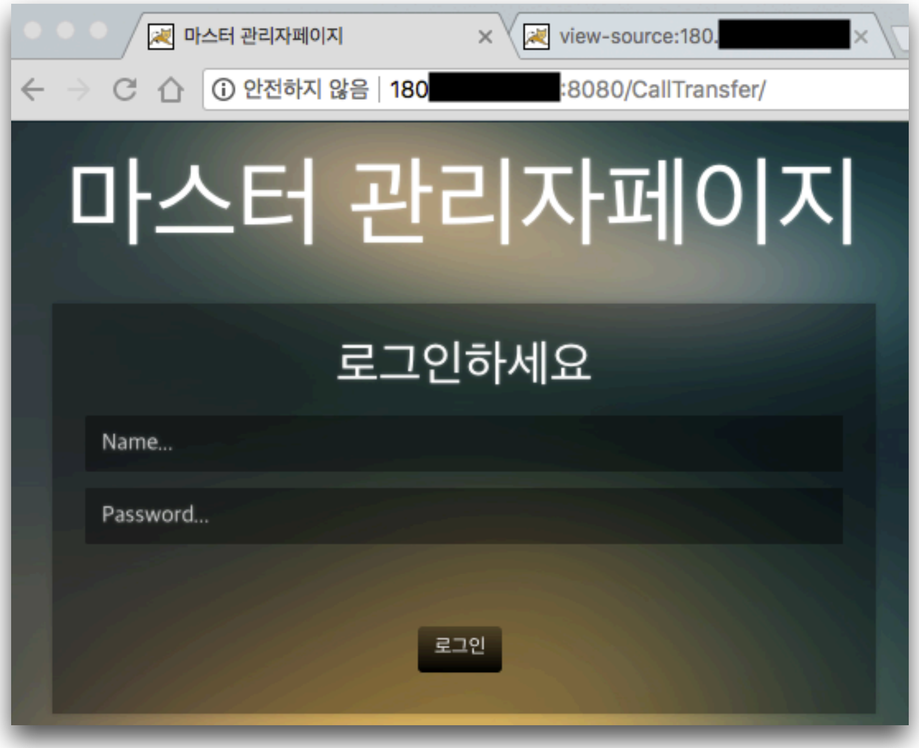

KT 100% 16:16
61.[redacted]
14
전체메뉴
뱅킹
대출
로그인
[redacted]저축은행
대한민국 저축은행을 바꾸다
스마트
예적금 가입
대출
웰컴 스마트뱅킹
처음이세요?
조회
이체
카드실적으로 금리우대
체크플러스 정기적금
간편하고 빠른
간편송금
공지
HOME
영업점안내
고객센터
인증센터
본인인증


登录到 Windows
Microsoft
Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
用户名(U):
密码(P):
确定
取消
选项(O) >>

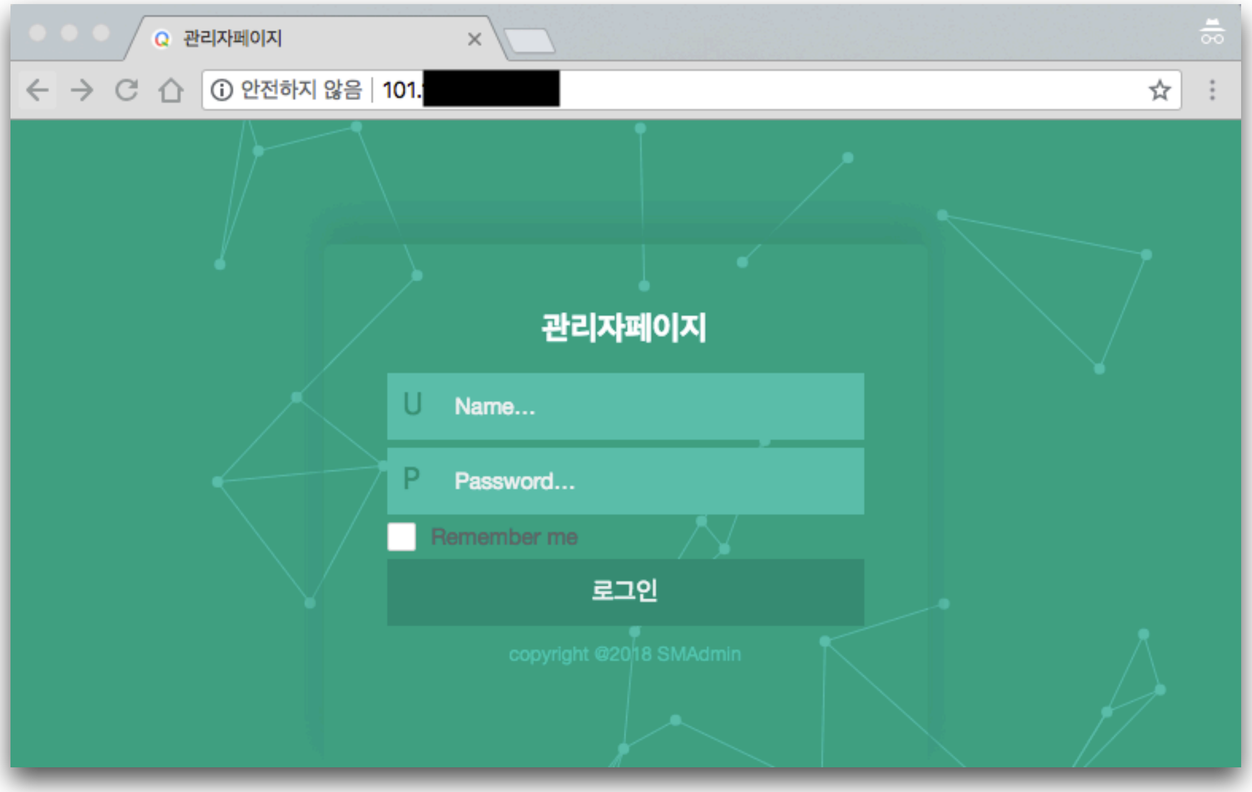
관련 서버(C&C) 살펴보기

C&C 서버 로그인 페이지(8080)





C&C 서버 로그인 페이지(80)



마무리

마무리

- 전통적인 보이스피싱 + 악성 안드로이드 앱 = 새로운 유형의 보이스피싱의 등장
- 확보된 정보에 따르면 유포지의 지리학적 위치는 대만
- 전화 받는 가짜 상담원의 한국인 같은 한국어 구사능력
- 지속적인 기능 개선으로 악성 앱을 “고도화” 하는 중
- 유포지, C&C IP 차단 등 제한적 대응 중
- 공격자의 070번호 차단을 통한 대응을 준비 중 (통신사 협조 필요)
- 한국, 대만, 인터폴이 공조하여 현재 수사 중

QnA

Special Thanks to EnergyBrothers & Sister(darbong)