나는 악마를 보았다

Prologue by Bulgom

2014년 11월 말쯤 대략 농협 텔레 뱅킹 사고가 세상에 알려진 그 즈음이다.
도용된 카드로 우리 회사 클라우드 서비스 요금이 결재 되었다고
결제 대행 PG 사로부터 연락이 왔고 조금 으니 경찰서로부터 참고인 조사받으라고
연락이 왔다.

고객 내역을 살펴보니 휴대폰 본인 인증을 통과하여, 이미 여러 대의 가상 서버를
신청하고 이용하고 있는 상태였다.
신청한 고객과 연락은 되지 않는 상태. 일단 서비스는 정지 시키고,
서버 사용자가 연락이 올 때까지 기다렸으나 연락이 오지 않았다.
다섯 대의 가상 서버로 이 친구가 무슨 범죄를 저질렀을지가 궁금해졌다.

재미있는 건 해커도 자신의 정보 보안에는 별로 관심이 없었던 것으로 보인다.
시스템 최초 세팅 시 패스워드를 입력 한 결과 이 해커는 우리가 만들어준
최초의 패스워드를 바꾸지 않은 상태였다.

그중 한 대의 서버에 접속해 들어간 순간 한순간 벌어진 입을 다물 수가 없었다.
악마들의 데스크톱 바탕 화면- 악마들의 작업장이 고스란히 드러났다.
온통 훔쳐온 개인 정보, 보안 카드 사진 찍은 것, 주유소 기름 넣었을 때에 찍힌 듯 한
카드 사진 등등.

일단 KISA와 경찰에 신고하고, ZDNET 기자에게 이를 제보하였다.
http://www.zdnet.co.kr/news/news_view.asp?artice_id=20141126140545

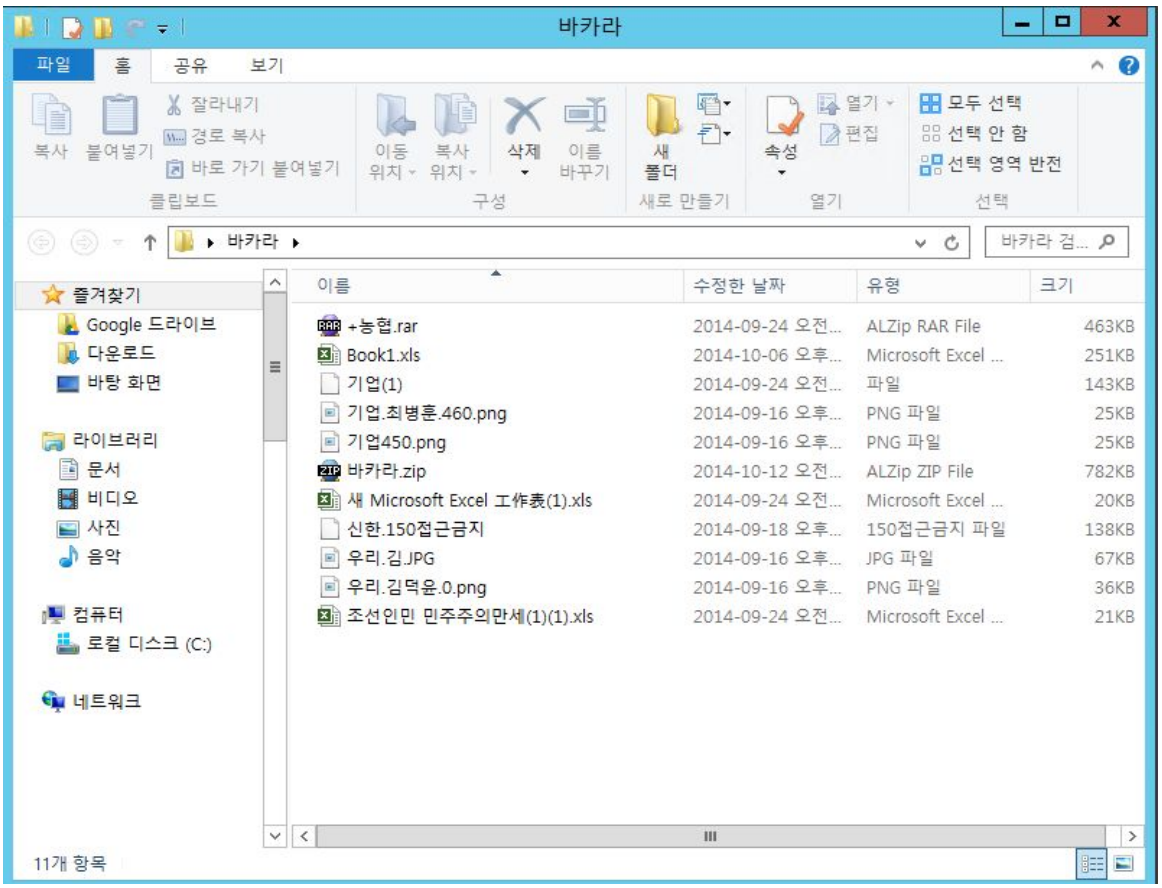
그리고 과연 개인 정보가 유출되어 그들이 그것을 이용해 우리의 돈을 노리는 작업을
하고 있는지, 공익성 차원에서 리포팅을 해야겠다고 마음 먹고분석을 하게 되었다.

두 달여 간의 짬짬이 분석한 결과물이 아래의 자료이다.

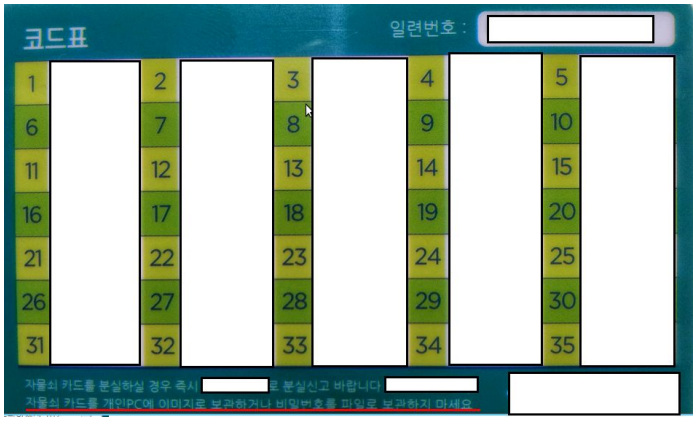
내용이 상당히 길므로 pdf 자료로도 볼 수가 있다.

[첨언]
분석 중에 통신사 본인 인증을 통과한 휴대폰 또한 도용된 휴대폰이었다.
실제 도용된 이가 우리 회사를 방문 한 바 있다. 악의라고는 하나도 없이 평범한 직장인
이 범죄의 소용돌이에 휘말린 사례다.

휴대폰이 도용된 사람의 경우 수백여 개의 사이트 모든 로그인 아이디와 패스워드 정보가 키로거 악성코드 공격으로 해커들에게 다 넘어간 상태, 정상적인 생활이 불가능할 것으로 보였다.



[인증서 파일과 잔액조회까지 마친 상태로 보이는 파일들]



[고객용 뱅킹 보안카드 이미지 파일]

사장님이 경찰서를 갔다 오시면서 서버를 하나 던져 주셨다

서버를 대략 살펴보니 몇칠 전 TV에서 봤던 뱅킹 사고가 생각이 났다.

아무래도 이번 뱅킹 해킹 사건과 관련이 있을 거라 생각들이 들어

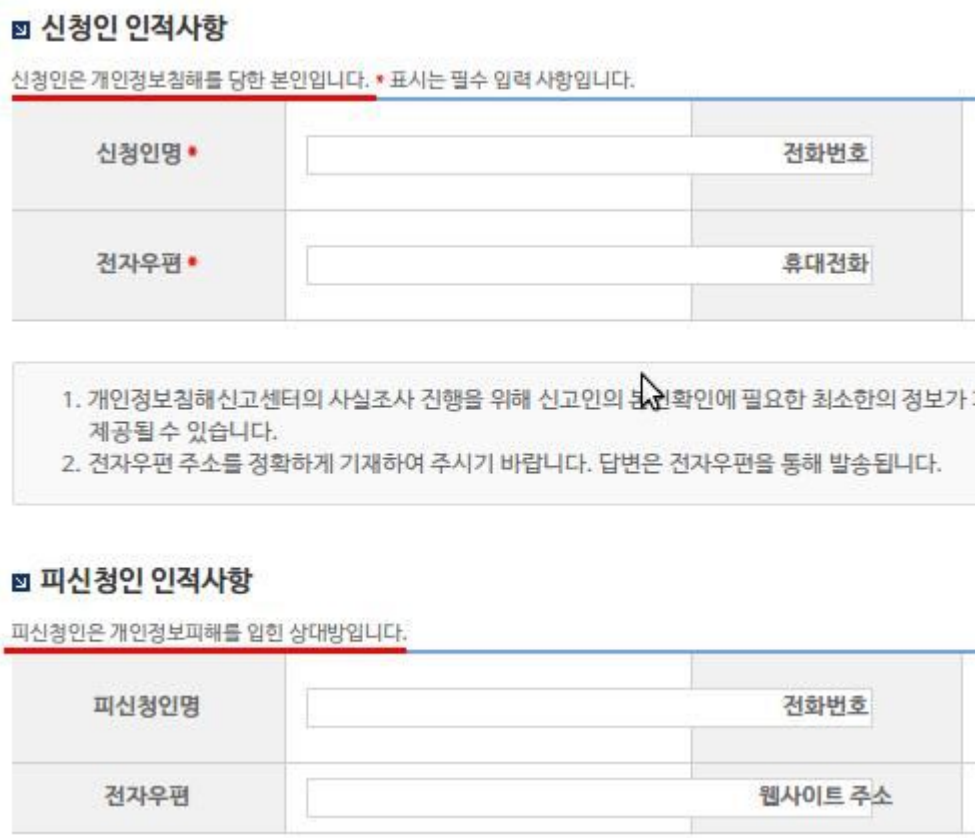
국번 없이 118번 KISA 한국 인터넷 진흥원에 전화를 걸었다.

“불특정 다수 국민들의 개인 정보가 불법적으로 수집되어 있는 서버가 있다.”라고 하니

KISA 개인정보보호사이트 내에 개인정보침해신고센터에 신고를 하라고 하였다.

신고하기 버튼을 눌러 양식을 보아하니...

보통 피해를 입은 사람이 피해를 입힌 사람을 신고하는 양식인듯하다.



엔지니어 생활 8년차에 이런 사건은 처음이라 좀 낯설고 당황스러웠다.

신청인에는 나의 정보를 적고 피신청인은 이 사람이 누군지 모르니 미상으로 적고

신고를 하였으며 또한 사이버 경찰 수사관에 의뢰하여 서버에 대한 조사도 진행하였다.

그리고 일주일이 지난 뒤 KISA로부터 처리 결과가 수신되었다.

어려운 말 같지만 한마디로 **경찰서에 신고 하라는것이다.**

이미 경찰은 한번 왔다 갔으니 범인을 잡길 기다리면 되는 것이고

나는 혹시나 해커가 남긴 단서가 있을지도 모르니 조용히 추적을 해보았다.

해커가 사용한 상품

해커는 탈취한 공인인증서를 기반으로 명의를 도용하여 서비스 신청을 하였으며

스마일서브에서 제공하는 “WIN MAX 64” 라는 클라우드 서비스를 이용하였다

상품선택

상품명	SHARE	SINGLE	DOUBLE	TRIPLE	QUAD	OCTA
선택	◉	○	○	○	○	○
코어	Share	1 CORE	2 CORE	3 CORE	4 CORE	8 CORE
메모리	1GB	1GB	2GB	3GB	4GB	8GB
스토리지					100GB	
트래픽 요금안내	› 기준 : 다운로드 트래픽(서버에서 데이터가 나가는 것) - 전체 : 월 700GByte 제공, 추가 제공시 1GByte당 60원 - 해외 : 월 30GByte 제공, 추가 제공시 100MByte당 50원					

해커가 사용한 서버 스펙은 아래와 같다.

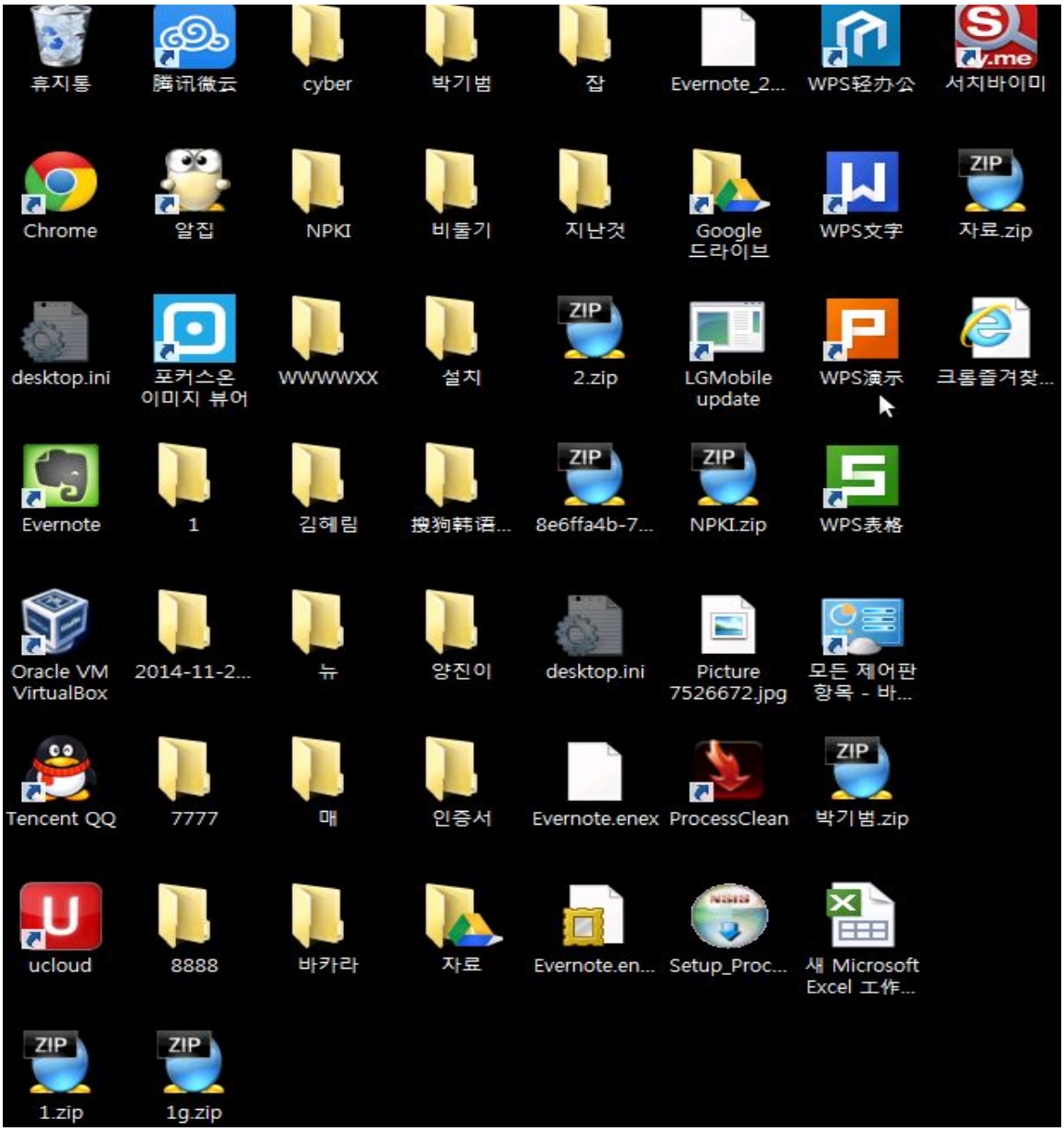
WINDOWS 2012 CPU SHARED 1G RAM 100G 저장공간

저렴한 가격에 윈도우즈 서버를 사용할 수 있으며

기본적으로 사용하는 데는 큰 불편함이 없는 사양이다.

서버 로그인 화면

최초 세팅 시 기본 제공하는 패스워드를 바꾸지 않아서 로그인하는 데는 무리가 없었다.



바탕화면에는 디렉터리, 아이콘, 파일 등이 정리되지 않은 채로 사용하고 있었다.

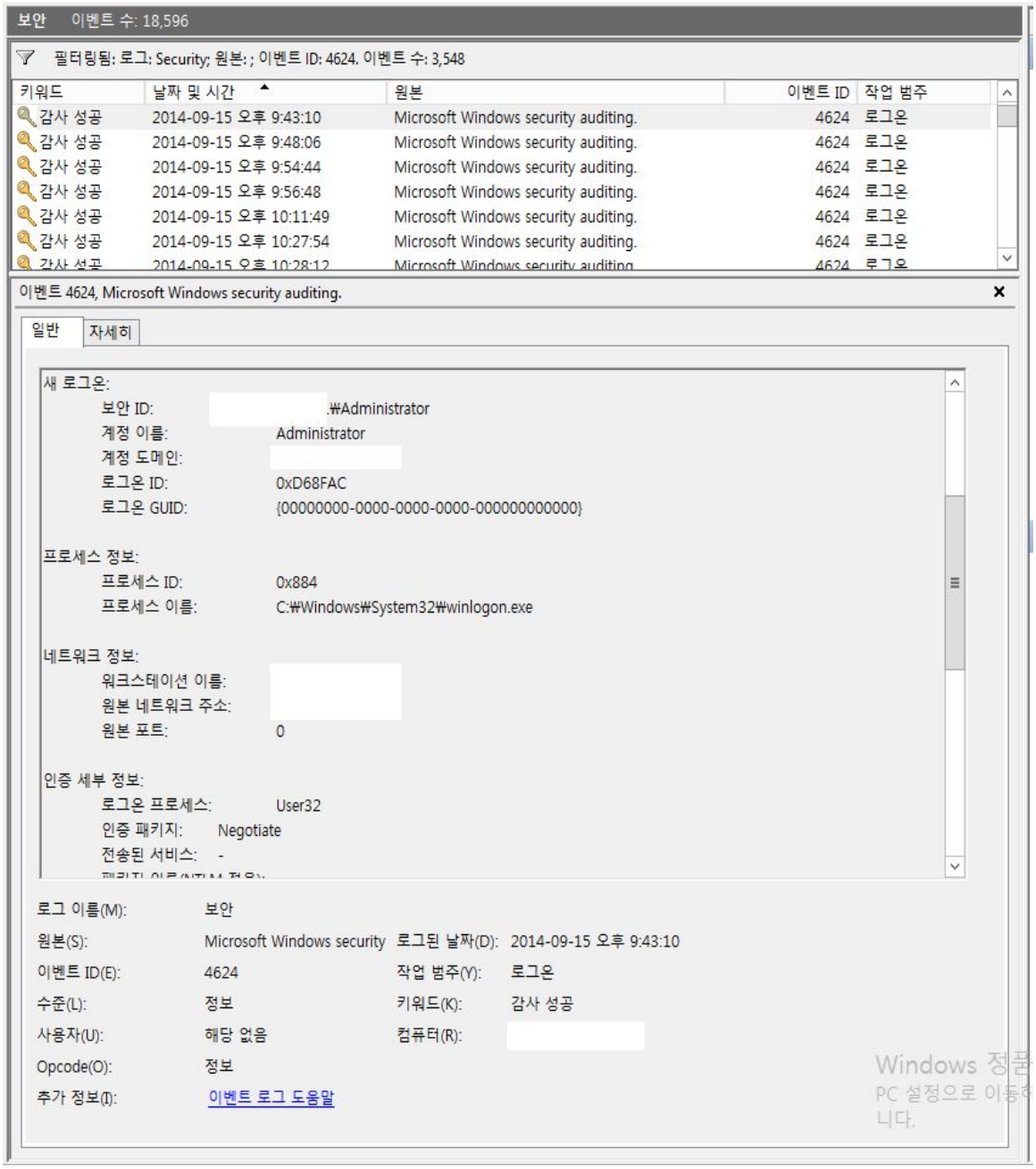
파일에 패스워드 지정하거나 방화벽 설정 등의 특별한 보안 설정은 확인할 수 없었으며

바탕화면이 지저분한 것과 의심스러운 이름의 폴더들이 존재하고 있었다

윈도우 감사 로그 확인

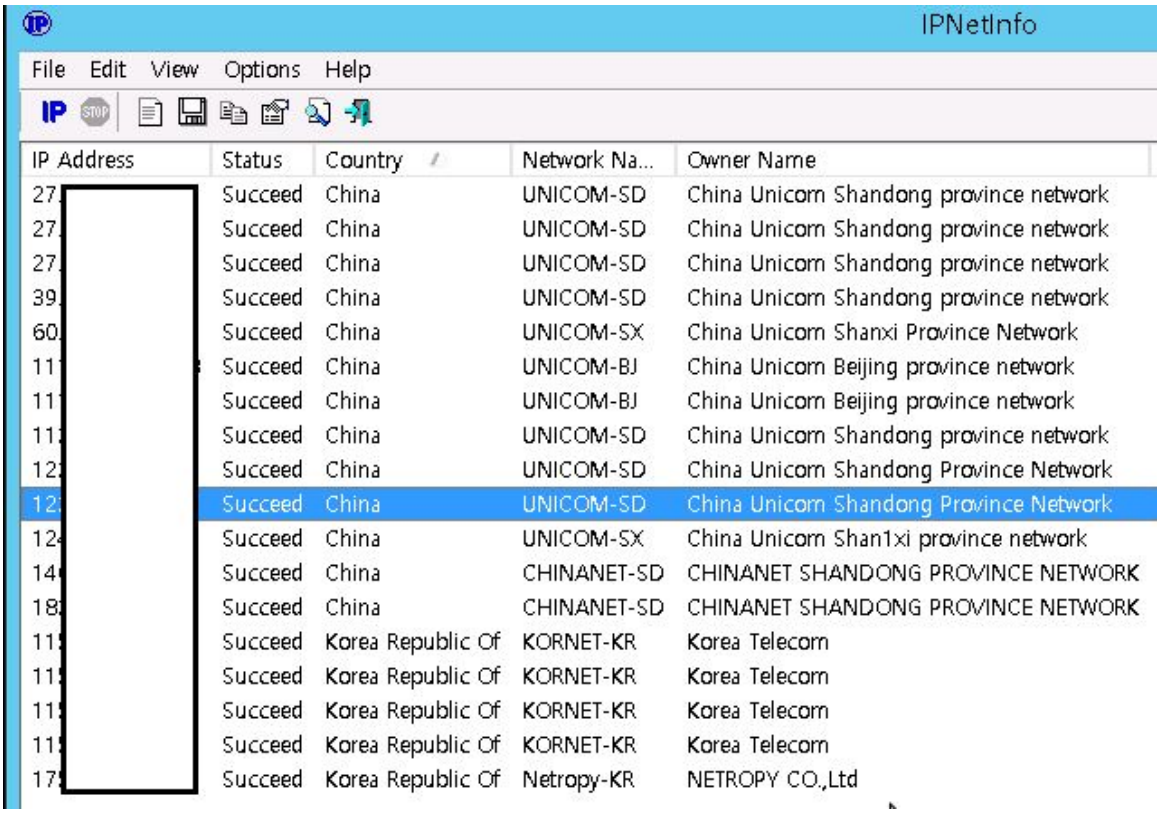
실제 서버의 사용자였을 해커가 어디쯤 위치하는지 파악하기 위해서

윈도우즈 감사로그를 점검해보았다.



우선 로그인 성공한 로그만을 필터 설정하여서 접속한 아이피만 추출해보았다

추출한 아이피는 아이피 검색 툴로 질의하였다



IP Address	Status	Country	Network Na...	Owner Name
27.	Succeed	China	UNICOM-SD	China Unicom Shandong province network
27.	Succeed	China	UNICOM-SD	China Unicom Shandong province network
27.	Succeed	China	UNICOM-SD	China Unicom Shandong province network
39.	Succeed	China	UNICOM-SD	China Unicom Shandong province network
60.	Succeed	China	UNICOM-SX	China Unicom Shanxi Province Network
11	Succeed	China	UNICOM-BJ	China Unicom Beijing province network
11	Succeed	China	UNICOM-BJ	China Unicom Beijing province network
11	Succeed	China	UNICOM-SD	China Unicom Shandong province network
12	Succeed	China	UNICOM-SD	China Unicom Shandong Province Network
12	Succeed	China	UNICOM-SD	China Unicom Shandong Province Network
12	Succeed	China	UNICOM-SX	China Unicom Shan1xi province network
14	Succeed	China	CHINANET-SD	CHINANET SHANDONG PROVINCE NETWORK
18	Succeed	China	CHINANET-SD	CHINANET SHANDONG PROVINCE NETWORK
11	Succeed	Korea Republic Of	KORNET-KR	Korea Telecom
11	Succeed	Korea Republic Of	KORNET-KR	Korea Telecom
11	Succeed	Korea Republic Of	KORNET-KR	Korea Telecom
11	Succeed	Korea Republic Of	KORNET-KR	Korea Telecom
17	Succeed	Korea Republic Of	Netropy-KR	NETROPY CO.,Ltd

해커들은 어디에서 접속하였을까?

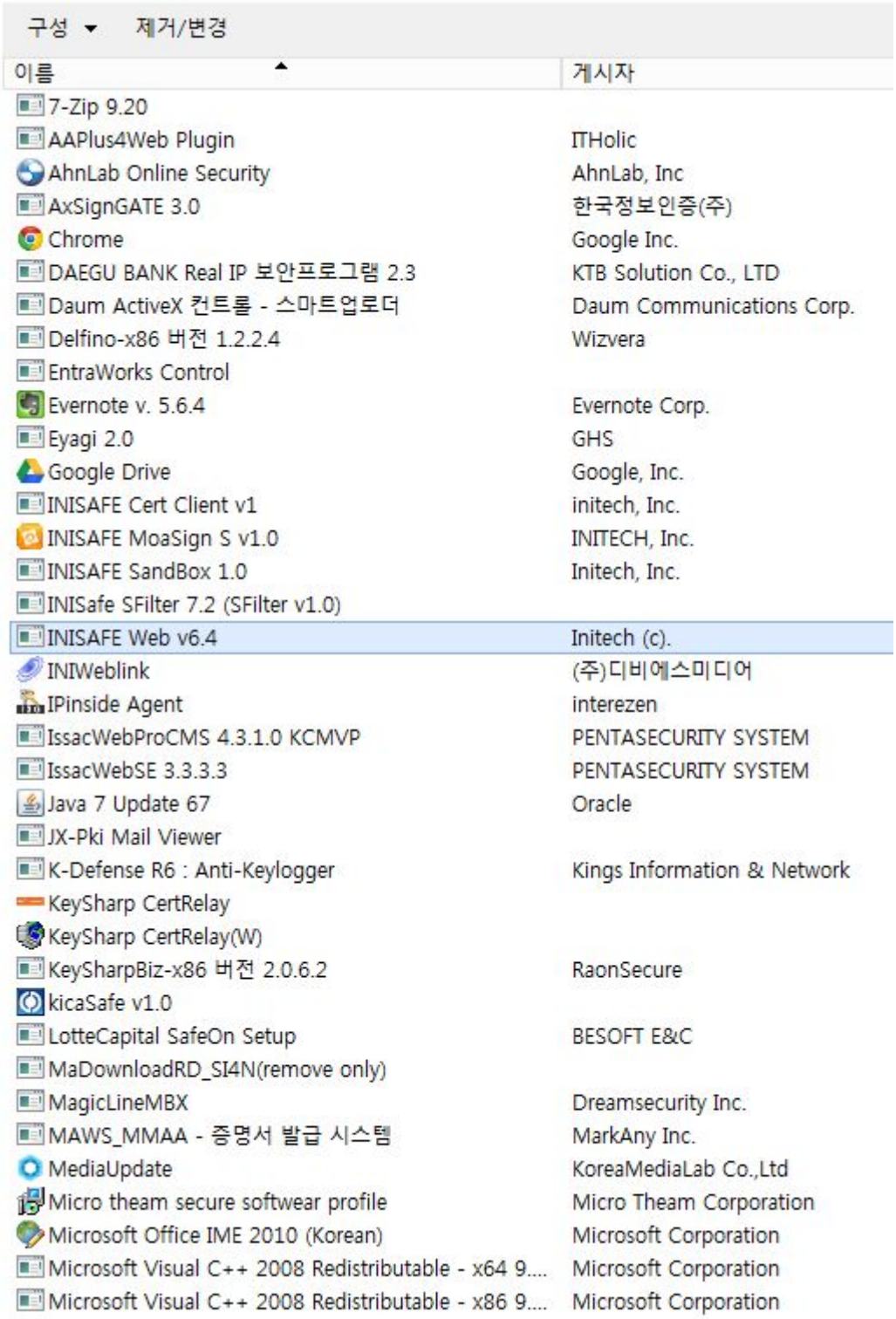
18개의 아이피에서 해당 서버로 접근한 로그가 남아 있으며

중국 14개의 아이피는 IP가 등록된 주소는 베이징, 산둥성, 산시성이며

국내 아이피 4개는 분당 정자동, 서울 송파동 쪽이었다

중국과 한국이 연관되어 있는 간접적인 증거가 될 수 있겠다

서버에 설치된 프로그램



구성 ▾ 제거/변경

이름	게시자
7-Zip 9.20	
AAPlus4Web Plugin	ITHolic
AhnLab Online Security	AhnLab, Inc
AxSignGATE 3.0	한국정보인증(주)
Chrome	Google Inc.
DAEGU BANK Real IP 보안프로그램 2.3	KTB Solution Co., LTD
Daum ActiveX 컨트롤 - 스마트업로더	Daum Communications Corp.
Delfino-x86 버전 1.2.2.4	Wizvera
EntraWorks Control	
Evernote v. 5.6.4	Evernote Corp.
Eyagi 2.0	GHS
Google Drive	Google, Inc.
INISAFE Cert Client v1	initech, Inc.
INISAFE MoaSign S v1.0	INITECH, Inc.
INISAFE SandBox 1.0	Initech, Inc.
INISafe SFilter 7.2 (SFilter v1.0)	
INISAFE Web v6.4	Initech (c).
INIWeblink	(주)디비에스미디어
IPinside Agent	interezen
IssacWebProCMS 4.3.1.0 KCMVP	PENTASECURITY SYSTEM
IssacWebSE 3.3.3.3	PENTASECURITY SYSTEM
Java 7 Update 67	Oracle
JX-Pki Mail Viewer	
K-Defense R6 : Anti-Keylogger	Kings Information & Network
KeySharp CertRelay	
KeySharp CertRelay(W)	
KeySharpBiz-x86 버전 2.0.6.2	RaonSecure
kicaSafe v1.0	
LotteCapital SafeOn Setup	BESOFT E&C
MaDownloadRD_SI4N(remove only)	
MagicLineMBX	Dreamsecurity Inc.
MAWS_MMAA - 증명서 발급 시스템	MarkAny Inc.
MediaUpdate	KoreaMediaLab Co.,Ltd
Micro theam secure softwear profile	Micro Theam Corporation
Microsoft Office IME 2010 (Korean)	Microsoft Corporation
Microsoft Visual C++ 2008 Redistributable - x64 9....	Microsoft Corporation
Microsoft Visual C++ 2008 Redistributable - x86 9....	Microsoft Corporation

구성 ▾ 제거

이름	게시자
MiPlatform_InstallBase320	TOBESOFT
MiPlatform_InstallEngine320U	TOBESOFT
MiPlatform_Updater320	TOBESOFT
MSXML 4.0 SP2 파서 및 SDK	Microsoft Corporation
Navipop	ONPURE
NEWSPOT insu24 (Remove only)	http://www.additcom.com/
npEfdsWCtrl	INCA Internet Co., Ltd.
npPCStatus	INCA Internet Co., Ltd.
nProtect KeyCrypt V5.0	INCA Internet Co., Ltd.
nProtect KeyCrypt V6.0	INCA Internet Co., Ltd.
nProtect Netizen v5.5	INCA Internet Co., Ltd.
Oracle VM VirtualBox 4.1.12	Oracle Corporation
Printmade2	NagoSoft, Inc.
ProcessClean 2.35a	ProcessClean
QQ International	Tencent Technology(Shenzhen)...
searchlike	
Searchline-nc	
Secure Holic PNP Plugin	SecureHolic
SignGATE EWS v4.0	
SoftCamp Secure KeyStroke 4.0	
SSI	Korea Contents Network,Inc
TouchEn firewall32	
TouchEn Key for Application	SoftSecurity Co., Ltd.
TouchEn key with E2E for 32bit	RaonSecure Co., Ltd.
Trust Reader Web 버전 1.1.1.2	SGA Co.,Ltd. RedBC
TrustNET WebToolKit for SecuiSFNCOM	UNETsystem
ucloud	Kt
VB Runtimes Pack, release 7	http://www.tnk-bootblock.co.uk
Verain(Wizvera Mozilla Plugin) - 1,0,2,8	Wizvera
Veraport20(보안모듈 관리 프로그램) - 2,0,0,21	Wizvera
window connector	GOMSEK.COM
Window Search	
WindowAdvertisement	WindowAdvertisement
Windows Desktop BT Icons Ver 5.1.1.4	
windows for smart install	Korea Contents Network,Inc
Windows Internet Explorer KoreanKeyword V.2.2.1.1	
Windows Keymoa Patch Drivers	MS Media Corp.

Windows Server 2012 Essentials KOR MP	Microsoft Corporation
WindowsTab Uninstall	
WiseGrid ActiveX	
Wordkey Reader	adnet
WPS Office ??版 (9.1.0.4885)	Kingsoft Corp.
XecureExpressI	
XecureWeb Control	SoftForum Co., Ltd.
XecureWeb UnifiedPlugin	
yessign7 ActiveX Control	금융결제원
네이버 ActiveX 가이드	NAVER Corp.
腾讯微云	腾讯科技(深圳)有限公司
微软拼音简捷 2012 流行词汇更新 (KB2723161)	Microsoft
百度软件中心助手 1.3.0.41	Beijing baidu Netcom science a...
삼성생명 증명서발급	MarkAny Inc.
알집 9.0	ESTsoft Corp.
알툴바 3.47	ESTsoft Corp.
알툴즈 업데이트	ESTsoft Corp.
인증서 로밍 클라이언트 (1.14.724.1)	BTWorks, Inc.
포커스온 이미지 뷰어	Pintosoft
한게임 자동 인스톨러	
홈케어	HomeCare
휴대폰인증서(보관)서비스	

QQ International은 중국에서 많이 사용하는 메신저 프로그램이다

프로그램 리스트를 간략하게 분류 및 정리해 보았다.

압축 관련 프로그램

인터넷 보안 (뱅킹) 로그인에 사용되는 모듈 프로그램

인증서 관련 모듈 (보관 서비스, 로밍서비스, 증명서 발급)

자료 공유를 위한 클라우드 서비스와 메신저
- 다음 스마트 업로더 Active X
- Evernote
- Google drive
- ucloud
- 텐센트 클라우드
- Baidu cloud
- QQ international

Eyagi 2.0 : 알뜰폰 http://eyagi.co.kr 관련된 모듈

Oracle VM Virtubox : 가상화 서버를 생성할 수 있는 프로그램 (Vmware와 유사)

Process clean : 시스템 정보 및 레지스트리 관련 툴

WPS OFFICE : 중국에서 제작된 무료 OFFICE 프로그램 (MS-OFFICE 기능이라고 보면 됨)

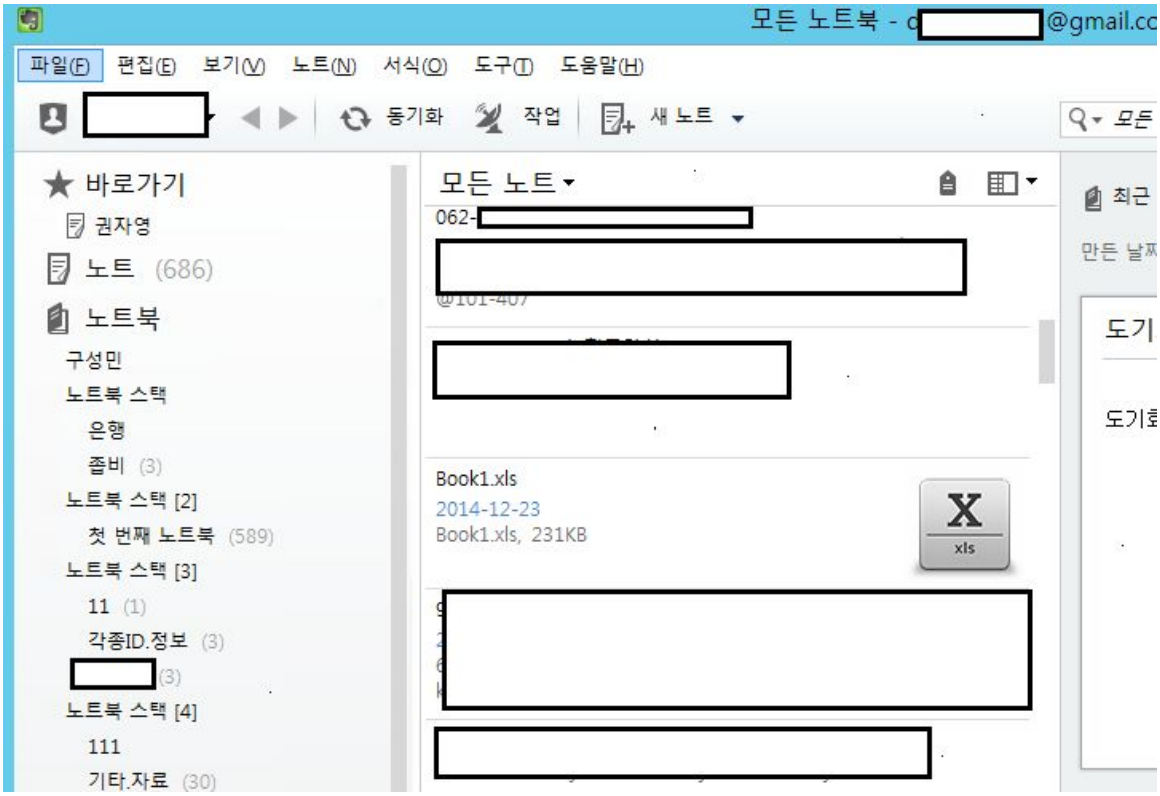
뱅킹 관련 프로그램이 많이 설치돼 있었으며 중국에서 사용하는 메신저,

클라우드 등의 프로그램도 설치되어 있었다.

Evernote

설치된 프로그램에 혹시나 자동 로그인 설정이 되어 있는 것이 있는지 확인하였으며

Evernote라는 프로그램에 자동 로그인 기능이 활성화되어 있었다



[스마트폰 및 PC에서 메모나 이미지 등을 효율적으로 보관하기 위한 노트 프로그램]

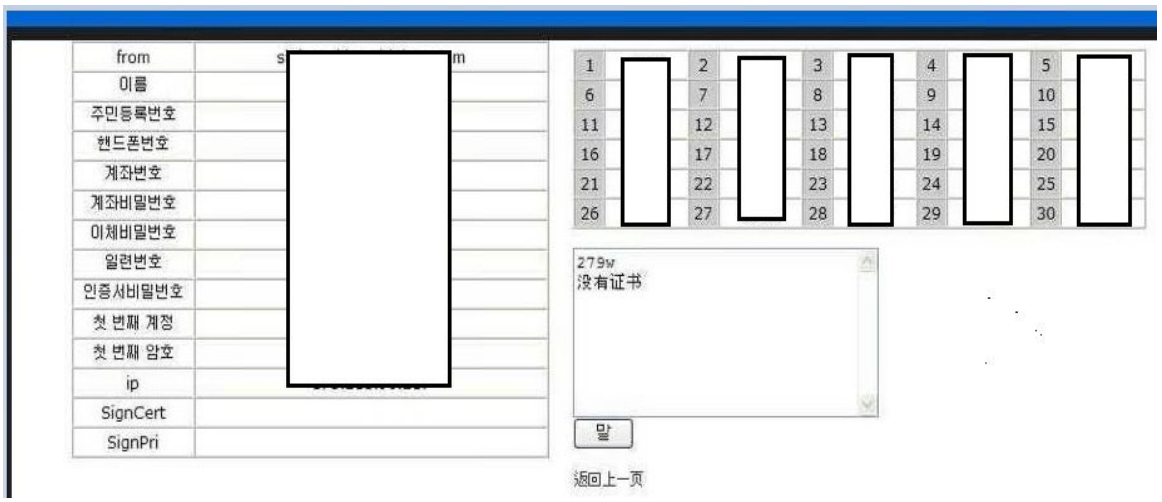
686건의 자료들이 노트에 저장되어 있으며 개인 정보들이 보관되어 있었다.

에버노트를 통해서 정보를 업데이트 및 공유하였을 것으로 파악된다

그렇다면 저장된 개인 정보는 무엇이 있는가? (종류별 분류를 해보았다)

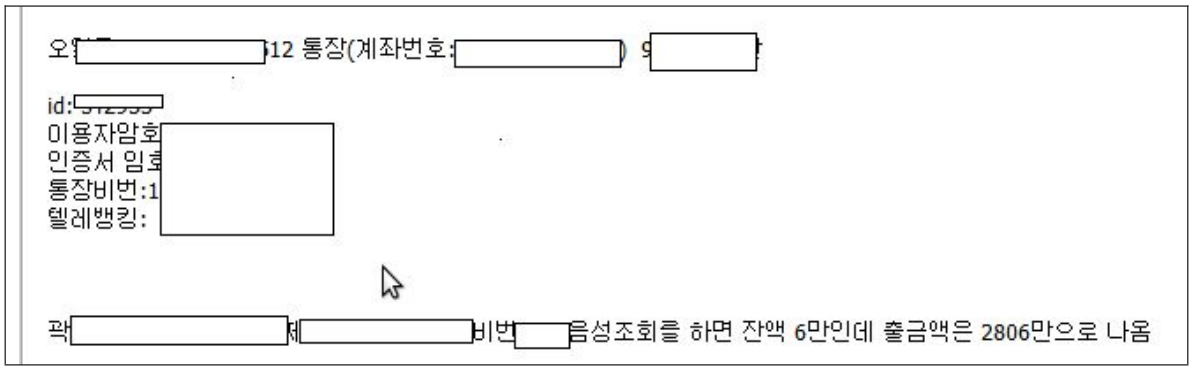
개인 인터넷 뱅킹 정보 (약 241건)

이름, 주민등록번호, 핸드폰번호, 계좌번호, 비밀번호, 일련번호, 인증서 비밀번호, 계정, 보안코드, ip 정보



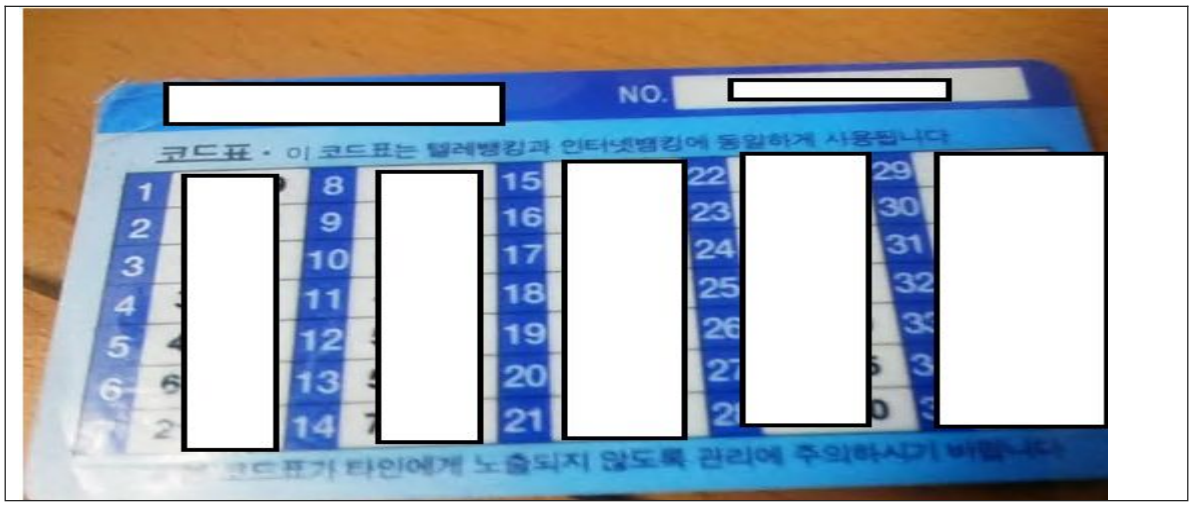
뱅킹 보안 설정이 없는 상태라면 공인 인증서만 있으면 이체 가능하리라 본다

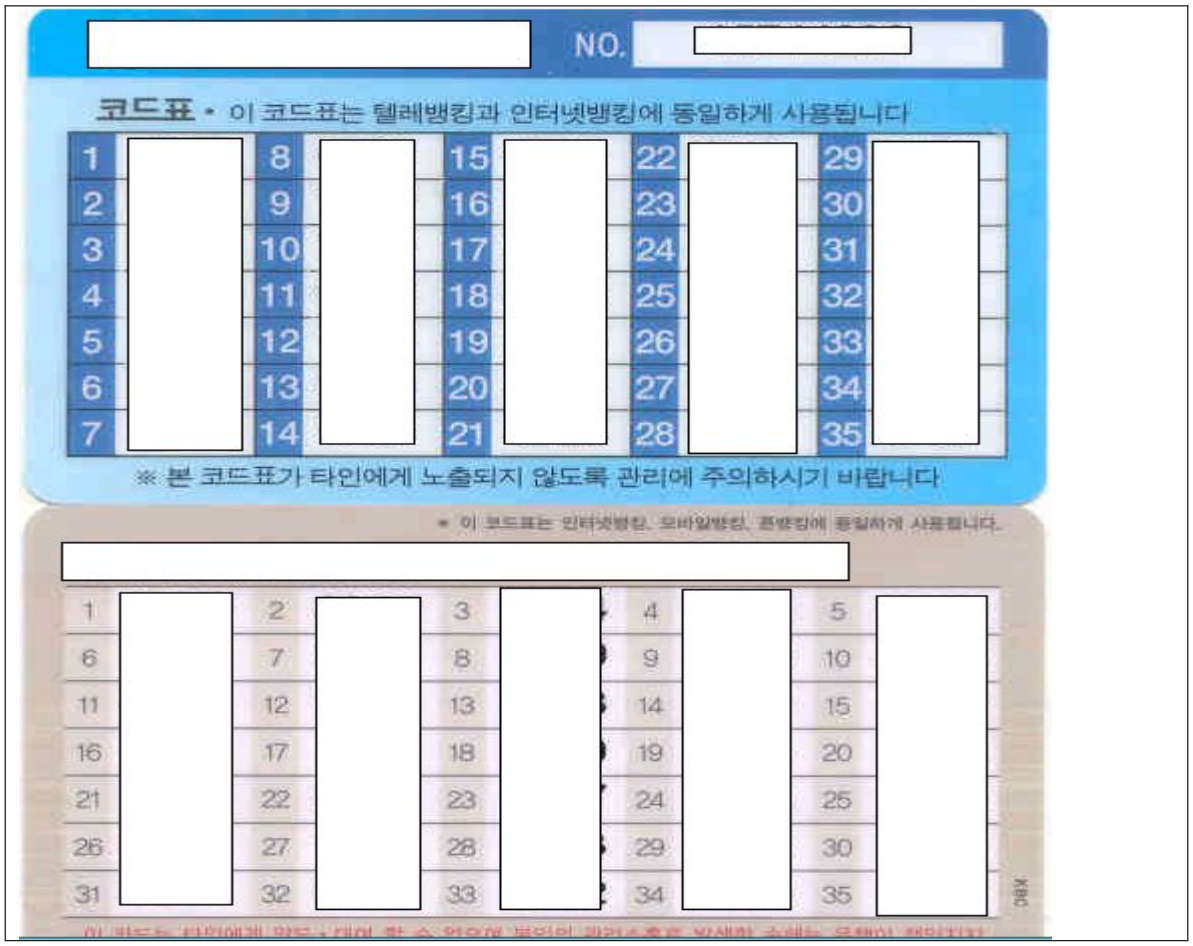
텔레뱅킹 정보 (2건)



해당 서버에는 텔레뱅킹 정보도 소수 포함되어 있었다

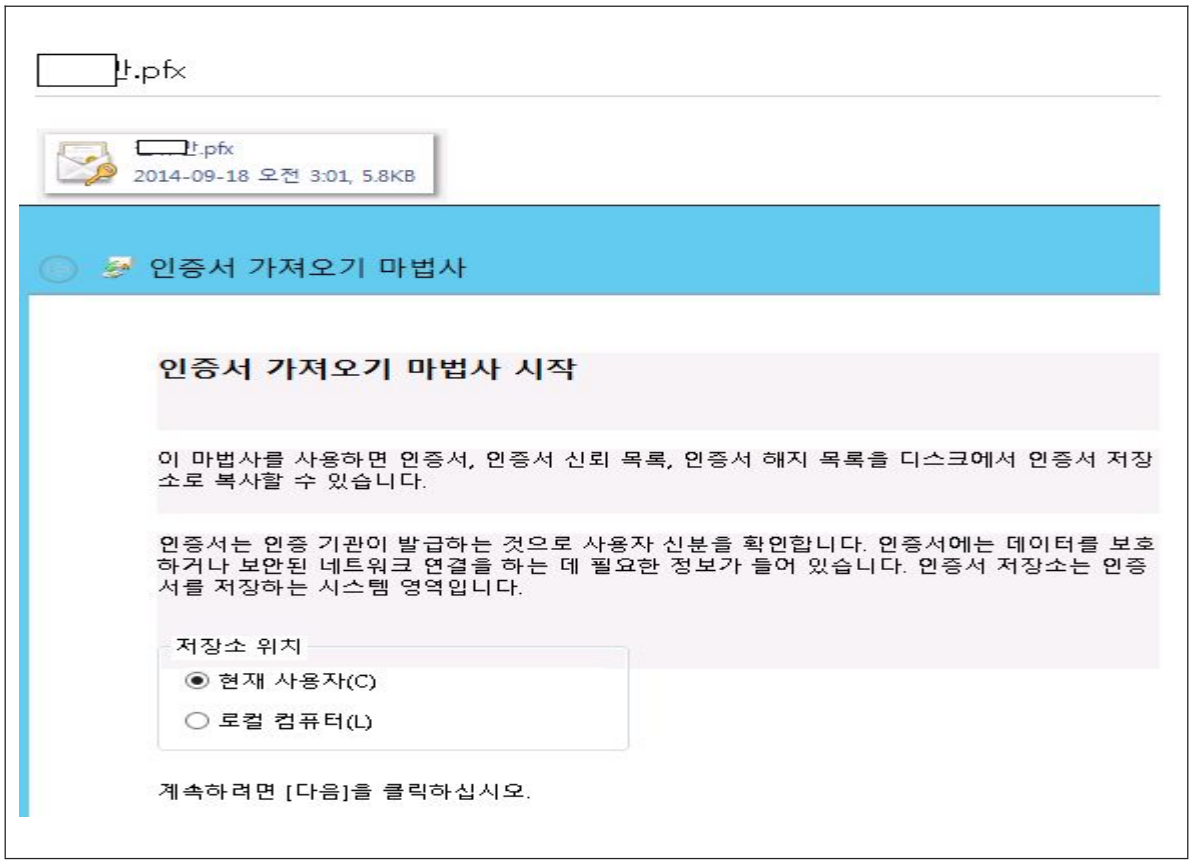
뱅킹 보안카드 이미지 파일 (약 10건)

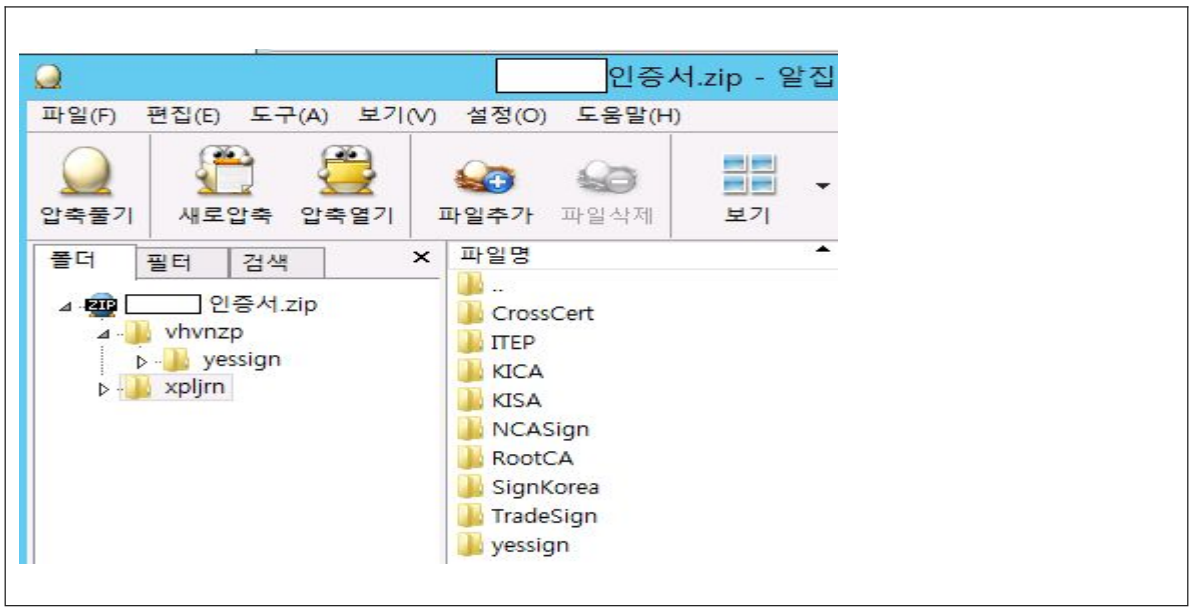




보안카드 이미지 파일을 저장매체에 저장하다가 유출된 것으로 파악된다

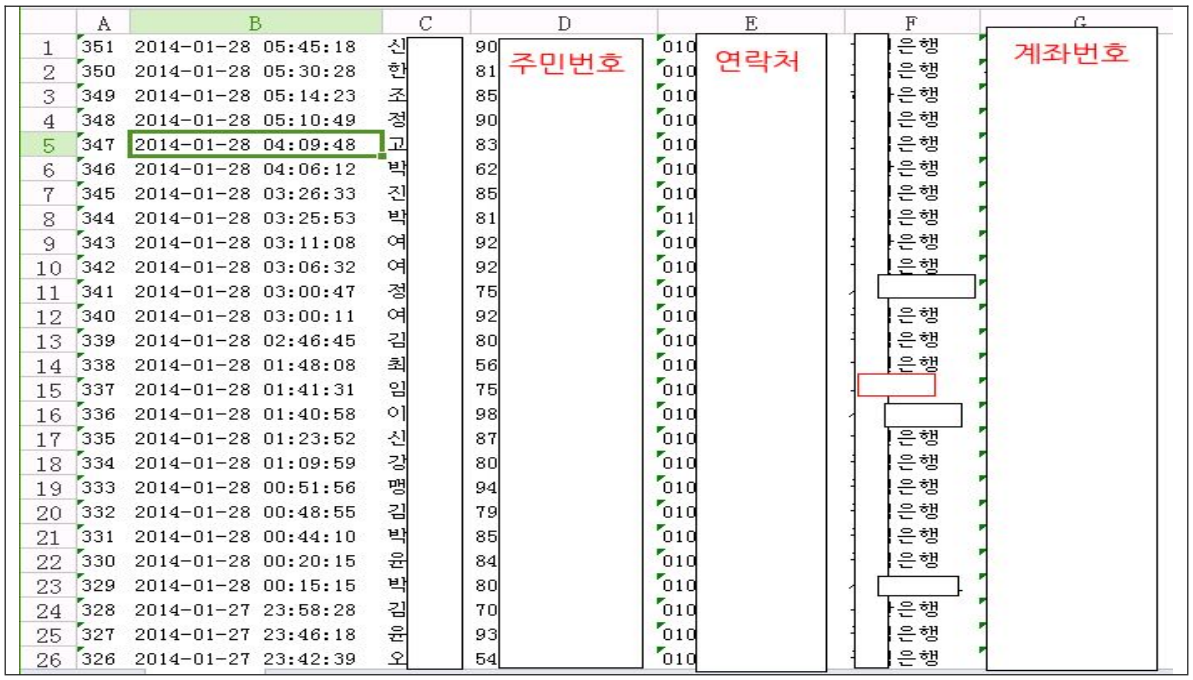
공인인증서 파일 (약 234건)

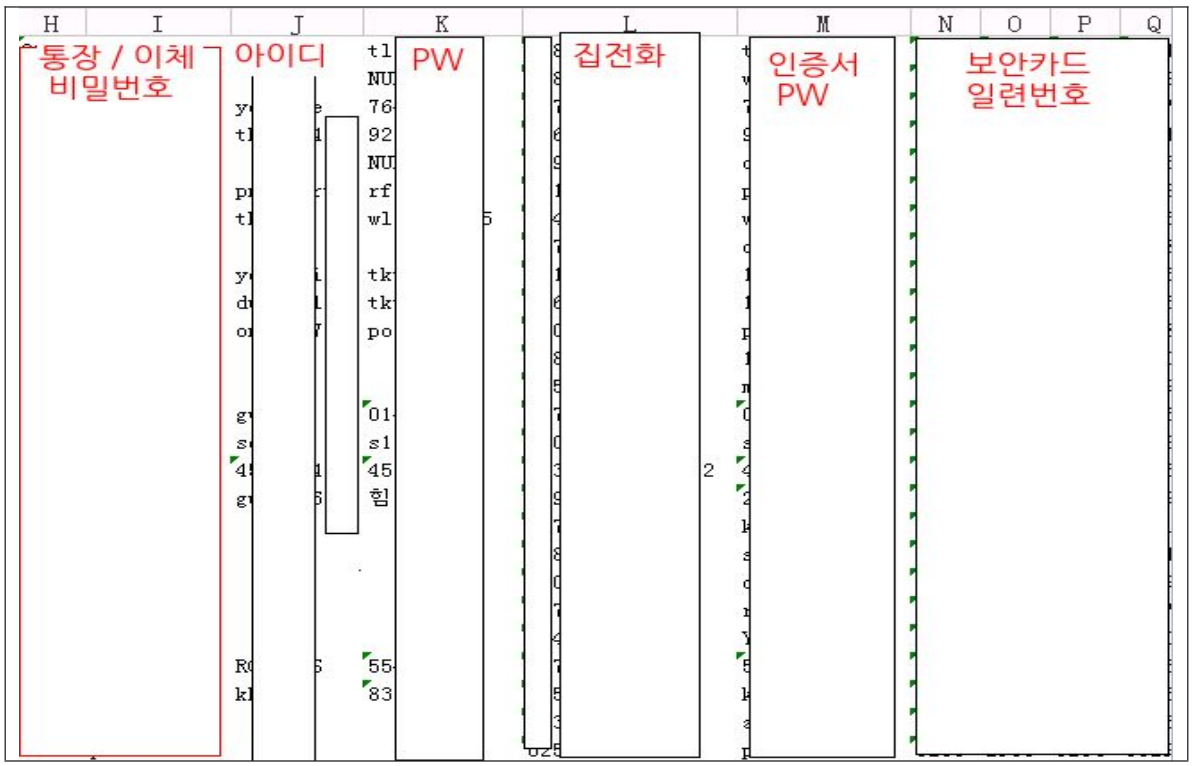




개인 공인인증서 유출은 꽤 심각해 보인다

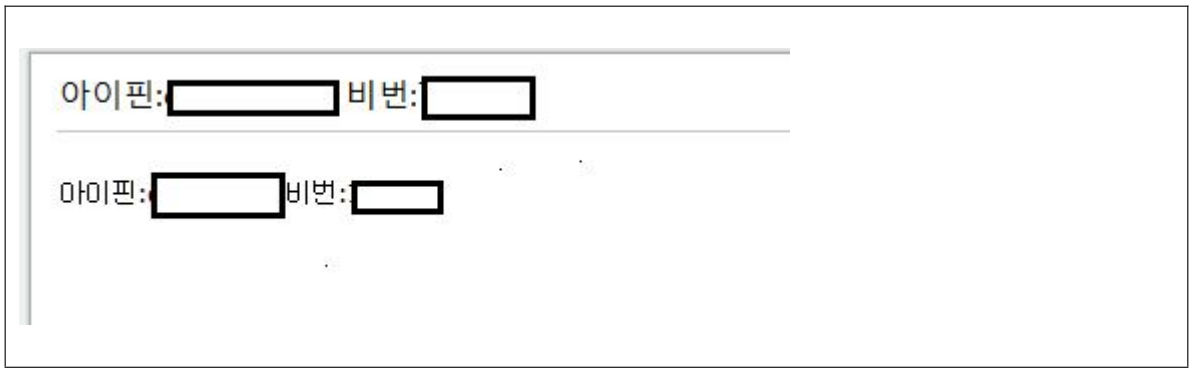
엑셀파일로 정리한 개인 계좌정보 (약 531명)





“신X, 농X, 국X, 외X, 삼X, 하X, 우X, 새X, 기X” 은행 사용자

아이핀 계정 정보 (약 15건)



사용자 실명인증 및 아이디/패스워드 찾기가 가능하므로 유출되면 치명적이다

이동통신사 계정 (약 6건)

전화 착신이 목적이었을 텐데 수집된 양은 많지 않았다

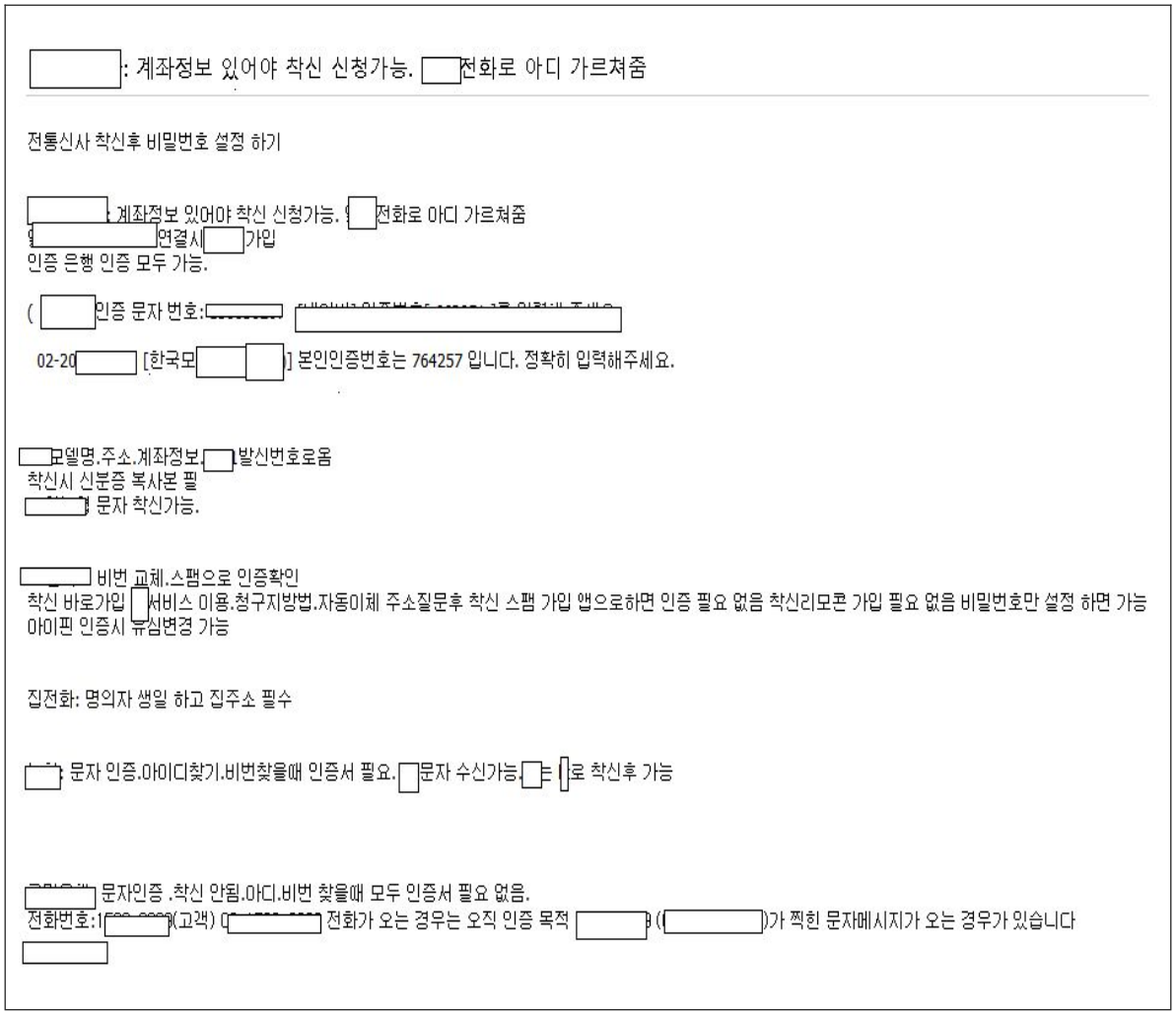
이유는 아래와 같지 않을까 생각된다.

1. 몇 년 전 착신으로 인한 뱅킹 사고로 인해 이미 이슈화되었으며

2. 사용자들의 스마트폰 데이터 사용량 확인으로 자주 로그인 확인

3. 은행에서 착신된 전화로는 인증이 안되는 은행이 많기 때문

전화 와 휴대폰을 착신하기 위한 메모들이 아래와 같이 저장되어 있었다



: 계좌정보 있어야 착신 신청가능. 전화로 아디 가르쳐줌

전통신사 착신후 비밀번호 설정 하기

: 계좌정보 있어야 착신 신청가능. 전화로 아디 가르쳐줌
연결시 가입
인증 은행 인증 모두 가능.

(인증 문자 번호:

02-20 [한국모] 본인인증번호는 764257 입니다. 정확히 입력해주세요.

모델명.주소.계좌정보. 발신번호로옴
착신시 신분증 복사본 필
문자 착신가능.

비번 교체.스팸으로 인증확인
착신 바로가입 서비스 이용.청구지방법.자동이체 주소질문후 착신 스팸 가입 앱으로하면 인증 필요 없음 착신리모콘 가입 필요 없음 비밀번호만 설정 하면 가능
아이핀 인증시 유심변경 가능

집전화: 명의자 생일 하고 집주소 필수

문자 인증.아이디찾기.비번찾을때 인증서 필요. 문자 수신가능 로 착신후 가능

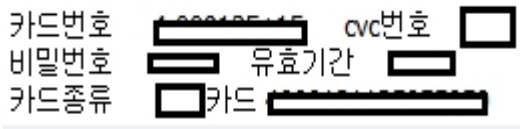
문자인증 ,착신 안됨.아디.비번 찾을때 모두 인증서 필요 없음.
전화번호: (고객) 전화가 오는 경우는 오직 인증 목적 ( )가 찍힌 문자메시지가 오는 경우가 있습니다

통신사별 착신하는 방법과 필요한 서류, 그리고 착신된 전화로

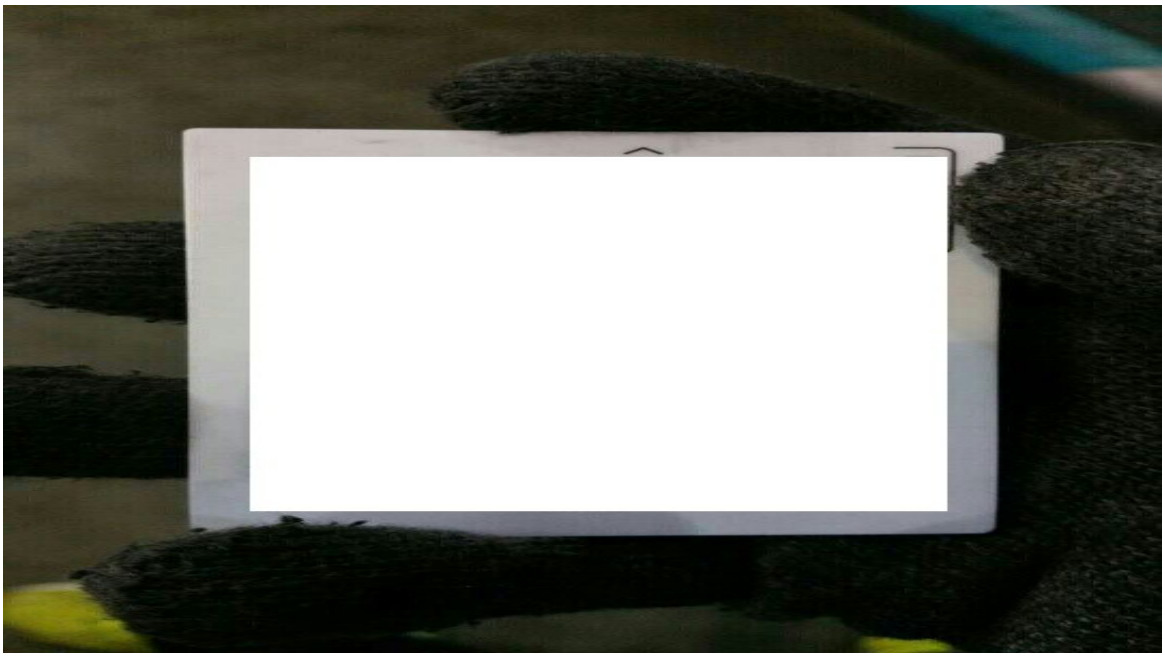
인증 가능한 은행 등의 정보들이 저장되어 있다

신용카드 정보 (약 28건)

카드 번호, 카드 비밀번호, 유효기간, cvc 코드



신용카드 이미지 파일 (약 31건)



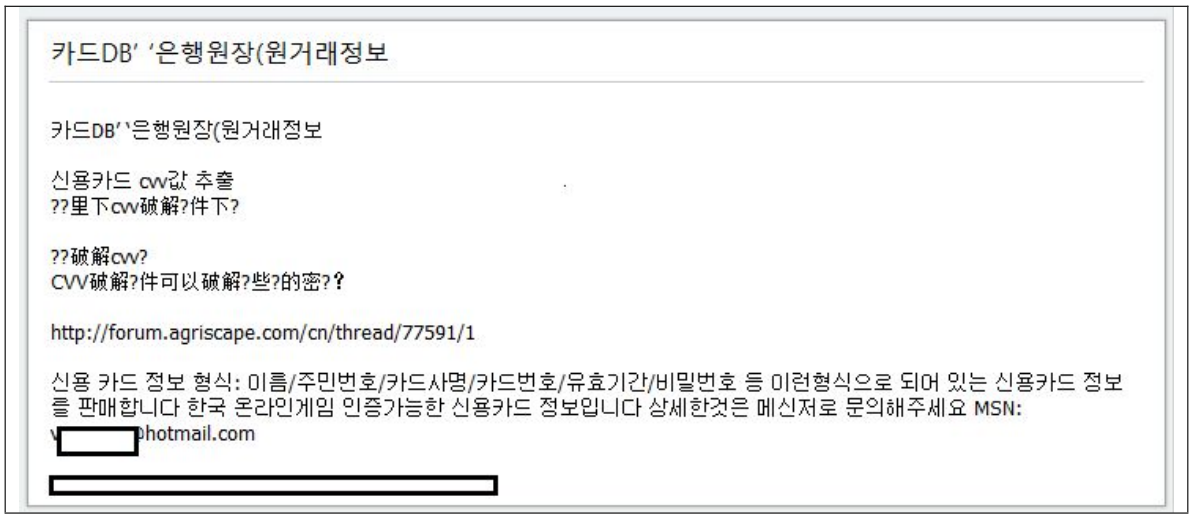
주유소에서 고객 카드를 카메라로 찍어 저장한 모습

배경화면과 검은 장갑이 해당 장소는 주유소라고 말해주고 있다

실제 대전에서 아래 링크와 같은 사건이 발생한 적 있다

http://www.daejonilbo.com/news/newsitem.asp?pk_no=1108908

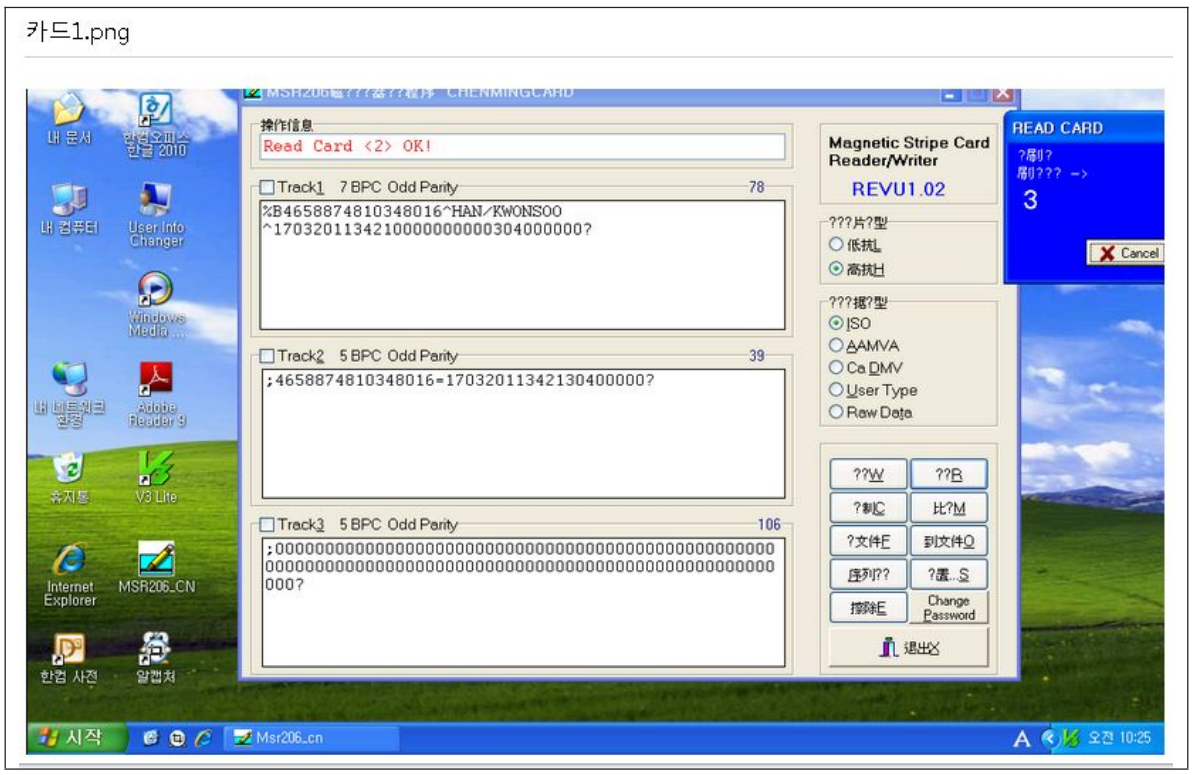
이렇게 작업된 카드 정보들은 수집되어 판매가 되고 있는 거래 정보 내역



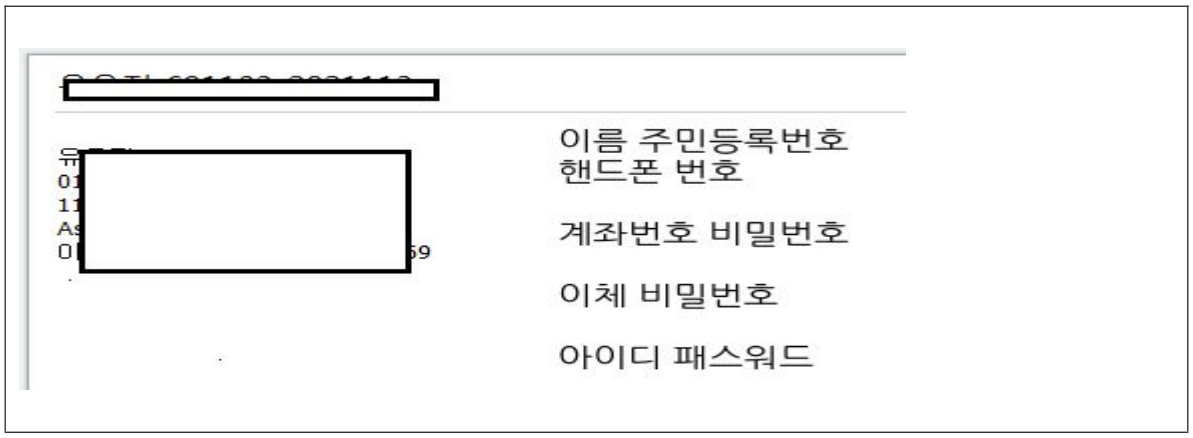
카드 거래 이유 중에 하나가 국내 게임사이트 인증에 사용되는 것 같다

거래만 된다면 다행이지만 아래 프로그램은 카드 복제가 가능하리라 판단되는

마그네틱 카드 READ/WRITER 프로그램의 모습



개인정보 (67건) 과 불완전한 뱅킹정보 (67건)



위 정보만으로는 금전적 이득이 불가능하며 해커집단에서 계속 보이스피싱 및

무작위 대입 등의 방법으로 패스워드를 찾아내려고 노력할 것이다

개인이 자주 사용하는 패스워드도 메신저로 주고받은 메모가 발견되었다

위와 같이 패스워드 패턴 추출 가능한 이유 중 하나는

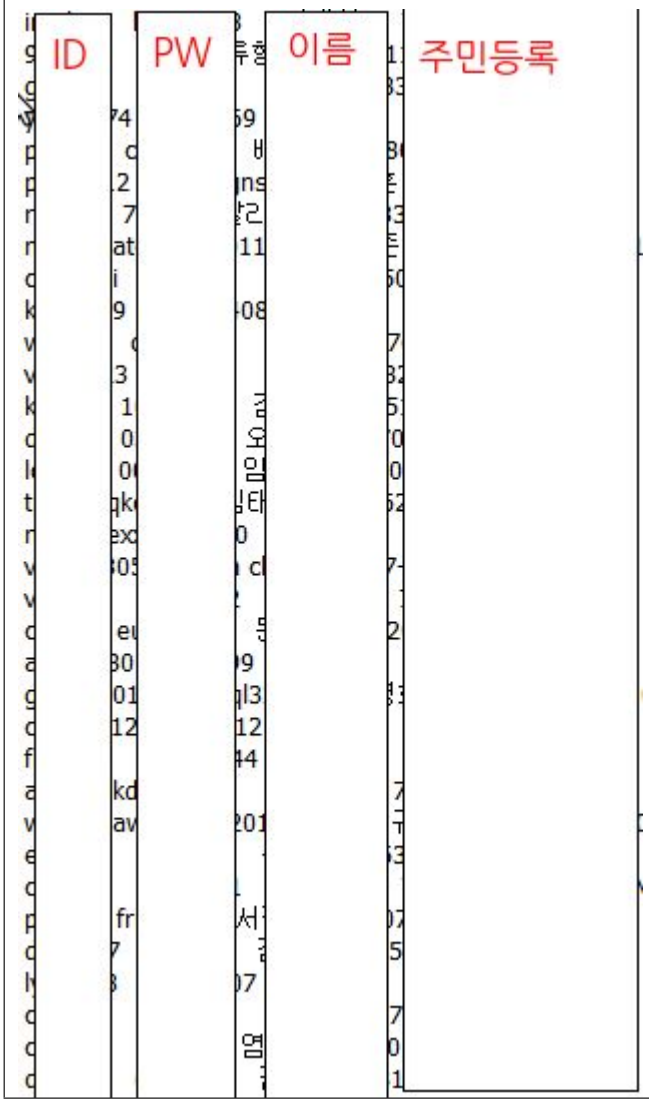
사용자들이 자신의 어떤 신체정보, 주소, 생일, 전화번호 등과 같은

자신의 개인 정보들을 조합하여 패스워드를 만들기 때문이다.

아래를 보면 어떤 사이트에서 유출되었는지 모르겠으나 아이디, 패스워드,

이름, 주민등록번호가 저장되어 있는 파일이다.

아이디, 패스워드, 이름, 주민등록번호 정보 (약 1500건)



유출된 사이트와 동일한 아이디 / 패스워드를 사용하는 경우에는

가입된 또 다른 사이트도 털리게 되는 피해가 발생할 수 있다

무작위 휴대폰 번호 모음

단순 이동통신사 전화번호 텍스트 파일 (약 325,000개 번호)

010 으로 시작 하는 전화번호 모음

위 정보에는 휴대폰 번호만 나열되어 있으므로 용도는 대량 스팸 발송하여

피싱사이트로 유인하기 위해 사용되었을 것이다.

보이스 피싱에 관련된 정보도 다량 수집되어 있었다

대출정보 (약 627명 정보)

대출	주민번호	휴대폰	주소	대출구분	직장명	지점	접수일시	처리상태
이	7	01	경기	사업자				오토
김	6	01	서울	직장인				오토
김	7	01	경기	직장인				오토
박	6	01	전남	직장인				오토
이	5	01	경기	직장인				오토
이	6	01	충북	직장인				오토
주	6	01	강원	직장인				오토
최		01	서울	직장인				오토
전		01	경기	주부				오토
김		01	경기	직장인				오토
정		01	경북	직장인				오토
배		01	경기	직장인				오토
강		01	경기	직장인				오토
박		01	서울	직장인				오토
박		01	서울	직장인				오토
이		01	경기	직장인				오토

위 대출정보를 이용한 보이스 피싱 방법으로 보이는 멘트

1.안녕하세요 햇살론 상담원 ooo입니다
고객님께서 1000만원 신청하신거 맞으시져? ==접수지 본인확인
년이자 월이자 알려줌 상환가능하시겠습니까?
저희는 연이율 14 %이고 1년 동안 사용가능하1년만기시 이자 연체 없으시면
1년단위로 최장 5년까지 연장가능합니다
필요서류는 신분증사본 원초본등본 승인금액부여받으실통장앞면부
최근3개월거래내역서를 보내주시면됩니다
승인금액부여받으실통장은요 어느은행으로하실겁니까
저희는 새마을금고 우체국 제일은행 신협 (국민은행)우리은행 만 거래하고있습니다
고객이 물어보면 (다른은행은 전산상에 저희회사하고 클레인안돼있습니다.=)
또한 통장이 텔레뱅킹가입되셔야만 합니다 왜냐면 사용등록을 하셔야하고 본인자금이라는것을
인증받기위해서 하는겁니다
서류보내실 팩스번호는 저희가 문자로 넣어드릴겁니다. 언제 가능하시겠습니까

2)고객님 보내신 서류를 잘 받았구요 지금 심사과에 넘어갔습니다.심사는 1-2시간정도
걸리시구요 결과가 나오는대로 바로 연락드리겠습니다
(30분뒤 전화해서 심사과과장이 연락오셨는데요 고객님께서 등급이나 사금융쪽에
사용하는 금액 조회건수가 많다고 핑계로이런서류가필요하시더라구요 잔고증명서 요구함
잔고증명서라면 고객님 신청하신대출자금에 20%좌우요구함 직원들나름대로)

3)고객님께서 상환능력을 체크하기위해서 본인이름으로된 잔고증명서를(무조건 부여받을잔고통장이여야만함)
저희한테 보내주셔야합니다
부여받으실은행가셔서 잔고증명서를 떼여주라고하시면 됩니다 다시팩스로 넣어달라고함

4)잔고서 서류 다받고나서 ======= 30분뒤
고객님 신청하신금액이 (얼마)정도 승인되였습니다 빠른시간내에 스마트폰이나 컴퓨터를 이용하셔서
사용등록을 해주세요 그러시면 자금을 바로 이용하실수있습니다.
홈페이지는 심사과에서 고객님 핸드폰에 문자넣어드릴겁니다
사용등록은 언제쯤가능하시죠? 홈페이지 접속하시면 오른쪽창에 진행상황이라고있는데요 클릭하시고
성함하고 주민번호입력하시면은 승인금액이 나옵니다 .(초록색확인버튼 누르고 사용등록절차를함)

알고도 속는 보이스피싱 멘트 메모들도 알아보자

이동통신사 보이스 피싱 1

박[redacted] 고객님 안녕 [redacted]텔레콤 [redacted]담당 [redacted] 팀장 입니다..

다름이 아니고 어제 저녁 즉 6월 3일 저녁 7시경 [redacted]

[redacted]에 위치한 [redacted]텔레콤 [redacted] 대리점을 방문한 사실이

있으신지?..

고객님의 신분증을 제시하고 휴대폰 개통 신청이 접수 되었는데

현제 고객님의 거주지와 강원[redacted]는 거리가 너무 멀어서

일단 개통 보류를 하고 ,고객님께 확인후 개통을 도와드리려고 전화를 드렸습니다..
고객님 직접 방문하여

개통을 신청 하셨는지 확인하기 위해 연락 드렸습니다.

개통 사실이 있으신가요?

제육안으로 확인 되진 않았지만 현제 서류 상으로 보아도

고객님의 신분증을 위조하여 지방 대리점을 다니며 개통을

시도하는것으로 포착 되고 있습니다...

저의 [redacted]텔레콤 에서는 고객님의 피해를 최소화 하기위해

자체 신규개통 블라인드 시스템을

도입하고 지금 부터 ..[redacted]고객님은

본인 외 어떤 대리인도 대신하여 휴대폰 개통을

할수 없게 조치에 동의 하시는거죠..

네 감사 합니다..그럼 님 본인 확인절차를 하겠습니다..

현제 이용 중이신 휴대폰 번호 010 [redacted]

맞으세죠?[redacted]

그럼 본인의 신분증 발행일 또는 운전 면허증의 면허 번호를

부탁 드립니다. 네 감사 합니다.. 확인되셨구요
앞으로도 명의도용이나

부정개통 피헤 없길 바랍니다...고객님 저는 상담원[redacted]

이동통신사 보이스피싱 2

고객님..

고객만족 XX 입니다. 김팀장 입니다.

다름이 아니고 오늘 고객님 휴대폰 분실정지건 때문에 전화드렸습니다

고객님 본인이 직접 하시거나 가족 분중에 실수로 접수된것 아니신거죠?

그럼 전혀 모르는제3의 인물이 XXX 고객님의 개인정보를 취득해서 본인동의없이 저지른 행위로 판단되는데..

고객님의 개인정보를 알고 있기에 또 같은일이 발생할수도 있기에 이런 상황에서는
개인정보 블라인드라는제도가 있습니다.

이제도는 본인또는 개인정보를 알고 있는 타인이라고 해도 미리 설정해 두신 비밀번호를 모른다면 변경,해지.또는 어떤 작은 일이라도 할수 없이 보호안전 이라고 보시면 됩니다.

이용 방법은 앞으로 매장을 방문을 하시던 ars고객센터를 이용하셔도 안내맨트후에 비밀번호를 누르라는 맨트가 나오실 껍니다..

그럼면 설정하신 비밀번호를 누르셔야 다음진행이 됩니다.. 네 그럼 설정하실 비밀번호를 4자리를 말씀해 주세요...

만약에 비밀번호를 기억하시지 못할 때는 대리점 방문은 안되지고요 각 지점을 신분증을 지참 하셔서 비밀번호 변경을하셔야 합니다.

3077 번호는 음성사서함 또는 개인인증 번호로 설정 되어있어서 같은 번호는 안되시고요..다른번호 부탁 드립니다.

네 등록 되셨구요..그럼 앞으로는 좀전에 설명해드린데로 이용하시면 됩니다..
혹시궁금하시 사항이 있으신가요? 네감사 합니다..

고객 만족 XX 담당 김XX 입니다..감사 합니다.

카드사 보이스 피싱 1

회원님 안녕하세요
XX카드 정보유출에 의해 회원님들에 유출 여부를 진단해 드리고 있습니다.
회원님이 맞으신다면 지금 바로 개인정보 유출 여부를 알려드리겠 습니다.

XX카드를 소유 하고 계신 고객님 맞으시면 "예"또는 "아니요" 로 답변 부탁드립니다.

소유하고 。계신 카드 번호 마지막 4자리와
CVC 카드뒷면에 숫자 7자리 중에 마지막 숫자 3자리를 적어서 보내주시면

바로 결과를 알려 드리겠습니다.

카드사 보이스 피싱 2

답변 부탁 드려요. 전XX 고객님..
주유상품권은 자택으로 베송해 드리겠습니다
자택주소 : 서울시 XX구 XX동 맞으시죠.?

연락처: 010 - **** - 0*1* 맞으시죠.?

XXX님이 현제 보유하고 계신 저의 XX카드

카드번호: **** - **1* - 2*9* - *0.?? ㅊㅍㅍ 102
마지막 2자리 숫자 부탁 드립니다.
CVV: 카드 뒷면 마지막3자리 숫자 부탁 드립니다
그리고 마직막으로 카드의 비밀번호 뒤에 2자리 숫자 부탁 드립니다..
이것으로 XX카드 고객정보 유출로 인한 보상지원 안내를 끝으로 말씀드렸던
"주유권 3만원" 권을 자택으로 발송해드리겠습니다.
질문에 답해주신 XXX 고객님께 다시한번 감사 드립니다.
XX카드 고객만족 XX 이였습니다.

대출정보를 이용한 보이스 피싱

안녕하세요. 저희는 XX XX XX 지원 센터 입니다.
금융권 관련대출 연체나채 무로 인하여 어려움 겪고 있는 분들 정부에서 지원해주는 제도로 원금에 일부와 이자를 탕감해주는 제도가 있어서 연락 드렸습니다.
혹시 현재 채무로 인하여 추심중에 계시거나 은행권 거래 정지, 재산 압류 압류 들어와 있지는 않으신지요?
(네)
개인회생 제도로써 도움을 드리려고 연락 드렸습니다.
채무금액이 천만원 이상이신분들에게 개인회생 제도가 적용되고 있습니다.
채무금액이 얼마나 되시는지요?
(천만원이상)
이후 상담일지 에 있는 부분을 질의응답 한다.

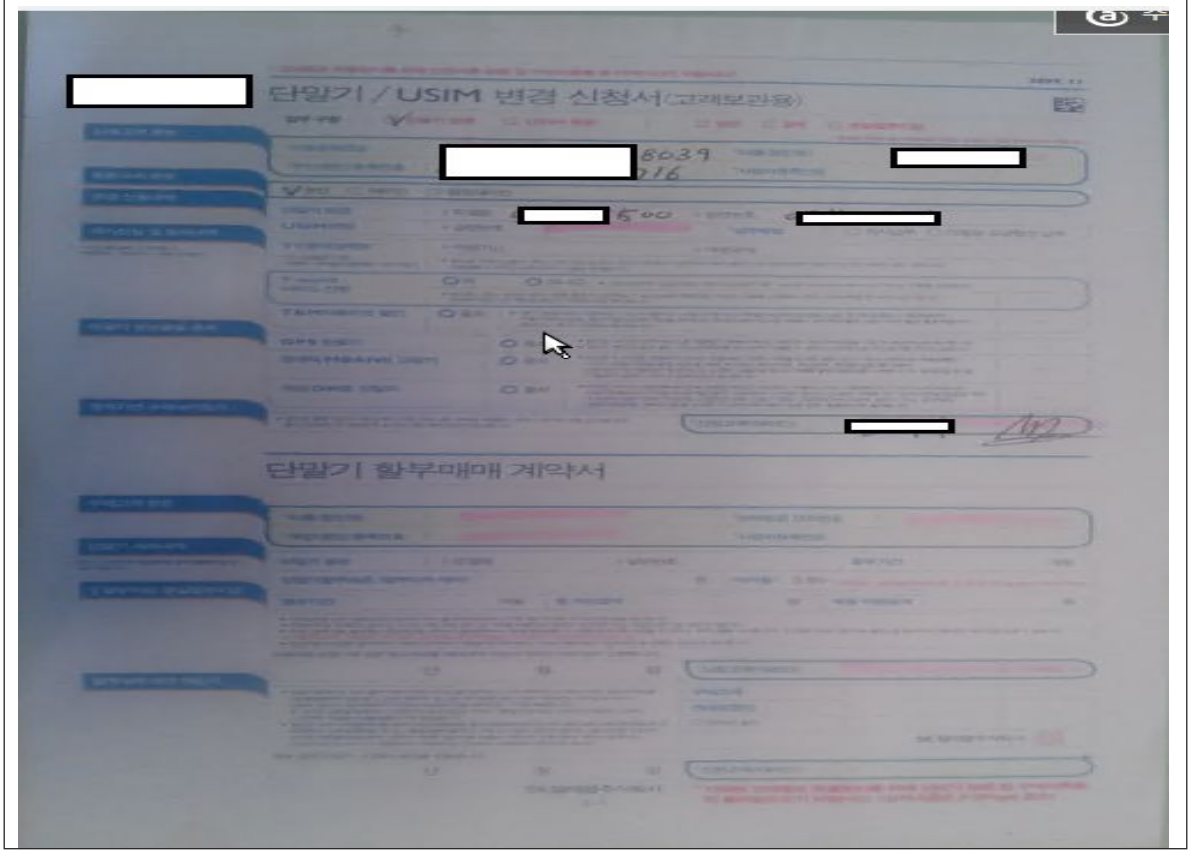
이미 전화한 상대방의 모든 신상 금융 정보를 알고 있으며

전화를 건 목적은 중요한 몇 개의 정보를 더 알아내기 위함이다

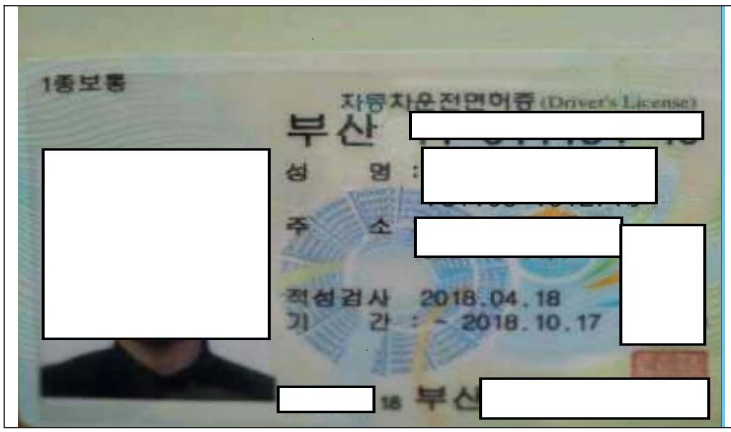
이미 알고 있는 정보를 던지고 필요로 하는 정보를 얻어내는 패턴이다

단말기 / USIM 변경 신청서 (2건)

신청서 2건 (사용자 이름 : 정XX, 원XX)



신분증 스캔본 4개 (한국 2개, 중국 2개)



불법 대포폰 용도로 사용하고 있을 거라 판단된다

도용한 명의로 가입한 사이트로 보이는 정보 (7건)

권XX, 전XX, korXXX, 서XX, 정XX, 박XX, 최XX

http://www.olleh.com/ OLLEH.COM [올레닷컴] 국내최초! 1.8GHz 황금주파수 광대역 LTE-A

https://www.annextele.com:440/member/regiinput.asp ANNEXTELE.COM 대한민국대표 MVNO - 에넥스텔레콤 2.0

https://www.wooriepro.com/ WOORIEPRO.COM 우리은행 전자입찰시스템

https://www.g-pin.go.kr/jsp/connect/saml/loginid/login_popup.jsp G-PIN.GO.KR 아이핀 - 인터넷주민번호대체수단

https://aname.siren24.com/ugp/jsp/ugp_id_j01.jsp SIREN24.COM 메인화면 | 아이핀

http://www.olleh.com/ OLLEH.COM :: 만족 발로 뛰겠소 dododo olleh ::

https://my.qook.co.kr/my/reg/ktindex.php QOOK.CO.KR :: 고객만족, 뛰고 또 뛰겠소 dododo olleh ::

ttps://cert.vno.co.kr/IPIN/member.cb VNO.CO.KR 아이핀 - 인터넷주민번호대체수단

http://center.kbiz.or.kr/EP/web/kfsb/member/KEP_Member_Regist.jsp KBIZ.OR.KR Kbiz-"HOPE21 중소기업중앙회"

78 https://www.safebill.co.kr/etax/index.jsp SAFEBILL.CO.KR 전자세금계산서 - SafeBill

https://www.qmembers.com/oc/kuti/OCFK_UTI_login.jsp QMEMBERS.COM Q멤버스_기아자동차 오너를 위한 멤버십 서비스

http://www.tworld.co.kr/jsp/fla_index.jsp TWORLD.CO.KR 생각대로 이루어지는 세상 T world

31 http://www.hyundaicard.com/um/ID461000_01HA.do HYUNDAICARD.COM 현대카드

http://www.tworld.co.kr/jsp/common/loginout/view/cm8_login_page.jsp TWORLD.CO.KR 생각대로 이루어지는 세상 T world

ttp://www.tworld.co.kr/jsp/common/loginout/view/cm8_login_page.jsp TWORLD.CO.KR 생각대로 이루어지는 세상 T world

http://internet.qook.co.kr/login/login.php QOOK.CO.KR QOOK 인터넷

http://www.megapass.net/index.php MEGAPASS.NETQOOK 인터넷

2 http://www.wooribank.com/ WOORIBANK.COM 우리은행

http://nid.naver.com/nidlogin.login NAVER.COM 메일 쓰기 :: 네이버 메일

http://www.giro.or.kr/index.giro GIRO.OR.KR 빠르고 간편한 통합납부서비스 인터넷지로

http://www.hanabank.com/online/banking/index.jsp HANABANK.COM Intelligent Banking - HanaBank.com[15-034]

http://www.ibk.co.kr/login/login.jsp IBK.CO.KR 기업은행[2A] - Login

http://www.show.co.kr/index.asp SHOW.CO.KR 세상에 없던, 세상이 기다리는 SHOW

그냥 우리가 알고 있는 사이트는 다 가입되어 있다고 봐도 무방하며

실제 위 도용된 명의 중 하나가 우리 사이트에 가입신청하여 서비스를

이용하기도 하였다

금융권 ARS 전화번호

농협 1544-2100 / 1588-2100

하나 1599-1111

신한 1577-8000 카드사 1544-8800

국민 1599-9999 / 1644-9999 / 1588-9999

우리 1599-5000 / 1588-5000

부산 1588-6200

기업 1566-2566 / 1566-2588

광주 1588-3388

제일 1588-1599

외환 1588-3500

씨티 1588-7000

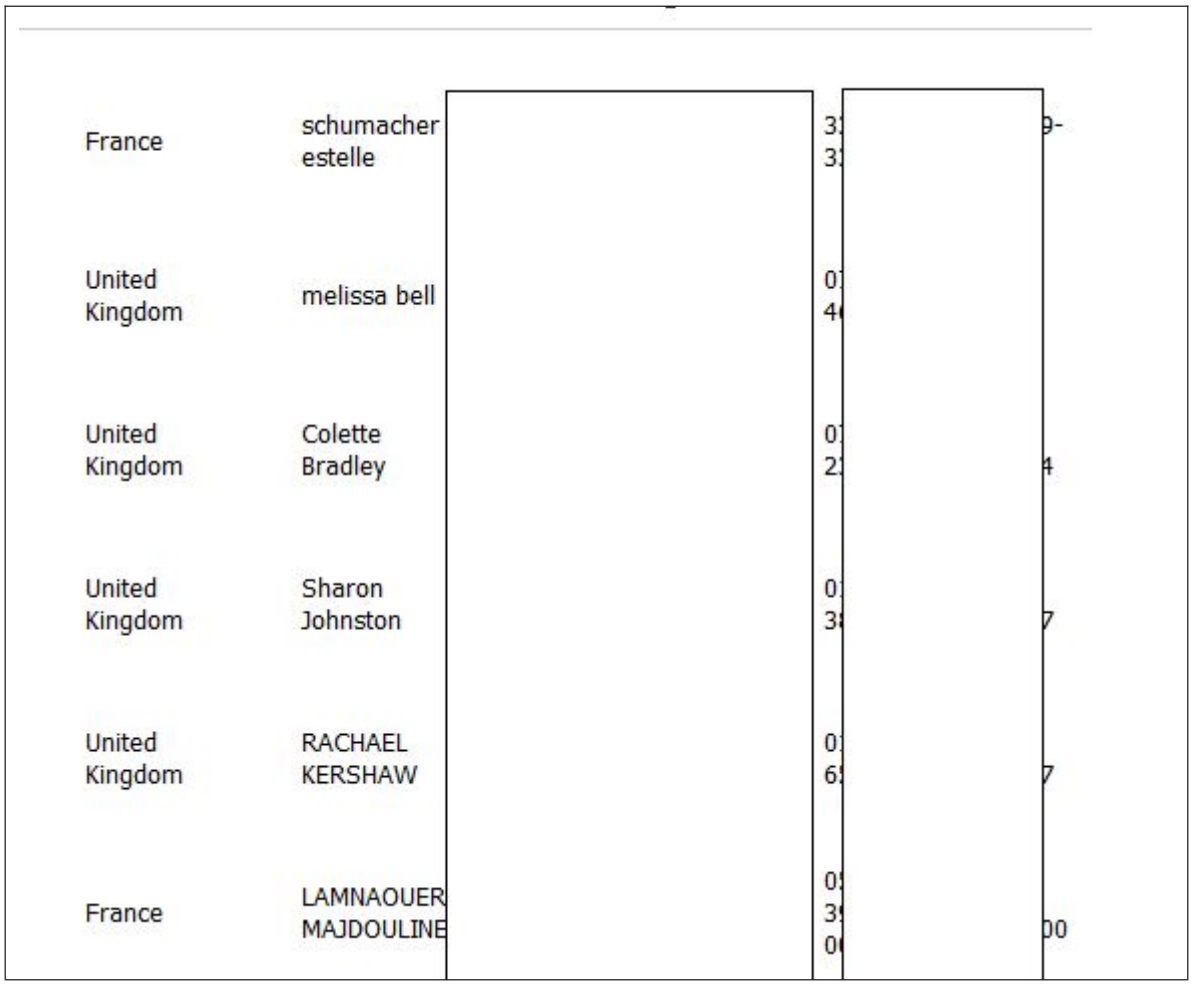
새마을 1599-9000

위 은행사 이외 카드회사, 보험회사 등의 전화번호가 저장되어 있었다

실제로 보이스 피싱이나 취득한 금융 개인 정보를 활용하기 위한

문의 전화를 하였던 건 아니었을까 조심스레 유추해본다

해외 개인 정보 (31건)



France	schumacher estelle	3 3		9-
United Kingdom	melissa bell	0 4		
United Kingdom	Colette Bradley	0 2		4
United Kingdom	Sharon Johnston	0 3		7
United Kingdom	RACHAEL KERSHAW	0 6		7
France	LAMNAOUER MAJDOULINE	0 3 0		00

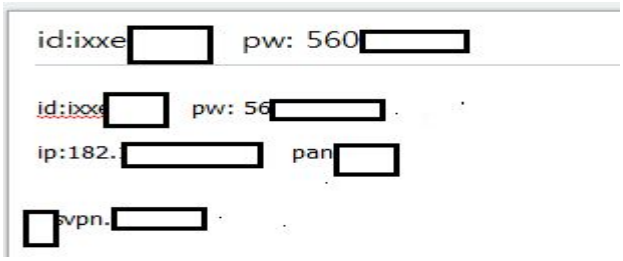
나라, 사용자 이름과 일련번호로 이루어진 2개의 필드값을 가지고 있었는데

어떠한 용도일지는 확실치 않다

개인 정보를 불법 취득하기 위해 사용하였던 서비스나 자원들

VPN 계정 정보 (2개 계정)

국내 VPN 서비스 주소 / 아이디 / 패스워드



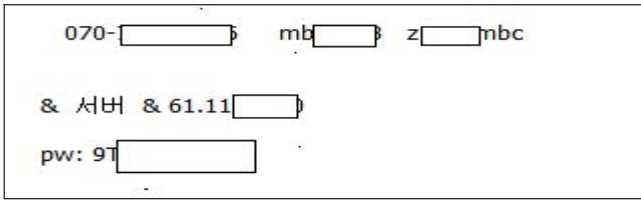
VPN 서버는 주로 해커들이 자신의 아이피를 감추기 위해 사용된다

윈도우 서버 계정 정보 (4개 계정)

IP Address XXX
x

윈도우 서버는 원활한 자료 공유를 위해 사용할 가능성이 높다

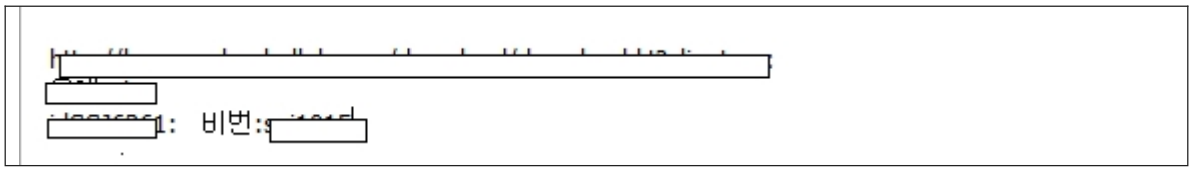
070 VOIP 전화기 계정 정보 (3개 계정)



070 인터넷 전화 특성상 아이피 추적이 힘들기 때문에

보이스 피싱 용도로 사용되었을 거라 추정됨

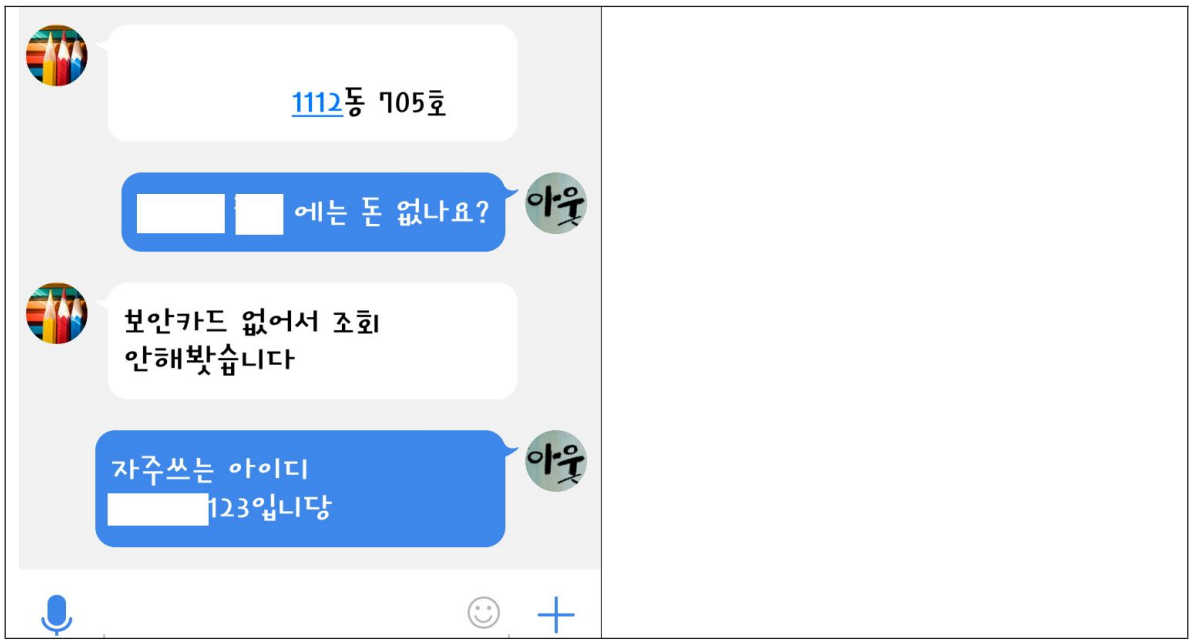
클라우드 계정 (1건)

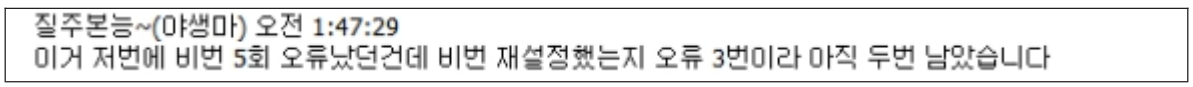


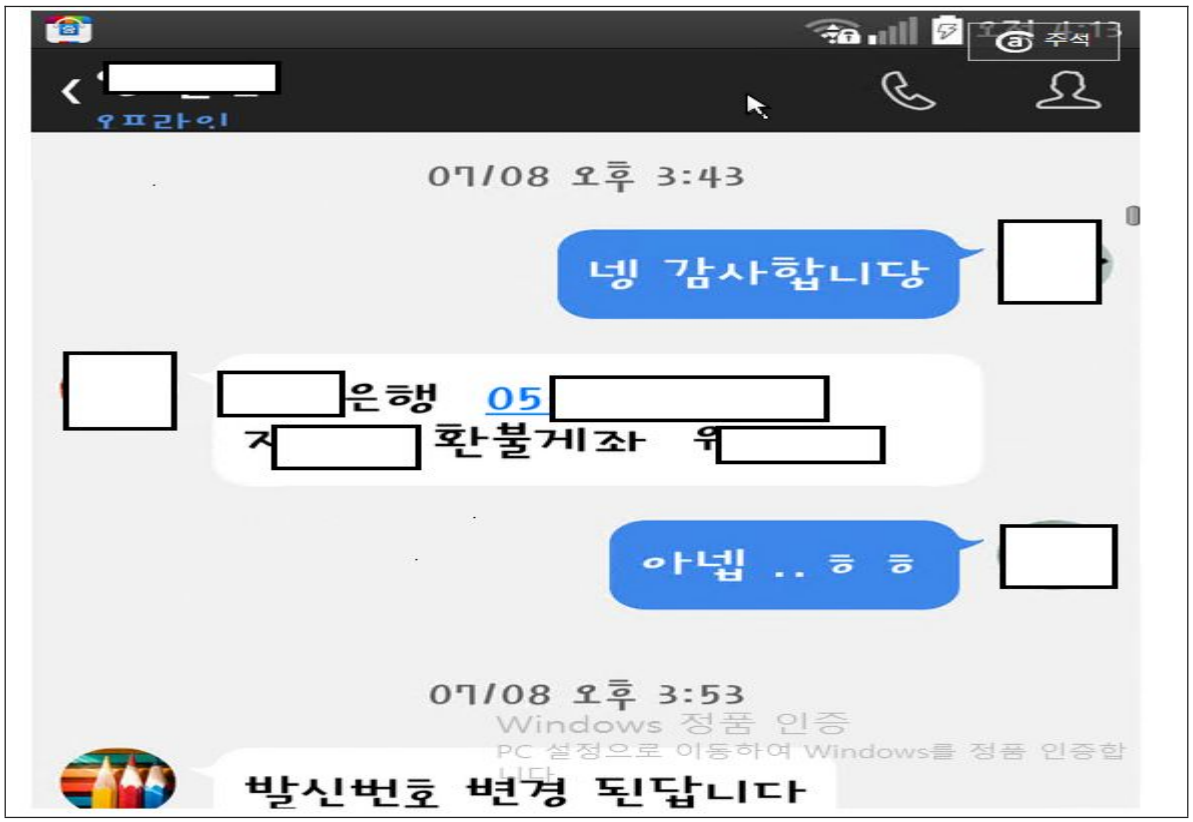
Evernote 와 마찬가지로 데이터 공유 및 저장을 위해 사용되었을 것이며

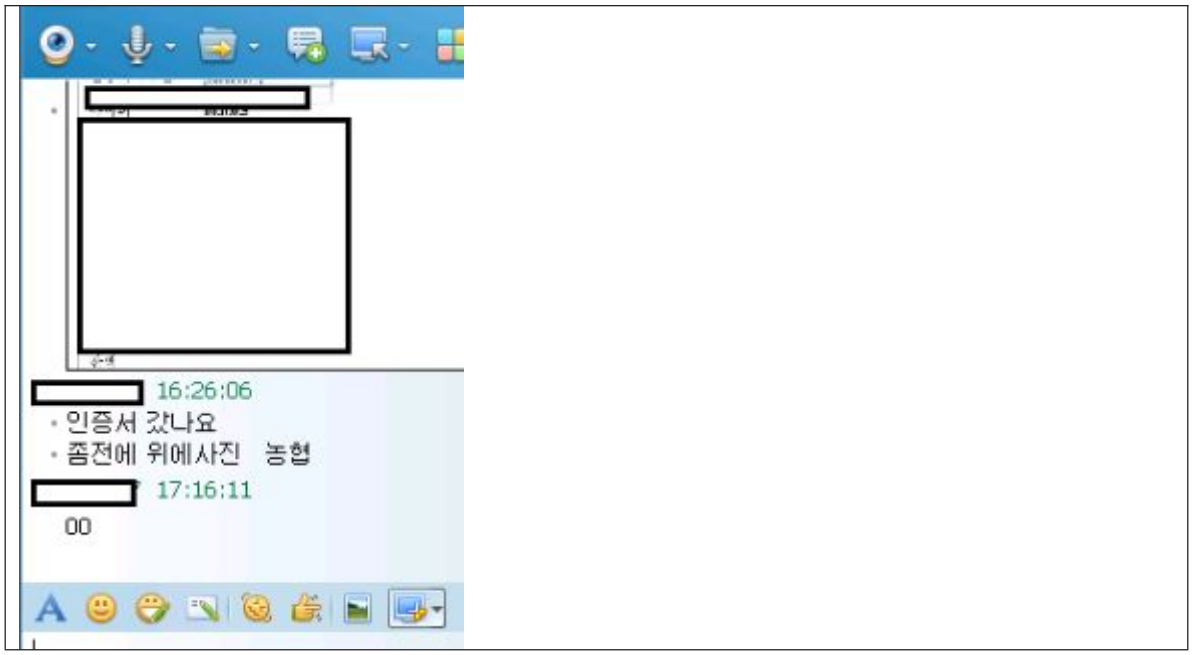
명의 도용된 피해자 계정일 수도 있기 때문에 따로 확인은 하지 않았다

메신져 대화 내역 캡쳐 내역 (약 10건)









자료공유 및 의사소통을 위하여 메신져를 사용하고 있음을 확인할수 있다

그외 저장된 해커들의 정보들

위치.협조 동의서.귀국내한 동의서.출국 입국허가서

위치.협조 동의서.귀국내한 동의서.출국 입국허가세

25일 작업 일지.

25일 작업 일지.

[redacted] [redacted] 자동이체 계좌 확인후 착신전환 신청 동시에 [redacted]가입해서
메세지 메신저 가입 하면끝

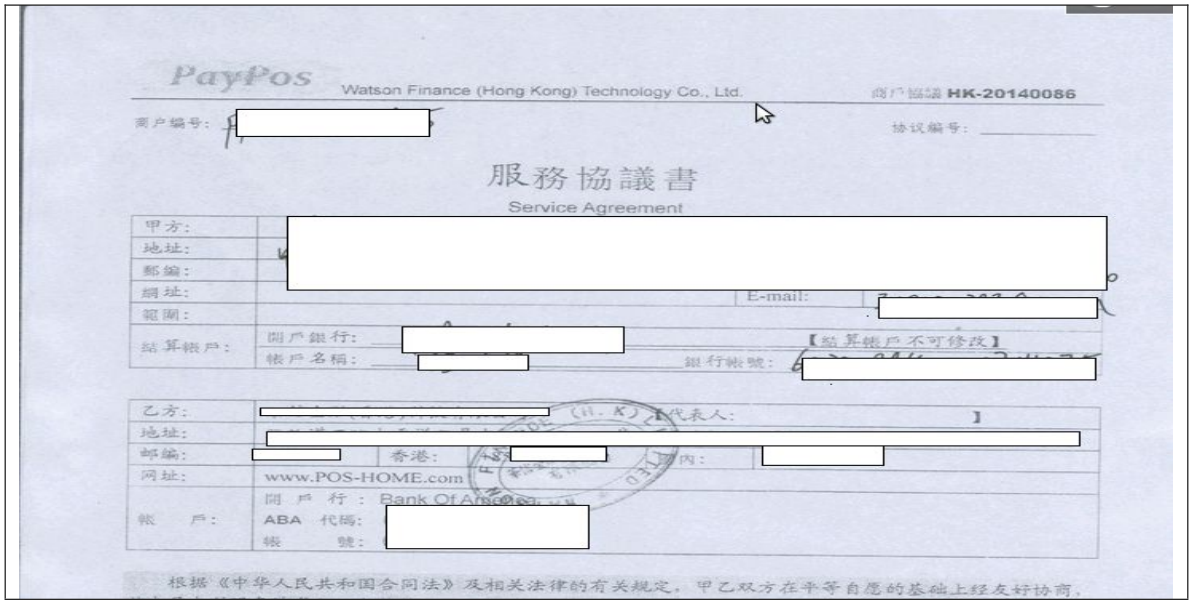
[redacted]신분증 분실 착신 등록후 [redacted]인증서발행 작업중 비밀번호 설정하기 필수

建设银行：6222 8023 9758 1107 103 崔香淑 250원입니다

建设银行：6222 8023 9758 1107 103 崔香淑 250원입니다
이돈으로 큰 회식했다...ㅎㅎㅎ배터지게 난 행복하다 맛있는것 먹어서 ㅎㅎㅎㅎ

그리고 아래 한문으로 된 문서도 하나 확인했는데 은행에 관련된

문서인듯하며 어떤 용도의 문서인지는 더 확인해봐야겠다



PayPos

Watson Finance (Hong Kong) Technology Co., Ltd.

HK-20140086

服務協議書

Service Agreement

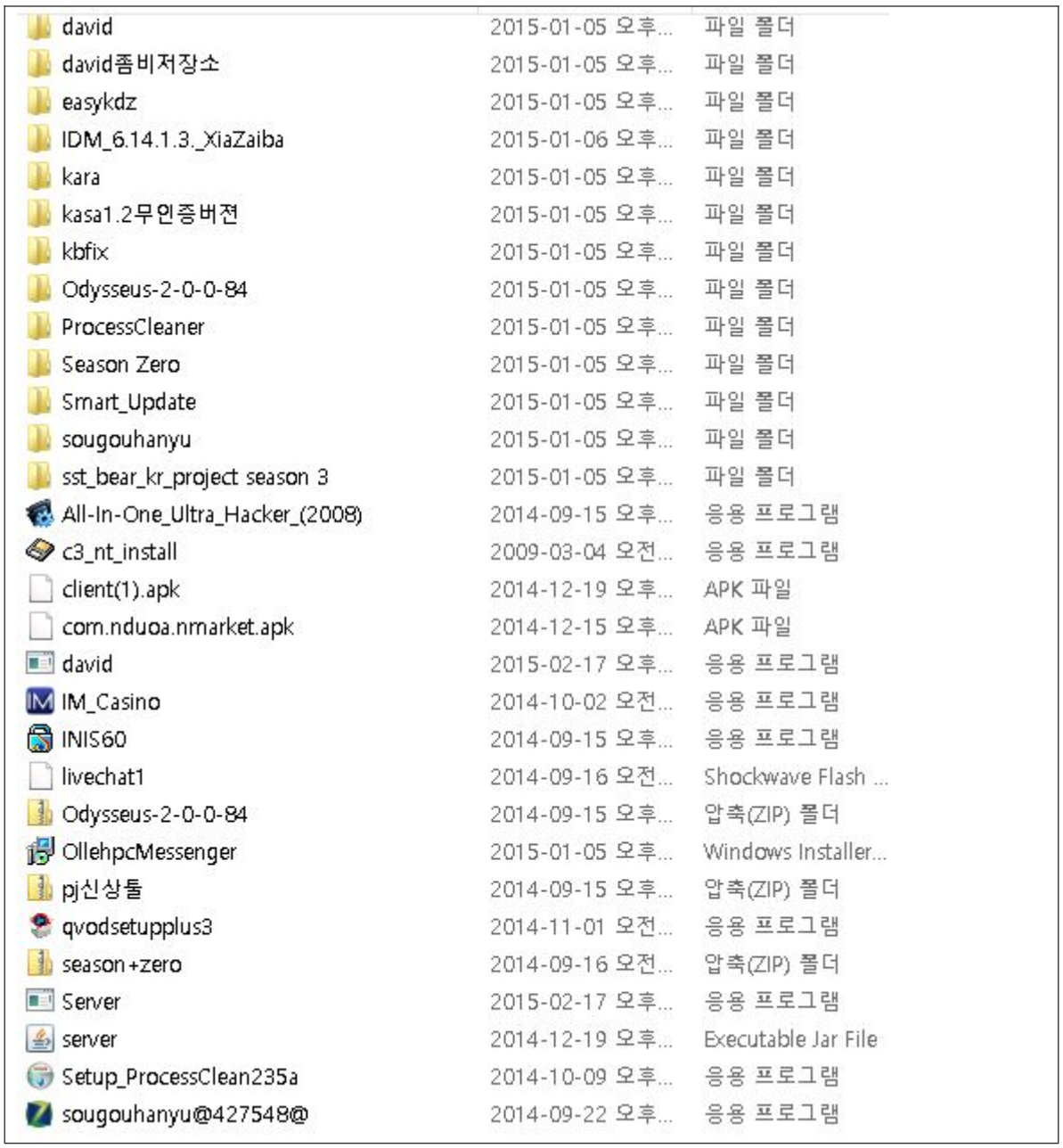
파일 중에는 아래와 같은 제목으로 된 파일이 하나 있었는데 내용은

북한과 관련된 내용은 아니었다

조선인민 민주주의만세(1)(1).xls

지금부터는 서버에 저장된 해킹툴에 대해서 확인해 보았다

우선 서버에 저장된 프로그램들을 모아서 한 폴더에 간추려 보았다



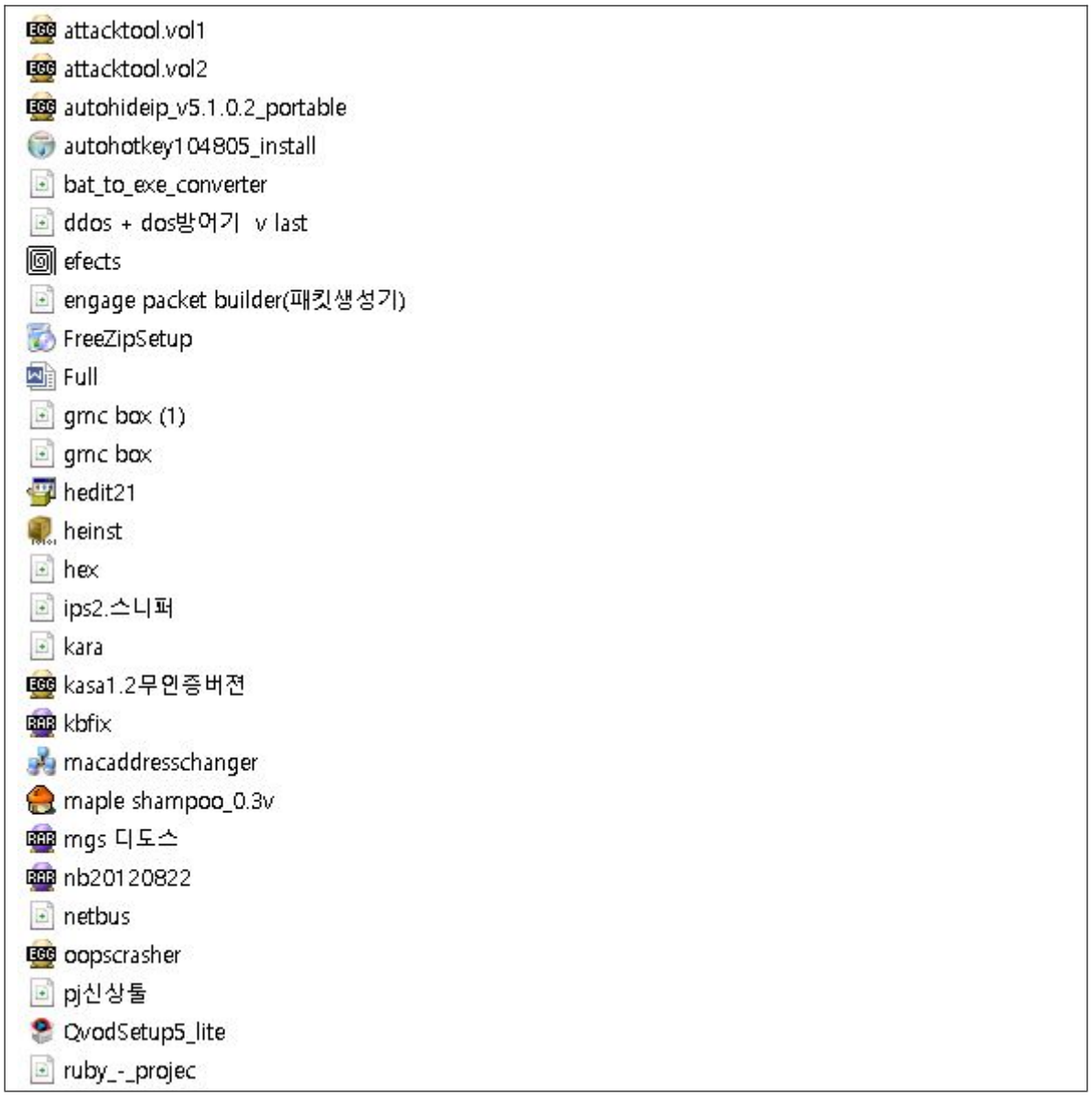
david	2015-01-05 오후...	파일 폴더
david좀비저장소	2015-01-05 오후...	파일 폴더
easykdz	2015-01-05 오후...	파일 폴더
IDM_6.14.1.3._XiaZaiba	2015-01-06 오후...	파일 폴더
kara	2015-01-05 오후...	파일 폴더
kasa1.2무인증버젼	2015-01-05 오후...	파일 폴더
kbfix	2015-01-05 오후...	파일 폴더
Odysseus-2-0-0-84	2015-01-05 오후...	파일 폴더
ProcessCleaner	2015-01-05 오후...	파일 폴더
Season Zero	2015-01-05 오후...	파일 폴더
Smart_Update	2015-01-05 오후...	파일 폴더
sougouhanyu	2015-01-05 오후...	파일 폴더
sst_bear_kr_project season 3	2015-01-05 오후...	파일 폴더
All-In-One_Ultra_Hacker_(2008)	2014-09-15 오후...	응용 프로그램
c3_nt_install	2009-03-04 오전...	응용 프로그램
client(1).apk	2014-12-19 오후...	APK 파일
com.nduoa.nmarket.apk	2014-12-15 오후...	APK 파일
david	2015-02-17 오후...	응용 프로그램
IM_Casino	2014-10-02 오전...	응용 프로그램
INIS60	2014-09-15 오후...	응용 프로그램
livechat1	2014-09-16 오전...	Shockwave Flash ...
Odysseus-2-0-0-84	2014-09-15 오후...	압축(ZIP) 폴더
OllehpcMessenger	2015-01-05 오후...	Windows Installer...
pj신상툴	2014-09-15 오후...	압축(ZIP) 폴더
qvodsetupplus3	2014-11-01 오전...	응용 프로그램
season+zero	2014-09-16 오전...	압축(ZIP) 폴더
Server	2015-02-17 오후...	응용 프로그램
server	2014-12-19 오후...	Executable Jar File
Setup_ProcessClean235a	2014-10-09 오후...	응용 프로그램
sougouhanyu@427548@	2014-09-22 오후...	응용 프로그램

하나의 디렉토리에 실행가능하거나 문서 이외에 모든 파일을 모아두었다

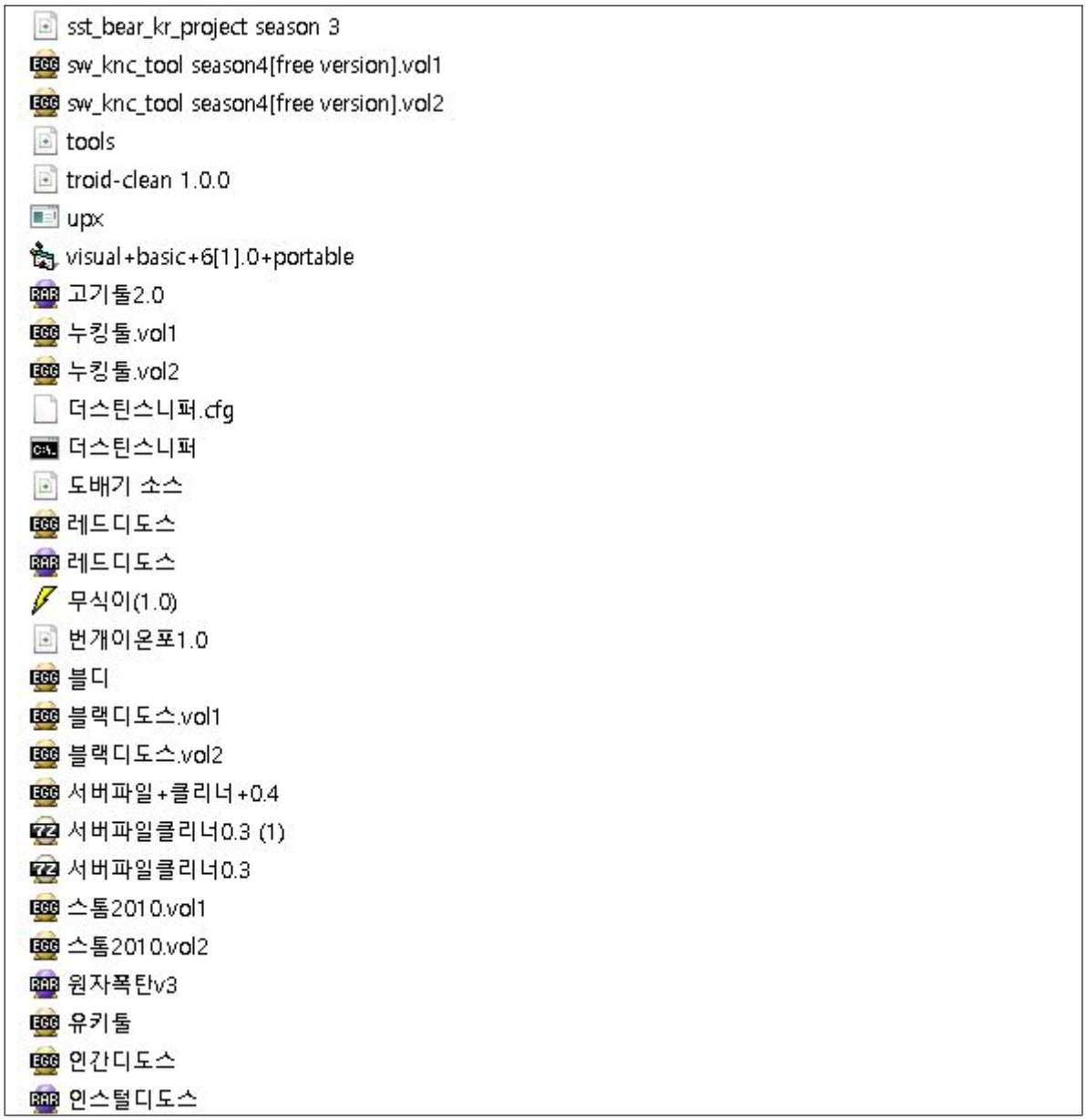
종합툴 모음1


ANFlooder
http_ping_attacker
MSWINSCK.OCX
Read Me
UDP Flooder v2.0
udp어택기
Yagamisoohra_사이트_대규모_트래픽_공...
Yagamisoohra_사이트어태커
yagamisoohra_의_슈퍼신상털기_3.0
Yagamisoohra+사이트+대규모+트래픽+...
도스어택1.7
신상
신상털기1
신상털기3
신상털기5
어택기
All-In-One_Ultra_Hacker_(2008)
c3_nt_install
client(1).apk
com.nduoa.nmarket.apk
IM_Casino
INIS60
livechat1
Odysseus-2-0-0-84
OllehpcMessenger
pj신상툴
qvodsetupplus3
season+zero
server
Setup_ProcessClean235a
sougouhanyu@427548@
SurfingGhost
SW9.0
이름없음_01
종합툴
종합툴2
카페 도배기 v6
확인
희귀zero[1]

종합툴 모음2


attacktool.vol1
attacktool.vol2
autohideip_v5.1.0.2_portable
autohotkey104805_install
bat_to_exe_converter
ddos + dos방어기 v last
efects
engage packet builder(패킷생성기)
FreeZipSetup
Full
grnc box (1)
grnc box
hedit21
heinst
hex
ips2.스니퍼
kara
kasa1.2무인증버젼
kbfix
macaddresschanger
maple shampoo_0.3v
mgs 디도스
nb20120822
netbus
oopscrasher
pj신상툴
QvodSetup5_lite
ruby_-_projec

종합툴 모음3



신상털기, 디도스, 누킹, 도배기, 스니퍼 관련한 해킹 툴이 저장되어 있다

한우툴 (Season Zero)

좀비PC를 만들 수 있고 디도스 공격 등 여러가지 해킹 기능이 포함된 해킹툴

여러 폴더에 버전별로 저장이 되어 있었으며 위 화면만 출력된 후 특정 DLL 파일이 없다는 메시지와 함께 실행되지는 않았다

Extension spoofer

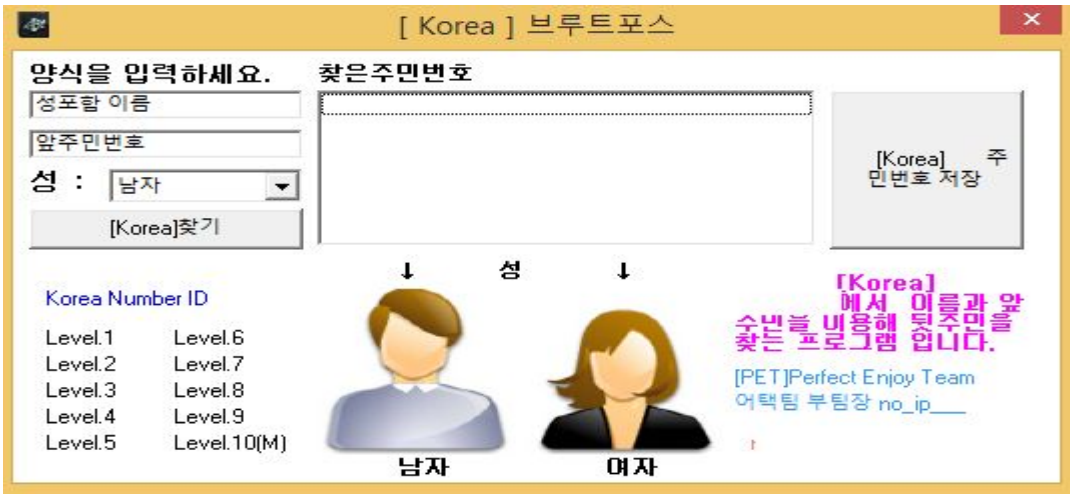
파일의 확장자를 변조할 수 있는 유틸리티

주로 EXE악성코드 실행파일을 Mp3, 동영상 파일 등으로 변조할 때 사용된다

Awrcp (원격제어 프로그램)

원격 제어 프로그램인데 좀비 PC들의 원격제어를 위해 사용할 거라 판단됨

부르트포스라는 프로그램



이름을 입력하면 주민등록번호를 웹하드 DB에 검색한 뒤 출력한다고 함

실제로 실행시켜봤지만 동작하지는 않았음

HDSI 3.0 / NBSI 웹해킹툴

SQL 인젝션 공격에 사용되며 정보 유출의 목적으로 사용된다고 합니다

해킹툴을 살펴보니.....

서버에 저장된 해킹툴을 살펴보았으나 실행되는 건 거의 없었으며

백신에서 해당 해킹툴을 잡아내어 실행이 불가능했다

서버에서 많이 저장된 툴 중 하나는 “한우툴” 이라는 해킹 툴인데

인터넷에서는 프로그램과 좀비 PC들도 거래가 되고 있는 상황인 것 같다

시간이 된다면 한우툴에 대해서 좀 더 분석이 필요하리라 생각된다

내용들을 분석한 결과...

두 달 동안 서버를 분석한 결과 아래와 같은 결과에 도달했다

“해커들의 타깃은 일반 뱅킹 사용자이며 직접 은행을 해킹한 근거는 없다”

서버에 저장된 정보를 분석해보면

이미 노출된 개인 정보를 바탕으로 보이스피싱을 시도하고

악성코드를 통해서 좀비 PC로 만들거나 피싱이나 파밍을 통해

계좌정보, 보안카드 정보, 공인인증서 등의 정보를 획득한 것으로 파악된다

다만 해당 서버는 정보 공유의 목적으로 이용된 서버이기 때문에

구체적인 해킹 방법이나 해커들의 실체에 대해서는 더 이상 알 수는 없었다

하지만 이러한 분석을 통해서 해커들이 어떠한 정보를 원하는지를 통해

우리가 지켜야 할 개인 정보와 예방 방법을 유추할 수가 있었다

금융 피해 예방법

PC 보안

1. 불안하면 PC 포맷 후 백신프로그램 설치

2. 무료 백신 혹은 결재하고 유료 백신 사용하기 (한번 술값이면 1년간 사용 가능함)

3. 인터넷뱅킹하는 PC와 게임 인터넷 하는 PC 분리시키기

4. 인터넷에서 돌아다니는 파일 아무거나 실행하지 않기 (정품 사용하기)

5. PC에서 개인 정보 저장 금지 및 인터넷상에 개인 정보 입력 금지

6. 가입된 사이트 3개월마다 패스워드 변경하기

7. 패스워드는 자기 개인 정보 포함하지 말 것 (생일, 핸드폰번호, 주소 등)

8. 모든 사이트의 패스워드는 동일하게 사용하지 않기

9. 특히 공인인증서, 아이핀, 계좌 비밀번호, 카드 비밀번호등은 영문자,숫자,특수문자 포함하여 최대한 복잡하게 구성하고 중복하여 사용하지 않기

10. 토렌트 프로그램 사용 자제하기 (악성코드 파일 배포 가능성 존재함)

11. 패스워드 자동 저장 및 관리해주는 프로그램은 편리하지만 유출되면 치명적이다

12. 신용카드는 평상시에 해외 결재 차단으로 설정해둔다

13. 은행 사이트에서 제공하는 모든 보안 서비스를 설정하여 사용한다

14. 불편하더라도 계좌의 1회 혹은 1일 최대 이체한도를 반드시 최소한도로 지정한다

15. 공인인증서는 USB에 보관하되 아무 데서나 꼽지 않으며 사용할 때만 연결한다

16. 되도록이면 보안카드보다는 안전한 OTP를 사용한다

보이스 피싱 예방

17. 전화상으로 개인 정보 말하지 않기 (문자 포함)

18. 전화 온 상대방이 진짜 콜센터 직원인지 의심하기

19. 무료, 이벤트, 각종 문자 및 모든 ARS 모든 메시지는 모두 의심해야 한다

20. 보이스 피싱은 자기만 조심한다고 끝나는 게 아니며 가족에게도 시도한다

일상생활

21. 스마트폰 및 마그네틱 카드는 빌려주지 않는다

22. 카드 결제 시 카드 단말기 앞에서 자신이 직접 결재한다

23. 스팸전화 차단 부가서비스 이용

현재 금융권에서는 FDS 이상 징후 탐지시스템을 구축 중에 있다

고객들의 금융 활동 패턴이 수집되려면 시간이 소요되며

100% 완벽한 시스템은 아니므로 사용자의 안전은 스스로 지켜야 한다

현재 이 문서에서 파악한 Evernote 해커의 계정은 아직도 업데이트가

계속 진행되고 있으며 방치하는 경우 금융 피해자가 늘어갈 전망으로 보인다

본 문서를 통해서 인터넷 뱅킹 사용에 대한 경각심을 가졌으면 하는 바램이며

예방 방법을 통해서 자신의 재산을 안전하게 지켰으면 한다