Security Stream, reaching into cells

AhnLab
ASEC (AhnLab Security Emergency response Center)
Malware Researcher
Paul Chung

Contents

01 Introduction of ASEC

02 Traditional Organ Infection

03 Reaching into Cells

04 Capillaries as well

05 Always Be Prepared

1. Introduction of ASEC

AhnLab資安應變中心
ASEC (AhnLab Security Emergency response Center)

AhnLab

ASEC have specific goal, it's protect customer's IT asset and infra from internet threats, since October 2001

ASEC - AhnLab Security Emergency response Center

AhnLab Security Emergency Response Center (ASEC) is a world-class emergency response organization composed of malicious code analysts and security experts. We monitor and respond to emergencies 24/7, protecting customers safely from malicious codes and security threats spreading around the world.

24/7應變中心

1. 24/7 Response System

ASEC monitors new security threats found around the world 24 hours a day, 7 days a week, and responding quickly and effectively taking action.

透過迅速回應降低資安損害

2. Minimizing the Damage of Security Threats by Promt Action

ASEC develops and distributes anti-virus signatures, anti-spyware signatures, and network signatures to be prepared against new malicious codes, spyware and security threats looming. ASEC also provides analytic information to our clients.

分析惡意程式碼並提供對應解決方案

3. Analyzing Malicious Codes & Providing Relevant Movements

ASEC provides customers with detailed analysis of vulnerabilities presented by malicious codes and spywares. ASEC Monthly Report is also distributed to inform customers of damages from malicious codes & spywares, and newly found movements.

更新佈署惡意程式碼至所有AhnLab產品線

4. Engine Development

To respond quickly to new forms of malicious code and spyware, ASEC develops and upgrades to all product lines of AhnLab.

© AhnLab, Inc. All rights reserved.

ASEC資安應變流程
ASEC Threat Response solutions and process

AhnLab

◆**ENDPOINT SECURITY**
Anti-Virus Engine for V3 and other products

1988 Vaccine, 1995 V3 Warp Engine, 2003 V3 Flight Engine and 2007 V3 TS Engine
Present ASD(AhnLab Smart Defense)

◆ **NETWORK SECURITY**
Network signatures for TrusGuard and other network products

◆ **MOBILE SECURITY**
Mobile Anti-Virus Engine for V3 Mobile

© AhnLab, Inc. All rights reserved.

威脅整合報告，ASEC Report

Threat Intelligence Report, ASEC Report

AhnLab

ASEC is a global security response group consisting of malware analysts and security experts.

This monthly report is published by ASEC, and it focuses on the most significant security threats and the latest security technologies to guard against these threats.

© AhnLab, Inc. All rights reserved.

威脅整合報告，ASEC Blog
Threat Intelligence Report, ASEC Blog

AhnLab

ASECBLOG
THREAT RESEARCH & RESPONSE BLOG

국내외 악성코드와 보안위협에 실시간 대응하는 AhnLab ASEC 블로그

HOME | ASEC 소개 | 보안위협 동향 | 악성코드 정보 | 취약점 정보

NATIONAL SECURITY BUREAU

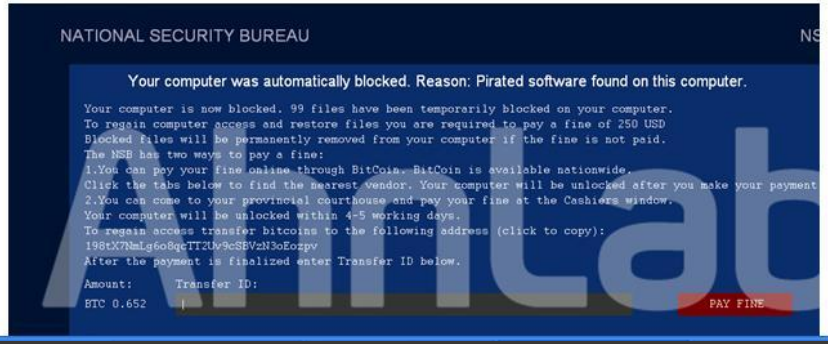
악성코드 정보 2015/01/23 11:03

Your computer was automatically blocked

작년부터 악명을 떨친 랜섬웨어는 크립토락커(CryptoLocker)와 크립토월(CryptoWall)이 있다. 이러한 랜섬웨어는 시스템 내부의 특정 파일을 암호화한 후 암호화 해제를 빌미로 돈을 요구한다. 하지만 최근 사용자에게 몸값을 요구하는 새로운 악성코드가 발견되었다.

이 악성코드는 국가안보국(National security bureau, NSB)으로 가장하여 사용자에게 경고 메시지 표기 및 시스템 사용을 방해한다. 이를 해결하기 위해서 미화 250달러를 입금하도록 유도하고 있다.

해당 악성코드에 감염되면, 아래 **[그림 1]**와 같은 화면이 나타나면서 "불법 소프트웨어가 탐지되어, 시스템을 사용을 차단하였습니다."는 메시지를 화면에 보여준다. 또한, 다른 프로그램의 실행을 방해하고, 메시지를 강제로 종료하여도 자동으로 다시 실행되므로 사용자는 시스템을 정상적으로 사용할 수 없다.



SOCIAL MEDIA

@AhnLab_SecuInfo
안랩 보안정보 통합 트위터

CATEGORY

- 전체 글보기 (969)
  - 악성코드 정보 (552)
  - ASEC소개 및 공지 (32)
  - 취약점 정보 (172)
  - 보안위협 이슈 (0)
  - 보안위협 동향 (121)
  - 조치 가이드 (37)
  - 보안 툴 사용법 (28)
  - 자주 묻는 질문 (FAQ) (24)
  - ASEC 일기 (1)

ARTICLES

문서에 포함된 매크... (1)
CTB Locker 랜섬웨어.
2014년 MAC 악성코...
NATIONAL SECURITY...

COMMENTS

http://pc114.tistо... 3sun 2014
글이 쓰여진 시기보... Realitist 2014
덕분에 좋은 정보... S매니저 2013
글 잘보고 갑니다.... 매:지구름 2013

TRACKBACKS

Crappy Bird - A Mu... Crappy Bird - A Mu... 01/26

© AhnLab, Inc. All rights reserved.

ASD (AhnLab Smart Defense)

AhnLab雲端智能中心
ASD (AhnLab Smart Defense)

AhnLab

AhnLab Smart Defense

Global Cyber Threat Intelligence

- Real-time collection and analysis
- Millions of sensors around the world
- A wide range of cyber threats
- Collects 500,000+ samples

Hybrid Analysis System

- DNA Scans
- Whitelists
- Signature/Behavior-based rules
- Reputation rules
- Correlation rules

The Power of Cloud

- Fast identification of variants
- Automated responses
- Enhanced zero-day detection
- Minimized false-positives

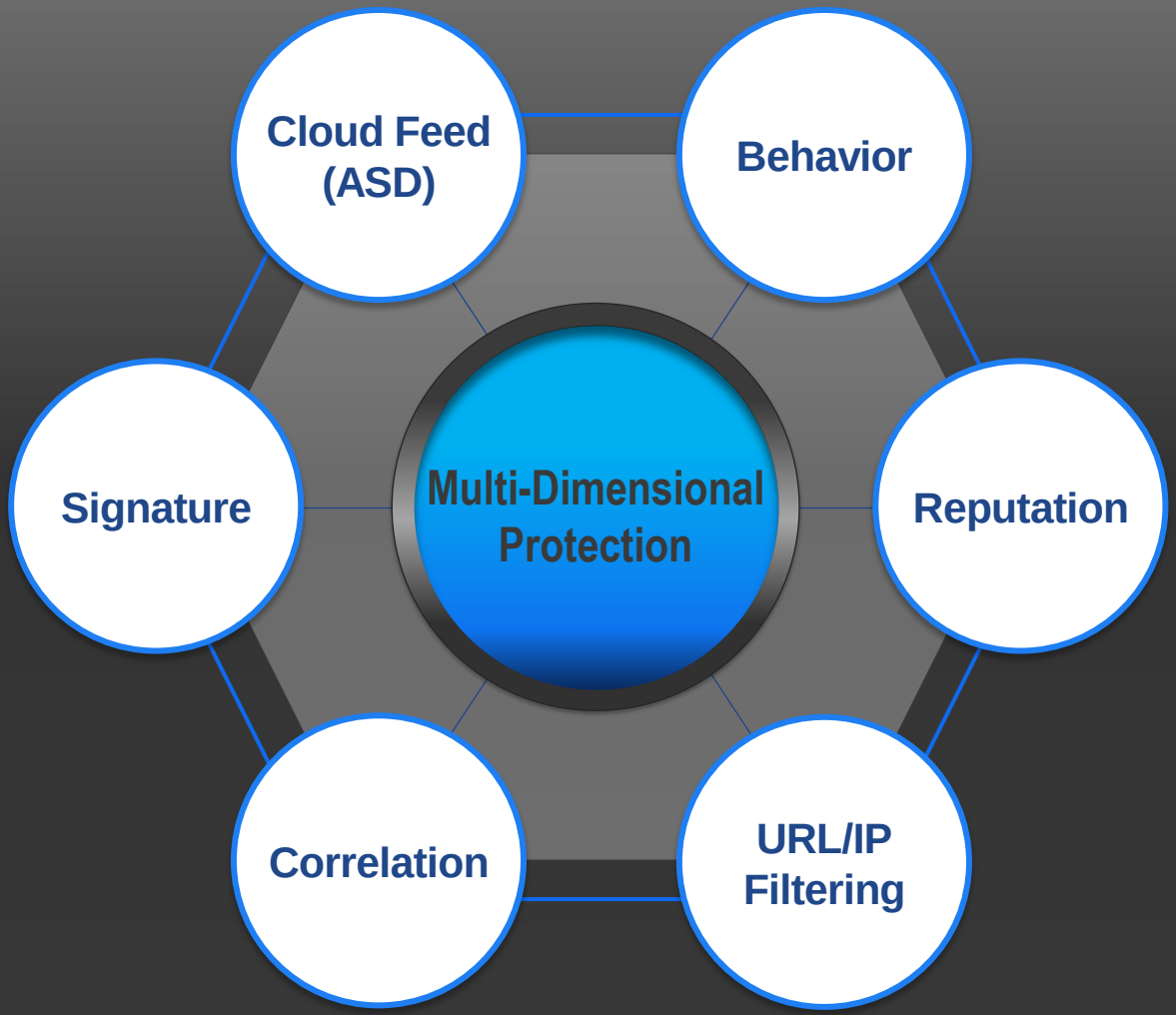
Early Response to Emerging Threats

Proactive Response to Evolving Threats

© AhnLab, Inc. All rights reserved.

AhnLab雲端智能中心-多維度防護

ASD (AhnLab Smart Defense)



© AhnLab, Inc. All rights reserved.

A-FIRST
AhnLab - Forensics & Incident Response Service Team

數位鑑識與災害回應
Digital Forensics & Incident Response

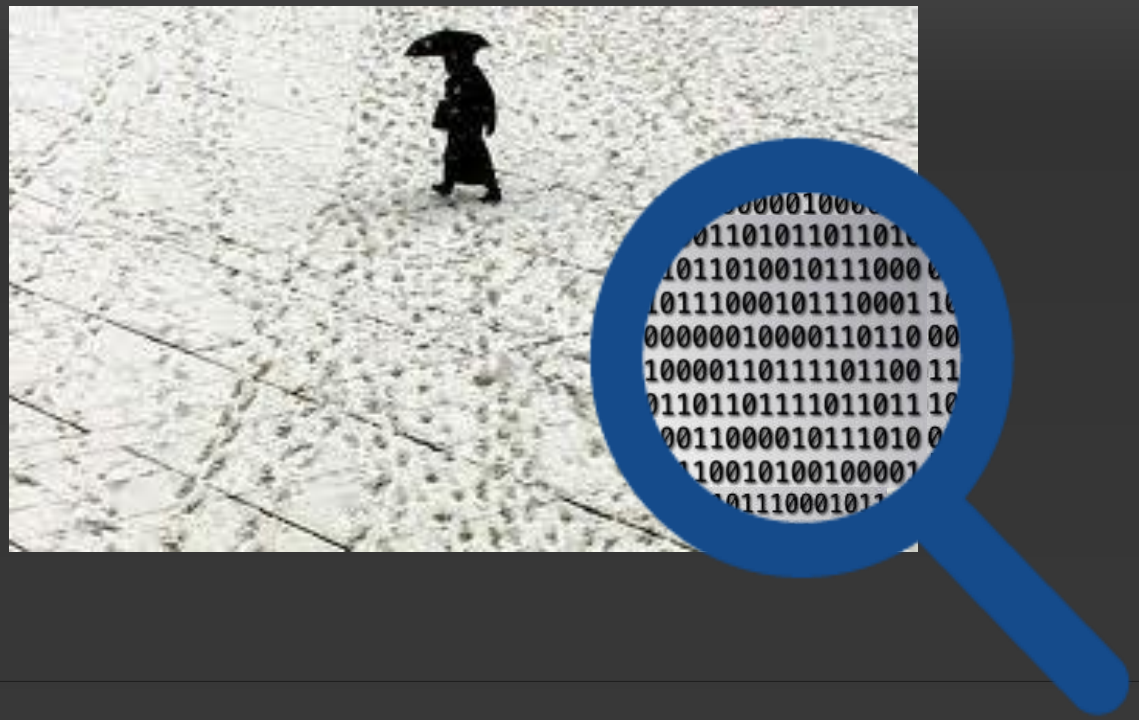
AhnLab

◆ Digital Forensics

- Extracting evidence from computer or other any kind of digital devices

- Has been Focusing on the targeted attack such as APT

- Making a timeline in order to tracking any kind of footprints



© AhnLab, Inc. All rights reserved.

2. Traditional Organ Infection

駭客就在你我身邊-Target
Around the World – Target

AhnLab

2013, 1.1億 (110 million)

© AhnLab, Inc. All rights reserved.

駭客就在你我身邊-JPMorgan Chase

Around the World – JPMorgan Chase

AhnLab

2014, 7600萬 (76 million)

© AhnLab, Inc. All rights reserved.

SnapchatDB!

Bringing 4.6 million users' information to your fingertips...

Download the database as SQL dump as CSV text

2014, 460萬 (4.6 million)

```
mysql> select phone, username from records
           where username like '%sex%'
            or username like '%porn%';

+------------+-----------------+
| phone      | username        |
+------------+-----------------+
| 21232104[illegible] | lsexy[illegible]  |
| 21239081[illegible] | sexyp[illegible]  |
| 21292016[illegible] | sexxx[illegible]  |
| 21364000[illegible] | jesse[illegible]  |
```

```
| 87051066[illegible] | sexyy
| 87051420[illegible] | sexay
| 87051475[illegible] | freck
| 87051950[illegible] | msx.s
| 87053008[illegible] | sexyb
| 87053014[illegible] | seans
| 87053031[illegible] | sexay
| 87053080[illegible] | sexyb
| 87053230[illegible] | sexym
```

© AhnLab, Inc. All rights reserved.

3. Reaching into Cells

2013, 個體攻擊
Attacking Individuals

© AhnLab, Inc. All rights reserved.

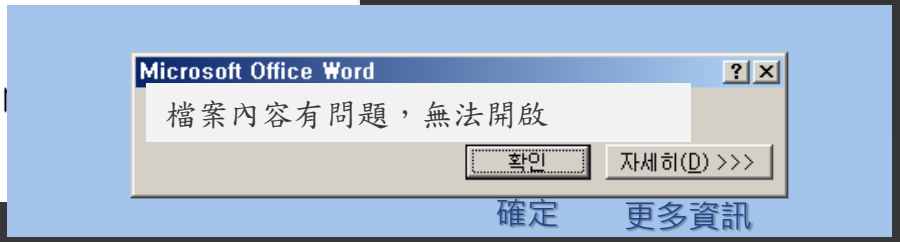
文件加密
Documents Encrypted

AhnLab

pFile	Raw Data	Value
00000000	21 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00	!.c.r.y.p.t.e.d.
00000010	21 00 00 00 31 00 34 00 34 00 35 00 37 00 41 00	!...1.4.4.5.7.A.
00000020	32 00 30 00 38 00 36 00 34 00 35 00 34 00 46 00	2.0.8.6.4.5.4.F.
00000030	39 00 46 00 33 00 30 00 46 00 30 00 45 00 43 00	9.F.3.0.F.0.E.C.
00000040	33 00 36 00 38 00 35 00 42 00 30 00 33 00 36 00	3.6.8.5.B.0.3.6.
00000050	45 00 42 00 00 00 E9 8B 6D CC 4F F0 FA F6 1D FF	E.B.....m.O.....
00000060	B0 66 AB D4 01 A2 58 FA 15 EF FC 51 E	
00000070	0D C3 D0 BD 4F 07 81 61 8E E8 F2 D1 2	
00000080	19 EC C5 68 02 65 1A A6 25 DC 03 29 1	
00000090	04 79 B5 85 00 35 5E 86 5A 22 21 A7 E	
000000A0	BE 25 91 1C D0 6D C5 7E 50 13 96 CC 6	
000000B0	22 68 2C 11 10 FC 79 C5 DA 79 55 60 2	
000000C0	62 8F 66 D9 7B 71 1F 5E 57 85 2C D1 6	

pFile	Raw Data	Value
00000000	D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00	....
00000010	00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00	........>.......
00000020	06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00	....
00000030	19 00 00 00 00 00 00 00 00 10 00 00 FE FF FF FF	....
00000040	00 00 00 00 FE FF FF FF 00 00 00 00 18 00 00 00	....
00000050	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	....
00000060	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	....
00000070	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	....

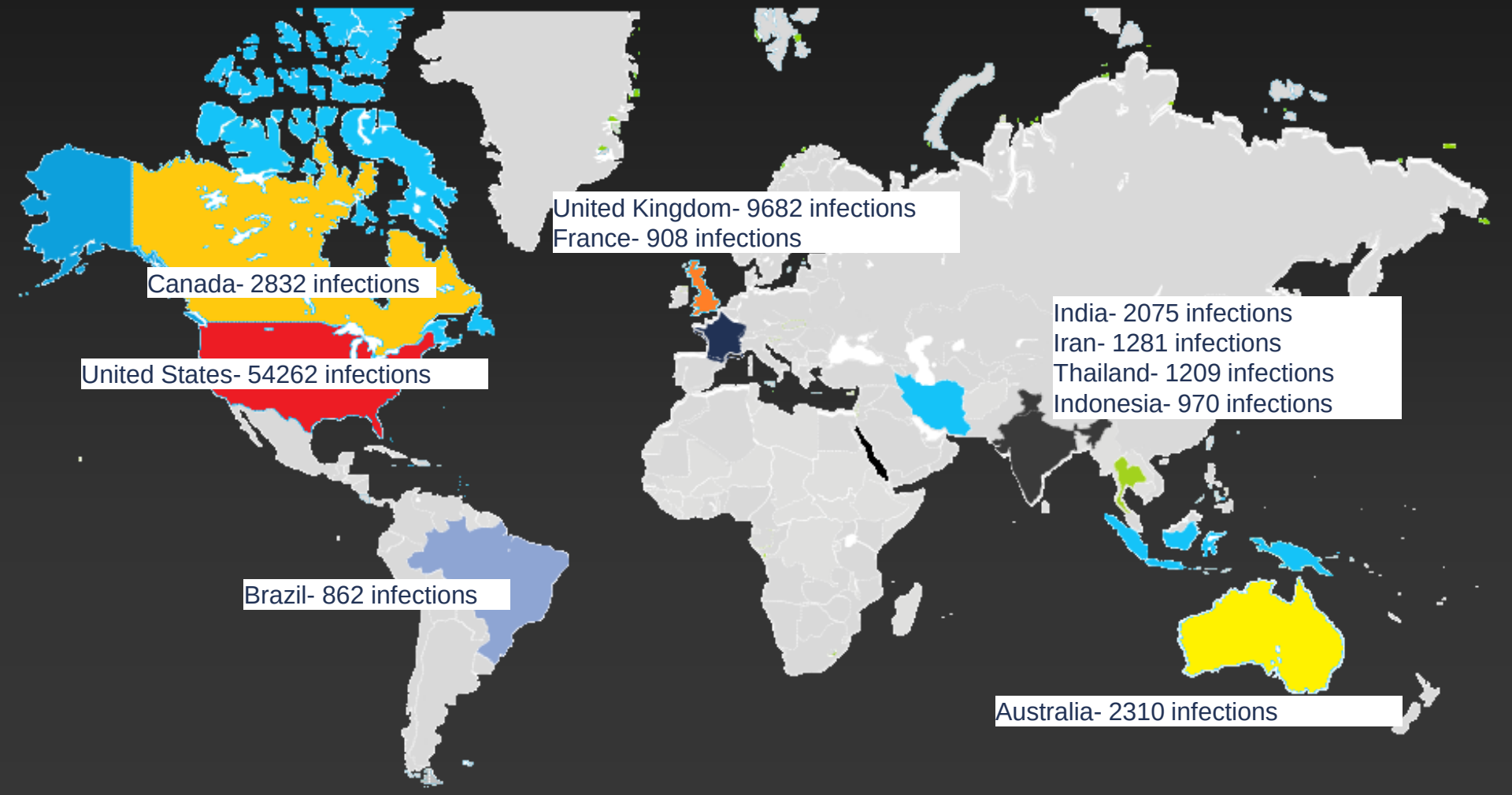
pFile	Raw Data	Value
00000000	50 4B 03 04 14 00 06 00 08 00 00 00 21 00 71 0E	PK.........!.q.
00000010	39 2B 70 01 00 00 A0 05 00 00 13 00 DB 01 5B 43	9+p.........[C
00000020	6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D	ontent_Types].xm
00000030	6C 20 A2 D7 01 28 A0 00 02 00 00 00 00 00 00 00	l ...(..........
00000040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00000050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00000060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00000150	39 89 D5 FF 70 15 75 F3 09 9F C5 07 EB 1E 70 92	9
00000160	21 69 E5 6E 69 AF E8 72 B5 07 BA 66 AD 34 1E A6	!
00000170	94 4E 8C 52 7F 85 73 02 B3 05 7B FC 30 22 4D 19	.
00000180	CE 0B E2 6E A7 D2 2B 59 9F 5C 70 A9 DB 7D 6D 83	.
00000190	7E 9A F9 5F 5F 03 8D E8 4E 6A 31 C0 F1 82 27 26	~



© AhnLab, Inc. All rights reserved.

勒索就在世界各地發生中
Ransomware

AhnLab



Source: **CryptoLocker Working Group - "Roy Arends, Nominet UK" Sinkhole data collected** ***Date: October 15 2013 – January 27 2014***

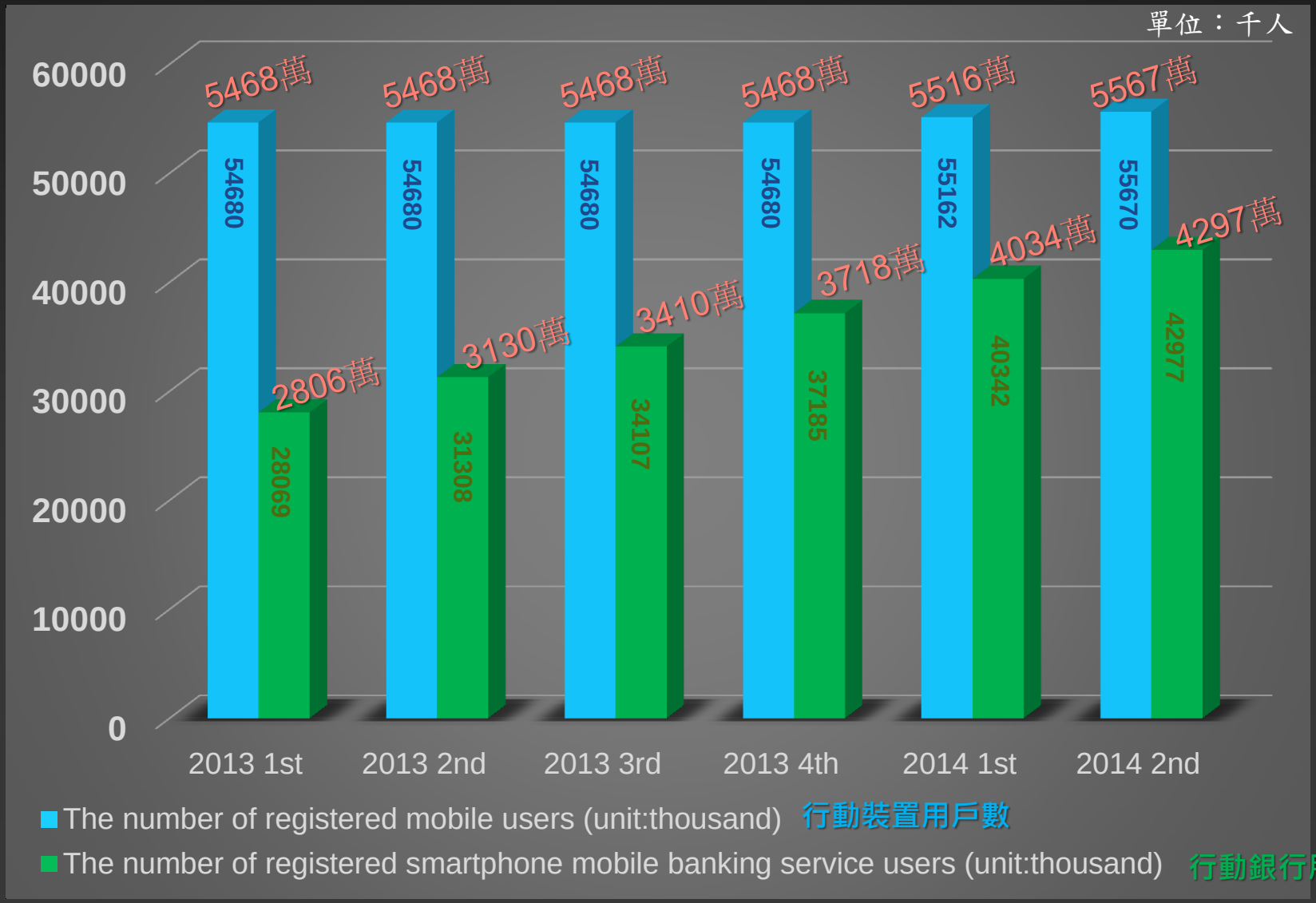
© AhnLab, Inc. All rights reserved.

4. Capillaries as well

行動銀行用戶逐年上升

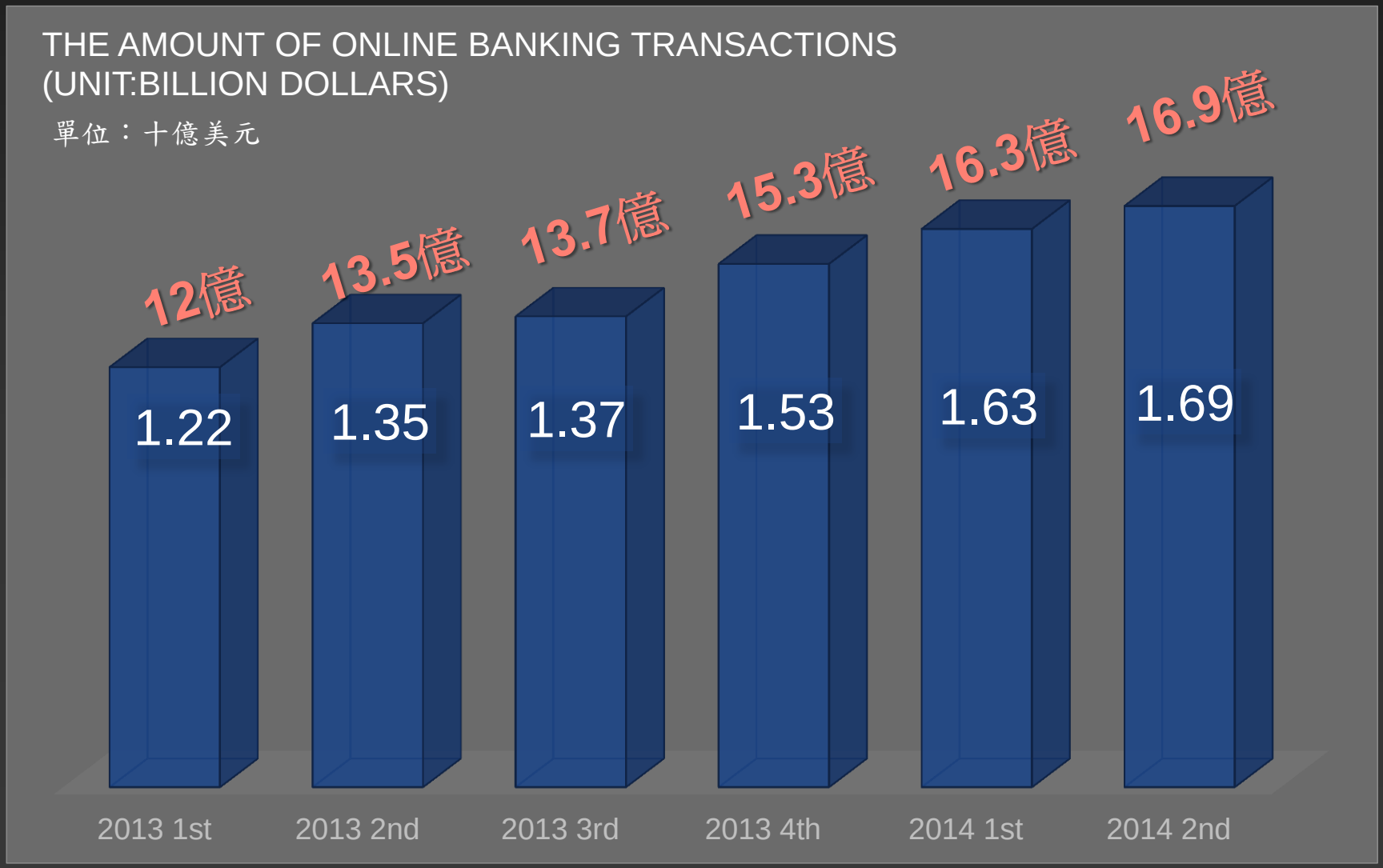
Mobile Banking Users are Increasing

AhnLab



© AhnLab, Inc. All rights reserved.

行動銀行線上交易量逐年上升
Mobile Banking Users are Increasing

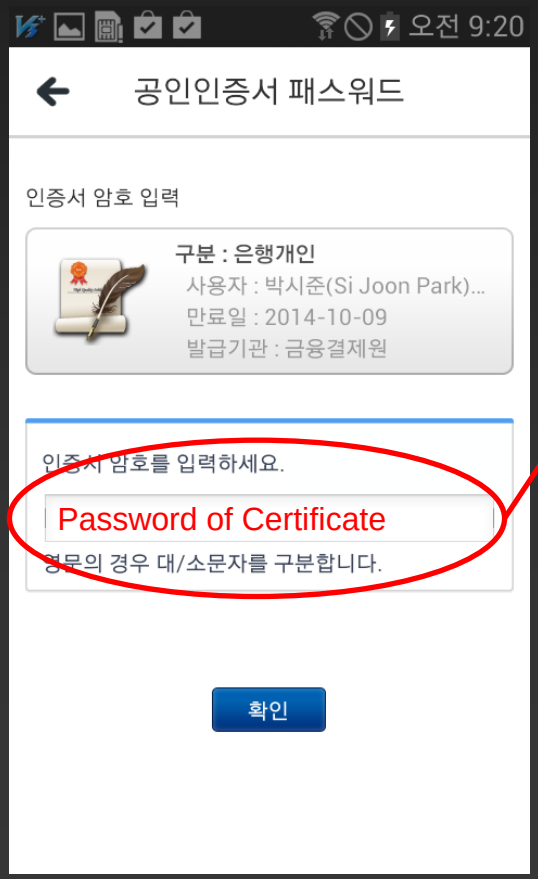


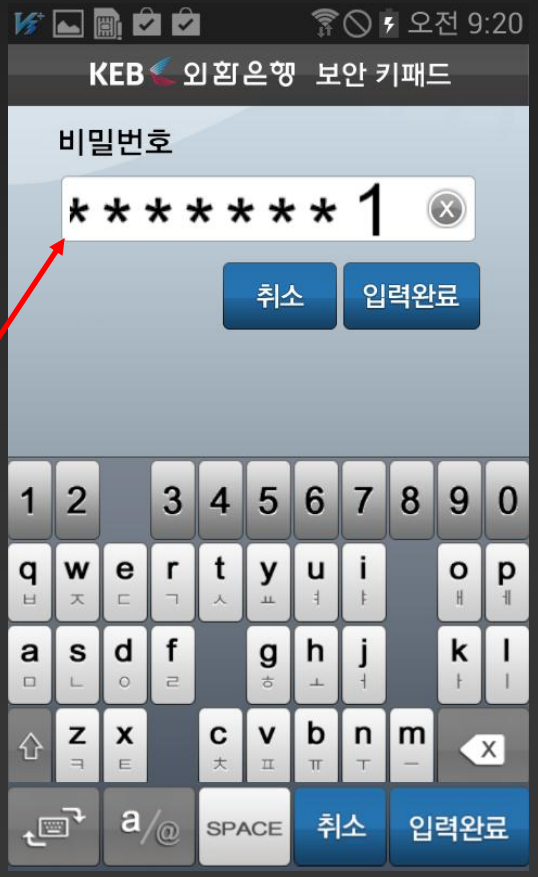
© AhnLab, Inc. All rights reserved.

行動銀行-登入
Mobile Banking

AhnLab

- For Login



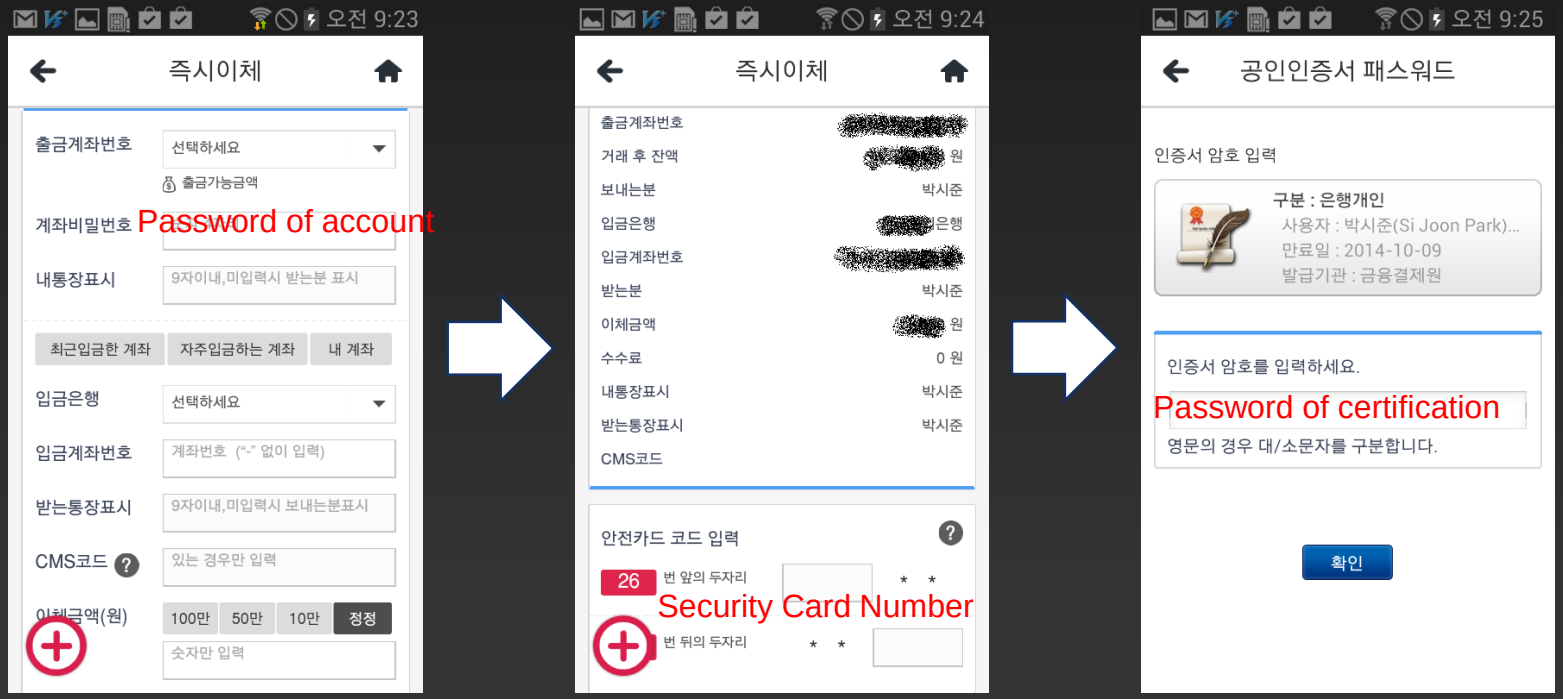


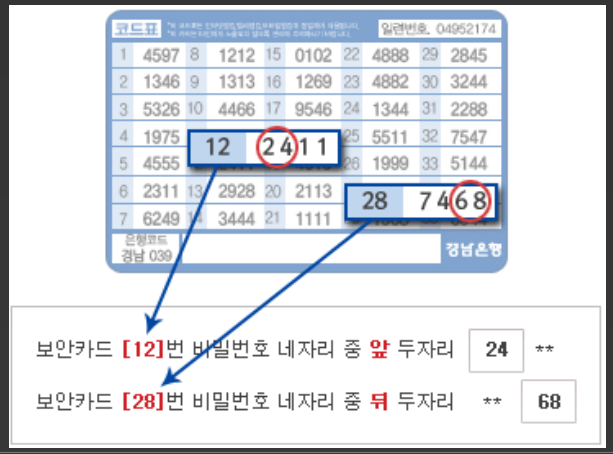
© AhnLab, Inc. All rights reserved.

行動銀行-轉帳交易
Mobile Banking

AhnLab

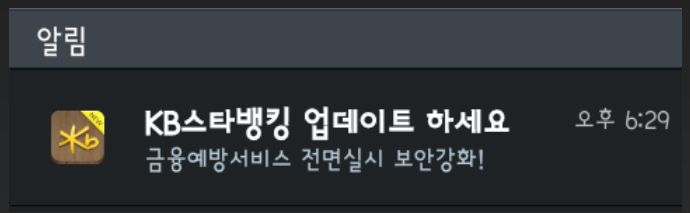
- For Transfer





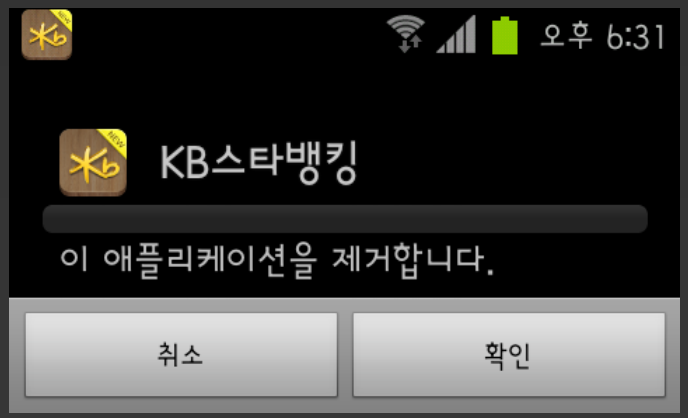
© AhnLab, Inc. All rights reserved.

置換銀行apps成惡意軟體
Replace banking apps

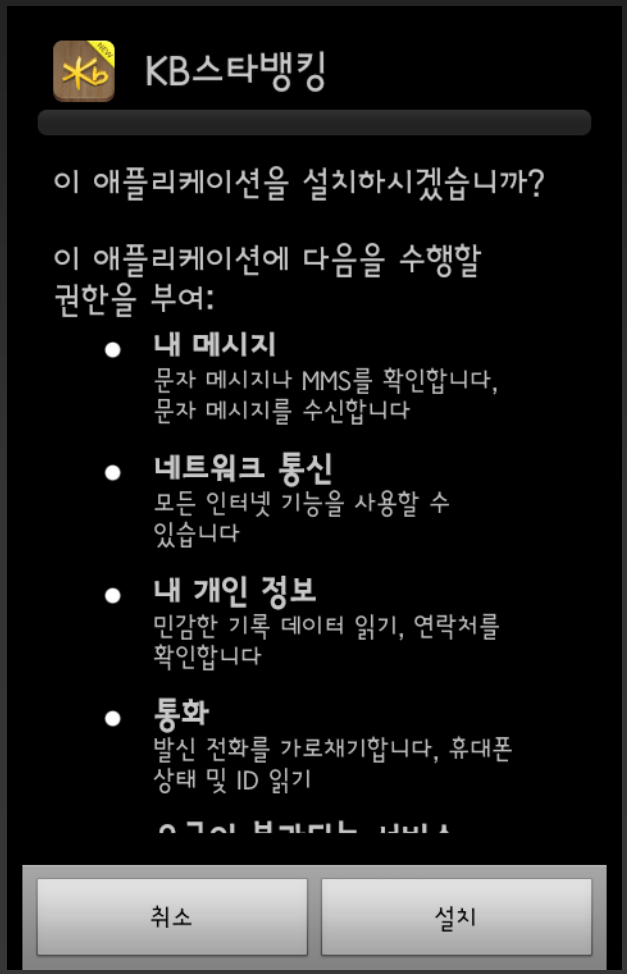


Notification bar

Please update ‘KBStarBanking’



Uninstall ‘KBStarBanking’



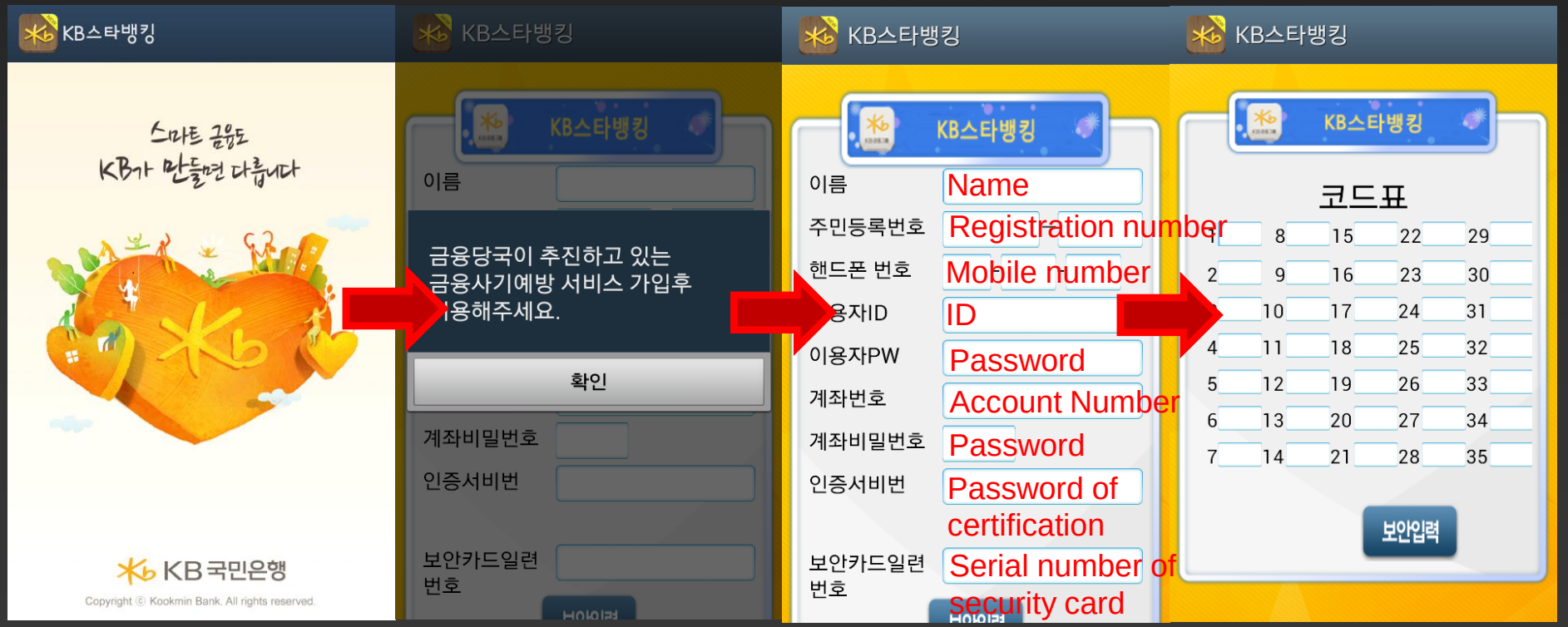
Install malware application

© AhnLab, Inc. All rights reserved.

置換銀行apps成惡意軟體
Replace banking apps

AhnLab

惡意軟體要求重新輸入所有銀行帳戶資料

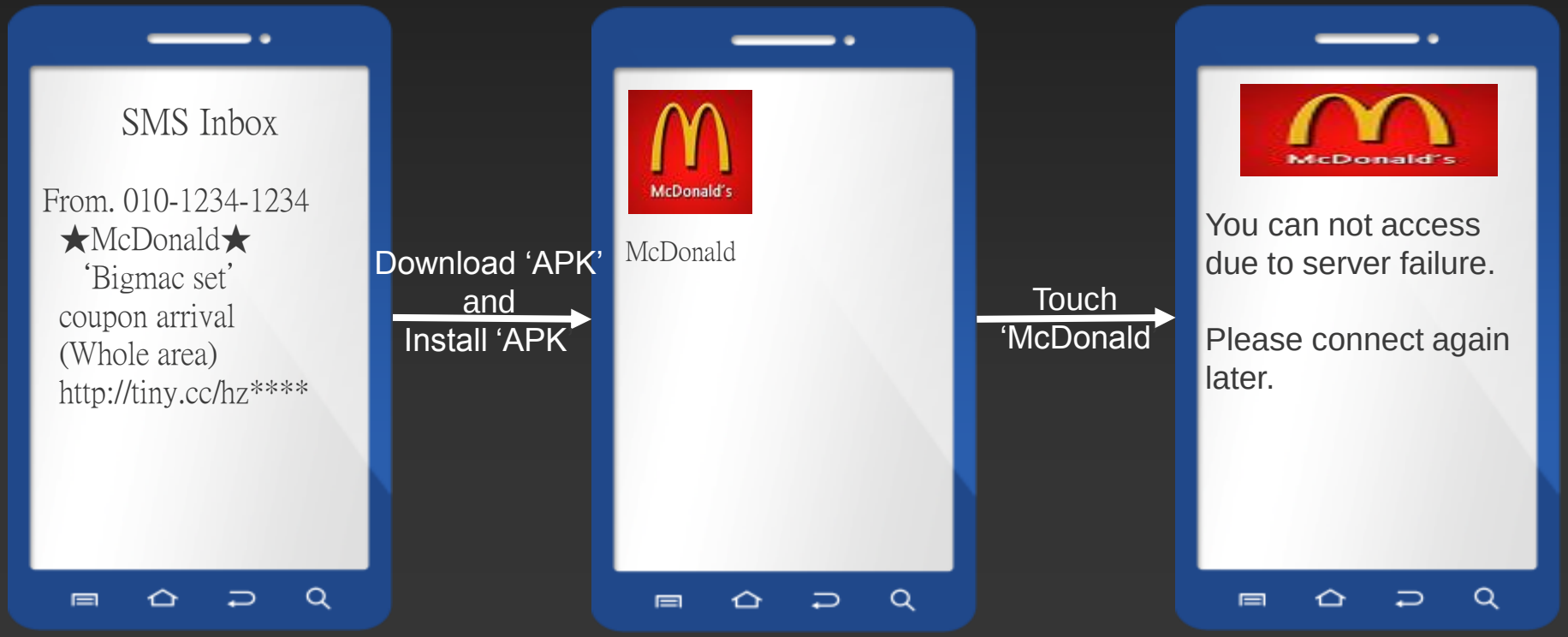


Fake banking app
: request banking information from user

© AhnLab, Inc. All rights reserved.

社交工程
Social Engineering

AhnLab



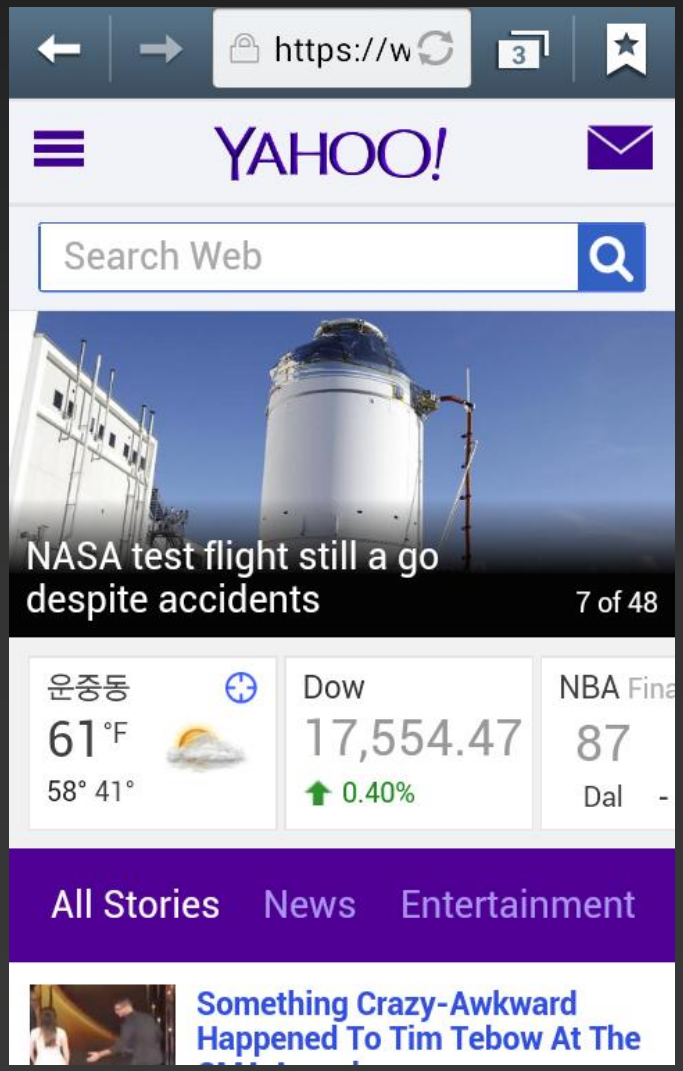
A month later….. $300 was added to the phone bill of the users

© AhnLab, Inc. All rights reserved.

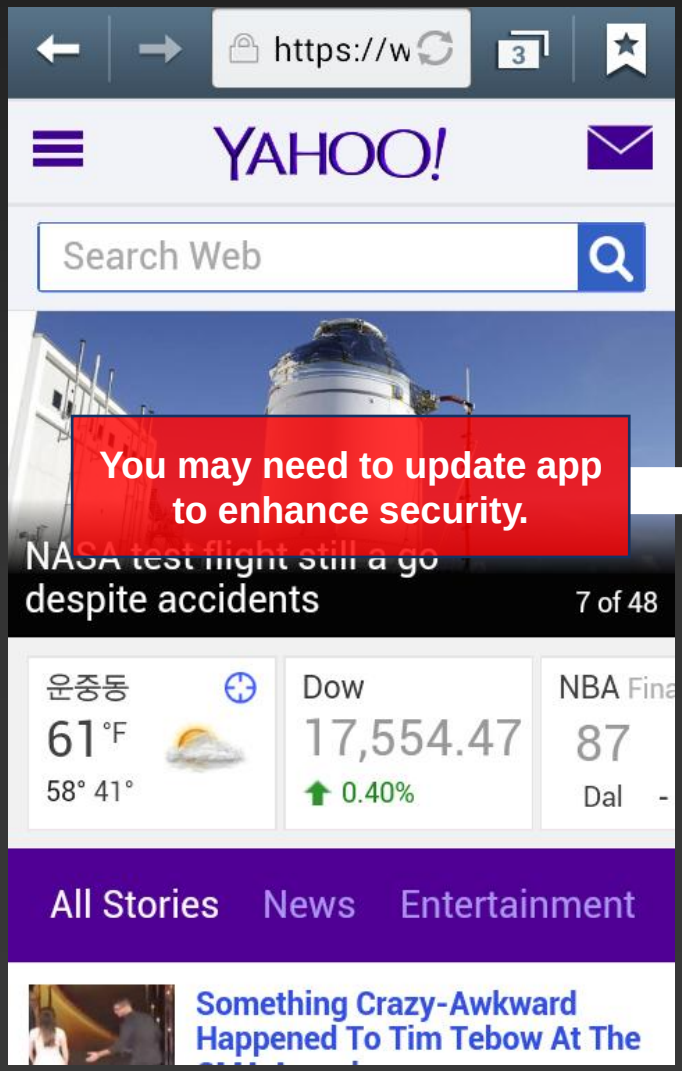
無線路由器的漏洞
Wireless router vulnerabilities

AhnLab

- Connected to normal AP



- Connected to AP in changed DNS



Download malware 'APK'

© AhnLab, Inc. All rights reserved.

Attacking Anti-Virus Apps

AhnLab

```
- uses-permission -
<uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
```

```
private void FV(Context p4) {
    p4.getSystemService("activity").killBackgroundProcesses(Conf.LV);
    return;
}
```

```
Conf.LV = "com.ahnlab.v3mobileplus";
```

- Shutting down the anti-virus apps

```
v5 = this.getPackageManager();
v2 = v5.getInstalledApplications(8192);
v1 = 0;
while (v1 < v2.size()) {
    v0 = v2.get(v1);
    if(v0.loadLabel(v5).equalsIgnoreCase(AppContacts.aname) != 0) {
        v6 = new Intent("android.intent.action.DELETE", Uri.parse(new StringBuilder("package:").append(v0.packageName).toString()));
        v6.addFlags(268435456);
        this.startActivity(v6);
    }
```

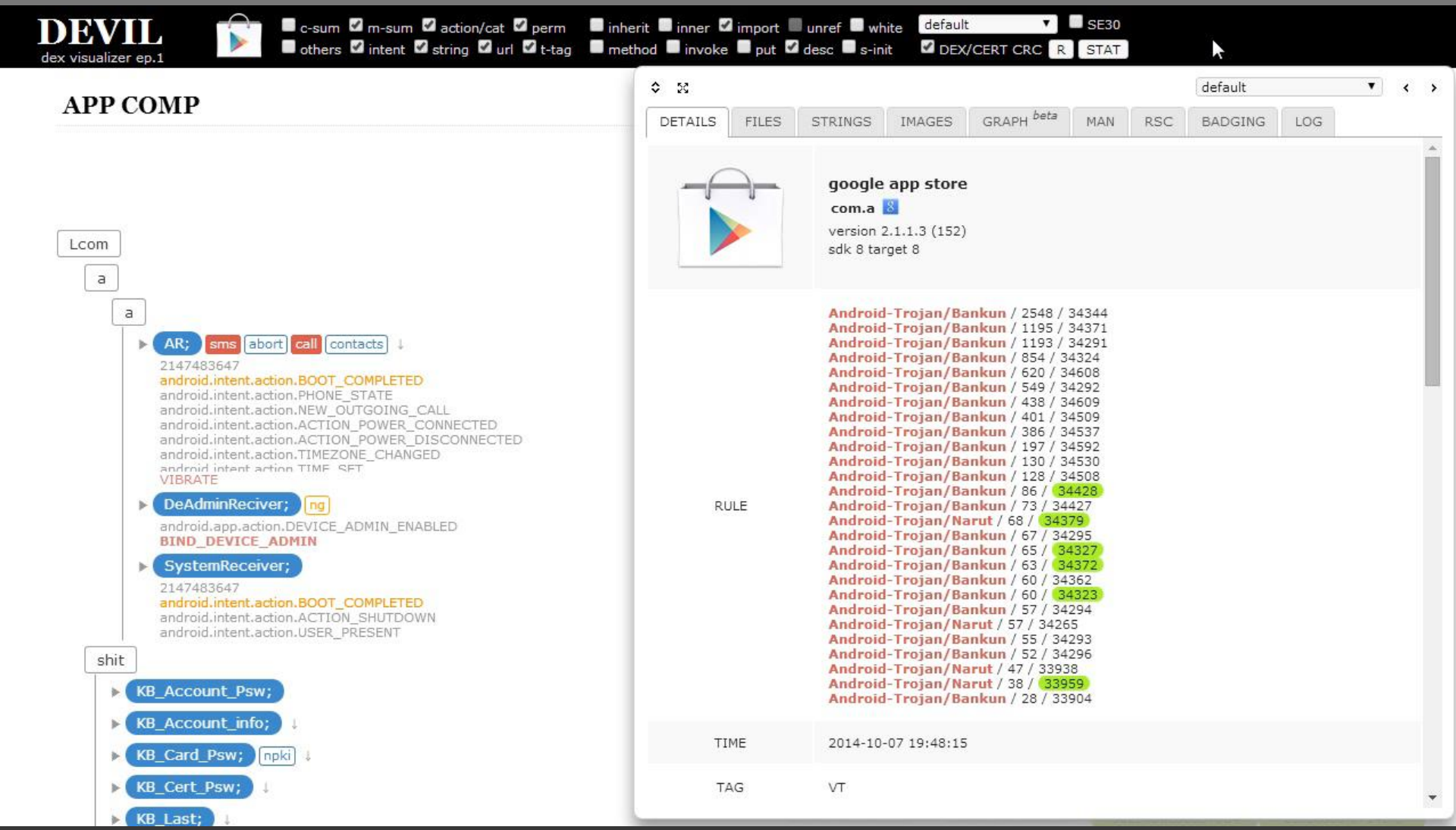
```
static AppContacts() {
        ..........
        AppContacts.aname = "AhnLab V3 Mobile Plus 2.0";
        ..........
    }
```

- Uninstalling anti-virus apps

© AhnLab, Inc. All rights reserved.

DEVIL – DEX Visualizer

AhnLab



© AhnLab, Inc. All rights reserved.

5. Always Be Prepared

Always Be Prepared

AhnLab

Full use of the functions

Unknown Source

[사이버경찰청] 출석요구서

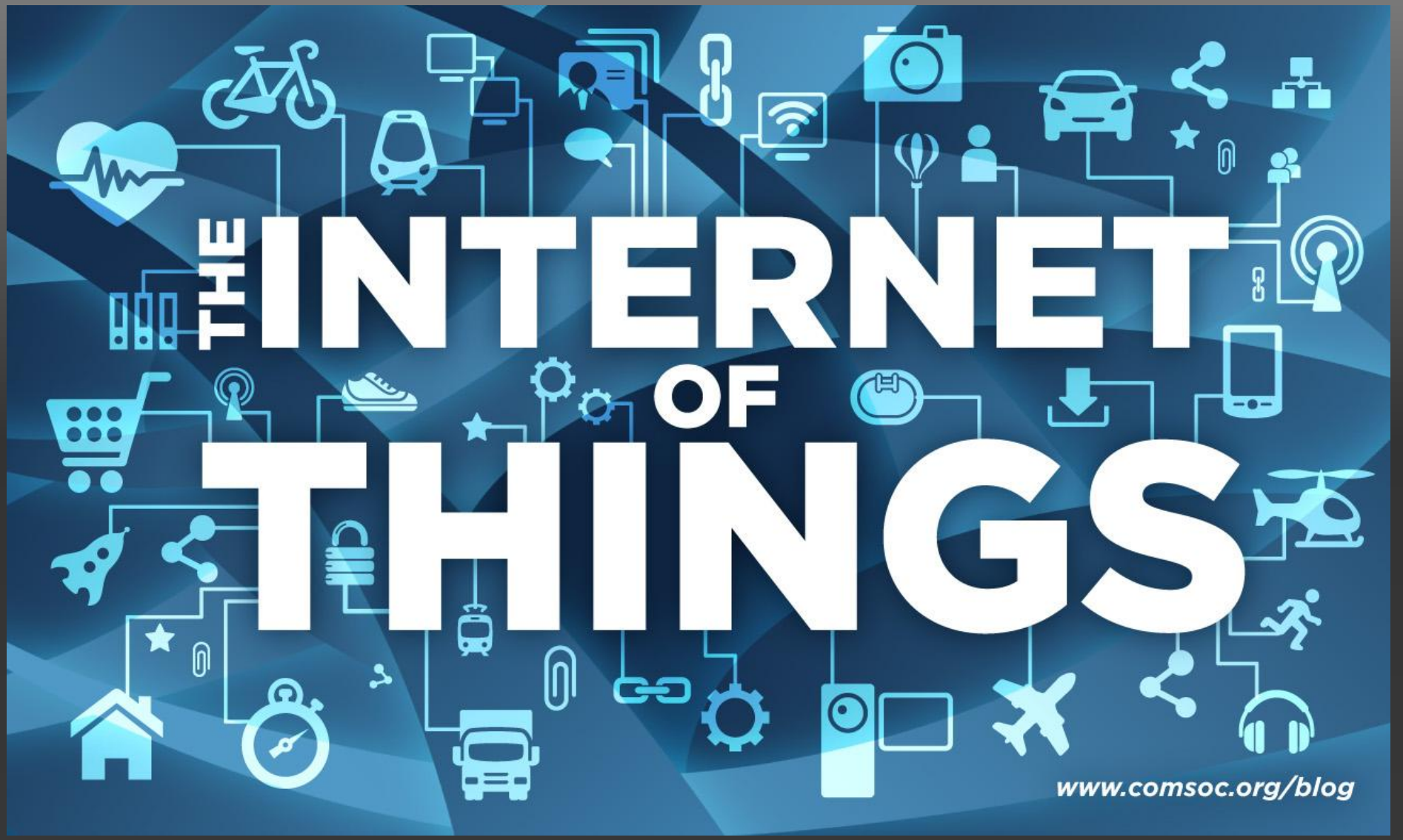
URL included

사건조회후출석일시확인

www.onlainn.com

© AhnLab, Inc. All rights reserved.

Always Be Prepared



© AhnLab, Inc. All rights reserved.

DESIGN YOUR SECURITY