Abstrak

Hanya lebih dari sebulan lalu, pengguna iOS yang memperingatkan ancaman untuk perangkat mereka dengan malware XcodeGhost. Apple cepat menanggapi, mencatat aplikasi yang terinfeksi dari App Store dan mengeluarkan fitur keamanan baru untuk menghentikan malware tersebut. Melalui pemantauan terus menerus dari jaringan pelanggan kami, para peneliti FireEye telah menemukan bahwa, meskipun respon cepat, ancaman XcodeGhost telah mempertahankan vulnerability dan telah dimodifikasi(menjadi backdoor).
Kata kunci : xcodeghost, ios,App sore, backdoor.

1. Pendahuluan

Para *Researcher* baru-baru ini menemukan sepotong iOS malware yang disebut XcodeGhost di sejumlah aplikasi di Apple App Store. Pembuat malware XcodeGhost mampu membuat kode berbahaya ke aplikasi ini tanpa sepengetahuan para pengembang aplikasi '. Aplikasi ini tidak curiga termasuk aplikasi konsumen populer seperti WeChat dan CamCard, menampilkan potensi untuk malware XcodeGhost berdampak berpotensi ratusan juta korban.

XcodeGhost adalah bagian dari malware yang dapat mencuri data dan berpotensi mengelabui orang agar memberikan informasi pribadi. Pembuat malware XcodeGhost mampu mengemas alat yang digunakan oleh iOS yang sah dan pengembang OSX untuk membuat aplikasi. Ketika para pengembang menciptakan aplikasi mereka menggunakan malware ini dirusak-dengan alat, mereka tidak sadar dimasukkan ke dalam aplikasi mereka, meskipun para pengembang tidak perlu sengaja menonaktifkan beberapa pemeriksaan keamanan untuk menggunakan alat ini.

Penulis membahas sebuah study komprehensif untuk dapat mengamati aktifitas Malware, menunjukkan bahaya serangan malware xcodeghost pada aplikasi wechat di ios pada

1.1 Rumusan Masalah

malware membuat jalan ke daftar tumbuh aplikasi yang diterbitkan hidup dengan Apple App Store. Pemahaman kami adalah bahwa Apple sedang bekerja untuk menghapus aplikasi ini dari App Store

Berdasarkan uraian latar belakang masalah diatas, maka dapat di ambil rumusan masalah, yaitu bagaimana menganalisis xcodeghost malware.

1.2 Batasan Masalah

Batasan masalah pada penelitian ini dipaparkan sebagai berikut

1. Malware yang digunakan berbasis ipk pada piranti ios.
2. Menggunakan script phyton sebagai eksekusi malware analysis
3. Menggunakan Virtualbox sebagai tools untuk virtual server
4. Menggunakan windows di virtualbox dan linux operating system
5. Tidak menggunakan Snort sebagai deteksi. Deteksi menggunakan wireshark dan collasoft sebagai alat bantu.
6. Menggunakan virustotal.com, hybrid-analysis.com dan malwr.com sebagai perbandingan
7. Menggunakan tools ollydbg sebagai tools pembantu analisis.

1.3 Tujuan Penulisan

Berdasarkan uraian dari latar belakang masalah maka penulis, memiliki tujuan penelitian yaitu :

1. Menerapkan bahaya dan pencegahan terhadap malware xcodeghost

1.4 Manfaat Penulisan

1. Sebagai tindakan *awareness* dari tim malware ID-SIRTII untuk pencegahan malware xcodeghost di indonesia dan malware yang sejenisnya.
2. Sebagai referensi bagi peneliti lain yang ingin melakukan penelitian dalam bidang keamanan jaringan dan keamanan sistem komputer

1.5 Metodelogi Penelitian

1. Penulis juga menggunakan study literatur dan study pustaka yang bertujuan untuk mengambil semua bahan tentang malware terutama sandworm malware.

Sistematika penulisan

BAB 1 Pendahuluan

Pada bab ini penulis memberikan gambaran umum tentang penelitian ini dan latar belakang mengenai penelitian ini

BAB 2 Landasan Teori

Pada bab ini penulis memerikan tentang landasan teori yang digunakan dalam melakukan penelitian ini.

BAB 3 Pembahasan

Pada bab ini penulis membahasa tentang malware xcodeghost

BAB 4 Kesimpulan

Pada bab ini penulis membahas tentang kesimpulan

2. Landasan Teori

2.1 Malware

Malware (worm, virus dan trojan) adalah sebuah ancaman baik yang dikenal dalam dunia computing dan komunitas networking (mzheng & pclee & sclui 2012). Malware (malicious software) adalah sebuah ancaman serius dalam cyber security (gregio & paulo & vigna 2012). Malware berasal dari dua kata kombinasi yaitu malicious dan software, dan digunakan untukl indikasi banyak program yang tidak diinginkan. Menurut G, McGraw and Morrisett malware sebagai code yang ditambah, dirubah dari sebuah sofware dalam perintah dengan sengaja membahayakan atau merusak fungsi utama dalam sistem.

Pengertian komputer forensik secara umum adalah sebuah proses keilmuan yang digunakan untuk mengumpulkan, menganalisa serta menghadirkan barang bukti pada sebuah aktivitas kejahatan yang melibatkan teknologi komputer. Dalam perkembangannya komputer forensik saat ini lebih dikenal dengan digital forensik hal ini karena dampak dari pesatnya perkembangan teknologi komputer yang bukan hanya berbentuk komputer konvensional tapi juga mencakup semua perangkat digital yang menggunakan prinsip kerja teknologi komputer didalamnya.

Beberapa pengertian dari digital forensik adalah sebagai berikut :

a. Dr. H. B. Wolfe, serangkaian metode teknik dan prosedur untuk mengumpulkan bukti dari peralatan dan berbagai perangkat penyimpanan media komputasi digital, yang dapat disajikan di pengadilan dalam format yang koheren dan bermakna.

b. Steve Hailey Pemeliharaan, identifikasi, ekstraksi, interpretasi, dan dokumentasi bukti komputer, untuk memasukan aturan bukti, proses hukum, integritas bukti, pelaporan faktual dari informasi yang ditemukan, dan memberikan pendapat ahli dalam pengadilan hukum atau lainnya hukum dan atau proses administratif sebagaimana dengan apa yang ditemukan.

c. Marcella, Digital Forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam kejahatan computer.

Tujuan malware xcodeghost

iOS apps dapat diinfeksi dengan XcodeGhost malware and melakukan koleksi informasi tentang device-device dan kemudian melakukan encrypt dan upload data tersebut ke command

dan control (C2) servers yang dijalankan oleh attackers melalui HTTP protocol. system and app information itu yang dapat di kumpulkan termasuk:

- Current time
- Current infected app’s name
- The app’s bundle identifier
- Current device’s name and type
- Current system’s language and country
- Current device’s UUID
- Network type

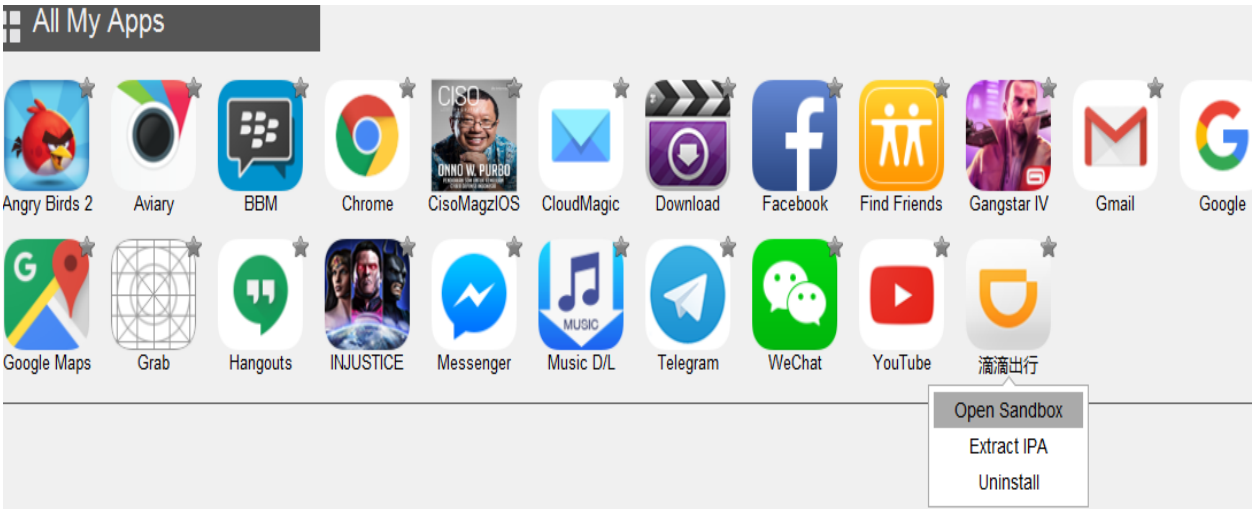
Bab 3 Pembahasan

Fox-IT (fox-it.com), sebuah perusahaan keamanan berbasis di Belanda, memeriksa semua nama domain C2 dari laporan kami di sensor jaringan mereka dan telah menemukan ribuan lalu lintas berbahaya di luar Cina. Menurut data mereka, iOS aplikasi ini juga terinfeksi:

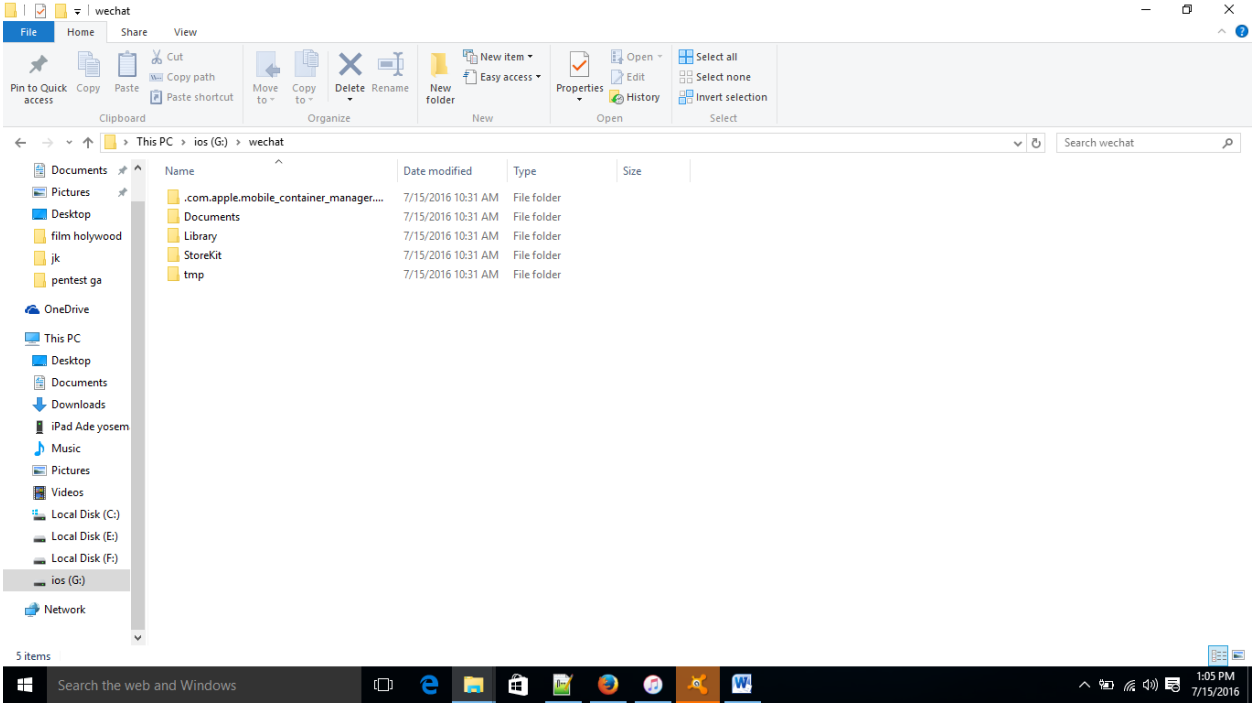
iOS apps dapat diinfeksi dengan XcodeGhost malware and melakukan koleksi informasi tentang device-device dan kemudian melakukan encrypt dan upload data tersebut ke command dan control (C2) servers yang dijalankan oleh attackers melalui HTTP protocol. system and app information itu yang dapat di kumpulkan termasuk:

- Current time
- Current infected app’s name
- The app’s bundle identifier
- Current device’s name and type
- Current system’s language and country
- Current device’s UUID
- Network type

Aplikasi wechat dalam ios

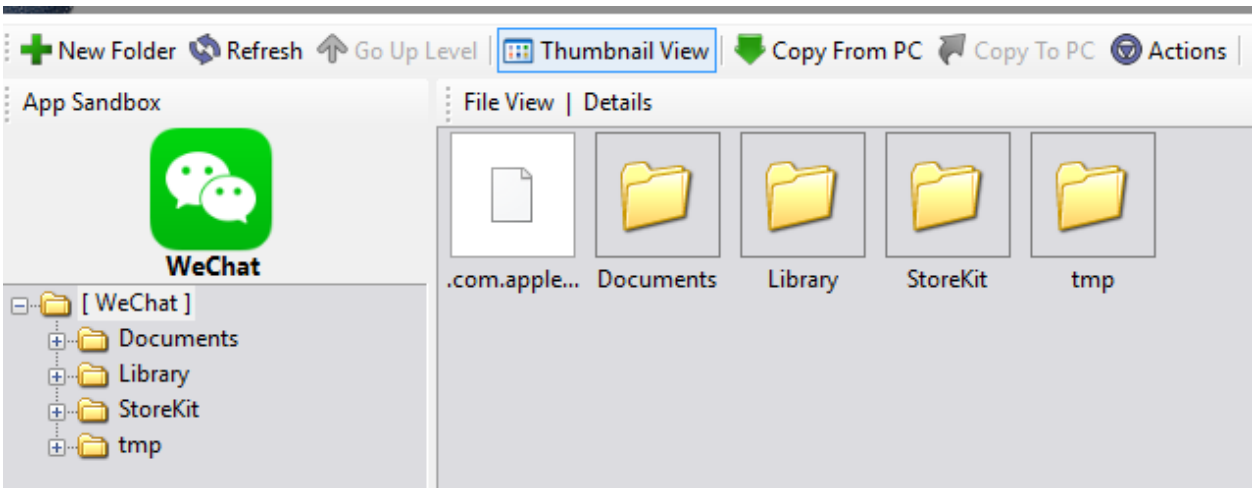


Aplikasi wechat setelah di ektrak

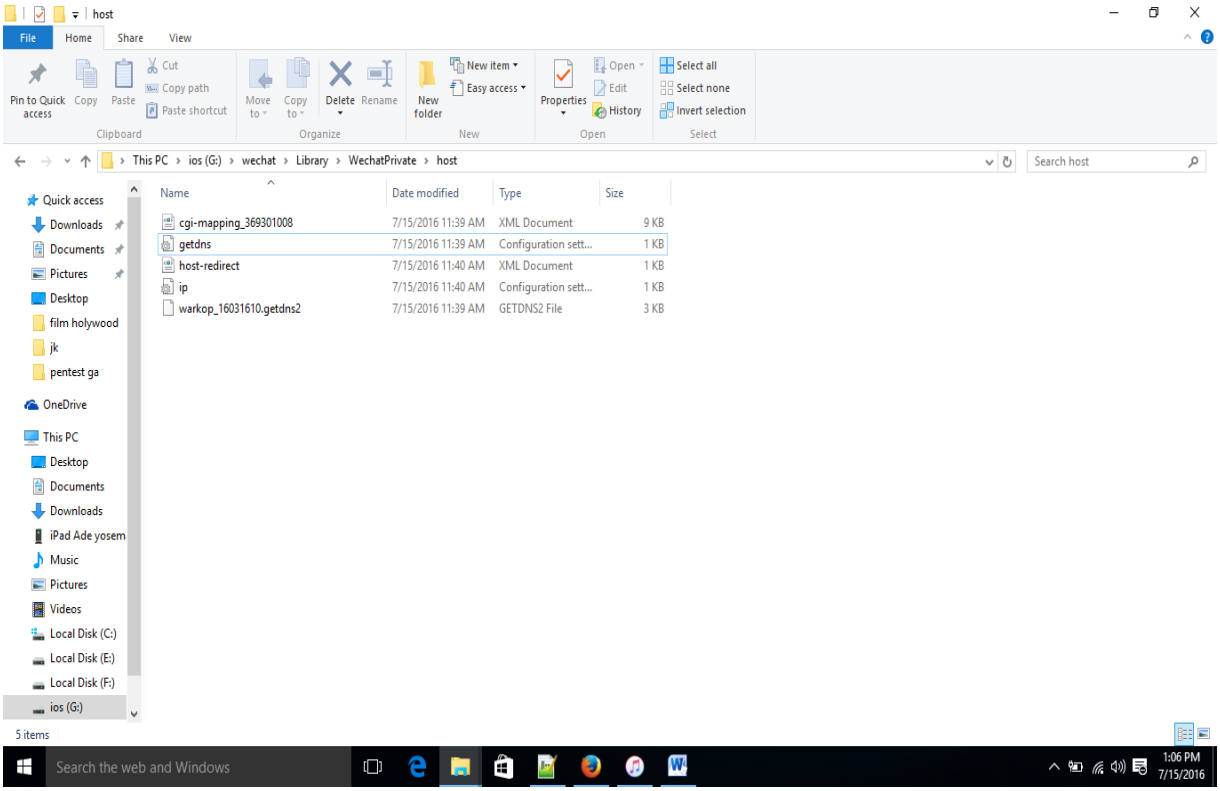


Setelah .ipa di ekstrak ke dalam folder dengan menggunakan ifunbox pada laptop/pc.informasi infunbox bisa di download

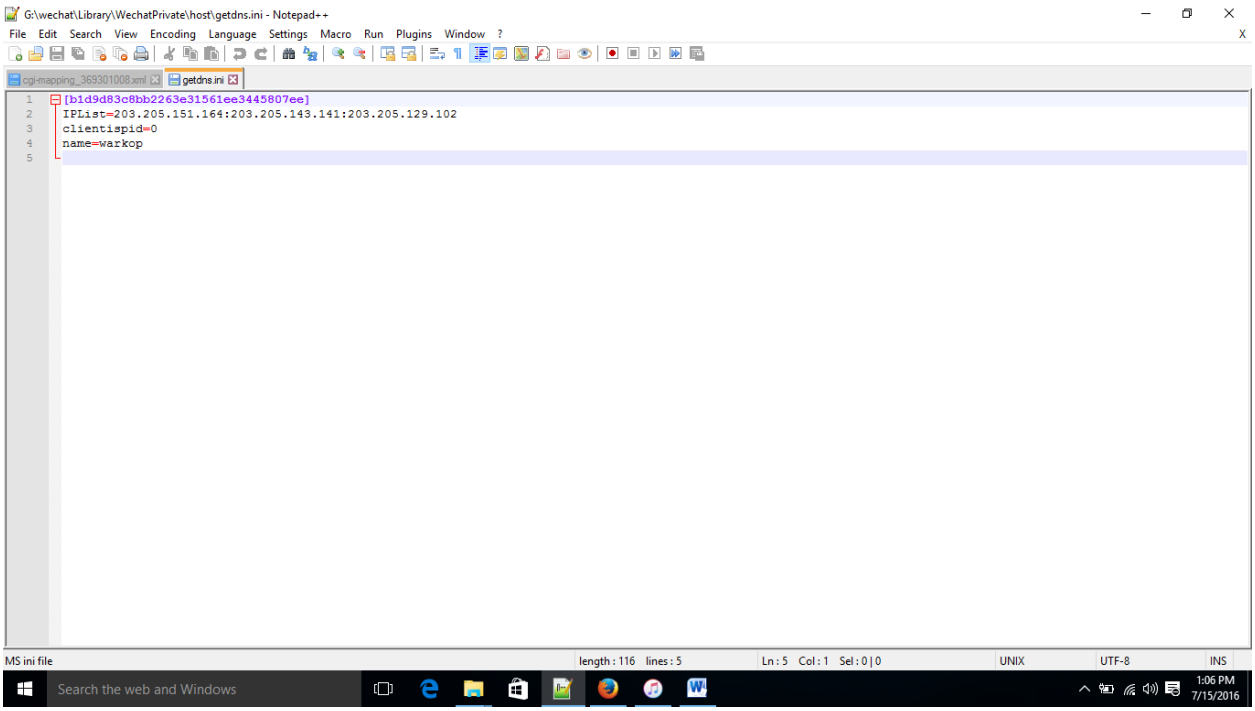
Wechat structures



Penulis membuka folder pada G:\wechat\Library\WechatPrivate\host.



Wechat menyimpan informasi dns users dan wifi ssid ‘



Setelah penulis membuka file getdns.ini (configuration settings) G:\wechat\Library\WechatPrivate\host penulis dapatkan

[b1d9d83c8bb2263e31561ee3445807ee]

IPList=203.205.151.164:203.205.143.141:203.205.129.102

clientispid=0

name=warkop

yang artinya bahwa aplikasi wechat pada smartphone tersebut menyimpan alamat ip **203.205.151.164 (**Shenzhen Tencent Computer Systems Company Limited)

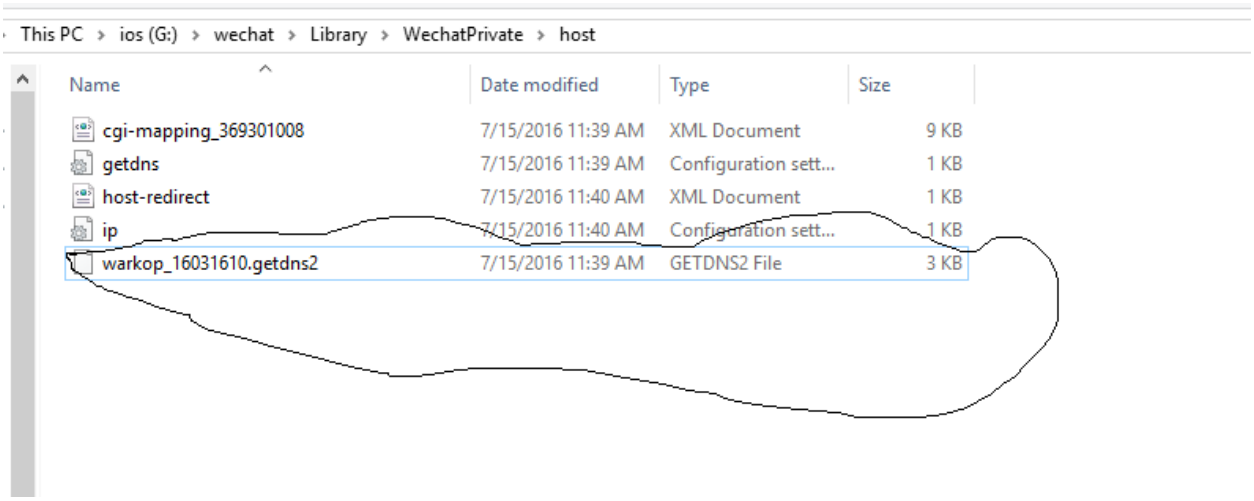
IP Address 203.205.151.164

```
inetnum:        203.205.128.0 - 203.205.159.255
netname:        TENCENT-NET-AP
descr:          Shenzhen Tencent Computer Systems Company Limited
descr:          Tencent Building, Kejizhongyi Avenue,Hi-techPark,
descr:          NanshanDistrict, Shenzhen
country:        CN
admin-c:        DR196-AP
tech-c:         JW2054-AP
mnt-by:         MAINT-CNNIC-AP
mnt-routes:     MAINT-TENCENT-NET-AP-CN
mnt-irt:        IRT-CNNIC-CN
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20110411
```

```
source:         APNIC

irt:            IRT-CNNIC-CN
address:        Beijing, China
e-mail:         ipas@cnnic.cn
abuse-mailbox:  ipas@cnnic.cn
admin-c:        IP50-AP
tech-c:         IP50-AP
auth:           # Filtered
remarks:        Please note that CNNIC is not an ISP and is not
remarks:        empowered to investigate complaints of network abuse.
remarks:        Please contact the tech-c or admin-c of the network.
mnt-by:         MAINT-CNNIC-AP
changed:        ipas@cnnic.cn 20110428
source:         APNIC

person:         Dreams Ruan
address:        Tencent Building, Kejizhongyi Avenue, Hi-
techPark,Nanshan District,Shenzhen
country:        CN
phone:          +86-755-86013388-84520
fax-no:         +86-755-86013030
e-mail:         dreamsruan@tencent.com
nic-hdl:        DR196-AP
mnt-by:         MAINT-CNNIC-AP
changed:        ipas@cnnic.cn 20100510
source:         APNIC

person:         Jsquare Wu
address:        Tencent Building, Kejizhongyi Avenue, Hi-
techPark,Nanshan District,Shenzhen
country:        CN
phone:          +86-755-86013388-88441
fax-no:         +86-755-86013030
e-mail:         jsquare@tencent.com
nic-hdl:        JW2054-AP
mnt-by:         MAINT-CNNIC-AP
changed:        ipas@cnnic.cn 20100510
source:         APNIC

route:          203.205.128.0/19
descr:          Tencent routes
```

```
origin:         AS132203
notify:         martyma@tencent.com
mnt-lower:      MAINT-TENCENT-NET-AP-CN
mnt-routes:     MAINT-TENCENT-NET-AP-CN
mnt-by:         MAINT-TENCENT-NET-AP-CN
changed:        martyma@tencent.com 20130109
source:         APNIC
```

203.205.143.141 (Shenzhen Tencent Computer Systems Company Limited)
203.205.129.102 (Shenzhen Tencent Computer Systems Company Limited)
Name=warkop (salah satu nama wifi RND di Id-SIRTII/cc)



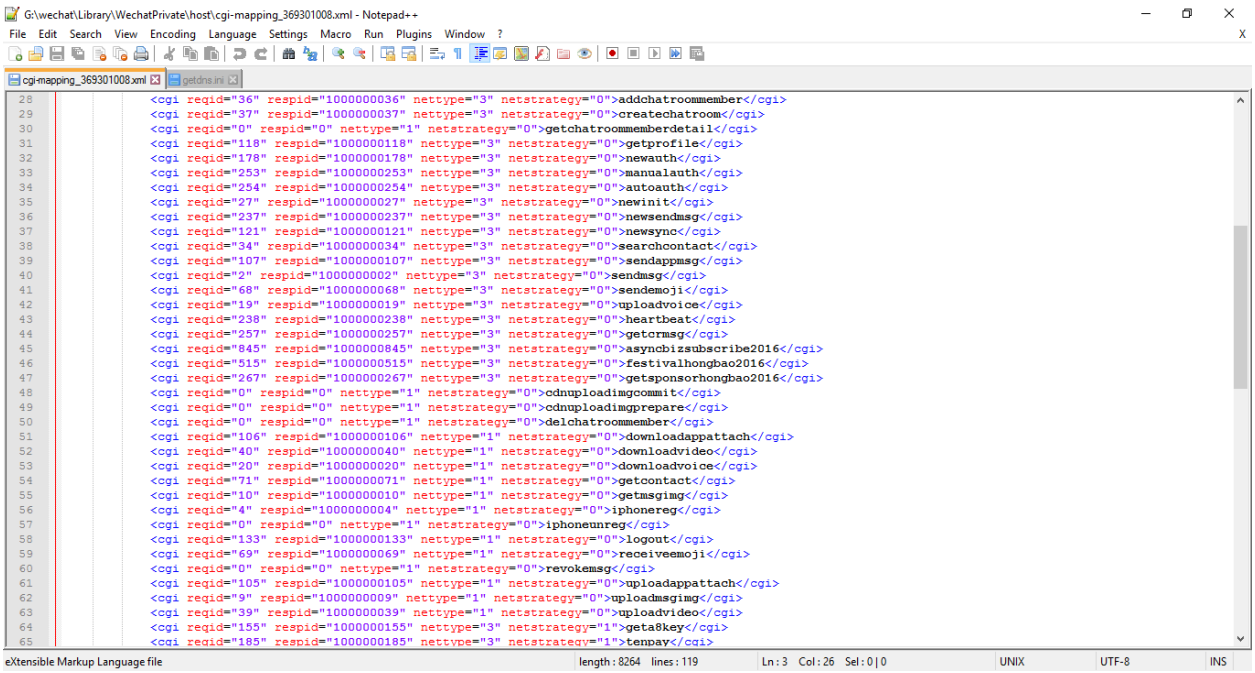
Wechat menyimpan *iphonereg/ iPhoneRegistration* dari users

Penulis juga menemukan xml berisi <cgi reqid="4" respid="1000000004" nettype="1" netstrategy="0">iphonereg</cgi>

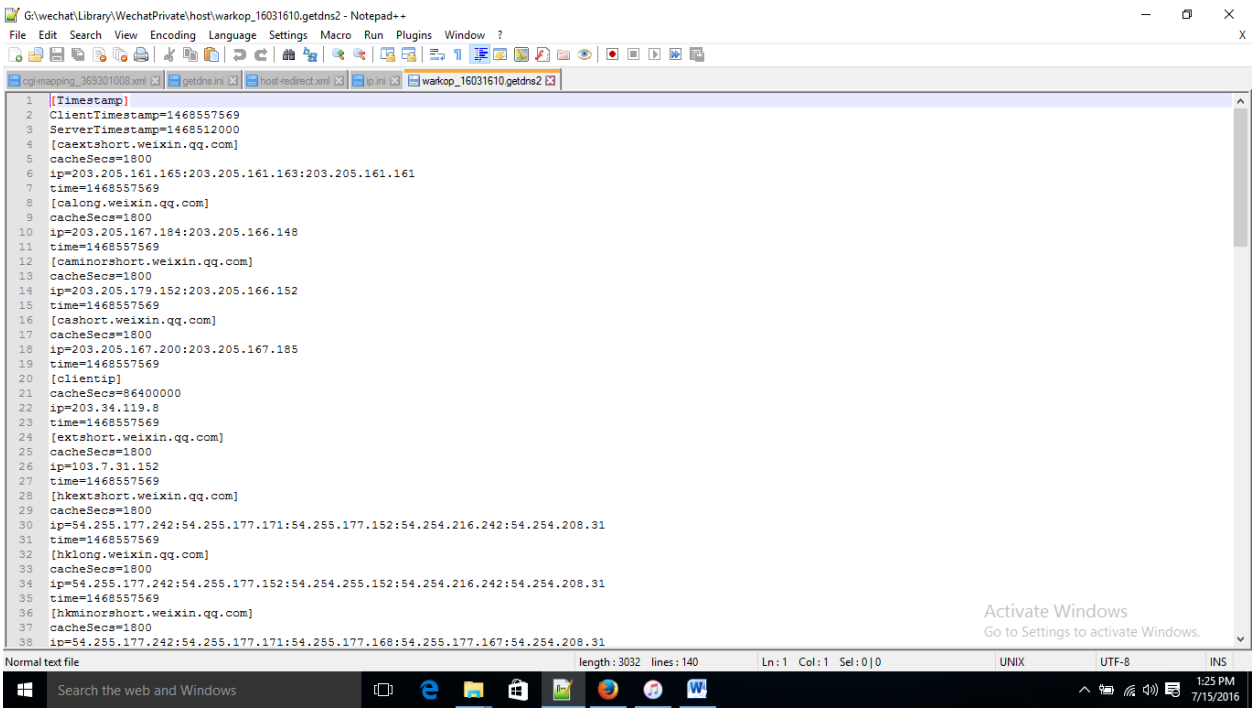
<cgi reqid="0" respid="0" nettype="1" netstrategy="0">iphoneunreg</cgi>

<cgi reqid="133" respid="1000000133" nettype="1" netstrategy="0">logout</cgi>

Bahwa aplikasi wechat juga mencatat imei iphone penguna dalam bagian xml.



C n C server telah menginfeksi ios devices sebagai zombies dengan menginfeksi ios device pengguna



Pada gambar di atas penulis mendapatkan informasi data yang bersumber dari G:\wechat\Library\WechatPrivate\host\warkop_16031610.getdns2 yaitu

ip=203.205.161.165:203.205.161.163:203.205.161.161 (Shenzhen Tencent Computer Systems Company Limited)
time=1468557569
[calong.weixin.qq.com]
cacheSecs=1800
ip=203.205.167.184:203.205.166.148 161 (Shenzhen Tencent Computer Systems Company Limited)
time=1468557569
[caminorshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.179.152:203.205.166.152
time=1468557569
[cashort.weixin.qq.com]
cacheSecs=1800
ip=203.205.167.200:203.205.167.185
time=1468557569
[clientip]
cacheSecs=86400000
ip=203.34.119.8
time=1468557569
[extshort.weixin.qq.com]
cacheSecs=1800
ip=103.7.31.152
time=1468557569
[hkextshort.weixin.qq.com]
cacheSecs=1800
ip=54.255.177.242:54.255.177.171:54.255.177.152:54.254.216.242:54.254.208.31
time=1468557569
[hklong.weixin.qq.com]
cacheSecs=1800
ip=54.255.177.242:54.255.177.152:54.254.255.152:54.254.216.242:54.254.208.31
time=1468557569
[hkminorshort.weixin.qq.com]
cacheSecs=1800
ip=54.255.177.242:54.255.177.171:54.255.177.168:54.255.177.167:54.254.208.31
time=1468557569
[hkshort.weixin.qq.com]

cacheSecs=1800
ip=54.255.177.242:54.255.177.171:54.255.177.168:54.254.255.152:54.254.208.31
time=1468557569
[localhost]
cacheSecs=1800
ip=127.0.0.1
time=1468557569
[long.weixin.qq.com]
cacheSecs=1800
ip=103.7.31.151
time=1468557569
[minorshort.weixin.qq.com]
cacheSecs=1800
ip=103.7.31.152
time=1468557569
[mlextshort.weixin.qq.com]
cacheSecs=1800
ip=117.191.87.144:117.191.87.143:117.191.87.139
time=1468557569
[mllong.weixin.qq.com]
cacheSecs=1800
ip=220.171.124.143:220.171.124.140:220.171.124.139
time=1468557569
[mlminorshort.weixin.qq.com]
cacheSecs=1800
ip=117.191.87.144:117.191.87.143:117.191.87.139
time=1468557569
[mlshort.weixin.qq.com]
cacheSecs=1800
ip=117.191.87.144:117.191.87.143:117.191.87.139
time=1468557569
[sh2tjextshort.weixin.qq.com]
cacheSecs=1800
ip=103.7.31.152
time=1468557569
[sh2tjlong.weixin.qq.com]
cacheSecs=1800

ip=203.205.147.218
time=1468557569
[sh2tjminorshort.weixin.qq.com]
cacheSecs=1800
ip=103.7.31.152
time=1468557569
[sh2tjshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.147.173
time=1468557569
[shextshort.weixin.qq.com]
cacheSecs=1800
ip=103.7.31.152
time=1468557569
[short.weixin.qq.com]
cacheSecs=1800
ip=103.7.31.152
time=1468557569
[sz2tjextshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.128.104
time=1468557569
[sz2tjlong.weixin.qq.com]
cacheSecs=1800
ip=203.205.147.218
time=1468557569
[sz2tjminorshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.128.104
time=1468557569
[sz2tjshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.147.173
time=1468557569
[szextshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.128.104

time=1468557569
[szlong.weixin.qq.com]
cacheSecs=1800
ip=203.205.128.103
time=1468557569
[szminorshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.128.104
time=1468557569
[szshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.128.104
time=1468557569
[tjextshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.128.104
time=1468557569
[tjlong.weixin.qq.com]
cacheSecs=1800
ip=203.205.147.218
time=1468557569
[tjshort.weixin.qq.com]
cacheSecs=1800
ip=203.205.147.173
time=1468557569

semua IP tersebut adalah ip 161 (Shenzhen Tencent Computer Systems Company Limited)

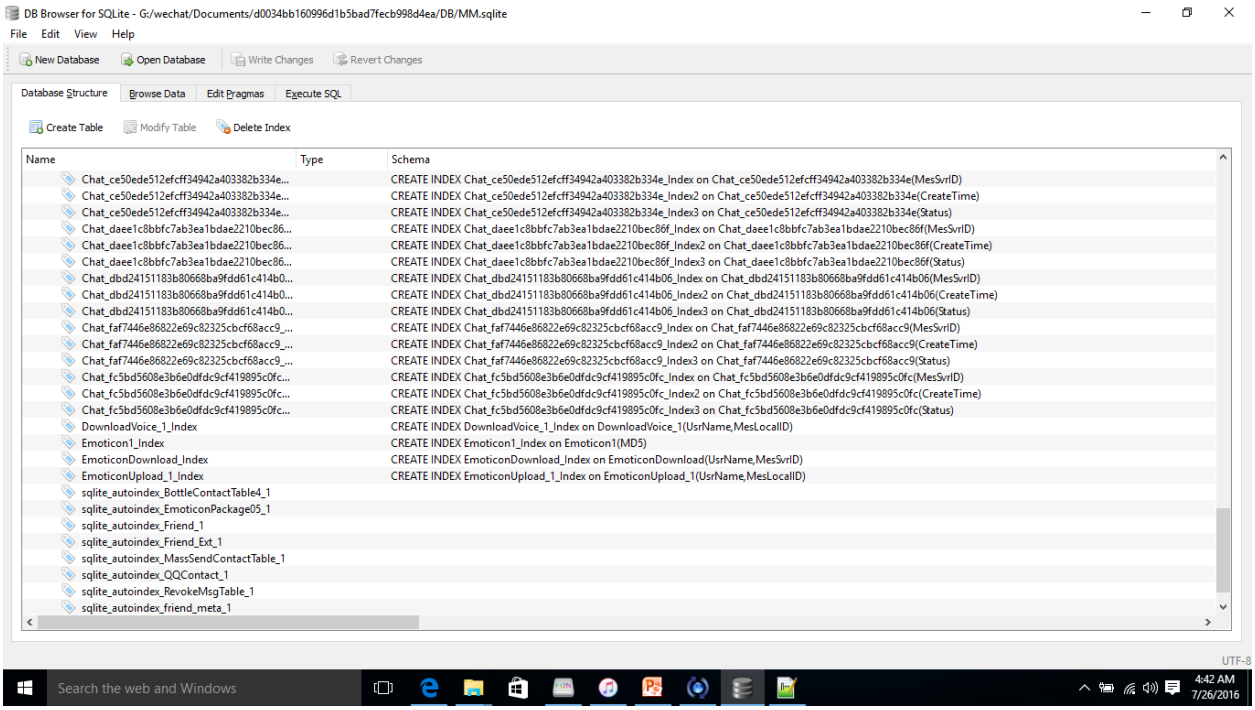
```
inetnum:        203.205.128.0 - 203.205.159.255
netname:        TENCENT-NET-AP
descr:          Shenzhen Tencent Computer Systems Company Limited
descr:          Tencent Building, Kejizhongyi Avenue,Hi-techPark,
descr:          NanshanDistrict, Shenzhen
```

kesimpulan bahwa aplikasi wechat mengumpulkan informasi seperti Current device's UUID,Network type current time yang mengacu pada tujuan malware itu sendiri yang mennggumpulkan informasi dat pengguna/information gathering (lihat pada bab 2 landasan teori).

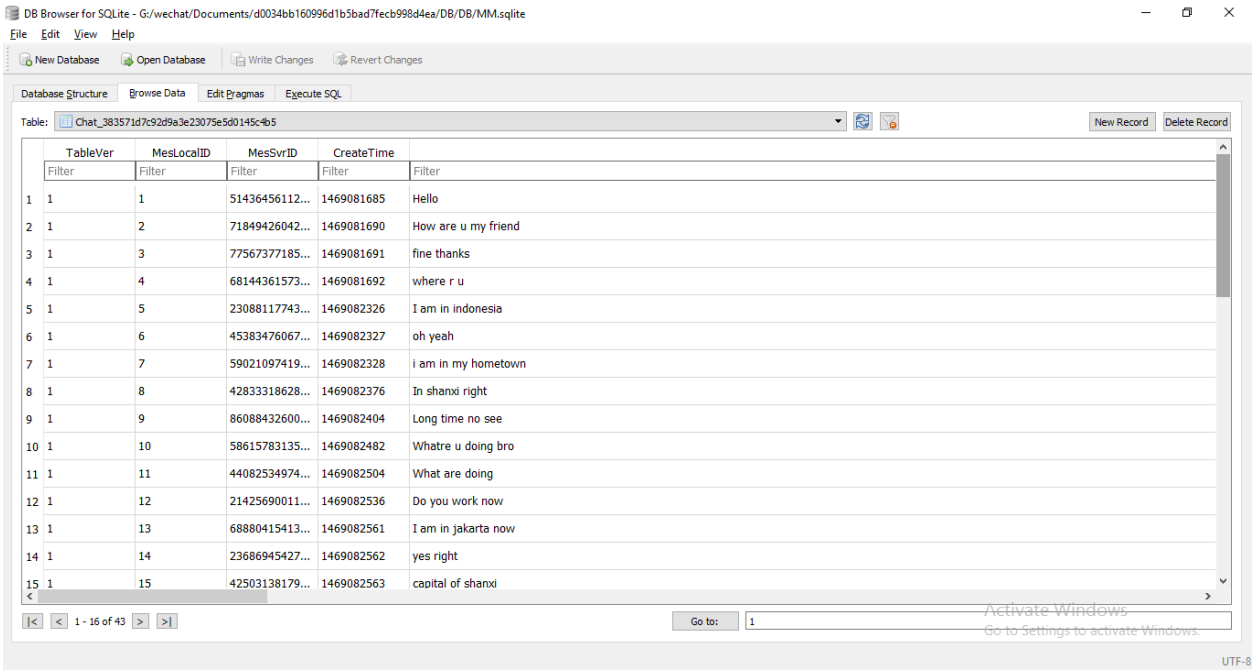
Penulis jug mendapatkan finding bahwa dalam directory G:\wechat\Documents\d0034bb160996d1b5bad7fecb998d4ea\DB ditemukan penyimpan history

chatting users disimpan dalam file tersebut(MM.sqlite). penulis menggunkan tools DB.Browser.for.SQLite-3.9.1-win32 untuk membuka file .sqlite tersebut .

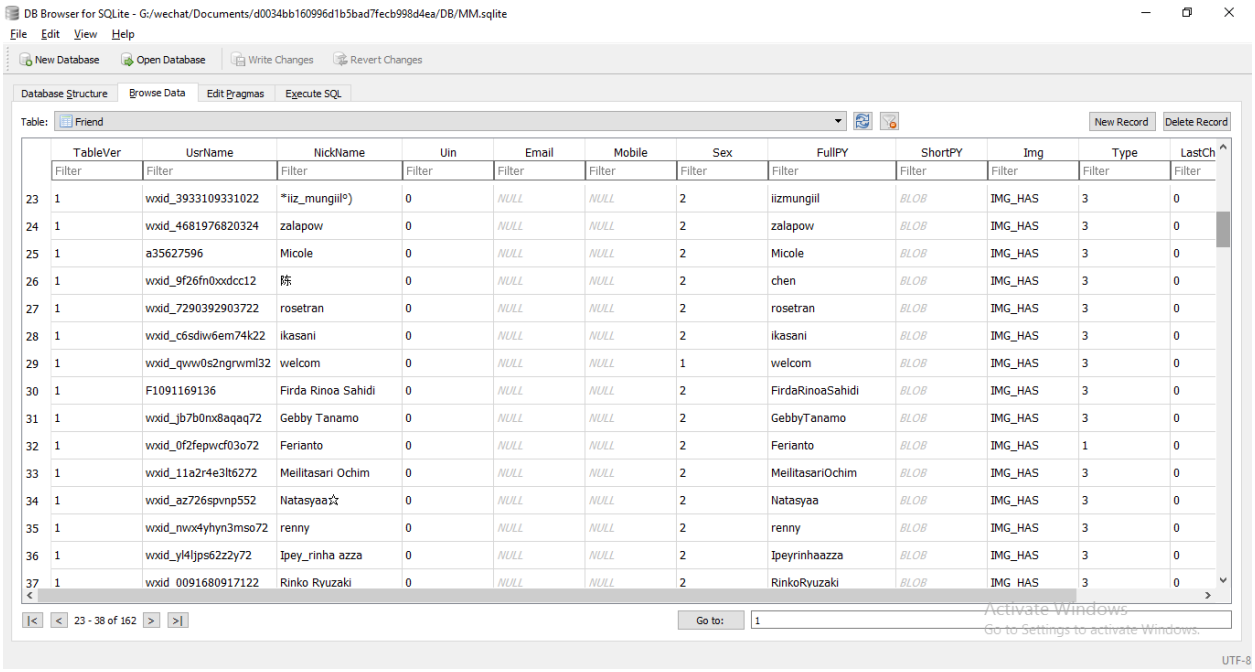
Database chat dan database setting di store pada local



Message pada wechat tidak di encrypt



Friend list di wechat jug tidak di encrypt



Kesimpulan aplikasi wechat tidak menggunakan enkripsi sehingga data dengan mudah di baca tanpa harus melakukan decode dan data diikumpulkan pada file direktori wechat tersebut sehingga rawan terkena data leak / pencurian data informasi pengguna

Sedang whats app meluncurkan end to end encryption

Enkripsi WhatsApp end-to-end ini adalah untuk mengamankan data berkirim pesan para penggunanya tanpa harus takut data tersebut disadap oleh pihak ketiga (pemerintah bahkan pihak whatsApp sekalipun tak bisa mengetahui apa saja yang kamu kirim). Encrypsi dengan mengunakn aes 256 dalam mode cbc dan HMAC –SHA256 untuk otentifikasi

Kesimpulan

Bahwa xcodeghost menginfeksi pengguna ios yang rentan pada aplikasi chatting. Vulnerability terkait dengan enkripsi yang tidak digunaka pada aplikasi wechat sehingga data confidential rentan untuk di leak atau terkena sniff.

Kesimpulan

1. Sebagai awareness kepada masyarakat agar lebih aware dalam memakai aplikasi pada smartphone

2. Pasang firewall dan peralatan industri yang efektif untuk memastikan perilaku komunikasi antara jaringan kontrol dan jaringan informasi untuk menerima pengawasan ketat.
3. Gunakan enkripsi aes aau sejenis sehingga data pada smartphone terhindar terkena bahaya sniffing

Daftar pustaka

[1] Prayudi, yusuf yudi , Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics, HACKING AND DIGITAL FORENSICS EXPOSE (H@DFEX 2014) – ISSN: 2338-0276. 2014.

[2] https://www.f-secure.com

[3] https://avcaesar.malware.lu/

[4] https://malwr.com

[5] http://virustotal.com/

[6] https://www.hybrid-analysis.com