



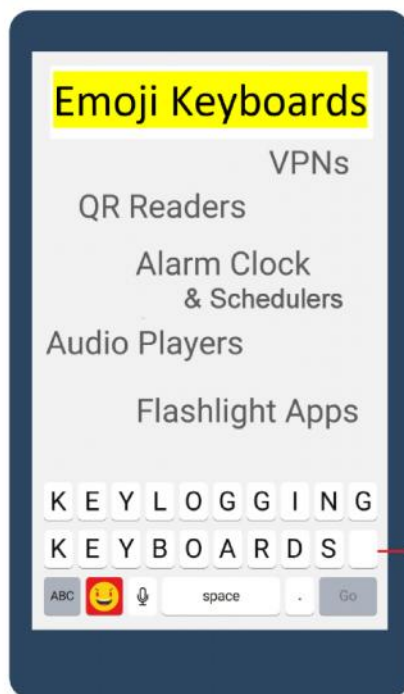
# Global Malware Pandemic:

Chinese Next Generation SmartPhone and Tablet Malware

## Threat Report: Emoji Keyboards

Exploiting Unknown Apple® iOS Vulnerabilities

(also affects Google Android)



# 孫子兵法

CONSUMER VERSION OF THIS THREAT REPORT: November 16, 2016

by Gary S. Miliefsky, fmDHS, CISSP® CEO, SnoopWall, Inc.

## Subverting a Well Designed Apple iOS Security Model

The question we asked, here at SnoopWall, was “is there hidden malware that makes it past Apple iTunes security screening, en masse?” We already know this happens all the time on Google’s Play store, but Apple? Is it even possible. Some question if the ‘counterfeit’ shopping apps that made it on the Apple iTunes store was a one time occurrence or not? It’s easy for Apple to cleanup iTunes and on November 8, 2016 they removed hundreds of counterfeit apps. But did that leave us all feeling safer and more secure? Should we trust Apple’s ability to stay one step ahead of the next threat? Is mobile banking and mobile commerce now so safe to operate on your iPhone? Could Nation state actors (and Cybercriminals) already be on your iPhone the way they have been on Chinese developed Android devices? The answers to these questions follow...

You must first understand how good of a job Apple has done at building a security model into their devices. Anyone can develop an Android smartphone, hence you hear in the news how all the Chinese made Android smartphones are ‘accidentally’ sending PII to China. Apple strongly controls and tests their hardware design to specification so it’s a stronger, closed system, from the beginning.

### **iOS is a HARDENED OS:**

iOS offers full disk encryption with built-in hardened encryption (device KEY, file KEY, Keychain API, Data Protection API, etc).

iOS currently boots with a low-level boot loader then verifies iBoot

Apple defends well against native code exploits using both address space layout randomization (ASLR) and XN bit (which stands for eXecute Never).

ASLR randomizes memory location of program executable, data, heap and stack every time it is launched.

To block cross application memory attacks the XN bit allows the OS to mark segments of a program's memory such as heap and stack as unexecutable

Jailbreaking does not allow you to disable the ios sandbox, only to run apps outside of it.

The latest version of the iPhones and iOS, are using an Elliptical Encryption Key Exchange, augmented by the onboard Cryptography Chip.

Therefore, THERE IS NO MASTER KEY.

End-user PINs are resolved via the Cryptographic Chip. 10 tries and the iPhone is ‘bricked’. Any changes to this system, would require hardware and software changes, weakening the system and leaving it vulnerable to hackers. Apple manages all multi-tasking in specially managed threads. Except Keyboard, Audio Player, Alarm Clock and VPN Client, most processes are not allowed to run in the background. Rarely are vulnerabilities uncovered, however, when they are, Apple fixes them as fast as humanly possible. Hours to days, not weeks or months. As to Google Android, numerous vulnerabilities are uncovered and fixed at a reasonable pace, however Google does not own all the hardware, so they don’t get patched fast enough. Phone manufacturers are very slow to respond, leaving gaping holes in different Android hardware.

There are some weaknesses we've uncovered in the Apple security model as follows:

**Jailbreak Detection?** Smart malware developers can create **jailbreak detection bypasses** that fake replies to function calls to make it look like the device is not jailbroken, when it still is.

In Apple's favor, they have a Secure Boot and Process Sandboxing model that's very strong.

#### **SECURE BOOT and PROCESS SANDBOXING ("Seat-belt"):**

Secure Boot

Boot rom contains Apple Public Key

Verifies the Low Level Bootloader (LLB)

However, where there is strength, there are those determined to find chinks in the armor, such as follows:

#### **EXPLOIT and REMOVE the "Seat-belt":**

Jailbreaking Exploits the Boot Loader

Breaks the 'chain' of trust

Apple can't change the Boot ROM so this is most desired place to exploit. This requires physical access to the phone.

#### **STEALING USER PHOTOS:**

In some versions of iOS, photos in

`/private/var/mobile/Media/Photos/`

the only protection against applications abusing this type of privilege is Apple's application review process. If you take check or credit card photos and do OCR, you are at risk. Better to use 3<sup>rd</sup> party ENCRYPTION libraries for storage.

So now, we turn to the **Apple iTunes Review Process?** Serious hackers have already created apps that are

**Bridging the webkit** - so you access native iOS API's via JavaScript

**Dynamic patching** - look at **InstaStock** for example by **Charlie Miller**

**Intentionally exploitable vulnerabilities** - write code with a buffer overflow that when triggered causes unseen code to execute - see **Jekyll** by **Georgia Tech**

The bottom line: To exploit an Apple iPhone or iPad remotely, users need to download apps.

#### **CONSUMER NEEDS TO DOWNLOAD AN APP:**

App must be trusted by Apple in iTunes

App must have special permissions, which are rare

If App owns network traffic or runs in background, game on.

It's that simple! As we've uncovered at SnoopWall, exclusively in this Threat Report, we've found trusted apps that are absolutely malicious in nature and even way beyond what would be acceptable 'consumer analytics' features (also known as Creepware). We've broken this down into STRONG REMOTE EXPLOITS and WEAKER REMOTE EXPLOITS. While these exploits are remotely stealing information, they must first be planted on the consumers' smartphone or tablet. And what better way than to make very attractive and feature rich apps?

**STRONG REMOTE EXPLOITS:**

**Emoji Keyboards**

VPN clients

Audio Players

Alarm Clocks

**WEAKER REMOTE EXPLOITS:**

o QR Readers

o Flashlight Apps

o Others with Malvertising

libraries collecting user data

## Our Findings

This SnoopWall Threat Report focuses on malicious apps which exploits Apple iPhone and iPad (iOS) operating system vulnerabilities and disguises themselves as trusted applications. We also cover the Google Android operating system in this report, however, it's important to note that Apple has a much more stringent security model, hence this discovery is rather unique and innovative, when it comes to taking advantage of iOS.

It's harder to poke holes in Apple devices, so some brilliant programming has taken place, mostly from what appears to be Chinese actors, employed by Chinese government owned telecommunications companies and therefore, we at SnoopWall, continue to probe to see if the developers of these Emoji Keyboards are in fact a front for 3PLA, the Third Office of the People's Liberation Army, also known as China's version of the "NSA".

This could also most likely why these exploits have not resulting in much mBanking or mCommerce fraud, even though the PII necessary to steal one's identity is absolutely being shipped to servers hosted in China. It will only be a matter of time before this causes a watershed event where mobile banks, credit unions and retailers apps suffer breaches that result in credit cards and end-users identities being sold on the black market, like we've seen traditionally from spear phishing attacks and malware targeted at the multibillion user community running Microsoft Windows. Read through to the end of this report to see if you come to the same possible two conclusions we've reached, here at SnoopWall.



**Figure 1: Trusted, yet malicious apps, in the iTunes store. *The worst offender: Emoji Keyboards***



***“This is a Global Malware Pandemic with at least ½ of all Smartphones infected, at the end-users’ discretion and acceptance”***

Gary S. Miliefsky, Cybersecurity Expert, CEO, SnoopWall, Inc.



While we’ve uncovered five kinds of applications in the Apple iTunes store that can run as background or ‘eavesdropping’ tasks, three of five are extremely limited in their capabilities. They are alarm clocks, audio players and calendar/scheduling applications. The two most onerous are VPN clients and Emoji Keyboards. The VPNs are sending packets to servers all over the globe, however, as the data is encrypted, it’s hard to prove they copy the unencrypted information off to criminal or nation state servers. In summary, we’re focused on the most

heavily downloaded applications in which we've been able to collect enough evidence that they are truly malicious in nature and being used as covert spyware tools – the Emoji Keyboards.

On Apple, we estimate at least 50% of devices are infected – that's roughly 250,000,000 while on Android, we find, as they are more popular devices, also roughly 500,000,000 infected, maybe more than 50%. What's so interesting about these Emoji Keyboards is that they are exploiting one of the only remaining holes we've found on iOS for an app to collect all personally identifiable information (PII) all the time. Once a user has overlaid their default keyboard with a third party keyboard, and given it permission to run, it has escalated privileges over any other app, with the VPN coming in second for special permissions.

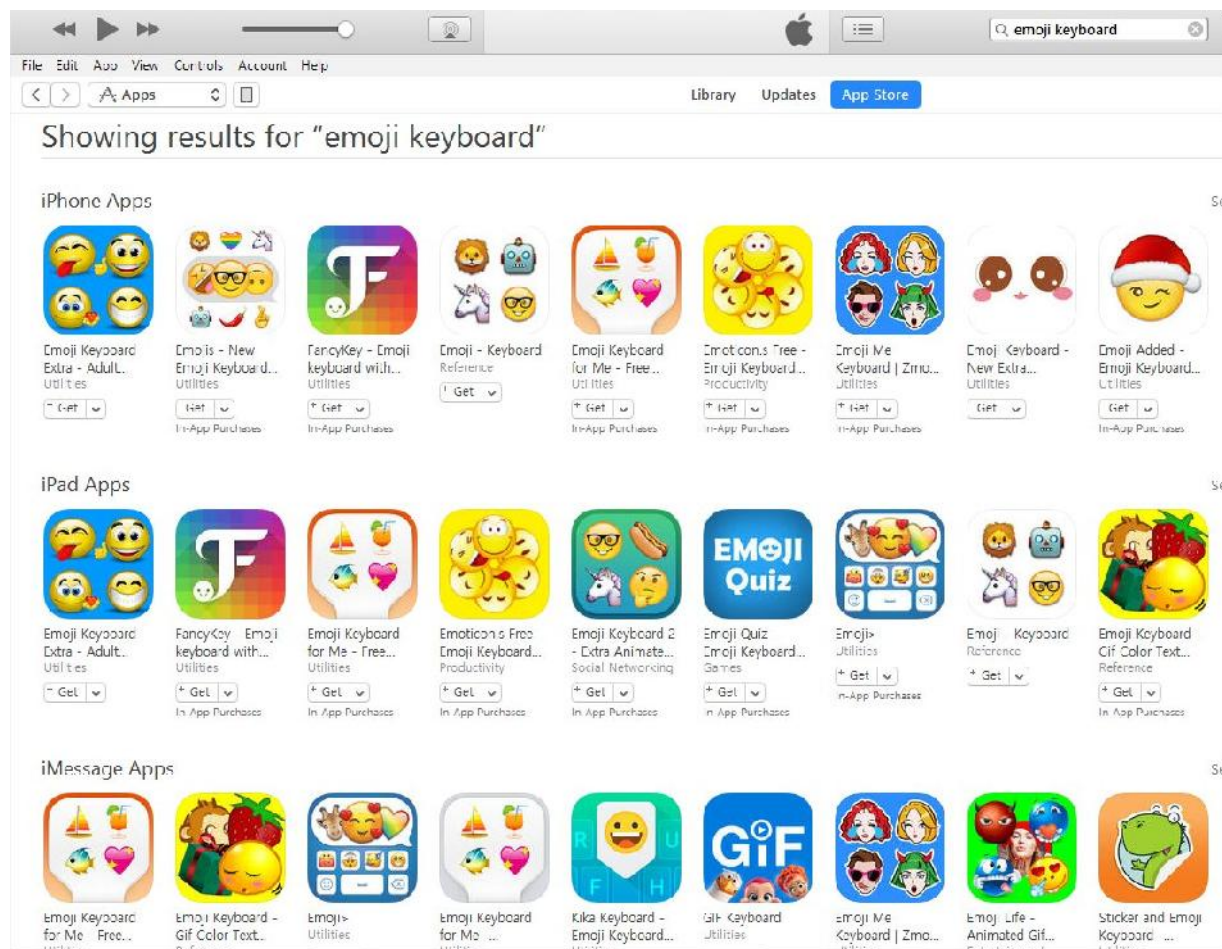
### **Keylogging Grows Up – Emoji Keyboards Geolocate, Eavesdrop on Microphone and Tap Keystrokes**

Keylogging technology has been a known threat vector for many years, however, for Apple iOS and Google Android, it's a new attack methodology on Smartphones and Tablets.

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. In particular, SnoopWall has discovered advanced keylogging technology known as “Remote access software keyloggers.” These are local software keyloggers with an added feature that allows access to the locally recorded data from a remote location. Remote communication may be achieved using one of these methods:

1. Data is uploaded to a website, database or an FTP server.
2. Data is periodically emailed to a pre-defined email address.
3. Data is wirelessly transmitted by means of an attached hardware system.

The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine to be accessed. Most of these aren't stopped by HTTPS encryption because that only protects data in transit between computers; this is a threat in your own computer - the one connected to the keyboard. (Source: Wikipedia.org).



**Figure 2: Emoji Keyboards Flooding the iTunes store.**

### Keyboard Replacement Apps as Keyloggers and Covert Channels

The first question you should ask yourself is “why does a keyboard replacement need internet access?”. The second question you should ask yourself is “why would a keyboard replacement need access to my phone ID, my contacts, my SMS and my phone log?”. There are many more questions you should ask based on the permissions these apps request.


While there are many Keyboard replacement applications available for Apple iPhones and iPads, Windows Smartphone and Google Android devices, we have randomly chosen to look at many of the top 20 (of the hundreds of Emoji Keyboards available) and look for patterns of malicious behavior, which we found.

Some of the top Emoji Keyboards use encryption to send/hide information, connect to servers in China, serve up advertisements that lead to additional malware installation sites. For example,

one of the modules used for alleged advertisement purposes leads to “goodphone.mobi”: <http://www.who.is/whois/goodphone.mobi>, which is hosted by Hichina Zhicheng Technology Ltd (420) <http://www.internic.net/registrars/registrar-420.html> Which someone also claims to be an online marketplace: <http://www.85222.tradebig.com/> however affiliated sites appear to be a scam: <https://www.scamwarners.com/forum/viewtopic.php?f=10&t=28148> in part of some sort of large internet fraud ring. In addition, HICHINA also hosts some very bad malware sites:

- ) <https://zeustracker.abuse.ch/faq.php>
- ) <https://zeustracker.abuse.ch/monitor.php?host=hruner.com>
- ) <https://zeustracker.abuse.ch/monitor.php?host=www.witkey.com>

One of the key servers, various Emoji Keyboards connect to is located, here: 61.145.124.174

IP Lookup Result From IP Locator on IP Map	IP Locator & IP Lookup Basic Tracking Info
	<p>IP Address: 61.145.124.174  <a href="#">[IP Blacklist Check]</a></p> <p>Reverse DNS: ** server can't find 174.124.145.61.in-addr.arpa: SERVFAIL</p> <p>Hostname: 61.145.124.174</p> <p><b>Lookup IP Address Location For IP: 61.145.124.174</b></p> <p>Continent: Asia (AS)</p> <p>Country: China 🇨🇳 (CN)</p> <p>Capital: Beijing</p> <p>State: Guangdong</p> <p>City Location: <b>Guangzhou</b></p> <p>ISP: China Telecom</p> <p>Organization: China Telecom Guangdong</p> <p>AS Number: AS58466 CHINANET Guangdong province network</p> <p>Time Zone: Asia/Chongqing</p> <p>Local Time: 05:24:52</p> <p>Timezone GMT offset: 28800</p> <p>Sunrise / Sunset: 06:41 / 17:42</p>
	<p><b>Extra IP Lookup Finder Info for IP Address: 61.145.124.174</b></p> <p>Continent Lat/Lon: 29.8405 / 89.296</p> <p>Country Lat/Lon: 35 / 105</p> <p>City Lat/Lon: (23.1167) / (113.25)</p> <p>IP Language: Standard Chinese (Mandarin/Putonghua), Yue (Cantonese), Wu (Shanghaiese), Minbei (Fuzhou), Minnan (Hokkien-Taiwanese), Xiang, Gan, Hakka dialects, minority languages</p> <p>IP Address Speed: Broadband (Cable/DSL) Internet Speed  <a href="#">[Check Internet Speed]</a></p> <p>IP Currency: Renminbi (CNY)</p> <p>IDD Code: +86</p>



This is a server belonging to <http://en.chinatelecom.com.cn/> a State owned telecommunications company. China Telecom rerouted about 15% of foreign Internet traffic through Chinese servers for 18 minutes that was only once detected. It may still be happening on occasion, in smaller slices. The traffic included the commercial websites of Dell, IBM, Microsoft, and Yahoo! as well as government and military sites in the United States. China Telecom denied hijacking any Internet traffic: [http://en.wikipedia.org/wiki/China\\_Telecom#Rerouted\\_Internet\\_traffic](http://en.wikipedia.org/wiki/China_Telecom#Rerouted_Internet_traffic). In addition, others post to 120.197.85.102. This server belongs to China Mobile Communications Corporation: [http://en.wikipedia.org/wiki/China\\_Mobile#Overseas\\_activities](http://en.wikipedia.org/wiki/China_Mobile#Overseas_activities) as well as to 69.28.52.35, 209.177.95.172 which belongs to ChinaCache: <http://en.wikipedia.org/wiki/ChinaCache> and sending encrypted data to this address 69.28.52.35, in particular, owned now by “Zenlayer” the Chinese government backed Cloud services provider with offices in the USA.

Another top Emoji keyboard used on both the Apple iTunes and the Google Play store visits 58.83.195.16. This is another Chinese webhosting company, Beijing Shijihengying Technology Co. Ltd, operating out of Beijing and looks similar to HICHINA.

Have you checked the permissions?

Have you visited their websites?

Have you read their privacy policies?

Have you looked at the names of all of the top developers and the Chinese government owned or backed telecommunications companies where these Emoji Keyboard developers work?

At SnoopWall, we have and we find it very suspicious, to say the least.

## Conclusion

These apps, like others, appear to 'monetize' through advertisement networks. However, let's take a deeper look at the hardware i/o (input/output) ports they access as well as consumer/end-user identity information off the device. They are able to find accounts on the device, add or remove accounts, read your contacts, read your text messages (SMS), read your call log, test access to protected storage, modify or delete the contents of your USB storage, record audio, view Wi-Fi connections, learn about the device network information and internet connection status, obtain device ID and call information by reading the phone status and device identifiers and run automatically in the background at startup (which is required for a keyboard app – the perfect vehicle for Trojan-based creepware or malware). The top emoji keyboards are very invasive to say the least and installed on too many devices, leveraging keyboard, microphone and internet access, preventing devices from sleeping while sending and receiving encrypted information over the Internet.

Using Occam's razor (also written as Ockham's razor, and *lex parsimoniae* in Latin, which means law of parsimony), which is a problem-solving principle attributed to William of Ockham (c. 1287–1347), I have come to the simplest conclusion. The principle can be interpreted as stating Among competing hypotheses, the one with the fewest assumptions should be selected. Simply put, without any additional assumptions, it's obvious Emoji Keyboards are either a) an effort of the Chinese government to perform espionage on at least ½ of the smartphones in the world or b) their lack of oversight on their own employees, who choose to write these applications while employed in Chinese telecommunications agencies and companies, owned or backed by their government. I would gather that if it is a), then the agency in charge of this effort is 3PLA, aka, the Chinese version of the US NSA.gov – National Security Agency and if it is b) then you should expect to see your PII stolen and used to commit cyber-crime. Time will tell.

## Recommendation

SnoopWall recommends using the built-in keyboard on your tablets and smartphones. You should delete these Keyboard Replacement Apps and not install any unless they are verified to not eavesdrop on you. In addition, the other types of spyware apps listed in this report should be removed. If it uses too many permissions on your device (keyboard, microphone, gps, wifi, etc.) it's probably a risky app.

## Detailed Evidence

*Detailed Reports Available for Review Confidentially Subject to SnoopWall Approval and official Counter-cyber-espionage & Cybercrime Units of the US Government and Trusted Nation State Partners of the United States*

You are reading the **consumer facing report**. For a more detailed report including decompiled source code, network packet traces and other evidence, you must be with a US Government agency such as the FBI.gov or the US Department of Justice Cybercrime.gov division.

## About The Author



Gary is the CEO of SnoopWall, Inc. and a co-inventor of the company's innovative breach prevention technologies. He is a cyber-security expert and a frequent invited guest on national and international media commenting on mobile privacy, cyber security, cyber-crime and cyber terrorism, also covered in both Forbes and Fortune Magazines. He has been extremely active in the INFOSEC arena, most recently as the Editor of Cyber Defense Magazine. Miliefsky is a Founding Member of the US Department of Homeland Security (<http://www.DHS.gov>), the National Information Security Group (<http://www.NAISG.org>) and the OVAL advisory board of MITRE responsible for the CVE Program (<http://CVE.mitre.org>). He also assisted the National Infrastructure Advisory Council (NIAC), which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace as well as the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Previously, Gary has been founder and/or inventor for technologies and corporations sold and licensed to Hexis Cyber, Intel/McAfee, IBM, Computer Associates and BlackBox Corporation. Gary is a member of ISC2.org and is a CISSP®. Email him at [ceo@snoopwall.com](mailto:ceo@snoopwall.com).

Learn more about SnoopWall's cybersecurity expert CEO at:

<http://www.snoopwall.com/media/>

For CEO interviews and Press Inquiries Contact:

Brittany Thomas, News & Experts, Tel: 727-443-7115 Ext: 221

Email: [brittany@newsandexperts.com](mailto:brittany@newsandexperts.com)