Cheetah Mobile

Mobile Security Report

2015

2016/1/20

CM Security
Resarch Lab

cheetahmobile

Overview of Global Mobile Security in 2015

- **Android virus rose sharply**

In 2015, the number of Android viruses exceeded 9.5 million, which is larger than twice the total number of the past three years. And compared with 2014's 2.8 million, the growth rate of 2015 was over 22%.

- **Root Trojans soared in 2015**

2015 is the year of the Root Trojan. As it gains system-level privilege, Root Trojans can take complete control of the device and are very hard to remove.

- **Mobile payment has been targeted by viruses**

With the popularization of mobile payment, the number of malwares targeting mobile banking increased rapidly.

- **Data leakage caused great damage**

Thousands of companies and hundreds of millions of users have been affected by information leakage in 2015.

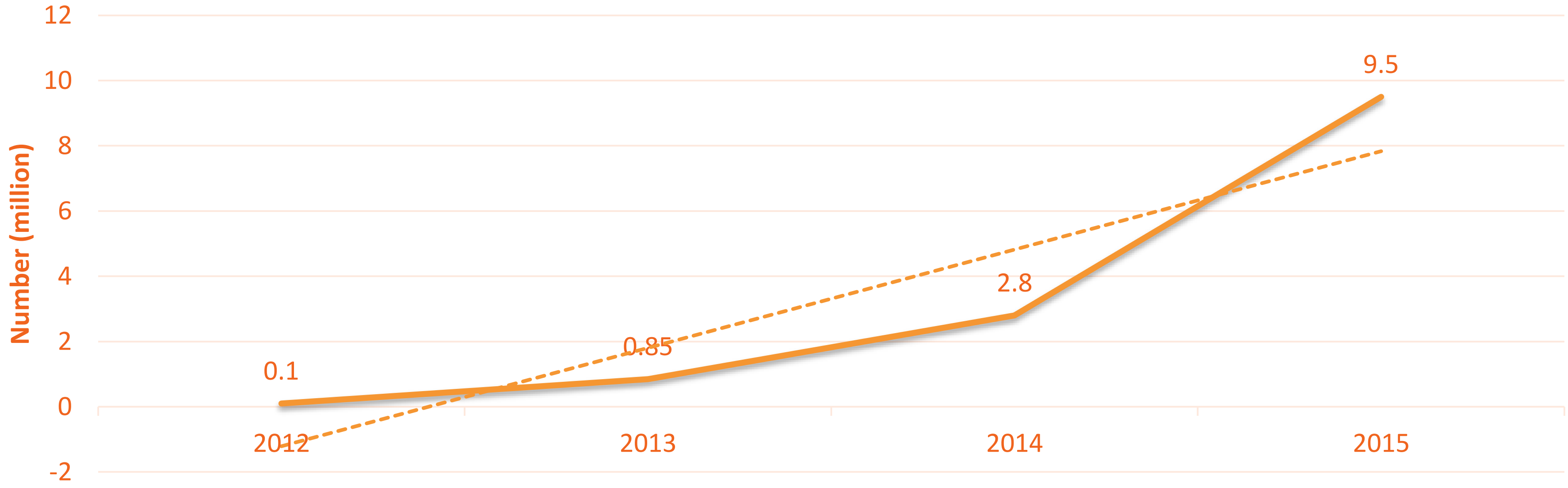
- **Android vulnerabilities emerge one after another**

From the Stagefright vulnerability which affected 95% Android devices to the wormhole compromising millions of Android users, it seemed Android vulnerabilities would never end.

Overview of Android Viruses

In 2015, the number of Android viruses exceeded 9.5 million, which is over three times as many as that of 2014. In the last four years, Android viruses have been increasing at an astonishing rate.

2012-2015 Android Malware Growth Line

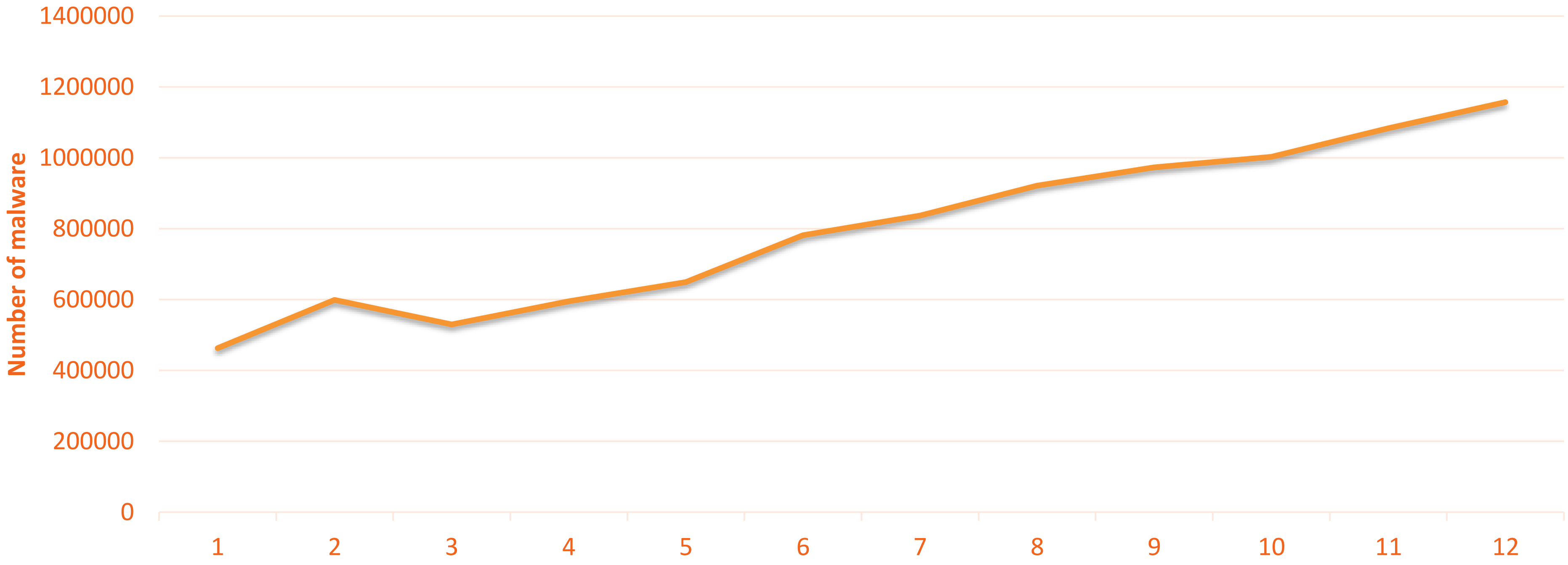


CM Security Resarch Lab

cheetahmobile

The number of viruses of 12 months 2015

- In 2015, the number of Android viruses increased month on month



CM Security Resarch Lab

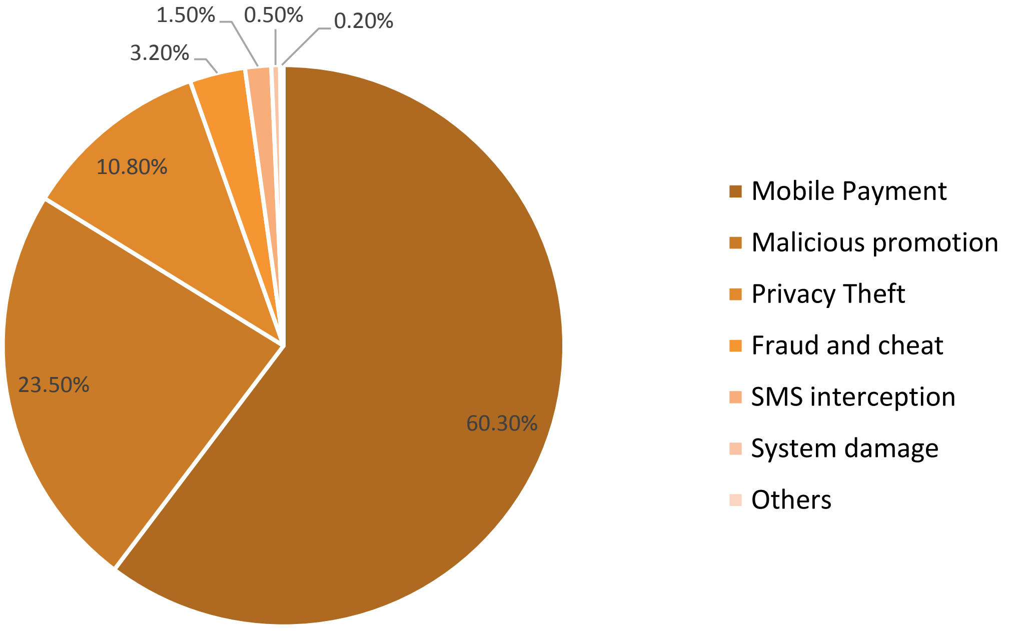
cheetahmobile

Mobile payment viruses account for 60%

Among the 9.5 million viruses, over 60% are related to mobile payment. Mobile payment malwares disguised as normal payment pages lure users to enter their personal information, including bank account information, ID information and phone number to steal personal property.

The surge of mobile payment viruses is closely related to the popularization of mobile payment and phone banking.

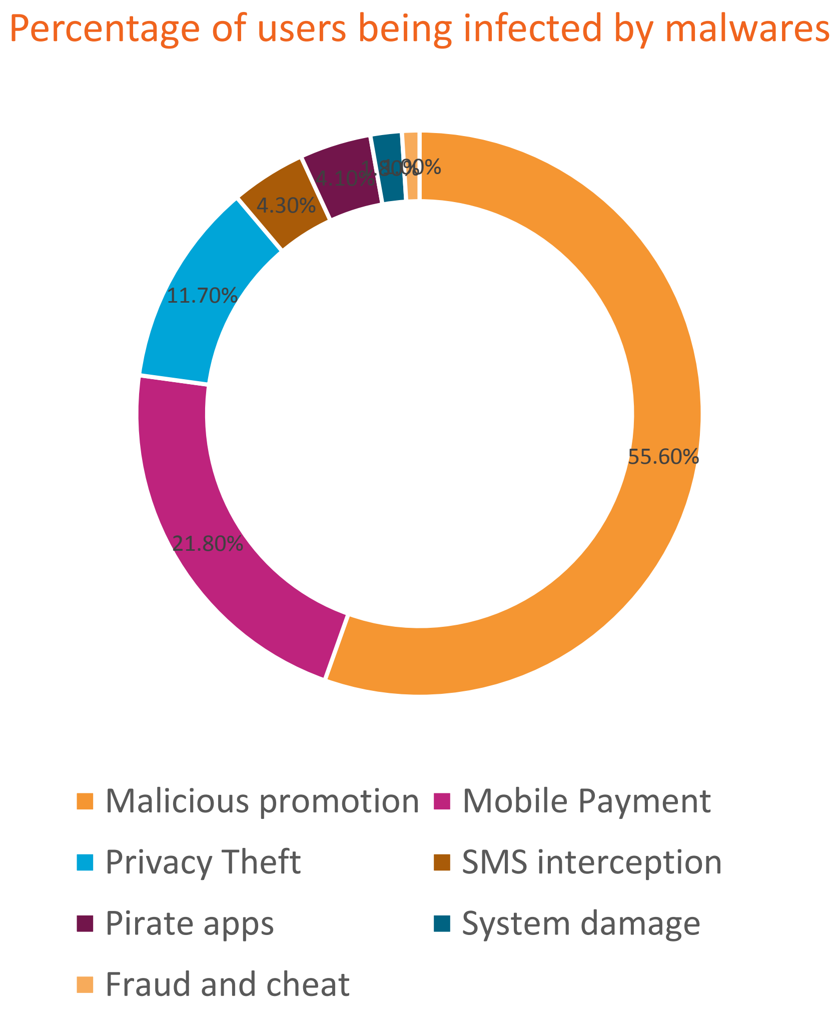
Categories and percentage of malware samples



CM Security Resarch Lab

cheetahmobile

Over 50% Android users have been affected by malicious promotion malwares



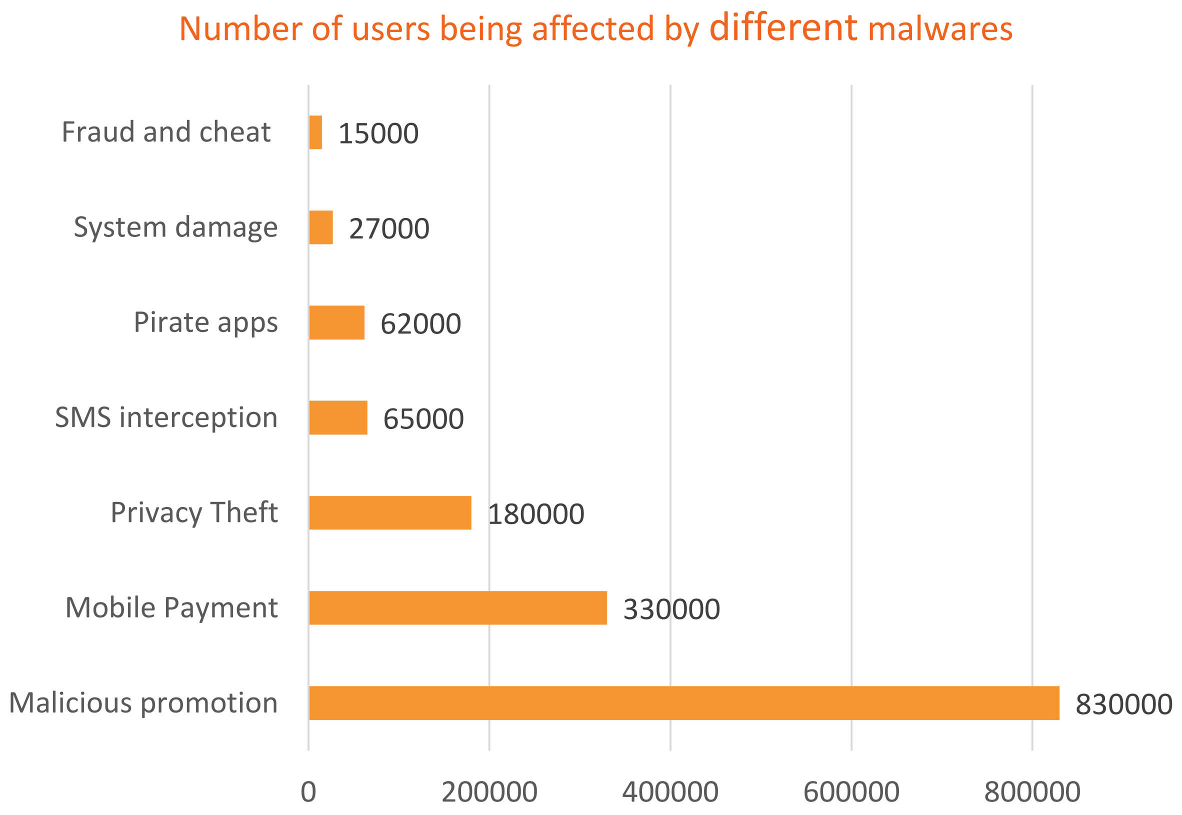
Among all the malicious behaviors of malware, the most common one is promotion. These malwares keep popping up advertisements and force installation of unwanted apps which are very hard to uninstall. Over 55% of Android users have been affected by malicious promotion malwares.

Privacy theft Trojan is also a common one. Generally, it hides in users’ mobile devices to steal text messages, contact information, location, and even personal photos. These malwares can cause severe losses to users due to data leakage.

CM Security Resarch Lab

cheetahmobile

The number of users being affected by different malwares

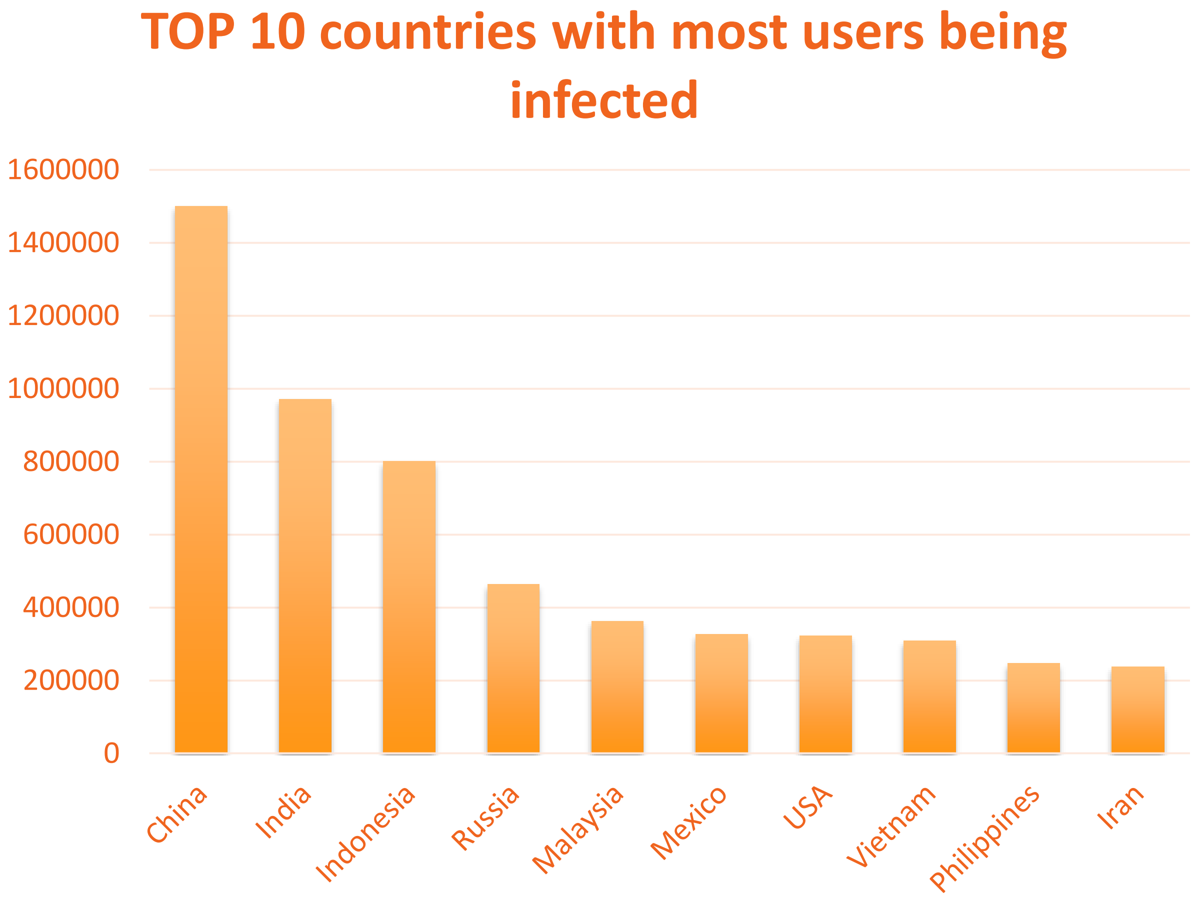


In 2015, over 800,000 Android users were affected by malicious promotion malwares, while mobile payment viruses caused information losses to more than 300,000 users.

TOP10 countries with most users being affected by malwares

In 2015, China, India and Indonesia were the three most severely afflicted countries.

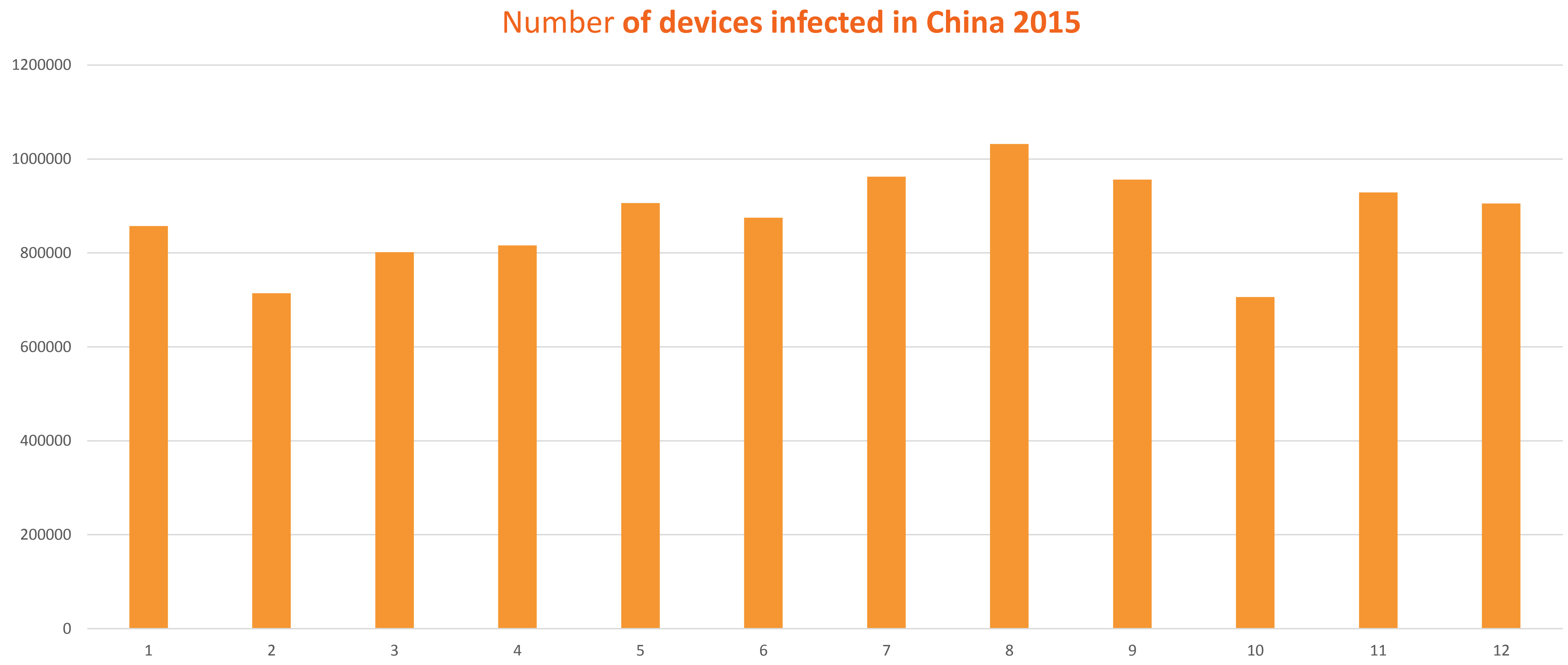
Apart from large Android user bases, another reason of these countries becoming the worst-hit ones is that third-party app markets are prevailing in these areas, and most of these third-party app markets have been contaminated by malwares due to the weak monitoring of third-party app markets.



CM Security Resarch Lab

cheetahmobile

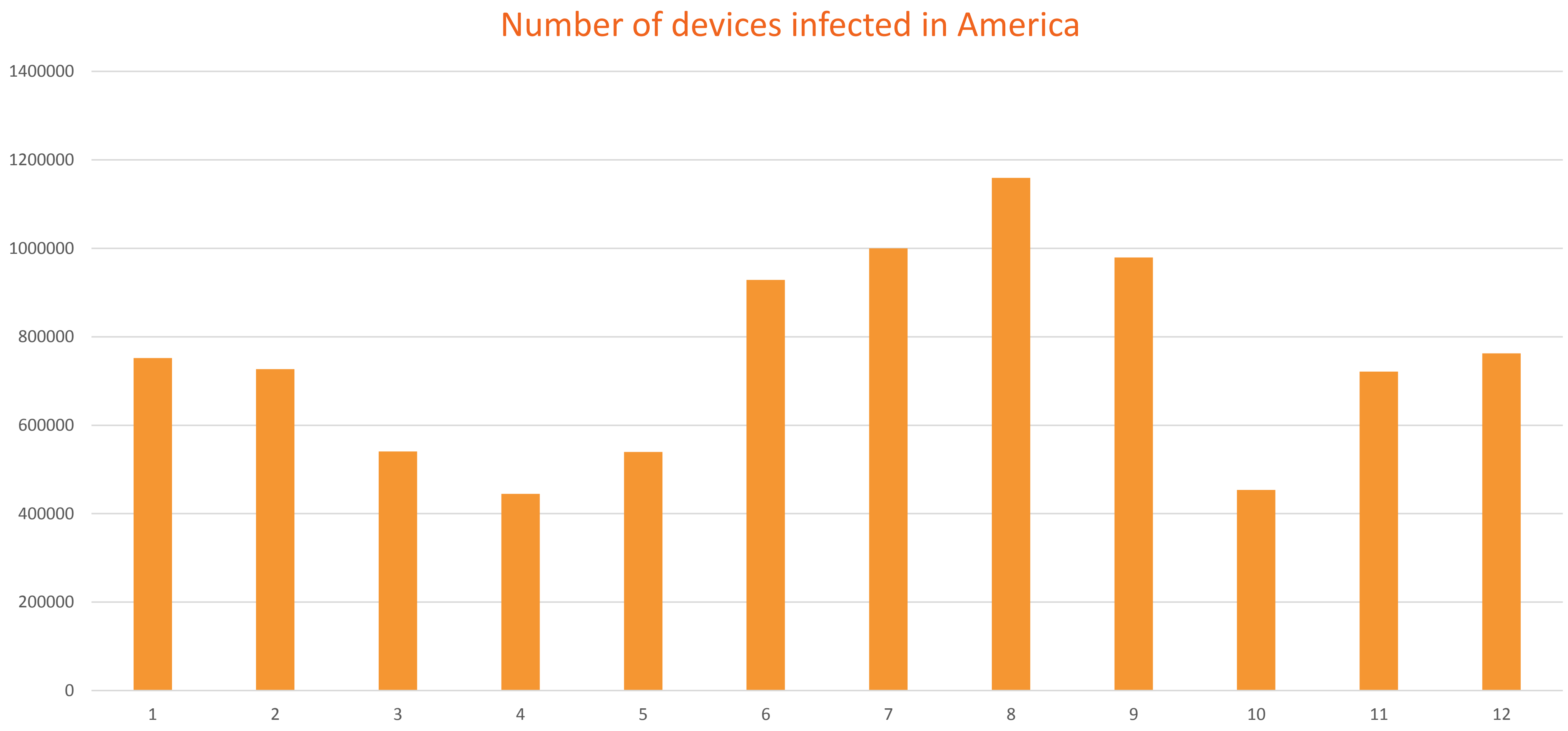
Number of devices infected in China 2015



CM Security Resarch Lab

cheetahmobile

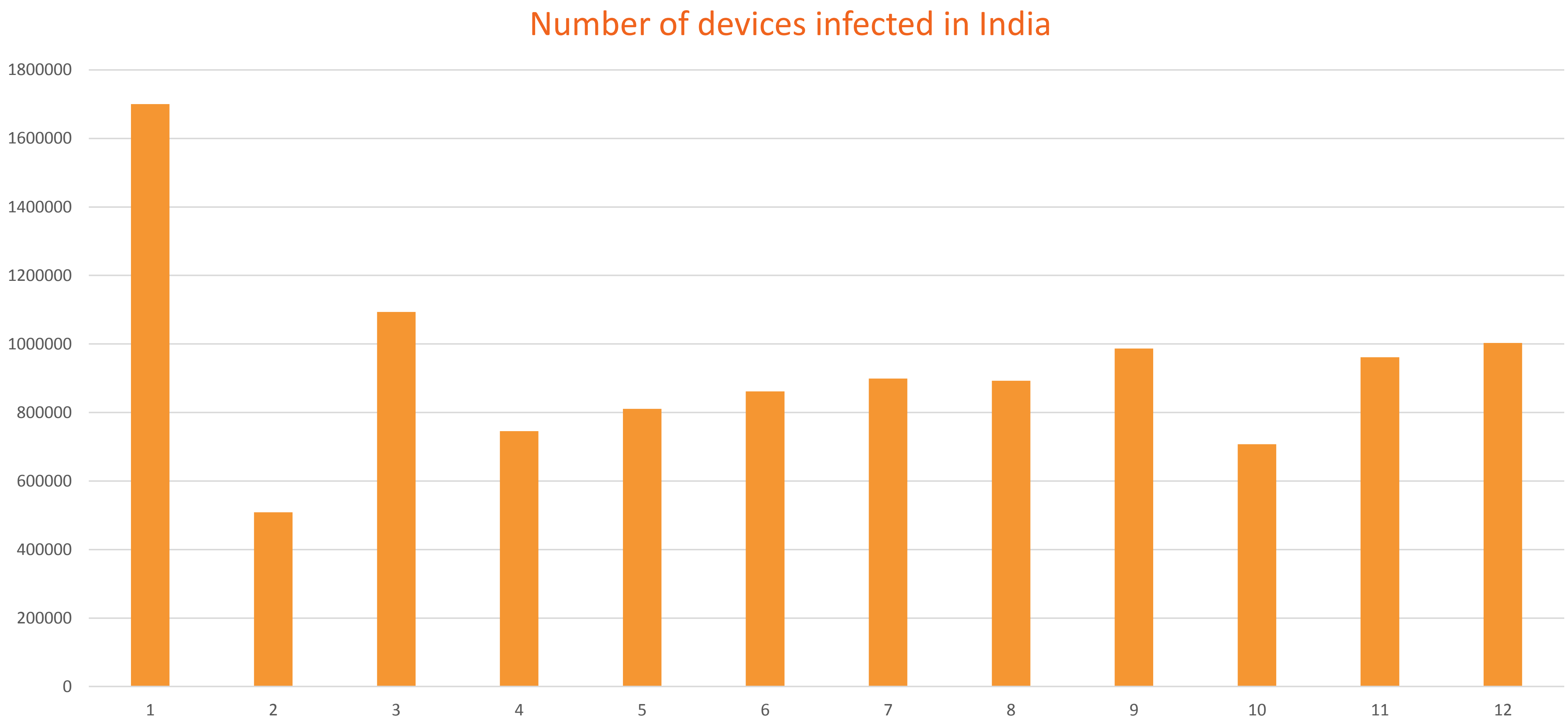
Number of devices infected in America 2015



CM Security
Resarch Lab

cheetahmobile

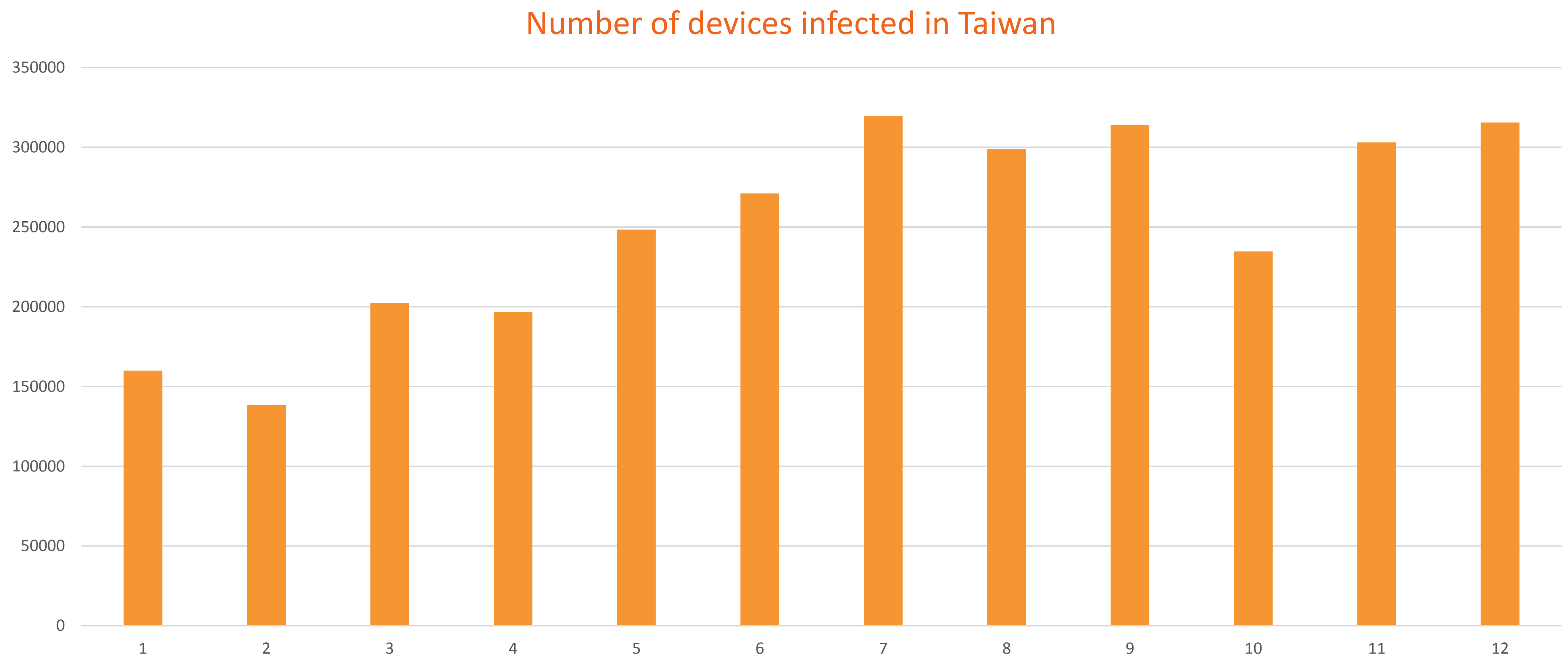
Number of devices infected in India 2015



CM Security
Resarch Lab

cheetahmobile

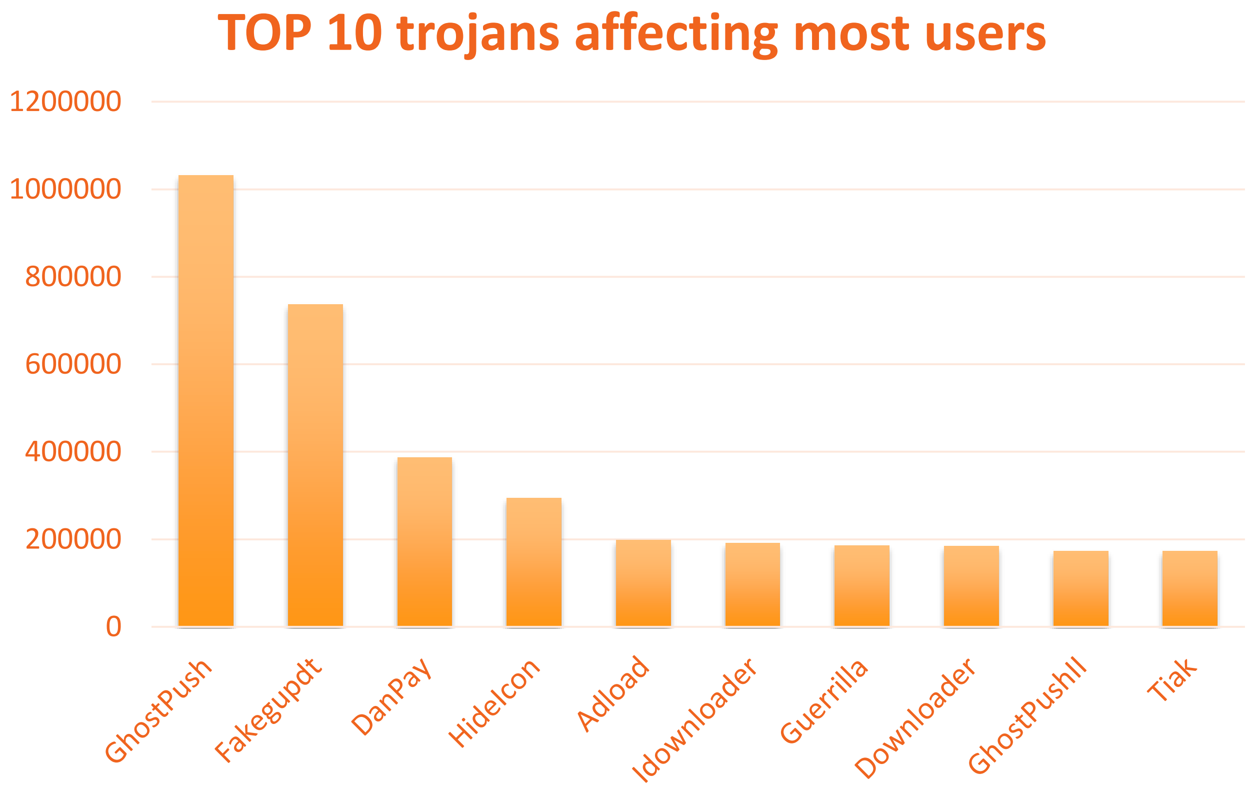
Number of devices infected in Taiwan 2015



CM Security Resarch Lab

cheetahmobile

TOP 10 Trojans affecting most users



In 2015, the Trojan which rose most significantly was the Root Trojan. This kind of Trojan is able to gain the system-level privilege of users' Android devices, and hide itself in the most covert part, which makes it very hard to remove. The most typical example is the stubborn Ghost Push and its variants.

CM Security Resarch Lab

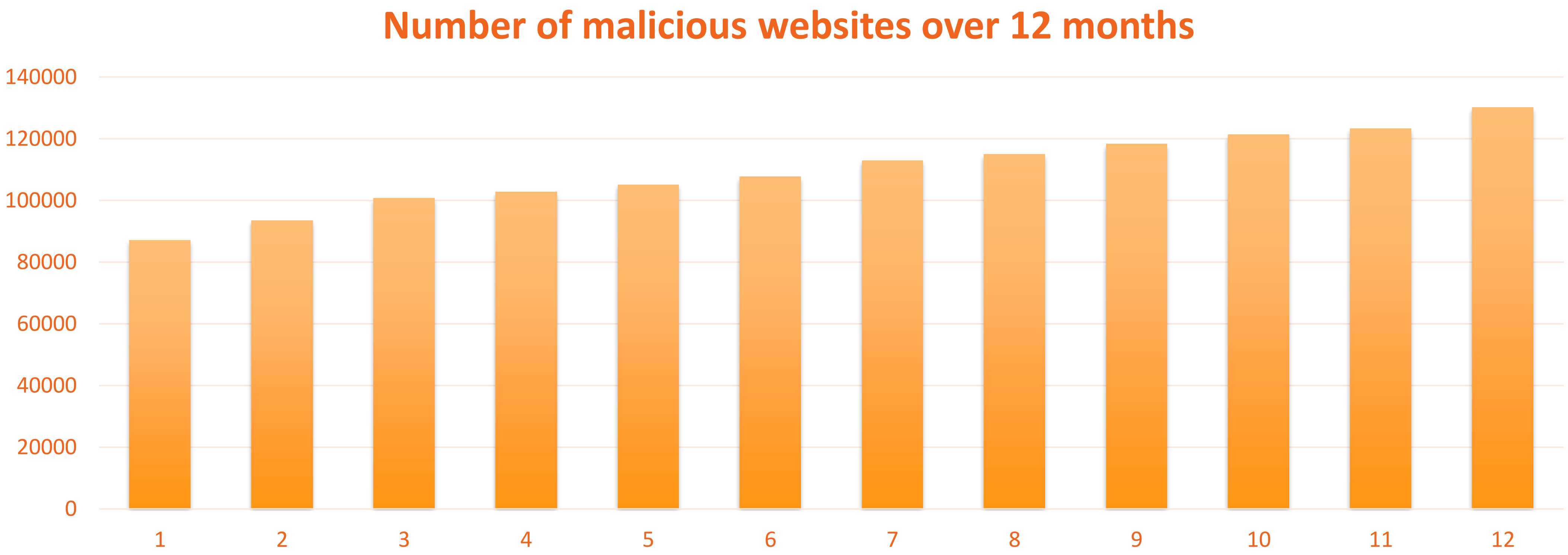
cheetahmobile

Phishing Sites in 2015

In 2015, Cheetah Mobile detected over 1,300,000 malicious websites. The number of malicious sites increased month on month, reaching its peak in December.

As the last months of the year are the festival and shopping season, people are willing to spending money, which online fraudsters seized as a chances to commit cyber crime.

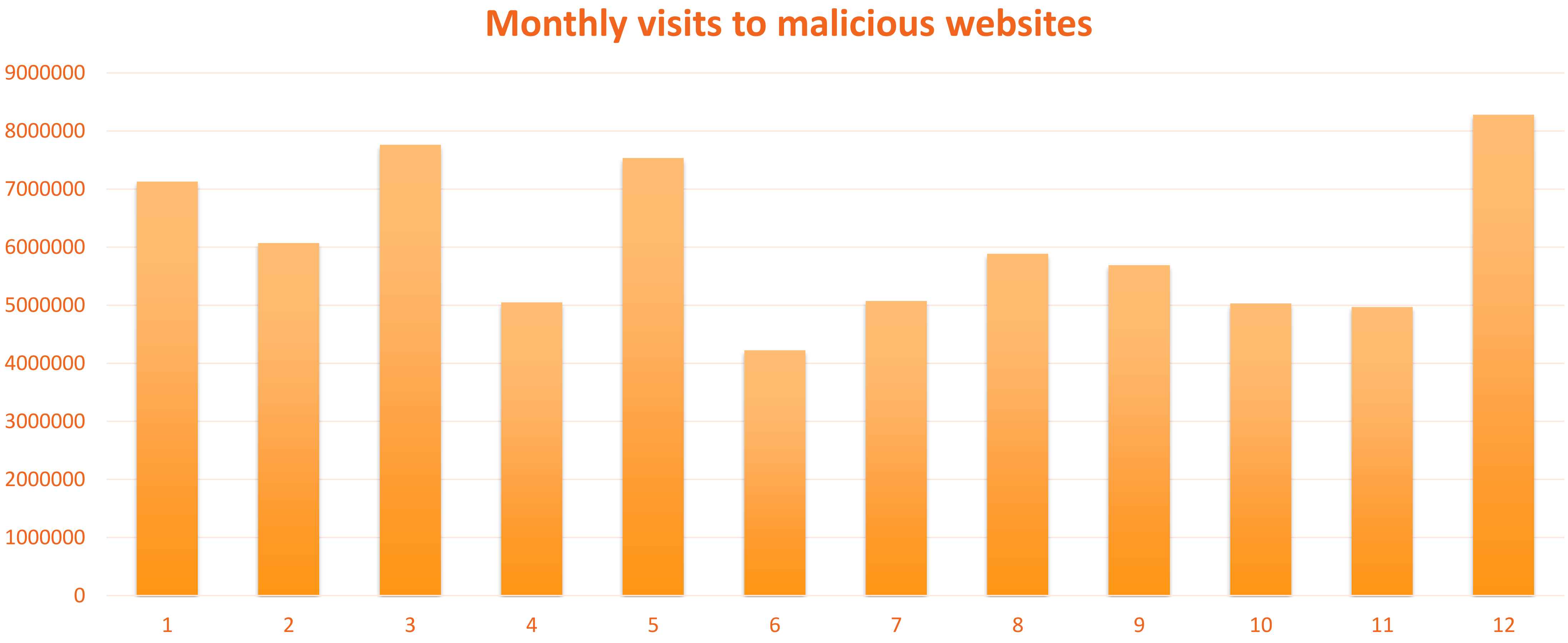
Number of malicious websites over 12 months



CM Security Resarch Lab

cheetahmobile

Monthly visits to malicious websites

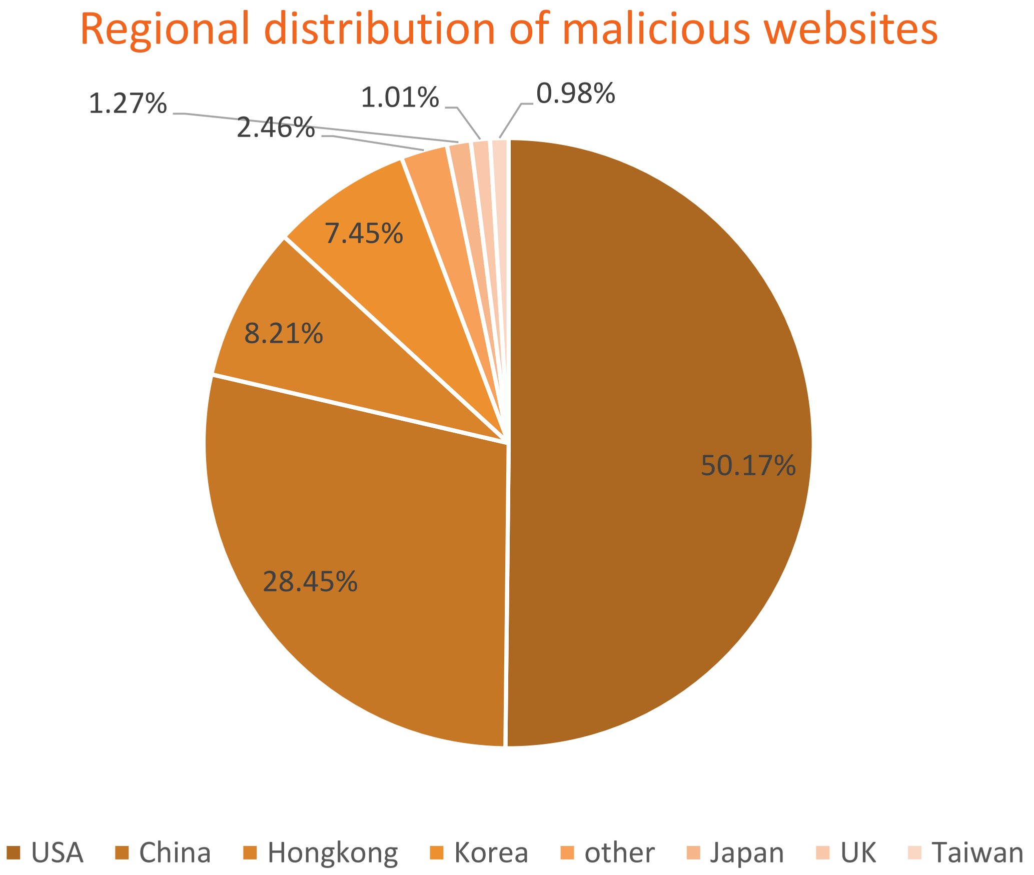


CM Security Resarch Lab

cheetahmobile

Regional distribution of malicious websites

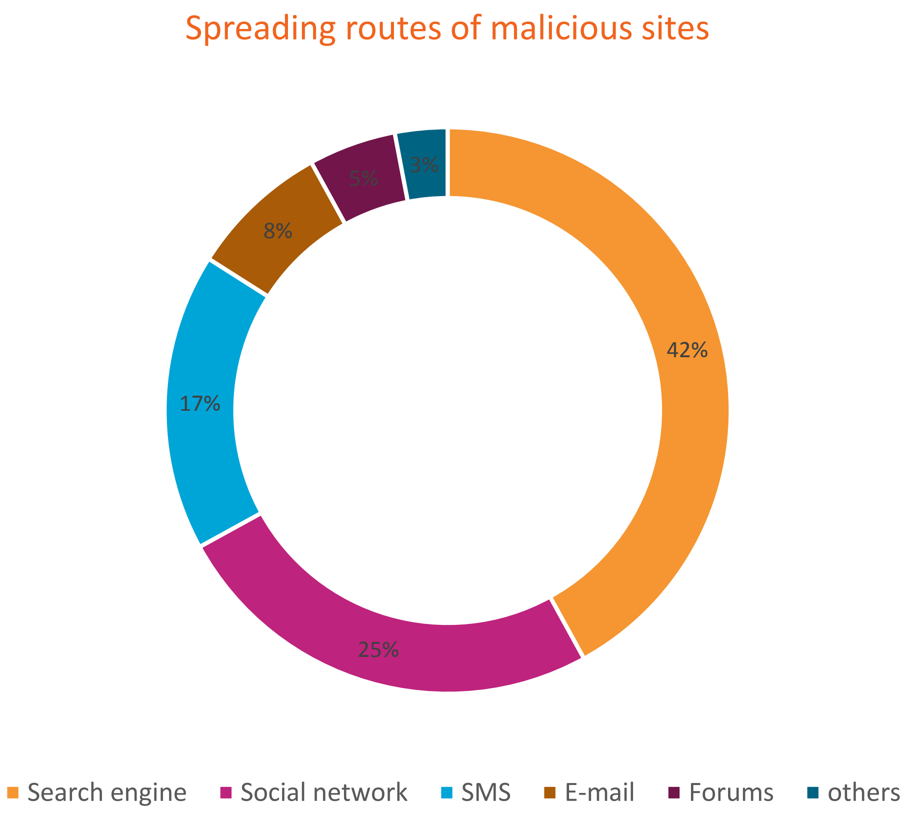
- In 2015, malicious websites were mainly distributed in the United States, China, and Korea. About 50% malicious websites were based in America, and China accounted for about 28%.



CM Security Resarch Lab

cheetahmobile

Spreading routes of malicious sites



Spreading routes of malicious sites

The main transmission routes of malicious sites are search engine, social networks and SMS. Social networks have become fraudsters favorite tool to spreading phishing sites as they have the most active users. Cyber criminals usually embed phishing sites into breaking news to lure users to click. SMS and email with phishing sites are also common tricks of scammers.

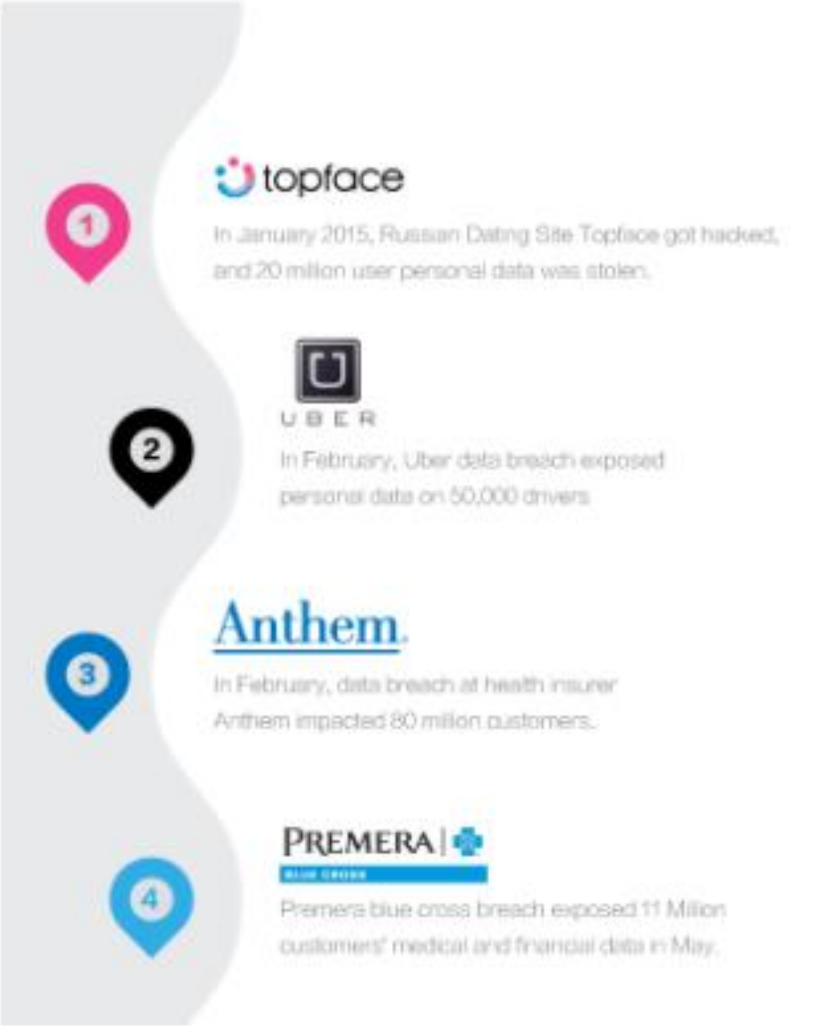
Review of biggest data leakages in 2015

In recent years, data leakage has become one of the most annoying security vulnerabilities to organizations. In 2015, thousands of organizations around the world had their data leaked due to cyber attack, encumbering hundreds of millions of users.

The biggest data leakage events in 2015 were:

- **Anthem (**the second biggest insurance company of America): 80 million customers' and employees' personal information
- **OPM**: About 27 million employees' and applicants' personal information
- **Ashley Madison:** 37 million users' personal information
- **Hacking Team**: 400GB data was leaked and scattered on the internet.

Major data leakage events



1 topface

In January 2015, Russian Dating Site Topface got hacked, and 20 million user personal data was stolen.

2 UBER

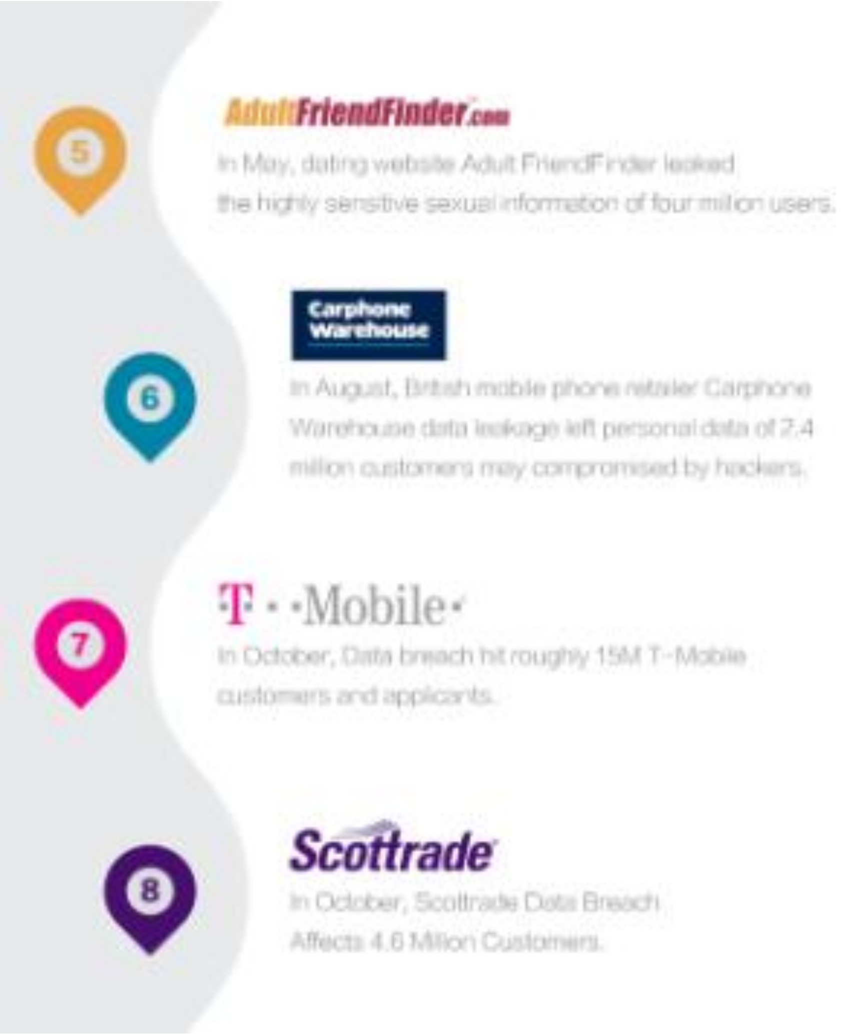
In February, Uber data breach exposed personal data on 50,000 drivers

3 Anthem.

In February, data breach at health insurer Anthem impacted 80 million customers.

4 PREMERA | BLUE CROSS

Premera blue cross breach exposed 11 Million customers' medical and financial data in May.



5 AdultFriendFinder.com

In May, dating website Adult FriendFinder leaked the highly sensitive sexual information of four million users.

6 Carphone Warehouse

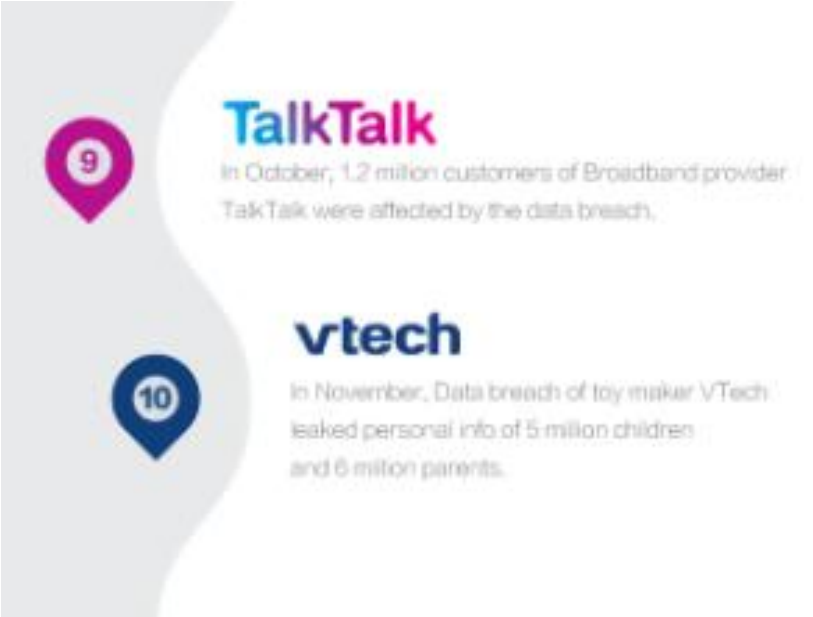
In August, British mobile phone retailer Carphone Warehouse data leakage left personal data of 7.4 million customers may compromised by hackers.

7 T · ·Mobile·

In October, Data breach hit roughly 15M T-Mobile customers and applicants.

8 Scottrade

In October, Scottrade Data Breach Affects 4.6 Million Customers.



9 TalkTalk

In October, 1.2 million customers of Broadband provider TalkTalk were affected by the data breach.

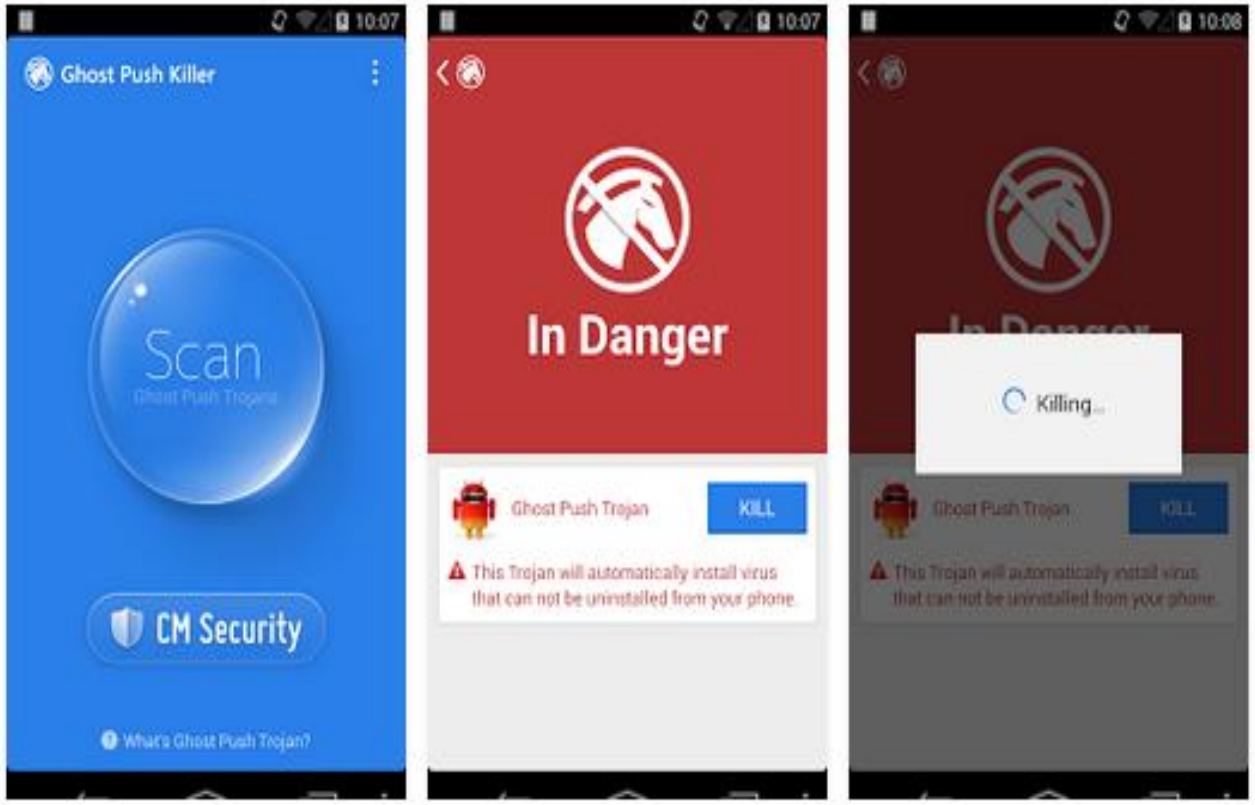
10 vtech

In November, Data breach of toy maker VTech leaked personal info of 5 million children and 6 million parents.

CM Security Resarch Lab

cheetahmobile

The Most Annoying Viruses in 2015



This Trojan will automatically install virus that can not be uninstalled from your phone

Most stubborn---Ghost Push

In October 2015, Cheetah Mobile Security Lab warned Android users against the outbreak of Ghost Push’s several variants which have infected over 900,000 Android users in 116 countries. It is able to obtain full control over smartphones and tablets and this makes it nearly impossible to get rid of. What makes it even worse is it would push app installations without the user’s consent to earn promotion fees from advertisers.

- **Most Evil--- Pre-installed Trojan**

Researchers from the Cheetah Mobile Security Lab found a dangerous Trojan, dubbed Cloudsota, pre-installed on certain Android tablets. Over 150 countries have been affected by this Trojan, with Mexico, USA and Turkey suffering the most.

● Most Attractive--- ‘Party pics’ Trojan

Users would receive a text from a strange number, which says ‘Come and check out our party pics! Your friends are there!’ with a link under it. Once they click into it, instead of seeing their friends, their mobile phone would instead get a nasty Trojan virus.

‘PARTY PICS’
Trojan from China
is Aiming at U.S. Android Users!

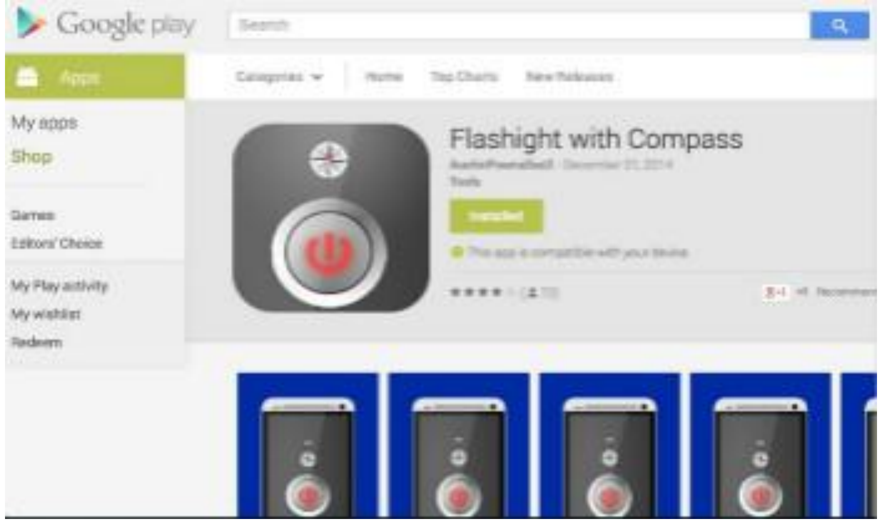
Come and check out our party pics!
Your friends are there!
http://[redacted] [Click]

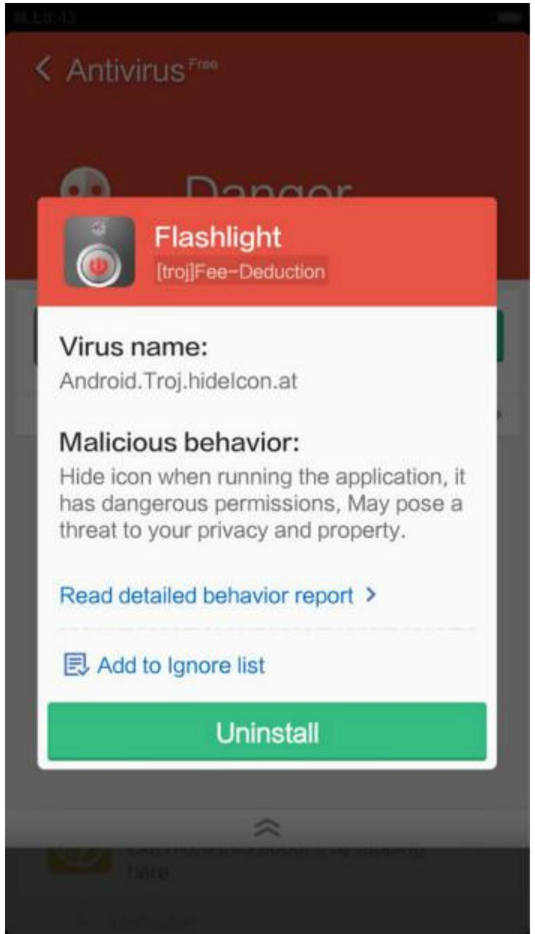
CM Security Resarch Lab

cheetahmobile

● Most-Elusive---Hideicon Malware

The CM Security Research Lab identified five malicious apps available to download on Google Play that contained a type of malware called HideIcon. HideIcon infected more than 56,000 devices in 2015. The malware disguised itself as useful tools like flashlights and compasses, and stole users' personal data and pushed full screen ads frequently to victim's devices.



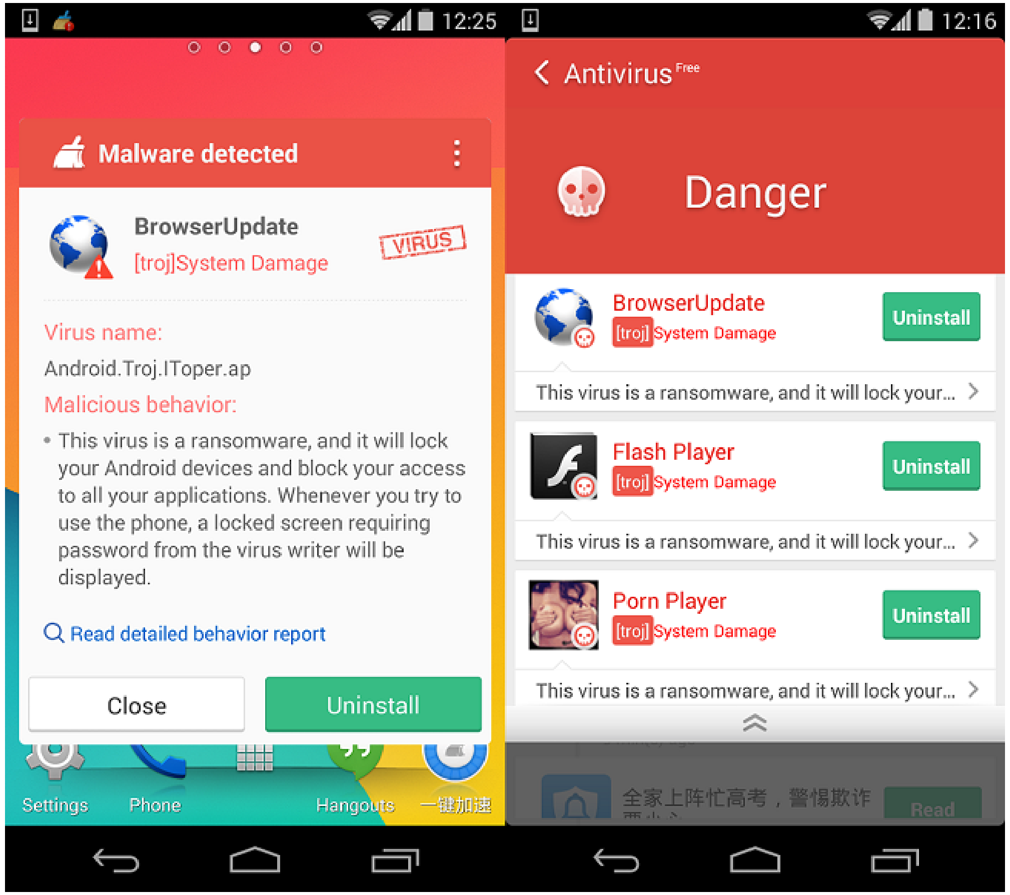


Virus name:
Android.Troj.hideIcon.at

Malicious behavior:
Hide icon when running the application, it has dangerous permissions, May pose a threat to your privacy and property.

CM Security Resarch Lab

cheetahmobile



BrowserUpdate
[troj]System Damage

Virus name:
Android.Troj.IToper.ap

Malicious behavior:

- This virus is a ransomware, and it will lock your Android devices and block your access to all your applications. Whenever you try to use the phone, a locked screen requiring password from the virus writer will be displayed.

Read detailed behavior report

BrowserUpdate
[troj]System Damage
This virus is a ransomware, and it will lock your...

Flash Player
[troj]System Damage
This virus is a ransomware, and it will lock your...

Porn Player
[troj]System Damage
This virus is a ransomware, and it will lock your...

全家上阵忙高考，警惕欺诈

• Most Annoying -iToper

CM Security Research detected a ransomware named iToper, which was transmitted over phone forums and third party app markets. Once the virus got activated, it killed all other activities running on the phone, locked the device, and then displayed fake warnings from the FBI which tried to extort money from users.

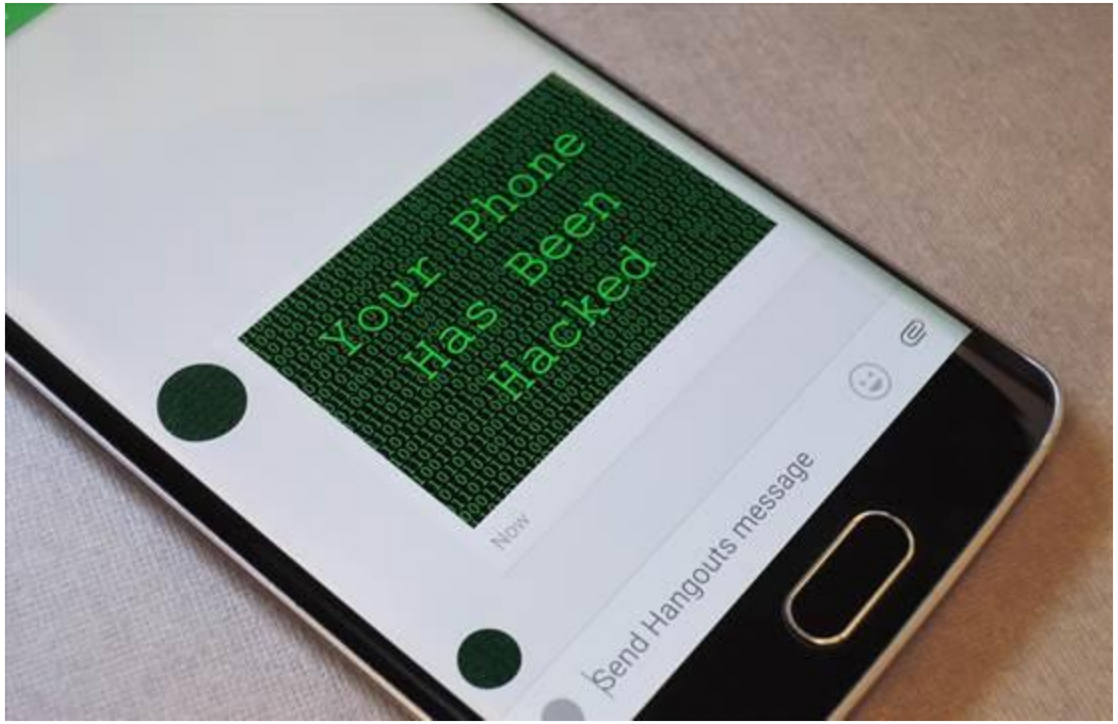
- **Most Costly- ‘Android Installer Hijacking’**

The 'Android Installer Hijacking' vulnerability let third parties compromise users’ Android phones, installing malware and stealing data. As many as 49.5 per cent of all Android devices, including tablets, ran the risk of falling foul to the problem

CM Security Resarch Lab

cheetahmobile

Critical Vulnerabilities in 2015



TOP 1： Stagefright

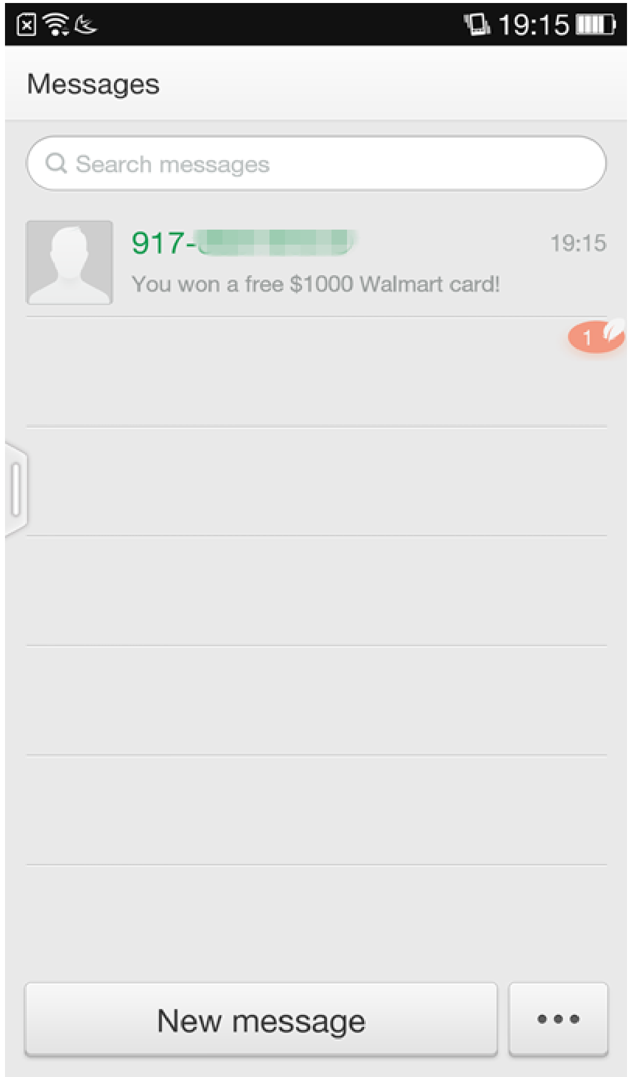
Stagefright makes 95% of Android devices running version 2.2 to 5.1 susceptible to hackers to take total control over users' phones with a simple picture message (MMS). The vulnerability actually resides in a core Android component called "Stagefright," a multimedia playback library used by Android to process, record and play multimedia files.

CM Security
Resarch Lab

cheetahmobile

Top2: Homescreen Applications

In May 2015, CM Security Research Lab discovered that many homescreen applications contain potential safety threats. These apps created fake SMS messages and presented them to the user for viewing which put users to risk of being hacked.



917-[redacted] 19:15
You won a free $1000 Walmart card!

CM Security Resarch Lab

cheetahmobile

TOP 3：Certifi-gate

Certifi-gate is a set of flaws in the authorization methods between mobile Remote Support Tool (mRST), which is widely used by Android device manufacturer and network service provider. This vulnerability can let hackers access any device freely, and initiate actions including screen shoot, keyboard records, and privacy stealing and front door access. Millions of Android devices are under the risk of attack from hackers, including the latest version Lollipop, which is believed to be the most secure version ever.

TOP 4 ： GHOST

A critical vulnerability called GHOST was found, which affects all Linux systems. Attackers can use this flaw to gain system privileges, which means the data we use frequently and store on webpages can easily be stolen. What’s worse, hackers can use this flaw to secretly implant viruses on sites and endanger users at any moment.

TOP 5：Freak Attack

In May, Apple and Google were both working on fixes to a decade-old security flaw that could leave millions of users' mobile web browsers vulnerable to hacking. Users of the browsers were vulnerable to having their electronic communications intercepted when visiting any of hundreds of thousands of websites.

Mobile Security Predictions for 2016

We believe that big changes for mobile security are ahead in 2016. So where is cyberspace heading? What surprises await us?

● **New security features in Android 5.0 Lollipop and its successors are expected to make Android phones more secure.**

Android 5.0+ and 6.0 have two important security features ——Security Enhanced Linux and full device encryption， which make them more secure than other versions. Currently Android 5.0+ have covered over 30% of Android users, and the kernels of flagship models of major Android vendors have been upgraded to Android 5.0+ or Android 6.0. With more and more Android devices being upgraded to Android 5.0+ or 6.0, we can expect a more secure Android ecosystem.

- **As Google Play becomes available in China, Chinese app markets are expected to become more standardized and secure.**

Google Play has a much more secure ecosystem with its strict monitoring system. Google Play is set to enter the Chinese market and will bring a more transparent, standardized and healthy application distribution channel to help create a healthy environment for the Chinese Android ecosystem.

- **More effective steps will be taken by Google to enhance Android security in 2016.**

Google is expected to take measures to improve the security of Android and it will probably crack down on third-party app stores and restrict the permissions available to apps through the Google Play submission process.

- **Globally, mobile payment methods will be attacked more frequently.**

With the more and more wide use of mobile payment, online criminals will probably conduct more attacks towards people’s mobile payments systems.