Privacy and Security Issues in BAT Web Browsers

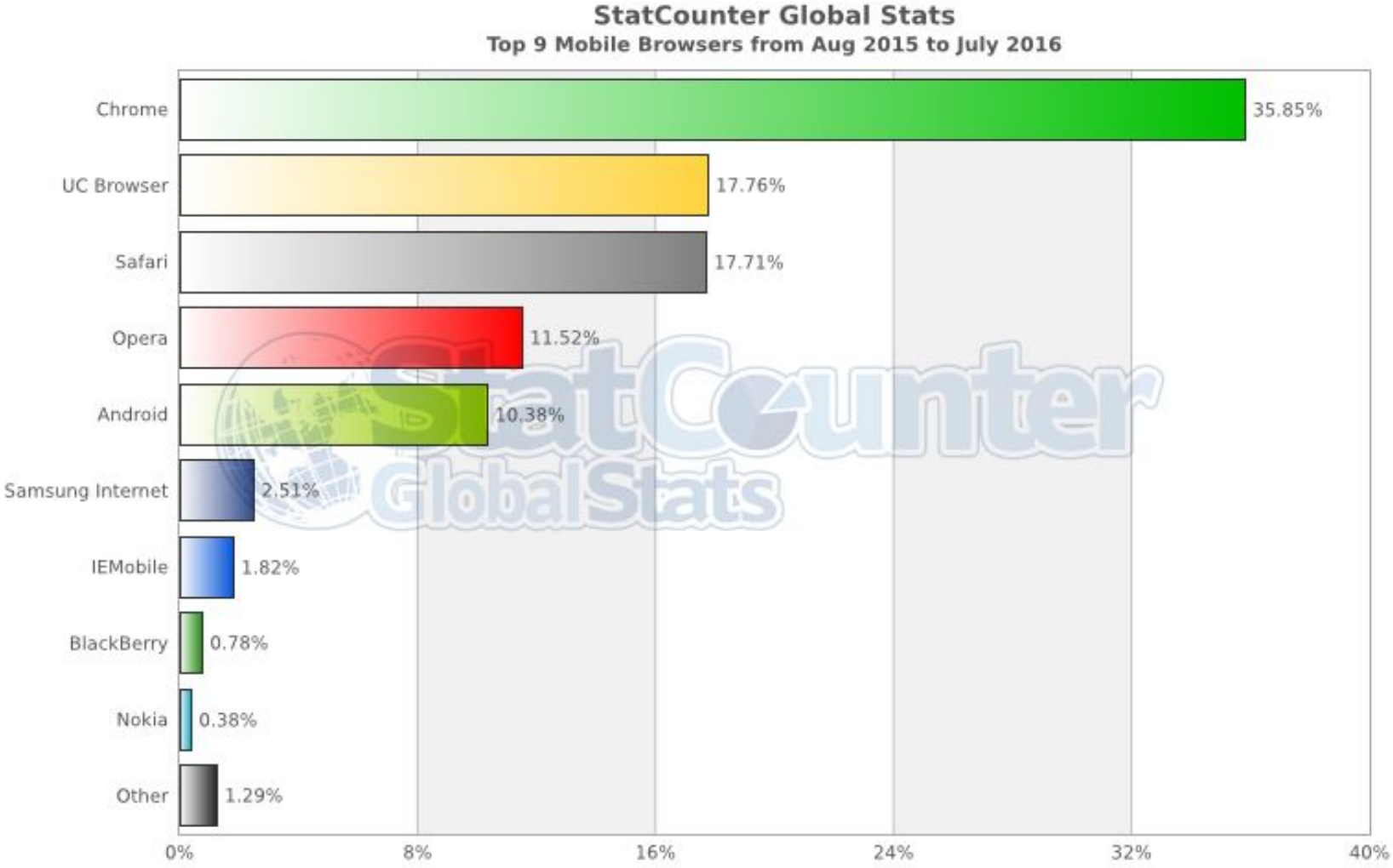
Jeffrey Knockel, Adam Senft, Ron Deibert
Citizen Lab, Munk School of Global Affairs, University of Toronto
Dept. of Computer Science, University of New Mexico

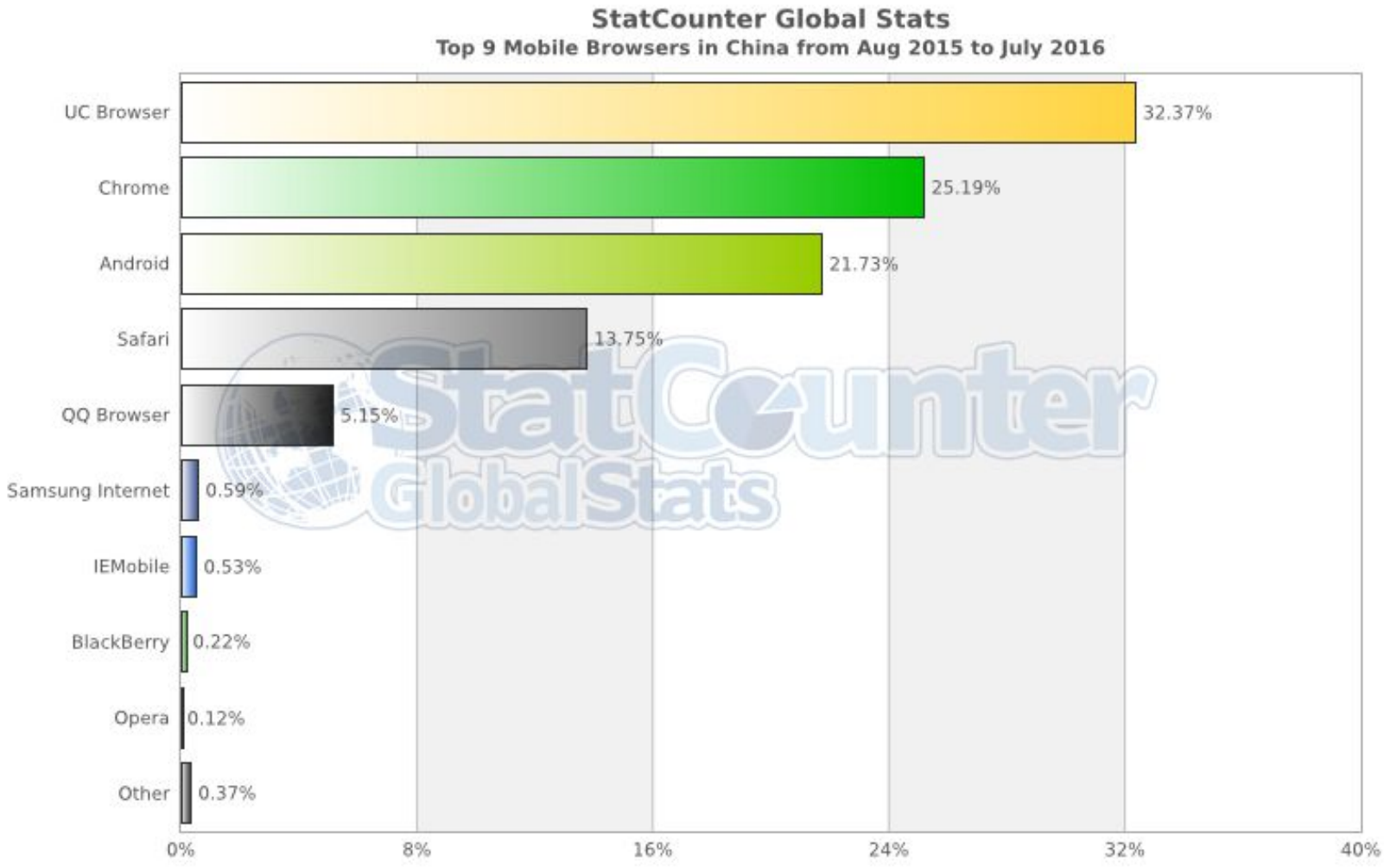
What’s the most popular mobile web browser?

What’s the second most popular mobile web browser?

After Google Chrome, UC Browser is most popular mobile browser in world

The Alibaba Group company over the last couple of years has become No.2 mobile browser in the world and has consolidated its position as the No. 1 mobile browser in three most populous countries of Asia - China, India and Indonesia.


StatCounter Global Stats
Top 9 Mobile Browsers from Aug 2015 to July 2016
Chrome
35.85%
UC Browser
17.76%
Safari
17.71%
Opera
11.52%
Android
10.38%
Samsung Internet
2.51%
IEMobile
1.82%
BlackBerry
0.78%
Nokia
0.38%
Other
1.29%
0%
8%
16%
24%
32%
40%
StatCounter
GlobalStats


StatCounter Global Stats
Top 9 Mobile Browsers in China from Aug 2015 to July 2016
UC Browser
32.37%
Chrome
25.19%
Android
21.73%
Safari
13.75%
QQ Browser
5.15%
Samsung Internet
0.59%
IEMobile
0.53%
BlackBerry
0.22%
Opera
0.12%
Other
0.37%
0%
8%
16%
24%
32%
40%
StatCounter
GlobalStats

BAT (Baidu Alibaba Tencent) Browsers

Baidu Browser
(百度浏览器)

UC Browser
(UC浏览器)

QQ Browser
(QQ浏览器)

Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)

DSD GCHQ GCSB NSA

Success Stories

* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop
  * Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics

Technical analysis

- Reverse engineered Android & Windows versions
- Findings:
  - Found that each uses “easily decryptable” crypto (or sometimes no crypto) to transmit sensitive data
  - Found that most have insecure self-updating processes vulnerable to remote code execution

Kinds of sensitive data typically sent

- Personally identifiable
  - MAC address
  - IMEI
  - IMSI
- Location
  - GPS
  - Active wireless access point
  - In-range wireless access points
- Activity
  - Search keywords
  - URL of every http(s) page visited
  - Title of every https(s) page visited

“Easily decryptable” crypto

- Easily decryptable by reverse engineering the software
- Someone eavesdropping on network traffic can decrypt
- *E.g.*, naive “homebrew” crypto algorithms
- Symmetric crypto algorithms with hard-coded keys
- Asymmetric crypto with huge flaws

Example transmission (encrypted)

```
m90.!.Ã#Ù.GÚ}å.~%..7ÛÅC.\ ..§+xKû.,ý...%/@&..cq*.Í2äh:ÜÈ´Ü>ë..½.OL8."|.°±..¿
Ü.ôýî. Ï¡°_.Wß.p..dÄ·..¬à»®ðÕZìÁn..¶w.äb.!â.©Öà.&.J.Ë.ü7.5 w-.°,°.Ý$......0F
.ß.#¶>.{$..CW[¿=.P.é.ôH.nÞóTnM¸...ý.ËÙ+.îPÝû..u¦p.ãCËhìì!×¥ïæ 1Ï³¿.Þ@h.«Ww.X
.u,¬W..å{.H9ù·.Ä×#.S..@..!x.¢$w...¾;ýdt©Ì.öR.£(jY¦T|¸æsÐ~Ñö}.pOnJ$..M5E.ÃÅc.
ÿãJç©.Ë©.¦JzÄa/¥%jM.´Ê.ØÑ/r¾..çÃÁì|F-.G±:°iíS¢¬òÏk8í$^6.p;.V¬é.YQ¡.ùÕ.ÿ+Í£..
ÿ+V.##.5.Í¯P.(ß¯h..O±ç¨.O>v2-äµ&r×À..dð.Ät;. ,©`×.Ñì..×.÷ªÕ¢å...O._Û¶.Át"ì´ö
ZX.].ÑBùù.Ìªf&cõ.ÓïW.ÒÙK.ßæ.°.W.ò.¿ñí3¯...è]G.Trg.¶»fKKb.ª.Ý.W B..B.oª.c#..ú
..ÃÏ.Þ..¡µê.+².2Å
```

How to decrypt this?

- Reverse engineer the software
- Symmetric crypto :(
- Discover algorithm: homebrew XOR
- Discover the key: "b59e216a8067d108"
- Write a python script

Example transmission by UC Browser (encrypted)

```
m90.!.Ã#Ù.GÚ}å.~%..7ÛÅC.\ ..§+xKû.,ý...%/@&..cq*.Í2äh:ÜÈ´Ü>ë..½.OL8."|.°±..¿
Ü.ôýî. Ï¡°_.Wß.p..dÄ·..¬à»®ðÕZìÁn..¶w.äb.!â.©Öà.&.J.Ë.ü7.5 w-.°,°.Ý$......0F
.ß.#¶>.{$..CW[¿=.P.é.ôH.nÞóTnM¸...ý.ËÙ+.îPÝû..u¦p.ãCËhìì!×¥ïæ 1Ï³¿.Þ@h.«Ww.X
.u,¬W..å{.H9ù·.Ä×#.S..@..!x.¢$w...¾;ýdt©Ì.öR.£(jY¦T|¸æsÐ~Ñö}.pOnJ$..M5E.ÃÅc.
ÿãJç©.Ë©.¦JzÄa/¥%jM.´Ê.ØÑ/r¾..çÃÁì|F-.G±:°iíS¢¬òÏk8í$^6.p;.V¬é.YQ¡.ùÕ.ÿ+Í£..
ÿ+V.##.5.Í¯P.(ß¯h..O±ç¨.O>v2-äµ&r×À..dð.Ät;. ,©`×.Ñì..×.÷ªÕ¢å...O._Û¶.Át"ì´ö
ZX.].ÑBùù.Ìªf&cõ.ÓïW.ÒÙK.ßæ.°.W.ò.¿ñí3¯...è]G.Trg.¶»fKKb.ª.Ý.W B..B.oª.c#..ú
..ÃÏ.Þ..¡µê.+².2Å
```

Decrypted

bluesky.1.5.1.1.10?cache=3102618000&ka=&kb=e2e63e260805aea910e1c2ce02b05211&kc=3b5d366db90b1b60e22260a0278331f8v0000002e9952d46&firstpid=0501&bid=800&ver=5.5.10106.5&defalutbrowser=UCHTML.AssocFile.HTML&flashver=&hi=Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz&0&VB3bb90c33-fc547c89&searchaddress=google&searchbar=google&searchquick=google&openurltab=0&showsearch=1&showextension=1&applyall=0&cloudspeed=0&autopage=0&autologin=0&theme_id=569&wallpaper_id=207&autoclearhistory=0&service=1&sis_fool=5.1.2600_SP3_x86&tch=0&ad_switch=10&lang=zh-CN

Example 2 encrypted

m90...._Õ.÷.y.]¢=»ù¤Ìü<.Oò+DÛxh..Æj.¤]ß?;..u.Öá..7Ò.p`üPÐ·.O"c.ïoÔ¸$ Ä.Úm.¯.
ø.¤Ñ.$"gÉ^¿<kp8äL½.XgEÇ\0ïn...Ü5.F|¢?í.ª3..Ím5°.êó....ü÷Ö% 7a.`(þ/mXa¥nÁS...
Õø.·.Ý.÷tÈØ3'gÿ.j...ß±È.À0Bxä.Ù.8´î½û]üI3Ñe.O³¿G.Ö|.+½.ñpJÊÑ.+V.huÚ.È[~Ø.SG¨
¶ÐLp`Ñ!.Þf^4eåá.ç1s.ÈfdÐ>Öz÷v\6K.ÁÐ¥9.ýÈ~^...¥Í5.þ.st·U.Ó´®.dÄE[ñFÀ.ÎF²L..ýê
th=.zãé¬;ë=\nL..ØÔÕ¼..[+ÊÔÌ.¯Þ!!'alrÖ.0..qJ®\9Uë..¶Y.ýk·2Ñg¬DÚ5Á.ó%<qE.u.`ÿ.
®â.2o.Ú½.÷¤.Ô.]uùz.ø.ç.Å..Üú`ã (WäÓ.Ç.yà#:¶+ÝA9.µ3.:1!öf¬.XE.£.ð÷¬1ð.ÐCT.5/¿
*ØHø~©P.ÉJ .L©Gq..`..OO9:.'ùïHÊG..úLÇ..Ï.¡.×öJ¶¤,ao+/.©.ËZ.Ø..ÚN....|.Ê8.æ.p
.9¯F.ð`.ÖôáÆ©.ëXü.1©>W.§.X2Å.c..r¸{.Í°^.+î.y{.çáÀ..N®Ü,_ùR%.Æ%uµÍÉc£.7ù&.n..
íH×Ë <¯P.ÖZðuÑ¥1.».mu.È. 7æÌ¶,Ý .Tj&×ýó£&.;´ä.á.ý÷÷...B..³.u[...).rïw¸;.èQ)W
.e]Ü.:ÑôúU.õ$óm-ûÔ}¡õÓ..@^b\..îâ%!Élq,ÅQPô..í sÓ..±....9ïNÉ¢mÆÍÍßéÁ.ý±r.÷§ö.
.q$.).§y5Bî.Q.Xôù.Ì^nÊKÒ.ðM·."t» «.ZÀ3mAØ¶Õ

Example 2 decrypted

```
bluesky.1.25.1.1.7?cache=3766412000&ka=&kb=e2e63e260805aea910e1c2ce02b05211&
kc=3b5d366db90b1b60e22260a0278331f8v0000002e9952d46&firstpid=0501&bid=800&ve
r=5.5.10106.5&type=1&ssl=1&bandwidth=29.63&target_ip=64.106.20.27&redirect_s
tart=0&redirect_duration=0&dns_start=0&dns_duration=218&connect_start=218&co
nnect_duration=251&request_start=469&request_duration=916&response_start=138
5&response_duration=1&dom_start=1386&dom_duration=268&dom_interactive=234&do
m_content_load_start=1420&dom_content_load_duration=0&load_event_start=1654&
load_event_duration=26&t0=1385&t1=1719&t2=1719&t3=1420&total_requests=2&requ
ests_via_network=2&cloud_acceleration_enabled=0&average_of_request_duration=
809&average_of_t2_duration=859&private_data=host=www.cs.unm.edu|url=https://
www.cs.unm.edu/~jeffk/&lang=zh-CN
```

Baidu Browser

- RC4 key "HR2ER"
- AES key "h9YLQoINGWyOBYYk"
- XOR mask (0x2D382324), bit rotations
- Base64 encoding with nonstandard alphabet:

```
qogjOuCRNkfil5p4SQ3LAmxGKZTdesvB6z_YPahMI9t80rJyHW1DEwFbc7nUVX2-
```

- Modified TEA crypto + non-standard block cipher mode, key "vb%,J^d@2B1l'Abn" (*)
- …

Baidu Browser

Data leaks across Windows & Android versions

Type	**Data Point**
PII	MAC address, hard drive serial number, IMEI
Activity	Search terms, Full HTTP(S) URLs, HTML page titles
Location	GPS coordinates, in-range WiFi access points

UC Browser

- Homebrew XOR-based algorithm with various keys ("b59e216a8067d108", "e19237a3a933f7eb", "aa171021f9438cb2")
- XOR mask "\xee\xb9\xe9\xb3\x81\x8e\x97\xa7"
- ...

UC Browser

Data leaks across Windows & Android versions

Type	Data Point
PII	IMEI, IMSI, Hard drive serial number, base board serial number, file system volume number
Activity	Full HTTP(S) URLs, Search terms

QQ Browser

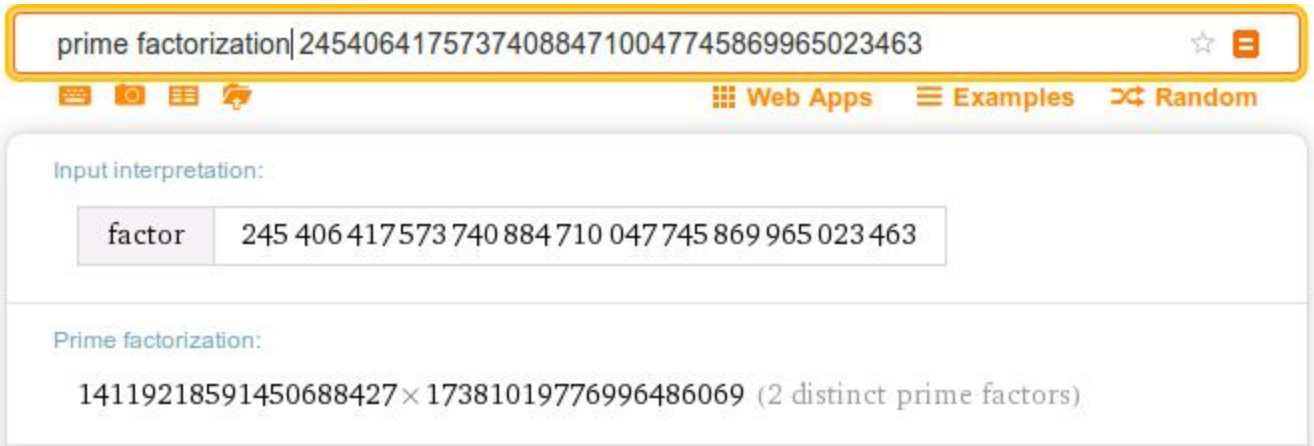
- RSA public key 24540641757374088471004774586996502346 3

QQ Browser

- To factor it, we built our own quantum computer

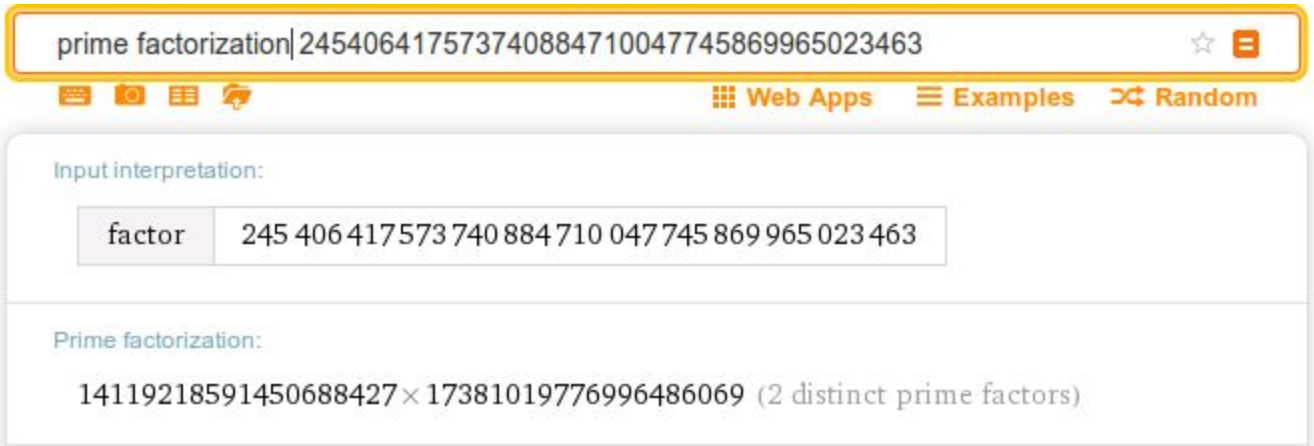
QQ Browser

- RSA public key 2454064175737408847100477458699650234 63



QQ Browser

- RSA public key 24540641757374088471004774586996502346 3



- Also same peculiar TEA crypto as Baidu Browser (*)
- …

QQ Browser

Data leaks across Windows & Android versions

Type	Data Point
PII	Machine hostname, Gateway MAC address, Hard drive serial number, Windows user security identifier, IMEI, IMSI, Android ID, QQ username, WiFi MAC address
Activity	Search terms, Full HTTP(S) URLs
Location	In-range WiFi access points, Active WiFi access point

Vulnerable SDK

- Code leaking personally identifying and locational data in browser actually from a Baidu SDK
- Found SDK in hundreds of Google Play store apps (some very popular)
- ES File Explorer File Manager (com.estrongs.android.pop) has 100,000,000 – 500,000,000 installs
- Other browsers have SDKs?

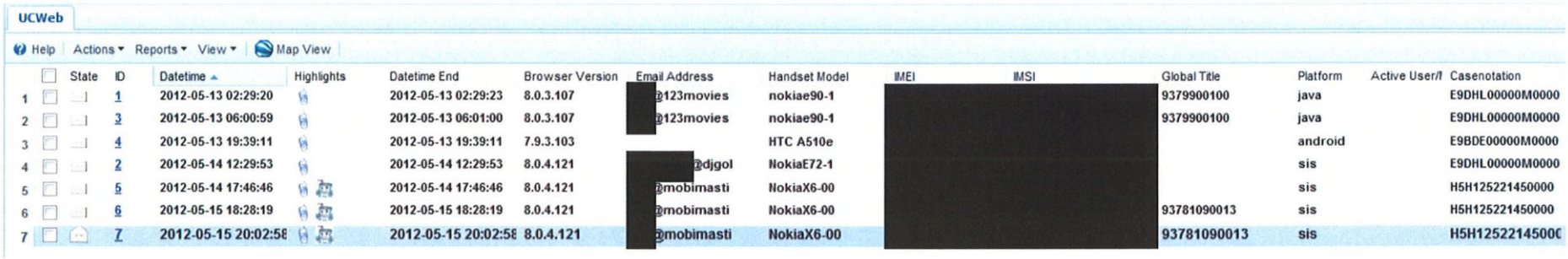
Vulnerabilities in update processes

- Remote code execution
- Vulnerabilities
  - Failing to check digital signatures (or protected with easily decryptable crypto)
    - Baidu Android, Baidu Windows, QQ Android, UC Windows
  - Failing to check version numbers → downgrade to vulnerable version
    - QQ Windows
  - Failing to check app name → sidegrade to vulnerable product
    - QQ Windows, UC Android

Success Stories

* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop
  * Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics

UCWeb – XKS Microplugin



UCWeb

Help | Actions | Reports | View | Map View

	State	ID	Datetime	Highlights	Datetime End	Browser Version	Email Address	Handset Model	IMEI	IMSI	Global Title	Platform	Active User/I	Casenotation
1		1	2012-05-13 02:29:20		2012-05-13 02:29:23	8.0.3.107	[redacted]@123movies	nokiae90-1	[redacted]		9379900100	java		E9DHL00000M0000
2		3	2012-05-13 06:00:59		2012-05-13 06:01:00	8.0.3.107	[redacted]@123movies	nokiae90-1			9379900100	java		E9DHL00000M0000
3		4	2012-05-13 19:39:11		2012-05-13 19:39:11	7.9.3.103		HTC A510e				android		E9BDE00000M0000
4		2	2012-05-14 12:29:53		2012-05-14 12:29:53	8.0.4.121	[redacted]@djgol	NokiaE72-1				sis		E9DHL00000M0000
5		5	2012-05-14 17:46:46		2012-05-14 17:46:46	8.0.4.121	[redacted]@mobimasti	NokiaX6-00				sis		H5H125221450000
6		6	2012-05-15 18:28:19		2012-05-15 18:28:19	8.0.4.121	[redacted]@mobimasti	NokiaX6-00			93781090013	sis		H5H125221450000
7		7	2012-05-15 20:02:58		2012-05-15 20:02:58	8.0.4.121	[redacted]@mobimasti	NokiaX6-00			93781090013	sis		H5H12522145000

UCWeb

* Led to discovery of active comms channel from [redacted]

(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from [redacted] that is associated with the [redacted] as they are known within the [redacted] hierarchy area of responsibility is for covert activities in Europe, North America, and South America. The customer [redacted] leveraged a ***Convergence Discovery capability that enabled the discovery of a covert channel associated with smart phone browser activity in passive collection****. The covert channel originates from users who use UCBrowser (mobile phone compact web browser).* ***The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in*** *[redacted] Initial investigation has determined that perhaps malware can be associated when the covert channel is established. [redacted] covert exfil activity identifies SIGINT opportunity where potentially none may have existed before. Target offices that have access to X-KEYSCORE can search within this type of traffic based on their IMSI or IMEI to determine target presence*

Responsible Disclosure

Difficulties in submitting

Different conceptions of PII

Whac-a-mole

Why were there such similarities?

- Recall: the kinds of sensitive data leaked look very similar
- In one case, identically peculiar crypto algorithm

Market Factors

- Highly competitive market
- Collect it all
- Buying a (vulnerability) ecosystem

Why the similarities?

Political factors

- Lack of access to Google Play
- Chinese regulatory pressures
  - 2015 anti-terrorism law
  - Network security offices

Takeaways

- Security researchers should pay more attention to these understudied apps
- Huge user bases + major vulnerabilities = opportunity for user benefit
- Finding vulnerabilities in popular browsers is becoming increasingly difficult
- Any researcher that even looked at this traffic in Wireshark would know there is a problem
- We need to better engage with these companies and put pressure on them to design better products

Acknowledgments

This material is based upon work supported by the U.S. National Science Foundation under Grant Nos. #1420716 and #1518878. Jeffrey Knockel's research for this project was supported by the Open Technology Fund's Information Control Fellowship Program. Adam Senft's research for this project was supported by the John D. and Catherine T. MacArthur Foundation (Ronald J. Deibert, Principal Investigator). The authors would like to thank Seth Hardy, Masashi Crete-Nishihata, Andrew Hilts, Sarah McKune, and Jason Q. Ng for assisting with this research.

Questions?