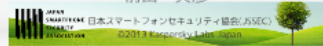


2013年のスマートフォンの脅威と
2014年の脅威予測



株式会社カスペルスキー
情報セキュリティラボ
前田 典彦



モバイル環境のマルウェア

- ・ 急激の増大
- ・ 質の悪化

高度化するAndroidマルウェア

Backdoor.AndroidOS.Obad.a

- ・ コード難読化・暗号化
- ・ 脆弱性悪用 (*)
- ・ バックグラウンドでの動作
- ・ 特権モード奪取
- ・ Botnetを構成

* Android OS, AndroidManifest.xml, Device Manager



チベット・ウイグル人権活動家
に対する一連の攻撃

「レッドアウトバー」件数

2013年のスマートフォンの脅威と 2014年の脅威予測



株式会社カスペルスキー
情報セキュリティラボ
前田 典彦



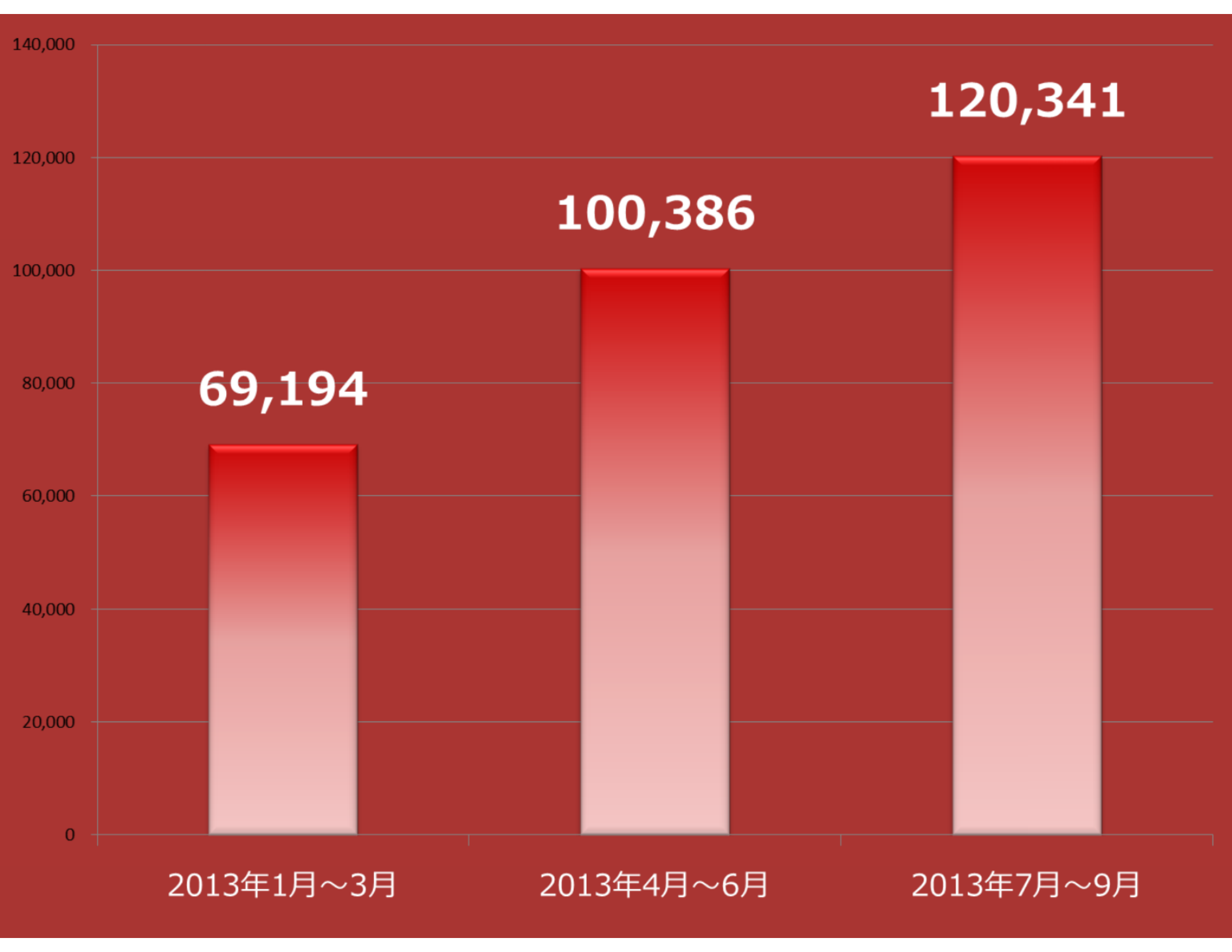
モバイル環境のマルウェア

- ・ 激増の時代
- ・ 質の変遷



モバイル系のマルウェア数





2013年1月~3月

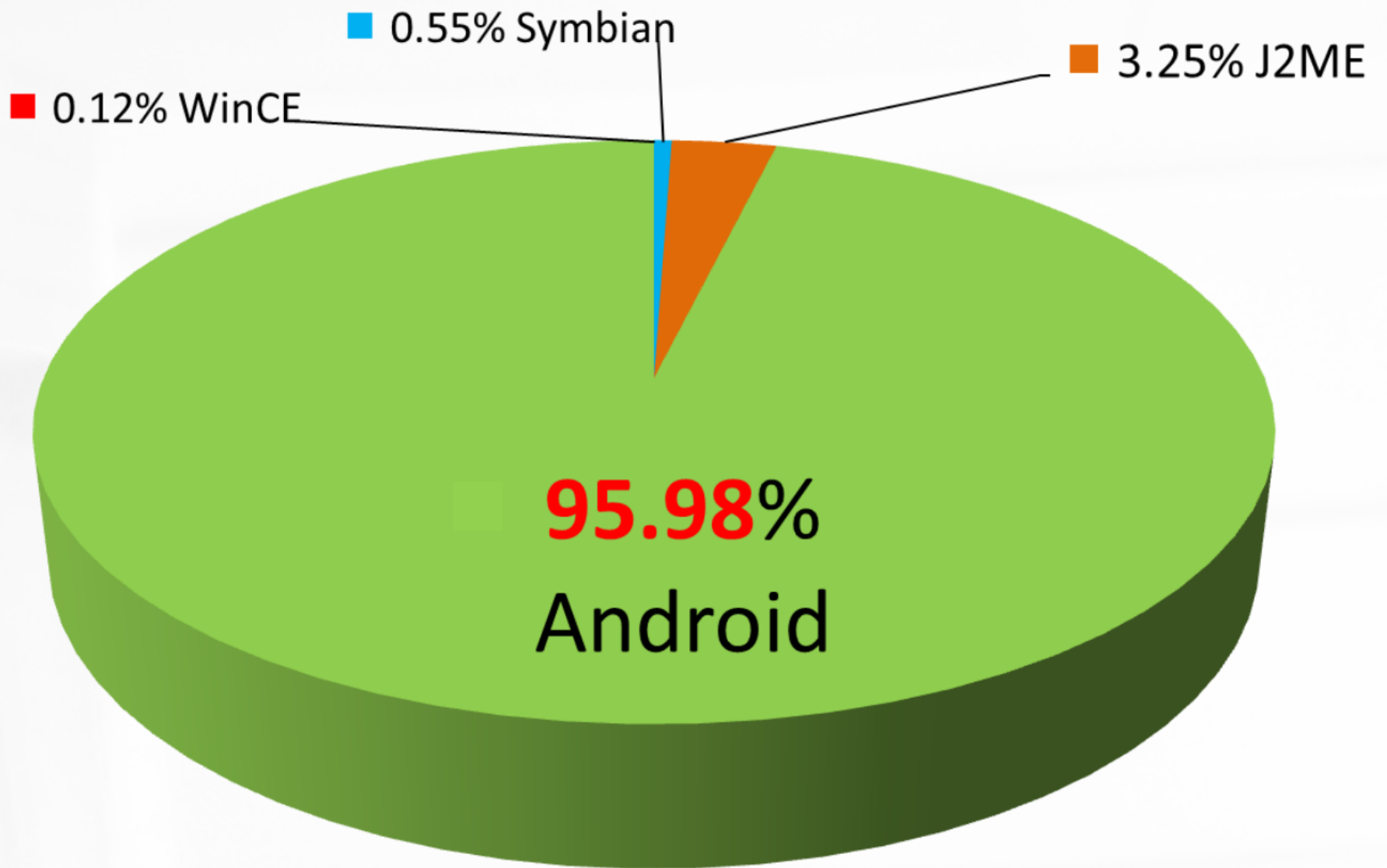
2013年4月~6月

2013年7月~9月

69,194

100,386

120,341



(2013年3月現在)

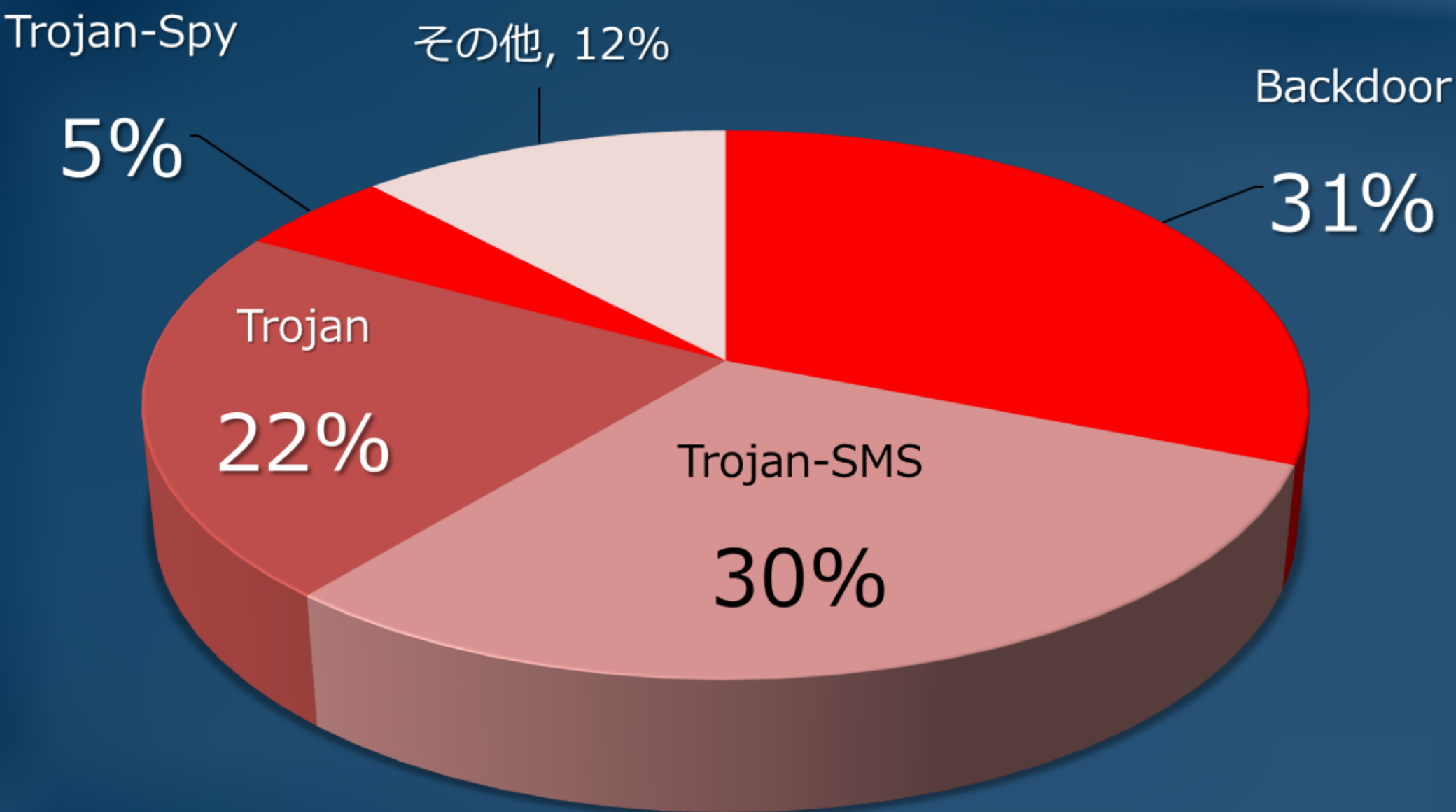






% J2ME

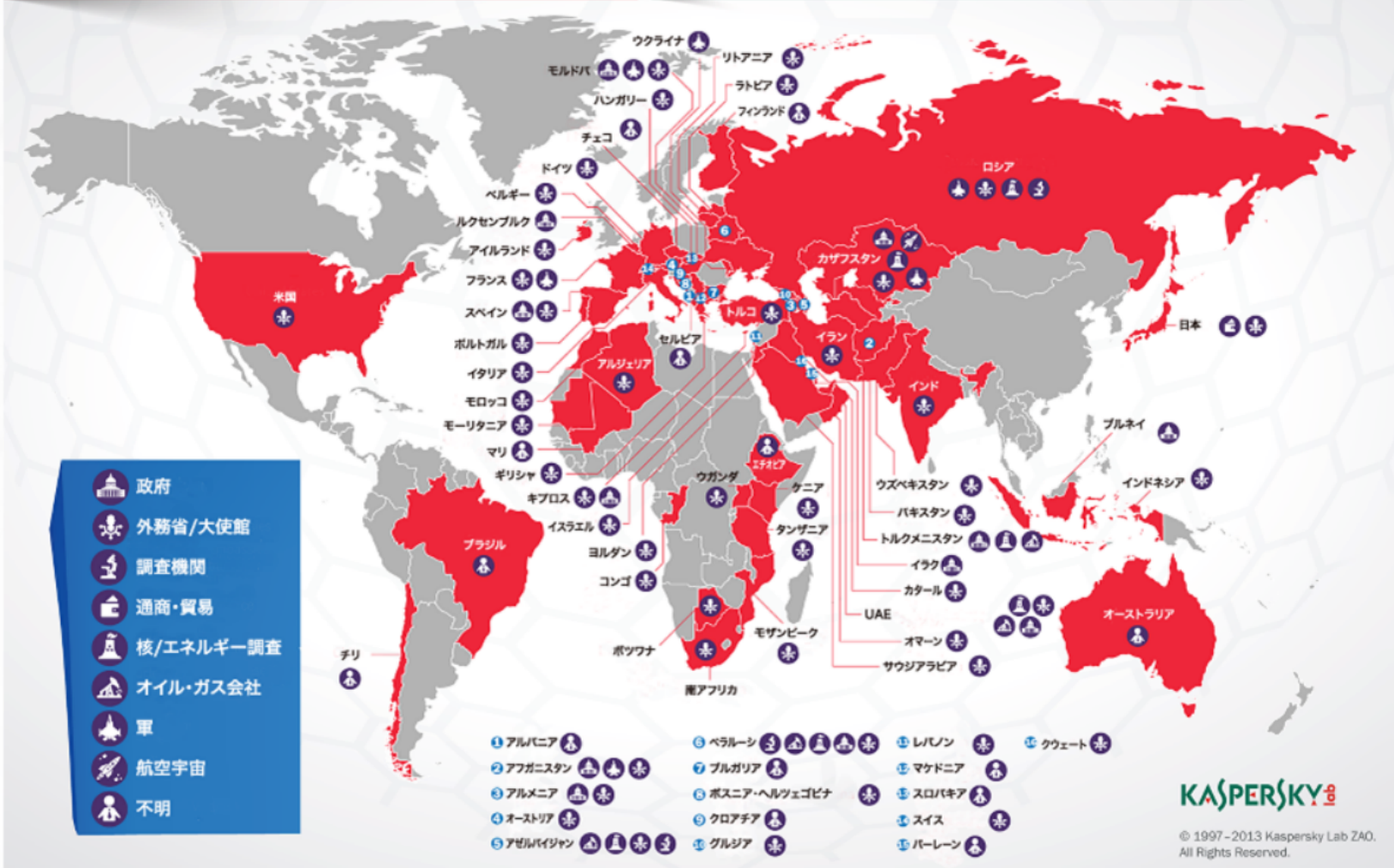




2013年7月～9月のマルウェア種別統計

「レッドオクトーバー」作戦

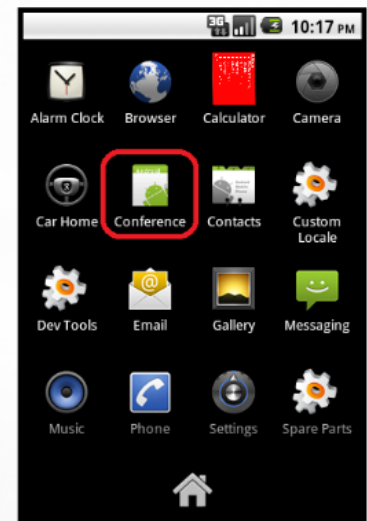
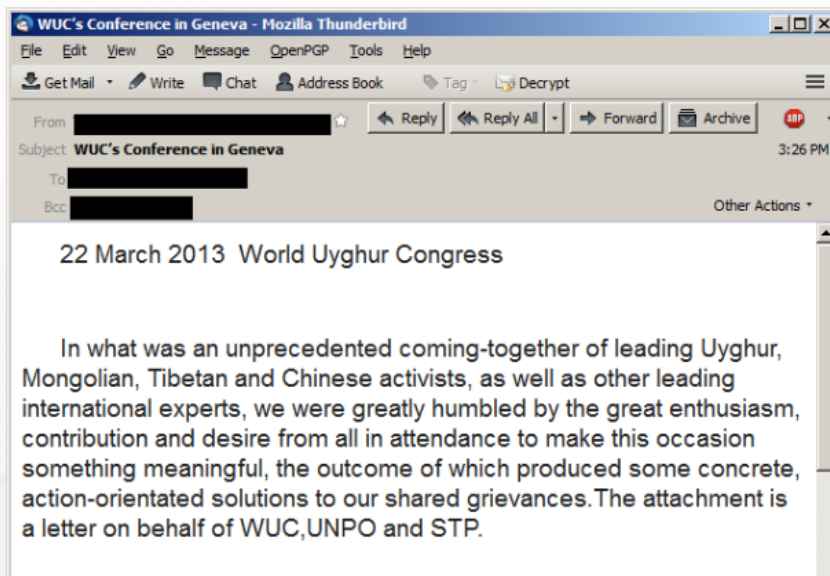
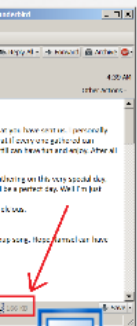
高度なサイバー諜報ネットワークによる被害



KASPERSKY

© 1997 - 2013 Kaspersky Lab ZAO. All Rights Reserved.

チベット・ウイグル人権活動家 に対する一連の攻撃



WUC's Co
in Geneva

On behal
the Word
Congress
the Unrep
Nations a
Organiza
and the S
Threaten
(STP), Hu
Rights in
Implicati
East Turk
Tibet and
Southern
In what w
unpreced



... Dalai Lama's birthday on July 6 to be low-key affair - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Mail Write Chat Address Book Tag

Reply Reply All Forward Archive

From [Redacted]

Subject Dalai Lama's birthday on July 6 to be low-key affair 4:39 AM

To [Redacted] Other Actions

Dear Friends,

Just dropped by to say that we went through those video links that you have sent us. I personally feel the selections are very relevant and appropriate. It will be great if every one gathered can participate and enjoy. I suppose we don't have to be perfect but still can have fun and enjoy. After all it's a celebration and if we manage to get it right, even better.

Another thing that I wanted to say is that, since most of us are gathering on this very special day, why don't we collect the green book contribution. I think that will be a perfect day. Well I'm just placing my own opinion.

We will be bringing Khabsey from Kerry! Lets hope it comes out delcious.

Greetings again from here.

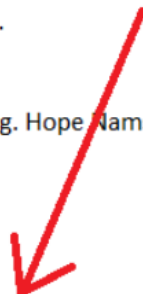
Please prepare the 2 following songs by all the tibetans as our group song. Hope Namsel can have these videos on her lap top

and play it on OHP while we sing together.

1- YANG- NYEN <http://www.youtube.com/watch?v=TImlAdxAxqc>

1 attachment: Dalai Lama's birthday on July 6 to be low-key affair.doc 166 KB Save

(G)o (S)ave (C)opy



Another thing that I wanted to say is that, since most of us are gathering on this very special day, why don't we collect the green book contribution. I think that will be a perfect day. Well I'm just placing my own opinion.

We will be bringing Khabsey from Kerry! Lets hope it comes out delcious.

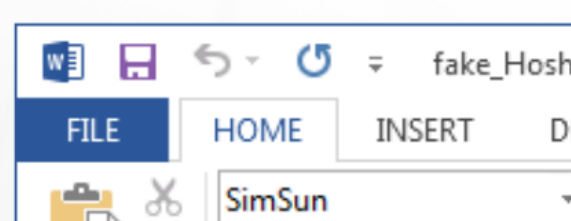
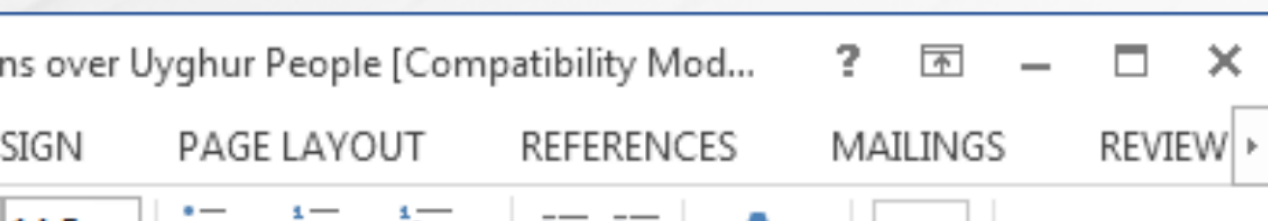
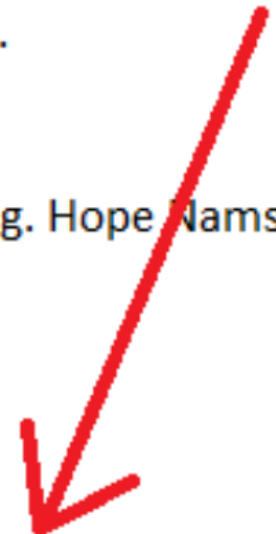
Greetings again from here.

Please prepare the 2 following songs by all the tibetans as our group song. Hope Namsel can have these videos on her lap top

and play it on OHP while we sing together.

1- YANG- NYEN <http://www.youtube.com/watch?v=TImlAdxAxgc>

1 attachment: Dalai Lama's birthday on July 6 to be low-key affair.doc 166 KB





fake_Concerns over Uyghur People [Compatibility Mod... ? - - -]

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW

Clipboard Font Paragraph Styles Editing

Concerns over Uyghur People's Fundamental Rights Under the New Chinese Leadership

The Chinese government has been placing tight constraints on Uyghur People's Fundamental Rights, from economy, social, education, religion to freedom of speech. As people across the globe shared their hopes and dreams for 2013 with families and friends at the turn of the New Year, reports that Uyghur writer Nurmemet Yasin had died in Shaya prison 'sometime in 2011' were still unconfirmed. The confusion surrounding Nurmemet Yasin's condition serves as a damning indictment not only on the treatment of Uyghur political prisoners by the Chinese authorities, but also on the lack of information made available on them to the outside world. Secrecy is so pervasive in the Chinese penal system that even when a Uyghur serves their sentence, as was the case in 2012 with website administrator Nureli Obul, it remains unknown if they were actually released. Uyghurs also tasted official retribution if they attempted to cross Chinese borders to seek refuge from government repression. In January 2012, Radio Free Asia described how Musa Muhammad, one of 20 Uyghur asylum seekers forcibly deported from Cambodia on December 19, 2009, had been sentenced to 17 years in prison by a Chinese court during a closed trial. *China's Confined* reports, the Uyghur American Association also reported that 17 Uyghur refugees forcibly deported from Islam Urayin, had also been sent

PAGE 1 OF 2 456 WORDS

fake_Hosh Hewer [Compatibility Mode] - Word (Trial) ? - - -

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW

Clipboard Font Paragraph Styles Editing

Hosh Hewer


Putun Dunyadiki Sherq Turkistanliq qerindashlar. Bizning medinyetimiz we tariximiz, putun millitimiz bahqilarning qolida monopoliyebolup, bashqilarning yersharidindin supurup tashlaydighan reqi obiktigha aylinip qaldi. Del mushundaq peytte, bizning medenyitimizni bashqilar bizning medenyitimizde oz medenyitidep teshviq qilip, tala-taranj qilivatnaqta. Hem sheherlirimizni cheqip izini zni yoqataqta. Shunlashqa hazir biz Uyghur ziyaliliri, bolupmu ijtimaipepde oqighan yazghuclirimiz, tarixchilirimiz, alimlirimiz, tetqiqatchilirimiz birliship, helq ara Uyghur medenyet merkiqurupchiqtuq. Buning board ezaliri, otturaAsiya we Bashqa doletlerdinmu terkiptap qanbolup, Amerikida 7 neper pishqedem hadimlarning yitek chiligide boldi. Biz buni qurupchiqqanqha 2 yilbolhamb olghanbolsimu, ihtisadi we her hilsewepler tupeyli hem we imkaniyetlirimizni toluqlap bolalmighanliqimiz uchun kichikip olan qilduq. Medenyet Merkiqi bizge Fort washin gitondin 109 no yer, 3 qewetlik bina olduq. Yeqinda un inggha mektep, kutuphane, korsezmihane, neshriyat we Uyghur sen' et merkiqi we din we tilmektiwi hem helqimizning oz-ara uchrishish organliri, toy-chay qilish merike

PAGE 1 OF 2 272 WORDS

fake_Kadeer Logistics detail [Compatibility Mode] - Wor... ? - - -

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW

Clipboard Font Paragraph Styles Editing



**DUKE UNIVERSITY
AMERICAN
GRAND STRATEGY**
AN STRATEGIC INITIATIVE OF DUKES

*The Duke Program in American Grand Strategy
Presents:*

Ms. RebiyaKadeer

February 11-12, 2012
Duke University
The University of North Carolina at Chapel Hill

PAGE 1 OF 6 1345 WORDS

fake_Jenwediki yinghina iltimas qilish Jedwili [Compat... ? - - -]

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW

Clipboard Font Paragraph Styles Editing

Times New Roman 11

„Xitayning Yengi Rehberliki: Sherqiy Turkistan, Tibet we Jenubi Monghulyede Kishlik Hoquq, Demokirasiye we Azatliqa qaritilwatqan Xirislar“ namlig Xelqaralig Muhakime yighini

Jenwa, Swetsariya 11-13-Mart 2013

Iltimas Qilish Jedweli

Intivoli eniq, usghulit bulidighan shakilde, imken her kempoterde teldurup, essenditit aditiga yallang

World Uyghur Congress, Adolf-Kobinger-5, 80336 München.
Email: emserken@gmail.com, yakir.dobras@gmail.com Fax: +49 89 34249789

I. Iltimas qilghuchi haqide melumat

Isim-Familisi (Passportidek yezilishi):	Ilbat Hassan
Tughulghan waxti:	17.06.1962, Tughulghan Yeri:Ghulna
Dölet Teweligi:	USA, Hazir Turwatqan Döliiti:USA
Passport Numuri:	Document, Passporting berilgen waxti:February 25, 2009
Passporting toshidighan waxti:	February 25, 2019

II. Iltimas qilghuchining alaqilishish melumati

PAGE 1 OF 1 144 WORDS



From [Redacted] ☆

Reply Reply All Forward Archive



Subject WUC's Conference in Geneva

3:26 PM

To [Redacted]

Bcc [Redacted]

Other Actions

22 March 2013 World Uyghur Congress

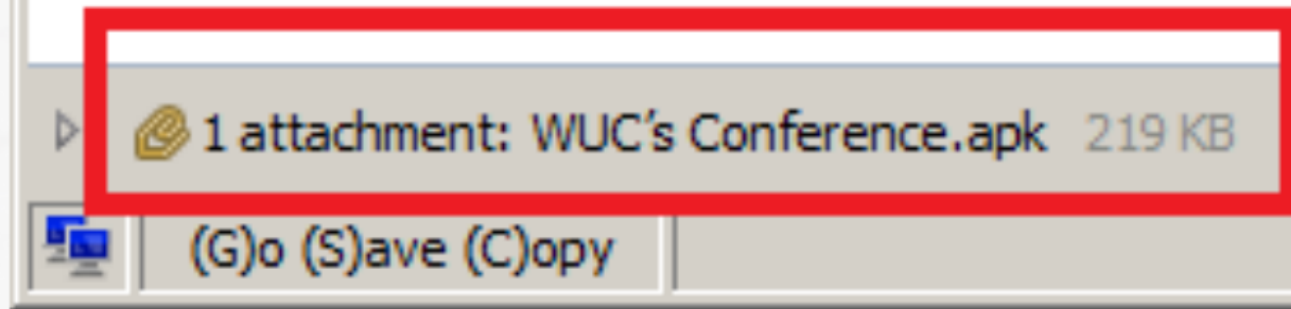
In what was an unprecedented coming-together of leading Uyghur, Mongolian, Tibetan and Chinese activists, as well as other leading international experts, we were greatly humbled by the great enthusiasm, contribution and desire from all in attendance to make this occasion something meaningful, the outcome of which produced some concrete, action-orientated solutions to our shared grievances. The attachment is a letter on behalf of WUC, UNPO and STP.

1 attachment: WUC's Conference.apk 219 KB

Save

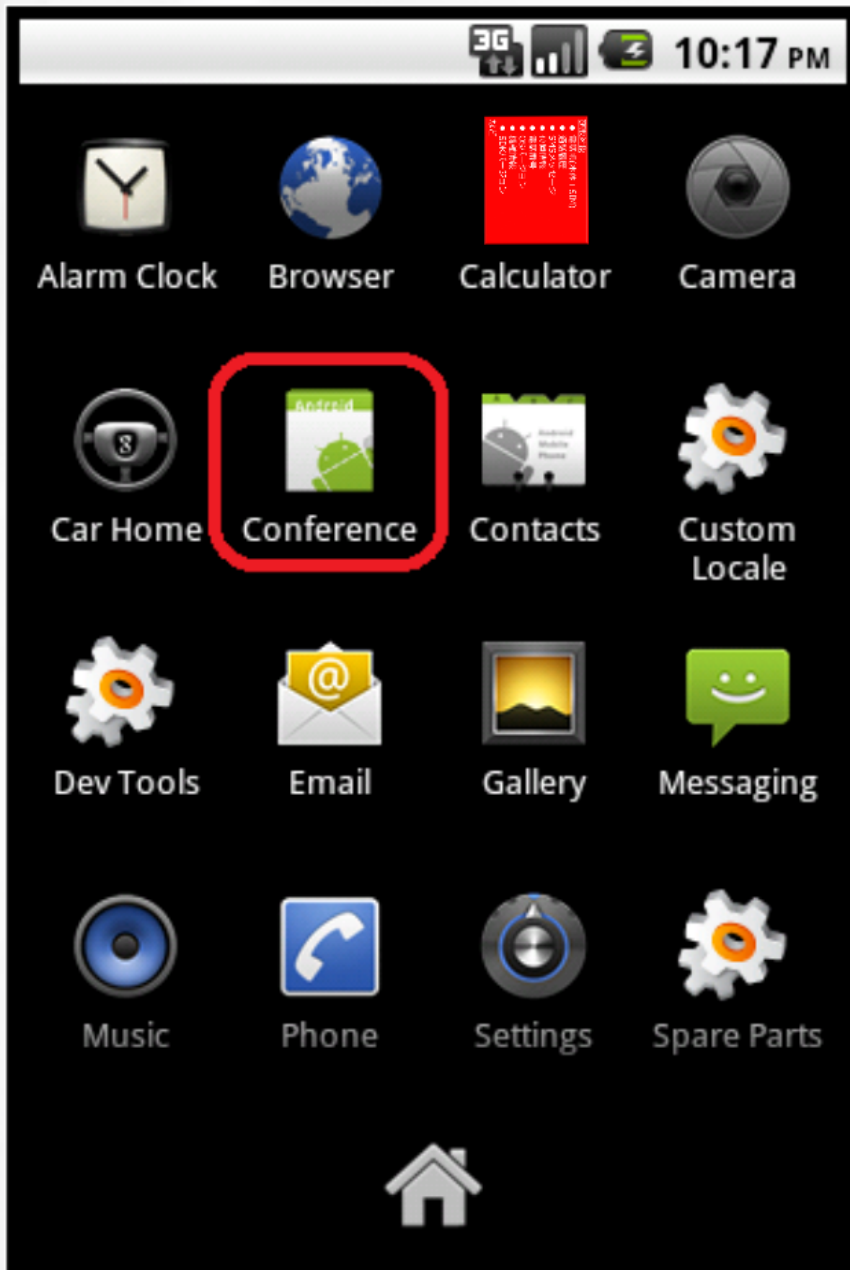


international experts, we were greatly humbled by the contribution and desire from all in attendance to make something meaningful, the outcome of which produced action-orientated solutions to our shared grievance. I am sending a letter on behalf of WUC, UNPO and STP.



Backdoor.AndroidOS.Chuli.a





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

窃取対象

- 電話帳(本体+SIM)
- 通話履歴
- SMSメッセージ
- 位置情報
- 電話番号
- OSバージョン
- 機種情報
- SDKバージョン

など

高度化するAndroidマルウェア

Backdoor.AndroidOS.Obad.a

- コード難読化・暗号化
- 脆弱性悪用 (*)
- バックグラウンドでの動作
- 特権モード奪取
- Botnetを構成



(*) DEX2JAR, AndroidManifest.xml, Device Manager

18:17

com.android.system.ad...

Do you want to install this application?

Allow this application to:

- **Your messages**
edit SMS or MMS, read SMS or MMS, receive SMS
- **Network communication**
create Bluetooth connections, full Internet access
- **Your personal information**
read contact data, read sensitive log data
- **Storage**
modify/delete SD card contents
- **Phone calls**
intercept outgoing calls, read phone state and identity
- **Services that cost you money**
directly call phone numbers, send SMS messages
- **System tools**

Cancel Install

18:18

Activate device administrator?

System

Attention! To install the application, you need to admin access!

Activating this administrator will allow the app com.android.system.admin to perform the following operations:

- **Lock the screen**
Control when your device locks, requiring that you re-enter your password.

Cancel Activate

Saving screenshot...

System

com.android.system.admin has been denied superuser permissions:
id

2014年の予測





ありがとうございました

株式会社カスペルスキー
前田 典彦
maeda@kaspersky.co.jp



Kaspersky, カスペルスキーは、Kaspersky Lab, ZAOの登録商標です。その他の会社名・製品名等は一般的に各社の登録商標ないしは商標です。本文書の無断配布・転記載・複製を禁止します。本文書の内容は事前の予告なく変更する場合があります。

©2013 Kaspersky Labs Japan

2013年11月28日 JSSEC日本スマートフォンセキュリティ協会 技術部会主催
「2013年のスマートフォンの脅威と2014年の脅威予測」カンファレンス @東京電機大学