HELLO APTS IN THE MIDDLE EAST

By **Mohamad Amin Hasbini**

Senior Security Researcher

Kaspersky Lab

Introduction

Name: Mohamad Amin Hasbini

- Senior Security Researcher - Kaspersky Lab - Global Research and Analysis Team www.kaspersky.com
- X-DataConsult www.dcgroup.com
- Board member - Securing Smart Cities www.securingsmartcities.org
- PHD student - Brunel University London www.brunel.ac.uk

Agenda

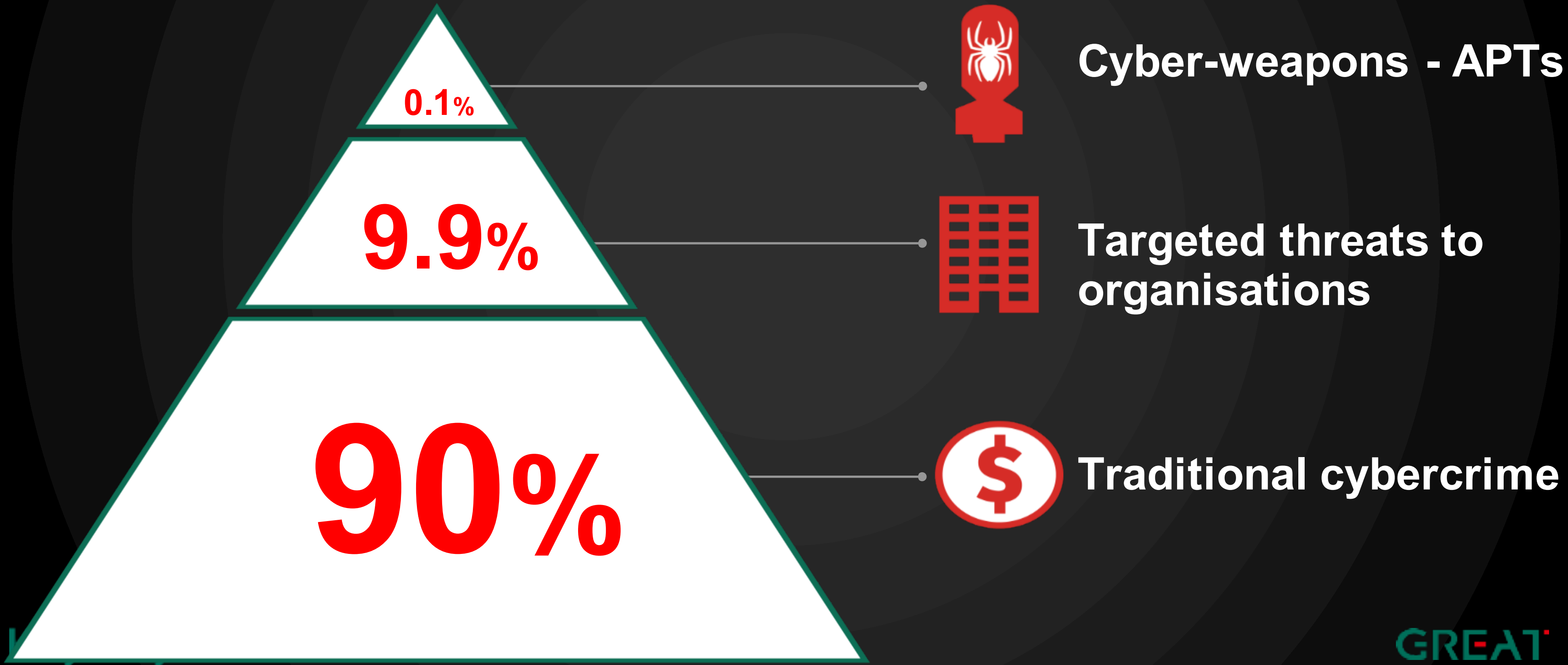
Volatile Cedar

Carbanak

TURLA

APTs

The nature of the threats - 2016



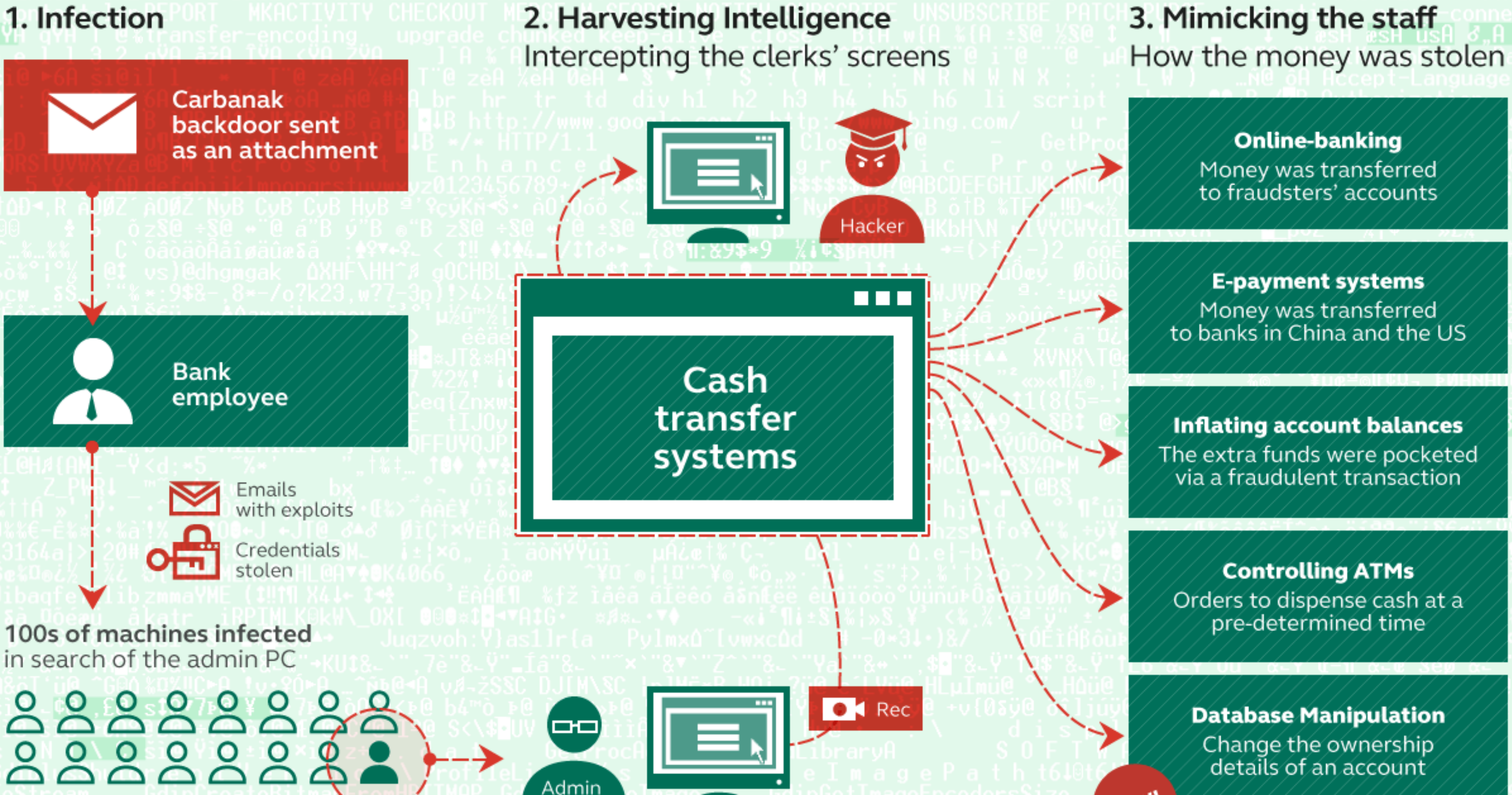
0.1% — Cyber-weapons - APTs

9.9% — Targeted threats to organisations

90% — Traditional cybercrime

CARBA

How the Carbanak cybergang targets financial organizations



1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected
in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

Hacker

Cash transfer systems

Rec

Admin

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

Database Manipulation
Change the ownership details of an account

Carbanak 2015

- Attacks in budget deps
- Change registration data of shareholders' in depository

New C&C Panels?

- Samples
- Passive DNS and domains
- Other’s IOCs?..

Oh look

```
Notice: Undefined index: HTTP_HOST
in /var/www/html/application/
modules/Crypt.php on line 6
```

Oh look

Scan
ALL the
hosts!

Stage 1

SYN-scan
the globe

Stage 2

Interrogate the hosts

New C&C Panels!

+

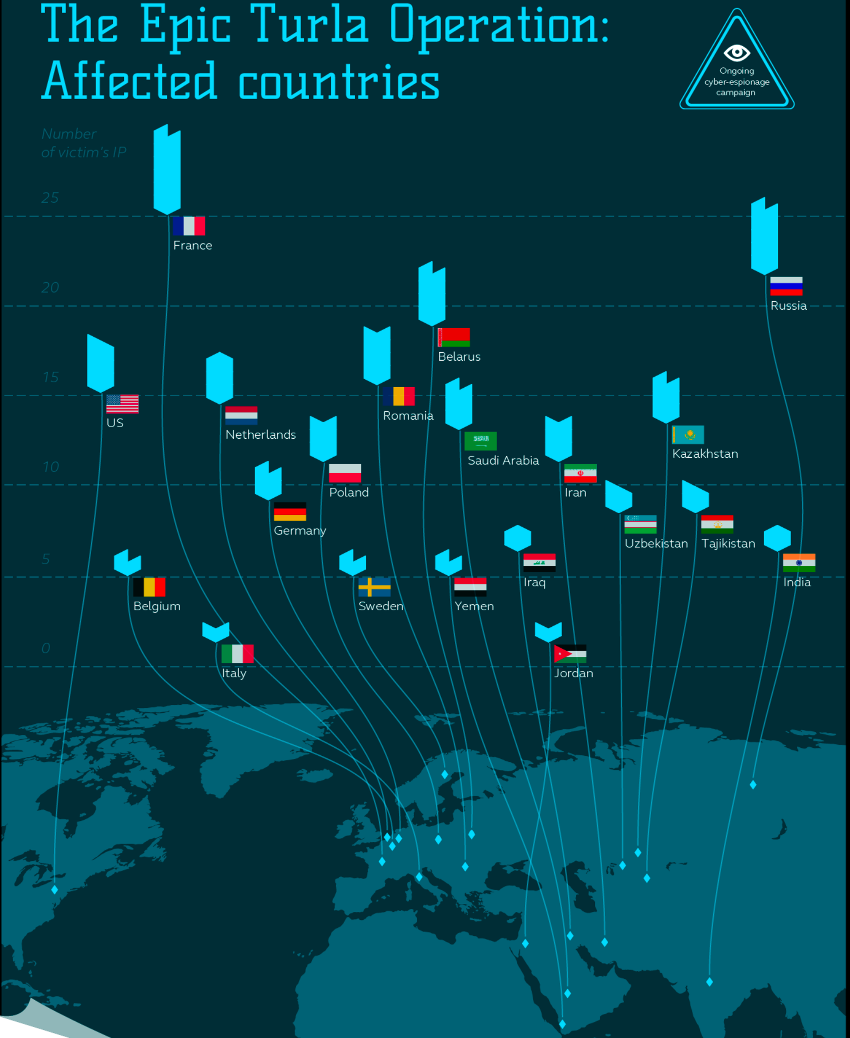
= Carbanak intel

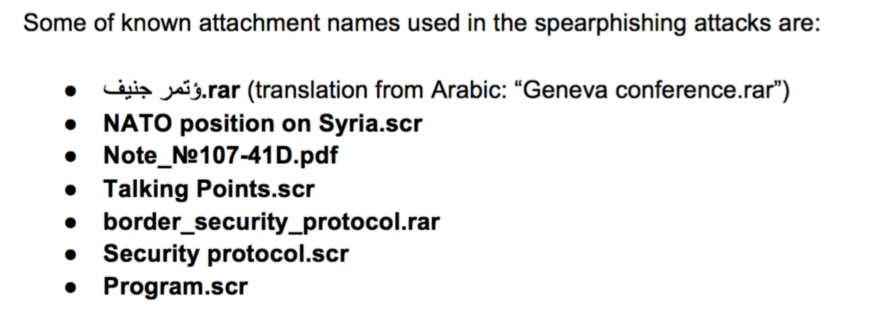
CARBANAK SUMMARY

1. Global criminals’ ATP
2. Spear-phishing is everything
3. It is all about MONEY

TURLA

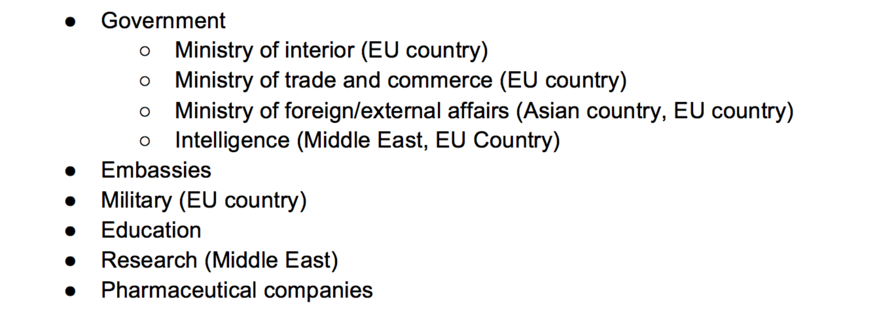
The Epic Turla Operation: Affected countries



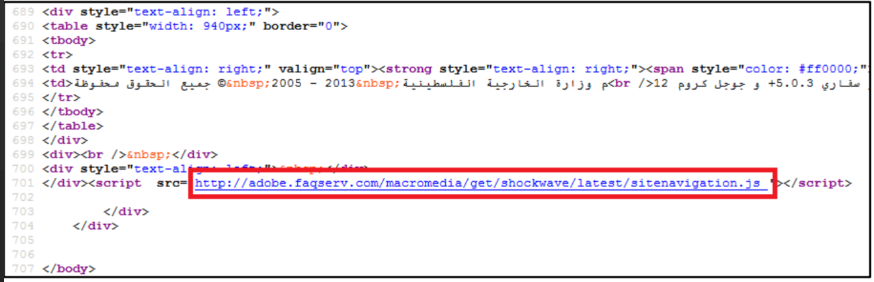


Some of known attachment names used in the spearphishing attacks are:

- **مؤتمر جنيف.rar** (translation from Arabic: “Geneva conference.rar”)
- **NATO position on Syria.scr**
- **Note_№107-41D.pdf**
- **Talking Points.scr**
- **border_security_protocol.rar**
- **Security protocol.scr**
- **Program.scr**

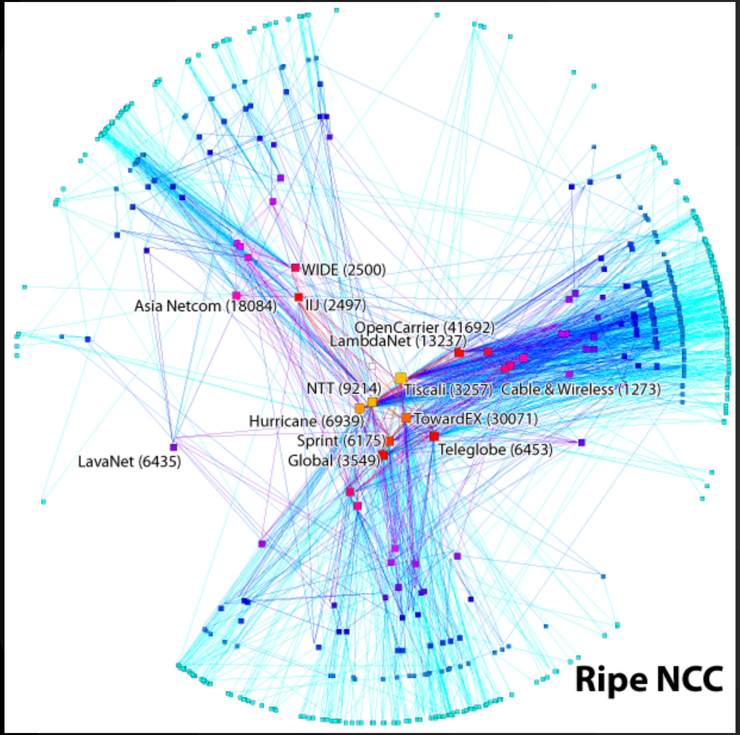


- Government
  - Ministry of interior (EU country)
  - Ministry of trade and commerce (EU country)
  - Ministry of foreign/external affairs (Asian country, EU country)
  - Intelligence (Middle East, EU Country)
- Embassies
- Military (EU country)
- Education
- Research (Middle East)
- Pharmaceutical companies

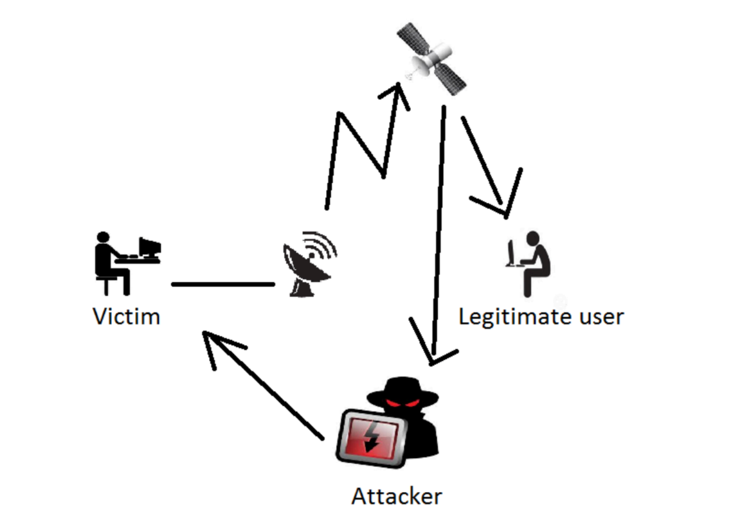


```
<div style="text-align: left;">
<table style="width: 940px;" border="0">
<tbody>
<tr>
<td style="text-align: right;" valign="top"><strong style="text-align: right;"><span style="color: #ff0000;"
<td>جميع الحقوق محفوظة ©&nbsp;2005 - 2013&nbsp;وزارة الخارجية الفلسطينية<br />م سفاري 5.0.3+ و جوجل كروم 12
</tr>
</tbody>
</table>
</div>
<div><br />&nbsp;</div>
<div style="text-al
</div><script  src= http://adobe.faqserv.com/macromedia/get/shockwave/latest/sitenavigation.js '></script>


        </div>
    </div>



</body>
```

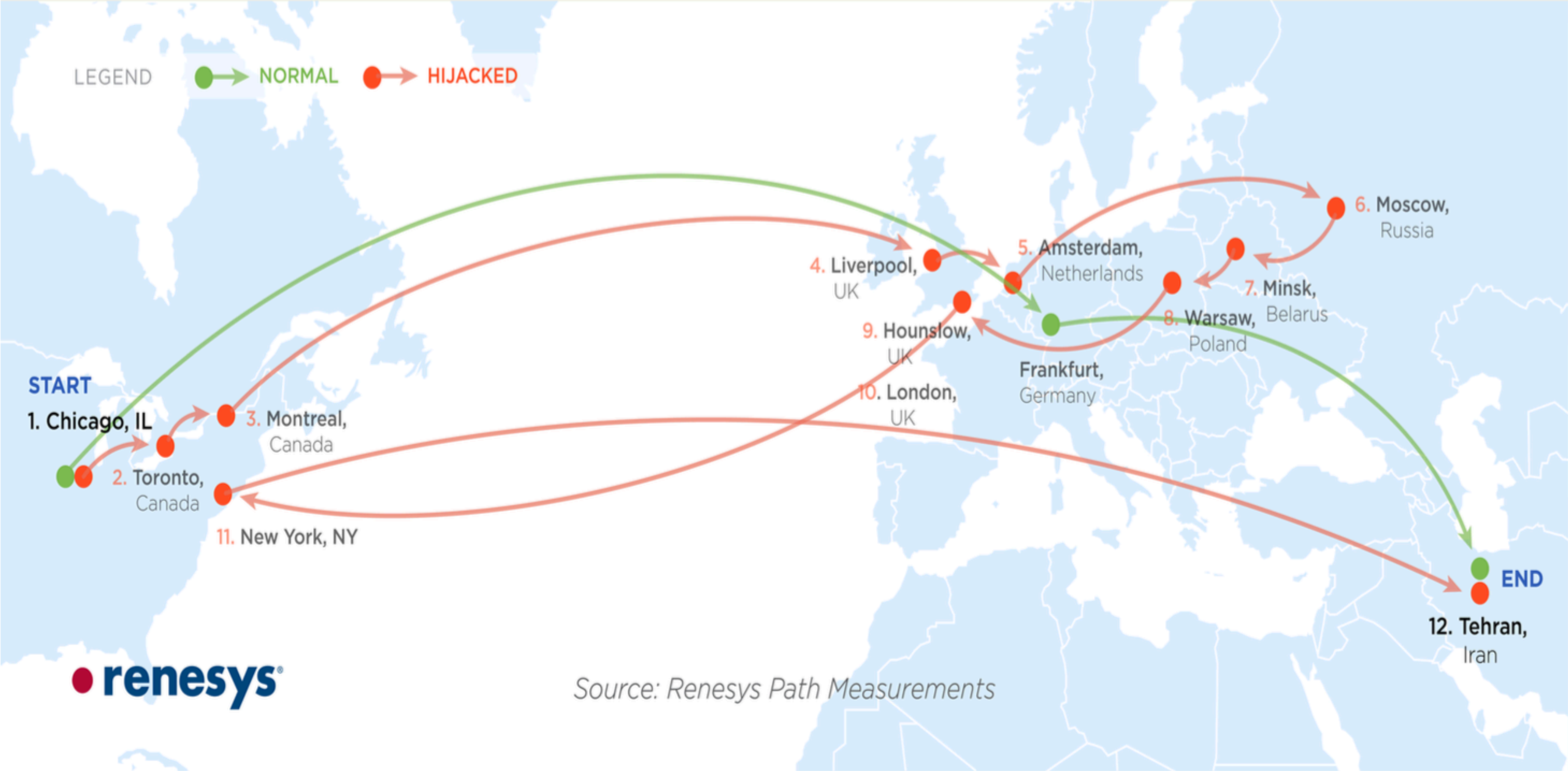
TURLA Satellite


WIDE (2500)
Asia Netcom (18084)
IIJ (2497)
OpenCarrier (41692)
LambdaNet (13237)
NTT (9214)
Tiscali (3257)
Cable & Wireless (1273)
Hurricane (6939)
TowardEX (30071)
Sprint (6175)
Teleglobe (6453)
Global (3549)
LavaNet (6435)
Ripe NCC

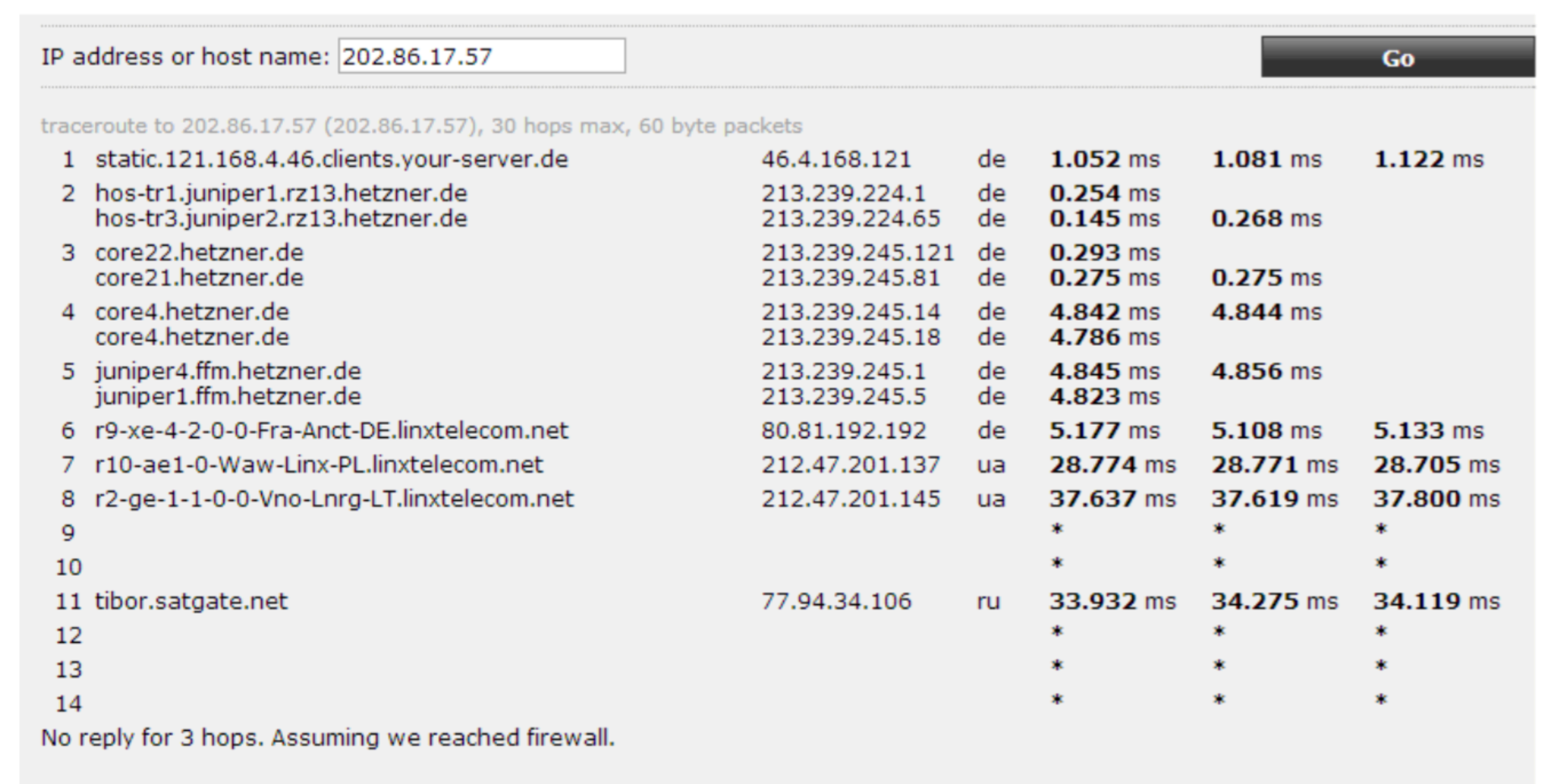
Country	Infrastructure
Lebanon	2 providers, 4 ip addresses
Iraq	1 provider, 1 ip address
Nigeria	2 providers, 4 ip addresses
United Arab Emirates	1 provider, 4 ip addresses
Denmark	1 provider, 3 ip addresses
United Kingdom	1 provider, 1 ip address
Zambia	1 provider, 1 ip address
Afghanistan	1 provider, 1 ip address
Somalia	1 provider, 1 ip address



Traceroute Path 4: from **Chicago**, IL to **Tehran**, Iran



Source: Renesys Path Measurements



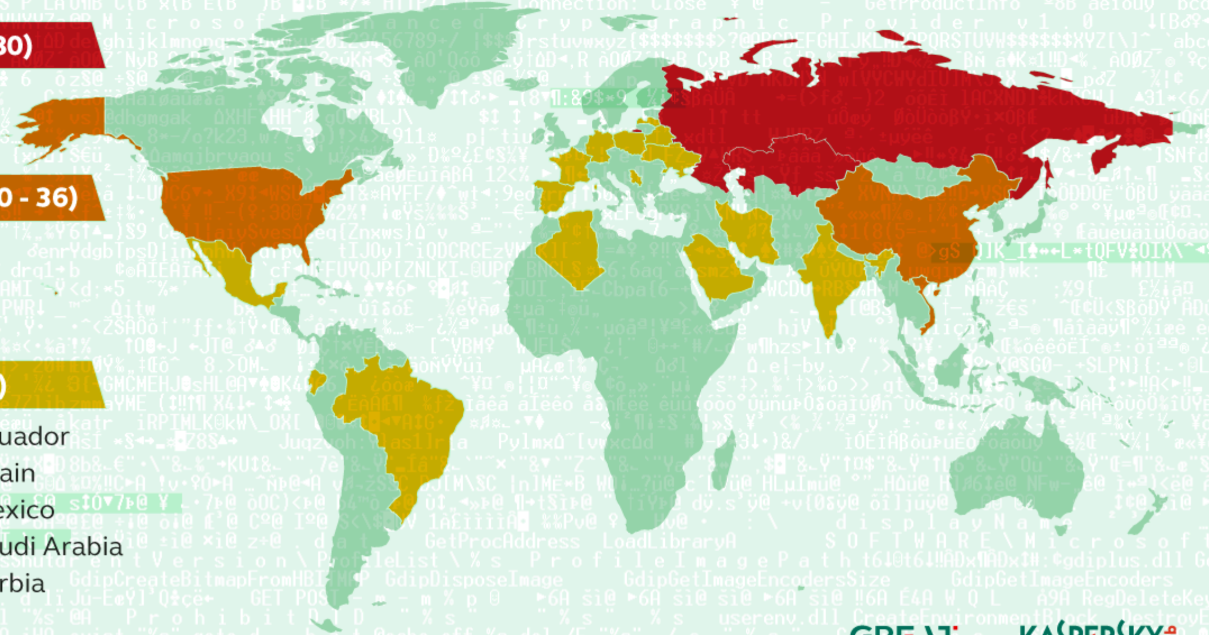
IP address or host name: 202.86.17.57

```
traceroute to 202.86.17.57 (202.86.17.57), 30 hops max, 60 byte packets
  1  static.121.168.4.46.clients.your-server.de  46.4.168.121     de  1.052 ms   1.081 ms   1.122 ms
  2  hos-tr1.juniper1.rz13.hetzner.de            213.239.224.1    de  0.254 ms
     hos-tr3.juniper2.rz13.hetzner.de            213.239.224.65   de  0.145 ms   0.268 ms
  3  core22.hetzner.de                           213.239.245.121  de  0.293 ms
     core21.hetzner.de                           213.239.245.81   de  0.275 ms   0.275 ms
  4  core4.hetzner.de                            213.239.245.14   de  4.842 ms   4.844 ms
     core4.hetzner.de                            213.239.245.18   de  4.786 ms
  5  juniper4.ffm.hetzner.de                     213.239.245.1    de  4.845 ms   4.856 ms
     juniper1.ffm.hetzner.de                     213.239.245.5    de  4.823 ms
  6  r9-xe-4-2-0-0-Fra-Anct-DE.linxtelecom.net   80.81.192.192    de  5.177 ms   5.108 ms   5.133 ms
  7  r10-ae1-0-Waw-Linx-PL.linxtelecom.net       212.47.201.137   ua  28.774 ms  28.771 ms  28.705 ms
  8  r2-ge-1-1-0-0-Vno-Lnrg-LT.linxtelecom.net   212.47.201.145   ua  37.637 ms  37.619 ms  37.800 ms
  9                                                                   *          *          *
 10                                                                   *          *          *
 11  tibor.satgate.net                           77.94.34.106     ru  33.932 ms  34.275 ms  34.119 ms
 12                                                                   *          *          *
 13                                                                   *          *          *
 14                                                                   *          *          *
No reply for 3 hops. Assuming we reached firewall.
```

Map of targets of the Turla group

Turla is a sophisticated cyberespionage group that has been active for more than 8 years. The attackers behind Turla have infected hundreds of computers in more than 45 countries.

Government institutions · Embassies · Military entities · Education organizations · Research organizations · Pharmaceutical companies



High infection rate (36 - 80)

Kazakhstan
Russia

Medium infection rate (10 - 36)

China
Vietnam
USA

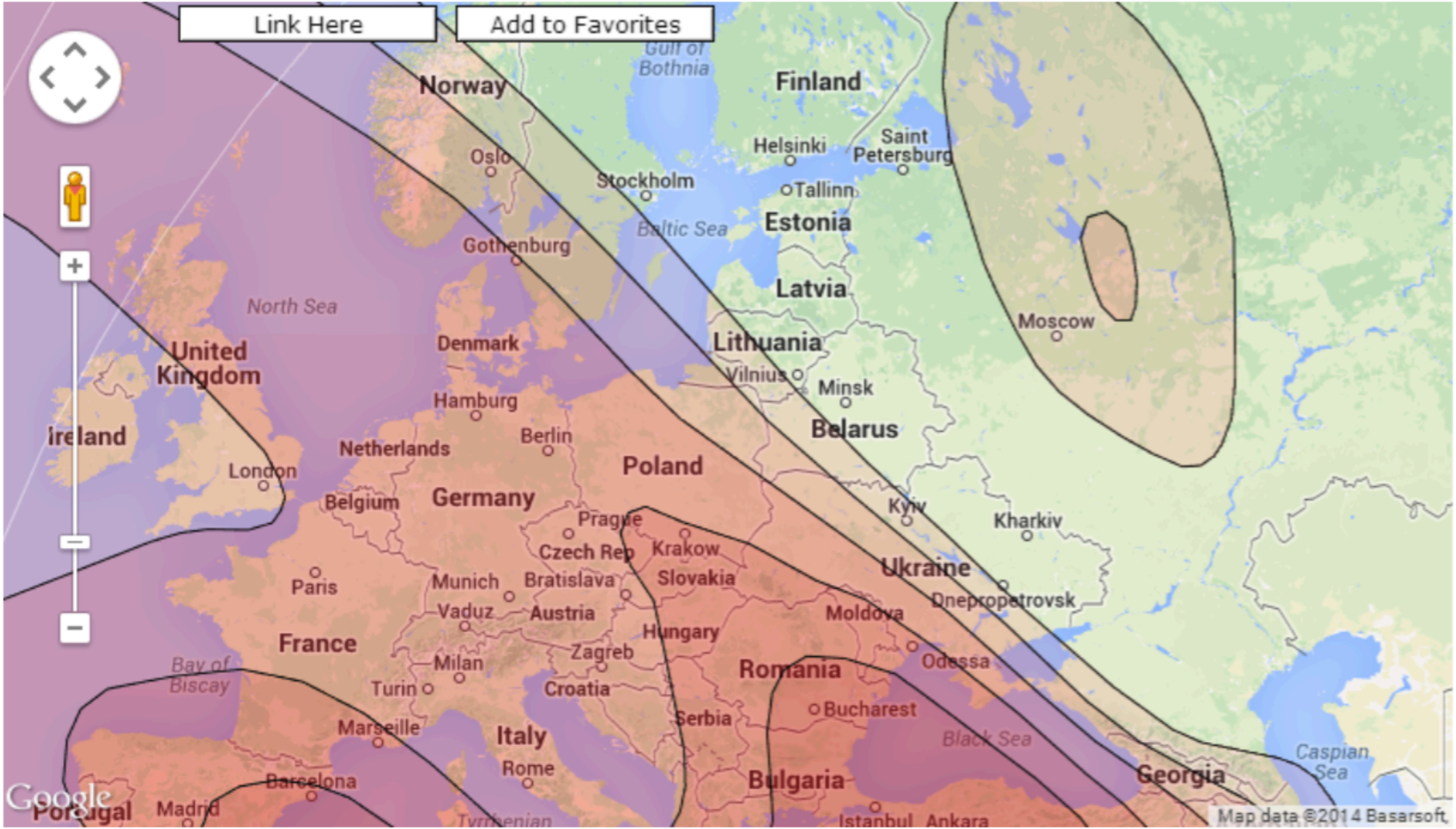
Low infection rate (1 - 10)

Poland
Ukraine
Germany
India
France

Iran
Latvia
Algeria
Brazil
Belarus

Ecuador
Spain
Mexico
Saudi Arabia
Serbia

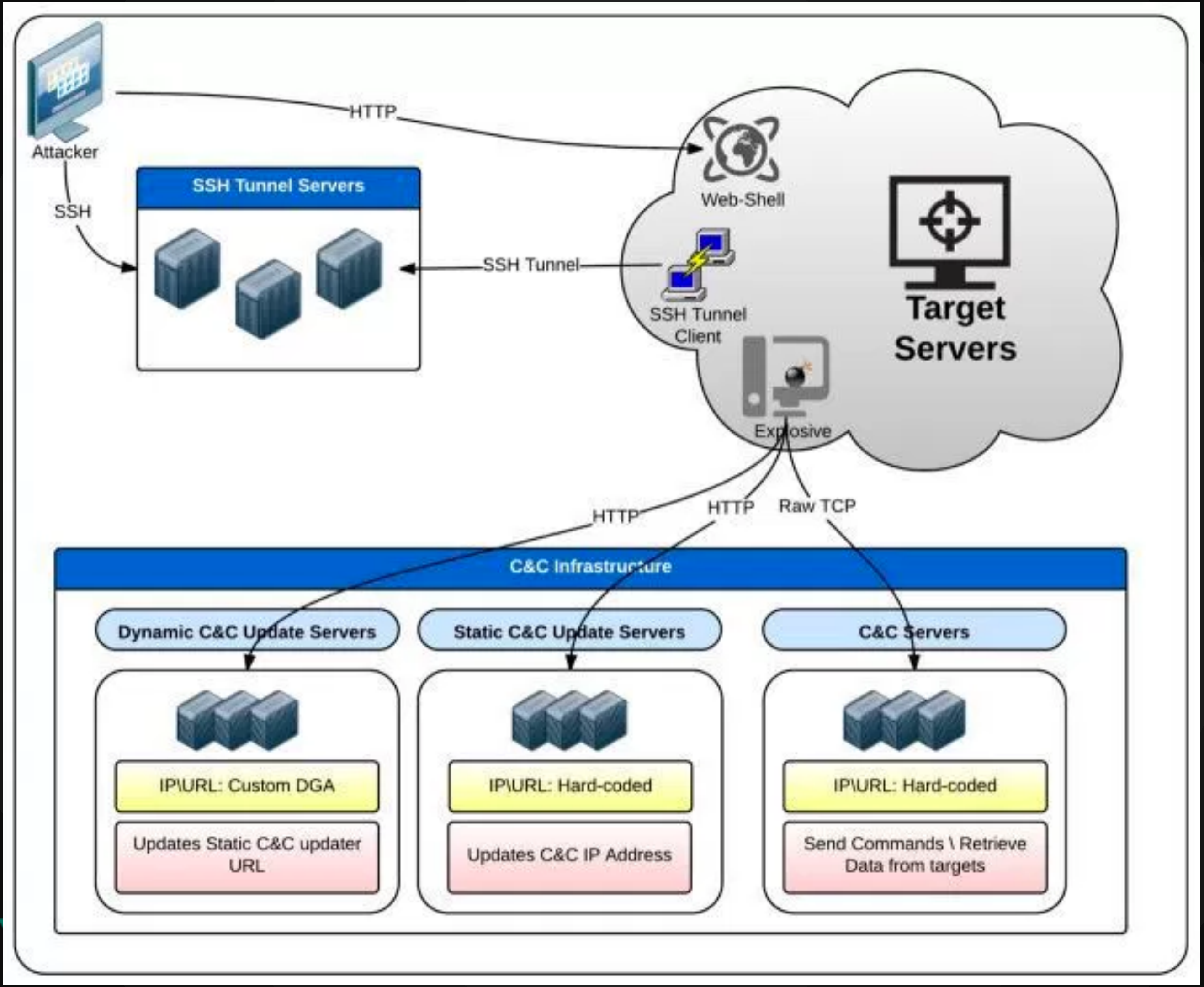
GREAT KASPERSKY lab


Link Here
Add to Favorites
Gulf of Bothnia
Finland
Norway
Helsinki
Saint Petersburg
Oslo
Stockholm
Tallinn
Estonia
Baltic Sea
Gothenburg
Latvia
North Sea
Moscow
Denmark
Lithuania
United Kingdom
Vilnius
Minsk
Hamburg
Ireland
Berlin
Belarus
Netherlands
Poland
London
Germany
Belgium
Kyiv
Kharkiv
Prague
Czech Rep
Krakow
Paris
Munich
Bratislava
Slovakia
Ukraine
Vaduz
Austria
Dnepropetrovsk
Moldova
France
Hungary
Milan
Zagreb
Odessa
Bay of Biscay
Turin
Croatia
Romania
Bucharest
Marseille
Italy
Serbia
Black Sea
Caspian Sea
Georgia
Rome
Barcelona
Bulgaria
Portugal
Madrid
Tyrrhenian
Istanbul
Ankara
Google
Map data ©2014 Basarsoft

TURLA SUMMARY

1. BGP Hijacking and Satellites
2. Anonymous infections
3. State-sponsored attack

Volatile Cedar



Attacker

HTTP

SSH

SSH Tunnel Servers

SSH Tunnel

Web-Shell

SSH Tunnel Client

Explosive

Target Servers

HTTP

HTTP

Raw TCP

C&C Infrastructure

Dynamic C&C Update Servers

IP\URL: Custom DGA

Updates Static C&C updater URL

Static C&C Update Servers

IP\URL: Hard-coded

Updates C&C IP Address

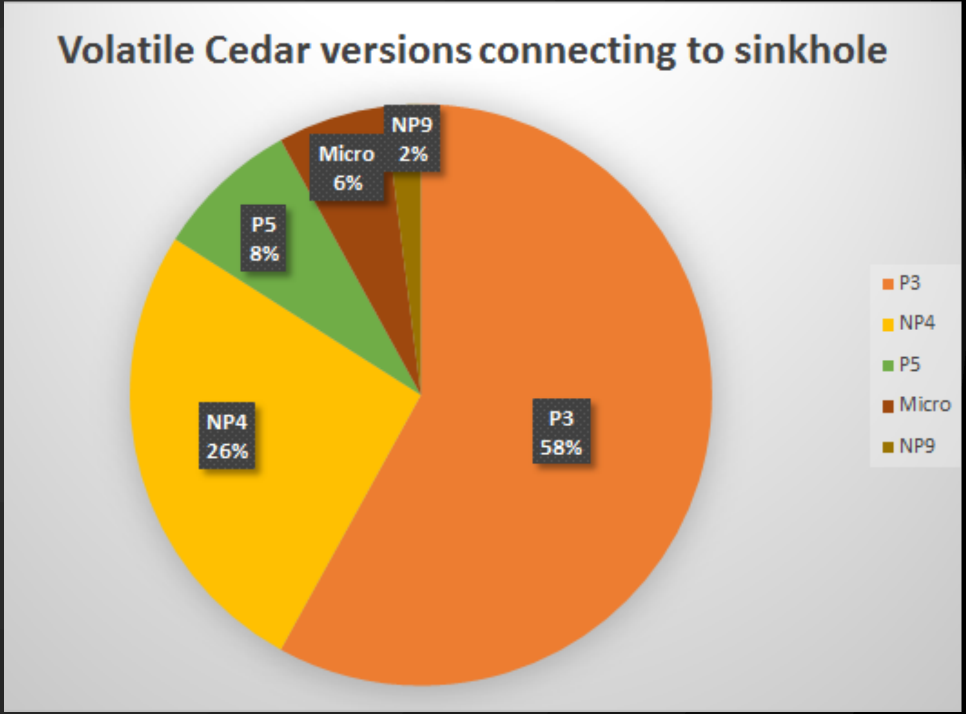
C&C Servers

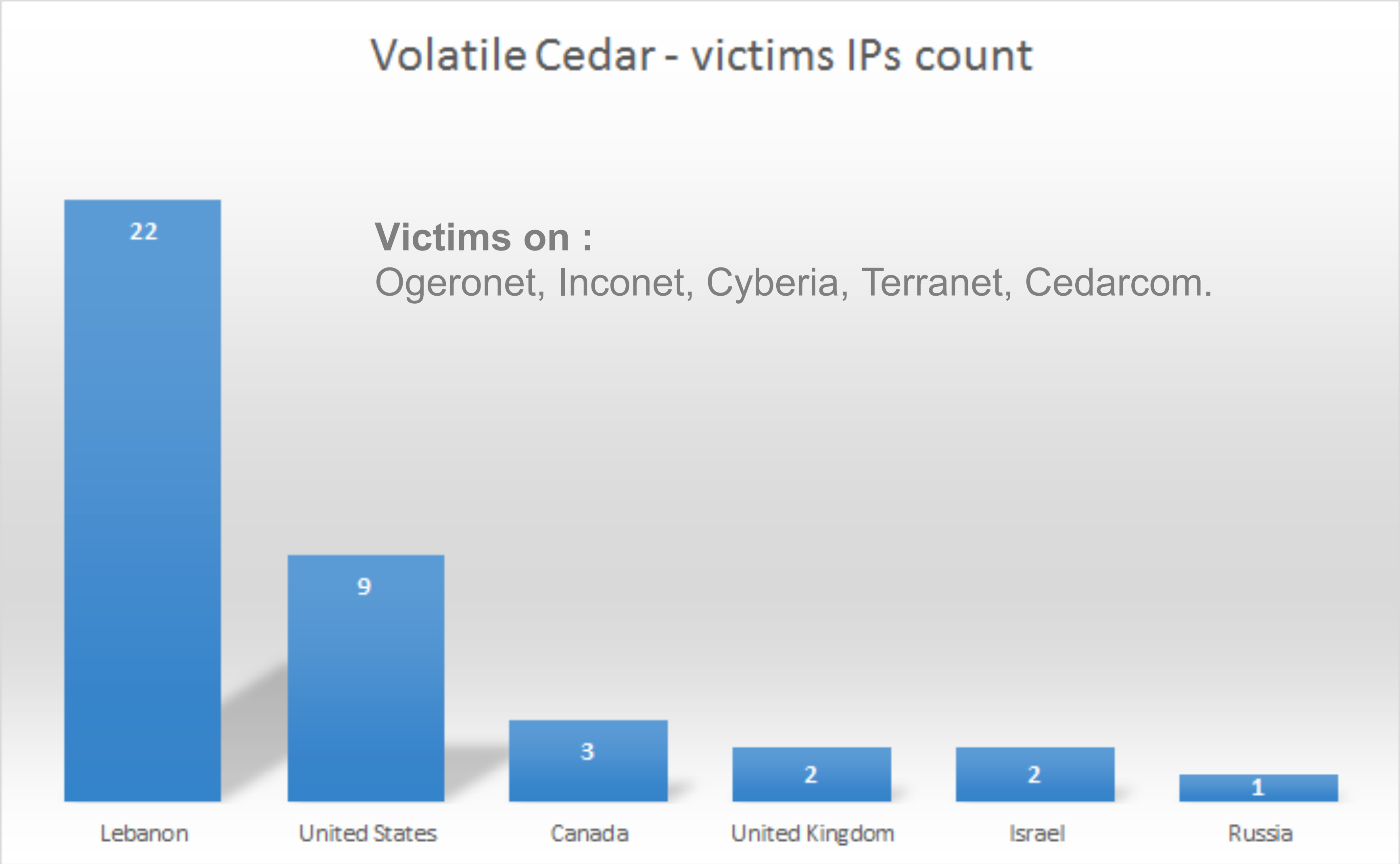
IP\URL: Hard-coded

Send Commands \ Retrieve Data from targets

The victims belong to several categories:

- Government
- Telecom Operators
- Educational Institutions

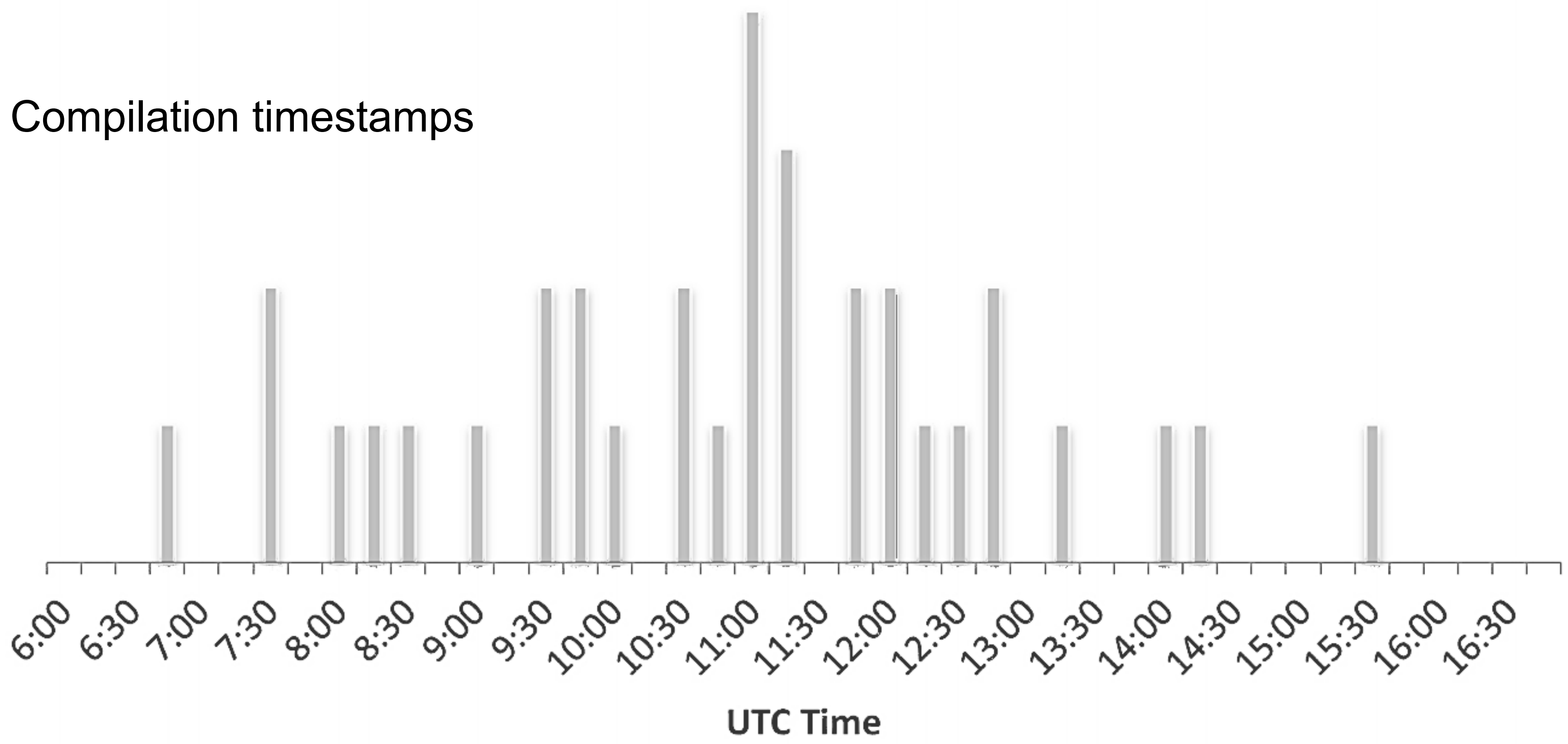




Volatile Cedar - victims IPs count

Victims on :
Ogeronet, Inconet, Cyberia, Terranet, Cedarcom.

Compilation timestamps



GREAT

Importance of **Threat Intelligence**

- Identifying threats
- Localizing threat data
- Learning attackers techniques
- Attack readiness
- Decision making support

Epic submarine battle

GREAT

Stay Close…

Mohamad Amin Hasbini

Senior Security Researcher

Global Research and Analysis Team (GReAT)

Amin.Hasbini@Kaspersky.com

Twitter/Linkedin: @mahasbini

Thank you