Observations on the (Mostly) Inadvertent Effect of Data Management on International Cybercrime Investigations

Don Allison
Director Forensics and Incident Response
KoreLogic
RVASec 2013

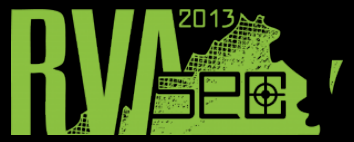
KoreLogic SECURITY

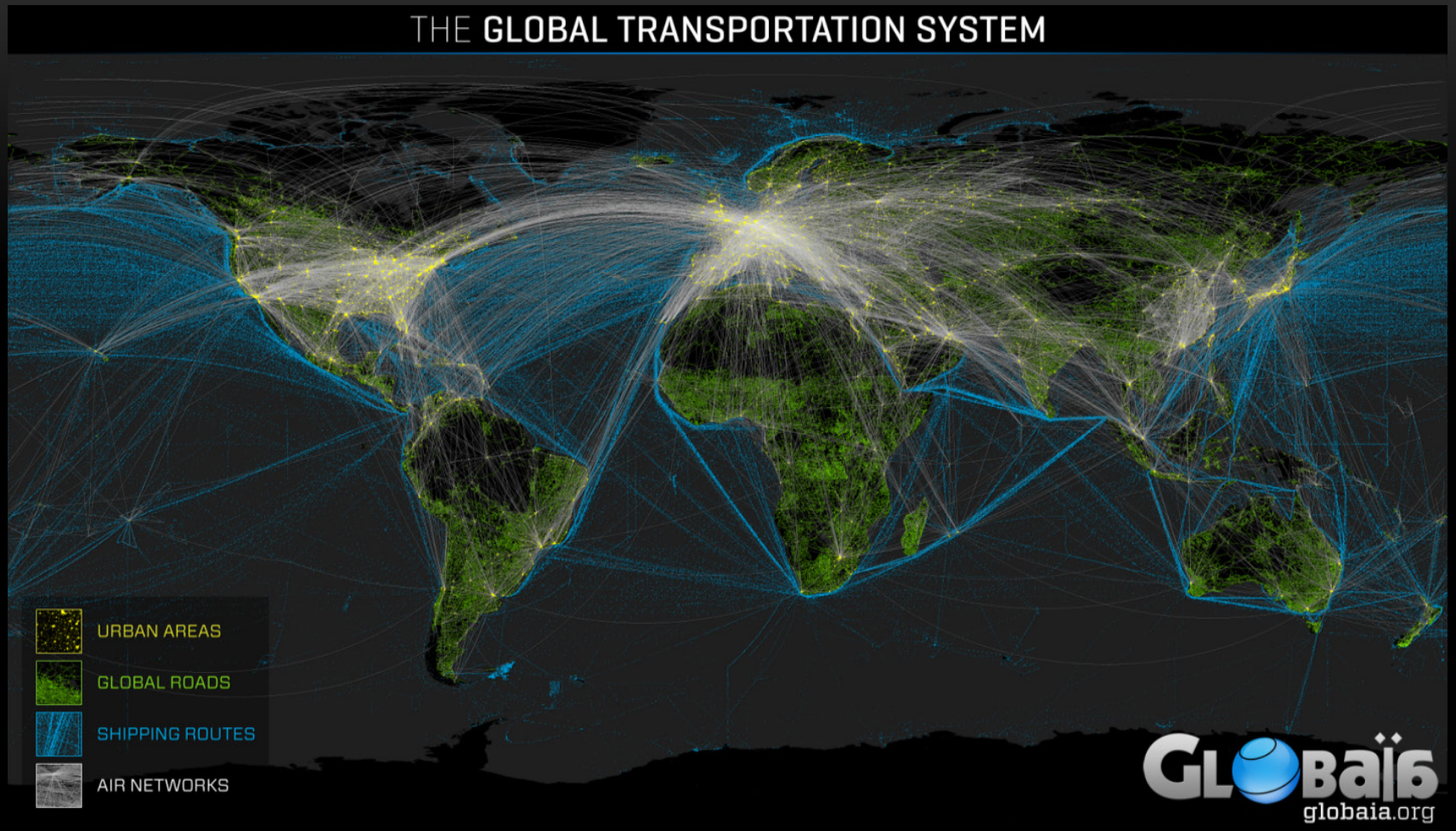
RVASec 2013

DISCLAIMER

- The presentation contents express the viewpoints of the author and are not reviewed for correctness or accuracy by his employer. Any opinions, comments, solutions or other commentary expressed by the presenter are not endorsed or recommended by his employer or any other entity.
- Any resemblance to real persons, living or dead is purely coincidental. Void where prohibited. Some assembly required. Batteries not included. Contents may settle during shipment. Use only as directed. No other warranty expressed or implied. Do not use while operating a motor vehicle or heavy equipment. May be too intense for some viewers. If condition persists, consult your physician. Subject to change without notice. Edited for television. Not responsible for direct, indirect, incidental or consequential damages resulting from any defect, error or failure to perform. Sanitized for your protection. Sign here without admitting guilt. Driver does not carry cash.
- Decision of the judges is final.
- This supersedes all previous notices.

The Internet's Transnational Laws





http://globaia.org/en/anthropocene/gts.jpg

Transportation Routes

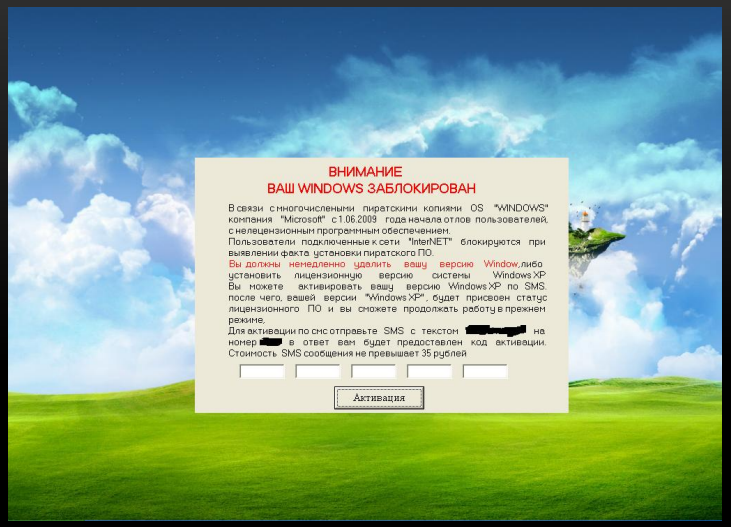
KoreLogic SECURITY

RVASec 2013

Major City Interconnects

KoreLogic SECURITY

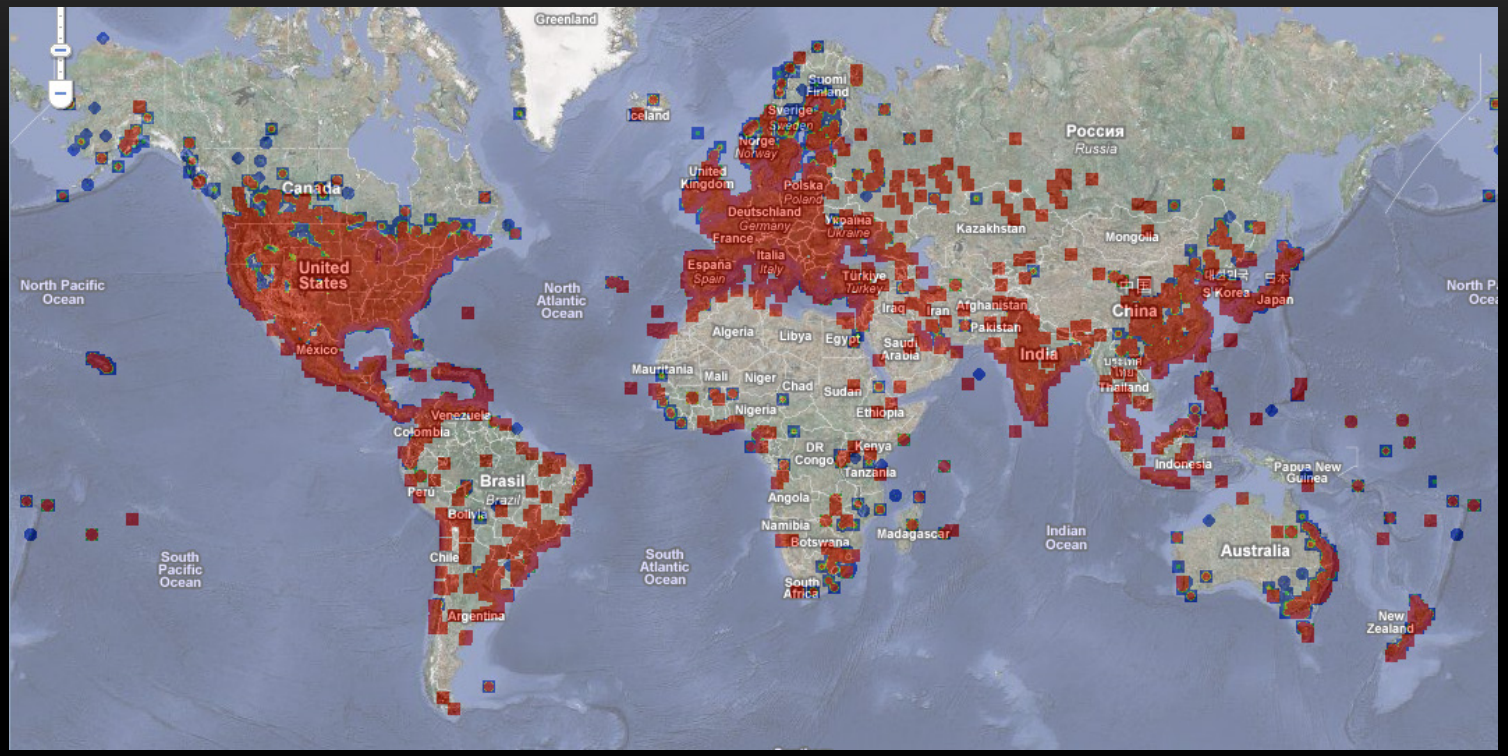
RVASec 2013



KoreLogic SECURITY

Geographically Aware Malware

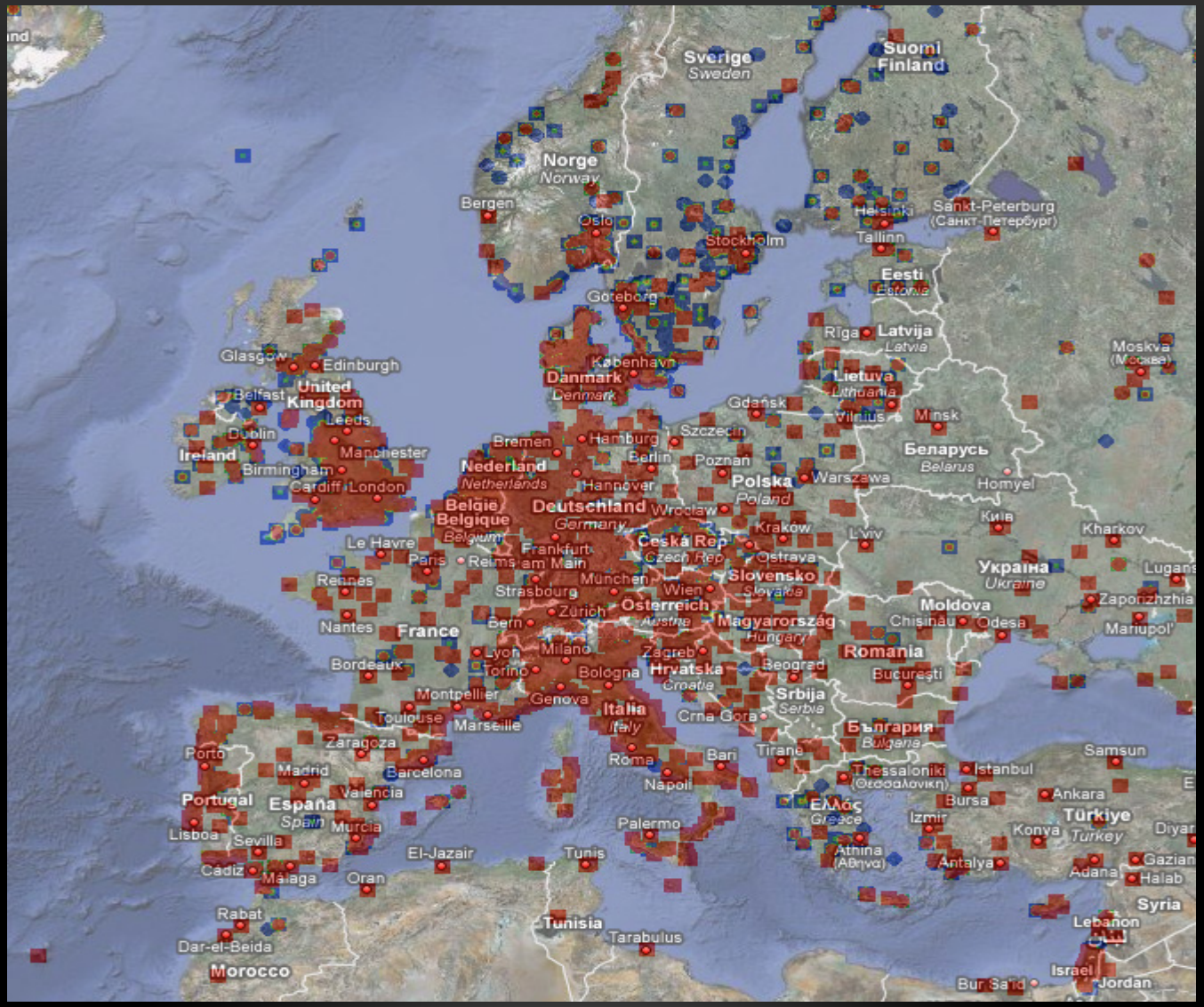
RVA 2013



Conficker

KoreLogic SECURITY

RVAsec 2013


Sverige
Sweden
Suomi
Finland
Norge
Norway
Bergen
Oslo
Stockholm
Helsinki
Sankt-Peterburg
Tallinn
Eesti
Riga
Latvija
Moskva
Glasgow
Edinburgh
København
Danmark
Lietuva
Belfast
United
Kingdom
Gdańsk
Minsk
Leeds
Dublin
Ireland
Manchester
Bremen
Hamburg
Szczecin
Беларусь
Birmingham
Nederland
Berlin
Poznan
Polska
Warszawa
Cardiff
London
Hannover
Homyel
België
Belgique
Deutschland
Wrocław
Kraków
Lviv
Kharkov
Le Havre
Frankfurt
Česká Rep
Ostrava
Україна
Paris
Reims
am Main
Slovensko
Rennes
München
Wien
Strasbourg
Zürich
Österreich
Moldova
Nantes
France
Bern
Magyarország
Chisinau
Odesa
Mariupol'
Lyon
Milano
Zagreb
Romania
Bordeaux
Torino
Bologna
Hrvatska
Beograd
București
Montpellier
Genova
Srbija
Italia
Toulouse
Marseille
Crna Gora
България
Zaragoza
Tirana
Samsun
Porto
Roma
Bari
Madrid
Barcelona
Thessaloniki
Istanbul
Valencia
Napoli
Portugal
España
Bursa
Ankara
Ελλάς
Türkiye
Palermo
Izmir
Lisboa
Sevilla
Murcia
Konya
Tunis
El-Jazair
Athina
Antalya
Cadiz
Málaga
Oran
Adana
Halab
Syria
Rabat
Tunisia
Lebanon
Tarabulus
Dar-el-Beida
Morocco
Israel
Jordan
Bur Said

Conficker

If it ends in .com, .net, .cc, .tv and .name
it's seizable

http://www.ntia.doc.gov/legacy/ntiahome/domainname/agreements/summary-factsheet.htm

Identify the geographic location of the systems that support, process, store, and backup your data

Use of subcontractors and their management of your data (including cloud providers)

Encryption transmission standards (Import - export requirements)

Data breach liability including notification procedures, data security standards, and other technical security measures for each jurisdiction

Litigation hold procedures for each jurisdiction

E-discovery procedures for each jurisdiction

Business continuity/disaster recovery procedures

Provisions in case of dispute (data held hostage)

Onward transfer agreements if 3rd party/cloud providers are changed

Data destruction agreements

Points of contact - including jurisdictional aware counsel

Privacy laws

Blocking statutes

Native language speakers

rackspace 2004 indymedia

Data Concerns

KoreLogic SECURITY

RVAsec 2013

https://commons.wikimedia.org/wiki/File%3AContainerschiff_Hanjin_Chicago.jpg, By Oliver Ohm (Photovision at de.wikipedia) (Own work) [CC-BY-SA-2.0 (www.creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons

KoreLogic SECURITY

The Cloud

RVA 2013

The geographical locations of the cloud provider's servers

The cloud provider's use of subcontractors

Encryption and transmission standards

Data breach liability, including notification procedures

Data security standards, and other technical security measures

Backups, confidentiality provisions, auditing rights, logs, and other related responsibilities

Procedures in the event of a litigation hold and/or discovery request

The cloud company's business continuity plan/disaster recovery procedures

Provisions in the event of a dispute with the cloud company (so that data cannot be held hostage)

Onward transfer agreements (in the event that the business migrates cloud providers)

If the topic of APTs gets information security to be addressed at the highest levels of an organization it may still be a useful topic.

There are many other threats that are out there and the APT is not the only threat that spends a fair amount of time in your computer systems and takes your data.

You are more likely to encounter losses from internal and legal problems than to lose significant data to an APT.

What you call hacking may be a legitimate business in its jurisdiction

Despite some wonderful minds and great products, there still is no promise of data security on the Internet.

The OFF button is the only technology answer to date; however, it seems to have a few unwanted limitations

One solution is available to help protect a company's data and impact an investigation

Data Management

Change your mindset and change your culture

Security is a process - not a technology

You are in an all out business war for your data - accept it

Must identify the truly important data - everything else is cat videos

Get help with legal requirements for retention and other concerns

Plan storage and backup space accordingly

Make non-essential data and systems resilient - be willing to lose non-essential data

Get control of your data – it is not where you think it is

Classify it

Plan and map out where each level of classified data should reside – use jurisdictions to your advantage

Define who should have access to each level of data - monitor those people (especially C-level and domain admin)

Tie security to individual responsibility - have consequences for incidents

CLASSIFICATION

OWNERSHIP

Attribution

Critical Data

KoreLogic SECURITY

RVAsec 2013

Data Management in an Investigation

- Questions?
- Comments?
- Tell the Geek to go home?
- You may cross examine the witness…