Safeguarding The Internet

Agustín Speziale
Product Manager
LATAM
Level 3

Safeguarding The Internet

Razones para realizar esta presentación:

Dar a conocer el Laboratorio.

Comentar los objetivos.

Realizar un repaso del proyecto.

Mencionar las herramientas y técnicas utilizadas.

Motivar la replicación de esta idea en otras organizaciones.

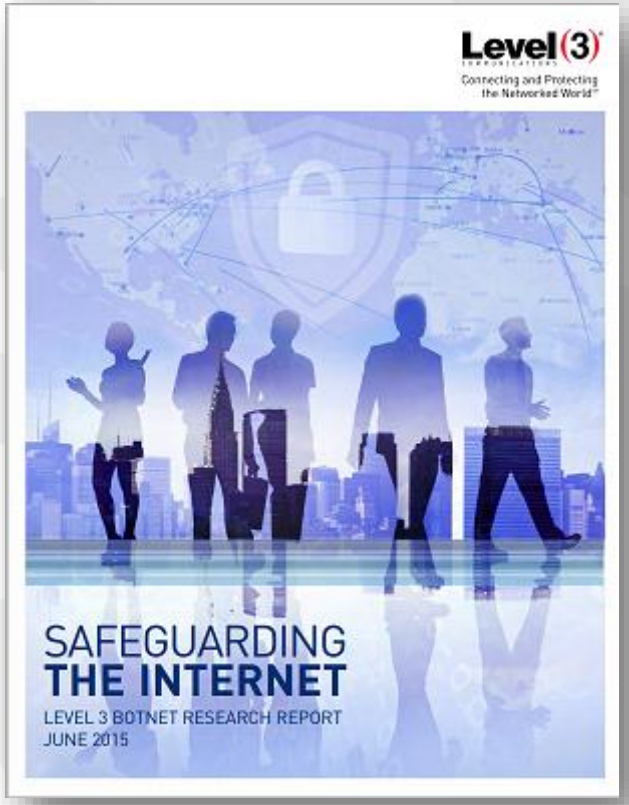
Compartir las conclusiones.

Compartir el informe.

Motivar la colaboración con otras organizaciones.

Safeguarding The Internet

Reporte Junio 2015



Safeguarding: término utilizado para denotar las medidas para proteger la salud, el bienestar y los derechos humanos de las personas, que permiten a la gente a vivir **libres** de opresiones de terceros.

***Botnet Research Report*:**
Actionable threat intelligence to safeguard our customers and the Internet

Escenario Contemporáneo de la Cyberseguridad

Las amenazas sobre Internet van modificándose en su forma, complejidad, volumen y tiempos

Aprox. 8% de los dispositivos móviles han sido infectados por algún malware.
Source: McAfee Labs Threat Report Q1 2015

Alrededor de 1,800 nuevas familias de virus fueron detectadas durante el año pasado.
Source: Fortinet Threat Landscape Report 2014

Han aumentado las amenazas a los núcleos de los sistemas: NTP, Heartbleed, Winshock, Shellshock
Source: McAfee Labs Threat Report Q1 February 2015

$3.5M El promedio global del costo en las empresas por violaciones a sus datos aprox un 15% mas del costo en 2013
Source: Ponemon 2014 Cost of Data Breach Study: Global Analysis

160K nuevos prototipos de malware liberados todos los días.
Source: Panda Quarterly Report, 2014

Los accesos a Internet en países emergentes crecen al doble que el promedio

Al final de 2014 la cantidad de usuarios de Internet a nivel mundial ha llegado a casi **3 mil millones**.

Esto corresponde a una penetración del **40% globalmente** hablando.

Dos-tercios del universo de usuarios de Internet pertenecen a los países emergentes

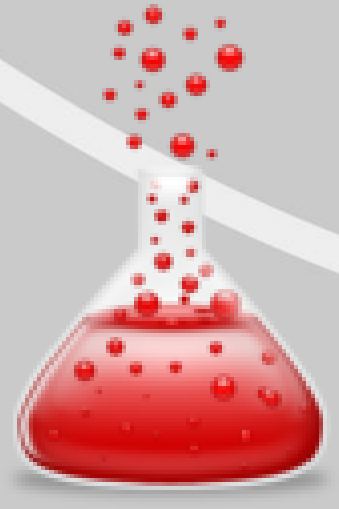
90% Mas del 90 por ciento de las personas que no están utilizando **Internet** pertenecen al países emergentes.

Source: The World in 2014: ICT Facts and Figures, International Telecommunications Union, 2014

Source link: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

lacnic24
lacnog
28/9 - 2/10
bogotá, colombia

Sobre el Lab



Safeguarding The Internet

Ante el escenario actual:

Debemos contar con un laboratorio específico.

Creado en 2010

Su mayor crecimiento durante 2014

"*Las compañías de telecomunicaciones son un forma rápida de mitigar el riesgo de amenazas de Internet*"
Level 3 Reseach Lab

Safeguarding The Internet

Objetivos:

Encontrar las amenazas ocultas.

Permitir a otras áreas tomar acciones.
Comunicarlas a los clientes, cuando aplique.
Ofrecer mejores prácticas para proteger información.

Estrategia actual:

Utilizar herramientas Open Source (facilitar replicación)

Basados en:

Data Analisys
Machine Learning
Algoritmos de big data.


115 Tera (aprox)


No es Big Data

Herramientas Open Source

Scala Documentation API Learn Quickref Contribute SIPs/SLIPs Search

Tutorials

New to Scala?

Tutorials geared for people coming...

- ...from Java AVAILABLE
- ...from Ruby IN PROGRESS
- ...from Python IN PROGRESS

FAQ

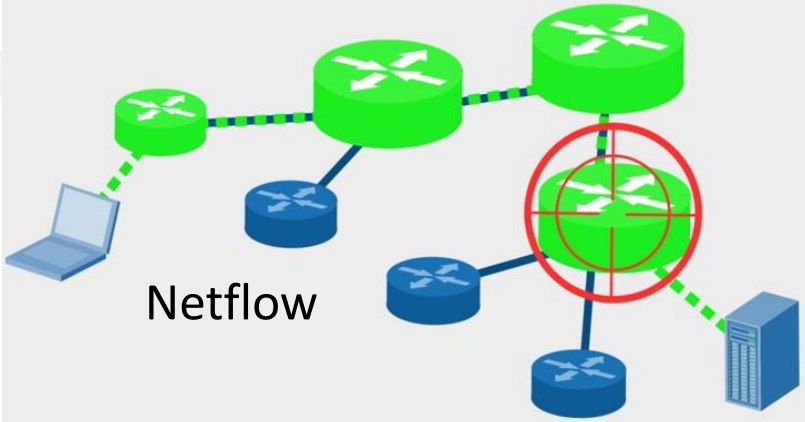
Frequently Asked Questions (and their answers!)

- How do I find what some symbol means or does?
- How does yield work?
- What are Scala context and view bounds?
- What is the difference between view, stream and iterator?
- What is breakOut, and how does it work?
- How can I chain/nest implicit conversions?
- Where does Scala look for implicits?

A Tour of Scala

Bite-size pieces of the essentials...

- Introduction
- Unified Types
- Classes
- Traits
- Mixin Class Composition
- Anonymous Function Syntax
- Higher-order Functions
- Nested Functions
- Currying
- Case Classes
- Pattern Matching
- Singleton Objects
- XML Processing
- Regular Expression Patterns
- Extractor Objects
- Sequence Comprehensions
- Generic Classes
- Variances
- Upper Type Bounds



Spark *Lightning-fast cluster computing*

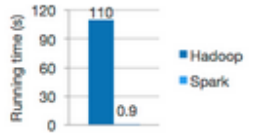
Download Libraries Documentation Examples Community FAQ

Apache Spark™ is a fast and general engine for large-scale data processing.

Speed

Run programs up to 100x faster than Hadoop MapReduce in memory, or 10x faster on disk.

Spark has an advanced DAG execution engine that supports cyclic data flow and in-memory computing.



Logistic regression in Hadoop and Spark

Ease of Use

Write applications quickly in Java, Scala, Python, R.

Spark offers over 80 high-level operators that make it easy to build parallel apps. And you can use it *interactively* from the Scala, Python and R shells.

```
text_file = spark.textFile("hdfs://...")

text_file.flatMap(lambda line: line.split())
    .map(lambda word: (word, 1))
    .reduceByKey(lambda a, b: a+b)
```

Word count in Spark's Python API

Generality

Combine SQL, streaming, and complex analytics.

Spark powers a stack of libraries including SQL and DataFrames, MLlib for machine learning, GraphX, and Spark Streaming. You can combine these libraries seamlessly in the same application.

Runs Everywhere

Spark runs on Hadoop, Mesos, standalone, or in the cloud. It can access diverse data sources including HDFS, Cassandra, HBase, and S3.

You can run Spark using its standalone cluster mode, on EC2, on Hadoop YARN, or on Apache Mesos. Access data in HDFS, Cassandra, HBase, Hive, Tachyon, and any Hadoop data source.

Mas de 10 herramientas

Safeguarding The Internet

Elementos, Algoritmos y Herramientas

Elementos:
Datos
Programación & Sistemas
Algoritmos
Probabilidad y Estadísticas

Herramientas de Big Data:
Shark, **Spark**, Storm, **Hive**, **Cloudera** ,
ML/Oryx, Mahout, Pig, Sqoop, **Oozie**,
HBase, Zookeeper, **Impala**, Graph x

Safeguarding The Internet

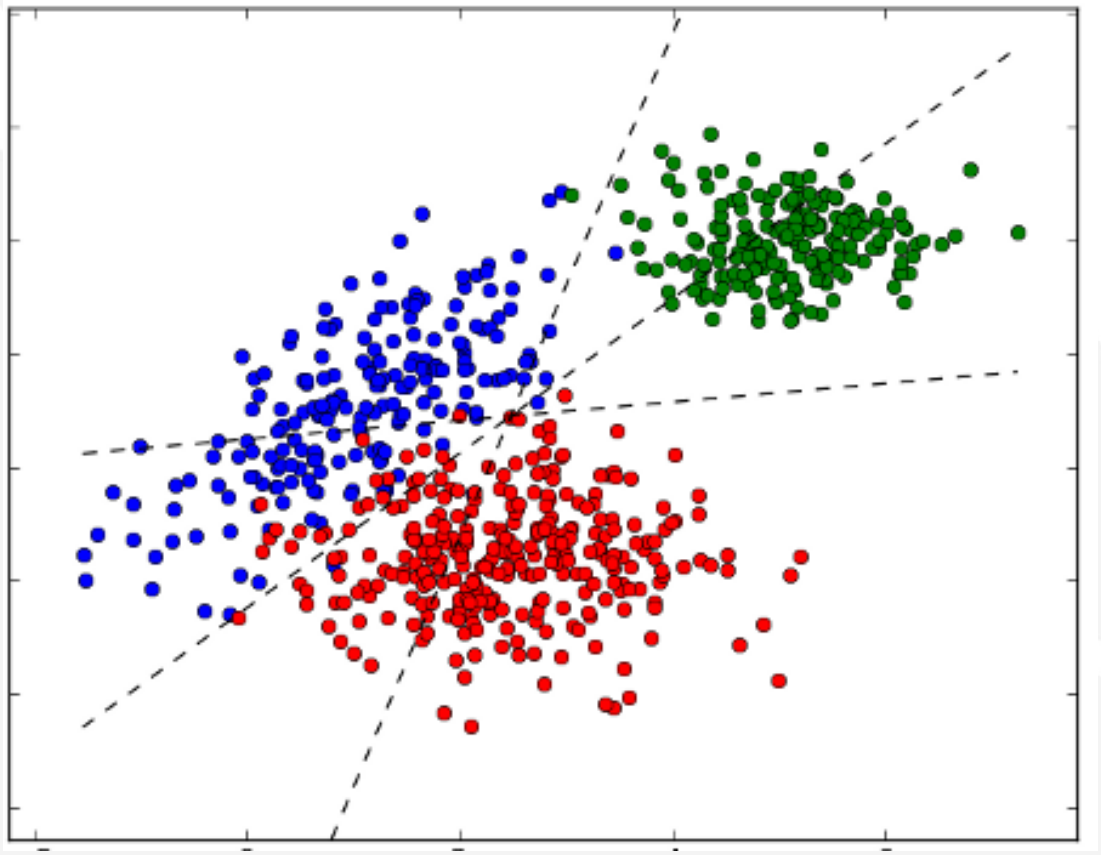
Herramientas y Técnicas

Machine Learning:

Puertos

ML Lib (Spark)

Clusters



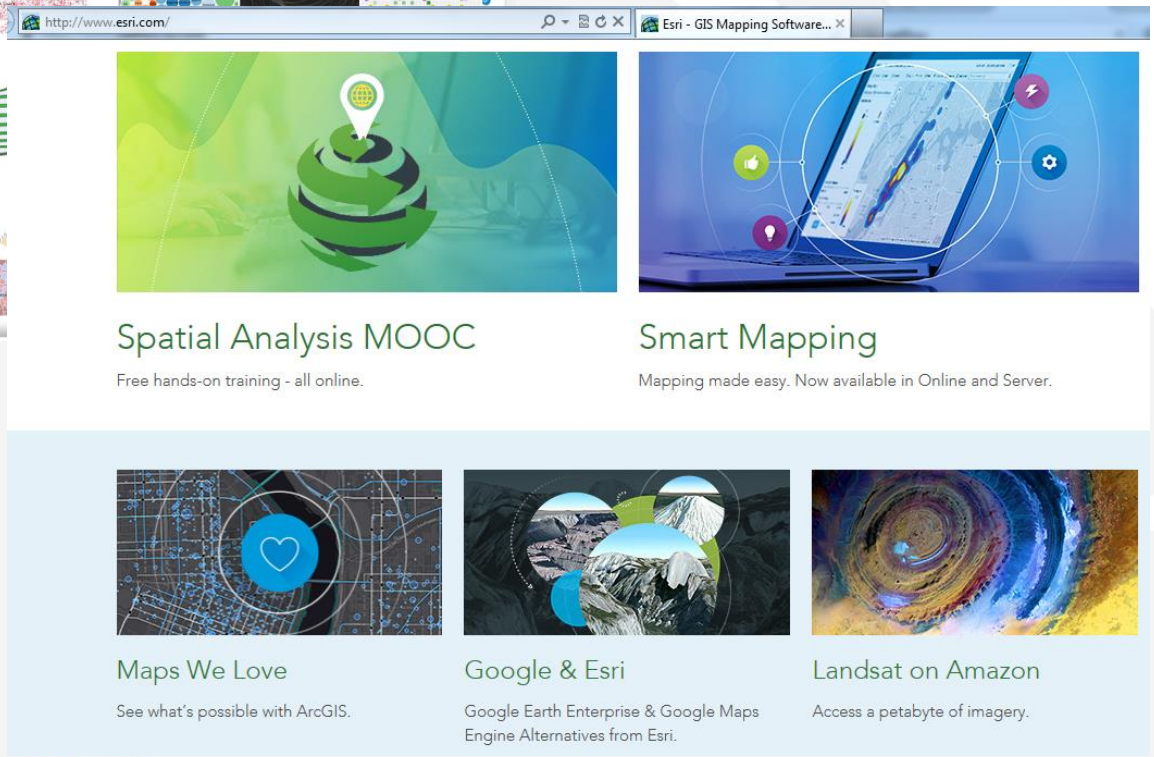
Safeguarding The Internet

Herramientas y Técnicas

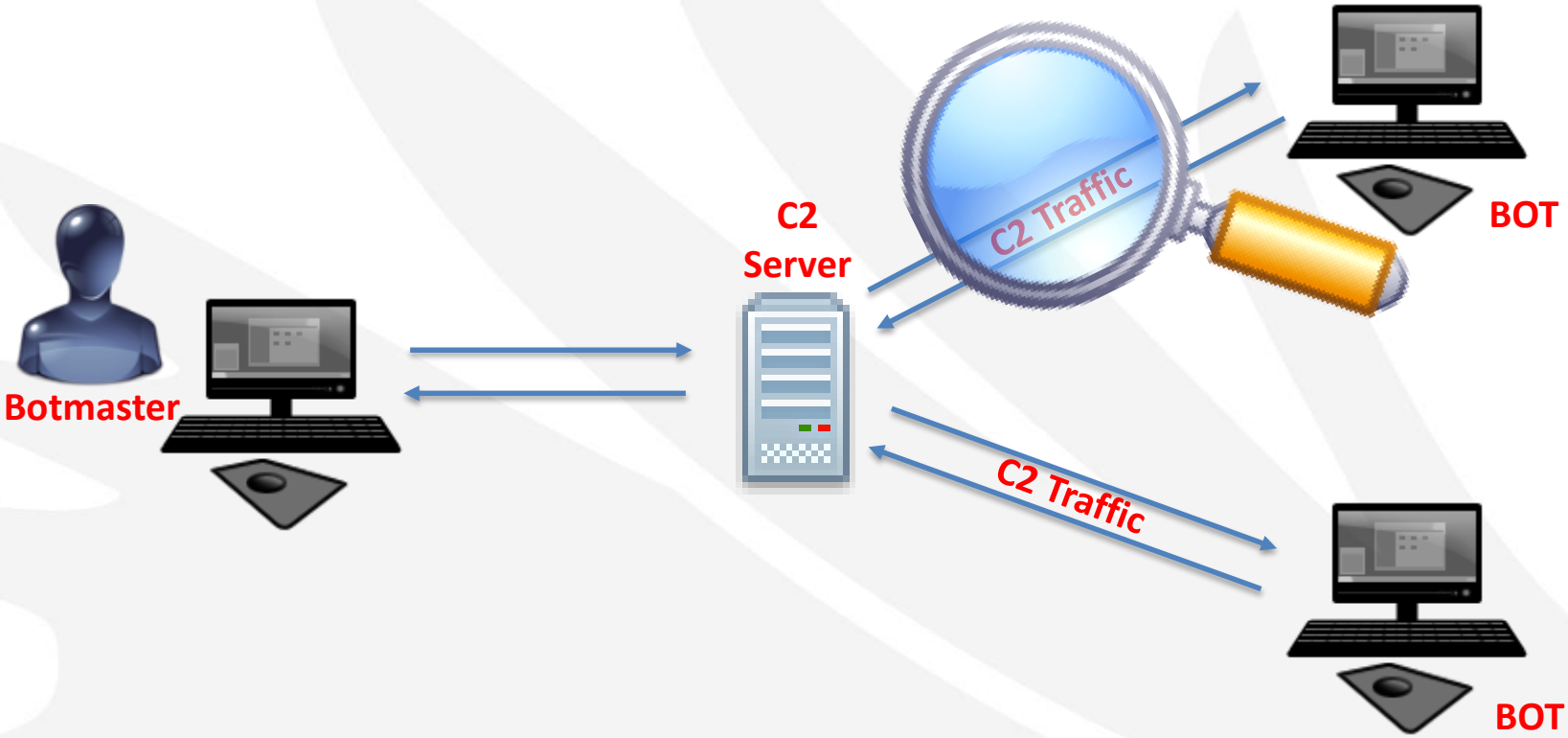
Data Análisis + Visualización:

http://d3js.org/

http://www.esri.com/



Control and Command "C2"



45 mil millones de sesiones de NetFlow por día

Se identifica, y remueve, en promedio una red de servidores de C2 por día

Safeguarding The Internet

Level 3 Threat Research Labs
Email de contacto: level3threatlabs@level3.com

Sugerencia:

Incluir en el subject: [LACNOG]

Recomendaciones

Clasificación de los Datos: Activos de la Organización

1 **Comprender el valor, ubicación y accesos a los datos de valor**

- Salud
- Documentos legales
- Financiera
- Marketing
- Datos de las tarjetas
- Titulares / Blogs

Evaluar sus Aplicaciones

2 **Comprender sus aplicaciones, su seguridad y los datos que controlan o acceden.**

- Procesamiento de Pagos
- ERP
- E-Commerce
- CRM
- Test and Develop

Infraestructura IT

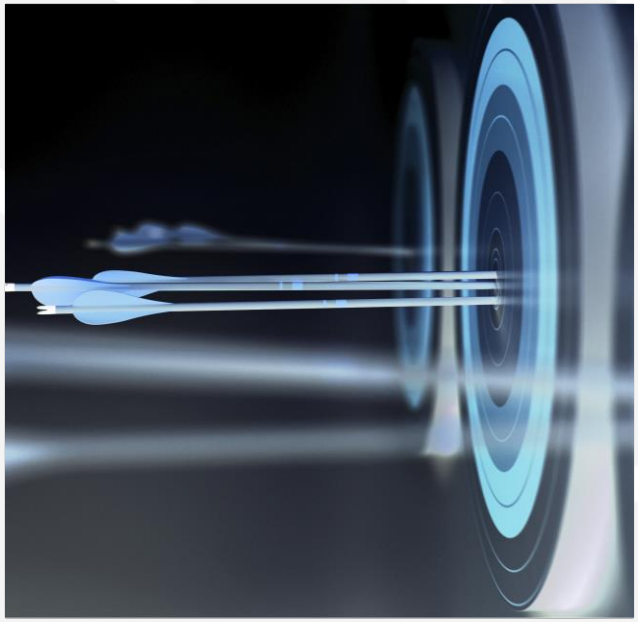
3 Auditar su arquitectura

- Foco en simplicidad
- Complejidad es un riesgo
- Segmentación
- APIs
- Orchestration
- Storage y Backup
- Controles de Acceso

Aceptar este estado como “Normal”

4 Comprender que sus datos pueden estar bajo amenaza.

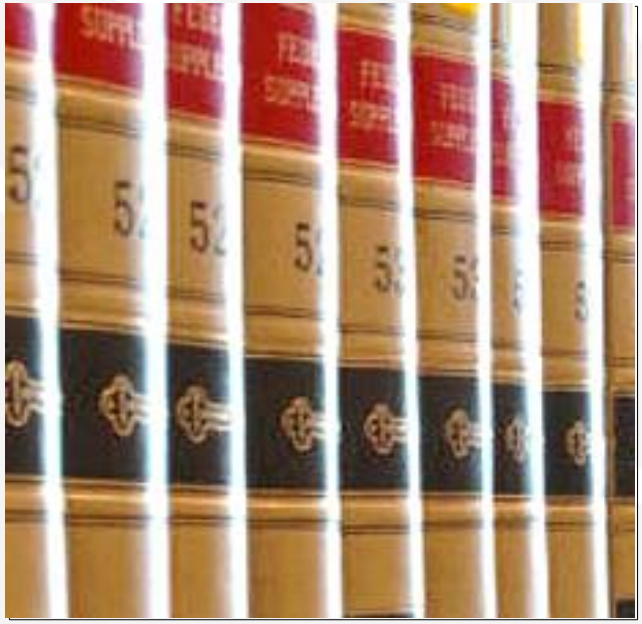
- **Amenzas**
  - Internas
  - Externas
  - Físicas
- **Objetivos**
  - Acciones Proactivas.
  - Anuncios públicos, contratos y otros datos públicos.
  - Naturaleza de su organización, cultura y negocios.



Gobernanza y Riesgo

5 Temer a la amenaza externa, no al auditor

- Mirar mas allá de las reglas y estándares.
- Desarrollar un enfoque basado en riesgos para la gestión de amenazas y vulnerabilidades
- Establecer y adherirse a un gobierno, riesgo y cumplimiento marco

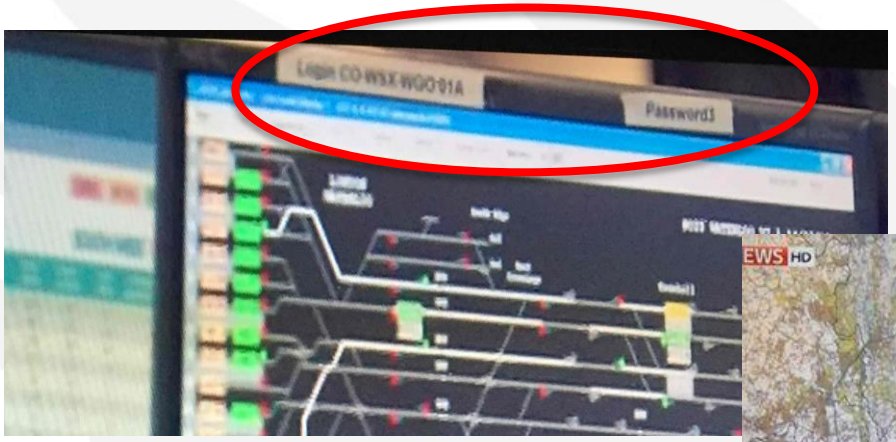


Colaboración

6 Colaborar con Service Providers y Peers

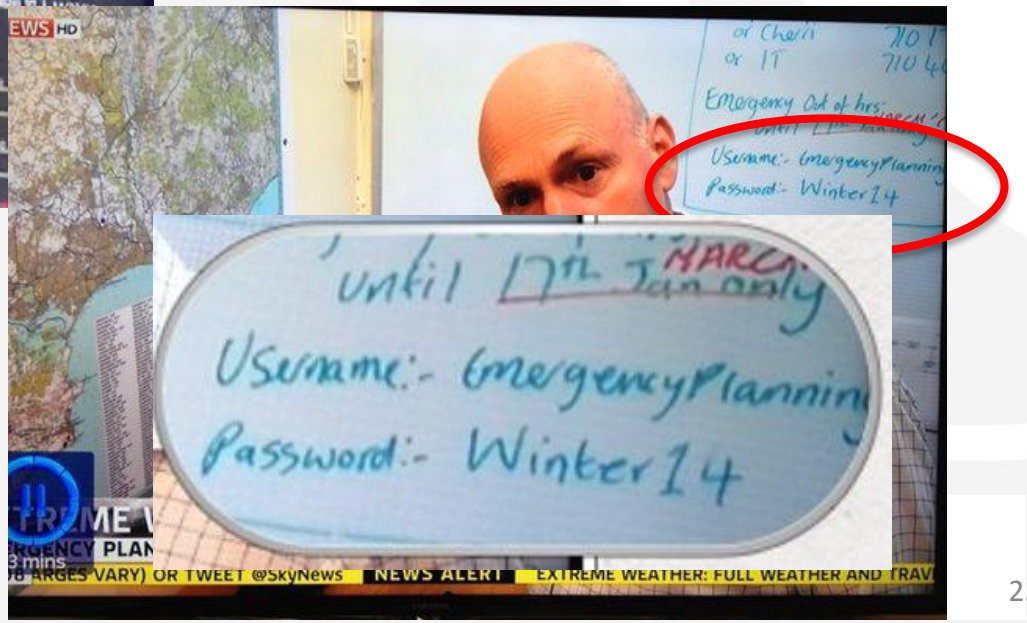
- Algunos controles se relacionan mejor con proveedores de servicios (redes, cloud, threat intelligence, etc.)
- La colaboración con peers es vital.
- Aprovechar los recursos: estándares , programas, eventos, consorcios, etc.

Mejores Prácticas
Ejemplo: Casos muy públicos, lapsus no técnológicos



◄ **Estación de control de trenes**

Alertas meteorológicas ►



Estadísticas

10 PRINCIPALES PAÍSES QUE GENERAN TRÁFICO DE C2 MUNDIALMENTE

1. Estados Unidos
2. Ucrania
3. Rusia
4. Holanda
5. Alemania
6. Turquía
7. Francia
8. Reino Unido
9. Vietnam
10. Rumania

Fuente: Level 3SN Threat Research Labs, 1º trimestre de 2015

4 PRINCIPALES PAÍSES QUE GENERAN TRÁFICO DE C2 EN AMÉRICA LATINA

1. Panamá
2. Argentina
3. Brasil
4. México

Fuente: Level 3[SN] Threat Research Labs, 1º trimestre de 2015

10 PRINCIPALES PAÍSES EN AMÉRICA LATINA QUE SE COMUNICAN CON C2s

1. Brasil

2. Argentina

3. México

4. Venezuela

5. Equador

6. Colombia

7. Chile

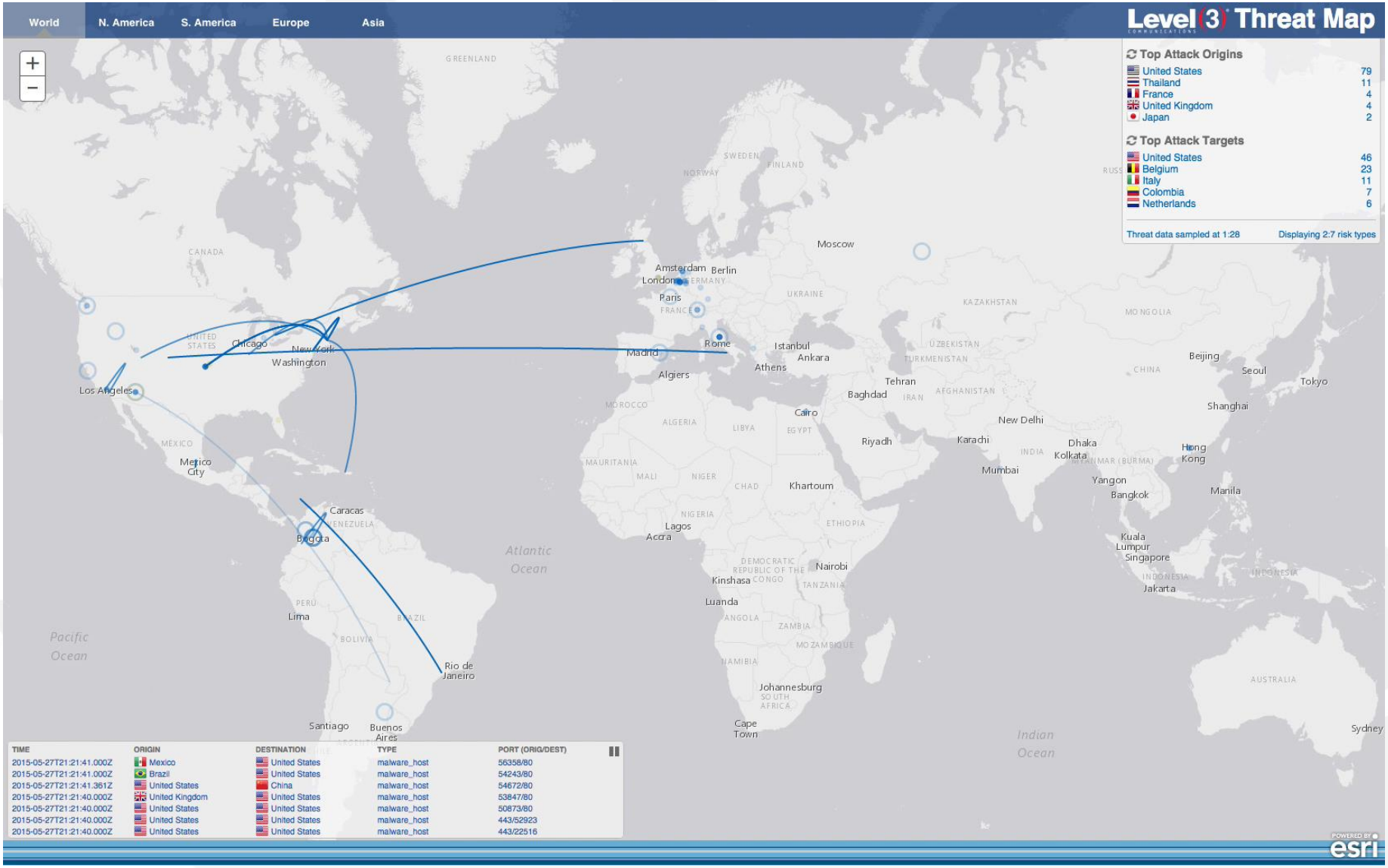
8. Perú

9. Costa Rica

10. Bolivia

Fuente: Level 3[SN] Threat Research Labs, 1º trimestre de 2015

Visualización de los orígenes y objetivos



Threat Intelligence View

Click image to watch video

Visit: http://threatmap/ image for live feed available via Level 3 VPN only.

¡Muchas Gracias!

Referencias:

http://www.level3.com/~/media/files/white-paper/en_secur_wp_botnetresearchreport.ashx
http://www.dc.uba.ar/events/eci/2014/cursos
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf
http://www.fortinet.com/sites/default/files/whitepapers/Threat-Landscape-2014.pdf
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf
http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-a
http://www.pandasecurity.com/mediacenter/press-releases/malware-still-generated-rate-160
https://software.intel.com/sites/default/files/article/402274/etl-big-data-with-hadoop.pdf
https://spark.apache.org/
http://www.scala-lang.org/
https://github.com/eraclitux/machine-learning-netflow/blob/master/machinelearning-netflow
http://research.ijcaonline.org/volume36/number2/pxc3976258.pdf
http://d3js.org/
http://blog.level3.com/security/
http://personals.ac.upc.edu/pbarlet/reports/netflow_classification-techrep.pdf
http://www.esri.com/
http://grigory.us/big-data.html
http://lintool.github.io/MapReduceAlgorithms/MapReduce-book-final.pdf
http://francistseng.com/