Retos que surgen con Big Data para el manejo y protección de información

Augusto Pecho; Felipe Moreno

Universidad Nacional de Ingeniería

December 13, 2015

Overview

Introducción

Utilizar grandes cantidades de datos para gestionar las amenazas de seguridad debido a la magnitud de datos de la Internet y el hecho de que la población mundial está en aumento de forma constante, requiere proteger a los usuarios de la ciberdelincuencia que se puede ver como un juego de números.

Herramientas de análisis de datos grandes serán la primera línea de defensa para proporcionar programas integrales e integrados de predicción de amenaza a la seguridad, detección y disuasión y prevención.

El director gerente de FBR Capital Markets y Analista Senior de Investigación, Daniel Ives, dijo: "El mercado de esas herramientas de software podría ser de $ 15 mil millones a $ 20 mil millones durante los próximos tres años".

Vendedores que aprovechan el Big Data Analytics

- IBM: Análisis de Seguridad
- Splunk: Seguridad y Fraude
- Actividad Inversora
  - Sqrrl
  - Endgame
  - DB Networks
  - Rapid7
- Nuevos ingresantes
  - Hortonworks
  - SAS Institute

Big Data: Las 3 Vs

Volumen

El aumento de cantidades de información trae consigo un incremento en la cantidad de amenazas contra esa información.

Variedad

Se crean nuevos métodos para realizar la ciberdelincuencia, los mismos ciberdelincuentes ponen a prueba sus malware para ver que funcionen sin ser detectados.

Velocidad

Ciberdelincuentes pueden transformar sitios legítimos en sitios corruptos a una velocidad increíble. Cada vez resulta más difícil rastrear debido al constante movimiento de información que se lleva a cabo en la red mundial.

Metadata

En el mundo se ha estado impulsando una iniciativa de datos abiertos para mover a los gobiernos a ser un administrador de datos.

El objetivo en la liberación de los datos es la de servir mejor al público y promover el crecimiento económico a través de su reutilización.

Los Metadatos adecuados aumentan las posibilidades de que los conjuntos de datos sean reutilizados correctamente.

Se requiere de un historial para conocer de dónde y a dónde van los datos.

Perfiles de amenazas (i)

Tipos

1. Malware
2. Pishing
3. Hacking
4. Spam
5. Espionaje cibernético
6. Amenazas internas
7. Errores humanos

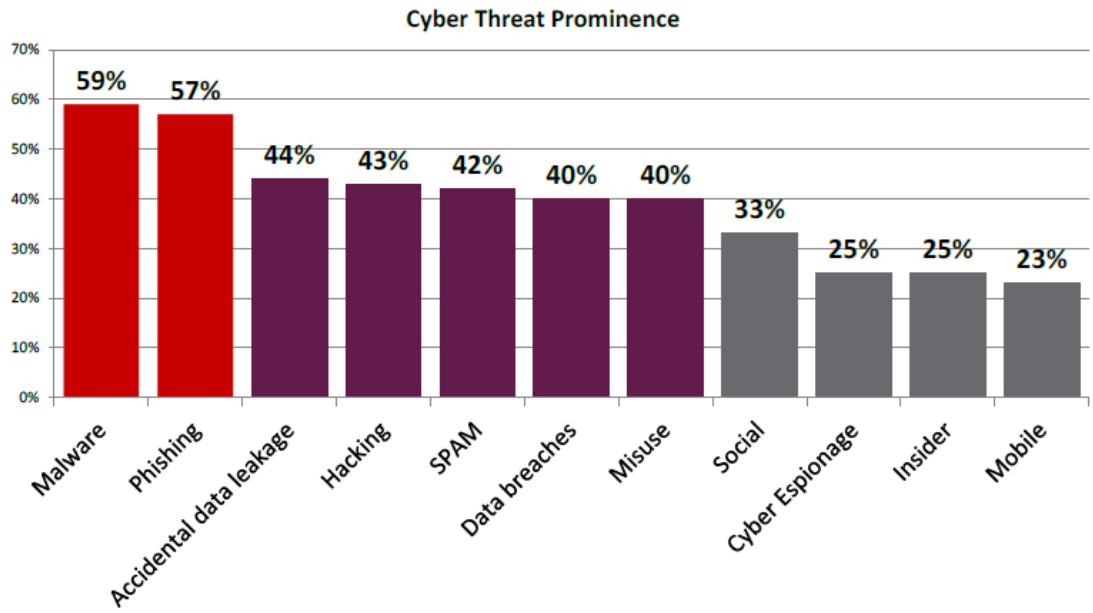

Figure : Proporción de cyber ataques

Perfiles de amenazas (ii)

Las amenazas móviles son el vector emergente. Sólo el 44% de todos los participantes en el estudio creen que están bien preparados, mientras que el 47% dice que son algo preparados. Esta es la categoría de amenaza con el porcentaje más bajo de preparación combinada, y refleja la rapidez con que la informática móvil está superando los mecanismos de seguridad establecidos, técnicas y educación.

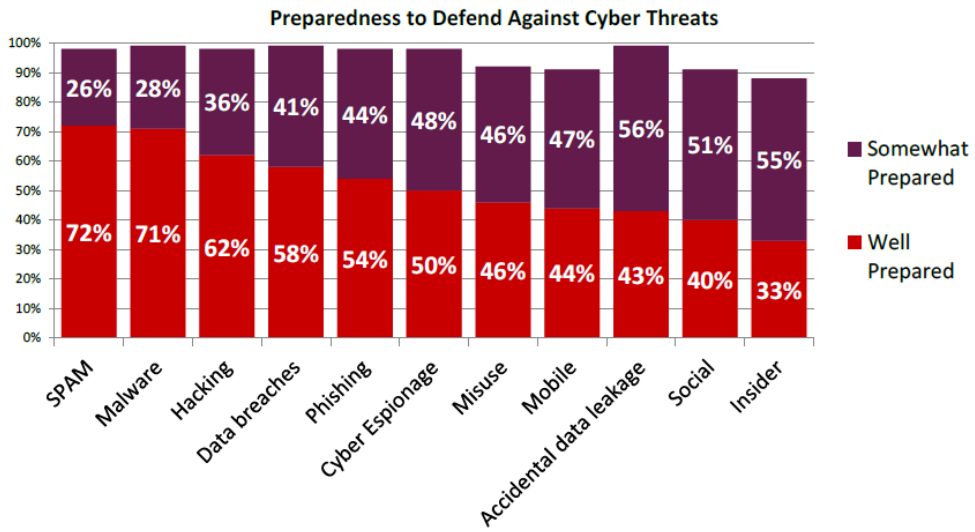

Figure : Preparación para defenderse ante cyber ataques

Ejemplo de aplicaciones en Big Data

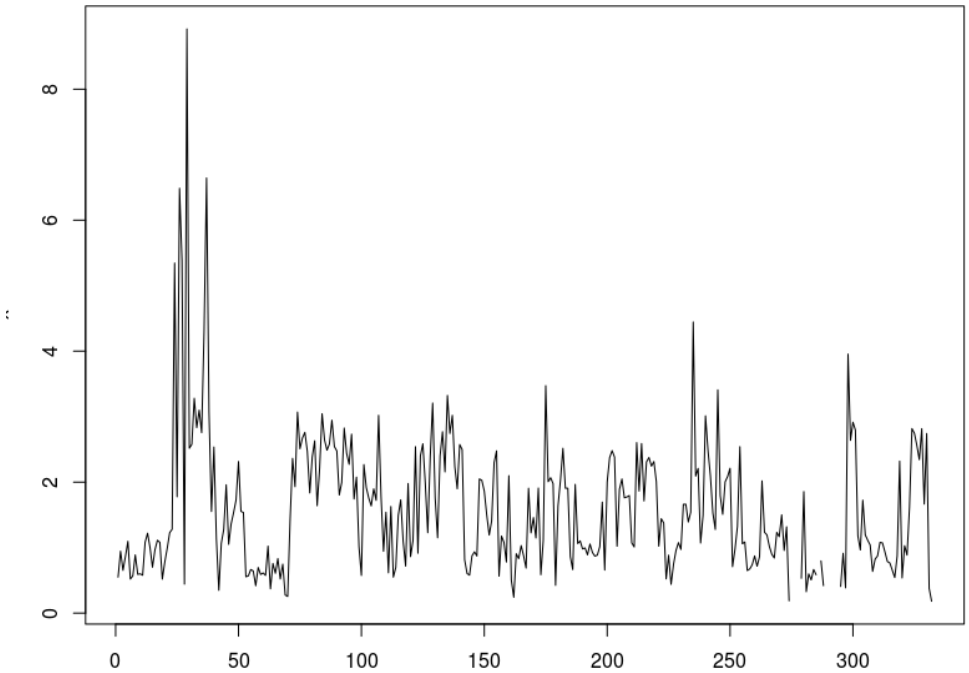

Figure : Variación de concentración de nitrato

Ejemplo de aplicaciones en Big Data

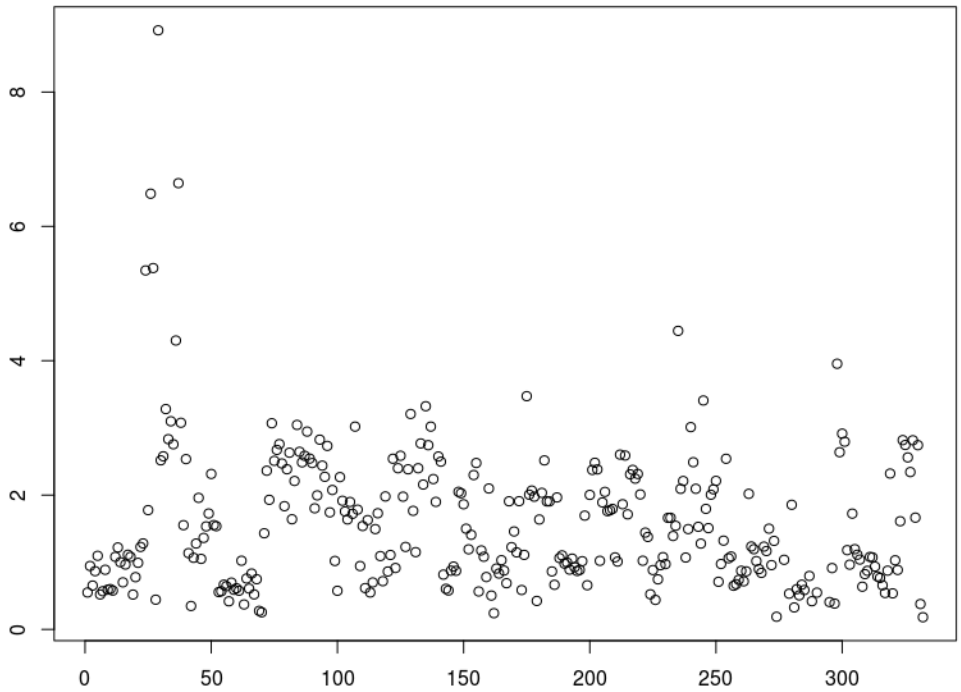

Figure : Variación de concentración de sulfato

References

- Obrst, L., Chase, P., Markeloff, R., Developing an Ontology of the Cyber-security Domain, Semantic Technology for Intelligence, Defense and Security (STIDS) 2012, GMU, Fairfax, VA, 2012
- Big data: The next frontier for innovation, competition, and productivity. James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers. McKinsey Global Institute. May 2011.
- Using Data for Systemic Financial Risk Management. Mark Flood, H V Jagadish, Albert Kyle, Frank Olken, and Louiqa Raschid. Proc. Fifth Biennial Conf. Innovative Data Systems Research, Jan. 2011.
- LM Cyber Security and Transformational Technologies Keeping Systems and Data Safe.
- Big Data Analytics for Security Intelligence 2013 Cloud Security Alliance – All Rights Reserved.
- CV: Capital de riesgo; `https://es.wikipedia.org/wiki/Capital_riesgo`
- Cybersecurity is the killer app for big data analytics by Steve Morgan `http://www.csoonline.com/article/2942083/big-data-security/cybersecurity-is-the-killer-app-for-big-data-analytics.html`

The End