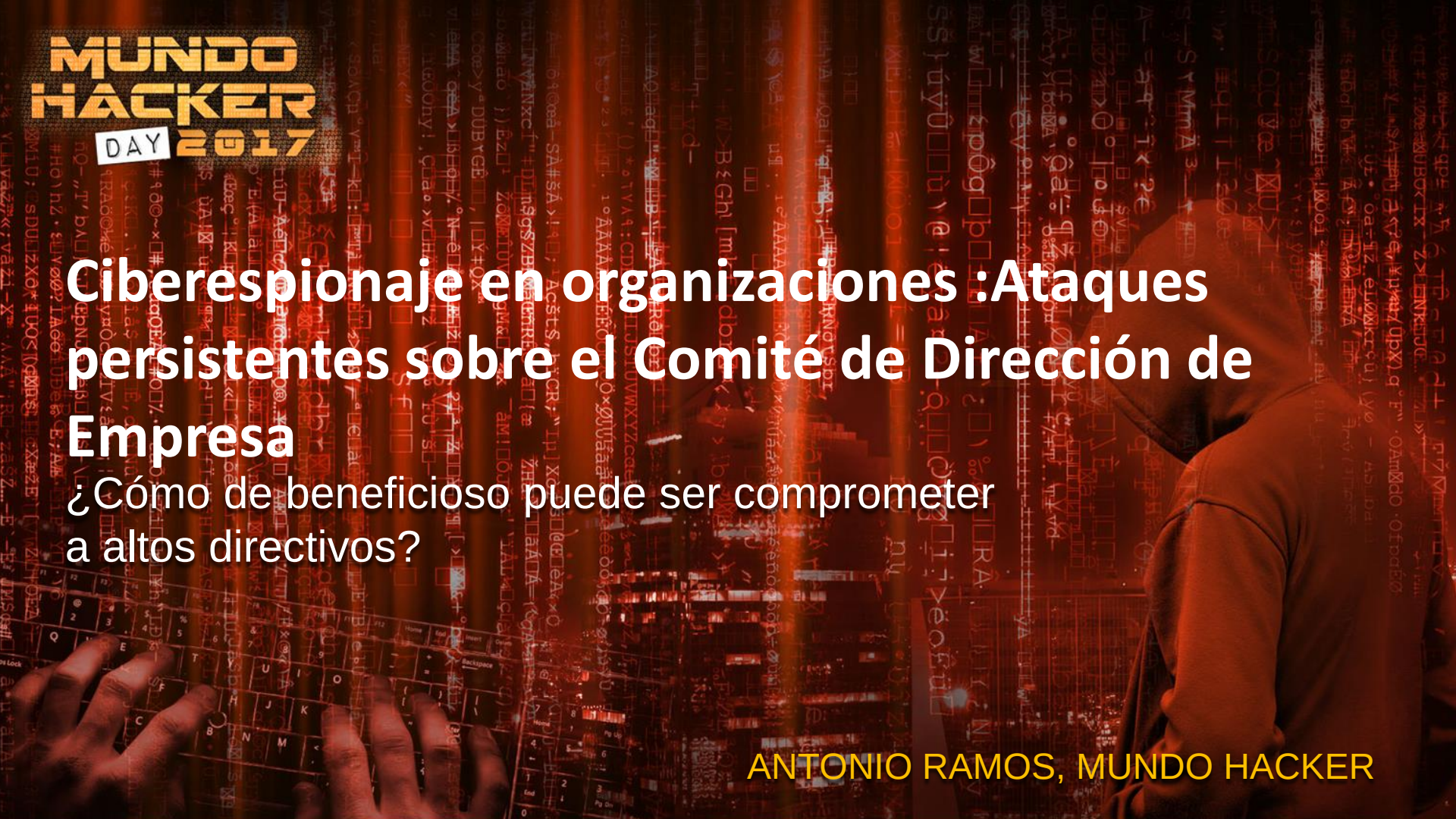


Ciberespionaje en organizaciones :Ataques persistentes sobre el Comité de Dirección de Empresa

¿Cómo de beneficioso puede ser comprometer a altos directivos?

ANTONIO RAMOS, MUNDO HACKER

¿Qué es el espionaje digital o ciberespionaje?

¿Mito o realidad?

Veamos antecedentes recientes

Equation group victims map

Finance · Government · Diplomatic / Embassies · Research institution · Energy / Infrastructure · University · Military · Aerospace · Telecommunications · Medical · Islamic Scholars · Media · Other / Unknown

High infection rate

- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Medium-level infection rate

- Lebanon
- Yemen
- United Arab Emirates
- Algeria
- Kenya
- United Kingdom
- Libya
- Mexico
- Qatar
- Egypt

Low infection rate

- Turkey
- Somalia
- Myanmar
- Germany
- South Africa
- Nigeria
- United States
- Venezuela
- Sudan
- Palestinian
- Morocco
- Malaysia
- Kazakhstan
- Iraq
- Brazil
- Uganda
- Switzerland
- Singapore
- Philippines
- Peru
- France
- Equador
- Belgium
- Bahrain

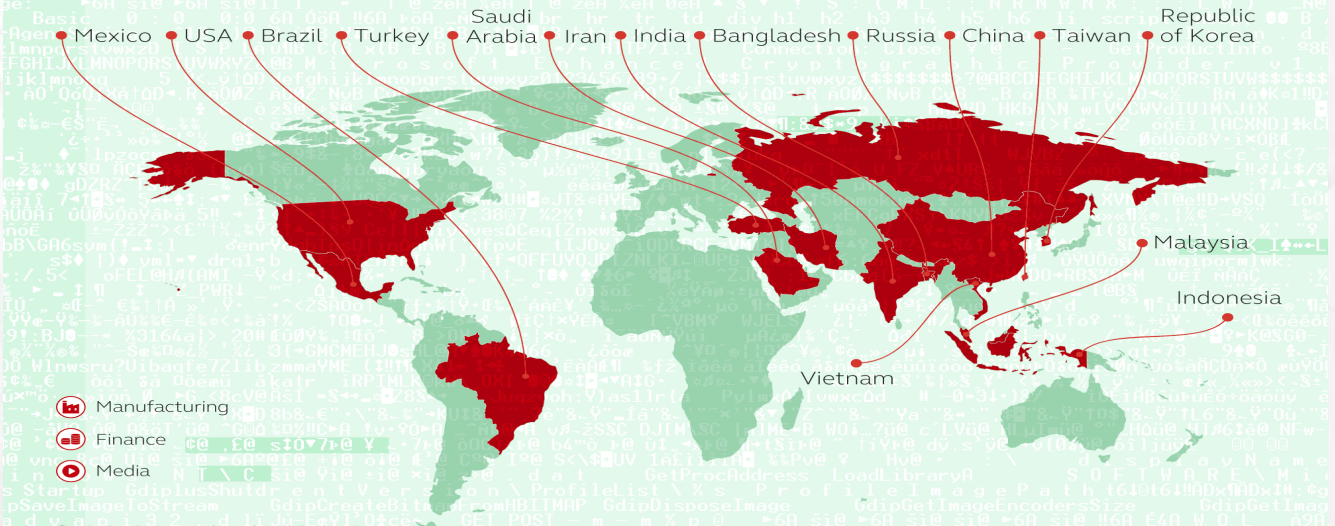
GREAT KASPERSKY lab


OBSERVED GLOBAL APT1 ACTIVITY
1 Norway
5 United Kingdom
2 Canada
1 Belgium
1 Japan
1 Luxemborg
1 France
3 Israel
3 India
2 Switzerland
115 United States
1 UAE
2 Taiwan
2 Singapore
1 South Africa

The targets of the Lazarus Group

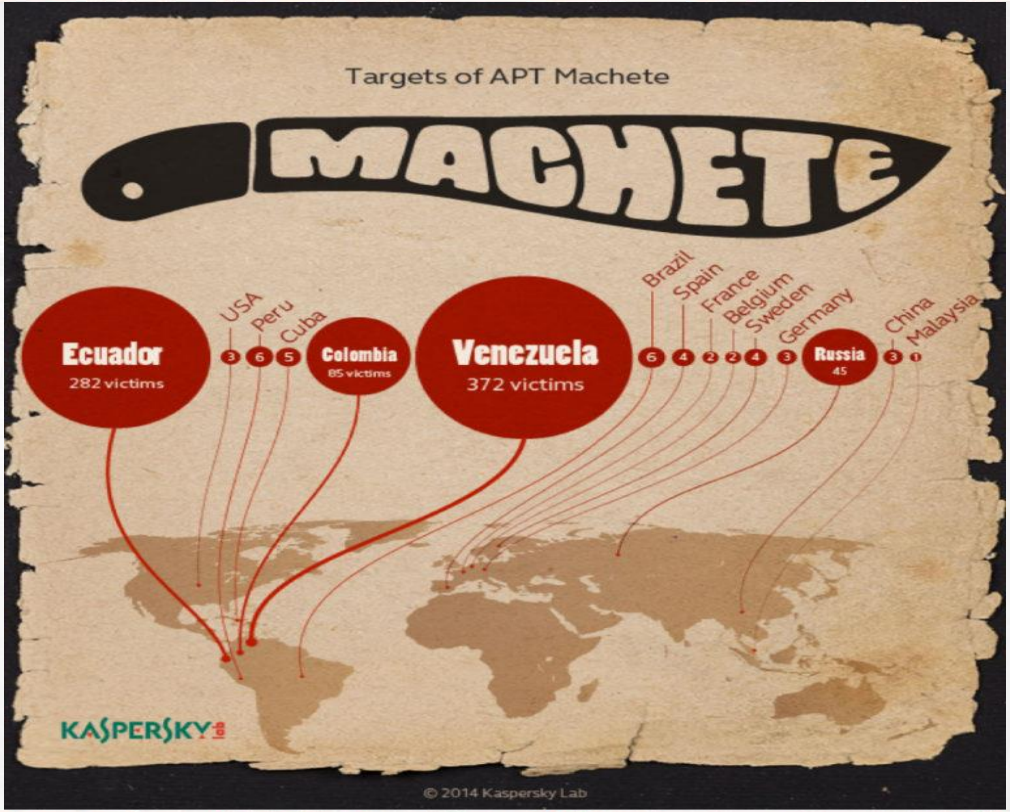
The most affected regions and countries by the Lazarus group malware

Lazarus Group is a highly malicious entity responsible for data destruction as well as conventional cyber-espionage campaigns targeting financial institutions, media stations, and manufacturing companies, among others, since at least 2009.



The statistics are based on Kaspersky Lab's own data and on data provided by Novetta in frame of Operation Blockbuster.
Read more at: www.operationblockbuster.com

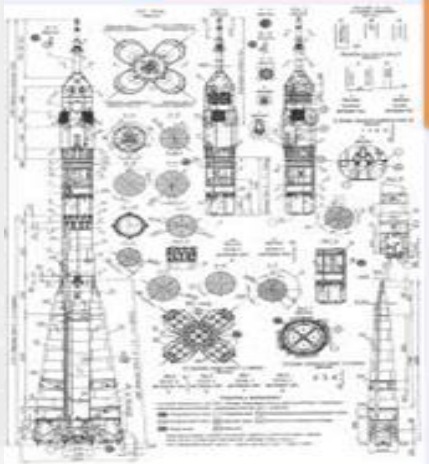
GREAT KASPERSKY lab


Targets of APT Machete
MACHETE
Ecuador
282 victims
USA 3
Peru 6
Cuba 5
Colombia
85 victims
Venezuela
372 victims
Brazil 6
Spain 4
France 2
Belgium 2
Sweden 4
Germany 3
Russia
45
China 3
Malaysia 1
KASPERSKY
© 2014 Kaspersky Lab

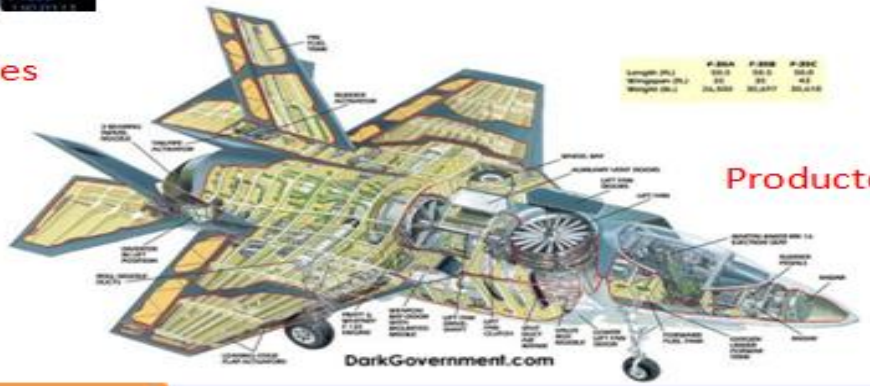
Por poner una línea temporal “La operación Aurora” 2009 contra directivos de Google y empresas de distintos sectores productivos y financieros puso de manifiesto la importancia del tema que tratamos

El ciclo de vida es fácil de entender

Actores



Factores motivadores



Producto

Veamos un sencillo ejercicio como prueba conceptual:

El ingenio de algunos hacker contratados o con otro tipo de motivación junto con la información libre en la red de las compañías: directivos, cargos, ocupaciones puede preparar una operación dirigida y creíble por la víctima 100 %

PRÁCTICA 1

Evil Microsoft document for your fun and profit

Evil Microsoft document for your fun and profit

1. *Se ha obtenido información de los objetivos y personal bajo su responsablidad en redes sociales linekdin, facebook, twitter, prensa digital, etc.*
2. *Se genera el documento para el objetivo/s que mayor probabilidad tenga.*
3. *Se genera el código malicioso necesario para la sustracción de información trabajando su indetectabilidad y salto de protecciones digitales que se entienda dispone la organización.*
4. *Se fija el momento (día y hora) adecuado para la operación.*
5. *Se lanza el ataque y se cruzan lo dedos.*

Evil Microsoft document for your fun and profit

REALIZACION DE LA PRÁCTICA PASO A PASO

(EN CASO DE PROBLEMAS DE CONEXIÓN, ETC VIDEO GRABADO DE LA PRÁCTICA)

Esto también tiene
su aplicación civil dentro del contexto de la Auditoría Interna

Un marco legal consultado por Auditoría Interna

Unos dispositivos propiedad de la organización

Una investigación de fraude, delito o actividades en contra de la organización de altos Directivos que escapan a los controles establecidos

¿Cuándo aplicarla?

Dificultad geográfica de acceso

Dificultad de acceso al entorno

Necesidad de máxima discreción (No participación de IT)

Hostilidad hacia el auditor interno

El acceso destaparía sospechas sobre la investigación

PARA FINALIZAR LA APLICACIÓN DEL ABC DE LA CIBERSEGURIDAD

A

B

C

Video Demo de lo que sucede cuando no se cumplen

Espero lo pasen genial en este encuentro CELAES 2017- QUITO

Esta .ppt todavía no dice “hola”

Gracias por vuestro tiempo ;-)

Antonio Ramos