KASPERSKY

Si no le teme al Chikungunya

Témale a una APT

JESUS CALLE
SYSTEMS ENGINEER
Kaspersky lab

Mar, 2015

AGENDA

- MALWARE CRECIENDO
- DONDE ENMARCAR UNA APT
- EJEMPLOS DE APT
- COMO PROTEGERSE DE UNA APT
- CONCLUSIONES

- MALWARE CRECIENDO

Como ha evolucionado el malware

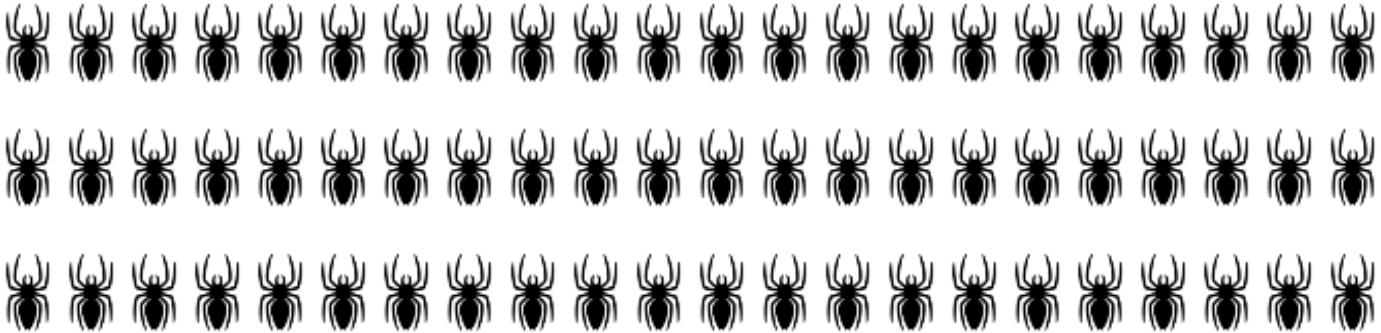
1994

Un nuevo virus aparecía cada hora

Como ha evolucionado el malware

2006

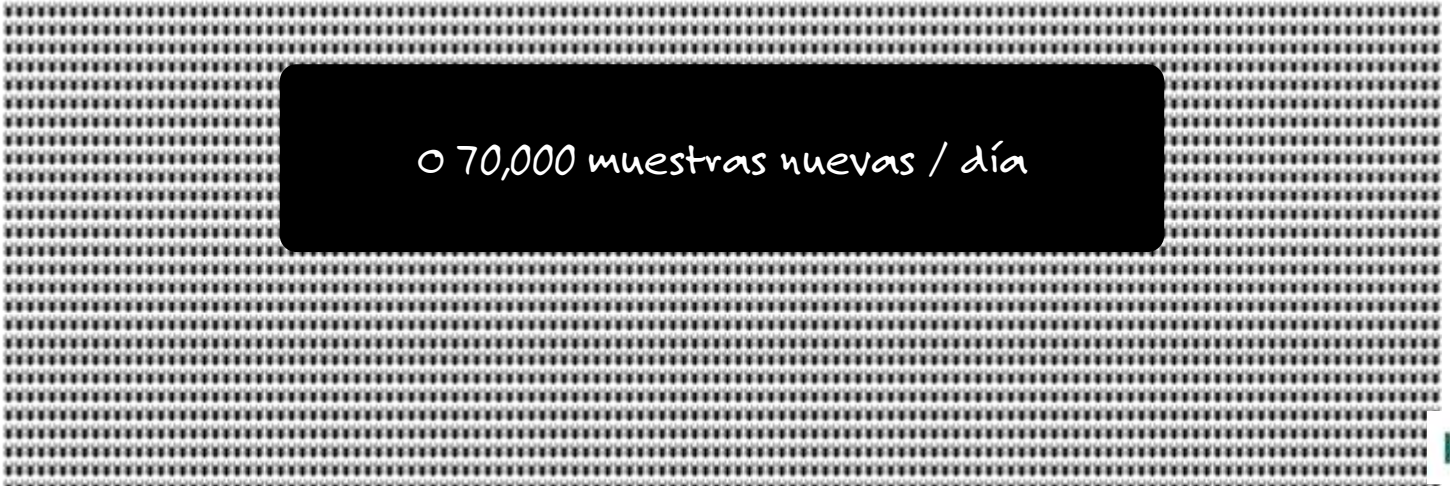
Un nuevo virus aparecía cada minuto



Como ha evolucionado el malware

2011

Un nuevo virus aparecía cada segundo



Analizando el

2014 ?

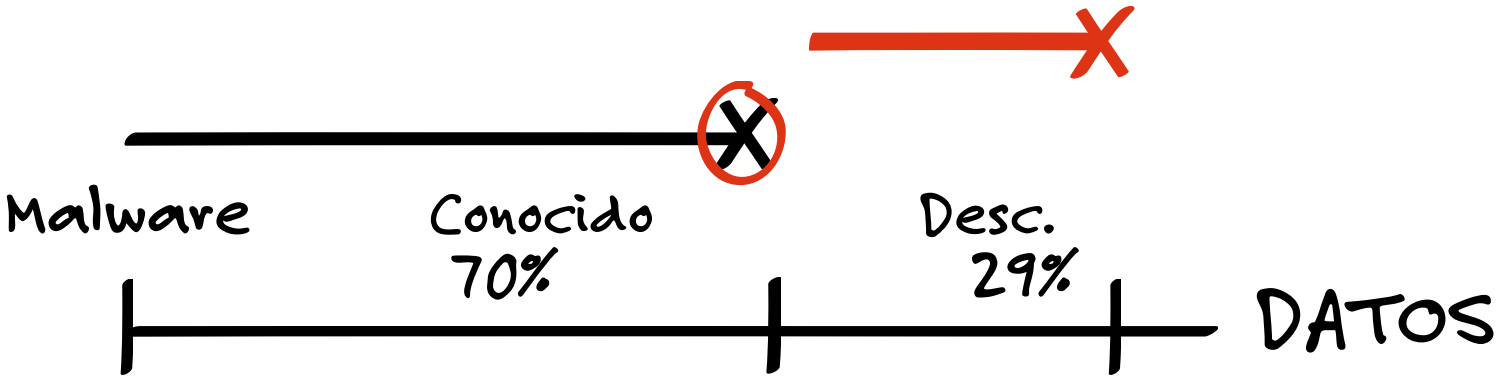
315.000 nuevas muestras por día

KASPERSKY lab

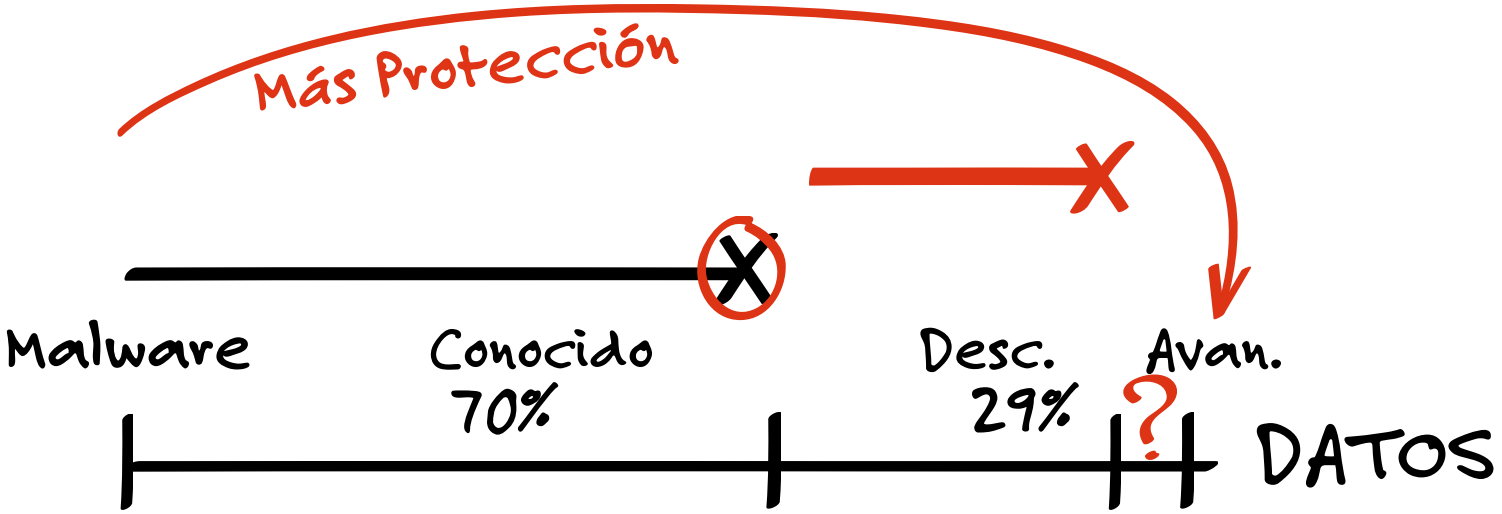
- DONDE ENMARCAR UNA APT

KASPERSKY lab

El Malware en el punto final es un hecho



El Malware en el punto final es un hecho



Ese pequeño porcentaje avanzado:

- APT (Advanced Persistent Threats) - MALWARE
  - Campañas cibernéticas contra un objetivo definido
  - Usan la última tecnología disponible o la desarrollan
  - Cuanto cuesta? No importa el objetivo se debe lograr
  - Vulnerabilidades de día 0, certificados robados, etc.
    - Ciber sabotaje
    - Ciber espionaje
    - Robo de Datos
    - Borrado de Datos
    - DDoS
    - Facilitando ataques
    - Vigilancia
    - Robo de Dinero

https://apt.securelist.com/

Que no se considera APT:

- Robos de datos **aún** no explicados, fallas humanas, etc
  - Sony – Target - HD

El ataque a Sony Pictures es masivo: filtrados guiones, despidos y más

EL MUNDO

Edición España · Versión Clásica

SECCIONES | Internacional | EEUU | México | Argentina | Brasil | Cuba | Colombia | Venez

LIGA » En directo: Levante-Celta

EEUU La firma de seguridad Norse ha presentado un informe que desmonta la teoría del FBI

El ataque a Sony fue una venganza de una ex empleada y otros 5 individuos

Figure 1.

KrebsonSecurity

In-depth security news and investigation

07 **Home Depot Hit By Same Malware as Target**

http://www.elmundo.es/internacional/2014/12/30/54a30537ca4741322b8b457b.html

http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf

http://www.gore.com/articulos/14763/Como-se-llevo-a-cabo-el-ataque-a-Target

KASPERSKY

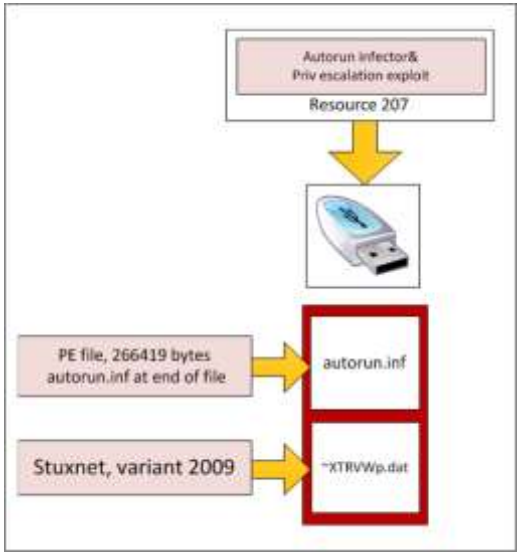
APTs (Advanced Persistent Threats)

- EJEMPLOS DE APT

KASPERSKY

Ciber sabotaje

- Stuxnet
  - Retrasar el programa nuclear iraní
  - Actuó en Natanz
  - Tecnología de punta, vulnerabilidades de día cero, certificados digitales
  - No actuó solo, fue una campaña
  - 300.000 apariciones en el mundo



https://securelist.com/blog/incidents/33174/back-to-stuxnet-the-missing-link-64/

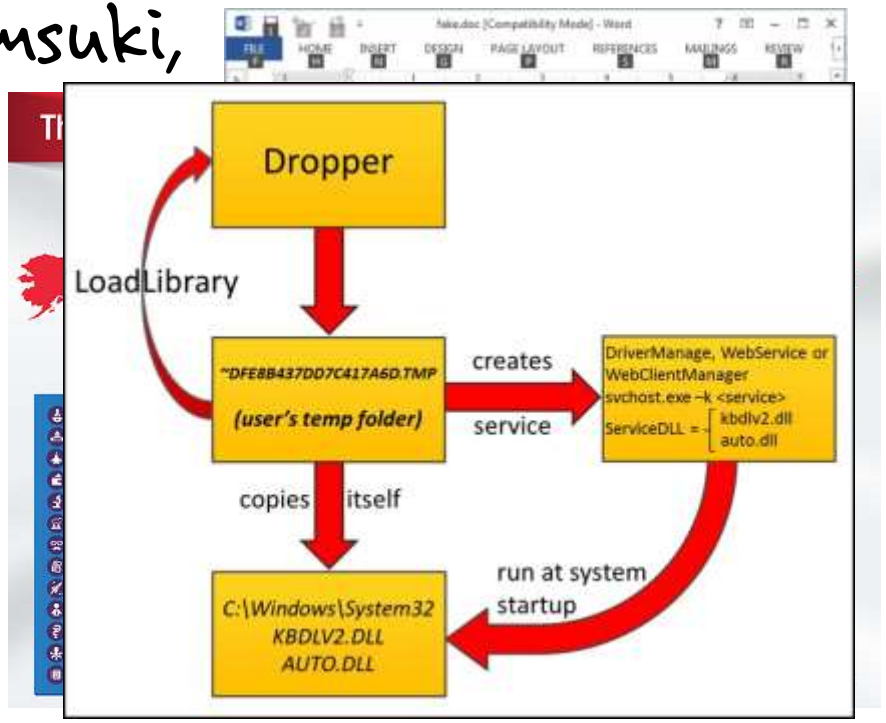
Ciber espionaje

- Duqu, Flame, Octubre Rojo, DH
  - Dq: Buscando solo *.dwg
  - FL: Encendiendo el micrófono del PC
  - OR: Tomando información de sedes diplomáticas en todo el mundo
  - DH: Hospitalidad

http://securelist.com/blog/incidents/32463/duqu-faq-33/
http://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/
http://securelist.com/blog/incidents/57647/the-red-october-campaign/

Robo de datos

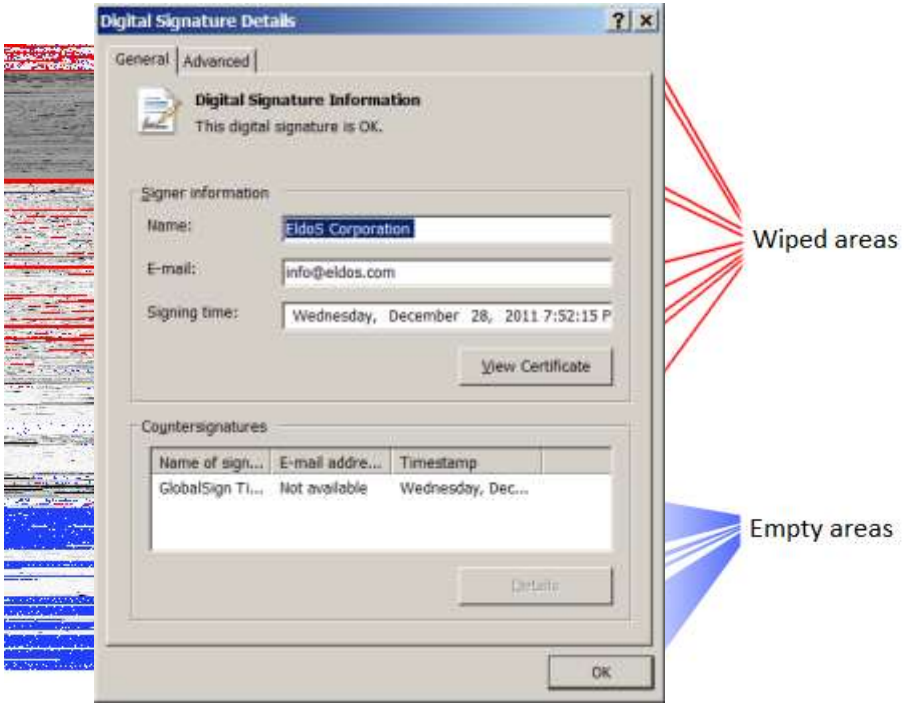
- Net Traveller, Icefog, Kimsuki,
  - NT: contra Compañías de petróleo y gas, instituciones educativas y gubernamentales
  - IF: contra Japón y Sur Corea
  - KSK: Desde CdN deshabilitando fw, y robando información



http://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/
http://securelist.com/blog/research/57331/the-icefog-apt-a-tale-of-cloak-and-three-daggers/
http://securelist.com/analysis/publications/57915/the-kimsuky-operation-a-north-korean-apt/

Borrado de datos

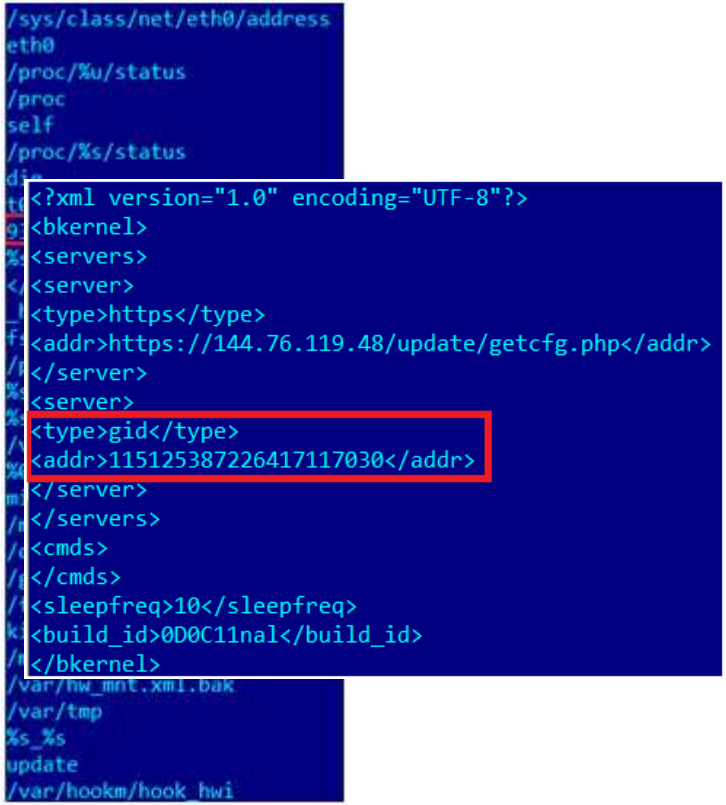
- Wiper, Shamoon
  - Wpr: ITU encuentra algunos indicios de un sw borrador
  - Smn: la petrolera Aramco es víctima del ataque que usa certificados digitales



http://securelist.com/blog/incidents/34088/what-was-that-wiper-thing-48/
http://securelist.com/blog/incidents/34369/shamoon-the-wiper-in-detail

DDoS

- Black Energy
  - Ataque registrado en Rusia
  - Diferentes compañías (BE2, BE3)
  - Plugins y scripts personalizados para el ataque
  - Multiplataforma

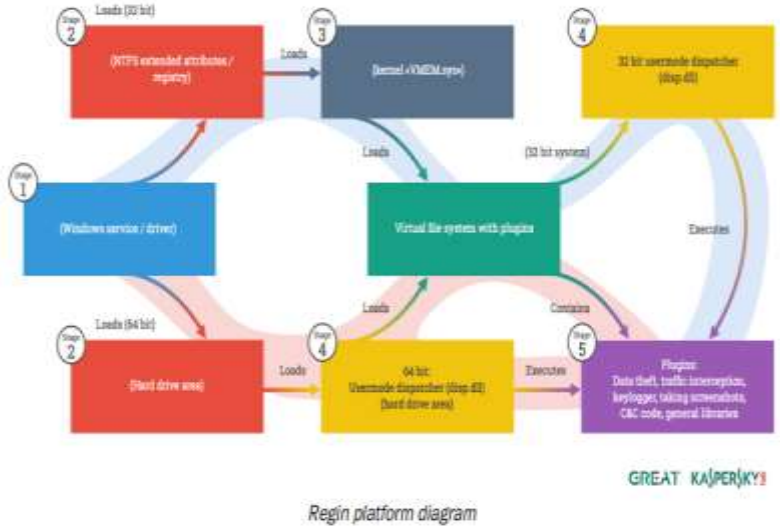


http://securelist.com/blog/research/67353/be2-custom-plugins-router-abuse-and-target-profiles/

KASPERSKY

Facilitando otros ataques

- Reign
  - Una de las Ciber herramientas más antigua encontrada a la fecha (2003)
  - Contra operadores de telecomunicaciones, gobiernos, instituciones financieras, de investigación.



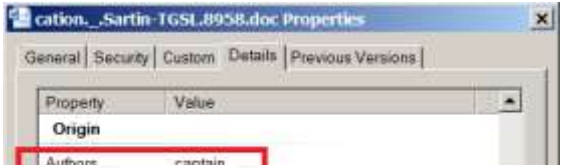
Regin platform diagram

http://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/

KASPERSKY

Vigilancia

- Finspy, SABPUB, TeamSpy
  - Servicios de información
  - Búsqueda de datos de activistas
  - Sólo se vende a establecimientos legales



http://securelist.com/analysis/publications/36996/mobile-malware-evolution-part-6/
http://securelist.com/blog/incidents/33208/new-version-of-osx-sabpub-confirmed-mac-apt-attacks-19/
http://securelist.com/blog/incidents/35520/the-teamspy-crew-attacks-abusing-teamviewer-for-

Robo de dinero

- Carbanak

- 11 países
- 70 objetivos
- 1 Billón de dólares

https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

Latinoamérica no se queda atrás

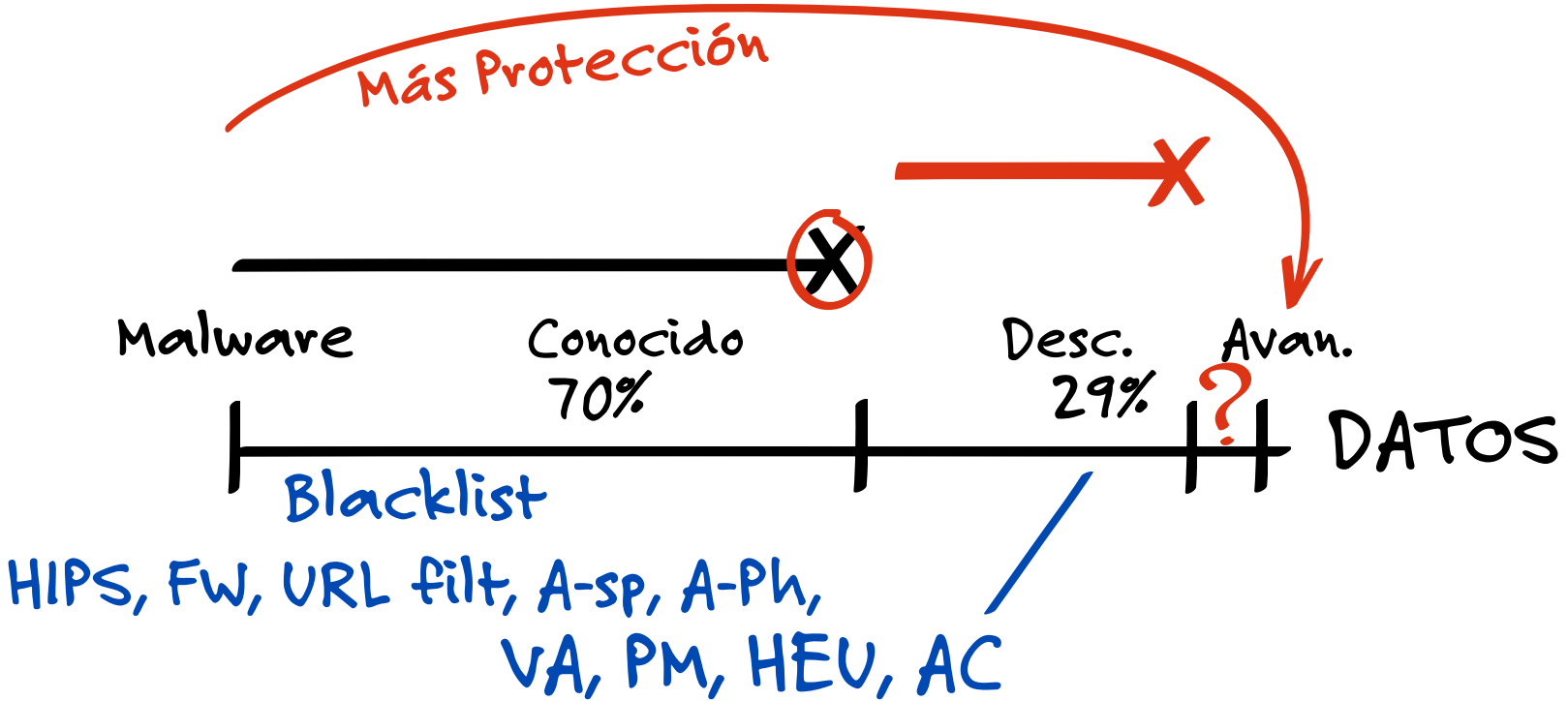
- Careto y El machete
  - Careto: robo de información desde 2007 contra gobiernos, activistas y otros, víctimas localizadas en Latam, Europa y África.
  - Machete: espionaje de alto nivel afectó en especial países del área andina

http://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/
https://securelist.com/blog/research/66108/el-machete/

- COMO PROTEGERSE DE UNA APT

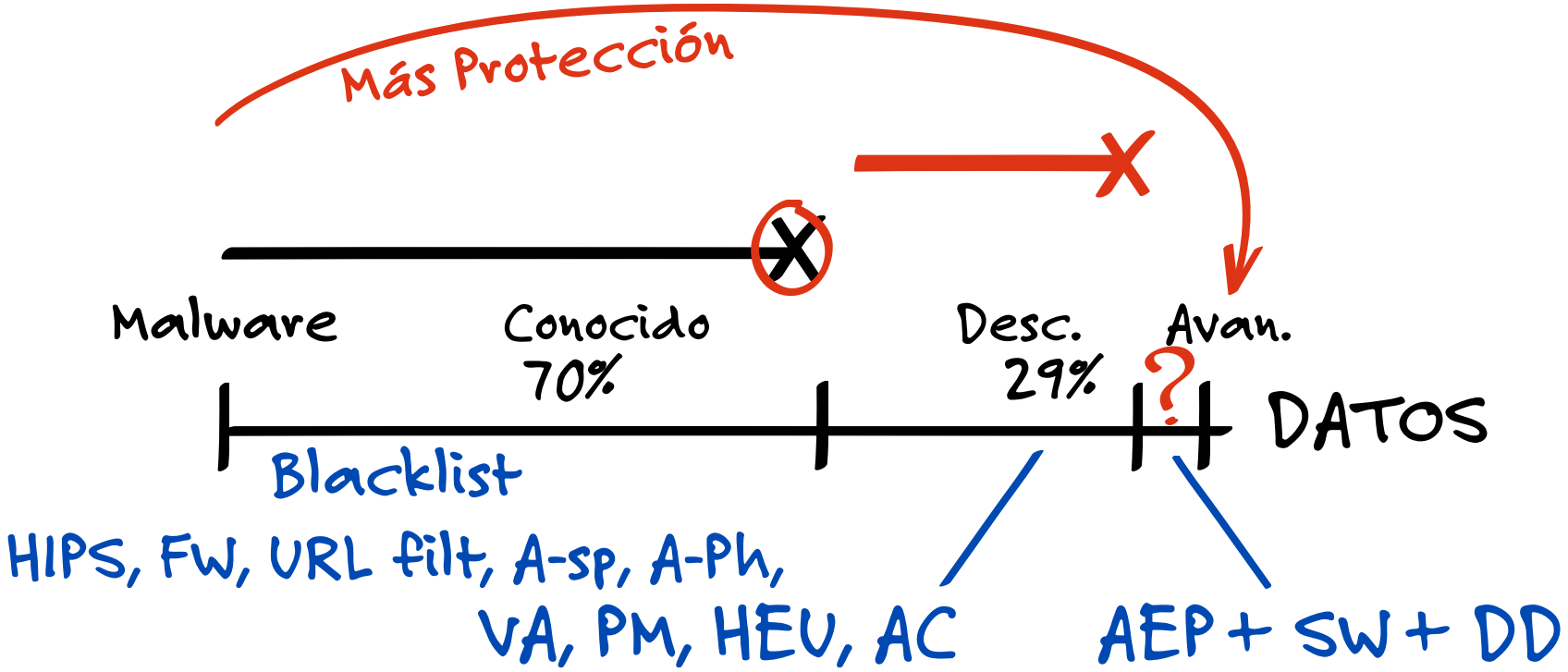
KASPERSKY lab

El Malware en el punto final es un hecho



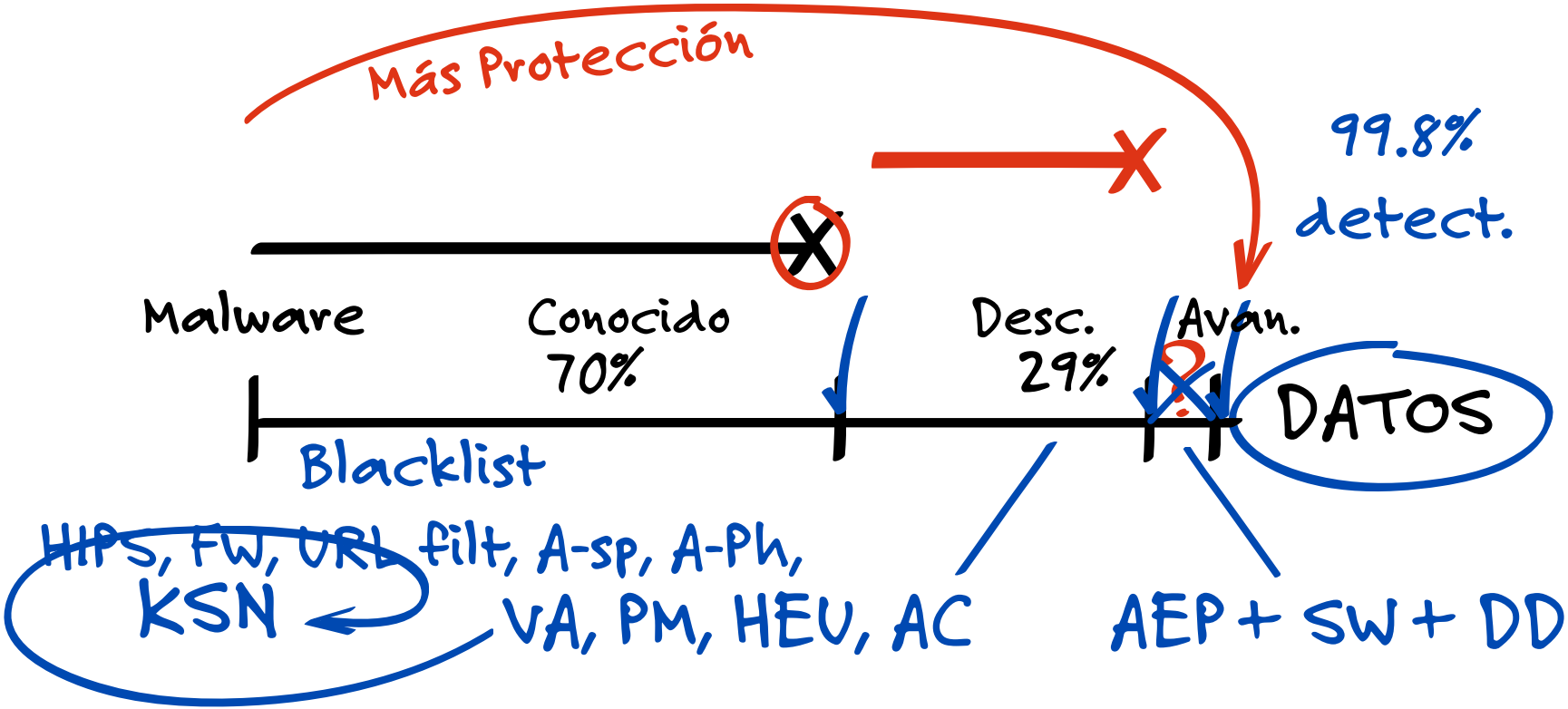
Hay que parar el establecimiento del MW

El Malware en el punto final es un hecho



Hay que parar el establecimiento del MW

El Malware en el punto final es un hecho



Hay que parar el establecimiento del MW

KASPERSKY

- CONCLUSIONES

CONCLUSIONES

- APTS: no son ciencia ficción
  - La protección de punto final no es un juego
  - Cualquiera puede ser victima
  - Información, dinero, poder, todos son los móviles
  - Está usted protegido contra APTs?
  - Su fabricante reconoce APTs, estudia APTs?
  - Cualquier porcentaje de protección adicional sirve!

MuCHAs GRaCiAS!

- JESUS.CALLE@KASPERSKY.COM

KASPERSKY lab