Deloitte.

Information Security Community

Emmanuel Santiago

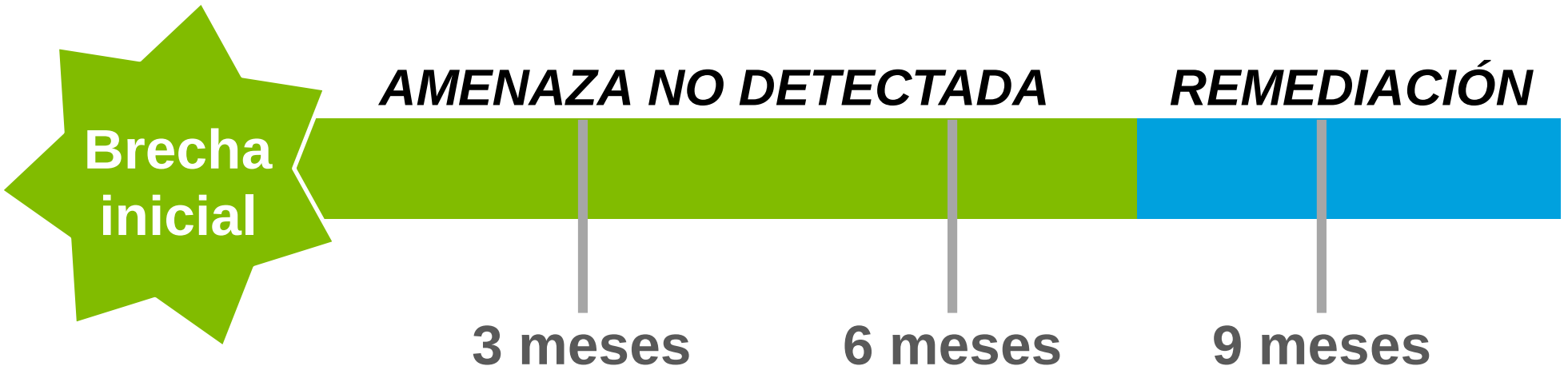
4 de septiembre de 2014

Contenido

- El alto costo de no estar preparado
- Conociendo al adversario
- Estadísticas del mundo real
- Caso de estudio

El alto costo de no estar preparado

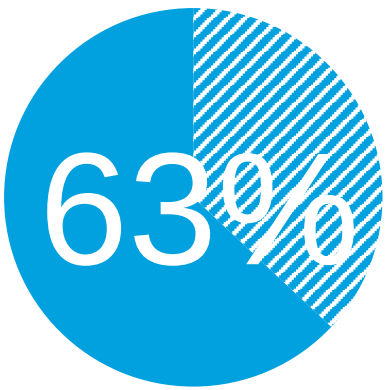
El alto costo de no estar preparado



DÍAS*

Atacantes sin ser detectados

*media en días



De las compañías se enteraron de estar comprometidos por un tercero

De las víctimas tenía el anti-virus actualizado

Conociendo al adversario

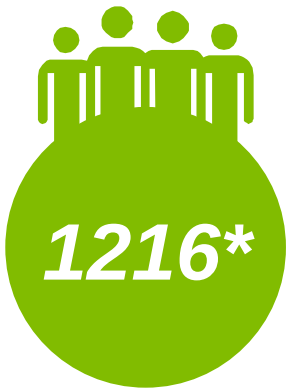
Conociendo al adversario

La detección del exploit es crítica

Cualquier etapa después de la explotación puede ser discutida

Estadísticas del mundo real

Resultados de Pruebas de Valor



1216* CLIENTES

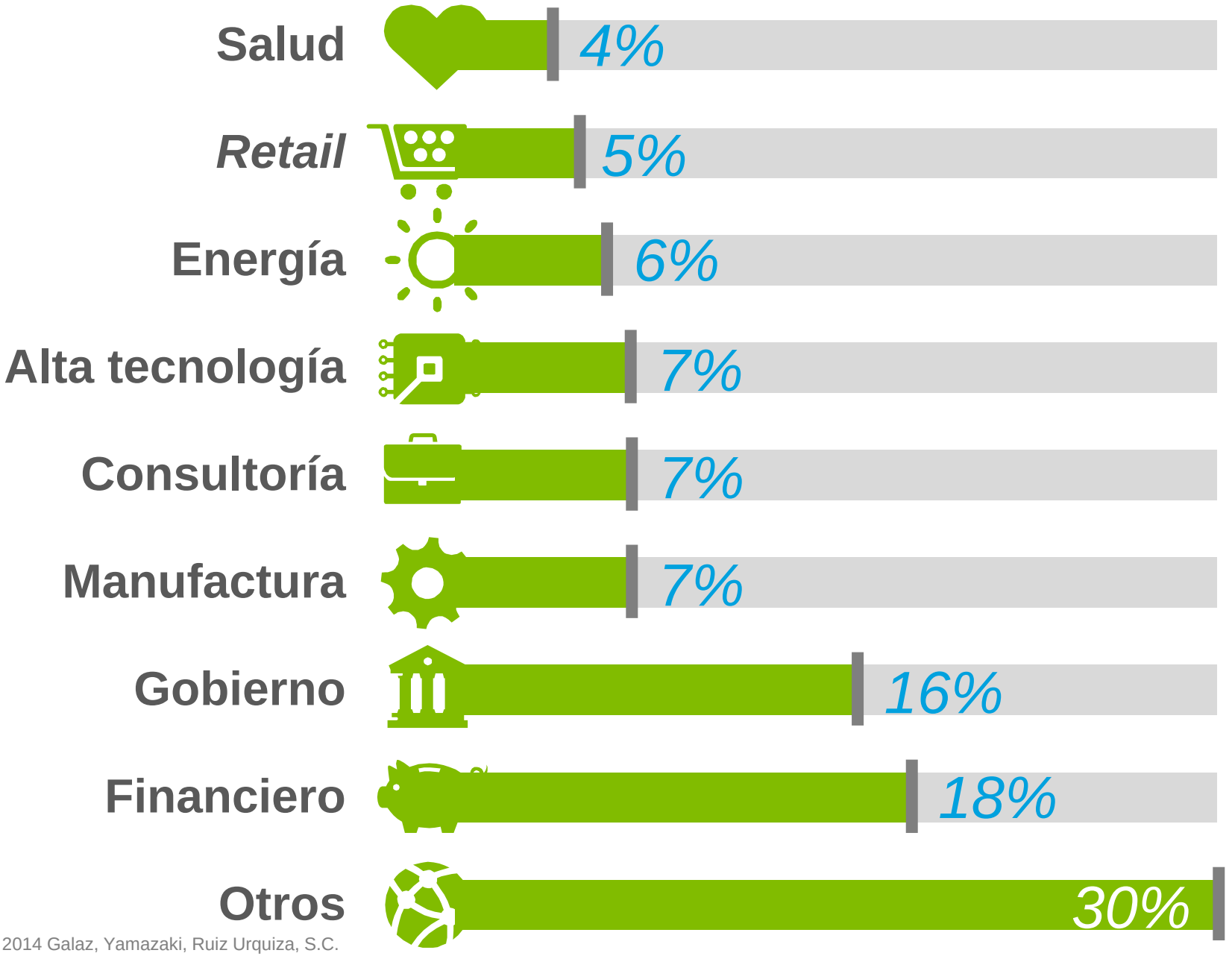
20+ CLIENTES COMPROMETIDOS

63 PAÍSES

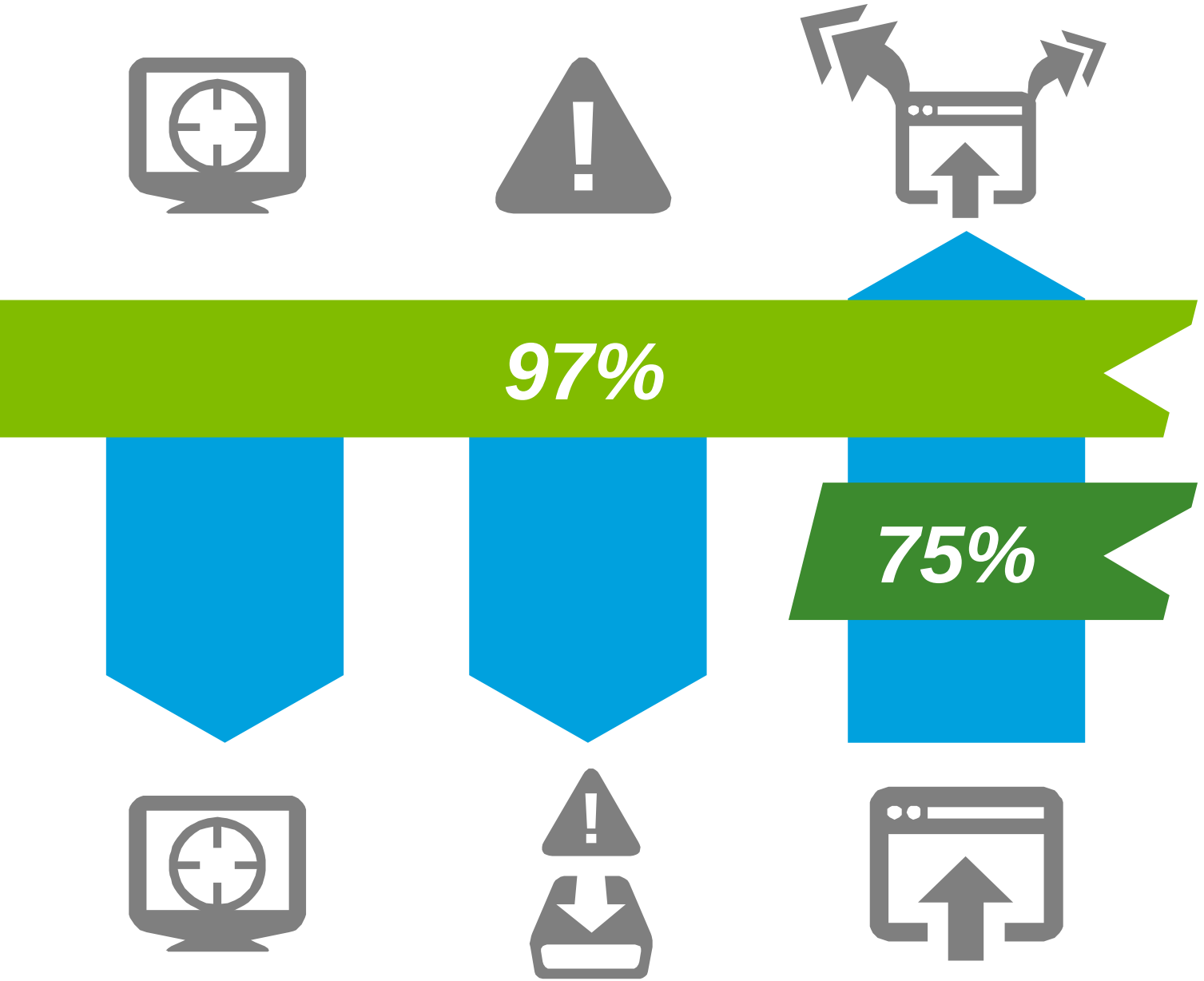
20+ INDUSTRIAS

27% TENÍAN APT

Pruebas de Valor por Industria



¿Funcionan los controles tradicionales?



Estaban comprometidos

De los clientes contaba con comunicación de Comando y control

Ataques por cliente por semana

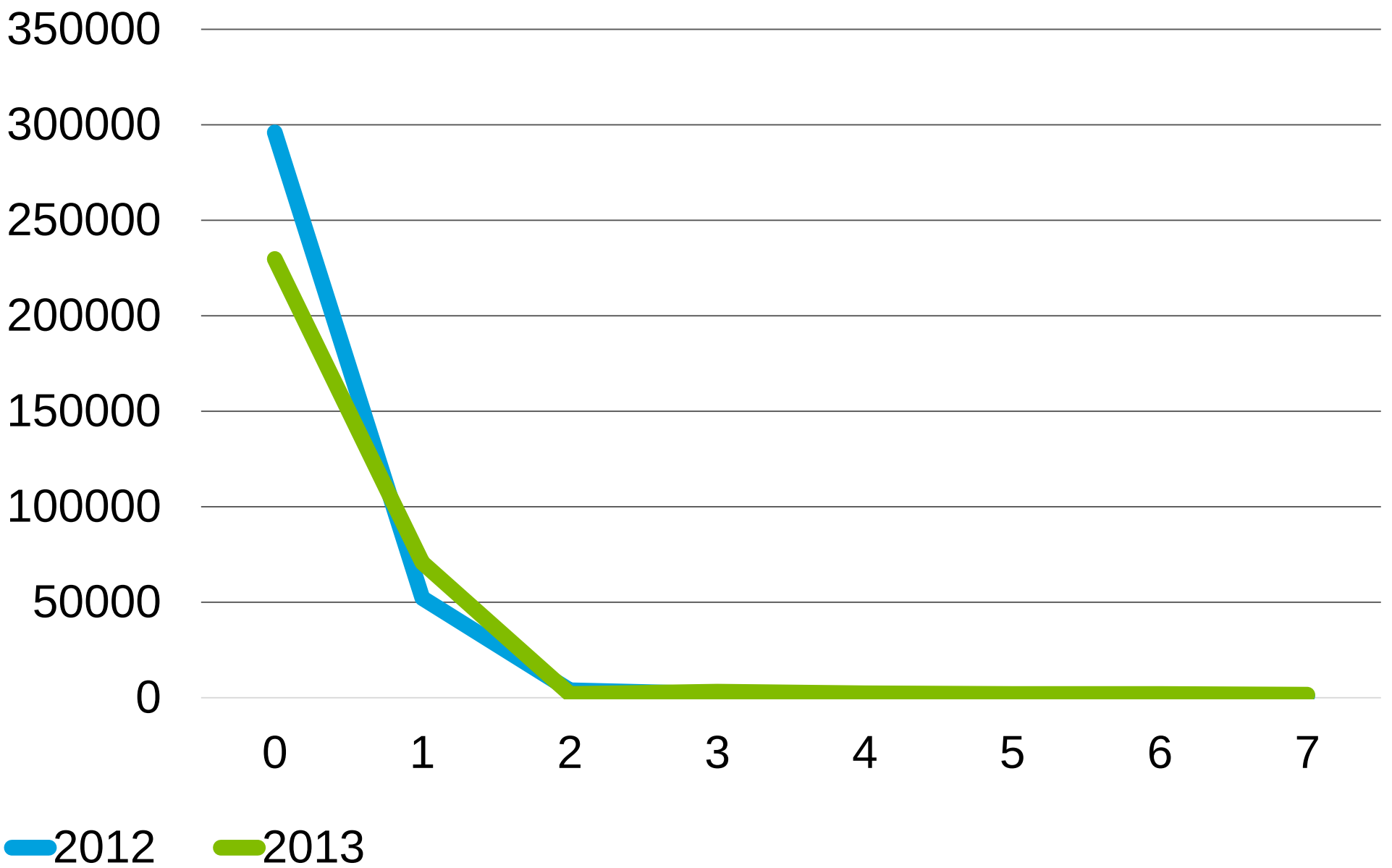
91
Host impactados

Exploit  ***1.59***

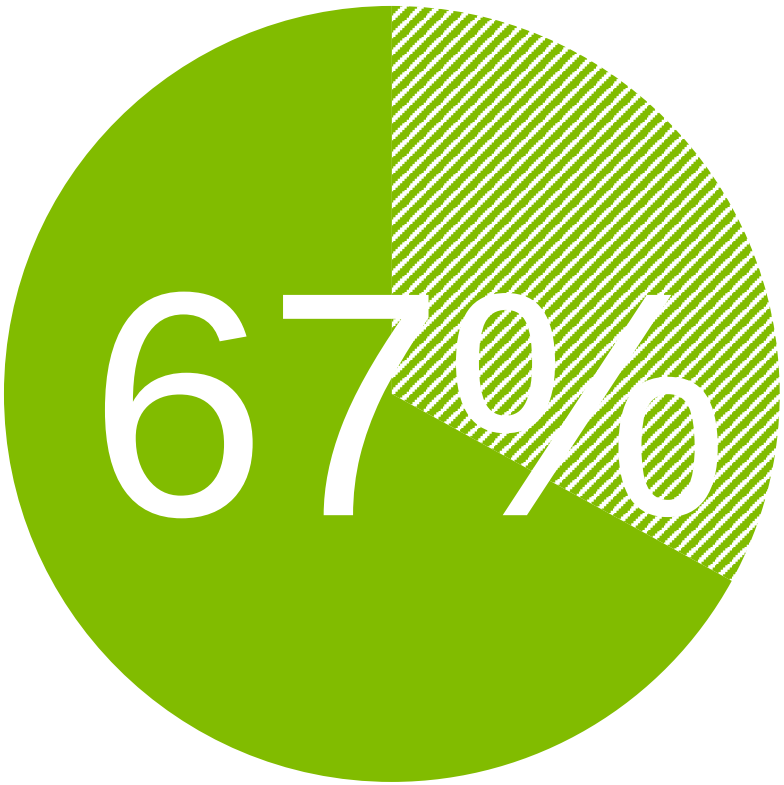
Malware download  ***122***

Command and Control  ***1658***

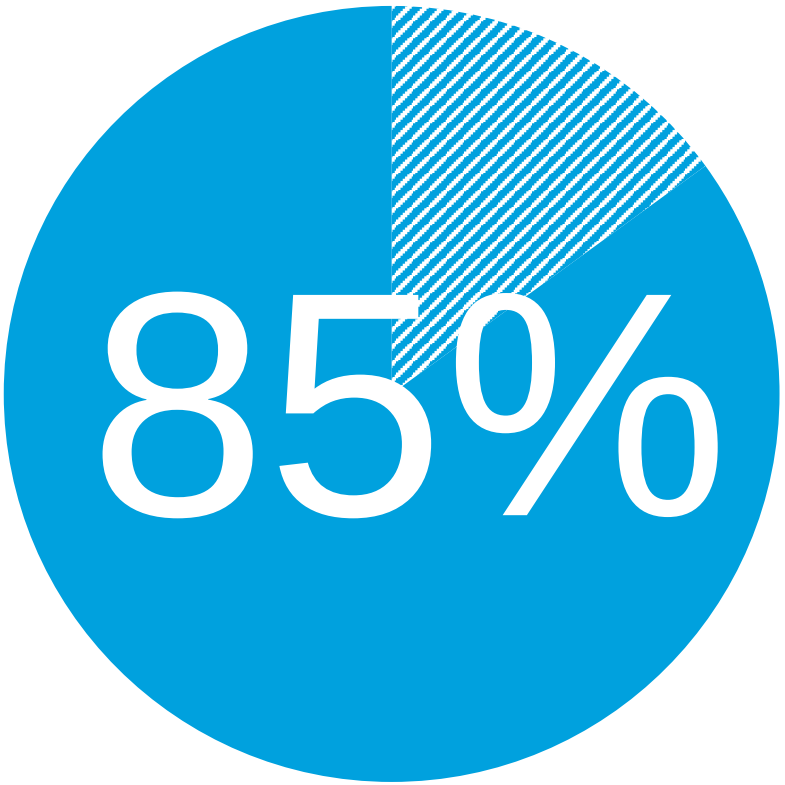
¿Dos horas?



¿Caza fantasmas?

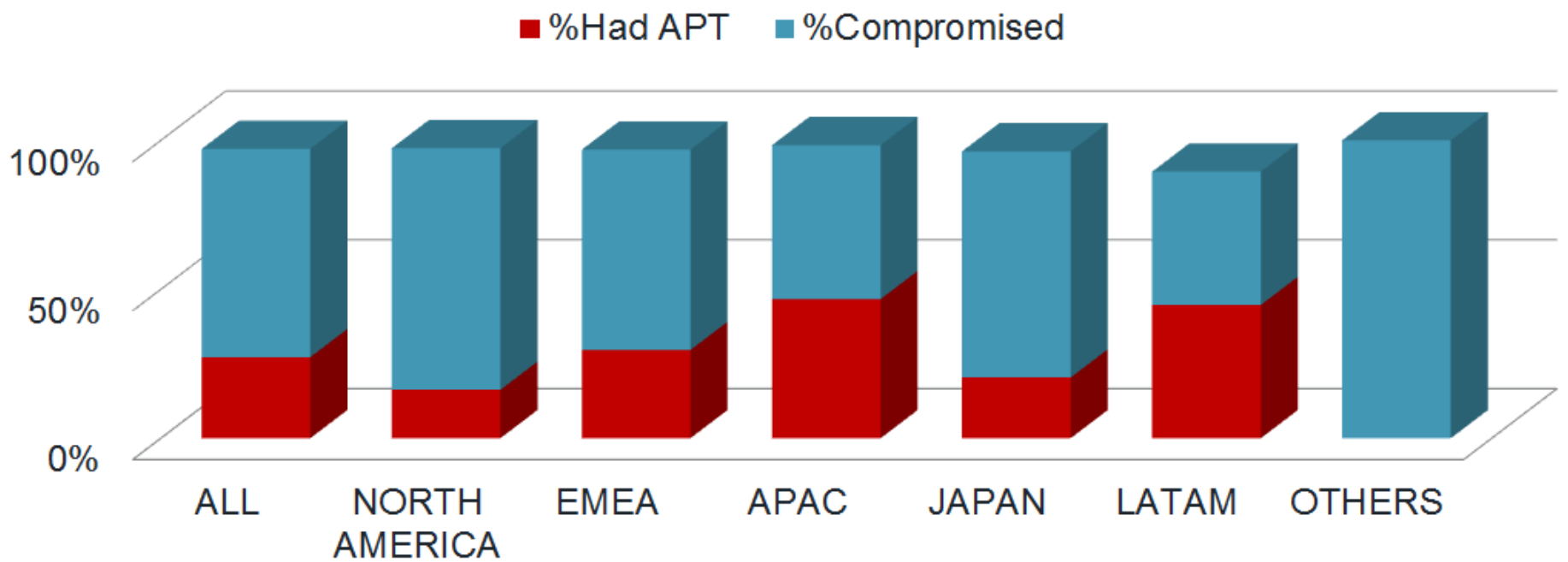


Del malware solo existe una vez



Del malware desaparece después de una hora

Resultados PoV por región



Caso de estudio
Operación Clandestine Fox

Inside the Investigation
Clandestine Fox Zero-Day

How FireEye Found the Zero-Day

FireEye's Investigation

FireEye's discovery of the Internet Explorer zero-day exploit was the result of close collaboration between experts from our Mandiant incident response team, the FireEye Managed Defense service and FireEye Labs researchers.

Inside the Investigation
Clandestine Fox Zero-Day

22:00 Dynamic Threat Intelligence Updates

FireEye intelligence teams translate information about the new zero-day exploit into intelligence and within 24-hours from the initial discovery, millions of FireEye MVX virtual machines are updated, protecting thousands of organizations across the FireEye Global Defense Community.

10:00 Vendor Notification and Responsible Disclosure

FireEye researchers notify Microsoft of the discovery and work with their security team on technical details as well as public announcements

Inside the Investigation
Clandestine Fox Zero-Day

0:00 Exploit Discovery

The first indication of this zero-day comes from the FireEye Managed Defense service, which constantly monitors

0:15 Incident Response Investigation

The Mandiant Incident Response team investigates and captures network traffic (Pcaps) to better understand the exploit, determine who may be conducting the campaign and why.

0:30 Zero-Day Analysis

The FireEye Zero-Day Discovery team analyzes the exploit using proprietary tools to more fully understand the techniques and tactics of the attackers who are carrying out Operation Clandestine Fox.

Q&A

Deloitte.