Del USB a la web: cómo tu sitio propaga malware
• Pablo Ramos, Security Researcher de ESET Latinoamérica

➢ Bla ble bli blo blu!

➢ @ESETLA

➢ @ramospablo
Antes
Antes
Después
Después
Después
¿Para qué es útil un sitio web?

• Malware
• Phishing
• Botnets
• Cibercrimen
Casos reales y estadísticas
Análisis Malc0de y MDL

• Brasil es el país con más reportes en Latinoamérica, y el sexto en el mundo en cantidad de reportes.

• Ranking en Latinoamérica: Brasil (88%), Chile, Argentina y Ecuador.

• Una URL reportada tarda hasta 4 días en limpiar el malware.
Los resultados

• Primer acceso al sitio web: 10:01hs.
• Último acceso al sitio web: 15:25 hs.
• 5 horas de accesos...
• 164 accesos.
• **35 tarjetas de crédito válidas.**
Phishing

OWASP
The Open Web Application Security Project
13 mil archivos
27 mil registros
8 mil contraseñas
Botnets

Dorkbot, sitios afectados:

- http://www.antiquitebonton.it/wp-content/plugins/updates/16upjmrlzz.exe
- http://www.antiquitebonton.it/wp-content/plugins/updates/18upjmrlzz.exe
- http://www.worldcounselling.com/IMG00359268.JPG
- http://iwantescort.com/libs/thumb/domit.txt
- http://www.jdkim.com//bbs/data/date/drlzz.txt
- http://www.aceinfosys.co.kr//bbs/data/update/do.txt
- http://www.endenter.com/wp-includes/js/updt/do.txt
- http://www.beautifulthaibride.com/do.txt
¿Qué pasa adentro del laboratorio?
Hola, ¿qué necesita?
#%@#! Ustedes detectan mi sitio web como infectado. #%@#!
Su sitio web ESTÁ infectado, solo que usted no lo sabe.
Su sitio web ESTÁ infectado, solo que usted no lo sabe.
#%@#! Listo, arreglado. #%@#!
Listo, arreglado.
Dos meses después...
Si su sitio web está infectado...
En verdad es así...
Tens of thousands of web sites affected in ongoing mass SQL injection attack

By Dancho Danchev

Hundreds of thousands of legitimate web sites are currently affected in a mass SQL injection attack that has been ongoing for the past several months. The ongoing mass SQL injection attacks, are directly related to last year's scareware-serving Lizamoon mass SQL injection attacks.

The cybercriminals behind it, are automatically exploiting the legitimate web sites, and embedding a tiny script on the affected pages, abusing an input validation flaw, or exploiting vulnerable and outdated versions of the web application software running on them.
Servidores vulnerados según dominio del país

- Argentina: 21%
- Brasil: 14%
- Chile: 4%
- Perú: 7%
- Venezuela: 3%
- México: 14%
- Paraguay: 3%
Preguntas
¡Muchas Gracias!

Pablo Ramos (@ramospablo)
Security Researcher