Information Security Inc.

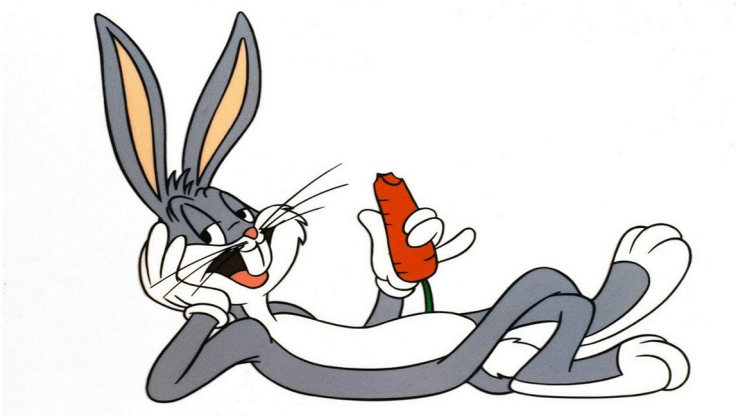
Securing Bussiness since 2003

# Cybersecurity Highlights

No hables a oídos del anecio,porque menospreciará la prudencia de tus razones. Proverbios 23

# INFORMATION SECURITY OVERVIEW

## ¿QUÉ HAY DE NUEVO, VIEJO?



https://www.infobae.com/america/mexico/2020/06/12/fue-secuestrada-en-nicaragua-y-prostituida-en-mexico-el-infierno-de-una-esclava-sexual-del-narco/

Cuando escapó, relató a la Unidad Especializada en Investigación de Tráfico de Menores, Personas y Órganos en México que **a las víctimas de trata de personas les colocan chips para rastrear sus movimientos y no dejar que escapen**, cómo se deshacen los narcos de los cuerpos, que existen clientes que **pagan por torturar**, y que casi nadie escapa.

# DANIELA TENÍA INJERTADO UN CHIP RASTREADOR [2020]

https://www.muyseguridad.net/2020/06/10/skimmer-esconde-greenworks/

# SKIMMERS 4.0 (HARD + SOFT + WIFI ) AHORA CON AUTODESTRUCCIÓN→ GRUPO MAGECART [2020]

https://www.businessinsider.es/honda-enel-afectadas-ciberataque-ransomware-snake-656817

# Honda y una filial de Enel, afectadas por el 'ransomware' Snake: así ha sido el ciberataque, según varios analistas de ciberseguridad

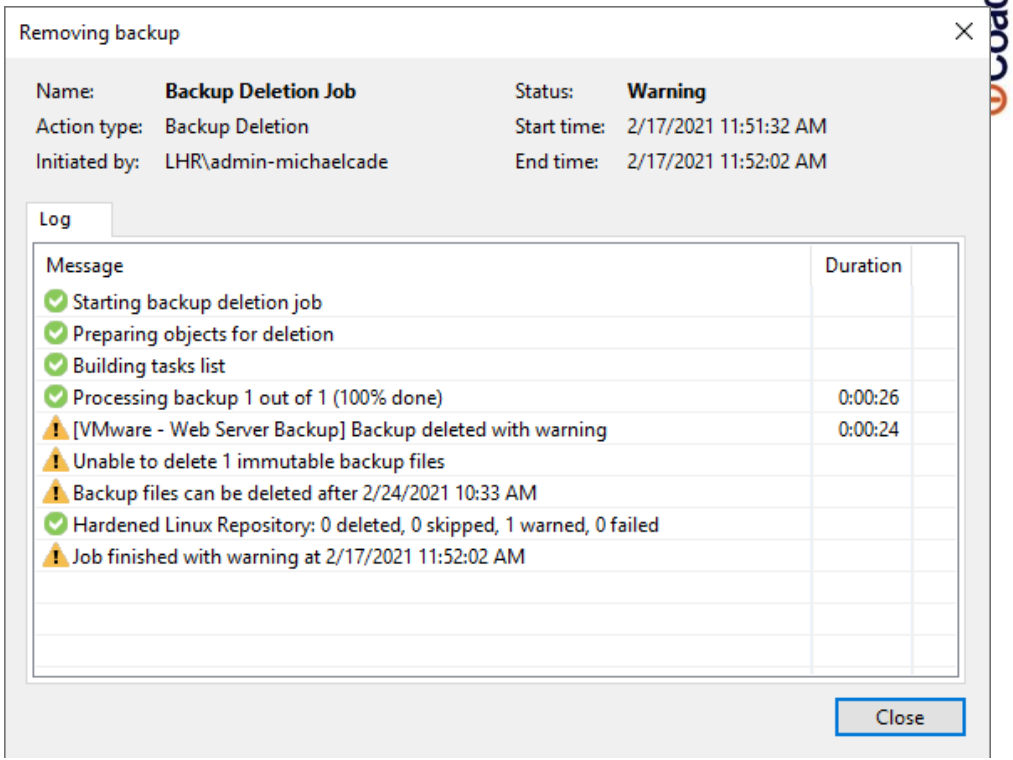
**Alberto R. Aguiar** 10 Jun 2020 12:16h.

## ADVANCED PERSISTENT THREAT → RANSONWARE

# ¿QUÉ HAY DE NUEVO, VIEJO?

NO ES LA IDEA HACERLES PROPAGANDA A LOS CIBERDELINCUENTES, ASI QUE VAMOS A IDENTIFICAR ALGUNAS TÉCNICAS DE PROTECCIÓN.

Ej: Ransonware → Immutable Backup (ver más)



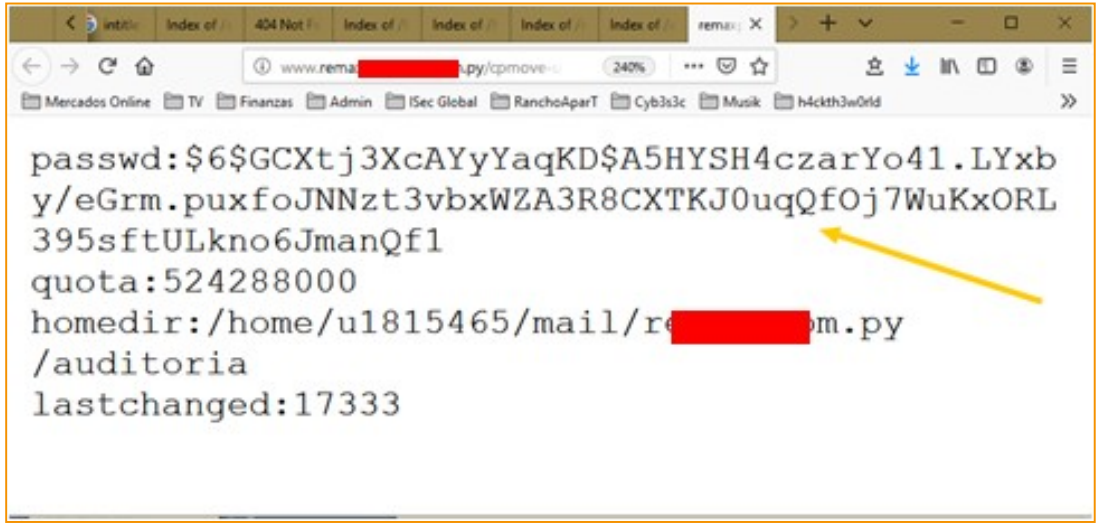
# ANALICEMOS PORQUE PASAN ESTAS COSAS:

- el otro día escuché una charla de **desarrolladores**, que decían…

- quiero capturar las cookies que **cachea** el webserver y **pasarlas** como parámetro al servidor de base de datos, **¿se podrá?**

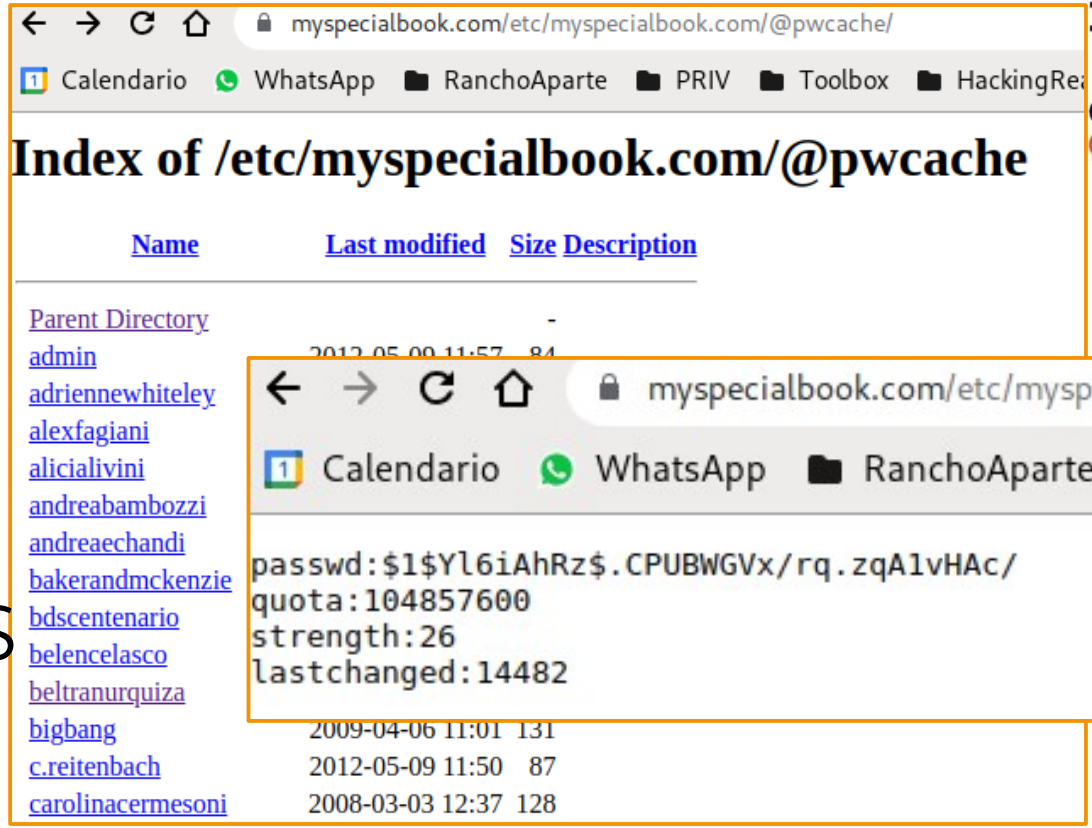
# Buscando cache’s en la web:

- intitle:index.of homedir/tmp/
- intitle:index.of pwcache



# ¿Qué? ¿Cachea Paswords?

SÍ LOS MUCHACHOS CACHEAN PASSWORDS



# ¿Qué? ¿Cachea CÓDIGO?

SÍ LOS MUCHACHOS CACHEAN CÓDIGO

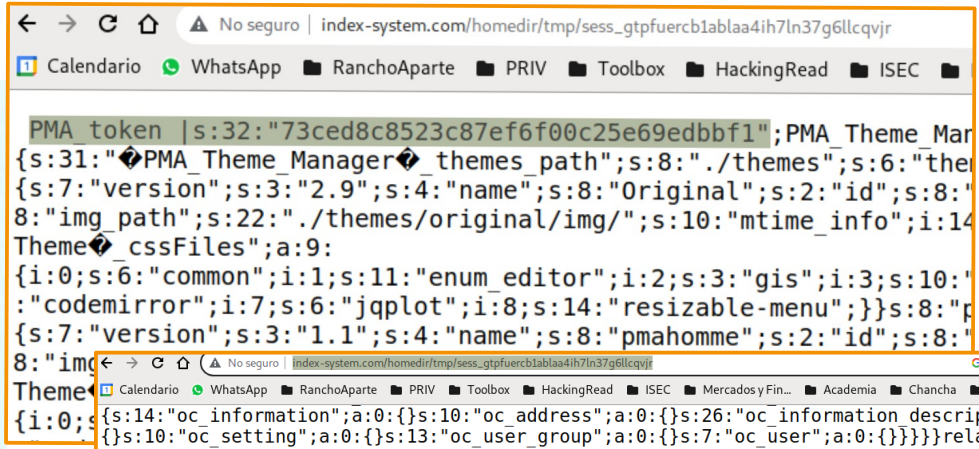
myspecialbook.com/etc/myspecialbook.com/contact/filter

Calendario WhatsApp RanchoAparte PRIV Toolbox

```
# Exim filter

# Auto Generated by cPanel.  Do not manually edit this file as your char

if not first_delivery and error_message then finish endif

#VR
if
 $message_body contains "pregunta"
 or $message_body contains "presupuesto"
 or $message_body contains "regalo"
 or $message_body contains "libro"
 or $message_body contains "book"
 or $message_body contains "ediciÃ³n"
 or $header_subject: contains "pregunta"
 or $header_subject: contains "presupuesto"
 or $header_subject: contains "regalo"
 or $header_subject: contains "libro"
 or $header_subject: contains "book"
 or $header_subject: contains "ediciÃ³n"
then
 deliver "vr@myspecialbook.com"
```

# ¡ah no!  Pero seguro la sesiones no las cachea...

SÍ LOS MUCHACHOS CACHEAN LAS SESIONES COMPLETAS



# MOMENTO DEL MONO INCREÍBLE →

# ¿Quién dijo que todo está perdido?

Yo vengo a ofrecer mi corazón

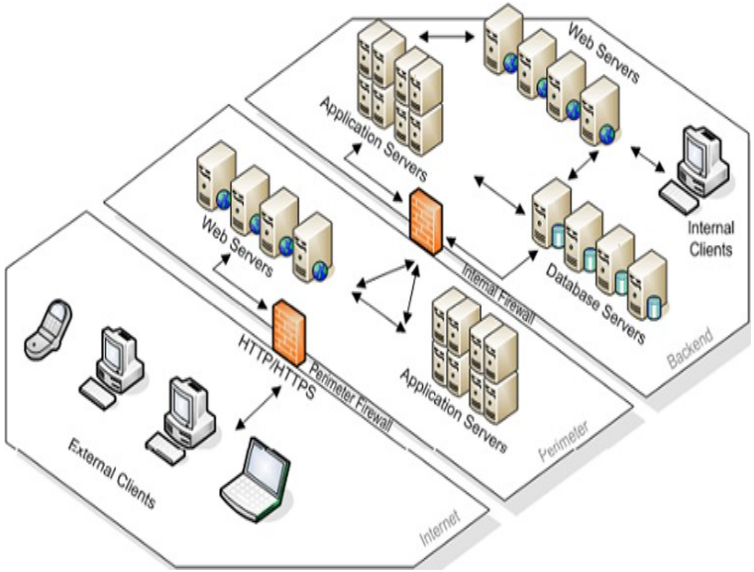
Tanta sangre que se llevó el río

Yo vengo a ofrecer mi corazón

No será tan fácil, ya sé que pasa. No será tan simple como pensaba

# MUCHACHOS NO TODO ESTA PERDIDO, ALGUNAS SOLUCIONES:

- TRABAJAR SOBRE LA ARQUITECTURA




- TRABAJAR SOBRE LA NORMATIVA
- RFC, ISO, NIST, OWASP…
  1) DESARROLLO
  2) TESTING
  3) PRODUCCIÓN

Information Security Inc.

Securing Bussiness since 2003

# EN QUÉ LOS PODEMOS AYUDAR NOSOTROS?

No hables a oídos del anecio,porque menospreciará la prudencia de tus razones. Proverbios 23

Information Security Inc.

Securing Bussiness since 2003

Information Security Management

# Gestión de Seguridad de la Información

Este tipo de consultorías de tiene su base en los aspectos funcionales de la Seguridad de la Información, trabajamos en **diseño, implementación, asesoramiento y capacitación** de **Programas Integrales de Seguridad.**

Information Security Inc.

Securing Bussiness since 2003

Ethical Hacking

# Aspectos técnicos de Seguridad de la Información

En este tipo de consultorías utilizamos **herramientas, técnicas y pruebas de hacking para identificar las vulnerabilidades** con el propósito de asegurar un sistema. Se **enfoca en simular técnicas utilizadas por los atacantes** para verificar la existencia de vulnerabilidades en el sistema, de forma ordenada y con la metodología OSSTMM, OWASP y EC-COUNCIL.

iSEC Information Security Inc.

Securing Bussiness since 2003

## Legal

**Asistencia y asesoramiento sobre Aspectos Legales** en temas como Delitos Informáticos, Sarbanes Oxley, Pericias Forenses, Investigaciones, Fraudes, Espionaje Industrial, Políticas de Recursos Humanos y la protección integral de intangibles.

## Computer Forensics

Brindamos **soluciones prácticas** que aporten elementos relacionados con la Seguridad de la Información desde el punto de vista legal, en este aspecto nos enfocamos en tres áreas conductoras: **incident response, computer forensics, investigación de fuentes abiertas.**

iCoaching

# #whoami

Christian Javier Vila

CTO Director de Tecnologías – ISEC Global Inc.

C|EH Certified Ethical Hacker, EC Council.

Sub Inspector (r) de la Policía de Seguridad Aeroportuaria

Especialista Investigación de Homicidios (MAT N° 510, ACRA)

Agente de Inteligencia (FAA)

christian.vila@isec-global.net

Investigaciones y estudios , exposiciones y congresos en Latinoamérica

- Identificación de Posición Absoluta Temporal de dispositivos móviles, Universidad INACAP Chile (Patagonia Hacking), enlace aquí.
- Herramientas digitales de fuentes abiertas para la investigación criminal (CIBSI 2017), enlace aquí.
- Ciberseguridad Financiera – Criptomonedas, Centroamérica, enlace aquí.
- SHODAN.io como herramienta de seguridad y pentesting, Google GDG Neuquén, enlace aquí.
- Análisis técnico del ataque de ransomware WannaCrypt (iCoaching), enlace al trabajo aquí.
- Técnicas de OSint “Le ocurrió a un amigo”, (Infosecurity), enlace al trabajo aquí.
- Ciberdelitos, desde la escena hasta la corte (Universidad de Río Negro, Infosecurity), enlace al trabajo aquí.
- Laboratorio “Metadata Exposed”, Instituto Prueger, Neuquén (ARG), enlace al trabajo aquí
- IoT Security, Google GDG Neuquén, enlace al trabajo aquí.

# eof()

powered by Cvila

Cada una de las partes protegerá la información obtenida durante el desarrollo del curso de la misma manera en que protege su propia información confidencial, haciéndose responsable por cualquier daño/perjuicio que se pudiera ocasionar por el uso indebido de la información accedida. Nuestros documentos entregables y papeles de trabajo serán de acceso exclusivo para los alumnos, quien podrá disponer para su uso de todos los entregables, que no incluyen metodología ni software utilizado.
PROHBIDA SU REPRODUCCIÓN PARCIAL O TOTAL DEL MATERIAL