

Ransomware: Un flagelo que nos concierne a todos.

Victor Chisava

Victor.Chisava@Kaspersky.com

Seminario Miércoles del Exportador - PromPerú

05 de Mayo de 2017

Lima, Perú

Contenido

Índice:

- 1. Conceptos Populares.**
- 2. Definición Técnica & Practica.**
- 3. Como Protegermos?**
- 4. Conclusión.**

Conceptos Populares

Conceptos Populares

Virus:

Cuando hay un problema desconocido en tu PC y no sabes a que culpar.

Anti-Virus:

Producto que debe resolver todos los problemas desconocidos.

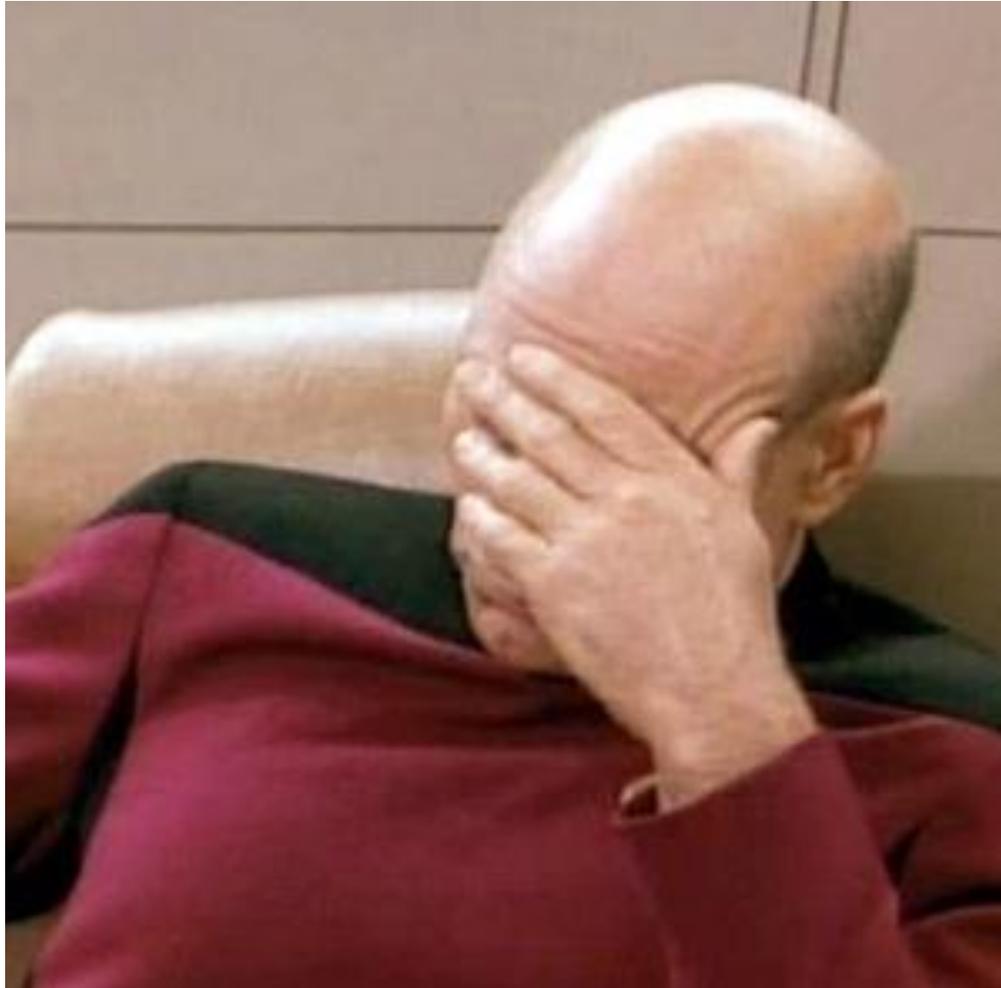
Ransomware:

Virus que daña la información la cual debe ser recuperada por cualquier anti-virus.

Gestión de Parches? Lo tenemos controlado!



Los Anti-Virus están para proteger a los usuarios!



En conclusión:



Que es el ransomware?

Definición Técnica (WikiPedia):

Un *ransomware* (del inglés *ransom*, 'rescate', y *ware*, por *software*) es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de *ransomware* cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Que es el ransomware?

Definición Practica

<https://www.youtube.com/watch?v=4jHsOrgrG-4>

Versiones

Windows



Certificado y Calificación Tributaria - Message (Plain Text)

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

95 20 15

View **Next >>**

The screenshot shows a Windows email client window titled "Certificado y Calificación Tributaria - Message (Plain Text)". The main content is a ransomware message from CTB-Locker. The message is displayed on a dark grey background with a yellow and black striped border. It includes a warning icon and a countdown timer showing "95 20 15". The message text is in Spanish and English, warning that personal files are encrypted and that the user has 96 hours to pay for decryption. The message also includes instructions to press "View" and "Next" buttons. The background shows a sidebar with "FILE" and "MESSAGE" tabs, and a list of messages. The bottom of the window shows a "No Items" message.

OSX

Restore your documents

Your documents have been corrupted!

Unfortunately your documents have been corrupted somehow. In the list below you want to restore documents" button at

We can restore your documents!

Don't you worry! We can help you restore your documents. As a matter of fact, we are the only ones that can help you with that. For a small fee we are willing to restore all your documents and guarantee you that it will never happen again!

Name

Payment

	Choose:
 	€30 <input type="radio"/>
	€30 <input type="radio"/>
Credit card 	€20 <input checked="" type="radio"/> 

SSL SECURE 

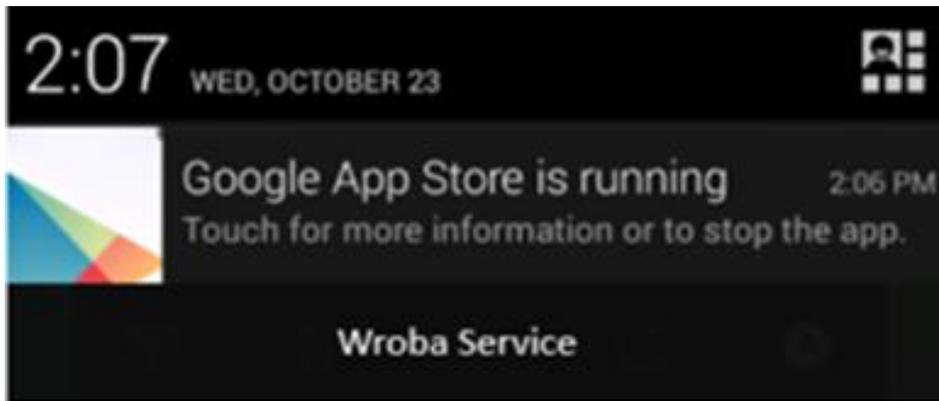
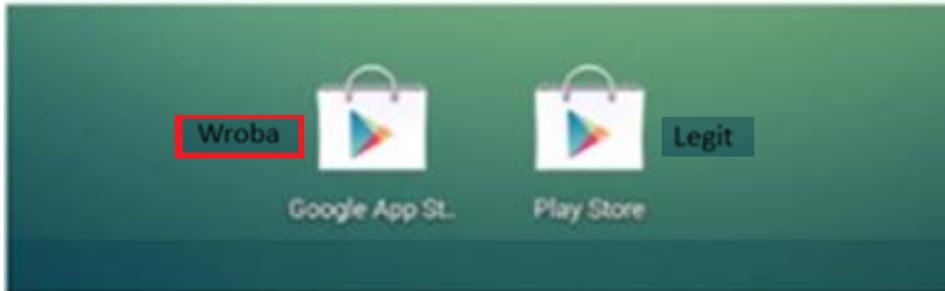
« Previous Next »

Restore documents »

Prueba de Concepto

- No cifra los archivos
- Cifra algunos archivos.
- Bajo impacto.
- Muestra una solicitud de rescate pero la característica es inoperativa... Por el momento.

Ransomware para Android



**За просмотр
запрещенного(Педофилия,Зоофилия
и т.д.) порно ваш телефон
блокирован!**



Все Фото и видео материалы с вашей камеры
переданны на рассмотрение.
Для разблокировки вашего телефона и
удаление метериалов
вам необходимо оплатить штраф 1000 руб. в
течении 24 часов
Для этого вам нужно пополнить Номер
+79147011354
В ближайшем терминале оплаты.
ВНИМАНИЕ: При попытке избежать штрафа
Все данные будут направлены в публичные
источники

Linux

SECURELIST

LOG IN

THREATS

CATEGORIES

TAGS

ENCYCLOPEDIA

SambaCry is coming

By [Mikhail Kuzin](#), [Yaroslav Shmelev](#), [Dmitry Galov](#) on June 9, 2017. 10:07 pm

RESEARCH

BACKDOOR

CRYPTOCURRENCIES

VULNERABILITIES AND EXPLOITS

WANNACRY

Not long ago, news appeared online of a younger sibling for the sensational vulnerability EternalBlue. The story was about a new vulnerability for *nix-based systems – EternalRed (aka SambaCry). This vulnerability (CVE-2017-7494) relates to all versions of [Samba](#), starting from 3.5.0, which was released in 2010, and was patched only in the latest versions of the package (4.6.4/4.5.10/4.4.14).

On May 30th our honeypots captured the first attack to make use of this particular vulnerability, but the payload in this exploit had nothing in common with the Trojan-Crypt that was EternalBlue and [WannaCry](#). Surprisingly, it was a cryptocurrency mining utility!

Como protegernos?

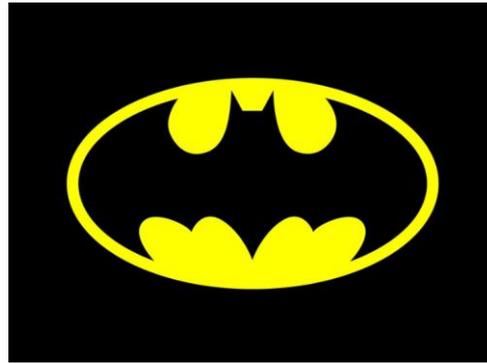
7 Pasos cruciales



Adquiera una solución:



INTELIGENTE



EFICIENTE



RAPIDA

Conclusión

Es mejor prevenir...



Enlaces de interés

[Mapa Global de Amenazas por País](http://cybermap.kaspersky.com/)

[**http://cybermap.kaspersky.com/**](http://cybermap.kaspersky.com/)

[Bitácora de Ataques Dirigidos](https://apt.securelist.com)

[**https://apt.securelist.com**](https://apt.securelist.com)

[Kaspersky Lab Blog](https://blog.kaspersky.com.mx)

[**https://blog.kaspersky.com.mx**](https://blog.kaspersky.com.mx)

[Kaspersky Lab Ransomware Decryption Tools](https://noransom.kaspersky.com/)

[**https://noransom.kaspersky.com/**](https://noransom.kaspersky.com/)

[Datos KSN en tiempo real](http://kaspersky-cyberstat.com/)

[**http://kaspersky-cyberstat.com/**](http://kaspersky-cyberstat.com/)

[Securelist](https://www.securelist.lat)

[**https://www.securelist.lat**](https://www.securelist.lat)

[Website Noticias de Seguridad](https://threatpost.com)

[**https://threatpost.com**](https://threatpost.com)

[No More Ransom Project](https://www.nomoreransom.org/)

[**https://www.nomoreransom.org/**](https://www.nomoreransom.org/)

Muchas Gracias!!

Victor M. Chisava

Presales Manager – Andean Region

Kaspersky Lab LATAM

Victor.Chisava@Kaspersky.com

Wire: Vimaro

Signal: (+57) 301 677-7018

www.kaspersky.com