UNA ESPERIENZA CON UN VIRUS CRYPTOLOCKER

Compusoft di Claudio Driussi – http://compusoft.it

In questo talk vedremo

*** Che cos'è un cryptolocker o ramsonware**
*** Brevi cenni di crittografia**
*** Come difendersi**

Incominciamo...

“Un virus cryptolocker crittografa i files del nostro computer per renderli inutilizzabili e chiede un riscatto per renderli nuovamente leggibili”

GLI ELEMENTI DI UNA INFEZIONE SONO

- Lista delle e-mail da contattare
- Il virus
- La richiesta di pagamento

LISTA E-MAIL

Tutti noi riceviamo malta spam.

Chi produce un virus ha la necessità di diffonderlo, per questo si procura una lista di e-mail da contattare.

Gli indirizzi e-mail vengono raccolti in modo lecito o rubati.

Se qualcuno ruba le nostre credenziali e-mail ha accesso alla nostra rubrica.

IL VIRUS

Il virus cryptolocker è diverso dagli altri virus il suo scopo non è quello di replicarsi, ma di essere eseguito una volta sola.

In pochi minuti deve essere in grado di leggere e criptare un numero enorme di files.

Di solito accede sequenzialmente ai dischi del computer attaccato e poi passa alle risorse di rete.

Di solito i files vengono rinominati e nella cartella vengono salvati i files in formato html e txt con le istruzioni per pagare il riscatto.

Se ci si accorge velocemente e si spegne il computer, può succedere di trovare metà disco criptato e metà in chiaro.

PAGAMENTO DEL RISCATTO

Il pagamento del riscatto avviene mediante bitcoins che sono una moneta elettronica non tracciabile

Se non ci sono alternative al pagamento, si devono acquistare i bitcoins e la burocrazia può essere fastidiosa. I venditori di bitcoins chiedono l'autenticazione del compratore e la validazione avviene con intervento umano.

STORIA DELLA CRITTOGRAFIA

La crittografia è un sistema che permette di offuscare un messaggio in modo che sia comprensibile solo a chi è autorizzato a leggerlo.

Si può utilizzare un gergo convenuto come ad esempio nel film Windtalkers:
https://it.wikipedia.org/wiki/Windtalkers

Oppure si può usare una chiave di codifica e decodifica:
http://www.html.it/guide/guida-crittografia-e-pgp/

CRITTOGRAFIA MANUALE

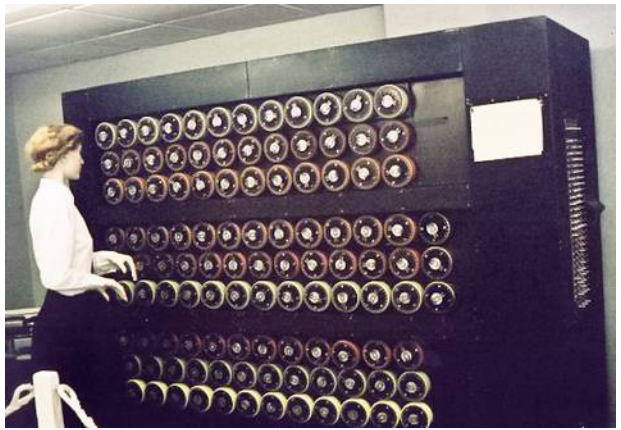
la trasposizione dei caratteri

Il codice Giulio Cesare

I codice di Vigenère

Altri codici

CRITTOGRAFIA ELETTORMECCANICA



La macchina Enigma e la Bomba di Turing

CRITTOGRAFIA COMPUTERIZZATA

DES e IDEA

Chiave pubblica e privata

L'algoritmo RSA

RSA è da 100 a 1000 volte più lento di IDEA

COME DIFERNDERSI

Gli attacchi riguardano soprattutto Windows.

Fare sempre i backup e controllare che funzionino.

L’anello debole è sempre il fattore umano.

LA POSTA ELETTRONICA

Gli attacchi arrivano per posta, **non aprire gli allegati sospetti** ed in caso di dubbio **non aprire gli allegati sospetti**.

Controllare il mittente spesso non è chi dice di essere

Windows non fa vedere le estensioni dei files spesso i files non sono del tipo che dicono di essere

Meglio Thunderbird?

LE CONTROMISURE

Gli antivirus sono poco efficaci perché i cryptolocker non sono virus classici.

Il canarino in miniera: https://www.cybereason.com

Pagare? Se serve si

I cryptolocker usano algoritmi deboli perché devono essere veloci

Meglio pagare chi fornisce servizi di cryptoanalisi che i delinquenti.

http://www.decryptolocker.it/

GRAZIE!

Domande?

Potente contattarmi:

- info@compusoft.it