LA MINACCIA RANSOMWARE NELLA PMI

Niente più riscatti ai Cybercriminali: tutto ciò che serve sapere per mettere al sicuro i dati aziendali

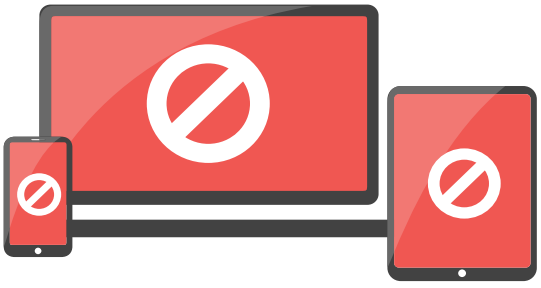
1 Cos'è il Ransomware?

Per **Ransomware** si intende una tipologia particolare di Malware, o software malevolo (non propriamente un virus) che **blocca il computer** o dispositivo mobile dell'utente-vittima o **cripta i file** in esso contenuti, **chiedendo un riscatto in denaro** in cambio della rimozione "indolore" di tali restrizioni. Nel più fortunato dei casi, effettuato il pagamento del riscatto viene fornita all'utente una chiave, un codice da inserire per disattivare il ransomware e riportare la situazione alla normalità.

Tipologie di Ransomware

Tutti i principali Ransomware ricadono in due categorie: i Blocker e gli Encryptor

I Blocker: Come suggerisce il nome, i Blocker bloccano l'accesso al sistema operativo o al browser, rendendoli inutilizzabili fino al pagamento del riscatto. Sono generalmente più facili da trattare rispetto agli Encryptor



I Blocker bloccano completamente l'accesso al dispositivo

Gli Encryptor: Più recenti e al giorno d'oggi più diffusi rispetto ai Blocker, non bloccano l'intero sistema ma criptano i file degli utenti salvati sull'hard disk. Differentemente da quanto avviene con i Blocker, i file degli utenti sono personali ed unici, quindi la limitazione posta dal Ransomware non può essere aggirata reinstallando il sistema operativo.

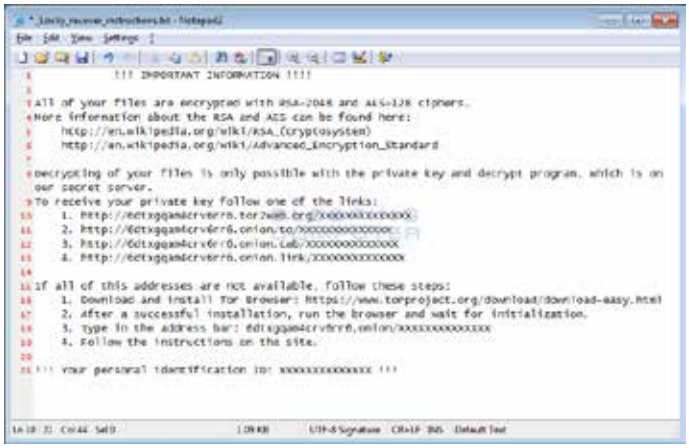
Gli Encryptor criptano i file presenti sul dispositivo

Cosa accade al Computer quando viene infettato?

Determinare se il proprio Computer o dispositivo mobile è stato infettato da Ransomware non è difficile. I segni principali che indicano la presenza di un'infezione da ransomware sono:

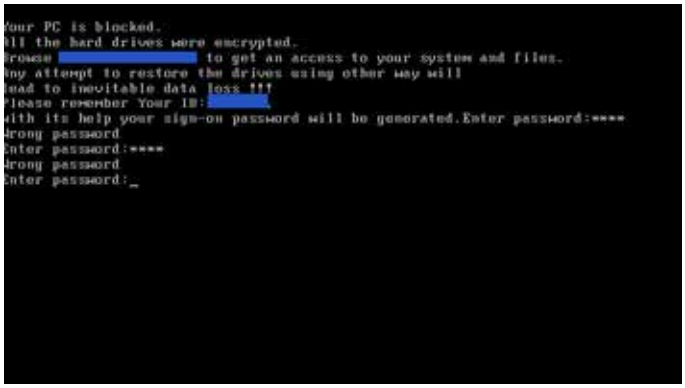
- **Blocco dello Schermo**
  Nel caso dei Blocker, si tratta di solito di una finestra o immagine a pieno schermo che non può essere chiusa, nella quale sono contenute le istruzioni per il pagamento del riscatto.

1 -Esempio di blocco dello Schermo



2 - Esempio di Ransomware Note

3 - Esempio di messaggio inviato dalle "autorità"



4 - Esempio di alterazione dell'avvio del computer

- **Cifratura e Ransom-Note**
  Gli Encryptor, impediscono l'accesso ai file criptati, ma non sempre bloccano lo schermo; generalmente lasciano un file, o "nota di riscatto" sulla macchina infettata, con le istruzioni per il pagamento.

- **Messaggi provenien i da mitten i fasulli**
  Non sempre i Ransomware chiedono apertamente un riscatto: più di frequente il messaggio popup che appare risulta provenire da mittenti "ufficiali": spesso questi sono le forze dell'ordi-ne (Polizia Postale, Guardia di Finanza...), che dichiarano di aver trovato materiali pedoporno-grafici o altri contenuti illegali sul computer e di averlo bloccato fino al pagamento di una "multa". Il malware è in grado di adattare il proprio messaggio alla posizione GPS dell'utente, risultando, ad esempio proveniente dall'FBI ad un utente americano e dalla Guardia di Finanza ad un utente italiano. Un altro possibile falso mittente è il computer stesso, che afferma di aver identificato un software senza licenza in esecuzione e richiede che venga effettuato il pagamento della licenza.

- **Alterazione del normale processo di avvio del computer**
  In questo caso il Ransomware interrompe il normale processo di avvio del computer infettato: un messaggio appare non appena il computer viene acceso, impedendo di caricare il sistema operativo per rimuovere l'infezione.

Caratteristiche del Riscatto

Non esiste un riscatto "tipico", la somma richiesta può spaziare dalle poche decine alle decine di migliaia di euro. Non è raro tuttavia che i cybercriminali chiedano una somma relativamente "bassa": in questo modo, è più probabile che la vittima preferisca pagare piuttosto che "sprecare" tempo e risorse preziose per cercare un'altra via (ciò è particolarmente accentuato quando ad essere colpite sono le aziende, in cui intervengono meccanismi ancora più complessi)

Il pagamento del riscatto può avvenire in diverse forme: portafogli online anonimi, pagamenti tramite cellulare, ma la più frequente è la **moneta criptata**, anche detta **bitcoin**, che rende più difficile tracciare il proprietario del portafoglio e migliora le probabilità per i cybercriminali di non essere rintracciati.

2 Dai Cybercriminali alla vittima: come si “contrae” il Ransomware?

Un mito da sfatare: il ransomware, ed i malware in generale, non sono esclusivi di chi adotta una condotta “sregolata” sul web, visitando siti poco raccomandabili ed aprendo tutte le mail di spam. **E’ facile essere infettati da un ransomware, e si è a rischio anche senza fare nulla di male.**

Chiunque può essere vittima di Ransomware.

Mail o Download da fonti sconosciute / false

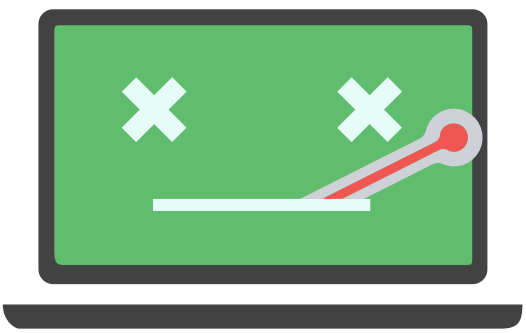
Il vettore di ransomware più comune è la **mail**. Essi possono presentarsi come allegati utili o importanti (una fattura urgente, un articolo interessante, un’app gratuita, una allegato da un amico). E’ sufficiente aprire l’allegato per infettare il computer

Driver Infetti

Il malware può propagarsi da un computer all’altro attraverso i dispositivi removibili (ad esempio le chiavette USB) se utilizzati su diversi computer.

Vulnerabilità

Vulnerabilità del sistema operativo, del browser delle app, della rete possono permettere al Ransomware di infettare il computer anche solo navigando in internet. Per questo motivo è molto importante aggiornare i software di sicurezza ed il sistema operativo. Le vulnerabilità possono anche essere frutto dell’infezione non “curata” di un altro malware.



Applicazioni infette

Alcuni software o applicativi possono contenere malware: barre degli strumenti installate sul browser, generatori di chiavi di attivazione per software, eseguibili di terze parti (file .exe), applicazioni di messaggistica, siti per la condivisione di file.

3 Ma quanto è effettivamente seria la Minaccia?

Un Fenomeno in Crescita

La minaccia del Ransomware ha conosciuto negli ultimi anni una crescita esponenziale, classificandosi tra quelle con il tasso di diffusione più alto, al punto di poterla quasi definire un'epidemia. Secondo le analisi **Kaspersky Lab**,se nel periodo 2014-2015 gli attacchi registrati sono stati 131.111, nel 2015-2016 il loro numero è salito a 718.536, risultando in pratica più che **quintuplicato**.
L'**Italia** non solo è nella top-10 dei paesi con la percentuale più alta di utenti colpiti dal Ransomware, ma è **tra i primi 3**, assieme a Stati Uniti e Germania.

PMI tra i bersagli preferiti

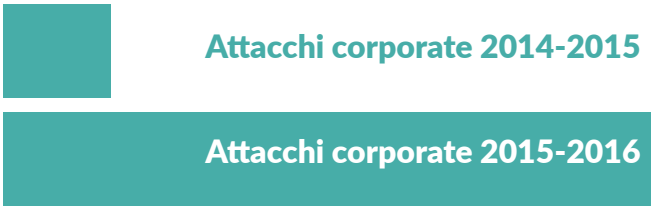
I dati sul Ransomware nella Piccola e Media impresa sono ancora più preoccupanti: secondo i dati raccolti da Kaspersky Security Network (KSN), nel periodo 2015-2016 il **numero di attacchi contro le aziende è aumentato di circa 6 volte** (da 27.000 a 158.000) rispetto al 2014-2015. I ransomware hanno quindi cercato di crittografare i dati di **un utente corporate su dieci.**
Nell'ambito corporate, sono soprattutto le piccole e medie imprese a pagare le conseguenze di questo aumento: rispetto alle grandi imprese, le **PMI** sono rese **più vulnerabili** dalla mancanza di sistemi di protezione sofisticati, e l'inaccessibilità ai dati causata dalle infezioni ransomware può determinare perdite significative o bloccare le attività, rendendo il pagamento del riscatto il "male minore" da sopportare per ripristinare al più presto la continuità del business.

718.536

Utenti vittime di Ransomware nel periodo 2015-2016

Gli attacchi Ransomware sono aumentati di 5,5 volte rispetto allo scorso anno

Italia tra i 3 paesi più colpiti



Gli attacchi Ransomware ai danni delle aziende sono aumentati di 6 volte rispetto allo scorso anno

Nell' ultimo anno, un utente corporate su 10 è rimasto vittima di ransomware

4 Come comportarsi se si è colpiti da Ransomware

COSA NON FARE:

- **Pagare il Riscatto:** Il pagamento del riscatto non è mai raccomandato, principalmente perché non garantisce affatto che i file siano effettivamente ripristinati. Può capitare, come nel caso del ransomware Ranscam, che i cybercriminali cancellino semplicemente i file invece di criptarli, chiedendo comunque il riscatto con la promessa di restituirli. Oppure possono verificarsi malfunzionamenti "accidentali" del ransomware stesso che rendono irrecuperabili i dati, anche con la chiave giusta. Secondo la ricerca KAspersky Lab, circa il 20% delle vittime di ransomware ha pagato, ma non ha mai avuto indietro i propri file. Il pagamento del riscatto costituisce inoltre una prova per i cybercriminali che il ransomware è un modo efficace per estorcere denaro, incoraggiandoli a perpetrare la loro attività e spingendone altri ad entrare nel business.

COSA FARE:

Per rimuovere il ransomware dal computer:

- Se il ransomware ha impedito completamente l'avvio del sistema operativo, utilizzare Kaspersky WindowsUnlocker, uno strumento gratuito in grado di rimuovere un blocker e di far avviare Windows.
- Utilizzare un antivirus ed antimalware per rimuovere il ransomware

Per ripristinare i file senza pagare il riscatto:

- Se era stato effettuato un backup, una copia di sicurezza dei file, ripristinarli da lì
- Se non era stato effettuato un backup dei dati, utilizzare un decryptor, ovvero uno strumento in grado di decifrare i dati criptati. Tutti i decryptor gratuiti creati da Kaspersky Lab si possono trovare su Noransom.kaspersky.com.

5 Prevenire è meglio che curare: come evitare di essere infettati

- **Effettuare periodicamente un backup** dei file importanti; è consigliabile avere due copie di backup dei file, una salvata sul cloud ed una fisica (su un hard-disk, su un altro computer, etc.)
- Premunirsi di **strumenti robusti per la protezione dei dispositivi. Kaspersky Lab** offre una varietà di soluzioni di sicurezza per mettere in sicurezza computer e dispositivi mobili, pensate specificamente per le imprese:

KASPERSKY lab

  - **Kaspersky Anti-Ransomware Tool for Business:** Strumento gratuito per la protezione dei dati aziendali da Ransomware e Cryptomalware, che funziona con la maggior parte dei software di sicurezza (non richiede di avere installata una soluzione Kaspersky per essere utilizzato).
  - **Kaspersky Endpoint Security for Business:** Protezione degli endpoint, controlli e sicurezza mobile

- **Mantenere aggiornati** i software, le applicazioni ed il sistema operativo.
- **Non aprire email ed allegati da utenti non attendibili, sconosciuti o sospetti** (ad esempio: l'autenticità di una e-mail improvvisa proveniente da un lontano conoscente con una frase del tipo "guarda le foto delle mie vacanze!" e un link per visualizzarle dovrebbe quantomeno essere messa in dubbio prima di cliccare sul link)
- **Rendere visibili le estensioni dei file** su Windows Explorer, per rendere più facile l'individuazione di file potenzialmente malevoli; tipi di file a rischio sono .exe', '.vbs' and '.scr'
- Se si ha il sospetto che il proprio computer sia infetto, **disconnetterlo immediatamente dalla rete** o dal Wi-Fi, per evitare che il malware si diffonda.

Sources:

http://www.kaspersky.com/it/about/news/virus/2016/kaspersky-lab-un-attacco-crypto-ransomware-su-dieci-colpisce-gli-utenti-aziendali

http://www.kaspersky.com/it/internet-security-center/threats/ransomeware

https://blog.kaspersky.it/ransomware-faq/9290/

https://blog.kaspersky.it/ransomware-blocker-to-cryptor/8444/

http://www.wsj.com/articles/ransomware-a-growing-threat-to-small-businesses-1429127403

http://www.kaspersky.com/it/about/news/virus/2016/Kaspersky-Lab-attacchi-crypto-ransomware-quintuplicati-con-718-mila-utenti-colpiti-in-un-anno

https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf

http://www.superantispyware.com/blog/2013/08/07/all-you-need-to-know-about-ransomware/