lineaEDP DA OLTRE 30 ANNI LA VOCE DEI CIO

SIGN IN / REGISTRATI
NEWSLETTER
Cerca... NEL SITO NEL NETWORK

TECNOLOGIA | MERCATO | CIO | PUBBLICA AMMINISTRAZIONE

LineaEDP »

RANSOMWARE : I VIRUS CHE CHIEDONO IL RISCATTO

Leggi più tardi

A cura di Alessandro Canella, Chief Operations Officer di ITcare

Cosa è un Ransomware

Un Ransomware è un virus che blocca del tutto o in parte l'accesso a un sistema informatico, e lo sblocca dietro pagamento di un corrispettivo, tipicamente su conti irrintracciabili.

L'approccio è **di nuova concezione**: invece di bloccare l'accesso al computer danneggiandolo (e come negli ultimi anni costringerci a chiamare un tecnico per ripristinare tutto), bloccare inesorabilmente l'accesso ai dati ed ai documenti rendendoli illeggibili.

Come teorizzato da Young e Yung nel 1997, i file vengono **"chiusi a chiave"** uno per uno con delle chiavi RSA (Rivest-Shamir-Adleman) : vere e proprie chiavi matematiche che richiedono anni per essere aperte e rendono i file illeggibili se non si ha la chiave principale per aprirli.

Anche se lo scenario era già stato teorizzato, le condizioni ideali di applicazione si sono verificate a partire dal 2010: dall'introduzione del **Bitcoin**, una valuta monetaria virtuale, sicura e irrintracciabile.

Grazie all'avvento del Bitcoin ed alla sua successiva diffusione, i soldi versati per gli illeciti sono pressochè al sicuro e le frodi su internet sono diventate realtà su larga scala e i primi ransomware hanno visto diffusione intorno al 2013.

Dai report Microsoft, **l'Italia è il secondo paese più colpito** dopo gli USA nel primo semestre 2016; Kaspersky stima che gli utenti corporate colpiti sono tra il 6 e il 13% grazie alla maggiore protezione dei network aziendali complessi e questo porta a una incidenza del fenomeno vicina al 90% sulle infrastrutture di privati e PMI.

Inizialmente studiati per attaccare Windows e i formati file più comuni (foto, documenti) nel corso del tempo sono uscite infezioni per tutti i sistemi più diffusi e con maggior numero di file attaccati per garantire maggior probabilità di successo.

ALTRO IN

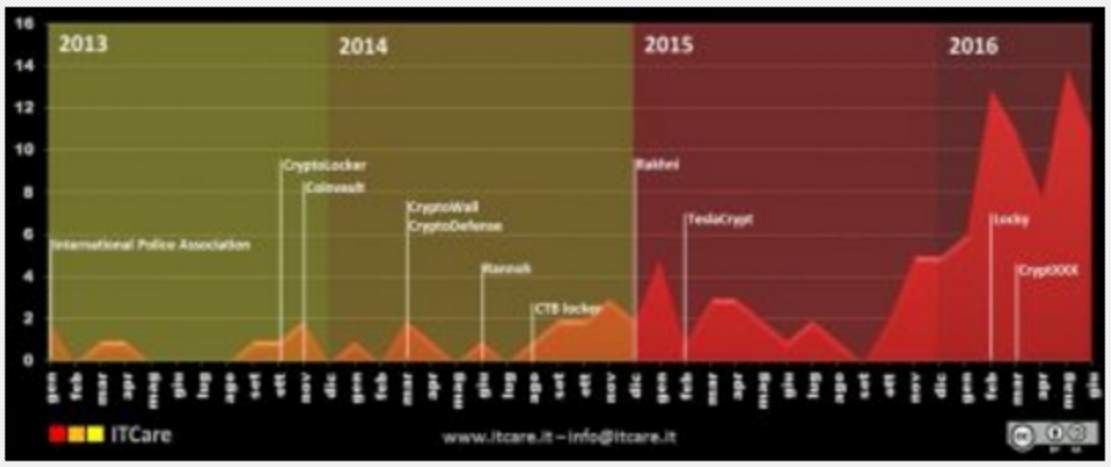
> Olimpiadi sicure... anche online
> Visibilità totale sull'esperienza utente nella gestione delle applicazioni
> CA Technologies ha a cuore il futuro
> Landesk lancia la nuova versione di Service Desk 2016
> Da Ca e Microsoft offerta per il cloud

Le stime del fenomeno Ransomware

La sola Kaspersky Security Network, riporta **più di 700mila infezioni rilevate nel 2015** : 280mila circa nel primo semestre e 500mila nel secondo mostrando quindi una crescita esponenziale dovuta anche al dilagare di nuove versioni.

I ransomware stimati in circolazione, secondo una interessante ricerca indipendente (Mosh @nyxbone and Roth @cyb3rops) a luglio 2016 sono circa 180 dei quali un 8% non completamente identificati.

Questa timeline rappresenta il **grafico delle nuove versioni mese per mese nell'ultimo triennio**, con evidenziati alcuni protagonisti significativi.



Il motivo di tanta diffusione è semplice: **AVAST** ha analizzato il trend di un ransomware di costo basso, stimando allo stato attuale circa 400mila dollari di ricavo nel solo primo mese. Secondo Symantec infatti, la media dei costi di riscatto è passata dai 250 euro nel 2015 ai **600** nel 2016 portando (secondo una stima FBI) il ricavo a circa **$1.6 milioni nei soli USA nel 2015**.

Come si contrae l'infezione

I ransomware usano gli stessi veicoli dei virus degli ultimi anni per attaccarsi utilizzando vulnerabilità già presenti nei sistemi : email di phising, codice Java o plugin di alcune pagine web (Adobe Flash in questo senso fa la parte del leone, quale veicolo di infezione); inoltre come riporta WhoIsHostingThis in alcuni casi l'infezione si propaga attraverso Spyware precedentemente presenti sul PC.

In agosto 2016 sono stati scoperti virus anche in email autorizzate e lecite di siti a diffusione mondiale.

Una volta installato il virus, richiede a un pool di server web di supporto – che i malviventi hanno approntato per tempo – una chiave specifica da abbinare a quel sistema e utilizzando i normali componenti del sistema operativo inizia a chiudere i file, partendo tipicamente dalle cartelle più usate per poi continuare la ricerca sull'intero sistema.

In molti casi pertanto – soprattutto nelle infrastrutture semplici quali PMI e utenti small business – vengono colpite **anche le unità di backup** tipicamente connesse e accessibili dal computer.

I file vengono pertanto bloccati uno ad uno e a una velocità di circa 5 Gb al minuto su un pc medio, **circa un quarto d'ora per perdere tutto**. In alcuni casi visivamente non si nota nulla finchè non si tenta di aprirli ma in ogni singola cartella appare un file aggiuntivo (file di testo, file HTML o immagine) che contiene le istruzioni per effettuare il pagamento.

Come si recuperano i dati

La prima cosa da fare è **spegnere immediatamente il PC infetto**, in modo da impedire al virus – se ancora possibile – di continuare a crittare i file; poi va **rimosso il virus e eliminata l'infezione** , ma il problema non è risolto.

Tutto quello che serve è un programma, scritto appositamente per ogni singolo PC, che rimuova le chiavi dai file bloccati. **Questo programma viene rilasciato dal programmatore del virus a un costo di qualche Bitcoin**, compreso solitamente tra i 300 e i 1000 euro. E' necessario aprire un conto in Bitcoin e versare dentro il corrispettivo in Euro, solitamente comunque la procedura è spiegata dal virus stesso.

La questione è se pagare o meno, e quella è soggettiva. Tipicamente effettuato il saldo in circa una giornata si riceve il software di sblocco, ma non sono rari i casi in cui l'hacker magari non restituisce nulla: potrebbe essere già su una spiaggia tropicale o in qualche prigione deciso a non collaborare. E' normale in questi casi infatti **chiedere una prova precedente al pagamento**, inviando allo stesso dei file di prova (possibilmente non contenenti indizi su quanto sono importanti i dati perduti per non solleticare ulteriormente il malfattore).

In alcuni casi le aziende di security sono riuscite a riprodurre il programma di sblocco e pertanto ci sono **speranze per il ripristino senza oneri che non quelli del tecnico**, ma questo tipicamente vale solo per poche versioni di Ransomware : tipicamente dove il programmatore ha creato virus non perfettamente funzionanti o dove la legge ha recuperato l'insieme delle chiavi e le ha rese disponibili a tutti.

In alternativa, i sistemi di **backup** del computer permettono di recuperare i files, ma solo se non sono stati attaccati dal virus stesso rendendo impossibile il ripristino.

Come ci si difende

Il primo concetto da comprendere è quello della **gestione della sicurezza**.

I ransomware stanno solamente sfruttando un problema noto ai vostri consulenti: la mancanza di protezione dei dati. Non si può dare la colpa a internet o agli hacker, stanno solo svolgendo bene il loro lavoro.

Tipicamente infatti, sia che stiamo parlando di un PC, che di una rete complessa, **le persone non danno il giusto valore ai propri dati**: fino a quando questi non sono irrimediabilmente persi, si da per scontato che essi siano disponibili, integri e affidabili.

Chi non ha adottato procedure di sicurezza, ha omesso di proteggere i propri dati semplicemente perchè non ha compreso effettivamente le problematiche di un sistema informatico.

Si da per scontato che le procedure impostate siano corrette e efficienti, devono svolgere la loro funzione: si è acquistato un sistema e quindi sicuramente sta lavorando bene.

La strategia di molti si basa su questa insana certezza, nessuno si è mai preoccupato di tentare un ripristino dei dati dal backup, o di controllare se l'antivirus è aggiornato: un sistema di protezione oltre ad avere un design adeguato, deve avere e un sistema di controllo e gestione dei problemi che possa garantire la **perfetta efficienza dell'infrastruttura**.

Un sistema di protezione efficace deve comprendere e controllare:

Area di impatto del problema: deve essere attiva una buona politica di segregazione dei dati: ognuno deve avere accesso ai soli dati che lo riguardano, gli stessi software di gestione e controllo del PC devono avere un proprio utente dedicato e ben identificato.

Superficie di attacco della minaccia: visto come si propagano i virus (sistemi obsoleti, email sospette, attacchi diretti, pagine web ecc..) è necessario: filtrare pagine e server web malevoli, filtrare con un antispam le email, controllare i file in ingresso e in uscita con un antivirus. Ma non solo: servono password complesse per ogni persona che accede al PC, aggiornamenti puntuali di Windows, software e sistemi di backup non esposti al contagio, sistemi antivirus efficaci e controllati.

Procedure di salvataggio e ripristino : ultimo dettaglio, ma non meno importante è la gestione della protezione e le procedure per ripartire dopo il danno. Fare il backup dei dati in modo manuale porta a dimenticarsene dopo averlo fatto due o tre volte, rendendolo de facto inutile. Tutte le procedure di sicurezza vanno gestite nei tempi e nei modi consigliati. Sempre.