RANSOMWARE E CRYPTOVIRUS

COSA SONO E COME DIFENDERSI

Luigi Duraccio

www.informatoreinformatico.it

Informatore Informatico

Inroduzione

Con queste poche pagine vorrei aiutarti a non perdere le tue informazioni aziendali subendo, inopinatamente, un attacco da un cryptovirus.

Il primo consiglio è di non fare da solo o fidarsi di consigli da sentito dire: affidati a personale esperto, preparato e competente.

Se invece hai già subito la cifratura dei dati, è probabile che siano irrecuperabili. I consigli che troverai potrebbero essere utili per non trovarti più nella stessa situazione.

Anche in questo caso il consiglio è di non fare di testa tua ma affidati a personale esperto e competente in modo da essere consigliato nel modo corretto.

Se non sai a chi rivolgerti o non trovi nessuno in grado di aiutarti, contattami.

luigi@informatore informatico.it

Una minaccia subdola.

Potresti aver già ricevuto, o magari lo hai sentito raccontare da colleghi o amici, delle mail da Enel o TIM, oppure fatture in allegato da fornitori che abitualmente non usano questo canale, o ancora da persone che conosci bene, il cui indirizzo è nella tua rubrica ma che non aspettavi. Ecco, potrebbe essere un tentativo di infettare il tuo pc, o la tua rete: stai per cadere vittima di un **Cryptovirus** o meglio di un **Ransomware**.

Prima di farti prendere dalla irrefrenabile curiosità di aprire il file allegato metti in moto i neuroni.

Ma che cos'è un Cryptovirus?

Si tratta di una minaccia, della famiglia dei Ransomware, il cui scopo è di insinuarsi nel tuo PC e prendere in ostaggio i tuoi dati al fine di chiedere un riscatto: "ransom" significa appunto riscatto!

I primi che si sono diffusi, ne avrai certo sentito parlare, sono stati conosciuti come "il virus della Guardia di Finanza", o "il virus della Polizia Postale". Si trattava di malware che bloccavano il PC dell'utente con una schermata e lo accusavano di aver rilevato sul computer materiale di carattere pedopornografico. Veniva inoltre fatta la richiesta di pagamento di una somma in denaro per far cadere le accuse.

Da due o tre anni siamo alle prese con una diversa tipologia di ransomware: gli **encryption ransomware**. Questi ultimi sono molto più **pericolosi**, molto più diffusi (siamo alle prese infatti con una serie massiccia di attacchi) e stanno diventando sempre più **difficili da rimuovere, resistenti** ai software di decifratura; sono conosciuti con i nomi **Cryptolocker, TeslaCrypt, CTB Locker, CryptoWall.**

Il meccanismo l'ho accennato poco fa: ricevi una mail con un allegato, non ci fai molta attenzione, doppio click sull'allegato e …. la frittata è fatta.

La momentanea distrazione o la mancanza di informazione al riguardo sono le condizioni che i malviventi, perché tali sono, sfruttano per infettare il pc, o tutta la rete, del malcapitato.

Ebbene si, hai letto bene: queste infezioni non si fermano al vostro pc ma **si estendono a tutta la rete**, ai server, alle cartelle condivise, i sistemi di archiviazione di massa (HDD esterni, ed altro): insomma **infettano tutto quello che è possibile infettare.**

Una minaccia subdola.

Se in questo momento ti stai nascondendo dietro considerazioni del tipo: "a me non è mai capitato", oppure "ma figurati se vengono a prendere di mira proprio me", oppure ancora " ma io sono a posto" senza curarti di verificare se sia vero, sappi che ….

…. la questione fondamentale non è se capiterà anche a te, ma quando capiterà!

Il mio scopo, arrivati a questo punto, è darti pochi **consigli pratici**, poche indicazioni o **alert**, per fare in modo che tu non debba trovarti nelle stesse condizioni di molti miei clienti: **senza poter utilizzare neanche un file salvato nel pc.**

Come opera un cryptovirus.

Ma come lavora e come si si diffonde un cryptovirus?

I criminali informatici, attraverso un invio massivo di posta elettronica, anche utilizzando dei PC zombie (pc di utenti ignari, infettati da malware), inviano mail ai destinatari presenti nella loro rubrica. Spesso cambiano, risultando così più efficaci: una volta TIM, una volta Enel, un'altra SDA. Sono casi reali di cui si è molto scritto anche sui quotidiani.

Una volta che per **errore o disattenzione** cliccate sull'allegato l'infezione si attiva.

Solitamente si tratta di un file .exe, contenente un eseguibile o un JavaScript. Spesso l'estensione .exe è nascosta. Una volta lanciato il contenuto del file .exe, questo si connette ad un server gestito dai criminali, detto server C&C o Command & Control. Anche in questo caso, probabilmente, si tratterà di un PC zombie, da dove verranno prese le chiavi per la cifratrura. La chiave pubblica verrà salvata sul pc della vittima e quella privata, che servirà per la cifratura, resta in mano al delinquente.

A questo punto inizia la fase di cifratura: vengono cifrate immagini, documenti, disegni, file di backup, ecc. e agiscono sia sul **PC locale** che su **tutte le unità di rete raggiungibili (server, NAS, condivisioni, ecc.).**

Terminata questa fase avviene il contatto. Il criminale informa che ha compromesso tutti i file e chiederà il pagamento di un riscatto per fornire la chiave privata e consentire la decriptazione dei file. Il pagamento viene chiesto in bitcoin in modo da rendere irrintracciabile il beneficiario.

Quanto siamo vulnerabili?

Come molti prima di te stai sicuramente pensando, a me non può capitare, io non apro allegati che non conosco, io non tratto dati sensibili, ecc, salvo poi trovarti in lacrime quando la frittata è fatta: è probabile che io non ti possa aiutare; sappi però che **far finta che il problema non esiste certamente non lo rimuove**. Spero solo che non sarai la prossima vittima!

Per iniziare devi sapere che eventi negativi come quelli di cui stiamo parlando, accadono essenzialmente per le **seguenti motivazioni**:

Mancanza di competenze o superficialità o distrazione.

Mancanza di sicurezza

Mancanza di procedure di ripristino

Mancanza di controllo

Ma esaminiamole un attimo ad una ad una

1.Mancanza di competenze o superficialità o distrazione.

Si tratta quasi sempre di mancanza di informazioni.

Questa condizione può però dipendere da un atteggiamento di pigrizia o di insofferenza verso l'informatica. E' un atteggiamento colpevole nel non voler conoscere, anche minimamente, gli strumenti che si usano quotidianamente per il lavoro, ma anche per la pigrizia o superficialità, ad esempio, nel leggere e comprendere i messaggi che ci da il pc: c'è una finestra che si apre in continuazione, anche se clicco su X: non si può levare? Ma cosa c'è scritto? Non lo so, non l'ho letta....

Ecco, questa situazione è quotidiana ed è, quasi sempre, la storia di un disastro annunciato. I cyber criminali conoscono molto bene questa situazione ed è di questo che si nutrono, e di questo approfittano.

2.Mancanza di sicurezza.

Gli antivirus sono spesso un optional: rallentano il pc, si dice. Questo generalmente accade su macchine vecchie con sistemi operativi obsoleti (ci sono ancora in giro Win XP!!), ma invece di aggiornare il parco macchine si disattiva l'antivirus. Al massimo troviamo antivirus gratuiti.

Non parliamo poi dei Firewall (questi sconosciuti!). La percentuale di aziende che possiede un firewall, o che sa di cosa si tratta è veramente imbarazzante!

3.Mancanza di procedure di ripristino

Anche qui quasi nessuno sa di cosa si tratti, o pensa di essere a posto ed invece non lo è, o non hanno niente. Ma cosa sono? Sono quelle attività o procedure da attivare in caso di evento negativo e consentono di ripristinare, appunto, la normale attività di una azienda od organizzazione. Il ripristino deve avere un impatto minimo, o almeno sostenibile, in termini di tempi e di costi.

4.Mancanza di controllo

Qui tutti fanno tutto e devono avere accesso a tutto! E' la situazione tipica quando si chiede di definire i livelli di autorizzazione all'accesso ai dati (file o cartelle). E' una caratteristica tutta italiana che personalmente ascrivo a quei limiti o difetti di cui abbiamo parlato prima: insofferenza nei confronti dello strumento, pigrizia.

Questo è un grande problema di cui nessuno sembra rendersi conto: quando tutti gli utenti hanno accesso a tutto (es. le cartelle condivise di un server), è sufficiente che il PC di un singolo utente sia compromesso per rischiare di compromettere i dati di tutti gli altri utenti.

Come ci si protegge.

Il primo concetto importante è che non esiste una soluzione sicura al 100%. E' possibile però **ridurre i rischi al minimo** ma soprattutto è possibile **evitare di perdere tutti i tuoi dati.** Ti darò 5 strumenti che ti serviranno per difenderti adeguatamente dai rischi di cui stiamo parlando e che sono:

Modifica dei Comportamenti

Assegnare Autorizzazioni e privilegi

Usare Antivirus e Antimalware

Installare un Firewall

Backup e piani di ripristino

1.Modificare i comportamenti

Il primo strumento ha a che fare con i comportamenti; è uno strumento importantissimo, peraltro **a costo zero**.

Come ho già detto **i comportamenti a rischio** - la insofferenza verso gli strumenti informatici, la pigrizia, la mancanza di attenzione, la fretta, ed anche la mancanza di competenze - sono i **fattori principali** su cui fanno affidamento i criminali informatici al fine di penetrare i vostri sistemi informatici e arrecare danni rilevanti.

Non è pensabile che un qualsiasi lavoratore maneggi strumenti di lavoro senza conoscerne le modalità di utilizzo, le procedure di sicurezza ed i relativi rischi. Non è accettabile quindi che un lavoratore che utilizzi strumenti informatici non sia **adeguatamente preparato!**

Abbiamo detto che il veicolo principe attraverso il quale si diffondono i cryptovirus sono le **email**; solo un po' di **attenzione** può ridurre al minimo il rischio. Quando ricevi una mail sospetta, fermati un attimo a pensare e fatti alcune domande: Chi è che mi manda questa mail? Lo conosco? Stavo aspettando una mail da lei o da lui? E' scritta in un italiano corretto? Il file allegato è un .pdf, .doc, .jpg, oppure nasconde una seconda estensione, .exe, .vbs, ecc…? Se dovessi avere un qualsiasi **dubbio, non aprire l'allegato!**

Ma che cos'è una "doppia estensione" e come riconoscerla.

Come ci si protegge.

Quando crei un documento, ad esempio con word, e la salvi chiamandola con un nome qualsiasi, es. report.doc, vedrai comparire una icona chiamata report con la estensione.doc nascosta. E' il modo predefinito con cui opera Windows.

Molti degli attacchi approfittano proprio di questa funzionalità.

Ora, i modi per verificare la vera estensione di un file sono vari: ti posso consigliare ad esempio di salvare l'allegato sul desktop del pc invece di eseguirlo direttamente cliccandoci sopra quando ti trovi ancora all'interno della posta elettronica; in questo modo sarà più facile verificare l'estensione. Se non ti fidi, contatta il tuo assistente informatico di riferimento che ti saprà dire cosa è meglio fare.

Anche **l'icona** ti può aiutare. Un file PDF sarà identificato con una icona come questa 

mentre un file exe avrà una icona diversa 

Ora che hai compreso quanto è importante prestare attenzione e quindi hai un primo strumento per difenderti, non può essere sufficiente l'attenzione. **L'errore è sempre in agguato**: per stanchezza, per fretta, per distrazione. Vediamo allora gli ulteriori strumenti di difesa.

2.Assegnare autorizzazioni e privilegi differenti

Anche questo è uno strumento a **costo zero**, o al massimo a bassissimo costo se ti dovessi rivolgere a qualcuno per le configurazioni.

Normalmente quando propongo di assegnare privilegi di accesso a cartelle o documenti condivisi mi si risponde o che in azienda non esistono segreti, o che "qui tutti fanno tutto". Non si tratta di tenere nascosti dei segreti, ma ancora una volta, di **proteggere il patrimonio della azienda**.

Il senso di assegnare autorizzazioni all'accesso risiede nella necessità di **evitare che**, chiunque dovesse prendere un ransomware, magari navigando per i fatti suoi su internet, **infetti anche il software che gestisce la contabilità e tutto il data base.** Anche gli accessi ai singoli PC andrebbero profilati autorizzazioni differenti in funzione di chi effettua l'accesso.

Come ci si protegge.

Ora sai anche quanto è importante utilizzare le password ed i livelli di autorizzazione: non prevedere un sistema di protezione con diversi livelli di autorizzazioni è una gravissima mancanza ed espone la tua azienda ad un rischio che potrebbe metterla in ginocchio.

Anche il **sistema di autorizzazioni**, però, non ti mette al riparo dalle infezioni, ma almeno evita che le stesse si propaghino per tutta l'azienda. E' un'arma **molto efficace e non usarla**, tanto più che non costa, **è una azione irresponsabile**.

3.Antivirus e antimalware

I sistemi antivirus sono la **prima linea di d**ifesa contro eventi negativi come quelli di cui stiamo parlando. Purtroppo molto spesso, anzi troppo spesso, quando consiglio un sistema antivirus le risposte sono:

- ma noi stiamo attenti
- tanto su internet non ci andiamo
- il costo per tutti i pc sarebbe troppo elevato
- il pc o il software gestionale funziona meglio senza
- perché devo pagare quando esistono quelli gratuiti

Magari anche tu rientri in una di queste casistiche. Mi sembra evidente che ci sono delle cose che devi sapere.

Innanzitutto i virus **non arrivano solo da internet**; la maggior parte delle infezioni e delle intrusioni si propaga attraverso la **posta elettronica** o attraverso **dispositivi** di archiviazione di **massa removibili (chiavette usb ed altro**).

In secondo luogo i rallentamenti del pc spesso dipendono dal fatto che la macchina è obsoleta con sistema operativo vecchio (win XP), o la stai utilizzando male (es. il desktop pieno di icone).

Riguardo al costo o ai software gratuiti ti invito a fare una riflessione: **quanto costa ricaricare tutti i dati della contabilità** se viene infettato il database del gestionale aziendale? Inoltre gli **antivirus gratuiti** sono sconsigliabili perché **non sono mai aggiornati** con la stessa frequenza, non degli antivirus a pagamento professionali, ma dei malware e ransomware.

Questi subiscono aggiornamenti continui ed **avere un sistema antivirus in ritardo con gli aggiornamenti equivale a non averlo!**

4.Firewall

Che cos'è un firewall? Per molti è una entità sconosciuta, molti altri conoscono quello di windows: in realtà parleremo di strumenti hardware che vengono integrati nella tua rete e che, per così dire, **dirigono il traffico e bloccano le richieste di accesso indesiderate.**

Cosa deve fare un firewall? Le tre funzioni fondamentali per cui il firewall è stato progettato sono:

- Fungere da elemento centrale dell'infrastruttura di sicurezza della rete.
- Agire come punto di controllo degli accessi per tutto il traffico, consentendo o negando l'accesso alla rete sulla base di regole precise.
- Eliminare il rischio dell'"ignoto" : viene consentito il traffico conosciuto e implicitamente negato quello non conosciuto.

L'efficacia con cui l'azienda opera dipende sensibilmente dalle applicazioni utilizzate dai dipendenti e dai contenuti che le applicazioni stesse trasportano. Consentirne semplicemente alcune e bloccarne altre potrebbe costituire un fattore inibitorio per il successo aziendale.

Col tempo l'evoluzione delle applicazioni utilizzate nelle aziende che si insinuano in spazi non controllati dai firewall, le necessità di semplificare le attività lavorative hanno portato come conseguenza che il firewall non è più in grado di svolgere al meglio la sua funzione. Ecco perché oggi si parla di Next Generation Firewall.

Non entrerò adesso nello specifico dell'argomento, limitandomi ad indicare, in generale, ciò che deve garantire un firewall in termini di prestazioni; approfondiremo l'argomento in un prossimo white paper.

In breve il firewall deve essere in grado di **garantire la funzionalità** per cui è stato progettato alla **velocità nece**ssaria per soddisfare le esigenze della azienda **senza compromettere** l'efficienza e la produttività.

5.Backup e piano di ripristino

Abbiamo detto che **non esite un sistema di protezione sicuro al 100%.** Bisogna quindi prendere in considerazione anche il caso in cui tutte le misure di sicurezza di cui abbiamo parlato fino ad ora non siano riuscite a fermare la minaccia.

Un backup efficiente ed un sistema di ripristino dati sono **l'ultima sicurezza** per essere certi di garantirsi un recupero dei dati, anche immediato!

Quando abbiamo detto che non è possibile recuperare i dati criptati in realtà abbiamo detto una inesattezza. Esistono numerose aziende che hanno costruito il loro business sul tentativo di recupero dei dati cifrati da cryptovirus; il recupero però non è sempre garantito in quanto, soprattutto ultimamente, si sono evoluti diventando **resistenti ai tool di decriptazione**.

Inoltre potrebbe capitare che **il costo** della operazione di recupero diventi **più alto del riscatto** richiesto **o troppo costoso** in assoluto. Le alternative a tua disposizione diventano quindi o pagare un riscatto o affidarsi al tentativo di recupero, spendendo in ogni caso molti soldi, con dei tempi di attesa per il completamento della procedura di diversi giorni, e senza la certezza di recuperare tutto.

In realtà, a queste due alternative, ne puoi aggiungere una terza, molto meno costosa. Con una spesa di **poche decine di euro** all'anno potresti garantirti il **recupero, quasi immediato dei tuoi dati** in caso di evento negativo anche se non legato direttamente ad un cryptovirus.

Stiamo parlando di un **sistema di backup** efficiente e di un **piano di recupero dati.** Stiamo parlando di **non aspettare che il disastro si compia ma di agire preventivamente.**

Ma quando un piano di ripristino può considerarsi sicuro, affidabile e efficiente?

La cosa più importante, per assicurarsi il recupero dei dati, non è avere un sistema di backup, o almeno non è solo questo. La cosa **più importante** di un sistema di backup infatti è **il piano di ripristino**:

avere i dati salvati da "qualche parte" senza sapere se e come recuperarli, equivale, evidentemente, a non averlo; non posso scoprire di dover risolvere una serie di problemi che non avevo previsto, nel momento in cui ho bisogno di ripristinare i miei dati!

Il piano di ripristino consiste nel stabilire le **procedure** da mettere in campo nel momento in cui si verifichi un evento dannoso e nel effettuare periodicamente delle **verifiche di recupero** dei dati simulando una situazione critica. Queste procedure pianificate e l'attività di recupero devono dare esito positivo al 100%: non è sufficiente quindi effettuare il test su un paio di file campione!

Una delle frasi che mi sento dire più di frequente, quando parlo di protezione e disponibilità dei dati, di ripristino è: ma noi facciamo il backup!

Ora, ammesso che sia vero, o ammesso che sia fatto come si deve, per intenderci non su una "pennetta" o su un semplice "hard disk esterno", se chiedo se e come viene fatto il ripristino (….??): "noi non lo abbiamo mai fatto ", "fino ad ora non ci è mai servito".

Se anche tu pensi questa sia una situazione verificabile nella tua azienda, **hai un serio problema!**

Ma, tornando a parlare di backup e ripristini, la cosa più importante che devi sapere, quindi, è che un **ransomware che attacca il PC attacca anche tutto quello che dal PC risulta raggiungibile**: Hard disk USB, pendrive, NAS, ecc. sono tutti dispositivi "a rischio", perché sono attaccabili direttamente dal cryptovirus. Per questo motivo **sistemi basati sulla semplice copia di file e cartelle**, che tu reputi importanti, su una chiavetta USB, su un disco esterno, su un NAS o altro, **non possono assolutamente essere considerati sicuri!**

Questo significa che corri seriamente il serio rischio di trovare cifrati, non solo i dati che pensavi di avere al sicuro, ma anche i backup indispensabili per il loro ripristino.

Ti do un **consiglio**: prima di tutto **scorda i backup su** qualsiasi **dispositivo USB**, poiché sarebbe troppo semplice corromperlo insieme a tutto il resto. Se vuoi una soluzione che costi poco puoi utilizzare un **NAS**; **assicurati** però col tuo tecnico di fiducia che sia di fatto **impossibile al virus accedere** alla cartella contenente i salvataggi, e che sia **in grado di effettuare un ripristino** in qualsiasi momento. Chiedi quindi di fare anche una **prova di ripristino!**

Come opera un cryptovirus.

Se per caso volessi, o avessi bisogno di un parere diverso, visto che sei arrivato alla fine della lettura, ti ho riservato **un bonus**: ho deciso di offrirti **un'ora di consulenza sull'argomento backup, e tre mesi di servizio di backup on line gestito.**

In pratica metto **i tuoi dati dentro una cassaforte blindata.**

Con il **backup gestito**, in pratica, penso a tutto io. Verifico gli esiti dei backup, effettuo i test di ripristino in modo trasparente e senza dover fermare il tuo lavoro, nemmeno per un'istante. Tutti i report li metterò a tua disposizione. Anche se ti servisse ripristinare un file, una cartella o un intero sistema, penserò io a tutto.

Ora che siamo al termine di questo ebook, voglio fare due precisazioni.

La prima è che il testo che hai letto è una prima edizione. Tratta un argomento che è in continua evoluzione. Non è quindi possibile essere esaustivi al 100%, potrebbero essere comparse nuove varianti di ransomware o potrebbero essere stati modificati i criteri di attacco.

La seconda è che non posso trattare argomenti e tecniche di difesa strettamente legate al tipo di infrastruttura presente nella tua azienda.

Le modalità di riduzione dei rischi e di difesa sono strettamente legate, ad esempio, al tipo di server, al tipo di software e/o alla versione utilizzata, ecc.

In riferimento a ciò rinnovo la mia disponibilità a fornire supporto e chiarimenti se ne volessi fare richiesta.

Per contattarmi i miei riferimenti sono i seguenti:

http://www.facebook.com/informatoreinformatico

Luigi6607

luigi@informatoreinformatico.com