# Broglio Riccardo

*CONSULENZA & ASSISTENZA Internet, hardware e software*


## Febbraio 2016 - CRYPTOLOCKER (E SIMILI): PIAGA DEL NUOVO MILLENNIO.

*Che cos'è Cryptolocker*

E' un Virus che appartiene alla categoria dei Ransomware, famiglia dei Malware. Il ransomware è un tipo di malware che una volta eseguito sul sistema della vittima ne prende il controllo (impedendone l'accesso o cifrando i dati) e chiede un riscatto per rimuovere la limitazione.

*Come Funziona*

Cryptolocker è a tutti gli effetti un Virus appartenente ai Trojans (Cavalli di Troia), che partono dalla loro infezione, criptando e modificando tutti (o in parte) i file dell'utente dei sistemi Microsoft Windows. Dunque mette a rischio tutti i Documenti, Desktop, Musica, Foto Video e tutti quei collegamenti personali nei files della cartella di sistema, nella nostra macchina e nelle cartelle del server direttamente accessibili da quel computer. Il tutto viene criptato generalmente utilizzando un algoritmo di cifratura asimmetrica RSA a 2.048 o 4.096 bit. Spesso i files originali vengono cancellati.

L'utente non conoscendo la chiave di decriptazione per ripristinare i files come in originale, non è in grado né di leggere, eseguire, aprire nessun file personale. Per sbloccare la cifratura e ovviamente decriptare definitivamente i files, all'utente non rimane altro che versare un riscatto (tramite finestre di alerts) preposto dagli autori del virus e dell'infezione, solo tramite il pagamento di somme di denaro definite spesso in bitcoins (in modo che i flussi di denaro non possano essere rintracciati), i quali possono raggiungere quote anche di svariate migliaia di euro, dipende dalla mole di dati infetti. All'utente quindi (PROBABILMENTE) viene rilasciata la chiave necessaria per decodificare i files "tenuti in ostaggio".

C'è chi sostiene che per risolvere o liberarsi del riscatto e dell'infezione dei files di Cryptolocker o ransomware, non ci sia altra soluzione che procedere al pagamento per ottenere la chiave richiesta. Questo in virtù del fatto che le condizioni e la robustezza dell'algoritmo di criptazione RSA è molto solida, tanto che adoperandosi con metodi "Brute Force" per conto nostro, ci si impiegherebbe anche troppo tempo per poter decodificare una semplice stringa (dipende sempre dalla potenza di calcolo che abbiamo a disposizione).

L'algoritmo RSA, come gli altri algoritmi asimmetrici, basa il suo funzionamento sull'utilizzo di una chiave privata e di una pubblica. Nel caso dei ransomware, la chiave pubblica viene conservata sul sistema dell'utente mentre quella privata viene mantenuta sui server degli sviluppatori. Ogni file crittografato con una chiave pubblica, può essere decodificato solamente da chi è in possesso della corrispondente chiave privata.

**La difficoltà maggiore sta nel fatto che, gran parte dei sistemi Anti-Virus, non rilevano questo tipo di Ransomware se non dopo ormai che l'infezione risulta operativa.**

*Alcuni sintomi (comuni a tutti i malware)*

- Computer è estremamente lento nell'utilizzo. Si avvia normalmente ma poi diventa inutilizzabile.
- Non si riesce a fare nessuna operazione in tempi accettabili.

la causa del malfunzionamento: un malware è attivo e sta sfruttando le risorse del computer per qualche scopo illecito.

Di fronte ad un malware di tipo CryptoLocker, la rimozione diventa estremamente delicata. Per vari motivi. Il principale è che se si rimuove completamente il malware non è più possibile procedere con il pagamento del riscatto e, quindi, rientrare in possesso dei files che sono stati crittografati.

Ad essere infettati sono non solo i privati, ma anche Enti, Aziende, PMI, Cooperative, grosse realtà commerciali ed in primis Istituzioni e Pubblica Amministrazione.


*Dott. Ing. Riccardo Broglio*

*Consulenza & Assistenza Hardware, Software e Internet.*
*Via Mazzini, 11 – 22070 – Guanzate (Co)*
*Cell. 338-8297320 Fax 02-70032418 e-mail: riccardo@broglio.it*
Cod. Fisc. BRGRCR71M07F205R - P.IVA: 02572040133 http://www.broglio.it


*Canali di diffusione ed infezione*.

Cryptolocker attacca principalmente i files della cartella personale dell'utente. Ma questo non accade se non viene eseguito un comando diretto disposto dall'utente. Visionare quindi il file infetto da Ransomware non comporta pericolo, ma diventa pericoloso se viene eseguito o decompresso. Quindi per agire, distribuirsi e infettare sfrutta diversi canali di contagio:

**– allegati di messaggi email Spam o Phishing.**

L'infezione di Cryptolocker si diffonde perché l'utente del computer ha aperto un allegato non sicuro. Se dubitate del mittente di un'email, non aprite allegati in essa contenuti. Se un'email contiene allegati sospetti, non li aprite. Se vi viene offerto, tramite email, un guadagno economico, dubitate del suo contenuto. Insomma, per essere sicuri dobbiamo dare retta ai consigli dei nostri genitori: non dobbiamo accettare caramelle dagli sconosciuti. Il problema è che, spesso, le caramelle ci vengono offerte attraverso falsi messaggi di posta provenienti da persone che conosciamo.

Molti ad esempio a riferimento di falsi ordini eseguiti da qualche sito e-commerce (amazon, Paypal, Ebay, Poste), a fatture di società quali Telecom, Enel, Gas o comunicazioni di false consegne dei corrieri più famosi a livello nazionale, opportunità di lavoro, comunicazioni amministrative da enti pubblici o governativi o privati, recupero dati o credenziali di account, MMS da un numero di cellulare, immagini o documenti da amici o conoscenti ecc…

Qualsiasi allegato ricevuto in posta elettronica DEVE essere considerato potenzialmente pericoloso, e valutato anche con l'apporto dell'intelligenza umana, dall'utente o, in casi dubbi, da un tecnico

- potrebbe essere un virus o un codice malevolo non ancora riconosciuto e di conseguenza fatto filtrare erroneamente dall'antispam e dall'antivirus
- potrebbe essere un virus che ha infettato il computer di un vostro corrispondente che è stato aggiunto alla white list dell'antispam (su vostra richiesta o di un collega)
- potrebbe essere un virus o un codice malevolo che vi è stato inoltrato da un ignaro collega attraverso la posta interna
- potrebbe essere un codice realizzato ad hoc e quindi tecnicamente non un vero e proprio virus, non riconoscibile come minaccia dai sistemi antispam / antivirus.

Gli allegati potenzialmente pericolosi si riconoscono dalle icone o meglio dalle estensioni cioè la parte del nome che segue il punto (es: in DOCUMENTO.DOC l'estensione è DOC, in FOGLIO.XLS è XLS)

Le estensioni pericolose più diffuse sono

- Programmi eseguibili .EXE, .CMD, .BAT, .SCR, .JAR, .PIF, .COM, .DLL, .MSC, .MSI, .HTA, .MSP, JS, .PS1, .PS2, REG, .LNK, .INF, .VB, .VBS, .VBE
- File di archivio .ZIP, .RAR perché ingannano più facilmente l'antispam e possono contenere gli altri tipi di file pericolosi
- Macro di office .DOCM, .DOTM, .XLSM, .XLTM, .XLAM, .PPTM, .POTM, .PPAM, .PPSM, .SLDM
- Documenti Office (Word Excel, Powerpoint) . DOC, .DOCX, .DOT-XLS, PPT

Premesso questo, non c'è ragione al mondo per aprire un allegato che abbia una estensione che non conosciamo e non c'è ragione al mondo per aprire un allegato di tipo eseguibile o macro (quindi che SIA EXE, CMD, BAT, PIF, SCR, JAR, WS, VBS, DOTM, XLAM, ecc.) Se si riceve un allegato con una estensione diversa da queste, il livello di attenzione DEVE ESSERE MASSIMO e NON SI DEVE ASSOLUTAMENTE APRIRE L'ALLEGATO.

Anche le estensioni ZIP, RAR, 7ZIP devono essere considerate quasi sicuramente PERICOLOSE e NON SI DEVE ASSOLUTAMENTE APRIRE L'ALLEGATO, al massimo in caso di lecita provenienza, chiedere supporto ad un esperto informatico

Per le estensioni conosciute (quindi che DOC, DOCX, XLS, PDF) l'attenzione deve sempre essere alta!!


*Dott. Ing. Riccardo Broglio*

*Consulenza & Assistenza Hardware, Software e Internet.*
*Via Mazzini, 11 – 22070 – Guanzate (Co)*
*Cell. 338-8297320 Fax 02-70032418 e-mail: riccardo@broglio.it*
Cod. Fisc. BRGRCR71M07F205R - P.IVA: 02572040133 http://www.broglio.it

Un altro modo di ingannare i sistemi e gli utenti è l'uso della doppia estensione. Se L'utente riceve un allegato che si chiama APRIMI.PDF.exe sarà portato a credere di avere a che fare con un innocuo documento PDF, in realtà è l'estensione presente DOPO il punto situato più a destra che definisce il tipo di file. Si tratta quindi di un eseguibile (EXE) che con ogni probabilità sarà stato nominato in quel modo con scopi fraudolenti.

Attenzione anche che a volte il virus non viene allegato al messaggio, ma in quest'ultimo viene incluso un collegamento ad un sito esterno. Se l'utente clicca sul collegamento, avvia il download del virus.

La provenienza del messaggio, in sé, non costituisce una garanzia. Tipicamente questi messaggi fraudolenti usano tecniche di mascheramento (spoofing) e di ingegneria sociale per apparire "normali", nascondere le caratteristiche che potrebbero mettere in allarme e indurre gli utenti ad aprirli.

– distribuzione di software pirata attraverso i più comini canali peer2peer (che spesso contengono malware) come emule, torrent, ecc

– utilizzo di vulnerabilità presenti nelle applicazioni, programmi o servizi web non aggiornati tempestivamente (Flash Player Java, ecc.).

*La prevenzione: unico strumento ottimale. Backup-dati*

I software Anti-Virus e Anti-Malware spesso sono inefficaci, quindi è comprensibile non possano fare al caso nostro. È quindi impossibile pensare di proteggere i sistemi di un'azienda, di uno studio professionale o di un ente pubblico con gli antivirus ed antimalware tradizionali, installati sui singoli client e che utilizzano il classico approccio basato sull'impiego delle firme virali. Per ottemperare in maniera adeguata ad una corretta campagna preventiva, questi sono i punti essenziali da seguire:

1. Impostare Backup Periodici su sistemi in rete NAS o unità removibili.

Il tutto va sistemato in dispositivi regolarmente protetti, in modo da permettere un ripristino pulito dei nostri dati nel caso si dovesse verificare un'infezione.

2. Usufruire della tecnologia VM (VMWare – Hyper-V, XenServer) o Cloud con versioning service.

Ove sia richiesta la versione e cronologia dei nostri files. Una soluzione ottimale per le pubbliche amministrazioni o altre strutture che adottano servizi Terminal, è quella di conformarsi ad uno standard di sicurezza per recuperare i dati in tempo reale, mantenendo varie versioni cronologiche dei files attraverso l'infrastruttura stessa. Da ultimo, osserviamo che i ransomware provvedono a cifrare solamente file che hanno determinate estensioni (PDF, DOC, DOCX, ODT, XLS, XLSX, JPG, AVI,…). Rinominare i file con estensioni astruse (ad esempio .PROTEZ) può aiutare ad evitare il blocco da parte di Cryptoloker nel malaugurato caso in cui dovesse insediarsi sul sistema.

**IN CASO DI INFEZIONE (AD ESEMPIO COMPARSA POPUP CON RICHIESTA DI RISCATTO), SPEGNERE IMMEDIATAMENTE IL COMPUTER – ANCHE BRUTALMENTE - E NON RIACCENDERLO. CONTATTARE SUBITO UN ESPERTO!!!**

*Un Virus in Mutazione*

Al giorno d'oggi con la potenza di calcolo disponibile, i virus non rimangono mai isolati e si evolvono ed aggiornano, mutando effetto e sinapsi, ottenendo più varianti come Cryptowall, CBT-Locker e l'ultimo di questi giorni (01/2016) TeslaCrypt sfruttando sempre di più in modo massiccio le campagne di phishing.

In questi primi giorni del 2016 si sta diffondendo un nuovo ransomware chiamato Ransom32. Ransom32 può essere creato/scaricato attraverso un sito raggiungibile tramite TOR. Ransom32, infatti, non è solo un malware ma rappresenta un vero è proprio servizio (RaaS - Ransomware as a Service) che consente di generare il proprio malware. Il servizio fornito è semplice ed efficace: chiunque può creare la propria copia personalizzata del ransomware purché disponga di

un indirizzo bitcoin (indirizzo che dovrebbe essere utilizzato dalla vittima per pagare il riscatto). Gli sviluppatori di Ransom32 guadagnano prelevando, da ogni riscatto pagato, il 25%. La peculiarità di questo ransomware sta nel fatto che è stato interamente sviluppato utilizzando una piattaforma che consente agli sviluppatori di creare applicazioni native per Linux, Mac e Windows utilizzando vari linguaggi di programmazione (HTML5, CSS3, Javascript a WebGL). L'utilizzo di tale piattaforma consente di creare un eseguibile Chromium che viene eseguito dal browser. Proprio questa caratteristica rende Ransom32 allo stesso tempo interessante e temuto: **il ransomware può essere potenzialmente eseguito su diverse piattaforme (Linux, Mac e Windows).**

*Come avviene l'infezione, come si propaga, come ci si accorge della presenza del malware, come vengono attaccati i files*

Cryptolocker (o uno dei sui simili) crittografa i dati presenti nei files, e molto spesso cambia l'estensione degli stessi, inoltre appaiono in ogni cartella infetta dei files che contengono le istruzioni da seguire per pagare il riscatto e procedere con l'eliminazione della crittografia. Questi files vengono creati in ogni cartella colpita dal malware. Il contenuto dei files criptati è completamente illeggibile. La crittografia sostituisce i caratteri standard con caratteri simili agli ideogrammi, utilizzando un algoritmo di crittografia univoco e impossibile da decifrare. Cryptolocker attacca i files in maniera da distribuire la diffusione su tutte le unità disco presenti nel sistema. Files presenti sul disco C:, nei dischi di rete Z; e nella chiavetta USB della firma digitale connessa al computer al momento dell'infezione. Cryptolocker si propagaimmediatamente in tutte le direzioni, aggredendo tutte le unità connesse al sistema. Cryptolocker agisce anche su files presenti nel cestino.

*Il recupero*

Il recupero è possibile SOLO dalla presenza di supporti di backup non connessi al momento dell'infezione. Un backup, per essere efficace, deve essere fatto su supporti che vengono connessi solamente per il tempo strettamente necessario all'esecuzione della procedura di backup, previa verifica che il sistema sia pulito.

*Come difendersi*

Per tutelarsi bisogna predisporre sul proprio computer:

- Un antivirus sempre aggiornato.
- Il firewall di Windows sempre attivato.
- La sicurezza che sul computer non siano installati programmi inutili e nocivi, come le toolbar o le estensioni per i browser Internet (Ask Toolbar e similari).
- L'esistenza di una copia di backup dei dati su un supporto normalmente disconnesso come un hard disk esterno o una pennetta USB. Tale supporto deve essere connesso al computer per il tempo strettamente necessario alla creazione o all'aggiornamento del backup.

Se si utilizza un sistema di Cloud come Dropbox, si tenga bene in mente che se i files vengono crittografati da un malware, vengono poi sincronizzati con il Cloud. Se compare quindi una richiesta di riscatto disconnettere immediatamente il computer da Internet, per tutelare i files sul server cloud. Un atteggiamento consapevole nell'utilizzo del computer, che presti la dovuta attenzione alle operazioni effettuate, che eviti distrazioni durante l'utilizzo dell'email e che non porti l'utente a scaricare programmi da Internet senza averne controllato attentamente la fonte.

**Senza backup, i files sono potenzialmente irrecuperabili ed il danno sarà ingente.**

La presenza di un backup sicuro è presupposto fondamentale per l'integrità dei dati non solo di un ufficio, ma anche di un singolo utente che utilizza per scopi personali il computer a casa. Solo seguendo TUTTI queste semplici regole potremo evitare il diffondersi di queste attività illegali e criminali di richieste di riscatto.

**Diffondete questo documento per aiutare i vostri conoscenti a difendersi da questi cyber attacchi.**


*Dott. Ing. Riccardo Broglio*

*Consulenza & Assistenza Hardware, Software e Internet.*

*Via Mazzini, 11 – 22070 – Guanzate (Co)*

*Cell. 338-8297320 Fax 02-70032418 e-mail: riccardo@broglio.it*

Cod. Fisc. BRGRCR71M07F205R - P.IVA: 02572040133 http://www.broglio.it