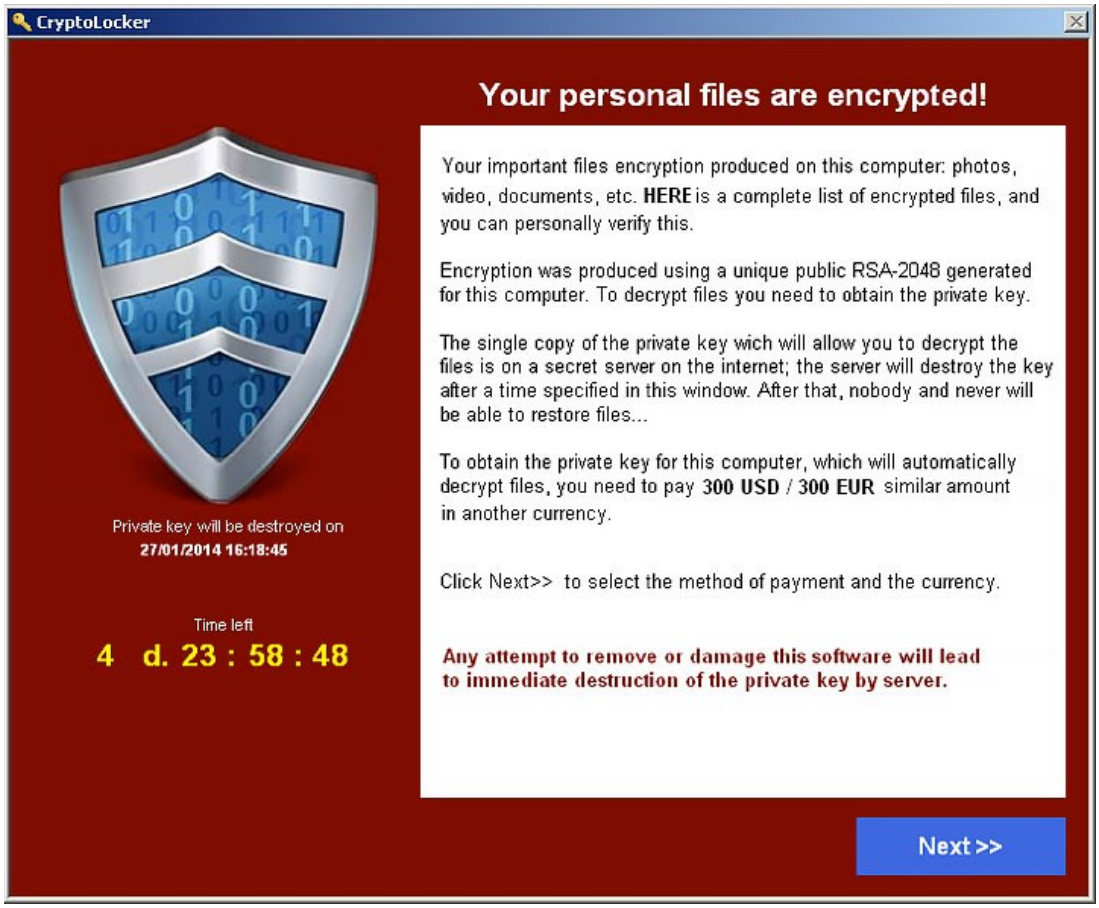
Cryptolocker e Ransomware

I criminali informatici lavorano continuamente nel cercare nuovi modi per diffondere malware e guadagnare soldi con richieste di riscatto, truffe, inganni, hijacking o intrusioni.

I virus informatici di oggi non sono più quelli che ti rovinano il computer costringendoti a reinstallare il sistema, sono invece molto più subdoli, restano spesso invisibili e non sono interessati a creare danni, ma a ottenere denaro o informazioni private.



Uno dei malware più diffusi in questi ultimi due anni sono i cosiddetti **Ransomware**, che si presentano come programmi **legittimi** capaci di prendere in "ostaggio" il PC.

CryptoLocker è il nome di un virus **Ransomware** (una variante è **Cryptowall**).

Quello che avviene sul computer dopo essere stati colpiti da uno di questi virus è che ***i file personali memorizzati vengono crittografati e resi inaccessibile***.

In altre parole ogni foto, documento Office, file di testo, PDF e qualsiasi altra cosa è salvata nella cartella dei documenti diventa illeggibile e bloccato perchè su questi file viene messa

una **protezione di crittografia** che è impossibile o quasi da rimuovere senza la relativa chiave o password.

Prof. Sergio D. ROSELLI

Il virus chiederà quindi di pagare una certa somma di denaro, di solito 299 Euro, per ricevere la chiave di decript e recuperare i files.

Se non si vuol pagare l'organizzazione criminale responsabile di questo virus, anche rimuovendo il malware, i file restano comunque inaccessibili e non più recuperabili.

L'estorsione operata da **CryptoLocker** è molto efficace infatti il riscatto non è richiesto per liberare il computer (che si libera comunque ripulendolo dal virus, *anche rimuovendo il virus, non c'è modo di recuperare i file bloccati*) ma alcuni **dati e file che vengono bloccati con una chiave di criptatura recuperabile solo** pagando.

Se i file vengono criptati da **CryptoLocker** e non si ha una copia di backup, essi saranno persi.

La prevenzione

A causa però degli effetti permanenti di questo virus, l'unica arma di sicurezza è la prevenzione, evitando così ogni possibilità di essere infettato. In ogni caso rimuovere i **Ransomware** è una procedura relativamente elaborata ma non difficile.

Prevenire il virus è quindi abbastanza semplice e non limita in alcun modo le attività sul PC.

1) **Avere un Antivirus aggiornato sul PC**

   Tutti i computer Windows hanno già l'antivirus Windows Defender installato che si aggiorna automaticamente. In ogni caso, qualsiasi antivirus si utilizzi, è importante tenerlo sempre aggiornato con le nuove definizioni virus.

2) **Avere il PC con Windows aggiornato**

   Significa che il servizio **Windows Update** deve essere attivo.

3) **Rimuovere o aggiornare i plugin dei browser**

   Se si utilizza una vecchia versione di plugin (Java, Flash, ecc.), le possibilità di beccare l'infezione aumentano esponenzialmente.

4) **Assicurarsi che il browser sia aggiornato sempre all'ultima versione**

   Chrome si aggiorna automaticamente ma per ogni altro browser conviene verificare se ci sono aggiornamenti da scaricare.

5) **Tenere attivo il Controllo Account Utente**

Il **Controllo Account Utente**, detto anche **UAC**, è quella funzione di Windows che blocca l'esecuzione di file fino a che non interviene l'utente a confermarla.

Per configurare il livello di attenzione del controllo account utente in Windows, aprire il *Pannello di controllo -> Account Utente -> Modifica impostazioni Controllo account utente*.

Si tratta del messaggio di richiesta che consente alla App (richiedente) di apportare modifiche al sistema e che compare quando si esegue un nuovo programma.

Disattivando UAC si perde il controllo su eventuali malware che tentano di eseguirsi automaticamente sul computer. Tenendolo invece attivo si può bloccare ogni azione di file pericolosi o non riconosciuti.

6) **Fare attenzione a non aprire allegati delle Email provenienti da indirizzi sconosciuti o che sembrano false.**

La Mail è ancora oggi il veicolo preferito dai virus. Sono sempre i messaggi falsi (Phishing), come quelli della Banca, di Paypal, delle utenze telefoniche e di energia o di ricevute per acquisti online (mai fatti), quelli che contengono sicuramente il virus. A volte sono allegati che, una volta aperti, infettano il PC, mentre altre volte sono solo dei link che portano l'utente ad aprire una pagina web con codice dannoso.

Cosa succede se il virus infetta il computer

Non appena il malware colpisce il computer, compare un messaggio che ci avverte del fatto che tutti i nostri file importanti del computer sono stati "**encrypted**".

Il messaggio continua dicendo che per avere i file indietro serve la chiave di decriptazione che si può ricevere pagando una somma di riscatto di alcunie centinaia di euro.

Nella videata c'è un timer a scadenza entro il quale pagare il riscatto con la somma richiesta, che aumenterà di valore se il tempo assegnato viene superato.

Provando ad aprire i file jpg, doc, pdf e altri nella cartella dei documenti, si riceverà un errore di accesso e di fatto elle cartelle con i files crittografati troveremo tre file di istruzioni chiamati: ***DECRYPT_INSTRUCTION.txt, DECRYPT_INSTRUCTION.html, DECRYPT_INSTRUCTION.url*** che riportano le istruzioni per pagare il riscatto.

E' possibile ***evitare l'effetto del virus*** **quindi l'estorsione** spegnendo e staccando la connessione di rete del computer non appena ci si accorge dell'infezione.

Prof. Sergio D. ROSELLI

Il riscatto

Il riscatto si paga in **BitCoin**, la valuta digitale anonima che rende i trasferimenti di denaro non tracciabili. Bisogna quindi andare in uno dei siti dove comprare BitCoin e seguire le istruzioni per il pagamento.

Pagando si ottiene la password per l'accesso ai file bloccati sul computer (gli autori del malware non dovrebbero avere alcun interesse e nemmeno alcun vantaggio a ingannare gli utenti).

Se non si volesse cedere all'estorsione, è opportuno :

- riavviare il PC in modalità provvisoria
- usare **rKill** per fermare i processi esterni a Windows
- scansionare con **Malwarebytes Antimalware** e con **HitMan Pro** per cancellare ogni traccia del malware.

Per saperne di più su come rimuovere Cryptolocker e sul processo di pagamento richiesto per sbloccare i file, andare al sito Bleeping Computer oppure sul **sito DrWeb** è possibile verificare se il tipo di crittografia usata dal **trojan cryptolocker** che ha colpito il nostro PC è più o meno difficile da decifrare. Sul sito **Emsisoft** è possibile invece reperire uno "**sbloccatore"** per recuperare i file criptati dai virus **HydraCrypt** e **UmbreCrypt**.