# BITCOIN. WHO IS?

di Carlo G. Alvano

Un brutto giorno, accedendo al mio computer apparve un messaggio sconvolgente: ABBIAMO CRIPTATO I VOSTRI FILE CON IL VIRUS CRYPTOLOCKER !!! I vostri file importanti (compresi quelli sui dischi di rete, USB, ecc): foto, video, documenti, eccetera, sono stati criptati con il nostro virus CryptoLocker. L'unico modo per ripristinare i file è quello di pagare noi in bitcoin. In caso contrario, i file verranno persi". Seguivano le istruzioni per pagare il riscatto e questo poteva avvenire solo con una moneta elettronica virtuale chiamata "bitcoin" da versare su indirizzi informatici non rintracciabili e non in una qualsiasi banca. Cosa che naturalmente non feci ma con ciò non ottenni i file sequestrati. Né la Procura, alla quale mi rivolsi, e la Polizia Postale incaricata delle indagini furono in grado di individuare gli estorsori.

Provate ad immaginare il danno. L'esistenza di noi tutti non può fare a meno delle nuove tecnologie e se uscendo di casa abbiamo dimenticato il cellulare, oppure tastandoci non lo troviamo addosso, ci prende il panico. Tutta la nostra esistenza dipende dalle nuove tecnologie tanto che il nostro Paese ha istituita l'Agenzia per l'Italia digitale. Anche l'iscrizione a scuola dei nostri figli o la semplice richiesta di un passaporto, avviene *on line*. Ed è così che in questo nuovo sistema all'insegna del "fai da te da casa", vecchi reati si riciclano e diventano nuovi con nomi nuovi di origine anglosassone i quali a loro volta hanno decretata la fine della bonifica fascista della lingua italiana che avrebbe dovuta essere priva di parole straniere.

Non si dice più rapimento ma *ransomware* ed il soggetto rapito non sono cose o persone ma *files* elettronici, il pagamento per la liberazione non avviene con moneta a corso legale ma con criptovaluta, una moneta nuova elettronica che sfugge a qualunque tipo di controllo. La più famosa si chiama bitcoin, il suo simbolo è ฿ una lettera "b" maiuscola attraversata da una barra verticale o anche due.

Si tratta di un'unità di misura che attualmente alla data del 14/9/2017 vale la stupefacente somma di 3.198,00 euro ed all'inverso con 1 euro si acquista appena lo 0,00031 di un BTC. Questo per dare semplicemente un'idea dell'enorme importanza che ha assunto dal 2009 questo fenomeno mondiale che sta sconvolgendo le economie di tutto il pianeta ed è per questo che ne parlo.

Non si sa chi sia l'inventore, ma per convenzione si fa riferimento allo pseudonimo Satoshi Nakamoto per indicare una persona, di cui non si conosce il sesso, il quale nel 2008 con questo nome pubblicò per primo il protocollo di trasmissione a distanza di quella che viene definita una moneta, ma tale non è perché non si vede e non si tocca, né viene emessa da alcuna banca centrale, non necessita di banche intermediarie e viene negoziata solo da un computer ad un altro. Si è cercato anche di capire se si tratta di moneta nel senso comune della parola oppure di una merce di scambio come avveniva nel baratto. Caratteristica questa che rende il bitcoin sovranazionale ed esportabile al nostro seguito in qualunque parte del mondo senza affrontare dogane. Basta un pc o uno smartphone con una linea internet per fare pagamenti o acquisti. Al riguardo di recente si è sperimentata una linea internet su satellite per fare una transazione in bitcoin nel bel mezzo di un deserto.

Ciò non esclude che è anche possibile prelevare contanti o versare contanti nel proprio conto bitcoin, i quali vengono convertiti secondo il tasso di cambio vigente in quel momento, con cambio in altra moneta, da un qualunque sportello bancario automatico, i c.d ATM (Automated Teller Machine), separato e non integrato con Visa, Mastercard o altri circuiti di pagamento utilizzati dagli istituti bancari. Il primo BTM installato in Italia funziona ad Udine dal 20 febbraio 2014.

A differenza del denaro contante, che viene stampato da un'autorità centrale che ne garantisce l'autenticità e distribuito da banche che funzionano da intermediari garantendone la circolazione mediante bonifici a pagamento, l'utente bitcoin deve fare tutto da solo con programmi di software specifici senza rivolgersi ad alcuno. È già accettata come mezzo di pagamento da grossi gruppi mondiali tipo AMAZON o da circuiti di carte di pagamento quali PAY PAL. Nessun Paese, ha dichiarata illegale questa criptovaluta, tranne la Cina pochi giorni orsono, al solo scopo però di poterne creare una propria in esclusiva per finanziare i suoi progetti statali, con questo dimostrando di crederci e di aver colte grandi opportunità. L'Estonia ritiene che il bitcoin sia un mezzo di pagamento, e che di conseguenza le operazioni finanziarie dovrebbero essere soggette a tassazione, ma non si capisce come, visto che non è individuabile. Nel 2015 è stato installato in Estonia il primo BTM ed è stato anche il primo negli Stati baltici. Utilizzando tale macchina, si possono fare solo operazioni in bitcoins. Il 24 agosto scorso, l' Estonia ha presentato un progetto per battere la prima criptomoneta di Stato chiamandola Estcoin, che dovrebbe affiancarsi all'euro in una sorta di mercato parallelo. Servirebbe a raccogliere fondi per avviare progetti innovativi, condivisi tra pubblico e privato mediante lo sviluppo di un sistema finanziario digitale definito ICO (Initial Coin Offering), un'offerta pubblica di moneta, che funziona grosso modo come l'offerta pubblica iniziale per le aziende che intendono quotarsi in Borsa. Questo sistema è molto utilizzato dalle *start up*.

Ad ostacolare l'espansione della nuova moneta, si profilano all'orizzonte nuovi problemi che per forza di cose costringeranno le autorità monetarie a dover trovare dei provvedimenti. A parte la questione che vengono scavalcati nel monopolio che detengono, stati canaglia come la Corea del Nord per aggirare le restrizioni commerciali adottate dal Consiglio di Sicurezza dell'Onu stanno incrementando gli attacchi degli hackers per rubare criptovalute sui mercati, forti della difficoltà di essere rintracciati. Uno dei metodi, oltre quello subito da me del "*ransom payment*", consiste nell'invio di mail contenenti dei *malware* al personale dei mercati di scambio. L'FBI ne è più che convinto e sta esaminando il cyber-attacco da 81 milioni di dollari alla New York Fed. Nella Corea del Sud sono stati sottratti 3.800 bitcoin che, al cambio odierno, varrebbero circa 15 milioni di dollari.

Il problema più grosso consiste però nel fatto che ad essere attratti da queste possibilità è sempre di più la cyber criminalità comune. Con 100 dollari in bitcoin, puoi acquistare un programma di malware e inviarlo ai computer delle vittime, di solito elenchi mail sottratti in rete e sui riscatti incassati paghi il 15 per cento al venditore.

Una delle forme più usate sono le bollette dei servizi che imitano quelle emesse da Telecom o Enel, contenenti allegati con il virus che se si aprono infettano il pc come da me descritto. Molti utenti ormai sono accorti a non aprire mail sospette, tuttavia ultimamente gli attacchi sono diventati di massa perché alla portata di tutti. Una banda criminale ha rubato alla NSA l'agenzia americana un programma per l'attacco informatico ai russi che si diffonde facilmente attraverso la rete interna di una organizzazione, e non ad un singolo pc, impedendogli di funzionare. Questo programma è stato immesso gratuitamente sulla rete e molti lo stanno utilizzando come una manna dal cielo.

Dopo l'estorsione subita mi sono rivolto all'FBI che aveva sgominata una banda ed era venuta in possesso dei codici di decifratura. Per intenderci, i dati che abbiamo, non vengono portati all'esterno, ma pur restando all'interno del nostro pc che ne diventa la prigione, non sono più visibili perché criptati con un algoritmo molto complicato. L'unico modo è quello di venire in possesso del codice di decifratura,(quello promesso in corrispettivo del pagamento) che a sua volta è un altro algoritmo, come dire l'antidoto al veleno che è diverso per ogni

cifratura. Purtroppo sono stato sfortunato perché l'FBI non aveva quello specifico occorrente a me.

L'unico modo per difendersi è quello di effettuare un backup giornaliero di tutti i dati che si elaborano e mantenerli su un hard disk esterno, che può anche essere semplicemente una chiave usb con memoria adeguata alle nostre esigenze. Cosa che da quel giorno faccio, dopo aver dovuto resettare tutta la mia rete aziendale ed aver cercato di recuperare presso i destinatari quanto più possibile degli archivi di tanti anni. Vi assicuro è un grosso lavoro con notevole dispendìo di tempo e danaro. Altra precauzione è anche quella di togliere l'alimentazione elettrica ai pc dopo l'uso, perché l'intrusione può avvenire attraverso il nostro indirizzo IP su internet. Ma attenzione perché il malware sta già arrivando sugli smartphone e lì non vi sono fili che tengano. Bisogna imparare ad essere vigili ed attenti, e la raccomandazione va soprattutto ai meno tecnologicamene preparati.