

Un tempo colpivano le persone oggi i dati. Il business dei sequestri cibernetici

Pubblicato: Lunedì 20 Settembre 2021



La notte del 9 luglio 1973 **Paul Getty III**, sedicenne, viene sequestrato a Roma, tra piazza Navona e Trastevere, dove di solito vende collanine fatte con le sue mani. L'autenticità del rapimento è però messa a lungo in discussione a causa della personalità e stile di vita del giovane. Si ipotizza che lo scapestrato hippy chic, erede di una delle famiglie più ricche del mondo, con una certa confidenza con la droga, abbia inscenato il rapimento per spillare soldi al nonno **Paul Getty II**. Questi trasmette da Londra che non verserà una lira di riscatto: «Ho molti nipoti, se pago per uno mi toccherà pagare per tutti». (Foto di Pete Linforth da Pixabay)

La svolta arriva il 14 novembre, quando alla redazione de *Il Messaggero* viene recapitato un plico con un ciuffo di capelli e un orecchio (spedito 28 giorni prima per posta!). Otto giorni dopo una telefonata avverte il centralinista de *Il Tempo*: “Ci sono alcune fotografie di Paul sull’autostrada Roma-Napoli, vicino a Valmontone. Cinque polaroid dentro un barattolo. Le foto del ragazzo con l’orecchio mozzato”. C’è anche un messaggio: «La famiglia più ricca del mondo dimostra di essere anche la più Caina». E i rapitori minacciano altre mutilazioni.

Dalla sua reggia il nonno finalmente cede. La madre tratta con i sequestratori, il 12 dicembre un emissario dei Getty consegna il denaro: **un miliardo e 700 milioni di lire**. Settantadue ore dopo, il ragazzo viene rilasciato fra la Basilicata e la Calabria, vicino a Lauria.

IL NUOVO BUSINESS DEI SEQUESTRI

Dopo quasi 50 anni, **i sequestri nell'era dell'economia basata sul valore dei dati** hanno cambiato obiettivo e tecnologie. Dalla selezione accurata dei ricchi di allora, oggi tutti siamo diventati potenziale mercato dei sequestratori. Ad aprile 2021 un piccolo editore di libri scolastici del mid-west degli **Stati Uniti** riceve un attacco da un **hacker** di nome **Woris**, che minaccia di bloccare tutti i siti e le attività online di servizio alle scuole primarie, i clienti principali dell'azienda, se non viene pagato un riscatto di **1,75 milioni di dollari**. Per aumentare la pressione, Woris minaccia di contattare le famiglie per informarli della propria intenzione di passare ai pedofili informazioni per creare identità false con cui creare documenti che permetterebbero l'accesso alle scuole come se fossero parenti o genitori.

L'hacker opera con la complicità di **DarkSide**, un gruppo russo che fornisce servizi di hackeraggio ai criminali di tutto il mondo. È disarmante leggere il tenore delle conversazioni chat di servizio utilizzata per i "clienti". Woris scrive: «Mi sono divertito a vedere la perversità della mia anima quando ho inventato la finta storia dei pedofili». E ancora: «Il pannello di controllo del vostro servizio di assistenza è difficile da usare e mi fa perdere un sacco di tempo».

In questo momento, anche **hackers con capacità tecniche mediocri** possono trasformarsi in una minaccia alla sicurezza nazionale degli Stati, perché grazie a servizi come quelli di **DarkSide**, nel frattempo chiuso e sostituito da altri come **BlackMatter**, la barriera intellettuale all'ingresso è bassissima. Come Microsoft fornisce "software-as-a-service", così le **bande criminali forniscono assistenza tecnica agli hackers**, negoziano con chi viene attaccato, **processano i pagamenti in criptovalute**, forniscono le campagne di comunicazione personalizzate per fare pressione, e, se serve, bloccano altri sistemi secondari a supporto della richiesta di riscatto. Hanno **un listino prezzi che va da una commissione del 25%** per riscatti fino a **500 mila dollari** e si abbassa **fino al 10% per importi oltre i 5 milioni**.

Durante gli anni del Covid, **le attività dei sequestri cibernetici** sono cresciute enormemente, trasformandosi in un "**business**" molto strutturato. C'è chi "buca" le reti di protezione, altri che si occupano di **prendere il controllo dei sistemi e dei dati**, chi fornisce il supporto tecnico per gestire il riciclaggio del riscatto; ci sono perfino quelli che si occupano delle relazioni con i media e gestiscono i rapporti con le autorità di sicurezza.

COME FUNZIONA UN ATTACCO CYBER

La prima cosa che accade è che la vittima riceve un messaggio sullo schermo con istruzioni e minacce blande, in cui si spiega che i computer, i server e i dati sono stati criptati e cancellati tutti i back-up. Per **decriptare le informazioni**, bisogna accedere ad un sito web attraverso una chiave speciale che viene comunicata. Il messaggio seguente è che ogni tentativo di recuperare o sbloccare autonomamente i dati rischia di danneggiarli definitivamente e di renderli inservibili. Inoltre, si viene informati che i dati confidenziali sono stati sottratti e duplicati per essere venduti e diffusi ad altre organizzazioni che possono minacciare di pubblicarli. **E poi iniziano le trattative per il "rilascio"**.

PERCHÉ LE ORGANIZZAZIONI SONO IN RUSSIA

Una delle ragioni per cui spesso queste organizzazioni sono basate in **Russia** è che tutte le persone ed enti basati negli **Stati dell'ex-Unione Sovietica** sono protetti dagli attacchi, per evitare che i tentacoli di Putin vengano attivati contro di loro. In pratica si tratta di un sodalizio micidiale. Le **autorità moscovite** hanno dichiarato apertamente che **non perseguiranno i criminali cibernetici** per attacchi compiuti al di là delle frontiere. Dopo i paradisi fiscali, sono arrivate le zone di libero crimine online.

IN ITALIA GLI ATTACCHI HANNO SUPERATO QUOTA 3,6 MILIONI

Cos'hanno in comune un oleodotto americano, Olympus, la società globale giapponese di tecnologia biomedicale, la regione **Lazio**, l'ospedale San Giovanni di Roma? Sono state vittime di attacchi nel 2021. Tra gli anni '70 e '90 ci furono in Italia circa **600 sequestri di persona** a scopo di estorsione. Nel primo semestre del 2021, gli **attacchi hacker hanno superato quota 3,6 milioni solo nel nostro Paese**. Si tratta di un boom pari al **93% rispetto allo stesso periodo dello scorso anno**, quando le intrusioni raggiunsero quota 1,9 milioni.

Globalmente **Kaspersky**, società leader nella sicurezza informatica, **ha rilevato 1,5 miliardi di attacchi contro dispositivi Internet of Things (IoT)** nella prima metà di quest'anno. Non solo dalla Russia, ovviamente. Il business è diventato globale ed è la nuova frontiera della guerra economica tra le grandi potenze. Di fronte a questo scenario evolutivo, siamo tutti chiamati ad una forte presa di consapevolezza dei comportamenti e sistemi di protezione e prevenzione a tutti i livelli.

“Il problema non è il problema. Il problema è il tuo atteggiamento verso il problema. Comprendi?”, Jack Sparrow.

di Giuseppe Geneletti g.geneletti@methodos.com