E la prospettiva futura dei pirati

È bastato un semplice click per togliere il carburante a una grossa fetta degli Stati Uniti d'America. È quanto successo venerdì scorso, all'impianto della società di raffinazione del petrolio Colonial Pipeline di Pelham, Alabama. Uno dei più grandi gasdotti degli Stati Uniti è stato messo in ginocchio da un attacco informatico che l'ha costretto a una temporanea chiusura. Per giorni l'area che va dal Texas a New York non è stata rifornita di benzina, diesel e carburante per aerei. Solo ora l'attività sta lentamente riprendendo.
Ma quello al gasdotto è solo l'ultima di una costellazione di cyber attacchi, che negli ultimi anni hanno registrato un sensibile aumento. A dicembre 2020 un click era bastato alla principale agenzia di intelligence russa per colpire il governo americano, in particolare il Dipartimento del Tesoro e il Dipartimento del Commercio. E poi ancora a marzo 2021, sempre con un click, un gruppo di hacker legati alla Cina ha violato i server di Microsoft Exchange, attaccando migliaia di organizzazioni in tutto il mondo. Luoghi e tempi diversi, modalità simili. Il minimo comune denominatore è che questi attacchi sembrano avere sempre più forza e quindi maggiori conseguenze sulle vite di tutti noi. Creano e manovrano i conflitti geopolitici e mettono in evidenza come le strutture di rete di organismi nazionali e privati siano ancora molto fragili e impreparate.
L'attacco al gasdotto - Venerdì mattina la società petrolifera Colonial Pipeline ha annunciato di aver dovuto chiudere, in seguito ad un attacco informatico, oltre 8.850 km di gasdotto, che trasportano il 45% delle forniture di carburante nella costa orientale degli Stati uniti. L'impianto conduce oltre 2,5 milioni di barili di benzina raffinata e carburante per aerei al giorno e copre l'area che va dal Texas a New York. L'azienda ha messo offline i suoi sistemi informatici evitando così che i cybercriminali potessero mettere le mani su informazioni che gli avrebbero consentito di manipolare in remoto i comandi di sicurezza del gasdotto, causando esplosioni o possibili perdite di carburante. Sabato, Colonial Pipeline ha ripristinato le sue reti informatiche, ma il transito di carburante è ripartito solo parzialmente. I disagi provocati dall'attacco hacker potrebbero durare giorni. La società infatti gestisce infrastrutture chiave tra la costa del Golfo degli Stati Uniti e l'area del porto di New York, e il loro stop per un periodo prolungato ha già iniziato a far schizzare i prezzi della benzina sulla costa Est del Paese. Ieri i prezzi dei carburanti negli Stati Uniti sono saliti del 4,2%. Intanto dalla Casa Bianca hanno fatto sapere che "Il governo federale sta lavorando attivamente per valutare le implicazioni di questo incidente, evitare interruzioni dell'approvvigionamento e aiutare la società a ripristinare le operazioni del gasdotto il più rapidamente possibile".
L'FBI, il dipartimento dell'energia e la Casa Bianca, dopo alcune indagini, hanno confermato che quello di cui l'azienda era stata vittima era stato un attacco "ramsomware", ovvero un virus che paralizza i sistemi informatici criptando i dati importanti con lo scopo di estorcere un riscatto. Secondo quanto rivelato a Reuters da un ex funzionario e tre fonti del settore si

sospetta che dietro l'attacco informatico ci sia il collettivo DarkSide, probabilmente legato alla Russia ed al Cremlino. Ma Biden ieri ha tirato il freno, sottolineando come finora non ci siano "prove basate sui nostri servizi segreti che la Russia sia implicata".
Che cos'è un attacco ramsomware - Con la parola ransomware viene indicata una classe di malware (ovvero programmi informatici usati per disturbare le operazioni svolte da un utente) che rende inaccessibili i dati dei computer infettati e chiede il pagamento di un riscatto per ripristinarli. Hanno come unico scopo l'estorsione di denaro, attraverso un "sequestro di file", che vengono criptati e quindi resi inutilizzabili. Negli ultimi anni gli attacchi definiti ramsoware sono aumentati sensibilmente. Lo conferma il Rapporto Clusit 2021: i ransomware nell'anno 2018 rappresentavano il 23% di tutti i malware, che nel 2019 sono diventati quasi la metà (46%) e nel 2020 sono arrivati al 67%. In pratica sono ransomware i due terzi degli attacchi informatici.

Secondo i dati di Check Point, una tra le principali aziende di sicurezza informatica, in media, ogni 10 secondi un'organizzazione nel mondo è vittima di un attacco ransomware. In Italia un'azienda viene colpita da questo tipo di attacchi 817 volte alla settimana, 122 volte in più rispetto a quanto viene registrato nel resto del mondo. Numeri che rendono l'idea di quanto questa tipologia di attacco informatico sia diventata frequente. "Questi attacchi riescono facilmente perché hanno molti benefici e pochi punti a sfavore. Un tempo le informazioni si intercettavano attraverso emissari o infiltrati, ma era un affare più complicato. Oggi invece vengono veicolate attraverso reti invisibili e gli autori difficilmente vengono riconosciuti. E quanto più le nostre informazioni sono esposte su un perimetro importante, tanto più sono suscettibili di questi attacchi" spiega Pamela Pace, direttore generale di Obiectivo, azienda leader in Italia nella gestione della sicurezza informatica. L'esperta racconta come, normalmente, gli hacker riescano ad introdursi all'interno dei computer per alcune "vulnerabilità umane". "Attacchi come quello al gasdotto degli Stati Uniti riescono perché alcune persone che lavorano per l'amministrazione pubblica o società private lasciano finestre aperte sul computer o vanno inavvertitamente a cliccare su link o mail" spiega Pace.
Secondo l'esperta oggi i cyber attacchi hanno sempre più come scopo la pressione politica. "Riuscire in un attacco informatico significa oggi manifestare la propria forza politica. Basti pensare anche solo all'attacco che ha riguardato, qualche giorno fa Belnet, la società belga che fornisce servizi Internet alle agenzie governative del Paese. Anche se non è stato detto in modo chiaro ed esplicito, pare che sia un attacco proveniente dalla Cina. Oggi c'è una lotta a far emergere il proprio potere politico attraverso gli attacchi informatici".

Cyber attacchi nella storia
Ed in effetti i cyber attacchi alle infrastrutture critiche dei Paesi sono stati una delle principali preoccupazioni dell'ultimo decennio. A metà del 2009, alcuni pirati informatici esperti hanno individuato almeno due falle nel sistema di controllo dei server di Google, violandone l'accesso. Questo famoso attacco informatico è stato ribattezzato "Operazione Aurora", ed è stato caratterizzato dall'accesso illecito alla banca dati di grosse aziende degli Usa, asset strategici nei campi della sicurezza, difesa militare e ricerca tecnologica. Secondo Google stesso, l'offensiva è partita dalla Cina. L'attacco ha avuto risvolti politici importanti, con la presa di posizione di figure cardine come l'allora Segretario di Stato americano Hillary Clinton.
Nel 2012 l'Iran è stato accusato di un attacco ai sistemi informatici di Saudi Aramco, uno dei maggiori produttori mondiali di petrolio, che ha distrutto 30.000 computer. Quell'attacco era

stato considerato allora la risposta al cyber attacco che nel giugno precedente Usa e Israele avevano messo in atto contro l'industria energetica iraniana.
Ma già due anni prima, nel 2010, c'era stato uno dei più pericolosi attacchi informatici mai realizzati nella storia. Una vera e propria offensiva operata dal Governo americano e da quello israeliano ai danni della centrale nucleare iraniana di Natanz, attraverso un cyber virus, chiamato Stuxnet, in grado di sabotarne il software di gestione delle centrifughe. Nello specifico, questo malware aveva il compito di bloccare le turbine e, di conseguenza, tutta la produzione nucleare dell'impianto.
E poi ancora. Un altro attacco a un impianto petrolchimico saudita nel 2017 quasi provocato un grave disastro industriale. Ma l'impianto è stato fermato rapidamente e gli investigatori in seguito hanno attribuito l'attacco ad un gruppo di hacker russi. Quest'anno, alcuni pirati di internet hanno preso per poco tempo il controllo di un acquedotto in una piccola cittadina vicino a Tampa, in Florida. Un attacco che sembrava avesse come scopo l'avvelenamento dell'acqua, ma il tentativo hacker è stato presto interrotto.
Come dimenticare inoltre l'affare Solarwinds, quello che è stato definito come il più grande attacco di cyberspionaggio ai danni del governo statunitense degli ultimi anni. Attraverso i prodotti tecnologici della piattaforma Orion, commercializzati dalla società texana SolarWinds e utilizzati da diversi enti governativi Usa, un gruppo di hacker ha compiuto per mesi attività di spionaggio della posta elettronica. L'attacco è stato attribuito dagli esperti ad alcuni funzionari dell'intelligence russa, che avrebbero così cercato di interferire con le elezioni presidenziali del 2020. Ma ciò che ha colpito di questo attacco è stata la sua estensione. Gli hacker infatti sono stati in grado di colpire non solo agenzie governative, ma centinaia di società private e aziende in tutto il mondo.
Un approccio sbagliato alla sicurezza informatica - Che siano diretti contro aziende private o organizzazioni nazionali, gli attacchi cibernetici non fanno altro che mostrare come l'approccio alla sicurezza informatica internazionale, in buona parte basato sulle operazioni offensive e di deterrenza, abbia fallito. Biden, dal momento in cui si è insediato alla Casa Bianca, ha promesso una maggiore attenzione alla sicurezza dei sistemi informatici. Ma ciò non è bastato. "Servono azioni di governo con strategie ben definite in base alle esigenze. Criteri specifici, modelli organizzativi da mettere in campo. Le aziende, ma anche i governi hanno strategie ancora troppo deboli. Bisogna capire che investire sulla cybersicurezza oggi è un business. Non basta essere leader nella tecnologia per essere preparati e gli Stati Uniti ne sono una prova" commenta l'esperta Pace.
Dopo l'attacco al gasdotto degli Stati Uniti, l'amministrazione del presidente degli Stati Uniti Joe Biden ha intensificato il dibattito su un ordine esecutivo volto a rafforzare la cybersicurezza. Secondo il "New York Times", si tratterebbe di una sorta di una sorta di nuova "road map" per la difesa cibernetica degli Stati Uniti che imporrebbe nuovi standard di sicurezza digitale per le agenzie federali e per le aziende che sviluppano i software in uso alle istituzioni. Alle agenzie verrebbe chiesto di adottare un approccio di "zero fiducia" nei confronti dei propri fornitori di software, cui verrebbe consentito l'accesso ai sistemi federali "solo quando necessario"; ai contraenti, invece, verrebbe imposto di certificare con costanza l'assenza di malware e altre vulnerabilità sui loro prodotti. Chi dovesse violare tali regole non potrebbero più vendere software al governo federale e, come conseguenza, sarebbe fortemente penalizzato sul mercato. L'ordine esecutivo, che dovrebbe essere annunciato nelle prossime settimane, prevede anche l'istituzione di un "consiglio di revisione degli incidenti di cybersicurezza", incaricato di indagare sui principali attacchi.