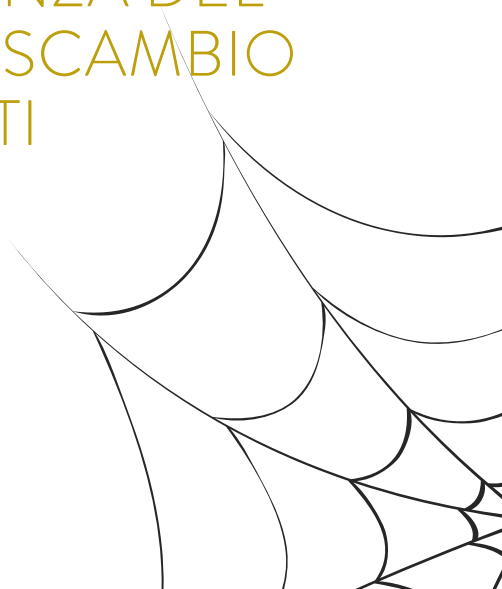
LA SFIDA DEL CYBER CRIME

di BENIAMINO MUSTO

OGGI, IL PERICOLO DI ATTACCHI INFORMATICI È DIVENTATO MOLTO PIÙ SISTEMATICO CHE IN PASSATO. I CRIMINALI CIBERNETICI, CHE HANNO AFFINATO LE LORO TECNICHE, SFRUTTANO A PROPRIO VANTAGGIO LA TRANSNAZIONALITÀ DELLA RETE. UNA RISPOSTA EFFICACE PER CONTRASTARLI PUÒ ARRIVARE SOLO DA UNA COSTANTE CONOSCENZA DEL FENOMENO, FAVORENDO LO SCAMBIO DI INFORMAZIONI TRA GLI STATI



La mattina dello scorso 21 ottobre i cittadini della costa orientale degli Stati Uniti si sono svegliati con una brutta sorpresa. Molti dei siti web che erano abituati a utilizzare, tipo **Twitter**, **Spotify**, **Reddit**, **PayPal**, **eBay** e **Yelp**, risultavano irraggiungibili. Qualcuno aveva messo nel mirino *Dyn*, un gruppo del New Hampshire che funziona come l'elenco telefonico di internet e il cui mancato funzionamento impedisce ai siti di caricarsi. Dyn, come tutti i *Dns* (*Domain name server*) offre un servizio che traduce il semplice nome di un sito web in un indirizzo IP che i computer usano per identificare se stessi su una rete. Senza di esso, ciascun utente per collegarsi a un determinato sito dovrebbe digitare numeri (e non parole) nel browser. Uno dei dati più inquietanti di questo attacco è venuto alla luce una volta scoperto che a portarlo avanti erano state centinaia di migliaia di telecamere di sorveglianza, tutte connesse in rete. L'esponenziale aumento degli oggetti connessi a internet ha moltiplicato il pericolo.

Corrado Giustozzi, esperto di sicurezza cibernetica presso l'Agenzia per l'Italia digitale (**Agid**), incaricato di sviluppare il *Computer emergency response team* (Cert) della Pubblica Amministrazione, sostiene che "i criminali sono per definizione un passo avanti a chi difende: appena viene inventata una nuova serratura per la porta, il ladro inventa un nuovo modo per aprirla". Giustozzi tiene a precisare che il quadro generale è molto complesso ed è importante non fare di tutta l'erba un fascio. "Uno dei principali problemi degli attacchi cyber è proprio quello riguardante l'attribuzione: è difficile capire chi sta facendo che cosa, perché è facile mascherare le proprie tracce in rete. Per cui è bene fare delle precise distinzioni: una cosa è il crimine organizzato, un'altra sono le attività di spionaggio, e un'altra ancora le attività di sabotaggio per fini ideologici".

LA TRANSNAZIONALITÀ DELLA RETE

Se fino a qualche anno fa le minacce informatiche erano tutto sommato sporadiche, oggi il pericolo è sistematico. "La criminalità ha imparato a utilizzare le tecnologie per il proprio tornaconto – spiega Giustozzi – e ha messo a frutto l'esperienza maturata in decenni per rendere efficace la propria azione. Per esempio, sfruttando al meglio la intrinseca transnazionalità della rete". Non a caso una delle cose che la criminalità riesce a fare meglio è quella di spostare le proprie attività nello Stato più conveniente in funzione del crimine: si ruba una carta di credito nel Paese A, la si utilizza nel Paese B, si riciclano i proventi nel Paese C, e così via. Questo gioco, per *i cattivi,* è molto facile (e redditizio). Per *i buoni*, invece, non lo è altrettanto, perché si devono fare i conti con normative macchinose che variano da Paese a Paese.

***Corrado Giustozzi**, esperto di sicurezza cibernetica presso l'Agid*

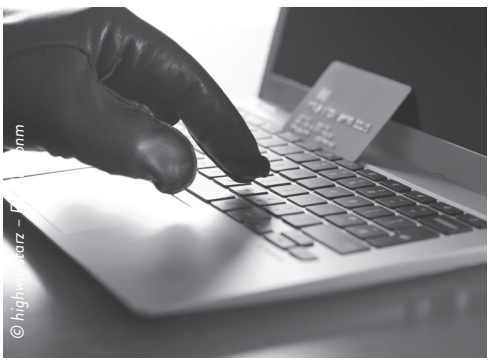
SE I DATI FINISCONO IN OSTAGGIO

I punti di attenzione delle minacce emergenti, su tutti, sono due: il ransomware (come ad esempio il famoso *Cryptolocker*) e il cosiddetto *Man in the mail*. Il primo è una minaccia costituita dall'infiltrazione di un malware all'interno della rete di un'azienda, attraverso cui vengono codificati tutti i dati digitali in modo da renderli inutilizzabili. Per poterli riavere, l'organizzazione criminale chiede il pagamento di un riscatto che

generalmente deve essere versato in *bitcoin* o un'altra criptovaluta virtuale (*vedi box*) che permette un anonimato quasi perfetto e rende quasi del tutto non rintracciabili le transazioni.
"Questa minaccia, in circolazione da anni, si è recentemente evoluta raggiungendo livelli preoccupanti", osserva Giustozzi, sottolineando che "è molto difficile avere statistiche precise perché non c'è l'obbligo di denuncia. Gli analisti sono d'accordo nell'affermare che la minaccia è cresciuta perché le email inviate come phishing o spam sono sempre più sofisticate e credibili".

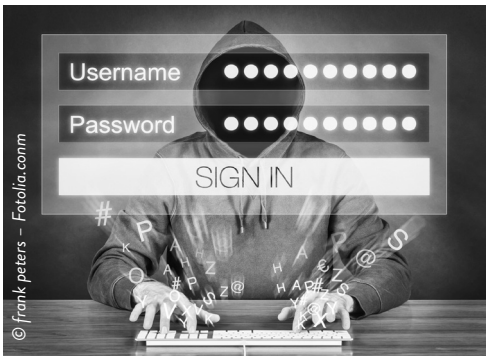
LA SANITÀ NEL MIRINO

Ultimamente si è assistito a una specializzazione di questa minaccia: anziché sparare nel mucchio, alcune organizzazioni prendono esplicitamente di mira determinati settori deboli. Uno di questi è la sanità. Sono sempre di più gli attacchi verso gli ospedali, vulnerabili e più portati a pagare. "L'ospedale è una struttura poco difesa – spiega Giustozzi – perché il tema sicurezza è declinato in campo medico, nel benessere dei pazienti. L'ospedale, in genere, non è visto come bersaglio di criminali. Lo è sicuramente meno rispetto a una banca". Ciò non significa che in un ospedale non vi sia nulla da rubare. "Gli ospedali non sono preparati contro queste minacce. Eppure la posta in gioco, cioè l'incolumità dei pazienti, è alta. I criminali riescono a bloccare i sistemi sanitari (come i computer della parte amministrativa) e non li rimettono in funzione fino a che non viene pagato un riscatto". Risulta evidente che un ospedale non possa fermarsi, perché altrimenti le persone rischierebbero la vita. E quindi si paga.
Anche la Pubblica Amministrazione è un soggetto meno difeso rispetto ai privati "per via della carenza dei mezzi. Questo è un po' endemico – ammette Giustozzi – perché i sistemi sono più obsoleti. Uno studio effettuato tre anni fa dall'Università La Sapienza di Roma sulla preparazione della Pa verso la minaccia



UN PORTAFOGLIO DI BITCOIN

Il bitcoin è la più nota tra le cosiddette criptovalute, utilizzate in rete per il possesso e il trasferimento anonimo del denaro. I dati necessari a utilizzare i propri bitcoin possono essere salvati su uno o più computer sotto forma di portafoglio digitale, oppure mantenuti presso terzi che svolgono funzioni simili a una banca. I bitcoin possono essere trasferiti su internet verso chiunque disponga di un *indirizzo bitcoin*. Grazie alle caratteristiche *peer to peer* del web e alla mancanza di un ente centrale è impossibile per qualunque Autorità il blocco dei trasferimenti e il sequestro di bitcoin senza il possesso delle relative chiavi. Inoltre è impossibile anche la svalutazione conseguente all'immissione di nuova valuta: la quantità di nuova moneta creabile è un numero finito. Il bitcoin si autoquota, dunque non fa uso di un ente centrale: utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni e sfrutta la crittografia per gestire gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione di proprietà. Può essere scambiato in danaro reale, attraverso istituti di credito che accettano pagamenti in valuta reale e restituiscono bitcoin. Esistono altre criptovalute, ma il bitcoin è quella indubbiamente quella che fino a ora ha avuto più successo.



cibernetica ha fatto emergere un quadro a macchia di leopardo, con alcuni soggetti virtuosi e altre amministrazioni, più decentrate, meno efficaci nella risposta agli attacchi".

L'UOMO NELLA POSTA

L'altro fenomeno in ascesa è il già citato Man in the mail. Gli hacker riescono a ottenere, con metodi più o meno fantasiosi, un accesso ai sistemi di posta elettronica di un'azienda (i bersagli prediletti sono le aziende commerciali, chi si occupa di import/export e in generale i fornitori). Una volta entrati, penetrano nelle caselle di posta degli impiegati chiave, tenendone d'occhio le email. Nel momento in cui c'è un contratto che va a buon fine, cioè quando si concretizza una vendita di merci che prevede il pagamento di una fattura, mandano una falsa mail, ma apparentemente proveniente dal soggetto che deve ricevere il bonifico, dove si comunica che, per motivi che variano a seconda dei casi, le coordinate bancarie sono cambiate. Tutto appare coerente: colui che deve effettuare il bonifico, invia il danaro agli hacker che poi fanno sparire i soldi. "Man in the mail – osserva Giustozzi – è un fenomeno sommerso: i media generalisti non ne parlano ma sta diventando molto diffuso, e colpisce prevalentemente le Pmi sia in Italia sia all'estero".

LO SCAMBIO DI INFORMAZIONI PER CONTRASTARE IL FENOMENO

Secondo Giustozzi per contrastare la cyber criminalità, la misura più importante è quella di mettere a fattor comune quello che si fa e quello che si osserva, esattamente come accade per le malattie con le misure di profilassi, da cui si parte per costruire una base di conoscenza statistica del fenomeno, che è il primo punto per iniziare un lavoro tutti insieme. Questo già viene fatto, con la rete di Cert nazionali. Ma va adeguato tutto il sistema europeo a questo tipo di cooperazione. La direttiva europea *Nis* (*Network and information security*), approvata a giugno, impone agli Stati membri di adeguare a un livello comune e coerente la prevenzione alle minacce cyber con misure organizzative e tecnologiche. Nello specifico, si chiede il consolidamento della rete di interscambio informativo della rete dei Cert: ogni Nazione dovrà stabilire l'Autorità che sarà punto di contatto con le altre e le regole di condivisione delle informazioni. La direttiva Nis renderà poi obbligatoria la notifica degli incidenti, imponendo agli operatori dei settori critici la notifica a un'Autorità nazionale. La direttiva si applica a tutti quei soggetti che operano nell'ambito dei *servizi essenziali*. La definizione di servizio essenziale, dal 2013, è oggetto di discussione ma attualmente comprende sia gli operatori di infrastrutture critiche (energia, mercati finanziari, sanità, acqua, trasporti, banche, infrastrutture digitali e provider Dns) sia i principali fornitori di servizi della società dell'informazione (e-commerce, social network, cloud computing, motori di ricerca, financial provider).

A tutti i soggetti sono imposti specifici oneri quali l'implementazione di uno standard minimo di sicurezza e l'obbligo di notifica degli incidenti di una certa rilevanza alle Autorità nazionali, che ogni Stato dovrà autorizzare o costituire allo scopo. Ciò comporterà l'adozione di politiche di sicurezza e di gestione delle violazioni informatiche, nonché l'istituzione di personale appositamente formato per la risposta rapida agli incidenti informatici. I tempi per l'attuazione da parte di ogni Stato sono lunghi: 21 mesi per il varo di una normativa quadro, e ulteriori sei mesi per il censimento degli operatori di servizi essenziali. Tutte le Autorità nazionali dovranno poi comunicare questi dati a un'autorità europea, l'**Enisa**, che è l'agenzia Ue che ha curato la costituzione della rete dei Cert: Corrado Giustozzi fa parte del gruppo di 20 esperti che definisce la strategia di questa agenzia.