il venerdì di Repubblica

diffusione:192543
tiratura:288775

SCIENZE
PAROLA D'ORDINE?

PHISHING MA NON SOLO. COME NON ABBOCCARE

LE FRODI ONLINE CRESCONO (+15 PER CENTO NEL 2023) CON STRUMENTI SEMPRE PIÙ RAFFINATI. IL SUPER ESPERTO **GIOVANNI ZICCARDI** CE NE SVELA I MECCANISMI. PER IMPARARE A DIFENDERSI MEGLIO

di **Giuliano Aluffi**

«PAGA tutto e fallo subito, grazie»: così dice un'email del capo che chiede di versare ben 25 milioni di euro dell'azienda su un conto sconosciuto. Per evitare dubbi, il capo invita a una videoconferenza su Teams dove lui e altri due dirigenti rassicurano sull'operazione. Così il funzionario fa partire il bonifico. E da qualche parte nel mondo una squadra di delinquenti stappa lo champagne: sì, hanno appena rubato 25 milioni all'azienda. Grazie al deepfake – la tecnologia di intelligenza artificiale che permette di assumere in video le fattezze di un'altra persona e di imitarne anche la voce – a convincere il malcapitato su Teams sono stati proprio i truffatori. È successo davvero, il mese scorso, a Hong Kong, ed è solo uno degli esempi dell'evoluzione dei crimini informatici. Meno spettacolare ma più vicino a noi quanto avvenuto sei mesi fa a Cremona: la U.S. Cremonese Calcio doveva versare 1,7 milioni di euro alla squadra belga Genk per l'acquisto dell'attaccante Cyriel Dessers. Ma un hacker si è intromesso nella corrispondenza tra le due squadre, e in un'email ha rimpiazzato le coordinate bancarie specificate dai belgi con le sue, così da ricevere fraudolentemente il denaro. La polizia postale ha scoperto in tempo la truffa *man in the middle* e bloccato il bonifico.

Giovanni Ziccardi, docente all'università degli studi di Milano, è l'autore di ***Dati avvelenati*** (Raffaello Cortina, 352 pagine, 16 euro)

DALL'HACKER SOLITARIO AL POOL

Secondo l'ultimo rapporto della stessa polizia postale, le frodi informatiche che sono in crescita: più 15 per cento nel 2023 rispetto al 2022, con 10.606 casi trattati e un totale di oltre 40 milioni di euro di somme sottratte. «Nell'ultimo decennio il crimine digitale è cambiato: prima i malfattori erano hacker con grandi competenze tecniche, che agivano come lupi solitari. Oggi invece è un mondo assai più strutturato, e si sono abbassate di molto le barriere di accesso alla "professione": si tratta per lo più di truffatori che non hanno bisogno di essere super-competenti perché possono avvalersi facilmente di esperti. C'è un vasto mercato sia di servizi che di dati (come credenziali e password) rubati a ignari cittadini e venduti a chi vuole usarli per arricchirsi» spiega uno dei massimi esperti italiani sul tema, Giovanni Ziccardi, professore di Informatica giuridica presso l'università degli studi di Milano, che sviscera questo sottomondo nel saggio *Dati avvelenati* (Raffaello Cortina). «I criminali informatici oggi operano in organizzazioni simili a vere e proprie aziende. Il lavoro è diviso tra programmatori di malware, persuasori, che entrano in contatto con le vittime per indurle a comportamenti imprudenti, addetti al riciclaggio abili a magheggi con le criptovalute, e tante altre nuove figure "professionali"». La più paradossale è quella del supporto tecnico alle vittime di truffe ed estorsioni. «Viene offerto per esempio a chi non sa usare le criptovalute (come i bitcoin), ambite dai criminali perché irrintracciabili», spiega il docente. «Oggi il cyber-crimine più redditizio, e in continua crescita, è il ransomware (da *ransom*, ricatto): può colpirci se apriamo gli allegati di messaggi infetti o clicchiamo su link malevoli.

LE TRUFFE PIÙ COMUNI

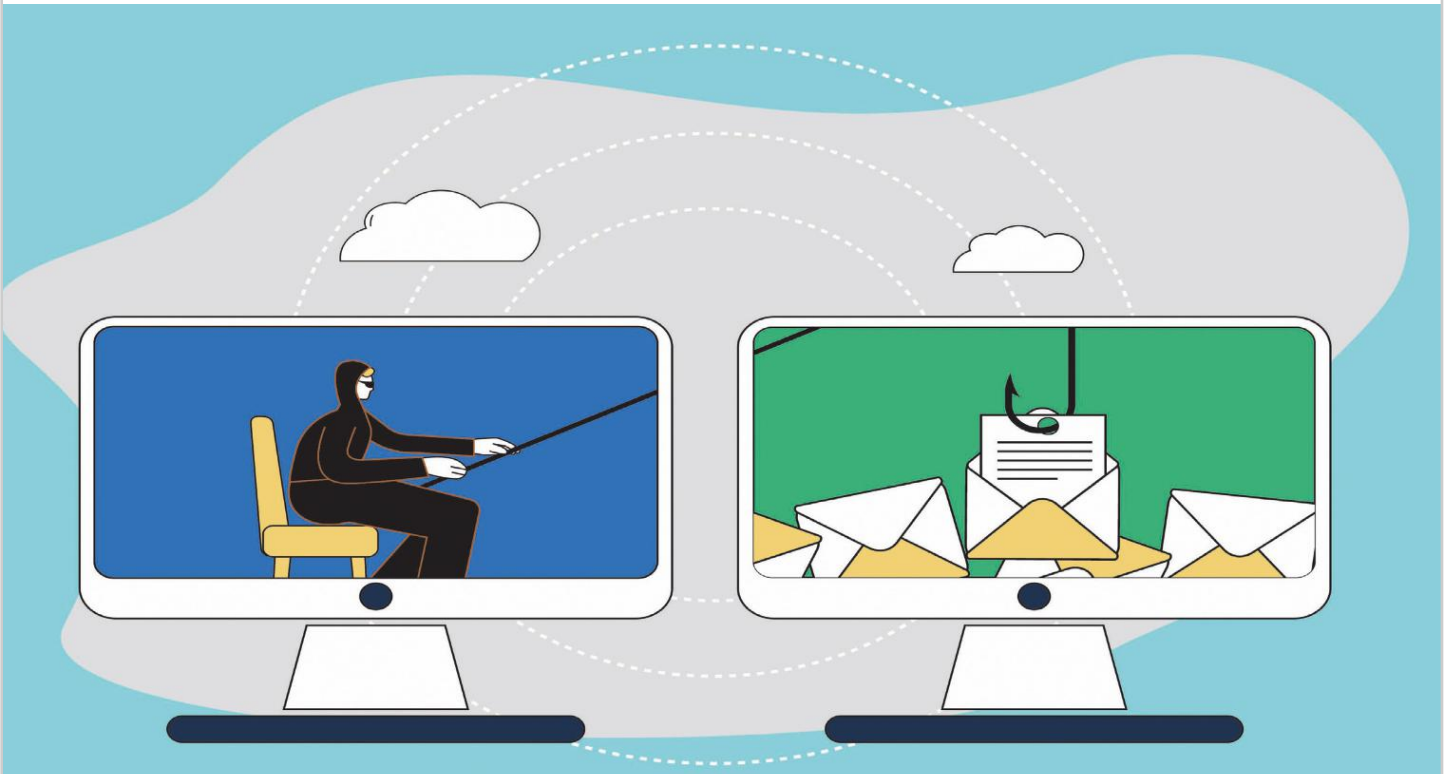
PHISHING
I criminali inviano email fingendosi mittenti legittimi (soprattutto banche) invitando ad accedere al proprio conto tramite un link che, se cliccato, porta a una pagina web fraudolenta, del tutto simile a quella della vera banca, che carpirà le credenziali di accesso della persona, così da svuotargli il conto.

SMISHING
È come il phishing, ma il link fraudolento viene inviato via sms.

RANSOMWARE
Un programma malevolo, scaricato cliccando un link o un allegato ricevuto per email, cripta i file del computer della vittima, rendendoli inutilizzabili. Un messaggio esorta la vittima a pagare un riscatto in criptovalute (200-1.000 euro) per poter sbloccare i suoi file.

il venerdì di Repubblica

diffusione:192543
tiratura:288775



VISHING
(phishing vocale) Il malfattore contatta la vittima (al telefono o con chiamata vocale su Whatsapp) fingendosi il call center di una banca e chiedendo i dati di accesso al conto con la scusa di effettuare verifiche su presunti ammanchi.

MAN-IN-THE-MIDDLE
Un hacker viola la casella email della vittima e modifica la corrispondenza tra questa e una terza persona, in particolare le coordinate bancarie per pagamenti, in modo da intercettare fraudolentemente il denaro.

GETTY IMAGES

In questi casi sul nostro computer verrà scaricato un programma che, di nascosto, cripta tutti i file, rendendoli irrecuperabili a meno di non essere in possesso di una chiave crittografica. Compiuta l'opera, ci apparirà una schermata che ci informa di ciò che è successo e ci offre la chiave, chiedendo in cambio una somma in criptovalute. E c'è sempre un link a una specie di "help desk" che ci guiderà nell'acquisto di bitcoin e si assicurerà che il versamento vada a buon fine».

La figura perversa del "facilitatore" compare anche in altri tipi di frodi, una di queste può avvenire sulle piattaforme di commercio elettronico come eBay o Subito. «Se stiamo vendendo un oggetto, ci contatta un potenziale acquirente dicendo che potremo prelevare subito i suoi soldi presso un Postamat (i bancomat di Poste Italiane) offrendosi di guidarci nell'operazione per telefono. Arrivati al Postamat, il malfattore ci induce, con una parlantina che non ci lascia il tempo di riflettere, a inserire il nostro Bancomat "per far attivare il sistema". E alla fine fa in modo che siamo noi a versare i nostri soldi sul suo conto, invece del contrario» osserva Ziccardi.

«La capacità di persuadere è sempre più cruciale: oggi circa il 50 per cento delle azioni di hacking fanno leva sull'inganno». Non serve più essere maghi del computer: «Nel dark web – ovvero i siti e forum non indicizzati dai motori di ricerca classici, dove opera chiunque voglia agire sottotraccia – vengono pubblicizzati dei "programmi di affiliazione" che offrono a chiunque lo desideri sia il software necessario a infettare i computer altrui, sia altri servizi necessari al compimento delle estorsioni», spiega l'esperto. «Il neocriminale dovrà soltanto corrispondere, a estorsione avvenuta, una percentuale del bottino». Bottino che può essere ingente. L'ultimo report dell'Enisa (Agenzia dell'Unione europea per la cybersicurezza) mostra che il costo medio di un grave incidente informatico nel settore sanitario è di 300mila euro.

«FARE IL BACKUP DEI DATI SU UN **SUPPORTO ESTERNO** PUÒ SALVARLI. BANALE? POCHI LO FANNO«

Siamo tutti vulnerabili? «Lo siamo quanto più sovrastimiamo le nostre capacità: oggi report Ue indicano che in Italia il 48 per cento delle persone over 14 manca di competenze di base su Internet. Possiamo difenderci dai ransomware diventando più cauti e informati, e facendo un backup regolare dei nostri file su un supporto esterno, come una chiavetta Usb», consiglia Ziccardi. «Per le aziende, una pratica raccomandata dall'Enisa è detta "3-2-1": prevedere, per tutti i dati, tre copie, usando due supporti di archiviazione diversi e con una copia custodita al di fuori della sede principale». Del resto una massima hacker ben sintetizza la questione: "Ci sono due tipi di persone al mondo: quelli che fanno il backup, e quelli che hanno perso i dati". ◻