Attacco hacker nel mondo Violati migliaia di server

Nel mirino anche l'Italia. Per i tecnici minaccia di livello alto, oggi vertice a Palazzo Chigi

ROMA Una corsa contro il tempo per avvisare il maggior numero di aziende con sistemi informatici prodotti dall'americana Vmware affinché corrano ai ripari, per eliminare le vulnerabilità che potrebbero spianare la strada a virus ransomware, capaci di bloccare tutto. È quella scattata alle 2 di domenica notte, quando gli specialisti dell'Agenzia per la cybersicurezza nazionale si sono accorti della falla a livello nazionale e hanno lanciato un invito per l'aggiornamento immediato di tutti i sistemi interessati. In particolare quelli nel settore della sanità. Un allarme mondiale partito dalla Francia, scenario della prima segnalazione venerdì scorso, diffuso poi in Finlandia, Turchia, Germania, Regno Unito, Canada e Usa.

Fino a ieri sera, secondo i vertici dell'Acn, nel nostro Paese non risultavano sistemi compromessi dagli hacker, ma con il passare delle ore il rischio è destinato ad aumentare. Anche perché il malware sfrutta il mancato aggiornamento del sistema nonostante già nel 2021 i produttori di server Vmware avessero fornito le *patch*, ovvero le correzioni necessarie per far fronte alla vulnerabilità del sistema. Alcuni le hanno utilizzate, molti altri no. E adesso l'ondata di attacchi ransomware, già in circolazione, potrebbe abbattersi anche sull'Italia.

La matrice ancora non è chiara, ci sono segnali che dietro ci possano essere hacker russi, più probabilmente due gruppi misti, e non si esclude con ramificazioni criminali, ma l'attenzione è molto alta. Il Computer security incident response team Italia (Csirt-It) dell'Agenzia ha avviato una campagna di informazione per avvertire istituzioni e aziende, grandi e piccole, mentre la polizia postale ha attivato i centri operativi di sicurezza cibernetica per il monitoraggio della Rete. Un sistema di difesa nazionale che si è attivato nel giro di poche ore, anche perché gli effetti di un ransomware si sono già visti in passato — come l'attacco alla Regione Lazio di due anni fa — con il virus che cripta i file sul sistema scelto come bersaglio e gli hacker che pretendono un riscatto per rilasciarli alla vittima. Le richieste di pagamento in bitcoin sono già arrivate.

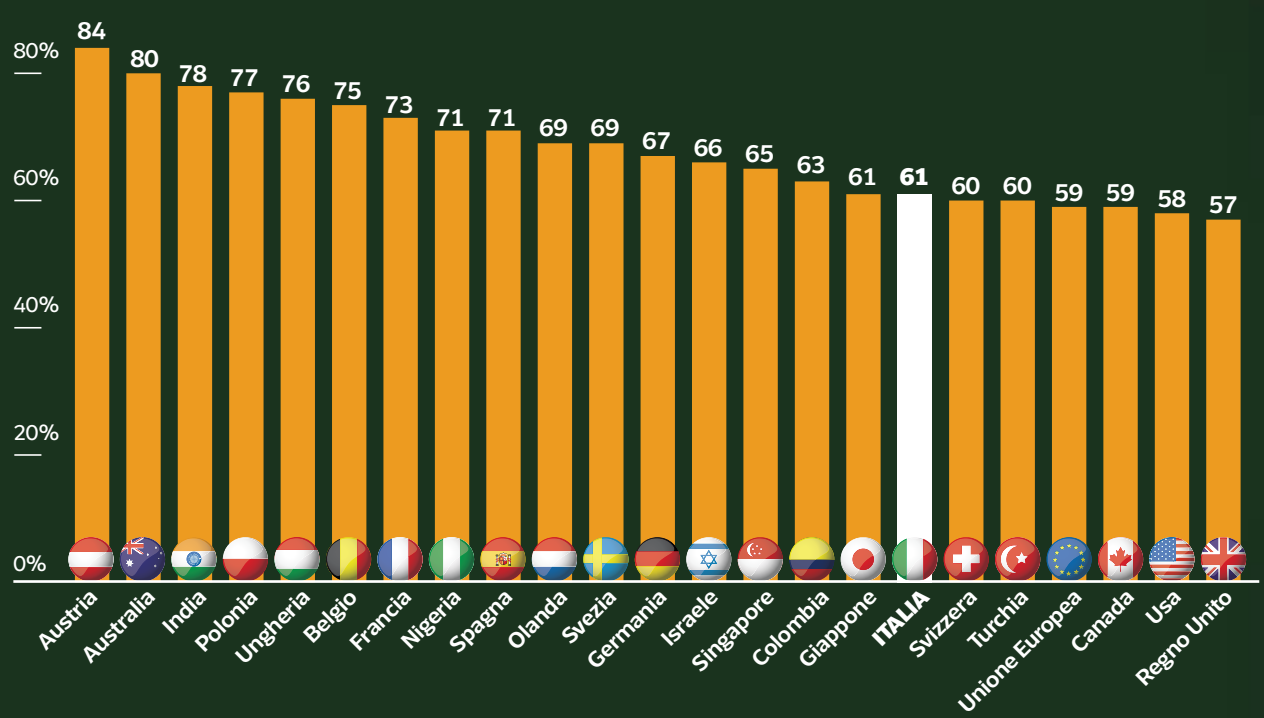
La richiesta La schermata comparsa su alcuni dei server colpiti dall'attacco. «Pagate entro tre giorni o diffonderemo i dati e alzeremo il prezzo»

Un'intrusione che sfrutta gli allegati di mail in apparente

I numeri

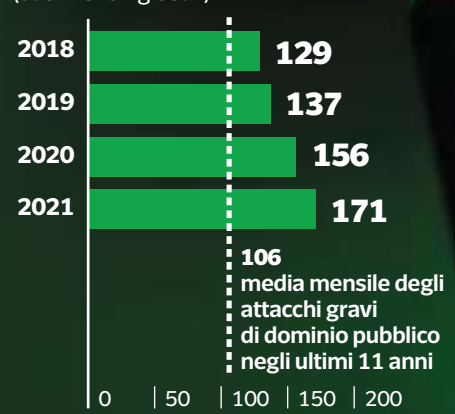
Il ransomware nel mondo

(percentuale di organizzazioni colpite nel 2022)



L'aumento dei blitz

(dati mensili globali)



Gli attacchi censiti

(tra il 2018 e il 2021)

L'intervista

«Colpiti sistemi molto diffusi Chi non li aveva aggiornati ha aperto la porta all'assalto»

L'esperto di sicurezza: così hanno agito i cyber criminali

ROMA «Già due anni fa la casa madre Vmware, e quindi la linea di prodotto ESXi, ha scritto ai clienti di utilizzare le *patch* di aggiornamento, ma a oggi molte aziende non l'hanno fatto. Un po' di sano allarmismo non fa mai male in questo campo, però bisogna tenere presente che gli hacker stanno scansionando il web alla ricerca di obiettivi da colpire». A spiegare quello che sta accadendo è Remo Marini, presidente della Fondazione F3rm1, che si occupa di ricerca e sviluppo nell'ambito della cybersecurity e dell'innovazione tecnologica.

Chi è Remo Marini, 47 anni, presidente della Fondazione F3RM1 che si occupa di sicurezza cibernetica

Chi c'è dietro questi attacchi?

«Due gruppi cyber criminali, Black Basta (che ha già colpito Acea, *ndr*), di origine russa, e ESXiArgs, che potrebbe trattarsi di una joint venture fra criminalità russa e cinese. Hanno sviluppato un tool, ovvero un sistema automatico, che sfrutta le vulnerabilità dei server e inietta un malware: così cercano le vittime sul web per colpirle».

Al momento chi è più a rischio?

«Per sfruttare la vulnerabilità bisogna trovarsi di fronte a due errori commessi dai dipartimenti di *information technology* delle aziende. Innanzitutto non aver aggiornato i sistemi usando le *patch* fornite dalle aziende produttrici. Inoltre aver esposto direttamente su internet senza protezioni di sicurezza, i servizi vulnerabili, rilevabili così attraverso le scansioni degli hackers attaccanti».

Perché tutto è partito dalla Francia?

«Proprio perché sono state rilevate le vulnerabilità a seguito delle non corrette procedure di sicurezza da parte dei clienti del provider Ovh. Non sono stati utilizzati i sistemi di sicurezza raccomandati e gli hacker hanno potuto dilagare. È accaduto il 3 febbraio scorso, sono bastati due giorni per scatenare il panico. Del resto i due sistemi in questione sono molto diffusi, non c'è ditta che non li usi: ottimizzano l'utilizzo delle risorse informatiche, permettendo quello di più sistemi contemporaneamente in un unico server fisico. Improponibile al giorno d'oggi, anche a livello economico, non usare macchine virtuali. L'importante, come detto, è aver una gestione dei sistemi orientata alla sicurezza e con relativi piani di *patching*».

L'intenzione degli hacker è solo chiedere un riscatto?

«Una volta entrati in un sistema possono fare ciò che vogliono, dalla gestione dei sistemi all'esfiltrazione dei dati o la loro criptazione».

> È partito tutto dalla Francia perché un fornitore non ha utilizzato i sistemi di sicurezza raccomandati

Secondo lei, c'è un collegamento con la guerra in Ucraina?

«Non penso, questi sono criminali. C'erano anche prima. Sono russi ma rimbalzano da una parte all'altra del mondo: usano sistemi *command&control* per gestire le *botnet*, ovvero i pc infetti. La loro "firma" si scopre proprio dall'analisi di questo modo d'agire».

Quale altro sistema ha un'azienda per proteggersi?

«Affidarsi a uno specialista in cybersicurezza. Soprattutto oggi per i rischi che si corrono e come evolvono in maniera molto rapida. Bisogna capire che adesso sei mesi in questo settore corrispondono a un'era geologica. Leggere costantemente come si muovono i gruppi criminali è fondamentale».

R.Fr.

za innocue perché provenienti spesso da finti soggetti istituzionali. «Siamo stati in grado di censire diverse decine di sistemi nazionali verosimilmente compromessi e allertare numerosi soggetti i cui sistemi sono esposti ma non ancora compromessi», spiegano proprio dall'Agenzia.

Per i tecnici il livello della minaccia è «alto-arancione», tanto che il governo — sottolineano da Palazzo Chigi — «segue con attenzione gli sviluppi dell'attacco». Oggi alle 9 il sottosegretario Alfredo Mantovano incontrerà il direttore di Acn Roberto Baldoni e la direttrice del Dipartimento informazione e sicurezza Elisabetta Belloni. Proprio ieri Acea ha ripristinato «la funzionalità dei sistemi informatici dopo l'attacco cyber che ha interessato l'azienda lo scorso 2 febbraio ad opera del gruppo ransomware Black Basta. Allo stato attuale le analisi statiche e dinamiche della minaccia non hanno evidenziato compromissione dei dati personali».

Rinaldo Frignani

Dalla Francia
I primi ad accorgersene sono stati i francesi, probabilmente per via dell'ampio numero di infezioni sui sistemi di alcuni provider

Il contagio
Qualche migliaio i server compromessi a livello globale, tra i Paesi più colpiti in Europa c'è anche la Finlandia. E poi Canada e Stati Uniti

Cosa sono i ransomware

Si tratta di software che hanno un intento criminale: ricattare ("ransom") ed estorcere denaro

Come funzionano

I criminali per lungo tempo hanno utilizzato questi software in modo quasi indisturbato. Gli estorsori mantengono un basso profilo. Solo di recente le aziende hanno iniziato a denunciarli. Di solito gli hacker chiedono un riscatto in bitcoin

Corriere della Sera

Il retroscena

di **Paolo Ottolina**

Enti, aziende, Comuni a rischio ricatto: «Paga in bitcoin o sveliamo i tuoi dati»

La «vulnerabilità» nei software era nota da due anni

MILANO Concedeteci di usare una frase fatta, eppure talvolta non meno vera, che spesso abbiamo sentito per gravi fatti di cronaca: «Una strage annunciata». In tarda serata i sistemi colpiti e bloccati dall'attacco ransomware avevano superato in tutto il mondo quota 2.100. Un numero che sale rapidamente. La vulnerabilità sfruttata dai cybercriminali era tutt'altro che sconosciuta. La soluzione, la «patch» (toppa) come si dice in gergo, era stata rilasciata ben due anni fa, nel febbraio 2021, da VMware, l'azienda del software coinvolto. «E tre giorni fa il Cert francese (il Centro di risposta agli allarmi cyber, *ndr*) aveva lanciato l'allerta: è stata più o meno ignorata e questo fatto è di una gravità sconcertante» ci dice Corrado Giustozzi, divulgatore ed esperto di cybersicurezza, partner di Rexilience.

Gang, non terroristi
Secondo gli analisti si tratterebbe di cyber gang non collegate ai terroristi internazionali

Ogni attacco informatico sfrutta sempre una vulnerabilità nel software. In questo caso quella riscontrata nei diffusi software di «virtualizzazione» della californiana VMware («virtualizzare» significa fare girare in modo simulato un software o un sistema su un altro hardware). In questo caso la soluzione per il problema era stata messa a disposizione da VMware ben due anni fa, nel febbraio 2021. «C'è di mezzo una catena infinita di sciatteria e disinteresse per non aver fatto gli aggiornamenti dovuti... E per di più il software in questione può essere attaccato solo se esposto su Internet, cosa che andrebbe evitata. Chi è nei guai non dico che se li è andati a cercare ma di certo non si è mosso in tempo con le contromisure» dice con amarezza Giustozzi.

Tra gli oltre 2.100 server colpiti ci sono moltissime aziende e pubbliche amministrazioni (tra cui il Comune francese di Biarritz, uno dei pochi bersagli trapelati al momento). Sui computer bloccati dal ransomware viene lasciata una nota che dice: «Allarme rosso!!! Abbiamo hackerato con successo la tua azienda. Tutti i file vengono rubati e crittografati da noi. Se si desidera recuperare i file o evitare la perdita di file, si prega di inviare 2.0 bitcoin. Invia denaro entro 3 giorni, altrimenti divulgheremo alcuni dati e aumenteremo il prezzo. Se non invii bitcoin, informeremo i tuoi clienti della violazione dei dati tramite e-mail e messaggi di testo».

Il wallet, il portafoglio digitale, su cui versare i bitcoin è differente in ogni nota di riscatto, così come l'importo (a volte vengono chiesti 2,064921 bitcoin, altre 2,01584 e così via: con la quotazione attuale sono circa 42 mila euro). Nessun link di riferimento per il pagamento. Gli esperti però sono concordi: l'offensiva sembra essere legata a cybergang comuni. Comuni non per le abilità ma nel senso che mancano (almeno al momento) collegamenti con il terrorismo internazionale o con situazioni geopolitiche di attualità. Non nota la nazionalità, anche se la maggior parte dei gruppi attivi nel ransomware gravita nell'Europa dell'Est.

Il caso è emblematico di una realtà esplosiva per numeri e conseguenze: quella del ransomware e dei ricatti digitali, che (dati Trend Micro 2022) vedono l'Italia esposta, primo Paese in Europa e settimo al mondo per numero di attacchi. Che fare? «Predicare belle cose non serve, perché non si fanno. C'è ancora una ignoranza clamorosa nelle aziende e nella Pubblica amministrazione sulla sicurezza informatica, che da troppi viene vista non come una componete strategica per la sopravvivenza stessa di queste realtà, ma come un qualcosa simile alle lampadine da sostituire o agli ascensori da aggiustare» dice ancora Corrado Giustozzi. Che poi suggerisce: «Serve una normativa che non si può ignorare, come è stato fatto per le norme antisismiche, quelle antincendio o di sanità pubbliche. E occorrerebbero norme come quelle per i sequestri di persona negli anni 70, che vietino o rendano difficile ai soggetti colpiti di pagare i riscatti, per non alimentare il circolo vizioso».

I precedenti

Il blitz contro i siti di Senato e Difesa

Il 10 maggio il gruppo hacker filorusso Killnet ha lanciato un attacco ai siti istituzionali italiani di Senato e Difesa e alle piattaforme Iss e Aci: le autorità hanno negato il furto di dati sensibili

Il tentativo all'Eurovision

Fino al 14 maggio gli hacker russi di Killnet hanno tentato di bloccare l'Eurovision per impedire la vittoria del gruppo ucraino Klaus Orchestra, che poi ha trionfato

I portali di polizia e Campidoglio

Killnet ha rivendicato anche l'attacco della notte del 16 maggio al sito della polizia di Stato italiana e poi al Comune di Roma, che lo ha respinto senza riportare alcun danno

Tim, una domenica a singhiozzo. «Ma i pirati non c'entrano»

Migliaia di segnalazioni specialmente sulla rete fissa nelle città. Il servizio ripristinato in serata

Lo stop

● Problemi in tutta Italia, ieri, per la rete Tim, con migliaia di segnalazioni di disservizi. L'azienda ha rilevato «un problema di interconnessione internazionale» poi rientrato. La polizia postale ha escluso un cyberattacco, parlando di «problemi tecnici sulla rete Internet fissa e non su quella mobile»

MILANO È stata una domenica molto difficile per l'Italia digitale. Al cyberattacco si è aggiunto un lungo disservizio sulla rete di Tim, che per lunghe ore ha lasciato a piedi (o ha fortemente rallentato, con connettività a singhiozzo) i navigatori che accedono al web attraverso l'ex monopolista. Disagi arrivati a stretto giro dal lunghissimo «down» delle mail di Libero e Virgilio, al termine di un periodo che ha evidenziato la fragilità del web italiano.

La rete di Tim ha funzionato a singhiozzo a partire dalle 11 di ieri, con migliaia di segnalazioni di disservizi registrate da pagine quali *Downdetector* e *Assistenza-clienti.it*. Il problema è via via rientrato e si è risolto definitivamente nel pomeriggio dopo il lavoro dei tecnici di Tim. «Con riferimento al disservizio che si è verificato oggi (ieri, *ndr*), Tim comunica che il problema è rientrato e il servizio si è stabilizzato alle ore 16:55. Dalle verifiche effettuate, il problema ha riguardato il flusso dati su rete internazionale che ha generato un impatto anche in Italia. L'azienda si scusa con i propri clienti per il disagio arrecato» ha fatto sapere Telecom Italia con un comunicato emesso intorno alle 20.

Già durante il pomeriggio il disservizio era stato attribuito a un «problema di interconnessione internazionale». Nessun legame diretto dunque con l'offensiva ransomware che ha coinvolto diversi Paesi del mondo tra cui anche l'Italia. Dopo le prime verifiche, era stata anche la polizia postale a escludere l'ipotesi di cyberattacco per il «down» di Tim, parlando più semplicemente di «problemi tecnici che interessano la rete Internet fissa e non quella mobile». Anche se in verità, sui social network come Twitter, diversi utenti avevano segnalato disagi persino sui cellulari. In particolare per chi si trovava all'estero, con le sim Tim tagliate fuori dal roaming e quindi inservibili.

L'impatto dei problemi è stato notevole per la rete italiana: secondo Netblock, organizzazione che monitora il traffico Internet globale, l'Italia durante la giornata di ieri è scesa fino al 26% della sua connettività consueta. I problemi (benché l'azienda non confermi) hanno probabilmente coinvolto il Bgp, il Border gateway protocol, che è centrale nel funzionamento della Rete delle reti e che può essere spiegato come «l'ufficio postale di Internet». Il Bgp è responsabile dell'esame dei percorsi disponibili che i dati potrebbero utilizzare per viaggiare sulla rete globale, nello stesso modo in cui le Poste decidono che strada fa una lettera quando la imbuchiamo.

Il calcio
Proteste anche per i disturbi alle partite Dazn: problemi dell'operatore telefonico

Le segnalazioni delle difficoltà degli utenti si sono riversate nel corso della giornata sul servizio di customer care di Tim e sui social, con hashtag come #TimDown o #LaTim che rapidamente hanno guadagnato il primo posto tra i temi più twittati dagli italiani.

Rabbia e preoccupazione che si sono sovrapposte alla domenica calcistica, ormai sempre più legata alla disponibilità di una buona connessione. Molte proteste in particolare dalla zona di Napoli, con tanti abbonati alla Serie A impossibilitati a seguire la capolista impegnata sul campo dello Spezia. Dazn a sua volta è stata presa d'assalto e ha dovuto chiarire con un tweet che si trattava di «problemi sulla rete Internet di uno dei principali operatori telefonici».

P. Ott.

La parola

ACN

È l'acronimo dell'Agenzia per la cybersicurezza nazionale, l'Autorità italiana per la tutela della sicurezza nazionale in ambito informatico e nello spazio cibernetico che ha anche il compito di assicurare il coordinamento tra i soggetti pubblici coinvolti nella materia. È stata istituita dal governo Draghi con un decreto poi convertito nella legge 109 del 4 agosto 2021. Il dg è Roberto Baldoni