

Sicurezza IT


Pmi, è cyber allarme: sempre più nel mirino degli attacchi hacker

Nel 2022 crescono del 45% le denunce di assalti ai dati con richiesta di riscatto
Manifattura e servizi colpiti nel 53% dei casi

di Ivan Cimmarusti — a pagina 2

Piccole e medie imprese e studi professionali: gli hacker all'attacco

Il report. Nel 2022 per la Polizia postale il ransomware segna un più 45%
Manifattura e servizi più colpiti. Molti scelgono di pagare: si rischia il pizzo 2.0

 **Pochi investimenti nella sicurezza informatica mettono a repentaglio i dati gestiti dalle società**

Ivan Cimmarusti

Nell'ultimo anno le denunce per attacchi hacker gravi ai server italiani sono aumentate del 45 per cento. Bersaglio dei cybercriminali sono soprattutto le piccole e medie imprese, vittime del *ransomware*, cioè un virus informatico che "esfiltra" o "cripta" dati riservati allo scopo di chiederne il riscatto in criptovalute. E le aziende del manifatturiero e dei servizi, da sole, assorbono il 53% delle intrusioni informatiche totali segnalate nel corso del 2022 alla Polizia postale.

Eppure, l'aumento delle denunce non è in grado di fotografare l'ampiezza di un fenomeno, a forte connotazione transnazionale, che in alcuni casi può andare ben oltre l'estorsione, per sfociare in forme di

spionaggio industriale sulle aziende del made in Italy.

Poche denunce, tante intrusioni
Stando alle analisi del Cnaipic, articolazione della Polizia postale che si occupa dell'anticrimine informatico, il gap tra numero di segnalazioni e lancio di *malware* verso l'industria italiana è molto elevato. Tradotto: ci sono poche denunce rispetto alle azioni *hacker* quotidianamente monitorate dalla Polizia postale, diretta da Ivano Gabrielli. Lo rende possibile un nuovo approccio della criminalità informatica. Le *cybergang* si sono accorte che azioni *ransomware* imponenti su amministrazioni centrali, con richieste di riscatto milionarie, non portavano da nessuna parte. Diversamente, tante intrusioni in piccole realtà produttive, con richieste di riscatto relativamente modeste, inducevano le vittime a pagare e a non denunciare, anche per evitare il danno reputazionale

conseguente alla comunicazione obbligatoria al Garante della privacy per la violazione dei dati.

Di conseguenza, rilevano gli investigatori, le imprese hackerate – soprattutto quelle piccole – per riottenere dati sensibili trafugati o bloccati con codici cifrati, trovano spesso più conveniente pagare. Una mossa che può avere effetti devastanti: si rischia di finire nelle "liste dei pagatori", cioè tra quei soggetti che periodicamente sono bersaglio di attacchi *ransomware*. Una specie di pizzo 2.0.



Superficie 70 %

Le piccole e medie imprese

Basta leggere i più recenti report per accorgersi di questa strategia diretta alle Pmi italiane. In un'informativa del 17 febbraio scorso si legge che «dall'analisi delle sole segnalazioni e informative rilevate, trattate e coordinate sul territorio dal Cnaipic nel corso del 2022 è emerso che il settore più colpito da questo fenomeno è quello industriale-manufatturiero, caratterizzato maggiormente dalle piccole e medie imprese con una percentuale del 33%, sul totale dei casi trattati nel periodo di riferimento». Restando sul fronte impresa-professioni, le aziende di servizi e gli studi professionali, invece, assorbono il 20% degli attacchi.

Il minor numero di attacchi, invece, si registra su settori «strategici» caratterizzati da più importanti investimenti in termini di cybersicurezza. Così si scopre che il comparto sanità ha subito l'8% degli attacchi, istituzioni centrali ed editoria il 4%, trasporti il 3% e il sistema bancario solo l'1 per cento.

Cyberguerra

Lo scenario globale della minaccia cyber ha da tempo occupato un ruolo centrale nelle agende di politica di sicurezza dell'Ue. Gli analisti dell'*intelligence* sono ormai concordi nel ritenere che sempre più spesso organismi statali si affidano a cybercriminali per mascherare operazioni di spionaggio con il furto di dati sensibili. Dallo scoppio della guerra in Ucraina, infatti, sono stati rilanciati numerosi alert in tal senso, segnalando i rischi di operazioni di cyber-spionaggio collegati al conflitto.

Stando alle valutazioni della Polizia postale, sono in corso campagne massive a livello internazionale dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici quali comunicazione e difesa. Tra questi figurano campagne di *phishing*, diffusione di *malware* distruttivi (specialmente *ransomware*) e attacchi Ddos, come quello lanciato la scorsa settimana dal collettivo filo-russo NoName057

che ha mandato in stallo per alcune ore i siti web di ministeri, dei Carabinieri, della banca Bper e del gruppo A2A. Un'azione considerata dimostrativa dimostrativa contro la visita a Kiev della premier Giorgia Meloni.

© RIPRODUZIONE RISERVATA

RANSOMWARE

Le fasi dell'attacco

L'attacco *ransomware* base viene condotto utilizzando un virus informatico che avvia una sequenza di fasi per aprire la strada ad un «*cryptolocker*» in grado di rendere inservibile il sistema colpito. Successivamente gli attaccanti richiedono di essere contattati sul *dark web*. Così gli attaccati ricevono le istruzioni per riottenere l'accesso al sistema, ma solo dopo aver effettuato un pagamento in «*cryptovaluta*» su di un «*wallet*» riconducibile alla *cybergang*.



61%
Pmi nel mirino

Attacchi a livello globale
Secondo gli analisti, nel 2022 il 61% degli attacchi con ran-

somware a livello globale ha riguardato piccole e medie imprese. Scarsi investimenti sul fronte della cybersicurezza le rende maggiormente appetibili agli occhi delle *cybergang*, come emerge dagli alert delle autorità di cybersicurezza.

Il monitoraggio

I TARGET

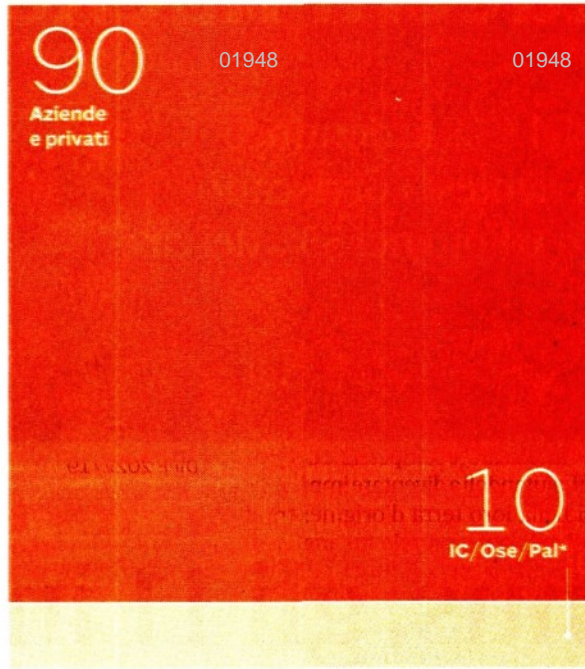
Attacchi, Ransomware per tipologia di vittima
Dati in %, 2022

3
1
1
2
Bancario



BERSAGLIO

Dal pubblico
al privato
Dati in %, 2022

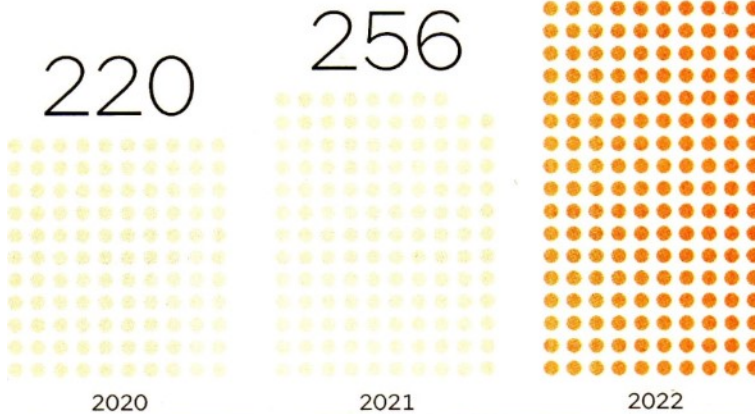


(*) Infrastrutture critiche; Operatori di servizi essenziali; Piccole amministrazioni locali

ATTACCHI GRAVI

La differenza negli ultimi tre anni

● = 2 ATTACCHI



Fonte: Polizia Postale e delle Comunicazioni 2023

vademecum

La Polizia postale ha elaborato un vademecum destinato al mondo dell'industria, allo scopo di prevenire spiacevoli e dannose intrusioni informatiche nei sistemi.

1

SICUREZZA

Aggiornamenti e software antivirus

- Utilizzo delle postazioni di lavoro esclusivamente per le attività strettamente legate all'attività di ufficio.
- Installazione periodica degli aggiornamenti di sicurezza dei sistemi operativi client/server e degli applicativi software utilizzati.
- Verifica che i Pc siano dotati di software di protezione (antivirus, firewall eccetera) e che le firme siano costantemente aggiornate.
- Eseguire il log out dagli applicativi al termine dell'attività lavorativa ed evitare, in generale, di rimanere loggati su più applicativi se non strettamente necessario.
- Non installare software non consentiti dalle policy della propria organizzazione e/o provenienti da fonti non ufficiali.
- Gestione delle reti wi-fi con adeguati sistemi di protezione.
- Cautela nell'utilizzo di pen drive o hard disk esterni limitandosi solo a quelli di sicura provenienza

2

01948

PASSWORD

Autenticazioni a due fattori

- Corretta gestione delle password con scadenza periodica e requisiti minimi di lunghezza e complessità. Un utile riferimento è rappresentato dalla versione 4.0 del documento Owasp Asvs (Application Security Verification Standard) che suggerisce, per le password utenti, una lunghezza minima di 12 caratteri.
- Utilizzare, ove possibile, l'autenticazione 2FA (2 factor authentication), in particolare per eventuali accessi remoti in Vpn alla propria infrastruttura Ict.
- Evitare di salvare password all'interno di file non cifrati o su documenti cartacei incustoditi.
- Evitare di utilizzare la stessa password per più applicativi.
- Evitare di salvare le password nei browser

3

01948

NAVIGAZIONE

Cautele nell'aprire email e messaggi

- Verificare sempre che il dominio di effettiva provenienza delle email ricevute sia congruo con il nominativo del mittente.
- Porre la massima cautela nella gestione di email sospette evitando di cliccare sui link contenuti e di aprire allegati.
- Verificare sempre la genuinità del dominio visitato via internet (Url presenti nella barra degli indirizzi del browser) prima di inserire credenziali di autenticazione di qualsiasi servizio web