Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2021: 232.485
Diffusione 05/2021: 254.214
Lettori Ed. I 2021: 1.734.000
Quotidiano - Ed. nazionale

CORRIERE DELLA SERA

Dir. Resp.: Luciano Fontana

08-AGO-2021
da pag. 1-9 /
foglio 1 / 3
www.datastampa.it

L'INCHIESTA

Hacker, quali sono le aziende ricattate Diciassette miliardi pagati in 4 mesi

di **Alessio Lana** e **Fiorenza Sarzanini**

In un rapporto riservato dell'intelligence la guerra, oramai globale, e le strategie dei cybercriminali. In soli quattro mesi incassati 17 miliardi di riscatto. Ecco come agiscono, chi sono e quali aziende hanno colpito.

a pagina 9

Il rapporto riservato sulle strategie della «ransom mafia» Oltre il 50% delle vittime cede: dal colosso Acer 42 milioni

Pagati 17 miliardi in quattro mesi Così gli hacker ricattano le aziende

L'inchiesta

di **Alessio Lana**
e **Fiorenza Sarzanini**

Maze, una sigla semplice. Una sigla che per almeno due anni è stata l'incubo delle aziende pubbliche e private, dei governi, di multinazionali come Canon, Lg, Xerox. Un gruppo di hacker in grado di bloccare sistemi, rubare dati, ricattare società e privati. Un gruppo pericoloso che per primo ha utilizzato la strategia del «name & shame», letteralmente nominare e svergognare. Il primo novembre 2020 ha dichiarato «chiuso il progetto» in grande stile, con un comunicato stampa pubblicato online in cui sottolineava che non ci sarebbero stati successori. Ma non è scomparso. Anzi. Già qualche mese prima della resa, un'altra banda, addirittura più capace e potente, era comparsa sulla scena: Egregor. In un anno ha sferrato oltre 200 attacchi e gli analisti ritengono possa essere lo schermo per gli affiliati di Maze. E poi ce ne sono tanti altri perché questa *Ransom Mafia*, come è stata definita, ricalca il mondo criminale «analogico»: individui che si riuniscono in gang, formano e sciolgono alleanze, si raggruppano in cartelli.

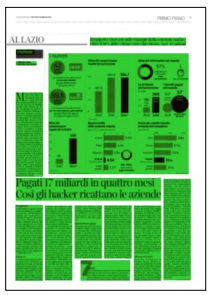
Il rapporto

A raccontare la guerra ormai diventata globale è un rapporto riservato dell'intelligence italiana che ricostruisce le strategie di questi cybercriminali, i loro obiettivi, le loro origini. Contiene nomi e date di una battaglia di cui l'Italia ha visto gli effetti più evidenti con l'assalto contro la Regione Lazio. Ma riporta soprattutto un dato che fa ben comprendere quale sia la posta in gioco: nel 2019 sono stati pagati 9,7 miliardi di euro per impedire ai criminali di bloccare i sistemi aziendali e diffondere le informazioni riservate, nel primo quadrimestre del 2021 questa cifra ha già raggiunto i 17 miliardi di euro.

L'attacco

Un attacco ransomware utilizza questi virus telematici per «limitare l'accesso al sistema informativo degli utenti e crittografare il disco rigido». I file diventano illeggibili dal legittimo proprietario che per sbloccarli ha bisogno di una specifica chiave crittografica. Ed è a questo punto che scatta il ricatto. Generalmente sullo schermo dei computer attaccati compare un avviso che invita ad aprire una pagina dove si trovano le istruzioni per il pagamento, nella maggior parte in criptovalute. Per i meno esperti c'è anche un'assistenza clienti multilingue.

Ma già dalla fine del 2020 la strategia si è evoluta, diventando ancor più subdola. Generalmente «l'operazione prevede che prima di procedere con la cifratura dei dati presenti nel sistema possa essere effettuata un'esfiltrazione di tutte le informazioni — spiegano gli analisti —. Fino allo scorso anno gli attacchi ransomware prevedevano quasi esclusivamente la crittografia dei dati che venivano resi indisponibili a tempo indeterminato. Nell'ultimo anno si è aggiunta la divulgazione dei dati nel dark web». È questa la «rivoluzione» di Maze, la «double extortion» (doppia estorsione): se non



Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2021: 232.485
Diffusione 05/2021: 254.214
Lettori Ed. I 2021: 1.734.000
Quotidiano - Ed. nazionale

CORRIERE DELLA SERA

Dir. Resp.: Luciano Fontana

08-AGO-2021
da pag. 1-9 /
foglio 2 / 3
www.datastampa.it

paghi per avere la chiave crittografica o tenti di aggirare il riscatto mettiamo i tuoi dati online. Dai brevetti alle informazioni dei clienti o degli utenti, tante informazioni sensibili rischiano di diventare pubbliche. Così si stima che tra il 50 e il 70 per cento delle vittime, alla fine, pagano.

Ransomware gang

Finora gli attacchi ransomware hanno colpito gestori delle reti energetiche e telefoniche, scuole e ospedali ma anche società quotate in Borsa. Hanno ricattato aziende di piccolo e medio livello che la pubblicazione dei dati avrebbe annientato e colossi industriali disponibili a pagare pur di mettere al sicuro le informazioni riservate. Ma soprattutto hanno trattato direttamente con i governi, proprio come avviene quando le formazioni terroristiche catturano gli ostaggi. Secondo l'ultimo rapporto *The State of Ransomware 2021* di Sophos, la maggior parte degli attacchi arriva da Russia, Cina e Corea del Nord ma ci sono altri focolai in Vietnam, Ucraina, India. I più clamorosi sono stati sferrati dal gruppo Revil nel 2021. In marzo hanno chiesto al colosso taiwanese Acer 42 milioni di euro. In aprile la medesima cifra a un partner di Apple per non diffondere segreti industriali. Subito dopo hanno preso di mira JBS Foods, che ha subito una richiesta per 9,3 milioni di euro, e in luglio, tramite il fornitore Kaseya, sono penetrati nei sistemi di numerose aziende chiedendo un totale di 59,5 milioni di euro. Alcune imprese hanno pubblicamente ammesso gli assalti. Nel maggio scorso la Colonial Pipeline, oleodotto che rifornisce la costa orientale degli Stati Uniti, ha pagato 3,7 milioni di euro al gruppo DarkSide per recuperare i propri dati e con l'intervento dell'Fbi ne ha poi recuperati 1,9. In Italia, il 6 agosto, il Gruppo Zegna ha rivelato di «non aver ceduto al ricatto». In realtà la lista di chi, nel nostro Paese, è stato colpito e ha pagato oppure è riuscito a fermare il ransomware è lungo, ma gli investigatori raccomandano di non diffonderla proprio per non dare vantaggi ai criminali e soprattutto enfatizzare la loro attività illecita.

Attacco a Israele

Qualche settimana fa Pay2Key, che ha matrice iraniana, ha pubblicato un post con l'elenco delle ditte colpite in Israele: Portnox, Israel Aerospace Industries, Habana, InterElectric, Mt, InfiApps e gli analisti ritengono si tratti «di un attacco con immediata finalità economica ma soprattutto una minaccia per gli interessi geopolitici di Stati attraverso le loro infrastrutture critiche». Da una parte le gang hanno un peso anche nelle relazioni internazionali. Come riportato dal *New York Times*, l'improvvisa scomparsa dei russi Revil in luglio, proprio dopo aver messo a ferro e fuoco gli Stati Uniti, è da attribuire a un accordo mirato tra Joe Biden e Vladimir Putin. Dall'altra si muovono anche come vere e proprie aziende. Premiano l'innovazione e lavorano per tenere alta la reputazione: se qualcuno riesce a riottenere i dati senza pagare è un problema, si diventa poco credibili. Sono organizzazioni ben strutturate, con decine di sviluppatori e macchinari e così, per ammortizzare i costi, hanno ideato il *Ransomware as a service* (Raas), «una variazione dei modelli di business rispetto a chi vende software legali», come spiegano gli analisti. Gli autori offrono il loro ransomware su licenza permettendo agli acquirenti di aggiungerlo ai propri attacchi. Esattamente come un software aziendale. In cambio chiedono una provvigione «tra il 20 e il 30 per cento dei riscatti pagati», possono rivendicare più vittime e quindi accrescere la fama della propria opera. E più il ransomware funziona più criminali lo vogliono. Come un qualsiasi prodotto di successo.

7 i giorni
trascorsi dall'attacco hacker al Centro elaborazione dati della Regione Lazio che il primo agosto ha disattivato tutti i sistemi informatici, compresi quelli del portale Salute e della rete vaccinale. Il sito per la prenotazione dei vaccini anti Covid è tornato a funzionare il 5 agosto

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2021: 232.485
Diffusione 05/2021: 254.214
Lettori Ed. I 2021: 1.734.000
Quotidiano - Ed. nazionale

CORRIERE DELLA SERA

Dir. Resp.: Luciano Fontana

08-AGO-2021
da pag. 1-9 /
foglio 3 / 3
www.datastampa.it

I numeri

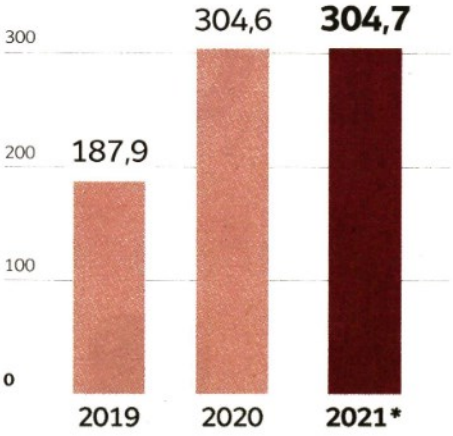
42 milioni di euro

La richiesta di riscatto record **a una sola azienda** *(gruppo REvil ad Acer nel marzo 2021)*

59,5 milioni di euro

La richiesta di riscatto record **per un solo attacco a più aziende** *(gruppo REvil nell'attacco a Kaseya nel luglio 2021)*

Attacchi ransomware registrati nel mondo



*inizio 2021

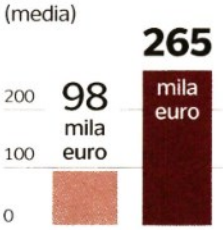
Attacchi informatici nel mondo

67% degli attacchi informatici **sono ransomware**

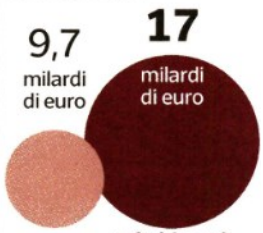
1 ogni **11 secondi**

Le richieste di risarcimento

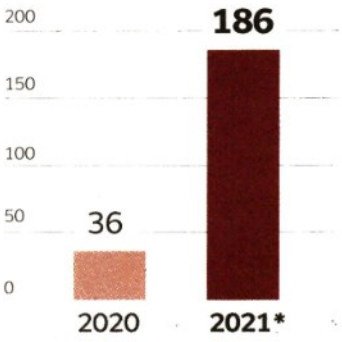
(media)



I riscatti pagati nel mondo



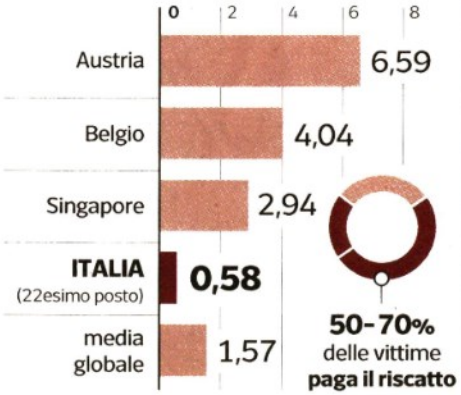
Attacchi ransomware registrati in Italia



*inizio 2021

Spesa media delle aziende colpite

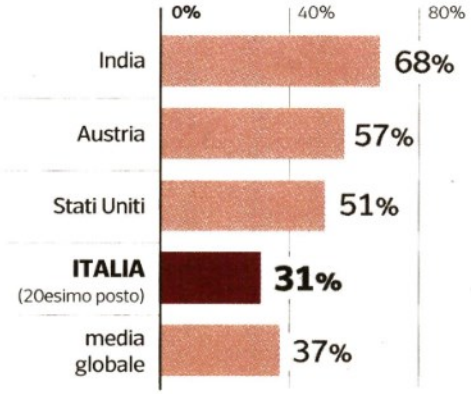
(dati 2021 in milioni di euro)



50-70% delle vittime **paga il riscatto**

Paesi più colpiti rispetto al totale del campione

(dati 2021)



Fonti: Polizia Postale, Sophos, Sonic Wall, McAfee, Kaspersky

Corriere della Sera