CORRIERE DELLA SERA

27-LUG-2017
pagina 16
foglio 1 / 3

Unicredit, il maxiattacco degli hacker

Interessati 400 mila clienti dei prestiti. La banca: nessuna violazione dei conti correnti, password al sicuro

La vicenda

- Unicredit ha subito un attacco hacker che ha coinvolto 400 mila clienti titolari di prestiti personali o di cessione del quinto
- Gli accessi non autorizzati sono stati scoperti e denunciati dalla stessa banca
- L'attacco è avvenuto usando le piattaforme di un partner commerciale esterno all'istituto

L'inchiesta
Indaga la Procura di Milano. Due attacchi a settembre-ottobre e giugno-luglio

MILANO Attacco hacker a Unicredit: circa 400 mila dati anagrafici, codici fiscali e Iban sono stati rubati dai sistemi del gruppo milanese attraverso alcune piattaforme collocate presso un partner commerciale esterno della banca, con il quale Unicredit colloca prestiti personali e cessioni del quinto. Sono proprio questi i clienti colpiti da una serie di «accessi non autorizzati» avvenuti in diversi momenti in due periodi distinti: settembre-ottobre 2016 e giugno-luglio 2017.

A rivelarlo è stata ieri mattina la stessa banca guidata da Jean Pierre Mustier: in nessun modo, ha specificato la nota del gruppo, sono stati attaccati, rubati o sono stati a rischio i soldi e i conti correnti dei clienti né sono state sottratte password o altri elementi per operare sui conti con transazioni o trasferimenti di denaro. Unicredit ha anche presentato un esposto alla procura di Milano, finita sul tavolo del procuratore aggiunto Alberto Nobili, responsabile del pool antiterrorismo e quindi competente anche di cybercrime, e del pm Enrico Pavone. Le indagini sono condotte dalla Polizia Postale. Chi può essere stato? E perché? «Non abbiamo conoscenza dello scopo dell'acquisizione di questi dati», ha detto Daniele Tonella, amministratore delegato di Ubis e capo dell'Information Technology global Unicredit.

L'allarme è scattato nella notte tra il 24 e il 25 luglio, ha spiegato Tonella, da un controllo di routine che ha fatto emergere alcune anomalie. Dalle verifiche è emerso che sfruttando una falla nel sistema esterno collocato presso la società partner, gli hacker abbiano scoperto un varco nella schermata iniziale del programma che consente l'accesso al sistema informativo di Unicredit per i clienti che hanno acquistato prodotti di credito al consumo. Da lì sono passati, riuscendo ad accedere alle schede iniziali delle schede di altri clienti e di rubarle («esfiltrarle», in gergo). A sottrarre i dati di 400 mila persone sarebbe stato utilizzato un «automa», cioè un software che scansiona automaticamente le schede e ne memorizza i dati. Che siano stati rubati emerge dalle varie tracce informatiche («log») lasciate dai vari accessi.

La reazione di Unicredit è stata immediata: dapprima sono state bloccate le utenze dei dipendenti della società partner (di cui non è stato divulgato il nome) usate per accedere ai dati; quindi sono state alzate le barriere informatiche; è stato verificato il numero dei clienti coinvolti e i periodi dell'attacco; sono stati avvisati Bce e Banca d'Italia e il consiglio d'amministrazione, avviato un audit interno e contemporaneamente istruite le filiali sulle risposte da dare e attivato un numero verde (800-323285). Una proceduta volta a minimizzare i danni, anche di immagine, considerata la mole di clienti coinvolti (400 mila su 7,5 milioni di clienti totali in Italia). Non a caso Unicredit ha specificato nella nota che il piano al 2019 prevede di investire «2,3 miliardi di euro per rafforzare e rendere sempre più efficaci i propri sistemi informatici». Ieri avevano chiamato il numero verde 4.600 persone, mentre in 2.600 avevano chiesto informazioni in filiale. Per sicurezza Unicredit non contatterà i clienti via posta elettronica o con chiamate dirette, per evitare il fenomeno del «phishing» (mail-pirata che mimando i siti di una banca rubano password e codici di accesso) e le truffe telefoniche.

Fabrizio Massaro

L'attacco e la difesa

Gli accessi non autorizzati nei sistemi di Unicredit

1 I CLIENTI COINVOLTI

400 mila

7,5 milioni
i clienti totali di Unicredit in Italia

Sono stati coinvolti solo soggetti titolari di prestiti personali e cessione del quinto

2 DA DOVE È PARTITO L'ACCESSO NON AUTORIZZATO

Da una società esterna, partner commerciale di Unicredit: vende ai clienti i prestiti al consumo offerti dal gruppo. L'attacco è partito da più utenze personali di dipendenti di questa società (non resa nota)

3 A QUANDO RISALE L'ATTACCO?

Dalle analisi di Unicredit sono due i periodi in cui l'accesso non autorizzato è avvenuto: settembre-ottobre 2016 e poi giugno-luglio 2017

4 COME SONO ENTRATI?

La società dispone di un accesso a un sistema informativo di Unicredit per verificare i clienti. Una falla nella schermata iniziale dell'applicazione ha consentito di consultare i dati di altri clienti Unicredit (titolari di prestiti personali)

5 COME HANNO SPULCIATO I DATI...

L'ipotesi è che abbiano utilizzato un «automa», cioè un software per scansionare e copiare i dati

6 E QUALI HANNO COPIATO?

I dati anagrafici del cliente, il codice fiscale, i codici Iban. Non sono stati «esfiltrati» dati che permettono di operare sui conti correnti (per esempio, le password)

7 L'ALLARME IN UNICREDIT...

Gli accessi non autorizzati sono stati scoperti nella notte tra il 24 e il 25 luglio scorsi nell'ambito di alcuni controlli di routine

8 E LE VERIFICHE

Dall'esame delle tracce informatiche (i cosiddetti «log») sono emersi gli accessi non autorizzati

9 LA REAZIONE

Unicredit ha immediatamente bloccato le utenze che venivano usate per accedere ai dati. Ha alzato le barriere informatiche per evitare altri attacchi. Ha verificato il numero di clienti coinvolti e i dati rubati

10 LA DENUNCIA

La banca ha avvisato le autorità bancarie (Bce e Banca d'Italia), informato il board e preparato le filiali a fornire informazioni ai clienti e attivato un numero verde. Ieri mattina, poi, la diffusione del comunicato stampa sull'attacco e la presentazione di un esposto in Procura

11 IL RAPPORTO CON I CLIENTI

La banca sta contattando i clienti interessati mediante canali di comunicazione specifici. Per ragioni di sicurezza non vengono utilizzate la posta elettronica o le telefonate dirette