

# Crimini in rete, una impresa su 17.000 è danneggiata

EDEN UBOLDI

Solo una impresa su 17.000 ha subito un danno economico a causa di un crimine informatico. Ecco uno dei principali risultati emersi in «Sicurezza e frodi informatiche in banca», il rapporto del consorzio ABI Lab sulla sicurezza online nel 2016, realizzato nell' ambito delle attività di ricerca del CertFin (Computer emergency response team). Nello scorso anno, infatti, per quanto riguarda le imprese clienti, il 93,2% delle transazioni fraudolente e il 96,5% degli importi corrispettivi sono stati efficacemente bloccati o recuperati, percentuali di successo più alte rispetto alla clientela retail (91% di transazioni fraudolente e il 94% degli importi sono stati bloccati o recuperati). Complessivamente gli importi associati alle transazioni anomale su tutta la clientela sono diminuite del 34,4% rispetto al 2015, a conferma dell' attenzione delle banche per la sicurezza informatica. Per la sottrazione del denaro, i frodatori prediligono i bonifici, perché consentono in una singola operazione di spostare importi ingenti: per il segmento corporate, il 61,9% delle transazioni anomale effettuate avviene tramite bonifico a un' altra banca italiana, mentre per quello retail si tratta del 57,5%. Se in passato i cybercriminali erano soliti utilizzare anche l' espediente della ricarica a una carta prepagata, nel 2016 questo trend è stato fortemente diminuito. Riguardo alle tipologie di attacchi, nel caso delle imprese, la maggioranza dei furti delle credenziali d' accesso ai servizi di internet e mobile banking è avvenuta attraverso campagne di diffusione di malware (si tratta di un codice malevolo che può essere diffuso attraverso programmi, documenti o messaggi di posta elettronica, in grado di rendere disponibili informazioni riservate e codici d' accesso al truffatore), mentre per la clientela al dettaglio con le tecniche di phishing (truffa informatica effettuata inviando un' e-mail al cliente per carpire dati riservati come il numero di carta di credito e password di accesso al servizio di home banking). Anche il momento in cui si realizza l' attività truffaldina è diverso per i due profili: per il retail l' 81,1% delle frodi è stato realizzato durante sessioni



di log in specifiche, per i clienti corporate il 61,5% degli attacchi sono stati eseguiti durante le sessioni di log in del cliente, durante le quali i malviventi interferiscono nel flusso comunicativo tra cliente e banca, cambiando i dati in tempo reale.