© LA RIPRODUZIONE E LA UTILIZZAZIONE DEGLI ARTICOLI E DEGLI ALTRI MATERIALI PUBBLICATI NEL PRESENTE GIORNALE SONO ESPRESSAMENTE RISERVATE

CRIMINI AL COMPUTER

CENTO I RAGGIRATI. LA BANDA, 4 CALABRESI E UN ABRUZZESE, COLPIVA IN TUTTA ITALIA. INDAGINE DEI CARABINIERI DI MESSINA

Scoperta maxi truffa informatica: 5 arresti

In meno di due mesi avrebbero incassato un milione e 200 mila euro, soldi fatti sparire tramite passaggi su vari conti bancari

Le accuse, a vario titolo, nei confronti degli arrestati sono di associazione per delinquere finalizzata alla frode informatica, accesso abusivo a sistema informatico o telematico e sostituzione di persona.

Letizia Barbera
MESSINA

••• Un'organizzazione con base in Calabria, ma attiva sull'intero territorio nazionale specializzata a sottrarre denaro dai conti correnti bancari on line. Un raggiro scoperto con l'operazione «Fraudatores» che ha portato a cinque arresti per, a vario titolo, associazione per delinquere finalizzata alla frode informatica, accesso abusivo a sistema informatico o telematico e sostituzione di persona. L'organizzazione composta da quattro calabresi ed un abruzzese riusciva a colpire in tutta Italia. Il gip Salvatore Mastoreni, su richiesta della procura di Messina diretta dal procuratore Maurizio de Lucia, ha disposto anche il sequestro preventivo di oltre 1 milione 200 mila di euro.

«Un'associazione super organizzata» come la definisce il gip nell'ordinanza «dotata di strumenti e metodi operativi perfettamente organizzati». Le indagini dei carabinieri del Nucleo investigativo di Messina con il reparto indagini telematica del Ros, coordinati dal sostituto procuratore Antonella Fradà, sono cominciate a febbraio quando i carabinieri si sono imbattuti in una pec sospetta. E proprio da questo punto sono cominciati gli accertamenti che hanno portato in Calabria, nella fascia jonica reggina. Si è scoperto che l'organizzazione sarebbe stata in grado di modificare, sui principali siti web istituzionali (Telemaco Infocamere, www.inipec.gov.it, www.registroimprese.it, etc..), gli indirizzi di posta elettronica certificata, la pec, di alcuni tra i più noti istituti di credito nazionali ed esteri, sostituendoli con quelli di analoghe caselle di posta certificata, denominate in modo simile alle originali, intestate a persone ignare o inesistenti. L'attacco cibernetico si attuava attraverso il Mitm (man in the middle): grazie alla falsa pec da un lato gli indagati riuscivano ad interporsi tra i titolari dei conti correnti on line e i rispettivi istituti e, dall'altro, ad entrare in possesso delle credenziali di accesso ai rapporti finanziari, utilizzando le quali disponevano una sequenza di operazioni home-banking in favore di ulteriori conti bancari, intestati a ignare vittime di furto d'identità ma gestiti dagli stessi appartenenti al gruppo. Per rendere più credibile la loro truffa, avevano creato anche profili facebook. Diversi i casi scoperti dai carabinieri in pochi mesi di indagine come quello di una donna della provincia di Milano che aveva contattato la falsa pec per chiudere il proprio conto corrente. Era stata ricontatta telefonicamente da un finto funzionario della banca che era riuscito a farsi indicare i codici per operare su quel conto. La donna era convinta che il suo conto era chiuso ma, in realtà, erano stati sostituiti tutti i suoi recapiti con altri e siccome sul conto c'erano pochi euro, la carta di credito è stata utilizzata per compiere una serie di acquisti on line. Anche un'altra donna di Milano aveva fornito le sue credenziali ma poco dopo, verificava la sua situazione bancaria scoprendo che era appena stato effettuato un bonifico di 49 mila euro dal suo conto corrente verso un conto intestato ad una terza persona, a sua volta raggirata. Ad un uomo di Bergamo, la cui moglie è deceduta, era stato fatto credere di potere risolvere in tempi rapidi il problema della successione alla moglie nel conto corrente. L'anziano, per sua fortuna, aveva fornito dei codici sbagliati quando si è recato in banca l'impiegata ha scoperto tutto e lo ha salvato.

L'arresto è scattato per Giuseppe Cesare Tricarico, 37 anni, di Gioiosa Ionica, Davide Tricarico, 33 anni di Grotteria, entrambi già agli arresti domiciliari per altro, Nicola Ameduri, 35 anni di Gioiosa Ionica e Nicodemo Porporino, 54 anni di Grotteria e Antonello Cancelli, 35 anni di Avezzano in provincia dell'Aquila. (*LEBA*)

Le indagini dei carabinieri partite quando si sono imbattuti in una pec (posta elettronica certificata) sospetta

L'INTERVISTA. Gerardo Costabile, esperto informatico

«Attenzione alle email Lì ci sono le trappole»

Andrea D'Orazio

Sembrerebbe il titolo di un romanzo giallo, ma è il nome che identifica, con efficacia, il meccanismo di truffa finanziaria scoperto dai carabinieri di Messina: «man in the middle», letteralmente, «l'uomo in mezzo». Sistema diffuso o rarità? Gerardo Costabile, amministratore delegato della società DeepCyber, specializzata in intelligence e cyber security, ex investigatore della guardia di finanza ora consulente per il settore bancario e per la magistratura, nonché docente universitario, allarga lo sguardo sull'orizzonte internazionale e inquadra subito «uno stratagemma fraudolento praticato in tutto il mondo, non solo ai danni di correntisti e istituti di credito, ma anche e soprattutto delle aziende».

••• Un esempio concreto?

«Prendiamo il caso di una società di costruzioni: prima la si studia attentamente per capire quali sono le ditte di cemento o di altre materie prime con cui lavora, poi il truffatore si interpone tra l'ufficio acquisti e i fornitori in modo tale da falsificare Iban e fatture. I clienti pensano di pagare correttamente, ma i soldi finiscono su un altro conto corrente, magari a Dubai. Questo metodo viene usato anche per intromettersi tra banche e imprese».

••• Per attuarlo bisogna essere esperti di informatica?

«In realtà, il modus operandi individuato dalle indagini siciliane non richiede grandi competenze, e il ricorso al linguaggio digitale è opzionale, anche se, indubbiamente, può agevolare la truffa. In questo episodio, ad esempio, è stata usata la posta elettronica certificata per avere più credibilità di fronte alle vittime, ma determinate è stata l'abilità dei truffatori ad apprendere e sfruttare i punti deboli dei correntisti. L'informatica è invece alla base di un'altra tecnica utilizzata per gabbare banche e clienti, più sofisticata, subdola e altrettanto diffusa».

Gerardo Costabile

••• Cioè?

«Infettare con un virus i computer degli utenti che gestiscono online i conti aperti negli istituti di credito, creando un falsa interfaccia per le transazioni bancarie. In tal modo, il cliente crede di effettuare un bonifico di un certo valore, ma quando va a controllare si accorge che la somma è più alta e il destinatario è diverso. Il virus viene diffuso di solito attraverso l'email: basta cliccare su allegati o link cosiddetti "malevoli" e finiamo nel mirino del pirata di turno».

••• Dal lato del cliente, come ci si può difendere da questi attacchi?

«Con semplici regole. Mi limito a ricordarne un paio. Innanzitutto, aggiornare almeno una volta al mese sia il sistema operativo del computer sia i vari software che utilizziamo nei nostri dispositivi, senza dimenticare di fare altrettanto con gli antivirus. Ma attenzione, bisogna avere la stessa cura con le applicazioni degli smartphone, che oggi sono il vero scrigno dei nostri segreti e vengono usati quanto o più del Pc, anche per effettuare bonifici».

••• E sul fronte banche? Gli anticorpi sono all'altezza della sfida?

«Rispetto a qualche anno fa, gli istituti investono di più in cyber security, hanno innalzato tutta la parte relativa all'autenticazione delle transizioni con le password temporanee e stanno implementando l'intelligence antifrode cooperando tra loro. Bisogna insistere su questa strada, aumentando il numero di analisti ed esperti, perché da sola l'informatica non basta. Detto ciò, il rischio zero non esiste, altrimenti si romperebbe l'equilibrio tra difese ed esigenze dei clienti: più il sistema è blindato, più i correntisti troverebbero difficoltà ad effettuare operazioni online». (*ADO*)