



# Criminalità informatica in Romania



**Dr. Marian Mandroc**  
Ufficiale di collegamento  
Polizia Romania

La Direzione di Contrasto alla Criminalità informatica, presso Ispettorato Generale della Polizia Romena è nata nel 2008, attraverso la riorganizzazione dell'Ufficio di Contrasto alla Criminalità informatica e aree di competenza con i seguenti compiti:

- prevenzione e contrasto dei reati informatici;
- prevenzione e contrasto dei reati pedopornografici via internet;
- prevenzione e contrasto dei reati con le carte di credito;
- controlli informatici e la elaborazione dei dati informatici ottenuti a seguito di accesso, conservazione e intercettazione di dati informatici;

Una caratteristica molto importante dell'evoluzione del fenomeno criminale di tipo informatico come parte integrante del fenomeno criminale organizzato in Romania, è quella del nuovo orientamento dei gruppi criminali.

Si osserva che una parte delle reti criminali organizzate che agivano a livello transnazionale, e che in passato svolgevano le loro attività in altri campi quali: traffico di autovetture rubate, traffico di esseri umani e anche traffico di sostanze stupefacenti, attualmente si occupano

della commissione di reati con carte di credito e su internet, e che le somme ottenute fraudolentemente in seguito a questo tipo di attività è nettamente superiore a quelle ottenute in passato.

I principali fattori che hanno spinto i gruppi criminali ad orientarsi verso la commissione di reati di tipo informatico sono:

- guadagni elevati in tempi molto brevi e con rischi relativamente minimi;
- la prova della commissione del reato necessita nella maggior parte dei casi, di informazioni da parte di diverse Autorità competenti di altrettanti Stati, (per lo più a seguito di richieste di assistenza giudiziaria / cooperazione internazionale), che sono procedure lente e con un costo elevato;
- facile accesso ad attrezzature informatiche moderne che permettono di commettere tali attività illecite, anche molto complesse;
- la facilità di spostamento rapido da uno Stato all'altro da parte del gruppo criminale ( infatti il pedinamento del gruppo criminale ed il monitoraggio delle loro attività illecite diventano procedure molto difficili da realizzare da parte delle Autorità competenti in tempi brevi).

Nel nostro paese, la criminalità informatica si manifesta principalmente sotto due aspetti:

**frodi informatiche** che consistono in vendite all'asta di beni fittizi, violazione dei conti correnti di alcuni siti utilizzati nel commercio elettronico, ed in ultimo siti di *phishing*;

**frodi con carte di credito** che consistono nella alterazione di sportelli ATM, per la successiva cattura di informazioni dalle bande magnetiche delle carte di credito.

Gli obiettivi perseguiti dai gruppi crimi-



nali che agiscono in questo campo, dimostrano che questi hanno come scopo la realizzazione di un prodotto finanziario sostanziale, a tal proposito, utilizzano dei giovani, con notevoli capacità informatiche, conoscitori delle più recenti tecnologie, che quindi sono organizzati e coordinati dai leader dei gruppi criminali a livello internazionale.

Analizzando il fenomeno criminale, si evidenziano i seguenti principali "modus operandi", per la captazione illecita di dati quali codici PIN, dati personali etc:

**phishing**: consiste nella creazione di pagine internet false che imitano le pagine istituzionali finanziari (per esempio banche o esercizi commerciali), nell'invio di messaggi email con lo scopo di indurre in errore le potenziali vittime, per ottenere dati sensibili quali: numerazione carte di credito, data di scadenza, passwords, coordinate dei conti bancari, etc;

**skimming**: consiste nel copiare le bande magnetiche delle carte di credito con lo scopo di clonarle. Recentemente questo fenomeno ha conosciuto una vera esplosione in termini di espansione del fenomeno. Per quanto riguarda le tecniche di manipolazione degli ATM e dei terminali POS, si è registrata una rapidissima evoluzione delle tecniche e dei dispositivi artigianali realizzati per tali scopi illeciti (catture i dati delle bande magnetiche delle carte di credito e dei codici PIN degli ignari utenti).

All'estero, le principali attività svolte dai cittadini romeni consistono in:

- installazione di dispositivi "skimmer" presso i bancomat oppure di "microchip" all'interno degli apparati POS allo scopo

della captazione dei dati dalle carte di credito/debito;

-lo scaricamento “download” di questi dati sui computer per la successiva riscrittura della nuova carta di credito;

-la trasmissione dei dati delle carte di credito in Romania, dove si realizza la “nuova” carta di credito;

-ritiro delle somme di denaro dagli sportelli bancomat oppure acquisto di prodotti;

Per quanto riguarda i dispositivi che si installano nei POS, ci si riferisce a *microchip*, cioè memorie che “registano” le informazioni dalle carte di credito. I microchip sono installati con il consenso di alcuni commessi che svolgono la loro attività presso diversi commercianti oppure entrando in modo illegale all’interno dei negozi e montandoli negli apparecchi POS.

Riguardo agli sportelli bancomat, ognuno di essi viene studiato a seconda del paese dove si opera, effettuando delle foto, che vengono inviate in Romania, per la realizzazione di tastiere ed il resto dei dispositivi necessario all’acquisizione dei dati delle carte di credito e relativi codici PIN.

Una volta realizzate tali dispositivi vengono inviati all’estero per essere utilizzati dai gruppi criminali.

In Romania si realizzano principalmente i dispositivi che vengono installati sugli sportelli bancomat ed i terminali POS, e l’attività di prelievo fraudolento di somme di denaro tramite la creazione di carte di credito contraffatte.

Si rappresenta che l’attività di un gruppo di questo tipo, è coordinata dalla Romania direttamente attraverso gli uomini di col-



legamento che si trovano nei paesi colpiti e che svolgono delle attività ben precise.

Le attività intervento sono principalmente



le seguenti:

- di coordinamento dei gruppi criminali da parte dei leader delle organizzazioni criminali, operanti a livello internazionale

- di installazione dei dispositivi da parte dei gruppi criminali operanti all’estero;

- di prelievo di somme di denaro tramite carte di credito contraffatte da membri dell’organizzazione operanti all’estero oppure in patria ;

- creazione di dispositivi per la captazione dei codici delle carte di credito presso sportelli bancomat e terminali POS tramite specialisti del settore delle frodi informatiche ;

- di scaricamento dei dati dalle bande magnetiche delle carte di credito carpite illegalmente tramite specialisti del settore delle frodi informatiche ;

- di trasporto di dispositivi, informazioni tecniche e denaro all’estero tramite membri fidati individuati dall’organizzazione criminale;

E’ importante sottolineare che le informazioni delle bande magnetiche delle carte di credito e le immagini dell’equipaggiamento o i tipi di bancomat, sono trasmesse regolarmente via posta elettronica.

I reati specializzati nella commissione di questo tipo di reati provengono in prevalenza dalle seguenti province: Bacau, Dolj, Constanta, Valcea, Bihor, Brasov, Dimbovita, Iasi, Olt, Mehedinti, Hunedoara e Bucarest.

I paesi presi di mira sono i seguenti: Francia, Italia, Gran Bretagna, Germania, Belgio, SUA, Spagna e Olanda.

**Violano i server per manie di grandezza**

Quest’anno, i reati informatici, hanno avuto una valenza senza precedenti.

La maggior parte di quelli che commettono questi tipi di reato, sono i giovani o anche adolescenti, dotati dal punto di vista intellettuale, che hanno fatto del computer una vera e propria passione. E’ vero che la maggior parte di questi violano i server di alcune compagnie, istituzioni pubbliche o agenzie governative americane, sia per mania di grandezza sia per dimostrare semplicemente a quelli che stanno loro intorno di quello di cui sono capaci.

Più grave è però il fatto che ultimamente, sono apparsi dei casi in cui, questi giovani hanno capito che possono diventare ricchi in maniera rapida, e non hanno esitato ad associarsi per questo scopo ai membri di organizzazioni criminali a livello mondiale, così sostengono i specialisti in materia della Polizia.

La presenza dei hacker romeni si è sentita sul “mercato internazionale” sin dal 1999, quando 6 giovani (4 ragazzi e 2 ragazze) riuniti sotto nome di “Pentaguard” hanno attaccato più reti governative della Cina e degli USA, dopodiché hanno unito le loro forze con un gruppo simile in Russia e in soli due mesi, hanno violato 20 server governativi, hanno distrutto il server delle Forze Armate USA di stanza in Corea e sono riusciti ad entrare anche nel sistema difensivo della Difesa americana.