# ATTACCHI INFORMATICI NEL 2014

## COSA ASPETTARSI? COSA TEMERE?

*Marco Bozzetti, OAI founder*

Insieme al Rapporto 2013 OAI, in questo periodo sono stati pubblicati numerosi rapporti internazionali che, oltre a fare il punto sulla situazione nel 2013, stimano gli attacchi più critici e/o più probabili che potrebbero occorre nel presente anno. Come evidenziato nella fig. 1 dal Rapporto 2013 i tre attacchi più temuti per il prossimo futuro sono nell'ordine il malware, il furto 'fisico' di apparati ICT, il furto di informazioni dai dispositivi d'utente sia mobili che fissi.

Contrariamente all'edizione scorsa, il social engineering non è più sul podio ma si classifica al 5° posto. La nuova famiglia di attacchi introdotta, i TA, Targeted Attacks, e gli APT, Advanced Persistent Threats, si posiziona al 12° posto, ragionevolmente temuta solo da grandi organizzazioni potenziali target. Nella voce 'Altro' sono stati specificati attacchi a sistemi di controllo industriale quali DCS, distributed control system, e Scada, supervisory control and data acquisition, che molti considerano attacchi TA-APT.

Facendo riferimento al confronto delle previsioni di attacchi più temuti delle scorse edizioni OAI, confronto puramente indicativo data la diversità dei campioni dei rispondenti, emerge che le stime di attacco più temibile sono profondamente cambiate anno dopo anno, ma sono rimasti sempre 'caldi' i codici maligni, il social engineering, il furto di informazioni da dispositivi fissi e mobili, i furti fisici di dispositivi ICT.

Le possibili motivazioni per gli attacchi sono invece state stimate in maniera molto simile nelle varie edizioni di OAI, come evidenziato nella fig. 2. Il punto di discontinuità in figura è dato dal termine di 'hacktivism', introdotto per la prima volta nell'edizione 2013. Al primo posto è la frode informatica, cui segue il vandalismo e il sabotaggio. Da quest'anno al quarto posto l' hacktivism.

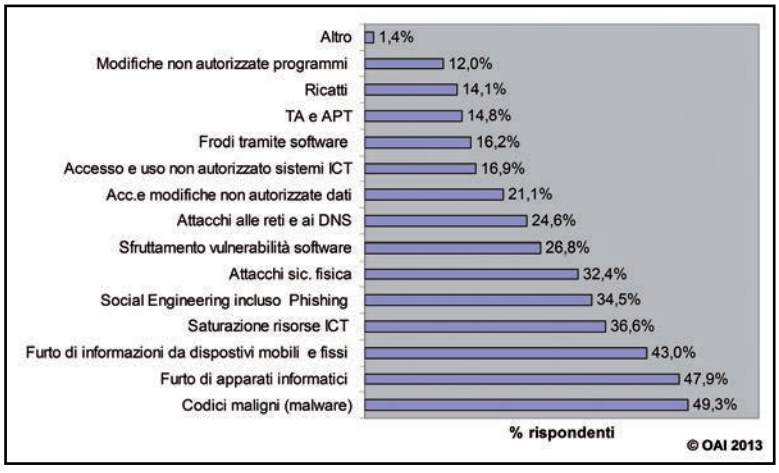


*Fig. 1 - Gli attacchi più temuti nel prossimo futuro dal Rapporto 2013 OAI*

### Cosa indicano gli altri rapporti?

Gran parte dei rapporti con previsioni sugli attacchi nel 2014 ed oltre sono internazionali e l'Italia per gli attacchi ICT gioca, almeno per ora, un ruolo marginale rispetto ad altri paesi: nel 2013 infatti l'Italia era stimata a meno dell'1% rispetto a tutti gli attacchi a livello mondiale. Questo forse grazie all'elevato numero di piccole e micro imprese con sistemi informatici di limitate dimensioni che non sono un target interessante per i cyber criminali. Ciò non significa che l'Italia sia un'isola felice priva di attacchi informatici, ma

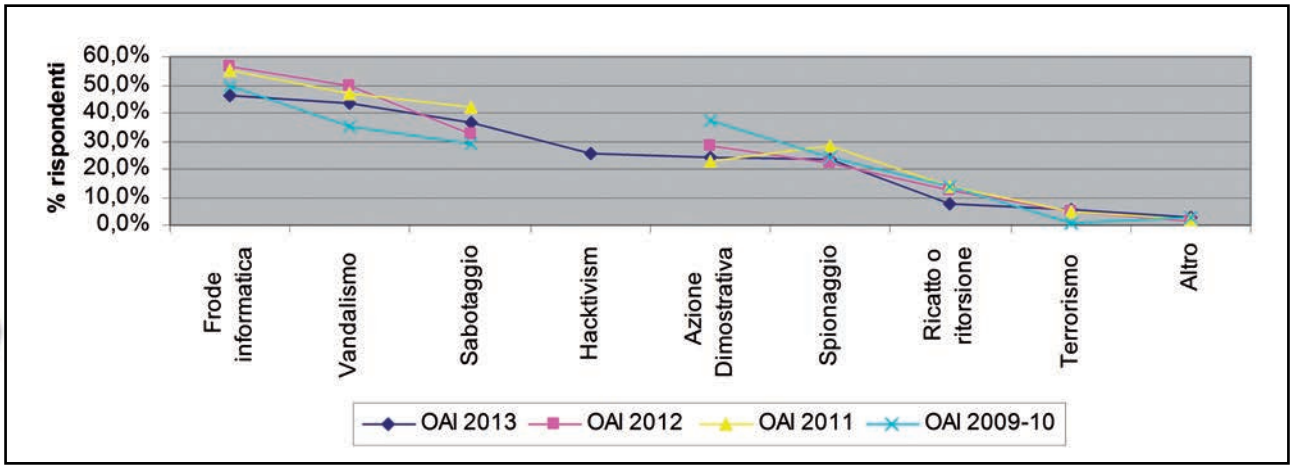


*Fig. 2 - Le probabili motivazioni per gli attacchi dai vari Rapporti OAI*

che è relativamente limitato il numero di attacchi subiti e rilevati, e in media è limitato anche l'effetto di tali attacchi.

Considerando le previsioni di alcuni dei più noti rapporti (tra cui quelli di Enisa Microsoft IBM XForce, McAfee, Sophos, Trend Micro, Websense), tutti enfatizzano la crescita in numero, criticità e sofisticazione degli attacchi futuri. Più in dettaglio ho cercato di sintetizzare le varie previsioni di questi rapporti nei seguenti punti:

- codici maligni: se ne introducono di nuovi sempre più sofisticati, e si creano nuovi malware basandosi sui programmi di quelli 'antichi' e non più considerati oltre che su software (tipicamente di base) non più supportato dal produttore, ma ancora 'in produzione'. In particolare destano forte preoccupazione per il prossimo futuro:
  - i malware per i dispositivi mobili, soprattutto per tablet e smartphone, che aumenteranno fortemente in volume e sofisticazione;
  - i ransomware, suddivisi
    - in lock-screen, che provocano l'inutilizzabilità della risorsa ICT, normalmente un pc, visualizzando un messaggio con la richiesta di riscatto del criminale, perché rimuova il malware;
    - i ransomware crittografici, ora fortemente in crescita, che criptano dati e file bloccandoli fino al pagamento di un riscatto: tipico esempio il CryptoLocker, che utilizza chiavi a 2048 bit;
- forte crescita di attacchi di social engineering;
- aumento come numero e come sofisticazione di TA e APT;
- attacco ai big data, in pratica grandi repository di informazioni, molte delle quali di interesse per i cyber criminali;
- aumento attacchi basati sulla saturazione delle risorse ICT, i DoS/DDoS, Denial of Service/ Distributed DoS;
- sfruttamento vulnerabilità software di base e in particolare di HTML5;
- attacchi ai servizi in cloud, che apre nuovi spazi di vulnerabilità, così come dettagliato nel rapporto CSA, Cloud Security Alliance, di febbraio 2014 con le nove principali minacce per il cloud: data breaches, data loss, account hijacking, insecure APIs, malicious insiders, abuse of cloud services, insufficient 'due diligence', shared technology issues;
- consolidamento di nuovi kit di exploit, quali Neutrino e Redkit,che andranno a sostituire il ben noto e diffuso Blackhole, il cui presunto autore è stato arrestato in Russia;
- attacchi all'Internet delle cose (Internet of Things);
- attacchi a Bitcoin e alle monete virtuali, soprattutto con l'utilizzo di dispositivi mobili.

**Marco Bozzetti**
marco.bozzetti@malaboadvisoring.it