Cybersecurity, dagli USA arrivano gli “Zombie”

Dal 1° dicembre 2016 l’FBI può “hackerare” ogni computer a scopo investigativo. Si riapre il dibattito tra privacy e sicurezza[1]

***“La battaglia contro i cybercriminali deve essere combattuta ad armi pari. Gli Stati Uniti indicano una strada che anche il nostro legislatore dovrebbe seguire, per dotare le forze dell’ordine di strumenti efficaci”*, rileva Maurizio Mensi, professore di Diritto dell’informazione all’Università LUISS Guido Carli di Roma.**

Dal 1° dicembre 2016 negli Stati Uniti l’FBI può farsi rilasciare un mandato per “hackerare” a scopo investigativo un computer ovunque questo si trovi. Ciò in seguito all’entrata in vigore di un emendamento alla *Rule 41* del codice di procedura penale (le *Federal Rules of Criminal Procedure*), che consente ad un giudice statunitense di autorizzare l’accesso da remoto ad un dispositivo elettronico anche al di fuori della propria giurisdizione. Dopo aver superato il vaglio di diverse istanze giurisdizionali, la norma federale è stata ritenuta legittima dalla Corte Suprema lo scorso aprile e il Congresso non è intervenuto per emendarla prima della sua entrata in vigore. Pertanto, l’FBI ha ora la possibilità di accedere attraverso la rete Internet a computer anche qualora siano occultati da software anonimi come TOR o per individuare quelli infettati dal *malware* che li ha resi parte della rete botnet, metodo usato da criminali per diffondere spam o virus su larga scala, come nel caso dei fratelli Occhionero. Si tratta di una rete di computer, noti come bot o zombie, comandata a distanza che appartengono per lo più ad ignari utenti che, non avendo protetto adeguatamente il proprio sistema, sono stati infettati e catturati nella botnet. In questo caso il computer viene reso controllabile e utilizzato per lanciare attacchi o infettarne altri. Il problema è molto rilevante, sia per le dimensioni che sta assumendo sia per i danni anche economici che provoca, a causa dei sistemi tecnologici compromessi in seguito agli attacchi e dei siti disabilitati, talora inondati da un’ingente quantità di traffico creato artificialmente. L’emendamento alla norma federale ha suscitato aspre critiche. Ne sono state evidenziate le pesanti conseguenze per la privacy dei cittadini americani e la circostanza che l’ordine di accesso in questo caso riguardi i computer delle vittime, non quelli degli autori del cyber crime. Ecco perché da taluni è stata ritenuta una misura sproporzionata in quanto autorizza una sorta di “hackeraggio” di massa ad opera di un soggetto pubblico. Il Dipartimento di Giustizia USA si è difeso sostenendo che la ricerca e l’intromissione nel computer zombie serve a risalire all’origine dell’infezione, a comprenderne l’entità e le sue caratteristiche al fine di consentirne la rimozione. Tale misura sarebbe pertanto indispensabile per fronteggiare il crescente numero di crimini commessi da utenti anonimi e che derivano dalle botnet infette, ed essenziale per combattere reati come la distribuzione online di materiale pedopornografico. Insomma, torna alla ribalta il tema delle regole che disciplinano i poteri investigativi delle forze di polizia; ci si chiede in particolare fino a che punto e a quali condizioni possa essere consentito l’utilizzo su larga scala di invasivi strumenti di “hackeraggio” come quello autorizzato negli Stati Uniti. Come rileva Mensi, “*in Italia la Corte di Cassazione a Sezioni Unite ha autorizzato nell’aprile 2016 l’uso del virus Trojan per captare “conversazioni o comunicazioni tra presenti” in procedimenti “relativi a delitti di criminalità organizzata, anche terroristica” nonché “quelli comunque facenti capo a un’associazione per delinquere, con esclusione del mero concorso di persone nel reato”, indicando una strada che a questo punto potrebbe essere percorsa anche dal legislatore, con uno specifico intervento normativo*”.

Maurizio Mensi *insegna Diritto dell’economia alla Scuola Nazionale dell’Amministrazione e Diritto dell’informazione e della comunicazione alla LUISS Guido Carli. È stato procuratore dello Stato, funzionario della Commissione europea (D.G. Telecomunicazioni e Servizio Giuridico), avvocato dello Stato e docente alla Cà’ Foscari di Venezia, Direttore del Servizio Giuridico dell’AgCom. Avvocato ed esperto TAIEX della Commissione europea, è autore di varie pubblicazioni in tema di comunicazioni elettroniche, media, regolazione e concorrenza.*

[1] Il tema è ripreso dalla rubrica Impronte Digitali, Airpress, dicembre 2016.