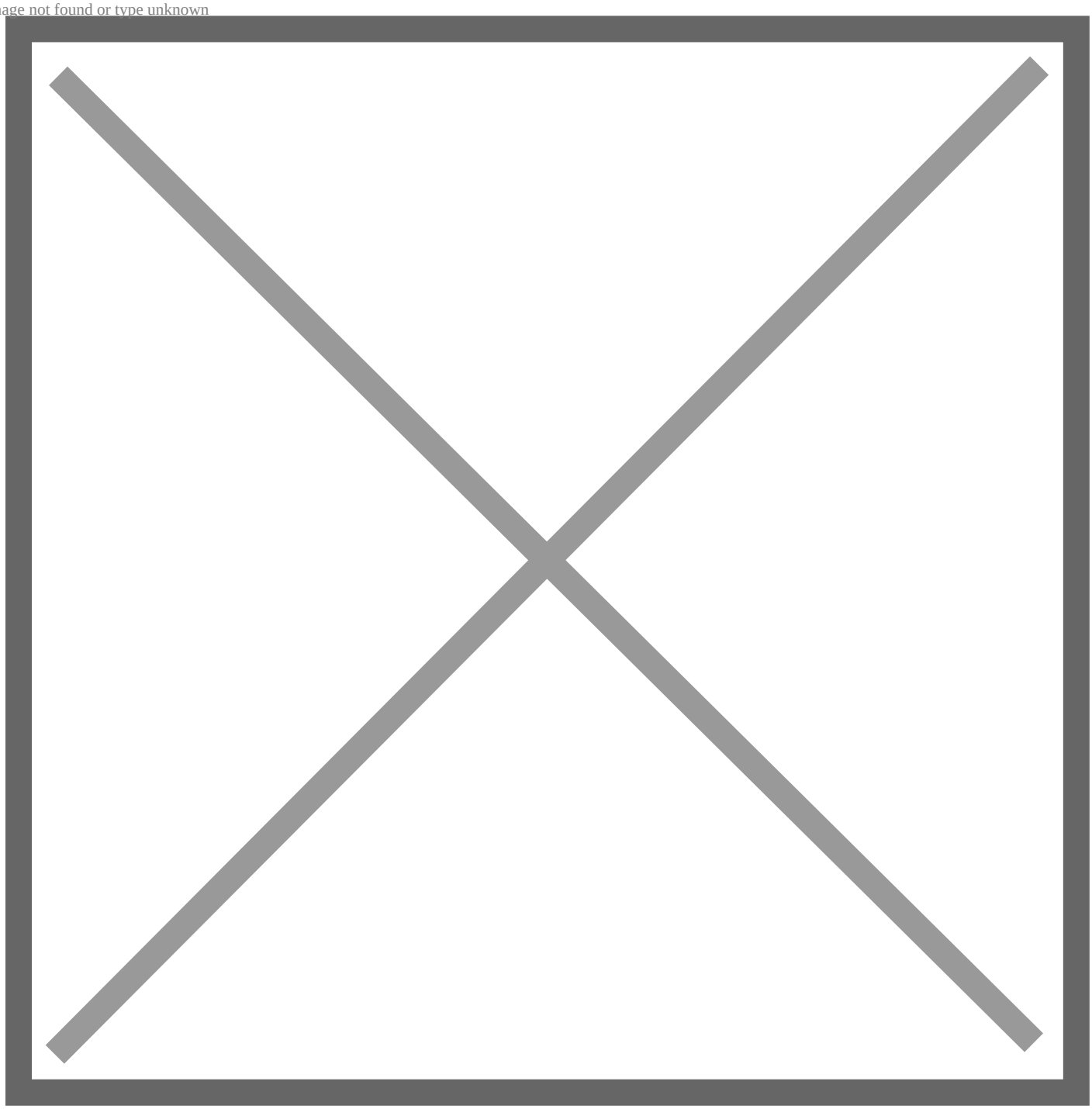
Image not found or type unknown



CRISI UCRAINA

Crimea, una guerra invisibile è iniziata sul Web

INTERNACIONAL 12_03_2014

Ucraina, hacker in azione

Image not found or type unknown

In Crimea non si stemperano le tensioni militari. Russi e filo russi assediano le poche installazioni rimaste nelle mani dei soldati di Kiev e hanno espugnato senza sparare un colpo i posti di frontiera tra Ucraina e Repubblica di Crimea mentre un velivolo da ricognizione ucraino sarebbe stato messo in fuga domenica dal fuoco esploso da terra mentre sorvolava la località di Armiansk, nel settore occidentale dell'istmo di Perekop, che unisce la Crimea all'entroterra continentale. Fonti di Kiev hanno attribuito la responsabilità dell'episodio agli "aggressori russi", ma, al di là delle provocazioni e delle pressioni militari, Mosca avrebbe già utilizzato armi ben più pesanti ma invisibili per "punire" l'Ucraina. Decine di reti informatiche sono state attaccate da un nuovo virus particolarmente aggressivo, in grado di sabotare tutti i filtri, superare ogni difesa e assicurare agli hacker che lo manovrano "pieno accesso remoto al sistema compromesso" come ha riferito una relazione di Bae Systems, colosso britannico della difesa che ha una divisione specializzata nella guerra elettronica e cyber warfare. Il

software nocivo è stato chiamato Snake (serpente) o anche Ouroboros, termine ellenistico che indica il serpente che si morde la coda fino a formare un cerchio perfetto, emblema dell'eterno ritorno.

Il virus sarebbe in grado di rimanere inerte e nascosto per parecchi giorni ed è ritenuto difficilissimo da scoprire. Appare molto simile allo Stuxnet, il virus con cui nel 2010 Stati Uniti e Israele riuscirono a sabotare i computer iraniani che gestivano le installazioni nucleari e in particolare l'arricchimento dell'uranio ritardando di alcuni anni il programma atomico di Teheran. Le origini dello Snake non sono ancora state accertate ma secondo i tecnici britannici i suoi creatori sembrerebbero operare nell'area compresa all'interno del fuso orario di Mosca, e nel codice-base del virus i tecnici britannici avrebbero individuato elementi di testo in lingua russa. Dati comunque insufficienti ad accusare direttamente il governo di Mosca come ben sanno anche gli Stati Uniti che in passato hanno registrato attacchi cyber la cui origine è stata localizzata in Cina ma senza per questo poter provare la connivenza del regime di Pechino. Secondo Nigel Inkster esperto di Bae Systems, dietro i cyber-attacchi contro le reti informatiche delle istituzioni ucraine ci sarebbe la Russia.

«In termini probabilistici, la lista dei sospetti si riduce a un unico soggetto» ha dichiarato al quotidiano The Financial Times lo stesso Inkster, che fino al 2006 si occupava di cyber war per l'Mi6, i servizi di spionaggio di Sua Maestà. «Ancora poco tempo fa i russi mantenevano un basso profilo, ma non ho dubbi sul fatto che siano in grado di compiere l'intera gamma di attacchi informatici, dal semplice blocco di una rete fino ad azioni molto più sofisticate». Lo Snake esiste dal 2010 ma dall'inizio del 2014 ha intensificato la propria attività e l'Ucraina si configura come il suo bersaglio principale: su 56 attacchi del "serpente" registrati negli ultimi quattro anni a livello mondiale ben 32 sono stati diretti contro Kiev. Nel 2013 l'Ucraina è stata nel mirino degli hacker che gestiscono questo virus otto volte ma dall'inizio di quest'anno i cyber attacks sono già saliti a quattordici. Mosca del resto avrebbe "firmato" negli anni scorsi importanti azioni di questo tipo paralizzando le reti informatiche di banche ed enti statali dell'Estonia nel 2007.

Ovviamente non ci sono mai state prove definitive circa il ruolo russo in un attacco che per tre settimane paralizzò i siti internet del governo, del parlamento, di banche, giornali ed emittenti. Quello estone è stato il primo episodio di un attacco coordinato contro un Paese in un contesto non di guerra aperta, ma altri episodi simili attribuiti a Mosca si verificarono in Lettonia due anni più tardi. Nell'agosto 2008 l'intervento militare russo contro i georgiani in appoggio ai secessionisti di Abkhazia e Ossezia del Sud fu

accompagnato da un cyber attacco contro le reti televisive e i canali di comunicazioni della Georgia che paralizzò non solo le comunicazioni militari ma anche la possibilità del governo di Tblisi di rivolgersi alla popolazione.

Oggi la cyber war è considerata una minaccia prioritaria perché è in grado di colpire pesantemente le infrastrutture strategiche di un Paese o di un'alleanza senza provocare un solo morto, senza esplodere un solo colpo di canone e soprattutto senza mostrare palesemente l'identità del nemico. Cina, Russia, Stati Uniti, Israele e Gran Bretagna sembrano essere i Pesi che hanno sviluppato maggiori capacità offensive e difensive in questo settore che vede anche l'Europa e la Nato attrezzarsi in modo sempre più coordinato. Per questa ragione il primo supporto che l'Alleanza Atlantica potrebbe essere chiamata a fornire all'Ucraina in base all'impegno di rafforzare la cooperazione annunciato nei giorni scorsi dal segretario generale Anders Fogh Rasmussen potrebbe riguardare proprio la difesa delle reti informatiche sensibili ucraine dagli attacchi degli hacker di Mosca.