Cassandra Crossing/ Backdoor: un gioco in cui tutti perdono

(365)—Una backdoor è una backdoor per i buoni e per i cattivi. Imporre alle aziende di lasciare aperto uno spiraglio nel proprio codice…

Cassandra Crossing/ Backdoor: un gioco in cui tutti perdono

(365)—Una backdoor è una backdoor per i buoni e per i cattivi. Imporre alle aziende di lasciare aperto uno spiraglio nel proprio codice potrebbe spalancare le porte ad un olocausto informatico

15 gennaio 2016—"*Strano gioco. L'unico modo di vincere è non giocare*": ci era arrivato persino Joshua, il W.O.P.R. di Wargames, un computer nato per la guerra, a capire che ci sono guerre nelle quali non vince nessuno. I 24 indulgenti lettori perdoneranno certo a Cassandra questa ennesima e datata citazione cinematografica, che è frequentemente un biglietto da pagare volendo leggere le sue pagine. E' interessante tirare le somme di due notizie che si sono succedute nelle ultime settimane.

La prima: partendo da una apparentemente nuova posizione della Cina sul tecnocontrollo si è cominciato a discutere su come le multinazionali americane dovrebbero comportarsi se il governo cinese chiedesse l'inserimento di backdoor o la possibilità di decriptare i device venduti da Apple o da qualunque altra multinazionale dell'IT e dell'elettronica di consumo. Non si tratta di richieste peculiari di una nazione non democratica, visto che sia gli Stati Uniti che diversi paesi europei attuano regolarmente (o vorrebbero attuare) identiche iniziative. E per una volta la cronaca rende evidente che non siamo nell'ambito della paranoia ma della "geopolitica informatica" di una lotta combattuta nel cyberspazio.

La seconda: le backdoor scovate nel sistema operativo di Juniper, un grande produttore di device per il networking e la (ahem…) sicurezza informatica, indipendentemente da chi ce le abbia messe ed eventualmente su richiesta di chi, sono come la punta di un iceberg, rivelano la sicura presenza di una grosso problema invisibile perché sotto il pelo dell'acqua. Se dubbi ancora ci fossero sul fatto che l'"affaire" Juniper possa essere un episodio isolato, anche dopo l'emergere di un problema apparentemente simile anche per Fortinet, consiglio la lettura di questo post di un ricercatore che avrebbe individuato una ulteriore e più insidiosa falla costituita, in buona sostanza, dalla mancata inizializzazione del "seme" di una algoritmo di crittografia basato su equazioni ellittiche. Forse una backdoor nella backdoor? Anche se una successiva analisi ha messo in dubbio la reale sfruttabilità di questo errore, si tratta comunque di un esempio da manuale di quanto sia facile scrivere, per errore o volontariamente, un software apparentemente a posto ma in realtà fallato o "backdoorato".

In un ormai vetusto articolo del lontano 2005, Cassandra citava lo storico tenta-

tivo di backdooring del kernel Linux 2.6, scoperto solo per caso, che consisteva nell'aggiunta di un singolo carattere ad una singola riga di codice. Per la precisione, di un "=".Il problema di fondo è che i complessi rapporti tra multinazionali e superpotenze economiche rendono la creazione di "backdoor di stato" un problema insolubile, un pessimo affare per tutti. Il software fallato è già un grave problema connaturato alla produzione di software, senza bisogno di aggiungervi volontariamente ulteriori "bachi".La complessità del mondo globalizzato, rende impossibile ad un "buono" inserire una backdoor che riesca a colpire solo i "cattivi" desiderati. Altri "cattivi" ed altri "buoni" sfrutteranno senz'altro la stessa backdoor per scopi diversi e magari opposti, e tutti ci rimetteranno. Lo dicono da anni tutti gli esperti di sicurezza informatica e di crittografia.

E' un gioco a somma negativa, dove anche chi vince perde, simile ad un altro "gioco" il, M.A.D., la Mutua Distruzione Assicurata, che è stato giocato per 30 anni durante la guerra fredda, e che ha portato almeno un paio di volte il mondo sull'orlo di un olocausto nucleare.

Concludendo, visto che qualunque persona che abbia lavorato nella sicurezza informatica può garantire che produrre od utilizzare software di cattiva qualità o con backdoor (anche se garantite da uno Stato "buono") introdotte per lottare contro canaglie, terroristi e pedoterrosatanisti, inevitabilmente si ritorcerà contro chi l'ha voluto, perché non imparare dalla storia e smetterla subito?Oltretutto superpotenze e multinazionali hanno avuto, hanno e sempre avranno poteri maggiori degli individui in tanti campi: non serve che li tengano tutti in ostaggio con l'introduzione delle backdoor di stato.Perciò, in un mondo dove gli interessi sono contrapposti e la lotta arriva regolarmente fino alla guerra ed alla strage di civili, bandire un'arma di distruzione di massa (le backdoor sono un'arma senza usi pacifici, come il gas nervino o le bombe H) che fa "perdere" tutti sarebbe una ottima idea.

Un dibattito internazionale ed iniziative come il trattato START potrebbero essere una risposta efficace alle backdoor di stato, e certo contribuirebbero a far prendere più sul serio alla gente quello che succede nelle loro tasche e negli altri oggetti informatici di loro proprietà.

ONU? Parlamento Europeo? Non è che per caso c'è qualcuno all'ascolto di una umile profetessa?Senza una robusta iniezione di ragionevolezza, gli incroci di interessi tra stati politicamente contrapposti e multinazionali commercialmente in concorrenza, tutti quanti legati tra loro da lacci e lacciuoli politici, legislativi e commerciali, creeranno un casino galattico che interesserà contemporaneamente il mondo materiale ed il cyberspazio.Vogliamo davvero un olocausto informatico?

Originally published at punto-informatico.it.

By Marco A. L. Calamari on April 15, 2021.

Canonical link