PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4624 di Mercoledì 29 gennaio 2020

Attacchi GPS: prima lo jamming, ora lo spoofing

Negli ultimi tempi gli attacchi informatici che coinvolgono la costellazione GPS sono diventati assai più incisivi, portando non solo al disturbo del segnale, ma addirittura alla creazione di posizioni non corrette.

I mezzi tecnici di informazione hanno dato recentemente ampio risalto a una situazione che si è verificata nel porto di Shanghai, vicino alla foce del fiume Huangpu. Si tratta di un tratto marittimo ad altissimo traffico e l'utilizzo di sistemi automatici di identificazione di una imbarcazione e della sua posizione rappresenta una autentica necessità.

Ricordo ai lettori che, per legge internazionale, tutte le navi commerciali devono installare dei trasponder della rete AIDS *automatic identification system*. Ogni pochi secondi, questi dispositivi trasmettono l'identità della imbarcazione, la posizione, la rotta, e la velocità. Inoltre il dispositivo permette di visualizzare i dati AIS che sono trasmessi da altre imbarcazioni nelle vicinanze, in modo che il capitano abbia una chiara visione del traffico e possa crescere in misura significativa il livello di sicurezza nell'attraversamento di acque molto frequentate.

Secondo quanto segnalato dai tecnici, una nave ha visualizzato sul proprio schermo AIS un'altra imbarcazione, che stava imboccando lo stesso canale marittimo ad una velocità di circa sette nodi. Improvvisamente questa nave è scomparsa dal display. Alcuni minuti dopo, il display ha visualizzato la stessa nave come ancorata al molo. Questo fenomeno si è ripetuto due o tre volte, fino al punto in cui il capitano ha preso il binocolo e ha osservato il molo, rilevando che questa imbarcazione era stata ormeggiata al molo per tutta la durata di questa situazione anomala.

Ecco il motivo per cui il capitano ritenne opportuno segnalare questo evento alle appropriate autorità, che avviarono delle indagini e scoprirono che dozzine di altre imbarcazioni a Shanghai, nell'ultimo anno, erano rimaste vittime di una nuova tipologia di attacco al sistema GPS, che non consiste solo nel disturbo del segnale, il cosiddetto fenomeno di jamming, ma anche di creazione di una falsa posizione di una imbarcazione, fenomeno chiamato spoofing.

Prima di fare la segnalazione, il capitano si è accertato che tutti gli apparati di bordo fossero correttamente funzionanti, i connettori ben fissati e gli apparati pienamente operativi.

La segnalazione è stata inoltrata al Cento navigazione della guardia costiera degli Stati Uniti, che fa da punto di raccolta di tutte le anomalie afferenti a GPS, in tutto il mondo. Il problema legato a questa tipologia di attacco è che quando un comandante perde il segnale GPS, ad esempio per un attacco per jamming, può utilizzare i mezzi tradizionali di supporto alla navigazione, come le carte, il radar e la navigazione a vista. Ma se il segnale viene invece alterato, l'imbarcazione sembra trovarsi in una posizione completamente diversa e questa notizia, trasmessa alle imbarcazioni nelle vicinanze, può portare a incidenti marittimi.

Questa situazione è stata approfondita da ricerche specifiche, che hanno permesso di accertare che il problema non riguardava solo le imbarcazioni, ma anche altri utenti GPS. In particolare, gli investigatori hanno accertato che anche i ciclisti, che usavano navigatori GPS, ricevevano informazioni alterate circa la loro posizione.

Ricordo ai lettori che le forze aeree degli Stati Uniti mantengono una costellazione di almeno 24 satelliti GPS, che orbitano attorno alla terra. Vi è una certa ridondanza, ad oggi 31 satelliti, in modo che eventuali avarie siano messe sotto controllo.

Ogni satellite trasmette dei codici generati sulla base della posizione del satellite e dell'ora effettiva, misurata con un orologio atomico ad altissima precisione. Ogni orologio è sincronizzato con quello degli altri satelliti.

Un ricevitore GPS che riceve i segnali da un solo satellite può determinare la sua posizione in modo abbastanza approssimato, migliorandola ulteriormente se riceve un segnale da un secondo satellite e da un terzo satellite. In questo caso la posizione è determinata con elevata accuratezza; se poi viene ricevuto il segnale di un quarto satellite si può anche rilevare la quota alla quale si trova il ricevitore.

Che fosse possibile attaccare con sistemi di jamming il segnale ricevuto da un ricevitore GPS è fatto ben noto, ma la creazione di false posizioni rappresenta un salto di qualità, che richiede competenze informatiche e tecnologiche assai più evolute; le conseguenze di questa situazione possono essere assai più gravi, rispetto alla pura e semplice compromissione della ricezione del segnale GPS.

A questo punto, ci si potrebbe chiedere come mai questo fenomeno si verifichi con estrema frequenza proprio nel tratto di mare sopra indicato.

Le indagini delle forze dell'ordine hanno messo in evidenza che il fenomeno potrebbe essere ricondotto all'attività di imbarcazioni, che effettuano estrazione abusiva di sabbia dal fondo del canale, svolgendo un'attività che è stata da tempo proibita, per i rischi che presenta sulla solidità delle vie periferiche e delle banchine.

Il lettore potrebbe essere stupito da questa situazione, perché tende a dare un basso valore alla sabbia; in realtà una imbarcazione con una stiva piena di sabbia può valere fino a 85.000 $, sul

mercato delle costruzioni cinesi, perennemente affamato di questo prodotto.

È evidente che i malviventi, che possono effettuare un'operazione di spoofing, possono muovere le navi cariche di sabbia attraverso questo braccio marittimo, senza permetterne la loro accurata identificazione da parte delle forze dell'ordine.

Sulla base di questo scenario, invito i lettori a meditare su quali potrebbero essere i possibili utilizzi futuri di questa tecnologia criminosa, che rappresenta un autentico salto di qualità, rispetto a tecnologie precedentemente purtroppo già in uso.

Adalberto Biasiotti