PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5251 di Venerdì 07 ottobre 2022

Attacco informatico: smishing, spoofing, spam call e spam text

Gli attaccanti informatici, come è del tutto naturale, diventano sempre più evoluti e cercano di superare i blocchi, che i soggetti attaccati gradualmente attivano. Facciamo insieme una breve panoramica delle tecnologie di attacco e difesa.

Negli ultimi tempi sono cresciuti in maniera significativa gli attacchi con spam text. In particolare, questi messaggi fanno riferimento a temi legati alla COVID 19, ad esempio presentando connessioni a siti Web, sui quali è possibile acquistare prodotti farmaceutici e dispositivi di protezione individuale, inserendo i dati della carta di credito. Con la graduale diminuzione della attenzione al problema della COVID 19, questi messaggi si sono diradati.

Un'altra famiglia di questi attacchi con spam text fa riferimento all'invio di un testo, che si suppone provenga dalla vostra banca, oppure, ad esempio, da Amazon, nel quale vi si chiede di verificare un vostro acquisto. Per poter accedere al sito e vedere di quale acquisto si tratta, occorre inserire i dati bancari o della carta di credito.

Chi scrive ha ricevuto spam text, apparentemente provenienti dall'ufficio di polizia giudiziaria (non si sa bene di quali paesi), che comunicavano gli estremi di una condanna penale, che poteva essere riscattata con un pagamento con carta di credito.

Gli attacchi precedenti agli spam text sono gli spam calls. Quando la tecnologia telefonica si è spostata dalle linee fisse ai telefoni cellulari ed all'invio di messaggi di testo, come SMS, gli attaccanti hanno utilizzato tecniche di attacco, nelle quali veniva alterato il numero da cui proveniva la chiamata. Con questo sistema, anche il blocco della chiamata a poco serviva, perché in pratica ogni 100- 200 chiamate l'attaccante modificava il numero, dal quale sembrava giungere la chiamata.

Con questo tipo di attacco era inoltre estremamente difficile rintracciare il numero del chiamante ed attivare eventuali indagini da parte della polizia postale o dall'autorità garante per la protezione dei dati personali.

Questa alterazione del numero del chiamante è diventata ancora più raffinata, quando l'attaccante ha potuto modificare alcuni numeri telefonici, facendo in modo che 5 o 6 cifre fossero simili a quelle di un soggetto noto al chiamante, come ad esempio il proprio medico di famiglia, la banca o simili.

Si chiama invece smishing (acronimo di SMS phishing) una nuova forma di attacco phising, che utilizza i messaggi SMS per catturare l'attenzione del chiamante. Il messaggio è configurato in modo tale da richiedere al chiamato di cliccare su un link con tutte le conseguenze che il lettore può facilmente immaginare.

Come difendersi?

Il più semplice sistema di difesa, a parte la installazione di applicativi ormai già disponibili sul mercato ed in grado di mettere in guardia il chiamato, è quello di ignorare queste chiamate. È anche possibile bloccare il numero da cui le chiamate provengono ma, come accennato in precedenza, l'attaccante può modificare con estrema facilità il numero chiamante, rendendo assai difficile anche il rintraccio del malvivente.

Ad oggi, sembra che nella corsa tra guardie e ladri, i ladri siano un pochettino più avanti!

Adalberto Biasiotti

---

www.puntosicuro.it