PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5669 di Mercoledì 24 luglio 2024

Una pericolosa conseguenza dello sciagurato aggiornamento di CrowdStrike

Anche troppi articoli sono stati dedicati a questo sciagurato aggiornamento, ma vi sono delle conseguenze potenzialmente assai pericolose, che sono state messi in evidenza dal Centro nazionale per la sicurezza informatica del Regno Unito.

Nel Regno Unito, il centro nazionale per la sicurezza informatica ha messo in evidenza alcune potenziali conseguenze, che nascono dalla drammatica situazione che ha colpito, il 19 luglio 2024, i sistemi Microsoft. Milioni di apparati, nel mondo intero, sono rimasti bloccati, come conseguenza di un errore, fatto da un'azienda di sicurezza informatica, e presente in un applicativo di aggiornamento lanciato dall'azienda stessa.

Come purtroppo è già successo più volte negli anni, dei malintenzionati sono stati assai rapidi nel trarre un vantaggio da questo evento, che non è stato causato da un incidente afferente alla sicurezza o ad un attacco informatico.

Il centro nazionale per la sicurezza informatica ha già registrato un aumento notevole di messaggi phishing, lanciati da criminali informatici, che hanno pensato bene di approfittare di questa situazione. In particolare, nei messaggi phising si annuncia la disponibilità di software aggiornati, che permettono di mettere sotto controllo l'evento dannoso. In realtà, questi software aggiornati non rappresentano altro che applicativi, che si introducono nel sistema informatico del cliente e ne catturano i dati. Nell'analisi condotta dal centro nazionale del Regno Unito, questi messaggi sono stati inviati sia a soggetti privati, sia ad aziende.

Questo messaggio di allarme è stato condiviso anche dalla United States Cybersecurity and Infrastructure Security Agency (CISA), che ha affermato che negli Stati Uniti la situazione è altrettanto grave.

Ecco il motivo per cui entrambi questi prestigiosi enti di sicurezza informatica hanno raccomandato a tutti i responsabili di sistemi informativi di essere certi che siano in funzione dei sistemi di controllo del phishing a due livelli.

Anche lo Australian Cyber Security Centre (ACSC) ha segnalato incremento un incremento significativo di attività criminose.

Ecco il motivo per cui i responsabili dei sistemi informativi devono prestare la massima attenzione a questi tipi di attacco, che sfruttano il momento di panico, che indubbiamente si è diffuso in molte strutture informatiche, inducendo i responsabili della sicurezza informatica ad attivare qualsiasi sistema disponibile per mettere sotto controllo la situazione e riprendere la normale funzionalità.

La stessa azienda, che ha causato l'anomalia, CrowdStrike, ha confermato questa situazione, indicando in particolare un file ZIP, dal nome crowdstrike-hotfix.zip.

Secondo gli esperti di questa azienda, questo file è accompagnato da istruzioni in lingua spagnola, che cercano di indurre il destinatario a caricare l'applicativo per recuperare la piena funzionalità del suo sistema informativo.

Adalberto Biasiotti

---

www.puntosicuro.it