# Lockbit 3.0: Il Gruppo Russo dietro l'attacco hacker alla Pubblica Amministrazione Italiana. Tutti i dettagli

Data: Invalid Date | Autore: Redazione

Un'Analisi dettagliata dell'attacco ransomware e delle implicazioni per la sicurezza informatica"

Un nuovo attacco informatico sta mettendo in ginocchio la pubblica amministrazione italiana. L'azione, che è in corso da diversi giorni, è stata scoperta l'8 dicembre ma solo recentemente ne sono emersi i dettagli. Fonti attendibili confermano che il colpevole è un noto gruppo russofono chiamato Lockbit, già responsabile di attacchi simili alla Regione Lazio nel 2021 e all'Agenzia delle Entrate nel 2022. Lockbit è una banda di criminali informatici che ha sviluppato diverse versioni del ransomware che porta il loro nome.

L'obiettivo più recente dell'attacco è stata Westpole, un'azienda che fornisce servizi cloud alla pubblica amministrazione. Secondo le fonti, il ransomware utilizzato è la terza versione denominata Lockbit 3.0. Questo tipo di attacco prevede il pagamento di un riscatto in criptovalute. Al momento, l'attacco sembra estendersi ampiamente, e l'Agenzia per la cybersicurezza nazionale (ACN) è al lavoro per cercare di arginarne gli effetti.

Le indagini sono ancora in corso, e al momento non è possibile quantificare completamente i danni causati dal virus. Westpole ha annunciato di essere riuscita a ripristinare il 50% dei propri sistemi, ma il restante 50% presenta ancora problemi. L'ACN ha dichiarato che il processo di ripristino è lento

e complesso, e non è chiaro quando potrà essere completato. C'è anche il rischio che le pubbliche amministrazioni coinvolte possano essere incapaci di erogare alcuni servizi e obblighi verso i propri dipendenti, incluso il pagamento degli stipendi di dicembre, che potrebbe subire ritardi.

Lockbit non è nuovo a questo tipo di attacchi ed è uno dei gruppi di criminali informatici più attivi nel campo della cibersicurezza. Attivo dal 2019, il suo nome è ormai ben noto in Italia, soprattutto a causa delle azioni che ha compiuto. Tra gli attacchi più noti, ricordiamo quelli alla Regione Lazio lo scorso agosto, oltre a quelli contro Thalesgroup e Accenture.

Il gruppo Lockbit opera principalmente come un ransomware as a service (RaaS), il che significa che sviluppa il software malevolo e lo affitta ad altri criminali informatici che eseguono l'attacco effettivo. Questo modello di business consente loro di guadagnare una percentuale dei profitti ottenuti dal riscatto.

La nuova versione di Lockbit sembra richiedere il pagamento del riscatto in criptovalute, in particolare Zcash, una scelta che sta attirando l'attenzione degli esperti.

Spero che queste informazioni siano di tuo interesse! Se hai altre domande o hai bisogno di ulteriori dettagli, sarò felice di aiutarti.

In aggiornamento

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/lockbit-30-il-gruppo-russo-dietro-lattacco-hacker-alla-pubblica-amministrazione-italiana-tutti-i-dettagli/137515