Sarbloh, il ransomware che vendica i contadini

- Arturo Di Corinto, 18.03.2021

Hacker's Dictionary . Anche i ransomware possono avere scopi politici, ma restano una piaga economica per i settori manifatturiero, assicurativo e farmaceutico. Secondo IBM il ransomware Sodinokibi coi suoi ricatti ha portato in tasca ai cybercriminali oltre 123 milioni di dollari solo nell'ultimo anno

Un “malware” è qualsiasi programma informatico usato per disturbare le operazioni svolte dall’utente di un computer. Prima che il termine fosse coniato nel 1990 da Yisrael Radai, ogni software malevolo prendeva il nome di virus. Anche i ransomware sono particolari categorie di malware, e hanno la finalità di limitare l’accesso a un dispositivo o di impedire l’uso di specifici file se l’utente infettato non paga un riscatto (ransom). Ma come negli anni ‘90 i virus non avevano sempre uno scopo distruttivo, oggi ci sono dei ransomware che hanno scopi dimostrativi e di carattere politico.

Se ne sono accorti gli esperti di sicurezza venuti in contatto col ransomware *Sarbloh*, che blocca i sistemi infetti e invia messaggi a sostegno delle proteste di migliaia di agricoltori in India in rivolta contro le nuove leggi sull’agricoltura che mettono a rischio la loro sopravvivenza.

Questo malware, distribuito tramite documenti Microsoft Office dannosi include infatti una dichiarazione di supporto verso i contadini che protestano da novembre. Attivati in seguito a una campagna di e-mail di phishing o scaricabili da siti Web compromessi, quando gli utenti abilitano il contenuto di tali documenti il ransomware cifra il sistema ospite. A quel punto compare un documento di testo in cui è presente sia una richiesta di riscatto che il messaggio di supporto agli agricoltori: “Il popolo indiano è stato a lungo il volto delloppressione. Oggi i potenti prendono alla gola contadini indù, sikh e musulmani e cercano di portargli via i mezzi di sussistenza. Non riusciranno nei loro sinistri progetti”.

Michael Gillespie, specialista di ransomware e creatore della piattaforma specializzata No More Ransom, ritiene che Sarbloh si basi su un ransomware open source noto come KhalsaCrypt per il quale al momento non ci sono strumenti di decrittazione, quindi le vittime di questa infezione dovranno ricorrere al backup dei loro sistemi o pagare il riscatto.

Secondo l’ultimo rapporto di IBM X-Force, nel 2020 il numero di attacchi ransomware è cresciuto rispetto al 2019: quasi il 60% di quelli analizzati è caratterizzato da una strategia di doppia estorsione in base alla quale i dati sono crittografati e rubati e le vittime minacciate della loro diffusione qualora non avvenga il pagamento. Il 36% dei data breach tracciati nel 2020 è stato originato da attacchi ransomware, suggerendo che data breach e attacchi ransomware comincino a coincidere.

Il ransomware Sodinokibi (REvil), rappresenta il 22% di tutti i ransomware osservati da X-Force. IBM stima che Sodinokibi abbia esfiltrato circa 21,6 terabyte di dati, che quasi due terzi delle vittime abbiano pagato il riscatto richiesto e il 43% perso i propri dati. Il risultato è che i responsabili di Sodinokibi hanno guadagnato oltre 123 milioni di dollari nellultimo anno.

Uno dei “gestori” di quest’ultimo tipo di ransomware ha accettato l’intervista di un ricercatore di Recorded Future, Dmitry Smilyanets, in cui sostiene che il ransomware sia unarma perfetta per la

guerra informatica: “Diversi affiliati hanno accesso a un sistema di lancio di missili balistici, uno a un incrociatore della Marina degli Stati Uniti, un terzo a una centrale nucleare e un quarto a una fabbrica di armi. Ci si può iniziare una guerra”. Ma poi dice: “non ne vale la pena. le conseguenze non sono redditizie”. Nel farlo cita le nazioni povere che “non possono pagare i riscatti” e le attività del settore manifatturiero, assicurativo e farmaceutico che invece possono farlo e che per questo sono diventate un loro target privilegiato.

© 2021 IL NUOVO MANIFESTO SOCIETÀ COOP. EDITRICE