PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4337 di Mercoledì 24 ottobre 2018

La vera storia di un drammatico virus

Una azienda specializzata britannica ha studiato a fondo un virus, appartenente alla famiglia dei ransomware, chiamato SamSam. La storia di questo virus è edificante per tutti gli esperti di sicurezza informatica.

I lettori sanno bene che il ransomware è uno dei virus più pericolosi che attualmente possano attaccare un sistema informativo. Un'azienda specializzata britannica ha scoperto un gran numero di informazioni su uno specifico virus, chiamato SamSam. Questo virus ha permesso ai suoi sviluppatori di portare a casa 56 milioni di dollari in bitcoin in poco tempo.

Per solito gli applicativi ransomware vengono diffusi a centinaia di migliaia di copie, e il riscatto che viene chiesto ai gestori dei computer coinvolti è dell'ordine di un centinaio di dollari, da pagare in bitcoin.

I malviventi che utilizzano questo applicativo invece effettuano attacchi mirati, e gli utenti colpiti sono in numero inferiore, ma il riscatto che viene richiesto può superare i 50.000 $. Secondo lo studio sviluppato da questa azienda specializzata, nel solo 2018 i riscatti che hanno pagato gli utenti colpiti da questo virus superano i 300.000 $ al mese.

Il metodo di attacco ha una forte componente manuale e ciò consente all'attaccante di attuare delle contromisure, se il soggetto attaccato cerca di attivare delle misure protettive.

Ad esempio, se il processo di cifratura dei dati viene, per una ragione qualunque, interrotto, il malware si autocancella e non rimane alcuna traccia, che possa essere esaminata dagli investigatori.

Questo applicativo criptografico colpisce non solo i file di dati, ma anche programmi, come ad esempio Windows Office, in cui molti file non vengono normalmente copiati su un backup di sicurezza.

Ecco perché talvolta la disponibilità della chiave di cifratura non è sufficiente, ma occorre reinstallare molti applicativi.

Inoltre questo studio ha messo in evidenza come gli attaccanti siano decisamente evoluti e il software di attacco non sia sempre lo stesso, ma si evolva con il passare del tempo.

Questo ransomware è apparso per la prima volta nel dicembre 2015, colpendo grandi aziende, ospedali, scuole ed i sistemi informativi di amministrazioni comunali. Le notizie in merito alla sua diffusione sono state rallentate, per il fatto che gli attaccanti hanno preso molte precauzioni per nascondere il metodo di attacco e cancellare qualsiasi traccia dell'attacco, una volta ottenuto il riscatto.

Le cifre che abbiamo sopra riportato, in termini di riscatti pagati, sono state calcolate analizzando gli indirizzi cui sono stati inviati i riscatti in bitcoin. I malviventi sono stati anche abbastanza attenti a spostare immediatamente le somme ricevute in un sito nel dark Web, che ha un indirizzo unico per ogni sistema informativo attaccato. Dopo che il pagamento è stato ricevuto, gli attaccanti spostano la criptovaluta in un sistema complicato di conti incrociati, che permette di disperdere il pagamento in numerose piccole transazioni.

Al termine di questa indagine, l'azienda specializzata ha offerto tutt'una serie di indicazioni alle aziende che potrebbero essere colpite da questo virus, facendo comunque presente che non esistono soluzioni perfette. Un sistema attivo e stratificato di protezioni di sicurezza rappresenta indubbiamente la risposta migliore.

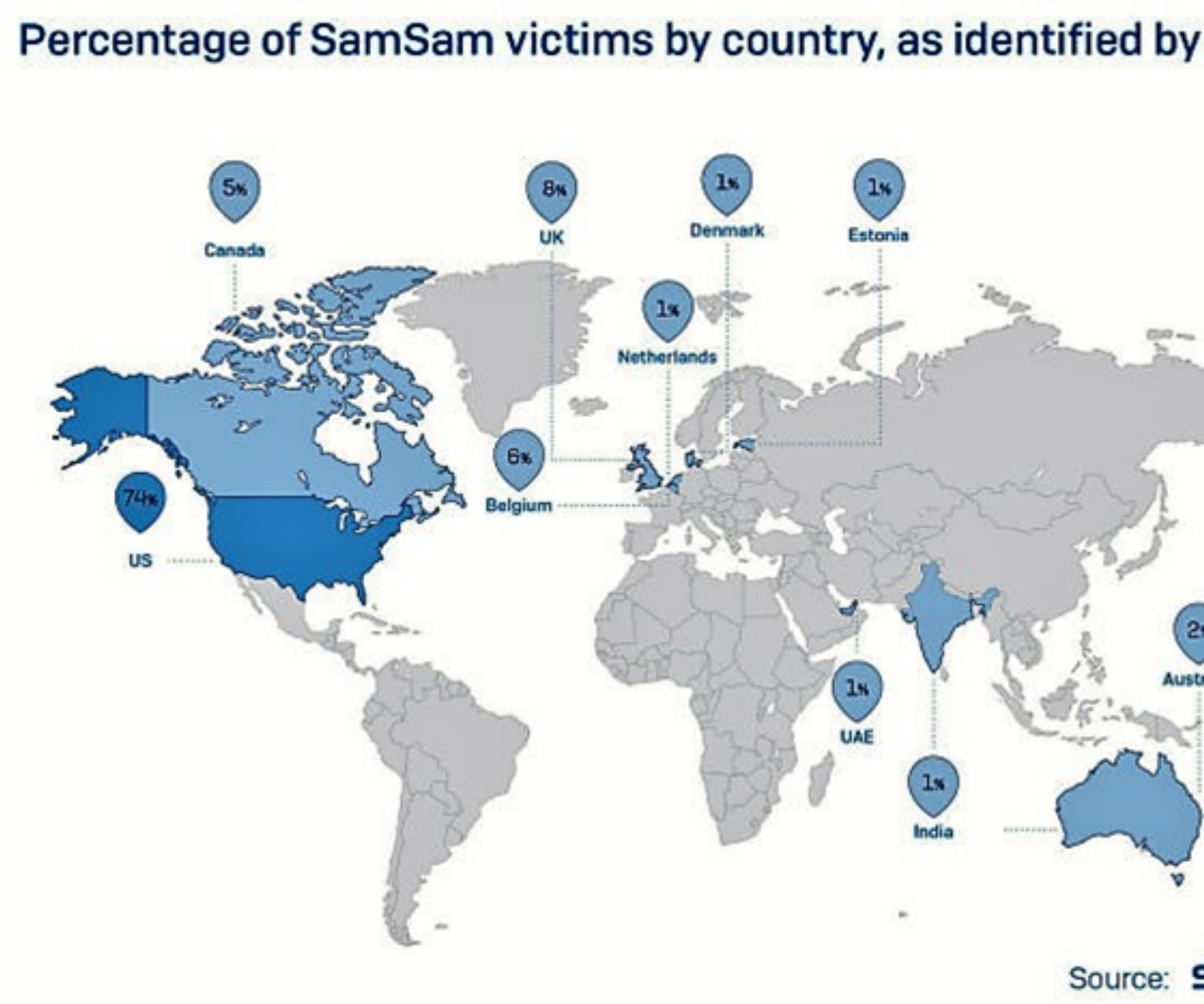
Tanto per cominciare, si raccomanda di utilizzare sempre un'autentica a più fattori, per rendere più difficile l'attacco proveniente da postazioni esterne, che si collegano sulla rete privata virtuale.

Anche l'adozione di procedure di valutazione di vulnerabilità e test di penetrazione possono dare utili indicazioni sul livello di sicurezza dell'azienda in causa.

Si raccomanda che i backup non solo siano off line ma anche off site, in modo da rendere molto difficile la compromissione contemporanea dei dati in linea e dei dati in backup.

Infine, la messa disponibilità e la verifica periodica dell'efficienza ed efficacia di un sistema di disaster recovery rappresenta un prezioso strumento di ripristino dell'attività, ove il sistema informativo sia stato colpito.

La mappa allegata a questo articolo da un'idea della distribuzione percentuale, del mondo, delle aziende colpite.



Adalberto Biasiotti

www.puntosicuro.it