PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4012 di giovedì 18 maggio 2017

Un appunto sui recenti attacchi cibernetici

I mezzi di informazione di massa hanno dato ampio risalto agli attacchi cibernetici, che hanno colpito numerosi paesi del mondo. Vediamo quale tipologia di attacco è stata utilizzata da hacker ancora non individuati. Di Adalberto Biasiotti.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

E' probabile che molti dei nostri lettori non abbiano una specifica competenza nel settore della sicurezza informatica ed ecco la ragione per la quale ritengo opportuno illustrare brevemente non solo gli strumenti utilizzati, ma anche le modalità di attacco e soprattutto le modalità di richiesta di riscatto e di prevenzione dell'attacco stesso.

L'applicativo in questione sembra sia stato sviluppato inizialmente dalla NSA national security agency e sia stato poi sottratto da hackers, ancora non individuati. I sospetti si sono inizialmente concentrati su un lavoratore a contratto della NASA, Hal Martin, che però era stato già messo in prigione qualche tempo fa. Naturalmente questo non significa che egli non abbia reso disponibili queste informazioni a soggetti, ancora in libertà.

Che poi queste informazioni siano state utilizzate per lanciare l'attacco da un qualunque paese del mondo, come ad esempio la Cina o la Corea del Nord, sui quali paesi si è inizialmente concentrata l'attenzione mondiale, è fatto secondario.

Cominciamo ad esaminare l'applicativo che è stato messo a punto.

L'applicativo in questione, che nella versione elaborata dalla national security agency si chiama WannaCry, vale a dire "mi viene da piangere", una volta inserito in un sistema informativo provvede alla cifratura dei dati presenti nel sistema, utilizzando un algoritmo criptografico di buon livello. Per poter accedere nuovamente ai dati è indispensabile venire a conoscenza della parola chiave, utilizzata in fase di cifratura.

È bene sottolineare che questo applicativo fraudolento è in grado di cifrare, e quindi rendere inaccessibili, solo i dati che si trovano nel sistema principale. Se i dati vengono regolarmente copiati su un supporto di backup, conservato all'esterno del sistema informativo, questi ultimi dati evidentemente non vengono compromessi.

Occorre quindi sottolineare sin da adesso il fatto che l'attacco ha coinvolto i dati custoditi in sistemi informativi, e non i dati custoditi su supporti di backup separati. Il fatto che in alcuni casi i gestori di sistemi informativi siano stati impossibilitati a rendere il servizio previsto alla popolazione, come è successo nel caso degli ospedali britannici, fa riferimento al fatto che non si

era ancora provveduto a sostituire i dati cifrati con i dati di backup, oppure, caso ben più preoccupante, i dati di backup non erano stati aggiornati con la appropriata diligenza o, caso estremo al quale preferiscono pensare, non era stata avviata e gestita regolarmente una procedura per il backup di dati, custoditi nel sistema informativo.

Chi scrive ha avuto esperienza diretta, tramite un paio di conoscenti, di attacchi che sono andati a buon fine, per il semplice fatto che i conoscenti non avevano predisposto appropriate ed accurate procedure di backup di dati, presenti nel sistema informativo.

Quando l'applicativo fraudolento riesce quindi a cifrare i dati, sul monitor dell'operatore appare una schermata, che lo informa del fatto che il suo sistema è stato attaccato ed egli può accedere nuovamente ai dati protetti, solamente se si utilizza una chiave criptografica, che viene fornita a pagamento del riscatto.

Ricordo al proposito che il nome attribuito a questo applicativo è proprio applicativo di riscatto. Nell'esperienza, purtroppo già maturata da chi scrive, in relazione ai conoscenti vari, il comportamento degli hackers è tutto sommato "corretto", nel senso che, una volta pagato il riscatto, l'hacker ha sempre fornito la corretta parola chiave e il recupero dei dati è avvenuto integralmente.

Da questo punto di vista, quindi, questo attacco è stato effettuato con modalità già ben note e pubblicizzate da tempo in tutti i siti, che si occupano di sicurezza informatica.

Neppure innovativo è il sistema, grazie al quale il gestore del sistema attaccato può pagare il riscatto ed ottenere la parola chiave.

Il sistema utilizzato è quello di pagare in bitcoin, che è una particolare valuta, esistente solo in forma virtuale del mondo Internet, che oltretutto ha un valore dinamico estremamente variabile. Il valore di questa moneta virtuale, comparato al dollaro oppure all'euro, varia in maniera straordinaria dal giorno alla notte e quindi non si deve richiedere un pagamento in bitcoin, ma un pagamento in dollari, trasformati in bitcoins.

L'utilizzo di questa particolare moneta impedisce di rintracciare l'hacker e viene utilizzata ormai da anni per applicazioni talvolta oneste e talvolta fraudolente. Il tutto viene gestito da economici applicativi chiamati ransomware-as-a-service (RaaS).

In passato l'attività degli hacker era invece impostata in un altro modo; ad esempio, sullo schermo appariva un messaggio nel quale si informava il gestore del sistema che erano stati riscontrati degli applicativi installati in modo illegittimo e che, se voleva evitare una denuncia ai proprietari degli applicativi, avrebbe dovuto pagare una somma in bitcoin.

A questo punto ci si può domandare cosa fare per prevenire questo tipo di attacchi.

Valgono le consuete raccomandazioni di non aprire link e messaggi di posta elettronica che provengono da siti ignoti o che sono scritti in una lingua, piena di errori.

Le misure principali di protezione sono evidentemente quelle di effettuare regolarmente il backup dei dati, introdurre rigide misure di controllo sull'accesso ai dati e mantenere aggiornato quanto più possibile l'applicativo antivirus, di cui tutti dovrebbero essere dotati.

Ricordo, ad esempio, che subito dopo questo attacco uno dei maggiori fornitori di sistemi antivirus ha diffuso un aggiornamento massiccio, proprio per aggiornare le difese esistenti, secondo le ultime notizie diffuse fra i tecnici informatici.

Ad esempio, è bene adottare una politica sistematica che prevede che, prima di collegarsi al sistema di posta elettronico, l'operatore si colleghi all'aggiornamento del applicativo antivirus, in modo da essere certo che, quando si collegherà ad una area potenzialmente critica, come l'area di messaggeria elettronica, le proprie difese siano aggiornate.

Si tratta di misure che costano certamente molto meno e che sono più efficaci, rispetto al pagamento di un riscatto, anche solo di qualche centinaio di dollari!

Adalberto Biasiotti



Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it