PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4958 di Venerdì 18 giugno 2021

Siamo sicuri di conoscere a fondo gli attacchi per ransomware?

In inglese la parola ransomware significa riscatto. Si fa quindi riferimento ad applicativi che introducono delle anomalie nel sistema informativo attaccato, alle quali si può porre rimedio pagando un riscatto.

Questi attacchi sono cominciati nel 2018 e stanno acquistando un ruolo sempre più dominante sullo scenario di attacchi criminali ai sistemi informativi.

Anche se crescono le difese che i responsabili informatici hanno a disposizione, sembra che crescano assai più rapidamente le competenze degli attaccanti, che sono in grado di neutralizzare le difese attivate dai soggetti attaccati.

Oggi le vittime di questi attacchi sono costrette a fronteggiare tre diverse situazioni:

- Come posso ripristinare l'accesso ai miei dati e sistemi?
- Quali dati sono stati sottratti, mentre i malviventi avevano attaccato il mio sistema?
- Che obblighi abbiamo di riferire l'attacco alle autorità costituite?

Risparmio ai lettori l'elenco dei numerosi nomi che sono stati attribuiti ai software attaccanti, perché i nomi continua a crescere, mano a mano che si evolvono questi software attaccanti.

Tanto per cominciare, ormai si sono identificati dei gruppi criminali che hanno un *modus operandi* affatto particolare e tutto sommato facilmente riconoscibile.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Durante la fase iniziale dell'attacco, il criminale, oppure un gruppo di criminali, accede al sistema informativo attaccato e conduce un'accurata ricognizione del sistema stesso, cercando di individuare quali siano i sistemi o i dati che sembrano essere maggiormente rilevanti per la corrente funzionalità del soggetto attaccato.

Dopo aver identificato i bersagli più attraenti, il malvivente passa alla seconda fase dell'attacco, che si concentra sui sistemi e dati che sono stati individuati come di particolare interesse.

Quando questa fase è stata portata a termine, è possibile passare alla fase successiva, che prevede la sottrazione dei dati critici o la attivazione di procedure, che rendono impossibile l'accesso ai dati stessi, da parte del legittimo proprietario.

A questo punto viene lanciata la richiesta di riscatto.

La richiesta di riscatto viene spesso resa più violenta, perché i malviventi possono pubblicare una piccola parte dei dati sottratti, in modo da far perdere la faccia al sito attaccato e dimostrare come la richiesta di riscatto è fondata su valide basi.

Questa pubblicizzazione su scala ridotta dei dati viene spesso chiamata con l'espressione inglese "shaming", che vuol dire danneggiare l'immagine del sito Web del soggetto attaccato.

Se l'organizzazione vittima dell'attacco decide di pagare il riscatto, i dati vengono ripristinati nella loro integrità e quelli temporaneamente estratti per aumentare la pressione sul soggetto ricattato vengono nuovamente inseriti nel sistema attaccato.

In qualche raro caso la richiesta di riscatto viene attuata in due fasi:

- nella prima fase si chiede riscatto per recuperare l'accesso ai dati,
- nella seconda fase si chiede un riscatto per togliere i dati pubblicizzati.

Una recentissima tecnica di attacco, che purtroppo si è già manifestata, consiste nella collusione con un dipendente del soggetto attaccato, che è incaricato di inserire il software criminoso. È evidente che con questa tipologia di attacco le difese contro attacchi provenienti dall'esterno diventano assai meno efficaci e la protezione da questi attacchi diventa assai più complessa.

Quali misure di prevenzione adottare

Gli esperti suggeriscono numerose tecniche, tra le quali si pone in maggiore evidenza una tecnica di autentica a molti fattori per accesso a distanza al sistema informativo; si raccomanda inoltre di addestrare il personale, con sessioni specifiche di formazione e con test pratici per ridurre al minimo gli attacchi portati attraverso tecniche di social engineering.

Una delle tecniche più efficienti ed efficaci è indubbiamente quella di effettuare con frequenza dei backup completi di tutti i dati, accertandosi che questi backup siano custoditi in reti separate e protette, in modo che gli attaccanti non riescano a colpire contemporaneamente i dati on-line ed i dati di backup.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it