Debellato il ransomware? Non basta…

Giu 22, 2020 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

I pirati informatici, oltre al malware principale, installano invariabilmente backdoor e altri strumenti per garantirsi una presenza nella rete.

Ricorda un po' il detto riguardante il dito e la luna, ma secondo gli esperti di sicurezza i recenti attacchi portati dal gruppo **Maze** potrebbero rappresentare una scossa in grado di convincere le aziende a un approccio più "saggio" nel caso in cui si verifichino attacchi ransomware.

Il tema, come spiega **Lawrence Abrams** su **Bleeping Computer**, è quello del rischio che il malware rappresenti solo la punta dell'iceberg. In molti casi, però, le aziende che vengono colpite commettono l'errore di considerare l'incidente chiuso una volta rimosso il ransomware, senza approfondire in maniera adeguata l'incidente.

Le ultime notizie di cronaca riguardanti i pirati di **Maze** (ne abbiamo parlato in questo articolo) dimostrano però quanto sia pericoloso un atteggiamento del genere. **Il loro modus operandi, che prevede il furto di dati oltre all'installazione del ransomware, dimostra che l'estorsione legata alla codifica dei file è solo uno dei problemi**.



L’equivoco, probabilmente, è legato alla similitudine con gli attacchi ransomware che prendono di mira i privati cittadini, in cui il vettore di infezione è spesso rappresentato da un file allegato a un messaggio di posta elettronica. Insomma: qualcosa che potremmo definire come un “incidente isolato”.

I cyber criminali che colpiscono le aziende, invece, agiscono seguendo una strategia attentamente pianificata che prevede, come prima mossa, la violazione dei sistemi aziendali e un’attività di movimento laterale che gli permette di ottenere l’accesso a tutte le risorse critiche.

Nella logica di un cyber criminale, infatti, un attacco con un ransomware è lo stadio finale di un’attività che può essere stata portata avanti per giorni, settimane o addirittura mesi.

Anche una volta rimosso il ransomware e recuperati i file, il rischio che i pirati abbiano ancora accesso a singoli dispositivi o all’intera rete aziendale è quindi elevatissimo. Ciò che è necessario, quindi, è fare un controllo accurato e una sorta di operazione di “bonifica” che metta al riparo i sistemi da ulteriori attacchi.

Non solo: l’analisi dei sistemi può consentire di individuare eventuali furti di dati che erano precedentemente passati inosservati.

Condividi l’articolo

InvisiMole: ecco come agiscono i professionisti del cyber-spionaggio

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/22/debellato-il-ransomware-non-basta/?utm_source=rss&utm_medium=rss&utm_campaign=debellato-il-ransomware-non-basta