Raffica di attacchi ransomware ai NAS

Ago 01, 2019 Marco Schiaffino Attacchi, Gestione dati, In evidenza, Intrusione, Malware, News, RSS 1

I pirati stanno usando tecniche di Brute Forcing per accedere ai dispositivi. I dati al loro interno vengono crittografati e viene chiesto un riscatto in Bitcoin.

L'allarme è partito da **Sinology**, ma non lasciamoci ingannare: l'ondata di attacchi segnalata dal produttore taiwanese non interessa solo i **NAS** del produttore con sede a Taipei, ma anche prodotti di altre aziende.

Quello a cui si sta assistendo, secondo quanto racconta l'azienda, sarebbe un attacco pianificato che sfrutta botnet di dispositivi IoT per cercare di accedere ai dispositivi utilizzando password di uso comune e credenziali predefinite.

Una volta ottenuto l'accesso al NAS, i pirati informatici utilizzano un classico cripto-ransomware per codificare tutti i dati memorizzati sul dispositivo e lasciano in chiaro soltanto un file di testo nel quale viene chiesto il riscatto per ottenere la chiave che consente di recuperare i dati.

L'alert pubblicato su Internet raccomanda agli utenti di disabilitare l'account di amministrazione predefinito e modificare la password per l'accesso utilizzandone una complessa. Nel caso dei prodotti Sinology, il consiglio è anche quello di abilitare la funzione **Auto Block**.

Si tratta di uno strumento che blocca automaticamente il collegamento a un indirizzo IP quando vengono effettuati troppi tentativi di accesso.

Non è un periodo felice per i proprietari di NAS. Solo qualche giorno fa è infatti emersa una vulnerabilità dei vecchi dispositivi **Iomega** (ne abbiamo parlato in questo articolo) mentre i modelli più recenti dello storico marchio (oggi proprietà di **Lenovo**)sembrano essere stati presi di mira da un gruppo di cyber-criminali che, anche in questo caso, punta a ottenere un riscatto dalle vittime.

Il modus operandi, però, è lievemente diverso da quello riportato da Sinology. **In questo caso, infatti, i file non vengono crittografati ma semplicemente cancellati**. Al pagamento del riscatto, sostengono i pirati nel messaggio che lasciano sul disco, seguirebbe la restituzione dei file.

Come riporta Bleeping Computer, sul cui forum sono arrivate numerose segnalazioni di utenti colpiti in questo modo, i file possono però essere recuperati utilizzando un software di recovery.

Condividi l’articolo

SystemBC: il malware per nascondere il malware LibreOffice corregge una falla ma suggerisce di usare la vecchia versione

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/01/raffica-di-attacchi-ransomware-ai-nas/