Registrato un massiccio attacco ransomware tramite infezione di sistemi VMware

L'Agenzia per la cybersicurezza nazionale, ACN, invita ad aggiornare tutti i sistemi vulnerabili oggetto dell'attacco

Comunicato stampa del 5 Febbraio 2023

www.acn.gov.it

Il Computer Security Incident Response Team Italia (Csirt-IT) dell'Agenzia per la Cybersicurezza Nazionale, ACN, ha rilevato un massiccio attacco tramite un **ransomware** già in circolazione che prende di mira i **server VMware ESXi**.

La vulnerabilità sfruttata dagli attaccanti per distribuire il ransomware è già stata corretta nel passato dal produttore, ma non tutti coloro che usano i sistemi attualmente interessati l'hanno risolta.

I server presi di mira, se privi delle *patch,* cioè delle "correzioni" adeguate, possono aprire le porte agli **hacker criminali impegnati a sfruttarla in queste ore** dopo la forte crescita di attacchi registrata nel weekend.

I primi ad accorgersene sono stati i francesi, probabilmente per via dell'ampio numero di infezioni registrato sui sistemi di alcuni provider in Francia. Successivamente l'ondata di attacchi si è spostata su altri paesi tra cui l'Italia.

In questo momento sono qualche migliaio i **server compromessi in tutto il mondo**, dai paesi europei come **Francia** – paese più colpito - **Finlandia** e **Italia**, fino al Nord America, in **Canada e negli Stati Uniti.**

In Italia sono decine le realtà che hanno riscontrato l'attività malevola nei loro confronti ma secondo gli analisti sono destinate ad aumentare.

Lo sfruttamento della vulnerabilità consente in una fase successiva di portare attacchi ransomware che, come è noto, cifrano i sistemi colpiti rendendoli inutilizzabili fino al pagamento di un riscatto per avere la chiave di decifrazione.

L'autorità nazionale per la sicurezza informatica, ACN, ribadisce che è prioritario per chiunque chiudere le falle individuate e sviluppare un'**adeguata strategia di protezione.**

Per i tecnici dell'ACN, infatti, "***siamo stati in grado di censire diverse decine di sistemi nazionali verosimilmente compromessi e allertato numerosi soggetti i cui sistemi sono esposti ma non ancora compromessi. Tuttavia, rimangono ancora alcuni sistemi esposti, non compromessi, dei quali non è stato possibile risalire al soggetto proprietario. Questi sono chiamati immediatamente ad aggiornare i loro sistemi***".

La vulnerabilità individuata dalle recenti analisi come la CVE-2021–21974 (già sanata dal vendor nel febbraio 2021), riguarda i sistemi esposti su Internet che offrono servizi di virtualizzazione basati sul prodotto VMWare ESXi, e ha un impatto elevato, stimato dalla comunità tecnica come "rischio alto/arancione" **(70,25/100).**

E tuttavia non si esclude che anche altre vulnerabilità possano essere sfruttate da attori malevoli.

A questo riguardo, l'Agenzia per la Cybersicurezza Nazionale, attraverso lo CSIRT Italia, ha pubblicato nella giornata di ieri uno specifico bollettino sul portale pubblico https://csirt.gov.it, che include anche le procedure per risolvere la vulnerabilità, ai quali i responsabili tecnici dei servizi IT pubblici e privati sono invitati a fare riferimento.

----------/----------

Che cos'è un Ransomware: Un ransomware è un malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari. https://www.csirt.gov.it/glossario/23

Che cos'è l'Agenzia per la Cybersicurezza Nazionale (ACN): L'ACN è l'Autorità nazionale per la cybersicurezza istituita con il D.L. 14 giugno 2021, n. 82, a tutela degli interessi nazionali nel cyberspazio. Garantisce l'implementazione della **strategia nazionale di cybersicurezza** adottata dal Presidente del Consiglio, promuove un quadro normativo coerente nel settore, ed esercita funzioni ispettive e sanzionatorie. Sviluppa collaborazioni a livello internazionale con agenzie omologhe. Assicura il coordinamento tra i soggetti pubblici e la realizzazione di azioni pubblico-private volte a **garantire la sicurezza e la resilienza cibernetica per lo sviluppo digitale del Paese**.