PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 5071 di Venerdì 17 dicembre 2021

Il ransomware colpisce anche infrastrutture critiche

I criminali che perpetrano attacchi per ransomware non hanno riguardo alcuno per i destinatari dei loro attacchi: una serie di attacchi contro infrastrutture critiche, riferite al trattamento delle acque, che hanno colpito alcune aziende americane.

Le infrastrutture di trattamento delle acque, per depurarle prima di immetterle nei canali di scolo o per sterilizzarle al punto da poter essere utilizzate come acqua potabile, rappresentano una componente importantissima della rete delle infrastrutture critiche di una qualsiasi nazione. La indisponibilità di acqua potabile o la immissione nei canali di scolo di acqua non correttamente depurata rappresentano infatti delle situazioni di particolari criticità.

Giunge notizia del fatto che i criminali informatici hanno già perpetrato, degli Stati Uniti, degli attacchi per ransomware contro aziende di questo tipo.

Nell'agosto 2020, una variante del programma ransomware, chiamato Ghost (fantasma), è stata lanciata contro una azienda di trattamento delle acque della California. Il virus è stato scoperto dopo circa un mese dalla dall'inserimento nel sistema informativo aziendale, quando tre server di tipo SCADA (supervisory control and data acquisition) hanno visualizzato il messaggio con la richiesta di riscatto.

Nel luglio 2021, i malviventi hanno inserito un'altra variante di un applicativo ransomware nel sistema informativo di un'azienda che trattava acque reflue, sempre utilizzando, come porta d'ingresso, il computer SCADA dell'azienda. I responsabili aziendali sono stati costretti a gestire manualmente tutta l'attività di depurazione, finché non sono stati ripristinate le piene funzionalità del computer SCADA.

Nel marzo 2021, un altro attacco con una variante ransomware è stato perpetrato contro una azienda di trattamento delle acque del Nevada. Anche in questo caso, il ransomware ha coinvolto il sistema SCADA e i sistemi di backup. L'attacco, in questo caso, ha causato danni di minore gravità, perché il sistema SCADA veniva utilizzato per attività di monitoraggio e non per il pieno controllo delle attività di trattamento.

Da quanto sopra si trae la conclusione che è bene che tutte le aziende italiane, che svolgono attività similari, alzino il livello di guardia e di protezione dei loro sistemi informativi, per evitare che anche malviventi italiani possano perpetrare questa tipologia di attacchi.

Adalberto Biasiotti

---

www.puntosicuro.it