

La guerra ibrida è già iniziata: cyberattacco al Brennero, cresce l’offensiva degli hacker filorussi contro l'Europa

Pubblicato il 07/11/2026

Un attacco informatico contro la società che realizza la Galleria di Base del Brennero riaccende l'allarme sulla sicurezza delle infrastrutture strategiche europee. Dietro l'intrusione potrebbe esserci il gruppo russofono Everest. L'episodio arriva a pochi giorni dai sabotaggi informatici contro gli impianti frigoriferi dei supermercati europei, rivendicati da due collettivi filorussi. Cresce la preoccupazione per una minaccia capace di colpire trasporti, filiere alimentari e servizi essenziali.

La minaccia informatica torna a colpire il cuore delle infrastrutture strategiche europee. Questa volta l'obiettivo è la Galleria di Base del Brennero, una delle più importanti opere ferroviarie del continente, destinata a potenziare i collegamenti tra Italia e Austria lungo il corridoio europeo Scandinavo-Mediterraneo.

La società BBT SE, responsabile della realizzazione dell'opera, ha confermato di aver subito un cyberattacco mirato, avvenuto a metà ottobre e reso pubblico nelle ultime ore dalla stampa austriaca.

Secondo quanto riportato dal quotidiano Tiroler Tageszeitung e dall'emittente pubblica austriaca ORF, dietro l'operazione potrebbe esserci Everest, un'organizzazione criminale informatica russofona, specializzata nel furto di dati e nelle estorsioni digitali.

La pista russa viene dunque presa in considerazione, ma l'attribuzione non è ancora definitiva. Inoltre, l'eventuale coinvolgimento di criminali informatici russofoni non dimostrerebbe automaticamente una responsabilità del governo di Mosca.

Brennero sotto attacco: violati i sistemi informatici

Secondo le informazioni diffuse dalla società, gli aggressori sono riusciti ad accedere senza autorizzazione ad alcuni dati raggiungibili attraverso Internet.

Una volta individuata l'intrusione, BBT SE ha attivato le procedure di sicurezza, isolando immediatamente i sistemi interessati e incaricando specialisti esterni di effettuare le necessarie analisi forensi.

Le autorità competenti sono state informate e sono in corso accertamenti per stabilire l'esatta portata della violazione, individuare i responsabili e verificare quali informazioni possano essere state compromesse.

L'azienda ha precisato che, sulla base degli elementi attualmente disponibili, l'attacco non avrebbe provocato conseguenze sulle attività operative e sui lavori di costruzione del tunnel.

Rimane tuttavia aperta la questione relativa alla natura dei dati eventualmente sottratti e alla profondità dell'intrusione.

Chi sono gli hacker di Everest: la pista russa

Il nome emerso nelle ricostruzioni è quello di Everest, una rete internazionale di cybercriminali russofoni conosciuta per le operazioni di estorsione informatica.

Il gruppo utilizza il furto di informazioni come strumento di pressione sulle organizzazioni colpite, minacciando in alcuni casi la pubblicazione dei dati sottratti per ottenere pagamenti.

L'eventuale coinvolgimento di Everest nell'attacco al Brennero costituirebbe un ulteriore segnale della vulnerabilità delle grandi infrastrutture europee.

Diversamente dai gruppi apertamente filorussi che rivendicano operazioni a sfondo politico, Everest viene descritto soprattutto come un'organizzazione criminale orientata al profitto. Non sono quindi emersi elementi sufficienti per classificare l'intrusione al Brennero come un'operazione ordinata dal Cremlino.

L'aspetto più preoccupante riguarda comunque il bersaglio: un'infrastruttura ferroviaria di rilevanza internazionale, inserita in una rete di trasporti fondamentale per la mobilità civile, la logistica e, potenzialmente, anche per il trasferimento di mezzi e materiali militari in ambito europeo.

Dai supermercati al Brennero: gli ultimi cyberattacchi che hanno colpito l'Europa

L'attacco alla società della Galleria del Brennero arriva a pochi giorni da una serie di episodi che hanno portato la minaccia informatica direttamente nella vita quotidiana dei cittadini europei.

Tra il 1° e il 3 novembre, diversi impianti di refrigerazione commerciale sono stati colpiti da intrusioni informatiche che hanno consentito agli aggressori di modificare da remoto i parametri di funzionamento dei sistemi frigoriferi.

L'operazione ha interessato strutture in più Paesi europei, compresa l'Italia, provocando anomalie nelle temperature di conservazione e, in diversi casi, il deterioramento di prodotti alimentari.

Il 4 novembre è arrivata una rivendicazione attraverso un video diffuso dai collettivi hacker NoName057(16) e Z-Pentest, entrambi considerati filorussi.

A differenza dell'episodio del Brennero, per il quale viene valutato il possibile coinvolgimento di Everest, gli attacchi alla catena del freddo sono stati accompagnati da una rivendicazione esplicita. Resta comunque necessario distinguere la rivendicazione dalla verifica tecnica delle responsabilità.

Colpita anche una banca del sangue in Francia: il rischio per i servizi essenziali

Uno degli episodi più delicati riguarda la Francia, dove gli aggressori hanno preso di mira anche i sistemi di refrigerazione utilizzati per la conservazione del sangue.

L'attacco ha provocato alterazioni dei parametri di funzionamento, ma i sistemi di allarme hanno permesso di intervenire prima che le scorte venissero compromesse. Secondo quanto riferito dal presidente dell'Établissement français du sang, Frédéric Pacoud, nessuna sacca di sangue è andata perduta.

L'episodio dimostra quanto un'intrusione informatica possa rappresentare una minaccia che supera il semplice danno economico.

Non si tratta più soltanto di sottrarre informazioni o bloccare siti Internet: l'accesso abusivo ai sistemi digitali può alterare direttamente il funzionamento di apparecchiature fisiche, con possibili conseguenze sulla sicurezza alimentare, sulla sanità e sulla continuità dei servizi essenziali.

Secondo una mappatura citata dalla Rai, in Italia sarebbero circa 2.700 i sistemi della catena del freddo potenzialmente vulnerabili. Una cifra che indica l'esposizione al rischio, non il numero di impianti effettivamente attaccati.

L'allarme del Viminale: «Un'iniziativa coordinata a livello europeo»

La gravità degli episodi ha portato all'intervento del ministro dell'Interno Matteo Piantedosi.

Interpellato il 3 novembre sugli attacchi agli impianti di refrigerazione, il ministro ha espresso preoccupazione per un fenomeno verificatosi contemporaneamente in diversi Paesi europei, definendolo presumibilmente un'iniziativa coordinata caratterizzata da evidente ostilità.

Le verifiche sono affidate agli specialisti dell'Agenzia per la Cybersicurezza Nazionale e della Polizia Postale.

Anche il vicepresidente del Copasir, Giovanni Donzelli, ha richiamato il tema della guerra ibrida, sostenendo che gli attacchi informatici dimostrano la necessità di rafforzare gli investimenti nella sicurezza e nella difesa nazionale.

Gli accertamenti dovranno chiarire se gli episodi più recenti facciano parte di campagne coordinate oppure siano azioni autonome condotte da organizzazioni differenti.

La guerra ibrida: colpire l'Europa senza sparare un colpo

Gli avvenimenti degli ultimi giorni mostrano come la dimensione digitale sia ormai parte integrante della sicurezza nazionale.

Una rete ferroviaria, un impianto industriale, una catena di distribuzione alimentare o un sistema sanitario possono diventare bersagli di operazioni informatiche capaci di provocare conseguenze nel mondo reale.

È uno dei principi della cosiddetta guerra ibrida, nella quale strumenti militari tradizionali possono affiancarsi ad attacchi informatici, sabotaggi, disinformazione e pressioni economiche per indebolire un avversario.

Nel caso degli attacchi ai frigoriferi, la rivendicazione dei gruppi filorussi NoName057(16) e Z-Pentest rafforza l'attenzione verso la dimensione politica delle operazioni. Nel caso del Brennero, invece, l'ipotesi Everest suggerisce anche una possibile finalità criminale ed estorsiva.

Non esistono attualmente prove pubbliche che consentano di ricondurre tutti questi episodi a un'unica regia russa.

Tuttavia, il succedersi di intrusioni contro infrastrutture e attività economiche europee evidenzia una vulnerabilità che non può essere sottovalutata.

La ricerca pubblicata il 22 ottobre dalla società di cybersicurezza Forescout aveva già documentato oltre venti attacchi rivendicati dall'inizio dell'anno contro sistemi di refrigerazione industriale e commerciale, molti dei quali associati a gruppi filorussi.

Il problema, dunque, non nasce con gli episodi di novembre, ma si inserisce in una minaccia già osservata dagli specialisti della sicurezza informatica.

Il Brennero è un obiettivo strategico: la cybersecurity diventa una questione di difesa nazionale

Il cyberattacco contro BBT SE assume un significato particolare proprio per l'importanza della Galleria di Base del Brennero.

L'infrastruttura rappresenta uno dei principali progetti di collegamento ferroviario tra l'Italia e l'Europa centrale. La sua futura capacità di trasporto avrà rilevanza non soltanto economica e commerciale, ma anche per la resilienza logistica del continente.

In uno scenario europeo caratterizzato da crescenti tensioni internazionali, la protezione delle infrastrutture strategiche costituisce una componente fondamentale della sicurezza collettiva.

Difendere un'infrastruttura oggi non significa soltanto proteggerla fisicamente, ma anche garantire la sicurezza delle reti informatiche che ne permettono la progettazione, la realizzazione e il funzionamento.

L'episodio del Brennero, gli attacchi ai supermercati e il tentativo di compromettere la refrigerazione delle scorte di sangue in Francia dimostrano quanto sia sottile il confine tra sicurezza informatica e sicurezza materiale.

Se le indagini dovessero confermare il coinvolgimento di Everest, si aggiungerebbe un nuovo episodio riconducibile alla criminalità informatica russofona. Resterebbe comunque da dimostrare qualsiasi eventuale collegamento con interessi statali.

La lezione è già evidente: l'Europa deve proteggere non soltanto i propri confini geografici, ma anche quelli digitali. Perché una vulnerabilità informatica, oggi, può trasformarsi in un problema concreto per infrastrutture, imprese e cittadini.

Fonti

- ANSA – Cyberattacco alla società della Galleria del Brennero, 7 novembre 2026
- ORF Tirol – Hackerangriff auf den Brenner-Basistunnel, 6 novembre 2026
- RaiNews – Attacchi ai refrigeratori e allarme del Viminale, 3 novembre 2026
- RaiNews – Attacco ai frigoriferi e banca del sangue in Francia, 4 novembre 2026
- Agenda Digitale – Analisi tecnica degli attacchi ai frigoriferi, 5 novembre 2026