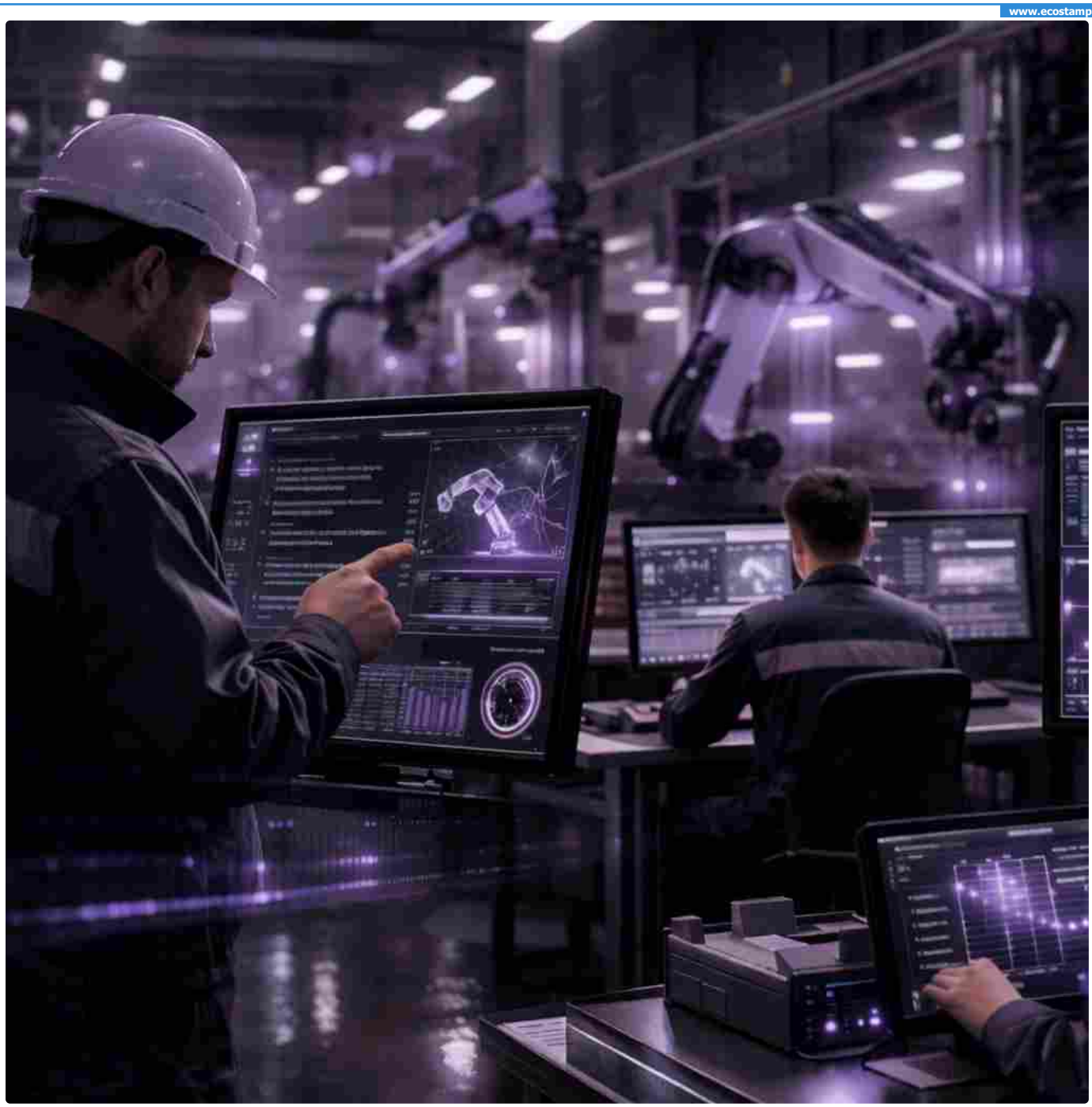
PROGETTOINDUSTRIA.COM

RELATECH analizza l'evoluzione delle minacce Cyber

Posted on 25th March 2026 | In BIG_ARTICLE

PROGETTOINDUSTRIA.COM



***RELATECH** ANALIZZA L'EVOLUZIONE DELLE MINACCE CYBER: ATTACCHI SEMPRE PIÙ AUTOMATIZZATI E MIRATI ALLE IDENTITÀ DIGITALI. L'analisi di **RELATECH** sulle minacce 2026*

La crescita della superficie di attacco digitale e l'aumento delle minacce informatiche evidenziati dai principali osservatori del settore trovano conferma anche nei dati del Risk Operations Center di Relatech.

Relatech, leader nelle **soluzioni digitali,** presenta un'analisi aggiornata dell'evoluzione delle **minacce informatiche** che colpiscono oggi imprese e organizzazioni. La **crescente digitalizzazione dei processi aziendali, la diffusione di infrastrutture cloud, l'interconnessione di sistemi e dispositivi e l'aumento dei servizi digitali esposti su Internet stanno ampliando rapidamente la superficie di attacco a disposizione dei cyber criminali.**

In questo scenario, caratterizzato da attacchi sempre più automatizzati e mirati, diventano sempre più centrali il monitoraggio continuo delle infrastrutture digitali e la capacità di individuare tempestivamente attività sospette.

Il quadro è confermato anche dai principali osservatori del settore. Secondo il Rapporto Clusit sulla sicurezza ICT in Italia, gli attacchi informatici continuano a crescere sia a livello globale sia nel nostro Paese.

Analogamente, l'**ENISA Threat Landscape** evidenzia come ransomware, phishing e compromissione delle credenziali rappresentino i principali vettori di attacco cyber, mentre il **Data Breach Investigations Report (DBIR) di Verizon** sottolinea come una quota significativa delle violazioni informatiche sia legata proprio all'abuso di credenziali e identità digitali compromesse.

Queste tendenze trovano riscontro anche nei dati raccolti dal **Risk Operations Center di Relatech**, il centro di sicurezza attraverso cui l'azienda monitora e analizza quotidianamente migliaia di eventi cyber provenienti dalle infrastrutture digitali dei propri clienti.

L'analisi, basata sugli eventi rilevati negli ultimi sei mesi, offre una fotografia concreta dell'evoluzione recente delle minacce digitali.

All'interno di questa strategia di protezione opera Relatech Cloud Security, la business unit del Gruppo dedicata alla protezione delle infrastrutture digitali e dei dati aziendali.

L'area integra competenze in cyber security, cloud e IT infrastructure, offrendo servizi gestiti e soluzioni personalizzate progettate per rafforzare la resilienza cibernetica delle organizzazioni. Tra le attività rientrano servizi di monitoraggio e gestione della sicurezza attraverso centri operativi SOC e NOC attivi 24/7, oltre all'integrazione di piattaforme tecnologiche progettate su misura per proteggere gli ambienti digitali aziendali.

L'analisi degli eventi gestiti dal SOC di Relatech, classificati secondo il framework internazionale MITRE ATT&CK, consente di individuare con precisione le principali tecniche utilizzate dagli attaccanti. ***Nel periodo analizzato gli attacchi rilevati sono aumentati del 44%, passando da circa 32.000 episodi nell'agosto 2025 a oltre 46.000 nel gennaio 2026.***

Tra le tecniche più diffuse emerge in particolare il **credential access, che rappresenta circa il 30% degli eventi rilevati,** seguito dai tentativi di initial access (24,4%), attraverso cui gli attaccanti cercano di ottenere il primo accesso alle infrastrutture della vittima. ***Un ulteriore 11% degli eventi riguarda attività di command and control, che indicano tentativi di mantenere il controllo dei sistemi compromessi e stabilire canali di comunicazione con infrastrutture esterne.***

Tra gli eventi più frequentemente rilevati figurano attività di scanning delle infrastrutture esposte, tentativi di accesso non autorizzato tramite credential attack e numerose operazioni riconducibili a tecniche di brute force e password spraying, utilizzate dagli attaccanti per individuare credenziali valide e ottenere un primo punto di ingresso nelle reti aziendali.

Le analisi del SOC – ***unità centralizzata, composta da esperti di sicurezza e tecnologie avanzate, che monitora, rileva, analizza e risponde alle minacce informatiche 24/7*** – indicano inoltre che la compromissione delle credenziali di accesso rappresenta la principale causa degli incidenti osservati, spesso ottenuta attraverso campagne di phishing o tentativi automatizzati di accesso alle credenziali sfruttando configurazioni deboli o sistemi esposti su Internet.

Parallelamente, il SOC ha rilevato anche numerosi eventi riconducibili alle fasi successive del ciclo di attacco, tra cui privilege escalation, lateral movement e command and control, che indicano tentativi da parte degli attaccanti di espandere progressivamente la propria presenza all'interno delle reti compromesse e mantenere il controllo dei sistemi.

"Le attività che osserviamo quotidianamente dal nostro centro operativo confermano che gli attacchi informatici stanno diventando sempre più automatizzati, scalabili e mirati alle identità digitali", commenta **Andrea Ferrazzi, Cybersecurity & Cloud Business Unit Director di Relatech**. *"Non si tratta più di eventi isolati, ma di processi strutturati attraverso cui gli attaccanti individuano vulnerabilità nelle infrastrutture esposte. In questo contesto le organizzazioni devono rafforzare la propria postura di sicurezza adottando modelli basati su monitoraggio continuo, analisi avanzata delle minacce e capacità di risposta rapida agli incidenti. La capacità di anticipare e rilevare tempestivamente le anomalie diventa oggi un fattore decisivo per proteggere infrastrutture, dati e continuità operativa"*

ABOUT RELATECH

Relatech, ***è un fornitore leader di soluzioni digitali abilitanti, attivo nei mercati della Digital Transformation, dell'Automazione Industriale e della Cybersecurity,*** *supportando PMI e grandi aziende nei loro percorsi di innovazione e trasformazione digitale, sia in Italia che all'estero.* ***Offre soluzioni end-to-end — dalle prime interazioni digitali con il mondo esterno fino all'automazione industriale — basate su tecnologie avanzate come Intelligenza Artificiale, Cybersecurity, Cloud, IoT e Big Data, oltre a servizi di Advisory, Formazione ICT e Analisi dei Dati, promuovendo un'innovazione responsabile e una crescita sostenibile****. Grazie a un solido ecosistema di Ricerca & Sviluppo e a partnership strategiche — tra cui Microsoft — l'azienda guida le imprese verso un Rinascimento Digitale, in cui la tecnologia è accessibile e abilitante per tutti. Il presente comunicato stampa è online su www.relatech.com (sezione Investor Relations/Comunicati stampa).*

www.relatech.com

Andrea Ferrazzi | attacchi | cyber security | EFA AUTOMAZIONE | minacce | RELATECH

Recommended Posts

KRIWAN: le buone pompe intelligenti

Pompe volumetriche industriali: il cuore silenzioso dell'efficienza produttiva

Misura di portata dell'idrogeno, da ICM

ITAL CONTOL METERS: monitoraggio delle emissioni nelle fonderie