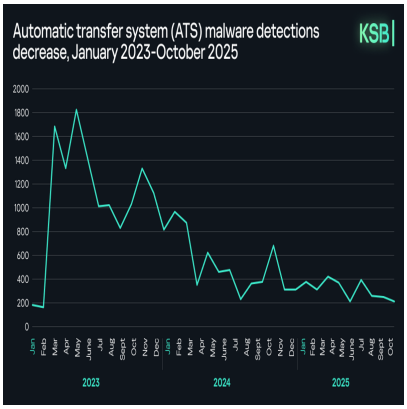

Kaspersky: cresce nel 2025 la pressione cyber sul settore finanziario tra AI, blockchain e reti criminali

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky pubblica il suo Security Bulletin

2025, che ripercorre le piÃ¹ importanti sfide di cybersecurity dellâ??anno passato e offre uno sguardo al futuro. Questo KSB Ã¨ dedicato alla sicurezza nel settore finanziario e fornisce una panoramica dei casi piÃ¹ importanti, delle tendenze chiave e delle minacce in evoluzione. Questâ??anno il settore finanziario ha affrontato un panorama informatico in rapida evoluzione, con la diffusione di malware attraverso le app di messaggistica, attacchi supportati dallâ??intelligenza artificiale, compromissioni della supply chain e frodi basate sulla tecnologia NFC.

La sicurezza informatica nel settore finanziario nel 2025 in cifre

[1] Dati KSN, da novembre 2024 a ottobre 2025.

[2] Novembre 2024 â?? ottobre 2025 vs novembre 2022 â?? ottobre 2023.

[3] Da novembre 2024 a ottobre 2025.

Trend e casi di cybersecurity che caratterizzano il settore finanziario nel 2025

Attacchi su larga scala alla supply chain: il settore finanziario ha dovuto affrontare una serie di attacchi senza precedenti alla supply chain, ovvero incidenti che sfruttano le vulnerabilitÃ dei fornitori terzi per raggiungere i loro obiettivi primari. Le violazioni hanno dimostrato come le vulnerabilitÃ dei fornitori terzi possano propagarsi attraverso le reti di pagamento nazionali, influenzando anche i sistemi centrali.

La criminalitÃ organizzata collabora con i cybercriminali: le organizzazioni criminali combinano sempre piÃ¹ spesso metodi fisici e digitali, creando attacchi piÃ¹ sofisticati e coordinati. Le istituzioni finanziarie hanno dovuto affrontare minacce che combinano social engineering, manipolazione interna ed exploit tecnici.

Vecchi malware, nuovi canali: i criminali informatici sfruttano sempre piÃ¹ spesso le app di messaggistica piÃ¹ diffuse per diffondere malware, passando dal phishing via e-mail ai canali social. I trojan bancari vengono riscritti per utilizzare le piattaforme di messaggistica come nuovo canale di distribuzione, consentendo infezioni su larga scala.

Lâ??AI porta i malware a nuovi livelli: questâ??anno, il malware basato sullâ??AI ha incorporato sempre piÃ¹ tecniche di propagazione e di evasione automatizzate, consentendo agli attacchi di diffondersi piÃ¹ rapidamente e di raggiungere un numero maggiore di obiettivi. Questa automazione riduce anche il tempo tra la creazione e la diffusione del malware.

Attacchi al mobile banking e frodi NFC: il malware Android che utilizza tecniche ATS (Automated Transfer System) permette di automatizzare le transazioni fraudolente, modificando gli importi e i destinatari dei trasferimenti in tempo reale senza che lâ??utente se ne accorga. Anche gli attacchi basati sulla tecnologia NFC sono diventati una delle principali tendenze, consentendo sia frodi fisiche in luoghi affollati che truffe tramite social engineering e app false che imitano quelle delle banche.

Lâ??infrastruttura C2 basata su blockchain Ã¨ in aumento: gli autori di attacchi crimeware incorporano sempre piÃ¹ spesso comandi malware negli smart contract blockchain, prendendo di mira il Web3 per rubare criptovalute. Questo metodo garantisce la persistenza e rende lâ??infrastruttura estremamente difficile da rimuovere. Lâ??utilizzo della blockchain per operazioni C2 consente agli autori degli attacchi di mantenere il controllo anche se i server tradizionali vengono spenti, evidenziando un nuovo livello di resilienza negli attacchi informatici.

Presenza di ransomware: questo tipo di attacchi Ã¨ stata una minaccia persistente per il settore finanziario nella maggior parte delle regioni questâ??anno. A livello mondiale, il 12,8% delle organizzazioni finanziarie B2B Ã¨ stato colpito da ransomware, con il 12,9% in Africa, il 12,6% in America Latina e il 9,4% in Russia e CSI[1].

Scomparsa di alcuni gruppi di malware: alcune famiglie di malware potrebbero scomparire, poichÃ© la loro attivitÃ dipende direttamente dalle operazioni di specifici gruppi criminali.

â??Nel 2025, le minacce informatiche finanziarie si sono evolute creando un panorama complesso, con attacchi che hanno colpito sia le aziende che gli utenti finali. I gruppi criminali hanno combinato sempre piÃ¹ spesso strumenti digitali, accesso privilegiato, intelligenza artificiale e blockchain per ampliare le loro operazioni, costringendo le organizzazioni a proteggere non solo i propri sistemi, ma anche le reti umane che li supportanoâ?•ha affermato Fabio Assolini, Head of the Americas & Europe Units, Kaspersky GReAT.

Previsioni: cosa dovrÃ affrontare la cybersecurity finanziaria nel 2026

[1] Dati KSN, da novembre 2024 a ottobre 2025.

Per garantire sicurezza, gli esperti di Kaspersky consigliano di:

Le organizzazioni finanziarie possono adottare una strategia di sicurezza informatica basata sullâ??ecosistema che unisce persone, processi e tecnologia:

Per ulteriori informazioni sulla nostra esperienza nel settore finanziario e per trovare soluzioni adeguate alla mitigazione dei rischi, Ã¨ possibile visitare il nostro sito web.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Dicembre 17, 2025
Autore
redazione