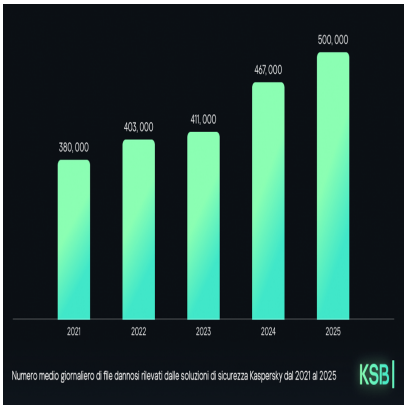

Number of the Year: Kaspersky ha rilevato mezzo milione di file dannosi al giorno nel 2025

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

I sistemi di rilevamento di Kaspersky hanno scoperto una media di 500.000 file dannosi al giorno nel 2025, registrando un aumento del 7% rispetto allâ??anno precedente. In Italia alcuni tipi di minacce hanno mostrato una crescita: câ??Ã¨ stato un aumento del 65% nelle rilevazioni di password stealer, un incremento del 73% nelle rilevazioni di backdoor e una crescita del 148% nelle rilevazioni di spyware rispetto al 2024.

Questi risultati fanno parte della serie Kaspersky Security Bulletin, in cui vengono analizzate le principali tendenze della cybersicurezza dellâ??anno passato.

A livello globale Windows rimane lâ??obiettivo principale dei cyberattacchi. Nel corso del 2025, il 48% degli utenti Windows Ã¨ stato vittima di diversi tipi di minacce. Per gli utenti Mac, questa percentuale si aggira intorno al 29%.

Minacce web

In Italia circa il 27% degli utenti Ã¨ stato vittima di minacce web, ovvero malware che prendono di mira gli utenti quando sono online. Le minacce web non si limitano alle attivitÃ online, ma coinvolgono in ultima analisi Internet in un determinato momento per causare danni.

Minacce on-device

Il 25% degli utenti italiani Ã¨ stato vittima di attacchi on-device, che includono malware diffuso tramite unitÃ USB rimovibili, supporti esterni, o che inizialmente si insinua nel computer in forma non aperta (ad esempio, programmi in installer complessi, file crittografati, ecc.).

Trend regionali dal 2024 al 2025 (rilevamento malware)

Europa

Italia

â??Lâ??attuale panorama delle minacce informatiche Ã¨ caratterizzato da attacchi sempre piÃ¹ sofisticati contro organizzazioni e individui in tutto il mondo. Una delle scoperte piÃ¹ significative fatte da Kaspersky questâ??anno Ã¨ stata la ricomparsa di Hacking Team dopo il rebranding del 2019, con il suo spyware commerciale Dante utilizzato nella campagna APT ForumTroll, che integrava exploit zero-day nei browser Chrome e Firefox. Le vulnerabilitÃ rimangono il modo piÃ¹ diffuso utilizzato dagli aggressori per introdursi nelle reti aziendali, seguito dallâ??uso di credenziali rubate, da cui deriva lâ??aumento di password stealer e spyware registrati questâ??anno. Sono comuni anche gli attacchi alla supply chain, compresi quelli ai software open source. Questâ??anno il numero di questi attacchi Ã¨ aumentato in modo significativo e abbiamo persino assistito alla diffusione del primo worm NPM Shai-Huludâ?•, ha commentato Alexander Liskin, Head of Threat Research di Kaspersky.

â??Questo panorama delle minacce sempre piÃ¹ complesso rende fondamentale per le organizzazioni lâ??implementazione di solide strategie di sicurezza cybersecurity per evitare mesi di inattivitÃ in caso di attacchi. Anche i singoli utenti dovrebbero sempre utilizzare soluzioni di sicurezza affidabili, altrimenti

mettono a rischio non solo i propri dati e il proprio denaro, ma anche quelli delle organizzazioni per cui lavoranoâ?•.

A questo link sono disponibili maggiori informazioni sugli altri report KSB.

Per essere protetti, Kaspersky suggerisce di seguire i seguenti consigli.

Utenti finali:

Aziende:

Tutte le statistiche contenute in questo report sono state fornite da Kaspersky Security Network (KSN). Per il 2025, le analisi coprono il periodo da novembre 2024 a ottobre 2025.

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 16, 2025
Autore
redazione