Kaspersky: aumentano le violazioni informatiche alle PMI a causa della ricomparsa di attacchi basati su Microsoft Excel

Descrizione

(Adnkronos) â?? Milano, 26 giugno 2024. In occasione della Giornata Internazionale delle PMI, che ricorre il 27 giugno, un nuovo
report
di Kaspersky rivela che il numero di infezioni registrate dal settore Ã¨ aumentato del 5% nel primo trimestre del 2024, rispetto allo stesso periodo dello scorso anno, 2.402 utenti si sono imbattuti in malware e software indesiderati nascosti o che imitano prodotti software, con 4.110 file unici distribuiti sotto le sembianze di software per le PMI. Questo dato indica un aumento dell'8% rispetto all'anno precedente e suggerisce un costante intensificarsi dell'attivitÃ dei criminali informatici.
Secondo il nuovo report di Kaspersky, le piccole e medie imprese (PMI) sono sempre piÃ¹ spesso prese di mira dai criminali informatici e la forma di attacco piÃ¹ diffusa continua a essere quella dei Trojan, particolarmente pericolosi perchÃ©, a differenza dei virus, non possono autoreplicarsi e di solito imitano software legittimi. La loro versatilitÃ e capacitÃ di eludere le tradizionali misure di sicurezza li rende uno strumento efficace e molto diffuso. Da gennaio ad aprile 2024, Kaspersky ha registrato un numero di attacchi Trojan pari a 100.465, in aumento del 7% rispetto allo stesso periodo del 2023, e 83.145 attacchi in piÃ¹ rispetto alla principale minaccia rilevata da DangerousObjects, che ha registrato 17.320 attacchi, circa 6.994 in piÃ¹ rispetto allâ??anno scorso. Microsoft Excel Ã¨ tornato a essere il piÃ¹ importante canale di attacco, passando dal quarto al primo posto tra il 2023 e il 2024. Microsoft Word si Ã¨ classificato al secondo posto, mentre Microsoft PowerPoint e Salesforce sono state le terze applicazioni piÃ¹ bersagliate. Per accedere alle informazioni sulle minacce legate al settore delle PMI, gli analisti di Kaspersky hanno incrociato applicazioni selezionate, come MS Office, MS Teams, Skype e altri programmi utilizzati dalle piccole-medie imprese con la telemetria Kaspersky Security Network (KSN). CiÃ² consente di determinare la percentuale di file dannosi e software indesiderati legati a questi programmi, nonchÃ© il numero di utenti attaccati da questi file. Il phishing rimane una minaccia costante nel settore delle PMI e puÃ² avere conseguenze dannose per le aziende. I dipendenti ricevono link a siti web apparentemente familiari e legittimi che imitano servizi molto comuni, portali aziendali e piattaforme bancarie online. Una volta effettuato l'accesso, i dipendenti rivelano inavvertitamente nomi utente e password ai criminali informatici o scatenano attacchi informatici automatici, compromettendo le informazioni sensibili e la sicurezza aziendale. "La nostra intelligence rivela che l'errore umano, spesso dovuto a una scarsa consapevolezza in materia di sicurezza informatica, rimane una vulnerabilitÃ significativa per le PMI. Inoltre, l'uso abituale di Microsoft Excel allâ??interno degli uffici costituisce un terreno fertile per i criminali informatici che possono nascondere e manipolare dati dannosi in grandi dataset che sono poi ampiamente condivisi allâ??interno dell'azienda. Sebbene le PMI possano pensare di non essere un bersaglio, fanno parte di un enorme ecosistema di risorse interconnesse e i criminali informatici sfrutteranno qualsiasi punto debole. Per questo motivo, Ã¨ fondamentale che tutte le PMI definiscano policy chiare per l'accesso a qualsiasi asset aziendale e si assicurino che di ricordare regolarmente al personale l'importanza di seguire le regole di base della cybersecurity", ha commentato Vasily Kolesnikov, Cybersecurity Expert, Kaspersky.
Proteggere il settore delle PMI dai crescenti interessi dei criminali informatici Ã¨ fondamentale per le

sfide economiche, sociali e ambientali globali che ci attendono, in particolare nelle nazioni emergenti in crescita. Secondo i dati delle Nazioni Unite, 7 posti di lavoro su 10 nelle economie emergenti sono nel settore delle PMI, mentre l'accesso ai finanziamenti Ã¨ sproporzionato e rende piÃ¹ difficile per le imprese del settore proteggersi dagli attacchi. Il report completo Ã¨ consultabile su Securelist.com
Per proteggere le aziende dalle minacce informatiche, Ã¨ importante prendere in considerazione le seguenti linee guida: â?¢ Per proteggere l'azienda da un'ampia gamma di minacce, Ã¨ possibile utilizzare le soluzioni della linea di prodotti Kaspersky Next, che offrono protezione in tempo reale, visibilitÃ delle minacce, funzionalitÃ di analisi e risposta EDR e XDR per le organizzazioni di qualsiasi dimensione e settore. In base alle esigenze attuali e alle risorse disponibili, Ã¨ possibile scegliere il livello di prodotto piÃ¹ adatto e migrare facilmente a un altro in caso di cambiamento dei requisiti di cybersecurity. â?¢ Trasformare i dipendenti in un ulteriore livello di protezione contro i cyberattacchi causati dall'uomo grazie a Kaspersky Automated Security Awareness Platform, una soluzione che insegna a comportarsi in modo sicuro su Internet e che include una simulazione di attacco di phishing, in modo che i dipendenti sappiano riconoscere le e-mail di phishing e le altre esche di social engineering. â?¢ L'implementazione di Kaspersky Professional Services ottimizza il workload del reparto IT, che Ã¨ sottoposto a notevoli sfide. Gli esperti Kaspersky valutano lo stato della sicurezza IT attuale, quindi installano e configurano il software Kaspersky in modo rapido e corretto per garantire prestazioni continue. Inoltre, l'assistenza Kaspersky Premium Support facilita la risoluzione rapida degli incidenti tecnici, con un minore impatto sui processi aziendali. â?¢ Fornire al personale una formazione di base sull'igiene della sicurezza informatica e simulare un attacco di phishing per essere sicuri che sappiano distinguere le e-mail di phishing. â?¢ Stabilire una policy di accesso alle risorse aziendali, comprese caselle di posta elettronica, cartelle condivise e documenti online. Ã? importante tenerla aggiornata e rimuovere l'accesso se un dipendente non ne ha piÃ¹ bisogno per svolgere il proprio lavoro o quando lascia l'azienda. Utilizzare un software di intermediazione per la sicurezza di accesso al cloud che aiuti a gestire e monitorare l'attivitÃ dei dipendenti all'interno dei servizi cloud e ad applicare i criteri di sicurezza. â?¢ Eseguire regolarmente il backup dei dati essenziali per garantire la sicurezza delle informazioni aziendali in caso di emergenza.

Informazioni su Kaspersky
Kaspersky Ã¨ unâ??azienda globale di sicurezza informatica e digital privacy fondata nel 1997. Le profonde competenze in materia di Threat Intelligence e sicurezza si trasformano costantemente in soluzioni e servizi innovativi per proteggere aziende, infrastrutture critiche, governi e utenti in tutto il mondo. Il portfolio completo di sicurezza dellâ??azienda comprende una protezione leader degli endpoint e diverse soluzioni e servizi di sicurezza specializzati e soluzioni Cyber Immune, per combattere le sofisticate minacce digitali in continua evoluzione. Oltre 400 milioni di utenti sono protetti dalle tecnologie Kaspersky e aiutiamo 220.000 aziende a tenere al sicuro ciÃ² che piÃ¹ conta per loro. Per ulteriori informazioni Ã¨ possibile consultare https://www.kaspersky.it/

Seguici su:

Tweets by KasperskyLabIT

http://www.facebook.com/kasperskylabitalia

https://www.linkedin.com/company/kaspersky-lab-italia

https://www.instagram.com/kasperskylabitalia/

https://t.me/KasperskyItalia

Contatto di redazione:
Noesis Kaspersky Italia
kaspersky@noesis.net
Piazza Sigmund Freud, 1 â?? Milano â??immediapresswebinfo@adnkronos.com (Web Info)

Categoria

1. News Nazionali

Tag

1. adnkronos
2. comunicati

Data di creazione
Giugno 26, 2024
Autore
admin