2 DIPENDENTI SU 10 INSERISCONO LE PROPRIE CREDENZIALI NEI FORM TRAPPOLA DELLE MAIL DI PHISHING

- ***Oltre 170 mila credenziali di accesso a portali aziendali critici compromesse nel 2024***
- ***L'Italia tra i primi cinque Paesi in Europa con 60.000 dispositivi infetti: i dati di Yarix (Var Group)***

Treviso, 16 luglio 2025 – **Due dipendenti su dieci, pari al 20% del personale di un'azienda, finiscono per inserire inconsapevolmente le proprie credenziali nei moduli ingannevoli contenuti nelle email di phishing,** messaggi che simulano comunicazioni ufficiali – come quelle di una banca, di un fornitore o di un collega – e che inducono l'utente a cliccare su un link e compilare un modulo con username e password. Il numero è in aumento rispetto al dato del 13,4% registrato per il 2023.

Lo attesta l'Y-Report 2025, il report annuale di **Yarix**, centro di competenza per la cybersecurity di **Var Group**, secondo il quale **cresce l'esposizione delle aziende italiane agli attacchi informatici**.

In aggiunta al phishing, si sta diffondendo sempre più anche un'altra modalità di furto di dati: le informazioni sensibili vengono carpite con un apposito software malevolo denominato Infostealer, letteralmente un *"ladro di informazioni"*: solo nel corso del **2024**, il team YCTI (Yarix Cyber Threat Intelligence) ha identificato **oltre 8,1 milioni di sistemi compromessi differenti** (pc, telefoni aziendali, tablet…) e più di **920 milioni di credenziali compromesse da questo tipo di software (+376.7% rispetto al 2023)**.

Tra le credenziali compromesse identificate, **oltre 170 mila** avrebbero permesso di accedere a **portali aziendali critici** gestiti da diversi fornitori di tecnologia, come reti private virtuali (VPN), spesso utilizzate dai dipendenti a lavoro da remoto e Firewall, "barriere" di sicurezza che filtrano la comunicazione tra l'interno e l'esterno dell'organizzazione.

Questa particolare tipologia di software malevolo viene diffuso principalmente attraverso **campagne di phishing e software piratati**, attraverso un modus operandi comunemente utilizzato dalle **gang ransomware**. Una volta infettato il dispositivo, **l'Infostealer raccoglie dati sensibili** e li trasmette al cybercriminale: da credenziali salvate sul browser a carte di credito, fino a cookies e wallets. Questi, specialmente se associati a servizi critici e ancora validi, permettono agli attaccanti di accedere ai sistemi aziendali.

Secondo i dati raccolti da Yarix, **l'Italia nel 2024 è stato il quinto Paese in Europa per dispositivi infetti (60.000, +57.9% rispetto al 2023),** preceduta da Spagna (120 mila), Germania (73 mila), Polonia (71 mila) e Francia (66 mila), e seguita da Romania (54 mila), Regno Unito (44 mila), Portogallo (34 mila) e Ungheria (29 mila). Nel corso del 2024, i team di sicurezza del centro di competenza Yarix hanno inoltre gestito e analizzato diversi incidenti **BEC (Business Email Compromise)**, ovvero email apparentemente legittime, inviate da indirizzi compromessi o contraffatti, che simulano comunicazioni ufficiali per indurre l'utente ad aprire allegati o cliccare link dannosi.

Tra gli incidenti analizzati, il **42% degli attacchi si è concentrato nel primo trimestre del 2024**, facilitati dalla diffusione di nuovi ***Phishing-as-a-Service, "kit"*** **pronti all'uso** che consentono anche a chi ha competenze informatiche minime di accedere a strumenti di phishing avanzati. Tale strumento ha permesso ai cybercriminali di **aggirare i sistemi di autenticazione a più fattori** e **ottenere l'accesso diretto alla casella di posta elettronica delle vittime**. In questi casi, il punto di ingresso dell'attacco è stato principalmente una e-mail di phishing contenente un link o un allegato

malevolo, inviata a un destinatario legittimo. Una volta compromesso, l'account è stato a propria volta sfruttato per condurre ulteriori attacchi all'interno dell'organizzazione o verso contatti esterni.

Tra i settori più colpiti tramite BEC compaiono il **Manufacturing (23,72%)** e il **Food (8,33%).**

"Il phishing non è più un rischio riservato alle grandi aziende: oggi anche le PMI italiane sono nel mirino di attacchi sempre più sofisticati e automatizzati. La diffusione di strumenti come gli Infostealer e i kit di Phishing-as-a-Service abbassa la soglia tecnica per i cybercriminali che, anche senza conoscenze approfondite di hacking, hanno la possibilità di lanciare campagne di phishing su larga scala. L'Italia è tra i Paesi europei più colpiti, ed è dunque fondamentale che anche le imprese di piccole e medie dimensioni investano in formazione, prevenzione e monitoraggio continuo", ha dichiarato **Mirko Gatto, Head of Cybersecurity di Var Group.**

Metodologia

Il report offre uno studio dei dati ricevuti e analizzati da parte di Yarix durante il 2024, considerato come periodo di riferimento. Le informazioni provengono da un panel specifico di aziende monitorate dal Security Operation Center e corrispondono alla base clienti di Yarix, che comprende una vasta gamma di settori dell'economia nazionale. Vengono inoltre inclusi i dati relativi alla gestione di incidenti informatici di aziende che non erano precedentemente clienti. Le imprese rappresentate nel panel analizzato hanno in media oltre un migliaio di dipendenti e generano fatturati superiori ai 50 milioni di euro.
I dati sono stati normalizzati statisticamente e resi omogenei al fine di poterli utilizzare come output quantitativo affidabile e in grado di supportare valutazioni qualitative. Tutti i dati raccolti sono stati automaticamente resi anonimi e aggregati per garantire la privacy, eliminando qualsiasi associazione tra le informazioni e le aziende coinvolte.

Var Group

Var Group è l'operatore leader nel settore dei servizi e delle soluzioni digitali, con un fatturato di 823 milioni di Euro al 30 aprile 2024. Grazie alla professionalità delle oltre 3.850 persone, accompagna le imprese nel loro percorso di trasformazione digitale. Ha una presenza territoriale in 13 paesi nel mondo (Italia, Francia, Germania, Spagna, Austria, Svizzera, Albania, Romania, Lettonia, Messico, USA, India e Brasile) e una profonda conoscenza dei processi aziendali che le permettono di essere vicina agli imprenditori nella definizione di modelli di business evoluti. L'offerta Var Group si arricchisce costantemente grazie alla ricerca continua e alla stretta collaborazione con i più importanti brand tecnologici e digitali, start up e poli universitari, che le consentono di essere al fianco dei maggiori distretti industriali quali Food & Beverage, Pharma, Automotive, Meccanico, Fashion & Luxury, Furniture, GDO & Retail, Finance e Pubblica amministrazione, esaltandone l'eccellenza. La sinergia e la specializzazione dei suoi centri di competenza permettono alle imprese di sfruttare al meglio i benefici del digitale e di sviluppare progetti in ambito Collaborative Workspace, Business Applications, Digital Experience, Industry Solutions, Cyber security, Data Science, Digital as a Service, Digital infrastructure, Industrial Digital Twin e Sustainability Solutions.

Fa parte del Gruppo Sesa, operatore di riferimento in Italia nell'offerta di innovazione tecnologica e soluzioni informatiche e digitali per il segmento business con ricavi consolidati per Euro 3,2 Miliardi al 30 aprile 2024. Sesa S.p.A. è quotata sul mercato Euronext STAR Milano e persegue una strategia di sviluppo sostenibile a beneficio dei propri Stakeholder basata sulle competenze delle risorse umane e l'attenzione alla responsabilità ambientale e sociale. Var Group aderisce al Global Compact ONU, ha acquisito la certificazione ambientale ISO 14001 e la certificazione Great Place To Work nel Novembre 2023 e conseguito il rating Ecovadis a livello Silver.

Yarix

Yarix è il brand di competenza per la cybersecurity di Var Group e uno dei più riconosciuti, innovativi e autorevoli attori italiani nel settore della sicurezza informatica. Da oltre 20 anni fornisce servizi e soluzioni di cyber security e business continuity a industrie, organizzazioni governative e militari, aziende sanitarie e università. Fondata nel 2001, Yarix è oggi uno dei più importanti player in Italia. Dispone di uno dei più avanzati Cognitive Security Operation Center in Italia e si avvale di team di persone specializzate in sicurezza difensiva e offensiva, Cyber Threat Intelligence, Incident Response.

Communication & Media Relations Var Group
Sara Lazzeretti
Mail: s.lazzeretti@vargroup.it
Mob. 3391705791

Ufficio stampa
Community
var@community.it
Claudia Laria – 335 790 4158
Andrea Canu – 334 636 7718