Y-REPORT DI YARIX

ITALIA BERSAGLIO DI RANSOMWARE E INFOSTEALER

28 MILA INCIDENTI DI SICUREZZA NEL 2022

- Oltre 175 mila gli eventi di sicurezza rilevati dal SOC di Yarix, GDO e Fashion i settori più colpiti
- L'Italia al 5° posto per attacchi ransomware su scala mondiale e 5° in Europa per esfiltrazione di credenziali
- Attacchi più efficaci contro grandi aziende, manifesti etici a difesa del settore sanitario e programmi di Bug Bounty tra i trend che hanno caratterizzato il 2022 del cybercrime

Treviso, 3 maggio 2023 – **L'Italia nella lista dei 5 Paesi più colpiti da attacchi ransomware e al 5° posto in Europa per credenziali esfiltrate.**

Sono questi alcuni dei dati restituiti da **Yarix**, business unit Digital Security di Var Group, che nel **"2023 Y-Report"** ha tracciato una panoramica sulle **cyber minacce che hanno investito l'Italia nel 2022**.

Dei 175.045 eventi di sicurezza intercettati nel 2022**, GDO** (12%) **e Moda** (11%) hanno rappresentato i comparti più colpiti, insieme al **sistema bancario e finanziario (10%) e all'Industria Chimica (9%)**. Il **Manufacturing** (23%), l'industria dei **Servizi** (14%) e il **Food and Beverage** (11%) sono invece risultati i settori più esposti a incidenti con un livello di gravità "alto" o "critico".

Di questi eventi, il Security Operation Center (SOC) di Yarix ha rilevato **28.493 incidenti di sicurezza** di gravità media, alta e critica, con un incremento significativo nell'ultimo trimestre dell'anno, conseguenza delle numerose vulnerabilità critiche emerse sugli applicativi di largo consumo.

"L'evolvere della tecnologia e della connessione – e dunque della società - porta con sé una trasformazione naturale del crimine che colpisce con nuove dinamiche e nuovi obiettivi - commenta **Mirko Gatto, CEO di Yarix & Head of Digital Security Var Group.** - *Nel 2022 abbiamo osservato un affinamento delle tecniche delle organizzazioni cybercriminali, che ricorrono a strumenti sempre più sofisticati sia per fare breccia nelle aziende che per evadere le misure di sicurezza schierate in difesa. All'aumento del livello di specializzazione della catena di attacco, la community di sicurezza informatica è chiamata a contrapporre una difesa su due fronti, proattivo e reattivo, per garantire una gestione dell'incidente tempestiva ed efficace. In questo scenario si rende indispensabile adottare strumenti sempre più all'avanguardia, senza tralasciare il tema sempre attuale della formazione e della sensibilizzazione delle persone. La protezione organizzata su questi binari concorre a creare una struttura solida in grado di anticipare e rispondere alle minacce verso l'infrastruttura IT del business".*

Italia bersaglio ransomware

Nello scenario offerto dal Cyber Threat Intelligence di Yarix, **l'Italia spicca per l'incidenza di ransomware,** che si conferma uno dei maggiori fattori di rischio per la sicurezza delle aziende e del sistema Paese: a livello globale, rientra **nella lista dei 5 Paesi più targettizzati da attacchi ransomware**, preceduta solamente da Stati Uniti, Regno Unito, Canada e Germania.

Lockbit, insieme ad AlphV/BlackCat e Hive, resta tra i gruppi più attivi**. Tra gli obiettivi privilegiati dei gruppi ransomware svettano le Strutture commerciali**, davanti a Servizi Finanziari, Industria Edile, Legal & Business e Retail & ingrosso.

Tra le novità dell'anno, Yarix segnala la nascita di **38 nuove ransomware gang costituite nel 2022** sempre più abili nel non lasciare tracce, rendendo più complessa l'identificazione del punto d'ingresso degli attaccanti e dunque della vulnerabilità. In crescita, inoltre la complessità delle tecniche, tattiche e procedure (TTP) utilizzate.

Infine, guardando agli infostealer (software malevolo atto al furto di dati), **l'Italia si posiziona nella top 20 mondiale e al 5° posto a livello europeo per credenziali esfiltrate**, preceduta da Polonia, Francia, Germania, Spagna.

I TREND DEL 2022

Di seguito alcune delle tendenze che hanno caratterizzato le attività dei gruppi criminali nell'anno 2022:

- **Alcuni gruppi ransomware hanno bandito il settore sanitario dai loro obiettivi.** Ragnar Locker, ad esempio, dopo un attacco ai danni di un'azienda ospedaliera italiana, ha pubblicato un messaggio che inaugura la sua politica "zero files encryption". Un caso analogo è stato osservato con il gruppo LockBit che, a seguito della criptazione dei dati di un ospedale pediatrico canadese, ha offerto a titolo gratuito il "decryptor" e ha condannato l'accaduto, allontanando al contempo l'affiliato responsabile dell'attacco.
- Numerose famiglie ransomware sono state aggiornate per rendere i gruppi ransomware **ancora più aggressivi ed efficaci nel colpire le grandi aziende.**
- **I servizi di tipo RaaS sono in aumento e crescono gli affiliati ai gruppi criminali**.
- **Cresce la tendenza di rendere note le chat tra i gruppi cyber criminali e le loro vittime**, per aumentare la pressione durante il processo di negoziazione. Tra i gruppi che ricorrono a questo metodo, Lorenz e LockBit.
- **In crescita i programmi fedeltà dei gruppi criminali:** nel 2022 LockBit ha messo in palio 1 milione di dollari complessivi in cambio di segnalazioni su vulnerabilità o semplicemente per ricevere idee su come migliorare il proprio business model.

Il report è stato redatto secondo i dati forniti dal **Cognitive Security Operation Center (CSOC)** dell'azienda, tra i più evoluti in Italia, e le analisi del **Cyber Threat Intelligence Team (YCTI)** – atto all'investigazione sotto copertura delle attività dei Threat Actor, integrate dalle ricerche sulle azioni di rilevamento, contenimento e gestione della crisi del team di **Incident Response (YIR)** e dai trend rilevati dal **Red team (YRT)**.

Yarix

Yarix è la società a capo della business unit Digital Security di Var Group: da 20 anni fornisce servizi e soluzioni di cyber security a industrie, enti governativi e militari, aziende del comparto sanitario e università. Fondata nel 2001, da Mirko Gatto e Stefano Meller, Yarix è oggi tra i più importanti player sul territorio nazionale con uno dei più importanti e tecnologicamente evoluti Cognitive SOC (Security Operation Center) per il monitoraggio delle reti aziendali. Una cyber control room attiva 24/7, in grado di intercettare proattivamente e bloccare qualsiasi segnale di un tentativo di attacco.
Var Group e Yarix offrono alle aziende italiane che affrontano le sfide dell'innovazione tecnologica e della trasformazione digitale, un nuovo livello di protezione che non può più essere né solo fisica, né solo informatica, ma richiede una visione integrata e d'insieme. Yarix offre un approccio globale ed olistico alla

Security, attraverso il monitoraggio costante e un'analisi obiettiva di tutti i contesti, per ottenere risposte adeguate a prevenire i rischi per le aziende.
Yarix mette a disposizione delle Forze dell'Ordine le sue expertise, collaborando con esse sia sul piano della formazione nei confronti di agenti e funzionari, sia sul piano della consulenza, in occasione di indagini che richiedono competenze specifiche in Digital Forensics. Esempio di questa collaborazione il Protocollo di Intesa firmato con la Polizia di Stato per la prevenzione e il contrasto dei crimini informatici su sistemi informativi critici.
Yarix è stata inoltre la prima azienda privata italiana a far parte del FIRST – Forum for Incident Response and Security Teams – organismo internazionale che riunisce i soggetti pubblici e privati più importanti per la prevenzione e gestione congiunta di incidenti di sicurezza. FIRST aggrega, tra gli altri, la Nasa, Google e Apple.

Ufficio stampa
Community Strategic Communications Advisers
var@communitygroup.it
Giulia Vaccaro – 342 086 5017
Claudia Laria – 335 7904158