Y-REPORT 2024

NEL 2023, RADDOPPIATI GLI EVENTI DI SICUREZZA, AUMENTATI DEL 300% QUELLI DI GRAVITÀ CRITICA E TRIPLICATI GLI INCIDENTI: A RISCHIO LA RISERVATEZZA DEI DATI

- *Nel 2023, Yarix ha rilevato circa 311 mila eventi di sicurezza, quasi il doppio rispetto al 2022 (+87%); triplicati inoltre gli incidenti sfociati in violazioni*
- *L'Italia si conferma tra i 5 Paesi più bersagliati al mondo dai ransomware, Manufacturing (19%), IT (12%), Banking & Finance (11%) i settori più colpiti a livello globale*
- *193 milioni di credenziali compromesse da malware Infostealer (+180% rispetto al 2022), Italia tra i primi 3 Paesi colpiti in Europa*
- *Tra i trend del 2023, l'utilizzo dell'Intelligenza Artificiale come strumento di difesa e l'hacktivismo per motivi ideologici contro target italiani ed europei*

Treviso, 5 giugno 2024 – **Yarix**, società a capo della business unit Digital Security di Var Group, **ha presentato il nuovo Y-Report, la settima edizione dello studio sul panorama degli eventi e degli incidenti informatici che hanno interessato il mondo nel 2023**, con particolare focus sull'Italia.

Nel corso del 2023, i sistemi di monitoraggio del Security Operation Center di Yarix (YSOC) hanno rilevato **circa 311 mila eventi di sicurezza (+87% rispetto al 2022)**, occorrenze che indicano possibili violazioni di un sistema, un servizio o una rete informatica: **quasi il doppio** rispetto al dato dell'anno precedente. Di questi, **circa 83 mila** (+190%, dato triplicato rispetto al 2022) **sono evoluti in incidenti di sicurezza**, concatenazioni di eventi che possono causare la perdita di riservatezza, integrità o disponibilità dei dati aziendali e dei servizi erogati dagli asset informatici protetti, e il loro utilizzo per commettere illeciti.

Gli eventi di gravità critica hanno subìto un aumento del 300%, conseguenza delle **numerose vulnerabilità emerse in applicativi software di uso comune.**

I settori più impattati sono stati il Manufacturing (15%), a causa della maggior presenza negli ambienti produttivi di dispositivi legacy, spesso fuori supporto o comunque non più mantenuti dai produttori**,** il **Fashion (14%)** per l'elevata esposizione legata alla presenza globale degli shop online, e l'area **Energy & Utilities (10%).**

"L'analisi evidenzia un aumento significativo degli eventi di sicurezza nel 2023. Tuttavia, riscontriamo anche un forte impegno verso l'innovazione tecnologica per affrontare le sfide di sicurezza informatica. L'aumento degli attacchi rilevati è infatti da attribuire anche agli sviluppi di nuovi scenari di monitoraggio che sfruttano tecnologie avanzate come Machine Learning (ML) e Intelligenza Artificiale (IA), le quali hanno portato a una maggiore efficacia nell'identificazione delle minacce", ha dichiarato **Mirko Gatto**, CEO di Yarix e Head della Digital Security di Var Group. *"Ad esempio, attraverso la nostra piattaforma di Intelligenza Artificiale **Egyda** in uso nel SOC, che integra hyper-automation e machine learning, sono stati previsti e bloccati l'80% degli attacchi totali rilevati negli ultimi 16 mesi, con tempi di analisi più che dimezzati".*

Ransomware

L'Italia si conferma al quinto posto tra i Paesi più bersagliati dai ransomware, dopo Stati Uniti, Regno Unito, Germania e Canada.

Dei 4.474 incidenti su perimetro globale mappati dal team di Yarix Cyber Threat Intelligence (YCTI), causati da **65 gruppi ransomware, LockBit** risulta il gruppo più attivo, contribuendo da solo al 22% degli attacchi totali.

Anche rispetto al ransomware, il **Manufacturing** si conferma il settore più colpito **(19%).** Seguono **IT (12%), Banking & Finance (11%)**, **Healthcare (9%)** e settore **Educational (6%).** Complessivamente, questi settori hanno registrato il 57% attacchi totali ad opera dei ransomware.

Infostealer

Nel corso del 2023 il team YCTI ha identificato oltre 193 milioni di credenziali compromesse a livello globale da malware Infostealer (+180% rispetto al 2022) esfiltrate da oltre 2,8 milioni di sistemi compromessi. **Oltre 60 mila credenziali esfiltrate erano riconducibili a portali aziendali** (come, ad esempio, VPN e firewall di diversi vendor), rivendute poi nei mercati *underground* e sfruttate per ottenere l'accesso iniziale a un sistema aziendale

L'Italia si posiziona al 20esimo posto su scala mondiale per sistemi compromessi identificati, **con un totale di oltre 38 mila dispositivi compromessi (+123 % rispetto al 2022)**, **e al terzo posto su scala europea,** preceduta da Spagna (60 mila) e Germania (47 mila) e seguita da Francia (36 mila), Polonia (32 mila) e Regno Unito (29 mila).

Hacktivismo

- **L'hacktivismo (crasi di *hacking* e *activism*, l'hackeraggio per motivi politici e ideologici) contro target europei ed italiani è aumentato**. Nel 2023 sono nati e si sono consolidati gruppi hacktivisti pro-Russia, che hanno attuato nuove tattiche volte a destabilizzare i Paesi europei sfruttando le tensioni sociali interni alle società occidentali. Tra questi, gli attacchi condotti contro svariati target - trasporti e logistica, energy & utilities, settore finanziario e settore governativo - in Belgio, Francia e Germania da dicembre 2023 con l'intento, esplicitamente dichiarato dal gruppo pro-Russia NoName057, di sostenere le proteste degli agricoltori in corso nei paesi citati. La strategia applicata è quella della dottrina sovietica delle "misure attive" (*aktivnye meroprijatija*) per influenzare la società civile del nemico e provocare disordini pubblici al suo interno;

- **Crescono le operazioni cyber condotte da hacktivisti pro-Palestina/filo-araba/filo-musulmana**, molti dei quali affiliati a Indonesia e Malaysia, **e pro-Israele**, riconducibili in maggioranza a India e la stessa Israele, relativamente all'escalation del conflitto Israele-Hamas;

- **Il settore trasporti (aereo, marittimo, compagnie di trasporto pubblico, spedizione e logistica) è preso di mira dai gruppi hacktivisti con attacchi di tipo DDoS** - Distributed Denial of Service, che impediscono il funzionamento di un sito o un server. Ciò avviene sia per generare dei disagi ad aziende e consumatori (interruzione di siti web di trasporti,

impossibilità ad acquistare titoli di viaggio e operazioni di check-in ecc…) che per sfruttare l'eco mediatica rivendicando l'attacco nei canali di comunicazione ufficiali dei gruppi. Nel primo trimestre del 2024, Danimarca (10%), **Italia (10%)**, Repubblica Ceca (9%) sono stati i 3 Paesi più colpiti da attacchi DDoS & Web-Defacement, una sorta di vandalismo digitale in cui viene modificata senza consenso l'aspetto di una pagina web o dell'intero sito, allo scopo di lanciare messaggi offensivi o politici.

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

Yarix

Yarix è la società a capo della business unit Digital Security di Var Group e una delle aziende italiane più innovative nel comparto della sicurezza informatica: da oltre 20 anni fornisce servizi e soluzioni di cyber security, a industrie, enti governativi e militari, aziende del comparto sanitario e università.
Fondata nel 2001, Yarix è oggi tra i più importanti player sul territorio nazionale. Dispone di un Cognitive Security Operation Center tra i più evoluti in Italia e si avvale di team specializzati in defensive e offensive security, Cyber Threat Intelligence, Incident Response.
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, supportando gli ufficiali di pubblica sicurezza nell'identificazione delle prove memorizzate all'interno di sistemi e dispositivi informatici. 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.
Oggi la business unit Digital Security di Var Group, di cui Yarix è parte, è un centro di competenze specialistiche per la sicurezza digitale, con sedi in Italia e in Europa, in grado di assicurare una difesa avanzata in ambito cyber security, network & edge security, cloud security.

Metodologia Y-Report 2024

Il report elabora i dati proveniente da un panel di aziende monitorate dal SOC di Yarix, rappresentativo dei diversi settori economici italiani ed europei, ricevuti e analizzati durante il 2023. 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.