Operazione FashionMirror

FRODI ONLINE

YARIX, SCOPERTA UNA RETE DI OLTRE 13 MILA FAKE SHOP

Nel mirino marchi internazionali e del Made in Italy nei settori Moda, Giocattoli e Arredamento

Treviso, 26 gennaio 2023 – **Yarix**, divisione Digital Security di Var Group, rende noto di aver condotto un'**indagine a livello mondiale sul fenomeno dei fake shop**, che ha portato all'identificazione di un'**infrastruttura criminale con oltre 13 mila siti fraudolenti, di cui 1200 associati a 48 marchi italiani.**

L'indagine, che ha visto in prima linea il team di **Cyber Threat Intelligence di Yarix (YCTI)**, è stata avviata nelle prime settimane di gennaio 2023 ed è stata tempestivamente segnalata alla **Polizia Postale e delle comunicazioni**, organo preposto al contrasto delle frodi e dei reati informatici, che ha avviato l'operazione di take down degli shop fraudolenti.
Le operazioni di smantellamento dei domini sono attualmente in corso.

I **fake shop** sono store che riproducono in maniera estremamente fedele gli store originali, in grado di registrare e sottrarre dati finanziari nonché dati identificativi e di contatto. Attività di questo tipo hanno delle conseguenze significative sul brand, a livello reputazionale ed economico, oltre che sul consumatore incauto, i cui dati personali e delle carte di credito vengono carpiti durante il tentativo di acquisto.

Secondo quanto emerso nel corso dell'indagine, la campagna fraudolenta risulta **attiva almeno dal 2020;** dagli indizi raccolti, è possibile ipotizzare che, dalla sua creazione, sia stata costituita da oltre 15 mila domini usati per attività di scam. Al momento della scoperta**, i fake shop ancora online e attivi erano 13 mila.**

Tra i settori più colpiti il settore **Moda**, con grandi marchi del Made in Italy e internazionali. Una percentuale minore ha coinvolto anche i settori **Giocattoli e Arredamento**.

"La pandemia ha contribuito a cambiare le nostre abitudini di spesa e l'e-commerce sta vivendo un'epoca d'oro: negli ultimi anni sono aumentati gli acquisti negli shop online sia per beni che per servizi. Anche il cyber-crimine si adegua ai trend per cercare nuove occasioni di guadagno, e i fake shop sono una delle truffe a cui prestare attenzione. L'indagine del nostro CTI ci ha permesso di rilevare un network consolidato di oltre 13mila domini civetta creato per estorcere denaro ai consumatori più incauti", ha dichiarato **Mirko Gatto, CEO di Yarix**. *"Raccomandiamo agli utenti che effettuano acquisti online di prestare attenzione ai domini, verificando ad esempio la validità degli URL e la presenza del protocollo https e di acquistare solamente dagli store ufficiali".*

Matteo Neri, YCTI Team Lead, ha commentato l'operazione: *"Si tratta di una delle infrastrutture di shop online fraudolenti più grandi e prolifiche mai individuata in Yarix. L'organizzazione era minuziosa: il threat actor, di origine cinese e attivo dal 2020, aveva pieno controllo*

sull'infrastruttura, che manteneva attiva rimpiazzando l'hosting provider a ogni tentativo di take down del sito. Questo garantiva che il network rimanesse online."

Le analisi del team di Threat Intelligence sul codice, i server e i servizi utilizzati nel backend dell'infrastruttura - come i gateway di pagamento o i servizi email usati dai threat actor - hanno permesso agli esperti di attribuire la rete di shop fraudolenti a un **gruppo di origine cinese.**

Per occultare la localizzazione del server, il threat actor sfruttava dei servizi CDN (Content Delivery Network), ovvero un network globale di data center collegati su reti differenti che facilitano la distribuzione dei contenuti web. In questo modo, non rivelava il reale hosting provider e le coordinate del server.

Grazie a questo stratagemma, **il 90% dell'infrastruttura appariva collocata negli USA, Panama e Turchia**; analisi più approfondite sulla posizione reale del server hanno permesso di rilevare delle tracce dell'infrastruttura criminale anche in **Europa.**

Nel suo recente report, Yarix aveva evidenziato come **il biennio 2021-2022 fosse stato caratterizzato da un incremento dei crimini informatici nel settore dell'e-commerce**, con picchi dall'ultima settimana di novembre a fine dicembre, in corrispondenza di periodi di forte traffico come il Black Friday e quello delle festività natalizie. Con riferimento al 2023, lo studio aveva stimato **una perdita globale di oltre 48 miliardi di dollari** proprio a causa truffe online.

Yarix

Yarix è la società a capo della linea di business Digital Security di Var Group: da 20 anni fornisce servizi e soluzioni di cyber security, business continuity e disaster recovery 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 un laboratorio di ricerca e sviluppo a Tel Aviv e 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, 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.

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