TRA NOVEMBRE E DICEMBRE AUMENTATE LE FRODI ONLINE

YARIX: NEL 2023 LE TRUFFE CAUSERANNO AL SETTORE DELL'E-COMMERCE PERDITE PER OLTRE 48 MILIARDI DI DOLLARI

PHISHING, FAKE SHOP E E-SKIMMING, LE TRUFFE PIU' DIFFUSE AI DANNI DEI CYBER CONSUMATORI

Treviso, 29 Dicembre 2022 – All'ascesa del settore dell'e-commerce corrisponde un aumento del numero dei crimini informatici contro esercenti e cyber consumatori.
Secondo **Yarix, divisione Digital Security di Var Group, nel 2023 le truffe online causeranno al settore dell'e-commerce perdite globali di oltre 48 miliardi di dollari,** registrando un incremento del 20% rispetto alle stime del 2022. Secondo quanto analizzato, **i reati aumenterebbero nel periodo che va dal black Friday alle feste natalizie.**

Con un tasso di crescita annuale dei ricavi pari al 16,45% e un numero di utenti che dovrebbe raggiungere i 42,1 milioni entro il 2027, l'e-Commerce in Italia si conferma come settore in ascesa e sempre più appetibile per i cybercriminali, soprattutto in periodi di forte traffico come quelli del black Friday e delle feste natalizie. Secondo l'analisi comparativa effettuata dal team di Yarix Cyber Threat Intelligence (YCTI) nel biennio 2021-2022, si registra **un incremento dei crimini informatici nei confronti dell'e-commerce nel periodo che va dall'ultima settimana di novembre a fine dicembre con un incremento degli attacchi di phishing contro il settore bancario rispetto allo stesso periodo del 2021.**

"*Il crimine è un fenomeno che evolve con l'evolversi della società: non c'è dunque da sorprendersi nel notare come ad un incremento del traffico sugli e-commerce corrisponda anche un aumento dell'azione dei cyber criminali. Secondo i dati elaborati dalla fintech svedese Klarna, il volume di vendite online della settimana del Black Friday 2022 ha registrato una crescita esponenziale rispetto allo scorso anno (+130%) con aumenti del +204% nel periodo 21-24 Novembre.* – commenta **Mirko Gatto, CEO di Yarix** – *Il progresso tecnologico porta con sé anche una maggiore diversificazione della tipologia di cyber-crimini, che spazia ora dalle più comuni frodi finanziarie ai più sofisticati casi di Man-in-the-Middle. A intensificarsi anche la diffusione di "guide", disponibili sul dark web, su come hackerare e-commerce, effettuare rimborsi o spedizioni fraudolente o mettere in campo attività di ingegneria sociale. Un fenomeno in crescita che necessita di un approccio nuovo che promuova non solo azioni legali, ma anche una cultura della sicurezza e dell'attenzione da parte di tutti gli attori coinvolti attorno al crescente fenomeno dell'e-commerce"*.

"*La cultura della sicurezza include anche il controllo continuo e costante dei propri movimenti bancari, non solo nel momento in cui sospettiamo che qualcosa non vada*" aggiunge **Gianluca Zanini, CEO di Kleis**, società della divisione Digital Security di Var Group specializzata nella protezione delle aziende del settore bancario, finanziario ed e-commerce dalle frodi informatiche legate al Digital Payment. "*I frodatori fanno affidamento proprio su questo tipo di leggerezza. Il punto di partenza deve essere sempre il senso critico*".

<u>I trend relativi alle minacce cyber per il 2023 nel settore e-Commerce:</u>

- **Truffe sui social media**: a un registrato aumento della presenza di e-commerce sui maggiori social networks aumenta il numero di utenti che si affidano a indicatori di affidabilità come numero di

connessioni di un account o periodo di attività dello stesso, indicatori facilmente emulabili da attori malevoli per la creazione di account fake;

- **Phishing**: le attività di phishing hanno registrato una crescita nel 2022 e, secondo le stime per il 2023, il trend continuerà la propria ascesa. A livello globale, il phishing correlato all'e-commerce è aumentato del 170% con 7.523.412 attacchi nel secondo trimestre del 2022 rispetto ai soli 2.790.774 del primo trimestre del 2022.
- **Frodi nei pagamenti online**: in seguito alla diffusione capillare di mobile device e un più ampio accesso ad Internet a livello globale, è più probabile che le persone utilizzino nuove tipologie di pagamento quali i digital wallets e la modalità Buy-Now-Pay-Later (BNPL), più vulnerabili ad attacchi informatici.
- **Hackeraggio di Mobile device**: i dispositivi mobili si stanno evolvendo come un importante canale di opportunità per i criminali informatici poiché un numero sempre crescente di utenti preferisce utilizzare i propri dispositivi mobili su più fronti: comunicazioni aziendali e personali, acquisti online ed in generale operazioni bancarie;
- **Fake shops**: online store che riproducono in maniera estremamente fedele gli store originali in grado di registrare e sottrarre dati finanziari nonché dati identificativi e di contatto.
  A questi si aggiungono diversi canali su Telegram in cui vengono proposti articoli di brand noti a prezzi nettamente inferiori a quelli di mercato. Tali attività producono un danno alla reputazione del brand nonché al potenziale cliente che acquista incautamente articoli contraffatti.

Frodi e-commerce - le più comuni:

- **Credit Card Fraud**
  Si verifica quando un criminale informatico utilizza i dati della carta di credito rubati per acquistare prodotti su uno store di e-Commerce. È possibile rilevare e frenare tali attività installando, ad esempio, sistemi quali gli Address Verification Service (AVS).
  Un'ulteriore forma di frode è quella in cui il truffatore ruba dati personali e identificativi di un utente per ottenere una nuova carta di credito.
- **Refund Fraud**
  La frode sui resi si verifica quando gli acquirenti cercano di ingannare i rivenditori durante tutto il processo di restituzione del prodotto. Tale frode può assumere diverse forme, quali a titolo esemplificativo le seguenti:
  - ***wardrobing,*** restituzione di oggetti che sono già stati utilizzati;
  - ***receipt fraud,*** si verifica quando i truffatori utilizzano una ricevuta falsa per ottenere un rimborso su un presunto articolo difettoso o di cui si afferma non sia mai stato ricevuto;
  - ***bricking***, prevede la restituzione di un prodotto per un rimborso totale. In questa forma di frode l'articolo per cui si richiede il rimborso è stato privato delle componenti di maggior valore, che saranno poi rivendute dal criminale. Il bricking è una frode comune nell'industria elettronica.
- **Ingegneria sociale**
  Qualsiasi attività volta ad influenzare o manipolare un individuo al fine di ottenere dati riservati e/o confidenziali. Esempi di ingegneria sociale:
  - **Phishing**: dove l'attaccante invia e-mail apparentemente provenienti da una fonte attendibile per ottenere informazioni confidenziali;
  - **Vishing**: dove l'attaccante utilizza una telefonata verso il target con lo scopo di raccogliere dati e ottenere le informazioni confidenziali;
  - **Smishing**: dove l'attaccante invia messaggi affinché il destinatario compia azioni quali visitare un sito web o cliccare su un link fornito per scaricare un allegato dal contenuto malevolo.
- **Fake Shop**

- **E-Skimming**
  L'e-Skimming comporta l'infezione delle pagine di pagamento di un sito web con software malevolo. L'intenzione è quella di rubare i dettagli personali e di pagamento dei clienti.

Lo Swap SIM

Non solo i messaggi (sms, email, whatsapp etc.) ma anche le notifiche delle applicazioni installate potrebbero essere compromesse o sostituite da malware.
Le aziende di e-Commerce e le banche, per contrastare il fenomeno delle frodi online, si sono mosse infatti creando sistemi di autenticazione a due o più fattori, che utilizzano servizi collegati direttamente alla SIM del cliente.
I frodatori però hanno risposto con una tipologia di frode in continuo aumento, la truffa dallo Swap SIM.
Lo Swap SIM consiste nel prendere possesso del numero di cellulare della vittima per accedere ai servizi e alle informazioni collegate alla SIM, come, ad esempio, le push notification della banca o dell'e-commerce.

I segnali che devono farci sospettare che di essere vittime dello Swap SIM sono:

- quando il telefono smette di funzionare;
- quando non si connette alla rete;
- quando il telefono non ci permette di effettuare chiamate o mandare sms.

Se, riavviato lo smartphone il problema non si risolve, occorre contattare il servizio clienti del proprio Operatore telefonico e chiedere spiegazioni.
Se l'operatore confermerà che è stata richiesta una sostituzione della SIM, allora si è vittime di uno Swap SIM.
Anche una chiamata da parte di un operatore del gestore telefonico (o presunto tale) che vi avvisa di problemi di linea sul vostro smartphone può essere un segnale che si è caduti vittima dello Swap SIM.