Report di Yarix sull'e-Commerce

IL BLACK FRIDAY SUL DARK WEB: IN VENDITA 30 MILIONI DI DATI DI UTENTI ITALIANI

- **Scoperta una possibile compravendita di 30 milioni di dati in vendita sul dark web per campagne di scam e phishing su larga scala**
- **Compromessi oltre 66mila dispositivi con credenziali di accesso italiane: il 33% riguarda le principali piattaforme italiane di e-Commerce**
- **Attività malevole in aumento in concomitanza del Black Friday e del Cyber Monday: + 50% di fake shop nel fashion**

Treviso, 28 novembre 2023 – In occasione delle indagini condotte per il Black Friday, il team di Cyber Threat Intelligence di **Yarix (YCTI)**, divisione Digital Security di Var Group**,** ha portato alla luce un forum underground sul dark web che metteva in vendita **30 milioni di recapiti telefonici di utenti italiani,** in pacchetti contenenti volumi considerevoli di informazioni quali **nome, cognome, indirizzo e-mail, residenza e domicilio**, **a prezzi accessibili ai più**.
I dati potrebbero essere stati utilizzati per condurre **campagne malevole** di varia natura in occasione del Black Friday, come **phishing** (truffe tramite email, messaggi o via telefono) e altre operazioni di Social Engineering. Gli accertamenti sull'origine del TA (threat actor) e sulla legittimità/provenienza del data set sono tutt'ora in corso.

Il periodo del **Black Friday** e del **Cyber Monday**, quest'anno in calendario il 24 e 27 novembre, rappresenta uno dei momenti più importanti per gli acquisti: nel 2022, gli italiani hanno speso mediamente 5,3 miliardi di euro nel weekend dedicato allo shopping online, con una media di 169 euro a persona (Coldiretti/Ixe). Anche i cybercriminali si preparano agli acquisti: le due ricorrenze nel mese di novembre sono infatti tra gli eventi che, a livello globale**, espongono maggiormente le aziende e i consumatori al rischio cyber legato all'e-Commerce**.

La società di sicurezza informatica Yarix ha pertanto condotto un'indagine sul dark web e i forum underground per analizzare i movimenti dei threat actor e le operazioni malevole in preparazione ai giorni dello **shopping natalizio**.

Tra gennaio e ottobre 2023, Yarix ha rilevato **oltre 66mila dispositivi compromessi contenenti credenziali di accesso italiane**, il 33% riguardanti le principali piattaforme italiane di e-Commerce.

In aggiunta all'aumento della vendita di dati relativi a consumatori italiani, sul dark web, **Yarix ha visibilità di una continua vendita di exploit e vulnerabilità, alcune delle quali riguardano software utilizzati dalle piattaforme di e-Commerce**. Come notato da Yarix, l'offerta dei threat actor per l'acquisto parte da una base di 100 USD fino ad arrivare al milione di dollari pagati in criptovaluta.
Le telemetrie elaborate dal team di YCTI per il mese di ottobre e la prima metà di novembre hanno inoltre constatato **un aumento dei fake shop** - store che riproducono in maniera estremamente fedele gli store originali per sottrarre dati personali e di pagamento - del settore fashion**. Confrontato con lo stesso periodo nel 2022, è stato registrato un incremento complessivo del 50%.**

"Nel mese di Novembre, con l'arrivo delle feste natalizie e in occasione delle campagne di sconto legate al Black Friday e al Cyber Monday, si registrano trend di spesa superiori alla media e un aumento del traffico sui siti di e-Commerce; la tendenza si trasforma, però, in un'occasione per i cybercriminali, che attraverso truffe di vario tipo, più o meno articolate, riescono a sottrarre una mole sempre maggiore di dati da rivendere sul dark web", ha dichiarato **Mirko Gatto**, **CEO di Yarix**. *"I*

Threat Actor rivendono poi i dati sottratti e organizzati in banche dati attraverso forum e black market nel Dark Web basandosi sugli interessi dei compratori fraudolenti. Il bottino ha un prezzo irrisorio, sempre più accessibile ad una tipologia specifica di crimine che ha come obiettivo l'appropriazione di credenziali di utenti privati. Parliamo di un fenomeno in costante e preoccupante crescita, tanto da aver determinato l'importanza di una specifica categoria di criminali informatici, denominata Initial Access Brokers (IAB), il cui ruolo consiste appunto nella vendita di punti di ingresso al perimetro informatico di aziende e organizzazioni".

Consigli per utenti finali

Per evitare di incorrere in frodi online e proteggere i propri dati personali in vista dello shopping dell'ultimo periodo dell'anno, Yarix raccomanda di:

- effettuare gli acquisti solo sui siti e le app ufficiali dei negozi e non fornire dettagli di pagamento su siti sospetti. Strumenti come trustpilot.com possono aiutare i consumatori a capire se l'e-Commerce è valido o no;
- assicurarsi che il sito usi il certificato https e presenti il lucchetto nella barra degli indirizzi, anche nel momento del pagamento;
- prestare attenzione ad attività di social engineering: non cliccare mai su link provenienti da fonti sconosciute o scaricare allegati senza prima verificare l'identità del mittente. Errori di spelling nel dominio o nel testo di mail e messaggi sono delle "red flags".

Consigli per le aziende

Per ridurre il rischio di minacce cyber rivolte agli store di e-Commerce, in questo periodo caldo di acquisti, Yarix raccomanda di:

- abilitare i protocolli TLS (https) più recenti per proteggere al meglio la comunicazione tra cliente finale ed e-Commerce;
- implementare processi, servizi e tecnologie di DLP (Data Loss Prevention) per proteggere i dati degli utenti finali e tenere traccia di eventuali accessi, esportazione o salvataggio di informazioni sensibili da parte di amministratori, customer care o da chi ha i privilegi di consultare, modificare o leggere i dati degli utenti finali;
- adottare sistemi di backup e snapshot continuativi (più volte al giorno) al fine di garantire un sistema di backup/restore immediato e rapido, limitando la perdita di dati in caso di incidente informatico o compromissione dell'applicativo e-Commerce;
- implementare processi, servizi e tecnologie di sicurezza per identificare e risolvere vulnerabilità applicative;
- implementare processi e servizi di brand monitoring per identificare e contrastare attivamente shop fraudolenti che hanno l'obiettivo di truffare gli utenti finali e che danneggiano il brand se non vengono svolte attività di contrasto in modo continuativo;
- implementare processi, servizi e tecnologie per proteggere il sito web da attacchi conosciuti (es: sfruttando tecnologie Web Application Firewall);
- è consigliabile infine utilizzare un'istanza di hosting o istanza cloud dedicata e non condivisa con altri portali web al fine di proteggere l'integrità dei dati e la reputazione dello store online.

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.

Ufficio stampa
Community Strategic Communications Advisers
var@communitygroup.it
Giulia Vaccaro – 342 086 5017
Claudia Laria – 335 790 4158