Comunicato Stampa Campari Group

Attacco *malware*: aggiornamento sulla sicurezza dei dati

Milano, 4 dicembre 2020-Campari Group ha annunciato di essere stato vittima di un attacco ransomware mirato a seguito di un accesso non autorizzato alla propria rete. A seguito di indagini tecniche, Campari Group è ora in grado di confermare che alcuni dati personali e aziendali sono stati compromessi.

Campari Group intende porgere le proprie scuse più sincere per ogni eventuale complicazione e preoccupazione che tale situazione possa causare ai propri dipendenti, clienti, fornitori, partner commerciali potenzialmente coinvolti, nonché ai suoi numerosi stakeholder.

Poiché è in corso un'indagine, è possibile che nuovi fatti possano venire alla luce in futuro.

Di seguito è riportata una sintesi generale di quanto appurato alla data di questo comunicato stampa.

A – Informazioni che è stato verificato essere compromesse

(i) Active Directory dei dipendenti - contenente i dati personali di n. 4.736 dipendenti, n. 1.443 ex dipendenti e n. 1.088 consulenti (nome, cognome, indirizzo e-mail, numeri di cellulare (solo dipendenti ed ex dipendenti), ruolo, linee di riporto, numero identificativo personale nel Network Campari) tutti come erano registrati in tale elenco per scopi aziendali;

(ii) Alcuni contratti, documenti e dati personali, dati contabili prinicipalmente riferiti alla consociata statunitense del gruppo (Campari America LLC).

B - Dati personali e aziendali potenzialmente compromessi (esfiltrati, crittografati e / o a cui è stato fatto accesso)

(i) Dati aziendali e / o personali (principalmente dati di contatto inclusi nome, cognome, indirizzo, e-mail, numeri di telefono), informazioni commerciali e dettagli di pagamento di clienti, fornitori e altri partner commerciali di Campari Group - il numero globale stimato di clienti attivi è 10.000 e dei fornitori attivi è 8.500. Possono essere presenti anche dati di contatto di giornalisti (nome, cognome, indirizzo, e-mail, numeri di telefono nell'ordine di 1.000) e curricula vitae di candidati;

(ii) Dati personali di dipendenti ed ex dipendenti inclusi nome, cognome, indirizzo personale, indirizzo e-mail, ruolo, numeri di telefono, dettagli di pagamento, compenso, valutazioni delle prestazioni, documenti di identità, contenuto di documenti / file archiviati da tali dipendenti in cartelle di rete, contenuto della casella di posta elettronica in Outlook - il numero massimo globale è stimato in 6.000;

(iii) Documenti e informazioni aziendali riservati (come contratti, analisi, presentazioni, contabilità) - 2 TB di dati esfiltrati il cui contenuto non è ancora possibile determinare a causa delle conseguenze dell'attacco.

C – Altre informazioni
Campari Group non detiene sistematicamente carte di credito personali o altre informazioni di pagamento o credenziali o qualsiasi altro tipo di password personale.
Non vi sono evidenze di accessi non autorizzati ai siti web di Campari Group.
Tutte le password aziendali per accedere alla rete di Campari Group erano crittografate.

D- Potenziali conseguenze della violazione – Consigli sulla sicurezza
Potenziali conseguenze della violazione derivante dalla perdita di riservatezza sono: l'uso improprio dei dati di contatto, tentativi di *phishing*, contatti indesiderati, tentativi di frode (soprattutto qualora documenti d'identità e password fossero archiviati nelle cartelle di rete di Campari Group), alterazione dei dettagli di pagamento e conseguenti errori di pagamento da parte di Campari Group o a Campari Group (es. modifica codici IBAN).
Campari Group ha tenuto informati i propri dipendenti e stakeholder e ha offerto supporto per il furto di identità dove di prassi.
Alcuni semplici consigli sulla sicurezza:
• non rispondere a richieste o messaggi sospetti (soprattutto in relazione ai pagamenti, come la modifica dei dettagli di pagamento o la richiesta di password o informazioni sul conto bancario);
• non aprire alcun link a meno che non si sia assolutamente sicuri che provenga da una fonte affidabile.

E - Misure difensive e indagini
Campari Group sta implementando tutte le azioni ritenute opportune in questa fase per proteggere ulteriormente il proprio ambiente informatico e, quindi, i dati personali e aziendali ivi archiviati (verifica di tutti i server e dispositivi degli utenti finali, ulteriore innalzamento dei livelli di sicurezza del proprio ambiente informatico mediante misure di hardening, processo di autenticazione multifattoriale per impedire accessi non autorizzati, accelerazione del trasferimento in Cloud).
L'indagine sulle informazioni potenzialmente acquisite o compromesse sta continuando e siamo in costante contatto con le autorità per la protezione dei dati nonché collaborando pienamente con le forze di polizia.

F - Contatto per informazioni e supporto
Per richiedere informazioni su dati personali potenzialmente compromessi o per altro supporto è possibile contattare Daniele di Maiuta, il nostro responsabile della protezione dei dati del gruppo all'indirizzo gpdp.office@campari.com.

* * *

PER ULTERIORI INFORMAZIONI:

Investor Relations

Chiara Garavini Tel. +39 335 5761337 E-mail: chiara.garavini@campari.com

Corporate Communications

Enrico Bocedi Tel. +39 346 5005458 E-mail: enrico.bocedi@campari.com