DOCUMENTI RISERVATI DI EMA SUL VACCINO PFIZER
TROVATI NEL DARK WEB, GRAZIE AL TEAM DI CYBER INTELLIGENCE DI YARIX

IL LEAK CONTIENE INFORMAZIONI SU PRODUZIONE, VALIDAZIONE E COMMERCIALIZZAZIONE DEL VACCINO

È IN CORSO UN'INDAGINE DELLA POLIZIA POSTALE, ALLERTATA DA YARIX.

Empoli, 11 gennaio 2021 – Si riferisce all'attacco hacker subito da EMA – l'Agenzia Europea Del Farmaco – il leak rinvenuto nei giorni scorsi dal team di **Cyber Intelligence** di Yarix, linea di business Digital Security di Var Group. Oltre **33 Megabyte, 5 cartelle e 50 file di informazioni classificate sull'iter autorizzativo e commerciale del vaccino Pfizer-BioNTech (BNT162b2)** in capo ad EMA: materiale rubato dagli hacker il 9 dicembre 2020 e al centro di attività investigativa da parte degli inquirenti di tutta Europa, alla ricerca di materiale documentale particolarmente sensibile perché relativo ad un oggetto – il vaccino contro il Covid – su cui si gioca la sostenibilità sanitaria ed economica del pianeta. La scoperta messa a segno da Yarix pone fine alla ricerca e dà l'avvio all'indagine della **Polizia Postale** italiana.

"I nostri esperti di cyber intelligence sono infiltrati, ormai da mesi, all'interno dei forum underground più frequentati, nel dark web, da hacker e personaggi della cybercriminalità internazionale. È grazie a questo delicato lavoro 'sotto copertura' e a competenze investigative ultra specialistiche, fiore all'occhiello per il nostro Paese, che è stato possibile scoprire il leak EMA/Pfizer: immediatamente abbiamo denunciato l'accaduto alla Polizia Postale, con cui abbiamo da tempo un accordo di collaborazione" – commenta **Mirko Gatto, CEO di Yarix, linea di business Digital Security di Var Group** – "*Il ritrovamento ci dice molto della capacità delle cyber gang di infiltrarsi nelle organizzazioni pubbliche e private, al cuore di processi decisionali strategici. Il dark web diventa, così, lo spazio della ritorsione e del ricatto, in cui rendere pubblici dati sensibili che gli hacker non siano riusciti a farsi remunerare dalle proprie vittime o in cui riversare informazioni capaci di distruggere reputazione e sicurezza. Un territorio da conoscere e presidiare, con risorse e uomini addestrati a misurarsi con questo contesto di frontiera".*

Dinamica della scoperta

- In prima battuta, gli esperti di Yarix hanno trovato i documenti all'interno di un noto forum underground. L'autore del post contenente il leak avrebbe creato il proprio profilo appositamente per caricare le informazioni rubate, cessando successivamente ogni attività;
- Il post dal titolo *"Astonishing fraud! Evil Pfffizer! Fake vaccines!"* riporta la data del 30 dicembre 2020 ore 19:30 ed è stato successivamente rimosso dagli amministratori;
- Oltre al link per scaricare il leak (non più disponibile), il post rimanda ad un thread postato in un altro forum. Questa volta in lingua russa;
- Proprio questo secondo post sarebbe quello originale, come suggerisce la data di pubblicazione (30 dicembre 2020 ore 15:25). Anche in questo caso, l'autore del post è un utente iscritto alla piattaforma solo per l'inserimento del materiale in oggetto;
- Ad oggi il post originale, dapprima rimosso, risulta nuovamente disponibile sul dark web ed aggiornato con nuovi link di condivisione e file consultabili.

<u>Dentro il Leak</u>

- L'archivio scaricato è denominato "EMA_LEAKS.zip". Pesa **33,4MB** e contiene due ulteriori archivi (formato 7z) e un file di testo con la password di estrazione;
- I singoli archivi contengono documenti riservati ripartiti in 5 cartelle e 50 file. Il materiale contiene numerosi **riferimenti a personale di EMA, Pfizer-BioNTech e Commissione Europea**.

- L’analisi ha rivelato la presenza di estratti di conversazioni confidenziali fra il personale EMA e membri della Commissione Europea, relativamente al **processo di produzione, validazione e commercializzazione** del vaccino;
- Sono presenti diversi **screenshot e documenti PDF** che rimandano al **portale Eudralink**, utilizzato internamente all’EMA per le comunicazioni sicure e riservato al solo personale autorizzato;
- Non sussistono elementi certi che consentano di confermare che i dati recuperati siano solo una parte del Leak o se effettivamente includano tutti i dati sottratti nel breach. Certa è, invece, l’intenzione che il leak sottende da parte dei cybercriminali: quella di arrecare un importante danno di reputazione e credibilità a EMA e Pfizer.

Per ulteriori informazioni
Communication & Media Relations Var Group
Sara Lazzeretti
Mail: s.lazzeretti@vargroup.it
Mob. 3391705791

Ufficio stampa
Community Strategic Communications Advisers
var@communitygroup.it
Mob. 345 7357751

Var Group S.p.A.
Var Group www.vargroup.it, con un fatturato di 396 milioni di Euro al 30 aprile 2020, oltre 2500 collaboratori 23 sedi in tutta Italia, 7 all’estero in Spagna, Germania, Austria, Romania, Svizzera e Cina, è uno dei principali partner per l’innovazione del settore ICT. Sostiene la competitività delle imprese del Made in Italy con offerte dedicate ai maggiori distretti italiani come: Manufacturing, Food & Wine, Meccanica industriale, Automotive, Fashion, Furniture Retail & Gdo. La proposta Var Group si rinnova quotidianamente grazie alla ricerca continua e alla stretta collaborazione con Start up e Poli Universitari. Le imprese si trovano di fronte a sfide sempre più complesse: devono poter contare su soluzioni innovative e specializzate. L’offerta Var Group trae la sua forza dalla profonda conoscenza dei processi aziendali e dall’integrazione di più elementi. È frutto del lavoro di Business Unit focalizzate nello sviluppo di progetti di: Customer Experience, Digital Process, Digital Cloud, Digital Security, Smart Services, Cognitive & Advanced Analytics e Business Technologies Solutions. Var Group appartiene al Gruppo Sesa S.p.A., operatore di riferimento in Italia nell’offerta di soluzioni IT a valore aggiunto per il segmento business con ricavi consolidati per Euro 1,776 miliardi al 30 aprile 2020. La società capogruppo Sesa S.p.A. è quotata sul segmento STAR del mercato MTA di Borsa Italiana.