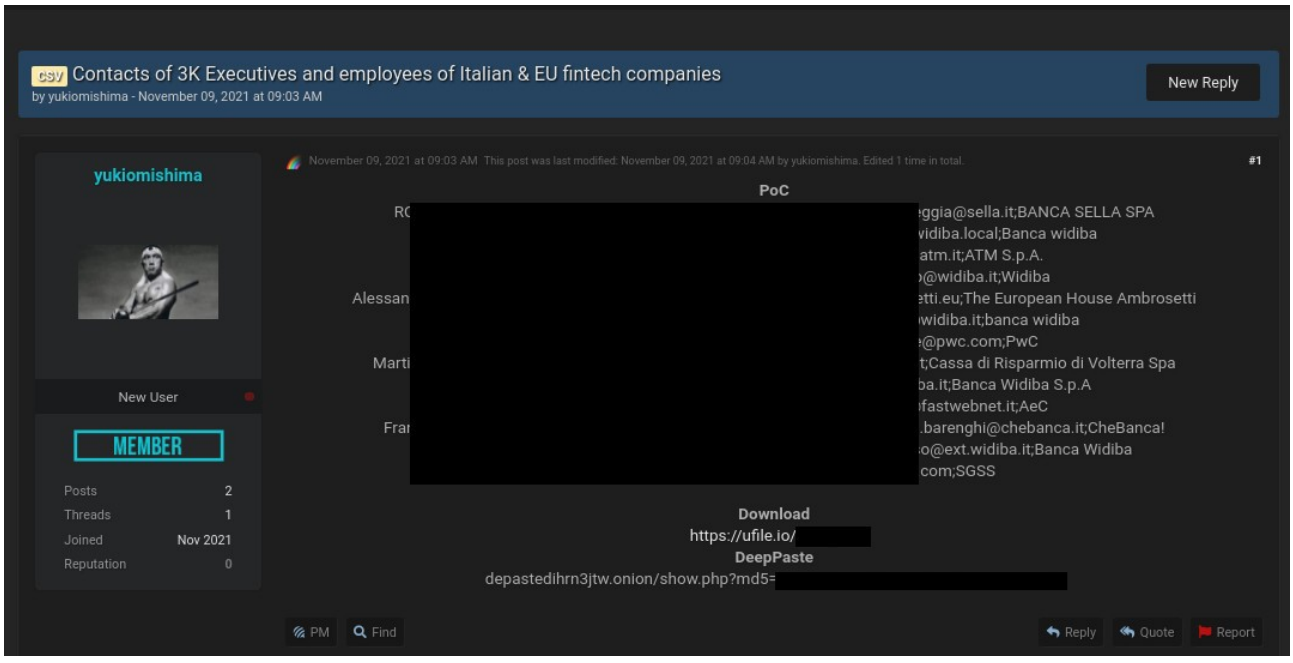
Leak di dati di dirigenti italiani ed europei nel DarkWeb

https://yoroi.company

nota per la stampa del 20 Novembre 2021

Il Cert Yoroi ha individuato un insieme di dati relativi a dirigenti di aziende italiane dei settori bancario e assicurativo in ambienti underground cyber-criminali.

Si tratta della pubblicazione di **3887 contatti telefonici e email di personale** di alto profilo di centinaia di aziende private e pubbliche in vendita nel DarkWeb che potrebbero essere oggetto nelle **prossime settimane** di **tentativi di frode** o di **cyber attacchi** basati sul social engineering. Il rischio è che diventino bersaglio dell così dette Ceo-fraud, la truffa dei manager, dette anche BEC, in cui a partire da una serie di dati personali i criminali riescono a impersonare i legittimi titolari degli account di posta per frodare le vittime prescelte.



Per questo il Cert Yoroi invita ad allertare il personale di banche e assicurazioni di fronte a email inattese, a verificare o propri contatti e a rispondere con attenzione a telefonate impreviste, infine a segnalare messaggi e richieste sospette agli organi di sicurezza interni alla propria azienda.

Il fenomeno delle truffe via email è infatti in crescita e secondo l'FBI ha prodotto **$1,8 miliardi di danni alle aziende nel solo 2020,** una somma **superiore** ai proventi dei riscatti basati sul **ransomware**. Lo scorso agosto grazie alle indagini di Europol sono stati 23 i sospetti incriminati a seguito di una serie di truffe Bec effettuate contemporaneamente in 20 paesi - Paesi Bassi, Romania, Irlanda e altri -. che hanno frodato decine di aziende per circa 1 milione di euro.

È utile ricordare che le truffe di tipo **Business Email Compromise** (BEC) sono una forma di frode tramite posta elettronica in cui il cyber-criminale si "maschera" da manager o dipendente per indurre il destinatario a rispondere a una richiesta inattesa come ad esempio il trasferimento di denaro su un conto diverso da quello solito facendo leva sull'autorità del presunto mittente dell'email e sull'urgenza dell'azione.

Di seguito alcune categoria di questo tipo di truffa:

1. **Truffa alle risorse umane**: l'attaccante si presenta come appartenente al settore delle risorse umane e sollecita informazioni di identificazione personale (PII) in modo da utilizzarle per estorcere denaro o per preparare un attacco più complesso.
2. **Truffa alla contabilità**: l'attaccante impersona un fornitore attendibile dell'azienda usando email contraffatte. Successivamente fa richiesta di pagare la fattura su un conto diverso da quello usato in precedenza dal fornitore.
3. **Truffa del Ceo**: l'attaccante si spaccia come dirigente di alto livello dell'azienda bersaglio. In genere la truffa consiste nella richiesta di trasferire dei fondi un conto fasullo a cui il criminale può attingere direttamente o tramite un intermediario.

In genere queste richieste appaiono credibili in quanto sono arricchite di particolari relative alla funzione del destinatario e alla conoscenza delle dinamiche aziendali, **ma si caratterizzano per giungere alla fine della giornata lavorativa o in prossimità del week end** quando i dipendenti sono stanchi e hanno fretta di chiudere le attività settimanali.

Nelle truffe BEC, i cybercriminali **raccomandano alle vittime di mantenere riservata la comunicazione** ricevuta via email, di comunicare solo via email e di non chiedere altre spiegazioni al telefono.

Bisogna pertanto fare attenzione alle richieste insolite e urgenti fatte in un italiano impreciso e provenienti da indirizzi email sconosciuti o simili a prima vista agli originali, per ingannare le vittime (ad esempio con domini del tipo tUazienda.com al posto di tuazienda.it) o chiedendo al destinatario di rispondere a un diverso indirizzo di risposta.

Yoroi consiglia infine di mantenere alto il livello di consapevolezza degli impiegati e dei clienti, avvisandoli periodicamente delle minacce in corso e di utilizzare un team di esperti per salvaguardare la sicurezza del perimetro "cyber". Per avere un indice di minaccia in tempo reale si consiglia di visitare il seguente link: Yoroi Cyber Security Index

@yoroisecurity www.linkedin.com/company/yoroi/	Media Advisor Arturo Di Corinto (+39) 335 6785259	https://www.yoroi.company https://blog.yoroi.company/ https://yomi.yoroi.company