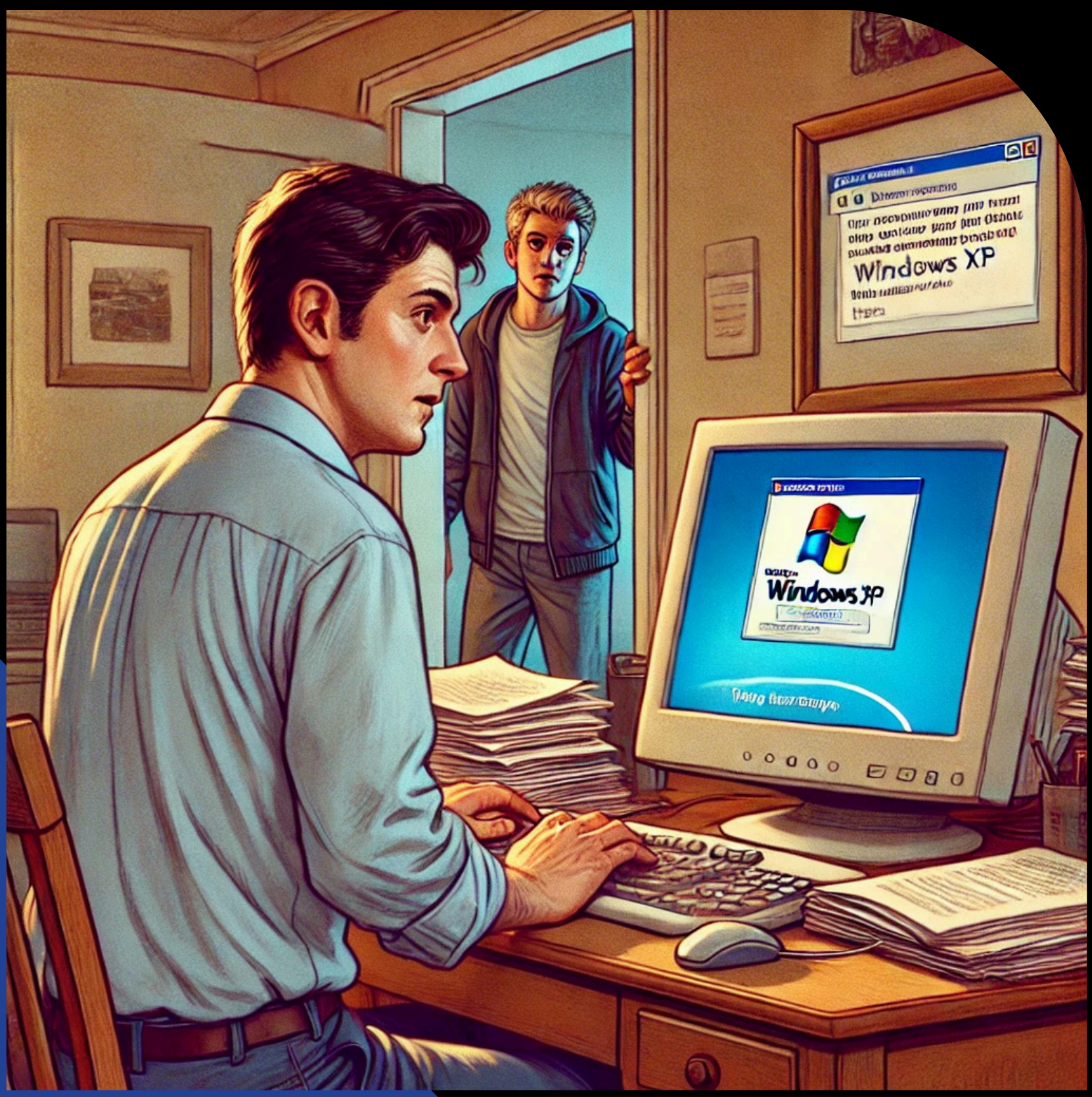
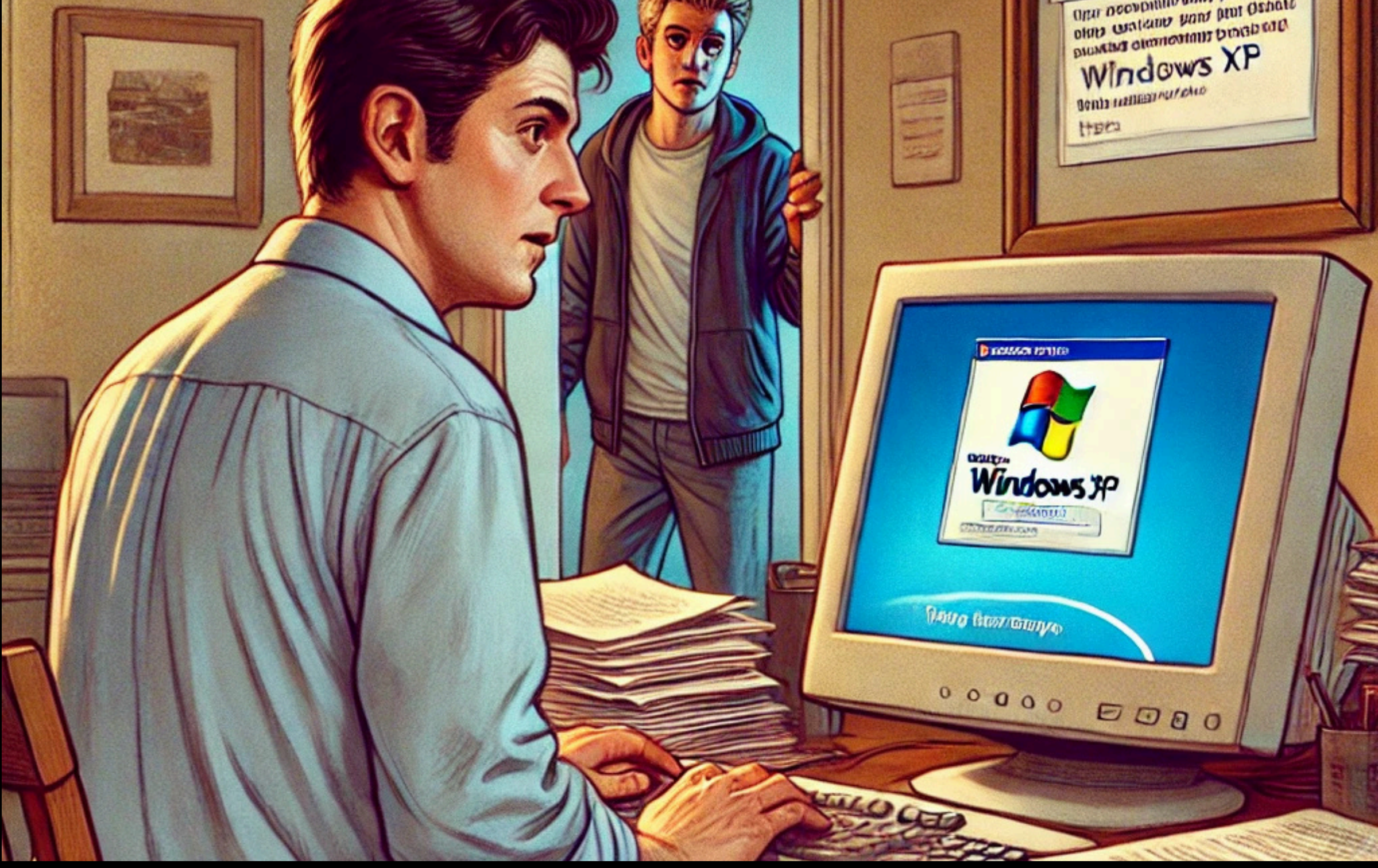
Semkel
RISK & THREAT INTELLIGENCE

LE VOYAGE D'UNE MENACE

Episode 1

Quand l'ordinateur familial met en péril votre entreprise





JEAN

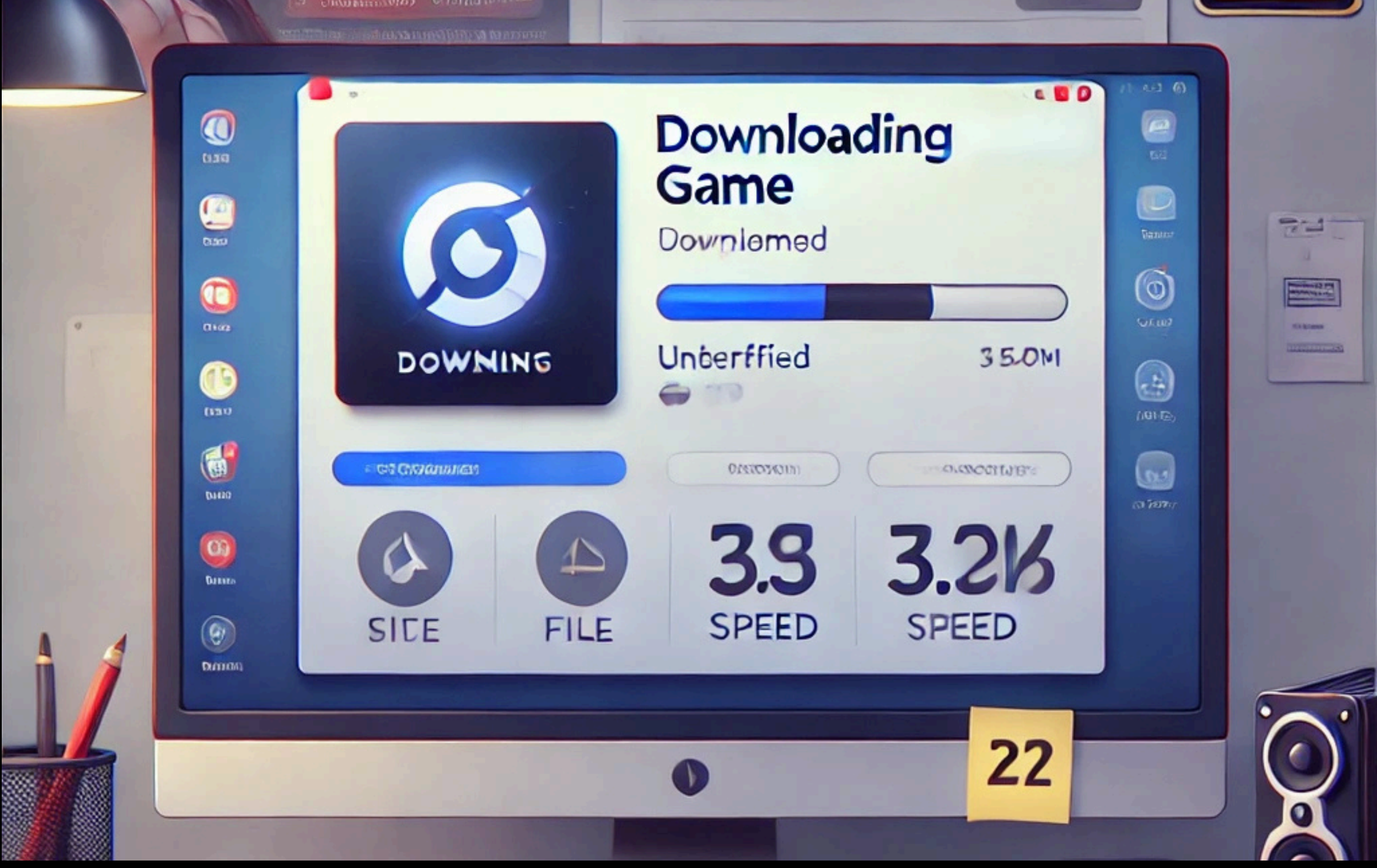
RESPONSABLE FINANCIER

DEPUIS 2020

JEAN A OUBLIÉ SON CÂBLE DE CHARGEUR DE PC PRO. IL DOIT ABSOLUMENT IMPRIMER SON RAPPORT POUR DEMAIN.

IL VA UTILISER L'ORDINATEUR FAMILIAL POUR ACCÉDER AU SYSTÈME D'INFORMATION DE SON ENTREPRISE.

MAIS CE MÊME ORDINATEUR EST PARTAGÉ AVEC D'AUTRES MEMBRES DE LA FAMILLE...



LUCAS

FILS DE JEAN

DEPUIS 2008

LUCAS VOULAIT ABSOLUMENT JOUER À CE NOUVEAU JEU.

IL EST ALLÉ LE TÉLÉCHARGER SUR UN SITE PIRATE ET PROPOSANT UNE VERSION CORROMPUE DU JEU.

LUCAS A PU JOUER MAIS....

LUCAS A INSTALLÉ SANS LE SAVOIR L'INFOSTEALER RACCOON SUR L'ORDINATEUR FAMILIAL QUI N'EST PAS PROTÉGÉ

RACCOON

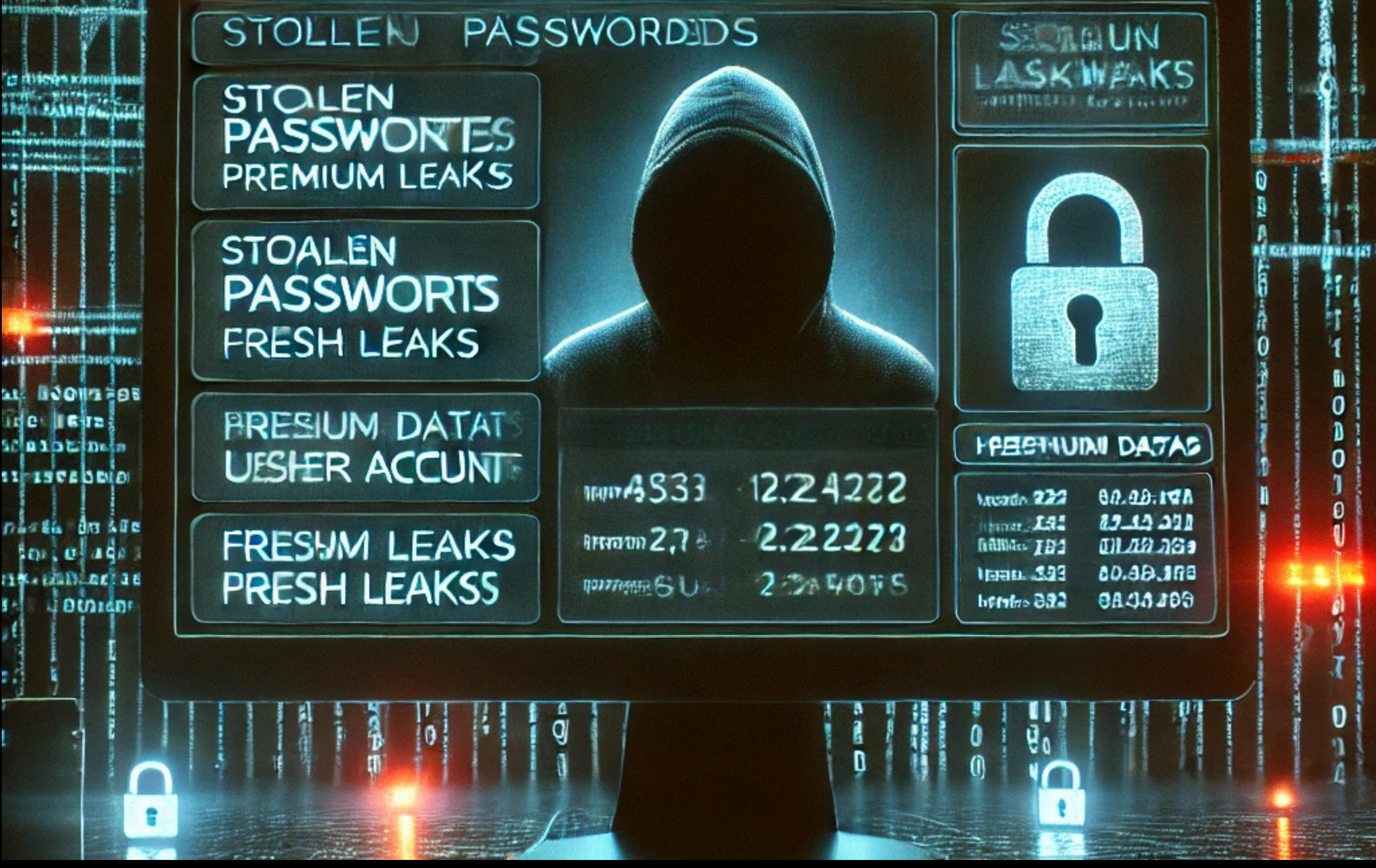
INFOSTEALER

DEPUIS 2019

RACCOON EST UN MALWARE SPÉCIALISÉ DANS LE VOL DE DONNÉES SENSIBLES, COMME LES IDENTIFIANTS, MOTS DE PASSE, ETC.

IL S'INFILTRE SOUVENT VIA DES LOGICIELS PIRATÉS, DES EMAILS DE PHISHING OU DES SITES WEB COMPROMIS.

UNE FOIS INSTALLÉ SUR UN APPAREIL, IL COLLECTE DISCRÈTEMENT LES INFORMATIONS ET LES ENVOIE À SES OPÉRATEURS. CES DONNÉES VOLÉES SONT ENSUITE VENDUES SUR LE DARK WEB OU EXPLOITÉES POUR D'AUTRES CYBERATTAQUES.



SHADOW LYNX

HACKER

DEPUIS 2010

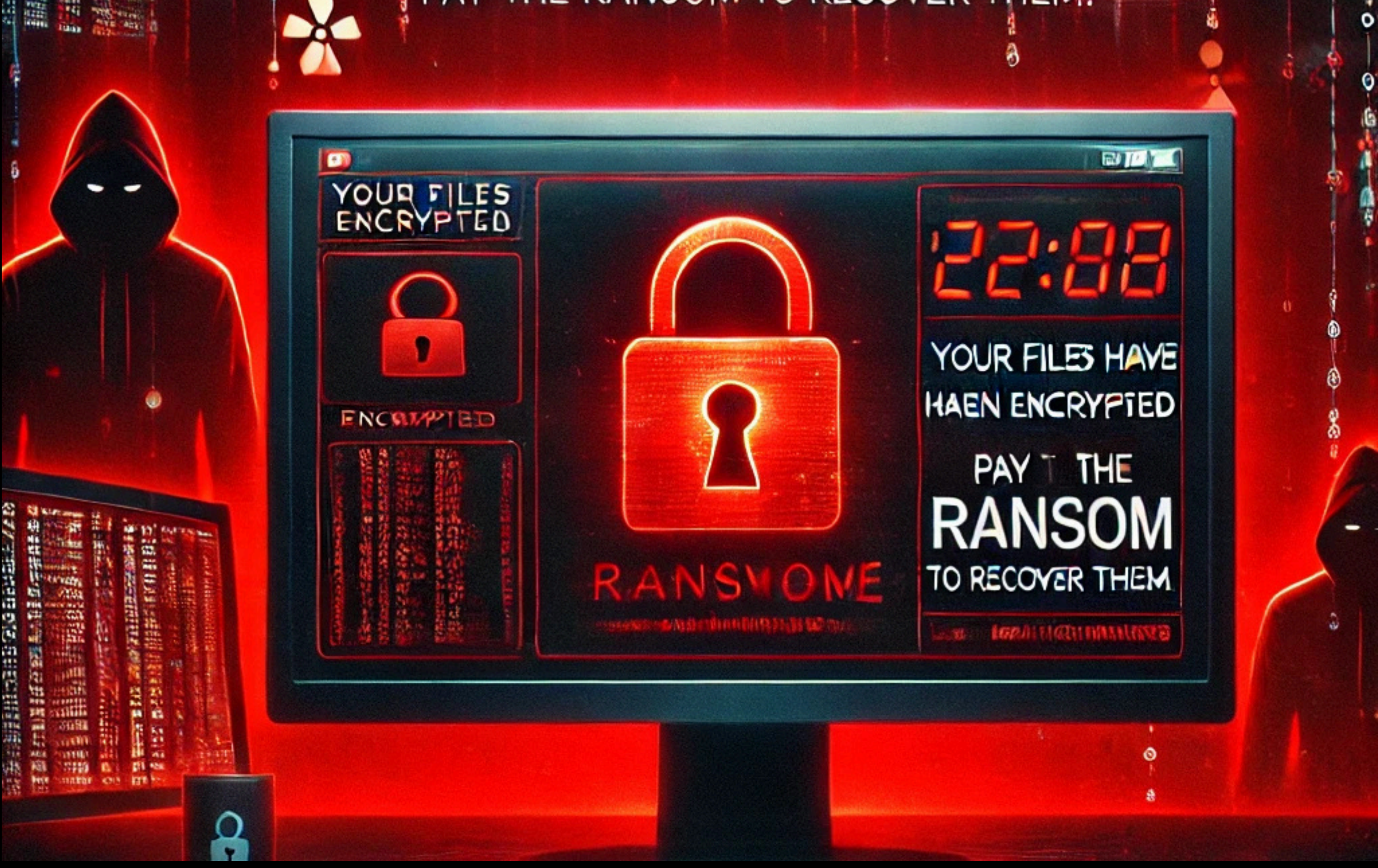
UN HACKER OU GROUPE DE HACKERS S’EMPARE AINSI DU MOT DE PASSE DE JEAN.

LES HACKERS VONT ANALYSER LA VALEUR DU MOT DE PASSE.

JEAN EST RESPONSABLE FINANCIER D’UN GROS COURTIER EN ASSURANCE : NOVENSURE.

LE MOT DE PASSE EST MIS EN VENTE SUR UNE MARKETPLACE DU DARKWEB.

UN GROUPE SPÉCIALISÉ DANS LE RANSOMWARE S’EN PORTE ACQUÉREUR



CRYPTIC.JACKAL

GROUPE DE HACKER

DEPUIS 2012

LE GROUPE VA UTILISER L'IDENTITÉ DE JEAN CHEZ NOVENSURE POUR PRENDRE LE TEMPS DE S'INFILTRER.

ILS VONT ANALYSER L'ORGANIGRAMME DE L'ENTREPRISE ET ÉTUDIER LE SYSTÈME D'INFORMATION POUR POUVOIR EN PRENDRE LE CONTRÔLE.

UNE FOIS PRÊTS, ILS VONT COMMENCER LEURS ACTIONS :

1. **EXFILTRATION DE DONNÉES**
2. **CORRUPTION DES SAUVEGARDES**
3. **MISE EN PLACE D'UN RANSOMWARE**

NOVENSURE

COURTIER EN ASSURANCE

DEPUIS 1998

LA SOCIÉTÉ NOVENSURE SE RETROUVE PARALYSÉE.

100 MILLIONS € DE CA À RISQUE. PLUS AUCUN SYSTÈME NE FONCTIONNE.
PLUS DE COMPTABILITÉ, PLUS DE FACTURATION, PLUS DE NOUVEAUX CLIENTS.

LES HACKERS ONT PUBLIÉS LEUR REVENDICATIONS

CONSÉQUENCES :

- **PERTE DE CONFIANCE DES CLIENTS ET PARTENAIRES**
- **PERTE D’ACTIVITÉS : ILS ONT MIS 2 MOIS À TOUT REMETTRE EN ROUTE**

COÛT TOTAL: 10 MILLIONS € ENTRE LA PERTE D’ACTIVITÉS ET LE COÛT DE LA REMÉDIATION

QU’AURAIT DÛ FAIRE NOVENSURE AVANT L’INCIDENT ?

- METTRE EN PLACE UNE GOUVERNANCE CYBER (DOUBLE AUTHENFICATION, SENSIBILISATION DU PERSONNEL….)
- DÉPLOYER UN SERVICE DE SURVEILLANCE DES INCIDENTS EXTERNES (FUITE DE DONNÉES, VOL D’IDENTIFIANTS…)
- INTÉGRER UNE SURVEILLANCE DU SYSTÈME D’INFORMATION À LEUR POLITIQUE DE CYBERSÉCURITÉ (TRAFIC ANORMAL, EXFILTRATION DE DONNÉES….)
- PRENDRE DES SAUVERGARDES EXTERNES SÉCURISÉES

Semkel
RISK & THREAT INTELLIGENCE

Avec SEMKEL, la société Novensure aurait été protégée et conseillée :

- ANALYSE DES RISQUES
- PROPOSITION DE PLAN D'ACTIONS
- DÉTECTION EN TEMPS RÉEL DES MENACES
- REMÉDIATION DES INCIDENTS

Surveillance 24/7 de vos risques et menaces numériques

semkel.com ou +33 (0) 4 78 51 13 79