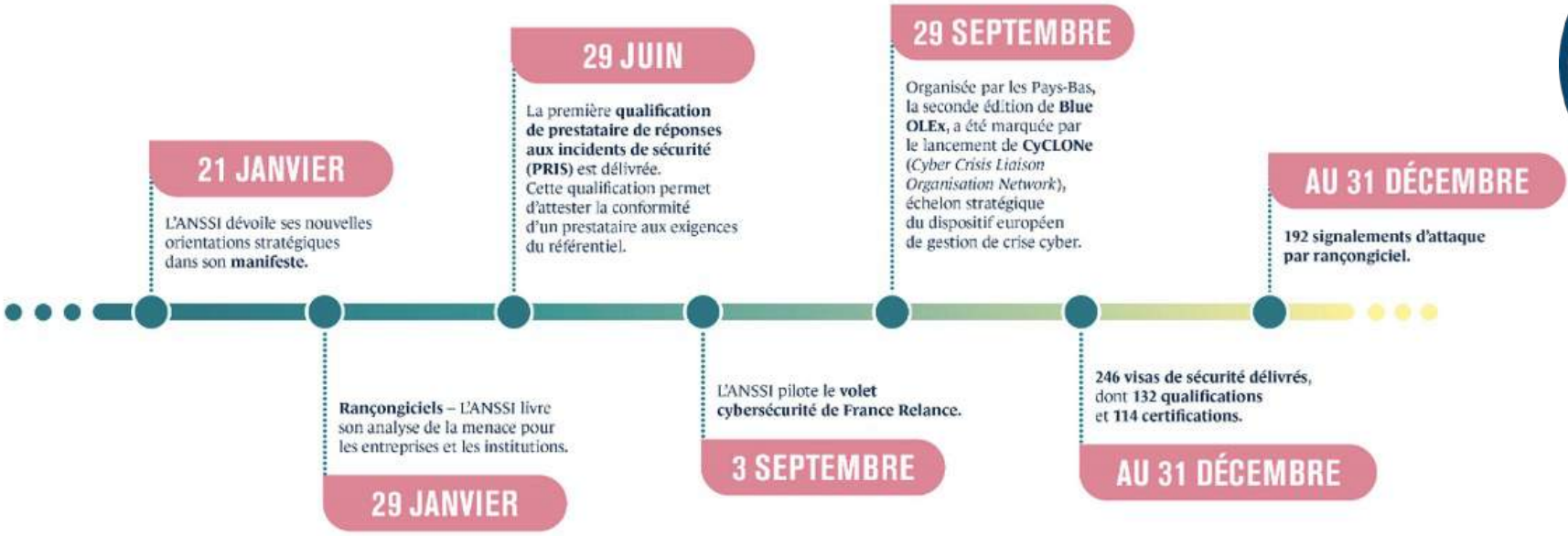
proofpoint®

Rançongiciels : anticiper pour ne pas subir, l'humain au cœur du dispositif

Loïc Guézo — Directeur de la Stratégie, Proofpoint
Secrétaire Général du CLUSIF, réserviste PN

2020 : « La menace croît de manière exponentielle »



« Il faut aussi que les victimes potentielles soient sensibles au danger et que des acteurs privés apportent des solutions. Il faut se placer en amont des attaques pour les aider à comprendre où elles en sont dans leur niveau de sécurité »

proofpoint.

18 février 2021 - présentation de la stratégie nationale pour la cybersécurité.

« 1082 intrusions avérées dans des systèmes d'information en 2021, pour 786 en 2020. +37 % »

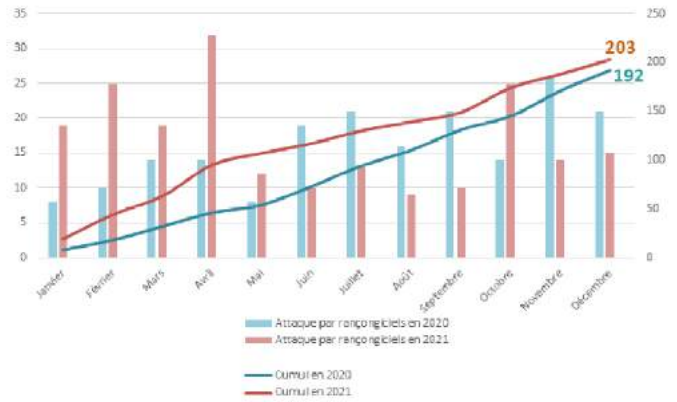


Fig. 1.2. – Statistiques concernant les attaques par rançongiciels traitées par l'ANSSI en 2020 et 2021.

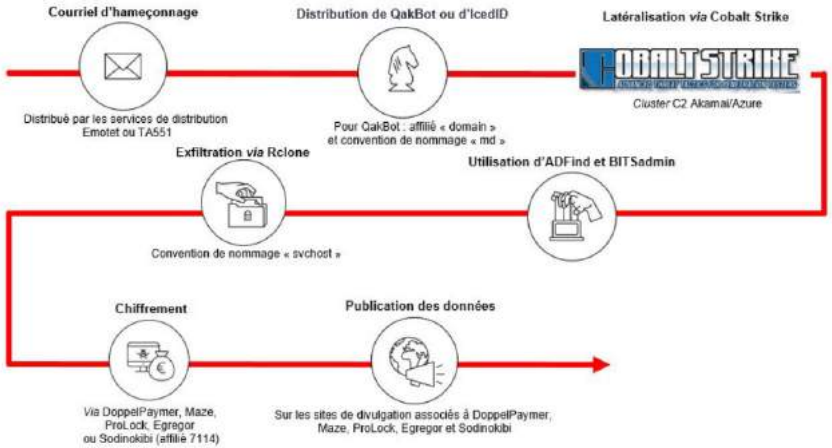


Fig. 1.1. – Chaîne d'infection récapitulative associée au groupe cybercriminel Lockean.


MENU | L'HEBDO | Fil info

L'EXPRESS

S'abonner - 1er mois offert

Actualité économique | Coronavirus : la crise financière | Coronavirus : les entreprises s'adaptent face à la crise | L'économie mondiale à l'arrêt | Les 35 heures | La con

C'est dans l'actu

Une cyberattaque "chirurgicale" a visé des groupes français du BTP et de la sphère publique

Une dizaine d'entreprises françaises ont été visées en mars 2022 par une cyberattaque assez élaborée, détectée par le cabinet Proofpoint.

proofpoint.

Rapport du CERT-W 2022 : tendances et analyses d'un an de réponses à incidents

Les attaquants pénètrent dans les systèmes d'information majoritairement en volant des comptes utilisateurs valides

Les accès à ces comptes sont obtenus par la récupération de **mots de passe** fuités, l'achat de base de données sur le darknet, en exploitant la faiblesse de certains mots de passe, et par le **phishing** qui exploite les manques en matière d'hygiène cybersécurité.

Les infrastructures Active Directory sont toujours des cibles clés pour les attaquants et ont été impliquées dans **8 crises cyber sur 9** gérées par le CERT-W durant la période 2021-22.

Aujourd'hui, selon notre **cyber benchmark** de la maturité des entreprises, 90% des entreprises ont compris qu'il fallait déployer un programme de sensibilisation, mais seulement 15% d'entre elles le font de manière professionnalisée, en adaptant les messages et les outils à différentes populations. Il faut combiner les efforts vers les collaborateurs à des solutions technologiques pour maximiser les effets des actions de sensibilisation.

https://fr.wavestone.com/fr/insight/cert-w-2022-cybersecurite-tendances-analyses/

proofpoint.

L'attaque de ransomware contre FatFace

Chronologie d'une attaque

1

1988

La société FatFace est fondée.
Son chiffre d'affaires en 2020 est de 198,1 millions GBP pour plus de 200 boutiques.

2

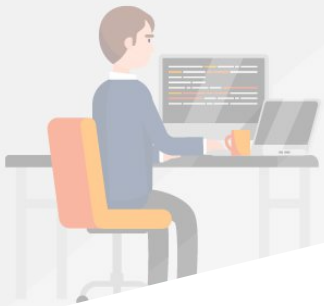
10 janv. 2021

Le gang Conti infiltre le réseau de FatFace par le biais d'une attaque de phishing.

3

10-17 janv. 2021

Conti obtient des droits administrateur et se déplace latéralement sur le réseau.



4

17 janv. 2021

Une attaque de ransomware est exécutée et entraîne l'exfiltration de plus de 200 Go de données.

5

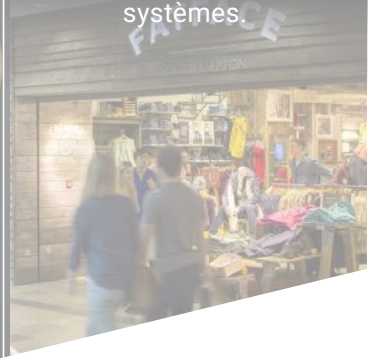
Janv.-mars 2021

FatFace verse une rançon de 2 millions USD à Conti pour récupérer l'accès à ses systèmes.

6

24 mars 2021

FatFace informe ses clients de la compromission de ses systèmes.



L'attaque de ransomware contre FatFace

Chronologie d'une attaque

1

1988

La société FatFace est fondée.
Son chiffre d'affaires en 2020 est de 198,1 millions GBP pour plus de 200 boutiques.

2

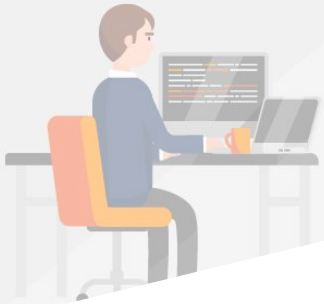
10 janv. 2021

Le gang Conti infiltre le réseau de FatFace par le biais d'une attaque de phishing.

3

10-17 janv. 2021

Conti obtient des droits administrateur et se déplace latéralement sur le réseau.



4

17 janv. 2021

Une attaque de ransomware est exécutée et entraîne l'exfiltration de plus de 200 Go de données.

5

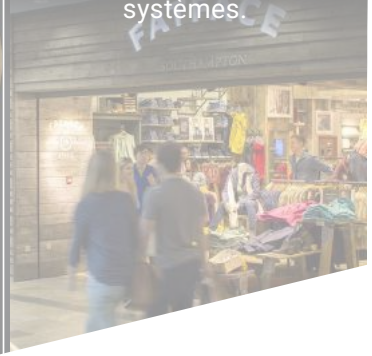
Janv.-mars 2021

FatFace verse une rançon de 2 millions USD à Conti pour récupérer l'accès à ses systèmes.

6

24 mars 2021

FatFace informe ses clients de la compromission de ses systèmes.



L'attaque de ransomware contre FatFace

Chronologie d'une attaque

1

1988

La société FatFace est fondée.
Son chiffre d'affaires en 2020 est de 198,1 millions GBP pour plus de 200 boutiques.

2

10 janv. 2021

Le gang Conti infiltre le réseau de FatFace par le biais d'une attaque de phishing.

3

10-17 janv. 2021

Conti obtient des droits administrateur et se déplace latéralement sur le réseau.

4

17 janv. 2021

Une attaque de ransomware est exécutée et entraîne l'exfiltration de plus de 200 Go de données.

5

Janv.-mars 2021

FatFace verse une rançon de 2 millions USD à Conti pour récupérer l'accès à ses systèmes.

6

24 mars 2021

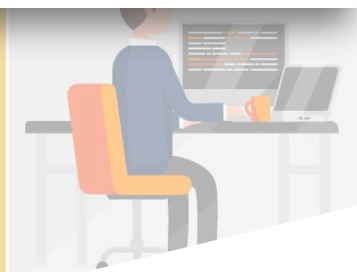
FatFace informe ses clients de la compromission de ses systèmes.

L'attaque de ransomware contre FatFace

Chronologie d'une attaque

La société FatFace est fondée.
Son chiffre d'affaires en 2020 est de 198,1 millions GBP pour plus de 200 boutiques.

attaque de phishing.



4

17 janv. 2021

Une attaque de ransomware est exécutée et entraîne l'exfiltration de plus de 200 Go de données.

5

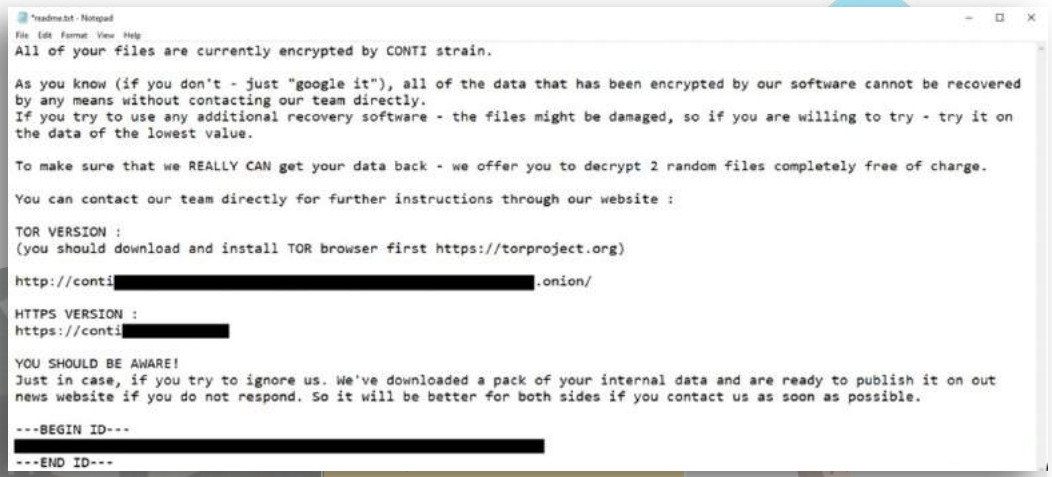
Janv.-mars 2021

FatFace verse une rançon de 2 millions USD à Conti pour récupérer l'accès à ses systèmes.

6

24 mars 2021

FatFace informe ses clients de la compromission de ses systèmes.



```
readme.txt - Notepad
File  Edit  Format  View  Help
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered
by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on
the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://conti[redacted].onion/

HTTPS VERSION :
https://conti[redacted]

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out
news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

---BEGIN ID---
[redacted]
---END ID---
```

L'attaque de ransomware contre FatFace

Chronologie d'une attaque

1

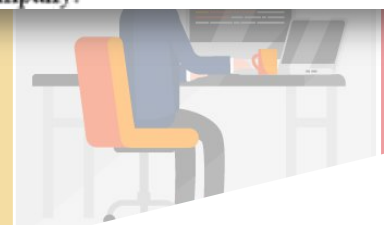
1988

La société FatFace est fondée.
Son chiffre d'affaires en 2020 est de 198,1 millions GBP pour plus de 200 boutiques.

10

Le ga
le rés
par
attaq

Support: Well, your online sales seem pretty nice to me, we've went through the databases and the traffic statistics before calculating the initial offer.
27 days ago
Support: I will need some time to discuss with my boss if we have go down a bit though, basing to the fact that you have a large offline retail network. And we will review the financial documents that are in our possession.
27 days ago
[redacted] Yes, please discuss with your boss. We have a ecommerce presence, but it is small and it only makes up about 25% of our revenue. The majority of our sales and profit comes from our stores which have basically come to a halt
27 days ago
Support: And what about your cyber insurance? Most of our attacks are covered by the insurance companies when the demands cannot be handled by other reasons.
27 days ago
Support: Seems like we've found what we have looked for in your papers. Our demands are lower than your insurance coverage. I have no idea how this can break you when you are insured for 7,500,000 GBP. I suppose it's time to contact your insurance company.



5

Janv.-mars 2021

FatFace verse une rançon de 2 millions USD à Conti pour récupérer l'accès à ses systèmes.

6

24 mars 2021

FatFace informe ses clients de la compromission de ses systèmes.

L'attaque de ransomware contre FatFace

Chronologie d'une attaque

1

1988

La société FatFace est fondée.
Son chiffre d'affaires en 2020 est de 198,1 millions GBP pour plus de 200 boutiques.

2

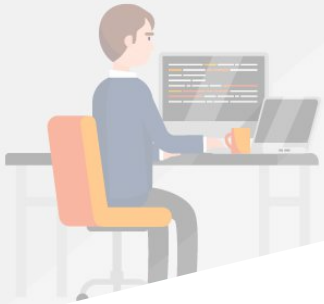
10 janv. 2021

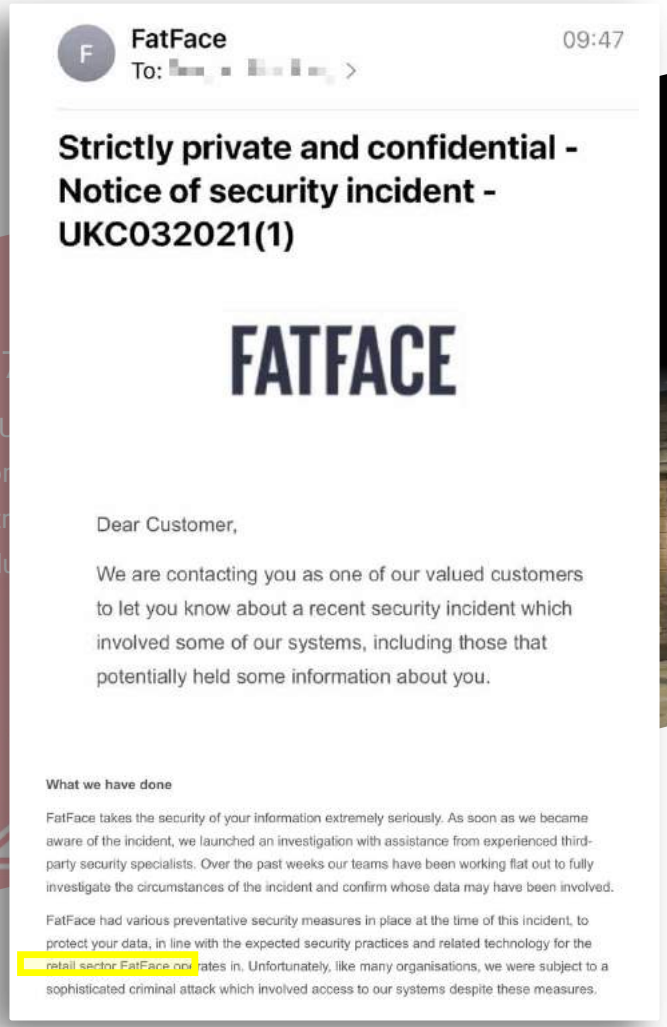
Le gang Conti infiltre le réseau de FatFace par le biais d'une attaque de phishing.

3

10-17 janv. 2021

Conti obtient des droits administrateur et se déplace latéralement sur le réseau.





F FatFace 09:47
To: [redacted]

Strictly private and confidential - Notice of security incident - UKC032021(1)

FATFACE

Dear Customer,

We are contacting you as one of our valued customers to let you know about a recent security incident which involved some of our systems, including those that potentially held some information about you.

What we have done

FatFace takes the security of your information extremely seriously. As soon as we became aware of the incident, we launched an investigation with assistance from experienced third-party security specialists. Over the past weeks our teams have been working flat out to fully investigate the circumstances of the incident and confirm whose data may have been involved.

FatFace had various preventative security measures in place at the time of this incident, to protect your data, in line with the expected security practices and related technology for the retail sector FatFace operates in. Unfortunately, like many organisations, we were subject to a sophisticated criminal attack which involved access to our systems despite these measures.

6

24 mars 2021

FatFace informe ses clients de la compromission de ses systèmes.

L'attaque de ransomware contre FatFace

Chronologie d'une attaque

1

1988

La société FatFace est fondée.
Son chiffre d'affaires en 2020 est de 198,1 millions GBP pour plus de 200 boutiques.

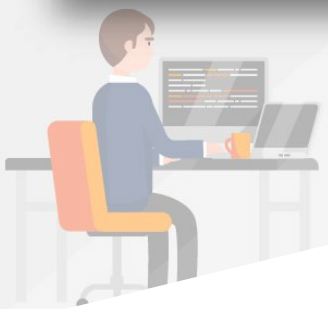
2

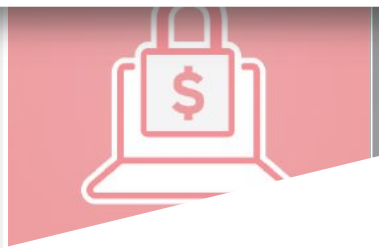
10 janv. 2021

Le gang Conti infiltre le réseau de FatFace par le biais d'une attaque de phishing.

10

Con
ac
dépla





Rosi Prescott
16 reviews GB

3 hours ago

Security Breach kept secret

Astonishing to be kept in the dark for over 2 months since the security breach exposed our email and residential addresses, telephone numbers and elements of our credit/debit cards. The thieves would have had a field day during that time when we victims were blissfully unaware of the situation. Quite shocking. Do NOT shop at Fat Face. They have outmoded and inadequate systems in place to secure your data.

Useful Share

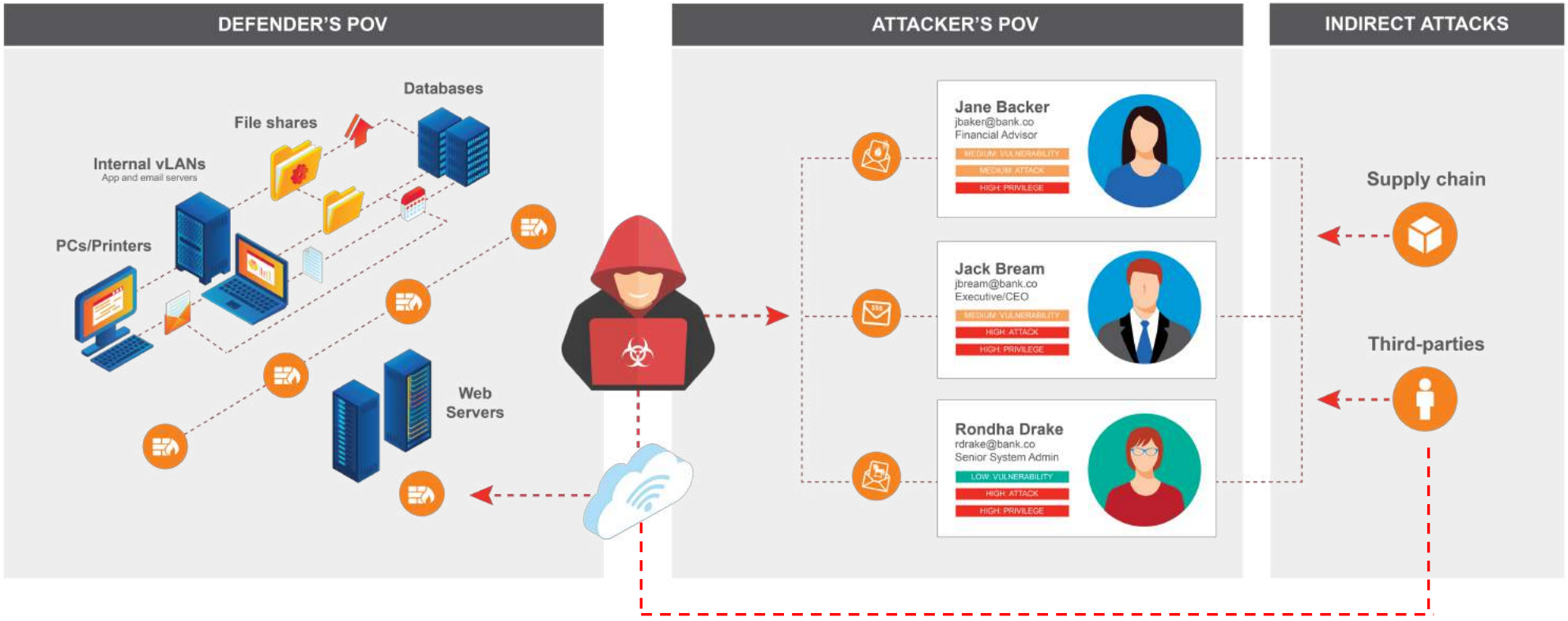
© Trustpilot

6

24 mars 2021

FatFace informe ses clients de la compromission de ses systèmes.

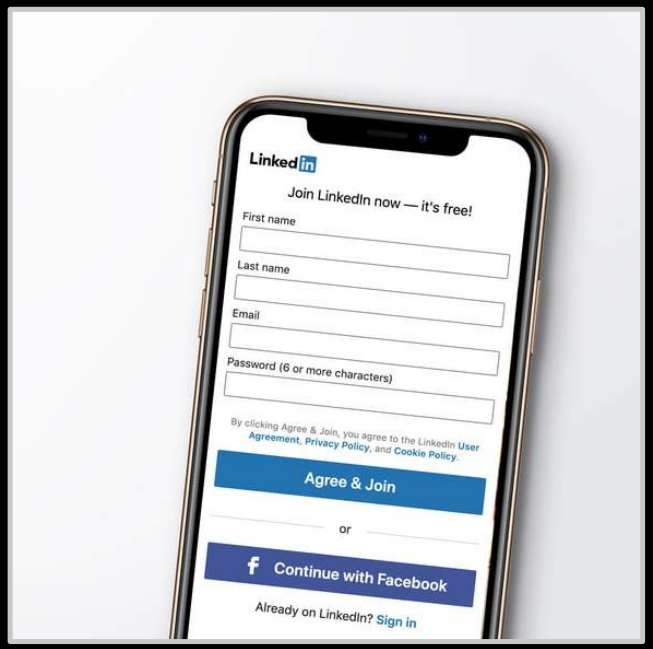
Les cybercriminels ne piratent plus les systèmes…
Ils s'y connectent…



Comment les cybercriminels exploitent les collaborateurs

L'ingénierie sociale au cœur de la plupart des attaques

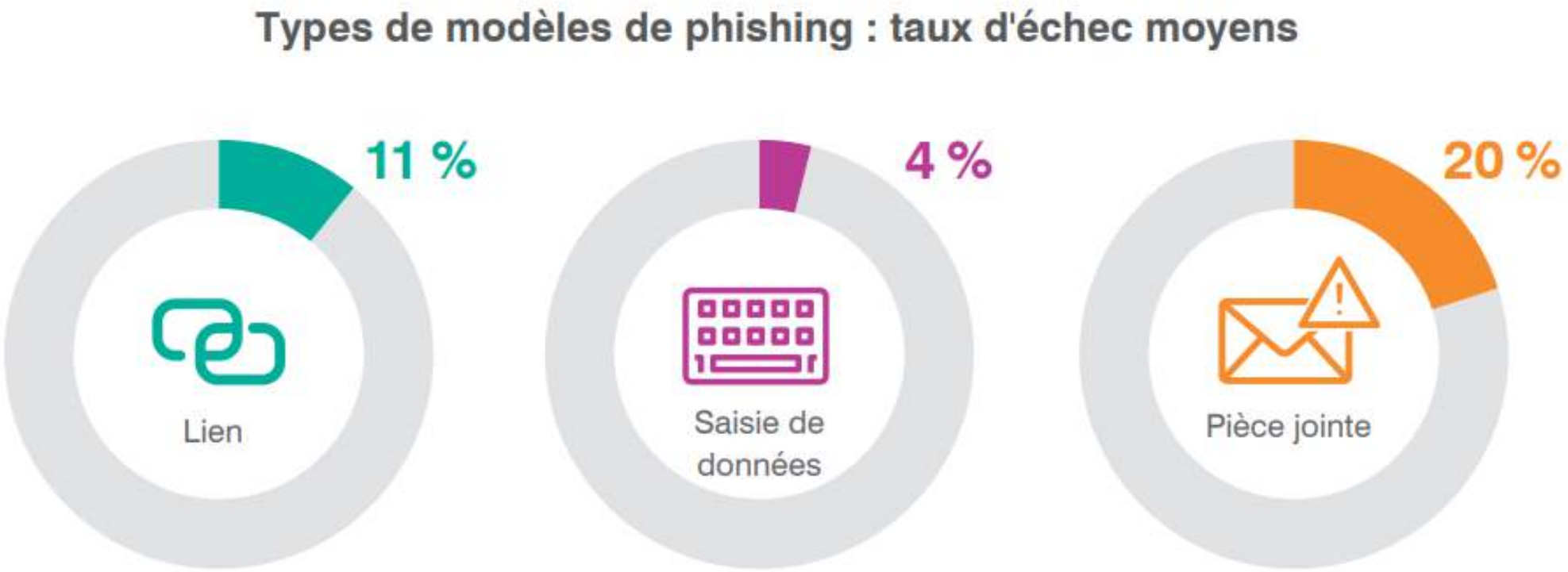
EXÉCUTION DU CODE DES CYBERCRIMINELS À LEUR PROFIT



COMMUNICATION DES IDENTIFIANTS AUX CYBERCRIMINELS

TRANSFERT DE FONDS OU DE DONNÉES AUX CYBERCRIMINELS

Exécution du code du cybercriminel

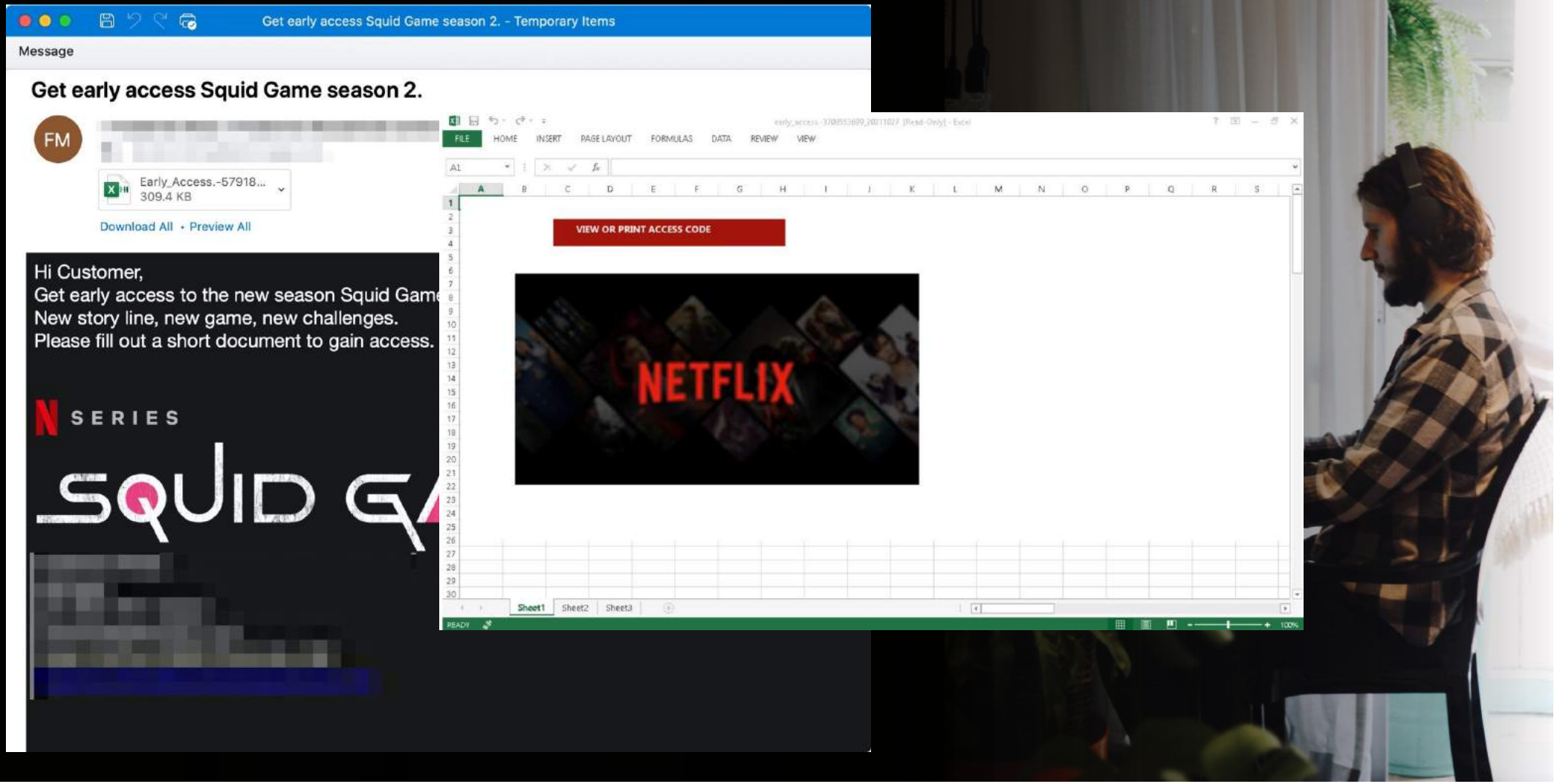


1 utilisateur sur 5 est susceptible d'interagir avec une pièce jointe non sollicitée

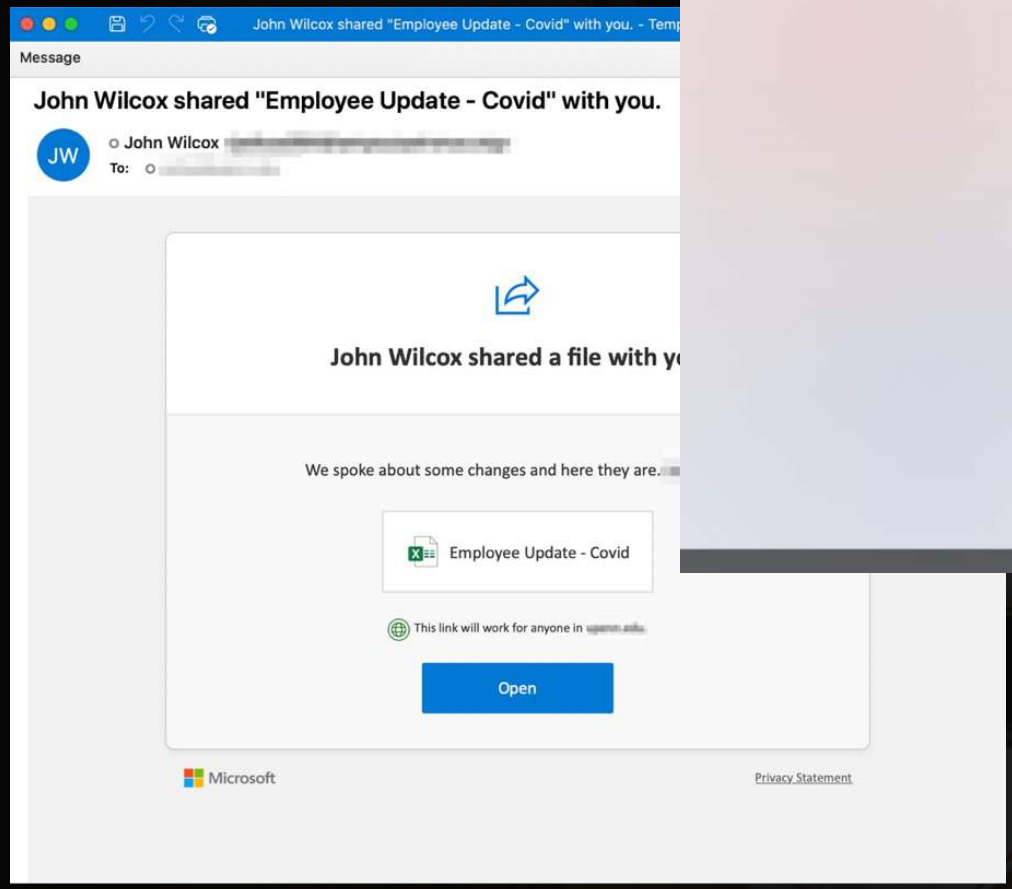
proofpoint.

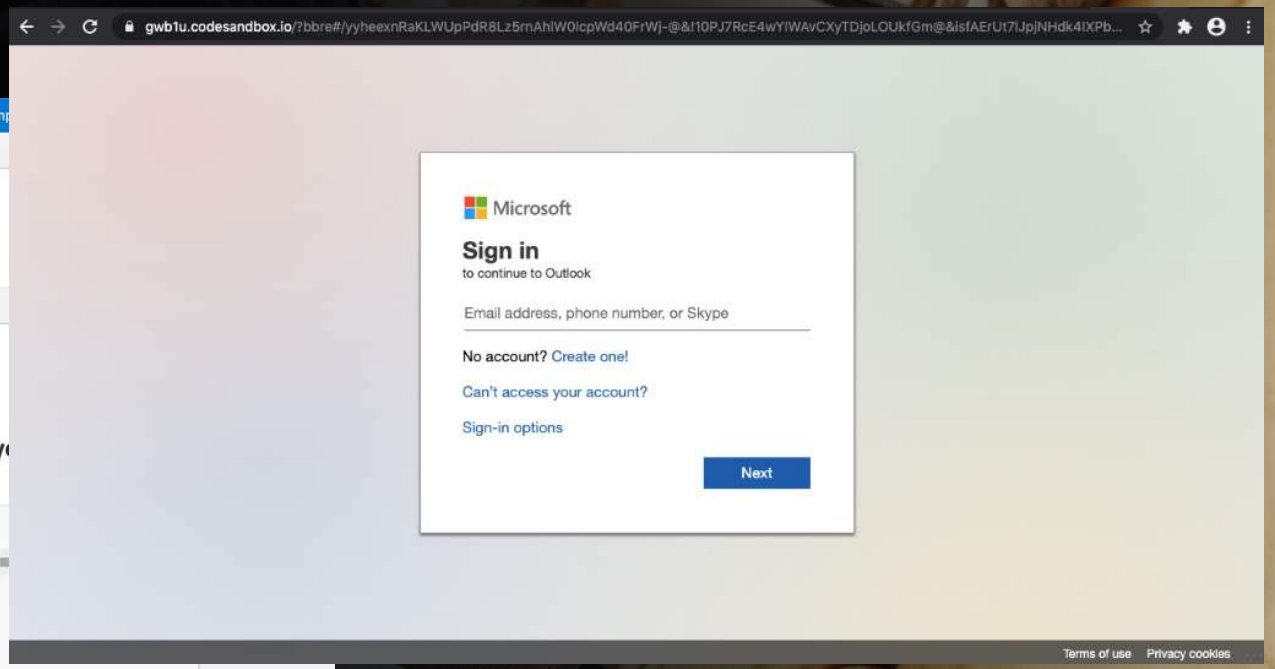
* Source : Rapport State of Phish 2022 de Proofpoint

Exécution du code du cybercriminel



Communication des identifiants

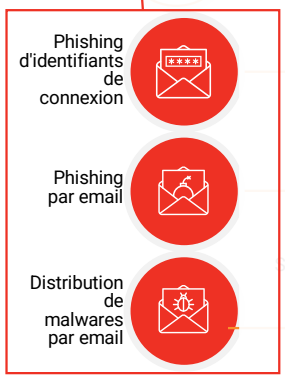




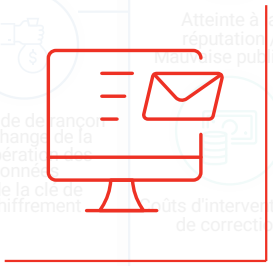
Tout commence par un email de phishing

Anatomie d'une attaque de ransomware

Accès initial	Consolidation et préparation	Exécution du ransomware	Impact sur la cible
Le cybercriminel cherche un moyen d'infiltrer l'entreprise	Le cybercriminel tente d'accéder aux terminaux critiques et à l'interface d'administration des serveurs	Une fois tous les systèmes identifiés et infectés et les informations collectées, le cybercriminel envoie la charge virale du ransomware	Le cybercriminel vole et chiffre les données, puis demande une rançon



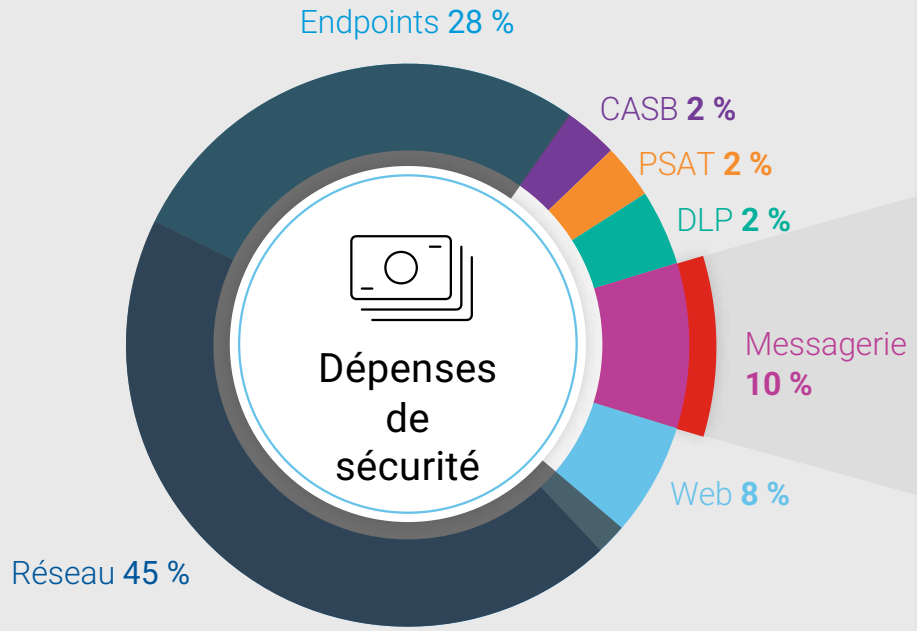
75 % des attaques de ransomwares commencent par un **email de phishing***



* Source : Unit 42 Ransomware Threat Report
(Rapport sur les ransomwares de Unit 42) de Palo Alto Networks LIEN

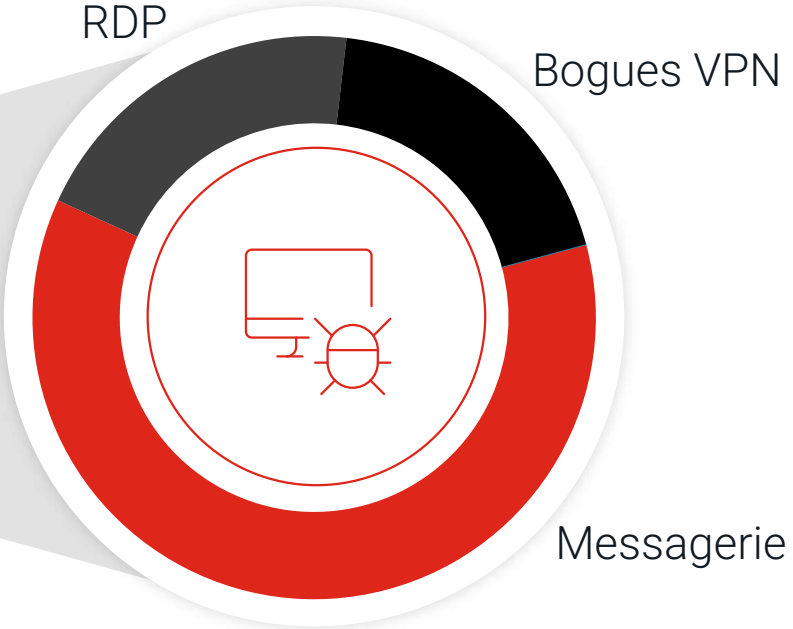
proofpoint.

Adoptez une approche préventive



Source : Gartner Information Security, Worldwide 2019-2025, mise à jour du 4e trim. 2020 (prévisions 2021)

ACCÈS INITIAL PAR RANSOMWARE



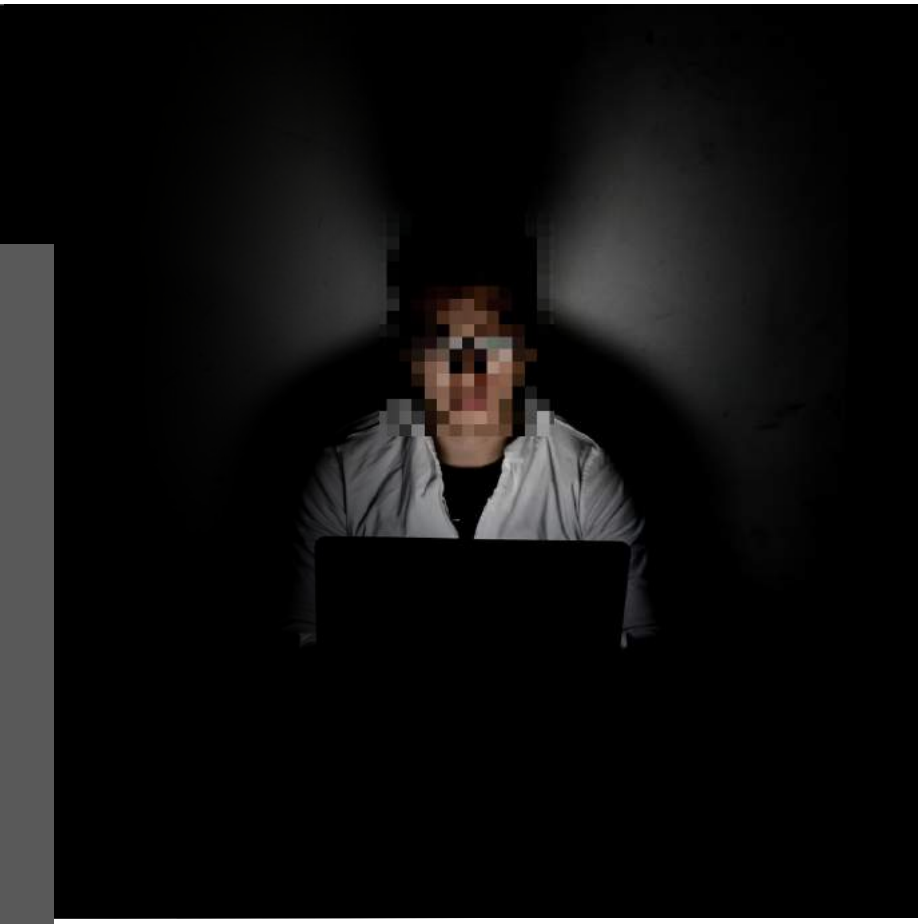
61 % des attaques de ransomwares sont transmises par email

Source : rapport DBIR 2020 de Verizon

Remontez la chaîne d'attaque en protégeant la messagerie

Nous avons infiltré votre réseau par le biais d'une attaque de **phishing**.
L'email contenant la pièce jointe malveillante a été ouvert par un collaborateur. L'utilisateur a été invité à inclure la macro du document, à afficher le contenu, à cliquer sur le lien, etc. La solution ?
Rendre impossible l'exécution d'une telle attaque !
Comment ? À vous de le découvrir…

Gang de ransomware Clop



Défense en profondeur contre les ransomwares

Proofpoint vous montre la voie

La plate-forme Proofpoint Threat Protection

Prévention en temps réel et mesures proactives :
Préparation, prévention et détection de l'infection initiale

Passerelle de messagerie sécurisée

Proofpoint Email Protection

Sandbox

Proofpoint Targeted Attack Protection (TAP)

Formation et sensibilisation à la sécurité informatique

Proofpoint Security Awareness Training

Correction après la distribution :
Reprise d'activité et prévention du déplacement latéral et de la persistance

Isolation

Proofpoint Browser Isolation

Réponse

Proofpoint Threat Response Auto-Pull

proofpoint.

https://www.proofpoint.com/sites/default/files/solution-briefs/pfpt-fr-sb-proofpoint-and-tehtris-technical-alliance.pdf

proofpoint.

FICHE SOLUTION

Alliance technique entre Proofpoint et Tehtris

<TEHTRIS>
FACE THE UNPREDICTABLE

Threat intelligence et neutralisation automatique des cybermenaces

Produits

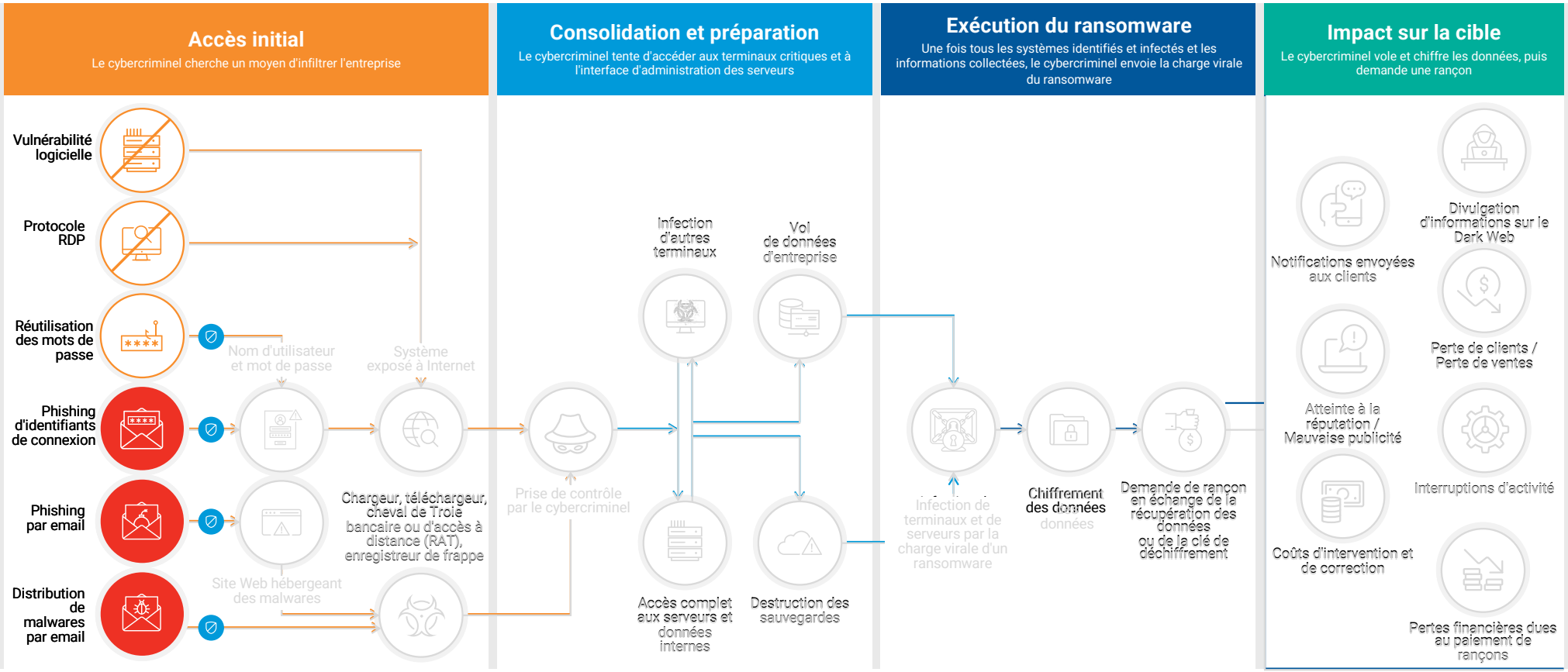
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- TEHTRIS XDR

Principaux avantages

L'email est désormais le vecteur d'infection de prédilection pour la grande majorité des cybermenaces en circulation dans le monde. Selon un récent rapport du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), par exemple, le phishing par email et le spear phishing représentent 80 % des cyberattaques ciblant les entreprises[1]. Ces attaques consistent à tromper les utilisateurs pour les inciter à divulguer leurs données personnelles ou bancaires en se faisant passer pour un tiers de confiance.

CAMPUS CYBER
PARTENAIRE

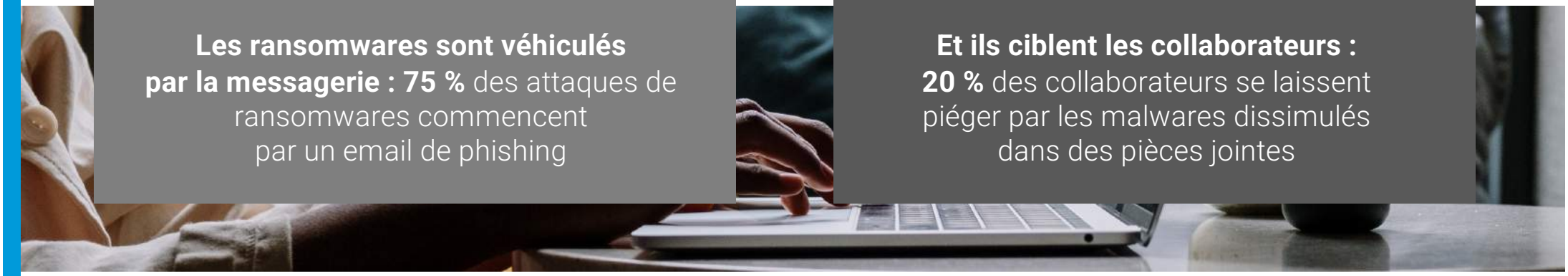
Adoptez une approche proactive pour protéger vos collaborateurs des ransomwares



proofpoint.

État idéal

Recommandations



Les ransomwares sont véhiculés par la messagerie : 75 % des attaques de ransomwares commencent par un email de phishing

Et ils ciblent les collaborateurs : 20 % des collaborateurs se laissent piéger par les malwares dissimulés dans des pièces jointes

Pour faire passer le risque d'attaque de ransomwares en dessous de la barre des 1 % :

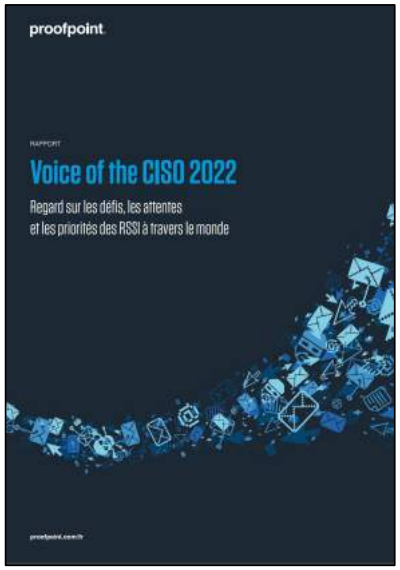
1. Réduisez le risque de menaces email
2. Protégez les services exposés à Internet
3. Corrigez les vulnérabilités et les erreurs de configuration

proofpoint.

Rapport Le facteur humain 2022

L'approche des conseils d'administration en matière de cybersécurité en 2022

Rapport State of the Phish 2022



Rapport Voice of the CISO 2022