aDvens

SECURITY FOR THE DIGITAL AGE

CYBER-ATTAQUE : LE JOUR D'APRÈS

FIC TALK 2020

1ER PURE-PLAYER FRANÇAIS DE LA CYBERSÉCURITÉ

Depuis près de 20 ans, nous accompagnons nos clients pour les aider à prendre de l'avance et faire de la sécurité un actif différentiateur.

200
Collaborateurs
Paris, Lille, Lyon, Bordeaux & Nantes

30%
Croissance annuelle

+300
Clients actifs
En France et à l'international

HISTOIRE VÉCUE…

Alerte dans un centre hospitalier !

Contexte de l'hôpital ciblé

- 13 établissements, 3000 employés, 1500 lits
- +180 000 consultations par an
- 1900 endpoints (postes et serveurs)

Sollicitation du CSIRT

- Suspicion d'infection virale
- Demande d'intervention CSIRT pour
  - ➔ Identifier le malware et l'ensemble des machines infectées
  - ➔ Déterminer si une exfiltration de données est survenue
  - ➔ Fournir les recommandations pour l'éradication

EMOTET

D’abord les banques, puis ensuite le reste du monde : un malware redoutable et considéré comme l’un des plus destructeurs et des plus coûteux…

“Emotet infections have cost SLTT governments up to $1 million per incident to remediate”

CISA CYBER+INFRASTRUCTURE

- Propagation par mail
- Exploitation de la faille EternalBlue
- Mise à jour via C&C, détection des VM, plusieurs méthodes de persistance
- **Polymorphe**

INTERVENTION DU CSIRT ADVENS

1ère vague de nettoyage
1768 Virus différents sur 1500 postes

2ème vague de nettoyage
Virus persistants sur 650 postes (EMOTET)

+ 3 serveurs avec backdoors actives…

L'apport de l'EDR

- La nature d'EMOTET rend les solutions antivirales peu-efficaces.
- Le CSIRT a déployé un EDR dans le cadre du traitement de l'incident
- **1 745 agents installés en 3h**
- Déploiement via SCCM sans impact négatif identifié

ET MAINTENANT ?

CAPITALISER

Capitaliser pour s'améliorer

- Organiser un retour d'expérience… pas uniquement sur le volet opérationnel
- Expliquer, comprendre, communiquer !

Revoir les processus et adapter l'organisation

- Vérifier ce qui a marché dans la gestion de crise
- Repenser la stratégie de cyber-résilience

REPENSER LES FONDATIONS

Durcir les systèmes de protections et les composants

- Anti-Spam, Firewall, switching, serveurs et postes

Challenger l'architecture et la sécurité de l'Active Directory

- Un élément central qu'il faut parfois renforcer après un incident

Envisager de « gros travaux » le cas échéant

- Segmentation, refonte de l'infrastructure réseau, etc.

PRÉPARER L'AVENIR

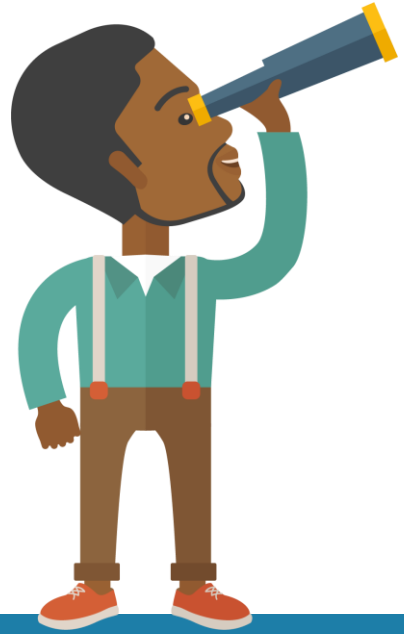
Comment tirer profit des enseignements de la crise… et des découvertes technologiques associées ?

Conserver une capacité de détection renforcée

- L'exemple d'EMOTET souligne les limites de l'antivirus traditionnel.

Se doter d'une force de réaction et de remédiation

- Nettoyer 78% du parc en quelques jours, ça peut servir…



Autant de bonnes raisons qui ont poussé le client à se doter de l'EDR utilisé par le CSIRT Advens

ZOOM : EDR-AS-A-SERVICE

Se doter d'une protection centrée sur l'attaque (et non plus sur l'équipement)

- Renverser le rapport de force entre attaquants et défenseurs

Disposer d'un service managé (et pas juste une « techno »)

- Antivirus
- Antivirus « Next Gen »
- EDR
- Intégration dans le SOC

Être accompagné en permanence en cas d'alerte

- Réactivité, proximité, efficacité

Questions / Réponses

advens.fr

SECURITY FOR THE DIGITAL AGE

Paris +33 1 84 16 30 25
Lille +33 3 20 68 41 81
Lyon +33 4 28 29 08 29
Bordeaux +33 5 35 54 82 84