Septembre 2016

Rapport sur le paysage des menaces

McAfee Labs

Vol d'informations

Types de fuites, méthodes et responsables

53 %
des compromissions sont découvertes par une personne externe à l'entité qui en est victime.

62 %
des compromissions concernent les données des clients ou du personnel.

Près de 40 %
des fuites de données impliquent un support physique quelconque.

68 %
des compromissions concernent des fuites de données devant être déclarées pour respecter les impératifs réglementaires.

Plus de 25 %
des entreprises ne surveillent pas l'accès aux données des clients ou du personnel.

Seuls 37 %
des entreprises déploient des solutions de surveillance des terminaux, y compris des activités utilisateur et des supports physiques.

Les hôpitaux en danger

Des logiciels de demande de rançon (ransomware) infectent les hôpitaux.

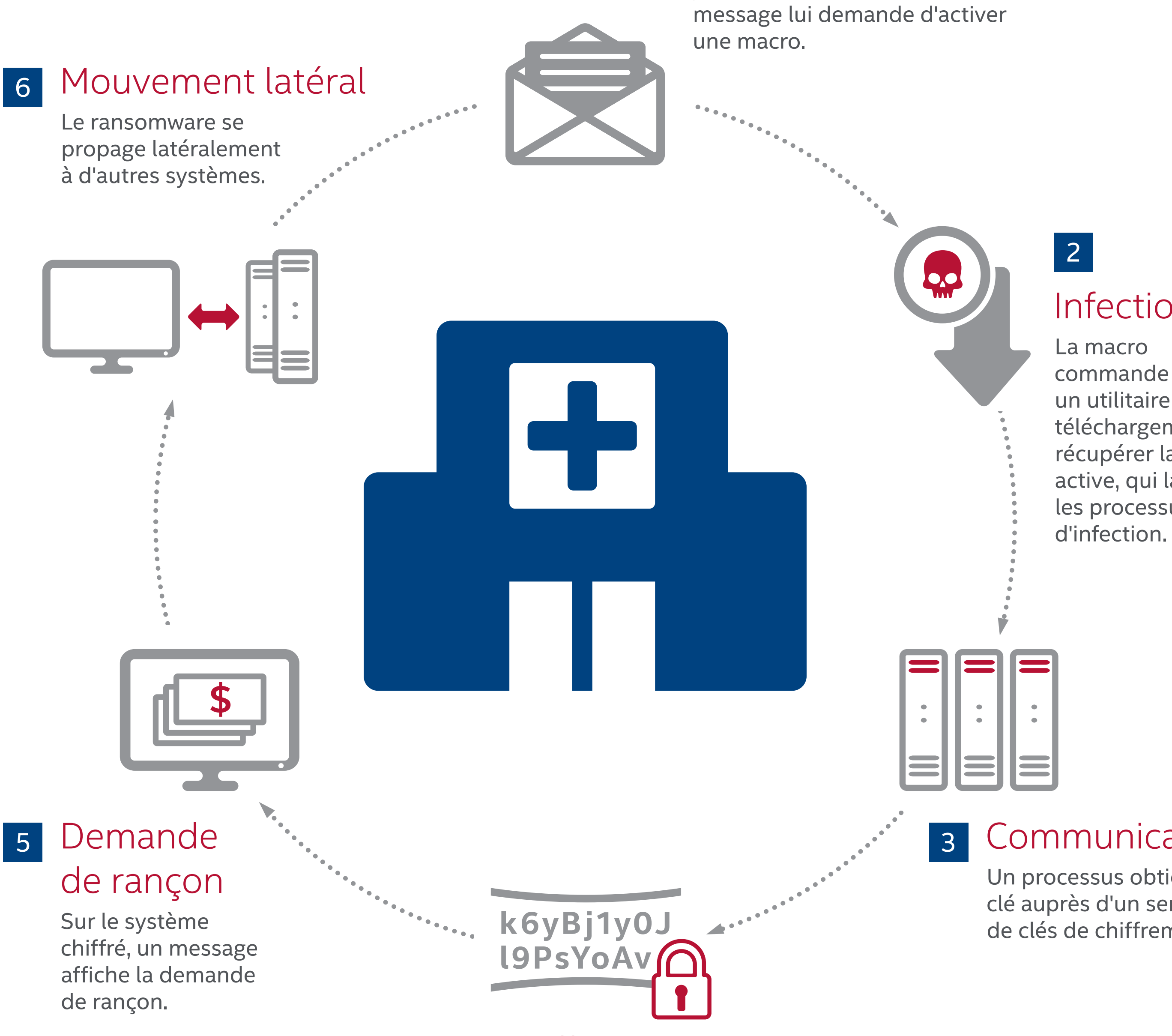
Pourquoi cet intérêt des auteurs de ransomware pour les hôpitaux ?

Anciens systèmes
Ils possèdent des anciens systèmes mal sécurisés.

Équipements médicaux
Les équipements médicaux ont une sécurité insuffisante ou inexistante.

Soins des patients
Ils ont besoin d'un accès instantané aux informations pour traiter au mieux les patients.

Étapes d'une attaque de ransomware contre un hôpital



1 **Distribution**
Un utilisateur reçoit en pièce jointe un document Word et un message lui demande d'activer une macro.

2 **Infection**
La macro commande à un utilitaire de téléchargement de récupérer la charge active, qui lance les processus d'infection.

3 **Communication**
Un processus obtient une clé auprès d'un serveur de clés de chiffrement.

4 **Chiffrement**
Les fichiers importants sont identifiés et chiffrés à l'aide de la clé.

5 **Demande de rançon**
Sur le système chiffré, un message affiche la demande de rançon.

6 **Mouvement latéral**
Le ransomware se propage latéralement à d'autres systèmes.

19 hôpitaux
Au moins 19 hôpitaux ont été infectés par des logiciels de demande de rançon aux premier et deuxième trimestres.

17 000 $
Au 1er trimestre, un hôpital californien a versé une rançon de 17 000 dollars pour restaurer ses fichiers et systèmes, après avoir connu une indisponibilité des services pendant 5 jours.

100 000 $
Intel Security a découvert qu'au 1er trimestre, une vague d'attaques liées ciblant les hôpitaux a rapporté environ 100 000 dollars en rançons.

Outils d'analyse

L'apprentissage automatique pour bloquer les attaquants

L'apprentissage automatique (machine learning) consiste à automatiser l'analyse en se servant d'ordinateurs pour enrichir les connaissances.

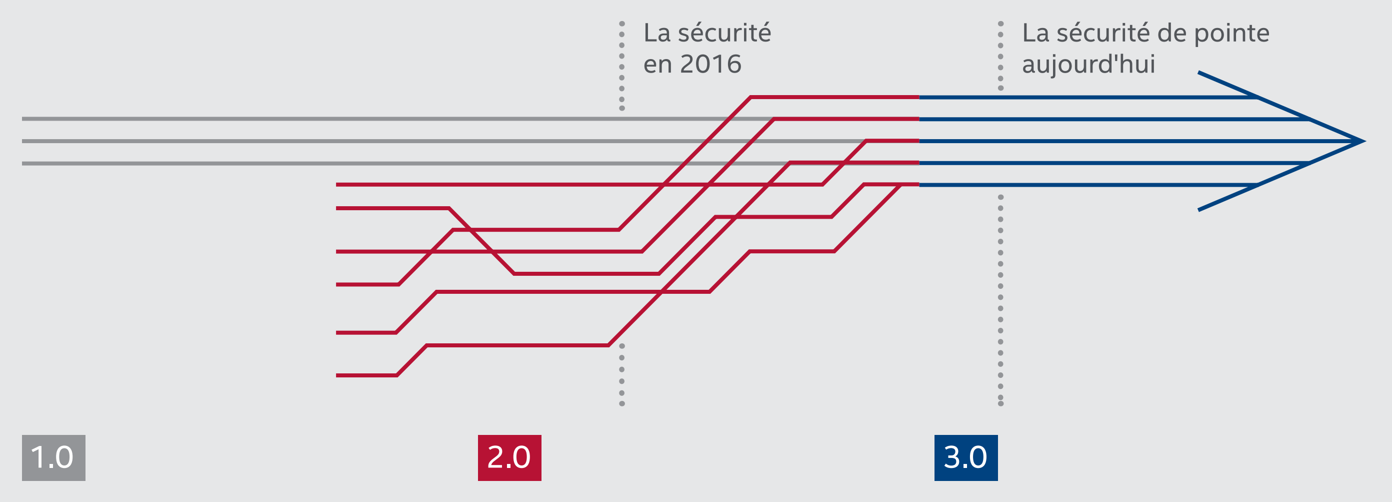
Analyse prescriptive
Recommandations à suivre face à une situation qui ne manquera pas de survenir

Analyse descriptive
Description des événements survenus

Analyse prédictive
Prévision des événements à venir

Analyse de diagnostic
Raisons expliquant les événements survenus

L'évolution de l'analyse



1.0
Solutions d'analyse 1.0
- Ensembles de données structurées, générés en interne
- Analyse descriptive et de diagnostic
- Solutions réactives mais utiles

2.0
Solutions d'analyse 2.0
- Big Data : grands volumes de données complexes, non structurées
- Données issues de sources internes et externes

3.0
Solutions d'analyse 3.0
- Utilisation de l'apprentissage automatique avec les Big Data, l'apprentissage profond et l'informatique cognitive
- Découverte et acquisition de connaissances rapides et proactives

Source : Texte adapté de l'International Institute for Analytics (IIA)

Statistiques sur les menaces

On enregistre 316 nouvelles menaces par minute, soit plus de 5 par seconde.

Logiciels malveillants (malware) — 32 %
Le nombre de nouveaux échantillons de logiciel malveillants au 2e trimestre s'élève à 41 millions, soit le 2e record historique. **La collection de logiciels malveillants de McAfee Labs a progressé de 32 % l'année dernière, pour franchir la barre des 600 millions d'échantillons**.

Logiciels malveillants sur mobiles — 151 %
Le nombre de nouveaux échantillons de logiciels malveillants découverts au 2e trimestre, près de 2 millions, constitue lui aussi un record. **Le nombre total de logiciels malveillants a augmenté de 151 % au cours de l'année dernière**.

Logiciels de demande de rançon (ransomware) — 128 %
Le nombre de nouveaux échantillons de ransomware découverts au 2e trimestre a battu tous les records, avec plus de 1,3 million. **Le nombre total de ransomwares a augmenté de 128 % au cours de l'année dernière**.

Logiciels malveillants de macro — 106 %
Les nouveaux chevaux de Troie de téléchargement sont responsables de l'augmentation de plus de 200 % des nouveaux logiciels malveillants de macro au 2e trimestre. **Le nombre total de logiciels malveillants de macro a augmenté de 106 % au cours de l'année dernière**.

McAfee Global Threat Intelligence

48,6 milliards de requêtes reçues par McAfee GTI en moyenne chaque jour

McAfee GTI

100 millions
Les protections de McAfee GTI contre les URL malveillantes ont légèrement augmenté par rapport à l'année dernière et s'élèvent à **100 millions par jour au 2e trimestre**.

104 millions
Les protections de McAfee GTI contre les fichiers malveillants ont baissé de **77 % par rapport à l'année dernière et s'élèvent à 104 millions par jour au 2e trimestre**.

30 millions
Les protections de McAfee GTI contre les programmes potentiellement indésirables ont baissé de **83 % par rapport à l'année dernière et s'élèvent à 30 millions par jour au 2e trimestre**.

29 millions
Les protections de McAfee GTI contre les adresses IP dangereuses ont connu l'augmentation la plus élevée de ces deux dernières années et s'élèvent à **29 millions par jour, soit une augmentation trimestrielle de 128 %**.

Rapport de McAfee Labs sur le paysage des menaces — Septembre 2016

Pour obtenir le rapport complet : www.mcafee.com/September2016ThreatsReport.

Intel Security

© 2016 McAfee, Inc.
912_0816_info_sept-2016-quarterly-threats