Cyber-sécurité : comment le secteur de santé est attaqué

Dans son rapport « Spotlight » sur les menaces informatiques ciblant le secteur de la santé « *, Vectra confirme l'exposition de l'écosystème médical aux cyberattaques.

La cause ? » Une surface d'attaque qui s'est considérablement élargie, avec la croissance du nombre d'objets connectés (IoT) utilisés, de réseaux non partitionnés, de faibles contrôles d'accès, et de la dépendance à des systèmes vieillissants. Les vulnérabilités en résultant sont exploitées par des cybercriminels pour voler des informations personnelles, des informations médicales protégées, et pour perturber le fonctionnement de services médicaux. » explique le rapport.

Voici les 5 principaux enseignements à retenir.

1- Les attaquants utilisent des tunnels HTTPS pour cacher leurs communications C&C (utilisées pour commander une attaque à distance).
Cette méthode est la plus utilisée dans le cadre d'attaques qui ciblent les organismes médicaux. Elle repose sur une communication externe impliquant de multiples sessions sur de longues périodes de temps donnant ainsi l'impression de n'être qu'un trafic web chiffré tout à fait normal.

2- Les attaquants utilisent également couramment des tunnels DNS cachés pour dissimuler l'exfiltration de données des réseaux des structures de santé qu'ils ciblent.
D'autres comportements compatibles avec l'exfiltration de données peuvent, également, être causés par des outils informatiques et de sécurité utilisant la communication DNS.

3- Une fois infiltrés, les attaquants procèdent à la reconnaissance des réseaux, via des scans Darknet internes et l'analyse de comptes Microsoft Server Message Block (SMB).
Les scans Darknet internes se déroulent lorsque des périphériques hôtes internes recherchent des adresses IP internes qui n'existent pas sur le réseau. De leur côté, les analyses de comptes SMB se produisent lorsqu'un périphérique hôte utilise rapidement plusieurs comptes via le protocole SMB qui est généralement utilisé pour le partage de fichiers.

4- Le ransomware, en baisse dans le secteur médical : de nombreuses organisations en ont été victimes ces dernières années, mais la tendance du ransomware est à la baisse sur la période du rapport (2ème semestre 2018). Pour un hôpital, il demeure tout de même essentiel de détecter ces attaques avant que les fichiers ne soient chiffrés et que toutes les opérations cliniques ne soient interrompues.

5 – Les attaques par Botnet sont opportunistes et n'ont pas de cibles privilégiées : bien qu'elles persistent partout, leur taux d'occurrence dans le secteur de la santé est inférieur à celui d'autres industries.

*Le « Spotlight Report on Healthcare » se base sur les observations et données d'un rapport plus global de Vectra mené auprès de 354 entreprises dans 8 industries différentes, parmi lesquelles la santé.