AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Plan d’action préventif pour réduire le risque d’une compromission massive de domaines Windows et de sauvegardes en cas d’attaques par rançongiciel

CERT Santé

Statut : Validé | *Classification : Publique* | *Version : 1.3*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1 CONTEXTE

Depuis décembre 2020, plusieurs structures de santé ont subi des attaques par rançongiciel qui ont provoqué, pour certaines d'entre elles, un impact majeur sur la continuité de leurs activités. L'ensemble des systèmes Windows a été compromis et les sauvegardes ont été supprimées, entrainant des pertes de données irréversibles.

Pour la plupart de ces établissements, l'attaquant est entré dans le système d'information (SI) à partir d'un accès VPN, ce qui lui a permis de contourner les mécanismes de protection des postes de travail (antivirus, EDR, proxy, …). Il exploite ensuite une vulnérabilité (ex : faille de sécurité sur les contrôleurs du domaine) pour obtenir un accès administrateur du domaine. Une fois l'accès obtenu, il supprime les sauvegardes et déploie l'outil de chiffrement des machines du parc. Ces actions sont réalisées avec des outils légitimes (disponible sur étagère ou même Microsoft : psexec, bitlocker), ce qui permet de rester sous les radars des outils de sécurité qui assimilent ces actions à de l'administration « courante ».

Le CERT Santé a constaté que de nombreuses structures de santé n'ont pas mis en place les mesures préventives permettant de limiter les conséquences de ce type d'attaque. Ce plan d'action préventif propose de renforcer la sécurité de 5 points stratégiques du système d'information (SI) d'une structure : système de sauvegarde, système de gestion des environnements, administration des systèmes, l'accès à distance par VPN et le proxy. L'ensemble de ces mesures doit permettre de limiter l'impact d'une attaque par rançongiciel et ralentir la progression de l'attaquant sur le SI.

Attention, ces mesures ne constituent pas à elles seules une protection suffisante de votre SI contre l'ensemble des menaces et il est important de vous inscrire dans une démarche de durcissement et d'amélioration de la sécurité en profondeur sur le long terme.

Pour rappel, une fiche de prévention est disponible pour vous aider à mettre en place les mesures de protection contre les maliciels : https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiche_Maliciel_P_RSSI.pdf .

2 PLAN D'ACTION

Ces actions sont présentées par ordre de priorité de mise en œuvre et peuvent être réalisées en parallèle.

2.1 SAUVEGARDE(S) ET HYPERVISEUR(S)

Objectif de l'action : si les contrôleurs du domaine ou un compte à privilège venaient à être compromis, il ne doit pas être possible d'altérer les sauvegardes, ni les snapshots et machines virtuelles sur l'hyperviseur.

Actions à très court terme :

- Si possible avoir des sauvegardes déconnectées du réseau (exemple : bandes) à condition qu'il soit simple de les restaurer.
- L'authentification pour accéder à l'interface d'administration de l'hyperviseur et du serveur de sauvegarde ne doit pas être lien avec l'Active Directory (AD), et si possible privilégier une authentification à deux facteurs.
- Si le système qui héberge votre hyperviseur et/ou votre serveur de sauvegarde est sous Windows alors il ne doit pas être intégrée au domaine AD.
- Dans les deux cas du dessus, utiliser uniquement des comptes locaux avec des mots de passe uniques et forts.
- Restreindre l'accès aux composants d'administration aux seules adresses IP des rebonds ou postes autorisés (que cela soit l'interface d'administration de la sauvegarde/hyperviseur ou l'administration du serveur qui l'héberge).
- L'utilisateur qui lance l'agent de sauvegarde sur les différentes machines ne doit pas avoir d'accès sur l'interface d'administration de l'application de sauvegarde.
- Veiller à ce qu'ils soient à jour des patchs de sécurité.

Impact de mise en œuvre : il ne devrait pas y avoir d'impact sur les services au-delà du changement de mode de connexion sur l'hyperviseur et le serveur de sauvegarde.

Exemple de déploiement : https://forums.veeam.com/veeam-backup-replication-f2/pen-test-and-off-domain-backup-infrastructure-t63213.html

2.2 MISE A JOUR CONTRE LES FAILLES ACTIVEMENT EXPLOITEES

Objectif de l'action : corriger les failles de sécurité les plus exploitées par les attaquants pour monter en privilège sur le SI.

Actions à très court terme :

Nous recommandons que l'ensemble des vulnérabilités suivantes soient patchées dans l'ordre de priorité suivant :

1. Contrôleurs de domaine ;
2. Serveurs critiques (Exchange, WSUS, AV..) ;
3. Autres serveurs Windows ;
4. Postes des administrateurs ;
5. Postes utilisateurs.

A minima, les vulnérabilités suivantes doivent être patchées :

- Sur les contrôleurs de domaine : Zerologon - https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-020/
- Sur les contrôleurs de domaine : Vulnérabilité SIGRed affectant les DNS Windows - https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-005/
- Sur l'ensemble du parc Windows : Eternal Blue (MS17-010) - https://support.microsoft.com/fr-fr/topic/comment-v%C3%A9rifier-que-la-mise-%C3%A0-jour-ms17-010-est-install%C3%A9e-f55d3f13-7a9c-688c-260b-477d0ec9f2c8
- Sur l'ensemble du parc Windows : Spouleur d'impression (CVE-2021-36958) - https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-014/
- Sur les serveurs exchange : HAFNIUM (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) - https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-004/
- Sur les serveurs exchange : patch avril 2021 - https://techcommunity.microsoft.com/t5/exchange-team-blog/released-april-2021-exchange-server-security-updates/ba-p/2254617
- Sur les serveurs exchange : ProxyShell (août 2021) - https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-017/

De plus, il est impératif de maintenir à jours les antivirus (logiciel et signatures). Il est important de ne pas négliger les alertes antivirus remontées sur les serveurs, ces événements n'ont rien d'anodins.

Pour rappel, il est recommandé de faire un instantané (snapshot) de votre machine virtuelle avant toute mise à jour pour être en capacité de restaurer l'environnement en cas de problème.

Impact de mise en œuvre : réaliser ces actions sur des horaires adaptés.

2.3 SEGMENTATION DES SERVICES D'ADMINISTRATION WINDOWS

Objectif de l'action : rendre obligatoire le respect du bon cheminement d'administration du parc, afin de ralentir l'attaquant cherchant à se propager dans le parc même s'il obtient un compte à privilège.

Actions à très court terme :

- Définir les machines qui ont le droit d'administrer les contrôleurs de domaines et les serveurs socles à risque : il peut s'agir des postes des administrateurs ou de préférence d'un rebond d'administration RDP (en dehors de l'AD, durci, et si possible avec une authentification à deux facteurs).
- Configurer les contrôleurs de domaine pour n'accepter que des connexions en RDP en provenance du rebond d'administration ou postes d'admin.
- Configurer par GPO l'ensemble des serveurs Windows et postes de travail Windows pour n'accepter que des connexions en RDP/wmi/powershell/psexec en provenance du rebond d'administration ou postes d'admin ainsi que des contrôleurs de domaine (sauf pour la partie RDP).
- Si vous n'utilisez pas le powershell à distance, et/ou psexec (partage administratif) sur votre parc alors désactiver les services sur l'ensemble des machines concernées.

Vous trouverez l'ensemble des commandes GPO détaillées pour réaliser ces actions, ainsi que des informations complémentaires dans la documentation de "Fireeye - Stratégie de protection et de confinement des ransomwares" : https://www.fireeye.fr/content/dam/fireeye-www/regional/fr_FR/current%20threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf .

Attention pour que cette politique soit efficace sur les postes, il est important que vos utilisateurs ne soient pas administrateur local de leur poste.

Si vous souhaitez aller plus loin, nous vous conseillons l'application du plan de modernisation rapide (RAMP) "phase 1" basé sur les recommandations Microsoft : https://secframe.com/ramp/phase1/ .

Impact de mise en œuvre : pas d'impact identifié sur les services.

2.4 ACCES VPN

Objectif de l'action : Limiter les possibilités d'accès au SI par le compte VPN même si un attaquant obtient un identifiant/mot de passe valide, tout en permettant d'être alerté d'une connexion suspecte sur le VPN afin de pouvoir agir rapidement.

Actions à très court terme :

- Veiller à ce qu'ils soient à jour des patchs de sécurité.
- Mettre en place un script afin de surveiller (en temps réel) les authentifications réussies sur votre VPN à partir d'adresses IP publiques venant de l'étranger (vous pouvez utiliser notre outil : https://github.com/cybersante/Blacklist_tools/tree/master/checkbl avec l'utilisation de crontab sur les logs VPN). Attention, il ne s'agit pas de bloquer les accès aux adresses IP venant de l'étranger car l'attaquant finirait par passer par une adresse française et vous n'auriez rien vu !
- Mise en place d'une authentification à deux facteurs.

Impact de mise œuvre : aucun impact sur le script d'alerte et la mise en place d'une authentification à deux facteurs peut être importante si vous avez un grand nombre d'utilisateurs (VPN).

2.5 PROXY WEB SORTANT

Objectif de l'action : rendre difficile la prise en main totale par un attaquant à distance d'une machine compromise sur le réseau interne.

Actions à très court terme :

- Mettre en place un proxy web sortant. Dans le cas d'une première mise en œuvre, il est préconisé de mettre un proxy dans le mode "transparent" afin de pouvoir l'intégrer très rapidement sans impact sur la configuration du parc.
- Activer sur le proxy la vérification des protocoles (cela sous-entend aussi que les ports en sortie sont limités à : 80, 443). Cette option va permettre de "casser" les canaux de communication que veut établir l'attaquant. L'impact de l'activation de cette option va être que l'ensemble des outils de type "prise de main à distance (RAT)" (ex: Teamviewer) ne fonctionnera plus. Cependant si des exceptions sont mis en place pour des postes ou des serveurs légitimes à utiliser ce type d'outil en sachant que cela permettra aussi à un attaquant d'utiliser cette faiblesse.
    - Il ne s'agit pas avec cette option de désactiver le chiffrement lors de connexions "https" qui utilisent le SSL/TLS. Cette option permet de regarder si les certificats de chiffrement présenté par le serveur/client sont valides ou non et donc qu'il s'agit bien de l'utilisation réel du protocole TLS/SSL.

Impact de mise en place : le proxy transparent n'a aucun impact sur le parc, seul l'activation de la vérification des protocoles peut avoir un impact sur vos outils RAT installés dans votre parc.

3 CONCLUSION

Le CERT Santé recommande de mettre en place rapidement ces actions, même si certaines peuvent demander un effort important. Cet effort et les bénéfices associés sont à évaluer au regard des moyens et des délais nécessaires pour reconstruire tout ou partie du SI en cas de destruction totale des systèmes connectés à l'AD.

De plus, ces actions ne constituent qu'une première étape dans le renforcement de la sécurité de votre SI qui doit faire l'objet d'une surveillance et d'une amélioration continue.