le cnam
Île-de-France

Rapport d'analyse

SEC102 année 2022-2023 semestre 1

Date d'examen : 28/01/2023

Nom auditeur : JOBERT

Prénom auditeur : Louis

Consignes

Note importante: ne pas modifier le format et la structure du fichier.
Les réponses peuvent être multiples et devront être séparées par une virgule

Réponse aux incidents

Veuillez décrire les étapes de la réponse aux incidents que vous suivriez dans un cas concrêt et la procédure de réponse à l'incident.

n°	Etape	Description
01-001	* Isolation *	Isoler les ordinateurs impactés et potentiellement impactés
01-002	* Evaluation *	Évaluer l'impact et appliquer un niveau de gravité
01-003	* Coordination *	Coordonner le travail à effectuer en fonction des personnes qui doivent travailler sur l'incident et leurs tâches
01-004	* Communication *	Créer des canaux de communications, ne pas hésiter à déléguer certaines tâches
01-005	* Sauvegarde *	Eviter au maximum la perte de données, effectuer des copies d'images réseau et disque
01-006	* Identification *	Identifier l'étendue de l'opération d'attaque, plusieurs mécanismes de persistance auront pû être utilisés
01-007	* Objectif *	Identifier l'objectif final de l'attaque, le but de cette backdoor
01-008	* Modification *	Examiner les modifications apportées par le malware sur les ordinateurs
01-009	* Théorisation *	Développer des théories relatives aux motifs de l'incident, et réaliser des expériences pour prouver ou réfuter ces théories
01-010	* Utilisation *	Utiliser les outils existants déjà déployés avant d'essayer de déployer et d'apprendre un nouvel outil lors de la récupération (éviter des pertes de temps)
01-011	* Réponse *	Passer en revue les processus de réponses aux incidents pour identifier et résoudre les lacunes trouvées pendant l'incident

Analyse mémoire RAM

Synthèse de l'analyse

n°	Question	Réponses
02-001	*Date de compromssion (eg.YYYYMMDD-HH:MM:SS)*	20140429-20:54:04
02-002	*Vecteur de compromssion*	La clef USB
02-003	*Vulnerabilités exploitées (eg. CVE-YYYY-XXXX)*	CVE-2009-4324
02-004	*Profil d'analyse*	–profile=WinXPSP2x86
02-005	*PID du processus vérolé*	852
02-006	*IP du CC*	169.254.154.85:3460
02-007	*Nom des fichiers illégitimes (sous la forme de name.exe ou name.dll)*	smss.exe , csrss.exe , wuauctl.exe
02-008	*Port utilisé par le malware*	3460
02-009	*PID du parent du malware*	660
02-010	*Nombre de page RWX du malware*	55

Méthodologie d'analyse

Veuillez décrire les étapes de vos analyses qui vous ont permis de trouver des preuves numériques.
Veuillez ne pas dépasser une page d'écriture.

Détection du système d'exploitation et version de l'image mémoire. Exécution de la commande suivante à l'aide de Volatility : volatility -f "SEC102 - 302 - Windows XP Target.memraw" imageinfo Ensuite savoir combien de processus étaient en cours d'exécution sur le système au moment de la capture de l'image mémoire. Exécution de la commande suivante : volatility -f "SEC102 - 302 - Windows XP Target.memraw" –profile=WinXPSP2x86 pslist Certains processus en cours d'exécution ne semblent pas être légitimes (csrss), peut-être tentent-ils de se cacher. Execution de la commande : volatility -f "SEC102 - 302 - Windows XP Target.memraw" –profile=WinXPSP2x86 psxview | grep False Il s'affiche des processus False, c'est une forte indication qu'un processus

essaie de se cacher. Les logiciels malveillants ont une structure command & control, une fois qu'ils ont infecté un système, ils doivent se reconnecter au centre de commande. Il faut examiner les connexions réseau établies par le logiciel malveillant. Execution de la commande : volatility -f "SEC102 - 302 - Windows XP Target.memraw" –profile=WinXPSP2x86 connscan Rien d'anormal de détécté. Pour voir quels programmes ont récemment été exécutés sur un système, nous avons exécuté la commande "userassist", nous avons trouvé un executable suspect " wuauctl.exe".

Cette commande nous a permis de voir l'enchainement des commandes réalisées dans le but comprendre la chronologie des actions réalisés par l'attaquant: volatility -f "SEC102 - 302 - Windows XP Target.memraw" –profile=WinXPSP2x86 userassist

1)L'attaquant a essayé d'exploiter une vulnérabilité sans succés, il essaie ensuite de tester les mots de passe Admin. il a fini par y arrivé avec le mot de passe "admin", 2)L'attaquant a lancé une opération de scan des ports ouverts et disponibles avec la commande Tcpview.exe à le 2014-04-29 21:01:17, cette commande a été lancée depuis le cmd le même jour à 20:57:24 vu avec la commade psscan 3)le PPid de la cmd est PID852 explorer.exe que l'attanquant a utilisé pour attaquer la machine depuis le port 3460 et IP 169.254.154.85. 4)Avec la commande Userassist, nous avons remarqué que l'attaquant a introduit un fichier 7-zip qui s'autodézip et libere le malware WUAUctl.exe

Nous devons vérifier ce que ce malware a fait sur le système, comme les fichiers qu'il a créés et si du code a été injecté. Exécution de la commande "malfind" et vider la sortie dans un répertoire : volatility -f "SEC102 - 302 - Windows XP Target.memraw" –profile=WinXPSP2x86 –dump-dir ~Desktop/malfind |more Cette commande affiche divers PID qui ont été infectés; nous pouvons également voir le PID 852 découvert lors de l'enquête sur la connexion réseau. La commande "malfind" a entraînée un grand nombre de fichiers des différents processus infectés par le logiciel malveillant. La sortie de cette commande affiche divers PID qui ont été infectés ; nous pouvons également voir le PID ID 856 que nous avons découvert plus tôt lors de notre enquête sur la connexion réseau. Analyse des paquets via Virustotal dont le pid est 852 : découverte du malware Backdoor:Win32/Darkmoon.E (appelation Microsoft) Lien sur le CVE en question : https://www.cvedetails.com/cve/CVE-2009-4324.

Analyse dump disque dur

Synthèse de l'analyse

n°	Question	Réponses
03-001	*Date de compromssion (eg.YYYYMMDD-HH:MM:SS)*	2012-10-12 22:47:08
03-002	*Vecteur de compromission*	clef USB
03-003	*Nom du compte illégitime*	HACKER, Daili
03-004	*Type de partition*	NTFS
03-005	*Chemins du malware (eg: C:\Users\temp) :*	C:\Winddows\system32
03-006	*Clés de registre modifiées :*	
03-007	*Adresse Ip de la Machine*	169.254.189.70
03-008	*Numéro du volume de stockage de la provenance du malware (de type* xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	-11e2-93e7-0800278e4279
03-009	*Nom du fichier source du malware*	wuauctl.exe
03-010	*Nom et numero de série des supports amovibles connectées*	11092803010028

Méthodologie d'analyse

Veuillez décrire les étapes de vos analyses qui vous ont permis de trouver des preuves numériques.
Veuillez ne pas dépasser une page d'écriture.

1/Lancement de l'analyse du fichier .vmdk via Autopsy, 2/Etude des differents processus, recherches du fichier identifié dans l'analyse mémoire,

- Récupération du hash du programme suspect et analyse dans virustotal.com,
- Recherche des CVE associées à cette menace,
- Découverte de deux comptes user suspects: Hacker et Daily creer depuis une clé USB.

3/Lancement de l'analyse du fichier via plaso,

- `Execution de la commande psteal et recupreation du résultat dans un fichier .csv,`
- `Tri des événements en fonction des dates identifiées dans l'analyse mémoire,`

4/Etude de la timeline et de la cohérence de chronologie des événements, 5/Mise en corrélation avec des résultats de l'analyse mémoire, 6/Rédaction du compte rendu,

Analyse du malware

Synthèse de l'analyse

n°	Question	Réponses
04-001	*Nom du malware*	Backdoor.Darkmoon , Win32:Agent-TZE [Trj]
04-002	*Nom du fichier malveillant*	
04-003	*Classification*	Trojan de type Backdoor
04-004	*Système d'exploitation (eg. Windows 8, Windows 2000, …)*	WinXPSP2 , WinXPSP3
04-005	*Architecture (x86, x86_64, arm32, arm64)*	x86
04-006	*Méthode de persistence*	Backdoor
04-007	*Password de connexion*	admin
04-008	*MD5 hash*	Win32:Agent-TZE [Trj] : 3197943eaf6561664199383c188a1e64 , Backdoor.Darkmoon : 670fbd8374cd84389982162db70acde1
04-009	*Date de compilation (format YYYYMMDD-HH:MM:SS)*	
04-010	*Fonctionalités*	Backdoor, élévation de privilèges, connexion réseau distance, malware de type botnet, obfuscation, mécanisme de persistance

Méthodologie d'analyse

Analyse du .vmdk dans Virustotal : Nous avons trouvé le premier Trojan Win32:Agent-TZE [Trj] Avec Volatility nous avons utilisé la commande Malfind, puis nous avons copier les captures de paquets réseaux pour ensuite les analyser, puis analyse des paquets avec Virustotal, le malware Backdoor.Darkmoon a été détecté.

Veuillez décrire les étapes de vos analyses qui vous ont permis de comprendre le fonctionnement du malware. Avec Autopsy nous avons effectué une timeline, on

voit clairement que le malware est introduit par un support physique (clé USB) après avoir changé les droits

Veuillez ne pas dépasser une page d'écriture.

TimeLine and conclusion

Timeline

n°	Question	Réponses
05-001	*Date de dépose du malware*	Selon Autopsy 2013-06-30 14h58m54s
05-002	*Date de la première execution du malware*	Selon Autopsy 2013-06-30 14h58m54s
05-003	*Date d'exécution du processus vérolé*	Selon Volatility 2013-07-03 22h17m07s

Conclusion

n°	Question	Réponses
06-001	*Sévérité (faible, moyenne, élevée)*	élevée
06-002	*Nombre de machine(s) infectée(s)*	deux
06-003	*Système d'exploitation affecté*	WinXPSP2
06-004	*Type de malware (eg:keylogger)*	Trojan
06-005	*Type d'attaque (eg:phishing)*	Backdoor
06-006	*Nom de la souche du malware*	Ce malware aurait été déposé par un autre malware
06-007	*IOC*	Périmètre : Lister les ports libres et utilisés, point de transmission : créations de nouveaux processus, persistance : présences de tâches et de paramètres indiquant qu'un point de terminaison est compromis, connexion : vers un serveur distant pour télécharger des fichiers infectés utilisés dans l'attaque, mouvement latéral : élévation de privilèges et utilisation des droits Admin pour executer des processus normalement bloqués, accès aux données : activité sur la machine en dehors des heures de travail habituelles

Veuillez décrire les recommandations que vous proposeriez

Administrateurs :

MAJ des antivirus, Analyse de l'ensemble du parc informatique, des serveurs, MAJ logiciel antimalware + analyse complete, Formatage machine infectee + nouvelle image, Changer l'integralite des mdp admin, Désactiver les logiciels comme psexec qui permettent l'élévation de privileges, GPO plus restrictives, …

Machines utilisateurs :

Mise a jour des systemes en Win10, Bloquer les sites dangereux ou certains contenus (Réseaux sociaux, services type Dropbox, WeTransfer), …

Utilisateurs :

Sensibilisation du personnel sur les menaces informatiques, Appliquer les recommandations et bonnes pratiques de l'ANSI, …

Annexes

Analyse de la mémoire vive

Analyse de disque

Analyse du malware

```
If you need copy and paste code
Enter code here
Else remove line in back quotes
```