ABDOUL-AZID Amine

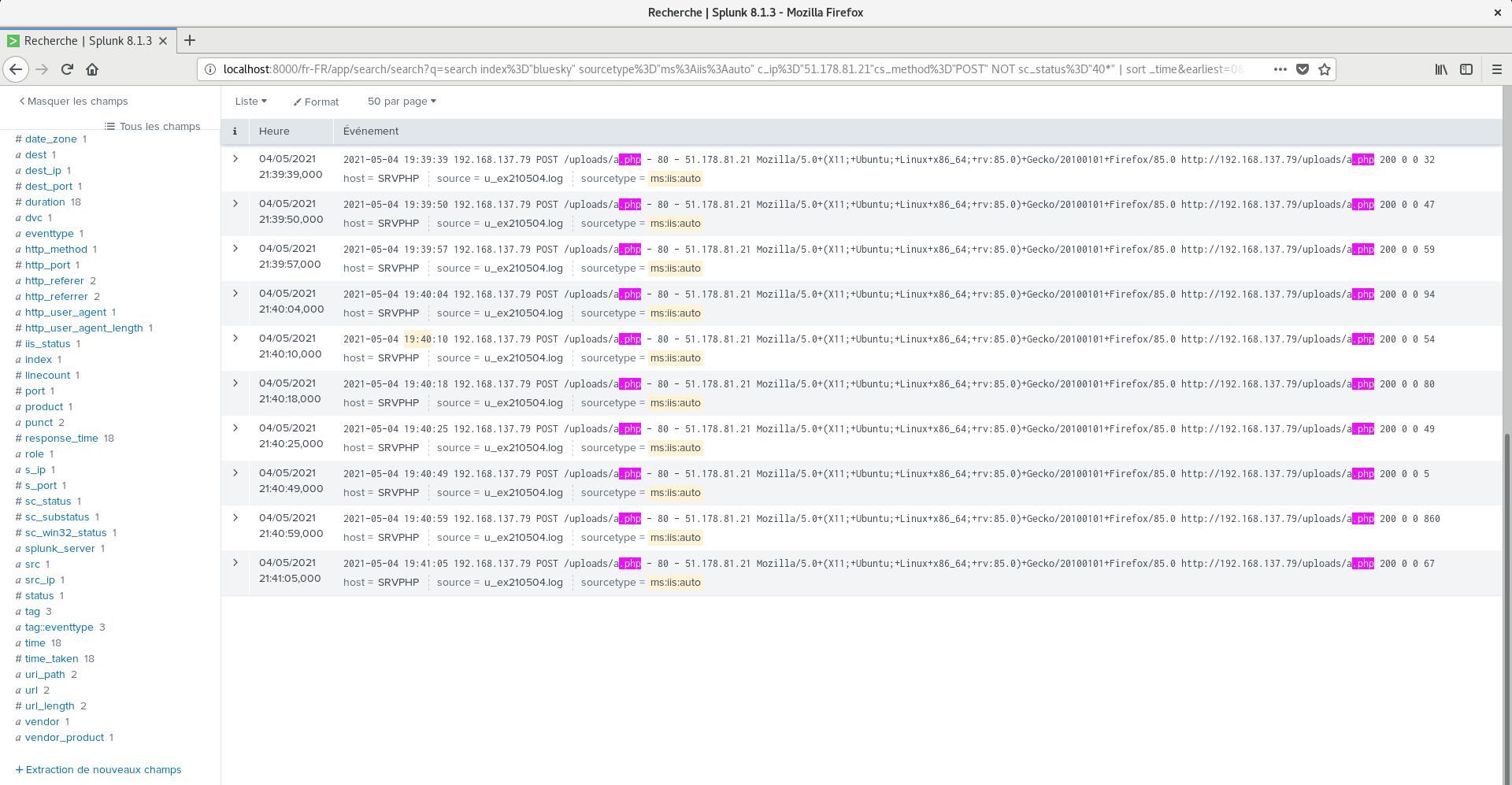
SENE Martial

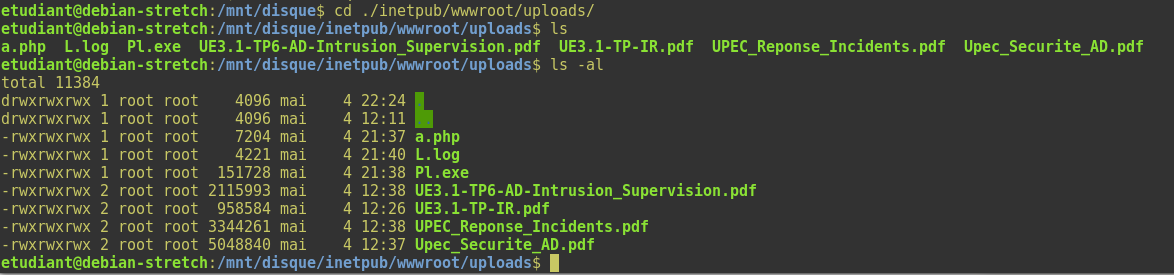
SARAVANANE Kavirajan

**TP Réponse à Incident de sécurité**

Synthèse 2

Le fichier créer par l’attaquant est a.php qui était stocké dans le dossier /mnt/disque/inetub/wwwroot/uploads.





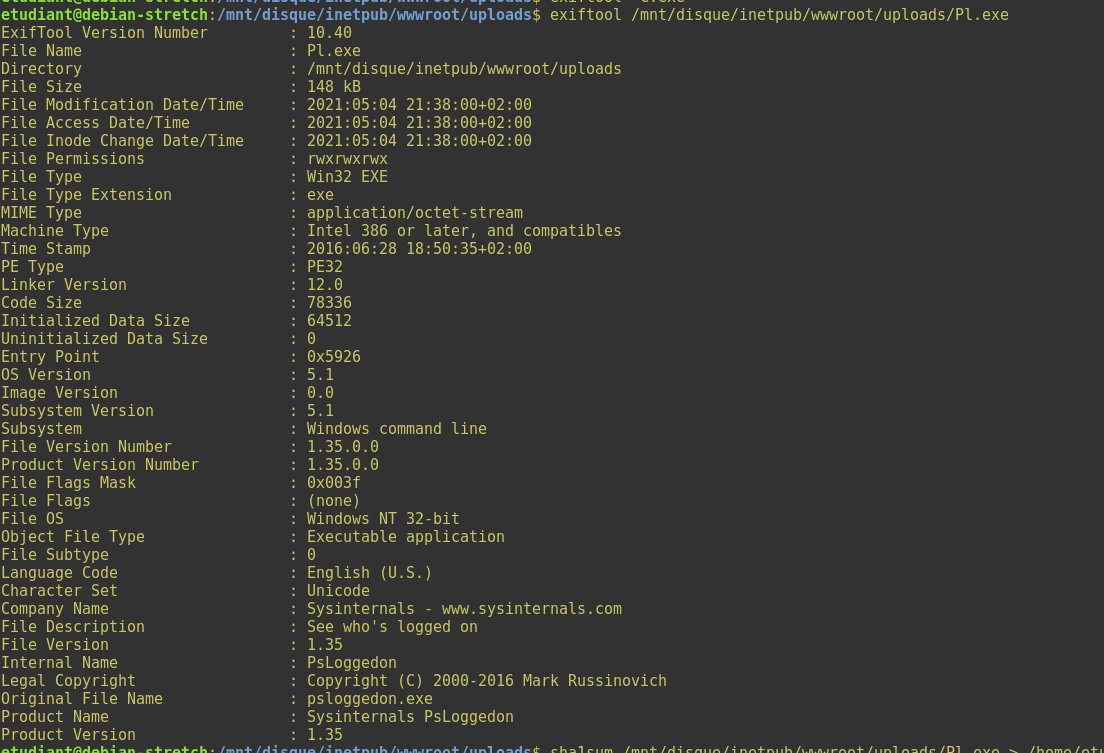
Le code permet d’exécuter des commandes en tant que compte utilisateur du server php

Ce type de fichier est un marqueur et une vulnérabilité (webshell).

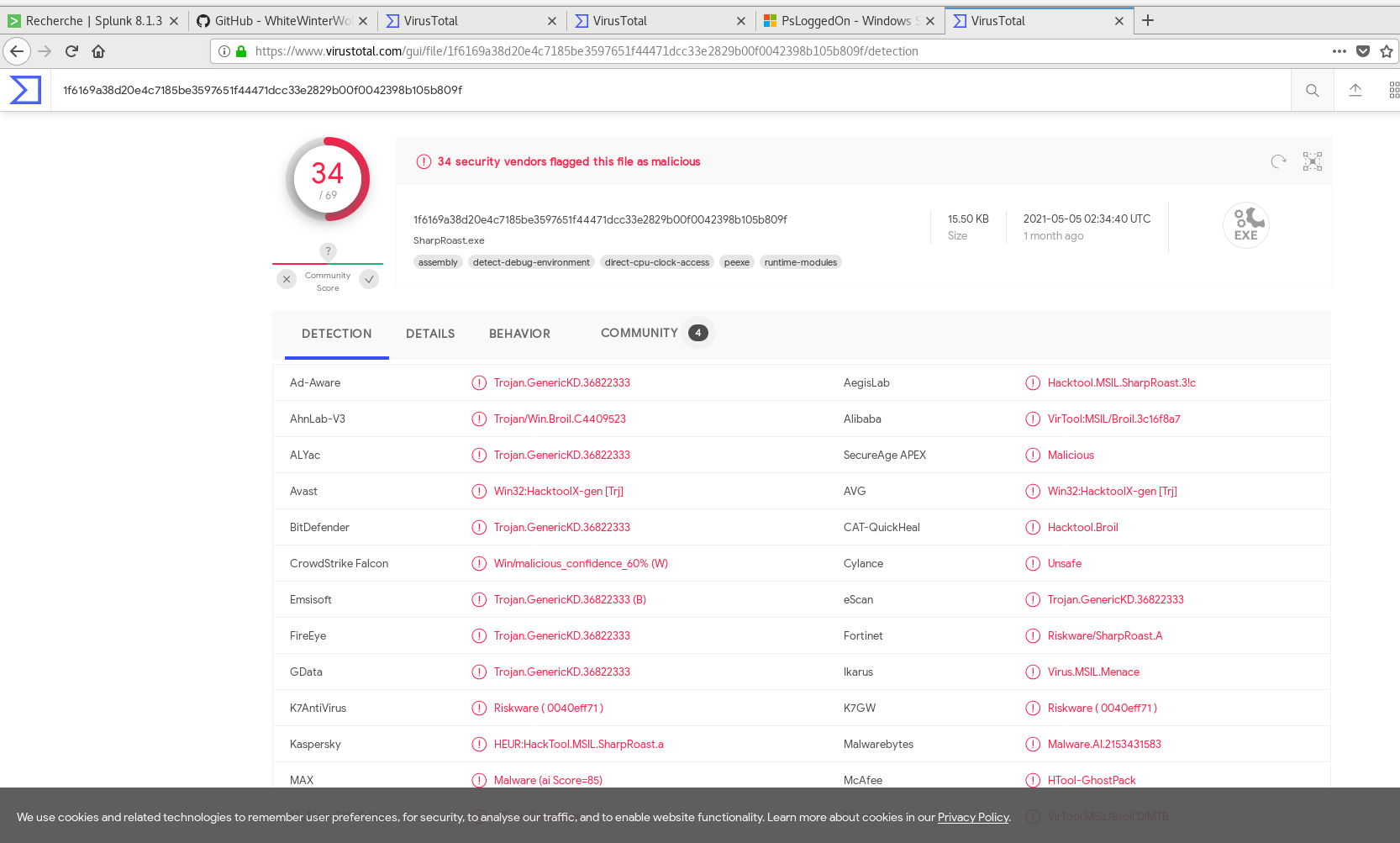
Dans le fichier upload.php, nous observons que seul des fichier PHP sont censés être uploader, cependant, nous observons que le code ne test aucunement les extensions des fichiers uploader ce qui créer une vulnérabilité.

Synthèse 3

Sha1 de Ps.exe

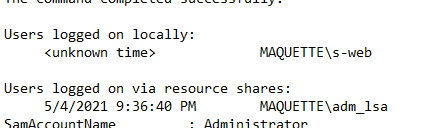






L’attaquant a utilisé le fichier pl.exe et s.exe. P.exe est utilisé via l’outil Pstools. Le s.exe utilise une faille de kerberoasting. Il liste tous les comptes avec un SPN (service principal name).

Le webshell de l’attaquant avec l’utilisateur avec s-web. L’attaquant essaye d’élever ses droits en créant un nouvel utilisateur.



Il utilise la vulnérabilité wwwolf.

Nous observons que son évaluation de privilèges a réussi grâce à l’event ID4624. L’adresse ip était de 51.178.81.21 pour passer à 51.178.81.33.

|  |  |  |
| --- | --- | --- |
| Event.EventData.IpAddress | Event.EventData.ProcessName | Event.EventData.SubjectUserName |
| 51.178.81.33 | C:\Windows\System32\svchost.exe | SRVPHP$ |

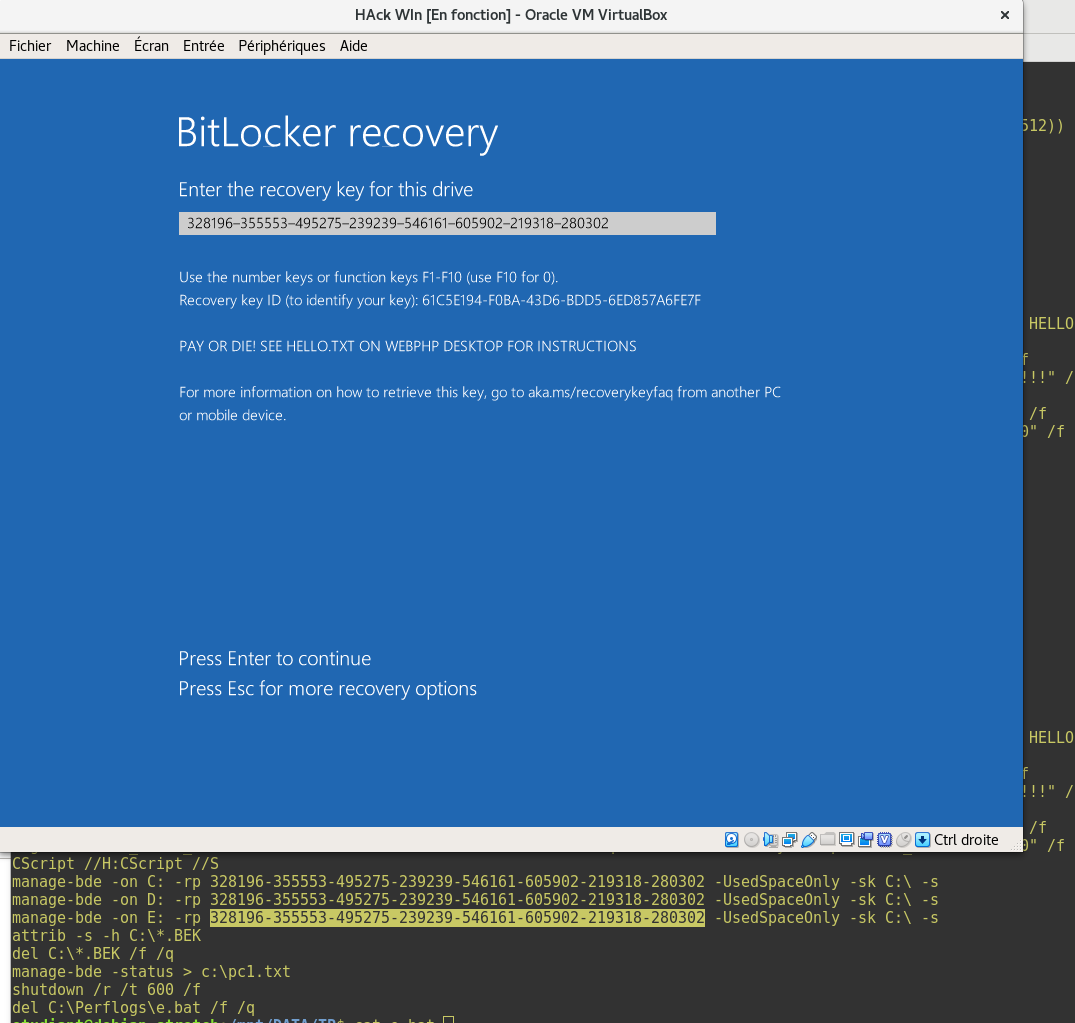
|  |  |  |
| --- | --- | --- |
| Event.EventData.TargetUserName | Event.System.Computer | Event.System.EventID |
| administrator | SRVPHP.maquette.ldap389.info | 4624 |

Pour corriger cette vulnérabilité, il faudrait interdire le SPN sur les comptes

Synthèse 4

Le moyen de déploiement utilisé est le fichier ps.exe.

Le chiffrement est compliqué a empêché car le chiffrement par BitLocker n’est pas détecté par l’antivirus. Dans le cas où le fichier aurait été supprimé proprement avec réécriture sur le disque, il aurait été compliqué de récupérer la clef.



Synthèse 5

Les tâches planifiées sont stockés dans le registre en lançant un script PowerShell et allant chercher le code dans un registre contenant un Shell code empire

Backdoor est le nom du compte créer par l’attaquant en ayant des droits lambda sans privilège particulier.

