TLP:WHITE

DFIR4vSphere

https://github.com/ANSSI-FR/DFIR4vSphere

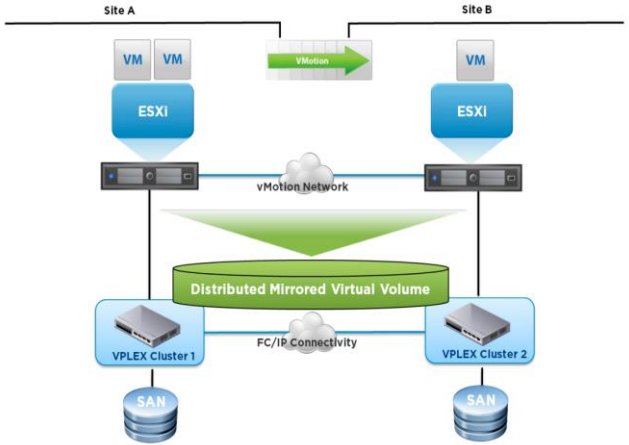
Léonard SAVINA

CoRIIN 2022

vSphere présentation

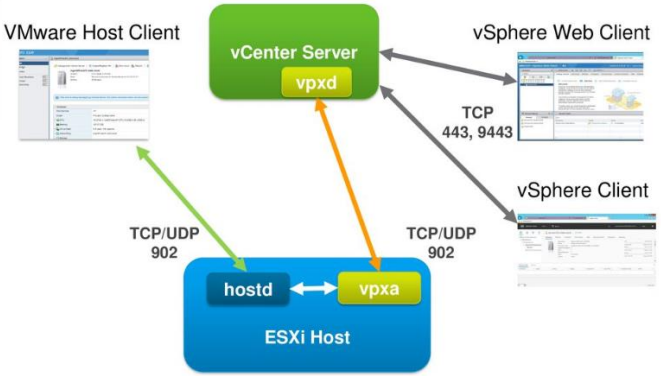
Solution de virtualisation composée d'hyperviseurs de type 1 (ESXi) et d'une solution de gestion centralisée (VCenter).

- **vMotion** (2004): Permet la migration des VMs d'un hôte ESXi à un autre. Permet le **HA** et le **DRS**. Les VMs sont stockés sur le datastore qui est en général un espace de stockage partagé (SAN, NAS, vSAN).
- **vSAN** (2014): Représentation logique d'un SAN via la réplication du stockage des disques en attachement direct.



https://blogs.vmware.com/performance/2013/11/vmware-vsphere-5-5-vmotion-on-emc-vplex-metro.html

vSphere présentation



https://virtualundercity.blogspot.com/2019/10/hostd-vpxa-vpxd.html

› ESXi: Noyau VMKernel, système de fichiers VMFS.

```
[root@esx2:/] uname -a
VMkernel esx2.localdomain 7.0.3 #1 SMP Release
[root@esx2:/] cat /etc/shadow
root:$6$4clS0…
dcui:*:13358…
```

› VCenter Server Appliance: Noyau Linux (Photon), base interne (vPostgres) ou externe (Oracle).

```
root@vca[/]# uname -a
Linux vca.ldap389.local 4.19.191-1.ph3 #1-photon SMP
```

› L'attachement de l'ESXi à la console VCenter créé un compte *vpxuser* sur l'hyperviseur et permet la communication entre *vpxa* (ESXi) et *vpxd* (VCenter).

```
[root@esx2:/] cat /etc/shadow
…
vpxuser:$6$XDb…
```

TLP:WHITE

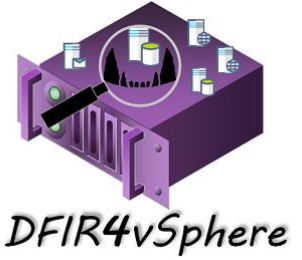
vSphere: adhérence Active Directory

- Un ESXi peut être joint à l'Active Directory: par défaut les membres du groupe AD nommé **ESX Admins** ont des privilèges élevés sur l'hôte (*https://kb.vmware.com/s/article/2075361*). Analyser les modifications de ce groupe via les journaux de sécurité ou avec ADTimeline (*https://github.com/anssi-fr/adtimeline*).

```
PS C:\> .\ADTimeline.ps1 -customgroups "ESX Admins"
```

- La base d'authentification au VCenter est souvent l'Active Directory. La compromission d'un compte AD ayant des privilèges sur le VCenter entraîne la compromission des hôtes ESXi qui lui sont attachés, donc des machines virtuelles hébergées sur ces hôtes.

DFIR4vSphere: Présentation



DFIR4vSphere se base sur le module PowerShell **PowerCLI** et permet de collecter des artéfacts forensiques via deux fonctions:

- **Start-VC_Investigation** récupère l'inventaire des ESXi rattachés au VCenter, les permissions positionnées sur la console et les journaux contenant les appels d'API vSphere réalisés (*VI Events*). Un bundle de support peut aussi être généré, cependant une analyse forensique Linux classique du VCenter est aussi recommandée.

- **Start-ESXi_Investigation** collecte des informations et *bundles* de support des hôtes ESXi.

Start-VC_Investigation: Journaux VCenter

- Les journaux du VCenter sont collectés grâce à la méthode **EventManager.CreateCollectorForEvents**, plus performante que la fonction **Get-VIEvents** fournie dans le module PowerCLI. Méthode utilisée par Luc Dekens dans **Get-VIEventPlus** (*https://www.lucd.info/2013/03/31/get-the-vmotionsvmotion-history*)

- Avec le paramètre **LightVIEvents** seuls les types d'évènements considérés comme d'intérêt sont collectés. Tous les types d'événements sont documentés par William Lam. (*https://github.com/lamw/vcenter-event-mapping*) et sont paramétrables via **LightVIEventTypesId.**

- Les journaux sont collectés au format **JSON**.

```
PS C:\> $enddate = get-date
PS C:\> $startdate = $enddate.adddays(-30)
PS C:\> Start-VC_Investigation -StartDate $startdate -Enddate $enddate -LightVIEvents
```

Start-ESXi_Investigation

La fonction **Start-ESXi_Investigation** va collecter:

- Diverses informations sur les hyperviseurs ESXi ciblés au travers de **ESXCLI** (*https://developer.vmware.com/web/tool/7.0/esxcli*): processus actifs, services, connexions actives, comptes locaux, delta de configuration… Sous forme de fichiers **CSV**.
- Un bundle de support de chaque ESXi ciblé via l'option **ESXBundle**.

La fonction peut cibler un hyperviseur en particulier:

```
PS C:\> Start-ESXi_Investigation -Name %ESXi% -ESXBundle
```

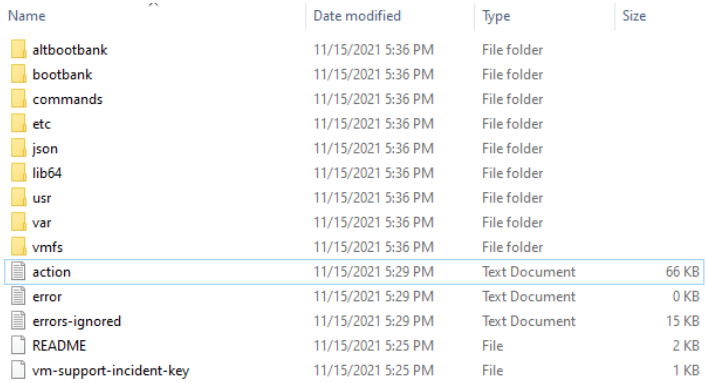
Ou un ensemble d'hyperviseurs récupérés avec la commande PowerCLI **Get-VMHost**

```
PS C:\> Get-VMHost | Start-ESXi_Investigation -ESXBundle
```

Start-ESXi_Investigation: Le bundle de support

C'est une archive **TGZ** générée par l'outil **vm-support** à partir de fichiers **Manifest** situés dans */etc/vmware/vm-support/*.mfx*. On y trouve:

- Dossiers **commands** et **json**: les résultats de commandes tels que la liste et arbre des processus, condensats de binaires dans certains dossiers (/bin, /sbin...), connexions réseau actives…
- Dossiers **bootbank** et **altbootbank**: les informations concernant la partition de boot et celle de secours.
- Le reste des dossiers est l'arborescence telle que sur l'ESXi, seuls certains fichiers étant sélectionnés (en fonction des instructions *.mfx* lancées). On y retrouve donc les journaux locaux.



Name	Date modified	Type	Size
altbootbank	11/15/2021 5:36 PM	File folder	
bootbank	11/15/2021 5:36 PM	File folder	
commands	11/15/2021 5:36 PM	File folder	
etc	11/15/2021 5:36 PM	File folder	
json	11/15/2021 5:36 PM	File folder	
lib64	11/15/2021 5:36 PM	File folder	
usr	11/15/2021 5:36 PM	File folder	
var	11/15/2021 5:36 PM	File folder	
vmfs	11/15/2021 5:36 PM	File folder	
action	11/15/2021 5:29 PM	Text Document	66 KB
error	11/15/2021 5:29 PM	Text Document	0 KB
errors-ignored	11/15/2021 5:29 PM	Text Document	15 KB
README	11/15/2021 5:25 PM	File	2 KB
vm-support-incident-key	11/15/2021 5:25 PM	File	1 KB

https://www.virten.net/2015/10/whats-inside-an-esxi-vm-support-bundle/

Start-ESXi_Investigation: Le bundle de support

Les principaux journaux d'intérêt collectés par le bundle support sont :

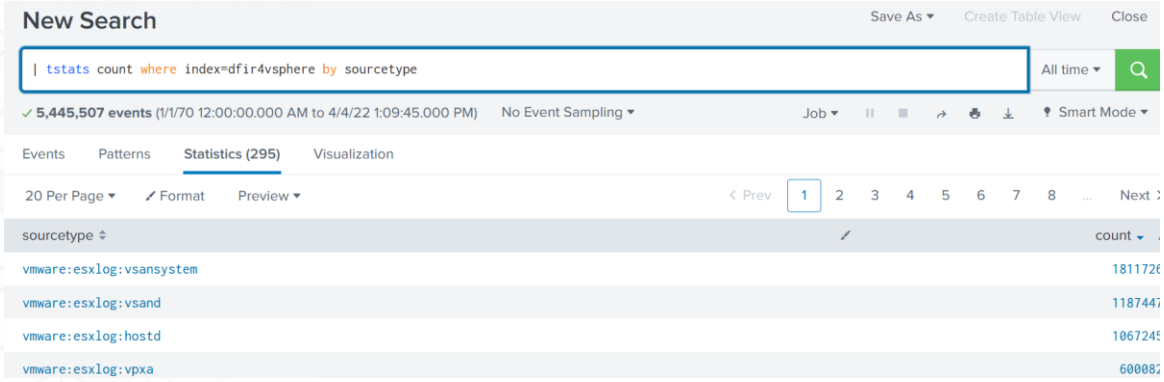
Chemin log	Commentaire
/var/run/log/auth.log	Evènements liés à l'authentification sur l'hyperviseur.
/var/run/log/hostd*(log | gz)	Actions liées à la gestion/configuration de l'ESXi et des machines virtuelles.
/var/run/log/shell.log	Commandes tapées via le shell (SSH, DCUI).
/vmfs/volumes/%DatastoreID%/%VMName%/vmware.log	Actions de gestion/configuration sur une machine virtuelle particulière.
/var/run/log/vpxa*(log | gz)	Agent VCenter sur hôte ESXi

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-832A2618-6B11-4A28-9672-93296DA931D0.html

TLP:WHITE

DFIR4vSphere: Analyse des journaux avec Splunk

- Les journaux issus du VCenter et de la commande **Start-VC_Investigation** s'indexent facilement car ils sont au format **JSON**, l'horodatage étant la valeur de **CreatedTime**.
- Les journaux situés dans le dossier */var/run/logs* de chaque bundle de support collectés avec **Start-ESXi_Investigation** s'indexent à l'aide du **Splunk Add-on for VMware ESXi Logs** (*https://splunkbase.splunk.com/app/5603/*).



vSphere – Outils publics pour purple teaming

Ces outils permettent de mieux comprendre les attaques possibles sur cet environnement et de générer les traces nécessaires à leur détection:

https://github.com/JamesCooteUK/SharpSphere

https://github.com/horizon3ai/vcenter_saml_login

D'autres outils, bien que non spécifiques à vSphere peuvent être utilisés, par exemple, pour maintenir un accès sur un hyperviseur ESXi:

https://github.com/orangetw/tsh

TLP:WHITE

Cybercrime – Rançongiciels et vSphere

Le chiffrement des machines virtuelles hébergées sur un hyperviseur permet à l'attaquant de:

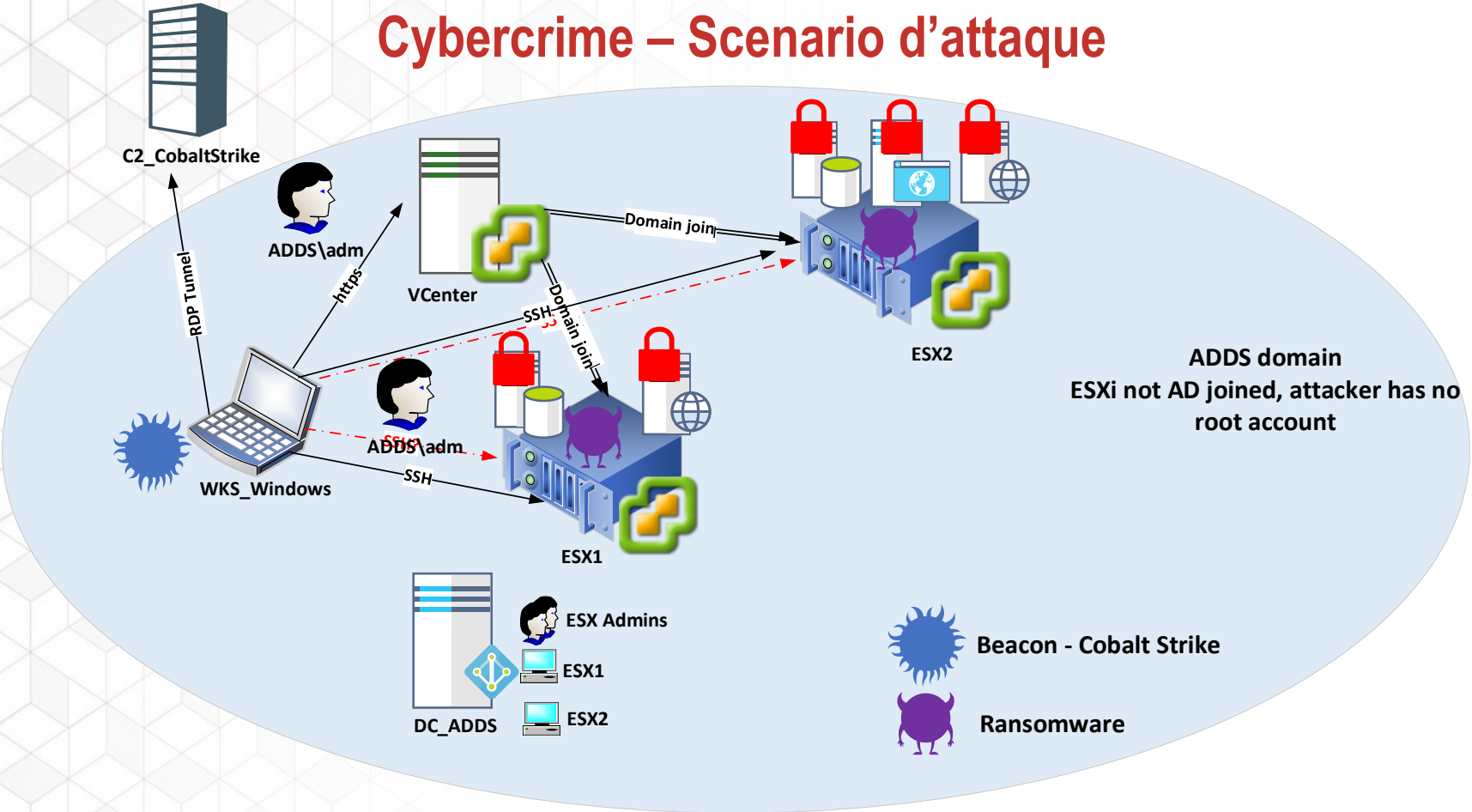
- Chiffrer avec la même souche des machines virtuelles d'OS différents regroupées au sein d'un même *datastore;*
- Contourner la détection et éventuel blocage du chiffrement qui peut être effectué par la solution de sécurité installée sur les machines virtuelles;
- Contourner des politiques de filtrage réseau entre machines virtuelles.

https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

https://news.sophos.com/en-us/2021/10/05/python-ransomware-script-targets-esxi-server-for-encryption/

TLP:WHITE

Cybercrime – Scenario d'attaque



TLP:WHITE

Cybercrime – Chronologie de l'incident

Date (UTC)	Source	Activité
2022-06-06 12:00:01	VCenter - VIEvents	Authentification de *ADDS\adm* au VCenter depuis *WKS_Windows*
2022-06-06 12:00:05	VCenter - VIEvents	Activation de SSH sur les hôtes *ESX1* et *ESX2*.
2022-06-06 12:00:20	ESXi1– auth.log	Tentatives d'authentification SSH depuis *WKS_Windows*
2022-06-06 12:09:43	VCenter - VIEvents	Jonction au domaine *ADDS* de *ESX1* puis *ESX2*
2022-06-06 12:20:27	ADTimeline	Création du groupe *ADDS\ESX Admins*
2022-06-06 12:20:30	ADTimeline	Ajout du compte *ADDS\adm* au groupe *ADDS\ESX Admins*
2022-06-0612:22:55	ESX1 – auth.log	Connexion SSH réussie de *ADDS\adm* depuis *WKS_Windows*
2022-06-06 12:23:01	VCenter - VIEvents	Upload du fichier *xxx.pyz*
2022-06-06 12:23:20	ESX1 – shell.log	Lancement de ***python xxx.pyz /vmfs/volumes/XXXX-XXXX***
2022-06-06 12:23:21	VCenter - VIEvents	Début arrêt successifs des machines virtuelles du datastore.

TLP:WHITE

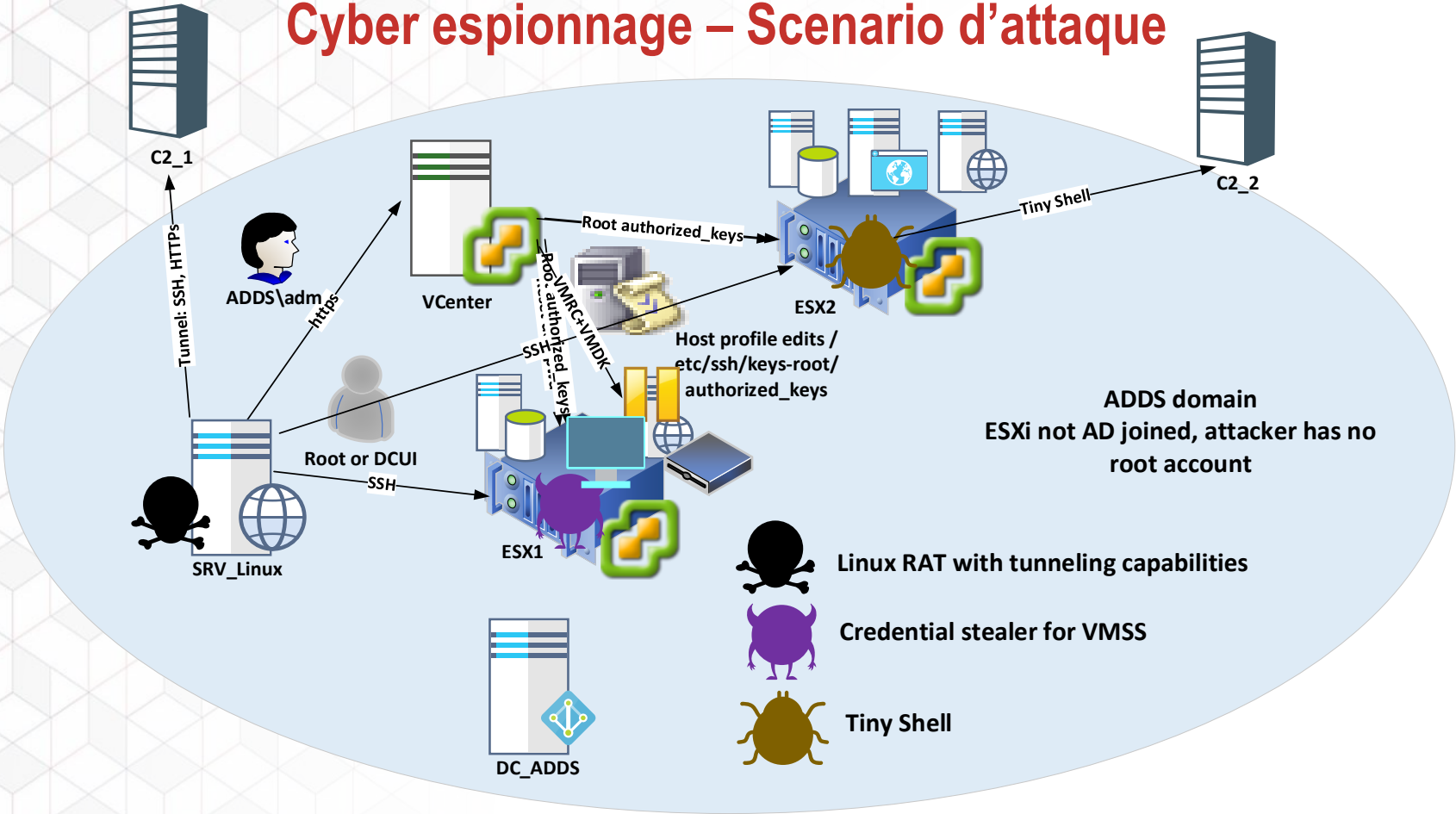
Cyber espionnage – vSphere une cible de choix

Dans le cadre d'espionnage un attaquant peut tirer partie de la technologie vSphere pour:

- Contourner des politiques de filtrage réseau entre machines virtuelles;
- Exfiltrer de la donnée via le téléchargement de disques virtuels;
- Obtenir une capture de la mémoire sans lever de détection au niveau de la solution de sécurité installée sur les machines virtuelles (*https://kb.vmware.com/s/article/2003941*);
- Utiliser les identifiants obtenus via la capture mémoire pour se connecter directement au travers de la **VMRC** (*https://docs.vmware.com/en/VMware-Remote-Console/index.html*)sur la machine virtuelle cible;
- Persister sur un environnement Windows sans utiliser un seul code malveillant sur ce système d'exploitation.

TLP:WHITE

Cyber espionnage – Scenario d'attaque



TLP:WHITE

Cyber espionnage – Chronologie de l'incident 1/2

Date (UTC)	Source	Activité
2022-06-06 12:00:01	VCenter - VIEvents	Authentification de *ADDS\adm* au VCenter depuis *SRV_Linux*
2022-06-06 12:00:18	VCenter - VIEvents	Réinitialisation du mot de passe de *dcui* sur *ESX1* puis *ESX2* https://www.hypervisor.fr/?p=6005
2022-06-06 12:01:22	VCenter - VIEvents	Création du Host Profile nommé *Deploy* pour ajout *authorized_keys* https://www.virten.net/2014/02/howto-esxi-ssh-public-key-authentication/
2022-06-06 12:09:43	ESX1– auth.log	Connexion SSH réussie de *dcui* sur *ESX1* depuis *SRV_Linux*
2022-06-06 12:20:27	ESX1 – shell.log	Lancement de ***cat /etc/ssh/keys-root/authorized_keys***
2022-06-06 12:21:24	VCenter - VIEvents	Suppression du Host Profile nommé *Deploy*.
2022-06-06 12:22:55	VCenter - VIEvents	Suspension puis reprise de la VM *SRV_WinIIS* pour génération vmss
2022-06-06 12:23:01	ESX1– auth.log	Connexion SSH réussie de *root* sur *ESX1* depuis *SRV_Linux*
2022-06-06 12:23:20	VCenter - VIEvents	Upload du fichier *yyy*
2022-06-06 12:23:21	ESX1– shell.log	Lancement de ***chmod 755 yyy***
2022-06-06 12:23:23	ESX1– shell.log	Lancement de ***./yyy /vmfs/volumes/XXXX-XXXX/WebServer/WebServerXXX.vmss***

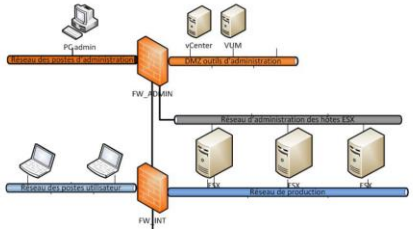
TLP:WHITE

Cyber espionnage – Chronologie de l'incident 2/2

Date (UTC)	Source	Activité
2022-06-06 12:24:01	ESX1– shell.log	Lancement de ***rm -f yyy***
2022-06-06 12:25:09	VCenter - VIEvents	Initialisation d'une session VMRC sur la VM *SRV_WinIIS*
2022-06-06 12:26:01	VCenter - VIEvents	Upload du fichier *SRV_WinIIS07-flat.vmdk*
2022-06-06 12:27:03	ESX1– vmware.log	Attachement du disque *SRV_WinIIS07-flat.vmdk* à la VM *SRV_WinIIS*
2022-06-06 12:32:41	ESX1– vmware.log	Détachement du disque *SRV_WinIIS07-flat.vmdk* à la VM *SRV_WinIIS*
2022-06-06 12:32:50	VCenter - VIEvents	Download du fichier *SRV_WinIIS07-flat.vmdk*
2022-06-06 12:34:55	ESX1– shell.log	Lancement de ***rm –f SRV_WinIIS07-flat.vmdk***
2022-06-06 12:37:01	ESX2– auth.log	Connexion SSH réussie de *root* sur *ESX2* depuis *SRV_Linux*
2022-06-06 12:38:20	VCenter - VIEvents	Upload du fichier *ttt*
2022-06-06 12:38:40	ESX2– shell.log	Lancement de ***mv ttt /bin/vmtsh***
2022-06-06 12:38:44	ESX2– shell.log	Lancement de ***chmod 755 vmtsh***
2022-06-06 12:38:49	ESX2– shell.log	Lancement de ***./vmtsh***

TLP:WHITE

Sécuriser vSphere: Quelques pistes



- Patcher https://www.vmware.com/security/advisories.html
- Administrer la solution depuis un réseau d'administration.
- Mettre en place un supervision de sécurité sur les journaux vSphere.
- Auditer les permissions VCenter (impact sur le modèle AD en Tier).
- Plusieurs guides de sécurisation sont proposées par l'éditeur:

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-412EF981-D4F1-430B-9D09-A4679C2D04E7.html

https://via.vmw.com/scg

- Autres ressources

https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-les-architectures-basees-sur-vmware-vsphere-esxi/

https://www.hub.trimarcsecurity.com/posts/categories/vmware - Demetrios Mustakas

TLP:WHITE

QUESTIONS?

https://github.com/ANSSI-FR/DFIR4vSphere