

MARC BLANCHARD VIRUS DOCTEUR

Protocole d'éradication de CONFIKER/DOWNADUP en réseau d'entreprise

PROTOCOLE d'ACTION en cas de ver DOWNADUP/CONFIKER nouvelle génération sur un réseau Entreprise

Bit Defender Client Security 3.1.7 ou supérieur :

NMAP version 5.00 ou supérieur

KB security patch Microsoft

Bloquer sur les parefeux de l'entreprise le port 445

Lien Produits BitDefender 3.1.7 et pour la Console :

http://download.bitdefender.com/SMB/Workstation_Security_and_Management/BitDefender_Client_Security/Windows/Current/FR/Version_3.0/

Les Addons pour la Console:

[http://download.bitdefender.com/SMB/Workstation_Security_and_Management/BitDefender_Client_Security/Windows/Current/FR/Version_3.0/server_addon/BitDefender_Security_for_Windows_Servers_Server_Addon_\(for_32_bit_Management_Servers\)_fr.exe](http://download.bitdefender.com/SMB/Workstation_Security_and_Management/BitDefender_Client_Security/Windows/Current/FR/Version_3.0/server_addon/BitDefender_Security_for_Windows_Servers_Server_Addon_(for_32_bit_Management_Servers)_fr.exe)

Antivirus du serveur

<http://content-down.bitdefender.com/SMB/Windows%20Servers/Current/FR/>

Outil de désinstallation serveur en cas de nécessité:

ftp://ftp.editions-profil.fr/Versions_Evaluation/BitDefender/Windows/Serveurs/v2/Windows_Serveurs_Uninstall_Tool.exe

NMAP :

<http://nmap.org/dist/nmap-5.00.tar.bz2>

KB Microsoft :

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS08-068.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS09-001.msp>

Outil de désinfection BitDefender

PROTOCOLE A APPLIQUER : En cas de pandémie de ver/worm/stormworm

Méthodes et plan d'action.

ATTENTION : Respecter cette méthode dans l'ordre décrit. Si une des étapes est oubliée, le ver risque de réagir et changer de comportement, et par conséquent incontrôlable.

PS : cette procédure est actuellement adaptée au ver CONFIKER/DOWNADUP, et nous nous réservons le droit de la modifier sans préavis et en temps réel pour répondre aux résultantes des attaques zero day.

Préparations :

1/ Prendre une machine sous linux, la connecter au réseau instable, et installer NMAP comme noté dans ce bulletin

2/ Installer ou passer en version BitDefender console Client Security 3.1.7, BitDefender Business client 11.0.0.8 et BitDefender Security for Windows Server 3.3.0 sur tous les postes et serveurs.

3/ Télécharger les KB de Microsoft sur la machine où se trouve la console BitDefender Client Security 3.1.7

4/ Appliquer la règle suivante sur les parefeux connectés à internet :

Inbound : Deny : source 0.0.0.0 destination 0.0.0.0 port : source 445 destination 445 on TCP+UDP

Outbound : Deny : source 0.0.0.0 destination 0.0.0.0 port : source 445 destination 445 on TCP+UDP

Préparations et Procédures d'installations / Migrations

NOTA : Cette section n'est pas le plan d'action (voir plus bas)

Installation NMAP sur la machine Linux:

Si vous avez une distribution RedHat, CentOs ou Fedora récente téléchargez le package comme suit :

```
yum install nmap
```

Sinon téléchargez les sources puis compilez le. Attention si vous êtes sur une plateforme 64bits, il faut installer les bibliothèques libstdc++

```
wget http://nmap.org/dist/nmap-5.00.tar.bz2 tar xjfv nmap-5.00.tar.bz2 cd nmap-5.00 ./configure
```

make make install

Utilisation qu'il faudra lancer lors de l'étape du plan d'action :

Pour tester le réseau :

```
nmap -PN 192.168.0.0/24 -p139,445 -n -v script smb-check-vulns script-args safe=1
```

Pour loguer le résultat :

```
nmap -PN 192.168.0.0/24 -p139,445 -n -v script smb-check-vulns script-args safe=1 >>
/directory/resultat.log
```

Tous postes infectés seront taggué comme INFECTED.

Si POSSIBLY INFECTED, soit NMAP n'arrive pas à tester (imprimantes réseaux, SAN, Samba Linux, etc) ou soit une vulnérabilité sur cette machine reste active si elle est sous Windows --> Cette machine devra être analysée par l'administrateur

Installation / Migration des produits BitDefender :

I) LES PRES REQUIS D'INSTALLATION

Les postes serveurs: Net Framework version 2 minimum *(SP2)* Dernière Mise à jour Windows *(SP2 minimum)* Pare-feu Windows désactivé (PAR LES SERVICES) Partage de fichiers et d'imprimantes activé 800 Mo (minimum) de libre sur le lecteur C:\ Workgroup: partage simple désactivé

Les postes clients Net Framework version 2 minimum *(SP2)* Dernière Mise à jour Windows *(SP2 minimum)* Partage de fichiers et d'imprimantes activés 115 Mo (minimum) de libre sur le lecteur C:\ Workgroup: partage simple désactivé TOUS LES POSTES CLIENTS DOIVENT ETRE ALLUMES.

II) INSTALLATION DE LA CONSOLE

1] Suppression des programmes Allez dans l'ajout/suppression de programmes de windows. Désinstallez tous les produits BitDefender étant sur la machine serveur.

2] Appliquez l'utilitaire de désinstallation « Windows_Server_Uninstall_Tool.exe » (utilitaire téléchargé précédemment)

3] Redémarrer votre serveur.

AVANT D'ALLER PLUS LOIN IL EST IMPERATIF QUE TOUS LES PRE REQUIS DU SERVEUR SOIENT MIS EN PLACE.

4] Installation BitDefender Client Security.

Sélectionnez une installation personnalisée Gardez les paramètres par défauts et faites suivant. Selon les besoins sélectionnez votre type de serveur. Conservez les ports par défauts Installez

une nouvelle base SQL. Garder les options par défaut. Si vous rencontrez des problèmes changer l'instance en « BDMS2 »

7] Installation de l'addon (téléchargé précédemment).

BitDefender_Security_for_Windows_Servers_Server_Addon_(for_32_bit_Management_Servers)_fr.exe

III) INSTALLATIONS DE BITDEFENDER FOR FILE SERVER

1] Installation Installez BitDefender Security for File Server que vous avez téléchargé précédemment. BitDefender_Security_for_Windows_Servers_v3_(x64 ou x86)_FR.exe

2] Choix des composants Sélectionnez le composant BitDefender for File Server uniquement.

3] Terminez l'installation

4] Redémarrer le poste serveur (important)

Installez BitDefender for File Server sur tous les serveurs de votre parc

IV) DEPLOIEMENT DES POSTES CLIENTS

1] Lancez BitDefender Client Security Double-cliquez sur l'application BitDefender Client Security présente sur le bureau.

2] Identification Identifiez-vous sur la console. Le mot de passe par défaut étant « admin » BitDefender Management Console sous forme de deux fenêtres, celle de gauche permettant de sélectionner les différents menus puis celle de droite qui vous permet de configurer les paramètres.

3] Authentification Rendez-vous dans l'onglet « outils », puis cliquez sur « Administrateurs des authentifications » enfin cliquez sur le boutons « + » en haut à droite.

Renseignez les champs.

4] Enregistrement du produit. Allez dans l'onglet « outils », puis dans « enregistrement » enfin rentrez votre clef d'activation Bitdefender Client Security.

5] Création d'un groupe. Pour administrer les postes clients, la création d'un groupe est nécessaire. Au niveau de la fenêtre de gauche de la console, allez dans « dossier ordinateur ». Dans cette arborescence, 3 menus sont présents. Cliquez droit sur le premier (ordinateurs administrés) et créer un groupe.

6] Création d'une politique Antivirus Dans l'arborescence de gauche, rendez-vous dans le module "politiques". Allez dans créer une nouvelle politique, puis dans l'écran de droite, double cliquez sur « Paramètre Antivirus »

7] Paramétrage de la politique Cochez la protection en temps réel. Mettez le niveau de protection en "Personnalisée" Modifier les actions appliquées en cas de détection :

Action à appliquer lorsqu'un fichier infecté est trouvé Première action : Désinfecter le fichier
Deuxième action : Mettre en quarantaine

Action à appliquer lorsqu'un fichier suspect est trouvé Première action : Désinfecter le fichier
Deuxième action : Mettre en quarantaine

Conservez les autres options par défaut. Cliquez sur terminer.

8] Affectation de la politique **APPLIQUER CETTE POLITIQUE AU GROUPE QUE VOUS AVEZ CRÉÉE**

Pour se faire, mettez le groupe en surbrillance. Planification: "Une fois" Puis cliquer sur "cliquez ici pour affecter cette politique"

Grâce à cette politique, chaque nouveau poste intégrant ce groupe recevra l'antivirus automatiquement.

9] Déploiement de l'agent. Rendez-vous dans l'onglet "outils" et sélectionnez le module "Network Builder"

Dans le cadran de gauche vous retrouverez tous les postes du réseau. Dans le cadran de droite vous retrouverez vos groupes.

Grâce au procédé glisser/déposer, déplacez les postes clients dans le groupe créé.

Attention! Ne rentrez pas les serveurs dans ce groupe.

Enfin cliquez sur "Appliquer les modifications"

10] Notifications des utilisateurs Une fenêtre nommée "Déploiement de l'agent" s'affiche.

Dans celle ci, cocher les options suivantes:

Installer l'agent sans interface utilisateur Faire un ping des ordinateurs cibles avant le déploiement Ne pas redémarrer à la fin de l'installation

Enfin vérifiez le nom du serveur et lancez le déploiement.

11] Etat de l'avancement Gardez la fenêtre de contrôle Network Builder jusqu'à la fin du

déploiement. Certains postes seront en échec. Cela signifie que ces postes ne disposent pas des prérequis énoncés ci-dessus. Il est donc important de faire le nécessaire pour pouvoir procéder au déploiement.

Faites les mises à jour Windows et .NET Framework de ces postes.

12] Création d'un serveur de mise à jour Vous pouvez définir un serveur local de mises à jour. Pour ce faire, allez dans « Démarrer », « Programmes », « Bitdefender Management Server » puis « Serveur de mise à jour BitDefender ».

Dans l'assistant de configuration gardez l'adresse par défaut.

Indiquez ensuite un répertoire de stockage de mises à jour. C'est ici que les bases virales seront téléchargées. Utilisez le port 80 (ou bien un port libre et ouvert sur votre Firewall).

Sélectionnez les composants Business Client et File server. Faites suivre.

Un écran résume les paramètres de la configuration. Pour terminer appuyez sur le bouton « Mettre à jour ».

13] Création des politiques

Retournez dans la console. Pour terminer ce déploiement, rendez-vous dans les politiques.

Créer les deux politiques suivantes :

Politique « Paramètre du Pare-feu »

Cochez les options suivantes :

Pare-feu activé Appliquer le profil générique à tous les réseaux Profil générique Profil actuel Règles essentielles

Laissez les réponses automatiques par défaut et terminer la configuration. Appliquez cette politique au groupe créé.

Politique « Mise à jour planifiée »

Emplacement principal : http://adresse_ip_serveur Emplacement secondaire <http://upgrade.bitdefender.com> (cochez la case si un proxy existe)

Paramétrez votre proxy (si proxy il y a)

Puis terminer la politique

Assignez-la au groupe créé.

La migration est terminée

Installation des mises en place des KB de Microsoft prêt à être déployé lorsque le plan d'action

3. Installer BitDefender antivirus sur ce serveur et lancer une mise à jour.
4. Vérifier que l'analyse temps réel de ce serveur soit avec les options pour les fichiers infectés et suspects : 1ere action : désinfecter ? 2eme action : 40aine
5. Aller dans la console de management BD (ne pas confondre avec la console de l'antivirus serveur) installée sur ce serveur.
6. Application et déploiement sur tous les postes et serveurs d'une politique de l'analyse temps réel de BD (BitDefender) sur TOUS LES FICHIERS pour les fichiers infectés et suspects Action : Désinfecter / Mise en 40aine
7. Vérifier, via la console BD, que toutes les machines du réseau soient à jour avec cette politique de sécurité, et appliquer cette règle pour les nouveaux postes connectés. Il est à noter que certaines machines du réseau ne seront pas forcément à jour au niveau moteur d'analyse ou signatures. Notez ces postes, mais n'intervenez pas tout de suite physiquement. Passer au point suivant.
8. Mettez en place une politique de règles du firewall de BitDefender à partir de la console BD avec les règles suivantes. Ces règles sont temporaires mais doivent être obligatoirement déployées.

Configuration de la politique du pare-feu

Paramètre général Activer le pare-feu : Bloquer le trafic : Utiliser un profil générique pour tous réseaux :

Paramètres du profil Profil Générique :

Appliquer les paramètres à: Profil actuel :

Vérifiez que toutes les autres options soient décochées exceptés "les politiques d'administration".

Nous allons temporairement pour la désinfection bloquer les ports suivants :

445 en TCP et UDP 139 en TCP et UDP

Appliquez les règles suivantes :

a. Blocage du port 445/TCP

Cliquez sur "Gérer Les Règles" Cliquez sur "Ajouter une règle" Dans processus, laisser décochée cette option Protocol : basculez sur TCP Direction : basculez sur Tout Action : basculez sur refuser

Source Adresse IP : mettez à 0.0.0.0 Mask : appliquer à 0.0.0.0 Port : basculez sur spécifier un port et écrire "445"

Destination Adresse IP : fixer à 0.0.0.0 Mask : fixer à 0.0.0.0 Port : déclarer "N'importe quel

ports"

Cliquez sur "ajouter"

b. Blocage du port 445/UDP

Cliquez sur "Gérer Les Règles" Cliquez sur "Ajouter une règle" Dans processus, laisser décochée cette option Protocol : basculez sur UDP Direction : basculez sur Tout Action : basculez sur refuser

Source Adresse IP : mettez à 0.0.0.0 Mask : appliquer à 0.0.0.0 Port : basculez sur spécifier un port et écrire "445"

Destination Adresse IP : fixer à 0.0.0.0 Mask : fixer à 0.0.0.0 Port : déclarer "N'importe quel ports"

Cliquez sur "ajouter"

c. Blocage du port 139/TCP

Cliquez sur "Gérer Les Règles" Cliquez sur "Ajouter une règle" Dans processus, laisser décochée cette option Protocol : basculez sur TCP Direction : basculez sur Tout Action : basculez sur refuser

Source Adresse IP : mettez à 0.0.0.0 Mask : appliquer à 0.0.0.0 Port : basculez sur spécifier un port et écrire "139"

Destination Adresse IP : fixer à 0.0.0.0 Mask : fixer à 0.0.0.0 Port : déclarer "N'importe quel ports"

Cliquez sur "ajouter"

d. Blocage du port 139/UDP

Cliquez sur "Gérer Les Règles" Cliquez sur "Ajouter une règle" Dans processus, laisser décochée cette option Protocol : basculez sur UDP Direction : basculez sur Tout Action : basculez sur refuser

Source Adresse IP : mettez à 0.0.0.0 Mask : appliquer à 0.0.0.0 Port : basculez sur spécifier un port et écrire "139"

Destination Adresse IP : fixer à 0.0.0.0 Mask : fixer à 0.0.0.0 Port : déclarer "N'importe quel ports"

Cliquez sur "ajouter" Cliquez ensuite sur « terminer »

Une fois toutes les règles ajoutées, allez dans "autres paramètres"

Dans les "autres paramètres", vérifiez que les réponses automatiques soient sur "OUI IMPOSE"

9. Lancer NMAP avec la machine linux :

```
nmap -PN 192.168.0.0/24 -p139,445 -n -v script-smb-check-vulns script-args safe=1 >>  
/directory/etape1.log
```

Garder précieusement ce log, il servira de référence pour les analyses ultérieures lorsque la procédure sera terminée. Ne pas s'inquiéter sur le nombre de machines qui seront notées comme INFECTED, nous allons les traiter dans les points suivants de ce plan d'action

10. Prendre la console BD, et déployer le script WMI concernant tous les patches KB de Microsoft (notés dans la procédure de ce document) sur tout le parc. Même si vous pensez que les machines sont à jour, repassez le script WMI, si les KB sont déjà installés, ils ne seront pas réinstallés.

11. Prendre la console BD, et déployer le script WMI de blocage des USB temporairement, le temps du nettoyage du parc. Cette étape est OBLIGATOIRE car un des vecteurs de ce ver est les unités USB via leurs insertions dans les ordinateurs.

12. Lancer NMAP avec la machine linux :

```
nmap -PN 192.168.0.0/24 -p139,445 -n -v script-smb-check-vulns script-args safe=1 >>  
/directory/etape2.log
```

13. Vérifier ce log en prêtant attention aux machines notées INFECTED. N'intervenez physiquement pas encore sur ces machines. On les traitera plus tard dans le protocole.

14. Vérifier dans la console BD si ces machines ont bien subies une mise à jour des KB, de la politique concernant le temps réel de l'antivirus, et des scripts WMI et USB. Si tel n'est pas le cas, renforcer ces postes sur les politiques. Si cela ne fonctionne pas, noter ces adresses IP et passer à l'étape suivante

15. Créer et déployer sur tout le parc, la règle de déploiement de l'outil de désinfection. Attendre que cette règle soit lancée sur tous les postes et serveurs.

16. Forcer une règle de mise à jour des signatures et moteurs BitDefender sur l'ensemble des machines et serveurs du parc.

17. Créer une règle d'analyse forcée pour tous les postes et serveurs du parc sur le root (C:\), le répertoire Windows et le répertoire Documents & Settings sur TOUS LES FICHIERS pour les fichiers infectés et suspects: Action : Désinfecter / Mise en 40aine

18. Vérifier que cette opération a été effectuée pour tous les postes et serveurs du parc

19. Lancer NMAP avec la machine linux :

```
nmap -PN 192.168.0.0/24 -p139,445 -n -v script-smb-check-vulns script-args safe=1 >>  
/directory/etape3.log
```

20. Vérifier ce log en prêtant attention aux machines notées INFECTED et POSSIBLY INFECTED.

Aller physiquement sur ces machines INFECTED et déconnectez les du réseau, ces machines sont vulnérables. Il faudra les patcher manuellement.

Si ce sont des machines NT, Win98, ME, il faudra ne plus les reconnecter du réseau. Aucun support de KB n'est fourni par Microsoft.

Pour les machines POSSIBLY INFECTED, il s'agit souvent de machines Linux avec samba et ces machines ne sont pas vulnérables à ce ver.

Si il s'agit d'une machine Windows, déconnectez les immédiatement physiquement du réseau, il faut appliquer les KB et outil de désinfection manuellement.

21. Relancer NMAP avec la machine linux :

```
nmap -PN 192.168.0.0/24 -p139,445 -n -v script-smb-check-vulns script-args safe=1 >>
/directory/etape4.log
```

22. Vérifier si aucune machine est noté INFECTED dans le log. Si tel est le cas, plus aucune machine n'est infectée, aller au point suivant du protocole

23. Aller sur la console BD et redonner les accès a tout le parc des clefs USB via le script WMI prévu à cet effet.

24. Toujours sur la console BD, redonnez les politiques du firewall BD qui étaient déclarées avant l'infection. Déployer ces règles de firewall.

25. Relancer NMAP avec la machine linux :

```
nmap -PN 192.168.0.0/24 -p139,445 -n -v script-smb-check-vulns script-args safe=1 >>
/directory/etape5.log
```

Vérifier si aucune machine est noté INFECTED dans le log. Si tel est le cas, plus aucune machine n'est infectée, aller au point suivant du protocole. Sinon des machines restent INFECTED et si il s'agit d'une machine Windows, déconnectez les immédiatement physiquement du réseau, il faut appliquer les KB et outil de désinfection manuellement.

26. Le cas important : les ordinateurs portables. Selon la politique de votre entreprise, il y a plusieurs possibilités de forcer les mises à jour de ces postes.

- Modifier le fichier DHCP.CONF avec des mac-address en forçant les portables à binder une IP qui n'est pas celle du réseau lorsqu'ils se connectent sur la RJ45, et faire une intervention manuelle.

- Dans le même esprit, ouvrir un WLAN sur votre réseau physique sur lequel serait installé un autre serveur BitDefender qui appliquerait les opérations ci-dessus. Une fois effectuées, désinstaller l'agent BD de cette machine, et la reconnecter au réseau initial. L'agent BD du réseau local sera réinstallé avec les politiques de l'entreprise.

- Ou donner à l'administrateur ce portable pour vérification manuelle sur laquelle les KB,

installation de l'antivirus devront être installées.

NOTES IMPORTANTES : Si dans le réseau des machines NT, ME, Windows 98 ou Windows 95 sont connectées, ces machines sont vulnérables et aucun patch n'a été fourni par Microsoft.

Le temps d'application du protocole, ces machines doivent IMPERATIVEMENT être déconnectées du réseau. Par la suite, des solutions s'offrent à vous :

- Faire migrer ces machines avec des OS plus récents.
- Installer un pare-feu logiciel en bloquant les Inbounds et Outbound sur les ports 139 et 445
- Installer un pare-feu physique (des petits boîtiers aujourd'hui sont commercialisés) en bloquant les Inbounds et Outbound sur les ports 139 et 445

Copyright : Blanchard [Virus Docteur] Marc - 2009-10-02 17:10:01
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>