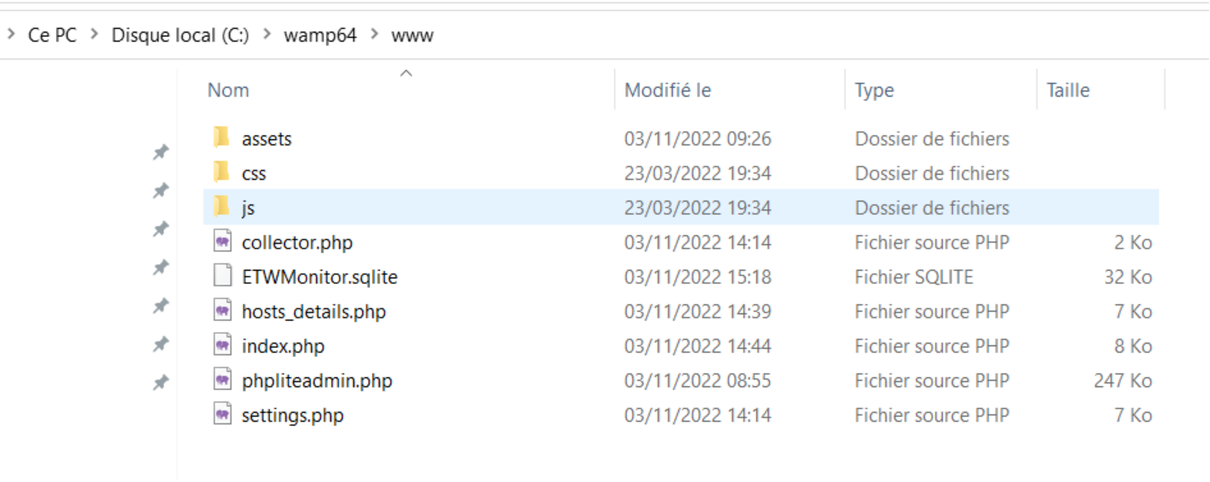
ETWMonitor

INSTALLATION HOW TO

Processus Thief

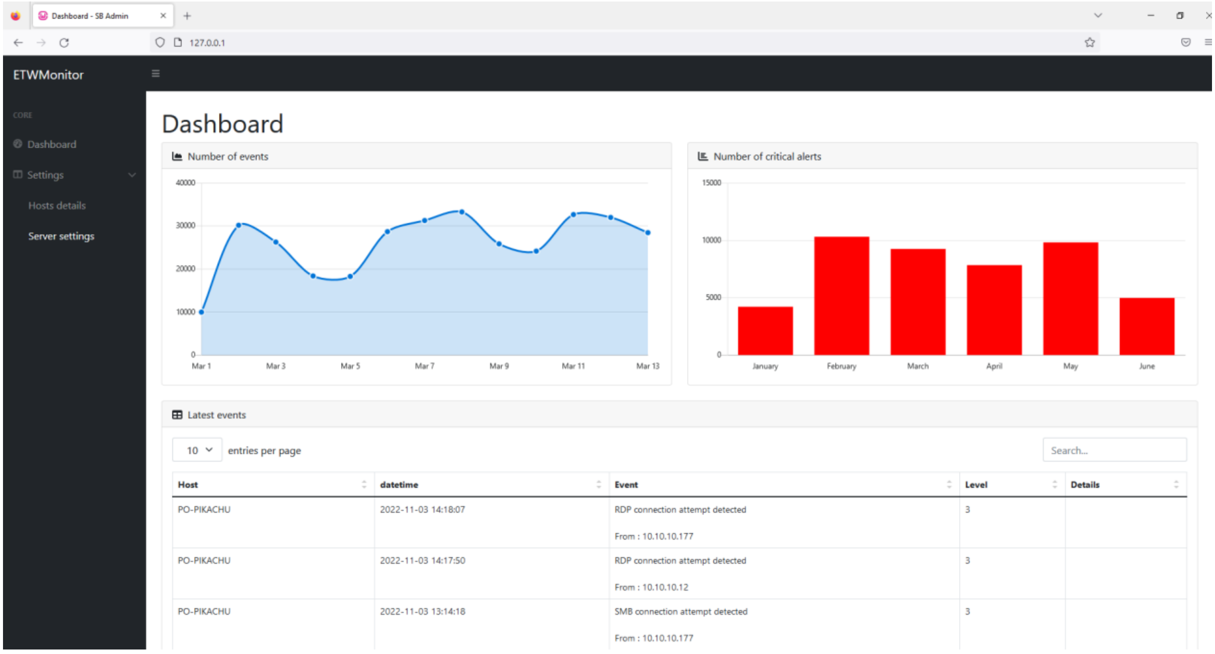
November 2022

1. Unzip the "ETWMonitor.Server.v2.0.zip" archive in the web server directory



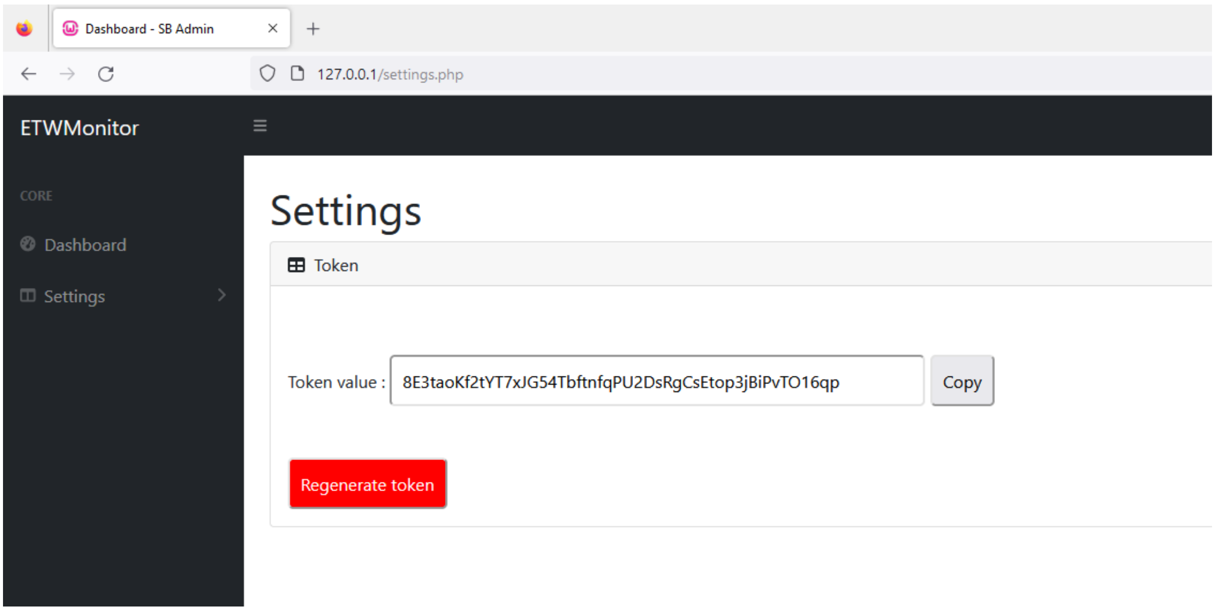
Nom	Modifié le	Type	Taille
assets	03/11/2022 09:26	Dossier de fichiers	
css	23/03/2022 19:34	Dossier de fichiers	
js	23/03/2022 19:34	Dossier de fichiers	
collector.php	03/11/2022 14:14	Fichier source PHP	2 Ko
ETWMonitor.sqlite	03/11/2022 15:18	Fichier SQLITE	32 Ko
hosts_details.php	03/11/2022 14:39	Fichier source PHP	7 Ko
index.php	03/11/2022 14:44	Fichier source PHP	8 Ko
phpliteadmin.php	03/11/2022 08:55	Fichier source PHP	247 Ko
settings.php	03/11/2022 14:14	Fichier source PHP	7 Ko

2. From a browser, access the monitoring web interface



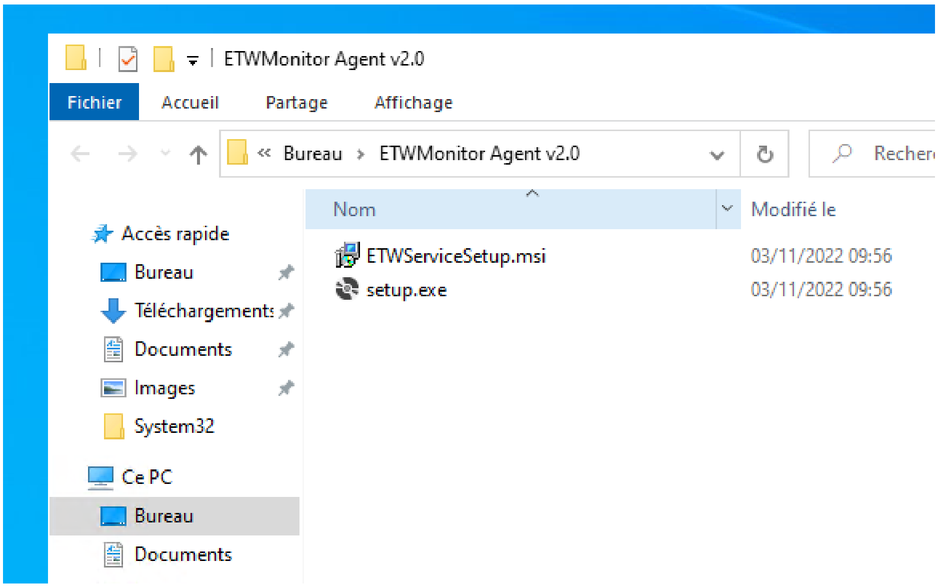
Host	datetime	Event	Level	Details
PO-PIKACHU	2022-11-03 14:18:07	RDP connection attempt detected From : 10.10.10.177	3	
PO-PIKACHU	2022-11-03 14:17:50	RDP connection attempt detected From : 10.10.10.12	3	
PO-PIKACHU	2022-11-03 13:14:18	SMB connection attempt detected From : 10.10.10.177	3	

3. From the **settings** interface, generate a new communication token and copy it



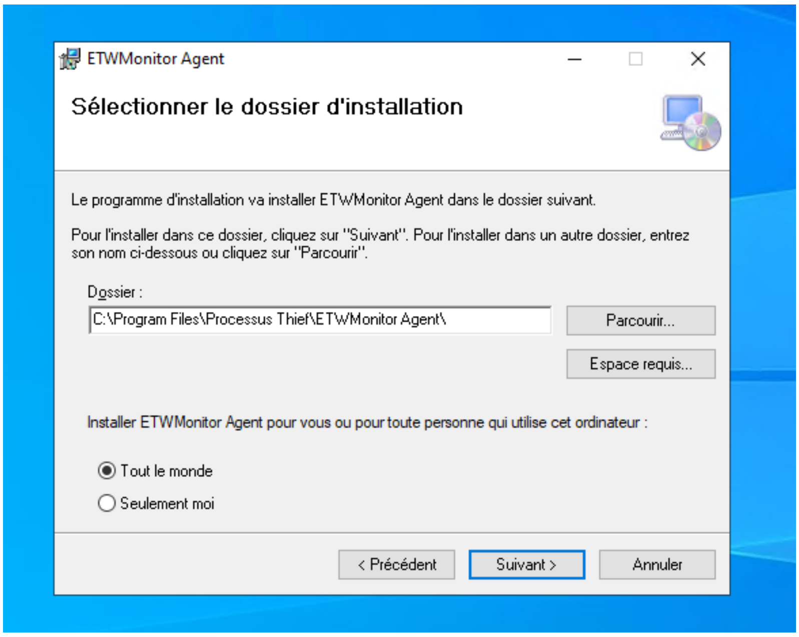
Token value : 8E3taoKf2tYT7xJG54TbftnfqPU2DsRgCsEtop3jBiPvTO16qp

4. On the server you want to monitor, unzip the "ETWMonitor.Agent.v2.0.zip" archive and start the **setup.exe** program



Nom	Modifié le
ETWServiceSetup.msi	03/11/2022 09:56
setup.exe	03/11/2022 09:56

5. Leave the default options checked and go to the end of the installation



ETWMonitor Agent

Sélectionner le dossier d'installation

Le programme d'installation va installer ETWMonitor Agent dans le dossier suivant.

Pour l'installer dans ce dossier, cliquez sur "Suivant". Pour l'installer dans un autre dossier, entrez son nom ci-dessous ou cliquez sur "Parcourir".

Dossier : C:\Program Files\Processus Thief\ETWMonitor Agent\

Installer ETWMonitor Agent pour vous ou pour toute personne qui utilise cet ordinateur :

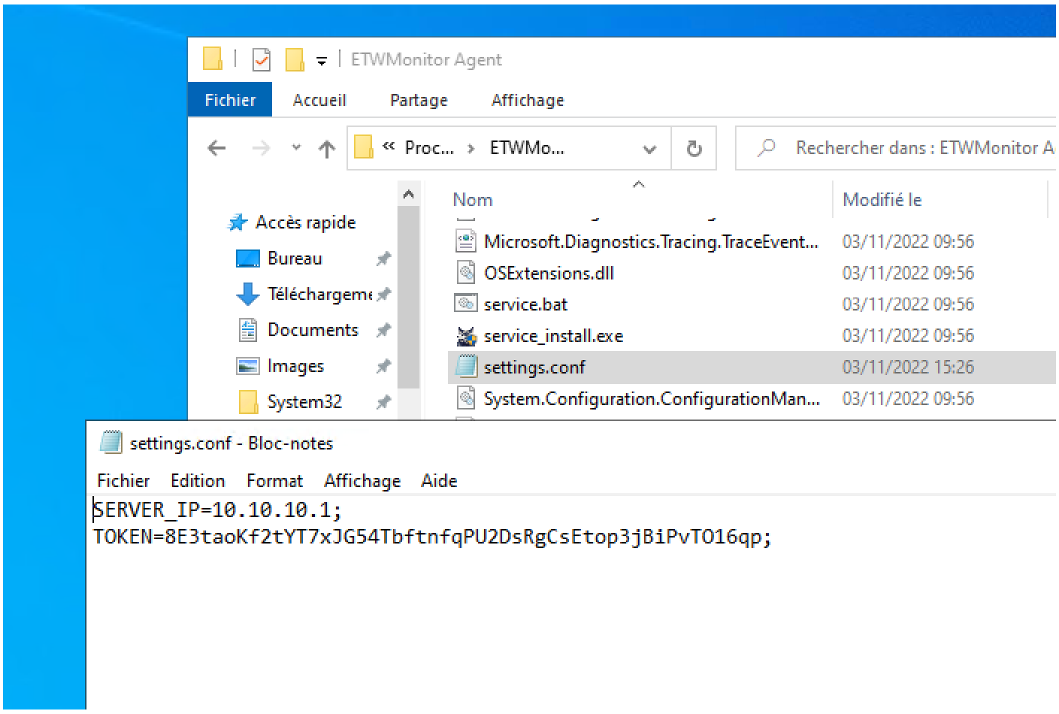
● Tout le monde

○ Seulement moi

6. Once the installation is complete, navigate to the installation directory(*) and edit the **settings.conf** file

* Default location is : **C:\Program Files\Processus Thief\ETWMonitor Agent**

Add the **server IP address** and the **server token** you copied earlier respecting the syntax already in place then save and **restart your computer**



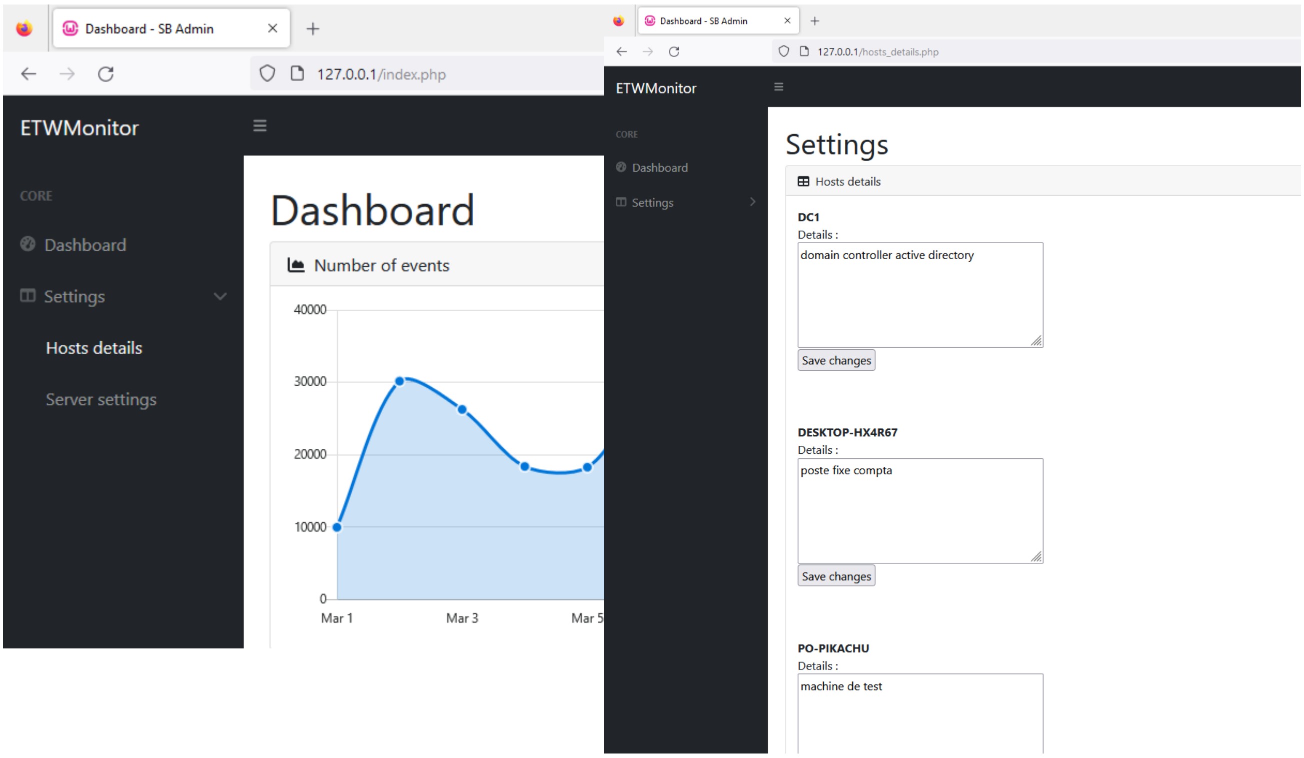
ETWMonitor Agent

Nom	Modifié le
Microsoft.Diagnostics.Tracing.TraceEvent...	03/11/2022 09:56
OSExtensions.dll	03/11/2022 09:56
service.bat	03/11/2022 09:56
service_install.exe	03/11/2022 09:56
settings.conf	03/11/2022 15:26
System.Configuration.ConfigurationMan...	03/11/2022 09:56

settings.conf - Bloc-notes

```
SERVER_IP=10.10.10.1;
TOKEN=8E3taoKf2tYT7xJG54TbftnfqPU2DsRgCsEtop3jBiPvTO16qp;
```

7. On the server monitoring interface you can add details for an active host by clicking on **Hosts details** link



Settings

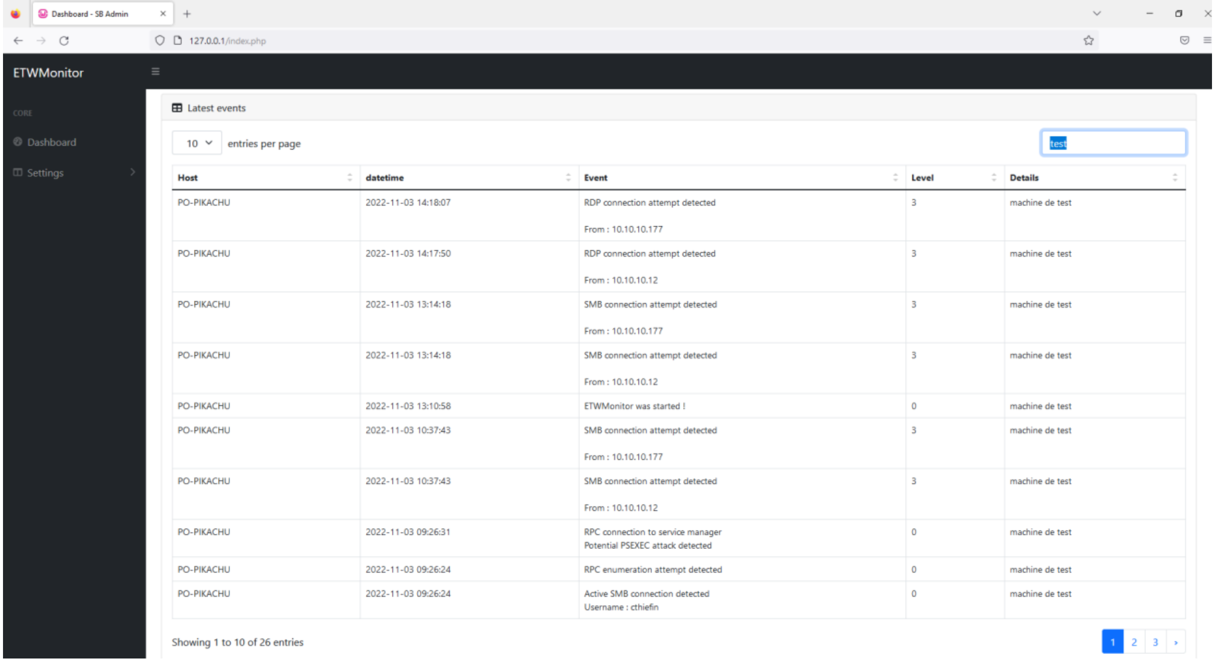
Hosts details

DC1
Details :
domain controller active directory
Save changes

DESKTOP-HX4R67
Details :
poste fixe compta
Save changes

PO-PIKACHU
Details :
machine de test

8. You can now receive the latest notifications from each monitor server and filter by hostnames or details you specified for each one



Latest events

10 entries per page

test

Host	datetime	Event	Level	Details
PO-PIKACHU	2022-11-03 14:18:07	RDP connection attempt detected From : 10.10.10.177	3	machine de test
PO-PIKACHU	2022-11-03 14:17:50	RDP connection attempt detected From : 10.10.10.12	3	machine de test
PO-PIKACHU	2022-11-03 13:14:18	SMB connection attempt detected From : 10.10.10.177	3	machine de test
PO-PIKACHU	2022-11-03 13:14:18	SMB connection attempt detected From : 10.10.10.12	3	machine de test
PO-PIKACHU	2022-11-03 13:10:58	ETWMonitor was started !	0	machine de test
PO-PIKACHU	2022-11-03 10:37:43	SMB connection attempt detected From : 10.10.10.177	3	machine de test
PO-PIKACHU	2022-11-03 10:37:43	SMB connection attempt detected From : 10.10.10.12	3	machine de test
PO-PIKACHU	2022-11-03 09:26:31	RPC connection to service manager Potential PSEXEC attack detected	0	machine de test
PO-PIKACHU	2022-11-03 09:26:24	RPC enumeration attempt detected	0	machine de test
PO-PIKACHU	2022-11-03 09:26:24	Active SMB connection detected Username : cthiefin	0	machine de test

Showing 1 to 10 of 26 entries

1 2 3 ›