STREAMSCAN

ANALYSE

RANCONGICIEL NITROGEN

OCT 2024 //

Introduction

Le but de cette analyse est de disséquer le rançongiciel **Nitrogen** distribué par **Nitrogen Ransomware Group** pour mieux comprendre son fonctionnement.

Ce rançongiciel a beaucoup de points en commun avec le rancongiciel **LukaLocker** distribué par le groupe **Volcano Demon.**

Hash du rançongiciel Nitrogen

- MD5 : b580be9e58374b7c3a1e91922e982d3b
- SHA-1 : bcb9455f82f17483a625e61b3cb52aa20835dc6e
- SHA-256 : 55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47c18c88be

Information sur le fichier

- Taille du fichier : 1.36 MB (1428992 bytes)

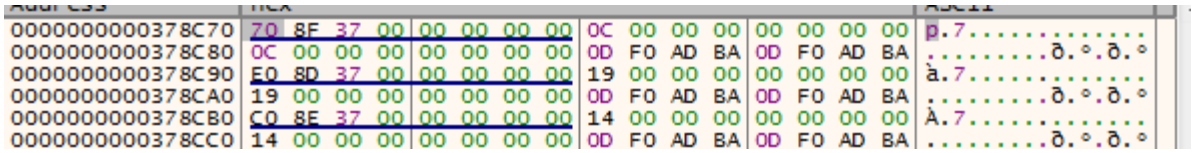
Autres fichiers liés au rançongiciel Nitrogen

Nom de fichier	SHA1	Description
truesight.sys	363068731e87bcee19ad5cb802e14f9248465d31	Pilote vulnérable utilisé de manière abusive pour mettre fin à un processus tel qu'un antivirus ou un EDR.
protector.exe	ebd3eb216aac16277b13a5e832f3ff5843ae7d0d	Terminateur de processus

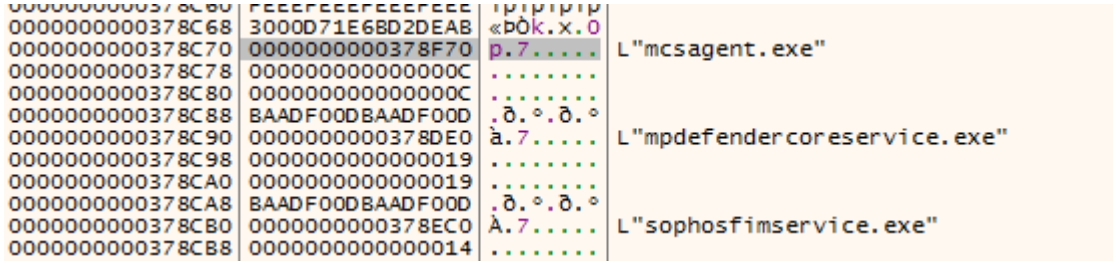
Analyse des fichiers protector.exe et truesight.sys

Le fichier **truesight.sys** contient une liste de 1877 logiciels de sécurité, dont AV/EDR.

A l'exécution, le rançongiciel Nitrogen extrait la liste de tous les processus actifs sur la machine ciblée et les stocke dans un tableau, comme le montre l'image ci-dessous.



```
0000000000378C70 70 8F 37 00 00 00 00 00 0C 00 00 00 00 00 00 00 p.7.............
0000000000378C80 0C 00 00 00 00 00 00 00 0D F0 AD BA 0D F0 AD BA .........ð.°.ð.°
0000000000378C90 E0 8D 37 00 00 00 00 00 19 00 00 00 00 00 00 00 à.7.............
0000000000378CA0 19 00 00 00 00 00 00 00 0D F0 AD BA 0D F0 AD BA .........ð.°.ð.°
0000000000378CB0 C0 8E 37 00 00 00 00 00 14 00 00 00 00 00 00 00 À.7.............
0000000000378CC0 14 00 00 00 00 00 00 00 0D F0 AD BA 0D F0 AD BA .........ð.°.ð.°
```

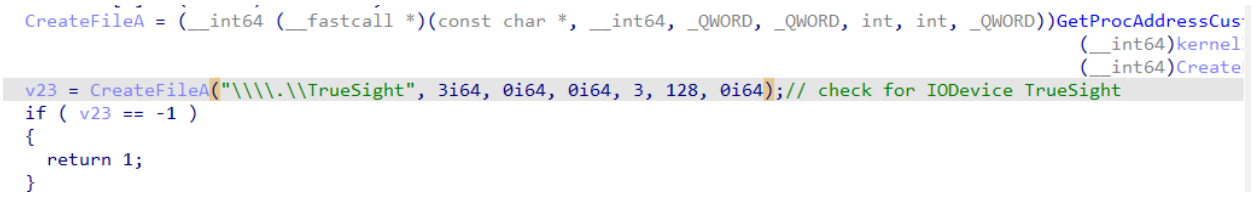


```
0000000000378C68 3000D71E6BD2DEAB «ÞÒk.x.0
0000000000378C70 0000000000378F70 p.7..... L"mcsagent.exe"
0000000000378C78 000000000000000C ........
0000000000378C80 000000000000000C ........
0000000000378C88 BAADF00DBAADF00D .ð.°.ð.°
0000000000378C90 0000000000378DE0 à.7..... L"mpdefendercoreservice.exe"
0000000000378C98 0000000000000019 ........
0000000000378CA0 0000000000000019 ........
0000000000378CA8 BAADF00DBAADF00D .ð.°.ð.°
0000000000378CB0 0000000000378EC0 À.7..... L"sophosfimservice.exe"
0000000000378CB8 0000000000000014 ........
```

Il recherche ensuite un service nommé "**truesight**" qui est lié à un logiciel "**RogueKiller**", développé par Adlice Software dans le cadre de son programme anti-malware gratuit.

```
strcpy(v21.m128i_i8, "Advapi32.dll");
strcpy(si128.m128i_i8, "OpenServiceA");
OpenServiceA = (__int64 (__fastcall *)(__int64, __int64, __int64))GetProcAddressCustom((__int64)&v21, (
v1 = OpenServiceA(v3, serviceName, 0xF01FFi64);
if ( !v1 )                                  // does service "truesight" exist?
{
  strcpy(si128.m128i_i8, "CreateServiceA");   // else create new service
  strcpy(v21.m128i_i8, "Advapi32.dll");
  CreateServiceA = (__int64 (__fastcall *)(__int64, __int64, __int64, __int64, int, int, _DWORD, const
  v1 = CreateServiceA(
         v3,
         serviceName,
         serviceName,
         0xF01FFi64,
         1,
         3,
         0,
         "C:\\truesight.sys",
         0i64,
         0i64,
         0i64,
         0i64,
         0i64);
```

Si le service "**truesight**" existe, il continuera jusqu'à la fin du processus, sinon, il créera un nouveau service avec le pilote situé "C:\Ntruesight.sys".



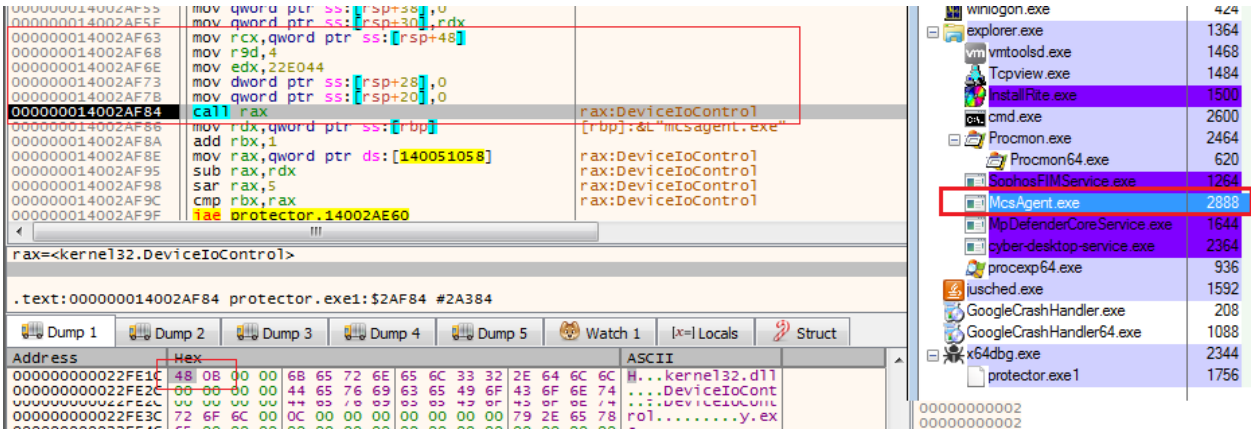
```
CreateFileA = (__int64 (__fastcall *)(const char *, __int64, _QWORD, _QWORD, int, int, _QWORD))GetProcAddressCus
                                                                                              (__int64)kernel
                                                                                              (__int64)Create
v23 = CreateFileA("\\\\.\\TrueSight", 3i64, 0i64, 0i64, 3, 128, 0i64);// check for IODevice TrueSight
if ( v23 == -1 )
{
  return 1;
}
```

Ensuite, il vérifiera la présence du dispositif nommé "**\NTrueSight**" en utilisant **CreateFileA**.

Cela donne un accès et un contrôle directs au pilote.

```
DeviceIOControl = (void (__fastcall *)(__int64, __int64, int *, __int64, _Q
DeviceIOControl(hDevice, 0x22E044i64, &pid, 4i64, 0i64, 0, &v24, 0i64);
```

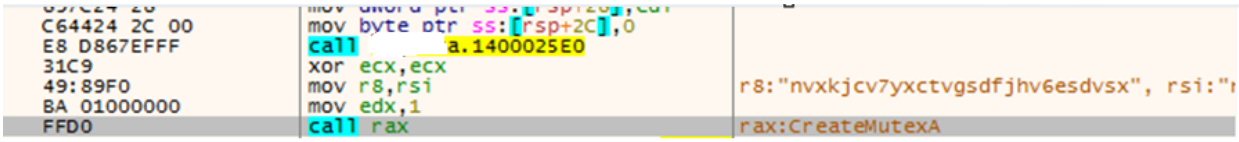
Enfin, en utilisant le **DeviceIOControl** avec un code de **0x22E044**, il peut mettre fin au processus cible en transmettant l'ID du processus (pid).



Une fois le processus cible terminé, il se met en veille, puis continue à vérifier les processus trouvés s'ils sont en cours d'exécution et les termine s'ils existent toujours.

Analyse du ransomware Nitrogen:

Par défaut, le rancongiciel crée un mutex nommé "**nvxkjcv7yxctvgsdfjv6esdvsx**". En utilisant le paramètre "**-no-mutex"**, il empêche la création de ce mutex et n'autorise qu'une seule instance du ransomware à être exécutée en même temps.

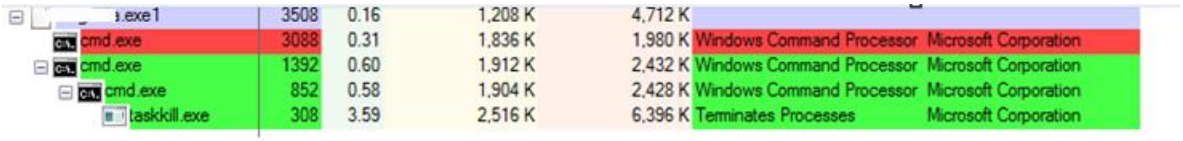


Le paramètre ***-sd-killer-off*** est utilisé pour désactiver l'arrêt des processus, car ces activités prennent quelques secondes.

```
if ( (unsigned __int8)is_sd_killer_off() )
  kill_processes_services();
```

Il utilise l'API "système" pour exécuter deux commandes.

Il crée de multiples processus engendrant **taskkill.exe** qui met fin aux processus liés aux produits Antivirus et de sécurité.



L'arbre des processus montre l'apparition de **cmd.exe** et de **taskkill.exe** qui terminent les processus.

```
ChangeServiceConfigA(
  hService,
  SERVICE_NO_CHANGE,
  SERVICE_DISABLED,
  0xFFFFFFFF,
  0i64,
  0i64,
  0i64,
  0i64,
  0i64,
  0i64,
  0i64);
CloseServiceHandle(v6);
CloseServiceHandle(v4);
sub_14010B900((__int64)L"Service %s disabled successfully.\n", v1[2]);
```

Le rancongiciel utilise également l'API **ChangeServiceConfigA** pour désactiver les services liés à l'antivirus, à la base de données et aux sauvegardes afin de crypter avec succès les fichiers liés à ces services.

Voici les AV/EDR et autres produits de sécurité qui sont arrêtés ou empêchés de fonctionner par le rançongiciel.

- Sophos
- Symantec
- McAfee
- Avast
- Défenseur
- Malwarebytes
- Windows Defender
- BitDefender
- Spyhunter
- Kaspersky
- SentinelOne

Sauvegarde et récupération

- Acronis

- Symantec
- Veeam
- SQL Safe
- Bases de données

Microsoft SQL Server
- MySQL
- IBM DB2
- Oracle
- Serveurs de courrier électronique
- Microsoft Exchange

Virtualisation et Cloud
- VMWare
- BlueStripe
- ProLiant

Accès et surveillance à distance
- Alerter
- Journal de bord
- UI0Detect
- WinVNC4

Outils d'accès en nuage et à distance
- TeamViewer
- VNC
- Google

Navigateurs web
- Firefox
- Chrome

Logiciels de bureautique et de productivité
- Microsoft Office

Pour le paramètre "**-exit-safe-boot**", le ransomware modifie les configurations du chargeur de démarrage à l'aide de l'outil Windows intégré **bcdedit.exe** pour désactiver le mode de récupération et le mode sans échec.

```
if ( (unsigned __int8)is_exit_safe_boot() )
{
  system("bcdedit /deletevalue {default} safeboot");// delete safeboot
  system("shutdown -r -t 0");
}
```

En ce qui concerne les modes de chiffrement utilisés par le rançongiciel, nous avons observé qu'ils sont similaires au code source de Conti qui a fait l'objet d'une fuite.

```
if (EncryptMode) {

	if (!plstrcmpiW(EncryptMode, OBFW(L"all"))) {

		g_EncryptMode = ALL_ENCRYPT;
		global::SetEncryptMode(g_EncryptMode);

	}
	else if (!plstrcmpiW(EncryptMode, OBFW(L"local"))) {

		g_EncryptMode = LOCAL_ENCRYPT;
		global::SetEncryptMode(g_EncryptMode);

	}
	else if (!plstrcmpiW(EncryptMode, OBFW(L"net"))) {

		g_EncryptMode = NETWORK_ENCRYPT;
		global::SetEncryptMode(g_EncryptMode);

	}
	else if (!plstrcmpiW(EncryptMode, OBFW(L"backups"))) {

		g_EncryptMode = BACKUPS_ENCRYPT;
		global::SetEncryptMode(g_EncryptMode);

	}
```

Extrait de code de Conti

Modes de cryptage :

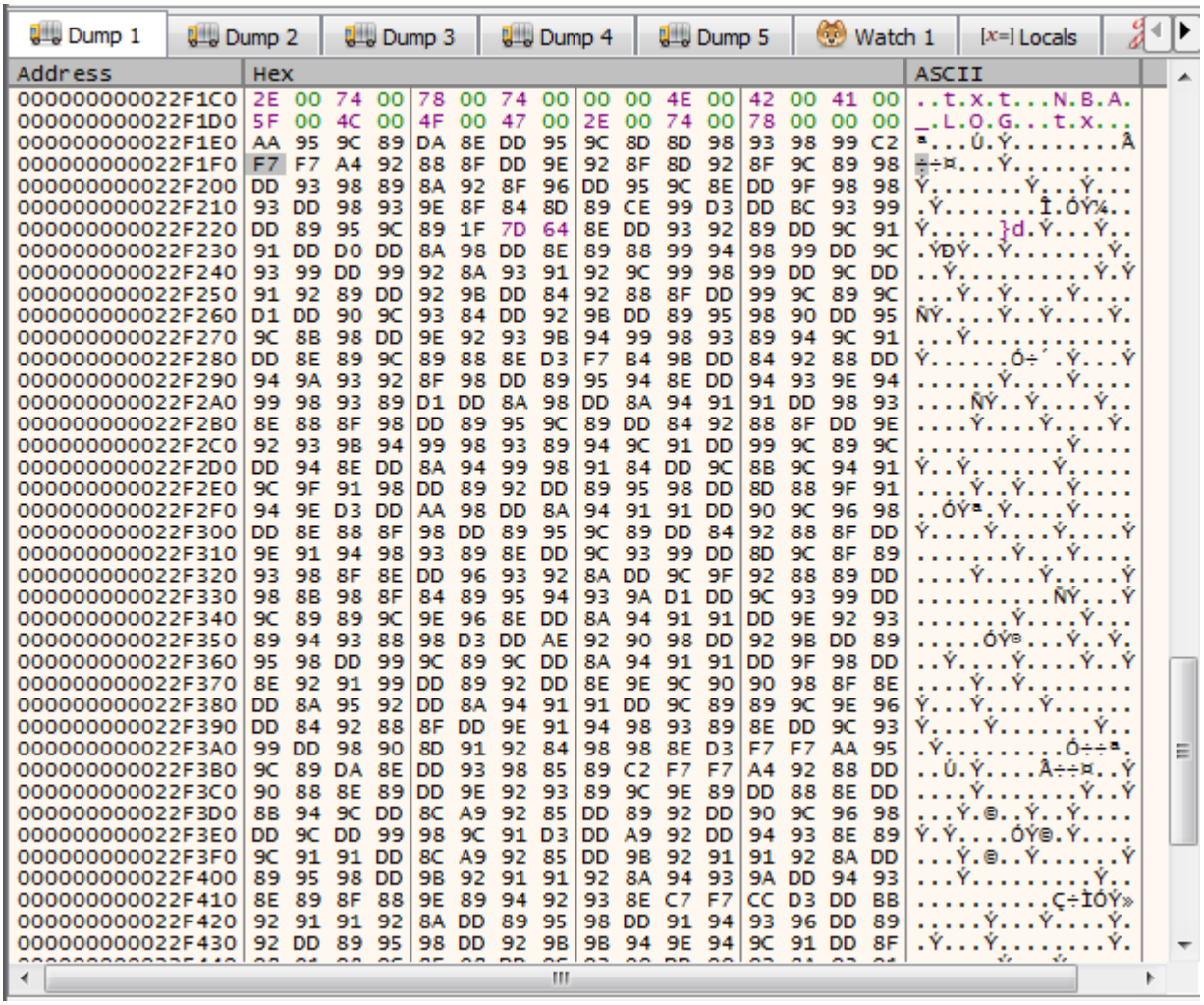
```
if ( ((unsigned int)mode_encryption() == 11 || (unsigned int)mode_encryption() == 10) && (unsigned int)get_drives(v14) )
{                                       // -m local or -m all
  for ( i = v14[0]; i; i = *(_QWORD *)(i + 32) )
  {
    v13 = *(_QWORD *)(i + 8);
    drive_path.m128i_i64[0] = (__int64)&v16;
    sub_140033F30(drive_path.m128i_i64, *(_WORD **)i, *(_QWORD *)i + 2 * v13);
    encryption((unsigned __int16 **)&drive_path);
    sub_1400F32B0((void **)&drive_path);
  }
}
```

Pour le mode ***local*** et ***all***, le rançongiciel vérifie si la valeur par défaut est 11 (local) ou 10 (all), puis il chiffre les fichiers dans tous les lecteurs.

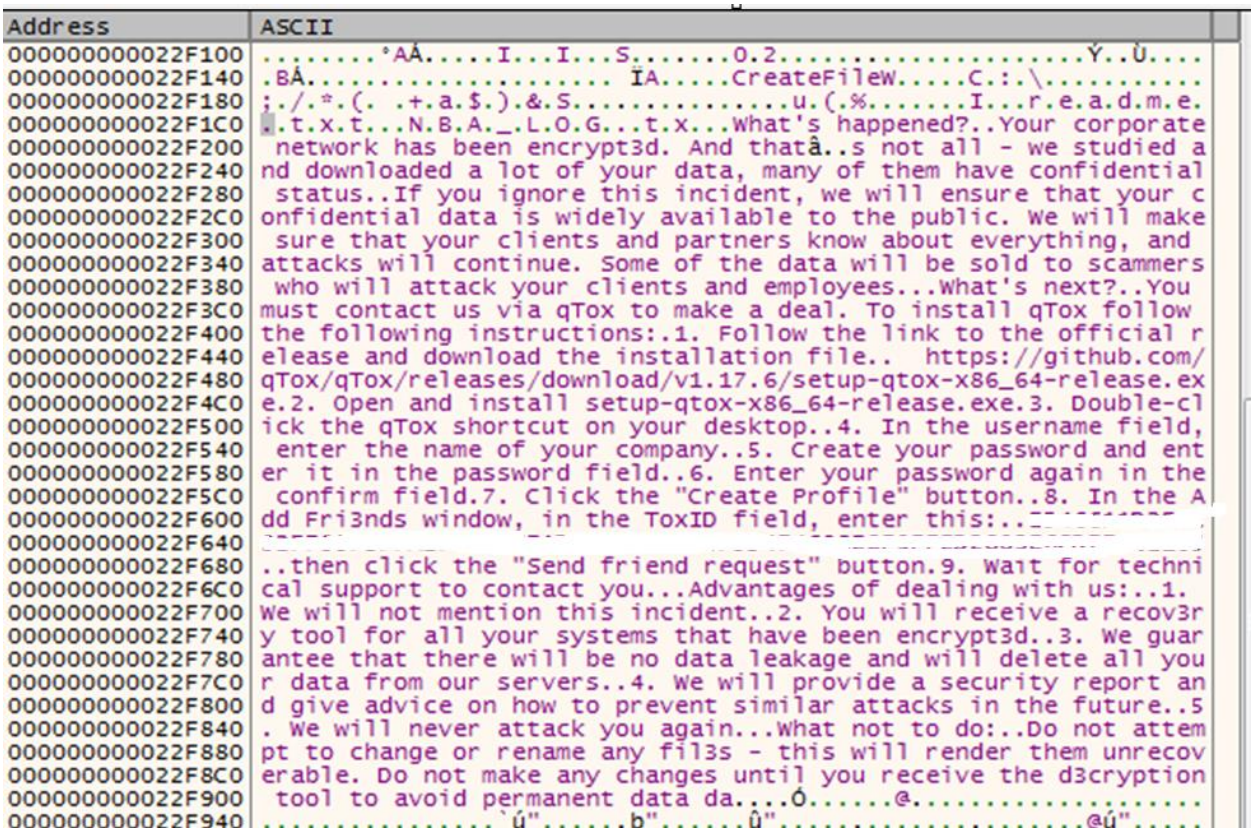
Address	Hex	ASCII
000000000022F1B4	72 00 65 00 61 00 64 00 6D 00 65 00 2E 00 74 00	r.e.a.d.m.e...t.
000000000022F1C4	78 00 74 00 00 00 4E 00 42 00 41 00 5F 00 4C 00	x.t...N.B.A._.L.
000000000022F1D4	4F 00 47 00 2E 00 74 00 78 00 00 00 00 00 3D 00	O.G...t.x.....=.
000000000022F1E4	00 00 00 00 B0 0D 00 00 00 00 00 00 08 F6 22 00	....°.........ö".

```
0000000140011C5F    45:31C9                 xor r9d,r9d
0000000140011C62    45:31C0                 xor r8d,r8d
0000000140011C65    BA 00000040             mov edx,40000000
0000000140011C6A    48:89D9                 mov rcx,rbx                 rcx:L"C:\\readme.txt", rbx:L"C:\\readme.txt"
0000000140011C6D    48:C74424 30 00000000   mov qword ptr ss:[rsp+30],0
0000000140011C76    C74424 28 00000000      mov dword ptr ss:[rsp+28],0
0000000140011C7E    C74424 20 02000000      mov dword ptr ss:[rsp+20],2
0000000140011C86    FFD0                    call rax                    rax:CreateFileW
```

Le rançongiciel crée ensuite une note de rançon nommée "**readme.txt**" à l'aide de l'API **CreateFileW.**

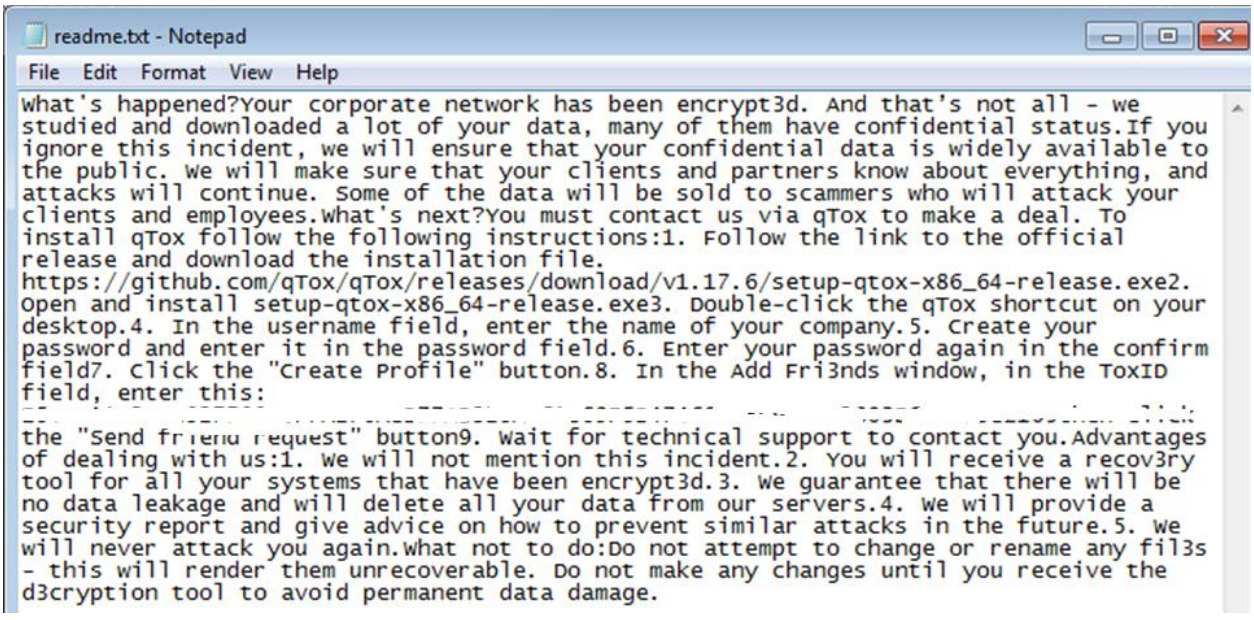


Note de rançon chiffrée



Address	ASCII
000000000022F100	........°AÁ.....I...I...S.......O.2.....................Ý..Ù....
000000000022F140	.BÁ..................... ÏA.....CreateFileW.....C.:.\..........
000000000022F180	;./.*.(. .+.a.$.).&.S..............u.(.%.......I...r.e.a.d.m.e.
000000000022F1C0	.t.x.t...N.B.A._.L.O.G...t.x...What's happened?..Your corporate
000000000022F200	network has been encrypt3d. And thatâ..s not all - we studied a
000000000022F240	nd downloaded a lot of your data, many of them have confidential
000000000022F280	status..If you ignore this incident, we will ensure that your c
000000000022F2C0	onfidential data is widely available to the public. We will make
000000000022F300	sure that your clients and partners know about everything, and
000000000022F340	attacks will continue. Some of the data will be sold to scammers
000000000022F380	who will attack your clients and employees...What's next?..You
000000000022F3C0	must contact us via qTox to make a deal. To install qTox follow
000000000022F400	the following instructions:.1. Follow the link to the official r
000000000022F440	elease and download the installation file.. https://github.com/
000000000022F480	qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.ex
000000000022F4C0	e.2. Open and install setup-qtox-x86_64-release.exe.3. Double-cl
000000000022F500	ick the qTox shortcut on your desktop..4. In the username field,
000000000022F540	enter the name of your company..5. Create your password and ent
000000000022F580	er it in the password field..6. Enter your password again in the
000000000022F5C0	confirm field.7. Click the "Create Profile" button..8. In the A
000000000022F600	dd Fri3nds window, in the ToxID field, enter this:..[redacted]
000000000022F640	[redacted]
000000000022F680	..then click the "Send friend request" button.9. Wait for techni
000000000022F6C0	cal support to contact you...Advantages of dealing with us:..1.
000000000022F700	We will not mention this incident..2. You will receive a recov3r
000000000022F740	y tool for all your systems that have been encrypt3d..3. We guar
000000000022F780	antee that there will be no data leakage and will delete all you
000000000022F7C0	r data from our servers..4. We will provide a security report an
000000000022F800	d give advice on how to prevent similar attacks in the future..5
000000000022F840	. We will never attack you again...What not to do:..Do not attem
000000000022F880	pt to change or rename any fil3s - this will render them unrecov
000000000022F8C0	erable. Do not make any changes until you receive the d3cryption
000000000022F900	tool to avoid permanent data da....Ó.....@.....
000000000022F940	..... `ú".....b".....û".....@ú".....

Note de rançon déchiffrée



readme.txt - Notepad

File Edit Format View Help

what's happened?Your corporate network has been encrypt3d. And that's not all - we studied and downloaded a lot of your data, many of them have confidential status.If you ignore this incident, we will ensure that your confidential data is widely available to the public. We will make sure that your clients and partners know about everything, and attacks will continue. Some of the data will be sold to scammers who will attack your clients and employees.What's next?You must contact us via qTox to make a deal. To install qTox follow the following instructions:1. Follow the link to the official release and download the installation file.
https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe2. Open and install setup-qtox-x86_64-release.exe3. Double-click the qTox shortcut on your desktop.4. In the username field, enter the name of your company.5. Create your password and enter it in the password field.6. Enter your password again in the confirm field7. Click the "Create Profile" button.8. In the Add Fri3nds window, in the ToxID field, enter this:
[redacted]
the "Send friend request" button9. Wait for technical support to contact you.Advantages of dealing with us:1. We will not mention this incident.2. You will receive a recov3ry tool for all your systems that have been encrypt3d.3. We guarantee that there will be no data leakage and will delete all your data from our servers.4. We will provide a security report and give advice on how to prevent similar attacks in the future.5. We will never attack you again.What not to do:Do not attempt to change or rename any fil3s - this will render them unrecoverable. Do not make any changes until you receive the d3cryption tool to avoid permanent data damage.

Note de rançon

Le rancongiciel tient une liste de dossiers qu'il ne chiffre pas:

- $Recycle.Bin
- tmp
- winnt
- temp
- pouce
- $RECYCLE.BIN
- Informations sur le volume du système
- Botte
- Fenêtres
- Trend Micro
- perflogs

Le ransomware ne chiffre pas les fichiers ayant les extensions suivantes :

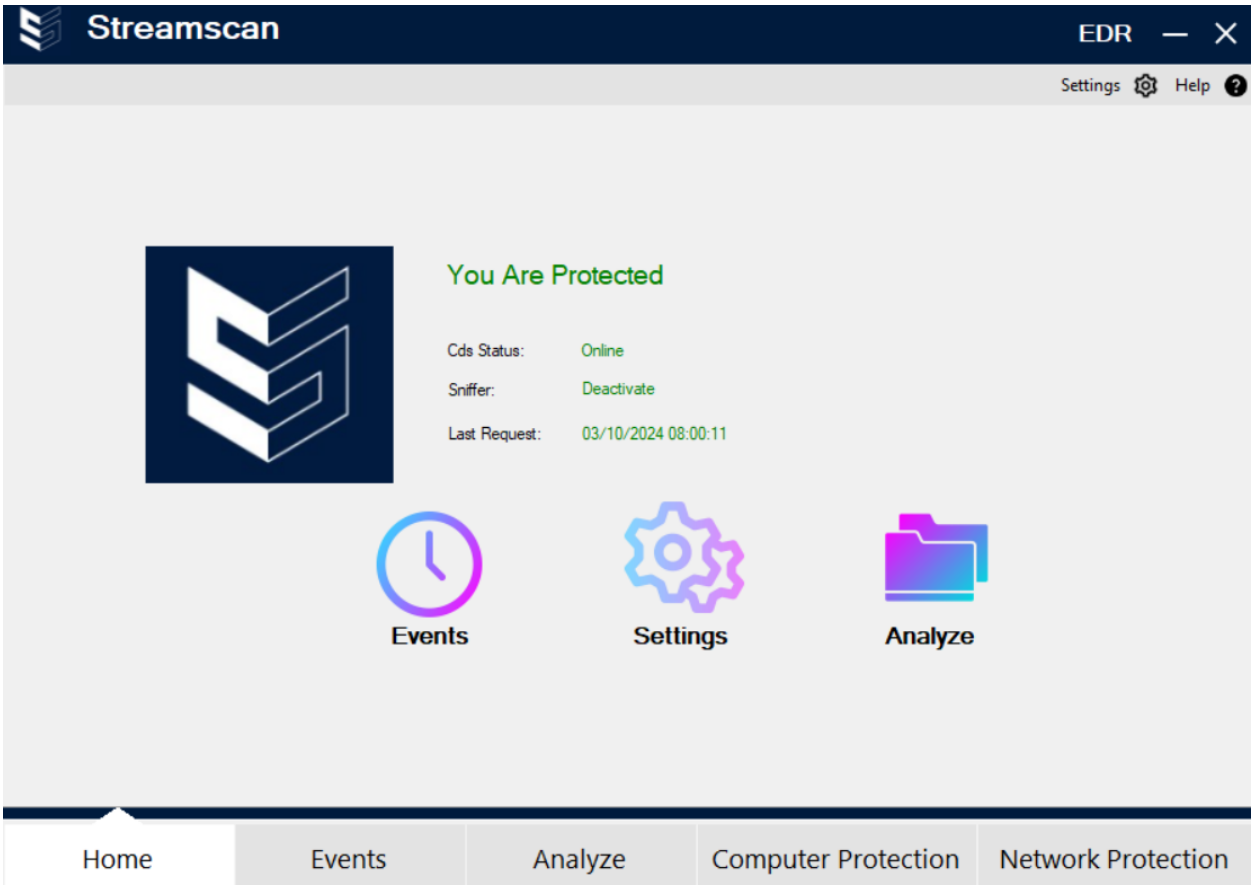
- *.exe
- *.dll
- *.lnk
- *.sys
- *.msi
- readme.txt
- NBA_LOG.txt
- *.bat

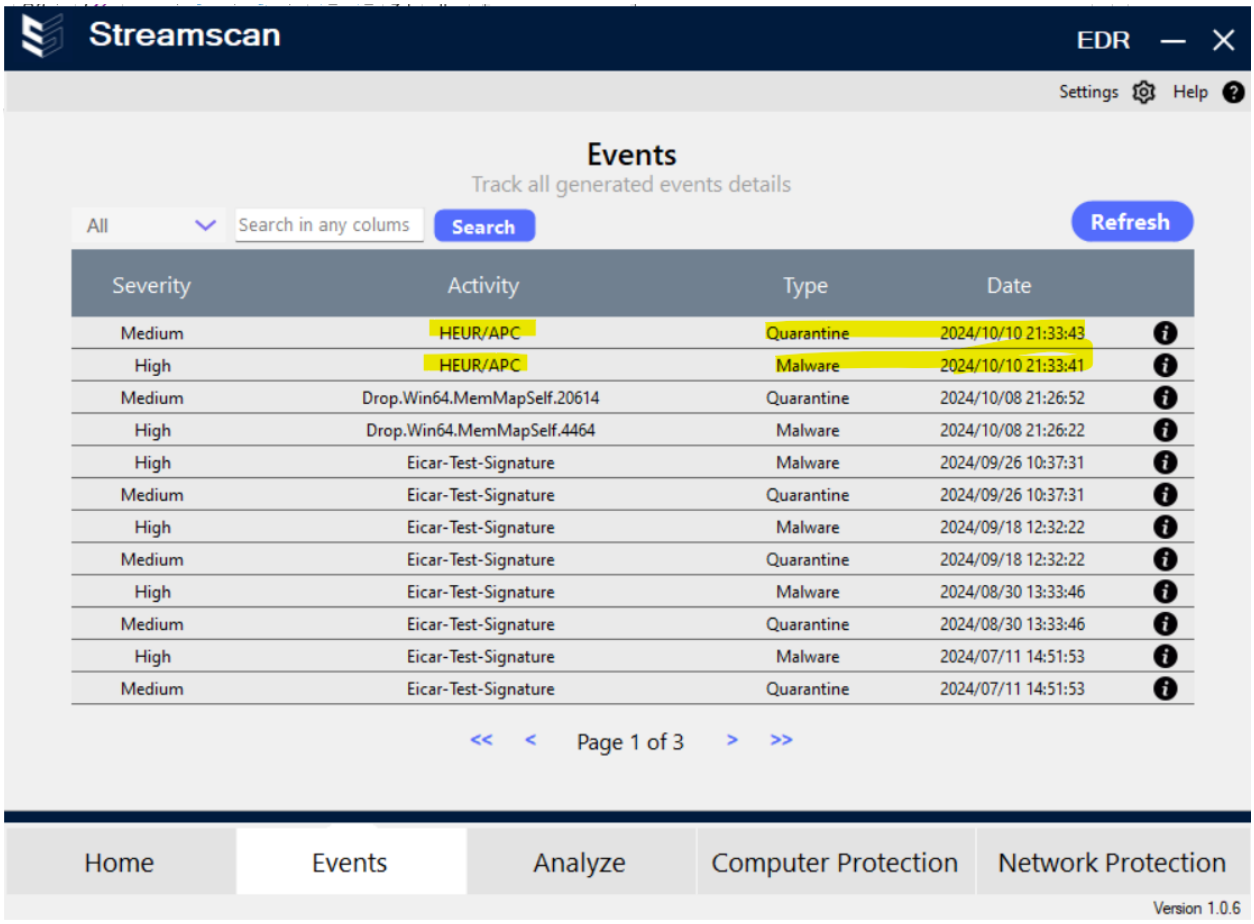
Chiffrement des fichiers

Les fichiers chiffrés par le rançongiciel ont l'extension ***.NBA**.

Détection et blocage du rançongiciel Nitrogen par notre EDR Streamscan

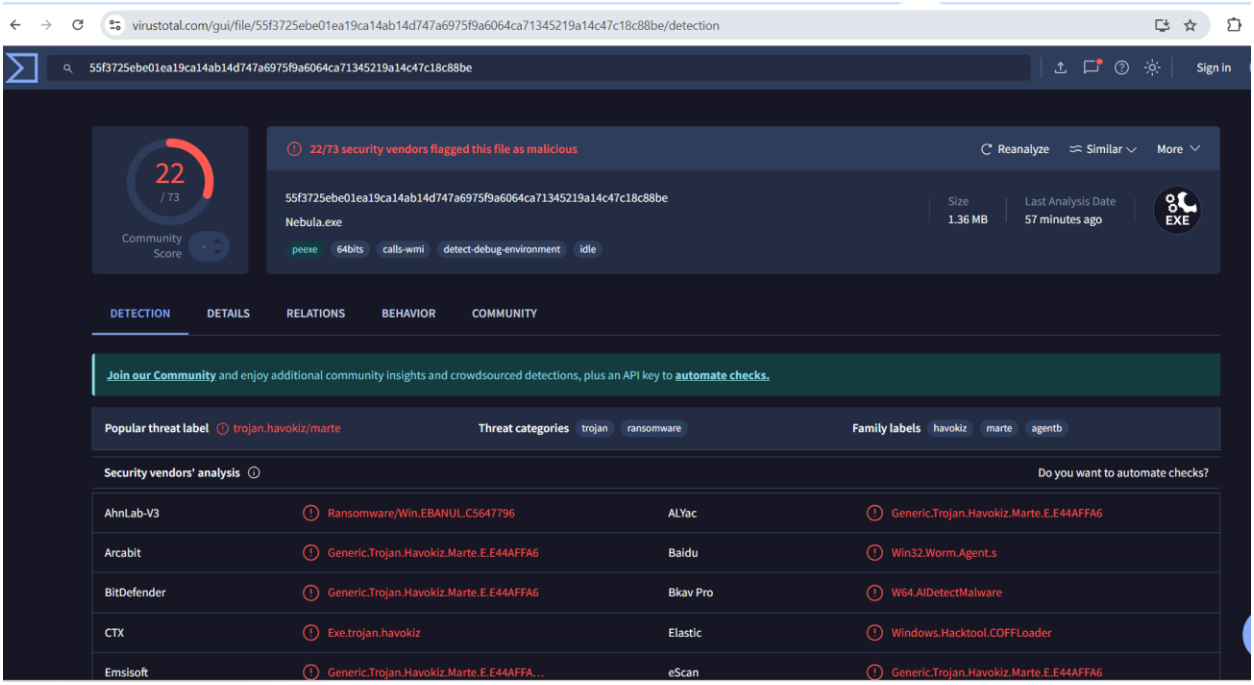
Nous avons analysé le rançongiciel via Streamscan EDR qui l'a détecté et mis en quarantaine.




Streamscan
EDR
Settings
Help
Events
Track all generated events details
All
Search in any colums
Search
Refresh
Severity
Activity
Type
Date
Medium HEUR/APC Quarantine 2024/10/10 21:33:43
High HEUR/APC Malware 2024/10/10 21:33:41
Medium Drop.Win64.MemMapSelf.20614 Quarantine 2024/10/08 21:26:52
High Drop.Win64.MemMapSelf.4464 Malware 2024/10/08 21:26:22
High Eicar-Test-Signature Malware 2024/09/26 10:37:31
Medium Eicar-Test-Signature Quarantine 2024/09/26 10:37:31
High Eicar-Test-Signature Malware 2024/09/18 12:32:22
Medium Eicar-Test-Signature Quarantine 2024/09/18 12:32:22
High Eicar-Test-Signature Malware 2024/08/30 13:33:46
Medium Eicar-Test-Signature Quarantine 2024/08/30 13:33:46
High Eicar-Test-Signature Malware 2024/07/11 14:51:53
Medium Eicar-Test-Signature Quarantine 2024/07/11 14:51:53
<< < Page 1 of 3 > >>
Home
Events
Analyze
Computer Protection
Network Protection
Version 1.0.6

Analyse du rancongiciel via Virustotal

Nous avons analysé le rançongiciel via Virustotal le **10 octobre 2024**. C'était la 1ere fois que ce fichier était analysé via Virustotal. 22 antivirus sur 73 ont été capables de le détecter sur Virustoal.



Références

- https://github.com/ph4nt0mbyt3/Darkside
- https://www.halcyon.ai/blog/halcyon-identifies-new-ransomware-operator-volcano-demon-serving-up-lukalocker

STREAMSCAN

Cet article vous a été présenté par **Streamscan**. Notre solution de détection et réponse gérées (DRG) combine notre technologie de détection de cybermenaces **CDS** basée sur l'AI, notre **EDR** et le soutien de notre équipe de chasseurs de cybermenaces, pour fournir la sécurité réseau dont votre organisation a besoin.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment StreamScan peut vous aider à protéger votre entreprise ou votre organisation

Courriel : info@streamscan.ai

Tel : 1 877 208-9040

-