

ANALYSE

RANCONGICIEL SPACECOLON

JAN 2025 //

Introduction

Le présent rapport concerne l'analyse d'un binaire malicieux qui se trouve être un ransomware. Les détails sur le fichier sont :

- Nom : **auto.exe**
- Hash SHA 1 = 28d0d07c190fd9827560d3e59dd70a8a26392f82
- Hash MD5 : c6c413543a540df9e8bba36aae7518e1
- Taille: 6.37 MB (6674944 bytes)

L'objectif de l'analyse (rétro-ingénierie de code malicieux) est de mieux comprendre ce rançongiciel ainsi que son comportement. Nos analyses lient ce ransomware au groupe Space Colon. Il se peut aussi qu'il soit distribué sur d'autres noms.

Analyse statique du ransomware

Ce ransomware est une application GUI écrite avec Delphi. D'après nos recherches, l'échantillon le plus ancien de ce ransomware est apparu en mars 2023.

La manière la plus simple de traiter les fichiers binaires Delphi est d'utiliser Interactive Delphi Reconstructor (IDR), qui analyse avec précision les structures de données internes et les types de fichiers binaires. Il permet également d'inspecter l'interface graphique sans exécuter l'application.

Le point d'entrée de l'interface graphique serait l'événement Form1.OnCreate qui est commun aux applications basées sur l'interface graphique. Par défaut, la fonction S & E, qui signifie rechercher et crypter, procède automatiquement au cryptage.

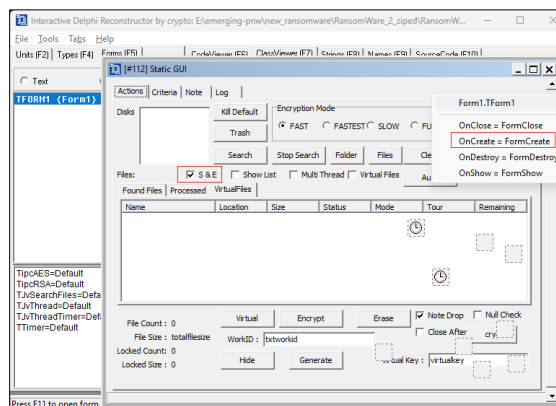


Figure 1: En utilisant l'inspection sans tête de l'IDR, nous pouvons visualiser l'interface graphique et les propriétés et antécédents de ses composants.

Initialisation :

Pendant l'initialisation du ransomware, la note de rançon est décodée en mémoire à l'aide du schéma de codage base64. Plus tard, un fichier nommé ".id_rsa" situé dans "C:\NUsers\NDesertSun" qui est

potentiellement la machine de l'acteur de la menace, cependant, aucune corrélation n'a été trouvée en rapport avec le nom d'utilisateur "DesertSun". Le nom de fichier ".id_rsa" est un nom par défaut utilisé par SSH lors de la génération d'une paire de clés. Comme il n'existe pas sur le système, il est simplement ignoré pendant l'exécution, mais pendant le débogage, il soulève une exception qui provoque le plantage du programme.

```

(*(*v3 + 28))(v3, &v23, *v3); // get encoded ransom note
r_decode_ransom_note(v23, &v24, v3, a2, a3); // decoded ransom note
(*(*v3 + 48))(v3, v24);
v4 = sub_475380(v16);
ExceptionList = &savedregs;
v14[1] = &loc_6F7CDF;
v14[0] = NtCurrentTeb()->NtTib.ExceptionList;
__writefsdword(0, v14);
>(*v4->load_from_file + 27))(v4, L"c:\\Users\\DesertSun\\.id_rsa");// load_from_file
__writefsdword(0, v14[0]);
dword_7F97B0 = sub_6FE63C(v16, &byte_6EF438, -1LL);
LOBYTE(v5) = 1;
dword_7F97AC = sub_6FE008(-1LL, &byte_6EC0F4, v5, 10);// TThreadedQueue<System.String>
LOBYTE(v6) = 1;
dword_7F97B8 = sub_5472EC(VMT_546654_TCriticalSection, v6);
n_threads = sub_6FEFA0(v16);
sub_57E758>(*v26 + 1084), &v22); // TForm1.SizeMinUnit:TComboBox
ExceptionList = v22;
TGroupBox_GetCaption>(*v26 + 1072), &v21); // 100 - Atleast
v7 = r_str_to_int(v21);
v8 = r_size_to_byte_size(v7, ExceptionList);
r_set_min_size>(*v26 + 1300 + 784), SHIDWORD(v8), v9, SHIDWORD(v8), v8);

```

Figure 2: Form1.OnCreate - Décode la note et vérifie l'existence de "C:\NUsers\NDesertSun\N.id_rsa" et initialise les fils de discussion pour la création.

Outre l'initialisation, le ransomware a la capacité de charger un fichier personnalisé "note.txt" et des extensions à chiffrer nommées "ext.txt". Il tue également divers processus et services susceptibles de verrouiller les fichiers et d'empêcher le chiffrement des fichiers critiques. Enfin, les dossiers de la corbeille de tous les lecteurs sont effacés du lecteur "A" au lecteur "Z".

```

if ( r_is_file_exist(L"note.txt", 1) )
    ((*(*v26 + 1008) + 728) + 108)(*v26 + 1008) + 728, L"note.txt");
r_is_file_exist(L"ext.txt", 1);
r_show_process_services_list(v26);
kernel32_sleep_1(0x3E8u);
r_clear_recycle_bin(v3);
kernel32_sleep_1(0x3E8u);

```

Figure 3: Autres routines trouvées dans la fonction d'initialisation

006FD280	8D95 88FDFFFF	lea eax,dword ptr ss:[ebp-278]	[ebp-278]:L"x32dbg.exe"
006FD286	E8 DBED2FF	call auto.429198	
006FD28B	8B85 88FDFFFF	mov eax,dword ptr ss:[ebp-278]	[ebp-278]:L"x32dbg.exe"
006FD2C1	E8 2A52FFFF	call auto.6F24F0	
006FD2C6	A1 44827100	mov eax,dword ptr ds:[718244]	eax:L"x32dbg.exe"
006FD2CB	8B00	mov eax,dword ptr ds:[eax]	eax:L"x32dbg.exe"
006FD2CD	E8 1A61F4FF	call auto.6433EC	
006FD2D2	33C0	xor eax,eax	eax:L"x32dbg.exe"
006FD2D4	FA	pop edx	

Figure 4: Empêche le débogage du processus car il met fin à tous les processus qui ne figurent pas dans la liste des processus autorisés.

```

if ( v1 )
{
    hProcess = kernel32_OpenProcess(1u, 0, v11[3]);
    if ( hProcess )
    {
        v4 = &savedregs;
        v3[1] = &loc_6F25F3;
        v3[0] = NtCurrentTeb()->NtTib.ExceptionList;
        __writefsdword(0, v3);
        kernel32_TerminateProcess(hProcess, 0);
        __writefsdword(0, v3[0]);
        v4 = &loc_6F25FA;
        kernel32_CloseHandle_0(hProcess);
    }
}

```

Figure 5: Le pseudocode montre que l'énumération et l'arrêt des processus

```

v9 = advapi32_OpenServiceW(v7, v8, v12);
if ( v9 )
{
    if ( advapi32_ControlService(v9, SERVICE_CONTROL_STOP, &ServiceStatus)
        && advapi32_QueryServiceStatus(v9, &ServiceStatus) )
    {
        do
        {
            if ( ServiceStatus.dwCurrentState == 1 )
                break;
            dwCheckPoint = ServiceStatus.dwCheckPoint;
            kernel32_Sleep_1(0x1388u);
            if ( !advapi32_QueryServiceStatus(v9, &ServiceStatus) )
                break;
        }
        while ( dwCheckPoint <= ServiceStatus.dwCheckPoint );
        v16 = ServiceStatus.dwCurrentState == 1;
    }
    advapi32_CloseServiceHandle(v9);
}
advapi32_CloseServiceHandle(v7);

```

Figure 6: Enumération et arrêt d'un service à l'aide de l'API ControlService avec le code de contrôle SERVICE_CONTROL_STOP

```

LOWORD(a1) = 'A';
do
{
    (unknown_libname_87)(v5, a1);
    r_concatenate_string(&v6, v5, L"\\$Recycle.Bin\\");
    LOBYTE(v1) = 1;
    if ( r_is_dir_exist(v6, v1) )
        r_clear_recycle_bin(v6);
    ++a1;
}
while ( a1 != '[' ); // Checks until 'Z' before '['

```

Figure 7: Les dossiers de la corbeille sur tous les lecteurs sont énumérés de "A" à "Z" et l'effacent.

006F26B2	8945 EA	mov dword ptr ss:[ebp-16],eax	[ebp-16]:L"C:\\\$Recycle.Bin\\"
006F26B5	33C0	xor eax,eax	
006F26B7	8945 EE	mov dword ptr ss:[ebp-12],eax	
006F26BA	66:C745 F2 1406	mov word ptr ss:[ebp-E],614	
006F26C0	33C0	xor eax,eax	
006F26C2	8945 FC	mov dword ptr ss:[ebp-4],eax	
006F26C5	8D45 E2	lea eax,dword ptr ss:[ebp-1E]	
006F26C8	50	push eax	
006F26C9	E8 628BE5FF	call <JMP.&SHFileOperationW>	

Figure 8: Utilisation de SHFileOperationW avec la commande de suppression de fichier

006F9F67	8D55 E0	lea edx,dword ptr ss:[ebp-20]	[ebp-20]:L"*.mdf;*.1df;*.ndf;*.dbf;*.db;*.dbs;
006F9F6A	8883 FC040000	mov eax,dword ptr ds:[ebx+4FC]	
006F9F70	E8 370CE6FF	call auto.55ABAC	
006F9F75	8855 E0	mov edx,dword ptr ss:[ebp-20]	[ebp-20]:L"*.mdf;*.1df;*.ndf;*.dbf;*.db;*.dbs;
006F9F7E	8883 14050000	mov eax,dword ptr ds:[ebx+514]	
006F9F84	E8 AB40FEFF	call auto.6DE034	
006F9F89	EB 16	jmp auto.6F9FA1	
006F9F8B	8883 14050000	mov eax,dword ptr ds:[ebx+514]	
006F9F91	8880 10030000	mov eax,dword ptr ds:[eax+310]	
006F9F97	8A 0A00FF00	mov al,auto.cF1000	

edx=03637E7C L"*.mdf;*.1df;*.ndf;*.dbf;*.db;*.dbs;*.log1;*.dat;*.mdb;*.ora;*.fdb;*.wt;*.gdb;*.bak;*.backup;*.v1b;*.v auto.006FA08C

Figure 9: Analyse la liste intégrée des extensions de fichiers cibles

Chiffrement :

La ransomware utilise la bibliothèque IPWorks Encrypt, qui met en œuvre un cryptage puissant à l'aide des principales normes cryptographiques, intégrées dans sa ressource qui peut être attribuée à la Turquie selon certaines sources non confirmées.

```
module = r_load_module(result);
if ( module )
{
    IPWorksEncrypt_EvtStr = r_get_proc_address(module, "IPWorksEncrypt_EvtStr");
    IPWorksEncrypt_Stream = r_get_proc_address(module, "IPWorksEncrypt_Stream");
    IPWorksEncrypt_RSA_Create = r_get_proc_address(module, "IPWorksEncrypt_RSA_Create");
    IPWorksEncrypt_RSA_Destroy = r_get_proc_address(module, "IPWorksEncrypt_RSA_Destroy");
    IPWorksEncrypt_RSA_Set = r_get_proc_address(module, "IPWorksEncrypt_RSA_Set");
    IPWorksEncrypt_RSA_Get = r_get_proc_address(module, "IPWorksEncrypt_RSA_Get");
    IPWorksEncrypt_RSA_GetLastError = r_get_proc_address(module, "IPWorksEncrypt_RSA_GetLastError");
    IPWorksEncrypt_RSA_GetLastErrorCode = r_get_proc_address(module, "IPWorksEncrypt_RSA_GetLastErrorCode");
    IPWorksEncrypt_RSA_SetLastErrorAndCode = r_get_proc_address(module, "IPWorksEncrypt_RSA_SetLastErrorAndCode");
    IPWorksEncrypt_RSA_GetEventError = r_get_proc_address(module, "IPWorksEncrypt_RSA_GetEventError");
    IPWorksEncrypt_RSA_GetEventErrorCode = r_get_proc_address(module, "IPWorksEncrypt_RSA_GetEventErrorCode");
    IPWorksEncrypt_RSA_SetEventErrorAndCode = r_get_proc_address(
        module,
        "IPWorksEncrypt_RSA_SetEventErrorAndCode");
    IPWorksEncrypt_RSA_CheckIndex = r_get_proc_address(module, "IPWorksEncrypt_RSA_CheckIndex");
    IPWorksEncrypt_RSA_Do = r_get_proc_address(module, "IPWorksEncrypt_RSA_Do");
}
```

Figure 10: Les API d'IPWorks récoltées et utilisées pour le chiffrement

```
-----BEGIN RSA PUBLIC KEY-----
\r\nMIGJAoGBANaTwGg0UuiyRgdxFnDq89RxtkxkxIF0cZ4JLqg
M7zPIY5Agh9r2rk\r\nl8DR0aneOr+OWPBgmJiYN33fdCty1FMzan
x/WVfuENyamjZPyVqy4SS4KPLdwsZw\r\n\r\nSAkGNCieKSO4tEA
mlF4Gz+bG4FoSO1FU50BqRIK99ccSiro4MTAgMBAAE=\r\n\r\n
---END RSA PUBLIC KEY-----\r\n
```

Figure 11: Clé publique RSA

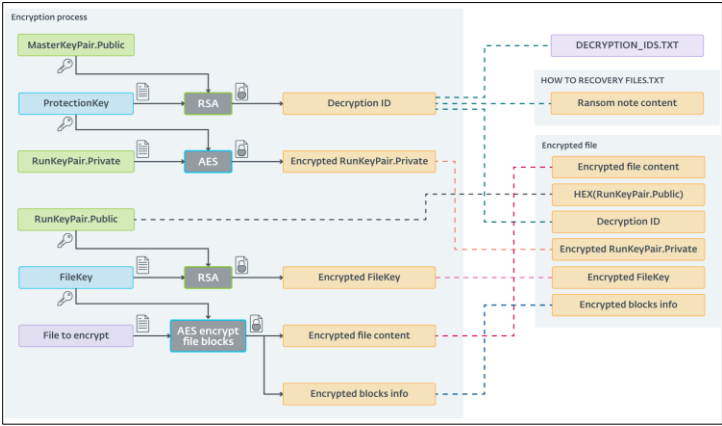


Figure 12: Schéma de cryptage complexe utilisé par Space Colon.

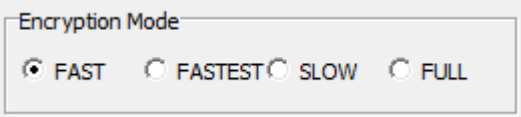


Figure 13: Modes de cryptage

Cinq modes de cryptage sont disponibles, et la plupart d'entre eux fonctionnent de la même manière, mais avec des types différents de cryptage des fichiers.

- Complet - cryptage complet
- Le plus rapide - crypte le premier 1% de la taille totale du fichier
- Cryptage rapide - intermittent
- Cryptage lent - intermittent

- Effacement - d'après l'échantillon binaire, il semble que cette fonction ne fonctionne pas comme prévu. Toutefois, si elle est utilisée, certaines parties du fichier sont remplacées par une constante qui le rend irrécupérable.

```

000B1160: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1170: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1180: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1190: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B11A0: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B11B0: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B11C0: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B11D0: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B11E0: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B11F0: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1200: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1210: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1220: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1230: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1240: 80 6A CC 5C-02 98 4B B5-80 3A 42 E8-9F E5 29 C0 Cj 0JK C: B0fo > L
000B1250: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1260: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1270: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1280: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1290: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B12A0: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B12B0: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B12C0: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B12D0: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B12E0: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B12F0: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1300: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1310: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1320: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1330: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
000B1340: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111

```

Figure 14: Exemple de cryptage intermittent en mode rapide et lent

Comme le cryptage est assez complexe, nous ne notons que les parties importantes, comme suit :

- Marqueur d'infection - TIMATOMA# ou TIMATOMAFULL# pour un cryptage complet
- ID de décryptage - Les ID peuvent être trouvés dans la note de rançon et le fichier DECRYPTION_IDS.TXT.
- Blocs cryptés - contient les décalages de début et de fin des blocs cryptés.

```

04532840: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
04532850: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
04532860: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
04532870: 31 31 31 31-31 31 31 31-31 31 31 31-31 31 31 31 1111111111111111
04532880: 54 49 4D 41-54 4F 4D 41-23 6D 30 64-37 66 55 72 TIMATOMA#0047FUF
04532890: 71 39 53 59-42 48 61 49 54 55 57-39 74 69 37 q9SYBha1e39W9t17
045328A0: 70 78 4E 46-65 63 51 67 76 76-21 56 73 62 pxNFecQggjlv/6sb
045328B0: 6A 76 30 36-62 48 56 40 42 43 42-39 2F 39 38 74 jo06hK0JBEBV/98t
045328C0: 39 68 55 74-51 55 37 57-46 23 32 44-32 44 32 44 9klt0U0F#2D2D2D
045328D0: 32 44 32 44-34 32 34 35-34 37 34 39-34 45 32 30 2D2D424547494E20
045328E0: 35 32 35 33-34 31 32 30-35 30 35 35-34 32 34 43 525341205055424C
045328F0: 34 39 34 33-32 30 34 47 47 47 47-32 44 32 44 4943204B45592D2D
04532900: 32 44 32 44-32 44 30 47 47 47 47-32 44 32 44 2D2D2D0D0A4D4947
04532910: 34 41 34 31-36 46 34 37-34 32 34 31-34 41 36 35 4A416F4742414A63
04532920: 36 35 34 39-34 34 35 33-34 32 33 37-35 41 36 35 6549445342375A65
04532930: 37 41 34 44-35 38 34 45-34 46 34 44-35 32 36 36 7A4D584E4F4D5266
04532940: 34 44 36 31-37 32 33 35-34 33 37 36-35 39 34 32 4D61723543765942
04532950: 34 39 33 39-32 49 36 49-34 45 36 46-34 34 34 35 4838286B4F6B4445

```

Figure 15: Marqueur d'infection et autres informations stockées à la fin du fichier crypté

```

04533375: 30 33 34 43-30 33 37 40-33 33 42 42-33 32 44 30 054E037F5B852B6
04533385: 44 34 35 42-45 32 43 44-30 39 30 38-32 32 42 30 D45BE2CD090822B0
04533395: 38 36 39 46-39 33 34 41-39 45 35 33-38 41 39 38 869F934A9E538A98
04533405: 31 39 36 32-36 41 37 41-41 31 39 44-41 35 39 38 19626A7A19DA598
04533415: 34 42 34 33-45 44 46 42-32 39 41 32-39 45 42 38 4B43EDFB29029F88
04533425: 46 39 42 34-32 36 37 43-23 30 3A 37-32 35 35 38 F9B4267C0:725584
04533435: 34 23 37 32-35 35 38 37-32 3A 37 32-35 35 38 34 4#7255872:725584
04533445: 23 31 34 35-31 31 37 34-34 30 37 32-35 35 38 34 #14511744:725584
04533455: 23 32 31 37-36 33 37 34-34 30 37 32-35 35 38 34 #21767616:725584
04533465: 23 32 39 30-32 33 37 30-30 30 37 32-35 35 38 34 #29023488:725584
04533475: 23 33 36 32-37 39 33 36-30 3A 37 32-35 35 38 34 #36279360:725584
04533485: 23 34 33 35-33 35 32 33-32 3A 37 32-35 35 38 34 #43535232:725584
04533495: 23 35 30 37-39 31 31 30-34 3A 37 32-35 35 38 34 #50791104:725584
04533505: 23 35 38 30-34 36 39 37-36 3A 37 32-35 35 38 34 #58046976:725584
04533515: 23 36 35 33-30 32 38 34-38 3A 37 32-35 35 38 34 #65302848:725584

```

Figure 16: Blocs cryptés commençant par le décalage zéro jusqu'à 725584 en décimal, et ainsi de suite.

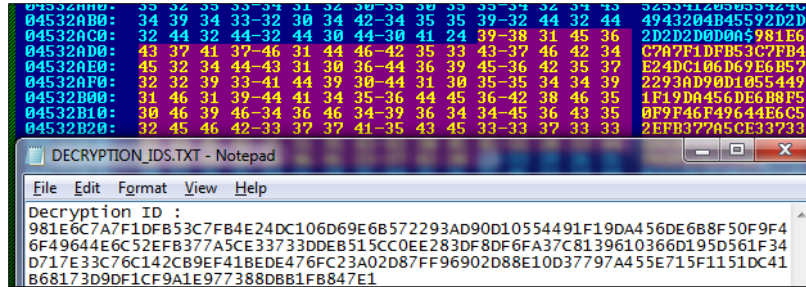


Figure 17: L'ID de décryptage ajouté au fichier crypté se trouve dans le fichier DECRYPTION_IDS.TXT.

Au cours du processus de cryptage, les noms des fichiers cryptés sont encodés en Base64 et complétés par ***.Encrypting** afin d'éviter toute réinfection. Si les fichiers sont déjà cryptés, ils sont complétés par ***.Encrypted**.

```

if ( sub_6F1BB4(v132, v128, v127) )
{
    r_concatenate_string(&v67, v128, L".Encrypted");
    LOBYTE(v30) = 1;
    v118 = sub_477604(&off_44E590, v30, v67, 2, 0x8000);
    v50 = 0LL;
    LOBYTE(v31) = 2;
    (*(v118 + 40))(v118, v31);
    sub_4732D4(v111, &v65);
    r_concatenate_string(&v66, L"TIMATOMAFULL#", v65);
}

```

Figure 18: Le mode de cryptage complet ajoute **TIMATOMAFULL#** comme marqueur, puis renomme le fichier crypté avec l'extension ***.Encrypted**.

Name	Date modified	Type	Size
setuptools-20.10.1-py2.py3-none-any.whl	6/25/2016 11:46 PM	WHL File	498 KB
pip-8.1.1-py2.py3-none-any.whl.Encrypting.MAP	11/26/2024 7:06 AM	MAP File	3 KB
pip-8.1.1-py2.py3-none-any.whl.Encrypting	6/25/2016 11:46 PM	ENCRYPTING File	1,170 KB
HOW TO RECOVERY FILES	11/26/2024 7:04 AM	Text Document	3 KB
DECRYPTION_IDS	11/26/2024 7:04 AM	Text Document	1 KB

Figure 19: ajoute l'extension ***.Encrypting** pendant le chiffrement et ajoute ***.Encrypted** une fois le chiffrement terminé, ce qui inclut également l'ajout de la note de rançon "HOW TO RECOVERY FILES.txt" et du fichier "DECRYPTION_IDS.txt"

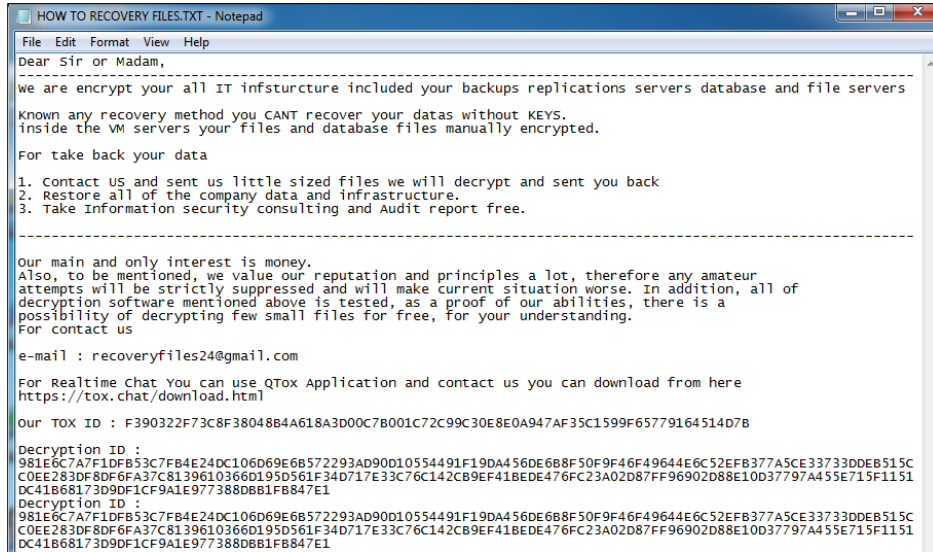


Figure 20: Note de rançon contenant les identifiants de décryptage et l'email de contact

Enfin, si la case "**Fermer après**" est cochée, un fichier batch d'autosuppression sera déposé et exécuté.

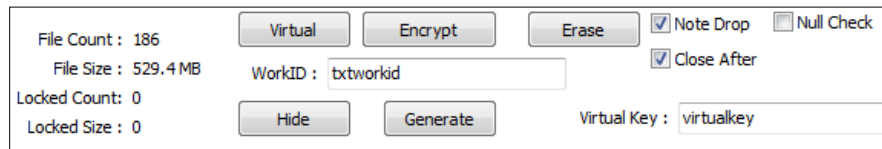


Figure 21: Interface utilisateur avec cases à cocher et autres paramètres

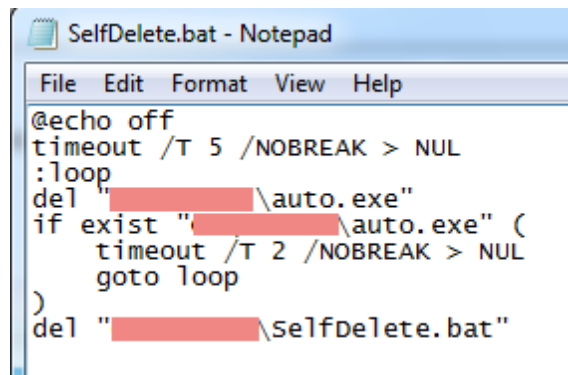
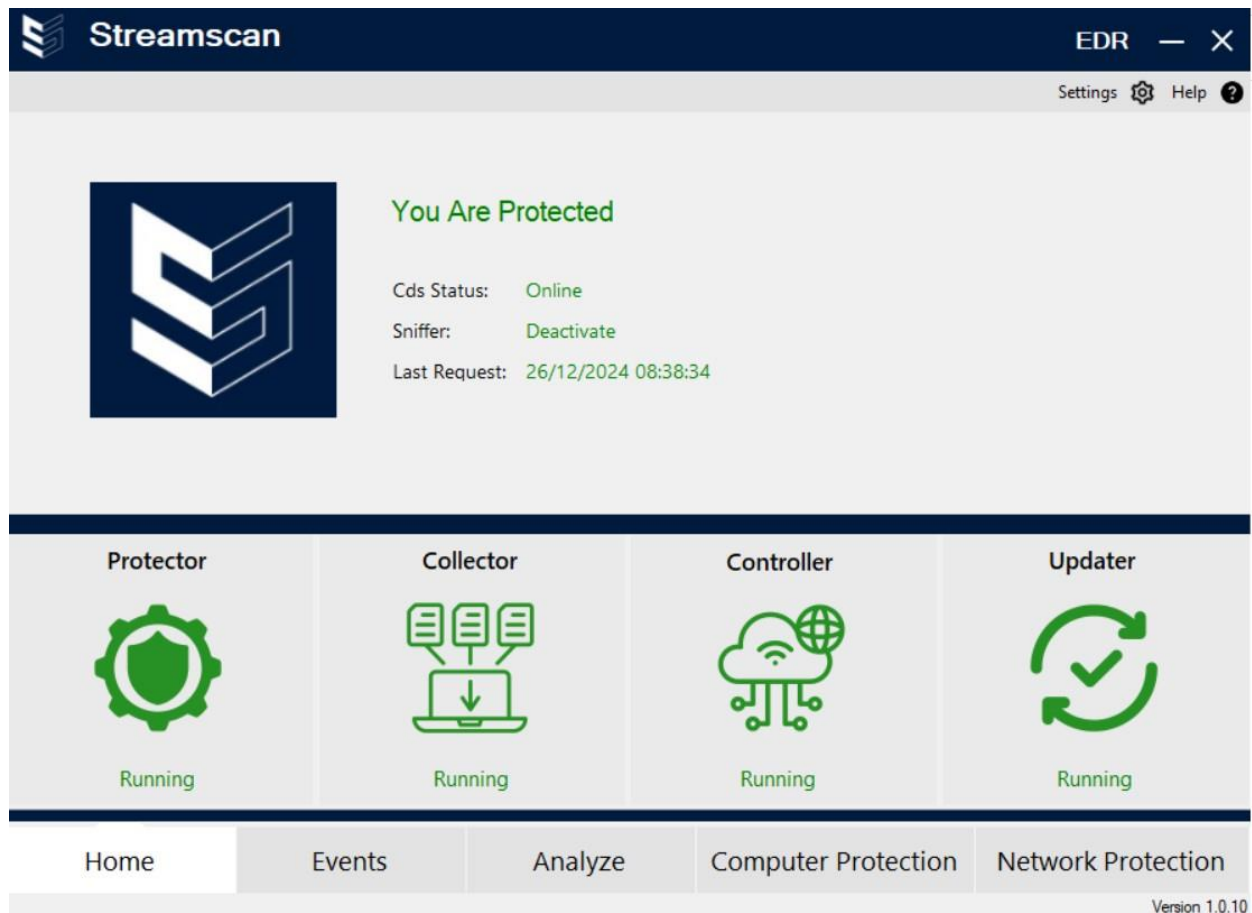


Figure 22: Auto-effacement par dépôt d'un fichier batch dans le même chemin d'accès au fichier auto.exe

Detection par notre Streamscan EDR

Ce rançongiciel est détecté et bloqué par l'EDR de Streamscan.



The screenshot displays the Streamscan EDR interface. At the top, the title bar shows 'Streamscan' and 'EDR' with window control icons. Below the title bar, there are 'Settings' and 'Help' options. The main content area features a large 'You Are Protected' message in green, accompanied by the Streamscan logo. To the right of the logo, the status is detailed: 'Cds Status: Online', 'Sniffer: Deactivate', and 'Last Request: 26/12/2024 08:38:34'. Below this, a row of four components is shown, each with an icon and the status 'Running': Protector (shield icon), Collector (laptop with data icon), Controller (cloud with globe icon), and Updater (refresh icon). At the bottom, a navigation bar includes 'Home', 'Events', 'Analyze', 'Computer Protection', and 'Network Protection'. The version number 'Version 1.0.10' is located in the bottom right corner.

Component	Status
Protector	Running
Collector	Running
Controller	Running
Updater	Running

Home | Events | Analyze | Computer Protection | Network Protection

Version 1.0.10

The screenshot displays the Streamscan EDR interface. At the top, the logo and name 'Streamscan' are on the left, and 'EDR' with window controls are on the right. Below the header, there are 'Settings' and 'Help' links. The main section is titled 'Events' with the subtitle 'Track all generated events details'. It includes a filter dropdown set to 'All', a search bar with the text 'Search in any colums', a 'Search' button, and a 'Refresh' button. A table with five columns (Severity, Activity, Type, Date, and an info icon) lists four events. The first two rows are highlighted in yellow. The bottom of the interface features a navigation bar with 'Home', 'Events', 'Analyze', 'Computer Protection', and 'Network Protection' tabs, and a version number 'Version 1.0.10' in the bottom right corner.

Severity	Activity	Type	Date	
High	TR/Ransom.qmswj	Malware	2024/12/26 15:13:08	i
Medium	TR/Ransom.qmswj	Quarantine	2024/12/26 15:13:07	i
High	Eicar-Test-Signature	Malware	2024/12/18 12:10:48	i
Medium	Eicar-Test-Signature	Quarantine	2024/12/18 12:10:47	i

Conclusion :

Il semble que Space Colon continue d'améliorer son arsenal en ajoutant des fonctions que d'autres n'ont pas encore mises en œuvre, en modifiant la logique de cryptage, mais la complexité peut provoquer des erreurs ou empêcher de récupérer les fichiers cryptés.

Annexe :

Annexe A. Extensions qui sont chiffrés par le ransomware

.mdf;.ldf;*.ndf;*.dbf;*.db;*.dbs;*.log1;*.dat;*.mdb;*.ora;*.fdb;*.wt;*.gdb;*.bak;*.backup;*.vib;*.vbk;*.vbm;*.tib;*.tibx;*.dmp;*.tuf;*.trn;*.zip;*.7z;*.rar;*.archive;*.vhd;*.vhdx;*.avhdx;*.rct;*.pst;*.sql;*.pdf;*.xlsx;*.xls;*.doc;*.docx;*.pstx;*.vmrk;*.vmx;*.fbk;*.ibd;*.myd;*.mdbx;*.d0;*.d1;*.d3;*.b1;*.bck;*.tiff;*.tif;*.dwg;*.dxf;*.lbl;*.db1;*.001;*.0001;*.seq;*.vix;*.bkf;*.gbk;*.ova;*.eml;*.ptb;*.saj;*.sko;*.skp;*.srd;*.nyf;*.itdb;*.dbc;*.edb;*.nsf;*.ib;*.db2;*.ai;*.ost;*.ostx;*.002;*.003;*.004;*.005;*.006;*.007;*.cbd;*.d2;*.d4;*.da1;*.da2;*.da3;*.da4;*.rpd;*.edp;*.vrb;*.vswp;*.idx;*.ebk;*.rpt;*.vct;*.vcx;*.cdx;*.hbp;*.msg;*.ldb;*.alt;*.dbw;*.qrp;*.upd;*.old;*.jet;*.ol2;*.sic;*.bco;*.hrl;*.a06;*.a01;*.a02;*.a03;*.bac;*.3dm;*.3dmbak;*.psd;*.jpg;*.mp4;*.mov;*.pptx;*.ppt;*.tmp;*.cdr;*.ard;*.usr;*.btr;*.qvx;*.008;*.hlp;*.sldrpt;*.SLDLFP;*.SLDPRT;*.SLDDRW;*.rfs;*.llp;*.slp;*.spl;*.one;*.SLDASM;*.gan;*.rpo;*.ntf;*.ndk;*.nbf;*.nx1;*.bik;*.dxt5_2d;*.cgd;*.tga;*.avi;*.pak;*.ms;*.danger;*.tar;*.tar.gz;*.frm;*.myi;*.accdb;*.sqlite;*.sqlite3;*.redo;*.log;*.box;*.ndx;*.nsg;*.fmp12;*.fp7;*.fp5;*.couch;*.qbw;*.qbb;*.qba;*.qbm;*.sai;*.xslm;*.indd;*.3ds;*.max;*.blend;*.qic;*.sna;*.gho;*.ghs;*.iv2i;*.pbd;*.pqb;*.afi;*.mrimg;*.spf;*.bi4;*.rbf;*.obk;*.oeb;*.rdb;*.bup;*.bkup;*.cfgbak;*.nb7;*.lst;*.cbu;*.bpf;*.ctf;*.bkip;*.fbf;*.fbw;*.ful;*.stm;*.imd;*.ibdata;*.vmsd;*.vmsn;*.csv;*.elg;*.fxl;*.mtx;*.vob;*.trc;*.arc;*.bdmp;*.dbdmp;*.df;*.vmxf;*.encvrt;*.psm;*.par;*.dft;*.asm;*.adm;*.rtf;*.sev;*.qsm;*.stp;*.mmo;*.sqlaudit;*.rman;*.arc;*.1*;*.2*;*.3*;*.4*;*.5*;*.6*;*.7*;*.8*;*.9*;*.sna;*.prt;*.tgz;*.wim;*.raw;*.pri;*.pcb;*.mat;*.pod;*.step;*.c1;*.axf;*.sldrpt;*.BBCK;*.BBCK3;*.pdb;*.full;*.diff;*.bin;*.zip

Annexe B. Le ransomware efface les extensions suivantes :

.bak ; .backup ; .vib ; .vbk ; .vbm ; .tib ; .tibx ; .vrb ; .bco ; .bucket

Annexe C. Extensions virtuelles - Extensions liées aux machines virtuelles :

.vmrk ; .vhd ; .vhdx ; .avhdx ; .vdi ; .encvrt

Annexe D. Extensions lentes :

.mdf ; .ldf ; .dbf ; .ora ; .nsf ; .ib ; .ibd ; .fdb ; .myd

Annexe E. Fichiers et extensions sur liste noire (non chiffrées)

NTUSER.dat	windows.edb	.msi
icudtl.dat	.exe	.cab
NTUSER.dat.log1	.dll	unins0
usrclass.dat	.ocx	\NFenêtres\N
usrclass.dat.log1	.sys	c:\NFenêtres
webcachev01.dat	.crypté	.bat
pouces.db	.cryptage	.com
Fichiers communs	.encrypting.map	.inf

.ini
.cmd
.drv

.reg
.nt
.ntfs

settings.dat
\\Fichiers communs
mpenginedb.db

Les CIO :

Nom de fichier/Autres	SHA1	Description
auto.exe	28d0d07c190fd9827560d3e59dd70a8a26392f82	Space Colon ransomware
%windir%\AdminArsenal\PDQDeployRunner\service-1\PDQDeployRunner-1.exe		Utilisation potentielle du PDQ Deploy pour déployer silencieusement un ransomware, comme on peut le voir dans les journaux d'événements.
procdump.exe	f4d82f11ca773a5606a2bc07add94a0cc76827ec	Possibilité d'abus de ProcDump de SysInternals en vidant la mémoire de processus critiques comme LSASS
SelfDelete.bat		Utilisé pour se supprimer lui-même.
COMMENT RECOUVRIR LES FICHIERS.txt		Note de rançon
DECRYPTION_IDS.txt		ID de décryptage
F390322F73C8F38048B4A618A3D00C7B001C72C99C30E8E0A947AF35C1599F65779164514D7B		ID TOX utilisé par l'acteur de la menace comme canal de communication
recoveryfiles24[.]gmail[.]com		Adresse électronique de l'auteur de la menace

TTPs :

Catégorie	ID	Nom	Description
Développement des ressources	T1588.002	Obtenir des capacités : Outil	L'acteur de la menace installe potentiellement le PDQ Deploy, qui a déjà été utilisé par un autre ransomware.
Exécution	T1204	Exécution par l'utilisateur	Le ransomware repose sur l'exécution par l'utilisateur, car il utilise des outils tiers qui nécessitent une interaction avec l'utilisateur.

			Ex. procdump.exe, PDQ Deploy
	T1059.003	Interprète de commandes et de scripts : Shell de commande Windows	Exécute SelfDelete.bat
Défense Evasion	T1057	Découverte du processus	Énumérer les processus et les services
	T1562.001	Affaiblir les défenses : Désactiver ou modifier des outils	Met fin aux processus ou aux services susceptibles d'empêcher le cryptage des fichiers.
	T1140	Désobfusquer/décoder des fichiers ou des informations	Les chaînes sont codées en Base64 et utilisent des algorithmes de cryptage avancés pour crypter les fichiers.
	T1070.004	Suppression des indicateurs : Suppression de fichiers	Se supprime lui-même à l'aide d'un fichier batch.
Impact	T1485	Destruction des données	Certains fichiers sont irrécupérables en raison de la logique complexe mise en œuvre sur le site , qui est sujette à des erreurs.
	T1486	Des données cryptées pour plus d'impact	Cryptage des fichiers sensibles