Sandbagility : un framework d'introspection en mode hyperviseur pour Microsoft Windows

François Khourbiga[1] et Eddy Deligne[2]
francois.khourbiga@orange.com
eddy.deligne@intradef.gouv.fr

[1] Orange Cyberdéfense
[2] DGA Maîtrise de l'Information

Résumé. *Sandbagility* est un framework en *Python* destiné à fournir une API haut-niveau pour automatiser et instrumenter un système virtuel invité fonctionnant sous Microsoft Windows n'ayant subi aucune modification. En l'occurrence, ce framework s'appuie sur les travaux publiés par Nicolas Couffin au SSTIC 2016 [5]. Les travaux en question ont donné lieu à l'implémentation d'un protocole, appelé *Fast Debugging Protocol*, en modifiant l'hyperviseur de `VirtualBox`. L'origine du framework *Sandbagility* débute là où *Winbagility* se termine. Il offre ainsi une complémentarité et une continuité des travaux précédents, tout en apportant de nouvelles fonctionnalités.

1 Introduction

Le framework a été développé dans le but d'analyser des codes malveillants. Toutefois, ses fonctionnalités ne se limitent pas à ce type d'étude et son usage peut être généralisé à n'importe quel logiciel fonctionnant sous Microsoft Windows.

Dans le domaine de l'analyse de code malveillant, on peut citer trois approches fondamentales :

- l'analyse statique du fichier, du langage machine natif ou interprété ;
- l'analyse dynamique du code malveillant [3] ;
- et l'analyse en *sandbox*.

Dans ce papier, c'est l'analyse d'un code malveillant au moyen d'une *sandbox* qui sera abordée sur la base du constat ci-après.

1.1 Problématique

Lorsqu'un code malveillant est soumis à une *sandbox*, cette dernière joue le rôle de « boîte noire », avec une ou plusieurs entrées, un processus

d'analyse et une sortie. Cette approche en « boîte noire » peut s'avérer très efficace lorsque le code malveillant n'embarque aucun mécanisme inconnu de détection ou d'évasion de *sandbox* et d'*anti-debug*.

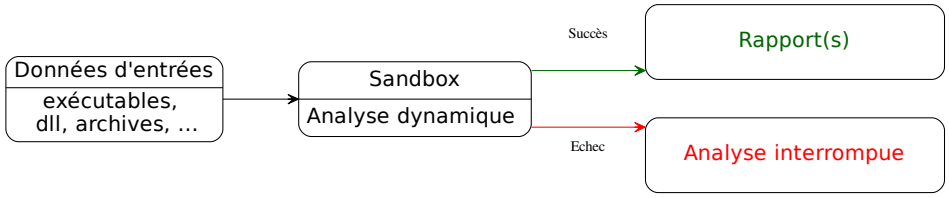

Fig. 1. Processus d'analyse en boîte noire

Cependant, lorsqu'un code malveillant met en œuvre des mécanismes de protection (*anti-debug*, détection ou évasion de *sandbox*), les informations obtenues peuvent être biaisées. Le papier *Bypassing modern sandbox technologies* [10] illustre les résultats d'expérimentations visant à contourner ou entraver l'analyse effectuée par *sandbox*.

Il n'est pas rare de constater qu'une analyse de code malveillant soit interrompue, ce qui implique des résultats incomplets, voire dans certains cas, aucun résultat. Dans ce genre de situation, il devient nécessaire pour l'analyste de procéder manuellement à l'analyse du code malveillant, avant de pouvoir adapter la *sandbox* au cas étudié.

1.2 Objectifs

Le framework *Sandbagility* a été conçu pour adresser cette problématique. Pour cela, le framework permet de :

1. fournir à l'analyste une solution intermédiaire et complémentaire, entre l'analyse automatisée (p.ex. **`Cuckoo Sandbox`**) et l'analyse dynamique (ex. **`Windbg`**) ;
2. limiter l'empreinte sur le système virtuel invité et réduire la surface de détection exposée afin d'être aussi furtif que possible ;
3. simplifier et réduire le temps d'analyse pour permettre une analyse semi-autonome ;

Analyse hybride Le positionnement du framework en tant que solution hybride permet d'alterner simplement et rapidement entre une analyse dynamique et une analyse automatisée par l'écriture de script. Pour répondre

à cette contrainte, le langage `Python` a été choisi pour le framework. Ce langage à l'avantage d'être largement utilisé par la communauté, offre de nombreux *packages* et est relativement performant. Ainsi, l'analyste peut profiter de la console `IPython` pour réaliser des opérations de manière interactive avec le système invité.

Analyse furtive Le framework *Sandbagility* souhaite limiter autant que possible son empreinte sur le système cible. De ce fait, aucun agent n'est installé sur le système cible.

Le framework s'appuie sur le protocole `FDP` pour installer des points d'arrêt totalement furtifs et pour contrôler l'exécution de la machine virtuelle.

De plus, aucune modification n'est apportée au système d'exploitation invité, notamment au démarrage par l'ajout de la directive `/DEBUG`. Ceci a l'avantage de maintenir nos capacités d'analyse face à un code malveillant complexe, en mode noyau ou qui serait destiné à contourner le mécanisme de sécurité *PatchGuard* (automatiquement désactivé en mode `/DEBUG`).

Utilisation simple Le framework *Sandbagility* a été conçu pour simplifier au maximum l'instrumentation et l'analyse d'un code malveillant, pour cela il s'appuie sur une architecture pensée pour abstraire les différents espaces d'exécution et sous-systèmes de Microsoft Windows, et rendre ces notions transparentes pour l'analyste.

Ainsi, il sera aisé de suivre l'exécution d'un code malveillant à travers tous les modes suivants :

- espace noyau ;
- espace utilisateur ;
- processus 64 bits ;
- processus 32 bits ;
- processus dans le sous-système *WoW64*.

2 État de l'art

Dans cette section, nous ferons un bref panorama des solutions existantes qui traitent de la problématique d'analyse de code malveillant.

Il existe deux approches distinctes, à savoir :

- réaliser l'introspection de la machine virtuelle à partir d'un hyperviseur comme `LibVMI` ou `pyRebox` ;
- utiliser des agents directement installés ou exécutés sur le système cible.

2.1 Définitions

VMI Dans la littérature, la notion d'introspection est intimement liée à la notion de machine virtuelle et d'hyperviseur [11], connu sous l'appellation *Virtual Machine Introspection* (`VMI`). Pour faire simple, un hyperviseur a un accès et un contrôle complet sur le système invité. Il peut avoir une vue exhaustive de l'état de la mémoire, des processeurs et être notifié lors d'actions bas-niveau, comme par exemple un accès à la mémoire en lecture, écriture ou exécution [14]

L'introspection peut donc être décrite comme l'action d'observer, depuis un environnement extérieur, l'intérieur du système que l'on souhaite analyser, dans le but d'identifier la sémantique des opérations qu'il réalise.

Agents L'autre approche consiste à modifier le système cible pour en obtenir des informations. Généralement, les modifications apportées au système invité impliquent l'installation de pilotes noyau (*drivers*) ou d'agents. Un agent peut être défini comme un programme ou un service en espace utilisateur dédié à la communication avec le système d'analyse et à l'exécution des tâches sur le système cible.

2.2 Cuckoo Sandbox

En matière d'analyse automatisée de code malveillant, `Cuckoo Sandbox` s'inscrit comme une référence [12]. Cette solution présente l'avantage d'être *Open-Source* et peut être déployée localement. Ce qui n'est pas le cas d'autres solutions qui sont proposées uniquement comme des services en ligne tels que `malwr` ou `ThreatExprt`.

Cuckoo Sandbox s'appuie sur l'installation d'agents dans le système invité pour :

- communiquer avec le système virtuel invité ;
- créer et configurer une machine virtuelle ;
- installer des *hooks* dans le système invité pour le suivi des appels de fonctions.

L'utilisation de *hooks* installés dans le système cible en mode utilisateur présente par nature une problématique en matière d'analyse de code malveillant, comme l'explique Sick Thorsten [13].

De la même façon, l'usage d'agent dans le système analysé a pour conséquence d'augmenter la surface exposée au code malveillant ainsi que le risque de détection, d'évasion et d'entrave lors de l'analyse [6].

2.3 LibVMI

`LibVMI` est une bibliothèque `C` avec des *bindings* `Python` qui facilite l'analyse bas niveau d'une machine virtuelle en cours d'exécution en affichant sa mémoire, en interceptant les événements matériels et en accédant aux registres `vCPU`. La bibliothèque `LibVMI` peut utiliser les environnements de virtualisation `KVM` et `XEN` pour étendre ses fonctionnalités en matière d'introspection [15].

Il est à noter que `LibVMI` dépend du framework `Volatility` [7] pour réaliser l'introspection d'une machine virtuelle.

2.4 DRAKVUF

`DRAKVUF` [9] est un système d'analyse automatisée de code malveillant basé sur `LibVMI` et `XEN` [2] pour réaliser l'introspection de la machine virtuelle. `DRAKVUF` s'appuie sur le framework `REKALL` pour analyser le système invité.

2.5 PyRebox

`PyRebox` [4] est une *sandbox* scriptable en `Python` dédiée à la rétroconception. `PyRebox` est basé sur `QEMU` pour fournir des capacités d'analyse dynamique et de *debug*. `PyRebox` permet d'inspecter une machine virtuelle `QEMU`, de modifier sa mémoire ou ses registres, d'en instrumenter l'exécution et offre également un *shell*.

`PyRebox` dépend également du framework `Volatility` pour réaliser l'introspection d'une machine virtuelle.

2.6 Conclusion

Les solutions présentées dans notre état de l'art sont adhérentes aux systèmes *GNU/Linux* ou *Unix* et dépendent d'un framework de forensique pour réaliser l'introspection du système invité. Le choix d'une implémentation sous Microsoft Windows va permettre à Sandbagility de profiter des fichiers de symboles fournis par Microsoft pour analyser le système invité.

3 Solution

Sandbagility est un framework `Python` d'introspection de machine virtuelle fonctionnant sous Microsoft Windows. L'introspection de la machine virtuelle est réalisée uniquement au moyen des fichiers de symboles de *debug* de Microsoft.

Il s'appuie sur une version modifiée de `VirtualBox` suite aux travaux de Nicolas Couffin [5]. Ses travaux ont donné lieu à l'implémentation d'un protocole *Fast Debugging Protocol* (`FDP`) pour permettre l'introspection d'une machine virtuelle. Le protocole `FDP` dispose d'une `API` simple et performante, avec un *binding* `Python`. En résumé, ce protocole offre :

- une interface permettant l'introspection d'une machine virtuelle au moyen d'une `API Python` ;
- la mise en place des points d'arrêts furtifs ;
- des performances élevées au moyen de plusieurs type de points d'arrêts.

3.1 Architecture

Le framework *Sandbagility* est conçu sur la base d'une architecture à trois niveaux (voir figure 2) :

- le noyau — **Core** — qui propose les primitives bas-niveau de contrôle de la machine virtuelle, des points d'arrêts, de lecture/écriture des registres et de la mémoire ;
- la couche d'abstraction — **Helper** — fournit les fonctions haut-niveau pour réaliser les opérations d'introspection et d'instrumentation du système cible (en s'appuyant sur un **OS Helper** spécifique au système virtualisé) ;
- les composants d'analyse — **Monitors/Plugins** — qui permettent de réaliser le suivi d'un code malveillant, de journaliser ses actions, d'extraire des fichiers suspects...

Core Le noyau du framework *Sandbagility* sert essentiellement de couche d'abstraction entre les fonctionnalités du framework et la méthode d'instrumentation de la machine analysée. Dans notre cas, le noyau du framework *Sandbagility* repose sur l'interface proposée par *FDP* [5]. Le *binding* `Python` de ce protocole offre toutes les primitives bas-niveau pour contrôler et réaliser l'introspection d'une machine virtuelle.

Le protocole *FDP* fournit les primitives bas-niveau qui permettent de :

- lire et écrire les registres du CPU ;
- lire et écrire la mémoire de l'invité ;
- injecter des interruptions, notamment de type *PAGE FAULT* ;
- ajouter/supprimer des points d'arrêts (*Hardware*, *Software* ou *Hyper*) ;
- exécuter en mode continu, pas-à-pas et mise en pause du système invité.

Helper L'ensemble des API de haut-niveau est implémenté ou exposé par la couche d'abstraction *helper*. Le *helper* s'appuie sur le *core* et implémente les principales fonctions pour instrumenter et introspecter à haut niveau un système invité sous Microsoft Windows. Cette introspection du système invité est réalisée par le composant **OsHelper**. Le *helper* permet de :

- gérer des points d'arrêts pour notifier des *callback* de traitement ;
- supporter des fichiers de symboles de *debug pdb* ;
- réaliser l'introspection avancée du système invité Microsoft Windows.

Dans l'exemple ci-dessous, on utilise la console **IPython** pour interagir avec le système cible en cours d'exécution. La première étape consiste à importer et instancier un *helper* pour se connecter à la machine virtuelle appelée **Windows 10 x64 - 14393** avec le protocole **FDP**. L'appel à la méthode **PsGetCurrentProcess** permet de retourner un objet représentant le processus courant.

```
In [1]: from Sandbagility.Core.FDP import FDP
In [2]: from Sandbagility.Helper import Helper
In [3]: helper = Helper('Windows 10 x64 - 14393', FDP)

In [4]: print(helper.PsGetCurrentProcess())

PROCESS fffff802c064f940
SessionId:        -1  Cid:    0    Peb:                0  ParentCid:
       0
DirBase:   1aa000  ObjectTable: ffff8e0c25401340  HandleCount: 777
Image: Idle
```

Monitors et Plugins Le dernier niveau de l'architecture du framework *Sandbagility* est constitué des composants d'analyses. Ils peuvent être de deux types : *monitor* ou *plugin* :

- un *plugin* est une extension pour *Sandbagility*, elle peut être utilisée pour instrumenter le système cible de manière plus ou moins complexe ;
- un *monitor* est un gestionnaire pour un ou plusieurs évènements sur le système d'exploitation analysé.

Dans les sections suivantes, nous présenterons quelques exemples de *plugins* et de *monitors* pour aider le lecteur à appréhender quelques cas d'utilisation du framework *Sandbagility*.

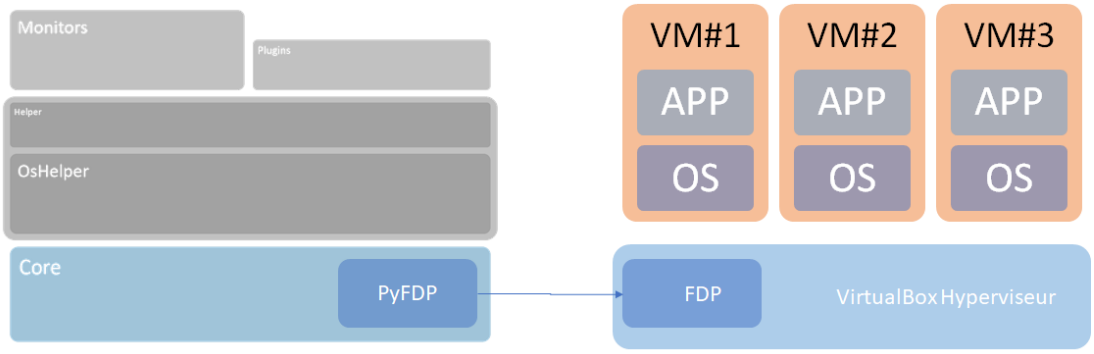

Fig. 2. Architecture du framework

Fig. 3. Sandbagility Core

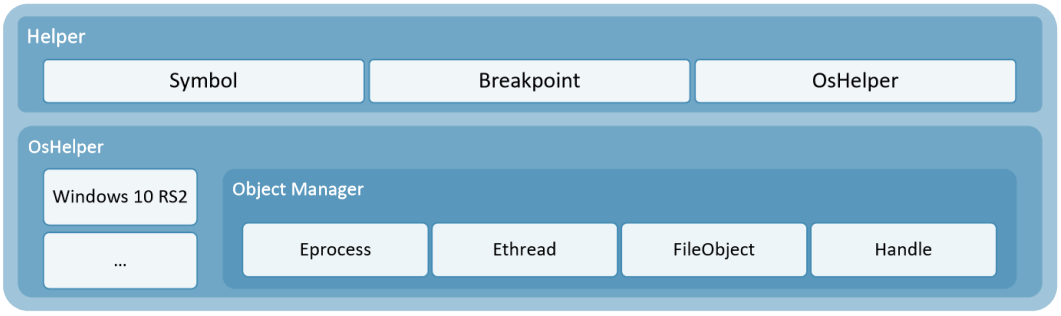

Fig. 4. Sandbagility Helper

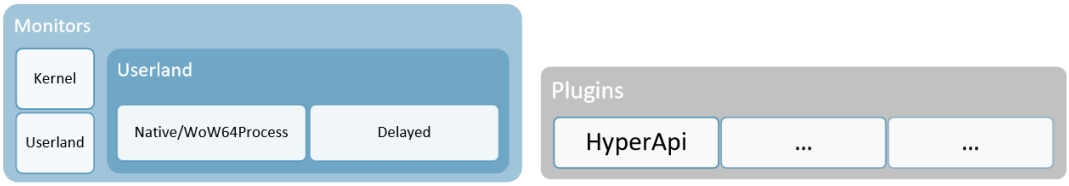

Fig. 5. Plugin et Monitor

Plugin Hypervisor based Application Programming Interface Lorsque l'on souhaite mettre en place un environnement d'analyse de type *sandbox*, il est nécessaire de réaliser certaines actions sur le système analysé, comme :

- téléverser le code malveillant et ses dépendances ;
- configurer, au besoin, le système ;
- procéder à l'exécution initiale du code malveillant.

Nous allons présenter un *plugin* destiné à automatiser l'analyse de code malveillant, sans recourir à l'installation d'agent sur le système. Ce *plugin*, appelé **HyperApi**, peut être définit comme une interface de programmation applicative basée sur l'hyperviseur. Il permet de provoquer une exécution de code arbitraire sur le système invité depuis l'hyperviseur. Pour cela, on utilise une méthode qui consiste à détourner le fil d'exécution légitime d'un processus choisi pour contrôler le flux d'exécution et réaliser des opérations arbitraires.

Pour ce faire, le *plugin* doit :

1. sauvegarder le contexte du fil d'exécution courant : pile et registres ;
2. mettre en place les paramètres en fonction des différents appels de fonctions ;
3. placer la valeur courante de l'*instruction pointer* comme adresse de retour ;
4. modifier l'*instruction pointer* pour pointer vers la fonction souhaitée ;
5. exécuter le système invité jusqu'à l'adresse de retour ;
6. récupérer la valeur de retour dans le registre **rax** ;
7. restaurer le contexte du fil d'exécution.

L'exemple ci-dessous illustre l'utilisation du *plugin* **HyperApi** pour faire appel aux **API Win32** à partir du processus **explorer.exe**. Après avoir instancié le *plugin* **HyperApi** avec le **Helper**, on fait appel à la méthode **AcquireContext** pour se placer dans le contexte du processus dans lequel on souhaite opérer les actions. Ensuite, il est possible de faire appel aux méthodes implémentées par le *plugin*, comme par exemple **WinExec** pour ouvrir ou exécuter un fichier, avant de libérer le contexte avec la méthode **ReleaseContext**.

```
In [1]: from Sandbagility.Core.FDP import FDP
   ...: from Sandbagility.Helper import Helper
   ...:
   ...: helper = Helper('Windows 10 x64 - 14393', FDP)
   ...:
   ...: from Sandbagility.Windows.HyperWin32Api import HyperWin32Api
        as HyperApi
```

```
   ...:
   ...: hapi = HyperApi(helper)

In [2]: hapi.AcquireContext('explorer.exe')

In [3]: hapi.WinExec(b'cmd.exe')
Out[3]: 33

In [4]: hapi.ReleaseContext()

In [5]:
```

Monitor Un *monitor* offre une couche d'abstraction complète du fonctionnement du système analysé pour simplifier la collecte des évènements. Pour chaque évènement, un *monitor* remonte à l'utilisateur :

- le type d'évènement, son nom, tel qu'il a été défini par le monitor ;
- de l'information associée à l'évènement en fonction de son type ;
- de l'information sur le processus qui a provoqué l'évènement.

Ci-dessous figure un exemple d'utilisation d'un *monitor* dédié à l'analyse des accès fichiers sous Windows. Dans notre cas, **`FileIoMonitor`** est enregistré pour suivre ce type d'opération associées au processus **`notepad.exe`**. Ainsi, l'utilisateur obtient les informations suivantes :

```
In [1]: from Sandbagility.Core.FDP import FDP
   ...: from Sandbagility.Helper import Helper

In [2]: helper = Helper('Windows 10 x64 - 14393', FDP)

In [3]: Notepad = helper.SwapContext('notepad.exe')

In [4]: print(Notepad)

PROCESS ffffc28abc7d32c0
SessionId:         1  Cid:  d44.538    Peb:       6eb8a31000
    ParentCid:  6d8
DirBase: 53851000  ObjectTable: ffff8e0c2c569f40  HandleCount: 166
Image: notepad.exe


In [9]: from Sandbagility.Monitors.FileIo import FileIoMonitor

In [10]: FileIoMonitor(helper, Notepad, verbose=True)
Out[10]: <Sandbagility.Monitors.FileIo.FileIoMonitor at 0
    x2a1d3e2d358>

In [11]: helper.Run()
2018-03-23 14:39:38,035 File         INFO     CreateFile  :
Process: notepad.exe, Cid:    d44.538,
{
```

```
    'lpFileName':'C:\\Windows\\Branding\\Basebrd\\Basebrd.dll',
    'dwDesiredAccess':2147483648,
    'dwShareMode':5,
    'lpSecurityAttributes':0,
    'dwCreationDisposition':472446402563,
    'dwFlagsAndAttributes':472446402560,
    'hTemplateFile':0,
    'Return':692
}
2018-03-23 14:39:38,077 File         INFO     CreateFile  :
Process: notepad.exe, Cid:    d44.538,
{
    'lpFileName':'C:\\Windows\\Branding\\Basebrd\\Basebrd.dll',
    'dwDesiredAccess':2147483648,
    'dwShareMode':5,
    'lpSecurityAttributes':0,
    'dwCreationDisposition':472446402563,
    'dwFlagsAndAttributes':472446402560,
    'hTemplateFile':0,
    'Return':696
}
2018-03-23 14:39:38,203 File         INFO     CreateFile  :
Process: notepad.exe, Cid:    d44.538,
{
    'lpFileName':'C:\\Windows\\Branding\\Basebrd\\Basebrd.dll',
    'dwDesiredAccess':2147483648,
    'dwShareMode':5,
    'lpSecurityAttributes':0,
    'dwCreationDisposition':472446402563,
    'dwFlagsAndAttributes':472446402560,
    'hTemplateFile':0,
    'Return':692
}
2018-03-23 14:39:38,233 File         INFO     CreateFile  :
Process: notepad.exe, Cid:    d44.538,
{
    'lpFileName':'C:\\Windows\\Branding\\Basebrd\\Basebrd.dll',
    'dwDesiredAccess':2147483648,
    'dwShareMode':5,
    'lpSecurityAttributes':0,
    'dwCreationDisposition':472446402563,
    'dwFlagsAndAttributes':472446402560,
    'hTemplateFile':0,
    'Return':696
}
```

L'utilisateur peut également ajouter des filtres sur les évènements, en enregistrant une *callback* sur les évènements.

```
    Monitor = FileIoMonitor(helper, Notepad)
    Monitor.RegisterPostCallback(Handler)

    def Filter(monitor):
        if monitor.LastOperation.Action == 'CreateFile':
          print("Filename : %s" % monitor.LastOperation.Detail.
              lpFileName)
```

Dans ce cas, nous aurons sur la console la sortie suivante :

```
Filename : C:\Users\Public\Desktop
Filename : C:\Users\user\OneDrive\desktop.ini
Filename : C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\
    AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms
Filename : \\?\Volume{ed9c75a3-0000-0000-0000-501f00000000}
Filename : \\?\STORAGE#Volume#{6d4e60e4-2314-11e8-8cfd-806e6f6e6963
    }#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Filename : \\?\Volume{6d4e60f4-2314-11e8-8cfd-806e6f6e6963}
Filename : \\?\STORAGE#Volume#{6d4e60e4-2314-11e8-8cfd-806e6f6e6963
    }#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
```

L'utilisation d'un *monitor* est finalement une opération simplifiée au maximum, qui peut être réalisée de façon interactive avec **`IPython`** ou avec un script autonome.

Espace noyau et espace utilisateur Le framework a été conçu pour s'adapter au besoin de l'analyste. De ce fait, l'utilisateur peut créer et développer son propre *monitor*. Ce concept impose de distinguer un *monitor* dédié à l'espace noyau d'un *monitor* dédié à l'espace utilisateur.

Cependant, ils héritent tout deux d'une classe mère qui permet de conserver une cohérence entre les deux types de *monitors*. Cette classe *monitor* offre :

- un gestionnaire de points d'arrêt ;
- un gestionnaire de symboles ;
- la gestion des processus 32 et 64 bits ;
- la lecture des paramètres de fonctions (entrées/sorties ; 32/64 bits) ;
- un gestionnaire d'évènements ;
- un gestionnaire générique d'événements.

La classe *monitor* s'appuie essentiellement sur les fichiers de symboles de Microsoft (**`PDB`**) mais également sur des fichiers de signatures de fonctions de type *header* **`C`** (**`.h`**).

L'implémentation d'un *monitor* est définie par :

- un nom, qui sera le type d'évènement ;
- ses dépendances, les modules (**`DLL`**) qui nécessitent d'être chargés ;
- les points d'arrêt à enregistrer ;
- les informations spécifiques à enregistrer.

L'exemple ci-dessous est un *monitor* conçu pour gérer les événements de type **`InternetOpen`** et **`InternetOpenUrl`**. La classe **`InternetMonitor`** hérite d'une classe générique de *monitor* en espace utilisateur. Elle déclare

les éventuelles dépendances aux modules, pour le chargement des fichiers de symboles, et installe des points d'arrêts sur les symboles dont les événements seront automatiquement collectés.

```
from Sandbagility.Monitor import UserlandGenericMonitor as
    UserlandMonitor

class InternetMonitor(UserlandMonitor):

    _LOGGER = 'Internet'
    _DEPENDENCIES = ['WININET.dll']

    def __install__(self, NotifyLoadImage=None):

        self.SetBreakpoint('WININET!InternetOpenA')
        self.SetBreakpoint('WININET!InternetOpenW')

        self.SetBreakpoint('WININET!InternetOpenUrlA')
        self.SetBreakpoint('WININET!InternetOpenUrlW')

        return True
```

Ci-dessous figure un exemple de sortie du *monitor* **InternetMonitor**. On constate que le processus **microsoftedgecp.exe** a fait appel à la fonction **InternetOpen** avec des paramètres comme **dwFlags** ou encore **lpszAgent**.

```
2018-02-13 22:00:10,494 Internet             INFO
InternetOpen                  :
Process: microsoftedgecp.exe ,
Cid:   fa4.1040,
{
    'lpszAgent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
        AppleWebKit/537.36 (KHTML, like Gecko)
        Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393',
    'dwAccessType': 0,
    'lpszProxyName': 0,
    'lpszProxyBypass': 0,
    'dwFlags': 1924413784064,
    'Return': 13369348
}
2018-02-13 22:00:10,498 Internet             INFO
InternetOpen
Process: microsoftedgecp.exe ,
Cid:   fa4.1040,
{
    'lpszAgent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
        AppleWebKit/537.36 (KHTML, like Gecko)
        Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393',
    'dwAccessType': 0,
    'lpszProxyName': 0,
    'lpszProxyBypass': 0,
    'dwFlags': 268435456,
    'Return': 13369348
}
```

Il s'agit là, d'un exemple de *monitor* basé sur l'implémentation générique d'un *monitor* en espace utilisateur. Si cette implémentation ne permet pas à l'analyste de répondre à son besoin, il aura la possibilité de développer un *monitor* spécifique.

Le framework Sandbagility propose une API très haut niveau, pour simplifier son utilisation. Pour pouvoir implémenter une telle API, il est nécessaire dans un premier temps d'analyser le système invité afin de retrouver des données essentielles (fonctions, structures).

3.2 Introspection de Microsoft Windows

Lorsqu'un système d'exploitation s'exécute dans une machine virtuelle, il n'a pas connaissance de l'existence de l'hyperviseur. Il peut ainsi accéder aux ressources matérielles de manière transparente. Tandis que l'hyperviseur fonctionne sans attribuer de sémantique à l'activité du système invité.

Ce modèle disruptif entre l'hyperviseur et la machine virtuelle constitue le vide sémantique. Le framework *Sandbagility* vise à remplir ce vide pour déterminer la sémantique des actions réalisées par le système invité.

Dans ce papier, nous tenterons d'amener le lecteur à comprendre les étapes pour combler ce vide sémantique et permettre l'introspection du système Windows.

Combler le vide sémantique Pour nous aider dans cette tâche, nous avons choisi d'utiliser autant que possible les fichiers de symboles mis à disposition par Microsoft. À l'image de ce qui est fait par le débuggeur **`Windbg`** de Microsoft, qui permet de traduire un symbole en adresse virtuelle.

L'exemple suivant illustre la traduction du symbole **`nt!NtWriteFile`** en son adresse virtuelle avec **`Windbg`**.

```
kd> x nt!NtWriteFile
fffff801‘a2ed37d0 nt!NtWriteFile (<no parameter info>)
```

La première étape indispensable à l'introspection est le chargement du fichier de symboles correspondant à la version courante du noyau de Windows sur le système analysé. Pour cela, nous devrons accomplir les étapes suivantes :

1. rechercher l'adresse virtuelle de base du noyau (**`ntoskrnl.exe`**) ;
2. identifier sa version ;
3. charger le fichier de symbole correspondant.

Recherche du noyau Windows La recherche en mémoire du noyau de Windows s'appuie sur le registre **MSR_LSTAR**. Ce registre contient l'adresse virtuelle en espace noyau d'un *handler* responsable de gérer la transition entre l'espace utilisateur et l'espace noyau. Ce *handler* est exécuté à travers l'instruction **sysenter**, présente sur une architecture *x86_64*.

> Dans la version 64 bits de Windows 10 - 14393 qui a été étudiée, la valeur de ce registre pointe vers l'adresse virtuelle invitée correspondant au *handler* **nt!KiSystemCall64**.

C'est donc à partir du registre **MSR_LSTAR** qu'il nous est possible de trouver l'adresse virtuelle de base du noyau (**ntoskrnl.exe**). Il suffit de parcourir la mémoire virtuelle du système invité en remontant vers les adresses basses à la recherche d'une signature particulière. Cette signature est spécifique à l'en-tête de tout fichier exécutable sous Microsoft Windows au format **PE** (*Portable Executable*) [https://msdn.microsoft.com/library/windows/desktop/ms680547(v=vs.85).aspx].

```
In [13]: '%x' % helper.KeGetKernelBaseAddress()
Out[13]: 'fffff802c0293000'

In [16]: helper.ReadVirtualMemory(0xfffff802c0293000, 2)
Out[16]: b'MZ'
```

Program Database À présent, nous devons identifier la version du noyau de Windows afin de charger le fichier de symboles **PDB** correspondant et permettre l'introspection du système Windows. Les fichiers de symboles sont téléchargeables à partir du site de Microsoft, et ce, pour toutes les versions de Windows : [https ://msdl.microsoft.com/download/symbols]

Ces fichiers de symboles, souvent appelés **PDB** (nom de leur extension, pour *Program Database*) contiennent :

- les noms des fonctions non statiques et des variables globales ;
- les informations pour chaque pile de fonctions (Frame pointer optimization) ;
- les types des objets.

Tous les fichiers de symboles sont identifiés de manière unique avec un **GUID** (*Global Unique Identifier*) et un nom. Ces deux informations sont contenues dans les fichiers exécutables fournies par Microsoft.

L'entête d'un fichier exécutables (**PE**) contient une structure de données, appelée **IMAGE_DEBUG_DIRECTORY** que l'on peut retrouver dans

le **DataDirectory** de l'**OPTIONAL_HEADER**. Les informations de *debug* se trouvent dans une structure de données que nous avons appelée **RSDS_DEBUG_FORMAT**. Grâce à cette structure, on obtient le **GUID** et le nom du fichier de symboles.

```
struct RSDS_DEBUG_FORMAT
{
    DWORD Signature; // RSDS
    BYTE  Guid[16];
    DWORD Age;
    CHAR  PdbFileName[1];
}
```

Dans l'exemple ci-après, *Sandbagility* permet de retrouver les informations liées au fichier de symboles à partir de l'adresse de base d'un module, en l'occurrence le noyau de Windows.

```
In [3]: '%x' % helper.KeGetKernelBaseAddress()
Out[3]: 'fffff802c0293000'

In [4]: helper.SymGetModulePdbPath(0xfffff802c0293000)
Out[4]: 'D:\\Symbols\\ntkrnlmp.pdb\\
    dd08dd42692b43f199a079d60e79d2171\\ntkrnlmp.pdb'
```

Gestion des fichiers de symboles Désormais, la dernière étape consiste à charger le fichier de symboles, en indiquant l'adresse de base du noyau de Windows et son **GUID** et être capable de faire la traduction d'un symbole en adresse virtuelle. Cette étape est le concept fondamental de *Sandbagility* pour l'introspection du système Microsoft Windows.

Nous savons que les fichiers de symboles permettent de traduire un symbole en une adresse virtuelle. Ils peuvent contenir d'autres informations de valeur :

- les variables globales et locales ;
- les enregistrements de type *Frame Pointer Omission* (**FPO**) ;
- le numéro de la ligne correspondante dans les fichiers sources ;
- les noms de fonctions et leurs points d'entrée ;
- les types des objets/structures.

Le framework *Sandbagility* s'appuie sur la bibliothèque d'aide au *debug* (*Debug Help Library*) et plus particulièrement sur le composant intitulé *Windows Image Helper*. Ce composant se présente sous la forme d'une bibliothèque de fonctions dynamiques appelée **dbghelp.dll** (SLL fournie par Microsoft via le SDK ou WDK) qui permet de gérer :

– les symboles au travers de fichiers ou d'un serveur ;
– les fichiers de type **Minidump** ;
– les serveurs de source.

À l'aide de ce composant, il est possible de traduire dynamiquement tout symbole en son adresse virtuelle et inversement. L'utilisation des fichiers de symboles par le framework permet de limiter son adhérence vis-à-vis d'une version particulière de Microsoft Windows. Il devient très simple de supporter les futures versions de Microsoft Windows.

À présent, le framework permet de traduire simplement un nom de symbole en un object **Python**.

```
In [5]: '%x' % helper.SymLookupByName('nt!NtWriteFile')
Out[5]: 'fffff802c06ef7d0'
```

Les fichiers de symboles contiennent également la définition des principaux types d'objets/structures utilisées par le système Microsoft Windows. Par exemple, le *debugger* Windbg de Microsoft permet, au moyen de la commande **dt** d'afficher un type de donnée.

L'exemple ci-dessous illustre une sortie de Windbg pour le type **_UNICODE_STRING**.

```
kd> dt _UNICODE_STRING
ntdll!_UNICODE_STRING
   +0x000 Length           : Uint2B
   +0x002 MaximumLength    : Uint2B
   +0x008 Buffer           : Ptr64 Wchar
```

Le framework permet de réaliser une opération similaire à celle de windbg, mais plus puissante car elle a l'avantage de retourner des objets **Python** de type **ctypes.Structure**.

Dans l'exemple ci-après, on utilise le framework *Sandbagility* pour placer un point d'arrêt sur la fonction **NtCreateFile** en espace noyau. Après avoir exécuté le système invité avec la méthode **Run**, on peut inspecter le parametre **ObjectAttributes** de type **_OBJECT_ATTRIBUTES**. Le champs **ObjectName** dans cette structure pointe sur une structure de type **_UNICODE_STRING** qui indique le nom du fichier à ouvrir, en l'occurrence **imageres.dll.mui**.

```
In [1]: from Sandbagility.Core.FDP import FDP
   ...: from Sandbagility.Helper import Helper

In [2]: helper = Helper('Windows 10 x64 - 14393', FDP)

In [3]: helper.SetBreakpoint('nt!NtCreateFile')
```

```
Out[3]: 4

In [4]: helper.Run()

In [5]: ObjectAttributes = helper.ReadStructure(helper.dbg.r8, 'nt!
    _OBJECT_ATTRIBUTES')

In [6]: helper.ReadUnicodeString(ObjectAttributes.ObjectName)
Out[6]: \??\c:\windows\system32\en-US\imageres.dll.mui
```

Processus sous Windows

Identifier le processus courant Dans le cadre de l'analyse d'un code malveillant (par exemple, `wannacry`), le framework s'appuie sur l'installation de *monitor* pour capturer les événements réalisés sur le système analysé. Cependant, seuls les événements réalisés par le processus analysé doivent être journalisés. Pour ce faire, il est nécessaire d'identifier le processus ou fil d'exécution (*thread*) en cours d'exécution lorsqu'un *monitor* est notifié. La figure 6 montre les différentes étapes permettant cette identification.

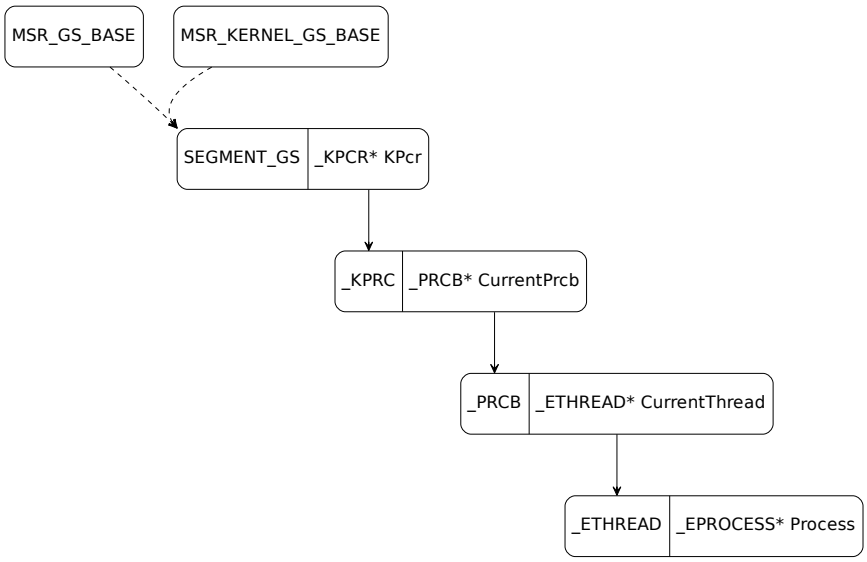

Fig. 6. Identification du processus courant

Pour identifier le processus en cours d'exécution, le framework s'appuie sur l'adresse virtuelle relative au segment *GS*. Cette adresse vir-

tuelle peut être obtenue par la lecture du registre **MSR_GS_BASE** ou **MSR_KERNEL_GS_BASE**.

Le segment **GS** pointe vers une structure de type **_KPCR**, dans laquelle le champ **CurrentPrcb** pointe vers une structure du même nom **_PRCB**. Cette dernière structure contient l'adresse d'une structure de type **_ETHREAD** qui décrit le fil d'exécution courant. Chaque fil d'exécution est rattaché à un processus dans lequel il s'exécute. Le champ **Process** de la structure **_ETHREAD** pointe vers une structure de type **_EPROCESS**.

Énumérer les processus Sous Microsoft Windows, les processus forment une liste doublement chaînée (pour être parcouru en avant et en arrière).

De ce fait, il suffit de trouver un objet **_EPROCESS** en mémoire pour énumérer l'ensemble des processus actifs. Cette liste doublement chaînée est matérialisée par le champ **ActiveProcessLinks**. Le noyau Windows maintient un point d'entrée sur cette liste doublement chainée, il s'agit en l'occurrence du symbole **nt!PsActiveProcessHead**.

L'exemple ci-dessous, la fonction **PsEnumProcesses()** permet d'énumérer la liste doublement chainée à partir du symbole **nt!PsActiveProcessHead** et retourner une liste de **tuple** contenant le nom du processus et son identifiant unique (*PID* ou **UniqueProcessId**).

```
In [20]: [ (p.ImageFileName, p.UniqueProcessId) for p in helper.
    PsEnumProcesses() ]
Out[20]:
[('System', 4),
 ('smss.exe', 320),
 ('csrss.exe', 400),
 ('smss.exe', 452),
 ('wininit.exe', 460),
 ('csrss.exe', 468),
 ('winlogon.exe', 520),
 ('services.exe', 544),
 ('lsass.exe', 552),
 ...
```

Sémantique d'un processus Chaque processus sous Windows dispose d'un objet en espace noyau qui le définit. Cet objet s'appuie sur une structure de donnée appelée **_EPROCESS**. Cette structure contient de nombreuses informations relatives à l'environnement du processus, telles que :

- le chemin du fichier exécutable ;
- la liste des modules chargés ;
- l'environnement **SysWow64** ;
- la ligne de commande utilisée à l'exécution.

Dans l'exemple ci-après, on utilise la méthode **ReadStructure** (présenté dans la section précédente) pour lire une structure **_EPROCESS** à partir d'une adresse virtuelle. Ainsi, pour obtenir le nom du processus **ImageFileName** associé à l'objet **_EPROCESS**, il suffit de faire appel à la propriété **ImageFileName**.

```
In [34]: eprocess = helper.ReadStructure(0xffffc28abc352780, 'nt!
    _EPROCESS')
In [35]: bytes(eprocess.ImageFileName)
Out[35]: b'taskhostw.exe\x00\x00'
```

La sémantique d'un processus ne se limite pas à la structure **_EPROCESS**. On peut ajouter *a minima* les informations contenues dans des structures comme **_PROCESS_ENVIRONMENT_BLOCK** [1], **_RTL_USER_PROCESS_PARAMETERS** ou encore **_LDR_DATA**.

Ci-dessous un exemple de sortie du framework dans la console **IPython**. Le framework s'appuie sur une représentation interne de l'objet **_EPROCESS**. Cette représentation se présente avec le type `ProcessObject`. Ainsi, on peut afficher simplement les informations liées au processus **wininit.exe** dont l'objet est stocké dans la variable **wininit**.

```
In [16]: type(wininit)
Out[16]: Sandbagility.Windows.ntoskrnl.ProcessObject

In [17]: str(wininit.CreateTime)
Out[17]: '2018-03-08 22:25:35.769390'

In [18]: print(wininit)

PROCESS ffffc28abcbaa080
SessionId:       -1  Cid:  1cc    Peb:       fc40767000  ParentCid:
    184
DirBase:  264f000  ObjectTable: ffff8e0c254e1480  HandleCount: 100
Image: wininit.exe
    7ffbb39b0000-7ffbb3b81000     578997b2 C:\Windows\SYSTEM32\ntdll
        .dll
    7ffbb3630000-7ffbb36db000     57899a29 C:\Windows\System32\
        KERNEL32.DLL
    7ffbb0490000-7ffbb06ad000     57899809 C:\Windows\System32\
        KERNELBASE.dll
    7ffbb01c0000-7ffbb02b5000     578997b5 C:\Windows\System32\
        ucrtbase.dll
    7ffbb2ea0000-7ffbb2fc1000     578997f7 C:\Windows\System32\
        RPCRT4.dll
    7ffbb2a40000-7ffbb2a99000     57899a7c C:\Windows\System32\
        sechost.dll
```

L'accès aux ressources L'une des notions les plus importantes sous Microsoft Windows est le concept de *handle*. Un *handle* représente une

ressource qui a été allouée et dont l'accès a été contrôlé par le système. Ce *handle* est valable uniquement dans le contexte du processus pour lequel il a été autorisé.

L'autorisation par le système est réalisée en confrontant le *Token* de l'entité (*Thread*, *Process*) qui demande, le descripteur de sécurité de la ressource demandée (*Security Descriptor*) et les droits d'accès demandés (`READ_ACCESS`, `WRITE_ACCESS`, etc.).

De façon très sommaire, lorsqu'un processus sous Windows souhaite écrire dans un fichier, il réalise les trois actions suivantes :

1. récupérer un *handle* (descripteur) du fichier à partir de son chemin ;
2. écrire dans le fichier en utilisant le *handle* obtenu précédemment ;
3. fermer le *handle* pour libérer le fichier.

Dans le framework *Sandbagility*, nous avons choisi de réaliser l'introspection d'un processus pour parcourir sa liste de *handle* et identifier, à tout moment, les ressources auxquelles il accède.

Dans l'exemple qui suit, le framework permet de traduire le *handle* passé à la fonction **`NtWriteFile`** en premier argument dans le registre **`rcx`**. On traduit alors la valeur de ce *handle* avec la méthode **`ObReferenceObjectByHandle`** dans le contexte du processus courant pour obtenir le chemin du fichier associé, en l'occurrence **`V01.log`**.

```
In [1]: from Sandbagility.Core.FDP import FDP
   ...: from Sandbagility.Helper import Helper

In [2]: helper = Helper('Windows 10 x64 - 14393', FDP)

In [3]: helper.SetBreakpoint('nt!NtWriteFile')
Out[3]: 4

In [4]: helper.Run()

In [5]: helper.dbg.rcx
Out[5]: 1052

In [6]: ActiveProcess = helper.PsGetCurrentProcess()

In [7]: ActiveProcess.ObReferenceObjectByHandle(1052)
Out[7]: \Users\user\AppData\Local\Microsoft\Windows\WebCache\V01.log
```

Traduction de handle L'introspection de la table de *handle* d'un processus s'appuie sur la structure **`_EPROCESS`**. Cette structure **`_EPROCESS`** contient un champ **`ObjectTable`** qui pointe vers une structure de type **`_HANDLE_TABLE`**. Dans cette structure se trouve un champ **`TableCode`** qui pointe sur un tableau de **`_HANDLE_TABLE_ENTRY`**.

Dans la suite de ce papier, nous appellerons ce tableau un **_HANDLE_TABLE_DIRECTORY**. Chaque entrée de type **_HANDLE_TABLE_ENTRY** représente un *handle* qui a été alloué par le système. Chacune de ces entrées contient *a minima* une référence vers l'objet noyau correspondant au *handle*. Associés à cette entrée, on peut retrouver les droits d'accès accordés à ce *handle*.

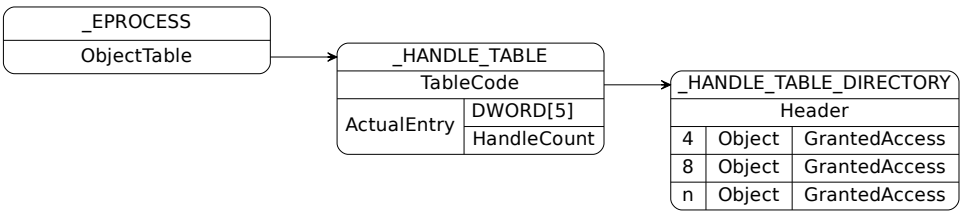

Fig. 7. Table de *handle*

Il est à noter qu'un **_HANDLE_TABLE_DIRECTORY** ne peut contenir plus de 512 *handle*. Par conséquent, lorsque le processus nécessite des *handle* supplémentaires, le système lui alloue un nouvel **_HANDLE_TABLE_DIRECTORY** pouvant contenir 512 nouveaux *handle*.

Dans ce dernier cas, le champ **TableCode** de la structure **_HANDLE_TABLE** pointe sur un tableau de **_HANDLE_TABLE_DIRECTORY**. Le nombre de **_HANDLE_TABLE_DIRECTORY** alloués pour le processus courant est maintenu dans l'octet de poids faible du champ **TableCode**.

4 wannacry : Une sandbox en 90 jours

Comme indiqué dans l'introduction, le code malveillant `wannacry` a été choisi pour servir de référence et valider le framework *Sandbagility*.

`wannacry` est un code malveillant, que l'on peut désigner de rançongiciel ou **CryptoLocker**. Durant son exécution, il a pour but de chiffrer les données de l'utilisateur présentes sur le système. Il propose ensuite à l'utilisateur de déchiffrer les fichiers en échange d'une somme d'argent. Ce code malveillant présentait la particularité d'exploiter une vulnérabilité dans la version 1 du composant **SMB** de Microsoft Windows pour se propager.

Pour procéder à l'analyse de `wannacry`, il est nécessaire de capturer, *a minima*, les événements suivants sous Microsoft Windows :

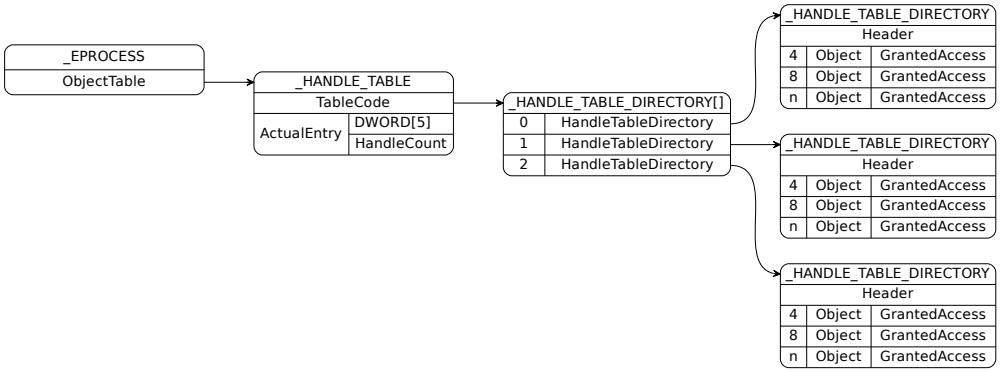

Fig. 8. Table indirecte de *handle*

1. identifier et suivre les processus malveillants ;
2. identifier et collecter les fichiers copiés, écrits et exécutés ;
3. analyser les algorithmes cryptographiques employés ;

4.1 Processus et services

Dans le cadre de l'analyse de `wannacry`, il est nécessaire de suivre l'exécution du code malveillant dès son point d'entrée et de suivre la création des processus affiliés.

Processus Microsoft Windows offre une **`API`** noyau, utilisée pour enregistrer des *callbacks*, qui seront notifiées pour les événements du type :

- création et destruction de processus avec `PsSetCreateProcessNotifyRoutine` ;
- création et destruction de fil d'exécution (**`thread`**) avec `PsSetThreadNotifyRoutine` ;
- chargement et déchargement de bibliothèque de liens dynamique (**`DLL`**) avec `PsSetLoadImageNotifyRoutine`.

L'approche consiste à développer un *monitor* qui tire profit de ce mécanisme de notification noyau et ainsi collecter tous les événements liés aux processus, fils d'exécution et bibliothèques de liens dynamique. L'étude du fonctionnement interne de ce mécanisme de notification a permis de développer un *monitor* appelé **`PsNotifyRoutines`**. Ce *monitor* retrouve les callbacks déjà présents sur le système et ajoute des points d'arrêt sur celles-ci afin d'être notifié pour chacun des cas.

```
2018-03-25 01:04:36,937 Process      INFO    CreateProcess : Process:
     wannacry.exe , Cid:   dd0.928, C:\WINDOWS\tasksche.exe /i
```

En théorie, le *monitor* décrit précédemment devrait permettre de suivre toutes les créations de processus réalisées par **wannacry**. Cependant, la sortie obtenue se termine avec une seule opération de création de processus, en l'occurrence **tasksche.exe** avec en paramètre **/i**. Un parcours du code désassemblé du **wannacry** permet de révéler la création et l'exécution d'un service Windows sous le nom **mssecsvc2.0**.

Services Il est à noter que l'exécution d'un service sous Windows est réalisée par le processus **services.exe**. C'est pour cette raison que la sortie précédente est incomplète. De ce fait, il devient nécessaire de suivre la création et le démarrage d'un service et d'inclure les créations de processus faite par **services.exe**.

Pour répondre à cette problématique, nous avons développé un *monitor* *ServiceMonitor* qui permet de suivre les opérations qui consistent à :

- Ouvrir, créer et supprimer un service ;
- Changer une configuration ;
- Enregistrer ou démarrer un **Service Control Dispatcher** ;
- Envoyer des codes de contrôle.

Ce *monitor* s'appuie sur des fonctions implémentées dans la bibliothèque de liens dynamiques **sechost.dll** comme **OpenService**, **CreateService**, **StartService**, etc.

Dorénavant, au moyen du framework *Sandbagility* nous pouvons suivre l'exécution de **wannacry** en y incluant la création de service. La sortie présentée en annexe montre que le deuxième événement capturé correspond à la création d'un service nommée **dtuynyjtysq538**, puis la création d'un processus par **services.exe** avec la ligne de commande **cmd.exe /c** "C :\ProgramData\dtuynyjtysq538\tasksche.exe".

4.2 Fichiers

Dans la section précédente, nous avons présenté comment il est possible de suivre l'exécution du code malveillant **wannacry** au travers de la création de processus et de services. Cependant, il manque une information essentielle, à savoir, le suivi lié à la création et l'écriture de fichiers. Pour répondre à cette nouvelle contrainte, le framework *Sandbagility* s'appuie sur un *monitor* appelé **FileIo** qui a pour but suivre les opérations de type

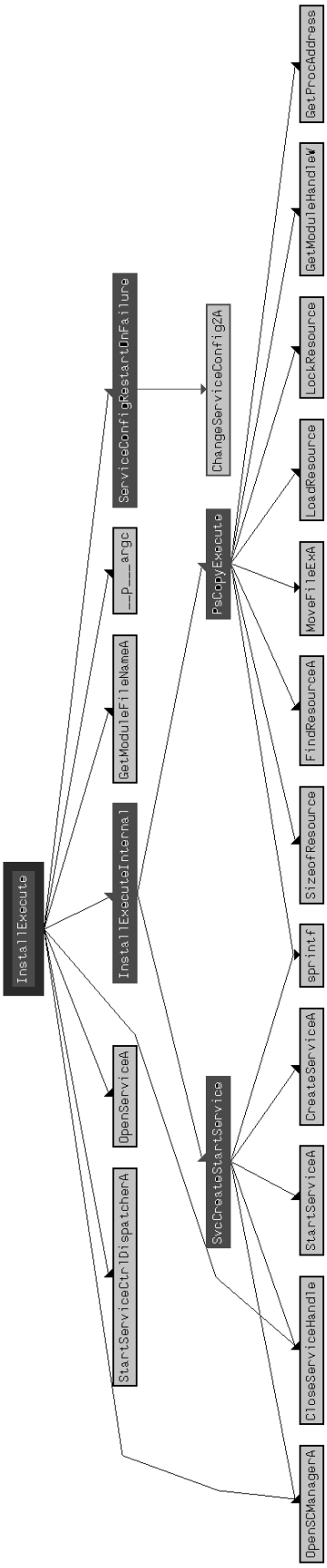

Fig. 9. Diagramme fonctionnel d'installation

WriteFile et **ReadFile** dont les fonctions sont implémentées dans la bibliothèque de liens dynamiques **kernelbase.dll**.

Le *monitor* en question, qui hérite d'une classe générique de *monitor* en espace utilisateur, se présente sous la forme suivante :

```
from Sandbagility.Monitor import UserlandGenericMonitor as
    UserlandMonitor

class FileIoMonitor(UserlandMonitor):

    _LOGGER = 'File'
    _DEPENDENCIES = ['kernelbase.dll']

    def __install__(self, NotifyLoadImage=None):

      self.SetBreakpoint('kernelbase!WriteFile')
      self.SetBreakpoint('kernelbase!ReadFile')

      return True
```

Dans l'extrait fourni en annexe , on peut observer les opérations suivantes sur les fichiers :

- la création de fichier exécutable **tasksche.exe**, **taskdl.exe**, **taskse.exe** et **@WanaDecryptor@.exe** dans**\ProgramData\dtuynyjtysq538** ;
- la création de nombreux fichiers avec l'extension **.wnry** dans le répertoire **\ProgramData\dtuynyjtysq538** ;
- la création de fichier de script 56291522146484**.bat** et **m.vbs** ;
- la création de fichier avec l'extension **.WNCRYT**.

Dans la suite de ce papier, nous ne détaillerons pas l'utilité de ces fichiers pour le code malveillant, dans la mesure où il existe de nombreux rapports d'analyse.

Ressources Dans le domaine de l'analyse de code malveillant sous Windows, il existe un mécanisme largement employé, qui consiste à embarquer des ressources directement dans le fichier exécutable. Ces ressources peuvent être des icônes, des définitions pour des fenêtres de boîtes de dialogues, etc. Il peut également s'agir de fichiers binaires, par exemple un exécutable.

Afin d'être capable de suivre les éventuels accès aux ressources d'un fichier exécutable, nous avons développé un *monitor* dédié à suivre l'appel aux **API** qui permettent à un programme de manipuler des ressources. En l'occurrence, il s'agit des fonctions **FindResource**, **LoadResource** et **SizeOfResource** qui sont implémentées dans les bibliothèques de liens dynamique **kernelbase.dll** et **kernel32.dll**.

```
2018-03-27 12:58:38,145 Service      INFO     CreateService :
    Process: tasksche.exe, Cid:    ff0.fec, 'dtuynyjtysq538'
2018-03-27 12:58:44,358 Resource     INFO     AcquireResource
    : Process: tasksche.exe, Cid:    420.7c8, 'XIA'
```

Dans le cas de **wannacry**, il embarque une ressource binaire qui peut être identifiée sous le nom **XIA**. Pour accéder à cette ressource binaire, le code malveillant fait successivement appel aux fonctions **FindResource** , **LoadResource** et **SizeOfResource** qui est journalisée sous le libellé **AcquireResource**. Cette ressource est une archive au format **ZIP** qui contient l'ensemble des fichiers qui seront décompressés dans le répertoire **ProgramData\dtuynyjtysq538**.

4.3 Cryptographie

L'objectif d'un code malveillant comme **wannacry** est de chiffrer les données de l'utilisateur présent sur le système pour l'inciter à payer une rançon pour déchiffrer ses fichiers en contrepartie. Pour réaliser ces opérations de chiffrement, **wannacry** s'appuie sur le fournisseur de service cryptographique de Microsoft Windows (*Cryptographique Service Provider* ou **CSP**). Les fonctions cryptographiques offertes par ce fournisseur sont les suivantes :

- accéder au fournisseur de service ;
- générer et échanger des clés cryptographiques ;
- encoder et décoder des objets ;
- chiffrer et déchiffrer des données ;
- condenser (*hacher*) et signer numériquement.

Comme pour l'analyse des opérations précédentes, nous avons développé un *monitor* dédié au suivi des évènements liés au fournisseur de service cryptographique. Ce *monitor* appelé **CryptoProvider** a pour objectif de suivre les quelques fonctions offertes par le fournisseur de service cryptographique de Windows. Parmi elles, les fonctions de chiffrement et de déchiffrement, de génération de clés, d'import et d'export de clés.

Cette approche permet d'éclairer l'analyste sur le schéma cryptographique employé par **wannacry**.

```
2018-04-06 09:32:38,042 Crypto       INFO     CryptImportKey:
    Process: tasksche.exe, Cid:    be0.424, 'PRIVATEKEYBLOB'
2018-04-06 09:32:38,072 Crypto       INFO     CryptDecrypt  :
    Process: tasksche.exe, Cid:    be0.424, 16
2018-04-06 09:32:38,355 Crypto       INFO     CryptImportKey:
    Process: tasksche.exe, Cid:    be0.424, 'PUBLICKEYBLOB'
```

```
2018-04-06 09:32:39,096 Crypto       INFO     CryptGenKey    :
    Process: tasksche.exe, Cid:    be0.424, 2048
2018-04-06 09:32:39,106 Crypto       INFO     CryptExportKey:
    Process: tasksche.exe, Cid:    be0.424, 'PUBLICKEYBLOB'
2018-04-06 09:32:39,113 Crypto       INFO     CryptExportKey:
    Process: tasksche.exe, Cid:    be0.424, 'PUBLICKEYBLOB'
2018-04-06 09:32:39,143 Crypto       INFO     CryptExportKey:
    Process: tasksche.exe, Cid:    be0.424, 'PRIVATEKEYBLOB'
2018-04-06 09:32:39,164 Crypto       INFO     CryptEncrypt   :
    Process: tasksche.exe, Cid:    be0.424, 256
2018-04-06 09:32:39,172 Crypto       INFO     CryptEncrypt   :
    Process: tasksche.exe, Cid:    be0.424, 256
2018-04-06 09:32:39,181 Crypto       INFO     CryptEncrypt   :
    Process: tasksche.exe, Cid:    be0.424, 256
2018-04-06 09:32:39,190 Crypto       INFO     CryptEncrypt   :
    Process: tasksche.exe, Cid:    be0.424, 256
2018-04-06 09:32:39,200 Crypto       INFO     CryptEncrypt   :
    Process: tasksche.exe, Cid:    be0.424, 256
2018-04-06 09:32:39,218 Crypto       INFO     CryptImportKey:
    Process: tasksche.exe, Cid:    be0.424, 'PUBLICKEYBLOB'
```

Dans l'extrait de sortie ci-dessus, le processus **tasksche** identifié précédemment, fait appels aux fonctions du fournisseur de service cryptographique dont les événements sont suivis par le *monitor*. La succession de ces appels de fonctions laisse penser que **wannacry** déchiffre une clé de 128 bits après avoir importé une clé. L'hypothèse suivante peut également être émise, après avoir générée une clé de 20148 bits, cette dernière est dérivée au moyen des appels à la fonction **CryptEncrypt**.

5 Conclusion

À travers l'exemple de **wannacry**, nous avons tenté de démontrer la simplicité avec laquelle il est possible de suivre de nouveaux évènements en utilisant la notion de *monitor*. L'implémentation des *monitors* permet à l'utilisateur de s'affranchir en partie de la complexité du système d'exploitation Windows, et de se concentrer sur son analyse et l'étude des paramètres.

En s'appuyant sur le protocole **FDP** et les fichiers de symboles de Microsoft, *Sandbagility* offre une **API** puissante d'analyse semi-automatisé de machine virtuelle Windows fonctionnant avec **VirtualBox**. Ce framework intègre la couche nécessaire à l'introspection d'un système d'exploitation Windows en tirant parti des fichiers de symboles de Microsoft. Cette approche permet de réduire la dépendance et l'adhérence du framework à la version du système installé.

Le choix du langage **Python** pour le développement du framework *Sandbagility* lui permet d'être modifiable et évolutif à moindre frais. Ainsi,

le framework ne se limite pas qu'à l'étude des codes malveillant ou aux processus utilisateurs mais peut être étendu à l'analyse de tout programme notamment en espace noyau Windows.

Références

1. Khairul Akram Zainol Ariffin, Ahmad Kamil Mahmood, and Jafreezal Jaafar. Investigating the PROCESS block for memory analysis. In *Proceedings of the 11th WSEAS international conference on Applied Computer Science*, pages 21–29, 2011.
2. Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield. Xen and the art of virtualization. In *ACM SIGOPS operating systems review*, volume 37, pages 164–177. ACM, 2003.
3. Joan Calvet. *Analyse dynamique de logiciels malveillants*. PhD thesis, École Polytechnique de Montréal, 2013.
4. Cisco-Talos. PyRebox. `https://github.com/Cisco-Talos/pyrebox`, 2018.
5. Nicolas Couffin. Winbagility : Débogage furtif et introspection de machine virtuelle. *SSTIC*, 2016.
6. Olivier Ferrand. How to detect the cuckoo sandbox and to strengthen it ? *Journal of Computer Virology and Hacking Techniques*, 11(1) :51–58, 2015.
7. Volatility Foundation. Volatility. `https://github.com/volatilityfoundation/volatility`, 2018.
8. François Khourbiga and Eddy Deligne. Sandbagility : Framework d'introspection pour Microsoft Windows. *SSTIC*, 2018.
9. Tamas K Lengyel, Steve Maresca, Bryan D Payne, George D Webster, Sebastian Vogl, and Aggelos Kiayias. Scalability, fidelity and stealth in the DRAKVUF dynamic malware analysis system. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pages 386–395. ACM, 2014.
10. Gustav Lundsgård and Victor Nedström. Bypassing modern sandbox technologies. 2016.
11. Michael Pearce, Sherali Zeadally, and Ray Hunt. Virtualization : Issues, security threats, and solutions. *ACM Computing Surveys (CSUR)*, 45(2) :17, 2013.
12. Cuckoo Sandbox. *Cuckoo Sandbox Book*. 2017.
13. Thorsten Sick. Cuckoo Sandbox vs. Reality. `https://blog.avira.com/cuckoo-sandbox-vs-reality-2/`, 2014.
14. Rich Uhlig, Gil Neiger, Dion Rodgers, Amy L Santoni, Fernando CM Martins, Andrew V Anderson, Steven M Bennett, Alain Kagi, Felix H Leung, and Larry Smith. Intel virtualization technology. *Computer*, 38(5) :48–56, 2005.
15. Haiquan Xiong, Zhiyong Liu, Weizhi Xu, and Shuai Jiao. Libvmi : a library for bridging the semantic gap between guest OS and VMM. In *Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on*, pages 549–556. IEEE, 2012.

A Annexes

A.1 Processus et services

```
2018-03-27 11:35:56,866 Process      INFO     CreateProcess : Process: wannacry.exe , Cid:
       1228.122c, C:\WINDOWS\tasksche.exe /i
2018-03-27 11:35:57,487 Service      INFO     CreateService : Process: tasksche.exe, Cid:
      12a8.12ac, 'dtuynyjtysq538'
2018-03-27 11:35:57,615 Process      INFO     CreateProcess : Process: services.exe, Cid:
        220.36c, cmd.exe /c "C:\ProgramData\dtuynyjtysq538\tasksche.exe"
2018-03-27 11:36:00,913 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      12b4.12b8, C:\ProgramData\dtuynyjtysq538\tasksche.exe
2018-03-27 11:36:03,906 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.12cc, attrib +h .
2018-03-27 11:36:04,134 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.12cc, icacls . /grant Everyone:F /T /C /Q
2018-03-27 11:36:04,350 Process      INFO     CreateProcess : Process: attrib.exe  , Cid:
      12dc.12e0, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 11:36:04,572 Process      INFO     CreateProcess : Process: icacls.exe  , Cid:
      12e4.12e8, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 11:36:06,836 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, icacls . /grant Everyone:F /T /C /Q
2018-03-27 11:36:06,900 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, attrib +h .
2018-03-27 11:36:07,319 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.1324, taskdl.exe
2018-03-27 11:36:07,683 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, taskdl.exe
2018-03-27 11:36:08,052 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.12cc, C:\Windows\system32\cmd.exe /c 284781522143356.bat
2018-03-27 11:36:08,389 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      1344.1348, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 11:36:32,369 Service      INFO     StartService  : Process: tasksche.exe, Cid:
      12a8.12ac, 'dtuynyjtysq538'
2018-03-27 11:36:35,381 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      1344.1348, cscript.exe  //nologo m.vbs
2018-03-27 11:36:41,603 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.1324, taskdl.exe
2018-03-27 11:36:42,939 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, taskdl.exe
2018-03-27 11:36:43,904 Process      INFO     ExitProcess   : Process: cmd.exe     , Cid:
           1344, cscript.exe  //nologo m.vbs
2018-03-27 11:36:54,808 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, C:\Windows\system32\cmd.exe /c 284781522143356.bat
2018-03-27 11:37:17,800 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.1324, taskdl.exe
2018-03-27 11:37:23,260 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, taskdl.exe
2018-03-27 11:37:54,960 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.1324, taskdl.exe
2018-03-27 11:37:55,506 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, taskdl.exe
2018-03-27 11:38:00,229 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.12cc, @WanaDecryptor@.exe co
2018-03-27 11:38:00,499 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.12cc, cmd.exe /c start /b @WanaDecryptor@.exe vs
2018-03-27 11:38:01,080 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      11b8.11b0, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 11:38:05,626 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      11b8.11b0, @WanaDecryptor@.exe  vs
2018-03-27 11:38:07,084 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, cmd.exe /c start /b @WanaDecryptor@.exe vs
2018-03-27 11:38:10,544 Process      INFO     CreateProcess : Process: @WanaDecryptor@.exe
      , Cid:  11a8.11b4, TaskData\Tor\taskhsvc.exe
2018-03-27 11:38:11,014 Process      INFO     CreateProcess : Process: taskhsvc.exe, Cid:
      12f8.1304, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 11:38:17,857 Process      INFO     CreateProcess : Process: @WanaDecryptor@.exe
      , Cid:    bac.270, cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy
     delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {
     default} recoveryenabled no & wbadmin delete catalog -quiet
2018-03-27 11:38:18,356 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      13b8.13b4, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 11:38:18,538 Process      INFO     ExitProcess   : Process: conhost.exe , Cid:
           11fc, @WanaDecryptor@.exe  vs
```

```
2018-03-27 11:38:20,368 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      13b8.13b4, vssadmin  delete shadows /all /quiet
2018-03-27 11:38:21,444 Process      INFO     ExitProcess   : Process: cmd.exe     , Cid:
           13b8, vssadmin  delete shadows /all /quiet
2018-03-27 11:38:21,567 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
      13b8.13b4, wmic  shadowcopy delete
2018-03-27 11:38:26,224 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.1334, taskse.exe C:\ProgramData\dtuynyjtysq538\@WanaDecryptor@.exe
2018-03-27 11:38:27,330 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.1334, cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
     "dtuynyjtysq538" /t REG_SZ /d "\"C:\ProgramData\dtuynyjtysq538\tasksche.exe\"" /f
2018-03-27 11:38:27,899 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
        b44.62c, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 11:38:29,316 Process      INFO     CreateProcess : Process: taskse.exe  , Cid:
      10e4.10ec, "C:\ProgramData\dtuynyjtysq538\@WanaDecryptor@.exe"
2018-03-27 11:38:30,312 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, taskse.exe C:\ProgramData\dtuynyjtysq538\@WanaDecryptor@.exe
2018-03-27 11:38:31,446 Process      INFO     ExitProcess   : Process: cmd.exe     , Cid:
           13b8, wmic  shadowcopy delete
2018-03-27 11:38:33,985 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
      12c8.1324, taskdl.exe
2018-03-27 11:38:35,858 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, taskdl.exe
2018-03-27 11:38:36,683 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
        b44.62c, reg  add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "
     dtuynyjtysq538" /t REG_SZ /d "\"C:\ProgramData\dtuynyjtysq538\tasksche.exe\"" /f
2018-03-27 11:38:38,931 Process      INFO     ExitProcess   : Process: cmd.exe     , Cid:
     b44, reg  add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "dtuynyjtysq538"
     /t REG_SZ /d "\"C:\ProgramData\dtuynyjtysq538\tasksche.exe\"" /f
2018-03-27 11:38:39,836 Process      INFO     ExitProcess   : Process: cmd.exe     , Cid:
           13b8, \??\C:\Windows\system32\conhost.exe 0x4
2018-03-27 11:38:40,375 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid:
           12c8, cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
     "dtuynyjtysq538" /t REG_SZ /d "\"C:\ProgramData\dtuynyjtysq538\tasksche.exe\"" /f
```

A.2 Journaux d'accès aux fichiers

```
2018-03-27 12:28:01,412 Process      INFO     CreateProcess : Process: wannacry.exe , Cid:
         a98.538, C:\WINDOWS\tasksche.exe /i
2018-03-27 12:28:02,502 File INFO     ReadFile      : Process: tasksche.exe, Cid:    ff0.
     fec, '\\Windows\\tasksche.exe'
2018-03-27 12:28:02,530 File INFO     WriteFile     : Process: tasksche.exe, Cid:    ff0.
     fec, '\\ProgramData\\dtuynyjtysq538\\tasksche.exe'
2018-03-27 12:28:02,546 File INFO     ReadFile      : Process: tasksche.exe, Cid:    ff0.
     fec, '\\Windows\\tasksche.exe'
2018-03-27 12:28:02,564 File INFO     WriteFile     : Process: tasksche.exe, Cid:    ff0.
     fec, '\\ProgramData\\dtuynyjtysq538\\tasksche.exe'
2018-03-27 12:28:02,578 File INFO     ReadFile      : Process: tasksche.exe, Cid:    ff0.
     fec, '\\Windows\\tasksche.exe'
2018-03-27 12:28:02,645 File INFO     WriteFile     : Process: tasksche.exe, Cid:    ff0.
     fec, '\\ProgramData\\dtuynyjtysq538\\tasksche.exe'
2018-03-27 12:28:02,656 File INFO     ReadFile      : Process: tasksche.exe, Cid:    ff0.
     fec, '\\Windows\\tasksche.exe'
2018-03-27 12:28:02,675 File INFO     WriteFile     : Process: tasksche.exe, Cid:    ff0.
     fec, '\\ProgramData\\dtuynyjtysq538\\tasksche.exe'
2018-03-27 12:28:02,690 File INFO     ReadFile      : Process: tasksche.exe, Cid:    ff0.
     fec, '\\Windows\\tasksche.exe'
2018-03-27 12:28:02,710 File INFO     WriteFile     : Process: tasksche.exe, Cid:    ff0.
     fec, '\\ProgramData\\dtuynyjtysq538\\tasksche.exe'
2018-03-27 12:28:02,736 File INFO     ReadFile      : Process: tasksche.exe, Cid:    ff0.
     fec, '\\Windows\\tasksche.exe'
2018-03-27 12:28:02,764 File INFO     WriteFile     : Process: tasksche.exe, Cid:    ff0.
     fec, '\\ProgramData\\dtuynyjtysq538\\tasksche.exe'
2018-03-27 12:28:02,780 File INFO     ReadFile      : Process: tasksche.exe, Cid:    ff0.
     fec, '\\Windows\\tasksche.exe'
2018-03-27 12:28:02,812 File INFO     WriteFile     : Process: tasksche.exe, Cid:    ff0.
     fec, '\\ProgramData\\dtuynyjtysq538\\tasksche.exe'
2018-03-27 12:28:02,912 Service      INFO     CreateService : Process: tasksche.exe, Cid:
        ff0.fec, 'dtuynyjtysq538'
2018-03-27 12:28:02,976 Process      INFO     CreateProcess : Process: services.exe, Cid:
        220.3a0, cmd.exe /c "C:\ProgramData\dtuynyjtysq538\tasksche.exe"
2018-03-27 12:28:06,977 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
        ba4.f84, C:\ProgramData\dtuynyjtysq538\tasksche.exe
2018-03-27 12:28:07,466 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\b.wnry'
```

```
2018-03-27 12:28:08,448 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\c.wnry'
2018-03-27 12:28:08,493 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_bulgarian.wnry'
2018-03-27 12:28:08,601 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_chinese (simplified).wnry'
2018-03-27 12:28:08,689 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_chinese (traditional).wnry'
2018-03-27 12:28:08,806 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_croatian.wnry'
2018-03-27 12:28:08,938 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_czech.wnry'
2018-03-27 12:28:09,005 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_danish.wnry'
2018-03-27 12:28:09,072 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_dutch.wnry'
2018-03-27 12:28:09,142 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_english.wnry'
2018-03-27 12:28:09,203 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_filipino.wnry'
2018-03-27 12:28:09,271 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_finnish.wnry'
2018-03-27 12:28:09,358 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_french.wnry'
2018-03-27 12:28:09,431 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_german.wnry'
2018-03-27 12:28:09,528 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_greek.wnry'
2018-03-27 12:28:09,800 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_indonesian.wnry'
2018-03-27 12:28:09,866 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_italian.wnry'
2018-03-27 12:28:09,954 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_japanese.wnry'
2018-03-27 12:28:10,057 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_korean.wnry'
2018-03-27 12:28:10,191 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_latvian.wnry'
2018-03-27 12:28:10,296 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_norwegian.wnry'
2018-03-27 12:28:10,374 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_polish.wnry'
2018-03-27 12:28:10,443 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_portuguese.wnry'
2018-03-27 12:28:10,516 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_romanian.wnry'
2018-03-27 12:28:10,597 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_russian.wnry'
2018-03-27 12:28:10,679 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_slovak.wnry'
2018-03-27 12:28:10,767 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_spanish.wnry'
2018-03-27 12:28:10,869 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_swedish.wnry'
2018-03-27 12:28:10,966 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_turkish.wnry'
2018-03-27 12:28:11,045 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\msg\\m_vietnamese.wnry'
2018-03-27 12:28:11,150 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\r.wnry'
2018-03-27 12:28:11,197 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\s.wnry'
2018-03-27 12:28:13,471 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\t.wnry'
2018-03-27 12:28:13,589 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\taskdl.exe'
2018-03-27 12:28:13,698 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\taskse.exe'
2018-03-27 12:28:13,774 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\u.wnry'
2018-03-27 12:28:14,267 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\c.wnry'
2018-03-27 12:28:14,357 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
       420.7c8, attrib +h .
2018-03-27 12:28:14,540 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
       420.7c8, icacls . /grant Everyone:F /T /C /Q
```

```
2018-03-27 12:28:14,623 Process      INFO     CreateProcess : Process: attrib.exe  , Cid:
        c08.c2c, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 12:28:15,010 Process      INFO     CreateProcess : Process: icacls.exe  , Cid:
        318.d1c, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 12:28:15,461 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\t.wnry'
2018-03-27 12:28:15,679 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\c.wnry'
2018-03-27 12:28:17,110 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid
     :420, icacls . /grant Everyone:F /T /C /Q
2018-03-27 12:28:18,186 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\00000000.pky'
2018-03-27 12:28:18,363 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\00000000.eky'
2018-03-27 12:28:18,384 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\00000000.pky'
2018-03-27 12:28:18,494 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.
     ccc, '\\ProgramData\\dtuynyjtysq538\\00000000.res'
2018-03-27 12:28:18,988 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid
     :420, attrib +h .
2018-03-27 12:28:19,045 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
        420.e0c, taskdl.exe
2018-03-27 12:28:19,565 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\00000000.pky'
2018-03-27 12:28:19,595 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\00000000.res'
2018-03-27 12:28:19,641 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\c.wnry'
2018-03-27 12:28:19,669 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\u.wnry'
2018-03-27 12:28:19,752 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe'
2018-03-27 12:28:19,763 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\u.wnry'
2018-03-27 12:28:19,776 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe'
2018-03-27 12:28:20,018 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:20,063 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid
     :420, taskdl.exe
2018-03-27 12:28:20,408 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
        420.7c8, C:\Windows\system32\cmd.exe /c 56291522146484.bat
2018-03-27 12:28:20,457 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\r.wnry'
2018-03-27 12:28:20,485 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:20,635 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
        ca0.64c, \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2018-03-27 12:28:21,647 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\@Please_Read_Me@.txt'
2018-03-27 12:28:21,676 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe'
2018-03-27 12:28:21,689 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\@WanaDecryptor@.exe'
2018-03-27 12:28:21,697 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe'
2018-03-27 12:28:21,710 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\@WanaDecryptor@.exe'
2018-03-27 12:28:21,786 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:22,086 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:22,102 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\AppV\\Setup\\@Please_Read_Me@.txt'
2018-03-27 12:28:23,108 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:23,541 File INFO     WriteFile     : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\m.vbs'
2018-03-27 12:28:24,693 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:24,748 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\m.vbs'
2018-03-27 12:28:24,962 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:24,989 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\m.vbs'
```

```
2018-03-27 12:28:25,527 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:25,546 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\User Account Pictures\\@Please_Read_Me@.txt'
2018-03-27 12:28:26,367 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
    .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:26,529 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
    .64c, '\\ProgramData\\dtuynyjtysq538\\m.vbs'
2018-03-27 12:28:27,886 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
    .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:28,285 Process      INFO     CreateProcess : Process: cmd.exe     , Cid:
       ca0.64c, cscript.exe  //nologo m.vbs
2018-03-27 12:28:29,223 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:29,235 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\@Please_Read_Me@.txt'
2018-03-27 12:28:29,549 File INFO     ReadFile      : Process: cscript.exe , Cid:    e44
    .70c, '\\Windows\\SysWOW64\\cscript.exe'
2018-03-27 12:28:30,445 File INFO     ReadFile      : Process: cscript.exe , Cid:    e44
    .70c, '\\ProgramData\\dtuynyjtysq538\\m.vbs'
2018-03-27 12:28:30,880 File INFO     ReadFile      : Process: cscript.exe , Cid:    e44
    .70c, '\\Windows\\SysWOW64\\wshom.ocx'
2018-03-27 12:28:32,524 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows\\SystemData\\S-1-5-18\\ReadOnly\\LockScreen_Z
    \\LockScreen___1024_0768_notdimmed.jpg'
2018-03-27 12:28:32,547 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows\\SystemData\\S-1-5-18\\ReadOnly\\LockScreen_Z
    \\LockScreen___1024_0768_notdimmed.jpg.WNCRYT'
2018-03-27 12:28:32,608 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows\\SystemData\\S-1-5-18\\ReadOnly\\LockScreen_Z
    \\LockScreen___1024_0768_notdimmed.jpg'
2018-03-27 12:28:32,956 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows\\SystemData\\S-1-5-18\\ReadOnly\\LockScreen_Z
    \\LockScreen___1024_0768_notdimmed.jpg.WNCRYT'
2018-03-27 12:28:34,801 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows Defender\\Network Inspection System\\Support\\
    NisLog.txt'
2018-03-27 12:28:34,819 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows Defender\\Network Inspection System\\Support\\
    NisLog.txt.WNCRYT'
2018-03-27 12:28:34,898 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows Defender\\Network Inspection System\\Support\\
    NisLog.txt'
2018-03-27 12:28:34,925 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows Defender\\Network Inspection System\\Support\\
    NisLog.txt.WNCRYT'
2018-03-27 12:28:35,445 File INFO     WriteFile     : Process: cscript.exe , Cid:    e44
    .70c, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:37,107 Process      INFO     ExitProcess   : Process: cmd.exe     , Cid:
    ca0, cscript.exe  //nologo m.vbs
2018-03-27 12:28:38,024 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:38,036 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows Live\\@Please_Read_Me@.txt'
2018-03-27 12:28:38,060 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:38,075 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows Live\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:39,634 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows NT\\MSScan\\WelcomeScan.jpg'
2018-03-27 12:28:39,674 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows NT\\MSScan\\WelcomeScan.jpg.WNCRYT'
2018-03-27 12:28:39,837 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows NT\\MSScan\\WelcomeScan.jpg'
2018-03-27 12:28:39,881 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows NT\\MSScan\\WelcomeScan.jpg.WNCRYT'
2018-03-27 12:28:39,956 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:39,969 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows NT\\MSScan\\@Please_Read_Me@.txt'
2018-03-27 12:28:39,993 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:40,007 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Windows NT\\MSScan\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:41,795 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
    .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
```

```
2018-03-27 12:28:42,457 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:42,479 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\defaultuser0\\AppData\\Local\\@Please_Read_Me@.txt'
2018-03-27 12:28:42,504 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:42,520 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\defaultuser0\\AppData\\Local\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:43,722 Service      INFO     StartService  : Process: tasksche.exe, Cid:
        ff0.fec, 'dtuynyjtysq538'
2018-03-27 12:28:44,570 Process      INFO     ExitProcess   : Process: conhost.exe , Cid:
     db8, C:\WINDOWS\tasksche.exe /i
2018-03-27 12:28:45,496 File INFO     ReadFile      : Process: cmd.exe     , Cid:    ca0
     .64c, '\\ProgramData\\dtuynyjtysq538\\56291522146484.bat'
2018-03-27 12:28:47,738 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\defaultuser0\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles
     \\CachedImage_1024_768_POS4.jpg'
2018-03-27 12:28:47,768 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\defaultuser0\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles
     \\CachedImage_1024_768_POS4.jpg.WNCRYT'
2018-03-27 12:28:47,841 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\defaultuser0\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles
     \\CachedImage_1024_768_POS4.jpg'
2018-03-27 12:28:47,862 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\defaultuser0\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles
     \\CachedImage_1024_768_POS4.jpg.WNCRYT'
2018-03-27 12:28:48,481 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid
     :420, C:\Windows\system32\cmd.exe /c 56291522146484.bat
2018-03-27 12:28:48,662 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:48,685 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\@Please_Read_Me@.txt'
2018-03-27 12:28:48,713 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:48,736 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:49,080 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@Please_Read_Me@.txt'
2018-03-27 12:28:49,102 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\ConnectedDevicesPlatform\\@Please_Read_Me@.txt'
2018-03-27 12:28:49,127 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\dtuynyjtysq538\\@WanaDecryptor@.exe.lnk'
2018-03-27 12:28:49,143 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\ConnectedDevicesPlatform\\@WanaDecryptor@.exe.lnk
     '
2018-03-27 12:28:49,544 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Microsoft\\Internet Explorer\\brndlog.txt'
2018-03-27 12:28:49,598 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Microsoft\\Internet Explorer\\brndlog.txt.WNCRYT'
2018-03-27 12:28:49,682 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Microsoft\\Internet Explorer\\brndlog.txt'
2018-03-27 12:28:49,702 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Microsoft\\Internet Explorer\\brndlog.txt.WNCRYT'
2018-03-27 12:28:53,204 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.
     ccc, '\\ProgramData\\dtuynyjtysq538\\00000000.res'
2018-03-27 12:28:55,614 Process      INFO     CreateProcess : Process: tasksche.exe, Cid:
        420.e0c, taskdl.exe
2018-03-27 12:28:56,435 Process      INFO     ExitProcess   : Process: tasksche.exe, Cid
     :420, taskdl.exe
2018-03-27 12:29:06,926 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
     \\LocalState\\ConstraintIndex\\Apps_{e2ad21c5-58e6-406d-946d-6f3b570cdfcb}\\0.0.
     filtertrie.intermediate.txt'
2018-03-27 12:29:06,952 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
     \\LocalState\\ConstraintIndex\\Apps_{e2ad21c5-58e6-406d-946d-6f3b570cdfcb}\\0.0.
     filtertrie.intermediate.txt.WNCRYT'
2018-03-27 12:29:07,032 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
     \\LocalState\\ConstraintIndex\\Apps_{e2ad21c5-58e6-406d-946d-6f3b570cdfcb}\\0.0.
     filtertrie.intermediate.txt'
2018-03-27 12:29:07,052 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
     \\LocalState\\ConstraintIndex\\Apps_{e2ad21c5-58e6-406d-946d-6f3b570cdfcb}\\0.0.
     filtertrie.intermediate.txt.WNCRYT'
2018-03-27 12:29:07,475 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
```

```
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsconversions.txt'
2018-03-27 12:29:07,499 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsconversions.txt.WNCRYT'
2018-03-27 12:29:07,551 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsconversions.txt'
2018-03-27 12:29:07,566 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsconversions.txt.WNCRYT'
2018-03-27 12:29:07,923 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsglobals.txt'
2018-03-27 12:29:07,947 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsglobals.txt.WNCRYT'
2018-03-27 12:29:07,998 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsglobals.txt'
2018-03-27 12:29:08,095 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appsglobals.txt.WNCRYT'
2018-03-27 12:29:08,204 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appssynonyms.txt'
2018-03-27 12:29:08,225 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appssynonyms.txt.WNCRYT'
2018-03-27 12:29:08,278 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appssynonyms.txt'
2018-03-27 12:29:08,292 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      appssynonyms.txt.WNCRYT'
2018-03-27 12:29:08,384 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      settingsconversions.txt'
2018-03-27 12:29:08,410 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      settingsconversions.txt.WNCRYT'
2018-03-27 12:29:08,515 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      settingsconversions.txt'
2018-03-27 12:29:08,536 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      settingsconversions.txt.WNCRYT'
2018-03-27 12:29:08,689 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      settingsglobals.txt'
2018-03-27 12:29:08,715 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      settingsglobals.txt.WNCRYT'
2018-03-27 12:29:08,767 File INFO     ReadFile       : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
      \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
      settingsglobals.txt'
2018-03-27 12:29:08,780 File INFO     WriteFile      : Process: tasksche.exe, Cid:    420.7
      c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
```

```
    \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
    settingsglobals.txt.WNCRYT'
2018-03-27 12:29:08,881 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
    settingssynonyms.txt'
2018-03-27 12:29:08,905 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
    settingssynonyms.txt.WNCRYT'
2018-03-27 12:29:08,961 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
    settingssynonyms.txt'
2018-03-27 12:29:08,997 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\ConstraintIndex\\Input_{4c32d54c-ede4-4ee0-b6ef-861e712a2839}\\
    settingssynonyms.txt.WNCRYT'
2018-03-27 12:29:09,156 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180498955994.txt'
2018-03-27 12:29:09,195 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180498955994.txt.WNCRYT'
2018-03-27 12:29:09,268 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180498955994.txt'
2018-03-27 12:29:09,284 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180498955994.txt.WNCRYT'
2018-03-27 12:29:09,336 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\dtuynyjtysq538\\f.wnry'
2018-03-27 12:29:09,375 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180752514225.txt'
2018-03-27 12:29:09,396 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180752514225.txt.WNCRYT'
2018-03-27 12:29:09,448 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180752514225.txt'
2018-03-27 12:29:09,464 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650180752514225.txt.WNCRYT'
2018-03-27 12:29:09,515 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650194603407053.txt'
2018-03-27 12:29:09,543 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650194603407053.txt.WNCRYT'
2018-03-27 12:29:09,596 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650194603407053.txt'
2018-03-27 12:29:09,616 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650194603407053.txt.WNCRYT'
2018-03-27 12:29:09,709 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650215873127425.txt'
2018-03-27 12:29:09,747 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650215873127425.txt.WNCRYT'
2018-03-27 12:29:09,877 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650215873127425.txt'
2018-03-27 12:29:09,901 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.Cortana_cw5n1h2txyewy
    \\LocalState\\DeviceSearchCache\\AppCache131650215873127425.txt.WNCRYT'
2018-03-27 12:29:19,865 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles\\
    CachedImage_1024_768_POS4.jpg'
2018-03-27 12:29:19,912 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles\\
    CachedImage_1024_768_POS4.jpg.WNCRYT'
2018-03-27 12:29:19,975 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles\\
    CachedImage_1024_768_POS4.jpg'
```

```
2018-03-27 12:29:19,993 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\Users\\user\\AppData\\Roaming\\Microsoft\\Windows\\Themes\\CachedFiles\\
    CachedImage_1024_768_POS4.jpg.WNCRYT'
2018-03-27 12:29:22,458 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\AppV\\Setup\\OfficeIntegrator.ps1'
2018-03-27 12:29:22,517 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\AppV\\Setup\\OfficeIntegrator.ps1.WNCRYT'
2018-03-27 12:29:22,589 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\AppV\\Setup\\OfficeIntegrator.ps1'
2018-03-27 12:29:22,611 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\AppV\\Setup\\OfficeIntegrator.ps1.WNCRYT'
2018-03-27 12:29:22,755 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\background.png'
2018-03-27 12:29:22,776 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\background.png.WNCRYT'
2018-03-27 12:29:22,878 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\background.png'
2018-03-27 12:29:22,895 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\background.png.WNCRYT'
2018-03-27 12:29:22,971 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\device.png'
2018-03-27 12:29:22,994 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\device.png.WNCRYT'
2018-03-27 12:29:23,112 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\device.png'
2018-03-27 12:29:23,138 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\device.png.WNCRYT'
2018-03-27 12:29:23,270 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\overlay.png'
2018-03-27 12:29:23,289 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\overlay.png.WNCRYT'
2018-03-27 12:29:23,491 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\overlay.png'
2018-03-27 12:29:23,508 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\overlay.png.WNCRYT'
2018-03-27 12:29:23,619 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\superbar.png'
2018-03-27 12:29:23,638 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\superbar.png.WNCRYT'
2018-03-27 12:29:23,714 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\superbar.png'
2018-03-27 12:29:23,728 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{113527a4-45d4-4b6f-b567-97838
    f1b04b0}\\superbar.png.WNCRYT'
2018-03-27 12:29:23,885 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
    d3decd87120}\\background.png'
2018-03-27 12:29:23,991 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
    d3decd87120}\\background.png.WNCRYT'
2018-03-27 12:29:24,043 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
    d3decd87120}\\background.png'
2018-03-27 12:29:24,061 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
    d3decd87120}\\background.png.WNCRYT'
2018-03-27 12:29:24,223 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
    d3decd87120}\\watermark.png'
2018-03-27 12:29:24,244 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
    c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
    d3decd87120}\\watermark.png.WNCRYT'
```

```
2018-03-27 12:29:24,342 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
     d3decd87120}\\watermark.png'
2018-03-27 12:29:24,355 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Device Stage\\Device\\{8702d817-5aad-4674-9ef3-4
     d3decd87120}\\watermark.png.WNCRYT'
2018-03-27 12:29:24,781 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Search\\Data\\Applications\\Windows\\tmp.edb'
2018-03-27 12:29:24,805 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Search\\Data\\Applications\\Windows\\tmp.edb.WNCRYT'
2018-03-27 12:29:24,984 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Search\\Data\\Applications\\Windows\\tmp.edb'
2018-03-27 12:29:25,002 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Search\\Data\\Applications\\Windows\\tmp.edb.WNCRYT'
2018-03-27 12:29:25,522 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.bmp'
2018-03-27 12:29:25,543 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.bmp.WNCRYT'
2018-03-27 12:29:25,603 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.bmp'
2018-03-27 12:29:25,744 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.bmp.WNCRYT'
2018-03-27 12:29:26,069 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.png'
2018-03-27 12:29:26,090 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.png.WNCRYT'
2018-03-27 12:29:26,244 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.png'
2018-03-27 12:29:26,257 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\guest.png.WNCRYT'
2018-03-27 12:29:26,540 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user-192.png'
2018-03-27 12:29:26,671 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user-192.png.WNCRYT'
2018-03-27 12:29:26,721 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user-192.png'
2018-03-27 12:29:26,734 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user-192.png.WNCRYT'
2018-03-27 12:29:27,005 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.bmp'
2018-03-27 12:29:27,244 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.bmp.WNCRYT'
2018-03-27 12:29:27,304 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.bmp'
2018-03-27 12:29:27,376 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.bmp.WNCRYT'
2018-03-27 12:29:27,709 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.png'
2018-03-27 12:29:27,736 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.png.WNCRYT'
2018-03-27 12:29:27,805 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.png'
2018-03-27 12:29:27,824 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\User Account Pictures\\user.png.WNCRYT'
2018-03-27 12:29:28,120 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\cversions.2.db'
2018-03-27 12:29:28,150 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\cversions.2.db.WNCRYT'
2018-03-27 12:29:28,199 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\cversions.2.db'
2018-03-27 12:29:28,210 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\cversions.2.db.WNCRYT'
2018-03-27 12:29:28,350 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.
     ccc, '\\ProgramData\\dtuynyjtysq538\\00000000.res'
2018-03-27 12:29:28,520 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{6AF0698E-D558-4F6E-9B3C-3716689AF493
     }.2.ver0x0000000000000001.db'
2018-03-27 12:29:28,563 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{6AF0698E-D558-4F6E-9B3C-3716689AF493
     }.2.ver0x0000000000000001.db.WNCRYT'
2018-03-27 12:29:28,641 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{6AF0698E-D558-4F6E-9B3C-3716689AF493
     }.2.ver0x0000000000000001.db'
2018-03-27 12:29:28,757 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{6AF0698E-D558-4F6E-9B3C-3716689AF493
     }.2.ver0x0000000000000001.db.WNCRYT'
```

```
2018-03-27 12:29:29,016 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2
     }.2.ver0x0000000000000001.db'
2018-03-27 12:29:29,046 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2
     }.2.ver0x0000000000000001.db.WNCRYT'
2018-03-27 12:29:29,130 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2
     }.2.ver0x0000000000000001.db'
2018-03-27 12:29:29,283 File INFO     WriteFile     : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows\\Caches\\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2
     }.2.ver0x0000000000000001.db.WNCRYT'
2018-03-27 12:29:29,738 File INFO     ReadFile      : Process: tasksche.exe, Cid:    420.7
     c8, '\\ProgramData\\Microsoft\\Windows Live\\WLive48x48.png'
```