

CLÔTURE ET LIVRAISON DU PROJET DAVFI

Livraison de la version Windows

2

Introduction

Projet DAVFI - Jalons

3

- Débuté en octobre 2012
- Livraison version Android octobre 2013. Commercialisation en cours.
- Livraison versions Linux (filtrage http, client, librairie, IHM) début septembre 2014 – Industrialisation en cours avec la GN
- Livraison versions Windows (IHM et module résident) ce jour
- Livraison d'outils annexes de gestion des bases et d'outils divers (moteur DAVFI type VirusTotal)
- Livraison chaine de collecte et de classification des malware (en lieu et place d'Alphalink)

4

DAVFI Windows

La version « phare » du projet

Présentation générale

5

- Architecture fortement multithreadée
- Code fortement optimisé pour performances optimales
 - ▣ Cela a nécessité des compromis techniques acceptables sans sacrifier les performances antivirales
- Tout ce qui est en relation avec la console centrale (partie TecLib) n'a pu être ni implémenté ni testé
 - ▣ Devra être fait durant la phase d'industrialisation
 - ▣ Les productions techniques afférentes sont cependant prêtes et transférées (source + personnels)

Présentation générale (2)

6

- Tous les codes sources ont été audités et assainis
 - ▣ Analyse statique par *flawfinder* (rapports fournis sur le DVD)
 - ▣ Analyse dynamique par *Valgrind* (rapports fournis sur le DVD)
- Documentation fournie par module
- Codes source commentés *in extenso*
- Quatre modules centraux : 1, 4, 5 et 6
 - ▣ Les autres sont transverses et intégrés dans les autres modules, IHM et module résident (service + pilote).

Application certifiée Microsoft

7

- L'ensemble du module résident (pilote + services) a été testé avec la certification Microsoft
 - ▣ Conformité à la norme Microsoft
 - ▣ Garantie de stabilité, de sécurité et de performances
 - ▣ Label de qualité *de facto*
- Quelques points (mineurs) en cours de finalisation
 - ▣ TimeOut sur cas particuliers (lecteurs FAT16 et 32)
 - ▣ Dépendants des choix stratégiques et commerciaux
 - ▣ Les autres AV ne les passent pas tous non plus, certains très peu

AScanFile 992014

Project Selection **Tests** Results Package

Run Selected

View Details

View By

Certification

| <input type="checkbox"/> | Sta | Test Name | Length | Target | Machine(s) |
|--------------------------|-----|--|---------|--------------|------------|
| <input type="checkbox"/> | ✓ | Setup Registry Test for Filter Driver Logo Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Object ID test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Mapped File IO Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | File IO Tests Win7 | 05h 00m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✗ | Antivirus Installable File System Filter Test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✗ | Installable File System Filter Test Win7 | 02h 00m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | ReparsePoints Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Txf2 Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | SMB_OplockRDR Win7 | 03h 20m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | callback test for process, thread, image and dbgprint Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | race test during process termination Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | process management test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | callback test for object Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Winsock Core Functional Test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✗ | Registry Symbolic Link Test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✗ | Registry Callback Tests Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Transactional Registry Wow Regressions Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | ShellReg APIs Unicode Test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | DeleteKeyEx Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | NtUnLoadKey2 Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | NtLoadKeyEx Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | SaveKeyEx Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | RegBadParameterTests-UNICODE Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | NT Registry APIs Invalid Params Test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Get Set Key Security Test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✗ | UNICODE Registry APIs Test Win7 | 30m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Oplocks Test Win7 | 01h 00m | AVFISCANFILE | WINDOWS7TE |
| <input type="checkbox"/> | ✓ | Syscache Test Win7 | 01h 30m | AVFISCANFILE | WINDOWS7TE |

AScanFile 992014

- Targets
 - AVFISCANFILE\SYS DEVICE\MUP
- OS Platforms
 - Windows 7 Client x64
- Product Types
 - File System
 - File System Anti Virus
- Test Status
 - Basic
 - Functional
 - Reliability
 - Certification

Passed: 23 test(s)
 Failed: 5 test(s)
 Running: 0 test(s)
 Not Run: 0 test(s)
Total: 28 test(s)
- Experiences
- Optional
- Machine Status
 - WINDOWS7TEST-PC ✓

View: Complete Browse...

| | | |
|-----------------------|--------------------------|---|
| Context Index: | | 2660203575 |
| Current: | | Test :UpdateOnCloseTest Group :CloseCleanupDelete Status :C000001C (IFSTEST_TEST_FILE_TIME_ERROR) WSystemText :\uponc\uponc1.dat TestVariant :00000003 Last64GeneralValue :01CFDB678C5C3000 Expected64GeneralValue :01A8E78F1E4CB000 Description :{Msg# CloseDel!uponc!23} Failure last access time did not fit in the acceptable range. Acceptable 01a8e78f1e4cb000 to 01a8e78f1e4cb000 observed 01cfdb678c5c3000.Non exFAT Lookup Query : http://www.microsoft.com/ContentRedirect.asp?prd=IFSKit&id=CloseDel!uponc!23&pver=2195 WDKTUID: A72C4D26-977B-19CB-2E11-D6F93917D718 |
| Parent: | | WTTLOG |
| Start Test | 9/28/2014 6:11:02.645 PM | Test :UpdateOnCloseTest Group :CloseCleanupDelete Status :C000001C (IFSTEST_TEST_FILE_TIME_ERROR) WSystemText :\uponc\uponc1.dat TestVariant :00000003 Last64GeneralValue :01CFDB678C5C3000 Expected64GeneralValue :01A8E78F1E4CB000 Description : {Msg# CloseDel!uponc!23} Failure last access time did not fit in the acceptable range. Acceptable 01a8e78f1e4cb000 to 01a8e78f1e4cb000 observed 01cfdb678c5c3000.Non exFAT Lookup Query : http://www.microsoft.com/ContentRedirect.asp?prd=IFSKit&id=CloseDel!uponc!23&pver=2195 WDKTUID: A72C4D26-977B-19CB-2E11-D6F93917D718 |
| Error | 9/28/2014 6:11:02.645 PM | 62C.188 : +TEST+SEV2 : Test :UpdateOnCloseTest Group :CloseCleanupDelete Status :C000001C (IFSTEST_TEST_FILE_TIME_ERROR) WSystemText :\uponc\uponc1.dat TestVariant :00000003 Last64GeneralValue :01CFDB678C5C3000 Expected64GeneralValue :01A8E78F1E4CB000 Description :{Msg# CloseDel!uponc!23} Failure last access time did not fit in the acceptable range. Acceptable 01a8e78f1e4cb000 to 01a8e78f1e4cb000 observed 01cfdb678c5c3000.Non exFAT Lookup Query : http://www.microsoft.com/ContentRedirect.asp?prd=IFSKit&id=CloseDel!uponc!23&pver=2195 WDKTUID: A72C4D26-977B-19CB-2E11-D6F93917D718 |
| File: | | d:\w7rmtm\testsrc\basetest\core_file_services\ifs_test_kit\code\main\main.c Line: 1239 |
| Error Type: | | 0x0 |
| Error Code: | | Error 0x00000000 |
| Error Text: | | |
| End Test | 9/28/2014 6:11:02.645 PM | Test :UpdateOnCloseTest Group :CloseCleanupDelete Status :C000001C (IFSTEST_TEST_FILE_TIME_ERROR) WSystemText :\uponc\uponc1.dat TestVariant :00000003 Last64GeneralValue :01CFDB678C5C3000 Expected64GeneralValue :01A8E78F1E4CB000 Description : {Msg# CloseDel!uponc!23} Failure last access time did not fit in the acceptable range. Acceptable 01a8e78f1e4cb000 to 01a8e78f1e4cb000 observed 01cfdb678c5c3000.Non exFAT Lookup Query : http://www.microsoft.com/ContentRedirect.asp?prd=IFSKit&id=CloseDel!uponc!23&pver=2195 WDKTUID: A72C4D26-977B-19CB-2E11-D6F93917D718 |
| Result: | | Fail |
| Repro: | | ifstest.exe l: -g Virus /n Ifstest-Local-Fat32Results.log /N 356789AB /T /p /m /E /j /r c: -d \Fat -a \datacoh.exe /u ifstest /U *rw53w52 |

| HCK Manager - [Ifstest-Local-Fat32Results.wtl - Report] | | |
|---|--|---|
| HCK Manager - [RegCbTestCtrl.wtl - Report] | | |
| View: | Complete | Browse... |
| Message | 9/28/2014 7:06:09.892 PM | B1C.3D4 : +VAR+PASS 9 : Tc_UnregisterCloseRace - passed |
| End Test | 9/28/2014 7:06:09.892 PM | Tc_UnregisterCloseRace - passed |
| Result: | Pass | |
| Repro: | RegCbTestCtrl.exe -regr | |
| Message | 9/28/2014 7:06:09.892 PM | B1C.3D4 : 8192 0000 04:06:10 : TcRunRegressions - test #10, Tc_SaveRestoreReplace |
| Message | 9/28/2014 7:06:09.892 PM | B1C.3D4 : 8192 0000 04:06:10 : Tc_SaveRestoreReplace - entering |
| Message | 9/28/2014 7:06:09.892 PM | B1C.3D4 : 8192 0000 04:06:10 : TcRegisterCallback - succeeded - altitude 1000, cookie 1cfdb835e3afb22 |
| Message | 9/28/2014 7:06:10.892 PM | B1C.3D4 : 8192 0000 04:06:10 : Tc_SaveRestoreReplace - [FAIL] RegRestoreKey failed, error 0x5 |
| Context | | |
| Context Index: | 3911508546 | |
| Current: | Tc_SaveRestoreReplace - one or more failures above | |
| Parent: | WTTLOG | |
| Message | 9/28/2014 7:06:10.892 PM | B1C.3D4 : 8192 0000 04:06:10 : TcUnregisterCallback - succeeded - cookie 1cfdb835e3afb22 |
| Start Test | 9/28/2014 7:06:10.892 PM | Tc_SaveRestoreReplace - one or more failures above |
| Error | 9/28/2014 7:06:10.892 PM | B1C.3D4 : +VAR+SEV1 10 : Tc_SaveRestoreReplace - one or more failures above |
| File: | d:\w7rmtm.public.amd64fre\internal\sdkttools\inc\ntlogwrap.c | Line: 557 |
| Error Type: | | |
| Error Code: | 0x0 | |
| Error Text: | Error 0x00000000 | |
| End Test | 9/28/2014 7:06:10.892 PM | Tc_SaveRestoreReplace - one or more failures above |
| Result: | Fail | |
| Repro: | RegCbTestCtrl.exe -regr | |
| Message | 9/28/2014 7:06:10.892 PM | B1C.3D4 : 8192 0000 04:06:10 : TcWaitForServiceState - Waiting for service 458a40 to enter state 1... |
| Pass/Fail Result Rollup Counts | 9/28/2014 7:06:10.892 PM | |
| Total: | 11 | |
| Passed: | 10 | |
| Failed: | 1 | |
| Blocked: | 0 | |
| Warned: | 0 | |
| Skipped: | 0 | |

| HCK Manager - [RegSymlink.wtl - Report] | | |
|---|---|--|
| View: Complete [Browse...] | | |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : Calling RegDeleteValue [root: 00000000000000F6; subvalue: _TestSubvalue] |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : RegDeleteValue succeeded. |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : Calling RegQueryInfoKey for key 00000000000000F6 |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : RegQueryInfoKey successful. |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : 0 subkeys found |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : 0 values found |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : Calling UtilRegRestoreKey for key 0000000000000112, file name: RegSymlinkTestOutput.test, flags: 8 |
| Context | | |
| Context Index: | 1326948942 | |
| Current: | UtilRegRestoreKey error 5 | |
| Parent: | WTTLOG | |
| Start Test | 9/28/2014 7:05:41.894 PM | UtilRegRestoreKey error 5 |
| Error | 9/28/2014 7:05:41.894 PM | 338.96C : +VAR+SEV1 15 : UtilRegRestoreKey error 5 |
| File: | d:\w7rmtm.public.amd64fre\internal\sdkttools\inc\ntlogwrap.c Line: 557 | |
| Error Type: | | |
| Error Code: | 0x0 | |
| Error Text: | Error 0x00000000 | |
| Context | | |
| Context Index: | 2241951469 | |
| Current: | RegCloseKey failed. [hKey: 0000000000000000, error: 6] | |
| Parent: | WTTLOG | |
| End Test | 9/28/2014 7:05:41.894 PM | UtilRegRestoreKey error 5 |
| Result: | Fail | |
| Repro: | RegSymlink.exe | |
| Message | 9/28/2014 7:05:41.894 PM | 338.96C : 8192 0000 04:05:41 : Calling Cleanup Reg Ops Test... |
| Start Test | 9/28/2014 7:05:41.894 PM | RegCloseKey failed. [hKey: 0000000000000000, error: 6] |
| Error | 9/28/2014 7:05:41.894 PM | 338.96C : +VAR+SEV1 16 : RegCloseKey failed. [hKey: 0000000000000000, error: 6] |
| File: | d:\w7rmtm.public.amd64fre\internal\sdkttools\inc\ntlogwrap.c Line: 557 | |
| Error Type: | | |
| Error Code: | 0x0 | |

| HCK Manager - [RegSymlink.wtl - Report] | |
|--|---|
| File Edit View Explorers Tools Window Help | |
| View: Complete Browse... | |
| Message | 9/28/2014 7:12:10.286 PM 7E0.B58 : VAR[PASS] 337 : SAVE/RESTORE TEST, RegSaveKey (0x10c, C:\regtestU.hive) ok |
| Start Test | 9/28/2014 7:12:10.286 PM End Variation reported |
| Message | 9/28/2014 7:12:10.286 PM 7E0.B58 : +VAR+PASS 337 : End Variation reported |
| End Test | 9/28/2014 7:12:10.286 PM End Variation reported |
| Result: | Pass |
| Repro: | Regbetau.exe -f param.lis |
| Error | 9/28/2014 7:12:10.286 PM 7E0.B58 : VAR[SEV2] 338 : SAVE/RESTORE TEST, RegRestoreKey (0x10c, C:\regtestU.hive) failed -> 0x5 |
| File: | d:\w7rtmt\testsrc\basetest\kernel\cm\regbeta\saverstr.c Line: 181 |
| Error Type: | |
| Error Code: | 0x0 |
| Error Text: | Error 0x00000000 |
| Start Test | 9/28/2014 7:12:10.286 PM End Variation reported |
| Error | 9/28/2014 7:12:10.286 PM 7E0.B58 : +VAR+SEV2 338 : End Variation reported |
| File: | d:\w7rtmt\testsrc\basetest\kernel\cm\regbeta\saverstr.c Line: 191 |
| Error Type: | |
| Error Code: | 0x0 |
| Error Text: | Error 0x00000000 |
| End Test | 9/28/2014 7:12:10.286 PM End Variation reported |
| Result: | Fail |
| Repro: | Regbetau.exe -f param.lis |
| Error | 9/28/2014 7:12:10.286 PM 7E0.B58 : VAR[SEV2] 339 : ENUM QUERY TEST (after restore), RegOpenKeyEx (HKEY (0x0000000000000010C)\Registry Beta Create Test) -> 0x2 |
| File: | d:\w7rtmt\testsrc\basetest\kernel\cm\regbeta\enumqry.c Line: 482 |
| Error Type: | |
| Error Code: | 0x0 |
| Error Text: | Error 0x00000000 |
| Start Test | 9/28/2014 7:12:10.286 PM End Variation reported |
| Error | 9/28/2014 7:12:10.286 PM 7E0.B58 : +VAR+SEV2 339 : End Variation reported |
| File: | d:\w7rtmt\testsrc\basetest\kernel\cm\regbeta\enumqry.c Line: 485 |

Module d'analyse des fichiers

13

- Analyse couplée de deux entités.
 - ▣ Un pilote de notification.
 - ▣ Un service d'analyse.
- Deux chaînes d'analyses dans le service.
 - ▣ Une pour les exécutables.
 - ▣ Une autre pour les documents avec contenu actif

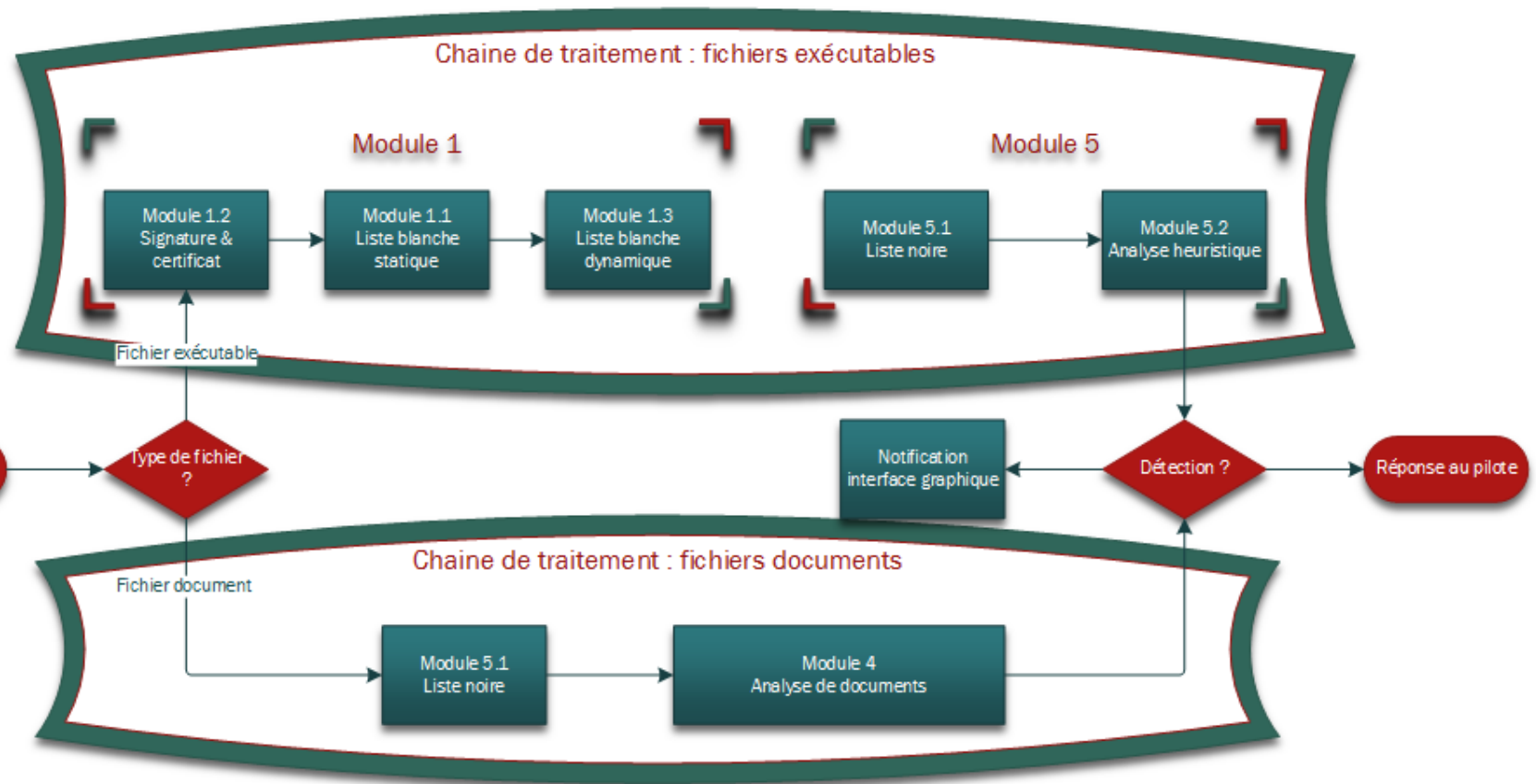
Structure modulaire et double

14

- Une application cliente (IHM) avec fonctionnalités réduites (pour l'utilisateur) et accès au mode Ninja (via la future console centrale; non testée)
- Cette application est en communication avec le module résident
 - ▣ Defense en profondeur
 - ▣ Si l'un des deux modes tombe, le second assure le relai.

Détail du fonctionnement du service d'analyse

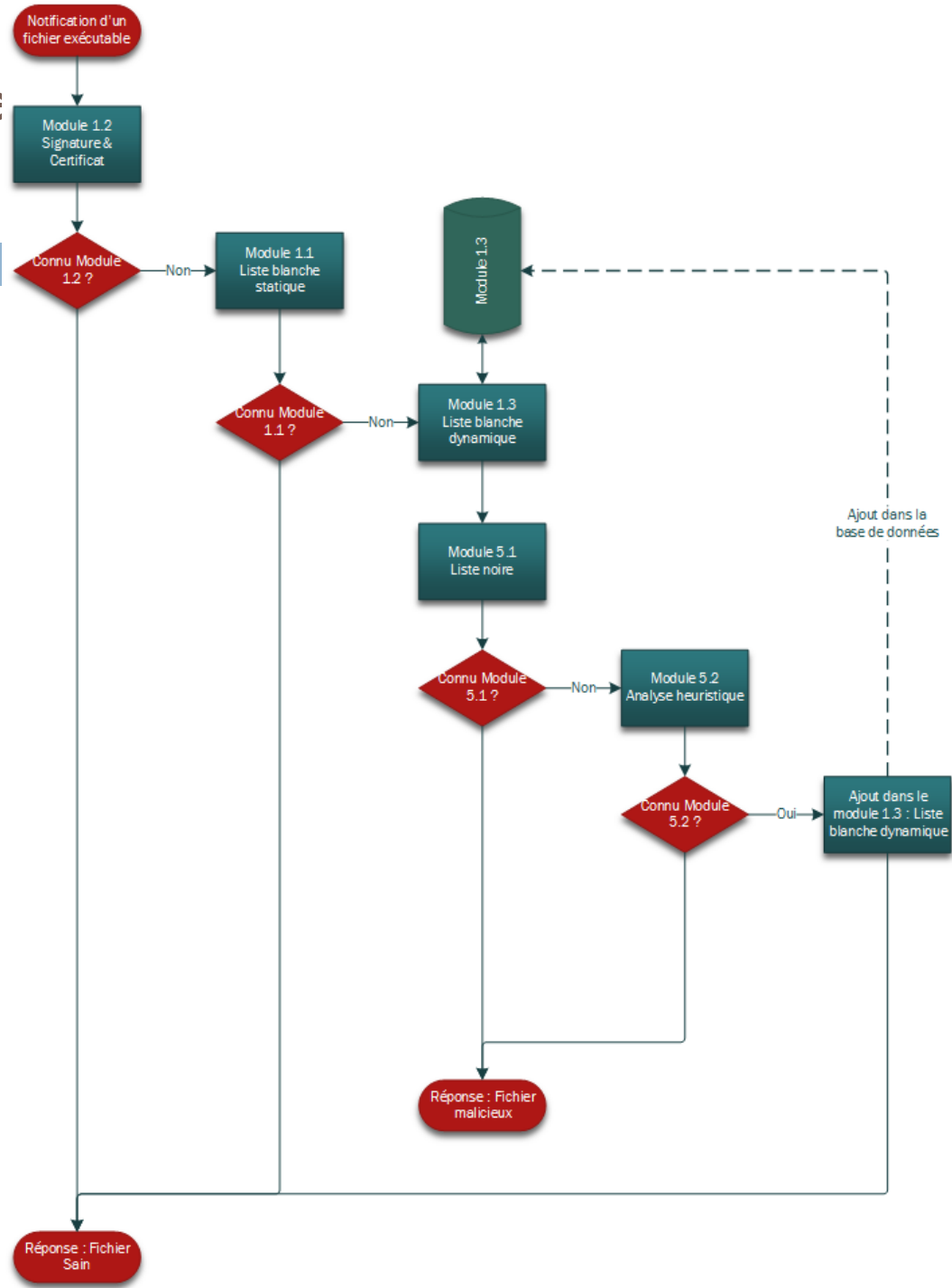
15



Détail de

ables

16



Module 1

17

- Modules 1.1 et 1.3 :
 - ▣ Module de liste blanches : permet de stocker dans des listes blanches (statique et dynamique) des fichiers dont on sait qu'ils sont sains (typiquement le dossier Windows) en conservant leur signature sha256. Ainsi, si un fichier de ces listes est testé, il sera considéré comme sain.
- Module 1.2 :
 - ▣ Module de vérification de certificats : permet de tester la présence d'un certificat de confiance dans le fichier testé. Si un tel certificat est trouvé, le fichier est alors considéré comme sain.
- Sans la console centrale, pas de mise à jour de la liste blanche dynamique permettant d'avoir un complément à la liste statique au fur et à mesure des mises à jour de Windows, afin de s'assurer que le système ne sera pas malencontreusement touché suite à une mise à jour.

Module 4

18

- Analyse des documents bureautiques
 - MS Office 97 → 2013
 - LibreOffice/OpenOffice 3.2 → 4.3
 - PDF 1.x
- Nettoyage des documents
 - Recodage
 - Transcodage
- Tout est configurable en mode Ninja

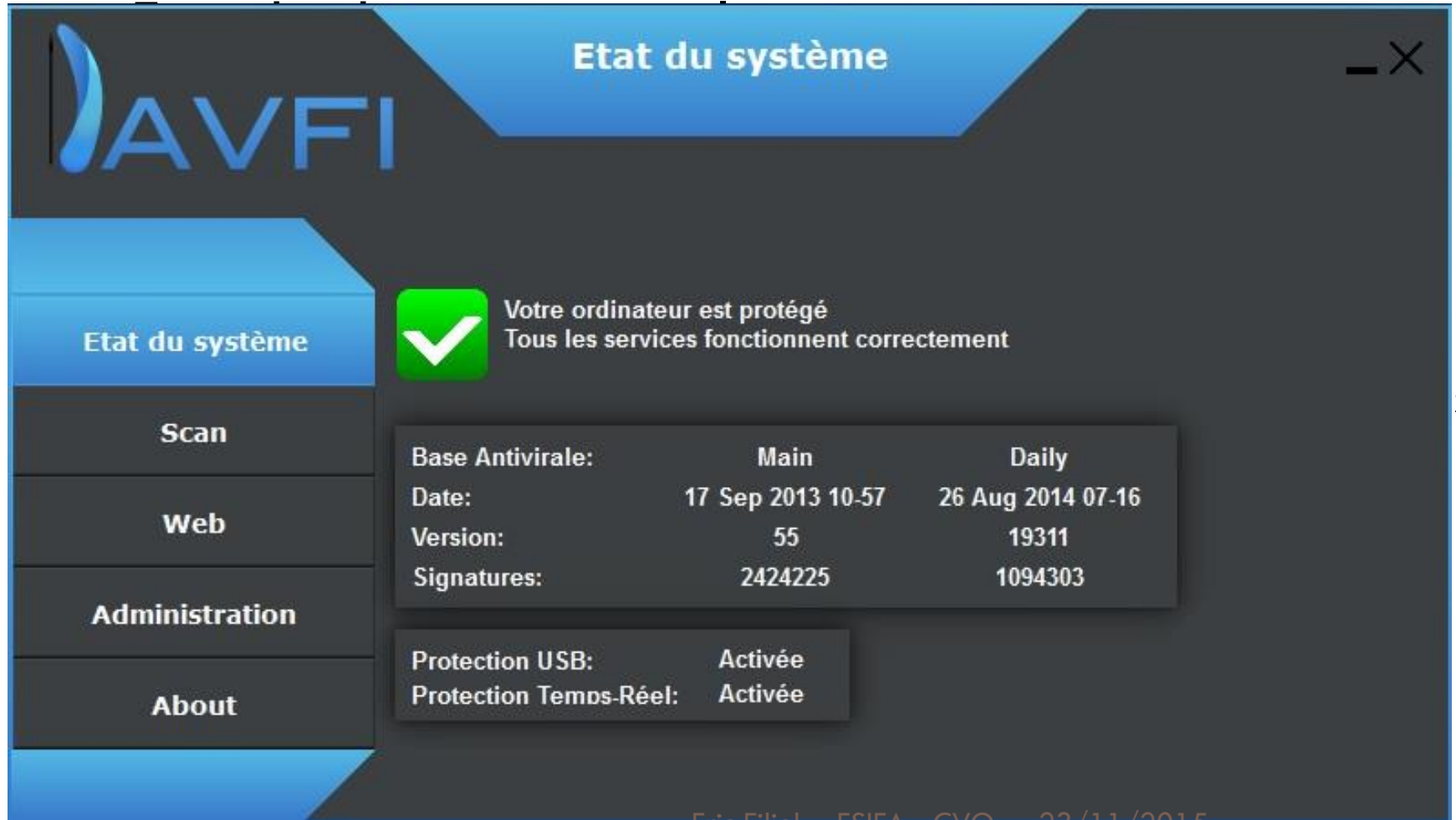
Interface

19

- Etat des bases antivirales
- Scan à la demande
- Planification d'analyse
- Analyse des périphériques USB
- Protection Temps-Réel de la sécurité des applications bureautiques
- Mini navigateur Web sécurisé

Interface

20



The screenshot shows the AVFI system status interface. The title bar reads "Etat du système". The AVFI logo is in the top left. A sidebar on the left contains menu items: "Etat du système", "Scan", "Web", "Administration", and "About". The main area displays a green checkmark icon and the text: "Votre ordinateur est protégé" and "Tous les services fonctionnent correctement". Below this, there are two tables of system information.

| Base Antivirale: | Main | Daily |
|------------------|-------------------|-------------------|
| Date: | 17 Sep 2013 10-57 | 26 Aug 2014 07-16 |
| Version: | 55 | 19311 |
| Signatures: | 2424225 | 1094303 |

| | |
|------------------------|---------|
| Protection USB: | Activée |
| Protection Temps-Réel: | Activée |

Impact de l'absence de la console centrale

21

- Du fait de la non disponibilité de la console centrale (partie TecLib) :
 - ▣ Impossibilité de mettre à jour les fichiers de configuration de l'utilisateur pour l'analyse des documents pour le module 4
 - ▣ Impossibilité de mettre en place la connexion en mode administrateur via l'interface graphique
 - ▣ Impossibilité de remonter les logs vers la console centrale lors d'un scan à la demande
 - ▣ Impossibilité de tester ces 3 fonctionnalités.

Module 5.1

22

- Scan par signatures (base SEClamav)
- Bases optimisées combinatoirement
 - ▣ Bases précurseurs
 - ▣ Bases complètes
- Deux bases : génériques et OIV (grâce au CA seul fournisseur de codes inconnus)
- Outils de création de signatures fournis
- MD5 remplacée systématiquement par SHA256 lorsque possible.

Module 5.2

23

- Module qui permet l'analyse statique de fichiers exécutables. Utilise des méthodes mathématiques et combinatoires afin d'analyser les fichiers.
- Difficultés :
 - ▣ le module 5.2 ayant un taux de faux positifs très faible mais non nul, il est possible que certains fichiers système soient touchés (après des mise à jour Windows). C'est ici qu'interviennent les listes blanches (en particulier 1.3).
 - ▣ Cependant, sans mise à jour dynamique grâce à la console centrale (non fournie), le module 5.2 ne peut être installé que sur une machine qui a servi à créer la liste blanche statique.

Sécurité de l'antivirus

24

- Protection des pilotes et des services **à la demande en fonction des clients.**
 - ▣ Pilote non interruptible
 - ▣ Service inarrêtable (non tuable).
 - ▣ Pilote de protection des exécutable tiers.
- Pour les démonstrations (et dans le msi) la protection maximale est désactivée
 - ▣ Sinon il serait impossible de désinstaller l'antivirus
 - ▣ Décision à prendre à l'issue de la phase d'industrialisation.

Protection de l'antivirus

25

- Protection des fichiers.
 - ▣ Mise en lecture seule des fichiers binaires de l'antivirus.
 - ▣ Absence de console centrale et de mise à jour contraignante.
- Protection du registre.
 - ▣ Protection des clés référençant les services et les pilotes.

Impact de l'absence de console centrale

26

- **Retard** dans le développement
 - Développement annexes **hors champ** direct de celui de l'**ESIEA**
 - Système de mise à jour basique
 - "Perte de temps" dans l'imagination de **solutions annexes**
 - Prise en main de l'écriture des normes xml pour la notification de la console centrale
 - Attente de solutions ou d'actions de Teclib qui ne sont **jamais arrivées**
- **Détournement** de ressources et de développeurs
 - Les équipes du laboratoire étant déjà fortement réduites...
- Remise au cause de la **sécurité optimale prévue et souhaitée**
 - Une partie de la **protection** de l'antivirus a du être revue et reportée dans la phase d'industrialisation
 - **Pénalisation** dans l'**efficacité de la détection** et dans la **fiabilité** des listes blanches (modules 1)
 - Oblige à **limiter** ou **brider** certains concepts ou développements imaginés pour le DAVFI
 - Les tests **de l'administration** centralisée et du traitement des menaces, du déploiement, des remontées d'alerte n'ont pu être faits.
- Les ressources (code source et personnels) sont transférés à Nov'lt pour prise en compte lors de la phase d'industrialisation.

27

Démonstrations

Demonstrations

28

- IHM
- Comparaison sécurité
 - ▣ Avira 0 – DAVFI 1
- Module résident
- Scan divers
- Opérations diverses

29

Conclusion

Transfert

30

- Transfert de la propriété intellectuelle pleine et entière pour industrialisation et commercialisation
- Transfert d'une équipe complète et experte
 - ▣ 7 ingénieurs juniors ayant été impliqués dans le développement de DAVFI
 - ▣ 1 docteur (UPMC)/ingénieur (X79) senior (soutien versions Linux et IHM)
 - ▣ 1 personnel responsable administratif senior
- Je conserve la propriété morale (Art. 113-1 & 121-1 du CPI)

Mediatisation (SP8)

31

- Le labo (C + V)O a fortement et directement contribué à la médiatisation technique et scientifique du projet
 - Envoyé Special (France 2)
 - Zone Interdite (M6)
 - Blogs Korben et Zataz
 - Tribunes diverses (01net, SécuritéOff...)
 - Challenge NDH 2014 en liaison avec Qwant
 - Contacts industriels (EMAT, Sonim, Qwant, Cristal consulting...)
- Nov'IT dispose de conditions très favorables pour la commercialisation.

Bilan

32

- Projet mené dans le respect des couts et des délais !
- Organisation du passage de relais dans les meilleures conditions
 - ▣ Nov'IT dispose de conditions optimales pour débiter la phase d'industrialisation et de commercialisation
- Nombreuses difficultés rencontrées cependant
 - ▣ Défaut Alphalink
 - ▣ Retards de paiement administration
 - ▣ Attitude de Microsoft
 - ▣ Impossibilité de recruter des personnels qualifiés (marché tendu, profils et compétences rares...)
 - ▣ Partie Teclib non livrée
 - ▣ Difficultés internes ESIEA.

Aspects PostDAVFI

33

- Le labo (C + V)⁰ assure le suivi et le soutien sur les modules 4 et 5.1 (versions livrées uniquement)
 - ▣ pour les autres modules, les personnels afférents sont transférés à Nov'IT qui devient *de facto* indépendant
- Stagiaires 3A, 4A et 5A prépositionnés (trois années de souplesse en termes RH) chez Nov'IT
- Projet 4A cette année au profit Nov'IT (4 stagiaires):

Questions & réponses

Signature du PV de livraison