SOUTENANCE DE STAGE

CRUCIANI DAVID

2020-2021

TUTEUR UNIVERSITÉ : MME. HERRMANN

TUTEUR ENTREPRISE : M. DULAUNOY

PLAN

- Entreprise
- Présentation du sujet
- Réalisation du projet
- Avenir du projet
- Conclusion

I. ENTREPRISE

SECURITY MADEIN.LU

fournir une réponse systématique aux menaces et incidents de sécurité informatique.

rassembler, examiner, signaler et répondre

MISP

PLAN

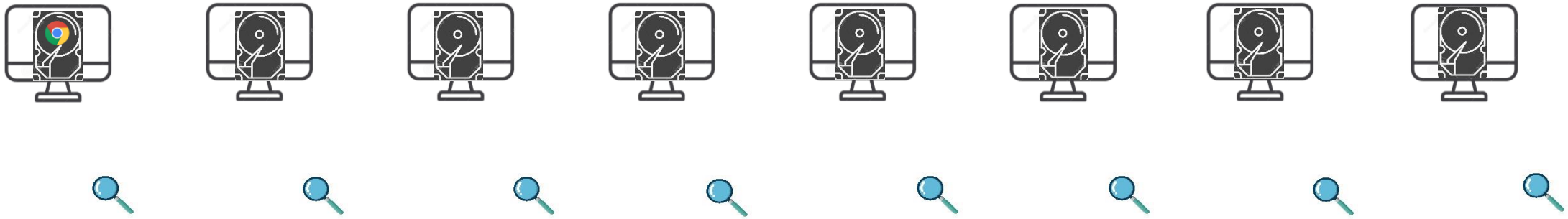
- Entreprise
- **Présentation du sujet**
- Réalisation du projet
- Avenir du projet
- Conclusion

II. PRÉSENTATION DU SUJET

Créer des profils d’activités et d’usages d’utilisateurs en utilisant des artefacts

Utiliser des artefacts remarquables afin de déterminer si un logiciel a été installé ou est installé sur une machine

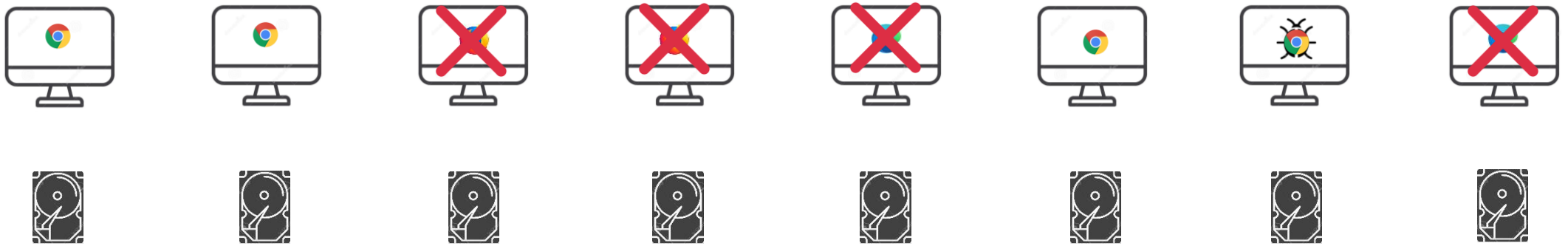
II. PRÉSENTATION DU SUJET



1h par disque

7h pour trouver le bon

II. PRÉSENTATION DU SUJET



3h de moins

II. PRÉSENTATION DU SUJET

"ça sert à trier mes merdes" A. Dulaunoy

https://github.com/CIRCL/factual-rules

https://github.com/CIRCL/factual-rules-generator

PLAN

- Entreprise
- Présentation du sujet
- **Réalisation du projet**
- Avenir du projet
- Conclusion

III. RÉALISATION DU PROJET - ANALYSE DE DISQUE

- Acquisition
- Conversion
- Préparation
- Analyse

III. RÉALISATION DU PROJET - VMS

Utiliser des artefacts remarquables afin de déterminer si un logiciel a été installé ou est installé sur une machine

- VM Windows sous VirtualBox
  - *VBoxManage*

- Copier-coller
- Qemu-img

III. RÉALISATION DU PROJET - INSTALLATION

Installateur:

- Chocolatey
- Msiexec
- Exe (humain)

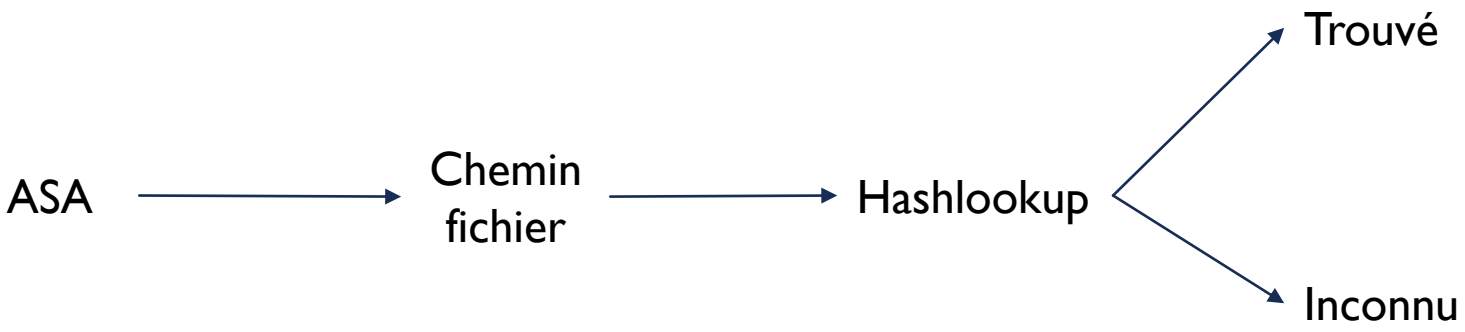
- Dossier partagé
  - Tache
  - Exe
  - AsaReport

III. RÉALISATION DU PROJET - INSTALLATION

```
1  Read the task to do;
2  si Uninstall alors
3  |  appManager() ; //uninstallation
4  |  SDelete();
5  sinon
6  |  AsaCollect() ; //point of comparaison
7  |  appManager() ; //installation
8  |  Search for exe path;
9  |  copy of exe;
10 |  run of exe;
11 |  AsaCollect() ; //point of comparaison
12 |  AsaExport() ; //creation of the report
13 fin
14 Shutdown
```

- SDelete
- ASA (AttackSurfaceAnalyzer)

III. RÉALISATION DU PROJET - INSTALLATION



III. RÉALISATION DU PROJET - CRÉATION YARA

3 résultat possible

- Exe
- Fls
- Strings

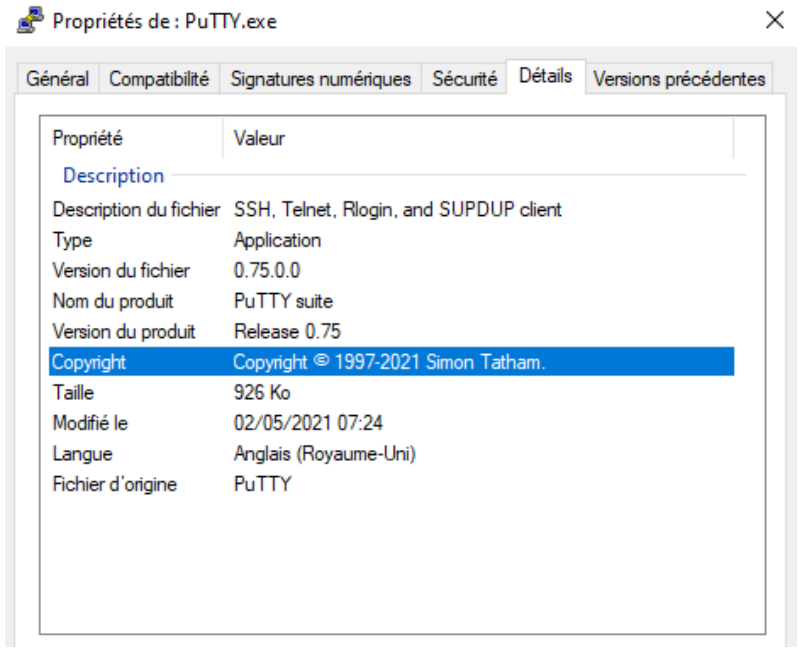
```
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClu:              :~/VM/My_Windows$ strings out_first.img | head -n 30
r/r 6-128-4:    $Bitmap t&fh
r/r 6-128-5:    $Bitmap TCPAu2
r/r 7-128-1:    $Boot   r,fh
d/d 11-144-4:   $Extend fSfSfUfh
+ d/d 29-144-2: $Delete( Invalid partition table
++ -/d * 446078-144-1:  Error loading operating system
+++ -/r * 446079-128-3: Missing operating system
+ r/r 25-144-6: $ObjId:( NTFS
+ r/r 24-144-3: $Quota:( NTFSu
+ r/r 24-144-2: $Quota:( TCPAu$
+ r/r 26-144-5: $Repars( fSfSfU
+ d/d 27-144-2: $RmMeta( fY[ZfYfY
++ r/r 28-128-4:         A disk read error occurred
++ r/r 28-128-2:         BOOTMGR is compressed
++ r/r 28-128-6:         Press Ctrl+Alt+Del to restart
++ r/r 28-128-8:         An operating system wasn't found. Try disconnecting any drives that don't
++ d/d 31-144-51:        contain an operating system.
+++ -/r * 451479-128-1: g:H
+++ -/r * 451480-128-1: g:J@
+++ -/r * 451481-128-1: f`gf
+++ -/r * 451482-128-1: fPgf
+++ -/r * 451487-128-5: fSfPfQfVfW
++ d/d 30-144-5:         f_f^fYf
+++ r/r 32-128-2:        fQfW
+++ r/r 32-128-4:        fTfVgf
+++ r/r 33-128-1:        fPfPgf
+++ r/r 34-128-1:        fPgf
+++ r/r 35-128-1:        fPgf
+ r/r 98184-128-50:      fZfYfBfQfV
+ r/r 98184-128-51:      f^fYf
r/r 2-128-1:    $LogFil(
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr
d/d 58-144-5:   $Recycle.Bin
+ d/d 101184-144-1:     S-1-5-21-2810184817-710479300-78394590-1(
```

III. RÉALISATION DU PROJET - CRÉATION YARA

- Fichier traité ligne par ligne
- Vérifie conformité:
  - Taille
  - Correspondance
  - existence

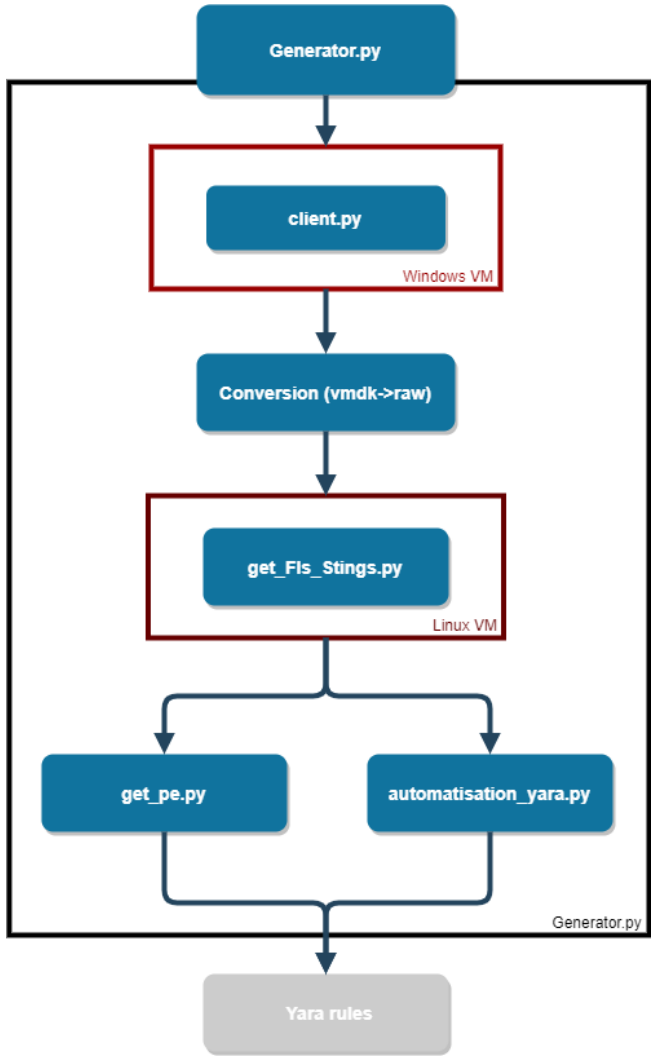
```
rule PuTTY_uninstall {
        meta:
                description = "Auto generation for PuTTY"
                author = "David Cruciani"
                date = "2021-09-08"
                versionApp = "Release 0.75"
                uuid = "32a2d663-0c3f-418e-b8d9-e10a0e53c420"
                uninstaller = "msiexec"
        strings:
                $s0 = /putty\.exe\|a07396d107f47123h/
                $s1 = /puttygen\.exe\|a8e024fc7459f5f3/
                $s2 = /PUTTY\.EXE/
                $s3 = / PUTTY\(\~1/
                $s4 = /\(SMW   PUTTYM\~1\.LNK/
                $s5 = /\(SMW   PUTTYW\~1\.LNK/
                $s6 = /\(SMW   PuTTY\.lnk/
                $s7 = /\(SMW   PuTTYgen\.lnk/
                $s8 = /putty\~/
                $s9 = /puttygen\~/
                $s10 = /putty web site\~/
                $s11 = /putty manual\~/
                $s12 = /PuTTY README/
                $s13 = /putty\.msi/
                $s14 = /PuTTY/
                $s15 = /PuTTY release 0\.75 \(64\-bit\)/
                $s16 = /PuTTY release 0\.75 \(64\-bit\)/
                $s17 = /\*\|PuTTYB\*\|/
                $s18 = /Eputty/
                $s19 = /O\*\|PuTTY/
                $s20 = /\(Gputty w/
                $s21 = /siteOPuTTY W/
                $s22 = /SimonTatham\.PuTTY/
                $s23 = /C\:\\Program Files\\PuTTY\\/
                $s24 = /PuTTY64/
                $s25 = /PuTTY Installer/
        condition:
                 ext_var of ($s*)
```

III. RÉALISATION DU PROJET - CRÉATION YARA



CompanyName, ProductName, FileDescription, InternalName, OriginalFileName.

III. RÉALISATION DU PROJET



PLAN

- Entreprise
- Présentation du sujet
- Réalisation du projet
- **Avenir du projet**
- Conclusion

IV. AVENIR DU PROJET

- Durée trop longue
  - 30 min *strings*
  - 30 min *ASA*
- Donner liste vulnérabilités
- Hashlookup

PLAN

- Entreprise
- Présentation du sujet
- Réalisation du projet
- Avenir du projet
- **Conclusion**

V. CONCLUSION

- Réalisé de zero
- 2 dépôt GitHub
- Règle utilisable sur disque

- Beaucoup appris
- Manque de Forensic à l'Université

III. RÉALISATION DU PROJET - YARA

rule_test.yar

```
rule rule_test
{
    strings:
        $s0 = "oui"
        $s1 = /\+/
        $s2 = "=20"
    condition:
        $s0 and $s1 and not $s2
}
```

test.txt

```
oui
10+10
=20
```

rule_test.yar

```
rule rule_test
{
    strings:
        $s0 = "oui"
        $s1 = /\+/
        $s2 = "=20"
    condition:
        all of them
}
```

C:\Windows\System32\cmd.exe

```
B:\Téléchargement\Logiciel\yara-v4.1.0-1612-win64>yara64.exe -w -s rule_test.yar test.txt

B:\Téléchargement\Logiciel\yara-v4.1.0-1612-win64>
```

Pas de résultat

```
B:\Téléchargement\Logiciel\yara-v4.1.0-1612-win64>yara64.exe -w rule_test.yar test.txt
rule_test test.txt
```