intrinsec
BUSINESS CONTINUITY AND SECURITY

Advanced Protection Techniques

Ou comment utiliser des APT contre les APT

Qui sommes-nous

Vasileios FRILIGKOS & Florian GUILBERT
Analyste CERT & SOC
Vasileios.Friligkos@intrinsec.com
Florian.Guilbert@intrinsec.com

@ktinoulas

@flgy

Contexte

- Augmentation du nombre des cyber-attaques
  - 42% d'augmentation entre 2011 et 2012 - [FireEye2012]
- Amélioration des techniques employées
  - Évolution du GameOver Zeus (rootkit, chiffrement)
  - Prévention contre les analyses (Careto)
  - Contournement d'EMET (Bromium Labs)
  - Propagation ultrasonique (BadBios)
- Est-il encore possible de se protéger ?
  - 0-day
  - Spear-phishing / water-holing
  - Périmètres étendus

Contexte

- Plus de la moitié des intrusions sont détectées par une organisation tierce (CERT, autorités gouvernementales)
  - → **63 %** [Mandiant - M-Trends 2013]
  - → **69 %** [Verizon – DBI Report 2013]

- Moyenne de **243** jours avant la détection d'une compromission [Mandiant - M-Trends 2013]

- **78 %** des attaques auraient pu être évitées grâce à des contrôles simples [Verizon - DBI Report 2013]

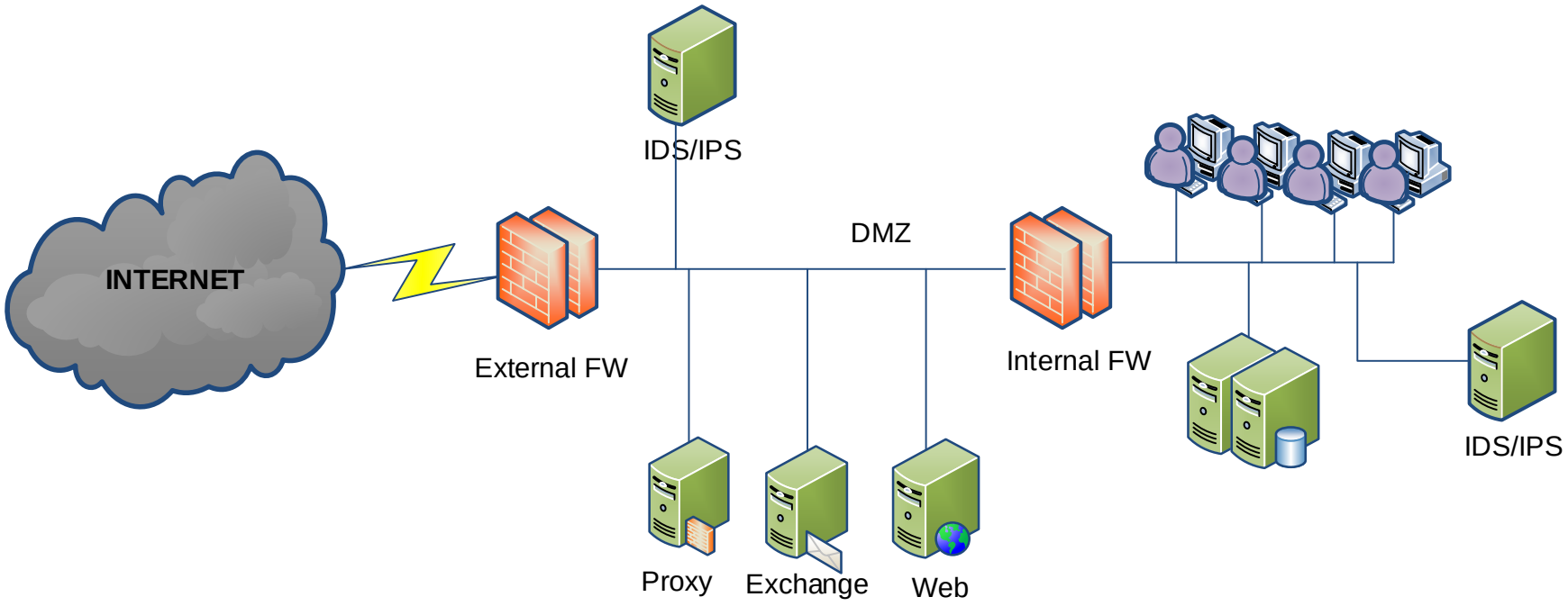
Les APT contre les APT

- Techniques de détection
  - Basées sur le management de logs de sécurité (SIEM)
  - Augmenter la visibilité sur notre périmètre
- Techniques de réponse sur incident
  - Réaction
  - Capitalisation
- Rien d'excessivement complexe
  - Mais nécessite une certaine maturité sur son SI

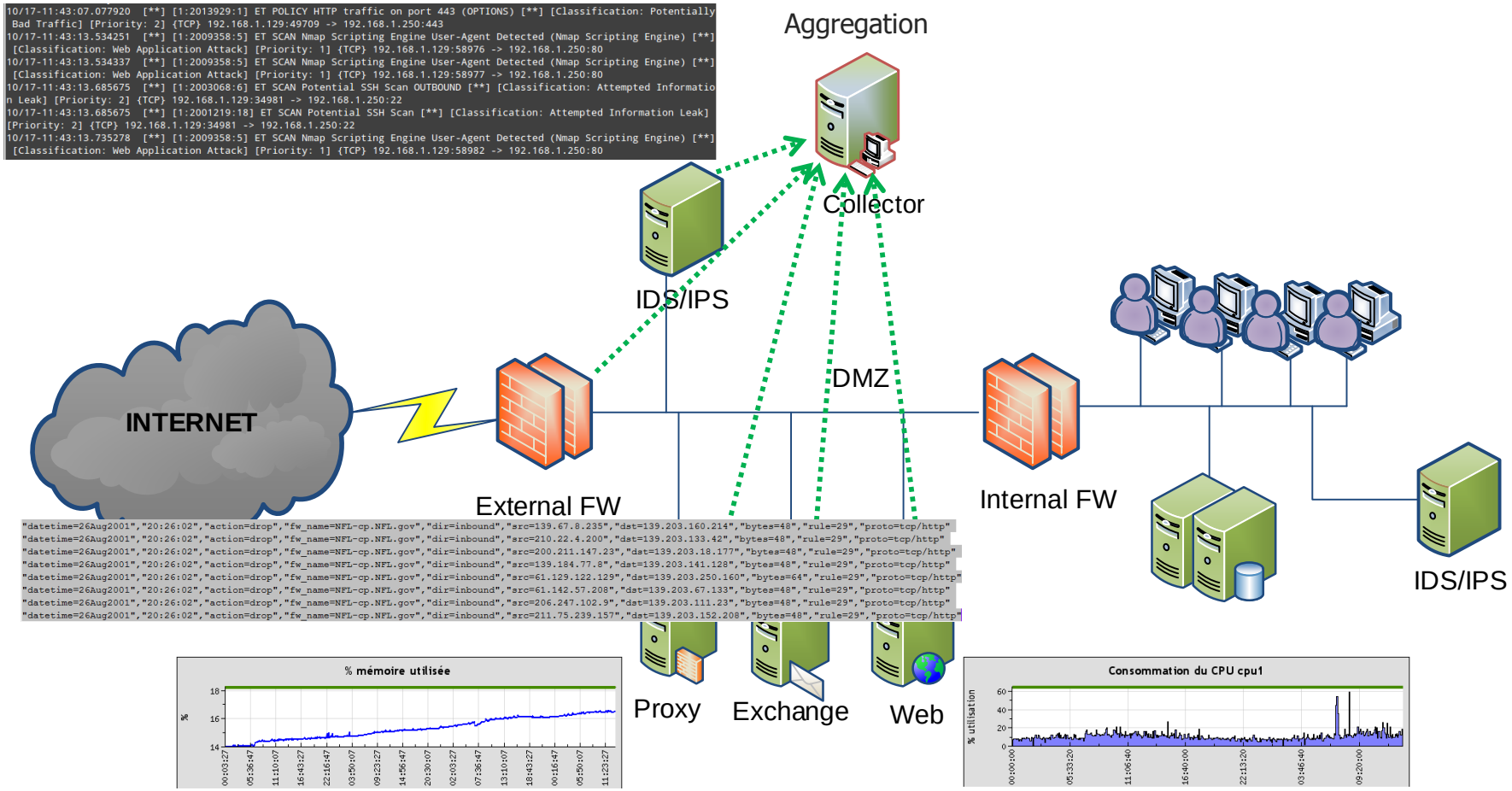
Détection

- Centralisation – Formalisation
  - Intégration de différents formats
  - Utilisation d'un protocole unique pour décrire les évènements
- Agrégation – Enrichissement des données
  - Minimise le volume des données
  - Classification des évènements (metadata)
- Corrélation – plusieurs facteurs
  - Temporelle, spatiale
  - Signatures, comportement légitime
  - Détection de motifs complexes, suppression de faux positifs

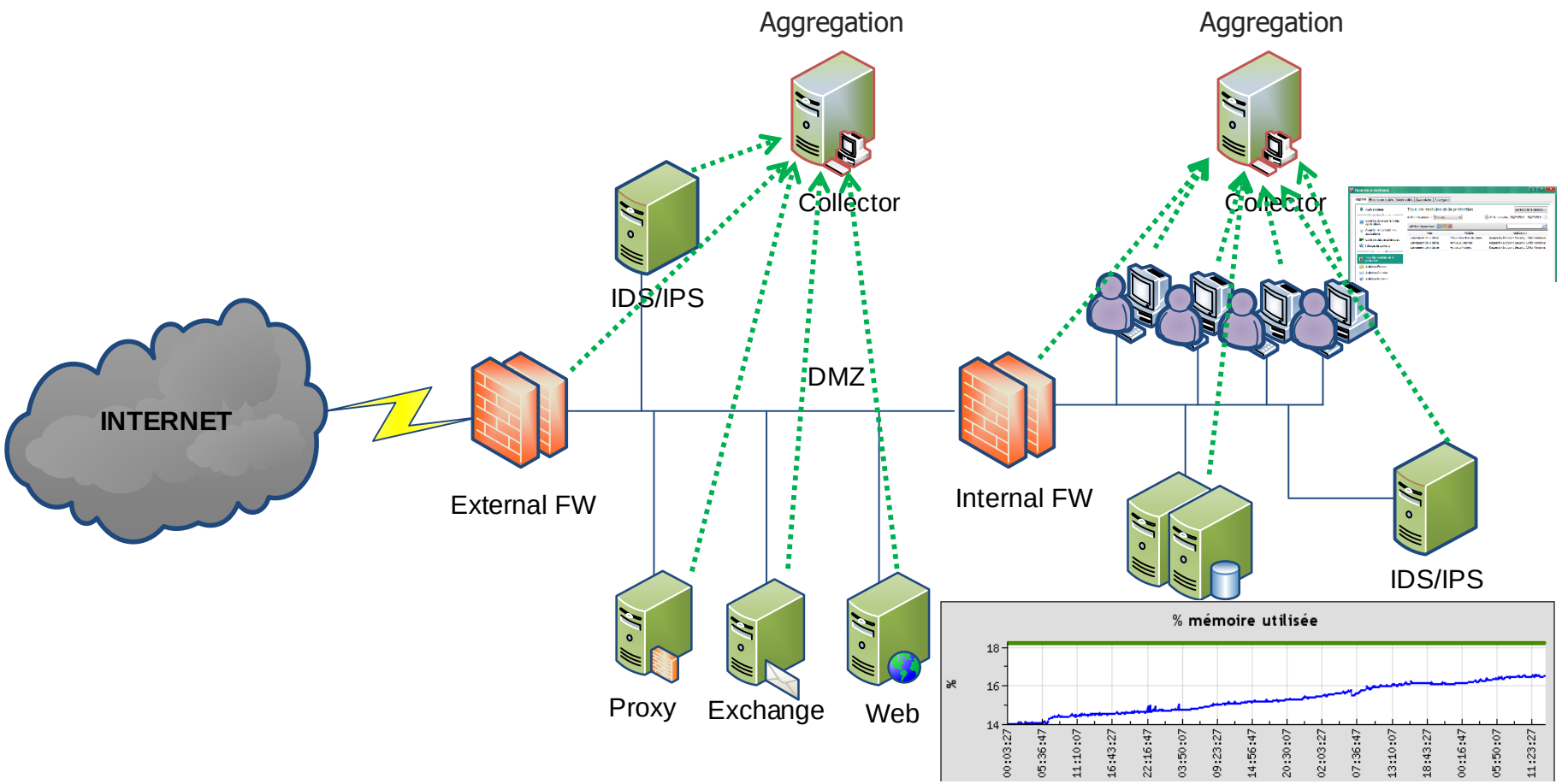
Procédure



Procédure

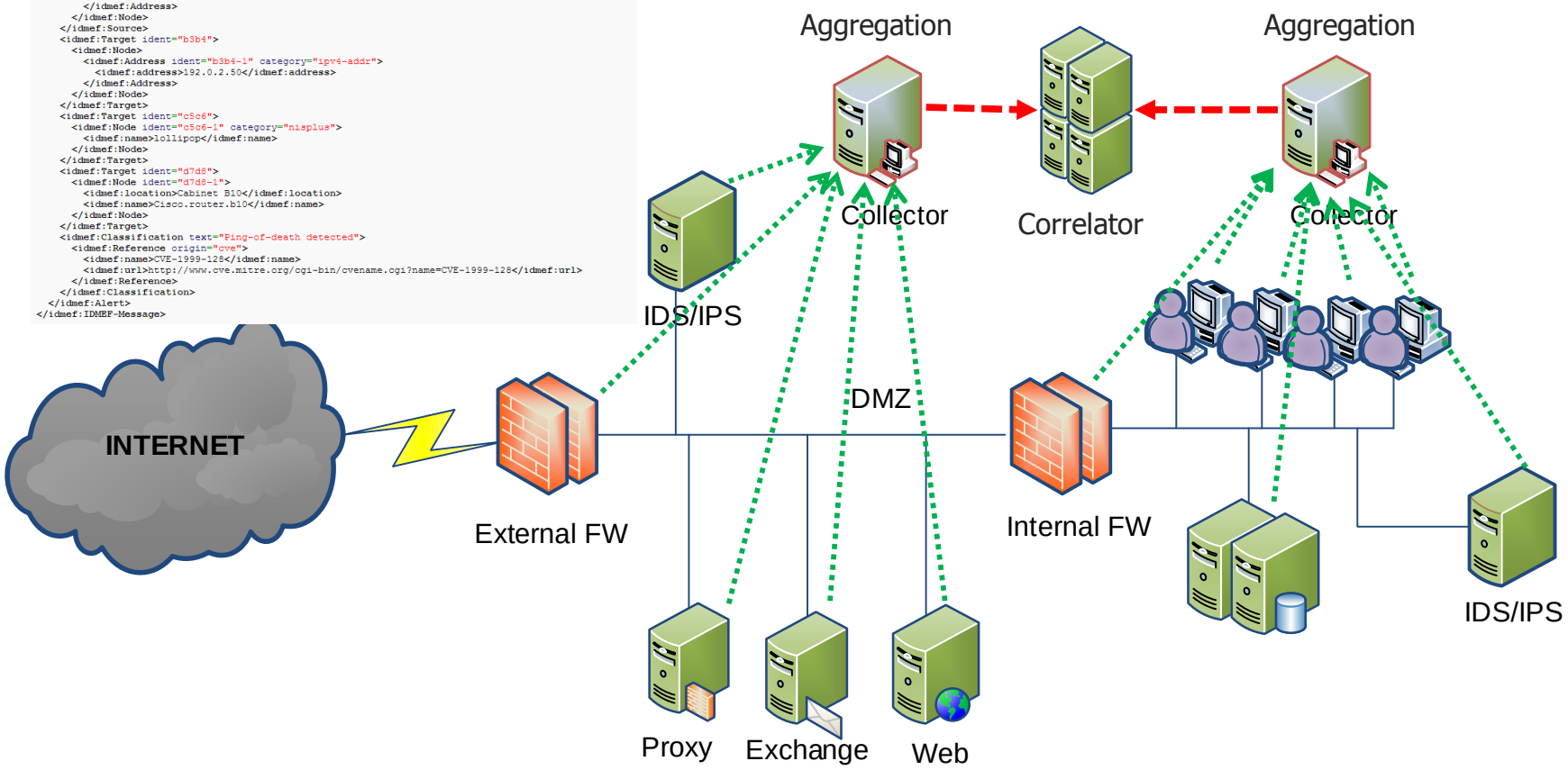


Procédure

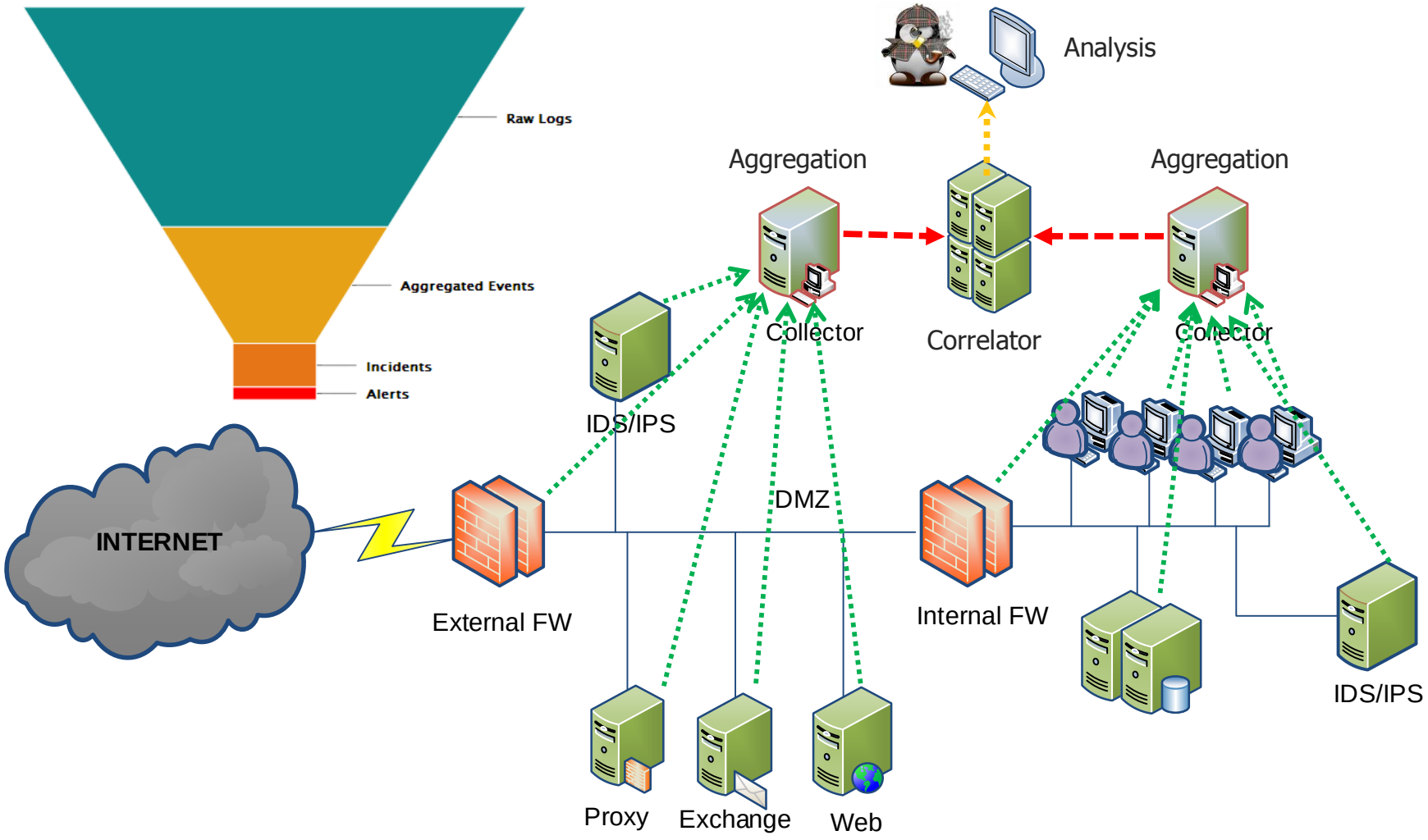


Procédure

```
<?xml version="1.0" encoding="UTF-8"?>
<idmef:IDMEF-Message xmlns:idmef="http://iana.org/idmef" version="1.0">
  <idmef:Alert messageid="abc123456789">
    <idmef:Analyzer analyzerid="bc-sensor01">
      <idmef:Node category="dns">
        <idmef:name>sensor.example.com</idmef:name>
      </idmef:Node>
    </idmef:Analyzer>
    <idmef:CreateTime ntpstamp="0xbc71f4f5.0xef449129">2000-03-09T10:01:25.93464Z</idmef:CreateTime>
    <idmef:Source ident="a1a2" spoofed="yes">
      <idmef:Node ident="a1a2-1">
        <idmef:Address ident="a1a2-2" category="ipv4-addr">
          <idmef:address>192.0.2.200</idmef:address>
        </idmef:Address>
      </idmef:Node>
    </idmef:Source>
    <idmef:Target ident="b3b4">
      <idmef:Node>
        <idmef:Address ident="b3b4-1" category="ipv4-addr">
          <idmef:address>192.0.2.50</idmef:address>
        </idmef:Address>
      </idmef:Node>
    </idmef:Target>
    <idmef:Target ident="c5c6">
      <idmef:Node ident="c5c6-1" category="nisplus">
        <idmef:name>lollipop</idmef:name>
      </idmef:Node>
    </idmef:Target>
    <idmef:Target ident="d7d8">
      <idmef:Node ident="d7d8-1">
        <idmef:location>Cabinet B10</idmef:location>
        <idmef:name>Cisco.router.b10</idmef:name>
      </idmef:Node>
    </idmef:Target>
    <idmef:Classification text="Ping-of-death detected">
      <idmef:Reference origin="cve">
        <idmef:name>CVE-1999-128</idmef:name>
        <idmef:url>http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-128</idmef:url>
      </idmef:Reference>
    </idmef:Classification>
  </idmef:Alert>
</idmef:IDMEF-Message>
```



Procédure



Évènements

- Caractéristiques communes des menaces

- Intrusion
  - → Reconnaissance
  - → Exploitation
  - → Rebond / escalade
  - → Persistance
  - → Acte malveillant

- Malware
  - → Infection
  - → Coordination (C&C)
  - → Acte malveillant

→ Définition d'une baseline

→ Détection d'activités malveillantes

Scénario 1 : Attaque web

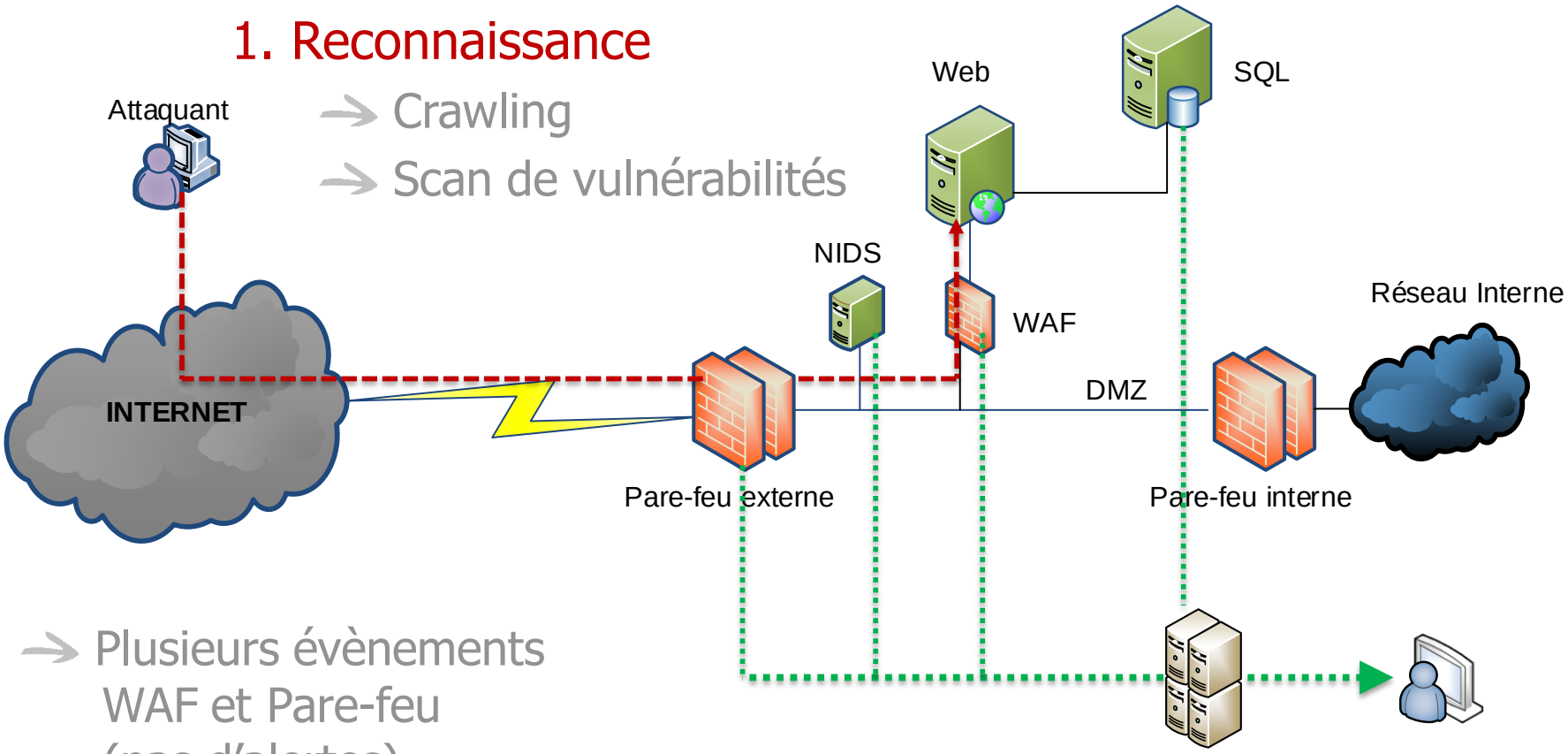
- Attaque web
  - Obfuscation des payloads
  - Scan applicatif
  - Exploitation de vulnérabilités applicatives
  - Déploiement d'un webshell
  - Exfiltration de données

- Périmètre
  - Pare-feu applicatif
  - NIDS
  - Serveur web
  - Serveur SQL

Scénario 1 : Attaque web

1. Reconnaissance

- Crawling
- Scan de vulnérabilités



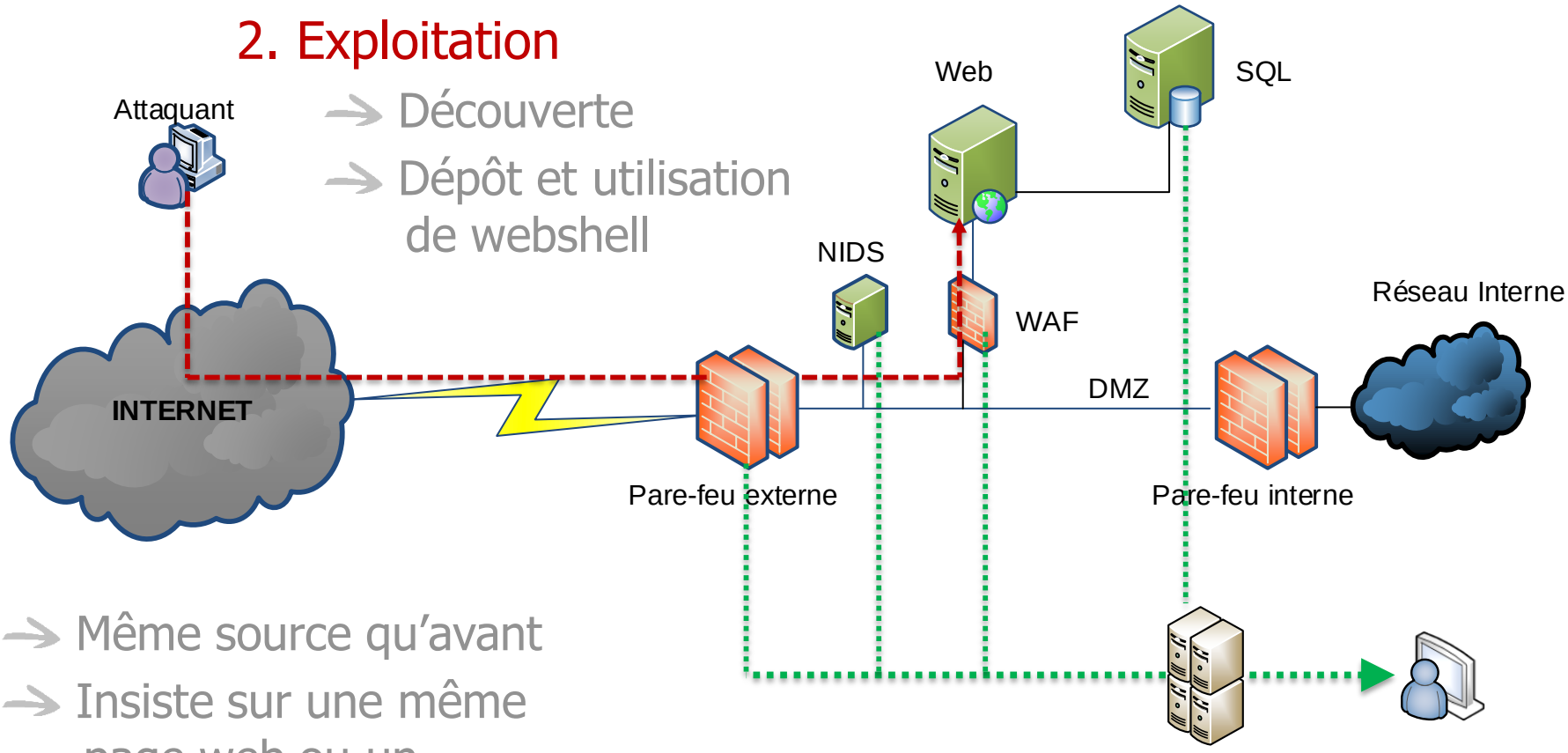
- Plusieurs évènements WAF et Pare-feu (pas d'alertes)
- Même adresse source

→ Scan web potentiel – niveau 3

Scénario 1 : Attaque web

2. Exploitation

- Découverte
- Dépôt et utilisation de webshell

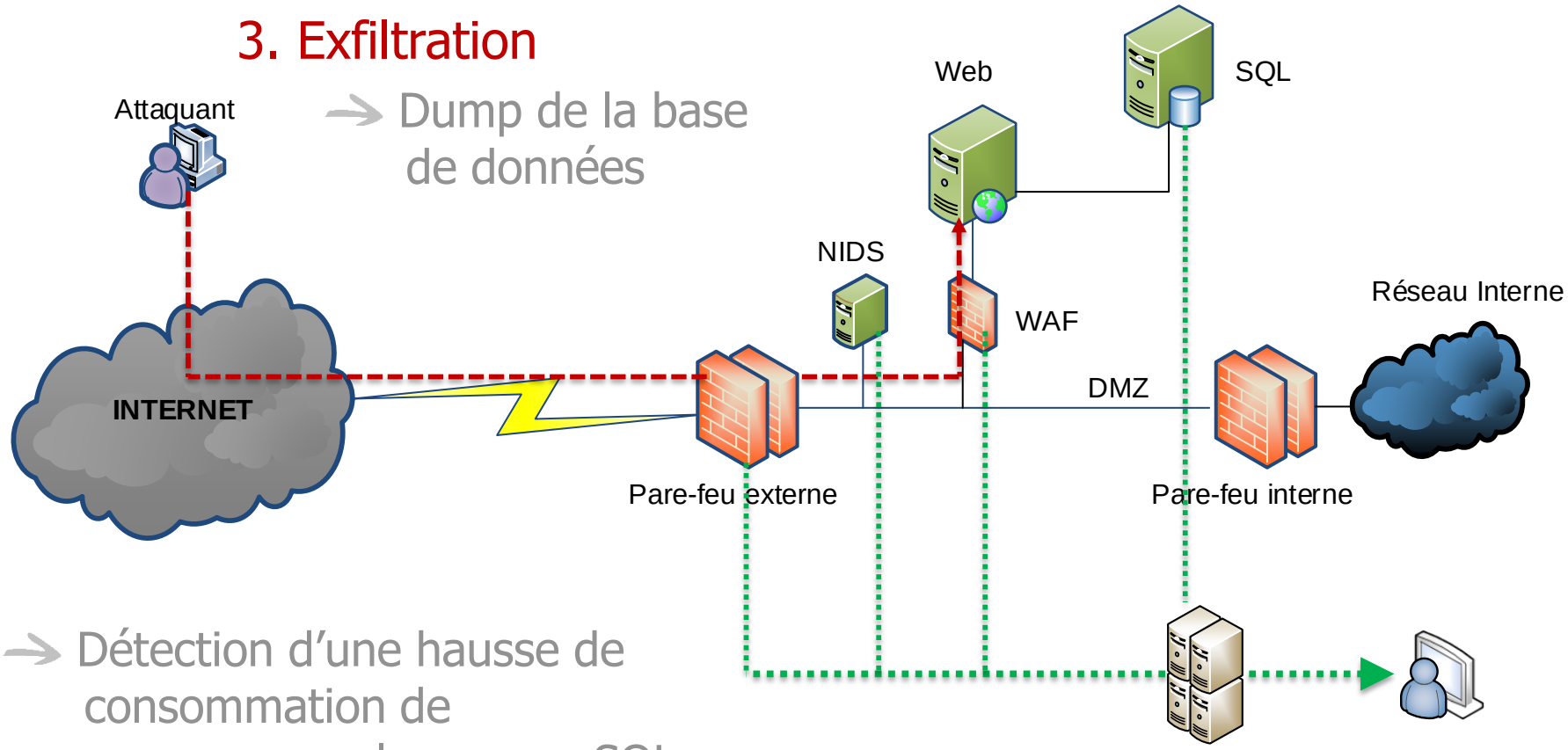


- Même source qu'avant
- Insiste sur une même page web ou un paramètre spécifique

➡ Scan web persistant – niveau 2

Scénario 1 : Attaque web

3. Exfiltration

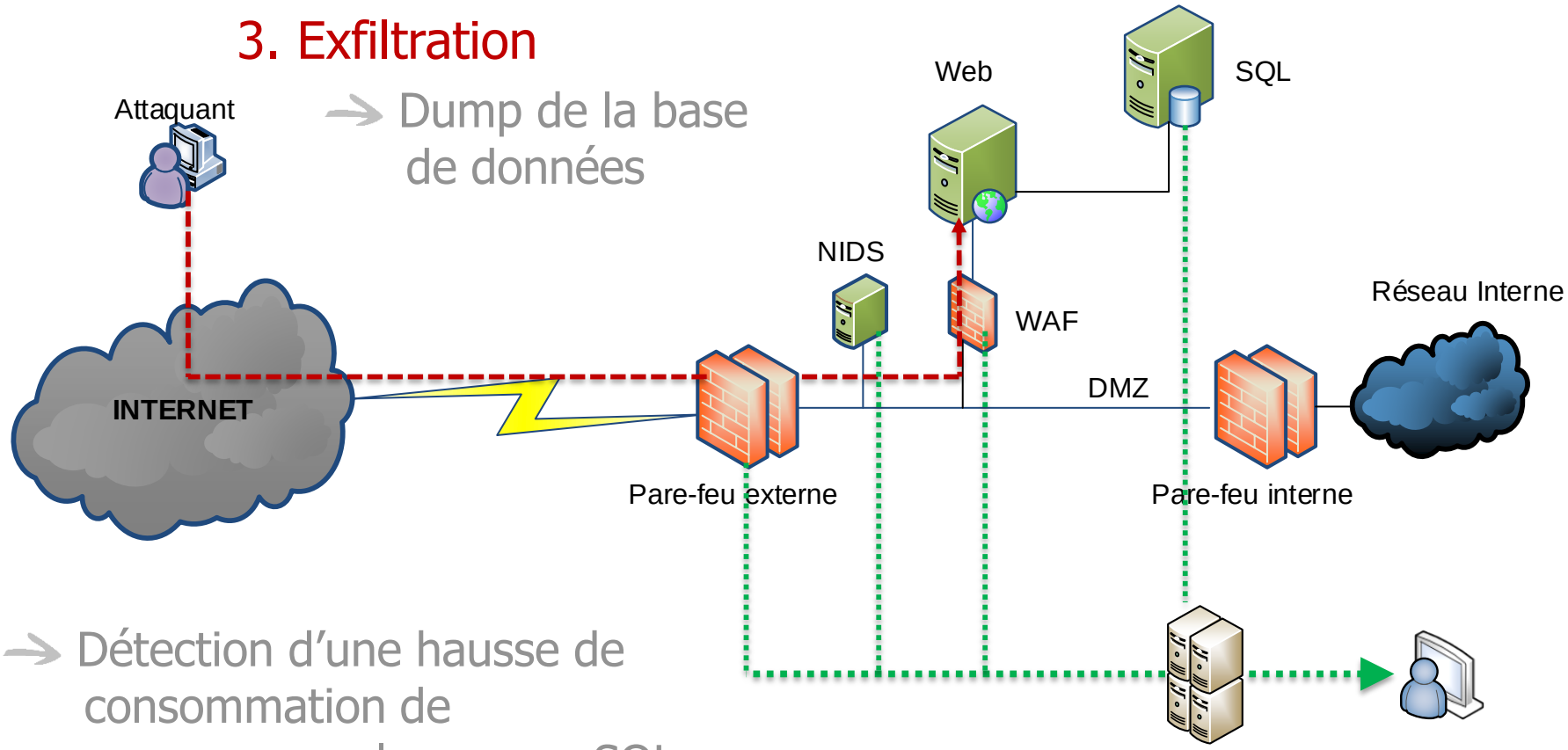


- Détection d'une hausse de consommation de ressource sur le serveur SQL
- Hors période de backup

→ Augmentation de la sévérité de tous les évènements liés à la base SQL

Scénario 1 : Attaque web

3. Exfiltration

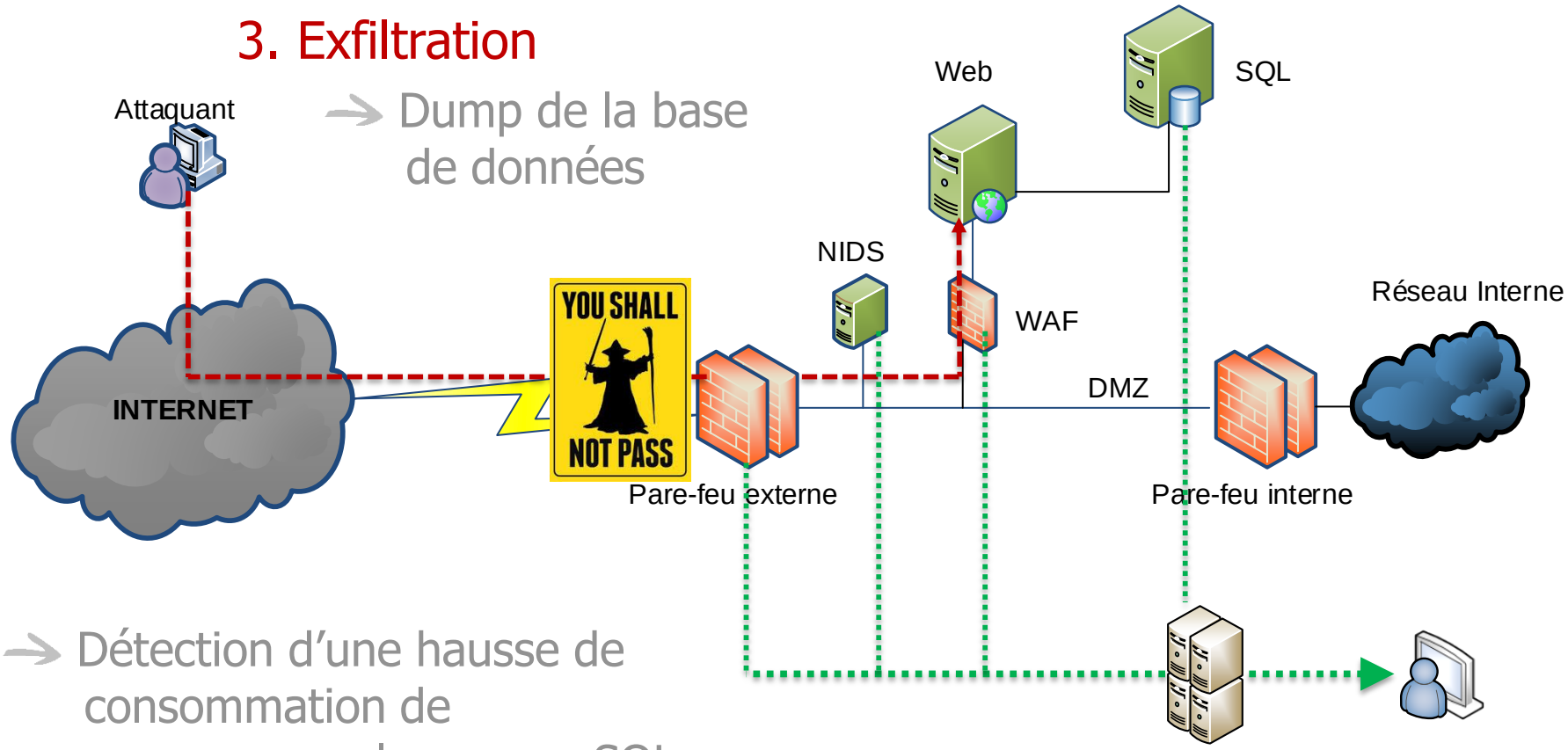


- Détection d'une hausse de consommation de ressource sur le serveur SQL
- Hors période de backup

→ Compromission – niveau 1

Scénario 1 : Attaque web

3. Exfiltration



- Détection d'une hausse de consommation de ressource sur le serveur SQL
- Hors période de backup

→ Compromission – niveau 1

Résultats

- Attaque contournant les systèmes de signatures classiques

- Détection basée sur :
  - Le nombre d'évènements supérieur à un comportement normal (Baseline)
  - Concentration sur quelques modules (pages, paramètres)
  - Surveillance de ressources (CPU, I/O, RAM)
  - Niveau de sévérité dynamique

Résultats

- Attaque contour 

signatures classiques

- Détection basée sur :
  - Le nombre d'évènements supérieur à un comportement normal (Baseline)
  - Concentration sur quelques modules (pages, paramètres)
  - Surveillance de ressources (CPU, I/O, RAM)
  - Niveau de sévérité dynamique

Réaction

- Avoir une détection efficace n'empêche pas certaines menaces

- Procédure de réaction
  - 24/7
  - Minimisation de la durée d'intervention
  - Procédure d'analyse
  - Capitalisation
  - Partage avec la communauté

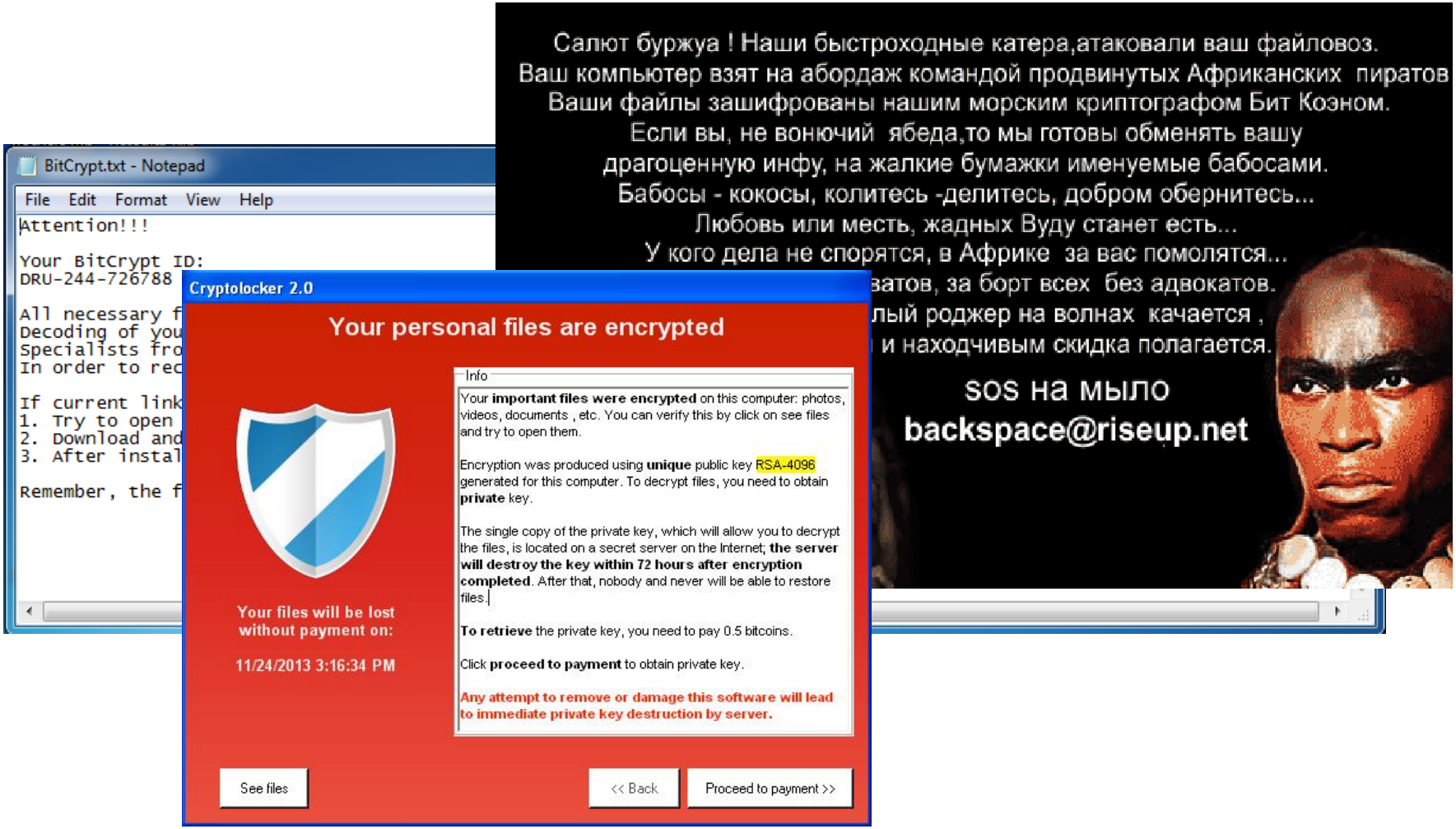
- Amélioration du niveau de sécurité
  - Développement de nouvelles signatures (IOC)
  - Réduction du temps de détection et de réaction
  - Limitation des impacts

Scénario 2 : Ransomware

- Nouvelle variante de ransomware cryptographique
  - Infection par email
  - Contact Command & Control
  - Chiffrement des fichiers locaux et sur des partages
  - Cryptographie symétrique et asymétrique
  - Notification à l'utilisateur

- Détection effectuée par le malware suite à l'acte malveillant

Scénario 2 : Ransomware



Scénario 2 : Ransomware

- Nouvelle variante de ransomware cryptographique
  - Infection par email
  - Contact Command & Control
  - Chiffrement des fichiers locaux et sur des partages
  - Cryptographie symétrique et asymétrique
  - Notification à l'utilisateur

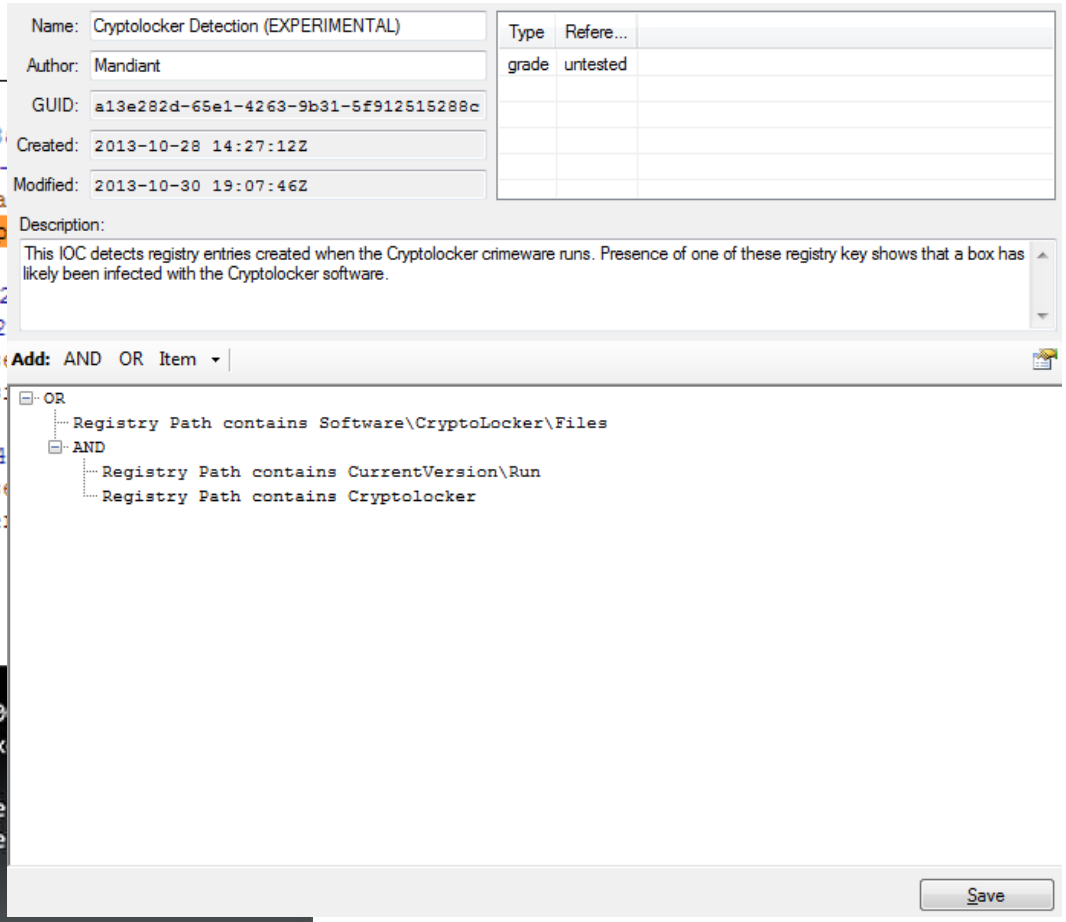
- Détection effectuée par le malware suite à l'acte malveillant
  - Pas d'IP / URL blacklistées
  - Pas de signatures Anti-virus ou IDS

Analyse de la menace

- Extraction des IOC
  - → Création de signatures spécifiques
  - → Raffinement des procédés de détection
    - ✓ Détection plus rapide - DGA
    - ✓ Exhaustivité

Extraction des IOC

```
▼<definition>
 ▼<Indicator operator="OR" id="7ea605b7-8
  ▼<IndicatorItem id="a71eb0d7-afe5-4708-
     <Context document="RegistryItem" sea
     <Content type="string">Software\Cryp
   </IndicatorItem>
  ▼<Indicator operator="AND" id="bfbef8a2
   ▼<IndicatorItem id="42e96998-7161-4f2
     <Context document="RegistryItem" s
     <Content type="string">CurrentVers
   </IndicatorItem>
   ▼<IndicatorItem id="5d5b8296-01c9-414
     <Context document="RegistryItem" s
     <Content type="string">Cryptolocke
   </IndicatorItem>
  </Indicator>
 </Indicator>
</definition>
```

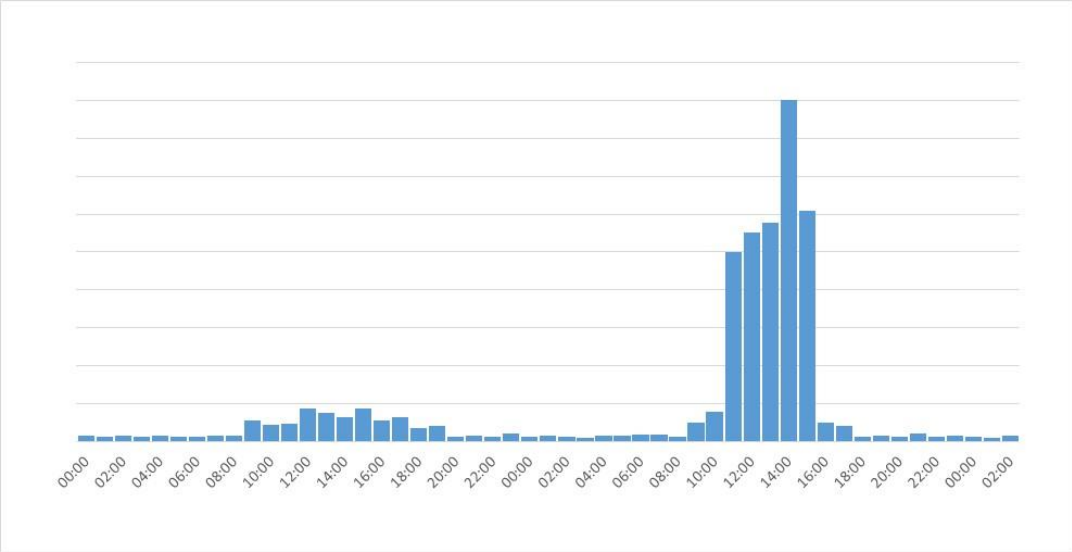


Analyse de la menace

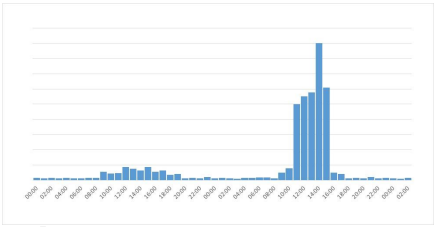
- Extraction des IOC
  - → Création de signatures spécifiques
  - → Raffinement des procédés de détection
    - ✓ Détection plus rapide - DGA
    - ✓ Exhaustivité
- Développement de procédure de réaction de la menace
  - → Isolation de l'équipement infecté
  - → Isolation des volumes sensibles

Analyse de la menace

- Renforcement de la politique de sécurité
  - → Activation des Windows events (ObjectAccess)



Analyse de la menace



- Renforcement de la politique de sécurité
  - → Activation des Windows events (ObjectAccess)
  - → Limitation des répertoires pouvant exécuter des binaires
    - ✓ Interdire %AppData%, %LocalAppData%, $Recycle.Bin
  - → Mettre en place un système de backup
    - ✓ Volume shadow
- Développement de moyens spécifiques contre la menace
  - → Attaquants en constante innovation VS un environnement totalement contrôlé par les « défenseurs »
    - ✓ POC : Honeyfile (Fichier de surveillance)

Honeyfile - POC

- Reprendre le principe des honeypots

- Depuis l'analyse du ransomware
  - → Le malware chiffre **tous** les fichiers *.doc, *.jpg, …
  - → Modifie forcément ces fichiers (renommage, suppression, écriture)

- Des fichiers honeyfile.{doc, jpg, …}
  - → Placés dans des endroits stratégiques
  - → Supervisés par un « watchdog » surveillant les interactions avec les processus

- Permet d'identifier les processus suspects

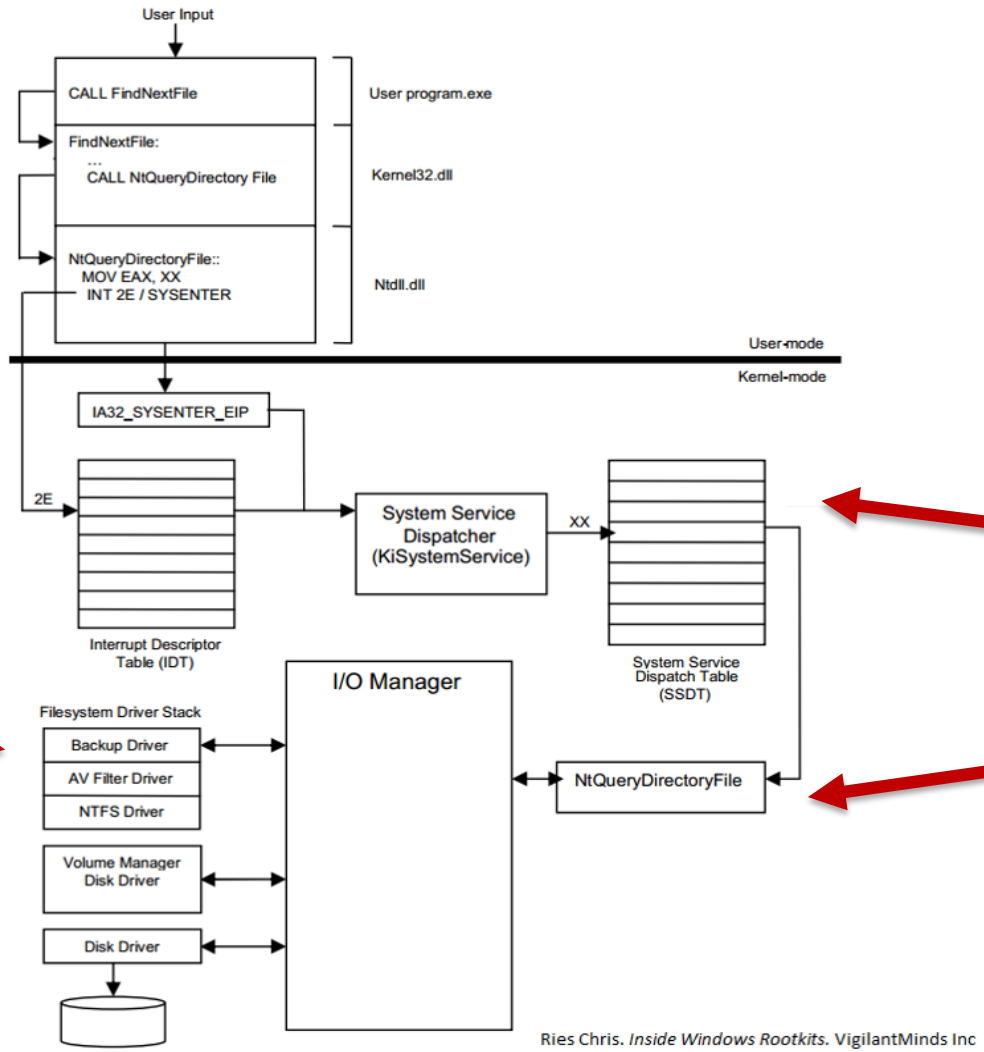
Windows Internals - Hooking

Userland Hooks

IDT Hooks ou SYSTENTER Hook

Layered Driver

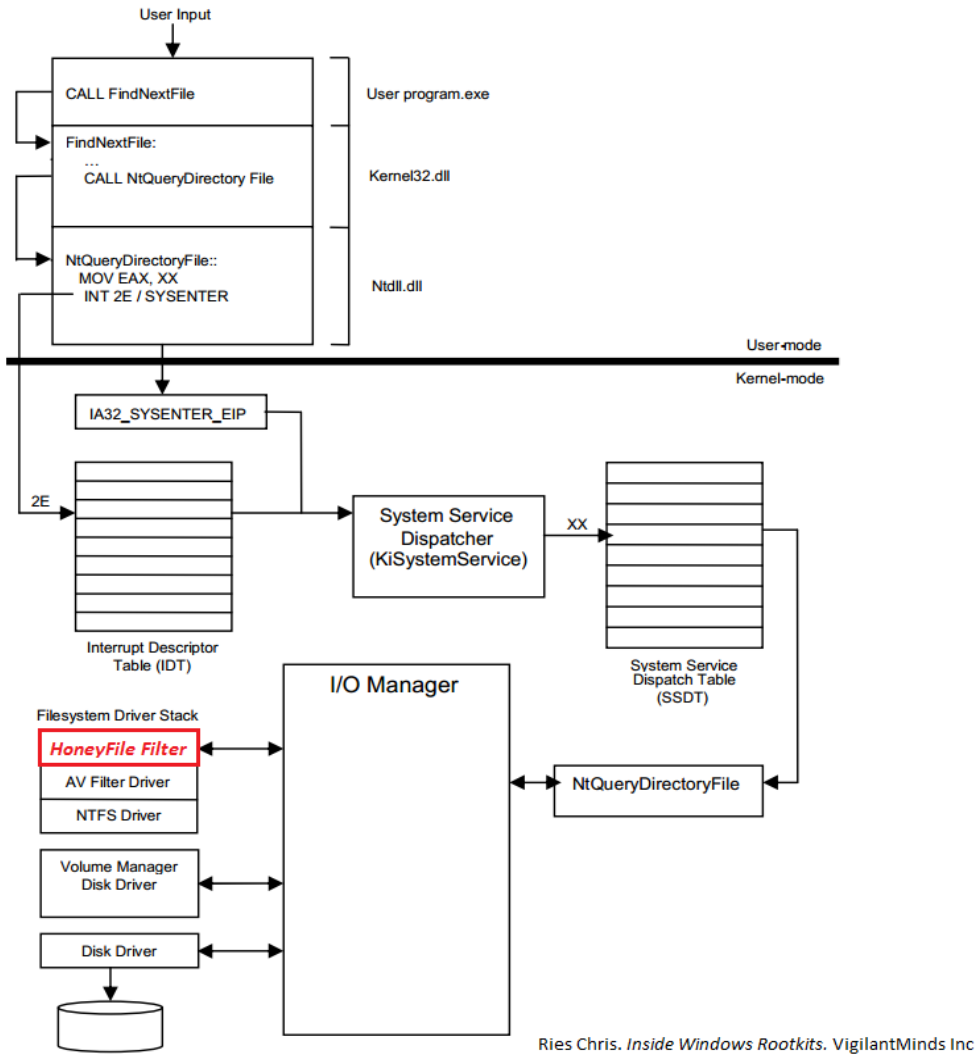
Driver Hooks



Ries Chris. *Inside Windows Rootkits*. VigilantMinds Inc

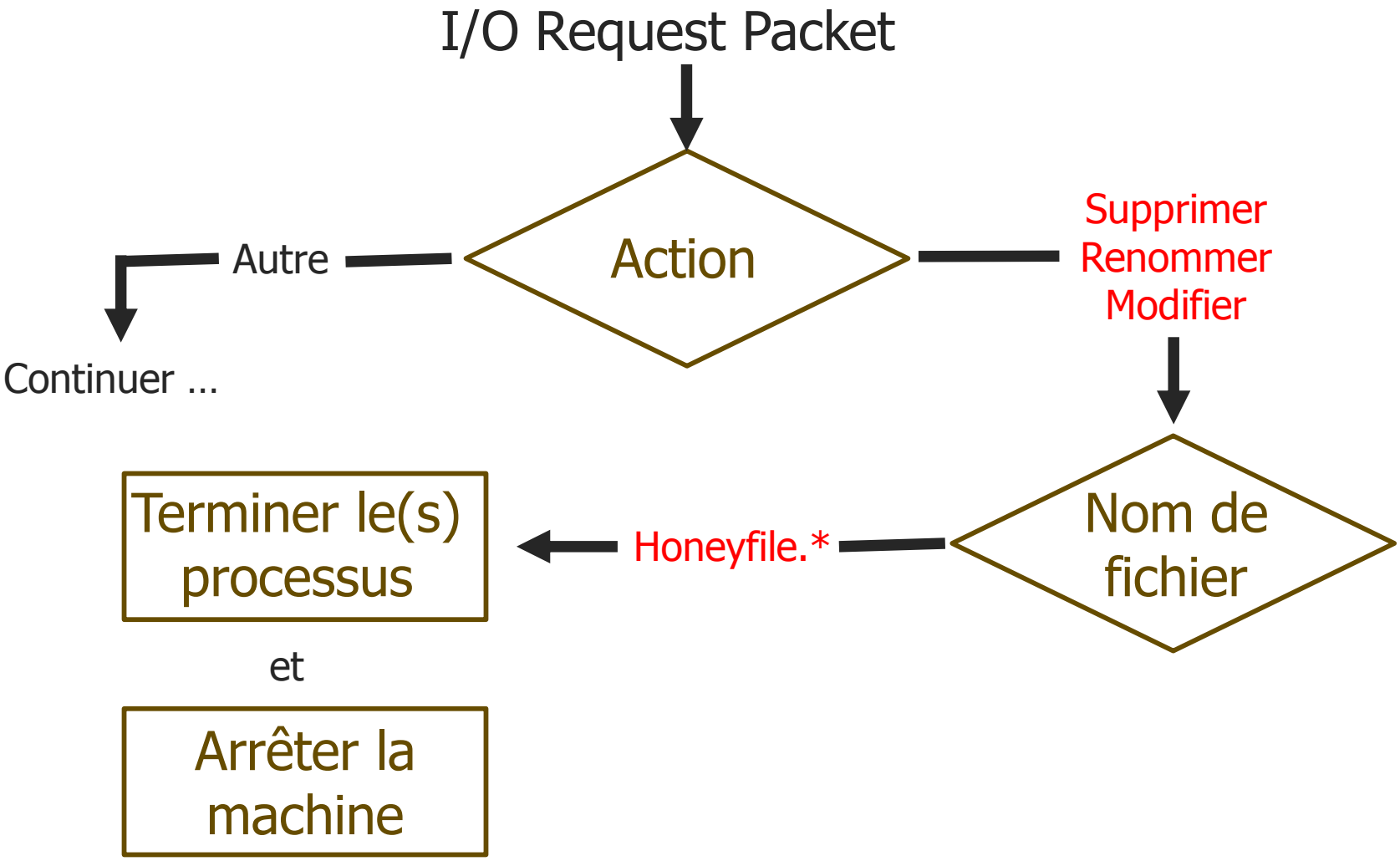
Honeyfile

Interception des IRP

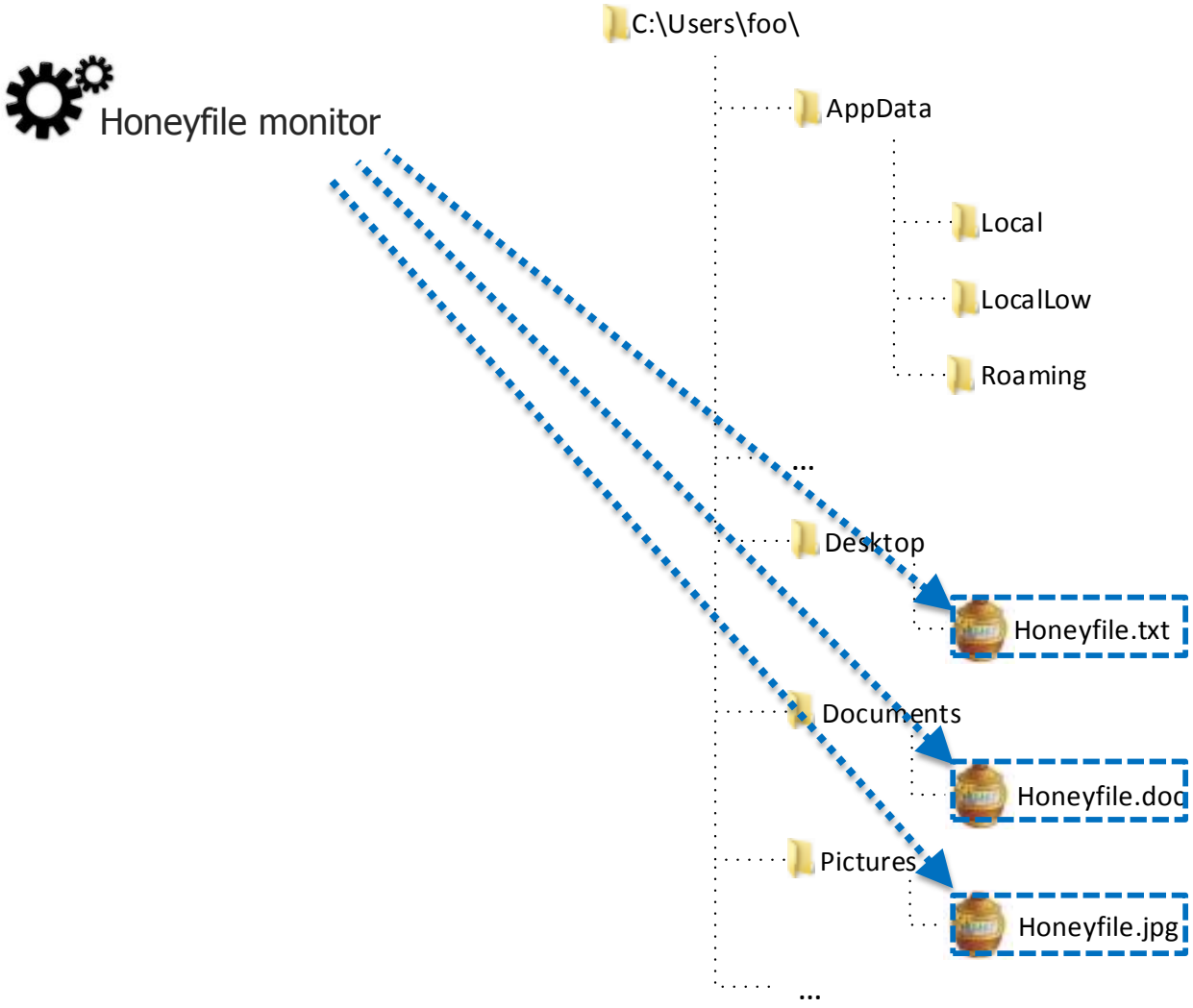


Ries Chris. *Inside Windows Rootkits*. VigilantMinds Inc

Honeyfile

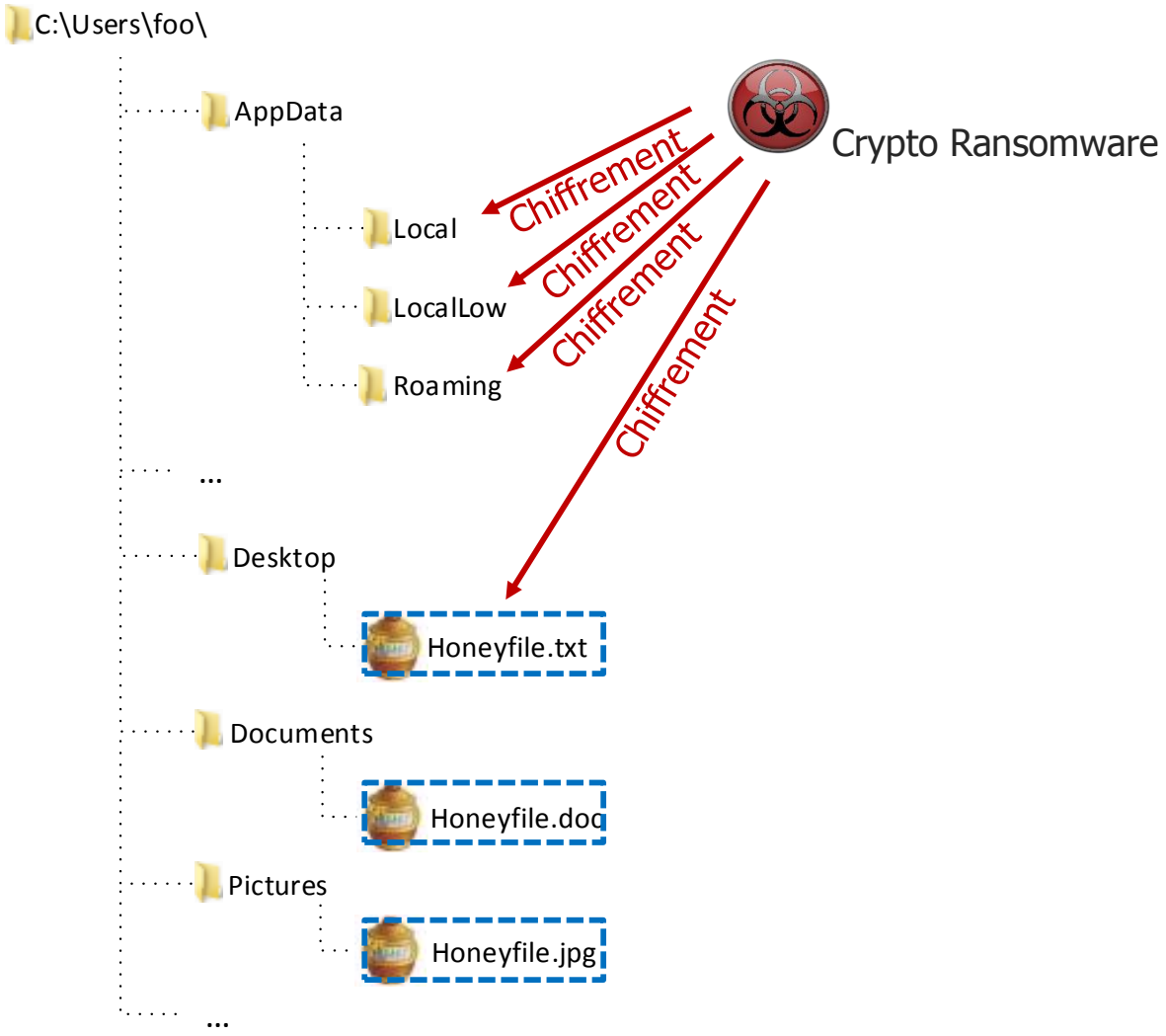


Honeyfile - POC

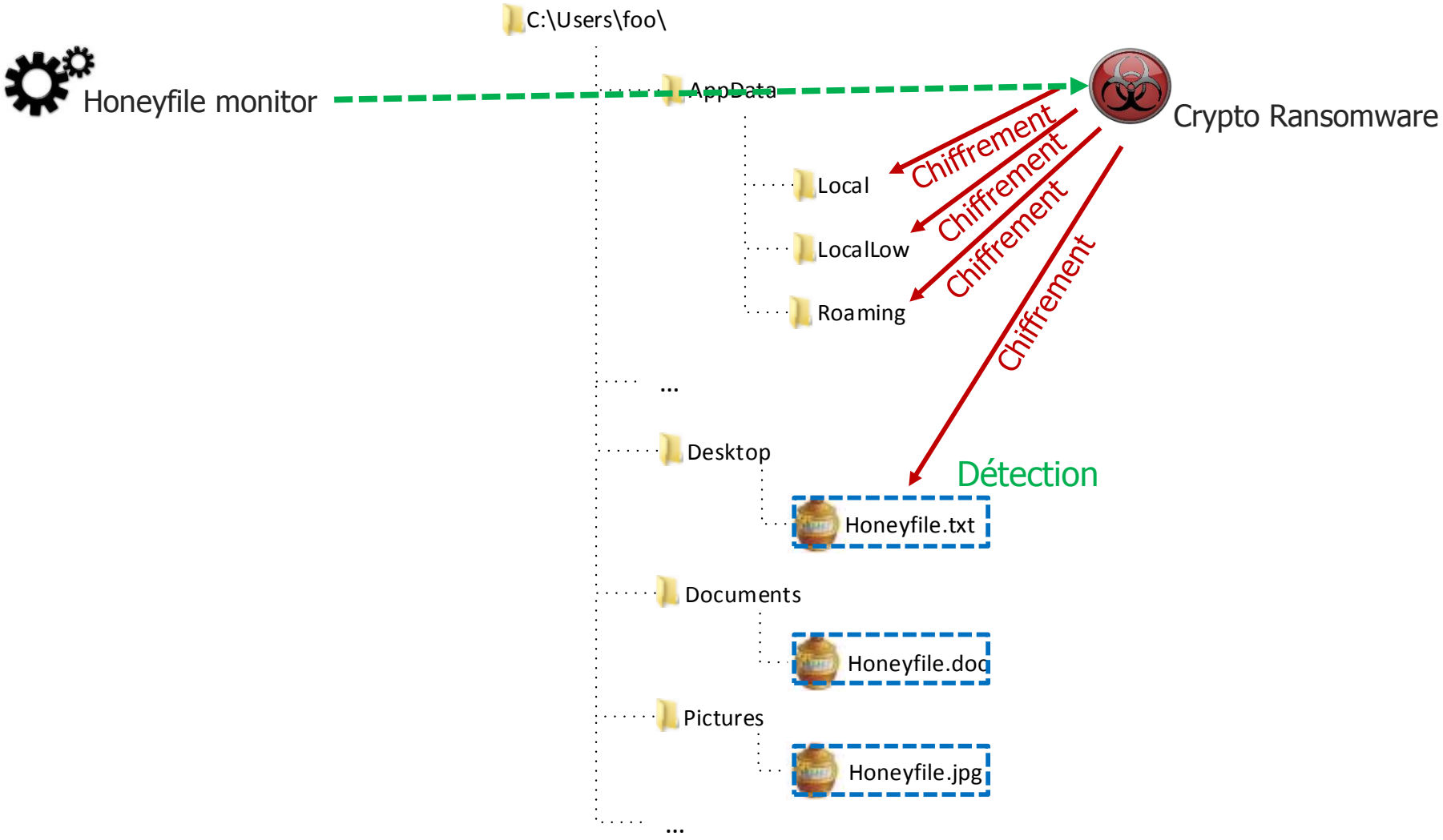


Honeyfile - POC

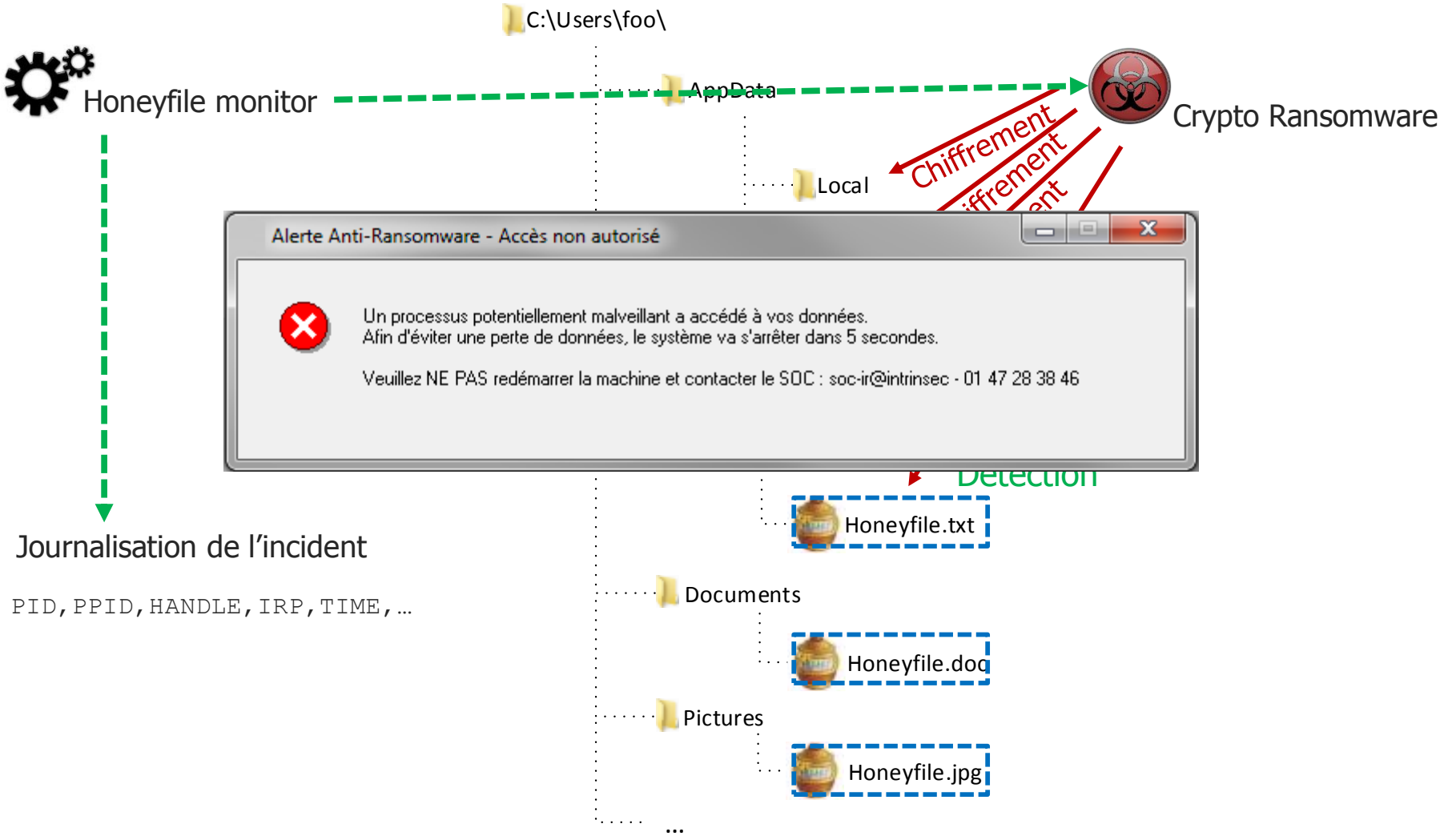
Honeyfile monitor



Honeyfile - POC



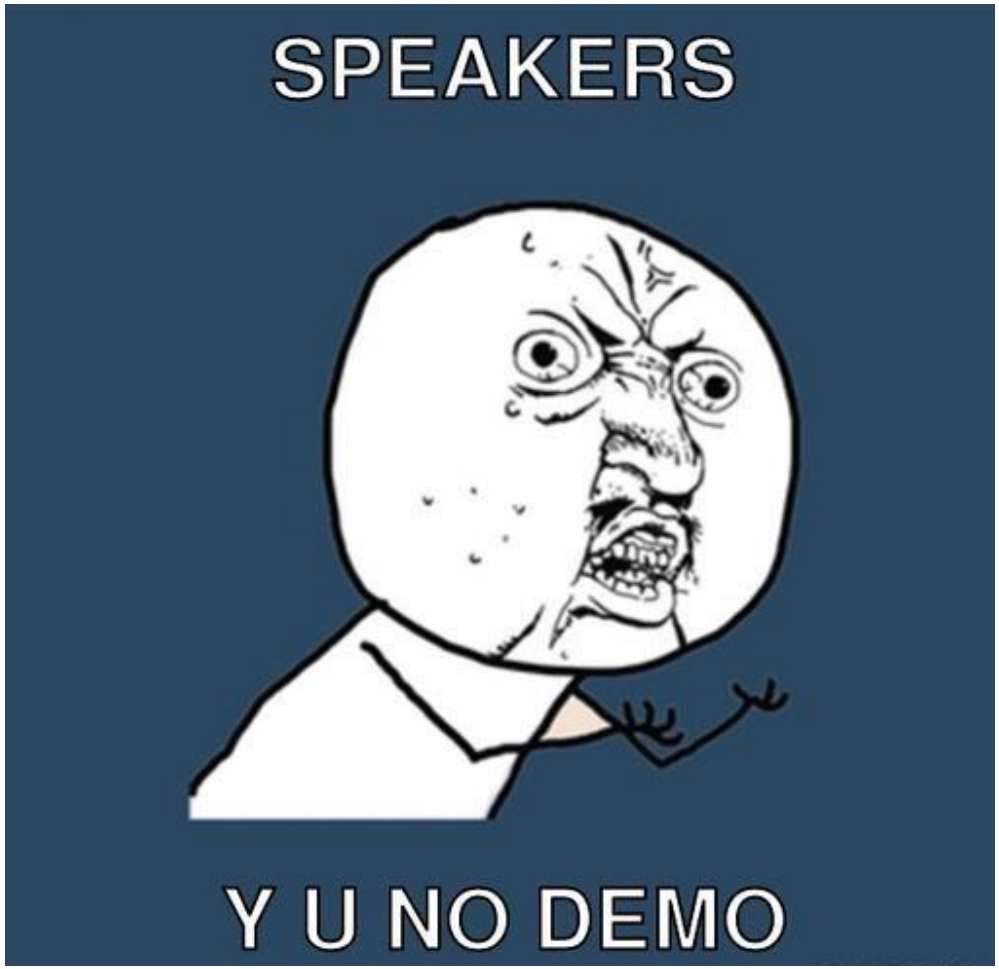
Honeyfile - POC



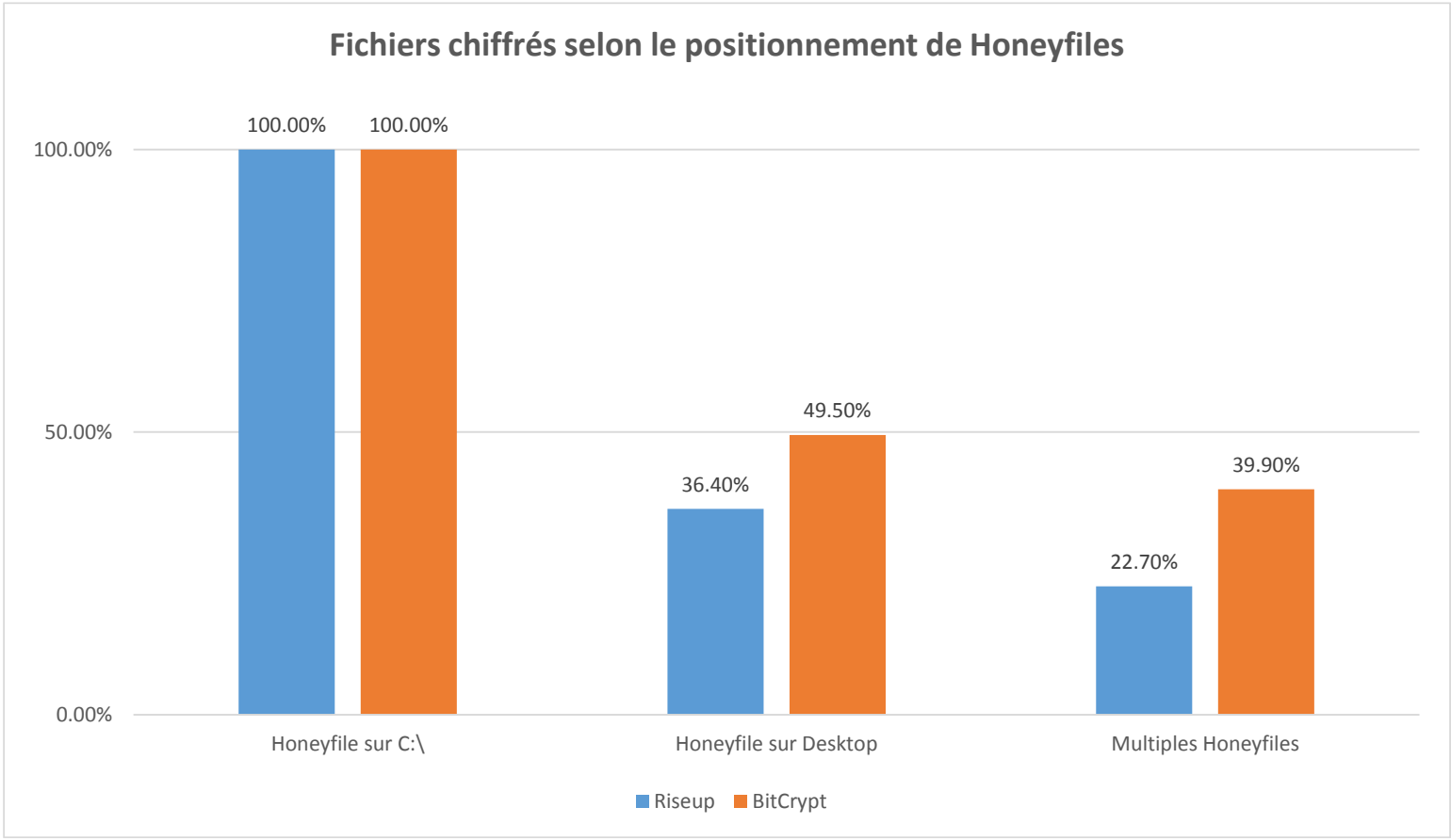
Honeyfile – Résultats

- Protocole :
  - 2 ransomware
    - ✓ Riseup
    - ✓ Bitcrypt
  - 3 cas d'utilisation
    1. Un unique honeyfile placé à la racine
    2. Un unique honeyfile placé sur le bureau des utilisateurs
    3. Des honeyfiles placés dans des sous-répertoires utilisateurs
  - Plusieurs fichiers témoins sur le système
  - Machine virtuelle Windows 7

Honeyfile – POC



Honeyfile – Résultats



Honeyfile - POC

Problématiques

Que faire ?

- ✓ Eteindre la machine
- ✓ Terminer l'arbre du processus
- ✓ Bloquer les IRP : suppression, renommage, modification
- ✓ Journaliser en local ou à distance

Partages réseaux

- ✓ Installer le module sur le serveur (performance et action ?)
- ✓ Installer le module sur chaque poste (exhaustivité)

Conclusion

- Où en est on ?
  - → APT :
    - ✓ Advanced Persistent Threat
    - ✓ Groupe spécialisé
    - ✓ Ressources « illimités »
    - ✓ But : compromission du SI cible
  - → Société lambda :
    - ✓ Cœur de métier ≠ Sécurité
    - ✓ Limitation budgétaire
    - ✓ Manque d'expertise

- **Impossibilité de se protéger à 100%**

Conclusion

- Mais possibilité de minimiser les impacts
  - → Avoir une visibilité sur le SI
  - → Amélioration des techniques de détection
  - → Établir des procédures
    - ✓ Réaction sur plusieurs niveaux (astreintes, analyses, etc.)
    - ✓ Capitalisation
    - ✓ Partage avec la communauté
- Ce ne sont pas des techniques complexes
  - → Mais elles nécessitent :
    - ✓ Une expertise interne ou externe
    - ✓ Une maturité et des moyens pour la gestion de son périmètre

Merci pour votre attention

Questions ?