Prévention et analyse de cyber-attaques

import-module IncidentResponse

Julien Bachmann / Sylvain Pionchon

SCRT

Agenda

- Problématique
- Reconnaissance
- Attaques sur les machines
- Post-Exploitation
- Conclusion

Bio

- Julien
- CISSP
- Ingénieur sécurité @ SCRT

- Sylvain
- Ingénieur sécurité @ SCRT

Agenda

Problématique

Reconnaissance

Attaques sur les machines

Post-Exploitation

Conclusion

problématique | constat

- Défenses actuelles
  - Périmétriques
  - Antivirus
  - IDS ?

problématique | constat

- Attaques actuelles
  - *“80 % des attaques utilisent les collaborateurs”*
  - 0day
  - Attaques supposées avancées et persistantes
  - *“advanced attackers != advanced attacks”*

problématique | constat

- Détection
  - *Cas #1* : pas ou peu de politique de logs
  - *Cas #2* : Pokemon de la sécurité
- En résumé
  - Détection lors d'un impact sur le business
  - Manque de données pour tracer un incident

problématique | une solution

- *Tour de garde de la sécurité*
- Utilisation des journaux d'événements
  - Calquer les actions de l'attaquant sur des événements à détecter
- Problème
  - Besoin de ressources pour trier
  - Connaître les événements suspicieux
  - Uniquement Windows sera traité ici

Agenda

Problématique

Reconnaissance

Attaques sur les machines

Post-Exploitation

Conclusion

reconnaissance | intro

- Première étape d'un attaquant
  - Connaître les machines actives
  - Services accessibles
- Principe
  - Scan de ports
  - Sessions anonymes

reconnaissance | scan de ports

- Firewalls sur le réseau interne
  - Traitement des logs
- Windows
  - Firewall intégré
  - Sur les serveurs critiques
  - Mais pas de détection scan de ports

reconnaissance | scan de ports

- Détection basique
  - Par défaut trois profils de firewall
  - Stockage dans le journal d'évènements du firewall
  - 5157 (*tcp*), 5152 (*ip*)

reconnaissance | scan de ports

- Détection basique
  - Possibilité d'enregistrer dans un fichier les évènements (DROP-ALLOW) du Firewall

```
Date | Time | action | proto | src-ip | dst-ip | s
  | src-port | dst-port
```

  - En Powershell 3.0 :

```
Set-NetFirewallProfile -All -DefaultInboundAction
  Block -DefaultOutboundAction Allow -LogFileName
  mylog.log
```

reconnaissance | scan de ports

- Détection basique
  - Analyse des logs en Powershell

```
2013-10-08 15:53:25 DROP TCP 10.51.41.18 10.51.41.12 36975 135 44 S 1160419701 0 1024 - - - RECEIVE
2013-10-08 15:53:25 DROP TCP 10.51.41.18 10.51.41.12 36975 445 44 S 1160419701 0 1024 - - - RECEIVE
2013-10-08 15:53:25 DROP TCP 10.51.41.18 10.51.41.12 36975 139 44 S 1160419701 0 1024 - - - RECEIVE
2013-10-08 15:53:26 DROP TCP 10.51.41.18 10.51.41.12 36976 443 44 S 1160485236 0 1024 - - - RECEIVE
```

IP Source

Port Destination

reconnaissance | null sessions

- Principe
  - Connexion sans compte
  - En réalité, *NT Authority\Anonymous Logon*
  - Plus d'actualité sur les environnements pré-2008
  - Apparait également si la délégation n'est plus autorisée pour des comptes critiques

reconnaissance | null sessions

- Détection
  - Lecture du journal d'événements Windows via cmdlet Powershell *Get-EventLog*
  - Possibilité de filtrer les recherches :
    - InstanceId : 528 / 529 (Success / Failure)
    - Username : NT AUTHORITY\Anonymous Logon
  - Exemple Powershell :

```
Get-EventLog -Logname 'Security' -InstanceId 528
 -username 'NT AUTHORITY\Anonymous Logon'
```

Agenda

Problématique

Reconnaissance

Attaques sur les machines

Post-Exploitation

Conclusion

attaques | mots de passe

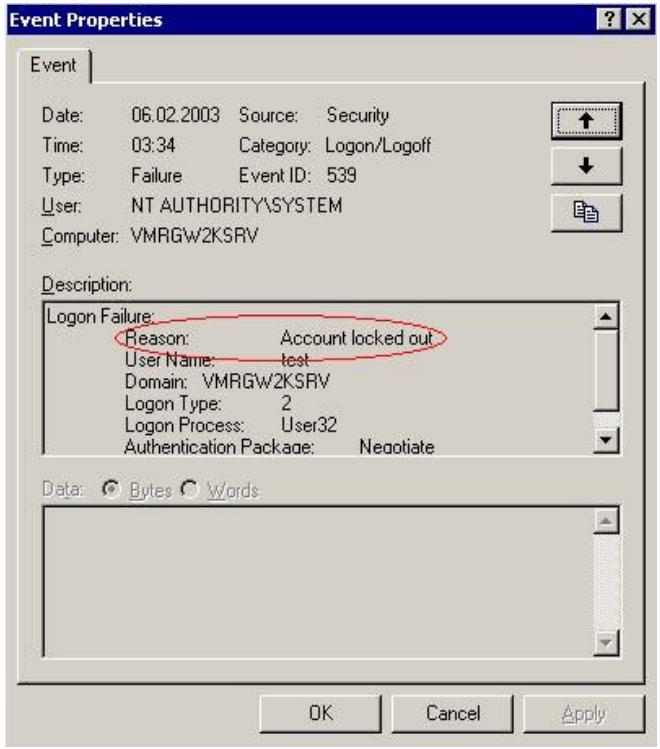
- Recherchés par attaquant
  - Permettent de gagner des accès
- Méthodes
  - Brute-force
  - Extraction des condensats
  - Extraction des *clairs* depuis la mémoire

attaques | mots de passe

- Extraction
  - Rejoint la détection d'outils
- Brute-force
  - Tentatives d'authentification échouées
  - Événement *logon failure*
  - Événement *user account locked out*

attaques | mots de passe

- Brute-force *online*
  - Génère beaucoup de bruit
- Fail2ban en powershell



attaques | exploitation

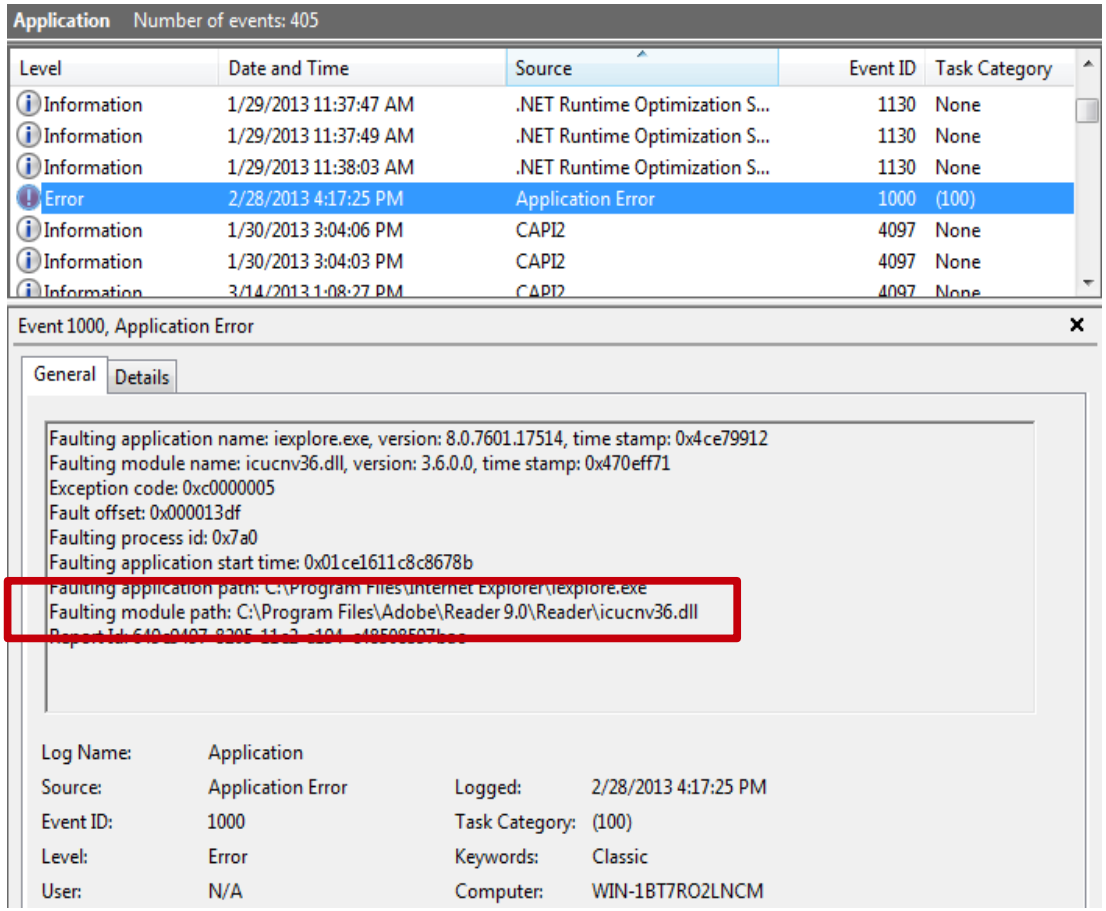
- Exécution de code
  - Exploitation d'une vulnérabilité logicielle
  - Contexte d'une application théoriquement autorisée

attaques | exploitation

- Détection difficile
  - Tant que l'application ne plante pas
- Crash
  - Échec de l'exploitation
  - Événements générés par chaque application dans *Applications and Services Logs*
  - Requête *WER*

attaques | exploitation

- Exemple de Crash



- Crash de Internet Explorer
- Le chargement de *icucnv36.dll* génère une erreur
- Injection de code
- Exploit CVE-2010-3654

attaques | exploitation

- Détection avancée avec EMET

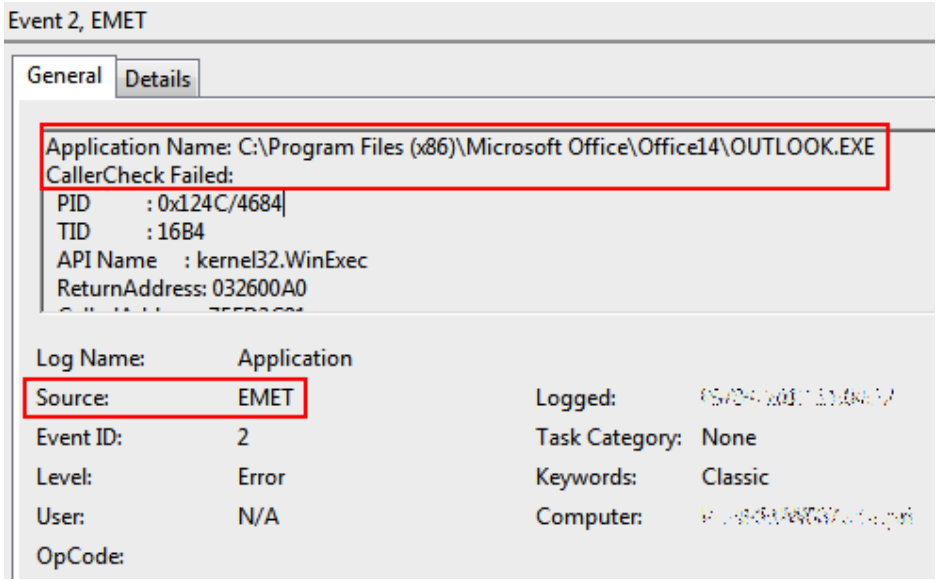
App Name	DEP	BottomUpAS...	EAF	MandatoryASLR	SEHOP	HeapSpr...	LoadLib	NullPage	MemP...	Caller	SimExecF...	StackPivot
Acrobat.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AcroRd32.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
chrome.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
EXCEL.EXE	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
iexplore.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
INFOPATH.EXE	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
java.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

- *EMET Notifier* enregistre les évènements dans le journal Windows

attaques | exploitation

- Détection avancée avec EMET

  - *event id* 1 ou 2 dans le journal d'événements Windows



attaques | exploitation

- Détection avancée avec EMET

  - Filtrage via *l'émetteur du log*

```
Get-Eventlog -Log application -EntryType error
        -InstanceId 1,2 -Source emet
```

Agenda

Problématique

Reconnaissance

Attaques sur les machines

Post-Exploitation

Conclusion

post-exploitation | intro

- Pour arriver à ses fins
  - Besoin de privilèges spécifiques
  - Garder un accès
  - Exfiltration de données
- Résultantes
  - Utilisation d'outils, droits spécifiques
  - Création/modifications de comptes
  - Connexions vers l'extérieur

post-exploitation | action privilégiée

- *Sensitive Privilege use*
  - 7 privilèges dangereux
    - SeDebugPrivilege
    - SeCreateTokenPrivilege
    - …
  - Créer beaucoup d'évènements !
  - Filtrage sur le champ *Privileges* sur eventID 578 (2003) ou 4674 (2008+)

post-exploitation | outils

- Outils pour collecter de l'information
  - *Keylogger*
  - *Trojan*
  - Extracteur mot de passe
- L'attaquant utilise toujours ce type d'outils pour gagner du temps

post-exploitation | outils

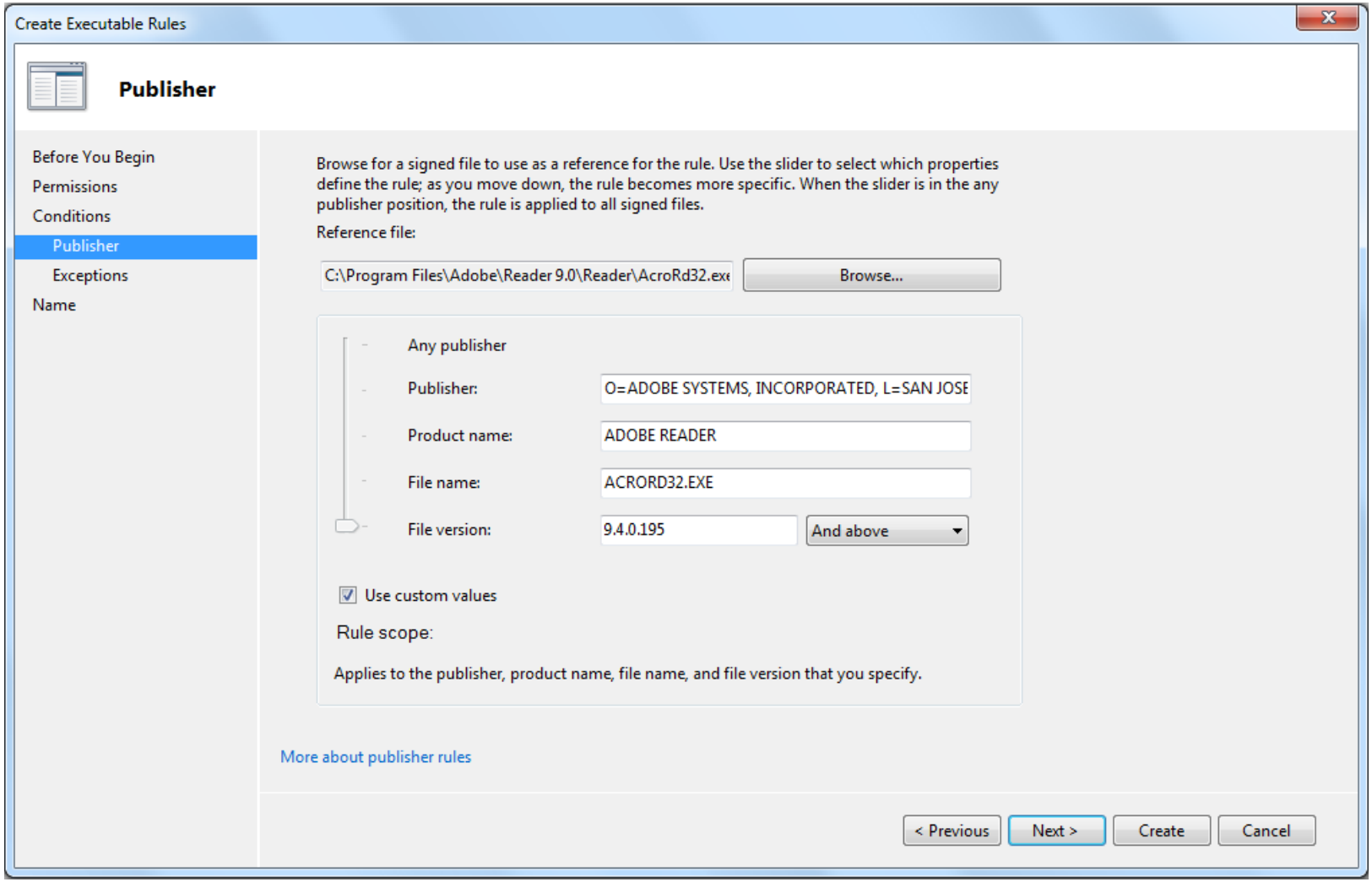
- Comparaison hash de l'exécutable avec une base
  - Online : Jotti, VirusTotal, Eureca
  - Locale : NIST (good), OWASP (bad)
- Récupération des exécutables par date

```
Get-ChildItem -Recurse -Path C:\" -Include *.exe | Where-
  Object { $_.CreationTime -ge "03/01/2013" -and
  $_.CreationTime -le "03/13/2013" }
```

post-exploitation | outils

- AppLocker
  - Bloquer/Détecter l'exécution de programmes non autorisés
  - Activable via GPO
  - Trois types de règles
    - Chemin d'accès
    - Hash
    - Signature

post-exploitation | outils



post-exploitation | outils

- AppLocker
  - Deux modes de fonctionnement
    - *Audit only*
    - *Enforce rules*
  - Récupérer les logs via cmdlet Powershell

```
Get-AppLockerFileInformation -EventLog -Logname
  "Microsoft-Windows-AppLocker\EXE and DLL" -EventTyp
  Audited -Statistics
```

post-exploitation | comptes

- Création d'un compte « backdoor » pour pérenniser l'accès
- L'attaquant n'est pas obligé de connaître le mot de passe/hash administrateur pour créer le compte

  - utilisation *token delegate* et WinRM
  - *pass-the-hash*

post-exploitation | comptes

- Points à surveiller dans l'AD
  - Création d'un compte
  - Ajout dans un groupe privilégié/intéressant
    - ex : r&d
  - Compte qui n'expire jamais
  - Compte verrouillé, déverrouillé, supprimé

post-exploitation | comptes

- Powershell est notre ami :)
  - Journal d'événements Windows
  - *Search-ADAccount* du module *Active Directory*

post-exploitation | connexions

- Exfiltration de données
    - Centralisation du contrôle des postes
    - Encapsulation des commandes
        - DNS, HTTP, SMTP, IRC
    - Utilisation de cryptographie

post-exploitation | connexions

- Déterminer les connexions vers l'extérieur
  - *netstat -ano*

```
TCP    10.51.41.12:49830      10.51.41.120:443       ESTABLISHED     3528
```

- Log des requêtes DNS
  - Activation depuis *Debug Logging*
  - System32\dns\Dns.log

post-exploitation | connexions

- DNS/IP Blacklist
  - Nombreuses bases en ligne
    - drone.abuse.ch
    - b.barracudacentral.org
    - alienvault
  - Recherche DNS via *IP.drone.abuse.ch*

post-exploitation | connexions

- Sinkhole / Blackhole
  - Rediriger tous les domaines suspicieux vers une IP
  - Monitoring des requêtes
    - http
    - ftp
    - irc
    - smtp

Agenda

Problématique

Reconnaissance

Attaques sur les machines

Post-Exploitation

Conclusion

Conclusion

- Utilisation de différentes technologies indispensables
- Automatiser la première étape
- *Threat intelligence*
- Outils de corrélation
- Ressources humaine nécessaires
- Ne pas oublier la protection

Outils

- Module Powershell avec les différentes fonctions présentées aujourd'hui
- Certains scripts sont exécutés périodiquement via le Task Scheduler Windows
- Coming soon ... sur notre site web www.scrt.ch et blog.scrt.ch

Questions?

Merci!

Contact:

julien@scrt.ch / sylvain@scrt.ch

@milkmix_ / @pwnhst

http://blog.scrt.ch