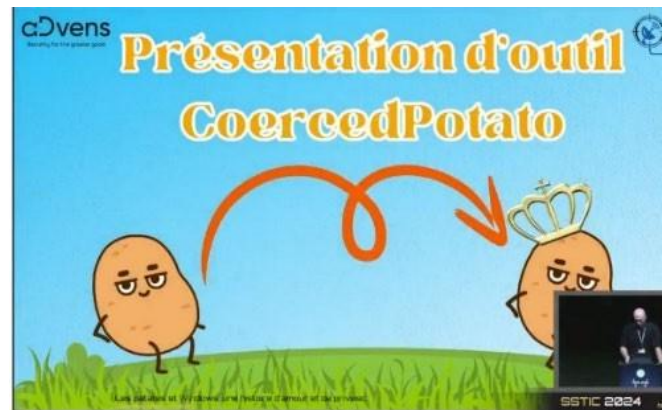


## 1. CoercedPotato Windows

Pendant mon stage, j'ai pu effectuer un test sur une méthode d'attaque d'élévation de privilège afin de vérifier si l'EDR permettait la protection contre cette attaque.

Le SSTIC est une conférence de cybersécurité qui a eu lieu pendant mon stage. Une méthode d'élévation de privilège y a été présentée.



### *Objectifs du Test*

1. Évaluer l'efficacité de l'outil CoercedPotato pour élever les privilèges sous Windows.
2. Tester la détection et la réponse de CrowdStrike aux activités de CoercedPotato.
3. Comprendre les mécanismes d'authentification et de token sous Windows utilisés par CoercedPotato.

### 1.1 Résumé de la présentation

La présentation présente CoercedPotato, un nouvel outil exploitant des concepts connus pour élever les privilèges sous Windows. CoercedPotato combine les techniques des "Potatoes" avec des fonctions RPC vulnérables pour obtenir des droits NT AUTHORITY\SYSTEM.

## 1.2 Introduction

Les exploits "Potatoes" permettent d'élever des privilèges en passant d'un compte de service à NT AUTHORITY\SYSTEM. CoercedPotato utilise les privilèges SeAssignPrimaryToken et SeImpersonatePrivilege.

Les privilèges **SeImpersonatePrivilege** et **SeAssignPrimaryToken** permettent de démarrer des processus au nom d'un autre utilisateur. Ces privilèges sont critiques pour les techniques "Potatoes" et permettent d'obtenir des droits SYSTEM.

Les access tokens sont des objets décrivant le contexte de sécurité d'un processus ou d'un thread. CoercedPotato utilise DuplicateTokenEx pour convertir des impersonation tokens en primary tokens et ainsi créer des processus avec des privilèges SYSTEM.

### « Named Pipe »

CoercedPotato utilise les "Named Pipes" pour forcer l'authentification du compte SYSTEM sur un serveur pipe contrôlé par l'attaquant. La fonction ImpersonateNamedPipeClient permet de s'approprier le contexte de sécurité du client.

L'outil Coercer de P0dalirius montre qu'il existe de nombreuses fonctions RPC exploitables pour forcer une authentification. CoercedPotato combine ces techniques pour élever les privilèges localement.

### (C++)

CoercedPotato utilise C++ pour créer un serveur pipe, forcer l'authentification et démarrer un processus avec des privilèges SYSTEM. Les étapes clés incluent la création du serveur pipe, la coercition de l'authentification et l'appel des fonctions RPC vulnérables.

```
PS D:\> .\precompiled\CoercedPotato.exe --command cmd.exe

CoercedPotato
@Hack0ura @Prepouce

[+] RUNNING ALL KNOWN EXPLOITS.
[PIPESERVER] Creating a thread launching a server pipe listening on Named Pipe \\.\pipe\coerced\pipe\spoolss.
[PIPESERVER] Named pipe '\\.\pipe\coerced\pipe\spoolss' listening...

[MS-RPRN] [*] Attempting MS-RPRN functions...

[MS-RPRN] Starting RPC functions fuzzing...
[MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotificationEx with target path: \\127.0.0.1\pipe\coerced
[MS-RPRN] [*] Error code returned : 1722
-> [-] Exploit failed, unknown error, trying another function...
[MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotification with target path: \\127.0.0.1\pipe\coerced
[MS-RPRN] [*] Error code returned : 1722
-> [-] Exploit failed, unknown error, trying another function...
[MS-RPRN] None of MS-RPRN worked...
```

## 1.3 Tests Effectués

### 1. Test de Création de Serveur Pipe

- Description : Création d'un serveur pipe en attente d'une connexion du compte SYSTEM.
- Résultat : Le serveur pipe a été créé avec succès, et une connexion du compte SYSTEM a été établie.
- Commentaire : CrowdStrike a détecté l'activité de création du pipe, mais n'a pas bloqué la connexion.

### 2. Test de Coercition d'Authentification

- Description : Utilisation de la fonction RPC vulnérable EfsRpcOpenFileRaw pour forcer l'authentification du compte SYSTEM sur le serveur pipe.
- Résultat : L'authentification a été forcée avec succès, permettant d'obtenir un impersonation token du compte SYSTEM.
- Commentaire : CrowdStrike a généré une alerte pour l'activité RPC suspecte, mais n'a pas bloqué l'exploitation.

### 3. Test de Création de Processus avec Privilèges SYSTEM

- Description : Utilisation du token obtenu pour créer un processus cmd.exe avec des privilèges SYSTEM.
- Résultat : Le processus cmd.exe a été démarré avec succès avec les privilèges SYSTEM.
- Commentaire : CrowdStrike a détecté l'élévation des privilèges et a bloqué le processus cmd.exe.

## Analyse des Résultats

## 1.4 Description de CrowdStrike

CrowdStrike, c'est l'antivirus et la protection qu'on utilise chez Cyklad pour surveiller tout ce qui se passe sur tous les postes de leurs client il propose aussi de gérer les alertes .

### *Fonctionnalités principales de CrowdStrike*

#### **Surveillance en Temps Réel :**

CrowdStrike surveille en continu tout ce qui se passe sur les postes. Il repère direct les comportements suspects et les anomalies. Grâce à ça, on peut détecter et réagir vite aux menaces avant qu'elles ne causent des problèmes.

### Alertes Automatisées :

CrowdStrike envoie des alertes pour chaque action suspecte qu'il repère. Ces alertes peuvent être gérées automatiquement où demander qu'un technicien intervienne. Par exemple, si quelque chose de louche est détecté, CrowdStrike prévient direct l'équipe de sécurité pour qu'ils vérifient.

### Gestion des Incidents :

Si personne n'est disponible pour répondre à une alerte, CrowdStrike peut isoler l'ordi concerné en le mettant en quarantaine. Cela évite que la menace se propage et permet de gérer le problème plus tard.

### Réponse Automatique :

CrowdStrike peut aussi gérer certaines alertes tout seul. Par exemple, il peut bloquer un processus malveillant dès qu'il le repère. Cette réaction rapide réduit le temps d'exposition aux menaces et limite les dégâts pour l'entreprise.

### Isolation et Remédiation :

Quand une menace est repérée, CrowdStrike peut isoler l'ordinateur infecté du réseau pour éviter toute interaction avec les autres systèmes. Cette isolation permet de contenir le problème jusqu'à ce qu'un technicien puisse intervenir et régler le souci.

## 1.5 Utilisation de CrowdStrike chez Cyklad

Pendant mon stage chez Cyklad, j'ai pu voir à quel point CrowdStrike est efficace dans plusieurs situations concrètes.

### Surveillance Continue et Alertes

#### Détection d'Activités Suspectes :

Par exemple, lors d'un test de sécurité, j'ai utilisé un outil appelé CoercedPotato pour simuler une attaque où on essaye de prendre plus de privilèges. CrowdStrike a détecté cela directement et a envoyé une alerte disant qu'il y avait une tentative de contourner les défenses.

#### Gestion des Alertes :

Les alertes envoyées par CrowdStrike arrivaient directement à l'équipe de sécurité. Si personne ne répondait, CrowdStrike pouvait isoler l'ordinateur touché pour éviter que la menace se répande.


## Réponse aux Incidents

### Blocage Automatique :

Après avoir repéré CoercedPotato, CrowdStrike a bloqué le processus suspect tout seul, empêchant toute action malveillante. Cette capacité à réagir automatiquement a montré à quel point CrowdStrike est efficace pour prévenir les incidents de sécurité.

### Avantages de l'utilisation de CrowdStrike

- **Réactivité** : CrowdStrike réagit super vite aux menaces, ce qui réduit le temps pour répondre aux incidents.
- **Visibilité** : La plateforme montre tout ce qui se passe sur les ordinateurs, ce qui aide à repérer les comportements suspects.
- **Efficacité** : En bloquant directement les choses suspectes, CrowdStrike empêche les attaques avant qu'elles ne fassent trop de dégâts.



**CoercedPotato.exe on PC-MATTEO by matteo**

Jun. 12, 2024 14:55:41

Tags

true\_positive

Description

A process launched that is likely associated with an exploit kit. Review the process tree.

Edit status

Investigate

Actions

Summary

Severity

High

Process

CoercedPotato.exe

Tactic & technique

Defense Evasion via  
Exploitation for Defense Evasion

Start time

Jun. 12, 2024 14:55:41

End time

Jun. 12, 2024 14:55:41

Assigned to

Matteo Baux

Status

Closed

Related incident

[View incident](#)

### Full details

Process - [See more details](#)

Process

CoercedPotato.exe

Actions taken

Process blocked

Severity

High

Objective

[Keep Access](#)

Tactic

[Defense Evasion](#)

Technique

[Exploitation for Defense Evasion](#)

Description

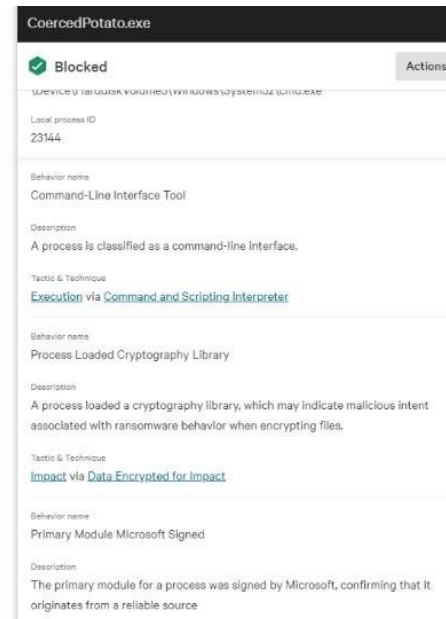
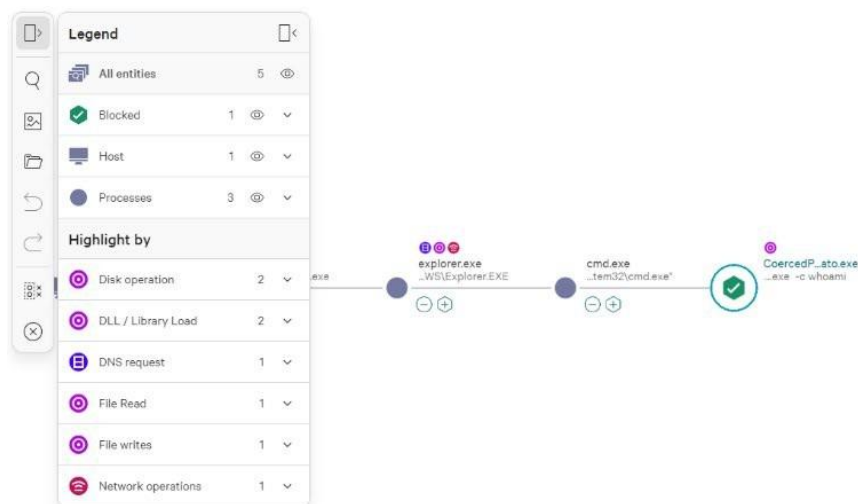
A process launched that is likely associated with an exploit kit. Review the process tree.

Command line

`.\CoercedPotato.exe -c whoami`

File path

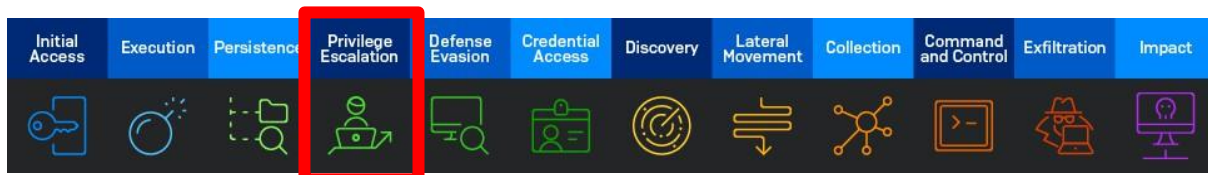
`\Device\HarddiskVolume3\Users\matteo\OneDrive - Cyklad\Private\Outils\CoercedPotato\x64\Debug\CoercedPotato.exe`



## Conclusion

Le test a démontré que CoercedPotato est capable d'élever les privilèges sous Windows en exploitant des fonctions RPC vulnérables. CrowdStrike a réussi à détecter et bloquer les activités suspectes.

MITRE ATT&CK est un référentiel de tactiques et techniques utilisées par les cyberattaquants. Il aide les professionnels de la cybersécurité à comprendre les méthodes des attaquants, à identifier les menaces et à renforcer les défenses.



(<https://attack.mitre.org/>) Voici la liste des attaques les plus utilisées, notre attaque se situe la phase Privilège Escalation