



Document de qualification des alertes

d'après les fiches réflexes de traitement des alertes cybersécurité
client Scholia

Nicolas Clerbout
Date : 15 mars 2024
3 alertes traitées

Alerte 1/3 : Création d'un compte local

Etape 1 : Comprendre la détection

- 1) La création d'un compte local, dans le cadre d'une attaque, *correspondrait* à l'étape « Command and Control » de la Cyber Kill-Chain (étape postérieure à l'exploitation de vulnérabilité et l'installation après accès initial).
- 2) Du point de vue de la matrice MITRE ATT&CK, la création d'un compte local *correspondrait* à la tactique « Persistence » (TA0003) avec la technique « Create Account » (T1136, en particulier T1136.001 – Local account).
- 3) PROBABLE Faux Positif : la tentative de création de compte est faite depuis le compte Administrateur ADM_JDUBOIS qui ne présente pas de signe de compromission et n'a pas été signalé comme tel.
- 4) Règle de détection. : Une alerte est créée quand une tentative est faite de créer un nouveau compte utilisateur au sein du SI.

Etape 2 : Analyse de l'observable « *hostname* »

- 1) Nom de la machine affectée par l'alerte : SRV-FORMASUP-001.
- 2) Il s'agit d'un Serveur. Le nom indique un lien avec le projet « Formation Supérieure »
- 3) Enrichissement : Il s'agit d'un serveur sous Windows Server 2022 d'applications métiers (cf. CMDB). Comme indiqué dans le ticket CHANGE5900, ce serveur fait partie des actifs impactés par la mise à jour de l'application FORMASUP approuvée par le comité d'architecture MEP.

Etape 3 : Analyse de l'observable « *account* »

- 1) Le compte impliqué dans la tentative de création de compte local est : ADM_JDUBOIS.
- 2) Il s'agit donc d'une tentative en totale cohérence avec le rôle du compte Administrateur associé à Jean Dubois.
- 3) Enrichissement : Le compte ADM_JDUBOIS a les privilèges pour réaliser ce genre de tâches admin (cf. Annuaire). De plus, c'est bien le compte ADM_JDUBOIS qui a informé via le ticket CHANGE5900 des modifications à venir dans le cadre de la mise à jour de l'application FORMASUP.

Etape 4 : Analyse de l'événement d'intérêt

1) Log Windows (id=U6ohyoQBpt9xH_Dc8HHU) du 30 novembre 2022 à 12h49.

2) Nom du process : net.exe

Nom du process parent : powershell_ise.exe

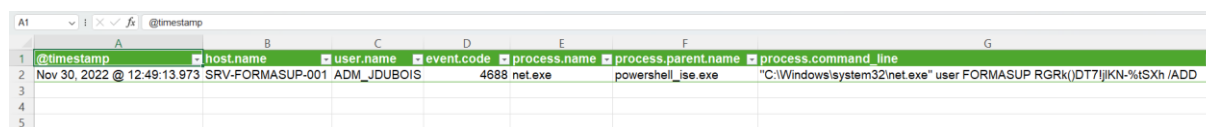
Ligne de commande :

"C:\Windows\system32\net.exe", user, FORMASUP, RGRk()DT7!j!KN-%tSXh, /ADD

3) Affichage des champs :

- timestamp
- host.name
- user.name
- event.code
- process.name
- process.parent.name
- process.command_line
- process.args

Exportation des informations au format CSV ensuite chargées dans un document Excel, voir Pièce Jointe au Task Log correspondant sur TheHive :



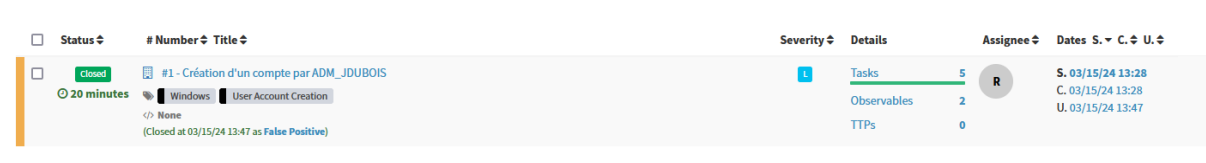
@timestamp	host.name	user.name	event.code	process.name	process.parent.name	process.command_line
Nov 30, 2022 @ 12:49:13.973	SRV-FORMASUP-001	ADM_JDUBOIS	4688	net.exe	powershell_ise.exe	"C:\Windows\system32\net.exe" user FORMASUP RGRk()DT7!j!KN-%tSXh /ADD

Alerte 1/3 – Etape 4 : log création de compte utilisateur – filtre par champs

Le processus ne semble pas malicieux : « net.exe » est un processus Windows permettant la gestion de divers aspects du Système d'Exploitation, dont la gestion des utilisateurs. Le processus a visiblement été lancé comme ligne de commande dans PowerShell. La commande a été effectuée avec le compte à privilèges ADM_JDUBOIS, ce qui est également normal.

Etape 5 : Qualification

Faux Positif : Utilisation légitime du compte à privilèges pour créer un utilisateur. Le processus parent (powershell_ise.exe) n'est pas inhabituel. Cohérent avec les informations communiquées dans le ticket CHANGE5900.



Status	# Number	Title	Severity	Details	Assignee	Dates	S.	C.	U.
Closed	#1	Création d'un compte par ADM_JDUBOIS	Low	Tasks: 5, Observables: 2, TTPs: 0	R	S: 03/15/24 13:28, C: 03/15/24 13:28, U: 03/15/24 13:47			

Alerte 2/3 : Exécution de PowerShell avec l'argument « Download »

Etape 1 : Comprendre la détection

- 1) Le téléchargement d'un exécutable *corresponderait*, dans le cadre d'une attaque, à l'étape « Install » de la Cyber Kill-Chain (étape postérieure à l'exploitation de vulnérabilité qui a permis l'exécution de la commande Powershell)
- 2) Du point de vue de la matrice MITRE ATT&CK, le téléchargement d'un exécutable via PowerShell *corresponderait* à la Tactique « Execution », Technique « Command and Scripting Interpreter » (T1059, en particulier T1059.001 - PowerShell).
- 3) POSSIBLE Faux Positif : Effectuer un téléchargement via PowerShell n'est pas typique pour des usagers standards mais c'est une possibilité dans certains cas. Il faut donc enrichir l'alerte pour déterminer s'il s'agit d'une action légitime ou non.
- 4) Règle de détection : Une alerte est créée quand une exécution de PowerShell présente l'argument « Download » (Télécharger) car il pourrait s'agir d'une tentative d'installation de malware.

Etape 2 : Analyse de l'URL

- 1) URL requêtée :
`hxxps://github.com/zaproxy/zaproxy/releases/download/v2.12.0/ZAP_2_12_0_windows.exe`
- 2) Domaine : github.com
Domaine bien connu, en général de confiance (mais peut parfois être exploité par acteurs malveillants). Pas de signalement sur VirusTotal.
- 3) Chemin du fichier :
`/zaproxy/zaproxy/releases/download/v2.12.0/ZAP_2_12_0_windows.exe`
- 4) Le fichier est un exécutable. Le chemin et le nom du fichier évoquent un proxy et donc un outil qui permettrait la redirection du trafic. C'est donc un fichier probablement malicieux.

Etape 3 : Analyse de l'observable « account »

- 1) Compte : « pen TEST »
- 2) Ce compte n'est pas un compte de service et n'est pas nominatif. Il ne semble pas disposer de privilèges, mais cela demeure à confirmer. Le nom du compte évoque une simulation d'attaque dans le cadre d'une opération de Red Team.

3) Enrichissement : Le ticket REQUEST3562 « Déclaration test d'intrusion » semble correspondre : annonce d'un test par Mohammed Beziz (Ingénieur, département Sécurité et Tests d'intrusions, cf. Annuaire) avec un compte local.

Etape 4 : Analyse de l'observable « hostname »

1) Nom de la machine : DESKTOP-EDZ84

2) La machine semble être un poste de travail (« Desktop »). Le nom de la machine n'évoque pas à lui seul un projet en particulier.

3) Enrichissement : Le ticket REQUEST3562 confirme que cette machine est celle utilisée pour le test d'intrusion. Cette machine est attribuée à Mohammed Beziz et il s'agit bien d'un poste de travail (cf. CMDB). Le ticket mentionne que ce test est réalisé dans le contexte du projet MYSCHOOL.

Etape 5 : Qualification

Faux Positif : activité prévue dans le cadre d'un test d'intrusion préalablement déclaré dans le ticket REQUEST3562.

Status	# Number	Title	Severity	Details	Assignee	Dates	S.	C.	U.
closed	#2	Execution de powershell avec l'argument "Download" sur DESKTOP-EDZ84	Low	Tasks: 5 Observables: 3 TTPs: 0	R	S. 03/15/24 13:52 C. 03/15/24 13:52 U. 03/15/24 14:11			
19 minutes		Windows Powershell execution with "download" keyword Install TA0002 / T1059.001							
		None (Closed at 03/15/24 14:11 as False Positive)							

Alerte 3/3 : Mail suspect

Etape 1 : Investigation auprès de l'utilisateur

Questions à poser à l'utilisateur pendant l'entretien :

- *Ce message a-t-il provoqué votre méfiance ? Pourquoi ?*
- *Connaissez-vous le principe du phishing ?*
- *Votre boîte mail ou votre poste de travail ont-ils émis des avertissements concernant ce message ?*
- *Avez-vous vérifié l'**adresse mail** de l'expéditeur ?*
- *Avez-vous cliqué sur un des liens présents dans le message ?*
- *Si le message avait une pièce jointe, l'avez-vous téléchargée ?*
- *Avez-vous répondu à ce message ?*
- *Recevez-vous beaucoup de messages de ce genre sur votre boîte mail pro ? sur votre boîte mail personnelle ?*
-

Etape 2 : Méthodologie d'analyse des composants du mail

1) En-tête :

- Vérification de l'adresse mail de l'expéditeur
- Vérification du domaine
- Vérification de l'adresse IP : fait-elle partie des IoC déjà identifiés ? + vérification sur VirusTotal

2) Corps du mail :

- Le mail présente-t-il de grossières fautes d'orthographe ? **Oui**
- Le langage présente-t-il des éléments anxiogènes en prétendant une situation urgente ? **Oui**
- Le mail a-t-il des pièces jointes ? **NC**
Points de vigilance : fichiers exécutables (.exe, etc.) ; archives (.zip, etc.) ; Documents de type Office (.docx, .xlsx ou équivalents, potentiellement avec macros activées) ; Documents PDF.
- Le mail présente-t-il des liens suspects ? **Oui**
Points de vigilance : domaines suspects ; multiples occurrences de la même url pour des liens/boutons différents.

3) Qualification de la menace :

Pour l'utilisateur : risque de vol de coordonnées bancaires et autres données personnelles, avec possibilité de pertes financières et/ou de vol d'identité. Risque de compromission du poste de travail.

Pour l'entreprise : risque de connexion externe vers attaquant et donc risque d'accès initial par agent ou groupe malicieux et de compromission du poste du travail du SI

4) Sensibilisation des utilisateurs.

Il est sans doute utile d'utiliser cet exemple pour :

- (a) montrer la réalité de la menace de phishing ;
- (b) renforcer la sensibilisation sur les moyens de reconnaître les tentatives de phishing ;
- (c) consolider l'assimilation de la bonne pratique de signaler les messages suspects comme cela a été le cas cette fois-ci.

Suggestions : distribuer à nouveau la fiche de bonnes pratiques cyber concernant la sensibilisation au risque de phishing + envisager de lancer une campagne de simulation de phishing.

Etape 3 : Qualification

Vrai Positif : Il s'agit d'une tentative de phishing. Les domaines des différents liens et de l'adresse mail de l'expéditeur ont leur place dans la liste des IoCs à surveiller.