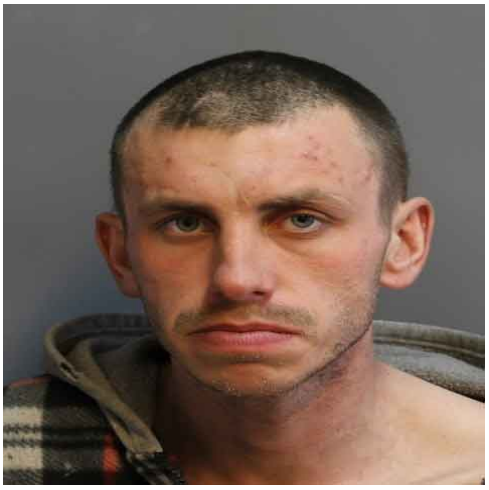
ALERTE - INTRUSION DÉTECTÉE

Suspect : Suspect inconnu

Période : 2025-11-01 20:23:55 -> 2025-11-01 20:24:54



1. Résumé des activités

Ce qui s’est passé entre 20 h 23 et 20 h 55 le 1 novembre 2025 L’intrus a d’abord ouvert le fichier *tracking_activity.py* dans Visual Studio Code et a cliqué plusieurs fois dans cet éditeur, en prenant des captures d’écran à chaque changement de fenêtre. Il a ensuite utilisé la fonction de recherche du système, puis a lancé l’application Spotify à plusieurs reprises (on voit neuf processus *Spotify.exe* qui démarrent en même temps). Pendant ce temps, il a ouvert d’autres programmes : le gestionnaire de tâches en arrière-plan (*backgroundTaskHost.exe*), le composant Windows *RuntimeBroker*, puis, à 20 h 40, il a démarré des consoles (*conhost.exe*), le client Windows Protection Control (*WpcTok.exe*) et plusieurs instances de *git.exe* (outil de gestion de code). Il a aussi accédé aux *Paramètres* de Windows, a copié du texte depuis le presse-papier (« print(output["json_path"] »), et a continué à prendre des captures d’écran de chaque fenêtre active. **Pourquoi c’est risqué** - **Multiples lancements d’applications** (Spotify, git, consoles) peuvent masquer des programmes malveillants qui s’exécutent en arrière-plan sans que l’utilisateur s’en rende compte. - **Prises de captures d’écran** et **copies du presse-papier** permettent de récupérer des informations visibles à l’écran (code source, données sensibles, mots de passe éventuels). - **Lancement de processus système** (*backgroundTaskHost*, *RuntimeBroker*, *WpcTok*) peut indiquer que des services de Windows sont détournés pour exécuter du code non autorisé. - **Utilisation de Git** pourrait servir à télécharger ou à pousser du code vers un serveur externe, facilitant le vol ou la modification de projets. - **Accès aux paramètres** montre que l’intrus a cherché à explorer ou à modifier la configuration du système, ce qui peut être le prélude à des changements de sécurité (désactivation d’antivirus, modification de politiques, etc.). En résumé, l’intrus a très rapidement navigué entre plusieurs applications, a capturé ce qui était affiché à l’écran et a lancé de nombreux programmes, ce qui représente un danger de **vol de données**, de **compromission du système** et de **possibilité d’installation de logiciels malveillants**. Il est recommandé de vérifier les processus en cours, de changer les mots de passe, de scanner la machine avec un antivirus à jour et de

surveiller les dépôts Git pour d’éventuelles.

2. Tableau des activités clés

Heure (UTC)	Action	Détails
2025-11-01 20:23:55	window_change	title:tracking_activity.py - shacks-2025 - Visual Stu
2025-11-01 20:23:55	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:23:57	mouse_click	x:487, y:478, button:Button.left, window_title:tracki
2025-11-01 20:23:57	mouse_click	x:466, y:497, button:Button.left, window_title:tracki
2025-11-01 20:23:58	mouse_click	x:455, y:518, button:Button.left, window_title:tracki
2025-11-01 20:23:58	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:00	mouse_click	x:570, y:1041, button:Button.left, window_title:trac
2025-11-01 20:24:00	window_change	title:Rechercher
2025-11-01 20:24:01	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:02	mouse_click	x:976, y:438, button:Button.left, window_title:Rech
2025-11-01 20:24:03	window_change	title:Spotify
2025-11-01 20:24:04	window_change	title:Spotify Free
2025-11-01 20:24:04	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:05	process_start	pid:10432, name:backgroundTaskHost.exe, usern
2025-11-01 20:24:05	process_start	pid:9152, name:Spotify.exe, username:IPG3ALEX
2025-11-01 20:24:05	process_start	pid:19648, name:Spotify.exe, username:IPG3ALE
2025-11-01 20:24:05	process_start	pid:35332, name:Spotify.exe, username:IPG3ALE
2025-11-01 20:24:05	process_start	pid:3396, name:Spotify.exe, username:IPG3ALEX
2025-11-01 20:24:05	process_start	pid:16524, name:Spotify.exe, username:IPG3ALE
2025-11-01 20:24:05	process_start	pid:8268, name:Spotify.exe, username:IPG3ALEX
2025-11-01 20:24:05	process_start	pid:27116, name:RuntimeBroker.exe, username:I
2025-11-01 20:24:07	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:09	mouse_click	x:996, y:435, button:Button.left, window_title:Spoti
2025-11-01 20:24:10	process_start	pid:25796, name:Spotify.exe, username:IPG3ALE
2025-11-01 20:24:10	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:11	mouse_click	x:649, y:1058, button:Button.left, window_title:Spo
2025-11-01 20:24:12	window_change	title:Rechercher
2025-11-01 20:24:12	mouse_click	x:422, y:650, button:Button.left, window_title:Rech
2025-11-01 20:24:13	mouse_click	x:586, y:555, button:Button.left, window_title:tracki
2025-11-01 20:24:13	window_change	title:tracking_activity.py - shacks-2025 - Visual Stu
2025-11-01 20:24:14	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:15	keystroke	key:Key.ctrl_l
2025-11-01 20:24:15	keystroke	key:'\x03'
2025-11-01 20:24:16	clipboard_copy	content:print(output["json_path"])

2025-11-01 20:24:16	mouse_click	x:626, y:1054, button:Button.left, window_title:trac
2025-11-01 20:24:16	keystroke	key:Key.ctrl_l
2025-11-01 20:24:17	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:17	keystroke	key:'\x16'
2025-11-01 20:24:17	window_change	title:Rechercher
2025-11-01 20:24:20	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:20	process_start	pid:25792, name:backgroundTaskHost.exe, usern
2025-11-01 20:24:23	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:24	mouse_click	x:832, y:1055, button:Button.left, window_title:Rec
2025-11-01 20:24:25	keystroke	key:Key.backspace
2025-11-01 20:24:26	mouse_click	x:504, y:474, button:Button.left, window_title:Rech
2025-11-01 20:24:26	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:26	window_change	title:tracking_activity.py - shacks-2025 - Visual Stu
2025-11-01 20:24:29	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:31	mouse_click	x:1374, y:1051, button:Button.left, window_title:tra
2025-11-01 20:24:32	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:32	window_change	title:Spotify Free
2025-11-01 20:24:32	mouse_click	x:1902, y:37, button:Button.left, window_title:Spoti
2025-11-01 20:24:33	window_change	title:tracking_activity.py - shacks-2025 - Visual Stu
2025-11-01 20:24:34	mouse_click	x:546, y:1058, button:Button.left, window_title:trac
2025-11-01 20:24:34	window_change	title:Rechercher
2025-11-01 20:24:35	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:36	mouse_click	x:532, y:415, button:Button.left, window_title:Rech
2025-11-01 20:24:36	window_change	title:Paramètres
2025-11-01 20:24:38	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:38	mouse_click	x:120, y:263, button:Button.left, window_title:Para
2025-11-01 20:24:40	mouse_click	x:1919, y:0, button:Button.left, window_title:Param
2025-11-01 20:24:40	process_start	pid:9312, name:conhost.exe, username:IPG3ALE
2025-11-01 20:24:40	process_start	pid:29792, name:conhost.exe, username:IPG3AL
2025-11-01 20:24:40	process_start	pid:11392, name:WpcTok.exe, username:IPG3AL
2025-11-01 20:24:40	process_start	pid:32940, name:git.exe, username:IPG3ALEX\ale
2025-11-01 20:24:40	process_start	pid:9196, name:git.exe, username:IPG3ALEX\alex
2025-11-01 20:24:40	process_start	pid:32236, name:conhost.exe, username:IPG3AL
2025-11-01 20:24:40	process_start	pid:5488, name:git.exe, username:IPG3ALEX\alex
2025-11-01 20:24:40	process_start	pid:20952, name:git.exe, username:IPG3ALEX\ale
2025-11-01 20:24:40	window_change	title:tracking_activity.py - shacks-2025 - Visual Stu
2025-11-01 20:24:41	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:44	mouse_click	x:70, y:254, button:Button.left, window_title:trackin
2025-11-01 20:24:44	screenshot	file_path:tracking/screenshots/screenshot_176202

2025-11-01 20:24:48	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:51	screenshot	file_path:tracking/screenshots/screenshot_176202
2025-11-01 20:24:53	mouse_click	x:1009, y:1060, button:Button.left, window_title:tra
2025-11-01 20:24:53	window_change	title:Lenovo Vantage
2025-11-01 20:24:54	screenshot	file_path:tracking/screenshots/screenshot_176202