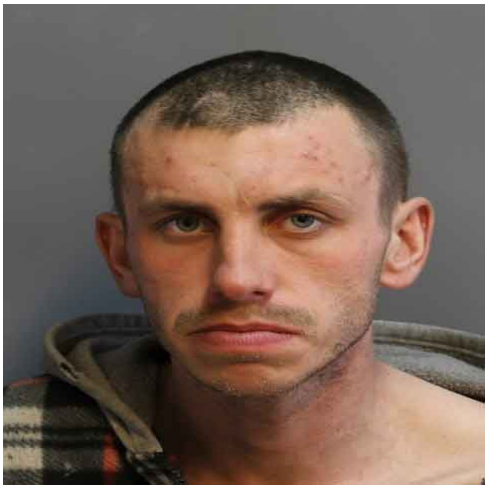
ALERTE - INTRUSION DÉTECTÉE

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 min 55 s et 20 h 24 min 54 s le 1er novembre 2025 Pendant environ une minute, l’ordinateur a été utilisé de façon très active : le programme *tracking_activity.py* s’est ouvert dans Visual Studio Code, puis l’utilisateur a navigué entre plusieurs fenêtres (recherche Windows, Spotify, les paramètres, Lenovo Vantage, etc.). De nombreux clics de souris et quelques frappes de clavier ont été enregistrés, ainsi que plusieurs captures d’écran de chaque fenêtre affichée. En parallèle, plusieurs processus ont été lancés, dont *Spotify.exe* (plusieurs instances), *backgroundTaskHost.exe*, *RuntimeBroker.exe*, *conhost.exe*, *WpcTok.exe* (outil de protection Windows) et plusieurs instances de *git.exe*. **Risques potentiels pour un utilisateur non-technique** - **Exposition de données personnelles** : les captures d’écran montrent tout ce qui était affiché à l’écran (codes, recherches, applications ouvertes). Si ces images contenaient des informations sensibles (identifiants, projets en cours, données privées), elles pourraient être récupérées par un tiers malveillant. - **Exécution de programmes non désirés** : le lancement de multiples processus, notamment plusieurs instances de Spotify et de *git.exe*, peut indiquer que des scripts automatisés ou des logiciels ont été exécutés sans le consentement explicite de l’utilisateur, ce qui augmente la surface d’attaque. - **Collecte de comportements** : le suivi du déplacement de la souris, des clics et des frappes de clavier constitue une forme de surveillance. Un tel enregistrement pourrait être exploité pour deviner des mots de passe, des habitudes de travail ou d’autres informations confidentielles. - **Possibles failles de sécurité** : l’ouverture fréquente de la fenêtre « Paramètres » et le lancement de *WpcTok.exe* (composant du pare-feu Windows) suggèrent que des modifications système pourraient être en cours. Si elles sont mal configurées, elles peuvent affaiblir la protection de l’ordinateur. **En résumé**, pendant cette courte période, l’ordinateur a été intensément manipulé, avec de nombreuses captures d’écran, enregistrements de clics et plusieurs programmes lancés. Cela expose potentiellement des informations privées et montre que des actions automatisées ou non autorisées ont eu lieu, ce qui pourrait être exploité par un attaquant pour voler des données ou affaiblir la sécurité du système. Il est recommandé de vérifier les

captures d’écran, de s’assurer que les processus lancés sont légitimes, de changer les mots de passe éventuellement exposés et de renforcer les paramètres de sécurité (antivirus, pare-feu, mise à jour des logiciels).

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:IPG3ALI
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:IPG3ALI
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