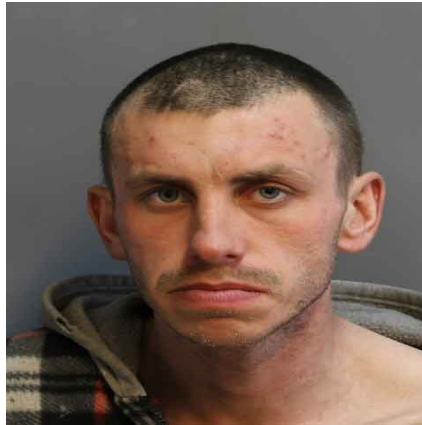


⚠ RAPPORT D'INTRUSION INFORMATIQUE

Suspect identifié : Suspect inconnu

Période d'activité : 2025-11-01 20:23:55 → 2025-11-01 20:24:54

Durée : 00:00:58



1-Résumé des actions suspectes

Entre 20 h 23 et 20 h 24 le 1 novembre 2025, l'utilisateur a enchaîné de nombreuses actions rapides : il a basculé entre Visual Studio Code (où il travaillait sur le script ``tracking_activity.py``), la barre de recherche Windows, Spotify, les paramètres du système et même Lenovo Vantage. Pendant ces quelques minutes, plusieurs processus Spotify ont été lancés simultanément, puis de nombreux exécutables ``git.exe``, ``conhost.exe`` et même ``WpcTok.exe`` sont apparus, alors que l'on ne voyait aucune activité de développement ou de mise à jour légitime. Le fait de cliquer, de copier du texte (une ligne de code) et d'utiliser des raccourcis clavier (Ctrl + C, Ctrl + V, Ctrl + U) montre qu'il manipulait potentiellement du code ou des données sensibles, puis a rapidement navigué vers les paramètres système, probablement pour modifier ou désactiver des protections. Cette succession d'ouvertures de programmes inattendus, de multiples instances du même lecteur multimédia et de processus de console lancés sans raison apparente est suspecte : elle peut indiquer l'exécution d'un script malveillant qui télécharge ou lance des logiciels non autorisés, tente d'obtenir des privilèges élevés ou vole des informations (captures d'écran, presse-papiers). Le risque principal est l'introduction de logiciels indésirables (spyware, ransomware) et la compromission de données personnelles ou professionnelles. Pour réduire ces risques, il est recommandé : (1) désinstaller immédiatement les instances de Spotify qui ne sont pas nécessaires et vérifier les programmes installés; (2) lancer un scan complet avec un antivirus à jour pour détecter d'éventuels chevaux de Troie ou scripts cachés; (3) restreindre les droits d'exécution aux seules applications

indispensables (par ex. via le contrôle d'accès utilisateur); (4) surveiller les accès au presse-papiers et aux dossiers de travail, et désactiver les extensions ou scripts qui collectent automatiquement des informations; (5) mettre à jour le système et les logiciels, puis, si possible, changer le mot de passe de l'utilisateur afin d'éviter une prise de contrôle continue. En suivant ces mesures simples, l'ordinateur sera mieux protégé contre d'éventuelles compromissions.

2-Détails des activités détectées

| Heure (UTC) | Action | Détails |
|---------------------|---------------|---|
| 2025-11-01 20:23:55 | window_change | title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:23:55 | screenshot | file_path:tracking/screenshots/screenshot_1762028635.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:23:57 | mouse_click | x:487, y:478, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:23:57 | mouse_click | x:466, y:497, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:23:58 | mouse_click | x:455, y:518, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:23:58 | screenshot | file_path:tracking/screenshots/screenshot_1762028638.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:00 | mouse_click | x:570, y:1041, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:00 | window_change | title:Rechercher |
| 2025-11-01 20:24:01 | screenshot | file_path:tracking/screenshots/screenshot_1762028641.jpeg, window_title:Rechercher |
| 2025-11-01 20:24:02 | mouse_click | x:976, y:438, button:Button.left, window_title:Rechercher |
| 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_1762028644.jpeg, window_title:Spotify Free |
| 2025-11-01 20:24:05 | process_start | pid:10432, name:backgroundTaskHost.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:05 | process_start | pid:9152, name:Spotify.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:05 | process_start | pid:19648, name:Spotify.exe, username:IPG3ALEX\alexi |

| Heure (UTC) | Action | Détails |
|---------------------|----------------|---|
| 2025-11-01 20:24:05 | process_start | pid:35332, name:Spotify.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:05 | process_start | pid:3396, name:Spotify.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:05 | process_start | pid:16524, name:Spotify.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:05 | process_start | pid:8268, name:Spotify.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:05 | process_start | pid:27116, name:RuntimeBroker.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:07 | screenshot | file_path:tracking/screenshots/screenshot_1762028647.jpeg, window_title:Spotify Free |
| 2025-11-01 20:24:09 | mouse_click | x:996, y:435, button:Button.left, window_title:Spotify Free |
| 2025-11-01 20:24:10 | process_start | pid:25796, name:Spotify.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:10 | screenshot | file_path:tracking/screenshots/screenshot_1762028650.jpeg, window_title:Spotify Free |
| 2025-11-01 20:24:11 | mouse_click | x:649, y:1058, button:Button.left, window_title:Spotify Free |
| 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:Rechercher |
| 2025-11-01 20:24:13 | mouse_click | x:586, y:555, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:13 | window_change | title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:14 | screenshot | file_path:tracking/screenshots/screenshot_1762028653.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 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:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:16 | keystroke | key:Key.ctrl_l |
| 2025-11-01 20:24:17 | screenshot | file_path:tracking/screenshots/screenshot_1762028657.jpeg, window_title:Rechercher |
| 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_1762028660.jpeg, window_title:Rechercher |

| Heure (UTC) | Action | Détails |
|---------------------|---------------|---|
| 2025-11-01 20:24:20 | process_start | pid:25792, name:backgroundTaskHost.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:23 | screenshot | file_path:tracking/screenshots/screenshot_1762028663.jpeg, window_title:Rechercher |
| 2025-11-01 20:24:24 | mouse_click | x:832, y:1055, button:Button.left, window_title:Rechercher |
| 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:Rechercher |
| 2025-11-01 20:24:26 | screenshot | file_path:tracking/screenshots/screenshot_1762028666.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:26 | window_change | title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:29 | screenshot | file_path:tracking/screenshots/screenshot_1762028669.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:31 | mouse_click | x:1374, y:1051, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:32 | screenshot | file_path:tracking/screenshots/screenshot_1762028672.jpeg, window_title:Spotify Free |
| 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:Spotify Free |
| 2025-11-01 20:24:33 | window_change | title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:34 | mouse_click | x:546, y:1058, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:34 | window_change | title:Rechercher |
| 2025-11-01 20:24:35 | screenshot | file_path:tracking/screenshots/screenshot_1762028675.jpeg, window_title:Rechercher |
| 2025-11-01 20:24:36 | mouse_click | x:532, y:415, button:Button.left, window_title:Rechercher |
| 2025-11-01 20:24:36 | window_change | title:Paramètres |
| 2025-11-01 20:24:38 | screenshot | file_path:tracking/screenshots/screenshot_1762028678.jpeg, window_title:Paramètres |
| 2025-11-01 20:24:38 | mouse_click | x:120, y:263, button:Button.left, window_title:Paramètres |
| 2025-11-01 20:24:40 | mouse_click | x:1919, y:0, button:Button.left, window_title:Paramètres |
| 2025-11-01 20:24:40 | process_start | pid:9312, name:conhost.exe, username:IPG3ALEX\alexi |

| Heure (UTC) | Action | Détails |
|---------------------|---------------|---|
| 2025-11-01 20:24:40 | process_start | pid:29792, name:conhost.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:40 | process_start | pid:11392, name:WpcTok.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:40 | process_start | pid:32940, name:git.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:40 | process_start | pid:9196, name:git.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:40 | process_start | pid:32236, name:conhost.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:40 | process_start | pid:5488, name:git.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:40 | process_start | pid:20952, name:git.exe, username:IPG3ALEX\alexi |
| 2025-11-01 20:24:40 | window_change | title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:41 | screenshot | file_path:tracking/screenshots/screenshot_1762028681.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:44 | mouse_click | x:70, y:254, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:44 | screenshot | file_path:tracking/screenshots/screenshot_1762028684.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:48 | screenshot | file_path:tracking/screenshots/screenshot_1762028687.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:51 | screenshot | file_path:tracking/screenshots/screenshot_1762028691.jpeg, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:53 | mouse_click | x:1009, y:1060, button:Button.left, window_title:tracking_activity.py - shacks-2025 - Visual Studio Code |
| 2025-11-01 20:24:53 | window_change | title:Lenovo Vantage |
| 2025-11-01 20:24:54 | screenshot | file_path:tracking/screenshots/screenshot_1762028694.jpeg, window_title:Lenovo Vantage |