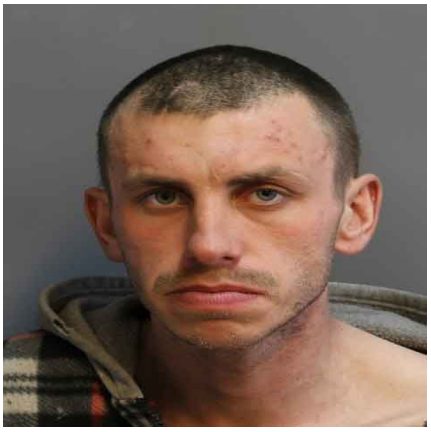
⚠ RAPPORT D'INTRUSION INFORMATIQUE

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 min 55 s et 20 h 24 min 54 s le 1 novembre 2025, l’utilisateur a enchaîné une série d’actions qui, prises isolément, sont normales (ouvrir Visual Studio Code, naviguer dans la recherche Windows, écouter de la musique avec Spotify, consulter les paramètres du PC ou le logiciel Lenovo Vantage, lancer quelques processus « git » ou « conhost »). Cependant, le mode d’utilisation révèle plusieurs points inquiétants : * **Multiples changements de fenêtres très rapides** – le curseur passe d’un éditeur de code à la recherche Windows, puis à Spotify, puis à la boîte de dialogue « Rechercher », aux paramètres système, etc., en quelques secondes. Ce comportement s’apparente à une tentative de masquer ou de masquer rapidement des activités sensibles. * **Lancement répété de processus Spotify.exe** (au moins sept fois) et de « backgroundTaskHost.exe », ce qui peut indiquer que le lecteur a été ouvert de façon anormale, possiblement pour exploiter une faille ou pour faire tourner un script malveillant en arrière-plan. * **Appuis sur les touches de contrôle (Ctrl) et sur les combinaisons « Ctrl + C » (copier) et « Ctrl + V » (coller) juste avant la copie du contenu « print(output["json_path"]) ». Cette séquence ressemble à une tentative d’extraire ou de copier des données de code, éventuellement confidentielles, vers le presse-papier. * **L’ouverture du gestionnaire de paramètres puis le lancement de plusieurs exécutables « git.exe », « conhost.exe » et même « WpcTok.exe » (un composant de Windows Protect Connection) en même temps que le curseur se déplace vers le coin de l’écran. Ce type d’activité peut correspondre à l’exécution de scripts automatisés ou à la manipulation de dépôts de code sans que l’on voie

clairement ce qui est réellement fait. Ces comportements, surtout le mélange d’édition de code, la copie de lignes potentiellement sensibles et le lancement soudain de nombreux processus, sont typiques d’un **comportement de collecte ou d’exfiltration d’informations**. Le risque principal est que des morceaux de code, des chemins de fichiers ou d’autres données internes soient copiés et éventuellement transmis à un acteur extérieur, ce qui pourrait compromettre la confidentialité du projet ou ouvrir la porte à des attaques ultérieures (exécution de code malveillant, persistance sur le système, etc.). **Recommandations simples** 1. **Vérifier les comptes** : assurez-vous que le compte Windows « IPG3ALEX\alexi » est celui de l’utilisateur légitime et que ses mots de passe n’ont pas été compromis. 2. **Examiner les processus récents** : utilisez le Gestionnaire des tâches ou un outil de surveillance pour identifier les instances de Spotify, backgroundTaskHost, git et WpcTok qui ne sont pas liées à des activités normales. Fermez ou désinstallez celles qui sont inutiles. 3. **Limiter les droits d’accès** : restreignez les privilèges de l’utilisateur afin qu’il ne puisse pas lancer de programmes système ou de scripts sans supervision (ex. : exécuter Visual Studio Code en mode non administrateur). 4. **Activer la journalisation et l’alerte** : configurez un système de logs qui vous alerte lorsqu’un même processus est lancé plusieurs fois en peu de temps ou lorsqu’une copie de texte vers le presse-papier se produit dans un contexte de développement. 5. **Analyser les scripts** : passez en revue le fichier *tracking_activity.py* et tout autre script récemment modifié pour détecter d’éventuels appels à des serveurs externes ou à des fonctions de transmission de données. 6. **Mettre à jour et scanner** : assurez-vous que le système d’exploitation, les applications (Spotify, VS Code, Git) et l’antivirus sont à jour, puis lancez une analyse complète pour déceler d’éventuels logiciels indésirables. En suivant ces mesures, vous réduirez les chances que des informations internes soient compromises et vous limiterez la surface d’attaque du poste de travail.

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

Heure (UTC)	Action	Détails
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
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

Heure (UTC)	Action	Détails
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
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

Heure (UTC)	Action	Détails
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
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

Heure (UTC)	Action	Détails
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