別添資料

VS Codeを悪用した手口及び痕跡・検知策

2025年1月8日

警察庁

1 はじめに

(1) 背景

遅くとも2024年6月頃から、Microsoft社が開発及び提供しているコードエディタであるVisual Studio Code[1](以下、「VS Code」といいます。)の開発トンネル機能(Microsoft dev tunnels)[2]を、サイバー攻撃に悪用した手口が見られています。

この開発トンネル機能は本来、ソフトウェア開発者等が遠隔地からコンピュータに接続し、リモートでソフトウェアの開発を行ったり、コマンドでコンピュータを操作するために使用されます[3]。

(2) 目的

本資料では、類似手口を用いたサイバー攻撃の被害拡大防止及び被害の未然防止のための適切なセキュリティ対策を講じていただくことを目的として、VS Codeを悪用した手口及びその分析結果に基づく痕跡・検知策の一例を紹介いたします。

ただし、本資料は分析結果の一例であり、今後異なる手口が使われる可能性もあることなどから、本資料で紹介する痕跡・検知策に加えて、更なる検知策を取り入れる必要がある場合もあり得る点にご留意ください。

2-1 攻撃手口

① 標的型メールにより、被害者のパソコンをANELマルウェアに感染させます。

② VS Codeの開発トンネル機能（Microsoft dev tunnels）を使用するため、VS Code CLI（Command Line Interface）ツールをマルウェアの機能でダウンロードします。

③ VS Code CLIを起動する際に、開発トンネル機能を使用するオプションを指定します。このオプション指定によりVS Code Server[4]が起動します。VS Code Serverは開発トンネルを通じて外部からのコマンド等を受け取る役割を持ちます。

なお、VS Code Serverは、コンソール画面から起動しますが、他のソフトウェアと組み合わせることで、コンソール画面を表示せずに起動することができます。被害者が起動に気づかないようにコンソール画面を表示しない手法をとっていた事例を確認しています。

④ 攻撃者は、遠隔から開発トンネル[5]を通じて感染パソコンに接続し、PowerShellでのコマンド実行等を行っていたとみられます。

2-2 攻撃手口

概略図

攻撃者

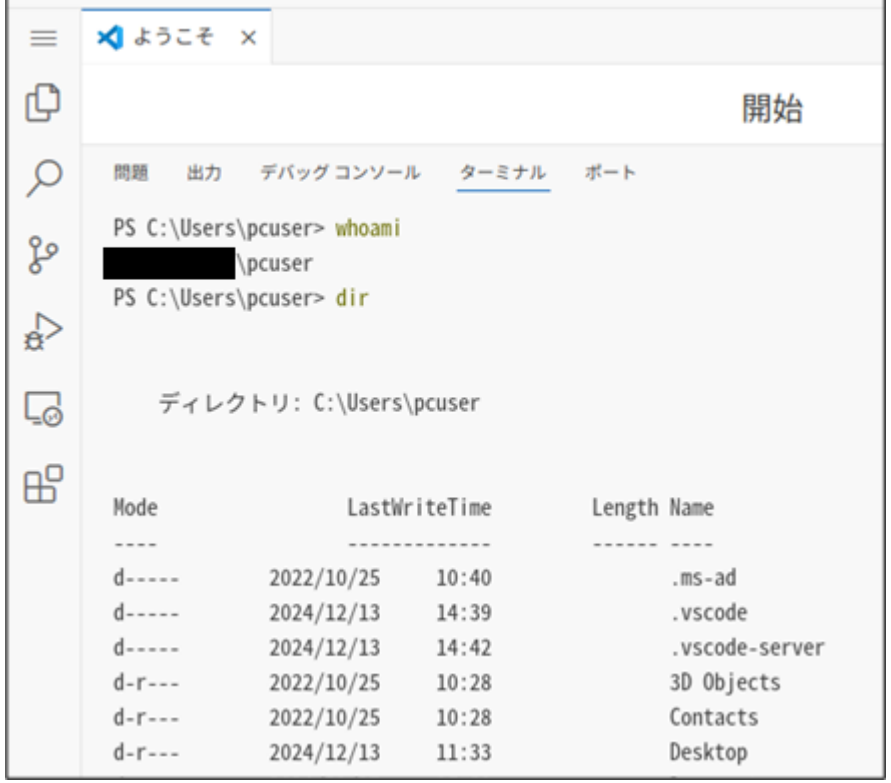
Webブラウザ、GitHubアカウント等を用いて、
外部から被害者パソコンに接続

vscode.dev 等
Visual Studio関連サーバー

④ VS Codeの開発トンネル機能を利用して、
コマンドを実行

開発トンネル
（通信先は3-5を参照）

感染パソコンでVS Codeを実行しているユーザとして
任意のコマンドを実行可能



CLIツール画面

① 標的型メール攻撃によりマルウェアに感染

感染パソコン

② VS Code CLI版をダウンロード

VS Code
CLI版

コンソール画面を表示
せずに遠隔操作をする
ことも可能。

③ VS Code 開発トンネル機能を起動

VS Code
Server

ターミナル
（PowerShell）

図1：概略図

3-1 痕跡・検知策

VS Codeを悪用した手口を分析したところ、特定のフォルダの作成やイベントログ等から痕跡を確認できる場合がありました。

これらの分析結果における例や気づきなどを以下に記載しますので、検知策を検討する際に参考としてください。

(1) フォルダ C:¥Users¥{ユーザ名}内に .vscode や .vscode-server フォルダが作成されている場合がありました(図2)。

また、これらのフォルダが隠し属性で作成されている場合がありました。

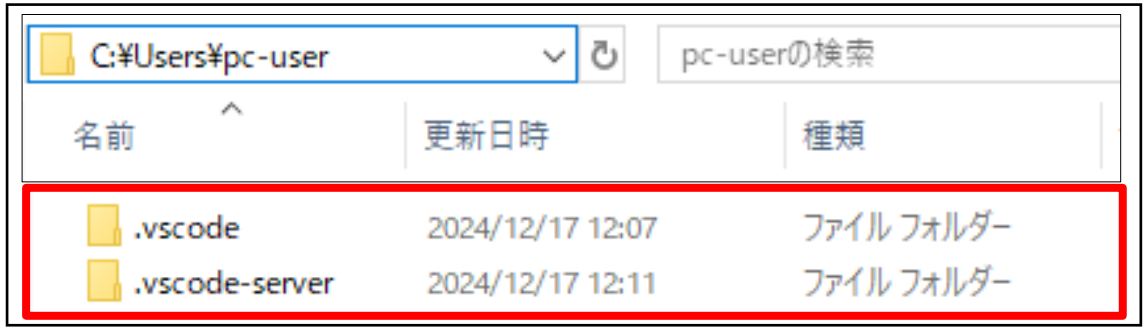


図2:フォルダの作成例

※ 上記スクリーンショットは、ユーザー名 pc-user を使用した検証環境によるもの。

3-2 痕跡・検知策

（2）イベントログ

○ イベントログ「Microsoft-Windows-Powershell/Operational」に、実行したPowerShellのコマンド履歴が残存している場合がありました。

○ イベントログ「Security」のイベントID「5379」において、項目TargetNameに「vscode-cli-0.vscode-cli」と記録されている場合がありました（図3）。

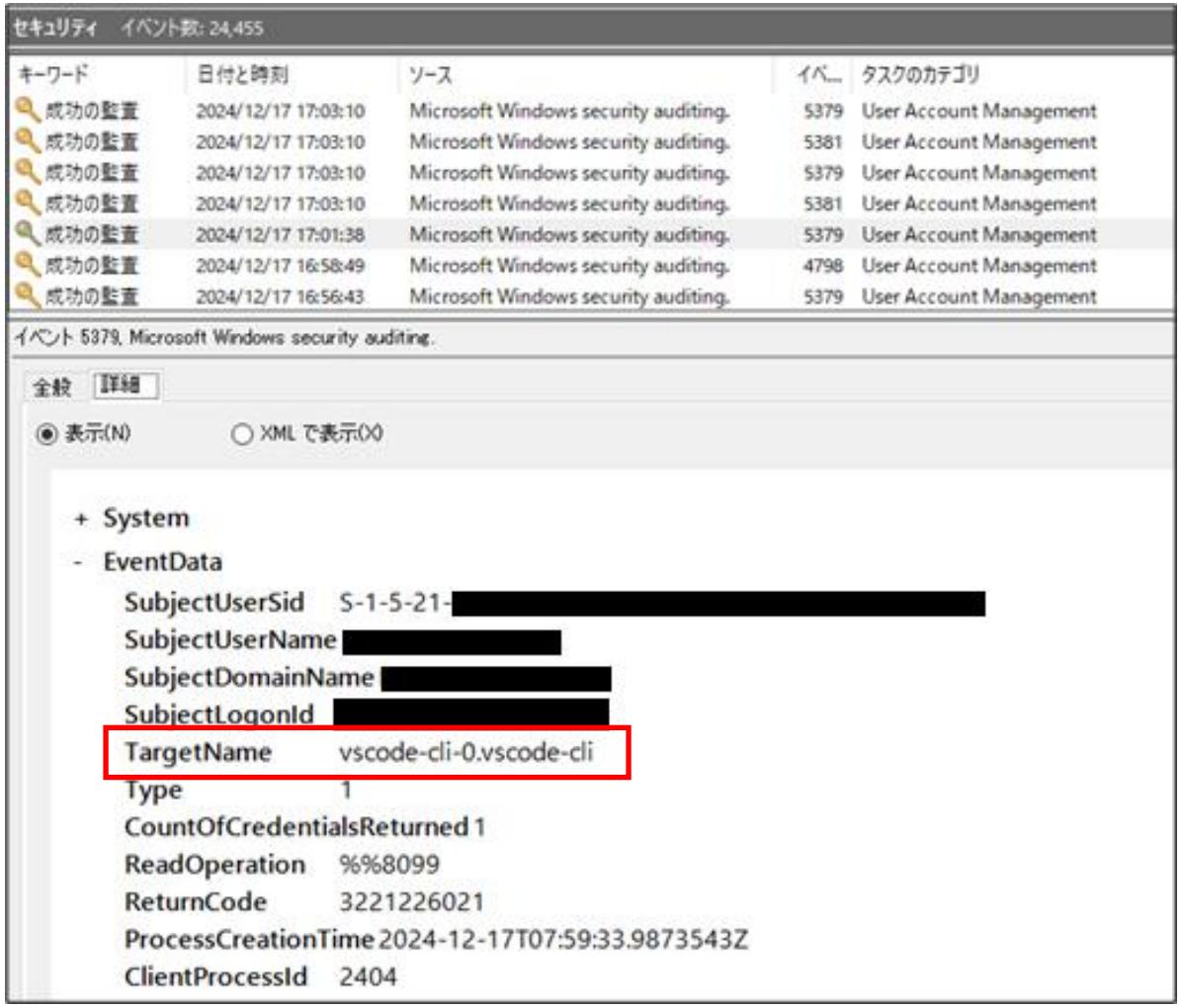


図3：イベントログ「Security」

3-3 痕跡・検知策

（3）コントロールパネル

Windows資格情報の汎用資格情報において、VS Code Serverの実行に伴い、文字列「インターネットまたはネットワークのアドレス：vscode-cli-0.vscode-cli」及び文字列「ユーザ名：vscode-cli-0」が記録された資格情報を確認できる場合がありました（図4）。

図4：コントロールパネル / ユーザーアカウント / 資格情報の管理 / Windows資格情報

3-4 痕跡・検知策

（4） ファイル名及びプロセス起動

VS Code Serverの実行に伴い、ファイル名がnode.exeであるファイルが起動した事例がありましたので、ファイル名やプロセス起動から検知できる可能性があります[6]。

node.exeは以下のパスで確認されています。

node.exeが保存されていたパス：

C:¥Users¥{ユーザー名}¥.vscode¥cli¥servers¥Stable-{40桁の16進数}¥server¥node.exe

また、開発トンネル機能からターミナルを起動した場合、node.exeの子プロセスとしてPowerShellがpwsh.exeという名称で起動したことを確認しました。

ただし、特定のファイル名による監視や確認を検知策とする場合には、ファイル名が変更される可能性も考慮してください。

3-5 痕跡・検知策

（5） 通信の確認

開発トンネルを作成する際の認証や、開発トンネルへのアクセス時に、表1に示すドメインへの通信が発生する可能性があります[7]。

これらのドメインへの業務時間外の通信や、VS Codeを使用しない部門からの通信が、ログ等において記録されている可能性があります。

他方、当該手口の対策としてgithub.com等への通信を遮断すると、通常業務に影響を与える可能性があります。

また、開発トンネルに関するドメインに含まれている[clusterID]の値の一覧は以下のURLで確認することができます。

`https://global.rel.tunnels.api.visualstudio.com/api/v1/clusters`

通信するタイミング	通信先ドメイン	
認証時	github.com	login.microsoftonline.com
開発トンネルへのアクセス時	global.rel.tunnels.api.visualstudio.com	[clusterId].rel.tunnels.api.visualstudio.com
	[clusterId]-data.rel.tunnels.api.visualstudio.com	*.[clusterId].devtunnels.ms
	*.devtunnels.ms	

表1：認証及び開発トンネルアクセス時の通信先ドメイン

4 参考文献

[1] https://code.visualstudio.com

[2] https://code.visualstudio.com/docs/remote/tunnels

[3] https://marketplace.visualstudio.com/items?itemName=ms-vscode.remote-server

[4] https://code.visualstudio.com/docs/remote/vscode-server

[5] https://learn.microsoft.com/ja-jp/azure/developer/dev-tunnels/overview

[6] https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_3_sasada_hazuru_en.pdf

[7] https://learn.microsoft.com/ja-jp/azure/developer/dev-tunnels/security#domains