令和８年９月１８日
警察庁
国家サイバー統括室

北朝鮮サイバー攻撃グループ「WaterPlum」によるIT技術者を標的としたサイバー攻撃並びに北朝鮮IT労働者の我が国、米国及び欧州における活動実態等について

警察庁は、国家サイバー統括室（NCO）、米国連邦捜査局（FBI）、米国国防総省サイバー犯罪センター（DC3）、豪州通信情報局（ASD）豪州サイバーセキュリティセンター（ACSC）、ドイツ連邦情報庁（BND）及びドイツ連邦憲法擁護庁（BfV）とともに、民間事業者からの情報提供や、警察庁関東管区警察局サイバー特別捜査部及び関係都道府県警察の捜査・分析により、北朝鮮を背景とするサイバー攻撃グループ「WaterPlum」（ウォータープラム）（関連名称： Contagious Interview）の攻撃手口や、北朝鮮IT労働者による外貨獲得活動及び採用応募活動の実態を明らかにしました。

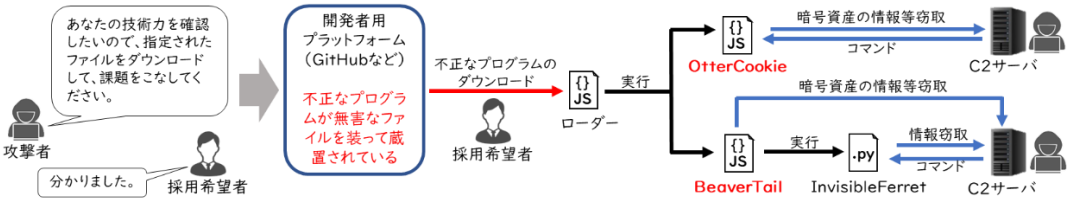
我が国のIT技術者の方や、クラウドソーシングを利用した業務発注・委託をされている事業者は、以下の手口例及び緩和策を参考に、適切なセキュリティ対策を講じていただきますようお願いします。

1 エグゼクティブ・サマリー

- WaterPlum は、IT 技術者に対し、サイバー攻撃を行っています。このサイバー攻撃グループは、警戒心の薄い求職者のコンピュータネットワークに密かに侵入し、機密情報の収集や暗号資産を盗み出すことを主な目的として、日本、米国、欧州及びその他の国々を標的としています。
- 警察庁と FBI は、WaterPlum と一部の北朝鮮 IT 労働者が、北朝鮮朝鮮労働党(WPK)中央委員会軍需工業部 313 総局の指揮下で運用されていると評価しています。WaterPlum はヘッドハンティングを装い、正規の人工知能(AI)企業、暗号資産企業、非代替性トークン(NFT)企業、あるいは人材紹介サービスになりすまして、世界中のソフトウェア開発者や IT 技術者を標的に、魅力的な求人情報を持ちかけます。
- WaterPlum は、我が国を含む 100 以上の国と地域において、3 万台以上とみられる端末に対しマルウェアを感染させ、7 千件以上の暗号資産ウォレット情報を窃取しています。また、WaterPlum が管理する暗号資産ウォレットに、少なくとも約 17 億円相当[1]の暗号資産が送金されていたことが判明しました。
- 我が国で初めて、国内の支援者(Domestic Enabler、ドメスティック・イネーブラー、以下単に「支援者」という。)による「ラップトップ・ファーム」(支援者の居宅内に設置された、北朝鮮 IT 労働者が遠隔操作する PC)を把握し、捜査及び解体しました。北朝鮮 IT 労働者は、関連捜査で判明した分を含め、暗号資産等、数億円相当を海外に送金していました。
- WaterPlum の一部メンバーは、日本や米国の企業で専門的な IT 業務やウェブシステム設計・開発の仕事に就くことに成功しており、得られた収益は北朝鮮の資金源となっています。
- 警察庁は、FBI、その他パートナーと協力を継続し、北朝鮮に利益をもたらすサイバー攻撃や、北朝鮮の IT 労働者による外貨獲得活動を明らかにし、対策を講じています。

2 WaterPlum による IT 技術者個人等を標的とするサイバー攻撃

(1) 代表的な攻撃手口



- WaterPlum は、Web 関係のフリーランサー等を含む IT 技術者に対し、暗号資産窃取を主な目的としたサイバー攻撃を行っています。
- 標的にされた IT 技術者の勤務先や、北朝鮮 IT 労働者に業務発注した企業内から、暗号資産や個人情報等の情報が窃取されたり、窃取された機微な情報を悪用・脅迫されたりする可能性があります。
- WaterPlum は、ソーシャルメディア、オンライン求人サイト、ギグワークプラットフォーム、フリーランスマーケットプレイスなどを通じて、世界中の求職者にアプローチします。採用活動の過程において、WaterPlum は求職者に対し、技術的なオンライン面接に参

[1] 約 1,071 万ドル(1 ドル 159 円で換算)

加するか、あるいは技術的なコーディング課題を完了させることを求めます。 面接やコーディング課題が行われる際、WaterPlum は求職者に対し、複数のオンライン共同開発プラットフォームやコードリポジトリに掲載されている不正なプログラムをダウンロードさせ、そのファイルを用いてオンラインビデオ会議プラットフォームの不具合を診断・修正するか、あるいは与えられたコーディング課題を完成させるよう指示します。

- WaterPlum は、悪意のある Node Package Manager[2]（NPM）パッケージをアップロードし、そこに BeaverTail[3]、InvisibleFerret[4]、OtterCookie[5]、OtterCandy[6]、StoatWaffle[7] といったマルウェアファミリー及びその亜種を埋め込みます。
- WaterPlum は、マルウェアローダーを介して被害者のコンピュータネットワークにバックドアを設置した後、リモートアクセスツール（RAT）を用いて、接続性および被害システムへの横展開経路を維持します。また、情報窃取ツール（Infostealer）で被害者の機密データや暗号資産を流出させ、第三者のコマンド＆コントロール（C2）IP アドレスへ送信し、感染端末やネットワーク、データストレージの遠隔管理を行います。
- WaterPlum の一部メンバーは、北朝鮮 IT 労働者として企業の Web システムに関する画面設計、開発に関する業務を行っています。彼らは、オンラインチャットプラットフォームを利用して日本や米国の開発者と通信することがあります。同グループは日本・米国・その他諸国に拠点を持つ国際的な支援者（イネーブラー）を活用し、ラップトップ・ファームの設置・管理を実施させています。これらの支援者は、WaterPlum が利用するための仮想プライベートサーバー（VPS） の作成・管理も実施しており、WaterPlum が実際の作業場所を隠蔽しつつ委託 IT 業務を遂行し、収益を上げることを手助けしています。
- WaterPlum は、被害者の端末から窃取した認証情報を用いて、被害者を雇用している組織のコンピュータネットワークに侵入し、スパイ活動や知的財産の盗難、企業環境内へのさらなる横展開を可能とします。また、盗まれた身分証画像は、北朝鮮 IT 労働者が外貨獲得のために被害者になりすますことにも利用され得ます。その他に標的となる機微なデータは以下のとおりです。
  - ウェブブラウザに保存された認証情報（ID、パスワード等）

---

[2] NPM は JavaScript ランタイム環境 Node.js のデフォルトパッケージマネージャで、主にソフトウェア開発者がサードパーティのコードライブラリをインストール、共有、管理するために使用されます。

[3] BeaverTail マルウェアは、NPM パッケージ内部や GitHub や Bitbucket などのリポジトリから隠されてダウンロードされる JavaScript ベースのマルウェアです。

[4] InvisibleFerret マルウェアは、被害者のコンピュータネットワークへのアクセスを可能にする Python ベースのバックドアです。

[5] OtterCookie マルウェアは、JavaScript ベースのリモートアクセス型トロイ（RAT）であり、情報窃取機能も備えたマルウェアです。

[6] OtterCandy マルウェアは、OtterCookie と RATatouille の機能を組み合わせたものです。

[7] StoatWaffle はモジュラー構造の Node.js マルウェアファミリーで、マルウェアローダー、認証情報収集コンポーネント、永続性と被害者システムへの横展開を実現する RAT を組み合わせており、悪意ある Microsoft Visual Studio Code（VS Code）プロジェクトを通じて配布されます。このマルウェアはブロックチェーンをテーマにしたプロジェクトリポジトリをデコイとして利用し、フォルダが開かれかつ被害者に信頼されたときに自動実行コードをトリガーする悪質な VS Code 設定ファイルを埋め込んでいます。

- クリップボードの情報、キー入力の記録（キー入力ログ）及びスクリーンショット
- 暗号資産ウォレットのデータ（秘密鍵、シードフレーズ等）
- PC や共有フォルダ内にある、アクターが関心を持つファイルやデータ（運転免許証、パスポート等の身分証画像）

（2） 警察庁で把握した被害と影響

- 2025 年 12 月頃から 2026 年 7 月にかけて、少なくとも、我が国を含む 100 以上の国と地域で、3 万台以上とみられる PC がマルウェアに感染していました。
- 主な標的は、Web 関係のデザイナーやエンジニアのほか、暗号資産やブロックチェーン、Web3 と呼ばれる分野の技術者とみられます。
- WaterPlum によるマルウェア感染では、7 千件以上の暗号資産ウォレット情報の窃取が判明しました。
- WaterPlum が管理する暗号資産ウォレットに、少なくとも約 17 億円相当の暗号資産が送金されていたことが判明しました。

（3） 対策・緩和策

- 業務で使用する PC や暗号資産・個人情報を扱う PC で、むやみに第三者が関与したコードを実行せず、仮想マシン等のサンドボックス内でコードを実行してください。また、コード実行前に、難読化されている部分がないか、一見して動作を理解できない内容が含まれていないかを確認してください。
- 指示に従ってウィンドウ内に貼り付けたコマンド（スクリプト）に、以下のような文字列が含まれる場合は、特に注意が必要です。事前に、実行した際の動作を想定・理解できる場合を除き、実行しないでください。

curl	base64	-enc	mshta
Invoke-WebRequest -uri		iwr -uri	hidden

- ウイルス対策ソフトが検知した場合や、感染が疑われる場合は、速やかに Wi-Fi の切断や LAN ケーブルを抜く等、外部との通信を遮断してください。
- ウイルス対策ソフトが検知・駆除したからといって安心しないでください。検知前に暗号資産を含む情報が既に窃取された可能性を考慮し、速やかに別の PC 等から新たなウォレットを作成し、すべての資産を送金して待避させてください。また、新たなウォレットのシードフレーズは印刷や紙に書き写すなどして、PC 内に保管しないことを推奨します。
- さらに、ウイルス対策ソフトで検知できていない別のマルウェアが潜伏している可能性がありますので、必要なデータのバックアップを取得したうえで、PC の初期化（再セットアップ）を推奨します。
- EDR と呼ばれるソフトウェア等を活用し PC の挙動を監視することで、侵害挙動の早期発見やマルウェア感染を抑止することが可能です。
- 採用応募活動などで、自身が関与していない VSCode のプロジェクトを開くよう依頼された場合は、必ず「制限モード」で開くことを心がけてください。
  - プロジェクトを開いた際に「このフォルダ内のファイルの作成者を信頼しますか？」と警告メッセージが表示されるので、「いいえ」を選ぶと制限モードで開くことができます。

- 制限モードで開くことで、手口例に記載した .vscode/tasks.json 内に記述された処理を実行させないことができます。
- VSCodeの制限モード又は別のエディタ等で .vscode/tasks.json ファイルを開き、何らかのファイルをダウンロード・実行させるようなコードが書かれていないか確認してください。

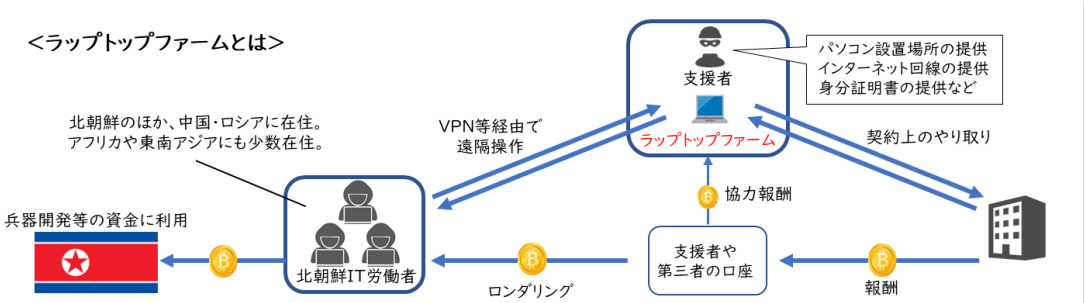
- ただし、条件や設定によってはVSCodeの警告が表示されない場合があるため、以下のことに注意してください。
  - 開くように依頼されたプロジェクトを、過去に「信頼する」と設定したフォルダ内で開かない。(自身のプロジェクト内に、依頼されたプロジェクトを配置しない。)
  - 設定 security.workspace.trust.enabled で、「ワークスペースの信頼を有効にする制御」を無効にしない(チェックボックスを OFF にしない)。

(4) WaterPlum メンバーの活動実態(参考)

- 「Magicam」といった、AI による顔画像交換ソフトを使用しオンライン面接を行っていましたが、数分だけ利用し、その後はネットワークの状態を口実に映像を無効にするよう、仲間内で助言していました。
- ある北朝鮮の記念日に、一定時間ゲーム(主にシミュレーションゲーム)を行ってもよいと指示が出されていました。また、サッカー動画を視聴している状況もみられました。
- 「NaturalReader」のような音声読み上げソフトを使い、日本語の発音を勉強していました。
- 機械翻訳や生成 AI は無料サービスや無料プランを多用していました。

3 北朝鮮 IT 労働者によるラップトップ・ファームを使った外貨獲得活動など

(1) 活動の概要



- 北朝鮮 IT 労働者は、我が国に居住する支援者から提供を受けた身分証明書画像を悪用し、支援者になりすまして業務を受注していたほか、支援者が受注した業務を請け負って報酬を得たり、支援者の銀行口座を報酬の振込先として指定し、支援者から報酬を送金してもらったりしています。
- 北朝鮮 IT 労働者は、関連捜査で判明した分を含め、暗号資産等、数億円相当を海外へ送金しています。
- これらの活動は、北朝鮮 IT 労働者が支援者宅に遠隔操作用 PC を設置させる、いわゆるラップトップ・ファームと呼ばれる手口のほか、支援者が借りた VPS を使用することで、居場所や作業場所を偽装して行われています。
- 北朝鮮 IT 労働者は、ラップトップ・ファームや VPS を使い、国内外のクラウドソーシング・サービスにおいて、オンライン上で業務を受注し、実際に受注した業務を行っていま

した。作業を行う北朝鮮人は北朝鮮国内に居住するほか、中国やロシアに拠点を持ち、少数はアフリカや東南アジアにも居住しています。

- 北朝鮮 IT 労働者に対して業務を発注し報酬を支払った場合、または外貨獲得の幇助行為を行った場合、国内法令や対北朝鮮制裁の違反行為に問われるおそれがあります。

（2）警察庁で把握した被害と影響

- 北朝鮮 IT 労働者は、主に外貨獲得を目的としていますが、併せて悪質なサイバー活動が行われるケースもあります。北朝鮮 IT 労働者と知らずに、プログラム開発業務の一部を外注した企業が、受注していた北朝鮮 IT 労働者との間で報酬の支払に関するトラブルが生じた際、北朝鮮 IT 労働者が、自身の担当していたプログラムのソースコードをインターネットに公開した事例がありました。
- 北朝鮮 IT 労働者が作成に関わった Web サイトにおいて、後に Web サイトが改ざんされ、正常に表示されなくなる事例がありました。

（3）北朝鮮 IT 労働者に協力しないための対策

- 自宅に第三者が遠隔操作可能な PC をむやみに設置しないでください。北朝鮮 IT 労働者が、身分を偽って、「海外からだと制約があって仕事がしにくい」等と言って設置を依頼してきたり、いわゆるブローカーが北朝鮮 IT 労働者との関係性や事情を説明せずに依頼してきたりするケースが考えられます。
- 取引相手や関係者が北朝鮮 IT 労働者である可能性を把握したら、速やかに警察へご相談ください。北朝鮮の者と知って報酬を支払ったり、身分証明書（画像を含む）を提供したりすると、犯罪に加担する可能性があります。
- 業務を発注・委託する際は、受注先企業の提携先や再委託先等に北朝鮮 IT 労働者が関与している可能性を考慮し、外注・再委託に関する禁止条項や契約内容を明確にすることで、北朝鮮の外貨獲得活動に加担するリスクを低減するようにしてください。
- 北朝鮮 IT 労働者に外注すると、「3（2） 警察庁で把握した被害と影響」で記載したような、顧客（発注元）にも影響が及ぶ被害が発生する可能性があるほか、北朝鮮 IT 労働者が自らに割り当てられた認証情報を悪用して発注元から機微情報を窃取したり、業務上のやり取りを通じてマルウェア感染を図ったりする可能性もありますので、以下の点に注意してください。
  - 面接時は、後述する国内企業への採用応募活動に関する「4（2） 対策・緩和策」を参考に、北朝鮮 IT 労働者とみられる者の採用を防止するようにしてください。
  - また、北朝鮮 IT 労働者か否かに関わらず、外注先に提供する情報（ソースコード、認証情報等）やアクセス許可範囲は、必要最小限かつ最小権限とするほか、万が一、外注先が北朝鮮 IT 労働者とみられる者や、悪意を持つ者である可能性を把握した際は、速やかにアカウントやセッションの無効化を行ってください。

4 北朝鮮 IT 労働者による国内暗号資産取引所への採用応募活動

（1）北朝鮮 IT 労働者による採用応募の実例

- 2025 年 5 月、日本の暗号資産取引事業者「bitFlyer」（ビットフライヤー）社のエンジニア職への採用応募がありました。
- 応募者は北朝鮮 IT 労働者とみられ、同社の採用フォームに別人になりすました履歴書

を添付し、仲介事業者を介さず直接応募していました。なお、連絡先メールアドレスにはGmail が使用されていました。

- 応募者は採用フォームのアクセス時に VPN（NETNUT Proxy、Astrill VPN、High Speed Rabbit Proxy）を使用していました。
- 職務経歴書は、応募者に以下のような共通の特徴がありました。
  - 保持スキルが多種多様で、プログラミング言語、暗号資産を含むブロックチェーン、クラウドサービス等に関する、それぞれ 10 種類以上の豊富な知見と経験
  - 欧州の大学を卒業した後、欧州やアジアなど世界各地の都市での職歴
- 同社は、応募者が北朝鮮 IT 労働者である可能性を考慮したうえで、オンライン面接を実施したところ、応募者は、見た目がアジア系の印象であり、マレーシア出身でフィンランド在住と説明し、採用面接では母国語をマレー語及び中国語であると答えていました。
- 面接中は英語でのやりとりでしたが、英会話レベルは学歴・職歴と比較すると高いとは言えませんでした。また、職務経歴書に記載されたスキルに応じた質問に対しては、簡単な質問には答えられるものの、抽象的な回答に終始したり、回答をごまかしたりするような場面も見られました。
- その他、面接中には以下のような特徴がみられました。
  - 日本への引っ越し（出社）を拒否するか、「半年先なら」と回答する。
  - 暗号資産での給与支払いに固執する。
  - しきりに別モニターを確認し、画面内容を読み上げているような様子がある。
  - 時折、背後で他人の話し声が聞こえる。
  - 映像が途切れる、コマ送りになる。

  なお、同社は応募者の不審点に気づき適切に対応したため、採用や被害には至っていません。

（2） 対策・緩和策

- 普段応募が少ない職種に対して、短期間で多数の応募があった場合は特に注意が必要です。応募フォームで確認できる場合は、Whois 等によってアクセス元 IP アドレスと応募者の居住地が合致するか確認することを推奨します。なお、北朝鮮 IT 労働者は、VPN を多用しているとみられますので、注意が必要です。
- 連絡先に電話番号が記載されている場合、電話をかけてもつながらないか使われていない場合があります。連絡先の確認を徹底してください。
- 職務経歴書に記載されたスキルについて、面接の場で具体的に説明を求めてください。応募してきた人物は一人に見えても、実際は複数の者が関与・連携しているため、メール等でやりとりすると、多くのスキルを持っているかのように感じる場合があります。また、資格については認定番号を確認するほか、保持資格に矛盾が疑われる場合も、面接時に詳しく説明を求めてください。（例えば、資格取得や取得間隔に一定期間が必要となるものがあります。）
- 応募者の出身地、天候、趣味など個人的な情報を質問することで、なりすましを露呈させることができます。
- 北朝鮮 IT 労働者は、リモートワークや暗号資産による報酬支払いに固執する傾向があります。また、海外の本人名義以外の口座に送金させようとする傾向もありますので、応募者や取引先がこれらの傾向を示した場合は特に注意してください。

5 WaterPlum 及び北朝鮮 IT 労働者の関連性

- 警察庁と FBI は、WaterPlum によるサイバー攻撃と北朝鮮 IT 労働者による一部の外貨獲得活動は、どちらも朝鮮労働党中央委員会軍需工業部 313 総局が中心的な役割を果たしていると評価しています。
- WaterPlum の攻撃者が利用していた IP アドレスと、北朝鮮 IT 労働者が「ラップトップ・ファーム」やクラウドソーシング・サービスへ接続する際に利用していた IP アドレス、さらに国内暗号資産取引所（bitFlyer）の採用へ応募した北朝鮮 IT 労働者が利用していた IP アドレスが合致しました。

6 最後に

- この注意喚起に記載した手口は一例であり、今後も手法が変化・巧妙化する可能性がありますので、国内外のセキュリティ専門機関による注意喚起や、セキュリティベンダーが公表するレポートに関心を持つようにしてください。

7 謝辞

本注意喚起のリリースに際し、ご協力をいただきました。
- NTT セキュリティ・ジャパン株式会社
- 株式会社 bitFlyer

8 参考情報（リンク）

- 北朝鮮 IT 労働者に関する各国・企業等に対する注意喚起（警察庁等）
  https://www.npa.go.jp/bureau/security/northkorea_IT/NK_IT_202607.html
- Fact Sheet: Democratic People's Republic of Korea（北朝鮮）情報技術労働者に関するガイダンス（2022 年 5 月 16 日）
  https://ofac.treasury.gov/media/923131/download?inline
- Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers（2023 年 10 月 18 日）
  https://www.ic3.gov/PSA/2023/PSA231018
- North Korean IT Workers Conducting Data Extortion（2025 年 1 月 23 日）
  https://www.ic3.gov/PSA/2025/PSA250123
- Private Sector Security Advisory 02/24: North Korean IT Workers（2024年10月1日）
  https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/economic-and-scientific-protection/2024-10-01-security-advisory.html

以上