令 和 7 年 1 月 8 日
警　　察　　庁
内閣サイバーセキュリティセンター

MirrorFace によるサイバー攻撃について（注意喚起）

警察庁及び内閣サイバーセキュリティセンターでは、2019 年頃から現在に至るまで、日本国内の組織、事業者及び個人に対する、以下のサイバー攻撃キャンペーンが、「MirrorFace」（ミラーフェイス）（別名、「Earth Kasha」（アース カシャ））と呼ばれるサイバー攻撃グループによって実行されたと評価しています。

1 2019 年から 2023 年にかけて、主に我が国のシンクタンク、政府（退職者含む）、政治家、マスコミに関係する個人や組織に対し、不正なプログラム（マルウェア）を添付したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されました。（以下「攻撃キャンペーンA」とします。）
2 2023 年頃から、インターネットに接続されたネットワーク機器に対し、ソフトウェアのぜい弱性を悪用して標的ネットワーク内に侵入するサイバー攻撃が確認されました。主な標的は我が国の半導体、製造、情報通信、学術、航空宇宙の各分野でした。（以下「攻撃キャンペーンB」とします。）
3 2024 年6月頃から、主に我が国の学術、シンクタンク、政治家、マスコミに関係する個人や組織に対して、マルウェアをダウンロードするリンクを記載したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されています。（以下「攻撃キャンペーンC」とします。）

攻撃キャンペーンA及びCは、いずれも標的型メール攻撃ですが、使用されるマルウェアや感染手法は異なります。攻撃キャンペーンAでは LODEINFO と呼ばれるマルウェアが使用され、主に添付ファイルの開封を感染の起点としていましたが、攻撃キャンペーンCでは ANEL と呼ばれるマルウェアが使用され、主にメール本文のリンク先を感染の起点としていたことを確認しています。また、侵入後、各キャンペーンを通じて確認されていた Windows Sandbox の悪用だけでなく、キャンペーン C では Visual Studio Code (VS Code) を悪用する手口も確認しています。

警察庁サイバー特別捜査部及び警視庁ほか道府県警察による捜査等で判明した、攻撃対象、手口、攻撃インフラ等を分析した結果、MirrorFace による攻撃キャンペーンは、主に我が国の安全保障や先端技術に係る情報窃取を目的とした、中国の関与が疑われる組織的なサイバー攻撃活動であると評価しています。

この注意喚起は、MirrorFace によるサイバー攻撃の手口を公表することで、標的となる組織、事業者及び個人に、直面するサイバー空間の脅威を認識いただくとともに、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おります。あわせて、機器の不審な動きやネットワークの不審な通信を検知した際には、速やかに所管省庁、警察、内閣サイバーセキュリティセンター、セキュリティ関係機関等に情報提供いただきますようお願いします。

なお、MirrorFace の手口、検知策、緩和策は、以下のとおりです。

【手口、検知策、緩和策】

1　侵入手口

(1) 攻撃キャンペーン A

- 2019 年 12 月頃から 2023 年 7 月頃にかけて把握した、標的となる受信者に対して、マルウェアを含むファイルを添付したメールを送付して受信者が添付ファイルを開くことにより、マルウェアに感染させる手口です。なお、この攻撃キャンペーンによる感染が原因とみられる侵害活動が、2024 年 5 月頃まで継続していた事例を把握しています。
- 標的となった対象は、主に我が国のシンクタンク、政府（退職者含む）、政治家、マスコミに関係する個人や組織です。
- 送信元メールアドレスは、Gmail や Microsoft Outlook メールアドレスの使用や、第三者の正規アドレスの悪用（認証情報を窃取し、本人になりすまして送付）した事例を把握しています。
- 送信者名は、受信者が所属する（又は所属していた）組織の元幹部や、受信者が関心のある専門分野の有識者を詐称した事例を多く把握しています。
- メールの件名は、全体的に送付時期の安全保障情勢や国際情勢に関連したものが多く、一例として、「日米同盟」、「台湾海峡」、「ロシア・ウクライナ戦争」、「自由で開かれたインド太平洋」といったキーワードを含むもの、「勉強会案内」、「会合資料」、「委員会名簿」といった受信者の関心を引くもの、送信者（受信者と交流のある人物を詐称）の氏名や名字で「●●●●です。」といったものなど、様々な事例を把握しています。
- また、最初からファイルを添付して送付せず、受信者が興味を引く資料の提供を申し出て、メールのやりとりの中でファイルを添付した事例、受信先組織が主催するセミナーの申込不備を指摘したメールのやりとりでファイルを添付し、受信者が添付ファイルを開くように誘導した事例もありました。
- 添付ファイルは、Microsoft Word や Microsoft Excel のほか、VHD ファイル（仮想ハードディスクイメージ）や ISO ファイル（光学ディスクイメージ）を使った事例を把握しており、多くは、Microsoft Office ファイルのマクロを有効化することによって、LODEINFO と呼ばれるマルウェアに感染します。
- その後、LilimRAT や NOOPDOOR と呼ばれる別のマルウェアに感染させた事例や、Windows Sandbox を悪用したマルウェア実行事例を把握しています。

(2) 攻撃キャンペーン B

- 2023 年 2 月頃から 10 月頃にかけて、VPN 機器（クラウド向け仮想アプライアンスを含む）の脆弱性や、何らかの手段で得た認証情報（クライアント証明書を含む）の悪用により侵入されたとみられる事例のほか、外部公開サーバの SQL インジェクションの脆弱性を悪用したとみられる事例を把握しています。なお、この攻撃キャンペーンによる侵入が原因とみられる侵害活動が、2024 年 1 月頃や 6 月頃まで継続していた事例を把握しています。
- 標的となったのは、主に我が国の半導体、製造、情報通信、学術、航空宇宙の各分野です。
- 侵入後の VPN 機器に、Neo-reGeorg トンネリングツールや、オープンソースの WebShell が設置された事例を把握しています。
- 侵入後、Active Directory サーバ（以下「AD サーバ」とします。）への侵害、Microsoft 365 への不正アクセス、仮想化サーバへの不正アクセス及び仮想マシンイメージの取得事例を

把握しています。

- また、コンピュータを Cobalt Strike BEACON、LODEINFO、NOOPDOOR と呼ばれるマルウェアに感染させた事例を把握しています。

(3) 攻撃キャンペーン C

- 2024 年 6 月頃から、標的となる受信者に対して、ファイルをダウンロードさせるリンクが記載されたメールを送付し、受信者がダウンロードした Zip ファイルを展開後に、Microsoft Office 文書を開いてマクロを有効化すること、また、Microsoft Office 文書に偽装されたリンクファイル(拡張子が lnk)を開くことにより、ANEL と呼ばれるマルウェアに感染させる手口を把握しています。
- 標的となったのは、主に我が国の学術、シンクタンク、政治家、メディアに関係する個人や組織です。
- 送信元メールアドレスは、Gmail や Microsoft Outlook メールアドレスの使用や、第三者の正規アドレスの悪用(認証情報を窃取し、本人になりすまして送付)を把握しています。
- 送信者名は、マスコミ関係者、受信者が関心のある専門分野の有識者を詐称した者、悪用した正規アドレスの使用者名で送付した事例を把握しています。
- メールの件名は、「取材のご依頼」、「所蔵資料のおすすめ」、「国際情勢と日本外交」といったキーワードを含む事例を把握しています。
- メールの本文は、詐称された送信者が過去に第三者とやりとりしていたメールを何らかの手段で窃取し、一部だけ改変して送付しているとみられるため、違和感がありません。
- また、NOOPDOOR と呼ばれるマルウェアに感染させた事例や、Windows Sandbox を悪用したマルウェア実行、Microsoft 社が提供する Visual Studio Code (VS Code) の開発トンネル機能 (Microsoft dev tunnels)を遠隔操作ツールとして悪用した事例を把握しています。

2 悪用されたとみられるネットワーク機器の脆弱性

(1) Array Networks Array AG 及び vxAG

- CVE-2023-28461

(2) Fortinet 社 FortiOS 及び FortiProxy

- CVE-2023-27997

(3) Citrix ADC 及び Citrix Gateway

- CVE-2023-3519

3 Windows Sandbox の悪用

Windows Sandbox とは、Windows 10 Pro 若しくは Enterprise バージョン 1903 以降、又は Windows 11(Windows Home エディションを除く)に標準で含まれているソフトウェアで、実行する PC(ホストコンピュータ)とは別に実行される、一時的な仮想化された Windows デスクトップ環境です。

通常は、ホストコンピュータから隔離された環境を一時的に利用するためのものですが、攻撃者は、Windows Sandbox の起動設定を悪用し、永続的かつ密かにホストコンピュータ内に保存したマルウェアを Windows Sandbox 内で実行し、C2 サーバ(攻撃者の命令に基づいて動作する、マルウェアに感染したコンピュータに指令を送り、制御の中心となるサーバのこと)と通信させていました。

この手口は、遅くとも 2023 年6月頃から使用していたとみられます。この手口では、ホストコンピュータ上のウイルス対策ソフトや EDR 等による監視の目を逃れてマルウェアを実行可能で、ホストコンピュータをシャットダウン又は再起動すると、Windows Sandbox 内の痕跡が消去されるため、証跡の

調査が困難です。
Windows Sandbox を悪用した手口、痕跡、検知策については、別添資料【Windows Sandbox を悪用した手口及び痕跡・検知策】を参照してください。

4 Visual Studio Code (VS Code) の悪用

Visual Studio Code (VS Code) とは、プログラム開発で利用されることが多い、コードエディタと呼ばれるソフトウェアです。Microsoft 社が無償で提供しており、プラグインなどの豊富な拡張機能も利用可能です。

攻撃者は、侵入先 PC へ密かに CLI ツール(コマンドライン・インターフェイス版)の VS Code をダウンロード及びインストールし、同ソフトウェアの開発トンネル機能 (Microsoft dev tunnels) を使用することで、遠隔からのコマンド実行を可能にします。

同開発トンネル機能 (Microsoft dev tunnels) が使用する通信先との不審な通信が発生していないか監視・確認してください。

VS Code を悪用した手口、痕跡、検知策については、別添資料【VS Code を悪用した手口及び痕跡・検知策】を参照してください。

5 検知と緩和策

(1) 標的型メール (受信者向け)

○ 普段からの交流相手であってもメールアドレスに注意

送信者が所属する組織のメールアドレスや、過去にやりとりした実績のあるメールアドレスから受信したメールであっても、普段と少しでも異なる状況や違和感があれば、添付ファイルを開いたり、リンクをクリックしたりせず、送信者に確認してください。

例えば、普段は Microsoft Office ファイルをそのまま添付するやりとりが多いのに、パスワード付き Zip ファイルが届く場合、拡張子が VHD や ISO といった日頃のやりとりでは見かけない形式のファイルが届く場合や、Google Drive や OneDrive 等のリンクからファイルをダウンロードさせようとする場合は、不審と判断して送信者や所属組織のシステム管理者などに確認・相談してください。

もし、不審な添付ファイルを開いてしまった場合や、ウイルス対策ソフトが検知した場合は、直ちにシステム管理者に連絡・相談してください。

○ 安易に「コンテンツの有効化」をクリックしない

添付ファイルやダウンロードしたファイルを開いた際に、Microsoft Office ファイルのマクロ「コンテンツの有効化」ボタンをクリックさせるよう誘導される場合がありますが、安易にクリックしないでください。マクロとは、自動的に様々な処理を行うことが可能な便利な機能ですが、受信したファイル内容(論文、申込書、案内など)の表示・閲覧にマクロのような高度な機能が真に必要か検討し、不審と感じたらファイルの提供元に確認してください。

(2) 全般 (システム管理者向け)

○ 広範囲かつ長期間にわたるログの集中保存・管理

ログは、侵害の原因と範囲の把握に必要不可欠な情報源です。侵害の原因と範囲が分からなければ、封じ込めや根本的な対策がとれず、内部に脅威が残存するリスクが高まります。また、攻撃者は、侵入先のサーバや機器のログを消去する可能性がありますので、ログは、可能な限り別のサーバへ集約して保存するようにしてください。

ログを集約・分析する仕組みは「SIEM（Security Information and Event Management）」と呼ばれています。中小規模組織で予算に限りがある場合は、米 CISA が提供する「Logging Made Easy（LME）」ツールの構築・利用も可能です。

(3) VPN 等のネットワーク機器 （システム管理者向け）

○ ログの監視・確認

例えば、職員が国内居住者だけなのに、海外からのログイン履歴がないかといった観点や、通常と UserAgent が異なるログイン履歴がないかといった観点など、「普段と違う、違和感のある」ログがないかという観点でログの監視・確認を行ってください。

○ ログ設定の確認

VPN 機器のログにおいて、VPN アクセス元 IP アドレスにループバックアドレス（127.0.0.2 など）が記録されている事例がありました。不審・不正な VPN 接続がないか確認するため、適切にアクセス元 IP アドレスが記録されるように設定をしてください。

○ アカウントの管理

管理者用及び保守用アカウントについては、アクセス元 IP アドレスを制限し、事前・事後の使用申請・報告とアクセスログの差異がないか監視・確認してください。

また、長期間放置された（ログイン実績の無い）アカウントがないか定期的に確認するとともに、不要なユーザアカウントはロックするか、長く複雑なパスワードを設定し、アクセス試行がないか監視してください。

○ 内部ネットワークに向けた不審な活動の監視

VPN 機器を送信元とする内部ネットワークでの不審な活動（AD サーバやファイルサーバへのアクセスなど）がないか監視・確認してください。

VPN 機器に設置されたトンネルやバックドアを経由した通信は、機器の LAN 側 IP アドレスが送信元になる可能性があります。製品や設定によっては、VPN ユーザ個別に IP アドレスを割り当てずに、機器の LAN 側 IP アドレスが送信元になる可能性がありますので、設定や仕様を確認して、監視に活用可能か検討してください。

○ 脆弱性に関する情報収集と適切な対応

警察庁や都道府県警察のほか、IPA や JPCERT/CC による注意喚起、米 CISA の KEV カタログなどの情報源を活用し、ネットワーク機器の脆弱性に関する情報収集を行うようにしてください。

セキュリティベンダーのレポートや、公的機関の注意喚起等で、特に国家を背景とする標的型サイバー攻撃で悪用された可能性があると指摘されている脆弱性を持つ機器を利用している場合、実害を把握できていなくても、ネットワーク機器へのバックドア設置や、検知できていないサーバ・PC へのマルウェア感染が発生している可能性がありますので、パッチの適用やファームウェアの更新を行いつつ、念のため前述したようなログの確認を行い、内部への侵入・侵害が発生していないか確認してください。

なお、一度でも侵害されてしまった機器は、パッチの適用やファームウェアの更新を行ったとしても、バックドアが削除されない場合や、何らかの脆弱性が残る場合がありますので、機器を交換してください。

(4) Windows の設定・監視 （管理者向け）

○ 業務に必要の無い機能やソフトウェアの有効・使用状況の確認

業務上使用することがなければ、Windows Sandbox の機能を無効にすることを検討してください。また、無効にした場合は、不自然に有効化されていないか確認してください。

意図せずに VS Code がインストールされていないか、もしくは動作していないかを確認してください。また、開発トンネル機能 （Microsoft dev tunnels） が使用する通信先との不審な通信が発生していないか監視・確認してください。（別添資料【VS Code を悪用した手口及び痕跡・検知策】を参照。）

○ ウイルス対策ソフトの検知状況の監視・確認

ウイルス対策ソフトが何らかのマルウェアを検知した場合、検知した場所（機器、フォルダ）や、検知名などが、重大性を判断する目安となる場合があります。例えば「C:¥Windows¥System32」フォルダで検知した場合や、検知名を Web 検索した結果、セキュリティベンダーによって国家背景のサイバー攻撃グループが使うマルウェアとして報告されていた場合などは、深刻な情報窃取が継続していた可能性があります。

また、ウイルス対策ソフトがマルウェアを検知して駆除したからといって、安全な状態になったとは限りません。検知できていないマルウェアがどこかに潜伏している可能性があります。

調査においては、検知したサーバや PC を起点に、侵入経路や原因、侵害範囲を特定するため、様々なログを統合して時系列を遡りながら調査・分析することがあります。

素早いインシデント対応と封じ込めをするために、前述したようなログを長期間にわたって集中管理できる仕組みの導入を推奨します。

6 謝辞

検知・緩和策の一部記載に際し、ご協力をいただきました。

- 独立行政法人情報処理推進機構(IPA) サイバーレスキュー隊 J-CRAT
- 伊藤忠サイバー＆インテリジェンス株式会社

7 参考情報 （各種リンク）

- LME (Logging Made Easy)
  https://www.cisa.gov/resources-tools/services/logging-made-easy
- 学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）
  https://www.npa.go.jp/bureau/cyber/pdf/R041130_cyber_alert_1.pdf

以上