京都府サイバー攻撃対策通信

第１０４号
R07.1.10

MirrorFaceによるサイバー攻撃について

警察庁は令和７年１月８日、中国の関与が疑われるサイバー攻撃グループ「MirrorFace」（ミラーフェイス）、別名「Earth Kasha」（アース カシャ）によるサイバー攻撃キャンペーンに関して、注意喚起文書を発表しました。

同グループは、2019年頃から現在に至るまで、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組織的なサイバー攻撃を行っています。

攻撃キャンペーンの特徴

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（「LODEINFO」と呼ばれるマルウェア）を添付したメールを送信してマルウェアに感染させ、情報を窃取

② 2023年頃から、主に我が国の半導体、製造、情報通信、学術、航空宇宙の各分野を標的に、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

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、「ANEL」と呼ばれる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、情報を窃取

侵入後、Windows Sandbox、Visual Studio Codeを悪用する手口も確認

サイバー攻撃の対策

◆メール受信時◆

○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、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、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。

○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。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、不審と感じたら送信者に確認してください。

上記のほか、システム管理者向けの対策も掲載されています。
警察庁Webサイト「MirrorFaceによるサイバー攻撃について（注意喚起）」
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html
をご確認ください。

異常を検知すれば、警察へ速報をお願いします

京都府下京警察署警備課
電話：075-352-0110（内線 464）

千年を守る　未来を創る