

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)

近年、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム(マルウェア)を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。

このサイバー攻撃に共通する特徴は以下のとおりです。

(1) 手口

- ・ 実在する組織の社員・職員をかたり、イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メールが送られてくる。
- ・ 日程や内容の調整に関するやりとりのメールの中で、資料や依頼内容と称した URL リンクが本文に記載されたり、資料・原稿等という名目のファイルが添付されたりする。当該 URL をクリックしたり添付ファイルを開いたりすると、マルウェアに感染する。

(2) 送信元メールアドレスの例

- ・ 表示名<見覚えのない不審なメールアドレス>
- ・ <詐称対象の人物名>@<詐称対象の組織略号>.com
- ・ <詐称対象の人物名>@<詐称対象の組織略号>.org
- ・ <詐称対象の人物名>@<著名なフリーメール(yahoo.co.jp、gmail.com、outlook.com 等)のドメイン>

(3) 不審メールの件名の例

- ・ 【依頼】インタビュー取材をお願いします
- ・ 研究会へのゲスト参加のお願い【●●●●●●●●】
- ・ 【ご出講依頼】●●●●●●勉強会

※ ●には実在する組織名等が入る

また、以前より、WEB メールサービスへの不正ログインの発生を警告する内容のメールを模したメールを送付し、当該 WEB メールサービスの正規サイトを装ったフィッシングサイトに誘導して ID 及びパスワードを窃取することで、保存されているメールを盗み見たり、受信するメールを他のメールアドレスに自動転送する設定を施したりするサイバー攻撃の手法も確認されています。

学術関係者、シンクタンク研究員を始めとする皆様におかれましては、このような組織的なサイバー攻撃が実施されていることに関して認識を高く持っていただくとともに、以下に示す事項を参考に、

適切にセキュリティ対策を講じていただくようお願いいたします。併せて、不審な動き等を検知した際には、速やかに警察又は内閣サイバーセキュリティセンターに情報提供いただきますよう、重ねてお願いいたします。

【怪しいと感じた際に実施すべき事項】

- 別の手法での送信名義人への確認
 - ・ 送信元として知人の名が記載されたメールであっても、少しでも内容に不審な点を感じた場合は、当該メールへの返信以外の方法で送信者に内容の確認を行ってください。

- ウイルス対策ソフトのフルスキャン
 - ・ ウイルス対策ソフトを最新の状態にして、フルスキャンを実施してください。

- アクセス履歴、転送設定の確認
 - ・ 不正利用の疑いがある場合や、ログインアラートメールを受信した場合は、WEB メールサービスにログインし、アクセス履歴を確認してください。もし、身に覚えのないログインが成功していた場合は、パスワードを変更してください。
 - ・ その際、当該ログインアラートメールが偽のものである可能性があるため、メール内のリンクはクリックせず、ブラウザから直接 WEB メールサービスにログインしてください。
 - ・ WEB メール転送設定がされていないか確認してください。

- 関係機関への相談
 - ・ 具体的な被害の相談については、最寄りの警察署又は下記の都道府県警察本部のサイバー犯罪相談窓口若しくは内閣官房内閣サイバーセキュリティセンターにお問い合わせください。
警察庁サイバー警察局 <https://www.npa.go.jp/cyber/soudan.html>
(都道府県警察本部のサイバー犯罪相談窓口)
内閣官房内閣サイバーセキュリティセンター nisc_soudanmadoguchi@cyber.go.jp

【リスク低減のために普段から実施すべき事項】

- ウイルス対策ソフトによるスキャン
 - ・ パソコンは、定期的にウイルス対策ソフトによるフルスキャンを実施してください(毎日～週1程度)。
 - ・ 最新のウイルスを検知できるよう、ウイルス対策ソフトの定義ファイル(パターンファイル)は毎日更新してください。

- WEB メールサービス等のログインアラートの設定
 - ・ WEB メールサービス等には、海外等の通常と異なるネットワーク環境からのログイン等が確認された際にアラートメールを送付する機能があるので、これを設定してください。

○ 二要素認証の設定

- ・ WEB メールサービス等には、ログイン時に本人確認のための秘密情報を2つ使用して認証を行う二要素認証という機能(例えば、パスワードと認証アプリ)があるので、これを設定してください。
- ・ 二要素認証の二段階目の認証手段には、認証アプリ、SMS、メールがよく使われます。セキュリティ上は認証アプリが推奨されています。

○ パスワードに関する注意事項

- ・ パスワードは、十分に長く複雑なものにしてください。
- ・ パスワードは、他のサービスと使い回さず、それぞれのサービスで個別のパスワードを設定してください。

(以上)