令和４年 11 月 30 日
警察庁サイバー警察局
内閣サイバーセキュリティセンター

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 メールの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）

標的型サイバー攻撃、不審メールにご注意ください！

警察庁 National Police Agency　NISC

講演依頼、取材依頼等を騙り
URLリンクから悪意あるファイルをダウンロードさせる

特徴

- 実在する組織の社員・職員を騙り、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る。
- その後、日程や内容の調整に関するメールのやり取りを通して、資料や依頼内容と称したURLリンクの記載されたメールが送られたり、資料・原稿等が添付ファイルとして送付されたりする。

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＞
  ※内閣 太郎 <naikaku.taro@example.com>等
- ＜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のドメイン＞
  ※yahoo.co.jp、gmail.com、outlook.jp等

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

有識者からの原稿の送付等を騙り
添付ファイルを開けさせる

●●様

お世話になっております。●●●●●●の▲▲▲▲▲▲と申します。
私ども●●●●●●の主催する勉強会（非公開）につきまして、先生のご都合を内々にお伺いしたく、ご連絡させていただきました。
…
（具体的な依頼内容）
…
何かご不明な点等ございますれば、何なりとお知らせください。
どうぞよろしくお願い申し上げます。

▲▲▲▲▲▲　●●●●●●
…
（詐称人物の偽の連絡先）

皆様

平素は大変お世話になっております。
先日、■■新聞に標記の拙稿が掲載されました。
ご興味がありましたら、電子版を送付いたします。

＜署名＞

怪しいと思ったら…

警察庁 National Police Agency　NISC

ログインアラートの受信

- アラートメールを受信し、身に覚えのないログインが成功していた場合は、急いでパスワードを変更してください。
- 一方、ログインアラートを装ったフィッシングメールが確認されているので、パスワードを入力する際は、URLをよく確認してください。

ウイルス対策ソフトのスキャン

- 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。
- ウイルス対策ソフトが検知した際は、検知画面を保存（スクリーンショット、スマートフォン等で撮影）し、検知名（マルウェア名）や検知場所（フォルダ・ファイル名）の記録をお願いします。
- また可能であれば、検知したマルウェアは駆除・削除せず、検疫・隔離した状態でご連絡ください。

メールパスワードの変更

- 漏洩や不正利用の疑いがあれば、至急、パスワードを変更してください。
- パソコンがマルウェアに感染している場合、パスワードを変更しても攻撃者が入手できる可能性があるので、マルウェアに感染していないかも確認する必要があります。

転送設定の確認

- メールの転送設定がされていないか確認してください。
- 転送設定がされている場合には、その状況を保存（スクリーンショット、スマートフォンでの撮影）し、設定が変更された状況の記録をお願いします。

相談窓口

具体的な被害の相談については、最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口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)

警察庁 National Police Agency　NISC

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

日頃の備え

標的型サイバー攻撃事例への注意

- 事例と同じような接触を受けた場合、不審な点があれば電子メール等とは別のルートで確認をおこなうなど、サイバー攻撃の被害に遭わないよう注意を怠らないようお願いします。

ウイルス対策ソフト

- 定期的にフルスキャンを実施してください（毎日～週１程度）。定義ファイル（パターンファイル）が更新されると、それまで検知できなかったマルウェアが検知できるようになります。

ログインアラート

- メールサービスやISPによっては、Webメールのログイン時等に、通常と異なる状況（海外からのログイン等）が確認された際、アラートメールを送付してくれる機能があるので、設定する。

二要素認証

- 二要素認証は、本人確認のための秘密情報を２つ使用して認証を行う仕組みです。（例えば、パスワードと認証アプリ）
- 例えフィッシング詐欺に遭ってパスワードを盗まれたとしても、２つ目の認証を突破できなければ実害は発生しません。
- パスワードと組み合わせる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が、セキュリティ上は認証アプリが推奨されています。

メールパスワード

- 十分に長く複雑なものにしてください。
- 使い回しせず、それぞれのサービスで個別のパスワードに設定してください。