

このたび、弊事務所のパソコン 2 台がウイルス (Emotet) に感染し、弊所の弁護士および所員を装ったメールが複数送信されていることが確認されました。

現在判明している調査結果については、下記のとおりです。

引き続き、被害防止と原因究明・拡散防止のため、調査を継続していきます。

なお、弊所の所員を騙る不審メールを受信された場合には、URL のリンク先を開いたり、メールの添付ファイルを開封しないようにお願いします。

身に覚えのない不審なメールを受信された場合は開かず削除してください。

記

1. これまでの経緯と対応

2019 年 12 月 9 日(月)	20:40 頃	所内所員(A)が社外よりマルウェア Emotet への感染を狙う攻撃メールを受信し、メールに添付された Word 形式のファイルを受信者が開き、Word ファイルを開いた後に表示される「コンテンツの有効化」を実行。
	20:45 頃	上記所員 A のなりすましメール (送信元メールアドレスは外部ドメイン) を所内で複数受信。
	21:00 頃	所内に不審なメールを開かぬよう注意喚起メール送信。
	21:22 頃	所員 A より添付ファイルを開封したことの報告。
	21:23 頃	マルウェア Emotet への感染が疑われる所員 A の PC を所内ネットワークより遮断。
	22:31 頃	所員 A の PC についてウイルススキャン実施をしたところ、ウイルスを検知。駆除を確認。
2019 年 12 月 10 日 (火)	午前	所内全 PC のウイルススキャン実施。
	11:08 頃	所員 B の PC についてウイルススキャン実施をしたところ、ウイルスを検知。駆除を確認。
	18:25 頃	お取引先様よりお電話を頂き、所員 B のなりすましメール (送信元メールアドレスは外部ドメイン) が社外へ送信されていることを確認。
2019 年 12 月 11 日(水)	午後	クライアント様へお詫びと注意喚起メールを送信開始。

2. 窃取された情報

感染が確認された所員 A および所員 B とメールの送受信があった一部のメールアドレス、氏名、メール内容（ただし、メール内容が流出したものにつきましては、過去メールをやり取りした際に宛先に含まれていない、本文と全く関係のない『外部』へのメール本文の流出は、現時点では確認されておられません）。

3. ウイルス感染による影響範囲

現時点では、窃取されたメールアドレスの件数は判明していません。

また、過去の送受信メールの添付ファイルの外部流出は、現時点では確認されておられません。

メール内容が流出したものにつきましては、過去メールをやり取りした際に宛先に含まれていない、本文と全く関係のない『外部』へのメール本文の流出は、現時点では確認されておられません。

なお、感染が確認された所員 A および所員 B は企業法務部門の所員であり、債権回収部門および事業管理部門からのメールアドレス、氏名、メール内容の流出は一切確認されておられません。

4. 再発防止策

弊所におきましては、情報セキュリティには十分注意しておりますが、不正アクセスの防止など引き続き対策を強化しておりますので、ご理解とご協力をお願い致します。

5. お客様へのお願い

弊所の弁護士および所員からのメールは「～@suzukiyasuyuki-lawoffice.com」のメールアドレスを使用しております。弊所の弁護士および所員からのメールを受信した際には、送信元のメールアドレスをご確認ください。現時点では不審メールは弊所のメールアドレス以外から送信されていることを確認しております。

このようなメールについては、URL のリンク先を開いたり、メールの添付ファイルを開封しないようお願いいたします。

身に覚えのない不審なメールを受信された場合は開かず削除してください。

また、弊所のお取引先やお取引先のご担当者名義を装った偽造メールが送信されているという情報が届いております。偽装メールと判別しにくいものとなっている場合がございますので、ご注意ください。ご注意いただきますようお願い申し上げます。

もし、何らかの被害に遭われた場合は、下記情報をご覧の上、ご対応をするか、最寄りの警察もしくは、専門機関や消費者生活センター等へお問い合わせください。

◆JPCERT/CC マルウェア Emotet への対応 FAQ

<https://blogs.jpCERT.or.jp/ja/2019/12/emotetfaq.html>

6. その他

弊所はプライバシーマーク付与事業者であるため、本件については、プライバシーマーク指定審査機関である一般社団法人 日本情報システム・ユーザー協会（JUAS）に報告をいたします。

以上