お客様・取引先　各位

令和 2 年 1 月 24 日
株式会社ソリッドシステムソリューションズ
代表取締役　鳥谷部　浩

【重要】迷惑メール（なりすましメール）に関するお詫びとお知らせ(最終)

令和 2 年 1 月 16 日午前 10：00 頃、弊社社員を装った差出人よりメールが送信されているという事象が確認されました。直ちに緊急対策チームを設置し調査した結果、マルウェアに感染した PC が 2 台(管理部所属)存在していた事を特定いたしました。

弊社のお客様、また取引先をはじめとする関係者の皆様には、多大なご迷惑をおかけしておりますことを深くお詫び申し上げます。

詳細は以下の通り、ご報告させて頂きます。

【経緯】

1 月 16 日、9 時半頃、弊社のメールセキュリティシステムにて異常を示すアラートが発生されている事を確認し、直ちに調査に入りました。その後まもなく、弊社のお取引先様より、弊社従業員の差出人表記で不審な電子メールが着信している旨の連絡がございました。

調査の結果、管理部門に存在する特定用途のみに使用する 2 台(うち 1 台は旧 OS を利用)において、マルウェアである Emotet 感染を確認いたしました。

もう 1 台に関しては、Emotet 初期感染後、セキュリティ対策ソフトウェアにより、駆除が実施されていた状態です。

【感染原因に関して】

今回の感染 PC1 台において、取引先名を名乗る迷惑メールに添付されていた不正なファイルを開封してしまった事に起因する事が判明しております。

また、今回の事故において対象となる旧 OS の PC1 台は、新 PC へのデータ移行も含めデータ参照等の利用時のみ電源を投入する形で利用しており、OS のセキュリティパッチ更新や、セキュリティソフトの定義データが最新化されていない等、不完全な状態である事を確認しております。

そのような状態で、Emotet 感染された不正なメールが、弊社の外部電子メールフィルタに隔離されていましたが、通常取引先、及び社内からのアカウント名だったため、通過を許可し、この PC 上の Outlook において、受信、添付された WORD 文書ファイルを開封したところ、不正なマクロプログラムが実行され初期感染が発生したと特定されています。

【被害範囲の特定に関して】

今回の事故においての被害範囲は、感染対象となる旧 OS の PC1 台に保存されている、電子メール送受信履歴から、メールアカウント(個人名、メールアドレス、CC、BCC 含む)、メールボックス情報を窃取され、外部のサーバーから、弊社のアカウント名を表記、不正に利用した状態で送信されています。

現時点で、上記以外にお客様からの 2 次被害、弊社における 2 次被害等は確認されておりません。

1 月 24 日現在、不正に利用されたと推測される電子メールアカウント数は、87 個となっております。

社内においては、開発部門、営業部門はネットワークが分離、別セグメントで管理されており、境界におけるセキュリティチェック等から、水平展開での感染等は確認されておりません。

また、各種サーバーでの感染被害、乗っ取り、等の被害は無いことを確認しており、迷惑メールは弊社から送信されているものではない事を確認しております。

尚、このマルウェアにより発生した迷惑メール、不審なメールの受信は外部における不正送信を実施している多数のメールサーバー(迷惑メール送信サーバー)から送信されているため、弊社で停止する事が出来ない状況です。

当分の間、この事象は続く事が予想されますが、迷惑メール送信サーバー等に対しては、セキュリティーベンダー各社の対応により、今後、収束に向かう事を予測しております。

【業務復旧、対応に関して】

弊社では感染が確認された 1 月 16 日、18 時において、弊社全ネットワーク配下に接続済み、接続可能なすべての PC 端末、サーバー等のチェックを終え、24 時間体制での監視モードに切り替える等、感染端末が存在しない事を確認し、業務復旧に至っております。

お客様、お取引様に対しては、1 月 16 日中に第一報として、電話、電子メール、WEB サイト等でご案内とご説明をさて頂き、翌日、17 日は第二報として WEB サイトに掲載等、個別にご連絡、ご説明をさせて頂きました。一方で、問合せに関しては、随時担当者が対応している状況です。

また、ご不安なお客様に対しては、カスペルスキー社にて駆除ツール、レスキューディスク等を無償提供しておりますのでご案内させて頂きます。

本文書を持って、最終とさせて頂きますが、お客様及びお取引様に対しては、個別にご説明などの対応を行っております。

【再発防止、対策に関して】

今回の事故を受け、以下のような対策を既に実施しております。

- 外部持ち込み PC の検査強化と利用制限を実施、社内検知システムの導入。
- 各種セキュリティに対する知識と意識の周知徹底。
- セキュリティインシデント発生時の対応マニュアルの見直し。
- 電子メールフィルタリングシステムの検知レベル強化。
- 各種ログインパスワードの変更と管理者権限のチェック。
- 資産管理システム、及び各種アクセス、ネットワーク接続ログの監査強化。
- 外部接続可能 PC の利用アプリケーションの制限。
- 従業員利用 PC におけるウィルス対策ソフトウェア、エンドポイントセキュリティーのポリシー見直しと適用内容の徹底したチェック。
- セキュリティベンダーであるカスペルスキー社との連携強化、情報交換による外部支援、監査強化。
- 社内ネットワークセグメントにおける境界フィルタリングの実施。
- 社内共有フォルダ等におけるアクセス制限のチェック、見直し。

お客様及びお取引様におかれましても、上記対策で実施頂ける箇所がございましたら、ご検討ください。

尚、暫定的な処置として、今後は弊社からの正式な電子メールの送信にあたり、以下のような措置を取らせて頂きます。

弊社から送信される正式な電子メールの件名には「[SLD-SYS-SOL+(送信日の年下 2 桁月日)]」という表記のされたものを送信させて頂きます。

例. 2020 年 1 月 24 日に送信したメールの場合

件名：[SLD-SYS-SOL200124] ○○○の件について

お客様及びお取引様にて、メールフィルタリングを実施される場合は、上記件名をフィルタ条件として許可するルールを策定頂ければ幸いです。

また、弊社の正式なメールヘッダー情報等、フィルタリング解除における情報が必要な場合はお問い合わせ窓口までお問合せください。

【弊社社員を名乗る不審メールを受け取られた方へのお願い】

- 弊社からのメールを受信した場合には、送信元のメールアドレスを十分にご確認ください。
- 弊社社員(差出人)のメールアカウント名や表記ではなく、実際のメールアドレスをご確認ください。
- 弊社より正式な添付ファイルを送信する場合は、添付ファイルが暗号化された本文とパスワード通知の 2 通のメールが届きます。WORD 文書ファイル等が暗号化されず直接添付されることはございません。
- その他、不審な本文のメールに添付されているファイルや、本文に記載されたリンクについては、開かない様にお願いをいたします。

【ご注意、予防等に関して】

今回の事故を受け、弊社よりお客様及びお取引様に対して、以下の通り、注意喚起させて頂きます。

● 以下のアップデートが実施されているかご確認ください。
マイクロソフト セキュリティ情報 MS17-010
Microsoft Windows SMB サーバー用のセキュリティ更新プログラム（4013389）
WindowsOS を利用されている PC で、このアップデートが実施されていない場合、Emotet 感染すると水平展開され他の PC に感染する事が予想されます。

● 添付される WORD 文書ファイルに関して
先にもご説明しておりますが、今回の事案では、不審な WORD 文書ファイルが添付されているケースが殆どです。
この WORD 文書ファイルは開かないようにお願いいたします。開いてしまった場合、「コンテンツの有効化」ボタンは押さないようにしてください。

● URL リンクに関して
先にもご説明しておりますが、今回の事案で送信される電子メール内に、URL リンクが記載されている場合がございます。URL リンクはクリックしないようにしてください。
このリンクをクリックしてしまうと、外部の不正なファイルダウンロードサイトに接続される場合がございます。

その他、以下の情報も参照ください。

【参考】IPA 情報処理推進機構 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html

弊社ではカスペルスキー社のエンドポイントセキュリティーを PC 端末で利用しておりますが、「ふるまい検知」「セルフディフェンス」といった、通常とは違う PC 内部の動きや未知のウィルスを検知する機能が各社セキュリティソフトウェアにも存在するかと思います。
そのような機能を有効にしますと、マルウェアの実行が行われた際、許可されずに被害を防止できる可能性が高くなります。

【弊社製品に関しての影響】

弊社製品及びサービスである All Gather CRM 及び All Gather Cloud に関しては、開発部門、品質管理部門等、関係する領域は完全に異なるセグメントで管理されており、厳重なセキュリティチェックの基、提供を実施しております。
また、一般向けクラウドサービスに関しては、通常、Microsoft 社の Azure での提供となっており、こちらも最高レベルのセキュリティ管理の基、サービス提供を実施しております。
従いまして、製品、サービスに関して、本件における影響は皆無である事を確認しております。

以上となりますが、
弊社では、情報セキュリティ対策チームを再編成し、改めて情報管理、セキュリティ対策等において見直しと、強化を進めてまいります。

・お問い合わせ窓口
電話番号：017-721-3399（受付時間：平日 10 時～17 時）

・各営業所

東京オフィス
〒105-0012
東京都港区芝大門 2-2-1
ユニゾ芝大門二丁目ビル 6 階
TEL：03-6402-5560
FAX：03-6402-5565

青森オフィス
〒030-0823
青森県青森市橋本 2-13-5
大同生命ビル 5 階
TEL：017-721-3399
FAX：017-721-3382

以上