2020 年 11 月 14 日

ウエインズグループ
横浜トヨペット株式会社

横浜トヨペット株式会社におけるコンピュータウイルス感染と それを発端にした当社を騙った「なりすましメール」に関するお詫びとご報告

日頃より横浜トヨペットをご愛顧いただきありがとうございます。
さて、2020 年 7 月 29 日より発生しております「なりすましメール」に関しまして、関係者の皆様に多大なご迷惑とご心配をおかけしておりますことを深くお詫び申し上げます。

9 月 30 日のリリースの通り、詳細の調査が完了いたしましたので、本件の経緯等について下記の通りご報告いたします。

記

1. 事象概要

・横浜トヨペット内 LAN に接続しているパソコン端末 12 台がコンピュータウイルス（マルウエア）「Emotet」に感染していることを確認しました。
・また、上記端末の感染を発端にして、同端末上のメールソフトで過去にやり取りをした関係者（弊社社員、弊社グループ会社社員等）の名前を騙る不審メールが、弊社管理下にあるサーバやこれらの関係者とは全く無関係なサーバより送信されるようになったことを確認しております。

2. 経緯

7 月 28 日　弊社内 LAN に接続しているパソコン端末 1 台にて Word ファイル(.doc) が添付されたメールを受信。同端末にて、添付ファイルを開いたことにより Emotet ウイルスに感染。ウイルスの活動により、大量の不審メールが弊社とは無関係な宛先を中心に配信される。

7 月 29 日　弊社内 LAN に接続されている多数の端末で Emotet メールを受信。
11 台で開封・ウイルス感染が広がり、サーバおよび端末に存在しているメールアドレス宛になりすましメールが大量に配信される。
この時点で、過去のメール本文のコピーを含む内容の不審メールが、無関係な外部のメールサーバより送信される。
不審メールの宛先は、同端末上のメールソフトで過去にやり取りをした相手先アドレスを中心に、弊社と関係のない宛先も含まれていた。

なお、送信者名は前述の通り実在の関係者を騙っているが、送信元のアドレス自体は弊社と関係ない他組織のアドレスであった。感染の拡大を止めるため、感染可能性の疑いがある端末の電源をシャットダウンし、ネットワークを全切断するが、配信が続く。

7 月 29 日　感染の確認と影響範囲が広範にわたることを危惧し、ホームページに公表（7 月 29 日リリース）。
専門調査機関を交えた対策チームの設立。

7 月 31 日　大量の不審メール配信に弊社管理下のメールサーバが踏み台にされている可能性が存在したため、サーバの停止を実行。これに伴いメールによる問い合わせを一時休止（7 月 31 日リリース）。

8 月 5 日　簡易調査により、一連のインシデントが、Emotet によるものであると判明。11 拠点 11 台の感染が確実となった。（8 月 5 日リリース）。
詳細の調査を専門調査機関へ委託、全拠点の端末を対象とした攻撃痕跡調査を開始。

9 月 30 日　調査進捗を公表（9 月 30 日リリース）。

3. 被害規模と範囲について

攻撃痕跡調査の結果、最終的に 12 台の感染を確認いたしました。「同ウイルスに関する過去の報告および現時点での不審メールの内容から、漏洩した情報は、感染した端末のメールソフトに履歴の残っていた「送受信した相手のメールアドレスと名前」「メール本文」であることを確認しております。

また、ウイルスが活動の痕跡を消しており、抜き取られた情報数の把握はできておりません。

なお、当該端末ではお客様のクレジット情報や銀行口座情報等の個人情報は扱っておりません。

4. 弊社の関係者を騙る不審メールを受信された皆様へのお願い

弊社の社員を名乗るメールを受信し、かつ添付ファイルが付いている場合、メールアドレスをご確認ください。弊社社員が業務用に使っているメールにつきましては、基本的に「****@yokohama- toyopet.jp」を利用しておりますので、これ以外のアドレスが使われた心当たりのない内容のメールにつきましては、削除いただきますよう、よろしくお願い申し上げます。

なお、Emotet の不審メールについては、Word ファイルが添付されているケース以外に、Word ファイルの入ったパスワード付き zip ファイルが添付され、メール本文にパスワードが記載されているもの、Web 会議の招集を模すなど新しいパターンが発生しております。zip ファイル付きメール の場合、一般的なメールサーバ上のウイルス対策では防げない可能性が極めて高くなりますので、一層の注意が必要となります。

※「Emotet」の詳細につきましては、下記「JPCERT/CC」サイトをご覧ください。

マルウェア Emotet の感染拡大および新たな攻撃手法について

https://www.jpcert.or.jp/newsflash/2020090401.html

5. 今後の対策について

これまでに実施した対策は下記となります。

・感染疑いのある端末のネットワーク切り離しとマルウェア駆除と初期化
・感染の糸口となった Word,Excel 等のマクロ自動実行の無効化
・メールサービスをより安全性の高い環境へ変更
・全社員に対するサイバーセキュリティ教育
・サイバーセキュリティ対策プロジェクトチームの設営・アセスメントの実施

今回については、端末上での対策（ウイルス対策ソフト等によるチェック）で侵入を防ぐことができなかったことから、現在の各端末上での対策に加え、出口対策（漏洩対策、セキュリティインシデント対応チームの設営)、被害拡大防止の仕組みについても早期に導入したいと考えております。

また、システム面での対応だけでなく、研修等を通じて社員の情報セキュリティに関するリテラシー向上についても図っていく所存です。

今回の件につきましては、新たな事実が判明しましたらご報告いたします。

関係者の皆様に多大なるご迷惑をおかけしましたことを重ねてお詫び申し上げます。

以上

お問い合わせ先：横浜トヨペット株式会社　お客様相談室
お電話：０１２０－６６３－３８３
メールアドレス：info@yokohama-toyopet.jp