報道関係各位

2022 年 3 月 7 日

セキュリティ連盟

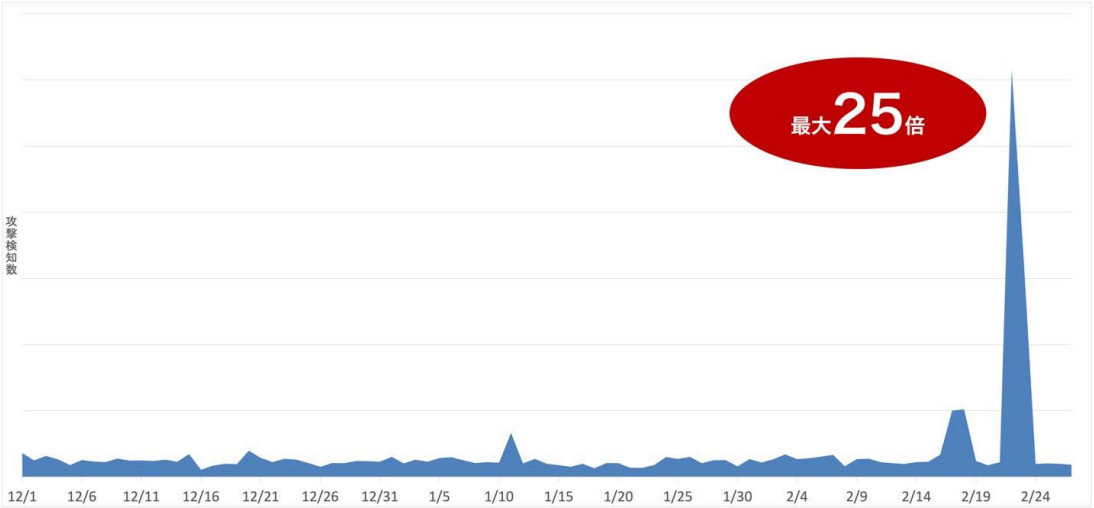
セキュリティ連盟、サイバー攻撃の急増に注意喚起
加盟企業より必要なセキュリティ対策を発信
不審なアクセスを検知した場合には直ちにご相談を

サイバーセキュリティ対策の重要性啓発を目的として結成され、啓発アクション『日本の DX をもっと安全に～サイバー攻撃被害ゼロを目指して～』を推進するセキュリティ連盟は、昨今のサイバー攻撃の急増を受け、注意喚起を行います。不審なアクセスや攻撃を検知した場合は、セキュリティ連盟までご相談ください。

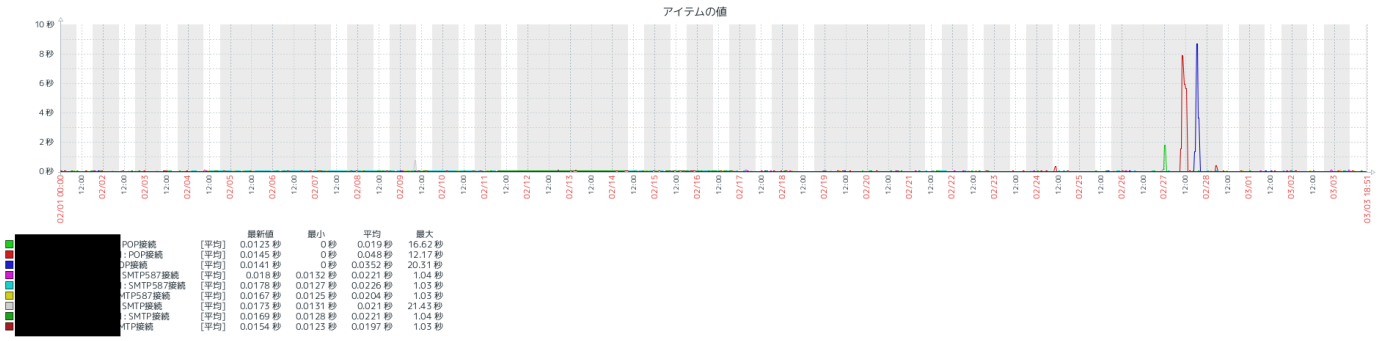
■不審なアクセスを複数検知

セキュリティ連盟の発起人でもある株式会社サイバーセキュリティクラウドは、日本国内 15,000 以上のサイトを対象とした調査で、2 月 16 日以降不審な攻撃者による不正アクセス、正確には BOT や脆弱性スキャンツールなどによる攻撃の検知が急増していることを確認しました。直近 3 ヶ月平均と比べて最大 25 倍もの攻撃が検知されています。

また、加盟企業である株式会社ネットアシストが提供するサーバの監視保守代行サービス『MSP アシスト』の監視データによると 2 月 27 日頃から複数のサーバにおいてメールサービス(POP3・SMTP 等)の遅延件数が急増しており、その一部は海外の IP アドレスからの DoS 攻撃が原因であると確認しています。



▲サイバーセキュリティクラウドが検知した攻撃数の推移



▲ネットアシストが検知したメールサービス遅延時間の推移

■サイバー攻撃への対策

加盟企業のクラウドセーフ株式会社は 2021 年 11 月後半より確認されているマルウェア『Emotet』について、次の対策を実施することを推奨しています。

緊急で必要な対策
1. パスワード付き圧縮ファイルを不用意に解凍しないなど組織内へ注意喚起の実施
2. 感染が疑われる端末使用のユーザのメール等、認証情報の変更
3. 感染が疑われる端末使用のユーザのブラウザに保存されている認証情報の変更
4. 必要に応じて Excel や Word ファイルのマクロ無効化
5. 組織内の全てのコンピュータでウイルス対策ソフトによるスキャンを実施
6. %TEMP%で Emotet が検出された際は、専門家による影響範囲の確認

中長期で検討が必要な対策
7. パスワード付き圧縮ファイル利用廃止の検討
8. クラウドサービスの利用やテレワークをする際には、多要素認証またはそれに類する対策を実施

Emotet は 2014 年頃からオンラインバンキングの認証情報を窃取することを目的としたマルウェアとして認識されています。様々なアップデートを繰り返し 2019 年 10 月頃から何度も日本国内で感染が拡大しました。2021 年 1 月、EUROPOL（欧州刑事警察機構）が Emotet のインフラ基盤を無効化（テイクダウン）したことを発表しましたが、2021 年 11 月後半より活動の再開が確認されています。Emotet は、主にマクロ付きの Excel や Word ファイル、またこれらのドキュメントファイルをパスワード付き Zip ファイルとしてメールに添付する形式など複数の方法で配信されています。各種認証情報、保存されているメールやアドレス情報などの窃取を行うことが可能なほか、追加のマルウェアのダウンロード・実行など様々なことが可能となっています。
もしメール情報が窃取されている場合、機微な情報が盗まれるだけでなく、その情報を悪用した攻撃メールが送信され社内や関係組織への被害拡大へとつながる可能性があるため注意が必要です。

また、発起人である株式会社サイバーセキュリティクラウドは、企業が取るべきセキュリティ対策として次の 3 つを推奨しています。

1.技術的対策
技術的な対策として、まずはセキュリティ製品の導入や、侵入を防ぐ取り組みを実施することです。また、実施すべき対策を出来うる限りリストアップして可視化することも大切です。全ての対策を即時に実行できない場合もあるので、必要最低限手をつけることができるものから対策を始めましょう。社内でどの対策を実施できるか議論を重ねることで、サイバーセキュリティ対策における問題を再認識することもできます。

＜技術的対策の例＞
PC へのウイルス対策ソフトの導入、IDS/IPS の導入、WAF の導入
使用しているソフトウェアの定期的な更新、セキュリティ診断の実施

脆弱性を出さないことを意識したシステム作り

2.物理的対策
物理的対策とは、盗難・災害といった物理的要因に対する対策を指します。
実際に起こりえるかはわかりませんが、万が一のことを想定して、対策を行いましょう。

＜物理的対策の例＞
防犯カメラの設置、社員デスクの施錠徹底、オフィスの施錠徹底、入退室記録の管理
生体認証システムの導入、耐震強化、耐震設備の導入

3.人的対策
人的な対策はセキュリティに対してのルールを設定する対策です。またルールを設定するだけでなく、社員に遵守してもらうように説明会などの教育も併せて重要となります。

＜人的対策の例＞
業務の持ち帰りの制限、パスワード管理のルール決め、標的型メールについての教育
セキュリティ教育の実施、インシデント発生時の連絡・報告体制の決定

技術・物理・人の 3 つの対策を実施することでより安全性を高めることができるでしょう。

■関係 7 省庁によるサイバーセキュリティ対策の強化についての注意喚起

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。令和 4 年 3 月 1 日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

関係 7 省庁：経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター
サイバーセキュリティ対策の強化について（注意喚起）
https://www.meti.go.jp/press/2021/03/20220301007/20220301007-1.pdf

セキュリティ連盟とは？

サイバーセキュリティ対策の重要性啓発を通じ、国民経済と国民生活の向上及び公共の福祉の増進に寄与することを目的とする団体です。今後は公共性・公益性の高さから一般社団法人化しての活動展開を予定しています。

セキュリティ連盟による主な活動内容

・セキュリティ啓発アクション『日本の DX をもっと安全に～サイバー攻撃被害ゼロを目指して～』の企画・実行
- サイバーセキュリティ対策の普及啓発イベントやセミナーなどの開催
- 最新のサイバー攻撃情報（トレンド）・対策事例などの情報発信
- セキュリティインシデントに関するクローズドセミナーの実施
- セキュリティ担当者・情報システム担当者の為のコミュニティ形成・運営

・セキュリティ連盟の加盟企業間での情報交換とそれを基にした情報発信

日本の DX をもっと安全に

・本アクション特設サイトの URL：https://www.cscloud.co.jp/dx-security

セキュリティ連盟加盟企業：41 社一覧（商号略・敬称略・アルファベット順・50 音順）

DXHR、G-gen、GMO グローバルサイン・ホールディングス、LRM、Maromaro、PJ-T&C、Spider Labs、
TOKAI コミュニケーションズ、TOWN、YONA、アールワークス、アイビーシー、アイレット、アジアクエスト、アピリッツ、ウイル、
エーアイセキュリティラボ、かっこ、クラウドエース、クラウドセーフ、クラスメソッド、クララオンライン、サーバーワークス、サイバーコマンド、
サイバーセキュリティクラウド、サイバーリーズン・ジャパン、サンロフト、シーズ、スプライン・ネットワーク、ソフテック、タイムシェア、高山、
ネットアシスト、ハートビーツ、ハイパーボックス、ビヨンド、フューチャースピリッツ、ブロードバンドタワー、ユニティ、ライド、レンジフォース