2021 年 05 月 28 日

サービス＆セキュリティ株式会社 e-Gate センター

ニューノーマル時代によるセキュリティインシデントの移り変わり

1. 概要

2020年4月の緊急事態宣言から約1年が経ち、テレワーク、リモート会議、オンライン営業の導入など、企業の業務形態に変化が見られました。このニューノーマルな時代への移り変わりにともない、セキュリティインシデントも増加の傾向が見られ攻撃者の手口もまた変化してきております。今回は変化があった1年間の間で、どのようなセキュリティインシデントが増加したか、また最新の傾向や対策を合わせてご紹介いたします。

2. フィッシング詐欺の増加、手口の変化

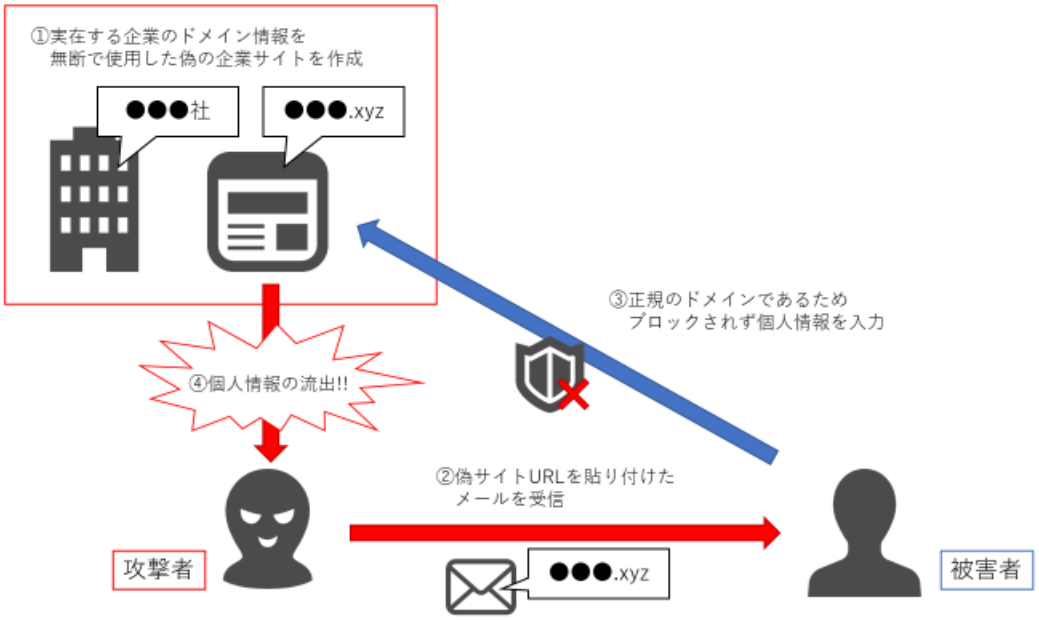
昨年からの 1 年間で非常に大きく増加したセキュリティインシデントは、不特定多数の個人を狙ったフィッシング詐欺となります。

e-Gate センターでも非常に多くのフィッシングメールが観測されております。過去 2020 年 10 月にフィッシング件数の急増として取り上げましたが、その後も継続して検知件数は増加しており、2020 年 5 月と比べて 2020 年 10 月には約 16 倍の検知件数、さらに 5 ヶ月経過した 2021 年 3 月には 10 月の約 2.5 倍の検知件数となっております。

【図 1】e-Gate センターにおけるフィッシングメール検知件数

過去に取り上げているフィッシング件数の急増については、以下の記事をご参照ください。
『フィッシング件数の急増について』
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11188

件数の増加と共に手口についても変化してきております。一般的なフィッシングの手口では、フィッシングメールに大手ショッピングサイトや国内大手のカード会社を装った"偽サイト"へのリンクを貼り付け、リンク先で偽のログインフォームやカード情報を入力するよう誘導して個人情報を騙し取ります。こちらで使われる"偽サイト"は今までは全く関係のないドメイン名や正規のドメイン名を一部変えたものを使用していました。ですが、最近確認されている"偽サイト"では実在する会社の正規のドメイン名のトップレベルドメイン（TDL）を変えたドメインを取得し、あたかも一般企業サイトであるかのように見せかける手口が増加してきております。攻撃者はこの手口を用いることで、一般的なセキュリティソフトのブロック機能の回避だけでなく、ドメイン情報から悪性サイトであるかを検査するリアルタイム検知機能まで回避することが可能となります。



【図 2】新たなフィッシングの手口

●対策

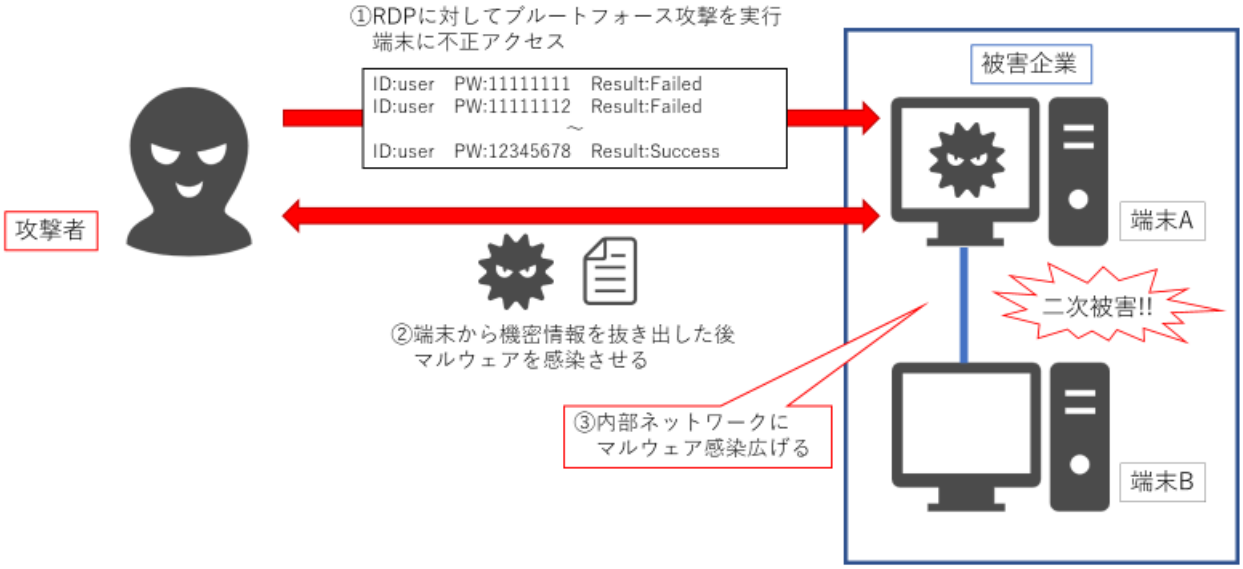
フィッシングの新たな手口について、以下の対策が有効となります。

・メールアドレス、タイトル、本文、リンク等に不審な点がないか、メール内容に一貫性があるかを確認する
・リンク先のサイトに不審な点がないか、安全であるかをサイトチェッカーや仮想ブラウザで確認する
・セキュリティ機器の導入・監視を行うことにより、不審な通信に対しての未然の発見・即時の対応が可能

3. リモートデスクトップ接続を狙った乗っ取り操作

自宅からのリモートワークが増加した影響でリモートデスクトップ接続を狙う攻撃も増加しました。

リモートデスクトップ接続を狙った攻撃は主に Windows に標準搭載されているリモートデスクトッププロトコル（RDP）に対してブルートフォース攻撃を行い、脆弱なパスワードで管理している端末を乗っ取ります。また乗っ取りが成功した端末から機密情報を不正に奪取した後、端末自体をマルウェア感染させて企業内のネットワークに二次被害を発生させることで信用低下や身代金を要求する手口が発見されています。



【図 3】RDP を狙う攻撃イメージ

またリモートデスクトップ接続を行うツールの脆弱性を狙った攻撃も発生しております。実際に 2021 年 2 月に米国で起こったセキュリティインシデントでは、浄水場の管理システムにて使用していたリモートアクセスツール「TeamViewer」の脆弱性を利用して不正にリモートから操作を行い、排水管洗浄に用いられる水酸化ナトリウムの設定値を規定値の約 100 倍に変更するという事件が発生しております。本事件では不正にリモートから操作されてしまった端末を従業員が監視していたため、即座に規定値に戻すことで大きな影響はありませんでした。こういった大きなセキュリティインシデントが発生する前にリモートでの接続方法については適切に管理することが重要となります。

●対策

リモートデスクトップ接続を狙った攻撃に対して、下記の対策が有効となります。

・リモートで接続する必要のない端末は RDP を無効にする
・接続するアカウントのパスワードを強固なものにする
・境界ファイアウォールでポート 3389 または他の RDP ポートを外部接続不可にする
・アクセスツールを用いる場合はバージョン管理を怠らないようにする
・エンドポイントセキュリティソフトの導入を行い、設定が改ざんされないようパスワードで保護する

過去にもリモートデスクトップ接続に対しての攻撃についてご紹介しております。以下の記事も合わせてご参照ください。
『リモートデスクトップサービスの脆弱性「BlueKeep」について』
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9976

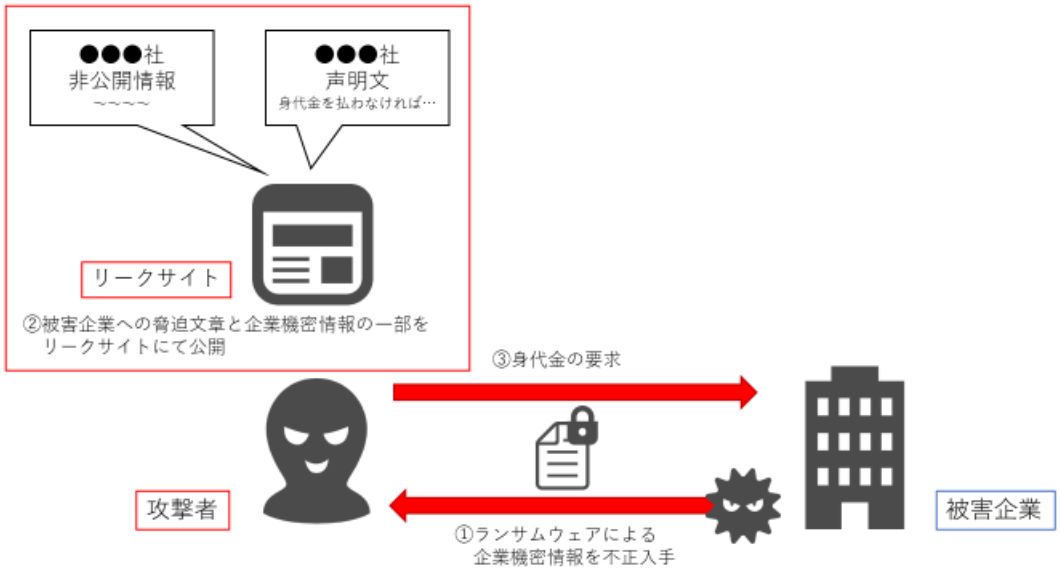
4. ランサムウェア被害の増加

規模の大きなセキュリティインシデントとしては、大企業を狙ったランサムウェアによる被害が増加しました。IPA が公開している「情報セキュリティ 10 大脅威 2021」でも社会に影響力を与えた脅威として「ランサムウェアによる被害」が組織標的ランキングの 1 位にランクインしております。

従来のランサムウェアでは攻撃の標的が不特定多数にばらまく手法が多かったのに対し、昨年からの 1 年間では過去 2020 年 11 月にも取り上げている Ryuk ランサムウェアのような標的型の攻撃手法が多く見られました。

過去に取り上げている Ryuk ランサムウェアについては、以下の記事をご参照ください。
『Ryuk ランサムウェアの特徴と対策』
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11221

また感染後の脅迫方法にも変化が現れました。従来の暗号化された情報資産に対しての身代金要求の他に、Ragnar Lockerランサムウェアではリークサイトを用意して身代金を払わない企業の機密情報をリークするといった二重の脅迫や、SunCryptランサムウェアでは二重脅迫に加えて、身代金を払わなければDDoS等の別の攻撃も行う宣言をするといった更なる多重脅迫を行う新しい手口が確認されています。



【図 4】ランサムウェア被害による多重脅迫の手口

これらのランサムウェアの感染経路としては、前述 3 章「リモートデスクトップ接続を狙った乗っ取り操作」でも紹介した不正に操作を行うことによって感染させる場合や、Emotetのようなメール添付ファイルからの感染が主な感染経路となります。Emotetからの感染は現状落ち着いてきてはおりますが、亜種や新たな感染手口が現れる可能性があるため今後も対策が必要となります。

●対策

ランサムウェア感染を防ぐための対策として、下記が有効となります。

・不審な送信元からメールのリンクや添付ファイルを開かない

・マクロの実行設定が無効になっていることを確認する

・メールや文書ファイルを閲覧しているとき、身に覚えのない警告ウインドウが表示された場合、警告の意味が分からない場合は操作を中断する。

・セキュリティ機器の導入・監視を行うことにより、不審な通信に対しての未然の発見・即時の対応が可能

5. 昨年時との振り返り、今後について

働き方に変化が現れた昨年 2020 年 6 月の緊急事態宣言解除後頃には、ホームルーターなどの IoT 機器のボット化を狙った攻撃や Web 会議サービスの不正利用による情報漏えいが多く発生しておりました。その後 1 年間で攻撃の手口も多様化していき、不特定多数の個人を狙ったフィッシング詐欺の急増やランサムウェアでの大企業への標的型の攻撃も多く見られる結果となりました。このような攻撃の急速な変化に対応するためには、常に最新のセキュリティ状態を保つことやセキュリティインシデント発生時に即時に対応できるようなセキュリティ体制が必要となります。

常に最新のセキュリティ状態を保つためには、端末にセキュリティソフトを利用するだけでなく、ファイアウォールや IPS といったネットワークセキュリティ機器の導入をご検討ください。ネットワークセキュリティ機器を導入することにより、マルウェアや悪質な攻撃のふるまい等を検知して、攻撃者からの通信を遮断することが可能です。また、ネットワークセキュリティ機器が出力するログやネットワーク接続のアクセスログを監視・分析することで、セキュリティインシデントの未然防止や早期発見による即時対応が可能となります。

しかし、社内のシステム部門の体制だけでこれらの運用を行うには多くのコストがかかってしまい、対応が困難な場合があります。そのような場合は、外部の SOC（セキュリティオペレーションセンター）にネットワーク機器の運用をアウトソーシングするという手段も有効です。

6. 参考情報

・フィッシング対策協議会
2021/04 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202104.html

・CNN
浄水システムに不正侵入、苛性ソーダ濃度１００倍に設定　米フロリダ州
https://www.cnn.co.jp/usa/35166249.html

・IPA　情報処理推進機構
情報セキュリティ 10 大脅威 2021
https://www.ipa.go.jp/security/vuln/10threats2021.html

7. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp