電子メール: クリックは慎重に

フィッシング、不正行為、その他の詐欺から保護する方法

CISCO

目次

はじめに 3

送信者と受信者 3

ビジネスにとっての意味 3

必要とされる対策 4

現在の電子メールとフィッシングの状況 6

一般的な電子メール攻撃のタイプ 7

Office 365 のフィッシング 7

ビジネス メール詐欺 8

デジタル恐喝 9

「パッケージと請求書」型のスパム 10

前払い詐欺 11

電子メールのマルウェア 12

電子メールの配信インフラストラクチャ 13

ボットネット 13

バルク電子メール ツールキット 14

手段としての詐欺 15

電子メール攻撃から保護する方法 17

フィッシング メールの明らかな兆候 17

攻撃予防戦略 19

備えを固める 20

電子メール攻撃から組織を保護する方法 21

シスコ サイバーセキュリティ シリーズ 22

はじめに

昨年スパムは 40 歳を迎えました。1978 年、当時 Digital Equipment Corporation のマーケティング マネージャだった Gary Thuerk 氏が、新製品の発売を知らせるメッセージをインターネットの原型である ARPANET で 393 人に送ったのが最初のスパムと言われています。このメッセージも、現在のスパムと同じく歓迎されませんでした。Thuerk 氏は厳しく叱責され、二度と同じ事をしないよう注意されたのです。

今も叱責するだけで止めば良いのですが、そう簡単ではありません。40 年の間にスパムは急激に広がり、医薬品、ダイエット商品、求人などの不要な案内で受信トレイはいつもいっぱいです。フィッシングやマルウェアといった、はるかに大きな脅威も増えています。フィッシングが最初に考え出されたのは 30 年以上前です。マルウェアも電子メールで配布されるようになって数十年たちます。

現在、電子メールの多くが不要なスパムで、状況はますます悪化しています。その量は驚異的で、Talos Intelligence によると、2019 年 4 月に送信された電子メール全体の 85% がスパムでした。スパム メールの割合だけでなく、量も増加し続けています。4 月のスパムは過去 15 ヵ月で最も多くなりました。

送信者と受信者

電子メールは、詐欺師が使うのにほぼ理想的な手段だと言えます。電子メールを受け取ったユーザは、必ず内容を確認して何らかの判断をし、場合によってはクリックなどの操作をします。人の優しさに付け込んだソーシャル エンジニアリングを上手く駆使すれば、ユーザを行動に移させることができます。

ソーシャル エンジニアリングは攻撃者にとって理想的な攻撃ベクトルであるだけでなく、組織的な防御も難しくします。電子メールによる攻撃がユーザを標的にしないことはほぼ皆無です。一般的に使われる手段では、侵害された Web サイトや、エクスプロイト キットを隠した危険な Web サイトへのリンクを送り付けます。ただしいずれにせよ、それらのリンクをクリックしなければ攻撃が成り立たないのは変わりません。

ビジネスにとっての意味

CISO にとって頭痛の種が電子メールであることは不思議ではありません。最新の CISO ベンチマーク調査では、電子メール内の悪意のあるリンクをクリックするといったユーザの行動を防ぐことについて、CISO の 56% が、かなりまたは極めて困難であると感じていることがわかりました。これは調査したセキュリティ上の懸念事項の中で最も高く、パブリック クラウドにあるデータやモバイル デバイスの利用に関する懸念よりも高くなっています。

同時に、攻撃の頻度も問題になっています。たとえば調査した CISO の 42% は、悪意のあるスパム メールを開いたことが原因だと判明しているセキュリティ インシデントに対処した経験があります。同様に 36% は、フィッシング攻撃で情報が盗まれるインシデントにも対処した経験があります。CISO ベンチマーク データによると、CISO は電子メールの脅威を組織で 1 番のセキュリティ リスクだと考えています。

2018 年にシスコが委託して ESG が実施した別の調査では、回答者の 70% が、電子メールの脅威に対する保護がますます難しくなっていると訴えています。電子メールによる攻撃の影響については、回答者の 75% が重大な運用上の影響があったと答え、47% が深刻な財務面の影響があったと報告しています。

必要とされる対策

必要性とリスクの両方を同時に守るにはどうすればよいでしょうか。多くの組織は、クラウドへの移行が解決策になると考えてきました。しかし、クラウドは電子メールの危険を解決する確実な方法ではありません。大抵のケースで、問題を先送りにしているにすぎません。セキュリティの問題は解消せず、むしろ継続し続けます。

電子メールによる脅威が与える全体的な影響を最小限に抑える方法はいくつかあります。このドキュメントでは、現在最もよく見られるタイプの電子メール攻撃について簡単に紹介しながら、最近の脅威の状況について説明します。攻撃者たちの行動、目的、背後にあるインフラストラクチャについて詳しく分析します。さらに、ビジネスの安全性を維持するためにできることや、電子メールによる脅威を見極める方法についてもご説明します。

「毎日平均で 412,000 件もの電子メール メッセージを受け取っていますが、そのうち 266,000 件は当社の STMP エンジンにたどり着けてもいません。Talos がグローバルな脅威インテリジェンスに基づいてこれらメッセージをブロックしているためです」

SUNY Old Westbury 社、最高セキュリティ責任者、Milind Samant 氏

「企業は、セキュリティとビジネス リスク、さらにユーザ エクスペリエンスでバランスを取る必要があります。バランスが取れたら、次に必要なのは問題が発生した時にアクティブに応答して防御を適用するプログラムです。人的ミスは実際に起こり、これを狙った数十億ドル規模のサイバー犯罪産業が存在しています。このミスに備え、発生時には迅速に対応できるようにする必要があります。人的ミスに付け込んでセキュリティ防御の突破に成功している攻撃、資産やソフトウェアの脆弱性をターゲットにしている熱心な攻撃者などを毎日目にする一方で、アクティブな検出と応答でこれら攻撃をあぶりだして封じ込めている実態を毎日のように確認しています。このように当社のセキュリティ プログラムは優れた効果を発揮しています。」

シスコ、最高情報セキュリティ責任者、Steve Martino

現在の電子メールとフィッシングの状況

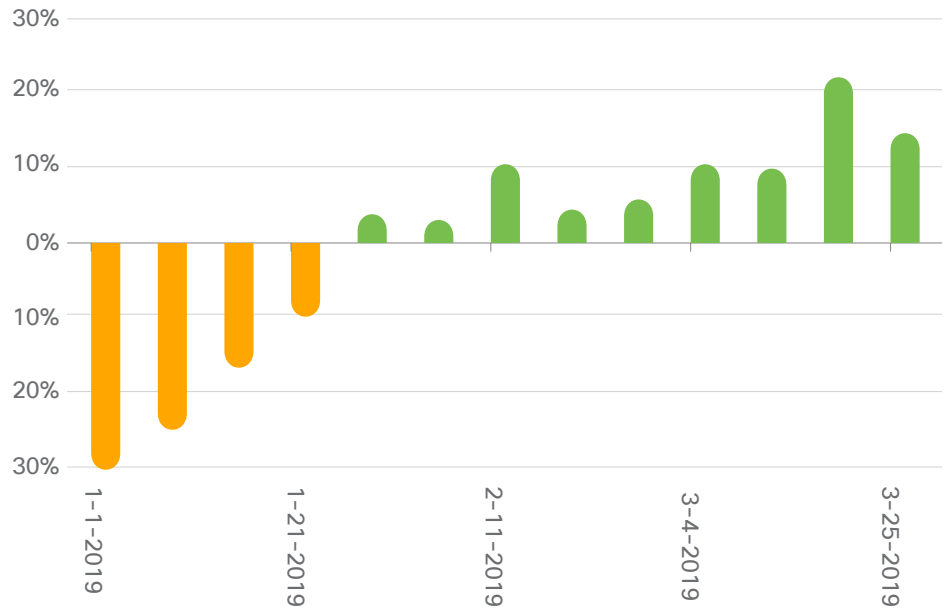
電子メールに見られる危険は多数あります。シスコが寄稿している Verizon 社の 2018 Data Breach Investigations Report によると、電子メールはマルウェアの配布(92.4%)とフィッシング(96%)の両方で一番よく使われている手段です。不正な電子メールに反応すると、クリプトマイニングの被害やクレデンシャルの盗難に合うことがあるほか、悪質なソーシャル エンジニアリング詐欺に引っかかって多額を失うこともあります。これを企業レベルで考えると、不正な電子メールで生じる混乱はかなり大きなものになります。

ユーザはどのようにして電子メール詐欺に引っかかるのでしょうか。Duo Security にたずねてみました。同社のチームは数年前に無料の Duo Insight ツールを作成しました。このツールでは、自分で偽のフィッシング キャンペーンを作成して社内に仕掛け、だれがだまされるか調べることができます。

これには残念ながら多数のユーザが引っかかっています。The 2018 Duo Trusted Access Report によると、実行したフィッシング シミュレーション キャンペーンの 62% が、少なくとも 1 セットのユーザ クレデンシャルを入手できました。すべての受信者のうち、ほぼ 4 分の 1 が電子メール内のフィッシング リンクをクリックしました。さらにその半分が偽の Web サイトにクレデンシャルを入力しています。

この成功率を見ると、電子メールがフィッシング キャンペーンでよく使われるのも当然だと言えます。実際、Cisco Umbrella が特定した新しいフィッシング ドメインの数を考えると、フィッシング アクティビティは急増していると思われます。そこで、2019 年の第 1 四半期の週平均を取り、この平均と毎週を比較しました。図 1 の結果は、始まりはゆっくりでしたが、その後新しく作成されるドメインの数が急速に増え、四半期の最初の週から最後にかけては 64% の増加があったことを示しています。

図 1　毎週の新しいフィッシング ドメインと第 1 四半期の週平均の比較



出典:Cisco Umbrella

一般的な電子メール攻撃のタイプ

次に、現在最もよく見られる電子メールを使った詐欺の概要について説明します。ラップトップを開いて受信トレイを表示すると、次の未読メッセージがある様子を想像してください。

Office 365 のフィッシング

送信元が Microsoft 社のように見える電子メールを受信します。Office 365 の電子メール アドレスがエラーまたはポリシー違反により使えなくなることを知らせる内容です。これを避けるには、記載されているリンクからアドレスを確認するしかないということです。

これは Office 365 のクレデンシャルを狙ったフィッシング攻撃です。使われている電子メールや URL は、micros0ftsupport@hotmail.com など、いかにも Office 365 で使われているもののように見えます。リンクをクリックすると、電子メール アドレスとパスワードの入力を求める、公式サイトと同様のログイン ページが表示されます。

ただし、このサイトは偽物です。クレデンシャルを手に入れた攻撃者は、Microsoft 関連の他のサービスに勝手にログインし、連絡先を収集します。よく使われるのは、電子メール アカウントにログインし、別のフィッシング URL を含む偽物の電子メール(件名:FYI など)を連絡先に送信する手法です。

このようなスタイルの攻撃は増大しています。シスコのパートナー企業が Agari で公表した Q2 2019 Email Fraud and Identity Deception Trends レポートによると、高度な電子メール攻撃の 27% は侵害された電子メール アカウントから開始されています。侵害された電子メールが発端のフィッシング攻撃が全体の 20% だった 2018 年の第 4 四半期から 7% のアップです。

ターゲットになっているのは Office 365 だけではありません。同様のフィッシング攻撃は、Google 社のクラウド電子メール サービスである Gmail や G Suite など、他のクラウドベースの電子メール サービスでも確認されています。Google アカウントが広く普及し、インターネット全域のさまざまな Web サイトへのログインに利用されていることを考えると、攻撃者が Google 関連のフィッシング サイトを作成しているのも頷けます。

同様のフィッシング攻撃は、Gmail や G Suite など他のクラウドベースの電子メール サービスでも確認されている

図 2　フィッシング サイトは Microsoft のサインイン ページに意図的に似せて作られている

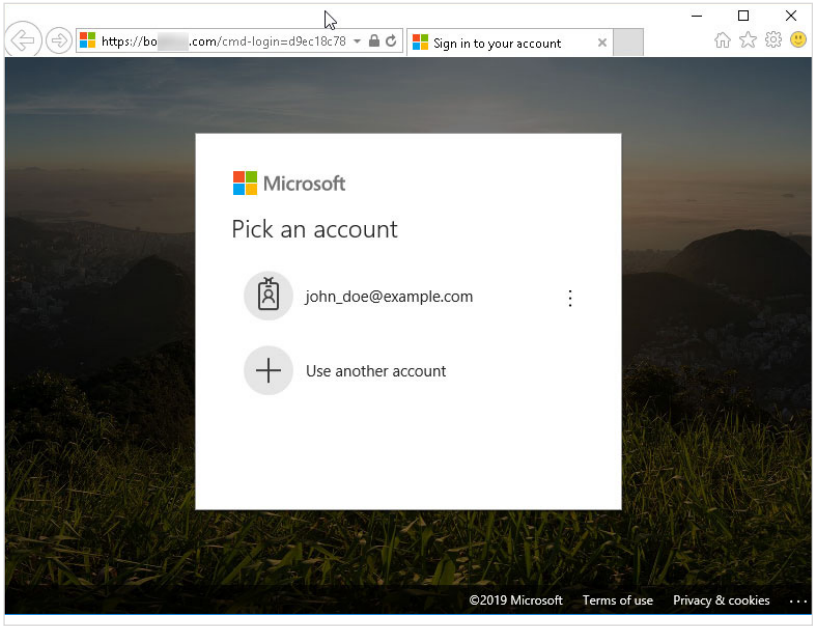
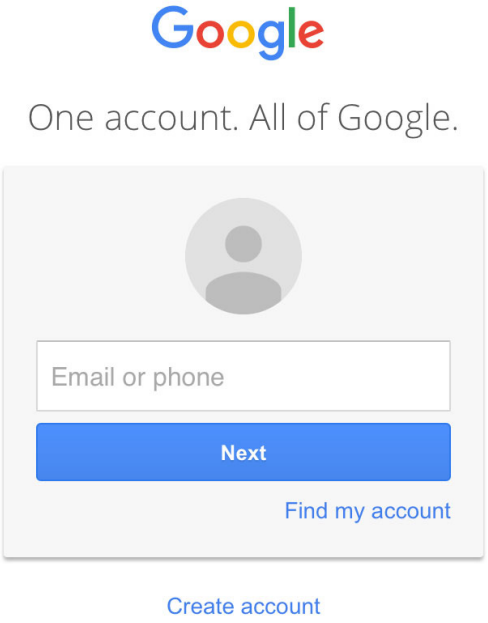


図 3　Google アカウントのログイン例。本物と偽物を見分けられますか。



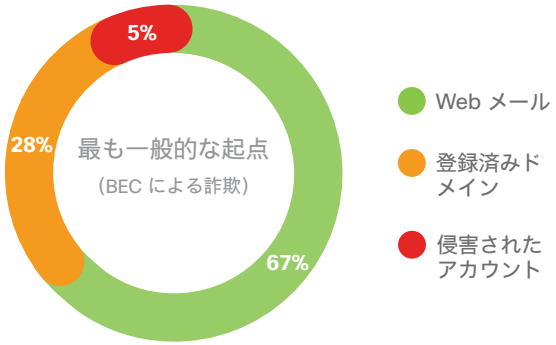
ビジネス メール詐欺

さて、今週は会社の大きな会議があり、重要な業務の継続に必要な数名を除いて全員が会社にいません。あなたは財務チームのメンバーで、必要最低限の社員として会社に残っています。突然、CFO からと思われる「支払い不履行」という件名の電子メールが受信トレイに届きました。電子メールの説明によると、先週実行するはずだった支払いができなかったために、会社のサプライ チェーンが中断する可能性があるようです。電信送金の手順が記載されたファイルが添付されています。送信者は最後に、この件に関して 1 時間以内に電話すると伝えています。

これはよくあるビジネス メール詐欺(BEC)です。BEC による詐欺は電子メール詐欺の一種です。攻撃者は最高責任者レベルの経営幹部を装い、受信者をだまして「職務の一環として」不正行為(不正にお金を振り込ませるなど)に加担させようとします。実際に電話もかけてきて経営幹部になりすますこともあります。これが意外と成功しているようです。インターネット犯罪苦情センター(IC3)によると、BEC 詐欺による 2018 年の損失は 13 億米ドルに達しました。

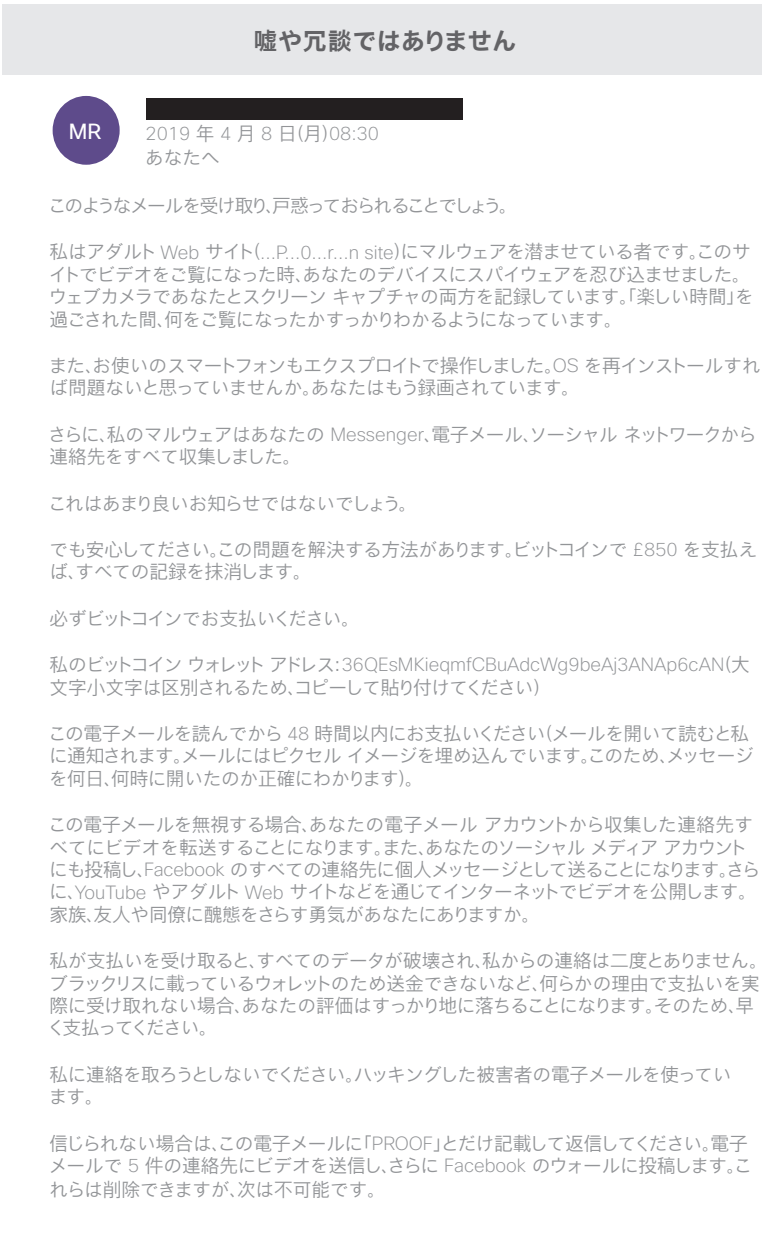
Office 365 フィッシング詐欺と同様に、BEC でも攻撃者は侵害されたアカウントを利用していると思われるでしょう。驚くべきことに、Agari Q2 2019 Email Fraud and Identity Deception Trends レポートによると、侵害されたアカウントを使っているのはこれら詐欺の約 5% のみです。このような攻撃の 3 分の 2 は依然として無料の Web メール アカウントを使って攻撃を開始していますが、残りの 28% は登録済みドメインを使って攻撃をカスタマイズして作成しています。カスタマイズした攻撃のパーソナライズは電子メールの本文にまで及んでいます。Agari によると、BEC 電子メールの 5 件のうち 1 件にターゲットの受信者の名前が含まれています。

図 4　BEC 電子メールの起点。



出典: Agari Data, Inc.

図 5　最近のデジタル恐喝の例


嘘や冗談ではありません

MR [redacted]
2019 年 4 月 8 日(月)08:30
あなたへ

このようなメールを受け取り、戸惑っておられることでしょう。

私はアダルト Web サイト(...P...0...r...n site)にマルウェアを潜ませている者です。このサイトでビデオをご覧になった時、あなたのデバイスにスパイウェアを忍び込ませました。ウェブカメラであなたとスクリーン キャプチャの両方を記録しています。「楽しい時間」を過ごされた間、何をご覧になったかすっかりわかるようになっています。

また、お使いのスマートフォンもエクスプロイトで操作しました。OS を再インストールすれば問題ないと思っていませんか。あなたはもう録画されています。

さらに、私のマルウェアはあなたの Messenger、電子メール、ソーシャル ネットワークから連絡先をすべて収集しました。

これはあまり良いお知らせではないでしょう。

でも安心してください。この問題を解決する方法があります。ビットコインで £850 を支払えば、すべての記録を抹消します。

必ずビットコインでお支払いください。

私のビットコイン ウォレット アドレス:36QEsMKieqmfCBuAdcWg9beAj3ANAp6cAN(大文字小文字は区別されるため、コピーして貼り付けてください)

この電子メールを読んでから 48 時間以内にお支払いください(メールを開いて読むと私に通知されます。メールにはピクセル イメージを埋め込んでいます。このため、メッセージを何日、何時に開いたのか正確にわかります)。

この電子メールを無視する場合、あなたの電子メール アカウントから収集した連絡先すべてにビデオを転送することになります。また、あなたのソーシャル メディア アカウントにも投稿し、Facebook のすべての連絡先に個人メッセージとして送ることになります。さらに、YouTube やアダルト Web サイトなどを通じてインターネットでビデオを公開します。家族、友人や同僚に醜態をさらす勇気があなたにありますか。

私が支払いを受け取ると、すべてのデータが破壊され、私からの連絡は二度とありません。ブラックリスに載っているウォレットのため送金できないなど、何らかの理由で支払いを実際に受け取れない場合、あなたの評価はすっかり地に落ちることになります。そのため、早く支払ってください。

私に連絡を取ろうとしないでください。ハッキングした被害者の電子メールを使っています。

信じられない場合は、この電子メールに「PROOF」とだけ記載して返信してください。電子メールで 5 件の連絡先にビデオを送信し、さらに Facebook のウォールに投稿します。これらは削除できますが、次は不可能です。

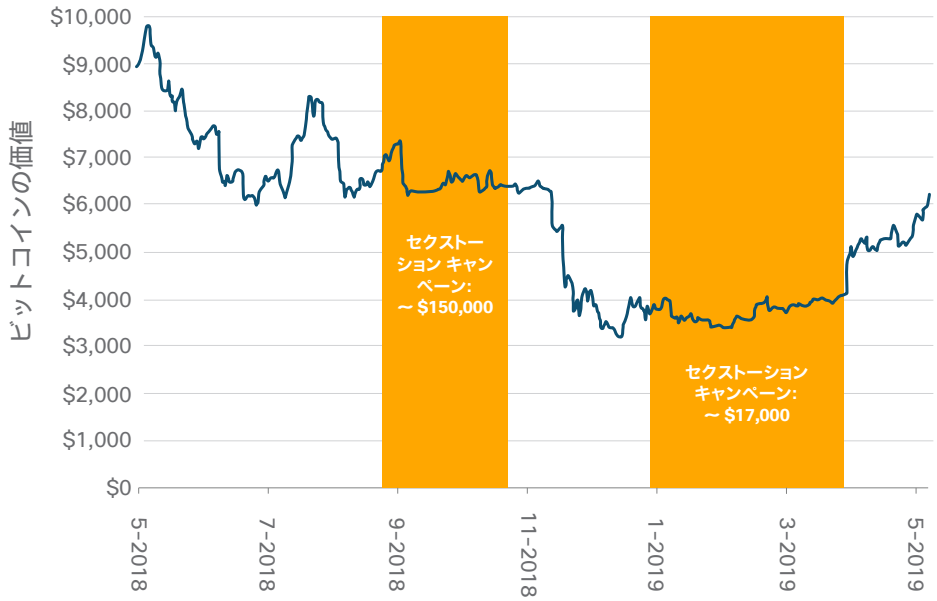
デジタル恐喝

件名に「嘘や冗談ではありません」と表示された電子メール**が受信トレイに届いています。**電子メールの送信者は、自分が侵害しているアダルト ビデオの Web サイトにあなたがアクセスしたと言っています。また、あなた自身と、あなたが見ていたビデオをウェブカメラで録画したとも言っています。さらに、あなたの連絡先リストを入手しており、ビットコインで数百ドル(数千ドルではない)支払わなければ、録画した内容をその連絡先に送信すると言っています。

これはデジタル恐喝です。従来の恐喝シナリオと唯一異なるのは、言っていることがすべて嘘だという点です。詐欺師は Web サイトを侵害していなければ、録画もしておらず、連絡先リストも持っていません。あなたをだまして信じ込ませようとしているだけです。

このタイプの電子メール詐欺のさまざまな形式については、今月の脅威のブログ記事、デジタル恐喝:脅迫対象が身体的安全にまで及び始めるで説明しています。

図 6　ビットコインの価値（USD）とセクストーション キャンペーンの被害額の比較



出典: Cisco Talos

これは注目されている手口で、攻撃者にとって大きな収益源になっています。デジタル恐喝キャンペーンによる被害額は 2018 年の終わりに数十万ドル規模に達しました。ただし、Cisco Talos が実施した最新の分析によると、2019 年 1 月～ 3 月にかけては被害額が減少しています。これら被害額の上昇と減少は、例外的な落ち込みもありますが、ビットコインの価値と緩やかに連動しています。現在ビットコインの価値は上昇していますが、デジタル恐喝の支払いにも同じことが起こるかどうかが今後注目されます。

「パッケージと請求書」型のスパム

「こんなモバイル アプリのサブスクリプションなんて購入した覚えはないのに」と言いながら電子メールを読んでいます。電子メールによると、ムービー クラブのライフタイム サブスクリプションを購入したことになっています。しかし請求書に記載されている場所を見ると、スリランカで購入しています。スリランカになど住んでいません。「何かの間違いのはず」と、添付されている PDF をすぐに開いて調べようとします。

この PDF にはエクスプロイトが含まれており、最終的に Emotet がデバイスにダウンロードされてしまいます。手口はさまざまですが、注文していないパッケージ、購入していない何かの請求書、登録していない月払いのサブスクリプションやサービスをかたるものがほとんどです。これは、銀行のクレデンシャル情報の盗難やクリプトマイニングなど、あらゆる被害につながる可能性があります。

図 7　UPS からのメールを装った Emotet 詐欺メール

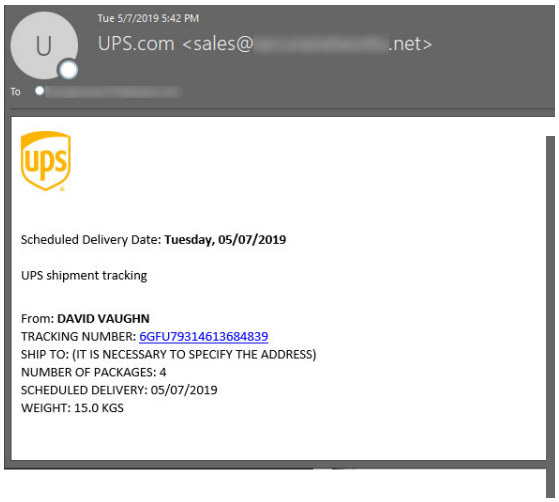


図 8　最近の前払い詐欺の例。

Mr. Christoper A. Wray

CW　連邦捜査局(FBI)長官
受信者: [redacted]
返信先: [redacted]

受益者宛て

オフィスの倫理規範によると、連絡時は常に最初が肝心です。私は、連邦捜査局(FBI)長官の Christopher A. Wray です。この公式の覚書は、米国政府に勤務している一部の職員が不正な手段であなたの資金を流用しようとし、それが発覚したことをお知らせするものです。このことは、容疑者を逮捕した後、連邦捜査局(FBI)の懲戒部に属す秘密諜報員を通じて、本日明らかになりました。

この容疑者は、今朝早く、多額の現金を国外に持ち出そうとしていたところ、ダレス国際空港で逮捕されました。米国のマネー ロンダリング法令により、このような大金を現金で国外に持ち出すことはできません。米国 1982 年マネー ロンダリング法に基づいて、このような企ては犯罪行為であり、処罰の対象になります。この法令はほとんどの先進国で世界的に適用される法律であり、テロとマネー ロンダリングの撲滅を目的としています。

同部で収集された情報から、問題となっている資金が実際にはあなたのものであることが判明しましたが、支払いを担当する職員が倫理規範に対処しているため支払いが遅れています。現在のところ、この資金は支払い銀行で管理されており、この問題で私たちに誠実に対応していただければ、滞りなくあなたにお返しすることができます。また、今日の社会に潜む犯罪者の関与を回避するために、この取引は厳重に監視されており、あらゆる段階であなたの積極的な協力が必要です。

当該資金が本当にあなたに帰属していることを証明する貴重な記録があるため、本日、2019 年 5 月 9 日付けで、支払い銀行の経営管理担当者に当該資金を当該認定受益者としてあなたに支払うように指示しました。いずれにしても、以下に示す情報を提供していただく必要があります(正式な検証のため)。

1. ファースト ネーム、ミドルネーム、ラスト ネーム
2. 年齢
3. 職業
4. 婚姻状況
5. 直通電話/ファックス番号
6. 住所

この正規の義務にただちに従ってください。これにより、認可された支払い銀行による支払いを受けられるようになります。

公式文書。

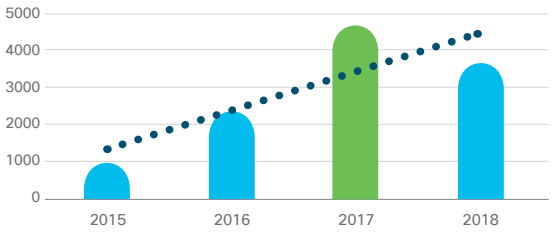
Mr. Christopher A. Wray
連邦捜査局(FBI)長官

前払い詐欺

FBI から電子メールが届くことなどそうそうありません。ましてや、1,050 万ドルの送金指示が保留になっていることを知らせる電子メールなどめったにありません。電子メールに返信さえすれば、支払いを受け取るために必要な手順を知らせると言っています。

これは典型的な前払い詐欺です。名前が示すように、攻撃者は、約束されたお金(決して受け取れない大金)を送金する前に手数料を要求します。これは以前からある電子メール詐欺のひとつですが、長年にわたって形が変化しています。自分の財産を分け与えたい外国の王族から、信用情報に問題がある人へのローンの承認など、さまざまな手口があります。このような電子メール詐欺は今でもあり、毎年、数千件が米国の Better Business Bureau(BBB)に報告されています。

図 9　BBB に報告された前払い詐欺の年別件数。
(ローン等保証金支払いに対する債務不履行、ナイジェリア/外国為替、ロマンス詐欺、クレジット信用情報回復/債務救済、投資、旅行/休暇詐欺タイプ カテゴリの合計)



出典: Better Business Bureau

電子メールのマルウェア

マルウェアの大部分は、今も電子メールで配布されています。以前はもっとわかりやすく、電子メールに .exe ファイルが直接添付されていました。しかし、添付されている実行可能ファイルをむやみに開くのは危険だとユーザが気付くようになったため、悪意のある攻撃者は戦術を変えました。

最近では、間接的にマルウェアを配布することが多くなっています。一般的なビジネス文書といった疑われにくい添付ファイルや、メッセージ本文に含まれている URL が使われています。これらはすべて、普通の電子メール通信でよく送られるものばかりです。これは、バイナリファイルや希に使用される種類の添付ファイルを検出する従来の電子メール スキャンをすり抜けるのが目的です。

この点は、今年に入って(2019 年 1 月 ～ 4 月)疑わしいと判断された電子メールの添付ファイルを見るとよくわかります。バイナリ ファイルは、悪意のある添付ファイル全体の 2% 未満です。これは .exe ファイルだけでなく、すべてのバイナリを含みます。実行可能ファイル、Java、および Flash が定期的に検出されていた数年前からかなり変化しています。Java と Flash は人気が衰退し、バイナリと合わせても添付ファイル全体のわずか 1.99% です。

.zip ファイルなどのアーカイブは悪意のある添付ファイルの約 3 分の 1 を占め、よく使われる上位 10 タイプのファイルのうち 4 つがこのタイプです。

表 1　悪意のある添付ファイルのタイプ

タイプ	パーセンテージ
Office	42.8%
アーカイブ	31.2%
スクリプト	14.1%
PDF	9.9%
バイナリ	1.77%
Java	0.22%
フラッシュ	0.0003%

出典: Talos Intelligence

最も一般的な添付ファイルの種類は、オフィスで日常的に送られているタイプばかりです。悪意のある 5 つのファイル タイプのうち 2 つが Microsoft Office ドキュメントです。

では、攻撃者の注目が集まっているのはどのような添付ファイルなのでしょうか。添付ファイル全体のほぼ 3 分の 1 を占めるのが、.zip ファイルなどのアーカイブです。よく使われる上位 10 種類のファイルのうち 4 つがこのタイプです。.js ファイルなどのスクリプトは全体の 14.1% を占めています。これらのスクリプトは、悪意のある添付ファイルのタイプについて調べた前回の調査(2018 年の Annual Cybersecurity Report (ACR))から激増しています。前回の時点で、.js ファイルは XML および HTML と合わせても全体のわずか 1% でした。

スクリプトが悪意のある添付ファイルとして使われる頻度は増え続けており、2018 年と比べてほぼ 5% の上昇となりました。スパムで使われる PDF ドキュメントの数も踏まえると、悪意のある添付ファイルの半数以上が、現代の職場で普通に使われているドキュメント タイプだと言えます。

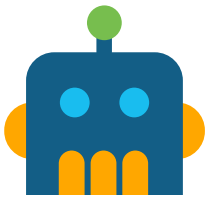
表 2　電子メールの悪意のある拡張子上位 10。

拡張子	パーセンテージ
.doc	41.8%
.zip	26.3%
.js	14.0%
.pdf	9.9%
.rar	3.9%
.exe	1.7%
.docx	0.8%
.ace	0.5%
.gz	0.5%
.xlsx	0.2%

出典: Talos Intelligence

電子メールの配信インフラストラクチャ

次は、電子メールのタイプやペイロードから離れ、悪意のある電子メールが配信される様子を見てみましょう。詐欺師がスパム キャンペーンの開始で主に使う方法には、ボットネットとバルク電子メール ツールキットの 2 つがあります。



ボットネット

スパム ボットネットは、現在送信されているスパムの大半で主な手段として圧倒的に多く使われています。有名なスパム ボットネットには以下があります。

Necurs

Necurs ボットネットは 2012 年に初めて登場し、ゼウスからランサムウェアに至るまで、さまざまな脅威を拡散してきました。過去の活動はかなり注目を集めましたが、少なくともメディアに取り上げられる頻度で言えば、Necurs の影は薄くなっているように思われます。ただし、このボットネットは依然としてかなり活発です。実際、Necurs ボットネットは、デジタル恐喝を含むさまざまな詐欺で主に使われている配布手段です。

Necurs の詳細については、Cisco Talos による分析、多方面に触手を伸ばす Necurs ボットネットをご覧ください。

Emotet

Emotet によって送信されるスパムの多くは、「パッケージと請求書」タイプに分類されます。Emotet はモジュラ型マルウェアで、スパムボット プラグインが含まれています。Emotet を操る攻撃者は、他の脅威を配布するチャネルとして Emote を使うことでお金を手に入れています。つまり、Emote から送られる大半のスパムの目的はより多くのシステムを感染させ、悪意のある配布チャンネルの到達範囲をさらに拡張することです。

Emotet は被害者のメールボックスからコンテンツを盗むため、多くの場合、受信者にはこれまでの会話の一部のように思わせつつ、悪意のある（ただし本物に見える）スレッド メッセージを作り上げることができます。また、Emotet は SMTP クレデンシャルを盗み、被害者の送信メール サーバをスパムの送信手段として勝手に使うことでも知られています。

Emotet の詳細については、サイバーセキュリティ レポート シリーズの前回の脅威レポート、今日の重大な脅威から防御するをご覧ください。

> **「Cisco E メール セキュリティにより、検出にかかる時間が減ったほか、スパムも約 80% 減少しました」**
>
> **フロリダ州サラソータ市、セキュリティ責任者、Jacquelyn Hemmerich 氏**

Gamut

Gamut ボットネットは、近くに住む人とのデートや親密な関係に誘う内容を中心とするスパムを拡散し続けています。他にも、医薬品や求人関連のメッセージを送るキャンペーンなどがあります（図 10 を参照）。

さまざまなドメインを登録していますが、インフラストラクチャ自体はかなりシンプルです。多くの場合は 1 つのドメインの下に複数のサブドメインがあり、使われる IP アドレスは同じです。提供されているサービスが正当かどうかをシスコでは確認していませんが、登録プロセスは個人情報のフィッシングが目的のように見えます。

図 10 Gamut ボットネットから送信されたスパム メール。

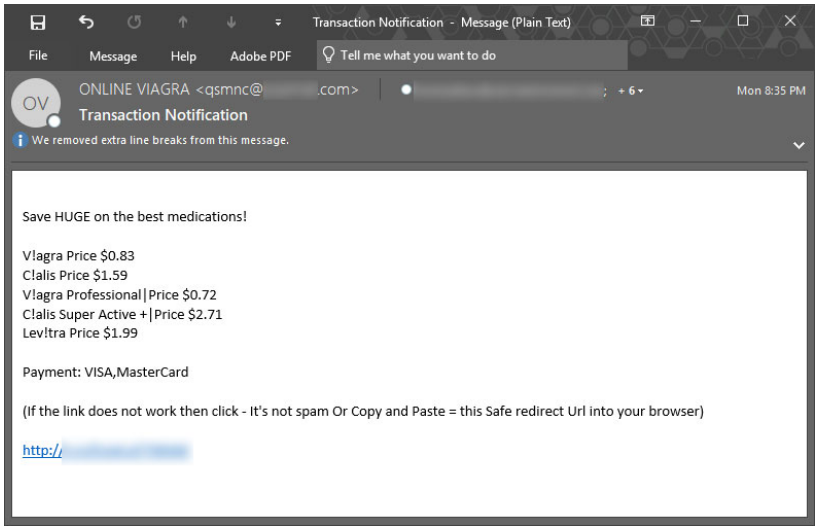
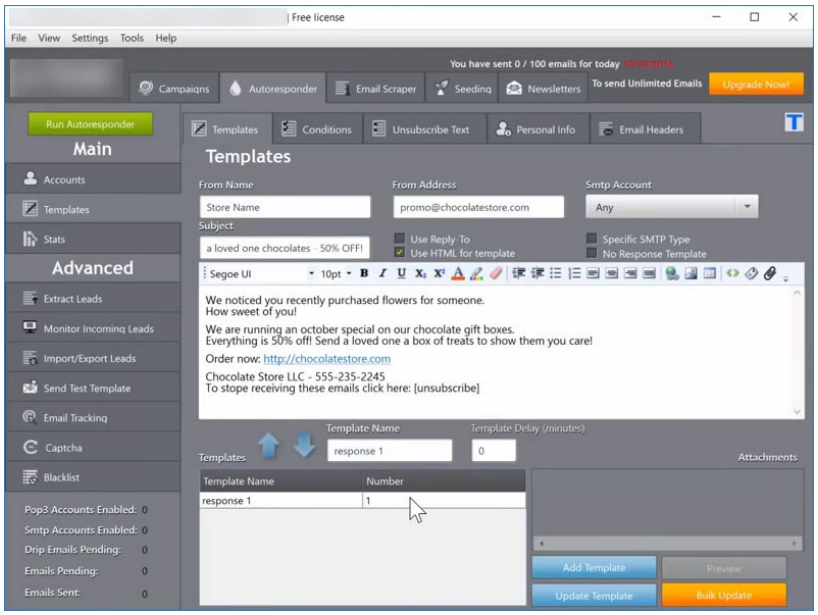


図 11 スパム ツールキットの例。



バルク電子メール ツールキット

多くのスパム送信者は別の手段として、大量の電子メールを送信するツールキットを購入して利用しています。これらのツールの多くは半分合法です。ハンドメイドのオーダー シャワー カーテンを販売している場合、技術的にはこれらツールキットを利用してオプトイン メーリング リストを作成し、バルク電子メール送ることでブランドの認知度を高めることができます。ただし、このようなツールキットに含まれる、ユニークなハッシュ値を生成するために送信元 IP アドレスをローテーションする機能や添付ファイルをカスタマイズして再作成できる機能などが合法的なシナリオで使われることはあまりありません。

Cisco Talos では最近、悪意のある攻撃者がバルク電子メール ツールと、データ漏洩で得られたと思われる大量の電子メール アドレスのリストを販売している Facebook グループを発見しました。これらの購入者は、各ツールを明らかに不正な目的のために使っていました。

手段としての詐欺

電子メールは手段に過ぎず、ほどんどの目的は詐欺です。組織犯罪では特にそう言えます。

電子メールは手段に過ぎず、ほどんどの目的は詐欺です。組織犯罪では特にそう言えます。BEC を仕掛けている悪意のある攻撃者は、企業から何千ドルも詐取しようとしています。デジタル恐喝者は、ユーザをだましてビットコインを不正に得ようとしています。また、前払い詐欺はその名の通りです。

目新しいものはありません。電子メールは犯罪者が不正を犯すために使っている最新ツールの 1 つにすぎません。これまでも犯罪者は、各世代のテクノロジーの隙をつくことで得られる不正な利益をできるだけ多く得ようと必死でした。

ドイツ連邦警察(Bundeskriminalamt BKA)と FBI で記録されている損失を見ると、記録がある全サイバー犯罪の損失の 80% 以上が詐欺の追跡に起因する可能性があります。損失には正確な定量化と記録が難しい実体のないものがあるため、この「記録されている」点が重要です。つまり、記録されている統計情報がかなり信頼できるものであることを意味します。

詐欺がサイバー犯罪の損失の最大の要因であるというのは正しいと言えます。実際、FBI の統計情報で指摘されている 2 つの詐欺手法、つまり、ビジネス メール詐欺(BEC)と電子メール アカウントの侵害(EAC)について調査したところ、2018 年の損失は 13 億ドルでした。また、何度も言及しているサイバー犯罪に関する分析フォームによると、ランサムウェアについて記録された同等の損失は 360 万ドルでした。各徴候を見る限り、検出されていない詐欺に関連する損失は増加し続けるという事実に変わりはありません。BEC/EAC に関連する損失は、2016 年と 2017 年の間だけで 78% も上昇しています。

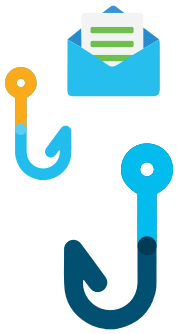
「Cisco E メール セキュリティにより、管理業務から電子メール セキュリティの負担がなくなり、他の分野に注力できるようになりました。このソリューションは、あらゆる脅威を捉えてくれます。電子メールのセキュリティに関して正しい選択ができたことで安心しています」

Technology Concepts & Design, Inc. 社 シニア IT アーキテクト Steven Wujek 氏

詐欺およびサイバー犯罪の損失の詳細については、サイバー犯罪と詐欺に関するシスコのブログ シリーズをご覧ください。

「セキュリティに対する包括的なアプローチとは、セキュリティ製品の問題やビジネス上の重要課題を対象にするだけではありません。ビジネス全域の人、プロセス、テクノロジーが対象になります。シスコでは、個人や個人が実行する業務を安全に行えるよう支援することに焦点を当てた、人を中心としたアプローチから始めます。その方法の 1 つは、従業員が疑わしい電子メールをクリックする前に、それを認識して報告できるようになるための実践的なヒントを提供することです」

シスコ、最高情報セキュリティ責任者、Steve Martino



電子メール攻撃から保護する方法

フィッシング メールの明らかな兆候

電子メールで配布される脅威に関しては、それが脅威であることを示す矛盾した点が必ずあるため、どこを見ればよいかわかっていれば簡単に見分けられます。次に例を示します。それぞれの詳細については、次のページを参照してください。

宛先：you@youremail.com

1 送信元：Amazon Shipping <amz@123fnord.com>

件名：お注文について

拝啓

2 注文してありがとうございました。詳細は次のとおりです。

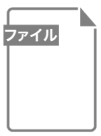
購入品：Puppy Food™ の毎月定期購入
メーカー Puppy Food
月額コスト：121 米ドル
日時：2019 年 5 月 3 日 10:21
IP アドレス：254.189.234.159.01
購入国：グアテマラ

3 購読を希望されない場合は、以下の手順に従ってすぐにキャンセルしてください。または、

4 クレジット カード情報を以下にご入力ください。

5 http://badphishingsite.com/dontgothere.html

どうぞよろしくお願い申し上げます。
Amazon Shipping



6 **dontopenthisis.bad**

図 12 開いているドキュメントのマクロに関する Microsoft Office の警告。

1. **送信元:のアドレス。**送信元のアドレスに記載されている名前と電子メール アドレスが一致していない。
2. **スペルと文法の間違いが多く、ロゴがぼやけている。**電子メールが適当に作成されているように見える場合は、正当なメールではない可能性がある。
3. **切迫感がある。**すぐに対処するように要求される場合、切迫感が感じられる場合、好奇心をあおっている場合は、かなり疑わしい。
4. **個人情報または機密情報を要求する。**個人、財務、機密情報を求める迷惑メールには返信しない。
5. **不正に見える URL。**多くのフィッシング電子メールの URLはよく見ると変なところがあるため、クリックしないこと。URL がテキスト リンク内に表示されていない場合は、カーソルを合わせてブラウザの下部で確認する。怪しい場合はクリックしない。
6. **認識されていないファイル タイプ。**ほとんどの会社で、これまでに電子メールで送信しているファイル タイプは数種類のみ。見たことのないファイル タイプの場合は開かないこと。

また、次の点に注意してください。

- **ゆっくり行動する。**平均的な人で、電子メールに目を通してから行動に移るのに 8 ~ 10 秒です。ゆっくりと目を通し、フィッシング攻撃を示す手がかりがないか探します。
- **あまりにも「うまい話し」には裏があると考える。**何百万ドルもくれると書かれていませんか。恥をかかせる、傷つけると脅していませんか。おそらくまったくの嘘です。
- **警告には細心の注意を払う。**送信者を知っていて添付ファイルを開く場合は、有効にする必要がある拡張機能やマクロに関するバナーの警告に細心の注意を払ってください（図 12）。表示されていたとしても、これが必要になることはほどんどありません。

攻撃予防戦略

電子メールの脅威がもたらすリスクを軽減するために実行できるアプローチは複数あります。

フィッシング訓練を定期的に実行します。フィッシング、特にかなりカスタマイズされたフィッシング攻撃に対しては、従業員が最大の防御策になります。従業員が明らかなフィッシング攻撃を見分けられるようになると、エンドポイントの侵害で最も多い原因を阻止できます。

認識力を高めるには、会社で定期的なフィッシング訓練を実施し、ユーザをテストして指導します。実際に使われている最新の手法をエミュレートし、直面するかもしれない最新の手口をユーザに知らせます。シスコでは、これらの訓練を毎月実行することを推奨しています。まずは簡単なフィッシング キャンペーンのテストから始め、徐々に難易度を高めるようにしてください。模擬のフィッシング攻撃(例:フィッシングに関する詳しい情報が記載されたテスト用の「悪意のある」URL を送るなど)に引っかかったユーザには、すぐに指導を行います。組織内で危険度が高く、策略に引っかかると深刻な損害が生じる可能性があるユーザについては、フィッシング キャンペーン対策としてカスタマイズしたトレーニングを実施します。

多要素認証を利用します。企業の電子メール アカウントのクレデンシャルが盗まれた場合でも、多要素認証を利用していれば、アカウントへのアクセスを狙う攻撃者を阻止できます。

多要素認証の利点はそのシンプルさです。たとえば、誰かがあなたの、または同僚のログイン クレデンシャルを入手し、ログインを試みているとします。多要素認証では、クレデンシャルを所有しているユーザにメッセージを自動的に送信し、たった今ログインを試みたか確認します。これにより、不正なログイン試行はすべて確認して完全に拒否できます。これで攻撃は阻止されます。

ソフトウェアを最新に保ちます。場合によっては、悪意のある URL を含む電子メールが、エクスプロイトのあるページにユーザを誘導することがあります。ブラウザやソフトウェア、プラグインを最新に保つことは、このような攻撃によってもたらされるリスクを軽減できます。

知らない人には絶対に送金しないでください。これにより、前払い詐欺と BEC による詐欺を防げます。要求について疑わしい点がある場合は、返答しないでください。特に BEC については、電信送金の場合は上司などの承認を必要とする厳格なポリシーを用意し、代理の署名者を指名してください。

ログインの要求には注意してください。ログイン クレデンシャルを盗もうとする悪意のある攻撃者は、ユーザの使い慣れたログイン ページを作成するためならあらゆる手口を使います。ログイン プロンプトが表示された場合は、必ず URL を見て、正規の所有者のサイトであることを確認してください。ポップアップ スタイルのウィンドウが表示される場合は、ウィンドウを広げて完全な URL、または少なくとも完全なドメインが見えるようにしてください。

電子メールが信頼できる内容であることを確認します。デジタル恐喝や前払い詐欺などの場合、正当な電子メールであると納得させるために、送信者が手の込んだストーリーを作り上げることがよくあります。シナリオの説明に矛盾はありませんか。技術面、財務プロセスの観点、またはその他の点からストーリーに何か穴はありませんか。ある場合、疑いを持って対応してください。

備えを固める

電子メールによる脅威では、返信させる、URL をクリックさせる、添付ファイルを開かせるために、あの手この手でユーザをだまし、誘惑しようとします。このため、悪意のある電子メールを捉えて隔離し、スパムをフィルタリングできる電子メール セキュリティ ソフトウェアを利用することが正しい対策になります。

電子メール セキュリティを利用している組織の割合は、残念ながら減少しています。最新の CISO ベンチマーク調査によると、組織を危険にさらす脅威の手段の第 1 位は電子メールだと報告されていますが、脅威に対する防御の方法として電子メール セキュリティを利用している組織は調査対象の 41% に過ぎません。電子メール セキュリティを利用している組織が 56% だった 2014 年からダウンしています。

この低下には考えられる原因がいくつかあります。ひとつはクラウドへの移行です。シスコの依頼で ESG 社が実施した最近の調査によれば、回答者の 80% 以上がクラウドベースの電子メール サービスを組織で利用しています。クラウドでホストする電子メール サービスを選ぶ組織が増えるにつれ、オンサイトの専用電子メール アプライアンスは必要とされなくなっています。一部の IT チームは、それらが不要だと考えているためです。

多くのクラウド電子メール サービスでは基本的なセキュリティ機能が提供されていますが、何層も重ねた保護の必要性は非常に重要です。実際、ESG 社が実施した同じ調査では、クラウドベースに移行した回答者の 43% が、電子メールの防御にはクラウドのセキュリティ機能だけでは不十分だと実感したと述べています。結局のところ、IT チームにはポリシーの設定、可視化と制御、サンドボックスの利用、外部の遮断機能の活用といった対応が依然として求められています。

セキュリティ チームが現在直面している別の問題は、攻撃対象領域が広がり、保護が必要なエリアが増えていることです。脅威の増加にセキュリティ予算が追いついていない場合、チームは大きな攻撃対象領域をカバーするためにいつのまにか一部のリソースを縮小していることがあります。

電子メールが最も一般的な脅威の手段であることを考えると、電子メール保護の重要性を強調しすぎることはできません。サイバー リスクの評価では、最も重要なエントリ ポイントにおける防御態勢とリスク管理システムが大きなウエイトを占めます。その他については、侵害が発生した場合の組織への攻撃とリスクの可能性の大きさを基準に徐々に順位を下げていきます。次に、潜在的な損失の危険度に合わせてリソースを割り当てます。

また Gartner 社は、フィッシング攻撃に対する防御を高める方法として、セキュリティおよびリスク マネージャ(SRM)に次の 3 方向アプローチを実践するように提案しています。

1. セキュアな電子メール ゲートウェイおよびその他のコントロールをアップグレードし、フィッシングに対する保護を向上させる。
2. 従業員をソリューションに組み込み、疑わしい攻撃を検出して対応する能力を強化する。
3. ビジネスマネージャと連携し、機密データと財務トランザクションの処理に関する標準的な操作手順を作成する。

電子メール攻撃から組織を保護する方法

これまでは、フィッシング メールの明らかな兆候と、攻撃を防御する方法についてご説明しました。ここでは、2019 年の電子 メール セキュリティ テクノロジーで予想されることについて解説します。

電子メールベースの攻撃に対して組織を防御するには、これまでのように階層型のアプローチによるセキュリティが不可欠です。十分な試行を重ねた複数の電子メール セキュリティ機能があり、現在も大いに役立っています。

例:

- 迷惑メールや悪意のあるスパムを受信トレイから除外するには、今もスパム防御が必要です。
- マルウェアや URL のブロック機能などの電子メール脅威防御は、電子メール内の悪意のあるリンクに対抗する URL インテリジェンスに加えて、添付ファイルに含まれるマルウェア、スペア フィッシング、ランサムウェア、クリプトマイニングのブロックで不可欠です。
- 統合サンドボックスは、電子メールで到着した新しいファイルに悪意があるかどうかをすばやく理解するためにバックグラウンドで自動的に実行されます。

脅威の状況は絶えず進化し、悪意のある攻撃者は攻撃を仕掛けるための新たな方法を常に探しているため、どれほど対策を取っても十分すぎることはありません。

絶え間なく変わる状況に対応できるようにするには、十分な試行を重ねた機能に加えて、次のセキュリティ テクノロジーが役立ちます。

- 高度なフィッシング攻撃をブロックするために、機械学習を使って電子メールの身元と行動の関係を理解して認証する、より高度なフィッシング保護機能が登場しています。
- DMARC ドメイン保護を有効にし、フィッシング キャンペーンで攻撃者が本物の企業ドメインを使えないようにすることで、企業のブランドを保護できるようになりました。
- メッセージの隔離機能は、メッセージを保留にして添付ファイルを分析してから、受信者に送信する、悪意のある添付ファイルを削除する、メッセージを完全に削除することができるため便利です。
- 電子メール修復は、受信者に配信した後に悪意のあるファイルであることが検出された場合、悪意のある添付ファイルがあるメッセージをメールボックスから隔離し直せるため便利です。
- STIX の外部電子メール脅威フィードが電子メール セキュリティ製品で広く使われるようになりました。製品に元々ある脅威インテリジェンス以外の特定業種向けの脅威フィードを利用したい組織に便利です。
- 高度なマルウェアまたはメッセージが送り付けられている環境内の特定のユーザや受信トレイを把握しようと、電子メール セキュリティと幅広いセキュリティ関連機能の統合が広まっています。

「シスコは、2019 年 Forrester Wave のエンタープライズ電子メール セキュリティ分野でリーダーに選出されました。導入オプション、攻撃に対する保護、電子メール認証、パフォーマンスと運用（拡張性と信頼性を含む）、テクノロジーのリーダーシップで最高評価を受けています。」

The Forrester Wave™: Enterprise Email Security, Q2 2019

シスコ サイバーセキュリティ シリーズ

シスコは過去 10 年間にわたり、全世界のサイバーセキュリティの状態に関心を持つセキュリティ プロフェッショナルを対象とした、最も信頼のおけるセキュリティと脅威インテリジェンスに関する多くの情報を公開してきました。これらの包括的なレポートでは、脅威の状況や組織にとっての脅威の意味を詳しく解説するとともに、データ漏洩がもたらす悪影響から組織を守るためのベスト プラクティスを紹介してきました。

シスコのソート リーダーシップに対する新しいアプローチの中で、シスコ セキュリティはシスコ サイバーセキュリティ シリーズという旗印を掲げ、一連の調査とそのデータに基づく出版物を発行しています。シスコはそのタイトル数を増やし、それぞれに関心事の異なるセキュリティ プロフェッショナル向けのさまざまなレポートを提供してきました。セキュリティ業界の脅威研究者やイノベータに幅広い高度な専門知識を求めた 2019 年の一連のレポートには、データ プライバシー ベンチマーク調査、脅威レポート、CISO ベンチマーク調査などがあり、今後もいくつかのレポートが発表される予定です。

詳しい情報、およびすべてのレポートとアーカイブ コピーへのアクセスについては、https://www.cisco.com/c/ja_jp/products/security/security-reports.html を参照してください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

THRT_02_0519_r1JA　19.06