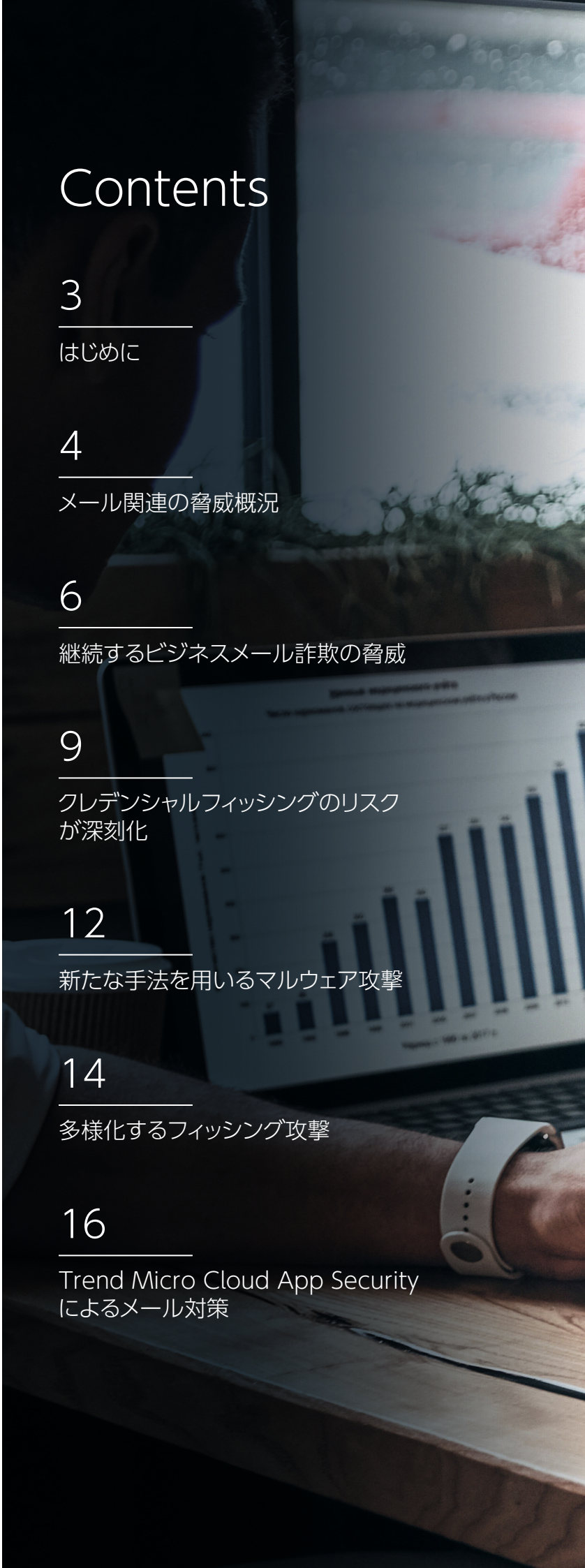
クラウドメールの法人組織を狙う「すり抜け」の脅威

2019年Trend Micro Cloud App Security レポート

TREND MICRO | research

Contents



トレンドマイクロの「Trend Micro Cloud App Security™ 」は、クラウドメールサービスに組み込まれたセキュリティをすり抜けた約1,270万件の高リスクのメール関連脅威を検出してブロックしました。本レポートでは、企業のセキュリティ対策の検討に役立つ情報として、2019年の注目すべきメール関連脅威の概況を解説します。

はじめに

クラウドコンピューティングは急速な成長を遂げながら[1]、近い将来さらに拡大すると考えられており、世界の市場は数年で2018年の2倍以上に成長すると予測されています[2]。特にメールアカウントが他の多くのファイルホスティングサービスやコラボレーションツールとつながって機能するようになった中、クラウドベースのビジネスメールにおいても同様の変化が見られたことは当然と言えるでしょう[3]。

このような変化とともにクラウドベースのプラットフォームやサービスを狙う脅威が規模と複雑さを増しており、サイバー犯罪者は特にクラウドメールサービスを標的として狙っています。企業のこうしたプラットフォームやサービスの利用増加に伴い、サイバー犯罪者は従来のソーシャルエンジニアリングや、巧妙なマルウェアの利用、さらには機械学習（AI）の分野の新技術までを悪用し[4]、さまざまな方法でユーザを攻撃してくるでしょう。

2019年はビジネスメール詐欺（BEC）[5]や認証情報を詐取するフィッシングメール（クレデンシャルフィッシング）など、メールの脅威が継続すると同時に、サイバー犯罪者は攻撃キャンペーンを効果的にするための新しい手法や戦略を展開してきました。

1 https://www.trendmicro.com/vinfo/us/security/news/security-technology/the-cloud-what-it-is-and-what-it-s-for

2 https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html

3 https://www.statista.com/statistics/497864/cloud-business-email-market/

4 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/foreseeing-a-new-era-cybercriminals-using-machine-learning-to-create-highly-advanced-threats

5 https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

メール関連の脅威概況

クラウド型セキュリティ技術基盤「Trend Micro™ Smart Protection Network™（SPN）」は、2019年に470億を超えるメール関連の脅威をブロックしました。これは前年比14%増となっています。さらに「Microsoft® Office 365™ Exchange™ Online」「OneDrive® for Business」「SharePoint®Online」「Gmail」「Google ドライブ」といったさまざまなクラウドベースのアプリケーションやサービスを保護するAPIベースのソリューション「Trend Micro Cloud App Security™」は、約1,270万件の高リスクのメール関連脅威を検出してブロックしました。

2019年はマルウェアに関連する検出台数はわずかに減少しましたが、フィッシングメールやビジネスメール詐欺関連の脅威は大幅に増加しています。

メール関連の脅威は減少したのではなくクラウドへと移行しています。そうした中、多くの企業はそれぞれセキュリティ対策を備えたクラウドベースのシステムを使用しています。「Microsoft Office 365 E3」「Microsoft Office 365 E5」の脅威対策サービスやGoogleのサービスに組み込まれたセキュリティサービスに頼る企業もいれば、サードパーティのメールゲートウェイを使用している企業もいます。Trend Micro Cloud App Securityの検出結果からは、膨大な数の脅威がこれらのセキュリティフィルタをすり抜けている現実が浮き彫りとなり、より強固な多層防御のアプローチの必要性が明らかになっています。

例えば、約8万人のOffice 365ユーザを持つ企業では、Microsoft内のメールセキュリティフィルタを通過した後にもかかわらず、Trend Micro Cloud App Securityが55万件以上の高リスクのメール脅威を検出しました。これは1人あたり平均7件の高リスクのメールの脅威が受信されることを意味しています。これらの大部分はフィッシング詐欺の攻撃であり、企業規模を考えると想定の範囲内ではあるものの、他方で懸念となるのは、2万7,000件を超えるビジネスメール詐欺も検出された点です。ビジネスメール詐欺の性質を考慮すると、たった1度の攻撃が企業に甚大な経済的損失をもたらす可能性があるためです[6]。

メール関連脅威は大企業のみならず、中小・中堅企業にも着弾することが予想されます。実際、約1,000人のGmailユーザを持つ企業でも、Trend Micro Cloud App Securityは3か月間で900件を超える高リスクのメール脅威を検出しました。これはユーザと脅威の比率がほぼ1：1となります。直面する脅威の件数自体は膨大ではないものの、多くの中小・中堅企業ではセキュリティに長けた人員やリソースの不足から、十分な対策を講じることが難しいという課題があるでしょう[7]。

---

[6] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fbi-report-global-bec-losses-exceeded-us-12-billion-in-2018

[7] https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/small-and-midsize-businesses-face-greater-cybersecurity-risks-and-challenges

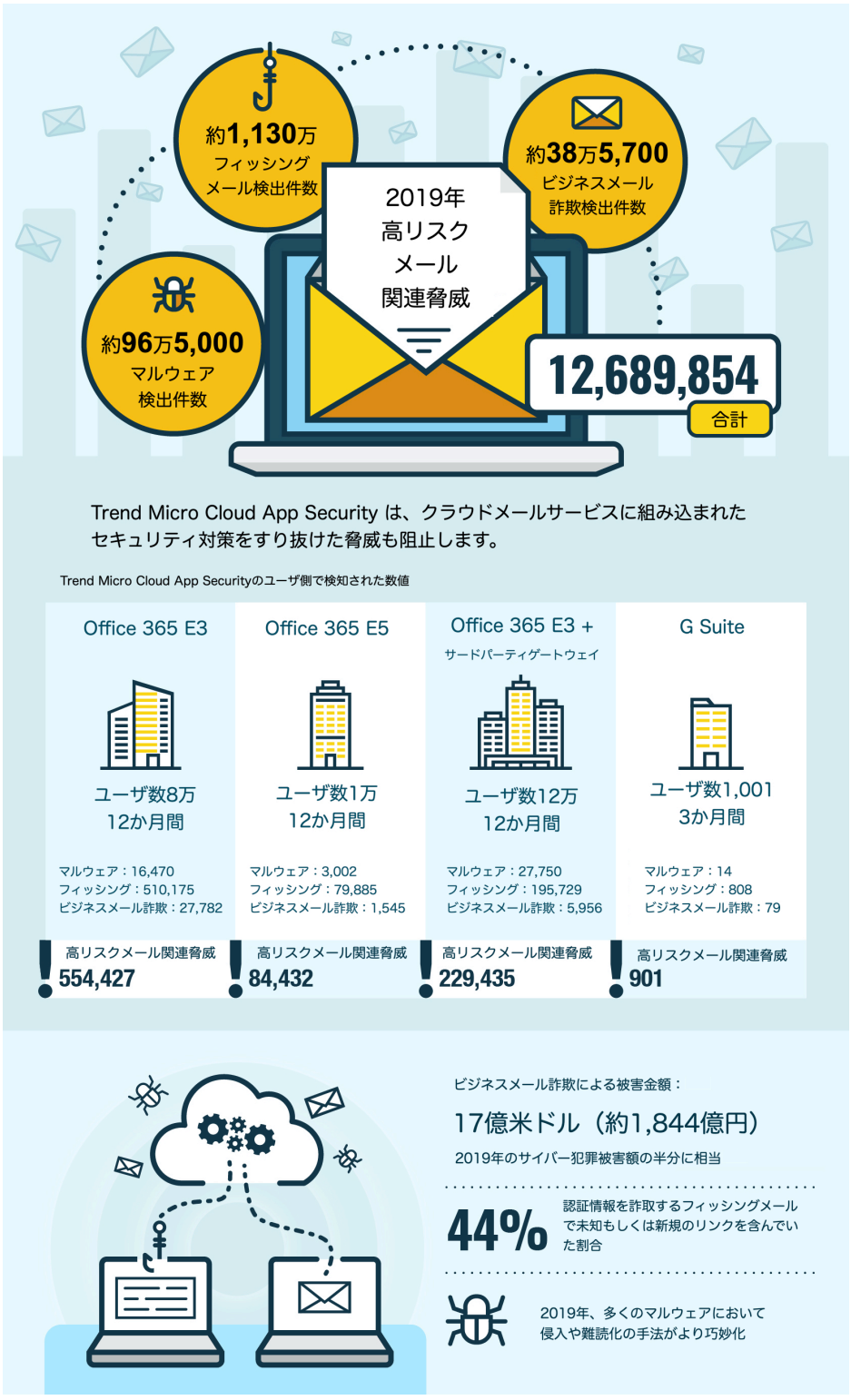


図1：メール関連の脅威概況

継続するビジネスメール詐欺の脅威

ビジネスメール詐欺（BEC）は、2019年もサイバー犯罪者にとって重要な金儲けの手段となっていたと言えます。米国連邦捜査局（FBI）によると、2019年だけでビジネスメール詐欺の被害額は17億米ドル（約1,844億円）となっています[8]。これは2019年のサイバー犯罪被害額の半分に相当します。Trend Micro Cloud App Securityが検出したビジネスメール詐欺の件数は、2018年の10万件以上から2019年は40万件近くとなり、大幅な271％増を示しました。この点からもビジネスメール詐欺は、依然として企業にとって深刻な問題であり、メール関連の全体検出件数に占めるビジネスメール詐欺の割合は前年比3倍となっています。

機械学習（AI）技術によってメールの書き手の癖を解析することで検出されるビジネスメール詐欺の割合は、2018年の7％から2019年は21％に増加しています。さらにこの分析からは、ビジネスメール詐欺を駆使する攻撃者が従来のソーシャルエンジニアリングよりも巧妙な手法を探索している状況もうかがえました。

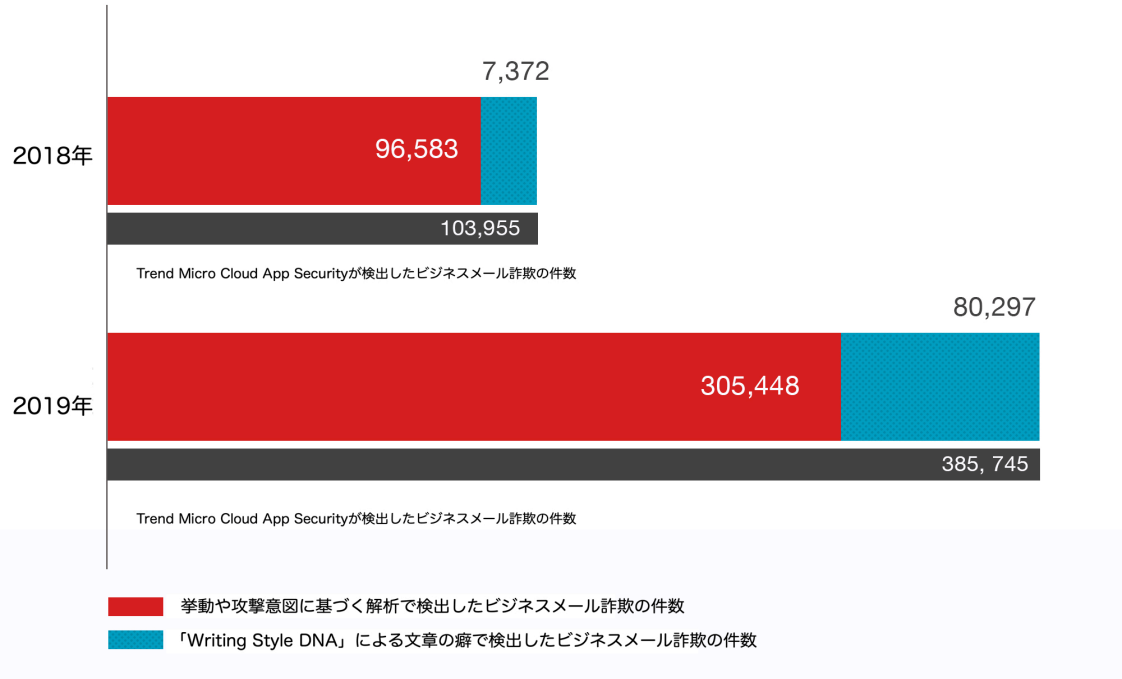
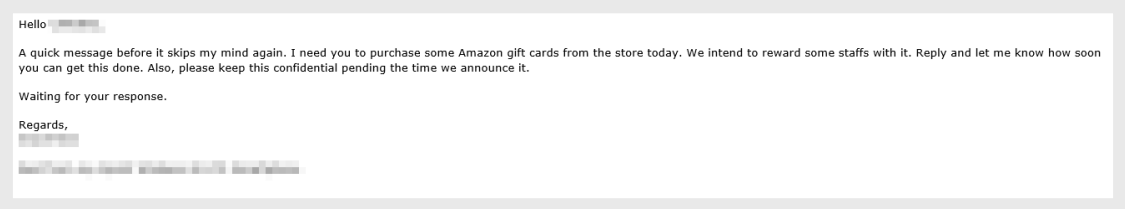


図2：Trend Micro Cloud App Securityによるビジネスメール詐欺検出件数内訳（全世界）

[8] https://www.bankinfosecurity.com/fbi-bec-losses-totaled-17-billion-in-2019-a-13717

ビジネスメール詐欺はこの数年増加しています[9]。サイバー犯罪者は過去に成功した攻撃手口を継続して用いてくる傾向があり、これは2019年のビジネスメール詐欺にも当てはまります。メールで偽の請求書を送って電信送金の支払いを依頼する攻撃は2019年も顕著な手口として確認されました[10]。他方、ギフトカードを利用したビジネスメール詐欺も2019年から確認され始め[11]、第4四半期に最も一般的な手口の1つとなりました[12]。ギフトカードによるビジネスメール詐欺は、受信者の仲介や、銀行や法執行機関によって閉鎖される恐れのある送金先口座に依存する必要がなく、実質的に攻撃者側で余計なやりとりが伴わない取引が可能になります。ただしFBIによると、こうしたギフトカードによるビジネスメール詐欺でも電信送金のリクエストが伴う事例を確認しています。


Hello [redacted]

A quick message before it skips my mind again. I need you to purchase some Amazon gift cards from the store today. We intend to reward some staffs with it. Reply and let me know how soon you can get this done. Also, please keep this confidential pending the time we announce it.

Waiting for your response.

Regards,

[redacted]

図3：Trend Micro Cloud App Securityによって検出されたギフトカードを利用したビジネスメール詐欺の一例。会話体の文章であるため、受信側が油断する可能性もある。

ビジネスメール詐欺自体でも、通常の手口を利用しつつ、新たな手法を進化させ始めています。例えば、注目すべき変化の1つは、企業の最高経営責任者になりすますCEO詐欺メールの件数が減少している点です。米国財務省の金融犯罪執行ネットワークは、2019年のレポートの中で[13]、2017年のサンプル件数の33%を占めていたCEO詐欺の割合が、2018年には12%のみであったと報告しています。この点から、ビジネスメール詐欺の攻撃者は、なりすましの対象としてより新しく、利用しやすいものを探し始めていることが推測されます。

ビジネスメール詐欺を利用するサイバー犯罪者は、ソーシャルエンジニアリングの手口にも工夫を施しています。従来、ビジネスメール詐欺では、電信送金をリクエストする偽の請求書メールに依存していました。しかし2019年、ビジネスメール詐欺グループ「London Blue」は[14]、購入価格の30%を電信送金する必要があるなどというメッセージにより、標的の企業に対して海外企業の買収条件を通知するビジネスメールを利用しました。2019年12月の別の事例では、サイバー犯罪者は、まず中国のベンチャーキャピタル企業の従業員のアカウントを侵害し[15]、その後、この企業の取引先であるイスラエルのスタートアップ企業のドメインを偽装して、最終的には起業時の資金提供のために用意されていた100万米ドル（約1億850万円）の持ち出しに成功しました。

---

9 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-average-bec-attacks-per-month-increased-by-120-from-2016-to-2018

10 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-business-email-compromise-scheme-reroutes-paycheck-by-direct-deposit

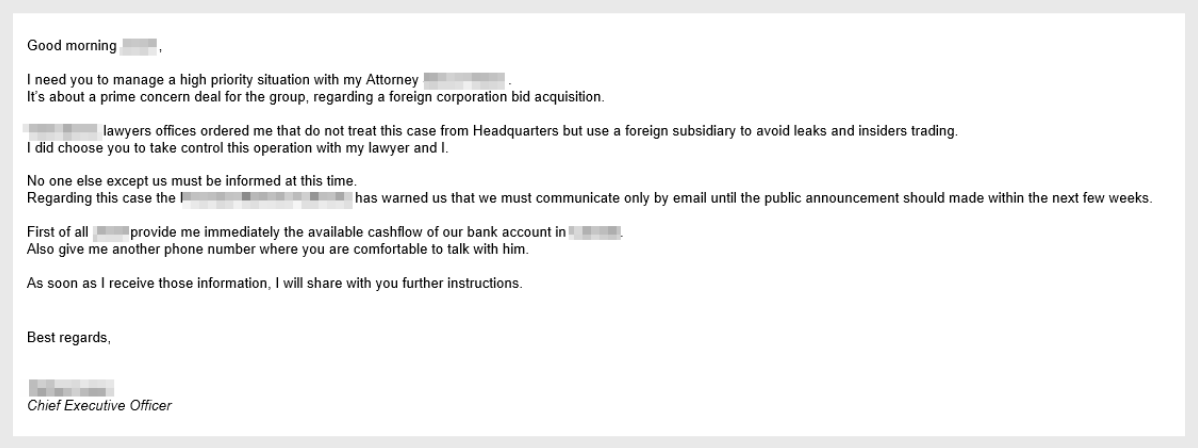
11 https://www.ic3.gov/media/2018/181024.aspx

12 https://www.darkreading.com/fbi-business-email-compromise-cost-businesses-$17b-in-2019/d/d-id/1337035

13 https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

14 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/london-blue-group-using-evolving-bec-techniques-in-their-attacks

15 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scam-successfully-steals-us-1-million-using-look-alike-domains



Good morning [redacted],

I need you to manage a high priority situation with my Attorney [redacted].
It's about a prime concern deal for the group, regarding a foreign corporation bid acquisition.

[redacted] lawyers offices ordered me that do not treat this case from Headquarters but use a foreign subsidiary to avoid leaks and insiders trading.
I did choose you to take control this operation with my lawyer and I.

No one else except us must be informed at this time.
Regarding this case the [redacted] has warned us that we must communicate only by email until the public announcement should made within the next few weeks.

First of all [redacted] provide me immediately the available cashflow of our bank account in [redacted].
Also give me another phone number where you are comfortable to talk with him.

As soon as I receive those information, I will share with you further instructions.

Best regards,

[redacted]
Chief Executive Officer

図4：Trend Micro Cloud App Securityにより検出された買収条件の通知メールになりすましたビジネスメール詐欺の一例。金額についてはまだ言及されていないため、事前段階のメールと考えられる。

ビジネスメール詐欺の攻撃者は非営利団体も標的にしています。2019年の主要な事例としては、米テキサス州のマナー独立学区に対する230万米ドル（約2億4,900万円）の損失が発生した攻撃[16]や、175万米ドル（約1億9,000万円）の損失につながった米オハイオ州のオハイオ教会を狙った攻撃[17]が挙げられます。2019年に米ノースカロライナ州[18]や米ジョージア州[19]などで数百万米ドルの損失が発生した事例からもわかるとおり、地方自治体も標的となっています。

16 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/texas-school-district-loses-2-3-million-to-phishing-scam-bec

17 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scammers-steal-us-1-75-million-from-an-ohio-church

18 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/us-1-7-million-stolen-from-north-carolina-county-after-bec-scammers-posed-as-contractor

19 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-invoices-used-by-bec-scammers-to-defraud-griffin-georgia-us-800-000

クレデンシャルフィッシングのリスクが深刻化

2017年および2018年の「Trend Micro Cloud App Securityレポート」[20]では、Microsoft Office 365ユーザがフィッシング攻撃の標的[21]になっている点を指摘しており、2019年も例外ではありません。SPNのデータによると、2019年にブロックされたOffice 365関連のフィッシング攻撃の固有リンク数は、2018年の2倍以上に急増しています。

約1万人のOffice 365ユーザを持つ企業では、こうしたフィッシング攻撃が主な課題となりました。この企業においてTrend Micro Cloud App Securityは、この企業を標的とする41万件を超えるフィッシング攻撃を検出およびブロックし、そのうち10万件以上がスパムメール、30万件以上がクレデンシャルフィッシングのメールでした。550人のOffice 365ユーザを持つ企業では、2,600件を超えるフィッシング攻撃を検出およびブロックしました。これらのメールは、メールサービスに組み込まれたセキュリティフィルタを突破したものであり、突破していないフィッシング攻撃を含むとその数はさらに多くなります。

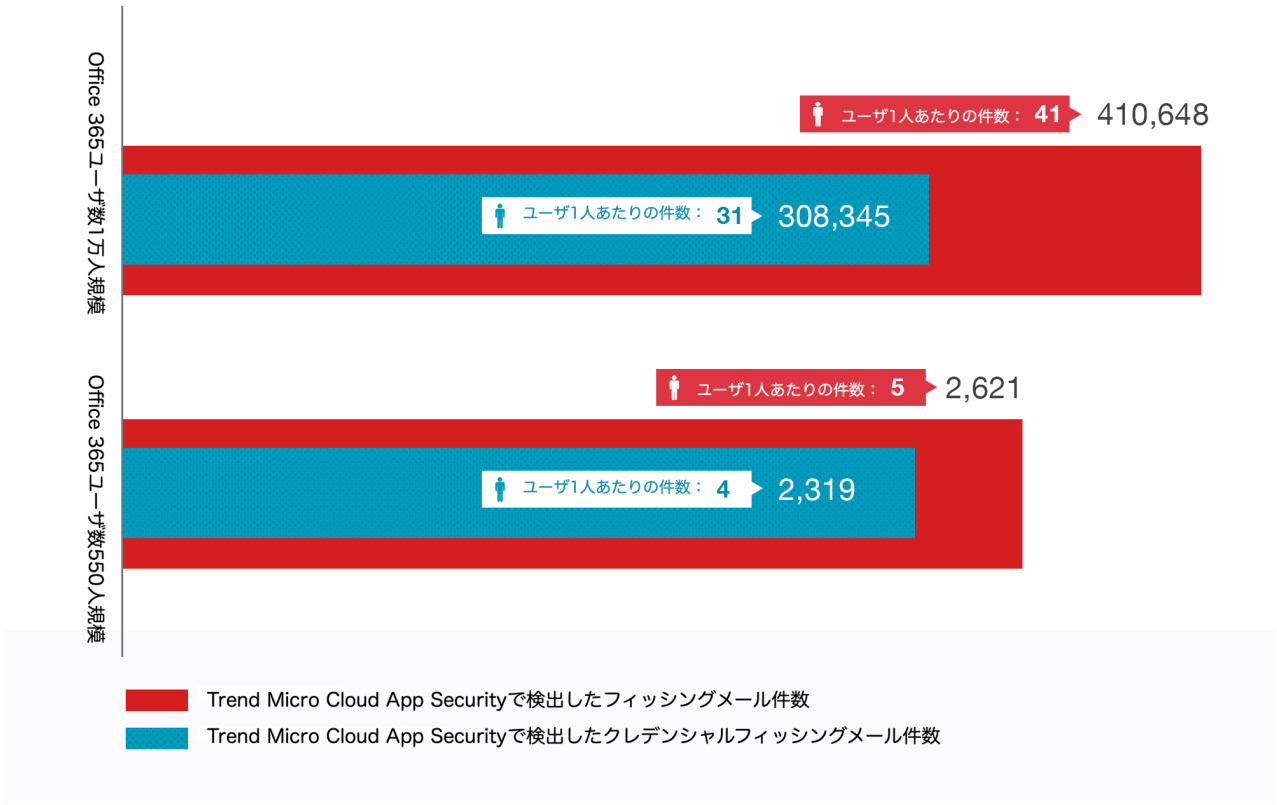


図5：Trend Micro Cloud App Securityによるフィッシングメール検出件数内訳（全世界）

[20] https://www.trendmicro.com/ja_jp/about/trendpark/cloud-app-security-2018-report-201904-01-01.html

[21] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-over-20-of-phishing-campaigns-target-microsoft-users

Office 365のユーザはフィッシング攻撃の対象であり、特にクレデンシャルフィッシング攻撃の標的となっています。さらに攻撃者はOffice 365管理者アカウント[22]も狙ってきています。攻撃者が管理者アカウントを乗っ取り、Office 365ユーザの認証情報を制御できるようになると、そこから個々のアカウントへのアクセスが可能になります。乗っ取られた管理者アカウントからは、企業のOffice 365ドメインとそこに接続されているすべてのアカウントが制御される危険性があります。

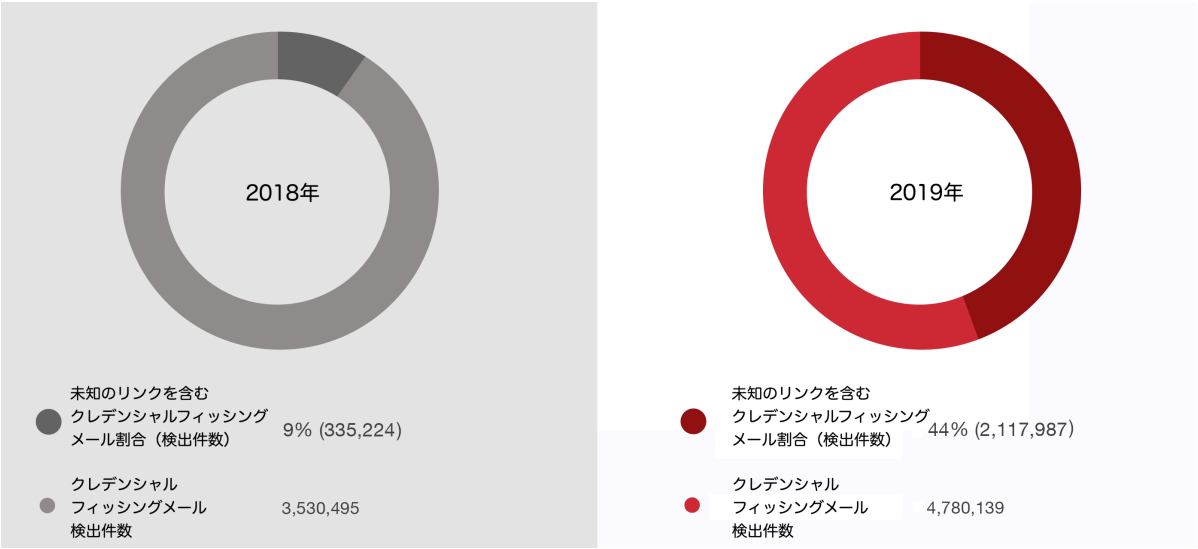


図6：Trend Micro Cloud App Securityにより検出されたクレデンシャルフィッシング攻撃内訳（全世界）

2019年におけるクレデンシャルフィッシング攻撃の検出数は増加し、2018年から35%増となりました。そうした中、未知のリンクを含むクレデンシャルフィッシング攻撃の検出数増加が顕著となっています。2018年は未知のリンクを含むクレデンシャルフィッシングメールの割合が9%でしたが、2019年にはその割合が44%となっています。

この増加の理由としては、サイバー犯罪者がセキュリティ対策ソフトの検出回避のため、誘導先のフィッシングサイトを更新して新たなリンクを頻繁に反映させていた可能性が挙げられます。また、新たなサイバー犯罪者グループが多数登場し、独自のURLを使用して攻撃キャンペーンを開始している可能性もあるでしょう。こうした理由によって、不明なURLの検出が大幅に増加していると推測されます。

クレデンシャルフィッシング攻撃の手口は巧妙になっており、音声を使用するクラウド共有プラットフォームの悪用は、2019年の注目すべき戦術と言えるでしょう。例えば、2019年7月に発生したクレデンシャルフィッシング攻撃キャンペーンでは、偽のOneNote Onlineページが使用され[23]、このページは、偽のMicrosoftログインページにリンクされたSharePointサブドメイン上にホストされていました。

---

22 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminals-going-after-office-365-administrators-using-hijacked-accounts-to-perform-phishing-attacks

23 https://www.trendmicro.com/vinfo/us/security/news/security-technology/new-phishing-campaign-uses-onenote-audio-to-lure-users-to-fake-microsoft-login-page

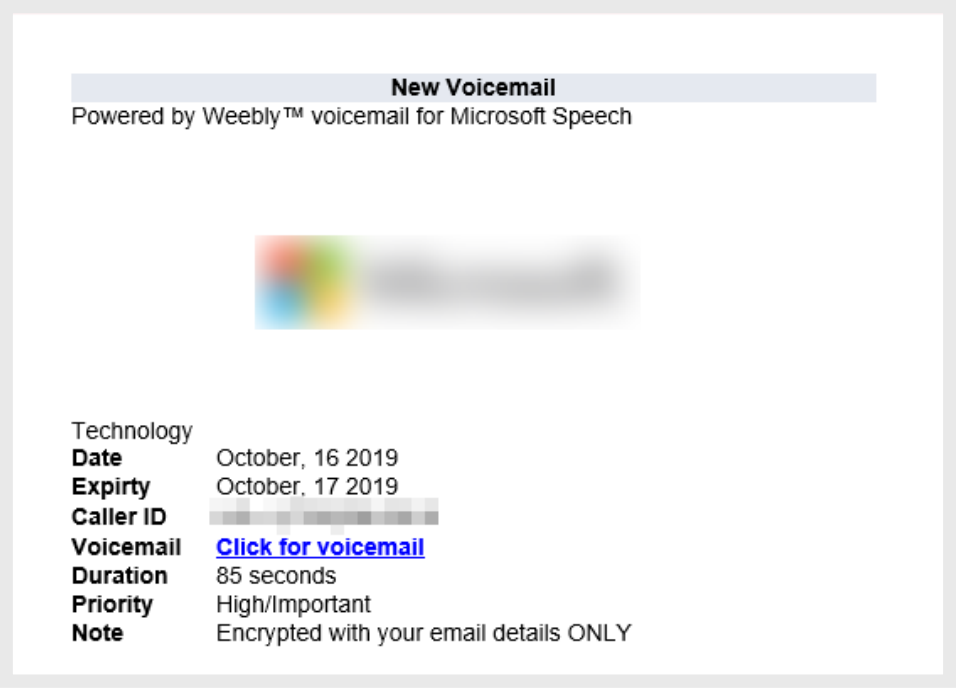


図7：Trend Micro Cloud App Securityが検知した偽のボイスメール通知の例

なお、2019年上半期のレポート「The Rising Tide of Credential Phishing」[24]では、その他の認証情報を詐取するフィッシング攻撃の手法について詳しく説明しています。

[24] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-rising-tide-of-credential-phishing

新たな手法を用いるマルウェア攻撃

2019年にマルウェアの検出件数は減少傾向が見られ、2018年に100万以上に達していたものが、2019年には100万を下回っています。しかし、年間を通じて確認されたマルウェアの亜種は、依然としてさまざまな機能を駆使していました。

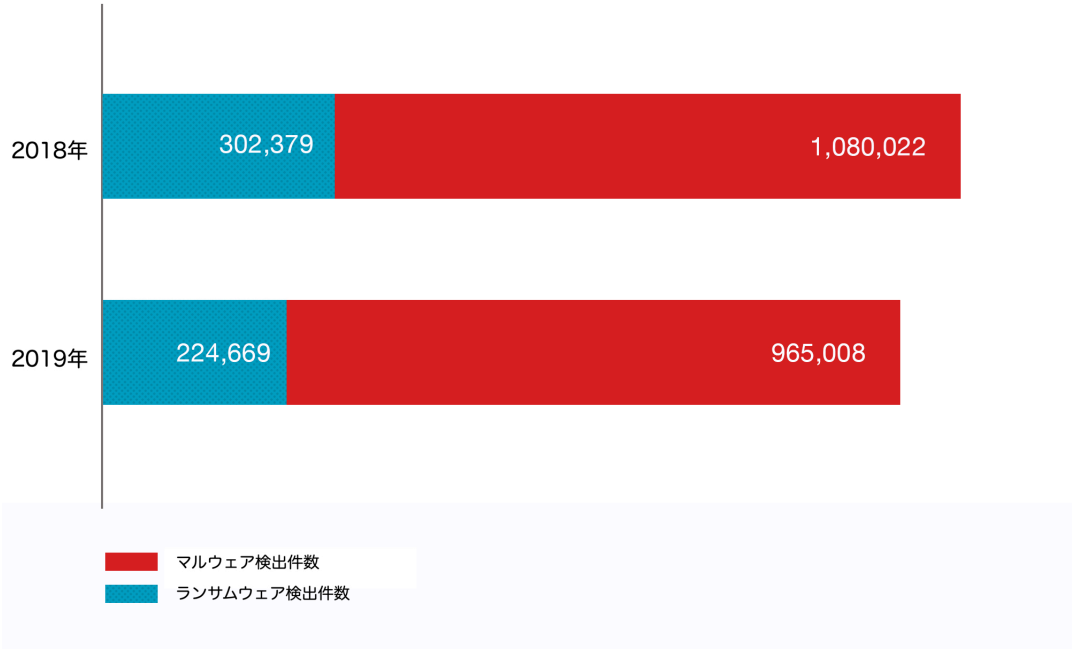


図8：Trend Micro Cloud App Securityによるマルウェアおよびランサムウェアの検出件数（全世界）

例えば、サイバー犯罪者グループ「Cloud Atlas（別名：Inception）」[25]による2019年の攻撃キャンペーンは、表面的にはこれまで同様の活動を展開していたように見えます。しかし実際は、他の多くのフィッシング攻撃キャンペーンと同様、フィッシングメールを用いてより高い効果が得られる標的を狙っていました。中でも注目されるのは、そこで利用されていた不正な添付ファイルです。彼らが利用したMicrosoft Officeの文書ファイルには、リモートサーバから読み込まれた不正なテンプレートが含まれていました。これによる難読化の手法で静的解析やフォレンジック解析をすり抜けることが可能となります。

さらに、このテンプレートは不正なHTMLアプリケーションを実行し、これによってバックドア活動が行われます。HTMLアプリケーションおよびバックドア活動は、いずれも検出回避のために常に属性を変更するポリモーフィックの特質を備えていました。最終的なペイロードには、文書の情報を窃取してコマンド＆コントロール（C&C）サーバに送信するように設計されたコンポーネントや、感染端末からパスワードを窃取するパスワードグラバーが含まれていました。

[25] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cloud-atlas-group-updates-infection-chain-with-polymorphic-malware-to-evade-detection

また、マルウェア拡散におけるISOファイルの使用が見られてきています[26]。2019年8月、マルウェア「LokiBot」（「LOKIBOT」ファミリーとして検出対応）[27]が、不正なISOファイルが添付されたスパムメールで拡散され、さらにデータを他のデータに埋め込む隠ぺい手法であるステガノグラフィーによって、攻撃経路の隠ぺいが行われていました。同じ月、遠隔操作ツール（RAT）「FlawedAmmyy」（「FLAWEDAMMYY」ファミリーとして検出対応）の感染にISOファイルの添付を用いたサイバー犯罪グループ「TA505」についてもトレンドマイクロでは報告していました。

2019年はスパムメールやフィッシング攻撃のキャンペーンにおけるRATの急増を確認しています。2019年7月、トレンドマイクロのリサーチャは、リモート実行や情報窃取機能を備えた多機能ツールのRAT型マルウェア「Remcos」（「REMCOS」ファミリーとして検出対応）[28]を配信するフィッシングメールを確認しました。この攻撃では、検出回避のために多数の難読化やアンチデバッグの技術を駆使していました。同じ月、多段階の複数ペイロードを備えた攻撃キャンペーン[29]が南米地域の金融および政府機関を標的にしていました。この攻撃キャンペーンではRAT型マルウェア「Imminent Monitor」（「SHADESRAT」「FYNLOSKI」「IMMONRAT」「BOILOD」の各ファミリーとして検出対応）および「Proyecto」（「BOILOD」「HPBLADABINDI」「XRAT」の各ファミリーとして検出対応）が利用されていました。さらに攻撃キャンペーンの背後にいるサイバー犯罪者グループは、C&Cサーバ用に使い捨てメールアドレスの作成が可能なサービスを使用していました。また、トレンドマイクロのハニーポットで検知された別のスパムメールキャンペーンでは[30]、プログラミング言語「AutoIT」でコンパイルされたペイロードを使用する情報窃取型マルウェア「Negasteal（別名：Agent Tesla）」（「NEGASTEAL」ファミリーとして検出対応）およびRAT型マルウェア「Ave Maria（別名：Warzone）」（「AVEMARIA」ファミリーとして検出対応）が含まれていました。

---

26 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-spam-campaign-uses-iso-image-files-to-deliver-lokibot-and-nanocore

27 https://blog.trendmicro.com/trendlabs-security-intelligence/lokibot-gains-new-persistence-mechanism-uses-steganography-to-hide-its-tracks/

28 https://blog.trendmicro.com/trendlabs-security-intelligence/analysis-new-remcos-rat-arrives-via-phishing-email/

29 https://blog.trendmicro.com/trendlabs-security-intelligence/spam-campaign-targets-colombian-entities-with-custom-proyecto-rat-email-service-yopmail-for-cc/

30 https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-negasteal-agent-tesla-ave-maria-delivered-via-malspam/

多様化するフィッシング攻撃

ここ数年でメールを利用した攻撃は多面的な傾向を示してきています。ソーシャルエンジニアリングへの警戒心が高まるにつれ、サイバー犯罪者は状況に応じてフィッシング攻撃を効果的にするための新しい手法を展開してきています。

サイバー犯罪者は単一のURL、IPアドレス、もしくはドメインを使用したメールを送信する代わりに、パブリッククラウドとホスティングのインフラ双方を駆使する[31]ことで、攻撃メールをより正当なものに見えるように工夫しています。その他、乗っ取ったメールアカウントを使用して、やりとりが進行中のメールスレッドに返信し[32]、疑われずに企業内の従業員を狙ってきます。こうした傾向は2019年に入ってさらに高まり、乗っ取られたOffice 365アカウントにより1か月で150万件のメールが送信されたケースも報告されました[33]。

さらにはフィッシング対策機関「Anti-Phishing Working Group」によると、2019年第1四半期だけでフィッシングサイトでのHTTPS使用は58%増加したと報告しています[34]。この急増からも、サイバー犯罪者が利用するフィッシングサイトが不正であることを隠ぺいするためにあらゆる手段を講じている状況がうかがえます。

2019年はフィッシング攻撃が複雑さを増す傾向も確認され、複数のフィッシングサイトを用いて多段階のフィッシング攻撃を使用する攻撃キャンペーン「Heatstroke」[35]が典型的な事例と言えます。その他、フィッシング攻撃に使用するキット自体に難読化が施され、ブラウザによるソースコードの確認で民話のテキストが表示されるケースも確認されました。これにより、攻撃経路の追跡を阻止し、セキュリティリサーチャによるコード分析を回避しようとしていたと推測されます。

---

31 https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/smarter-phishing-techniques-cybersecurity-tools-advanced

32 https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/

33 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/compromised-office-365-accounts-used-to-send-1-5-million-email-threats-in-march

34 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites

35 https://blog.trendmicro.com/trendlabs-security-intelligence/heatstroke-campaign-uses-multistage-phishing-attack-to-steal-paypal-and-credit-card-information/

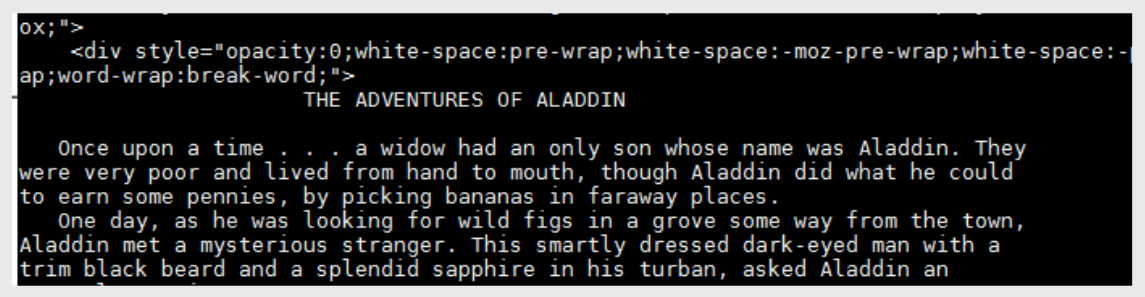


図9：「Heatstroke」のフィッシングサイトのソースコードをブラウザで確認しようとすると代わりに民話の文書が表示される。

過去に使用されていた手口も2019年後半に再び確認されました。ユーザのトークンをサイバー犯罪者に送信するように設計されたログインページへ誘導させるフィッシングの手法が利用され[36]、サイバー犯罪者は認証情報が更新された後でも被害者のOffice 365アカウントにアクセスできました。

2019年はフィッシング攻撃の対象範囲も拡大しました。トレンドマイクロのリサーチャが確認したフィッシング攻撃キャンペーンの1つでは、人気のソーシャルメディアアプリ「Instagram」[37]が攻撃対象となっていました。1万5,000から7万人のフォロワーを持つ人気のInstagramユーザが標的となり、サイバー犯罪者にそのアカウント情報が詐取されています。その後、サイバー犯罪者は詐取したアカウントからInstagramの確認依頼に見せかけたフィッシングメールをフォロワーへ送信し、彼らの認証情報を詐取するために設計されたフィッシングサイトへ誘導していました。

こうして詐取されたアカウント情報はおそらく金銭的な恐喝に利用された可能性があります。サイバー犯罪者にとって価値があるのは、自身のアカウントを取り戻すために一定の金額を支払うことをいとわないユーザでしょう。

[36] https://krebsonsecurity.com/2020/01/tricky-phish-angles-for-persistence-not-passwords/

[37] https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/

Trend Micro Cloud App Security によるメール対策

メール関連の脅威は2019年も継続しており、特にビジネスメール詐欺は依然としてサイバー犯罪者にとって有益なビジネスモデルとなっていました。この点は、多様化する手口の可能性が示されたほか、検出件数の増加からも明らかと言えます。さらに、クレデンシャルフィッシング攻撃で使用された未知のリンク数の増加は、新たに参入したサイバー犯罪者やURLを頻繁に更新するこれまでのサイバー犯罪者によって、攻撃キャンペーンが次々と展開されている状況を示しています。一方、マルウェアの検出件数がわずかに減少したものの、2019年はマルウェアを感染させるためにより巧妙な手口の展開が確認された年でもありました。

こうしたメール関連の脅威概況を考慮すると、企業のツールがクラウドに移行する中、もはや単一のセキュリティゲートウェイやサービスだけでは、セキュリティ対策として十分ではないと言えるでしょう。企業は規模の大小に関係なく、これらさまざまな脅威がもたらす大きな危険にさらされています。

企業ではTrend Micro Cloud App Securityなどの総合的かつ多層防御のセキュリティソリューションを検討する必要があります。こうしたソリューションは、機械学習を駆使してメッセージ本文の不審なコンテンツや添付ファイルを分析して検出することにより、Office 365やG Suiteなどのメールやコラボレーションのプラットフォームに組み込まれたセキュリティ機能を補完します。

Trend Micro Cloud App Securityは、サンドボックスでのマルウェア分析、文書のエクスプロイト検出、ファイルレピュテーション、Emailレピュテーション、Webレピュテーションなどの技術を駆使し、Office 365やPDF文書内に隠ぺいされたマルウェアを検出します。さらに、Box、Dropbox、Google ドライブ、SharePoint Online、OneDrive for Businessといったアプリケーション向けに情報漏えい対策（DLP）および高度なマルウェア対策を提供しており、これらのクラウドベースのアプリケーション全体で一貫したDLPポリシーを有効化できます。また、ユーザや管理者を保持しながら、ベ

ンダのAPIを通じたクラウドからクラウドへの直接統合を提供することで、既存のクラウド設定とのシームレスな統合を実現します。さらに、サンドボックスによるマルウェア解析前に脅威リスクを評価することで、追加リソースの必要性を最小限に抑えます。

Trend Micro Cloud App Securityはサービスとしてのソフトウェア（SaaS）向けの最先端のセキュリティに基づき、ビジネスメール詐欺およびクレデンシャルフィッシング攻撃という2つの主要な脅威に対抗するため、機械学習（AI）で強化された技術「Writing Style DNA」[38]を提供します。この技術は機械学習（AI）により過去のメールの文章からユーザの癖を分析し、疑わしいメールの文章と比較することで、メールが正規かどうかを判断します。一方、「Computer Vision」の機能[39]は画像分析と機械学習を組み合わせて、ロゴやブランドの形態、ログインフォーム、その他のサイトコンテンツをチェックします。さらにこれらの情報をサイトのレピュテーション情報や光学式文字認識（OCR）と一緒に保持することで、偽サイトや不正サイトをチェックし、誤検知の回避にも役立てることができます。

最適なセキュリティ技術を導入したとしても、堅固なセキュリティを実現する上では人的要素が不可欠となります。企業では従業員に対してメールの脅威に関するセキュリティ教育を実施し[40]、こうした攻撃の手口や対応方法を周知しておく必要があります。この場合、不審なメールに見られる文法エラーやスペルミスに注意しておくことも含まれます。とりわけ、財務上の取引などの場合、メールによるやり取りや操作に関しては、細心の注意を払う必要があります。

なお、企業は、メールとエンドポイントのセキュリティに関する無料の評価サービスを利用できます（日本でのサービス提供は後日開始する予定です）。 この評価サービスは潜在的な脅威が潜んでいないかメールボックスをスキャンするためにTrend Micro Cloud App Securityを使用しています。

---

38 https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/curbing-the-bec-problem-using-ai-and-machine-learning

39 https://blog.trendmicro.com/stop-office-365-credential-theft-with-an-artificial-eye/

40 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/infosec-guide-email-threats

TREND MICRO

〒151-0053

東京都渋谷区代々木2-1-1　新宿マインズタワー

大代表 TEL：03-5334-3600 FAX：03-5334-4008

http://www.trendmicro.com

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。

TREND MICRO | research