王国への鍵

侵害された社用メールアカウントが、
サイバー犯罪者にとって最も魅力的な
攻撃ベクトルになっている理由とは

KELA

王国への鍵：侵害された社用メールアカウントが、サイバー犯罪者にとって最も魅力的な攻撃ベクトルになっている理由とは

KELA サイバー犯罪インテリジェンスセンター

目次

調査結果の主なポイント

- サイバー犯罪のエコシステムが発展し、サービタイゼーション（物品ではなくサービスを提供して使用料を受け取るビジネスモデル）が進んだ結果、脅威アクターが企業の Web メールを簡単に入手できるようになっています。人気の高い Web メール（アカウント）専門ショップとしては、XLeet や Odin、Lufix、Xmina が挙げられます。
- KELA が分析を行った結果、上述の Web メール専門ショップで最も人気の高い電子メールホスティングプロバイダーは Office 365 であることが判明しました。最も規模の大きい Web メールショップは XLeet であり、同ショップで売り出されている Web メール 1 件あたりの平均価格は 25 米ドルとなりました。
- 脅威アクターは、侵害した電子メールアカウントを使って容易く利益を手にしようと目論んでおり、Web メール専門ショップはそういったサイバー犯罪者が不正行為によって入手した何百件もの社用メールアカウントを販売できる場となっています。また他の脅威アクターにとっても、今や Web メール専門ショップを利用することで様々な条件（業界や国など）に基づいて、理想的な標的を簡単に探し出せるようになっています。
- 脅威アクターが購入した Web メールアカウントを収益化する手口は、アカウント情報を悪用した金銭窃取から、より大きな利益が期待できるフィッシング攻撃やビジネスメール詐欺（BEC）、マルウエア攻撃まで多岐にわたります。
- フィッシングは、脅威アクターや、国家の支援を受けて偵察活動を専門に行う APT グループが一般的に使っている攻撃手法であり、彼らも Web メールの自動売買ショップで社用メールアカウントの資格情報を購入している可能性があります。
- マルウエアも、侵害した電子メールアカウントを使って多大な利益を手にしようと企むアクターが一般的に使用しているツールです。攻撃者が金銭を窃取したり高額な身代金を手に入れる目的で、情報窃取型トロイの木馬やランサムウエアを使った攻撃を実行する場合、その第 1 ステップとなるソーシャルエンジニアリングの段階でマルウエアが使用されます。

序章

脅威アクターは、サイバー犯罪のエコシステムの中で常に新たな収益化の機会を模索しており、企業の機密データに不正アクセスして悪用することで利益を手にしようと企んでいます。一方サイバー犯罪フォーラムでは、侵害された様々なデータ（データベースやソースコード、社内文書、企業が使用している電子メールなどのサービスを利用する際に必要な資格情報）が出回っています。そして万が一社用メールアカウントの資格情報が脅威アクターの手に渡ってしまった場合は、アクターがそのアカウントユーザーの利用しているコンテンツを閲覧したり、そのアカウントを使って正当なメールに見せかけたフィッシングメールを送信することが可能となります。

今や脅威アクターは新たに登場したマーケットプレースやショップで、攻撃に使用する社用メールアカウントを手軽に購入することができるようになっています。なお、本レポートで言及する Web メールとは、様々なビジネスメールプロバイダーが提供する Web ベースのインターフェースや Web ブラウザを使って送受信されるメールを指します。つまり Web メールの場合、ユーザーがインターネットに接続してさえいれば社用メールにアクセスすることが可能であり、一方で一般的な電子メールクライアントの場合はデスクトップのプログラムを介する必要があります。今回我々は、電子メールアドレスを専門とする自動売買ショップで、脅威アクターらが社用メールの資格情報数十万件を売りに出している状況に着目し、サイバー犯罪者の作業を容易にしているショップ（XLeet、Odin、Xmina、Lufix など）について詳細な調査を行いました。今回のレポートでは、アクターがアクセスを入手する手口と、フィッシングやビジネスメール詐欺、マルウエアをはじめとする様々な攻撃手法を通じた収益化の手口について詳述します。

ゴール：電子メールアカウントの乗っ取り

多くの人はプライベートと仕事の両面で、ほぼあらゆる日常の活動に電子メールを使用しています。その結果、企業の電子メールにアクセスして機密情報を窃取しようと企むサイバー犯罪者にとって、今や社用メールアカウントは貴重な標的となっています。

サイバー犯罪者が社用メールアカウントに不正アクセスする手口は多岐にわたりますが、最も一般的な手口としては以下が挙げられます。

クラッキング

クラッキングの場合、攻撃者はブルートフォース攻撃や辞書攻撃を行ってユーザーのパスワードを特定します。ブルートフォース攻撃であれば、ユーザーが使用しているログイン情報を推測して試行錯誤でパスワードを入力し、辞書攻撃であれば、様々な単語のリストを用いてパスワードを入力し、保護されているセキュリティシステムを突破します。

窃取

資格情報を窃取する場合、攻撃者は、マルウエアやフィッシングキャンペーンを介してユーザーから直接資格情報を窃取しています。よく使用されているマルウエアのひとつは、被害者の端末に感染してユーザー名やパスワードなどの資格情報を収集する、情報窃取型トロイの木馬です。情報窃取型マルウエアに感染した場合、感染した端末やデバイス（「ボット」と呼ばれます）のデータや、ブラウザに保存されていた情報（「ログ」と呼ばれます）が窃取されます。またサイバー犯罪フォーラムでは、商品化された情報窃取マルウエア（「Redline」や「Raccoon」、「Mars」、「Vidar」など）も広く販売されています。その他に資格情報を窃取する手口としては、サイバー犯罪者がソーシャルエンジニアリング攻撃を行い、ユーザーから直接資格情報を窃取するという手法も挙げられます。

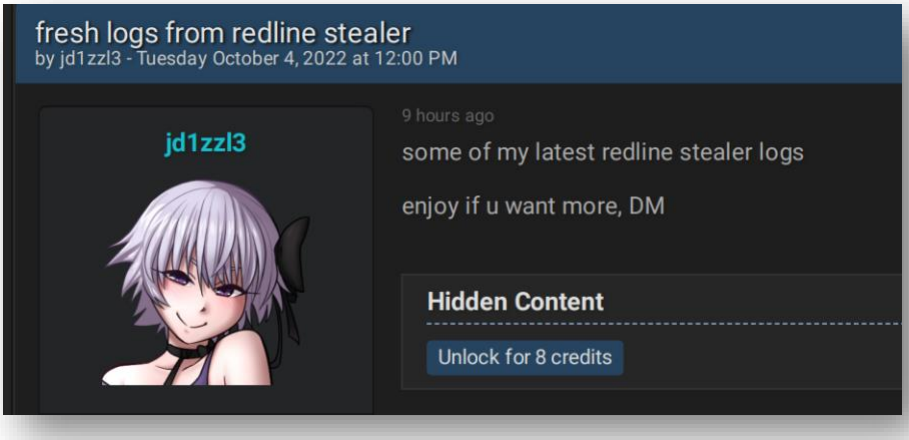
スタッフィング

スタッフィングとは、あるデータ侵害で漏えいした資格情報を使って、他のサービスのアカウントにログインする手法です（例えば、サービス A 用の資格情報がすでに漏えいした場合、その資格情報を使い回してサービス B にログインするなど）。サイバー犯罪のエコシステムでは、ランサムウエアのブログやデータリークサイトで公開されたデータ、複数のデータ侵害をとりまとめたデータダンプなど、漏えいした様々なデータベースが多数公開されています。そして漏えいしたデータの中には、従業員や顧客の電子メールアドレスやパスワード、その他個人を特定できる情報が含まれている場合があり、サイバー犯罪者は、そういった貴重な情報を利用して不正行為を行っています。また、窃取されたデータベースも様々なフォーラムで取引され

ており、アンダーグラウンドのフォーラム「BreachForums」でも、サイバー犯罪者が企業のデータベースを販売・交換したり公開しています。

購入

サイバー犯罪者は、他のサイバー犯罪者が侵害した社用メールアカウントの資格情報やログを購入することもあります。「RussianMarket」や「TwoEasy」、「Genesis」など自動化されたボットネットマーケットプレースでは、サイバー犯罪者が窃取した資格情報が販売されており、そういったマーケットで資格情報を購入すれば様々なリソースにアクセスすることが可能となります。またアンダーグラウンドのフォーラムであれば、電子メールアカウントの資格情報を販売者から直接購入するということも可能であり、技術的な知識やスキルのないサイバー犯罪者でも企業の機密データにアクセスできる手段となっています。



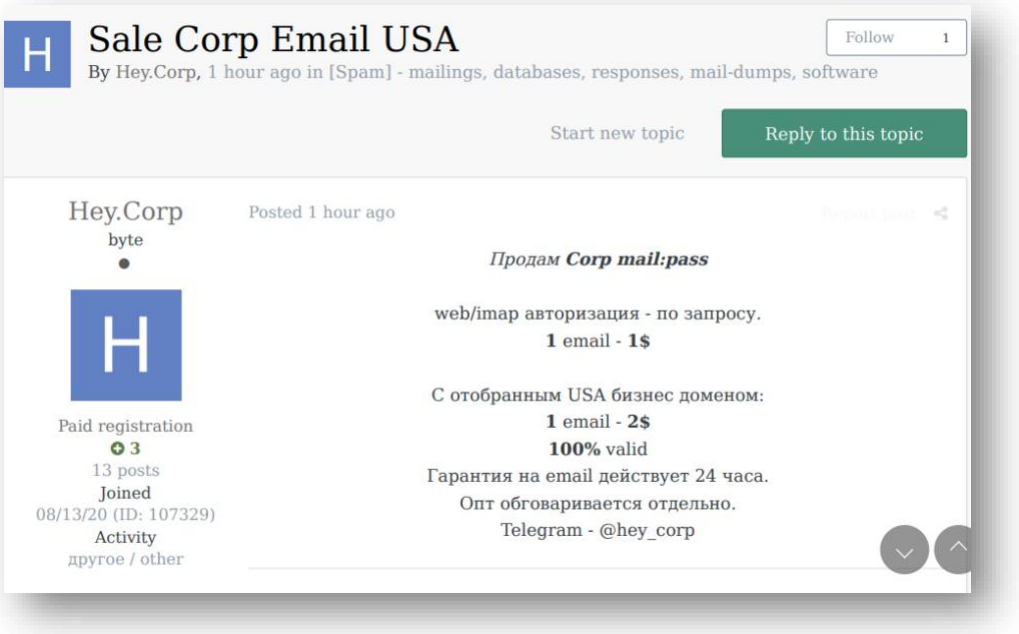
マルウエア「Redline」を使って収集したログ（ウェブブラウザの情報）を販売しているアクター

社用メールの「アクセス」を販売する脅威アクター

サイバー犯罪者は、サーバーへアクセスする方法から社用メール、その他のサービスやツール（CMS、CRM、WordPress、その他）の資格情報にいたるまで、様々な侵入経路や攻撃経路を「アクセス」と呼んでいます。我々は、過去数年にわたり組織の様々な「アクセス」を販売しているサイバー犯罪フォーラムを監視してきましたが、最近、社用メールの資格情報を販売す

るショップの数が増加の一途をたどっている状況を受け、脅威アクターがどのように企業の電子メールアカウントを侵害（またはメールアカウントの資格情報を窃取）しているのかという点に注目しました。

社用メールアカウントのアクセスはサイバー犯罪者らの間で需要が高まっており、サイバー犯罪フォーラムにおける最近の活動にもその様子が現れています。例えば 2022 年 2 月 22 日には、某アクターが様々な米国企業の社用メールアカウントのアクセスを売り出していました。このアクターは、自らが販売しているアカウントはすべて有効であり、購入者は 2 要素認証不要でアカウントにアクセスできると主張して、アカウント 1 件につき 2 米ドルで販売していました。

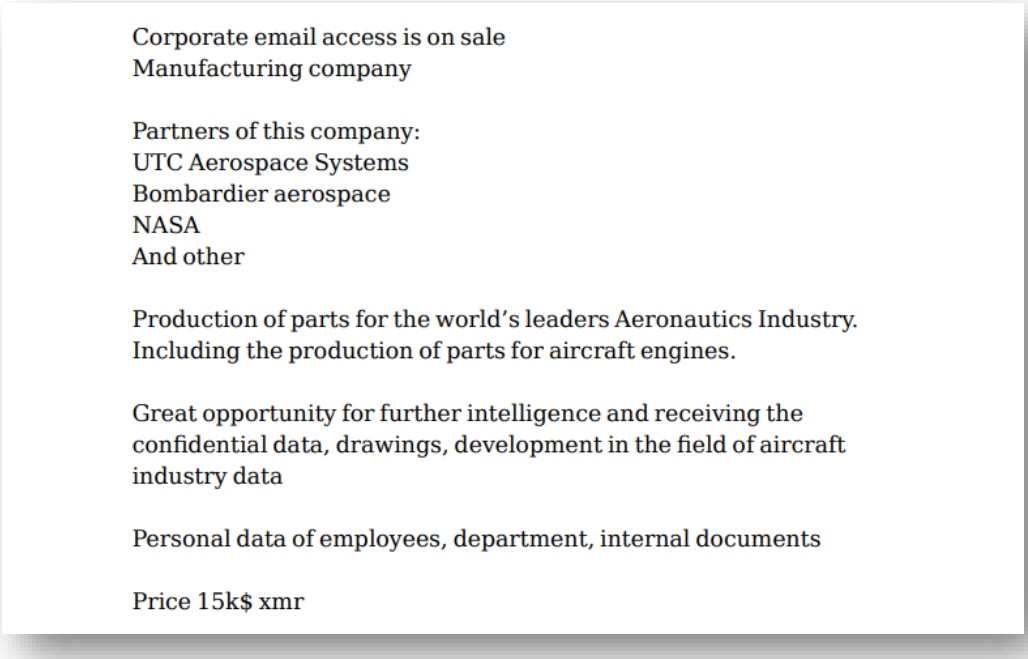


米国企業の社用メールアカウントのアクセスを販売しているアクター

アンダーグラウンドのフォーラムでは、政府が使用する電子メールアカウントのアクセスも定期的に売り出されています。2022 年 7 月 14 日には、某アクターがトルコ人閣僚の電子メールアカウントを売りに出し、また同日中にそのアクセスが買い取られた旨を明言していました。さらに 2022 年 7 月 31 日には別のアクターが、南アジアに拠点を置く某警察隊の電子メールアカウントのアクセスを、1 アカウントにつき 80 米ドルで売りに出していました。その他最近で

は、アクター「leaksmart（別名 Shadowhacker）」が、米国の政府関連組織で使用されている電子メールアカウントのアクセスを売りに出していたことも観察されています。

ランサムウエアグループやランサムウエアオペレーターの代表者も、電子メールアカウントのアクセスを販売しています。2022 年 11 月 22 日には、ランサムウエア「Everest」のオペレーターが、カナダの航空宇宙機器製造企業で使用されている電子メールアカウントのアクセスを 15,000 米ドルで売りに出していました。


Corporate email access is on sale
Manufacturing company

Partners of this company:
UTC Aerospace Systems
Bombardier aerospace
NASA
And other

Production of parts for the world's leaders Aeronautics Industry.
Including the production of parts for aircraft engines.

Great opportunity for further intelligence and receiving the confidential data, drawings, development in the field of aircraft industry data

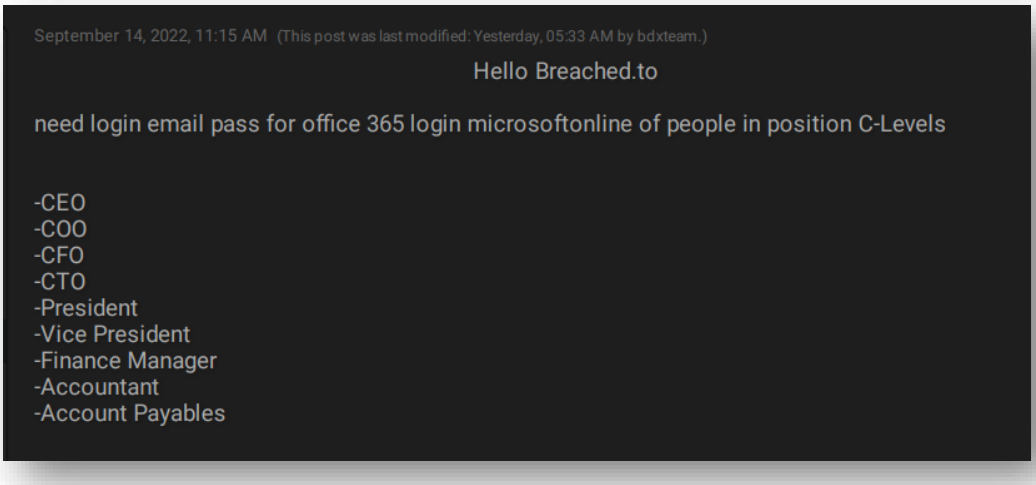
Personal data of employees, department, internal documents

Price 15k$ xmr

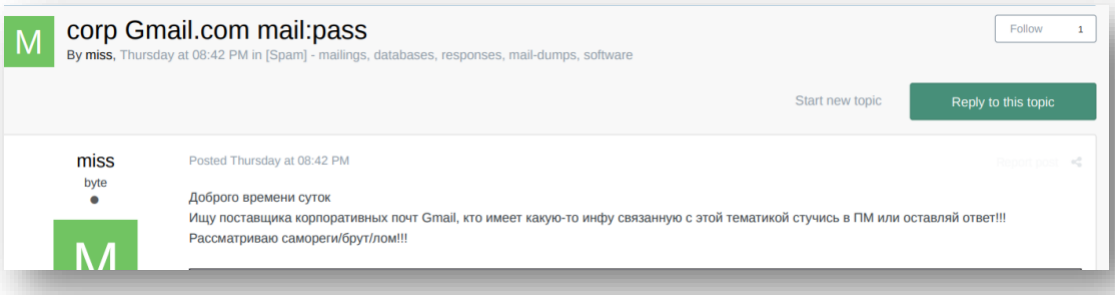
「Everest」がカナダの航空宇宙機器製造企業で使用されている
電子メールアカウントのアクセスを販売している投稿

企業で使用されている電子メールアカウントにも大きな需要が見られます。例えば 2022 年 9 月 14 日には某アクターが、「経営幹部が Microsoft Office で使用している電子メールアカウントのログイン資格情報」を販売してくれる人物を探していました。またこのアクターは、自分が買い取りたい電子メールアカウントユーザーの役職として、CEO や COO、CFO、CTO、財務部門マネージャー、経理担当者などを挙げていました。これらの役職が担う役割から、我々はこ

のアクターが経営幹部になりすまして緊急の電子送金を実行させる、いわゆるビジネスメール詐欺（BEC）を企んでいるものと推測しています。

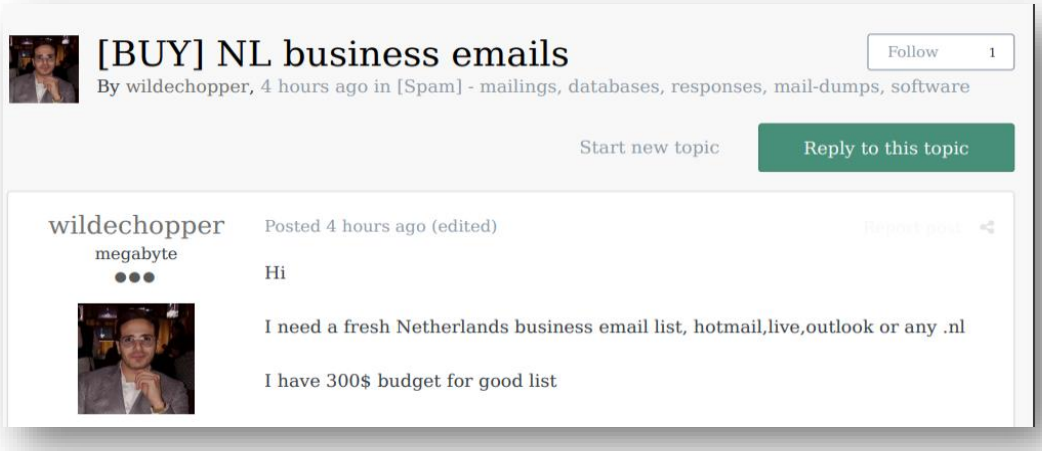


アクターが「経営幹部が Microsoft Office で使用している電子メールアカウントの資格情報」を購入したいと述べている投稿

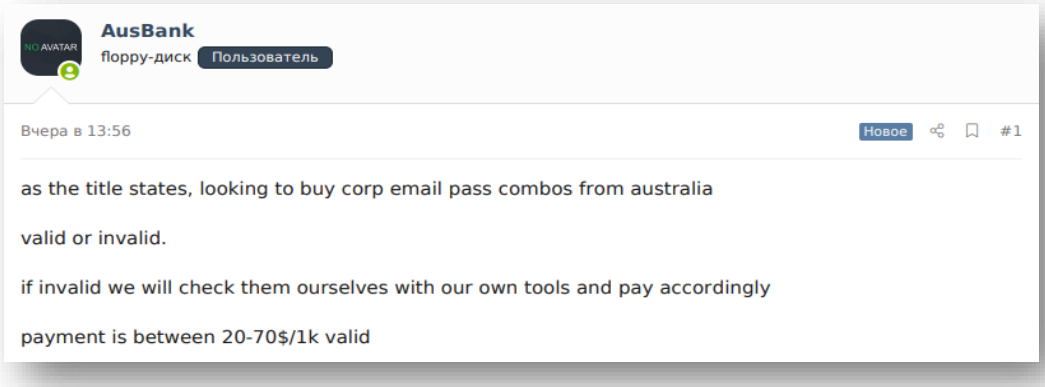


アクターが「ビジネス用 Gmail ユーザーの電子メールアカウント」を購入したいと述べている投稿

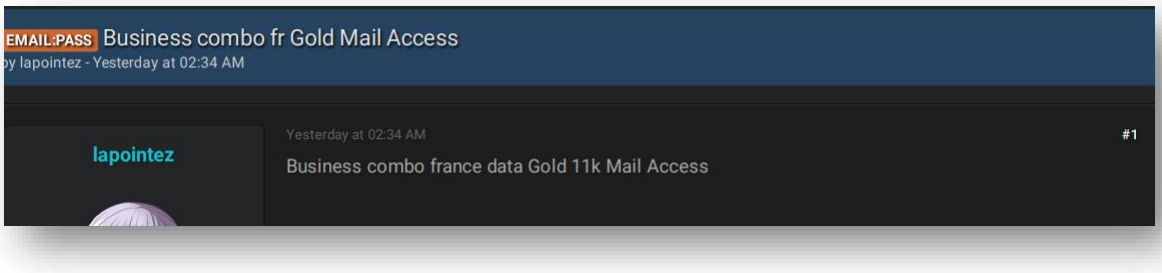
アクターが購入している「商品」は、もはや特定の企業で使用されている社用メールアカウントのアクセスだけではありません。彼らは攻撃に使用する目的で、特定の国々のコンボリスト*も探しています。2022 年 8 月 6 日には、某アクターが「オランダ企業の社用メールのコンボリストに関心があり、300 米ドルを支払う用意がある」とのメッセージを投稿していましたが、このような買い取りの申し出は毎週投稿されています。（*コンボリストとは、資格情報［一般的には平文テキスト］のリストが保存されたテキストファイルであり、様々なリークデータから寄せ集められた資格情報が含まれています）



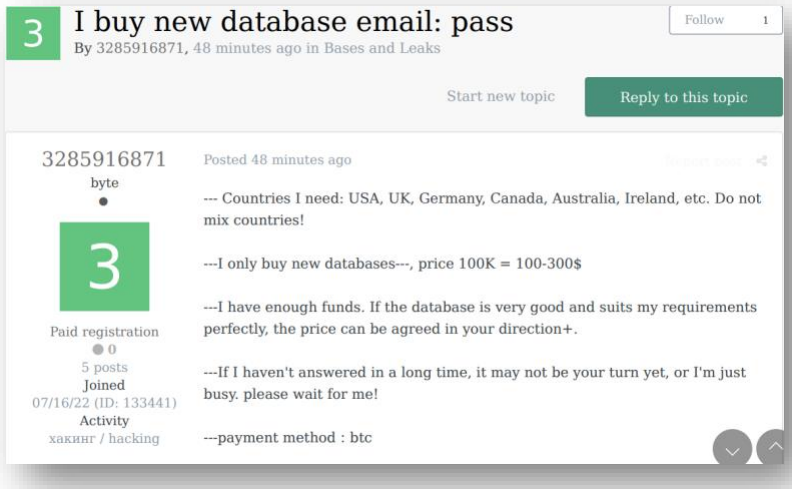
オランダ企業の電子メールアカウントに関心を持っているアクターの投稿



アクターがオーストラリア企業のコンボリスト買い取りを申し出ている投稿



アクターがフランス企業のコンボリストを販売している投稿



アクターが様々な国のコンボリストを募集し、買い取りを申し出ている投稿

社用 Web メールの資格情報を販売する自動売買ショップ

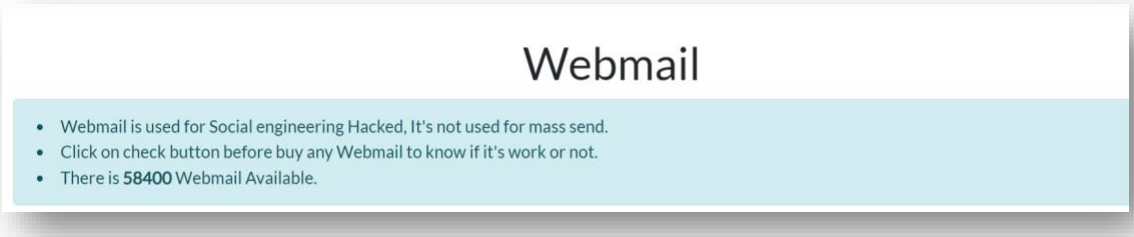
長きにわたり、脅威アクターが社用メールアカウントを購入する場合はサイバー犯罪フォーラムで手作業にて商品を探すことを余儀なくされており、みなそれぞれの目的に合った販売者を自力で探して必要な商品を購入していました。その一方で販売者となる脅威アクターも、他の

サイバー犯罪者の興味をそそるアクセスやコンボリストを手頃な価格で提供するためには、まず自分でその商品の販売メッセージを投稿する必要がありました。

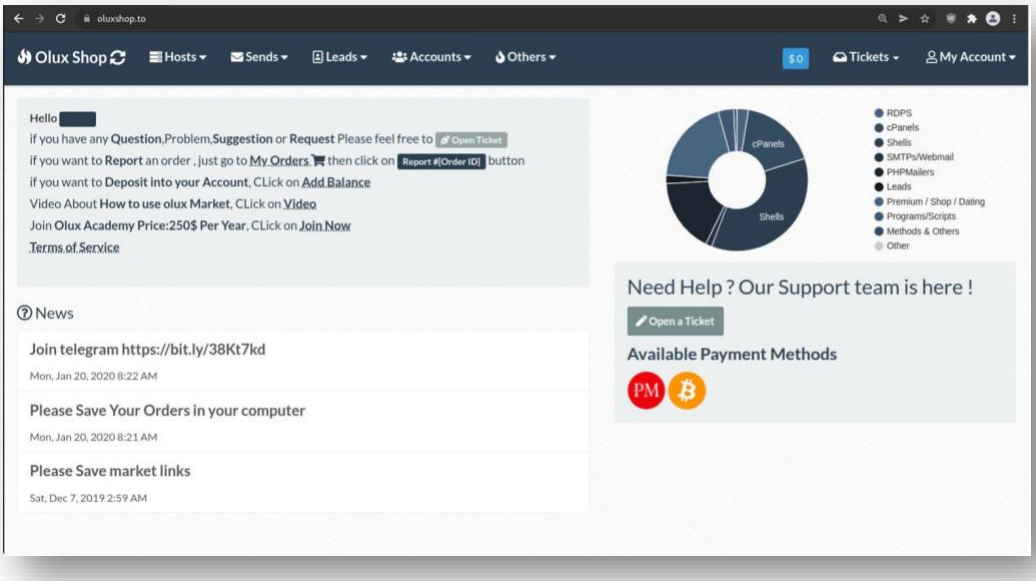
しかし我々が以前公開したレポートでもお伝えしたとおり、サイバー犯罪のエコシステムは、サービタイゼーションと売買の自動化を中心に急速な進化を遂げています。かつてクレジットカードやログの専門ショップが登場した時と同じように、2019 年には企業の Web メールを専門とする新たなショップやマーケットが登場するようになり、その結果サイバー犯罪者の作業もより容易なものとなりました。

このような状況を受けて最近我々も、企業の Web メールアカウントを販売する自動売買ショップ（**XLeet や Odin、Xmina、Lufix など**）を自社のデータレイクに追加しました。それら自動売買ショップでは、ホスティングサービス（cPanels や RDP、シェル）やアカウント（ストリーミングや VPN、電子メールマーケティング）を標的とする様々なスパムツール、攻撃に悪用可能な情報（電子メールアカウントの資格情報やコンボリスト）、企業で使用されている Web メールアカウントなどが販売されています。またこれらショップの多くは、Web メールアカウントのアクセスが実際に使用可能である「証拠」を確認できる、高度な機能を提供しています。この「証拠」には、電子メールアカウントにアクセスできることを実演形式で確認できるタイプのものもあれば、侵害したアカウントの受信ボックスを撮影したスクリーンショットを閲覧できるタイプのものもあります。KELA のサイバー犯罪調査プラットフォームではそれら証拠のデータを収集しており、侵害されたデバイスやユーザーの名前を簡単に確認できる仕組みになっています。

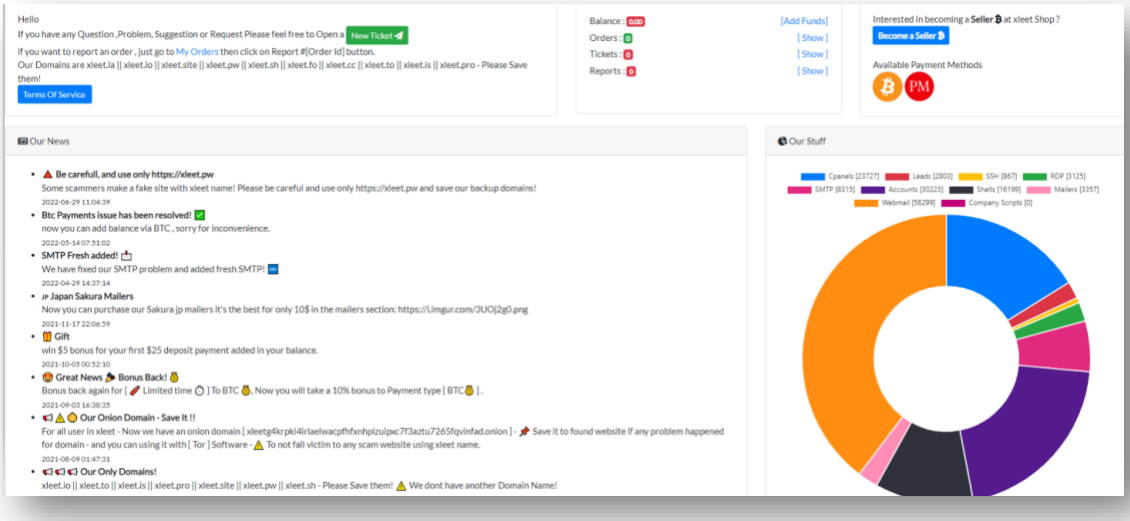
XLeet と Odin の Web メール販売セクションには、サイバー犯罪者にとっての Web メールの使用方法に関する注意書きとして、「Web メールはソーシャルエンジニアリングを用いたハッキングに使用するものであり、大量送信に使用するものではありません」との説明が掲載されています。これは、Web メールとはあくまで 1 件の電子メールアカウントであり、ビジネスメール詐欺（BEC）などのソーシャルエンジニアリング攻撃で使用する商品であること、大量のメッセージを送信する際に使用できる「侵害された SMTP サーバー」とは異なる商品であることを意味していると思われます。



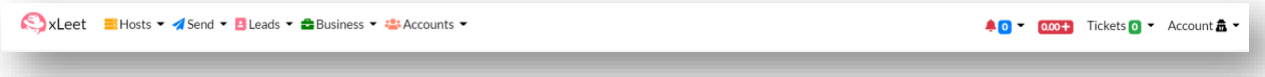
なお、XLeet や Odin、Xmina、Lufix はショップのデザインや機能が似ており、これまでに一部のアクターが「XLeet と Olux は同じソースコードを使用している」と主張していたこと、そして 2022 年 9 月 16 日には某アクターが Olux/XLeet の「スクリプト」を販売すると主張していたことが観察されています。その他 2021 年 7 月 13 日には、某脅威アクターが XLeet や Olux に似たウェブサイトを作る目的で Web 開発者を探していたことが確認されています。さらに XLeet と Olux は同じ商品カテゴリを使用しています。これらの情報を総合すると、XLeet と Odin、Xmina、Lufix は同じようなレイアウトテンプレートを使用している可能性があり、また恐らくは同じソースコードを使用しているものと思われます。



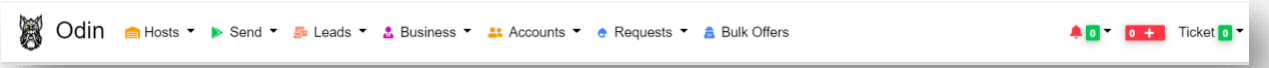
2020 年にソースコードが流出した「Olux」の旧ホームページ



先に掲載した「Olux」の UI を思わせる「XLeet」の UI

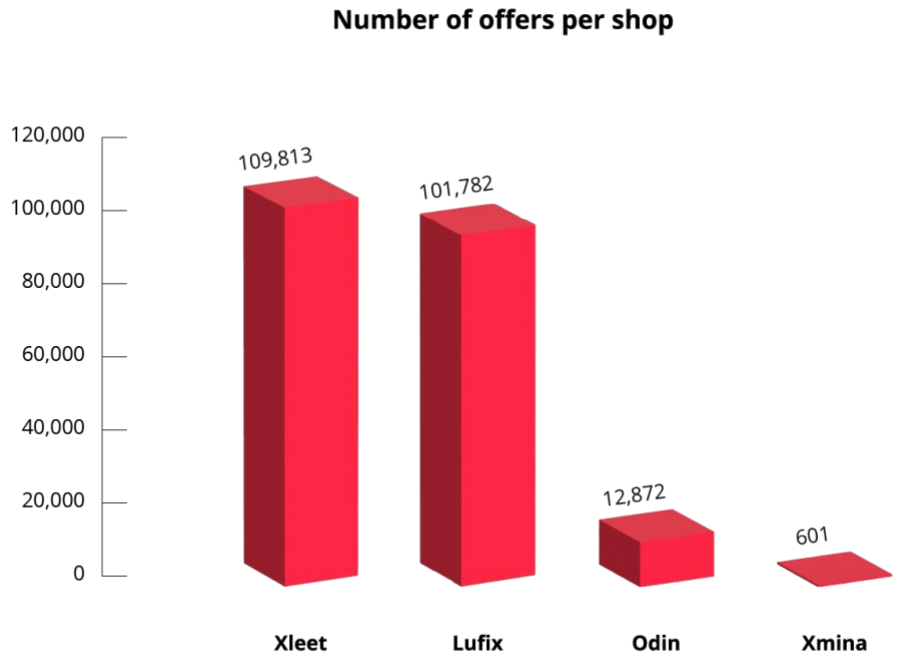


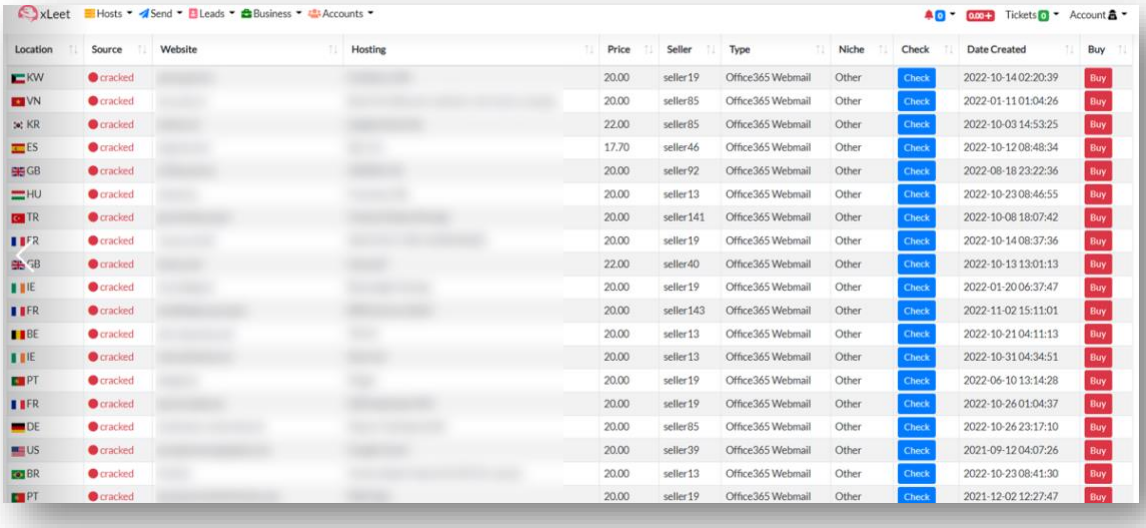
「XLeet」のヘッダーメニュー



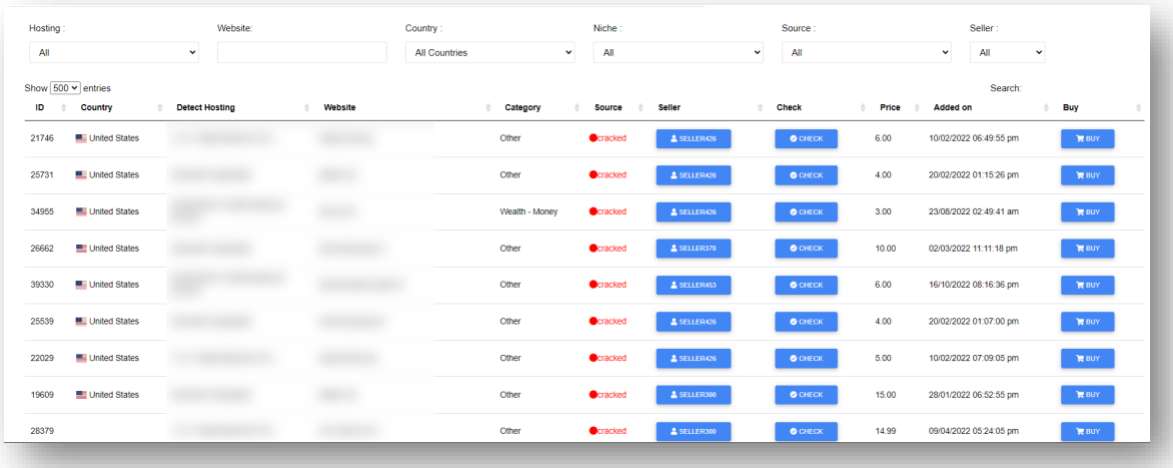
「Odin」のヘッダーメニュー

ショップでは、購入希望者が特定の条件に基づいて電子メールアカウントをソートし、希望の商品を見つけることができる仕組みとなっています。最も成熟しているショップは XLeet であり、同ショップは 2019 年 5 月からサイバー犯罪フォーラムで宣伝を行っています。また XLeet は、販売している資格情報の件数においても最大規模のショップとなっています。

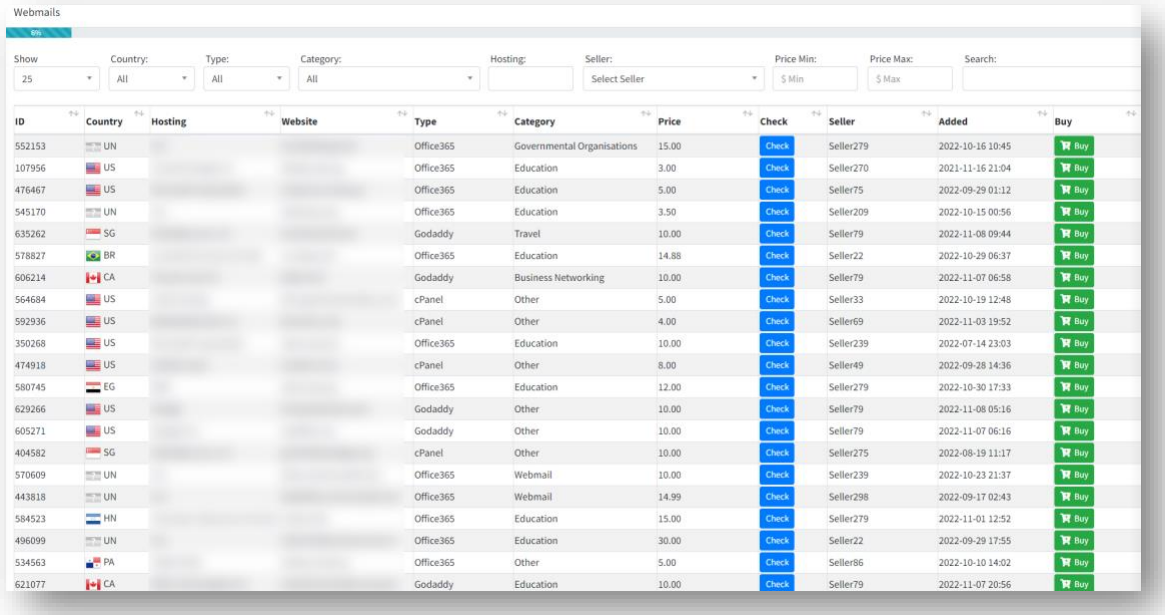




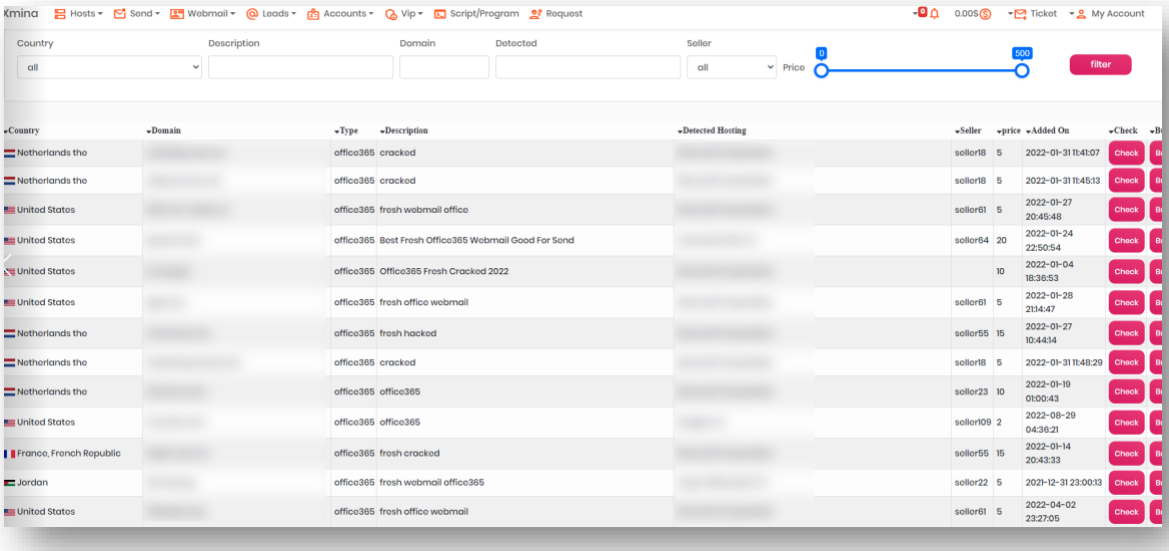
「XLeet」の Web メールセクション



「Odin」の Web メールセクション



「Lufix」の Web メールセクション



「Xmina」の Web メールセクション

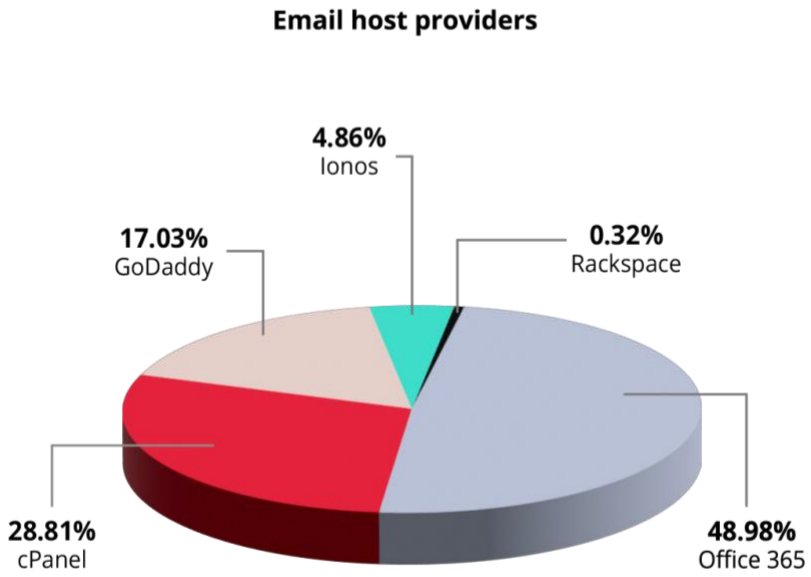
Odin と Lufix は 2020 年から営業していますが、Xmina は 2022 年初旬に登場した新しいショップです。我々の監視活動では、4 ショップ（Odin、Lufix、Xmina、XLeet）全体で **22 万 5,000 件を超える Web メール**が売りに出されていたことを観察しました。今回我々は、このデータをもとに最も大きなショップを特定し、また侵害された電子メールアカウントを購入する際にサイバー犯罪者が最も重視している指標を洗い出しました。

我々が 4 ショップを調査した結果、最も標的とされているビジネス用電子メールプロバイダーは「Microsoft 365」、「GoDaddy」、「Rackspace」、「Ionos」であることが判明しました。また一部のショップでは、「cPanel」へのアクセスも販売していました（cPanel のインターフェースを利用して Web メールにアクセスすることができます）。

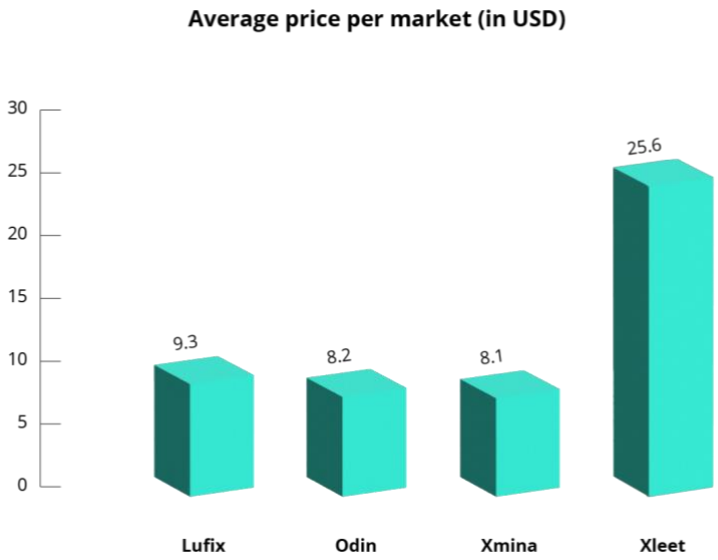
今回調査対象となった 4 ショップの場合、いずれの Web メールセクションも、ユーザーが以下のようなカテゴリで商品をフィルタリングできる仕組みになっています。

- **企業のウェブサイト**

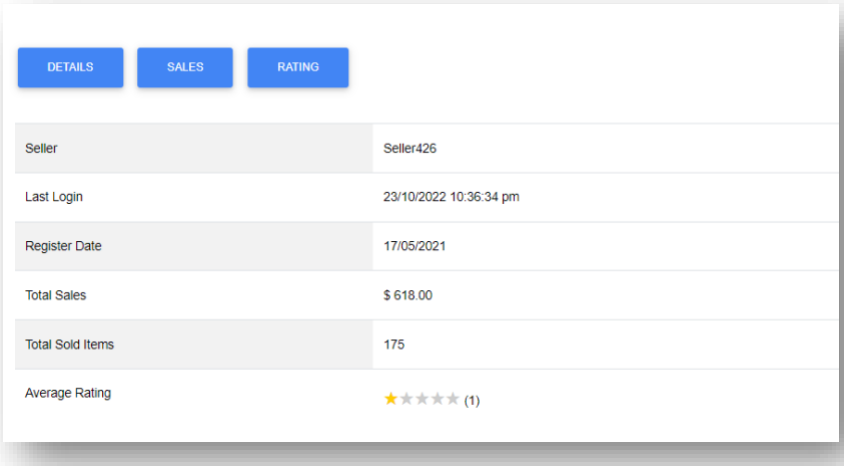
- **国**：4 ショップで宣伝されている電子メールを調査した結果、米国が最も人気の高い国となりました。この理由としては、サイバー犯罪者が高い利益を獲得するべく支払い能力のある収益性の高い企業に重点を置いているということが挙げられます。
- **ビジネス用電子メールプロバイダーの種類**：人気の高さでは Microsoft Office 365 が 1 位となり、その次に cPanel、Godaddy、Ionos、Rackspace が続きました。cPanel の場合、ユーザーは cPanel のインターフェースにある電子メールカテゴリから Web メールにアクセスすることができます。



- **価格**：Lufix や Odina、Xmina で販売されている社用 Web メールの平均価格は 8.5 米ドルとなりました。一方で、XLeet の社用 Web メールの平均価格は、その 3 倍を超える 25.6 米ドルとなりました。



- **分野**：企業の事業分野を指しており、Lufix では「カテゴリ」と呼ばれています。
- **販売者**：販売者は、名前ではなく「販売者 1」や「販売者 2」のように数字で登録されています。ただし Odin では販売者に関する追加情報を提供しており、ユーザーが「販売者」のボタンをクリックすると、その販売者がこれまでに販売したすべての商品、販売金額の合計、評価を閲覧することができます。また、各販売者に寄せられたユーザーからのフィードバックを閲覧することもできます。

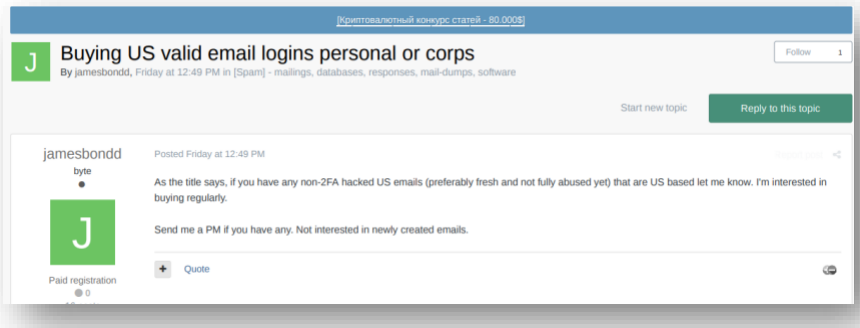


販売者のランクが表示されている様子（Odin）

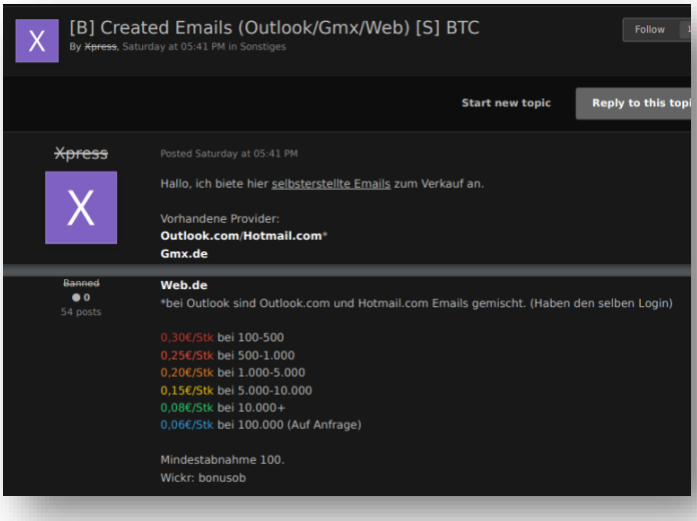
- **ソース**：ソースには、電子メールアカウントのアクセスを入手した方法が表示されます。ソースがカテゴリとして表示されているのは、XLeet と Odin のみであり、その種類は「ハッキング（またはクラッキング）」、「ログ」、「自作（created）」の 3 つに分かれています。XLeet で販売されている電子メールアカウントの場合、その 98%はハッキング（またはクラッキング）によって窃取されていました。

  「ログ」は、情報窃取マルウエアによって窃取されたデータ（電子メールやパスワードを含む）を指す用語です。サイバー犯罪フォーラムでは、脅威アクターが頻繁にログを販売しており、そういった投稿には被害者の Web ブラウザから収集された詳細情報も併せて掲載されています。ログは、ボットネット専用マーケットでボットネットとしても販売されており、その場合はボットマルウエアに感染した端末のユーザーがブラウザに保存していた全アカウント情報が商品（ボットネット）に含まれています。一方、XLeet などの Web メール専用ショップの場合は、ログから抽出した社用メールの資格情報のみがログカテゴリで商品として販売されています。

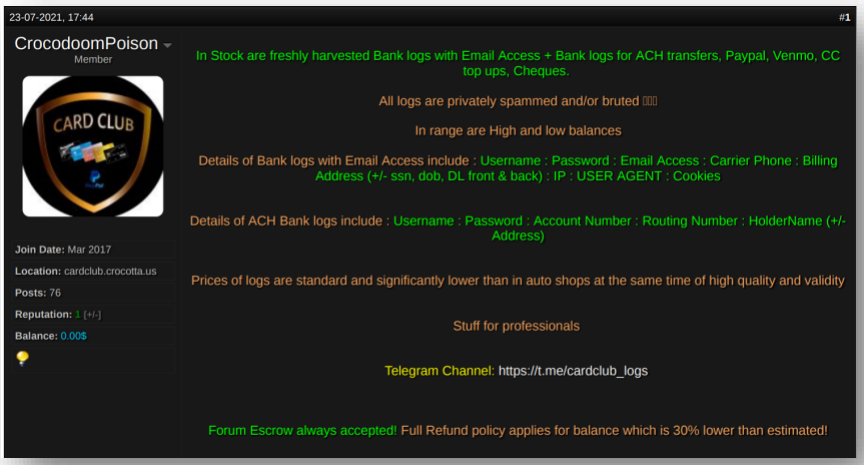
  我々は、3 つ目のカテゴリとなる「自作（created）」とは、アクターが標的企業と同じドメイン名を使用して作成した電子メールアカウントであると考えています。サイバー犯罪フォーラムでは、このような電子メールアカウントも人気の商品となっています。



アクターが「不正アクセスされた電子メールアカウント」の購入を希望している投稿



アクターが「自作した電子メールアカウント」を売りに出している投稿



アクターが銀行のログイン資格情報と電子メールアカウントの
アクセスを販売している投稿

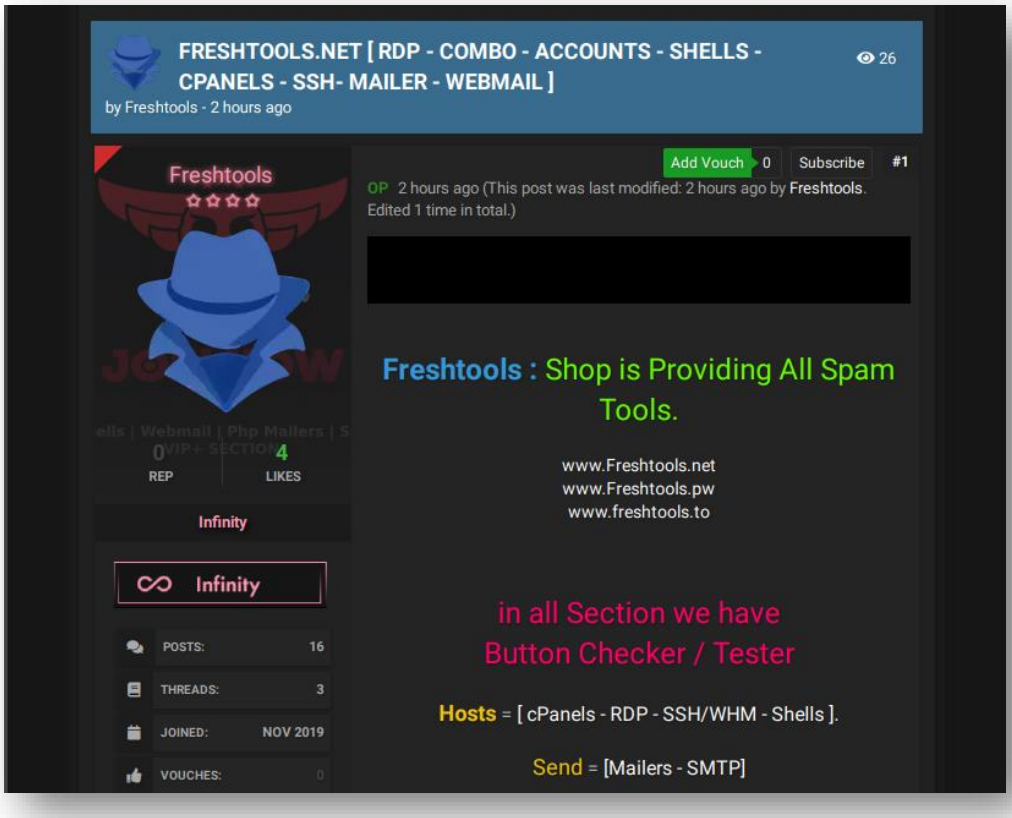
- **チェック用ツール**。窃取した電子メールアカウントの資格情報が有効なものであるのかを確認できる、専用のチェックツールが存在します。またサイバー犯罪者の間で交わされるチャットの情報に基づくと、電子メールアカウントそのものの有効性を確認するツールも数百個存在しています（LetsExtract Email Studio Business、Email Checker Pro、SendBlaster Pro など）。さらに Web メールを専門に扱うショップでは、購入者が実際に Web メールを購入する前に「チェックサービス」を利用できるようになっており、アクターが購入したい Web メールを決定した後に「チェック」ボタンをクリックすると、その Web メールの資格情報が現在も有効であるか否かを確認することができる仕組みになっています（下図参照）。

Price	Seller	Type	Niche	Check	Date Created	Buy
20.00	seller143	Office365 Webmail	Other	Check	2022-11-13 09:31:10	Buy
20.00	seller139	Office365 Webmail	Other	Check	2022-09-07 09:35:10	Buy
20.00	seller139	Office365 Webmail	Other	Check	2022-08-24 09:37:12	Buy
25.30	seller92	Office365 Webmail	Other	noT working	2021-10-16 13:01:18	Buy
20.00	seller19	Office365 Webmail	Other	Check	2022-02-20 05:20:39	Buy
15.00	seller7	Office365 Webmail	Other	Check	2022-11-09 13:17:52	Buy
20.00	seller141	Office365 Webmail	Other	Check	2022-09-13 15:07:14	Buy
15.00	seller19	Office365 Webmail	Other	Check	2022-11-14 12:12:40	Buy
20.00	seller139	Office365 Webmail	Other	Check	2022-10-08 12:05:50	Buy
20.00	seller13	Office365 Webmail	Other	Working	2022-11-16 01:38:56	Buy

「チェック」ボタンをクリックすると、Web メールアカウントのアクセスが有効か否か判明する。

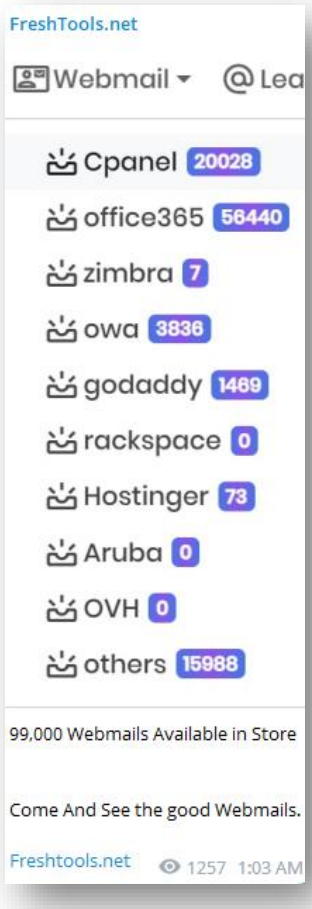
その他のショップや Telegram チャンネル

これまでに詳述したとおり、自動売買ショップはサイバー犯罪者の間で注目を集めており、先述のショップよりも規模は小さいものの、同様のサービス（Web メール、SMTP、シェル、RDP、cPanel、その他）を販売しているショップは他にも存在します。以下に取りあげる「FreshTools」もそのうちのひとつです。



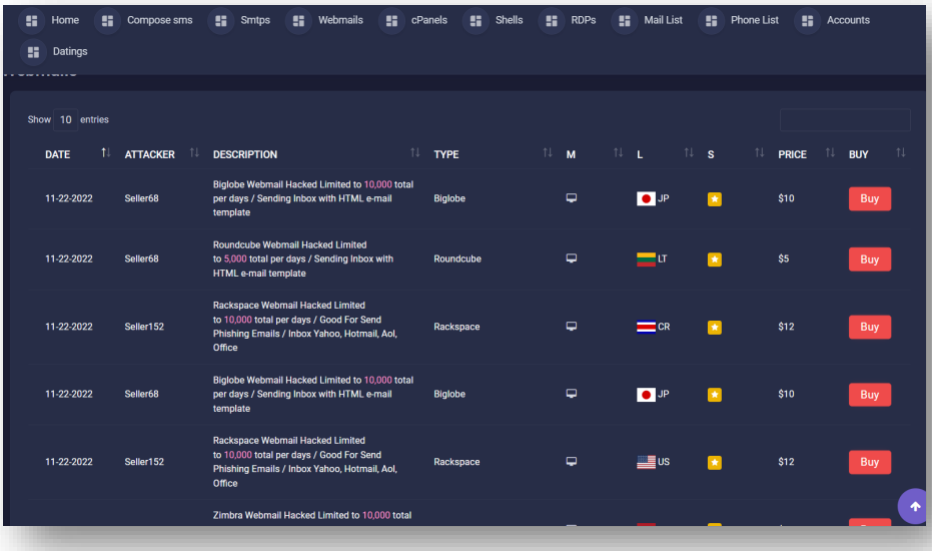
フォーラム「Cracked」に掲載された「FreshTools」の広告

FreshTools は Telegram でもチャンネルを開設しており、チャンネル登録者数は 1,000 人を超えています。我々が監視している他のショップと同様に、FreshTools で多く扱われている商品の電子メールプロバイダーは Office 365 です。FreshTools のチャンネル管理者は、ショップが新たに導入したチェックツールや投入した商品（Web メール）に関する最新情報をチャンネル上で公開しています。またこのチャンネルにはボット機能があり、購入者や販売者が注文や返金、その他に関する最新情報を受け取れるようになっています。



「FreshTools」は Web メールセクションを定期的に更新し、
様々な電子メールホスティングプロバイダーを追加している。

その他には、アクター「0daysec」が「HaxorID」という名のウェブサイトを宣伝していたことも確認されています。この HaxorID は、攻撃者がウェブサイトの改ざんに関する情報を公開する場となっていますが、様々なハッキングツールや Web メールアカウントのアクセスも販売しています。このサイトで販売されている Web メールのプロバイダーは、Office365 や Zimbra、Godaddy、Owa、Hostinger、cPanel などであり、価格は 5 米ドル～12 米ドルとなっています。ただし、同サイトの Web メールセクションで販売されている電子メールアカウント数はわずか 20 件にとどまっています（本ブログ執筆時点）。



「HaxorID」の Web メールセクション

社用メールがサイバー攻撃へと発展するまで

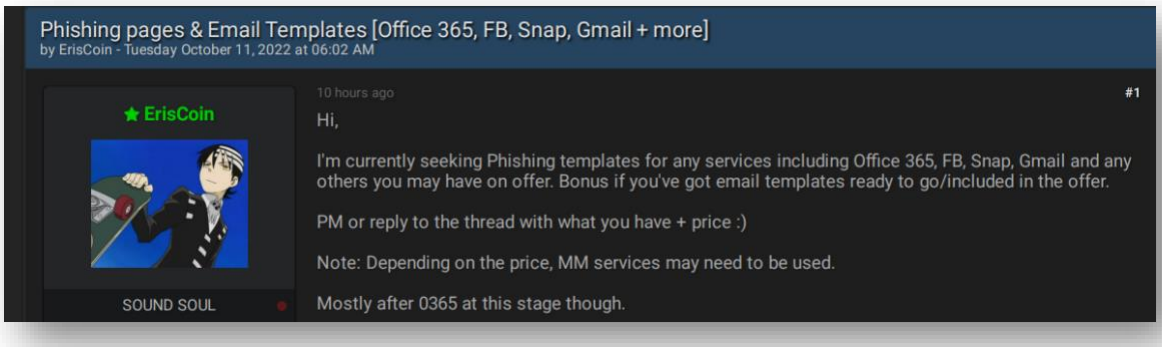
サイバー犯罪のサプライチェーンには、電子メールを悪用して利益を手にしようと目論む様々な利害関係者が関わっています。販売者となるアクターは、ショップやフォーラムを利用して電子メールアカウントのアクセスを販売し、一方購入者となるアクターは、それらのアクセスをそのまま収益化したり、さらに大きな利益を生み出すであろうサイバー攻撃に利用しています。今やアクターは、侵害した社用メールアカウントをフィッシングからビジネスメール詐欺（BEC）やマルウエアを使った攻撃にいたるまで、様々な手口に悪用しているのです。

サイバー犯罪者の間で交わされるチャットを調査すると、電子メールアカウントのアクセスを収益化するにあたって実に様々な手法があることがうかがえます。例えば、スキルの低いアクターであればサイバー犯罪フォーラムでアクセスを販売し、「電子メールアカウントのサプライチェーン」の一員になるというパターンが考えられ、単独で攻撃を行う熟練アクターであれば、アクセスを利用してより高度な攻撃を実行するというパターンが考えられるでしょう。次のセクションでは、想定される攻撃パターンについて解説します。

フィッシングによる電子メールアカウントの収益化

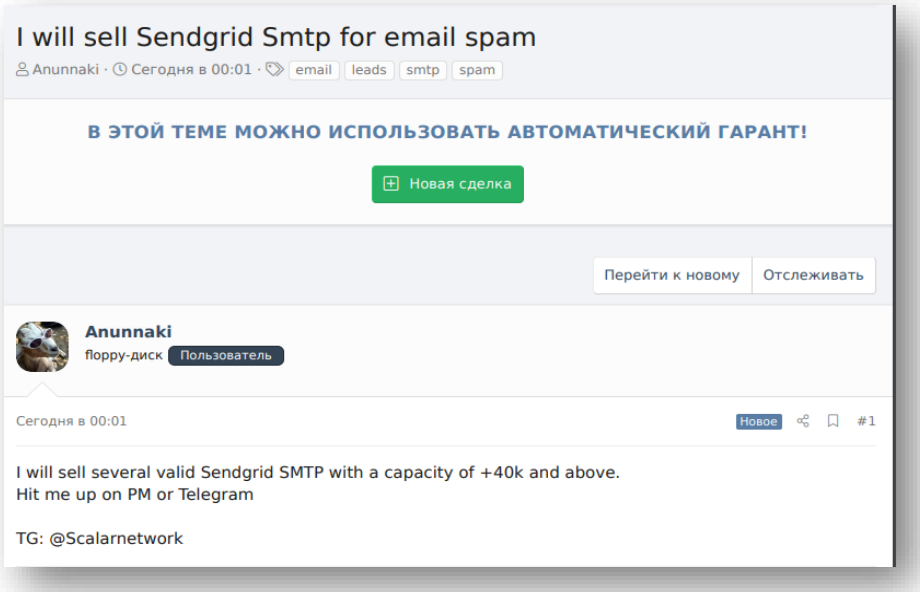
フィッシングはよく使われている攻撃手法であり、被害者をおびき寄せてパスワードやクレジットカード番号などの機密情報を明かすよう誘導します。フィッシング攻撃は人的ミスを悪用し、被害者が「信用できる」と見なす組織に機密情報を提供するよう行動を操る、ソーシャルエンジニアリング戦術がベースとなっています。そのため、フィッシングメールを配信する際に企業の電子メールアカウントを使用できれば、被害者からの信頼を得やすく、攻撃者にとって有利になります。

アンダーグラウンドのサイバー犯罪社会では、専用のテンプレートからフィッシングページやフィッシングキットにいたるまで、フィッシング攻撃のプロセスを容易にするツールやチュートリアルを入手することができます。



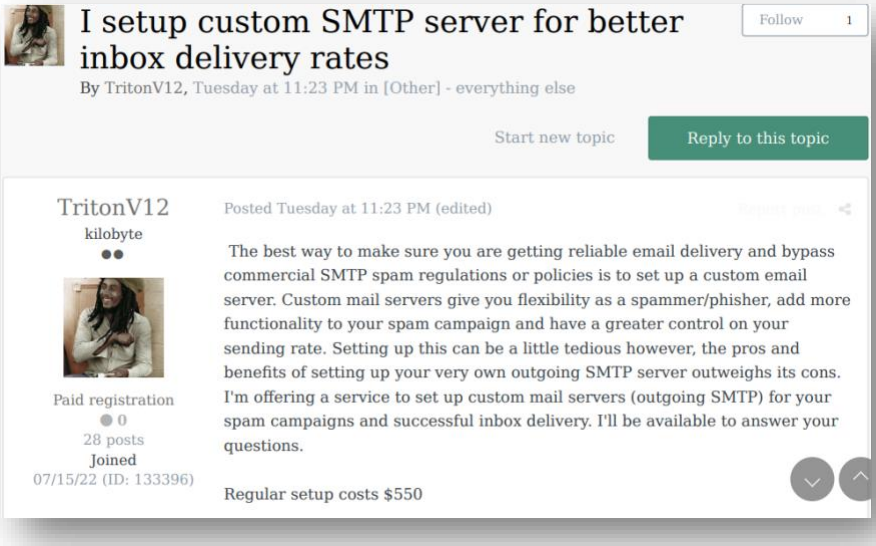
アクターが Office 365 をはじめとする様々な電子メールサービスの
フィッシング用テンプレートを探している投稿

サイバー犯罪フォーラムには、フィッシング攻撃のプロセスを容易にすると謳う様々な SMTP サービスが存在します。例えば、侵害した SMTP サーバーを悪用すれば、侵害された組織のドメインを使用してフィッシングメールを正当なものに見せつつ、多数の人々に送信することが可能となります。



アクターがスパムメールに利用可能な「Sendgrid」の

SMTP サーバー（又はサービス）を販売している投稿



アクターがスパムキャンペーンやフィッシングキャンペーンに利用可能な

SMTP サーバーを販売している投稿

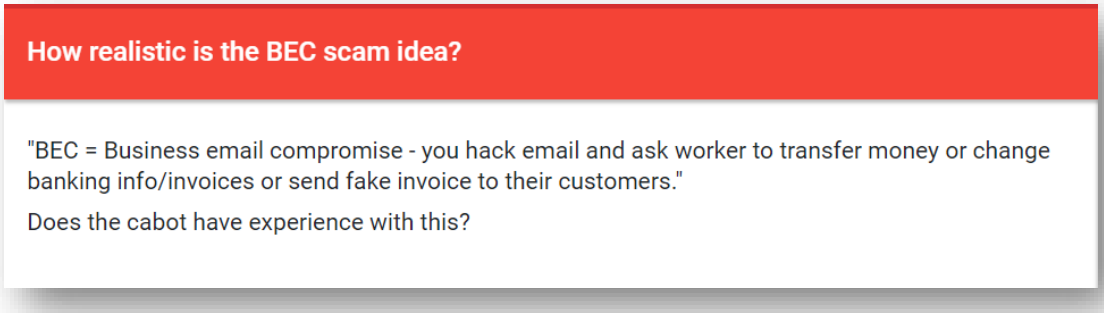
合法的な企業で使用されている社用メールアカウントのアクセスが自動売買ショップで販売されているという状況、そして上述したようなツールが存在しているという状況が、今やフィッシング攻撃のプロセスを著しく容易なものにしており、その結果、スキルのない多数のアクターがフィッシング攻撃に惹きつけられる事態となっています。

ビジネスメール詐欺による電子メールアカウントの収益化

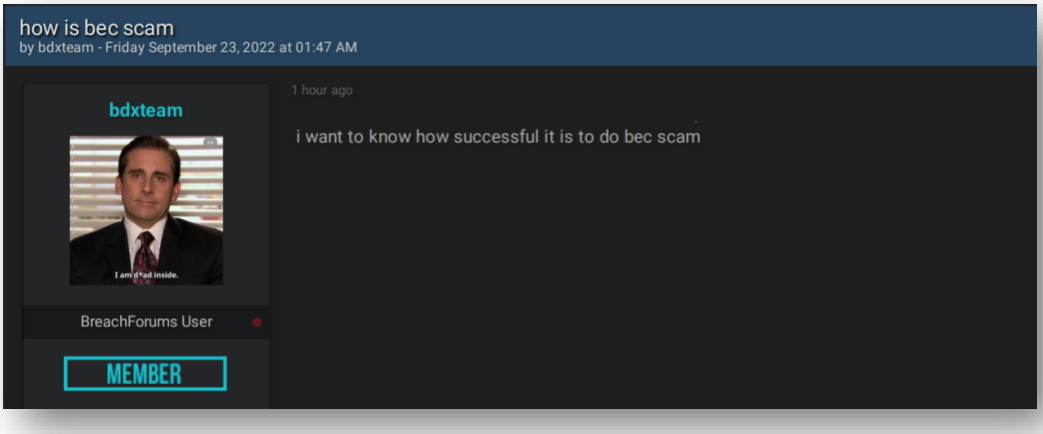
ビジネスメール詐欺（BEC）とは、被害者を騙して攻撃者が管理するアカウントや場所に資金を送金させる攻撃手法であり、電子メールアカウント侵害（EAC：Email Account Compromise）とも呼ばれています。2021 年に米連邦捜査局（FBI）が行った報告では、ビジネスメール詐欺で窃取された被害金額の合計が、ランサムウエア攻撃で窃取された被害金額の総額を大幅に上回っていることが判明しました[1]。ビジネスメール詐欺の場合は主にソーシャルエンジニアリングを駆使するため、マルウエア攻撃ほどに高度な技術的スキルは必要ありません。にもかかわらずその収益性が非常に高いことから、サイバー犯罪のエコシステムでビジネスメール詐欺の人気が高まっています。

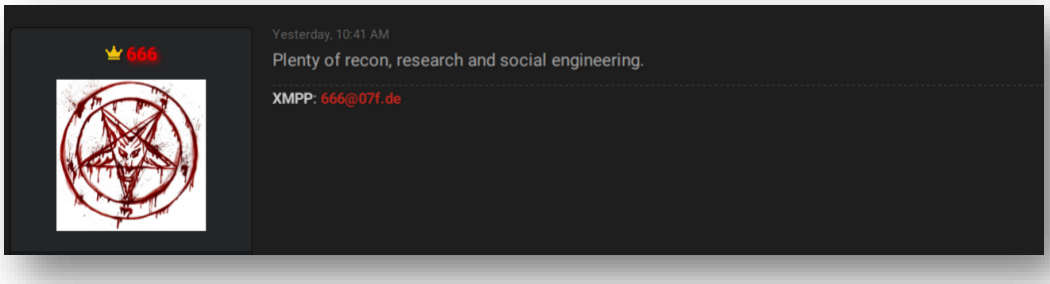
そして脅威アクターの間でも、ビジネスメール詐欺に関する質問や情報共有が行われています。例えばアクター「arch6661」は、ビジネスメール詐欺に従事している人物を探すメッセージをフォーラム「XSS」に投稿していました。恐らくこの arch6661 は、ビジネスメール詐欺を実行して金銭を窃取するだけのスキルを有するハッカーを探していたものと思われます。その後、この呼びかけに対して別のアクター「TESTAROSSA」が「自分はビジネスメール詐欺を行っており、2 万～2000 万米ドルの金銭を窃取できる」と返信していました。

[1]ランサムウエア攻撃による損失額の合計が 4,900 万米ドルであったのに対し、ビジネスメール詐欺による損失額の合計は 24 億米ドルとなりました。なお、身代金を支払ったか否かに関する情報については透明性に欠けるため、ランサムウエア攻撃による経済的損失については追跡することがより困難である点にご留意ください。また、米連邦捜査局（FBI）の報告は、被害者からの自主的な申し立て 3,729 件に基づいたものであり、実際にはそれ以上の被害者が存在しています。



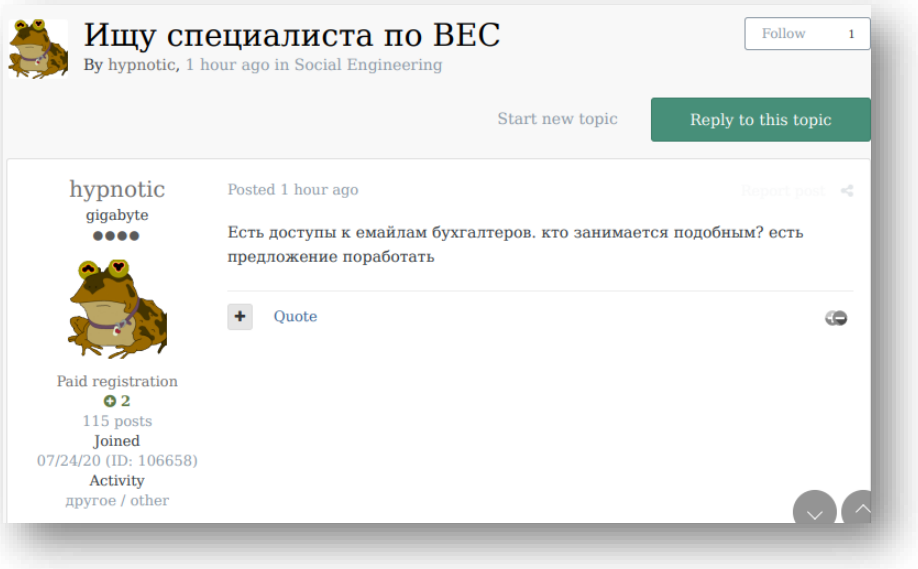
アクターがビジネスメール詐欺（BEC）の目的について説明している投稿



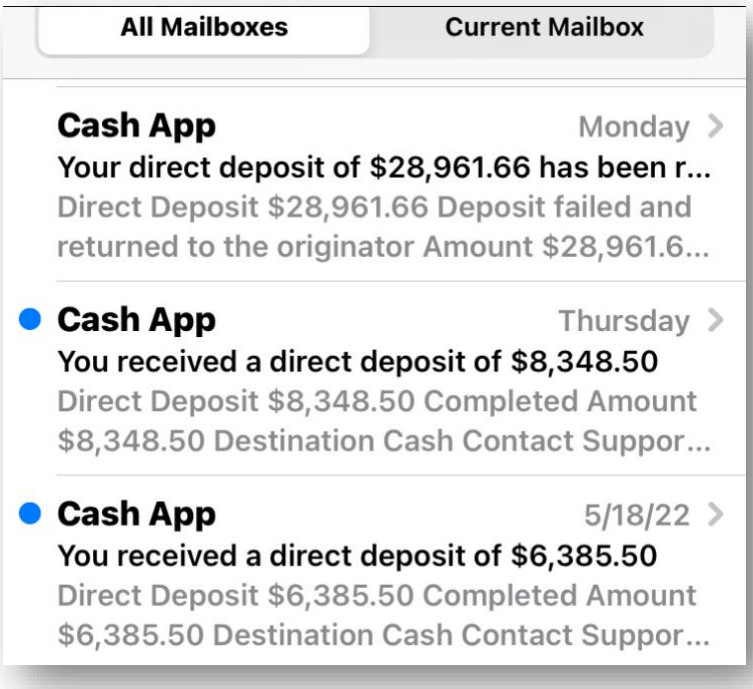


「Actor 666」が、ビジネスメール詐欺を成功させるには複数の戦術が必要であると主張している投稿

サイバー犯罪者同士が協力した事例は他にもあります。2022 年 7 月 7 日には、アクター「hypnotic」が「経理担当者の電子メールにアクセス可能な、ビジネスメール詐欺のスペシャリストを探している」とのメッセージを Exploit に投稿しました。この hypnotic は、偽の請求書に対する支払処理に必要な権限と業務上の資格情報を持つ財務会計担当者の電子メールアカウントを標的にしようと考えていたものと思われます。その後、この呼びかけに対してアクター「LastOneLeft」が、「複数の経理担当者アカウントで『仕事』をしており、すでに大金を窃取している」と返信し、さらにその証拠をスクリーンショットにして投稿していました。



アクターがビジネスメール詐欺の専門家を探している投稿



アクターがビジネスメール詐欺に成功し、金銭を窃取した証拠を掲載した投稿

また、組織の CEO や CFO を標的とした最近のビジネスメール詐欺キャンペーンでは、「Adversary-in-The-Middle（AiTM）」というテクニックを使ったスピアフィッシング攻撃が行われ、多要素認証で保護されていた企業幹部の Microsoft 365 アカウントさえもが不正アクセスを受けていました。

ビジネスメール詐欺の場合、アクター1 人で数千もの企業を標的にし、数百万ドルもの損害をもたらすことが可能となります。さらに今では自動売買マーケットのおかげで、アクターが多数の社用メールアカウントを標的に、より大規模な攻撃を簡単に実行できるようになっています。ビジネスメール詐欺を行うサイバー犯罪グループ「SilverTerrier」を例に挙げると、同グループが標的にした被害者の数は 5 万人を超えていました。SilverTerrier は世界中の企業数千社に対して詐欺行為を働いており、2021 年には同グループのメンバー数人が逮捕される事態となりました。この時インターポールが行った発表によると、メンバーの 1 人が所有していたノート PC には、80 万件を超える潜在的被害者（組織）のメールアカウント資格情報が保存されていたということです。

マルウエアによる電子メールアカウントの収益化

マルウエア攻撃とは、ランサムウエアや情報窃取型トロイの木馬、スパイウエアなど、あらゆる種類の悪意あるソフトウエアを使った攻撃を指します。サイバー犯罪者は、侵害した企業の電子メールアカウントを使用してソーシャルエンジニアリングを行い、被害者をおびき寄せて悪意あるペイロードをダウンロードさせることにより、標的のネットワークにマルウエアを展開するための最初の侵入経路を確保することが可能となります。

アクターは、被害者（組織）の端末にマルウエアをインストールすることによって、簡単に利益を手にすることができるようになります。例えば、情報窃取型トロイの木馬を被害者の端末等にインストールすれば、被害者が銀行口座で使用している資格情報を窃取して口座に不正アクセスし、現金を引き出すことが可能となります。またランサムウエアを展開すれば、身代金を要求することも可能となります。ランサムウエアグループは、自らの活動をスピーディに収益化するべく恐喝行為を戦術として採用しており、被害者が身代金を支払わない場合は重要なデータを公開すると脅迫しています。

一方、サイバー犯罪フォーラムでは、脅威アクターが様々なマルウエアのキャンペーンについて情報を共有しています。2022 年 3 月 29 日には脅威アクター「digitalninja」が、マルウエアを拡散する最も良い方法について質問していました。この問いに対して寄せられた回答は、まさにサイバー犯罪のサプライチェーンに出回っている電子メールアカウントのアクセスに価値があることを意味するものでした。例えば脅威アクター「n0nce」が寄せた回答の中では、数人の標的を選んで個別に電子メールを送信するという手口が提案されていました。

また昨年は、大手の家具量販会社「IKEA」社がサイバー攻撃を受けましたが、この攻撃は同社の電子メールアカウントが侵害されていたことに端を発したものでした。攻撃主であった脅威アクターは窃取した返信メールを悪用して、IKEA 社従業員を標的とした内部的なフィッシング攻撃を展開しており、IKEA 社は従業員に対して、「進行中のやり取りに対する返信を装って、従業員の電子メールアカウントから攻撃（悪意あるメールの配信）が行われている」と警告していました。またこのインシデントで送信された電子メールには、受信者のデバイスにマルウエアをインストールする機能を持つ、不正な文書が添付されていました。

意識向上が重要なポイント

サイバー犯罪者は、多額の金銭を手にすることのできる新たな攻撃手法を常に模索しています。2022 年 2 月には研究者から、これまで以上に多くの組織（78%）が電子メールに端を発したランサムウエア攻撃の被害にあっており、僅差でビジネスメール詐欺（77%）が続いているとの報告が寄せられています。この調査結果は、技術的な脆弱性を悪用する攻撃手法よりも人間の行動を操る攻撃手法を好むタイプのサイバー犯罪者にとって、電子メールが好ましい攻撃経路となっていることを表しています。今や侵害された社用メールアカウントは、フィッシングやビジネスメール詐欺、様々なマルウエアによる感染などの攻撃を通じて簡単に収益化できる、貴重なアイテムとなっているようです。

サイバー犯罪のエコシステムではサービタイゼーションと売買の自動化に重点が置かれており、Web メール専門ショップが賑わいを見せています。そして XLeet や Odin、Xmina、Lufix などのショップが企業の Web メールを販売しているおかげで、サイバー犯罪者も大量の電子メールを手頃な価格で購入して多数の標的を攻撃することが可能となり、彼らの活動がこれまでよりも容易なものとなりました。

こういった状況を鑑み、組織の皆様におかれましては、以下の活動を確実かつ継続的に実行されるよう提言いたします。

- **従業員、顧客、サプライヤーおよびパートナー企業**にサイバー分野に関するトレーニングを行い、オンライン上での資格情報および個人情報の安全な取り扱い方法を教示します。またこのトレーニングでは、疑わしい活動（詐欺の可能性がある電子メールや認証されていない個人・電子メールアドレスからの異常なリクエストなど）を特定する方法についても説明します。組織のサイバーセキュリティにおいては人的要因が重要な役割を果たすため、組織の規模が大きくなればなるほどサイバー犯罪者にとっては攻撃の機会が増加します。したがって、先述したサイバーセキュリティトレーニングを策定し、顧客やサプライヤー・パートナー企業を含むすべての組織において受講を必須とすることで、従業員のミスを利用した侵害が生じる可能性を大幅に低減することができます。

- 組織の従業員や顧客に対し、使用しているすべてのサービスおよびプラットフォームにおける**定期的なパスワード変更**を課します。また新しいパスワードについては、侵害されたユーザーが現在またはこれまでに使用していたパスワードとは異なるものとします。
- **サイバー犯罪業界の状況を監視**して、新たな傾向や脅威を確認します。攻撃者は、新たな詐欺の手口を日々開発しています。そのためサイバー犯罪者の戦術を理解し、サイバー犯罪マーケットに精通することで、進化する脅威により効果的に対処するとともに経済的損失を減少させることが可能となります。

我々は常時様々なショップを監視し、侵害された社用 Web メールに関する状況を調査しています。そしてそれらの情報をもとにインテリジェンスをリアルタイムに配信し、お客様企業が不正アクセスされたアカウントを特定してサイバー攻撃を防止することができるよう支援しています。

KELA のサイバー犯罪インテリジェンスプラットフォームは、お客様を脅かす脅威を数分で特定します（無料）。是非お試しください。